NetApp 하드웨어 기반 암호화를 구성합니다
ONTAP 9

NetApp
February 12, 2026

목차

NetApp 하드웨어 기반 암호화를 구성합니다

ONTAP 하드웨어 기반 암호화에 대해 알아보세요

NetApp 하드웨어 기반 암호화는 FDE(전체 디스크 암호화)가 쓰일 때 데이터를 지원합니다. 펌웨어에 저장된 암호화 키가 없으면 데이터를 읽을 수 없습니다. 암호화 키는 인증된 노드에서만 액세스할 수 있습니다.

NetApp 하드웨어 기반 암호화 이해

노드는 외부 키 관리 서버 또는 Onboard Key Manager에서 검색된 인증 키를 사용하여 자체 암호화 드라이브에 대해 자신을 인증합니다.

- 외부 키 관리 서버는 KMIP(Key Management Interoperability Protocol)를 사용하여 노드에 키를 제공하는 스토리지 환경의 타사 시스템입니다. 데이터와 다른 스토리지 시스템에 있는 외부 키 관리 서버를 구성하는 것이 가장 좋습니다.
- Onboard Key Manager는 데이터와 동일한 스토리지 시스템의 노드에 인증 키를 제공하는 기본 제공 도구입니다.

하드웨어 기반 암호화와 NetApp 볼륨 암호화를 사용하여 자체 암호화 드라이브에서 데이터를 "이중 암호화"할 수 있습니다.

자체 암호화 드라이브가 사용되면 코어 덤프도 암호화됩니다.

HA 쌍이 암호화 SAS 또는 NVMe 드라이브(SED, NSE, FIPS)를 사용 중인 경우 항목의 지침을 따라야 합니다 FIPS 드라이브 또는 SED를 보호되지 않는 모드로 되돌리는 중입니다 시스템을 초기화하기 전에 HA 쌍 내의 모든 드라이브(부팅 옵션 4 또는 9) 이렇게 하지 않을 경우 드라이브를 용도 변경할 경우 향후의 데이터 손실이 발생할 수 있습니다.

지원되는 자체 암호화 드라이브 유형입니다

다음과 같은 두 가지 유형의 자체 암호화 드라이브가 지원됩니다.

- 자체 암호화 FIPS 인증 SAS 또는 NVMe 드라이브가 모든 FAS 및 AFF 시스템에서 지원됩니다. FIPS 드라이브라고 하는 이러한 드라이브는 Federal Information Processing Standard Publication 140-2, 레벨 2의 요구 사항을 준수합니다. 인증된 기능을 통해 드라이브에 대한 서비스 거부 공격을 방지하는 것과 같은 암호화 외에도 보호 기능을 사용할 수 있습니다. FIPS 드라이브를 동일한 노드 또는 HA 쌍의 다른 유형의 드라이브와 혼합할 수 없습니다.
- ONTAP 9.6부터 FIPS 테스트를 거치지 않은 자체 암호화 NVMe 드라이브가 AFF A800, A320 이상 시스템에서 지원됩니다. SED_라고 하는 이러한 드라이브는 FIPS 드라이브와 동일한 암호화 기능을 제공하지만 동일한 노드 또는 HA 쌍의 비암호화 드라이브와 혼합될 수 있습니다.
- FIPS 검증을 거친 모든 드라이브는 FIPS 검증을 거친 펌웨어 암호화 모듈을 사용합니다. FIPS 드라이브 암호화 모듈은 드라이브 외부에서 생성된 키를 사용하지 않습니다(드라이브에 입력된 인증 암호는 드라이브의 펌웨어 암호화 모듈에서 키 암호화 키를 얻는 데 사용됩니다).

비암호화 드라이브는 SED 또는 FIPS 드라이브가 아닌 드라이브입니다.

Flash Cache 모듈이 있는 시스템에서 NSE를 사용하는 경우, NVE 또는 NAE도 활성화해야 합니다. NSE는 Flash Cache 모듈에 상주하는 데이터를 암호화하지 않습니다.

외부 키 관리 사용 시기

일반적으로 온보드 키 관리자를 사용하는 것이 더 저렴하고 더 편리하긴 하지만 다음 중 하나라도 해당하는 경우 외부 키 관리를 사용해야 합니다.

- 조직의 정책에는 FIPS 140-2 레벨 2(또는 그 이상) 암호화 모듈을 사용하는 키 관리 솔루션이 필요합니다.
- 암호화 키를 중앙 집중식으로 관리하는 다중 클러스터 솔루션이 필요합니다.
- 기업은 인증 키를 시스템 또는 데이터와 다른 위치에 저장하는 추가적인 보안을 필요로 합니다.

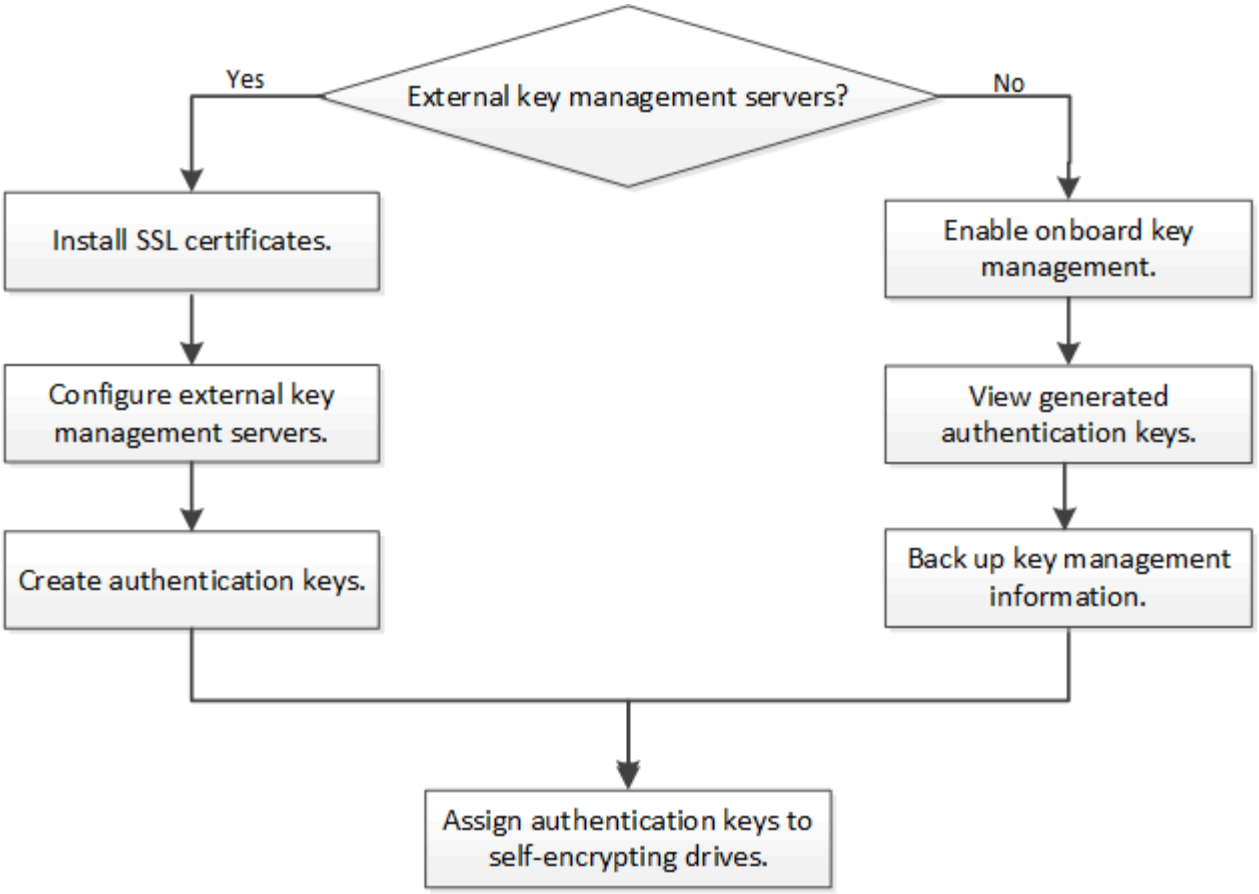
지원 세부 정보

다음 표에는 중요한 하드웨어 암호화 지원 세부 정보가 나와 있습니다. 지원되는 KMIP 서버, 스토리지 시스템 및 디스크 쉘프에 대한 최신 정보는 상호 운용성 매트릭스 를 참조하십시오.

리소스 또는 기능	지원 세부 정보
비동종 디스크 세트	• FIPS 드라이브를 동일한 노드 또는 HA 쌍의 다른 유형의 드라이브와 혼합할 수 없습니다. HA 쌍을 준수하는 것은 동일한 클러스터에서 규정을 준수하지 않는 HA 쌍과 공존할 수 있습니다. • SED는 동일한 노드 또는 HA 쌍에서 비암호화 드라이브와 혼합될 수 있습니다.
드라이브 유형입니다	• FIPS 드라이브는 SAS 또는 NVMe 드라이브가 될 수 있습니다. • SED는 NVMe 드라이브여야 합니다.
10Gb 네트워크 인터페이스	ONTAP 9.3부터 KMIP 키 관리 구성은 외부 키 관리 서버와의 통신을 위한 10Gb 네트워크 인터페이스를 지원합니다.
키 관리 서버와의 통신을 위한 포트	ONTAP 9.3부터는 모든 스토리지 컨트롤러 포트를 사용하여 키 관리 서버와 통신할 수 있습니다. 그렇지 않으면 키 관리 서버와 통신하기 위해 e0M 포트를 사용해야 합니다. 스토리지 컨트롤러 모델에 따라 부팅 프로세스 중에 키 관리 서버와 통신하기 위해 특정 네트워크 인터페이스를 사용하지 못할 수 있습니다.
MetroCluster(MCC)	• NVMe 드라이브는 MCC를 지원합니다. • SAS 드라이브는 MCC를 지원하지 않습니다.

하드웨어 기반 암호화 워크플로우

클러스터가 자체 암호화 드라이브에 인증하려면 키 관리 서비스를 구성해야 합니다. 외부 키 관리 서버 또는 온보드 키 관리자를 사용할 수 있습니다.



관련 정보

- "NetApp Hardware Universe를 참조하십시오"
- "NetApp 볼륨 암호화 및 NetApp 애그리게이트 암호화"

외부 키 관리를 구성합니다

ONTAP 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 KMIP(Key Management Interoperability Protocol)를 사용하여 노드에 키를 제공하는 스토리지 환경의 타사 시스템입니다.

온보드 키 관리자를 사용하여 NVE(NetApp Volume Encryption)를 구현할 수 있습니다. ONTAP 9.3 이상에서는 외부 키 관리(KMIP)와 온보드 키 관리자를 사용하여 NVE를 구현할 수 있습니다. ONTAP 9.11.1부터 클러스터에 여러 외부 키 관리자를 구성할 수 있습니다. 을 참조하십시오 클러스터링된 키 서버를 구성합니다.

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 하드웨어 기반 암호화를 위한 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.

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.

시작하기 전에

- KMIP SSL 클라이언트 및 서버 인증서를 설치해야 합니다.
- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- MetroCluster 환경에서:

- 외부 키 관리자를 구성하기 전에 MetroCluster 환경을 구성해야 합니다.
- 두 클러스터에 동일한 KMIP SSL 인증서를 설치해야 합니다.

단계

1. 클러스터의 Key Manager 접속 구성:

   "+ 보안 키 관리자 외부 활성화 - vserver admin_SVM-key-servers host_name | ip_address:port,… -client-cert client_certificate-server-ca-cert server_CA_certificates+'

   - `security key-manager external enable`명령이 `security key-manager setup` 명령을 대체합니다. 명령을 실행하여 외부 키 관리 구성을 변경할 수 `security key-manager external modify` 있습니다. 에 대한 자세한 내용은 `security key-manager external enable` "ONTAP 명령 참조입니다"을 참조하십시오.
   - MetroCluster 환경에서 관리 SVM에 대한 외부 키 관리를 구성하는 경우 를 반복해야 합니다 `security key-manager external enable` 명령을 파트너 클러스터에 표시합니다.

   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 -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. 구성된 모든 KMIP 서버가 연결되어 있는지 확인합니다.

   'Security key-manager external show-status-node_name-vserver SVM-key-server host_name|ip_address:port-key-server-status available|not-responding|unknown'

   `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
      cluster1
               10.0.0.10:5696                                    available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                   available
node2
      cluster1
               10.0.0.10:5696                                    available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                   available

6 entries were displayed.
```

관련 정보

- 클러스터링된 외부 키 서버를 구성합니다
- "보안 키 관리자 외부 활성화"
- "보안 키 관리자 외부 상태 표시"

ONTAP 9.5 및 이전 버전에서 하드웨어 기반 암호화를 위한 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.

ONTAP에서 클러스터된 외부 키 서버를 구성합니다

ONTAP 9.11.1부터 SVM에서 클러스터링된 외부 키 관리 서버에 대한 연결을 구성할 수 있습니다. 클러스터형 키 서버를 사용하면 SVM에서 기본 키 서버와 보조 키 서버를 지정할 수 있습니다. ONTAP 키를 등록하거나 검색할 때 먼저 기본 키 서버에 액세스를 시도한 후 작업이 성공적으로 완료될 때까지 순차적으로 보조 서버에 액세스를 시도합니다.

NetApp Storage Encryption(NSE), NetApp Volume Encryption(NVE), NetApp Aggregate Encryption(NAE) 키에 외부 키 서버를 사용할 수 있습니다. SVM은 최대 4개의 기본 외부 KMIP 서버를 지원할 수 있습니다. 각 기본 서버는 최대 3개의 보조 키 서버를 지원할 수 있습니다.

이 작업에 대해

- 이 프로세스는 KMIP를 사용하는 주요 서버만 지원합니다. 지원되는 키 서버 목록을 보려면 를 확인하십시오 "NetApp 상호 운용성 매트릭스 툴".

시작하기 전에

- "SVM에 대해 KMIP 키 관리를 활성화해야 합니다".
- 클러스터의 모든 노드에서 ONTAP 9.11.1 이상이 실행되고 있어야 합니다.
- 서버 목록의 순서는 다음과 같습니다. `-secondary-key-servers` 매개변수는 외부 키 관리(KMIP) 서버의 액세스 순서를 반영합니다.

클러스터링된 키 서버를 생성합니다

구성 절차는 기본 키 서버를 구성했는지 여부에 따라 달라집니다.

SVM에 **1**차 및 **2**차 키 서버를 추가합니다

단계

1. 클러스터(관리 SVM)에 대해 키 관리가 활성화되지 않았는지 확인하세요.

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

   SVM에 이미 최대 4개의 기본 키 서버가 활성화되어 있는 경우 새 기본 키 서버를 추가하기 전에 기존 기본 키 서버 중 하나를 제거해야 합니다.

2. 기본 키 관리자를 활성화합니다.

   ```
   security key-manager external enable -vserver <svm_name> -key-servers
   <primary_key_server_ip> -client-cert <client_cert_name> -server-ca-certs
   <server_ca_cert_names>
   ```

   - 포트를 지정하지 않으면 `-key-servers` 매개변수의 경우 기본 포트 5696이 사용됩니다.

   > 실행 중이라면 `security key-manager external enable` MetroCluster 구성에서 관리 SVM에 대한 명령을 실행하려면 두 클러스터에서 모두 명령을 실행해야 합니다. 개별 데이터 SVM에 대해 명령을 실행하는 경우 두 클러스터 모두에서 명령을 실행할 필요는 없습니다. NetApp 두 클러스터 모두에서 동일한 키 서버를 사용할 것을 강력히 권장합니다.

3. 기본 키 서버를 수정하여 보조 키 서버를 추가합니다. 그만큼 `-secondary-key-servers` 매개변수는 최대 3개의 주요 서버를 쉼표로 구분하여 나열할 수 있습니다.

   ```
   security key-manager external modify-server -vserver <svm_name> -key
   -servers <primary_key_server> -secondary-key-servers <list_of_key_servers>
   ```

   - 보조 키 서버에 대한 포트 번호를 포함하지 마십시오. `-secondary-key-servers` 매개변수. 기본 키 서버와 동일한 포트 번호를 사용합니다.

   > 실행 중이라면 `security key-manager external` MetroCluster 구성에서 관리 SVM에 대한 명령을 실행하려면 두 클러스터에서 모두 명령을 실행해야 합니다. 개별 데이터 SVM에 대해 명령을 실행하는 경우 두 클러스터 모두에서 명령을 실행할 필요는 없습니다. NetApp 두 클러스터 모두에서 동일한 키 서버를 사용할 것을 강력히 권장합니다.

기존 기본 키 서버에 보조 키 서버를 추가합니다

단계

1. 기본 키 서버를 수정하여 보조 키 서버를 추가합니다. 그만큼 `-secondary-key-servers` 매개변수는 최대 3개의 주요 서버를 쉼표로 구분하여 나열할 수 있습니다.

   ```
   security key-manager external modify-server -vserver <svm_name> -key
   -servers <primary_key_server> -secondary-key-servers <list_of_key_servers>
   ```

   - 보조 키 서버에 대한 포트 번호를 포함하지 마십시오. `-secondary-key-servers` 매개변수. 기본 키 서버와 동일한 포트 번호를 사용합니다.

실행 중이라면 `security key-manager external modify-server` MetroCluster 구성에서 관리 SVM에 대한 명령을 실행하려면 두 클러스터에서 모두 명령을 실행해야 합니다. 개별 데이터 SVM에 대해 명령을 실행하는 경우 두 클러스터 모두에서 명령을 실행할 필요는 없습니다. NetApp 두 클러스터 모두에서 동일한 키 서버를 사용할 것을 강력히 권장합니다.

보조 키 서버에 대한 자세한 내용은 다음을 참조하세요. [mod-secondary].

클러스터링된 키 서버를 수정합니다

보조 키 서버를 추가 및 제거하고, 보조 키 서버의 액세스 순서를 변경하거나, 특정 키 서버의 지정(기본 또는 보조)을 변경하여 클러스터형 외부 키 서버를 수정할 수 있습니다. MetroCluster 구성에서 클러스터된 외부 키 서버를 수정하는 경우 NetApp 두 클러스터에서 동일한 키 서버를 사용할 것을 강력히 권장합니다.

보조 키 서버를 수정합니다

`security key-manager external modify-server`명령의 `-secondary-key-servers` 매개변수를 사용하여 보조 키 서버를 관리합니다. 그만큼 `-secondary-key-servers` 매개변수는 쉼표로 구분된 목록을 허용합니다. 목록에서 보조 키 서버의 지정된 순서는 보조 키 서버의 액세스 순서를 결정합니다. 보조 키 서버가 다른 순서로 입력된 상태에서 `security key-manager external modify-server` 명령을 실행하여 액세스 순서를 수정할 수 있습니다. 보조 키 서버에 대한 포트 번호를 포함하지 마세요.

실행 중이라면 `security key-manager external modify-server` MetroCluster 구성에서 관리 SVM에 대한 명령을 실행하려면 두 클러스터에서 모두 명령을 실행해야 합니다. 개별 데이터 SVM에 대해 명령을 실행하는 경우 두 클러스터 모두에서 명령을 실행할 필요는 없습니다.

보조 키 서버를 제거하려면 유지하려는 키 서버를 포함하세요. `-secondary-key-servers` 매개변수를 선택하고 제거하려는 매개변수는 생략합니다. 모든 보조 키 서버를 제거하려면 인수를 사용하세요. `-` , 없음을 의미합니다.

기본 및 보조 키 서버를 변환합니다

다음 단계에 따라 특정 키 서버의 지정(기본 또는 보조)을 변경할 수 있습니다.

기본 키 서버를 보조 키 서버로 변환

단계

1. SVM에서 기본 키 서버를 제거합니다.

```
security key-manager external remove-servers
```

> 실행 중이라면 `security key-manager external remove-servers` MetroCluster 구성에서 관리 SVM에 대한 명령을 실행하려면 두 클러스터에서 모두 명령을 실행해야 합니다. 개별 데이터 SVM에 대해 명령을 실행하는 경우 두 클러스터 모두에서 명령을 실행할 필요는 없습니다.

2. 수행하다클러스터링된 키 서버를 생성합니다 이전 기본 키 서버를 보조 키 서버로 사용하는 절차입니다.

보조 키 서버를 기본 키 서버로 변환

단계

1. 기존 기본 키 서버에서 보조 키 서버를 제거합니다.

```
security key-manager external modify-server -secondary-key-servers
```

- 실행 중이라면 `security key-manager external modify-server -secondary-key-servers` MetroCluster 구성에서 관리 SVM에 대한 명령을 실행하려면 두 클러스터에서 모두 명령을 실행해야 합니다. 개별 데이터 SVM에 대해 명령을 실행하는 경우 두 클러스터 모두에서 명령을 실행할 필요는 없습니다.
- 기존 키 서버를 제거하는 동안 보조 키 서버를 기본 키 서버로 변환하는 경우, 제거 및 변환을 완료하기 전에 새 키 서버를 추가하려고 하면 키 중복이 발생할 수 있습니다.

1. 수행하다클러스터링된 키 서버를 생성합니다 이전 보조 키 서버를 새로운 클러스터형 키 서버의 기본 키 서버로 사용하는 절차입니다.

참조하다[mod-secondary] 자세한 내용은.

관련 정보

- 자세히 알아보세요 `security key-manager external` 에서"ONTAP 명령 참조입니다"

ONTAP 9.6 이상에서 인증 키를 생성합니다

'Security key-manager key create' 명령을 사용하여 노드의 인증 키를 생성한 후 구성된 KMIP 서버에 저장할 수 있습니다.

이 작업에 대해

보안 설정에서 데이터 인증과 FIPS 140-2 인증을 위해 다른 키를 사용해야 하는 경우 각각에 대해 별도의 키를 만들어야 합니다. 그렇지 않은 경우 데이터 액세스에 사용하는 것과 동일한 인증 키를 FIPS 규정 준수에 사용할 수 있습니다.

ONTAP은 클러스터의 모든 노드에 대해 인증 키를 생성합니다.

- Onboard Key Manager가 활성화된 경우 이 명령은 지원되지 않습니다. 그러나 Onboard Key Manager가

활성화되면 두 개의 인증 키가 자동으로 생성됩니다. 키는 다음 명령을 사용하여 볼 수 있습니다.

```
security key-manager key query -key-type NSE-AK
```

- 구성된 키 관리 서버가 이미 128개 이상의 인증 키를 저장하고 있으면 경고가 표시됩니다.
- 사용하여명령을 수 `security key-manager key delete` 사용하지 않는 키를 삭제할 있습니다. `security key-manager key delete`지정된 키가 현재 ONTAP에서 사용 중인 경우 명령이 실패합니다. (이 명령을 사용하려면 보다 큰 `Privileges`가 있어야 `admin` 합니다.)

> MetroCluster 환경에서 키를 삭제하기 전에 키가 파트너 클러스터에서 사용되고 있지 않은지 확인해야 합니다. 파트너 클러스터에서 다음 명령을 사용하여 키가 사용되고 있지 않은지 확인할 수 있습니다.
>
> - `storage encryption disk show -data-key-id <key-id>`
> - `storage encryption disk show -fips-key-id <key-id>`

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 클러스터 노드의 인증 키를 생성합니다.

```
security key-manager key create -key-tag <passphrase_label> -prompt-for
-key true|false
```

> 설정을 `prompt-for-key=true` 사용하면 클러스터 관리자에게 암호화된 드라이브를 인증할 때 사용할 암호를 묻는 메시지가 표시됩니다. 그렇지 않으면 시스템이 자동으로 32바이트 암호를 생성합니다. `security key-manager key create`명령이 `security key-manager create-key` 명령을 대체합니다. 에 대한 자세한 내용은 `security key-manager key create` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예제에서는 32바이트 암호를 자동으로 생성하는 "cluster1"에 대한 인증 키를 만듭니다.

```
cluster1::> security key-manager key create
Key ID: <id_value>
```

2. 인증 키가 생성되었는지 확인합니다.

```
security key-manager key query -node node
```

`security key-manager key query`명령이 `security key-manager query key` 명령을 대체합니다.

출력에 표시되는 키 ID는 인증 키를 참조하는 데 사용되는 식별자입니다. 실제 인증 키 또는 데이터 암호화 키가 아닙니다.

다음 예제에서는 "cluster1"에 대해 인증 키가 생성되었는지 확인합니다.

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: external
          Node: node1

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID: <id_value>
node1                                    NSE-AK    yes
    Key ID: <id_value>

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node2                                    NSE-AK    yes
    Key ID: <id_value>
node2                                    NSE-AK    yes
    Key ID: <id_value>
```

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

관련 정보

- "저장 암호화 디스크 표시"

ONTAP 9.5 이전 버전에서 인증 키를 만듭니다

'Security key-manager create-key' 명령을 사용하여 노드의 인증 키를 생성한 후 구성된 KMIP 서버에 저장할 수 있습니다.

이 작업에 대해

보안 설정에서 데이터 인증과 FIPS 140-2 인증을 위해 다른 키를 사용해야 하는 경우 각각에 대해 별도의 키를 만들어야 합니다. 그렇지 않은 경우 데이터 액세스에 사용하는 FIPS 준수에 동일한 인증 키를 사용할 수 있습니다.

ONTAP은 클러스터의 모든 노드에 대해 인증 키를 생성합니다.

- 온보드 키 관리가 활성화된 경우 이 명령은 지원되지 않습니다.
- 구성된 키 관리 서버가 이미 128개 이상의 인증 키를 저장하고 있으면 경고가 표시됩니다.

  키 관리 서버 소프트웨어를 사용하여 사용하지 않는 키를 삭제한 다음 명령을 다시 실행할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 클러스터 노드의 인증 키를 생성합니다.

   보안 키 관리자 만들기 키

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

   > 출력에 표시되는 키 ID는 인증 키를 참조하는 데 사용되는 식별자입니다. 실제 인증 키 또는 데이터 암호화 키가 아닙니다.

   다음 예제에서는 "cluster1"에 대한 인증 키를 만듭니다.

   ```
   cluster1::> security key-manager create-key
      (security key-manager create-key)
   Verifying requirements...

   Node: cluster1-01
   Creating authentication key...
   Authentication key creation successful.
   Key ID: <id_value>

   Node: cluster1-01
   Key manager restore operation initialized.
   Successfully restored key information.

   Node: cluster1-02
   Key manager restore operation initialized.
   Successfully restored key information.
   ```

2. 인증 키가 생성되었는지 확인합니다.

   보안 키 관리자 쿼리

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

   다음 예제에서는 "cluster1"에 대해 인증 키가 생성되었는지 확인합니다.

```
cluster1::> security key-manager query

  (security key-manager query)

          Node: cluster1-01
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag         Key Type  Restored
--------------  --------  --------
cluster1-01     NSE-AK    yes
       Key ID: <id_value>


          Node: cluster1-02
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag         Key Type  Restored
--------------  --------  --------
cluster1-02     NSE-AK    yes
       Key ID: <id_value>
```

ONTAP 외부 키 관리를 사용하여 FIPS 드라이브 또는 SED에 데이터 인증 키 할당

'스토리지 암호화 디스크 수정' 명령을 사용하여 데이터 인증 키를 FIPS 드라이브 또는 SED에 할당할 수 있습니다. 클러스터 노드는 이 키를 사용하여 드라이브에서 암호화된 데이터를 잠그거나 잠금 해제합니다.

이 작업에 대해

자체 암호화 드라이브는 인증 키 ID가 기본값이 아닌 값으로 설정된 경우에만 무단 액세스로부터 보호됩니다. 키 ID 0x0이 있는 제조업체 보안 ID(MSID)는 SAS 드라이브의 표준 기본값입니다. NVMe 드라이브의 경우 표준 기본값은 빈 키 ID로 표시되는 null 키입니다. 키 ID를 자체 암호화 드라이브에 할당하면 시스템은 해당 인증 키 ID를 기본값이 아닌 값으로 변경합니다.

이 절차는 중단되지 않습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. FIPS 드라이브 또는 SED에 데이터 인증 키 할당:

   'Storage encryption disk modify -disk_disk_ID_-data-key-id_key_ID_'

   에 대한 자세한 내용은 `storage encryption disk modify` "ONTAP 명령 참조입니다"을 참조하십시오.

'Security key-manager query-key-type NSE-AK' 명령어를 이용하여 키 ID를 확인할 수 있다.

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
<id_value>

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

2. 인증 키가 할당되었는지 확인합니다.

   스토리지 암호화 디스크 표시

   에 대한 자세한 내용은 `storage encryption disk show` "ONTAP 명령 참조입니다"을 참조하십시오.

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------------
0.0.0   data <id_value>
0.0.1   data <id_value>
[...]
```

관련 정보

- "저장 암호화 디스크 표시"
- "저장 암호화 디스크 표시 상태"

온보드 키 관리를 구성합니다

ONTAP 9.6 이상에서 온보드 키 관리를 활성화합니다

Onboard Key Manager를 사용하여 FIPS 드라이브 또는 SED에 대한 클러스터 노드를 인증할 수 있습니다. Onboard Key Manager는 데이터와 동일한 스토리지 시스템의 노드에 인증 키를 제공하는 기본 제공 도구입니다. Onboard Key Manager는 FIPS-140-2 레벨 1을 준수합니다.

Onboard Key Manager를 사용하여 클러스터가 암호화된 데이터에 액세스하는 데 사용하는 키를 보호할 수 있습니다. 암호화된 볼륨 또는 자체 암호화 디스크에 액세스하는 각 클러스터에서 Onboard Key Manager를 활성화해야 합니다.

이 작업에 대해

클러스터에 노드를 추가할 때마다 보안 키 관리자 온보드 활성화 명령을 실행해야 합니다. MetroCluster 구성에서는 먼저 로컬 클러스터에서 보안 키 관리자 온보드 활성화를 실행한 다음 원격 클러스터에서 동일한 암호를 사용하여 보안 키 관리자 온보드 동기화를 실행해야 합니다.

자세히 알아보세요 `security key-manager onboard enable` 그리고 `security key-manager onboard`

sync 에서"ONTAP 명령 참조입니다" .

기본적으로 노드를 재부팅할 때는 키 관리자 암호를 입력할 필요가 없습니다. MetroCluster를 제외하고, 사용자가 재부팅 후 암호문을 입력하도록 'cc-mode-enabled=yes' 옵션을 사용할 수 있습니다.

Common Criteria 모드('cc-mode-enabled=yes')에서 Onboard Key Manager를 활성화하면 다음과 같은 방식으로 시스템 동작이 변경됩니다.

- 시스템은 Common Criteria 모드에서 작동 중일 때 연속 실패한 클러스터 암호 시도를 모니터링합니다.

  NSE(NetApp 스토리지 암호화)가 활성화되어 있고 부팅 시 올바른 클러스터 암호를 입력하지 않으면 시스템이 드라이브를 인증할 수 없고 자동으로 재부팅됩니다. 이 문제를 해결하려면 부팅 프롬프트에서 올바른 클러스터 암호를 입력해야 합니다. 시스템이 부팅되면 24시간 동안 클러스터 암호를 매개 변수로 요구하는 명령에 대해 최대 5회 연속 클러스터 암호를 올바르게 입력할 수 있습니다. 제한에 도달한 경우(예: 클러스터 암호를 5회 연속으로 올바르게 입력하지 않은 경우) 24시간 제한 시간이 경과할 때까지 기다리거나 노드를 재부팅하여 제한을 재설정해야 합니다.

- 시스템 이미지 업데이트는 NetApp RSA-3072 코드 서명 인증서와 SHA-384 코드 서명 다이제스트를 함께 사용하여 일반적인 NetApp RSA-2048 코드 서명 인증서와 SHA-256 코드 서명 다이제스트 대신 이미지 무결성을 확인합니다.

  업그레이드 명령은 다양한 디지털 서명을 검사하여 이미지 내용이 변경되거나 손상되지 않았는지 확인합니다. 검증이 성공하면 이미지 업데이트는 다음 단계로 진행됩니다. 검증이 실패하면 이미지 업데이트가 실패합니다. 자세히 알아보세요 cluster image 에서"ONTAP 명령 참조입니다" .

Onboard Key Manager는 휘발성 메모리에 키를 저장합니다. 시스템을 재부팅하거나 정지하면 휘발성 메모리 내용이 지워집니다. 정상적인 작동 조건에서는 시스템을 정지하면 30초 이내에 휘발성 메모리 콘텐츠가 지워집니다.

시작하기 전에

- NSE를 외부 키 관리(KMIP) 서버와 함께 사용할 경우 외부 키 관리자 데이터베이스를 삭제해야 합니다.

  "외부 키 관리에서 온보드 키 관리로 전환"

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- Onboard Key Manager를 구성하기 전에 MetroCluster 환경을 구성해야 합니다.

단계

1. 키 관리자 설정 명령을 시작합니다.

   '보안 키 관리자 온보드 활성화-cc-모드 사용 예|아니오'

   cc-mode-enabled=yes`재부팅 후 사용자가 키 관리자 암호를 입력하도록 요구하도록 설정합니다. `- cc-mode-enabled`MetroCluster 구성에서는 옵션이 지원되지 않습니다. `security key-manager onboard enable`명령이 `security key-manager setup 명령을 대체합니다.

   다음 예제에서는 재부팅할 때마다 암호를 입력할 필요 없이 키 관리자 설치 명령을 cluster1에서 시작합니다.

2. 32~256자 사이의 암호를 입력하세요. "`cc-mode`"의 경우 64~256자 사이의 암호를 입력하세요.

   지정된 ""cc-mode"" 암호가 64자 미만이면 키 관리자 설정 작업에 암호 프롬프트가 다시 표시되기 전에 5초의 지연이 발생합니다.

3. 암호 확인 프롬프트에서 암호를 다시 입력합니다.
4. 시스템이 인증 키를 생성하는지 확인하세요.

   'security key-manager key query 노드

   `security key-manager key query`명령이 `security key-manager query key` 명령을 대체합니다.

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

작업을 마친 후

나중에 사용할 수 있도록 암호를 스토리지 시스템 외부의 안전한 위치에 복사합니다.

시스템은 클러스터의 복제된 데이터베이스(RDB)에 주요 관리 정보를 자동으로 백업합니다. 재해 복구를 위해 이 정보를 수동으로 백업해야 합니다.

관련 정보

- "클러스터 이미지 명령"
- "보안 키 관리자 외부 활성화"
- "보안 키 관리자 키 쿼리"
- "보안 키 관리자 온보드 활성화"
- "외부 키 관리에서 온보드 키 관리로 전환"

ONTAP 9.5 이전 버전에서 온보드 키 관리를 활성화합니다

Onboard Key Manager를 사용하여 FIPS 드라이브 또는 SED에 대한 클러스터 노드를 인증할 수 있습니다. Onboard Key Manager는 데이터와 동일한 스토리지 시스템의 노드에 인증 키를 제공하는 기본 제공 도구입니다. Onboard Key Manager는 FIPS-140-2 레벨 1을 준수합니다.

온보드 키 관리자를 사용하면 클러스터가 암호화된 데이터에 액세스하는 데 사용하는 키를 보호할 수 있습니다. 암호화된 볼륨이나 자체 암호화 디스크에 액세스하는 각 클러스터에서 Onboard Key Manager를 활성화합니다.

이 작업에 대해

클러스터에 노드를 추가할 때마다 보안 키 관리자 설정 명령을 실행해야 합니다.

MetroCluster 구성이 있는 경우 다음 지침을 검토하십시오.

- ONTAP 9.5에서는 로컬 클러스터에서 보안 키 관리자 설정, 원격 클러스터에서 보안 키 관리자 설정 -동기화 -MetroCluster -구성 예 를 각각 동일한 암호를 사용하여 실행해야 합니다.
- ONTAP 9.5 이전에는 로컬 클러스터에서 보안 키 관리자 설정을 실행하고 약 20초 정도 기다린 다음 원격 클러스터에서 동일한 암호를 사용하여 보안 키 관리자 설정을 실행해야 합니다.

기본적으로 노드를 재부팅할 때는 키 관리자 암호를 입력할 필요가 없습니다. ONTAP 9.4부터 '-enable-cc-mode yes' 옵션을 사용하여 재부팅 후 사용자가 암호를 입력하도록 할 수 있습니다.

NVE의 경우 '-enable-cc-mode yes'를 설정하면 볼륨 생성 및 볼륨 이동 시작 명령으로 생성한 볼륨이 자동으로 암호화됩니다. 볼륨 만들기에는 -encrypt true를 지정할 필요가 없습니다. 볼륨 이동 시작의 경우 -encrypt-destination true를 지정하지 않아도 됩니다.

실패한 암호 구문을 시도한 후에는 노드를 다시 재부팅해야 합니다.

시작하기 전에

- 외부 키 관리(KMIP) 서버와 함께 NSE를 사용하는 경우 외부 키 관리자 데이터베이스를 삭제하세요.

  "외부 키 관리에서 온보드 키 관리로 전환"

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- Onboard Key Manager를 구성하기 전에 MetroCluster 환경을 구성하세요.

단계

1. 키 관리자 설정을 시작합니다.

   '보안 키 관리자 설정-활성화-cc-모드 예|아니오'

   ONTAP 9.4부터는 사용자가 재부팅 후 키 관리자 암호를 입력하도록 하는 '-enable-cc-mode yes' 옵션을 사용할 수 있습니다. NVE의 경우 '-enable-cc-mode yes'를 설정하면 볼륨 생성 및 볼륨 이동 시작 명령으로 생성한 볼륨이 자동으로 암호화됩니다.

   다음 예제에서는 재부팅할 때마다 암호를 입력할 필요 없이 키 관리자를 cluster1에서 설정하기 시작합니다.

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. 온보드 키 관리를 구성하라는 메시지가 나타나면 "예"를 입력합니다.
3. 암호문 프롬프트에서 32자에서 256자 사이의 암호문을 입력하거나 64에서 256자 사이의 암호문을 "cc-mode"로 입력합니다.

   지정된 ""cc-mode"" 암호가 64자 미만이면 키 관리자 설정 작업에 암호 프롬프트가 다시 표시되기 전에 5초의 지연이 발생합니다.

4. 암호 확인 프롬프트에서 암호를 다시 입력합니다.
5. 모든 노드에 대해 키가 구성되었는지 확인합니다.

   `security key-manager show-key-store`

   자세히 알아보세요 `security key-manager show-key-store` 에서"ONTAP 명령 참조입니다" .

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

Node: node1
Key Store: onboard
Key ID                                                               Used By
-----------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK

Node: node2
Key Store: onboard
Key ID                                                               Used By
-----------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK
```

작업을 마친 후

ONTAP 클러스터의 복제된 데이터베이스(RDB)에 주요 관리 정보를 자동으로 백업합니다.

온보드 키 관리자 암호를 구성한 후에는 해당 정보를 저장 시스템 외부의 안전한 위치에 수동으로 백업하세요. 보다 "온보드 키 관리 정보를 수동으로 백업합니다" .

관련 정보

- "온보드 키 관리 정보를 수동으로 백업합니다"
- "보안 키 관리자 설정"
- "보안 키 관리자 show-key-store"
- "외부 키 관리에서 온보드 키 관리로 전환"

ONTAP 온보드 키 관리를 사용하여 FIPS 드라이브 또는 SED에 데이터 인증 키 할당

'스토리지 암호화 디스크 수정' 명령을 사용하여 데이터 인증 키를 FIPS 드라이브 또는 SED에 할당할 수 있습니다. 클러스터 노드는 이 키를 사용하여 드라이브의 데이터에 액세스합니다.

이 작업에 대해

자체 암호화 드라이브는 인증 키 ID가 기본값이 아닌 값으로 설정된 경우에만 무단 액세스로부터 보호됩니다. 키 ID

0x0이 있는 제조업체 보안 ID(MSID)는 SAS 드라이브의 표준 기본값입니다. NVMe 드라이브의 경우 표준 기본값은 빈 키 ID로 표시되는 null 키입니다. 키 ID를 자체 암호화 드라이브에 할당하면 시스템은 해당 인증 키 ID를 기본값이 아닌 값으로 변경합니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. FIPS 드라이브 또는 SED에 데이터 인증 키 할당:

   'Storage encryption disk modify -disk_disk_ID_-data-key-id_key_ID_'

   에 대한 자세한 내용은 `storage encryption disk modify` "ONTAP 명령 참조입니다"을 참조하십시오.

   'Security key-manager key query-key-type NSE-AK' 명령어를 이용하여 키 ID를 확인할 수 있다.

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   <id_value>

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

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

2. 인증 키가 할당되었는지 확인합니다.

   스토리지 암호화 디스크 표시

   에 대한 자세한 내용은 `storage encryption disk show` "ONTAP 명령 참조입니다"을 참조하십시오.

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   ------------------------------------------------------------------
   0.0.0   data <id_value>
   0.0.1   data <id_value>
   [...]
   ```

관련 정보

- "저장 암호화 디스크 표시"
- "저장 암호화 디스크 표시 상태"

ONTAP FIPS 드라이브에 FIPS 140-2 인증 키 할당

'-FIPS-key-id' 옵션과 함께 'storage encryption disk modify' 명령을 사용하여 FIPS 140-2 인증 키를 FIPS 드라이브에 할당할 수 있습니다. 클러스터 노드는 드라이브에 대한 서비스 거부 공격을 방지하는 것과 같이 데이터 액세스 이외의 드라이브 작업에 이 키를 사용합니다.

이 작업에 대해

보안 설정에서 데이터 인증과 FIPS 140-2 인증을 위해 다른 키를 사용해야 할 수 있습니다. 그렇지 않은 경우 데이터 액세스에 사용하는 FIPS 준수에 동일한 인증 키를 사용할 수 있습니다.

이 절차는 중단되지 않습니다.

시작하기 전에

드라이브 펌웨어는 FIPS 140-2 규정 준수를 지원해야 합니다. 를 클릭합니다 "NetApp 상호 운용성 매트릭스 툴" 지원되는 드라이브 펌웨어 버전에 대한 정보를 제공합니다.

단계

1. 먼저 데이터 인증 키를 할당했는지 확인해야 합니다. 이 작업은 를 사용하여 수행할 수 있습니다 외부 키 관리자 또는 을 누릅니다 Onboard Key Manager(온보드 키 관리자. 'storage encryption disk show' 명령을 사용하여 키가 할당되었는지 확인합니다.
2. SED에 FIPS 140-2 인증 키 할당:

   'Storage encryption disk modify -disk_disk_id_-FIPS-key-id_FIPS_authentication_key_id_'

   '보안 키 관리자 쿼리' 명령을 사용하여 키 ID를 볼 수 있습니다.

   ```
   cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
   <id_value>

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

3. 인증 키가 할당되었는지 확인합니다.

   스토리지 암호화 디스크 show-FIPS

   에 대한 자세한 내용은 `storage encryption disk show` "ONTAP 명령 참조입니다"을 참조하십시오.

```
cluster1::> storage encryption disk show -fips
Disk    Mode FIPS-Compliance Key ID
------  ----
--------------------------------------------------------------------
2.10.0  full <id_value>
2.10.1  full <id_value>
[...]
```

관련 정보

- "저장 암호화 디스크 수정"
- "저장 암호화 디스크 표시"
- "저장 암호화 디스크 표시 상태"

ONTAP에서 KMIP 서버 연결을 위해 클러스터 차원의 FIPS 호환 모드를 사용하도록 설정합니다

'보안 구성 수정' 명령을 -FIPS 사용' 옵션과 함께 사용하면 전송 중인 데이터에 대해 클러스터 차원의 FIPS 호환 모드를 사용할 수 있습니다. 이렇게 하면 클러스터가 KMIP 서버에 연결할 때 FIPS 모드에서 OpenSSL을 사용하게 됩니다.

이 작업에 대해

클러스터 전반의 FIPS 호환 모드를 사용하도록 설정하면 클러스터에서 TLS1.2 및 FIPS 인증 암호 그룹만 자동으로 사용됩니다. 클러스터 차원의 FIPS 호환 모드는 기본적으로 해제되어 있습니다.

클러스터 전체 보안 구성을 수정한 후에는 클러스터 노드를 수동으로 재부팅해야 합니다.

시작하기 전에

- 스토리지 컨트롤러는 FIPS 호환 모드로 구성해야 합니다.
- 모든 KMIP 서버는 TLSv1.2를 지원해야 합니다. TLSv1.2는 클러스터 차원의 FIPS 호환 모드가 활성화된 경우 KMIP 서버에 대한 연결을 완료해야 합니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. TLSv1.2가 지원되는지 확인합니다.

   '보안 설정 표시 - 지원 - 프로토콜'

   에 대한 자세한 내용은 `security config show` "ONTAP 명령 참조입니다"을 참조하십시오.

```
cluster1::> security config show
          Cluster                                                  Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       false      TLSv1.2, TLSv1.1, TLSv1 ALL:!LOW:         yes
                                             !aNULL:!EXP:
                                             !eNULL
```

3. 클러스터 전체 FIPS 호환 모드 사용:

   보안 설정 수정 - FIPS 활성화 True-Interface SSL

   에 대한 자세한 내용은 `security config modify` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 클러스터 노드를 수동으로 재부팅합니다.
5. 클러스터 차원에서 FIPS 호환 모드가 활성화되어 있는지 확인합니다.

   '보안 구성 쇼'

```
cluster1::> security config show
          Cluster                                                  Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       true       TLSv1.2, TLSv1.1        ALL:!LOW:         yes
                                             !aNULL:!EXP:
                                             !eNULL:!RC4
```