Architettura

NetApp Solutions

NetApp
April 26, 2024

Sommario

Architettura

Panoramica

Parte dell'affidabilità di una soluzione cloud è la comprensione dell'architettura e del modo in cui è protetta. In questa sezione vengono descritti diversi aspetti dell'architettura Cloud Volumes Service di Google per ridurre i potenziali problemi relativi alla protezione dei dati, nonché le aree in cui potrebbero essere necessarie ulteriori procedure di configurazione per ottenere un'implementazione più sicura.

L'architettura generale di Cloud Volumes Service può essere suddivisa in due componenti principali: Il piano di controllo e il piano dati.

Piano di controllo

Il piano di controllo di Cloud Volumes Service è l'infrastruttura di back-end gestita dagli amministratori Cloud Volumes Service e dal software di automazione nativo NetApp. Questo piano è completamente trasparente per gli utenti finali e include networking, hardware per lo storage, aggiornamenti software e così via per contribuire a fornire valore a una soluzione residente nel cloud come Cloud Volumes Service.

Piano dati

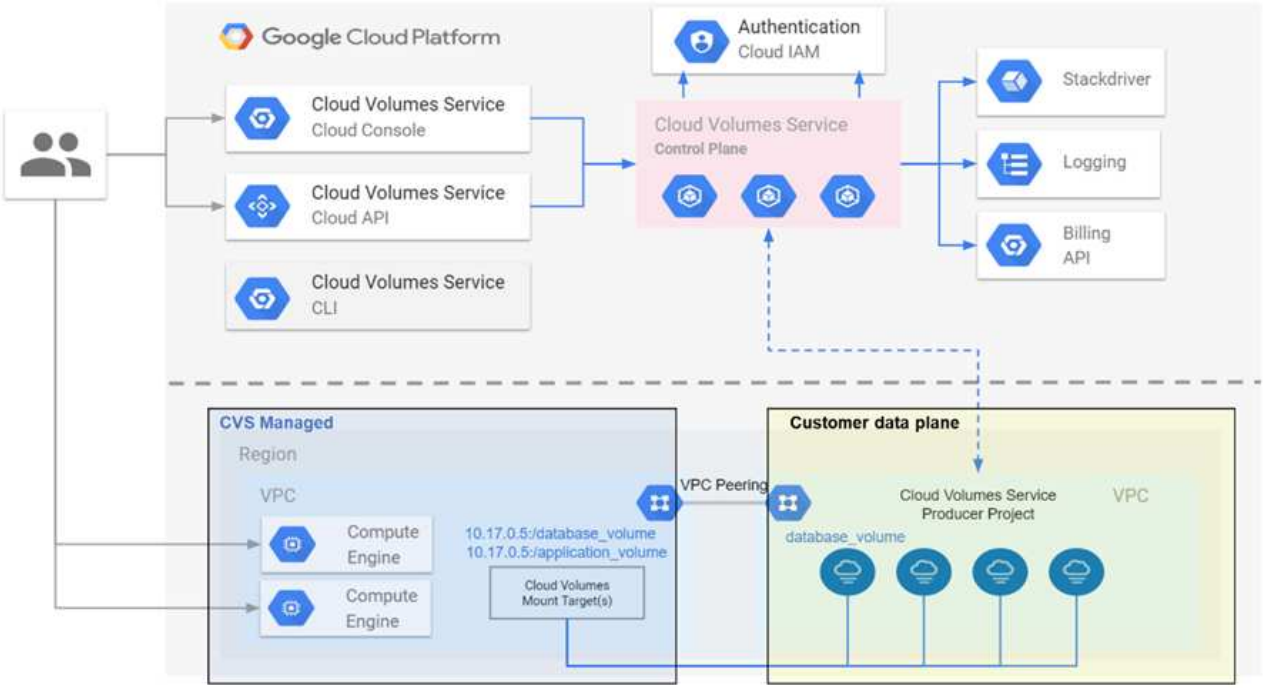
Il piano dati di Cloud Volumes Service include i volumi di dati effettivi e la configurazione generale di Cloud Volumes Service (ad esempio controllo degli accessi, autenticazione Kerberos e così via). Il data plane è interamente sotto il controllo degli utenti finali e dei consumatori della piattaforma Cloud Volumes Service.

Esistono differenze distinte nel modo in cui ciascun piano viene protetto e gestito. Le seguenti sezioni illustrano queste differenze, a partire da una panoramica dell'architettura Cloud Volumes Service.

Architettura Cloud Volumes Service

In modo simile ad altri servizi nativi di Google Cloud come CloudSQL, Google Cloud VMware Engine (GCVE) e FileStore, Cloud Volumes Service utilizza "PSA di Google" per fornire il servizio. In PSA, i servizi sono costruiti all'interno di un progetto di service Producer, che utilizza "Peering della rete VPC" per connettersi al cliente del servizio. Il produttore del servizio viene fornito e gestito da NetApp e il consumatore del servizio è un VPC in un progetto del cliente, che ospita i client che desiderano accedere alle condivisioni di file Cloud Volumes Service.

La figura seguente, a cui si fa riferimento da "sezione architettura" Della documentazione di Cloud Volumes Service, mostra una vista di alto livello.



La parte sopra la linea tratteggiata mostra il piano di controllo del servizio, che controlla il ciclo di vita del volume. La parte sotto la linea tratteggiata mostra il piano dati. La casella blu a sinistra rappresenta l'utente VPC (consumatore di servizi), la casella blu a destra rappresenta il produttore di servizi fornito da NetApp. Entrambi sono connessi tramite peering VPC.

Modello di tenancy

In Cloud Volumes Service, i singoli progetti sono considerati locatari unici. Ciò significa che la manipolazione di volumi, copie Snapshot e così via viene eseguita in base al progetto. In altre parole, tutti i volumi sono di proprietà del progetto in cui sono stati creati e solo quel progetto può gestire e accedere ai dati all'interno di essi per impostazione predefinita. Questa è considerata la vista del piano di controllo del servizio.

VPC condivisi

Nella vista del piano dati, Cloud Volumes Service può connettersi a un VPC condiviso. È possibile creare volumi nel progetto di hosting o in uno dei progetti di servizio connessi al VPC condiviso. Tutti i progetti (host o servizio) connessi a quel VPC condiviso sono in grado di raggiungere i volumi a livello di rete (TCP/IP). Poiché tutti i client con connettività di rete sul VPC condiviso possono potenzialmente accedere ai dati attraverso protocolli NAS, il controllo dell'accesso sul singolo volume (come gli elenchi di controllo dell'accesso utente/gruppo (ACL) e i nomi host/indirizzi IP per le esportazioni NFS) deve essere utilizzato per controllare chi può accedere ai dati.

È possibile collegare Cloud Volumes Service a un massimo di cinque VPC per progetto del cliente. Sul piano di controllo, il progetto consente di gestire tutti i volumi creati, indipendentemente dal VPC a cui sono collegati. Sul piano dati, i VPC sono isolati l'uno dall'altro e ciascun volume può essere collegato solo a un VPC.

L'accesso ai singoli volumi è controllato da meccanismi di controllo degli accessi specifici del protocollo (NFS/SMB).

In altre parole, a livello di rete, tutti i progetti connessi al VPC condiviso sono in grado di vedere il volume, mentre, dal lato di gestione, il piano di controllo consente solo al progetto proprietario di vedere il volume.

Controlli del servizio VPC

I controlli dei servizi VPC stabiliscono un perimetro di controllo degli accessi intorno ai servizi Google Cloud collegati a Internet e accessibili in tutto il mondo. Questi servizi forniscono il controllo degli accessi attraverso le identità degli utenti, ma non possono limitare le richieste di posizione di rete da cui provengono. I controlli dei servizi VPC colmano questa lacuna introducendo le funzionalità per limitare l'accesso a reti definite.

Il piano dati Cloud Volumes Service non è connesso a Internet esterno ma a VPC privati con confini di rete ben definiti (perimetri). All'interno di tale rete, ciascun volume utilizza il controllo degli accessi specifico del protocollo. Qualsiasi connettività di rete esterna viene creata esplicitamente dagli amministratori di progetto di Google Cloud. Il piano di controllo, tuttavia, non fornisce le stesse protezioni del piano dati e può essere utilizzato da chiunque disponga di credenziali valide ("Token JWT").

In breve, il data plane Cloud Volumes Service offre la funzionalità di controllo dell'accesso alla rete, senza il requisito di supportare i controlli dei servizi VPC e non utilizza esplicitamente i controlli dei servizi VPC.

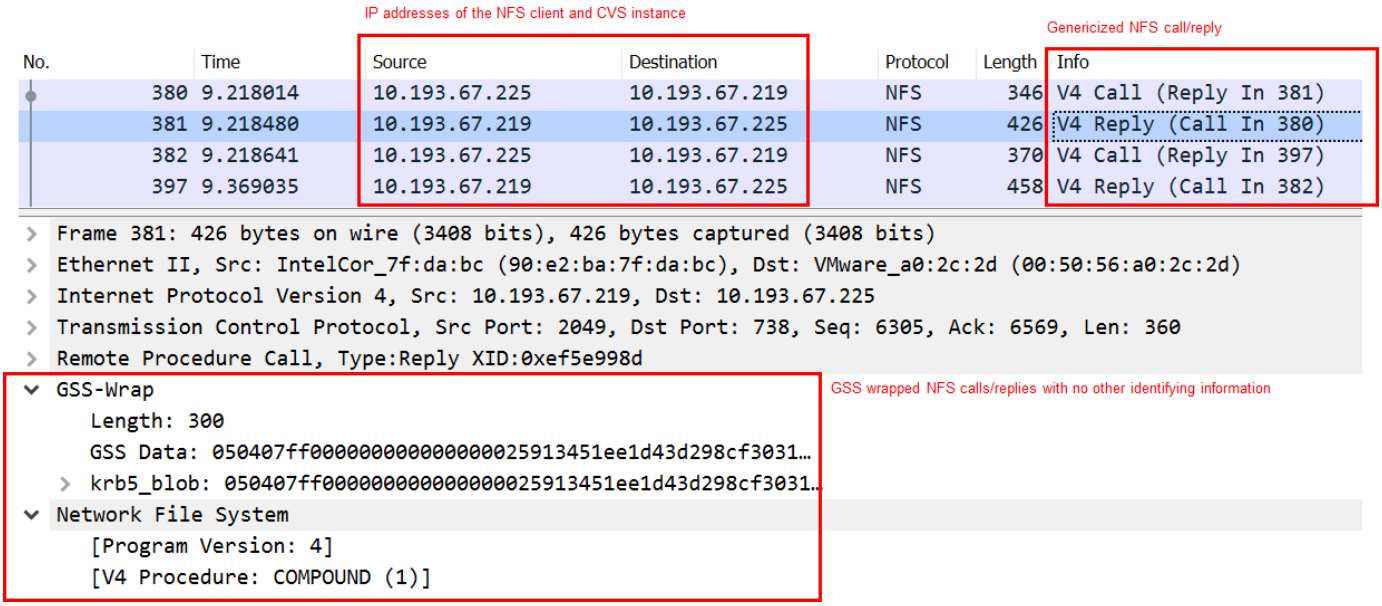
Considerazioni su sniffing/trace dei pacchetti

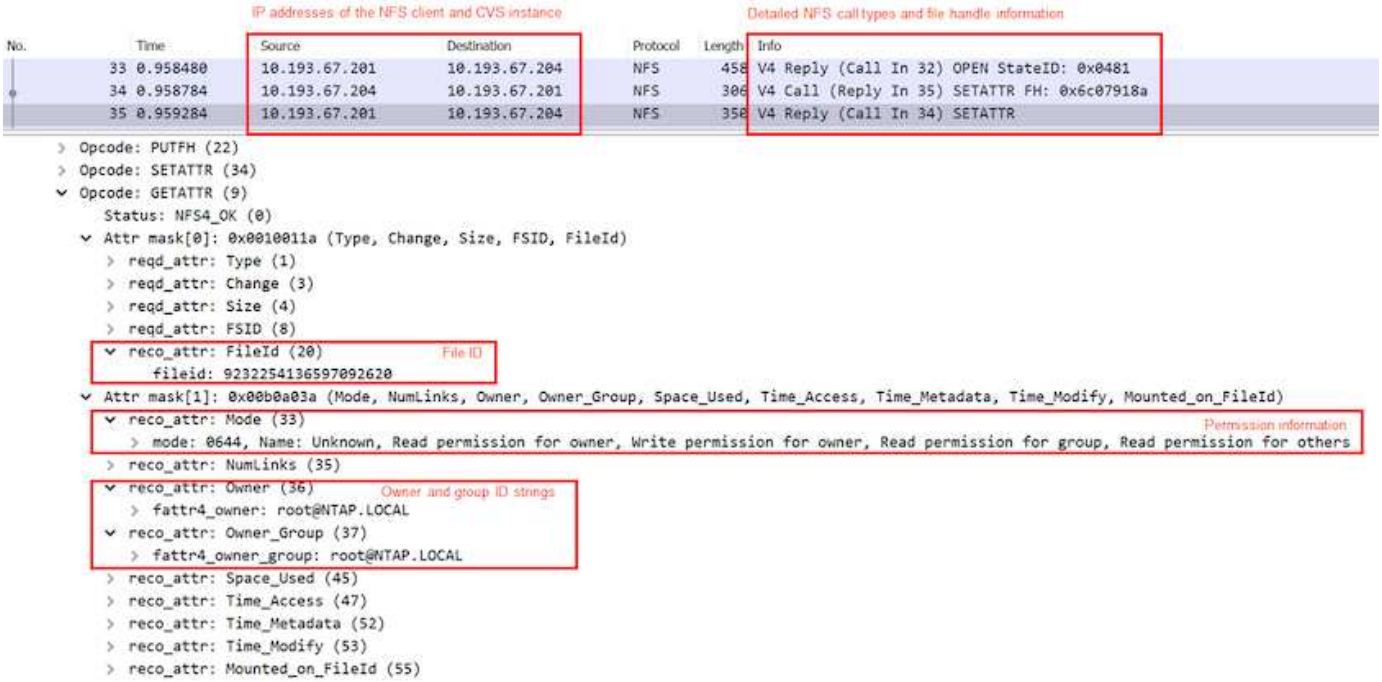
Le acquisizioni di pacchetti possono essere utili per la risoluzione di problemi di rete o di altro tipo (come permessi NAS, connettività LDAP e così via), ma possono anche essere utilizzate in modo malizioso per ottenere informazioni su indirizzi IP di rete, indirizzi MAC, nomi di utenti e gruppi e sul livello di sicurezza utilizzato sugli endpoint. A causa del modo in cui vengono configurate le regole di rete, VPC e firewall di Google Cloud, l'accesso indesiderato ai pacchetti di rete dovrebbe essere difficile da ottenere senza le credenziali di accesso dell'utente o. "Token JWT" nelle istanze cloud. Le acquisizioni di pacchetti sono possibili solo sugli endpoint (ad esempio macchine virtuali) e solo sugli endpoint interni al VPC, a meno che non venga utilizzato un VPC condiviso e/o un tunnel di rete esterno/inoltro IP per consentire esplicitamente il traffico esterno agli endpoint. Non esiste alcun modo per eseguire lo sniff del traffico al di fuori dei client.

Quando si utilizzano VPC condivisi, la crittografia in-flight con NFS Kerberos e/o "Crittografia SMB" può mascherare gran parte delle informazioni raccolte dalle tracce. Tuttavia, parte del traffico viene ancora inviato in formato non crittografato, ad esempio "DNS" e. "Query LDAP". La figura seguente mostra un'acquisizione di pacchetti da una query LDAP non crittografata proveniente da Cloud Volumes Service e le potenziali informazioni di identificazione esposte. Le query LDAP in Cloud Volumes Service attualmente non supportano la crittografia o LDAP su SSL. CVS-Performance supporta la firma LDAP, se richiesto da Active Directory. CVS-SW non supporta la firma LDAP.

UnixUserPassword viene interrogata da LDAP e non viene inviata in testo non crittografato, ma in un hash con salatura. Per impostazione predefinita, Windows LDAP non compila i campi unixUserPassword. Questo campo è necessario solo se è necessario sfruttare Windows LDAP per gli accessi interattivi tramite LDAP ai client. Cloud Volumes Service non supporta gli accessi LDAP interattivi alle istanze.

La figura seguente mostra un'acquisizione di pacchetti da una conversazione Kerberos NFS accanto a un'acquisizione di NFS su AUTH_SYS. Si noti come le informazioni disponibili in una traccia siano diverse tra le due e come l'abilitazione della crittografia in-flight offra una maggiore sicurezza generale per il traffico NAS.





Interfacce di rete delle macchine virtuali

Un trucco che gli autori degli attacchi potrebbero tentare di aggiungere una nuova scheda di interfaccia di rete (NIC) a una macchina virtuale in "modalità promiscua" (Mirroring delle porte) o attivare la modalità promiscua su una scheda di rete esistente per eseguire lo sniff di tutto il traffico. In Google Cloud, l'aggiunta di una nuova NIC richiede l'arresto completo di una macchina virtuale, che crea avvisi, in modo che gli hacker non possano farlo inosservato.

Inoltre, le NIC non possono essere impostate sulla modalità promiscua e attiveranno avvisi in Google Cloud.

Architettura del piano di controllo

Tutte le azioni di gestione di Cloud Volumes Service vengono eseguite tramite API. La gestione Cloud Volumes Service integrata nella console cloud GCP utilizza anche l'API Cloud Volumes Service.

Gestione di identità e accessi

Gestione di identità e accessi ("IAM") È un servizio standard che consente di controllare l'autenticazione (accessi) e l'autorizzazione (autorizzazioni) per le istanze di progetto di Google Cloud. Google IAM offre un audit trail completo delle autorizzazioni di autorizzazione e rimozione. Attualmente Cloud Volumes Service non fornisce il controllo del piano di controllo.

Panoramica delle autorizzazioni

IAM offre permessi granulari integrati per Cloud Volumes Service. È possibile trovare un "completa l'elenco delle autorizzazioni granulari qui".

IAM offre anche due ruoli predefiniti chiamati `netappcloudvolumes.admin` e. `netappcloudvolumes.viewer`. Questi ruoli possono essere assegnati a specifici utenti o account di servizio.

Assegnare ruoli e autorizzazioni appropriati per consentire agli utenti IAM di gestire Cloud Volumes Service.

Di seguito sono riportati alcuni esempi di utilizzo delle autorizzazioni granulari:

- Creare un ruolo personalizzato con solo autorizzazioni Get/List/create/Update in modo che gli utenti non possano eliminare i volumi.
- Utilizzare un ruolo personalizzato solo con `snapshot.*` Autorizzazioni per creare un account di servizio utilizzato per creare un'integrazione Snapshot coerente con l'applicazione.
- Creare un ruolo personalizzato da delegare `volumereplication.*` a utenti specifici.

Account di servizio

Per effettuare chiamate API Cloud Volumes Service tramite script o. "Terraform", è necessario creare un account di servizio con `roles/netappcloudvolumes.admin` ruolo. È possibile utilizzare questo account di servizio per generare i token JWT necessari per autenticare le richieste API Cloud Volumes Service in due modi diversi:

- Generare una chiave JSON e utilizzare le API di Google per derivare un token JWT da essa. Questo è l'approccio più semplice, ma implica la gestione manuale dei segreti (la chiave JSON).
- Utilizzare "Rappresentazione dell'account di servizio" con `roles/iam.serviceAccountTokenCreator`. Il codice (script, Terraform e così via). funziona con "Credenziali predefinite dell'applicazione" e rappresenta l'account del servizio per ottenere le autorizzazioni. Questo approccio riflette le Best practice di sicurezza di Google.

Vedere "Creazione dell'account di servizio e della chiave privata" Nella documentazione di Google Cloud per ulteriori informazioni.

API Cloud Volumes Service

L'API Cloud Volumes Service utilizza un'API basata SU REST utilizzando HTTPS (TLSv1.2) come trasporto di rete sottostante. È possibile trovare la definizione API più recente "qui" E informazioni su come utilizzare l'API all'indirizzo "Cloud Volumes API nella documentazione cloud di Google".

L'endpoint API viene gestito e protetto da NetApp utilizzando la funzionalità HTTPS standard (TLSv1.2).

Token JWT

L'autenticazione all'API viene eseguita con token bearer JWT ("RFC-7519"). I token JWT validi devono essere ottenuti utilizzando l'autenticazione IAM di Google Cloud. A tale scopo, è necessario recuperare un token da IAM fornendo una chiave JSON dell'account di servizio.

Registrazione dell'audit

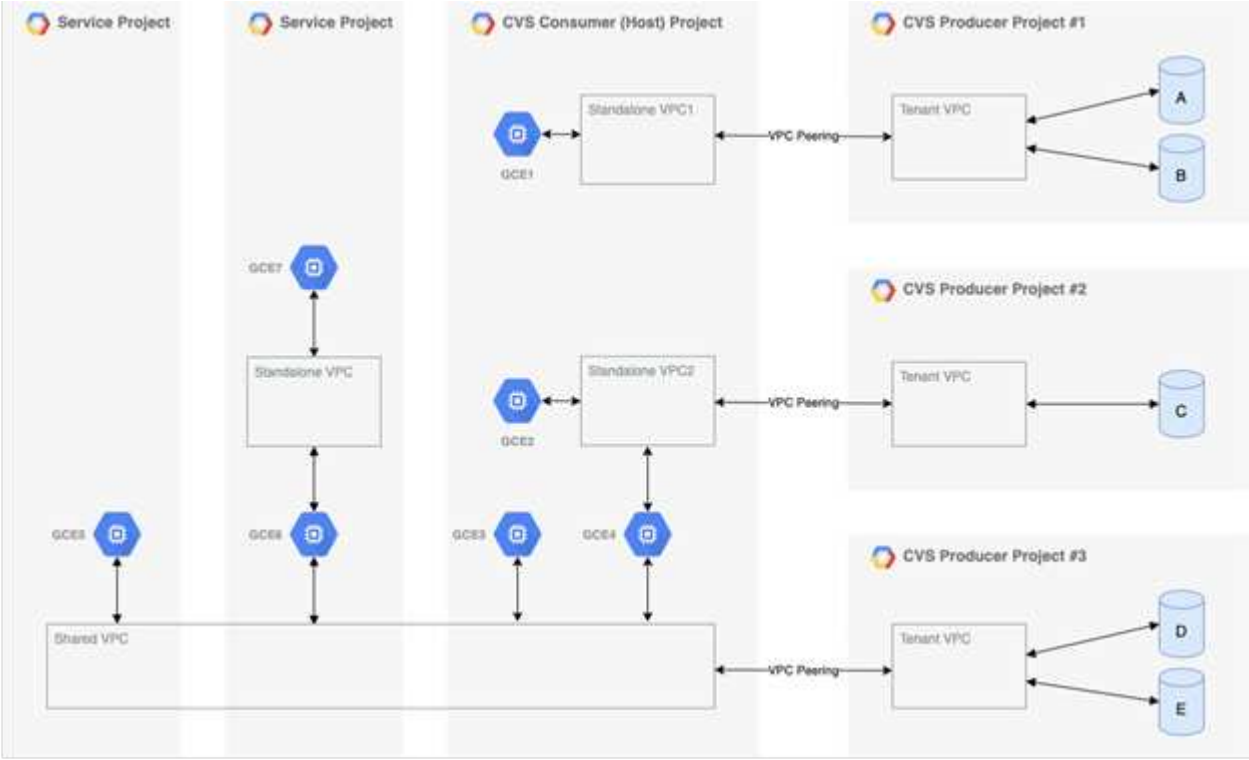
Attualmente, non sono disponibili registri di audit del piano di controllo accessibili dall'utente.

Architettura del data plane

Cloud Volumes Service per Google Cloud sfrutta Google Cloud "accesso ai servizi privati" framework. In questo framework, gli utenti possono connettersi a Cloud Volumes Service. Questo framework utilizza i costrutti di peering di Service Networking e VPC come altri servizi Google Cloud, garantendo un isolamento completo tra i tenant.

Per una panoramica dell'architettura di Cloud Volumes Service per Google Cloud, consulta "Architettura per Cloud Volumes Service".

Le VPC degli utenti (standalone o condiviso) vengono collegate ai VPC all'interno dei progetti di tenant gestiti da Cloud Volumes Service, che ospitano i volumi.



La figura precedente mostra un progetto (il progetto consumer CVS al centro) con tre reti VPC collegate a Cloud Volumes Service e più macchine virtuali del motore di calcolo (GCE1-7) che condividono volumi:

- VPC1 consente a GCE1 di accedere ai volumi A e B.
- VPC2 consente a GCE2 e GCE4 di accedere al volume C.
- La terza rete VPC è un VPC condiviso, condiviso con due progetti di servizio. Consente a GCE3, GCE4, GCE5 e GCE6 di accedere ai volumi D ed E. Le reti VPC condivise sono supportate solo per volumi del tipo di servizio CVS-Performance.

GCE7 non può accedere ad alcun volume.

I dati possono essere crittografati sia in transito (utilizzando la crittografia Kerberos e/o SMB) che a riposo in Cloud Volumes Service.

Crittografia dei dati in transito

I dati in transito possono essere crittografati a livello di protocollo NAS e la rete Google Cloud stessa viene crittografata, come descritto nelle sezioni seguenti.

Rete Google Cloud

Google Cloud crittografa il traffico a livello di rete come descritto in "Crittografia in transito" Nella documentazione di Google. Come indicato nella sezione "architettura dei servizi cloud Volumes", Cloud

Volumes Service viene fornito da un progetto di produttore PSA controllato da NetApp.

Nel caso di CVS-SW, il tenant produttore esegue Google VM per fornire il servizio. Il traffico tra le macchine virtuali dell'utente e le macchine virtuali Cloud Volumes Service viene crittografato automaticamente da Google.

Sebbene il percorso dei dati per CVS-Performance non sia completamente crittografato sul layer di rete, NetApp e Google utilizzano una combinazione "Di crittografia IEEE 802.1AE (MACsec)", "incapsulamento" (Crittografia dei dati) e reti con restrizioni fisiche per proteggere i dati in transito tra il tipo di servizio CVS-Performance di Cloud Volumes Service e Google Cloud.

Protocolli NAS

I protocolli NAS NFS e SMB forniscono una crittografia opzionale per il trasporto a livello di protocollo.

Crittografia SMB

"Crittografia SMB" Fornisce la crittografia end-to-end dei dati SMB e protegge i dati da eventi di intercettazione su reti non attendibili. È possibile attivare la crittografia sia per la connessione dati client/server (disponibile solo per i client compatibili con SMB3.x) che per l'autenticazione del server/controller di dominio.

Quando la crittografia SMB è attivata, i client che non supportano la crittografia non possono accedere alla condivisione.

Cloud Volumes Service supporta le crittografie di sicurezza RC4-HMAC, AES-128-CTS-HMAC-SHA1 e AES-256-CTS-HMAC-SHA1 per la crittografia SMB. SMB negozia con il tipo di crittografia più elevato supportato dal server.

NFSv4.1 Kerberos

Per NFSv4.1, CVS-Performance offre l'autenticazione Kerberos come descritto in "RFC7530". È possibile attivare Kerberos in base al volume.

Il tipo di crittografia attualmente più potente disponibile per Kerberos è AES-256-CTS-HMAC-SHA1. NetApp Cloud Volumes Service supporta AES-256-CTS-HMAC-SHA1, AES-128-CTS-HMAC-SHA1, DES3 e DES per NFS. Supporta anche ARCFOUR-HMAC (RC4) per il traffico CIFS/SMB, ma non per NFS.

Kerberos offre tre diversi livelli di sicurezza per i montaggi NFS, che offrono la possibilità di scegliere il livello di sicurezza Kerberos.

Come da RedHat "Opzioni di montaggio comuni" documentazione:

```
sec=krb5 uses Kerberos V5 instead of local UNIX UIDs and GIDs to
authenticate users.
sec=krb5i uses Kerberos V5 for user authentication and performs integrity
checking of NFS operations using secure checksums to prevent data
tampering.
sec=krb5p uses Kerberos V5 for user authentication, integrity checking,
and encrypts NFS traffic to prevent traffic sniffing. This is the most
secure setting, but it also involves the most performance overhead.
```

Di norma, più il livello di sicurezza Kerberos deve essere elevato, più le performance sono peggiori, in quanto

client e server trascorrono del tempo a crittografare e decrittare le operazioni NFS per ogni pacchetto inviato. Molti client e server NFS supportano l'offload AES-NI sulle CPU per un'esperienza generale migliore, ma l'impatto delle performance di Kerberos 5p (crittografia completa end-to-end) è significativamente maggiore dell'impatto di Kerberos 5 (autenticazione dell'utente).

La seguente tabella mostra le differenze in termini di sicurezza e performance di ciascun livello.

Livello di sicurezza	Sicurezza	Performance
NFSv3: SIS	• Meno sicuro; testo normale con ID utente/ID gruppo numerici • In grado di visualizzare UID, GID, indirizzi IP client, percorsi di esportazione, nomi file, permessi nelle acquisizioni di pacchetti	• Ideale per la maggior parte dei casi
NFSv4.x: SIS	• Più sicuro di NFSv3 (ID client, corrispondenza stringa nome/stringa di dominio) ma ancora testo normale • Possibilità di visualizzare UID, GID, indirizzi IP client, stringhe di nomi, ID di dominio, percorsi di esportazione, nomi di file, permessi nelle acquisizioni di pacchetti	• Ideale per carichi di lavoro sequenziali (come macchine virtuali, database, file di grandi dimensioni) • Cattivo con elevato numero di file/metadati elevati (30-50% peggiore)

Livello di sicurezza	Sicurezza	Performance
NFS: Krb5	• Crittografia Kerberos per le credenziali in ogni pacchetto NFS: Esegue il wrapping di UID/GID di utenti/gruppi nelle chiamate RPC nel wrapper GSS • L'utente che richiede l'accesso al montaggio deve disporre di un ticket Kerberos valido (tramite nome utente/password o scambio manuale della scheda della chiave); il ticket scade dopo un periodo di tempo specificato e l'utente deve eseguire nuovamente l'autenticazione per l'accesso • Nessuna crittografia per le operazioni NFS o i protocolli ausiliari come mount/portmapper/nlm (possono vedere percorsi di esportazione, indirizzi IP, handle di file, permessi, nomi di file, atime/mtime in pacchetti capture)	• Migliore nella maggior parte dei casi per Kerberos; peggiore di AUTH_SYS

Livello di sicurezza	Sicurezza	Performance
NFS: Krb5i	• Crittografia Kerberos per le credenziali in ogni pacchetto NFS: Esegue il wrapping di UID/GID di utenti/gruppi nelle chiamate RPC nel wrapper GSS • L'utente che richiede l'accesso al montaggio deve disporre di un ticket Kerberos valido (tramite nome utente/password o scambio manuale della scheda delle chiavi); il ticket scade dopo un periodo di tempo specificato e l'utente deve eseguire nuovamente l'autenticazione per l'accesso • Nessuna crittografia per le operazioni NFS o i protocolli ausiliari come mount/portmapper/nlm (possono vedere percorsi di esportazione, indirizzi IP, handle di file, permessi, nomi di file, atime/mtime in pacchetti capture) • Il checksum GSS Kerberos viene aggiunto a ogni pacchetto per garantire che nulla intercetti i pacchetti. Se i checksum corrispondono, è consentita la conversazione.	• Meglio di krb5p perché il payload NFS non è crittografato; solo l'overhead aggiunto rispetto a krb5 è il checksum di integrità. Le performance di krb5i non saranno molto peggiori di krb5, ma si verificherà un certo degrado.

Livello di sicurezza	Sicurezza	Performance
NFS: Krb5p	• Crittografia Kerberos per le credenziali in ogni pacchetto NFS: Esegue il wrapping di UID/GID di utenti/gruppi nelle chiamate RPC nel wrapper GSS • L'utente che richiede l'accesso al montaggio deve disporre di un ticket Kerberos valido (tramite nome utente/password o scambio manuale di keytab); il ticket scade dopo il periodo di tempo specificato e l'utente deve eseguire nuovamente l'autenticazione per l'accesso • Tutti i payload dei pacchetti NFS sono crittografati con il wrapper GSS (non è possibile visualizzare handle di file, permessi, nomi di file, atime/mtime nelle acquisizioni di pacchetti). • Include il controllo dell'integrità. • Il tipo di operazione NFS è visibile (FSINFO, ACCESS, GETATTR e così via). • I protocolli ausiliari (mount, portmap, nlm e così via) non sono crittografati (possono vedere percorsi di esportazione, indirizzi IP)	• Performance peggiori dei livelli di sicurezza; krb5p deve crittografare/decrittare di più. • Performance migliori rispetto a krb5p con NFSv4.x per carichi di lavoro con elevato numero di file.

In Cloud Volumes Service, un server Active Directory configurato viene utilizzato come server Kerberos e server LDAP (per cercare le identità degli utenti da uno schema compatibile con RFC2307). Non sono supportati altri server Kerberos o LDAP. NetApp consiglia vivamente di utilizzare LDAP per la gestione delle identità in Cloud Volumes Service. Per informazioni su come NFS Kerberos viene mostrato nelle acquisizioni di pacchetti, consulta la sezione ""Considerazioni su sniffing/traccia dei pacchetti"."

Crittografia dei dati a riposo

Tutti i volumi in Cloud Volumes Service sono crittografati a riposo utilizzando la crittografia AES-256, il che significa che tutti i dati utente scritti sui supporti sono crittografati e possono essere decifrati solo con una chiave per volume.

- Per CVS-SW, vengono utilizzate chiavi generate da Google.
- Per CVS-Performance, i tasti per volume sono memorizzati in un gestore di chiavi integrato in Cloud Volumes Service.

A partire da novembre 2021, è stata resa disponibile l'anteprima delle chiavi di crittografia gestite dal cliente (CMEK). In questo modo è possibile crittografare le chiavi per volume con una chiave master per progetto, per regione, ospitata in "Google Key Management Service (KMS)." KMS consente di collegare i key manager esterni.

Per informazioni sulla configurazione di KMS per CVS-Performance, vedere "Impostazione delle chiavi di crittografia gestite dal cliente".

Firewall

Cloud Volumes Service espone più porte TCP per le condivisioni NFS e SMB:

- "Porte richieste per l'accesso NFS"
- "Porte richieste per l'accesso SMB"

Inoltre, le configurazioni SMB, NFS con LDAP, incluso Kerberos, e a doppio protocollo richiedono l'accesso a un dominio Active Directory di Windows. Le connessioni di Active Directory devono essere "configurato" in base all'area geografica. I controller di dominio Active Directory vengono identificati tramite "Rilevamento DC basato su DNS" Utilizzando i server DNS specificati. Vengono utilizzati tutti i controller di dominio restituiti. L'elenco dei controller di dominio idonei può essere limitato specificando un sito Active Directory.

Cloud Volumes Service raggiunge gli indirizzi IP dell'intervallo CIDR allocati con `gcloud compute address` comando mentre "A bordo del Cloud Volumes Service". È possibile utilizzare questo CIDR come indirizzi di origine per configurare i firewall in entrata nei controller di dominio Active Directory.

I controller di dominio Active Directory devono "Esporre le porte ai CIDR Cloud Volumes Service come indicato qui".