Inizia ad utilizzare Azure

Cloud Manager 3.8

NetApp
March 25, 2024

Sommario

Inizia ad utilizzare Azure

Introduzione a Cloud Volumes ONTAP per Azure

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

Creare un connettore

Se non si dispone di un "Connettore" Tuttavia, un amministratore dell'account deve crearne uno. "Scopri come creare un connettore in Azure".

Quando crei il tuo primo ambiente di lavoro Cloud Volumes ONTAP, Cloud Manager ti chiede di implementare un connettore se non ne hai ancora uno.

Pianificare la configurazione

Cloud Manager offre pacchetti preconfigurati che soddisfano i tuoi requisiti di carico di lavoro, oppure puoi creare la tua configurazione. Se si sceglie una configurazione personalizzata, è necessario comprendere le opzioni disponibili. "Scopri di più".

Configurare la rete

1. Assicurarsi che VNET e le subnet supportino la connettività tra il connettore e Cloud Volumes ONTAP.
2. Abilitare l'accesso a Internet in uscita dal VNET di destinazione in modo che il connettore e Cloud Volumes ONTAP possano contattare diversi endpoint.

   Questo passaggio è importante perché il connettore non è in grado di gestire Cloud Volumes ONTAP senza accesso a Internet in uscita. Se è necessario limitare la connettività in uscita, fare riferimento all'elenco degli endpoint per "Il connettore e Cloud Volumes ONTAP".

"Scopri di più sui requisiti di rete".

Avviare Cloud Volumes ONTAP utilizzando Cloud Manager

Fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro), selezionare il tipo di sistema che si desidera implementare e completare la procedura guidata. "Leggi le istruzioni dettagliate".

Link correlati

- "Valutazione"
- "Creazione di un connettore da Cloud Manager"
- "Creazione di un connettore da Azure Marketplace"
- "Installazione del software del connettore su un host Linux"
- "Cosa fa Cloud Manager con le autorizzazioni Azure"

Pianificazione della configurazione di Cloud Volumes ONTAP in Azure

Quando si implementa Cloud Volumes ONTAP in Azure, è possibile scegliere un sistema preconfigurato che soddisfi i requisiti del carico di lavoro oppure creare una configurazione personalizzata. Se si sceglie una configurazione personalizzata, è necessario comprendere le opzioni disponibili.

Scelta di un tipo di licenza

Cloud Volumes ONTAP è disponibile in due opzioni di prezzo: Pay-as-you-go e Bring Your Own License (BYOL). Per il pay-as-you-go, puoi scegliere tra tre licenze: Explore, Standard o Premium. Ogni licenza offre diverse capacità e opzioni di calcolo.

"Configurazioni supportate per Cloud Volumes ONTAP 9.7 in Azure"

Comprendere i limiti dello storage

Il limite di capacità raw per un sistema Cloud Volumes ONTAP è legato alla licenza. Ulteriori limiti influiscono sulle dimensioni degli aggregati e dei volumi. Durante la pianificazione della configurazione, è necessario conoscere questi limiti.

"Limiti di storage per Cloud Volumes ONTAP 9.7 in Azure"

Dimensionamento del sistema in Azure

Il dimensionamento del sistema Cloud Volumes ONTAP può aiutarti a soddisfare i requisiti di performance 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

Esaminare i tipi di macchine virtuali supportati in "Note di rilascio di Cloud Volumes ONTAP" Quindi, esaminare i dettagli relativi a ciascun tipo di macchina virtuale supportato. Tenere presente che ogni tipo di macchina virtuale supporta un numero specifico di dischi dati.

- "Documentazione di Azure: Dimensioni generali delle macchine virtuali"
- "Documentazione di Azure: Dimensioni delle macchine virtuali ottimizzate per la memoria"

Tipo di disco Azure

Quando crei volumi per Cloud Volumes ONTAP, devi scegliere lo storage cloud sottostante che Cloud Volumes ONTAP utilizza come disco.

I sistemi HA utilizzano i blob di pagina Premium. Nel frattempo, i sistemi a nodo singolo possono utilizzare due tipi di dischi gestiti Azure:

- *Dischi gestiti SSD Premium* offrono performance elevate per carichi di lavoro i/o-intensive a un costo più elevato.
- I *dischi gestiti SSD standard* offrono performance costanti per i carichi di lavoro che richiedono IOPS ridotti.
- *Dischi gestiti HDD standard* sono una buona scelta se non hai bisogno di IOPS elevati e vuoi ridurre i

costi.

Per ulteriori informazioni sui casi di utilizzo di questi dischi, vedere "Documentazione di Microsoft Azure: Quali tipi di dischi sono disponibili in Azure?".

Dimensioni del disco Azure

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

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

Quando si sceglie una dimensione del disco, è necessario prendere in considerazione diversi fattori. Le dimensioni del disco influiscono sul costo dello storage, sulle dimensioni dei volumi che è possibile creare in un aggregato, sulla capacità totale disponibile per Cloud Volumes ONTAP e sulle performance dello storage.

Le prestazioni di Azure Premium Storage sono legate alle dimensioni del disco. I dischi più grandi offrono IOPS e throughput più elevati. Ad esempio, la scelta di dischi da 1 TB può offrire prestazioni migliori rispetto ai dischi da 500 GB, a un costo superiore.

Non esistono differenze di performance tra le dimensioni dei dischi per lo storage standard. È necessario scegliere le dimensioni del disco in base alla capacità richiesta.

Fare riferimento a Azure per IOPS e throughput in base alle dimensioni del disco:

- "Microsoft Azure: Prezzi dei dischi gestiti"
- "Microsoft Azure: Page Blobs pricing"

Scelta di una configurazione che supporti Flash cache

Una configurazione Cloud Volumes ONTAP in Azure include lo storage NVMe locale, che Cloud Volumes ONTAP utilizza come *Flash cache* per migliorare le performance. "Scopri di più su Flash cache".

Foglio di lavoro con le informazioni di rete di Azure

Quando si implementa Cloud Volumes ONTAP in Azure, è necessario specificare i dettagli della rete virtuale. È possibile utilizzare un foglio di lavoro per raccogliere le informazioni dall'amministratore.

Informazioni su Azure	Il tuo valore
Regione	
Rete virtuale (VNET)	
Subnet	
Gruppo di sicurezza di rete (se si utilizza il proprio)	

Scelta della velocità di scrittura

Cloud Manager consente di scegliere un'impostazione della velocità di scrittura per i sistemi Cloud Volumes ONTAP a nodo singolo. Prima di scegliere una velocità di scrittura, è necessario comprendere le differenze tra le impostazioni normali e alte e i rischi e le raccomandazioni quando si utilizza un'elevata velocità di scrittura.

Differenza tra la velocità di scrittura normale e l'alta velocità di scrittura

Quando si sceglie la normale velocità di scrittura, i dati vengono scritti direttamente su disco, riducendo così la probabilità di perdita di dati in caso di un'interruzione non pianificata del sistema.

Quando si sceglie un'elevata velocità di scrittura, i dati vengono memorizzati nel buffer prima che vengano scritti su disco, garantendo prestazioni di scrittura più rapide. A causa di questo caching, vi è la possibilità di perdita di dati in caso di un'interruzione non pianificata del sistema.

La quantità di dati che è possibile perdere in caso di interruzione non pianificata del sistema è l'intervallo degli ultimi due punti di coerenza. Un punto di coerenza è l'azione di scrittura dei dati bufferizzati su disco. Un punto di coerenza si verifica quando il registro di scrittura è pieno o dopo 10 secondi (a seconda di quale condizione si verifica per prima). Tuttavia, le performance del volume di AWS EBS possono influire sul tempo di elaborazione dei punti di coerenza.

Quando utilizzare un'elevata velocità di scrittura

L'elevata velocità di scrittura è una buona scelta se per il carico di lavoro sono richieste prestazioni di scrittura rapide e se si può resistere al rischio di perdita di dati in caso di un'interruzione non pianificata del sistema.

Consigli quando si utilizza un'elevata velocità di scrittura

Se si attiva l'alta velocità di scrittura, è necessario garantire la protezione in scrittura a livello di applicazione.

Scelta di un profilo di utilizzo del volume

ONTAP include diverse funzionalità di efficienza dello storage che consentono di ridurre la quantità totale di storage necessaria. Quando crei un volume in Cloud Manager, puoi scegliere un profilo che abiliti queste funzionalità o un profilo che le disabiliti. Dovresti saperne di più su queste funzionalità per aiutarti a decidere quale profilo utilizzare.

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

Thin provisioning
: Presenta uno storage logico maggiore per gli host o gli utenti rispetto al pool di storage fisico. Invece di preallocare lo spazio di storage, lo spazio di storage viene allocato dinamicamente a ciascun volume durante la scrittura dei dati.

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

Compressione
: Riduce la capacità fisica richiesta per memorizzare i dati comprimendo i dati all'interno di un volume su storage primario, secondario e di archivio.

Requisiti di rete per implementare e gestire Cloud Volumes ONTAP in Azure

Configura la tua rete Azure in modo che i sistemi Cloud Volumes ONTAP possano funzionare correttamente. Ciò include il collegamento in rete per il connettore e Cloud Volumes ONTAP.

Requisiti per Cloud Volumes ONTAP

I seguenti requisiti di rete devono essere soddisfatti in Azure.

Accesso a Internet in uscita per Cloud Volumes ONTAP

Cloud Volumes ONTAP richiede l'accesso a Internet in uscita per inviare messaggi a NetApp AutoSupport, che monitora in maniera proattiva lo stato dello storage.

I criteri di routing e firewall devono consentire il traffico HTTP/HTTPS ai seguenti endpoint in modo che Cloud Volumes ONTAP possa inviare messaggi AutoSupport:

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

"Scopri come configurare AutoSupport".

Gruppi di sicurezza

Non è necessario creare gruppi di sicurezza perché Cloud Manager fa questo per te. Se è necessario utilizzare il proprio, fare riferimento alle regole del gruppo di protezione elencate di seguito.

Numero di indirizzi IP

Cloud Manager assegna il seguente numero di indirizzi IP a Cloud Volumes ONTAP in Azure:

- Nodo singolo: 5 indirizzi IP
- Coppia HA: 16 indirizzi IP

Si noti che Cloud Manager crea una LIF di gestione SVM sulle coppie ha, ma non sui sistemi a nodo singolo in Azure.

LIF è un indirizzo IP associato a una porta fisica. Per strumenti di gestione come SnapCenter è necessaria una LIF di gestione SVM.

Connessione da Cloud Volumes ONTAP a Azure BLOB storage per il tiering dei dati

Se si desidera eseguire il tiering dei dati cold allo storage Azure Blob, non è necessario configurare una connessione tra il Tier di performance e il Tier di capacità, purché Cloud Manager disponga delle autorizzazioni necessarie. Cloud Manager abilita un endpoint del servizio VNET se la policy di Cloud Manager dispone delle seguenti autorizzazioni:

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

Queste autorizzazioni sono incluse nella versione più recente "Policy di Cloud Manager".

Per ulteriori informazioni sull'impostazione del tiering dei dati, vedere "Tiering dei dati cold su storage a oggetti a basso costo".

Connessioni a sistemi ONTAP in altre reti

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

Per istruzioni, fare riferimento a. "Documentazione di Microsoft Azure: Crea una connessione Site-to-Site nel portale Azure".

Requisiti per il connettore

Configura la tua rete in modo che il connettore possa gestire risorse e processi all'interno del tuo ambiente di cloud pubblico. Il passaggio più importante è garantire l'accesso a Internet in uscita a vari endpoint.

Se la rete utilizza un server proxy per tutte le comunicazioni a Internet, è possibile specificare il server proxy dalla pagina Impostazioni. Fare riferimento a. "Configurazione del connettore per l'utilizzo di un server proxy".

Connessioni alle reti di destinazione

Un connettore richiede una connessione di rete ai VPC e ai VNet in cui si desidera implementare Cloud Volumes ONTAP.

Ad esempio, se si installa un connettore nella rete aziendale, è necessario impostare una connessione VPN a VPC o VNET in cui si avvia Cloud Volumes ONTAP.

Accesso a Internet in uscita

Il connettore richiede l'accesso a Internet in uscita per gestire risorse e processi all'interno del tuo ambiente di cloud pubblico. Un connettore contatta i seguenti endpoint durante la gestione delle risorse in Azure:

Endpoint	Scopo
https://management.azure.com https://login.microsoftonline.com	Consente a Cloud Manager di implementare e gestire Cloud Volumes ONTAP nella maggior parte delle regioni Azure.
https://management.microsoftazure.de https://login.microsoftonline.de	Consente a Cloud Manager di implementare e gestire Cloud Volumes ONTAP nelle regioni di Azure Germania.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Consente a Cloud Manager di implementare e gestire Cloud Volumes ONTAP nelle regioni di Azure US Gov.
https://api.services.cloud.netapp.com:443	Richieste API a NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Fornisce l'accesso a immagini, manifesti e modelli software.
https://repo.cloud.support.netapp.com	Utilizzato per scaricare le dipendenze di Cloud Manager.
http://repo.mysql.com/	Utilizzato per scaricare MySQL.

Endpoint	Scopo
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Consente a Cloud Manager di accedere e scaricare manifesti, modelli e immagini di aggiornamento di Cloud Volumes ONTAP.
https://cloudmanagerinfraprod.azurecr.io	Accesso alle immagini software dei componenti container per un'infrastruttura che esegue Docker e fornisce una soluzione per l'integrazione dei servizi con Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Consente a NetApp di eseguire lo streaming dei dati dai record di audit.
https://cloudmanager.cloud.netapp.com	Comunicazione con il servizio Cloud Manager, che include gli account Cloud Central.
https://netapp-cloud-account.auth0.com	Comunicazione con NetApp Cloud Central per l'autenticazione utente centralizzata.
https://mysupport.netapp.com	Comunicazione con NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Comunicazione con NetApp per la registrazione del supporto e delle licenze di sistema.
https://ipa-signer.cloudmanager.netapp.com	Consente a Cloud Manager di generare licenze (ad esempio, una licenza FlexCache per Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Necessario per connettere i sistemi Cloud Volumes ONTAP a un cluster Kubernetes. Gli endpoint consentono l'installazione di NetApp Trident.
*.blob.core.windows.net	Richiesto per coppie ha quando si utilizza un proxy.
Varie sedi di terze parti, ad esempio: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org Le sedi di terze parti sono soggette a modifiche.	Durante gli aggiornamenti, Cloud Manager scarica i pacchetti più recenti per le dipendenze di terze parti.

Sebbene sia necessario eseguire quasi tutte le attività dall'interfaccia utente SaaS, sul connettore è ancora disponibile un'interfaccia utente locale. Il computer che esegue il browser Web deve disporre di connessioni ai seguenti endpoint:

Endpoint	Scopo
L'host del connettore	Per caricare la console di Cloud Manager, è necessario inserire l'indirizzo IP dell'host da un browser Web. A seconda della connettività con il cloud provider, è possibile utilizzare l'IP privato o un IP pubblico assegnato all'host: • Un IP privato funziona se si dispone di una VPN e di un accesso diretto alla rete virtuale • Un IP pubblico funziona in qualsiasi scenario di rete In ogni caso, è necessario proteggere l'accesso alla rete assicurandosi che le regole del gruppo di protezione consentano l'accesso solo da IP o subnet autorizzati.
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	Il browser Web si connette a questi endpoint per un'autenticazione utente centralizzata tramite NetApp Cloud Central.
https://widget.intercom.io	Per chat in-product che ti consente di parlare con gli esperti cloud di NetApp.

Regole del gruppo di sicurezza per Cloud Volumes ONTAP

Cloud Manager crea gruppi di sicurezza Azure che includono le regole in entrata e in uscita necessarie per il corretto funzionamento di Cloud Volumes ONTAP. È possibile fare riferimento alle porte a scopo di test o se si preferisce utilizzare i propri gruppi di protezione.

Il gruppo di sicurezza per Cloud Volumes ONTAP richiede regole sia in entrata che in uscita.

Regole in entrata per sistemi a nodo singolo

Le regole elencate di seguito consentono il traffico, a meno che la descrizione non noti che blocca lo specifico traffico in entrata.

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
1000 inbound_ssh	22 TCP	Qualsiasi a qualsiasi	Accesso SSH all'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi
1001 inbound_http	80 TCP	Qualsiasi a qualsiasi	Accesso HTTP alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
1002 inbound_111_tcp	111 TCP	Qualsiasi a qualsiasi	Chiamata a procedura remota per NFS
1003 inbound_111_udp	111 UDP	Qualsiasi a qualsiasi	Chiamata a procedura remota per NFS

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
1004 inbound_139	139 TCP	Qualsiasi a qualsiasi	Sessione del servizio NetBIOS per CIFS
1005 inbound_161-162 _tcp	161-162 TCP	Qualsiasi a qualsiasi	Protocollo di gestione di rete semplice
1006 inbound_161-162 _udp	161-162 UDP	Qualsiasi a qualsiasi	Protocollo di gestione di rete semplice
1007 inbound_443	443 TCP	Qualsiasi a qualsiasi	Accesso HTTPS alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
1008 inbound_445	445 TCP	Qualsiasi a qualsiasi	Microsoft SMB/CIFS su TCP con frame NetBIOS
1009 inbound_635_tcp	635 TCP	Qualsiasi a qualsiasi	Montaggio NFS
1010 inbound_635_udp	635 UDP	Qualsiasi a qualsiasi	Montaggio NFS
1011 inbound_749	749 TCP	Qualsiasi a qualsiasi	Kerberos
1012 inbound_2049_tcp	2049 TCP	Qualsiasi a qualsiasi	Daemon del server NFS
1013 inbound_2049_udp	2049 UDP	Qualsiasi a qualsiasi	Daemon del server NFS
1014 inbound_3260	3260 TCP	Qualsiasi a qualsiasi	Accesso iSCSI tramite LIF dei dati iSCSI
1015 inbound_4045-4046_tcp	4045-4046 TCP	Qualsiasi a qualsiasi	NFS lock daemon e network status monitor
1016 inbound_4045-4046_udp	4045-4046 UDP	Qualsiasi a qualsiasi	NFS lock daemon e network status monitor
1017 inbound_10000	10000 TCP	Qualsiasi a qualsiasi	Backup con NDMP
1018 inbound_11104-11105	11104-11105 TCP	Qualsiasi a qualsiasi	Trasferimento dei dati SnapMirror
3000 inbound_deny _all_tcp	Qualsiasi porta TCP	Qualsiasi a qualsiasi	Blocca tutto il traffico TCP in entrata
3001 inbound_deny _all_udp	Qualsiasi porta UDP	Qualsiasi a qualsiasi	Blocca tutto il traffico UDP in entrata
65000 AllowVnetInBound	Qualsiasi porta qualsiasi protocollo	Da VirtualNetwork a VirtualNetwork	Traffico in entrata dall'interno di VNET
65001 AllowAzureLoad BalancerInBound	Qualsiasi porta qualsiasi protocollo	AzureLoadBalancer a qualsiasi	Traffico di dati dal bilanciamento del carico standard di Azure
65500 DenyAllInBound	Qualsiasi porta qualsiasi protocollo	Qualsiasi a qualsiasi	Bloccare tutto il traffico in entrata

Regole in entrata per i sistemi ha

Le regole elencate di seguito consentono il traffico, a meno che la descrizione non noti che blocca lo specifico traffico in entrata.

> I sistemi HA hanno meno regole in entrata rispetto ai sistemi a nodo singolo perché il traffico dati in entrata passa attraverso il bilanciamento del carico standard di Azure. Per questo motivo, il traffico proveniente dal bilanciamento del carico deve essere aperto, come mostrato nella regola "AllowAzureLoadBalancerInBound".

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
100 inbound_443	443 qualsiasi protocollo	Qualsiasi a qualsiasi	Accesso HTTPS alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
101 inbound_111_tcp	111 qualsiasi protocollo	Qualsiasi a qualsiasi	Chiamata a procedura remota per NFS
102 inbound_2049_tcp	2049 qualsiasi protocollo	Qualsiasi a qualsiasi	Daemon del server NFS
111 inbound_ssh	22 qualsiasi protocollo	Qualsiasi a qualsiasi	Accesso SSH all'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi
121 inbound_53	53 qualsiasi protocollo	Qualsiasi a qualsiasi	DNS e CIFS
65000 AllowVnetInBound	Qualsiasi porta qualsiasi protocollo	Da VirtualNetwork a VirtualNetwork	Traffico in entrata dall'interno di VNET
65001 AllowAzureLoad BalancerInBound	Qualsiasi porta qualsiasi protocollo	AzureLoadBalancer a qualsiasi	Traffico di dati dal bilanciamento del carico standard di Azure
65500 DenyAllInBound	Qualsiasi porta qualsiasi protocollo	Qualsiasi a qualsiasi	Bloccare tutto il traffico in entrata

Regole in uscita

Il gruppo di protezione predefinito per Cloud Volumes ONTAP apre tutto il traffico in uscita. Se questo è accettabile, attenersi alle regole di base per le chiamate in uscita. Se sono necessarie regole più rigide, utilizzare le regole avanzate in uscita.

Regole di base in uscita

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

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

Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte richieste per le comunicazioni in uscita da Cloud Volumes ONTAP.

L'origine è l'interfaccia (indirizzo IP) del sistema Cloud Volumes ONTAP.

Servizio	Porta	Protocollo	Origine	Destinazione	Scopo
Active Directory	88	TCP	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Autenticazione Kerberos V.
	137	UDP	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Servizio nomi NetBIOS
	138	UDP	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS
	139	TCP	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS
	389	TCP E UDP	LIF di gestione dei nodi	Insieme di strutture di Active Directory	LDAP
	445	TCP	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	464	TCP	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	464	UDP	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos
	749	TCP	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Kerberos V change & set Password (RPCSEC_GSS)
	88	TCP	Data LIF (NFS, CIFS, iSCSI)	Insieme di strutture di Active Directory	Autenticazione Kerberos V.
	137	UDP	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Servizio nomi NetBIOS
	138	UDP	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS
	139	TCP	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS
	389	TCP E UDP	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	LDAP
	445	TCP	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	464	TCP	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	464	UDP	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos
	749	TCP	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Kerberos V change & set password (RPCSEC_GSS)
DHCP	68	UDP	LIF di gestione dei nodi	DHCP	Client DHCP per la prima installazione

Servizio	Porta	Protocollo	Origine	Destinazione	Scopo
DHCPS	67	UDP	LIF di gestione dei nodi	DHCP	Server DHCP
DNS	53	UDP	LIF di gestione dei nodi e LIF dei dati (NFS, CIFS)	DNS	DNS
NDMP	18600–18699	TCP	LIF di gestione dei nodi	Server di destinazione	Copia NDMP
SMTP	25	TCP	LIF di gestione dei nodi	Server di posta	Gli avvisi SMTP possono essere utilizzati per AutoSupport
SNMP	161	TCP	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	161	UDP	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	162	TCP	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	162	UDP	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
SnapMirror	11104	TCP	LIF intercluster	ONTAP Intercluster LIF	Gestione delle sessioni di comunicazione tra cluster per SnapMirror
	11105	TCP	LIF intercluster	ONTAP Intercluster LIF	Trasferimento dei dati SnapMirror
Syslog	514	UDP	LIF di gestione dei nodi	Server syslog	Messaggi di inoltro syslog

Regole del gruppo di sicurezza per il connettore

Il gruppo di protezione per il connettore richiede regole sia in entrata che in uscita.

Regole in entrata

L'origine delle regole in entrata nel gruppo di sicurezza predefinito è 0.0.0.0/0.

Porta	Protocollo	Scopo
22	SSH	Fornisce l'accesso SSH all'host del connettore
80	HTTP	Fornisce l'accesso HTTP dai browser Web client all'interfaccia utente locale
443	HTTPS	Fornisce l'accesso HTTPS dai browser Web client all'interfaccia utente locale

Regole in uscita

Il gruppo di protezione predefinito per il connettore apre tutto il traffico in uscita. Se questo è accettabile, attenersi alle regole di base per le chiamate in uscita. Se sono necessarie regole più rigide, utilizzare le regole avanzate in uscita.

Regole di base in uscita

Il gruppo di protezione predefinito per il connettore include le seguenti regole in uscita.

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

Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte richieste per la comunicazione in uscita dal connettore.

L'indirizzo IP di origine è l'host del connettore.

Servizio	Porta	Protocollo	Destinazione	Scopo
Active Directory	88	TCP	Insieme di strutture di Active Directory	Autenticazione Kerberos V.
	139	TCP	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS
	389	TCP	Insieme di strutture di Active Directory	LDAP
	445	TCP	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	464	TCP	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	749	TCP	Insieme di strutture di Active Directory	Modifica e impostazione della password Kerberos V di Active Directory (RPCSEC_GSS)
	137	UDP	Insieme di strutture di Active Directory	Servizio nomi NetBIOS
	138	UDP	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS
	464	UDP	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos

Servizio	Porta	Protocollo	Destinazione	Scopo
Chiamate API e AutoSupport	443	HTTPS	LIF gestione cluster ONTAP e Internet in uscita	Chiamate API ad AWS e ONTAP e invio di messaggi AutoSupport a NetApp
Chiamate API	3000	TCP	LIF gestione cluster ONTAP	Chiamate API a ONTAP
DNS	53	UDP	DNS	Utilizzato per la risoluzione DNS da parte di Cloud Manager

Lancio di Cloud Volumes ONTAP in Azure

È possibile avviare un sistema a nodo singolo o una coppia ha in Azure creando un ambiente di lavoro Cloud Volumes ONTAP in Cloud Manager.

Prima di iniziare

- Si dovrebbe avere un "Connettore associato all'area di lavoro".

> Per creare un connettore, è necessario essere un amministratore dell'account. Quando crei il tuo primo ambiente di lavoro Cloud Volumes ONTAP, Cloud Manager ti chiede di creare un connettore se non ne hai ancora uno.

- "Si dovrebbe essere pronti a lasciare il connettore sempre in funzione".
- È necessario aver scelto una configurazione e ottenuto le informazioni di rete di Azure dall'amministratore. Per ulteriori informazioni, vedere "Pianificazione della configurazione di Cloud Volumes ONTAP".
- Per implementare un sistema BYOL, è necessario il numero seriale a 20 cifre (chiave di licenza) per ciascun nodo.

A proposito di questa attività

Quando Cloud Manager crea un sistema Cloud Volumes ONTAP in Azure, crea diversi oggetti Azure, come un gruppo di risorse, interfacce di rete e account di storage. Al termine della procedura guidata, è possibile visualizzare un riepilogo delle risorse.

> **Potenziale perdita di dati**
>
> L'implementazione di Cloud Volumes ONTAP in un gruppo di risorse condiviso esistente non è consigliata a causa del rischio di perdita di dati. Sebbene il rollback sia attualmente disattivato per impostazione predefinita quando si utilizza l'API per la distribuzione in un gruppo di risorse esistente, l'eliminazione di Cloud Volumes ONTAP potenzialmente eliminerà altre risorse da quel gruppo condiviso.
>
> La Best practice consiste nell'utilizzare un nuovo gruppo di risorse dedicato per Cloud Volumes ONTAP. Questa è l'opzione predefinita e consigliata solo quando si implementa Cloud Volumes ONTAP in Azure da Cloud Manager.

Fasi

1. Nella pagina ambienti di lavoro, fare clic su **Aggiungi ambiente di lavoro** e seguire le istruzioni.
2. **Scegli una località**: Seleziona **Microsoft Azure** e **nodo singolo Cloud Volumes ONTAP** o **alta disponibilità Cloud Volumes ONTAP**.
3. **Dettagli e credenziali**: Se si desidera, modificare le credenziali e la sottoscrizione di Azure, specificare il nome del cluster e del gruppo di risorse, aggiungere tag, se necessario, quindi specificare le credenziali.

   La seguente tabella descrive i campi per i quali potrebbero essere necessarie indicazioni:

Campo	Descrizione
Nome ambiente di lavoro	Cloud Manager utilizza il nome dell'ambiente di lavoro per assegnare un nome sia al sistema Cloud Volumes ONTAP che alla macchina virtuale Azure. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di protezione predefinito.
Nome gruppo di risorse	Mantenere il nome predefinito per il nuovo gruppo di risorse o deselezionare **Usa predefinito** e immettere il proprio nome per il nuovo gruppo di risorse. La Best practice consiste nell'utilizzare un nuovo gruppo di risorse dedicato per Cloud Volumes ONTAP. Sebbene sia possibile implementare Cloud Volumes ONTAP in un gruppo di risorse condiviso esistente utilizzando l'API, non è consigliabile a causa del rischio di perdita di dati. Per ulteriori informazioni, vedere l'avviso riportato sopra.
Tag	I tag sono metadati per le risorse Azure. Quando si inseriscono i tag in questo campo, Cloud Manager li aggiunge al gruppo di risorse associato al sistema Cloud Volumes ONTAP. È possibile aggiungere fino a quattro tag dall'interfaccia utente durante la creazione di un ambiente di lavoro e aggiungerne altri dopo la creazione. Tenere presente che l'API non si limita a quattro tag durante la creazione di un ambiente di lavoro. Per informazioni sui tag, fare riferimento a. "Documentazione di Microsoft Azure: Utilizzo di 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 Gestore di sistema di OnCommand o la relativa CLI.
Modifica credenziali	È possibile scegliere credenziali Azure diverse e un abbonamento Azure diverso da utilizzare con questo sistema Cloud Volumes ONTAP. Per implementare un sistema Cloud Volumes ONTAP pay-as-you-go, devi associare un abbonamento Azure Marketplace all'abbonamento Azure selezionato. "Scopri come aggiungere le credenziali".

   Il video seguente mostra come associare un abbonamento Marketplace a un abbonamento Azure:

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

4. **Servizi**: Mantieni abilitati i servizi o disabilita i singoli servizi che non vuoi utilizzare con Cloud Volumes ONTAP.
   - "Scopri di più sulla conformità al cloud".
   - "Scopri di più sul backup nel cloud".
5. **Location & Connectivity** (posizione e connettività): Selezionare una posizione e un gruppo di sicurezza e selezionare la casella di controllo per confermare la connettività di rete tra Cloud Manager e la posizione di destinazione.

6. **License and Support Site account**: Specificare se si desidera utilizzare la funzione pay-as-you-go o BYOL, quindi specificare un account NetApp Support Site.

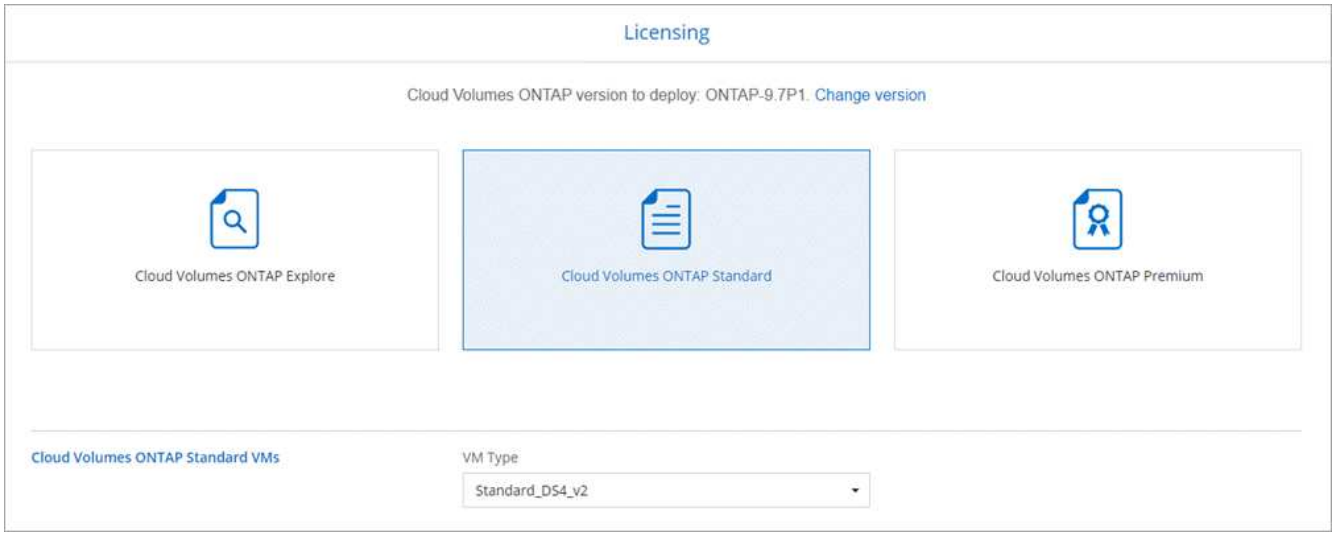
   Per informazioni sul funzionamento delle licenze, vedere "Licensing".

   Un account NetApp Support Site è opzionale per il pay-as-you-go, ma necessario per i sistemi BYOL. "Scopri come aggiungere account NetApp Support Site".

7. **Pacchetti preconfigurati**: Selezionare uno dei pacchetti per implementare rapidamente un sistema Cloud Volumes ONTAP oppure fare clic su **Crea la mia configurazione**.

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

8. **Licenza**: Modificare la versione di Cloud Volumes ONTAP in base alle esigenze, selezionare una licenza e selezionare un tipo di macchina virtuale.



   Se le esigenze cambiano dopo l'avvio del sistema, è possibile modificare il tipo di licenza o macchina virtuale in un secondo momento.

   > Se è disponibile una release Release Candidate, General Availability o patch più recente per la versione selezionata, Cloud Manager aggiorna il sistema a quella versione durante la creazione dell'ambiente di lavoro. Ad esempio, l'aggiornamento si verifica se si seleziona Cloud Volumes ONTAP 9.6 RC1 e 9.6 GA è disponibile. L'aggiornamento non si verifica da una release all'altra, ad esempio da 9.6 a 9.7.

9. **Iscriviti al marketplace Azure**: Segui la procedura se Cloud Manager non è riuscito ad abilitare le implementazioni programmatiche di Cloud Volumes ONTAP.
10. **Risorse di storage sottostanti**: Scegliere le impostazioni per l'aggregato iniziale: Un tipo di disco, una dimensione per ciascun disco e se attivare il tiering dei dati per lo storage Blob.

    Tenere presente quanto segue:

    - Il tipo di disco è per il volume iniziale. È possibile scegliere un tipo di disco diverso per i volumi successivi.
    - Le dimensioni del disco sono per tutti i dischi nell'aggregato iniziale e per eventuali aggregati aggiuntivi creati da Cloud Manager quando si utilizza l'opzione di provisioning semplice. È possibile creare

aggregati che utilizzano una dimensione del disco diversa utilizzando l'opzione di allocazione avanzata.

Per informazioni sulla scelta del tipo e delle dimensioni di un disco, vedere "Dimensionamento del sistema in Azure".

- Quando si crea o si modifica un volume, è possibile scegliere un criterio di tiering del volume specifico.
- Se si disattiva il tiering dei dati, è possibile attivarlo sugli aggregati successivi.

"Scopri di più sul tiering dei dati".

11. **Write Speed & WORM** (solo sistemi a nodo singolo): Scegliere **normale** o **alta** velocità di scrittura e attivare lo storage WORM (Write Once, Read Many), se desiderato.

    La scelta di una velocità di scrittura è supportata solo nei sistemi a nodo singolo.

    "Scopri di più sulla velocità di scrittura".

    NON è possibile attivare WORM se è stato attivato il tiering dei dati.

    "Scopri di più sullo storage WORM".

12. **Secure Communication to Storage & WORM** (solo ha): Scegliere se abilitare una connessione HTTPS agli account di storage Azure e attivare lo storage WORM (Write Once, Read Many), se lo si desidera.

    La connessione HTTPS proviene da una coppia ha di Cloud Volumes ONTAP 9.7 agli account di storage Azure. L'attivazione di questa opzione può influire sulle prestazioni di scrittura. Non è possibile modificare l'impostazione dopo aver creato l'ambiente di lavoro.

    "Scopri di più sullo storage WORM".

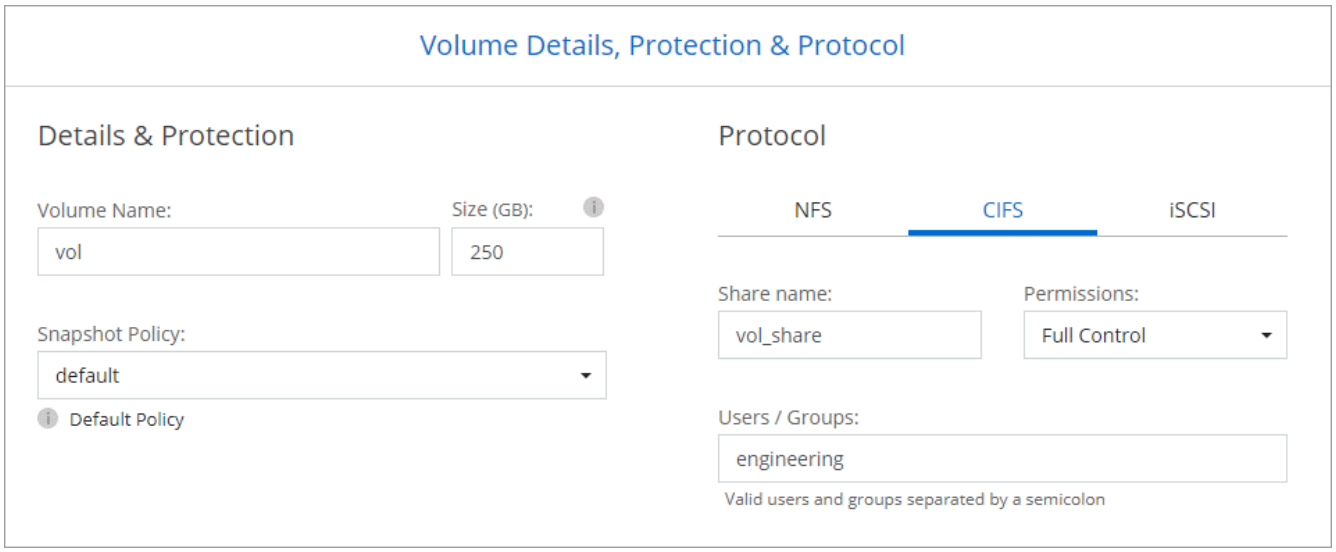
13. **Create Volume** (Crea volume): Inserire i dettagli del nuovo volume o fare clic su **Skip** (Ignora).

    Alcuni dei campi di questa pagina sono esplicativi. La seguente tabella descrive i campi per i quali potrebbero essere necessarie indicazioni:

Campo	Descrizione
Dimensione	Le dimensioni massime che è possibile inserire dipendono in gran parte dall'attivazione o meno del thin provisioning, che consente di creare un volume più grande dello storage fisico attualmente disponibile per l'IT.
Controllo degli accessi (solo per NFS)	Un criterio di esportazione definisce i client nella subnet che possono accedere al volume. Per impostazione predefinita, Cloud Manager inserisce un valore che fornisce l'accesso a tutte le istanze nella subnet.
Permessi e utenti/gruppi (solo per CIFS)	Questi campi consentono di controllare il livello di accesso a una condivisione per utenti e gruppi (detti anche elenchi di controllo degli accessi o ACL). È possibile specificare utenti o gruppi Windows locali o di dominio, utenti o gruppi UNIX. Se si specifica un nome utente Windows di dominio, è necessario includere il dominio dell'utente utilizzando il formato dominio/nome utente.

Campo	Descrizione
Policy di Snapshot	Una policy di copia Snapshot specifica la frequenza e il numero di copie Snapshot NetApp create automaticamente. Una copia Snapshot di NetApp è un'immagine del file system point-in-time che non ha alcun impatto sulle performance e richiede uno storage minimo. È possibile scegliere il criterio predefinito o nessuno. È possibile scegliere nessuno per i dati transitori, ad esempio tempdb per Microsoft SQL Server.
Opzioni avanzate (solo per NFS)	Selezionare una versione NFS per il volume: NFSv3 o NFSv4.
Initiator group e IQN (solo per iSCSI)	Le destinazioni di storage iSCSI sono denominate LUN (unità logiche) e vengono presentate agli host come dispositivi a blocchi standard. I gruppi di iniziatori sono tabelle dei nomi dei nodi host iSCSI e controllano quali iniziatori hanno accesso a quali LUN. Le destinazioni iSCSI si collegano alla rete tramite schede di rete Ethernet standard (NIC), schede TOE (TCP offload Engine) con iniziatori software, adattatori di rete convergenti (CNA) o adattatori host busto dedicati (HBA) e sono identificate da nomi qualificati iSCSI (IQN). Quando si crea un volume iSCSI, Cloud Manager crea automaticamente un LUN. Abbiamo semplificato la creazione di un solo LUN per volume, per cui non è necessario alcun intervento di gestione. Dopo aver creato il volume, "Utilizzare IQN per connettersi al LUN dagli host".

La seguente immagine mostra la pagina Volume compilata per il protocollo CIFS:



14. **CIFS Setup**: Se si sceglie il protocollo CIFS, impostare 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 il server CIFS si unisce.
Dominio Active Directory da unire	L'FQDN del dominio Active Directory (ad) a cui si desidera che il server CIFS si unisca.

Campo	Descrizione
Credenziali autorizzate per l'accesso al dominio	Il nome e la password di un account Windows con privilegi sufficienti per aggiungere computer all'unità organizzativa (OU) specificata nel dominio ad.
Nome NetBIOS del server CIFS	Un nome 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 i servizi di dominio ad Azure come server ad per Cloud Volumes ONTAP, 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 dai servizi di dominio ad di Azure"^]
Dominio DNS	Il dominio DNS per la SVM (Storage Virtual Machine) di Cloud Volumes ONTAP. Nella maggior parte dei casi, il dominio è lo stesso del dominio ad.
Server NTP	Selezionare **Use Active Directory Domain** (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, utilizzare l'API. Vedere "Guida per sviluppatori API di Cloud Manager" per ulteriori informazioni.

15. **Profilo di utilizzo, tipo di disco e policy di tiering**: Scegliere se attivare le funzionalità di efficienza dello storage e modificare la policy di tiering dei volumi, se necessario.

    Per ulteriori informazioni, vedere "Comprensione dei profili di utilizzo dei volumi" e. "Panoramica sul tiering dei dati".

16. **Review & Approve** (Rivedi e approva): Consente di rivedere e confermare le selezioni.
    a. Esaminare i dettagli della configurazione.
    b. Fare clic su **ulteriori informazioni** per rivedere i dettagli sul supporto e le risorse di Azure che Cloud Manager acquisterà.
    c. Selezionare le caselle di controllo **ho capito…**.
    d. Fare clic su **Go**.

Risultato

Cloud Manager implementa il sistema Cloud Volumes ONTAP. Puoi tenere traccia dei progressi nella timeline.

In caso di problemi durante l'implementazione del sistema Cloud Volumes ONTAP, esaminare il messaggio di errore. È inoltre possibile selezionare l'ambiente di lavoro e fare clic su **Ricomcreare ambiente**.

Per ulteriore assistenza, visitare il sito Web all'indirizzo "Supporto NetApp Cloud Volumes ONTAP".

Al termine

- Se è stata fornita una condivisione CIFS, assegnare agli utenti o ai gruppi le autorizzazioni per i file e le cartelle e verificare che tali utenti possano accedere alla condivisione e creare un file.
- Se si desidera applicare le quote ai volumi, utilizzare System Manager o l'interfaccia 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.

Informazioni sul copyright

Informazioni sul marchio commerciale