



Inizia a utilizzare Google Cloud Cloud Volumes ONTAP

NetApp
June 27, 2024

Sommario

- Inizia a utilizzare Google Cloud 1
 - Guida rapida per Cloud Volumes ONTAP in Google Cloud 1
 - Pianificare la configurazione di Cloud Volumes ONTAP in Google Cloud 2
 - Requisiti di rete per Cloud Volumes ONTAP in Google Cloud 6
 - Pianificazione dei controlli dei servizi VPC in GCP 16
 - Creare un account di servizio per il tiering e i backup dei dati 19
 - Utilizzo di chiavi di crittografia gestite dal cliente con Cloud Volumes ONTAP 22
 - Impostare la licenza per Cloud Volumes ONTAP in Google Cloud 23
 - Lancio di Cloud Volumes ONTAP in Google Cloud 28
 - Verifica dell'immagine della piattaforma Google Cloud 42

Inizia a utilizzare Google Cloud

Guida rapida per Cloud Volumes ONTAP in Google Cloud

Inizia a utilizzare Cloud Volumes ONTAP per Google Cloud 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 Google Cloud"](#)

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 sulla pianificazione della configurazione"](#).

3

Configurare la rete

1. Assicurarsi che il VPC e le subnet supportino la connettività tra il connettore e Cloud Volumes ONTAP.
2. Se si prevede di abilitare il tiering dei dati, ["Configurare la subnet Cloud Volumes ONTAP per l'accesso privato a Google"](#).
3. Se si sta implementando una coppia ha, assicurarsi di disporre di quattro VPC, ciascuno con la propria subnet.
4. Se si utilizza un VPC condiviso, fornire il ruolo *Compute Network User* all'account del servizio Connector.
5. 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

Impostare un account di servizio

Cloud Volumes ONTAP richiede un account di servizio cloud Google per due scopi. Il primo è quando si attiva ["tiering dei dati"](#) Per tierare i dati cold allo storage a oggetti a basso costo in Google Cloud. Il secondo si verifica quando si attiva ["Backup e ripristino BlueXP"](#) per eseguire il backup dei volumi in uno storage a oggetti a basso costo.

È possibile configurare un account di servizio e utilizzarlo per entrambi gli scopi. L'account di servizio deve

avere il ruolo **Storage Admin**.

["Leggi le istruzioni dettagliate"](#).

5

Abilitare le API di Google Cloud

["Abilita le seguenti API di Google Cloud nel tuo progetto"](#). Queste API sono necessarie per implementare il connettore e Cloud Volumes ONTAP.

- API di Cloud Deployment Manager V2
- API Cloud Logging
- API Cloud Resource Manager
- API di Compute Engine
- API IAM (Identity and Access Management)

6

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"](#)
- ["Installazione del software del connettore su un host Linux"](#)
- ["Cosa fa BlueXP con le autorizzazioni Google Cloud"](#)

Pianificare la configurazione di Cloud Volumes ONTAP in Google Cloud

Quando si implementa Cloud Volumes ONTAP in Google Cloud, 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 di Google Cloud. ["Visualizza l'elenco completo delle regioni supportate"](#).

Scegliere un tipo di computer supportato

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

["Configurazioni supportate per Cloud Volumes ONTAP in GCP"](#)

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 GCP"](#)

Dimensionare il sistema in GCP

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

Tipo di macchina

Esaminare i tipi di computer supportati in ["Note di rilascio di Cloud Volumes ONTAP"](#) Quindi, esamina i dettagli di Google relativi a ciascun tipo di computer supportato. Abbina i requisiti di carico di lavoro al numero di vCPU e di memoria per il tipo di computer. Si noti che ogni core della CPU aumenta le performance di rete.

Per ulteriori informazioni, fare riferimento a quanto segue:

- ["Documentazione di Google Cloud: Tipi di computer standard N1"](#)
- ["Documentazione Google Cloud: Performance"](#)

Tipo di disco GCP

Quando crei volumi per Cloud Volumes ONTAP, devi scegliere lo storage cloud sottostante utilizzato da Cloud Volumes ONTAP per un disco. Il tipo di disco può essere uno dei seguenti:

- *Dischi persistenti SSD Zonal*: I dischi persistenti SSD sono ideali per i carichi di lavoro che richiedono elevati tassi di IOPS casuali.
- *Dischi persistenti bilanciati zonali*: Questi SSD bilanciano le performance e i costi fornendo IOPS per GB inferiori.
- *Dischi persistenti standard zonali* : i dischi persistenti standard sono economici e possono gestire operazioni di lettura/scrittura sequenziali.

Per ulteriori informazioni, vedere ["Documentazione di Google Cloud: Dischi persistenti zonali \(Standard e SSD\)"](#).

Dimensioni del disco GCP

Quando si implementa un sistema Cloud Volumes ONTAP, è necessario scegliere una dimensione iniziale del disco. Dopodiché, puoi lasciare che BlueXP gestisca la capacità di un sistema per te, ma se vuoi creare aggregati, tieni presente quanto segue:

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

- Determinare lo spazio necessario, tenendo in considerazione le performance.
- Le performance dei dischi persistenti si ridimensionano automaticamente in base alle dimensioni del disco e al numero di vCPU disponibili per il sistema.

Per ulteriori informazioni, fare riferimento a quanto segue:

- ["Documentazione di Google Cloud: Dischi persistenti zonali \(Standard e SSD\)"](#)
- ["Documentazione di Google Cloud: Ottimizzazione delle performance di dischi persistenti e SSD locali"](#)

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 di Cloud Volumes ONTAP in Google Cloud"](#).
- ["Documenti di Google Cloud: Quote delle risorse"](#)

Il motore di calcolo per il cloud di Google applica quote sull'utilizzo delle risorse, in modo da garantire che non sia stato raggiunto il limite prima di implementare Cloud Volumes ONTAP.



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 GCP, è necessario specificare i dettagli della rete virtuale. È possibile utilizzare un foglio di lavoro per raccogliere le informazioni dall'amministratore.

Informazioni di rete per un sistema a nodo singolo

Informazioni GCP	Il tuo valore
Regione	
Zona	
Rete VPC	
Subnet	
Policy firewall (se si utilizza il proprio)	

Informazioni di rete per una coppia ha in più zone

Informazioni GCP	Il tuo valore
Regione	
Zona per nodo 1	
Zona per il nodo 2	

Informazioni GCP	Il tuo valore
Zona per il mediatore	
VPC-0 e subnet	
VPC-1 e subnet	
VPC-2 e subnet	
VPC-3 e subnet	
Policy firewall (se si utilizza il proprio)	

Informazioni di rete per una coppia ha in una singola zona

Informazioni GCP	Il tuo valore
Regione	
Zona	
VPC-0 e subnet	
VPC-1 e subnet	
VPC-2 e subnet	
VPC-3 e subnet	
Policy firewall (se si utilizza il proprio)	

Scegliere una velocità di scrittura

BlueXP consente di scegliere un'impostazione della velocità di scrittura per Cloud Volumes ONTAP, ad eccezione delle coppie ad alta disponibilità (ha) in Google Cloud. 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 Google Cloud

Configura il tuo network Google Cloud in modo che i sistemi Cloud Volumes ONTAP possano funzionare correttamente.

Se si desidera implementare una coppia ha, è necessario ["Scopri come funzionano le coppie ha in Google Cloud"](#).

Requisiti per Cloud Volumes ONTAP

I seguenti requisiti devono essere soddisfatti in Google Cloud.

Requisiti specifici per i sistemi a nodo singolo

Se si desidera implementare un sistema a nodo singolo, assicurarsi che la rete soddisfi i seguenti requisiti.

Un VPC

Un Virtual Private Cloud (VPC) è richiesto per un sistema a nodo singolo.

Indirizzi IP privati

BlueXP assegna 3 o 4 indirizzi IP privati a un sistema a nodo singolo in Google Cloud.

È possibile saltare la creazione della LIF di gestione delle VM di storage se si implementa Cloud Volumes ONTAP utilizzando l'API e si specifica il seguente flag:

```
skipSvmManagementLif: true
```



LIF è un indirizzo IP associato a una porta fisica. Per strumenti di gestione come SnapCenter è necessaria una LIF di gestione delle macchine virtuali dello storage (SVM).

Requisiti specifici delle coppie ha

Se si desidera implementare una coppia ha, assicurarsi che la rete soddisfi i seguenti requisiti.

Una o più zone

È possibile garantire l'elevata disponibilità dei dati implementando una configurazione ha in più zone o in una singola zona. BlueXP richiede di scegliere più zone o una singola zona quando si crea la coppia ha.

- Zone multiple (consigliato)

L'implementazione di una configurazione ha in tre zone garantisce la disponibilità continua dei dati in caso di guasto all'interno di una zona. Si noti che le prestazioni di scrittura sono leggermente inferiori rispetto all'utilizzo di una singola zona, ma sono minime.

- Zona singola

Quando viene implementato in una singola zona, una configurazione Cloud Volumes ONTAP ha utilizza una policy di posizionamento distribuita. Questa policy garantisce che una configurazione ha sia protetta da un singolo punto di guasto all'interno della zona, senza dover utilizzare zone separate per ottenere l'isolamento degli errori.

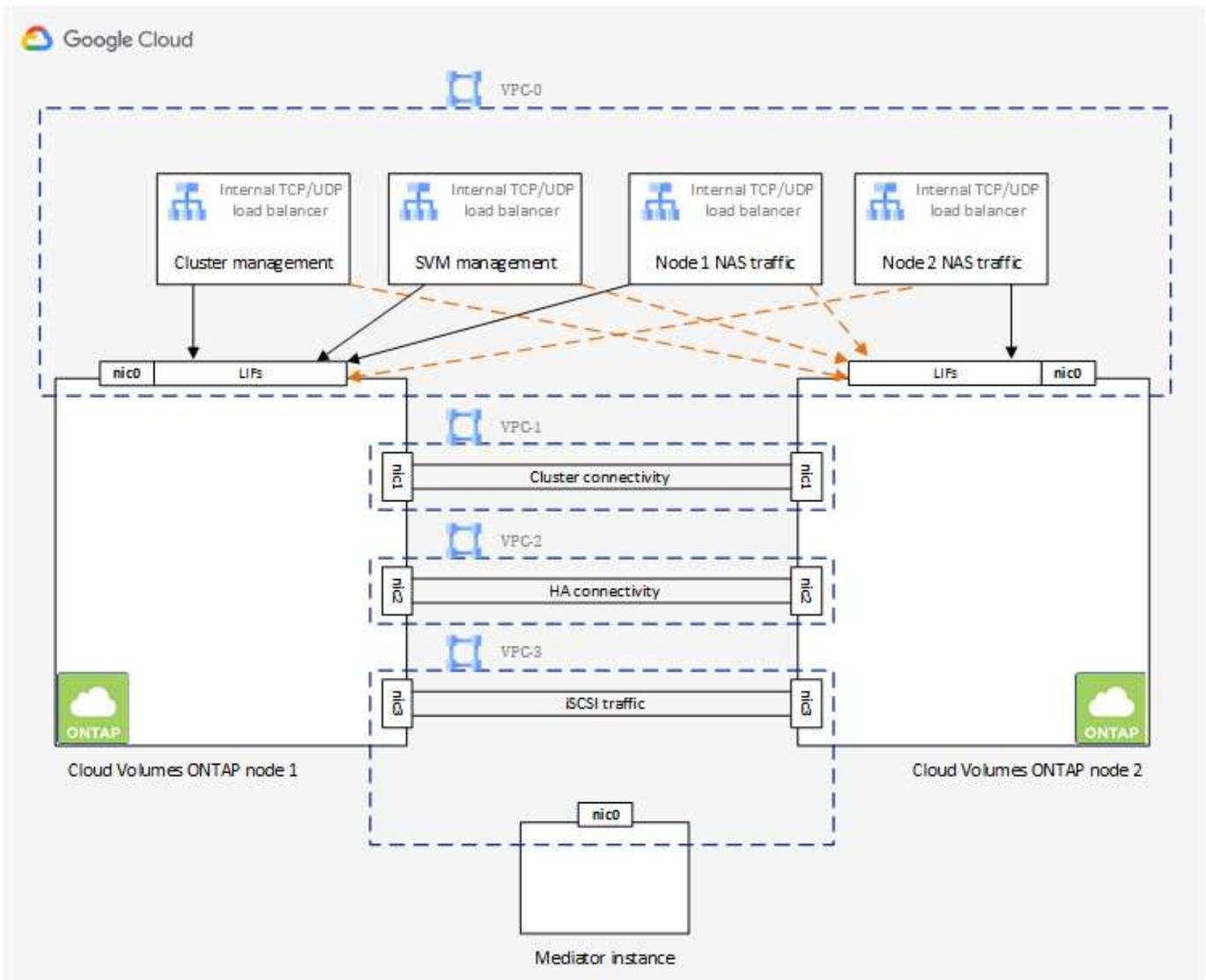
Questo modello di implementazione riduce i costi perché non sono previsti costi di uscita dei dati tra le zone.

Quattro cloud privati virtuali

Per una configurazione ha sono necessari quattro Virtual Private Clouds (VPC). Sono necessari quattro VPC perché Google Cloud richiede che ogni interfaccia di rete risieda in una rete VPC separata.

BlueXP richiede di scegliere quattro VPC quando si crea la coppia ha:

- VPC-0 per le connessioni in entrata ai dati e ai nodi
- VPC-1, VPC-2 e VPC-3 per la comunicazione interna tra i nodi e il mediatore ha



Subnet

Per ogni VPC è necessaria una subnet privata.

Se si posiziona il connettore in VPC-0, sarà necessario attivare Private Google Access sulla subnet per accedere alle API e abilitare il tiering dei dati.

Le subnet di questi VPC devono avere intervalli CIDR distinti. Non possono avere intervalli CIDR sovrapposti.

Indirizzi IP privati

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

• **Nodo singolo**

BlueXP alloca 4 indirizzi IP a un sistema con singolo nodo:

- LIF di gestione dei nodi
- LIF gestione cluster
- LIF dati iSCSI



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.

- LIF NAS

È possibile saltare la creazione della LIF di gestione delle VM di storage se si implementa Cloud Volumes ONTAP utilizzando l'API e si specifica il seguente flag:

```
skipSvmManagementLif: true
```

• **Coppia ha**

BlueXP alloca gli indirizzi IP 12-13 a una coppia ha:

- 2 LIF di gestione dei nodi (e0a)
- 1 LIF di gestione del cluster (e0a)
- 2 LIF iSCSI (e0a)



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.

- 1 o 2 LIF NAS (e0a)
- 2 LIF cluster (e0b)
- 2 indirizzi IP ha Interconnect (e0c)
- 2 indirizzi IP iSCSI RSM (e0d)

È possibile saltare la creazione della LIF di gestione delle VM di storage se si implementa Cloud Volumes ONTAP utilizzando l'API e si specifica il seguente flag:

```
skipSvmManagementLif: true
```

Bilanciatori di carico interni

BlueXP crea automaticamente quattro bilanciatori di carico interni di Google Cloud (TCP/UDP) che gestiscono il traffico in entrata verso la coppia ha di Cloud Volumes ONTAP. Non è richiesta alcuna configurazione. Questo requisito è stato elencato semplicemente per informarti del traffico di rete e per mitigare eventuali problemi di sicurezza.

Un bilanciamento del carico è per la gestione del cluster, uno per la gestione delle macchine virtuali di storage (SVM), uno per il traffico NAS al nodo 1 e l'altro per il traffico NAS al nodo 2.

La configurazione per ciascun bilanciamento del carico è la seguente:

- Un indirizzo IP privato condiviso
- Un controllo globale dello stato di salute

Per impostazione predefinita, le porte utilizzate dal controllo dello stato di salute sono 63001, 63002 e 63003.

- Un servizio backend TCP regionale
- Un servizio di backend UDP regionale
- Una regola di inoltro TCP
- Una regola di inoltro UDP
- L'accesso globale è disattivato

Anche se l'accesso globale è disattivato per impostazione predefinita, è supportata l'abilitazione dell'IT post-implementazione. L'abbiamo disattivata perché il traffico tra regioni avrà latenze significativamente più elevate. Volevamo assicurarci che non avessi avuto un'esperienza negativa a causa di montaggi incrociati accidentali. L'attivazione di questa opzione è specifica per le esigenze aziendali.

VPC condivisi

Cloud Volumes ONTAP e il connettore sono supportati in un VPC condiviso Google Cloud e anche in VPC standalone.

Per un sistema a nodo singolo, il VPC può essere un VPC condiviso o un VPC standalone.

Per una coppia ha, sono necessari quattro VPC. Ciascuno di questi VPC può essere condiviso o standalone. Ad esempio, VPC-0 potrebbe essere un VPC condiviso, mentre VPC-1, VPC-2 e VPC-3 potrebbero essere VPC standalone.

Un VPC condiviso consente di configurare e gestire centralmente le reti virtuali in più progetti. È possibile configurare reti VPC condivise nel *progetto host* e implementare le istanze di connettori e macchine virtuali Cloud Volumes ONTAP in un *progetto di servizio*. ["Documentazione di Google Cloud: Panoramica VPC condivisa"](#).

["Esaminare le autorizzazioni VPC condivise richieste e descritte nella sezione implementazione di Connector"](#)

Mirroring dei pacchetti in VPC

"[Mirroring dei pacchetti](#)" Deve essere disattivato nel VPC Google Cloud in cui si implementa Cloud Volumes ONTAP. Cloud Volumes ONTAP non può funzionare correttamente se il mirroring dei pacchetti è attivato.

Accesso a Internet in uscita

Cloud Volumes ONTAP richiede 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 di 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 firewall 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 firewall 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 si utilizza una coppia ha, il mediatore ha non richiede l'accesso a Internet in uscita.

Se BlueXP notifica che non è possibile inviare messaggi AutoSupport, "[Risolvere i problemi della configurazione AutoSupport](#)".

Regole del firewall

Non è necessario creare regole firewall perché BlueXP fa questo per te. Se è necessario utilizzare il proprio, fare riferimento alle regole del firewall elencate di seguito.

Tenere presente che per una configurazione ha sono necessari due set di regole firewall:

- Un set di regole per i componenti ha in VPC-0. Queste regole consentono l'accesso ai dati a Cloud Volumes ONTAP. [Scopri di più](#).
- Un altro insieme di regole per i componenti ha in VPC-1, VPC-2 e VPC-3. Queste regole sono aperte per le comunicazioni in entrata e in uscita tra i componenti ha. [Scopri di più](#).

Se si desidera eseguire il tiering dei dati cold in un bucket di storage Google Cloud, la subnet in cui risiede Cloud Volumes ONTAP deve essere configurata per l'accesso privato Google (se si utilizza una coppia ha, questa è la subnet in VPC-0). Per istruzioni, fare riferimento a "[Documentazione di Google Cloud: Configurazione di Private Google Access](#)".

Per ulteriori passaggi necessari per impostare il tiering dei dati in BlueXP, 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 Google Cloud e i sistemi ONTAP in altre reti, è necessario disporre di una connessione VPN tra il VPC e l'altra rete, ad esempio la rete aziendale.

Per istruzioni, fare riferimento a. ["Documentazione di Google Cloud: Panoramica di Cloud VPN"](#).

Regole del firewall

BlueXP crea regole di Google Cloud Firewall che includono le regole in entrata e in uscita di cui Cloud Volumes ONTAP ha bisogno per funzionare correttamente. È possibile fare riferimento alle porte a scopo di test o se si preferisce utilizzare le proprie regole firewall.

Le regole del firewall per Cloud Volumes ONTAP richiedono regole sia in entrata che in uscita. Se si sta implementando una configurazione ha, queste sono le regole firewall per Cloud Volumes ONTAP in VPC-0.

Tenere presente che per una configurazione ha sono necessari due set di regole firewall:

- Un set di regole per i componenti ha in VPC-0. Queste regole consentono l'accesso ai dati a Cloud Volumes ONTAP.
- Un altro insieme di regole per i componenti ha in VPC-1, VPC-2 e VPC-3. Queste regole sono aperte per le comunicazioni in entrata e in uscita tra i componenti ha. [Scopri di più](#).



Cerchi informazioni sul connettore? ["Visualizzare le regole del firewall per il connettore"](#)

Regole in entrata

Quando si crea un ambiente di lavoro, è possibile scegliere il filtro di origine per la policy firewall predefinita durante l'implementazione:

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

Se si utilizza una policy firewall personalizzata, assicurarsi di aggiungere tutte le reti che devono comunicare con Cloud Volumes ONTAP, ma anche di aggiungere entrambi gli intervalli di indirizzi per consentire al bilanciamento del carico interno di Google di funzionare correttamente. Questi indirizzi sono 130.211.0.0/22 e 35.191.0.0/16. Per ulteriori informazioni, fare riferimento a. ["Documentazione di Google Cloud: Regole del firewall per il bilanciamento del carico"](#).

Protocollo	Porta	Scopo
Tutti gli ICMP	Tutto	Eseguire il ping dell'istanza
HTTP	80	Accesso HTTP alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
HTTPS	443	Connettività con il connettore e accesso HTTPS alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
SSH	22	Accesso SSH all'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi

Protocollo	Porta	Scopo
TCP	111	Chiamata a procedura remota per NFS
TCP	139	Sessione del servizio NetBIOS per CIFS
TCP	161-162	Protocollo di gestione di rete semplice
TCP	445	Microsoft SMB/CIFS su TCP con frame NetBIOS
TCP	635	Montaggio NFS
TCP	749	Kerberos
TCP	2049	Daemon del server NFS
TCP	3260	Accesso iSCSI tramite LIF dei dati iSCSI
TCP	4045	Daemon di blocco NFS
TCP	4046	Network status monitor per NFS
TCP	10000	Backup con NDMP
TCP	11104	Gestione delle sessioni di comunicazione tra cluster per SnapMirror
TCP	11105	Trasferimento dei dati SnapMirror con LIF intercluster
TCP	63001-63050	Bilanciamento del carico delle porte delle sonde per determinare quale nodo è integro (richiesto solo per coppie ha)
UDP	111	Chiamata a procedura remota per NFS
UDP	161-162	Protocollo di gestione di rete semplice
UDP	635	Montaggio NFS
UDP	2049	Daemon del server NFS
UDP	4045	Daemon di blocco NFS
UDP	4046	Network status monitor per NFS
UDP	4049	Protocollo NFS rquotad

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.

Protocollo	Porta	Scopo
Tutti gli ICMP	Tutto	Tutto il traffico in uscita
Tutti i TCP	Tutto	Tutto il traffico in uscita
Tutti gli UDP	Tutto	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	Protocollo	Porta	Origine	Destinazione	Scopo
Active Directory	TCP	88	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Autenticazione Kerberos V.
	UDP	137	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Servizio nomi NetBIOS
	UDP	138	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS
	TCP	139	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS
	TCP E UDP	389	LIF di gestione dei nodi	Insieme di strutture di Active Directory	LDAP
	TCP	445	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	TCP	464	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	UDP	464	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos
	TCP	749	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Kerberos V change & set Password (RPCSEC_GSS)
	TCP	88	Data LIF (NFS, CIFS, iSCSI)	Insieme di strutture di Active Directory	Autenticazione Kerberos V.
	UDP	137	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Servizio nomi NetBIOS
	UDP	138	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS
	TCP	139	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS
	TCP E UDP	389	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	LDAP
	TCP	445	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	TCP	464	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	UDP	464	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos
	TCP	749	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Kerberos V change & set password (RPCSEC_GSS)

Servizio	Protocollo	Porta	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
Cluster	Tutto il traffico	Tutto il traffico	Tutte le LIF su un nodo	Tutte le LIF sull'altro nodo	Comunicazioni tra cluster (solo Cloud Volumes ONTAP ha)
Backup della configurazione	HTTP	80	LIF di gestione dei nodi	\Http://<connector-IP-address>/occm/offbo xconfig	Inviare i backup della configurazione al connettore. "Informazioni sui file di backup della configurazione" .
DHCP	UDP	68	LIF di gestione dei nodi	DHCP	Client DHCP per la prima installazione
DHCPS	UDP	67	LIF di gestione dei nodi	DHCP	DHCP server (Server DHCP)
DNS	UDP	53	LIF di gestione dei nodi e LIF dei dati (NFS, CIFS)	DNS	DNS
NDMP	TCP	1860-18699	LIF di gestione dei nodi	Server di destinazione	Copia NDMP
SMTP	TCP	25	LIF di gestione dei nodi	Server di posta	Gli avvisi SMTP possono essere utilizzati per AutoSupport
SNMP	TCP	161	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	UDP	161	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	TCP	162	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	UDP	162	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
SnapMirror	TCP	11104	LIF intercluster	ONTAP Intercluster LIF	Gestione delle sessioni di comunicazione tra cluster per SnapMirror
	TCP	11105	LIF intercluster	ONTAP Intercluster LIF	Trasferimento dei dati SnapMirror

Servizio	Protocollo	Porta	Origine	Destinazione	Scopo
Syslog	UDP	514	LIF di gestione dei nodi	Server syslog	Messaggi di inoltro syslog

Regole per VPC-1, VPC-2 e VPC-3

In Google Cloud, una configurazione ha viene implementata in quattro VPC. Le regole del firewall necessarie per la configurazione ha in VPC-0 sono [Elencato sopra per Cloud Volumes ONTAP](#).

Nel frattempo, le regole predefinite del firewall create da BlueXP per le istanze in VPC-1, VPC-2 e VPC-3 consentono la comunicazione in ingresso su *tutti* protocolli e porte. Queste regole consentono la comunicazione tra i nodi ha.

La comunicazione dai nodi ha al mediatore ha avviene sulla porta 3260 (iSCSI).



Per consentire un'elevata velocità di scrittura per le nuove implementazioni di coppie Google Cloud ha, è necessaria un'unità di trasmissione massima (MTU) di almeno 8,896 byte per VPC-1, VPC-2 e VPC-3. Se si sceglie di aggiornare VPC-1, VPC-2 e VPC-3 esistenti a una MTU di 8,896 byte, è necessario arrestare tutti i sistemi ha esistenti che utilizzano questi VPC durante il processo di configurazione.

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 firewall in Google Cloud"](#)

Pianificazione dei controlli dei servizi VPC in GCP

Quando si sceglie di bloccare l'ambiente Google Cloud con i controlli dei servizi VPC, è necessario comprendere come BlueXP e Cloud Volumes ONTAP interagiscono con le API di Google Cloud e come configurare il perimetro dei servizi per implementare BlueXP e Cloud Volumes ONTAP.

I controlli dei servizi VPC consentono di controllare l'accesso ai servizi gestiti da Google all'esterno di un perimetro attendibile, di bloccare l'accesso ai dati da posizioni non attendibili e di ridurre i rischi di trasferimento dei dati non autorizzato. ["Scopri di più su Google Cloud VPC Service Controls"](#).

Come i servizi NetApp comunicano con VPC Service Controls

BlueXP comunica direttamente con le API di Google Cloud. Questo viene attivato da un indirizzo IP esterno a Google Cloud (ad esempio, da `api.services.cloud.netapp.com`) o da un indirizzo interno assegnato a BlueXP Connector all'interno di Google Cloud.

A seconda dello stile di implementazione del connettore, potrebbero essere necessarie alcune eccezioni per il perimetro del servizio.

Immagini

Sia Cloud Volumes ONTAP che BlueXP utilizzano le immagini di un progetto all'interno del GCP gestito da NetApp. Questo può influire sulla distribuzione di BlueXP Connector e Cloud Volumes ONTAP, se l'organizzazione dispone di un criterio che blocca l'utilizzo di immagini non ospitate all'interno dell'organizzazione.

È possibile implementare un connettore manualmente utilizzando il metodo di installazione manuale, ma Cloud Volumes ONTAP dovrà anche estrarre le immagini dal progetto NetApp. È necessario fornire un elenco consentito per implementare un connettore e Cloud Volumes ONTAP.

Implementazione di un connettore

L'utente che implementa un connettore deve essere in grado di fare riferimento a un'immagine ospitata nel projectId *netapp-cloudmanager* e al numero di progetto *14190056516*.

Implementazione di Cloud Volumes ONTAP

- L'account del servizio BlueXP deve fare riferimento a un'immagine ospitata nel projectId *netapp-cloudmanager* e al numero di progetto *14190056516* del progetto del servizio.
- L'account di servizio per l'agente di servizio API di Google predefinito deve fare riferimento a un'immagine ospitata nel projectId *netapp-cloudmanager* e al numero di progetto *14190056516* del progetto di servizio.

Di seguito sono riportati alcuni esempi delle regole necessarie per estrarre queste immagini con VPC Service Controls.

Servizio VPC controlla le policy del perimetro

I criteri consentono eccezioni ai set di regole VPC Service Controls. Per ulteriori informazioni sulle policy, visitare il "[GCP VPC Service Controls Policy Documentation](#)".

Per impostare i criteri richiesti da BlueXP, accedere al perimetro dei controlli dei servizi VPC all'interno dell'organizzazione e aggiungere i seguenti criteri. I campi devono corrispondere alle opzioni fornite nella pagina delle policy VPC Service Controls. Si noti inoltre che le regole **all** sono obbligatorie e che i parametri **OR** devono essere utilizzati nel set di regole.

Regole di ingresso

```
From:
  Identities:
    [User Email Address]
  Source > All sources allowed
To:
  Projects =
    [Service Project]
  Services =
    Service name: iam.googleapis.com
      Service methods: All actions
    Service name: compute.googleapis.com
      Service methods:All actions
```

OPPURE

```
From:
  Identities:
    [User Email Address]
  Source > All sources allowed
To:
  Projects =
    [Host Project]
  Services =
    Service name: compute.googleapis.com
    Service methods: All actions
```

OPPURE

```
From:
  Identities:
    [Service Project Number]@cloudservices.gserviceaccount.com
  Source > All sources allowed
To:
  Projects =
    [Service Project]
    [Host Project]
  Services =
    Service name: compute.googleapis.com
    Service methods: All actions
```

Regole di uscita

```
From:
  Identities:
    [Service Project Number]@cloudservices.gserviceaccount.com
To:
  Projects =
    14190056516
  Service =
    Service name: compute.googleapis.com
    Service methods: All actions
```



Il numero di progetto sopra indicato è il progetto *netapp-cloud-manager* utilizzato da NetApp per memorizzare le immagini per il connettore e per Cloud Volumes ONTAP.

Creare un account di servizio per il tiering e i backup dei dati

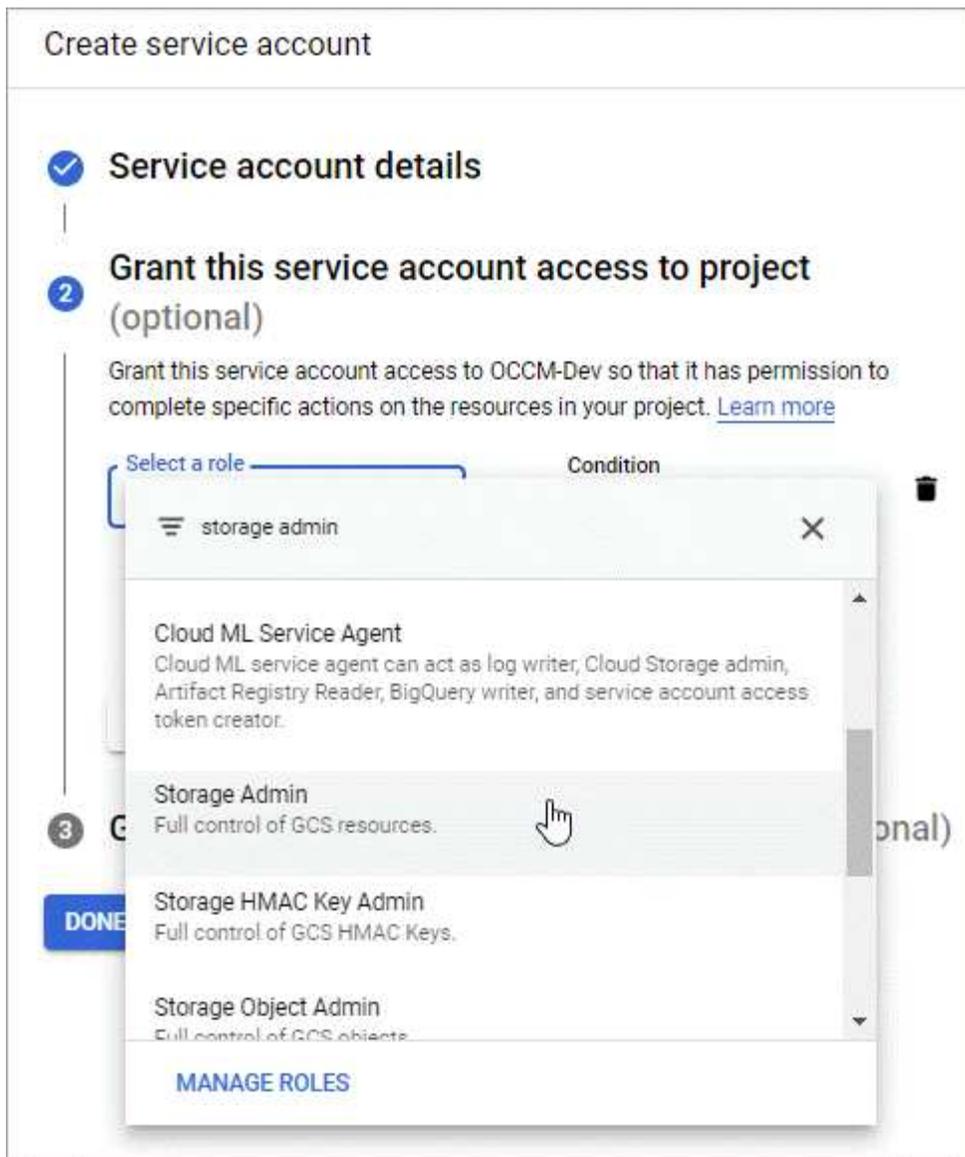
Cloud Volumes ONTAP richiede un account di servizio cloud Google per due scopi. Il primo è quando si attiva "[tiering dei dati](#)" Per tierare i dati cold allo storage a oggetti a basso costo in Google Cloud. Il secondo si verifica quando si attiva "[Backup e ripristino BlueXP](#)" per eseguire il backup dei volumi in uno storage a oggetti a basso costo.

Cloud Volumes ONTAP utilizza l'account di servizio per accedere e gestire un bucket per i dati a più livelli e un altro bucket per i backup.

È possibile configurare un account di servizio e utilizzarlo per entrambi gli scopi. L'account di servizio deve avere il ruolo **Storage Admin**.

Fasi

1. Nella console di Google Cloud, "[Accedere alla pagina Service accounts \(account servizio\)](#)".
2. Selezionare il progetto.
3. Fare clic su **Create service account** (Crea account servizio) e fornire le informazioni richieste.
 - a. **Dettagli account servizio**: Inserire un nome e una descrizione.
 - b. **Consenti a questo account di servizio l'accesso al progetto**: Selezionare il ruolo **Storage Admin**.



- c. **Consenti agli utenti di accedere a questo account del servizio:** Aggiungi l'account del servizio Connector come *utente dell'account del servizio* a questo nuovo account del servizio.

Questa fase è necessaria solo per il tiering dei dati. Non è necessario per il backup e il ripristino di BlueXP.

Create service account

- ✓ Service account details
- ✓ Grant this service account access to project (optional)
- 3 Grant users access to this service account (optional)
Grant access to users or groups that need to perform actions as this service account. [Learn more](#)

Service account users role

netapp-cloud-manager@iam.gserviceaccount.com

Grant users the permissions to deploy jobs and VMs with this service account

Service account admins role

Grant users the permission to administer this service account

DONE CANCEL

Quali sono le prossime novità?

Quando si crea un ambiente di lavoro Cloud Volumes ONTAP, sarà necessario selezionare l'account del servizio in un secondo momento.

Details and Credentials

default-project Google Cloud Project	gcp-sub2 Marketplace Subscription	<div style="border: 1px solid #0070c0; padding: 2px 5px; display: inline-block;">Edit Project</div>
---	--------------------------------------	---

Details

Working Environment Name (Cluster Name)

Service Account 🔴

Service Account Name

+ Add Labels Optional Field | Up to four labels

Credentials

User Name

Password

Confirm Password

Utilizzo di chiavi di crittografia gestite dal cliente con Cloud Volumes ONTAP

Mentre Google Cloud Storage crittografa sempre i tuoi dati prima che vengano scritti su disco, puoi utilizzare l'API BlueXP per creare un sistema Cloud Volumes ONTAP che utilizza *chiavi di crittografia gestite dal cliente*. Si tratta di chiavi che vengono generate e gestite in GCP utilizzando il Cloud Key Management Service.

Fasi

1. Assicurarsi che l'account di servizio di BlueXP Connector disponga delle autorizzazioni corrette a livello di progetto, nel progetto in cui è memorizzata la chiave.

Le autorizzazioni sono fornite in "[Per impostazione predefinita, le autorizzazioni dell'account di servizio del connettore](#)", Ma potrebbe non essere applicato se si utilizza un progetto alternativo per il Cloud Key Management Service.

Le autorizzazioni sono le seguenti:

- `cloudkms.cryptoKeyVersions.useToEncrypt`
- `cloudkms.cryptoKeys.get`
- `cloudkms.cryptoKeys.list`
- `cloudkms.keyRings.list`

2. Assicurarsi che l'account di servizio per ["Agente di servizio di Google Compute Engine"](#) Dispone delle autorizzazioni Cloud KMS Encrypter/Decrypter sulla chiave.

Il nome dell'account del servizio utilizza il seguente formato: "Servizio-[numero_progetto_servizio]@compute-system.iam.gserviceaccount.com".

["Documentazione Google Cloud: Utilizzo di IAM con Cloud KMS - assegnazione di ruoli a una risorsa"](#)

3. Ottenere l'id della chiave richiamando il comando get per `/gcp/vsa/metadata/gcp-encryption-keys` Chiamata API o selezionando "Copy Resource Name" (Copia nome risorsa) sulla chiave nella console GCP.
4. Se si utilizzano chiavi di crittografia gestite dal cliente e tiering dei dati per lo storage a oggetti, BlueXP tenta di utilizzare le stesse chiavi utilizzate per crittografare i dischi persistenti. Tuttavia, prima di tutto, dovrai abilitare i bucket di storage Google Cloud per utilizzare le chiavi:
 - a. Individuare l'agente del servizio Google Cloud Storage seguendo la ["Documentazione Google Cloud: Ottenere l'agente del servizio Cloud Storage"](#).
 - b. Accedere alla chiave di crittografia e assegnare all'agente del servizio Google Cloud Storage le autorizzazioni di crittografia/decrypter Cloud KMS.

Per ulteriori informazioni, fare riferimento a. ["Documentazione Google Cloud: Utilizzo di chiavi di crittografia gestite dal cliente"](#)

5. Utilizzare il parametro "GcpEncryption" con la richiesta API durante la creazione di un ambiente di lavoro.

Esempio

```
"gcpEncryptionParameters": {  
  "key": "projects/project-1/locations/us-east4/keyRings/keyring-  
1/cryptoKeys/generatedkey1"  
}
```

Fare riferimento a. ["Documenti sull'automazione BlueXP"](#) Per ulteriori informazioni sull'utilizzo del parametro "GcpEncryption".

Impostare la licenza per Cloud Volumes ONTAP in Google Cloud

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

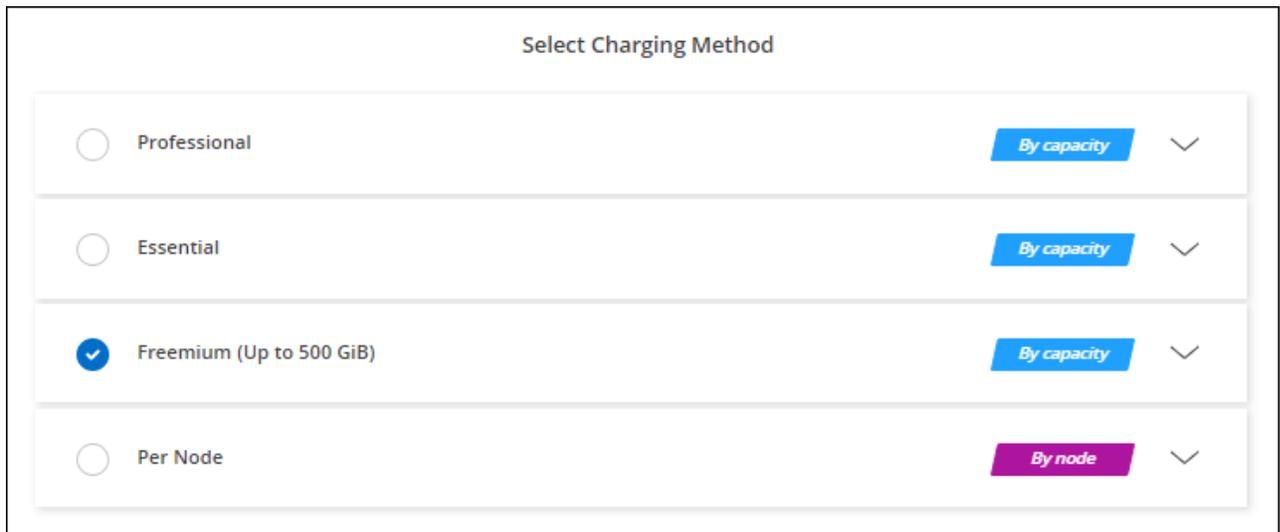
1. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.

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 Google Cloud 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](#)".

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



Select Charging Method		
<input type="radio"/>	Professional	By capacity
<input type="radio"/>	Essential	By capacity
<input checked="" type="radio"/>	Freemium (Up to 500 GiB)	By capacity
<input type="radio"/>	Per Node	By node

["Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in Google Cloud"](#).

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 orario a pagamento (PAYGO) da Google Cloud 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.

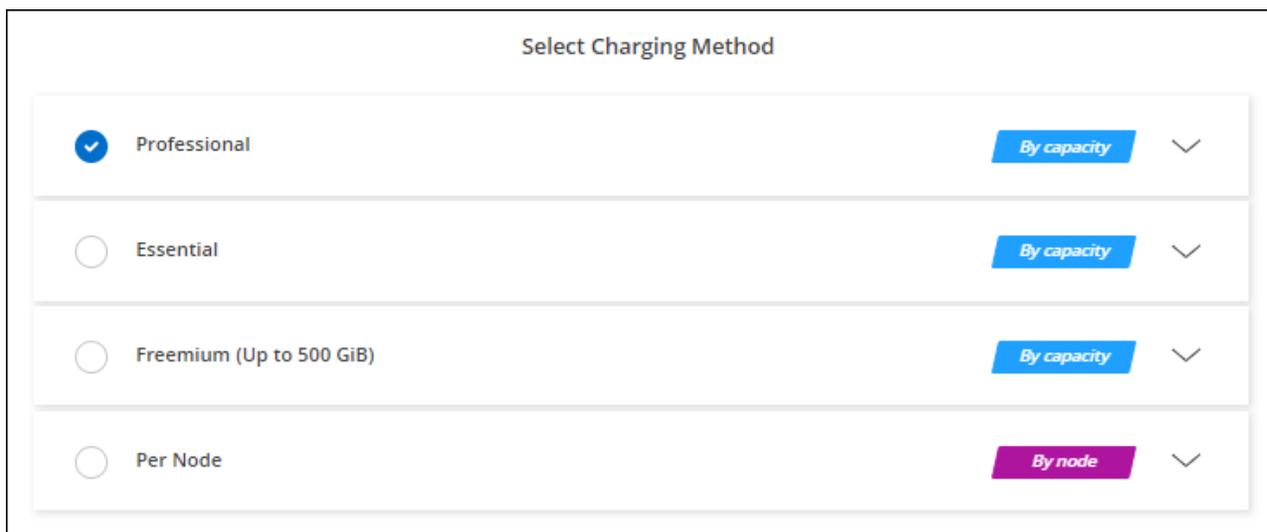
La licenza deve essere disponibile sul portafoglio digitale BlueXP prima di poter essere utilizzata con Cloud Volumes ONTAP. Se necessario, è possibile ["Aggiungere manualmente la licenza al portafoglio digitale BlueXP"](#).

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 Google Cloud 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.

- 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 Google Cloud"](#).

Abbonamento PAYGO

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

Quando crei un ambiente di lavoro Cloud Volumes ONTAP, BlueXP ti chiede di sottoscrivere il contratto disponibile in Google Cloud 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 Google Cloud Marketplace.

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

Select Charging Method	
<input checked="" type="radio"/> Professional	By capacity
<input type="radio"/> Essential	By capacity
<input type="radio"/> Freemium (Up to 500 GiB)	By capacity
<input type="radio"/> Per Node	By node

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



Puoi gestire gli abbonamenti a Google Cloud Marketplace associati ai tuoi account dalla pagina Impostazioni > credenziali. ["Scopri come gestire le tue credenziali e sottoscrizioni Google Cloud"](#)

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 Google Cloud Marketplace.

Dopo che NetApp condivide l'offerta privata con te, puoi selezionare il piano annuale quando ti iscrivi da Google Cloud 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**, quindi seguire le istruzioni per iscriversi al piano annuale in Google Cloud Marketplace.
 - b. In Google Cloud, seleziona il piano annuale condiviso con il tuo account, 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.

Select Charging Method

<input checked="" type="radio"/> Professional	By capacity	∨
<input type="radio"/> Essential	By capacity	∨
<input type="radio"/> Freemium (Up to 500 GiB)	By capacity	∨
<input type="radio"/> Per Node	By node	∨

["Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in Google Cloud"](#).

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](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.

Select Charging Method

Keystone

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1

By capacity

^

Professional

By capacity

v

Essential

By capacity

v

Freemium (Up to 500 GiB)

By capacity

v

Per Node

By node

v

["Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in Google Cloud"](#).

Lancio di Cloud Volumes ONTAP in Google Cloud

È possibile avviare Cloud Volumes ONTAP in una configurazione a nodo singolo o come coppia ha in Google Cloud.

Prima di iniziare

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"](#).
 - L'account del servizio associato al connettore ["deve disporre delle autorizzazioni necessarie"](#)
- Comprensione della configurazione che si desidera utilizzare.

Dovresti aver preparato scegliendo una configurazione e ottenendo le informazioni di rete di Google Cloud dal tuo 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"](#).

- Le API di Google Cloud dovrebbero essere ["abilitato nel tuo progetto"](#):
 - API di Cloud Deployment Manager V2
 - API Cloud Logging
 - API Cloud Resource Manager
 - API di Compute Engine
 - API IAM (Identity and Access Management)

Avvio di un sistema a nodo singolo in Google Cloud

Creare un ambiente di lavoro in BlueXP per avviare Cloud Volumes ONTAP in Google Cloud.

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 località**: Seleziona **Google Cloud** e **Cloud Volumes ONTAP**.
4. Se richiesto, ["Creare un connettore"](#).
5. **Dettagli e credenziali**: Selezionare un progetto, specificare un nome di cluster, selezionare un account di servizio, aggiungere etichette e 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 all'istanza di Google Cloud VM. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di protezione predefinito.
Nome account servizio	Se si intende utilizzare "tiering dei dati" oppure "Backup e ripristino BlueXP" Con Cloud Volumes ONTAP, è necessario attivare account di servizio e selezionare un account di servizio con il ruolo di amministratore dello storage predefinito. "Scopri come creare un account di servizio" .
Aggiungi etichette	Le etichette sono metadati per le risorse Google Cloud. BlueXP aggiunge le etichette al sistema Cloud Volumes ONTAP e alle risorse di Google Cloud associate al sistema. È possibile aggiungere fino a quattro etichette dall'interfaccia utente durante la creazione di un ambiente di lavoro e aggiungerne altre dopo la creazione. Si noti che l'API non limita l'utente a quattro etichette quando crea un ambiente di lavoro. Per informazioni sulle etichette, fare riferimento a "Documentazione Google Cloud: Risorse per l'etichettatura" .

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 <i>admin</i> o modificarlo in un nome utente personalizzato.
Modifica progetto	<p>Selezionare il progetto in cui si desidera che Cloud Volumes ONTAP risieda. Il progetto predefinito è il progetto in cui risiede BlueXP.</p> <p>Se nell'elenco a discesa non sono presenti progetti aggiuntivi, l'account del servizio BlueXP non è ancora stato associato ad altri progetti. Accedere alla console di Google Cloud, aprire il servizio IAM e selezionare il progetto. Aggiungere l'account del servizio con il ruolo BlueXP a quel progetto. Dovrai ripetere questo passaggio per ogni progetto.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  Account di servizio impostato per BlueXP, "come descritto in questa pagina". </div> <p>Fare clic su Add Subscription (Aggiungi abbonamento) per associare le credenziali selezionate a un abbonamento.</p> <p>Per creare un sistema Cloud Volumes ONTAP pay-as-you-go, devi selezionare un progetto Google Cloud associato a un abbonamento a Cloud Volumes ONTAP da Google Cloud Marketplace.</p>

Il video seguente mostra come associare un abbonamento a pagamento a Marketplace al progetto Google Cloud. In alternativa, seguire la procedura per effettuare l'iscrizione nella ["Associazione di un abbonamento a Marketplace con le credenziali Google Cloud"](#) sezione.

► https://docs.netapp.com/it-it/test//media/video_subscribing_gcp.mp4 (video)

6. **Servizi:** Selezionare i servizi che si desidera utilizzare sul sistema. Per selezionare il backup e ripristino BlueXP o per utilizzare il tiering BlueXP, è necessario aver specificato l'account di servizio nel passaggio 3.



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. **Posizione e connettività:** Selezionare una posizione, scegliere una policy firewall e confermare la connettività di rete allo storage Google Cloud per il tiering dei dati.

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

Campo	Descrizione
Verifica della connettività	Per eseguire il tiering dei dati cold in un bucket di storage cloud Google, la subnet in cui risiede Cloud Volumes ONTAP deve essere configurata per l'accesso privato a Google. Per istruzioni, fare riferimento a. "Documentazione Google Cloud: Configurazione di Private Google Access" .

Campo	Descrizione
Policy firewall generata	<p>Se si consente a BlueXP di generare il criterio firewall, è necessario scegliere come consentire il traffico:</p> <ul style="list-style-type: none"> • Se si sceglie Selected VPC only (solo VPC selezionato), il filtro di origine per il traffico in entrata corrisponde all'intervallo di sottorete del VPC selezionato e all'intervallo di sottorete del VPC in cui si trova il connettore. Questa è l'opzione consigliata. • Se si sceglie All VPC, il filtro di origine per il traffico in entrata corrisponde all'intervallo IP 0.0.0.0/0.
Utilizza policy firewall esistenti	<p>Se si utilizza un criterio firewall esistente, assicurarsi che includa le regole richieste. Link: Learn About firewall rules for Cloud Volumes ONTAP.</p>

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 **Crea la mia 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 computer.



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 viene eseguito da una versione all'altra, ad esempio da 9,6 a 9,7.

11. **Risorse di storage sottostanti**: Scegliere le impostazioni per l'aggregato iniziale: Un tipo di disco e le dimensioni di ciascun disco.

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 ["Dimensionare il sistema in Google Cloud"](#).

12. **Flash cache, velocità di scrittura e WORM**:

a. Attivare **Flash cache**, se lo si desidera.



A partire da Cloud Volumes ONTAP 9.13.1, *Flash cache* è supportato sui tipi di istanze n2-standard-16, n2-standard-32, n2-standard-48 e n2-standard-64. Non è possibile disattivare Flash cache dopo l'implementazione.

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

["Scopri di più sulla velocità di scrittura"](#).



L'opzione **High** write speed (velocità di scrittura elevata) offre un'elevata velocità di scrittura e un'unità MTU (Maximum Transmission Unit) di 8,896 byte. Inoltre, la MTU superiore di 8,896 richiede la selezione di VPC-1, VPC-2 e VPC-3 per l'implementazione. Per ulteriori informazioni su VPC-1, VPC-2 e VPC-3, vedere ["Regole per VPC-1, VPC-2 e VPC-3"](#).

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

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.

13. **Tiering dei dati nella piattaforma cloud di Google:** Scegliere se attivare il tiering dei dati sull'aggregato iniziale, scegliere una classe di storage per i dati a più livelli, quindi selezionare un account di servizio con il ruolo di amministratore dello storage predefinito (richiesto per Cloud Volumes ONTAP 9.7 o versione successiva), Oppure seleziona un account Google Cloud (richiesto per Cloud Volumes ONTAP 9.6).

Tenere presente quanto segue:

- BlueXP imposta l'account del servizio sull'istanza di Cloud Volumes ONTAP. Questo account di servizio fornisce le autorizzazioni per il tiering dei dati a un bucket di storage Google Cloud. Assicurarsi di aggiungere l'account del servizio Connector come utente dell'account del servizio di tiering, altrimenti non è possibile selezionarlo da BlueXP
- Per informazioni sull'aggiunta di un account Google Cloud, vedere ["Configurazione e aggiunta di account Google Cloud per il tiering dei dati con 9.6"](#).
- 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 su aggregati successivi, ma è necessario spegnere il sistema e aggiungere un account di servizio dalla console di Google Cloud.

["Scopri di più sul tiering dei dati"](#).

14. **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.
Initiator group e IQN (solo per iSCSI)	<p>Le destinazioni di storage iSCSI sono denominate LUN (unità logiche) e vengono presentate agli host come dispositivi a blocchi standard.</p> <p>I gruppi di iniziatori sono tabelle dei nomi dei nodi host iSCSI e controllano quali iniziatori hanno accesso a quali LUN.</p> <p>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).</p> <p>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".</p>

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

Volume Details, Protection & Protocol

Details & Protection	Protocol
<p>Volume Name: <input style="width: 200px;" type="text" value="vol"/> Size (GB): <input style="width: 80px;" type="text" value="250"/></p> <p>Snapshot Policy: <input style="width: 300px;" type="text" value="default"/></p> <p><small>Default Policy</small></p>	<p style="text-align: center;"> <input type="radio"/> NFS <input checked="" type="radio"/> CIFS <input type="radio"/> iSCSI </p> <hr/> <p>Share name: <input style="width: 150px;" type="text" value="vol_share"/> Permissions: <input style="width: 150px;" type="text" value="Full Control"/></p> <p>Users / Groups: <input style="width: 300px;" type="text" value="engineering"/></p> <p><small>Valid users and groups separated by a semicolon</small></p>

15. **CIFS Setup:** Se si sceglie il protocollo CIFS, impostare un server CIFS.

Campo	Descrizione
Indirizzo IP primario e secondario DNS	<p>Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server CIFS.</p> <p>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.</p> <p>Se si configura Google Managed Active Directory, per impostazione predefinita è possibile accedere ad utilizzando l'indirizzo IP 169.254.169.254.</p>
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.
Unità organizzativa	<p>L'unità organizzativa all'interno del dominio ad da associare al server CIFS. L'impostazione predefinita è CN=computer.</p> <p>Per configurare Google Managed Microsoft ad come server ad per Cloud Volumes ONTAP, immettere OU=computer,OU=cloud in questo campo.</p> <p>"Documentazione Google Cloud: Unità organizzative in Google Managed Microsoft ad"</p>
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.

Campo	Descrizione
Server NTP	<p>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.</p> <p>Nota: È possibile configurare un server NTP solo quando si crea un server CIFS. Non è configurabile dopo aver creato il server CIFS.</p>

16. **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](#)".

17. **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 Google Cloud 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 **Ricomporre 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 ha in Google Cloud

Creare un ambiente di lavoro in BlueXP per avviare Cloud Volumes ONTAP in Google Cloud.

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 località:** Seleziona **Google Cloud** e **Cloud Volumes ONTAP ha**.

4. **Dettagli e credenziali:** Selezionare un progetto, specificare un nome di cluster, selezionare un account di servizio, aggiungere etichette e 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 all'istanza di Google Cloud VM. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di protezione predefinito.
Nome account servizio	Se si intende utilizzare "Tiering BlueXP" oppure "Backup e ripristino BlueXP" Services (servizi), è necessario attivare lo switch Service account (account servizio) e selezionare l'account di servizio che ha il ruolo di amministratore dello storage predefinito.
Aggiungi etichette	<p>Le etichette sono metadati per le risorse Google Cloud. BlueXP aggiunge le etichette al sistema Cloud Volumes ONTAP e alle risorse di Google Cloud associate al sistema.</p> <p>È possibile aggiungere fino a quattro etichette dall'interfaccia utente durante la creazione di un ambiente di lavoro e aggiungerne altre dopo la creazione. Si noti che l'API non limita l'utente a quattro etichette quando crea un ambiente di lavoro.</p> <p>Per informazioni sulle etichette, fare riferimento a "Documentazione Google Cloud: Risorse per l'etichettatura".</p>
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 <i>admin</i> o modificarlo in un nome utente personalizzato.
Modifica progetto	<p>Selezionare il progetto in cui si desidera che Cloud Volumes ONTAP risieda. Il progetto predefinito è il progetto in cui risiede BlueXP.</p> <p>Se nell'elenco a discesa non sono presenti progetti aggiuntivi, l'account del servizio BlueXP non è ancora stato associato ad altri progetti. Accedere alla console di Google Cloud, aprire il servizio IAM e selezionare il progetto. Aggiungere l'account del servizio con il ruolo BlueXP a quel progetto. Dovrai ripetere questo passaggio per ogni progetto.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  Account di servizio impostato per BlueXP, "come descritto in questa pagina". </div> <p>Fare clic su Add Subscription (Aggiungi abbonamento) per associare le credenziali selezionate a un abbonamento.</p> <p>Per creare un sistema Cloud Volumes ONTAP pay-as-you-go, devi selezionare un progetto Google Cloud associato a un abbonamento a Cloud Volumes ONTAP da Google Cloud Marketplace.</p>

Il video seguente mostra come associare un abbonamento a pagamento a Marketplace al progetto Google

Cloud. In alternativa, seguire la procedura per effettuare l'iscrizione nella ["Associazione di un abbonamento a Marketplace con le credenziali Google Cloud"](#) sezione.

► https://docs.netapp.com/it-it/test//media/video_subscribing_gcp.mp4 (video)

5. **Servizi:** Selezionare i servizi che si desidera utilizzare sul sistema. Per selezionare il backup e ripristino BlueXP o per utilizzare BlueXP Tiering, è necessario aver specificato l'account di servizio nel passaggio 3.



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. **Ha Deployment Models** (modelli di implementazione ha): Scegliere più zone (consigliato) o una singola zona per la configurazione ha. Quindi selezionare una regione e zone.

["Scopri di più sui modelli di implementazione ha"](#).

7. **Connettività:** Selezionare quattro diversi VPC per la configurazione ha, una subnet in ciascun VPC, quindi scegliere un criterio firewall.

["Scopri di più sui requisiti di rete"](#).

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

Campo	Descrizione
Policy generata	Se si consente a BlueXP di generare il criterio firewall, è necessario scegliere come consentire il traffico: <ul style="list-style-type: none">• Se si sceglie Selected VPC only (solo VPC selezionato), il filtro di origine per il traffico in entrata corrisponde all'intervallo di sottorete del VPC selezionato e all'intervallo di sottorete del VPC in cui si trova il connettore. Questa è l'opzione consigliata.• Se si sceglie All VPC, il filtro di origine per il traffico in entrata corrisponde all'intervallo IP 0.0.0.0/0.
USA esistente	Se si utilizza un criterio firewall esistente, assicurarsi che includa le regole richieste. "Scopri le regole del firewall per Cloud Volumes ONTAP" .

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 **Crea la mia 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 computer.



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 viene eseguito da una versione all'altra, ad esempio da 9,6 a 9,7.

11. **Risorse di storage sottostanti:** Scegliere le impostazioni per l'aggregato iniziale: Un tipo di disco e le dimensioni di ciascun disco.

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 ["Dimensionare il sistema in Google Cloud"](#).

12. **Flash cache, velocità di scrittura e WORM:**

- a. Attivare **Flash cache**, se lo si desidera.



A partire da Cloud Volumes ONTAP 9.13.1, *Flash cache* è supportato sui tipi di istanze n2-standard-16, n2-standard-32, n2-standard-48 e n2-standard-64. Non è possibile disattivare Flash cache dopo l'implementazione.

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

["Scopri di più sulla velocità di scrittura"](#).



L'opzione **High** write speed con i tipi di istanze n2-standard-16, n2-standard-32, n2-standard-48 e n2-standard-64 offre un'elevata velocità di scrittura e un'unità MTU (Maximum Transmission Unit) di 8,896 byte. Inoltre, la MTU superiore di 8,896 richiede la selezione di VPC-1, VPC-2 e VPC-3 per l'implementazione. L'elevata velocità di scrittura e una MTU di 8,896 dipendono dalle funzionalità e non possono essere disabilitate singolarmente all'interno di un'istanza configurata. Per ulteriori informazioni su VPC-1, VPC-2 e VPC-3, vedere ["Regole per VPC-1, VPC-2 e VPC-3"](#).

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

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.

13. **Data Tiering in Google Cloud:** Scegliere se attivare il tiering dei dati sull'aggregato iniziale, scegliere una classe di storage per i dati a più livelli, quindi selezionare un account di servizio con il ruolo predefinito Storage Admin.

Tenere presente quanto segue:

- BlueXP imposta l'account del servizio sull'istanza di Cloud Volumes ONTAP. Questo account di servizio fornisce le autorizzazioni per il tiering dei dati a un bucket di storage Google Cloud. Assicurarsi di aggiungere l'account del servizio Connector come utente dell'account del servizio di tiering, altrimenti non è possibile selezionarlo da BlueXP.
- 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 su aggregati successivi, ma è necessario spegnere il sistema e aggiungere un account di servizio dalla console di Google Cloud.

["Scopri di più sul tiering dei dati"](#).

14. **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)	<p>Le destinazioni di storage iSCSI sono denominate LUN (unità logiche) e vengono presentate agli host come dispositivi a blocchi standard.</p> <p>I gruppi di iniziatori sono tabelle dei nomi dei nodi host iSCSI e controllano quali iniziatori hanno accesso a quali LUN.</p> <p>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).</p> <p>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".</p>

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

Volume Details, Protection & Protocol

Details & Protection

Volume Name: Size (GB):

Snapshot Policy:

Default Policy

Protocol

NFS CIFS iSCSI

Share name: Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

15. **CIFS Setup:** Se si sceglie il protocollo CIFS, impostare un server CIFS.

Campo	Descrizione
Indirizzo IP primario e secondario DNS	<p>Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server CIFS.</p> <p>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.</p> <p>Se si configura Google Managed Active Directory, per impostazione predefinita è possibile accedere ad utilizzando l'indirizzo IP 169.254.169.254.</p>
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.

Campo	Descrizione
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 Google Managed Microsoft ad come server ad per Cloud Volumes ONTAP, immettere OU=computer,OU=cloud in questo campo. "Documentazione Google Cloud: Unità organizzative in Google Managed Microsoft ad"
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.

16. **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"](#).

17. **Review & Approve** (Rivedi e approva): Consente di rivedere e confermare le selezioni.

- Esaminare i dettagli della configurazione.
- Fare clic su **ulteriori informazioni** per visualizzare i dettagli relativi al supporto e alle risorse Google Cloud che BlueXP acquisterà.
- Selezionare le caselle di controllo **ho capito....**
- 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.

Verifica dell'immagine della piattaforma Google Cloud

Panoramica sulla verifica delle immagini di Google Cloud

La verifica delle immagini di Google Cloud è conforme ai requisiti di sicurezza NetApp avanzati. Sono state apportate modifiche allo script che genera le immagini per firmare l'immagine lungo il percorso utilizzando le chiavi private generate specificamente per questa attività. È possibile verificare l'integrità dell'immagine GCP utilizzando il digest firmato e il certificato pubblico per Google Cloud che possono essere scaricati tramite ["NSS"](#) per una release specifica.



La verifica dell'immagine Google Cloud è supportata dal software Cloud Volumes ONTAP versione 9.13.0 o superiore.

Converti l'immagine in formato raw su Google Cloud

L'immagine utilizzata per implementare nuove istanze, aggiornamenti o utilizzata in immagini esistenti verrà condivisa con i client tramite ["Il NetApp Support Site \(NSS\)"](#). Il digest firmato e i certificati saranno disponibili per il download attraverso il portale NSS. Assicurarsi di scaricare il digest e i certificati per la release corretta corrispondente all'immagine condivisa dal supporto NetApp. Ad esempio, 9.13.0 immagini avranno un digest con 9.13.0 firme e certificati disponibili su NSS.

Perché è necessario questo passaggio?

Le immagini di Google Cloud non possono essere scaricate direttamente. Per verificare l'immagine rispetto al digest firmato e ai certificati, è necessario disporre di un meccanismo per confrontare i due file e scaricare l'immagine. Per farlo, devi esportare/convertire l'immagine in un formato disk.raw e salvare i risultati in un bucket di storage su Google Cloud. Il file disk.raw viene archiviato e compresso nel processo.

L'account utente/servizio avrà bisogno di privilegi per eseguire le seguenti operazioni:

- Accesso al bucket di storage Google
- Scrivi al bucket di storage Google
- Creazione di processi di cloud build (utilizzati durante il processo di esportazione)
- Accesso all'immagine desiderata
- Creare attività di esportazione delle immagini

Per verificare l'immagine, è necessario convertirla in un formato disk.raw e quindi scaricarla.

Utilizza la riga di comando di Google Cloud per esportare l'immagine di Google Cloud

Il modo preferito per esportare un'immagine in Cloud Storage è utilizzare ["comando di esportazione delle immagini di calcolo di gcloud"](#). Questo comando prende l'immagine fornita e la converte in un file disk.raw che viene tarred e gzipato. Il file generato viene salvato nell'URL di destinazione e può essere scaricato per la verifica.

Per eseguire questa operazione, l'utente/account deve disporre dei privilegi necessari per accedere e scrivere nel bucket desiderato, esportare l'immagine e creare cloud (utilizzati da Google per esportare l'immagine).

Esportare l'immagine di Google Cloud utilizzando gcloud

Fare clic per visualizzare lo script

```
$ gcloud compute images export \  
  --destination-uri DESTINATION_URI \  
  --image IMAGE_NAME  
  
# For our example:  
$ gcloud compute images export \  
  --destination-uri gs://vsa-dev-bucket1/example-user-exportimage-  
gcp-demo \  
  --image example-user-20230120115139  
  
## DEMO ##  
# Step 1 - Optional: Checking access and listing objects in the  
destination bucket  
$ gsutil ls gs://example-user-export-image-bucket/  
  
# Step 2 - Exporting the desired image to the bucket  
$ gcloud compute images export --image example-user-export-image-demo  
--destination-uri gs://example-user-export-image-bucket/export-  
demo.tar.gz  
Created [https://cloudbuild.googleapis.com/v1/projects/example-demo-  
project/locations/us-central1/builds/xxxxxxxxxxxxx].  
Logs are available at [https://console.cloud.google.com/cloud-  
build/builds;region=us-central1/xxxxxxxxxxxxx?project=xxxxxxxxxxxxx].  
[image-export]: 2023-01-25T18:13:48Z Fetching image "example-user-  
export-image-demo" from project "example-demo-project".  
[image-export]: 2023-01-25T18:13:49Z Validating workflow  
[image-export]: 2023-01-25T18:13:49Z Validating step "setup-disks"  
[image-export]: 2023-01-25T18:13:49Z Validating step "image-export-  
export-disk"  
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z  
Validating step "setup-disks"  
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z  
Validating step "run-image-export-export-disk"  
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z  
Validating step "wait-for-inst-image-export-export-disk"  
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z  
Validating step "copy-image-object"  
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z  
Validating step "delete-inst"  
[image-export]: 2023-01-25T18:13:51Z Validation Complete  
[image-export]: 2023-01-25T18:13:51Z Workflow Project: example-demo-  
project  
[image-export]: 2023-01-25T18:13:51Z Workflow Zone: us-central1-c
```

```
[image-export]: 2023-01-25T18:13:51Z Workflow GCSPath: gs://example-
demo-project-example-bkt-us/
[image-export]: 2023-01-25T18:13:51Z Example scratch path:
https://console.cloud.google.com/storage/browser/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px
[image-export]: 2023-01-25T18:13:51Z Uploading sources
[image-export]: 2023-01-25T18:13:51Z Running workflow
[image-export]: 2023-01-25T18:13:51Z Running step "setup-disks"
(CreateDisks)
[image-export.setup-disks]: 2023-01-25T18:13:51Z CreateDisks: Creating
disk "disk-image-export-image-export-r88px".
[image-export]: 2023-01-25T18:14:02Z Step "setup-disks" (CreateDisks)
successfully finished.
[image-export]: 2023-01-25T18:14:02Z Running step "image-export-export-
disk" (IncludeWorkflow)
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "setup-disks" (CreateDisks)
[image-export.image-export-export-disk.setup-disks]: 2023-01-
25T18:14:02Z CreateDisks: Creating disk "disk-image-export-export-disk-
image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Step
"setup-disks" (CreateDisks) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "run-image-export-export-disk" (CreateInstances)
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:02Z CreateInstances: Creating instance "inst-image-
export-export-disk-image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Step
"run-image-export-export-disk" (CreateInstances) successfully finished.
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:08Z CreateInstances: Streaming instance "inst-image-
export-export-disk-image-export-image-export--r88px" serial port 1
output to https://storage.cloud.google.com/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px/logs/inst-
image-export-export-disk-image-export-image-export--r88px-serial-
port1.log
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Running
step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:08Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
watching serial port 1, SuccessMatch: "ExportSuccess", FailureMatch:
["ExportFailed:"] (this is not an error), StatusMatch: "GCEExport:".
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
```

```
StatusMatch found: "GCEExport: <serial-output key:'source-size-gb'  
value:'10'>"  
[image-export.image-export-export-disk.wait-for-inst-image-export-  
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance  
"inst-image-export-export-disk-image-export-image-export--r88px":  
StatusMatch found: "GCEExport: Running export tool."  
[image-export.image-export-export-disk.wait-for-inst-image-export-  
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance  
"inst-image-export-export-disk-image-export-image-export--r88px":  
StatusMatch found: "GCEExport: Disk /dev/sdb is 10 GiB, compressed size  
will most likely be much smaller."  
[image-export.image-export-export-disk.wait-for-inst-image-export-  
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance  
"inst-image-export-export-disk-image-export-image-export--r88px":  
StatusMatch found: "GCEExport: Beginning export process..."  
[image-export.image-export-export-disk.wait-for-inst-image-export-  
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance  
"inst-image-export-export-disk-image-export-image-export--r88px":  
StatusMatch found: "GCEExport: Copying \"/dev/sdb\" to gs://example-  
demo-project-example-bkt-us/example-image-export-20230125-18:13:49-  
r88px/outs/image-export-export-disk.tar.gz."  
[image-export.image-export-export-disk.wait-for-inst-image-export-  
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance  
"inst-image-export-export-disk-image-export-image-export--r88px":  
StatusMatch found: "GCEExport: Using \"/root/upload\" as the buffer  
prefix, 1.0 GiB as the buffer size, and 4 as the number of workers."  
[image-export.image-export-export-disk.wait-for-inst-image-export-  
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance  
"inst-image-export-export-disk-image-export-image-export--r88px":  
StatusMatch found: "GCEExport: Creating gzipped image of \"/dev/sdb\"."  
[image-export.image-export-export-disk.wait-for-inst-image-export-  
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance  
"inst-image-export-export-disk-image-export-image-export--r88px":  
StatusMatch found: "GCEExport: Read 1.0 GiB of 10 GiB (212 MiB/sec),  
total written size: 992 MiB (198 MiB/sec)"  
[image-export.image-export-export-disk.wait-for-inst-image-export-  
export-disk]: 2023-01-25T18:14:59Z WaitForInstancesSignal: Instance  
"inst-image-export-export-disk-image-export-image-export--r88px":  
StatusMatch found: "GCEExport: Read 8.0 GiB of 10 GiB (237 MiB/sec),  
total written size: 1.5 GiB (17 MiB/sec)"  
[image-export.image-export-export-disk.wait-for-inst-image-export-  
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance  
"inst-image-export-export-disk-image-export-image-export--r88px":  
StatusMatch found: "GCEExport: Finished creating gzipped image of  
\"/dev/sdb\" in 48.956433327s [213 MiB/s] with a compression ratio of  
6."
```

```

[image-export.image-export-export-disk.wait-for-inst-image-export-export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance "inst-image-export-export-disk-image-export-image-export--r88px": StatusMatch found: "GCEExport: Finished export in 48.957347731s"
[image-export.image-export-export-disk.wait-for-inst-image-export-export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance "inst-image-export-export-disk-image-export-image-export--r88px": StatusMatch found: "GCEExport: <serial-output key:'target-size-gb' value:'2'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance "inst-image-export-export-disk-image-export-image-export--r88px": SuccessMatch found "ExportSuccess"
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running step "copy-image-object" (CopyGCSObjects)
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running step "delete-inst" (DeleteResources)
[image-export.image-export-export-disk.delete-inst]: 2023-01-25T18:15:19Z DeleteResources: Deleting instance "inst-image-export-export-disk".
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step "copy-image-object" (CopyGCSObjects) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:34Z Step "delete-inst" (DeleteResources) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Step "image-export-export-disk" (IncludeWorkflow) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> source-size-gb:10
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> target-size-gb:2
[image-export]: 2023-01-25T18:15:34Z Workflow "image-export" cleaning up (this may take up to 2 minutes).
[image-export]: 2023-01-25T18:15:35Z Workflow "image-export" finished cleanup.

# Step 3 - Validating the image was successfully exported
$ gsutil ls gs://example-user-export-image-bucket/
gs://example-user-export-image-bucket/export-demo.tar.gz

# Step 4 - Download the exported image
$ gcloud storage cp gs://BUCKET_NAME/OBJECT_NAME SAVE_TO_LOCATION

```

```
$ gcloud storage cp gs://example-user-export-image-bucket/export-  
demo.tar.gz CVO_GCP_Signed_Digest.tar.gz  
Copying gs://example-user-export-image-bucket/export-demo.tar.gz to  
file://CVO_GCP_Signed_Digest.tar.gz  
Completed files 1/1 | 1.5GiB/1.5GiB | 185.0MiB/s
```

```
Average throughput: 213.3MiB/s
```

```
$ ls -l  
total 1565036  
-rw-r--r-- 1 example-user example-user 1602589949 Jan 25 18:44  
CVO_GCP_Signed_Digest.tar.gz
```

Estrarre i file compressi

```
# Extracting files from the digest  
$ tar -xf CVO_GCP_Signed_Digest.tar.gz
```



Vedere "[Documento Google Cloud sull'esportazione di un'immagine](#)" Per ulteriori informazioni su come esportare un'immagine tramite Google Cloud.

Verifica della firma dell'immagine

Verificare le immagini firmate di Google Cloud

Per verificare l'immagine firmata Google Cloud esportata, è necessario scaricare il file di digest dell'immagine da NSS per convalidare il file disk.raw e il contenuto del file di digest.

Riepilogo del flusso di lavoro per la verifica dell'immagine firmata

Di seguito viene riportata una panoramica del processo di verifica delle immagini firmato da Google Cloud.

- Dal "[NSS](#)", Scaricare l'archivio Google Cloud contenente i seguenti file:
 - Digest firmato (.sig)
 - Certificato contenente la chiave pubblica (.pem)
 - Catena di certificati (.pem)

Cloud Volumes ONTAP 9.13.0

Date Posted:

Restrictions on Encryption Technology

NetApp Volume Encryption (available with ONTAP 9.1 and later releases) provides for data-at-rest encryption that requires authorizations, permits, or licenses to import, export, re-export or use this software.

A state license for importing encryption equipment is required to import ONTAP 9.1 (or later) with NetApp Volume Encryption into Member States of the Eurasian Economic Union: Russia, Belarus, Kazakhstan, Armenia and Kyrgyzstan. Moreover, in certain cases, an end-user customer must have a valid state encryption license to this software.

Consult your legal advisor on this matter.

Cloud Volumes ONTAP
Non-Restricted Countries

If you are upgrading to ONTAP 9.13.0, and you are in "Non-restricted Countries", please download the image with NetApp Volume Encryption.

[DOWNLOAD 9130_V_IMAGE.TGZ \[2.58 GB\]](#)

[View and download checksums](#)

[DOWNLOAD 9130_V_IMAGE.TGZ.PEM \[451 B\]](#)

[View and download checksums](#)

[DOWNLOAD 9130_V_IMAGE.TGZ.SIG \[256 B\]](#)

[View and download checksums](#)

Cloud Volumes ONTAP
Restricted Countries

If you are unsure whether your company complied with all applicable legal requirements on encryption technology, download the image without NetApp Volume Encryption.

[DOWNLOAD 9130_V_NODAR_IMAGE.TGZ \[2.58 GB\]](#)

[View and download checksums](#)

[DOWNLOAD 9130_V_NODAR_IMAGE.TGZ.PEM \[451 B\]](#)

[View and download checksums](#)

[DOWNLOAD 9130_V_NODAR_IMAGE.TGZ.SIG \[256 B\]](#)

[View and download checksums](#)

Cloud Volumes ONTAP
Google Image Digest Files

[DOWNLOAD GCP-X-9-13-0_PKG.TAR.GZ \[7.52 KB\]](#)

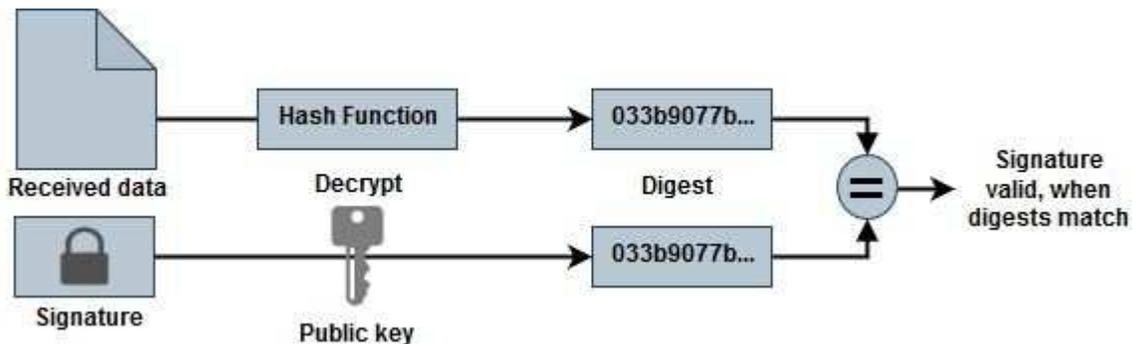
[View and download checksums](#)

Azure Image Digest File

[DOWNLOAD AZURE-9.13.0_PKG.TAR.GZ \[7.55 KB\]](#)

[View and download checksums](#)

- Scaricare il file disk.raw convertito
- Validare il certificato utilizzando la catena del certificato
- Validare il digest firmato utilizzando il certificato contenente la chiave pubblica
 - Decrittare il digest firmato utilizzando la chiave pubblica per estrarre il digest del file di immagine
 - Creare un digest del file disk.raw scaricato
 - Confrontare i due file digest per la convalida



Verifica del file disk.raw e del contenuto del file digest con OpenSSL

È possibile verificare il file disk.raw scaricato da Google Cloud rispetto al contenuto del file digest disponibile tramite "NSS" Con OpenSSL.



I comandi OpenSSL per la convalida dell'immagine sono compatibili con macchine Linux, Mac OS e Windows.

Fasi

1. Verificare il certificato utilizzando OpenSSL.

Fare clic per visualizzare lo script

```
# Step 1 - Optional, but recommended: Verify the certificate using
OpenSSL

# Step 1.1 - Copy the Certificate and certificate chain to a
directory
$ openssl version
LibreSSL 3.3.6
$ ls -l
total 48
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem

# Step 1.2 - Get the OSCP URL
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in <Certificate-
Chain.pem>)
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem)
$ echo $oscp_url
http://ocsp.entrust.net

# Step 1.3 - Generate an OSCP request for the certificate
$ openssl ocsf -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsf -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -reqout req.der

# Step 1.4 - Optional: Check the new file "req.der" has been
generated
$ ls -l
total 56
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der

# Step 1.5 - Connect to the OSCP Manager using openssl to send the
OCSP request
$ openssl ocsf -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${oscp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocspl -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -url ${ocsp_url} -resp_text
-respout resp.der
```

OCSP Response Data:

OCSP Response Status: successful (0x0)

Response Type: Basic OCSP Response

Version: 1 (0x0)

Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2

Produced At: Jan 19 15:14:00 2023 GMT

Responses:

Certificate ID:

Hash Algorithm: sha1

Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A

Issuer Key Hash: CE894F8251AA15A28462CA312361D261F8F8FE78

Serial Number: 5994B3D01D26D594BD1D0FA7098C6FF5

Cert Status: good

This Update: Jan 19 15:00:00 2023 GMT

Next Update: Jan 26 14:59:59 2023 GMT

Signature Algorithm: sha512WithRSAEncryption

0b:b6:61:e4:03:5f:98:6f:10:1c:9a:f7:5f:6f:c7:e3:f4:72:
f2:30:f4:86:88:9a:b9:ba:1e:d6:f6:47:af:dc:ea:e4:cd:31:
af:e3:7a:20:35:9e:60:db:28:9c:7f:2e:17:7b:a5:11:40:4f:
1e:72:f7:f8:ef:e3:23:43:1b:bb:28:1a:6f:c6:9c:c5:0c:14:
d3:5d:bd:9b:6b:28:fb:94:5e:8a:ef:40:20:72:a4:41:df:55:
cf:f3:db:1b:39:e0:30:63:c9:c7:1f:38:7e:7f:ec:f4:25:7b:
1e:95:4c:70:6c:83:17:c3:db:b2:47:e1:38:53:ee:0a:55:c0:
15:6a:82:20:b2:ea:59:eb:9c:ea:7e:97:aa:50:d7:bc:28:60:
8c:d4:21:92:1c:13:19:b4:e0:66:cb:59:ed:2e:f8:dc:7b:49:
e3:40:f2:b6:dc:d7:2d:2e:dd:21:82:07:bb:3a:55:99:f7:59:
5d:4a:4d:ca:e7:8f:1c:d3:9a:3f:17:7b:7a:c4:57:b2:57:a8:
b4:c0:a5:02:bd:59:9c:50:32:ff:16:b1:65:3a:9c:8c:70:3b:
9e:be:bc:4f:f9:86:97:b1:62:3c:b2:a9:46:08:be:6b:1b:3c:
24:14:59:28:c6:ae:e8:d5:64:b2:f8:cc:28:24:5c:b2:c8:d8:
5a:af:9d:55:48:96:f6:3e:c6:bf:a6:0c:a4:c0:ab:d6:57:03:
2b:72:43:b0:6a:9f:52:ef:43:bb:14:6a:ce:66:cc:6c:4e:66:
17:20:a3:64:e0:c6:d1:82:0a:d7:41:8a:cc:17:fd:21:b5:c6:
d2:3a:af:55:2e:2a:b8:c7:21:41:69:e1:44:ab:a1:dd:df:6d:
15:99:90:cc:a0:74:1e:e5:2e:07:3f:50:e6:72:a6:b9:ae:fc:
44:15:eb:81:3d:1a:f8:17:b6:0b:ff:05:76:9d:30:06:40:72:
cf:d5:c4:6f:8b:c9:14:76:09:6b:3d:6a:70:2c:5a:c4:51:92:
e5:cd:84:b6:f9:d9:d5:bc:8d:72:b7:7c:13:9c:41:89:a8:97:
6f:4a:11:5f:8f:b6:c9:b5:df:00:7e:97:20:e7:29:2e:2b:12:
77:dc:e2:63:48:87:42:49:1d:fc:d0:94:a8:8d:18:f9:07:85:

```

e4:d0:3e:9a:4a:d7:d5:d0:02:51:c3:51:1c:73:12:96:2d:75:
22:83:a6:70:5a:4a:2b:f2:98:d9:ae:1b:57:53:3d:3b:58:82:
38:fc:fa:cb:57:43:3f:3e:7e:e0:6d:5b:d6:fc:67:7e:07:7e:
fb:a3:76:43:26:8f:d1:42:d6:a6:33:4e:9e:e0:a0:51:b4:c4:
bc:e3:10:0d:bf:23:6c:4b
WARNING: no nonce in response
Response Verify OK
Certificate-GCP-CVO-20230119-0XXXXX.pem: good
  This Update: Jan 19 15:00:00 2023 GMT
  Next Update: Jan 26 14:59:59 2023 GMT

# Step 1.5 - Optional: Check the response file "response.der" has
been generated. Verify its contents.
$ ls -l
total 64
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der
-rw-r--r--  1 example-user  engr   806 Jan 19 16:51 resp.der

# Step 1.6 - Verify the chain of trust and expiration dates against
the local host
$ openssl version -d
OPENSSLDIR: "/private/etc/ssl"
$ OPENSSLDIR=$(openssl version -d | cut -d '"' -f2)
$ echo $OPENSSLDIR
/private/etc/ssl

$ openssl verify -untrusted <Certificate-Chain.pem> -CApath <OpenSSL
dir> <Certificate.pem>
$ openssl verify -untrusted Certificate-Chain-GCP-CVO-20230119-
0XXXXX.pem -CApath ${OPENSSLDIR} Certificate-GCP-CVO-20230119-
0XXXXX.pem
Certificate-GCP-CVO-20230119-0XXXXX.pem: OK

```

2. Inserire il file disk.raw scaricato, la firma e i certificati in una directory.
3. Estrarre la chiave pubblica dal certificato utilizzando OpenSSL.
4. Decrittare la firma utilizzando la chiave pubblica estratta e verificare il contenuto del file disk.raw scaricato.

Fare clic per visualizzare lo script

```
# Step 1 - Place the downloaded disk.raw, the signature and the
certificates in a directory
$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 2 - Extract the public key from the certificate
$ openssl x509 -pubkey -noout -in (certificate.pem) >
(public_key.pem)
$ openssl x509 -pubkey -noout -in Certificate-GCP-CVO-20230119-
0XXXXX.pem > CVO-GCP-pubkey.pem

$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 17:02 CVO-GCP-pubkey.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 3 - Decrypt the signature using the extracted public key and
verify the contents of the downloaded disk.raw
$ openssl dgst -verify (public_key) -keyform PEM -sha256 -signature
(signed digest) -binary (downloaded or obtained disk.raw)
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary disk.raw
Verified OK

# A failed response would look like this
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary
../sample_file.txt
Verification Failure
```

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.