Arquitectura

NetApp Solutions

NetApp
April 23, 2024

This PDF was generated from https://docs.netapp.com/es-es/netapp-solutions/ehc/ncvs-gc-architecture_overview.html on April 23, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Arquitectura . . . 1
Descripción general . . . 1
Arquitectura Cloud Volumes Service . . . 1
Arquitectura del plano de control . . . 5
Arquitectura de plano de datos . . . 6
Cifrado de datos en tránsito . . . 7
Cifrado de datos en reposo . . . 12
Servidor de seguridad . . . 13

Arquitectura

Descripción general

Parte de confiar en una solución cloud es comprender la arquitectura y el modo en el que se protege. En esta sección se presentan distintos aspectos de la arquitectura de Cloud Volumes Service en Google para ayudar a solucionar los posibles problemas relacionados con la seguridad de los datos, así como llamadas a áreas en las que se puedan necesitar pasos de configuración adicionales para obtener la puesta en marcha más segura.

La arquitectura general de Cloud Volumes Service se puede dividir en dos componentes principales: El plano de control y el plano de datos.

Plano de control

El plano de control en Cloud Volumes Service es la infraestructura de back-end gestionada por los administradores de Cloud Volumes Service y el software de automatización nativo de NetApp. Este plano es completamente transparente para los usuarios finales e incluye redes, hardware de almacenamiento, actualizaciones de software, etc. para ayudar a ofrecer valor a una solución residente en cloud como Cloud Volumes Service.

Plano de datos

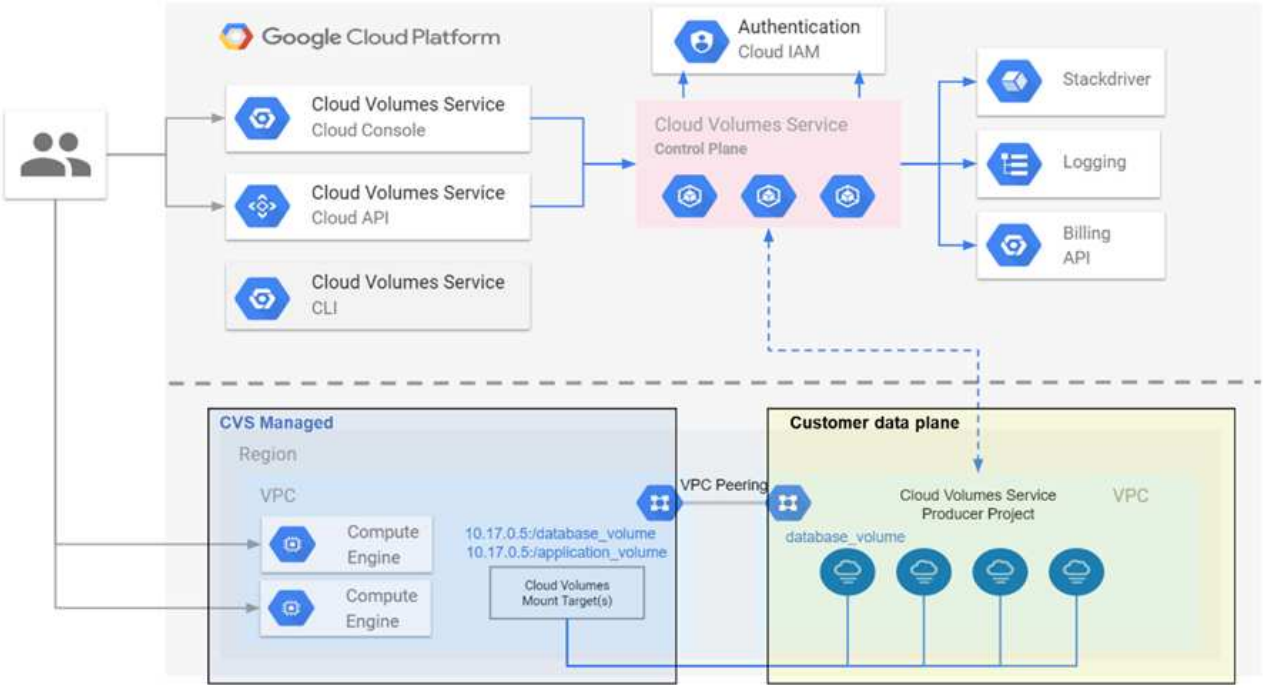
El plano de datos en Cloud Volumes Service incluye los volúmenes de datos reales y la configuración de Cloud Volumes Service general (como el control de acceso, la autenticación de Kerberos, etc.). El plano de datos está totalmente bajo el control de los usuarios finales y de los consumidores de la plataforma Cloud Volumes Service.

Existen diferencias distintas en cómo se asegura y gestiona cada plano. En las siguientes secciones se tratan estas diferencias, empezando por la descripción general de la arquitectura de Cloud Volumes Service.

Arquitectura Cloud Volumes Service

De forma similar a otros servicios nativos de Google Cloud como CloudSQL, Google Cloud VMware Engine (GCVE) y filestore, utiliza Cloud Volumes Service "Google PSA" para prestar el servicio. En PSA, los servicios se construyen dentro de un proyecto de productor de servicios, que utiliza "Agrupación de redes VPC" para conectarse con el consumidor de servicios. El productor de servicios lo proporciona y controla NetApp, y el consumidor de servicios es un VPC en un proyecto de cliente, que aloja a los clientes que desean acceder a recursos compartidos de archivos de Cloud Volumes Service.

La siguiente figura, a la que se hace referencia desde "sección de arquitectura" De la documentación de Cloud Volumes Service, muestra una vista de alto nivel.



La pieza situada encima de la línea de puntos muestra el plano de control del servicio, que controla el ciclo de vida del volumen. La pieza debajo de la línea de puntos muestra el plano de datos. El cuadro azul izquierdo muestra el VPC (consumidor de servicios) del usuario, el cuadro azul derecho es el productor de servicios que proporciona NetApp. Ambos se conectan mediante la agrupación de VPC.

Modelo de tenancy

En Cloud Volumes Service, los proyectos individuales se consideran inquilinos únicos. Esto significa que la manipulación de volúmenes, copias Snapshot, etc. se realiza por proyecto. En otras palabras, todos los volúmenes son propiedad del proyecto en el que se crearon y solo ese proyecto puede gestionar y acceder a los datos de su interior de forma predeterminada. Se considera la vista del plano de control del servicio.

VPC compartidos

En la vista del plano de datos, Cloud Volumes Service puede conectarse a un VPC compartido. Se pueden crear volúmenes en el proyecto de host o en uno de los proyectos de servicio conectados al VPC compartido. Todos los proyectos (host o servicio) conectados al VPC compartido pueden llegar a los volúmenes de la capa de red (TCP/IP). Debido a que todos los clientes con conectividad de red en el VPC compartido pueden acceder potencialmente a los datos mediante los protocolos NAS, se debe utilizar el control de acceso en el volumen individual (como las listas de control de acceso de usuarios/grupos (ACL) y los nombres de host/direcciones IP para las exportaciones de NFS para controlar quién puede acceder a los datos.

Puede conectar Cloud Volumes Service hasta a cinco VPC por proyecto de cliente. En el plano de control, el proyecto le permite gestionar todos los volúmenes creados, independientemente del VPC al que estén conectados. En el plano de datos, las PC están aisladas entre sí y cada volumen solo se puede conectar a un VPC.

El acceso a los volúmenes individuales está controlado por mecanismos de control de acceso específicos de los protocolos (NFS/SMB).

En otras palabras, en la capa de red, todos los proyectos conectados al VPC compartido pueden ver el volumen, mientras que, por el lado de la gestión, el plano de control solo permite que el proyecto del

propietario vea el volumen.

Controles de servicio VPC

Los controles de servicio VPC establecen un perímetro de control de acceso alrededor de los servicios de Google Cloud que están conectados a Internet y son accesibles en todo el mundo. Estos servicios proporcionan control de acceso a través de identidades de usuario, pero no pueden restringir desde qué solicitudes de ubicación de red se originan. Los controles de servicio VPC cierran esa brecha introduciendo las funcionalidades para restringir el acceso a las redes definidas.

El plano de datos Cloud Volumes Service no está conectado a Internet externo sino a ordenadores virtuales privados con límites de red bien definidos (perímetros). Dentro de esa red, cada volumen utiliza un control de acceso específico del protocolo. Los administradores de proyectos de Google Cloud crean explícitamente cualquier conectividad de red externa. Sin embargo, el plano de control no proporciona las mismas protecciones que el plano de datos y puede ser accesible por cualquier persona desde cualquier lugar con credenciales válidas ("Fichas JWT").

En resumen, el plano de datos Cloud Volumes Service proporciona la funcionalidad de control de acceso a la red, sin el requisito de admitir controles de servicio VPC y no utiliza de forma explícita los controles de servicio VPC.

Consideraciones sobre rastreo y rastreo de paquetes

Las capturas de paquetes pueden ser útiles para solucionar problemas de red u otros problemas (como permisos NAS, conectividad LDAP, etc.), pero también se pueden usar de forma malintencionada para obtener información sobre direcciones IP de red, direcciones MAC, nombres de usuarios y grupos, y sobre qué nivel de seguridad se está utilizando en los extremos. Debido a la forma en que se configuran las reglas de red, VPC y firewall de Google Cloud, el acceso no deseado a los paquetes de red debería ser difícil de obtener sin credenciales de inicio de sesión del usuario o "Fichas JWT" a las instancias de cloud. Las capturas de paquetes solo son posibles en extremos (como máquinas virtuales (VM)) y solo en extremos internos en el VPC, a menos que se utilice un VPC compartido o un reenvío de túnel/IP de red externo para permitir de forma explícita el tráfico externo a los extremos. No hay forma de sniff el tráfico fuera de los clientes.

Cuando se utilizan VPC compartidos, cifrado en tránsito con NFS Kerberos y/o. "Cifrado SMB" puede enmascarar gran parte de la información obtenida de las trazas. Sin embargo, cierto tráfico se sigue enviando en texto sin texto, como "DNS" y.. "Consultas LDAP". En la siguiente figura se muestra una captura de paquetes de una consulta LDAP de texto sin formato originada en Cloud Volumes Service y la información de identificación potencial que se expone. Las consultas LDAP en Cloud Volumes Service actualmente no admiten cifrado ni LDAP sobre SSL. CVS-Performance admite la firma LDAP, si es solicitada por Active Directory. CVS-SW no admite la firma LDAP.

IP addresses of the LDAP server and CVS instance

LDAP base DN and search type, search result

No.	Time	Source	Destination	Protocol	Length	Info
2320…	366.244071	10.194.0.6	10.10.0.11	LDAP	225	searchRequest(2) "DC=cvsdemo,DC=local" wholeSubtree
2320…	366.244381	10.10.0.11	10.194.0.6	LDAP	330	searchResRef(2) | searchResRef(2) | searchResRef(2) | searchResDone(2) success [0 results]

```
searchRequest
    baseObject: DC=cvsdemo,DC=local
    scope: wholeSubtree (2)
    derefAliases: neverDerefAliases (0)
    sizeLimit: 0
    timeLimit: 3
    typesOnly: False
    Filter: (&(objectClass=User)(uidNumber=1025))
      filter: and (0)
        and: (&(objectClass=User)(uidNumber=1025))
          and: 2 items
            Filter: (objectClass=User)
              and item: equalityMatch (3)
                equalityMatch
                    attributeDesc: objectClass
                    assertionValue: User
            Filter: (uidNumber=1025)
              and item: equalityMatch (3)
                equalityMatch
                    attributeDesc: uidNumber
                    assertionValue: 1025
    attributes: 7 items
        AttributeDescription: uid
        AttributeDescription: uidNumber
        AttributeDescription: gidNumber
        AttributeDescription: unixUserPassword
        AttributeDescription: name
        AttributeDescription: unixHomeDirectory
        AttributeDescription: loginShell
```

Filters used in the query
- Usernames
- Numeric IDs
- Group names
- Group IDs

Attributes queried

UnixUserPassword es consultada por LDAP y no se envía en texto sin formato sino en un hash salado. De forma predeterminada, LDAP de Windows no rellena los campos unixUserPassword. Este campo sólo es necesario si necesita aprovechar LDAP de Windows para inicios de sesión interactivos a través de LDAP a clientes. Cloud Volumes Service no admite inicios de sesión LDAP interactivos en las instancias.

En la siguiente figura se muestra una captura de paquetes desde una conversación Kerberos de NFS junto a una captura de NFS sobre AUTH_SYS. Tenga en cuenta que la información disponible en una traza difiere entre ambas y cómo habilitar el cifrado en tránsito ofrece una mayor seguridad general para el tráfico NAS.

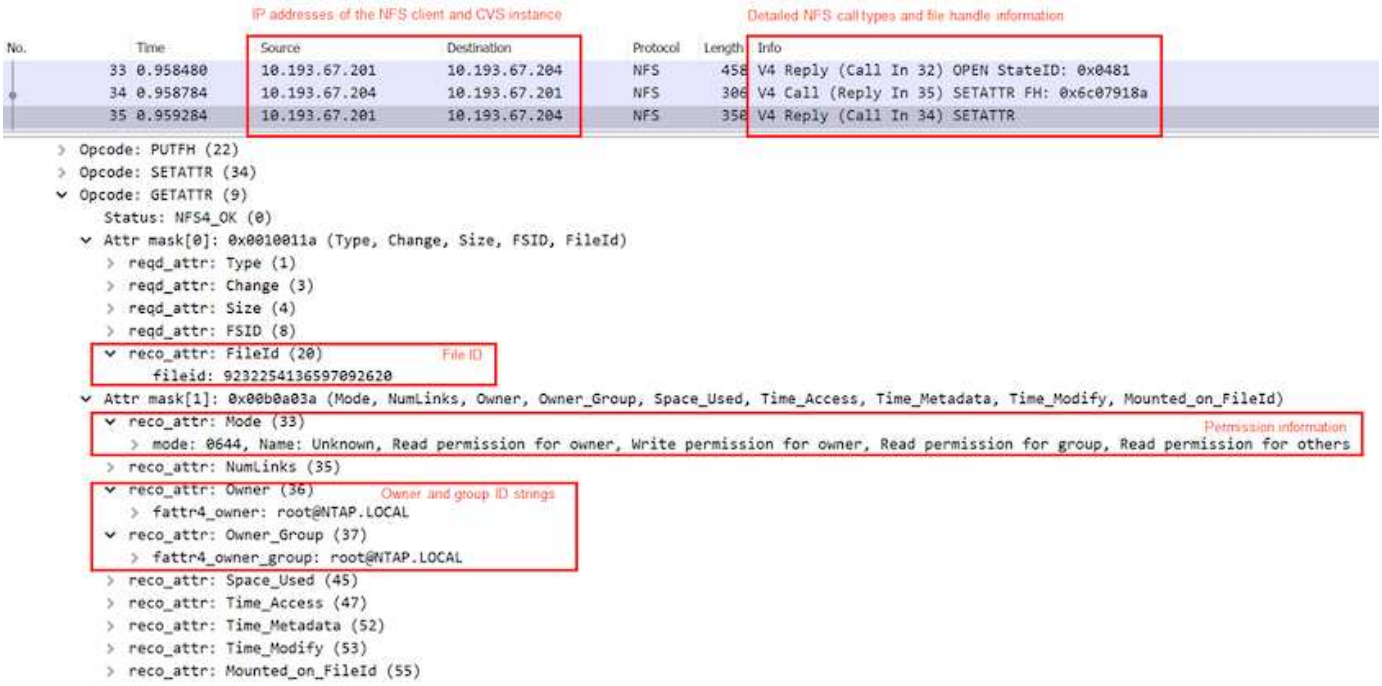
IP addresses of the NFS client and CVS instance

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
v GSS-Wrap
    Length: 300
    GSS Data: 050407ff0000000000000000025913451ee1d43d298cf3031…
  > krb5_blob: 050407ff0000000000000000025913451ee1d43d298cf3031…
v Network File System
    [Program Version: 4]
    [V4 Procedure: COMPOUND (1)]
```

GSS wrapped NFS calls/replies with no other identifying information



Interfaces de red de equipos virtuales

Un truco que los atacantes podrían intentar es agregar una nueva tarjeta de interfaz de red (NIC) a una VM en "modo promiscuo" (Duplicación de puertos) o habilite el modo promiscuo en una NIC existente para sniff todo el tráfico. En Google Cloud, agregar una nueva NIC requiere que una máquina virtual se cierre por completo, lo que crea alertas, por lo que los atacantes no pueden pasar por alto.

Además, las NIC no se pueden establecer en modo promiscuo y activarán alertas en Google Cloud.

Arquitectura del plano de control

Todas las acciones de gestión a Cloud Volumes Service se realizan mediante API. La gestión de Cloud Volumes Service integrada en la consola cloud de GCP también utiliza la API de Cloud Volumes Service.

Gestión de acceso e identidad

Gestión de acceso e identidad ("IAM") Es un servicio estándar que le permite controlar la autenticación (inicios de sesión) y la autorización (permisos) a las instancias de proyecto de Google Cloud. Google IAM proporciona un registro de auditoría completo de la autorización y eliminación de permisos. Actualmente, Cloud Volumes Service no proporciona auditoría del plano de control.

Información general sobre autorización/permisos

IAM ofrece permisos granulares integrados para Cloud Volumes Service. Puede encontrar un "complete aquí la lista de permisos granulares".

IAM también ofrece dos roles predefinidos llamados `netappcloudvolumes.admin` y.. `netappcloudvolumes.viewer`. Estos roles pueden asignarse a usuarios o cuentas de servicio específicos.

Asigne roles y permisos adecuados para permitir que los usuarios de IAM gestionen Cloud Volumes Service.

Algunos ejemplos para el uso de permisos granulares son los siguientes:

- Cree una función personalizada con sólo permisos get/list/create/update para que los usuarios no puedan eliminar volúmenes.
- Use un rol personalizado con solo `snapshot.*` Permisos para crear una cuenta de servicio que se utilice para crear una integración de Snapshot coherente con las aplicaciones.
- Cree un rol personalizado para delegar `volumereplication.*` para usuarios específicos.

Cuentas de servicio

Para realizar llamadas a la API de Cloud Volumes Service a través de scripts o. "Terraform", debe crear una cuenta de servicio con `roles/netappcloudvolumes.admin` función. Puede utilizar esta cuenta de servicio para generar los tokens JWT necesarios para autenticar las solicitudes de API de Cloud Volumes Service de dos maneras diferentes:

- Genere una clave JSON y utilice las API de Google para obtener un token de JWT de él. Este es el método más sencillo, pero implica la gestión de secretos manuales (la clave JSON).
- Uso "Suplantación de cuentas de servicio" con `roles/iam.serviceAccountTokenCreator`. El código (script, Terraform, etc.) se ejecuta con "Credenciales predeterminadas de la aplicación" e representa a la cuenta de servicio para obtener sus permisos. Este enfoque refleja las mejores prácticas de seguridad de Google.

Consulte "Creación de la cuenta de servicio y la clave privada" Para obtener más información, consulte la documentación de cloud de Google.

API de Cloud Volumes Service

La API de Cloud Volumes Service utiliza una API basada en REST usando HTTPS (TLSv1.2) como transporte de red subyacente. Puede encontrar la definición de API más reciente "aquí" E información acerca de cómo utilizar la API en "API de Cloud Volumes en la documentación de Google Cloud".

NetApp utiliza y protege el extremo de la API mediante la funcionalidad estándar HTTPS (TLSv1.2).

Fichas JWT

La autenticación a la API se realiza con tokens JWT portadores ("RFC-7519"). Se deben obtener tokens JWT válidos mediante la autenticación de Google Cloud IAM. Para ello, debe obtener un token del IAM mediante la obtención de una clave JSON de la cuenta de servicio.

Registro de auditoría

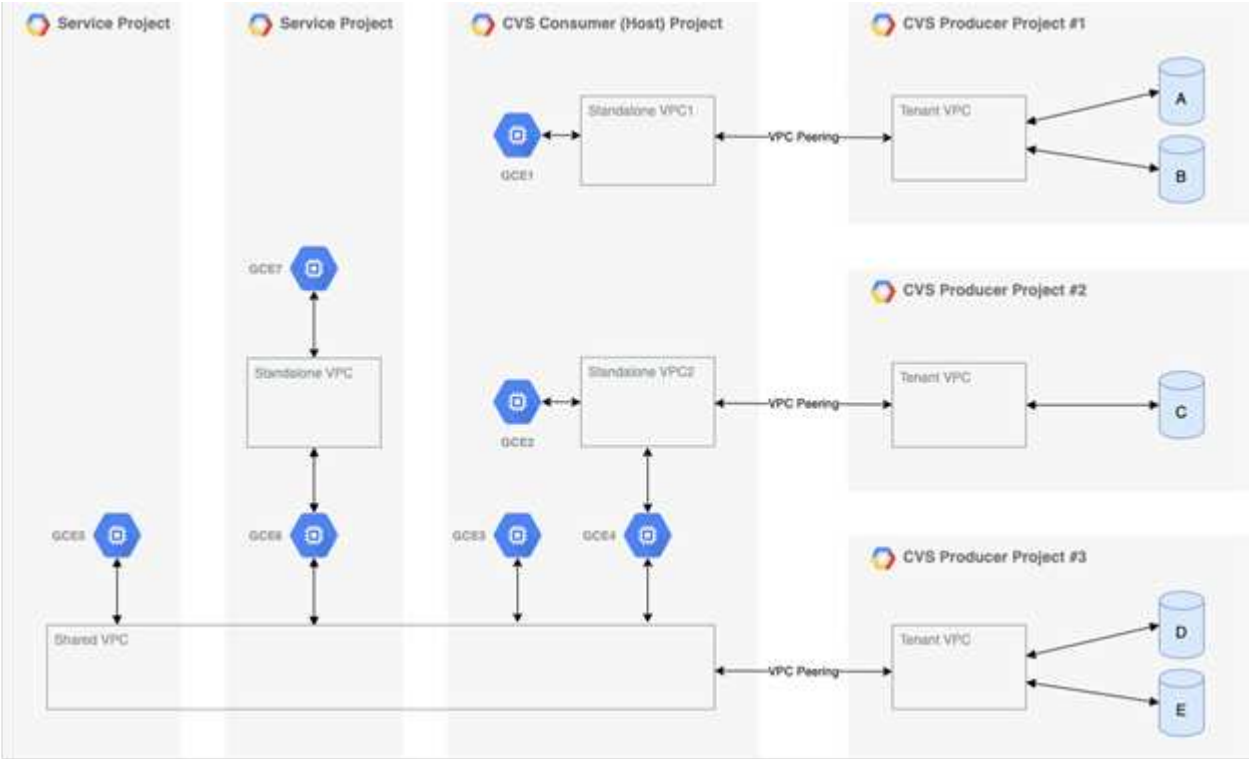
Actualmente, no hay registros de auditoría del plano de control a los que el usuario pueda acceder.

Arquitectura de plano de datos

Cloud Volumes Service para Google Cloud aprovecha Google Cloud "acceso a servicios privados" marco. En este marco, los usuarios pueden conectarse a Cloud Volumes Service. Este marco usa construcciones de paridad de Service Networking y VPC, al igual que otros servicios de Google Cloud, para garantizar un aislamiento completo entre clientes.

Para obtener información general sobre la arquitectura de Cloud Volumes Service para Google Cloud, consulte "Para Cloud Volumes Service".

Las VPC de usuario (independientes o compartidas) tienen una relación entre sí y las VPC dentro de los proyectos de arrendatarios administrados de Cloud Volumes Service, que alojan los volúmenes.



La figura anterior muestra un proyecto (el proyecto para consumidores CVS en el medio) con tres redes VPC conectadas a Cloud Volumes Service y a varios equipos virtuales de Compute Engine (GCE1-7) compartiendo volúmenes:

- VPC1 permite a GCE1 acceder a los volúmenes A y B.
- VPC2 permite a GCE2 y GCE4 acceder al volumen C.
- La tercera red VPC es un VPC compartido, compartido con dos proyectos de servicio. Permite a GCE3, GCE4, GCE5 y GCE6 acceder a los volúmenes D y E. Las redes VPC compartidas solo se admiten para volúmenes del tipo de servicio CVS-Performance.

GCE7 no puede acceder a ningún volumen.

Los datos se pueden cifrar tanto en tránsito (mediante Kerberos y/o cifrado SMB) como en reposo en Cloud Volumes Service.

Cifrado de datos en tránsito

Los datos en tránsito pueden cifrarse en la capa de protocolo NAS, y la propia red de Google Cloud está cifrada, tal y como se describe en las siguientes secciones.

Red de Google Cloud

Google Cloud cifra el tráfico en el nivel de la red, tal y como se describe en "Cifrado en tránsito" En la documentación de Google. Como se mencionó en la sección "Arquitectura de Cloud Volumes Services", Cloud Volumes Service se ofrece desde un proyecto de productor de PSA controlado por NetApp.

En caso de CVS-SW, el inquilino productor ejecuta las VM de Google para ofrecer el servicio. Google cifra automáticamente el tráfico entre los equipos virtuales del usuario y los equipos virtuales de Cloud Volumes Service.

Aunque la ruta de datos para CVS-Performance no está completamente cifrada en la capa de red, NetApp y Google usan una combinación de ambos "De cifrado IEEE 802.1AE (MACSec)", "encapsulación" (Cifrado de datos) y redes con limitaciones físicas para proteger los datos en tránsito entre el tipo de servicio CVS-Performance de Cloud Volumes Service y Google Cloud.

Protocolos NAS

Los protocolos NFS y SMB NAS proporcionan un cifrado de transporte opcional en la capa del protocolo.

Cifrado SMB

"Cifrado SMB" Proporciona cifrado integral de datos SMB y protege los datos de espionaje en redes que no son de confianza. Puede habilitar el cifrado tanto para la conexión de datos de cliente/servidor (solo disponible para clientes compatibles con SMB3.x) como para la autenticación de la controladora de servidor/dominio.

Cuando el cifrado SMB está habilitado, los clientes que no admiten el cifrado no pueden acceder al recurso compartido.

Cloud Volumes Service admite cifrados de seguridad RC4-HMAC, AES-128-CTS-HMAC-SHA1 y AES-256-CTS-HMAC-SHA1 para el cifrado SMB. SMB negocia con el tipo de cifrado más alto admitido por el servidor.

NFSv4.1 Kerberos

Para NFSv4.1, CVS-Performance ofrece autenticación de Kerberos, tal como se describe en "RFC7530". Puede activar Kerberos por volumen.

El tipo de cifrado disponible más actual para Kerberos es AES-256-CTS-HMAC-SHA1. Cloud Volumes Service de NetApp es compatible con AES-256-CTS-HMAC-SHA1, AES-128-CTS-HMAC-SHA1, DES3 y DES para NFS. También admite ARCFOUR-HMAC (RC4) para el tráfico CIFS/SMB, pero no para NFS.

Kerberos proporciona tres niveles de seguridad distintos para montajes NFS que ofrecen opciones para la solidez de la seguridad de Kerberos.

Según RedHat’s "Opciones de montaje comunes" documentación:

```
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.
```

Como regla general, cuanto mayor sea el nivel de seguridad de Kerberos, peor será el rendimiento, puesto que el cliente y el servidor pasan tiempo cifrando y descifrando las operaciones de NFS para cada paquete enviado. Muchos clientes y servidores NFS ofrecen soporte para la descarga de AES-ni a las CPU para una mejor experiencia general, pero el impacto en el rendimiento de Kerberos 5p (cifrado completo integral) es significativamente mayor que el impacto de Kerberos 5 (autenticación de usuario).

En la siguiente tabla se muestran las diferencias en el rendimiento y la seguridad de cada nivel.

Nivel de seguridad	Seguridad	Rendimiento
NFSv3: System	• Menos seguro; texto sin formato con ID de usuario/ID de grupo numéricos • Capaz de ver UID, GID, direcciones IP de cliente, rutas de exportación, nombres de archivos, permisos en capturas de paquetes	• Lo mejor para la mayoría de los casos
NFSv4.x: Sys	• Más seguro que NFSv3 (identificadores de cliente, coincidencia de cadena de nombre/cadena de dominio) pero texto sin formato • Se puede ver UID, GID, direcciones IP de cliente, cadenas de nombre, identificadores de dominio, rutas de exportación, nombres de archivo y permisos en capturas de paquetes	• Bueno para cargas de trabajo secuenciales (como equipos virtuales, bases de datos, archivos de gran tamaño) • Malo con un número elevado de archivos/metadatos altos (un 30-50% peor)

Nivel de seguridad	Seguridad	Rendimiento
NFS: Krb5	• El cifrado Kerberos para credenciales en cada paquete NFS envuelve UID/GID de usuarios/grupos en llamadas RPC en el contenedor GSS • El usuario que solicita el acceso al montaje necesita un ticket Kerberos válido (ya sea mediante el nombre de usuario/contraseña o el cambio de tabulación manual); el ticket caduca después de un período de tiempo especificado y el usuario debe volver a autenticarse para el acceso • No existe cifrado para operaciones de NFS ni para protocolos auxiliares como Mount/portmapper/nlm (puede ver rutas de exportación, direcciones IP, identificadores de archivos, permisos, nombres de archivos, atime/mtime en capturas de paquetes)	• Mejor en la mayoría de los casos para Kerberos; peor que AUTH_SYS

Nivel de seguridad	Seguridad	Rendimiento
NFS: Krb5i	• El cifrado Kerberos para credenciales en cada paquete NFS envuelve UID/GID de usuarios/grupos en llamadas RPC en el contenedor GSS • El usuario que solicita el acceso al montaje necesita un ticket Kerberos válido (ya sea mediante el nombre de usuario/contraseña o el cambio de tabulación manual); el ticket caduca después de un período de tiempo especificado y el usuario debe volver a autenticarse para el acceso • No existe cifrado para operaciones de NFS ni para protocolos auxiliares como Mount/portmapper/nlm (puede ver rutas de exportación, direcciones IP, identificadores de archivos, permisos, nombres de archivos, atime/mtime en capturas de paquetes) • La suma de comprobación de Kerberos GSS se agrega a cada paquete para garantizar que nada intercepta los paquetes. Si coinciden sumas de comprobación, se permite la conversación.	• Mejor que krb5p porque la carga útil NFS no está cifrada; solo la sobrecarga añadida en comparación con krb5 es la suma de comprobación de integridad. El rendimiento del krb5i no será mucho peor que el krb5, pero sí que se verá algo de degradación.

Nivel de seguridad	Seguridad	Rendimiento
NFS: Krb5p	• El cifrado Kerberos para credenciales en cada paquete NFS envuelve UID/GID de usuarios/grupos en llamadas RPC en el contenedor GSS • El usuario que solicita acceso al montaje necesita un ticket Kerberos válido (ya sea mediante nombre de usuario/contraseña o cambio manual de keytab); el ticket caduca después del período de tiempo especificado y el usuario debe volver a autenticarse para acceder • Todas las cargas de paquetes NFS se cifran con el contenedor GSS (no se pueden ver los identificadores de archivos, permisos, nombres de archivos, atime/mtime en capturas de paquetes). • Incluye comprobación de integridad. • El tipo de operación NFS es visible (FSINFO, ACCESS, GETATTR, etc.). • Los protocolos auxiliares (Mount, portmap, nlm, etc.) no están cifrados (puede ver rutas de exportación, direcciones IP)	• El peor rendimiento de los niveles de seguridad; krb5p debe cifrar/descifrar más. • Mejor rendimiento que krb5p con NFSv4.x para cargas de trabajo con un gran número de archivos.

En Cloud Volumes Service, un servidor de Active Directory configurado se utiliza como servidor Kerberos y servidor LDAP (para buscar identidades de usuario desde un esquema compatible con RFC2307). No se admiten otros servidores Kerberos o LDAP. NetApp recomienda encarecidamente utilizar LDAP para la gestión de identidades en Cloud Volumes Service. Para obtener más información acerca de cómo se muestra NFS Kerberos en capturas de paquetes, consulte la sección "“Consideraciones sobre rastreo y rastreo de paquetes”."

Cifrado de datos en reposo

Todos los volúmenes de Cloud Volumes Service se cifran en reposo mediante el cifrado AES-256, lo que significa que todos los datos de usuario escritos en medios se cifran y solo se pueden descifrar con una clave por volumen.

- Para CVS-SW, se usan claves generadas por Google.
- Para CVS-Performance, las claves por volumen se almacenan en un gestor de claves incorporado en

Cloud Volumes Service.

A partir de noviembre de 2021, ya estaba disponible la funcionalidad de obtener una vista previa de las claves de cifrado gestionadas por el cliente (CMEK). Esto permite cifrar las claves por volumen con una clave maestra por proyecto y por región alojada en "Servicio de administración de claves (KMS) de Google." KMS le permite asociar gestores de claves externos.

Para obtener información acerca de la configuración de KMS para CVS-Performance, consulte "Configurar las claves de cifrado gestionadas por el cliente".

Servidor de seguridad

Cloud Volumes Service expone varios puertos TCP para que sirvan a los recursos compartidos NFS y SMB:

- "Puertos necesarios para el acceso NFS"
- "Puertos necesarios para el acceso a SMB"

Además, SMB, NFS con LDAP incluido Kerberos y configuraciones de protocolo dual requieren acceso a un dominio de Windows Active Directory. Deben estar las conexiones de Active Directory "configurado" por región. Los controladores de dominio de Active Directory (DC) se identifican mediante el uso "Descubrimiento de DC basado en DNS" Utilizando los servidores DNS especificados. Se utiliza cualquiera de los DC devueltos. La lista de centros de datos elegibles se puede limitar especificando un sitio de Active Directory.

Cloud Volumes Service se dirige a través de direcciones IP del rango CIDR asignado con el `gcloud compute address` command mientras "Integración de Cloud Volumes Service". Puede utilizar este CIDR como direcciones de origen para configurar firewalls entrantes en los controladores de dominio de Active Directory.

Los controladores de dominio de Active Directory deben "Exponer los puertos a los CIDR de Cloud Volumes Service como se menciona aquí".

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.