



NetApp per GCP/GCVE

NetApp Solutions

NetApp
April 26, 2024

Sommario

- Multicloud ibrido NetApp con soluzioni VMware 1
 - Protezione dei carichi di lavoro su GCP/GCVE 1
 - Migrazione dei carichi di lavoro su GCP/GCVE 8
 - Disponibilità regionale: Datastore NFS supplementare per Google Cloud Platform (GCP) 28
 - Panoramica sulla sicurezza - NetApp Cloud Volumes Service (CVS) in Google Cloud 30

Multicloud ibrido NetApp con soluzioni VMware

Protezione dei carichi di lavoro su GCP/GCVE

Disaster recovery coerente con l'applicazione con replica NetApp SnapCenter e Veeam

Autori: Suresh Thoppay, NetApp

Panoramica

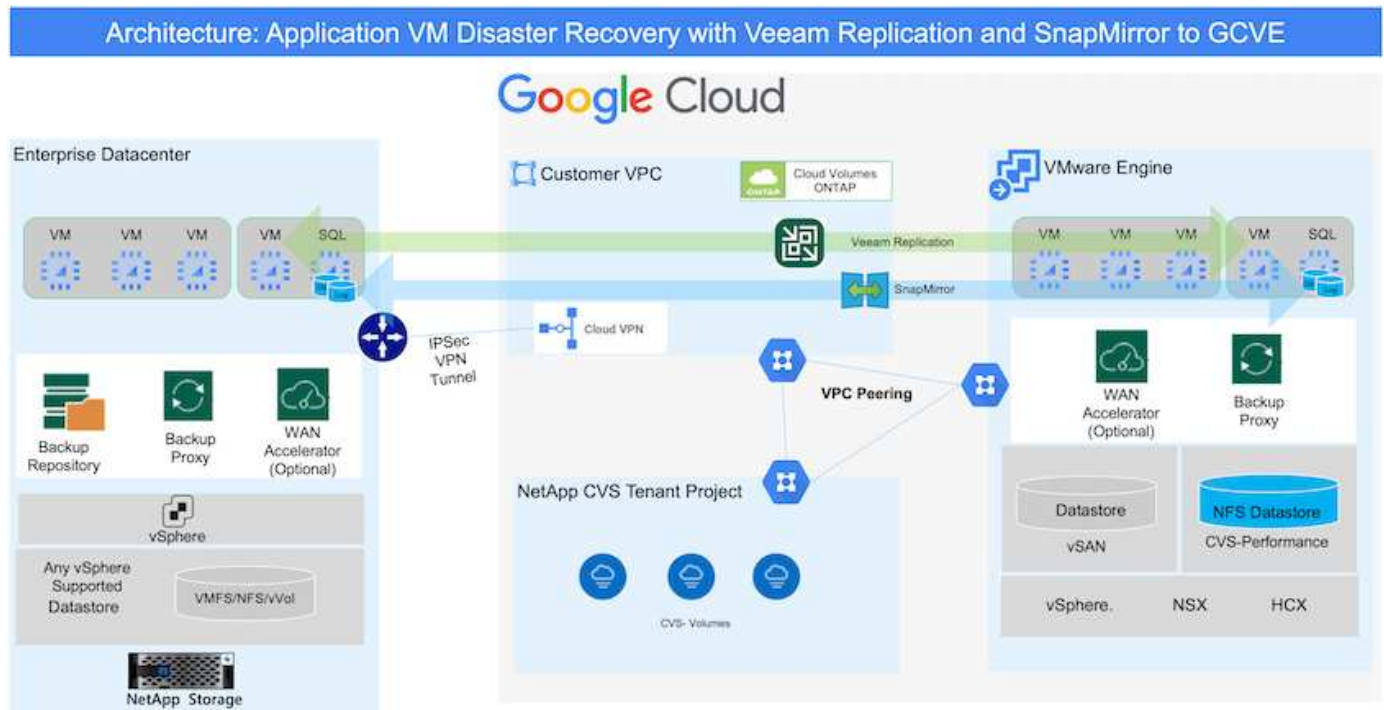
Molti clienti cercano una soluzione di disaster recovery efficace per le loro macchine virtuali applicative ospitate su VMware vSphere. Molti di loro utilizzano la soluzione di backup esistente per eseguire il recovery durante il disaster.

Molte volte questa soluzione aumenta l'RTO e non soddisfa le loro aspettative. Per ridurre l'RPO e l'RTO, la replica delle macchine virtuali Veeam può essere utilizzata anche da on-premise a GCVE, purché siano disponibili connettività di rete e ambiente con autorizzazioni appropriate.

NOTA: Veeam VM Replication non protegge i dispositivi storage connessi guest delle VM, come i supporti iSCSI o NFS, all'interno della VM guest. Necessità di proteggerli separatamente.

Per una replica coerente delle applicazioni per SQL VM e per ridurre l'RTO, abbiamo utilizzato SnapCenter per orchestrare le operazioni di snapmirror dei volumi di log e del database SQL.

Questo documento fornisce un approccio passo per passo per la configurazione e l'esecuzione del disaster recovery che utilizza NetApp SnapMirror, Veeam e Google Cloud VMware Engine (GCVE).



Presupposti

Questo documento si concentra sullo storage in-guest per i dati delle applicazioni (noto anche come guest Connected) e si presume che l'ambiente on-premise stia utilizzando SnapCenter per backup coerenti con le applicazioni.



Questo documento si riferisce a qualsiasi soluzione di backup o ripristino di terze parti. A seconda della soluzione utilizzata nell'ambiente, seguire le Best practice per creare policy di backup che soddisfino gli SLA dell'organizzazione.

Per la connettività tra l'ambiente on-premise e la rete Google Cloud, utilizza le opzioni di connettività come l'interconnessione dedicata o la VPN cloud. I segmenti devono essere creati in base alla progettazione della VLAN on-premise.



Esistono diverse opzioni per connettere i data center on-premise a Google Cloud, che ci impediscono di delineare un workflow specifico in questo documento. Fare riferimento alla documentazione di Google Cloud per il metodo di connettività on-premise-to-Google appropriato.

Implementazione della soluzione DR

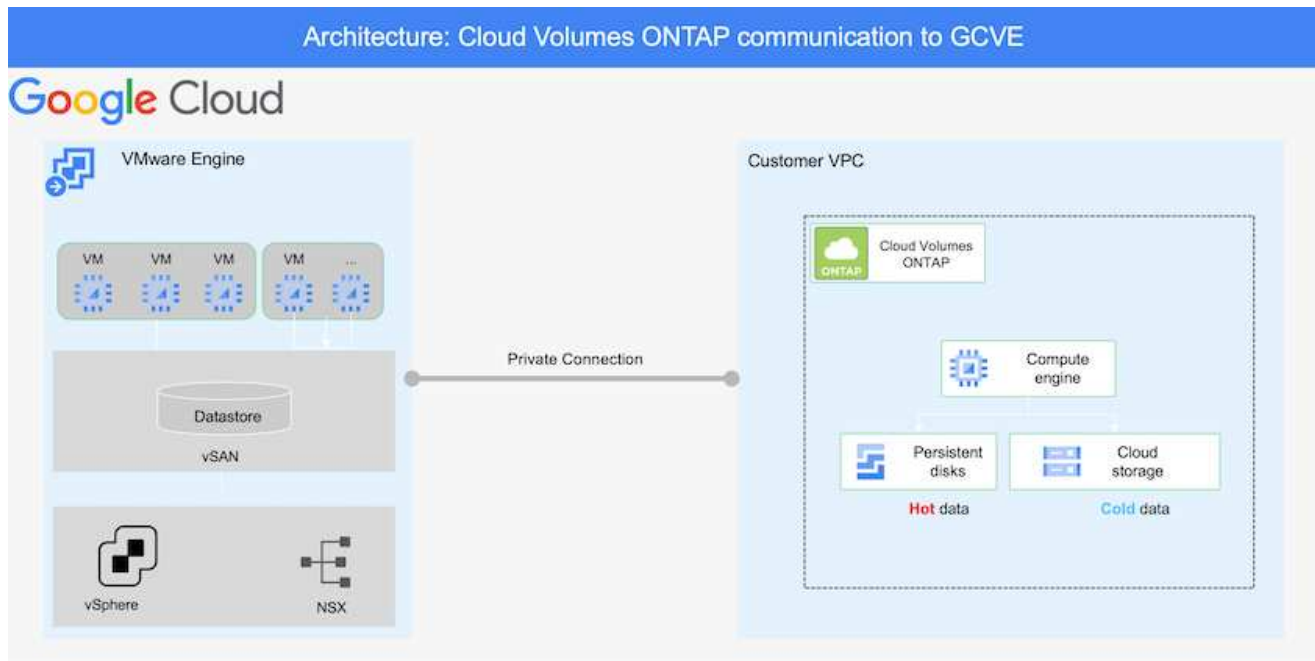
Panoramica sull'implementazione della soluzione

1. Assicurarsi che il backup dei dati dell'applicazione venga eseguito utilizzando SnapCenter con i requisiti RPO necessari.
2. Eseguire il provisioning di Cloud Volumes ONTAP con la dimensione dell'istanza corretta utilizzando BlueXP all'interno dell'abbonamento appropriato e della rete virtuale.
 - a. Configurare SnapMirror per i volumi applicativi rilevanti.
 - b. Aggiornare i criteri di backup in SnapCenter per attivare gli aggiornamenti di SnapMirror dopo i processi pianificati.
3. Installare il software Veeam e avviare la replica delle macchine virtuali sull'istanza di Google Cloud VMware Engine.
4. Durante un evento di emergenza, interrompere la relazione SnapMirror utilizzando BlueXP e attivare il failover delle macchine virtuali con Veeam.
 - a. Ricollegare i LUN iSCSI e i montaggi NFS per le macchine virtuali dell'applicazione.
 - b. Visualizzare le applicazioni online.
5. Richiamare il failback sul sito protetto risyncing inverso di SnapMirror dopo il ripristino del sito primario.

Dettagli sull'implementazione

Configurare CVO su Google Cloud e replicare i volumi su CVO

Il primo passo è configurare Cloud Volumes ONTAP su Google Cloud ("cvo") E replicare i volumi desiderati su Cloud Volumes ONTAP con le frequenze desiderate e le ritenzioni di snapshot.



Per istruzioni dettagliate di esempio sull'impostazione di SnapCenter e la replica dei dati, fare riferimento a. ["Configurazione della replica con SnapCenter"](#)

[Analisi della protezione di SQL VM con SnapCenter](#)

Configurare gli host GCVE e l'accesso ai dati CVO

Due fattori importanti da prendere in considerazione durante l'implementazione di SDDC sono le dimensioni del cluster SDDC nella soluzione GCVE e il tempo necessario per mantenere SDDC in servizio. Queste due considerazioni chiave per una soluzione di disaster recovery contribuiscono a ridurre i costi operativi complessivi. Il controller SDDC può contenere fino a tre host, fino a un cluster multi-host in un'implementazione su larga scala.

Il servizio di volume cloud di NetApp per datastore NFS e Cloud Volumes ONTAP per database SQL e log possono essere implementati su qualsiasi VPC e deve disporre di una connessione privata a tale VPC per montare datastore NFS e connettere le macchine virtuali a LUN iSCSI.

Per configurare GCVE SDDC, vedere ["Implementare e configurare l'ambiente di virtualizzazione su Google Cloud Platform \(GCP\)"](#). Come prerequisito, verificare che le macchine virtuali guest che risiedono sugli host GCVE siano in grado di utilizzare i dati da Cloud Volumes ONTAP dopo aver stabilito la connettività.

Dopo aver configurato correttamente Cloud Volumes ONTAP e GCVE, iniziare a configurare Veeam per automatizzare il ripristino dei carichi di lavoro on-premise su GCVE (macchine virtuali con VMDK delle applicazioni e macchine virtuali con storage in-guest) utilizzando la funzione di replica Veeam e sfruttando SnapMirror per le copie dei volumi delle applicazioni su Cloud Volumes ONTAP.

Installare i componenti Veeam

In base allo scenario di implementazione, il server di backup Veeam, il repository di backup e il proxy di backup che devono essere implementati. In questo caso di utilizzo, non è necessario implementare l'archivio di oggetti per Veeam e il repository scale-out.

["Fare riferimento alla documentazione Veeam per la procedura di installazione"](#)

Per ulteriori informazioni, fare riferimento a. ["Migrazione con Replica Veeam"](#)

Configurazione della replica delle macchine virtuali con Veeam

VMware on-premise e gCUE vCenter devono essere registrati con Veeam. ["Processo di replica di vSphere VM"](#) Nella fase di elaborazione guest della procedura guidata, selezionare Disable application processing (Disattiva elaborazione applicazioni), in quanto verrà utilizzato SnapCenter per il backup e il ripristino consapevoli dell'applicazione.

<https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=8b7e4a9b-7de1-4d48-a8e2-b01200f00692>

Failover di Microsoft SQL Server VM

<https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=9762dc99-081b-41a2-ac68-b01200f00ac0>

Vantaggi di questa soluzione

- Utilizza la replica efficiente e resiliente di SnapMirror.
- Effettua il ripristino in qualsiasi punto disponibile in tempo con la conservazione delle snapshot di ONTAP.
- È disponibile un'automazione completa per tutte le fasi necessarie per il ripristino di centinaia o migliaia di macchine virtuali, dalle fasi di convalida di storage, calcolo, rete e applicazioni.
- SnapCenter utilizza meccanismi di cloning che non modificano il volume replicato.
 - In questo modo si evita il rischio di corruzione dei dati per volumi e snapshot.
 - Evita le interruzioni di replica durante i flussi di lavoro dei test di DR.
 - Sfrutta i dati di DR per flussi di lavoro oltre il DR, come sviluppo/test, test di sicurezza, test di patch e upgrade e test di correzione.
- La replica Veeam consente di modificare gli indirizzi IP delle macchine virtuali sul sito DR.

Disaster recovery applicativo con replica SnapCenter, Cloud Volumes ONTAP e Veeam

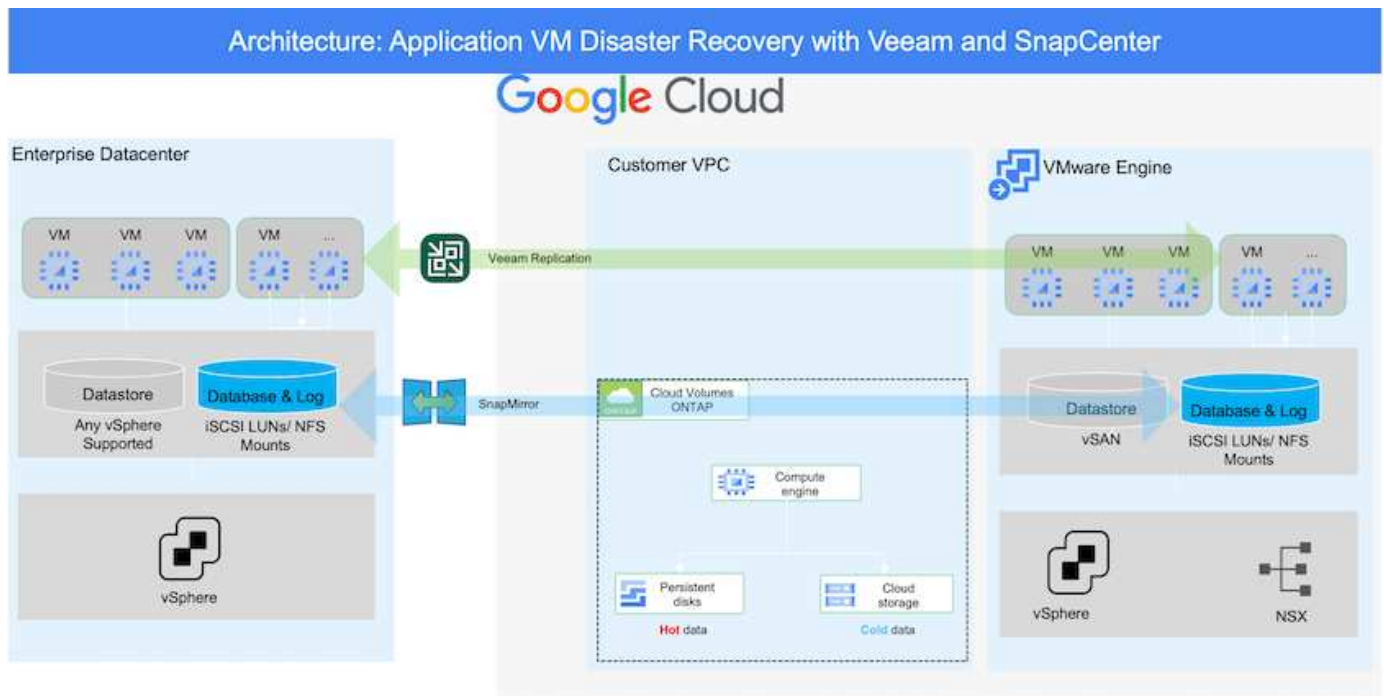
Autori: Suresh Thoppay, NetApp

Panoramica

Il disaster recovery nel cloud è un metodo resiliente e conveniente per proteggere i workload da interruzioni del sito e eventi di corruzione dei dati come ransomware. Con NetApp SnapMirror, è possibile replicare i workload VMware on-premise che utilizzano lo storage connesso agli ospiti su NetApp Cloud Volumes ONTAP in esecuzione su Google Cloud. Ciò riguarda i dati delle applicazioni, ma le macchine virtuali effettive. Il disaster

recovery dovrebbe coprire tutti i componenti dipendenti, tra cui macchine virtuali, VMDK, dati applicativi e altro ancora. A tale scopo, SnapMirror e Veeam possono essere utilizzati per ripristinare perfettamente i carichi di lavoro replicati da on-premise a Cloud Volumes ONTAP utilizzando lo storage vSAN per VM VMDK.

Questo documento fornisce un approccio passo per passo per la configurazione e l'esecuzione del disaster recovery che utilizza NetApp SnapMirror, Veeam e Google Cloud VMware Engine (GCVE).



Presupposti

Questo documento si concentra sullo storage in-guest per i dati delle applicazioni (noto anche come guest Connected) e si presume che l'ambiente on-premise stia utilizzando SnapCenter per backup coerenti con le applicazioni.



Questo documento si riferisce a qualsiasi soluzione di backup o ripristino di terze parti. A seconda della soluzione utilizzata nell'ambiente, seguire le Best practice per creare policy di backup che soddisfino gli SLA dell'organizzazione.

Per la connettività tra l'ambiente on-premise e la rete Google Cloud, utilizza le opzioni di connettività come l'interconnessione dedicata o la VPN cloud. I segmenti devono essere creati in base alla progettazione della VLAN on-premise.



Esistono diverse opzioni per connettere i data center on-premise a Google Cloud, che ci impediscono di delineare un workflow specifico in questo documento. Fare riferimento alla documentazione di Google Cloud per il metodo di connettività on-premise-to-Google appropriato.

Implementazione della soluzione DR

Panoramica sull'implementazione della soluzione

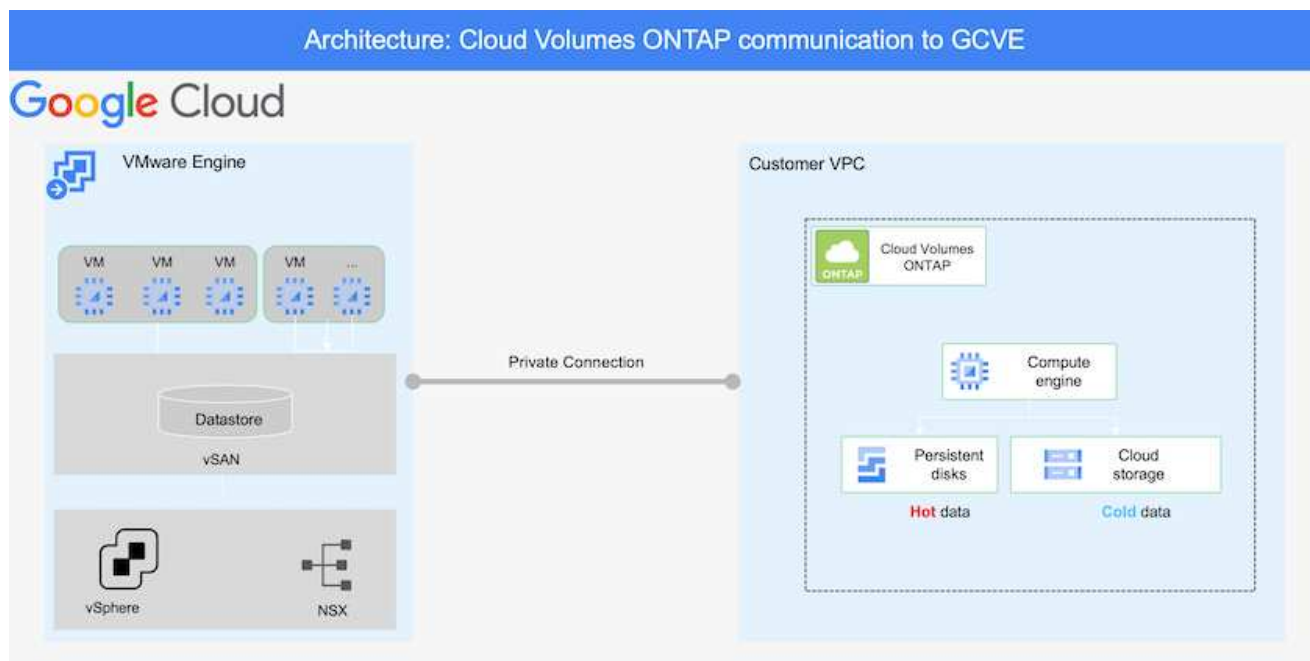
1. Assicurarsi che il backup dei dati dell'applicazione venga eseguito utilizzando SnapCenter con i requisiti RPO necessari.

2. Eseguire il provisioning di Cloud Volumes ONTAP con la dimensione dell'istanza corretta utilizzando Cloud Manager all'interno dell'abbonamento appropriato e della rete virtuale.
 - a. Configurare SnapMirror per i volumi applicativi rilevanti.
 - b. Aggiornare i criteri di backup in SnapCenter per attivare gli aggiornamenti di SnapMirror dopo i processi pianificati.
3. Installare il software Veeam e avviare la replica delle macchine virtuali sull'istanza di Google Cloud VMware Engine.
4. Durante un evento di disastro, interrompere la relazione SnapMirror utilizzando Cloud Manager e attivare il failover delle macchine virtuali con Veeam.
 - a. Ricollegare I LUN ISCSI e i montaggi NFS per le macchine virtuali dell'applicazione.
 - b. Visualizzare le applicazioni online.
5. Richiamare il failback sul sito protetto risyncing inverso di SnapMirror dopo il ripristino del sito primario.

Dettagli sull'implementazione

Configurare CVO su Google Cloud e replicare i volumi su CVO

Il primo passo è configurare Cloud Volumes ONTAP su Google Cloud ("cvo") E replicare i volumi desiderati su Cloud Volumes ONTAP con le frequenze desiderate e le ritenzioni di snapshot.



Per istruzioni dettagliate di esempio sull'impostazione di SnapCenter e la replica dei dati, fare riferimento a. ["Configurazione della replica con SnapCenter"](#)

[Configurazione della replica con SnapCenter](#)

Configurare gli host GCVE e l'accesso ai dati CVO

Due fattori importanti da prendere in considerazione durante l'implementazione di SDDC sono le dimensioni del cluster SDDC nella soluzione GCVE e il tempo necessario per mantenere SDDC in servizio. Queste due considerazioni chiave per una soluzione di disaster recovery contribuiscono a ridurre i costi operativi complessivi. Il controller SDDC può contenere fino a tre host, fino a un cluster multi-host in un'implementazione su larga scala.

Cloud Volumes ONTAP può essere implementato su qualsiasi VPC e deve disporre di una connessione privata a tale VPC per consentire la connessione della macchina virtuale alle LUN iSCSI.

Per configurare GCVE SDDC, vedere ["Implementare e configurare l'ambiente di virtualizzazione su Google Cloud Platform \(GCP\)"](#). Come prerequisito, verificare che le macchine virtuali guest che risiedono sugli host GCVE siano in grado di utilizzare i dati da Cloud Volumes ONTAP dopo aver stabilito la connettività.

Dopo aver configurato correttamente Cloud Volumes ONTAP e GCVE, iniziare a configurare Veeam per automatizzare il ripristino dei carichi di lavoro on-premise su GCVE (macchine virtuali con VMDK delle applicazioni e macchine virtuali con storage in-guest) utilizzando la funzione di replica Veeam e sfruttando SnapMirror per le copie dei volumi delle applicazioni su Cloud Volumes ONTAP.

Installare i componenti Veeam

In base allo scenario di implementazione, il server di backup Veeam, il repository di backup e il proxy di backup che devono essere implementati. In questo caso di utilizzo, non è necessario implementare l'archivio di oggetti per Veeam e il repository scale-out.
https://helpcenter.veeam.com/docs/backup/qsg_vsphere/deployment_scenarios.html["Fare riferimento alla documentazione Veeam per la procedura di installazione"]

Configurazione della replica delle macchine virtuali con Veeam

VCenter on-premise e gCVE vCenter devono essere registrati con Veeam. ["Processo di replica di vSphere VM"](#) Nella fase di elaborazione guest della procedura guidata, selezionare Disable application processing (Disattiva elaborazione applicazioni), in quanto verrà utilizzato SnapCenter per il backup e il ripristino consapevoli dell'applicazione.

[Processo di replica di vSphere VM](#)

Failover di Microsoft SQL Server VM

[Failover di Microsoft SQL Server VM](#)

Vantaggi di questa soluzione

- Utilizza la replica efficiente e resiliente di SnapMirror.
- Effettua il ripristino in qualsiasi punto disponibile in tempo con la conservazione delle snapshot di ONTAP.
- È disponibile un'automazione completa per tutte le fasi necessarie per il ripristino di centinaia o migliaia di macchine virtuali, dalle fasi di convalida di storage, calcolo, rete e applicazioni.
- SnapCenter utilizza meccanismi di cloning che non modificano il volume replicato.

- In questo modo si evita il rischio di corruzione dei dati per volumi e snapshot.
- Evita le interruzioni di replica durante i flussi di lavoro dei test di DR.
- Sfrutta i dati di DR per flussi di lavoro oltre il DR, come sviluppo/test, test di sicurezza, test di patch e upgrade e test di correzione.
- La replica Veeam consente di modificare gli indirizzi IP delle macchine virtuali sul sito DR.

Migrazione dei carichi di lavoro su GCP/GCVE

Migrazione dei carichi di lavoro nel datastore NetApp Cloud Volume Service su Google Cloud VMware Engine con VMware HCX - Guida rapida

Autore: NetApp Solutions Engineering

Panoramica: Migrazione di macchine virtuali con VMware HCX, datastore NetApp Cloud Volume Service e Google Cloud VMware Engine (GCVE)

Uno dei casi di utilizzo più comuni per il datastore Google Cloud VMware Engine e Cloud Volume Service è la migrazione dei carichi di lavoro VMware. VMware HCX è un'opzione preferita e offre vari meccanismi di migrazione per spostare macchine virtuali (VM) on-premise e i relativi dati negli archivi dati NFS Cloud Volume Service.

VMware HCX è principalmente una piattaforma di migrazione progettata per semplificare la migrazione delle applicazioni, il ribilanciamento dei carichi di lavoro e persino la business continuity tra i cloud. È incluso come parte di Google Cloud VMware Engine Private Cloud e offre diversi modi per migrare i workload e può essere utilizzato per le operazioni di disaster recovery (DR).

Il presente documento fornisce istruzioni dettagliate per il provisioning del datastore Cloud Volume Service, seguito dal download, dall'implementazione e dalla configurazione di VMware HCX, inclusi tutti i componenti principali on-premise e dal lato motore VMware di Google Cloud, tra cui Interconnect, Network Extension e ottimizzazione WAN per l'abilitazione di vari meccanismi di migrazione delle macchine virtuali.



VMware HCX funziona con qualsiasi tipo di datastore poiché la migrazione è a livello di VM. Pertanto, questo documento è valido per i clienti NetApp esistenti e non NetApp che intendono implementare Cloud Volume Service con Google Cloud VMware Engine per un'implementazione cloud VMware conveniente.

Passaggi di alto livello

Questo elenco fornisce i passaggi di alto livello necessari per associare e migrare le macchine virtuali a HCX Cloud Manager sul lato Google Cloud VMware Engine da HCX Connector on-premise:

1. Preparare HCX attraverso il portale Google VMware Engine.
2. Scaricare e implementare IL programma di installazione DI HCX Connector Open Virtualization Appliance (OVA) nel server VMware vCenter on-premise.
3. Attivare HCX con la chiave di licenza.
4. Associare il connettore VMware HCX on-premise con Google Cloud VMware Engine HCX Cloud Manager.
5. Configurare il profilo di rete, il profilo di calcolo e la mesh del servizio.
6. (Facoltativo) eseguire l'estensione di rete per evitare il re-IP durante le migrazioni.
7. Verificare lo stato dell'appliance e assicurarsi che sia possibile eseguire la migrazione.
8. Migrare i carichi di lavoro delle macchine virtuali.

Prerequisiti

Prima di iniziare, assicurarsi che siano soddisfatti i seguenti prerequisiti. Per ulteriori informazioni, consulta questa sezione ["collegamento"](#). Una volta soddisfatti i prerequisiti, inclusa la connettività, scaricare la chiave di licenza HCX dal portale VMware Engine di Google Cloud. Una volta scaricato il programma di installazione di OVA, procedere con la procedura di installazione come descritto di seguito.

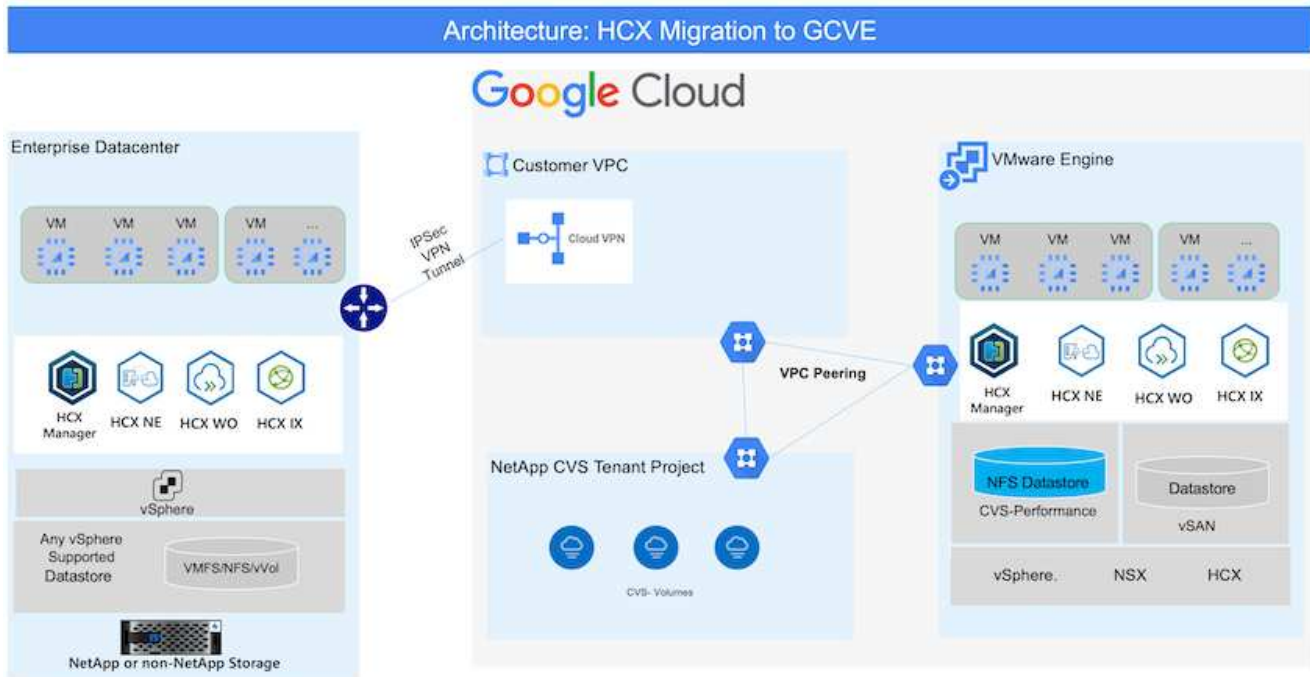


HCX Advanced è l'opzione predefinita e VMware HCX Enterprise Edition è disponibile anche attraverso un ticket di supporto e supportato senza costi aggiuntivi. Fare riferimento a. ["questo link"](#)

- Utilizza un data center software-defined (SDDC) Google Cloud VMware Engine esistente o crea un cloud privato utilizzando questo ["Link NetApp"](#) o questo ["Link di Google"](#).
- La migrazione delle macchine virtuali e dei dati associati dal data center abilitato VMware vSphere on-premise richiede la connettività di rete dal data center all'ambiente SDDC. Prima di migrare i carichi di lavoro, ["Configurare una connessione Cloud VPN o Cloud Interconnect"](#) tra l'ambiente on-premise e il rispettivo cloud privato.
- Il percorso di rete dall'ambiente VMware vCenter Server on-premise al cloud privato VMware Engine di Google Cloud deve supportare la migrazione delle macchine virtuali utilizzando vMotion.
- Assicurarsi di aver selezionato il necessario ["porte e regole del firewall"](#) Sono consentiti per il traffico vMotion tra vCenter Server on-premise e vCenter SDDC.
- Il volume NFS Cloud Volume Service deve essere montato come datastore in Google Cloud VMware Engine. Seguire i passaggi descritti in questa sezione ["collegamento"](#) Per collegare gli archivi dati Cloud Volume Service agli host Google Cloud VMware Engines.

Architettura di alto livello

A scopo di test, l'ambiente di laboratorio on-premise utilizzato per questa convalida è stato connesso tramite una VPN cloud, che consente la connettività on-premise con Google Cloud VPC.



Per uno schema più dettagliato su HCX, fare riferimento a. "[Link VMware](#)"

Implementazione della soluzione

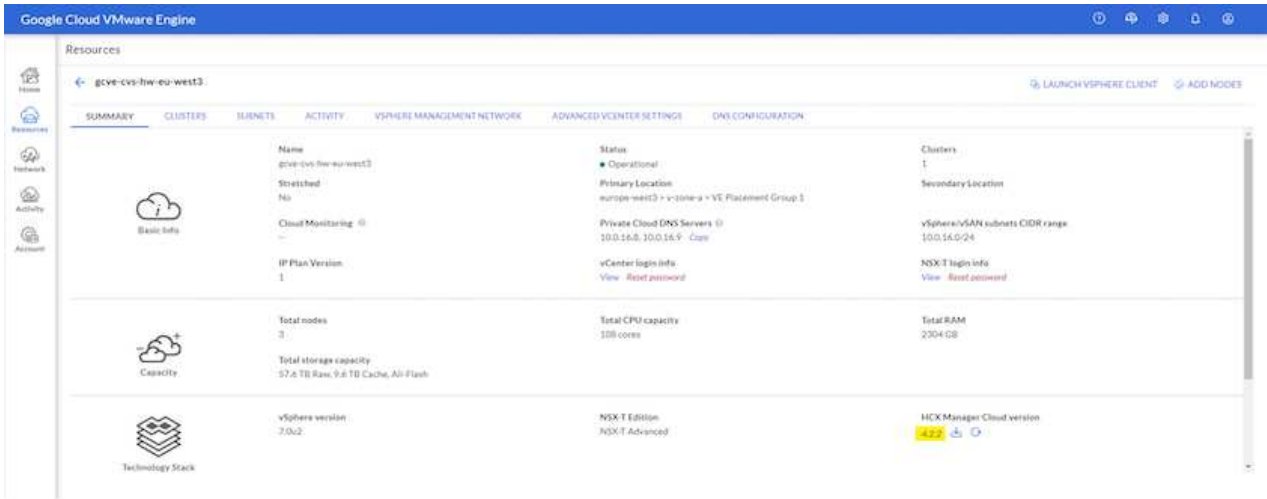
Seguire la serie di passaggi per completare l'implementazione di questa soluzione:

Fase 1: Preparazione DI HCX attraverso il portale Google VMware Engine

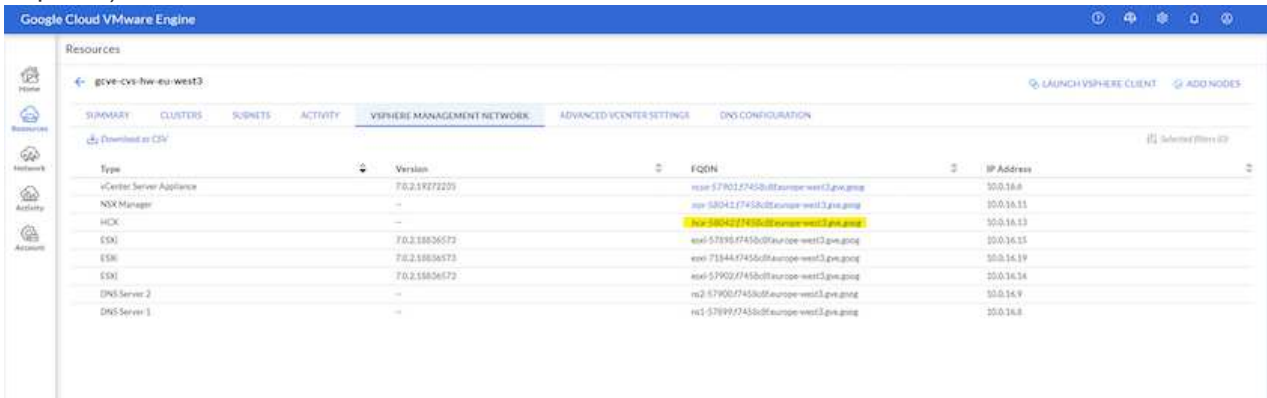
Il componente HCX Cloud Manager viene installato automaticamente durante il provisioning del cloud privato con VMware Engine. Per prepararsi all'associazione del sito, attenersi alla seguente procedura:

1. Accedi al portale Google VMware Engine e accedi A HCX Cloud Manager.

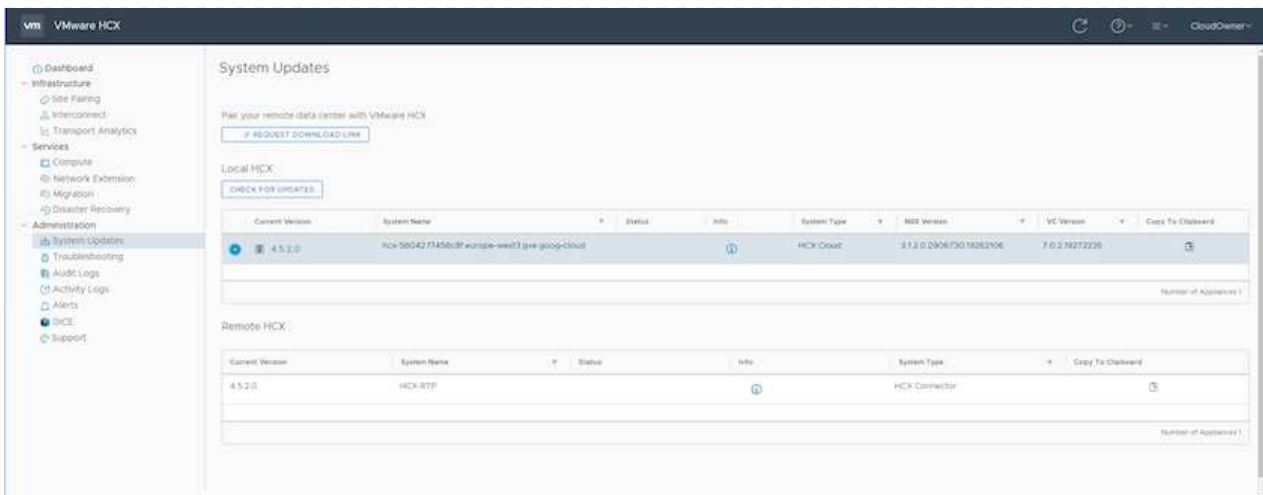
È possibile accedere ALLA console HCX facendo clic sul collegamento alla versione HCX



In alternativa, fare clic su HCX FQDN nella scheda vSphere Management Network (rete di gestione di vSphere).



2. In HCX Cloud Manager, accedere a **Administration > System Updates** (Amministrazione > aggiornamenti del sistema).
3. Fare clic su **Richiedi il download** e scaricare il file OVA.



4. Aggiornare HCX Cloud Manager alla versione più recente disponibile dall'interfaccia utente DI HCX Cloud Manager.

Fase 2: Implementazione dell'OVA del programma di installazione nel server vCenter on-premise

Affinché il connettore on-premise si connetta a HCX Manager in Google Cloud VMware Engine, assicurarsi che le porte firewall appropriate siano aperte nell'ambiente on-premise.

Per scaricare e installare HCX Connector nel server vCenter on-premise, attenersi alla seguente procedura:

1. Fare scaricare la OVA dalla console HCX su Google Cloud VMware Engine come indicato nella fase precedente.
2. Una volta scaricato l'OVA, implementarlo nell'ambiente VMware vSphere on-premise utilizzando l'opzione **Deploy OVF Template**.

The screenshot shows the 'Deploy OVF Template' wizard in vSphere. The wizard is at step 1: 'Select an OVF template'. The left sidebar shows the steps: 1. Select an OVF template, 2. Select a name and folder, 3. Select a compute resource, 4. Review details, 5. Select storage, 6. Ready to complete. The main area shows the 'Select an OVF template' section. It says 'Select an OVF template from remote URL or local file system'. Below that, it says 'Enter a URL to download and install the OVF package from the internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.' There are two radio buttons: 'URL' and 'Local file'. The 'Local file' option is selected. Below the radio buttons, there is a text input field with the URL 'http://https://remoteserver-address/filetoinstall.ovf'. Below the text input field, there is a button labeled 'UPLOAD FILES'. Below the button, there is a text input field with the file name 'VMware-HCX-Connector-4.5.2.0-20914338.ova'. At the bottom right, there are two buttons: 'CANCEL' and 'NEXT'.

3. Inserire tutte le informazioni richieste per l'implementazione di OVA, fare clic su **Avanti**, quindi fare clic su **fine** per implementare l'OVA di VMware HCX Connector.



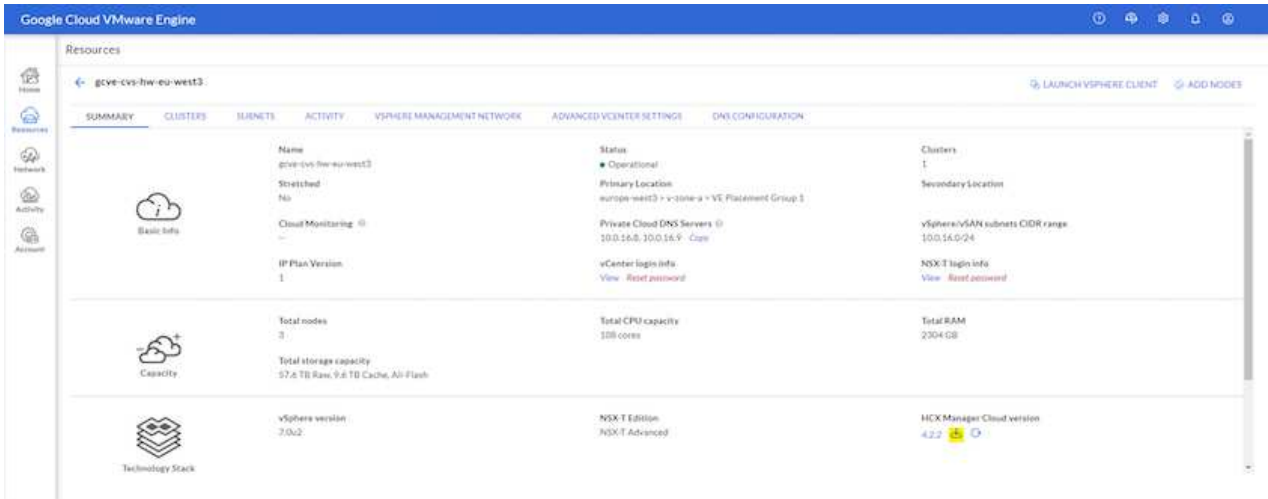
Accendere l'appliance virtuale manualmente.

Per istruzioni dettagliate, consultare ["Guida utente di VMware HCX"](#).

Fase 3: Attivare HCX Connector con la chiave di licenza

Dopo aver implementato VMware HCX Connector OVA on-premise e avviato l'appliance, completare la seguente procedura per attivare HCX Connector. Generare la chiave di licenza dal portale Google Cloud VMware Engine e attivarla in VMware HCX Manager.

1. Dal portale VMware Engine, fare clic su Resources (risorse), selezionare il cloud privato e **fare clic sull'icona di download sotto HCX Manager Cloud Version**



Aprire il file scaricato e copiare la stringa della chiave di licenza.

2. Accedere a VMware HCX Manager on-premise all'indirizzo "<https://hcxmanagerIP:9443>" utilizzando le credenziali di amministratore.



Utilizzare l'IP hcxmanagerIP e la password definiti durante l'implementazione di OVA.

3. Nella licenza, inserire la chiave copiata dal passaggio 3 e fare clic su **Activate** (attiva).



Il connettore HCX on-premise deve disporre di accesso a Internet.

4. In **posizione del data center**, fornire la posizione più vicina per l'installazione di VMware HCX Manager on-premise. Fare clic su **continua**.
5. In **Nome sistema**, aggiornare il nome e fare clic su **continua**.
6. Fare clic su **Sì, continua**.
7. In **Connect your vCenter**, fornire il nome di dominio completo (FQDN) o l'indirizzo IP di vCenter Server e le credenziali appropriate, quindi fare clic su **Continue** (continua).



Utilizzare l'FQDN per evitare problemi di connettività in un secondo momento.

8. In **Configure SSO/PSC** (Configura SSO/PSC), fornire l'indirizzo IP o il nome FQDN del Platform Services Controller (PSC) e fare clic su **Continue** (continua).



Per Embedded PSC, immettere l'indirizzo FQDN o IP di VMware vCenter Server.

9. Verificare che le informazioni immesse siano corrette e fare clic su **Restart** (Riavvia).
10. Dopo il riavvio dei servizi, vCenter Server viene visualizzato in verde nella pagina visualizzata.

VCenter Server e SSO devono disporre dei parametri di configurazione appropriati, che devono essere gli stessi della pagina precedente.



Questo processo richiede circa 10 - 20 minuti e l'aggiunta del plug-in al server vCenter.

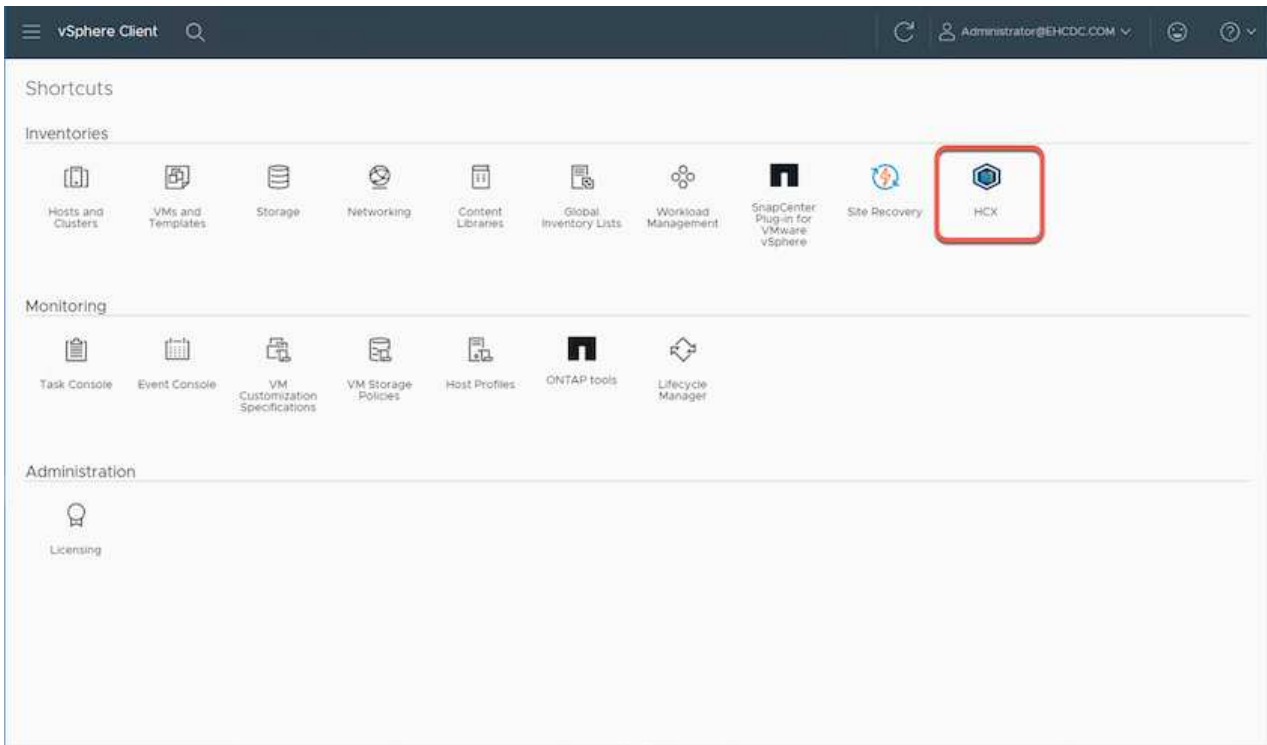
The screenshot displays the HCX Manager interface. At the top, the navigation bar includes 'vm HCX Manager', 'Dashboard', 'Appliance Summary', 'Configuration', and 'Administration'. The top right corner shows the IP address '172.21.254.155', version '4.5.2.0', and user 'admin'. The main content area is titled 'HCX-RTP' and provides system details: IP Address (172.21.254.155), Version (4.5.2.0), Uptime (13 days, 21 hours, 6 minutes), and Current Time (Thursday, 16 February 2023 05:59:00 PM UTC). To the right, resource usage is shown: CPU (26% used, 1543 MHz free), Memory (79% used, 2472 MB free), and Storage (9% used, 76G free). Below this, three configuration cards for 'NSX', 'vCenter', and 'SSO' are visible. Each card contains a URL and a 'MANAGE' button. The URLs for 'vCenter' and 'SSO' are both 'https://a300-vcso01.ehcdc.com' and are circled in red.

Component	URL	Status
NSX		
vCenter	https://a300-vcso01.ehcdc.com	Online
SSO	https://a300-vcso01.ehcdc.com	Online

Fase 4: Associazione on-premise di VMware HCX Connector con Google Cloud VMware Engine HCX Cloud Manager

Una volta implementato E configurato IL connettore HCX on-premise vCenter, stabilire la connessione a Cloud Manager aggiungendo l'accoppiamento. Per configurare l'associazione del sito, attenersi alla seguente procedura:

1. Per creare una coppia di siti tra l'ambiente vCenter on-premise e Google Cloud VMware Engine SDDC, accedere a vCenter Server on-premise e al nuovo plug-in HCX vSphere Web Client.



2. In Infrastructure (infrastruttura), fare clic su **Add a Site Pairing** (Aggiungi associazione sito).



Inserire l'indirizzo IP o l'URL di Google Cloud VMware Engine HCX Cloud Manager e le credenziali per l'utente con privilegi di ruolo Cloud Owner per l'accesso al cloud privato.

Connect to Remote Site



Remote HCX URL

https://hcx-58042.f7458c8f.europe-west3.g



Username

cloudowner@gve.local



Password

.....

CANCEL

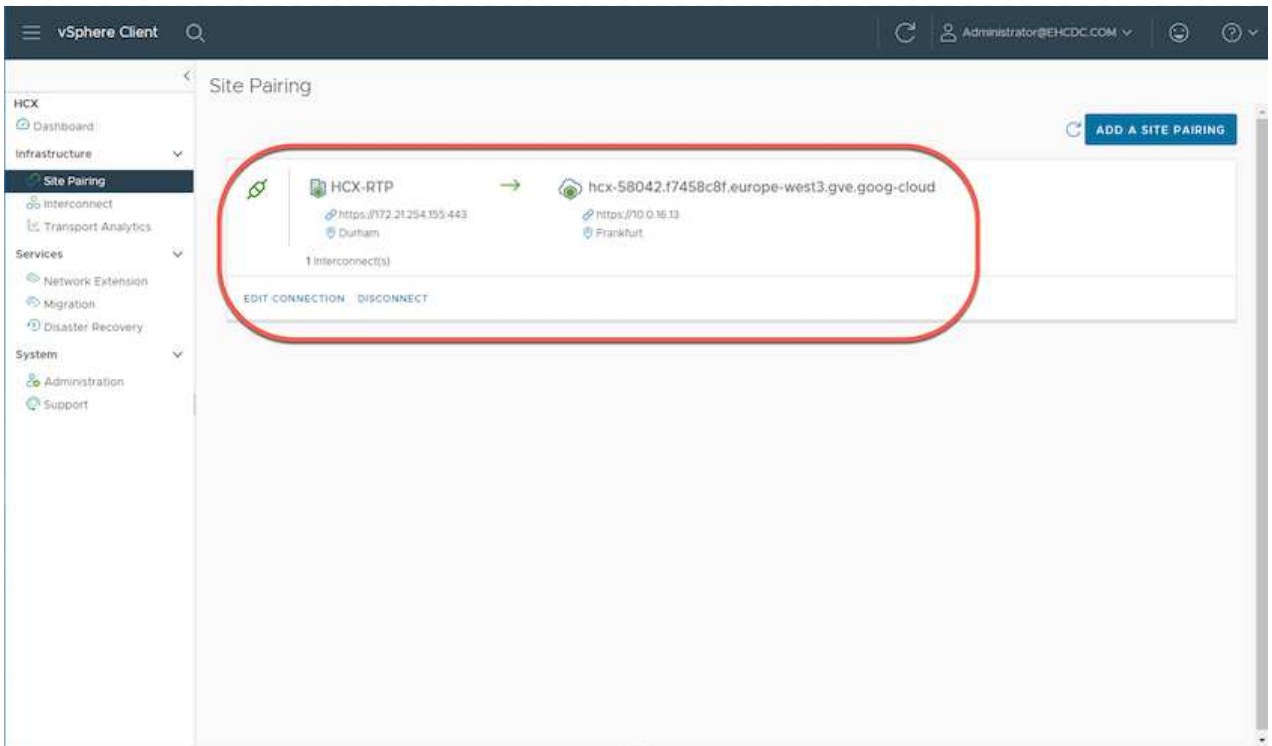
CONNECT

3. Fare clic su **Connect** (Connetti).



Il connettore VMware HCX deve essere in grado di instradare all'indirizzo IP DI HCX Cloud Manager tramite la porta 443.

4. Una volta creata l'associazione, l'associazione del sito appena configurata è disponibile nella dashboard HCX.



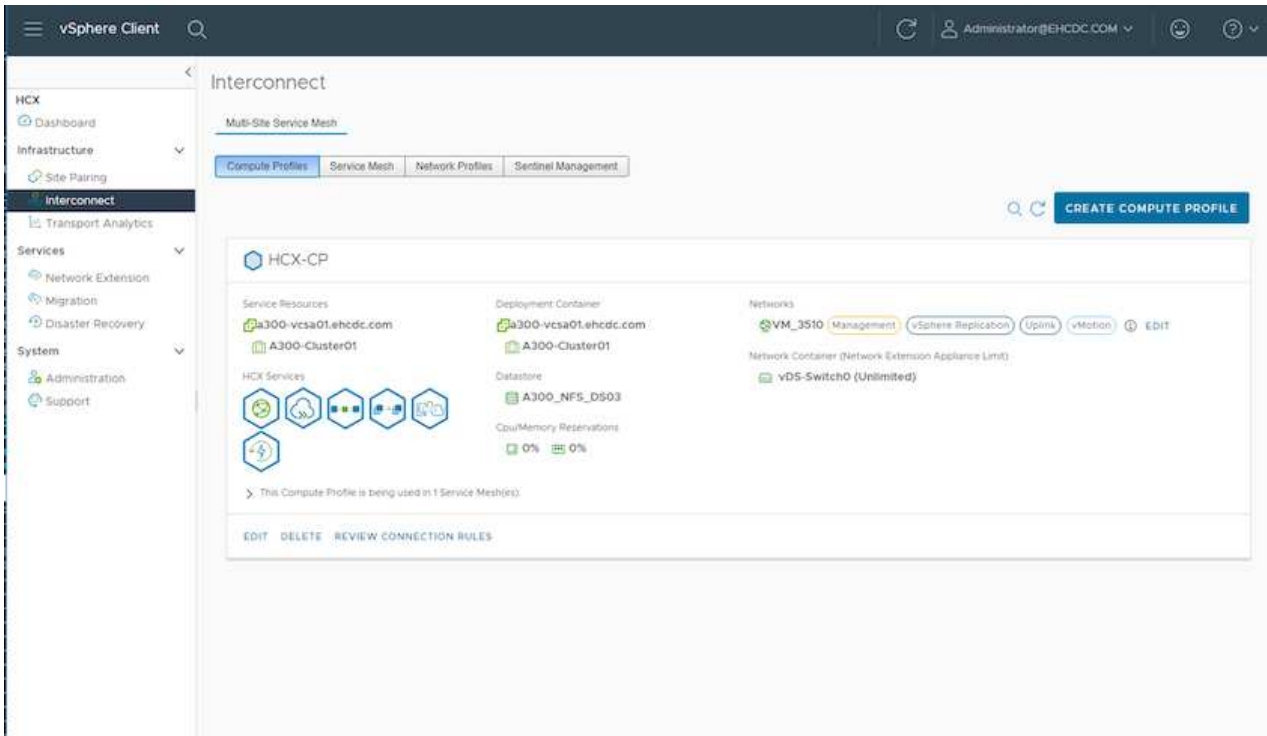
Fase 5: Configurare il profilo di rete, il profilo di calcolo e la mesh del servizio

L'appliance di servizio VMware HCX Interconnect offre funzionalità di replica e migrazione basata su vMotion su Internet e connessioni private al sito di destinazione. L'interconnessione offre crittografia, progettazione del traffico e mobilità delle macchine virtuali. Per creare un'appliance di servizio Interconnect, attenersi alla seguente procedura:

1. In Infrastructure (infrastruttura), selezionare **Interconnect > Multi-Site Service Mesh > Compute Profiles > Create Compute Profile** (interconnessione > Mesh servizio multi-sito > profili di calcolo > Crea profilo di calcolo)



I profili di calcolo definiscono i parametri di implementazione, incluse le appliance implementate e la parte del data center VMware accessibile al servizio HCX.

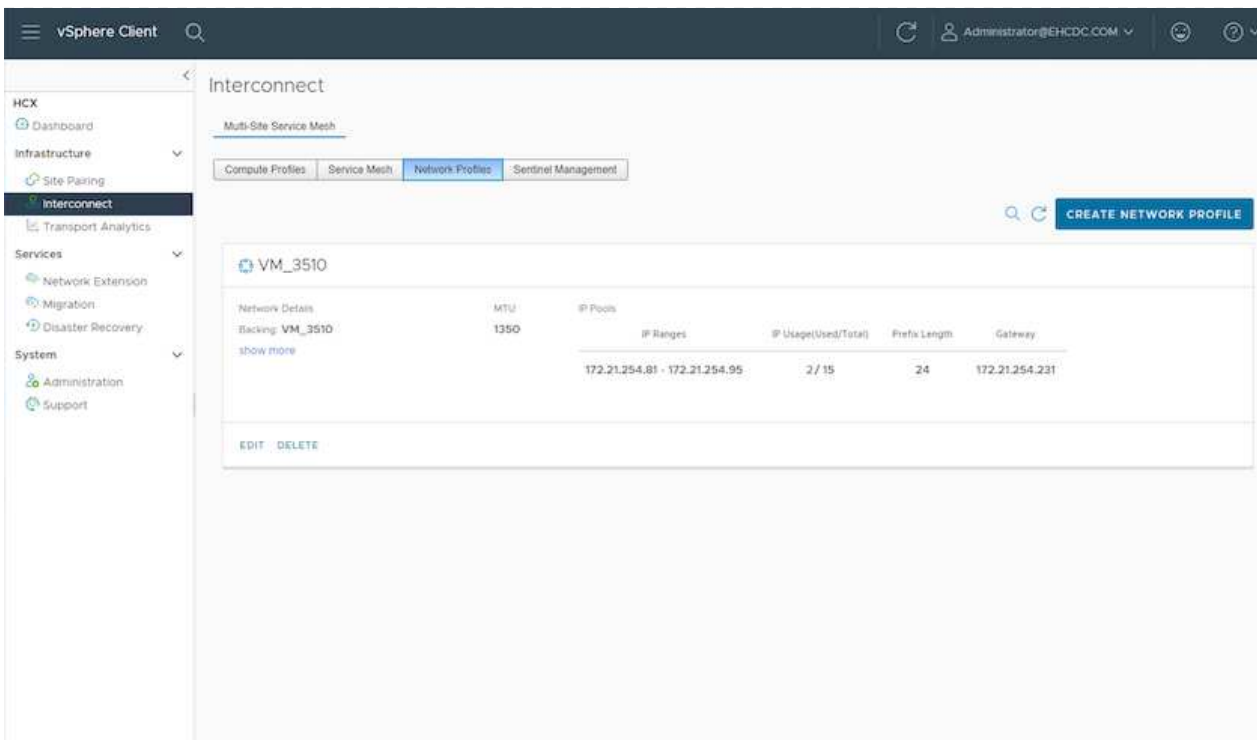


2. Una volta creato il profilo di calcolo, creare i profili di rete selezionando **Multi-Site Service Mesh > Network Profiles > Create Network Profile** (Mesh servizio multi-sito > profili di rete > Crea profilo di rete).

Il profilo di rete definisce un intervallo di indirizzi IP e reti utilizzati DA HCX per le proprie appliance virtuali.



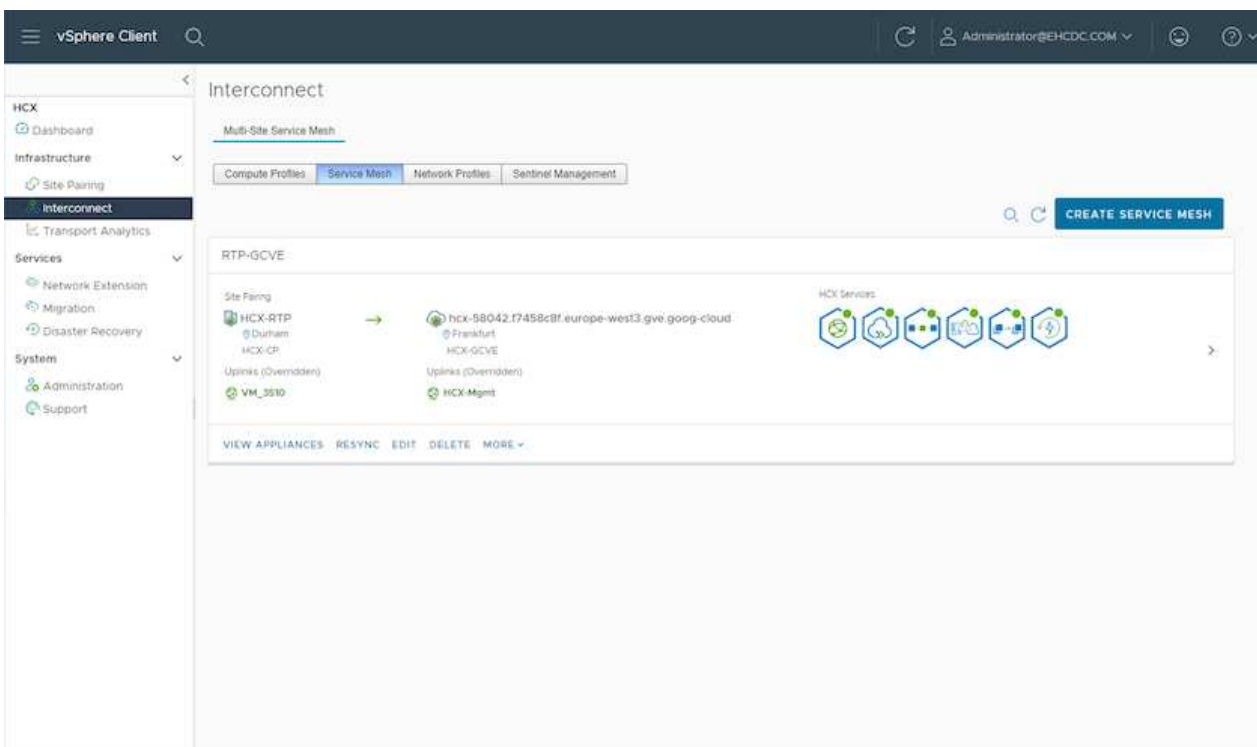
Questa operazione richiede due o più indirizzi IP. Questi indirizzi IP vengono assegnati dalla rete di gestione alle appliance di interconnessione.



3. A questo punto, i profili di calcolo e di rete sono stati creati correttamente.
4. Creare la Service Mesh selezionando la scheda **Service Mesh** all'interno dell'opzione **Interconnect** e selezionando i siti SDDC on-premise e GCVE.
5. Service Mesh specifica una coppia di profili di rete e di calcolo locale e remoto.



Nell'ambito di questo processo, le appliance HCX vengono implementate e configurate automaticamente sui siti di origine e di destinazione per creare un fabric di trasporto sicuro.



- Questa è la fase finale della configurazione. Il completamento dell'implementazione richiede circa 30 minuti. Una volta configurata la mesh del servizio, l'ambiente è pronto con i tunnel IPsec creati correttamente per migrare le macchine virtuali del carico di lavoro.

The screenshot displays the vSphere Client interface, specifically the 'Interconnect' section. The 'Appliances on HCX-RTP' table is visible, showing details for three appliances. The first two appliances, RTP-GCVR-0K-01 and RTP-GCVR-0K-02, are HCL WAN-01 and have a current version of 4.3.0. The third appliance, RTP-GCVR-WG-01, is HCL WAN-02 and has a current version of 7.3.0. The table also includes columns for Appliance Name, Appliance Type, IP Address, Management, Tunnel Status, and Current Version.

Appliance Name	Appliance Type	IP Address	Management	Tunnel Status	Current Version
RTP-GCVR-0K-01 id: 2045749-4001-4001-4001-4001-4001-4001 Compute: A300-01-01-01 Storage: A300-01-01-01	HCL WAN-01	172.21.254.01	Management	Uplink: Up	4.3.0
RTP-GCVR-0K-02 id: 4015121-4001-4001-4001-4001-4001-4001 Compute: A300-01-01-01 Storage: A300-01-01-01 Network: A300-01-01-01 Extended Network: V1	HCL WAN-01	172.21.254.02	Management	Uplink: Up	4.3.0
RTP-GCVR-WG-01 id: 0004708-4701-4701-4701-4701-4701-4701 Compute: A300-01-01-01 Storage: A300-01-01-01	HCL WAN-02				7.3.0

Fase 6: Migrazione dei carichi di lavoro

I carichi di lavoro possono essere migrati bidirezionalmente tra gli SDDC on-premise e GCVE utilizzando varie tecnologie di migrazione VMware HCX. Le VM possono essere spostate da e verso le entità attivate da VMware HCX utilizzando diverse tecnologie di migrazione, come LA migrazione in blocco HCX, HCX vMotion, HCX Cold Migration, HCX Replication Assisted vMotion (disponibile con HCX Enterprise Edition) e HCX OS Assisted Migration (disponibile con HCX Enterprise Edition).

Per ulteriori informazioni sui vari meccanismi di migrazione HCX, vedere ["Tipi di migrazione VMware HCX"](#).

L'appliance HCX-IX utilizza il servizio Mobility Agent per eseguire migrazioni vMotion, Cold e Replication Assisted vMotion (RAV).



L'appliance HCX-IX aggiunge il servizio Mobility Agent come oggetto host in vCenter Server. Il processore, la memoria, lo storage e le risorse di rete visualizzati su questo oggetto non rappresentano il consumo effettivo dell'hypervisor fisico che ospita l'appliance IX.

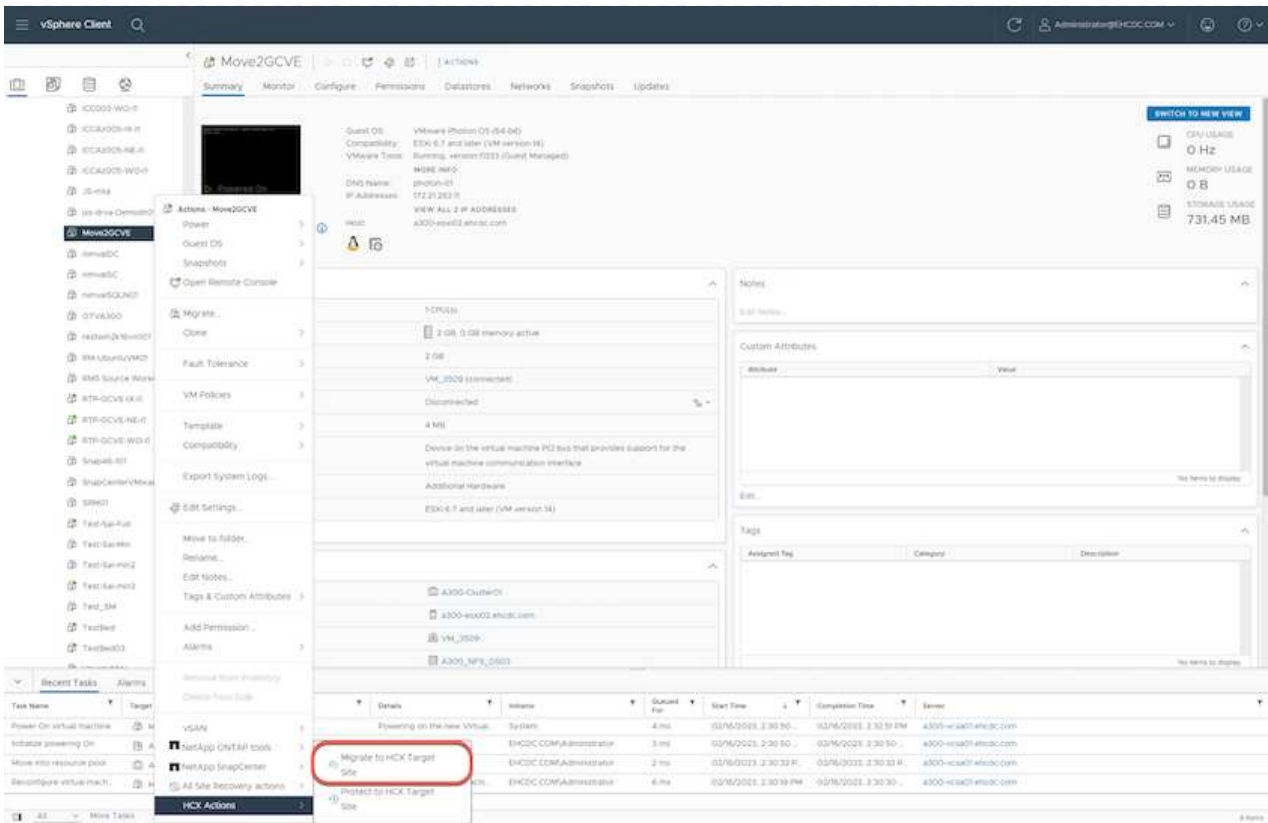
HCX vMotion

In questa sezione viene descritto il meccanismo vMotion DI HCX. Questa tecnologia di migrazione utilizza il protocollo VMware vMotion per migrare una macchina virtuale in GCVE. L'opzione di migrazione vMotion viene utilizzata per la migrazione dello stato della macchina virtuale di una singola macchina virtuale alla volta. Durante questo metodo di migrazione non si verifica alcuna interruzione del servizio.

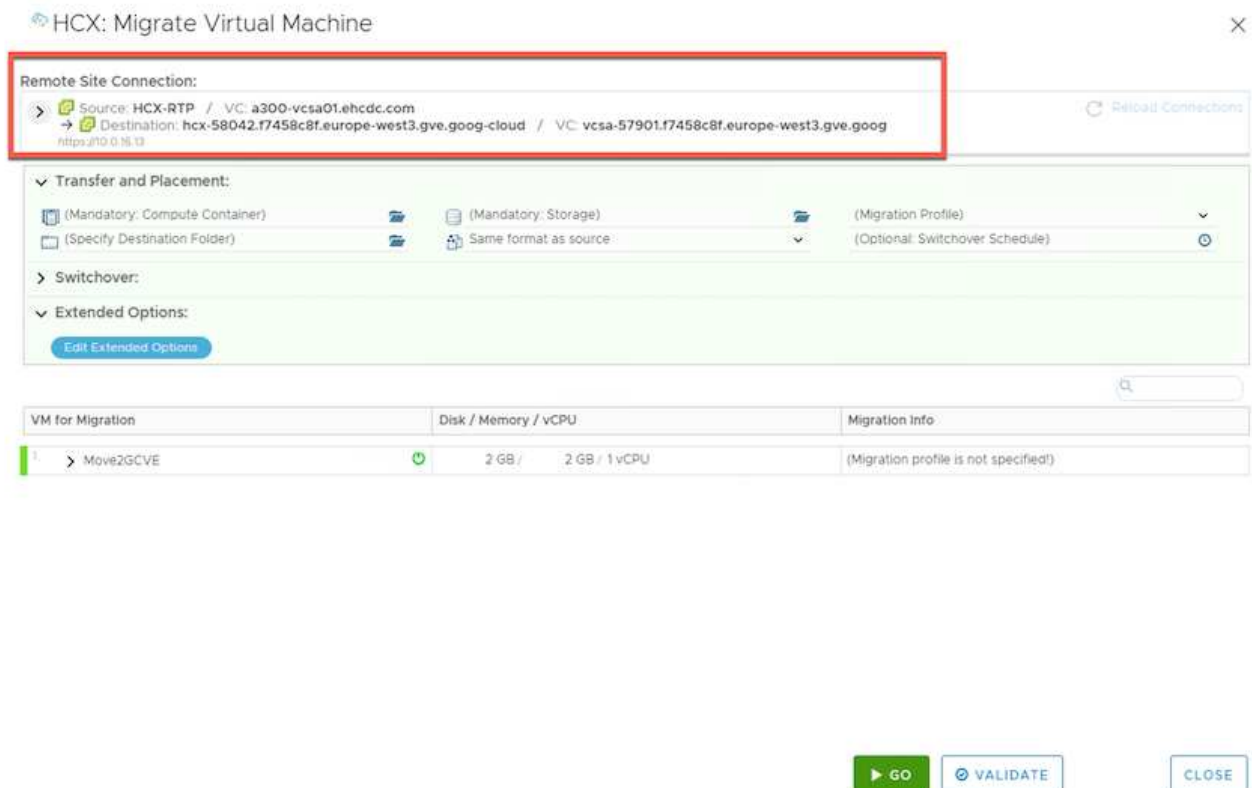


Network Extension deve essere installato (per il gruppo di porte a cui è collegata la macchina virtuale) per migrare la macchina virtuale senza dover modificare l'indirizzo IP.

1. Dal client vSphere on-premise, accedere a Inventory (inventario), fare clic con il pulsante destro del mouse sulla macchina virtuale da migrare e selezionare HCX Actions (azioni HCX) > Migrate to HCX Target Site (Migra al sito di destinazione HCX).



2. Nella procedura guidata Migrate Virtual Machine, selezionare Remote Site Connection (GCVE di destinazione).



3. Aggiornare i campi obbligatori (Cluster, Storage e Destination Network), quindi fare clic su Validate (convalida).

HCX: Migrate Virtual Machine

Remote Site Connection:

Source: HCX-RTP / VC: a300-vcsa01.ehcdc.com
 Destination: hcx-58042.f7458c8f.europe-west3.gcp.goog-cloud / VC: vcsa-57901.f7458c8f.europe-west3.gcp.goog
<https://10.0.16.13>

Transfer and Placement:

Workload: gcp-ve-4 (807.6 GB / 1 TB) vMotion
 (Specify Destination Folder) Same format as source (Optional: Switchover Schedule)

Switchover:

Extended Options:

Edit Extended Options

Retain MAC

VM for Migration	Disk / Memory / vCPU	Migration Info
1 Move2GCVE Workload: gcp-ve-4 (807.6 GB / 1 TB) (Specify Destination Folder) Same format as source <input type="checkbox"/> Force Power-off VM <input type="checkbox"/> Enable Seed Checkpoint Edit Extended Options Retain MAC	2 GB / 2 GB / 1 vCPU gcp-ve-4 (807.6 GB / 1 TB) Same format as source	vMotion
Network adapter 1 (VM_3509) → L2E_VM_3509-3509-a0041a8d		

GO

VALIDATE

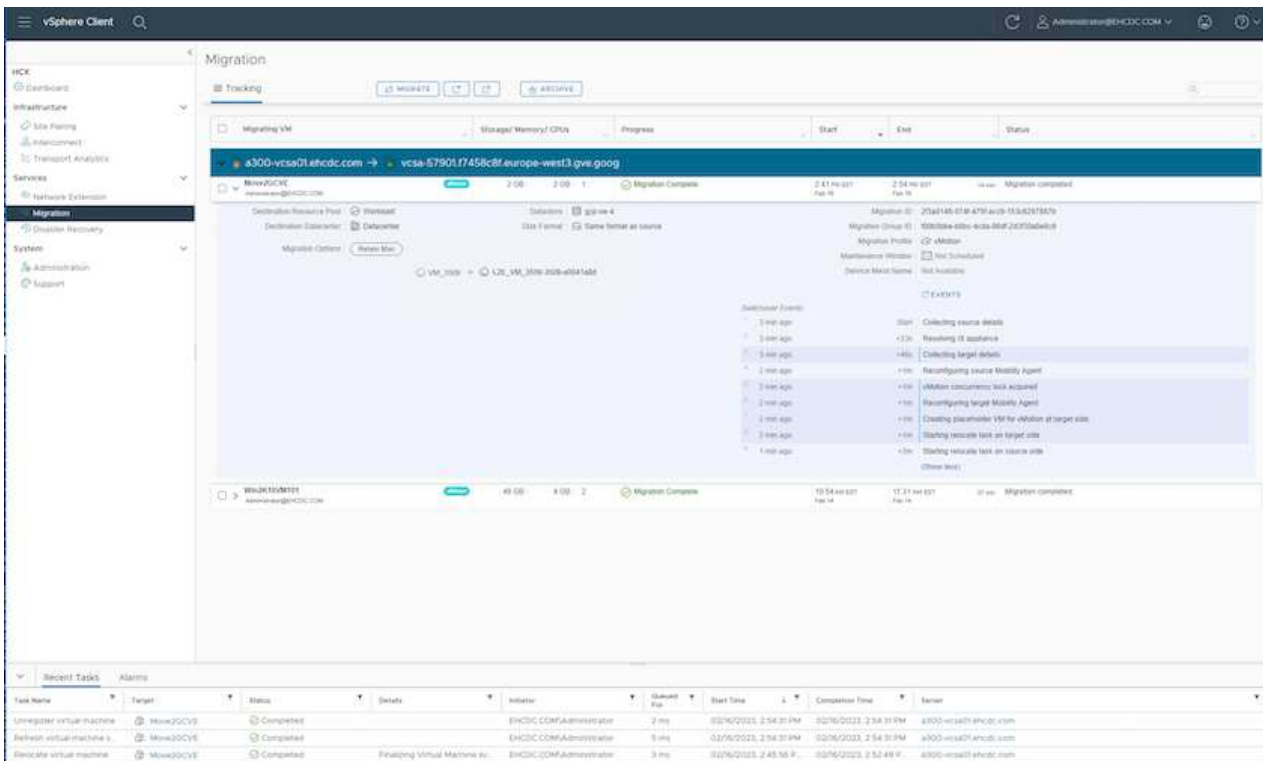
CLOSE

- Al termine dei controlli di convalida, fare clic su Go (Vai) per avviare la migrazione.



Il trasferimento vMotion acquisisce la memoria attiva della macchina virtuale, il suo stato di esecuzione, il suo indirizzo IP e il suo indirizzo MAC. Per ulteriori informazioni sui requisiti e sulle limitazioni di HCX vMotion, vedere ["Informazioni su VMware HCX vMotion e Cold Migration"](#).

- È possibile monitorare l'avanzamento e il completamento di vMotion dalla dashboard HCX > Migration (HCX > migrazione).



Il datastore NFS CVS di destinazione deve disporre di spazio sufficiente per gestire la migrazione.

Conclusione

Sia che tu stia prendendo di mira il cloud all-cloud o ibrido e i dati che risiedono su storage di qualsiasi tipo/vendor in on-premise, Cloud Volume Service e HCX offrono eccellenti opzioni per implementare e migrare i carichi di lavoro delle applicazioni, riducendo al contempo il TCO rendendo i requisiti dei dati perfetti per il livello applicativo. Qualunque sia il caso d'utilizzo, scegli Google Cloud VMware Engine insieme a Cloud Volume Service per una rapida realizzazione dei vantaggi del cloud, un'infrastruttura coerente e operazioni su cloud multipli e on-premise, portabilità bidirezionale dei carichi di lavoro e capacità e performance di livello Enterprise. Si tratta degli stessi processi e procedure familiari utilizzati per connettere lo storage e migrare le macchine virtuali utilizzando VMware vSphere Replication, VMware vMotion o persino la copia del file di rete (NFC).

Punti da asporto

I punti chiave di questo documento includono:

- Ora puoi utilizzare Cloud Volume Service come datastore su Google Cloud VMware Engine SDDC.
- È possibile migrare facilmente i dati dall'archivio dati on-premise a Cloud Volume Service.
- È possibile espandere e ridurre facilmente il datastore Cloud Volume Service per soddisfare i requisiti di capacità e performance durante l'attività di migrazione.

Video di Google e VMware come riferimento

Da Google

- ["Implementare HCX Connector con GCVE"](#)
- ["Configurare HCX ServiceMesh con GCVE"](#)
- ["Migrare VM con HCX in GCVE"](#)

Di VMware

- ["Implementazione DI HCX Connector per GCVE"](#)
- ["Configurazione HCX ServiceMesh per GCVE"](#)
- ["Migrazione del carico di lavoro HCX in GCVE"](#)

Dove trovare ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo documento, fare riferimento ai seguenti collegamenti Web:

- Documentazione di Google Cloud VMware Engine
["https://cloud.google.com/vmware-engine/docs/overview"](https://cloud.google.com/vmware-engine/docs/overview)
- Documentazione Cloud Volume Service
["https://cloud.google.com/architecture/partners/netapp-cloud-volumes"](https://cloud.google.com/architecture/partners/netapp-cloud-volumes)
- Guida utente di VMware HCX
["https://docs.vmware.com/en/VMware-HCX/index.html"](https://docs.vmware.com/en/VMware-HCX/index.html)

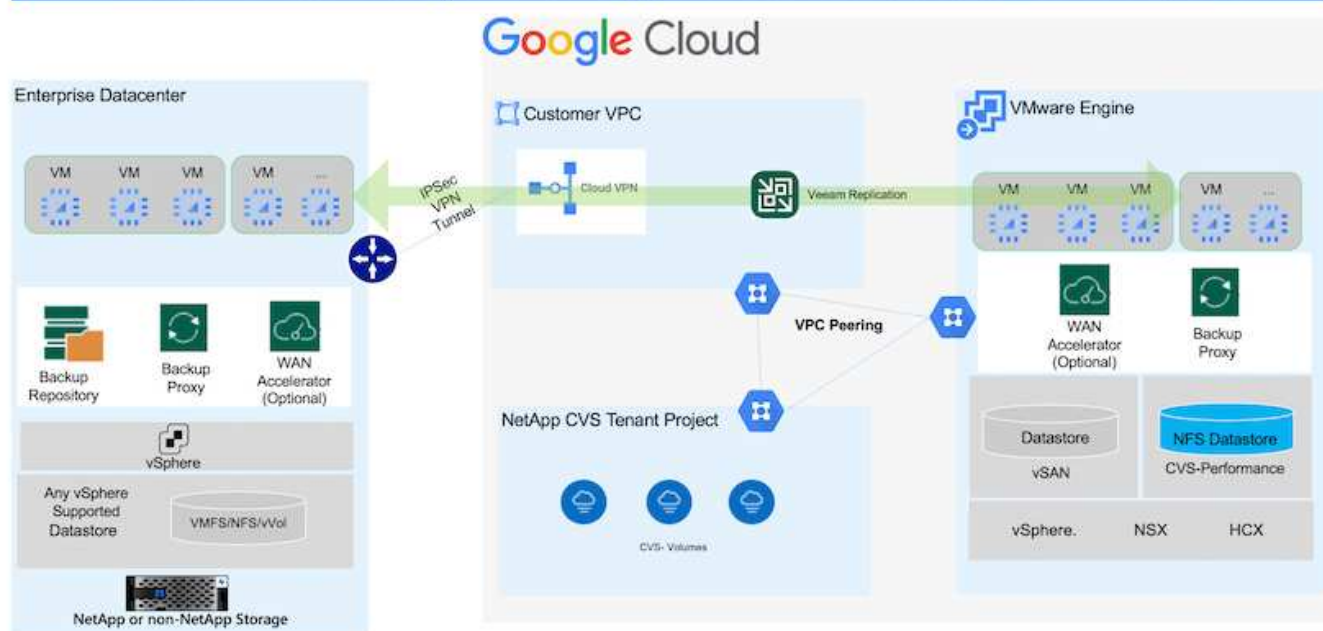
Migrazione delle macchine virtuali al servizio volumi cloud NetApp Datastore NFS su Google Cloud VMware Engine con la funzione di replica Veeam

Panoramica

Autori: Suresh Thoppay, NetApp

I carichi di lavoro delle macchine virtuali eseguiti su VMware vSphere possono essere migrati a Google Cloud VMware Engine (GCVE) utilizzando la funzione di replica Veeam.

Questo documento fornisce un approccio passo per passo per la configurazione e l'esecuzione della migrazione delle macchine virtuali che utilizza il servizio volumi cloud di NetApp, Veeam e il motore VMware di Google Cloud (GCVE).



Presupposti

Il presente documento presuppone che l'utente disponga di Google Cloud VPN o Cloud Interconnect o di un'altra opzione di rete per stabilire la connettività di rete dai server vSphere esistenti a Google Cloud VMware Engine.



Esistono diverse opzioni per connettere i data center on-premise a Google Cloud, che ci impediscono di delineare un workflow specifico in questo documento. Fare riferimento a ["Documentazione di Google Cloud"](#) Per il metodo di connettività on-premise-to-Google appropriato.

Implementazione della soluzione di migrazione

Panoramica sull'implementazione della soluzione

1. Assicurarsi che il datastore NFS dal servizio volumi cloud di NetApp sia montato su GCVE vCenter.
2. Assicurarsi che Veeam Backup Recovery sia implementato nell'ambiente VMware vSphere esistente
3. Crea processo di replica per avviare la replica delle macchine virtuali sull'istanza di Google Cloud VMware Engine.
4. Eseguire il failover del processo di replica Veeam.
5. Eseguire il failover permanente su Veeam.

Dettagli sull'implementazione

Assicurarsi che il datastore NFS dal servizio volumi cloud di NetApp sia montato su GCVE vCenter

Accedere a GCVE vCenter e assicurarsi che sia disponibile un datastore NFS con spazio sufficiente. In caso contrario, fare riferimento a ["Montare NetApp CVS come datastore NFS su GCVE"](#)

Assicurarsi che Veeam Backup Recovery sia implementato nell'ambiente VMware vSphere esistente

Fare riferimento a. ["Componenti di replica Veeam"](#) documentazione per l'installazione dei componenti richiesti.

Crea processo di replica per avviare la replica delle macchine virtuali sull'istanza di Google Cloud VMware Engine.

VCenter on-premise e gCVE vCenter devono essere registrati con Veeam. ["Processo di replica di vSphere VM"](#)

Ecco un video che spiega come ["Configurazione del processo di replica"](#).



La replica VM può avere un IP diverso dalla VM di origine e può anche essere collegata a un gruppo di porte diverso. Per ulteriori dettagli, consulta il video qui sopra.

Eseguire il failover del processo di replica Veeam

Per migrare le macchine virtuali, eseguire ["Eseguire il failover"](#)

Eseguire il failover permanente su Veeam.

Per trattare GCVE come nuovo ambiente di origine, eseguire ["Failover permanente"](#)

Vantaggi di questa soluzione

- L'infrastruttura di backup Veeam esistente può essere utilizzata per la migrazione.
- La replica Veeam consente di modificare gli indirizzi IP delle macchine virtuali sul sito di destinazione.
- È in grado di rimappare i dati esistenti replicati al di fuori di Veeam (come i dati replicati da BlueXP)
- È in grado di specificare diversi portgroup di rete sul sito di destinazione.
- Può specificare l'ordine di accensione delle macchine virtuali.
- Utilizza VMware Change Block Tracking per ridurre al minimo la quantità di dati da inviare attraverso la WAN.
- Capacità di eseguire script pre e post per la replica.
- Capacità di eseguire script pre e post per le snapshot.

Disponibilità regionale: Datastore NFS supplementare per Google Cloud Platform (GCP)

Il datastore NFS supplementare per GCVE è supportato con il servizio volumi cloud di NetApp.



Solo i volumi CVS-Performance possono essere utilizzati per GCVE NFS Datastore. Per la posizione disponibile, fare riferimento a. ["Mappa geografica globale"](#)

Google Cloud VMware Engine è disponibile presso le seguenti sedi

asia-northeast1 > v-zone-a > VE Placement Group 1
asia-northeast1 > v-zone-a > VE Placement Group 2
asia-south1 > v-zone-a > VE Placement Group 2
asia-south1 > v-zone-a > VE Placement Group 1
asia-southeast1 > v-zone-a > VE Placement Group 1
asia-southeast1 > v-zone-a > VE Placement Group 2
australia-southeast1 > v-zone-b > VE Placement Group 1
australia-southeast1 > v-zone-a > VE Placement Group 1
australia-southeast1 > v-zone-b > VE Placement Group 2
australia-southeast1 > v-zone-a > VE Placement Group 2
europe-west2 > v-zone-a > VE Placement Group 2
europe-west2 > v-zone-a > VE Placement Group 1
europe-west3 > v-zone-b > VE Placement Group 2
europe-west3 > v-zone-a > VE Placement Group 3
europe-west3 > v-zone-a > VE Placement Group 4
europe-west3 > v-zone-b > VE Placement Group 1
europe-west3 > v-zone-a > VE Placement Group 2
europe-west3 > v-zone-a > VE Placement Group 1
europe-west4 > v-zone-a > VE Placement Group 2
europe-west4 > v-zone-a > VE Placement Group 1
europe-west6 > v-zone-a > VE Placement Group 1
europe-west8 > v-zone-a > VE Placement Group 1
northamerica-northeast1 > v-zone-a > VE Placement Group 1
northamerica-northeast1 > v-zone-a > VE Placement Group 2
northamerica-northeast2 > v-zone-a > VE Placement Group 2
northamerica-northeast2 > v-zone-a > VE Placement Group 1
southamerica-east1 > v-zone-a > VE Placement Group 1
southamerica-east1 > v-zone-a > VE Placement Group 2
us-central1 > v-zone-a > VE Placement Group 2
us-central1 > v-zone-a > VE Placement Group 5
us-central1 > v-zone-a > VE Placement Group 1
us-central1 > v-zone-a > VE Placement Group 3
us-east4 > v-zone-a > VE Placement Group 5
us-east4 > v-zone-a > VE Placement Group 10
us-east4 > v-zone-a > VE Placement Group 6
us-east4 > v-zone-a > VE Placement Group 3
us-east4 > v-zone-b > VE Placement Group 5
us-east4 > v-zone-a > VE Placement Group 1
us-east4 > v-zone-b > VE Placement Group 1
us-east4 > v-zone-a > VE Placement Group 4
us-east4 > v-zone-b > VE Placement Group 6
us-east4 > v-zone-a > VE Placement Group 2
us-west2 > v-zone-a > VE Placement Group 3
us-west2 > v-zone-a > VE Placement Group 4
us-west2 > v-zone-a > VE Placement Group 5
us-west2 > v-zone-a > VE Placement Group 2
us-west2 > v-zone-a > VE Placement Group 1
us-west2 > v-zone-a > VE Placement Group 6

Per ridurre al minimo la latenza, il volume CVS di NetApp e GCVE in cui si intende montare il volume devono trovarsi nella stessa zona di disponibilità. Collabora con gli architetti delle soluzioni Google e NetApp per ottenere le ottimizzazioni di disponibilità e TCO.

Panoramica sulla sicurezza - NetApp Cloud Volumes Service (CVS) in Google Cloud

TR-4918: Panoramica sulla sicurezza - NetApp Cloud Volumes Service in Google Cloud

Oliver Krause, Justin Parisi, NetApp

Scopo del documento

La sicurezza, in particolare nel cloud in cui l'infrastruttura non è sotto il controllo degli amministratori dello storage, è fondamentale per affidare i tuoi dati alle offerte di servizi fornite dai cloud provider. Questo documento offre una panoramica delle offerte di sicurezza offerte da NetApp ["Cloud Volumes Service è disponibile in Google Cloud"](#).

Pubblico previsto

I destinatari del presente documento includono, a titolo esemplificativo e non esaustivo, i seguenti ruoli:

- Cloud provider
- Amministratori dello storage
- Architetti dello storage
- Risorse sul campo
- Decision maker aziendali

In caso di domande sul contenuto di questo report tecnico, consulta la sezione ["Contattaci."](#)

Abbreviazione	Definizione
CVS-SW	Cloud Volumes Service, CVS tipo di servizio
Performance CVS	Cloud Volume Service, tipo di servizio CVS-Performance
PSA	

In che modo Cloud Volumes Service in Google Cloud protegge i tuoi dati

Cloud Volumes Service in Google Cloud offre una moltitudine di modi per proteggere in modo nativo i tuoi dati.

Architettura sicura e modello di tenancy

Cloud Volumes Service offre un'architettura sicura in Google Cloud segmentando la gestione del servizio (piano di controllo) e l'accesso ai dati (piano dati) tra diversi endpoint in modo che nessuno dei due possa influire sull'altro (vedere la sezione ["Architettura Cloud Volumes Service"](#)). Utilizza Google ["accesso ai servizi privati"](#) (PSA) per fornire il servizio. Questo framework distingue tra il produttore di servizi, fornito e gestito da

NetApp, e il consumatore di servizi, che è un cloud privato virtuale (VPC) in un progetto del cliente, che ospita i client che desiderano accedere alle condivisioni di file Cloud Volumes Service.

In questa architettura, i tenant (vedere la sezione ["Modello di tenancy"](#)) Sono definiti come progetti Google Cloud che sono completamente isolati l'uno dall'altro, a meno che l'utente non sia esplicitamente connesso. I tenant consentono l'isolamento completo dei volumi di dati, dei servizi di nomi esterni e di altre parti essenziali della soluzione da parte di altri tenant utilizzando la piattaforma per volumi Cloud Volumes Service. Poiché la piattaforma Cloud Volumes Service è connessa tramite peering VPC, tale isolamento si applica anche ad essa. È possibile abilitare la condivisione di volumi Cloud Volumes Service tra più progetti utilizzando un VPC condiviso (vedere la sezione ["VPC condivisi"](#)). È possibile applicare i controlli di accesso alle condivisioni SMB e alle esportazioni NFS per limitare chi o cosa può visualizzare o modificare i set di dati.

Gestione efficace delle identità per il piano di controllo

Nel piano di controllo in cui avviene la configurazione Cloud Volumes Service, la gestione delle identità viene gestita tramite ["IAM \(Identity Access Management\)"](#). IAM è un servizio standard che consente di controllare l'autenticazione (accessi) e l'autorizzazione (autorizzazioni) per le istanze di progetto di Google Cloud. Tutta la configurazione viene eseguita con API Cloud Volumes Service su un trasporto HTTPS sicuro utilizzando la crittografia TLS 1.2 e l'autenticazione viene eseguita utilizzando token JWT per una maggiore sicurezza. L'interfaccia utente della console Google per Cloud Volumes Service converte l'input dell'utente in chiamate API Cloud Volumes Service.

Protezione avanzata - limita le superfici di attacco

Una parte della sicurezza effettiva consiste nel limitare il numero di superfici di attacco disponibili in un servizio. Le superfici di attacco possono includere una varietà di elementi, tra cui dati a riposo, trasferimenti in volo, accessi e set di dati stessi.

Un servizio gestito rimuove alcune delle superfici di attacco intrinsecamente nella sua progettazione. Gestione dell'infrastruttura, come descritto nella sezione ["Funzionamento del servizio"](#) è gestito da un team dedicato ed è automatizzato per ridurre il numero di volte in cui un umano tocca effettivamente le configurazioni, contribuendo a ridurre il numero di errori intenzionali e non intenzionali. La rete è disattivata in modo che solo i servizi necessari possano accedere l'uno all'altro. La crittografia viene inserita nello storage dei dati e solo il piano dati richiede attenzione per la sicurezza da parte degli amministratori di Cloud Volumes Service. Nascondendo la maggior parte della gestione dietro un'interfaccia API, la sicurezza viene ottenuta limitando le superfici di attacco.

Modello Zero Trust

Storicamente, la filosofia di sicurezza IT è stata quella di fidarsi, ma di verificare, e si è manifestata come affidandosi esclusivamente a meccanismi esterni (come firewall e sistemi di rilevamento delle intrusioni) per mitigare le minacce. Tuttavia, gli attacchi e le violazioni si sono evoluti per aggirare la verifica negli ambienti attraverso phishing, social engineering, minacce interne e altri metodi che forniscono la verifica per entrare nelle reti e causare caos.

Zero Trust è diventata una nuova metodologia per la sicurezza, con l'attuale mantra "fidarsi di nulla pur verificando tutto". Pertanto, per impostazione predefinita, non è consentito alcun accesso. Questo mantra viene applicato in diversi modi, tra cui firewall standard e sistemi di rilevamento delle intrusioni (IDS) e con i seguenti metodi:

- Metodi di autenticazione avanzata (ad esempio token Kerberos o JWT con crittografia AES)
- Singole fonti di identità sicure (come Windows Active Directory, Lightweight Directory Access Protocol (LDAP) e Google IAM)
- Segmentazione della rete e multi-tenancy sicura (solo i tenant possono accedere per impostazione

predefinita)

- Controlli granulari degli accessi con policy di accesso con privilegi minimi
- Piccoli elenchi esclusivi di amministratori affidabili e dedicati con audit digitale e percorsi cartacei

Cloud Volumes Service eseguito in Google Cloud rispetta il modello Zero Trust implementando la posizione "Trust Nothing, Verify Everything".

Crittografia

Crittografare i dati inattivi (vedere la sezione ["Crittografia dei dati a riposo"](#)) Utilizzando la crittografia XTS-AES-256 con NetApp Volume Encryption (NVE) e in-flight con ["Crittografia SMB"](#) O NFS Kerberos 5p. È facile sapere che i trasferimenti di replica tra regioni sono protetti dalla crittografia TLS 1.2 (vedere la sezione ["Replica tra regioni"](#)). Inoltre, Google Networking fornisce anche comunicazioni crittografate (vedere la sezione ["Crittografia dei dati in transito"](#)) per un ulteriore livello di protezione dagli attacchi. Per ulteriori informazioni sulla crittografia del trasporto, vedere la sezione ["Rete Google Cloud"](#).

Protezione dei dati e backup

La sicurezza non riguarda solo la prevenzione degli attacchi. Si tratta anche del modo in cui ripristiniamo gli attacchi in caso o quando si verificano. Questa strategia include backup e protezione dei dati. Cloud Volumes Service fornisce metodi per la replica in altre regioni in caso di interruzioni (vedere la sezione ["Replica tra regioni"](#)) o se un set di dati è interessato da un attacco ransomware. Inoltre, può eseguire backup asincroni dei dati in posizioni esterne all'istanza di Cloud Volumes Service utilizzando ["Backup Cloud Volumes Service"](#). Con backup regolari, la mitigazione degli eventi di sicurezza può richiedere meno tempo e risparmiare denaro e angoscia per gli amministratori.

Riduzione rapida del ransomware con copie Snapshot leader del settore

Oltre alla protezione dei dati e ai backup, Cloud Volumes Service fornisce il supporto per copie Snapshot immutabili (vedere la sezione ["Copie Snapshot immutabili"](#)) di volumi che consentono il ripristino da attacchi ransomware (vedere la sezione ["Funzionamento del servizio"](#)) entro pochi secondi dalla scoperta del problema e con interruzioni minime. I tempi e gli effetti di recovery dipendono dalla pianificazione di Snapshot, ma è possibile creare copie Snapshot che forniscono solo un'ora di delta negli attacchi ransomware. Le copie Snapshot hanno un effetto trascurabile sulle performance e sull'utilizzo della capacità e rappresentano un approccio a basso rischio e con premi elevati per la protezione dei set di dati.

Considerazioni sulla sicurezza e superfici di attacco

Il primo passo per comprendere come proteggere i dati consiste nell'identificare i rischi e le potenziali superfici di attacco.

Questi includono (a titolo esemplificativo) i seguenti elementi:

- Amministrazione e accessi
- Dati inattivi
- Dati in volo
- Rete e firewall
- Ransomware, malware e virus

La comprensione delle superfici di attacco può aiutarti a proteggere meglio i tuoi ambienti. Cloud Volumes Service in Google Cloud prende già in considerazione molti di questi argomenti e implementa le funzionalità di

sicurezza per impostazione predefinita, senza alcuna interazione amministrativa.

Garantire accessi sicuri

Quando si proteggono i componenti critici dell'infrastruttura, è fondamentale assicurarsi che solo gli utenti approvati possano accedere e gestire gli ambienti. Se gli attori danneggiati violano le credenziali amministrative, dispongono delle chiavi del castello e possono fare qualsiasi cosa: Modificare le configurazioni, eliminare volumi e backup, creare backdoor o disattivare le pianificazioni Snapshot.

Cloud Volumes Service per Google Cloud offre protezione dagli accessi amministrativi non autorizzati attraverso l'offuscamento dello storage come servizio (SaaS). Cloud Volumes Service è completamente gestito dal cloud provider senza alcuna disponibilità per l'accesso esterno. Tutte le operazioni di configurazione e configurazione sono completamente automatizzate, pertanto un amministratore umano non deve mai interagire con i sistemi, tranne in circostanze molto rare.

Se è necessario effettuare l'accesso, Cloud Volumes Service in Google Cloud protegge gli accessi mantenendo un elenco molto breve di amministratori attendibili che hanno accesso ai sistemi. Questo gatekeeping aiuta a ridurre il numero di potenziali attori danneggiati con accesso. Inoltre, il networking Google Cloud nasconde i sistemi dietro livelli di sicurezza di rete ed espone solo ciò che è necessario al mondo esterno. Per informazioni sull'architettura di Google Cloud e Cloud Volumes Service, consulta la sezione ["Architettura Cloud Volumes Service".](#)

Amministrazione e aggiornamenti dei cluster

Due aree con potenziali rischi per la sicurezza includono l'amministrazione del cluster (cosa succede se un attore cattivo ha accesso all'amministratore) e gli aggiornamenti (cosa succede se un'immagine software viene compromessa).

Protezione dell'amministrazione dello storage

Lo storage fornito come servizio elimina il rischio aggiunto di esposizione agli amministratori rimuovendo tale accesso agli utenti finali al di fuori del data center cloud. Invece, l'unica configurazione eseguita è per il piano di accesso ai dati da parte dei clienti. Ogni tenant gestisce i propri volumi e nessun tenant può raggiungere altre istanze di Cloud Volumes Service. Il servizio è gestito dall'automazione, con un elenco molto piccolo di amministratori attendibili che hanno accesso ai sistemi attraverso i processi descritti nella sezione ["Operazione di assistenza".](#)

Il tipo di servizio CVS-Performance offre la replica tra regioni come opzione per fornire la protezione dei dati a una regione diversa in caso di guasto di una regione. In questi casi, è possibile eseguire il failover di Cloud Volumes Service nella regione non interessata per mantenere l'accesso ai dati.

Aggiornamenti del servizio

Gli aggiornamenti aiutano a proteggere i sistemi vulnerabili. Ogni aggiornamento offre miglioramenti alla sicurezza e correzioni di bug che riducono al minimo le superfici di attacco. Gli aggiornamenti software vengono scaricati da repository centralizzati e convalidati prima che gli aggiornamenti siano autorizzati a verificare che le immagini ufficiali siano utilizzate e che gli aggiornamenti non siano compromessi dagli attori danneggiati.

Con Cloud Volumes Service, gli aggiornamenti vengono gestiti dai team dei provider di cloud, il che elimina l'esposizione ai rischi per i team di amministratori fornendo esperti con una buona esperienza nella configurazione e negli aggiornamenti che hanno automatizzato e testato completamente il processo. Gli aggiornamenti sono senza interruzioni e Cloud Volumes Service mantiene gli ultimi aggiornamenti per ottenere i migliori risultati complessivi.

Per informazioni sul team di amministratori che esegue questi aggiornamenti del servizio, vedere la sezione [""Operazione di assistenza""](#).

Protezione dei dati inattivi

La crittografia dei dati inattivi è importante per proteggere i dati sensibili in caso di furto, restituzione o riordinamento di un disco. I dati in Cloud Volumes Service sono protetti a riposo utilizzando la crittografia basata su software.

- Le chiavi generate da Google vengono utilizzate per CVS-SW.
- Per CVS-Performance, le chiavi per volume vengono memorizzate in un gestore di chiavi integrato in Cloud Volumes Service, che utilizza NetApp ONTAP CryptoMod per generare chiavi di crittografia AES-256. CryptoMod è elencato nell'elenco dei moduli validati di CMVP FIPS 140-2. Vedere ["FIPS 140-2 Cert n. 4144"](#).

A partire da novembre 2021, l'anteprima della funzionalità Customer-Managed Encryption (CMEK) è stata resa disponibile per CVS-Performance. Questa funzionalità consente di crittografare le chiavi per volume con chiavi master per progetto, per regione, ospitate in Google Key Management Service (KMS). KMS consente di collegare i key manager esterni.

Per ulteriori informazioni su come configurare KMS per CVS-Performance, ["Consultare la documentazione di Cloud Volumes Service"](#).

Per ulteriori informazioni sull'architettura, vedere la sezione [""Architettura Cloud Volumes Service""](#).

Protezione dei dati in volo

Oltre a proteggere i dati a riposo, è necessario essere in grado di proteggere i dati anche quando sono in volo tra l'istanza di Cloud Volumes Service e un client o una destinazione di replica. Cloud Volumes Service fornisce la crittografia per i dati in-flight su protocolli NAS utilizzando metodi di crittografia come la crittografia SMB utilizzando Kerberos, la firma/sigillatura dei pacchetti e NFS Kerberos 5p per la crittografia end-to-end dei trasferimenti di dati.

La replica dei volumi Cloud Volumes Service utilizza TLS 1.2, che sfrutta i metodi di crittografia AES-GCM.

La maggior parte dei protocolli insicuri in-flight, come telnet, NDMP e così via, sono disattivati per impostazione predefinita. Il DNS, tuttavia, non viene crittografato da Cloud Volumes Service (non supporta il DNS sec) e deve essere crittografato utilizzando la crittografia di rete esterna, se possibile. Vedere la sezione [""Crittografia dei dati in transito""](#) per ulteriori informazioni sulla protezione dei dati in volo.

Per informazioni sulla crittografia del protocollo NAS, vedere la sezione [""Protocolli NAS""](#).

Utenti e gruppi per le autorizzazioni NAS

Parte della protezione dei dati nel cloud implica un'autenticazione corretta di utenti e gruppi, in cui gli utenti che accedono ai dati vengono verificati come utenti reali nell'ambiente e i gruppi contengono utenti validi. Questi utenti e gruppi forniscono l'accesso iniziale alla condivisione e all'esportazione, nonché la convalida delle autorizzazioni per file e cartelle nel sistema di storage.

Cloud Volumes Service utilizza l'autenticazione standard di utenti e gruppi basata su Active Directory per le condivisioni SMB e le autorizzazioni di tipo Windows. Il servizio può anche sfruttare i provider di identità UNIX come LDAP per utenti e gruppi UNIX per le esportazioni NFS, la convalida dell'ID NFSv4, l'autenticazione Kerberos e gli ACL NFSv4.



Attualmente solo Active Directory LDAP è supportato con la funzionalità Cloud Volumes Service per LDAP.

Rilevamento, prevenzione e mitigazione di ransomware, malware e virus

Ransomware, malware e virus sono una minaccia persistente per gli amministratori e il rilevamento, la prevenzione e la mitigazione di tali minacce sono sempre in cima alla mente per le organizzazioni aziendali. Un singolo evento ransomware su un set di dati critico può potenzialmente costare milioni di dollari, quindi è utile fare ciò che è possibile per ridurre al minimo il rischio.

Sebbene Cloud Volumes Service attualmente non includa misure di rilevamento o prevenzione native, come la protezione antivirus o. ["rilevamento automatico ransomware"](#), Esistono diversi modi per eseguire rapidamente il ripristino da un evento ransomware attivando pianificazioni Snapshot regolari. Le copie Snapshot sono immutabili e i puntatori di sola lettura ai blocchi modificati nel file system, sono quasi istantanei, hanno un impatto minimo sulle performance e occupano spazio solo quando i dati vengono modificati o cancellati. È possibile impostare le pianificazioni per le copie Snapshot in modo che corrispondano all'obiettivo RPO (Acceptable Recovery Point Objective)/RTO (Recovery Time Objective) desiderato e mantenere fino a 1,024 copie Snapshot per volume.

Il supporto di Snapshot è incluso senza costi aggiuntivi (al di là dei costi di storage dei dati per blocchi modificati/dati conservati dalle copie Snapshot) con Cloud Volumes Service e, in caso di attacco ransomware, può essere utilizzato per eseguire il rollback su una copia Snapshot prima che si verifichi l'attacco. Il completamento dei ripristini Snapshot richiede pochi secondi e consente di tornare alla normale gestione dei dati. Per ulteriori informazioni, vedere ["La soluzione NetApp per ransomware"](#).

Per evitare che il ransomware influisca sul tuo business, è necessario un approccio multilivello che includa uno o più dei seguenti elementi:

- Protezione degli endpoint
- Protezione dalle minacce esterne attraverso firewall di rete
- Rilevamento di anomalie dei dati
- Backup multipli (on-site e off-site) di set di dati critici
- Test di ripristino regolari dei backup
- Copie Snapshot di NetApp immutabili in sola lettura
- Autenticazione a più fattori per infrastrutture critiche
- Controlli di sicurezza degli accessi al sistema

Questo elenco è lungi dall'essere esaustivo, ma è un buon modello da seguire quando si affronta il potenziale degli attacchi ransomware. Cloud Volumes Service in Google Cloud offre diversi modi per proteggere da eventi ransomware e ridurre i loro effetti.

Copie Snapshot immutabili

Cloud Volumes Service fornisce in modo nativo copie Snapshot immutabili in sola lettura, eseguite in base a una pianificazione personalizzabile per un rapido ripristino point-in-time in caso di eliminazione dei dati o se un intero volume è stato vittima di un attacco ransomware. I ripristini Snapshot delle copie Snapshot precedenti sono rapidi e riducono al minimo la perdita di dati in base al periodo di conservazione delle pianificazioni Snapshot e RTO/RPO. L'effetto delle performance con la tecnologia Snapshot è trascurabile.

Poiché le copie Snapshot in Cloud Volumes Service sono di sola lettura, non possono essere infettate dal ransomware a meno che il ransomware non sia proliferato nel dataset senza essere stato notato e siano state

acquisite copie Snapshot dei dati infettati dal ransomware. Per questo motivo è necessario considerare anche il rilevamento ransomware in base alle anomalie dei dati. Cloud Volumes Service non fornisce attualmente il rilevamento nativo, ma è possibile utilizzare un software di monitoraggio esterno.

Backup e ripristini

Cloud Volumes Service offre funzionalità di backup standard del client NAS (ad esempio backup su NFS o SMB).

- CVS-Performance offre replica di volumi cross-region ad altri volumi CVS-Performance. Per ulteriori informazioni, vedere ["replica di un volume"](#) Nella documentazione di Cloud Volumes Service.
- CVS-SW offre funzionalità di backup/ripristino dei volumi native del servizio. Per ulteriori informazioni, vedere ["backup nel cloud"](#) Nella documentazione di Cloud Volumes Service.

La replica dei volumi fornisce una copia esatta del volume di origine per un failover rapido in caso di disastro, inclusi gli eventi ransomware.

Replica tra regioni

CVS-Performance consente di replicare in modo sicuro i volumi nelle aree di Google Cloud per la protezione dei dati e archiviare i casi di utilizzo utilizzando la crittografia TLS1.2 AES 256 GCM su una rete di servizi back-end controllata da NetApp utilizzando interfacce specifiche utilizzate per la replica in esecuzione sulla rete di Google. Un volume primario (di origine) contiene i dati di produzione attivi e replica su un volume secondario (di destinazione) per fornire una replica esatta del dataset primario.

La replica iniziale trasferisce tutti i blocchi, ma gli aggiornamenti trasmettono solo i blocchi modificati in un volume primario. Ad esempio, se un database da 1 TB che risiede su un volume primario viene replicato nel volume secondario, nella replica iniziale viene trasferito 1 TB di spazio. Se il database contiene poche centinaia di righe (ipoteticamente, alcuni MB) che cambiano tra l'inizializzazione e il successivo aggiornamento, solo i blocchi con le righe modificate vengono replicati nel secondario (alcuni MB). In questo modo è possibile garantire che i tempi di trasferimento rimangano bassi e che gli addebiti di replica siano ridotti.

Tutte le autorizzazioni su file e cartelle vengono replicate nel volume secondario, ma le autorizzazioni di accesso alla condivisione (come criteri e regole di esportazione o condivisioni SMB e ACL di condivisione) devono essere gestite separatamente. In caso di failover di un sito, il sito di destinazione deve sfruttare gli stessi name service e le connessioni di dominio Active Directory per fornire una gestione coerente delle identità e delle autorizzazioni di utenti e gruppi. È possibile utilizzare un volume secondario come destinazione di failover in caso di disastro interrompendo la relazione di replica, che converte il volume secondario in lettura/scrittura.

Le repliche dei volumi sono di sola lettura, che fornisce una copia immutabile dei dati fuori sede per un rapido ripristino dei dati nei casi in cui un virus ha infettato i dati o ransomware ha crittografato il dataset primario. I dati di sola lettura non vengono crittografati, ma se il volume primario viene compromesso e si verifica la replica, anche i blocchi infetti vengono replicati. È possibile utilizzare copie Snapshot meno recenti e non interessate per il ripristino, ma gli SLA potrebbero non rientrare nell'intervallo dell'RTO/RPO promesso a seconda della velocità con cui viene rilevato un attacco.

Inoltre, puoi prevenire azioni amministrative dannose, come eliminazioni di volumi, eliminazioni Snapshot o modifiche di pianificazione Snapshot, con la gestione della replica cross-region (CRR) in Google Cloud. Ciò avviene creando ruoli personalizzati che separano gli amministratori dei volumi, che possono eliminare i volumi di origine ma non interrompere i mirror e quindi non eliminare i volumi di destinazione, dagli amministratori CRR, che non possono eseguire alcuna operazione sui volumi. Vedere ["Considerazioni sulla sicurezza"](#) Nella documentazione di Cloud Volumes Service per le autorizzazioni consentite da ciascun gruppo di amministratori.

Backup Cloud Volumes Service

Sebbene Cloud Volumes Service offra un'elevata durata dei dati, gli eventi esterni possono causare la perdita di dati. In caso di eventi di sicurezza come virus o ransomware, i backup e i ripristini diventano critici per la ripresa dell'accesso ai dati in modo tempestivo. Un amministratore potrebbe eliminare accidentalmente un volume Cloud Volumes Service. In alternativa, gli utenti vogliono semplicemente conservare le versioni di backup dei propri dati per molti mesi e mantenere lo spazio di copia Snapshot aggiuntivo all'interno del volume diventa una sfida in termini di costi. Sebbene le copie Snapshot siano il modo migliore per conservare le versioni di backup delle ultime settimane per ripristinare i dati persi, sono contenute all'interno del volume e vengono perse se il volume scompare.

Per tutti questi motivi, NetApp Cloud Volumes Service offre servizi di backup tramite ["Backup Cloud Volumes Service"](#).

Il backup di Cloud Volumes Service genera una copia del volume su Google Cloud Storage (GCS). Esegue il backup solo dei dati effettivi memorizzati nel volume, non dello spazio libero. Funziona come incrementale per sempre, il che significa che trasferisce il contenuto del volume una volta e da lì continua a eseguire il backup solo dei dati modificati. Rispetto ai classici concetti di backup con più backup completi, consente di risparmiare grandi quantità di storage di backup, riducendo i costi. Poiché il prezzo mensile dello spazio di backup è inferiore rispetto a un volume, è il posto ideale per mantenere le versioni di backup più a lungo.

Gli utenti possono utilizzare un backup Cloud Volumes Service per ripristinare qualsiasi versione di backup sullo stesso volume o su un volume diverso all'interno della stessa regione. Se il volume di origine viene cancellato, i dati di backup vengono conservati e devono essere gestiti (ad esempio, eliminati) in modo indipendente.

Il backup Cloud Volumes Service è integrato in Cloud Volumes Service come opzione. Gli utenti possono decidere quali volumi proteggere attivando il backup Cloud Volumes Service per volume. Vedere ["Documentazione di backup di Cloud Volumes Service"](#) per informazioni sui backup, consultare ["numero massimo di versioni di backup supportate"](#), pianificazione e ["prezzi"](#).

Tutti i dati di backup di un progetto vengono memorizzati all'interno di un bucket GCS, gestito dal servizio e non visibile all'utente. Ogni progetto utilizza un bucket diverso. Attualmente, i bucket si trovano nella stessa regione dei volumi Cloud Volumes Service, ma sono in corso di discussione ulteriori opzioni. Consultare la documentazione per conoscere lo stato più recente.

Il trasporto dei dati da un bucket Cloud Volumes Service a GCS utilizza reti Google interne al servizio con HTTPS e TLS1.2. I dati vengono crittografati a riposo con chiavi gestite da Google.

Per gestire il backup Cloud Volumes Service (creazione, eliminazione e ripristino dei backup), un utente deve disporre di ["roles/netappcloudvolumes.admin"](#) ruolo.

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

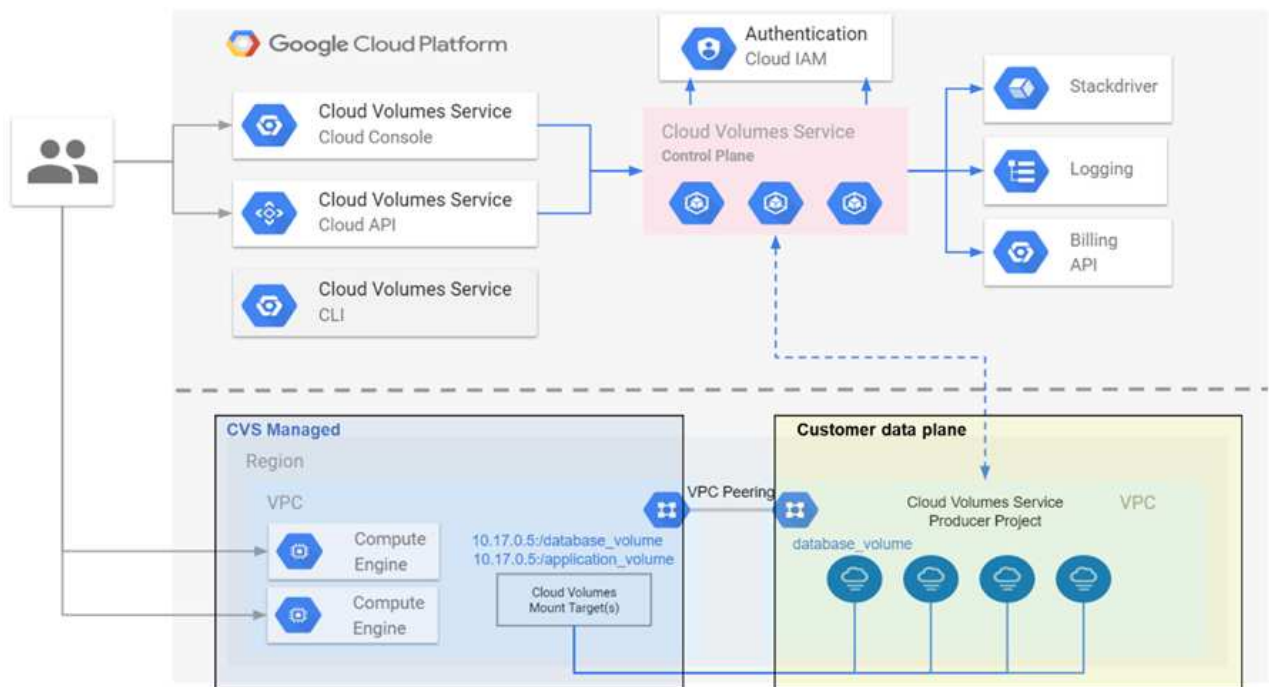
Il piano dati di Cloud Volumes Service include i volumi di dati effettivi e la configurazione generale di Cloud Volumes Service (ad esempio controllo degli accessi, autenticazione Kerberos e così via). Il data plane è interamente sotto il controllo degli utenti finali e dei consumatori della piattaforma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

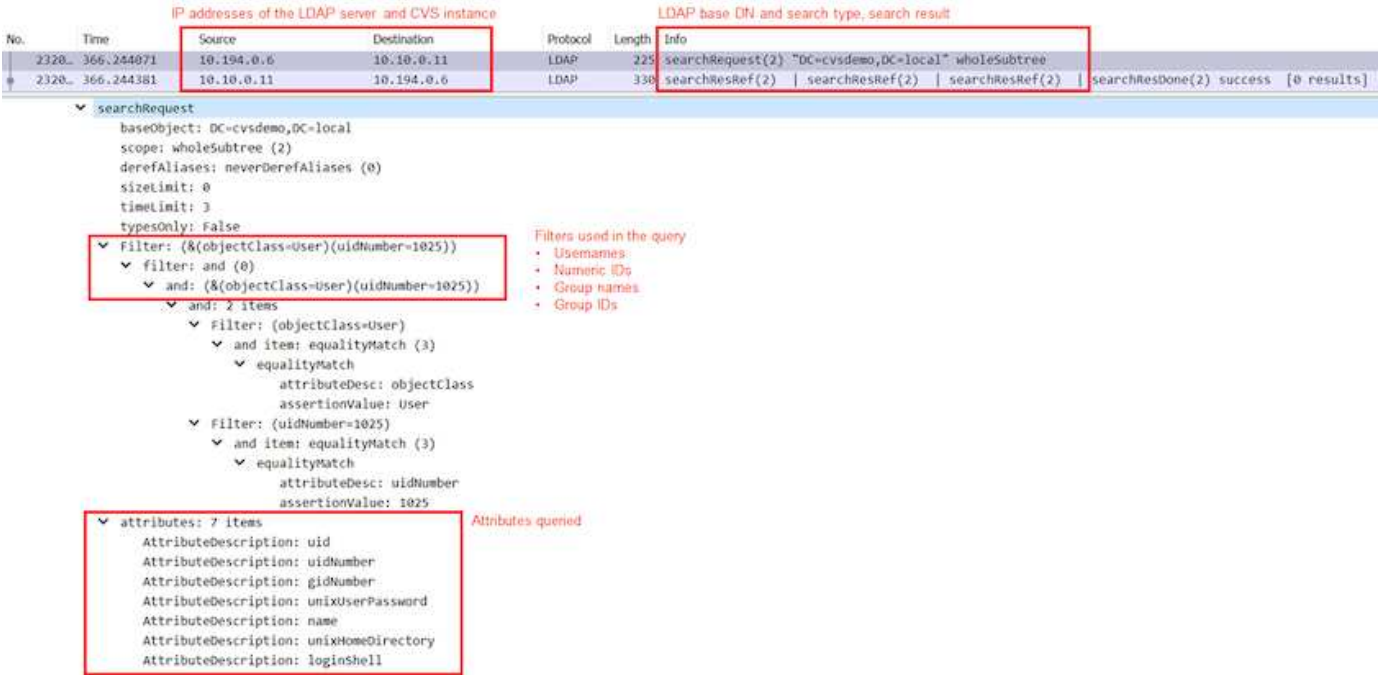
In breve, il data plane Cloud Volumes Service offre la funzionalità di controllo dell'accesso alla rete, senza il requisito di supportare i controlli dei servizi VPC e non utilizza esplicitamente i controlli dei servizi VPC.

Considerazioni su sniffing/tracce 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.

		IP addresses of the NFS client and CVS instance		Genericized NFS call/reply		
No.	Time	Source	Destination	Protocol	Length	Info
380	9.218014	10.193.67.225	10.193.67.219	NFS	346	V4 Call (Reply In 381)
381	9.218480	10.193.67.219	10.193.67.225	NFS	426	V4 Reply (Call In 380)
382	9.218641	10.193.67.225	10.193.67.219	NFS	370	V4 Call (Reply In 397)
397	9.369035	10.193.67.219	10.193.67.225	NFS	458	V4 Reply (Call In 382)

> Frame 381: 426 bytes on wire (3408 bits), 426 bytes captured (3408 bits)
 > Ethernet II, Src: IntelCor_7f:da:bc (90:e2:ba:7f:da:bc), Dst: VMware_a0:2c:2d (00:50:56:a0:2c:2d)
 > Internet Protocol Version 4, Src: 10.193.67.219, Dst: 10.193.67.225
 > Transmission Control Protocol, Src Port: 2049, Dst Port: 738, Seq: 6305, Ack: 6569, Len: 360
 > Remote Procedure Call, Type:Reply, XID:0xef5e998d

GSS-Wrapper
 Length: 300
 GSS Data: 050407ff000000000000000025913451ee1d43d298cf3031...
 > krb5_blob: 050407ff000000000000000025913451ee1d43d298cf3031...
 Network File System
 [Program Version: 4]
 [V4 Procedure: COMPOUND (1)]

GSS wrapped NFS calls/replies with no other identifying information

		IP addresses of the NFS client and CVS instance		Detailed NFS call types and file handle information		
No.	Time	Source	Destination	Protocol	Length	Info
33	0.958480	10.193.67.201	10.193.67.204	NFS	458	V4 Reply (Call In 32) OPEN StateID: 0x0481
34	0.958784	10.193.67.204	10.193.67.201	NFS	306	V4 Call (Reply In 35) SETATTR FH: 0x6c07918a
35	0.959284	10.193.67.201	10.193.67.204	NFS	358	V4 Reply (Call In 34) SETATTR

> Opcode: PUTFH (22)
 > Opcode: SETATTR (34)
 > Opcode: GETATTR (9)
 Status: NFS4_OK (0)
 Attr mask[0]: 0x0010011a (Type, Change, Size, FSID, FileId)
 > reqd_attr: Type (1)
 > reqd_attr: Change (3)
 > reqd_attr: Size (4)
 > reqd_attr: FSID (8)
 > reco_attr: FileId (20) File ID
 fileid: 9232254136597092620
 Attr mask[1]: 0x00b0a03a (Mode, NumLinks, Owner, Owner_Group, Space_Used, Time_Access, Time_Metadata, Time_Modify, Mounted_on_FileId)
 > reco_attr: Mode (33) Permission information
 > mode: 0644, Name: Unknown, Read permission for owner, Write permission for owner, Read permission for group, Read permission for others
 > reco_attr: NumLinks (35)
 > reco_attr: Owner (36) Owner and group ID strings
 > fattr4_owner: root@NTAP.LOCAL
 > reco_attr: Owner_Group (37)
 > fattr4_owner_group: root@NTAP.LOCAL
 > reco_attr: Space_Used (45)
 > reco_attr: Time_Access (47)
 > reco_attr: Time_Metadata (52)
 > reco_attr: Time_Modify (53)
 > reco_attr: Mounted_on_FileId (55)

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

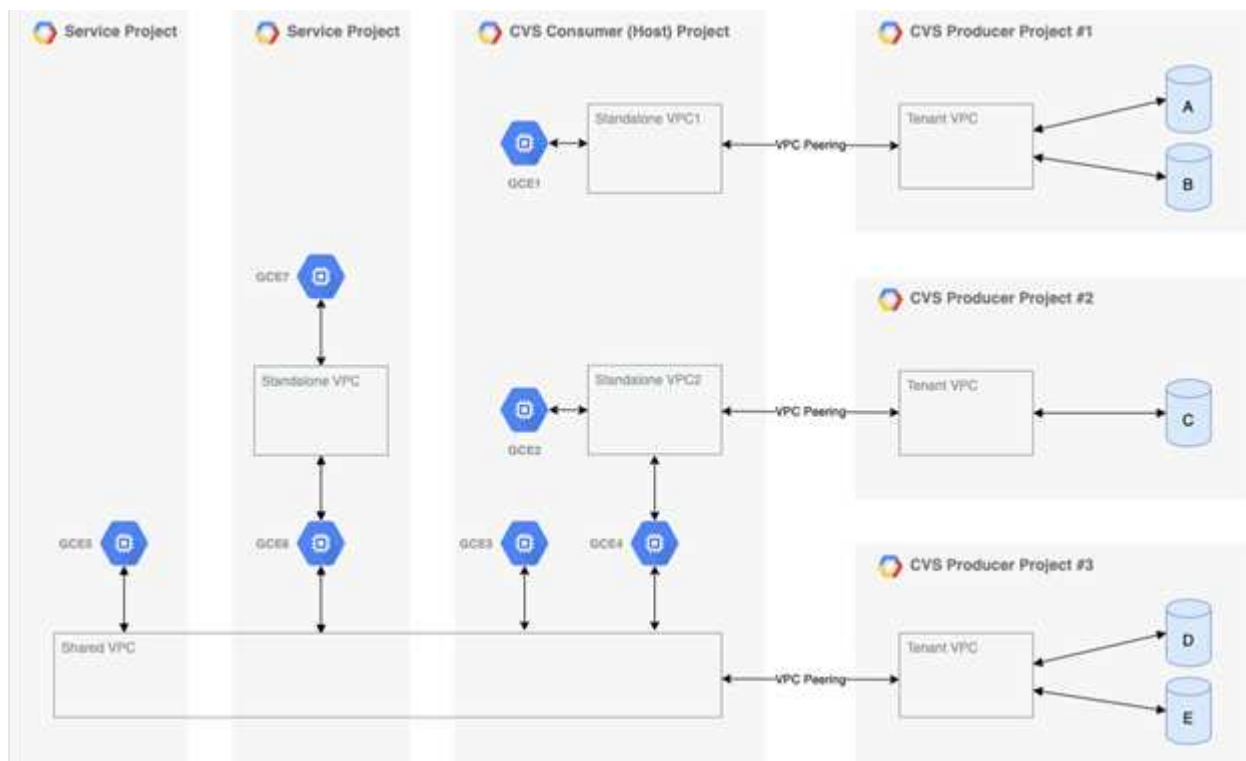
Attualmente, non sono disponibili registri di audit del piano di controllo accessibili dall'utente.

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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Ideale per la maggior parte dei casi
NFSv4.x: SIS	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none"> • 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) 	<ul style="list-style-type: none"> • Migliore nella maggior parte dei casi per Kerberos; peggiore di AUTH_SYS

Livello di sicurezza	Sicurezza	Performance
NFS: Krb5i	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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) 	<ul style="list-style-type: none"> • 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 ["configurate"](#) 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"](#).

Protocolli NAS

Panoramica dei protocolli NAS

I protocolli NAS includono NFS (v3 e v4.1) e SMB/CIFS (2.x e 3.x). Questi protocolli sono il modo in cui CVS consente l'accesso condiviso ai dati tra più client NAS. Inoltre, Cloud Volumes Service può fornire l'accesso simultaneo ai client NFS e SMB/CIFS (dual-Protocol) rispettando tutte le impostazioni di identità e autorizzazioni su file e cartelle nelle condivisioni NAS. Per mantenere la massima sicurezza possibile per il trasferimento dei dati, Cloud Volumes Service supporta la crittografia del protocollo in uso con la crittografia SMB e NFS Kerberos 5p.



Dual-Protocol è disponibile solo con CVS-Performance.

Nozioni di base sui protocolli NAS

I protocolli NAS consentono a più client su una rete di accedere agli stessi dati su un sistema storage, ad esempio Cloud Volumes Service su GCP. NFS e SMB sono i protocolli NAS definiti e operano su base client/server, dove Cloud Volumes Service agisce come server. I client inviano al server richieste di accesso, lettura e scrittura e il server è responsabile del coordinamento dei meccanismi di blocco dei file, dell'archiviazione delle autorizzazioni e della gestione delle richieste di identità e

autenticazione.

Ad esempio, se un client NAS desidera creare un nuovo file in una cartella, viene seguita la seguente procedura generale.

1. Il client richiede al server informazioni sulla directory (permessi, proprietario, gruppo, ID file, spazio disponibile, e così via); il server risponde con le informazioni se il client richiedente e l'utente hanno le autorizzazioni necessarie sulla cartella padre.
2. Se le autorizzazioni sulla directory consentono l'accesso, il client chiede al server se il nome del file creato esiste già nel file system. Se il nome del file è già in uso, la creazione non riesce. Se il nome del file non esiste, il server comunica al client che può procedere.
3. Il client invia una chiamata al server per creare il file con l'handle di directory e il nome del file e imposta l'accesso e i tempi di modifica. Il server invia un ID file univoco al file per assicurarsi che non vengano creati altri file con lo stesso ID.
4. Il client invia una chiamata per controllare gli attributi del file prima dell'operazione DI SCRITTURA. Se le autorizzazioni lo consentono, il client scrive il nuovo file. Se il protocollo/applicazione utilizza il blocco, il client richiede al server un blocco per impedire ad altri client di accedere al file mentre sono bloccati per evitare il danneggiamento dei dati.

NFS

NFS è un protocollo di file system distribuito che è uno standard IETF aperto definito in Request for Comments (RFC) che consente a chiunque di implementare il protocollo.

I volumi in Cloud Volumes Service vengono condivisi ai client NFS esportando un percorso accessibile a un client o a un set di client. Le autorizzazioni per montare queste esportazioni sono definite da policy e regole di esportazione, configurabili dagli amministratori di Cloud Volumes Service.

L'implementazione NetApp NFS è considerata uno standard di riferimento per il protocollo e viene utilizzata in innumerevoli ambienti NAS aziendali. Le sezioni seguenti illustrano NFS e le funzionalità di sicurezza specifiche disponibili in Cloud Volumes Service e le relative modalità di implementazione.

Utenti e gruppi UNIX locali predefiniti

Cloud Volumes Service contiene diversi utenti e gruppi UNIX predefiniti per varie funzionalità di base. Questi utenti e gruppi non possono essere modificati o cancellati. Non è possibile aggiungere nuovi utenti e gruppi locali a Cloud Volumes Service. Gli utenti e i gruppi UNIX al di fuori degli utenti e dei gruppi predefiniti devono essere forniti da un name service LDAP esterno.

La seguente tabella mostra gli utenti e i gruppi predefiniti e i relativi ID numerici. NetApp consiglia di non creare nuovi utenti o gruppi in LDAP o sui client locali che riutilizzano questi ID numerici.

Utenti predefiniti: ID numerici	Gruppi predefiniti: ID numerici
<ul style="list-style-type: none">• root:0• pcuser:65534• nessuno:65535	<ul style="list-style-type: none">• root:0• demone:1• pcuser:65534• nessuno:65535



Quando si utilizza NFSv4.1, l'utente root potrebbe essere visualizzato come nessuno quando si eseguono comandi di elenco di directory sui client NFS. Ciò è dovuto alla configurazione del mapping del dominio ID del client. Vedere la sezione chiamata [NFSv4.1 e l'utente/gruppo nessuno](#) per informazioni dettagliate su questo problema e su come risolverlo.

L'utente root

In Linux, l'account root ha accesso a tutti i comandi, file e cartelle in un file system basato su Linux. A causa della potenza di questo account, le Best practice di sicurezza spesso richiedono che l'utente root sia disattivato o limitato in qualche modo. Nelle esportazioni NFS, il potere di un utente root sui file e sulle cartelle può essere controllato in Cloud Volumes Service attraverso policy e regole di esportazione e un concetto noto come root squash.

Lo squashing root garantisce che l'utente root che accede a un montaggio NFS venga bloccato dall'utente numerico anonimo 65534 (vedere la sezione "[L'utente anonimo](#)") ed è attualmente disponibile solo quando si utilizza CVS-Performance selezionando Off per l'accesso root durante la creazione della regola dei criteri di esportazione. Se l'utente root viene bloccato nell'utente anonimo, non ha più accesso per eseguire chown o. "[comandi setuid/setgid \(il bit adesivo\)](#)" Su file o cartelle nel montaggio NFS, e i file o le cartelle creati dall'utente root mostrano l'UID anon come proprietario/gruppo. Inoltre, gli ACL NFSv4 non possono essere modificati dall'utente root. Tuttavia, l'utente root ha ancora accesso a chmod e ha eliminato i file per i quali non dispone di permessi espliciti. Se si desidera limitare l'accesso ai permessi di file e cartelle di un utente root, si consiglia di utilizzare un volume con ACL NTFS, creando un utente Windows denominato `root` e applicando le autorizzazioni desiderate ai file o alle cartelle.

L'utente anonimo

L'ID utente anonimo (anon) specifica un ID utente o un nome utente UNIX mappato alle richieste del client che arrivano senza credenziali NFS valide. Questo può includere l'utente root quando viene utilizzato lo squashing root. L'utente anon in Cloud Volumes Service è 65534.

Questo UID è normalmente associato al nome utente `nobody` oppure `nfsnobody` Negli ambienti Linux. Cloud Volumes Service utilizza anche 65534 come utente UNIX locale `pcuser` (vedere la sezione "[Utenti e gruppi UNIX locali predefiniti](#)"), che è anche l'utente di fallback predefinito per le mappature dei nomi da Windows a UNIX quando non è possibile trovare un utente UNIX valido corrispondente in LDAP.

A causa delle differenze nei nomi utente di Linux e Cloud Volumes Service per UID 65534, la stringa del nome per gli utenti mappati a 65534 potrebbe non corrispondere quando si utilizza NFSv4.1. Di conseguenza, potresti vedere `nobody` come utente di alcuni file e cartelle. Vedere la sezione "[NFSv4.1 e l'utente/gruppo nessuno](#)" per informazioni su questo problema e su come risolverlo.

Controllo degli accessi/esportazioni

L'accesso iniziale all'esportazione/condivisione per i montaggi NFS è controllato attraverso regole di policy di esportazione basate su host contenute in una policy di esportazione. Viene definito un IP host, un nome host, una subnet, un netgroup o un dominio per consentire l'accesso per montare la condivisione NFS e il livello di accesso consentito all'host. Le opzioni di configurazione delle regole dei criteri di esportazione dipendono dal livello Cloud Volumes Service.

Per CVS-SW, sono disponibili le seguenti opzioni per la configurazione dei criteri di esportazione:

- **Corrispondenza client.** elenco separato da virgole di indirizzi IP, elenco separato da virgole di nomi host, subnet, netgroup, nomi di dominio.
- **RO/RW access rules.** selezionare Read/write o Read only per controllare il livello di accesso all'esportazione. CVS-Performance offre le seguenti opzioni:

- **Corrispondenza client.** elenco separato da virgole di indirizzi IP, elenco separato da virgole di nomi host, subnet, netgroup, nomi di dominio.
- **RO/RW access rules.** selezionare Read/write o Read only per controllare il livello di accesso all'esportazione.
- **Root access (on/off).** configura root squash (vedere la sezione "[L'utente root](#)" per ulteriori informazioni).
- **Protocol type.** (tipo di protocollo): Limita l'accesso al montaggio NFS a una versione specifica del protocollo. Quando si specificano NFSv3 e NFSv4.1 per il volume, lasciare entrambe le caselle vuote o selezionare entrambe le caselle.
- **Livello di sicurezza Kerberos (quando si seleziona Enable Kerberos).** fornisce le opzioni krb5, krb5i e/o krb5p per l'accesso in sola lettura o in lettura/scrittura.

Modifica proprietà (chown) e gruppo di cambiamento (chgrp)

NFS su Cloud Volumes Service consente solo all'utente root di eseguire chown/chgrp su file e cartelle. Altri utenti visualizzano un `Operation not permitted` errore: anche sui file di loro proprietà. Se si utilizza il root squash (come descritto nella sezione "[L'utente root](#)"), la root viene bloccata in un utente non root e non è consentito l'accesso a chown e chgrp. Attualmente non esistono soluzioni alternative in Cloud Volumes Service per consentire chown e chgrp agli utenti non root. Se sono necessarie modifiche alla proprietà, prendere in considerazione l'utilizzo di volumi a doppio protocollo e impostare lo stile di protezione su NTFS per controllare le autorizzazioni dal lato Windows.

Gestione delle autorizzazioni

Cloud Volumes Service supporta entrambi i bit di modalità (come 644, 777 e così via per rwx) e gli ACL NFSv4.1 per controllare le autorizzazioni sui client NFS per i volumi che utilizzano lo stile di sicurezza UNIX. La gestione dei permessi standard viene utilizzata per questi (come chmod, chown o nfs4_setfacl) e funziona con qualsiasi client Linux che li supporti.

Inoltre, quando si utilizzano volumi a doppio protocollo impostati su NTFS, i client NFS possono sfruttare la mappatura dei nomi Cloud Volumes Service per gli utenti Windows, che vengono poi utilizzati per risolvere le autorizzazioni NTFS. Questo richiede una connessione LDAP a Cloud Volumes Service per fornire traduzioni da ID numerico a nome utente, in quanto Cloud Volumes Service richiede un nome utente UNIX valido per eseguire correttamente il mapping a un nome utente Windows.

Fornitura di ACL granulari per NFSv3

Le autorizzazioni di bit di modalità coprono solo proprietario, gruppo e tutti gli altri membri della semantica, il che significa che non esistono controlli granulari degli accessi utente per NFSv3 di base. Cloud Volumes Service non supporta gli ACL POSIX, né gli attributi estesi (come chattr), pertanto gli ACL granulari sono possibili solo nei seguenti scenari con NFSv3:

- Volumi di sicurezza NTFS (server CIFS richiesto) con mappature valide da UNIX a utenti Windows.
- Gli ACL NFSv4.1 vengono applicati utilizzando un client di amministrazione che monta NFSv4.1 per applicare gli ACL.

Entrambi i metodi richiedono una connessione LDAP per la gestione delle identità UNIX e un utente UNIX valido e informazioni di gruppo compilate (vedere la sezione "[LDAP](#)"). E sono disponibili solo con istanze CVS-Performance. Per utilizzare i volumi di sicurezza NTFS con NFS, è necessario utilizzare il protocollo doppio (SMB e NFSv3) o il protocollo doppio (SMB e NFSv4.1), anche se non vengono effettuate connessioni SMB. Per utilizzare gli ACL NFSv4.1 con i montaggi NFSv3, selezionare `Both (NFSv3/NFSv4.1)` come tipo di protocollo.

I bit in modalità UNIX standard non forniscono lo stesso livello di granularità delle autorizzazioni fornite dagli ACL NTFS o NFSv4.x. La tabella seguente confronta la granularità delle autorizzazioni tra i bit di modalità NFSv3 e gli ACL NFSv4.1. Per informazioni sugli ACL NFSv4.1, vedere ["Nfs4_acl - elenchi di controllo degli accessi NFSv4"](#).

Bit di modalità NFSv3	ACL NFSv4.1
<ul style="list-style-type: none"> • Impostare l'ID utente all'esecuzione • Impostare l'ID del gruppo all'esecuzione • Salva testo scambiato (non definito in POSIX) • Permesso di lettura per il proprietario • Permesso di scrittura per il proprietario • Autorizzazione di esecuzione per il proprietario di un file o autorizzazione di ricerca per il proprietario nella directory • Permesso di lettura per il gruppo • Permesso di scrittura per il gruppo • Autorizzazione di esecuzione per il gruppo su un file o autorizzazione di ricerca (ricerca) per il gruppo nella directory • Permesso di lettura per altri • Permesso di scrittura per altri • Autorizzazione di esecuzione per altri utenti su un file o autorizzazione di ricerca per altri utenti nella directory 	<p>Tipi di voci di controllo di accesso (ACE) (Allow/Nega/Audit) * flag di ereditarietà * eredità di directory * eredità di file * nessuna propagazione-eredità * eredità-solo</p> <p>Permessi * Read-data (file) / list-directory (directory) * write-data (file) / create-file (directory) * append-data (file) / create-subdirectory (directory) * execute (file) / change-directory (directory) * delete * delete-child * Read-attribute * write-attribute * Read-named-attribute * write-named * Read-ACL *-synchronize *-owner *-synchronize * -ACL *-synchronize *-lire</p>

Infine, l'appartenenza al gruppo NFS (sia in NFSv3 che in NFSv4.x) è limitata a un massimo predefinito di 16 per AUTH_SYS in base ai limiti dei pacchetti RPC. NFS Kerberos fornisce fino a 32 gruppi e gli ACL NFSv4 eliminano la limitazione attraverso ACL granulari di utenti e gruppi (fino a 1024 voci per ACE).

Inoltre, Cloud Volumes Service offre un supporto esteso per gruppi per estendere il numero massimo di gruppi supportati fino a 32. Questa operazione richiede una connessione LDAP a un server LDAP che contenga identità di gruppo e utenti UNIX valide. Per ulteriori informazioni sulla configurazione, vedere ["Creazione e gestione di volumi NFS"](#) Nella documentazione di Google.

ID utente e gruppo NFSv3

Gli ID utente e di gruppo NFSv3 vengono trasmessi in rete come ID numerici anziché come nomi. Cloud Volumes Service non risolve i nomi utente per questi ID numerici con NFSv3, con volumi di sicurezza UNIX che utilizzano solo i bit di modalità. Quando sono presenti ACL NFSv4.1, per risolvere correttamente l'ACL è necessario eseguire una ricerca di ID numerici e/o stringhe di nomi, anche quando si utilizza NFSv3. Con i volumi di sicurezza NTFS, Cloud Volumes Service deve risolvere un ID numerico a un utente UNIX valido e quindi eseguire il mapping a un utente Windows valido per negoziare i diritti di accesso.

Limitazioni di sicurezza degli ID utente e di gruppo NFSv3

Con NFSv3, il client e il server non devono mai confermare che l'utente che tenta una lettura o una scrittura con un ID numerico sia un utente valido; è semplicemente implicitamente attendibile. In questo modo, il file system si apre a potenziali violazioni semplicemente eseguendo lo spoofing di qualsiasi ID numerico. Per

evitare falle di sicurezza come questa, sono disponibili alcune opzioni per Cloud Volumes Service.

- L'implementazione di Kerberos per NFS obbliga gli utenti ad autenticarsi con un nome utente e una password o un file keytab per ottenere un ticket Kerberos per consentire l'accesso a un mount. Kerberos è disponibile con istanze CVS-Performance e solo con NFSv4.1.
- La limitazione dell'elenco di host nelle regole dei criteri di esportazione limita i client NFSv3 che hanno accesso al volume Cloud Volumes Service.
- L'utilizzo di volumi a doppio protocollo e l'applicazione di ACL NTFS al volume obbliga i client NFSv3 a risolvere gli ID numerici dei nomi utente UNIX validi per autenticarsi correttamente per accedere ai montaggi. Ciò richiede l'abilitazione di LDAP e la configurazione delle identità di utenti e gruppi UNIX.
- Lo squashing dell'utente root limita i danni che un utente root può fare a un montaggio NFS, ma non rimuove completamente i rischi. Per ulteriori informazioni, vedere la sezione "[L'utente root](#)."

In ultima analisi, la sicurezza NFS è limitata alla versione del protocollo in uso. NFSv3, pur essendo più performante in generale rispetto a NFSv4.1, non fornisce lo stesso livello di sicurezza.

NFSv4.1

NFSv4.1 offre maggiore sicurezza e affidabilità rispetto a NFSv3, per i seguenti motivi:

- Blocco integrato attraverso un meccanismo basato sul lease
- Sessioni stateful
- Tutte le funzionalità NFS su una singola porta (2049)
- Solo TCP
- Mapping del dominio ID
- Integrazione Kerberos (NFSv3 può utilizzare Kerberos, ma solo per NFS, non per protocolli ausiliari come NLM)

Dipendenze NFSv4.1

A causa delle funzionalità di sicurezza aggiuntive di NFSv4.1, sono coinvolte alcune dipendenze esterne che non erano necessarie per utilizzare NFSv3 (in modo simile a come SMB richiede dipendenze come Active Directory).

ACL NFSv4.1

Cloud Volumes Service offre il supporto per ACL NFSv4.x, che offrono vantaggi distinti rispetto alle normali autorizzazioni POSIX, come ad esempio:

- Controllo granulare dell'accesso degli utenti a file e directory
- Maggiore sicurezza NFS
- Maggiore interoperabilità con CIFS/SMB
- Rimozione del limite NFS di 16 gruppi per utente con sicurezza AUTH_SYS
- Gli ACL evitano la necessità di risoluzione degli ID di gruppo (GID), che rimuove efficacemente i GID limitNLSSv4.1 ACL sono controllati dai client NFS, non da Cloud Volumes Service. Per utilizzare gli ACL NFSv4.1, assicurarsi che la versione software del client li supporti e che siano installate le utility NFS appropriate.

Compatibilità tra ACL NFSv4.1 e client SMB

Gli ACL NFSv4 sono diversi dagli ACL a livello di file di Windows (ACL NTFS) ma presentano funzionalità simili. Tuttavia, in ambienti NAS multiprotocollo, se sono presenti ACL NFSv4.1 e si utilizza l'accesso a doppio protocollo (NFS e SMB sugli stessi set di dati), i client che utilizzano SMB2.0 e versioni successive non saranno in grado di visualizzare o gestire gli ACL dalle schede di sicurezza di Windows.

Come funzionano gli ACL NFSv4.1

Per riferimento, vengono definiti i seguenti termini:

- **Elenco di controllo di accesso (ACL).** elenco di voci delle autorizzazioni.
- **Voce di controllo di accesso (ACE).** una voce di autorizzazione nell'elenco.

Quando un client imposta un ACL NFSv4.1 su un file durante un'operazione SETATTR, Cloud Volumes Service imposta tale ACL sull'oggetto, sostituendo qualsiasi ACL esistente. Se un file non contiene ACL, le autorizzazioni di modalità per il file vengono calcolate dal PROPRIETARIO@, DAL GRUPPO@ e DA EVERYONE@. Se nel file sono presenti SUID/SGID/bit ADESIVI, questi non vengono influenzati.

Quando un client ottiene un ACL NFSv4.1 su un file durante un'operazione GETATTR, Cloud Volumes Service legge l'ACL NFSv4.1 associato all'oggetto, costruisce un elenco di ACE e restituisce l'elenco al client. Se il file ha un ACL NT o bit di modalità, un ACL viene costruito dai bit di modalità e restituito al client.

L'accesso viene negato se nell'ACL è presente un ACE DI NEGAZIONE; l'accesso viene concesso se esiste un ACE DI AUTORIZZAZIONE. Tuttavia, l'accesso viene negato anche se nessuna delle ACE è presente nell'ACL.

Un descrittore di sicurezza è costituito da un ACL di sicurezza (SACL) e da un ACL discrezionale (DACL). Quando NFSv4.1 interagisce con CIFS/SMB, il DACL viene mappato uno a uno con NFSv4 e CIFS. Il DACL è costituito dalle ACE DI AUTORIZZAZIONE e NEGAZIONE.

Se di base `chmod` Viene eseguito su un file o una cartella con gli ACL NFSv4.1 impostati, gli ACL degli utenti e dei gruppi esistenti vengono mantenuti, ma gli ACL PREDEFINITI DI PROPRIETARIO@, GRUPPO@, EVERYONE@ vengono modificati.

Un client che utilizza ACL NFSv4.1 può impostare e visualizzare ACL per file e directory nel sistema. Quando viene creato un nuovo file o sottodirectory in una directory che dispone di un ACL, tale oggetto eredita tutte le ACE nell'ACL che sono state contrassegnate con il appropriato ["flag di ereditarietà"](#).

Se un file o una directory dispone di un ACL NFSv4.1, tale ACL viene utilizzato per controllare l'accesso indipendentemente dal protocollo utilizzato per accedere al file o alla directory.

File e directory ereditano ACE da ACL NFSv4 nelle directory principali (possibilmente con modifiche appropriate), purché gli ACE siano stati contrassegnati con i flag di ereditarietà corretti.

Quando viene creato un file o una directory come risultato di una richiesta NFSv4, l'ACL del file o della directory risultante dipende dal fatto che la richiesta di creazione del file includa un ACL o solo permessi di accesso ai file UNIX standard. L'ACL dipende anche dalla presenza o meno di un ACL nella directory principale.

- Se la richiesta include un ACL, viene utilizzato tale ACL.
- Se la richiesta include solo le autorizzazioni di accesso ai file UNIX standard e la directory principale non dispone di un ACL, la modalità file client viene utilizzata per impostare le autorizzazioni di accesso ai file UNIX standard.

- Se la richiesta include solo le autorizzazioni di accesso ai file UNIX standard e la directory principale dispone di un ACL non ereditabile, un ACL predefinito basato sui bit di modalità passati alla richiesta viene impostato sul nuovo oggetto.
- Se la richiesta include solo autorizzazioni di accesso ai file UNIX standard ma la directory principale dispone di un ACL, le ACE nell'ACL della directory principale vengono ereditate dal nuovo file o directory, purché le ACE siano state contrassegnate con gli indicatori di ereditarietà appropriati.

Autorizzazioni ACE

Le autorizzazioni ACL NFSv4.1 utilizzano una serie di valori di lettere maiuscole e minuscole (ad esempio `rxtnCy`) per controllare l'accesso. Per ulteriori informazioni sui valori delle lettere, vedere ["PROCEDURA: Utilizzare l'ACL NFSv4"](#).

Comportamento dell'ACL di NFSv4.1 con ereditarietà di umask e ACL

["Gli ACL NFSv4 offrono l'ereditarietà degli ACL"](#). L'ereditarietà degli ACL indica che i file o le cartelle creati sotto gli oggetti con gli ACL NFSv4.1 impostati possono ereditare gli ACL in base alla configurazione di ["Flag di ereditarietà ACL"](#).

["Umask"](#) viene utilizzato per controllare il livello di autorizzazione al quale i file e le cartelle vengono creati in una directory senza l'intervento dell'amministratore. Per impostazione predefinita, Cloud Volumes Service consente a umask di eseguire l'override degli ACL ereditati, il che è un comportamento previsto come indicato in ["RFC 5661"](#).

Formattazione ACL

Gli ACL NFSv4.1 hanno una formattazione specifica. Il seguente esempio è un insieme ACE su un file:

```
A::ldapuser@domain.netapp.com:rwatTnNcCy
```

L'esempio precedente segue le linee guida del formato ACL di:

```
type:flags:principal:permissions
```

Un tipo di A significa "consenti". In questo caso, i flag Inherit non vengono impostati, in quanto l'entità non è un gruppo e non include l'ereditarietà. Inoltre, poiché l'ACE non è una voce DI AUDIT, non è necessario impostare gli indicatori di audit. Per ulteriori informazioni sugli ACL NFSv4.1, vedere ["http://linux.die.net/man/5/nfs4_acl"](http://linux.die.net/man/5/nfs4_acl).

Se l'ACL NFSv4.1 non è impostato correttamente (o una stringa di nomi non può essere risolta dal client e dal server), l'ACL potrebbe non funzionare come previsto oppure la modifica dell'ACL potrebbe non essere applicata e generare un errore.

Gli errori di esempio includono:

```
Failed setxattr operation: Invalid argument
Scanning ACE string 'A:: user@rwaDxtTnNcCy' failed.
```

NEGARE esplicitamente

Le autorizzazioni NFSv4.1 possono includere attributi DI NEGAZIONE esplicita per PROPRIETARIO, GRUPPO e CHIUNQUE. Ciò è dovuto al fatto che gli ACL di NFSv4.1 sono di tipo default-deny, il che significa che se un ACL non viene esplicitamente concesso da un ACE, viene negato. Gli attributi DI NEGAZIONE esplicita sovrascrivono le ACE DI ACCESSO, esplicite o meno.

GLI ACE DI NEGAZIONE vengono impostati con un tag di attributo di D.

Nell'esempio riportato di seguito, IL GRUPPO@ può disporre di tutte le autorizzazioni di lettura ed esecuzione, ma non di tutti gli accessi in scrittura.

```
sh-4.1$ nfs4_getfacl /mixed
A::ldapuser@domain.netapp.com:ratTnNcCy
A::OWNER@:rwaDxtTnNcCy
D::OWNER@:
A:g:GROUP@:rxtncy
D:g:GROUP@:waDTC
A::EVERYONE@:rxtncy
D::EVERYONE@:waDTC
```

GLI ACE DI NEGAZIONE devono essere evitati ogni volta che è possibile perché possono essere confusi e complicati; GLI ACL CHE NON sono esplicitamente definiti sono implicitamente negati. Quando si impostano LE ACE DI NEGAZIONE, agli utenti potrebbe essere negato l'accesso quando si prevede di ottenere l'accesso.

Il set precedente di ACE equivale a 755 in bit di modalità, il che significa:

- Il proprietario ha tutti i diritti.
- I gruppi sono di sola lettura.
- Altri hanno la sola lettura.

Tuttavia, anche se le autorizzazioni vengono regolate sull'equivalente 775, l'accesso può essere negato a causa del NEGAZIONE esplicita impostata su EVERYONE.

Dipendenze di mappatura del dominio ID NFSv4.1

NFSv4.1 sfrutta la logica di mappatura del dominio ID come livello di sicurezza per verificare che un utente che tenta di accedere a un montaggio NFSv4.1 sia effettivamente quello che afferma di essere. In questi casi, il nome utente e il nome del gruppo provenienti dal client NFSv4.1 aggiunge una stringa di nome e la invia all'istanza di Cloud Volumes Service. Se la combinazione di nome utente/gruppo e stringa ID non corrisponde, l'utente e/o il gruppo vengono esclusi dall'impostazione predefinita None User specificata in `/etc/idmapd.conf` sul client.

Questa stringa ID è un requisito per il corretto rispetto delle autorizzazioni, in particolare quando vengono utilizzati ACL NFSv4.1 e/o Kerberos. Di conseguenza, le dipendenze dei server dei nomi, come i server LDAP, sono necessarie per garantire la coerenza tra client e Cloud Volumes Service per una corretta risoluzione delle identità dei nomi di utenti e gruppi.

Cloud Volumes Service utilizza un ID statico predefinito del nome di dominio `defaultv4iddomain.com`. Per impostazione predefinita, i client NFS utilizzano il nome di dominio DNS per le impostazioni del nome di

dominio ID, ma è possibile modificare manualmente il nome di dominio ID in `/etc/idmapd.conf`.

Se LDAP è attivato in Cloud Volumes Service, Cloud Volumes Service automatizza il dominio ID NFS per modificare ciò che è configurato per il dominio di ricerca in DNS e i client non dovranno essere modificati a meno che non utilizzino nomi di ricerca di dominio DNS diversi.

Quando Cloud Volumes Service è in grado di risolvere un nome utente o un nome di gruppo in file locali o LDAP, viene utilizzata la stringa di dominio e gli ID di dominio non corrispondenti vengono eliminati a nessuno. Se Cloud Volumes Service non riesce a trovare un nome utente o un nome di gruppo nei file locali o LDAP, viene utilizzato il valore ID numerico e il client NFS risolve il nome in modo corretto (simile al comportamento di NFSv3).

Senza modificare il dominio ID NFSv4.1 del client in modo che corrisponda a quello utilizzato dal volume Cloud Volumes Service, si verifica quanto segue:

- Gli utenti e i gruppi UNIX con voci locali in Cloud Volumes Service (come root, come definito in utenti e gruppi UNIX locali) vengono ridotti al valore None.
- Gli utenti e i gruppi UNIX con voci in LDAP (se Cloud Volumes Service è configurato per l'utilizzo di LDAP) non vengono visualizzati se i domini DNS sono diversi tra client NFS e Cloud Volumes Service.
- Gli utenti e i gruppi UNIX senza voci locali o LDAP utilizzano il valore numerico ID e si risolvono nel nome specificato sul client NFS. Se non esiste alcun nome sul client, viene visualizzato solo l'ID numerico.

Di seguito sono riportati i risultati dello scenario precedente:

```
# ls -la /mnt/home/profl/nfs4/
total 8
drwxr-xr-x 2 nobody nobody 4096 Feb  3 12:07 .
drwxrwxrwx 7 root    root    4096 Feb  3 12:06 ..
-rw-r--r-- 1  9835    9835      0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 nobody  nobody      0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 nobody  nobody      0 Feb  3 12:06 root-user-file
```

Quando i domini ID client e server corrispondono, viene visualizzato lo stesso elenco di file:

```
# ls -la
total 8
drwxr-xr-x 2 root    root      4096 Feb  3 12:07 .
drwxrwxrwx 7 root    root      4096 Feb  3 12:06 ..
-rw-r--r-- 1  9835      9835      0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 apache  apache-group  0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 root    root        0 Feb  3 12:06 root-user-file
```

Per ulteriori informazioni su questo problema e su come risolverlo, vedere la sezione ["NFSv4.1 e l'utente/gruppo nessuno."](#)

Dipendenze Kerberos

Se si intende utilizzare Kerberos con NFS, è necessario disporre di quanto segue con Cloud Volumes Service:

- Dominio Active Directory per i servizi del centro di distribuzione Kerberos (KDC)
- Dominio Active Directory con attributi utente e gruppo popolati con informazioni UNIX per la funzionalità LDAP (NFS Kerberos in Cloud Volumes Service richiede un'associazione utente da SPN a utente UNIX per la corretta funzionalità).
- LDAP attivato sull'istanza di Cloud Volumes Service
- Dominio Active Directory per i servizi DNS

NFSv4.1 e l'utente/gruppo nessuno

Uno dei problemi più comuni riscontrati con una configurazione NFSv4.1 è quando un file o una cartella viene visualizzata in un elenco utilizzando `ls` di proprietà di `user:group` combinazione di `nobody:nobody`.

Ad esempio:

```
sh-4.2$ ls -la | grep prof1-file
-rw-r--r-- 1 nobody nobody    0 Apr 24 13:25 prof1-file
```

E l'ID numerico è 99.

```
sh-4.2$ ls -lan | grep prof1-file
-rw-r--r-- 1 99 99    0 Apr 24 13:25 prof1-file
```

In alcuni casi, il file potrebbe mostrare il proprietario corretto, ma `nobody` come gruppo.

```
sh-4.2$ ls -la | grep newfile1
-rw-r--r-- 1 prof1 nobody    0 Oct  9 2019 newfile1
```

Chi non è nessuno?

Il `nobody` L'utente in NFSv4.1 è diverso da `nfsnobody` utente. È possibile visualizzare il modo in cui un client NFS vede ciascun utente eseguendo `id` comando:

```
# id nobody
uid=99(nobody) gid=99(nobody) groups=99(nobody)
# id nfsnobody
uid=65534(nfsnobody) gid=65534(nfsnobody) groups=65534(nfsnobody)
```

Con NFSv4.1 `nobody` user (utente) è l'utente predefinito definito da `idmapd.conf` e può essere definito come qualsiasi utente che si desidera utilizzare.

```
# cat /etc/ldapd.conf | grep nobody
#Nobody-User = nobody
#Nobody-Group = nobody
```

Perché questo accade?

Poiché la sicurezza tramite il mapping della stringa del nome è un insieme di chiavi delle operazioni NFSv4.1, il comportamento predefinito quando una stringa del nome non corrisponde correttamente è quello di schiacciare l'utente a un utente che normalmente non avrà accesso a file e cartelle di proprietà di utenti e gruppi.

Quando vedi `nobody` Per l'utente e/o il gruppo negli elenchi di file, ciò significa generalmente che qualcosa in NFSv4.1 è configurato in modo errato. La distinzione tra maiuscole e minuscole può entrare in gioco qui.

Ad esempio, se `user1@CVSDemo.local` (uid 1234, gid 1234) sta accedendo a un'esportazione, Cloud Volumes Service deve essere in grado di trovare `user1@CVSDemo.local` (uid 1234, gid 1234). Se l'utente in Cloud Volumes Service è `USER1@CVSDemo.local`, non corrisponde (`USER1` maiuscolo e `user1` minuscolo). In molti casi, nel file dei messaggi sul client è possibile visualizzare quanto segue:

```
May 19 13:14:29 centos7 nfsidmap[17481]: nss_getpwnam: name
'root@defaultv4iddomain.com' does not map into domain 'CVSDemo.local'
May 19 13:15:05 centos7 nfsidmap[17534]: nss_getpwnam: name 'nobody' does
not map into domain 'CVSDemo.local'
```

Il client e il server devono accettare che un utente sia effettivamente quello che dichiara di essere, quindi è necessario controllare quanto segue per assicurarsi che l'utente che il client vede abbia le stesse informazioni dell'utente che Cloud Volumes Service vede.

- **NFSv4.x ID domain.** Client: `idmapd.conf` File; utilizzi di Cloud Volumes Service `defaultv4iddomain.com` e non possono essere modificati manualmente. Se si utilizza LDAP con NFSv4.1, Cloud Volumes Service modifica il dominio ID in quello utilizzato dal dominio di ricerca DNS, che è lo stesso del dominio ad.
- **Nome utente e ID numerici.** determina dove il client cerca i nomi utente e sfrutta la configurazione dello switch del name service: Client: `nsswitch.conf` E/o `passwd` locale e file di gruppo; Cloud Volumes Service non consente modifiche a questo, ma aggiunge automaticamente LDAP alla configurazione quando è attivato.
- **Nome del gruppo e ID numerici.** determina la posizione in cui il client cerca i nomi dei gruppi e sfrutta la configurazione dello switch del name service: Client: `nsswitch.conf` E/o `passwd` locale e file di gruppo; Cloud Volumes Service non consente modifiche a questo, ma aggiunge automaticamente LDAP alla configurazione quando è attivato.

In quasi tutti i casi, se si vede `nobody` Negli elenchi di utenti e gruppi dei client, il problema è la traduzione dell'ID dominio del nome utente o del gruppo tra Cloud Volumes Service e il client NFS. Per evitare questo scenario, utilizzare LDAP per risolvere le informazioni relative a utenti e gruppi tra client e Cloud Volumes Service.

Visualizzazione delle stringhe di ID nome per NFSv4.1 sui client

Se si utilizza NFSv4.1, durante le operazioni NFS viene eseguita una mappatura di stringa nome, come descritto in precedenza.

Oltre all'utilizzo `/var/log/messages` Per trovare un problema con gli ID NFSv4, è possibile utilizzare `"nfsidmap -l"` Sul client NFS per visualizzare i nomi utente correttamente mappati al dominio NFSv4.

Ad esempio, questo è l'output del comando dopo che un utente può essere trovato dal client e Cloud Volumes Service accede a un montaggio NFSv4.x:

```
# nfsidmap -l
4 .id_resolver keys found:
gid:daemon@CVSDemo.LOCAL
uid:nfs4@CVSDemo.LOCAL
gid:root@CVSDemo.LOCAL
uid:root@CVSDemo.LOCAL
```

Quando un utente non mappato correttamente nel dominio ID NFSv4.1 (in questo caso, `netapp-user`) tenta di accedere allo stesso mount e tocca un file, vengono assegnati `nobody:nobody`, come previsto.

```
# su netapp-user
sh-4.2$ id
uid=482600012(netapp-user), 2000(secondary)
sh-4.2$ cd /mnt/nfs4/
sh-4.2$ touch newfile
sh-4.2$ ls -la
total 16
drwxrwxrwx  5 root    root    4096 Jan 14 17:13 .
drwxr-xr-x.  8 root    root      81 Jan 14 10:02 ..
-rw-r--r--  1 nobody  nobody    0 Jan 14 17:13 newfile
drwxrwxrwx  2 root    root    4096 Jan 13 13:20 qtrees1
drwxrwxrwx  2 root    root    4096 Jan 13 13:13 qtrees2
drwxr-xr-x  2 nfs4    daemon 4096 Jan 11 14:30 testdir
```

Il `nfsidmap -l` l'output mostra l'utente `pcuser` nel display ma non `netapp-user`; si tratta dell'utente anonimo nella nostra regola dei criteri di esportazione (65534).

```
# nfsidmap -l
6 .id_resolver keys found:
gid:pcuser@CVSDemo.LOCAL
uid:pcuser@CVSDemo.LOCAL
gid:daemon@CVSDemo.LOCAL
uid:nfs4@CVSDemo.LOCAL
gid:root@CVSDemo.LOCAL
uid:root@CVSDemo.LOCAL
```

PMI

"PMI" È un protocollo di condivisione file di rete sviluppato da Microsoft che fornisce autenticazione centralizzata di utenti/gruppi, autorizzazioni, blocco e condivisione file a più client SMB su una rete Ethernet. I file e le cartelle vengono presentati ai client tramite condivisioni, che possono essere configurate con una vasta gamma di proprietà di condivisione e offrono il controllo degli accessi tramite permessi a livello di condivisione. SMB può essere presentato a qualsiasi client che offra supporto per il protocollo, inclusi client Windows, Apple e Linux.

Cloud Volumes Service supporta le versioni SMB 2.1 e 3.x del protocollo.

Controllo degli accessi/condivisioni SMB

- Quando un nome utente Windows richiede l'accesso al volume Cloud Volumes Service, Cloud Volumes Service cerca un nome utente UNIX utilizzando i metodi configurati dagli amministratori Cloud Volumes Service.
- Se viene configurato un provider di identità UNIX esterno (LDAP) e i nomi utente Windows/UNIX sono identici, i nomi utente di Windows verranno mappati 1:1 ai nomi utente UNIX senza alcuna configurazione aggiuntiva. Quando LDAP è attivato, Active Directory viene utilizzato per ospitare gli attributi UNIX per gli oggetti utente e gruppo.
- Se i nomi Windows e UNIX non corrispondono in modo identico, è necessario configurare LDAP in modo da consentire a Cloud Volumes Service di utilizzare la configurazione di mappatura dei nomi LDAP (vedere la sezione ["Utilizzo di LDAP per la mappatura asimmetrica dei nomi"](#)).
- Se LDAP non è in uso, gli utenti SMB di Windows si associano a un utente UNIX locale predefinito denominato `pcuser` In Cloud Volumes Service. Ciò significa che i file scritti in Windows dagli utenti che eseguono il mapping a `pcuser` Mostra la proprietà UNIX come `pcuser` In ambienti NAS multiprotocollo. `pcuser` qui è effettivamente il `nobody` Utente in ambienti Linux (UID 65534).

Nelle implementazioni solo con SMB, il `pcuser` Il mapping continua a verificarsi, ma non è importante, perché la proprietà di utenti e gruppi di Windows viene visualizzata correttamente e l'accesso NFS al volume solo SMB non è consentito. Inoltre, i volumi solo SMB non supportano la conversione in NFS o volumi a doppio protocollo dopo la loro creazione.

Windows sfrutta Kerberos per l'autenticazione del nome utente con i domain controller di Active Directory, che richiede uno scambio di nome utente e password con i controller di dominio ad, esterni all'istanza di Cloud Volumes Service. L'autenticazione Kerberos viene utilizzata quando `\\SERVERNAME` Il percorso UNC viene utilizzato dai client SMB ed è vero quanto segue:

- La voce DNS A/AAAA esiste per NOME SERVER
- Esiste un SPN valido per l'accesso SMB/CIFS per NOME SERVER

Quando viene creato un volume SMB Cloud Volumes Service, il nome dell'account del computer viene creato come definito nella sezione ["Come viene visualizzato Cloud Volumes Service in Active Directory."](#) Il nome account del computer diventa anche il percorso di accesso condiviso SMB perché Cloud Volumes Service sfrutta il DNS dinamico (DDNS) per creare le voci A/AAAA e PTR necessarie nel DNS e le voci SPN necessarie sull'account principal del computer.



Per creare le voci PTR, la zona di ricerca inversa per l'indirizzo IP dell'istanza Cloud Volumes Service deve esistere sul server DNS.

Ad esempio, questo volume Cloud Volumes Service utilizza il seguente percorso di condivisione UNC: \\cvs-east-433d.cvsdemo.local.

In Active Directory, queste sono le voci SPN generate dal servizio Cloud Volumes:

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
HOST/cvs-east-433d.cvsdemo.local
HOST/ CVS-EAST-433D
```

Questo è il risultato della ricerca DNS in avanti/indietro:

```
PS C:\> nslookup CVS-EAST-433D
Server: activedirectory.region.lab.internal
Address: 10. xx.0. xx
Name: CVS-EAST-433D.cvsdemo.local
Address: 10. xxx.0. x
PS C:\> nslookup 10. xxx.0. x
Server: activedirectory.region.lab.internal
Address: 10.xx.0.xx
Name: CVS-EAST-433D.CVSDemo.LOCAL
Address: 10. xxx.0. x
```

Facoltativamente, è possibile applicare un maggiore controllo degli accessi attivando/richiedendo la crittografia SMB per le condivisioni SMB in Cloud Volumes Service. Se la crittografia SMB non è supportata da uno degli endpoint, l'accesso non è consentito.

Utilizzo degli alias dei nomi SMB

In alcuni casi, potrebbe essere un problema di sicurezza per gli utenti finali conoscere il nome dell'account del computer in uso per Cloud Volumes Service. In altri casi, è sufficiente fornire un percorso di accesso più semplice agli utenti finali. In questi casi, è possibile creare alias SMB.

Se si desidera creare alias per il percorso di condivisione SMB, è possibile sfruttare ciò che è noto come record CNAME in DNS. Ad esempio, se si desidera utilizzare il nome \\CIFS per accedere alle condivisioni anziché a. \\cvs-east-433d.cvsdemo.local, Ma si desidera comunque utilizzare l'autenticazione Kerberos, un CNAME nel DNS che punta al record A/AAAA esistente e un ulteriore SPN aggiunto all'account del computer esistente fornisce l'accesso Kerberos.

cifs Properties

Alias (CNAME) Security

Alias name (uses parent domain if left blank):

cifs

Fully qualified domain name (FQDN):

cifs.cvsdemo.local

Fully qualified domain name (FQDN) for target host:

CVS-EAST-433D.CVSDemo.LOCAL Browse...

OK Cancel Apply

Questo è il risultato della ricerca diretta DNS dopo l'aggiunta di un CNAME:

```
PS C:\> nslookup cifs
Server: ok-activedirectory.us-east4-a.c.cv-solution-architect-
lab.internal
Address: 10. xx.0. xx
Name: CVS-EAST-433D.cvsdemo.local
Address: 10. xxx.0. x
Aliases: cifs.cvsdemo.local
```

Questa è la query SPN risultante dopo l'aggiunta di nuovi numeri di servizio:

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
cifs/cifs.cvsdemo.local
cifs/cifs
HOST/cvs-east-433d.cvsdemo.local
HOST/CVS-EAST-433D
```

In un'acquisizione di pacchetti, è possibile visualizzare la richiesta di configurazione della sessione utilizzando l'SPN legato al CNAME.

431	4.156722	SMB2	308	Negotiate Protocol Response
432	4.156785	SMB2	232	Negotiate Protocol Request
434	4.158108	SMB2	374	Negotiate Protocol Response
435	4.160977	SMB2	1978	Session Setup Request
437	4.166224	SMB2	322	Session Setup Response
438	4.166891	SMB2	152	Tree Connect Request Tree: \\cifs\IPC\$
439	4.168063	SMB2	138	Tree Connect Response


```

realm: CVSDemo.LOCAL
  ▼ sname
    name-type: kRB5-NT-SRV-INST (2)
    ▼ sname-string: 2 items
      SNameString: cifs
      SNameString: cifs
  ▼ enc-part
    etype: eTYPE-ARCFOUR-HMAC-MD5 (23)

```

Dialecti di autenticazione SMB

Cloud Volumes Service supporta quanto segue "dialetti" Per l'autenticazione SMB:

- LM
- NTLM
- NTLMv2
- Kerberos

L'autenticazione Kerberos per l'accesso alle condivisioni SMB è il livello di autenticazione più sicuro possibile. Con la crittografia AES e SMB attivata, il livello di sicurezza aumenta ulteriormente.

Cloud Volumes Service supporta anche la compatibilità con le versioni precedenti per l'autenticazione LM e NTLM. Quando Kerberos non è configurato correttamente (ad esempio quando si creano alias SMB), l'accesso alla condivisione viene ricallato ai metodi di autenticazione più deboli (ad esempio NTLMv2). Poiché questi meccanismi sono meno sicuri, sono disattivati in alcuni ambienti Active Directory. Se i metodi di autenticazione più deboli sono disattivati e Kerberos non è configurato correttamente, l'accesso alla condivisione non riesce perché non esiste un metodo di autenticazione valido.

Per informazioni sulla configurazione e la visualizzazione dei livelli di autenticazione supportati in Active Directory, vedere ["Sicurezza di rete: Livello di autenticazione di LAN Manager"](#).

Modelli di permesso

Permessi NTFS/file

Le autorizzazioni NTFS sono le autorizzazioni applicate a file e cartelle nei file system che aderiscono alla logica NTFS. È possibile applicare le autorizzazioni NTFS in Basic oppure Advanced e può essere impostato su Allow oppure Deny per il controllo degli accessi.

Le autorizzazioni di base includono:

- Controllo completo
- Modificare
- Lettura ed esecuzione
- Leggi
- Di scrittura

Quando si impostano le autorizzazioni per un utente o un gruppo, denominato ACE, si trova in un ACL. Le autorizzazioni NTFS utilizzano le stesse basi di lettura/scrittura/esecuzione dei bit in modalità UNIX, ma possono anche estendersi a controlli di accesso più granulari ed estesi (noti anche come permessi speciali), come Take Ownership, Create Folders/Append Data, Write Attributes e altro ancora.

I bit in modalità UNIX standard non forniscono lo stesso livello di granularità delle autorizzazioni NTFS (ad esempio, la possibilità di impostare autorizzazioni per singoli oggetti utente e gruppo in un ACL o di impostare attributi estesi). Tuttavia, gli ACL NFSv4.1 offrono le stesse funzionalità degli ACL NTFS.

Le autorizzazioni NTFS sono più specifiche delle autorizzazioni di condivisione e possono essere utilizzate insieme alle autorizzazioni di condivisione. Con le strutture di autorizzazione NTFS, si applicano le impostazioni più restrittive. Di conseguenza, le negazioni esplicite a un utente o a un gruppo sovrascrivono anche il controllo completo quando si definiscono i diritti di accesso.

Le autorizzazioni NTFS sono controllate dai client SMB di Windows.

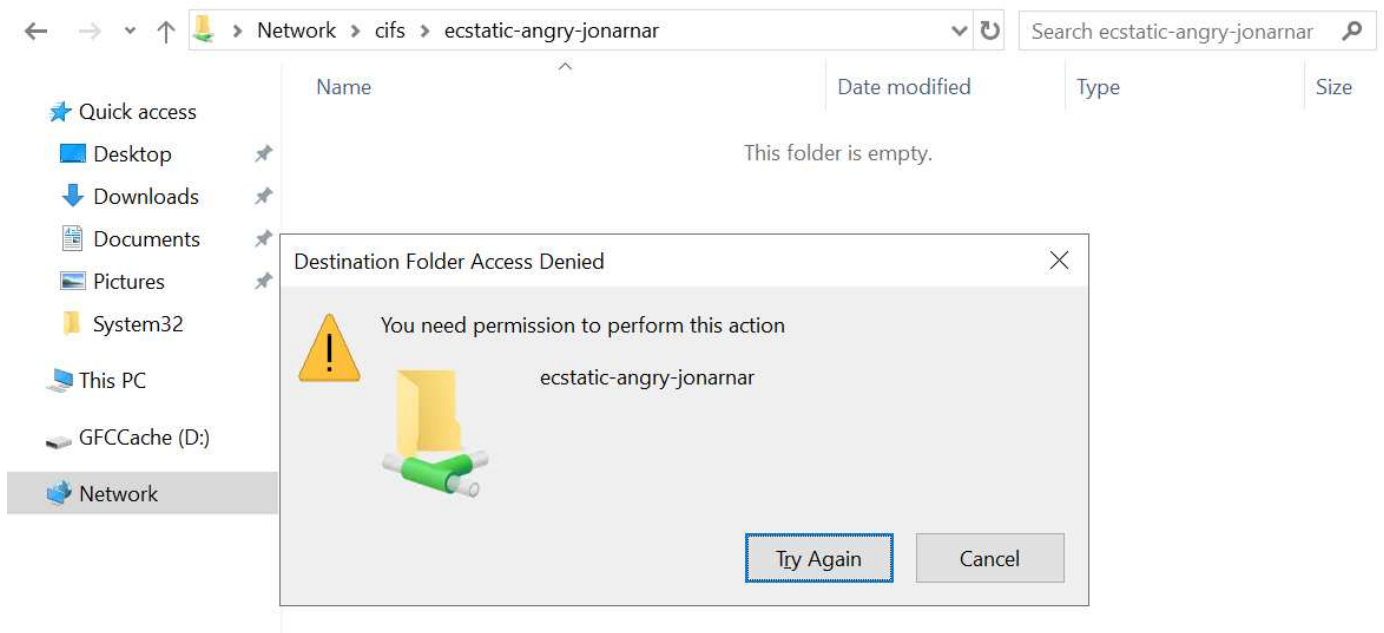
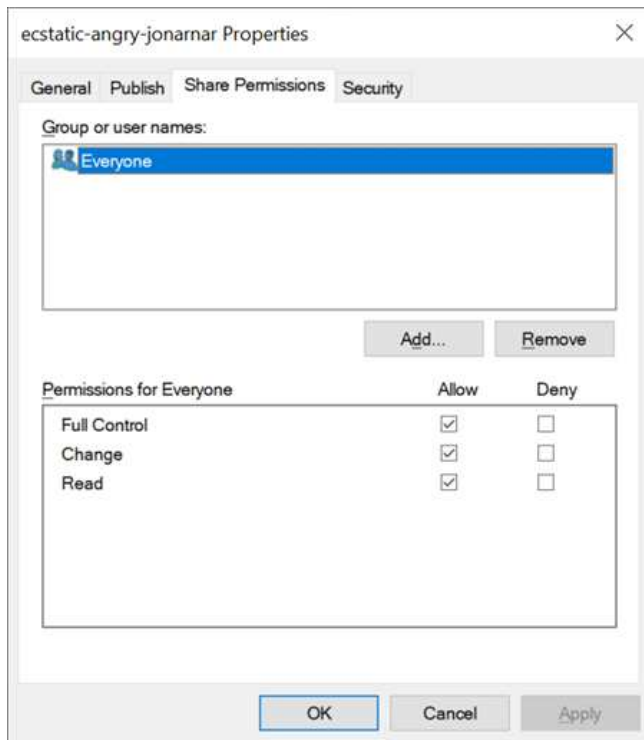
Autorizzazioni di condivisione

Le autorizzazioni di condivisione sono più generali delle autorizzazioni NTFS (solo lettura/modifica/controllo completo) e controllano la voce iniziale in una condivisione SMB, in modo simile al funzionamento delle regole dei criteri di esportazione NFS.

Sebbene le regole dei criteri di esportazione NFS controllino l'accesso attraverso informazioni basate su host come indirizzi IP o nomi host, le autorizzazioni di condivisione SMB possono controllare l'accesso utilizzando le ACE di utente e gruppo in un ACL condiviso. È possibile impostare gli ACL di condivisione dal client Windows o dall'interfaccia utente di gestione di Cloud Volumes Service.

Per impostazione predefinita, gli ACL di condivisione e gli ACL dei volumi iniziali includono Everyone con controllo completo. Gli ACL dei file devono essere modificati, ma le autorizzazioni di condivisione vengono ignorate dalle autorizzazioni dei file sugli oggetti nella condivisione.

Ad esempio, se a un utente è consentito solo l'accesso in lettura all'ACL del file di volume Cloud Volumes Service, viene negato l'accesso per creare file e cartelle anche se l'ACL di condivisione è impostato su Everyone con controllo completo, come illustrato nella figura seguente.



Per ottenere i migliori risultati di sicurezza, procedere come segue:

- Rimuovere tutti dagli ACL di file e condivisione e impostare l'accesso di condivisione per utenti o gruppi.
- Utilizzare i gruppi per il controllo degli accessi invece di singoli utenti per semplificare la gestione e velocizzare la rimozione/aggiunta degli utenti per condividere gli ACL attraverso la gestione dei gruppi.
- Consentire un accesso di condivisione meno restrittivo e più generale alle ACE sulle autorizzazioni di condivisione e bloccare l'accesso a utenti e gruppi con permessi di file per un controllo degli accessi più granulare.
- Evitare l'utilizzo generale di ACL di negazione esplicite, in quanto sovrascrivono gli ACL di consenso. Limitare l'utilizzo di ACL di negazione esplicite per utenti o gruppi che devono essere limitati all'accesso rapido a un file system.

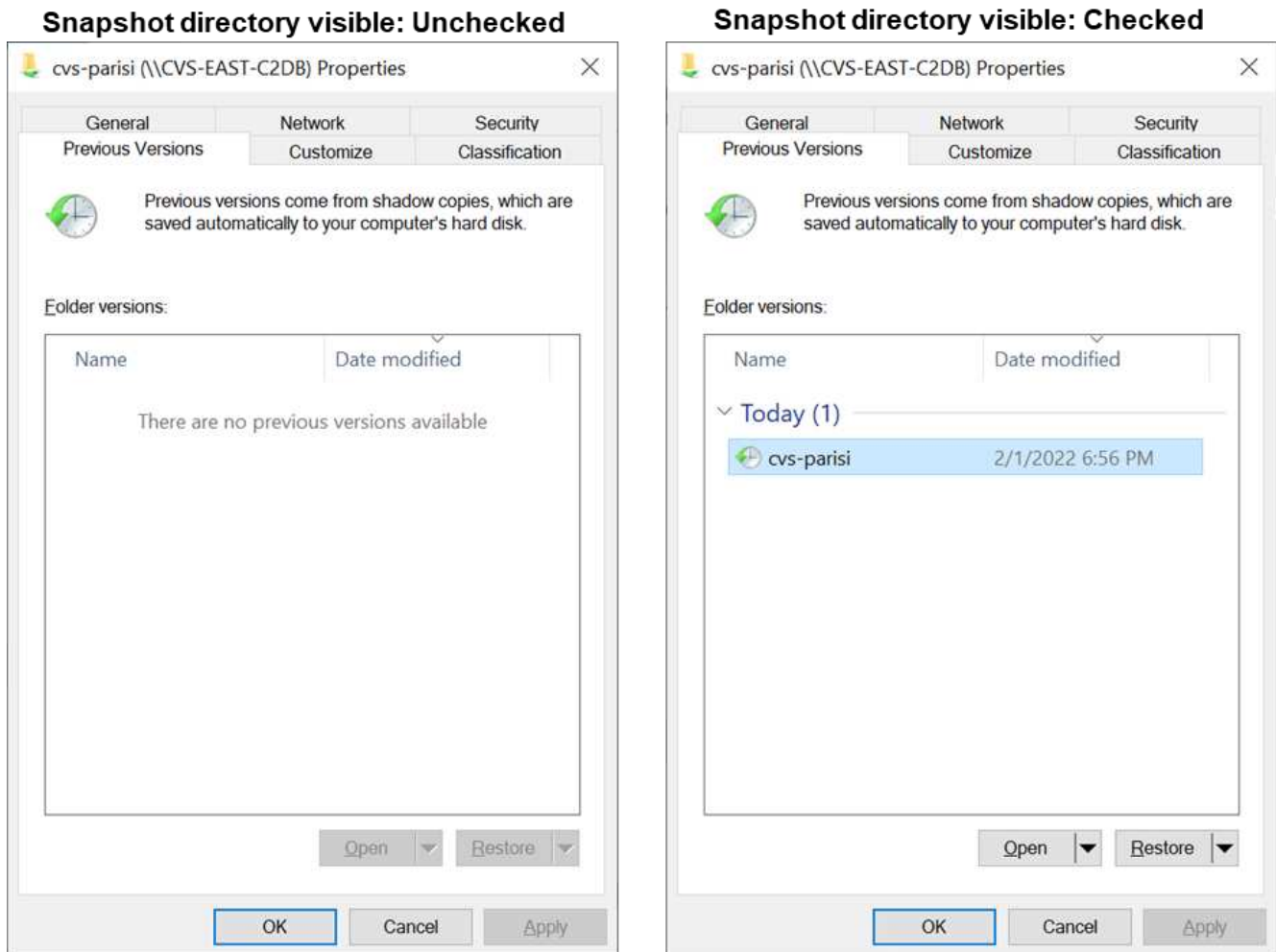
- Assicurarsi di prestare attenzione a. "[Ereditarietà ACL](#)" impostazioni durante la modifica delle autorizzazioni; l'impostazione del flag di ereditarietà al livello superiore di una directory o di un volume con un numero elevato di file indica che ogni file sotto a tale directory o volume ha ereditato le autorizzazioni aggiunte, che possono creare comportamenti indesiderati come accesso/negazione non intenzionale e lunga modifica delle autorizzazioni quando ogni file viene regolato.

SMB condivide le funzionalità di sicurezza

La prima volta che si crea un volume con accesso SMB in Cloud Volumes Service, viene visualizzata una serie di opzioni per la protezione di tale volume.

Alcune di queste scelte dipendono dal livello Cloud Volumes Service (prestazioni o software) e le scelte includono:

- **Rendi visibile la directory Snapshot (disponibile sia per CVS-Performance che per CVS-SW).** questa opzione controlla se i client SMB possono accedere o meno alla directory Snapshot in una condivisione SMB (\\server\share\~snapshot E/o versioni precedenti). L'impostazione predefinita non è selezionata, il che significa che il volume per impostazione predefinita nasconde e non consente l'accesso a ~snapshot Directory e non vengono visualizzate copie Snapshot nella scheda versioni precedenti del volume.



È possibile nascondere le copie Snapshot dagli utenti finali per motivi di sicurezza, di performance (nascondendo queste cartelle dalle scansioni AV) o di preferenza. Le istantanee di Cloud Volumes Service sono di sola lettura, quindi anche se sono visibili, gli utenti finali non possono eliminare o modificare i file nella

directory Snapshot. Si applicano le autorizzazioni per i file o le cartelle al momento dell'esecuzione della copia Snapshot. Se le autorizzazioni di un file o di una cartella cambiano tra le copie Snapshot, le modifiche si applicano anche ai file o alle cartelle nella directory Snapshot. Utenti e gruppi possono accedere a questi file o cartelle in base alle autorizzazioni. Sebbene non sia possibile eliminare o modificare i file nella directory Snapshot, è possibile copiare file o cartelle dalla directory Snapshot.

- **Attiva la crittografia SMB (disponibile sia per CVS-Performance che per CVS-SW).** la crittografia SMB è disattivata per impostazione predefinita nella condivisione SMB (non selezionata). Selezionando la casella viene attivata la crittografia SMB, il che significa che il traffico tra il client SMB e il server viene crittografato in-flight con i livelli di crittografia più elevati supportati negoziati. Cloud Volumes Service supporta la crittografia fino a AES-256 per le PMI. L'attivazione della crittografia SMB comporta una penalizzazione delle performance che potrebbe o meno essere evidente per i client SMB, approssimativamente nell'intervallo 10-20%. NetApp incoraggia vivamente i test per verificare se tale penalizzazione delle performance è accettabile.
- **Nascondi condivisione SMB (disponibile sia per CVS-Performance che CVS-SW).** l'impostazione di questa opzione nasconde il percorso di condivisione SMB dalla normale navigazione. Ciò significa che i client che non conoscono il percorso di condivisione non possono visualizzare le condivisioni quando accedono al percorso UNC predefinito (ad esempio `\\CVS-SMB`). Quando la casella di controllo è selezionata, solo i client che conoscono esplicitamente il percorso di condivisione SMB o che hanno il percorso di condivisione definito da un oggetto Criteri di gruppo possono accedervi (sicurezza tramite offuscamento).
- **Enable access-based enumeration (ABE) (solo CVS-SW).** questo è simile a nascondere la condivisione SMB, tranne che le condivisioni o i file sono nascosti solo agli utenti o ai gruppi che non dispongono delle autorizzazioni per accedere agli oggetti. Ad esempio, se utente Windows `joe` Non è consentito almeno l'accesso in lettura tramite le autorizzazioni, quindi l'utente Windows `joe` Impossibile visualizzare la condivisione SMB o i file. Questa opzione è disattivata per impostazione predefinita ed è possibile attivarla selezionando la casella di controllo. Per ulteriori informazioni su ABE, consultare l'articolo della Knowledge base di NetApp ["Come funziona Access Based Enumeration \(ABE\)?"](#)
- **Attiva il supporto delle condivisioni CA (Continuously Available) (solo CVS-Performance).** ["Condivisioni SMB sempre disponibili"](#) Fornire un modo per ridurre al minimo le interruzioni delle applicazioni durante gli eventi di failover replicando gli stati di blocco tra i nodi nel sistema di back-end Cloud Volumes Service. Non si tratta di una funzionalità di sicurezza, ma offre una migliore resilienza generale. Attualmente, solo le applicazioni SQL Server e FSLogix sono supportate per questa funzionalità.

Condivisioni nascoste predefinite

Quando viene creato un server SMB in Cloud Volumes Service, ne esistono ["condivisioni amministrative nascoste"](#) (Utilizzando la convenzione di naming in dollari) creati in aggiunta alla condivisione SMB del volume di dati. Questi includono l'accesso allo spazio dei nomi e l'IPC (sharing named pipe for communication between programs, come le chiamate di procedura remota (RPC) utilizzate per l'accesso a Microsoft Management Console (MMC)).

La condivisione IPC non contiene ACL di condivisione e non può essere modificata, ma viene utilizzata esclusivamente per le chiamate RPC e. ["Per impostazione predefinita, Windows non consente l'accesso anonimo a queste condivisioni"](#).

La condivisione consente l'accesso predefinito a BUILTIN/Administrators, ma l'automazione Cloud Volumes Service rimuove l'ACL della condivisione e non consente l'accesso a nessuno perché l'accesso alla condivisione consente la visibilità di tutti i volumi montati nei file system Cloud Volumes Service. Di conseguenza, tenta di accedere a. `\\SERVER\C$` non riuscito.

Account con diritti di amministratore/backup locali/BUILTIN

I server SMB di Cloud Volumes Service mantengono una funzionalità simile a quella dei normali server SMB di Windows, in quanto esistono gruppi locali (ad esempio BUILTIN/amministratori) che applicano i diritti di accesso a utenti e gruppi di dominio selezionati.

Quando si specifica un utente da aggiungere agli utenti di backup, l'utente viene aggiunto al gruppo BUILTIN/Backup Operators nell'istanza di Cloud Volumes Service che utilizza tale connessione, che ottiene quindi ["SeBackupPrivilege e SeRestorePrivilege"](#).

Quando si aggiunge un utente a Security Privilege Users, all'utente viene assegnato il privilegio SeSecurityPrivilege, utile in alcuni casi di utilizzo dell'applicazione, ad esempio ["SQL Server su condivisioni SMB"](#).

Backup Users

Provide a comma separated list of domain users or a domain group name that require elevated privileges to access volumes created by Cloud Volumes Service.

Accountnames
administrator,cvs-svc

Security Privilege Users


Provide a list of comma separated domain user accounts that require elevated privileges to manage security log for the Active Directory associated with Cloud Volumes Service.

Accountnames
administrator,cvs-svc

È possibile visualizzare le appartenenze ai gruppi locali di Cloud Volumes Service tramite MMC con i privilegi appropriati. La figura seguente mostra gli utenti aggiunti utilizzando la console di Cloud Volumes Service.

Backup Operators Properties

General

 Backup Operators

Description: Backup Operators group

Members:

- CVSDemo\Administrator
- CVSDemo\cvs-svc

Add... Remove

Changes to a user's group membership are not effective until the next time the user logs on.

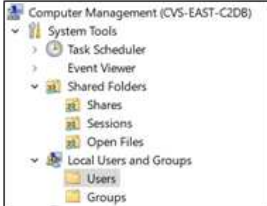

OK Cancel Apply Help

La seguente tabella mostra l'elenco dei gruppi BUILTIN predefiniti e gli utenti/gruppi aggiunti per impostazione predefinita.

Locale/gruppo BUILTIN	Membri predefiniti
BUILTIN/amministratori*	AMMINISTRATORI DI DOMINIO/dominio
BUILTIN/Backup Operator*	Nessuno
BUILTIN/guest	Dominio/dominio guest
UTENTI BUILTIN/Power	Nessuno
UTENTI BUILTIN/dominio	UTENTI DI DOMINIO/dominio


*Appartenenza al gruppo controllata nella configurazione della connessione ad Active Directory di Cloud Volumes Service.

È possibile visualizzare gli utenti e i gruppi locali (e i membri del gruppo) nella finestra MMC, ma non è possibile aggiungere o eliminare oggetti o modificare le appartenenze ai gruppi da questa console. Per impostazione predefinita, solo il gruppo Domain Admins e l'amministratore vengono aggiunti al gruppo BUILTIN/Administrators in Cloud Volumes Service. Al momento, non è possibile modificarlo.

Computer Management (CVS-EAST-C2DB)			Computer Management (CVS-EAST-C2DB)		
					
Name	Full Name	Description	Name	Description	
Administrator		Built-in administrator account	Administrators	Built-in Administrators group	
			Users	All users	
			Guests	Built-in Guests Group	
			Power Users	Restricted administrative privileges	
			Backup Operators	Backup Operators group	

Administrators Properties

General





Administrators

Description:

Built-in Administrators group

Members:

Administrator

CVSDemo\Domain Admins

Add...

Remove

Changes to a user's group membership are not effective until the next time the user logs on.

OK

Cancel

Apply

Help

Accesso MMC/Gestione computer

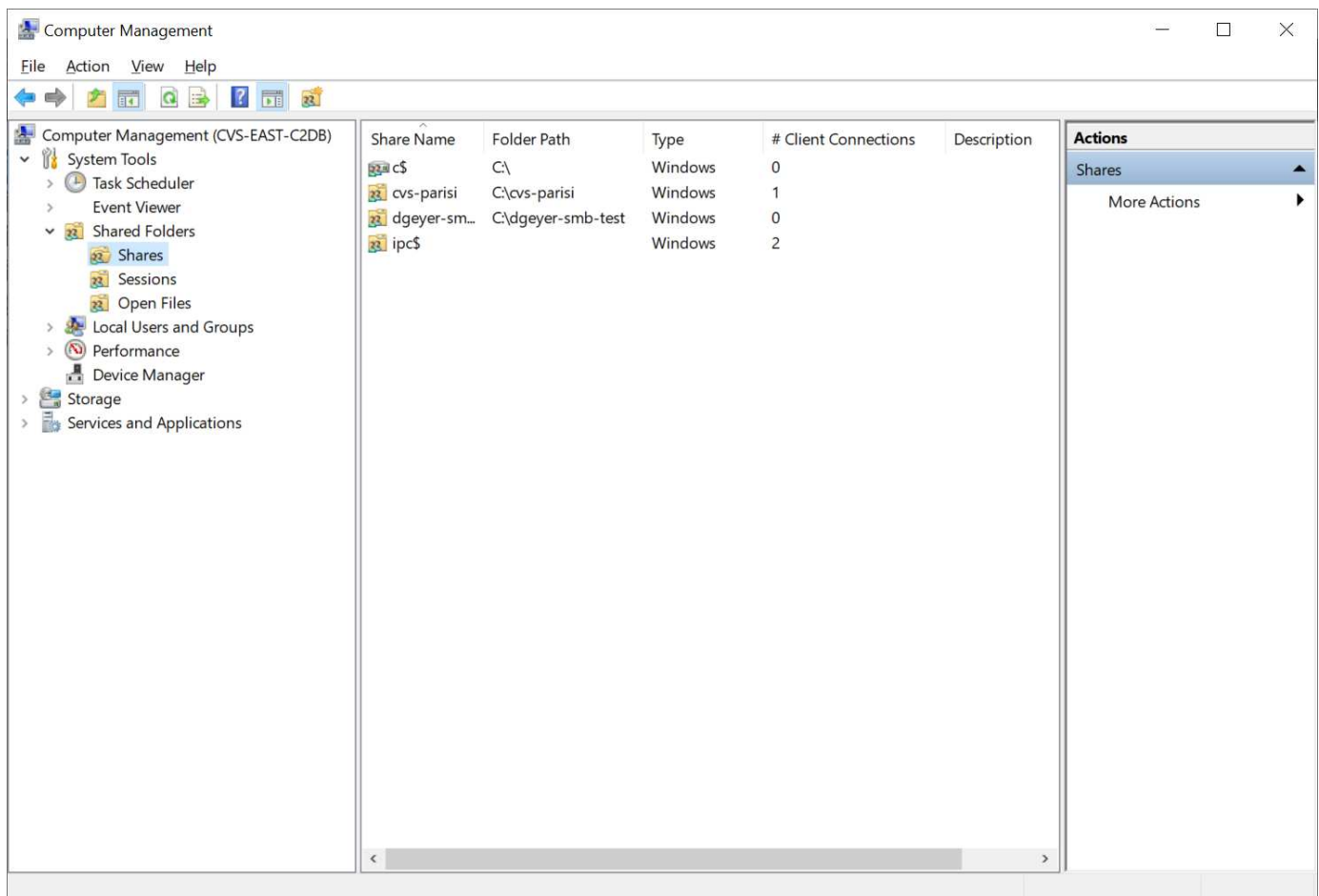
L'accesso SMB in Cloud Volumes Service fornisce la connettività alla MMC Gestione computer, che consente di visualizzare le condivisioni, gestire gli ACL delle condivisioni, visualizzare/gestire le sessioni SMB e aprire i file.

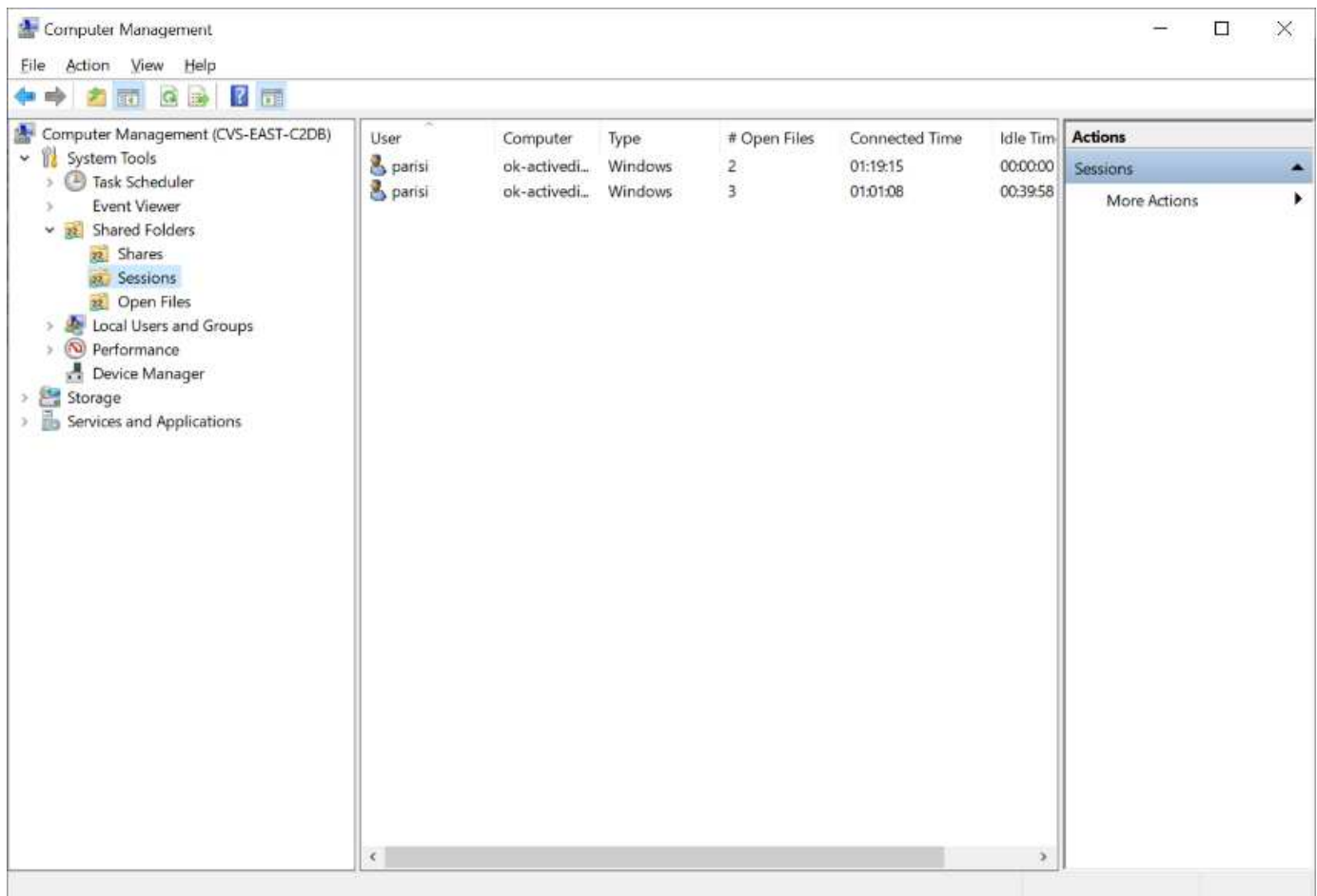
Per utilizzare MMC per visualizzare le condivisioni SMB e le sessioni in Cloud Volumes Service, l'utente attualmente connesso deve essere un amministratore di dominio. Agli altri utenti è consentito l'accesso per visualizzare o gestire il server SMB da MMC e ricevere una finestra di dialogo non si dispone delle autorizzazioni quando si tenta di visualizzare condivisioni o sessioni sull'istanza SMB di Cloud Volumes Service.

Per connettersi al server SMB, aprire Gestione computer, fare clic con il pulsante destro del mouse su Gestione computer, quindi selezionare Connetti a un altro computer. Viene visualizzata la finestra di dialogo Seleziona computer, in cui è possibile immettere il nome del server SMB (disponibile nelle informazioni sul volume Cloud Volumes Service).

Quando si visualizzano le condivisioni SMB con le autorizzazioni appropriate, vengono visualizzate tutte le condivisioni disponibili nell'istanza di Cloud Volumes Service che condividono la connessione Active Directory. Per controllare questo comportamento, impostare l'opzione Nascondi condivisioni SMB sull'istanza del volume Cloud Volumes Service.

Tenere presente che è consentita una sola connessione Active Directory per regione.





La seguente tabella mostra un elenco delle funzionalità supportate/non supportate per MMC.

Funzioni supportate	Funzioni non supportate
<ul style="list-style-type: none"> • Visualizza condivisioni • Visualizzare le sessioni SMB attive • Visualizzare i file aperti • Visualizzare utenti e gruppi locali • Visualizzare le appartenenze ai gruppi locali • Enumerare l'elenco di sessioni, file e connessioni ad albero nel sistema • Chiudere i file aperti nel sistema • Chiudere le sessioni aperte • Creare/gestire le condivisioni 	<ul style="list-style-type: none"> • Creazione di nuovi utenti/gruppi locali • Gestione/visualizzazione di utenti/gruppi locali esistenti • Visualizza eventi o log delle performance • Gestione dello storage • Gestione di servizi e applicazioni

Informazioni sulla sicurezza dei server SMB

Il server SMB di Cloud Volumes Service utilizza una serie di opzioni che definiscono le policy di sicurezza per le connessioni SMB, tra cui l'inclinazione del clock Kerberos, l'età del ticket, la crittografia e molto altro ancora.

La seguente tabella contiene un elenco di queste opzioni, le loro funzioni, le configurazioni predefinite e se possono essere modificate con Cloud Volumes Service. Alcune opzioni non si applicano a Cloud Volumes

Service.

Opzione di sicurezza	Che cosa fa	Valore predefinito	Può cambiare?
Inclinazione massima del clock Kerberos (minuti)	Disallineamento massimo del tempo tra Cloud Volumes Service e i controller di dominio. Se l'intervallo di tempo supera i 5 minuti, l'autenticazione Kerberos non riesce. Viene impostato sul valore predefinito di Active Directory.	5	No
Durata ticket Kerberos (ore)	Tempo massimo in cui un ticket Kerberos rimane valido prima di richiedere un rinnovo. Se non si verifica alcun rinnovo prima delle 10 ore, è necessario ottenere un nuovo biglietto. Cloud Volumes Service esegue automaticamente questi rinnovi. 10 ore è il valore predefinito di Active Directory.	10	No
Rinnovo massimo ticket Kerberos (giorni)	Numero massimo di giorni in cui un ticket Kerberos può essere rinnovato prima che sia necessaria una nuova richiesta di autorizzazione. Cloud Volumes Service rinnova automaticamente i ticket per le connessioni SMB. Sette giorni è il valore predefinito di Active Directory.	7	No
Timeout connessione KDC Kerberos (sec)	Il numero di secondi prima del timeout di una connessione KDC.	3	No
Richiedi firma per traffico SMB in entrata	Impostazione per richiedere la firma per il traffico SMB. Se impostata su true, i client che non supportano la firma non riescono a connettersi.	Falso	

Opzione di sicurezza	Che cosa fa	Valore predefinito	Può cambiare?
Richiedi complessità password per account utente locali	Utilizzato per le password degli utenti SMB locali. Cloud Volumes Service non supporta la creazione di utenti locali, pertanto questa opzione non si applica a Cloud Volumes Service.	Vero	No
Utilizzare start_tls per le connessioni LDAP di Active Directory	Utilizzato per attivare le connessioni TLS iniziali per Active Directory LDAP. Cloud Volumes Service attualmente non supporta l'abilitazione di questa opzione.	Falso	No
AES-128 e AES-256 Encryption for Kerberos sono abilitati	In questo modo si controlla se la crittografia AES viene utilizzata per le connessioni Active Directory e viene controllata con l'opzione Enable AES Encryption for Active Directory Authentication (attiva crittografia AES per l'autenticazione Active Directory) quando si crea o si modifica la connessione Active Directory.	Falso	Sì
Livello di compatibilità LM	Livello dei dialetti di autenticazione supportati per le connessioni Active Directory. Vedere la sezione " Dialetti di autenticazione SMB " per ulteriori informazioni.	ntlmv2-krb	No
Richiedi crittografia SMB per traffico CIFS in entrata	Richiede la crittografia SMB per tutte le condivisioni. Questa opzione non viene utilizzata da Cloud Volumes Service; impostare invece la crittografia per volume (vedere la sezione " SMB condivide le funzionalità di sicurezza ").	Falso	No

Opzione di sicurezza	Che cosa fa	Valore predefinito	Può cambiare?
Sicurezza della sessione client	Imposta la firma e/o il sealing per la comunicazione LDAP. Questa opzione non è attualmente impostata in Cloud Volumes Service, ma potrebbe essere necessaria nelle versioni future per risolvere . La risoluzione dei problemi di autenticazione LDAP dovuti alla patch di Windows è descritta nella sezione ""Associazione del canale LDAP"" .	Nessuno	No
Abilitazione SMB2 per connessioni DC	Utilizza SMB2 per le connessioni DC. Attivato per impostazione predefinita.	System-default	No
LDAP Referral Chasing	Quando si utilizzano più server LDAP, la ricerca dei riferimenti consente al client di fare riferimento ad altri server LDAP nell'elenco quando non viene trovata una voce nel primo server. Attualmente non è supportato da Cloud Volumes Service.	Falso	No
Utilizzare LDAPS per connessioni Active Directory sicure	Attiva l'utilizzo di LDAP su SSL. Attualmente non supportato da Cloud Volumes Service.	Falso	No
La crittografia è necessaria per la connessione DC	Richiede la crittografia per le connessioni DC riuscite. Disattivato per impostazione predefinita in Cloud Volumes Service.	Falso	No

Protocollo doppio/multiprotocollo

Cloud Volumes Service offre la possibilità di condividere gli stessi set di dati con client SMB e NFS mantenendo le autorizzazioni di accesso appropriate ("[protocollo doppio](#)"). Ciò avviene coordinando il mapping delle identità tra i protocolli e utilizzando un server LDAP backend centralizzato per fornire le identità UNIX a Cloud Volumes Service. È possibile utilizzare Windows Active Directory per fornire agli utenti Windows e UNIX una maggiore facilità di utilizzo.

Controllo degli accessi

- **Controlli di accesso alla condivisione.** determinare quali client e/o utenti e gruppi possono accedere a una condivisione NAS. Per NFS, le policy e le regole di esportazione controllano l'accesso dei client alle esportazioni. Le esportazioni NFS vengono gestite dall'istanza di Cloud Volumes Service. SMB utilizza le condivisioni CIFS/SMB e gli ACL di condivisione per fornire un controllo più granulare a livello di utente e gruppo. È possibile configurare gli ACL a livello di condivisione solo dai client SMB utilizzando ["Gestione MMC/computer"](#) Con un account che dispone dei diritti di amministratore sull'istanza di Cloud Volumes Service (vedere la sezione [""Account con diritti di backup/amministratore BUILTIN locale.""](#)).
- **File access control.** Controlla le autorizzazioni a livello di file o cartella e sono sempre gestite dal client NAS. I client NFS possono utilizzare i bit di modalità tradizionali (rwx) o gli ACL NFSv4. I client SMB sfruttano le autorizzazioni NTFS.

Il controllo dell'accesso per i volumi che servono dati a NFS e SMB dipende dal protocollo in uso. Per informazioni sulle autorizzazioni con protocollo doppio, vedere la sezione ["Modello di permesso."](#)

Mappatura dell'utente

Quando un client accede a un volume, Cloud Volumes Service tenta di mappare l'utente in entrata a un utente valido nella direzione opposta. Ciò è necessario per determinare l'accesso corretto tra i protocolli e per garantire che l'utente che richiede l'accesso sia effettivamente quello che afferma di essere.

Ad esempio, se un utente Windows ha denominato joe Tenta di accedere a un volume con autorizzazioni UNIX tramite SMB, quindi Cloud Volumes Service esegue una ricerca per trovare un utente UNIX corrispondente denominato joe. Se ne esiste uno, i file scritti in una condivisione SMB come utente Windows joe Viene visualizzato come utente UNIX joe Dai client NFS.

In alternativa, se si chiama un utente UNIX joe Tenta di accedere a un volume Cloud Volumes Service con autorizzazioni Windows, quindi l'utente UNIX deve essere in grado di eseguire il mapping a un utente Windows valido. In caso contrario, l'accesso al volume viene negato.

Attualmente, solo Active Directory è supportato per la gestione esterna delle identità UNIX con LDAP. Per ulteriori informazioni sulla configurazione dell'accesso a questo servizio, vedere ["Creazione di una connessione ad"](#).

Modello di permesso

Quando si utilizzano configurazioni a doppio protocollo, Cloud Volumes Service utilizza gli stili di sicurezza per i volumi per determinare il tipo di ACL. Questi stili di sicurezza vengono impostati in base al protocollo NAS specificato o, nel caso del protocollo doppio, è possibile scegliere al momento della creazione del volume Cloud Volumes Service.

- Se si utilizza solo NFS, i volumi Cloud Volumes Service utilizzano le autorizzazioni UNIX.
- Se si utilizza solo SMB, i volumi Cloud Volumes Service utilizzano le autorizzazioni NTFS.

Se si crea un volume a doppio protocollo, è possibile scegliere lo stile ACL alla creazione del volume. Questa decisione deve essere presa in base alla gestione delle autorizzazioni desiderata. Se gli utenti gestiscono le autorizzazioni dai client Windows/SMB, selezionare NTFS. Se gli utenti preferiscono utilizzare client NFS e chmod/chown, utilizzare gli stili di sicurezza UNIX.

Considerazioni per la creazione di connessioni Active Directory

Cloud Volumes Service consente di connettere l'istanza di Cloud Volumes Service a un server Active Directory esterno per la gestione delle identità per gli utenti SMB e UNIX.

Per utilizzare SMB in Cloud Volumes Service è necessario creare una connessione Active Directory.

La configurazione fornisce diverse opzioni che richiedono una certa considerazione per la sicurezza. Il server Active Directory esterno può essere un'istanza on-premise o nativo del cloud. Se si utilizza un server Active Directory on-premise, non esporre il dominio alla rete esterna (ad esempio con un DMZ o un indirizzo IP esterno). Utilizzare, invece, tunnel privati o VPN sicuri, trust di foresta unidirezionali o connessioni di rete dedicate alle reti on-premise con ["Accesso privato a Google"](#). Per ulteriori informazioni su, consultare la documentazione di Google Cloud ["Best practice per l'utilizzo di Active Directory in Google Cloud"](#).



CVS-SW richiede che i server Active Directory si trovino nella stessa regione. Se si tenta di stabilire una connessione CC in CVS-SW con un'altra regione, il tentativo non riesce. Quando si utilizza CVS-SW, assicurarsi di creare siti Active Directory che includono i controller di dominio Active Directory e specificare i siti in Cloud Volumes Service per evitare tentativi di connessione DC tra regioni.

Credenziali di Active Directory

Quando SMB o LDAP per NFS è attivato, Cloud Volumes Service interagisce con i controller di Active Directory per creare un oggetto account macchina da utilizzare per l'autenticazione. Questo non è diverso dal modo in cui un client SMB di Windows si unisce a un dominio e richiede gli stessi diritti di accesso alle unità organizzative (OU) in Active Directory.

In molti casi, i gruppi di protezione non consentono l'utilizzo di un account amministratore di Windows su server esterni come Cloud Volumes Service. In alcuni casi, l'utente amministratore di Windows viene disattivato completamente come procedura consigliata per la protezione.

Autorizzazioni necessarie per creare account di macchine SMB

Per aggiungere oggetti computer Cloud Volumes Service a un'Active Directory, un account che dispone di diritti amministrativi per il dominio o che dispone di ["autorizzazioni delegate per creare e modificare oggetti account macchina"](#) a un'unità organizzativa specificata. È possibile eseguire questa operazione con la delega guidata del controllo in Active Directory creando un'attività personalizzata che fornisce all'utente l'accesso alla creazione/eliminazione di oggetti computer con le seguenti autorizzazioni di accesso:

- Lettura/scrittura
- Crea/Elimina tutti gli oggetti figlio
- Lettura/scrittura di tutte le proprietà
- Modificare/reimpostare la password

Questa operazione consente di aggiungere automaticamente un ACL di sicurezza per l'utente definito all'unità organizzativa in Active Directory e di ridurre al minimo l'accesso all'ambiente Active Directory. Dopo la delega di un utente, il nome utente e la password possono essere forniti come credenziali Active Directory in questa finestra.



Il nome utente e la password passati al dominio Active Directory sfruttano la crittografia Kerberos durante la query e la creazione dell'oggetto account del computer per una maggiore sicurezza.

Dettagli della connessione ad Active Directory

Il ["Dettagli connessione Active Directory"](#) Fornire agli amministratori campi per fornire informazioni specifiche

sullo schema di Active Directory per il posizionamento degli account del computer, ad esempio:

- **Tipo di connessione Active Directory.** consente di specificare se la connessione Active Directory in una regione viene utilizzata per volumi di tipo Cloud Volumes Service o CVS-Performance. Se questa impostazione non è corretta su una connessione esistente, potrebbe non funzionare correttamente quando viene utilizzata o modificata.
- **Domain.** il nome di dominio di Active Directory.
- **Site.** limita i server Active Directory a un sito specifico per motivi di sicurezza e performance "[considerazioni](#)". Ciò è necessario quando più server Active Directory si estendono in aree diverse, in quanto Cloud Volumes Service attualmente non supporta l'autorizzazione di richieste di autenticazione Active Directory per i server Active Directory in un'area diversa dall'istanza di Cloud Volumes Service. Ad esempio, il controller di dominio Active Directory si trova in un'area supportata solo da CVS-Performance, ma si desidera una condivisione SMB in un'istanza CVS-SW.
- **Server DNS.** server DNS da utilizzare nelle ricerche dei nomi.
- **Nome NetBIOS (opzionale).** se lo si desidera, il nome NetBIOS del server. Questa opzione viene utilizzata quando vengono creati nuovi account computer utilizzando la connessione Active Directory. Ad esempio, se il nome NetBIOS è impostato su CVS-EAST, i nomi degli account del computer saranno CVS-EAST-{1234}. Vedere la sezione "[Come viene visualizzato Cloud Volumes Service in Active Directory](#)" per ulteriori informazioni.
- **Unità organizzativa (OU).** unità organizzativa specifica per la creazione dell'account del computer. Ciò è utile se si sta delegando il controllo a un utente per gli account di computer a una specifica unità organizzativa.
- **Crittografia AES.** è inoltre possibile selezionare o deselezionare la casella di controllo Enable AES Encryption for ad Authentication. L'attivazione della crittografia AES per l'autenticazione di Active Directory offre una maggiore sicurezza per le comunicazioni Cloud Volumes Service-Active Directory durante le ricerche di utenti e gruppi. Prima di attivare questa opzione, rivolgersi all'amministratore di dominio per verificare che i controller di dominio Active Directory supportino l'autenticazione AES.



Per impostazione predefinita, la maggior parte dei server Windows non disattiva le crittografia più deboli (AD esempio DES o RC4-HMAC), ma se si sceglie di disattivare le crittografia più deboli, verificare che la connessione Active Directory di Cloud Volumes Service sia stata configurata per abilitare AES. In caso contrario, si verificano errori di autenticazione. L'attivazione della crittografia AES non disattiva le crittografie più deboli, ma aggiunge il supporto per le crittografie AES all'account della macchina SMB di Cloud Volumes Service.

Dettagli area di autenticazione Kerberos

Questa opzione non si applica ai server SMB. Viene invece utilizzato durante la configurazione di NFS Kerberos per il sistema Cloud Volumes Service. Quando questi dettagli vengono popolati, viene configurato l'ambiente Kerberos NFS (simile a un file krb5.conf su Linux) e viene utilizzato quando NFS Kerberos viene specificato nella creazione del volume Cloud Volumes Service, in quanto la connessione Active Directory agisce come centro di distribuzione Kerberos NFS (KDC).



Attualmente i KDC non Windows non sono supportati per l'utilizzo con Cloud Volumes Service.

Regione

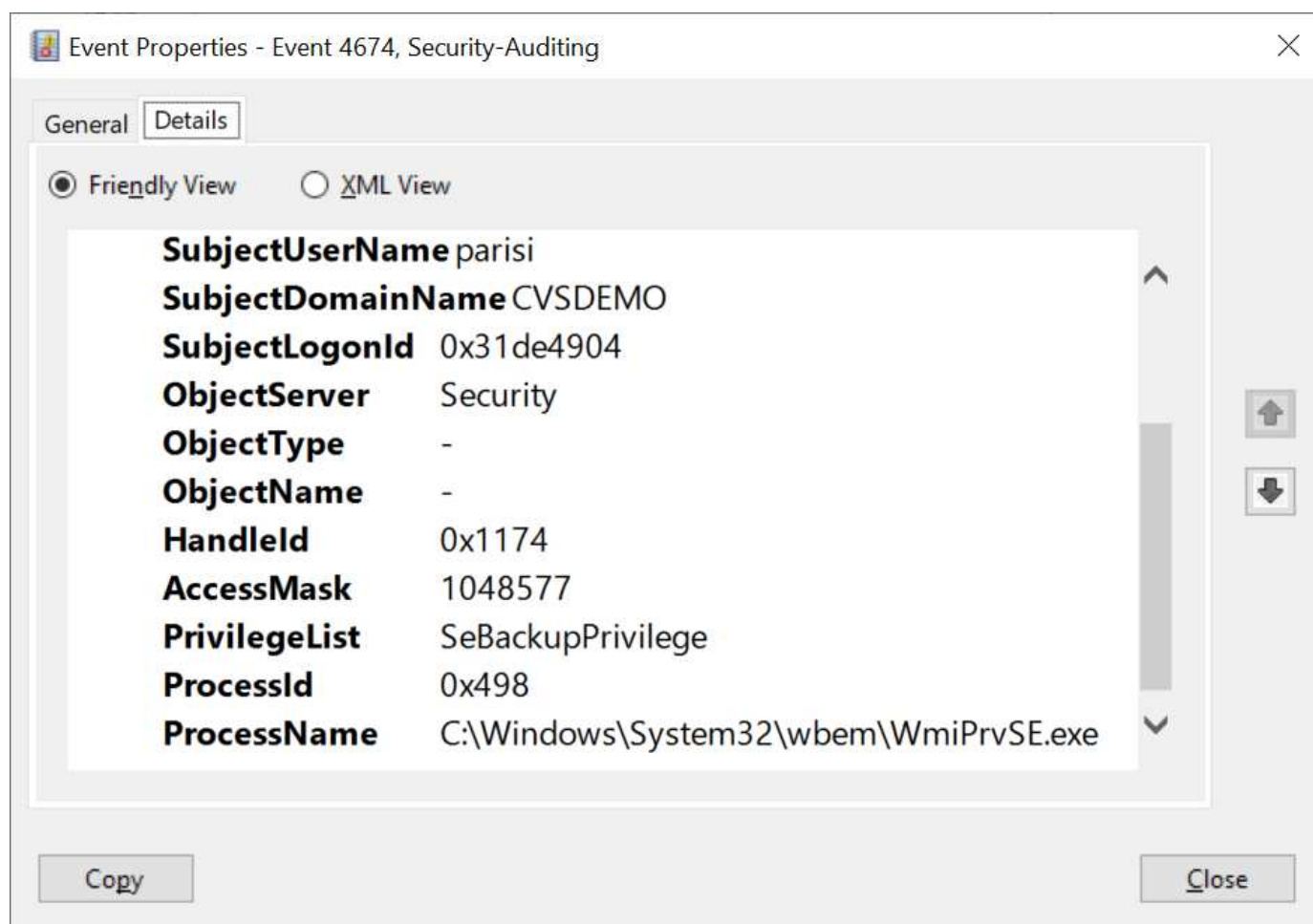
Una regione consente di specificare la posizione in cui risiede la connessione Active Directory. Questa regione deve essere la stessa del volume Cloud Volumes Service.

- **Local NFS Users with LDAP.** in questa sezione è disponibile anche un'opzione per consentire agli utenti

NFS locali con LDAP. Questa opzione deve essere lasciata deselezionata se si desidera estendere il supporto dell'appartenenza al gruppo di utenti UNIX oltre la limitazione di 16 gruppi di NFS (gruppi estesi). Tuttavia, l'utilizzo di gruppi estesi richiede un server LDAP configurato per le identità UNIX. Se non si dispone di un server LDAP, lasciare deselezionata questa opzione. Se si dispone di un server LDAP e si desidera utilizzare anche utenti UNIX locali (ad esempio root), selezionare questa opzione.

Utenti di backup

Questa opzione consente di specificare gli utenti Windows che dispongono delle autorizzazioni di backup per il volume Cloud Volumes Service. I privilegi di backup (SeBackupPrivilege) sono necessari per consentire ad alcune applicazioni di eseguire correttamente il backup e il ripristino dei dati nei volumi NAS. Questo utente dispone di un elevato livello di accesso ai dati nel volume, pertanto è necessario prendere in considerazione l'opzione "[abilitazione del controllo dell'accesso dell'utente](#)". Una volta attivato, gli eventi di controllo vengono visualizzati nel Visualizzatore eventi > Log di Windows > protezione.



Utenti con privilegi di sicurezza

Questa opzione consente di specificare gli utenti Windows che dispongono delle autorizzazioni per la modifica della protezione per il volume Cloud Volumes Service. Alcuni privilegi di sicurezza (SeSecurityPrivilege) sono necessari per alcune applicazioni ("[Ad esempio SQL Server](#)") per impostare correttamente le autorizzazioni durante l'installazione. Questo privilegio è necessario per gestire il registro di protezione. Sebbene questo privilegio non sia potente come SeBackupPrivilege, NetApp consiglia "[controllo dell'accesso degli utenti](#)" con questo livello di privilegio, se necessario.

Per ulteriori informazioni, vedere "[Privilegi speciali assegnati al nuovo accesso](#)".

Come viene visualizzato Cloud Volumes Service in Active Directory

Cloud Volumes Service viene visualizzato in Active Directory come un normale oggetto account del computer. Le convenzioni di denominazione sono le seguenti.

- CIFS/SMB e NFS Kerberos creano oggetti account macchina separati.
- NFS con LDAP attivato crea un account macchina in Active Directory per i binding LDAP Kerberos.
- I volumi a doppio protocollo con LDAP condividono l'account CIFS/SMB per LDAP e SMB.
- Gli account CIFS/SMB utilizzano una convenzione di naming name-1234 (ID casuale a quattro cifre con trattino aggiunto al nome <10 caratteri) per l'account del computer. È possibile definire IL NOME in base all'impostazione NetBIOS name (Nome NetBIOS) sulla connessione Active Directory (vedere la sezione "[Dettagli della connessione ad Active Directory](#)").
- NFS Kerberos utilizza NFS-NAME-1234 come convenzione di naming (fino a 15 caratteri). Se vengono utilizzati più di 15 caratteri, il nome è NFS-TRUNCED-NAME-1234.
- Le istanze CVS-Performance solo NFS con LDAP attivato creano un account SMB Machine per l'associazione al server LDAP con la stessa convenzione di denominazione delle istanze CIFS/SMB.
- Quando viene creato un account SMB Machine, le condivisioni amministrative nascoste predefinite (vedere la sezione "[Condivisioni nascoste predefinite](#)"), ma tali condivisioni non hanno ACL assegnati e non sono accessibili.
- Per impostazione predefinita, gli oggetti del centro di costo del computer vengono posizionati in CN=Computers, ma R è possibile specificare un'unità organizzativa diversa quando necessario. Vedere la sezione "[Autorizzazioni necessarie per creare account di macchine SMB](#)" Per informazioni sui diritti di accesso necessari per aggiungere/rimuovere oggetti account macchina per Cloud Volumes Service.

Quando Cloud Volumes Service aggiunge l'account del computer SMB ad Active Directory, vengono compilati i seguenti campi:

- cn (con il nome del server SMB specificato)
- DNSHostName (con SMBserver.domain.com)
- MSDS-SupportedEncryptionTypes (supporta DES_CBC_MD5, RC4_HMAC_MD5 se la crittografia AES non è attivata; se la crittografia AES è attivata, DES_CBC_MD5, RC4_HMAC_MD5, AES128_CTS_HMAC_SHA1_96, AES256_CTS_HMAC_SHA1_96 sono consentiti per lo scambio di account con il ticket SMB)
- Nome (con il nome del server SMB)
- SAMAccountName (con SMBserver)
- ServicePrincipalName (con host/smbserver.domain.com e host/smbserver SPN per Kerberos)

Se si desidera disattivare i tipi di crittografia Kerberos più deboli (enttype) sull'account del computer, è possibile modificare il valore MSDS-SupportedEncryptionTypes sull'account del computer scegliendo uno dei valori nella tabella seguente per consentire solo AES.

Valore MSDS-SupportedEncryptionTypes	Entype attivato
2	DES_CBC_MD5
4	RC4_HMAC
8	SOLO AES128_CTS_HMAC_SHA1_96
16	SOLO AES256_CTS_HMAC_SHA1_96

Valore MSDS-SupportedEncryptionTypes	Entype attivato
24	AES128_CTS_HMAC_SHA1_96 E AES256_CTS_HMAC_SHA1_96
30	DES_CBC_MD5, RC4_HMAC, AES128_CTS_HMAC_SHA1_96 E AES256_CTS_HMAC_SHA1_96

Per attivare la crittografia AES per gli account dei computer SMB, fare clic su Enable AES Encryption for ad Authentication (attiva crittografia AES per l'autenticazione ad) quando si crea la connessione Active Directory.

Per attivare la crittografia AES per NFS Kerberos, "[Consultare la documentazione di Cloud Volumes Service](#)".

Altre dipendenze del servizio infrastruttura NAS (KDC, LDAP e DNS)

Quando si utilizza Cloud Volumes Service per le condivisioni NAS, potrebbero essere necessarie dipendenze esterne per un corretto funzionamento. Queste dipendenze sono in gioco in circostanze specifiche. La seguente tabella mostra le varie opzioni di configurazione e le eventuali dipendenze richieste.

Configurazione	Dipendenze richieste
Solo NFSv3	Nessuno
Solo NFSv3 Kerberos	Active Directory di Windows: * KDC * DNS * LDAP
Solo NFSv4.1	Configurazione mappatura ID client (/etc/idmap.conf)
Solo NFSv4.1 Kerberos	<ul style="list-style-type: none"> Configurazione mappatura ID client (/etc/idmap.conf) Active Directory di Windows: LDAP DNS KDC
Solo SMB	Active Directory: * KDC * DNS
NAS multiprotocollo (NFS e SMB)	<ul style="list-style-type: none"> Configurazione del mapping dell'ID client (solo NFSv4.1; /etc/idmap.conf) Active Directory di Windows: LDAP DNS KDC

La rotazione/password del keytab Kerberos viene reimpostata per gli oggetti account macchina

Con gli account delle macchine SMB, Cloud Volumes Service pianifica il ripristino periodico delle password per l'account delle macchine SMB. Queste password vengono reimpostate utilizzando la crittografia Kerberos e vengono eseguite ogni quarta domenica in un orario casuale compreso tra LE 23:00 e L'1:00. Queste reimpostazioni delle password modificano le versioni delle chiavi Kerberos, ruotano le linguette memorizzate nel sistema Cloud Volumes Service e contribuiscono a mantenere un livello di sicurezza maggiore per i server SMB in esecuzione in Cloud Volumes Service. Le password dell'account macchina sono casuali e non sono note agli amministratori.

Per gli account delle macchine Kerberos NFS, la reimpostazione delle password avviene solo quando viene creata o scambiata una nuova keytab con il KDC. Attualmente, non è possibile eseguire questa operazione in Cloud Volumes Service.

Porte di rete per l'utilizzo con LDAP e Kerberos

Quando si utilizzano LDAP e Kerberos, è necessario determinare le porte di rete utilizzate da questi servizi. L'elenco completo delle porte utilizzate da Cloud Volumes Service è disponibile nella ["Documentazione Cloud Volumes Service sulle considerazioni relative alla sicurezza"](#).

LDAP

Cloud Volumes Service agisce come client LDAP e utilizza le query di ricerca LDAP standard per le ricerche di utenti e gruppi per le identità UNIX. LDAP è necessario se si intende utilizzare utenti e gruppi al di fuori degli utenti predefiniti standard forniti da Cloud Volumes Service. LDAP è necessario anche se si prevede di utilizzare NFS Kerberos con le identità dell'utente (ad esempio [user1@domain.com](#)). Attualmente, è supportato solo LDAP con Microsoft Active Directory.

Per utilizzare Active Directory come server LDAP UNIX, è necessario popolare gli attributi UNIX necessari per gli utenti e i gruppi che si intende utilizzare per le identità UNIX. Cloud Volumes Service utilizza un modello di schema LDAP predefinito che esegue query sugli attributi in base a ["RFC-2307-bis"](#). Di conseguenza, la seguente tabella mostra gli attributi minimi necessari di Active Directory da popolare per utenti e gruppi e per quale scopo viene utilizzato ciascun attributo.

Per ulteriori informazioni sull'impostazione degli attributi LDAP in Active Directory, vedere ["Gestione dell'accesso a doppio protocollo."](#)

Attributo	Che cosa fa
uid*	Specifica il nome utente UNIX
UidNumber*	Specifica l'ID numerico dell'utente UNIX
GidNumber*	Specifica l'ID numerico del gruppo primario dell'utente UNIX
Objectclass*	Specifica il tipo di oggetto utilizzato; Cloud Volumes Service richiede che l'opzione "user" sia inclusa nell'elenco delle classi di oggetti (per impostazione predefinita, è inclusa nella maggior parte delle implementazioni di Active Directory).
nome	Informazioni generali sull'account (nome reale, numero di telefono e così via, anche noto come gecost)
UnixUserPassword	Non è necessario impostare questo valore; non utilizzato nelle ricerche di identità UNIX per l'autenticazione NAS. Impostando questa opzione, il valore unixUserPassword configurato viene visualizzato in testo non crittografato.
UnixHomeDirectory	Definisce il percorso delle home directory UNIX quando un utente esegue l'autenticazione LDAP da un client Linux. Impostare questa opzione se si desidera utilizzare la funzionalità della home directory LDAP per UNIX.
LoginShell	Definisce il percorso della shell bash/profile per i client Linux quando un utente esegue l'autenticazione con LDAP.

*Indica che l'attributo è necessario per la corretta funzionalità con Cloud Volumes Service. Gli attributi rimanenti sono solo per uso lato client.

Attributo	Che cosa fa
cn*	Specifica il nome del gruppo UNIX. Quando si utilizza Active Directory per LDAP, questo viene impostato quando l'oggetto viene creato per la prima volta, ma può essere modificato in seguito. Questo nome non può essere uguale ad altri oggetti. Ad esempio, se l'utente UNIX denominato user1 appartiene a un gruppo denominato user1 sul client Linux, Windows non consente due oggetti con lo stesso attributo cn. Per risolvere questo problema, rinominare l'utente Windows con un nome univoco (ad esempio, user1-UNIX); LDAP in Cloud Volumes Service utilizza l'attributo uid per i nomi utente UNIX.
GidNumber*	Specifica l'ID numerico del gruppo UNIX.
Objectclass*	Specifica il tipo di oggetto utilizzato; Cloud Volumes Service richiede che il gruppo sia incluso nell'elenco delle classi di oggetti (questo attributo è incluso per impostazione predefinita nella maggior parte delle implementazioni di Active Directory).
MemberUid	Specifica quali utenti UNIX sono membri del gruppo UNIX. Con Active Directory LDAP in Cloud Volumes Service, questo campo non è necessario. Lo schema LDAP di Cloud Volumes Service utilizza il campo membro per le appartenenze ai gruppi.
Membro*	Richiesto per le appartenenze a gruppi/gruppi UNIX secondari. Questo campo viene compilato aggiungendo utenti Windows ai gruppi Windows. Tuttavia, se i gruppi Windows non hanno attributi UNIX popolati, non vengono inclusi negli elenchi di appartenenza del gruppo dell'utente UNIX. Tutti i gruppi che devono essere disponibili in NFS devono compilare gli attributi del gruppo UNIX richiesti elencati in questa tabella.

*Indica che l'attributo è necessario per la corretta funzionalità con Cloud Volumes Service. Gli attributi rimanenti sono solo per uso lato client.

Informazioni di binding LDAP

Per eseguire query agli utenti in LDAP, Cloud Volumes Service deve essere associato (login) al servizio LDAP. Questo accesso dispone di permessi di sola lettura e viene utilizzato per eseguire query sugli attributi LDAP UNIX per le ricerche di directory. Attualmente, i binding LDAP sono possibili solo utilizzando un account di macchina SMB.

È possibile attivare LDAP solo per CVS-Performance E utilizzarlo per volumi NFSv3, NFSv4.1 o a doppio protocollo. È necessario stabilire una connessione Active Directory nella stessa regione del volume Cloud Volumes Service per una corretta implementazione del volume abilitato LDAP.

Quando LDAP è attivato, in scenari specifici si verifica quanto segue.

- Se per il progetto Cloud Volumes Service viene utilizzato solo NFSv3 o NFSv4.1, viene creato un nuovo account computer nel controller di dominio Active Directory e il client LDAP in Cloud Volumes Service esegue l'associazione ad Active Directory utilizzando le credenziali dell'account del computer. Non vengono create condivisioni SMB per il volume NFS e le condivisioni amministrative nascoste predefinite (vedere la sezione [""Condivisioni nascoste predefinite""](#)) Hanno rimosso gli ACL di condivisione.
- Se per il progetto Cloud Volumes Service vengono utilizzati volumi a doppio protocollo, viene utilizzato solo l'account singolo del computer creato per l'accesso SMB per associare il client LDAP in Cloud Volumes Service ad Active Directory. Non vengono creati account macchina aggiuntivi.
- Se i volumi SMB dedicati vengono creati separatamente (prima o dopo l'attivazione dei volumi NFS con LDAP), l'account del computer per i binding LDAP viene condiviso con l'account del computer SMB.
- Se è attivato anche NFS Kerberos, vengono creati due account macchina: Uno per le condivisioni SMB e/o le binding LDAP e uno per l'autenticazione Kerberos NFS.

Query LDAP

Anche se i binding LDAP sono crittografati, le query LDAP vengono trasmesse via cavo in testo non crittografato utilizzando la porta LDAP comune 389. Questa porta nota non può essere modificata in Cloud Volumes Service. Di conseguenza, un utente con accesso allo sniffing dei pacchetti nella rete può visualizzare i nomi degli utenti e dei gruppi, gli ID numerici e le appartenenze ai gruppi.

Tuttavia, le macchine virtuali Google Cloud non possono sniff il traffico unicast di altre macchine virtuali. Solo le macchine virtuali che partecipano attivamente al traffico LDAP (ovvero, sono in grado di eseguire il binding) possono visualizzare il traffico proveniente dal server LDAP. Per ulteriori informazioni sullo sniffing dei pacchetti in Cloud Volumes Service, consulta la sezione [""Considerazioni su sniffing/traccia dei pacchetti""](#).

Impostazioni predefinite della configurazione del client LDAP

Quando LDAP è attivato in un'istanza di Cloud Volumes Service, per impostazione predefinita viene creata una configurazione del client LDAP con dettagli di configurazione specifici. In alcuni casi, le opzioni non sono valide per Cloud Volumes Service (non supportate) o non sono configurabili.

Opzione del client LDAP	Che cosa fa	Valore predefinito	Può cambiare?
Elenco server LDAP	Consente di impostare i nomi dei server LDAP o gli indirizzi IP da utilizzare per le query. Non utilizzato per Cloud Volumes Service. Viene invece utilizzato Active Directory Domain per definire i server LDAP.	Non impostato	No
Dominio Active Directory	Imposta il dominio Active Directory da utilizzare per le query LDAP. Cloud Volumes Service sfrutta i record SRV per LDAP nel DNS per trovare i server LDAP nel dominio.	Impostare sul dominio Active Directory specificato nella connessione Active Directory.	No

Opzione del client LDAP	Che cosa fa	Valore predefinito	Può cambiare?
Server Active Directory preferiti	Imposta i server Active Directory preferiti da utilizzare per LDAP. Non supportato da Cloud Volumes Service. Utilizzare i siti Active Directory per controllare la selezione del server LDAP.	Non impostato.	No
Eseguire il binding utilizzando le credenziali del server SMB	Esegue il binding a LDAP utilizzando l'account SMB Machine. Attualmente, l'unico metodo di binding LDAP supportato in Cloud Volumes Service.	Vero	No
Modello di schema	Modello di schema utilizzato per le query LDAP.	MS-AD-BIS	No
Porta del server LDAP	Il numero di porta utilizzato per le query LDAP. Attualmente Cloud Volumes Service utilizza solo la porta LDAP standard 389. LDAPS/porta 636 non è attualmente supportato.	389	No
LDAPS è attivato	Controlla se LDAP su SSL (Secure Sockets Layer) viene utilizzato per query e binding. Attualmente non supportato da Cloud Volumes Service.	Falso	No
Timeout query (sec)	Timeout per query. Se le query richiedono più tempo del valore specificato, le query non vengono eseguite correttamente.	3	No
Livello minimo di autenticazione bind	Il livello minimo di binding supportato. Poiché Cloud Volumes Service utilizza account di computer per i binding LDAP e Active Directory non supporta i binding anonimi per impostazione predefinita, questa opzione non viene utilizzata per motivi di sicurezza.	Anonimo	No

Opzione del client LDAP	Che cosa fa	Valore predefinito	Può cambiare?
DN di binding	Nome utente/distinto (DN) utilizzato per i binding quando viene utilizzato il binding semplice. Cloud Volumes Service utilizza account computer per i binding LDAP e attualmente non supporta l'autenticazione di binding semplice.	Non impostato	No
DN di base	Il DN di base utilizzato per le ricerche LDAP.	Il dominio Windows utilizzato per la connessione Active Directory, in formato DN (DC=dominio, DC=locale).	No
Ambito di ricerca di base	Ambito di ricerca per le ricerche DN di base. I valori possono includere base, onelevel o sottostruttura. Cloud Volumes Service supporta solo le ricerche in sottostruttura.	Sottostruttura	No
DN utente	Definisce il DN in cui l'utente avvia le ricerche per le query LDAP. Attualmente non supportato per Cloud Volumes Service, pertanto tutte le ricerche degli utenti iniziano dal DN di base.	Non impostato	No
Ambito della ricerca dell'utente	L'ambito di ricerca per le ricerche DN dell'utente. I valori possono includere base, onelevel o sottostruttura. Cloud Volumes Service non supporta l'impostazione dell'ambito di ricerca dell'utente.	Sottostruttura	No
DN gruppo	Definisce il DN in cui iniziano le ricerche di gruppo per le query LDAP. Attualmente non supportato per Cloud Volumes Service, quindi tutte le ricerche di gruppo iniziano dal DN di base.	Non impostato	No

Opzione del client LDAP	Che cosa fa	Valore predefinito	Può cambiare?
Ambito della ricerca di gruppo	Ambito di ricerca per le ricerche DN di gruppo. I valori possono includere base, onelevel o sottostruttura. Cloud Volumes Service non supporta l'impostazione dell'ambito di ricerca di gruppo.	Sottostruttura	No
DN netgroup	Definisce il DN in cui inizia la ricerca delle query LDAP da parte del netgroup. Attualmente non supportato per Cloud Volumes Service, pertanto tutte le ricerche dei netgroup iniziano dal DN di base.	Non impostato	No
Ambito della ricerca nel netgroup	Ambito di ricerca per le ricerche DN dei netgroup. I valori possono includere base, onelevel o sottostruttura. Cloud Volumes Service non supporta l'impostazione dell'ambito di ricerca del netgroup.	Sottostruttura	No
USA start_tls su LDAP	Sfrutta Start TLS per connessioni LDAP basate su certificato sulla porta 389. Attualmente non supportato da Cloud Volumes Service.	Falso	No
Attiva la ricerca netgroup-by-host	Attiva le ricerche di netgroup in base al nome host piuttosto che espandere i netgroup per elencare tutti i membri. Attualmente non supportato da Cloud Volumes Service.	Falso	No
DN netgroup-by-host	Definisce il DN in cui iniziano le ricerche netgroup-by-host per le query LDAP. Netgroup-by-host attualmente non è supportato per Cloud Volumes Service.	Non impostato	No

Opzione del client LDAP	Che cosa fa	Valore predefinito	Può cambiare?
Ambito di ricerca netgroup-by-host	Ambito di ricerca per le ricerche DN netgroup-by-host. I valori possono includere base, onelevel o sottostruttura. Netgroup-by-host attualmente non è supportato per Cloud Volumes Service.	Sottostruttura	No
Sicurezza della sessione client	Definisce il livello di sicurezza della sessione utilizzato da LDAP (Sign, Seal o NONE). La firma LDAP è supportata da CVS-Performance, se richiesto da Active Directory. CVS-SW non supporta la firma LDAP. Per entrambi i tipi di servizio, il sealing non è attualmente supportato.	Nessuno	No
Ricerca di riferimenti LDAP	Quando si utilizzano più server LDAP, la ricerca dei riferimenti consente al client di fare riferimento ad altri server LDAP nell'elenco quando non viene trovata una voce nel primo server. Attualmente non è supportato da Cloud Volumes Service.	Falso	No
Filtro di appartenenza al gruppo	Fornisce un filtro di ricerca LDAP personalizzato da utilizzare quando si cerca l'appartenenza a un gruppo da un server LDAP. Attualmente non supportato con Cloud Volumes Service.	Non impostato	No

Utilizzo di LDAP per la mappatura asimmetrica dei nomi

Cloud Volumes Service, per impostazione predefinita, esegue il mapping bidirezionale degli utenti Windows e UNIX con nomi utente identici senza alcuna configurazione speciale. Finché Cloud Volumes Service trova un utente UNIX valido (con LDAP), viene eseguita la mappatura del nome 1:1. Ad esempio, se utente Windows johnsmith Viene utilizzato, quindi, se Cloud Volumes Service riesce a trovare un utente UNIX denominato johnsmith In LDAP, la mappatura dei nomi riesce per quell'utente, tutti i file/cartelle creati da johnsmith Mostrare la corretta proprietà dell'utente e tutti gli ACL che influiscono johnsmith Sono onorati indipendentemente dal protocollo NAS in uso. Questa funzione è nota come mappatura dei nomi simmetrica.

Il mapping asimmetrico dei nomi si verifica quando l'identità dell'utente Windows e UNIX non corrispondono.

Ad esempio, se utente Windows `johnsmith` Ha un'identità UNIX di `jsmith`, Cloud Volumes Service ha bisogno di un modo per essere raccontata della variazione. Poiché Cloud Volumes Service attualmente non supporta la creazione di regole di mappatura dei nomi statiche, è necessario utilizzare LDAP per cercare l'identità degli utenti per le identità Windows e UNIX, al fine di garantire la corretta proprietà di file e cartelle e le autorizzazioni previste.

Per impostazione predefinita, Cloud Volumes Service include LDAP Nel ns-switch dell'istanza per il database della mappa dei nomi, in modo che per fornire la funzionalità di mappatura dei nomi utilizzando LDAP per i nomi asimmetrici, è sufficiente modificare alcuni attributi utente/gruppo per riflettere ciò che Cloud Volumes Service cerca.

La tabella seguente mostra gli attributi da inserire in LDAP per la funzionalità di mappatura asimmetrica dei nomi. Nella maggior parte dei casi, Active Directory è già configurato per eseguire questa operazione.

Attributo Cloud Volumes Service	Che cosa fa	Valore utilizzato da Cloud Volumes Service per la mappatura dei nomi
ObjectClass da Windows a UNIX	Specifica il tipo di oggetto utilizzato. (Ovvero, utente, gruppo, posixAccount e così via)	Deve includere l'utente (può contenere più altri valori, se lo si desidera).
Attributo da Windows a UNIX	Che definisce il nome utente Windows al momento della creazione. Cloud Volumes Service lo utilizza per le ricerche da Windows a UNIX.	Nessuna modifica necessaria; sAMAccountName corrisponde al nome di accesso di Windows.
UID	Definisce il nome utente UNIX.	Nome utente UNIX desiderato.

Cloud Volumes Service attualmente non utilizza prefissi di dominio nelle ricerche LDAP, pertanto gli ambienti LDAP di più domini non funzionano correttamente con le ricerche della mappa dei nomi LDAP.

Nell'esempio riportato di seguito viene illustrato un utente con il nome Windows `asymmetric`, Il nome UNIX ``unix-user`` E il comportamento che segue quando si scrivono file da SMB e NFS.

La figura seguente mostra l'aspetto degli attributi LDAP dal server Windows.

Published Certificates	Member Of	Password Replication	Dial-in	Object
Security	Environment	Sessions	Remote control	
General	Address	Account	Profile	Telephones
Remote Desktop Services Profile		COM+	Attribute Editor	

Attributes:

Attribute	Value
name	asymmetric
objectCategory	CN=Person,CN=Schema,CN=Configuration,
objectClass	top; person; organizationalPerson; user
objectGUID	de489556-dd7b-43a3-98fa-2722f79d67ed
objectSid	S-1-5-21-3552729481-4032800560-2279794
primaryGroupID	513 = (GROUP_RID_USERS)
pwdLastSet	1/19/2017 1:56:34 PM Eastern Standard Time
replPropertyMetaData	AttID Ver Loc.USN Org.DSA
sAMAccountName	asymmetric
sAMAccountType	805306368 = (NORMAL_USER_ACCOUNT)
uid	unix-user
uidNumber	1207

Da un client NFS, è possibile eseguire una query sul nome UNIX ma non sul nome di Windows:

```
# id unix-user
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
# id asymmetric
id: asymmetric: no such user
```

Quando un file viene scritto da NFS come `unix-user`, il seguente è il risultato del client NFS:

```
sh-4.2$ pwd
/mnt/home/ntfssh-4.2$ touch unix-user-file
sh-4.2$ ls -la | grep unix-user
-rwx----- 1 unix-user sharedgroup 0 Feb 28 12:37 unix-user-nfs
sh-4.2$ id
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
```

Da un client Windows, è possibile vedere che il proprietario del file è impostato sull'utente Windows appropriato:

```
PS C:\ > Get-Acl \\demo\home\ntfs\unix-user-nfs | select Owner
Owner
-----
NTAP\asymmetric
```

Al contrario, i file creati dall'utente Windows `asymmetric` Da un client SMB mostrare il proprietario UNIX appropriato, come mostrato nel testo seguente.

PMI:

```
PS Z:\ntfs> echo TEXT > asymmetric-user-smb.txt
```

NFS:

```
sh-4.2$ ls -la | grep asymmetric-user-smb.txt
-rwx----- 1 unix-user          sharedgroup   14 Feb 28 12:43 asymmetric-
user-smb.txt
sh-4.2$ cat asymmetric-user-smb.txt
TEXT
```

Binding del canale LDAP

A causa di una vulnerabilità dei controller di dominio Active Directory di Windows, "[Microsoft Security Advisory ADV190023](#)" Modifica il modo in cui i controller di dominio consentono i binding LDAP.

L'impatto per Cloud Volumes Service è lo stesso di qualsiasi client LDAP. Cloud Volumes Service attualmente non supporta il binding del canale. Poiché Cloud Volumes Service supporta la firma LDAP per impostazione predefinita attraverso la negoziazione, l'associazione del canale LDAP non dovrebbe rappresentare un problema. In caso di problemi di associazione a LDAP con l'associazione del canale attivata, seguire la procedura di risoluzione descritta in ADV190023 per consentire l'esecuzione dei binding LDAP da Cloud Volumes Service.

DNS

Active Directory e Kerberos hanno entrambe dipendenze dal DNS per la risoluzione dei nomi host all'IP/IP. Il DNS richiede che la porta 53 sia aperta. Cloud Volumes Service non apporà alcuna modifica ai record DNS, né supporta attualmente l'utilizzo di "[DNS dinamico](#)" sulle interfacce di rete.

È possibile configurare il DNS di Active Directory per limitare i server che possono aggiornare i record DNS. Per ulteriori informazioni, vedere "[DNS Windows sicuro](#)".

Si noti che le risorse all'interno di un progetto Google utilizzano per impostazione predefinita il DNS di Google Cloud, che non è connesso al DNS di Active Directory. I client che utilizzano il DNS cloud non possono risolvere i percorsi UNC restituiti da Cloud Volumes Service. I client Windows associati al dominio Active Directory sono configurati per utilizzare il DNS di Active Directory e possono risolvere tali percorsi UNC.

Per aggiungere un client ad Active Directory, è necessario configurare la relativa configurazione DNS in modo che utilizzi il DNS di Active Directory. Facoltativamente, è possibile configurare il DNS cloud per inoltrare le richieste al DNS di Active Directory. Vedere ["Perché il client non riesce a risolvere il nome NetBIOS SMB?"](#) per ulteriori informazioni.



Cloud Volumes Service attualmente non supporta DNSSEC e le query DNS vengono eseguite in formato non crittografato.

Controllo dell'accesso al file

Attualmente non supportato per Cloud Volumes Service.

Protezione antivirus

È necessario eseguire la scansione antivirus in Cloud Volumes Service sul client in una condivisione NAS. Attualmente non esiste alcuna integrazione antivirus nativa con Cloud Volumes Service.

Funzionamento del servizio

Il team di Cloud Volumes Service gestisce i servizi di back-end in Google Cloud e utilizza diverse strategie per proteggere la piattaforma e prevenire accessi indesiderati.

Ogni cliente ottiene la propria subnet univoca che ha accesso negato da altri clienti per impostazione predefinita e ogni tenant in Cloud Volumes Service ottiene il proprio namespace e la propria VLAN per l'isolamento totale dei dati. Dopo l'autenticazione di un utente, il Service Delivery Engine (SDE) può leggere solo i dati di configurazione specifici del tenant.

Sicurezza fisica

Con un'adeguata preapprovazione, solo i tecnici on-site e gli ingegneri di assistenza sul campo (FSE) con badge NetApp hanno accesso alla gabbia e ai rack per il lavoro fisico. La gestione dello storage e della rete non è consentita. Solo queste risorse on-site sono in grado di eseguire attività di manutenzione dell'hardware.

Per i tecnici in loco, viene presentato un ticket per la dichiarazione di lavoro (SOW) che include l'ID del rack e la posizione del dispositivo (RU) e tutti gli altri dettagli sono inclusi nel ticket. Per gli FSE NetApp, è necessario inoltrare un ticket di visita del sito con IL COLO e il biglietto include i dettagli, la data e l'ora del visitatore per scopi di verifica. Il SOW del FSE viene comunicato internamente a NetApp.

Team operativo

Il team operativo di Cloud Volumes Service è composto da tecnici di produzione e da un tecnico di affidabilità del sito (SRE) per i servizi di volume cloud e da tecnici di assistenza sul campo e partner per l'hardware. Tutti i membri del team operativo sono accreditati per il lavoro in Google Cloud e vengono mantenuti record dettagliati di lavoro per ogni ticket generato. Inoltre, è in atto un rigoroso processo di approvazione e controllo delle modifiche per garantire che ogni decisione venga esaminata in modo appropriato.

Il team SRE gestisce il piano di controllo e il modo in cui i dati vengono instradati dalle richieste dell'interfaccia utente all'hardware e al software di back-end in Cloud Volumes Service. Il team SRE gestisce anche le risorse di sistema, ad esempio i massimi di volume e inode. Gli SRE non possono interagire con i dati dei clienti o accedervi. Gli SRE forniscono inoltre il coordinamento con le RMA (Return Material Authorization), come le richieste di sostituzione di nuovi dischi o memoria per l'hardware back-end.

Responsabilità del cliente

I clienti di Cloud Volumes Service gestiscono la gestione dei ruoli utente e di Active Directory della propria organizzazione, nonché le operazioni di volume e dati. I clienti possono avere ruoli amministrativi e delegare le autorizzazioni ad altri utenti finali all'interno dello stesso progetto Google Cloud utilizzando i due ruoli predefiniti forniti da NetApp e Google Cloud (Administrator e Viewer).

L'amministratore può eseguire il peer di qualsiasi VPC all'interno del progetto del cliente a Cloud Volumes Service che il cliente ritiene appropriato. È responsabilità del cliente gestire l'accesso al proprio Google Cloud Marketplace Subscription e i VPC che hanno accesso al data plane.

Protezione SRE dannosa

Una preoccupazione che potrebbe sorgere è come Cloud Volumes Service protegge da scenari in cui si verifica un SRE dannoso o quando le credenziali SRE sono state compromesse?

L'accesso all'ambiente di produzione avviene solo con un numero limitato di individui SRE. I privilegi amministrativi sono ulteriormente limitati a pochi amministratori esperti. Tutte le azioni eseguite da chiunque nell'ambiente di produzione Cloud Volumes Service vengono registrate e qualsiasi anomalia alla linea di base o alle attività sospette viene rilevata dalla nostra piattaforma di Threat intelligence per la gestione delle informazioni sulla sicurezza e degli eventi (SIEM). Di conseguenza, le azioni dannose possono essere monitorate e mitigate prima che venga eseguito un danno eccessivo al backend Cloud Volumes Service.

Ciclo di vita del volume

Cloud Volumes Service gestisce solo gli oggetti all'interno del servizio, non i dati all'interno dei volumi. Solo i client che accedono ai volumi possono gestire i dati, gli ACL, i proprietari dei file e così via. I dati in questi volumi vengono crittografati a riposo e l'accesso è limitato ai tenant dell'istanza di Cloud Volumes Service.

Il ciclo di vita del volume per Cloud Volumes Service è create-update-delete. I volumi conservano le copie Snapshot dei volumi fino all'eliminazione dei volumi e solo gli amministratori Cloud Volumes Service validati possono eliminare i volumi in Cloud Volumes Service. Quando un amministratore richiede l'eliminazione di un volume, per verificare l'eliminazione è necessario inserire un ulteriore passo per il nome del volume. Dopo l'eliminazione di un volume, il volume non viene più utilizzato e non può essere recuperato.

Nei casi in cui un contratto Cloud Volumes Service venga rescisso, NetApp contrassegna i volumi per l'eliminazione dopo un determinato periodo di tempo. Prima della scadenza di tale periodo di tempo, è possibile ripristinare i volumi su richiesta del cliente.

Certificazioni

Cloud Volumes Services per Google Cloud è attualmente certificato in base agli standard ISO/IEC 27001:2013 e ISO/IEC 27018:2019. Il servizio ha inoltre ricevuto di recente il report di attestazione SOC2 di tipo I. Per informazioni sull'impegno di NetApp per la sicurezza e la privacy dei dati, vedere ["Compliance: Sicurezza dei dati e privacy dei dati"](#).

GDPR

I nostri impegni in materia di privacy e conformità al GDPR sono disponibili in diversi nostri ["contratti con i clienti"](#), come il nostro ["Addendum per l'elaborazione dei dati dei clienti"](#), che include ["Clausole contrattuali standard"](#) Fornito dalla Commissione europea. Inoltre, ci impegniamo a rispettare questi impegni nella nostra direttiva sulla privacy, supportata dai valori fondamentali stabiliti nel nostro Codice di condotta aziendale.

Ulteriori informazioni e informazioni di contatto

Per ulteriori informazioni sulle informazioni descritte in questo documento, consultare i seguenti documenti e/o siti Web:

- Documentazione Google Cloud per Cloud Volumes Service

["https://cloud.google.com/architecture/partners/netapp-cloud-volumes/"](https://cloud.google.com/architecture/partners/netapp-cloud-volumes/)

- Accesso al servizio privato di Google

https://cloud.google.com/vpc/docs/private-services-access?hl=en_US

- Documentazione sui prodotti NetApp

["https://www.netapp.com/support-and-training/documentation/"](https://www.netapp.com/support-and-training/documentation/)

- Programma del modulo di convalida crittografica: NetApp CryptoMod

["https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4144"](https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4144)

- La soluzione NetApp per ransomware

<https://www.netapp.com/pdf.html?item=/media/16716-sb-3938pdf.pdf&v=202093745>

- TR-4616: NFS Kerberos in ONTAP

<https://www.netapp.com/pdf.html?item=/media/19384-tr-4616.pdf>

Contattaci

Facci sapere come possiamo migliorare questo report tecnico.

Contattaci all'indirizzo doccomments@netapp.com. Includere IL REPORT TECNICO 4918 nell'oggetto.

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.