외부 키 관리를 구성합니다
ONTAP 9

NetApp
February 12, 2026

목차

외부 키 관리를 구성합니다

ONTAP NetApp Volume Encryption을 사용하여 외부 키 관리 구성에 대해 알아보세요.

하나 이상의 외부 키 관리 서버를 사용하여 클러스터가 암호화된 데이터에 액세스하는 데 사용하는 키를 보호할 수 있습니다. 외부 키 관리 서버는 키 관리 상호 운용성 프로토콜(KMIP)을 사용하여 노드에 키를 제공하는 스토리지 환경의 타사 시스템입니다. ONTAP Onboard Key Manager 외에도 여러 외부 키 관리 서버를 지원합니다.

ONTAP 9.10.1부터 다음을 사용할 수 있습니다. Azure Key Vault 또는 Google Cloud Key Manager 서비스 데이터 SVM에 대한 NVE 키를 보호합니다. ONTAP 9.11.1부터 클러스터에서 여러 개의 외부 키 관리자를 구성할 수 있습니다. 보다클러스터형 키 서버 구성 . ONTAP 9.12.0부터 다음을 사용할 수 있습니다. "AWS의 KMS" 데이터 SVM에 대한 NVE 키를 보호합니다. ONTAP 9.17.1부터 OpenStack을 사용할 수 있습니다. 바비칸 KMS 데이터 SVM에 대한 NVE 키를 보호합니다.

ONTAP System Manager를 사용하여 외부 키 관리자를 관리하세요

ONTAP 9.7부터 온보드 키 관리자를 사용하여 인증 및 암호화 키를 저장하고 관리할 수 있습니다. ONTAP 9.13.1부터는 외부 키 관리자를 사용하여 이러한 키를 저장하고 관리할 수도 있습니다.

Onboard Key Manager는 클러스터 내부의 보안 데이터베이스에 키를 저장하고 관리합니다. 범위는 클러스터입니다. 외부 키 관리자는 클러스터 외부에 키를 저장하고 관리합니다. 범위는 클러스터 또는 스토리지 VM일 수 있습니다. 하나 이상의 외부 키 관리자를 사용할 수 있습니다. 다음 조건이 적용됩니다.

- Onboard Key Manager가 활성화된 경우 클러스터 수준에서 외부 키 관리자를 활성화할 수 없지만 스토리지 VM 수준에서 설정할 수 있습니다.
- 외부 키 관리자가 클러스터 레벨에서 활성화된 경우 Onboard Key Manager를 활성화할 수 없습니다.

외부 키 관리자를 사용하는 경우 스토리지 VM 및 클러스터당 최대 4개의 기본 키 서버를 등록할 수 있습니다. 각 기본 키 서버는 최대 3개의 보조 키 서버로 클러스터링할 수 있습니다.

외부 키 관리자를 구성합니다

스토리지 VM에 대한 외부 키 관리자를 추가하려면 스토리지 VM에 대한 네트워크 인터페이스를 구성할 때 선택적 게이트웨이를 추가해야 합니다. 스토리지 VM이 네트워크 경로 없이 생성된 경우 외부 키 관리자에 대한 라우트를 명시적으로 생성해야 합니다. 을 참조하십시오 "LIF(네트워크 인터페이스) 생성".

단계

System Manager의 다양한 위치에서 외부 키 관리자를 구성할 수 있습니다.

1. 외부 키 관리자를 구성하려면 다음 시작 단계 중 하나를 수행합니다.

워크플로우	내비게이션	시작 단계

키 관리자를 구성합니다	• 클러스터 * > * 설정 * 을 선택합니다	보안 * 섹션으로 스크롤합니다. Encryption * 에서 을 선택합니다 . 외부 키 관리자 * 를 선택합니다.
로컬 계층을 추가합니다	• 스토리지 * > * 계층 *	Add Local Tier * 를 선택합니다. "키 관리자 구성" 확인란을 선택합니다. 외부 키 관리자 * 를 선택합니다.
스토리지를 준비합니다	• 대시보드 *	Capacity * 섹션에서 * Prepare Storage * 를 선택합니다. 그런 다음 "키 관리자 구성"을 선택합니다. 외부 키 관리자 * 를 선택합니다.
암호화 구성(스토리지 VM 범위의 키 관리자만 해당)	스토리지 * > * 스토리지 VM *	스토리지 VM을 선택합니다. 설정 * 탭을 선택합니다. 보안 * 아래의 * 암호화 * 섹션에서 을 선택합니다 .

2. 기본 키 서버를 추가하려면 + Add * IP 주소 또는 호스트 이름 * 및 * 포트 * 필드를 선택하고 입력합니다.
3. 기존에 설치된 인증서가 * KMIP Server CA Certificates * 및 * KMIP Client Certificate * 필드에 나열됩니다. 다음 작업 중 하나를 수행할 수 있습니다.
   - 키 관리자에 매핑할 설치된 인증서를 선택하려면 선택합니다 . (여러 서비스 CA 인증서를 선택할 수 있지만 하나의 클라이언트 인증서만 선택할 수 있습니다.)
   - 아직 설치되지 않은 인증서를 추가하고 외부 키 관리자에 매핑하려면 * 새 인증서 추가 * 를 선택합니다.
   - 외부 키 관리자에 매핑하지 않을 설치된 인증서를 삭제하려면 인증서 이름 옆에 있는 을 선택합니다 .
4. 보조 키 서버를 추가하려면 * 보조 키 서버 * 열에서 * 추가 * 를 선택하고 세부 정보를 제공합니다.
5. 구성을 완료하려면 * 저장 * 을 선택하십시오.

기존 외부 키 관리자를 편집합니다

외부 키 관리자를 이미 구성한 경우 해당 설정을 수정할 수 있습니다.

단계

1. 외부 키 관리자 구성을 편집하려면 다음 시작 단계 중 하나를 수행합니다.

범위	내비게이션	시작 단계
클러스터 범위 외부 키 관리자	• 클러스터 * > * 설정 * 을 선택합니다	보안 * 섹션으로 스크롤합니다. Encryption * 에서 를 선택한 다음 * Edit External Key Manager * 를 선택합니다.
스토리지 VM 범위 외부 키 관리자	스토리지 * > * 스토리지 VM *	스토리지 VM을 선택합니다. 설정 * 탭을 선택합니다. 보안 * 아래의 * 암호화 * 섹션에서 * 외부 키 관리자 편집 * 을 선택합니다.

2. 기존 키 서버가 * Key Servers * 표에 나열되어 있습니다. 다음 작업을 수행할 수 있습니다.
   - 를 선택하여 새 키 서버를 추가합니다 + Add .
   - 키 서버의 이름이 들어 있는 표 셀의 끝에서 를 선택하여 키 서버를 삭제합니다. 해당 기본 키 서버와 연결된 보조 키 서버도 구성에서 제거됩니다.

외부 키 관리자를 삭제합니다

볼륨이 암호화되지 않은 경우 외부 키 관리자를 삭제할 수 있습니다.

단계

1. 외부 키 관리자를 삭제하려면 다음 단계 중 하나를 수행합니다.

범위	내비게이션	시작 단계
클러스터 범위 외부 키 관리자	• 클러스터 * > * 설정 * 을 선택합니다	보안 * 섹션으로 스크롤합니다. Encryption * 에서 select를 ⋮선택한 다음 * Delete External Key Manager * 를 선택합니다.
스토리지 VM 범위 외부 키 관리자	스토리지 * > * 스토리지 VM *	스토리지 VM을 선택합니다. 설정 * 탭을 선택합니다. 보안 * 아래의 * 암호화 * 섹션에서 를 ⋮선택한 다음 * 외부 키 관리자 삭제 * 를 선택합니다.

키 관리자 간에 키를 마이그레이션합니다

클러스터에서 여러 키 관리자가 활성화된 경우 키를 한 키 관리자에서 다른 키 관리자로 마이그레이션해야 합니다. 이 프로세스는 System Manager에서 자동으로 완료됩니다.

- Onboard Key Manager 또는 외부 키 관리자가 클러스터 수준에서 활성화되어 있고 일부 볼륨이 암호화된 경우 그런 다음 스토리지 VM 수준에서 외부 키 관리자를 구성할 때 클러스터 수준에서 Onboard Key Manager 또는 외부 키 관리자에서 스토리지 VM 수준의 외부 키 관리자로 키를 마이그레이션해야 합니다. 이 프로세스는 System Manager에서 자동으로 완료됩니다.
- 스토리지 VM에서 암호화 없이 볼륨을 생성한 경우 키를 마이그레이션할 필요가 없습니다.

ONTAP 클러스터에 SSL 인증서 설치

클러스터와 KMIP 서버는 KMIP SSL 인증서를 사용하여 서로의 ID를 확인하고 SSL 연결을 설정합니다. KMIP 서버와의 SSL 연결을 구성하기 전에, 클러스터에 대한 KMIP 클라이언트 SSL 인증서와 KMIP 서버의 루트 인증 기관(CA)에 대한 SSL 공용 인증서를 설치해야 합니다.

이 작업에 대해

HA 쌍에서는 두 노드가 동일한 퍼블릭 및 프라이빗 KMIP SSL 인증서를 사용해야 합니다. 동일한 KMIP 서버에 여러 HA 쌍을 연결하는 경우, HA 쌍의 모든 노드는 동일한 공용 및 전용 KMIP SSL 인증서를 사용해야 합니다.

시작하기 전에

- 서버에서 시간을 동기화하여 인증서, KMIP 서버 및 클러스터를 생성해야 합니다.
- 클러스터를 위한 공용 SSL KMIP 클라이언트 인증서를 얻어야 합니다.
- 클러스터를 위한 SSL KMIP 클라이언트 인증서와 관련된 개인 키를 얻어야 합니다.
- SSL KMIP 클라이언트 인증서는 암호로 보호되어 있지 않아야 합니다.
- KMIP 서버의 루트 CA(인증 기관)에 대한 SSL 공용 인증서를 얻어야 합니다.
- MetroCluster 환경에서는 두 클러스터 모두에 동일한 KMIP SSL 인증서를 설치해야 합니다.

클러스터에 인증서를 설치하기 전이나 후에 KMIP 서버에 클라이언트 및 서버 인증서를 설치할 수 있습니다.

단계

1. 클러스터에 SSL KMIP 클라이언트 인증서를 설치합니다.

   'Security certificate install - vserver admin_svm_name -type client'

   SSL KMIP 공용 및 개인 인증서를 입력하라는 메시지가 표시됩니다.

   'cluster1::> security certificate install -vserver cluster1-type client'

2. KMIP 서버의 루트 CA(인증 기관)에 대한 SSL 공용 인증서를 설치합니다.

   'Security certificate install - vserver admin_svm_name -type server-ca'

   'cluster1::> security certificate install -vserver cluster1-type server-ca'를 입력합니다

관련 정보

- "보안 인증서 설치"

ONTAP 9.6 이상에서 NVE에 대한 외부 키 관리 활성화

KMIP 서버를 사용하여 클러스터가 암호화된 데이터에 액세스하는 데 사용하는 키를 보호합니다. ONTAP 9.6부터 데이터 SVM이 암호화된 데이터에 액세스하는 데 사용하는 키를 보호하기 위해 별도의 외부 키 관리자를 구성하는 옵션이 제공됩니다.

ONTAP 9.11.1부터 기본 키 서버당 최대 3개의 보조 키 서버를 추가하여 클러스터된 키 서버를 생성할 수 있습니다. 자세한 내용은 을 참조하십시오 클러스터링된 외부 키 서버를 구성합니다.

이 작업에 대해

최대 4개의 KMIP 서버를 클러스터나 SVM에 연결할 수 있습니다. 중복성과 재해 복구를 위해 최소 두 개의 서버를 사용하세요.

외부 키 관리 범위에 따라 주요 관리 서버가 클러스터의 모든 SVM을 보호할지 또는 선택한 SVM에만 안전할지 여부가 결정됩니다.

- 클러스터 범위 _ 를 사용하여 클러스터의 모든 SVM에 대한 외부 키 관리를 구성할 수 있습니다. 클러스터 관리자는 서버에 저장된 모든 키에 액세스할 수 있습니다.
- ONTAP 9.6부터는 _SVM SCOPE_를 사용하여 클러스터의 데이터 SVM을 위한 외부 키 관리를 구성할 수 있습니다. 이는 각 테넌트가 서로 다른 SVM(또는 SVM 세트)을 사용하여 데이터를 제공하는 멀티테넌트 환경에 가장 적합합니다. 지정된 테넌트의 SVM 관리자만 해당 테넌트의 키에 액세스할 수 있습니다.
- 멀티테넌트 환경의 경우 다음 명령을 사용하여 _MT_EK_MGMT_에 대한 라이센스를 설치합니다.

  'System license add-license-code <MT_EK_MGMT license code>'

  에 대한 자세한 내용은 `system license add` "ONTAP 명령 참조입니다"을 참조하십시오.

동일한 클러스터에서 두 범위를 모두 사용할 수 있습니다. SVM용으로 키 관리 서버를 구성한 경우 ONTAP에서는 이러한 서버만 사용하여 키를 보호합니다. 그렇지 않으면 ONTAP는 클러스터에 구성된 키 관리 서버로 키를 보호합니다.

클러스터 범위에서 온보드 키 관리를 구성하고 SVM 범위에서 외부 키 관리를 구성할 수 있습니다. 'Security key-manager key migrate' 명령을 사용하여 클러스터 범위의 온보드 키 관리에서 SVM 범위의 외부 키 관리자로 키를 마이그레이션할 수 있습니다.

에 대한 자세한 내용은 `security key-manager key migrate` "ONTAP 명령 참조입니다"을 참조하십시오.

시작하기 전에

- KMIP SSL 클라이언트 및 서버 인증서를 설치해야 합니다.
- KMIP 서버는 각 노드의 노드 관리 LIF에서 접근 가능해야 합니다.
- 이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.
- MetroCluster 환경에서:
  - 외부 키 관리를 활성화하기 전에 MetroCluster 완전히 구성해야 합니다.
  - 두 클러스터에 동일한 KMIP SSL 인증서를 설치해야 합니다.
  - 두 클러스터 모두에 외부 키 관리자를 구성해야 합니다.

단계

1. 클러스터의 Key Manager 접속 구성:

   'Security key-manager external enable - vserver admin_SVM-key-servers host_name | ip_address: port,… -client-cert client_certificate-server-ca-cert server_CA_certificates'를 참조하십시오

   > 그만큼 `security key-manager external enable` 명령은 다음을 대체합니다. `security key-manager setup` 명령. 클러스터 로그인 프롬프트에서 명령을 실행하면, *`admin_SVM`* 현재 클러스터의 관리 SVM으로 기본 설정됩니다. 당신은 실행할 수 있습니다 `security key-manager external modify` 외부 키 관리 구성을 변경하는 명령입니다.

   다음 명령을 실행하면 외부 키 서버가 3개인 'cluster1'에 대한 외부 키 관리가 활성화됩니다. 첫 번째 키 서버는 호스트 이름과 포트를 사용하여 지정되고, 두 번째 키는 IP 주소와 기본 포트를 사용하여 지정되며, 세 번째 키는 IPv6 주소와 포트를 사용하여 지정됩니다.

   ```
   clusterl::> security key-manager external enable -vserver cluster1 -key
   -servers
   ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
   -client-cert AdminVserverClientCert -server-ca-certs
   AdminVserverServerCaCert
   ```

2. SVM을 위한 키 관리자 구성:

   'Security key-manager external enable - vserver SVM-key-servers host_name | ip_address: port,… -client -cert client_certificate-server-ca-cert server_CA_certificates'를 참조하십시오

- SVM 로그인 프롬프트에서 명령을 실행하면, SVM 현재 SVM을 기본값으로 사용합니다. 당신은 실행할 수 있습니다 `security key-manager external modify` 외부 키 관리 구성을 변경하는 명령입니다.
- MetroCluster 환경에서 데이터 SVM을 위한 외부 키 관리를 구성하는 경우 를 반복할 필요가 없습니다 `security key-manager external enable` 명령을 파트너 클러스터에 표시합니다.

다음 명령을 실행하면 기본 포트 5696에서 단일 키 서버가 수신 대기하는 'vm1'에 대한 외부 키 관리가 활성화됩니다.

```
svm1l::> security key-manager external enable -vserver svm1 -key-servers
keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs
SVM1ServerCaCert
```

3. 추가 SVM에 대해 마지막 단계를 반복합니다.

명령을 사용하여 추가 SVM을 구성할 수도 있습니다 `security key-manager external add-servers`. `security key-manager external add-servers`명령이 `security key-manager add` 명령을 대체합니다. 에 대한 자세한 내용은 `security key-manager external add-servers` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 구성된 모든 KMIP 서버가 연결되어 있는지 확인합니다.

'Security key-manager external show-status-node node_name'입니다

`security key-manager external show-status`명령이 `security key-manager show -status` 명령을 대체합니다. 에 대한 자세한 내용은 `security key-manager external show-status` link:https://docs.netapp.com/us-en/ontap-cli/security-key-manager-external-show-status.html["ONTAP 명령 참조입니다"^]을 참조하십시오.

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                        Status
----  -------  ------------------------------------
-------------
node1
      svm1
               keyserver.svm1.com:5696                           available
      cluster1
               10.0.0.10:5696                                    available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234      available
               ks1.local:15696                                   available
node2
      svm1
               keyserver.svm1.com:5696                           available
      cluster1
               10.0.0.10:5696                                    available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234      available
               ks1.local:15696                                   available

8 entries were displayed.
```

5. 필요한 경우 일반 텍스트 볼륨을 암호화된 볼륨으로 변환합니다.

   `volume encryption conversion start`

   볼륨을 변환하기 전에 외부 키 관리자를 완전히 구성해야 합니다.

관련 정보

- 클러스터링된 외부 키 서버를 구성합니다
- "시스템 라이센스 추가"
- "보안 키 관리자 키 마이그레이션"
- "보안 키 관리자 외부 추가 서버"
- "보안 키 관리자 외부 상태 표시"

ONTAP 9.5 및 이전 버전에서 NVE에 대한 외부 키 관리 활성화

하나 이상의 KMIP 서버를 사용하여 클러스터에서 암호화된 데이터에 액세스하는 데 사용하는 키를 보호할 수 있습니다. 하나의 노드에 KMIP 서버를 최대 4개까지 연결할 수 있습니다. 이중화 및 재해 복구를 위해 최소 2대의 서버를 사용하는 것이 좋습니다.

이 작업에 대해

ONTAP는 클러스터의 모든 노드에 대해 KMIP 서버 연결을 구성합니다.

시작하기 전에

- KMIP SSL 클라이언트 및 서버 인증서를 설치해야 합니다.
- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 외부 키 관리자를 구성하기 전에 MetroCluster 환경을 구성해야 합니다.
- MetroCluster 환경에서는 두 클러스터에 동일한 KMIP SSL 인증서를 설치해야 합니다.

단계

1. 클러스터 노드에 대한 Key Manager 접속 구성:

   보안 키 관리자 설정

   키 관리자 설정이 시작됩니다.

   > MetroCluster 환경에서는 두 클러스터에서 모두 이 명령을 실행해야 합니다. 자세히 알아보세요 `security key-manager setup` 에서"ONTAP 명령 참조입니다" .

2. 각 프롬프트에 적절한 응답을 입력합니다.
3. KMIP 서버 추가:

   'Security key-manager add-address key_management_server_ipaddress

   ```
   clusterl::> security key-manager add -address 20.1.1.1
   ```

   > MetroCluster 환경에서는 두 클러스터 모두에서 이 명령을 실행해야 합니다.

4. 이중화를 위해 KMIP 서버를 추가로 추가합니다.

   'Security key-manager add-address key_management_server_ipaddress

   ```
   clusterl::> security key-manager add -address 20.1.1.2
   ```

   > MetroCluster 환경에서는 두 클러스터 모두에서 이 명령을 실행해야 합니다.

5. 구성된 모든 KMIP 서버가 연결되어 있는지 확인합니다.

   보안 키 관리자 표시 상태

   이 절차에 설명된 명령에 대해 자세히 알아보세요."ONTAP 명령 참조입니다" .

```
cluster1::> security key-manager show -status

Node            Port      Registered Key Manager  Status
--------------  ----      ----------------------  ---------------
cluster1-01     5696      20.1.1.1                available
cluster1-01     5696      20.1.1.2                available
cluster1-02     5696      20.1.1.1                available
cluster1-02     5696      20.1.1.2                available
```

6. 필요한 경우 일반 텍스트 볼륨을 암호화된 볼륨으로 변환합니다.

   ```
   volume encryption conversion start
   ```

   볼륨을 변환하기 전에 외부 키 관리자를 완전히 구성해야 합니다. MetroCluster 환경에서는 외부 키 관리자를 두 사이트에 모두 구성해야 합니다.

클라우드 공급자와 함께 ONTAP 데이터 SVM에 대한 NVE 키 관리

ONTAP 9.10.1부터 클라우드 호스팅 응용 프로그램에서 및 를 "Google Cloud Platform의 키 관리 서비스(Cloud KMS)"사용하여 ONTAP 암호화 키를 보호할 수 "Azure 키 저장소(AKV)"있습니다. ONTAP 9.12.0부터, 로 NVE 키를 보호할 수도 "AWS의 KMS"있습니다.

AWS KMS, AKV 및 Cloud KMS를 사용하여 보호할 수 있습니다 "NVE(NetApp Volume Encryption) 키" 데이터 SVM에만 해당.

이 작업에 대해

클라우드 공급자를 사용한 키 관리는 CLI 또는 ONTAP REST API를 사용하여 설정할 수 있습니다.

클라우드 공급자를 사용하여 키를 보호할 때는 기본적으로 데이터 SVM LIF가 클라우드 키 관리 엔드포인트와 통신하는 데 사용됩니다. 노드 관리 네트워크는 클라우드 공급자의 인증 서비스(Azure의 경우 login.microsoftonline.com, Cloud KMS의 경우 oauth2.googleapis.com)와 통신하는 데 사용됩니다. 클러스터 네트워크가 올바르게 구성되지 않은 경우 클러스터에서 키 관리 서비스를 제대로 사용할 수 없습니다.

클라우드 공급자 키 관리 서비스를 사용할 때는 다음과 같은 제한 사항을 숙지해야 합니다.

- NSE(NetApp 스토리지 암호화) 및 NAE(NetApp 애그리게이트 암호화)에 클라우드 공급자 키 관리를 사용할 수 없습니다. "외부 KMIP" 대신 사용할 수 있습니다.
- MetroCluster 구성에서는 클라우드 공급자 키 관리를 사용할 수 없습니다.
- 클라우드 공급자 키 관리는 데이터 SVM에서만 구성할 수 있습니다.

시작하기 전에

- 해당 클라우드 공급자에 KMS를 구성해야 합니다.
- ONTAP 클러스터 노드는 NVE를 지원해야 합니다.
- "VE(Volume Encryption) 및 MTEKM(Multi-tenant Encryption Key Management) 라이센스를 설치해야 합니다".. 이 라이선스는 에 "ONTAP 1 을 참조하십시오"포함되어 있습니다.

- 클러스터 또는 SVM 관리자여야 합니다.
- 데이터 SVM에는 암호화된 볼륨이 포함되어 있지 않아야 하며 키 관리자를 사용해야 합니다. 데이터 SVM에 암호화된 볼륨이 포함된 경우 KMS를 구성하기 전에 해당 볼륨을 마이그레이션해야 합니다.

외부 키 관리를 활성화합니다

외부 키 관리를 사용하는 방법은 사용하는 특정 키 관리자에 따라 다릅니다. 해당 키 관리자 및 환경의 탭을 선택합니다.

설치하고

시작하기 전에

- 암호화를 관리하는 IAM 역할이 사용할 AWS KMS 키에 대한 권한을 만들어야 합니다. IAM 역할에는 다음 작업을 허용하는 정책이 포함되어야 합니다.
  - `DescribeKey`
  - `Encrypt`
  - `Decrypt` 를 누릅니다 자세한 내용은 의 AWS 설명서를 참조하십시오 "보조금".

ONTAP SVM에서 **AWS KMV**를 활성화합니다

1. 시작하기 전에 AWS KMS에서 액세스 키 ID와 비밀 키를 모두 받으십시오.
2. 권한 수준을 고급으로 설정합니다. `set -priv advanced`
3. AWS KMS 활성화: `security key-manager external aws enable -vserver` *`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`*

   에 대한 자세한 내용은 `security key-manager external aws` "ONTAP 명령 참조입니다"을 참조하십시오.

Azure를 지원합니다

ONTAP SVM에서 **Azure Key Vault**를 활성화합니다

1. 시작하기 전에 Azure 계정에서 클라이언트 암호 또는 인증서로 적절한 인증 자격 증명을 얻어야 합니다. 또한 클러스터의 모든 노드가 정상 상태인지 확인해야 합니다. 명령을 사용하여 확인할 수 `cluster show` 있습니다. 에 대한 자세한 내용은 `cluster show` "ONTAP 명령 참조입니다"을 참조하십시오.
2. 권한 수준을 Advanced'et-priv advanced로 설정합니다
3. SVM의 보안 키 관리자 외부 Azure ENABLE - CLIENT-id_client_id_-tenant-id_tenant_id_-name-key-id_id_-authentication-method {certificate|client-secret} 에서 AKV를 활성화합니다. 메시지가 나타나면 Azure 계정에서 클라이언트 인증서 또는 클라이언트 암호를 입력합니다.
4. AKV가 올바르게 활성화되었는지 확인합니다. `security key-manager external azure show vserver` *`svm_name`* 서비스 상태가 양호하지 않은 경우 데이터 SVM LIF를 통해 AKV 키 관리 서비스에 대한 연결을 설정합니다.

   에 대한 자세한 내용은 `security key-manager external azure` "ONTAP 명령 참조입니다"을 참조하십시오.

Google 클라우드

ONTAP SVM에서 클라우드 **KMS** 지원

1. 시작하기 전에 JSON 형식으로 Google Cloud KMS 계정 키 파일의 개인 키를 받으십시오. GCP 계정에서 찾을 수 있습니다. 또한 클러스터의 모든 노드가 정상 상태인지 확인해야 합니다. 명령을 사용하여 확인할 수 `cluster show` 있습니다. 에 대한 자세한 내용은 `cluster show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 권한 수준을 고급으로 설정: `set -priv advanced`
3. SVM에서 Cloud KMS 사용 `security key-manager external gcp enable -vserver *svm_name* -project-id *project_id*-key-ring-name *key_ring_name* -key-ring -location *key_ring_location* -key-name *key_name*` 메시지가 표시되면 서비스 계정 개인 키로 JSON 파일의 내용을 입력합니다
4. Cloud KMS가 올바른 매개변수로 구성되었는지 확인하세요. `security key-manager external gcp show vserver *svm_name*` 의 상태 `kms_wrapped_key_status` 될 것이다 `"UNKNOWN"` 암호화된 볼륨이 생성되지 않은 경우. 서비스 도달성이 적절하지 않은 경우 데이터 SVM LIF를 통해 GCP 키 관리 서비스에 대한 연결을 설정합니다.

   에 대한 자세한 내용은 `security key-manager external gcp` "ONTAP 명령 참조입니다"을 참조하십시오.

하나 이상의 암호화된 볼륨이 데이터 SVM용으로 이미 구성되어 있고 admin SVM 온보드 키 관리자가 해당 NVE 키를 관리하는 경우 이러한 키를 외부 키 관리 서비스로 마이그레이션해야 합니다. CLI에서 이 작업을 수행하려면 다음 명령을 실행합니다. `security key-manager key migrate -from-Vserver *admin_SVM* -to-Vserver *data_SVM*`데이터 SVM의 모든 NVE 키가 성공적으로 마이그레이션될 때까지 테넌트의 데이터 SVM에 대해 암호화된 새 볼륨을 생성할 수 없습니다.

관련 정보

- "Cloud Volumes ONTAP용 NetApp 암호화 솔루션으로 볼륨 암호화"
- "보안 키 관리자 외부"

Barbican KMS로 ONTAP 키 관리

ONTAP 9.17.1부터 OpenStack을 사용할 수 있습니다. "바비칸 KMS" ONTAP 암호화 키를 보호하기 위해. Barbican KMS는 키를 안전하게 저장하고 액세스하는 서비스입니다. Barbican KMS는 데이터 SVM의 NetApp 볼륨 암호화(NVE) 키를 보호하는 데 사용할 수 있습니다. Barbican은 다음을 사용합니다. "오픈스택 Keystone" 인증을 위한 OpenStack의 ID 서비스입니다.

이 작업에 대해

CLI 또는 ONTAP REST API를 사용하여 Barbican KMS에서 키 관리를 구성할 수 있습니다. 9.17.1 릴리스에서는 Barbican KMS 지원에 다음과 같은 제한 사항이 있습니다.

- Barbican KMS는 NetApp Storage Encryption(NSE) 및 NetApp Aggregate Encryption(NAE)을 지원하지 않습니다. 대신 다음을 사용할 수 있습니다. "외부 KMIP" 또는 "온보드 키 관리자(OKM)" NSE 및 NVE 키의 경우.
- Barbican KMS는 MetroCluster 구성에서 지원되지 않습니다.
- Barbican KMS는 데이터 SVM에 대해서만 구성할 수 있습니다. 관리자 SVM에서는 사용할 수 없습니다.

달리 명시되지 않는 한, 관리자는 `admin` 권한 수준은 다음 절차를 수행할 수 있습니다.

시작하기 전에

- Barbican KMS와 OpenStack Keystone 구성해야 합니다. Barbican과 함께 사용하는 SVM은 Barbican 및 OpenStack Keystone 서버에 대한 네트워크 액세스 권한이 있어야 합니다.

- Barbican 및 OpenStack Keystone 서버에 사용자 지정 인증 기관(CA)을 사용하는 경우 CA 인증서를 설치해야 합니다. `security certificate install -type server-ca -vserver <admin_svm>` .

Barbican KMS 구성을 만들고 활성화합니다.

SVM에 대한 새로운 Barbican KMS 구성을 생성하고 활성화할 수 있습니다. SVM에는 비활성화된 Barbican KMS 구성이 여러 개 있을 수 있지만, 한 번에 하나만 활성화할 수 있습니다.

단계

1. SVM에 대한 새로운 비활성 Barbican KMS 구성을 만듭니다.

```
security key-manager external barbican create-config -vserver <svm_name>
-config-name <unique_config_name> -key-id <key_id> -keystone-url
<keystone_url> -application-cred-id
<keystone_applications_credentials_id>
```

   - `-key-id` Barbican 키 암호화 키(KEK)의 키 식별자입니다. 다음을 포함한 전체 URL을 입력하세요. `https://` .

> 일부 URL에는 물음표(?) 문자가 포함되어 있습니다. 물음표는 ONTAP 명령줄의 활성 도움말을 활성화합니다. 물음표가 있는 URL을 입력하려면 먼저 다음 명령을 사용하여 활성 도움말을 비활성화해야 합니다. `set -active-help false` . 활성 도움말은 나중에 다음 명령을 사용하여 다시 활성화할 수 있습니다. `set -active-help true` . 자세한 내용은 "ONTAP 명령 참조입니다" .

   - `-keystone-url` OpenStack Keystone 인증 호스트의 URL입니다. 다음을 포함한 전체 URL을 입력하세요. `https://` .
   - `-application-cred-id` 는 애플리케이션 자격 증명 ID입니다.

     이 명령을 입력하면 애플리케이션 자격 증명 비밀 키를 입력하라는 메시지가 표시됩니다. 이 명령은 비활성 Barbican KMS 구성을 생성합니다.

     다음 예제에서는 이름이 지정된 새 비활성 Barbican KMS 구성을 만듭니다. `config1` SVM의 경우 `svm1` :

```
cluster1::> security key-manager external barbican create-config
-vserver svm1 -config-name config1 -keystone-url
https://172.21.76.152:5000/v3 -application-cred-id app123 -key-id
https://172.21.76.153:9311/v1/secrets/<id_value>

Enter the Application Credentials Secret for authentication with
Keystone: <key_value>
```

2. 새로운 Barbican KMS 구성을 활성화하세요:

```
security key-manager keystore enable -vserver <svm_name> -config-name
<unique_config_name> -keystore barbican
```

이 명령을 사용하여 Barbican KMS 구성 간에 전환할 수 있습니다. SVM에 이미 활성화된 Barbican KMS 구성이 있는 경우, 해당 구성은 비활성화되고 새 구성이 활성화됩니다.

3. 새로운 Barbican KMS 구성이 활성화되었는지 확인하세요.

```
security key-manager external barbican check -vserver <svm_name> -node
<node_name>
```

이 명령은 SVM 또는 노드에서 활성 Barbican KMS 구성의 상태를 제공합니다. 예를 들어, SVM이 `svm1` 노드에서 `node1` 활성화된 Barbican KMS 구성이 있는 경우 다음 명령을 실행하면 해당 구성의 상태가 반환됩니다.

```
cluster1::> security key-manager external barbican check -node node1

Vserver: svm1
Node: node1

Category: service_reachability
              Status: OK

Category: kms_wrapped_key_status
              Status: OK
```

Barbican KMS 구성의 자격 증명 및 설정 업데이트

활성 또는 비활성 Barbican KMS 구성의 현재 설정을 보고 업데이트할 수 있습니다.

단계

1. SVM에 대한 현재 Barbican KMS 구성을 확인하세요.

```
security key-manager external barbican show -vserver <svm_name>
```

각 Barbican KMS 구성에 대한 키 ID, OpenStack Keystone URL 및 애플리케이션 자격 증명 ID가 SVM에 표시됩니다.

2. Barbican KMS 구성 설정을 업데이트합니다.

```
security key-manager external barbican update-config -vserver <svm_name>
-config-name <unique_config_name> -timeout <timeout> -verify
<true|false> -verify-host <true|false>
```

이 명령은 지정된 Barbican KMS 구성의 시간 초과 및 확인 설정을 업데이트합니다. `timeout` ONTAP Barbican의 응답을 기다리는 시간(초)을 결정합니다. 기본값은 `timeout` 10초입니다. `verify` 그리고 `verify-host` 연결하기 전에 Barbican 호스트의 ID와 호스트 이름을 각각 확인해야 하는지 여부를 결정합니다. 기본적으로 이러한 매개변수는 다음과 같이 설정됩니다. `true` . 그 `vserver` 그리고 `config-name` 매개변수는 필수입니다. 다른 매개변수는 선택 사항입니다.

3. 필요한 경우 활성 또는 비활성 Barbican KMS 구성의 자격 증명을 업데이트합니다.

```
security key-manager external barbican update-credentials -vserver
<svm_name> -config-name <unique_config_name> -application-cred-id
<keystone_applications_credentials_id>
```

이 명령을 입력하면 새로운 애플리케이션 자격 증명 비밀 키를 입력하라는 메시지가 표시됩니다.

4. 필요한 경우 활성 Barbican KMS 구성에 대해 누락된 SVM 키 암호화 키(KEK)를 복원합니다.
   a. 누락된 SVM KEK를 복원합니다. `security key-manager external barbican restore` :

```
security key-manager external barbican restore -vserver <svm_name>
```

이 명령은 Barbican 서버와 통신하여 활성 Barbican KMS 구성에 대한 SVM KEK를 복원합니다.

5. 필요한 경우 Barbican KMS 구성에 맞게 SVM KEK를 다시 키로 지정하세요.
   a. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

   b. SVM KEK를 다시 키로 지정 `security key-manager external barbican rekey-internal` :

```
security key-manager external barbican rekey-internal -vserver
<svm_name>
```

이 명령은 지정된 SVM에 대한 새로운 SVM KEK를 생성하고 볼륨 암호화 키를 새로운 SVM KEK로 다시 래핑합니다. 새로운 SVM KEK는 활성 Barbican KMS 구성으로 보호됩니다.

Barbican KMS와 Onboard Key Manager 간 키 마이그레이션

Barbican KMS에서 Onboard Key Manager(OKM)로 키를 마이그레이션할 수 있으며, 그 반대의 경우도 가능합니다. OKM에 대한 자세한 내용은 다음을 참조하세요. "ONTAP 9.6 이상에서 온보드 키 관리를 활성화합니다" .

단계

1. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

2. 필요한 경우 Barbican KMS에서 OKM으로 키를 마이그레이션합니다.

```
security key-manager key migrate -from-vserver <svm_name> -to-vserver
<admin_svm_name>
```

`svm_name` Barbican KMS 구성을 사용한 SVM의 이름입니다.

3. 필요한 경우 OKM에서 Barbican KMS로 키를 마이그레이션합니다.

```
security key-manager key migrate -from-vserver <admin_svm_name> -to
-vserver <svm_name>
```

Barbican KMS 구성 비활성화 및 삭제

암호화된 볼륨이 없는 활성 Barbican KMS 구성을 비활성화할 수 있으며, 비활성 Barbican KMS 구성을 삭제할 수 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

2. 활성 Barbican KMS 구성을 비활성화합니다.

```
security key-manager keystore disable -vserver <svm_name>
```

SVM에 NVE 암호화 볼륨이 있는 경우 해당 볼륨을 암호 해독해야 합니다. 키를 마이그레이션하다 Barbican KMS 구성을 비활성화하기 전에. 새로운 Barbican KMS 구성을 활성화할 때 NVE 볼륨을 복호화하거나 키를 마이그레이션할 필요는 없으며, 현재 활성화된 Barbican KMS 구성은 비활성화됩니다.

3. 비활성 Barbican KMS 구성을 삭제합니다.

```
security key-manager keystore delete -vserver <svm_name> -config-name
<unique_config_name> -type barbican
```