Erste Schritte in Microsoft Azure

Cloud Volumes ONTAP

NetApp
February 17, 2026

Inhalt

Erste Schritte in Microsoft Azure

Informieren Sie sich über die Bereitstellungsoptionen von Cloud Volumes ONTAP in Azure

NetApp bietet zwei Optionen für die Bereitstellung von Cloud Volumes ONTAP auf Azure. Cloud Volumes ONTAP verlässt sich traditionell auf die NetApp Console für Bereitstellung und Orchestrierung. Ab Cloud Volumes ONTAP 9.16.1 können Sie die Vorteile der direkten Bereitstellung im Azure Marketplace nutzen, einem optimierten Prozess, der Zugriff auf eine begrenzte, aber dennoch leistungsstarke Reihe von Funktionen und Optionen von Cloud Volumes ONTAP bietet.

Wenn Sie Cloud Volumes ONTAP direkt vom Azure Marketplace bereitstellen, müssen Sie weder den Konsolen-Agenten einrichten noch andere Sicherheits- und Onboarding-Kriterien erfüllen, die für die Bereitstellung von Cloud Volumes ONTAP über die Konsole erforderlich sind. Über den Azure Marketplace können Sie Cloud Volumes ONTAP mit wenigen Klicks schnell bereitstellen und die wichtigsten Funktionen und Möglichkeiten in Ihrer Umgebung erkunden.

Nach Abschluss der Bereitstellung im Azure Marketplace können Sie diese Systeme in der Konsole entdecken. Nach der Erkennung können Sie sie als Cloud Volumes ONTAP -Systeme verwalten und alle Konsolenfunktionen nutzen. Weitere Informationen finden Sie unter "Entdecken Sie die bereitgestellten Systeme in der Konsole" .

Hier ist der Funktionsvergleich zwischen den beiden Optionen. Beachten Sie, dass sich die Funktionen einer über den Azure Marketplace bereitgestellten eigenständigen Instanz ändern, wenn sie in der Konsole erkannt wird.

	Azure-Marktplatz	**NetApp Console**
Einarbeitung	Kürzere und einfachere, minimale Vorbereitung für den direkten Einsatz erforderlich	Längerer Onboarding-Prozess, einschließlich der Installation des Konsolen-Agenten
Unterstützte Typen virtueller Maschinen (VM)	Eds_v5- und Ls_v3-Instance-Typen	Vollständige Palette an VM-Typen.https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-azure.html["Unterstützte Konfigurationen in Azure"^]
Lizenz	Kostenlose Lizenz	Jede kapazitätsbasierte Lizenz."Cloud Volumes ONTAP -Lizenzierung"
* NetApp Unterstützung*	Nicht enthalten	Verfügbar, je nach Lizenztyp
Kapazität	Bis zu 500 GiB	Erweiterbar durch Konfiguration
Bereitstellungsmodell	Bereitstellung im Hochverfügbarkeitsmodus (HA) in einer einzelnen Verfügbarkeitszone (AZ)	Alle unterstützten Konfigurationen, einschließlich Einzelknoten- und HA-Modi, Einzel- und Mehrfach-AZ-Bereitstellungen

	Azure-Marktplatz	NetApp Console
Unterstützter Datenträgertyp	Verwaltete Premium-SSD-v2-Datenträger	Breitere Unterstützung."Standardkonfiguration für Cloud Volumes ONTAP"
Schreibgeschwindigkeit (schneller Schreibmodus)	Nicht unterstützt	Wird basierend auf Ihrer Konfiguration unterstützt. "Erfahren Sie mehr über die Schreibgeschwindigkeiten in Cloud Volumes ONTAP" .
Orchestrierungsfunktionen	Nicht verfügbar	Verfügbar über die NetApp Console, basierend auf dem Lizenztyp
Anzahl der unterstützten Speicher-VMs	Eine pro Bereitstellung	Mehrere Speicher-VMs, basierend auf Ihrer Konfiguration."Unterstützte Anzahl von Speicher-VMs"
Ändern des Instanztyps	Nicht unterstützt	Unterstützt
* FabricPool Stufeneinteilung*	Nicht unterstützt	Unterstützt

Weiterführende Links

- Direkte Bereitstellung im Azure Marketplace:"Stellen Sie Cloud Volumes ONTAP vom Azure Marketplace bereit"
- Bereitstellung über die Konsole:"Schnellstart für Cloud Volumes ONTAP in Azure"
- "Dokumentation zur NetApp Console"

Erste Schritte in der NetApp Console

Schnellstart für Cloud Volumes ONTAP in Azure

Beginnen Sie in wenigen Schritten mit Cloud Volumes ONTAP für Azure.

1 Erstellen eines Konsolenagenten

Wenn Sie kein "Konsolenagent" Sie müssen jedoch eines erstellen. "Erfahren Sie, wie Sie einen Konsolen-Agent in Azure erstellen"

Beachten Sie: Wenn Sie Cloud Volumes ONTAP in einem Subnetz bereitstellen möchten, in dem kein Internetzugang verfügbar ist, müssen Sie den Konsolenagenten manuell installieren und auf die NetApp Console zugreifen, die auf diesem Konsolenagenten ausgeführt wird. "Erfahren Sie, wie Sie den Konsolenagenten manuell an einem Ort ohne Internetzugang installieren."

2 Planen Sie Ihre Konfiguration

Die Konsole bietet vorkonfigurierte Pakete, die Ihren Workload-Anforderungen entsprechen, oder Sie können Ihre eigene Konfiguration erstellen. Wenn Sie Ihre eigene Konfiguration auswählen, sollten Sie die Ihnen zur Verfügung stehenden Optionen verstehen. Weitere Informationen finden Sie unter"Planen Sie Ihre Cloud

Volumes ONTAP -Konfiguration in Azure" .

3 Richten Sie Ihr Netzwerk ein

1. Stellen Sie sicher, dass Ihr VNet und Ihre Subnetze die Konnektivität zwischen dem Konsolenagenten und Cloud Volumes ONTAP unterstützen.
2. Aktivieren Sie den ausgehenden Internetzugriff vom Ziel-VPC für NetApp AutoSupport.

   Dieser Schritt ist nicht erforderlich, wenn Sie Cloud Volumes ONTAP an einem Standort bereitstellen, an dem kein Internetzugang verfügbar ist.

"Erfahren Sie mehr über die Netzwerkanforderungen" .

4 Starten Sie Cloud Volumes ONTAP

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

Weiterführende Links

- "Erstellen eines Konsolenagenten über die Konsole"
- "Erstellen eines Konsolen-Agenten aus dem Azure Marketplace"
- "Installieren der Konsolenagentensoftware auf einem Linux-Host"
- "Was die Konsole mit Berechtigungen macht"

Planen Sie Ihre Cloud Volumes ONTAP -Konfiguration in Azure

Wenn Sie Cloud Volumes ONTAP in Azure bereitstellen, können Sie ein vorkonfiguriertes System auswählen, das Ihren Workload-Anforderungen entspricht, oder Sie können Ihre eigene Konfiguration erstellen. Wenn Sie Ihre eigene Konfiguration auswählen, sollten Sie die Ihnen zur Verfügung stehenden Optionen verstehen.

Wählen Sie eine Cloud Volumes ONTAP -Lizenz

Für Cloud Volumes ONTAP sind mehrere Lizenzierungsoptionen verfügbar. Jede Option ermöglicht Ihnen die Auswahl eines Verbrauchsmodells, das Ihren Anforderungen entspricht.

- "Erfahren Sie mehr über die Lizenzierungsoptionen für Cloud Volumes ONTAP"
- "Erfahren Sie, wie Sie die Lizenzierung einrichten"

Wählen Sie eine unterstützte Region

Cloud Volumes ONTAP wird in den meisten Microsoft Azure-Regionen unterstützt. "Vollständige Liste der unterstützten Regionen anzeigen" .

Wählen Sie einen unterstützten VM-Typ

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

"Unterstützte Konfigurationen für Cloud Volumes ONTAP in Azure"

Speichergrenzen verstehen

Die Rohkapazitätsgrenze für ein Cloud Volumes ONTAP System ist an die Lizenz gebunden. Zusätzliche Beschränkungen wirken sich auf die Größe von Aggregaten und Volumina aus. Sie sollten sich dieser Beschränkungen bewusst sein, wenn Sie Ihre Konfiguration planen.

"Speicherlimits für Cloud Volumes ONTAP in Azure"

Dimensionieren Sie Ihr System in Azure

Durch die Dimensionierung Ihres Cloud Volumes ONTAP -Systems können Sie die Anforderungen an Leistung und Kapazität erfüllen. Bei der Auswahl eines VM-Typs, Datenträgertyps und einer Datenträgergröße sollten Sie einige wichtige Punkte beachten:

Typ der virtuellen Maschine

Sehen Sie sich die unterstützten virtuellen Maschinentypen im "Versionshinweise zu Cloud Volumes ONTAP" und überprüfen Sie dann Details zu jedem unterstützten VM-Typ. Beachten Sie, dass jeder VM-Typ eine bestimmte Anzahl von Datenträgern unterstützt.

- "Azure-Dokumentation: Allgemeine Größen virtueller Computer"
- "Azure-Dokumentation: Arbeitsspeicheroptimierte Größen virtueller Computer"

Azure-Datenträgertyp mit Einzelknotensystemen

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

Einzelknotensysteme können diese Arten von Azure Managed Disks verwenden:

- *Premium SSD Managed Disks* bieten hohe Leistung für I/O-intensive Workloads zu höheren Kosten.
- *Premium SSD v2 Managed Disks* bieten im Vergleich zu Premium SSD Managed Disks eine höhere Leistung mit geringerer Latenz zu geringeren Kosten.
- *Standard-SSD-Managed Disks* bieten konsistente Leistung 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 Einzelheiten zu den Anwendungsfällen dieser Festplatten finden Sie unter "Microsoft Azure-Dokumentation: Welche Datenträgertypen sind in Azure verfügbar?" .

Azure-Datenträgertyp mit HA-Paaren

HA-Systeme verwenden Premium SSD Shared Managed Disks, die beide eine hohe Leistung für E/A-intensive Workloads zu höheren Kosten bieten. HA-Bereitstellungen, die vor der Version 9.12.1 erstellt wurden, verwenden Premium-Seitenblobs.

Azure-Datenträgergröße

Wenn Sie Cloud Volumes ONTAP -Instanzen starten, müssen Sie die Standarddatenträgergröße für Aggregate auswählen. Die NetApp Console verwendet diese Datenträgergröße für das anfängliche Aggregat und für alle zusätzlichen Aggregate, die sie erstellt, wenn Sie die einfache Bereitstellungsoption verwenden. Sie können Aggregate erstellen, die eine andere Festplattengröße als die Standardgröße verwenden, indem Sie"Verwenden der erweiterten Zuordnungsoption" .

Alle Festplatten in einem Aggregat müssen die gleiche Größe haben.

Bei der Auswahl einer Festplattengröße sollten Sie mehrere Faktoren berücksichtigen. Die Festplattengröße hat Einfluss darauf, wie viel Sie für den Speicher bezahlen, auf die Größe der Volumes, die Sie in einem Aggregat erstellen können, auf die für Cloud Volumes ONTAP verfügbare Gesamtkapazität und auf die Speicherleistung.

Die Leistung von Azure Premium Storage ist an die Datenträgergröße gebunden. Größere Festplatten bieten höhere IOPS und einen höheren Durchsatz. Beispielsweise kann die Wahl von 1-TiB-Festplatten eine bessere Leistung bieten als 500-GiB-Festplatten, allerdings zu höheren Kosten.

Es gibt keine Leistungsunterschiede zwischen den Festplattengrößen für Standardspeicher. Sie sollten die Festplattengröße basierend auf der benötigten Kapazität auswählen.

Informationen zu IOPS und Durchsatz nach Datenträgergröße finden Sie in Azure:

- "Microsoft Azure: Managed Disks – Preise"
- "Microsoft Azure: Page Blobs-Preise"

Standardsystemfestplatten anzeigen

Zusätzlich zum Speicher für Benutzerdaten erwirbt die Konsole auch Cloud-Speicher für Cloud Volumes ONTAP -Systemdaten (Boot-Daten, Root-Daten, Core-Daten und NVRAM). Zu Planungszwecken kann es hilfreich sein, diese Details zu überprüfen, bevor Sie Cloud Volumes ONTAP bereitstellen.

"Anzeigen der Standarddatenträger für Cloud Volumes ONTAP -Systemdaten in Azure" .

Der Konsolenagent benötigt außerdem eine Systemfestplatte. "Details zur Standardkonfiguration des Konsolenagenten anzeigen" .

Sammeln von Netzwerkinformationen

Wenn Sie Cloud Volumes ONTAP in Azure bereitstellen, 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 (falls Sie Ihre eigene verwenden)	

Wählen Sie eine Schreibgeschwindigkeit

Über die Konsole können Sie eine Schreibgeschwindigkeitseinstellung für Cloud Volumes ONTAP auswählen. Bevor Sie eine Schreibgeschwindigkeit auswählen, sollten Sie die Unterschiede zwischen den normalen und hohen Einstellungen sowie die Risiken und Empfehlungen bei der Verwendung einer hohen Schreibgeschwindigkeit verstehen. "Erfahren Sie mehr über die Schreibgeschwindigkeit" .

Auswählen eines Volume-Nutzungsprofils

ONTAP umfasst mehrere Speichereffizienzfunktionen, die die von Ihnen benötigte Gesamtspeichermenge reduzieren können. Wenn Sie in der Konsole ein Volume 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.

Die Storage-Effizienzfunktionen von NetApp bieten folgende Vorteile:

Dünne Bereitstellung

Bietet Hosts oder Benutzern mehr logischen Speicher, als Sie tatsächlich in Ihrem physischen Speicherpool haben. Anstatt Speicherplatz vorab zuzuweisen, wird Speicherplatz jedem Volume dynamisch zugewiesen, während Daten geschrieben werden.

Deduplizierung

Verbessert die Effizienz, indem identische Datenblöcke lokalisiert und durch Verweise auf einen einzigen gemeinsamen Block ersetzt werden. Diese Technik reduziert den Speicherkapazitätsbedarf, indem redundante Datenblöcke, die sich auf demselben Datenträger befinden, eliminiert werden.

Komprimierung

Reduziert die zum Speichern von Daten erforderliche physische Kapazität durch Komprimieren von Daten innerhalb eines Volumes auf Primär-, Sekundär- und Archivspeicher.

Einrichten des Azure-Netzwerks für Cloud Volumes ONTAP

Die NetApp Console übernimmt die Einrichtung von Netzwerkkomponenten für Cloud Volumes ONTAP, wie z. B. IP-Adressen, Netzmasken und Routen. Sie müssen sicherstellen, dass ausgehender Internetzugang verfügbar ist, dass genügend private IP-Adressen verfügbar sind, dass die richtigen Verbindungen vorhanden sind und mehr.

Anforderungen für Cloud Volumes ONTAP

Die folgenden Netzwerkanforderungen müssen in Azure erfüllt sein.

Ausgehender Internetzugang

Cloud Volumes ONTAP -Systeme erfordern ausgehenden Internetzugang für den Zugriff auf externe Endpunkte für verschiedene Funktionen. Cloud Volumes ONTAP kann nicht ordnungsgemäß funktionieren, wenn diese Endpunkte in Umgebungen mit strengen Sicherheitsanforderungen blockiert sind.

Der Konsolenagent kontaktiert außerdem mehrere Endpunkte für den täglichen Betrieb. Informationen zu Endpunkten finden Sie unter "Vom Konsolenagenten kontaktierte Endpunkte anzeigen" Und "Vorbereiten des Netzwerks für die Verwendung der Konsole" .

Cloud Volumes ONTAP Endpunkte

Cloud Volumes ONTAP verwendet diese Endpunkte zur Kommunikation mit verschiedenen Diensten.

Endpunkte	Gilt für	Zweck	Bereitstellungsmodi	Auswirkungen bei Nichtverfügbarkeit
https://netapp-cloud-account.auth0.com	Authentifizierung	Wird zur Authentifizierung in der Konsole verwendet.	Standard- und eingeschränkte Modi.	Die Benutzerauthentifizierung schlägt fehl und die folgenden Dienste sind weiterhin nicht verfügbar: • Cloud Volumes ONTAP Dienste • ONTAP -Dienste • Protokolle und Proxy-Dienste
https://vault.azure.net	Schlüsseltresor	Wird verwendet, um geheime Clientschlüssel aus dem Azure Key Vault abzurufen, wenn kundenverwaltete Schlüssel (CMK) verwendet werden.	Standard-, eingeschränkter und privater Modus.	Cloud Volumes ONTAP Dienste sind nicht verfügbar.
https://api.bluexp.netapp.com/tenancy	Mietverhältnis	Wird verwendet, um die Cloud Volumes ONTAP -Ressourcen von der Konsole abzurufen, um Ressourcen und Benutzer zu autorisieren.	Standard- und eingeschränkte Modi.	Cloud Volumes ONTAP Ressourcen und die Benutzer sind nicht autorisiert.
https://mysupport.netapp.com/aods/asupmessage https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Wird verwendet, um AutoSupport Telemetriedaten an den NetApp Support zu senden.	Standard- und eingeschränkte Modi.	AutoSupport -Informationen bleiben unversehrt.
https://management.azure.com https://login.microsoftonline.com https://bluexpinfraprod.eastus2.data.azurecr.io https://core.windows.net	Öffentliche Regionen	Kommunikation mit Azure-Diensten.	Standard-, eingeschränkter und privater Modus.	Cloud Volumes ONTAP kann nicht mit dem Azure-Dienst kommunizieren, um bestimmte Vorgänge für die Konsole in Azure auszuführen.

Endpunkte	Gilt für	Zweck	Bereitstellungsmodi	Auswirkungen bei Nichtverfügbarkeit
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Region China	Kommunikation mit Azure-Diensten.	Standard-, eingeschränkter und privater Modus.	Cloud Volumes ONTAP kann nicht mit dem Azure-Dienst kommunizieren, um bestimmte Vorgänge für die Konsole in Azure auszuführen.
https://management.microsoftazure.de https://login.microsoftonline.de https://blob.core.cloudapi.de https://core.cloudapi.de	Deutschland Region	Kommunikation mit Azure-Diensten.	Standard-, eingeschränkter und privater Modus.	Cloud Volumes ONTAP kann nicht mit dem Azure-Dienst kommunizieren, um bestimmte Vorgänge für die Konsole in Azure auszuführen.
https://management.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net	Regierungsregionen	Kommunikation mit Azure-Diensten.	Standard-, eingeschränkter und privater Modus.	Cloud Volumes ONTAP kann nicht mit dem Azure-Dienst kommunizieren, um bestimmte Vorgänge für die Konsole in Azure auszuführen.
https://management.azure.microsoft.scloud https://login.microsoftonline.microsoft.scloud https://blob.core.microsoft.scloud https://core.microsoft.scloud	Regierungsregionen des Verteidigungsministeriums	Kommunikation mit Azure-Diensten.	Standard-, eingeschränkter und privater Modus.	Cloud Volumes ONTAP kann nicht mit dem Azure-Dienst kommunizieren, um bestimmte Vorgänge für die Konsole in Azure auszuführen.

Netzwerkproxykonfiguration des NetApp Console Agenten

Sie können die Proxyserverkonfiguration des NetApp Console Agenten verwenden, um ausgehenden Internetzugriff von Cloud Volumes ONTAP zu aktivieren. Die Konsole unterstützt zwei Arten von Proxys:

- **Expliziter Proxy**: Der ausgehende Datenverkehr von Cloud Volumes ONTAP verwendet die HTTP-Adresse des Proxyservers, der während der Proxykonfiguration des Konsolenagenten angegeben wurde. Der Administrator hat möglicherweise auch Benutzeranmeldeinformationen und Stammzertifizierungsstellenzertifikate für eine zusätzliche Authentifizierung konfiguriert. Wenn ein Stamm-CA-Zertifikat für den expliziten Proxy verfügbar ist, stellen Sie sicher , dass Sie dasselbe Zertifikat erhalten und mithilfe des "ONTAP CLI: Sicherheitszertifikat installieren" Befehl.
- **Transparenter Proxy**: Das Netzwerk ist so konfiguriert, dass ausgehender Datenverkehr von Cloud Volumes ONTAP automatisch über den Proxy für den Konsolenagenten geleitet wird. Beim Einrichten eines transparenten Proxys muss der Administrator für die Konnektivität von Cloud Volumes ONTAP nur

ein Stamm-CA-Zertifikat bereitstellen, nicht die HTTP-Adresse des Proxyservers. Stellen Sie sicher, dass Sie dasselbe Stamm-CA-Zertifikat erhalten und auf Ihr Cloud Volumes ONTAP System hochladen, indem Sie das "ONTAP CLI: Sicherheitszertifikat installieren" Befehl.

Informationen zum Konfigurieren von Proxy-Servern finden Sie im "Konfigurieren des Konsolenagenten zur Verwendung eines Proxyservers" .

IP-Adressen

Die Konsole weist Cloud Volumes ONTAP in Azure automatisch die erforderliche Anzahl privater IP-Adressen zu. Sie müssen sicherstellen, dass in Ihrem Netzwerk genügend private IP-Adressen verfügbar sind.

Die Anzahl der für Cloud Volumes ONTAP zugewiesenen LIFs hängt davon ab, ob Sie ein Einzelknotensystem oder ein HA-Paar bereitstellen. Ein LIF ist eine IP-Adresse, die einem physischen Port zugeordnet ist. Ein SVM-Management-LIF ist für Management-Tools wie SnapCenter erforderlich.

Ein iSCSI-LIF bietet Clientzugriff über das iSCSI-Protokoll und wird vom System für andere wichtige Netzwerk-Workflows verwendet. Diese LIFs sind erforderlich und sollten nicht gelöscht werden.

IP-Adressen für ein Einzelknotensystem

Die Console weist einem Einzelknotensystem 5 oder 6 IP-Adressen zu:

- Cluster-Verwaltungs-IP
- Knotenverwaltungs-IP
- Intercluster-IP für SnapMirror
- NFS/CIFS-IP
- iSCSI-IP

Die iSCSI-IP bietet Clientzugriff über das iSCSI-Protokoll. Es wird vom System auch für andere wichtige Netzwerk-Workflows verwendet. Dieses LIF ist erforderlich und sollte nicht gelöscht werden.

- SVM-Verwaltung (optional – nicht standardmäßig konfiguriert)

IP-Adressen für HA-Paare

Die Konsole weist während der Bereitstellung 4 NICs (pro Knoten) IP-Adressen zu.

Beachten Sie, dass die Console auf HA-Paaren eine SVM-Management-LIF erstellt, aber nicht auf Einzelknotensystemen in Azure.

NIC0

- Knotenverwaltungs-IP
- Intercluster-IP
- iSCSI-IP

Die iSCSI-IP bietet Clientzugriff über das iSCSI-Protokoll. Es wird vom System auch für andere wichtige Netzwerk-Workflows verwendet. Dieses LIF ist erforderlich und sollte nicht gelöscht werden.

NIC1

- Cluster-Netzwerk-IP

NIC2

- Cluster-Interconnect-IP (HA IC)

NIC3

- Pageblob NIC-IP (Festplattenzugriff)

NIC3 ist nur auf HA-Bereitstellungen anwendbar, die Page-Blob-Speicher verwenden.

Die oben genannten IP-Adressen werden bei Failover-Ereignissen nicht migriert.

Darüber hinaus sind 4 Frontend-IPs (FIPs) für die Migration bei Failover-Ereignissen konfiguriert. Diese Frontend-IPs befinden sich im Load Balancer.

- Cluster-Verwaltungs-IP
- NodeA-Daten-IP (NFS/CIFS)
- NodeB-Daten-IP (NFS/CIFS)
- SVM-Verwaltungs-IP

Sichere Verbindungen zu Azure-Diensten

Standardmäßig aktiviert die Konsole einen Azure Private Link für Verbindungen zwischen Cloud Volumes ONTAP und Azure Page Blob Storage-Konten.

In den meisten Fällen müssen Sie nichts tun – die Konsole verwaltet den Azure Private Link für Sie. Wenn Sie jedoch Azure Private DNS verwenden, müssen Sie eine Konfigurationsdatei bearbeiten. Sie sollten sich auch über eine Anforderung hinsichtlich des Speicherorts des Konsolen-Agenten in Azure im Klaren sein.

Sie können die Private Link-Verbindung auch deaktivieren, wenn dies für Ihre Geschäftsanforderungen erforderlich ist. Wenn Sie die Verknüpfung deaktivieren, konfiguriert die Konsole Cloud Volumes ONTAP so, dass stattdessen ein Service-Endpunkt verwendet wird.

"Erfahren Sie mehr über die Verwendung von Azure Private Links oder Service-Endpunkten mit Cloud Volumes ONTAP" .

Netzwerk für Azure VNet-Verschlüsselung

Cloud Volumes ONTAP unterstützt "Azure Virtual Network (VNet)-Verschlüsselung" die Verschlüsselung des VM-zu-VM-Datenverkehrs innerhalb eines VNet oder zwischen verbundenen VNets. Diese Funktion wird auf der Azure VNet-Ebene konfiguriert und ist unabhängig von der Cloud Volumes ONTAP-Topologie (Single Node oder HA).

Sie müssen lediglich sicherstellen, dass Accelerated Networking auf den Netzwerkkarten der VM aktiviert ist

und die Anforderungen und Einschränkungen der Azure VNet-Verschlüsselung überprüfen, bevor Sie die Funktion aktivieren. Sie sollten NetApp verwaltete Load-Balancer-Objekte nicht ändern.

"Azure documentation: VNet-Verschlüsselung und Accelerated Networking".

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 hierzu finden Sie im "Microsoft Azure-Dokumentation: Erstellen einer Site-to-Site-Verbindung im Azure-Portal" .

Port für die HA-Verbindung

Ein Cloud Volumes ONTAP HA-Paar umfasst eine HA-Verbindung, die es jedem Knoten ermöglicht, kontinuierlich zu prüfen, ob sein Partner funktioniert, und Protokolldaten für den nichtflüchtigen Speicher des anderen zu spiegeln. Die HA-Verbindung verwendet den 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 der TCP-Verkehr für Port 10006 geöffnet ist, damit das HA-Paar ordnungsgemäß funktionieren kann.

Nur ein HA-Paar in einer Azure-Ressourcengruppe

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

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

Sicherheitsgruppenregeln

Die Konsole erstellt Azure-Sicherheitsgruppen, die die eingehenden und ausgehenden Regeln für den erfolgreichen Betrieb von Cloud Volumes ONTAP enthalten. "Sicherheitsgruppenregeln für den Konsolenagenten anzeigen" .

Die Azure-Sicherheitsgruppen für Cloud Volumes ONTAP erfordern, dass die entsprechenden Ports für die interne Kommunikation zwischen den Knoten geöffnet sind. "Erfahren Sie mehr über die internen Ports von ONTAP" .

Wir empfehlen nicht, die vordefinierten Sicherheitsgruppen zu ändern oder benutzerdefinierte Sicherheitsgruppen zu verwenden. Wenn Sie dies jedoch tun müssen, beachten Sie, dass für den Bereitstellungsprozess das Cloud Volumes ONTAP -System vollständigen Zugriff innerhalb seines eigenen Subnetzes benötigt. Wenn Sie nach Abschluss der Bereitstellung die Netzwerksicherheitsgruppe ändern möchten, achten Sie darauf, dass die Cluster-Ports und HA-Netzwerk-Ports geöffnet bleiben. Dies gewährleistet eine nahtlose Kommunikation innerhalb des Cloud Volumes ONTAP Clusters (Any-to-Any-Kommunikation zwischen den Knoten).

Eingangsregeln für Einzelknotensysteme

Wenn Sie ein Cloud Volumes ONTAP -System hinzufügen und eine vordefinierte Sicherheitsgruppe auswählen, können Sie den Datenverkehr innerhalb einer der folgenden Gruppen zulassen:

- **Nur ausgewähltes VNet**: Die Quelle für eingehenden Datenverkehr ist der Subnetzbereich des VNet für das Cloud Volumes ONTAP -System und der Subnetzbereich des VNet, in dem sich der Konsolenagent befindet. Dies ist die empfohlene Option.
- **Alle VNets**: Die Quelle für eingehenden Datenverkehr ist der IP-Bereich 0.0.0.0/0.
- **Deaktiviert**: Diese Option schränkt den öffentlichen Netzwerkzugriff auf Ihr Speicherkonto ein und deaktiviert die Datenschichtung für Cloud Volumes ONTAP -Systeme. Dies ist eine empfohlene Option, wenn Ihre privaten IP-Adressen aufgrund von Sicherheitsbestimmungen und -richtlinien nicht einmal innerhalb desselben VNet offengelegt werden sollen.

Priorität und Name	Port und Protokoll	Quelle und Ziel	Beschreibung
1000 eingehendes SSH	22 TCP	Beliebig zu Beliebig	SSH-Zugriff auf die IP-Adresse des Cluster-Management-LIF oder eines Node-Management-LIF
1001 eingehendes_http	80 TCP	Beliebig zu Beliebig	HTTP-Zugriff auf die ONTAP System Manager-Webkonsole über die IP-Adresse des Cluster-Management-LIF
1002 inbound_111_tcp	111 TCP	Beliebig zu Beliebig	Remote Procedure Call für NFS
1003 inbound_111_udp	111 UDP	Beliebig zu Beliebig	Remote Procedure Call für NFS
1004 inbound_139	139 TCP	Beliebig zu Beliebig	NetBIOS-Dienstsitzung für CIFS
1005 inbound_161-162 _tcp	161-162 TCP	Beliebig zu Beliebig	Einfaches Netzwerkverwaltungsprotokoll
1006 inbound_161-162 _udp	161-162 UDP	Beliebig zu Beliebig	Einfaches Netzwerkverwaltungsprotokoll
1007 inbound_443	443 TCP	Beliebig zu Beliebig	Konnektivität mit dem Konsolenagenten und HTTPS-Zugriff auf die ONTAP System Manager-Webkonsole unter Verwendung der IP-Adresse des Cluster-Management-LIF
1008 inbound_445	445 TCP	Beliebig zu Beliebig	Microsoft SMB/CIFS über TCP mit NetBIOS-Framing
1009 inbound_635_tcp	635 TCP	Beliebig zu Beliebig	NFS-Mount
1010 inbound_635_udp	635 UDP	Beliebig zu Beliebig	NFS-Mount
1011 inbound_749	749 TCP	Beliebig zu Beliebig	Kerberos

Priorität und Name	Port und Protokoll	Quelle und Ziel	Beschreibung
1012 inbound_2049_tcp	2049 TCP	Beliebig zu Beliebig	NFS-Server-Daemon
1013 inbound_2049_udp	2049 UDP	Beliebig zu Beliebig	NFS-Server-Daemon
1014 inbound_3260	3260 TCP	Beliebig zu Beliebig	iSCSI-Zugriff über das iSCSI-Daten-LIF
1015 inbound_4045-4046_tcp	4045-4046 TCP	Beliebig zu Beliebig	NFS-Sperrdaemon und Netzwerkstatusmonitor
1016 inbound_4045-4046_udp	4045-4046 UDP	Beliebig zu Beliebig	NFS-Sperrdaemon und Netzwerkstatusmonitor
1017 eingehend_10000	10000 TCP	Beliebig zu Beliebig	Sicherung mit NDMP
1018 eingehend_11104-11105	11104-11105 TCP	Beliebig zu Beliebig	SnapMirror -Datenübertragung
3000 inbound_deny _all_tcp	Beliebiger TCP-Port	Beliebig zu Beliebig	Blockieren Sie den gesamten anderen eingehenden TCP-Verkehr
3001 inbound_deny _all_udp	Beliebiger Port UDP	Beliebig zu Beliebig	Blockieren Sie den gesamten anderen eingehenden UDP-Verkehr
65000 AllowVnetInBound	Beliebiger Port, jedes Protokoll	VirtualNetwork zu VirtualNetwork	Eingehender Datenverkehr aus dem VNet
65001 AllowAzureLoad BalancerInBound	Beliebiger Port, jedes Protokoll	AzureLoadBalancer zu Any	Datenverkehr vom Azure Standard Load Balancer
65500 DenyAllInBound	Beliebiger Port, jedes Protokoll	Beliebig zu Beliebig	Blockieren Sie den gesamten anderen eingehenden Datenverkehr

Eingehende Regeln für HA-Systeme

Wenn Sie ein Cloud Volumes ONTAP -System hinzufügen und eine vordefinierte Sicherheitsgruppe auswählen, können Sie den Datenverkehr innerhalb einer der folgenden Gruppen zulassen:

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

HA-Systeme haben weniger eingehende Regeln als Einzelknotensysteme, da der eingehende Datenverkehr über den Azure Standard Load Balancer geleitet wird. Aus diesem Grund sollte der Datenverkehr vom Load Balancer geöffnet sein, wie in der "AllowAzureLoadBalancerInBound"-Regel dargestellt.

- **Deaktiviert**: Diese Option schränkt den öffentlichen Netzwerkzugriff auf Ihr Speicherkonto ein und

deaktiviert die Datenschichtung für Cloud Volumes ONTAP -Systeme. Dies ist eine empfohlene Option, wenn Ihre privaten IP-Adressen aufgrund von Sicherheitsbestimmungen und -richtlinien nicht einmal innerhalb desselben VNet offengelegt werden sollen.

Priorität und Name	Port und Protokoll	Quelle und Ziel	Beschreibung
100 inbound_443	443 Jedes Protokoll	Beliebig zu Beliebig	Konnektivität mit dem Konsolenagenten und HTTPS-Zugriff auf die ONTAP System Manager-Webkonsole unter Verwendung der IP-Adresse des Cluster-Management-LIF
101 eingehend_111_tcp	111 Jedes Protokoll	Beliebig zu Beliebig	Remote Procedure Call für NFS
102 inbound_2049_tcp	2049 Jedes Protokoll	Beliebig zu Beliebig	NFS-Server-Daemon
111 eingehendes_ssh	22 Jedes Protokoll	Beliebig zu Beliebig	SSH-Zugriff auf die IP-Adresse des Cluster-Management-LIF oder eines Node-Management-LIF
121 inbound_53	53 Jedes Protokoll	Beliebig zu Beliebig	DNS und CIFS
65000 AllowVnetInBound	Beliebiger Port, jedes Protokoll	VirtualNetwork zu VirtualNetwork	Eingehender Datenverkehr aus dem VNet
65001 AllowAzureLoad BalancerInBound	Beliebiger Port, jedes Protokoll	AzureLoadBalancer zu Any	Datenverkehr vom Azure Standard Load Balancer
65500 DenyAllInBound	Beliebiger Port, jedes Protokoll	Beliebig zu Beliebig	Blockieren Sie den gesamten anderen eingehenden Datenverkehr

Ausgangsregeln

Die vordefinierte Sicherheitsgruppe für Cloud Volumes ONTAP öffnet den gesamten ausgehenden Datenverkehr. Wenn das akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Nachrichten. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Ausgangsregeln.

Grundlegende Ausgangsregeln

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

Hafen	Protokoll	Zweck
Alle	Alle TCP	Der gesamte ausgehende Verkehr
Alle	Alle UDP	Der gesamte ausgehende Verkehr

Erweiterte Ausgangsregeln

Wenn Sie strenge Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation von Cloud Volumes ONTAP erforderlich sind.

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

Service	Hafen	Protokoll	Quelle	Ziel	Zweck
Active Directory	88	TCP	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	137	UDP	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	138	UDP	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	NetBIOS-Datagrammdienst
	139	TCP	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	NetBIOS-Dienstsitzung
	389	TCP und UDP	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	LDAP
	445	TCP	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NetBIOS-Framing
	464	TCP	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern & festlegen (SET_CHANGE)
	464	UDP	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
	749	TCP	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (RPCSEC_GSS)
	88	TCP	Daten-LIF (NFS, CIFS, iSCSI)	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	137	UDP	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	138	UDP	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	NetBIOS-Datagrammdienst
	139	TCP	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	NetBIOS-Dienstsitzung
	389	TCP und UDP	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	LDAP
	445	TCP	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NetBIOS-Framing
	464	TCP	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern & festlegen (SET_CHANGE)
	464	UDP	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
	749	TCP	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern & festlegen (RPCSEC_GSS)

Service	Hafen	Protokoll	Quelle	Ziel	Zweck
AutoSupport	HTTPS	443	Knotenverwaltung LIF	mysupport.netapp.com	AutoSupport (HTTPS ist die Standardeinstellung)
	HTTP	80	Knotenverwaltung LIF	mysupport.netapp.com	AutoSupport (nur wenn das Transportprotokoll von HTTPS auf HTTP geändert wird)
	TCP	3128	Knotenverwaltung LIF	Konsolenagent	Senden von AutoSupport -Nachrichten über einen Proxyserver auf dem Konsolenagenten, wenn keine ausgehende Internetverbindung verfügbar ist
Konfigurationssicherungen	HTTP	80	Knotenverwaltung LIF	http://<IP-Adresse des Konsolenagenten>/occm/offboxconfig	Senden Sie Konfigurationssicherungen an den Konsolenagenten. "ONTAP-Dokumentation" .
DHCP	68	UDP	Knotenverwaltung LIF	DHCP	DHCP-Client für die Ersteinrichtung
DHCPS	67	UDP	Knotenverwaltung LIF	DHCP	DHCP-Server
DNS	53	UDP	Knotenverwaltungs-LIF und Daten-LIF (NFS, CIFS)	DNS	DNS
NDMP	18600–18699	TCP	Knotenverwaltung LIF	Zielserver	NDMP-Kopie
SMTP	25	TCP	Knotenverwaltung LIF	Mailserver	SMTP-Benachrichtigungen, können für AutoSupport verwendet werden
SNMP	161	TCP	Knotenverwaltung LIF	Monitorserver	Überwachung durch SNMP-Traps
	161	UDP	Knotenverwaltung LIF	Monitorserver	Überwachung durch SNMP-Traps
	162	TCP	Knotenverwaltung LIF	Monitorserver	Überwachung durch SNMP-Traps
	162	UDP	Knotenverwaltung LIF	Monitorserver	Überwachung durch SNMP-Traps
SnapMirror	11104	TCP	Intercluster LIF	ONTAP Intercluster-LIFs	Verwaltung von Intercluster-Kommunikationssitzungen für SnapMirror
	11105	TCP	Intercluster LIF	ONTAP Intercluster-LIFs	SnapMirror -Datenübertragung
Syslog	514	UDP	Knotenverwaltung LIF	Syslog-Server	Syslog-Weiterleitungsnachrichten

Anforderungen für den Konsolenagenten

Wenn Sie noch keinen Konsolenagenten erstellt haben, sollten Sie auch die Netzwerkanforderungen für den Konsolenagenten überprüfen.

- "Netzwerkanforderungen für den Konsolenagenten anzeigen"
- "Sicherheitsgruppenregeln in Azure"

Verwandte Themen

- "Überprüfen Sie das AutoSupport -Setup für Cloud Volumes ONTAP"
- "Erfahren Sie mehr über die internen Ports von ONTAP" .

Richten Sie Cloud Volumes ONTAP für die Verwendung eines vom Kunden verwalteten Schlüssels in Azure ein

Daten werden auf Cloud Volumes ONTAP in Azure mithilfe der Azure Storage Service Encryption mit einem von Microsoft verwalteten Schlüssel automatisch verschlüsselt. Sie können stattdessen jedoch 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 mit "Azure Storage Service-Verschlüsselung" . Die Standardimplementierung verwendet einen von Microsoft verwalteten Schlüssel. Es ist keine Einrichtung erforderlich.

Wenn Sie einen vom Kunden verwalteten Schlüssel mit Cloud Volumes ONTAP verwenden möchten, müssen Sie die folgenden Schritte ausführen:

1. Erstellen Sie in Azure einen Schlüsseltresor und generieren Sie dann einen Schlüssel in diesem Tresor.
2. Verwenden Sie in der NetApp Console die API, um ein Cloud Volumes ONTAP -System zu erstellen, das den Schlüssel verwendet.

So werden Daten verschlüsselt

Die Konsole verwendet einen Datenträgerverschlüsselungssatz, der die Verwaltung von Verschlüsselungsschlüsseln mit verwalteten Datenträgern und nicht mit Seitenblobs ermöglicht. Alle neuen Datenträger verwenden ebenfalls denselben Datenträgerverschlüsselungssatz. Niedrigere Versionen verwenden den von Microsoft verwalteten Schlüssel anstelle des vom Kunden verwalteten Schlüssels.

Nachdem Sie ein Cloud Volumes ONTAP -System erstellt haben, das für die Verwendung eines vom Kunden verwalteten Schlüssels konfiguriert ist, werden Cloud Volumes ONTAP Daten wie folgt verschlüsselt.

Cloud Volumes ONTAP Konfiguration	Für die Schlüsselverschlüsselung verwendete Systemfestplatten	Für die Schlüsselverschlüsselung verwendete Datenträger
Einzelner Knoten	• Stiefel • Kern • NVRAM	• Wurzel • Daten

Cloud Volumes ONTAP Konfiguration	Für die Schlüsselverschlüsselung verwendete Systemfestplatten	Für die Schlüsselverschlüsselung verwendete Datenträger
Azure HA – einzelne Verfügbarkeitszone mit Seitenblobs	• Stiefel • Kern • NVRAM	Keine
Azure HA – einzelne Verfügbarkeitszone mit gemeinsam genutzten verwalteten Datenträgern	• Stiefel • Kern • NVRAM	• Wurzel • Daten
Azure HA mehrere Verfügbarkeitszonen mit gemeinsam genutzten verwalteten Datenträgern	• Stiefel • Kern • NVRAM	• Wurzel • Daten

Alle Azure-Speicherkonten für Cloud Volumes ONTAP werden mit einem vom Kunden verwalteten Schlüssel verschlüsselt. Wenn Sie Ihre Speicherkonten während der Erstellung verschlüsseln möchten, müssen Sie die ID der Ressource in der Cloud Volumes ONTAP Erstellungsanforderung erstellen und angeben. Dies gilt für alle Arten von Bereitstellungen. Wenn Sie ihn nicht angeben, werden die Speicherkonten trotzdem verschlüsselt, aber die Konsole erstellt zuerst die Speicherkonten mit einer von Microsoft verwalteten Schlüsselverschlüsselung und aktualisiert dann die Speicherkonten, um den vom Kunden verwalteten Schlüssel zu verwenden.

Schlüsselrotation in Cloud Volumes ONTAP

Wenn Sie Ihre Verschlüsselungsschlüssel konfigurieren, müssen Sie das Azure-Portal verwenden, um die automatische Schlüsselrotation einzurichten und zu aktivieren. Durch das Erstellen und Aktivieren einer neuen Version von Verschlüsselungsschlüsseln wird sichergestellt, dass Cloud Volumes ONTAP die neueste Schlüsselversion automatisch erkennen und für die Verschlüsselung verwenden kann. So wird sichergestellt, dass Ihre Daten ohne manuelles Eingreifen sicher bleiben.

Informationen zum Konfigurieren Ihrer Schlüssel und zum Einrichten der Schlüsselrotation finden Sie in den folgenden Microsoft Azure-Dokumentationsthemen:

- "Konfigurieren der automatischen Rotation kryptografischer Schlüssel in Azure Key Vault"
- "Azure PowerShell – Aktivieren von kundenseitig verwalteten Schlüsseln"

> Stellen Sie nach der Konfiguration der Schlüssel sicher, dass Sie "*Automatische Drehung aktivieren*" , damit Cloud Volumes ONTAP die neuen Schlüssel verwenden kann, wenn die vorherigen Schlüssel ablaufen. Wenn Sie diese Option im Azure-Portal nicht aktivieren, kann Cloud Volumes ONTAP die neuen Schlüssel nicht automatisch erkennen, was zu Problemen bei der Speicherbereitstellung führen kann.

Erstellen einer benutzerseitig zugewiesenen verwalteten Identität

Sie haben die Möglichkeit, eine Ressource namens „benutzerseitig zugewiesene verwaltete Identität“ zu erstellen. Auf diese Weise können Sie Ihre Speicherkonten verschlüsseln, wenn Sie ein Cloud Volumes ONTAP -System erstellen. Wir empfehlen, diese Ressource zu erstellen, bevor Sie einen Schlüsseltresor

erstellen und einen Schlüssel generieren.

Die Ressource hat die folgende ID: `userassignedidentity` .

Schritte

1. Gehen Sie in Azure zu Azure-Diensten und wählen Sie **Verwaltete Identitäten** aus.
2. Klicken Sie auf **Erstellen**.
3. Geben Sie die folgenden Details an:
   - **Abonnement**: Wählen Sie ein Abonnement. Wir empfehlen, dasselbe Abonnement wie das Abonnement des Konsolenagenten zu wählen.
   - **Ressourcengruppe**: Verwenden Sie eine vorhandene Ressourcengruppe oder erstellen Sie eine neue.
   - **Region**: Wählen Sie optional dieselbe Region wie der Konsolenagent aus.
   - **Name**: Geben Sie einen Namen für die Ressource ein.
4. Fügen Sie optional Tags hinzu.
5. Klicken Sie auf **Erstellen**.

Erstellen eines Schlüsseltresors und Generieren eines Schlüssels

Der Schlüsseltresor muss sich im selben Azure-Abonnement und in derselben Region befinden, in der Sie das Cloud Volumes ONTAP -System erstellen möchten.

Wenn dueine benutzerseitig zugewiesene verwaltete Identität erstellt , während Sie den Schlüsseltresor erstellen, sollten Sie auch eine Zugriffsrichtlinie für den Schlüsseltresor erstellen.

Schritte

1. "Erstellen eines Schlüsseltresors in Ihrem Azure-Abonnement" .

   Beachten Sie die folgenden Anforderungen für den Schlüsseltresor:

   - Der Schlüsseltresor 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, darf aber *nicht* deaktiviert werden)
     - **Spülschutz**
     - **Azure Disk Encryption für die Volume-Verschlüsselung** (für Einzelknotensysteme, HA-Paare in mehreren Zonen und HA-Einzel-AZ-Bereitstellungen)

       Die Verwendung von vom Azure-Kunden verwalteten Verschlüsselungsschlüsseln hängt davon ab, ob die Azure-Datenträgerverschlüsselung für den Schlüsseltresor aktiviert ist.

   - Die folgende Option sollte aktiviert sein, wenn Sie eine benutzerseitig zugewiesene verwaltete Identität erstellt haben:
     - **Richtlinie zum Tresorzugriff**
2. Wenn Sie „Tresorzugriffsrichtlinie“ ausgewählt haben, klicken Sie auf „Erstellen“, um eine Zugriffsrichtlinie für den Schlüsseltresor zu erstellen. Wenn nicht, fahren Sie mit Schritt 3 fort.
   a. Wählen Sie die folgenden Berechtigungen aus:

- erhalten
- Liste
- entschlüsseln
- verschlüsseln
- Schlüssel auspacken
- Wrap-Schlüssel
- verifizieren
- Zeichen

b. Wählen Sie die vom Benutzer zugewiesene verwaltete Identität (Ressource) als Prinzipal aus.

c. Überprüfen und erstellen Sie die Zugriffsrichtlinie.

3. "Generieren eines Schlüssels im Schlüsseltresor" .

   Beachten Sie folgende Anforderungen an den Schlüssel:

   - Der Schlüsseltyp muss **RSA** sein.
   - Die empfohlene RSA-Schlüsselgröße ist **2048**, es werden jedoch auch andere Größen unterstützt.

Erstellen Sie ein System, das den Verschlüsselungsschlüssel verwendet

Nachdem Sie den Schlüsseltresor 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 durch die Verwendung der API unterstützt.

Erforderliche Berechtigungen

Wenn Sie einen vom Kunden verwalteten Schlüssel mit einem Cloud Volumes ONTAP System mit einem einzelnen Knoten verwenden möchten, stellen Sie sicher, dass der Konsolenagent 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"
```

"Aktuelle Liste der Berechtigungen anzeigen"

Schritte

1. Rufen Sie die Liste der Schlüsseltresore in Ihrem Azure-Abonnement mithilfe des folgenden API-Aufrufs ab.

   Für ein HA-Paar: `GET /azure/ha/metadata/vaults`

   Für einen einzelnen Knoten: `GET /azure/vsa/metadata/vaults`

Notieren Sie sich den **Namen** und die **Ressourcengruppe**. Sie müssen diese Werte im nächsten Schritt angeben.

"Erfahren Sie mehr über diesen API-Aufruf" .

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

   Für ein HA-Paar: `GET /azure/ha/metadata/keys-vault`

   Für einen einzelnen Knoten: `GET /azure/vsa/metadata/keys-vault`

   Notieren Sie sich den **Schlüsselnamen**. Sie müssen diesen Wert (zusammen mit dem Tresornamen) im nächsten Schritt angeben.

   "Erfahren Sie mehr über diesen API-Aufruf" .

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

   a. Für ein HA-Paar:

      `POST /azure/ha/working-environments`

      Der Anforderungstext muss die folgenden Felder enthalten:

      ```
      "azureEncryptionParameters": {
                    "key": "keyName",
                    "vaultName": "vaultName"
      }
      ```

      Fügen Sie die `"userAssignedIdentity": " userAssignedIdentityId"` Feld, wenn Sie diese Ressource zur Verwendung für die Speicherkontoverschlüsselung erstellt haben.

      "Erfahren Sie mehr über diesen API-Aufruf" .

   b. Für ein Single-Node-System:

      `POST /azure/vsa/working-environments`

      Der Anforderungstext muss die folgenden Felder enthalten:

      ```
      "azureEncryptionParameters": {
                    "key": "keyName",
                    "vaultName": "vaultName"
      }
      ```

      Fügen Sie die `"userAssignedIdentity": " userAssignedIdentityId"` Feld, wenn Sie diese Ressource zur Verwendung für die Speicherkontoverschlüsselung erstellt haben.

"Erfahren Sie mehr über diesen API-Aufruf" .

Ergebnis

Sie verfügen über ein neues Cloud Volumes ONTAP -System, das für die Verwendung Ihres vom Kunden verwalteten Schlüssels zur Datenverschlüsselung konfiguriert ist.

Einrichten der Lizenzierung für Cloud Volumes ONTAP in Azure

Nachdem Sie entschieden haben, welche Lizenzierungsoption Sie mit Cloud Volumes ONTAP verwenden möchten, sind einige Schritte erforderlich, bevor Sie diese Lizenzierungsoption beim Erstellen eines neuen Systems auswählen können.

Freemium

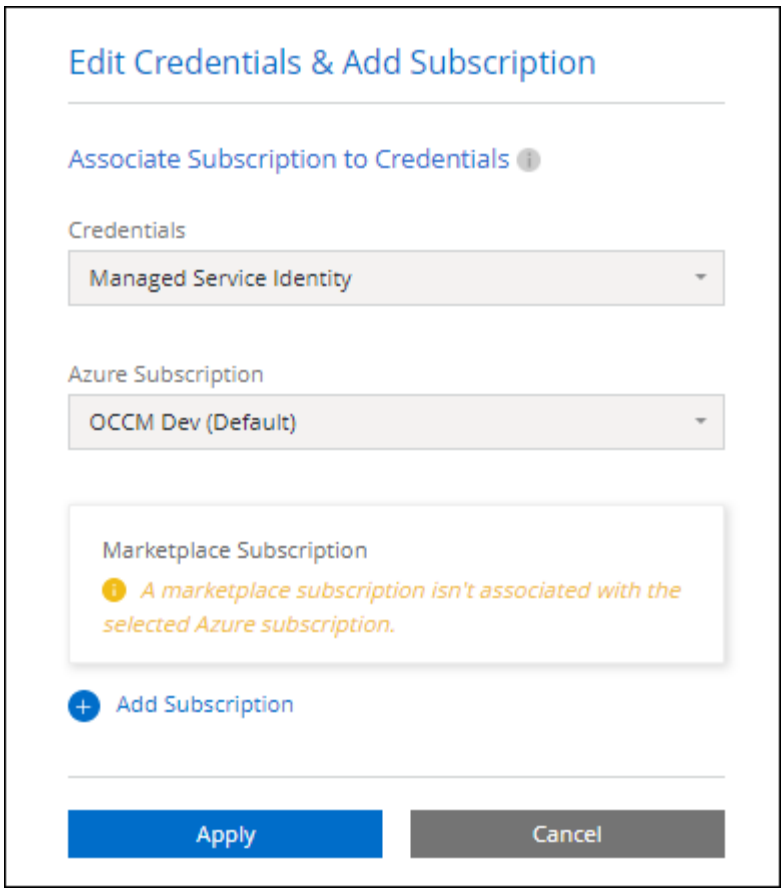
Wählen Sie das Freemium-Angebot, um Cloud Volumes ONTAP mit bis zu 500 GiB bereitgestellter Kapazität kostenlos zu nutzen. "Erfahren Sie mehr über das Freemium-Angebot" .

Schritte

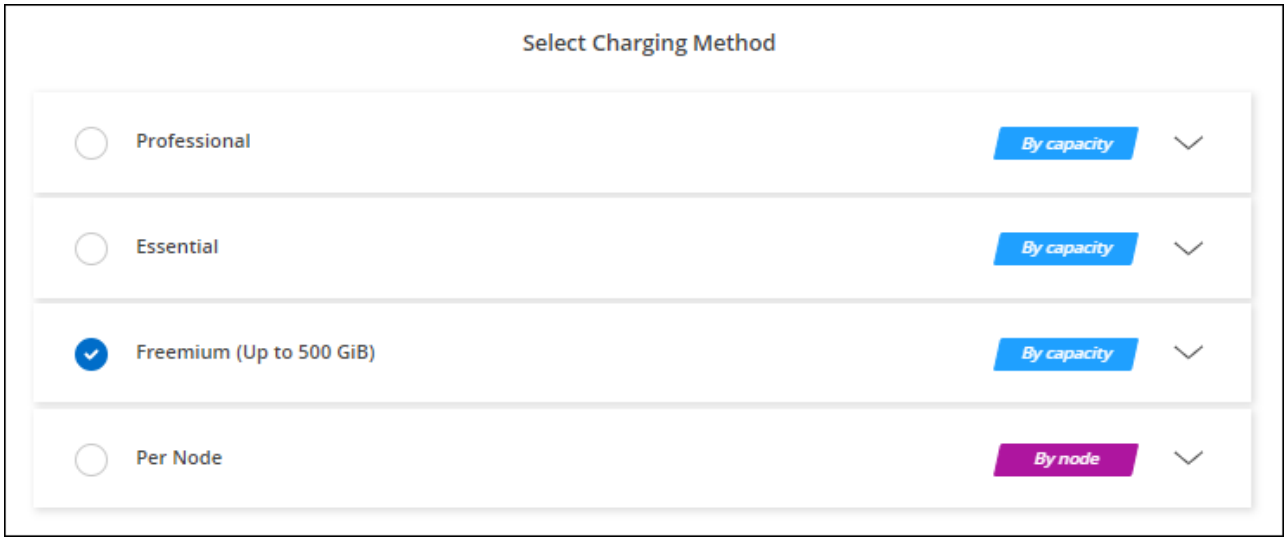
1. Wählen Sie im linken Navigationsmenü der NetApp Console*Speicher > Verwaltung* aus.
2. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Schritten.

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

    Ihnen werden keine Kosten über das Marktplatz-Abonnement berechnet, es sei denn, Sie überschreiten 500 GiB bereitgestellte Kapazität. Zu diesem Zeitpunkt wird das System automatisch auf das"Essentials-Paket" .



a. Nachdem Sie zur Konsole zurückgekehrt sind, wählen Sie **Freemium** aus, wenn Sie die Seite mit den Abrechnungsmethoden erreichen.



"Sehen Sie sich die Schritt-für-Schritt-Anleitung zum Starten von Cloud Volumes ONTAP in Azure an" .

Kapazitätsbasierte Lizenz

Mit der kapazitätsbasierten Lizenzierung können Sie für Cloud Volumes ONTAP pro TiB Kapazität bezahlen. Die kapazitätsbasierte Lizenzierung ist in Form eines *Pakets* verfügbar: das Essentials-Paket oder das Professional-Paket.

Die Pakete Essentials und Professional sind mit folgenden Verbrauchsmodellen bzw. Kaufoptionen erhältlich:

- Eine von NetApp erworbene Lizenz (Bring Your Own License (BYOL))
- Ein stündliches Pay-as-you-go-Abonnement (PAYGO) aus dem Azure Marketplace
- Ein Jahresvertrag

"Erfahren Sie mehr über kapazitätsbasierte Lizenzierung" .

In den folgenden Abschnitten wird beschrieben, wie Sie mit jedem dieser Verbrauchsmodelle beginnen.

BYOL

Zahlen Sie im Voraus, indem Sie eine Lizenz (BYOL) von NetApp erwerben, um Cloud Volumes ONTAP -Systeme bei jedem Cloud-Anbieter bereitzustellen.

> NetApp hat den Erwerb, die Verlängerung und die Erneuerung von BYOL-Lizenzen eingeschränkt. Weitere Informationen finden Sie unter "Eingeschränkte Verfügbarkeit der BYOL-Lizenzierung für Cloud Volumes ONTAP" .

Schritte

1. "Kontaktieren Sie den NetApp -Vertrieb, um eine Lizenz zu erhalten"
2. "Fügen Sie Ihr NetApp Support Site-Konto zur Konsole hinzu"

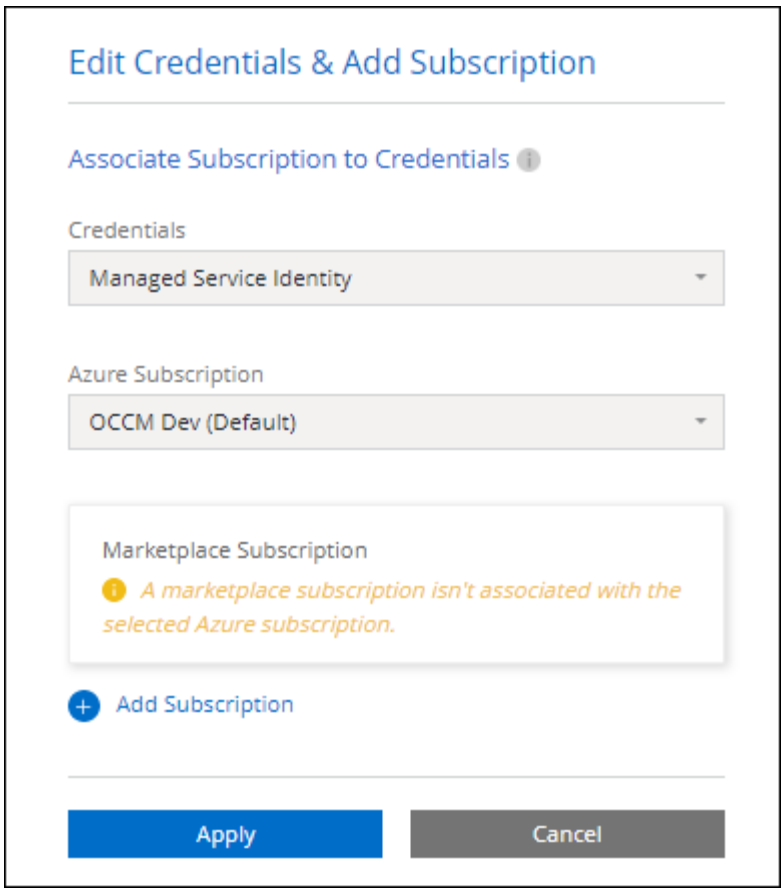
   Die Konsole fragt automatisch den Lizenzierungsdienst von NetApp ab, um Details zu den Lizenzen abzurufen, die mit Ihrem NetApp Support Site-Konto verknüpft sind. Wenn keine Fehler auftreten, fügt die Konsole die Lizenzen automatisch zur Konsole hinzu.

   Ihre Lizenz muss in der Konsole verfügbar sein, bevor Sie sie mit Cloud Volumes ONTAP verwenden können. Bei Bedarf können Sie"Fügen Sie die Lizenz manuell zur Konsole hinzu" .

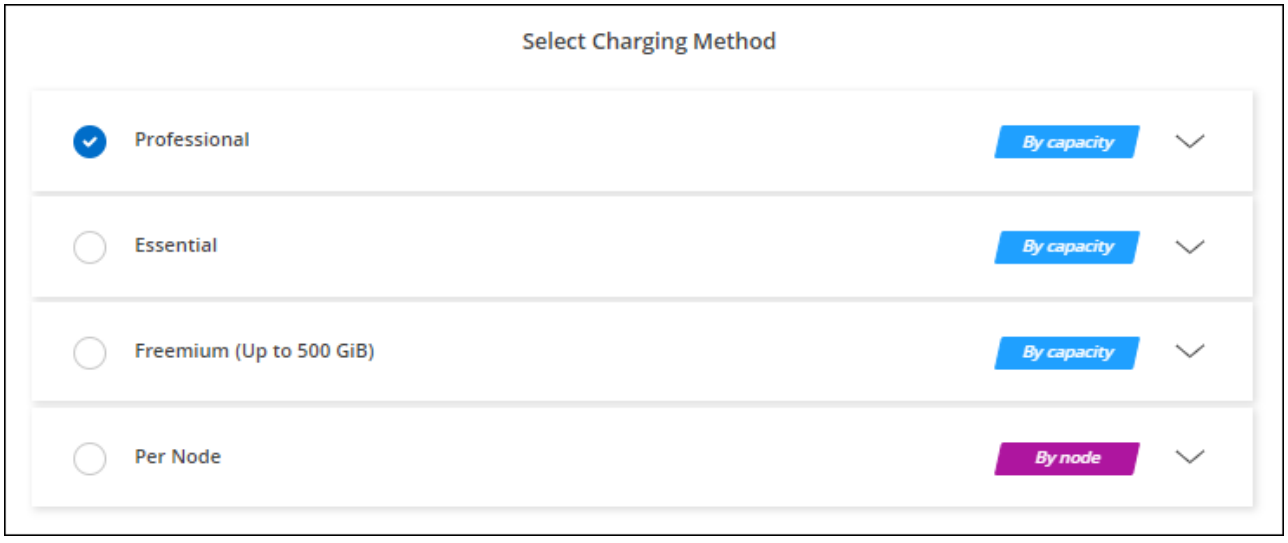
3. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Schritten.

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

      Die von Ihnen bei NetApp erworbene Lizenz wird immer zuerst in Rechnung gestellt. Wenn Sie jedoch Ihre lizenzierte Kapazität überschreiten oder die Laufzeit Ihrer Lizenz abläuft, wird Ihnen der Stundensatz auf dem Marktplatz in Rechnung gestellt.



a. Nachdem Sie zur Konsole zurückgekehrt sind, wählen Sie auf der Seite mit den Abrechnungsmethoden ein kapazitätsbasiertes Paket aus.



"Sehen Sie sich die Schritt-für-Schritt-Anleitung zum Starten von Cloud Volumes ONTAP in Azure an" .

PAYGO-Abonnement

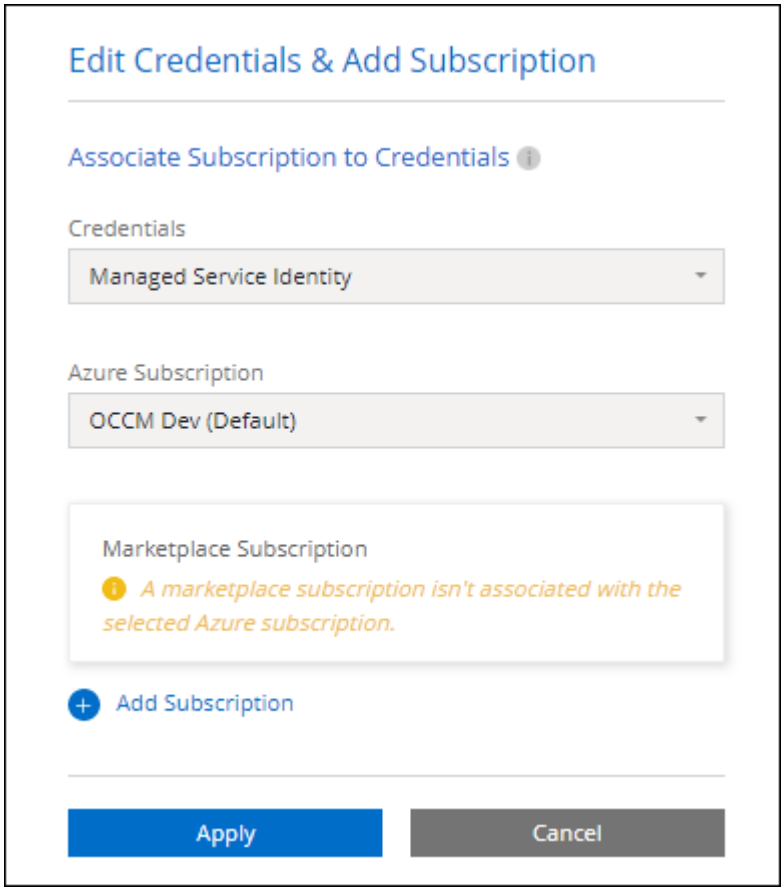
Zahlen Sie stundenweise, indem Sie das Angebot auf dem Marktplatz Ihres Cloud-Anbieters abonnieren.

Wenn Sie ein Cloud Volumes ONTAP -System erstellen, werden Sie von der Konsole aufgefordert, die im Azure Marketplace verfügbare Vereinbarung zu abonnieren. Dieses Abonnement wird dann zum Aufladen mit

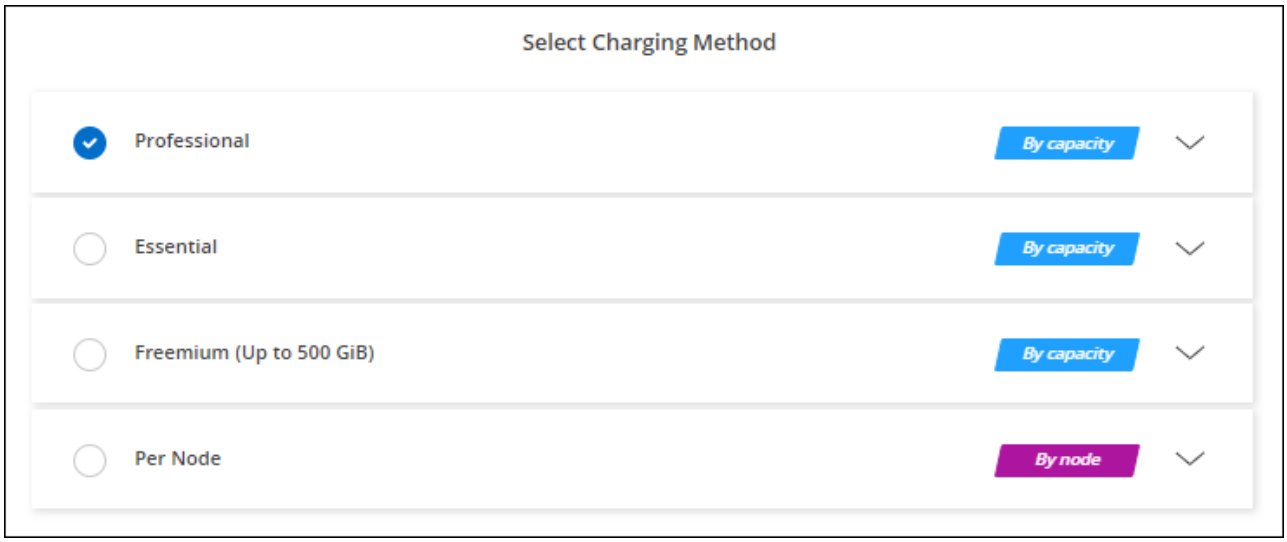
dem System verknüpft. Sie können dasselbe Abonnement für zusätzliche Systeme verwenden.

Schritte

1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.
2. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Schritten.
   a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldeinformationen bearbeiten > Abonnement hinzufügen** und folgen Sie dann den Anweisungen, um das Pay-as-you-go-Angebot im Azure Marketplace zu abonnieren.



   b. Nachdem Sie zur Konsole zurückgekehrt sind, wählen Sie auf der Seite mit den Abrechnungsmethoden ein kapazitätsbasiertes Paket aus.



"Sehen Sie sich die Schritt-für-Schritt-Anleitung zum Starten von Cloud Volumes ONTAP in Azure an" .

Sie können die mit Ihren Azure-Konten verknüpften Azure Marketplace-Abonnements auf der Seite „Einstellungen > Anmeldeinformationen“ verwalten. "Erfahren Sie, wie Sie Ihre Azure-Konten und -Abonnements verwalten"

Jahresvertrag

Bezahlen Sie Cloud Volumes ONTAP jährlich, indem Sie einen Jahresvertrag abschließen.

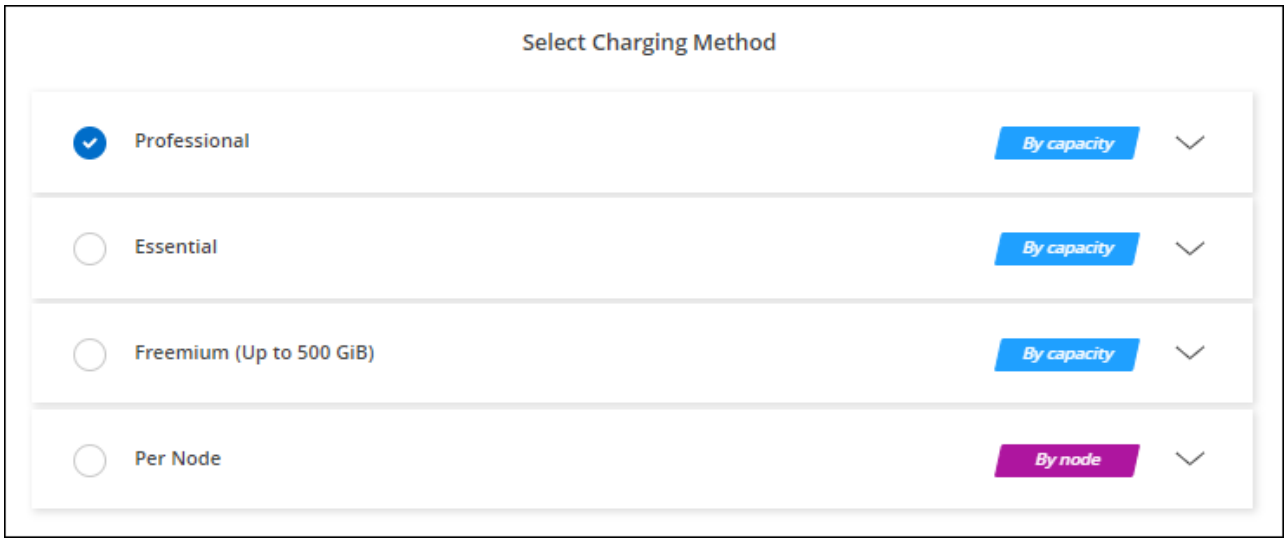
Schritte

1. Wenden Sie sich an Ihren NetApp Vertriebsmitarbeiter, um einen Jahresvertrag abzuschließen.

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

   Nachdem NetApp Ihnen das private Angebot mitgeteilt hat, können Sie bei der Systemerstellung den Jahresplan auswählen, wenn Sie sich im Azure Marketplace anmelden.

2. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Schritten.
   a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldeinformationen bearbeiten > Abonnement hinzufügen > Fortfahren**.
   b. Wählen Sie im Azure-Portal den Jahresplan aus, der mit Ihrem Azure-Konto geteilt wurde, und klicken Sie dann auf **Abonnieren**.
   c. Nachdem Sie zur Konsole zurückgekehrt sind, wählen Sie auf der Seite mit den Abrechnungsmethoden ein kapazitätsbasiertes Paket aus.



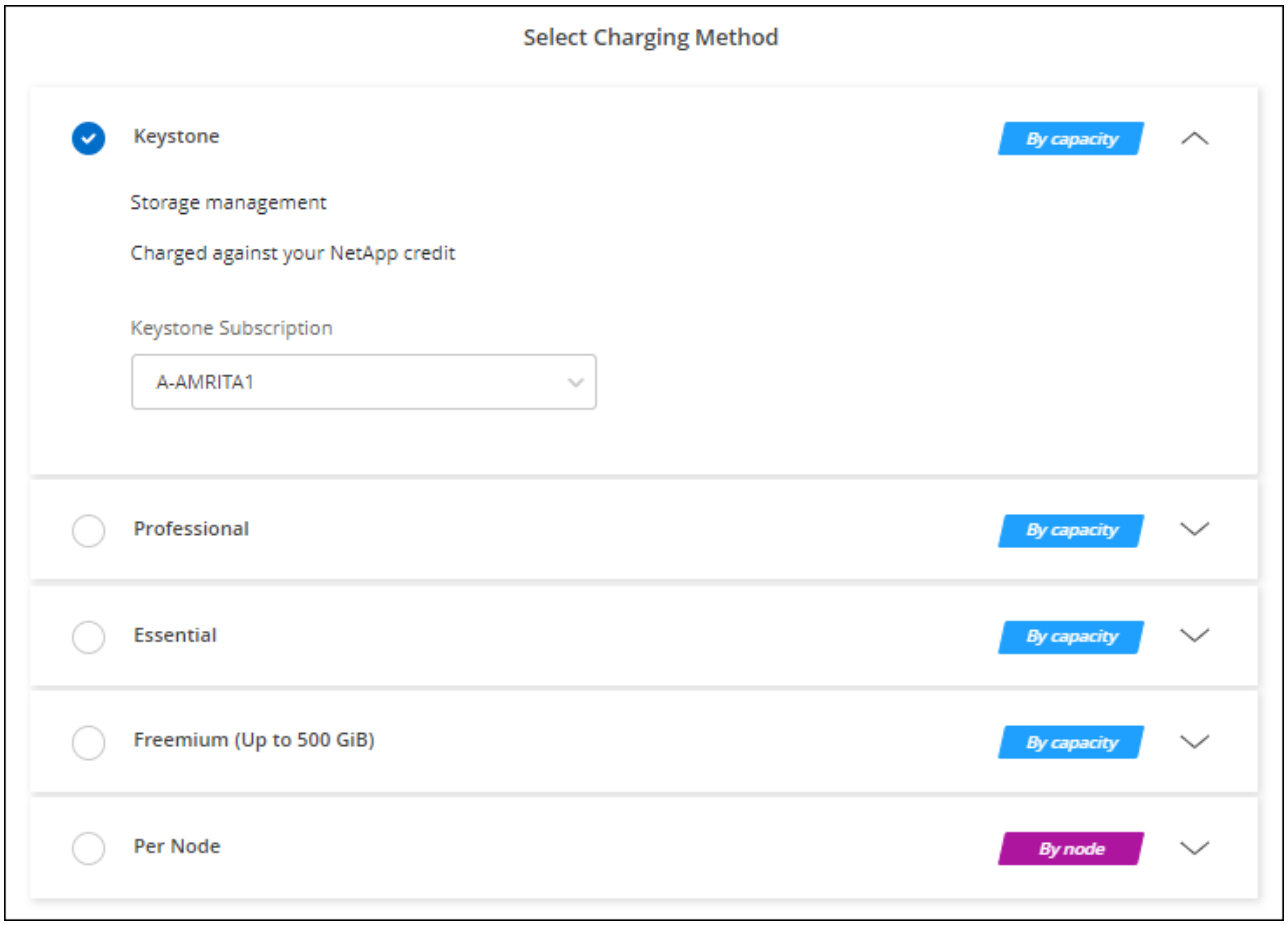
"Sehen Sie sich die Schritt-für-Schritt-Anleitung zum Starten von Cloud Volumes ONTAP in Azure an" .

Keystone Abonnement

Bei einem Keystone -Abonnement handelt es sich um einen Abonnementdienst mit nutzungsabhängiger Bezahlung. "Erfahren Sie mehr über NetApp Keystone -Abonnements" .

Schritte

1. Wenn Sie noch kein Abonnement haben, "NetApp kontaktieren"
2. mailto:ng-keystone-success@netapp.com [Kontaktieren Sie NetApp], um Ihr Benutzerkonto in der Konsole mit einem oder mehreren Keystone Abonnements zu autorisieren.
3. Nachdem NetApp Ihr Konto autorisiert hat,"Verknüpfen Sie Ihre Abonnements zur Verwendung mit Cloud Volumes ONTAP" .
4. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Schritten.
    a. Wählen Sie die Abrechnungsmethode „Keystone -Abonnement“ aus, wenn Sie zur Auswahl einer Abrechnungsmethode aufgefordert werden.



"Sehen Sie sich die Schritt-für-Schritt-Anleitung zum Starten von Cloud Volumes ONTAP in Azure an" .

Knotenbasierte Lizenz

Eine knotenbasierte Lizenz ist die Lizenz der vorherigen Generation für Cloud Volumes ONTAP. Eine knotenbasierte Lizenz kann von NetApp (BYOL) erworben werden und ist nur in bestimmten Fällen für Lizenzverlängerungen verfügbar. Weitere Informationen finden Sie unter:

- "Ende der Verfügbarkeit knotenbasierter Lizenzen"
- "Ende der Verfügbarkeit von knotenbasierten Lizenzen"
- "Konvertieren Sie eine knotenbasierte Lizenz in eine kapazitätsbasierte Lizenz"

Aktivieren Sie den Hochverfügbarkeitsmodus für Cloud Volumes ONTAP in Azure

Sie sollten den Hochverfügbarkeitsmodus (HA) von Microsoft Azure aktivieren, um ungeplante Failover-Zeiten zu reduzieren und die NFSv4-Unterstützung für Cloud Volumes ONTAP zu ermöglichen. Wenn Sie diesen Modus aktivieren, können Ihre Cloud Volumes ONTAP HA-Knoten bei ungeplanten Failovern auf CIFS- und NFSv4-Clients ein niedriges Recovery Time Objective (RTO) von 60 Sekunden erreichen.

Ab Cloud Volumes ONTAP 9.10.1 haben wir die ungeplante Failover-Zeit für Cloud Volumes ONTAP HA-Paare, die in Microsoft Azure ausgeführt werden, reduziert und Unterstützung für NFSv4 hinzugefügt. Um diese Verbesserungen für Cloud Volumes ONTAP verfügbar zu machen, müssen Sie die Hochverfügbarkeitsfunktion in Ihrem Azure-Abonnement aktivieren.

Informationen zu diesem Vorgang

NetApp Console fordert Sie mit diesen Details auf, wenn die Funktion in einem Azure-Abonnement aktiviert werden muss. Beachten Sie Folgendes:

- Es gibt keine Probleme mit der Hochverfügbarkeit Ihres Cloud Volumes ONTAP HA-Paares. Diese Azure-Funktion arbeitet mit ONTAP zusammen, um die vom Client beobachtete Anwendungsausfallzeit für NFS-Protokolle zu reduzieren, die aus ungeplanten Failover-Ereignissen resultiert.
- Das Aktivieren dieser Funktion hat keine Unterbrechungen für Cloud Volumes ONTAP HA-Paare.
- Das Aktivieren dieser Funktion für Ihr Azure-Abonnement verursacht keine Probleme mit anderen VMs.
- Cloud Volumes ONTAP verwendet einen internen Azure Load Balancer während Failovers von Cluster- und SVM-Management-LIFs auf CIFS- und NFS-Clients.
- Wenn der HA-Modus aktiviert ist, scannt die Konsole das System alle 12 Stunden, um die internen Azure Load Balancer-Regeln zu aktualisieren.

Schritte

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

1. "Greifen Sie über das Azure-Portal auf die Azure Cloud Shell zu"
2. Registrieren Sie die Funktion für den Hochverfügbarkeitsmodus:

```
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 ähnlich dem 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"
}
```

Weiterführende Links

1. "Microsoft Azure documentation: Übersicht über Hochverfügbarkeitsports"
2. "Microsoft Azure documentation: Erste Schritte mit der Azure CLI"

Aktivieren Sie VMOrchestratorZonalMultiFD für Cloud Volumes ONTAP in Azure

Für die Bereitstellung von VM-Instanzen in lokal redundanten Speicher-Einzelverfügbarkeitszonen (Local-Redundant Storage, LRS) sollten Sie die Microsoft `Microsoft.Compute/VMOrchestratorZonalMultiFD` Funktion für Ihre Abonnements. Im Hochverfügbarkeitsmodus (HA) erleichtert diese Funktion die Bereitstellung von Knoten in separaten Fehlerdomänen in derselben Verfügbarkeitszone.

Wenn Sie diese Funktion nicht aktivieren, erfolgt keine zonale Bereitstellung und die vorherige nicht zonale LRS-Bereitstellung wird wirksam.

Informationen zur VM-Bereitstellung in einer einzelnen Verfügbarkeitszone finden Sie unter"Hochverfügbarkeitspaare in Azure" .

Führen Sie diese Schritte als Benutzer mit „Eigentümer“-Berechtigungen aus:

Schritte

1. Greifen Sie über das Azure-Portal auf Azure Cloud Shell zu. Weitere Informationen finden Sie im "Microsoft Azure-Dokumentation: Erste Schritte mit Azure Cloud Shell" .
2. Registrieren Sie sich für die `Microsoft.Compute/VMOrchestratorZonalMultiFD` Funktion, indem Sie diesen Befehl ausführen:

   ```
   az account set -s <Azure_subscription_name_or_ID> az feature register --name VMOrchestratorZonalMultiFD --namespace Microsoft.Compute
   ```

3. Überprüfen Sie den Registrierungsstatus und das Ausgabebeispiel:

   ```
   az feature show -n VMOrchestratorZonalMultiFD --namespace Microsoft.Compute { "id": "/subscriptions/<ID>/providers/Microsoft.Features/providers/Microsoft.Compute/features/VMOrchestratorZonalMultiFD", "name": "Microsoft.Compute/VMOrchestratorZonalMultiFD", "properties": { "state": "Registered" }, "type": "Microsoft.Features/providers/features" }
   ```

Starten Sie Cloud Volumes ONTAP in Azure

Sie können ein Einzelknotensystem oder ein HA-Paar in Azure starten, indem Sie ein Cloud Volumes ONTAP-System in der NetApp Console erstellen.

Bevor Sie beginnen

Bevor Sie beginnen, benötigen Sie Folgendes.

- Ein Konsolenagent, der aktiv ist und läuft.
  - Sie sollten über eine "Konsolenagent, der mit Ihrem System verknüpft ist" .
  - "Sie sollten darauf vorbereitet sein, den Konsolenagenten immer laufen zu lassen" .

- Ein Verständnis der Konfiguration, die Sie verwenden möchten.

  Sie sollten eine Konfiguration geplant haben und die erforderlichen Azure-Netzwerkdetails von Ihrem Administrator erhalten haben. Weitere Informationen finden Sie unter "Planen Ihrer Cloud Volumes ONTAP Konfiguration" .

- Ein Verständnis dafür, was zum Einrichten der Lizenzierung für Cloud Volumes ONTAP erforderlich ist.

  "Erfahren Sie, wie Sie die Lizenzierung einrichten" .

Informationen zu diesem Vorgang

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

Möglicher Datenverlust

Die bewährte Methode besteht darin, 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 die Konsole Cloud Volumes ONTAP -Ressourcen im Falle eines Bereitstellungsfehlers oder einer Löschung aus einer freigegebenen Ressourcengruppe entfernen kann, kann es vorkommen, dass ein Azure-Benutzer versehentlich Cloud Volumes ONTAP -Ressourcen aus einer freigegebenen Ressourcengruppe löscht.

Starten Sie ein Cloud Volumes ONTAP -System mit einem Knoten in Azure

Wenn Sie ein Single-Node-Cloud Volumes ONTAP-System in Azure starten möchten, müssen Sie in der Console ein Single-Node-System erstellen.

Schritte

1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.
2. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Anweisungen.
3. **Wählen Sie einen Standort**: Wählen Sie **Microsoft Azure** und * Cloud Volumes ONTAP Single Node*.
4. Wenn Sie dazu aufgefordert werden, "Erstellen Sie einen Konsolenagenten" .
5. **Details und Anmeldeinformationen**: Ändern Sie optional die Azure-Anmeldeinformationen und das Abonnement, geben Sie einen Clusternamen an, fügen Sie bei Bedarf Tags hinzu und geben Sie dann die Anmeldeinformationen an.

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

Feld	Beschreibung
Systemname	Die Konsole verwendet den Systemnamen, um sowohl das Cloud Volumes ONTAP -System als auch die virtuelle Azure-Maschine zu benennen. Wenn Sie diese Option auswählen, wird der Name auch als Präfix für die vordefinierte Sicherheitsgruppe verwendet.

Feld	Beschreibung
Ressourcengruppen-Tags	Tags sind Metadaten für Ihre Azure-Ressourcen. Wenn Sie in dieses Feld Tags eingeben, fügt die Konsole sie der Ressourcengruppe hinzu, die mit dem Cloud Volumes ONTAP -System verknüpft ist. Sie können beim Erstellen eines Systems bis zu vier Tags über die Benutzeroberfläche hinzufügen und nach der Erstellung weitere hinzufügen. Beachten Sie, dass die API Sie beim Erstellen eines Systems nicht auf vier Tags beschränkt. Informationen zu Tags finden Sie unter "Microsoft Azure-Dokumentation: Verwenden von Tags zum Organisieren Ihrer Azure-Ressourcen" Die
Benutzername und Passwort	Dies sind die Anmeldeinformationen für das Cloud Volumes ONTAP Clusteradministratorkonto. Sie können diese Anmeldeinformationen verwenden, um über ONTAP System Manager oder die ONTAP CLI eine Verbindung zu Cloud Volumes ONTAP herzustellen. Behalten Sie den Standardbenutzernamen *admin* bei oder ändern Sie ihn in einen benutzerdefinierten Benutzernamen.
Anmeldeinformationen bearbeiten	Sie können für die Verwendung mit diesem Cloud Volumes ONTAP -System andere Azure-Anmeldeinformationen und ein anderes Azure-Abonnement auswählen. Sie müssen dem ausgewählten Azure-Abonnement ein Azure Marketplace-Abonnement zuordnen, um ein Cloud Volumes ONTAP System mit nutzungsbasierter Bezahlung bereitzustellen. "Erfahren Sie, wie Sie Anmeldeinformationen hinzufügen" .

6. **Dienste**: Aktivieren oder deaktivieren Sie die einzelnen Dienste, die Sie mit Cloud Volumes ONTAP verwenden möchten oder nicht.
   - "Erfahren Sie mehr über die NetApp Data Classification"
   - "Erfahren Sie mehr über NetApp Backup and Recovery"

   Wenn Sie WORM und Daten-Tiering nutzen möchten, müssen Sie Backup und Recovery deaktivieren und ein Cloud Volumes ONTAP System mit Version 9.8 oder höher bereitstellen.

7. **Standort**: Wählen Sie eine Region, eine Verfügbarkeitszone, ein VNet und ein Subnetz aus und aktivieren Sie dann das Kontrollkästchen, um die Netzwerkkonnektivität zwischen dem Konsolenagenten und dem Zielstandort zu bestätigen.

   Für Regionen in China werden Einzelknotenbereitstellungen nur in Cloud Volumes ONTAP 9.12.1 GA und 9.13.0 GA unterstützt. Sie können diese Versionen auf neuere Patches und Releases von Cloud Volumes ONTAP aktualisieren, wie"in Azure unterstützt" . Wenn Sie neuere Versionen von Cloud Volumes ONTAP in chinesischen Regionen bereitstellen möchten, wenden Sie sich an den NetApp Support. In den Regionen Chinas werden nur direkt von NetApp erworbene Lizenzen unterstützt, Marktplatz-Abonnements sind nicht verfügbar.

8. **Konnektivität**: Wählen Sie eine neue oder vorhandene Ressourcengruppe und entscheiden Sie dann, ob Sie die vordefinierte Sicherheitsgruppe oder Ihre eigene verwenden möchten.

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

Feld	Beschreibung
Ressourcengruppe	Erstellen Sie eine neue Ressourcengruppe für Cloud Volumes ONTAP oder verwenden Sie eine vorhandene Ressourcengruppe. Die bewährte Methode besteht darin, eine neue, dedizierte Ressourcengruppe für Cloud Volumes ONTAP zu verwenden. Obwohl es möglich ist , Cloud Volumes ONTAP in einer vorhandenen, gemeinsam genutzten Ressourcengruppe bereitzustellen, wird dies aufgrund des Risikos eines Datenverlusts nicht empfohlen. Weitere Einzelheiten finden Sie in der obigen Warnung. Wenn das von Ihnen verwendete Azure-Konto über die "erforderliche Berechtigungen" , entfernt die Konsole Cloud Volumes ONTAP -Ressourcen aus einer Ressourcengruppe, falls die Bereitstellung fehlschlägt oder gelöscht wird.
Generierte Sicherheitsgruppe	Wenn Sie die Sicherheitsgruppe von der Konsole erstellen lassen, müssen Sie auswählen, wie Sie den Datenverkehr zulassen: • Wenn Sie **Nur ausgewähltes VNet** auswählen, ist die Quelle für eingehenden Datenverkehr der Subnetzbereich des ausgewählten VNet und der Subnetzbereich des VNet, in dem sich der Konsolenagent befindet. Dies ist die empfohlene Option. • Wenn Sie **Alle VNets** auswählen, ist die Quelle für eingehenden Datenverkehr der IP-Bereich 0.0.0.0/0.
Vorhandene verwenden	Wenn Sie eine vorhandene Sicherheitsgruppe auswählen, muss diese die Anforderungen von Cloud Volumes ONTAP erfüllen. "Anzeigen der Standardsicherheitsgruppe" .

9. **Abrechnungsmethoden und NSS-Konto**: Geben Sie an, welche Abrechnungsoption Sie mit diesem System verwenden möchten, und geben Sie dann ein NetApp Support Site-Konto an.
   - "Erfahren Sie mehr über die Lizenzierungsoptionen für Cloud Volumes ONTAP" .
   - "Erfahren Sie, wie Sie die Lizenzierung einrichten" .
10. **Vorkonfigurierte Pakete**: Wählen Sie eines der Pakete aus, um schnell ein Cloud Volumes ONTAP System bereitzustellen, oder klicken Sie auf **Meine eigene Konfiguration erstellen**.

    Wenn Sie sich für eines der Pakete entscheiden, müssen Sie lediglich ein Volumen angeben und anschließend die Konfiguration prüfen und freigeben.
11. **Lizenzierung**: Ändern Sie bei Bedarf die Cloud Volumes ONTAP -Version und wählen Sie einen virtuellen Maschinentyp aus.

    Wenn für die ausgewählte Version ein neuerer Release Candidate, eine allgemeine Verfügbarkeit oder ein Patch-Release verfügbar ist, aktualisiert BlueXP das System beim Erstellen der Arbeitsumgebung auf diese Version. Das Update erfolgt beispielsweise, wenn Sie Cloud Volumes ONTAP 9.16.1 P3 auswählen und 9.16.1 P4 verfügbar ist. Das Update erfolgt nicht von einer Version zur nächsten, beispielsweise von 9.15 auf 9.16.
12. **Abonnieren Sie über den Azure Marketplace**: Diese Seite wird Ihnen angezeigt, wenn die Konsole keine programmgesteuerten Bereitstellungen von Cloud Volumes ONTAP aktivieren konnte. Befolgen Sie die auf dem Bildschirm aufgeführten Schritte. Siehe "Programmatische Bereitstellung von Marketplace-Produkten"

für weitere Informationen.

13. **Zugrunde liegende Speicherressourcen**: Wählen Sie Einstellungen für das anfängliche Aggregat: einen Datenträgertyp, eine Größe für jeden Datenträger und ob die Datenaufteilung auf Blob-Speicher aktiviert werden soll.

    Beachten Sie Folgendes:

    - Wenn der öffentliche Zugriff auf Ihr Speicherkonto innerhalb des VNet deaktiviert ist, können Sie das Daten-Tiering in Ihrem Cloud Volumes ONTAP System nicht aktivieren. Weitere Informationen finden Sie unter"Sicherheitsgruppenregeln" .
    - Der Datenträgertyp ist für das ursprüngliche Volume. Sie können für nachfolgende Volumes einen anderen Datenträgertyp auswählen.
    - Die Datenträgergröße gilt für alle Datenträger im anfänglichen Aggregat und für alle zusätzlichen Aggregate, die die Konsole erstellt, wenn Sie die einfache Bereitstellungsoption verwenden. Mithilfe der erweiterten Zuordnungsoption können Sie Aggregate erstellen, die eine andere Festplattengröße verwenden.

      Hilfe zur Auswahl von Datenträgertyp und -größe finden Sie unter"Dimensionierung Ihres Systems in Azure" .
    - Sie können beim Erstellen oder Bearbeiten eines Volumes eine bestimmte Volume-Tiering-Richtlinie auswählen.
    - Wenn Sie das Daten-Tiering deaktivieren, können Sie es für nachfolgende Aggregate aktivieren.

      "Weitere Informationen zum Daten-Tiering" .

14. **Schreibgeschwindigkeit & WORM**:

    a. Wählen Sie bei Bedarf die Schreibgeschwindigkeit **Normal** oder **Hoch**.

       "Erfahren Sie mehr über die Schreibgeschwindigkeit" .

    b. Aktivieren Sie bei Bedarf den WORM-Speicher (Write Once, Read Many).

       Diese Option ist nur für bestimmte VM-Typen verfügbar. Informationen zu den unterstützten VM-Typen finden Sie unter"Unterstützte Konfigurationen nach Lizenz für HA-Paare" .

       WORM kann nicht aktiviert werden, wenn die Datenschichtung für Cloud Volumes ONTAP Version 9.7 und darunter aktiviert wurde. Das Zurücksetzen oder Downgrade auf Cloud Volumes ONTAP 9.8 ist nach der Aktivierung von WORM und Tiering blockiert.

    "Erfahren Sie mehr über WORM-Speicher" .

    a. Wenn Sie den WORM-Speicher aktivieren, wählen Sie die Aufbewahrungsdauer aus.

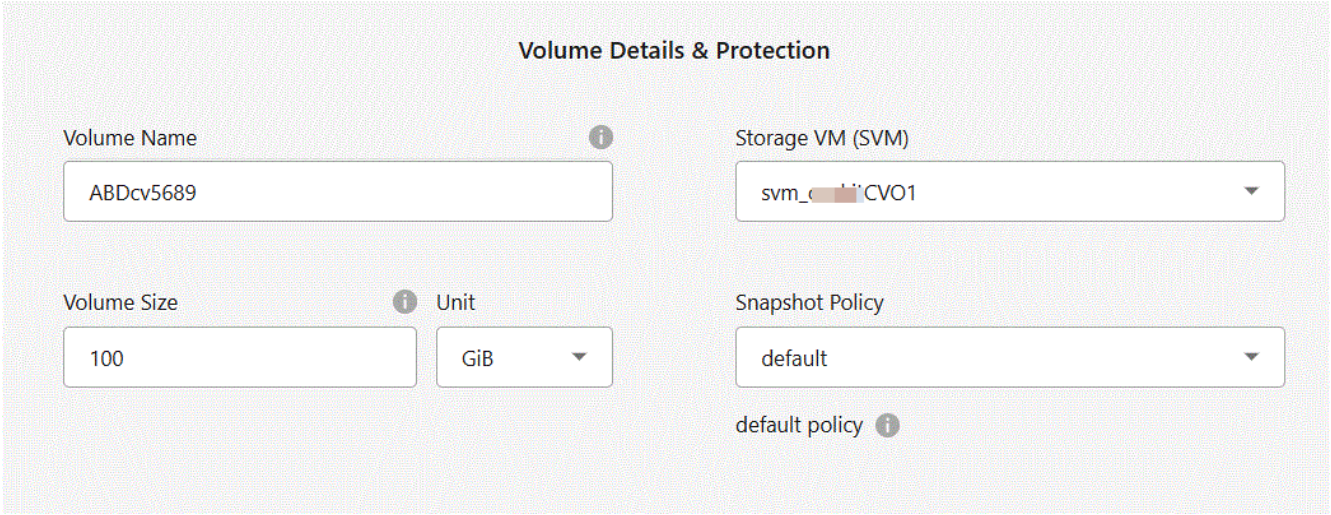
15. **Volume erstellen**: Geben Sie Details für das neue Volume ein oder klicken Sie auf **Überspringen**.

    "Erfahren Sie mehr über unterstützte Clientprotokolle und -versionen" .

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

Feld	Beschreibung
Größe	Die maximale Größe, die Sie eingeben können, hängt weitgehend davon ab, ob Sie Thin Provisioning aktivieren. Dadurch können Sie ein Volume erstellen, das größer ist als der ihm aktuell zur Verfügung stehende physische Speicher.
Zugriffskontrolle (nur für NFS)	Eine Exportrichtlinie definiert die Clients im Subnetz, die auf das Volume zugreifen können. Standardmäßig gibt die Konsole einen Wert ein, der Zugriff auf alle Instanzen im Subnetz gewährt.
Berechtigungen und Benutzer/Gruppen (nur für CIFS)	Mit diesen Feldern können Sie die Zugriffsebene auf eine Freigabe für Benutzer und Gruppen steuern (auch als Zugriffskontrolllisten oder ACLs bezeichnet). Sie können lokale oder Domänen-Windows-Benutzer oder -Gruppen oder UNIX-Benutzer oder -Gruppen angeben. Wenn Sie einen Windows-Domänenbenutzernamen angeben, müssen Sie die Domäne des Benutzers im Format Domäne\Benutzername angeben.
Snapshot-Richtlinie	Eine Snapshot-Kopierrichtlinie gibt die Häufigkeit und Anzahl der automatisch erstellten NetApp Snapshot-Kopien an. Eine NetApp Snapshot-Kopie ist ein zeitpunktbezogenes Dateisystem-Image, das keine Auswirkungen auf die Leistung hat und nur minimalen Speicherplatz benötigt. Sie können die Standardrichtlinie oder keine auswählen. Für vorübergehende Daten können Sie „Keine“ auswählen, beispielsweise „tempdb“ für Microsoft SQL Server.
Erweiterte Optionen (nur für NFS)	Wählen Sie eine NFS-Version für das Volume aus: entweder NFSv3 oder NFSv4.
Initiatorgruppe und IQN (nur für iSCSI)	iSCSI-Speicherziele werden als LUNs (logische Einheiten) bezeichnet und Hosts als Standardblockgeräte präsentiert. Initiatorgruppen sind Tabellen mit iSCSI-Hostknotennamen und steuern, welche Initiatoren Zugriff auf welche LUNs haben. iSCSI-Ziele stellen über Standard-Ethernet-Netzwerkadapter (NICs), TCP-Offload-Engine-Karten (TOE) mit Software-Initiatoren, konvergente Netzwerkadapter (CNAs) oder dedizierte Hostbusadapter (HBAs) eine Verbindung zum Netzwerk her und werden durch iSCSI-qualifizierte Namen (IQNs) identifiziert. Wenn Sie ein iSCSI-Volume erstellen, erstellt die Konsole automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volume erstellt haben, sodass keine Verwaltung erforderlich ist. Nachdem Sie das Volume erstellt haben,"Verwenden Sie den IQN, um von Ihren Hosts aus eine Verbindung zum LUN herzustellen" .

Das folgende Bild zeigt die erste Seite des Assistenten zur Volumeerstellung:



16. **CIFS-Setup**: Wenn Sie das CIFS-Protokoll gewählt haben, richten Sie einen CIFS-Server ein.

Feld	Beschreibung
DNS Primäre und sekundäre IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgelisteten DNS-Server müssen die Service Location Records (SRV) enthalten, die zum Auffinden der Active Directory-LDAP-Server und Domänencontroller für die Domäne erforderlich sind, der der CIFS-Server beitreten wird.
Beitretende Active Directory-Domäne	Der FQDN der Active Directory (AD)-Domäne, der der CIFS-Server beitreten soll.
Anmeldeinformationen, die zum Beitritt zur Domäne berechtigt sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
NetBIOS-Name des CIFS-Servers	Ein CIFS-Servername, der in der AD-Domäne eindeutig ist.
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domäne, die mit dem CIFS-Server verknüpft werden soll. Der Standardwert ist CN=Computers. Um Azure AD Domain Services als AD-Server für Cloud Volumes ONTAP zu konfigurieren, sollten Sie in dieses Feld **OU=AADDC Computers** oder **OU=AADDC Users** eingeben.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure-Dokumentation: Erstellen einer Organisationseinheit (OU) in einer von Azure AD Domain Services verwalteten Domäne"^]
DNS-Domäne	Die DNS-Domäne für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen ist die Domäne dieselbe wie die AD-Domäne.
NTP-Server	Wählen Sie **Active Directory-Domäne verwenden**, um einen NTP-Server mithilfe des Active Directory-DNS zu konfigurieren. Wenn Sie einen NTP-Server mit einer anderen Adresse konfigurieren müssen, sollten Sie die API verwenden. Weitere Informationen finden Sie im "Dokumentation zur NetApp Console" für Details. Beachten Sie, dass Sie einen NTP-Server nur beim Erstellen eines CIFS-Servers konfigurieren können. Es ist nicht mehr konfigurierbar, nachdem Sie den CIFS-Server erstellt haben.

17. **Nutzungsprofil, Datenträgertyp und Tiering-Richtlinie**: Wählen Sie aus, ob Sie Speichereffizienzfunktionen aktivieren möchten, und ändern Sie bei Bedarf die Volume-Tiering-Richtlinie.

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

18. **Überprüfen und 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 den Azure-Ressourcen anzuzeigen, die die Konsole erwerben wird.
    c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.
    d. Klicken Sie auf **Los**.

Ergebnis

Die Konsole stellt das Cloud Volumes ONTAP -System bereit. Sie können den Fortschritt auf der Audit-Seite verfolgen.

Wenn bei der Bereitstellung des Cloud Volumes ONTAP Systems Probleme auftreten, überprüfen Sie die Fehlermeldung. Sie können auch das System auswählen und auf **Umgebung neu erstellen** klicken.

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

Ändern Sie nach Abschluss des Bereitstellungsprozesses nicht die systemgenerierten Cloud Volumes ONTAP Konfigurationen im Azure-Portal, insbesondere nicht die System-Tags. Alle an diesen Konfigurationen vorgenommenen Änderungen können zu unerwartetem Verhalten oder Datenverlust führen.

Nach Abschluss

- Wenn Sie eine CIFS-Freigabe bereitgestellt haben, erteilen Sie Benutzern oder Gruppen Berechtigungen für die Dateien und Ordner und stellen Sie sicher, dass diese Benutzer auf die Freigabe zugreifen und eine Datei erstellen können.
- Wenn Sie Kontingente auf Volumes anwenden möchten, verwenden Sie ONTAP System Manager oder die ONTAP CLI.

  Mithilfe von Kontingenten können Sie den Speicherplatz und die Anzahl der von einem Benutzer, einer Gruppe oder einem Qtree verwendeten Dateien beschränken oder verfolgen.

Starten Sie ein Cloud Volumes ONTAP HA-Paar in Azure

Wenn Sie ein Cloud Volumes ONTAP HA-Paar in Azure starten möchten, müssen Sie in der Konsole ein HA-System erstellen.

Schritte

1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.
2. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Anweisungen.
3. Wenn Sie dazu aufgefordert werden, "Erstellen Sie einen Konsolenagenten" .
4. **Details und Anmeldeinformationen**: Ändern Sie optional die Azure-Anmeldeinformationen und das Abonnement, geben Sie einen Clusternamen an, fügen Sie bei Bedarf Tags hinzu und geben Sie dann die Anmeldeinformationen an.

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

Feld	Beschreibung
Systemname	Die Konsole verwendet den Systemnamen, um sowohl das Cloud Volumes ONTAP -System als auch die virtuelle Azure-Maschine zu benennen. Wenn Sie diese Option auswählen, wird der Name auch als Präfix für die vordefinierte Sicherheitsgruppe verwendet.
Ressourcengruppen-Tags	Tags sind Metadaten für Ihre Azure-Ressourcen. Wenn Sie in dieses Feld Tags eingeben, fügt die Konsole sie der Ressourcengruppe hinzu, die mit dem Cloud Volumes ONTAP -System verknüpft ist. Sie können beim Erstellen eines Systems bis zu vier Tags über die Benutzeroberfläche hinzufügen und nach der Erstellung weitere hinzufügen. Beachten Sie, dass die API Sie beim Erstellen eines Systems nicht auf vier Tags beschränkt. Informationen zu Tags finden Sie unter "Microsoft Azure-Dokumentation: Verwenden von Tags zum Organisieren Ihrer Azure-Ressourcen" Die
Benutzername und Passwort	Dies sind die Anmeldeinformationen für das Cloud Volumes ONTAP Clusteradministratorkonto. Sie können diese Anmeldeinformationen verwenden, um über ONTAP System Manager oder die ONTAP CLI eine Verbindung zu Cloud Volumes ONTAP herzustellen. Behalten Sie den Standardbenutzernamen *admin* bei oder ändern Sie ihn in einen benutzerdefinierten Benutzernamen.
Anmeldeinformationen bearbeiten	Sie können für die Verwendung mit diesem Cloud Volumes ONTAP -System andere Azure-Anmeldeinformationen und ein anderes Azure-Abonnement auswählen. Sie müssen dem ausgewählten Azure-Abonnement ein Azure Marketplace-Abonnement zuordnen, um ein Cloud Volumes ONTAP System mit nutzungsbasierter Bezahlung bereitzustellen. "Erfahren Sie, wie Sie Anmeldeinformationen hinzufügen" .

5. **Dienste**: Aktivieren oder deaktivieren Sie die einzelnen Dienste, je nachdem, ob Sie sie mit Cloud Volumes ONTAP verwenden möchten.
   - "Erfahren Sie mehr über die NetApp Data Classification"
   - "Erfahren Sie mehr über NetApp Backup and Recovery"

   Wenn Sie WORM und Daten-Tiering nutzen möchten, müssen Sie Backup und Recovery deaktivieren und ein Cloud Volumes ONTAP System mit Version 9.8 oder höher bereitstellen.

6. **HA-Bereitstellungsmodelle**:
   a. Wählen Sie **Einzelne Verfügbarkeitszone** oder **Mehrere Verfügbarkeitszonen**.
      - Wählen Sie für einzelne Verfügbarkeitszonen eine Azure-Region, eine Verfügbarkeitszone, ein VNet und ein Subnetz aus.

        Ab Cloud Volumes ONTAP 9.15.1 können Sie VM-Instanzen (Virtual Machine) im HA-Modus in einzelnen Verfügbarkeitszonen (AZs) in Azure bereitstellen. Sie müssen eine Zone und eine Region auswählen, die diese Bereitstellung unterstützen. Wenn die Zone oder Region die zonale Bereitstellung nicht unterstützt, wird der vorherige nicht zonale Bereitstellungsmodus für LRS verwendet. Informationen zu den unterstützten Konfigurationen für gemeinsam genutzte verwaltete Datenträger finden Sie unter"HA-Konfiguration einer einzelnen Verfügbarkeitszone mit gemeinsam genutzten verwalteten Datenträgern" .

      - Wählen Sie für mehrere Verfügbarkeitszonen eine Region, ein VNet, ein Subnetz, eine Zone für

Knoten 1 und eine Zone für Knoten 2 aus.

b. Aktivieren Sie das Kontrollkästchen **Ich habe die Netzwerkkonnektivität überprüft…**.

7. **Konnektivität**: Wählen Sie eine neue oder vorhandene Ressourcengruppe und entscheiden Sie dann, ob Sie die vordefinierte Sicherheitsgruppe oder Ihre eigene verwenden möchten.

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

Feld	Beschreibung
Ressourcengruppe	Erstellen Sie eine neue Ressourcengruppe für Cloud Volumes ONTAP oder verwenden Sie eine vorhandene Ressourcengruppe. Die bewährte Methode besteht darin, eine neue, dedizierte Ressourcengruppe für Cloud Volumes ONTAP zu verwenden. Obwohl es möglich ist , Cloud Volumes ONTAP in einer vorhandenen, gemeinsam genutzten Ressourcengruppe bereitzustellen, wird dies aufgrund des Risikos eines Datenverlusts nicht empfohlen. Weitere Einzelheiten finden Sie in der obigen Warnung. Sie müssen für jedes Cloud Volumes ONTAP HA-Paar, das Sie in Azure bereitstellen, eine dedizierte Ressourcengruppe verwenden. In einer Ressourcengruppe wird nur ein HA-Paar unterstützt. Bei der Konsole treten Verbindungsprobleme auf, wenn Sie versuchen, ein zweites Cloud Volumes ONTAP HA-Paar in einer Azure-Ressourcengruppe bereitzustellen. Wenn das von Ihnen verwendete Azure-Konto über die "erforderliche Berechtigungen" , entfernt die Konsole Cloud Volumes ONTAP -Ressourcen aus einer Ressourcengruppe, falls die Bereitstellung fehlschlägt oder gelöscht wird.
Generierte Sicherheitsgruppe	Wenn Sie die Sicherheitsgruppe von der Konsole erstellen lassen, müssen Sie auswählen, wie Sie den Datenverkehr zulassen: • Wenn Sie **Nur ausgewähltes VNet** auswählen, ist die Quelle für eingehenden Datenverkehr der Subnetzbereich des ausgewählten VNet und der Subnetzbereich des VNet, in dem sich der Konsolenagent befindet. Dies ist die empfohlene Option. • Wenn Sie **Alle VNets** auswählen, ist die Quelle für eingehenden Datenverkehr der IP-Bereich 0.0.0.0/0.
Vorhandene verwenden	Wenn Sie eine vorhandene Sicherheitsgruppe auswählen, muss diese die Anforderungen von Cloud Volumes ONTAP erfüllen. "Anzeigen der Standardsicherheitsgruppe" .

8. **Abrechnungsmethoden und NSS-Konto**: Geben Sie an, welche Abrechnungsoption Sie mit diesem System verwenden möchten, und geben Sie dann ein NetApp Support Site-Konto an.
   - "Erfahren Sie mehr über die Lizenzierungsoptionen für Cloud Volumes ONTAP" .
   - "Erfahren Sie, wie Sie die Lizenzierung einrichten" .
9. **Vorkonfigurierte Pakete**: Wählen Sie eines der Pakete aus, um schnell ein Cloud Volumes ONTAP System bereitzustellen, oder klicken Sie auf **Konfiguration ändern**.

   Wenn Sie sich für eines der Pakete entscheiden, müssen Sie lediglich ein Volumen angeben und

anschließend die Konfiguration prüfen und freigeben.

10. **Lizenzierung**: Ändern Sie die Cloud Volumes ONTAP -Version nach Bedarf und wählen Sie einen virtuellen Maschinentyp aus.

    Wenn für die ausgewählte Version ein neuerer Release Candidate, eine allgemeine Verfügbarkeit oder ein Patch-Release verfügbar ist, aktualisiert die Konsole das System beim Erstellen auf diese Version. Das Update erfolgt beispielsweise, wenn Sie Cloud Volumes ONTAP 9.13.1 auswählen und 9.13.1 P4 verfügbar ist. Das Update erfolgt nicht von einer Version zur nächsten, beispielsweise von 9.13 auf 9.14.

11. **Abonnieren Sie über den Azure Marketplace**: Befolgen Sie die Schritte, wenn die Konsole keine programmgesteuerten Bereitstellungen von Cloud Volumes ONTAP aktivieren konnte.
12. **Zugrunde liegende Speicherressourcen**: Wählen Sie Einstellungen für das anfängliche Aggregat: einen Datenträgertyp, eine Größe für jeden Datenträger und ob die Datenaufteilung auf Blob-Speicher aktiviert werden soll.

    Beachten Sie Folgendes:

    - Die Datenträgergröße gilt für alle Datenträger im anfänglichen Aggregat und für alle zusätzlichen Aggregate, die die Konsole erstellt, wenn Sie die einfache Bereitstellungsoption verwenden. Mithilfe der erweiterten Zuordnungsoption können Sie Aggregate erstellen, die eine andere Festplattengröße verwenden.

      Hilfe zur Auswahl einer Festplattengröße finden Sie unter"Dimensionieren Sie Ihr System in Azure" .

    - Wenn der öffentliche Zugriff auf Ihr Speicherkonto innerhalb des VNet deaktiviert ist, können Sie das Daten-Tiering in Ihrem Cloud Volumes ONTAP System nicht aktivieren. Weitere Informationen finden Sie unter"Sicherheitsgruppenregeln" .
    - Sie können beim Erstellen oder Bearbeiten eines Volumes eine bestimmte Volume-Tiering-Richtlinie auswählen.
    - Wenn Sie das Daten-Tiering deaktivieren, können Sie es für nachfolgende Aggregate aktivieren.

      "Weitere Informationen zum Daten-Tiering" .

    - Ab Cloud Volumes ONTAP 9.15.0P1 werden Azure-Seitenblobs für neue Bereitstellungen mit Hochverfügbarkeitspaaren nicht mehr unterstützt. Wenn Sie derzeit Azure-Seitenblobs in vorhandenen Bereitstellungen mit Hochverfügbarkeitspaaren verwenden, können Sie in den VMs der Edsv4- und Edsv5-Serie zu neueren VM-Instanztypen migrieren.

      "Erfahren Sie mehr über unterstützte Konfigurationen in Azure" .

13. **Schreibgeschwindigkeit & WORM**:

    a. Wählen Sie bei Bedarf die Schreibgeschwindigkeit **Normal** oder **Hoch**.

       "Erfahren Sie mehr über die Schreibgeschwindigkeit" .

    b. Aktivieren Sie bei Bedarf den WORM-Speicher (Write Once, Read Many).

       Diese Option ist nur für bestimmte VM-Typen verfügbar. Informationen zu den unterstützten VM-Typen finden Sie unter"Unterstützte Konfigurationen nach Lizenz für HA-Paare" .

       WORM kann nicht aktiviert werden, wenn die Datenschichtung für Cloud Volumes ONTAP Version 9.7

und darunter aktiviert wurde. Das Zurücksetzen oder Downgrade auf Cloud Volumes ONTAP 9.8 ist nach der Aktivierung von WORM und Tiering blockiert.

"Erfahren Sie mehr über WORM-Speicher" .

a. Wenn Sie den WORM-Speicher aktivieren, wählen Sie die Aufbewahrungsdauer aus.

14. **Sichere Kommunikation mit Speicher und WORM**: Wählen Sie, ob eine HTTPS-Verbindung zu Azure-Speicherkonten aktiviert werden soll, und aktivieren Sie bei Bedarf den WORM-Speicher (Write Once, Read Many).

    Die HTTPS-Verbindung besteht von einem Cloud Volumes ONTAP 9.7 HA-Paar zu Azure Page Blob Storage-Konten. Beachten Sie, dass das Aktivieren dieser Option die Schreibleistung beeinträchtigen kann. Sie können die Einstellung nicht mehr ändern, nachdem Sie das System erstellt haben.

    "Erfahren Sie mehr über WORM-Speicher" .

    WORM kann nicht aktiviert werden, wenn die Datenschichtung aktiviert wurde.

    "Erfahren Sie mehr über WORM-Speicher" .

15. **Volume erstellen**: Geben Sie Details für das neue Volume ein oder klicken Sie auf **Überspringen**.

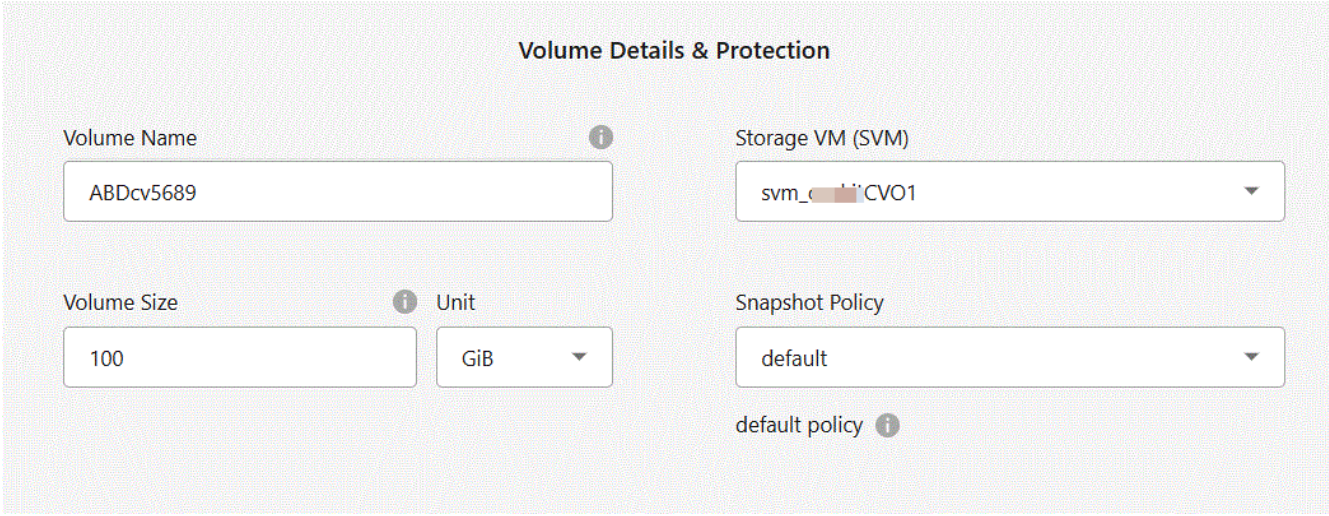
    "Erfahren Sie mehr über unterstützte Clientprotokolle und -versionen" .

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

Feld	Beschreibung
Größe	Die maximale Größe, die Sie eingeben können, hängt weitgehend davon ab, ob Sie Thin Provisioning aktivieren. Dadurch können Sie ein Volume erstellen, das größer ist als der ihm aktuell zur Verfügung stehende physische Speicher.
Zugriffskontrolle (nur für NFS)	Eine Exportrichtlinie definiert die Clients im Subnetz, die auf das Volume zugreifen können. Standardmäßig gibt die Konsole einen Wert ein, der Zugriff auf alle Instanzen im Subnetz gewährt.
Berechtigungen und Benutzer/Gruppen (nur für CIFS)	Mit diesen Feldern können Sie die Zugriffsebene auf eine Freigabe für Benutzer und Gruppen steuern (auch als Zugriffskontrolllisten oder ACLs bezeichnet). Sie können lokale oder Domänen-Windows-Benutzer oder -Gruppen oder UNIX-Benutzer oder -Gruppen angeben. Wenn Sie einen Windows-Domänenbenutzernamen angeben, müssen Sie die Domäne des Benutzers im Format Domäne\Benutzername angeben.
Snapshot-Richtlinie	Eine Snapshot-Kopierrichtlinie gibt die Häufigkeit und Anzahl der automatisch erstellten NetApp Snapshot-Kopien an. Eine NetApp Snapshot-Kopie ist ein zeitpunktbezogenes Dateisystem-Image, das keine Auswirkungen auf die Leistung hat und nur minimalen Speicherplatz benötigt. Sie können die Standardrichtlinie oder keine auswählen. Für vorübergehende Daten können Sie „Keine“ auswählen, beispielsweise „tempdb“ für Microsoft SQL Server.
Erweiterte Optionen (nur für NFS)	Wählen Sie eine NFS-Version für das Volume aus: entweder NFSv3 oder NFSv4.

Feld	Beschreibung
Initiatorgruppe und IQN (nur für iSCSI)	iSCSI-Speicherziele werden als LUNs (logische Einheiten) bezeichnet und Hosts als Standardblockgeräte präsentiert. Initiatorgruppen sind Tabellen mit iSCSI-Hostknotennamen und steuern, welche Initiatoren Zugriff auf welche LUNs haben. iSCSI-Ziele stellen über Standard-Ethernet-Netzwerkadapter (NICs), TCP-Offload-Engine-Karten (TOE) mit Software-Initiatoren, konvergente Netzwerkadapter (CNAs) oder dedizierte Hostbusadapter (HBAs) eine Verbindung zum Netzwerk her und werden durch iSCSI-qualifizierte Namen (IQNs) identifiziert. Wenn Sie ein iSCSI-Volume erstellen, erstellt die Konsole automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volume erstellt haben, sodass keine Verwaltung erforderlich ist. Nachdem Sie das Volume erstellt haben,"Verwenden Sie den IQN, um von Ihren Hosts aus eine Verbindung zum LUN herzustellen" .

Das folgende Bild zeigt die erste Seite des Assistenten zur Volumeerstellung:



16. **CIFS-Setup**: Wenn Sie das CIFS-Protokoll gewählt haben, richten Sie einen CIFS-Server ein.

Feld	Beschreibung
DNS Primäre und sekundäre IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgelisteten DNS-Server müssen die Service Location Records (SRV) enthalten, die zum Auffinden der Active Directory-LDAP-Server und Domänencontroller für die Domäne erforderlich sind, der der CIFS-Server beitreten wird.
Beitretende Active Directory-Domäne	Der FQDN der Active Directory (AD)-Domäne, der der CIFS-Server beitreten soll.
Anmeldeinformationen, die zum Beitritt zur Domäne berechtigt sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
NetBIOS-Name des CIFS-Servers	Ein CIFS-Servername, der in der AD-Domäne eindeutig ist.

Feld	Beschreibung
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domäne, die mit dem CIFS-Server verknüpft werden soll. Der Standardwert ist CN=Computers. Um Azure AD Domain Services als AD-Server für Cloud Volumes ONTAP zu konfigurieren, sollten Sie in dieses Feld **OU=AADDC Computers** oder **OU=AADDC Users** eingeben.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure-Dokumentation: Erstellen einer Organisationseinheit (OU) in einer von Azure AD Domain Services verwalteten Domäne"^]
DNS-Domäne	Die DNS-Domäne für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen ist die Domäne dieselbe wie die AD-Domäne.
NTP-Server	Wählen Sie **Active Directory-Domäne verwenden**, um einen NTP-Server mithilfe des Active Directory-DNS zu konfigurieren. Wenn Sie einen NTP-Server mit einer anderen Adresse konfigurieren müssen, sollten Sie die API verwenden. Weitere Informationen finden Sie im "Dokumentation zur NetApp Console" für Details. Beachten Sie, dass Sie einen NTP-Server nur beim Erstellen eines CIFS-Servers konfigurieren können. Es ist nicht mehr konfigurierbar, nachdem Sie den CIFS-Server erstellt haben.

17. **Nutzungsprofil, Datenträgertyp und Tiering-Richtlinie**: Wählen Sie aus, ob Sie Speichereffizienzfunktionen aktivieren möchten, und ändern Sie bei Bedarf die Volume-Tiering-Richtlinie.

    Weitere Informationen finden Sie unter"Auswählen eines Volume-Nutzungsprofils" ,"Übersicht über Data Tiering" , Und "KB: Welche Inline-Speichereffizienzfunktionen werden mit CVO unterstützt?"

18. **Überprüfen und 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 den Azure-Ressourcen anzuzeigen, die die Konsole erwerben wird.
    c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.
    d. Klicken Sie auf **Los**.

Ergebnis

Die Konsole stellt das Cloud Volumes ONTAP -System bereit. Sie können den Fortschritt auf der Audit-Seite verfolgen.

Wenn bei der Bereitstellung des Cloud Volumes ONTAP Systems Probleme auftreten, überprüfen Sie die Fehlermeldung. Sie können auch das System auswählen und auf **Umgebung neu erstellen** klicken.

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

Nach Abschluss

- Wenn Sie eine CIFS-Freigabe bereitgestellt haben, erteilen Sie Benutzern oder Gruppen Berechtigungen für die Dateien und Ordner und stellen Sie sicher, dass diese Benutzer auf die Freigabe zugreifen und eine Datei erstellen können.
- Wenn Sie Kontingente auf Volumes anwenden möchten, verwenden Sie ONTAP System Manager oder die ONTAP CLI.

  Mithilfe von Kontingenten können Sie den Speicherplatz und die Anzahl der von einem Benutzer, einer Gruppe oder einem Qtree verwendeten Dateien beschränken oder verfolgen.

Ändern Sie nach Abschluss des Bereitstellungsprozesses nicht die systemgenerierten Cloud Volumes ONTAP Konfigurationen im Azure-Portal, insbesondere nicht die System-Tags. Alle an diesen Konfigurationen vorgenommenen Änderungen können zu unerwartetem Verhalten oder Datenverlust führen.

Weiterführende Links

*"Planen Ihrer Cloud Volumes ONTAP -Konfiguration in Azure" *"Stellen Sie Cloud Volumes ONTAP in Azure über den Azure Marketplace bereit"

Überprüfen des Azure-Plattformimages

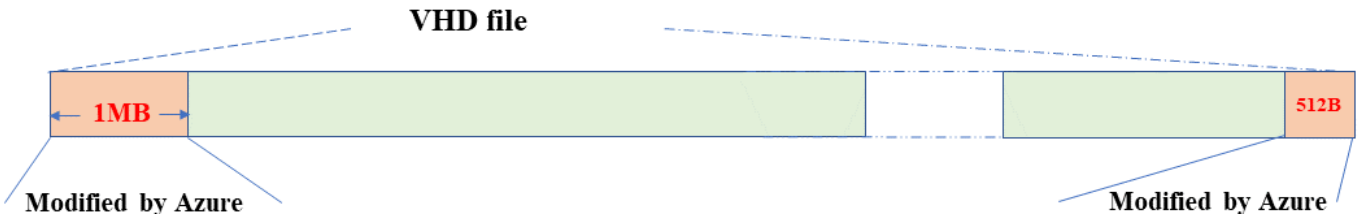
Azure Marketplace-Imageüberprüfung für Cloud Volumes ONTAP

Die Azure-Image-Verifizierung entspricht den erweiterten Sicherheitsanforderungen von NetApp . Das Überprüfen einer Bilddatei ist ein unkomplizierter Vorgang. Allerdings erfordert die Überprüfung der Azure-Image-Signatur besondere Überlegungen für die Azure-VHD-Image-Datei, da diese im Azure Marketplace geändert wird.

Die Azure-Image-Verifizierung wird auf Cloud Volumes ONTAP 9.15.0 und höher unterstützt.

Azures Änderung veröffentlichter VHD-Dateien

Die 1 MB (1048576 Bytes) am Anfang und 512 Bytes am Ende der VHD-Datei werden von Azure geändert. NetApp signiert die verbleibende VHD-Datei.



Im Beispiel ist die VHD-Datei 10 GB groß. Der von NetApp signierte Teil ist grün markiert (10 GB – 1 MB – 512 Byte).

Weiterführende Links

- "Seitenfehler-Blog: So signieren und verifizieren Sie mit OpenSSL"
- "Verwenden Sie das Azure Marketplace-Image, um ein VM-Image für Ihre Azure Stack Edge Pro-GPU zu erstellen | Microsoft Learn"
- "Exportieren/Kopieren eines verwalteten Datenträgers in ein Speicherkonto mithilfe der Azure CLI | Microsoft Learn"
- "Schnellstart für Azure Cloud Shell – Bash | Microsoft Learn"
- "So installieren Sie die Azure CLI | Microsoft Learn"
- "az storage blob copy | Microsoft Learn"
- "Mit Azure CLI Sign in – Anmeldung und Authentifizierung | Microsoft Learn"

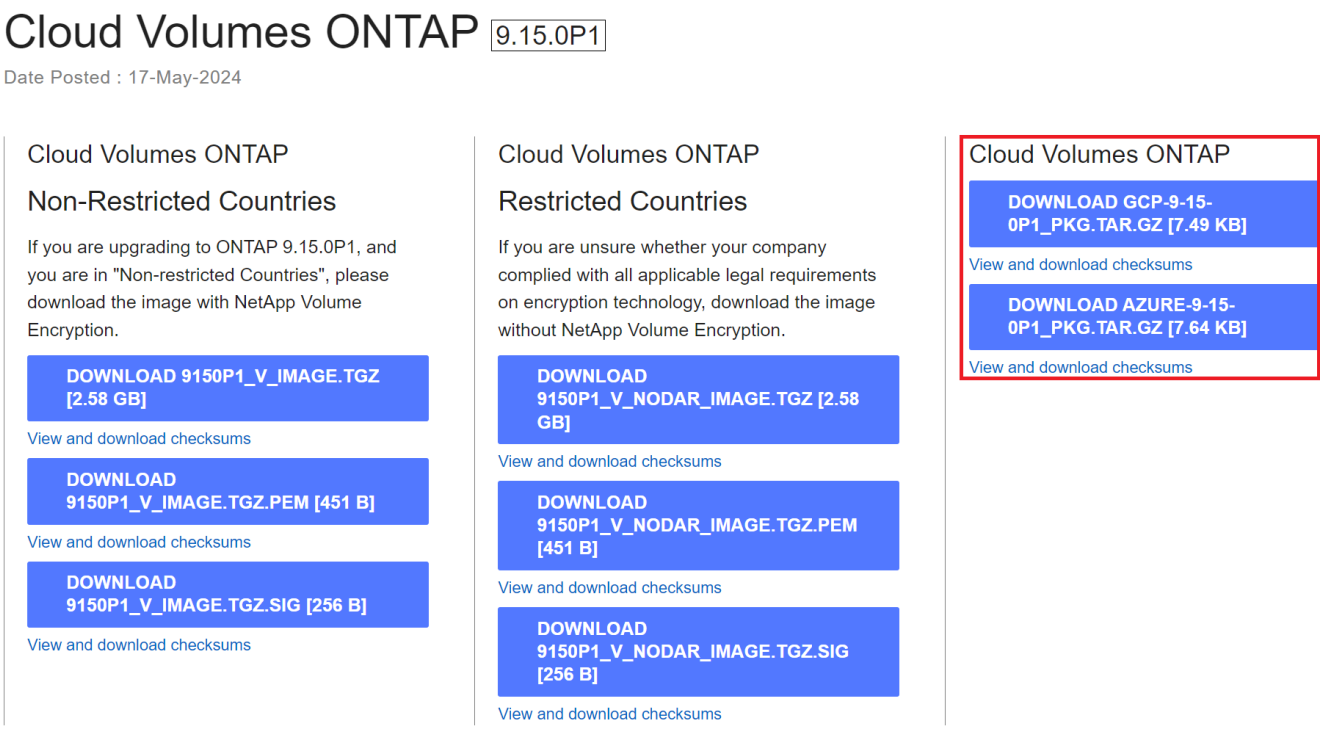
Laden Sie die Azure-Image-Datei für Cloud Volumes ONTAP herunter

Sie können die Azure-Imagedatei von der "NetApp Support Site" .

Die Datei *tar.gz* enthält die für die Bildsignaturüberprüfung erforderlichen Dateien. Zusammen mit der *tar.gz* -Datei sollten Sie auch die *Prüfsummen*-Datei für das Image herunterladen. Die Prüfsummendatei enthält die `md5` Und `sha256` Prüfsummen der *tar.gz*-Datei.

Schritte

1. Gehen Sie zum "Cloud Volumes ONTAP Produktseite auf der NetApp Support-Site" und laden Sie die erforderliche Softwareversion aus dem Bereich **Downloads** herunter.
2. Klicken Sie auf der Downloadseite von Cloud Volumes ONTAP auf die herunterladbare Datei für das Azure-Image und laden Sie die Datei *tar.gz* herunter.



3. Führen Sie unter Linux Folgendes aus: `md5sum AZURE-<version>_PKG.TAR.GZ` .

   Führen Sie unter macOS Folgendes aus: `sha256sum AZURE-<version>_PKG.TAR.GZ` .

4. Überprüfen Sie, ob die `md5sum` Und `sha256sum` Die Werte stimmen mit denen im heruntergeladenen Azure-Image überein.
5. Extrahieren Sie unter Linux und macOS die Datei *tar.gz* mit dem `tar -xzf` Befehl.

   Die extrahierte *tar.gz*-Datei enthält die Digest-Datei (*.sig*), die Datei mit dem öffentlichen Schlüsselzertifikat (*.pem*) und die Datei mit dem Kettenzertifikat (*.pem*).

   Beispielausgabe nach dem Extrahieren der tar.gz-Datei:

```
$ ls cert/ -l
-rw-r----- 1 netapp netapp  384 May  13 13:00 9.15.0P1_azure_digest.sig
-rw-r----- 1 netapp netapp 2365 May  13 13:00 Certificate-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 Certificate-Chain-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 version_readme
```

Exportieren Sie VHD-Images für Cloud Volumes ONTAP aus dem Azure Marketplace

Sobald das VHD-Image in der Azure-Cloud veröffentlicht ist, wird es nicht mehr von NetApp verwaltet. Stattdessen wird das veröffentlichte Image auf dem Azure-Marktplatz platziert. Wenn das Image bereitgestellt und im Azure Marketplace veröffentlicht wird, ändert Azure 1 MB am Anfang und 512 Byte am Ende der VHD. Um die Signatur der VHD-Datei zu überprüfen, müssen Sie das von Azure geänderte VHD-Image aus dem Azure Marketplace exportieren.

Bevor Sie beginnen

Stellen Sie sicher, dass die Azure CLI auf Ihrem System installiert ist oder die Azure Cloud Shell über das Azure-Portal verfügbar ist. Weitere Informationen zur Installation der Azure CLI finden Sie im "Microsoft-Dokumentation: So installieren Sie die Azure CLI" .

Schritte

1. Ordnen Sie die Cloud Volumes ONTAP -Version auf Ihrem System der Image-Version des Azure Marketplace zu, indem Sie den Inhalt der Datei *version_readme* verwenden. Die Cloud Volumes ONTAP -Version wird repräsentiert durch `buildname` und die Azure Marketplace-Imageversion wird dargestellt durch `version` in den Versionszuordnungen.

   Im folgenden Beispiel wird die Cloud Volumes ONTAP -Version `9.15.0P1` ist der Azure Marketplace-Imageversion zugeordnet `9150.01000024.05090105` . Diese Azure Marketplace-Imageversion wird später zum Festlegen der Image-URN verwendet.

   ```
   [
    "buildname": "9.15.0P1",
       "publisher": "netapp",
        "version": "9150.01000024.05090105"

   ]
   ```

2. Identifizieren Sie die Region, in der Sie die VMs erstellen möchten. Der Regionsname wird als Wert für die `locName` Variable beim Festlegen der URN des Marktplatzbilds. Führen Sie diesen Befehl aus, um die verfügbaren Regionen aufzulisten:

   ```
   az account list-locations -o table
   ```

In dieser Tabelle erscheint der Regionsname in der `Name` Feld.

```
$ az account list-locations -o table
DisplayName               Name                 RegionalDisplayName
------------------------  -------------------
-------------------------------------
East US                   eastus               (US) East US
East US 2                 eastus2              (US) East US 2
South Central US          southcentralus       (US) South Central US
...
```

3. Überprüfen Sie die SKU-Namen für die entsprechenden Cloud Volumes ONTAP Versionen und VM-Bereitstellungstypen in der folgenden Tabelle. Der SKU-Name wird als Wert für die `skuName` Variable beim Festlegen der URN des Marktplatzbilds.

   Beispielsweise sollten alle Einzelknotenbereitstellungen mit Cloud Volumes ONTAP 9.15.0 `ontap_cloud_byol` als SKU-Name.

* Cloud Volumes ONTAP Version*	**VM-Bereitstellung durch**	**SKU-Name**
9.17.1 und höher	Der Azure Marketplace	ontap_cloud_direct_gen2
9.17.1 und höher	Die NetApp Console	ontap_cloud_gen2
9.16.1	Der Azure Marketplace	ontap_cloud_direct
9.16.1	Die Konsole	ontap_cloud
9.15.1	Die Konsole	ontap_cloud
9.15.0	Die Konsole, Einzelknotenbereitstellungen	ontap_cloud_byol
9.15.0	Die Konsole, Hochverfügbarkeitsbereitstellungen (HA)	ontap_cloud_byol_ha

4. Nachdem Sie die ONTAP -Version und das Azure Marketplace-Image zugeordnet haben, exportieren Sie die VHD-Datei mithilfe der Azure Cloud Shell oder der Azure CLI aus dem Azure Marketplace.

Exportieren einer VHD-Datei mit Azure Cloud Shell unter Linux

Exportieren Sie aus Azure Cloud Shell das Marketplace-Image in die VHD-Datei (z. B. *9150.01000024.05090105.vhd*) und laden Sie es auf Ihr lokales Linux-System herunter. Führen Sie diese Schritte aus, um das VHD-Image vom Azure Marketplace abzurufen.

Schritte

1. Legen Sie die URN und andere Parameter des Marktplatzbilds fest. Das URN-Format ist `<publisher>:<offer>:<sku>:<version>` . Optional können Sie NetApp Marketplace-Images auflisten, um die richtige Image-Version zu bestätigen.

```
PS /home/user1> $urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
PS /home/user1> $locName="eastus2"
PS /home/user1> $pubName="netapp"
PS /home/user1> $offerName="netapp-ontap-cloud"
PS /home/user1> $skuName="ontap_cloud_byol"
PS /home/user1> Get-AzVMImage -Location $locName -PublisherName $pubName
-Offer $offerName -Sku $skuName |select version
...
141.20231128
9.141.20240131
9.150.20240213
9150.01000024.05090105
...
```

2. Erstellen Sie einen neuen verwalteten Datenträger aus dem Marketplace-Image mit der passenden Imageversion:

```
PS /home/user1> $diskName = "9150.01000024.05090105-managed-disk"
PS /home/user1> $diskRG = "fnf1"
PS /home/user1> az disk create -g $diskRG -n $diskName --image-reference
$urn
PS /home/user1> $sas = az disk grant-access --duration-in-seconds 3600
--access-level Read --name $diskName --resource-group $diskRG
PS /home/user1> $diskAccessSAS = ($sas | ConvertFrom-Json)[0].accessSas
```

3. Exportieren Sie die VHD-Datei vom verwalteten Datenträger in Azure Storage. Erstellen Sie einen Container mit der entsprechenden Zugriffsebene. In diesem Beispiel haben wir einen Container namens `vm-images` mit `Container` Zugriffsebene. Rufen Sie den Zugriffsschlüssel für das Speicherkonto aus dem Azure-Portal ab: **Speicherkonten > *Beispielname* > Zugriffsschlüssel > *Schlüssel1* > *Schlüssel* > Anzeigen > <*Kopie*>**

```
PS /home/user1> $storageAccountName = “examplesaname”
PS /home/user1> $containerName = “vm-images”
PS /home/user1> $storageAccountKey = "<replace with the above access
key>"
PS /home/user1> $destBlobName = “9150.01000024.05090105.vhd”
PS /home/user1> $destContext = New-AzureStorageContext
-StorageAccountName $storageAccountName -StorageAccountKey
$storageAccountKey
PS /home/user1> Start-AzureStorageBlobCopy -AbsoluteUri $diskAccessSAS
-DestContainer $containerName -DestContext $destContext -DestBlob
$destBlobName
PS /home/user1> Get-AzureStorageBlobCopyState –Container $containerName
–Context $destContext -Blob $destBlobName
```

4. Laden Sie das generierte Image auf Ihr Linux-System herunter. Verwenden Sie die `wget` Befehl zum Herunterladen der VHD-Datei:

```
wget <URL of filename/Containers/vm-images/9150.01000024.05090105.vhd>
```

Die URL folgt einem Standardformat. Zur Automatisierung können Sie die URL-Zeichenfolge wie unten gezeigt ableiten. Alternativ können Sie die Azure CLI verwenden `az` Befehl, um die URL abzurufen. Beispiel-URL:https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

5. Bereinigen des verwalteten Datenträgers

```
PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG -DiskName
$diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName
```

Exportieren einer VHD-Datei mit der Azure CLI unter Linux

Exportieren Sie das Marktplatz-Image mithilfe der Azure CLI von einem lokalen Linux-System in eine VHD-Datei.

Schritte

1. Melden Sie sich bei der Azure CLI an und listen Sie Marketplace-Images auf:

```
% az login --use-device-code
```

2. Um sich anzumelden, öffnen Sie die Seite in einem Webbrowser https://microsoft.com/devicelogin und geben Sie den Authentifizierungscode ein.

```
% az vm image list --all --publisher netapp --offer netapp-ontap-cloud
--sku ontap_cloud_byol
...
{
"architecture": "x64",
"offer": "netapp-ontap-cloud",
"publisher": "netapp",
"sku": "ontap_cloud_byol",
"urn": "netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105",
"version": "9150.01000024.05090105"
},
...
```

3. Erstellen Sie einen neuen verwalteten Datenträger aus dem Marketplace-Image mit der passenden Image-Version.

```
% export urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
% export diskName="9150.01000024.05090105-managed-disk"
% export diskRG="new_rg_your_rg"
% az disk create -g $diskRG -n $diskName --image-reference $urn
% az disk grant-access --duration-in-seconds 3600 --access-level Read
--name $diskName --resource-group $diskRG
{
  "accessSas": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
}
% export diskAccessSAS="https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
```

Um den Prozess zu automatisieren, muss das SAS aus der Standardausgabe extrahiert werden. Anleitungen finden Sie in den entsprechenden Dokumenten.

4. Exportieren Sie die VHD-Datei vom verwalteten Datenträger.

   a. Erstellen Sie einen Container mit der entsprechenden Zugriffsebene. In diesem Beispiel wird ein Container mit dem Namen `vm-images` mit `Container` Zugriffsebene verwendet wird.

   b. Rufen Sie den Zugriffsschlüssel für das Speicherkonto aus dem Azure-Portal ab: **Speicherkonten > *Beispielname* > Zugriffsschlüssel > *Schlüssel1* > *Schlüssel* > Anzeigen > <*Kopie*>**

      Sie können auch die `az` Befehl für diesen Schritt.

```
% export storageAccountName="examplesaname"
% export containerName="vm-images"
% export storageAccountKey="xxxxxxxxxx"
% export destBlobName="9150.01000024.05090105.vhd"

% az storage blob copy start --source-uri $diskAccessSAS --destination
-container $containerName --account-name $storageAccountName --account
-key $storageAccountKey --destination-blob $destBlobName

{
  "client_request_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_status": "pending",
  "date": "2022-11-02T22:02:38+00:00",
  "etag": "\"0xXXXXXXXXXXXXXXXX\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}
```

5. Überprüfen Sie den Status der Blobkopie.

```
% az storage blob show --name $destBlobName --container-name
$containerName --account-name $storageAccountName

....
    "copy": {
      "completionTime": null,
      "destinationSnapshot": null,
      "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxx",
      "incrementalCopy": null,
      "progress": "10737418752/10737418752",
      "source": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
      "status": "success",
      "statusDescription": null
    },
....
```

6. Laden Sie das generierte Image auf Ihren Linux-Server herunter.

```
wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>
```

Die URL folgt einem Standardformat. Zur Automatisierung können Sie die URL-Zeichenfolge wie unten gezeigt ableiten. Alternativ können Sie die Azure CLI verwenden `az` Befehl, um die URL abzurufen. Beispiel-URL:https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

7. Bereinigen des verwalteten Datenträgers

```
az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes
```

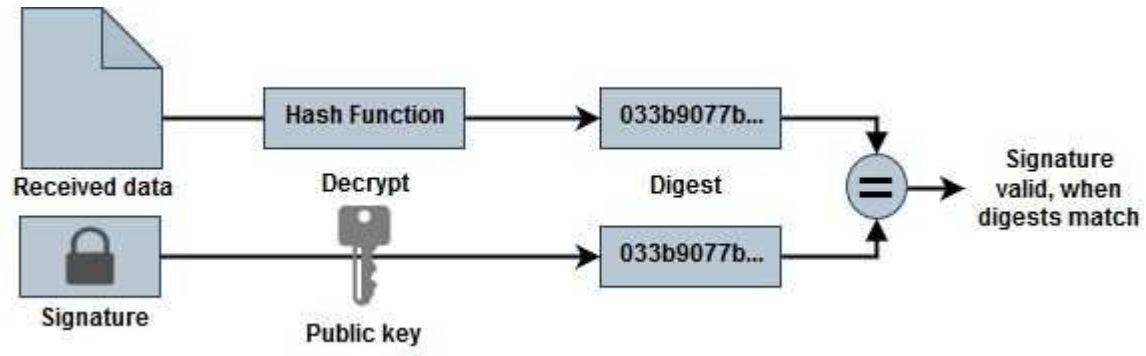
Dateisignatur überprüfen

Azure Marketplace-Imagesignaturüberprüfung für Cloud Volumes ONTAP

Der Azure-Imageüberprüfungsprozess generiert eine Digest-Datei aus der VHD-Datei, indem er am Anfang 1 MB und am Ende 512 Byte entfernt und dann eine Hash-Funktion anwendet. Um dem Signaturverfahren zu entsprechen, wird *sha256* zum Hashing verwendet.

Zusammenfassung des Workflows zur Dateisignaturüberprüfung

Nachfolgend finden Sie eine Übersicht über den Workflow-Prozess zur Dateisignaturüberprüfung.



- Herunterladen des Azure-Images von der "NetApp Support Site" und Extrahieren der Digest-Datei (.sig), der Public-Key-Zertifikatdatei (.pem) und der Kettenzertifikatdatei (.pem). Weitere Informationen finden Sie unter "Herunterladen der Azure-Image-Digest-Datei" für weitere Informationen.
- Überprüfung der Vertrauenskette.
- Extrahieren des öffentlichen Schlüssels (.pub) aus dem öffentlichen Schlüsselzertifikat (.pem).
- Entschlüsseln der Digest-Datei mithilfe des extrahierten öffentlichen Schlüssels.
- Vergleichen Sie das Ergebnis mit einem neu generierten Digest einer temporären Datei, die aus der Bilddatei erstellt wurde, nachdem 1 MB am Anfang und 512 Byte am Ende entfernt wurden. Dieser Schritt wird mithilfe des OpenSSL-Befehlszeilentools ausgeführt. Das OpenSSL-CLI-Tool zeigt eine entsprechende Meldung an, wenn die Zuordnung der Dateien erfolgreich war oder fehlgeschlagen ist.

```
openssl dgst -verify <public_key> -keyform <form> <hash_function>
-signature <digest_file> -binary <temporary_file>
```

Überprüfen der Azure Marketplace-Imagesignatur für Cloud Volumes ONTAP unter Linux

Die Überprüfung der Signatur einer exportierten VHD-Datei unter Linux umfasst die Validierung der Vertrauenskette, die Bearbeitung der Datei und die Überprüfung der Signatur.

Schritte

1. Laden Sie die Azure-Imagedatei von der "NetApp Support Site" und extrahieren Sie die Digest-Datei (.sig), die Public-Key-Zertifikatdatei (.pem) und die Kettenzertifikatdatei (.pem).

   Siehe "Herunterladen der Azure-Image-Digest-Datei" für weitere Informationen.

2. Überprüfen Sie die Vertrauenskette.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. Entfernen Sie 1 MB (1.048.576 Bytes) am Anfang und 512 Bytes am Ende der VHD-Datei. Bei der Verwendung `tail` , Die `-c +K` Option generiert Bytes aus dem K-ten Byte der Datei. Daher geht es 1048577 an `tail -c` .

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. Verwenden Sie OpenSSL, um den öffentlichen Schlüssel aus dem Zertifikat zu extrahieren und die extrahierte Datei (sign.tmp) mit der Signaturdatei und dem öffentlichen Schlüssel zu überprüfen.

   Die Eingabeaufforderung zeigt Meldungen an, die den Erfolg oder Misserfolg der Überprüfung basierend auf deren Erfolg anzeigen.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verification OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. Räumen Sie den Arbeitsbereich auf.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

Überprüfen der Azure Marketplace-Imagesignatur für Cloud Volumes ONTAP unter macOS

Die Überprüfung der Signatur einer exportierten VHD-Datei unter Linux umfasst die Validierung der Vertrauenskette, die Bearbeitung der Datei und die Überprüfung der Signatur.

Schritte

1. Laden Sie die Azure-Imagedatei von der "NetApp Support Site" und extrahieren Sie die Digest-Datei (.sig), die Public-Key-Zertifikatdatei (.pem) und die Kettenzertifikatdatei (.pem).

   Siehe "Herunterladen der Azure-Image-Digest-Datei" für weitere Informationen.

2. Überprüfen Sie die Vertrauenskette.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. Entfernen Sie 1 MB (1.048.576 Bytes) am Anfang und 512 Bytes am Ende der VHD-Datei. Bei der Verwendung `tail` , Die `-c +K` Option generiert Bytes aus dem K-ten Byte der Datei. Daher geht es 1048577 an `tail -c` . Beachten Sie, dass die Ausführung des Tail-Befehls unter macOS etwa zehn Minuten dauern kann.

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. Verwenden Sie OpenSSL, um den öffentlichen Schlüssel aus dem Zertifikat zu extrahieren und die extrahierte Datei (sign.tmp) mit der Signaturdatei und dem öffentlichen Schlüssel zu überprüfen. Die Eingabeaufforderung zeigt Meldungen an, die den Erfolg oder Misserfolg der Überprüfung basierend auf deren Erfolg anzeigen.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verified OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. Räumen Sie den Arbeitsbereich auf.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

Stellen Sie Cloud Volumes ONTAP vom Azure Marketplace bereit

Sie können die direkte Bereitstellung über den Azure Marketplace verwenden, um Cloud Volumes ONTAP schnell und einfach bereitzustellen. Über den Azure Marketplace können Sie Cloud Volumes ONTAP mit wenigen Klicks schnell bereitstellen und die wichtigsten Funktionen und Möglichkeiten in Ihrer Umgebung erkunden.

Weitere Informationen zu diesem Angebot finden Sie unter"Informieren Sie sich über die Angebote von Cloud Volumes ONTAP in der NetApp Console und im Marketplace." .

Informationen zu diesem Vorgang

Das Cloud Volumes ONTAP -System, das mithilfe der direkten Bereitstellung im Azure Marketplace bereitgestellt wird, verfügt über diese Eigenschaften. Beachten Sie, dass sich die Funktionen einer über den Azure Marketplace bereitgestellten eigenständigen Instanz ändern, wenn sie in der NetApp Console erkannt wird.

- Die neueste Cloud Volumes ONTAP -Version (9.16.1 oder höher).
- Eine kostenlose Lizenz für Cloud Volumes ONTAP , die auf 500 GiB bereitgestellte Kapazität begrenzt ist. Diese Lizenz beinhaltet keinen NetApp Support und hat kein Ablaufdatum.
- Zwei Knoten, die im Hochverfügbarkeitsmodus (HA) in einer einzigen Verfügbarkeitszone (AZ) konfiguriert und mit Standardseriennummern bereitgestellt sind. Die Storage-VMs (Storage-VMs) werden in einem"flexibler Orchestrierungsmodus" .
- Ein Aggregat für die standardmäßig erstellte Instanz.

- Eine verwaltete Premium-SSD-v2-Festplatte mit 500 GiB bereitgestellter Kapazität sowie eine Root- und eine Datenfestplatte.
- Eine bereitgestellte Datenspeicher-VM mit NFS-, CIFS-, iSCSI- und NVMe/TCP-Datendiensten. Sie können keine zusätzlichen Datenspeicher-VMs hinzufügen.
- Installierte Lizenzen für NFS, CIFS (SMB), iSCSI, Autonomous Ransomware Protection (ARP), SnapLock und SnapMirror.
- "ONTAP temperaturempfindliche Speichereffizienz (TSSE)", Volume-Verschlüsselung und externe Schlüsselverwaltung standardmäßig aktiviert.
- Diese Funktionen werden nicht unterstützt:
  - FabricPool -Stufen
  - Ändern des Speicher-VM-Typs
  - Schnellschreibmodus

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie über ein gültiges Azure Marketplace-Abonnement verfügen.
- Stellen Sie sicher, dass Sie die Netzwerkanforderungen für ein"HA-Bereitstellung in einer einzigen AZ" in Azure. Weitere Informationen finden Sie unter "Einrichten des Azure-Netzwerks für Cloud Volumes ONTAP" .
- Um Cloud Volumes ONTAP bereitzustellen, muss Ihnen eine dieser Azure-Rollen zugewiesen werden:
  - Der `contributor` Rolle mit den Standardberechtigungen. Weitere Informationen finden Sie im "Microsoft Azure-Dokumentation: Integrierte Azure-Rollen" .
  - Eine benutzerdefinierte RBAC-Rolle mit den folgenden Berechtigungen. Weitere Informationen finden Sie im "Azure-Dokumentation: Benutzerdefinierte Azure-Rollen" .

"Berechtigungen": [{ "Aktionen": ["Microsoft.AAD/register/action", "Microsoft.Resources/subscriptions/resourceGroups/write", "Microsoft.Network/loadBalancers/write", "Microsoft.ClassicCompute/virtualMachines/write", "Microsoft.Compute/capacityReservationGroups/deploy/action", "Microsoft.ClassicCompute/virtualMachines/networkInterfaces/associatedNetworkSecurityGroups/write", "Microsoft.Network/networkInterfaces/write", "Microsoft.Compute/virtualMachines/write", "Microsoft.Compute/virtualMachines/extensions/write", "Microsoft.Resources/deployments/validate/action", "Microsoft.Resources/subscriptions/resourceGroups/read", "Microsoft.Network/virtualNetworks/write", "Microsoft.Network/virtualNetworks/read", "Microsoft.Network/networkSecurityGroups/write", "Microsoft.Network/networkSecurityGroups/read", "Microsoft.Compute/disks/write", "Microsoft.Compute/virtualMachineScaleSets/write", "Microsoft.Resources/deployments/write", "Microsoft.Network/virtualNetworks/subnets/read", "Microsoft.Network/virtualNetworks/subnets/write"], "notActions": [], "dataActions": [], "notDataActions": [] }]

Wenn Sie den Ressourcenanbieter "Microsoft.storage" für Ihr Abonnement registriert haben, benötigen Sie nicht die `Microsoft.AAD/register/action` Erlaubnis. Weitere Informationen finden Sie im "Azure-Dokumentation: Azure-Berechtigungen für Speicher" .

Schritte

1. Suchen Sie auf der Azure Marketplace-Site nach NetApp -Produkten.
2. Wählen Sie * NetApp Cloud Volumes ONTAP direct*.
3. Klicken Sie auf **Erstellen**, um den Bereitstellungsassistenten zu starten.
4. Wählen Sie einen Plan aus. In der **Plan**-Liste werden normalerweise die neuesten Versionen von Cloud Volumes ONTAP angezeigt.
5. Geben Sie auf der Registerkarte **Grundlagen** die folgenden Details an:
   - **Abonnement**: Wählen Sie ein Abonnement aus. Die Bereitstellung wird an die Abonnementnummer gekoppelt.
   - **Ressourcengruppe**: Verwenden Sie eine vorhandene Ressourcengruppe oder erstellen Sie eine neue. Ressourcengruppen helfen bei der Zuweisung aller Ressourcen, wie z. B. Festplatten und Speicher-VMs, innerhalb einer einzigen Gruppe für ein Cloud Volumes ONTAP System.
   - **Region**: Wählen Sie eine Region aus, die die Azure HA-Bereitstellung in einer einzelnen AZ unterstützt. Sie sehen in der Liste nur die verfügbaren Regionen.
   - **Größe**: Wählen Sie eine Speicher-VM-Größe für die unterstützte verwaltete Premium-SSD-v2-Festplatte aus.
   - **Zone**: Wählen Sie eine Zone für die von Ihnen ausgewählte Region aus.
   - **Admin-Passwort**: Legen Sie ein Passwort fest. Mit diesem Admin-Passwort melden Sie sich nach der Bereitstellung am System an.
   - **Passwort bestätigen**: Geben Sie zur Bestätigung dasselbe Passwort erneut ein.
     - Fügen Sie auf der Registerkarte **Netzwerk** ein virtuelles Netzwerk und ein Subnetz hinzu oder wählen Sie sie aus den Listen aus.

       Um die Einschränkungen von Microsoft Azure einzuhalten, sollten Sie beim Einrichten eines neuen virtuellen Netzwerks ein neues Subnetz erstellen. Wenn Sie ein vorhandenes Netzwerk auswählen, sollten Sie ebenfalls ein vorhandenes Subnetz auswählen.

     - Um eine vordefinierte Netzwerksicherheitsgruppe auszuwählen, wählen Sie **Ja**. Wählen Sie **Nein** aus, um eine vordefinierte Azure-Netzwerksicherheitsgruppe mit den erforderlichen Verkehrsregeln zuzuweisen. Weitere Informationen finden Sie unter "Sicherheitsgruppenregeln für Azure" .
     - Bestätigen Sie auf der Registerkarte **Erweitert**, ob die beiden für diese Bereitstellung erforderlichen Azure-Funktionen festgelegt wurden. Siehe"Aktivieren Sie eine Azure-Funktion für Cloud Volumes ONTAP Single AZ-Bereitstellungen" Und"Aktivieren Sie den Hochverfügbarkeitsmodus für Cloud Volumes ONTAP in Azure" .
     - Sie können Name-Wert-Paare für die Ressourcen oder Ressourcengruppen auf der Registerkarte **Tags** definieren.
     - Überprüfen Sie auf der Registerkarte **Überprüfen + Erstellen** die Details und starten Sie die Bereitstellung.

Nach Abschluss

Wählen Sie das Benachrichtigungssymbol aus, um den Fortschritt Ihrer Bereitstellung anzuzeigen. Nachdem Cloud Volumes ONTAP bereitgestellt wurde, können Sie die für Vorgänge aufgelistete Speicher-VM anzeigen.

Sobald Sie darauf zugreifen können, verwenden Sie ONTAP System Manager oder die ONTAP CLI, um sich mit den von Ihnen festgelegten Administratoranmeldeinformationen bei der Speicher-VM anzumelden. Anschließend können Sie Volumes, LUNs oder Freigaben erstellen und die Speicherfunktionen von Cloud

Volumes ONTAP nutzen.

Beheben von Bereitstellungsproblemen

Cloud Volumes ONTAP -Systeme, die direkt über den Azure-Marktplatz bereitgestellt werden, umfassen keinen Support von NetApp. Wenn während der Bereitstellung Probleme auftreten, können Sie diese selbstständig beheben.

Schritte

1. Gehen Sie auf der Azure Marketplace-Site zu **Bootdiagnose > Serielles Protokoll**.
2. Laden Sie die Serienprotokolle herunter und untersuchen Sie sie.
3. Informationen zur Fehlerbehebung finden Sie in der Produktdokumentation und in den Knowledge Base-Artikeln (KB).
   - "Azure Marketplace-Dokumentation"
   - "NetApp Dokumentation"
   - "NetApp KB-Artikel"

Entdecken Sie die bereitgestellten Systeme in der Konsole

Sie können die Cloud Volumes ONTAP -Systeme, die Sie mithilfe der direkten Bereitstellung im Azure Marketplace bereitgestellt haben, ermitteln und auf der Seite **Systeme** in der Konsole verwalten. Der Konsolenagent erkennt die Systeme, fügt sie hinzu, wendet die erforderlichen Lizenzen an und schaltet die vollständigen Funktionen der Konsole für diese Systeme frei. Die ursprüngliche HA-Konfiguration in einer einzelnen AZ mit PSSD v2 Managed Disks bleibt erhalten und das System wird beim selben Azure-Abonnement und derselben Ressourcengruppe registriert wie die ursprüngliche Bereitstellung.

Informationen zu diesem Vorgang

Beim Erkennen der Cloud Volumes ONTAP -Systeme, die mithilfe der direkten Bereitstellung im Azure Marketplace bereitgestellt wurden, führt der Konsolenagent die folgenden Aufgaben aus:

- Ersetzt die freien Lizenzen der ermittelten Systeme als reguläre kapazitätsbasierte"Freemium-Lizenzen" .
- Behält die vorhandenen Funktionen der bereitgestellten Systeme bei und fügt die zusätzlichen Funktionen der Konsole hinzu, z. B. Datenschutz, Datenverwaltung und Sicherheitsfunktionen.
- Ersetzt die installierten Lizenzen auf den Knoten durch neue ONTAP -Lizenzen für NFS, CIFS (SMB), iSCSI, ARP, SnapLock und SnapMirror.
- Konvertiert die generischen Knotenseriennummern in eindeutige Seriennummern.
- Weist den Ressourcen nach Bedarf neue System-Tags zu.
- Wandelt die dynamischen IP-Adressen der Instanz in statische IP-Adressen um.
- Ermöglicht die Funktionalitäten von"FabricPool -Stufen" ,"AutoSupport" , Und"Einmal schreiben, oft lesen" (WORM)-Speicher auf den bereitgestellten Systemen. Sie können diese Funktionen bei Bedarf über die Konsole aktivieren.
- Registriert die Instanzen bei den NSS-Konten, die zu ihrer Erkennung verwendet werden.
- Aktiviert Kapazitätsmanagementfunktionen in"automatischer und manueller Modus" für die entdeckten Systeme.

Bevor Sie beginnen

Stellen Sie sicher, dass die Bereitstellung auf dem Azure-Marktplatz abgeschlossen ist. Der Konsolenagent kann die Systeme nur erkennen, wenn die Bereitstellung abgeschlossen ist und sie zur Erkennung

bereitstehen.

Schritte

In der Konsole folgen Sie dem Standardverfahren zum Erkennen vorhandener Systeme. Weitere Informationen finden Sie unter "Fügen Sie der Konsole ein vorhandenes Cloud Volumes ONTAP -System hinzu" .

> Während der Erkennung werden möglicherweise Fehlermeldungen angezeigt, die Sie jedoch ignorieren können, bis der Erkennungsprozess abgeschlossen ist. Ändern Sie während der Erkennung nicht die systemgenerierten Cloud Volumes ONTAP -Konfigurationen im Azure Marketplace-Portal, insbesondere nicht die System-Tags. Alle an diesen Konfigurationen vorgenommenen Änderungen können zu unerwartetem Systemverhalten führen.

Nach Abschluss

Nachdem die Erkennung abgeschlossen ist, können Sie die auf der Seite **Systeme** in der Konsole aufgelisteten Systeme anzeigen. Sie können verschiedene Verwaltungsaufgaben ausführen, wie zum Beispiel"Erweiterung des Aggregats" ,"Hinzufügen von Volumes" ,"Bereitstellung zusätzlicher Speicher-VMs" , Und"Ändern der Instanztypen" .

Weiterführende Links

Weitere Informationen zum Erstellen von Speicher finden Sie in der ONTAP -Dokumentation:

- "Erstellen von Volumes für NFS"
- "Erstellen von LUNs für iSCSI"
- "Freigaben für CIFS erstellen"