NetApp 암호화 관리

ONTAP 9

NetApp
February 12, 2026

목차

NetApp 암호화 관리

ONTAP에서 볼륨 데이터의 암호화를 해제합니다

볼륨 이동 시작 명령을 사용하여 볼륨 데이터를 이동하거나 암호화 해제할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 암호화된 기존 볼륨을 이동하고 볼륨의 데이터를 암호화 해제합니다.

   `volume move start -vserver` *`SVM_name`* `-volume volume_name -destination-aggregate` *`aggregate_name`* `-encrypt-destination false`

   에 대한 자세한 내용은 `volume move start` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 이름이 "vol1"인 기존 볼륨이 대상 애그리게이트 "aggr3"으로 이동하고 볼륨의 데이터 암호화를 해제합니다.

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3 -encrypt-destination false
   ```

   볼륨에 대한 암호화 키가 삭제됩니다. 볼륨의 데이터가 암호화되지 않습니다.

2. 볼륨에 암호화가 비활성화되어 있는지 확인합니다.

   볼륨 표시 암호화

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

   다음 명령을 실행하면 'cluster1'의 볼륨이 암호화되는지 여부가 표시됩니다.

   ```
   cluster1::> volume show -encryption

   Vserver  Volume    Aggregate    State     Encryption State
   -------  ------    ---------    -----     ----------------
   vs1      vol1      aggr1        online    none
   ```

ONTAP에서 암호화된 볼륨을 이동합니다

'volume move start' 명령을 사용하여 암호화된 볼륨을 이동할 수 있습니다. 이동된 볼륨은 동일한 애그리게이트 또는 다른 애그리게이트에 있을 수 있습니다.

이 작업에 대해

대상 노드 또는 대상 볼륨이 볼륨 암호화를 지원하지 않으면 이동이 실패합니다.

를 클릭합니다 `-encrypt-destination` 의 옵션입니다 `volume move start` 암호화된 볼륨의 경우 기본적으로 true입니다. 대상 볼륨을 암호화하지 않도록 지정해야 하는 요구 사항은 볼륨의 데이터를 실수로 암호화 해제하지 않도록 합니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 암호화된 기존 볼륨을 이동하고 볼륨의 데이터를 암호화된 상태로 유지:

   `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`*

   에 대한 자세한 내용은 `volume move start` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 이름이 "vol1"인 기존 볼륨이 대상 애그리게이트 "aggr3"으로 이동하고 볼륨의 데이터가 암호화된 상태로 유지됩니다.

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3
   ```

2. 볼륨에 암호화가 활성화되어 있는지 확인합니다.

   볼륨 쇼는 암호화된 사실이다

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

   다음 명령을 실행하면 암호화된 볼륨이 'cluster1'에 표시됩니다.

   ```
   cluster1::> volume show -is-encrypted true

   Vserver   Volume   Aggregate   State   Type   Size   Available   Used
   -------   ------   ---------   -----   ----   -----   ---------  ----
   vs1       vol1     aggr3      online     RW   200GB     160.0GB   20%
   ```

ONTAP에서 volume encryption key start 명령을 사용하여 볼륨의 암호화 키를 변경합니다

볼륨의 암호화 키를 정기적으로 변경하는 것이 가장 좋은 방법입니다. ONTAP 9.3부터는 '볼륨 암호화 키 다시 시작' 명령을 사용하여 암호화 키를 변경할 수 있습니다.

이 작업에 대해

키를 다시 입력하다 이전 키로 되돌릴 수 없습니다. 작업 중에 성능 문제가 발생하면 '볼륨 암호화 일시 중지' 명령을 실행하여 작업을 일시 중지하고 '볼륨 암호화 다시 시작' 명령을 실행하여 작업을 다시 시작할 수 있습니다.

키를 다시 입력하다 새 쓰기 및 해당 읽기에서 새 키가 사용됩니다. 그렇지 않으면 읽기에서 이전 키를 사용합니다.

SnapLock 볼륨을 다시 입력하다

단계

1. 암호화 키 변경:

   '볼륨 암호화 키 다시 시작 - SVM_NAME - volume volume volume_name'

   다음 명령을 실행하면 SVM의 vol1에 대한 암호화 키가 VS1 로 변경됩니다.

```
cluster1::> volume encryption rekey start -vserver vs1 -volume vol1
```

2. 키를 다시 입력하다

   볼륨 암호화 키를 다시 입력하다

   에 대한 자세한 내용은 `volume encryption rekey show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 키를 다시 입력하다

```
cluster1::> volume encryption rekey show

Vserver    Volume    Start Time           Status
-------    ------    ------------------   ---------------------------
vs1        vol1      9/18/2017 17:51:41   Phase 2 of 2 is in progress.
```

3. 키를 다시 입력하다

   볼륨 쇼는 암호화된 사실이다

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

   다음 명령을 실행하면 암호화된 볼륨이 'cluster1'에 표시됩니다.

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2      online    RW  200GB    160.0GB  20%
```

ONTAP 볼륨 이동 시작 명령을 사용하여 볼륨의 암호화 키를 변경합니다.

볼륨의 암호화 키를 정기적으로 변경하는 것이 가장 좋은 방법입니다. 명령을 사용하여 암호화 키를 변경할 수 `volume move start` 있습니다. 이동된 볼륨은 동일한 애그리게이트 또는 다른 애그리게이트에 있을 수 있습니다.

이 작업에 대해

SnapLock 또는 FlexGroup 볼륨을 다시 입력하다

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 기존 볼륨을 이동하고 암호화 키를 변경합니다.

   `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-generate-destination-key true`

   에 대한 자세한 내용은 `volume move start` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 이름이 ' * vol1 * '인 기존 볼륨이 대상 집합 ' * aggr2 * '로 이동하고 암호화 키가 변경됩니다.

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr2 -generate-destination-key true
   ```

   볼륨에 대한 새 암호화 키가 생성됩니다. 볼륨의 데이터는 암호화된 상태로 유지됩니다.

2. 볼륨에 암호화가 활성화되어 있는지 확인합니다.

   볼륨 쇼는 암호화된 사실이다

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

   다음 명령을 실행하면 암호화된 볼륨이 'cluster1'에 표시됩니다.

   ```
   cluster1::> volume show -is-encrypted true

   Vserver  Volume  Aggregate  State  Type  Size  Available  Used
   -------  ------  ---------  -----  ----  -----  ---------  ----
   vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
   ```

ONTAP NetApp 스토리지 암호화를 위한 인증 키 순환

NSE(NetApp Storage Encryption)를 사용할 때 인증 키를 회전할 수 있습니다.

이 작업에 대해

NSE 환경에서 인증 키를 회전하면 외부 키 관리자(KMIP)를 사용할 수 있습니다.

NSE 환경에서 인증 키를 회전하면 온보드 키 관리자(OKM)가 지원되지 않습니다.

단계

1. Security key-manager create-key 명령을 사용하여 새 인증 키를 생성합니다.

   인증 키를 변경하려면 먼저 새 인증 키를 생성해야 합니다.

2. 'storage encryption disk modify -disk * -data-key-id' 명령어를 이용하여 인증 키를 변경한다.

관련 정보

- "저장 암호화 디스크 수정"

ONTAP에서 암호화된 볼륨을 삭제합니다

'volume delete' 명령을 사용하여 암호화된 볼륨을 삭제할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 볼륨이 오프라인 상태여야 합니다.

단계

1. 암호화된 볼륨 삭제:

   `volume delete -vserver SVM_name -volume volume_name`

   에 대한 자세한 내용은 `volume delete` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 이름이 "vol1"인 암호화된 볼륨이 삭제됩니다.

   ```
   cluster1::> volume delete -vserver vs1 -volume vol1
   ```

   삭제를 확인하는 메시지가 나타나면 '예'를 입력합니다.

   24시간 후 볼륨에 대한 암호화 키가 삭제됩니다.

`-force true`옵션을 사용하여 `volume delete` 볼륨을 삭제하고 해당 암호화 키를 즉시 제거합니다. 이 명령을 사용하려면 고급 권한이 필요합니다. 에 대한 자세한 내용은 `volume delete` link:https://docs.netapp.com/us-en/ontap-cli/volume-delete.html["ONTAP 명령 참조입니다"^]을 참조하십시오.

작업을 마친 후

'volume recovery-queue' 명령을 사용하여 'volume delete' 명령을 실행한 후 보존 기간 동안 삭제된 볼륨을 복구할 수 있습니다.

`volume recovery-queue` *`SVM_name`* `-volume` *`volume_name`*

"볼륨 복구 기능 사용 방법"

암호화된 볼륨에서 데이터를 안전하게 제거합니다

암호화된 **ONTAP** 볼륨에서 데이터를 안전하게 제거하는 방법에 대해 알아보세요.

ONTAP 9.4부터 보안 제거를 사용하여 NVE 지원 볼륨에서 데이터를 중단 없이 스크럽할 수 있습니다. 암호화된 볼륨에 데이터를 스크러빙하면 물리적 미디어에서 데이터를 복구할 수 없습니다. 예를 들어, 블록 덮어쓰기 시 데이터 추적이 남아 있거나 비어 있는 테넌트의 데이터를 안전하게 삭제하기 위해 "스필지"가 남아 있을 수 있습니다.

Secure Purge는 NVE 지원 볼륨에서 이전에 삭제된 파일에 대해서만 작동합니다. 암호화되지 않은 볼륨은 스크럽 할 수 없습니다. 온보드 키 관리자가 아닌 KMIP 서버를 사용하여 키를 제공해야 합니다.

보안 제거 사용에 대한 고려 사항

- NetApp Aggregate Encryption(NAE)이 활성화된 Aggregate에서 생성된 볼륨은 보안 제거를 지원하지 않습니다.
- Secure Purge는 NVE 지원 볼륨에서 이전에 삭제된 파일에 대해서만 작동합니다.
- 암호화되지 않은 볼륨은 스크럽 할 수 없습니다.
- 온보드 키 관리자가 아닌 KMIP 서버를 사용하여 키를 제공해야 합니다.

ONTAP 버전에 따라 퍼지 기능을 다르게 보호합니다.

ONTAP 9.8 이상

- 보안 삭제는 MetroCluster 및 FlexGroup에서 지원됩니다.
- 제거할 볼륨이 SnapMirror 관계의 소스인 경우 보안 제거를 수행하기 위해 SnapMirror 관계를 중단할 필요가 없습니다.
- 재암호화 방법은 SnapMirror 데이터 보호를 사용하는 볼륨과 SnapMirror 데이터 보호(DP)를 사용하지 않는 볼륨 또는 SnapMirror 확장 데이터 보호를 사용하는 볼륨의 경우에 다릅니다.
  - 기본적으로 SnapMirror 데이터 보호(DP) 모드를 사용하는 볼륨은 볼륨 이동 다시 암호화 방법을 사용하여 데이터를 다시 암호화합니다.
  - 기본적으로 SnapMirror 데이터 보호 또는 XDP(SnapMirror Extended Data Protection) 모드를 사용하는 볼륨을 사용하지 않는 볼륨은 데이터 이동 없이 재암호화 방법을 사용합니다.
  - 이러한 기본값은 'secure purge re-encryption-method[volume-move|in-place-키를 다시 입력하다]' 명령을 사용하여 변경할 수 있습니다.
- 기본적으로 FlexVol 볼륨의 모든 스냅샷은 보안 제거 작업 중에 자동으로 삭제됩니다. 기본적으로 FlexGroup 볼륨 및 SnapMirror 데이터 보호를 사용하는 볼륨의 스냅샷은 안전한 삭제 작업 중에 자동으로 삭제되지 않습니다. 이러한 기본값은 명령을 사용하여 변경할 수 `secure purge delete-all-snapshots [true|false]` 있습니다.

ONTAP 9.7 이하**:**

- 보안 퍼지는 다음을 지원하지 않습니다.
  - 플랙스클론
  - SnapVault
  - FabricPool
- 제거할 볼륨이 SnapMirror 관계의 소스인 경우 볼륨을 제거하려면 SnapMirror 관계를 해제해야 합니다.

  볼륨에 사용 중인 스냅샷이 있는 경우 볼륨을 비우기 전에 스냅샷을 해제해야 합니다. 예를 들어, FlexClone 볼륨을 상위 볼륨에서 분할해야 할 수 있습니다.
- 보안 제거 기능을 성공적으로 호출하면 새 키를 사용하여 남아 있는 비퍼지된 데이터를 다시 암호화하는 볼륨 이동이 트리거됩니다.

  이동된 볼륨은 현재 애그리게이트에 있습니다. 이전 키는 자동으로 삭제되므로 삭제된 데이터를 스토리지 미디어에서 복구할 수 없습니다.

SnapMirror 관계 없이 암호화된 **ONTAP** 볼륨에서 데이터 스크럽

ONTAP 9.4부터 안전한 제거를 사용하여 NVE 지원 볼륨에서 중단 없이 "하위" 데이터를 사용할 수 있습니다.

이 작업에 대해

Secure-Purge는 삭제된 파일의 데이터 양에 따라 완료하는 데 몇 분에서 몇 시간까지 걸릴 수 있습니다. 'volume encryption secure-purge show' 명령을 사용하여 작업 상태를 볼 수 있습니다. 'volume encryption secure-purge abort' 명령을 사용하여 작업을 종료할 수 있습니다.

SAN 호스트에서 보안 제거를 수행하려면 제거할 파일이 포함된 전체 LUN을 삭제하거나 제거할 파일에 속한 블록에 대해 LUN에서 구멍을 뚫을 수 있어야 합니다. LUN을 삭제할 수 없거나 호스트 운영 체제에서 LUN의 구멍을 뚫을 수 없는 경우 보안 제거를 수행할 수 없습니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 이 작업에는 고급 권한이 필요합니다.

단계

1. 안전하게 제거할 파일 또는 LUN을 삭제합니다.
   - NAS 클라이언트에서 안전하게 제거할 파일을 삭제합니다.
   - SAN 호스트에서 제거할 파일에 속한 블록에 대해 LUN에서 안전하게 지우거나 구멍을 뚫을 LUN을 삭제합니다.
2. 스토리지 시스템에서 고급 권한 레벨로 변경합니다.

   세트 프리빌리지 고급

3. 안전하게 제거할 파일이 스냅샷에 있는 경우 스냅샷을 삭제합니다.

   `snapshot delete -vserver SVM_name -volume volume_name -snapshot`

4. 삭제된 파일을 안전하게 삭제:

   `volume encryption secure-purge start -vserver SVM_name -volume volume_name`

   다음 명령을 실행하면 삭제된 파일이 SVM의 vol1에서 VS1 형식으로 안전하게 삭제됩니다.

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

5. 보안 제거 작업의 상태를 확인합니다.

   볼륨 암호화 보안 제거 쇼

SnapMirror 비동기 관계를 사용하여 암호화된 ONTAP 볼륨에서 데이터 스크럽

ONTAP 9.8부터는 SnapMirror 비동기식 관계를 통해 NVE 지원 볼륨에서 중단 없이 데이터를 "스크럽" 데이터로 안전하게 제거할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 이 작업에는 고급 권한이 필요합니다.

이 작업에 대해

Secure-Purge는 삭제된 파일의 데이터 양에 따라 완료하는 데 몇 분에서 몇 시간까지 걸릴 수 있습니다. 'volume

encryption secure-purge show' 명령을 사용하여 작업 상태를 볼 수 있습니다. 'volume encryption secure-purge abort' 명령을 사용하여 작업을 종료할 수 있습니다.

> SAN 호스트에서 보안 제거를 수행하려면 제거할 파일이 포함된 전체 LUN을 삭제하거나 제거할 파일에 속한 블록에 대해 LUN에서 구멍을 뚫을 수 있어야 합니다. LUN을 삭제할 수 없거나 호스트 운영 체제에서 LUN의 구멍을 뚫을 수 없는 경우 보안 제거를 수행할 수 없습니다.

단계

1. 스토리지 시스템에서 advanced 권한 수준으로 전환합니다.

   세트 프리빌리지 고급

2. 안전하게 제거할 파일 또는 LUN을 삭제합니다.
   - NAS 클라이언트에서 안전하게 제거할 파일을 삭제합니다.
   - SAN 호스트에서 제거할 파일에 속한 블록에 대해 LUN에서 안전하게 지우거나 구멍을 뚫을 LUN을 삭제합니다.
3. 안전하게 제거할 비동기 관계의 대상 볼륨을 준비합니다.

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   -prepare true
   ```

   SnapMirror 비동기식 관계의 각 볼륨에 대해 이 단계를 반복합니다.

4. 안전하게 제거할 파일이 스냅샷에 있는 경우 스냅샷을 삭제합니다.

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

5. 안전하게 제거할 파일이 기본 스냅샷에 있는 경우 다음을 수행합니다.

   a. SnapMirror 비동기식 관계에서 대상 볼륨에 스냅샷을 생성합니다.

      ```
      volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume
      volume_name
      ```

   b. SnapMirror를 업데이트하여 기본 스냅샷을 앞으로 이동합니다.

      ```
      snapmirror update -source-snapshot snapshot_name -destination-path
      destination_path
      ```

   SnapMirror 비동기식 관계의 각 볼륨에 대해 이 단계를 반복합니다.

   a. 기본 스냅샷 수에 1을 더한 것과 같은 (a) 및 (b)단계를 반복합니다.

      예를 들어 기본 스냅샷이 두 개 있는 경우 (a) 및 (b) 단계를 세 번 반복해야 합니다.

   b. 기본 스냅샷이 있는지 확인합니다.
      `snapshot show -vserver SVM_name -volume volume_name`
   c. 기본 스냅샷 삭제:
      `snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot`

6. 삭제된 파일을 안전하게 삭제:

   `volume encryption secure-purge start -vserver svm_name -volume volume_name`

   SnapMirror 비동기식 관계의 각 볼륨에서 이 단계를 반복합니다.

   다음 명령을 실행하면 삭제된 파일이 SVM의 ""vol1""에서 "vs1""으로 안전하게 삭제됩니다.

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

7. 안전한 퍼지 작업의 상태를 확인합니다.

   볼륨 암호화 보안 제거 쇼

관련 정보

- "스냅미러 업데이트"

SnapMirror 동기 관계를 사용하여 암호화된 ONTAP 볼륨에서 데이터 스크럽

ONTAP 9.8부터 SnapMirror 동기식 관계를 통해 NVE 지원 볼륨에서 보안 삭제를 사용하여 중단 없이 데이터를 "스크럽"할 수 있습니다.

이 작업에 대해

삭제된 파일의 데이터 양에 따라 보안 제거를 완료하는 데 몇 분에서 몇 시간까지 걸릴 수 있습니다. 'volume encryption secure-purge show' 명령을 사용하여 작업 상태를 볼 수 있습니다. 'volume encryption secure-purge abort' 명령을 사용하여 작업을 종료할 수 있습니다.

> SAN 호스트에서 보안 제거를 수행하려면 제거할 파일이 포함된 전체 LUN을 삭제하거나 제거할 파일에 속한 블록에 대해 LUN에서 구멍을 뚫을 수 있어야 합니다. LUN을 삭제할 수 없거나 호스트 운영 체제에서 LUN의 구멍을 뚫을 수 없는 경우 보안 제거를 수행할 수 없습니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 이 작업에는 고급 권한이 필요합니다.

단계

1. 스토리지 시스템에서 고급 권한 레벨로 변경합니다.

   세트 프리빌리지 고급

2. 안전하게 제거할 파일 또는 LUN을 삭제합니다.
   - NAS 클라이언트에서 안전하게 제거할 파일을 삭제합니다.
   - SAN 호스트에서 제거할 파일에 속한 블록에 대해 LUN에서 안전하게 지우거나 구멍을 뚫을 LUN을 삭제합니다.

3. 안전하게 제거할 비동기 관계의 대상 볼륨을 준비합니다.

   ```
   volume encryption secure-purge start -vserver <SVM_name> -volume <volume_name>
   -prepare true
   ```

   SnapMirror 동기식 관계의 다른 볼륨에 대해 이 단계를 반복합니다.

4. 안전하게 제거할 파일이 스냅샷에 있는 경우 스냅샷을 삭제합니다.

   ```
   snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
   ```

5. 보안 제거 파일이 기본 스냅샷 또는 공통 스냅샷에 있는 경우 SnapMirror를 업데이트하여 공통 스냅샷을 앞으로 이동합니다.

   ```
   snapmirror update -source-snapshot <snapshot_name> -destination-path
   <destination_path>
   ```

   두 개의 일반적인 스냅샷이 있으므로 이 명령을 두 번 실행해야 합니다.

6. 보안 제거 파일이 애플리케이션 정합성 보장 스냅샷에 있는 경우 SnapMirror 동기식 관계에서 두 볼륨의 스냅샷을 삭제합니다.

   ```
   snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
   ```

   두 볼륨에서 이 단계를 수행합니다.

7. 삭제된 파일을 안전하게 삭제:

   ```
   volume encryption secure-purge start -vserver <SVM_name> -volume <volume_name>
   ```

   SnapMirror 동기식 관계의 각 볼륨에 대해 이 단계를 반복합니다.

   다음 명령을 실행하면 삭제된 파일이 SVM ""VS1""의 ""vol1""에서 안전하게 삭제됩니다.

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

8. 안전한 퍼지 작업의 상태를 확인합니다.

   볼륨 암호화 보안 제거 쇼

관련 정보

- "스냅미러 업데이트"

ONTAP 온보드 키 관리 암호문구 변경

NetApp 온보드 키 관리 암호를 정기적으로 변경할 것을 권장합니다. 새로운 암호문구는 저장 시스템 외부의 안전한 장소에 저장해야 합니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.
- 이 작업에는 고급 권한이 필요합니다.
- MetroCluster 환경에서 로컬 클러스터에서 암호를 업데이트한 후 파트너 클러스터에서 암호 업데이트를 동기화합니다.

단계

1. 고급 권한 레벨로 변경:

   세트 프리빌리지 고급

2. 온보드 키 관리 암호를 변경합니다. 사용하는 명령은 실행 중인 ONTAP 버전에 따라 달라집니다.

   ONTAP 9.6 이상

   보안 키 관리자 온보드 업데이트 암호문

   ONTAP 9.5 이하

   보안 키 관리자 업데이트 암호문

3. 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.

4. 암호 확인 프롬프트에서 암호를 다시 입력합니다.
5. MetroCluster 구성을 사용하는 경우 파트너 클러스터에서 업데이트된 암호를 동기화하세요.
   a. ONTAP 버전에 맞는 올바른 명령을 선택하여 파트너 클러스터에서 암호를 동기화하세요.

      ONTAP 9.6 이상

      ```
      security key-manager onboard sync
      ```

      ONTAP 9.5 이하

      - ONTAP 9.5에서 다음을 실행합니다.

        ```
        security key-manager setup -sync-metrocluster-config
        ```

      - ONTAP 9.4 및 이전 버전에서는 로컬 클러스터에서 암호를 업데이트한 후 20초간 기다린 후 파트너 클러스터에서 다음 명령을 실행합니다.

        보안 키 관리자 설정

   b. 메시지가 나타나면 새로운 암호를 입력하세요.

      두 클러스터 모두에서 동일한 암호를 사용해야 합니다.

작업을 마친 후

나중에 사용할 수 있도록 온보드 키 관리 암호를 저장 시스템 외부의 안전한 위치에 복사합니다.

온보드 키 관리 암호를 변경할 때마다 키 관리 정보를 수동으로 백업하세요.

관련 정보

- "온보드 키 관리 정보를 수동으로 백업합니다"
- "보안 키 관리자 온보드 업데이트 암호 구문"

ONTAP 온보드 키 관리 정보를 수동으로 백업하세요.

Onboard Key Manager 암호를 구성할 때마다 온보드 키 관리 정보를 스토리지 시스템 외부의 안전한 위치에 복사해야 합니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 이 작업에는 고급 권한이 필요합니다.

이 작업에 대해

모든 키 관리 정보는 클러스터의 복제된 데이터베이스(RDB)에 자동으로 백업됩니다. 또한 재해 발생 시 사용할 수 있도록 키 관리 정보를 수동으로 백업해야 합니다.

단계

1. 고급 권한 레벨로 변경:

   세트 프리빌리지 고급

2. 클러스터의 키 관리 백업 정보를 표시합니다.

이 ONTAP 버전의 경우…	이 명령 사용…
ONTAP 9.6 이상	보안 키 관리자 온보드 쇼 백업
ONTAP 9.5 이하	보안 키 관리자 백업 쇼

   다음 9.6 명령은 키 관리 백업 정보를 표시합니다. `cluster1` :

```
cluster1::> security key-manager onboard show-backup

     --------------------------BEGIN BACKUP--------------------------
     TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
     QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
     dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
     3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
     IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
     QRHwv+1aWvAAAAAAAAAAACQAAAAAAAAAgAAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
     BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
     AQAAAAMAAAAYAQAAAAAAADA5/ccAAAAAIgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAA
     AAAAAAAAAAACAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAACIAAAAAAAAA
     KAAAAAAAAACI8z/bAAAAAAAAAAAAAAAAAgAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
     AAAAAAAAAAkAAAAAAAAAAIAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
     LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAwAAABgBAAAAAAAA
     1cNLLwAAAAAiAAAAAAAAACgAAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAIAAAAAAAkA
     ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAAIgAAAAAAAAAoAAAAAAAAAJ4/cQsAAAAA
     AAAAAAAAAAACAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAACQAAAAAAAAA
     gAAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
     rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     ---------------------------END BACKUP---------------------------
```


3. 재해 발생 시 사용할 수 있도록 백업 정보를 스토리지 시스템 외부의 안전한 위치에 복사합니다.

관련 정보

- "보안 키 관리자 온보드 show-backup"
- "보안 키 관리자 백업이 표시됩니다"

ONTAP에서 온보드 키 관리 암호화 키를 복원합니다

가끔은 온보드 키 관리 암호화 키를 복원해야 할 수도 있습니다. 키를 복원해야 한다는 것을 확인한 후 Onboard Key Manager를 설정하여 키를 복원할 수 있습니다. 온보드 키 관리 암호화 키를 복원하는 절차는 ONTAP 버전에 따라 다릅니다.

시작하기 전에

- 외부 KMIP 서버와 함께 NSE를 사용하는 경우 외부 키 관리자 데이터베이스를 삭제합니다. 자세한 내용은 다음을 참조하세요."외부 키 관리에서 ONTAP 온보드 키 관리로 전환" .
- 이 작업을 수행하려면 클러스터 관리자여야 합니다.

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

ONTAP 9.6 이상

ONTAP 9.8 이상을 실행 중이고 루트 볼륨이 암호화된 경우 에 대한 절차를 따릅니다 [ontap-9-8].

1. 키를 복원해야 하는지 확인합니다. +'보안 키 관리자 키 쿼리 - node_node_'

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

2. 키 복원: + '보안 키 관리자 온보드 동기화

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

3. 암호 프롬프트에서 클러스터의 온보드 키 관리 암호를 입력합니다.

암호화된 루트 볼륨이 있는 ONTAP 9.8 이상

ONTAP 9.8 이상을 실행 중이고 루트 볼륨이 암호화된 경우 부팅 메뉴를 사용하여 온보드 키 관리 복구 암호를 설정해야 합니다. 부팅 미디어를 교체하는 경우에도 이 프로세스가 필요합니다.

1. 노드를 부팅 메뉴로 부팅하고 '(10) 온보드 키 관리 복구 비밀 설정' 옵션을 선택합니다.
2. 이 옵션을 사용하려면 'y'를 입력합니다.
3. 프롬프트에서 클러스터의 온보드 키 관리 암호를 입력합니다.
4. 프롬프트에서 백업 키 데이터를 입력합니다.

   백업 키 데이터를 입력한 후 노드는 부팅 메뉴로 돌아갑니다.

5. 부팅 메뉴에서 '(1) Normal Boot' 옵션을 선택합니다.

ONTAP 9.5 이하

1. 키를 복원해야 하는지 확인합니다. + '보안 키 관리자 키 쇼'
2. 키 복원: + S/S Security Key-manager setup -node_node_

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

3. 암호 프롬프트에서 클러스터의 온보드 키 관리 암호를 입력합니다.

ONTAP 외부 키 관리 암호화 키 복원

외부 키 관리 암호화 키를 수동으로 복원하고 다른 노드에 푸시할 수 있습니다. 클러스터 키를 생성할 때 일시적으로 중단했던 노드를 다시 시작하는 경우 이 작업을 수행할 수 있습니다.

이 작업에 대해

ONTAP 9.6 이상에서는 '보안 키 관리자 키 쿼리 노드_이름' 명령을 사용하여 키를 복원해야 하는지 확인할 수 있습니다.

ONTAP 9.5 이전 버전에서는 '보안 키 관리자 키 표시' 명령을 사용하여 키를 복원해야 하는지 확인할 수 있습니다.

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

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

시작하기 전에

이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

단계

1. ONTAP 9.8 이상을 실행 중이고 루트 볼륨이 암호화된 경우 다음을 수행합니다.

   ONTAP 9.7 이하를 실행 중이거나 ONTAP 9.8 이상을 실행 중이고 루트 볼륨이 암호화되지 않은 경우 이 단계를 건너뜁니다.

   a. bootargs:+'setenv kmip.init.ipaddr <ip-address>"etenv kmip.init.netmask <netmask>"etenv kmip.init.gateway <gateway>"setenv kmip.init.interface e0M"boot_ONTAP'을 설정합니다
   b. 노드를 부팅 메뉴로 부팅하고 '(11) Configure node for external key management' 옵션을 선택합니다.
   c. 프롬프트에 따라 관리 인증서를 입력합니다.

      모든 관리 인증서 정보를 입력하면 시스템이 부팅 메뉴로 돌아갑니다.

   d. 부팅 메뉴에서 '(1) Normal Boot' 옵션을 선택합니다.
2. 키 복원:

이 ONTAP 버전의 경우…	이 명령 사용…
ONTAP 9.6 이상	'Security key-manager external restore-vserver SVM-node-key-server host_name
ip_address:port-key-id key_id-key-tag key_tag'	ONTAP 9.5 이하

`node` 기본값은 모든 노드입니다.

온보드 키 관리가 활성화된 경우 이 명령은 지원되지 않습니다.

다음 ONTAP 9.6 명령은 외부 키 관리 인증 키를 "cluster1"의 모든 노드에 복원합니다.

```
clusterl::> security key-manager external restore
```

관련 정보

- "보안 키 관리자 외부 복원"

ONTAP 클러스터에서 KMIP SSL 인증서 교체

모든 SSL 인증서의 만료 날짜가 있습니다. 인증서가 만료되기 전에 인증서를 업데이트해야 인증 키에 대한 액세스 권한을 상실할 수 있습니다.

시작하기 전에

- 클러스터를 위한 대체 공용 인증서 및 개인 키를 확보해야 합니다(KMIP 클라이언트 인증서).
- KMIP 서버용 대체 공용 인증서(KMIP 서버-CA 인증서)를 받아야 합니다.
- 이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.
- MetroCluster 환경에서 KMIP SSL 인증서를 교체하는 경우 두 클러스터 모두에 동일한 대체 KMIP SSL 인증서를 설치해야 합니다.

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

단계

1. 새 KMIP 서버-CA 인증서를 설치합니다.

   'Security certificate install-type server-ca-vserver<>'를 선택합니다

2. 새 KMIP 클라이언트 인증서 설치:

   'Security certificate install-type client-vserver<>'

3. 키 관리자 구성을 업데이트하여 새로 설치된 인증서를 사용합니다.

   '보안 키 관리자 외부 수정 - vserver <>-client-cert <>-server-ca-certs <>'

   MetroCluster 환경에서 ONTAP 9.6 이상을 실행하고 있고 admin SVM에서 key manager 구성을 수정하려는 경우 구성의 두 클러스터 모두에서 명령을 실행해야 합니다.

새로 설치된 인증서를 사용하도록 키 관리자 구성을 업데이트하면 새 클라이언트 인증서의 공개/개인 키가 이전에 설치된 키와 다르면 오류가 반환됩니다. 를 참조하십시오"NetApp 지식 기반: 새 클라이언트 인증서 공개 키 또는 개인 키가 기존 클라이언트 인증서와 다릅니다." 이 오류를 무시하는 방법에 대한 지침은 다음을 참조하세요.

관련 정보

- "보안 인증서 설치"
- "보안 키 관리자 외부 수정"

ONTAP에서 FIPS 드라이브 또는 SED를 교체합니다

일반 디스크를 교체하는 것과 동일한 방법으로 FIPS 드라이브 또는 SED를 교체할 수 있습니다. 새 데이터 인증 키를 교체 드라이브에 할당하십시오. FIPS 드라이브의 경우 새 FIPS 140-2 인증 키를 할당할 수도 있습니다.

HA 쌍이 를 사용 중인 경우 "SAS 또는 NVMe 드라이브(SED, NSE, FIPS) 암호화", 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.

시작하기 전에

- 드라이브에서 사용하는 인증 키의 키 ID를 알아야 합니다.
- 이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 디스크가 실패로 표시되어 있는지 확인합니다.

   스토리지 디스크 고장

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

```
cluster1::> storage disk show -broken
Original Owner: cluster1-01
  Checksum Compatibility: block
                                                                  Usable
Physical
    Disk   Outage Reason HA Shelf Bay Chan   Pool  Type    RPM     Size
Size
    ------ ---- ------------ ---- --- ---- ------ -----  -----  -------
-------
    0.0.0  admin  failed  0b    1   0    A  Pool0  FCAL  10000  132.8GB
133.9GB
    0.0.7  admin  removed 0b    2   6    A  Pool1  FCAL  10000  132.8GB
134.2GB
[...]
```

2. 디스크 쉘프 모델의 하드웨어 가이드에 나와 있는 지침에 따라 장애가 발생한 디스크를 제거하고 새 FIPS 드라이브 또는 SED로 교체합니다.
3. 새로 교체한 디스크의 소유권을 할당합니다.

   'Storage disk assign-disk disk_name-owner node'

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

```
cluster1::> storage disk assign -disk 2.1.1 -owner cluster1-01
```

4. 새 디스크가 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>
1.10.0  data <id_value>
1.10.1  data <id_value>
2.1.1   open 0x0
[...]
```

5. 데이터 인증 키를 FIPS 드라이브 또는 SED에 할당합니다.

   "FIPS 드라이브 또는 SED(외부 키 관리)에 데이터 인증 키 할당"

6. 필요한 경우 FIPS 140-2 인증 키를 FIPS 드라이브에 할당합니다.

   "FIPS 140-2 인증 키를 FIPS 드라이브에 할당"

관련 정보

- "저장 디스크 할당"
- "저장 디스크 표시"
- "저장 암호화 디스크 표시"

FIPS 드라이브 또는 SED에 액세스할 수 없도록 설정합니다

FIPS 드라이브 또는 **SED**에서 **ONTAP** 데이터에 액세스할 수 없게 만드는 방법에 대해 알아보세요.

FIPS 드라이브 또는 SED에 있는 데이터를 영구적으로 액세스할 수 없지만 드라이브의 사용되지 않는 공간을 새 데이터에 계속 사용하려면 디스크를 삭제할 수 있습니다. 데이터를 영구적으로 액세스할 수 없도록 만들고 드라이브를 다시 사용하지 않으려면 해당 드라이브를 제거할 수 있습니다.

- 디스크 삭제

자체 암호화 드라이브를 삭제할 때 시스템은 디스크 암호화 키를 새 임의 값으로 변경하고, 전원 켜짐 잠금 상태를 false로 재설정하고, 키 ID를 기본값으로 설정합니다(제조업체 보안 ID 0x0(SAS 드라이브) 또는 null 키(NVMe 드라이브)). 이렇게 하면 디스크의 데이터에 액세스할 수 없게 되고 데이터를 검색할 수 없게 됩니다. 삭제된 디스크를 제로화되지 않은 스페어 디스크로 다시 사용할 수 있습니다.

- 디스크 폐기

  FIPS 드라이브 또는 SED를 제거할 때 시스템은 디스크 암호화 키를 알 수 없는 임의 값으로 설정하고 디스크를 복구할 수 없도록 잠급니다. 이렇게 하면 디스크를 영구적으로 사용할 수 없게 되고 디스크에 있는 데이터에 영구적으로 액세스할 수 없게 됩니다.

개별 자체 암호화 드라이브 또는 노드의 모든 자체 암호화 드라이브를 삭제하고 제거할 수 있습니다.

ONTAP에서 FIPS 드라이브 또는 SED를 삭제합니다

FIPS 드라이브 또는 SED에 있는 데이터를 영구적으로 액세스할 수 없도록 만들고 새 데이터에 드라이브를 사용하려면 'Storage encryption disk sanitize' 명령을 사용하여 드라이브를 삭제할 수 있습니다.

이 작업에 대해

자체 암호화 드라이브를 삭제할 때 시스템은 디스크 암호화 키를 새 임의 값으로 변경하고, 전원 켜짐 잠금 상태를 false로 재설정하고, 키 ID를 기본값으로 설정합니다(제조업체 보안 ID 0x0(SAS 드라이브) 또는 null 키(NVMe 드라이브)). 이렇게 하면 디스크의 데이터에 액세스할 수 없게 되고 데이터를 검색할 수 없게 됩니다. 삭제된 디스크를 제로화되지 않은 스페어 디스크로 다시 사용할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 보존해야 하는 데이터를 다른 디스크의 Aggregate로 마이그레이션합니다.
2. FIPS 드라이브 또는 SED에서 삭제되는 애그리게이트를 삭제합니다.

   'Storage aggregate delete-aggregate_aggregate_name_'

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

   에 대한 자세한 내용은 `storage aggregate delete` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 삭제할 FIPS 드라이브 또는 SED의 디스크 ID 식별:

   스토리지 암호화 디스크 데이터 필드 데이터 키 ID, FIPS 키 ID, 소유자

   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>
1.10.2  data <id_value>
[...]
```

4. FIPS 드라이브가 FIPS 준수 모드에서 실행 중인 경우 노드에 대한 FIPS 인증 키 ID를 기본 MSID 0x0으로 다시 설정합니다.

   'Storage encryption disk modify -disk_disk_id_-FIPS-key-id 0x0'

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

```
cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id 0x0

Info: Starting modify on 1 disk.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

5. 드라이브 완전 삭제:

   'Storage encryption disk sanitize -disk_disk_id_'

   이 명령을 사용하여 핫 스페어 또는 파손된 디스크만 삭제할 수 있습니다. 유형에 관계없이 모든 디스크를 필터링하려면 `-force-all-state` 옵션을 사용합니다. 에 대한 자세한 내용은 `storage encryption disk sanitize` "ONTAP 명령 참조입니다"을 참조하십시오.

   ⓘ ONTAP에서 계속하기 전에 확인 문구를 입력하라는 메시지를 표시합니다. 화면에 표시된 대로 정확하게 구문을 입력합니다.

```
cluster1::> storage encryption disk sanitize -disk 1.10.2

Warning: This operation will cryptographically sanitize 1 spare or
broken self-encrypting disk on 1 node.
         To continue, enter sanitize disk: sanitize disk

Info: Starting sanitize on 1 disk.
      View the status of the operation using the
      storage encryption disk show-status command.
```

6. 삭제된 디스크:'storage disk unfail-spare true-disk_disk_id_'의 장애를 해제합니다

7. 디스크에 소유자가 있는지 확인합니다. `storage disk show -disk disk_id`를 누릅니다 디스크에 소유자가 없는 경우 하나를 할당합니다. `storage disk assign -owner node -disk disk_id`
8. 삭제할 디스크를 소유하는 노드에 대한 노드 선택을 입력합니다.

   'system node run-node_node_name_'

   를 실행합니다 `disk sanitize release` 명령.

9. 노드 쉘을 종료합니다. 디스크 장애 복구 다시 취소: `storage disk unfail -spare true -disk disk_id`
10. 디스크가 이제 스페어이고 'storage disk show -disk_disk_id_'라는 Aggregate에서 재사용할 준비가 되었는지 확인합니다

관련 정보

- "저장 디스크 할당"
- "저장 디스크 표시"
- "저장 디스크가 고장나지 않음"
- "저장 암호화 디스크 수정"
- "스토리지 암호화 디스크 정리"
- "저장 암호화 디스크 표시 상태"

ONTAP에서 FIPS 드라이브 또는 SED를 제거합니다

FIPS 드라이브 또는 SED에 있는 데이터를 영구적으로 액세스할 수 없게 하고 드라이브를 다시 사용할 필요가 없는 경우 '저장소 암호화 디스크 폐기' 명령을 사용하여 디스크를 폐기할 수 있습니다.

이 작업에 대해

FIPS 드라이브 또는 SED를 제거할 때 시스템은 디스크 암호화 키를 알 수 없는 임의 값으로 설정하고 드라이브를 복구할 수 없도록 잠급니다. 이렇게 하면 디스크가 사실상 사용할 수 없게 되고 디스크에 있는 데이터에 영구적으로 액세스할 수 없게 됩니다. 그러나 디스크 레이블에 인쇄된 PSID(Physical Secure ID)를 사용하여 디스크를 공장 출하시 구성된 설정으로 재설정할 수 있습니다. 자세한 내용은 을 참조하십시오 "인증 키가 손실된 경우 FIPS 드라이브 또는 SED를 서비스에 반환합니다".

> Non-Returnable Disk Plus 서비스(NRD Plus)가 없는 경우 FIPS 드라이브 또는 SED를 폐기해서는 안 됩니다. 디스크를 폐기하면 보증이 무효화됩니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 보존해야 하는 데이터를 다른 디스크의 aggregate에 마이그레이션합니다.
2. 제거할 FIPS 드라이브 또는 SED의 Aggregate 삭제:

   'Storage aggregate delete-aggregate aggregate_name'을 선택합니다

```
cluster1::> storage aggregate delete -aggregate aggr1
```

에 대한 자세한 내용은 `storage aggregate delete` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 제거할 FIPS 드라이브 또는 SED의 디스크 ID 식별:

   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>
1.10.2  data <id_value>
[...]
```

4. 디스크 폐기:

   'Storage encryption disk destroy - disk disk_id'

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

   계속하기 전에 확인 문구를 입력하라는 메시지가 표시됩니다. 화면에 표시된 대로 정확하게 구문을 입력합니다.

```
cluster1::> storage encryption disk destroy -disk 1.10.2

Warning: This operation will cryptographically destroy 1 spare or broken
         self-encrypting disks on 1 node.
         You cannot reuse destroyed disks unless you revert
         them to their original state using the PSID value.
         To continue, enter
          destroy disk
         :destroy disk

Info: Starting destroy on 1 disk.
      View the status of the operation by using the
      "storage encryption disk show-status" command.
```

관련 정보

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

ONTAP의 FIPS 드라이브 또는 SED에서 긴급 데이터 삭제

보안 비상 시에 스토리지 시스템이나 KMIP 서버에서 전원을 사용할 수 없는 경우에도 FIPS 드라이브 또는 SED에 대한 액세스를 즉시 차단할 수 있습니다.

시작하기 전에

- KMIP 서버를 사용할 때 전원이 공급되지 않는 경우, 쉽게 파괴되는 인증 항목(예: 스마트 카드 또는 USB 드라이브)으로 KMIP 서버를 구성해야 합니다.
- 이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. FIPS 드라이브 또는 SED에서 긴급 데이터 파쇄 수행:

만약…	그러면…

스토리지 시스템에서 전원을 사용할 수 있으며 스토리지 시스템을 오프라인으로 전환할 수 있는 시간이 있습니다	a. 스토리지 시스템이 HA 쌍으로 구성된 경우 Takeover를 해제합니다. b. 모든 애그리게이트를 오프라인 상태로 전환하고 삭제합니다. c. 권한 수준을 advanced:+'et-Privilege advanced로 설정합니다 d. 드라이브가 FIPS 준수 모드에 있는 경우 노드에 대한 FIPS 인증 키 ID를 기본 MSID(+'STorage encryption disk modify -disk * -FIPS-key -id 0x0’로 다시 설정합니다 e. 스토리지 시스템을 중단합니다. f. 유지보수 모드로 부팅합니다. g. 디스크를 완전 삭제 또는 폐기: ◦ 디스크의 데이터에 액세스할 수 없도록 하고 디스크를 다시 사용할 수 있도록 하려면 + 디스크 암호화 sanitize-all을 선택합니다 ◦ 디스크에 있는 데이터에 액세스할 수 없도록 하고 디스크를 저장할 필요가 없으면 + 디스크 암호화 destroy disk_id1 disk_id2…"를 삭제합니다 디스크 암호화 삭제 및 디스크 암호화 삭제 명령은 유지 보수 모드에만 사용됩니다. 이러한 명령은 각 HA 노드에서 실행해야 하며 깨진 디스크에는 사용할 수 없습니다. h. 파트너 노드에 대해 이 단계를 반복합니다. 이렇게 하면 스토리지 시스템이 영구적으로 비활성화되며 모든 데이터가 지워집니다. 시스템을 다시 사용하려면 다시 구성해야 합니다.	스토리지 시스템에서 전원을 사용할 수 있으며 데이터를 즉시 제거해야 합니다

a. * 디스크에 있는 데이터에 액세스할 수 없도록 만들고 디스크를 다시 사용하려면 디스크를 삭제해야 합니다. * b. 스토리지 시스템이 HA 쌍으로 구성된 경우 Takeover를 해제합니다. c. 권한 수준을 고급으로 설정합니다. 세트 프리빌리지 고급 d. 드라이브가 FIPS 준수 모드인 경우 노드의 FIPS 인증 키 ID를 다시 기본 MSID로 설정합니다. 'Storage encryption disk modify -disk * -FIPS-key-id 0x0' e. 디스크 완전 삭제: 스토리지 암호화 디스크 완전 삭제 -disk * -force -all -states true	a. * 디스크에 있는 데이터에 액세스할 수 없도록 하고 디스크를 저장할 필요가 없는 경우, 다음 디스크를 파기하십시오: * b. 스토리지 시스템이 HA 쌍으로 구성된 경우 Takeover를 해제합니다. c. 권한 수준을 고급으로 설정합니다. 세트 프리빌리지 고급 d. 디스크 폐기: 스토리지 암호화 디스크 destroy-disk * -force-all -states true	스토리지 시스템에서 패닉이 발생하고 모든 데이터가 지워져 시스템이 영구적으로 비활성화된 상태로 유지됩니다. 시스템을 다시 사용하려면 다시 구성해야 합니다.
KMIP 서버에서 전원을 사용할 수 있지만 스토리지 시스템은 사용할 수 없습니다	a. KMIP 서버에 로그인합니다. b. 액세스를 방지하려는 데이터가 포함된 FIPS 드라이브 또는 SED와 연결된 모든 키를 제거합니다. 이렇게 하면 스토리지 시스템에서 디스크 암호화 키에 액세스할 수 없습니다.	KMIP 서버 또는 스토리지 시스템에서 전원을 사용할 수 없습니다

관련 정보

- "저장 암호화 디스크 파괴"
- "저장 암호화 디스크 수정"
- "스토리지 암호화 디스크 정리"

ONTAP 에서 인증 키가 손실된 경우 FIPS 드라이브 또는 SED를 서비스에 반환

FIPS 드라이브 또는 SED가 영구적으로 인증 키를 분실하여 KMIP 서버에서 검색할 수 없는 경우, 시스템은 FIPS 드라이브 또는 SED를 파손된 것으로 처리합니다. 디스크의 데이터에 액세스하거나 복구할 수 없지만 SED의 미사용 공간을 데이터에 다시 사용할 수 있도록 하는

단계를 수행할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

이 작업에 대해

FIPS 드라이브 또는 SED의 인증 키가 영구적으로 손실되어 복구할 수 없는 경우에만 이 프로세스를 사용해야 합니다.

디스크가 분할되어 있는 경우 이 프로세스를 시작하기 전에 먼저 분할되지 않아야 합니다.

> 디스크 파티션을 해제하는 명령은 진단 수준에서만 사용할 수 있으며 NetApp 지원팀의 감독 하에 수행해야 합니다. 계속 진행하기 전에 **NetApp** 지원팀에 문의하는 것이 좋습니다**.** 또한 다음을 참조할 수도 있습니다."NetApp 지식 기반: ONTAP 에서 스페어 드라이브의 파티션을 해제하는 방법" .

단계

1. FIPS 드라이브 또는 SED를 서비스 상태로 되돌리기:

SED가 다음과 같은 경우	다음 단계 사용…

FIPS 호환 모드가 아니거나 FIPS 호환 모드에서는 FIPS 키를 사용할 수 없습니다	a. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
	b. FIPS 키를 기본 제조 보안 ID 0x0:'스토리지 암호화 디스크 수정 - FIPS-key-id 0x0-DISK_DISK_id_'로 재설정합니다
	c. 작업이 성공했는지 확인합니다. '스토리지 암호화 디스크 표시 상태' 작업이 실패하면 이 항목의 PSID 프로세스를 사용합니다.
	d. 깨진 디스크 정리:'storage encryption disk sanitize -disk_disk_id_' 다음 단계로 진행하기 전에 'storage encryption disk show-status' 명령으로 작업이 성공했는지 확인합니다.
	e. 삭제된 디스크:'storage disk unfail-spare true-disk_disk_id_'의 장애를 해제합니다
	f. 디스크에 소유자가 있는지 확인합니다.
	`storage disk show -disk disk_id`
	를 누릅니다
	디스크에 소유자가 없는 경우 하나를 할당합니다.
	`storage disk assign -owner node -disk disk_id`
	i. 삭제할 디스크를 소유하는 노드에 대한 노드 선택을 입력합니다.
	'system node run-node_node_name_'
	를 실행합니다 `disk sanitize release` 명령.
	g. 노드 쉘을 종료합니다. 디스크 장애 복구 다시 취소:
	`storage disk unfail -spare true -disk disk_id`
	h. 디스크가 이제 스페어이고 'storage disk show -disk_disk_id_'라는 Aggregate에서 재사용할 준비가 되었는지 확인합니다

FIPS 준수 모드에서는 FIPS 키를 사용할 수 없으며 SED에는 레이블에 인쇄된 PSID가 있습니다	a. 디스크 레이블에서 디스크의 PSID를 가져옵니다.
	b. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
	c. 디스크를 출고 시 구성된 설정으로 재설정합니다. '스토리지 암호화 디스크 복원 -원본-디스크_디스크_id_-psid_disk_physical_secure_id_' 다음 단계로 진행하기 전에 '저장소 암호화 디스크 표시-상태' 명령으로 작업이 성공했는지 확인합니다.
	d. ONTAP 9.8P5 이하를 실행 중인 경우 다음 단계로 건너뜁니다. ONTAP 9.8P6 이상을 실행 중인 경우 살균된 디스크의 오류를 해제하십시오.
	`storage disk unfail -disk disk_id`
	e. 디스크에 소유자가 있는지 확인합니다.
	`storage disk show -disk disk_id`
	를 누릅니다
	디스크에 소유자가 없는 경우 하나를 할당합니다.
	`storage disk assign -owner node -disk disk_id`
	i. 삭제할 디스크를 소유하는 노드에 대한 노드 선택을 입력합니다.
	'system node run-node_node_name_'
	를 실행합니다 `disk sanitize release` 명령.
	f. 노드 쉘을 종료합니다. 디스크 장애 복구 다시 취소:
	`storage disk unfail -spare true -disk disk_id`
	g. 디스크가 이제 스페어이고 'storage disk show -disk_disk_id_'라는 Aggregate에서 재사용할 준비가 되었는지 확인합니다

관련 정보

- "저장 암호화 디스크 수정"
- "저장 암호화 디스크를 원래 상태로 되돌리기"
- "스토리지 암호화 디스크 정리"
- "저장 암호화 디스크 표시 상태"

ONTAP 에서 FIPS 드라이브 또는 SED를 보호되지 않은 모드로 되돌리기

노드에 대한 인증 키 ID가 기본값이 아닌 값으로 설정된 경우에만 FIPS 드라이브 또는 SED가 무단 액세스로부터 보호됩니다. 명령을 사용하여 키 ID를 기본값으로 설정하면 FIPS 드라이브 또는 SED를 보호되지 않는 모드로 되돌릴 수 `storage encryption disk modify` 있습니다. 보호되지 않은 모드의 FIPS 드라이브 또는 SED는 기본 암호화 키를 사용하는 반면 보호 모드의 FIPS 드라이브 또는 SED는 제공된 보안 암호화 키를 사용합니다. 드라이브에 암호화된 데이터가 있고 드라이브가 보호되지 않는 모드로 재설정되더라도 데이터는 여전히 암호화되어 노출되지 않습니다.

FIPS 드라이브나 SED가 보호되지 않은 모드로 돌아간 후 암호화된 데이터에 액세스할 수 없도록 하려면 다음 절차를 따르세요. FIPS와 데이터 키 ID가 재설정되면 기존 데이터는 해독할 수 없으며 원래 키를 복원하지 않는 한 액세스할 수 없습니다.

HA 쌍이 암호화 SAS 또는 NVMe 드라이브(SED, NSE, FIPS)를 사용 중인 경우 시스템을 초기화하기 전에 HA 쌍 내의 모든 드라이브에 대해 이 프로세스를 따라야 합니다(부팅 옵션 4 또는 9). 이렇게 하지 않을 경우 드라이브를 용도 변경할 경우 향후의 데이터 손실이 발생할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. FIPS 드라이브가 FIPS 준수 모드에서 실행 중인 경우 노드에 대한 FIPS 인증 키 ID를 기본 MSID 0x0으로 다시 설정합니다.

   'Storage encryption disk modify -disk_disk_id_-FIPS-key-id 0x0'

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

   ```
   cluster1::> storage encryption disk modify -disk 2.10.11 -fips-key-id
   0x0

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

   다음 명령을 사용하여 작업이 성공했는지 확인합니다.

   '스토리지 암호화 디스크 표시 상태'입니다

   "Disks Begun"과 "Disks Done"의 숫자가 같아질 때까지 show-status 명령을 반복합니다.

```
cluster1:: storage encryption disk show-status

            FIPS    Latest   Start               Execution   Disks
Disks Disks
Node        Support Request  Timestamp           Time (sec)  Begun
Done  Successful
-------     ------- -------- ------------------  ---------- ------
------  ----------
cluster1    true    modify   1/18/2022 15:29:38    3           14     5
5
1 entry was displayed.
```

3. 노드의 데이터 인증 키 ID를 기본 MSID 0x0으로 다시 설정합니다.

   'Storage encryption disk modify -disk_disk_id_-data-key-id 0x0

   SAS 또는 NVMe 드라이브를 보호되지 않는 모드로 반환하든 관계없이 '-data-key-id' 값은 0x0으로 설정되어야 합니다.

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

```
cluster1::> storage encryption disk modify -disk 2.10.11 -data-key-id
0x0

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

   다음 명령을 사용하여 작업이 성공했는지 확인합니다.

   '스토리지 암호화 디스크 표시 상태'입니다

   숫자가 같아질 때까지 show-status 명령을 반복합니다. "disks began"과 "disks done"의 숫자가 같으면 작업이 완료됩니다.

유지보수 모드

ONTAP 9.7부터 유지 관리 모드에서 FIPS 드라이브를 다시 입력하다 이전 섹션에서 ONTAP CLI 지침을 사용할 수 없는 경우에만 유지보수 모드를 사용해야 합니다.

단계

1. 노드에 대한 FIPS 인증 키 ID를 기본 MSID 0x0으로 다시 설정합니다.

   '디스크 암호화 키를 다시 입력하다 0x0_FIPS 0x0_disklist_'

2. 노드의 데이터 인증 키 ID를 기본 MSID 0x0으로 다시 설정합니다.

"디스크 암호화 0x0_disklist_"

3. FIPS 인증 키를 성공적으로 다시 입력했는지 확인합니다.

   디스크 암호화 show_FIPS

4. 데이터 인증 키가 다음 키로 성공적으로 다시 입력되었는지 확인합니다.

   디스크 암호화 쇼

   출력에는 기본 MSID 0x0 키 ID 또는 키 서버가 보유한 64자 값이 표시될 수 있습니다. 를 클릭합니다 `Locked?` 필드는 데이터 잠금을 의미합니다.

```
Disk        FIPS Key ID                  Locked?
----------- ---------------------------- -------
0a.01.0     0x0                           Yes
```

관련 정보

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

ONTAP에서 외부 키 관리자 연결을 제거합니다

서버가 더 이상 필요하지 않은 경우 노드에서 KMIP 서버를 분리할 수 있습니다. 예를 들어, 볼륨 암호화로 전환할 때 KMIP 서버를 분리할 수 있습니다.

이 작업에 대해

HA 쌍의 한 노드에서 KMIP 서버를 분리하면 시스템이 모든 클러스터 노드에서 서버의 연결을 자동으로 끊습니다.

KMIP 서버를 분리한 후 외부 키 관리를 계속 사용하려면 다른 KMIP 서버를 사용하여 인증 키를 제공할 수 있어야 합니다.

시작하기 전에

이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

단계

1. 현재 노드에서 KMIP 서버를 분리합니다.

이 ONTAP 버전의 경우…	이 명령 사용…
ONTAP 9.6 이상	'Security key-manager external remove-servers-vserver SVM-key-servers host_name
ip_address:port,…	ONTAP 9.5 이하

MetroCluster 환경에서는 admin SVM에 대해 두 클러스터 모두에서 이러한 명령을 반복해야 합니다.

다음 ONTAP 9.6 명령은 첫 번째 이름이 k1인 'cluster1'의 외부 키 관리 서버 2대에 대한 연결을 비활성화하며, 두 번째 주소는 IP 주소가 10.0.0.20인 기본 포트 5696에서 수신, 포트 24482에서 수신 대기 중입니다.

```
clusterl::> security key-manager external remove-servers -vserver
cluster-1 -key-servers ks1,10.0.0.20:24482
```

및 `security key-manager delete` 에 대한 자세한 `security key-manager external remove-servers` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

ONTAP 외부 키 관리 서버 속성 수정

ONTAP 9.6부터, 외부 키 관리 서버의 I/O 제한 시간 및 사용자 이름을 변경하기 위해 'Security key-manager external modify-server' 명령어를 사용할 수 있다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.
- 이 작업에는 고급 권한이 필요합니다.
- MetroCluster 환경에서는 관리 SVM을 위해 두 클러스터 모두에서 이러한 단계를 반복해야 합니다.

단계

1. 스토리지 시스템에서 고급 권한 레벨로 변경합니다.

   세트 프리빌리지 고급

2. 클러스터의 외부 키 관리자 서버 속성 수정:

   'Security key-manager external modify-server-vserver admin_SVM-key-server host_name|ip_address:port,… -timeout 1…60 - username user_name'입니다

   > 시간 초과 값은 초 단위로 표시됩니다. 사용자 이름을 수정하면 새 암호를 입력하라는 메시지가 표시됩니다. 클러스터 로그인 프롬프트에서 명령을 실행하면 '*admin_SVM*'이(가) 현재 클러스터의 admin SVM으로 기본 설정됩니다. 외부 키 관리자 서버 속성을 수정하려면 클러스터 관리자여야 합니다.

   다음 명령을 실행하면 기본 포트 5696에서 수신 대기하는 'cluster1' 외부 키 관리 서버의 시간 초과 값이 45초로 변경됩니다.

   ```
   clusterl::> security key-manager external modify-server -vserver
   cluster1 -key-server ks1.local -timeout 45
   ```

3. SVM에 대한 외부 키 관리자 서버 속성 수정(NVE만 해당):

   'Security key-manager external modify-server-vserver SVM-key-server host_name|ip_address:port,…

-timeout 1…60 - username user_name'입니다

> 시간 초과 값은 초 단위로 표시됩니다. 사용자 이름을 수정하면 새 암호를 입력하라는 메시지가 표시됩니다. SVM 로그인 프롬프트에서 명령을 실행하면 '*SVM*'이(가) 현재 SVM으로 기본 설정됩니다. 외부 키 관리자 서버 속성을 수정하려면 클러스터 또는 SVM 관리자여야 합니다.

다음 명령을 실행하면 기본 포트 5696에서 수신 대기 중인 'vm1' 외부 키 관리 서버의 사용자 이름과 암호가 변경됩니다.

```
svm1::> security key-manager external modify-server -vserver svm11 -key
-server ks1.local -username svm1user
Enter the password:
Reenter the password:
```

4. 추가 SVM에 대해 마지막 단계를 반복합니다.

관련 정보

- "보안 키 관리자 외부 수정 서버"

ONTAP의 온보드 키 관리에서 외부 키 관리로 전환합니다

온보드 키 관리에서 외부 키 관리로 전환하려면 온보드 키 관리 구성을 삭제해야 외부 키 관리를 활성화할 수 있습니다.

시작하기 전에

- 하드웨어 기반 암호화의 경우 모든 FIPS 드라이브 또는 SED의 데이터 키를 기본값으로 재설정해야 합니다.

  "FIPS 드라이브 또는 SED를 보호되지 않는 모드로 되돌리는 중입니다"

- 소프트웨어 기반 암호화의 경우 모든 볼륨의 암호화를 해제해야 합니다.

  "볼륨 데이터 암호화를 해제합니다"

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 클러스터의 온보드 키 관리 구성을 삭제합니다.

이 ONTAP 버전의 경우…	이 명령 사용…
ONTAP 9.6 이상	'Security key-manager 온보드 disable-vserver SVM
ONTAP 9.5 이하	보안 키 관리자 삭제 키 데이터베이스

및 `security key-manager delete-key-database` 에 대한 자세한 `security key-manager onboard disable` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

외부 키 관리에서 ONTAP 온보드 키 관리로 전환

온보드 키 관리로 전환하려면 온보드 키 관리를 활성화하기 전에 외부 키 관리 구성을 삭제하세요.

시작하기 전에

- 하드웨어 기반 암호화의 경우 모든 FIPS 드라이브 또는 SED의 데이터 키를 기본값으로 재설정해야 합니다.

  "FIPS 드라이브 또는 SED를 보호되지 않는 모드로 되돌리는 중입니다"

- 모든 외부 키 관리자 연결을 삭제해야 합니다.

  "외부 키 관리자 연결을 삭제하는 중입니다"

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

키 관리를 전환하는 단계는 사용 중인 ONTAP 버전에 따라 다릅니다.

ONTAP 9.6 이상

1. 고급 권한 레벨로 변경:

   세트 프리빌리지 고급

2. 다음 명령을 사용합니다.

   'Security key-manager external disable-vserver_admin_SVM_'

   MetroCluster 환경에서는 admin SVM에 대해 두 클러스터 모두에서 명령을 반복해야 합니다.

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

ONTAP 9.5 이하

'Security key-manager delete-KMIP-config' 명령어를 사용한다

자세히 알아보세요 `security key-manager delete-kmip-config` 에서"ONTAP 명령 참조입니다" .

관련 정보

- "보안 키 관리자 외부 비활성화"

ONTAP 부팅 프로세스 중에 키 관리 서버에 접속할 수 없는 경우 어떻게 됩니까?

ONTAP는 NSE에 구성된 스토리지 시스템이 부팅 프로세스 중 지정된 키 관리 서버에 연결할 수 없는 경우 원치 않는 동작을 방지하기 위해 특정 예방 조치를 취합니다.

스토리지 시스템이 NSE에 맞게 구성되고 SED가 리키 입력 및 잠겨 있고 SED의 전원이 켜져 있는 경우, 스토리지 시스템은 SED에 액세스하기 전에 키 관리 서버에서 필요한 인증 키를 검색하여 SED에 대한 자체 인증을 해야 합니다.

스토리지 시스템은 지정된 키 관리 서버에 최대 3시간 동안 접속을 시도합니다. 이 시간 이후에 스토리지 시스템이 해당 시스템에 연결할 수 없는 경우 부팅 프로세스가 중지되고 스토리지 시스템이 중지됩니다.

스토리지 시스템이 지정된 키 관리 서버에 성공적으로 접속하면 최대 15분 동안 SSL 연결을 시도합니다. 스토리지 시스템이 지정된 키 관리 서버와 SSL 연결을 설정할 수 없는 경우 부팅 프로세스가 중지되고 스토리지 시스템이 중지됩니다.

스토리지 시스템이 키 관리 서버에 연결하여 연결을 시도하는 동안 CLI에서 실패한 연결 시도에 대한 자세한 정보가 표시됩니다. Ctrl+C를 누르면 언제든지 연결 시도를 중단할 수 있습니다

보안 조치로서 SED는 제한된 수의 무단 액세스 시도만 허용하며, 그 이후에는 기존 데이터에 대한 액세스를 차단합니다. 스토리지 시스템이 지정된 키 관리 서버에 연결할 수 없어 적절한 인증 키를 얻을 수 없는 경우 기본 키로만 인증을 시도하여 시도 실패 및 패닉이 발생할 수 있습니다. 패닉이 발생할 경우 스토리지 시스템이 자동으로 재부팅되도록 구성된 경우 부팅 루프로 진입하여 SED에서 지속적인 인증 실패를 초래하게 됩니다.

이러한 시나리오에서 스토리지 시스템을 중단하는 것은 스토리지 시스템이 부팅 루프에 진입하지 못하도록 하는 것으로, SED가 영구적으로 잠기면 특정 횟수의 연속 인증 실패 횟수를 초과하여 의도하지 않은 데이터가 손실될 수 있습니다. 잠금 보호의 제한 및 유형은 제조 사양 및 SED 유형에 따라 다릅니다.

SED 유형	연속 실패한 인증 시도 횟수로 인해 잠금이 발생합니다	안전 한도에 도달하면 잠금 보호 유형입니다
HDD	1024	영구. 적절한 인증 키를 다시 사용할 수 있는 경우에도 데이터를 복구할 수 없습니다.
펌웨어 버전 NA00 또는 NA01이 있는 X440_PHM2800MCTO 800GB NSE SSD	5	임시. 잠금 기능은 디스크 전원을 껐다가 다시 켤 때까지만 적용됩니다.
펌웨어 버전 NA00 또는 NA01이 있는 X577_PHM2800MCTO 800GB NSE SSD	5	임시. 잠금 기능은 디스크 전원을 껐다가 다시 켤 때까지만 적용됩니다.
더 높은 펌웨어 버전의 X440_PHM2800MCTO 800GB NSE SSD	1024	영구. 적절한 인증 키를 다시 사용할 수 있는 경우에도 데이터를 복구할 수 없습니다.
펌웨어 버전이 더 높은 X577_PHM2800MCTO 800GB NSE SSD	1024	영구. 적절한 인증 키를 다시 사용할 수 있는 경우에도 데이터를 복구할 수 없습니다.
그 외 모든 SSD 모델	1024	영구. 적절한 인증 키를 다시 사용할 수 있는 경우에도 데이터를 복구할 수 없습니다.

모든 SED 유형의 경우 인증에 성공하면 시도 횟수가 0으로 재설정됩니다.

지정된 키 관리 서버에 도달하지 못해 스토리지 시스템이 중단된 경우 스토리지 시스템 부팅을 계속 시도하기 전에 먼저 통신 장애의 원인을 파악하고 수정해야 합니다.

기본적으로 **ONTAP** 암호화 비활성화

ONTAP 9.7부터 볼륨 암호화(VE) 라이센스가 있고 온보드 키 관리자 또는 외부 키 관리자를 사용하는 경우 애그리게이트 및 볼륨 암호화가 기본적으로 활성화됩니다. 필요한 경우 전체 클러스터에 대해 암호화를 기본적으로 사용하지 않도록 설정할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자이거나 클러스터 관리자가 권한을 위임한 SVM 관리자여야 합니다.

단계

1. ONTAP 9.7 이상에서 전체 클러스터에 대해 기본적으로 암호화를 사용하지 않도록 설정하려면 다음 명령을 실행합니다.

   'options-option-name encryption.data_at_rest_encryption.disable_by_default-option-value on’입니다