CLI를 사용하여 암호화를 관리합니다

ONTAP 9

NetApp
February 12, 2026

목차

CLI를 사용하여 암호화를 관리합니다

ONTAP 저장 데이터 암호화에 대해 알아보세요

NetApp은 스토리지 미디어가 용도 변경, 반환, 잘못된 위치 또는 도난된 경우 유휴 데이터를 읽을 수 없도록 소프트웨어 및 하드웨어 기반 암호화 기술을 모두 제공합니다.

- NVE(NetApp Volume Encryption)를 사용하는 소프트웨어 기반 암호화는 한 번에 하나의 볼륨 데이터 암호화를 지원합니다
- NSE(NetApp Storage Encryption)를 사용하는 하드웨어 기반 암호화는 데이터의 쓰기 시 전체 디스크 암호화(FDE)를 지원합니다.

NetApp 볼륨 및 집계 암호화 구성

ONTAP NetApp 볼륨 및 집계 암호화에 대해 알아보세요

NetApp Volume Encryption(NVE)은 유휴 데이터를 한 번에 하나의 볼륨으로 암호화하는 소프트웨어 기반 기술입니다. 스토리지 시스템에서만 액세스할 수 있는 암호화 키를 사용하면 기본 장치를 용도 변경, 반환, 잘못된 위치 변경 또는 도난 당한 경우 볼륨 데이터를 읽을 수 없습니다.

NVE 이해

NVE를 사용하면 메타데이터와 데이터(스냅샷 포함)가 모두 암호화됩니다. 데이터에 대한 액세스는 볼륨별로 고유한 XTS-AES-256 키를 통해 제공됩니다. 외부 키 관리 서버 또는 온보드 키 관리자(OKM)는 노드에 키를 제공합니다.

- 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 키를 제공하는 기본 제공 툴입니다.

ONTAP 9.7부터 볼륨 암호화(VE) 라이센스가 있고 온보드 키 관리자 또는 외부 키 관리자를 사용하는 경우 애그리게이트 및 볼륨 암호화가 기본적으로 활성화됩니다. VE 라이센스는 에 포함되어 "ONTAP 1 을 참조하십시오 "있습니다. 외부 또는 온보드 키 관리자를 구성할 때마다 새로운 애그리게이트 및 완전히 새로운 볼륨에 대해 유휴 데이터 암호화를 구성하는 방식이 변경됩니다. 새로운 애그리게이트에 NetApp NAE(Aggregate Encryption)가 기본적으로 사용되도록 설정됩니다. NAE 애그리게이트에 포함되지 않은 새로운 볼륨의 경우 기본적으로 NVE(NetApp Volume Encryption)가 활성화됩니다. 멀티 테넌트(multi-tenant) 키 관리를 사용하여 데이터 스토리지 가상 시스템(SVM)을 자체 키 관리자로 구성한 경우, SVM용으로 생성된 볼륨은 NVE로 자동으로 구성됩니다.

새 볼륨이나 기존 볼륨에서 암호화를 활성화할 수 있습니다. NVE는 중복제거, 압축을 비롯한 광범위한 스토리지 효율성 기능을 지원합니다. ONTAP 9.14.1부터 가능합니다 기존 SVM 루트 볼륨에서 NVE를 활성화합니다.

> SnapLock를 사용하는 경우 비어 있는 새 SnapLock 볼륨에서만 암호화를 활성화할 수 있습니다. 기존 SnapLock 볼륨에서는 암호화를 활성화할 수 없습니다.

NVE는 모든 유형의 애그리게이트(HDD, SSD, 하이브리드, 어레이 LUN), RAID 유형, ONTAP Select를 비롯한 지원되는 모든 ONTAP 구현에서 사용할 수 있습니다. 또한 하드웨어 기반 암호화와 NVE를 사용하여 자체 암호화

드라이브에서 데이터를 "이중 암호화"할 수 있습니다.

NVE가 활성화되면 코어 덤프도 암호화됩니다.

애그리게이트 레벨 암호화

일반적으로 암호화된 모든 볼륨에 고유한 키가 할당됩니다. 볼륨이 삭제되면 키와 함께 삭제됩니다.

ONTAP 9.6부터는 _NetApp 애그리게이트 암호화(NAE)_를 사용하여 암호화할 볼륨의 포함된 애그리게이트에 키를 할당할 수 있습니다. 암호화된 볼륨이 삭제되면 애그리게이트의 키가 유지됩니다. 키가 전체 Aggregate가 삭제된 경우 삭제됩니다.

인라인 또는 백그라운드 애그리게이트 레벨 중복제거를 수행하려는 경우 애그리게이트 레벨 암호화를 사용해야 합니다. 그 외에는 NVE에서 애그리게이트 레벨의 중복제거가 지원되지 않습니다.

ONTAP 9.7부터 볼륨 암호화(VE) 라이센스가 있고 온보드 키 관리자 또는 외부 키 관리자를 사용하는 경우 애그리게이트 및 볼륨 암호화가 기본적으로 활성화됩니다.

NVE 볼륨과 NAE 볼륨이 동일한 애그리게이트에 공존할 수 있습니다. 애그리게이트 레벨 암호화로 암호화된 볼륨은 기본적으로 NAE 볼륨입니다. 볼륨을 암호화할 때 기본값을 재정의할 수 있습니다.

'volume move' 명령을 사용하여 NVE 볼륨을 NAE 볼륨으로 변환하거나 그 반대로 변환할 수 있습니다. NAE 볼륨을 NVE 볼륨으로 복제할 수 있습니다.

NAE 볼륨에서는 'Secure purge' 명령어를 사용할 수 없다.

외부 키 관리 서버를 사용하는 경우

일반적으로 온보드 키 관리자를 사용하는 것이 더 저렴하고 더 편리하긴 하지만, 다음 중 하나라도 해당하는 경우 KMIP 서버를 설치해야 합니다.

- 암호화 키 관리 솔루션은 FIPS(Federal Information Processing Standards) 140-2 또는 KMIP OASIS KMIP 표준을 준수해야 합니다.
- 암호화 키를 중앙 집중식으로 관리하는 다중 클러스터 솔루션이 필요합니다.
- 기업은 인증 키를 시스템 또는 데이터와 다른 위치에 저장하는 추가적인 보안을 필요로 합니다.

외부 키 관리의 범위

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 명명된 SVM에 대한 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.
  - ONTAP 9.17.1부터 다음을 사용할 수 있습니다. 바비칸 KMS 데이터 SVM에 대해서만 NVE 키를 보호합니다.
  - ONTAP 9.10.1부터 를 사용할 수 있습니다 Azure Key Vault 및 Google Cloud KMS 데이터 SVM에 대해서만 NVE 키를 보호합니다. 이 기능은 9.12.0부터 AWS의 KMS에 사용할 수 있습니다.

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.

검증된 외부 키 관리자 목록은 에서 확인할 수 있습니다 "NetApp 상호 운용성 매트릭스 툴(IMT)". IMT의 검색 기능에 "Key Manager"라는 용어를 입력하면 이 목록을 확인할 수 있습니다.

Azure Key Vault 및 AWS KMS와 같은 클라우드 KMS 공급자는 KMIP를 지원하지 않습니다. 따라서 IMT에 나열되지 않습니다.

지원 세부 정보

다음 표에는 NVE 지원 세부사항이 나와 있습니다.

리소스 또는 기능	지원 세부 정보
플랫폼	AES-NI 오프로드 기능이 필요합니다. 해당 플랫폼에서 NVE와 NAE가 지원되는지 확인하려면 HWU(Hardware Universe)를 참조하십시오.
암호화	ONTAP 9.7부터 볼륨 암호화(VE) 라이센스를 추가하고 온보드 또는 외부 키 관리자를 구성한 경우 새로 생성된 애그리게이트 및 볼륨이 기본적으로 암호화됩니다. 암호화되지 않은 Aggregate를 생성해야 하는 경우 다음 명령을 사용합니다. '스토리지 집계 생성-암호화-집계-키 거짓'을 사용합니다 일반 텍스트 볼륨을 만들어야 하는 경우 다음 명령을 사용합니다. 볼륨 만들기-암호화 거짓 다음과 같은 경우 암호화가 기본적으로 활성화되지 않습니다. • VE 라이센스가 설치되지 않았습니다. • 키 관리자가 구성되지 않았습니다. • 플랫폼 또는 소프트웨어는 암호화를 지원하지 않습니다. • 하드웨어 암호화가 활성화됩니다.
ONTAP	모든 ONTAP 구현. Cloud Volumes ONTAP 지원은 ONTAP 9.5 이상에서 제공됩니다.
장치	HDD, SSD, 하이브리드, 어레이 LUN
RAID	RAID0, RAID4, RAID-DP, RAID-TEC.
볼륨	데이터 볼륨 및 기존 SVM 루트 볼륨. MetroCluster 메타데이터 볼륨의 데이터는 암호화할 수 없습니다. 9.14.1 이전 버전의 ONTAP에서는 NVE를 통해 SVM 루트 볼륨의 데이터를 암호화할 수 없습니다. ONTAP 9.14.1부터 ONTAP는 를 지원합니다 SVM 루트 볼륨에 NVE.

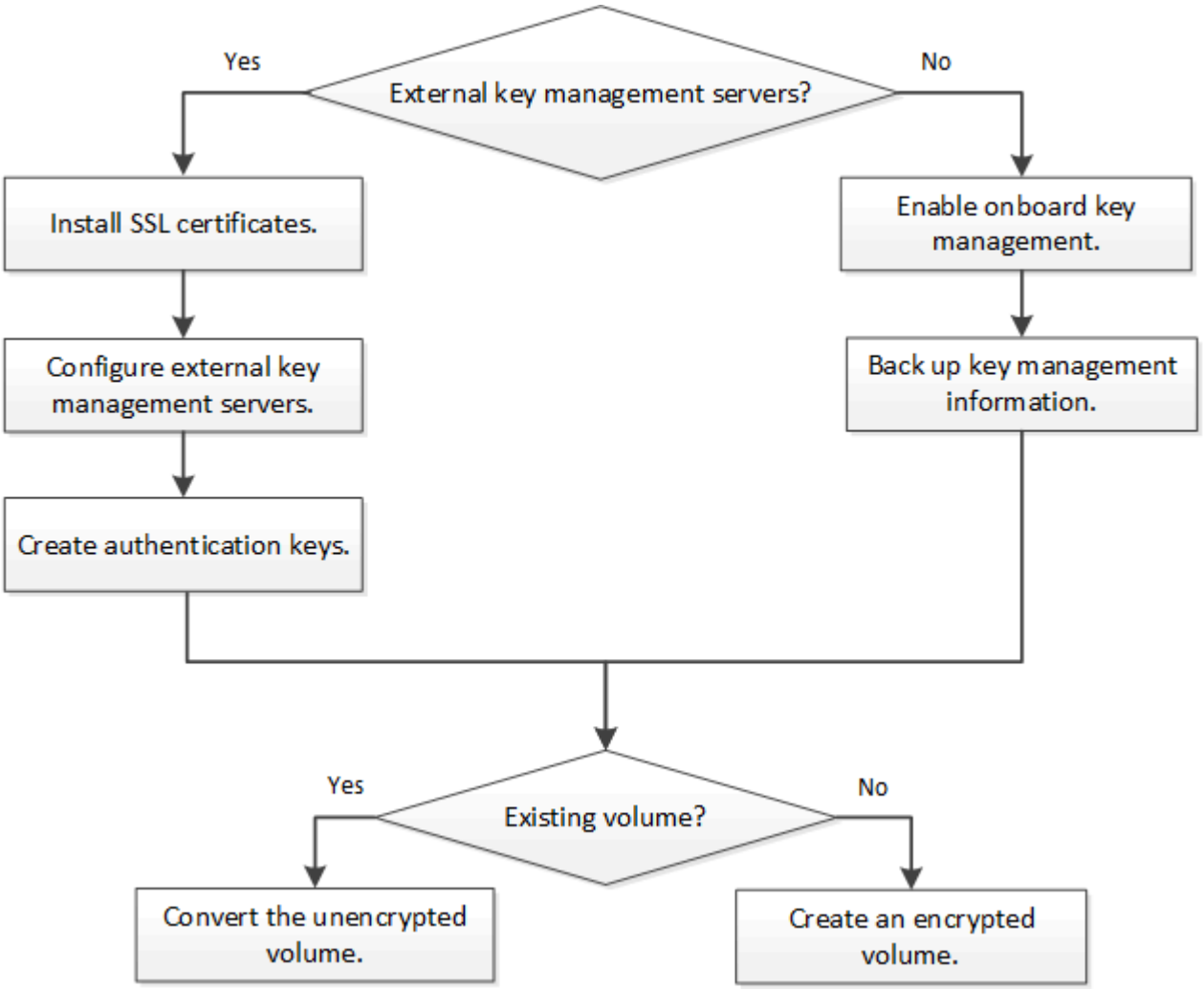
애그리게이트 레벨 암호화	ONTAP 9.6부터 NVE는 Aggregate 레벨의 암호화(NAE)를 지원합니다. • 인라인 또는 백그라운드 애그리게이트 레벨 중복제거를 수행하려는 경우 애그리게이트 레벨 암호화를 사용해야 합니다. • 집계 수준 암호화 볼륨을 다시 설정할 수 없습니다. • 애그리게이트 레벨 암호화 볼륨에서는 보안 제거가 지원되지 않습니다. • NAE는 데이터 볼륨 외에 SVM 루트 볼륨 및 MetroCluster 메타데이터 볼륨의 암호화를 지원합니다. NAE는 루트 볼륨 암호화를 지원하지 않습니다.
SVM 범위	MetroCluster 는 ONTAP 9.8부터 지원됩니다. ONTAP 9.6부터 NVE는 Onboard Key Manager가 아닌 외부 키 관리에 대해서만 SVM 범위를 지원합니다.
스토리지 효율성	중복제거, 압축, 컴팩션, FlexClone: 클론은 상위 클론에서 클론을 분할한 후에도 상위 클론과 동일한 키를 사용합니다. 를 수행해야 합니다 `volume move` 분할된 클론에서 분할된 클론에는 다른 키가 있습니다.
복제	• 볼륨 복제의 경우 소스 볼륨과 대상 볼륨의 암호화 설정이 다를 수 있습니다. 소스에 대해 암호화를 구성할 수 있고 대상에 대해 구성되지 않을 수도 있습니다. 소스에 구성된 암호화는 대상에 복제되지 않습니다. 소스 및 대상에서 암호화를 수동으로 구성해야 합니다. NVE를 구성합니다및 NVE를 사용하여 볼륨 데이터 암호화을 참조하십시오. • SVM 복제의 경우, 볼륨 암호화를 지원하는 노드가 타겟에 포함되지 않은 경우, 복제가 성공하지만 타겟 볼륨이 암호화되지 않은 한 타겟 볼륨이 자동으로 암호화됩니다. • MetroCluster 구성의 경우 각 클러스터는 구성된 키 서버에서 외부 키 관리 키를 가져옵니다. OKM 키는 구성 복제 서비스에 의해 파트너 사이트에 복제됩니다.
규정 준수	SnapLock 은 새로운 볼륨에 대해서만 규정 준수 및 엔터프라이즈 모드에서 모두 지원됩니다. 기존 SnapLock 볼륨에서는 암호화를 활성화할 수 없습니다.
FlexGroup 볼륨	FlexGroup 볼륨이 지원됩니다. 대상 애그리게이트는 소스 애그리게이트와 볼륨 레벨 또는 애그리게이트 레벨에서 동일한 유형이어야 합니다. ONTAP 9.5부터 FlexGroup 볼륨을 제자리에서 다시 입력하다
7-Mode 전환	7-Mode 전환 툴 3.3부터는 7-Mode 전환 툴 CLI를 사용하여, 클러스터링된 시스템의 NVE 지원 대상 볼륨으로의 복사본 기반 전환을 수행할 수 있습니다.

관련 정보

- "FAQ - NetApp 볼륨 암호화 및 NetApp 애그리게이트 암호화"
- "저장소 집계 생성"

ONTAP NetApp 볼륨 암호화 워크플로

볼륨 암호화를 활성화하려면 키 관리 서비스를 구성해야 합니다. 새 볼륨이나 기존 볼륨에서 암호화를 활성화할 수 있습니다.



"VE 라이센스를 설치해야 합니다" 그리고 NVE로 데이터를 암호화하기 전에 키 관리 서비스를 구성합니다. 라이센스를 설치하기 전에 다음을 수행해야 "ONTAP 버전이 NVE를 지원하는지 확인합니다"합니다.

NVE를 구성합니다

ONTAP 클러스터 버전이 **NVE**를 지원하는지 확인하세요**.**

라이센스를 설치하기 전에 클러스터 버전이 NVE를 지원하는지 확인해야 합니다. sion 명령을 사용하여 클러스터 버전을 확인할 수 있습니다.

이 작업에 대해

클러스터 버전은 클러스터의 모든 노드에서 실행되는 ONTAP의 가장 낮은 버전입니다.

단계

1. 클러스터 버전이 NVE를 지원하는지 확인

안절부절부절부절도

명령 출력에 "no Data at Rest Encryption" 텍스트가 표시되는 경우 또는 에 나와 있지 않은 플랫폼을 사용하는 경우에는 NVE가 지원되지 않습니다 `1Ono-DARE`"지원 세부 정보".

ONTAP 클러스터에 볼륨 암호화 라이선스 설치

VE 라이센스를 사용하면 클러스터의 모든 노드에서 이 기능을 사용할 수 있습니다. 이 라이센스는 NVE로 데이터를 암호화하기 전에 필요합니다. 에 포함되어 "ONTAP 1 을 참조하십시오"있습니다.

ONTAP One 이전에는 VE 라이센스가 암호화 번들에 포함되어 있었습니다. 암호화 번들이 더 이상 제공되지 않지만 여전히 유효합니다. 현재는 필요하지 않지만 기존 고객은 선택할 수 "ONTAP One으로 업그레이드하십시오"있습니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 영업 담당자로부터 VE 라이센스 키를 받았거나 ONTAP One이 설치되어 있어야 합니다.

단계

1. "VE 라이센스가 설치되어 있는지 확인합니다"..

   VE 라이센스 패키지 이름은 입니다 `VE`.

2. 라이센스가 설치되지 않은 경우"System Manager 또는 ONTAP CLI를 사용하여 설치합니다".

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 **NVE**에 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"

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 **SVM**에 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
```

ONTAP 9.6 이상에서 **NVE**에 대한 온보드 키 관리 활성화

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 동기화 명령을 실행해야 합니다.

MetroCluster 구성이 있는 경우 을 실행해야 합니다 `security key-manager onboard enable` 먼저 로컬 클러스터에서 명령을 실행한 다음 를 실행합니다 `security key-manager onboard sync` 원격 클러스터에 대해 동일한 암호를 사용하여 명령을 실행합니다. 를 실행할 때 `security key-manager onboard enable` 로컬 클러스터에서 명령을 실행한 다음 원격 클러스터에서 동기화하면 를 실행할 필요가 없습니다 `enable` 명령을 원격 클러스터에서 다시 수행합니다.

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. 재부팅 후 사용자가 암호를 입력하도록 요구하려면 'cc-mode-enabled=yes' 옵션을 사용할 수 있습니다.

NVE의 경우 cc-mode-enabled=yes를 설정하면 볼륨 생성, 볼륨 이동 시작 명령을 사용하여 생성한 볼륨이 자동으로 암호화됩니다. 볼륨 만들기에는 -encrypt true를 지정할 필요가 없습니다. 볼륨 이동 시작의 경우 -encrypt-destination true를 지정하지 않아도 됩니다.

CSfC(Commercial Solutions for Classified) 요구 사항을 충족하기 위해 ONTAP 저장 데이터 암호화를 구성할 때 NSE와 NVE를 함께 사용해야 하며, Common Criteria 모드에서 Onboard Key Manager가 활성화되어 있는지 확인해야 합니다. 보다"CSDC 솔루션 요약" .

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.

  클러스터 암호를 5번 입력하지 못하면 24시간을 기다리거나 노드를 재부팅하여 제한을 재설정하세요.

- 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. 검증에 성공하면 시스템은 이미지 업데이트 프로세스의 다음 단계로 진행합니다. 그렇지 않으면 이미지 업데이트에 실패합니다. 자세히 알아보세요 `cluster image` 에서"ONTAP 명령 참조입니다" .

온보드 키 관리자는 키를 휘발성 메모리에 저장합니다. 휘발성 메모리 내용은 시스템이 재부팅되거나 중단되면 지워집니다. 시스템은 중단되면 30초 이내에 휘발성 메모리를 지웁니다.

시작하기 전에

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

단계

1. 키 관리자 설정을 시작합니다.

   '보안 키 관리자 온보드 활성화-cc-모드 사용 예|아니오'

   재부팅 후 키 관리자 암호를 입력하도록 하려면 'cc-mode-enabled=yes'를 설정합니다. NVE의 경우 cc-mode-enabled=yes를 설정하면 볼륨 생성, 볼륨 이동 시작 명령을 사용하여 생성한 볼륨이 자동으로 암호화됩니다. MetroCluster 구성에서는 '-cc-mode-enabled' 옵션이 지원되지 않습니다. 보안 키매니저 온보드 활성화 명령은 보안 키매니저 설정 명령을 대체합니다.

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. 인증 키가 생성되었는지 확인합니다.

   '보안 키 관리자 키 쿼리 - 키 유형 NSE-AK'

   `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.

5. 선택적으로 일반 텍스트 볼륨을 암호화된 볼륨으로 변환할 수 있습니다.

   ```
   volume encryption conversion start
   ```

   볼륨을 변환하기 전에 Onboard Key Manager를 완전히 구성해야 합니다. MetroCluster 환경에서는 두 사이트 모두에서 Onboard Key Manager를 구성해야 합니다.

작업을 마친 후

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

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

관련 정보

- "클러스터 이미지 명령"
- "보안 키 관리자 외부 활성화"
- "보안 키 관리자 키 쿼리"

- "보안 키 관리자 온보드 활성화"

ONTAP 9.5 및 이전 버전에서 **NVE**에 대한 온보드 키 관리 활성화

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 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 NSE 또는 NVE를 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`

```
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
```

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

6. 필요한 경우 일반 텍스트 볼륨을 암호화된 볼륨으로 변환합니다.

   ```
   volume encryption conversion start
   ```

   볼륨을 변환하기 전에 Onboard Key Manager를 구성하세요. MetroCluster 환경에서는 두 사이트 모두에 구성합니다.

작업을 마친 후

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

온보드 키 관리자 암호를 구성할 때 재해 발생에 대비해 저장 시스템 외부의 안전한 위치에 정보를 백업하세요. 보다 "온보드 키 관리 정보를 수동으로 백업합니다" .

관련 정보

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

새로 추가된 **ONTAP** 노드에서 온보드 키 관리 활성화

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.

ONTAP 9.6 이상의 경우 다음을 실행해야 합니다. `security key-manager onboard sync` 클러스터에 노드를 추가할 때마다 명령을 실행합니다.

ONTAP 9.5 이전 버전의 경우, 클러스터에 노드를 추가할 때마다 '보안 키 관리자 설정' 명령을 실행해야 합니다.

온보드 키 관리 기능을 사용하여 클러스터에 노드를 추가하는 경우 이 명령을 실행하여 누락된 키를 새로 고칩니다.

MetroCluster 구성이 있는 경우 다음 지침을 검토하십시오.

- ONTAP 9.6부터 로컬 클러스터에서 보안 키 관리자 온보드 활성화를 먼저 실행한 다음 원격 클러스터에서 동일한 암호를 사용하여 보안 키 관리자 온보드 동기화를 실행해야 합니다.

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

- 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.

암호 입력에 실패하면 노드를 재부팅하세요. 재부팅 후 암호를 다시 입력해보세요.

관련 정보

- "클러스터 이미지 명령"
- "보안 키 관리자 외부 활성화"
- "보안 키 관리자 온보드 활성화"

NVE 또는 NAE를 사용하여 볼륨 데이터 암호화

NVE를 사용하여 **ONTAP** 볼륨 데이터를 암호화하는 방법에 대해 알아보세요.

ONTAP 9.7부터는 VE 라이센스 및 온보드 키 또는 외부 키 관리 기능이 있는 경우 기본적으로 애그리게이트 및 볼륨 암호화가 활성화됩니다. ONTAP 9.6 이하 버전의 경우 새 볼륨 또는 기존 볼륨에서 암호화를 활성화할 수 있습니다. 볼륨 암호화를 활성화하려면 VE 라이센스를 설치하고 키 관리를 활성화해야 합니다. NVE는 FIPS-140-2 레벨 1을 준수합니다.

ONTAP에서 **VE** 라이센스를 사용하여 애그리게이트 수준 암호화를 활성화합니다

ONTAP 9.7부터"VE 라이센스", 온보드 키 또는 외부 키 관리가 있는 경우 새로 생성된 애그리게이트와 볼륨은 기본적으로 암호화됩니다. ONTAP 9.6부터 애그리게이트 레벨 암호화를 사용하여 암호화할 볼륨에 포함된 애그리게이트에 키를 할당할 수 있습니다.

이 작업에 대해

인라인 또는 백그라운드 애그리게이트 레벨 중복제거를 수행하려는 경우 애그리게이트 레벨 암호화를 사용해야 합니다. 그 외에는 NVE에서 애그리게이트 레벨의 중복제거가 지원되지 않습니다.

애그리게이트 레벨 암호화를 위해 활성화된 애그리게이트를 *NAE aggregate*(NetApp 애그리게이트 암호화의 경우)라고 합니다. NAE 애그리게이트의 모든 볼륨은 NAE 또는 NVE 암호화로 암호화되어야 합니다. Aggregate 레벨의 암호화를 사용하면 Aggregate에서 생성한 볼륨이 NAE 암호화로 기본적으로 암호화됩니다. 대신 NVE 암호화를 사용하도록 기본값을 재정의할 수 있습니다.

NAE 애그리게이트에서는 일반 텍스트 볼륨이 지원되지 않습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 애그리게이트 레벨 암호화 활성화 또는 비활성화:

대상…	이 명령 사용…
ONTAP 9.7 이상을 사용하여 NAE 애그리게이트를 생성합니다	`storage aggregate create -aggregate aggregate_name -node node_name`

ONTAP 9.6으로 NAE 애그리게이트를 생성합니다	`storage aggregate create -aggregate aggregate_name -node node_name -encrypt-with -aggr-key true`
NAE가 아닌 집계를 NAE 집계로 변환합니다	`storage aggregate modify -aggregate aggregate_name -node node_name -encrypt-with -aggr-key true`
NAE 집계를 NAE가 아닌 집집합으로 변환합니다	`storage aggregate modify -aggregate aggregate_name -node node_name -encrypt-with -aggr-key false`

자세히 알아보세요 `storage aggregate modify` 에서 "ONTAP 명령 참조입니다" .

다음 명령을 실행하면 "aggr1"에서 집계 수준 암호화가 활성화됩니다.

- ONTAP 9.7 이상:

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

- ONTAP 9.6 이하:

```
cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with
-aggr-key true
```

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

2. Aggregate가 암호화를 사용하도록 설정되어 있는지 확인합니다.

'스토리지 집계 표시 필드 암호화 - 집계 키 사용'

다음 명령을 실행하면 "aggr1"이 암호화에 대해 활성화되어 있는지 확인합니다.

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key
aggregate            encrypt-aggr-key
-------------------- ----------------
aggr0_vsim4          false
aggr1                true
2 entries were displayed.
```

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

작업을 마친 후

'volume create' 명령을 실행하여 암호화된 볼륨을 생성합니다.

KMIP 서버를 사용하여 노드의 암호화 키를 저장하는 경우, ONTAP는 볼륨을 암호화할 때 암호화 키를 서버에 자동으로 "푸시"(푸시)"합니다.

ONTAP에서 새 볼륨에 대해 암호화를 활성화합니다

'volume create' 명령을 사용하여 새 볼륨에서 암호화를 활성화할 수 있습니다.

이 작업에 대해

NVE(NetApp Volume Encryption)를 사용하여 볼륨을 암호화하고 ONTAP 9.6, NetApp Aggregate Encryption(NAE)로 시작할 수 있습니다. NAE와 NVE에 대한 자세한 내용은 를 참조하십시오 볼륨 암호화 개요.

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

ONTAP에서 새 볼륨에 대한 암호화를 활성화하는 절차는 사용 중인 ONTAP 버전과 특정 구성에 따라 다릅니다.

- ONTAP 9.4부터 시작합니다(사용하는 경우) `cc-mode` Onboard Key Manager(온보드 키 관리자)를 설정할 때 로 생성한 볼륨입니다 `volume create` 명령은 사용자가 지정하든 관계없이 자동으로 암호화됩니다 `-encrypt true`.
- ONTAP 9.6 및 이전 버전에서는 을 사용해야 합니다 `-encrypt true` 와 함께 `volume create` 암호화를 활성화하는 명령(사용하지 않은 경우 `cc-mode`)를 클릭합니다.
- ONTAP 9.6에서 NAE 볼륨을 작성하려면 집계 수준에서 NAE를 활성화해야 합니다. 을 참조하십시오 VE 라이센스로 애그리게이트 레벨 암호화를 설정합니다 를 참조하십시오.
- ONTAP 9.7부터, "VE 라이센스"온보드 키 또는 외부 키 관리가 있는 경우 새로 생성된 볼륨이 기본적으로 암호화됩니다. 기본적으로 NAE 애그리게이트에서 생성된 새 볼륨은 NVE가 아닌 NAE 유형이 됩니다.
  - ONTAP 9.7 이상 릴리즈에서 추가하는 경우 `-encrypt true` 를 누릅니다 `volume create` NAE 애그리게이트에서 볼륨을 생성하는 명령은 볼륨에 NAE 대신 NVE 암호화가 있습니다. NAE 애그리게이트의 모든 볼륨은 NVE 또는 NAE로 암호화되어야 합니다.

NAE 애그리게이트에서는 일반 텍스트 볼륨이 지원되지 않습니다.

단계

1. 새 볼륨을 생성하고 볼륨에 암호화가 활성화되어 있는지 여부를 지정합니다. 새 볼륨이 NAE 애그리게이트에 있는 경우 기본적으로 볼륨은 다음 NAE 볼륨이 됩니다.

생성 방법…	이 명령 사용…
NAE 볼륨	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`*

NVE 볼륨	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt true` 를 누릅니다 NAE가 지원되지 않는 ONTAP 9.6 및 이전 버전에서는 `-encrypt true` NVE를 사용하여 볼륨을 암호화하도록 지정합니다. NAE 애그리게이트에서 볼륨이 생성되는 ONTAP 9.7 이상에서는 `-encrypt true` 대신 NAE의 기본 암호화 유형을 재정의하여 NVE 볼륨을 생성합니다.
일반 텍스트 볼륨입니다	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt false`

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

2. 볼륨에 암호화가 설정되어 있는지 확인합니다.

   볼륨 쇼는 암호화된 사실이다

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

결과

KMIP 서버를 사용하여 노드의 암호화 키를 저장하는 경우, ONTAP는 볼륨을 암호화할 때 암호화 키를 서버에 자동으로 "푸시" 합니다.

기존 **ONTAP** 볼륨에서 **NAE** 또는 **NVE** 활성화

둘 중 하나를 사용할 수 있습니다 `volume move start` 또는 을 누릅니다 `volume encryption conversion start` 기존 볼륨에서 암호화를 활성화하는 명령입니다.

이 작업에 대해

당신은 사용할 수 있습니다 `volume encryption conversion start` 볼륨을 다른 위치로 이동하지 않고도 기존 볼륨의 암호화를 "현재 위치"에서 활성화하는 명령입니다. 또는 다음을 사용할 수 있습니다. `volume move start` 명령.

볼륨 암호화 변환 시작 명령을 사용하여 기존 볼륨에서 암호화를 활성화합니다

당신은 사용할 수 있습니다 `volume encryption conversion start` 볼륨을 다른 위치로 옮기지 않고도 기존 볼륨의 암호화를 "그대로" 활성화하는 명령입니다.

변환 작업을 시작한 후에는 작업을 완료해야 합니다. 작업 중에 성능 문제가 발생하면 를 실행할 수 있습니다 `volume encryption conversion pause` 명령을 사용하여 작업을 일시 중지하고, 를 클릭합니다 `volume encryption conversion resume` 명령을 사용하여 작업을 재개합니다.

> 를 사용할 수 없습니다 `volume encryption conversion start` SnapLock 볼륨을 변환합니다.

단계

1. 기존 볼륨에서 암호화 활성화:

   '볼륨 암호화 변환 시작 - SVM_NAME - volume volume volume_name'

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

   다음 명령을 실행하면 기존 볼륨의 암호화가 설정됩니다 `vol1`:

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

   시스템에서 볼륨에 대한 암호화 키를 생성합니다. 볼륨의 데이터가 암호화됩니다.

2. 변환 작업의 상태를 확인합니다.

   볼륨 암호화 변환 표시

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

   다음 명령을 실행하면 변환 작업의 상태가 표시됩니다.

   ```
   cluster1::> volume encryption conversion show

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

3. 변환 작업이 완료되면 볼륨이 암호화에 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%
   ```

결과

KMIP 서버를 사용하여 노드의 암호화 키를 저장하는 경우, ONTAP는 볼륨을 암호화할 때 암호화 키를 서버에 자동으로 "푸시"(푸시)"합니다.

볼륨 이동 시작 명령을 사용하여 기존 볼륨에서 암호화를 활성화합니다

명령을 사용하여 기존 볼륨을 이동하여 암호화를 활성화할 수 `volume move start` 있습니다. 동일한 애그리게이트 또는 다른 애그리게이트를 사용할 수 있습니다.

이 작업에 대해

- ONTAP 9.8부터 볼륨 이동 시작을 사용하여 SnapLock 또는 FlexGroup 볼륨에서 암호화를 활성화할 수 있습니다.
- ONTAP 9.4부터 Onboard Key Manager를 설정할 때 ""cc-mode""를 활성화하면 "volume move start" 명령으로 생성한 볼륨이 자동으로 암호화됩니다. `-encrypt-destination true'는 지정하지 않아도 됩니다.
- ONTAP 9.6부터는 Aggregate 수준의 암호화를 사용하여 이동할 볼륨의 포함된 Aggregate에 키를 할당할 수 있습니다. 고유 키로 암호화된 볼륨을 _ NVE 볼륨 _ 이라고 합니다(NetApp 볼륨 암호화를 사용한다는 의미). 애그리게이트 레벨 키로 암호화된 볼륨을 _NAE 볼륨 _ (NetApp 애그리게이트 암호화의 경우)이라고 합니다. NAE 애그리게이트에서는 일반 텍스트 볼륨이 지원되지 않습니다.
- ONTAP 9.14.1부터 NVE로 SVM 루트 볼륨을 암호화할 수 있습니다. 자세한 내용은 을 참조하십시오 SVM 루트 볼륨에 NetApp 볼륨 암호화를 구성합니다.

시작하기 전에

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

"볼륨 이동 명령을 실행하는 위임 권한"

단계

1. 기존 볼륨을 이동하고 볼륨에 암호화가 활성화되어 있는지 여부를 지정합니다.

변환…	이 명령 사용…
NVE 볼륨에 대한 일반 텍스트 볼륨입니다	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination true`
NAE 볼륨에 대한 NVE 또는 일반 텍스트 볼륨(대상에 애그리게이트 레벨 암호화가 사용되는 것으로 가정)	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key true`
NVE 볼륨에 대한 NAE 볼륨	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key false`
Nae 볼륨을 일반 텍스트 볼륨으로	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false -encrypt-with-aggr-key false`
NVE 볼륨을 일반 텍스트 볼륨으로	`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 vol1인 일반 텍스트 볼륨이 NVE 볼륨으로 변환됩니다.

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

대상에서 애그리게이트 레벨 암호화를 사용하도록 설정한 경우 다음 명령을 실행하면 NVE 볼륨이나 일반 텍스트 볼륨 vol1이 NAE 볼륨으로 변환됩니다.

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

다음 명령을 실행하면 이름이 vol2인 NAE 볼륨이 NVE 볼륨으로 변환됩니다.

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-with-aggr-key false
```

다음 명령을 실행하면 이름이 vol2인 NAE 볼륨이 일반 텍스트 볼륨으로 변환됩니다.

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

다음 명령을 실행하면 이름이 vol2인 NVE 볼륨이 일반 텍스트 볼륨으로 변환됩니다.

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false
```

2. 클러스터 볼륨의 암호화 유형을 확인합니다.

   '볼륨 표시 필드 암호화 - 없음|볼륨|집계'를 입력합니다

   암호화 유형 필드는 ONTAP 9.6 이상에서 사용할 수 있습니다.

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

   다음 명령을 실행하면 'cluster2'의 볼륨 암호화 유형이 표시됩니다.

```
cluster2::> volume show -fields encryption-type

vserver  volume  encryption-type
-------  ------  ---------------
vs1      vol1    none
vs2      vol2    volume
vs3      vol3    aggregate
```

3. 볼륨에 암호화가 설정되어 있는지 확인합니다.

   볼륨 쇼는 암호화된 사실이다

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

   다음 명령을 실행하면 암호화된 볼륨이 'cluster2'에 표시됩니다.

```
cluster2::> volume show -is-encrypted true

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

결과

KMIP 서버를 사용하여 노드의 암호화 키를 저장하는 경우, 볼륨을 암호화할 때 ONTAP는 서버에 암호화 키를 자동으로 푸시합니다.

ONTAP SVM 루트 볼륨에 **NVE** 구성

ONTAP 9.14.1부터 스토리지 VM(SVM) 루트 볼륨에서 NetApp 볼륨 암호화(NVE)를 활성화할 수 있습니다. NVE에서는 루트 볼륨을 고유 키로 암호화하여 SVM의 보안을 강화합니다.

이 작업에 대해

SVM 루트 볼륨의 NVE는 SVM이 생성된 후에만 활성화할 수 있습니다.

시작하기 전에

- SVM 루트 볼륨은 NetApp 애그리게이트 암호화(NAE)로 암호화된 애그리게이트에 있어서는 안 됩니다.
- Onboard Key Manager 또는 외부 키 관리자를 사용하여 암호화를 활성화해야 합니다.
- ONTAP 9.14.1 이상을 실행해야 합니다.
- NVE로 암호화된 루트 볼륨이 포함된 SVM을 마이그레이션하려면 마이그레이션이 완료된 후 SVM 루트 볼륨을 일반 텍스트 볼륨으로 변환한 다음 SVM 루트 볼륨을 다시 암호화해야 합니다.
  - SVM 마이그레이션의 타겟 Aggregate에서 NAE를 사용하는 경우 루트 볼륨은 기본적으로 NAE를 상속합니다.
- SVM이 SVM 재해 복구 관계에 있는 경우:

- 미러링된 SVM의 암호화 설정은 대상에 복사되지 않습니다. 소스 또는 대상에서 NVE를 활성화한 경우 미러링된 SVM 루트 볼륨에서 NVE를 별도로 활성화해야 합니다.
- 타겟 클러스터의 모든 애그리게이트가 NAE를 사용하는 경우 SVM 루트 볼륨은 NAE를 사용합니다.

단계

ONTAP CLI 또는 System Manager를 사용하여 SVM 루트 볼륨에서 NVE를 활성화할 수 있습니다.

CLI를 참조하십시오

제자리에서 SVM 루트 볼륨에서 NVE를 사용하거나 애그리게이트 간에 볼륨을 이동하여 활성화할 수 있습니다.

루트 볼륨을 제자리에서 암호화합니다

1. 루트 볼륨을 암호화된 볼륨으로 변환:

   ```
   volume encryption conversion start -vserver svm_name -volume volume
   ```

2. 암호화가 성공했는지 확인합니다. 를 클릭합니다 `volume show -encryption-type volume` NVE를 사용하는 모든 볼륨의 목록을 표시합니다.

SVM 루트 볼륨을 이동하여 암호화

1. 볼륨 이동 시작:

   ```
   volume move start -vserver svm_name -volume volume -destination-aggregate
   aggregate -encrypt-with-aggr-key false -encrypt-destination true
   ```

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

2. 를 확인합니다 `volume move` 에서 작업이 성공했습니다 `volume move show` 명령. 를 클릭합니다 `volume show -encryption-type volume` NVE를 사용하는 모든 볼륨의 목록을 표시합니다.

시스템 관리자

1. 스토리지> 볼륨 으로 이동합니다.
2. 암호화할 SVM 루트 볼륨의 이름 옆에 있는 **Edit** 를 선택합니다 ⋮ .
3. 저장소 및 최적화 제목 아래에서 암호화 활성화 를 선택합니다.
4. 저장을 선택합니다.

ONTAP 노드 루트 볼륨에 **NVE** 구성

ONTAP 9.8부터 NetApp 볼륨 암호화를 사용하여 노드의 루트 볼륨을 보호할 수 있습니다.

이 작업에 대해

이 절차는 노드 루트 볼륨에 적용됩니다. SVM 루트 볼륨에는 적용되지 않습니다. SVM 루트 볼륨은 애그리게이트 레벨 암호화 및 ONTAP 9.14.1부터 NVE.

루트 볼륨 암호화가 시작되면 완료해야 합니다. 작업을 일시 중지할 수 없습니다. 암호화가 완료되면 루트 볼륨에 새 키를 할당할 수 없으며 보안 제거 작업을 수행할 수 없습니다.

시작하기 전에

- 시스템에서 HA 구성을 사용해야 합니다.
- 노드 루트 볼륨이 이미 생성되어 있어야 합니다.
- KMIP(Key Management Interoperability Protocol)를 사용하여 시스템에 온보드 키 관리자 또는 외부 키 관리 서버가 있어야 합니다.

단계

1. 루트 볼륨 암호화:

   ```
   volume encryption conversion start -vserver SVM_name -volume root_vol_name
   ```

2. 변환 작업의 상태를 확인합니다.

   볼륨 암호화 변환 표시

3. 변환 작업이 완료되면 볼륨이 암호화되었는지 확인합니다.

   '볼륨 표시 필드'

   다음은 암호화된 볼륨에 대한 출력 예입니다.

   ```
   ::> volume show -vserver xyz  -volume vol0 -fields is-encrypted
   vserver    volume is-encrypted
   ---------- ------ ------------
   xyz        vol0   true
   ```

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

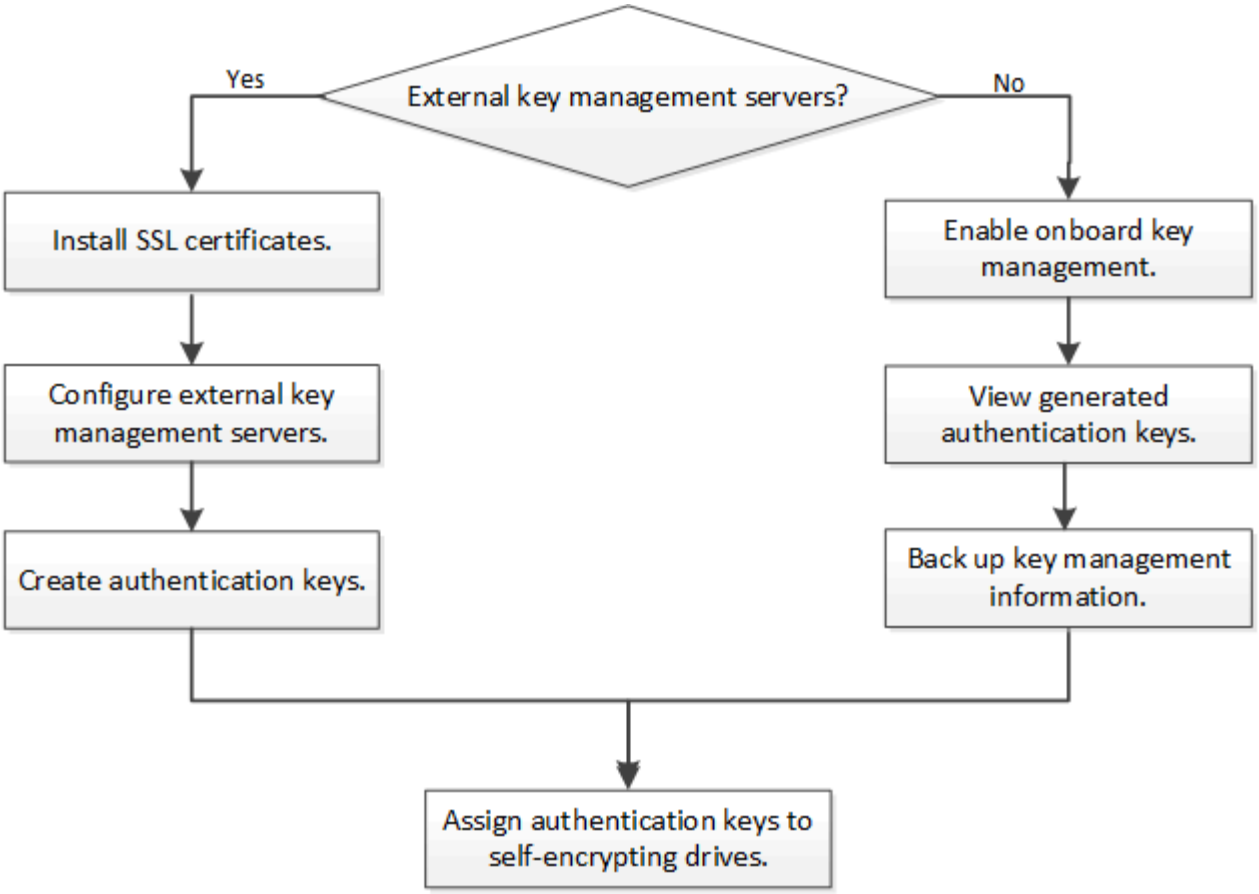
다음 표에는 중요한 하드웨어 암호화 지원 세부 정보가 나와 있습니다. 지원되는 KMIP 서버, 스토리지 시스템 및 디스크 쉘프에 대한 최신 정보는 상호 운용성 매트릭스 를 참조하십시오.

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 **SED**에 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

   `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 **SED**에 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
```

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--------------------------
    TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAAADuD+byAAAAACEAAAAAAAA
    QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
    dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAAAACgAAAAAAAAAAA
    3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAAAA
    IgAAAAAAAAAAAoAAAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAAACAAAAAAAAAAJAGr3tJA/LRzU
    QRHwv+1aWvAAAAAAAAAAAAACQAAAAAAAAAAAgAAAAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
    BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
    AQAAAAMAAAAYAQAAAAAAADA5/ccAAAAAIgAAAAAAAAAAAoAAAAAAAAAAAEOTcR0AAAAA
    AAAAAAAAAAACAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAAAACIAAAAAAAAAAA
    KAAAAAAAAAACI8z/bAAAAAAAAAAAAAAAAAgAAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
    AAAAAAAAAAAkAAAAAAAAAAAIAAAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
    LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAAwAAABgBAAAAAAAAAA
    1cNLLwAAAAAiAAAAAAAAAAAACgAAAAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAAIAAAAAAAkA
    ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAAIgAAAAAAAAAAAoAAAAAAAAAAAJ4/cQsAAAAA
    AAAAAAAAAAACAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAAAACQAAAAAAAAAAA
    gAAAAAAAAAAAN3Zq7AAAAALO7qD20+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 **SED**를 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 **SED**를 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 **SED**에서 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