Inizia a utilizzare Microsoft Azure

Cloud Volumes ONTAP

NetApp
April 23, 2024

Sommario

Inizia a utilizzare Microsoft Azure

Avvio rapido di Cloud Volumes ONTAP in Azure

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

1 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"

Se si desidera implementare Cloud Volumes ONTAP in una subnet in cui non è disponibile alcun accesso a Internet, è necessario installare manualmente il connettore e accedere all'interfaccia utente di BlueXP in esecuzione su tale connettore. "Scopri come installare manualmente il connettore in una posizione senza accesso a Internet"

2 Pianificare la configurazione

BlueXP offre pacchetti preconfigurati che soddisfano i requisiti del carico di lavoro, oppure è possibile creare una configurazione personalizzata. Se si sceglie una configurazione personalizzata, è necessario comprendere le opzioni disponibili. "Scopri di più".

3 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 VPC di destinazione per NetApp AutoSupport.

   Questo passaggio non è necessario se si implementa Cloud Volumes ONTAP in una posizione in cui non è disponibile alcun accesso a Internet.

"Scopri di più sui requisiti di rete".

4 Avviare Cloud Volumes ONTAP utilizzando BlueXP

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

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

Pianificare la 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.

Scegliere una licenza Cloud Volumes ONTAP

Per Cloud Volumes ONTAP sono disponibili diverse opzioni di licenza. Ciascuna opzione consente di scegliere un modello di consumo che soddisfi le proprie esigenze.

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

Scegliere una regione supportata

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

Scegliere un tipo di macchina virtuale supportato

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

"Configurazioni supportate per Cloud Volumes ONTAP 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 in Azure"

Dimensionare il 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 con sistemi a nodo singolo

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

I sistemi a nodo singolo possono utilizzare tre 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?".

Tipo di disco Azure con coppie ha

I sistemi HA utilizzano dischi gestiti condivisi SSD Premium che offrono performance elevate per carichi di lavoro i/o-intensive a un costo superiore. Le implementazioni HA create prima della release 9.12.1 utilizzano i blob di pagina Premium.

Dimensioni del disco Azure

Quando si avviano le istanze di Cloud Volumes ONTAP, è necessario scegliere la dimensione predefinita del disco per gli aggregati. BlueXP 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 1 disco TIB può offrire prestazioni migliori rispetto a 500 dischi GiB, 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"

Visualizzare i dischi di sistema predefiniti

Oltre allo storage per i dati degli utenti, BlueXP acquista anche lo storage cloud per i dati del sistema Cloud Volumes ONTAP (dati di avvio, dati root, dati core e NVRAM). A scopo di pianificazione, potrebbe essere utile esaminare questi dettagli prima di implementare Cloud Volumes ONTAP.

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

Il connettore richiede anche un disco di sistema. "Visualizza i dettagli sulla configurazione predefinita del connettore".

Raccogliere informazioni di rete

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)	

Scegliere una velocità di scrittura

BlueXP 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 normali e alte e i rischi e le raccomandazioni quando si utilizza un'elevata velocità di scrittura. "Scopri di più sulla velocità di scrittura".

Scegliere 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 si crea un volume in BlueXP, è possibile scegliere un profilo che attiva queste funzionalità o un profilo che le disattiva. 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 Cloud Volumes ONTAP in Azure

Configura la tua rete Azure in modo che i sistemi Cloud Volumes ONTAP possano funzionare correttamente.

Requisiti per Cloud Volumes ONTAP

I seguenti requisiti di rete devono essere soddisfatti in Azure.

Accesso a Internet in uscita

I nodi Cloud Volumes ONTAP richiedono l'accesso a Internet in uscita per NetApp AutoSupport, che monitora in modo proattivo lo stato di salute del sistema e invia messaggi al supporto tecnico NetApp.

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

Se non è disponibile una connessione Internet in uscita per l'invio di messaggi AutoSupport, BlueXP configura automaticamente i sistemi Cloud Volumes ONTAP in modo che utilizzino il connettore come server proxy. L'unico requisito è garantire che il gruppo di sicurezza del connettore consenta connessioni *inbound* sulla porta 3128. Dopo aver implementato il connettore, aprire questa porta.

Se sono state definite rigide regole in uscita per Cloud Volumes ONTAP, è necessario anche assicurarsi che il gruppo di sicurezza Cloud Volumes ONTAP consenta connessioni *in uscita* sulla porta 3128.

Dopo aver verificato che l'accesso a Internet in uscita è disponibile, è possibile testare AutoSupport per assicurarsi che sia in grado di inviare messaggi. Per istruzioni, fare riferimento a. "Documenti ONTAP: Configurazione di AutoSupport".

Se BlueXP notifica che non è possibile inviare messaggi AutoSupport, "Risolvere i problemi della configurazione AutoSupport".

Indirizzi IP

BlueXP assegna automaticamente il numero richiesto di indirizzi IP privati a Cloud Volumes ONTAP in Azure. È necessario assicurarsi che la rete disponga di un numero sufficiente di indirizzi IP privati.

Il numero di LIF allocati da BlueXP per Cloud Volumes ONTAP dipende dalla distribuzione di un sistema a nodo singolo o di una coppia ha. LIF è un indirizzo IP associato a una porta fisica. Per strumenti di gestione come SnapCenter è necessaria una LIF di gestione SVM.

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

Indirizzi IP per un sistema a nodo singolo

BlueXP assegna 5 o 6 indirizzi IP a un sistema a nodo singolo:

- IP di gestione del cluster

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

> L'IP iSCSI fornisce l'accesso del client sul protocollo iSCSI. Viene inoltre utilizzato dal sistema per altri importanti flussi di lavoro di rete. Questa LIF è obbligatoria e non deve essere eliminata.

- Gestione SVM (opzionale - non configurata per impostazione predefinita)

Indirizzi IP per coppie ha

BlueXP assegna gli indirizzi IP a 4 NIC (per nodo) durante l'implementazione.

Si noti che BlueXP crea una 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 del client sul protocollo iSCSI. Viene inoltre utilizzato dal sistema per altri importanti flussi di lavoro di rete. Questa LIF è obbligatoria e non deve essere eliminata.

NIC1

- IP della rete del cluster

NIC2

- Cluster Interconnect IP (IC ha)

NIC3

- IP NIC Pageblob (accesso al disco)

> NIC3 è applicabile solo alle implementazioni ha che utilizzano lo storage page blob.

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

Inoltre, 4 IP front-end (FIPS) sono configurati per la migrazione in caso di eventi di failover. Questi IP di frontend risiedono nel bilanciamento 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 Azure

Per impostazione predefinita, BlueXP attiva un collegamento privato Azure per le connessioni tra gli account di storage blob di pagina Cloud Volumes ONTAP e Azure.

Nella maggior parte dei casi, non c'è nulla da fare: BlueXP gestisce Azure Private link per te. Tuttavia, se si utilizza Azure Private DNS, sarà necessario modificare un file di configurazione. È inoltre necessario conoscere un requisito per la posizione del connettore in Azure.

È inoltre possibile disattivare la connessione Private link, se richiesto dalle esigenze aziendali. Se si disattiva il collegamento, BlueXP configura Cloud Volumes ONTAP in modo che utilizzi un endpoint del servizio.

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

Connessioni ad altri sistemi ONTAP

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 la rete aziendale.

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

Porta per l'interconnessione ha

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

Per impostazione predefinita, la comunicazione tra le LIF di interconnessione ha è aperta e non esistono regole di gruppo di sicurezza per questa porta. Tuttavia, se si crea un firewall tra le 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 Azure

È necessario utilizzare un gruppo di risorse *dedicato* per ogni coppia di Cloud Volumes ONTAP ha implementata in Azure. In un gruppo di risorse è supportata una sola coppia ha.

BlueXP presenta problemi di connessione se si tenta di implementare una seconda coppia Cloud Volumes ONTAP ha in un gruppo di risorse Azure.

Regole del gruppo di sicurezza

BlueXP crea gruppi di sicurezza Azure che includono le regole in entrata e in uscita di cui Cloud Volumes ONTAP ha bisogno per funzionare correttamente. Si consiglia di 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.

Cerchi informazioni sul connettore? "Visualizzare le regole del gruppo di protezione per il connettore"

Regole in entrata per sistemi a nodo singolo

Quando si crea un ambiente di lavoro e si sceglie un gruppo di protezione predefinito, è possibile scegliere di consentire il traffico all'interno di una delle seguenti opzioni:

- **Selezionato solo VNET**: L'origine del traffico in entrata è l'intervallo di sottorete di VNET per il sistema Cloud Volumes ONTAP e l'intervallo di sottorete di VNET in cui si trova il connettore. Questa è l'opzione consigliata.
- **Tutti i VNets**: L'origine del traffico in entrata è l'intervallo IP 0.0.0.0/0.

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
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	Connettività con il connettore e 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

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
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

Quando si crea un ambiente di lavoro e si sceglie un gruppo di protezione predefinito, è possibile scegliere di consentire il traffico all'interno di una delle seguenti opzioni:

- **Selezionato solo VNET**: L'origine del traffico in entrata è l'intervallo di sottorete di VNET per il sistema Cloud Volumes ONTAP e l'intervallo di sottorete di VNET in cui si trova il connettore. Questa è l'opzione consigliata.
- **Tutti i VNets**: L'origine del traffico in entrata è l'intervallo IP 0.0.0.0/0.

> 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	Connettività con il connettore e accesso HTTPS alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
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)

Servizio	Porta	Protocollo	Origine	Destinazione	Scopo
AutoSupport	HTTPS	443	LIF di gestione dei nodi	support.netapp.com	AutoSupport (HTTPS è l'impostazione predefinita)
	HTTP	80	LIF di gestione dei nodi	support.netapp.com	AutoSupport (solo se il protocollo di trasporto viene modificato da HTTPS a HTTP)
	TCP	3128	LIF di gestione dei nodi	Connettore	Invio di messaggi AutoSupport tramite un server proxy sul connettore, se non è disponibile una connessione Internet in uscita
Backup della configurazione	HTTP	80	LIF di gestione dei nodi	Http://<connector-IP-address>/occm/offboxconfig	Inviare i backup della configurazione al connettore. "Informazioni sui file di backup della configurazione".
DHCP	68	UDP	LIF di gestione dei nodi	DHCP	Client DHCP per la prima installazione
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

Requisiti per il connettore

Se non hai ancora creato un connettore, dovresti rivedere anche i requisiti di rete per il connettore.

- "Visualizzare i requisiti di rete per il connettore"
- "Regole del gruppo di sicurezza in Azure"

Impostare Cloud Volumes ONTAP in modo che utilizzi 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. Tuttavia, è possibile utilizzare la propria chiave di crittografia seguendo la procedura riportata in questa pagina.

Panoramica sulla crittografia dei dati

I dati Cloud Volumes ONTAP vengono crittografati automaticamente in Azure utilizzando "Azure Storage Service Encryption". 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, attenersi alla seguente procedura:

1. Da Azure, creare un vault delle chiavi e quindi generare una chiave in quel vault
2. Da BlueXP, utilizzare l'API per creare un ambiente di lavoro Cloud Volumes ONTAP che utilizza la chiave

Rotazione delle chiavi

Se si crea una nuova versione della chiave, Cloud Volumes ONTAP utilizza automaticamente la versione più recente.

Modalità di crittografia dei dati

BlueXP 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 i nuovi dischi dati utilizzano lo stesso set di crittografia del disco. Le versioni più basse utilizzeranno la chiave gestita da Microsoft, invece della chiave gestita dal cliente.

Dopo aver creato un ambiente di lavoro Cloud Volumes ONTAP configurato per l'utilizzo di una chiave gestita dal cliente, i dati Cloud Volumes ONTAP vengono crittografati come segue.

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

Configurazione di Cloud Volumes ONTAP	Dischi di sistema utilizzati per la crittografia delle chiavi	Dischi dati utilizzati per la crittografia delle chiavi
Singola zona di disponibilità di Azure ha con BLOB di pagina	• Avvio • Core • NVRAM	Nessuno
Singola zona di disponibilità di Azure ha con dischi gestiti condivisi	• Avvio • Core • NVRAM	• Radice • Dati
Ha di Azure diverse zone di disponibilità con dischi gestiti condivisi	• Avvio • Core • NVRAM	• Radice • Dati

Tutti gli account di storage Azure per Cloud Volumes ONTAP vengono crittografati utilizzando una chiave gestita dal cliente. Se si desidera crittografare gli account di storage durante la creazione, è necessario creare e fornire l'ID della risorsa nella richiesta di creazione CVO. Questo vale per tutti i tipi di implementazioni. Se non viene fornito, gli account di storage verranno comunque crittografati, ma BlueXP creerà prima gli account di storage con crittografia a chiave gestita da Microsoft e quindi aggiornerà gli account di storage per utilizzare la chiave gestita dal cliente.

Creare un'identità gestita assegnata dall'utente

È possibile creare una risorsa denominata identità gestita assegnata dall'utente. In questo modo è possibile crittografare gli account storage quando si crea un ambiente di lavoro Cloud Volumes ONTAP. Si consiglia di creare questa risorsa prima di creare un vault delle chiavi e di generare una chiave.

La risorsa ha il seguente ID: `userassignedidentity`.

Fasi

1. In Azure, accedere a servizi Azure e selezionare **identità gestite**.
2. Fare clic su **Create** (Crea).
3. Fornire i seguenti dettagli:
   - **Subscription**: Scegli un abbonamento. Si consiglia di scegliere lo stesso abbonamento di Connector.
   - **Gruppo di risorse**: Utilizzare un gruppo di risorse esistente o crearne uno nuovo.
   - **Regione**: Se si desidera, selezionare la stessa regione del connettore.
   - **Nome**: Immettere un nome per la risorsa.
4. Facoltativamente, aggiungere tag.
5. Fare clic su **Create** (Crea).

Creare un vault delle chiavi e generare una chiave

Il vault delle chiavi deve risiedere nella stessa sottoscrizione Azure e nella stessa regione in cui si intende creare il sistema Cloud Volumes ONTAP.

Se creazione di un'identità gestita assegnata dall'utente, durante la creazione del vault delle chiavi, è necessario creare anche una policy di accesso per il vault delle chiavi.

Fasi

1. "Creare un vault delle chiavi nell'abbonamento Azure".

   Tenere presente i seguenti requisiti per il vault delle chiavi:

   - Il vault delle chiavi deve risiedere nella stessa regione del sistema Cloud Volumes ONTAP.
   - Devono essere attivate le seguenti opzioni:
     - **Soft-delete** (questa opzione è attivata per impostazione predefinita, ma deve *non* essere disattivata)
     - **Protezione da spurgo**
     - **Azure Disk Encryption per la crittografia dei volumi** (per sistemi a nodo singolo o coppie ha in più zone)
   - Se è stata creata un'identità gestita assegnata dall'utente, deve essere attivata la seguente opzione:
     - **Policy di accesso al vault**
2. Se è stata selezionata la policy di accesso al vault, fare clic su Create (Crea) per creare una policy di accesso per il vault delle chiavi. In caso contrario, passare alla fase 3.
   a. Selezionare le seguenti autorizzazioni:
      - ottieni
      - elenco
      - decrittare
      - crittografare
      - tasto di savvolgimento
      - tasto di avvolgimento
      - verificare
      - segnale
   b. Selezionare l'identità gestita (risorsa) assegnata dall'utente come principale.
   c. Esaminare e creare la policy di accesso.
3. "Generare una chiave nell'archivio chiavi".

   Tenere presente i seguenti requisiti per la chiave:

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

Creare un ambiente di lavoro che utilizzi la chiave di crittografia

Dopo aver creato l'archivio delle chiavi e aver generato una chiave di crittografia, è possibile creare un nuovo sistema Cloud Volumes ONTAP configurato per l'utilizzo della chiave. Questi passaggi sono supportati dall'API BlueXP.

Autorizzazioni richieste

Se si desidera utilizzare una chiave gestita dal cliente con un sistema Cloud Volumes ONTAP a nodo singolo,

assicurarsi che BlueXP Connector 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"
```

"Visualizzare l'elenco più recente delle autorizzazioni"

Fasi

1. Ottenere l'elenco dei vault chiave nell'abbonamento Azure utilizzando la seguente chiamata API BlueXP.

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

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

   Prendere nota del **nome** e del **resourceGroup**. Sarà necessario specificare questi valori nel passaggio successivo.

   "Scopri di più su questa chiamata API".

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

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

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

   Prendere nota del **nome chiave**. Nel passaggio successivo, specificare tale valore (insieme al nome del vault).

   "Scopri di più su questa chiamata API".

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

   a. Per una coppia ha:

      `POST /azure/ha/working-environments`

      Il corpo della richiesta deve includere i seguenti campi:

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

> Includere il `"userAssignedIdentity": " userAssignedIdentityId"` se questa risorsa è stata creata per essere utilizzata per la crittografia dell'account di storage.

"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"
}
```

> Includere il `"userAssignedIdentity": " userAssignedIdentityId"` se questa risorsa è stata creata per essere utilizzata per la crittografia dell'account di storage.

"Scopri di più su questa chiamata API".

Risultato

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

Impostare la licenza per Cloud Volumes ONTAP in Azure

Dopo aver deciso quale opzione di licenza utilizzare con Cloud Volumes ONTAP, è necessario eseguire alcuni passaggi prima di poter scegliere l'opzione di licenza quando si crea un nuovo ambiente di lavoro.

Freemium

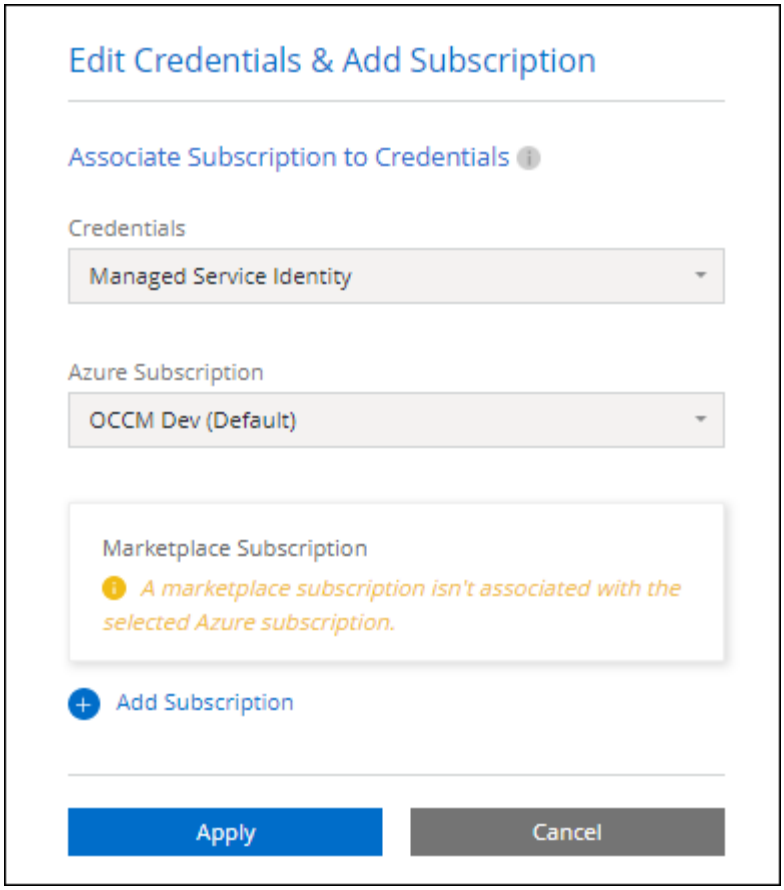
Scegli l'offerta Freemium per utilizzare Cloud Volumes ONTAP gratuitamente con un massimo di 500 GB di capacità fornita. "Scopri di più sull'offerta Freemium".

Fasi

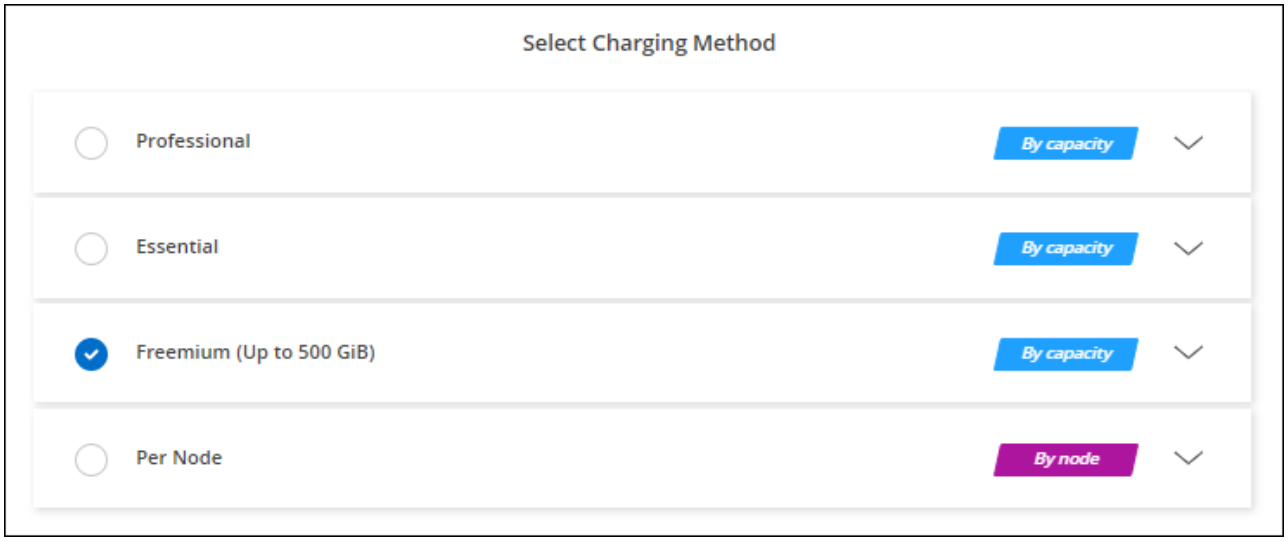
1. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. Nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire la procedura in BlueXP.

   a. Nella pagina **Dettagli e credenziali**, fare clic su **Modifica credenziali > Aggiungi abbonamento**, quindi seguire le istruzioni per iscriversi all'offerta pay-as-you-go in Azure Marketplace.

   L'abbonamento al marketplace non ti addebiterà alcun costo a meno che non superi i 500 GiB di capacità fornita, dopodiché il sistema viene automaticamente convertito in "Pacchetto Essentials".



a. Una volta visualizzato BlueXP, selezionare **Freemium** quando si accede alla pagina dei metodi di ricarica.



"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 un *pacchetto*: Il pacchetto Essentials o il pacchetto Professional.

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

- Una licenza (BYOL) acquistata da NetApp
- Un abbonamento oraria a pagamento (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 implementare i sistemi Cloud Volumes ONTAP in qualsiasi cloud provider.

Fasi

1. "Contattare il reparto vendite NetApp per ottenere una licenza"
2. "Aggiungi il tuo account NetApp Support Site a BlueXP"

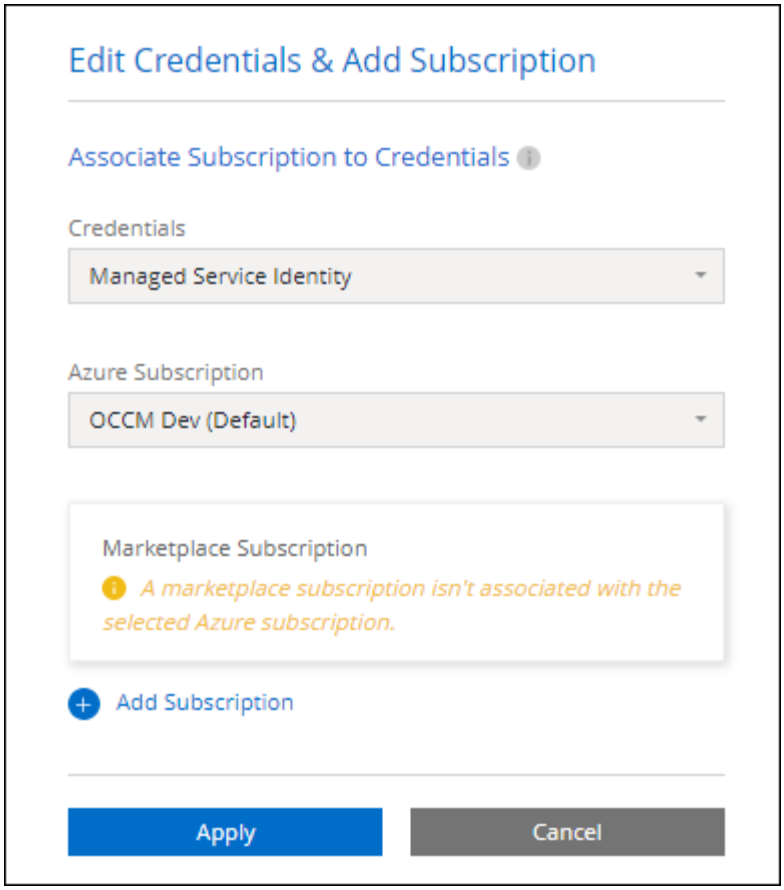
   BlueXP interroga automaticamente il servizio di licensing di NetApp per ottenere dettagli sulle licenze associate al tuo account NetApp Support Site. In assenza di errori, BlueXP aggiunge automaticamente le licenze al portafoglio digitale.

   La licenza deve essere disponibile sul portafoglio digitale BlueXP prima di poter essere utilizzata con Cloud Volumes ONTAP. Se necessario, è possibile "Aggiungere manualmente la licenza al portafoglio digitale BlueXP".

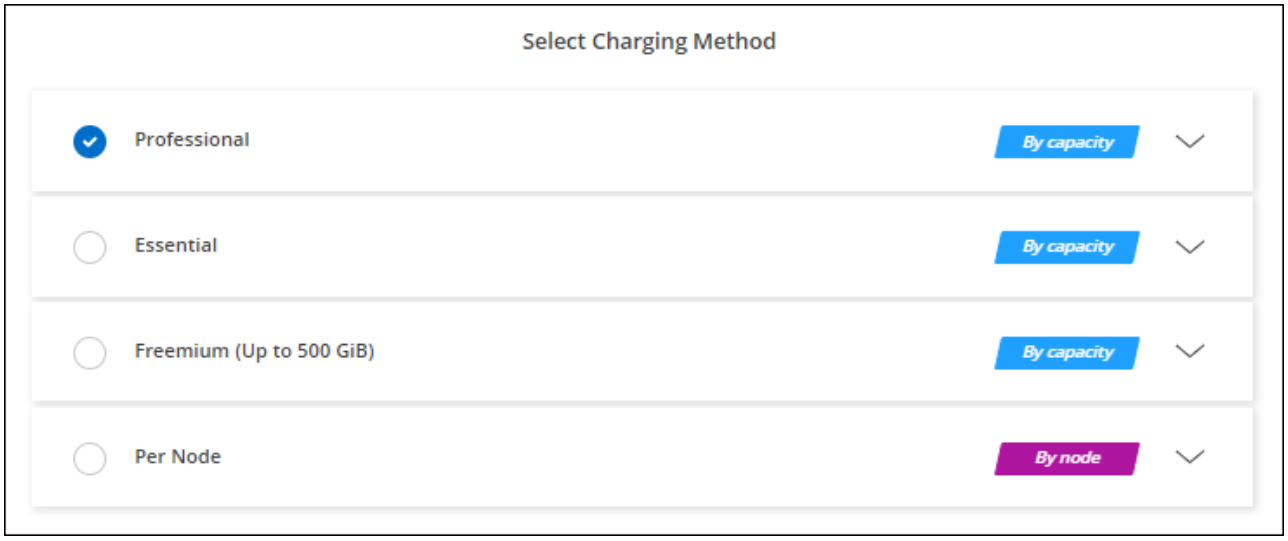
3. Nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire la procedura in BlueXP.

   a. Nella pagina **Dettagli e credenziali**, fare clic su **Modifica credenziali > Aggiungi abbonamento**, quindi seguire le istruzioni per iscriversi all'offerta pay-as-you-go in Azure Marketplace.

      La licenza acquistata da NetApp viene sempre addebitata per prima, ma verrà addebitato sulla tariffa oraria sul mercato se si supera la capacità concessa in licenza o se scade il termine della licenza.



a. Una volta visualizzato BlueXP, selezionare un pacchetto basato sulla capacità quando si accede alla pagina dei metodi di ricarica.



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

Abbonamento PAYGO

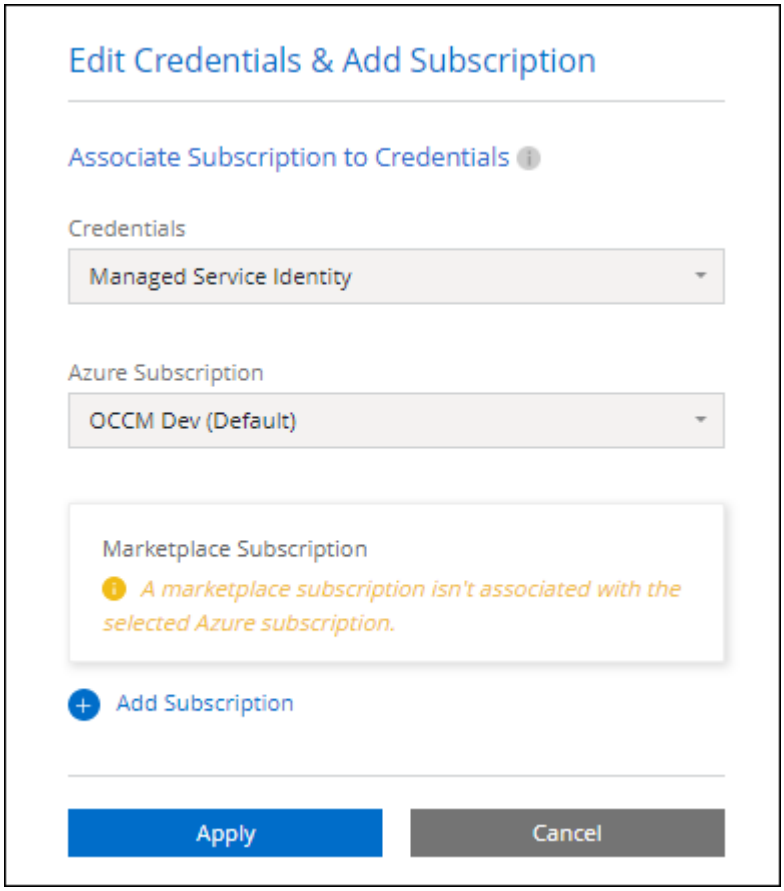
Paga ogni ora sottoscrivendo l'offerta sul mercato del tuo cloud provider.

Quando si crea un ambiente di lavoro Cloud Volumes ONTAP, BlueXP richiede di sottoscrivere il contratto disponibile in Azure Marketplace. Tale abbonamento viene quindi associato all'ambiente di lavoro per la

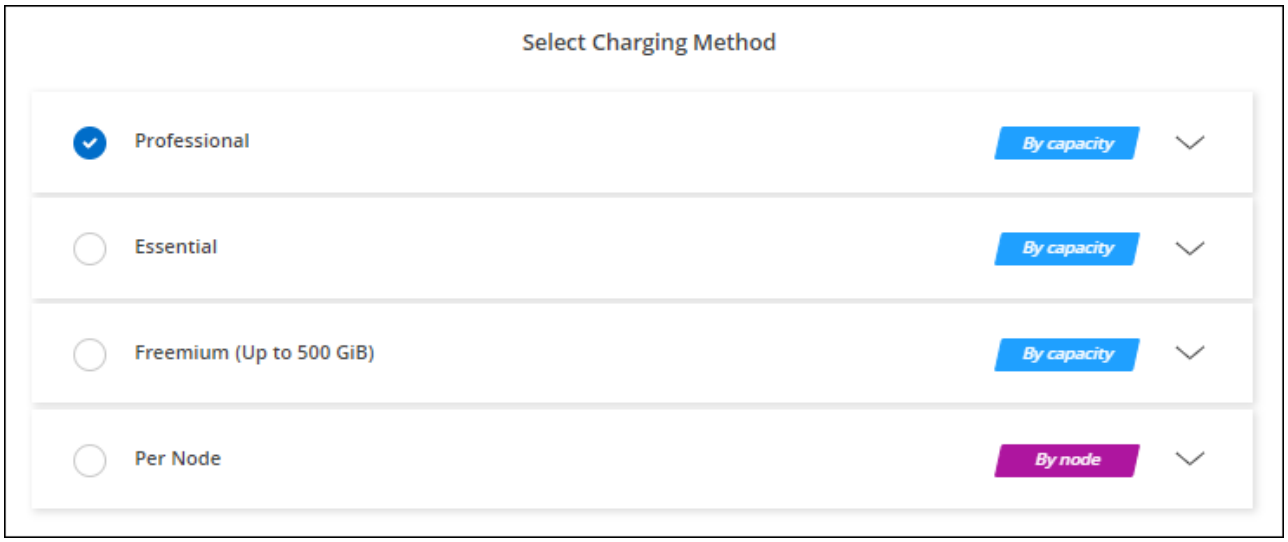
ricarica. È possibile utilizzare lo stesso abbonamento per altri ambienti di lavoro.

Fasi

1. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. Nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire la procedura in BlueXP.
   a. Nella pagina **Dettagli e credenziali**, fare clic su **Modifica credenziali > Aggiungi abbonamento**, quindi seguire le istruzioni per iscriversi all'offerta pay-as-you-go in Azure Marketplace.



   b. Una volta visualizzato BlueXP, selezionare un pacchetto basato sulla capacità quando si accede alla pagina dei metodi di ricarica.



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

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

Contratto annuale

Paga Cloud Volumes ONTAP ogni anno acquistando un contratto annuale.

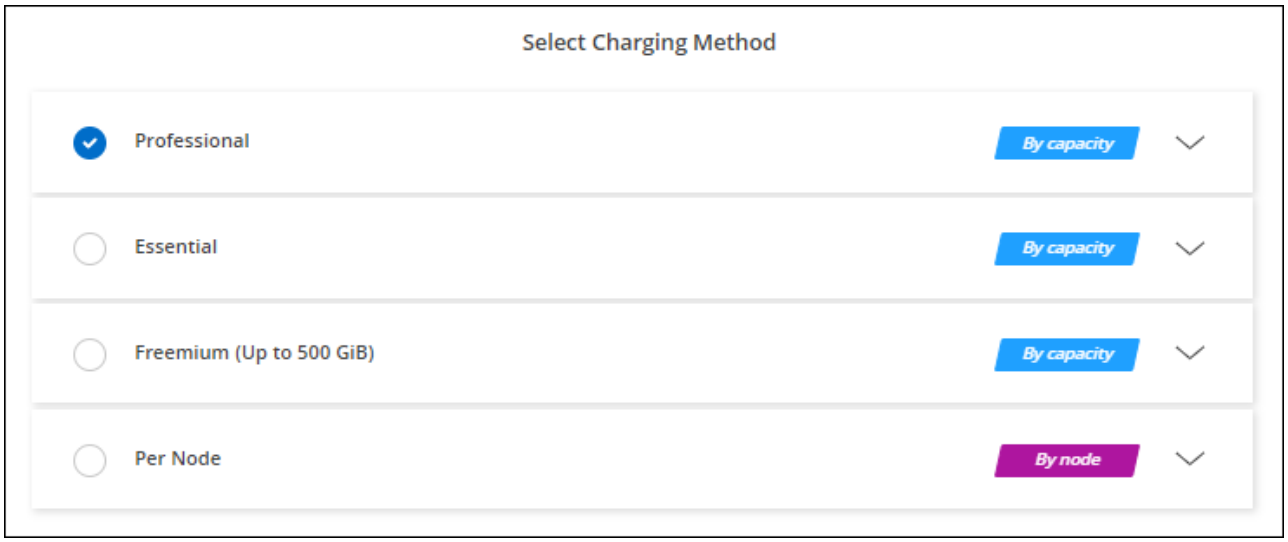
Fasi

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

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

   Dopo che NetApp condivide l'offerta privata con te, puoi selezionare il piano annuale quando ti iscrivi da Azure Marketplace durante la creazione dell'ambiente di lavoro.

2. Nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire la procedura in BlueXP.
   a. Nella pagina **Dettagli e credenziali**, fare clic su **Modifica credenziali > Aggiungi abbonamento > continua**.
   b. Nel portale Azure, seleziona il piano annuale condiviso con il tuo account Azure, quindi fai clic su **Iscriviti**.
   c. Una volta visualizzato BlueXP, selezionare un pacchetto basato sulla capacità quando si accede alla pagina dei metodi di ricarica.



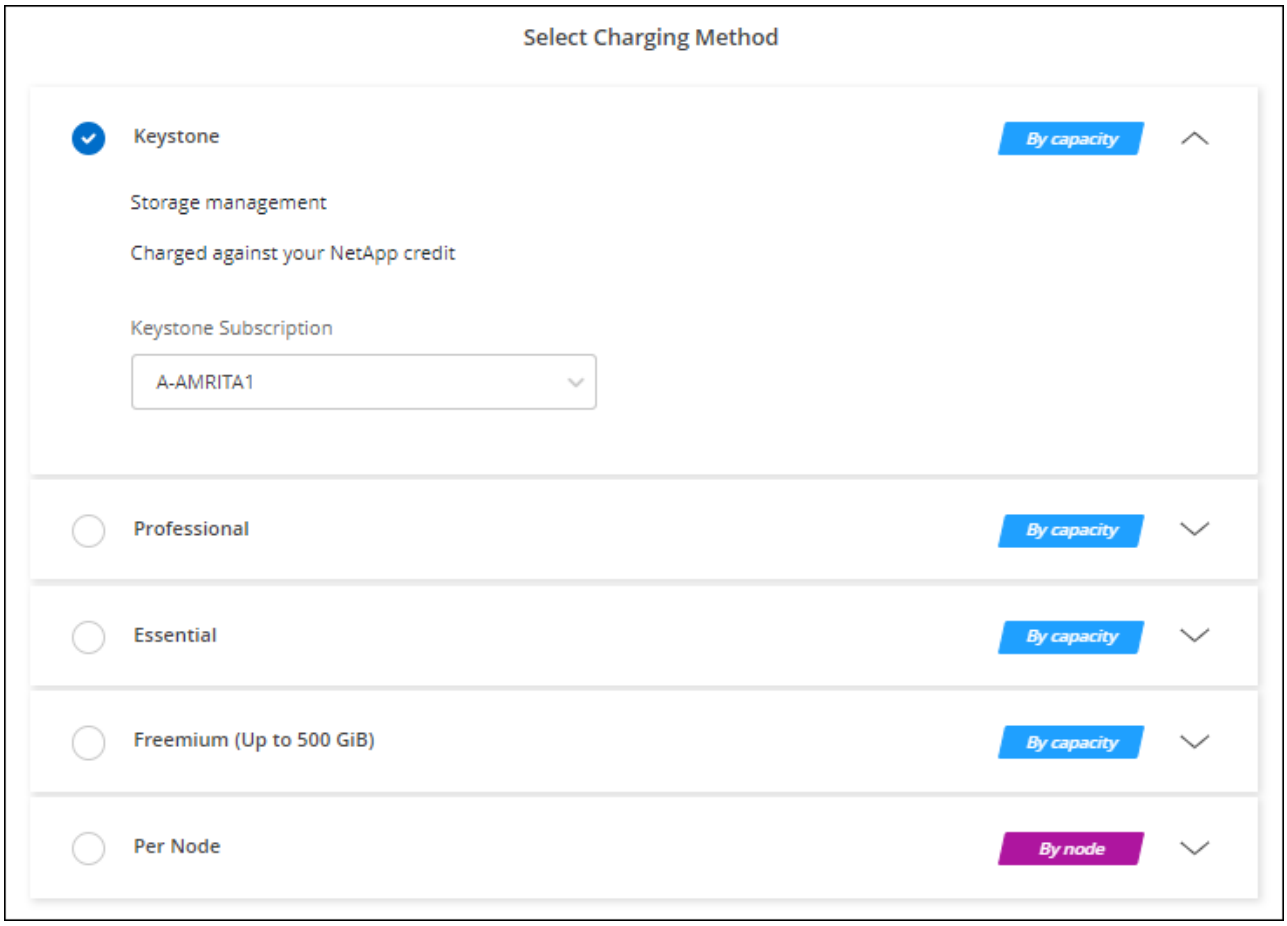
"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in Azure".

Iscrizione Keystone

Un abbonamento Keystone è un servizio basato su abbonamento pay-as-you-grow. "Scopri di più sugli abbonamenti NetApp Keystone".

Fasi

1. Se non disponi ancora di un abbonamento, "Contatta NetApp"
2. Mailto:ng-keystone-success@netapp.com[Contatta NetApp] per autorizzare il tuo account utente BlueXP con uno o più abbonamenti Keystone.
3. Dopo che NetApp ha autorizzato il tuo account, "Collega i tuoi abbonamenti per l'utilizzo con Cloud Volumes ONTAP".
4. Nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire la procedura in BlueXP.
    a. Quando richiesto, selezionare il metodo di ricarica per l'abbonamento Keystone.



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

Abilitare la modalità ad alta disponibilità in Azure

La modalità ad alta disponibilità di Microsoft Azure deve essere abilitata per ridurre i tempi di failover non pianificati e abilitare il supporto NFSv4 per Cloud Volumes ONTAP.

A partire dalla release 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, devi attivare la funzione di disponibilità elevata sul tuo abbonamento Azure.

BlueXP ti chiederà di inserire questi dettagli in un messaggio Action Required (azione richiesta) quando la funzione deve essere attivata con un abbonamento Azure.

Tenere presente quanto segue:

- Non ci sono problemi con l'alta disponibilità della tua coppia Cloud Volumes ONTAP ha. Questa funzionalità di Azure funziona in collaborazione con ONTAP per ridurre il tempo di interruzione dell'applicazione osservato dal client per i protocolli NFS che derivano da eventi di failover non pianificati.
- L'attivazione di questa funzione non comporta interruzioni per le coppie Cloud Volumes ONTAP ha.
- L'attivazione di questa funzione sul tuo abbonamento Azure non causerà problemi ad altre macchine virtuali.

Un utente di Azure che dispone dei privilegi di "Owner" può attivare la funzionalità dalla CLI di Azure.

Fasi

1. "Accedi a Azure Cloud Shell dal portale Azure"
2. Registrare la funzione 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. Se si desidera, verificare che la funzione sia ora registrata:

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

Azure CLI dovrebbe restituire un risultato simile a quanto segue:

```
{
  "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"
}
```

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 BlueXP.

Di cosa hai bisogno

Per creare un ambiente di lavoro, è necessario quanto segue.

- Un connettore funzionante.
  - Si dovrebbe avere un "Connettore associato all'area di lavoro".
  - "Si dovrebbe essere pronti a lasciare il connettore sempre in funzione".
- Comprensione della configurazione che si desidera utilizzare.

  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".

- Comprensione di ciò che è necessario per impostare le licenze per Cloud Volumes ONTAP.

  "Scopri come impostare le licenze".

A proposito di questa attività

Quando BlueXP crea un sistema Cloud Volumes ONTAP in Azure, crea diversi oggetti Azure, ad esempio 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**
>
> La Best practice consiste nell'utilizzare un nuovo gruppo di risorse dedicato per ciascun sistema Cloud Volumes ONTAP.
>
> L'implementazione di Cloud Volumes ONTAP in un gruppo di risorse condiviso esistente non è consigliata a causa del rischio di perdita di dati. Mentre BlueXP può rimuovere le risorse Cloud Volumes ONTAP da un gruppo di risorse condiviso in caso di errore di implementazione o di eliminazione, un utente Azure potrebbe accidentalmente eliminare le risorse Cloud Volumes ONTAP da un gruppo di risorse condiviso.

Avvio di 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 ambiente di lavoro a nodo singolo in BlueXP.

Fasi

1. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire le istruzioni.
3. **Scegli una posizione**: Seleziona **Microsoft Azure** e **nodo singolo Cloud Volumes ONTAP**.
4. Se richiesto, "Creare un connettore".
5. **Dettagli e credenziali**: Se necessario, modificare le credenziali e la sottoscrizione di Azure, specificare un nome del cluster, aggiungere tag, quindi specificare le credenziali.

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

Campo	Descrizione
Nome ambiente di lavoro	BlueXP 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.
Tag del gruppo di risorse	I tag sono metadati per le risorse Azure. Quando si inseriscono i tag in questo campo, BlueXP 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".

Campo	Descrizione
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 o la relativa CLI. Mantenere il nome utente predefinito *admin* o modificarlo in 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 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:

Iscriviti a BlueXP da Azure Marketplace

6. **Servizi**: Mantieni abilitati i servizi o disabilita i singoli servizi che non vuoi utilizzare con Cloud Volumes ONTAP.
   - "Scopri di più sulla classificazione BlueXP"
   - "Scopri di più sul backup e ripristino BlueXP"

   Se si desidera utilizzare WORM e il tiering dei dati, è necessario disattivare il backup e il ripristino BlueXP e implementare un ambiente di lavoro Cloud Volumes ONTAP con versione 9.8 o superiore.

7. **Location** (posizione): Selezionare una regione, una zona di disponibilità, VNET e una subnet, quindi selezionare la casella di controllo per confermare la connettività di rete tra il connettore e la posizione di destinazione.

   Per i sistemi a nodo singolo, è possibile scegliere l'area di disponibilità in cui si desidera implementare Cloud Volumes ONTAP. Se non si seleziona un AZ, BlueXP ne selezionerà uno.

8. **Connettività**: Scegliere un gruppo di risorse nuovo o esistente, quindi scegliere se utilizzare il gruppo di protezione predefinito o il proprio.

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

Campo	Descrizione
Gruppo di risorse	Creare un nuovo gruppo di risorse per Cloud Volumes ONTAP o utilizzare un gruppo di risorse esistente. 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, non è consigliabile a causa del rischio di perdita dei dati. Per ulteriori informazioni, vedere l'avviso riportato sopra. Se l'account Azure in uso dispone di "autorizzazioni richieste", BlueXP rimuove le risorse Cloud Volumes ONTAP da un gruppo di risorse, in caso di errore di implementazione o di eliminazione.

Campo	Descrizione
Gruppo di sicurezza generato	Se si lascia che BlueXP generi il gruppo di protezione, è necessario scegliere come consentire il traffico: • Se si sceglie **Selected VNET Only** (solo VNET selezionato), l'origine del traffico in entrata è l'intervallo di sottorete del VNET selezionato e l'intervallo di sottorete del VNET in cui si trova il connettore. Questa è l'opzione consigliata. • Se si sceglie **All VNets**, l'origine del traffico in entrata è l'intervallo IP 0.0.0.0/0.
USA esistente	Se si sceglie un gruppo di protezione esistente, questo deve soddisfare i requisiti Cloud Volumes ONTAP. "Visualizzare il gruppo di protezione predefinito".

9. **Charging Methods and NSS account** (metodi di addebito e account NSS): Specificare l'opzione di addebito che si desidera utilizzare con questo sistema, quindi specificare un account NetApp Support Site.
   - "Scopri le opzioni di licenza per Cloud Volumes ONTAP".
   - "Scopri come impostare le licenze".
10. **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.

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

    > Se è disponibile una release Release Candidate, General Availability o patch più recente per la versione selezionata, BlueXP 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 9.10.1 e 9.10.1 P4 è disponibile. L'aggiornamento non si verifica da una release all'altra, ad esempio da 9.6 a 9.7.

12. **Iscriviti al marketplace Azure**: Segui la procedura se BlueXP non è riuscito ad abilitare le implementazioni programmatiche di Cloud Volumes ONTAP.
13. **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 qualsiasi aggregato aggiuntivo creato da BlueXP 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".

14. **Velocità di scrittura e WORM**:

    a. Scegliere **normale** o **alta** velocità di scrittura, se lo si desidera.

    "Scopri di più sulla velocità di scrittura".

    b. Attivare lo storage WORM (Write Once, Read Many), se lo si desidera.

    Questa opzione è disponibile solo per alcuni tipi di macchine virtuali. Per scoprire quali tipi di macchine virtuali sono supportati, vedere "Configurazioni supportate dalla licenza per coppie ha".

    NON è possibile attivare WORM 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 viene bloccato dopo l'abilitazione DI WORM e tiering.

    "Scopri di più sullo storage WORM".

    a. Se si attiva lo storage WORM, selezionare il periodo di conservazione.

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

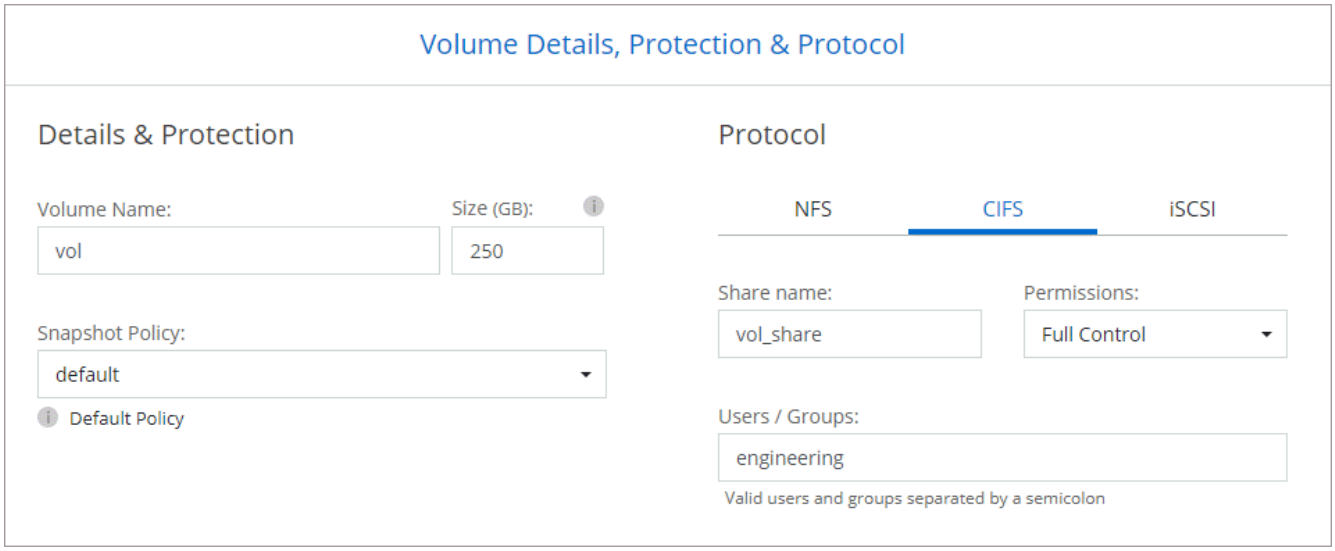
    "Scopri le versioni e i protocolli client supportati".

    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, BlueXP inserisce un valore che fornisce l'accesso a tutte le istanze della 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.
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.

Campo	Descrizione
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, BlueXP 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:



16. **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.
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.

Campo	Descrizione
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 "Documenti sull'automazione BlueXP" per ulteriori informazioni. Nota: 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 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".

18. **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 visualizzare i dettagli relativi al supporto e alle risorse Azure che BlueXP acquisterà.
    c. Selezionare le caselle di controllo **ho capito…**.
    d. Fare clic su **Go**.

Risultato

BlueXP 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.

Lancio di una coppia Cloud Volumes ONTAP ha in Azure

Se si desidera lanciare una coppia Cloud Volumes ONTAP ha in Azure, è necessario creare un ambiente di lavoro ha in BlueXP.

Fasi

1. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire le istruzioni.
3. Se richiesto, "Creare un connettore".
4. **Dettagli e credenziali**: Se necessario, modificare le credenziali e la sottoscrizione di Azure, specificare un nome del cluster, aggiungere tag, quindi specificare le credenziali.

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

Campo	Descrizione
Nome ambiente di lavoro	BlueXP 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.
Tag del gruppo di risorse	I tag sono metadati per le risorse Azure. Quando si inseriscono i tag in questo campo, BlueXP 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 o la relativa CLI. Mantenere il nome utente predefinito *admin* o modificarlo in 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 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:

   Iscriviti a BlueXP da Azure Marketplace

5. **Servizi**: Mantieni abilitati i servizi o disabilita i singoli servizi che non vuoi utilizzare con Cloud Volumes ONTAP.
   - "Scopri di più sulla classificazione BlueXP"
   - "Scopri di più sul backup e ripristino BlueXP"

> Se si desidera utilizzare WORM e il tiering dei dati, è necessario disattivare il backup e il ripristino BlueXP e implementare un ambiente di lavoro Cloud Volumes ONTAP con versione 9.8 o superiore.

6. **Modelli di implementazione ha**:
   a. Selezionare **Single Availability zone** o **Multiple Availability zone**.
   b. **Posizione e connettività** (AZ singolo) e **Regione e connettività** (AZS multiplo)
      - Per AZ singolo, selezionare una regione, VNET e subnet.
      - Per AZS multipli, selezionare una regione, VNET, subnet, zona per il nodo 1 e zona per il nodo 2.
   c. Selezionare la casella di controllo **ho verificato la connettività di rete…**.
7. **Connettività**: Scegliere un gruppo di risorse nuovo o esistente, quindi scegliere se utilizzare il gruppo di protezione predefinito o il proprio.

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

Campo	Descrizione
Gruppo di risorse	Creare un nuovo gruppo di risorse per Cloud Volumes ONTAP o utilizzare un gruppo di risorse esistente. 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, non è consigliabile a causa del rischio di perdita dei dati. Per ulteriori informazioni, vedere l'avviso riportato sopra. È necessario utilizzare un gruppo di risorse dedicato per ogni coppia di Cloud Volumes ONTAP ha implementata in Azure. In un gruppo di risorse è supportata una sola coppia ha. BlueXP presenta problemi di connessione se si tenta di implementare una seconda coppia Cloud Volumes ONTAP ha in un gruppo di risorse Azure. Se l'account Azure in uso dispone di "autorizzazioni richieste", BlueXP rimuove le risorse Cloud Volumes ONTAP da un gruppo di risorse, in caso di errore di implementazione o di eliminazione.
Gruppo di sicurezza generato	Se si lascia che BlueXP generi il gruppo di protezione, è necessario scegliere come consentire il traffico: • Se si sceglie **Selected VNET Only** (solo VNET selezionato), l'origine del traffico in entrata è l'intervallo di sottorete del VNET selezionato e l'intervallo di sottorete del VNET in cui si trova il connettore. Questa è l'opzione consigliata. • Se si sceglie **All VNets**, l'origine del traffico in entrata è l'intervallo IP 0.0.0.0/0.
USA esistente	Se si sceglie un gruppo di protezione esistente, questo deve soddisfare i requisiti Cloud Volumes ONTAP. "Visualizzare il gruppo di protezione predefinito".

8. **Charging Methods and NSS account** (metodi di addebito e account NSS): Specificare l'opzione di addebito che si desidera utilizzare con questo sistema, quindi specificare un account NetApp Support Site.
   - "Scopri le opzioni di licenza per Cloud Volumes ONTAP".
   - "Scopri come impostare le licenze".
9. **Pacchetti preconfigurati**: Selezionare uno dei pacchetti per implementare rapidamente un sistema Cloud Volumes ONTAP oppure fare clic su **Cambia configurazione**.

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

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

    > Se è disponibile una release Release Candidate, General Availability o patch più recente per la versione selezionata, BlueXP 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 9.10.1 e 9.10.1 P4 è disponibile. L'aggiornamento non si verifica da una release all'altra, ad esempio da 9.6 a 9.7.

11. **Iscriviti al marketplace Azure**: Segui la procedura se BlueXP non è riuscito ad abilitare le implementazioni programmatiche di Cloud Volumes ONTAP.
12. **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:

    - Le dimensioni del disco sono per tutti i dischi nell'aggregato iniziale e per qualsiasi aggregato aggiuntivo creato da BlueXP 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 delle dimensioni del disco, vedere "Dimensionare il 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".

13. **Velocità di scrittura e WORM**:

    a. Scegliere **normale** o **alta** velocità di scrittura, se lo si desidera.

       "Scopri di più sulla velocità di scrittura".

    b. Attivare lo storage WORM (Write Once, Read Many), se lo si desidera.

       Questa opzione è disponibile solo per alcuni tipi di macchine virtuali. Per scoprire quali tipi di macchine virtuali sono supportati, vedere "Configurazioni supportate dalla licenza per coppie ha".

       NON è possibile attivare WORM 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 viene bloccato dopo l'abilitazione DI WORM e tiering.

"Scopri di più sullo storage WORM".

a. Se si attiva lo storage WORM, selezionare il periodo di conservazione.

14. **Secure Communication to Storage & WORM**: 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 blob di pagina 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".

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

    "Scopri di più sullo storage WORM".

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

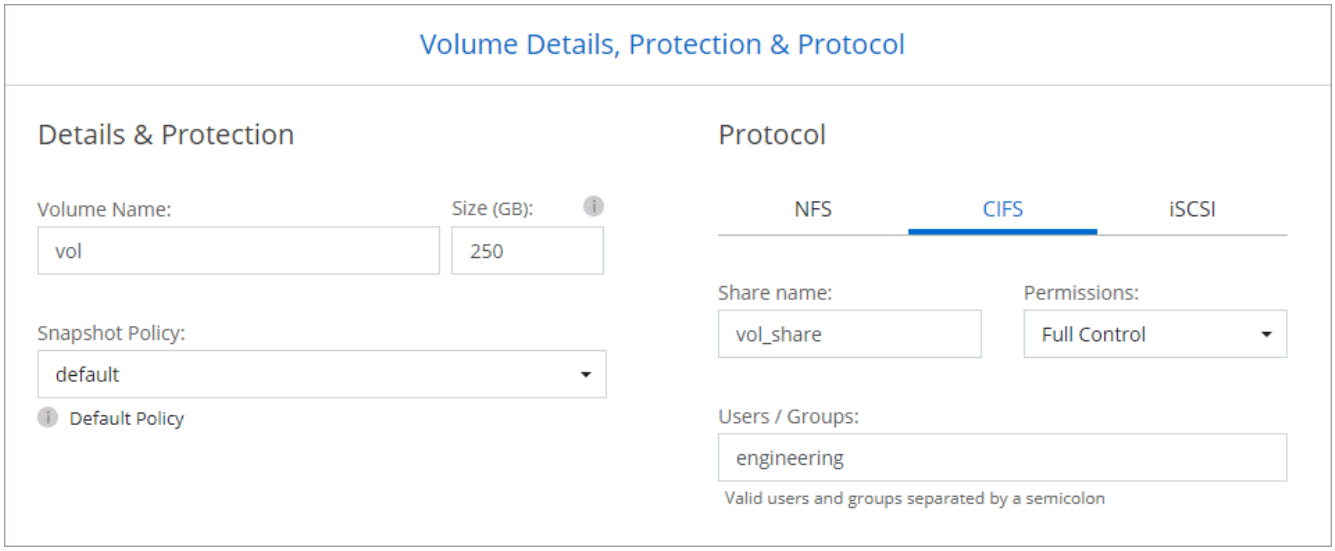
    "Scopri le versioni e i protocolli client supportati".

    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, BlueXP inserisce un valore che fornisce l'accesso a tutte le istanze della 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.
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.

Campo	Descrizione
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, BlueXP 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:



16. **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.
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.

Campo	Descrizione
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 "Documenti sull'automazione BlueXP" per ulteriori informazioni. Nota: 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 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 "Scegliere un profilo di utilizzo del volume" e. "Panoramica sul tiering dei dati".

18. **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 visualizzare i dettagli relativi al supporto e alle risorse Azure che BlueXP acquisterà.
    c. Selezionare le caselle di controllo **ho capito…**.
    d. Fare clic su **Go**.

Risultato

BlueXP 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.