있습니다
NetApp Solutions

NetApp
April 20, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/netapp-solutions/ehc/ncvs-gc-architecture_overview.html on April 20, 2024. Always check docs.netapp.com for the latest.

목차

있습니다 1
개요 1
Cloud Volumes Service 아키텍처 1
컨트롤 플레인 아키텍처 5
데이터 플레인 아키텍처 6
전송 중인 데이터 암호화 7
유휴 데이터 암호화 10
방화벽 11

있습니다

개요

클라우드 솔루션을 신뢰하는 것은 아키텍처와 보안 방식을 이해하는 것입니다. 이 섹션에서는 Google의 Cloud Volumes Service 아키텍처의 다양한 측면을 다루어 데이터 보안 방식에 대한 잠재적 우려를 완화하고 가장 안전한 배포를 위해 추가 구성 단계가 필요할 수 있는 영역을 설명합니다.

Cloud Volumes Service의 일반 아키텍처는 컨트롤 플레인과 데이터 플레인의 두 가지 주요 구성 요소로 나눌 수 있습니다.

컨트롤 플레인

Cloud Volumes Service의 제어 플레인은 Cloud Volumes Service 관리자와 NetApp 기본 자동화 소프트웨어가 관리하는 백엔드 인프라입니다. 이 방식은 최종 사용자에게 전혀 영향을 미치지 않으며 네트워킹, 스토리지 하드웨어, 소프트웨어 업데이트 등을 포함하여 Cloud Volumes Service와 같은 클라우드 상주 솔루션에 가치를 제공하는 데 도움을 줍니다.

데이터 플레인

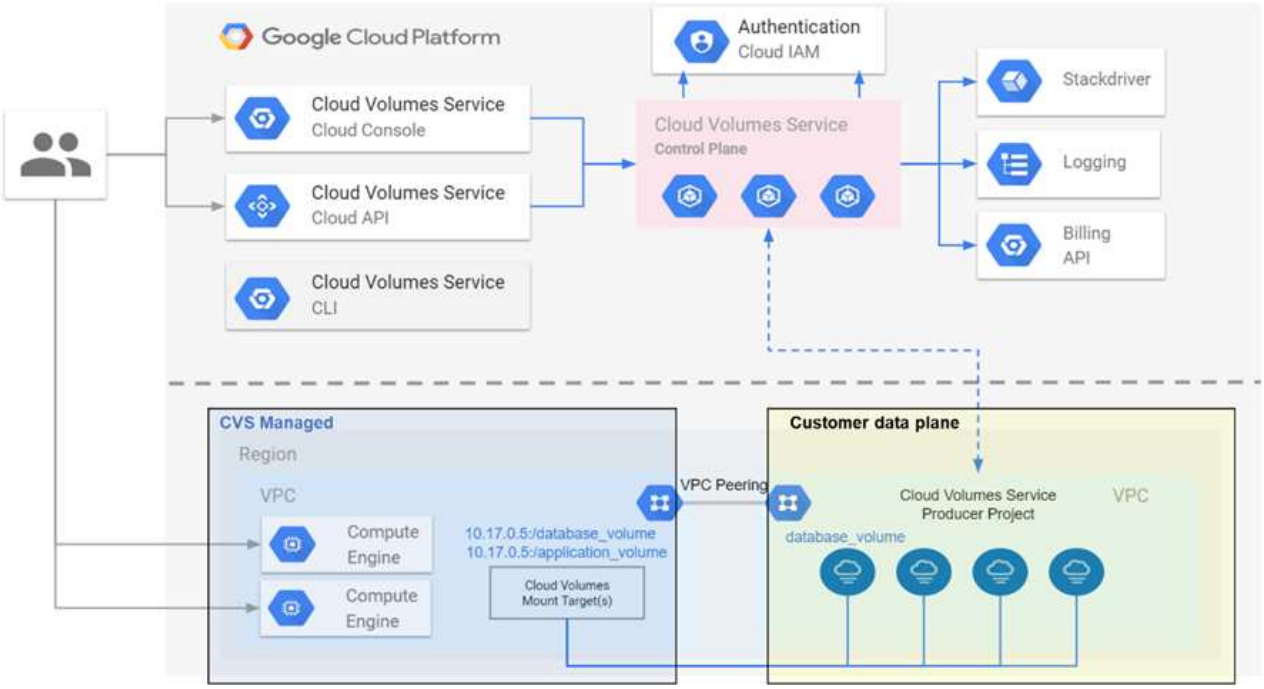
Cloud Volumes Service의 데이터 계층에는 실제 데이터 볼륨과 전체 Cloud Volumes Service 구성(액세스 제어, Kerberos 인증 등)이 포함됩니다. 데이터 플레인은 전적으로 최종 사용자와 Cloud Volumes Service 플랫폼 소비자를 제어하는 것입니다.

각 평면의 보안 및 관리 방법은 서로 다릅니다. 다음 섹션에서는 Cloud Volumes Service 아키텍처 개요부터 이러한 차이점에 대해 설명합니다.

Cloud Volumes Service 아키텍처

CloudSQL, GCVE(Google Cloud VMware Engine) 및 파일 저장소와 같은 다른 Google Cloud 네이티브 서비스와 유사한 방식으로 Cloud Volumes Service는 을 사용합니다 "Google PSA" 서비스를 제공합니다. PSA에서는 서비스를 사용하는 서비스 프로듀서 프로젝트에 내장하고 있습니다 "VPC 네트워크 피어링" 서비스 소비자에 연결합니다. 서비스 생산자는 NetApp에서 제공 및 운영하고, 서비스 소비자는 고객 프로젝트에서 VPC로, Cloud Volumes Service 파일 공유에 액세스하려는 클라이언트를 호스팅합니다.

에서 참조하는 다음 그림 "아키텍처 섹션을 참조하십시오" 에서는 Cloud Volumes Service 설명서의 개략적인 보기를 보여 줍니다.



점선 위의 파트는 볼륨 수명 주기를 제어하는 서비스의 컨트롤 평면을 보여줍니다. 점선 아래의 부분은 데이터 평면을 나타냅니다. 왼쪽 파란색 상자는 사용자 VPC(서비스 소비자)를 나타내고 오른쪽 파란색 상자는 NetApp에서 제공하는 서비스 생산업체입니다. 둘 다 VPC 피어링을 통해 연결됩니다.

테넌시 모델

Cloud Volumes Service에서 개별 프로젝트는 고유한 테넌트로 간주됩니다. 즉, 볼륨, 스냅샷 복사본 등을 프로젝트 단위로 조작할 수 있습니다. 즉, 모든 볼륨은 자신이 만든 프로젝트의 소유이며 해당 프로젝트에서만 기본적으로 해당 볼륨 내의 데이터를 관리하고 액세스할 수 있습니다. 이는 서비스의 컨트롤 플레인 뷰로 간주됩니다.

공유 **VPC**

데이터 평면 보기에서 Cloud Volumes Service는 공유 VPC에 연결할 수 있습니다. 호스팅 프로젝트 또는 공유 VPC에 연결된 서비스 프로젝트 중 하나에서 볼륨을 생성할 수 있습니다. 공유 VPC에 연결된 모든 프로젝트(호스트 또는 서비스)는 네트워크 계층(TCP/IP)에서 볼륨에 연결할 수 있습니다. 공유 VPC에서 네트워크 연결을 사용하는 모든 클라이언트는 NAS 프로토콜을 통해 데이터에 액세스할 수 있으므로 개별 볼륨의 액세스 제어(예: 사용자/그룹 ACL(액세스 제어 목록) 및 NFS 내보내기의 호스트 이름/IP 주소)를 사용하여 데이터에 액세스할 수 있는 사용자를 제어해야 합니다.

고객 프로젝트당 최대 5대의 VPC에 Cloud Volumes Service를 연결할 수 있습니다. 제어 플레인에서 프로젝트를 사용하면 연결된 VPC에 관계없이 생성된 모든 볼륨을 관리할 수 있습니다. 데이터 플레인에서 VPC는 서로 격리되며 각 볼륨은 하나의 VPC에만 연결할 수 있습니다.

개별 볼륨에 대한 액세스는 프로토콜별(NFS/SMB) 액세스 제어 메커니즘에 의해 제어됩니다.

즉, 네트워크 계층에서 공유 VPC에 연결된 모든 프로젝트가 볼륨을 볼 수 있는 반면 관리 측면에서는 소유자 프로젝트만 볼륨을 볼 수 있습니다.

VPC 서비스 제어

VPC 서비스 제어는 인터넷에 연결되어 있고 전 세계적으로 액세스할 수 있는 Google Cloud 서비스에 대한 액세스 제어 경계를 설정합니다. 이러한 서비스는 사용자 ID를 통해 액세스 제어를 제공하지만 어떤 네트워크 위치 요청이 시작되기까지의 지 제한할 수 없습니다. VPC 서비스는 정의된 네트워크에 대한 액세스를 제한하는 기능을 도입하여 이러한 격차를 해소합니다.

Cloud Volumes Service 데이터 플레인은 외부 인터넷에 연결되지 않고 잘 정의된 네트워크 경계(경계)가 있는 전용 VPC에 연결됩니다. 해당 네트워크 내에서 각 볼륨은 프로토콜별 액세스 제어를 사용합니다. 외부 네트워크 연결은 Google Cloud 프로젝트 관리자가 명시적으로 만듭니다. 그러나 컨트롤 플레인은 데이터 플레인과 동일한 보호 기능을 제공하지 않으며 모든 곳에서 유효한 자격 증명( )을 사용하여 액세스할 수 있습니다 "JWT 토큰")를 클릭합니다.

즉, Cloud Volumes Service 데이터 플레인은 VPC 서비스 제어를 지원할 필요 없이 VPC 서비스 제어를 명시적으로 사용하지 않고 네트워크 액세스 제어 기능을 제공합니다.

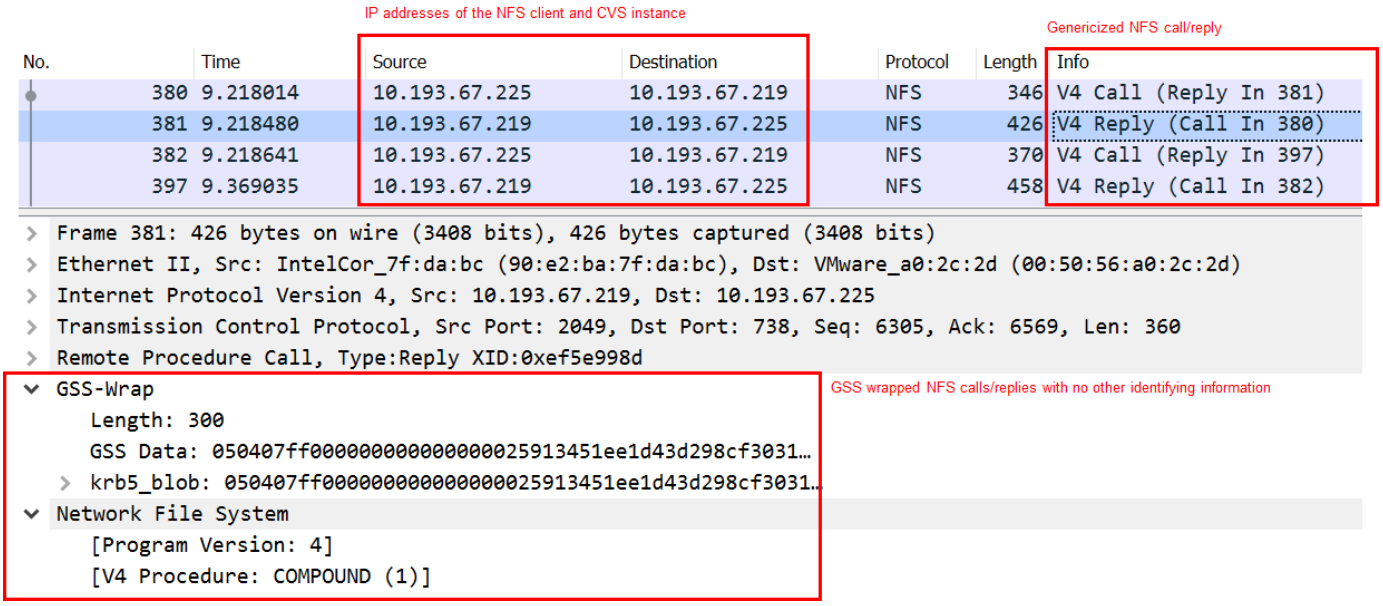
패킷 스니핑/추적 고려 사항

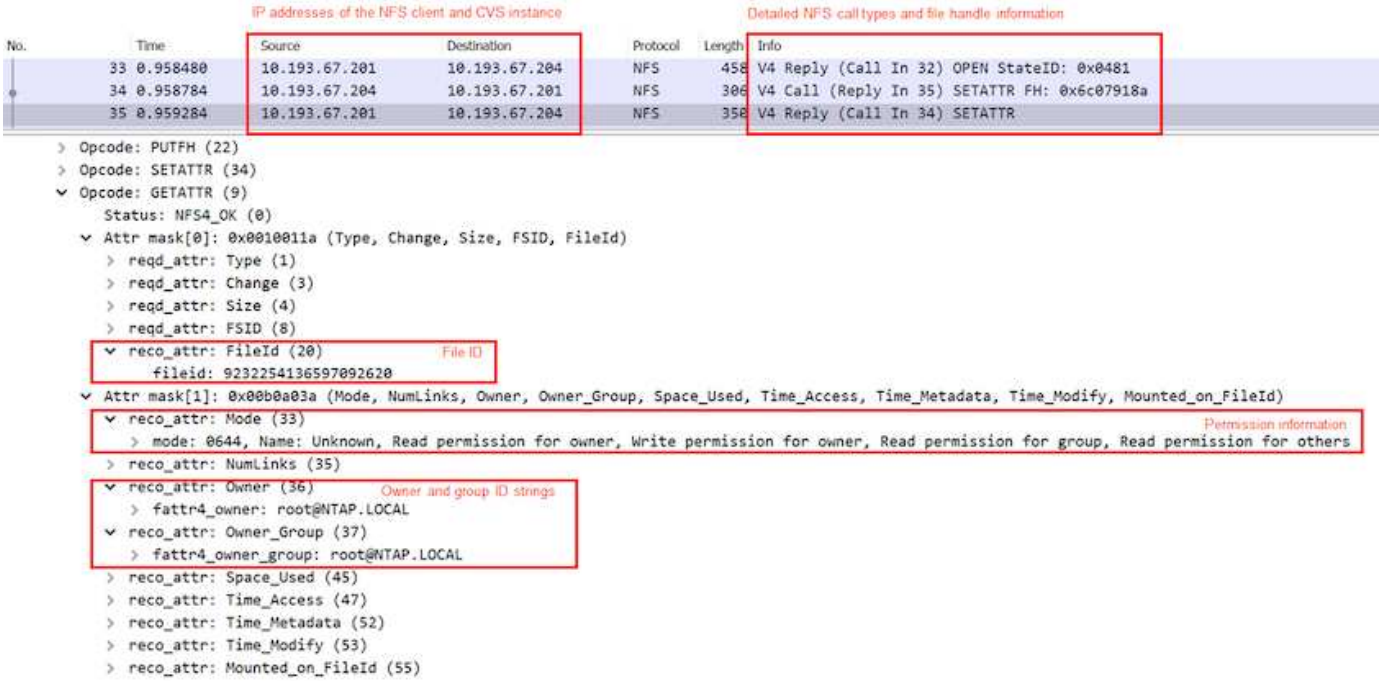
패킷 캡처는 네트워크 문제 또는 기타 문제(예: NAS 권한, LDAP 연결 등)를 해결하는 데 유용할 수 있지만 네트워크 IP 주소, MAC 주소, 사용자 및 그룹 이름 및 엔드포인트에서 사용되는 보안 수준에 대한 정보를 얻기 위해 악의적으로 사용할 수도 있습니다. Google Cloud 네트워킹, VPC 및 방화벽 규칙이 구성된 방식 때문에 사용자 로그인 자격 증명 또는 없이 네트워크 패킷에 대한 원치 않는 액세스를 얻기가 어렵습니다 "JWT 토큰" 클라우드로 인스턴스. 공유 VPC 및/또는 외부 네트워크 터널/IP 전달을 사용하여 엔드포인트에 대한 외부 트래픽을 명시적으로 허용하지 않는 한 패킷 캡처는 엔드포인트(예: 가상 머신(VM))에서만 가능하며 VPC 내부 엔드포인트에서만 가능합니다. 클라이언트 외부의 트래픽을 스니핑할 수 있는 방법은 없습니다.

공유 VPC를 사용하는 경우 NFS Kerberos 및/또는 를 사용하여 전송 중 암호화 "SMB 암호화" 트레이스에서 얻은 정보의 대부분을 가릴 수 있습니다. 그러나 일부 트래픽은 과 같은 일반 텍스트로 계속 전송됩니다 "DNS" 및 "LDAP 쿼리입니다". 다음 그림에서는 Cloud Volumes Service에서 생성된 일반 텍스트 LDAP 쿼리 및 노출된 잠재적 식별 정보의 패킷 캡처를 보여 줍니다. Cloud Volumes Service의 LDAP 쿼리는 현재 SSL을 통한 암호화 또는 LDAP를 지원하지 않습니다. Active Directory에서 요청하는 경우 CVS - 성능은 LDAP 서명을 지원합니다. CVS-SW는 LDAP 서명을 지원하지 않습니다.

unixUserPassword는 LDAP에 의해 쿼리되며 일반 텍스트로 전송되지 않고 소염 해시로 보내집니다. 기본적으로 Windows LDAP는 unixUserPassword 필드를 채우지 않습니다. 이 필드는 LDAP를 통해 클라이언트에 대화형 로그인을 위해 Windows LDAP를 활용해야 하는 경우에만 필요합니다. Cloud Volumes Service는 인스턴스에 대한 대화형 LDAP 로그인을 지원하지 않습니다.

다음 그림에서는 AUTH_SYS를 통한 NFS 캡처 옆에 있는 NFS Kerberos 대화의 패킷 캡처를 보여 줍니다. 추적에서 사용할 수 있는 정보가 두 가지 간에 어떻게 다른지, 그리고 전송 중 암호화를 사용하여 NAS 트래픽에 대한 전반적인 보안을 강화하는 방법을 확인하십시오.





VM 네트워크 인터페이스

공격자는 의 VM에 새 NIC(네트워크 인터페이스 카드)를 추가하려고 시도할 수 있습니다 "무차별 모드" 모든 트래픽을 스니핑하기 위해 기존 NIC에서 Promiscuous 모드를 활성화(포트 미러링)하거나 활성화합니다. Google Cloud에서 새 NIC를 추가하려면 VM을 완전히 종료해야 하므로 경고가 생성되므로 공격자가 이를 놓치지 않고 확인할 수 없습니다.

또한 NIC를 무차별 모드로 설정할 수 없으며 Google Cloud에서 경고를 트리거합니다.

컨트롤 플레인 아키텍처

Cloud Volumes Service에 대한 모든 관리 작업은 API를 통해 수행됩니다. GCP 클라우드 콘솔에 통합된 Cloud Volumes Service 관리도 Cloud Volumes Service API를 사용합니다.

ID 및 액세스 관리

ID 및 액세스 관리 ("IAM")는 Google Cloud 프로젝트 인스턴스에 대한 인증(로그인) 및 권한 부여(권한)를 제어할 수 있는 표준 서비스입니다. Google IAM은 권한 승인 및 제거에 대한 전체 감사 추적을 제공합니다. 현재 Cloud Volumes Service는 제어 평면 감사를 제공하지 않습니다.

인증/권한 개요

IAM은 Cloud Volumes Service에 대한 세분화된 기본 권한을 제공합니다. 를 찾을 수 있습니다 "여기에서 세분화된 사용 권한의 전체 목록을 확인할 수 있습니다".

IAM은 또한 netapcloudvolumes.admin과 netapcloudvolumes.viewer라는 두 가지 사전 정의된 역할을 제공합니다. 이러한 역할은 특정 사용자 또는 서비스 계정에 할당할 수 있습니다.

IAM 사용자가 Cloud Volumes Service를 관리할 수 있도록 적절한 역할 및 권한을 할당합니다.

세분화된 사용 권한을 사용하는 예는 다음과 같습니다.

- 사용자가 볼륨을 삭제할 수 없도록 get/list/create/update 권한만 가진 사용자 지정 역할을 만듭니다.
- '스냅샷 *' 권한으로만 사용자 지정 역할을 사용하여 애플리케이션 정합성 보장 스냅샷 통합을 구축하는 데 사용되는 서비스 계정을 생성합니다.
- 특정 사용자에게 '볼륨 증가 *'를 위임하는 사용자 지정 역할을 만듭니다.

서비스 계정

또는 스크립트를 통해 Cloud Volumes Service API 호출을 수행하는 방법 "Terraform(Terraform" 역할/netapcloudvolumes.admin의 역할을 사용하여 서비스 계정을 생성해야 합니다. 이 서비스 계정을 사용하여 Cloud Volumes Service API 요청을 인증하는 데 필요한 JWT 토큰을 다음 두 가지 방법으로 생성할 수 있습니다.

- JSON 키를 생성하고 Google API를 사용하여 JWT 토큰을 파생시킵니다. 이 방법이 가장 간단한 방법이지만 수동 비밀(JSON 키) 관리와 관련이 있습니다.
- 사용 "서비스 계정 가장" 역할/iam.serviceAccountTokenCreator` 포함. 이 코드(스크립트, Terraform 등)는 에서 실행됩니다 "애플리케이션 기본 자격 증명" 서비스 계정을 가장하여 권한을 얻습니다. 이 접근 방식은 Google 보안 모범 사례를 반영합니다.

을 참조하십시오 "서비스 계정 및 개인 키 생성" 자세한 내용은 Google 클라우드 설명서를 참조하십시오.

Cloud Volumes Service API를 참조하십시오

Cloud Volumes Service API는 HTTPS(TLSv1.2)를 기본 네트워크 전송으로 사용하여 REST 기반 API를 사용합니다. 최신 API 정의를 찾을 수 있습니다 "여기" 및 에서 API 사용 방법에 대한 정보를 참조하십시오 "Google Cloud 설명서에서 Cloud Volumes API를 참조하십시오".

API 엔드포인트는 표준 HTTPS(TLSv1.2) 기능을 사용하여 NetApp에서 작동 및 보안됩니다.

JWT 토큰

API에 대한 인증은 JWT 베어러 토큰을 사용하여 수행됩니다 ("RFC-7519")를 클릭합니다. Google Cloud IAM 인증을 사용하여 유효한 JWT 토큰을 얻어야 합니다. 서비스 계정 JSON 키를 제공하여 IAM에서 토큰을 가져와 수행해야 합니다.

로깅 감사

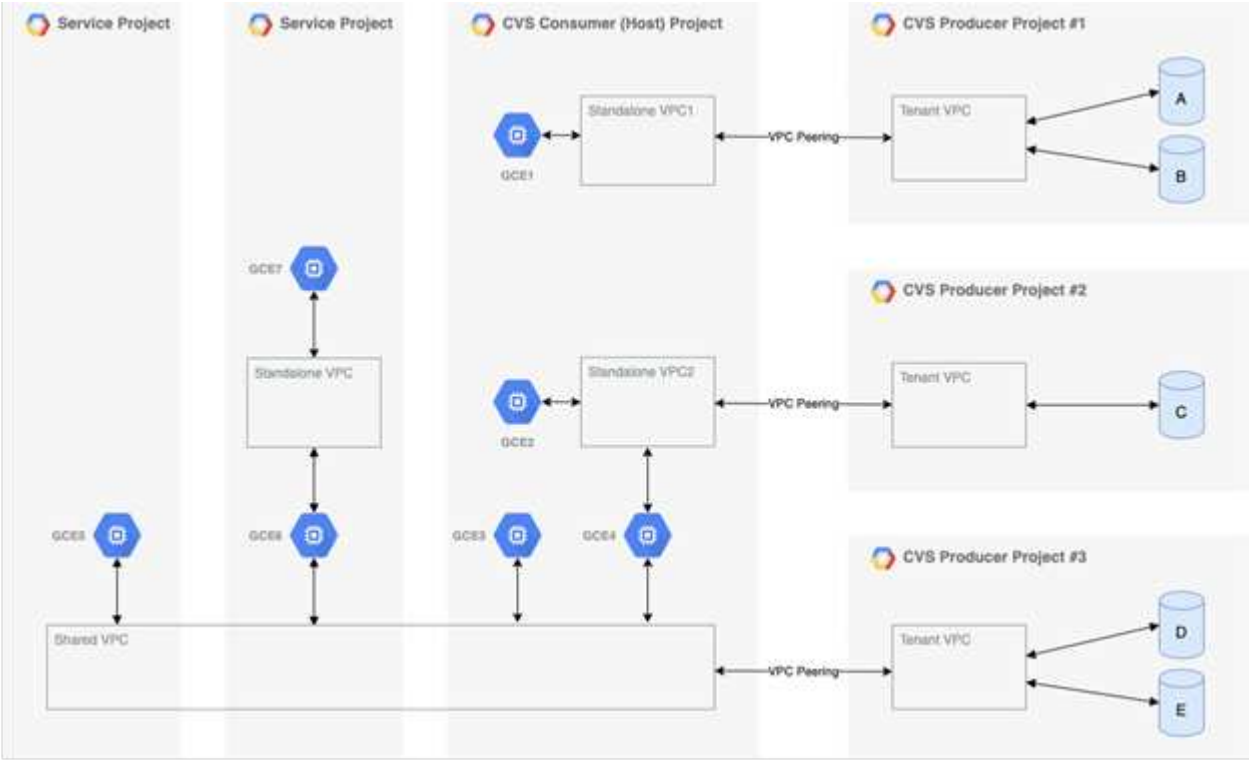
현재 사용자가 액세스할 수 있는 컨트롤 플레인 감사 로그를 사용할 수 없습니다.

데이터 플레인 아키텍처

Cloud Volumes Service for Google Cloud는 Google Cloud를 활용합니다 "프라이빗 서비스 액세스" 프레임워크: 이 프레임워크에서는 사용자가 Cloud Volumes Service에 연결할 수 있습니다. 이 프레임워크는 다른 Google Cloud 서비스와 같은 서비스 네트워킹 및 VPC 피어링 구조를 사용하여 테넌트 간의 완전한 격리를 보장합니다.

Google Cloud용 Cloud Volumes Service의 아키텍처 개요는 를 참조하십시오 "Cloud Volumes Service용 아키텍처".

사용자 VPC(독립 실행형 또는 공유)는 볼륨을 호스팅하는 Cloud Volumes Service 관리 테넌트 프로젝트 내의 VPC에 대해 자세히 살펴봅니다.



위 그림에서는 Cloud Volumes Service에 연결된 VPC 네트워크 3개와 볼륨을 공유하는 GCE1-7(다중 컴퓨팅 엔진 VM)이 포함된 프로젝트(중간 CVS 소비자 프로젝트)를 보여 줍니다.

- VPC1을 사용하면 GCE1이 볼륨 A와 B에 액세스할 수 있습니다

- VPC2는 GCE2와 GCE4가 볼륨 C에 액세스할 수 있도록 합니다
- 세 번째 VPC 네트워크는 공유 VPC로, 두 개의 서비스 프로젝트와 공유됩니다. GCE3, GCE4, GCE5 및 GCE6에서 D 및 E 볼륨에 액세스할 수 있습니다 공유 VPC 네트워크는 CVS 성능 서비스 유형의 볼륨에만 지원됩니다.

> GCE7은 어떤 볼륨에도 액세스할 수 없습니다.

데이터는 전송 중(Kerberos 및/또는 SMB 암호화 사용) 및 Cloud Volumes Service에 저장된 데이터를 모두 암호화할 수 있습니다.

전송 중인 데이터 암호화

전송 중인 데이터는 NAS 프로토콜 계층에서 암호화할 수 있으며, Google Cloud 네트워크 자체는 다음 섹션에 설명된 대로 암호화됩니다.

Google Cloud 네트워크

Google Cloud는 에 설명된 대로 네트워크 수준의 트래픽을 암호화합니다 "전송 중인 암호화" Google 문서. “Cloud Volumes Services 아키텍처” 섹션에서 언급한 것처럼 Cloud Volumes Service는 NetApp이 제어하는 PSA 생산자 프로젝트를 통해 제공됩니다.

CVS-SW의 경우 프로듀서 테넌트는 Google VM을 실행하여 서비스를 제공합니다. 사용자 VM과 Cloud Volumes Service VM 간의 트래픽은 Google에서 자동으로 암호화됩니다.

CVS의 데이터 경로 - 성능은 네트워크 계층에서 완전히 암호화되지 않지만, NetApp과 Google은 이 조합을 사용합니다 "IEEE 802.1AE 암호화(MACSec)", "캡슐화" (데이터 암호화) 및 물리적으로 제한된 네트워크를 통해 Cloud Volumes Service CVS - 성능 서비스 유형과 Google 클라우드 간에 전송 중인 데이터를 보호합니다.

NAS 프로토콜

NFS 및 SMB NAS 프로토콜은 프로토콜 계층에서 선택적 전송 암호화를 제공합니다.

SMB 암호화

"SMB 암호화" SMB 데이터의 엔드 투 엔드 암호화를 제공하고 신뢰할 수 없는 네트워크에서 데이터를 도청하지 못하도록 보호합니다. 클라이언트/서버 데이터 연결(SMB3.x 가능 클라이언트에만 사용 가능)과 서버/도메인 컨트롤러 인증에 대해 암호화를 설정할 수 있습니다.

SMB 암호화가 활성화된 경우 암호화를 지원하지 않는 클라이언트는 공유에 액세스할 수 없습니다.

Cloud Volumes Service는 SMB 암호화를 위한 RC4-HMAC, AES-128-CTS-HMAC-SHA1 및 AES-256-CTS-HMAC-SHA1 보안 암호를 지원합니다. SMB는 서버에서 지원되는 가장 높은 암호화 유형으로 협상합니다.

NFSv4.1 Kerberos

NFSv4.1의 경우 CVS - 성능은 에서 설명한 대로 Kerberos 인증을 제공합니다 "RFC7530". 볼륨별로 Kerberos를 활성화할 수 있습니다.

Kerberos에서 현재 가장 강력한 암호화 유형은 AES-256-CTS-HMAC-SHA1입니다. NetApp Cloud Volumes Service는 NFS용 AES-256-CTS-HMAC-SHA1, AES-128-CTS-HMAC-SHA1, DES3 및 DES를 지원합니다. 또한

CIFS/SMB 트래픽에 대해 ARCFOUR-HMAC(RC4)를 지원하지만 NFS에는 지원하지 않습니다.

Kerberos는 Kerberos 보안의 강화 방법을 선택할 수 있는 NFS 마운트에 대해 세 가지 서로 다른 보안 수준을 제공합니다.

RedHat에 따름 "일반 마운트 옵션" 설명서:

```
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.
```

일반적으로 Kerberos 보안 수준이 많을수록 클라이언트와 서버가 전송된 각 패킷의 NFS 작업을 암호화하고 해독하는 데 시간을 소비하므로 성능이 저하됩니다. 많은 클라이언트와 NFS 서버가 AES-NI 오프로딩을 CPU에 지원하므로 전반적인 환경이 개선되지만 Kerberos 5p(전체 엔드 투 엔드 암호화)의 성능 영향은 Kerberos 5(사용자 인증)의 영향보다 훨씬 큽니다.

다음 표에서는 보안 및 성능에 대한 각 수준의 차이점을 보여 줍니다.

보안 수준	보안	성능
NFSv3 - 시스템	• 최소 보안, 숫자 사용자 ID/그룹 ID가 있는 일반 텍스트 • UID, GID, 클라이언트 IP 주소, 내보내기 경로, 파일 이름, 패킷 캡처의 권한	• 대부분의 경우에 적합합니다
NFSv4.x - 시스템	• NFSv3(클라이언트 ID, 이름 문자열/도메인 문자열 일치)보다 더 안전하지만 여전히 일반 텍스트입니다 • UID, GID, 클라이언트 IP 주소, 이름 문자열, 도메인 ID를 볼 수 있습니다. 패킷 캡처의 내보내기 경로, 파일 이름, 권한	• 순차적 워크로드(예: VM, 데이터베이스, 대용량 파일)에 적합 • 파일 개수가 많음/메타데이터 많음(30~50% 악화)

보안 수준	보안	성능
NFS — krb5	• 모든 NFS 패킷의 자격 증명에 대한 Kerberos 암호화 - GSS 래퍼의 RPC 호출에서 사용자 /그룹의 UID/GID를 래핑합니다 • 마운트 액세스를 요청하는 사용자는 유효한 Kerberos 티켓(사용자 이름/암호 또는 수동 키 탭 교환)이 필요합니다. 티켓은 지정된 기간 후에 만료되며 사용자는 액세스를 위해 다시 인증해야 합니다 • 마운트/portmapper/NLM 같은 NFS 작업 또는 보조 프로토콜에 대한 암호화 없음(내보내기 경로, IP 주소, 파일 핸들, 권한, 파일 이름 패킷 캡처의 atime/mtime)	• Kerberos의 경우 대부분 최상, AUTH_SYS보다 나쁨
NFS — krb5i	• 모든 NFS 패킷의 자격 증명에 대한 Kerberos 암호화 - GSS 래퍼의 RPC 호출에서 사용자 /그룹의 UID/GID를 래핑합니다 • 마운트 액세스를 요청하는 사용자는 유효한 Kerberos 티켓(사용자 이름/암호 또는 수동 키 탭 교환)이 필요합니다. 티켓은 지정된 기간 후에 만료되며 사용자는 액세스를 위해 다시 인증해야 합니다 • 마운트/portmapper/NLM 같은 NFS 작업 또는 보조 프로토콜에 대한 암호화 없음(내보내기 경로, IP 주소, 파일 핸들, 권한, 파일 이름 패킷 캡처의 atime/mtime) • Kerberos GSS 체크섬은 패킷을 가로챌 수 없도록 모든 패킷에 추가됩니다. 체크섬이 일치하면 대화가 허용됩니다.	• NFS 페이로드가 암호화되지 않기 때문에 krb5p보다 낫습니다. krb5와 비교하여 추가된 오버헤드만 무결성 체크섬입니다. krb5i의 성능은 krb5보다 훨씬 나쁘지는 않지만 약간의 성능 저하가 발생할 수 있습니다.

보안 수준	보안	성능
NFS – krb5p	• 모든 NFS 패킷의 자격 증명에 대한 Kerberos 암호화 - GSS 래퍼의 RPC 호출에서 사용자 /그룹의 UID/GID를 래핑합니다 • 마운트 액세스를 요청하는 사용자는 유효한 Kerberos 티켓(사용자 이름/암호 또는 수동 키 탭 교환)이 필요합니다. 티켓은 지정된 기간 이후에 만료되며 사용자는 액세스를 위해 다시 인증해야 합니다 • 모든 NFS 패킷 페이로드는 GSS 래퍼로 암호화됩니다(패킷 캡처에서 파일 핸들, 권한, 파일 이름, atime/mtime을 볼 수 없음). • 무결성 검사를 포함합니다. • NFS 작업 유형이 표시됩니다(FSINFO, ACCESS, GETATTR 등). • 보조 프로토콜(마운트, 포트 맵, NLM 등)이 암호화되지 않음 - (내보내기 경로, IP 주소 확인 가능)	• 보안 수준의 최악의 성능: krb5p는 더 많은 암호화/암호 해독을 해야 합니다. • 파일 개수가 많은 워크로드에 대해 NFSv4.x를 사용할 경우 krb5p보다 성능이 더 우수합니다.

Cloud Volumes Service에서 구성된 Active Directory 서버는 Kerberos 서버 및 LDAP 서버로 사용됩니다(RFC2307 호환 스키마에서 사용자 ID를 조회하기 위해). 다른 Kerberos 또는 LDAP 서버는 지원되지 않습니다. Cloud Volumes Service에서 ID 관리를 위해 LDAP를 사용하는 것이 좋습니다. NFS Kerberos가 패킷 캡처에 표시되는 방법에 대한 자세한 내용은 섹션을 참조하십시오 ""“패킷 감지/추적 고려 사항”"

유휴 데이터 암호화

Cloud Volumes Service의 모든 볼륨은 AES-256 암호화를 사용하여 유휴 상태로 암호화되므로 미디어에 기록된 모든 사용자 데이터가 암호화되며 볼륨당 키를 통해서만 해독할 수 있습니다.

- CVS-SW의 경우 Google에서 생성한 키가 사용됩니다.
- CVS - 성능의 경우 볼륨별 키는 Cloud Volumes Service에 내장된 키 관리자에 저장됩니다.

2021년 11월부터 CMEK(고객 관리 암호화 키) 기능을 미리 볼 수 있습니다. 이렇게 하면 에서 호스팅되는 프로젝트별, 지역별 마스터 키를 사용하여 볼륨별 키를 암호화할 수 있습니다 "Google KMS(키 관리 서비스)." KMS를 사용하면 외부 키 관리자를 연결할 수 있습니다.

CVS용 KMS 구성 - 성능에 대한 자세한 내용은 을 참조하십시오 "고객이 관리하는 암호화 키 설정".

방화벽

Cloud Volumes Service는 NFS 및 SMB 공유를 지원하기 위해 여러 TCP 포트를 노출합니다.

- "NFS 액세스에 필요한 포트 수"
- "SMB 액세스에 필요한 포트"

또한 Kerberos를 비롯한 LDAP를 지원하는 SMB, NFS 및 이중 프로토콜 구성을 사용하려면 Windows Active Directory 도메인에 대한 액세스가 필요합니다. Active Directory 연결은 이어야 합니다 "구성됨" 지역별로 제공됩니다. Active Directory 도메인 컨트롤러(DC)는 를 사용하여 식별합니다 "DNS 기반 DC 검색" 지정된 DNS 서버를 사용합니다. 반환된 DC 중 하나가 사용됩니다. Active Directory 사이트를 지정하면 자격 있는 DC 목록을 제한할 수 있습니다.

Cloud Volumes Service는 와 함께 할당된 CIDR 범위의 IP 주소를 사용하여 에 도달합니다 `gcloud compute address` 명령을 실행하는 동안 "Cloud Volumes Service에 대한 온보딩". 이 CIDR을 소스 주소로 사용하여 Active Directory 도메인 컨트롤러에 대한 인바운드 방화벽을 구성할 수 있습니다.

Active Directory 도메인 컨트롤러가 필요합니다 "여기에 설명된 대로 Cloud Volumes Service CIDR에 포트를 노출합니다".

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이센스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이센스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 http://www.netapp.com/TM에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.