보안 및 데이터 암호화

Cloud Volumes ONTAP

NetApp
June 01, 2022

목차

보안 및 데이터 암호화

NetApp 암호화 솔루션으로 볼륨 암호화

Cloud Volumes ONTAP는 NVE(NetApp Volume Encryption) 및 NAE(NetApp Aggregate Encryption)를 지원합니다. NVE와 NAE는 FIPS 140-2를 준수하는 볼륨 유휴 데이터 암호화를 지원하는 소프트웨어 기반 솔루션입니다. "이러한 암호화 솔루션에 대해 자세히 알아보십시오".

NVE와 NAE는 모두 외부 키 관리자로 지원됩니다.

외부 키 관리자를 설정한 후 새 애그리게이트에 NAE가 기본적으로 사용하도록 설정됩니다. NAE 애그리게이트에 속하지 않는 새로운 볼륨은 기본적으로 NVE를 사용하도록 설정됩니다(예: 외부 키 관리자를 설정하기 전에 생성된 기존 애그리게이트가 있는 경우).

Cloud Volumes ONTAP는 온보드 키 관리를 지원하지 않습니다.

Cloud Volumes ONTAP 시스템은 NetApp 지원에 등록해야 합니다. NetApp 볼륨 암호화 라이센스는 NetApp Support에 등록된 각 Cloud Volumes ONTAP 시스템에 자동으로 설치됩니다.

- "Cloud Manager에 NetApp Support 사이트 계정 추가"
- "선불 종량제 시스템을 등록하는 중입니다"

Cloud Manager는 중국 지역에 있는 시스템에 NVE 라이센스를 설치하지 않습니다.

단계

1. 에서 지원되는 주요 관리자 목록을 검토합니다 "NetApp 상호 운용성 매트릭스 툴".

   Key Managers * 솔루션을 검색합니다.

2. "Cloud Volumes ONTAP CLI에 연결합니다".
3. 외부 키 관리를 구성합니다.
   - "Azure 키 저장소(AKV)"
     - "Google Cloud 키 관리 서비스"

Azure Key Vault를 사용하여 키를 관리합니다

을 사용할 수 있습니다 "Azure 키 저장소(AKV)" Azure로 배포된 응용 프로그램에서 ONTAP 암호화 키를 보호합니다.

AKV를 사용하여 보호할 수 있습니다 "NVE(NetApp Volume Encryption) 키" 데이터 SVM에만 해당.

AKV를 사용한 키 관리는 CLI 또는 ONTAP REST API를 사용하여 활성화할 수 있습니다.

AKV를 사용할 때는 기본적으로 데이터 SVM LIF가 클라우드 키 관리 엔드포인트와 통신하는 데 사용됩니다. 노드 관리 네트워크는 클라우드 공급자의 인증 서비스(login.microsoftonline.com 통신하는 데 사용됩니다. 클러스터 네트워크가 올바르게 구성되지 않은 경우 클러스터는 키 관리 서비스를 제대로 사용하지 않습니다.

필수 구성 요소

- Cloud Volumes ONTAP에서 버전 9.10.1 이상을 실행해야 합니다
- 설치된 볼륨 암호화(VE) 라이센스(NetApp 볼륨 암호화 라이센스는 NetApp Support에 등록된 각 Cloud Volumes ONTAP 시스템에 자동으로 설치됨)
- MTEKM(멀티 테넌트 암호화 키 관리) 라이센스가 설치되었습니다
- 클러스터 또는 SVM 관리자여야 합니다
- Active Azure 구독

제한 사항

- AKV는 데이터 SVM에서만 구성할 수 있습니다

구성 프로세스

이 단계에서는 Azure에 Cloud Volumes ONTAP 구성을 등록하는 방법과 Azure 키 저장소 및 키를 생성하는 방법을 설명합니다. 이 단계를 이미 완료한 경우, 특히 에서 올바른 구성 설정이 있는지 확인하십시오 Azure Key Vault를 작성합니다을 클릭한 다음 로 진행합니다 Cloud Volumes ONTAP 구성.

- Azure 애플리케이션 등록
- Azure 클라이언트 암호를 생성합니다
- Azure Key Vault를 작성합니다
- 암호화 키를 생성합니다
- Azure Active Directory 끝점 생성(HA만 해당)
- Cloud Volumes ONTAP 구성

Azure 애플리케이션 등록

1. 먼저 Cloud Volumes ONTAP가 Azure 키 저장소에 액세스하기 위해 사용할 Azure 구독에 응용 프로그램을 등록해야 합니다. Azure 포털에서 앱 등록 을 선택합니다.
2. 새 등록** 을 선택합니다.
3. 응용 프로그램의 이름을 제공하고 지원되는 응용 프로그램 유형을 선택합니다. Azure Key Vault 사용에 대한 기본 단일 테넌트 접미사 **Register** (등록**)을 선택합니다.
4. Azure 개요 창에서 등록한 애플리케이션을 선택합니다. 애플리케이션**(**클라이언트**) ID** 및 디렉토리**(**테넌트**) ID** 를 안전한 위치에 복사합니다. 등록 프로세스 후반부에 필요합니다.

Azure 클라이언트 암호를 생성합니다

1. Cloud Volumes ONTAP 응용 프로그램의 Azure 포털에서 인증서 및 암호 창을 선택합니다.
2. 새 클라이언트 암호** 클라이언트 비밀에 대한 의미 있는 이름을 입력합니다. NetApp에서는 24개월의 만료 기간을 권장하지만 특정 클라우드 거버넌스 정책에는 다른 설정이 필요할 수 있습니다.
3. 클라이언트 암호를 저장하려면 추가 를 선택합니다. 즉시 비밀의 값을 복사하고 나중에 구성할 수 있도록 안전한 곳에 저장합니다. 페이지를 벗어나 이동하면 암호 값이 표시되지 않습니다.

Azure Key Vault를 작성합니다

1. 기존 Azure 키 저장소가 있는 경우 Cloud Volumes ONTAP 구성에 연결할 수 있지만 이 프로세스의 설정에 액세스 정책을 적용해야 합니다.

2. Azure 포털에서 **Key Vaults** 섹션으로 이동합니다.
3. 작성 을 선택합니다. 리소스 그룹, 지역 및 가격 책정 계층을 비롯한 필수 정보를 입력하고 삭제된 볼트를 보존할 일수와 삭제 보호 활성화 여부를 선택합니다. 이 구성을 위해 기본값은 충분하지만 특정 클라우드 거버넌스 정책에는 다른 설정이 필요할 수 있습니다.
4. 액세스 정책을 선택하려면 다음 을 선택합니다.
5. 볼륨 암호화 옵션에 대한 **Azure** 디스크 암호화 및 권한 모델에 대한 볼트 액세스 정책을 선택합니다.
6. 액세스 정책 추가 를 선택합니다.
7. 템플릿에서 구성**(**선택 사항**)** 필드 옆의 캐럿을 선택합니다. 그런 다음 키**,** 비밀 및 인증 관리 를 선택합니다**.**
8. 각 드롭다운 권한 메뉴(키, 암호, 인증서)를 선택한 다음 메뉴 목록 상단의 모두 선택 을 선택하여 사용 가능한 모든 권한을 선택합니다. 다음과 같은 항목이 있어야 합니다.
   - 키 권한:19 선택됨
   - 비밀 권한:8 선택됨
   - 인증서 권한:16 선택됨
9. 액세스 정책을 만들려면 추가 를 선택합니다.
10. 다음 을 선택하여 네트워킹 옵션으로 진행합니다.
11. 적절한 네트워크 액세스 방법을 선택하거나 모든 네트워크 및 검토 **+** 작성을 선택하여 키 볼트를 작성합니다. (네트워크 액세스 방법은 거버넌스 정책 또는 회사 클라우드 보안 팀에서 규정할 수 있습니다.)
12. 키 볼트 URI 기록: 작성한 키 볼트에서 개요 메뉴로 이동하여 오른쪽 컬럼에서 볼트 **URI**를 복사합니다. 이 작업은 나중에 수행해야 합니다.

암호화 키를 생성합니다

1. Cloud Volumes ONTAP에 대해 만든 키 저장소 메뉴에서 키 옵션으로 이동합니다.
2. 새 키를 만들려면 **Generate/import** 를 선택합니다.
3. 기본 옵션을 **Generate** 로 설정된 상태로 둡니다.
4. 다음 정보를 제공합니다.
   - 암호화 키 이름입니다
   - 키 유형: RSA
   - RSA 키 크기: 2048
   - 활성화됨: 예
5. 암호화 키를 만들려면 만들기 를 선택합니다.
6. 키 메뉴로 돌아가서 방금 만든 키를 선택합니다.
7. 키 속성을 보려면 현재 버전 아래에서 키 ID를 선택합니다.
8. 키 식별자 필드를 찾습니다. 16진수 문자열을 포함하지만 포함되지 않는 최대 URI를 복사합니다.

Azure Active Directory 끝점 생성**(HA**만 해당**)**

1. 이 프로세스는 HA Cloud Volumes ONTAP 작업 환경을 위해 Azure 키 저장소를 구성하는 경우에만 필요합니다.
2. Azure 포털에서 가상 네트워크로 이동합니다.
3. Cloud Volumes ONTAP 작업 환경을 배포한 가상 네트워크를 선택하고 페이지 왼쪽의 **Subnets** 메뉴를

선택합니다.

4. 목록에서 Cloud Volumes ONTAP 구축의 서브넷 이름을 선택합니다.
5. 서비스 엔드포인트 제목으로 이동합니다. 드롭다운 메뉴의 목록에서 **Microsoft.AzureActiveDirectory**를 선택합니다.
6. 설정을 캡처하려면 저장을 선택합니다.

Cloud Volumes ONTAP 구성

1. 기본 SSH 클라이언트를 사용하여 클러스터 관리 LIF에 연결합니다.
2. ONTAP에서 고급 권한 모드 '고급 모드 해제'로 진입합니다
3. 원하는 데이터 SVM을 식별하고 DNS 구성 'vserver services name-service dns show'를 확인합니다
   a. 원하는 데이터 SVM에 대한 DNS 항목이 있고 Azure DNS에 대한 항목이 포함된 경우 별도의 조치가 필요하지 않습니다. 그렇지 않으면 Azure DNS, 프라이빗 DNS 또는 사내 서버를 가리키는 데이터 SVM용 DNS 서버 항목을 추가합니다. 클러스터 관리 SVM의 항목과 일치해야 합니다. 'vserver services name-service dns create-vserver_SVM_name_-domain_domain_-name-servers_ip_address_'
   b. SVM을 위해 DNS 서비스가 생성되었는지 확인합니다. 'vserver services name-service dns show'
4. 응용 프로그램 등록 후 저장된 클라이언트 ID와 테넌트 ID를 사용하여 Azure 키 볼트를 활성화합니다. '보안 키 관리자 외부 Azure enable - vserver_SVM_name_-client-id_Azure_client_ID_-tenant-id_Azure_tenant_ID_-name_Azure_key_name_-key-id_Azure_key_ID_
5. Key Manager 설정 'Security key-manager external Azure show'를 확인한다
6. Key Manager의 상태를 확인한다. '보안 Key-manager external Azure check' 출력 내용은 다음과 같다.

```
::*> security key-manager external azure check

Vserver: data_svm_name
Node: akvlab01-01

Category: service_reachability
    Status: OK

Category: ekmip_server
    Status: OK

Category: kms_wrapped_key_status
    Status: UNKNOWN
    Details: No volumes created yet for the vserver. Wrapped KEK status
will be available after creating encrypted volumes.

3 entries were displayed.
```

만약 'service_reachability' 상태가 'OK'가 아닌 경우, SVM은 필요한 모든 접속 및 권한으로 Azure Key Vault 서비스에 연결할 수 없습니다. 초기구성 시 kms_Wrapped_key_status가 unknown을 보고합니다. 첫 볼륨을 암호화하면 상태가 OK로 바뀝니다.

7. 선택 사항: 테스트 볼륨을 생성하여 AKV의 기능을 확인합니다. 'vol create-vserver_SVM_name_-volume_volume_name_-aggregate_aggr_-size_size_-state online-policy default'

   올바르게 구성된 경우 Cloud Volumes ONTAP는 자동으로 볼륨을 생성하고 볼륨 암호화를 활성화합니다.

8. 볼륨이 올바르게 생성되고 암호화되었는지 확인합니다. 이 경우 암호화된 매개 변수는 true로 표시됩니다. 'vol show-vserver_SVM_name_-fields is-encrypted'

Google의 클라우드 키 관리 서비스로 키를 관리합니다

을 사용할 수 있습니다 "Google Cloud Platform의 키 관리 서비스(Cloud KMS)" Google Cloud Platform에서 구축한 응용 프로그램에서 ONTAP 암호화 키를 보호합니다.

Cloud KMS를 사용한 키 관리는 CLI 또는 ONTAP REST API를 통해 활성화할 수 있습니다.

Cloud KMS를 사용할 때는 기본적으로 데이터 SVM LIF가 클라우드 키 관리 엔드포인트와 통신하는 데 사용됩니다. 노드 관리 네트워크는 클라우드 공급자의 인증 서비스(oauth2.googleapis.com 통신하는 데 사용됩니다. 클러스터 네트워크가 올바르게 구성되지 않은 경우 클러스터는 키 관리 서비스를 제대로 사용하지 않습니다.

필수 구성 요소

- Cloud Volumes ONTAP에서 버전 9.10.1 이상을 실행해야 합니다
- VE(Volume Encryption) 라이센스가 설치되었습니다
- MTEKM(멀티 테넌트 암호화 키 관리) 라이센스가 설치되었습니다
- 클러스터 또는 SVM 관리자여야 합니다
- Google Cloud Platform의 활성 서브스크립션입니다

제한 사항

- 클라우드 KMS는 데이터 SVM에서만 구성할 수 있습니다

구성

Google 클라우드

1. Google Cloud 환경에서는 "대칭 GCP 키 링 및 키를 생성합니다".
2. Cloud Volumes ONTAP 서비스 계정에 대한 사용자 지정 역할을 만듭니다.

```
gcloud iam roles create kmsCustomRole
    --project=<project_id>
    --title=<kms_custom_role_name>
    --description=<custom_role_description>

--permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersions.
list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVersions.
useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,cloudkms.loca
tions.get,cloudkms.locations.list,resourcemanager.projects.get
    --stage=GA
```

3. 사용자 지정 역할을 클라우드 KMS 키 및 Cloud Volumes ONTAP 서비스 계정에 할당합니다. "gcloud kms keys add-iam-policy-binding_key_name_—keyring_key_ring_name_—location_location_member ServiceAccount:_service_account_Name_—role projects/*customer_id*/kCustomRole"
4. 서비스 계정 JSON 키 다운로드:'gcloud iam service-accounts key create key-file --iam-account=*sa-name*@*project-id*.iam.gserviceaccount.com

Cloud Volumes ONTAP

1. 기본 SSH 클라이언트를 사용하여 클러스터 관리 LIF에 연결합니다.
2. 고급 권한 수준 설정 고급 으로 전환합니다
3. 데이터 SVM을 위한 DNS를 생성합니다. dns create-domain c.<*project*>.internal -name -servers_server_address_-vserver_SVM_name_'을 선택합니다
4. CMEK 항목 생성:'Security key-manager external GCP enable-vserver_SVM_name_-project-id_project_-key-ring-name_key_ring_name_-key-ring-location_location_-key-name_key_key_key_key_name_'입니다
5. 메시지가 표시되면 GCP 계정의 서비스 계정 JSON 키를 입력합니다.
6. 활성화된 프로세스가 성공했는지 확인합니다. '보안 키 - 관리자 외부 GCP 검사 - vserver_svm_name_'
7. 선택 사항: 암호화 'vol create_volume_name_-aggregate_aggregate_-vserver_vserver_name_-size 10G'를 테스트할 볼륨을 생성합니다

문제 해결

문제를 해결해야 하는 경우 위의 마지막 두 단계에서 원시 REST API 로그를 지정할 수 있습니다.

1. '세트 d'
2. 'systemshell-node_node_-command tail -f /mroot /etc/log/mlog/kmip2_client.log'

랜섬웨어에 대한 보호 개선

랜섬웨어 공격은 비즈니스 시간, 리소스 및 평판에 악영향을 줄 수 있습니다. Cloud Manager를 사용하면 랜섬웨어에 대한 NetApp 솔루션을 구축하고 가시성, 감지, 문제 해결을 위한 효율적인 툴을 제공할 수 있습니다.

단계

1. 작업 환경에서 * 랜섬웨어 * 아이콘을 클릭합니다.

2. 랜섬웨어에 대한 NetApp 솔루션 구현:

   a. 스냅샷 정책이 활성화되지 않은 볼륨이 있는 경우 * 스냅샷 정책 활성화 * 를 클릭합니다.

      NetApp Snapshot 기술은 랜섬웨어 해결을 위한 업계 최고의 솔루션을 제공합니다. 성공적인 복구의 핵심은 감염되지 않은 백업에서 복원하는 것입니다. Snapshot 복사본은 읽기 전용이므로 랜섬웨어 손상을 방지합니다. 또한 세분화하여 단일 파일 복사본 또는 전체 재해 복구 솔루션의 이미지를 생성할 수도 있습니다.

   b. FPolicy * 활성화 를 클릭하여 ONTAP의 FPolicy 솔루션을 활성화합니다. FPolicy 솔루션은 파일의 확장명에 따라 파일 작업을 차단할 수 있습니다.

      이 예방적 솔루션은 일반적인 랜섬웨어 파일 유형을 차단하여 랜섬웨어 공격으로부터 보호를 개선합니다.

      기본 FPolicy 범위는 다음 확장명의 파일을 차단합니다.

      마이크로, 암호화, 잠김, 암호화, 암호화, crinf, r5a, XRNT, XTBL, R16M01D05, pzdc, 양호, LOL!, OMG!, RDM, RK, encryptedRS, crjoker, enciped, LeChiffre

      Cloud Volumes ONTAP에서 FPolicy를 활성화하면 Cloud Manager에서 이 범위가 생성됩니다. 이 목록은 일반적인 랜섬웨어 파일 유형을 기반으로 합니다. Cloud Volumes ONTAP CLI에서 *vserver FPolicy scope* 명령을 사용하여 차단된 파일 확장명을 사용자 지정할 수 있습니다.