보안 관리

StorageGRID software

NetApp
July 23, 2026

목차

보안 관리

StorageGRID에서 보안 관리

Grid Manager에서 다양한 보안 설정을 구성하여 StorageGRID 시스템의 보안을 강화할 수 있습니다.

암호화 관리

StorageGRID는 데이터를 암호화할 수 있는 여러 옵션을 제공합니다. "사용 가능한 암호화 방법을 검토하십시오."데이터 보호 요구 사항에 맞는 옵션을 선택해야 합니다.

인증서 관리

HTTP 연결에 사용되는 "서버 인증서 구성 및 관리" 또는 클라이언트 또는 사용자 신원을 서버에 인증하는 데 사용되는 클라이언트 인증서를 사용할 수 있습니다.

키 관리 서버 구성

"키 관리 서버"을 사용하면 어플라이언스가 데이터 센터에서 제거되더라도 StorageGRID 데이터를 보호할 수 있습니다. 어플라이언스 볼륨이 암호화된 후에는 노드가 KMS와 통신할 수 없는 한 어플라이언스의 데이터에 액세스할 수 없습니다.

> 암호화 키 관리를 사용하려면 어플라이언스를 그리드에 추가하기 전에 설치 중에 각 어플라이언스에 대해 노드 암호화 설정을 활성화해야 합니다.

프록시 설정 관리

S3 플랫폼 서비스 또는 클라우드 스토리지 풀을 사용하는 경우 스토리지 노드와 외부 S3 엔드포인트 사이에 "스토리지 프록시 서버"을 구성할 수 있습니다. HTTPS 또는 HTTP를 사용하여 AutoSupport 패키지를 전송하는 경우 관리 노드와 기술 지원 사이에 "관리자 프록시 서버"을 구성할 수 있습니다.

방화벽 제어

시스템 보안을 강화하기 위해 "외부 방화벽"에서 특정 포트를 열거나 닫음으로써 StorageGRID 관리 노드에 대한 액세스를 제어할 수 있습니다. 또한 각 노드의 "내부 방화벽"를 구성하여 네트워크 액세스를 제어할 수도 있습니다. 배포에 필요한 포트를 제외한 모든 포트에 대한 액세스를 차단할 수 있습니다.

StorageGRID 암호화 방법 검토

StorageGRID는 데이터를 암호화하는 여러 옵션을 제공합니다. 사용 가능한 방법을 검토하여 데이터 보호 요구 사항에 맞는 방법을 선택하십시오.

이 표는 StorageGRID에서 사용 가능한 암호화 방법에 대한 개략적인 요약을 제공합니다.

암호화 옵션	작동 방식	적용 대상
Grid Manager의 키 관리 서버(KMS)	StorageGRID 사이트에 대해 "키 관리 서버 구성" 설정하고 "어플라이언스에 대한 노드 암호화 활성화". 그런 다음 어플라이언스 노드가 KMS에 연결하여 키 암호화 키(KEK)를 요청합니다. 이 키는 각 볼륨의 데이터 암호화 키(DEK)를 암호화하고 복호화합니다.	설치 중에 *노드 암호화*가 활성화된 어플라이언스 노드입니다. 어플라이언스의 모든 데이터는 물리적 손실이나 데이터 센터 외부로의 반출로부터 보호됩니다. 참고: KMS를 사용한 암호화 키 관리는 스토리지 노드 및 서비스 어플라이언스에서만 지원됩니다.
StorageGRID Appliance Installer의 드라이브 암호화 페이지	어플라이언스에 하드웨어 암호화를 지원하는 드라이브가 포함된 경우 설치 중에 드라이브 암호를 설정할 수 있습니다. 드라이브 암호를 설정하면 암호를 모르는 사람은 시스템에서 제거된 드라이브에서 유효한 데이터를 복구할 수 없습니다. 설치를 시작하기 전에 하드웨어 구성 > *드라이브 암호화*로 이동하여 노드의 모든 StorageGRID 관리형 자체 암호화 드라이브에 적용되는 드라이브 암호를 설정하십시오.	자체 암호화 드라이브가 내장된 어플라이언스입니다. 보안 드라이브에 저장된 모든 데이터는 물리적 손실이나 데이터 센터 외부 반출로부터 보호됩니다. 드라이브 암호화는 SANtricity에서 관리하는 드라이브에는 적용되지 않습니다. 자체 암호화 드라이브와 SANtricity 컨트롤러가 탑재된 스토리지 어플라이언스를 사용하는 경우 SANtricity에서 드라이브 보안을 활성화할 수 있습니다.
SANtricity System Manager의 드라이브 보안	StorageGRID 어플라이언스에서 드라이브 보안 기능이 활성화된 경우, "SANtricity System Manager"을 사용하여 보안 키를 생성하고 관리할 수 있습니다. 보안 드라이브의 데이터에 액세스하려면 이 키가 필요합니다.	전체 디스크 암호화(FDE) 드라이브 또는 자체 암호화 드라이브가 있는 스토리지 어플라이언스. 보안 드라이브의 모든 데이터는 물리적 손실이나 데이터 센터 외부 반출로부터 보호됩니다. 일부 스토리지 어플라이언스 또는 서비스 어플라이언스와는 함께 사용할 수 없습니다.
저장된 객체 암호화	Grid Manager에서 "저장된 객체 암호화" 옵션을 활성화합니다. 활성화되면 버킷 수준 또는 객체 수준에서 암호화되지 않은 모든 새 객체는 수집 중에 암호화됩니다.	새롭게 수집된 S3 객체 데이터. 기존에 저장된 객체는 암호화되지 않습니다. 객체 메타데이터 및 기타 민감한 데이터도 암호화되지 않습니다.

암호화 옵션	작동 방식	적용 대상
S3 버킷 암호화	PutBucketEncryption 요청을 실행하여 버킷에 대한 암호화를 활성화합니다. 객체 수준에서 암호화되지 않은 모든 새 객체는 수집 중에 암호화됩니다.	새로 수집된 S3 객체 데이터만 해당됩니다. 버킷에 대해 암호화 방식을 지정해야 합니다. 기존 버킷 객체는 암호화되지 않습니다. 객체 메타데이터 및 기타 민감한 데이터는 암호화되지 않습니다. "버킷에 대한 작업"
S3 객체 서버 측 암호화(SSE)	객체를 저장하기 위해 S3 요청을 보내고 `x-amz-server-side-encryption` 요청 헤더를 포함합니다.	새로 수집된 S3 객체 데이터만 해당됩니다. 객체에 대해 암호화 방식을 지정해야 합니다. 객체 메타데이터 및 기타 민감한 데이터는 암호화되지 않습니다. StorageGRID가 키를 관리합니다. "서버 측 암호화 사용"
고객이 제공한 키를 사용한 S3 객체 서버 측 암호화(SSE-C)	객체를 저장하기 위해 S3 요청을 보내고 세 가지 요청 헤더를 포함합니다. • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	새로 수집된 S3 객체 데이터만 해당됩니다. 객체에 대해 암호화 방식을 지정해야 합니다. 객체 메타데이터 및 기타 민감한 데이터는 암호화되지 않습니다. 키는 StorageGRID 외부에서 관리됩니다. "서버 측 암호화 사용"
외부 볼륨 또는 데이터 저장소 암호화	배포 플랫폼에서 지원하는 경우 StorageGRID 외부의 암호화 방법을 사용하여 전체 볼륨 또는 데이터 저장소를 암호화할 수 있습니다.	모든 볼륨 또는 데이터 저장소가 암호화되었다고 가정할 때, 모든 객체 데이터, 메타데이터 및 시스템 구성 데이터. 외부 암호화 방식은 암호화 알고리즘과 키에 대한 더욱 강력한 제어를 제공합니다. 나열된 다른 방식들과 함께 사용할 수 있습니다.

암호화 옵션	작동 방식	적용 대상
StorageGRID 외부의 객체 암호화	StorageGRID에 수집되기 전에 StorageGRID 외부의 암호화 방법을 사용하여 오브젝트 데이터와 메타데이터를 암호화합니다.	객체 데이터 및 메타데이터만 암호화됩니다(시스템 구성 데이터는 암호화되지 않습니다). 외부 암호화 방식은 암호화 알고리즘과 키에 대한 더욱 강력한 제어를 제공합니다. 나열된 다른 방식들과 함께 사용할 수 있습니다. "Amazon Simple Storage Service - 사용자 가이드: 클라이언트 측 암호화를 사용한 데이터 보호"

여러 암호화 방법 사용

필요에 따라 여러 암호화 방식을 동시에 사용할 수 있습니다. 예를 들면 다음과 같습니다.

- KMS를 사용하여 어플라이언스 노드를 보호할 수 있으며, SANtricity System Manager의 드라이브 보안 기능을 사용하여 동일한 어플라이언스에 있는 자체 암호화 드라이브의 데이터를 "이중 암호화"할 수도 있습니다.
- KMS를 사용하여 어플라이언스 노드의 데이터를 보호할 수 있으며, 저장된 객체 암호화 옵션을 사용하여 객체가 수집될 때 모든 객체를 암호화할 수도 있습니다.

객체 중 일부만 암호화가 필요한 경우, 버킷 또는 개별 객체 수준에서 암호화를 제어하는 것을 고려하십시오. 여러 수준의 암호화를 활성화하면 추가적인 성능 비용이 발생합니다.

관련 정보

"FIPS 인증 암호화 옵션에 대해 알아보기"

인증서 관리

StorageGRID에서 보안 인증서 관리

보안 인증서는 StorageGRID 구성 요소 간, 그리고 StorageGRID 구성 요소와 외부 시스템 간에 안전하고 신뢰할 수 있는 연결을 생성하는 데 사용되는 작은 데이터 파일입니다.

StorageGRID는 두 가지 유형의 보안 인증서를 사용합니다.

- HTTPS 연결을 사용할 때는 *서버 인증서*가 필요합니다. 서버 인증서는 클라이언트와 서버 간의 안전한 연결을 설정하는 데 사용되며, 서버의 신원을 클라이언트에게 인증하고 데이터에 대한 안전한 통신 경로를 제공합니다. 서버와 클라이언트는 각각 인증서 사본을 보유합니다.
- *클라이언트 인증서*는 클라이언트 또는 사용자의 신원을 서버에 인증하여 비밀번호만 사용하는 것보다 더 안전한 인증을 제공합니다. 클라이언트 인증서는 데이터를 암호화하지 않습니다.

클라이언트가 HTTPS를 사용하여 서버에 연결하면 서버는 공개 키가 포함된 서버 인증서를 응답으로 보냅니다. 클라이언트는 서버 서명과 자신이 소유한 인증서의 서명을 비교합니다. 서명이 일치하면 클라이언트는 동일한 공개 키를 사용하여 서버와 세션을 시작합니다.

StorageGRID는 일부 연결(예: 로드 밸런서 엔드포인트)에 대해서는 서버 역할을 하고, 다른 연결(예: CloudMirror 복제 서비스)에 대해서는 클라이언트 역할을 합니다.

기본 그리드 **CA** 인증서

StorageGRID 시스템 설치 중에 내부 Grid CA 인증서를 생성하는 내장 인증 기관(CA)이 있습니다. 이 Grid CA 인증서는 기본적으로 내부 StorageGRID 트래픽을 보호하는 데 사용됩니다. 외부 인증 기관(CA)을 통해 조직의 정보 보안 정책을 완벽하게 준수하는 사용자 지정 인증서를 발급받을 수도 있습니다.

비프로덕션 환경에서는 Grid CA 인증서를 사용하십시오. 운영 환경에서는 외부 인증 기관에서 서명한 사용자 지정 인증서를 사용하십시오. 인증서가 없는 보안되지 않은 연결도 지원되지만 권장하지 않습니다.

- 사용자 지정 CA 인증서는 내부 인증서를 제거하지 않습니다. 다만, 서버 연결 확인을 위해 지정된 인증서는 사용자 지정 인증서여야 합니다.
- 모든 사용자 지정 인증서는 "서버 인증서에 대한 시스템 강화 지침"을(를) 충족해야 합니다.
- StorageGRID는 CA의 인증서를 단일 파일(CA 인증서 번들이라고 함)로 묶는 기능을 지원합니다.

> StorageGRID에는 모든 그리드에서 동일한 운영 체제 CA 인증서도 포함되어 있습니다. 운영 환경에서는 운영 체제 CA 인증서 대신 외부 인증 기관에서 서명한 사용자 지정 인증서를 지정해야 합니다.

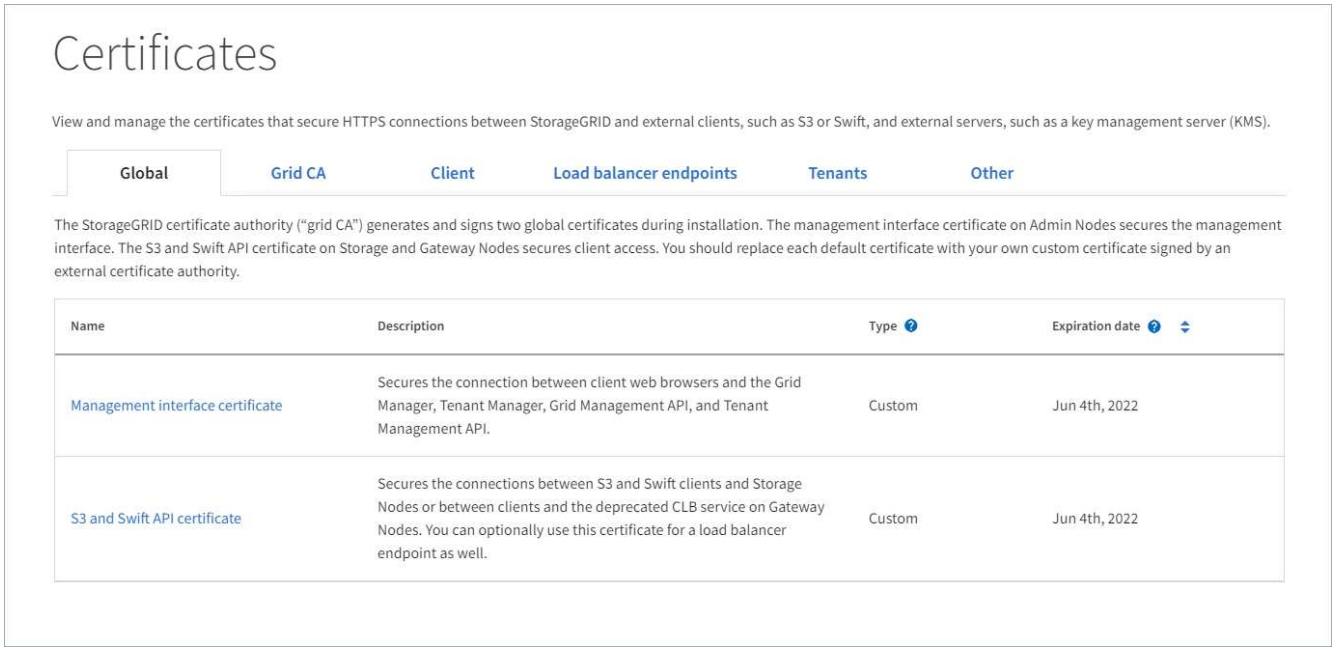
서버 및 클라이언트 인증서 유형의 변형은 여러 가지 방식으로 구현됩니다. 시스템을 구성하기 전에 특정 StorageGRID 구성에 필요한 모든 인증서를 준비해야 합니다.

보안 인증서 액세스

StorageGRID 인증서에 대한 모든 정보를 한 곳에서 확인할 수 있으며, 각 인증서의 구성 워크플로에 대한 링크도 제공됩니다.

단계

1. 그리드 관리자에서 구성 > 보안 > *인증서*를 선택합니다.



2. 인증서 페이지에서 탭을 선택하면 각 인증서 범주에 대한 정보를 확인하고 인증서 설정에 액세스할 수 있습니다. "적절한 권한"이(가) 있는 경우 탭에 액세스할 수 있습니다.

   - 전역: 웹 브라우저 및 외부 API 클라이언트에서 StorageGRID에 대한 액세스를 보호합니다.
   - **Grid CA**: 내부 StorageGRID 트래픽을 보호합니다.
   - 클라이언트: 외부 클라이언트와 StorageGRID Prometheus 데이터베이스 간의 연결을 보호합니다.
   - 로드 밸런서 엔드포인트: S3 클라이언트와 StorageGRID 로드 밸런서 간의 연결을 보호합니다.
   - 테넌트: ID 페더레이션 서버 또는 플랫폼 서비스 엔드포인트에서 S3 스토리지 리소스로의 연결을 보호합니다.
   - 기타: 특정 인증서가 필요한 StorageGRID 연결을 보호합니다.

     각 탭에 대한 설명과 추가 인증서 세부 정보 링크는 아래에 있습니다.

글로벌

글로벌 인증서는 웹 브라우저 및 외부 S3 API 클라이언트의 StorageGRID 액세스를 보호합니다. StorageGRID 인증 기관은 설치 중에 두 개의 글로벌 인증서를 생성합니다. 운영 환경에서는 외부 인증 기관에서 서명한 사용자 지정 인증서를 사용하는 것이 좋습니다.

- 관리 인터페이스 인증서: 클라이언트 웹 브라우저와 StorageGRID 관리 인터페이스 간의 연결을 보호합니다.
- S3 API 인증서: S3 클라이언트 애플리케이션이 객체 데이터를 업로드 및 다운로드하는 데 사용하는 스토리지 노드, 관리 노드 및 게이트웨이 노드에 대한 클라이언트 API 연결을 보호합니다.

설치된 글로벌 인증서에 대한 정보는 다음과 같습니다.

- 이름: 인증서 관리 링크가 포함된 인증서 이름입니다.
- 설명
- 유형: 사용자 지정 또는 기본값. + 그리드 보안 강화를 위해 항상 사용자 지정 인증서를 사용하는 것이 좋습니다.
- 만료일: 기본 인증서를 사용하는 경우 만료일이 표시되지 않습니다.

다음을 수행할 수 있습니다.

- 그리드 보안 강화를 위해 기본 인증서를 외부 인증 기관에서 서명한 사용자 지정 인증서로 교체하십시오.
  - "기본 StorageGRID 생성 관리 인터페이스 인증서 교체" Grid Manager 및 테넌트 관리자 연결에 사용됩니다.
  - "S3 API 인증서 교체"스토리지 노드 및 로드 밸런서 엔드포인트(선택 사항) 연결에 사용됩니다.
- "기본 관리 인터페이스 인증서 복원".
- "기본 S3 API 인증서 복원".
- "스크립트를 사용하여 자체 서명된 새 관리 인터페이스 인증서를 생성합니다.".
- "관리 인터페이스 인증서" 또는 "S3 API 인증서"을 복사하거나 다운로드합니다.

그리드 **CA**

StorageGRID 설치 중에 StorageGRID 인증 기관에서 생성된 그리드 CA 인증서은(는) 모든 내부 StorageGRID 트래픽을 보호합니다.

인증서 정보에는 인증서 만료일과 인증서 내용이 포함됩니다.

"Grid CA 인증서 복사 또는 다운로드"할 수 있지만, 변경할 수는 없습니다.

클라이언트

클라이언트 인증서외부 인증 기관에서 생성된 인증서는 외부 모니터링 도구와 StorageGRID Prometheus 데이터베이스 간의 연결을 보호합니다.

인증서 테이블에는 구성된 각 클라이언트 인증서에 대한 행이 있으며, 해당 인증서를 Prometheus 데이터베이스 액세스에 사용할 수 있는지 여부와 인증서 만료일이 표시됩니다.

다음을 수행할 수 있습니다.

- "클라이언트 인증서를 업로드하거나 새 인증서를 생성합니다."
- 인증서 이름을 선택하면 인증서 세부 정보가 표시됩니다. 여기서 다음을 수행할 수 있습니다.
  - "클라이언트 인증서 이름을 변경합니다."
  - "Prometheus 액세스 권한을 설정합니다."
  - "클라이언트 인증서를 업로드하고 교체하십시오."
  - "클라이언트 인증서를 복사하거나 다운로드하십시오."
  - "클라이언트 인증서를 제거합니다."
- 클라이언트 인증서를 빠르게 "편집", "연결" 또는 "제거"하려면 **Actions***를 선택하십시오**. *Actions** > *Remove*를 사용하여 최대 10개의 클라이언트 인증서를 선택하고 한 번에 제거할 수 있습니다.

로드 밸런서 엔드포인트

로드 밸런서 엔드포인트 인증서StorageGRID 게이트웨이 노드와 관리 노드에서 S3 클라이언트와 StorageGRID 로드 밸런서 서비스 간의 연결을 보호합니다.

로드 밸런서 엔드포인트 테이블에는 구성된 각 로드 밸런서 엔드포인트에 대한 행이 있으며, 해당 엔드포인트에 글로벌 S3 API 인증서 또는 사용자 지정 로드 밸런서 엔드포인트 인증서가 사용되는지 여부를 나타냅니다. 각 인증서의 만료일도 표시됩니다.

> ⓘ 엔드포인트 인증서 변경 사항이 모든 노드에 적용되는 데 최대 15분이 소요될 수 있습니다.

다음을 수행할 수 있습니다.

- "로드 밸런서 엔드포인트 보기", 인증서 세부 정보를 포함합니다.
- "FabricPool에 대한 로드 밸런서 엔드포인트 인증서를 지정합니다."
- "글로벌 S3 API 인증서 사용" 새로운 로드 밸런서 엔드포인트 인증서를 생성하는 대신.

테넌트

테넌트는 ID 페더레이션 서버 인증서 또는 플랫폼 서비스 엔드포인트 인증서를 사용하여 StorageGRID와의 연결을 보호할 수 있습니다.

테넌트 테이블에는 각 테넌트에 대한 행이 있으며 각 테넌트가 자체 ID 소스 또는 플랫폼 서비스를 사용할 권한이 있는지 여부를 나타냅니다.

다음을 수행할 수 있습니다.

- "Tenant Manager에 로그인하려면 테넌트 이름을 선택하세요."
- "테넌트 이름을 선택하여 테넌트 ID 페더레이션 세부 정보를 확인합니다."
- "테넌트 이름을 선택하여 테넌트 플랫폼 서비스 세부 정보를 확인합니다."
- "엔드포인트 생성 시 플랫폼 서비스 엔드포인트 인증서 지정"

기타

StorageGRID는 특정 목적을 위해 다른 보안 인증서를 사용합니다. 이러한 인증서는 기능 이름으로 나열됩니다. 다른 보안 인증서는 다음과 같습니다.

- 클라우드 스토리지 풀 인증서

- 이메일 알림 인증서
- 외부 syslog 서버 인증서
- 그리드 페더레이션 연결 인증서
- 신원 연동 인증서
- 키 관리 서버(KMS) 인증서
- 싱글 사인온 인증서

이 정보에는 함수가 사용하는 인증서 유형과 서버 및 클라이언트 인증서 만료일(해당하는 경우)이 표시됩니다. 함수 이름을 선택하면 브라우저 탭이 열리고 인증서 세부 정보를 보고 편집할 수 있습니다.

다른 인증서에 대한 정보를 보고 액세스하려면 "적절한 권한"이(가) 있어야 합니다.

다음을 수행할 수 있습니다.

- "S3, C2S S3 또는 Azure 클라우드 스토리지 풀 인증서 지정"
- "알림 이메일 알림에 사용할 인증서를 지정합니다."
- "외부 syslog 서버에 인증서 사용"
- "그리드 페더레이션 연결 인증서 교체"
- "ID 연동 인증서 보기 및 편집"
- "키 관리 서버(KMS) 서버 및 클라이언트 인증서 업로드"
- "신뢰 당사자 트러스트에 대한 SSO 인증서를 수동으로 지정"

보안 인증서 세부 정보

아래에는 각 보안 인증서 유형에 대한 설명과 구현 지침 링크가 제공됩니다.

관리 인터페이스 인증서

인증서 유형	설명	내비게이션 위치	세부 정보
서버	클라이언트 웹 브라우저와 StorageGRID 관리 인터페이스 간의 연결을 인증하여 사용자가 보안 경고 없이 Grid Manager 및 Tenant Manager에 액세스할 수 있도록 합니다. 이 인증서는 Grid Management API 및 Tenant Management API 연결도 인증합니다. 설치 중에 생성된 기본 인증서를 사용하거나 사용자 지정 인증서를 업로드할 수 있습니다.	구성 > 보안 > 인증서*로 이동하여 *전역 탭을 선택한 다음 *관리 인터페이스 인증서*를 선택합니다.	"관리 인터페이스 인증서 구성"

S3 API 인증서

인증서 유형	설명	내비게이션 위치	세부 정보
서버	스토리지 노드 및 로드 밸런서 엔드포인트에 대한 보안 S3 클라이언트 연결을 인증합니다(선택 사항).	구성 > 보안 > 인증서*로 이동하여 *전역 탭을 선택한 다음 *S3 API 인증서*를 선택합니다.	"S3 API 인증서 구성"

그리드 **CA** 인증서

기본 그리드 CA 인증서 설명을 참조하십시오.

관리자 클라이언트 인증서

인증서 유형	설명	내비게이션 위치	세부 정보
클라이언트	각 클라이언트에 설치되어 StorageGRID 외부 클라이언트 액세스를 인증할 수 있도록 합니다. • 승인된 외부 클라이언트가 StorageGRID Prometheus 데이터베이스에 액세스할 수 있도록 합니다. • 외부 도구를 사용하여 StorageGRID를 안전하게 모니터링할 수 있습니다.	구성 > 보안 > 인증서*로 이동한 다음 *클라이언트 탭을 선택합니다.	"클라이언트 인증서 구성"

로드 밸런서 엔드포인트 인증서

인증서 유형	설명	내비게이션 위치	세부 정보
서버	StorageGRID 게이트웨이 노드 및 관리 노드의 StorageGRID 로드 밸런서 서비스와 S3 클라이언트 간의 연결을 인증합니다. 로드 밸런서 엔드포인트를 구성할 때 로드 밸런서 인증서를 업로드하거나 생성할 수 있습니다. 클라이언트 애플리케이션은 StorageGRID에 연결하여 객체 데이터를 저장하고 검색할 때 로드 밸런서 인증서를 사용합니다. 사용자 지정 버전의 글로벌 S3 API 인증서 인증서를 사용하여 로드 밸런서 서비스에 대한 연결을 인증할 수도 있습니다. 글로벌 인증서를 로드 밸런서 연결 인증에 사용하는 경우 각 로드 밸런서 엔드포인트에 대해 별도의 인증서를 업로드하거나 생성할 필요가 없습니다. 참고: 로드 밸런서 인증에 사용되는 인증서는 StorageGRID 정상 작동 중에 가장 많이 사용되는 인증서입니다.	구성 > 네트워크 > 로드 밸런서 엔드포인트	• "로드 밸런서 엔드포인트 구성" • "FabricPool용 로드 밸런서 엔드포인트 생성"

클라우드 스토리지 풀 엔드포인트 인증서

인증서 유형	설명	내비게이션 위치	세부 정보
서버	StorageGRID 클라우드 스토리지 풀에서 S3 Glacier 또는 Microsoft Azure Blob 스토리지와 같은 외부 스토리지 위치로의 연결을 인증합니다. 각 클라우드 공급자 유형마다 다른 인증서가 필요합니다.	**ILM** > 스토리지 풀	"클라우드 스토리지 풀 생성"

이메일 알림 인증서

인증서 유형	설명	내비게이션 위치	세부 정보
서버와 클라이언트	StorageGRID 알림 전송에 사용되는 SMTP 이메일 서버와 StorageGRID 간의 연결을 인증합니다. • SMTP 서버와의 통신에 전송 계층 보안(TLS)이 필요한 경우 이메일 서버 CA 인증서를 지정해야 합니다. • SMTP 이메일 서버에서 인증을 위해 클라이언트 인증서가 필요한 경우에만 클라이언트 인증서를 지정하십시오.	알림 > 이메일 설정	"알림에 대한 이메일 알림 설정"

외부 **syslog** 서버 인증서

인증서 유형	설명	내비게이션 위치	세부 정보
서버	StorageGRID에서 이벤트를 기록하는 외부 syslog 서버 간의 TLS 또는 RELP/TLS 연결을 인증합니다. 참고: 외부 syslog 서버에 대한 TCP, RELP/TCP 및 UDP 연결에는 외부 syslog 서버 인증서가 필요하지 않습니다.	구성 > 모니터링 > 감사 및 **syslog** 서버	"외부 syslog 서버 사용"

그리드 페더레이션 연결 인증서

인증서 유형	설명	내비게이션 위치	세부 정보
서버와 클라이언트	현재 StorageGRID 시스템과 그리드 페더레이션 연결에 있는 다른 그리드 간에 전송되는 정보를 인증하고 암호화합니다.	구성 > 시스템 > 그리드 페더레이션	• "그리드 페더레이션 연결 생성" • "연결 인증서 순환"

ID 페더레이션 인증서

인증서 유형	설명	내비게이션 위치	세부 정보
서버	StorageGRID와 Active Directory, OpenLDAP 또는 Oracle Directory Server와 같은 외부 ID 공급자 간의 연결을 인증합니다. 관리자 그룹과 사용자를 외부 시스템에서 관리할 수 있도록 하는 ID 페더레이션에 사용됩니다.	구성 > 액세스 제어 > **ID** 연동	"ID 페더레이션 사용"

키 관리 서버**(KMS)** 인증서

인증서 유형	설명	내비게이션 위치	세부 정보
서버와 클라이언트	StorageGRID와 외부 키 관리 서버(KMS) 간의 연결을 인증합니다. KMS는 StorageGRID 어플라이언스 노드에 암호화 키를 제공합니다.	구성 > 보안 > 키 관리 서버	"키 관리 서버(KMS) 추가"

플랫폼 서비스 엔드포인트 인증서

인증서 유형	설명	내비게이션 위치	세부 정보
서버	StorageGRID 플랫폼 서비스와 S3 스토리지 리소스 간의 연결을 인증합니다.	테넌트 관리자 > 스토리지**(S3)** > 플랫폼 서비스 엔드포인트	"플랫폼 서비스 엔드포인트 생성" "플랫폼 서비스 엔드포인트 편집"

싱글 사인온**(SSO)** 인증서

인증서 유형	설명	내비게이션 위치	세부 정보
서버	Active Directory Federation Services(AD FS)와 같은 ID 페더레이션 서비스와 SSO(Single Sign-On) 요청에 사용되는 StorageGRID 간의 연결을 인증합니다.	구성 > 접근 제어 > 싱글 사인온	"싱글 사인온(SSO) 구성"

인증서 예시

예시 **1:** 로드 밸런서 서비스

이 예시에서 StorageGRID는 서버 역할을 합니다.

1. StorageGRID에서 로드 밸런서 엔드포인트를 구성하고 서버 인증서를 업로드하거나 생성합니다.
2. 로드 밸런싱 엔드포인트에 대한 S3 클라이언트 연결을 구성하고 동일한 인증서를 클라이언트에 업로드합니다.
3. 클라이언트가 데이터를 저장하거나 검색하려는 경우, HTTPS를 사용하여 로드 밸런서 엔드포인트에 연결합니다.
4. StorageGRID는 공개 키가 포함된 서버 인증서와 개인 키를 기반으로 한 서명을 응답으로 보냅니다.
5. 클라이언트는 서버의 서명과 자신이 보유한 인증서 사본의 서명을 비교합니다. 서명이 일치하면 클라이언트는 동일한 공개 키를 사용하여 세션을 시작합니다.
6. 클라이언트가 객체 데이터를 StorageGRID에 전송합니다.

예시 **2:** 외부 키 관리 서버**(KMS)**

이 예시에서 StorageGRID는 클라이언트 역할을 합니다.

1. 외부 키 관리 서버 소프트웨어를 사용하여 StorageGRID를 KMS 클라이언트로 구성하고 CA에서 서명한 서버 인증서, 공개 클라이언트 인증서 및 클라이언트 인증서용 개인 키를 얻습니다.
2. 그리드 관리자를 사용하여 KMS 서버를 구성하고 서버 및 클라이언트 인증서와 클라이언트 개인 키를 업로드합니다.
3. StorageGRID 노드가 암호화 키가 필요한 경우, 인증서의 데이터와 개인 키를 기반으로 한 서명을 포함하는 요청을 KMS 서버에 보냅니다.
4. KMS 서버는 인증서 서명을 검증하고 StorageGRID를 신뢰할 수 있다고 결정합니다.
5. KMS 서버는 유효성이 검증된 연결을 사용하여 응답합니다.

StorageGRID에서 지원되는 서버 인증서 유형

StorageGRID 시스템은 RSA 또는 ECDSA(Elliptic Curve Digital Signature Algorithm)로 암호화된 사용자 지정 인증서를 지원합니다.

보안 정책에 사용할 암호화 유형은 서버 인증서 유형과 일치해야 합니다. 예를 들어 RSA 암호화에는 RSA 인증서가 필요하고 ECDSA 암호화에는 ECDSA 인증서가 필요합니다. 자세한 내용은 "보안 인증서 관리"을 참조하십시오. 서버 인증서와 호환되지 않는 사용자 지정 보안 정책을 구성한 경우 "일시적으로 기본 보안 정책으로 되돌립니다.".

StorageGRID 클라이언트 연결을 보호하는 방법에 대한 자세한 내용은 "S3 클라이언트 보안"을 참조하십시오.

StorageGRID에서 관리 인터페이스 인증서를 구성합니다

기본 관리 인터페이스 인증서를 사용자 지정 인증서 하나로 교체하면 사용자가 보안 경고 없이 그리드 관리자 및 테넌트 관리자에 액세스할 수 있습니다. 또한 기본 관리 인터페이스 인증서로 되돌리거나 새 인증서를 생성할 수도 있습니다.

이 작업 정보

기본적으로 모든 관리 노드에는 그리드 CA에서 서명한 인증서가 발급됩니다. 이러한 CA 서명 인증서는 단일 공통 사용자 지정 관리 인터페이스 인증서와 해당 개인 키로 대체할 수 있습니다.

모든 관리 노드에 단일 사용자 지정 관리 인터페이스 인증서가 사용되므로 클라이언트가 그리드 관리자 및 테넌트 관리자에 연결할 때 호스트 이름을 확인해야 하는 경우 인증서를 와일드카드 또는 다중 도메인 인증서로 지정해야 합니다. 그리드의 모든 관리 노드와 일치하도록 사용자 지정 인증서를 정의하십시오.

서버에서 구성을 완료해야 하며, 사용 중인 루트 인증 기관(CA)에 따라 사용자는 Grid Manager 및 Tenant Manager에 액세스하는 데 사용할 웹 브라우저에 Grid CA 인증서를 설치해야 할 수도 있습니다.

서버 인증서 오류로 인해 운영이 중단되는 것을 방지하기 위해, 이 서버 인증서가 만료되려고 할 때 관리 인터페이스용 서버 인증서 만료 알림이 트리거됩니다. 필요한 경우, 구성 > 보안 > *인증서*를 선택하고 전역 탭에서 관리 인터페이스 인증서의 만료일을 확인하여 현재 인증서의 만료일을 볼 수 있습니다.

IP 주소 대신 도메인 이름을 사용하여 Grid Manager 또는 Tenant Manager에 액세스하는 경우 다음 중 하나가 발생하면 브라우저에 인증서 오류가 표시되고 이를 우회할 수 있는 옵션이 제공되지 않습니다.

- 사용자 지정 관리 인터페이스 인증서가 만료됩니다.
- 귀하 사용자 지정 관리 인터페이스 인증서에서 기본 서버 인증서로 되돌리기.

사용자 지정 관리 인터페이스 인증서 추가

사용자 지정 관리 인터페이스 인증서를 추가하려면 자체 인증서를 제공하거나 Grid Manager를 사용하여 인증서를 생성할 수 있습니다.

단계

1. 구성 > 보안 > *인증서*를 선택합니다.
2. 전역 탭에서 *관리 인터페이스 인증서*를 선택합니다.
3. *사용자 지정 인증서 사용*을 선택합니다.
4. 인증서를 업로드하거나 생성합니다.

인증서 업로드

필요한 서버 인증서 파일을 업로드합니다.

a. *인증서 업로드*를 선택합니다.

b. 필요한 서버 인증서 파일을 업로드합니다.

   - 서버 인증서: 사용자 지정 서버 인증서 파일(PEM 인코딩).
   - 인증서 개인 키: 사용자 지정 서버 인증서 개인 키 파일 (`.key`).

     EC 개인 키는 224비트 이상이어야 합니다. RSA 개인 키는 2048비트 이상이어야 합니다.

   - **CA** 번들: 각 중간 발급 인증 기관(CA)의 인증서가 포함된 단일 선택적 파일입니다. 이 파일에는 각 CA 인증서 파일이 PEM 형식으로 인코딩되어 인증서 체인 순서대로 연결되어 있어야 합니다.

c. *인증서 세부 정보*를 펼치면 업로드한 각 인증서의 메타데이터를 볼 수 있습니다. 선택적으로 CA 번들을 업로드한 경우 각 인증서가 별도의 탭에 표시됩니다.

   - 인증서 파일을 저장하려면 *인증서 다운로드*를 선택하고, 인증서 번들을 저장하려면 *CA 번들 다운로드*를 선택하십시오.

     인증서 파일 이름과 다운로드 위치를 지정하십시오. 파일을 확장자 `.pem`로 저장하십시오.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

   - 인증서 내용을 복사하여 다른 곳에 붙여넣으려면 인증서 **PEM** 복사 또는 *CA 번들 PEM 복사*를 선택하십시오.

d. *저장*을 선택합니다. + 사용자 지정 관리 인터페이스 인증서는 Grid Manager, Tenant Manager, Grid Manager API 또는 Tenant Manager API에 대한 모든 후속 새 연결에 사용됩니다.

인증서 생성

서버 인증서 파일을 생성합니다.

운영 환경의 모범 사례는 외부 인증 기관에서 서명한 사용자 지정 관리 인터페이스 인증서를 사용하는 것입니다.

a. *인증서 생성*을 선택합니다.

b. 인증서 정보를 지정합니다:

필드	설명
도메인 이름	인증서에 포함할 하나 이상의 정규화된 도메인 이름입니다. 여러 도메인 이름을 나타내려면 와일드카드 문자 *를 사용하십시오.
IP	인증서에 포함할 IP 주소를 하나 이상 입력하십시오.

필드	설명
제목 (선택 사항)	X.509 인증서 소유자의 주체 또는 고유명칭(DN). 이 필드에 값을 입력하지 않으면 생성된 인증서는 첫 번째 도메인 이름 또는 IP 주소를 주체 공통 이름(CN)으로 사용합니다.
유효 기간	인증서 발급일로부터 만료일까지의 일수입니다.
키 사용 확장 추가	선택된 경우(기본값이며 권장됨), 생성된 인증서에 키 사용 및 확장 키 사용 확장 기능이 추가됩니다. 이러한 확장 기능은 인증서에 포함된 키의 용도를 정의합니다. 참고: 인증서에 이러한 확장이 포함된 경우 이전 클라이언트와의 연결 문제가 발생하지 않는 한 이 확인란을 선택한 상태로 두십시오.

c. *생성*을 선택합니다.

d. 생성된 인증서의 메타데이터를 보려면 *인증서 세부 정보*를 선택하십시오.

   - 인증서 파일을 저장하려면 *인증서 다운로드*를 선택합니다.

     인증서 파일 이름과 다운로드 위치를 지정하십시오. 파일을 확장자 `.pem`로 저장하십시오.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

   - 인증서 내용을 복사하여 다른 곳에 붙여넣으려면 *인증서 PEM 복사*를 선택하십시오.

e. *저장*을 선택합니다. + 사용자 지정 관리 인터페이스 인증서는 Grid Manager, Tenant Manager, Grid Manager API 또는 Tenant Manager API에 대한 모든 후속 새 연결에 사용됩니다.

5. 웹 브라우저가 업데이트되도록 페이지를 새로 고침하십시오.

   새 인증서를 업로드하거나 생성한 후, 관련 인증서 만료 알림이 모두 사라지는 데 최대 하루가 소요될 수 있습니다.

6. 사용자 지정 관리 인터페이스 인증서를 추가하면 관리 인터페이스 인증서 페이지에 사용 중인 인증서에 대한 자세한 정보가 표시됩니다. + 필요에 따라 인증서 PEM을 다운로드하거나 복사할 수 있습니다.

기본 관리 인터페이스 인증서 복원

Grid Manager 및 Tenant Manager 연결에 기본 관리 인터페이스 인증서를 다시 사용하도록 되돌릴 수 있습니다.

단계

1. 구성 > 보안 > *인증서*를 선택합니다.
2. 전역 탭에서 *관리 인터페이스 인증서*를 선택합니다.
3. *기본 인증서 사용*을 선택합니다.

기본 관리 인터페이스 인증서를 복원하면 구성한 사용자 지정 서버 인증서 파일이 삭제되어 시스템에서 복구할 수 없습니다. 이후의 모든 새 클라이언트 연결에는 기본 관리 인터페이스 인증서가 사용됩니다.

4. 웹 브라우저가 업데이트되도록 페이지를 새로 고침하십시오.

스크립트를 사용하여 자체 서명된 새 관리 인터페이스 인증서를 생성합니다.

호스트 이름 유효성 검사가 엄격하게 필요한 경우 스크립트를 사용하여 관리 인터페이스 인증서를 생성할 수 있습니다.

시작하기 전에

- "특정 액세스 권한"이(가) 있습니다.
- You have the `Passwords.txt` 파일을 가지고 계시네요.

이 작업 정보

운영 환경의 모범 사례는 외부 인증 기관에서 서명한 인증서를 사용하는 것입니다.

단계

1. 각 관리 노드의 정규화된 도메인 이름(FQDN)을 확보하십시오.
2. 기본 관리 노드에 로그인합니다.
   a. 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`
   b. `Passwords.txt` 파일에 나와 있는 비밀번호를 입력하십시오.
   c. 루트 권한으로 전환하려면 다음 명령을 입력하십시오. `su -`
   d. `Passwords.txt` 파일에 나와 있는 비밀번호를 입력하십시오.

   루트 계정으로 로그인하면 프롬프트가 `$`에서 `#`로 변경됩니다.
3. StorageGRID에 새 자체 서명 인증서를 구성합니다.

```
$ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
```

   - `--domains`의 경우, 모든 관리 노드의 정규화된 도메인 이름을 나타내기 위해 와일드카드를 사용하십시오. 예를 들어, `*.ui.storagegrid.example.com`는 * 와일드카드를 사용하여 `admin1.ui.storagegrid.example.com`와 `admin2.ui.storagegrid.example.com`를 나타냅니다.
   - Set `--type` to `management` 관리 인터페이스 인증서를 구성하려면 이 옵션을 선택하십시오. 이 인증서는 Grid Manager 및 Tenant Manager에서 사용됩니다.
   - 기본적으로 생성된 인증서는 1년(365일) 동안 유효하며 만료되기 전에 다시 생성해야 합니다. `--days` 인수를 사용하여 기본 유효 기간을 재정의할 수 있습니다.

> 인증서의 유효 기간은 `make-certificate`가 실행되는 시점부터 시작됩니다. 관리 클라이언트가 StorageGRID와 동일한 시간 소스에 동기화되어 있는지 확인해야 합니다. 그렇지 않으면 클라이언트가 인증서를 거부할 수 있습니다.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 720
```

결과 출력에는 관리 API 클라이언트에 필요한 공개 인증서가 포함되어 있습니다.

4. 인증서를 선택하고 복사합니다.

   선택 항목에 BEGIN 태그와 END 태그를 포함하세요.

5. 명령 셸에서 로그아웃하세요. `$ exit`
6. 인증서가 구성되었는지 확인하십시오.
   a. 그리드 관리자에 액세스합니다.
   b. 구성 > 보안 > *인증서*를 선택합니다.
   c. 전역 탭에서 *관리 인터페이스 인증서*를 선택합니다.
7. 복사한 공개 인증서를 사용하도록 관리 클라이언트를 구성하십시오. BEGIN 및 END 태그를 포함하십시오.

관리 인터페이스 인증서 다운로드 또는 복사

관리 인터페이스 인증서 내용을 저장하거나 복사하여 다른 곳에서 사용할 수 있습니다.

단계

1. 구성 > 보안 > *인증서*를 선택합니다.
2. 전역 탭에서 *관리 인터페이스 인증서*를 선택합니다.
3. 서버 또는 **CA** 번들 탭을 선택한 다음 인증서를 다운로드하거나 복사하십시오.

인증서 파일 또는 **CA** 번들 다운로드

인증서 또는 CA 번들 `.pem` 파일을 다운로드하십시오. 선택 사항인 CA 번들을 사용하는 경우 번들에 포함된 각 인증서가 별도의 하위 탭에 표시됩니다.

a. 인증서 다운로드 또는 *CA 번들 다운로드*를 선택합니다.

   CA 번들을 다운로드하는 경우, CA 번들의 보조 탭에 있는 모든 인증서가 단일 파일로 다운로드됩니다.

b. 인증서 파일 이름과 다운로드 위치를 지정하십시오. 파일을 확장자 `.pem`로 저장하십시오.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

인증서 또는 **CA** 번들 **PEM** 복사

인증서 텍스트를 복사하여 다른 곳에 붙여넣으세요. 선택 사항인 CA 번들을 사용하는 경우, 번들에 포함된 각 인증서는 별도의 하위 탭에 표시됩니다.

a. 인증서 **PEM** 복사 또는 *CA 번들 PEM 복사*를 선택합니다.

   CA 번들을 복사하는 경우 CA 번들의 보조 탭에 있는 모든 인증서가 함께 복사됩니다.

b. 복사한 인증서를 텍스트 편집기에 붙여넣으세요.

c. 텍스트 파일을 확장자 `.pem`로 저장하세요.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

StorageGRID에서 S3 API 인증서 구성

스토리지 노드 또는 로드 밸런서 엔드포인트에 대한 S3 클라이언트 연결에 사용되는 서버 인증서를 교체하거나 복원할 수 있습니다. 교체용 사용자 지정 서버 인증서는 조직에 특화되어 있습니다.

Swift 관련 세부 정보는 이 버전의 문서 사이트에서 삭제되었습니다. 을 참조하십시오. "StorageGRID 11.8: S3 및 Swift API 인증서 구성"

이 작업 정보

기본적으로 모든 스토리지 노드에는 그리드 CA에서 서명한 X.509 서버 인증서가 발급됩니다. 이러한 CA 서명 인증서는 단일 공통 사용자 지정 서버 인증서와 해당 개인 키로 대체할 수 있습니다.

모든 스토리지 노드에 단일 사용자 지정 서버 인증서가 사용되므로 클라이언트가 스토리지 엔드포인트에 연결할 때 호스트 이름을 확인해야 하는 경우 인증서를 와일드카드 또는 다중 도메인 인증서로 지정해야 합니다. 그리드의 모든 스토리지 노드와 일치하도록 사용자 지정 인증서를 정의하십시오.

서버에서 구성을 완료한 후에는 사용 중인 루트 인증 기관(CA)에 따라 시스템에 액세스하는 데 사용할 S3 API 클라이언트에 Grid CA 인증서를 설치해야 할 수도 있습니다.

서버 인증서 오류로 인해 운영이 중단되는 것을 방지하기 위해 루트 서버 인증서 만료 예정 시 **S3 API**용 글로벌 서버 인증서 만료 알림이 발생합니다. 필요에 따라 구성 > 보안 > *인증서*를 선택하고 글로벌 탭에서 S3 API 인증서의 만료일을 확인하여 현재 인증서의 만료일을 확인할 수 있습니다.

사용자 지정 S3 API 인증서를 업로드하거나 생성할 수 있습니다.

사용자 지정 **S3 API** 인증서 추가

단계

1. 구성 > 보안 > *인증서*를 선택합니다.
2. 글로벌 탭에서 *S3 API 인증서*를 선택합니다.
3. *사용자 지정 인증서 사용*을 선택합니다.
4. 인증서를 업로드하거나 생성합니다.

인증서 업로드

필요한 서버 인증서 파일을 업로드합니다.

a. *인증서 업로드*를 선택합니다.

b. 필요한 서버 인증서 파일을 업로드합니다.

   - 서버 인증서: 사용자 지정 서버 인증서 파일(PEM 인코딩).
   - 인증서 개인 키: 사용자 지정 서버 인증서 개인 키 파일 (`.key`).

     EC 개인 키는 224비트 이상이어야 합니다. RSA 개인 키는 2048비트 이상이어야 합니다.

   - **CA** 번들: 각 중간 발급 인증 기관의 인증서가 포함된 단일 파일(선택 사항). 이 파일에는 각 CA 인증서 파일이 PEM 형식으로 인코딩되어 인증서 체인 순서대로 연결되어 있어야 합니다.

c. 인증서 세부 정보를 선택하면 업로드된 각 사용자 지정 S3 API 인증서의 메타데이터와 PEM이 표시됩니다. 선택적으로 CA 번들을 업로드한 경우 각 인증서가 별도의 탭에 표시됩니다.

   - 인증서 파일을 저장하려면 *인증서 다운로드*를 선택하고, 인증서 번들을 저장하려면 *CA 번들 다운로드*를 선택하십시오.

     인증서 파일 이름과 다운로드 위치를 지정하십시오. 파일을 확장자 `.pem`로 저장하십시오.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

   - 인증서 내용을 복사하여 다른 곳에 붙여넣으려면 인증서 **PEM** 복사 또는 *CA 번들 PEM 복사*를 선택하십시오.

d. *저장*을 선택하세요.

   사용자 지정 서버 인증서는 이후의 새로운 S3 클라이언트 연결에 사용됩니다.

인증서 생성

서버 인증서 파일을 생성합니다.

a. *인증서 생성*을 선택합니다.

b. 인증서 정보를 지정합니다:

필드	설명
도메인 이름	인증서에 포함할 하나 이상의 정규화된 도메인 이름입니다. 여러 도메인 이름을 나타내려면 와일드카드 문자 *를 사용하십시오.
IP	인증서에 포함할 IP 주소를 하나 이상 입력하십시오.

필드	설명
제목 (선택 사항)	X.509 인증서 소유자의 주체 또는 고유명칭(DN). 이 필드에 값을 입력하지 않으면 생성된 인증서는 첫 번째 도메인 이름 또는 IP 주소를 주체 공통 이름(CN)으로 사용합니다.
유효 기간	인증서 발급일로부터 만료일까지의 일수입니다.
키 사용 확장 추가	선택된 경우(기본값이며 권장됨), 생성된 인증서에 키 사용 및 확장 키 사용 확장 기능이 추가됩니다. 이러한 확장 기능은 인증서에 포함된 키의 용도를 정의합니다. 참고: 인증서에 이러한 확장이 포함된 경우 이전 클라이언트와의 연결 문제가 발생하지 않는 한 이 확인란을 선택한 상태로 두십시오.

c. *생성*을 선택합니다.

d. 생성된 사용자 지정 S3 API 인증서의 메타데이터 및 PEM을 표시하려면 *인증서 세부 정보*를 선택하십시오.

   - 인증서 파일을 저장하려면 *인증서 다운로드*를 선택합니다.

     인증서 파일 이름과 다운로드 위치를 지정하십시오. 파일을 확장자 `.pem`로 저장하십시오.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

   - 인증서 내용을 복사하여 다른 곳에 붙여넣으려면 *인증서 PEM 복사*를 선택하십시오.

e. *저장*을 선택하세요.

   사용자 지정 서버 인증서는 이후의 새로운 S3 클라이언트 연결에 사용됩니다.

5. 기본 StorageGRID 서버 인증서, 업로드된 CA 서명 인증서 또는 생성된 사용자 지정 인증서에 대한 메타데이터를 표시하려면 탭을 선택하십시오.

   새 인증서를 업로드하거나 생성한 후, 관련 인증서 만료 알림이 모두 사라지는 데 최대 하루가 소요될 수 있습니다.

6. 웹 브라우저가 업데이트되도록 페이지를 새로 고침하십시오.

7. 사용자 지정 S3 API 인증서를 추가하면 S3 API 인증서 페이지에 사용 중인 사용자 지정 S3 API 인증서에 대한 자세한 정보가 표시됩니다. + 필요에 따라 인증서 PEM을 다운로드하거나 복사할 수 있습니다.

기본 **S3 API** 인증서 복원

스토리지 노드에 대한 S3 클라이언트 연결에는 기본 S3 API 인증서를 다시 사용할 수 있습니다. 하지만 로드 밸런서 엔드포인트에는 기본 S3 API 인증서를 사용할 수 없습니다.

단계

1. 구성 > 보안 > *인증서*를 선택합니다.
2. 글로벌 탭에서 *S3 API 인증서*를 선택합니다.
3. *기본 인증서 사용*을 선택합니다.

   글로벌 S3 API 인증서의 기본 버전을 복원하면 구성한 사용자 지정 서버 인증서 파일이 삭제되어 시스템에서 복구할 수 없습니다. 이후 스토리지 노드에 대한 새로운 S3 클라이언트 연결에는 기본 S3 API 인증서가 사용됩니다.

4. 경고를 확인하고 기본 S3 API 인증서를 복원하려면 *확인*을 선택하십시오.

   루트 액세스 권한이 있고 사용자 지정 S3 API 인증서를 로드 밸런서 엔드포인트 연결에 사용한 경우, 기본 S3 API 인증서를 사용하여 더 이상 액세스할 수 없는 로드 밸런서 엔드포인트 목록이 표시됩니다. 영향을 받는 엔드포인트를 편집하거나 제거하려면 "로드 밸런서 엔드포인트 구성"으로 이동하십시오.

5. 웹 브라우저가 업데이트되도록 페이지를 새로 고침하십시오.

S3 API 인증서 다운로드 또는 복사

S3 API 인증서 내용을 저장하거나 복사하여 다른 곳에서 사용할 수 있습니다.

단계

1. 구성 > 보안 > *인증서*를 선택합니다.
2. 글로벌 탭에서 *S3 API 인증서*를 선택합니다.
3. 서버 또는 **CA** 번들 탭을 선택한 다음 인증서를 다운로드하거나 복사하십시오.

인증서 파일 또는 **CA** 번들 다운로드

인증서 또는 CA 번들 `.pem` 파일을 다운로드하십시오. 선택 사항인 CA 번들을 사용하는 경우 번들에 포함된 각 인증서가 별도의 하위 탭에 표시됩니다.

a. 인증서 다운로드 또는 *CA 번들 다운로드*를 선택합니다.

   CA 번들을 다운로드하는 경우, CA 번들의 보조 탭에 있는 모든 인증서가 단일 파일로 다운로드됩니다.

b. 인증서 파일 이름과 다운로드 위치를 지정하십시오. 파일을 확장자 `.pem`로 저장하십시오.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

인증서 또는 **CA** 번들 **PEM** 복사

인증서 텍스트를 복사하여 다른 곳에 붙여넣으세요. 선택 사항인 CA 번들을 사용하는 경우, 번들에 포함된 각 인증서는 별도의 하위 탭에 표시됩니다.

a. 인증서 **PEM** 복사 또는 *CA 번들 PEM 복사*를 선택합니다.

   CA 번들을 복사하는 경우 CA 번들의 보조 탭에 있는 모든 인증서가 함께 복사됩니다.

b. 복사한 인증서를 텍스트 편집기에 붙여넣으세요.

c. 텍스트 파일을 확장자 `.pem`로 저장하세요.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

관련 정보

- "S3 REST API 사용"
- "S3 엔드포인트 도메인 이름 구성"

StorageGRID Grid CA 인증서를 복사합니다

StorageGRID 내부 트래픽 보안을 위해 자체 인증 기관(CA)을 사용합니다. 사용자가 자체 인증서를 업로드하더라도 이 인증서는 변경되지 않습니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- "특정 액세스 권한"이(가) 있습니다.

이 작업 정보

사용자 지정 서버 인증서가 구성된 경우 클라이언트 애플리케이션은 사용자 지정 서버 인증서를 사용하여 서버를 확인해야 합니다. StorageGRID 시스템의 CA 인증서를 복사해서는 안 됩니다.

단계

1. 구성 > 보안 > 인증서*를 선택한 다음 *그리드 **CA** 탭을 선택합니다.

2. **PEM** 인증서 섹션에서 인증서를 다운로드하거나 복사합니다.

인증서 파일 다운로드

인증서 `.pem` 파일을 다운로드하세요.

a. *인증서 다운로드*를 선택합니다.

b. 인증서 파일 이름과 다운로드 위치를 지정하십시오. 파일을 확장자 `.pem`로 저장하십시오.

예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

인증서 **PEM** 복사

인증서 텍스트를 복사하여 다른 곳에 붙여넣으십시오.

a. *인증서 PEM 복사*를 선택합니다.

b. 복사한 인증서를 텍스트 편집기에 붙여넣으세요.

c. 텍스트 파일을 확장자 `.pem`로 저장하세요.

예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

FabricPool을 위한 StorageGRID 인증서 구성

엄격한 호스트 이름 유효성 검사를 수행하고 엄격한 호스트 이름 유효성 검사 비활성화를 지원하지 않는 S3 클라이언트(예: FabricPool를 사용하는 ONTAP 클라이언트)의 경우, 로드 밸런서 엔드포인트를 구성할 때 서버 인증서를 생성하거나 업로드할 수 있습니다.

시작하기 전에

- "특정 액세스 권한"이(가) 있습니다.
- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.

이 작업 정보

로드 밸런싱 엔드포인트를 생성할 때 자체 서명된 서버 인증서를 생성하거나 공인 인증 기관(CA)에서 서명한 인증서를 업로드할 수 있습니다. 운영 환경에서는 공인 CA에서 서명한 인증서를 사용하는 것이 좋습니다. CA에서 서명한 인증서는 서비스 중단 없이 교체할 수 있습니다. 또한 중간자 공격에 대한 방어력이 뛰어나 보안성이 더욱 강화됩니다.

다음 단계는 FabricPool을 사용하는 S3 클라이언트에 대한 일반적인 지침을 제공합니다. 자세한 정보 및 절차는 "StorageGRID를 FabricPool에 대해 구성합니다"을 참조하십시오.

단계

1. 선택적으로 FabricPool이 사용할 고가용성(HA) 그룹을 구성할 수 있습니다.
2. FabricPool이 사용할 S3 로드 밸런서 엔드포인트를 생성합니다.

HTTPS 로드 밸런서 엔드포인트를 생성할 때 서버 인증서, 인증서 개인 키 및 선택 사항인 CA 번들을 업로드하라는 메시지가 표시됩니다.

3. StorageGRID를 ONTAP의 클라우드 계층으로 연결합니다.

   로드 밸런서 엔드포인트 포트와 업로드한 CA 인증서에 사용된 정규화된 도메인 이름을 지정하십시오. 그런 다음 CA 인증서를 제공하십시오.

   중간 CA가 StorageGRID 인증서를 발급한 경우, 해당 중간 CA 인증서를 제공해야 합니다. StorageGRID 인증서가 루트 CA에서 직접 발급된 경우, 루트 CA 인증서를 제공해야 합니다.

StorageGRID에서 클라이언트 인증서 구성

클라이언트 인증서를 사용하면 승인된 외부 클라이언트가 StorageGRID Prometheus 데이터베이스에 액세스할 수 있으므로 외부 도구가 StorageGRID를 모니터링할 수 있는 안전한 방법을 제공합니다.

외부 모니터링 도구를 사용하여 StorageGRID에 액세스해야 하는 경우 Grid Manager를 사용하여 클라이언트 인증서를 업로드하거나 생성한 다음 해당 인증서 정보를 외부 도구에 복사해야 합니다.

"보안 인증서 관리" 및 "사용자 지정 서버 인증서 구성"을(를) 참조하십시오.

서버 인증서 오류로 인해 운영이 중단되는 것을 방지하기 위해, 해당 서버 인증서의 만료일이 다가오면 인증서 페이지에서 구성된 클라이언트 인증서 만료 알림이 표시됩니다. 필요에 따라 구성 > 보안 > *인증서*를 선택하고 클라이언트 탭에서 클라이언트 인증서의 만료일을 확인하여 현재 인증서의 만료일을 확인할 수 있습니다.

특수 구성된 어플라이언스 노드의 데이터를 보호하기 위해 키 관리 서버(KMS)를 사용하는 경우, "KMS 클라이언트 인증서 업로드"에 대한 특정 정보를 참조하십시오.

시작하기 전에

- 루트 액세스 권한이 있습니다.
- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 클라이언트 인증서를 구성하려면:
  - 관리 노드의 IP 주소 또는 도메인 이름을 알고 있습니다.
  - StorageGRID 관리 인터페이스 인증서를 구성한 경우, 관리 인터페이스 인증서를 구성하는 데 사용된 CA, 클라이언트 인증서 및 개인 키를 보유하고 있습니다.
  - 자체 인증서를 업로드하려면 인증서의 개인 키가 로컬 컴퓨터에 있어야 합니다.
  - 개인 키는 생성 당시 저장 또는 기록되어 있어야 합니다. 원래 개인 키가 없는 경우 새 개인 키를 생성해야 합니다.
- 클라이언트 인증서를 편집하려면:
  - 관리 노드의 IP 주소 또는 도메인 이름을 알고 있습니다.
  - 자신의 인증서 또는 새 인증서를 업로드하려면 개인 키, 클라이언트 인증서 및 CA(사용하는 경우)가 로컬 컴퓨터에 있어야 합니다.

클라이언트 인증서 추가

클라이언트 인증서를 추가하려면 다음 절차 중 하나를 사용하십시오.

- 관리 인터페이스 인증서가 이미 구성되었습니다.
- CA에서 발급한 클라이언트 인증서
- Grid Manager에서 생성된 인증서

관리 인터페이스 인증서가 이미 구성되었습니다.

고객이 제공한 CA, 클라이언트 인증서 및 개인 키를 사용하여 관리 인터페이스 인증서가 이미 구성된 경우 이 절차를 사용하여 클라이언트 인증서를 추가하십시오.

단계

1. 그리드 관리자에서 구성 > 보안 > 인증서*를 선택한 다음 *클라이언트 탭을 선택합니다.
2. *추가*를 선택합니다.
3. 인증서 이름을 입력합니다.
4. 외부 모니터링 도구를 사용하여 Prometheus 메트릭에 액세스하려면 *Prometheus 허용*을 선택하십시오.
5. *Continue*를 선택합니다.
6. 인증서 첨부 단계에서는 관리 인터페이스 인증서를 업로드하십시오.
   a. *인증서 업로드*를 선택합니다.
   b. *찾아보기*를 선택하고 관리 인터페이스 인증서 파일을 선택하십시오((`.pem`).
      - 클라이언트 인증서 세부 정보(**Client certificate details**)를 선택하면 인증서 메타데이터와 인증서 PEM이 표시됩니다.
      - 인증서 내용을 복사하여 다른 곳에 붙여넣으려면 *인증서 PEM 복사*를 선택하십시오.
   c. 그리드 관리자에 인증서를 저장하려면 *생성*을 선택하십시오.

      새 인증서는 클라이언트 탭에 나타납니다.
7. 외부 모니터링 도구 구성(예: Grafana).

CA에서 발급한 클라이언트 인증서

관리 인터페이스 인증서가 구성되지 않았고 CA에서 발급한 클라이언트 인증서와 개인 키를 사용하는 Prometheus용 클라이언트 인증서를 추가하려는 경우 이 절차를 사용하여 관리자 클라이언트 인증서를 추가하십시오.

단계

1. 다음 단계를 수행하십시오"관리 인터페이스 인증서 구성".
2. 그리드 관리자에서 구성 > 보안 > 인증서*를 선택한 다음 *클라이언트 탭을 선택합니다.
3. *추가*를 선택합니다.
4. 인증서 이름을 입력합니다.
5. 외부 모니터링 도구를 사용하여 Prometheus 메트릭에 액세스하려면 *Prometheus 허용*을 선택하십시오.
6. *Continue*를 선택합니다.

7. 인증서 첨부 단계에서는 클라이언트 인증서, 개인 키 및 CA 번들 파일을 업로드하십시오.
   a. *인증서 업로드*를 선택합니다.
   b. [찾아보기]를 선택하고 클라이언트 인증서, 개인 키 및 CA 번들 파일을 선택합니다(`.pem`).
      - 클라이언트 인증서 세부 정보(**Client certificate details**)를 선택하면 인증서 메타데이터와 인증서 PEM이 표시됩니다.
      - 인증서 내용을 복사하여 다른 곳에 붙여넣으려면 *인증서 PEM 복사*를 선택하십시오.
   c. 그리드 관리자에 인증서를 저장하려면 *생성*을 선택하십시오.

      새 인증서는 클라이언트 탭에 나타납니다.
8. 외부 모니터링 도구 구성(예: Grafana).

Grid Manager에서 생성된 인증서

관리 인터페이스 인증서가 구성되지 않았고 Grid Manager의 인증서 생성 기능을 사용하여 Prometheus용 클라이언트 인증서를 추가하려는 경우 이 절차를 사용하여 관리자 클라이언트 인증서를 추가하십시오.

단계

1. 그리드 관리자에서 구성 > 보안 > 인증서*를 선택한 다음 *클라이언트 탭을 선택합니다.
2. *추가*를 선택합니다.
3. 인증서 이름을 입력합니다.
4. 외부 모니터링 도구를 사용하여 Prometheus 메트릭에 액세스하려면 *Prometheus 허용*을 선택하십시오.
5. *Continue*를 선택합니다.
6. 인증서 첨부 단계에서는 *인증서 생성*을 선택하십시오.
7. 인증서 정보를 지정합니다:
   - **Subject** (선택 사항): X.509 인증서 소유자의 주체 또는 고유 이름(DN).
   - 유효 기간: 생성된 인증서가 생성된 시점부터 유효한 일수입니다.
   - 키 사용 확장 추가: 이 옵션을 선택하면(기본값이며 권장됨), 생성된 인증서에 키 사용 및 확장 키 사용 확장 기능이 추가됩니다.

     이러한 확장 기능은 인증서에 포함된 키의 용도를 정의합니다.

     인증서에 이러한 확장자가 포함된 경우 이전 클라이언트와의 연결 문제가 발생하지 않는다면 이 확인란을 선택한 상태로 두십시오.
8. *생성*을 선택합니다.
9. *클라이언트 인증서 세부 정보*를 선택하면 인증서 메타데이터와 인증서 PEM이 표시됩니다.

   이 대화 상자를 닫으면 인증서 개인 키를 볼 수 없습니다. 키를 복사하거나 다운로드하여 안전한 위치에 보관하십시오.
   - 인증서 내용을 복사하여 다른 곳에 붙여넣으려면 *인증서 PEM 복사*를 선택하십시오.

◦ 인증서 파일을 저장하려면 *인증서 다운로드*를 선택합니다.

인증서 파일 이름과 다운로드 위치를 지정하십시오. 파일을 확장자 `.pem`로 저장하십시오.

예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

◦ 인증서 개인 키를 복사하여 다른 곳에 붙여넣으려면 *개인 키 복사*를 선택합니다.

◦ 개인 키를 파일로 저장하려면 *개인 키 다운로드*를 선택합니다.

개인 키 파일 이름과 다운로드 위치를 지정하십시오.

10. 그리드 관리자에 인증서를 저장하려면 *생성*을 선택하십시오.

새 인증서는 클라이언트 탭에 나타납니다.

11. 그리드 관리자에서 구성 > 보안 > 인증서*를 선택한 다음 *전역 탭을 선택합니다.
12. *관리 인터페이스 인증서*를 선택하십시오.
13. *사용자 지정 인증서 사용*을 선택합니다.
14. 클라이언트 인증서 세부 정보 단계에서 certificate.pem 및 private_key.pem 파일을 업로드합니다. CA 번들을 업로드할 필요가 없습니다.
    a. *인증서 업로드*를 선택한 다음 *계속*을 선택합니다.
    b. 각 인증서 파일을 업로드하세요(`.pem`).
    c. 그리드 관리자에 인증서를 저장하려면 *저장*을 선택하십시오.

    새 인증서는 관리 인터페이스 인증서 페이지에 나타납니다.

15. 외부 모니터링 도구 구성(예: Grafana).

외부 모니터링 도구 구성

단계

1. Grafana와 같은 외부 모니터링 도구에서 다음 설정을 구성하십시오.
    a. 이름: 연결에 사용할 이름을 입력합니다.

    StorageGRID는 이 정보를 요구하지 않지만, 연결을 테스트하려면 이름을 제공해야 합니다.

    b. **URL**: 관리 노드의 도메인 이름 또는 IP 주소를 입력하십시오. HTTPS 및 포트 9091을 지정하십시오.

    예를 들면 다음과 같습니다. `https://admin-node.example.com:9091`

    c. **TLS** 클라이언트 인증 및 *CA 인증서 사용*을 활성화하십시오.
    d. TLS/SSL 인증 세부 정보 아래에 다음을 복사하여 붙여넣습니다:
        - 관리 인터페이스 CA 인증서를 **CA Cert**로
        - 클라이언트 인증서를 **Client Cert**로 설정합니다.
        - 클라이언트 키의 개인 키

e. **ServerName**: 관리 노드의 도메인 이름을 입력하십시오.

   ServerName은 관리 인터페이스 인증서에 표시된 도메인 이름과 일치해야 합니다.

2. StorageGRID 또는 로컬 파일에서 복사한 인증서와 개인 키를 저장하고 테스트하십시오.

   이제 외부 모니터링 도구를 사용하여 StorageGRID의 Prometheus 메트릭에 액세스할 수 있습니다.

   측정 기준에 대한 자세한 내용은 "StorageGRID 모니터링 지침"을 참조하십시오.

클라이언트 인증서 편집

관리자 클라이언트 인증서를 편집하여 이름을 변경하거나, Prometheus 액세스를 활성화 또는 비활성화하거나, 현재 인증서가 만료된 경우 새 인증서를 업로드할 수 있습니다.

단계

1. 구성 > 보안 > 인증서*를 선택한 다음 *클라이언트 탭을 선택합니다.

   인증서 만료일과 Prometheus 액세스 권한이 표에 나열되어 있습니다. 인증서 만료일이 임박했거나 이미 만료된 경우 표에 메시지가 표시되고 경고가 발생합니다.

2. 편집할 인증서를 선택합니다.
3. *편집*을 선택한 다음 *이름 및 권한 편집*을 선택합니다.
4. 인증서 이름을 입력합니다.
5. 외부 모니터링 도구를 사용하여 Prometheus 메트릭에 액세스하려면 *Prometheus 허용*을 선택하십시오.
6. 그리드 관리자에 인증서를 저장하려면 *계속*을 선택하십시오.

   업데이트된 인증서는 클라이언트 탭에 표시됩니다.

새 클라이언트 인증서 첨부

현재 인증서가 만료되면 새 인증서를 업로드할 수 있습니다.

단계

1. 구성 > 보안 > 인증서*를 선택한 다음 *클라이언트 탭을 선택합니다.

   인증서 만료일과 Prometheus 액세스 권한이 표에 나열되어 있습니다. 인증서 만료일이 임박했거나 이미 만료된 경우 표에 메시지가 표시되고 경고가 발생합니다.

2. 편집할 인증서를 선택합니다.
3. *편집*을 선택한 다음 편집 옵션을 선택합니다.

인증서 업로드

인증서 텍스트를 복사하여 다른 곳에 붙여넣으십시오.

a. *인증서 업로드*를 선택한 다음 *계속*을 선택합니다.

b. 클라이언트 인증서 이름을 업로드합니다(`.pem`).

   클라이언트 인증서 세부 정보(**Client certificate details**)를 선택하면 인증서 메타데이터와 인증서 PEM이 표시됩니다.

   - 인증서 파일을 저장하려면 *인증서 다운로드*를 선택합니다.

     인증서 파일 이름과 다운로드 위치를 지정하십시오. 파일을 확장자 `.pem`로 저장하십시오.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

   - 인증서 내용을 복사하여 다른 곳에 붙여넣으려면 *인증서 PEM 복사*를 선택하십시오.

c. 그리드 관리자에 인증서를 저장하려면 *생성*을 선택하십시오.

   업데이트된 인증서는 클라이언트 탭에 표시됩니다.

인증서 생성

인증서 텍스트를 생성하여 다른 곳에 붙여넣으세요.

a. *인증서 생성*을 선택합니다.

b. 인증서 정보를 지정합니다:

   - **Subject** (선택 사항): X.509 인증서 소유자의 주체 또는 고유 이름(DN).
   - 유효 기간: 생성된 인증서가 생성된 시점부터 유효한 일수입니다.
   - 키 사용 확장 추가: 이 옵션을 선택하면(기본값이며 권장됨), 생성된 인증서에 키 사용 및 확장 키 사용 확장 기능이 추가됩니다.

     이러한 확장 기능은 인증서에 포함된 키의 용도를 정의합니다.

     인증서에 이러한 확장자가 포함된 경우 이전 클라이언트와의 연결 문제가 발생하지 않는다면 이 확인란을 선택한 상태로 두십시오.

c. *생성*을 선택합니다.

d. 클라이언트 인증서 세부 정보(**Client certificate details**)를 선택하면 인증서 메타데이터와 인증서 PEM이 표시됩니다.

   이 대화 상자를 닫으면 인증서 개인 키를 볼 수 없습니다. 키를 복사하거나 다운로드하여 안전한 위치에 보관하십시오.

   - 인증서 내용을 복사하여 다른 곳에 붙여넣으려면 *인증서 PEM 복사*를 선택하십시오.
   - 인증서 파일을 저장하려면 *인증서 다운로드*를 선택합니다.

인증서 파일 이름과 다운로드 위치를 지정하십시오. 파일을 확장자 `.pem`로 저장하십시오.

예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

- 인증서 개인 키를 복사하여 다른 곳에 붙여넣으려면 *개인 키 복사*를 선택합니다.
- 개인 키를 파일로 저장하려면 *개인 키 다운로드*를 선택합니다.

  개인 키 파일 이름과 다운로드 위치를 지정하십시오.

e. 그리드 관리자에 인증서를 저장하려면 *생성*을 선택하십시오.

새 인증서는 클라이언트 탭에 나타납니다.

클라이언트 인증서 다운로드 또는 복사

클라이언트 인증서를 다운로드하거나 복사하여 다른 곳에서 사용할 수 있습니다.

단계

1. 구성 > 보안 > 인증서*를 선택한 다음 *클라이언트 탭을 선택합니다.
2. 복사하거나 다운로드할 인증서를 선택합니다.
3. 인증서를 다운로드하거나 복사합니다.

인증서 파일 다운로드

인증서 `.pem` 파일을 다운로드하세요.

a. *인증서 다운로드*를 선택합니다.
b. 인증서 파일 이름과 다운로드 위치를 지정하십시오. 파일을 확장자 `.pem`로 저장하십시오.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

인증서 복사

인증서 텍스트를 복사하여 다른 곳에 붙여넣으십시오.

a. *인증서 PEM 복사*를 선택합니다.
b. 복사한 인증서를 텍스트 편집기에 붙여넣으세요.
c. 텍스트 파일을 확장자 `.pem`로 저장하세요.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

클라이언트 인증서 제거

관리자 클라이언트 인증서가 더 이상 필요하지 않으면 삭제할 수 있습니다.

단계

1. 구성 > 보안 > 인증서*를 선택한 다음 *클라이언트 탭을 선택합니다.
2. 삭제할 인증서를 선택합니다.
3. *삭제*를 선택한 다음 확인합니다.

> 최대 10개의 인증서를 제거하려면 클라이언트 탭에서 제거할 각 인증서를 선택한 다음 작업 > *삭제*를 선택하십시오.

인증서가 제거된 후에는 해당 인증서를 사용하던 클라이언트가 StorageGRID Prometheus 데이터베이스에 액세스하려면 새 클라이언트 인증서를 지정해야 합니다.

${post_edited_translations.segment}

StorageGRID에서 TLS 및 SSH 정책 관리

TLS 및 SSH 정책은 클라이언트 애플리케이션과의 안전한 TLS 연결 및 내부 StorageGRID 서비스와의 안전한 SSH 연결을 설정하는 데 사용되는 프로토콜과 암호화 방식을 결정합니다.

보안 정책은 TLS 및 SSH를 사용하여 전송 중인 데이터를 암호화하는 방식을 제어합니다. 일반적으로 시스템이 Common Criteria를 준수해야 하거나 다른 암호화 방식을 사용해야 하는 경우가 아니라면 최신 호환성(기본값) 정책을 사용하는 것이 좋습니다.

> 일부 StorageGRID 서비스는 이러한 정책에 포함된 암호화 방식을 사용하도록 업데이트되지 않았습니다.

시작하기 전에

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

보안 정책을 선택합니다

단계

1. 구성 > 보안 > *보안 설정*을 선택합니다.

   TLS 및 **SSH** 정책 탭에는 사용 가능한 정책이 표시됩니다. 현재 활성화된 정책은 정책 타일에 녹색 체크 표시로 나타납니다.

2. 각 탭을 검토하여 사용 가능한 정책에 대해 알아보십시오.

최신 호환성(기본값)

강력한 암호화가 필요하고 특별한 요구 사항이 없는 경우 기본 정책을 사용하십시오. 이 정책은 대부분의 TLS 및 SSH 클라이언트와 호환됩니다.

레거시 호환성

이전 클라이언트와의 추가 호환성 옵션이 필요한 경우 레거시 호환성 정책을 사용하십시오. 이 정책의 추가 옵션으로 인해 최신 호환성 정책보다 보안성이 떨어질 수 있습니다.

공통 기준

공통 기준(Common Criteria) 인증이 필요한 경우 공통 기준 정책을 사용하십시오.

FIPS 엄격

Common Criteria 인증이 필요하고 외부 클라이언트가 로드 밸런서 엔드포인트, Tenant Manager 및 Grid Manager에 연결할 때 NetApp Cryptographic Security Module(NCSM) 3.0.8 또는 NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 모듈을 사용해야 하는 경우 FIPS 엄격 정책을 사용하십시오. 이 정책을 사용하면 성능이 저하될 수 있습니다.

NCSM 3.0.8 및 NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 모듈은 다음 작업에 사용됩니다.

- NCSM
  - 다음 서비스 간의 TLS 연결: ADC, AMS, CMN, DDS, LDR, SSM, NMS, mgmt-api, nginx, nginx-gw 및 cache-svc
  - 클라이언트와 nginx-gw 서비스(로드 밸런서 엔드포인트) 간의 TLS 연결
  - 클라이언트와 LDR 서비스 간의 TLS 연결
  - SSE-S3, SSE-C 및 저장된 객체 암호화 설정에 대한 객체 콘텐츠 암호화
  - SSH 연결

  자세한 내용은 NIST Cryptographic Algorithm Validation Program "인증서 번호 4838"을 참조하십시오.

- NetApp StorageGRID 커널 암호화 API 모듈

  NetApp StorageGRID 커널 암호화 API 모듈은 VM 및 StorageGRID 어플라이언스 플랫폼에서만 사용할 수 있습니다.

  - 엔트로피 수집
  - 노드 암호화

  자세한 내용은 NIST 암호화 알고리즘 검증 프로그램 "인증서 #A6242 ~ #A6257" 및 "엔트로피 인증서 #E223"을 참조하십시오.

참고: 이 정책을 선택하면 "롤링 재부팅 수행"모든 노드에서 NCSM이 활성화됩니다. 재부팅을 시작하고 모니터링하려면 유지 관리 > *롤링 재부팅*을 사용하십시오.

사용자 지정

사용자 지정 암호화 방식을 적용해야 하는 경우 사용자 지정 정책을 생성하십시오.

선택적으로, StorageGRID에 FIPS 140 암호화 요구 사항이 있는 경우 FIPS 모드 기능을 활성화하여 NCSM 3.0.8 및 NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 모듈을 사용할 수 있습니다.

a. `fipsMode` 매개변수를 `true`로 설정합니다.

b. 메시지가 표시되면 "롤링 재부팅 수행" 모든 노드에서 암호화 모듈을 활성화하십시오. 재부팅을 시작하고 모니터링하려면 **Maintenance** > *Rolling reboot*을 사용하십시오.

c. 지원 > *진단*을 선택하여 현재 활성화된 FIPS 모듈 버전을 확인하십시오.

3. 각 정책의 암호화 방식, 프로토콜 및 알고리즘에 대한 자세한 내용을 보려면 *세부 정보 보기*를 선택하십시오.
4. 현재 정책을 변경하려면 *정책 사용*을 선택합니다.

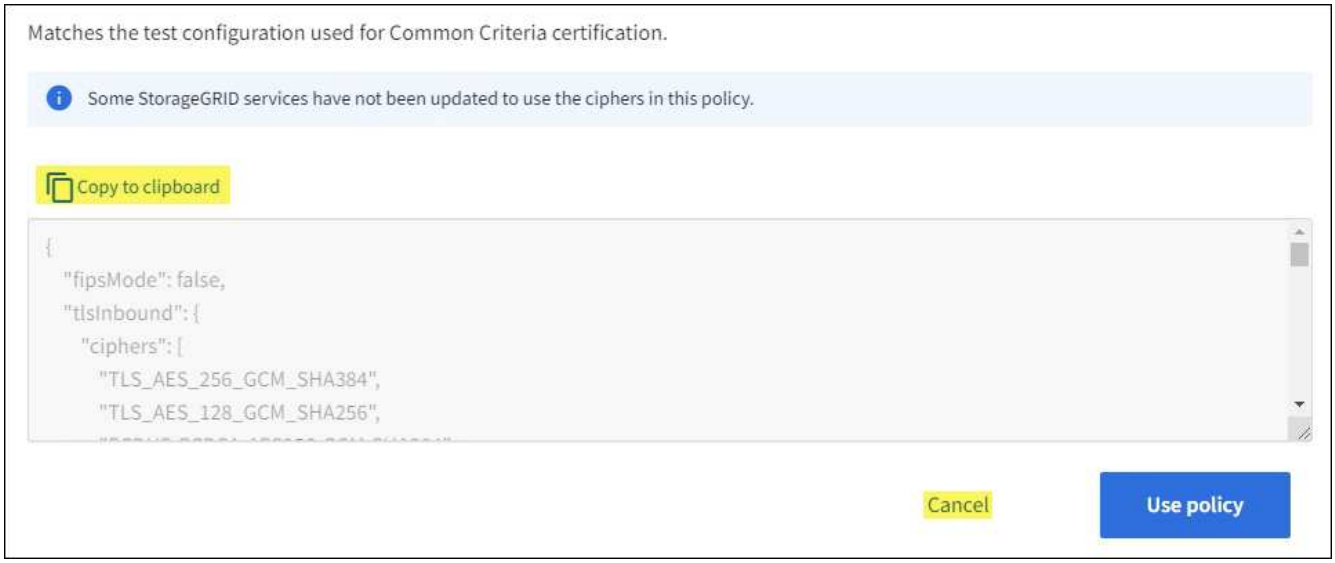
   정책 타일의 현재 정책 옆에 녹색 체크 표시가 나타납니다.

사용자 지정 보안 정책 생성

사용자 지정 암호화 방식을 적용해야 하는 경우 사용자 지정 정책을 만들 수 있습니다.

단계

1. 생성하려는 사용자 지정 정책과 가장 유사한 정책의 타일에서 *세부 정보 보기*를 선택합니다.
2. *클립보드에 복사*를 선택한 다음 *취소*를 선택합니다.



3. 사용자 지정 정책 타일에서 *구성 및 사용*을 선택합니다.
4. 복사한 JSON을 붙여넣고 필요한 변경 사항을 적용하십시오.
5. *사용 정책*을 선택합니다.

   사용자 지정 정책 타일에서 현재 정책 옆에 녹색 체크 표시가 나타납니다.

6. 필요에 따라 *구성 편집*을 선택하여 새 사용자 지정 정책을 추가로 변경할 수 있습니다.

일시적으로 기본 보안 정책으로 되돌리기

사용자 지정 보안 정책을 구성한 경우, 구성된 TLS 정책이 "구성된 서버 인증서"와 호환되지 않으면 Grid Manager에 로그인하지 못할 수 있습니다.

일시적으로 기본 보안 정책으로 되돌릴 수 있습니다.

단계

1. 관리자 노드에 로그인합니다.
   a. 다음 명령을 입력합니다. `ssh admin@Admin_Node_IP`
   b. `Passwords.txt` 파일에 나와 있는 비밀번호를 입력하십시오.
   c. 루트 권한으로 전환하려면 다음 명령을 입력하십시오. `su -`
   d. `Passwords.txt` 파일에 나와 있는 비밀번호를 입력하십시오.

      루트 계정으로 로그인하면 프롬프트가 `$`에서 `#`로 변경됩니다.
2. 다음 명령을 실행합니다.

   ```
   restore-default-cipher-configurations
   ```
3. 웹 브라우저를 통해 동일한 관리 노드에서 그리드 관리자에 접속합니다.
4. 보안 정책을 선택합니다의 단계에 따라 정책을 다시 구성하십시오.

StorageGRID 네트워크 및 객체 보안을 구성합니다

저장된 객체를 암호화하거나, 특정 S3 요청을 차단하거나, 클라이언트가 스토리지 노드에 연결할 때 HTTPS 대신 HTTP를 사용하도록 허용하는 등 네트워크 및 객체 보안을 구성할 수 있습니다.

저장된 객체 암호화

저장된 객체 암호화 기능을 사용하면 S3를 통해 수집되는 모든 객체 데이터를 암호화할 수 있습니다. 기본적으로 저장된 객체는 암호화되지 않지만, AES-128 또는 AES-256 암호화 알고리즘을 사용하여 객체를 암호화하도록 선택할 수 있습니다. 이 설정을 활성화하면 새로 수집되는 모든 객체가 암호화되지만 기존에 저장된 객체는 변경되지 않습니다. 암호화를 비활성화하면 현재 암호화된 객체는 계속 암호화된 상태로 유지되지만 새로 수집되는 객체는 암호화되지 않습니다.

저장된 객체 암호화 설정은 버킷 수준 또는 객체 수준 암호화로 암호화되지 않은 S3 객체에만 적용됩니다.

StorageGRID 암호화 방법에 대한 자세한 내용은 "StorageGRID 암호화 방법 검토"을 참조하십시오.

클라이언트 수정 방지

클라이언트 수정 방지는 시스템 전체 설정입니다. 클라이언트 수정 방지 옵션을 선택하면 다음 요청이 거부됩니다.

S3 REST API

- DeleteBucket 요청
- 기존 객체의 데이터, 사용자 정의 메타데이터 또는 S3 객체 태깅을 수정하려는 모든 요청

스토리지 노드 연결에 **HTTP** 활성화

기본적으로 클라이언트 애플리케이션은 스토리지 노드에 직접 연결할 때 HTTPS 네트워크 프로토콜을 사용합니다. 필요에 따라 비운영 그리드를 테스트할 때와 같이 이러한 연결에 HTTP를 활성화할 수도 있습니다.

S3 클라이언트가 스토리지 노드에 직접 HTTP 연결을 해야 하는 경우에만 스토리지 노드 연결에 HTTP를 사용하십시오. HTTPS 연결만 사용하는 클라이언트 또는 로드 밸런서 서비스에 연결하는 클라이언트의 경우("각 로드 밸런서 엔드포인트 구성"HTTP 또는 HTTPS를 사용하도록 구성할 수 있으므로) 이 옵션을 사용할 필요가 없습니다.

"요약: 클라이언트 연결을 위한 IP 주소 및 포트"을 참조하여 S3 클라이언트가 HTTP 또는 HTTPS를 사용하여 스토리지 노드에 연결할 때 사용하는 포트를 알아보십시오.

옵션을 선택합니다

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 루트 액세스 권한이 있습니다.

단계

1. 구성 > 보안 > *보안 설정*을 선택합니다.
2. 네트워크 및 개체 탭을 선택합니다.
3. 저장된 객체 암호화의 경우, 저장된 객체를 암호화하지 않으려면 없음(기본값) 설정을 사용하고, 저장된 객체를 암호화하려면 **AES-128** 또는 *AES-256*을 선택하십시오.
4. S3 클라이언트가 특정 요청을 하지 못하도록 하려면 *클라이언트 수정 방지*를 선택적으로 지정할 수 있습니다.

   이 설정을 변경하면 새 설정이 적용되는 데 약 1분이 소요됩니다. 구성된 값은 성능 및 확장성을 위해 캐시됩니다.

5. 클라이언트가 스토리지 노드에 직접 연결하고 HTTP 연결을 사용하려는 경우 스토리지 노드 연결에 **HTTP** 사용 을 선택적으로 선택할 수 있습니다.

   운영 환경의 그리드에서 HTTP를 활성화할 때는 요청이 암호화되지 않은 상태로 전송되므로 주의해야 합니다.

6. *저장*을 선택하세요.

StorageGRID 인터페이스 보안 설정을 변경합니다

인터페이스 보안 설정을 통해 사용자가 지정된 시간 이상 활동이 없을 경우 로그아웃되는지 여부와 API 오류 응답에 스택 추적을 포함할지 여부를 제어할 수 있습니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- "루트 액세스 권한"이(가) 있습니다.

이 작업 정보

보안 설정 페이지에는 브라우저 비활성 시간 초과 및 관리 **API** 스택 추적 설정이 포함되어 있습니다.

브라우저 비활성 시간 초과

사용자가 로그아웃되기 전에 브라우저가 비활성 상태로 유지될 수 있는 시간을 나타냅니다. 기본값은 15분입니다.

브라우저 비활성 시간 초과는 다음 요소에 의해서도 제어됩니다.

- 시스템 보안을 위해 별도의 구성 불가능한 StorageGRID 타이머가 포함되어 있습니다. 각 사용자의 인증 토큰은 사용자가 로그인한 후 16시간이 지나면 만료됩니다. 사용자 인증이 만료되면 브라우저 비활성 시간 초과가 비활성화되었거나 브라우저 시간 초과 값에 아직 도달하지 않았더라도 해당 사용자는 자동으로 로그아웃됩니다. 토큰을 갱신하려면 사용자는 다시 로그인해야 합니다.
- StorageGRID에 대해 SSO(Single Sign-On)가 활성화된 경우 ID 공급자에 대한 타임아웃 설정입니다.

  SSO가 활성화된 경우 사용자의 브라우저 시간 초과가 발생하면 사용자는 StorageGRID에 다시 액세스하려면 SSO 자격 증명을 다시 입력해야 합니다. 을(를) 참조하십시오. "SSO 작동 방식".

관리 **API** 스택 트레이스

Grid Manager 및 Tenant Manager API 오류 응답에 스택 트레이스를 반환할지 여부를 제어합니다.

이 옵션은 기본적으로 비활성화되어 있지만 테스트 환경에서는 이 기능을 활성화할 수 있습니다. 일반적으로 프로덕션 환경에서는 API 오류 발생 시 내부 소프트웨어 세부 정보가 노출되는 것을 방지하기 위해 스택 추적 기능을 비활성화 상태로 유지하는 것이 좋습니다.

단계

1. 구성 > 보안 > *보안 설정*을 선택합니다.
2. 인터페이스 탭을 선택합니다.
3. 브라우저 비활성 시간 초과 설정을 변경하려면:
   a. 아코디언을 펼치세요.
   b. 타임아웃 기간을 변경하려면 60초에서 7일 사이의 값을 지정하십시오. 기본 타임아웃은 15분입니다.
   c. 이 기능을 비활성화하려면 확인란의 선택을 해제하십시오.
   d. *저장*을 선택하세요.

      새 설정은 현재 로그인한 사용자에게는 영향을 미치지 않습니다. 새 타이머 설정이 적용되려면 사용자는 다시 로그인하거나 브라우저를 새로 고침해야 합니다.
4. 관리 API 스택 추적 설정을 변경하려면 다음 단계를 따르십시오.
   a. 아코디언을 펼치세요.
   b. 그리드 관리자 및 테넌트 관리자 API 오류 응답에 스택 트레이스를 반환하려면 확인란을 선택하십시오.

      API 오류 발생 시 내부 소프트웨어 세부 정보가 노출되는 것을 방지하기 위해 프로덕션 환경에서는 스택 추적 기능을 비활성화하십시오.

   c. *저장*을 선택하세요.

StorageGRID에서 외부 SSH 액세스 관리

그리드로 들어오는 트래픽에 대한 SSH 액세스를 외부 액세스 차단 또는 허용으로 관리할 수

있습니다. 외부 SSH 액세스 관리는 그리드 내 노드 간 트래픽에는 영향을 미치지 않습니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- "루트 액세스 권한"이(가) 있습니다.

이 작업 정보

시스템 보안 강화를 위해 외부 SSH 접속은 기본적으로 차단되어 있습니다. 문제 해결과 같이 인바운드 SSH 접속이 필요한 작업을 수행해야 하는 경우, 외부 접속을 일시적으로 허용하십시오. 작업이 완료되면 외부 접속을 차단하십시오.

단계

1. 구성 > 보안 > *보안 설정*을 선택합니다.
2. **SSH** 차단 탭을 선택합니다.
3. 외부 SSH 액세스를 관리하려면 수신 **SSH** 액세스 차단 옵션을 사용하십시오.
   a. 액세스를 차단하려면 확인란을 선택합니다(기본값).
   b. 액세스를 허용하려면 확인란을 선택 취소하십시오.

   서비스 랩톱과 다른 모든 그리드 노드 간에 22번 포트에 대한 액세스가 필요합니다. 유지 관리 작업이 완료되면 22번 포트에 대한 액세스를 제거하십시오.

4. *저장*을 선택하세요.

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.

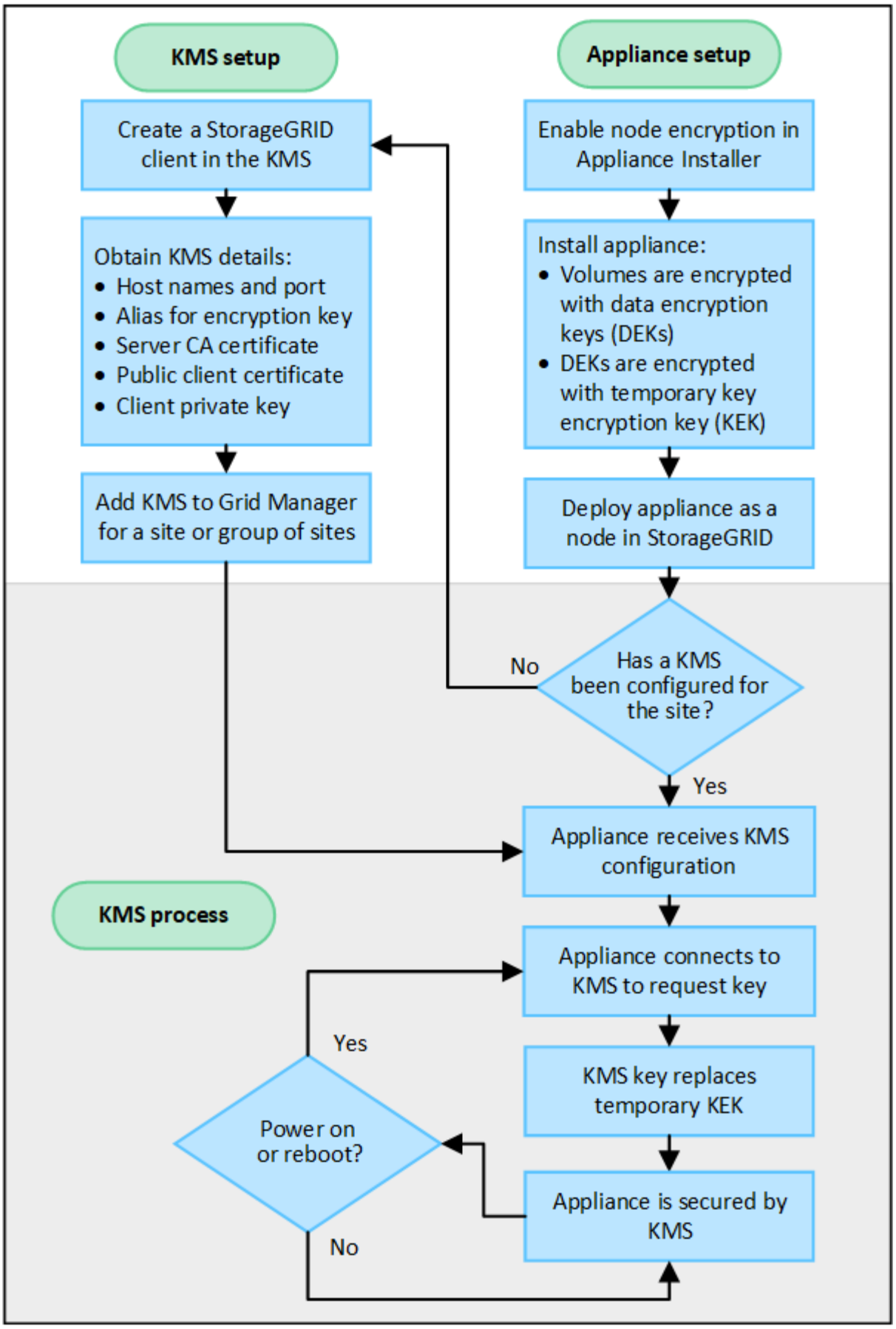
StorageGRID 어플라이언스 노드를 암호화 및 복호화하는 데 사용되는 외부 키를 생성하거나 관리하지 않습니다. StorageGRID 데이터를 보호하기 위해 외부 키 관리 서버를 사용하려는 경우, 해당 서버 설정 방법과 암호화 키 관리 방법을 숙지해야 합니다. 키 관리 작업은 본 설명서의 범위를 벗어납니다. 도움이 필요하면 키 관리 서버 설명서를 참조하거나 기술 지원에 문의하십시오.

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.

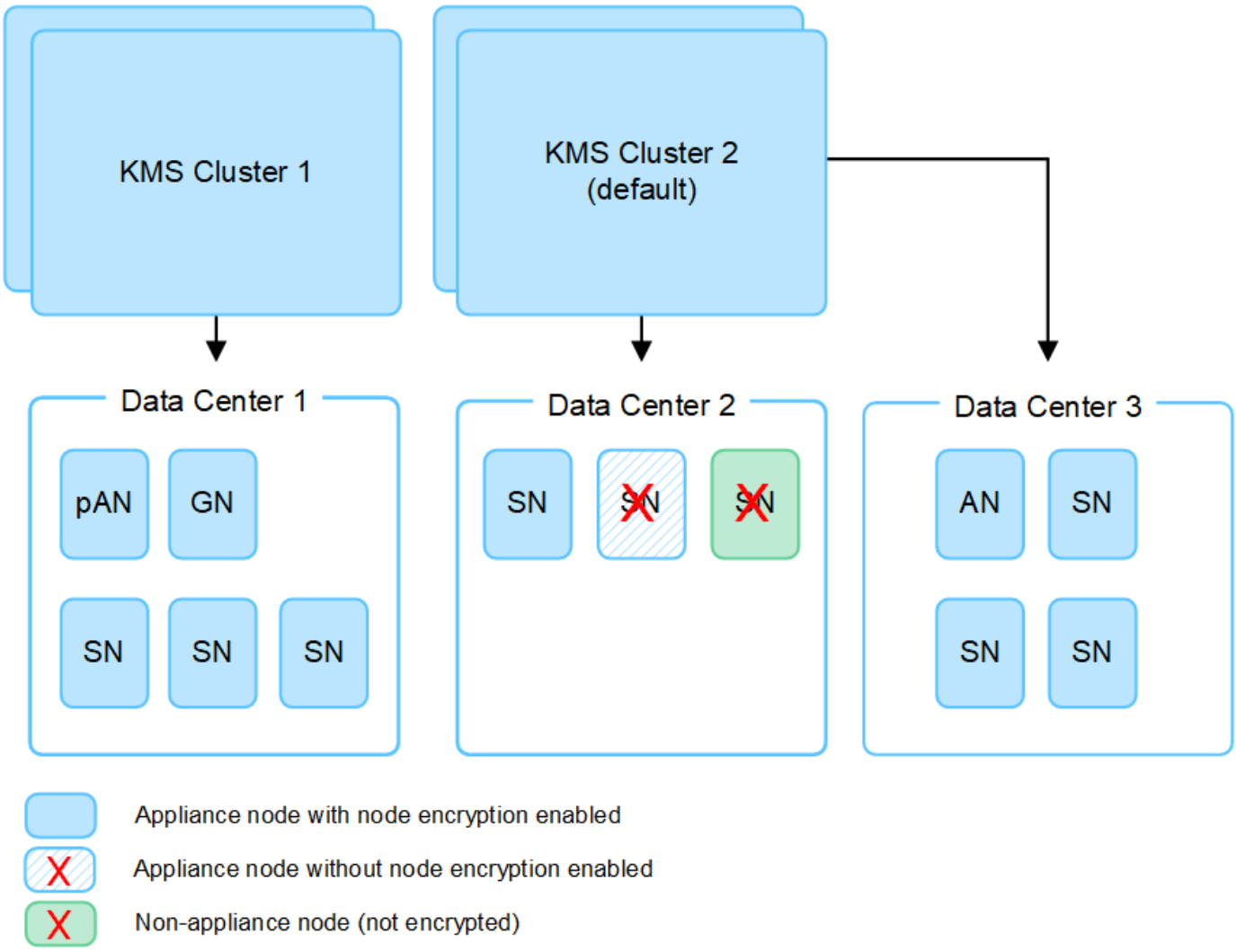
키 관리 서버는 몇 대가 필요합니까?

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.

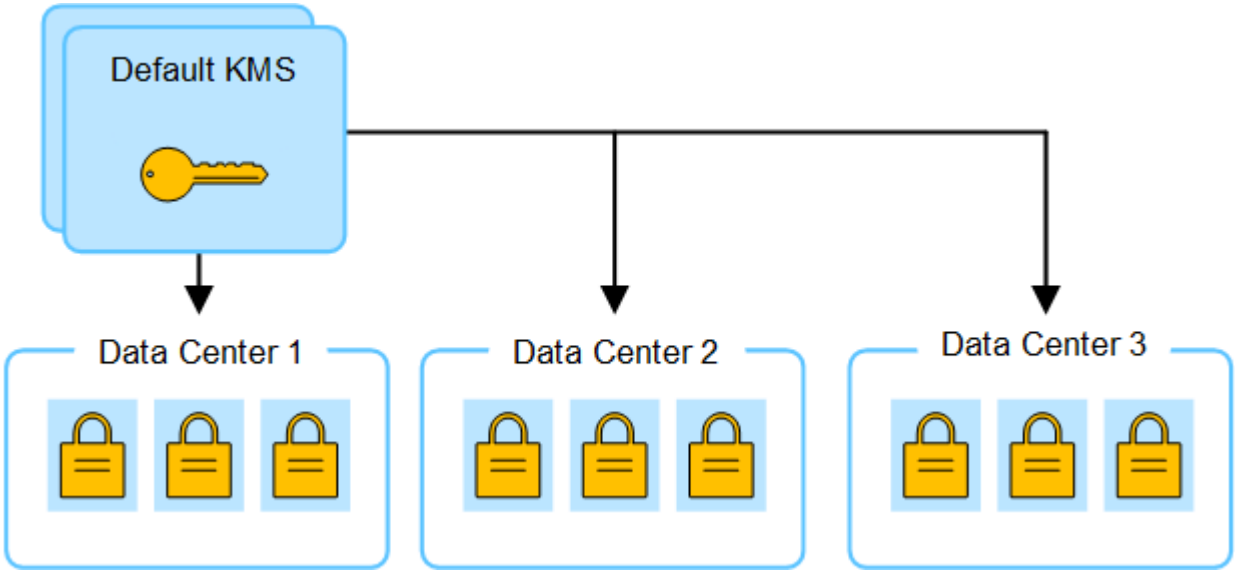
StorageGRID 사이트의 KMS 변경 시 고려 사항

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.

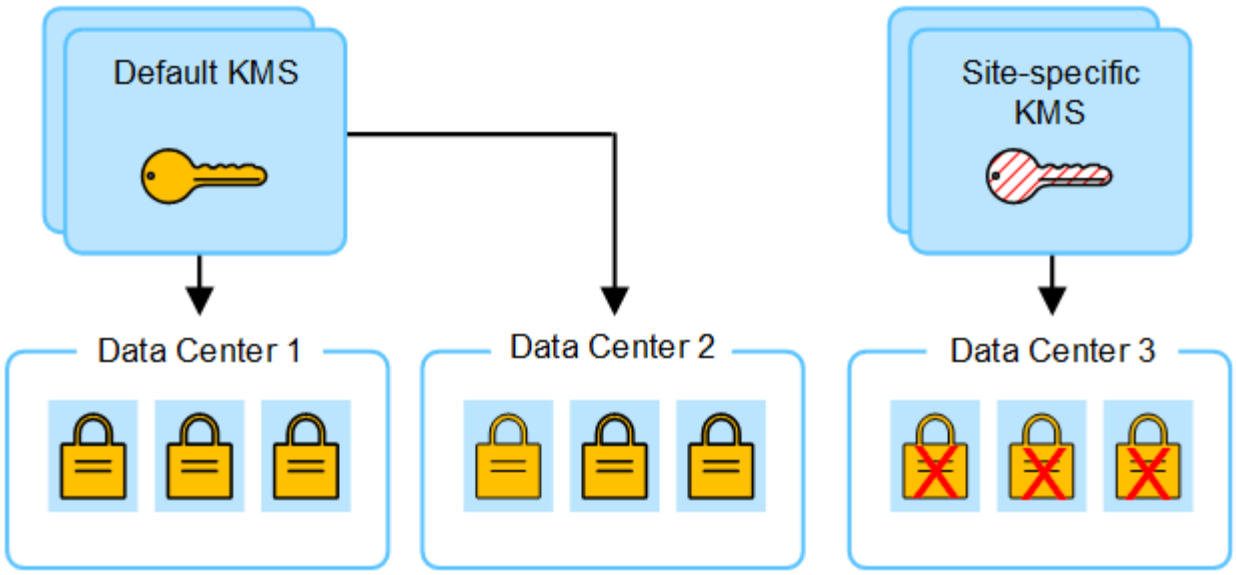
사이트에 사용되는 KMS를 변경하는 경우, 해당 사이트에서 이전에 암호화된 어플라이언스 노드를 새 KMS에 저장된 키를 사용하여 복호화할 수 있는지 확인해야 합니다. 경우에 따라 기존 KMS에서 새 KMS로 현재 버전의 암호화 키를 복사해야 할 수도 있습니다. KMS에 해당 사이트의 암호화된 어플라이언스 노드를 복호화하는 데 필요한 올바른 키가 있는지 반드시 확인해야 합니다.

예를 들면 다음과 같습니다.

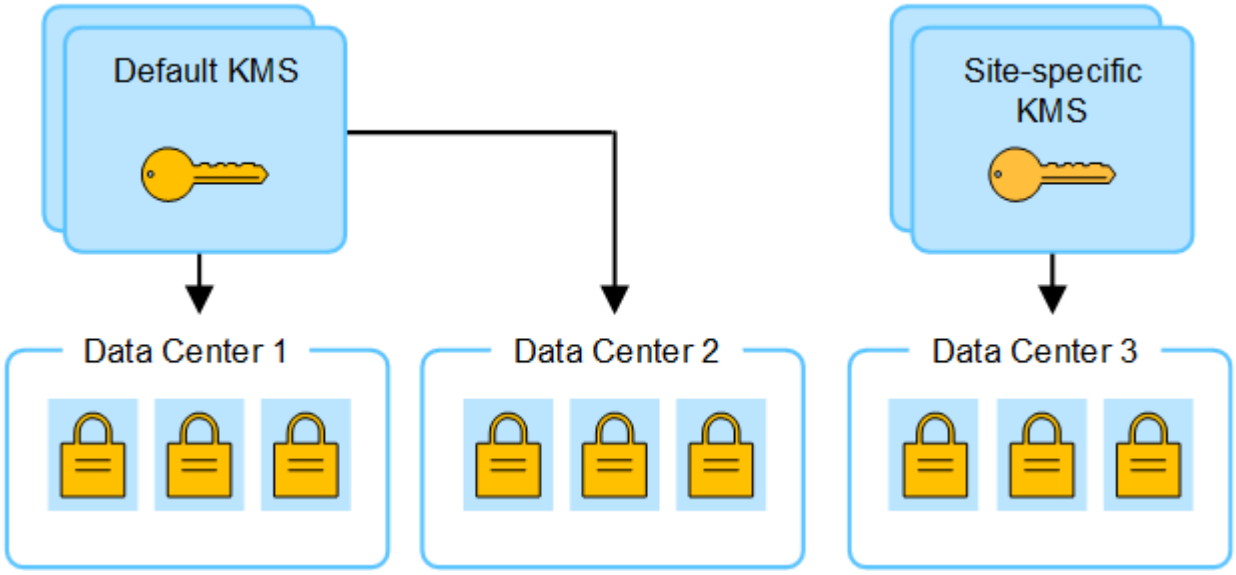
1. 처음에 전용 KMS가 없는 모든 사이트에 적용되는 기본 KMS를 구성합니다.
2. KMS가 저장되면 노드 암호화 설정이 활성화된 모든 어플라이언스 노드가 KMS에 연결하여 암호화 키를 요청합니다. 이 키는 모든 사이트의 어플라이언스 노드를 암호화하는 데 사용됩니다. 또한 동일한 키를 사용하여 해당 어플라이언스를 복호화해야 합니다.



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.

탭	필드	설명
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.

프록시 설정 관리

StorageGRID 스토리지 프록시 구성

플랫폼 서비스 또는 클라우드 스토리지 풀을 사용하는 경우 스토리지 노드와 외부 S3 엔드포인트 사이에 비투명 프록시를 구성할 수 있습니다. 예를 들어, 플랫폼 서비스 메시지를 인터넷상의 엔드포인트와 같은 외부 엔드포인트로 전송하려면 비투명 프록시가 필요할 수 있습니다.

구성된 스토리지 프록시 설정은 Kafka 플랫폼 서비스 엔드포인트에 적용되지 않습니다.

시작하기 전에

- "특정 액세스 권한"이(가) 있습니다.
- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.

이 작업 정보

단일 스토리지 프록시에 대한 설정을 구성할 수 있습니다.

단계

1. 구성 > 보안 > *프록시 설정*을 선택합니다.
2. 스토리지 탭에서 스토리지 프록시 활성화 확인란을 선택합니다.
3. 스토리지 프록시의 프로토콜을 선택합니다.
4. 프록시 서버의 호스트 이름 또는 IP 주소를 입력합니다.
5. 선택적으로 프록시 서버에 연결하는 데 사용되는 포트를 입력합니다.

   이 필드를 비워두면 프로토콜의 기본 포트(HTTP의 경우 80, SOCKS5의 경우 1080)가 사용됩니다.

6. *저장*을 선택하세요.

   스토리지 프록시를 저장한 후에는 플랫폼 서비스 또는 클라우드 스토리지 풀에 대한 새 엔드포인트를 구성하고 테스트할 수 있습니다.

   프록시 변경 사항이 적용되는 데 최대 10분이 소요될 수 있습니다.

7. StorageGRID의 플랫폼 서비스 관련 메시지가 차단되지 않도록 프록시 서버 설정을 확인하십시오.
8. 스토리지 프록시를 비활성화해야 하는 경우 확인란을 선택 해제하고 *저장*을 선택하십시오.

StorageGRID에서 관리자 프록시 설정 구성

HTTP 또는 HTTPS를 사용하여 AutoSupport 패키지를 전송하는 경우 관리 노드와 기술 지원(AutoSupport) 간에 비투명 프록시 서버를 구성할 수 있습니다.

AutoSupport에 대한 자세한 내용은 "AutoSupport 구성"을 참조하십시오.

시작하기 전에

- "특정 액세스 권한"이(가) 있습니다.
- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.

이 작업 정보

단일 관리 프록시에 대한 설정을 구성할 수 있습니다.

단계

1. 구성 > 보안 > *프록시 설정*을 선택합니다.

   프록시 설정 페이지가 나타납니다. 기본적으로 탭 메뉴에서 저장소가 선택되어 있습니다.

2. **Admin** 탭을 선택합니다.
3. 관리자 프록시 활성화 확인란을 선택하십시오.
4. 프록시 서버의 호스트 이름 또는 IP 주소를 입력합니다.
5. 프록시 서버에 연결하는 데 사용되는 포트를 입력합니다.
6. 선택적으로 프록시 서버의 사용자 이름과 암호를 입력합니다.

   프록시 서버에 사용자 이름이나 비밀번호가 필요하지 않은 경우 이 필드를 비워 두십시오.

7. 다음 중 하나를 선택하십시오.

   ◦ 관리자 프록시에 대한 연결을 보호하려면 *프록시 인증서 확인*을 선택하십시오. CA 번들을 업로드하여 관리자 프록시 서버에서 제공하는 SSL 인증서의 신뢰성을 확인하십시오.

   > 프록시 인증서가 검증되면 AutoSupport on Demand, StorageGRID를 통한 E-Series AutoSupport 및 StorageGRID 업그레이드 페이지의 업데이트 경로 결정이 작동하지 않습니다.

   CA 번들을 업로드하면 메타데이터가 표시됩니다.

   ◦ 관리자 프록시 서버와 통신할 때 인증서를 확인하지 않으려면 *프록시 인증서 확인 안 함*을 선택하십시오.

8. *저장*을 선택하세요.

   관리자 프록시가 저장되면 관리 노드와 기술 지원 간의 프록시 서버가 구성됩니다.

   > 프록시 변경 사항이 적용되는 데 최대 10분이 소요될 수 있습니다.

9. 관리자 프록시를 비활성화해야 하는 경우 관리자 프록시 활성화 확인란의 선택을 해제한 다음 *저장*을 선택하십시오.

방화벽 제어

외부 방화벽에서 **StorageGRID** 액세스 제어

외부 방화벽에서 특정 포트를 열거나 닫을 수 있습니다.

StorageGRID 관리 노드의 사용자 인터페이스 및 API에 대한 액세스는 외부 방화벽에서 특정 포트를 열거나 닫아 제어할 수 있습니다. 예를 들어, 시스템 액세스를 제어하는 다른 방법 외에도 방화벽에서 테넌트가 Grid Manager에 연결하지 못하도록 차단할 수 있습니다.

StorageGRID 내부 방화벽을 구성하려면 "내부 방화벽 구성"을 참조하십시오.

포트	설명	포트가 열려 있다면...
443	관리자 노드의 기본 HTTPS 포트	웹 브라우저와 관리 API 클라이언트는 그리드 관리자, 그리드 관리 API, 테넌트 관리자 및 테넌트 관리 API에 액세스할 수 있습니다. 참고: 포트 443은 일부 내부 트래픽에도 사용됩니다.
8443	관리 노드의 그리드 관리자 포트 제한	• 웹 브라우저와 관리 API 클라이언트는 HTTPS를 사용하여 그리드 관리자 및 그리드 관리 API에 액세스할 수 있습니다. • 웹 브라우저와 관리 API 클라이언트는 테넌트 관리자 또는 테넌트 관리 API에 접근할 수 없습니다. • 내부 콘텐츠 요청은 거부됩니다.
9443	관리 노드의 테넌트 관리자 포트 제한	• 웹 브라우저와 관리 API 클라이언트는 HTTPS를 사용하여 테넌트 관리자 및 테넌트 관리 API에 액세스할 수 있습니다. • 웹 브라우저와 관리 API 클라이언트는 Grid Manager 또는 Grid Management API에 액세스할 수 없습니다. • 내부 콘텐츠 요청은 거부됩니다.

제한된 Grid Manager 또는 Tenant Manager 포트에서는 싱글 사인온(SSO)을 사용할 수 없습니다. 사용자가 싱글 사인온으로 인증하도록 하려면 기본 HTTPS 포트(443)를 사용해야 합니다.

관련 정보

- "Grid Manager에 로그인합니다"
- "테넌트 계정 생성"
- "외부 통신"

StorageGRID에서 내부 방화벽 제어 관리

StorageGRID는 각 노드에 내부 방화벽을 포함하여 노드에 대한 네트워크 액세스를 제어함으로써 그리드의 보안을 강화합니다. 방화벽을 사용하여 특정 그리드 배포에 필요한 포트를 제외한 모든 포트에 대한 네트워크 액세스를 차단할 수 있습니다. 방화벽 제어 페이지에서 변경한 구성은 각 노드에 적용됩니다.

방화벽 제어 페이지의 세 가지 탭을 사용하여 그리드에 필요한 액세스 권한을 사용자 지정합니다.

- **Privileged address list**: 이 탭을 사용하여 닫힌 포트에 대한 특정 액세스를 허용할 수 있습니다. 외부 액세스 관리 탭에서 닫힌 포트에 액세스할 수 있도록 IP 주소 또는 서브넷(CIDR 표기법)을 추가할 수 있습니다.
- 외부 액세스 관리: 이 탭을 사용하여 기본적으로 열려 있는 포트를 닫거나 이전에 닫았던 포트를 다시 열 수 있습니다.
- 신뢰할 수 없는 클라이언트 네트워크: 이 탭을 사용하여 노드가 클라이언트 네트워크에서 들어오는 트래픽을 신뢰할지 여부를 지정합니다.

  이 탭의 설정은 '외부 액세스 관리' 탭의 설정을 재정의합니다.

  - 신뢰할 수 없는 클라이언트 네트워크를 가진 노드는 해당 노드에 구성된 로드 밸런싱 엔드포인트 포트(전역, 노드 인터페이스 및 노드 유형 바인딩 엔드포인트)에 대한 연결만 허용합니다.
  - 로드 밸런서 엔드포인트 포트는 외부 네트워크 관리 탭의 설정과 관계없이 신뢰할 수 없는 클라이언트 네트워크에서 _유일하게 열려 있는 포트_입니다.
  - 신뢰할 수 있는 경우, 외부 액세스 관리 탭에서 열린 모든 포트와 클라이언트 네트워크에서 열린 모든 로드 밸런서 엔드포인트에 액세스할 수 있습니다.

> ⓘ 한 탭에서 설정한 내용이 다른 탭에서 변경한 액세스 권한에 영향을 줄 수 있습니다. 네트워크가 예상대로 작동하는지 확인하려면 모든 탭의 설정을 확인하십시오.

내부 방화벽 제어를 구성하려면 "방화벽 제어 구성"을 참조하십시오.

외부 방화벽 및 네트워크 보안에 대한 자세한 내용은 "외부 방화벽에서 액세스 제어"을 참조하십시오.

특권 주소 목록 및 외부 액세스 관리 탭

'특권 주소 목록' 탭에서는 닫혀 있는 그리드 포트에 대한 액세스 권한이 부여된 하나 이상의 IP 주소를 등록할 수 있습니다. '외부 액세스 관리' 탭에서는 선택한 외부 포트 또는 모든 열린 외부 포트(외부 포트는 기본적으로 그리드에 속하지 않은 노드에서 액세스할 수 있는 포트)에 대한 외부 액세스를 차단할 수 있습니다. 이 두 탭은 그리드에 허용해야 하는 정확한 네트워크 액세스를 사용자 지정하기 위해 함께 사용할 수 있습니다.

> ⓘ 권한 있는 IP 주소는 기본적으로 내부 그리드 포트에 대한 액세스 권한이 없습니다.

예시 **1:** 유지 관리 작업을 위해 점프 호스트 사용

보안이 강화된 호스트인 점프 호스트를 네트워크 관리에 사용하려는 경우를 가정해 보겠습니다. 다음과 같은 일반적인 단계를 따를 수 있습니다.

1. 권한 있는 주소 목록 탭을 사용하여 점프 호스트의 IP 주소를 추가하십시오.
2. 외부 액세스 관리 탭을 사용하여 모든 포트를 차단할 수 있습니다.

> ⓘ 포트 443 및 8443을 차단하기 전에 우선 순위 IP 주소를 추가하십시오. 현재 차단된 포트에 연결된 모든 사용자(본인 포함)는 IP 주소가 우선 순위 주소 목록에 추가되지 않으면 Grid Manager에 액세스할 수 없게 됩니다.

구성을 저장하면 그리드의 관리 노드에 있는 모든 외부 포트가 점프 호스트를 제외한 모든 호스트에 대해 차단됩니다. 그러면 점프 호스트를 사용하여 그리드에서 유지 관리 작업을 더욱 안전하게 수행할 수 있습니다.

예시 **2:** 민감한 포트 잠금

민감한 포트와 해당 포트에서 실행되는 서비스를 차단하고 싶다고 가정해 보겠습니다. 다음과 같은 일반적인 단계를 따를 수 있습니다.

1. '권한 있는 주소 목록' 탭을 사용하여 서비스에 액세스해야 하는 호스트에만 액세스 권한을 부여하십시오.
2. 외부 액세스 관리 탭을 사용하여 모든 포트를 차단할 수 있습니다.

> Grid Manager 및 Tenant Manager에 액세스하는 데 할당된 포트(기본 설정 포트는 443 및 8443)에 대한 액세스를 차단하기 전에 권한 있는 IP 주소를 추가하십시오. 차단된 포트에 현재 연결된 모든 사용자(본인 포함)는 IP 주소가 권한 있는 주소 목록에 추가되지 않으면 Grid Manager에 액세스할 수 없게 됩니다.

구성을 저장하면 해당 포트와 해당 포트의 서비스는 권한 있는 주소 목록에 있는 호스트에서만 사용할 수 있습니다. 다른 모든 호스트는 요청이 어떤 인터페이스를 통해 들어오든 관계없이 해당 서비스에 액세스할 수 없습니다.

예시 **3:** 사용하지 않는 서비스에 대한 액세스 비활성화

네트워크 수준에서 사용하지 않을 일부 서비스를 비활성화할 수 있습니다. 예를 들어 HTTP S3 클라이언트 트래픽을 차단하려면 외부 액세스 관리 탭에서 토글을 사용하여 18084번 포트를 차단하면 됩니다.

신뢰할 수 없는 클라이언트 네트워크 탭

클라이언트 네트워크를 사용하는 경우, 명시적으로 구성된 엔드포인트에서만 인바운드 클라이언트 트래픽을 허용함으로써 악의적인 공격으로부터 StorageGRID를 보호할 수 있습니다.

기본적으로 각 그리드 노드의 클라이언트 네트워크는 신뢰할 수 있는 상태입니다. 즉, 기본적으로 StorageGRID는 모든 "사용 가능한 외부 포트"에서 각 그리드 노드에 대한 인바운드 연결을 신뢰합니다.

StorageGRID 시스템에 대한 악의적인 공격 위협을 줄이려면 각 노드의 클라이언트 네트워크를 _신뢰할 수 없음_으로 지정하십시오. 노드의 클라이언트 네트워크가 신뢰할 수 없는 경우 해당 노드는 로드 밸런서 엔드포인트로 명시적으로 구성된 포트에서만 수신 연결을 허용합니다. "로드 밸런서 엔드포인트 구성" 및 "방화벽 제어 구성"을 참조하십시오.

예시 **1:** 게이트웨이 노드는 **HTTPS S3** 요청만 허용합니다

게이트웨이 노드가 HTTPS S3 요청을 제외한 클라이언트 네트워크의 모든 인바운드 트래픽을 거부하도록 설정하려면 다음과 같은 일반적인 단계를 수행합니다.

1. 해당 "로드 밸런서 엔드포인트" 페이지에서 포트 443을 통해 HTTPS를 사용하는 S3용 로드 밸런서 엔드포인트를 구성하십시오.
2. 방화벽 제어 페이지에서 Untrusted를 선택하여 게이트웨이 노드의 클라이언트 네트워크를 신뢰할 수 없는 것으로 지정합니다.

구성을 저장하면 게이트웨이 노드의 클라이언트 네트워크로 들어오는 모든 인바운드 트래픽은 차단되지만, 포트 443의 HTTPS S3 요청과 ICMP 에코(핑) 요청은 예외적으로 허용됩니다.

예시 **2:** 스토리지 노드가 **S3** 플랫폼 서비스 요청을 보냅니다

스토리지 노드에서 S3 플랫폼 서비스로의 아웃바운드 트래픽은 허용하되, 클라이언트 네트워크에서 해당 스토리지 노드로의 인바운드 연결은 차단하고 싶다고 가정해 보겠습니다. 이 경우 일반적으로 다음과 같은 단계를 수행합니다.

- 방화벽 제어 페이지의 '신뢰할 수 없는 클라이언트 네트워크' 탭에서 스토리지 노드의 클라이언트 네트워크가 신뢰할

수 없음을 지정합니다.

구성을 저장하면 스토리지 노드는 클라이언트 네트워크에서 들어오는 트래픽을 더 이상 수락하지 않지만, 구성된 플랫폼 서비스 대상으로 나가는 요청은 계속 허용합니다.

예제 **3: Grid Manager**에 대한 액세스를 서브넷으로 제한하기

특정 서브넷에서만 Grid Manager에 대한 액세스를 허용하려고 한다고 가정합니다. 다음 단계를 수행합니다.

1. 관리 노드의 클라이언트 네트워크를 서브넷에 연결하십시오.
2. 신뢰할 수 없는 클라이언트 네트워크 탭을 사용하여 클라이언트 네트워크를 신뢰할 수 없는 네트워크로 구성하십시오.
3. 관리 인터페이스 로드 밸런서 엔드포인트를 생성할 때 포트를 입력하고 해당 포트에서 액세스할 관리 인터페이스를 선택하십시오.
4. 신뢰할 수 없는 클라이언트 네트워크에 대해 *예*를 선택하십시오.
5. '외부 액세스 관리' 탭을 사용하여 모든 외부 포트를 차단할 수 있습니다(해당 서브넷 외부 호스트에 대해 특권 IP 주소를 설정했는지 여부와 관계없음).

구성을 저장하면 지정한 서브넷에 있는 호스트만 Grid Manager에 액세스할 수 있습니다. 다른 모든 호스트는 차단됩니다.

StorageGRID 내부 방화벽을 구성합니다

StorageGRID 방화벽을 구성하여 StorageGRID 노드의 특정 포트에 대한 네트워크 액세스를 제어할 수 있습니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- "특정 액세스 권한"이(가) 있습니다.
- 귀하는 "방화벽 제어 관리" 및 "네트워킹 가이드라인"에 있는 정보를 검토하셨습니다.
- 관리 노드 또는 게이트웨이 노드가 명시적으로 구성된 엔드포인트에서만 수신 트래픽을 허용하도록 하려면 로드 밸런싱 엔드포인트를 정의해야 합니다.

> 클라이언트 네트워크 구성을 변경할 때, 로드 밸런서 엔드포인트가 구성되지 않은 경우 기존 클라이언트 연결이 실패할 수 있습니다.

이 작업 정보

StorageGRID는 각 노드에 내부 방화벽을 포함하고 있어 그리드 노드의 일부 포트를 열거나 닫을 수 있습니다. 방화벽 제어 탭을 사용하여 그리드 네트워크, 관리 네트워크 및 클라이언트 네트워크에서 기본적으로 열려 있는 포트를 열거나 닫을 수 있습니다. 또한 닫혀 있는 그리드 포트에 액세스할 수 있는 권한 있는 IP 주소 목록을 생성할 수도 있습니다. 클라이언트 네트워크를 사용하는 경우 노드가 클라이언트 네트워크에서 들어오는 트래픽을 신뢰할지 여부를 지정하고 클라이언트 네트워크의 특정 포트에 대한 액세스를 구성할 수 있습니다.

그리드 외부의 IP 주소에 대해 반드시 필요한 포트만 열도록 포트 수를 제한하면 그리드 보안이 강화됩니다. 방화벽 제어 탭 세 곳 각각의 설정을 사용하여 필요한 포트만 열리도록 할 수 있습니다.

방화벽 제어 사용에 대한 자세한 내용(예제 포함)은 "방화벽 제어 관리"을 참조하십시오.

외부 방화벽 및 네트워크 보안에 대한 자세한 내용은 "외부 방화벽에서 액세스 제어"을 참조하십시오.

액세스 방화벽 제어

단계

1. * 구성 * > * 보안 * > * 방화벽 제어 * 를 선택합니다.

   이 페이지의 세 탭에 대한 설명은 "방화벽 제어 관리"에 있습니다.

2. 방화벽 설정을 구성하려면 아무 탭이나 선택하십시오.

   이 탭들은 어떤 순서로든 사용할 수 있습니다. 한 탭에서 설정한 구성은 다른 탭에서 수행할 수 있는 작업에 영향을 미치지 않습니다. 그러나 한 탭에서 구성을 변경하면 다른 탭에 구성된 포트의 동작이 변경될 수 있습니다.

권한 있는 주소 목록

권한 있는 주소 목록 탭을 사용하여 기본적으로 닫혀 있거나 외부 액세스 관리 탭의 설정에 따라 닫혀 있는 포트에 호스트가 액세스할 수 있도록 허용할 수 있습니다.

특권 IP 주소 및 서브넷은 기본적으로 내부 그리드 액세스가 허용되지 않습니다. 또한, 특권 주소 목록 탭에서 열린 로드 밸런서 엔드포인트 및 추가 포트는 외부 액세스 관리 탭에서 차단된 경우에도 액세스할 수 있습니다.

'권한 있는 주소 목록' 탭의 설정은 '신뢰할 수 없는 클라이언트 네트워크' 탭의 설정을 재정의할 수 없습니다.

단계

1. Privileged address list 탭에서 닫힌 포트에 대한 액세스 권한을 부여할 주소 또는 IP 서브넷을 입력합니다.
2. 선택적으로 *다른 IP 주소 또는 CIDR 표기법의 서브넷 추가*를 선택하여 권한 있는 클라이언트를 추가할 수 있습니다.

   권한 목록에는 가능한 한 적은 주소만 추가하십시오.

3. 선택적으로 *특권 있는 IP 주소가 StorageGRID 내부 포트에 액세스하도록 허용*을 선택할 수 있습니다. 을 참조하십시오."StorageGRID 내부 포트"

   이 옵션을 선택하면 내부 서비스에 대한 일부 보호 기능이 제거됩니다. 가능하면 이 옵션을 비활성화하십시오.

4. *저장*을 선택하세요.

외부 액세스 관리

'외부 액세스 관리' 탭에서 포트를 닫으면, 해당 IP 주소를 권한 있는 주소 목록에 추가하지 않는 한 그리드 IP 주소가 아닌 다른 IP 주소로는 해당 포트에 액세스할 수 없습니다. 기본적으로 열려 있는 포트만 닫을 수 있으며, 닫아 놓은 포트만 열 수 있습니다.

'외부 액세스 관리' 탭의 설정은 '신뢰할 수 없는 클라이언트 네트워크' 탭의 설정을 재정의할 수 없습니다. 예를 들어, 노드가 신뢰할 수 없는 것으로 설정된 경우, '외부 액세스 관리' 탭에서 SSH/22 포트가 열려 있더라도 클라이언트 네트워크에서는 해당 포트가 차단됩니다. '신뢰할 수 없는 클라이언트 네트워크' 탭의 설정은 클라이언트 네트워크에서 닫힌 포트(예: 443, 8443, 9443)를 재정의합니다.

단계

1. *외부 액세스 관리*를 선택합니다. 해당 탭에는 그리드에 있는 모든 노드의 외부 포트(기본적으로 그리드에 속하지 않은 노드에서 액세스할 수 있는 포트) 목록이 표 형식으로 표시됩니다.
2. 다음 옵션을 사용하여 열고 닫을 포트를 구성하십시오.
   - 각 포트 옆에 있는 토글을 사용하여 선택한 포트를 열거나 닫습니다.
   - 표에 나열된 모든 포트를 열려면 *표시된 모든 포트 열기*를 선택하십시오.
   - 표에 나열된 모든 포트를 닫으려면 *표시된 모든 포트 닫기*를 선택하십시오.

   Grid Manager 포트 443 또는 8443을 닫으면, 귀하를 포함하여 차단된 포트에 현재 연결된 모든 사용자는 IP 주소가 권한 있는 주소 목록에 추가되지 않은 한 Grid Manager에 대한 액세스 권한을 잃게 됩니다.

   표 오른쪽의 스크롤 막대를 사용하여 사용 가능한 모든 포트를 확인하십시오. 검색 필드에 포트 번호를 입력하여 외부 포트 설정을 찾을 수 있습니다. 포트 번호를 부분적으로 입력할 수도 있습니다. 예를 들어 *2*를 입력하면 이름에 "2"가 포함된 모든 포트가 표시됩니다.
3. *저장*을 선택합니다

신뢰할 수 없는 클라이언트 네트워크

노드의 클라이언트 네트워크가 신뢰할 수 없는 경우, 해당 노드는 로드 밸런싱 엔드포인트로 구성된 포트와 이 탭에서 선택적으로 추가한 포트에서만 수신 트래픽을 허용합니다. 또한 이 탭을 사용하여 확장에 추가된 새 노드의 기본 설정을 지정할 수 있습니다.

로드 밸런싱 엔드포인트가 구성되지 않은 경우 기존 클라이언트 연결이 실패할 수 있습니다.

신뢰할 수 없는 클라이언트 네트워크 탭에서 변경한 구성 내용은 외부 액세스 관리 탭의 설정을 재정의합니다.

단계

1. *신뢰할 수 없는 클라이언트 네트워크*를 선택하십시오.
2. '새 노드 기본값 설정' 섹션에서 확장 절차에서 새 노드가 그리드에 추가될 때 기본 설정이 무엇이어야 하는지 지정합니다.
   - 신뢰됨(기본값): 확장에 노드가 추가되면 해당 클라이언트 네트워크가 신뢰됩니다.
   - 신뢰할 수 없음: 확장에서 노드가 추가되면 해당 노드의 클라이언트 네트워크는 신뢰할 수 없는 것으로 간주됩니다.

   필요에 따라 이 탭으로 돌아와 특정 새 노드의 설정을 변경할 수 있습니다.

   이 설정은 StorageGRID 시스템의 기존 노드에 영향을 미치지 않습니다.

3. 다음 옵션을 사용하여 명시적으로 구성된 로드 밸런서 엔드포인트 또는 추가로 선택한 포트에서만 클라이언트 연결을 허용해야 하는 노드를 선택하십시오.

   - 표에 표시된 모든 노드를 신뢰할 수 없는 클라이언트 네트워크 목록에 추가하려면 *표시된 노드에 대해 신뢰하지 않음*을 선택하십시오.
   - 표에 표시된 모든 노드를 신뢰할 수 없는 클라이언트 네트워크 목록에서 제거하려면 *표시된 노드에 대한 신뢰*를 선택하십시오.
   - 각 노드 옆에 있는 토글을 사용하여 선택한 노드에 대해 클라이언트 네트워크를 신뢰할 수 있음 또는 신뢰할 수 없음으로 설정하십시오.

     예를 들어, *표시된 노드에 대해 신뢰하지 않음*을 선택하여 모든 노드를 신뢰할 수 없는 클라이언트 네트워크 목록에 추가한 다음, 개별 노드 옆에 있는 토글 버튼을 사용하여 해당 노드만 신뢰할 수 있는 클라이언트 네트워크 목록에 추가할 수 있습니다.

     표 오른쪽의 스크롤 막대를 사용하여 사용 가능한 모든 노드를 확인했는지 확인하십시오. 검색 필드를 사용하여 노드 이름을 입력하면 해당 노드의 설정을 찾을 수 있습니다. 부분적으로 이름을 입력할 수도 있습니다. 예를 들어 *GW*를 입력하면 이름에 "GW"가 포함된 모든 노드가 표시됩니다.

4. *저장*을 선택하세요.

   새 방화벽 설정은 즉시 적용되고 효력이 발생합니다. 로드 밸런서 엔드포인트가 구성되지 않은 경우 기존 클라이언트 연결이 실패할 수 있습니다.