키 관리 서버 구성

StorageGRID software

NetApp
July 23, 2026

목차

키 관리 서버 구성

StorageGRID의 키 관리 서버에 대해 알아보십시오

키 관리 서버(KMS)는 키 관리 상호 운용성 프로토콜(KMIP)을 사용하여 연결된 StorageGRID 사이트의 StorageGRID 어플라이언스 노드에 암호화 키를 제공하는 외부 타사 시스템입니다.

StorageGRID는 특정 키 관리 서버만 지원합니다. 지원되는 제품 및 버전 목록은 "NetApp 상호 운용성 매트릭스 툴(IMT)"을 참조하십시오.

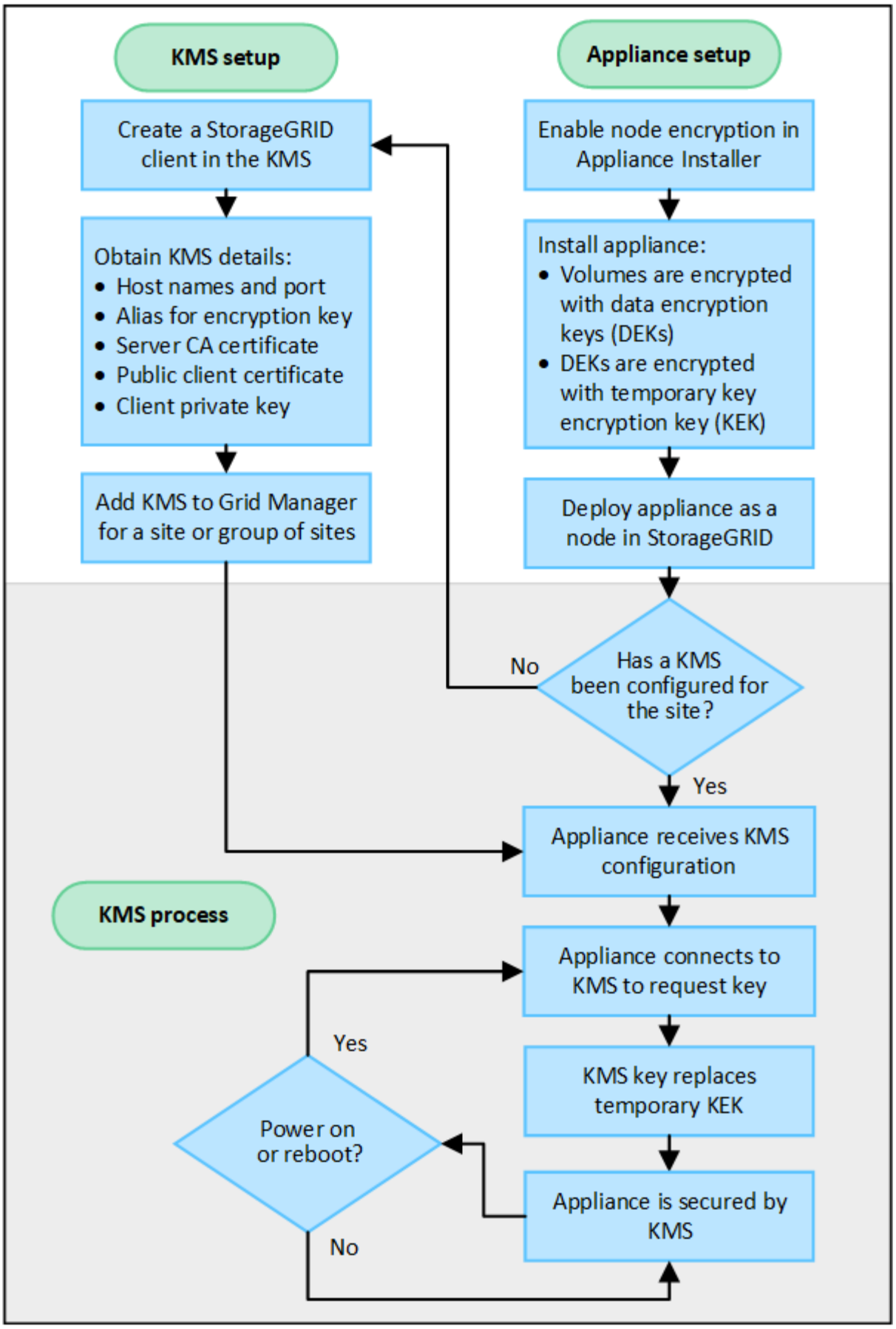
설치 시 노드 암호화 설정이 활성화된 StorageGRID 어플라이언스 노드의 노드 암호화 키를 관리하기 위해 하나 이상의 키 관리 서버를 사용할 수 있습니다. 이러한 어플라이언스 노드에 키 관리 서버를 사용하면 어플라이언스가 데이터 센터에서 제거되더라도 데이터를 보호할 수 있습니다. 어플라이언스 볼륨이 암호화된 후에는 노드가 KMS와 통신할 수 없는 한 어플라이언스의 데이터에 액세스할 수 없습니다.

> StorageGRID 어플라이언스 노드를 암호화 및 복호화하는 데 사용되는 외부 키를 생성하거나 관리하지 않습니다. StorageGRID 데이터를 보호하기 위해 외부 키 관리 서버를 사용하려는 경우, 해당 서버 설정 방법과 암호화 키 관리 방법을 숙지해야 합니다. 키 관리 작업은 본 설명서의 범위를 벗어납니다. 도움이 필요하면 키 관리 서버 설명서를 참조하거나 기술 지원에 문의하십시오.

StorageGRID 키 관리 서버 및 어플라이언스 구성

StorageGRID 어플라이언스 노드에서 StorageGRID 데이터를 보호하기 위해 키 관리 서버(KMS)를 사용하려면 먼저 두 가지 구성 작업을 완료해야 합니다. 하나 이상의 KMS 서버를 설정하고 어플라이언스 노드에 대한 노드 암호화를 활성화하는 것입니다. 이 두 가지 구성 작업이 완료되면 키 관리 프로세스가 자동으로 진행됩니다.

이 순서도는 KMS를 사용하여 어플라이언스 노드의 StorageGRID 데이터를 보호하는 주요 단계를 보여줍니다.



순서도는 KMS 설정과 어플라이언스 설정이 동시에 진행되는 것을 보여주지만, 요구 사항에 따라 새 어플라이언스

노드에 대한 노드 암호화를 활성화하기 전이나 후에 키 관리 서버를 설정할 수 있습니다.

키 관리 서버(KMS) 설정

키 관리 서버 설정에는 다음과 같은 주요 단계가 포함됩니다.

단계	참조하십시오
KMS 소프트웨어에 액세스하여 각 KMS 또는 KMS 클러스터에 StorageGRID 클라이언트를 추가하십시오.	"KMS에서 StorageGRID를 클라이언트로 구성합니다"
KMS에서 StorageGRID 클라이언트에 필요한 정보를 얻으십시오.	"KMS에서 StorageGRID를 클라이언트로 구성합니다"
그리드 관리자에 KMS를 추가하고, 단일 사이트 또는 기본 사이트 그룹에 할당하고, 필요한 인증서를 업로드하고, KMS 구성을 저장합니다.	"키 관리 서버(KMS) 추가"

어플라이언스를 설정합니다

KMS 사용을 위한 어플라이언스 노드 설정은 다음과 같은 주요 단계를 포함합니다.

1. 어플라이언스 설치의 하드웨어 구성 단계에서 StorageGRID Appliance Installer를 사용하여 어플라이언스에 대한 노드 암호화 설정을 활성화하십시오.

   > 어플라이언스를 그리드에 추가한 후에는 노드 암호화 설정을 활성화할 수 없으며, 노드 암호화가 활성화되지 않은 어플라이언스에는 외부 키 관리를 사용할 수 없습니다.

2. StorageGRID 어플라이언스 설치 프로그램을 실행합니다. 설치 과정에서 다음과 같이 각 어플라이언스 볼륨에 임의의 데이터 암호화 키(DEK)가 할당됩니다.
   - DEK는 각 볼륨의 데이터를 암호화하는 데 사용됩니다. 이러한 키는 어플라이언스 OS에서 LUKS(Linux Unified Key Setup) 디스크 암호화를 사용하여 생성되며 변경할 수 없습니다.
   - 각 개별 DEK는 마스터 키 암호화 키(KEK)로 암호화됩니다. 초기 KEK는 어플라이언스가 KMS에 연결될 때까지 DEK를 암호화하는 임시 키입니다.
3. 어플라이언스 노드를 StorageGRID에 추가합니다.

자세한 내용은 "노드 암호화 활성화"을 참조하십시오.

키 관리 암호화 프로세스(자동으로 발생)

키 관리 암호화에는 자동으로 수행되는 다음과 같은 주요 단계가 포함됩니다.

1. 노드 암호화가 활성화된 어플라이언스를 그리드에 설치하면 StorageGRID는 새 노드가 포함된 사이트에 KMS 구성이 있는지 확인합니다.
   - 사이트에 KMS가 이미 구성되어 있는 경우, 어플라이언스는 KMS 구성을 수신합니다.
   - 사이트에 KMS가 아직 구성되지 않은 경우, 사이트에 KMS를 구성하고 어플라이언스가 KMS 구성을 수신할 때까지 어플라이언스의 데이터는 임시 KEK에 의해 계속 암호화됩니다.

2. 해당 장치는 KMS 구성을 사용하여 KMS에 연결하고 암호화 키를 요청합니다.
3. KMS가 암호화 키를 어플라이언스로 전송합니다. KMS에서 전송된 새 키는 임시 KEK를 대체하며, 이제 어플라이언스 볼륨의 DEK를 암호화 및 복호화하는 데 사용됩니다.

> 암호화된 어플라이언스 노드가 구성된 KMS에 연결되기 전에 존재하는 모든 데이터는 임시 키로 암호화됩니다. 그러나 임시 키가 KMS 암호화 키로 교체될 때까지 어플라이언스 볼륨은 데이터 센터에서 제거되지 않도록 보호되는 것으로 간주해서는 안 됩니다.

4. 기기의 전원이 켜지거나 재부팅되면 KMS에 다시 연결하여 키를 요청합니다. 휘발성 메모리에 저장된 키는 전원 공급이 중단되거나 재부팅되면 손실될 수 있습니다.

StorageGRID 키 관리 서버 요구 사항 및 고려 사항

외부 키 관리 서버(KMS)를 구성하기 전에 고려 사항과 요구 사항을 이해해야 합니다.

지원되는 KMIP 버전은 무엇입니까?

StorageGRID는 KMIP 버전 1.4를 지원합니다.

"키 관리 상호 운용성 프로토콜 사양 버전 1.4"

네트워크 관련 고려 사항은 무엇인가요?

네트워크 방화벽 설정에서 각 어플라이언스 노드가 KMIP(Key Management Interoperability Protocol) 통신에 사용되는 포트를 통해 통신할 수 있도록 허용해야 합니다. KMIP의 기본 포트는 5696입니다.

노드 암호화를 사용하는 각 어플라이언스 노드가 해당 사이트에 대해 구성한 KMS 또는 KMS 클러스터에 네트워크 액세스할 수 있는지 확인해야 합니다.

지원되는 TLS 버전은 무엇입니까?

어플라이언스 노드와 구성된 KMS 간의 통신은 보안 TLS 연결을 사용합니다. StorageGRID KMS 또는 KMS 클러스터와의 KMIP 연결 시 KMS에서 지원하는 프로토콜 및 "TLS 및 SSH 정책"사용자가 사용하는 프로토콜에 따라 TLS 1.2 또는 TLS 1.3 프로토콜을 지원할 수 있습니다.

StorageGRID는 KMS와 연결할 때 프로토콜 및 암호화(TLS 1.2) 또는 암호화 스위트(TLS 1.3)를 협상합니다. 사용 가능한 프로토콜 버전과 암호화/암호화 스위트를 확인하려면 그리드의 활성 TLS 및 SSH 정책의 `tlsOutbound` 섹션을 참조하십시오(구성 > 보안 보안 설정).

어떤 어플라이언스가 지원됩니까?

키 관리 서버(KMS)를 사용하여 노드 암호화 설정이 활성화된 그리드 내 모든 StorageGRID 어플라이언스의 암호화 키를 관리할 수 있습니다. 이 설정은 StorageGRID Appliance Installer를 사용하여 어플라이언스를 설치하는 하드웨어 구성 단계에서만 활성화할 수 있습니다.

> 어플라이언스를 그리드에 추가한 후에는 노드 암호화를 활성화할 수 없으며, 노드 암호화가 활성화되지 않은 어플라이언스에는 외부 키 관리를 사용할 수 없습니다.

구성된 KMS를 StorageGRID 어플라이언스 및 어플라이언스 노드에 사용할 수 있습니다.

다음과 같은 소프트웨어 기반(어플라이언스 이외의) 노드에는 구성된 KMS를 사용할 수 없습니다:

- 가상 머신(VM)으로 배포된 노드
- Linux 호스트의 컨테이너 엔진 내에 배포된 노드

다른 플랫폼에 배포된 노드는 데이터 저장소 또는 디스크 수준에서 StorageGRID 외부의 암호화를 사용할 수 있습니다.

키 관리 서버는 언제 구성해야 합니까?

새로운 설치의 경우, 일반적으로 테넌트를 생성하기 전에 Grid Manager에서 하나 이상의 키 관리 서버를 설정해야 합니다. 이 순서를 따르면 노드에 객체 데이터가 저장되기 전에 노드가 보호됩니다.

어플라이언스 노드를 설치하기 전이나 후에 그리드 관리자에서 키 관리 서버를 구성할 수 있습니다.

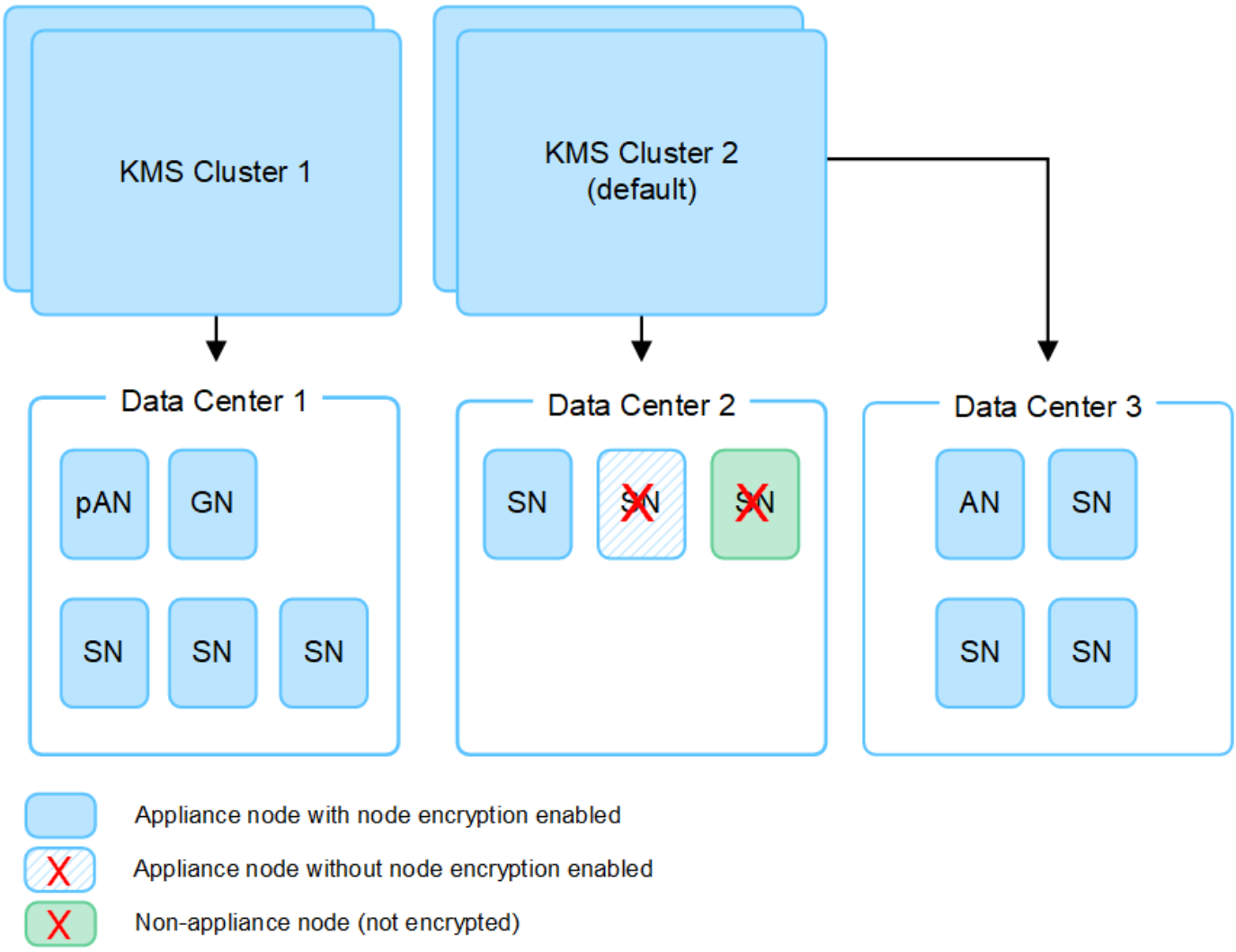
키 관리 서버는 몇 대가 필요합니까?

StorageGRID 시스템의 어플라이언스 노드에 암호화 키를 제공하기 위해 하나 이상의 외부 키 관리 서버(KMS)를 구성할 수 있습니다. 각 KMS는 단일 사이트 또는 여러 사이트에 있는 StorageGRID 어플라이언스 노드에 단일 암호화 키를 제공합니다.

StorageGRID는 KMS 클러스터 사용을 지원합니다. 각 KMS 클러스터는 구성 설정 및 암호화 키를 공유하는 여러 개의 복제된 키 관리 서버를 포함합니다. KMS 클러스터를 키 관리에 사용하면 고가용성 구성의 페일오버 기능이 향상되므로 권장됩니다.

예를 들어, StorageGRID 시스템에 데이터 센터 사이트가 세 개 있다고 가정해 보겠습니다. 첫 번째 KMS 클러스터는 데이터 센터 1의 모든 어플라이언스 노드에 키를 제공하도록 구성하고, 두 번째 KMS 클러스터는 나머지 모든 사이트의 어플라이언스 노드에 키를 제공하도록 구성할 수 있습니다. 두 번째 KMS 클러스터를 추가할 때 데이터 센터 2와 데이터 센터 3에 대한 기본 KMS를 구성할 수 있습니다.

어플라이언스가 아닌 노드 또는 설치 중에 노드 암호화 설정이 활성화되지 않은 어플라이언스 노드에는 KMS를 사용할 수 없습니다.



키를 교체하면 어떻게 됩니까?

보안 모범 사례로서, 구성된 각 KMS에서 사용하는 "암호화 키 교체"을(를) 주기적으로 확인해야 합니다.

새로운 키 버전이 출시되면:

- 해당 키는 KMS와 연결된 사이트의 암호화 어플라이언스 노드에 자동으로 배포됩니다. 배포는 키가 교체된 후 1시간 이내에 이루어져야 합니다.
- 암호화된 어플라이언스 노드가 새 키 버전이 배포될 때 오프라인 상태인 경우, 노드는 재부팅되는 즉시 새 키를 수신하게 됩니다.
- 어떤 이유로든 새 키 버전을 사용하여 어플라이언스 볼륨을 암호화할 수 없는 경우, 어플라이언스 노드에 대해 **KMS** 암호화 키 순환 실패 경고가 발생합니다. 이 경고를 해결하려면 기술 지원팀에 문의해야 할 수 있습니다.

암호화된 어플라이언스 노드를 재사용할 수 있습니까?

암호화된 어플라이언스를 다른 StorageGRID 시스템에 설치해야 하는 경우, 먼저 그리드 노드를 비활성화하여 객체 데이터를 다른 노드로 이동해야 합니다. 그런 다음 StorageGRID 어플라이언스 설치 프로그램을 사용하여 "KMS 구성 지우기". KMS 구성을 지우면 노드 암호화 설정이 비활성화되고 어플라이언스 노드와 StorageGRID 사이트의 KMS 구성 간의 연결이 제거됩니다.

KMS 암호화 키에 액세스할 수 없으면 어플라이언스에 남아 있는 모든 데이터에 더 이상 액세스할 수 없으며 영구적으로 잠깁니다.

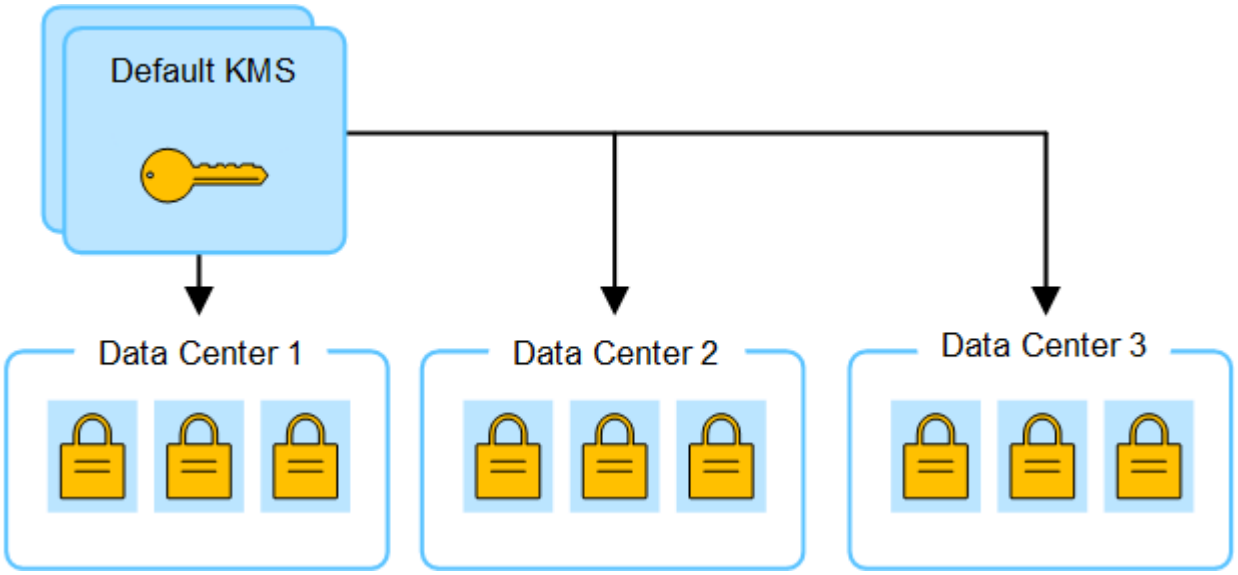
StorageGRID 사이트의 KMS 변경 시 고려 사항

각 키 관리 서버(KMS) 또는 KMS 클러스터는 단일 사이트 또는 여러 사이트에 있는 모든 어플라이언스 노드에 암호화 키를 제공합니다. 사이트에서 사용하는 KMS를 변경해야 하는 경우, 한 KMS에서 다른 KMS로 암호화 키를 복사해야 할 수 있습니다.

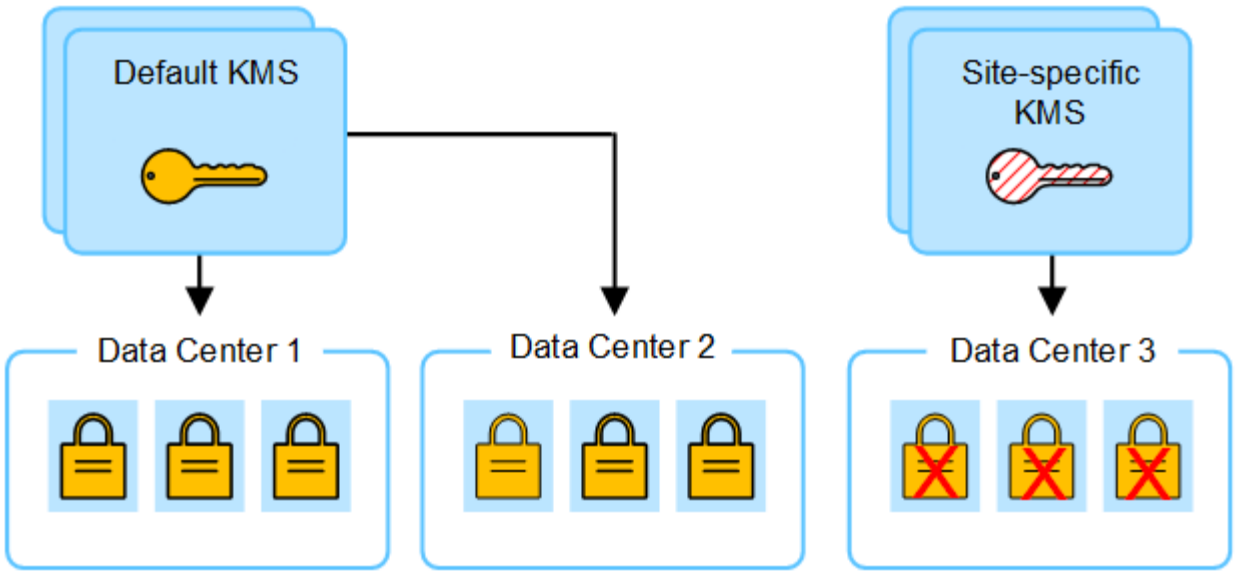
사이트에 사용되는 KMS를 변경하는 경우, 해당 사이트에서 이전에 암호화된 어플라이언스 노드를 새 KMS에 저장된 키를 사용하여 복호화할 수 있는지 확인해야 합니다. 경우에 따라 기존 KMS에서 새 KMS로 현재 버전의 암호화 키를 복사해야 할 수도 있습니다. KMS에 해당 사이트의 암호화된 어플라이언스 노드를 복호화하는 데 필요한 올바른 키가 있는지 반드시 확인해야 합니다.

예를 들면 다음과 같습니다.

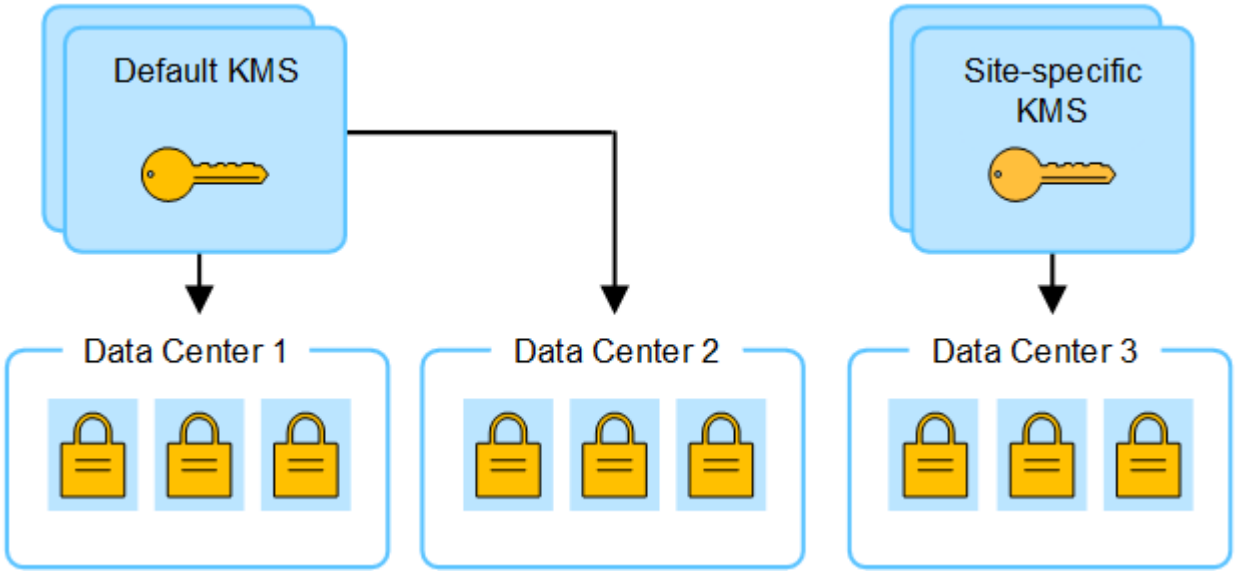
1. 처음에 전용 KMS가 없는 모든 사이트에 적용되는 기본 KMS를 구성합니다.
2. KMS가 저장되면 노드 암호화 설정이 활성화된 모든 어플라이언스 노드가 KMS에 연결하여 암호화 키를 요청합니다. 이 키는 모든 사이트의 어플라이언스 노드를 암호화하는 데 사용됩니다. 또한 동일한 키를 사용하여 해당 어플라이언스를 복호화해야 합니다.



3. 그림에서 데이터 센터 3에 해당하는 한 사이트에 대해 사이트별 KMS를 추가하기로 결정했습니다. 하지만 어플라이언스 노드가 이미 암호화되어 있기 때문에 사이트별 KMS의 구성을 저장하려고 하면 유효성 검사 오류가 발생합니다. 이 오류는 사이트별 KMS에 해당 사이트의 노드를 복호화하는 데 필요한 올바른 키가 없기 때문에 발생합니다.



4. 이 문제를 해결하려면 기본 KMS에서 현재 버전의 암호화 키를 새 KMS로 복사합니다. (엄밀히 말하면, 원래 키를 동일한 별칭을 가진 새 키로 복사하는 것입니다. 원래 키는 새 키의 이전 버전이 됩니다.) 이제 사이트별 KMS에 데이터 센터 3의 어플라이언스 노드를 복호화하는 데 필요한 올바른 키가 있으므로 StorageGRID에 저장할 수 있습니다.



사이트에 사용할 **KMS**를 변경하는 사용 사례

이 표는 사이트의 KMS를 변경하는 가장 일반적인 경우에 필요한 단계를 요약한 것입니다.

사이트 **KMS** 변경 사례	필수 단계
사이트별 KMS 항목이 하나 이상 있으며, 그중 하나를 기본 KMS로 사용하려고 합니다.	사이트별 KMS를 편집합니다. 키 관리 대상 필드에서 *다른 KMS에서 관리되지 않는 사이트(기본 KMS)*를 선택합니다. 이제 사이트별 KMS가 기본 KMS로 사용됩니다. 이는 전용 KMS가 없는 모든 사이트에 적용됩니다. "키 관리 서버(KMS) 편집"

사이트 **KMS** 변경 사례	필수 단계
기본 KMS가 있는 상태에서 확장 기능을 통해 새 사이트를 추가했습니다. 새 사이트에는 기본 KMS를 사용하고 싶지 않습니다.	1. 새 사이트의 어플라이언스 노드가 기본 KMS로 이미 암호화된 경우 KMS 소프트웨어를 사용하여 기본 KMS의 현재 암호화 키 버전을 새 KMS로 복사하십시오. 2. 그리드 관리자를 사용하여 새 KMS를 추가하고 사이트를 선택합니다. "키 관리 서버(KMS) 추가"
사이트의 KMS가 다른 서버를 사용하도록 하려는 경우.	1. 현장의 어플라이언스 노드가 기존 KMS에 의해 이미 암호화된 경우, KMS 소프트웨어를 사용하여 현재 버전의 암호화 키를 기존 KMS에서 새 KMS로 복사하십시오. 2. 그리드 관리자를 사용하여 기존 KMS 구성을 편집하고 새 호스트 이름 또는 IP 주소를 입력합니다. "키 관리 서버(KMS) 추가"

KMS에서 StorageGRID를 클라이언트로 구성합니다

KMS를 StorageGRID에 추가하려면 먼저 각 외부 키 관리 서버 또는 KMS 클러스터에 대해 StorageGRID를 클라이언트로 구성해야 합니다.

이 지침은 Thales CipherTrust Manager 및 Hashicorp Vault에 적용됩니다. 지원되는 제품 및 버전 목록은 "NetApp 상호 운용성 매트릭스 툴(IMT)"을 사용하십시오.

단계

1. KMS 소프트웨어에서 사용하려는 각 KMS 또는 KMS 클러스터에 대해 StorageGRID 클라이언트를 생성하십시오.

   각 KMS는 단일 사이트 또는 여러 사이트 그룹에 있는 StorageGRID 어플라이언스 노드에 대한 단일 암호화 키를 관리합니다.

2. 다음 두 가지 방법 중 하나를 사용하여 키를 생성합니다.
   - KMS 제품의 키 관리 페이지를 사용하십시오. 각 KMS 또는 KMS 클러스터에 대해 AES 암호화 키를 생성하십시오.

     암호화 키는 2,048비트 이상이어야 하며, 내보낼 수 있어야 합니다.

   - StorageGRID가 키를 생성하도록 합니다. "클라이언트 인증서 업로드 중" 이후 테스트하고 저장할 때 메시지가 표시됩니다.

3. 각 KMS 또는 KMS 클러스터에 대해 다음 정보를 기록하십시오.

   KMS를 StorageGRID에 추가할 때 이 정보가 필요합니다.

   - 각 서버의 호스트 이름 또는 IP 주소입니다.
   - KMS에서 사용하는 KMIP 포트입니다.
   - KMS에서 암호화 키에 대한 키 별칭입니다.

4. 각 KMS 또는 KMS 클러스터에 대해 인증 기관(CA)에서 서명한 서버 인증서 또는 PEM 형식으로 인코딩된 각 CA 인증서 파일이 인증서 체인 순서대로 연결된 인증서 번들을 확보하십시오.

   서버 인증서를 통해 외부 KMS가 StorageGRID에 자신을 인증할 수 있습니다.

   - 인증서는 개인정보보호 강화 메일(PEM) Base-64 인코딩 X.509 형식을 사용해야 합니다.
   - 각 서버 인증서의 주체 대체 이름(SAN) 필드에는 StorageGRID가 연결할 정규화된 도메인 이름(FQDN) 또는 IP 주소가 포함되어야 합니다.

     StorageGRID에서 KMS를 구성할 때 호스트 이름 필드에 동일한 FQDN 또는 IP 주소를 입력해야 합니다.

   - 서버 인증서는 KMS의 KMIP 인터페이스에서 사용하는 인증서와 일치해야 하며, KMIP 인터페이스는 일반적으로 포트 5696을 사용합니다.

5. 외부 KMS에서 StorageGRID에 발급한 공개 클라이언트 인증서와 해당 클라이언트 인증서의 개인 키를 확보하십시오.

   클라이언트 인증서를 통해 StorageGRID KMS에 자체 인증을 수행할 수 있습니다.

StorageGRID에 키 관리 서버 추가

StorageGRID 키 관리 서버 마법사를 사용하여 각 KMS 또는 KMS 클러스터를 추가합니다.

시작하기 전에

- "키 관리 서버 사용 시 고려 사항 및 요구 사항"를 검토했습니다.
- 귀하는 "KMS에서 StorageGRID를 클라이언트로 구성했습니다.", 그리고 각 KMS 또는 KMS 클러스터에 필요한 정보를 보유하고 있습니다.
- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 다음이 있습니다. "루트 액세스 권한"

이 작업 정보

가능하다면, 다른 KMS로 관리되지 않는 모든 사이트에 적용되는 기본 KMS를 구성하기 전에 사이트별 키 관리 서버를 구성하십시오. 기본 KMS를 먼저 생성하면 그리드의 모든 노드 암호화 어플라이언스가 기본 KMS로 암호화됩니다. 나중에 사이트별 KMS를 생성하려면 먼저 기본 KMS에서 현재 버전의 암호화 키를 새 KMS로 복사해야 합니다. 자세한 내용은 "사이트의 KMS를 변경할 때 고려 사항"을 참조하십시오.

1단계: KMS 세부 정보

키 관리 서버 추가 마법사의 1단계(KMS 세부 정보)에서는 KMS 또는 KMS 클러스터에 대한 세부 정보를 제공합니다.

단계

1. * 구성 * > * 보안 * > * 키 관리 서버 * 를 선택합니다.

   키 관리 서버 페이지가 구성 세부 정보 탭이 선택된 상태로 나타납니다.

2. *생성*을 선택합니다.

키 관리 서버 추가 마법사의 1단계(KMS 세부 정보)가 나타납니다.

3. KMS 및 해당 KMS에 구성한 StorageGRID 클라이언트에 대한 다음 정보를 입력하십시오.

필드	설명
KMS 이름	이 KMS를 식별하는 데 도움이 되는 설명적인 이름입니다. 1자에서 64자 사이여야 합니다.
키 이름	KMS의 StorageGRID 클라이언트에 대한 정확한 키 별칭입니다. 1~255자 사이여야 합니다. 참고: KMS 제품을 사용하여 키를 생성하지 않은 경우 StorageGRID에서 키를 생성하라는 메시지가 표시됩니다.
키 관리 대상:	이 KMS와 연결될 StorageGRID 사이트입니다. 가능하면 다른 KMS로 관리되지 않는 모든 사이트에 적용되는 기본 KMS를 구성하기 전에 사이트별 키 관리 서버를 구성해야 합니다. • 이 KMS가 특정 사이트의 어플라이언스 노드에 대한 암호화 키를 관리할 경우 해당 사이트를 선택하십시오. • *다른 KMS에서 관리되지 않는 사이트(기본 KMS)*를 선택하여 전용 KMS가 없는 사이트와 향후 확장에서 추가하는 모든 사이트에 적용될 기본 KMS를 구성합니다. 참고**:** 이전에 기본 KMS로 암호화된 사이트를 선택했지만 새 KMS에 기존 암호화 키의 최신 버전을 제공하지 않은 경우 KMS 구성을 저장할 때 유효성 검사 오류가 발생합니다.
포트	KMS 서버가 키 관리 상호 운용성 프로토콜(KMIP) 통신에 사용하는 포트입니다. 기본값은 KMIP 표준 포트인 5696입니다.
호스트 이름	KMS의 정규화된 도메인 이름 또는 IP 주소입니다. 참고**:** 서버 인증서의 SAN(Subject Alternative Name) 필드에는 여기에 입력한 FQDN 또는 IP 주소가 포함되어야 합니다. 그렇지 않으면 StorageGRID가 KMS 또는 KMS 클러스터의 모든 서버에 연결할 수 없습니다.

4. KMS 클러스터를 구성하는 경우, 클러스터의 각 서버에 호스트 이름을 추가하려면 *Add another hostname*을 선택하십시오.
5. *Continue*를 선택합니다.

2단계**:** 서버 인증서 업로드

키 관리 서버 추가 마법사의 2단계(서버 인증서 업로드)에서 KMS용 서버 인증서(또는 인증서 번들)를 업로드합니다. 서버 인증서를 통해 외부 KMS는 StorageGRID에 자신을 인증할 수 있습니다.

단계

1. *2단계(서버 인증서 업로드)*에서 저장된 서버 인증서 또는 인증서 묶음의 위치로 이동합니다.
2. 인증서 파일을 업로드합니다.

   서버 인증서 메타데이터가 표시됩니다.

   > 인증서 묶음을 업로드한 경우 각 인증서의 메타데이터가 별도의 탭에 표시됩니다.

3. *Continue*를 선택합니다.

3단계: 클라이언트 인증서 업로드

키 관리 서버 추가 마법사의 3단계(클라이언트 인증서 업로드)에서 클라이언트 인증서와 클라이언트 인증서 개인 키를 업로드합니다. 클라이언트 인증서를 통해 StorageGRID KMS에 자체 인증을 수행할 수 있습니다.

단계

1. *3단계(클라이언트 인증서 업로드)*에서 클라이언트 인증서가 있는 위치로 이동합니다.
2. 클라이언트 인증서 파일을 업로드합니다.

   클라이언트 인증서 메타데이터가 표시됩니다.

3. 클라이언트 인증서의 개인 키가 있는 위치로 이동합니다.
4. 개인 키 파일을 업로드합니다.
5. *테스트 후 저장*을 선택합니다.

   키가 없으면 StorageGRID에서 키를 생성하도록 요청하는 메시지가 표시됩니다.

   키 관리 서버와 어플라이언스 노드 간의 연결을 테스트합니다. 모든 연결이 유효하고 KMS에서 올바른 키가 발견되면 새 키 관리 서버가 키 관리 서버 페이지의 표에 추가됩니다.

   > KMS를 추가한 직후 키 관리 서버 페이지의 인증서 상태가 '알 수 없음'으로 표시됩니다. StorageGRID가 각 인증서의 실제 상태를 가져오는 데 최대 30분이 소요될 수 있습니다. 현재 상태를 확인하려면 웹 브라우저를 새로 고침해야 합니다.

6. *테스트 후 저장*을 선택했을 때 오류 메시지가 나타나면 메시지 내용을 확인한 후 *확인*을 선택하십시오.

   예를 들어 연결 테스트에 실패하면 422: Unprocessable Entity 오류가 발생할 수 있습니다.

7. 외부 연결을 테스트하지 않고 현재 구성을 저장해야 하는 경우 *강제 저장*을 선택하십시오.

   > *강제 저장*을 선택하면 KMS 구성이 저장되지만, 각 어플라이언스에서 해당 KMS로의 외부 연결은 테스트되지 않습니다. 구성에 문제가 있는 경우 해당 사이트에서 노드 암호화가 활성화된 어플라이언스 노드를 재부팅할 수 없을 수 있습니다. 문제가 해결될 때까지 데이터에 액세스할 수 없게 될 수도 있습니다.

8. 확인 경고 메시지를 검토하고 구성을 강제 저장하려면 *확인*을 선택합니다.

   KMS 구성이 저장되지만 KMS 연결은 테스트되지 않습니다.

StorageGRID에서 키 관리 서버 관리

키 관리 서버(KMS) 관리는 세부 정보 보기 또는 편집, 인증서 관리, 암호화된 노드 보기, 더 이상 필요하지 않을 때 KMS 제거 등을 포함합니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 다음이 있습니다. "필수 액세스 권한"

KMS 세부 정보 보기

StorageGRID 시스템의 각 키 관리 서버(KMS)에 대한 정보를 확인할 수 있으며, 여기에는 키 세부 정보와 서버 및 클라이언트 인증서의 현재 상태가 포함됩니다.

단계

1. * 구성 * > * 보안 * > * 키 관리 서버 * 를 선택합니다.

   키 관리 서버 페이지가 나타나고 다음 정보가 표시됩니다.

   - 구성 세부 정보 탭에는 구성된 키 관리 서버 목록이 표시됩니다.
   - 암호화된 노드 탭에는 노드 암호화가 활성화된 모든 노드가 나열됩니다.

2. 특정 KMS의 세부 정보를 확인하고 해당 KMS에서 작업을 수행하려면 KMS 이름을 선택하십시오. KMS 세부 정보 페이지에는 다음 정보가 표시됩니다.

필드	설명
키 관리 대상:	KMS와 연결된 StorageGRID 사이트입니다. 이 필드에는 특정 StorageGRID 사이트 또는 *다른 KMS(기본 KMS)에서 관리되지 않는 사이트*의 이름이 표시됩니다.
호스트 이름	KMS의 정규화된 도메인 이름 또는 IP 주소입니다. 키 관리 서버가 두 대인 클러스터의 경우, 두 서버의 정규화된 도메인 이름 또는 IP 주소가 모두 나열됩니다. 클러스터에 키 관리 서버가 두 대 이상인 경우, 첫 번째 KMS의 정규화된 도메인 이름 또는 IP 주소와 함께 클러스터에 있는 추가 키 관리 서버의 수가 나열됩니다. 예: `10.10.10.10 and 10.10.10.11` 또는 `10.10.10.10 and 2 others`. 클러스터의 모든 호스트 이름을 보려면 KMS를 선택하고 편집 또는 작업 > *편집*을 선택하십시오.

3. KMS 세부 정보 페이지에서 탭을 선택하여 다음 정보를 확인하십시오.

탭	필드	설명
주요 세부 정보	키 이름	KMS의 StorageGRID 클라이언트에 대한 키 별칭입니다.
키 UID	키의 최신 버전에 대한 고유 식별자입니다.	최종 수정일
키의 최신 버전 날짜 및 시간입니다.	서버 인증서	메타데이터
인증서의 메타데이터(일련 번호, 만료 날짜 및 시간, 인증서 PEM 등)입니다.	PEM 인증서	인증서용 PEM(privacy enhanced mail) 파일의 내용입니다.
클라이언트 인증서	메타데이터	인증서의 메타데이터(일련 번호, 만료 날짜 및 시간, 인증서 PEM 등)입니다.

4. 조직의 보안 규정에 따라 필요한 만큼 자주 *Rotate key*를 선택하거나 KMS 소프트웨어를 사용하여 키의 새 버전을 생성하십시오.

   키 순환이 성공적으로 완료되면 키 UID 및 최종 수정 필드가 업데이트됩니다.

> KMS 소프트웨어를 사용하여 암호화 키를 교체하는 경우, 마지막으로 사용한 키 버전에서 동일한 키의 새 버전으로 교체해야 합니다. 완전히 다른 키로 교체하지 마십시오.
>
> KMS의 키 이름(별칭)을 변경하여 키를 교체하려고 시도하지 마십시오. StorageGRID는 이전에 사용한 모든 키 버전(및 향후 사용할 모든 키 버전)이 동일한 키 별칭으로 KMS에서 액세스 가능해야 합니다. 구성된 KMS의 키 별칭을 변경하면 StorageGRID가 데이터를 복호화하지 못할 수 있습니다.

인증서 관리

서버 또는 클라이언트 인증서 관련 문제가 발생하면 즉시 해결하십시오. 가능하면 만료 전에 인증서를 교체하십시오.

> 데이터 액세스를 유지하려면 가능한 한 빨리 인증서 문제를 해결해야 합니다.

단계

1. * 구성 * > * 보안 * > * 키 관리 서버 * 를 선택합니다.
2. 표에서 각 KMS의 인증서 만료일 값을 확인하십시오.
3. KMS 인증서 만료일이 '알 수 없음'으로 표시되는 경우, 최대 30분 정도 기다린 후 웹 브라우저를 새로 고침하세요.
4. 인증서 만료 열에 인증서가 만료되었거나 만료가 임박했음을 나타내는 경우, 해당 KMS를 선택하여 KMS 세부 정보 페이지로 이동하십시오.
   a. *서버 인증서*를 선택하고 "만료일" 필드의 값을 확인하십시오.

b. 인증서를 교체하려면 *인증서 편집*을 선택하여 새 인증서를 업로드합니다.

c. 위의 하위 단계를 반복하고 서버 인증서 대신 *Client certificate*를 선택하십시오.

5. **KMS CA** 인증서 만료, **KMS** 클라이언트 인증서 만료, **KMS** 서버 인증서 만료 경고가 발생하면 각 경고의 설명을 기록하고 권장 조치를 수행하십시오.

   StorageGRID 인증서 만료일을 업데이트하는 데 최대 30분이 소요될 수 있습니다. 웹 브라우저를 새로 고침하여 최신 값을 확인하십시오.

> 서버 인증서 상태를 알 수 없음 상태가 표시되면 KMS에서 클라이언트 인증서 없이 서버 인증서를 가져올 수 있도록 설정되어 있는지 확인하십시오.

암호화된 노드 보기

StorageGRID 시스템에서 노드 암호화 설정이 활성화된 어플라이언스 노드에 대한 정보를 볼 수 있습니다.

단계

1. * 구성 * > * 보안 * > * 키 관리 서버 * 를 선택합니다.

   키 관리 서버 페이지가 나타납니다. 구성 세부 정보 탭에는 구성된 키 관리 서버가 표시됩니다.

2. 페이지 상단에서 암호화된 노드 탭을 선택합니다.

   암호화된 노드 탭에는 StorageGRID 시스템에서 노드 암호화 설정이 활성화된 어플라이언스 노드 목록이 표시됩니다.

3. 표에 있는 각 어플라이언스 노드 정보를 검토하십시오.

열	설명
노드 이름	어플라이언스 노드의 이름입니다.
노드 유형	노드 유형: 스토리지, 관리 또는 게이트웨이.
사이트	노드가 설치된 StorageGRID 사이트의 이름입니다.
KMS 이름	노드에 사용되는 KMS의 설명 이름입니다. KMS가 목록에 없으면 [구성 세부 정보] 탭을 선택하여 KMS를 추가하십시오. "키 관리 서버(KMS) 추가"
키 UID	어플라이언스 노드에서 데이터를 암호화 및 복호화하는 데 사용되는 암호화 키의 고유 ID입니다. 전체 키 UID를 보려면 텍스트를 선택하십시오. 하이픈(--)은 키 UID를 알 수 없음을 나타내며, 이는 어플라이언스 노드와 KMS 간의 연결 문제 때문일 수 있습니다.

열	설명
상태	KMS와 어플라이언스 노드 간의 연결 상태입니다. 노드가 연결된 경우 타임스탬프는 30분마다 업데이트됩니다. KMS 구성 변경 후 연결 상태가 업데이트되는 데 몇 분이 소요될 수 있습니다. 참고: 새 값을 보려면 웹 브라우저를 새로 고침하세요.

4. 상태 열에 KMS 문제가 표시되면 즉시 문제를 해결하십시오.

   정상적인 KMS 작동 중에는 상태가 *KMS에 연결됨*으로 표시됩니다. 노드가 그리드에서 연결이 끊어진 경우 노드 연결 상태가 (Administratively Down 또는 Unknown)으로 표시됩니다.

   다른 상태 메시지는 동일한 이름을 가진 StorageGRID 알림에 해당합니다.

   - KMS 구성 로드에 실패했습니다.
   - KMS 연결 오류
   - KMS 암호화 키 이름을 찾을 수 없습니다.
   - KMS 암호화 키 순환 실패
   - KMS 키로 어플라이언스 볼륨을 복호화하는 데 실패했습니다.
   - KMS가 구성되지 않았습니다.

   이러한 알림에 대해 권장되는 조치를 수행하십시오.

   데이터를 완벽하게 보호하려면 모든 문제를 즉시 해결해야 합니다.

KMS 편집

예를 들어 인증서 만료가 임박한 경우 키 관리 서버의 구성을 편집해야 할 수 있습니다.

시작하기 전에

- KMS에 대해 선택한 사이트를 업데이트할 계획이라면, "사이트의 KMS를 변경할 때 고려해야 할 사항"을(를) 검토하셨습니다.
- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 다음이 있습니다. "루트 액세스 권한"

단계

1. * 구성 * > * 보안 * > * 키 관리 서버 * 를 선택합니다.

   키 관리 서버 페이지가 나타나고 구성된 모든 키 관리 서버가 표시됩니다.

2. 편집할 KMS를 선택하고 작업 > *편집*을 선택합니다.

   또한 표에서 KMS 이름을 선택하고 KMS 세부 정보 페이지에서 *편집*을 선택하여 KMS를 편집할 수 있습니다.

3. 필요에 따라 키 관리 서버 편집 마법사의 *1단계(KMS 세부 정보)*에서 세부 정보를 업데이트할 수 있습니다.

필드	설명
KMS 이름	이 KMS를 식별하는 데 도움이 되는 설명적인 이름입니다. 1자에서 64자 사이여야 합니다.
키 이름	KMS의 StorageGRID 클라이언트에 대한 정확한 키 별칭입니다. 1~255자 사이여야 합니다. 키 이름을 수정해야 하는 경우는 드뭅니다. 예를 들어, KMS에서 별칭 이름이 변경되었거나 이전 키의 모든 버전이 새 별칭의 버전 기록에 복사된 경우에만 키 이름을 수정해야 합니다.
키 관리 대상:	사이트별 KMS를 편집하는 중이고 기본 KMS가 아직 없는 경우, 선택적으로 *다른 KMS(기본 KMS)에서 관리되지 않는 사이트*를 선택할 수 있습니다. 이 옵션을 선택하면 사이트별 KMS가 기본 KMS로 변환되어 전용 KMS가 없는 모든 사이트와 확장 시 추가된 모든 사이트에 적용됩니다. 참고**:** 사이트별 KMS를 편집하는 경우 다른 사이트를 선택할 수 없습니다. 기본 KMS를 편집하는 경우 특정 사이트를 선택할 수 없습니다.
포트	KMS 서버가 키 관리 상호 운용성 프로토콜(KMIP) 통신에 사용하는 포트입니다. 기본값은 KMIP 표준 포트인 5696입니다.
호스트 이름	KMS의 정규화된 도메인 이름 또는 IP 주소입니다. 참고**:** 서버 인증서의 SAN(Subject Alternative Name) 필드에는 여기에 입력한 FQDN 또는 IP 주소가 포함되어야 합니다. 그렇지 않으면 StorageGRID가 KMS 또는 KMS 클러스터의 모든 서버에 연결할 수 없습니다.

4. KMS 클러스터를 구성하는 경우, 클러스터의 각 서버에 호스트 이름을 추가하려면 *Add another hostname*을 선택하십시오.
5. *Continue*를 선택합니다.

   키 관리 서버 편집 마법사의 2단계(서버 인증서 업로드)가 나타납니다.
6. 서버 인증서를 교체해야 하는 경우 *찾아보기*를 선택하고 새 파일을 업로드하십시오.
7. *Continue*를 선택합니다.

   키 관리 서버 편집 마법사의 3단계(클라이언트 인증서 업로드)가 나타납니다.
8. 클라이언트 인증서와 클라이언트 인증서 개인 키를 교체해야 하는 경우, *찾아보기*를 선택하고 새 파일을 업로드하십시오.
9. *테스트 후 저장*을 선택합니다.

   영향을 받는 사이트의 모든 노드 암호화 어플라이언스 노드와 키 관리 서버 간의 연결을 테스트합니다. 모든 노드 연결이 유효하고 KMS에서 올바른 키가 발견되면 키 관리 서버가 키 관리 서버 페이지의 표에 추가됩니다.
10. 오류 메시지가 나타나면 메시지 내용을 검토하고 *확인*을 선택하십시오.

예를 들어, 이 KMS에 대해 선택한 사이트가 이미 다른 KMS에서 관리되고 있거나 연결 테스트에 실패한 경우 422: Unprocessable Entity 오류가 발생할 수 있습니다.

11. 연결 오류를 해결하기 전에 현재 구성을 저장해야 하는 경우 *강제 저장*을 선택하십시오.

> *강제 저장*을 선택하면 KMS 구성이 저장되지만, 각 어플라이언스에서 해당 KMS로의 외부 연결은 테스트되지 않습니다. 구성에 문제가 있는 경우 해당 사이트에서 노드 암호화가 활성화된 어플라이언스 노드를 재부팅할 수 없을 수 있습니다. 문제가 해결될 때까지 데이터에 액세스할 수 없게 될 수도 있습니다.

KMS 구성이 저장되었습니다.

12. 확인 경고 메시지를 검토하고 구성을 강제 저장하려면 *확인*을 선택합니다.

KMS 구성이 저장되지만 KMS 연결은 테스트되지 않습니다.

키 관리 서버(KMS) 제거

경우에 따라 키 관리 서버를 제거해야 할 수도 있습니다. 예를 들어, 사이트를 더 이상 사용하지 않는 경우 사이트별 KMS를 제거해야 할 수 있습니다.

시작하기 전에

- "키 관리 서버 사용 시 고려 사항 및 요구 사항"를 검토했습니다.
- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 다음이 있습니다. "루트 액세스 권한"

이 작업 정보

다음과 같은 경우 KMS를 제거할 수 있습니다.

- 사이트가 사용 중지되었거나 노드 암호화가 활성화된 어플라이언스 노드가 없는 경우 사이트별 KMS를 제거할 수 있습니다.
- 노드 암호화가 활성화된 어플라이언스 노드가 있는 각 사이트에 대해 사이트별 KMS가 이미 존재하는 경우 기본 KMS를 제거할 수 있습니다.

단계

1. * 구성 * > * 보안 * > * 키 관리 서버 * 를 선택합니다.

키 관리 서버 페이지가 나타나고 구성된 모든 키 관리 서버가 표시됩니다.

2. 제거할 KMS를 선택하고 작업 > *제거*를 선택합니다.

표에서 KMS 이름을 선택하고 KMS 세부 정보 페이지에서 *제거*를 선택하여 KMS를 삭제할 수도 있습니다.

3. 다음 사항이 사실인지 확인하십시오.
   - 노드 암호화가 활성화된 어플라이언스 노드가 없는 사이트에 대한 사이트별 KMS를 제거하려고 합니다.
   - 기본 KMS를 제거하려고 하지만, 노드 암호화가 있는 각 사이트에 대해 사이트별 KMS가 이미 존재합니다.
4. *예*를 선택합니다.

KMS 구성이 제거되었습니다.