



## 보안 및 데이터 암호화 Cloud Volumes ONTAP

NetApp  
July 22, 2024

# 목차

- 보안 및 데이터 암호화 ..... 1
  - NetApp 암호화 솔루션으로 볼륨 암호화 ..... 1
  - AWS 키 관리 서비스로 키를 관리합니다 ..... 1
  - Azure Key Vault를 사용하여 키를 관리합니다 ..... 2
  - Google의 클라우드 키 관리 서비스로 키를 관리합니다 ..... 9
  - 랜섬웨어에 대한 보호 개선 ..... 11

# 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 유향 데이터 암호화를 지원하는 소프트웨어 기반 솔루션입니다. ["이러한 암호화 솔루션에 대해 자세히 알아보십시오"](#).

NVE와 NAE는 모두 외부 키 관리자로 지원됩니다.

## AWS 키 관리 서비스로 키를 관리합니다

을 사용할 수 있습니다 ["AWS KMS\(Key Management Service\)"](#) Google Cloud Platform에서 구축한 응용 프로그램에서 ONTAP 암호화 키를 보호합니다.

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

KMS를 사용할 때는 기본적으로 데이터 SVM의 LIF가 클라우드 키 관리 엔드포인트와 통신하는 데 사용됩니다. 노드 관리 네트워크는 AWS의 인증 서비스와 통신하는 데 사용됩니다. 클러스터 네트워크가 올바르게 구성되지 않은 경우 클러스터는 키 관리 서비스를 제대로 사용하지 않습니다.

시작하기 전에

- Cloud Volumes ONTAP는 버전 9.12.0 이상을 실행해야 합니다
- 볼륨 암호화(VE) 라이선스 및 을(를) 설치해야 합니다
- MTEKM(멀티 테넌트 암호화 키 관리) 라이선스가 설치되어 있어야 합니다.
- 클러스터 또는 SVM 관리자여야 합니다
- 활성 AWS 구독이 있어야 합니다



데이터 SVM에 대한 키만 구성할 수 있습니다.

## 구성

설치하고

1. 을(를) 만들어야 합니다 ["허가"](#) 암호화를 관리하는 IAM 역할에 사용되는 AWS KMS 키의 경우 IAM 역할에는 다음 작업을 허용하는 정책이 포함되어야 합니다.
  - DescribeKey
  - Encrypt
  - Decrypt보조금을 생성하려면 을 참조하십시오 ["AWS 문서"](#).
2. ["적절한 IAM 역할에 정책을 추가합니다."](#) 이 정책은 을 지원해야 합니다 DescribeKey, Encrypt, 및 Decrypt 운영:

Cloud Volumes ONTAP

1. Cloud Volumes ONTAP 환경으로 전환하십시오.

2. 고급 권한 레벨로 전환합니다.

```
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 입력합니다.

5. AWS KMS가 올바르게 구성되었는지 확인합니다.

```
security key-manager external aws show -vserver svm_name
```

## 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.

시작하기 전에

- Cloud Volumes ONTAP에서 버전 9.10.1 이상을 실행해야 합니다
- 설치된 볼륨 암호화(VE) 라이선스(NetApp 볼륨 암호화 라이선스는 NetApp Support에 등록된 각 Cloud Volumes ONTAP 시스템에 자동으로 설치됨)
- 멀티 테넌트 암호화 키 관리(MT\_EK\_MGMT) 라이선스가 있어야 합니다
- 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 작성합니다**을 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. Azure 키 저장소 앱 등록을 위한 Azure 포털에서 인증서 및 비밀 창을 선택합니다.
2. 새 클라이언트 암호\*\* 를 선택합니다. 클라이언트 비밀에 의미 있는 이름을 입력합니다. NetApp에서는 24개월의 만료 기간을 권장합니다. 단, 특정 클라우드 거버넌스 정책에는 다른 설정이 필요할 수 있습니다.
3. 클라이언트 암호를 만들려면 추가 를 클릭합니다. 값\*\* 옆에 나열된 암호 문자열을 복사하여 에서 나중에 사용할 수 있도록 안전한 위치에 저장합니다 [Cloud Volumes ONTAP 구성](#). 페이지를 벗어나 이동하면 암호 값이 다시 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. **+Create**를 클릭하고 리소스 그룹, 지역 및 가격 책정 계층을 포함한 필수 정보를 입력합니다. 또한, 삭제된 볼트를 보관할 일 수를 입력하고 키 볼트에서 삭제 보호 활성화를 선택합니다.
4. 액세스 정책을 선택하려면 다음 을 선택합니다.
5. 다음 옵션을 선택합니다.
  - a. **Access configuration** 아래에서 **Vault access policy**를 선택합니다.
  - b. 리소스 액세스 아래에서 볼륨 암호화를 위한 **Azure** 디스크 암호화 를 선택합니다.
6. 액세스 정책을 추가하려면 **+ Create** 를 선택합니다.
7. 템플릿에서 구성 아래에서 드롭다운 메뉴를 클릭한 다음 키, 암호 및 인증서 관리\*\* 템플릿을 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:20이 선택되었습니다
  - 비밀 권한:8 선택됨
  - 인증서 권한:16 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. 에서 만든 기본 Azure 등록 응용 프로그램을 선택하려면 다음 을 클릭합니다 [Azure 애플리케이션 등록](#). 다음\*\* 을 선택합니다.



정책당 하나의 보안 주기만 할당할 수 있습니다.

### Create an access policy

Permissions

Principal

Application (optional)

Review + create

Only 1 principal can be assigned per access policy.  
Use the new embedded experience to select a principal. The previous popup experience can be accessed here. [Select a principal](#)

Search by object ID, name, or email address

Selected item

No item selected

Previous

Next

10. 검토 후 작성 이 나타날 때까지 다음 을 두 번 클릭합니다. 그런 다음 만들기 를 클릭합니다.
11. 다음 을 선택하여 네트워킹 옵션으로 진행합니다.
12. 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.)
13. 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
- 사용: 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(HA만 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 메뉴에서 다음을 선택합니다.
  - NET Framework 클래스 라이브러리 Control.OnEventArgs 클래스 참고: 이 속성은 .NET Framework 버전 2.0
  - **Microsoft.KeyVault**
  - **Microsoft.Storage**(선택 사항)



### SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ

3 selected

Service	Status	
Microsoft.Storage	Succeeded	
Microsoft.AzureActiveDirectory	Succeeded	
Microsoft.KeyVault	Succeeded	

Service endpoint policies

0 selected

### SUBNET DELEGATION

Delegate subnet to a service ⓘ

None

### NETWORK POLICY FOR PRIVATE ENDPOINTS

The network policy affects all private endpoints in this subnet. To use network security groups, application security groups, or user defined routes to control traffic going to a private endpoint, set the private endpoint network policy to enabled. [Learn more](#)

Private endpoint network policy

Disabled

Save

Cancel

6. 설정을 캡처하려면 저장을 선택합니다.

#### Cloud Volumes ONTAP 구성

1. 기본 SSH 클라이언트를 사용하여 클러스터 관리 LIF에 연결합니다.
2. ONTAP에서 고급 권한 모드로 들어갑니다.

```
set advanced -con off
```

3. 원하는 Data SVM을 식별하고 DNS 구성을 확인합니다.

```
vserver services name-service dns show
```

- 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. 이 값은 클러스터 관리자 SVM의 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 확인합니다.

```
vserver services name-service dns show
```

4. 응용 프로그램 등록 후 저장된 클라이언트 ID 및 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 Azure_key_vault_name -key-id  
Azure_key_ID
```

5. 키 관리자의 상태를 확인합니다.

```
security key-manager external azure check
```

출력은 다음과 같이 표시됩니다.

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

```
Vserver: data_svm_name
```

```
Node: akvlab01-01
```

```
Category: service_reachability
```

```
Status: OK
```

```
Category: ekvip_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.
```

를 누릅니다 service\_reachability 상태가 아닙니다 'OK' SVM은 필요한 모든 연결 및 사용 권한으로 Azure Key Vault 서비스에 연결할 수 없습니다. Azure 네트워크 정책 및 라우팅으로 인해 프라이빗 VNET가 Azure KeyVault Public 엔드포인트에 도달하지 못하도록 차단하지 않는지 확인합니다. 이러한 경우, VNET 내에서 키 볼트에 액세스하기 위해 Azure 프라이빗 끝점을 사용하는 것이 좋습니다. 또한 종점의 전용 IP 주소를 확인하기 위해 SVM에 정적 호스트 항목을 추가해야 할 수도 있습니다.

를 클릭합니다 kms\_wrapped\_key\_status 보고합니다 UNKNOWN 초기 구성 시 상태가 로 변경됩니다 OK 첫 번째 볼륨이 암호화된 후

6. 선택 사항: NVE의 기능을 확인하기 위한 테스트 볼륨을 생성합니다.

```
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.

7. 볼륨이 올바르게 생성되고 암호화되었는지 확인합니다. 있다면, 입니다 `-is-encrypted` 매개 변수는 로 표시됩니다 `true`.

```
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 SVM의 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.

시작하기 전에

- Cloud Volumes ONTAP에서 버전 9.10.1 이상을 실행해야 합니다
- VE(Volume Encryption) 라이선스가 설치되었습니다
- 멀티 테넌트 암호화 키 관리(MTEKM) 라이선스가 설치되어 있으며 Cloud Volumes ONTAP 9.12.1 GA부터 시작합니다.
- 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. 클라우드 KMS 키 및 Cloud Volumes ONTAP 서비스 계정에 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
```

4. 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. 기본 SSH 클라이언트를 사용하여 클러스터 관리 LIF에 연결합니다.

2. 고급 권한 레벨로 전환합니다.

```
set -privilege advanced
```

3. 데이터 SVM을 위한 DNS를 생성합니다.

```
dns create -domains c.<project>.internal -name-servers server_address -vserver
SVM_name
```

4. CMEK 항목 작성:

```
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 확인합니다.

```
security key-manager external gcp check -vserver svm_name
```

7. 선택 사항: 암호화를 테스트할 볼륨을 생성합니다
- ```
vol create volume_name -aggregate aggregate
-vserver vserver_name -size 10G
```

## 문제 해결

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

1. set 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. BlueXP를 사용하면 일반적인 랜섬웨어 파일 확장으로부터 보호하는 것과 자율적 랜섬웨어 방어(ARP)라는 두 가지 NetApp 솔루션을 랜섬웨어용 구현할 수 있습니다. 이러한 솔루션은 가시성, 감지, 문제 해결을 위한 효과적인 툴을 제공합니다.

## 일반적인 랜섬웨어 파일 확장명으로부터 보호

BlueXP를 통해 제공되는 랜섬웨어 방어 설정에서 ONTAP FPolicy 기능을 활용하여 일반적인 랜섬웨어 파일 확장 유형을 방지할 수 있습니다.

단계

1. Canvas 페이지에서 랜섬웨어 보호를 구성하는 시스템의 이름을 두 번 클릭합니다.
2. 개요 탭에서 기능 패널을 클릭한 다음 \* 랜섬웨어 보호 \* 옆에 있는 연필 아이콘을 클릭합니다.

| Information              |                            | Features                                                                              |
|--------------------------|----------------------------|---------------------------------------------------------------------------------------|
| Working Environment Tags | Tags                       |    |
| Scheduled Downtime       | Off                        |    |
| S3 Storage Classes       | Standard-Infrequent Access |    |
| Instance Type            | m5.xlarge                  |    |
| Write Speed              | Normal                     |  |
| Ransomware Protection    | Off                        |  |
| Support Registration     | Not Registered             |  |
| CIFs Setup               |                            |  |

3. 랜섬웨어에 대한 NetApp 솔루션 구현:

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



Cloud Volumes ONTAP에서 FPolicy를 활성화하면 BlueXP에서 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.

### Ransomware Protection

Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution for ransomware provides effective tools for visibility, detection, and remediation. [Learn More](#)

#### 1 Enable Snapshot Copy Protection

50 %  
Protection

1 Volumes without a Snapshot Policy

To protect your data, activate the default Snapshot policy for these volumes

Activate Snapshot Policy

#### 2 Block Ransomware File Extensions

ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.

[View Denied File Names](#)

Activate FPolicy

## 자율 랜섬웨어 보호

Cloud Volumes ONTAP는 워크로드 분석을 수행하여 랜섬웨어 공격을 나타낼 수 있는 비정상적인 활동을 사전에 감지하고 경고하는 ARP(Autonomous 랜섬웨어 Protection) 기능을 지원합니다.

를 통해 제공되는 파일 확장자 보호와 분리됩니다 "랜섬웨어 차단 설정"ARP 기능은 워크로드 분석을 사용하여 감지된 "비정상적인 활동"을 기반으로 잠재적인 공격에 대해 사용자에게 경고합니다. 랜섬웨어 차단 설정과 ARP 기능을 모두 포괄적인 랜섬웨어 방어에 함께 사용할 수 있습니다.

ARP 기능은 노드 기반 및 용량 기반 라이선스 모델 모두에서 BYOL 라이선스(1년, 2년, 3년 조건)에만 사용할 수 있습니다. Cloud Volumes ONTAP의 ARP 기능과 함께 사용하기 위해 별도의 새 애드온 라이선스를 구입하려면 NetApp 영업 담당자에게 문의해야 합니다.

추가 라이선스를 구입하여 디지털 지갑에 추가하면 Cloud Volumes ONTAP를 사용하여 볼륨별로 ARP를 활성화할 수 있습니다. 볼륨에 대한 ARP 구성은 ONTAP 시스템 관리자 및 ONTAP CLI를 통해 수행됩니다.

ONTAP 시스템 관리자 및 CLI에서 ARP를 활성화하는 방법에 대한 자세한 내용은 를 참조하십시오 "자율주행 랜섬웨어 보호 활성화".



라이센스가 없는 경우 라이선스가 부여된 기능을 사용할 수 없습니다.

## Autonomous Ransomware Protection

**0** TiB

Protected Capacity

**100** TiB

Precommitted capacity

**0** TiB

PAYGO

BYOL

**100 TiB**

Marketplace Contracts **0 TiB**



## 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 라이선스와 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 라이선스도 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 라이선스를 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 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

## 상표 정보

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