보안 및 데이터 암호화

Cloud Volumes ONTAP

NetApp
February 13, 2026

목차

보안 및 데이터 암호화

NetApp 암호화 솔루션을 사용하여 Cloud Volumes ONTAP 에서 볼륨 암호화

Cloud Volumes ONTAP NetApp Volume Encryption(NVE)과 NetApp Aggregate Encryption(NAE)을 지원합니다. NVE와 NAE는 볼륨의 FIPS 140-2 호환 저장 데이터 암호화를 지원하는 소프트웨어 기반 솔루션입니다. "이러한 암호화 솔루션에 대해 자세히 알아보세요" .

NVE와 NAE는 모두 외부 키 관리자를 통해 지원됩니다.

] endif::aws[] ifdef::azure[] endif::azure[] ifdef::gcp[] endif::gcp[] ifdef::aws[] endif::aws[] ifdef::azure[] endif::azure[] ifdef::gcp[] endif::gcp[

AWS Key Management Service를 사용하여 Cloud Volumes ONTAP 암호화 키 관리

사용할 수 있습니다"AWS의 키 관리 서비스(KMS)" AWS에 배포된 애플리케이션에서 ONTAP 암호화 키를 보호합니다.

AWS KMS를 통한 키 관리 기능은 CLI 또는 ONTAP REST API를 통해 활성화할 수 있습니다.

KMS를 사용할 때 기본적으로 데이터 SVM의 LIF가 클라우드 키 관리 엔드포인트와 통신하는 데 사용된다는 점에 유의하세요. 노드 관리 네트워크는 AWS 인증 서비스와 통신하는 데 사용됩니다. 클러스터 네트워크가 올바르게 구성되지 않으면 클러스터가 키 관리 서비스를 제대로 활용하지 못합니다.

시작하기 전에

- Cloud Volumes ONTAP 버전 9.12.0 이상을 실행해야 합니다.
- 볼륨 암호화(VE) 라이선스를 설치해야 합니다.
- MTEKM(Multi-tenant Encryption Key Management) 라이선스가 설치되어 있어야 합니다.
- 클러스터 또는 SVM 관리자여야 합니다.
- 활성 AWS 구독이 있어야 합니다.

ⓘ 데이터 SVM에 대해서만 키를 구성할 수 있습니다.

구성

AWS

1. 당신은 만들어야합니다"승인하다" 암호화를 관리하는 IAM 역할에서 사용될 AWS KMS 키에 대한 것입니다. IAM 역할에는 다음 작업을 허용하는 정책이 포함되어야 합니다.
    - `DescribeKey`
    - `Encrypt`
    - `Decrypt`보조금을 생성하려면 다음을 참조하세요."AWS 문서" .

2. "적절한 IAM 역할에 정책을 추가합니다."정책은 다음을 지원해야 합니다. `DescribeKey` , `Encrypt` , 그리고 `Decrypt` 운영.

Cloud Volumes ONTAP

1. Cloud Volumes ONTAP 환경으로 전환하세요.
2. 고급 권한 수준으로 전환:
   `set -privilege advanced`
3. AWS 키 관리자를 활성화합니다.
   `security key-manager external aws enable -vserver data_svm_name -region AWS_region -key-id key_ID -encryption-context encryption_context`
4. 메시지가 표시되면 비밀 키를 입력하세요.
5. AWS KMS가 올바르게 구성되었는지 확인하세요.
   `security key-manager external aws show -vserver svm_name`

Azure Key Vault를 사용하여 Cloud Volumes ONTAP 암호화 키 관리

Azure Key Vault(AKV)를 사용하면 Azure에 배포된 애플리케이션에서 ONTAP 암호화 키를 보호할 수 있습니다. 를 참조하세요"Microsoft 설명서" .

AKV는 데이터 SVM에 대해서만 NetApp 볼륨 암호화(NVE) 키를 보호하는 데 사용할 수 있습니다. 자세한 내용은 다음을 참조하세요. "ONTAP 문서" .

AKV를 사용한 키 관리 기능은 CLI 또는 ONTAP REST API를 통해 활성화할 수 있습니다.

AKV를 사용할 때 기본적으로 데이터 SVM LIF를 사용하여 클라우드 키 관리 엔드포인트와 통신한다는 점에 유의하세요. 노드 관리 네트워크는 클라우드 공급자의 인증 서비스(login.microsoftonline.com)와 통신하는 데 사용됩니다. 클러스터 네트워크가 올바르게 구성되지 않으면 클러스터가 키 관리 서비스를 제대로 활용하지 못합니다.

시작하기 전에

- Cloud Volumes ONTAP 버전 9.10.1 이상을 실행해야 합니다.
- 볼륨 암호화(VE) 라이선스가 설치됨(NetApp 볼륨 암호화 라이선스는 NetApp 지원에 등록된 각 Cloud Volumes ONTAP 시스템에 자동으로 설치됨)
- 다중 테넌트 암호화 키 관리(MT_EK_MGMT) 라이선스가 있어야 합니다.
- 클러스터 또는 SVM 관리자여야 합니다.
- 활성 Azure 구독

제한 사항

- AKV는 데이터 SVM에서만 구성될 수 있습니다.
- NAE는 AKV와 함께 사용할 수 없습니다. NAE에는 외부 지원 KMIP 서버가 필요합니다.
- Cloud Volumes ONTAP 노드는 15분마다 AKV를 폴링하여 접근성과 키 가용성을 확인합니다. 이 폴링 기간은 구성할 수 없으며, 폴링 시도에서 4번 연속 실패하면(총 1시간) 볼륨이 오프라인으로 전환됩니다.

구성 프로세스

설명된 단계에서는 Cloud Volumes ONTAP 구성을 Azure에 등록하는 방법과 Azure Key Vault 및 키를 만드는 방법을 설명합니다. 이미 이러한 단계를 완료한 경우 특히 올바른 구성 설정이 있는지 확인하십시오.Azure Key Vault 만들기 , 그리고 다음으로 진행합니다Cloud Volumes ONTAP 구성 .

- Azure 애플리케이션 등록
- Azure 클라이언트 비밀 만들기
- Azure Key Vault 만들기
- 암호화 키 생성
- Azure Active Directory 엔드포인트 만들기(HA 전용)
- Cloud Volumes ONTAP 구성

Azure 애플리케이션 등록

1. 먼저 Cloud Volumes ONTAP Azure Key Vault에 액세스하는 데 사용할 Azure 구독에 애플리케이션을 등록해야 합니다. Azure Portal에서 앱 등록을 선택합니다.
2. 신규 등록을 선택하세요.
3. 애플리케이션 이름을 입력하고 지원되는 애플리케이션 유형을 선택하세요. Azure Key Vault를 사용하려면 기본 단일 테넌트로 충분합니다. 등록을 선택하세요.
4. Azure 개요 창에서 등록한 애플리케이션을 선택합니다. 애플리케이션**(**클라이언트**) ID**와 디렉토리**(**테넌트**) ID**를 안전한 위치에 복사합니다. 이는 나중에 등록 과정에서 필요합니다.

Azure 클라이언트 비밀 만들기

1. Azure Key Vault 앱 등록을 위한 Azure Portal에서 인증서 및 비밀 창을 선택합니다.
2. 새로운 클라이언트 비밀번호를 선택하세요. 클라이언트 비밀번호에 의미 있는 이름을 입력하세요. NetApp 24개월 만료 기간을 권장하지만, 특정 클라우드 거버넌스 정책에는 다른 설정이 필요할 수 있습니다.
3. 추가를 클릭하여 클라이언트 비밀번호를 생성합니다. 값 열에 나열된 비밀 문자열을 복사하여 나중에 사용할 수 있도록 안전한 위치에 저장하세요.Cloud Volumes ONTAP 구성 . 해당 페이지에서 벗어나면 비밀번호 값은 다시 표시되지 않습니다.

Azure Key Vault 만들기

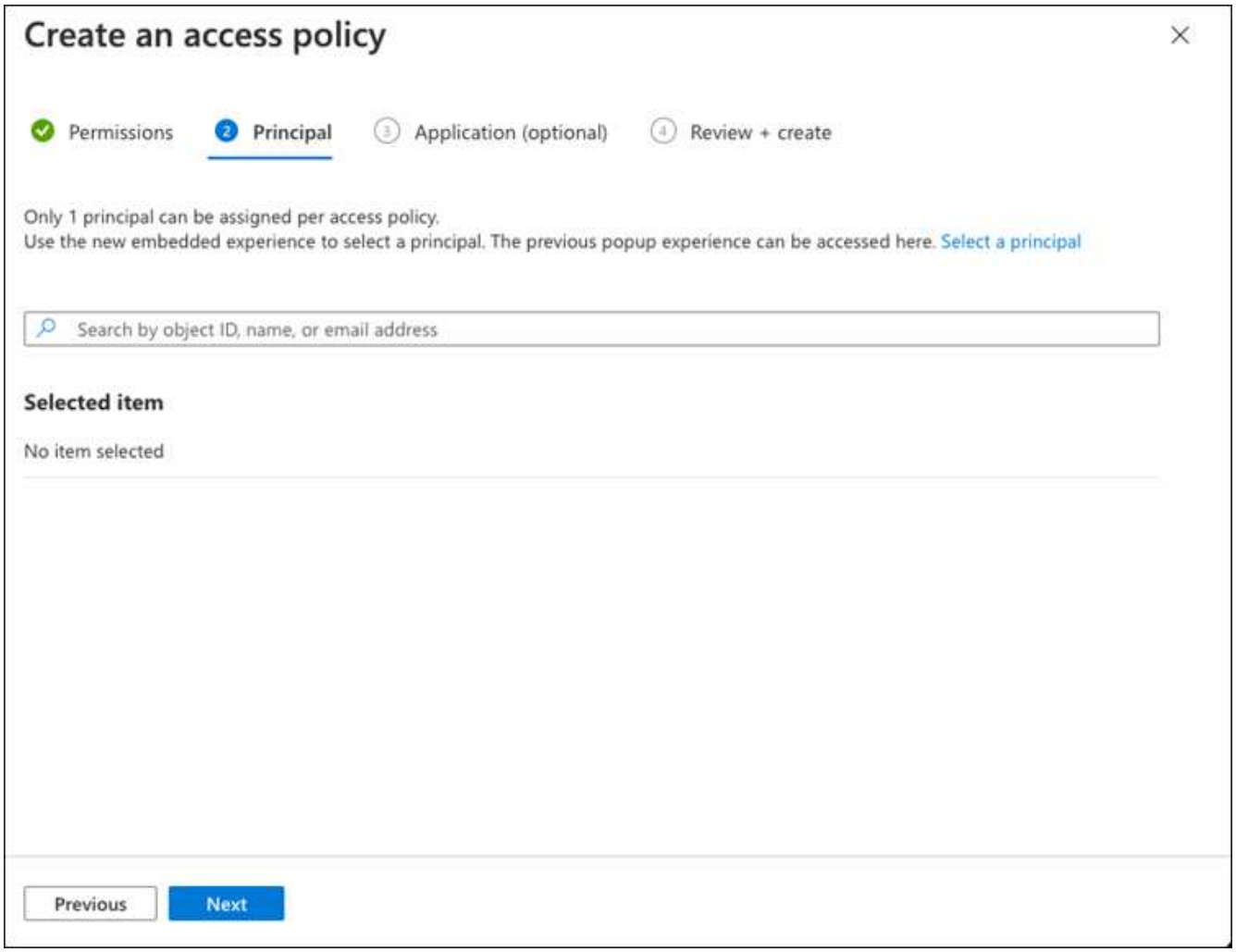
1. 기존 Azure Key Vault가 있는 경우 Cloud Volumes ONTAP 구성에 연결할 수 있습니다. 하지만 이 프로세스에서는 설정에 맞게 액세스 정책을 조정해야 합니다.
2. Azure Portal에서 키 자격 증명 모음 섹션으로 이동합니다.
3. **+**만들기를 클릭하고 리소스 그룹, 지역, 가격 책정 계층을 포함한 필수 정보를 입력합니다. 또한 삭제된 볼트를 보관할 일수를 입력하고 키 볼트에서 퍼지 보호 사용을 선택합니다.
4. 다음을 선택하여 액세스 정책을 선택하세요.
5. 다음 옵션을 선택하세요:
   a. 액세스 구성에서 **Vault** 액세스 정책을 선택합니다.
   b. 리소스 액세스에서 볼륨 암호화를 위해 **Azure Disk Encryption**을 선택합니다.
6. **+**만들기를 선택하여 액세스 정책을 추가합니다.
7. 템플릿에서 구성에서 드롭다운 메뉴를 클릭한 다음 키**,** 비밀번호 및 인증서 관리 템플릿을 선택합니다.

8. 각 드롭다운 권한 메뉴(키, 비밀, 인증서)를 선택한 다음 메뉴 목록 상단에서 모두 선택을 클릭하여 사용 가능한 모든 권한을 선택합니다. 다음이 있어야 합니다.
    - 주요 권한: 20개 선택됨
    - 비밀 권한: 8개 선택됨
    - 인증서 권한: 16개 선택됨


Create an access policy
1 Permissions
2 Principal
3 Application (optional)
4 Review + create
Configure from a template
Key, Secret, & Certificate Management
Key permissions
Key Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Cryptographic Operations
Select all
Decrypt
Encrypt
Unwrap Key
Wrap Key
Verify
Sign
Privileged Key Operations
Select all
Purge
Release
Rotation Policy Operations
Select all
Rotate
Get Rotation Policy
Set Rotation Policy
Secret permissions
Secret Management Operations
Select all
Get
List
Set
Delete
Recover
Backup
Restore
Privileged Secret Operations
Select all
Purge
Certificate permissions
Certificate Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Manage Contacts
Manage Certificate Authorities
Get Certificate Authorities
List Certificate Authorities
Set Certificate Authorities
Delete Certificate Authorities
Privileged Certificate Operations
Select all
Purge
Previous
Next

9. 다음을 클릭하여 주 Azure 등록 애플리케이션을 선택하십시오.Azure 애플리케이션 등록 . 다음을 선택하세요.

   정책당 한 명의 주체만 할당할 수 있습니다.



10. 다음을 두 번 클릭하여 검토 및 생성에 도달합니다. 그런 다음 만들기를 클릭합니다.
11. 다음을 선택하여 네트워킹 옵션으로 넘어갑니다.
12. 적절한 네트워크 액세스 방법을 선택하거나 모든 네트워크와 검토 **+** 생성을 선택하여 키 보관소를 만듭니다. (네트워크 액세스 방법은 거버넌스 정책이나 회사 클라우드 보안 팀에서 규정할 수 있습니다.)
13. 키 보관소 URI를 기록합니다. 생성한 키 보관소에서 개요 메뉴로 이동하여 오른쪽 열에서 보관소 **URI**를 복사합니다. 이것은 나중의 단계에서 필요합니다.

암호화 키 생성

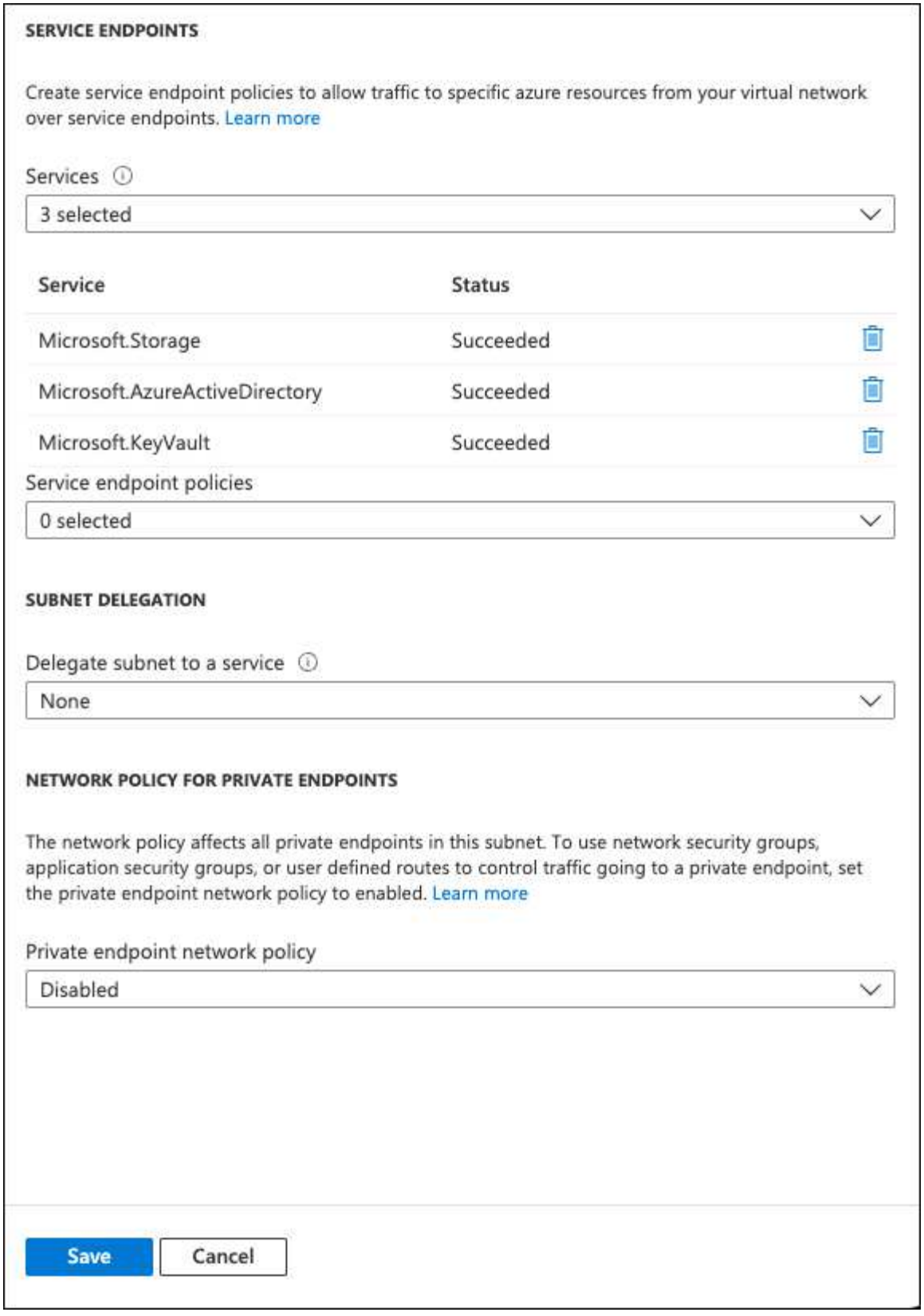
1. Cloud Volumes ONTAP 에 대해 생성한 Key Vault 메뉴에서 키 옵션으로 이동합니다.
2. 생성/가져오기를 선택하여 새 키를 만듭니다.
3. 기본 옵션을 생성으로 설정된 상태로 둡니다.
4. 다음 정보를 제공하세요.
   - 암호화 키 이름

- 키 유형: RSA
- RSA 키 크기: 2048
- 활성화됨: 예

5. 암호화 키를 생성하려면 생성을 선택하세요.
6. 키 메뉴로 돌아가서 방금 만든 키를 선택하세요.
7. 현재 버전에서 키 ID를 선택하여 키 속성을 확인하세요.
8. 키 식별자 필드를 찾으세요. 16진수 문자열을 제외하고 URI를 해당 문자열까지 복사합니다.

Azure Active Directory 엔드포인트 만들기**(HA** 전용**)**

1. 이 프로세스는 HA Cloud Volumes ONTAP 시스템에 대해 Azure Key Vault를 구성하는 경우에만 필요합니다.
2. Azure Portal에서 가상 네트워크로 이동합니다.
3. Cloud Volumes ONTAP 시스템을 배포한 가상 네트워크를 선택하고 페이지 왼쪽에 있는 서브넷 메뉴를 선택합니다.
4. 목록에서 Cloud Volumes ONTAP 배포에 대한 서브넷 이름을 선택합니다.
5. 서비스 엔드포인트 제목으로 이동합니다. 드롭다운 메뉴에서 다음을 선택하세요.
   - **Microsoft.AzureActiveDirectory**
   - 마이크로소프트 키볼트
   - **Microsoft.Storage** (선택 사항)



6. 저장을 선택하여 설정을 적용합니다.

Cloud Volumes ONTAP 구성

1. 원하는 SSH 클라이언트를 사용하여 클러스터 관리 LIF에 연결합니다.
2. ONTAP 에서 고급 권한 모드로 들어가세요:

```
set advanced -con off
```

3. 원하는 데이터 SVM을 식별하고 DNS 구성을 확인합니다.
   `vserver services name-service dns show`

   a. 원하는 데이터 SVM에 대한 DNS 항목이 있고 Azure DNS에 대한 항목이 포함되어 있는 경우 아무 작업도 필요하지 않습니다. 그렇지 않은 경우 Azure DNS, 개인 DNS 또는 온-프레미스 서버를 가리키는 데이터 SVM에 대한 DNS 서버 항목을 추가합니다. 이는 클러스터 관리 SVM 항목과 일치해야 합니다.
   `vserver services name-service dns create -vserver SVM_name -domains domain -name-servers IP_address`

   b. 데이터 SVM에 대한 DNS 서비스가 생성되었는지 확인하세요.
   `vserver services name-service dns show`

4. 애플리케이션 등록 후 저장된 클라이언트 ID와 테넌트 ID를 사용하여 Azure Key Vault를 활성화합니다.
   `security key-manager external azure enable -vserver SVM_name -client-id Azure_client_ID -tenant-id Azure_tenant_ID -name key_vault_URI -key-id full_key_URI`

   > 그만큼 `_full_key_URI` 가치는 활용되어야 합니다 `<https:// <key vault host name>/keys/<key label>` 체재.

5. Azure Key Vault를 성공적으로 활성화한 후 다음을 입력하십시오. `client secret value` 메시지가 표시되면.

6. 키 관리자의 상태를 확인하세요.
   `security key-manager external azure check` 출력은 다음과 같습니다.

```
::*> 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 아닙니다 `OK` SVM은 필요한 모든 연결 및 권한을 통해 Azure Key Vault 서비스에 연결할 수 없습니다. Azure 네트워크 정책과 라우팅이 개인 vNet이 Azure Key Vault 공용 엔드포인트에 도달하는 것을 차단하지 않는지 확인하세요. 그렇다면 vNet 내에서 Key Vault에 액세스하기 위해 Azure Private 엔드포인트를 사용하는 것을 고려하세요. 엔드포인트의 개인 IP 주소를 확인하려면 SVM에 정적 호스트 항목을 추가해야 할 수도 있습니다.

그만큼 `kms_wrapped_key_status` 보고할 것이다 `UNKNOWN` 초기 구성에서. 상태가 다음으로 변경됩니다. `OK` 첫 번째 볼륨이 암호화된 후.

7. 선택 사항: NVE의 기능을 확인하기 위해 테스트 볼륨을 만듭니다.

   ```
   vol create -vserver SVM_name -volume volume_name -aggregate aggr -size size
   -state online -policy default
   ```

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

8. 볼륨이 올바르게 생성되고 암호화되었는지 확인하세요. 그렇다면, `-is-encrypted` 매개변수는 다음과 같이 표시됩니다. `true` .
   ```
   vol show -vserver SVM_name -fields is-encrypted
   ```
9. 선택 사항: Azure Key Vault 인증 인증서의 자격 증명을 업데이트하려면 다음 명령을 사용하세요.
   ```
   security key-manager external azure update-credentials -vserver v1
   -authentication-method certificate
   ```

관련 링크

- "Azure에서 고객 관리 키를 사용하도록 Cloud Volumes ONTAP 설정"
- "Microsoft Azure 설명서: Azure Key Vault 정보"
- "ONTAP 명령 참조 가이드"

Google Cloud KMS를 사용하여 Cloud Volumes ONTAP 암호화 키 관리

사용할 수 있습니다"Google Cloud Platform의 키 관리 서비스(Cloud KMS)" Google Cloud Platform에 배포된 애플리케이션에서 Cloud Volumes ONTAP 암호화 키를 보호합니다.

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

Cloud KMS를 사용할 때 기본적으로 데이터 SVM의 LIF가 클라우드 키 관리 엔드포인트와 통신하는 데 사용된다는 점에 유의하세요. 노드 관리 네트워크는 클라우드 제공자의 인증 서비스(oauth2.googleapis.com)와 통신하는 데 사용됩니다. 클러스터 네트워크가 올바르게 구성되지 않으면 클러스터가 키 관리 서비스를 제대로 활용하지 못합니다.

시작하기 전에

- 시스템에서는 Cloud Volumes ONTAP 9.10.1 이상을 실행해야 합니다.
- 데이터 SVM을 사용해야 합니다. Cloud KMS는 데이터 SVM에서만 구성할 수 있습니다.
- 클러스터 또는 SVM 관리자여야 합니다.
- SVM에 볼륨 암호화(VE) 라이선스를 설치해야 합니다.
- Cloud Volumes ONTAP 9.12.1 GA부터 다중 테넌트 암호화 키 관리(MTEKM) 라이선스도 설치해야 합니다.
- 활성화된 Google Cloud Platform 구독이 필요합니다.

구성

구글 클라우드

1. Google Cloud 환경에서"대칭 GCP 키 링과 키를 생성합니다." .
2. Cloud KMS 키와 Cloud Volumes ONTAP 서비스 계정에 사용자 지정 역할을 할당합니다.
   a. 사용자 정의 역할을 만듭니다.

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

--permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersio
ns.list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVer
sions.useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,clou
dkms.locations.get,cloudkms.locations.list,resourcemanager.projects.g
et
    --stage=GA
```

   b. 생성한 사용자 지정 역할을 할당합니다.
   `gcloud kms keys add-iam-policy-binding` *`key_name`* `--keyring` *`key_ring_name`* `--location` *`key_location`* `--member serviceAccount:_service_account_Name_ --role projects/`*`customer_project_id`*`/roles/kmsCustomRole`

> Cloud Volumes ONTAP 9.13.0 이상을 사용하는 경우 사용자 지정 역할을 만들 필요가 없습니다. 미리 정의된 것을 할당할 수 있습니다 [`cloudkms.cryptoKeyEncrypterDecrypter` ^] 역할.

3. 서비스 계정 JSON 키 다운로드:
   `gcloud iam service-accounts keys create key-file --iam-account=`*`sa-name`*`@`*`project-id`*`.iam.gserviceaccount.com`

Cloud Volumes ONTAP

1. 원하는 SSH 클라이언트를 사용하여 클러스터 관리 LIF에 연결합니다.
2. 고급 권한 수준으로 전환:
   `set -privilege advanced`
3. 데이터 SVM에 대한 DNS를 생성합니다.
   `dns create -domains c.<`*`project`*`>.internal -name-servers` *`server_address`* `-vserver` *`SVM_name`*
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` *`key_ring_location`* `-key-name` *`key_name`*
5. 메시지가 표시되면 GCP 계정의 서비스 계정 JSON 키를 입력합니다.
6. 활성화된 프로세스가 성공했는지 확인하세요.
   `security key-manager external gcp check -vserver` *`svm_name`*
7. 선택 사항: 암호화를 테스트하기 위한 볼륨 생성 `vol create` *`volume_name`* `-aggregate` *`aggregate`*

```
-vserver vserver_name -size 10G
```

문제 해결

문제 해결이 필요한 경우 위의 마지막 두 단계에서 원시 REST API 로그를 추적할 수 있습니다.

1. `set d`
2. `systemshell -node node -command tail -f /mroot/etc/log/mlog/kmip2_client.log`

Cloud Volumes ONTAP 에 NetApp 랜섬웨어 보호 솔루션 활성화

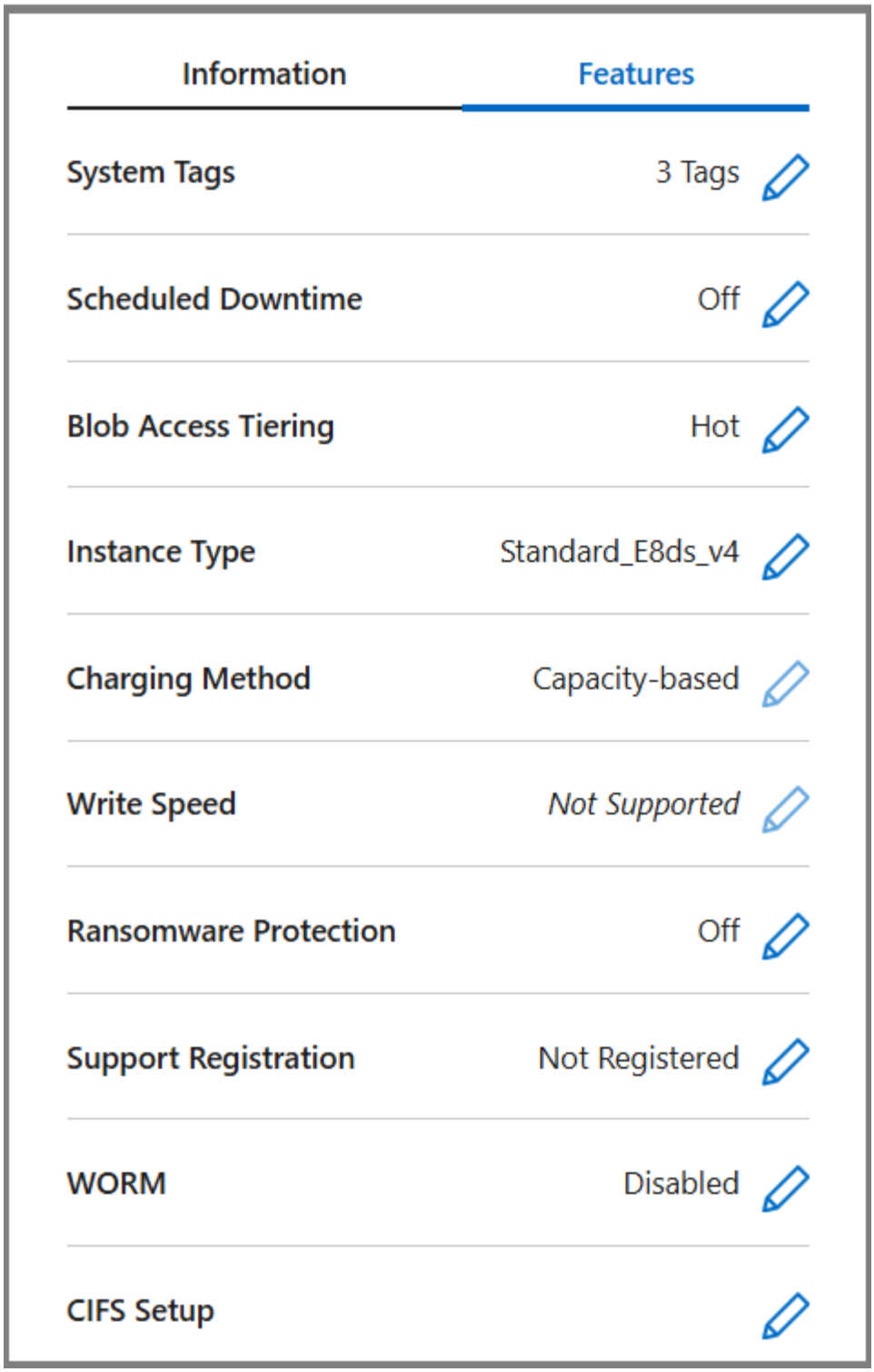
랜섬웨어 공격은 기업의 시간, 자원, 평판을 앗아갈 수 있습니다. NetApp Console 사용하면 랜섬웨어에 대한 두 가지 NetApp 솔루션, 즉 일반적인 랜섬웨어 파일 확장자로부터의 보호 및 자율 랜섬웨어 보호(ARP)를 구현할 수 있습니다. 이러한 솔루션은 가시성, 탐지 및 복구를 위한 효과적인 도구를 제공합니다.

일반적인 랜섬웨어 파일 확장자로부터 보호

콘솔에서 사용할 수 있는 랜섬웨어 보호 설정을 사용하면 ONTAP FPolicy 기능을 활용하여 일반적인 랜섬웨어 파일 확장자 유형으로부터 보호할 수 있습니다.

단계

1. 시스템 페이지에서 랜섬웨어 보호를 사용하도록 구성한 Cloud Volumes ONTAP 시스템의 이름을 두 번 클릭합니다.
2. 개요 탭에서 기능 패널을 클릭한 다음 랜섬웨어 보호 옆에 있는 연필 아이콘을 클릭합니다.



3. 랜섬웨어에 대한 NetApp 솔루션 구현:

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

      NetApp Snapshot 기술은 랜섬웨어 치료를 위한 업계 최고의 솔루션을 제공합니다. 성공적인 복구의 핵심은 감염되지 않은 백업에서 복원하는 것입니다. 스냅샷 사본은 읽기 전용이므로 랜섬웨어로 인한 손상을 방지할 수 있습니다. 또한 단일 파일 사본이나 완벽한 재해 복구 솔루션의 이미지를 만드는 세분성을 제공할 수도 있습니다.

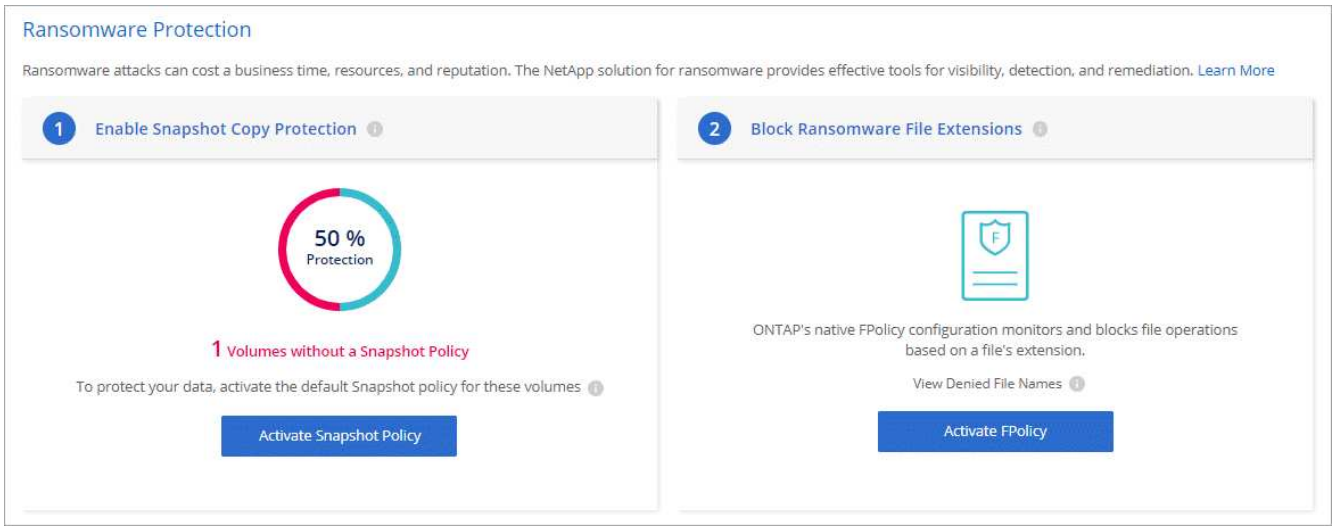
b. ONTAP의 FPolicy 솔루션을 활성화하려면 *FPolicy 활성화*를 클릭하세요. 이 솔루션은 파일 확장자를 기준으로 파일 작업을 차단할 수 있습니다.

   이 예방 솔루션은 일반적인 랜섬웨어 파일 유형을 차단하여 랜섬웨어 공격으로부터의 보호 기능을 강화합니다.

   기본 FPolicy 범위는 다음 확장자를 가진 파일을 차단합니다.

   마이크로, 암호화된, 잠긴, 크립토, 크립토, crinf, r5a, XRNT, XTBL, R16M01D05, pzdc, 좋은, LOL!, OMG!, RDM, RRK, encryptedRS, crjoker, EnCiPhErEd, LeChiffre

   이 범위는 Cloud Volumes ONTAP 에서 FPolicy를 활성화할 때 생성됩니다. 이 목록은 일반적인 랜섬웨어 파일 유형을 기반으로 작성되었습니다. Cloud Volumes ONTAP CLI의 *vserver fpolicy policy scope* 명령을 사용하여 차단된 파일 확장자를 사용자 정의할 수 있습니다.



자율형 랜섬웨어 보호

Cloud Volumes ONTAP 랜섬웨어 공격을 나타낼 수 있는 비정상적인 활동을 사전에 감지하고 경고하기 위해 워크로드에 대한 분석을 수행하는 ARP(Autonomous Ransomware Protection) 기능을 지원합니다.

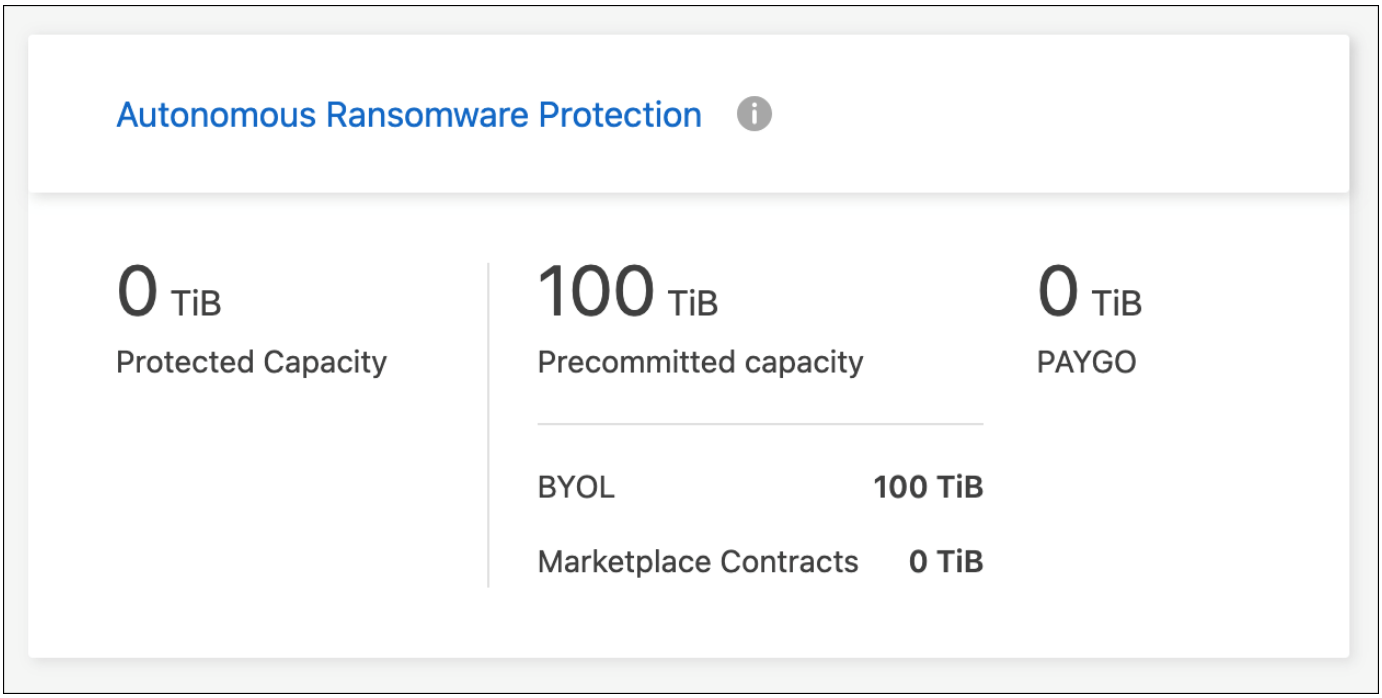
다음을 통해 제공되는 파일 확장자 보호와 별도로 "랜섬웨어 보호 설정" ARP 기능은 작업 부하 분석을 사용하여 감지된 "비정상적인 활동"을 기반으로 잠재적인 공격에 대해 사용자에게 경고합니다. 랜섬웨어 보호 설정과 ARP 기능은 모두 종합적인 랜섬웨어 보호를 위해 함께 사용할 수 있습니다.

ARP 기능은 추가 비용 없이 BYOL(Bring Your Own License) 및 마켓플레이스 구독을 통해 라이선스를 사용할 수 있습니다.

ARP 지원 볼륨에는 "학습 모드" 또는 "활성" 상태가 지정됩니다.

볼륨에 대한 ARP 구성은 ONTAP 시스템 관리자와 ONTAP CLI를 통해 수행됩니다.

ONTAP System Manager 및 ONTAP CLI를 사용하여 ARP를 활성화하는 방법에 대한 자세한 내용은 다음을 참조하십시오. "ONTAP 설명서: 자율 랜섬웨어 보호 활성화" .



Cloud Volumes ONTAP 에서 WORM 파일의 변조 방지 스냅샷 복사본을 만듭니다.

Cloud Volumes ONTAP 시스템에서 한 번 쓰고 여러 번 읽을 수 있는(WORM) 파일의 변조 방지 스냅샷 사본을 만들고 특정 보존 기간 동안 수정되지 않은 형태로 스냅샷을 보관할 수 있습니다. 이 기능은 SnapLock 기술을 기반으로 하며, 데이터 보호 및 규정 준수를 한층 더 강화합니다.

시작하기 전에

스냅샷 복사본을 만드는 데 사용하는 볼륨이 SnapLock 볼륨인지 확인하세요. 볼륨에서 SnapLock 보호를 활성화하는 방법에 대한 자세한 내용은 다음을 참조하십시오. "ONTAP 설명서: SnapLock 구성" .

단계

1. SnapLock 볼륨에서 스냅샷 복사본을 만듭니다. CLI 또는 시스템 관리자를 사용하여 스냅샷 복사본을 만드는 방법에 대한 자세한 내용은 다음을 참조하십시오. "ONTAP 설명서: 로컬 스냅샷 복사본 관리 개요" .

   스냅샷 복사본은 볼륨의 WORM 속성을 상속하므로 변조가 불가능합니다. 기본 SnapLock 기술은 지정된 보존 기간이 경과할 때까지 스냅샷이 편집 및 삭제되지 않도록 보호합니다.

2. 스냅샷을 편집해야 하는 경우 보존 기간을 수정할 수 있습니다. 자세한 내용은 다음을 참조하세요. "ONTAP 문서: 보존 시간 설정" .

> ⓘ 스냅샷 사본은 특정 보존 기간 동안 보호되지만, Cloud Volumes ONTAP 의 WORM 스토리지는 "신뢰할 수 있는 스토리지 관리자" 모델에서 작동하므로 클러스터 관리자가 소스 볼륨을 삭제할 수 있습니다. 또한 신뢰할 수 있는 클라우드 관리자는 클라우드 스토리지 리소스를 조작하여 WORM 데이터를 삭제할 수 있습니다.

관련 링크

- WORM에 대한 자세한 내용은 다음을 참조하세요."Cloud Volumes ONTAP 의 WORM 스토리지에 대해

알아보세요" .

- SnapLock 볼륨 충전에 대한 정보는 다음을 참조하세요."Cloud Volumes ONTAP 의 라이선싱 및 요금 청구" .