Erste Schritte in Microsoft Azure

Cloud Volumes ONTAP

NetApp
November 17, 2022

Inhaltsverzeichnis

Erste Schritte in Microsoft Azure

Schnellstart für Cloud Volumes ONTAP in Azure

Erste Schritte mit Cloud Volumes ONTAP für Azure

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 BlueXP (früher Cloud Manager) aufgefordert, einen Connector bereitzustellen, falls noch nicht vorhanden ist.

BlueXP 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 .".

<img src="https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-3.png" alt=„drei“> Einrichten des Netzwerks

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".

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

- "Erstellen eines Connectors von BlueXP"
- "Erstellen eines Connectors über den Azure Marketplace"
- "Installieren der Connector-Software auf einem Linux-Host"
- "Was BlueXP mit Berechtigungen macht"

Planen Sie Ihre 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.

Wählen Sie eine Cloud Volumes ONTAP Lizenz

Für Cloud Volumes ONTAP sind verschiedene Lizenzierungsoptionen verfügbar. Jede Option ermöglicht Ihnen, ein Nutzungsmodell auszuwählen, das Ihren Anforderungen entspricht.

- "Informieren Sie sich über Lizenzoptionen für Cloud Volumes ONTAP"
- "Erfahren Sie, wie Sie eine Lizenzierung einrichten"

Wählen Sie eine unterstützte Region aus

Cloud Volumes ONTAP wird in den meisten Microsoft Azure Regionen unterstützt. "Hier finden Sie die vollständige Liste der unterstützten Regionen".

Wählen Sie einen unterstützten VM-Typ aus

Cloud Volumes ONTAP unterstützt je nach Lizenztyp mehrere VM-Typen.

"Unterstützte Konfigurationen für Cloud Volumes ONTAP in Azure"

Analysieren Sie Ihre Storage-Grenzen

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-Grenzen für Cloud Volumes ONTAP in Azure"

Größe 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. BlueXP verwendet diese Festplattengröße für das anfängliche Aggregat und für alle zusätzlichen Aggregate, die es beim Verwenden der einfachen Bereitstellungsoption erstellt. 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. Beispiel: Durch das Auswählen von 1 tib Festplatten kann eine bessere Performance als 500 gib Festplatten zu höheren Kosten erzielt werden.

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"

Anzeigen von Standard-Systemfestplatten

Neben dem Storage für Benutzerdaten erwirbt BlueXP auch Cloud-Storage für Cloud Volumes ONTAP Systemdaten (Boot-Daten, Root-Daten, Core-Daten und NVRAM). Für die Planung können Sie diese Details überprüfen, bevor Sie Cloud Volumes ONTAP implementieren.

"Zeigen Sie die Standardfestplatten für Cloud Volumes ONTAP-Systemdaten in Azure an".

Für den Connector ist außerdem eine Systemfestplatte erforderlich. "Zeigen Sie Details zur Standardkonfiguration des Connectors an".

Sammeln von Netzwerkinformationen

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	

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

Wählen Sie eine Schreibgeschwindigkeit

Mit BlueXP können Sie eine Schreibgeschwindigkeitseinstellung für Cloud Volumes ONTAP auswählen. 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. "Erfahren Sie mehr über Schreibgeschwindigkeit".

Wählen Sie ein Volume-Auslastungsprofil aus

ONTAP umfasst mehrere Storage-Effizienzfunktionen, mit denen Sie die benötigte Storage-Gesamtmenge reduzieren können. Wenn Sie ein Volume in BlueXP 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 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

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

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

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

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

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

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

Wenn Sie von BlueXP darüber informiert werden, dass AutoSupport-Meldungen nicht gesendet werden können, "Fehler bei der AutoSupport Konfiguration beheben".

IP-Adressen

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

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

Beachten Sie, dass BlueXP in Azure eine SVM Management-LIF auf HA-Paaren erstellt, nicht jedoch auf Systemen mit einzelnen Nodes.

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

Sichere Verbindung zu Azure Services

Standardmäßig aktiviert BlueXP einen Azure Private Link für Verbindungen zwischen Cloud Volumes ONTAP- und Azure-Speicherkonten.

In den meisten Fällen müssen Sie nichts tun – BlueXP managt den Azure Private Link für Sie. Aber wenn Sie Azure Private DNS verwenden, dann müssen Sie eine Konfigurationsdatei bearbeiten. Sie sollten auch eine Anforderung für den Connector-Standort in Azure kennen.

Sie können die Private Link-Verbindung auch deaktivieren, wenn dies von Ihren geschäftlichen Anforderungen erforderlich ist. Wenn Sie den Link deaktivieren, konfiguriert BlueXP stattdessen Cloud Volumes ONTAP für die Verwendung eines Service-Endpunkts.

"Weitere Informationen zur Verwendung von Azure Private Links oder Service-Endpunkten mit Cloud Volumes ONTAP".

Verbindungen zu anderen ONTAP Systemen

Um Daten zwischen einem Cloud Volumes ONTAP System in Azure und ONTAP Systemen in anderen Netzwerken zu replizieren, benötigen Sie eine VPN-Verbindung zwischen dem Azure vnet und dem anderen Netzwerk, beispielsweise Ihrem Unternehmensnetzwerk.

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

Port für den HA Interconnect

Ein Cloud Volumes ONTAP HA-Paar enthält einen HA Interconnect, der jedem Knoten erlaubt, kontinuierlich zu überprüfen, ob sein Partner funktioniert und um Protokolldaten für den anderen nichtflüchtigen Speicher zu spiegeln. Das HA Interconnect verwendet TCP Port 10006 für die Kommunikation.

Standardmäßig ist die Kommunikation zwischen den HA Interconnect LIFs offen, und es gibt keine Sicherheitsgruppenregeln für diesen Port. Wenn Sie jedoch eine Firewall zwischen den HA Interconnect LIFs erstellen, müssen Sie sicherstellen, dass TCP Traffic für Port 10006 offen ist, damit das HA-Paar ordnungsgemäß arbeiten kann.

Nur ein HA-Paar in einer Azure-Ressourcengruppe

Sie müssen für jedes Cloud Volumes ONTAP HA-Paar, das Sie in Azure implementieren, eine *dedizierte* Ressourcengruppe verwenden. Es wird nur ein HA-Paar in einer Ressourcengruppe unterstützt.

Bei BlueXP treten Verbindungsprobleme auf, wenn Sie versuchen, ein zweites Cloud Volumes ONTAP HA-Paar in einer Azure Ressourcengruppe bereitzustellen.

Sicherheitsgruppen

Sie müssen keine Sicherheitsgruppen erstellen, weil BlueXP das für Sie tut. Wenn Sie Ihre eigene Verwendung benötigen, lesen Sie die unten aufgeführten Sicherheitsgruppenregeln.

Regeln für Sicherheitsgruppen

BlueXP 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

Wenn Sie eine Arbeitsumgebung erstellen und eine vordefinierte Sicherheitsgruppe auswählen, können Sie den Datenverkehr innerhalb einer der folgenden Optionen zulassen:

- **Nur vnet ausgewählt**: Die Quelle für eingehenden Datenverkehr ist der Subnetz-Bereich des vnet für das Cloud Volumes ONTAP-System und der Subnetz-Bereich des vnet, in dem sich der Connector befindet. Dies ist die empfohlene Option.
- **Alle VNets**: Die Quelle für eingehenden Datenverkehr ist der IP-Bereich 0.0.0.0/0.

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	Konnektivität mit dem Connector und 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
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

Priorität und Name	Port und Protokoll	Quelle und Ziel	Beschreibung
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

Wenn Sie eine Arbeitsumgebung erstellen und eine vordefinierte Sicherheitsgruppe auswählen, können Sie den Datenverkehr innerhalb einer der folgenden Optionen zulassen:

- **Nur vnet ausgewählt**: Die Quelle für eingehenden Datenverkehr ist der Subnetz-Bereich des vnet für das Cloud Volumes ONTAP-System und der Subnetz-Bereich des vnet, in dem sich der Connector befindet. Dies ist die empfohlene Option.
- **Alle VNets**: Die Quelle für eingehenden Datenverkehr ist der IP-Bereich 0.0.0.0/0.

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	Konnektivität mit dem Connector und 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)

Service	Port	Protokoll	Quelle	Ziel	Zweck
AutoSupport	HTTPS	443	Node Management-LIF	support.netapp.com	AutoSupport (HTTPS ist der Standard)
	HTTP	80	Node Management-LIF	support.netapp.com	AutoSupport (nur wenn das Transportprotokoll von HTTPS zu HTTP geändert wird)
	TCP	3128	Node Management-LIF	Stecker	Senden von AutoSupport-Nachrichten über einen Proxy-Server auf dem Connector, falls keine ausgehende Internetverbindung verfügbar ist
DHCP	68	UDP	Node Management-LIF	DHCP	DHCP-Client für die erstmalige Einrichtung
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

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.

Endpunkte	Zweck
https://support.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport Meldungen an den NetApp Support zu senden.
https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com	Um SaaS-Funktionen und -Services in BlueXP zur Verfügung zu stellen.
https://cloudmanagerinfraprod.azurecr.io https://*.blob.core.windows.net	Aktualisierung des Connectors und seiner Docker Komponenten.

Regeln für Sicherheitsgruppen

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

Regeln für eingehende Anrufe

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
TCP	3128	Ermöglicht Cloud Volumes ONTAP den Zugang zum Internet, um AutoSupport-Nachrichten an den NetApp Support zu senden. Sie müssen diesen Port nach der Bereitstellung des Connectors manuell öffnen.

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
API-Aufrufe und AutoSupport	443	HTTPS	Outbound-Internet und ONTAP Cluster Management LIF	API-Aufrufe an Azure und ONTAP, Cloud Data Sense, zum Ransomware-Service und Senden von AutoSupport-Nachrichten an NetApp
DNS	53	UDP	DNS	Wird für DNS Resolve von BlueXP verwendet

Cloud Volumes ONTAP einrichten, um einen vom Kunden gemanagten Schlüssel in Azure zu verwenden

Die Daten werden auf Cloud Volumes ONTAP in Azure automatisch verschlüsselt "Azure Storage Service Encryption" Mit einem von Microsoft gemanagten Schlüssel Aber Sie können Ihren eigenen Verschlüsselungsschlüssel verwenden, indem Sie die Schritte auf dieser Seite befolgen.

Übersicht über die Datenverschlüsselung

Cloud Volumes ONTAP-Daten werden in Azure automatisch verschlüsselt "Azure Storage Service Encryption".

Bei der Standardimplementierung wird ein von Microsoft verwalteter Schlüssel verwendet. Es ist keine Einrichtung erforderlich.

Wenn Sie einen vom Kunden gemanagten Schlüssel mit Cloud Volumes ONTAP verwenden möchten, müssen Sie folgende Schritte ausführen:

1. Aus Azure erstellen Sie einen Schlüsselspeicher und generieren Sie anschließend einen Schlüssel in diesem Vault
2. Verwenden Sie für BlueXP die API, um eine Cloud Volumes ONTAP-Arbeitsumgebung zu erstellen, in der der Schlüssel zum Einsatz kommt

Rotation von Schlüsseln

Wenn Sie eine neue Version Ihres Schlüssels erstellen, verwendet Cloud Volumes ONTAP automatisch die neueste Schlüsselversion.

Verschlüsselte Daten

Nachdem Sie eine Cloud Volumes ONTAP Arbeitsumgebung erstellt haben, in der ein vom Kunden gemanagter Schlüssel verwendet wird, werden Cloud Volumes ONTAP Daten wie folgt verschlüsselt.

Azure HA, eine einzelne Verfügbarkeitszone

- Alle Azure-Storage-Konten für Cloud Volumes ONTAP werden mit einem vom Kunden gemanagten Schlüssel verschlüsselt.[1]
- Neue Storage-Konten (z. B. beim Hinzufügen von Festplatten oder Aggregaten) verwenden ebenfalls den gleichen Schlüssel.[1]
- Ab ONTAP 9.10.1P3 verwendet BlueXP für NVRAM und die Core-Festplatte einen "Festplattenverschlüsselungssatz", Die das Management von Schlüsseln mit verwalteten Festplatten ermöglicht. Bei niedrigeren Versionen wird der von Microsoft verwaltete Schlüssel anstelle des vom Kunden verwalteten Schlüssels verwendet.

Single Node

- Alle Azure-Storage-Konten für Cloud Volumes ONTAP werden über einen vom Kunden gemanagten Schlüssel verschlüsselt. [1]
- Für Root-, Boot- und Datenfestplatten verwendet BlueXP einen "Festplattenverschlüsselungssatz", Die das Management von Schlüsseln mit verwalteten Festplatten ermöglicht.
- Neue Festplatten verwenden ebenfalls denselben Festplattenverschlüsselungssatz.
- Ab ONTAP 9.9.1P7 verwendet BlueXP für NVRAM und die Kernfestplatte einen Festplattenverschlüsselungssatz, der das Management von Schlüsseln mit verwalteten Laufwerken ermöglicht. Bei niedrigeren Versionen wird der von Microsoft verwaltete Schlüssel anstelle des vom Kunden verwalteten Schlüssels verwendet.

Fußnote

1. Wenn Sie Ihre Speicherkonten während ihrer Erstellung verschlüsseln möchten, müssen Sie in der Cloud Volumes ONTAP-Erstellungsanforderung die ID der Ressource erstellen und angeben. Dies gilt für alle Implementierungsarten. Wenn Sie dies nicht bereitstellen, werden die Speicherkonten weiterhin verschlüsselt, BlueXP erstellt jedoch zuerst die Speicherkonten mit von Microsoft administrierter Verschlüsselungsmethode und aktualisiert dann die Speicherkonten, um den vom Kunden verwalteten Schlüssel zu verwenden.

Erstellen eines Schlüsselgewölbes und Generieren eines Schlüssels

Der Schlüsselspeicher muss in demselben Azure Abonnement und derselben Region liegen, in der Sie das Cloud Volumes ONTAP System erstellen möchten.

Schritte

1. "Erstellen Sie einen Schlüsselspeicher in Ihrem Azure-Abonnement".

   Beachten Sie die folgenden Anforderungen für den Schlüsselspeicher:

   - Der Schlüsselgewölbe muss sich in derselben Region wie das Cloud Volumes ONTAP System befinden.
   - Die folgenden Optionen sollten aktiviert sein:
     - **Soft-delete** (diese Option ist standardmäßig aktiviert, muss aber nicht_ deaktiviert sein)
     - **Schutz löschen**
     - **Azure Disk Encryption für Volume Encryption**

2. "Einen Schlüssel im Schlüsselspeicher erzeugen".

   Beachten Sie die folgenden Anforderungen für den Schlüssel:

   - Der Schlüsseltyp muss **RSA** sein.
   - Die empfohlene RSA-Schlüsselgröße beträgt **2048**, andere Größen werden unterstützt.

Erstellen Sie eine Arbeitsumgebung, in der der Verschlüsselungsschlüssel verwendet wird

Nachdem Sie den Schlüsselspeicher erstellt und einen Verschlüsselungsschlüssel generiert haben, können Sie ein neues Cloud Volumes ONTAP-System erstellen, das für die Verwendung des Schlüssels konfiguriert ist. Diese Schritte werden von der BlueXP API unterstützt.

Wenn Sie einen vom Kunden verwalteten Schlüssel mit einem Cloud Volumes ONTAP-System mit einem einzelnen Knoten verwenden möchten, stellen Sie sicher, dass der BlueXP-Connector über die folgenden Berechtigungen verfügt:

```
"Microsoft.Compute/diskEncryptionSets/read"
"Microsoft.Compute/diskEncryptionSets/write",
"Microsoft.Compute/diskEncryptionSets/delete"
"Microsoft.KeyVault/vaults/deploy/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write"
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
```

"Zeigen Sie die aktuelle Liste der Berechtigungen an"

Die ersten drei Berechtigungen sind für HA-Paare nicht erforderlich.

Schritte

1. Nutzen Sie den folgenden BlueXP API-Aufruf, um die Liste der Schlüsselvaults in Ihrem Azure-

Abonnement zu erhalten.

Bei einem HA-Paar: `GET /azure/ha/metadata/vaults`

Für Single Node: `GET /azure/vsa/metadata/vaults`

Notieren Sie sich den **Namen** und die **resourceGroup**. Im nächsten Schritt müssen Sie diese Werte angeben.

"Weitere Informationen zu diesem API-Aufruf".

2. Rufen Sie die Liste der Schlüssel im Tresor mithilfe des folgenden BlueXP API-Aufrufs ab.

   Bei einem HA-Paar: `GET /azure/ha/metadata/keys-vault`

   Für Single Node: `GET /azure/vsa/metadata/keys-vault`

   Notieren Sie sich den **Keyname**. Im nächsten Schritt müssen Sie diesen Wert (zusammen mit dem Vault-Namen) angeben.

   "Weitere Informationen zu diesem API-Aufruf".

3. Erstellen Sie ein Cloud Volumes ONTAP-System mithilfe des folgenden BlueXP-API-Aufrufs.

   a. Bei einem HA-Paar:

      `POST /azure/ha/working-environments`

      Der Text der Anforderung muss die folgenden Felder enthalten:

```
"azureEncryptionParameters": {
                "key": "keyName",
                "vaultName": "vaultName",
                "userAssignedIdentity": " userAssignedIdentityId",
[Optional]***
}
```

      "Weitere Informationen zu diesem API-Aufruf".

   b. System mit einem einzelnen Node:

      `POST /azure/vsa/working-environments`

      Der Text der Anforderung muss die folgenden Felder enthalten:

```
"azureEncryptionParameters": {
                "key": "keyName",
                "vaultName": "vaultName",
                "userAssignedIdentity": " userAssignedIdentityId",
[Optional]***
}
```

+
"Weitere Informationen zu diesem API-Aufruf".

Sie verfügen über ein neues Cloud Volumes ONTAP System, das so konfiguriert ist, dass Sie Ihren vom Kunden gemanagten Schlüssel zur Datenverschlüsselung nutzen können.

Lizenzierung für Cloud Volumes ONTAP in Azure einrichten

Nachdem Sie sich für die Lizenzoption entschieden haben, die Sie mit Cloud Volumes ONTAP verwenden möchten, sind einige Schritte erforderlich, bevor Sie beim Erstellen einer neuen Arbeitsumgebung die Lizenzoption wählen können.

Freimium

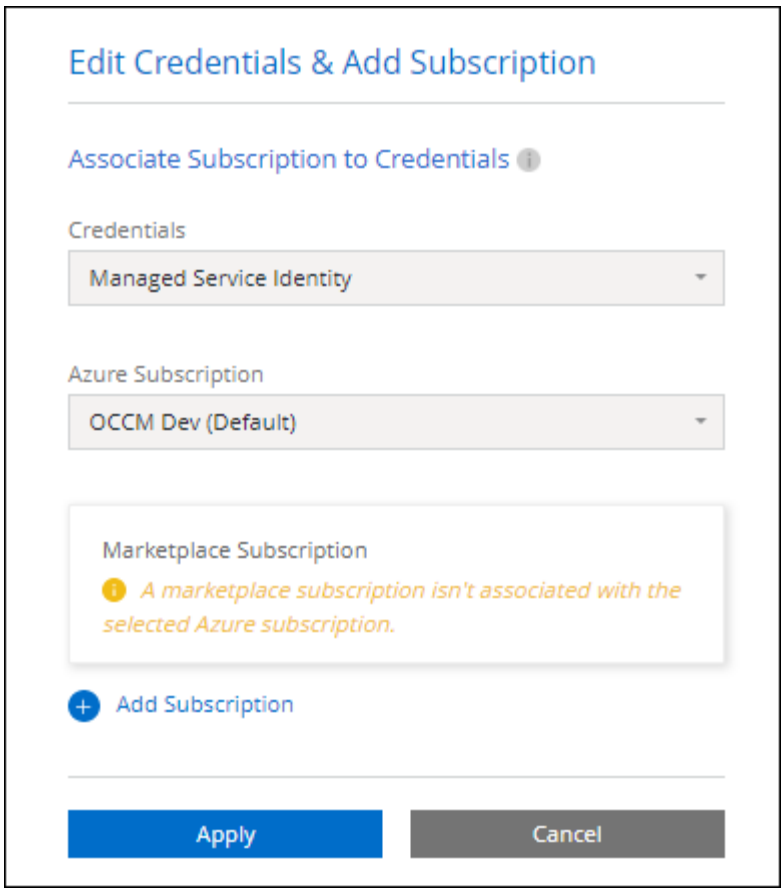
Wählen Sie das Freimium-Angebot aus, um Cloud Volumes ONTAP mit bis zu 500 gib bereitgestellter Kapazität kostenlos zu nutzen. "Erfahren Sie mehr über das Freemium Angebot".

Schritte

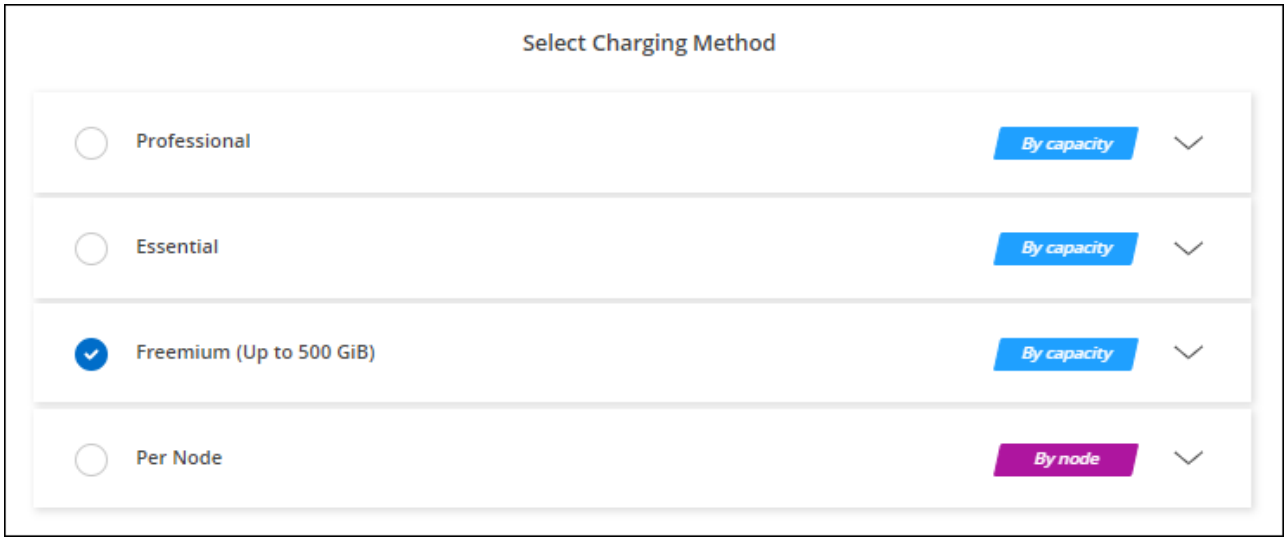
1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in BlueXP.

    a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldedaten bearbeiten > Abonnement hinzufügen** und befolgen Sie dann die Anweisungen, um das Pay-as-you-go-Angebot im Azure Marketplace zu abonnieren.

    Sie werden über das Marketplace-Abonnement nicht belastet, es sei denn, Sie überschreiten 500 gib der bereitgestellten Kapazität. Zu dieser Zeit wird das System automatisch in das konvertiert "Essentials-Paket".



a. Wenn Sie zu BlueXP zurückkehren, wählen Sie **Freemium**, wenn Sie die Seite mit den Lademethoden aufrufen.



"Sehen Sie sich Schritt-für-Schritt-Anleitungen an, um Cloud Volumes ONTAP in Azure zu starten".

Kapazitätsbasierte Lizenz

Dank der kapazitätsbasierten Lizenzierung können Sie für Cloud Volumes ONTAP pro tib Kapazität bezahlen. Kapazitätsbasierte Lizenzierung ist in Form eines *package*, dem Essentials-Paket oder dem Professional-Paket verfügbar.

Die Essentials- und Professional-Pakete sind mit den folgenden Verbrauchsmodellen erhältlich:

- Eine Lizenz (BYOL) von NetApp erworben
- Ein stündliches PAYGO-Abonnement (Pay-as-you-go) im Azure Marketplace
- Einem Jahresvertrag

"Hier erhalten Sie weitere Informationen zur kapazitätsbasierten Lizenzierung".

In den folgenden Abschnitten werden die ersten Schritte mit jedem dieser Nutzungsmodelle beschrieben.

BYOL

Bezahlen Sie vorab, indem Sie eine Lizenz (BYOL) von NetApp erwerben und Cloud Volumes ONTAP Systeme bei jedem Cloud-Provider implementieren.

Schritte

1. "Wenden Sie sich an den NetApp Sales, um eine Lizenz zu erhalten"
2. "Fügen Sie Ihr Konto für die NetApp Support Website zu BlueXP hinzu"

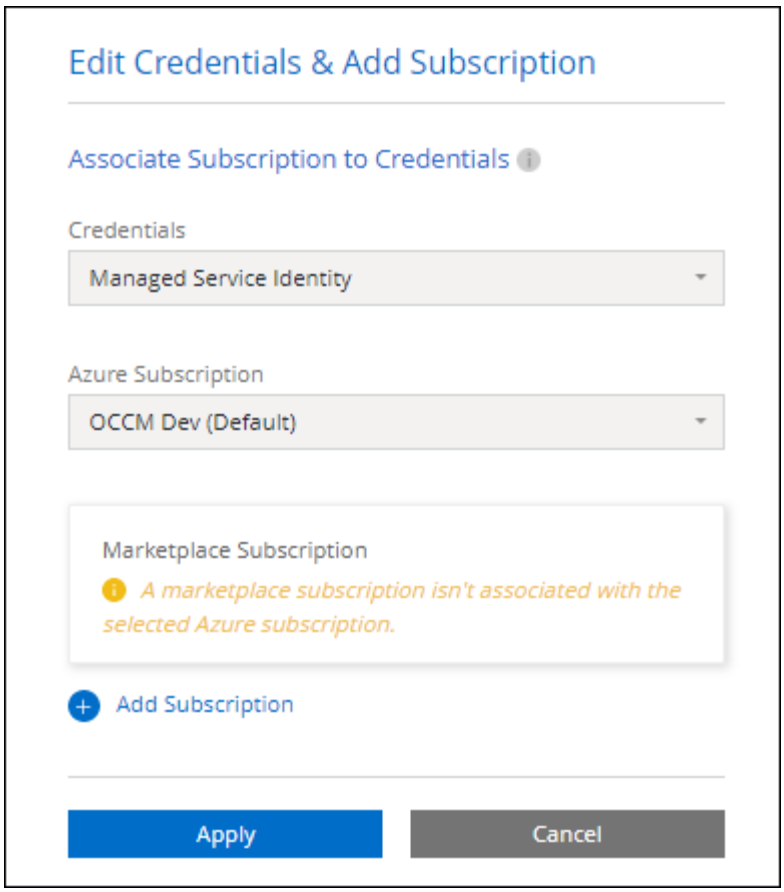
   BlueXP fragt den NetApp Lizenzierungsservice automatisch ab, um Details zu den Lizenzen zu erhalten, die mit Ihrem NetApp Support Site Konto verknüpft sind. Wenn keine Fehler auftreten, fügt BlueXP die Lizenzen automatisch dem Digital Wallet hinzu.

   Ihre Lizenz muss über die digitale Geldbörse verfügbar sein, bevor Sie sie mit Cloud Volumes ONTAP verwenden können. Wenn nötig, können Sie "Fügen Sie die Lizenz manuell zur Digital Wallet hinzu".

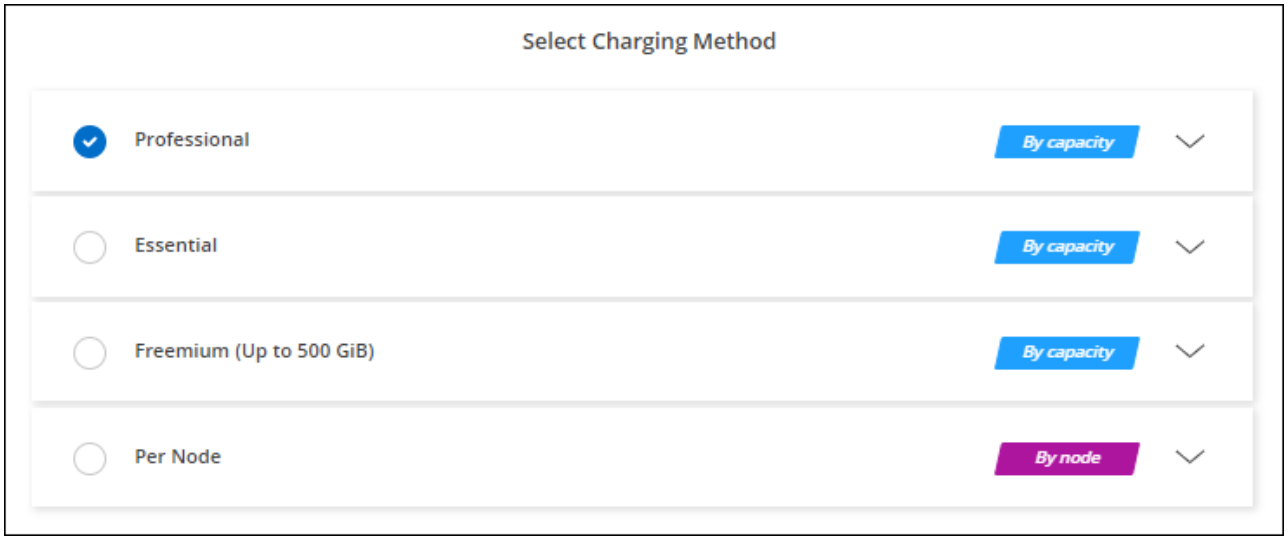
3. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in BlueXP.

   a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldedaten bearbeiten > Abonnement hinzufügen** und befolgen Sie dann die Anweisungen, um das Pay-as-you-go-Angebot im Azure Marketplace zu abonnieren.

      Die Lizenz, die Sie bei NetApp erworben haben, wird immer zuerst berechnet. Wenn Sie Ihre lizenzierte Kapazität überschreiten oder die Lizenzlaufzeit abgelaufen ist, werden Sie vom Stundensatz auf dem Markt in Rechnung gestellt.



a. Wenn Sie zu BlueXP zurückkehren, wählen Sie ein kapazitätsbasiertes Paket aus, wenn Sie die Seite mit den Lademethoden aufrufen.



"Sehen Sie sich Schritt-für-Schritt-Anleitungen an, um Cloud Volumes ONTAP in Azure zu starten".

PAYGO-Abonnement

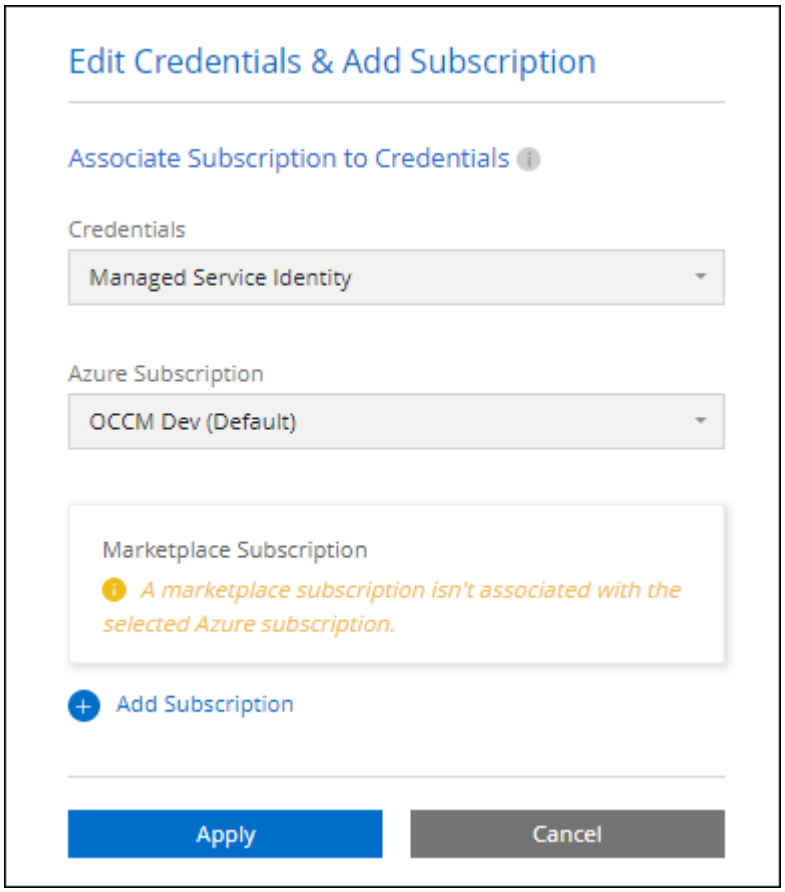
Sie bezahlen stündlich, indem Sie sich für das Angebot über den Marketplace Ihres Cloud-Providers anmelden.

Wenn Sie eine Cloud Volumes ONTAP-Arbeitsumgebung erstellen, werden Sie von BlueXP aufgefordert, den

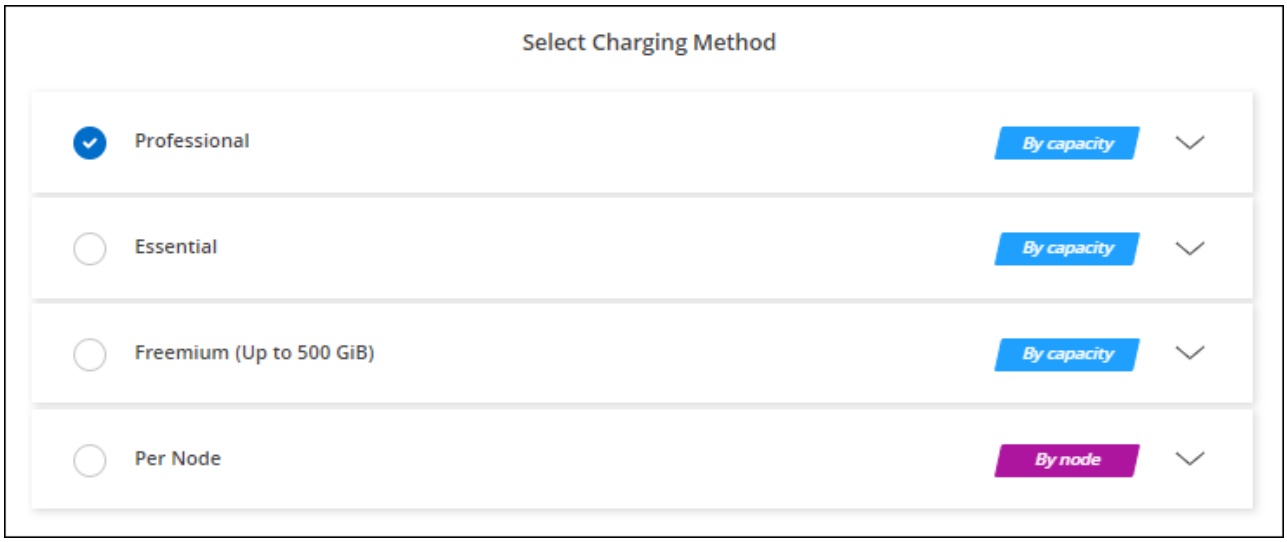
Vertrag zu abonnieren, der im Azure Marketplace verfügbar ist. Dieses Abonnement wird dann zur Verrechnung mit der Arbeitsumgebung verknüpft. Sie können das gleiche Abonnement auch für zusätzliche Arbeitsumgebungen nutzen.

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in BlueXP.
   a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldedaten bearbeiten > Abonnement hinzufügen** und befolgen Sie dann die Anweisungen, um das Pay-as-you-go-Angebot im Azure Marketplace zu abonnieren.



   b. Wenn Sie zu BlueXP zurückkehren, wählen Sie ein kapazitätsbasiertes Paket aus, wenn Sie die Seite mit den Lademethoden aufrufen.



"Sehen Sie sich Schritt-für-Schritt-Anleitungen an, um Cloud Volumes ONTAP in Azure zu starten".

Sie können die mit Ihren Azure-Konten verbundenen Azure Marketplace-Abonnements auf der Seite „Einstellungen“ > „Anmeldeinformationen“ managen. "Managen Sie Ihre Azure-Konten und -Abonnements"

Jahresvertrag

Sie bezahlen jährlich für Cloud Volumes ONTAP durch den Kauf eines Jahresvertrags.

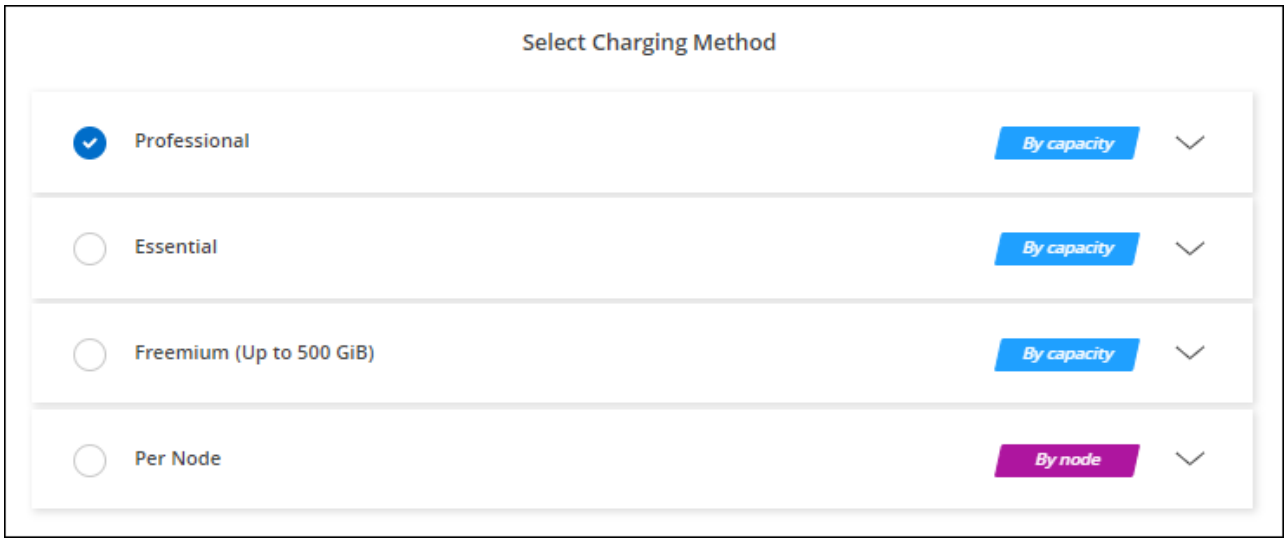
Schritte

1. Wenden Sie sich an Ihren NetApp Ansprechpartner, um einen Jahresvertrag zu erwerben.

   Der Vertrag ist als *privates* Angebot im Azure Marketplace erhältlich.

   Wenn NetApp Ihnen das private Angebot teilt, können Sie den Jahresplan auch auswählen, wenn Sie während der Erstellung der Arbeitsumgebung im Azure Marketplace abonnieren.

2. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in BlueXP.
   a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldeinformationen bearbeiten > Abonnement hinzufügen > Weiter**.
   b. Wählen Sie im Azure-Portal den Jahresplan aus, der mit Ihrem Azure-Konto geteilt wurde, und klicken Sie anschließend auf **Abonnieren**.
   c. Wenn Sie zu BlueXP zurückkehren, wählen Sie ein kapazitätsbasiertes Paket aus, wenn Sie die Seite mit den Lademethoden aufrufen.



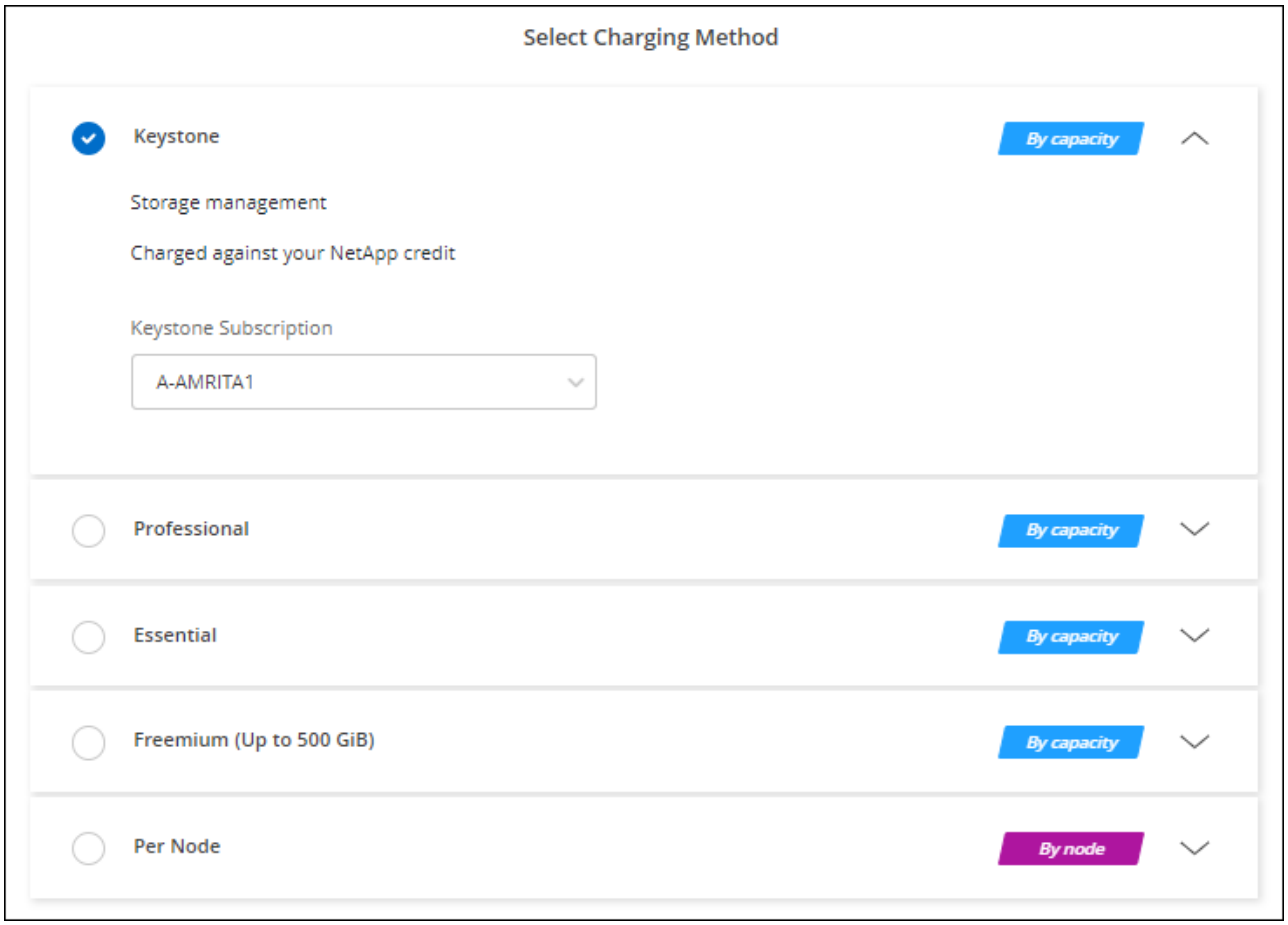
"Sehen Sie sich Schritt-für-Schritt-Anleitungen an, um Cloud Volumes ONTAP in Azure zu starten".

Keystone Flex Abonnement

Das Keystone Flex Abonnement ist ein abonnementbasierter Service mit nutzungsbasiertem Zahlungsmodell. "Weitere Informationen zu Keystone Flex Abonnements".

Schritte

1. Wenn Sie noch kein Abonnement haben, "Kontakt zu NetApp"
2. Mailto:ng-keystone-success@netapp.com [NetApp kontaktieren], um Ihr BlueXP Benutzerkonto über eine oder mehrere Keystone Flex Abonnements zu autorisieren.
3. Nachdem NetApp den Account autorisiert hat, "Verknüpfen Sie Ihre Abonnements für die Verwendung mit Cloud Volumes ONTAP".
4. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in BlueXP.
   a. Wählen Sie die Keystone Flex Subscription-Lademethode aus, wenn Sie dazu aufgefordert werden, eine Lademethode auszuwählen.



"Sehen Sie sich Schritt-für-Schritt-Anleitungen an, um Cloud Volumes ONTAP in Azure zu starten".

Aktivieren Sie den Hochverfügbarkeits-Modus in Azure

Der Hochverfügbarkeits-Modus von Microsoft Azure sollte aktiviert sein, um ungeplante Failover-Zeiten zu verringern und die NFSv4-Unterstützung für Cloud Volumes ONTAP zu aktivieren.

Ab der Version Cloud Volumes ONTAP 9.10.1 reduzierten wir die ungeplante Failover-Zeit für Cloud Volumes ONTAP HA-Paare, die in Microsoft Azure laufen, und fügten Unterstützung für NFSv4 hinzu. Um diese Verbesserungen für Cloud Volumes ONTAP verfügbar zu machen, müssen Sie die Hochverfügbarkeitsfunktion Ihres Azure Abonnements aktivieren.

In BlueXP werden Sie diese Angaben in einer Meldung „Aktion erforderlich“ eingeben, wenn die Funktion auf einem Azure-Abonnement aktiviert werden muss.

Beachten Sie Folgendes:

- Es gibt keine Probleme mit der Hochverfügbarkeit Ihres Cloud Volumes ONTAP HA-Paars. Diese Azure Funktion arbeitet in Kombination mit ONTAP, um die von Clients beobachteten Applikationsausfallzeiten für NFS-Protokolle zu reduzieren, die aus ungeplanten Failover-Ereignissen resultieren.
- Wenn Sie diese Funktion aktivieren, wird für Cloud Volumes ONTAP HA-Paare keine Unterbrechung verursacht.
- Wenn Sie diese Funktion auf Ihrem Azure-Abonnement aktivieren, treten keine Probleme bei anderen VMs

auf.

Ein Azure-Benutzer mit „Owner“-Berechtigungen kann die Funktion über die Azure-CLI aktivieren.

Schritte

1. "Greifen Sie über das Azure-Portal auf die Azure Cloud Shell zu"
2. Registrieren der Funktion des Hochverfügbarkeits-Modus:

```
az account set -s AZURE_SUBSCRIPTION_NAME_OR_ID
az feature register --name EnableHighAvailabilityMode --namespace
Microsoft.Network
az provider register -n Microsoft.Network
```

3. Überprüfen Sie optional, ob die Funktion jetzt registriert ist:

```
az feature show --name EnableHighAvailabilityMode --namespace
Microsoft.Network
```

Die Azure CLI sollte ein Ergebnis wie die folgenden zurückgeben:

```
{
  "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/providers/Microsoft.Features/providers/Microsoft.Network/fe
atures/EnableHighAvailabilityMode",
  "name": "Microsoft.Network/EnableHighAvailabilityMode",
  "properties": {
    "state": "Registered"
  },
  "type": "Microsoft.Features/providers/features"
}
```

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 BlueXP erstellen.

Um eine Arbeitsumgebung zu schaffen, benötigen Sie Folgendes.

- Ein Anschluss, der betriebsbereit ist.
  - Sie sollten ein haben "Anschluss, der Ihrem Arbeitsbereich zugeordnet ist".
  - "Sie sollten darauf vorbereitet sein, den Konnektor jederzeit in Betrieb zu nehmen".
- Ein Verständnis der zu verwendenden Konfiguration.

  Sie sollten eine Konfiguration auswählen und Azure Netzwerkinformationen von Ihrem Administrator

erhalten haben. Weitere Informationen finden Sie unter "Planung Ihrer Cloud Volumes ONTAP Konfiguration".

- Kenntnisse über die erforderlichen Voraussetzungen zur Einrichtung der Lizenzierung für Cloud Volumes ONTAP.

  "Erfahren Sie, wie Sie eine Lizenzierung einrichten".

Wenn BlueXP in Azure ein Cloud Volumes ONTAP-System erstellt, werden mehrere Azure-Objekte erstellt, z. B. eine Ressourcengruppe, Netzwerkschnittstellen und Speicherkonten. Sie können eine Zusammenfassung der Ressourcen am Ende des Assistenten überprüfen.

Risiko von Datenverlusten

Als Best Practice empfiehlt es sich, für jedes Cloud Volumes ONTAP System eine neue, dedizierte Ressourcengruppe zu verwenden.

Aufgrund des Risikos eines Datenverlusts wird die Bereitstellung von Cloud Volumes ONTAP in einer vorhandenen, gemeinsam genutzten Ressourcengruppe nicht empfohlen. Während BlueXP Cloud Volumes ONTAP-Ressourcen im Falle eines Ausfalls oder Löschvorgangs aus einer gemeinsam genutzten Ressourcengruppe entfernen kann, kann ein Azure Benutzer aus Versehen Cloud Volumes ONTAP-Ressourcen aus einer gemeinsam genutzten Ressourcengruppe löschen.

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Klicken Sie auf der Bildschirmseite auf **Arbeitsumgebung hinzufügen** und folgen Sie den Anweisungen.
3. **Wählen Sie einen Standort**: Wählen Sie **Microsoft Azure** und **Cloud Volumes ONTAP Single Node** oder **Cloud Volumes ONTAP High Availability**.
4. Wenn Sie dazu aufgefordert werden, "Einen Konnektor erstellen".
5. **Details und Anmeldeinformationen**: Optional können Sie die Azure-Anmeldedaten und das Abonnement ändern, einen Clusternamen angeben, bei Bedarf Tags hinzufügen und dann Anmeldedaten angeben.

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

Feld	Beschreibung
Name der Arbeitsumgebung	BlueXP 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.
Tags Für Ressourcengruppen	Tags sind Metadaten für Ihre Azure Ressourcen. Wenn Sie in dieses Feld Tags eingeben, fügt BlueXP diese der Ressourcengruppe hinzu, 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".

Feld	Beschreibung
Benutzername und Passwort	Dies sind die Anmeldeinformationen für das Cloud Volumes ONTAP Cluster-Administratorkonto. Sie können diese Anmeldedaten für die Verbindung mit Cloud Volumes ONTAP über System Manager oder dessen CLI verwenden. Behalten Sie den Standardbenutzernamen „*admin*“ bei, oder ändern Sie ihn in einen benutzerdefinierten Benutzernamen.
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/cloud-manager-cloud-volumes-

ontap//media/video_subscribing_azure.mp4 *(video)*

6. **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 Data Sense"
   - "Weitere Informationen zu Cloud Backup"
7. **Standort**: Wählen Sie eine Region, eine Verfügbarkeitszone, vnet und ein Subnetz aus, und aktivieren Sie dann das Kontrollkästchen, um die Netzwerkverbindung zwischen dem Connector und dem Zielspeicherort zu bestätigen.

   Bei Single-Node-Systemen können Sie die Verfügbarkeitszone auswählen, in der Sie Cloud Volumes ONTAP implementieren möchten. Wenn Sie keine AZ auswählen, wählt BlueXP eine für Sie aus.
8. **Konnektivität**: Wählen Sie eine neue oder bestehende Ressourcengruppe und wählen Sie dann aus, ob Sie die vordefinierte Sicherheitsgruppe verwenden oder Ihre eigene verwenden möchten.

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

Feld	Beschreibung
Verfügbarkeitszone	Bei Single-Node-Systemen können Sie die Verfügbarkeitszone auswählen, in der Sie Cloud Volumes ONTAP implementieren möchten. Wenn Sie keine AZ auswählen, wählt BlueXP eine für Sie aus.
Ressourcengruppe	Erstellen Sie eine neue Ressourcengruppe für Cloud Volumes ONTAP, oder verwenden Sie eine vorhandene Ressourcengruppe. 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 bereitzustellen, jedoch wird dies aufgrund des Risikos eines Datenverlusts nicht empfohlen. Weitere Informationen finden Sie in der oben stehenden Warnung. Sie müssen für jedes Cloud Volumes ONTAP HA-Paar, das Sie in Azure implementieren, eine dedizierte Ressourcengruppe verwenden. Es wird nur ein HA-Paar in einer Ressourcengruppe unterstützt. Bei BlueXP treten Verbindungsprobleme auf, wenn Sie versuchen, ein zweites Cloud Volumes ONTAP HA-Paar in einer Azure Ressourcengruppe bereitzustellen. Wenn im Azure Konto, das Sie verwenden, der angezeigt wird "Erforderliche Berechtigungen", BlueXP entfernt Cloud Volumes ONTAP-Ressourcen aus einer Ressourcengruppe, bei Ausfall oder Löschung der Bereitstellung.
Sicherheitsgruppe wurde generiert	Wenn Sie BlueXP die Sicherheitsgruppe für Sie generieren lassen, müssen Sie festlegen, wie Sie den Datenverkehr zulassen: • Wenn Sie **Selected vnet Only** wählen, ist die Quelle für eingehenden Datenverkehr der Subnetz-Bereich des ausgewählten vnet und der Subnetz-Bereich des vnet, in dem sich der Connector befindet. Dies ist die empfohlene Option. • Wenn Sie **Alle VNets** wählen, ist die Quelle für eingehenden Datenverkehr der IP-Bereich 0.0.0.0/0.

Feld	Beschreibung
Verwenden Sie vorhandene	Wenn Sie eine vorhandene Sicherheitsgruppe auswählen, muss diese die Cloud Volumes ONTAP-Anforderungen erfüllen. "Zeigen Sie die Standardsicherheitsgruppe an".

9. **Charging Methods and NSS Account**: Geben Sie an, welche Ladungsoption Sie mit diesem System verwenden möchten, und geben Sie dann ein NetApp Support Site Konto an.
   - "Informieren Sie sich über Lizenzoptionen für Cloud Volumes ONTAP".
   - "Erfahren Sie, wie Sie eine Lizenzierung einrichten".
10. **Vorkonfigurierte Pakete**: Wählen Sie eines der Pakete, um schnell ein Cloud Volumes ONTAP System bereitzustellen, oder klicken Sie auf **eigene Konfiguration erstellen**.

    Wenn Sie eines der Pakete auswählen, müssen Sie nur ein Volume angeben und dann die Konfiguration prüfen und genehmigen.
11. **Lizenzierung**: Ändern Sie die Cloud Volumes ONTAP-Version nach Bedarf und wählen Sie einen virtuellen Maschinentyp.

    Wenn für die ausgewählte Version eine neuere Version von Release Candidate, General Availability oder Patch Release verfügbar ist, aktualisiert BlueXP das System auf diese Version, wenn die Arbeitsumgebung erstellt wird. Das Update erfolgt beispielsweise, wenn Sie Cloud Volumes ONTAP 9.10.1 und 9.10.1 P4 auswählen. Das Update erfolgt nicht von einem Release zum anderen, z. B. von 9.6 bis 9.7.
12. **Vom Azure Marketplace abonnieren**: Folgen Sie den Schritten, wenn BlueXP programmatische Bereitstellungen von Cloud Volumes ONTAP nicht aktivieren kann.
13. **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 ist für alle Festplatten im ursprünglichen Aggregat und für alle zusätzlichen Aggregate bestimmt, die BlueXP erzeugt, 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".
14. **Schreibgeschwindigkeit & WURM** (nur Systeme mit einem Knoten): Wählen Sie **normale** oder **hohe** Schreibgeschwindigkeit und aktivieren Sie ggf. den WORM-Speicher (Write Once, Read Many).

"Erfahren Sie mehr über Schreibgeschwindigkeit".

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

"Erfahren Sie mehr über WORM Storage".

15. **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".

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

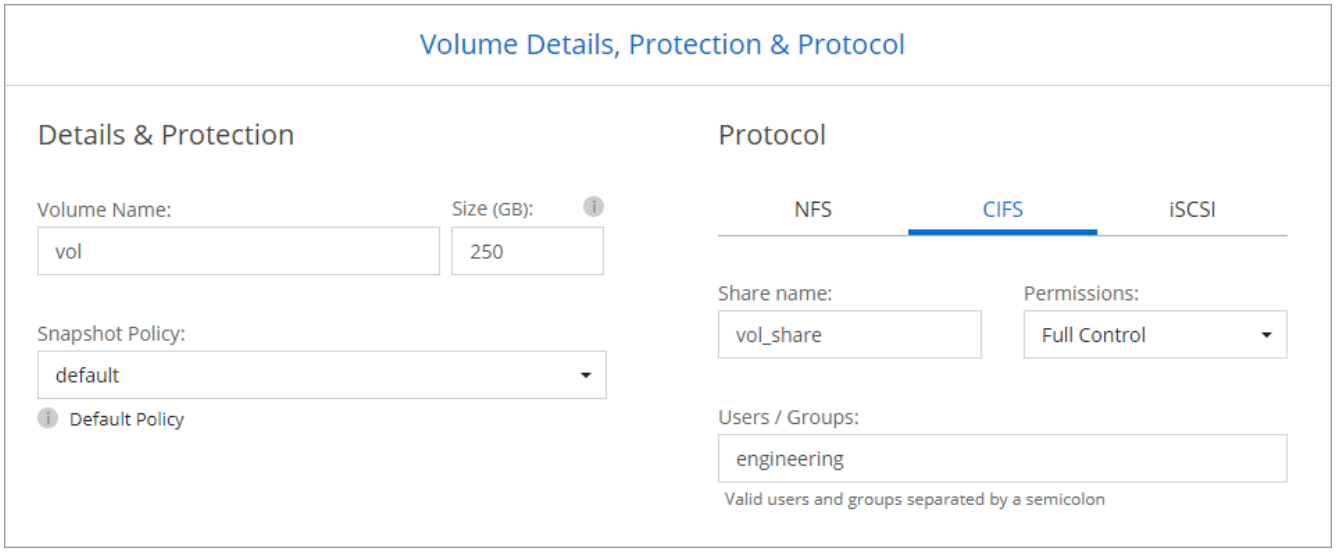
    "Hier erhalten Sie Informationen zu den unterstützten Client-Protokollen und -Versionen".

    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 BlueXP einen Wert ein, der Zugriff auf alle Instanzen im Subnetz bietet.
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 BlueXP automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volumen erstellen, so gibt es keine Verwaltung beteiligt. Nachdem Sie das Volume erstellt haben, "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:



17. **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 "BlueXP Automation Dokumentation" Entsprechende Details. Beachten Sie, dass Sie einen NTP-Server nur beim Erstellen eines CIFS-Servers konfigurieren können. Er ist nicht konfigurierbar, nachdem Sie den CIFS-Server erstellt haben.

18. **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".

19. **Überprüfen & Genehmigen**: Überprüfen und bestätigen Sie Ihre Auswahl.
    a. Überprüfen Sie die Details zur Konfiguration.
    b. Klicken Sie auf **Weitere Informationen**, um weitere Informationen zum Support und den Azure-Ressourcen zu erhalten, die BlueXP kaufen wird.
    c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.
    d. Klicken Sie Auf **Go**.

BlueXP 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.