NVE를 구성합니다

ONTAP 9

NetApp
September 12, 2024

목차

NVE를 구성합니다

클러스터 버전이 NVE를 지원하는지 확인합니다

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 ""1Ono-DARE""" 텍스트(""저장된 데이터 암호화 없음")가 표시되거나 에 나열되지 않은 플랫폼을 사용 중인 경우에는 NVE가 지원되지 않습니다 "지원 세부 정보".

   다음 명령어는 NVE가 'cluster1'에서 지원되는지 여부를 결정합니다.

   ```
   cluster1::> version -v
   NetApp Release 9.1.0: Tue May 10 19:30:23 UTC 2016 <1Ono-DARE>
   ```

   의 출력입니다 `1Ono-DARE` NVE가 클러스터 버전에서 지원되지 않음을 나타냅니다.

라이센스를 설치합니다

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

외부 키 관리 개요 구성

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.

> ONTAP 9.1 이전 버전의 경우 노드 관리 LIF를 외부 키 관리자를 사용하려면 먼저 노드 관리 역할로 구성된 포트에 할당해야 합니다.

NetApp 볼륨 암호화(NVE)는 ONTAP 9.1 이상에서 온보드 키 관리자를 지원합니다. ONTAP 9.3부터 NVE는 외부 키 관리(KMIP) 및 온보드 키 관리자를 지원합니다. ONTAP 9.10.1부터 를 사용할 수 있습니다 Azure Key Vault 또는 Google Cloud Key Manager Service NVE 키를 보호합니다. ONTAP 9.11.1부터는 클러스터의 여러 외부 키 관리자를 구성할 수 있습니다. 을 참조하십시오 클러스터링된 키 서버를 구성합니다.

System Manager로 외부 키 관리자를 관리합니다

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.

클러스터에 **SSL** 인증서를 설치합니다

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

ONTAP 9.6 이상(NVE)에서 외부 키 관리 지원

하나 이상의 KMIP 서버를 사용하여 클러스터에서 암호화된 데이터에 액세스하는 데 사용하는 키를 보호할 수 있습니다. ONTAP 9.6부터는 데이터 SVM이 암호화된 데이터에 액세스하는 데 사용하는 키를 보호하기 위해 별도의 외부 키 관리자를 구성할 수 있습니다.

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 클러스터 또는 SVM에 연결할 수 있습니다. 이중화 및 재해 복구를 위해 최소 2대의 서버를 사용하는 것이 좋습니다.

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>'

  전체 명령 구문은 명령에 대한 man 페이지를 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.

시작하기 전에

- KMIP SSL 클라이언트 및 서버 인증서를 설치해야 합니다.
- 이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.
- MetroCluster 환경에 대해 외부 키 관리를 활성화하려면 외부 키 관리를 활성화하기 전에 MetroCluster를 완전히 구성해야 합니다.
- MetroCluster 환경에서는 두 클러스터 모두에 KMIP SSL 인증서를 설치해야 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

   - 를 클릭합니다 `security key-manager external enable` 명령이 을 대체합니다 `security key-manager setup` 명령. 클러스터 로그인 프롬프트에서 명령을 실행하면 *`admin_SVM`* 기본값은 현재 클러스터의 관리 SVM입니다. 클러스터 범위를 구성하려면 클러스터 관리자여야 합니다. 를 실행할 수 있습니다 `security key-manager external modify` 외부 키 관리 구성을 변경하는 명령입니다.
   - 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.

   ```
   cluster1::> 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 기본적으로 'VM'이 현재 SVM으로 설정됩니다. SVM 범위를 구성하려면 클러스터 또는 SVM 관리자여야 합니다. 'Security key-manager external modify' 명령어를 실행하여 외부 키 관리 설정을 변경할 수 있다.
   - 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.

> 또한 'Security key-manager external add-servers' 명령을 사용하여 추가 SVM을 구성할 수도 있습니다. 보안 키 관리자 외부 서버 명령은 보안 키 관리자 추가 명령을 대체합니다. 전체 명령 구문은 man 페이지를 참조하십시오.

4. 구성된 모든 KMIP 서버가 연결되어 있는지 확인합니다.

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

> 보안 키-관리자 외부 show-status 명령은 보안 키-관리자 show-status 명령을 대체합니다. 전체 명령 구문은 man 페이지를 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. MetroCluster 환경에서는 외부 키 관리자를 두 사이트에 모두 구성해야 합니다.

ONTAP 9.5 이전 버전에서 외부 키 관리를 활성화합니다

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 클러스터 모두에 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 클러스터 모두에서 이 명령을 실행해야 합니다.

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

   전체 명령 구문은 man 페이지를 참조하십시오.

```
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 공급자를 통해 키를 관리합니다

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

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 클러스터는 키 관리 서비스를 제대로 사용하지 않습니다.

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`*

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. 'cluster show' 명령을 사용하여 확인할 수 있습니다.
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.

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 있습니다 `cluster show`.
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 매개 변수로 구성되었는지 확인합니다.
security key-manager external gcp show vserver *svm_name*
의 상태입니다 kms_wrapped_key_status 가 됩니다 "UNKNOWN" 암호화된 볼륨이 생성되지 않은 경우 서비스 상태가 양호하지 않은 경우 데이터 SVM LIF를 통해 GCP 키 관리 서비스에 대한 연결을 설정합니다.

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"

ONTAP 9.6 이상(NVE)에서 온보드 키 관리 지원

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.

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.

ONTAP 저장 시 데이터 암호화를 구성할 때 CSDC(Commercial Solutions for Classified)에 대한 요구사항을 충족하려면 NSE를 NVE와 함께 사용해야 하며 온보드 키 관리자가 일반 조건 모드에서 활성화되도록 해야 합니다. 을 참조하십시오 "CSDC 솔루션 요약" CSfC에 대한 자세한 내용은

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.

  부팅 시 올바른 클러스터 암호를 입력하지 않으면 암호화된 볼륨이 마운트되지 않습니다. 이 문제를 해결하려면 노드를 재부팅하고 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 확인하여 이미지 내용이 변경되거나 손상되지 않았는지 확인합니다. 유효성 검사에 성공하면 이미지 업데이트 프로세스가 다음 단계로 진행되고, 그렇지 않으면 이미지 업데이트가 실패합니다. 를 참조하십시오 `cluster image` 시스템 업데이트에 대한 정보를 보려면 man 페이지를 참조하십시오.

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

- 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.

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

```
cluster1::> security key-manager onboard enable

Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1"::    <32..256 ASCII characters long text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. 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.

3. 암호 확인 프롬프트에서 암호를 다시 입력합니다.
4. 인증 키가 생성되었는지 확인합니다.

   '보안 키 관리자 키 쿼리 - 키 유형 NSE-AK'

   > 보안 키-관리자 키 쿼리 명령은 보안 키-관리자 쿼리 키 명령을 대체합니다. 전체 명령 구문은 man 페이지를 참조하십시오.

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

```
cluster1::> security key-manager key query -key-type NSE-AK
               Node: node1
            Vserver: cluster1
        Key Manager: onboard
   Key Manager Type: OKM
 Key Manager Policy: -

 Key Tag                                Key Type Encryption   Restored

------------------------------------  -------- ------------ --------

node1                                  NSE-AK   AES-256      true

    Key ID:
00000000000000000200000000000100056178fc6ace6d91472df8a9286daacc00000000
00000000

node1                                  NSE-AK   AES-256      true

    Key ID:
00000000000000000200000000000100df1689a148fdfbf9c2b198ef974d0baa00000000
00000000

2 entries were displayed.
```

5. 필요한 경우 일반 텍스트 볼륨을 암호화된 볼륨으로 변환합니다.

   `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.

Onboard Key Manager 암호를 구성할 때마다 재해 발생 시 사용할 수 있도록 정보를 스토리지 시스템 외부의 안전한 위치에 수동으로 백업해야 합니다. 을 참조하십시오 "온보드 키 관리 정보를 수동으로 백업합니다".

ONTAP 9.5 이하(NVE)에서 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

- NSE 또는 NVE를 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 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.

   보안 키 관리자 키 쇼

   전체 명령 구문은 man 페이지를 참조하십시오.

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

Node: node1
Key Store: onboard
Key ID                                                                   Used By
-------------------------------------------------------------------
--------
00000000000000000200000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
00000000000000000200000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                                   Used By
-------------------------------------------------------------------
--------
00000000000000000200000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
00000000000000000200000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

6. 필요한 경우 일반 텍스트 볼륨을 암호화된 볼륨으로 변환합니다.

   ```
   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.

Onboard Key Manager 암호를 구성할 때마다 재해 발생 시 사용할 수 있도록 정보를 스토리지 시스템 외부의 안전한 위치에 수동으로 백업해야 합니다. 을 참조하십시오 "온보드 키 관리 정보를 수동으로 백업합니다".

새로 추가된 노드에서 온보드 키 관리를 활성화합니다

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 9.5 이전 버전의 경우, 클러스터에 노드를 추가할 때마다 '보안 키 관리자 설정' 명령을 실행해야 합니다.
>
> ONTAP 9.6 이상에서는 클러스터에 노드를 추가할 때마다 보안 키 관리자 동기화 명령을 실행해야 합니다.
>
> 온보드 키 관리가 구성된 클러스터에 노드를 추가하면 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.
- 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.