Inizia a usare Microsoft Azure

Cloud Volumes ONTAP

NetApp
February 17, 2026

Sommario

Inizia a usare Microsoft Azure

Scopri le opzioni di distribuzione di Cloud Volumes ONTAP in Azure

NetApp offre due opzioni per distribuire Cloud Volumes ONTAP su Azure. Cloud Volumes ONTAP si affida tradizionalmente alla NetApp Console per la distribuzione e l'orchestrazione. A partire da Cloud Volumes ONTAP 9.16.1, puoi sfruttare la distribuzione diretta di Azure Marketplace, un processo semplificato che fornisce accesso a un set limitato, ma comunque potente, di funzionalità e opzioni di Cloud Volumes ONTAP .

Quando distribuisci Cloud Volumes ONTAP direttamente da Azure Marketplace, non è necessario configurare l'agente della console o soddisfare altri criteri di sicurezza e onboarding richiesti per distribuire Cloud Volumes ONTAP tramite la console. Dall'Azure Marketplace puoi distribuire rapidamente Cloud Volumes ONTAP in pochi clic ed esplorare le sue funzionalità e capacità principali nel tuo ambiente.

Una volta completata la distribuzione in Azure Marketplace, è possibile individuare questi sistemi nella Console. Dopo l'individuazione, è possibile gestirli come sistemi Cloud Volumes ONTAP e sfruttare tutte le funzionalità della Console. Fare riferimento a "Scopri i sistemi distribuiti nella Console" .

Ecco il confronto delle funzionalità tra le due opzioni. Si noti che le funzionalità di un'istanza autonoma distribuita tramite Azure Marketplace cambiano quando viene rilevata nella Console.

	Mercato di Azure	**NetApp Console**
Integrazione	Più breve e più semplice, minima preparazione richiesta per l'impiego diretto	Processo di onboarding più lungo, inclusa l'installazione dell'agente della console
Tipi di macchine virtuali (VM) supportati	Tipi di istanza Eds_v5 e Ls_v3	Gamma completa di tipi di VM.https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-azure.html["Configurazioni supportate in Azure"^]
Licenza	Licenza gratuita	Qualsiasi licenza basata sulla capacità."Licenza Cloud Volumes ONTAP"
* Supporto NetApp *	Non incluso	Disponibile, in base al tipo di licenza
Capacità	Fino a 500 GiB	Espandibile tramite configurazione
Modello di distribuzione	Distribuzione in modalità ad alta disponibilità (HA) in una singola zona di disponibilità (AZ)	Tutte le configurazioni supportate, comprese le modalità a nodo singolo e HA, le distribuzioni AZ singole e multiple
Tipo di disco supportato	Dischi gestiti Premium SSD v2	Supporto più ampio."Configurazione predefinita per Cloud Volumes ONTAP"

	Mercato di Azure	NetApp Console
Velocità di scrittura (modalità di scrittura veloce)	Non supportato	Supportato, in base alla configurazione. "Scopri di più sulle velocità di scrittura in Cloud Volumes ONTAP" .
Capacità di orchestrazione	Non disponibile	Disponibile tramite NetApp Console, in base al tipo di licenza
Numero di VM di archiviazione supportate	Uno per distribuzione	Più VM di archiviazione, in base alla configurazione."Numero supportato di VM di archiviazione"
Modifica del tipo di istanza	Non supportato	Supportato
* Livelli FabricPool *	Non supportato	Supportato

Link correlati

- Distribuzione diretta di Azure Marketplace:"Distribuisci Cloud Volumes ONTAP dal marketplace di Azure"
- Distribuzione tramite la console:"Avvio rapido per Cloud Volumes ONTAP in Azure"
- "Documentazione NetApp Console"

Inizia con NetApp Console

Avvio rapido per Cloud Volumes ONTAP in Azure

Inizia a usare Cloud Volumes ONTAP per Azure in pochi passaggi.

Creare un agente Console

Se non hai un "Agente console" eppure devi crearne uno. "Scopri come creare un agente Console in Azure"

Tieni presente che se desideri distribuire Cloud Volumes ONTAP in una subnet in cui non è disponibile l'accesso a Internet, dovrai installare manualmente l'agente Console e accedere alla NetApp Console in esecuzione su tale agente Console. "Scopri come installare manualmente l'agente Console in una posizione senza accesso a Internet"

Pianifica la tua configurazione

La Console offre pacchetti preconfigurati che soddisfano i requisiti del tuo carico di lavoro, oppure puoi creare la tua configurazione personalizzata. Se scegli una configurazione personalizzata, dovresti conoscere le opzioni a tua disposizione. Per informazioni, fare riferimento a"Pianifica la configurazione Cloud Volumes ONTAP in Azure" .

Configura la tua rete

1. Assicurati che la tua VNet e le tue subnet supportino la connettività tra l'agente della console e Cloud Volumes ONTAP.
2. Abilita l'accesso a Internet in uscita dalla VPC di destinazione per NetApp AutoSupport.

Questo passaggio non è necessario se si distribuisce Cloud Volumes ONTAP in una posizione in cui non è disponibile l'accesso a Internet.

"Scopri di più sui requisiti di rete" .

4 Avvia Cloud Volumes ONTAP

Fare clic su **Aggiungi sistema**, selezionare il tipo di sistema che si desidera distribuire e completare i passaggi della procedura guidata. "Leggi le istruzioni passo passo" .

Link correlati

- "Creazione di un agente Console dalla Console"
- "Creazione di un agente console da Azure Marketplace"
- "Installazione del software dell'agente Console su un host Linux"
- "Cosa fa la Console con i permessi"

Pianifica la configurazione Cloud Volumes ONTAP in Azure

Quando distribuisci Cloud Volumes ONTAP in Azure, puoi scegliere un sistema preconfigurato che soddisfi i requisiti del tuo carico di lavoro oppure puoi creare una configurazione personalizzata. Se scegli una configurazione personalizzata, dovresti conoscere le opzioni a tua disposizione.

Scegli una licenza Cloud Volumes ONTAP

Sono disponibili diverse opzioni di licenza per Cloud Volumes ONTAP. Ogni opzione ti consente di scegliere il modello di consumo più adatto alle tue esigenze.

- "Scopri le opzioni di licenza per Cloud Volumes ONTAP"
- "Scopri come impostare le licenze"

Scegli una regione supportata

Cloud Volumes ONTAP è supportato nella maggior parte delle regioni Microsoft Azure. "Visualizza l'elenco completo delle regioni supportate" .

Scegli un tipo di VM supportato

Cloud Volumes ONTAP supporta diversi tipi di VM, a seconda del tipo di licenza scelto.

"Configurazioni supportate per Cloud Volumes ONTAP in Azure"

Comprendere i limiti di archiviazione

Il limite di capacità raw per un sistema Cloud Volumes ONTAP è legato alla licenza. Ulteriori limiti incidono sulle dimensioni degli aggregati e sui volumi. Quando pianifichi la tua configurazione, dovresti essere consapevole di questi limiti.

"Limiti di archiviazione per Cloud Volumes ONTAP in Azure"

Dimensiona il tuo sistema in Azure

Il dimensionamento del sistema Cloud Volumes ONTAP può aiutarti a soddisfare i requisiti di prestazioni e capacità. Quando si sceglie un tipo di macchina virtuale, un tipo di disco e una dimensione del disco, è necessario tenere presenti alcuni punti chiave:

Tipo di macchina virtuale

Guarda i tipi di macchine virtuali supportati in "Note sulla versione Cloud Volumes ONTAP" e quindi rivedere i dettagli su ciascun tipo di VM supportato. Tieni presente che ogni tipo di VM supporta un numero specifico di dischi dati.

- "Documentazione di Azure: dimensioni delle macchine virtuali per uso generico"
- "Documentazione di Azure: dimensioni delle macchine virtuali con memoria ottimizzata"

Tipo di disco Azure con sistemi a nodo singolo

Quando si creano volumi per Cloud Volumes ONTAP, è necessario scegliere lo storage cloud sottostante che Cloud Volumes ONTAP utilizza come disco.

I sistemi a nodo singolo possono utilizzare questi tipi di Azure Managed Disks:

- I dischi gestiti SSD Premium offrono prestazioni elevate per carichi di lavoro ad alta intensità di I/O a un costo più elevato.
- I dischi gestiti Premium SSD v2 offrono prestazioni più elevate con una latenza inferiore a un costo inferiore rispetto ai dischi gestiti Premium SSD.
- I dischi gestiti SSD standard garantiscono prestazioni costanti per carichi di lavoro che richiedono IOPS bassi.
- I dischi gestiti HDD standard sono una buona scelta se non hai bisogno di IOPS elevati e vuoi ridurre i costi.

Per ulteriori dettagli sui casi d'uso di questi dischi, fare riferimento a "Documentazione di Microsoft Azure: quali tipi di dischi sono disponibili in Azure?" .

Tipo di disco di Azure con coppie HA

I sistemi HA utilizzano dischi gestiti condivisi Premium SSD, entrambi in grado di garantire prestazioni elevate per carichi di lavoro ad alta intensità di I/O a un costo più elevato. Le distribuzioni HA create prima della versione 9.12.1 utilizzano blob di pagine Premium.

Dimensioni del disco di Azure

Quando si avviano istanze Cloud Volumes ONTAP , è necessario scegliere la dimensione del disco predefinita per gli aggregati. NetApp Console utilizza questa dimensione del disco per l'aggregato iniziale e per tutti gli aggregati aggiuntivi creati quando si utilizza l'opzione di provisioning semplice. È possibile creare aggregati che utilizzano una dimensione del disco diversa da quella predefinita"utilizzando l'opzione di allocazione avanzata" .

Tutti i dischi di un aggregato devono avere le stesse dimensioni.

Quando si sceglie la dimensione del disco, è necessario prendere in considerazione diversi fattori. Le dimensioni del disco influiscono sul costo dell'archiviazione, sulle dimensioni dei volumi che è possibile creare in aggregato, sulla capacità totale disponibile per Cloud Volumes ONTAP e sulle prestazioni di archiviazione.

Le prestazioni di Azure Premium Storage sono legate alle dimensioni del disco. I dischi più grandi

garantiscono IOPS e throughput più elevati. Ad esempio, la scelta di dischi da 1 TiB può garantire prestazioni migliori rispetto a dischi da 500 GiB, ma a un costo più elevato.

Non ci sono differenze di prestazioni tra le dimensioni dei dischi per Standard Storage. Dovresti scegliere la dimensione del disco in base alla capacità di cui hai bisogno.

Per informazioni su IOPS e velocità effettiva in base alle dimensioni del disco, fare riferimento ad Azure:

- "Microsoft Azure: prezzi di Managed Disks"
- "Microsoft Azure: prezzi dei Page Blobs"

Visualizza i dischi di sistema predefiniti

Oltre allo storage per i dati utente, la Console acquista anche storage cloud per i dati di sistema Cloud Volumes ONTAP (dati di avvio, dati root, dati core e NVRAM). Ai fini della pianificazione, potrebbe essere utile rivedere questi dettagli prima di distribuire Cloud Volumes ONTAP.

"Visualizza i dischi predefiniti per i dati di sistema Cloud Volumes ONTAP in Azure" .

L'agente Console richiede anche un disco di sistema. "Visualizza i dettagli sulla configurazione predefinita dell'agente della console" .

Raccogliere informazioni di rete

Quando si distribuisce Cloud Volumes ONTAP in Azure, è necessario specificare i dettagli sulla rete virtuale. Puoi utilizzare un foglio di lavoro per raccogliere le informazioni dal tuo amministratore.

Informazioni su Azure	Il tuo valore
Regione	
Rete virtuale (VNet)	
Sottorete	
Gruppo di sicurezza di rete (se ne utilizzi uno tuo)	

Scegli una velocità di scrittura

La console consente di scegliere un'impostazione della velocità di scrittura per Cloud Volumes ONTAP. Prima di scegliere una velocità di scrittura, è necessario comprendere le differenze tra le impostazioni normale e alta, nonché i rischi e i consigli relativi all'utilizzo di una velocità di scrittura elevata. "Scopri di più sulla velocità di scrittura" .

Scegli un profilo di utilizzo del volume

ONTAP include diverse funzionalità di efficienza di archiviazione che possono ridurre la quantità totale di spazio di archiviazione necessario. Quando si crea un volume nella Console, è possibile scegliere un profilo che abiliti queste funzionalità oppure un profilo che le disabiliti. Dovresti saperne di più su queste funzionalità per decidere quale profilo utilizzare.

Le funzionalità di efficienza dello storage NetApp offrono i seguenti vantaggi:

Provisioning sottile

Offre agli host o agli utenti più spazio di archiviazione logica di quello effettivamente disponibile nel pool di archiviazione fisico. Invece di preallocare lo spazio di archiviazione, lo spazio di archiviazione viene allocato dinamicamente a ciascun volume man mano che i dati vengono scritti.

Deduplicazione

Migliora l'efficienza individuando blocchi di dati identici e sostituendoli con riferimenti a un singolo blocco condiviso. Questa tecnica riduce i requisiti di capacità di archiviazione eliminando i blocchi ridondanti di dati che risiedono nello stesso volume.

Compressione

Riduce la capacità fisica necessaria per archiviare i dati comprimendoli all'interno di un volume su storage primario, secondario e di archivio.

Configurare la rete di Azure per Cloud Volumes ONTAP

La NetApp Console gestisce la configurazione dei componenti di rete per Cloud Volumes ONTAP, come indirizzi IP, maschere di rete e percorsi. È necessario assicurarsi che l'accesso a Internet in uscita sia disponibile, che siano disponibili sufficienti indirizzi IP privati, che siano attive le connessioni giuste e altro ancora.

Requisiti per Cloud Volumes ONTAP

In Azure devono essere soddisfatti i seguenti requisiti di rete.

Accesso a Internet in uscita

I sistemi Cloud Volumes ONTAP necessitano di accesso a Internet in uscita per accedere agli endpoint esterni per varie funzioni. Cloud Volumes ONTAP non può funzionare correttamente se questi endpoint sono bloccati in ambienti con requisiti di sicurezza rigorosi.

L'agente della console contatta anche diversi endpoint per le operazioni quotidiane. Per informazioni sugli endpoint, fare riferimento a "Visualizza gli endpoint contattati dall'agente della console" E "Preparare la rete per l'utilizzo della console" .

Endpoint Cloud Volumes ONTAP

Cloud Volumes ONTAP utilizza questi endpoint per comunicare con vari servizi.

Punti finali	Applicabile per	Scopo	Modalità di distribuzione	Impatto se non disponibile
\ https://netapp-cloud-account.auth0.com	Autenticazione	Utilizzato per l'autenticazione nella Console.	Modalità standard e limitata.	L'autenticazione dell'utente fallisce e i seguenti servizi rimangono non disponibili: • Servizi Cloud Volumes ONTAP • Servizi ONTAP • Protocolli e servizi proxy
https://vault.azure.net	Deposito chiavi	Utilizzato per recuperare le chiavi segrete del client da Azure Key Vault quando si utilizzano chiavi gestite dal cliente (CMK).	Modalità standard, limitata e privata.	I servizi Cloud Volumes ONTAP non sono disponibili.
\ https://api.bluexp.netapp.com/tenancy	Locazione	Utilizzato per recuperare le risorse Cloud Volumes ONTAP dalla Console per autorizzare risorse e utenti.	Modalità standard e limitata.	Le risorse Cloud Volumes ONTAP e gli utenti non sono autorizzati.
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Utilizzato per inviare i dati di telemetria AutoSupport al supporto NetApp .	Modalità standard e limitata.	Le informazioni AutoSupport non vengono recapitate.
\ https://management.azure.com \ https://login.microsoftonline.com \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://core.windows.net	Regioni pubbliche	Comunicazione con i servizi Azure.	Modalità standard, limitata e privata.	Cloud Volumes ONTAP non riesce a comunicare con il servizio Azure per eseguire operazioni specifiche per la console in Azure.

Punti finali	Applicabile per	Scopo	Modalità di distribuzione	Impatto se non disponibile
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Regione della Cina	Comunicazione con i servizi Azure.	Modalità standard, limitata e privata.	Cloud Volumes ONTAP non riesce a comunicare con il servizio Azure per eseguire operazioni specifiche per la console in Azure.
\ https://management.microsoftazure.de \ https://login.microsoftonline.de \ https://blob.core.cloudapi.de \ https://core.cloudapi.de	Regione Germania	Comunicazione con i servizi Azure.	Modalità standard, limitata e privata.	Cloud Volumes ONTAP non riesce a comunicare con il servizio Azure per eseguire operazioni specifiche per la console in Azure.
\ https://management.usgovcloudapi.net \ https://login.microsoftonline.us \ https://blob.core.usgovcloudapi.net \ https://core.usgovcloudapi.net	Regioni governative	Comunicazione con i servizi Azure.	Modalità standard, limitata e privata.	Cloud Volumes ONTAP non riesce a comunicare con il servizio Azure per eseguire operazioni specifiche per la console in Azure.
\ https://management.azure.microsoft.scloud \ https://login.microsoftonline.microsoft.scloud \ https://blob.core.microsoft.scloud \ https://core.microsoft.scloud	Regioni del Dipartimento della Difesa del governo	Comunicazione con i servizi Azure.	Modalità standard, limitata e privata.	Cloud Volumes ONTAP non riesce a comunicare con il servizio Azure per eseguire operazioni specifiche per la console in Azure.

Configurazione del proxy di rete dell'agente NetApp Console

È possibile utilizzare la configurazione dei server proxy dell'agente NetApp Console per abilitare l'accesso a Internet in uscita da Cloud Volumes ONTAP. La console supporta due tipi di proxy:

- **Proxy esplicito**: il traffico in uscita da Cloud Volumes ONTAP utilizza l'indirizzo HTTP del server proxy specificato durante la configurazione del proxy dell'agente della console. L'amministratore potrebbe anche aver configurato le credenziali utente e i certificati CA radice per un'autenticazione aggiuntiva. Se è disponibile un certificato CA radice per il proxy esplicito, assicurarsi di ottenere e caricare lo stesso certificato sul sistema Cloud Volumes ONTAP utilizzando "ONTAP CLI: installazione del certificato di sicurezza" comando.

- **Proxy trasparente**: la rete è configurata per instradare automaticamente il traffico in uscita da Cloud Volumes ONTAP tramite il proxy per l'agente della console. Quando si configura un proxy trasparente, l'amministratore deve fornire solo un certificato CA radice per la connettività da Cloud Volumes ONTAP, non l'indirizzo HTTP del server proxy. Assicurati di ottenere e caricare lo stesso certificato CA radice sul tuo sistema Cloud Volumes ONTAP utilizzando "ONTAP CLI: installazione del certificato di sicurezza" comando.

Per informazioni sulla configurazione dei server proxy, fare riferimento a "Configurare l'agente della console per utilizzare un server proxy" .

indirizzi IP

La console assegna automaticamente il numero richiesto di indirizzi IP privati a Cloud Volumes ONTAP in Azure. Devi assicurarti che la tua rete disponga di un numero sufficiente di indirizzi IP privati.

Il numero di LIF allocati per Cloud Volumes ONTAP dipende dal fatto che si distribuisca un sistema a nodo singolo o una coppia HA. Un LIF è un indirizzo IP associato a una porta fisica. Un LIF di gestione SVM è necessario per strumenti di gestione come SnapCenter.

> Un iSCSI LIF fornisce l'accesso client tramite il protocollo iSCSI e viene utilizzato dal sistema per altri importanti flussi di lavoro di rete. Questi LIF sono obbligatori e non devono essere eliminati.

Indirizzi IP per un sistema a nodo singolo

La NetApp Console assegna 5 o 6 indirizzi IP a un sistema a nodo singolo:

- IP di gestione del cluster
- IP di gestione dei nodi
- IP intercluster per SnapMirror
- IP NFS/CIFS
- IP iSCSI

> L'IP iSCSI fornisce l'accesso client tramite il protocollo iSCSI. Viene utilizzato dal sistema anche per altri importanti flussi di lavoro di rete. Questo LIF è obbligatorio e non deve essere eliminato.

- Gestione SVM (facoltativa, non configurata di default)

Indirizzi IP per coppie HA

Durante la distribuzione, la console assegna indirizzi IP a 4 NIC (per nodo).

Si noti che la NetApp Console crea un LIF di gestione SVM sulle coppie HA, ma non sui sistemi a nodo singolo in Azure.

NIC0

- IP di gestione dei nodi
- IP intercluster
- IP iSCSI

L'IP iSCSI fornisce l'accesso client tramite il protocollo iSCSI. Viene utilizzato dal sistema anche per altri importanti flussi di lavoro di rete. Questo LIF è obbligatorio e non deve essere eliminato.

NIC1

- IP di rete del cluster

NIC2

- IP di interconnessione del cluster (HA IC)

NIC3

- IP NIC Pageblob (accesso al disco)

NIC3 è applicabile solo alle distribuzioni HA che utilizzano l'archiviazione BLOB di pagina.

Gli indirizzi IP sopra indicati non migrano in caso di eventi di failover.

Inoltre, 4 IP frontend (FIP) sono configurati per migrare in caso di eventi di failover. Questi IP frontend risiedono nel bilanciatore del carico.

- IP di gestione del cluster
- IP dati NodeA (NFS/CIFS)
- IP dati NodeB (NFS/CIFS)
- IP di gestione SVM

Connessioni sicure ai servizi di Azure

Per impostazione predefinita, la console abilita un collegamento privato di Azure per le connessioni tra Cloud Volumes ONTAP e gli account di archiviazione BLOB di pagine di Azure.

Nella maggior parte dei casi, non c'è nulla che tu debba fare: la console gestisce il collegamento privato di Azure per te. Ma se si utilizza Azure Private DNS, sarà necessario modificare un file di configurazione. È inoltre necessario essere a conoscenza di un requisito relativo alla posizione dell'agente della console in Azure.

Se le esigenze aziendali lo richiedono, puoi anche disattivare la connessione Private Link. Se si disabilita il collegamento, la Console configura Cloud Volumes ONTAP in modo che utilizzi invece un endpoint di servizio.

"Scopri di più sull'utilizzo di Azure Private Links o endpoint di servizio con Cloud Volumes ONTAP" .

Networking per la crittografia di Azure VNet

Cloud Volumes ONTAP supporta "Crittografia di Azure Virtual Network (VNet)" la crittografia del traffico da VM a VM all'interno di una VNet o tra VNets in peering. Questa funzionalità è configurata a livello di VNet di Azure ed è indipendente dalla topologia di Cloud Volumes ONTAP (nodo singolo o HA).

È sufficiente assicurarsi che Accelerated Networking sia abilitato sulle schede di rete della macchina virtuale e verificare i requisiti e le limitazioni di crittografia della rete virtuale di Azure prima di abilitare la funzionalità. Non si devono modificare gli oggetti del servizio di bilanciamento del carico gestito NetApp.

"Documentazione Azure: crittografia VNet e Accelerated Networking".

Collegamenti ad altri sistemi ONTAP

Per replicare i dati tra un sistema Cloud Volumes ONTAP in Azure e sistemi ONTAP in altre reti, è necessario disporre di una connessione VPN tra la rete virtuale di Azure e l'altra rete, ad esempio la rete aziendale.

Per le istruzioni, fare riferimento al "Documentazione di Microsoft Azure: creare una connessione da sito a sito nel portale di Azure" .

Porta per l'interconnessione HA

Una coppia Cloud Volumes ONTAP HA include un'interconnessione HA, che consente a ciascun nodo di verificare continuamente se il partner funziona e di eseguire il mirroring dei dati di registro per la memoria non volatile dell'altro. L'interconnessione HA utilizza la porta TCP 10006 per la comunicazione.

Per impostazione predefinita, la comunicazione tra i LIF di interconnessione HA è aperta e non sono presenti regole di gruppo di sicurezza per questa porta. Tuttavia, se si crea un firewall tra i LIF di interconnessione HA, è necessario assicurarsi che il traffico TCP sia aperto per la porta 10006, in modo che la coppia HA possa funzionare correttamente.

Solo una coppia HA in un gruppo di risorse di Azure

È necessario utilizzare un gruppo di risorse *dedicato* per ogni coppia Cloud Volumes ONTAP HA distribuita in Azure. In un gruppo di risorse è supportata solo una coppia HA.

La console riscontra problemi di connessione se si tenta di distribuire una seconda coppia Cloud Volumes ONTAP HA in un gruppo di risorse di Azure.

Regole del gruppo di sicurezza

La console crea gruppi di sicurezza di Azure che includono le regole in ingresso e in uscita affinché Cloud Volumes ONTAP funzioni correttamente. "Visualizza le regole del gruppo di sicurezza per l'agente della console" .

I gruppi di sicurezza di Azure per Cloud Volumes ONTAP richiedono che le porte appropriate siano aperte per la comunicazione interna tra i nodi. "Scopri di più sulle porte interne ONTAP" .

Si sconsiglia di modificare i gruppi di sicurezza predefiniti o di utilizzare gruppi di sicurezza personalizzati. Tuttavia, se necessario, tieni presente che il processo di distribuzione richiede che il sistema Cloud Volumes ONTAP abbia accesso completo all'interno della propria subnet. Una volta completata la distribuzione, se si decide di modificare il gruppo di sicurezza di rete, assicurarsi di mantenere aperte le porte del cluster e le porte di rete HA. Ciò garantisce una comunicazione fluida all'interno del cluster Cloud Volumes ONTAP (comunicazione any-to-any tra i nodi).

Regole in entrata per sistemi a nodo singolo

Quando aggiungi un sistema Cloud Volumes ONTAP e scegli un gruppo di sicurezza predefinito, puoi scegliere di consentire il traffico all'interno di uno dei seguenti:

- **Solo VNet selezionata**: l'origine del traffico in entrata è l'intervallo di subnet della VNet per il sistema Cloud Volumes ONTAP e l'intervallo di subnet della VNet in cui risiede l'agente della console. Questa è l'opzione consigliata.
- **Tutte le reti virtuali**: l'origine del traffico in entrata è l'intervallo IP 0.0.0.0/0.

- **Disabilitato**: questa opzione limita l'accesso alla rete pubblica al tuo account di archiviazione e disabilita la suddivisione in livelli dei dati per i sistemi Cloud Volumes ONTAP . Questa è un'opzione consigliata se i tuoi indirizzi IP privati non devono essere esposti nemmeno all'interno della stessa rete virtuale a causa delle normative e delle policy di sicurezza.

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
1000 inbound_ssh	22 TCP	Da qualsiasi a qualsiasi	Accesso SSH all'indirizzo IP del LIF di gestione del cluster o di un LIF di gestione del nodo
1001 in entrata_http	80 TCP	Da qualsiasi a qualsiasi	Accesso HTTP alla console Web di ONTAP System Manager tramite l'indirizzo IP del LIF di gestione del cluster
1002 in entrata_111_tcp	111 TCP	Da qualsiasi a qualsiasi	Chiamata di procedura remota per NFS
1003 in entrata_111_udp	111 UDP	Da qualsiasi a qualsiasi	Chiamata di procedura remota per NFS
1004 in entrata_139	139 TCP	Da qualsiasi a qualsiasi	Sessione del servizio NetBIOS per CIFS
1005 in entrata_161-162 _tcp	161-162 TCP	Da qualsiasi a qualsiasi	Protocollo semplice di gestione della rete
1006 in entrata_161-162 _udp	161-162 UDP	Da qualsiasi a qualsiasi	Protocollo semplice di gestione della rete
1007 in entrata_443	443 TCP	Da qualsiasi a qualsiasi	Connettività con l'agente Console e accesso HTTPS alla console Web ONTAP System Manager utilizzando l'indirizzo IP del LIF di gestione del cluster
1008 in entrata_445	445 TCP	Da qualsiasi a qualsiasi	Microsoft SMB/CIFS su TCP con framing NetBIOS
1009 in entrata_635_tcp	635 TCP	Da qualsiasi a qualsiasi	Montaggio NFS
1010 in entrata_635_udp	635 UDP	Da qualsiasi a qualsiasi	Montaggio NFS
1011 in entrata_749	749 TCP	Da qualsiasi a qualsiasi	Kerberos
1012 in entrata_2049_tcp	2049 TCP	Da qualsiasi a qualsiasi	Demone del server NFS
1013 in entrata_2049_udp	2049 UDP	Da qualsiasi a qualsiasi	Demone del server NFS
1014 in entrata_3260	3260 TCP	Da qualsiasi a qualsiasi	Accesso iSCSI tramite i dati iSCSI LIF
1015 in entrata_4045-4046_tcp	4045-4046 TCP	Da qualsiasi a qualsiasi	Demone di blocco NFS e monitor dello stato della rete

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
1016 in entrata_4045-4046_udp	4045-4046 UDP	Da qualsiasi a qualsiasi	Demone di blocco NFS e monitor dello stato della rete
1017 in entrata_10000	10000 TCP	Da qualsiasi a qualsiasi	Backup tramite NDMP
1018 in entrata_11104-11105	11104-11105 TCP	Da qualsiasi a qualsiasi	Trasferimento dati SnapMirror
3000 inbound_deny _all_tcp	Qualsiasi porta TCP	Da qualsiasi a qualsiasi	Blocca tutto il resto del traffico TCP in entrata
3001 inbound_deny _all_udp	Qualsiasi porta UDP	Da qualsiasi a qualsiasi	Blocca tutto il resto del traffico UDP in entrata
65000 AllowVnetInBound	Qualsiasi porta Qualsiasi protocollo	Da rete virtuale a rete virtuale	Traffico in entrata dall'interno della VNet
65001 ConsentiAzureLoad BalancerInBound	Qualsiasi porta Qualsiasi protocollo	AzureLoadBalancer a qualsiasi	Traffico dati da Azure Standard Load Balancer
65500 DenyAllInBound	Qualsiasi porta Qualsiasi protocollo	Da qualsiasi a qualsiasi	Blocca tutto il resto del traffico in entrata

Regole in entrata per sistemi HA

Quando aggiungi un sistema Cloud Volumes ONTAP e scegli un gruppo di sicurezza predefinito, puoi scegliere di consentire il traffico all'interno di uno dei seguenti:

- **Solo VNet selezionata**: l'origine del traffico in entrata è l'intervallo di subnet della VNet per il sistema Cloud Volumes ONTAP e l'intervallo di subnet della VNet in cui risiede l'agente della console. Questa è l'opzione consigliata.
- **Tutte le reti virtuali**: l'origine del traffico in entrata è l'intervallo IP 0.0.0.0/0.

> I sistemi HA hanno meno regole in ingresso rispetto ai sistemi a nodo singolo perché il traffico dati in ingresso passa attraverso l'Azure Standard Load Balancer. Per questo motivo, il traffico proveniente dal Load Balancer dovrebbe essere aperto, come mostrato nella regola "AllowAzureLoadBalancerInBound".

- **Disabilitato**: questa opzione limita l'accesso alla rete pubblica al tuo account di archiviazione e disabilita la suddivisione in livelli dei dati per i sistemi Cloud Volumes ONTAP . Questa è un'opzione consigliata se i tuoi indirizzi IP privati non devono essere esposti nemmeno all'interno della stessa rete virtuale a causa delle normative e delle policy di sicurezza.

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
100 in entrata_443	443 Qualsiasi protocollo	Da qualsiasi a qualsiasi	Connettività con l'agente Console e accesso HTTPS alla console Web ONTAP System Manager utilizzando l'indirizzo IP del LIF di gestione del cluster

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
101 in entrata_111_tcp	111 Qualsiasi protocollo	Da qualsiasi a qualsiasi	Chiamata di procedura remota per NFS
102 in entrata_2049_tcp	2049 Qualsiasi protocollo	Da qualsiasi a qualsiasi	Demone del server NFS
111 inbound_ssh	22 Qualsiasi protocollo	Da qualsiasi a qualsiasi	Accesso SSH all'indirizzo IP del LIF di gestione del cluster o di un LIF di gestione del nodo
121 in entrata_53	53 Qualsiasi protocollo	Da qualsiasi a qualsiasi	DNS e CIFS
65000 AllowVnetInBound	Qualsiasi porta Qualsiasi protocollo	Da rete virtuale a rete virtuale	Traffico in entrata dall'interno della VNet
65001 ConsentiAzureLoad BalancerInBound	Qualsiasi porta Qualsiasi protocollo	AzureLoadBalancer a qualsiasi	Traffico dati da Azure Standard Load Balancer
65500 DenyAllInBound	Qualsiasi porta Qualsiasi protocollo	Da qualsiasi a qualsiasi	Blocca tutto il resto del traffico in entrata

Regole in uscita

Il gruppo di sicurezza predefinito per Cloud Volumes ONTAP apre tutto il traffico in uscita. Se ciò è accettabile, seguite le regole di base per le comunicazioni in uscita. Se hai bisogno di regole più rigide, usa le regole in uscita avanzate.

Regole di base in uscita

Il gruppo di sicurezza predefinito per Cloud Volumes ONTAP include le seguenti regole in uscita.

Porta	Protocollo	Scopo
Tutto	Tutti gli TCP	Tutto il traffico in uscita
Tutto	Tutti gli UDP	Tutto il traffico in uscita

Regole in uscita avanzate

Se hai bisogno di regole rigide per il traffico in uscita, puoi utilizzare le seguenti informazioni per aprire solo le porte necessarie per la comunicazione in uscita da parte di Cloud Volumes ONTAP.

La sorgente è l'interfaccia (indirizzo IP) sul sistema Cloud Volumes ONTAP .

Servizio	Porta	Protocollo	Fonte	Destinazione	Scopo
Directory attiva	88	TCP	Gestione dei nodi LIF	Foresta di Active Directory	Autenticazione Kerberos V
	137	UDP	Gestione dei nodi LIF	Foresta di Active Directory	Servizio di denominazione NetBIOS
	138	UDP	Gestione dei nodi LIF	Foresta di Active Directory	Servizio datagramma NetBIOS
	139	TCP	Gestione dei nodi LIF	Foresta di Active Directory	Sessione del servizio NetBIOS
	389	TCP e UDP	Gestione dei nodi LIF	Foresta di Active Directory	LDAP
	445	TCP	Gestione dei nodi LIF	Foresta di Active Directory	Microsoft SMB/CIFS su TCP con framing NetBIOS
	464	TCP	Gestione dei nodi LIF	Foresta di Active Directory	Kerberos V cambia e imposta la password (SET_CHANGE)
	464	UDP	Gestione dei nodi LIF	Foresta di Active Directory	Amministrazione delle chiavi Kerberos
	749	TCP	Gestione dei nodi LIF	Foresta di Active Directory	Kerberos V modifica e imposta password (RPCSEC_GSS)
	88	TCP	Dati LIF (NFS, CIFS, iSCSI)	Foresta di Active Directory	Autenticazione Kerberos V
	137	UDP	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Servizio di denominazione NetBIOS
	138	UDP	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Servizio datagramma NetBIOS
	139	TCP	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Sessione del servizio NetBIOS
	389	TCP e UDP	Dati LIF (NFS, CIFS)	Foresta di Active Directory	LDAP
	445	TCP	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Microsoft SMB/CIFS su TCP con framing NetBIOS
	464	TCP	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Kerberos V cambia e imposta la password (SET_CHANGE)
	464	UDP	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Amministrazione delle chiavi Kerberos
	749	TCP	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Kerberos V modifica e imposta password (RPCSEC_GSS)

Servizio	Porta	Protocollo	Fonte	Destinazione	Scopo
AutoSupport	HTTPS	443	Gestione dei nodi LIF	mysupport.netapp.com	AutoSupport (HTTPS è l'impostazione predefinita)
	HTTP	80	Gestione dei nodi LIF	mysupport.netapp.com	AutoSupport (solo se il protocollo di trasporto viene modificato da HTTPS a HTTP)
	TCP	3128	Gestione dei nodi LIF	Agente console	Invio di messaggi AutoSupport tramite un server proxy sull'agente Console, se non è disponibile una connessione Internet in uscita
Backup di configurazione	HTTP	80	Gestione dei nodi LIF	http://<indirizzo-IP-agente-console>/occm/offboxconfig	Inviare i backup della configurazione all'agente della console. "Documentazione ONTAP" .
DHCP	68	UDP	Gestione dei nodi LIF	DHCP	Client DHCP per la prima configurazione
DHCP	67	UDP	Gestione dei nodi LIF	DHCP	server DHCP
DNS	53	UDP	Gestione dei nodi LIF e dati LIF (NFS, CIFS)	DNS	DNS
NDMP	18600–18699	TCP	Gestione dei nodi LIF	Server di destinazione	Copia NDMP
SMTP	25	TCP	Gestione dei nodi LIF	Server di posta	Avvisi SMTP, possono essere utilizzati per AutoSupport
SNMP	161	TCP	Gestione dei nodi LIF	Monitorare il server	Monitoraggio tramite trappole SNMP
	161	UDP	Gestione dei nodi LIF	Monitorare il server	Monitoraggio tramite trappole SNMP
	162	TCP	Gestione dei nodi LIF	Monitorare il server	Monitoraggio tramite trappole SNMP
	162	UDP	Gestione dei nodi LIF	Monitorare il server	Monitoraggio tramite trappole SNMP
SnapMirror	11104	TCP	Intercluster LIF	LIF intercluster ONTAP	Gestione delle sessioni di comunicazione intercluster per SnapMirror
	11105	TCP	Intercluster LIF	LIF intercluster ONTAP	Trasferimento dati SnapMirror
Registro di sistema	514	UDP	Gestione dei nodi LIF	Server Syslog	Messaggi di inoltro Syslog

Requisiti per l'agente della console

Se non hai ancora creato un agente Console, dovresti anche esaminare i requisiti di rete per l'agente Console.

- "Visualizza i requisiti di rete per l'agente della console"
- "Regole del gruppo di sicurezza in Azure"

Argomenti correlati

- "Verifica la configurazione AutoSupport per Cloud Volumes ONTAP"
- "Scopri di più sulle porte interne ONTAP" .

Configurare Cloud Volumes ONTAP per utilizzare una chiave gestita dal cliente in Azure

I dati vengono crittografati automaticamente su Cloud Volumes ONTAP in Azure utilizzando Azure Storage Service Encryption con una chiave gestita da Microsoft. Ma puoi anche utilizzare la tua chiave di crittografia seguendo i passaggi descritti in questa pagina.

Panoramica sulla crittografia dei dati

I dati Cloud Volumes ONTAP vengono crittografati automaticamente in Azure utilizzando "Crittografia del servizio di archiviazione di Azure" . L'implementazione predefinita utilizza una chiave gestita da Microsoft. Non è richiesta alcuna configurazione.

Se si desidera utilizzare una chiave gestita dal cliente con Cloud Volumes ONTAP, è necessario completare i seguenti passaggi:

1. Da Azure, crea un archivio chiavi e quindi genera una chiave in tale archivio.
2. Dalla NetApp Console, utilizzare l'API per creare un sistema Cloud Volumes ONTAP che utilizzi la chiave.

Come vengono crittografati i dati

La console utilizza un set di crittografia del disco, che consente la gestione delle chiavi di crittografia con dischi gestiti e non con blob di pagine. Anche tutti i nuovi dischi dati utilizzano lo stesso set di crittografia del disco. Le versioni precedenti utilizzeranno la chiave gestita da Microsoft anziché quella gestita dal cliente.

Dopo aver creato un sistema Cloud Volumes ONTAP configurato per utilizzare una chiave gestita dal cliente, i dati di Cloud Volumes ONTAP vengono crittografati come segue.

Configurazione Cloud Volumes ONTAP	Dischi di sistema utilizzati per la crittografia delle chiavi	Dischi dati utilizzati per la crittografia delle chiavi
Nodo singolo	• Stivale • Nucleo • NVRAM	• Radice • Dati

Configurazione Cloud Volumes ONTAP	Dischi di sistema utilizzati per la crittografia delle chiavi	Dischi dati utilizzati per la crittografia delle chiavi
Zona di disponibilità singola di Azure HA con blob di pagine	• Stivale • Nucleo • NVRAM	Nessuno
Zona di disponibilità singola di Azure HA con dischi gestiti condivisi	• Stivale • Nucleo • NVRAM	• Radice • Dati
Zone di disponibilità multiple di Azure HA con dischi gestiti condivisi	• Stivale • Nucleo • NVRAM	• Radice • Dati

Tutti gli account di archiviazione di Azure per Cloud Volumes ONTAP vengono crittografati tramite una chiave gestita dal cliente. Se si desidera crittografare gli account di archiviazione durante la loro creazione, è necessario creare e fornire l'ID della risorsa nella richiesta di creazione Cloud Volumes ONTAP . Questo vale per tutti i tipi di distribuzioni. Se non lo fornisci, gli account di archiviazione saranno comunque crittografati, ma la Console crea prima gli account di archiviazione con la crittografia della chiave gestita da Microsoft e poi aggiorna gli account di archiviazione per utilizzare la chiave gestita dal cliente.

Rotazione delle chiavi in Cloud Volumes ONTAP

Quando si configurano le chiavi di crittografia, è necessario utilizzare il portale di Azure per impostare e abilitare la rotazione automatica delle chiavi. La creazione e l'abilitazione di una nuova versione delle chiavi di crittografia garantisce che Cloud Volumes ONTAP possa rilevare e utilizzare automaticamente la versione più recente della chiave per la crittografia, garantendo la sicurezza dei dati senza la necessità di un intervento manuale.

Per informazioni sulla configurazione delle chiavi e sull'impostazione della rotazione delle chiavi, fare riferimento ai seguenti argomenti della documentazione di Microsoft Azure:

- "Configurare la rotazione automatica delle chiavi crittografiche in Azure Key Vault"
- "Azure PowerShell - Abilita le chiavi gestite dal cliente"

> Dopo aver configurato le chiavi, assicurati di aver selezionato "*Abilita rotazione automatica*" , in modo che Cloud Volumes ONTAP possa utilizzare le nuove chiavi quando quelle precedenti scadono. Se non si abilita questa opzione nel portale di Azure, Cloud Volumes ONTAP non potrà rilevare automaticamente le nuove chiavi, il che potrebbe causare problemi con il provisioning dello storage.

Creare un'identità gestita assegnata dall'utente

Hai la possibilità di creare una risorsa denominata identità gestita assegnata dall'utente. In questo modo è possibile crittografare gli account di archiviazione quando si crea un sistema Cloud Volumes ONTAP . Si consiglia di creare questa risorsa prima di creare un archivio chiavi e generare una chiave.

La risorsa ha il seguente ID: `userassignedidentity` .

Passi

1. In Azure, vai a Servizi di Azure e seleziona **Identità gestite**.
2. Fare clic su **Crea**.
3. Fornire i seguenti dettagli:
   - **Abbonamento**: Scegli un abbonamento. Si consiglia di scegliere lo stesso abbonamento dell'agente della Console.
   - **Gruppo di risorse**: utilizza un gruppo di risorse esistente o creane uno nuovo.
   - **Regione**: facoltativamente, selezionare la stessa regione dell'agente Console.
   - **Nome**: inserisci un nome per la risorsa.
4. Facoltativamente, aggiungi dei tag.
5. Fare clic su **Crea**.

Crea un archivio di chiavi e genera una chiave

L'archivio delle chiavi deve risiedere nella stessa sottoscrizione e regione di Azure in cui si prevede di creare il sistema Cloud Volumes ONTAP .

Se tuha creato un'identità gestita assegnata dall'utente durante la creazione del key vault, dovresti anche creare una policy di accesso per il key vault.

Passi

1. "Crea un archivio chiavi nel tuo abbonamento Azure" .

   Tenere presente i seguenti requisiti per il key vault:

   - Il key vault deve risiedere nella stessa regione del sistema Cloud Volumes ONTAP .
   - Dovrebbero essere abilitate le seguenti opzioni:
     - **Eliminazione temporanea** (questa opzione è abilitata per impostazione predefinita, ma *non* deve essere disabilitata)
     - **Protezione anti-spurgo**
     - **Azure Disk Encryption per la crittografia dei volumi** (per sistemi a nodo singolo, coppia HA in più zone e distribuzioni HA in una sola zona di disponibilità)

       L'utilizzo delle chiavi di crittografia gestite dal cliente di Azure è subordinato all'abilitazione della crittografia del disco di Azure per l'insieme di credenziali delle chiavi.
   - Se hai creato un'identità gestita assegnata dall'utente, dovresti abilitare la seguente opzione:
     - **Politica di accesso al caveau**
2. Se hai selezionato Criterio di accesso al vault, fai clic su Crea per creare un criterio di accesso per il vault delle chiavi. In caso contrario, passare al passaggio 3.
   a. Selezionare le seguenti autorizzazioni:
      - Ottenere
      - lista
      - decifrare

        - crittografare
        - chiave di scarto
        - chiave di avvolgimento
        - verificare
        - cartello
    b. Selezionare l'identità gestita (risorsa) assegnata dall'utente come principale.
    c. Rivedere e creare la policy di accesso.
3. "Genera una chiave nel key vault" .

    Notare i seguenti requisiti per la chiave:

    - Il tipo di chiave deve essere **RSA**.
    - La dimensione consigliata della chiave RSA è **2048**, ma sono supportate anche altre dimensioni.

Creare un sistema che utilizzi la chiave di crittografia

Dopo aver creato il key vault e generato una chiave di crittografia, è possibile creare un nuovo sistema Cloud Volumes ONTAP configurato per utilizzare la chiave. Questi passaggi sono supportati tramite l'API.

Autorizzazioni richieste

Se si desidera utilizzare una chiave gestita dal cliente con un sistema Cloud Volumes ONTAP a nodo singolo, assicurarsi che l'agente della console disponga delle seguenti autorizzazioni:

```
"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"
```

"Visualizza l'elenco più recente delle autorizzazioni"

Passi

1. Ottieni l'elenco degli archivi di chiavi nella tua sottoscrizione di Azure utilizzando la seguente chiamata API.

    Per una coppia HA: `GET /azure/ha/metadata/vaults`

    Per nodo singolo: `GET /azure/vsa/metadata/vaults`

    Prendi nota di **nome** e **resourceGroup**. Sarà necessario specificare tali valori nel passaggio successivo.

    "Scopri di più su questa chiamata API" .

2. Ottieni l'elenco delle chiavi all'interno del vault utilizzando la seguente chiamata API.

    Per una coppia HA: `GET /azure/ha/metadata/keys-vault`

Per nodo singolo: `GET /azure/vsa/metadata/keys-vault`

Prendi nota di **keyName**. Sarà necessario specificare tale valore (insieme al nome del vault) nel passaggio successivo.

"Scopri di più su questa chiamata API" .

3. Creare un sistema Cloud Volumes ONTAP utilizzando la seguente chiamata API.

   a. Per una coppia HA:

      `POST /azure/ha/working-environments`

      Il corpo della richiesta deve includere i seguenti campi:

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

      Includi il `"userAssignedIdentity": " userAssignedIdentityId"` campo se hai creato questa risorsa per utilizzarla per la crittografia dell'account di archiviazione.

      "Scopri di più su questa chiamata API" .

   b. Per un sistema a nodo singolo:

      `POST /azure/vsa/working-environments`

      Il corpo della richiesta deve includere i seguenti campi:

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

      Includi il `"userAssignedIdentity": " userAssignedIdentityId"` campo se hai creato questa risorsa per utilizzarla per la crittografia dell'account di archiviazione.

   "Scopri di più su questa chiamata API" .

Risultato

Hai un nuovo sistema Cloud Volumes ONTAP configurato per utilizzare la chiave gestita dal cliente per la crittografia dei dati.

Configurare le licenze per Cloud Volumes ONTAP in Azure

Dopo aver deciso quale opzione di licenza utilizzare con Cloud Volumes ONTAP, sono

necessari alcuni passaggi prima di poter scegliere tale opzione di licenza durante la creazione di un nuovo sistema.

Freemium

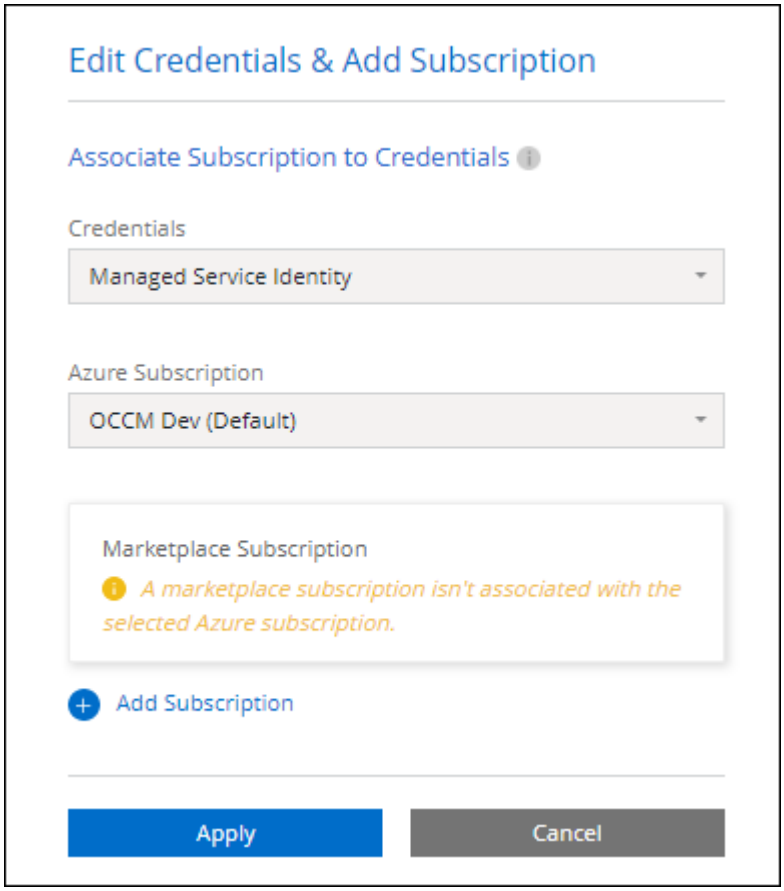
Seleziona l'offerta Freemium per utilizzare Cloud Volumes ONTAP gratuitamente con una capacità fornita fino a 500 GiB. "Scopri di più sull'offerta Freemium" .

Passi

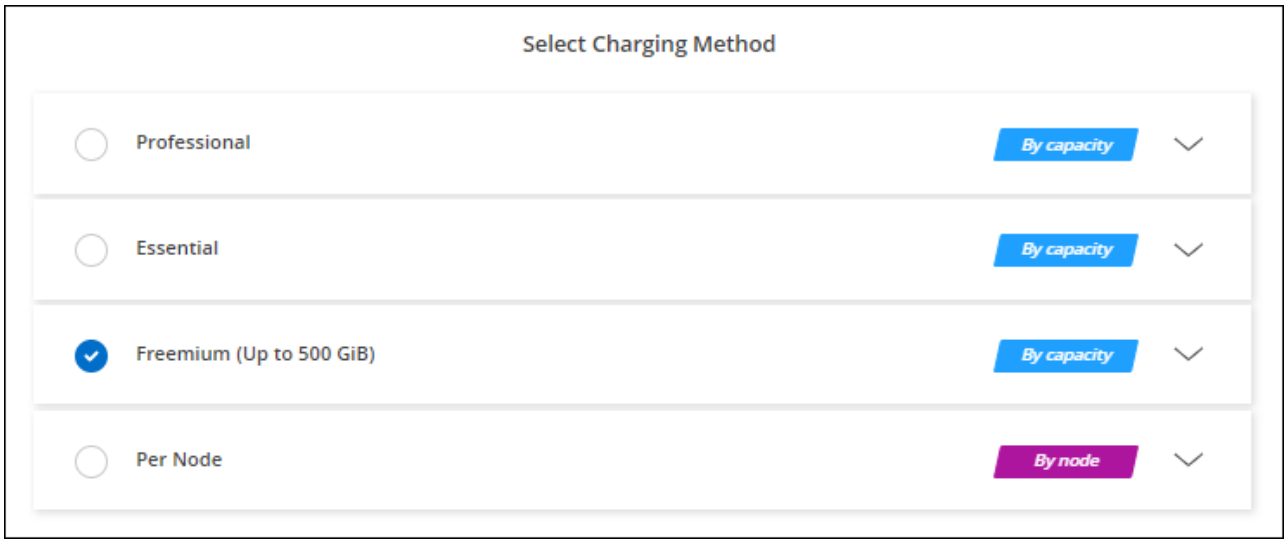
1. Dal menu di navigazione a sinistra della NetApp Console, selezionare **Storage > Gestione**.
2. Nella pagina **Sistemi**, fare clic su **Aggiungi sistema** e seguire i passaggi.

   a. Nella pagina **Dettagli e credenziali**, fare clic su **Modifica credenziali > Aggiungi sottoscrizione** e quindi seguire le istruzioni per sottoscrivere l'offerta con pagamento in base al consumo in Azure Marketplace.

      Non ti verrà addebitato alcun costo tramite l'abbonamento al marketplace a meno che tu non superi i 500 GiB di capacità fornita, momento in cui il sistema verrà automaticamente convertito in"Pacchetto essenziale" .



   a. Dopo essere tornato alla Console, seleziona **Freemium** quando arrivi alla pagina dei metodi di addebito.



"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in Azure" .

Licenza basata sulla capacità

Le licenze basate sulla capacità consentono di pagare Cloud Volumes ONTAP per TiB di capacità. Le licenze basate sulla capacità sono disponibili sotto forma di *pacchetto*: il pacchetto Essentials o il pacchetto Professional.

I pacchetti Essentials e Professional sono disponibili con i seguenti modelli di consumo o opzioni di acquisto:

- Una licenza (Bring Your Own License (BYOL)) acquistata da NetApp
- Un abbonamento orario con pagamento in base al consumo (PAYGO) da Azure Marketplace
- Un contratto annuale

"Scopri di più sulle licenze basate sulla capacità" .

Le sezioni seguenti descrivono come iniziare a utilizzare ciascuno di questi modelli di consumo.

BYOL

Paga in anticipo acquistando una licenza (BYOL) da NetApp per distribuire i sistemi Cloud Volumes ONTAP in qualsiasi provider cloud.

NetApp ha limitato l'acquisto, l'estensione e il rinnovo delle licenze BYOL. Per ulteriori informazioni, consulta "Disponibilità limitata delle licenze BYOL per Cloud Volumes ONTAP" .

Passi

1. "Contatta NetApp Sales per ottenere una licenza"
2. "Aggiungi il tuo account del sito di supporto NetApp alla console"

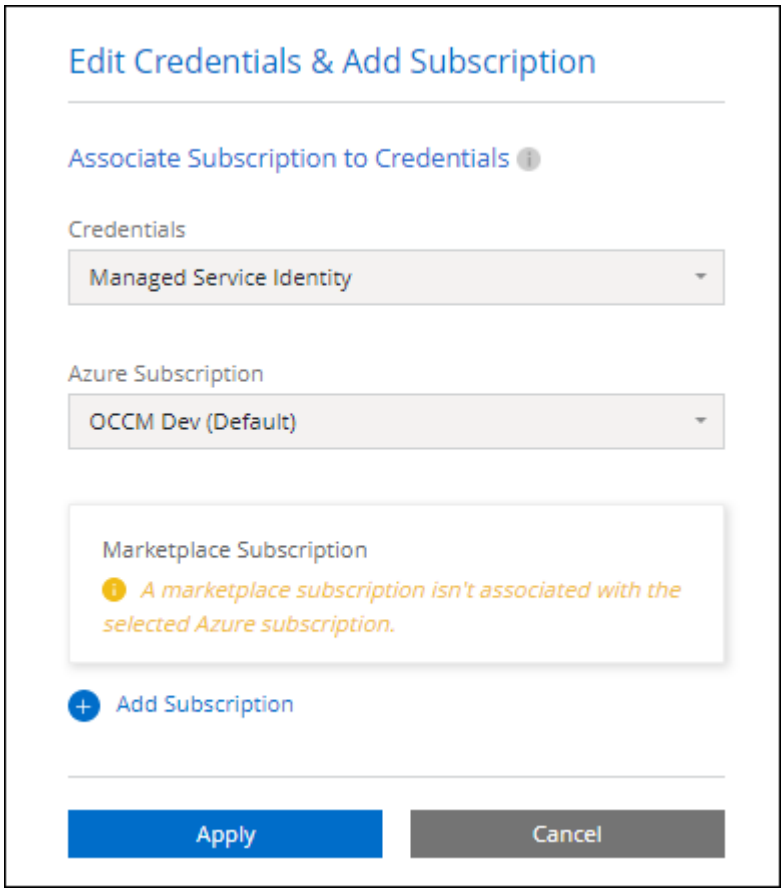
   La Console interroga automaticamente il servizio licenze di NetApp per ottenere dettagli sulle licenze associate al tuo account NetApp Support Site. Se non ci sono errori, la Console aggiunge automaticamente le licenze alla Console.

   La licenza deve essere disponibile nella Console prima di poterla utilizzare con Cloud Volumes ONTAP. Se necessario, puoi"aggiungere manualmente la licenza alla Console" .

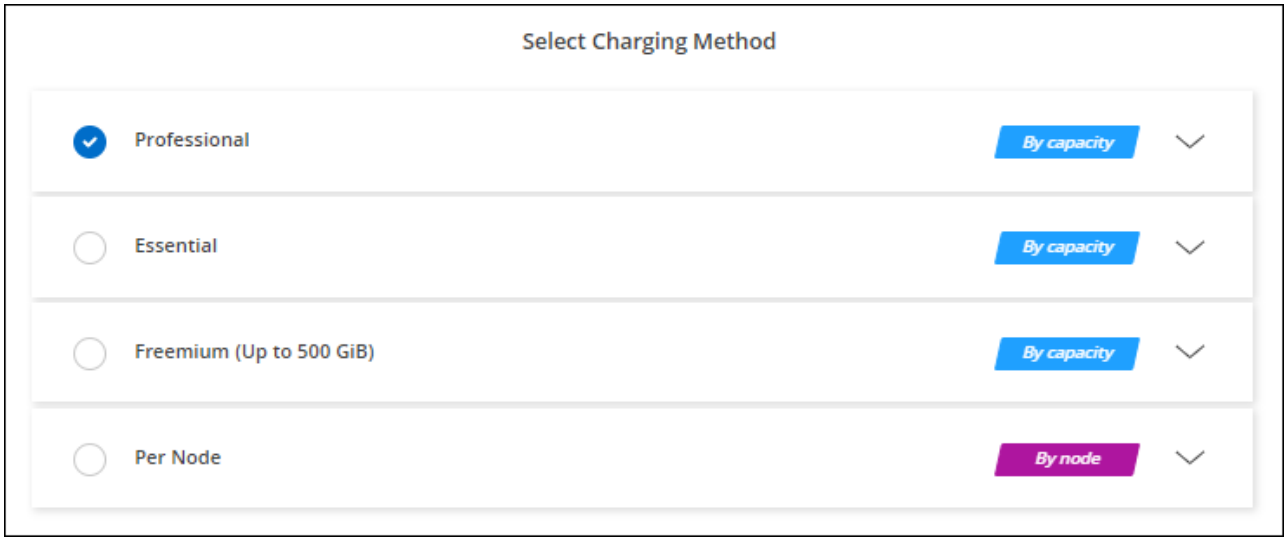
3. Nella pagina **Sistemi**, fare clic su **Aggiungi sistema** e seguire i passaggi.

   a. Nella pagina **Dettagli e credenziali**, fare clic su **Modifica credenziali > Aggiungi sottoscrizione** e quindi seguire le istruzioni per sottoscrivere l'offerta con pagamento in base al consumo in Azure Marketplace.

      La licenza acquistata da NetApp viene sempre addebitata per prima, ma ti verrà addebitata la tariffa oraria del marketplace se superi la capacità della licenza o se scade il termine della licenza.



   a. Dopo essere tornati alla Console, selezionate un pacchetto basato sulla capacità quando raggiungete la pagina dei metodi di ricarica.



"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in Azure" .

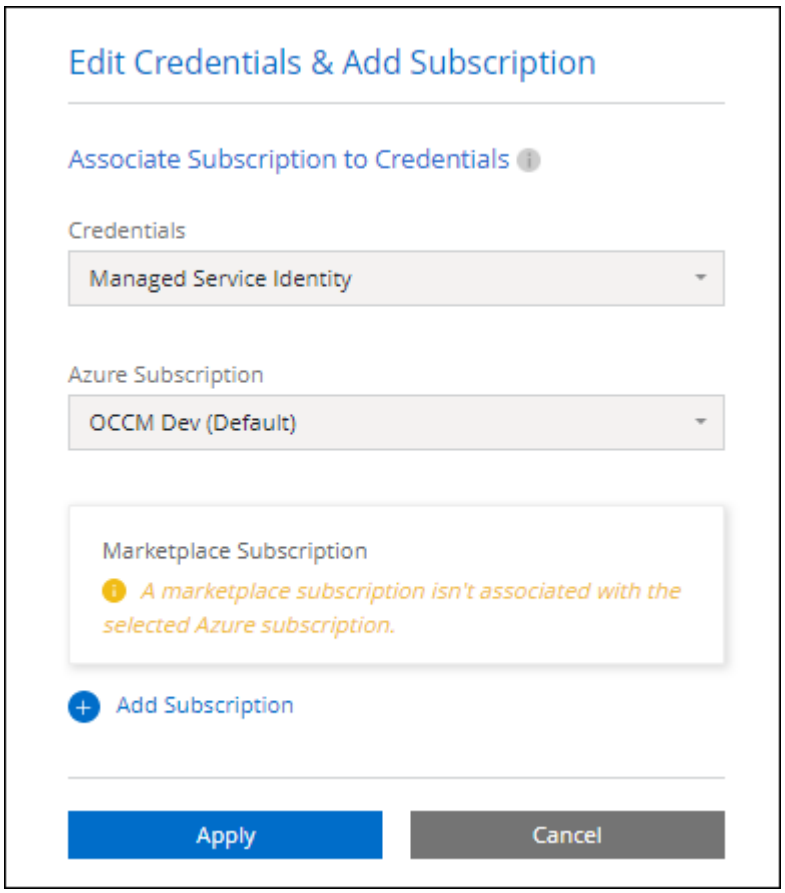
Abbonamento PAYGO

Paga a ore sottoscrivendo l'offerta dal marketplace del tuo provider cloud.

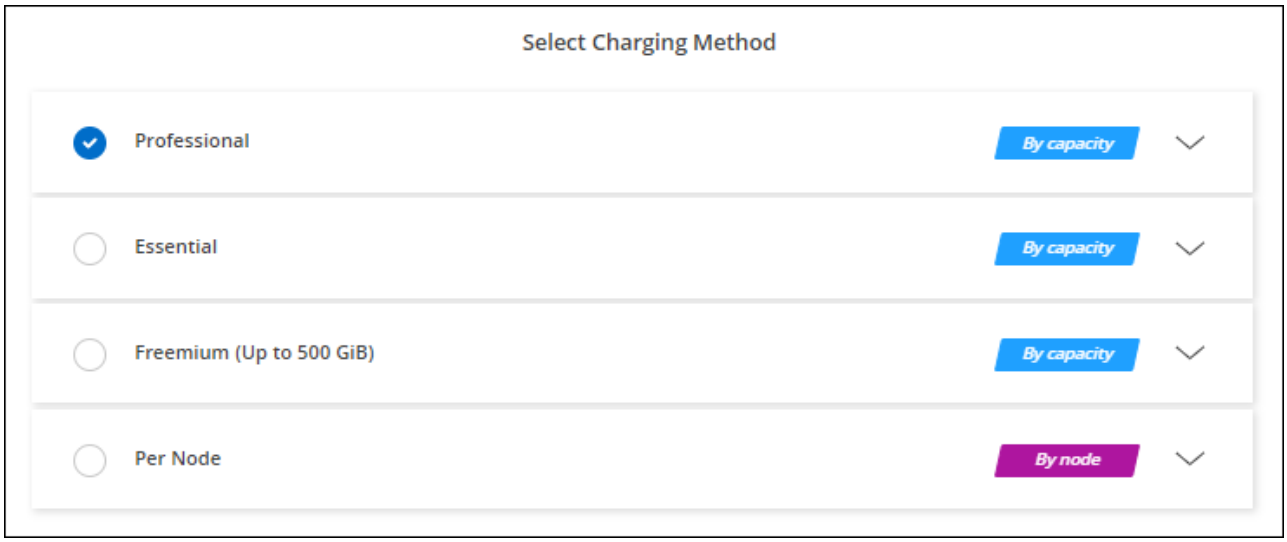
Quando si crea un sistema Cloud Volumes ONTAP , la Console richiede di sottoscrivere il contratto disponibile in Azure Marketplace. Tale abbonamento viene poi associato al sistema di addebito. È possibile utilizzare lo stesso abbonamento per sistemi aggiuntivi.

Passi

1. Dal menu di navigazione a sinistra, seleziona **Archiviazione > Gestione**.
2. Nella pagina **Sistemi**, fare clic su **Aggiungi sistema** e seguire i passaggi.
   a. Nella pagina **Dettagli e credenziali**, fare clic su **Modifica credenziali > Aggiungi sottoscrizione** e quindi seguire le istruzioni per sottoscrivere l'offerta con pagamento in base al consumo in Azure Marketplace.



   b. Dopo essere tornati alla Console, selezionate un pacchetto basato sulla capacità quando raggiungete la pagina dei metodi di ricarica.



"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in Azure" .

Puoi gestire gli abbonamenti di Azure Marketplace associati ai tuoi account Azure dalla pagina Impostazioni > Credenziali. "Scopri come gestire i tuoi account e abbonamenti Azure"

Contratto annuale

Paga annualmente Cloud Volumes ONTAP acquistando un contratto annuale.

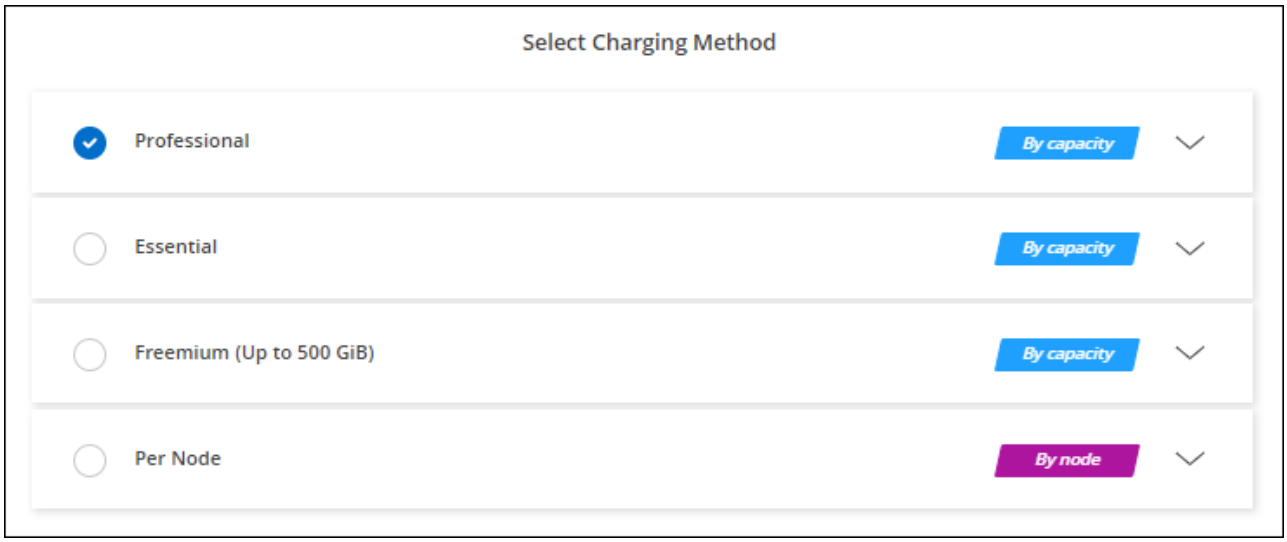
Passi

1. Contatta il tuo rappresentante commerciale NetApp per acquistare un contratto annuale.

   Il contratto è disponibile come offerta *privata* in Azure Marketplace.

   Dopo che NetApp avrà condiviso con te l'offerta privata, potrai selezionare il piano annuale quando ti iscrivi da Azure Marketplace durante la creazione del sistema.

2. Nella pagina **Sistemi**, fare clic su **Aggiungi sistema** e seguire i passaggi.
   a. Nella pagina **Dettagli e credenziali**, fare clic su **Modifica credenziali > Aggiungi abbonamento > Continua**.
   b. Nel portale di Azure, seleziona il piano annuale condiviso con il tuo account Azure, quindi fai clic su **Sottoscrivi**.
   c. Dopo essere tornati alla Console, selezionate un pacchetto basato sulla capacità quando raggiungete la pagina dei metodi di ricarica.



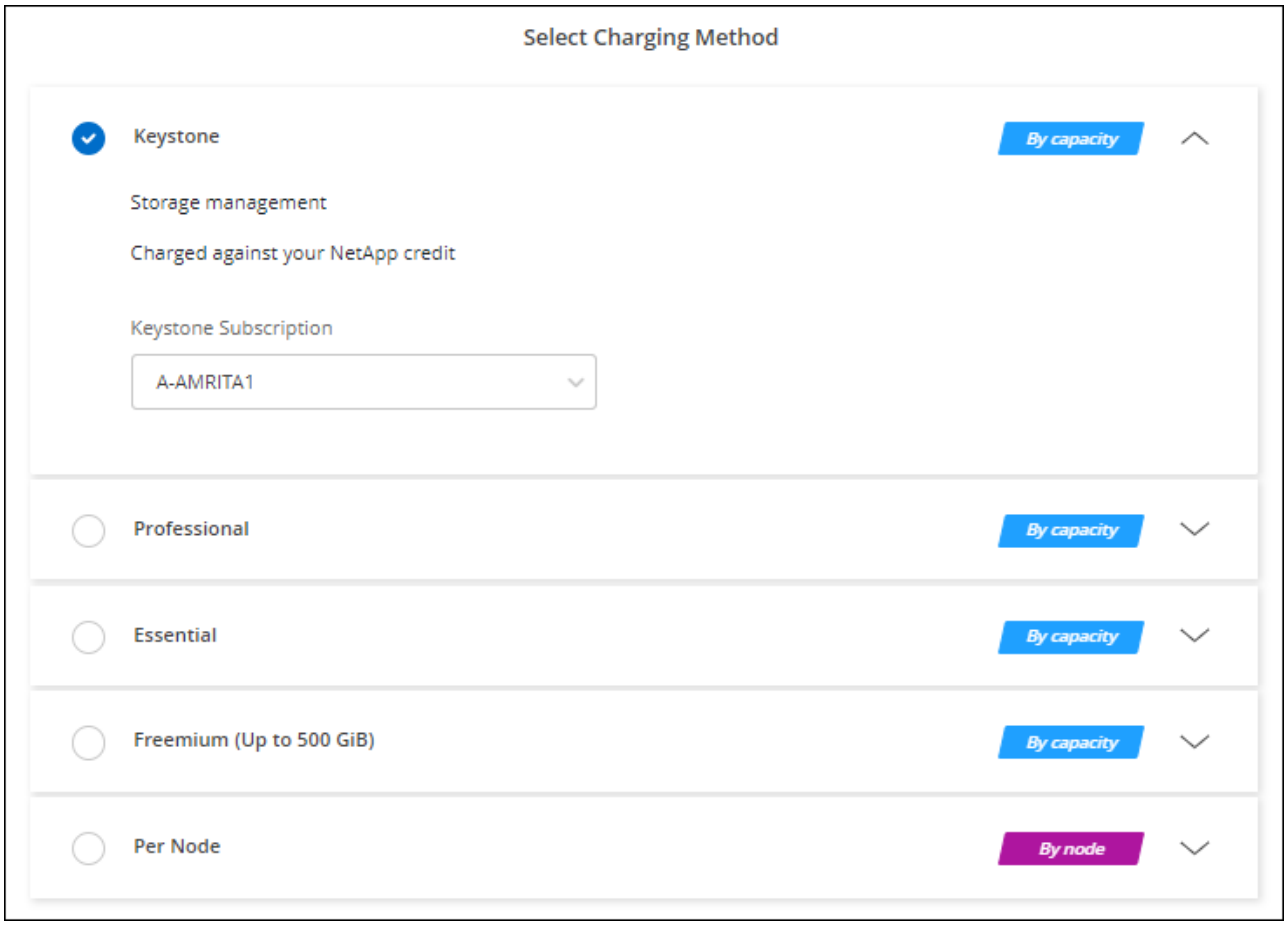
"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in Azure" .

Abbonamento Keystone

Un abbonamento Keystone è un servizio basato su un abbonamento con pagamento in base alla crescita. "Scopri di più sugli abbonamenti NetApp Keystone" .

Passi

1. Se non hai ancora un abbonamento, "contattare NetApp"
2. Contatta NetApp per autorizzare il tuo account utente nella Console con uno o più abbonamenti Keystone .
3. Dopo che NetApp autorizza il tuo account,"collega i tuoi abbonamenti per utilizzarli con Cloud Volumes ONTAP" .
4. Nella pagina **Sistemi**, fare clic su **Aggiungi sistema** e seguire i passaggi.
   a. Quando ti viene richiesto di scegliere un metodo di addebito, seleziona il metodo di addebito Keystone Subscription.



"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in Azure" .

Licenza basata su nodi

Una licenza basata su nodi è la licenza di precedente generazione per Cloud Volumes ONTAP. Una licenza basata su nodi può essere acquistata da NetApp (BYOL) ed è disponibile per i rinnovi di licenza solo in casi specifici. Per informazioni, fare riferimento a:

- "Fine della disponibilità delle licenze basate su nodi"
- "Fine della disponibilità delle licenze basate sui nodi"
- "Convertire una licenza basata su nodi in una licenza basata sulla capacità"

Abilita la modalità ad alta disponibilità per Cloud Volumes ONTAP in Azure

È consigliabile abilitare la modalità ad alta disponibilità (HA) di Microsoft Azure per ridurre i tempi di failover non pianificati e abilitare il supporto NFSv4 per Cloud Volumes ONTAP. Se abiliti questa modalità, i nodi HA di Cloud Volumes ONTAP possono raggiungere un recovery time objective (RTO) basso (60 secondi) durante i failover non pianificati sui client CIFS e NFSv4.

A partire da Cloud Volumes ONTAP 9.10.1, abbiamo ridotto il tempo di failover non pianificato per le coppie Cloud Volumes ONTAP HA in esecuzione in Microsoft Azure e aggiunto il supporto per NFSv4. Per rendere disponibili questi miglioramenti a Cloud Volumes ONTAP, è necessario abilitare la funzionalità di alta disponibilità nella sottoscrizione di Azure.

Informazioni su questo compito

NetApp Console ti richiede questi dettagli quando la funzionalità deve essere abilitata su un abbonamento Azure. Nota quanto segue:

- Non ci sono problemi con l'elevata disponibilità della coppia Cloud Volumes ONTAP HA. Questa funzionalità di Azure interagisce con ONTAP per ridurre i tempi di interruzione delle applicazioni osservati dal client per i protocolli NFS, derivanti da eventi di failover non pianificati.
- L'abilitazione di questa funzionalità non comporta interruzioni per le coppie Cloud Volumes ONTAP HA.
- L'abilitazione di questa funzionalità nell'abbonamento Azure non causa problemi alle altre VM.
- Cloud Volumes ONTAP utilizza un Azure Load Balancer interno durante i failover dei LIF di gestione del cluster e SVM sui client CIFS e NFS.
- Quando la modalità HA è abilitata, la console esegue la scansione del sistema ogni 12 ore per aggiornare le regole interne di Azure Load Balancer.

Passi

Un utente Azure con privilegi di *Owner* può abilitare la funzionalità dall'Azure CLI.

1. "Accedi ad Azure Cloud Shell dal portale di Azure"
2. Registra la funzionalità della modalità ad alta disponibilità:

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

3. Facoltativamente, verificare che la funzionalità sia ora registrata:

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

L'interfaccia della riga di comando di Azure dovrebbe restituire un risultato simile al seguente:

```
{
  "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"
}
```

Link correlati

1. "Microsoft Azure documentation: panoramica delle porte ad alta disponibilità"
2. "Microsoft Azure documentazione: Introduzione all'Azure CLI"

Abilita VMOrchestratorZonalMultiFD per Cloud Volumes ONTAP in Azure

Per distribuire istanze di VM in zone di disponibilità singole (AZ) con archiviazione ridondante locale (LRS), è necessario attivare Microsoft `Microsoft.Compute/VMOrchestratorZonalMultiFD` funzionalità per i tuoi abbonamenti. In modalità ad alta disponibilità (HA), questa funzionalità semplifica la distribuzione dei nodi in domini di errore separati nella stessa zona di disponibilità.

Se non si attiva questa funzionalità, la distribuzione zonale non avviene e diventa effettiva la precedente distribuzione non zonale LRS.

Per informazioni sulla distribuzione delle VM in una singola zona di disponibilità, fare riferimento a"Coppie ad alta disponibilità in Azure" .

Eseguire questi passaggi come utente con privilegi di "Proprietario":

Passi

1. Accedi ad Azure Cloud Shell dal portale di Azure. Per informazioni fare riferimento al "Documentazione di Microsoft Azure: Introduzione ad Azure Cloud Shell" .
2. Registrati per il `Microsoft.Compute/VMOrchestratorZonalMultiFD` funzionalità eseguendo questo comando:

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

3. Verificare lo stato della registrazione e il campione di output:

   ```
   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": "Registrato" }, "type": "Microsoft.Features/providers/features" }
   ```

Avvia Cloud Volumes ONTAP in Azure

È possibile avviare un sistema a nodo singolo o una coppia HA in Azure creando un sistema Cloud Volumes ONTAP nella NetApp Console.

Prima di iniziare

Prima di iniziare, ti occorre quanto segue.

- Un agente Console attivo e funzionante.
  - Dovresti avere un "Agente console associato al tuo sistema" .
  - "Dovresti essere pronto a lasciare l'agente della console sempre in esecuzione" .

- Una comprensione della configurazione che si desidera utilizzare.

  Dovresti farti fornire dall'amministratore una configurazione pianificata e i dettagli necessari sulla rete di Azure. Per ulteriori informazioni, fare riferimento a "Pianificazione della configurazione Cloud Volumes ONTAP" .

- Una comprensione di ciò che è necessario per impostare la licenza per Cloud Volumes ONTAP.

  "Scopri come impostare le licenze" .

Informazioni su questo compito

Quando la console crea un sistema Cloud Volumes ONTAP in Azure, crea diversi oggetti di Azure, ad esempio un gruppo di risorse, interfacce di rete e account di archiviazione. Alla fine della procedura guidata è possibile visualizzare un riepilogo delle risorse.

> **Potenziale di perdita di dati**
>
> La procedura consigliata è quella di utilizzare un nuovo gruppo di risorse dedicato per ciascun sistema Cloud Volumes ONTAP .
>
> Si sconsiglia di distribuire Cloud Volumes ONTAP in un gruppo di risorse condiviso esistente a causa del rischio di perdita di dati. Sebbene la Console possa rimuovere le risorse Cloud Volumes ONTAP da un gruppo di risorse condivise in caso di errore di distribuzione o eliminazione, un utente di Azure potrebbe eliminare accidentalmente le risorse Cloud Volumes ONTAP da un gruppo di risorse condivise.

Avvia un sistema Cloud Volumes ONTAP a nodo singolo in Azure

Se si desidera avviare un sistema Cloud Volumes ONTAP a nodo singolo in Azure, è necessario creare un sistema a nodo singolo nella Console.

Passi

1. Dal menu di navigazione a sinistra, seleziona **Archiviazione > Gestione**.
2. Nella pagina **Sistemi**, fare clic su **Aggiungi sistema** e seguire le istruzioni.
3. **Scegli una posizione**: seleziona **Microsoft Azure** e * Cloud Volumes ONTAP Single Node*.
4. Se richiesto, "creare un agente Console" .
5. **Dettagli e credenziali**: facoltativamente, modifica le credenziali e la sottoscrizione di Azure, specifica un nome per il cluster, aggiungi tag se necessario e quindi specifica le credenziali.

   Nella tabella seguente vengono descritti i campi per i quali potrebbe essere necessaria una guida:

Campo	Descrizione
Nome del sistema	La console utilizza il nome del sistema per denominare sia il sistema Cloud Volumes ONTAP sia la macchina virtuale di Azure. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di sicurezza predefinito.

Campo	Descrizione
Tag del gruppo di risorse	I tag sono metadati per le risorse di Azure. Quando si immettono tag in questo campo, la Console li aggiunge al gruppo di risorse associato al sistema Cloud Volumes ONTAP . Quando si crea un sistema, è possibile aggiungere fino a quattro tag dall'interfaccia utente, per poi aggiungerne altri dopo la creazione. Tieni presente che l'API non ti limita a quattro tag quando crei un sistema. Per informazioni sui tag, fare riferimento a "Documentazione di Microsoft Azure: utilizzo dei tag per organizzare le risorse di Azure" .
Nome utente e password	Queste sono le credenziali per l'account amministratore del cluster Cloud Volumes ONTAP . È possibile utilizzare queste credenziali per connettersi a Cloud Volumes ONTAP tramite ONTAP System Manager o ONTAP CLI. Mantenere il nome utente predefinito *admin* oppure modificarlo con un nome utente personalizzato.
Modifica credenziali	È possibile scegliere credenziali Azure diverse e un abbonamento Azure diverso da utilizzare con questo sistema Cloud Volumes ONTAP . Per distribuire un sistema Cloud Volumes ONTAP con pagamento in base al consumo, è necessario associare una sottoscrizione di Azure Marketplace alla sottoscrizione di Azure selezionata. "Scopri come aggiungere le credenziali" .

6. **Servizi**: abilita o disabilita i singoli servizi che desideri o non desideri utilizzare con Cloud Volumes ONTAP.
   - "Scopri di più sulla NetApp Data Classification"
   - "Scopri di più su NetApp Backup and Recovery"

   Se si desidera utilizzare WORM e il data tiering, è necessario disabilitare Backup e Recovery e distribuire un sistema Cloud Volumes ONTAP con versione 9.8 o successiva.

7. **Posizione**: selezionare una regione, una zona di disponibilità, una rete virtuale e una subnet, quindi selezionare la casella di controllo per confermare la connettività di rete tra l'agente della console e la posizione di destinazione.

   Per le regioni della Cina, le distribuzioni a nodo singolo sono supportate solo in Cloud Volumes ONTAP 9.12.1 GA e 9.13.0 GA. È possibile aggiornare queste versioni a patch e release successive di Cloud Volumes ONTAP come"supportato in Azure" . Se desideri distribuire versioni successive di Cloud Volumes ONTAP nelle regioni della Cina, contatta l'assistenza NetApp . Nelle regioni della Cina sono supportate solo le licenze acquistate direttamente da NetApp ; gli abbonamenti al marketplace non sono disponibili.

8. **Connettività**: scegli un gruppo di risorse nuovo o esistente e poi scegli se utilizzare il gruppo di sicurezza predefinito o il tuo.

   Nella tabella seguente vengono descritti i campi per i quali potrebbe essere necessaria una guida:

Campo	Descrizione
Gruppo di risorse	Crea un nuovo gruppo di risorse per Cloud Volumes ONTAP oppure utilizza un gruppo di risorse esistente. La procedura consigliata è quella di utilizzare un nuovo gruppo di risorse dedicato per Cloud Volumes ONTAP. Sebbene sia possibile distribuire Cloud Volumes ONTAP in un gruppo di risorse condiviso esistente, questa operazione non è consigliata a causa del rischio di perdita di dati. Per maggiori dettagli, vedere l'avviso sopra. Se l'account Azure che stai utilizzando ha il "permessi richiesti" , la Console rimuove le risorse Cloud Volumes ONTAP da un gruppo di risorse, in caso di errore di distribuzione o eliminazione.
Gruppo di sicurezza generato	Se lasci che sia la Console a generare il gruppo di sicurezza per te, devi scegliere come consentire il traffico: • Se si sceglie **Solo VNet selezionata**, l'origine del traffico in entrata è l'intervallo di subnet della VNet selezionata e l'intervallo di subnet della VNet in cui risiede l'agente della console. Questa è l'opzione consigliata. • Se si seleziona **Tutte le reti virtuali**, l'origine del traffico in entrata è l'intervallo IP 0.0.0.0/0.
Utilizzare esistente	Se si sceglie un gruppo di sicurezza esistente, questo deve soddisfare i requisiti di Cloud Volumes ONTAP . "Visualizza il gruppo di sicurezza predefinito" .

9. **Metodi di addebito e account NSS**: specifica quale opzione di addebito desideri utilizzare con questo sistema, quindi specifica un account del sito di supporto NetApp .
   - "Scopri le opzioni di licenza per Cloud Volumes ONTAP" .
   - "Scopri come impostare le licenze" .
10. **Pacchetti preconfigurati**: seleziona uno dei pacchetti per distribuire rapidamente un sistema Cloud Volumes ONTAP oppure fai clic su **Crea la mia configurazione**.

    Se si sceglie uno dei pacchetti, è sufficiente specificare un volume e quindi rivedere e approvare la configurazione.

11. **Licenze**: se necessario, modifica la versione di Cloud Volumes ONTAP e seleziona un tipo di macchina virtuale.

    Se per la versione selezionata è disponibile una versione Release Candidate, una versione General Availability o una patch più recente, BlueXP aggiorna il sistema a tale versione durante la creazione dell'ambiente di lavoro. Ad esempio, l'aggiornamento avviene se si seleziona Cloud Volumes ONTAP 9.16.1 P3 e 9.16.1 P4 è disponibile. L'aggiornamento non avviene da una versione all'altra, ad esempio dalla 9.15 alla 9.16.

12. **Iscriviti da Azure Marketplace**: questa pagina viene visualizzata se la console non è riuscita ad abilitare le distribuzioni programmatiche di Cloud Volumes ONTAP. Seguire i passaggi elencati sullo schermo. fare riferimento a "Distribuzione programmatica dei prodotti Marketplace" per maggiori informazioni.
13. **Risorse di archiviazione sottostanti**: scegli le impostazioni per l'aggregato iniziale: un tipo di disco, una

dimensione per ciascun disco e se abilitare la suddivisione dei dati in livelli nell'archiviazione BLOB.

Notare quanto segue:

- Se l'accesso pubblico al tuo account di archiviazione è disabilitato all'interno della VNet, non puoi abilitare la suddivisione in livelli dei dati nel tuo sistema Cloud Volumes ONTAP . Per informazioni, fare riferimento a"Regole del gruppo di sicurezza" .
- Il tipo di disco è per il volume iniziale. È possibile scegliere un tipo di disco diverso per i volumi successivi.
- La dimensione del disco si riferisce a tutti i dischi nell'aggregato iniziale e a tutti gli aggregati aggiuntivi creati dalla Console quando si utilizza l'opzione di provisioning semplice. È possibile creare aggregati che utilizzano dimensioni del disco diverse utilizzando l'opzione di allocazione avanzata.

  Per assistenza nella scelta del tipo e della dimensione del disco, fare riferimento a"Dimensionamento del sistema in Azure" .

- Quando si crea o si modifica un volume, è possibile scegliere una specifica politica di suddivisione in livelli del volume.
- Se si disabilita la suddivisione in livelli dei dati, è possibile abilitarla sugli aggregati successivi.

  "Scopri di più sulla suddivisione in livelli dei dati" .

14. **Velocità di scrittura e WORM**:

    a. Se lo desideri, seleziona la velocità di scrittura **Normale** o **Alta**.

       "Scopri di più sulla velocità di scrittura" .

    b. Se lo si desidera, attivare la memorizzazione WORM (write once, read many).

       Questa opzione è disponibile solo per alcuni tipi di VM. Per scoprire quali tipi di VM sono supportati, fare riferimento a"Configurazioni supportate per licenza per coppie HA" .

       WORM non può essere abilitato se il tiering dei dati è stato abilitato per Cloud Volumes ONTAP versione 9.7 e precedenti. Il ripristino o il downgrade a Cloud Volumes ONTAP 9.8 è bloccato dopo l'abilitazione di WORM e del tiering.

    "Scopri di più sullo storage WORM" .

    a. Se si attiva l'archiviazione WORM, selezionare il periodo di conservazione.

15. **Crea volume**: inserisci i dettagli per il nuovo volume o fai clic su **Salta**.

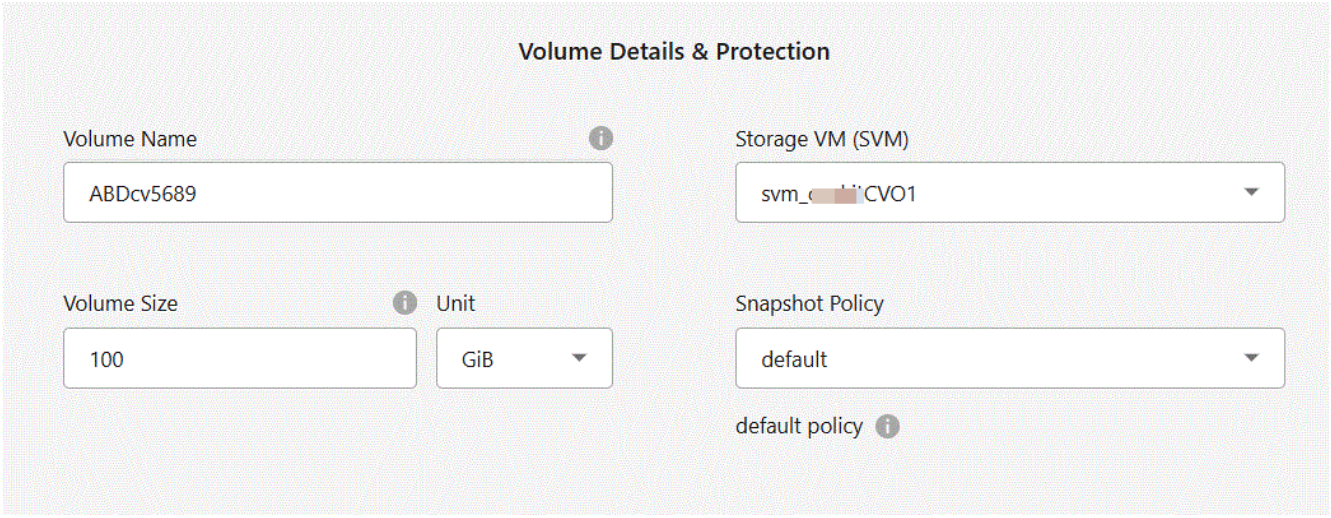
    "Scopri i protocolli e le versioni client supportati" .

    Alcuni campi di questa pagina sono autoesplicativi. Nella tabella seguente vengono descritti i campi per i quali potrebbe essere necessaria una guida:

Campo	Descrizione
Misurare	La dimensione massima che è possibile immettere dipende in larga misura dall'attivazione o meno del thin provisioning, che consente di creare un volume più grande dello spazio di archiviazione fisico attualmente disponibile.

Campo	Descrizione
Controllo degli accessi (solo per NFS)	Una policy di esportazione definisce i client nella subnet che possono accedere al volume. Per impostazione predefinita, la Console immette un valore che fornisce l'accesso a tutte le istanze nella subnet.
Autorizzazioni e utenti/gruppi (solo per CIFS)	Questi campi consentono di controllare il livello di accesso a una condivisione per utenti e gruppi (chiamati anche elenchi di controllo degli accessi o ACL). È possibile specificare utenti o gruppi Windows locali o di dominio oppure utenti o gruppi UNIX. Se si specifica un nome utente di dominio Windows, è necessario includere il dominio dell'utente utilizzando il formato dominio\nomeutente.
Politica di snapshot	Una policy di copia snapshot specifica la frequenza e il numero di copie Snapshot NetApp create automaticamente. Una copia Snapshot NetApp è un'immagine del file system in un dato momento che non ha alcun impatto sulle prestazioni e richiede uno spazio di archiviazione minimo. È possibile scegliere la policy predefinita o nessuna. Per i dati temporanei è possibile scegliere "nessuno": ad esempio, tempdb per Microsoft SQL Server.
Opzioni avanzate (solo per NFS)	Selezionare una versione NFS per il volume: NFSv3 o NFSv4.
Gruppo iniziatore e IQN (solo per iSCSI)	Le destinazioni di archiviazione iSCSI sono chiamate LUN (unità logiche) e vengono presentate agli host come dispositivi a blocchi standard. I gruppi di iniziatori sono tabelle di nomi di nodi host iSCSI e controllano quali iniziatori hanno accesso a quali LUN. Le destinazioni iSCSI si connettono alla rete tramite schede di rete Ethernet standard (NIC), schede TCP offload engine (TOE) con iniziatori software, schede di rete convergenti (CNA) o adattatori host bus dedicati (HBA) e sono identificate da nomi qualificati iSCSI (IQN). Quando si crea un volume iSCSI, la Console crea automaticamente un LUN. Abbiamo semplificato il tutto creando una sola LUN per volume, quindi non è richiesta alcuna gestione. Dopo aver creato il volume,"utilizzare l'IQN per connettersi al LUN dai tuoi host" .

L'immagine seguente mostra la prima pagina della procedura guidata per la creazione del volume:



16. **Configurazione CIFS**: se hai scelto il protocollo CIFS, configura un server CIFS.

Campo	Descrizione
Indirizzo IP primario e secondario DNS	Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server CIFS. I server DNS elencati devono contenere i record di posizione del servizio (SRV) necessari per individuare i server LDAP di Active Directory e i controller di dominio per il dominio a cui verrà aggiunto il server CIFS.
Dominio Active Directory a cui unirsi	FQDN del dominio Active Directory (AD) a cui si desidera che il server CIFS si unisca.
Credenziali autorizzate ad unirsi al dominio	Nome e password di un account Windows con privilegi sufficienti per aggiungere computer all'unità organizzativa (OU) specificata all'interno del dominio AD.
Nome NetBIOS del server CIFS	Nome del server CIFS univoco nel dominio AD.
Unità organizzativa	L'unità organizzativa all'interno del dominio AD da associare al server CIFS. L'impostazione predefinita è CN=Computer. Per configurare Azure AD Domain Services come server AD per Cloud Volumes ONTAP, è necessario immettere **OU=Computer AADDC** o **OU=Utenti AADDC** in questo campo.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentazione di Azure: creare un'unità organizzativa (OU) in un dominio gestito da Azure AD Domain Services"^]
Dominio DNS	Dominio DNS per la macchina virtuale di archiviazione (SVM) Cloud Volumes ONTAP . Nella maggior parte dei casi, il dominio è lo stesso del dominio AD.
Server NTP	Selezionare **Usa dominio Active Directory** per configurare un server NTP utilizzando il DNS di Active Directory. Se è necessario configurare un server NTP utilizzando un indirizzo diverso, è necessario utilizzare l'API. Fare riferimento al "Documentazione sull'automazione NetApp Console" per i dettagli. Si noti che è possibile configurare un server NTP solo quando si crea un server CIFS. Non è configurabile dopo aver creato il server CIFS.

17. **Profilo di utilizzo, tipo di disco e criterio di suddivisione in livelli**: scegli se abilitare le funzionalità di efficienza dell'archiviazione e modificare il criterio di suddivisione in livelli del volume, se necessario.

    Per maggiori informazioni, fare riferimento a"Comprensione dei profili di utilizzo del volume" E"Panoramica della suddivisione in livelli dei dati" .

18. **Rivedi e approva**: rivedi e conferma le tue selezioni.
    a. Esaminare i dettagli sulla configurazione.
    b. Fare clic su **Ulteriori informazioni** per esaminare i dettagli sul supporto e sulle risorse di Azure che la Console acquisterà.
    c. Seleziona le caselle di controllo **Ho capito…**.
    d. Fare clic su **Vai**.

Risultato

La console distribuisce il sistema Cloud Volumes ONTAP . È possibile monitorare i progressi nella pagina Audit.

Se riscontri problemi durante la distribuzione del sistema Cloud Volumes ONTAP , rivedi il messaggio di errore. È anche possibile selezionare il sistema e fare clic su **Ricrea ambiente**.

Per ulteriore assistenza, vai a "Supporto NetApp Cloud Volumes ONTAP" .

> Una volta completato il processo di distribuzione, non modificare le configurazioni Cloud Volumes ONTAP generate dal sistema nel portale di Azure, in particolare i tag di sistema. Qualsiasi modifica apportata a queste configurazioni potrebbe causare comportamenti imprevisti o perdite di dati.

Dopo aver finito

- Se hai predisposto una condivisione CIFS, assegna agli utenti o ai gruppi le autorizzazioni per i file e le cartelle e verifica che tali utenti possano accedere alla condivisione e creare un file.
- Se si desidera applicare quote ai volumi, utilizzare ONTAP System Manager o ONTAP CLI.

  Le quote consentono di limitare o tenere traccia dello spazio su disco e del numero di file utilizzati da un utente, un gruppo o un qtree.

Avvia una coppia Cloud Volumes ONTAP HA in Azure

Se si desidera avviare una coppia Cloud Volumes ONTAP HA in Azure, è necessario creare un sistema HA nella console.

Passi

1. Dal menu di navigazione a sinistra, seleziona **Archiviazione > Gestione**.
2. Nella pagina **Sistemi**, fare clic su **Aggiungi sistema** e seguire le istruzioni.
3. Se richiesto, "creare un agente Console" .
4. **Dettagli e credenziali**: facoltativamente, modifica le credenziali e la sottoscrizione di Azure, specifica un nome per il cluster, aggiungi tag se necessario e quindi specifica le credenziali.

   Nella tabella seguente vengono descritti i campi per i quali potrebbe essere necessaria una guida:

Campo	Descrizione
Nome del sistema	La console utilizza il nome del sistema per denominare sia il sistema Cloud Volumes ONTAP sia la macchina virtuale di Azure. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di sicurezza predefinito.
Tag del gruppo di risorse	I tag sono metadati per le risorse di Azure. Quando si immettono tag in questo campo, la Console li aggiunge al gruppo di risorse associato al sistema Cloud Volumes ONTAP . Quando si crea un sistema, è possibile aggiungere fino a quattro tag dall'interfaccia utente, per poi aggiungerne altri dopo la creazione. Tieni presente che l'API non ti limita a quattro tag quando crei un sistema. Per informazioni sui tag, fare riferimento a "Documentazione di Microsoft Azure: utilizzo dei tag per organizzare le risorse di Azure" .
Nome utente e password	Queste sono le credenziali per l'account amministratore del cluster Cloud Volumes ONTAP . È possibile utilizzare queste credenziali per connettersi a Cloud Volumes ONTAP tramite ONTAP System Manager o ONTAP CLI. Mantenere il nome utente predefinito *admin* oppure modificarlo con un nome utente personalizzato.

Campo	Descrizione
Modifica credenziali	È possibile scegliere credenziali Azure diverse e un abbonamento Azure diverso da utilizzare con questo sistema Cloud Volumes ONTAP . Per distribuire un sistema Cloud Volumes ONTAP con pagamento in base al consumo, è necessario associare una sottoscrizione di Azure Marketplace alla sottoscrizione di Azure selezionata. "Scopri come aggiungere le credenziali" .

5. **Servizi**: abilita o disabilita i singoli servizi a seconda che tu voglia utilizzarli con Cloud Volumes ONTAP.
   - "Scopri di più sulla NetApp Data Classification"
   - "Scopri di più su NetApp Backup and Recovery"

   Se si desidera utilizzare WORM e il data tiering, è necessario disabilitare Backup e Recovery e distribuire un sistema Cloud Volumes ONTAP con versione 9.8 o successiva.

6. **Modelli di distribuzione HA**:
   a. Selezionare **Zona di disponibilità singola** o **Zona di disponibilità multipla**.
      - Per singole zone di disponibilità, selezionare un'area di Azure, una zona di disponibilità, una rete virtuale e una subnet.

        A partire da Cloud Volumes ONTAP 9.15.1, è possibile distribuire istanze di macchine virtuali (VM) in modalità HA in singole zone di disponibilità (AZ) in Azure. È necessario selezionare una zona e una regione che supportino questa distribuzione. Se la zona o la regione non supporta la distribuzione zonale, viene seguita la precedente modalità di distribuzione non zonale per LRS. Per comprendere le configurazioni supportate per i dischi gestiti condivisi, fare riferimento a"Configurazione della zona di disponibilità singola HA con dischi gestiti condivisi" .

      - Per più zone di disponibilità, selezionare una regione, una rete virtuale, una subnet, una zona per il nodo 1 e una zona per il nodo 2.

   b. Seleziona la casella di controllo **Ho verificato la connettività di rete…**.

7. **Connettività**: scegli un gruppo di risorse nuovo o esistente e poi scegli se utilizzare il gruppo di sicurezza predefinito o il tuo.

   Nella tabella seguente vengono descritti i campi per i quali potrebbe essere necessaria una guida:

Campo	Descrizione
Gruppo di risorse	Crea un nuovo gruppo di risorse per Cloud Volumes ONTAP oppure utilizza un gruppo di risorse esistente. La procedura consigliata è quella di utilizzare un nuovo gruppo di risorse dedicato per Cloud Volumes ONTAP. Sebbene sia possibile distribuire Cloud Volumes ONTAP in un gruppo di risorse condiviso esistente, questa operazione non è consigliata a causa del rischio di perdita di dati. Per maggiori dettagli, vedere l'avviso sopra. È necessario utilizzare un gruppo di risorse dedicato per ogni coppia Cloud Volumes ONTAP HA distribuita in Azure. In un gruppo di risorse è supportata solo una coppia HA. La console riscontra problemi di connessione se si tenta di distribuire una seconda coppia Cloud Volumes ONTAP HA in un gruppo di risorse di Azure. Se l'account Azure che stai utilizzando ha il "permessi richiesti" , la Console rimuove le risorse Cloud Volumes ONTAP da un gruppo di risorse, in caso di errore di distribuzione o eliminazione.
Gruppo di sicurezza generato	Se lasci che sia la Console a generare il gruppo di sicurezza per te, devi scegliere come consentire il traffico: • Se si sceglie **Solo VNet selezionata**, l'origine del traffico in entrata è l'intervallo di subnet della VNet selezionata e l'intervallo di subnet della VNet in cui risiede l'agente della console. Questa è l'opzione consigliata. • Se si seleziona **Tutte le reti virtuali**, l'origine del traffico in entrata è l'intervallo IP 0.0.0.0/0.
Utilizzare esistente	Se si sceglie un gruppo di sicurezza esistente, questo deve soddisfare i requisiti di Cloud Volumes ONTAP . "Visualizza il gruppo di sicurezza predefinito" .

8. **Metodi di addebito e account NSS**: specifica quale opzione di addebito desideri utilizzare con questo sistema, quindi specifica un account del sito di supporto NetApp .
   - "Scopri le opzioni di licenza per Cloud Volumes ONTAP" .
   - "Scopri come impostare le licenze" .
9. **Pacchetti preconfigurati**: seleziona uno dei pacchetti per distribuire rapidamente un sistema Cloud Volumes ONTAP oppure fai clic su **Modifica configurazione**.

   Se si sceglie uno dei pacchetti, è sufficiente specificare un volume e quindi rivedere e approvare la configurazione.
10. **Licenze**: modifica la versione di Cloud Volumes ONTAP in base alle tue esigenze e seleziona un tipo di macchina virtuale.

    Se per la versione selezionata è disponibile una versione Release Candidate, una versione General Availability o una patch più recente, la Console aggiorna il sistema a tale versione durante la sua creazione. Ad esempio, l'aggiornamento avviene se si seleziona Cloud Volumes ONTAP 9.13.1 e se è disponibile la versione 9.13.1 P4. L'aggiornamento non avviene da una versione all'altra, ad esempio dalla 9.13 alla 9.14.

11. **Iscriviti da Azure Marketplace**: segui i passaggi se la console non riesce ad abilitare le distribuzioni programmatiche di Cloud Volumes ONTAP.
12. **Risorse di archiviazione sottostanti**: scegli le impostazioni per l'aggregato iniziale: un tipo di disco, una dimensione per ciascun disco e se abilitare la suddivisione dei dati in livelli nell'archiviazione BLOB.

    Notare quanto segue:

    - La dimensione del disco si riferisce a tutti i dischi nell'aggregato iniziale e a tutti gli aggregati aggiuntivi creati dalla Console quando si utilizza l'opzione di provisioning semplice. È possibile creare aggregati che utilizzano dimensioni del disco diverse utilizzando l'opzione di allocazione avanzata.

      Per assistenza nella scelta della dimensione del disco, fare riferimento a"Dimensiona il tuo sistema in Azure" .

    - Se l'accesso pubblico al tuo account di archiviazione è disabilitato all'interno della VNet, non puoi abilitare la suddivisione in livelli dei dati nel tuo sistema Cloud Volumes ONTAP . Per informazioni, fare riferimento a"Regole del gruppo di sicurezza" .
    - Quando si crea o si modifica un volume, è possibile scegliere una specifica politica di suddivisione in livelli del volume.
    - Se si disabilita la suddivisione in livelli dei dati, è possibile abilitarla sugli aggregati successivi.

      "Scopri di più sulla suddivisione in livelli dei dati" .

    - A partire da Cloud Volumes ONTAP 9.15.0P1, i BLOB di pagine di Azure non sono più supportati per le nuove distribuzioni di coppie ad alta disponibilità. Se attualmente si utilizzano BLOB di pagine di Azure in distribuzioni di coppie ad alta disponibilità esistenti, è possibile eseguire la migrazione a tipi di istanze di VM più recenti nelle VM della serie Edsv4 e nelle VM della serie Edsv5.

      "Scopri di più sulle configurazioni supportate in Azure" .

13. **Velocità di scrittura e WORM**:

    a. Se lo desideri, seleziona la velocità di scrittura **Normale** o **Alta**.

       "Scopri di più sulla velocità di scrittura" .

    b. Se lo si desidera, attivare la memorizzazione WORM (write once, read many).

       Questa opzione è disponibile solo per alcuni tipi di VM. Per scoprire quali tipi di VM sono supportati, fare riferimento a"Configurazioni supportate per licenza per coppie HA" .

       WORM non può essere abilitato se il tiering dei dati è stato abilitato per Cloud Volumes ONTAP versione 9.7 e precedenti. Il ripristino o il downgrade a Cloud Volumes ONTAP 9.8 è bloccato dopo l'abilitazione di WORM e del tiering.

    "Scopri di più sullo storage WORM" .

    a. Se si attiva l'archiviazione WORM, selezionare il periodo di conservazione.
14. **Comunicazione sicura con Storage e WORM**: scegli se abilitare una connessione HTTPS agli account di storage di Azure e attivare lo storage WORM (Write Once, Read Many), se lo desideri.

    La connessione HTTPS avviene da una coppia Cloud Volumes ONTAP 9.7 HA agli account di archiviazione BLOB di pagine di Azure. Tieni presente che l'abilitazione di questa opzione può influire sulle prestazioni di scrittura. Non è possibile modificare l'impostazione dopo aver creato il sistema.

"Scopri di più sullo storage WORM" .

WORM non può essere abilitato se è stato abilitato il tiering dei dati.

"Scopri di più sullo storage WORM" .

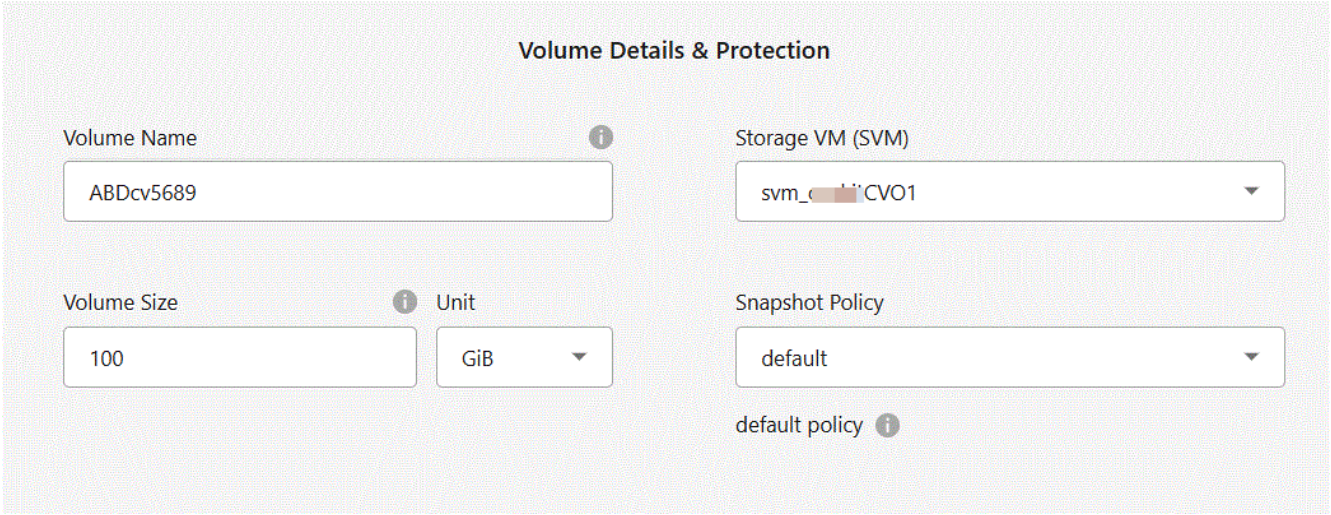
15. **Crea volume**: inserisci i dettagli per il nuovo volume o fai clic su **Salta**.

    "Scopri i protocolli e le versioni client supportati" .

    Alcuni campi di questa pagina sono autoesplicativi. Nella tabella seguente vengono descritti i campi per i quali potrebbe essere necessaria una guida:

Campo	Descrizione
Misurare	La dimensione massima che è possibile immettere dipende in larga misura dall'attivazione o meno del thin provisioning, che consente di creare un volume più grande dello spazio di archiviazione fisico attualmente disponibile.
Controllo degli accessi (solo per NFS)	Una policy di esportazione definisce i client nella subnet che possono accedere al volume. Per impostazione predefinita, la Console immette un valore che fornisce l'accesso a tutte le istanze nella subnet.
Autorizzazioni e utenti/gruppi (solo per CIFS)	Questi campi consentono di controllare il livello di accesso a una condivisione per utenti e gruppi (chiamati anche elenchi di controllo degli accessi o ACL). È possibile specificare utenti o gruppi Windows locali o di dominio oppure utenti o gruppi UNIX. Se si specifica un nome utente di dominio Windows, è necessario includere il dominio dell'utente utilizzando il formato dominio\nomeutente.
Politica di snapshot	Una policy di copia snapshot specifica la frequenza e il numero di copie Snapshot NetApp create automaticamente. Una copia Snapshot NetApp è un'immagine del file system in un dato momento che non ha alcun impatto sulle prestazioni e richiede uno spazio di archiviazione minimo. È possibile scegliere la policy predefinita o nessuna. Per i dati temporanei è possibile scegliere "nessuno": ad esempio, tempdb per Microsoft SQL Server.
Opzioni avanzate (solo per NFS)	Selezionare una versione NFS per il volume: NFSv3 o NFSv4.
Gruppo iniziatore e IQN (solo per iSCSI)	Le destinazioni di archiviazione iSCSI sono chiamate LUN (unità logiche) e vengono presentate agli host come dispositivi a blocchi standard. I gruppi di iniziatori sono tabelle di nomi di nodi host iSCSI e controllano quali iniziatori hanno accesso a quali LUN. Le destinazioni iSCSI si connettono alla rete tramite schede di rete Ethernet standard (NIC), schede TCP offload engine (TOE) con iniziatori software, schede di rete convergenti (CNA) o adattatori host bus dedicati (HBA) e sono identificate da nomi qualificati iSCSI (IQN). Quando si crea un volume iSCSI, la Console crea automaticamente un LUN. Abbiamo semplificato il tutto creando una sola LUN per volume, quindi non è richiesta alcuna gestione. Dopo aver creato il volume,"utilizzare l'IQN per connettersi al LUN dai tuoi host" .

    L'immagine seguente mostra la prima pagina della procedura guidata per la creazione del volume:



16. **Configurazione CIFS**: se hai scelto il protocollo CIFS, configura un server CIFS.

Campo	Descrizione
Indirizzo IP primario e secondario DNS	Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server CIFS. I server DNS elencati devono contenere i record di posizione del servizio (SRV) necessari per individuare i server LDAP di Active Directory e i controller di dominio per il dominio a cui verrà aggiunto il server CIFS.
Dominio Active Directory a cui unirsi	FQDN del dominio Active Directory (AD) a cui si desidera che il server CIFS si unisca.
Credenziali autorizzate ad unirsi al dominio	Nome e password di un account Windows con privilegi sufficienti per aggiungere computer all'unità organizzativa (OU) specificata all'interno del dominio AD.
Nome NetBIOS del server CIFS	Nome del server CIFS univoco nel dominio AD.
Unità organizzativa	L'unità organizzativa all'interno del dominio AD da associare al server CIFS. L'impostazione predefinita è CN=Computer. Per configurare Azure AD Domain Services come server AD per Cloud Volumes ONTAP, è necessario immettere **OU=Computer AADDC** o **OU=Utenti AADDC** in questo campo.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentazione di Azure: creare un'unità organizzativa (OU) in un dominio gestito da Azure AD Domain Services"^]
Dominio DNS	Dominio DNS per la macchina virtuale di archiviazione (SVM) Cloud Volumes ONTAP . Nella maggior parte dei casi, il dominio è lo stesso del dominio AD.
Server NTP	Selezionare **Usa dominio Active Directory** per configurare un server NTP utilizzando il DNS di Active Directory. Se è necessario configurare un server NTP utilizzando un indirizzo diverso, è necessario utilizzare l'API. Fare riferimento al "Documentazione sull'automazione NetApp Console" per i dettagli. Si noti che è possibile configurare un server NTP solo quando si crea un server CIFS. Non è configurabile dopo aver creato il server CIFS.

17. **Profilo di utilizzo, tipo di disco e criterio di suddivisione in livelli**: scegli se abilitare le funzionalità di efficienza dell'archiviazione e modificare il criterio di suddivisione in livelli del volume, se necessario.

    Per maggiori informazioni, fare riferimento a"Scegli un profilo di utilizzo del volume" ,"Panoramica della

suddivisione in livelli dei dati" , E "KB: Quali funzionalità di Inline Storage Efficiency sono supportate da CVO?"

18. **Rivedi e approva**: rivedi e conferma le tue selezioni.
    a. Esaminare i dettagli sulla configurazione.
    b. Fare clic su **Ulteriori informazioni** per esaminare i dettagli sul supporto e sulle risorse di Azure che la Console acquisterà.
    c. Seleziona le caselle di controllo **Ho capito…**.
    d. Fare clic su **Vai**.

Risultato

La console distribuisce il sistema Cloud Volumes ONTAP . È possibile monitorare i progressi nella pagina Audit.

Se riscontri problemi durante la distribuzione del sistema Cloud Volumes ONTAP , rivedi il messaggio di errore. È anche possibile selezionare il sistema e fare clic su **Ricrea ambiente**.

Per ulteriore assistenza, vai a "Supporto NetApp Cloud Volumes ONTAP" .

Dopo aver finito

- Se hai predisposto una condivisione CIFS, assegna agli utenti o ai gruppi le autorizzazioni per i file e le cartelle e verifica che tali utenti possano accedere alla condivisione e creare un file.
- Se si desidera applicare quote ai volumi, utilizzare ONTAP System Manager o ONTAP CLI.

  Le quote consentono di limitare o tenere traccia dello spazio su disco e del numero di file utilizzati da un utente, un gruppo o un qtree.

> Una volta completato il processo di distribuzione, non modificare le configurazioni Cloud Volumes ONTAP generate dal sistema nel portale di Azure, in particolare i tag di sistema. Qualsiasi modifica apportata a queste configurazioni potrebbe causare comportamenti imprevisti o perdite di dati.

Link correlati

*"Pianificazione della configurazione Cloud Volumes ONTAP in Azure" *"Distribuisci Cloud Volumes ONTAP in Azure da Azure Marketplace"

Verifica l’immagine della piattaforma Azure

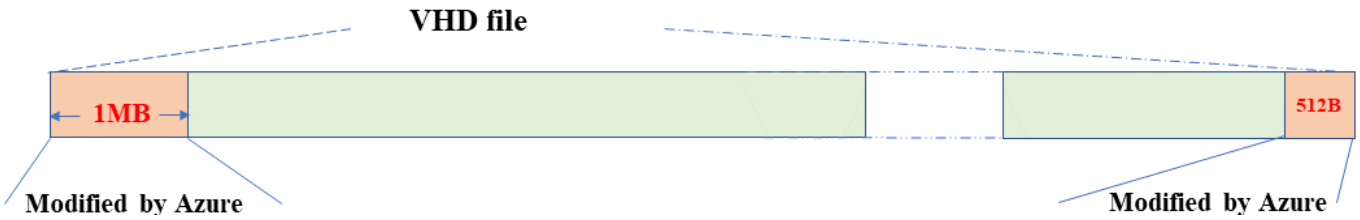
Verifica delle immagini di Azure Marketplace per Cloud Volumes ONTAP

La verifica delle immagini di Azure è conforme ai requisiti di sicurezza avanzati NetApp . La verifica di un file immagine è un processo semplice. Tuttavia, la verifica della firma dell’immagine di Azure richiede considerazioni specifiche per il file immagine VHD di Azure, poiché viene modificato in Azure Marketplace.

> La verifica delle immagini di Azure è supportata su Cloud Volumes ONTAP 9.15.0 e versioni successive.

Alterazione dei file VHD pubblicati da parte di Azure

1 MB (1048576 byte) all'inizio e 512 byte alla fine del file VHD vengono modificati da Azure. NetApp firma il file VHD rimanente.



Nell'esempio, il file VHD è di 10 GB. La parte firmata NetApp è contrassegnata in verde (10 GB - 1 MB - 512 byte).

Link correlati

- "Blog Page Fault: come firmare e verificare utilizzando OpenSSL"
- "Utilizzare l'immagine di Azure Marketplace per creare un'immagine di macchina virtuale per la GPU di Azure Stack Edge Pro | Microsoft Learn"
- "Esportare/copiare un disco gestito in un account di archiviazione tramite l'interfaccia della riga di comando di Azure | Microsoft Learn"
- "Guida introduttiva ad Azure Cloud Shell - Bash | Microsoft Learn"
- "Come installare l'interfaccia della riga di comando di Azure | Microsoft Learn"
- "copia blob di archiviazione az | Microsoft Learn"
- "Sign in con Azure CLI — Accesso e autenticazione | Microsoft Learn"

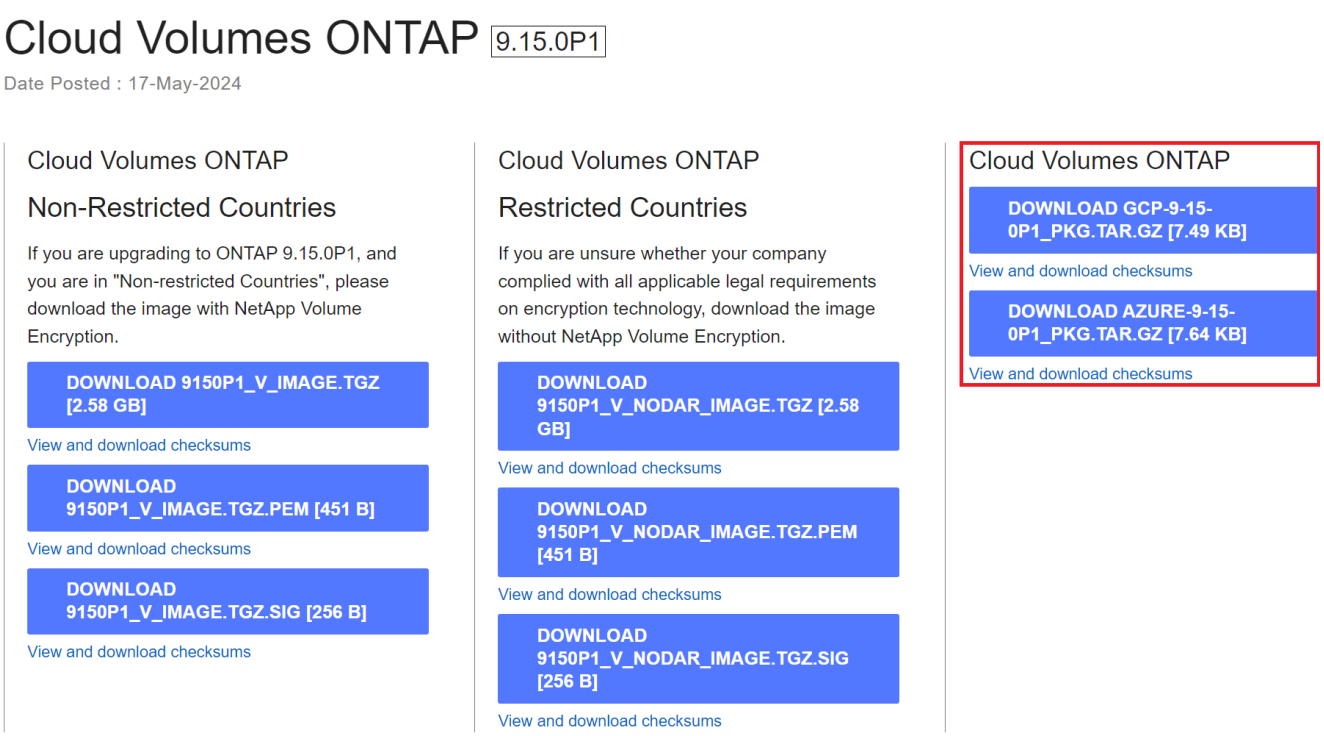
Scarica il file immagine di Azure per Cloud Volumes ONTAP

È possibile scaricare il file immagine di Azure da "Sito di supporto NetApp" .

Il file *tar.gz* contiene i file necessari per la verifica della firma dell'immagine. Insieme al file *tar.gz*, dovresti scaricare anche il file *checksum* per l'immagine. Il file di checksum contiene il `md5` E `sha256` checksum del file *tar.gz*.

Passi

1. Vai al "Pagina del prodotto Cloud Volumes ONTAP sul sito di supporto NetApp" e scaricare la versione software richiesta dalla sezione **Download**.
2. Nella pagina di download Cloud Volumes ONTAP , fare clic sul file scaricabile per l'immagine di Azure e scaricare il file *tar.gz*.



3. Su Linux, esegui `md5sum AZURE-<version>_PKG.TAR.GZ` .

   Su macOS, esegui `sha256sum AZURE-<version>_PKG.TAR.GZ` .

4. Verificare che il `md5sum` E `sha256sum` i valori corrispondono a quelli nell'immagine di Azure scaricata.
5. Su Linux e macOS, estrarre il file *tar.gz* utilizzando `tar -xzf` comando.

   Il file *tar.gz* estratto contiene il file digest (*.sig*), il file del certificato della chiave pubblica (*.pem*) e il file del certificato della catena (*.pem*).

   Esempio di output dopo l'estrazione del file tar.gz:

```
$ 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
```

Esportare immagini VHD per Cloud Volumes ONTAP da Azure Marketplace

Una volta pubblicata sul cloud di Azure, l'immagine VHD non è più gestita da NetApp. L'immagine pubblicata viene invece inserita nel marketplace di Azure. Quando l'immagine viene preparata e pubblicata su Azure Marketplace, Azure modifica 1 MB all'inizio e 512 byte alla fine del VHD. Per verificare la firma del file VHD, è necessario esportare l'immagine VHD modificata da Azure da Azure Marketplace.

Prima di iniziare

Assicurati che l'interfaccia della riga di comando di Azure sia installata sul tuo sistema oppure che Azure Cloud Shell sia disponibile tramite il portale di Azure. Per ulteriori informazioni su come installare l'interfaccia della riga di comando di Azure, fare riferimento a "Documentazione Microsoft: come installare l'interfaccia della riga di comando di Azure" .

Passi

1. Mappare la versione Cloud Volumes ONTAP sul sistema alla versione dell'immagine di Azure Marketplace utilizzando il contenuto del file *version_readme*. La versione Cloud Volumes ONTAP è rappresentata da `buildname` e la versione dell'immagine di Azure Marketplace è rappresentata da `version` nelle mappature delle versioni.

   Nell'esempio seguente, la versione Cloud Volumes ONTAP `9.15.0P1` è mappato alla versione dell'immagine di Azure Marketplace `9150.01000024.05090105` . Questa versione dell'immagine di Azure Marketplace viene utilizzata in seguito per impostare l'URN dell'immagine.

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

   ]
   ```

2. Identifica la regione in cui desideri creare le VM. Il nome della regione viene utilizzato come valore per `locName` variabile quando si imposta l'URN dell'immagine del marketplace. Per elencare le regioni disponibili, eseguire questo comando:

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

   In questa tabella, il nome della regione appare nella `Name` campo.

   ```
   $ 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. Esaminare i nomi SKU per le versioni Cloud Volumes ONTAP corrispondenti e i tipi di distribuzione delle VM nella tabella seguente. Il nome SKU viene utilizzato come valore per `skuName` variabile quando si imposta l'URN dell'immagine del marketplace.

   Ad esempio, tutte le distribuzioni a nodo singolo con Cloud Volumes ONTAP 9.15.0 dovrebbero utilizzare `ontap_cloud_byol` come nome SKU.

* Versione Cloud Volumes ONTAP *	**Distribuzione VM tramite**	**Nome SKU**
9.17.1 e versioni successive	Il marketplace di Azure	ontap_cloud_direct_gen2
9.17.1 e versioni successive	La NetApp Console	ontap_cloud_gen2
9.16.1	Il marketplace di Azure	ontap_cloud_direct
9.16.1	La console	ontap_cloud
9.15.1	La console	ontap_cloud
9.15.0	La console, distribuzioni a nodo singolo	ontap_cloud_byol
9.15.0	La console, distribuzioni ad alta disponibilità (HA)	ontap_cloud_byol_ha

4. Dopo aver mappato la versione ONTAP e l'immagine di Azure Marketplace, esportare il file VHD da Azure Marketplace utilizzando Azure Cloud Shell o Azure CLI.

Esportare file VHD utilizzando Azure Cloud Shell su Linux

Da Azure Cloud Shell, esporta l'immagine del marketplace nel file VHD (ad esempio, *9150.01000024.05090105.vhd*) e scaricala sul tuo sistema Linux locale. Per ottenere l'immagine VHD da Azure Marketplace, eseguire i passaggi seguenti.

Passi

1. Imposta l'URN e altri parametri dell'immagine del marketplace. Il formato URN è `<publisher>:<offer>:<sku>:<version>` . Facoltativamente, puoi elencare le immagini del marketplace NetApp per confermare la versione corretta dell'immagine.

```
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. Crea un nuovo disco gestito dall'immagine del marketplace con la versione dell'immagine corrispondente:

```
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. Esportare il file VHD dal disco gestito ad Azure Storage. Creare un contenitore con il livello di accesso appropriato. In questo esempio, abbiamo utilizzato un contenitore denominato `vm-images` con `Container` livello di accesso. Ottieni la chiave di accesso dell’account di archiviazione dal portale di Azure: **Account di archiviazione > *examplesaname* > Chiave di accesso > *key1* > *key* > Mostra > *<copia>***

```
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. Scarica l’immagine generata sul tuo sistema Linux. Utilizzare il `wget` comando per scaricare il file VHD:

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

L’URL segue un formato standard. Per l’automazione, è possibile ricavare la stringa URL come mostrato di seguito. In alternativa, puoi usare l’interfaccia della riga di comando di Azure `az` comando per ottenere l’URL. Esempio di URL:https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

5. Pulisci il disco gestito

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

Esportare il file VHD utilizzando l'interfaccia della riga di comando di Azure su Linux

Esportare l'immagine del marketplace in un file VHD tramite l'interfaccia della riga di comando di Azure da un sistema Linux locale.

Passi

1. Accedi all'interfaccia della riga di comando di Azure ed elenca le immagini del marketplace:

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

2. Per accedere, utilizzare un browser Web per aprire la pagina https://microsoft.com/devicelogin e inserisci il codice di autenticazione.

```
% 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. Crea un nuovo disco gestito dall'immagine del marketplace con la versione dell'immagine corrispondente.

```
% 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"
```

Per automatizzare il processo, è necessario estrarre il SAS dall'output standard. Per indicazioni fare riferimento ai documenti appropriati.

4. Esportare il file VHD dal disco gestito.

   a. Creare un contenitore con il livello di accesso appropriato. In questo esempio, un contenitore denominato `vm-images` con `Container` viene utilizzato il livello di accesso.

   b. Ottieni la chiave di accesso dell'account di archiviazione dal portale di Azure: **Account di archiviazione > *examplesaname* > Chiave di accesso > *key1* > *key* > Mostra > <*copia*>**

      Puoi anche usare il `az` comando per questo passaggio.

```
% 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. Controllare lo stato della copia del blob.

```
% 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. Scarica l'immagine generata sul tuo server Linux.

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

L'URL segue un formato standard. Per l'automazione, è possibile ricavare la stringa URL come mostrato di seguito. In alternativa, puoi usare l'interfaccia della riga di comando di Azure `az` comando per ottenere l'URL. Esempio di URL:https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

7. Pulisci il disco gestito

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

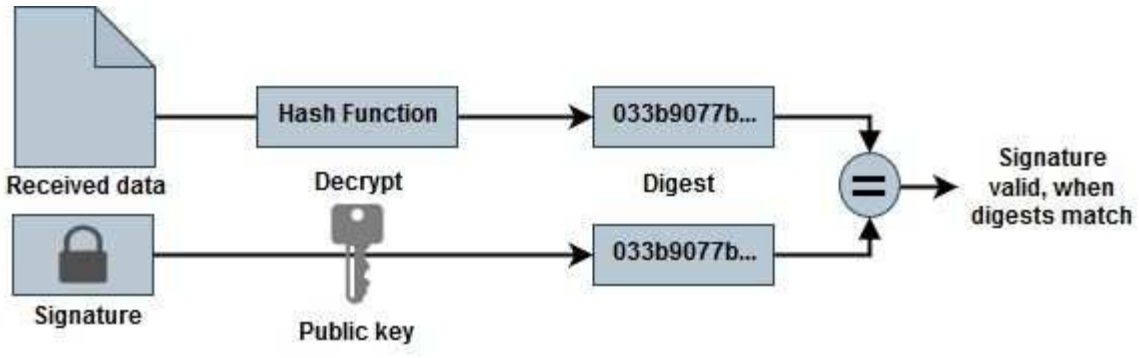
Verifica la firma del file

Verifica della firma dell'immagine di Azure Marketplace per Cloud Volumes ONTAP

Il processo di verifica dell'immagine di Azure genera un file digest dal file VHD eliminando 1 MB all'inizio e 512 byte alla fine, quindi applicando una funzione hash. Per abbinare la procedura di firma, per l'hashing viene utilizzato *sha256*.

Riepilogo del flusso di lavoro di verifica della firma del file

Di seguito è riportata una panoramica del processo di verifica della firma del file.



- Scaricamento dell'immagine di Azure da "Sito di supporto NetApp" ed estraendo il file digest (.sig), il file del certificato della chiave pubblica (.pem) e il file del certificato della catena (.pem). Fare riferimento a "Scarica il file digest dell'immagine di Azure" per maggiori informazioni.
- Verifica della catena di fiducia.
- Estrazione della chiave pubblica (.pub) dal certificato della chiave pubblica (.pem).
- Decifrare il file digest utilizzando la chiave pubblica estratta.
- Confronto del risultato con un digest appena generato di un file temporaneo creato dal file immagine dopo aver rimosso 1 MB all'inizio e 512 byte alla fine. Questo passaggio viene eseguito utilizzando lo strumento da riga di comando OpenSSL. Lo strumento OpenSSL CLI visualizza un messaggio appropriato in caso di successo o fallimento nella corrispondenza dei file.

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

Verifica la firma dell'immagine di Azure Marketplace per Cloud Volumes ONTAP su Linux

La verifica della firma di un file VHD esportato su Linux include la convalida della catena di attendibilità, la modifica del file e la verifica della firma.

Passi

1. Scarica il file immagine di Azure da "Sito di supporto NetApp" ed estrarre il file digest (.sig), il file del certificato della chiave pubblica (.pem) e il file del certificato della catena (.pem).

   Fare riferimento a "Scarica il file digest dell'immagine di Azure" per maggiori informazioni.

2. Verificare la catena di fiducia.

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

3. Rimuovere 1 MB (1.048.576 byte) all'inizio e 512 byte alla fine del file VHD. Quando si utilizza `tail` , IL `-c +K` L'opzione genera byte dal K-esimo byte del file. Pertanto, passa 1048577 a `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. Utilizzare OpenSSL per estrarre la chiave pubblica dal certificato e verificare il file estratto (sign.tmp) con il file della firma e la chiave pubblica.

   Il prompt dei comandi visualizza messaggi che indicano l'esito positivo o negativo della verifica.

```
% 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. Pulisci l'area di lavoro.

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

Verifica la firma dell'immagine di Azure Marketplace per Cloud Volumes ONTAP su macOS

La verifica della firma di un file VHD esportato su Linux include la convalida della catena di attendibilità, la modifica del file e la verifica della firma.

Passi

1. Scarica il file immagine di Azure da "Sito di supporto NetApp" ed estrarre il file digest (.sig), il file del certificato della chiave pubblica (.pem) e il file del certificato della catena (.pem).

   Fare riferimento a "Scarica il file digest dell'immagine di Azure" per maggiori informazioni.

2. Verificare la catena di fiducia.

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

3. Rimuovere 1 MB (1.048.576 byte) all'inizio e 512 byte alla fine del file VHD. Quando si utilizza `tail` , IL `-c +K` L'opzione genera byte dal K-esimo byte del file. Pertanto, passa 1048577 a `tail -c` . Tieni presente

che su macOS il comando tail potrebbe richiedere circa dieci minuti per essere completato.

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

4. Utilizzare OpenSSL per estrarre la chiave pubblica dal certificato e verificare il file estratto (sign.tmp) con il file della firma e la chiave pubblica. Il prompt dei comandi visualizza messaggi che indicano l'esito positivo o negativo della verifica.

```
% 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. Pulisci l'area di lavoro.

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

Distribuisci Cloud Volumes ONTAP dal marketplace di Azure

È possibile utilizzare la distribuzione diretta di Azure Marketplace per distribuire Cloud Volumes ONTAP in modo rapido e semplice. Dall'Azure Marketplace puoi distribuire rapidamente Cloud Volumes ONTAP in pochi clic ed esplorare le sue funzionalità e capacità principali nel tuo ambiente.

Per maggiori informazioni su questa offerta, fare riferimento a"Scopri di più sulle offerte Cloud Volumes ONTAP nella NetApp Console e nel marketplace" .

Informazioni su questo compito

Il sistema Cloud Volumes ONTAP distribuito tramite la distribuzione diretta di Azure Marketplace presenta le seguenti proprietà. Si noti che le funzionalità di un'istanza autonoma distribuita tramite Azure Marketplace cambiano quando viene rilevata nella NetApp Console.

- L'ultima versione Cloud Volumes ONTAP (9.16.1 o successiva).
- Una licenza gratuita per Cloud Volumes ONTAP limitata a 500 GiB di capacità fornita. Questa licenza non

include alcun supporto NetApp e non ha una data di scadenza.

- Due nodi configurati in modalità ad alta disponibilità (HA) in un'unica zona di disponibilità (AZ), dotati di numeri di serie predefiniti. Le macchine virtuali di storage (VM di storage) vengono distribuite in un"modalità di orchestrazione flessibile" .
- Un aggregato per l'istanza creata per impostazione predefinita.
- Un disco gestito Premium SSD v2 con capacità di provisioning di 500 GiB, un disco root e un disco dati.
- Una VM di archiviazione dati distribuita, con servizi dati NFS, CIFS, iSCSI e NVMe/TCP. Non è possibile aggiungere ulteriori VM di archiviazione dati.
- Licenze installate per NFS, CIFS (SMB), iSCSI, Autonomous Ransomware Protection (ARP), SnapLock e SnapMirror.
- "Efficienza di stoccaggio sensibile alla temperatura (TSSE) ONTAP", crittografia del volume e gestione delle chiavi esterne abilitate per impostazione predefinita.
- Queste funzionalità non sono supportate:
  - Struttura a FabricPool
  - Modifica del tipo di VM di archiviazione
  - Modalità di scrittura veloce

Prima di iniziare

- Assicurati di disporre di un abbonamento valido ad Azure Marketplace.
- Assicurati di soddisfare i requisiti di rete per un"Distribuzione HA in una singola AZ" in Azzurro. Fare riferimento a "Configurare la rete di Azure per Cloud Volumes ONTAP" .
- Per distribuire Cloud Volumes ONTAP è necessario che ti venga assegnato uno di questi ruoli di Azure:
  - IL `contributor` ruolo con le autorizzazioni predefinite. Per maggiori informazioni, fare riferimento al "Documentazione di Microsoft Azure: ruoli predefiniti di Azure" .
  - Un ruolo RBAC personalizzato con le seguenti autorizzazioni. Per maggiori informazioni, fare riferimento al "Documentazione di Azure: ruoli personalizzati di Azure" .

"autorizzazioni": [{ "azioni": ["Microsoft.AAD/register/azione",
"Microsoft.Resources/sottoscrizioni/GruppiDiRisorse/scrittura",
"Microsoft.Network/loadBalancers/scrittura", "Microsoft.ClassicCompute/Machines
virtuali/scrittura", "Microsoft.Compute/capacityReservationGroups/distribuzione/azione",
"Microsoft.ClassicCompute/Machines
virtuali/Interfacciadirete/associataGruppiDiSecurità/scrittura",
"Microsoft.Network/Interfacciadirete/scrittura", "Microsoft.Compute/Machines virtuali/scrittura",
"Microsoft.Compute/Machines virtuali/estensioni/scrittura",
"Microsoft.Resources/distribuzioni/validazione/azione",
"Microsoft.Resources/sottoscrizioni/GruppiDiRisorse/lettura",
"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": [] }]

Se hai registrato il provider di risorse "Microsoft.storage" nel tuo abbonamento, non hai bisogno di `Microsoft.AAD/register/action` permesso. Per maggiori informazioni, fare riferimento al "Documentazione di Azure: autorizzazioni di Azure per l'archiviazione" .

Passi

1. Dal sito di Azure Marketplace, cerca i prodotti NetApp .
2. Selezionare * NetApp Cloud Volumes ONTAP diretto*.
3. Fare clic su **Crea** per avviare la procedura guidata di distribuzione.
4. Seleziona un piano. L'elenco **Piano** in genere visualizza le versioni più recenti di Cloud Volumes ONTAP.
5. Nella scheda **Informazioni di base**, fornisci questi dettagli:
   - **Abbonamento**: Seleziona un abbonamento. L'implementazione sarà collegata al numero di abbonamento.
   - **Gruppo di risorse**: utilizza un gruppo di risorse esistente o creane uno nuovo. I gruppi di risorse aiutano ad allocare tutte le risorse, come dischi e VM di archiviazione, all'interno di un singolo gruppo per un sistema Cloud Volumes ONTAP .
   - **Regione**: seleziona una regione che supporti la distribuzione di Azure HA in una singola zona di disponibilità. Nell'elenco vengono visualizzate solo le regioni disponibili.
   - **Dimensione**: seleziona una dimensione di archiviazione VM per il disco gestito Premium SSD v2 supportato.
   - **Zona**: seleziona una zona per la regione selezionata.
   - **Password amministratore**: imposta una password. Questa password di amministratore verrà utilizzata per accedere al sistema dopo la distribuzione.
   - **Conferma password**: reinserisci la stessa password per conferma.
     - Nella scheda **Rete**, aggiungi una rete virtuale e una subnet oppure selezionale dagli elenchi.

       Per rispettare le restrizioni di Microsoft Azure, è necessario creare una nuova subnet quando si configura una nuova rete virtuale. Allo stesso modo, se si sceglie una rete esistente, è necessario selezionare una subnet esistente.

     - Per selezionare un gruppo di sicurezza di rete predefinito, selezionare **Sì**. Selezionare **No** per assegnare un gruppo di sicurezza di rete di Azure predefinito con le regole di traffico necessarie. Per ulteriori informazioni, fare riferimento a "Regole del gruppo di sicurezza per Azure" .
     - Nella scheda **Avanzate** verificare se sono state impostate le due funzionalità di Azure necessarie per questa distribuzione. Fare riferimento a"Abilita una funzionalità di Azure per le distribuzioni AZ singole Cloud Volumes ONTAP" E"Abilita la modalità ad alta disponibilità per Cloud Volumes ONTAP in Azure" .
     - Nella scheda **Tag** è possibile definire coppie nome-valore per le risorse o i gruppi di risorse.
     - Nella scheda **Revisiona + crea**, rivedi i dettagli e avvia la distribuzione.

Dopo aver finito

Seleziona l'icona di notifica per visualizzare lo stato di avanzamento della distribuzione. Dopo aver distribuito Cloud Volumes ONTAP , è possibile visualizzare la VM di archiviazione elencata per le operazioni.

Una volta accessibile, utilizzare ONTAP System Manager o ONTAP CLI per accedere alla VM di archiviazione

con le credenziali di amministratore impostate. Successivamente, è possibile creare volumi, LUN o condivisioni e iniziare a utilizzare le capacità di archiviazione di Cloud Volumes ONTAP.

Risolvere i problemi di distribuzione

I sistemi Cloud Volumes ONTAP distribuiti direttamente tramite Azure Marketplace non includono il supporto di NetApp. Se durante la distribuzione si verificano problemi, è possibile risolverli in modo indipendente.

Passi

1. Nel sito di Azure Marketplace, vai a **Diagnostica di avvio > Registro seriale**.
2. Scaricare ed esaminare i registri seriali.
3. Per la risoluzione dei problemi, consultare la documentazione del prodotto e gli articoli della knowledge base (KB).
   - "Documentazione di Azure Marketplace"
   - "Documentazione NetApp"
   - "Articoli della Knowledge Base NetApp"

Scopri i sistemi distribuiti nella Console

È possibile individuare i sistemi Cloud Volumes ONTAP distribuiti tramite la distribuzione diretta di Azure Marketplace e gestirli nella pagina **Sistemi** nella Console. L'agente Console rileva i sistemi, li aggiunge e applica le licenze necessarie, sbloccando così tutte le funzionalità della Console per questi sistemi. La configurazione HA originale in una singola AZ con dischi gestiti PSSD v2 viene mantenuta e il sistema viene registrato nella stessa sottoscrizione Azure e nello stesso gruppo di risorse della distribuzione originale.

Informazioni su questo compito

Dopo aver individuato i sistemi Cloud Volumes ONTAP distribuiti tramite la distribuzione diretta di Azure Marketplace, l'agente della console esegue queste attività:

- Sostituisce le licenze gratuite dei sistemi scoperti come normali licenze basate sulla capacità"Licenze Freemium" .
- Mantiene le funzionalità esistenti dei sistemi distribuiti e aggiunge le funzionalità aggiuntive della Console, come la protezione dei dati, la gestione dei dati e le funzionalità di sicurezza.
- Sostituisce le licenze installate sui nodi con nuove licenze ONTAP per NFS, CIFS (SMB), iSCSI, ARP, SnapLock e SnapMirror.
- Converte i numeri di serie dei nodi generici in numeri di serie univoci.
- Assegna nuovi tag di sistema alle risorse secondo necessità.
- Converte gli indirizzi IP dinamici dell'istanza in indirizzi IP statici.
- Abilita le funzionalità di"Struttura a FabricPool" ,"AutoSupport" , E"scrivi una volta, leggi molte volte" (WORM) di archiviazione sui sistemi distribuiti. Puoi attivare queste funzionalità dalla Console quando ne hai bisogno.
- Registra le istanze negli account NSS utilizzati per individuarle.
- Abilita le funzionalità di gestione della capacità in"modalità automatica e manuale" per i sistemi scoperti.

Prima di iniziare

Assicurarsi che la distribuzione sia completa su Azure Marketplace. L'agente della console può rilevare i sistemi solo quando la distribuzione è completa e sono disponibili per la rilevazione.

Passi

Nella Console, segui la procedura standard per rilevare i sistemi esistenti. Fare riferimento a "Aggiungere un sistema Cloud Volumes ONTAP esistente alla console" .

> Durante l'individuazione, potrebbero essere visualizzati messaggi di errore, ma è possibile ignorarli finché il processo di individuazione non sarà completato. Non modificare le configurazioni Cloud Volumes ONTAP generate dal sistema nel portale di Azure Marketplace durante l'individuazione, in particolare i tag di sistema. Qualsiasi modifica apportata a queste configurazioni potrebbe causare comportamenti imprevisti del sistema.

Dopo aver finito

Una volta completata l'individuazione, è possibile visualizzare i sistemi elencati nella pagina **Sistemi** nella Console. È possibile eseguire varie attività di gestione, come ad esempio"espandendo l'aggregato" ,"aggiunta di volumi" ,"provisioning di VM di storage aggiuntive" , E"modifica dei tipi di istanza" .

Link correlati

Per ulteriori informazioni sulla creazione di storage, fare riferimento alla documentazione ONTAP :

- "Creare volumi per NFS"
- "Creare LUN per iSCSI"
- "Crea azioni per CIFS"

Informazioni sul copyright

Informazioni sul marchio commerciale