보안 관리

StorageGRID 11.8

NetApp
May 17, 2024

목차

보안 관리

보안 관리: 개요

그리드 관리자에서 다양한 보안 설정을 구성하여 StorageGRID 시스템을 보호할 수 있습니다.

암호화 관리

StorageGRID는 데이터 암호화를 위한 여러 옵션을 제공합니다. 당신은 해야 한다 "사용 가능한 암호화 방법을 검토합니다" 데이터 보호 요구사항을 충족하는 스토리지 결정

인증서를 관리합니다

가능합니다 "서버 인증서를 구성하고 관리합니다" 서버에 대한 클라이언트 또는 사용자 ID를 인증하는 데 사용되는 클라이언트 인증서 또는 HTTP 연결에 사용됩니다.

키 관리 서버를 구성합니다

를 사용합니다 "키 관리 서버입니다" 어플라이언스를 데이터 센터에서 제거하더라도 StorageGRID 데이터를 보호할 수 있습니다. 어플라이언스 볼륨이 암호화된 후에는 노드에서 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 설정을 관리합니다

S3 플랫폼 서비스 또는 클라우드 스토리지 풀을 사용하는 경우 를 구성할 수 있습니다 "스토리지 프록시 서버입니다" 스토리지 노드 및 외부 S3 엔드포인트 간 HTTPS 또는 HTTP를 사용하여 AutoSupport 패키지를 보내는 경우 를 구성할 수 있습니다 "관리 프록시 서버" 관리 노드와 기술 지원 간

방화벽을 제어합니다

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

StorageGRID 암호화 방법을 검토합니다

StorageGRID는 데이터 암호화를 위한 여러 옵션을 제공합니다. 사용 가능한 방법을 검토하여 데이터 보호 요구 사항을 충족하는 방법을 결정해야 합니다.

이 표는 StorageGRID에서 사용할 수 있는 암호화 방법에 대한 상위 수준의 요약을 제공합니다.

암호화 옵션	작동 방식	적용 대상
Grid Manager의 키 관리 서버(KMS)	여러분 "키 관리 서버를 구성합니다" StorageGRID 사이트 및 의 경우 "어플라이언스에 대해 노드 암호화를 활성화합니다". 그런 다음 어플라이언스 노드가 KMS에 연결하여 키 암호화 키(KEK)를 요청합니다. 이 키는 각 볼륨의 DEK(데이터 암호화 키)를 암호화하고 해독합니다.	설치 중에 * 노드 암호화 * 가 활성화된 어플라이언스 노드 어플라이언스의 모든 데이터는 물리적 손실이나 데이터 센터에서 제거되는 것을 방지합니다. • 참고 *: KMS를 사용한 암호화 키 관리는 스토리지 노드 및 서비스 어플라이언스에서만 지원됩니다.
StorageGRID 어플라이언스 설치 프로그램의 드라이브 암호화 페이지	어플라이언스에 하드웨어 암호화를 지원하는 드라이브가 포함된 경우 설치 중에 드라이브 암호를 설정할 수 있습니다. 드라이브 암호를 설정하면 암호를 모르는 경우 시스템에서 제거된 드라이브에서 유효한 데이터를 복구할 수 없습니다. 설치를 시작하기 전에 * 하드웨어 구성 * > * 드라이브 암호화 * 로 이동하여 노드의 모든 StorageGRID에서 관리하는 자체 암호화 드라이브에 적용되는 드라이브 암호를 설정하십시오.	자체 암호화 드라이브를 포함하는 어플라이언스: 보안 드라이브의 모든 데이터는 데이터 센터에서 물리적 손실 또는 제거로부터 보호됩니다. 드라이브 암호화는 SANtricity에서 관리하는 드라이브에는 적용되지 않습니다. 자체 암호화 드라이브와 SANtricity 컨트롤러가 포함된 스토리지 어플라이언스가 있는 경우 SANtricity에서 드라이브 보안을 활성화할 수 있습니다.
SANtricity 시스템 관리자의 드라이브 보안	드라이브 보안 기능이 SG5700 또는 SG6000 스토리지 어플라이언스에 대해 활성화된 경우 를 사용할 수 있습니다 "SANtricity 시스템 관리자" 보안 키를 생성하고 관리합니다. 보안 드라이브의 데이터에 액세스하려면 키가 필요합니다.	FDE(전체 디스크 암호화) 드라이브 또는 자체 암호화 드라이브를 사용하는 스토리지 어플라이언스 보안 드라이브의 모든 데이터는 데이터 센터에서 물리적 손실 또는 제거로부터 보호됩니다. 일부 스토리지 어플라이언스나 서비스 어플라이언스와 함께 사용할 수 없습니다.
저장된 오브젝트 암호화	를 활성화합니다 "저장된 오브젝트 암호화" 옵션을 선택합니다. 이 기능을 사용하도록 설정하면 버킷 레벨이나 오브젝트 레벨에서 암호화되지 않은 새로운 모든 객체가 수집 중에 암호화됩니다.	새로 수집된 S3 및 Swift 오브젝트 데이터 저장된 기존 객체는 암호화되지 않습니다. 오브젝트 메타데이터 및 기타 중요한 데이터는 암호화되지 않습니다.

암호화 옵션	작동 방식	적용 대상
S3 버킷 암호화	버킷에 대한 암호화를 사용하도록 설정하기 위한 PutBucketEncryption 요청을 발행합니다. 오브젝트 레벨에서 암호화되지 않은 새로운 모든 오브젝트는 수집 중에 암호화됩니다.	새로 수집된 S3 오브젝트 데이터만 버킷에 대해 암호화를 지정해야 합니다. 기존 버킷 객체는 암호화되지 않습니다. 오브젝트 메타데이터 및 기타 중요한 데이터는 암호화되지 않습니다. "버킷 작업"
S3 오브젝트 서버 측 암호화(SSE)	오브젝트를 저장하고 을 포함하기 위한 S3 요청을 실행합니다 `x-amz-server-side-encryption` 요청 헤더.	새로 수집된 S3 오브젝트 데이터만 객체에 대해 암호화를 지정해야 합니다. 오브젝트 메타데이터 및 기타 중요한 데이터는 암호화되지 않습니다. StorageGRID가 키를 관리합니다. "서버측 암호화를 사용합니다"
고객이 제공한 키(SSE-C)를 사용한 S3 오브젝트 서버 측 암호화	S3 요청을 발급하여 오브젝트를 저장하고 세 개의 요청 헤더를 포함시킵니다. • `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 오브젝트 데이터만 객체에 대해 암호화를 지정해야 합니다. 오브젝트 메타데이터 및 기타 중요한 데이터는 암호화되지 않습니다. 키는 StorageGRID 외부에서 관리됩니다. "서버측 암호화를 사용합니다"
외부 볼륨 또는 데이터 저장소 암호화	구축 플랫폼에서 지원하는 경우 StorageGRID 외부의 암호화 방법을 사용하여 전체 볼륨 또는 데이터 저장소를 암호화합니다.	모든 볼륨 또는 데이터 저장소가 암호화되었다고 가정할 때 모든 오브젝트 데이터, 메타데이터 및 시스템 구성 데이터입니다. 외부 암호화 방법을 사용하면 암호화 알고리즘 및 키를 보다 강력하게 제어할 수 있습니다. 나열된 다른 방법과 결합할 수 있습니다.

암호화 옵션	작동 방식	적용 대상
StorageGRID 외부에서 개체 암호화	StorageGRID 외부에서 암호화 방법을 사용하여 오브젝트 데이터 및 메타데이터를 StorageGRID에 수집하기 전에 암호화합니다.	오브젝트 데이터 및 메타데이터만 (시스템 구성 데이터는 암호화되지 않음). 외부 암호화 방법을 사용하면 암호화 알고리즘 및 키를 보다 강력하게 제어할 수 있습니다. 나열된 다른 방법과 결합할 수 있습니다. "Amazon Simple Storage Service - 개발자 가이드: 클라이언트측 암호화를 사용하여 데이터 보호"

여러 암호화 방법을 사용합니다

요구 사항에 따라 한 번에 두 가지 이상의 암호화 방법을 사용할 수 있습니다. 예를 들면 다음과 같습니다.

- KMS를 사용하여 어플라이언스 노드를 보호하고 SANtricity 시스템 관리자의 드라이브 보안 기능을 사용하여 동일한 어플라이언스에 있는 자체 암호화 드라이브의 데이터를 "이중 암호화"할 수 있습니다.
- KMS를 사용하여 어플라이언스 노드의 데이터를 보호할 수 있으며 저장된 개체 암호화 옵션을 사용하여 수집될 때 모든 개체를 암호화할 수 있습니다.

오브젝트의 일부 부분만 암호화해야 하는 경우 대신 버킷 또는 개별 오브젝트 수준에서 암호화를 제어하는 것이 좋습니다. 여러 수준의 암호화를 사용하면 추가 성능 비용이 듭니다.

인증서를 관리합니다

보안 인증서 관리: 개요

보안 인증서는 StorageGRID 구성 요소와 StorageGRID 구성 요소 및 외부 시스템 간에 안전하고 신뢰할 수 있는 연결을 만드는 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 보안 연결을 설정하고, 클라이언트에 대한 서버 ID를 인증하고, 데이터에 대한 보안 통신 경로를 제공하는 데 사용됩니다. 서버와 클라이언트마다 인증서의 복사본이 있습니다.
- * 클라이언트 인증서 * 는 서버에 대한 클라이언트 또는 사용자 ID를 인증하여 암호만 사용하는 것보다 더 안전한 인증을 제공합니다. 클라이언트 인증서는 데이터를 암호화하지 않습니다.

클라이언트가 HTTPS를 사용하여 서버에 연결하면 서버는 공개 키가 포함된 서버 인증서로 응답합니다. 클라이언트는 서버 서명을 인증서 사본의 서명과 비교하여 이 인증서를 확인합니다. 서명이 일치하면 클라이언트는 동일한 공개 키를 사용하여 서버와 세션을 시작합니다.

StorageGRID는 로드 밸런서 끝점과 같은 일부 연결에 대한 서버 또는 CloudMirror 복제 서비스와 같은 다른 연결에 대한 클라이언트로 작동합니다.

- 기본 그리드 CA 인증서 *

StorageGRID에는 시스템 설치 중에 내부 그리드 CA 인증서를 생성하는 내장 CA(인증 기관)가 포함되어 있습니다. 그리드 CA 인증서는 기본적으로 내부 StorageGRID 트래픽을 보호하기 위해 사용됩니다. 외부 CA(인증 기관)는 조직의 정보 보안 정책을 완벽하게 준수하는 사용자 지정 인증서를 발급할 수 있습니다. 비프로덕션 환경에 대해 Grid CA 인증서를 사용할 수 있지만 프로덕션 환경에 가장 적합한 방법은 외부 인증 기관에서 서명한 사용자 지정 인증서를 사용하는 것입니다. 인증서가 없는 비보안 연결도 지원되지만 권장되지 않습니다.

- 사용자 지정 CA 인증서는 내부 인증서를 제거하지 않지만 사용자 지정 인증서는 서버 연결을 확인하기 위해 지정된 인증서여야 합니다.
- 모든 사용자 지정 인증서는 을 충족해야 합니다 "서버 인증서에 대한 시스템 강화 지침".
- StorageGRID는 CA의 인증서를 단일 파일(CA 인증서 번들이라고 함)로 번들링하는 것을 지원합니다.

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

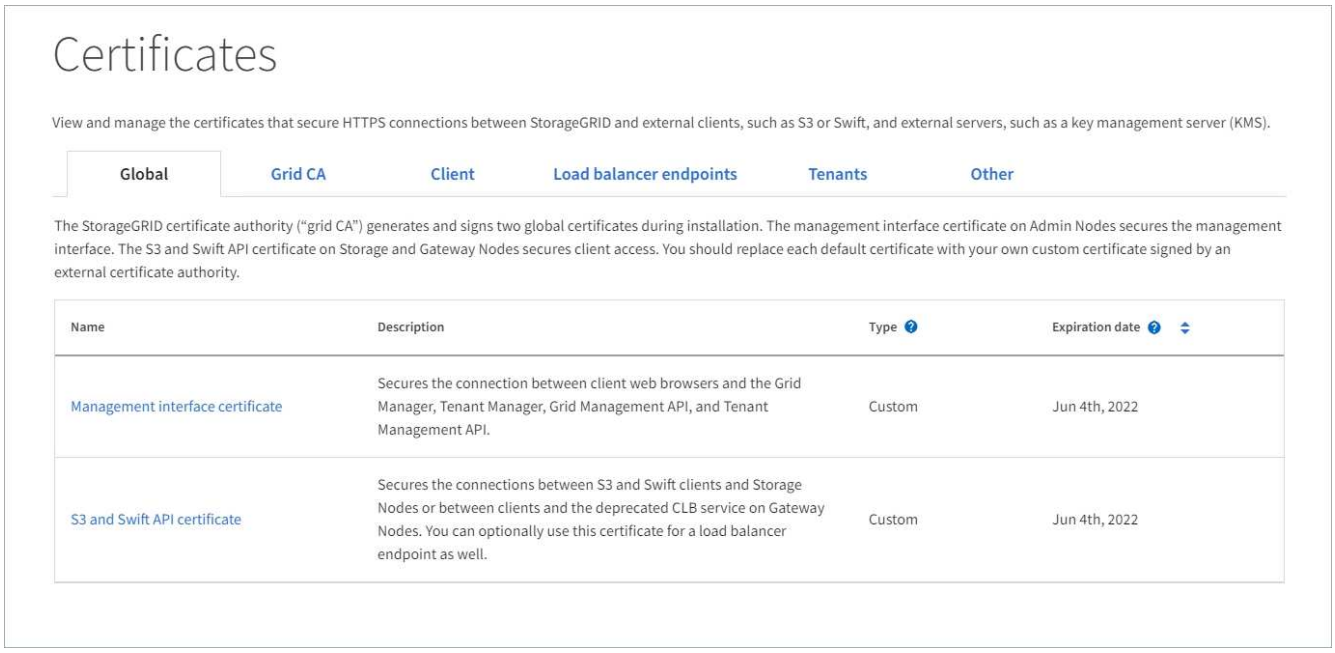
서버 및 클라이언트 인증서 유형의 변형은 여러 가지 방법으로 구현됩니다. 시스템을 구성하기 전에 특정 StorageGRID 구성에 필요한 모든 인증서를 준비해야 합니다.

보안 인증서에 액세스합니다

각 인증서의 구성 워크플로 링크와 함께 모든 StorageGRID 인증서에 대한 정보에 액세스할 수 있습니다.

단계

1. Grid Manager에서 * 구성 * > * 보안 * > * 인증서 * 를 선택합니다.



2. 인증서 페이지에서 탭을 선택하여 각 인증서 범주에 대한 정보를 확인하고 인증서 설정에 액세스합니다. 가 있는 경우 탭에 액세스할 수 있습니다 "적절한 권한".
   - * 글로벌 *: 웹 브라우저 및 외부 API 클라이언트에서 StorageGRID 액세스를 보호합니다.
   - * 그리드 CA *: 내부 StorageGRID 트래픽을 보호합니다.

- * 클라이언트 *: 외부 클라이언트와 StorageGRID Prometheus 데이터베이스 간의 연결을 보호합니다.
- * 로드 밸런서 엔드포인트 *: S3 및 Swift 클라이언트와 StorageGRID 로드 밸런서 간의 연결을 보호합니다.
- * 테넌트 *: ID 페더레이션 서버 또는 플랫폼 서비스 끝점에서 S3 스토리지 리소스에 대한 연결을 보호합니다.
- * 기타 *: 특정 인증서가 필요한 StorageGRID 연결을 보호합니다.

각 탭은 아래에 추가 인증서 세부 정보에 대한 링크와 함께 설명되어 있습니다.

글로벌

글로벌 인증서는 웹 브라우저 및 외부 S3 및 Swift API 클라이언트에서 StorageGRID 액세스를 보호합니다. 두 개의 글로벌 인증서는 처음에 설치 중에 StorageGRID 인증 기관에서 생성합니다. 프로덕션 환경의 모범 사례는 외부 인증 기관에서 서명한 사용자 지정 인증서를 사용하는 것입니다.

- 관리 인터페이스 인증서입니다: StorageGRID 관리 인터페이스에 대한 클라이언트 웹 브라우저 연결을 보호합니다.
- S3 및 Swift API 인증서: S3 및 Swift 클라이언트 애플리케이션이 오브젝트 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 있는 인증서 이름입니다.
- * 설명 *
- * 유형 *: 사용자 정의 또는 기본값 를 누릅니다 향상된 그리드 보안을 위해 항상 사용자 지정 인증서를 사용해야 합니다.
- * 만료 날짜 *: 기본 인증서를 사용하는 경우 만료 날짜가 표시되지 않습니다.

다음을 수행할 수 있습니다.

- 기본 인증서를 외부 인증 기관에서 서명한 사용자 지정 인증서로 교체하여 그리드 보안 강화:
  - "기본 StorageGRID 생성 관리 인터페이스 인증서를 교체합니다" Grid Manager 및 Tenant Manager 연결에 사용됩니다.
  - "S3 및 Swift API 인증서를 교체합니다" 스토리지 노드 및 로드 밸런서 엔드포인트(옵션) 연결에 사용됩니다.
- "기본 관리 인터페이스 인증서를 복원합니다."
- "기본 S3 및 Swift API 인증서를 복원합니다."
- "스크립트를 사용하여 자체 서명된 새 관리 인터페이스 인증서를 생성합니다."
- 를 복사 또는 다운로드합니다 "관리 인터페이스 인증서입니다" 또는 "S3 및 Swift API 인증서".

그리드 **CA**

를 클릭합니다 Grid CA 인증서StorageGRID 설치 중에 StorageGRID 인증 기관에서 생성한 는 모든 내부 StorageGRID 트래픽을 보호합니다.

인증서 정보에는 인증서 만료 날짜 및 인증서 내용이 포함됩니다.

가능합니다 "Grid CA 인증서를 복사하거나 다운로드합니다"하지만 변경할 수는 없습니다.

클라이언트

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

인증서 테이블에는 구성된 각 클라이언트 인증서에 대한 행이 있으며 인증서 만료 날짜와 함께 인증서를 Prometheus 데이터베이스 액세스에 사용할 수 있는지 여부를 나타냅니다.

다음을 수행할 수 있습니다.

- "새 클라이언트 인증서를 업로드하거나 생성합니다."
- 인증서 이름을 선택하면 다음 작업을 수행할 수 있는 인증서 세부 정보가 표시됩니다.
  - "클라이언트 인증서 이름을 변경합니다."
  - "Prometheus 액세스 권한을 설정합니다."
  - "클라이언트 인증서를 업로드하고 교체합니다."
  - "클라이언트 인증서를 복사하거나 다운로드합니다."
  - "클라이언트 인증서를 제거합니다."
- 빠른 작업을 하려면 * Actions * 를 선택합니다 "편집", "첨부", 또는 "제거" 클라이언트 인증서. 클라이언트 인증서를 최대 10개까지 선택하고 * Actions * > * Remove * 를 사용하여 한 번에 제거할 수 있습니다.

부하 분산 장치 엔드포인트

로드 밸런서 끝점 인증서 게이트웨이 노드와 관리 노드에서 S3 및 Swift 클라이언트와 StorageGRID 로드 밸런서 서비스 간의 연결을 보호합니다.

로드 밸런서 끝점 테이블에는 구성된 각 로드 밸런서 끝점에 대한 행이 있으며 전역 S3 및 Swift API 인증서나 사용자 지정 로드 밸런서 끝점 인증서가 끝점에 사용되고 있는지 여부를 나타냅니다. 각 인증서의 만료 날짜도 표시됩니다.

> 끝점 인증서 변경 내용을 모든 노드에 적용하는 데 최대 15분이 걸릴 수 있습니다.

다음을 수행할 수 있습니다.

- "로드 밸런서 끝점을 봅니다"인증서 세부 정보를 포함합니다.
- "FabricPool에 대한 로드 밸런서 끝점 인증서를 지정합니다."
- "글로벌 S3 및 Swift API 인증서를 사용합니다" 새 로드 밸런서 끝점 인증서를 생성하는 대신

테넌트

테넌트가 를 사용할 수 있습니다 ID 페더레이션 서버 인증서 또는 플랫폼 서비스 끝점 인증서 StorageGRID에 대한 연결을 보호합니다.

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

다음을 수행할 수 있습니다.

- "테넌트 관리자에 로그인할 테넌트 이름을 선택합니다"
- "테넌트 이름을 선택하여 테넌트 ID 페더레이션 세부 정보를 봅니다"
- "테넌트 이름을 선택하여 테넌트 플랫폼 서비스 세부 정보를 봅니다"
- "엔드포인트 생성 중에 플랫폼 서비스 끝점 인증서를 지정합니다"

기타

StorageGRID는 특정 목적으로 다른 보안 인증서를 사용합니다. 이러한 인증서는 기능 이름으로 나열됩니다. 기타 보안 인증서에는 다음이 포함됩니다.

- 클라우드 스토리지 풀 인증서

- 이메일 경고 알림 인증서
- 외부 syslog 서버 인증서
- 그리드 페더레이션 연결 인증서
- ID 페더레이션 인증서
- KMS(키 관리 서버) 인증서
- SSO(Single Sign-On) 인증서

정보는 함수에 사용되는 인증서 유형과 해당 서버 및 클라이언트 인증서 만료 날짜를 나타냅니다. 기능 이름을 선택하면 인증서 세부 정보를 보고 편집할 수 있는 브라우저 탭이 열립니다.

> 가 있는 경우에만 다른 인증서의 정보를 보고 액세스할 수 있습니다 "적절한 권한".

다음을 수행할 수 있습니다.

- "S3, C2S S3 또는 Azure에 대한 클라우드 스토리지 풀 인증서를 지정합니다"
- "경고 e-메일 알림에 사용할 인증서를 지정합니다"
- "외부 syslog 서버에 인증서를 사용합니다"
- "그리드 페더레이션 연결 인증서를 회전합니다"
- "ID 페더레이션 인증서를 보고 편집합니다"
- "KMS(키 관리 서버) 서버 및 클라이언트 인증서를 업로드합니다"
- "신뢰할 수 있는 당사자 트러스트를 위해 SSO 인증서를 수동으로 지정합니다"

보안 인증서 세부 정보입니다

각 보안 인증서 유형은 구현 지침에 대한 링크와 함께 아래에 설명되어 있습니다.

관리 인터페이스 인증서입니다

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버	클라이언트 웹 브라우저와 StorageGRID 관리 인터페이스 간의 연결을 인증하여 사용자가 보안 경고 없이 그리드 관리자 및 테넌트 관리자에 액세스할 수 있도록 합니다. 또한 이 인증서는 Grid Management API 및 테넌트 관리 API 연결을 인증합니다. 설치 중에 생성된 기본 인증서를 사용하거나 사용자 지정 인증서를 업로드할 수 있습니다.	• 구성 * > * 보안 * > * 인증서 * 에서 * 글로벌 * 탭을 선택한 다음 * 관리 인터페이스 인증서 * 를 선택합니다	"관리 인터페이스 인증서를 구성합니다"

S3 및 **Swift API** 인증서

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버	스토리지 노드에 대한 보안 S3 또는 Swift 클라이언트 연결을 인증하고 밸런서 엔드포인트를 로드합니다(선택 사항).	• 구성 * > * 보안 * > * 인증서 * 에서 * 글로벌 * 탭을 선택한 다음 * S3 및 Swift API 인증서 * 를 선택합니다	"S3 및 Swift API 인증서를 구성합니다"

Grid CA 인증서

를 참조하십시오 기본 그리드 CA 인증서 설명입니다.

관리자 클라이언트 인증서입니다

인증서 유형입니다	설명	내비게이션 위치	세부 정보
클라이언트	각 클라이언트에 설치되어 StorageGRID에서 외부 클라이언트 액세스를 인증할 수 있습니다. • 권한이 있는 외부 클라이언트가 StorageGRID Prometheus 데이터베이스에 액세스할 수 있습니다. • 외부 도구를 사용하여 StorageGRID를 안전하게 모니터링할 수 있습니다.	구성 * > * 보안 * > * 인증서 * 를 선택한 다음 * 클라이언트 * 탭을 선택합니다	"클라이언트 인증서를 구성합니다"

로드 밸런서 끝점 인증서

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버	게이트웨이 노드와 관리 노드에서 S3 또는 Swift 클라이언트와 StorageGRID 로드 밸런서 서비스 간의 연결을 인증합니다. 로드 밸런서 끝점을 구성할 때 로드 밸런서 인증서를 업로드하거나 생성할 수 있습니다. 클라이언트 응용 프로그램은 StorageGRID에 연결할 때 로드 밸런서 인증서를 사용하여 개체 데이터를 저장하고 검색합니다. 사용자 지정 버전의 Global을 사용할 수도 있습니다 S3 및 Swift API 인증서 로드 밸런서 서비스에 대한 연결을 인증하는 인증서입니다. 글로벌 인증서를 사용하여 로드 밸런서 연결을 인증하는 경우 각 로드 밸런서 끝점에 대해 별도의 인증서를 업로드하거나 생성할 필요가 없습니다. • 참고: * 로드 밸런서 인증에 사용되는 인증서는 일반적인 StorageGRID 작업 중에 가장 많이 사용되는 인증서입니다.	구성 * > * 네트워크 * > * 로드 밸런서 엔드포인트 *	• "로드 밸런서 엔드포인트를 구성합니다" • "FabricPool용 로드 밸런서 끝점을 만듭니다"

Cloud Storage Pool 엔드포인트 인증서입니다

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버	StorageGRID 클라우드 스토리지 풀에서 S3 Glacier 또는 Microsoft Azure Blob 스토리지와 같은 외부 스토리지 위치로 연결을 인증합니다. 각 클라우드 공급자 유형에는 다른 인증서가 필요합니다.	ILM * > * 스토리지 풀 *	"클라우드 스토리지 풀을 생성합니다"

이메일 경고 알림 인증서입니다

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버 및 클라이언트	SMTP 이메일 서버와 알림 알림에 사용되는 StorageGRID 간의 연결을 인증합니다. • SMTP 서버와의 통신에 TLS(Transport Layer Security)가 필요한 경우 전자 메일 서버 CA 인증서를 지정해야 합니다. • SMTP 전자 메일 서버에 인증을 위해 클라이언트 인증서가 필요한 경우에만 클라이언트 인증서를 지정합니다.	• 알림 * > * 이메일 설정 *	"알림에 대한 이메일 알림을 설정합니다"

외부 **syslog** 서버 인증서입니다

인증서 유형입니다	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 서버를 사용합니다"

그리드 페더레이션 연결 인증서

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버 및 클라이언트	그리드 페더레이션 연결에서 현재 StorageGRID 시스템과 다른 그리드 간에 전송된 정보를 인증하고 암호화합니다.	• 구성 * > * 시스템 * > * 그리드 페더레이션 *	• "그리드 페더레이션 연결을 만듭니다" • "연결 인증서를 회전합니다"

ID 페더레이션 인증서

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버	Active Directory, OpenLDAP 또는 Oracle Directory Server와 같은 외부 ID 공급자와 StorageGRID 간의 연결을 인증합니다. ID 페더레이션에 사용됩니다. 이 페더레이션을 사용하면 외부 시스템에서 관리 그룹 및 사용자를 관리할 수 있습니다.	• 구성 * > * 액세스 제어 * > * ID 페더레이션 *	"ID 페더레이션을 사용합니다"

KMS(키 관리 서버**)** 인증서

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버 및 클라이언트	StorageGRID와 StorageGRID 어플라이언스 노드에 암호화 키를 제공하는 외부 키 관리 서버(KMS) 간의 연결을 인증합니다.	구성 * > * 보안 * > * 키 관리 서버 *	"KMS(키 관리 서버) 추가"

플랫폼 서비스 끝점 인증서

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버	StorageGRID 플랫폼 서비스에서 S3 스토리지 리소스에 대한 연결을 인증합니다.	• 테넌트 관리자 * > * 스토리지(S3) * > * 플랫폼 서비스 엔드포인트 *	"플랫폼 서비스 끝점을 만듭니다" "플랫폼 서비스 끝점을 편집합니다"

SSO(Single Sign-On) 인증서

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

인증서 예

예 **1:** 부하 분산 서비스

이 예에서 StorageGRID는 서버 역할을 합니다.

1. 로드 밸런서 끝점을 구성하고 StorageGRID에서 서버 인증서를 업로드하거나 생성합니다.
2. 로드 밸런서 끝점에 S3 또는 Swift 클라이언트 연결을 구성하고 동일한 인증서를 클라이언트에 업로드합니다.
3. 클라이언트가 데이터를 저장하거나 검색하려는 경우 HTTPS를 사용하여 로드 밸런서 끝점에 연결합니다.
4. StorageGRID는 공개 키가 포함된 서버 인증서와 개인 키를 기반으로 하는 서명으로 응답합니다.
5. 클라이언트는 서버 서명을 인증서 사본의 서명과 비교하여 이 인증서를 확인합니다. 서명이 일치하면 클라이언트는 동일한 공개 키를 사용하여 세션을 시작합니다.
6. 클라이언트가 StorageGRID로 개체 데이터를 보냅니다.

예 **2:** 외부 키 관리 서버**(KMS)**

이 예에서 StorageGRID는 클라이언트 역할을 합니다.

1. 외부 키 관리 서버 소프트웨어를 사용하면 StorageGRID를 KMS 클라이언트로 구성하고 CA 서명된 서버 인증서, 공용 클라이언트 인증서 및 클라이언트 인증서에 대한 개인 키를 얻을 수 있습니다.
2. Grid Manager를 사용하여 KMS 서버를 구성하고 서버 및 클라이언트 인증서와 클라이언트 개인 키를 업로드합니다.
3. StorageGRID 노드에 암호화 키가 필요한 경우, 이 노드는 인증서의 데이터와 개인 키를 기반으로 하는 서명을 포함하는 KMS 서버에 요청합니다.
4. KMS 서버는 인증서 서명의 유효성을 검사하고 StorageGRID를 신뢰할 수 있는지 결정합니다.
5. KMS 서버는 검증된 연결을 사용하여 응답합니다.

서버 인증서를 구성합니다

지원되는 서버 인증서 유형입니다

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

> 보안 정책의 암호화 유형은 서버 인증서 유형과 일치해야 합니다. 예를 들어, RSA cipherer는 RSA 인증서가 필요하며, ECDSA cipherer는 ECDSA 인증서가 필요합니다. 을 참조하십시오 "보안 인증서를 관리합니다". 서버 인증서와 호환되지 않는 사용자 지정 보안 정책을 구성하면 됩니다 "일시적으로 기본 보안 정책으로 돌아갑니다".

StorageGRID가 클라이언트 연결을 보호하는 방법에 대한 자세한 내용은 을 참조하십시오 "S3 및 Swift 클라이언트에 대한 보안".

관리 인터페이스 인증서를 구성합니다

기본 관리 인터페이스 인증서를 단일 사용자 지정 인증서로 대체하면 보안 경고가 발생하지 않고 사용자가 Grid Manager 및 Tenant Manager에 액세스할 수 있습니다. 기본 관리 인터페이스

인증서로 되돌리거나 새 인증서를 생성할 수도 있습니다.

이 작업에 대해

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

모든 관리 노드에 하나의 사용자 지정 관리 인터페이스 인증서가 사용되므로 클라이언트가 Grid Manager 및 Tenant Manager에 연결할 때 호스트 이름을 확인해야 하는 경우 인증서를 와일드카드 또는 다중 도메인 인증서로 지정해야 합니다. 사용자 지정 인증서를 정의하여 그리드의 모든 관리 노드와 일치시킵니다.

서버에서 구성을 완료해야 하며 사용 중인 루트 인증 기관(CA)에 따라 사용자가 그리드 관리자 및 테넌트 관리자에 액세스하는 데 사용할 웹 브라우저에 그리드 CA 인증서를 설치해야 할 수도 있습니다.

> 실패한 서버 인증서로 인해 작업이 중단되지 않도록 하려면 이 서버 인증서가 곧 만료될 때 * Management Interface * 용 서버 인증서 만료 알림이 트리거됩니다. 필요에 따라 * 구성 * > * 보안 * > * 인증서 * 를 선택하고 글로벌 탭에서 관리 인터페이스 인증서의 만료 날짜를 보면 현재 인증서가 만료되는 시점을 확인할 수 있습니다.

> IP 주소 대신 도메인 이름을 사용하여 Grid Manager 또는 Tenant Manager에 액세스하는 경우, 다음 중 하나가 발생할 경우 브라우저에 인증서 오류가 표시되지 않고 무시하도록 옵션이 표시되지 않습니다.
>
> - 사용자 지정 관리 인터페이스 인증서가 만료됩니다.
> - 여러분 사용자 지정 관리 인터페이스 인증서에서 기본 서버 인증서로 되돌립니다.

사용자 지정 관리 인터페이스 인증서를 추가합니다

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

단계

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

인증서를 업로드합니다

필요한 서버 인증서 파일을 업로드합니다.

a. 인증서 업로드 * 를 선택합니다.

b. 필요한 서버 인증서 파일을 업로드합니다.

   - * 서버 인증서 *: 사용자 정의 서버 인증서 파일(PEM 인코딩).
   - * 인증서 개인 키 *: 사용자 지정 서버 인증서 개인 키 파일입니다 (`.key`)를 클릭합니다.

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

   - * CA 번들 *: 각 중간 발급 CA(인증 기관)의 인증서를 포함하는 단일 선택적 파일입니다. 파일에는 인증서 체인 순서에 연결된 PEM 인코딩된 CA 인증서 파일이 각각 포함되어야 합니다.

c. 업로드한 각 인증서의 메타데이터를 보려면 * 인증서 세부 정보 * 를 확장합니다. 선택적 CA 번들을 업로드한 경우 각 인증서는 자체 탭에 표시됩니다.

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

     인증서 파일 이름 및 다운로드 위치를 지정합니다. 파일을 확장자로 저장합니다 `.pem`.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

   - 다른 곳에 붙여넣을 인증서 내용을 복사하려면 * 인증서 PEM * 복사 또는 * CA 번들 PEM * 복사 를 선택합니다.

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

인증서를 생성합니다

서버 인증서 파일을 생성합니다.

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

a. 인증서 생성 * 을 선택합니다.

b. 인증서 정보를 지정합니다.

필드에 입력합니다	설명
도메인 이름	인증서에 포함할 하나 이상의 정규화된 도메인 이름입니다. 여러 도메인 이름을 나타내는 와일드카드로 * 를 사용합니다.
IP	인증서에 포함할 하나 이상의 IP 주소입니다.

필드에 입력합니다	설명
제목(선택 사항)	X.509 인증서 소유자의 주체 또는 고유 이름(DN)입니다. 이 필드에 값을 입력하지 않으면 생성된 인증서는 첫 번째 도메인 이름 또는 IP 주소를 CN(Subject Common Name)으로 사용합니다.
일 유효	인증서가 만료된 후 경과한 일 수입니다.
키 사용 확장을 추가합니다	이 옵션을 선택하면(기본값 및 권장) 키 사용 및 확장 키 사용 확장이 생성된 인증서에 추가됩니다. 이러한 확장은 인증서에 포함된 키의 용도를 정의합니다. • 참고 *: 인증서에 이러한 확장자가 포함되어 있을 때 이전 클라이언트와의 연결 문제가 발생하지 않는 한 이 확인란을 선택된 상태로 둡니다.

c. Generate * 를 선택합니다.

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

   ▪ 인증서 파일을 저장하려면 * 인증서 다운로드 * 를 선택합니다.

     인증서 파일 이름 및 다운로드 위치를 지정합니다. 파일을 확장자로 저장합니다 `.pem`.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

   ▪ 다른 곳에 붙여넣을 인증서 내용을 복사하려면 * 인증서 PEM * 복사 를 선택합니다.

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

5. 페이지를 새로 고쳐 웹 브라우저가 업데이트되도록 합니다.

> 새 인증서를 업로드하거나 생성한 후에는 관련 인증서 만료 알림을 지울 수 있도록 최대 하루 동안 기다립니다.

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

기본 관리 인터페이스 인증서를 복원합니다

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

단계

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

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

4. 페이지를 새로 고쳐 웹 브라우저가 업데이트되도록 합니다.

스크립트를 사용하여 자체 서명된 새 관리 인터페이스 인증서를 생성합니다

엄격한 호스트 이름 확인이 필요한 경우 스크립트를 사용하여 관리 인터페이스 인증서를 생성할 수 있습니다.

시작하기 전에

- 있습니다 "특정 액세스 권한".
- 을(를) 보유하고 있습니다 `Passwords.txt` 파일.

이 작업에 대해

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

단계

1. 각 관리 노드의 FQDN(정규화된 도메인 이름)을 얻습니다.
2. 기본 관리자 노드에 로그인합니다.
   a. 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`
   b. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.
   c. 루트로 전환하려면 다음 명령을 입력합니다. `su -`
   d. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.

      루트로 로그인하면 프롬프트가 에서 변경됩니다 `$` 를 선택합니다 `#`.
3. 자체 서명된 새 인증서를 사용하여 StorageGRID를 구성합니다.

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

   - 용 `--domains`에서 와일드카드를 사용하여 모든 관리 노드의 정규화된 도메인 이름을 나타냅니다. 예를 들면, 다음과 같습니다. `*.ui.storagegrid.example.com` 와일드카드를 사용하여 나타냅니다 `admin1.ui.storagegrid.example.com` 및 `admin2.ui.storagegrid.example.com`.
   - 설정 `--type` 를 선택합니다 `management` Grid Manager 및 Tenant Manager에서 사용하는 관리 인터페이스 인증서를 구성합니다.
   - 기본적으로 생성된 인증서는 1년(365일) 동안 유효하며 만료되기 전에 다시 만들어야 합니다. 를 사용할 수 있습니다 `--days` 기본 유효 기간을 재정의하는 인수입니다.

     > 인증서의 유효 기간은 언제 시작됩니다 `make-certificate` 가 실행됩니다. 관리 클라이언트가 StorageGRID와 동일한 시간 소스와 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 공용 인증서가 포함됩니다.

4. 인증서를 선택하고 복사합니다.

   선택 항목에 BEGIN 및 END 태그를 포함합니다.

5. 명령 셸에서 로그아웃합니다. `$ exit`
6. 인증서가 구성되었는지 확인합니다.
   a. 그리드 관리자에 액세스합니다.
   b. 구성 * > * 보안 * > * 인증서 * 를 선택합니다
   c. 글로벌 * 탭에서 * 관리 인터페이스 인증서 * 를 선택합니다.
7. 복사한 공용 인증서를 사용하도록 관리 클라이언트를 구성합니다. BEGIN 및 END Tags를 포함합니다.

관리 인터페이스 인증서를 다운로드하거나 복사합니다

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

단계

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

인증서 파일 또는 **CA** 번들을 다운로드합니다

인증서 또는 CA 번들을 다운로드합니다 `.pem` 파일. 선택적 CA 번들을 사용하는 경우 번들의 각 인증서가 자체 하위 탭에 표시됩니다.

a. 인증서 다운로드 * 또는 * CA 번들 다운로드 * 를 선택합니다.

   CA 번들을 다운로드하는 경우 CA 번들 보조 탭의 모든 인증서가 단일 파일로 다운로드됩니다.

b. 인증서 파일 이름 및 다운로드 위치를 지정합니다. 파일을 확장자로 저장합니다 `.pem`.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

인증서 또는 **CA** 번들 **PEM**을 복사합니다

인증서 텍스트를 복사하여 다른 곳에 붙여 넣습니다. 선택적 CA 번들을 사용하는 경우 번들의 각 인증서가 자체 하위 탭에 표시됩니다.

a. Copy certificate pem * 또는 * Copy CA bundle pem * 을 선택합니다.

   CA 번들을 복사하는 경우 CA 번들 보조 탭의 모든 인증서가 함께 복사됩니다.

b. 복사한 인증서를 텍스트 편집기에 붙여 넣습니다.

c. 텍스트 파일을 확장자로 저장합니다 `.pem`.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

S3 및 **Swift API** 인증서를 구성합니다

스토리지 노드에 대한 S3 또는 Swift 클라이언트 연결에 사용되는 서버 인증서를 교체하거나 복구하거나 밸런서 엔드포인트를 로드할 수 있습니다. 교체 사용자 지정 서버 인증서는 조직에 따라 다릅니다.

이 작업에 대해

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

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

서버 구성을 완료한 후 사용 중인 루트 CA(인증 기관)에 따라 시스템에 액세스하는 데 사용할 S3 또는 Swift API 클라이언트에 그리드 CA 인증서를 설치해야 할 수도 있습니다.

> 실패한 서버 인증서로 인해 작업이 중단되지 않도록 하려면 루트 서버 인증서가 곧 만료될 때 * S3 및 Swift API * 용 글로벌 서버 인증서 만료 알림이 트리거됩니다. 필요에 따라 * 구성 * > * 보안 * > * 인증서 * 를 선택하고 글로벌 탭에서 S3 및 Swift API 인증서의 만료 날짜를 보면 현재 인증서가 만료되는 시점을 확인할 수 있습니다.

사용자 지정 S3 및 Swift API 인증서를 업로드하거나 생성할 수 있습니다.

사용자 지정 **S3** 및 **Swift API** 인증서를 추가합니다

단계

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

인증서를 업로드합니다

필요한 서버 인증서 파일을 업로드합니다.

a. 인증서 업로드 * 를 선택합니다.

b. 필요한 서버 인증서 파일을 업로드합니다.

   - * 서버 인증서 *: 사용자 정의 서버 인증서 파일(PEM 인코딩).
   - * 인증서 개인 키 *: 사용자 지정 서버 인증서 개인 키 파일입니다 (`.key`)를 클릭합니다.

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

   - * CA 번들 *: 각 중간 발급 인증 기관의 인증서를 포함하는 단일 선택적 파일입니다. 파일에는 인증서 체인 순서에 연결된 PEM 인코딩된 CA 인증서 파일이 각각 포함되어야 합니다.

c. 업로드된 각 사용자 정의 S3 및 Swift API 인증서에 대한 메타데이터와 PEM을 표시하려면 인증서 세부 정보를 선택합니다. 선택적 CA 번들을 업로드한 경우 각 인증서는 자체 탭에 표시됩니다.

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

     인증서 파일 이름 및 다운로드 위치를 지정합니다. 파일을 확장자로 저장합니다 `.pem`.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

   - 다른 곳에 붙여넣을 인증서 내용을 복사하려면 * 인증서 PEM * 복사 또는 * CA 번들 PEM * 복사 를 선택합니다.

d. 저장 * 을 선택합니다.

   사용자 지정 서버 인증서는 이후에 새 S3 및 Swift 클라이언트 연결에 사용됩니다.

인증서를 생성합니다

서버 인증서 파일을 생성합니다.

a. 인증서 생성 * 을 선택합니다.

b. 인증서 정보를 지정합니다.

필드에 입력합니다	설명
도메인 이름	인증서에 포함할 하나 이상의 정규화된 도메인 이름입니다. 여러 도메인 이름을 나타내는 와일드카드로 * 를 사용합니다.
IP	인증서에 포함할 하나 이상의 IP 주소입니다.

필드에 입력합니다	설명
제목(선택 사항)	X.509 인증서 소유자의 주체 또는 고유 이름(DN)입니다. 이 필드에 값을 입력하지 않으면 생성된 인증서는 첫 번째 도메인 이름 또는 IP 주소를 CN(Subject Common Name)으로 사용합니다.
일 유효	인증서가 만료된 후 경과한 일 수입니다.
키 사용 확장을 추가합니다	이 옵션을 선택하면(기본값 및 권장) 키 사용 및 확장 키 사용 확장이 생성된 인증서에 추가됩니다. 이러한 확장은 인증서에 포함된 키의 용도를 정의합니다. • 참고 *: 인증서에 이러한 확장자가 포함되어 있을 때 이전 클라이언트와의 연결 문제가 발생하지 않는 한 이 확인란을 선택된 상태로 둡니다.

c. Generate * 를 선택합니다.

d. 생성된 사용자 정의 S3 및 Swift API 인증서에 대한 메타데이터와 PEM을 표시하려면 * 인증서 세부 정보 * 를 선택합니다.

   - 인증서 파일을 저장하려면 * 인증서 다운로드 * 를 선택합니다.

     인증서 파일 이름 및 다운로드 위치를 지정합니다. 파일을 확장자로 저장합니다 `.pem`.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

   - 다른 곳에 붙여넣을 인증서 내용을 복사하려면 * 인증서 PEM * 복사 를 선택합니다.

e. 저장 * 을 선택합니다.

   사용자 지정 서버 인증서는 이후에 새 S3 및 Swift 클라이언트 연결에 사용됩니다.

5. 탭을 선택하여 기본 StorageGRID 서버 인증서, 업로드된 CA 서명 인증서 또는 생성된 사용자 지정 인증서의 메타데이터를 표시합니다.

   > 새 인증서를 업로드하거나 생성한 후에는 관련 인증서 만료 알림을 지울 수 있도록 최대 하루 동안 기다립니다.

6. 페이지를 새로 고쳐 웹 브라우저가 업데이트되도록 합니다.

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

기본 **S3** 및 **Swift API** 인증서를 복원합니다

S3 및 Swift 클라이언트 연결에서 스토리지 노드에 대한 기본 S3 및 Swift API 인증서를 사용하도록 되돌릴 수 있습니다. 하지만 로드 밸런서 끝점에는 기본 S3 및 Swift API 인증서를 사용할 수 없습니다.

단계

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

   글로벌 S3 및 Swift API 인증서의 기본 버전을 복원하면 구성한 사용자 지정 서버 인증서 파일이 삭제되고 시스템에서 복구할 수 없습니다. 기본 S3 및 Swift API 인증서는 이후에 스토리지 노드에 대한 새 S3 및 Swift 클라이언트 연결에 사용됩니다.

4. 경고를 확인하고 기본 S3 및 Swift API 인증서를 복원하려면 * OK * 를 선택합니다.

   루트 액세스 권한이 있고 사용자 지정 S3 및 Swift API 인증서가 로드 밸런서 엔드포인트 연결에 사용된 경우 기본 S3 및 Swift API 인증서를 사용하여 더 이상 액세스할 수 없는 로드 밸런서 끝점의 목록이 표시됩니다. 로 이동합니다 "로드 밸런서 엔드포인트를 구성합니다" 영향을 받는 끝점을 편집하거나 제거합니다.

5. 페이지를 새로 고쳐 웹 브라우저가 업데이트되도록 합니다.

S3 및 Swift API 인증서를 다운로드하거나 복사합니다

다른 곳에서 사용할 수 있도록 S3 및 Swift API 인증서 내용을 저장하거나 복사할 수 있습니다.

단계

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

인증서 파일 또는 **CA** 번들을 다운로드합니다

인증서 또는 CA 번들을 다운로드합니다 `.pem` 파일. 선택적 CA 번들을 사용하는 경우 번들의 각 인증서가 자체 하위 탭에 표시됩니다.

a. 인증서 다운로드 * 또는 * CA 번들 다운로드 * 를 선택합니다.

   CA 번들을 다운로드하는 경우 CA 번들 보조 탭의 모든 인증서가 단일 파일로 다운로드됩니다.

b. 인증서 파일 이름 및 다운로드 위치를 지정합니다. 파일을 확장자로 저장합니다 `.pem`.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

인증서 또는 **CA** 번들 **PEM**을 복사합니다

인증서 텍스트를 복사하여 다른 곳에 붙여 넣습니다. 선택적 CA 번들을 사용하는 경우 번들의 각 인증서가 자체 하위 탭에 표시됩니다.

a. Copy certificate pem * 또는 * Copy CA bundle pem * 을 선택합니다.

   CA 번들을 복사하는 경우 CA 번들 보조 탭의 모든 인증서가 함께 복사됩니다.

b. 복사한 인증서를 텍스트 편집기에 붙여 넣습니다.

c. 텍스트 파일을 확장자로 저장합니다 `.pem`.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

관련 정보

- "S3 REST API 사용"
- "Swift REST API를 사용합니다"
- "S3 끝점 도메인 이름을 구성합니다"

Grid CA 인증서를 복사합니다

StorageGRID는 내부 CA(인증 기관)를 사용하여 내부 트래픽을 보호합니다. 인증서를 업로드해도 이 인증서는 변경되지 않습니다.

시작하기 전에

- 를 사용하여 그리드 관리자에 로그인했습니다 "지원되는 웹 브라우저".
- 있습니다 "특정 액세스 권한".

이 작업에 대해

사용자 지정 서버 인증서가 구성된 경우 클라이언트 응용 프로그램은 사용자 지정 서버 인증서를 사용하여 서버를 확인해야 합니다. StorageGRID 시스템에서 CA 인증서를 복사해서는 안 됩니다.

단계

1. 구성 * > * 보안 * > * 인증서 * 를 선택한 다음 * 그리드 CA * 탭을 선택합니다.
2. 인증서 PEM * 섹션에서 인증서를 다운로드하거나 복사합니다.

인증서 파일을 다운로드합니다

인증서를 다운로드합니다 `.pem` 파일.

a. 인증서 다운로드 * 를 선택합니다.
b. 인증서 파일 이름 및 다운로드 위치를 지정합니다. 파일을 확장자로 저장합니다 `.pem`.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

인증서 **PEM**을 복사합니다

인증서 텍스트를 복사하여 다른 곳에 붙여 넣습니다.

a. 인증서 PEM 복사 * 를 선택합니다.
b. 복사한 인증서를 텍스트 편집기에 붙여 넣습니다.
c. 텍스트 파일을 확장자로 저장합니다 `.pem`.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

FabricPool용 **StorageGRID** 인증서를 구성합니다

엄격한 호스트 이름 유효성 검사를 수행하고 FabricPool를 사용하는 ONTAP 클라이언트와 같은 엄격한 호스트 이름 유효성 검사 비활성화를 지원하지 않는 S3 클라이언트의 경우 로드 밸런서 끝점을 구성할 때 서버 인증서를 생성하거나 업로드할 수 있습니다.

시작하기 전에

- 있습니다 "특정 액세스 권한".
- 를 사용하여 그리드 관리자에 로그인했습니다 "지원되는 웹 브라우저".

이 작업에 대해

로드 밸런서 끝점을 만들 때 자체 서명된 서버 인증서를 생성하거나 알려진 CA(인증 기관)에서 서명한 인증서를 업로드할 수 있습니다. 프로덕션 환경에서는 알려진 CA가 서명한 인증서를 사용해야 합니다. CA에서 서명한 인증서는 중단 없이 회전할 수 있습니다. 또한 중간자 공격에 대한 보호 기능이 강화되어 보안이 더욱 강화되고 있습니다.

다음 단계에서는 FabricPool를 사용하는 S3 클라이언트에 대한 일반 지침을 제공합니다. 자세한 정보 및 절차는 를 참조하십시오 "FabricPool용 StorageGRID를 구성합니다".

단계

1. 선택적으로 FabricPool에서 사용할 고가용성(HA) 그룹을 구성합니다.
2. FabricPool에서 사용할 S3 로드 밸런서 끝점을 만듭니다.

   HTTPS 로드 밸런서 끝점을 만들면 서버 인증서, 인증서 개인 키 및 선택적 CA 번들을 업로드하라는 메시지가 표시됩니다.

3. StorageGRID을 ONTAP의 클라우드 계층으로 연결

   로드 밸런서 끝점 포트와 업로드한 CA 인증서에 사용된 정규화된 도메인 이름을 지정합니다. 그런 다음 CA 인증서를 제공합니다.

   > 중간 CA에서 StorageGRID 인증서를 발급한 경우 중간 CA 인증서를 제공해야 합니다. StorageGRID 인증서가 루트 CA에서 직접 발급된 경우 루트 CA 인증서를 제공해야 합니다.

클라이언트 인증서를 구성합니다

클라이언트 인증서를 사용하면 권한이 있는 외부 클라이언트가 StorageGRID Prometheus 데이터베이스에 액세스할 수 있으므로 외부 도구에서 StorageGRID를 모니터링하는 안전한 방법이 제공됩니다.

외부 모니터링 도구를 사용하여 StorageGRID에 액세스해야 하는 경우 그리드 관리자를 사용하여 클라이언트 인증서를 업로드하거나 생성하고 인증서 정보를 외부 도구에 복사해야 합니다.

을 참조하십시오 "보안 인증서를 관리합니다" 및 "사용자 지정 서버 인증서를 구성합니다".

> 실패한 서버 인증서로 인해 작업이 중단되지 않도록 하려면 이 서버 인증서가 곧 만료될 때 인증서 페이지 * 알림에 구성된 * 클라이언트 인증서 만료 알림이 트리거됩니다. 필요에 따라 * 구성 * > * 보안 * > * 인증서 * 를 선택하고 클라이언트 탭에서 클라이언트 인증서의 만료 날짜를 보면 현재 인증서가 만료되는 시점을 확인할 수 있습니다.

> KMS(키 관리 서버)를 사용하여 특수하게 구성된 어플라이언스 노드의 데이터를 보호하는 경우 에 대한 특정 정보를 참조하십시오 "KMS 클라이언트 인증서 업로드".

시작하기 전에

- 루트 액세스 권한이 있습니다.
- 를 사용하여 그리드 관리자에 로그인했습니다 "지원되는 웹 브라우저".
- 클라이언트 인증서를 구성하려면 다음을 따르십시오.
  - 관리 노드의 IP 주소 또는 도메인 이름이 있습니다.
  - StorageGRID 관리 인터페이스 인증서를 구성한 경우 관리 인터페이스 인증서를 구성하는 데 사용되는 CA, 클라이언트 인증서 및 개인 키가 있습니다.
  - 인증서를 업로드하려면 로컬 컴퓨터에서 인증서의 개인 키를 사용할 수 있습니다.
  - 개인 키는 생성 시 저장 또는 기록되어야 합니다. 원래 개인 키가 없으면 새 개인 키를 만들어야 합니다.
- 클라이언트 인증서를 편집하려면 다음을 따르십시오.
  - 관리 노드의 IP 주소 또는 도메인 이름이 있습니다.
  - 자체 인증서 또는 새 인증서를 업로드하려면 로컬 컴퓨터에서 개인 키, 클라이언트 인증서 및 CA(사용되는 경우)를 사용할 수 있습니다.

클라이언트 인증서를 추가합니다

클라이언트 인증서를 추가하려면 다음 절차 중 하나를 사용합니다.

- 관리 인터페이스 인증서가 이미 구성되어 있습니다
- CA 발급 클라이언트 인증서
- Grid Manager에서 인증서를 생성했습니다

관리 인터페이스 인증서가 이미 구성되어 있습니다

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

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 * 를 선택합니다.
5. Continue * 를 선택합니다.
6. 인증서 첨부 * 단계의 경우 관리 인터페이스 인증서를 업로드합니다.
   a. 인증서 업로드 * 를 선택합니다.
   b. Browse * 를 선택하고 관리 인터페이스 인증서 파일을 선택합니다 (`.pem`)를 클릭합니다.
      - 인증서 메타데이터와 인증서 PEM을 표시하려면 * 클라이언트 인증서 세부 정보 * 를 선택합니다.
      - 다른 곳에 붙여넣을 인증서 내용을 복사하려면 * 인증서 PEM * 복사 를 선택합니다.
   c. Grid Manager에 인증서를 저장하려면 * Create * 를 선택합니다.

      새 인증서가 클라이언트 탭에 나타납니다.
7. 외부 모니터링 툴을 구성합니다Grafana와 같은 기능을 사용할 수 있습니다.

CA 발급 클라이언트 인증서

관리 인터페이스 인증서가 구성되어 있지 않고 CA에서 발급한 클라이언트 인증서 및 개인 키를 사용하는 Prometheus에 대한 클라이언트 인증서를 추가하려는 경우 이 절차를 사용하여 관리자 클라이언트 인증서를 추가하십시오.

단계

1. 의 단계를 수행합니다 "관리 인터페이스 인증서를 구성합니다".
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 * 를 선택합니다.
6. Continue * 를 선택합니다.
7. 인증서 첨부 * 단계의 경우 클라이언트 인증서, 개인 키 및 CA 번들 파일을 업로드합니다.
   a. 인증서 업로드 * 를 선택합니다.

b. Browse * 를 선택하고 클라이언트 인증서, 개인 키 및 CA 번들 파일을 선택합니다 (`.pem`)를 클릭합니다.
   - 인증서 메타데이터와 인증서 PEM을 표시하려면 * 클라이언트 인증서 세부 정보 * 를 선택합니다.
   - 다른 곳에 붙여넣을 인증서 내용을 복사하려면 * 인증서 PEM * 복사 를 선택합니다.

c. Grid Manager에 인증서를 저장하려면 * Create * 를 선택합니다.

   새 인증서가 클라이언트 탭에 나타납니다.

8. 외부 모니터링 툴을 구성합니다Grafana와 같은 기능을 사용할 수 있습니다.

Grid Manager에서 인증서를 생성했습니다

관리 인터페이스 인증서가 구성되어 있지 않고 Grid Manager에서 인증서 생성 기능을 사용하는 Prometheus에 대한 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 * 를 선택합니다.
5. Continue * 를 선택합니다.
6. 인증서 첨부 * 단계에서 * 인증서 생성 * 을 선택합니다.
7. 인증서 정보를 지정합니다.
   - * subject * (선택 사항): X.509 주체 또는 인증서 소유자의 고유 이름(DN).
   - 유효한 * 일 수 *: 생성된 인증서가 생성된 시점부터 생성된 유효 일 수입니다.
   - * 키 사용 확장 추가 *: 선택한 경우(기본값 및 권장) 키 사용 및 확장 키 사용 확장이 생성된 인증서에 추가됩니다.

     이러한 확장은 인증서에 포함된 키의 용도를 정의합니다.

     > 인증서에 이러한 확장자가 포함되어 있을 때 이전 클라이언트에 연결 문제가 발생하지 않는 한 이 확인란을 선택된 상태로 둡니다.

8. Generate * 를 선택합니다.
9. [[CLIENT_CERT_DETAILS] 인증서 메타데이터와 인증서 PEM을 표시하려면 * 클라이언트 인증서 세부 정보 * 를 선택합니다.

   > 대화 상자를 닫은 후에는 인증서 개인 키를 볼 수 없습니다. 키를 안전한 위치에 복사하거나 다운로드합니다.

   - 다른 곳에 붙여넣을 인증서 내용을 복사하려면 * 인증서 PEM * 복사 를 선택합니다.
   - 인증서 파일을 저장하려면 * 인증서 다운로드 * 를 선택합니다.

     인증서 파일 이름 및 다운로드 위치를 지정합니다. 파일을 확장자로 저장합니다 `.pem`.

예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

- 다른 곳에 붙여넣을 인증서 개인 키를 복사하려면 * 개인 키 복사 * 를 선택합니다.
- 개인 키를 파일로 저장하려면 * 개인 키 다운로드 * 를 선택합니다.

  개인 키 파일 이름과 다운로드 위치를 지정합니다.

10. Grid Manager에 인증서를 저장하려면 * Create * 를 선택합니다.

    새 인증서가 클라이언트 탭에 나타납니다.

11. 그리드 관리자에서 * 구성 * > * 보안 * > * 인증서 * 를 선택한 다음 * 글로벌 * 탭을 선택합니다.
12. Management Interface certificate * 를 선택합니다.
13. 사용자 정의 인증서 사용 * 을 선택합니다.
14. 에서 certificate.pem 및 private_key.pem 파일을 업로드합니다 클라이언트 인증서 세부 정보입니다 단계. CA 번들을 업로드할 필요가 없습니다.
    a. 인증서 업로드 * 를 선택한 다음 * 계속 * 을 선택합니다.
    b. 각 인증서 파일을 업로드합니다 (`.pem`)를 클릭합니다.
    c. 인증서를 Grid Manager에 저장하려면 * 저장 * 을 선택합니다.

       새 인증서가 관리 인터페이스 인증서 페이지에 나타납니다.

15. 외부 모니터링 툴을 구성합니다Grafana와 같은 기능을 사용할 수 있습니다.

외부 모니터링 툴을 설정한다

단계

1. Grafana와 같은 외부 모니터링 도구에서 다음 설정을 구성합니다.
   a. * 이름 *: 연결 이름을 입력합니다.

      StorageGRID에는 이 정보가 필요하지 않지만 연결을 테스트하려면 이름을 입력해야 합니다.

   b. * URL *: 관리자 노드의 도메인 이름 또는 IP 주소를 입력합니다. HTTPS 및 포트 9091을 지정합니다.

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

   c. TLS 클라이언트 인증 * 및 * CA 인증 * 을 활성화합니다.
   d. TLS/SSL 인증 세부 정보 에서 다음을 복사하여 붙여 넣습니다.
      - CA 인증서** 에 대한 관리 인터페이스 CA 인증서입니다
      - 클라이언트 인증서**
      - 클라이언트 키에 대한 개인 키입니다
   e. * ServerName *: 관리 노드의 도메인 이름을 입력합니다.

      servername은 관리 인터페이스 인증서에 표시된 도메인 이름과 일치해야 합니다.

2. StorageGRID 또는 로컬 파일에서 복사한 인증서 및 개인 키를 저장하고 테스트합니다.

   이제 외부 모니터링 툴을 사용하여 StorageGRID에서 Prometheus 메트릭에 액세스할 수 있습니다.

   메트릭에 대한 자세한 내용은 를 참조하십시오 "StorageGRID 모니터링 지침".

클라이언트 인증서를 편집합니다

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

단계

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

   인증서 만료 날짜 및 Prometheus 액세스 권한이 표에 나열되어 있습니다. 인증서가 곧 만료되거나 이미 만료된 경우 테이블에 메시지가 나타나고 경고가 트리거됩니다.

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 * 를 선택합니다.
6. Grid Manager에 인증서를 저장하려면 * Continue * 를 선택합니다.

   업데이트된 인증서가 클라이언트 탭에 표시됩니다.

새 클라이언트 인증서를 연결합니다

현재 인증서가 만료되면 새 인증서를 업로드할 수 있습니다.

단계

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

   인증서 만료 날짜 및 Prometheus 액세스 권한이 표에 나열되어 있습니다. 인증서가 곧 만료되거나 이미 만료된 경우 테이블에 메시지가 나타나고 경고가 트리거됩니다.

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

인증서를 업로드합니다

인증서 텍스트를 복사하여 다른 곳에 붙여 넣습니다.

a. 인증서 업로드 * 를 선택한 다음 * 계속 * 을 선택합니다.
b. 클라이언트 인증서 이름을 업로드합니다 (`.pem`)를 클릭합니다.

   인증서 메타데이터와 인증서 PEM을 표시하려면 * 클라이언트 인증서 세부 정보 * 를 선택합니다.

   - 인증서 파일을 저장하려면 * 인증서 다운로드 * 를 선택합니다.

     인증서 파일 이름 및 다운로드 위치를 지정합니다. 파일을 확장자로 저장합니다 `.pem`.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

   - 다른 곳에 붙여넣을 인증서 내용을 복사하려면 * 인증서 PEM * 복사 를 선택합니다.
c. Grid Manager에 인증서를 저장하려면 * Create * 를 선택합니다.

   업데이트된 인증서가 클라이언트 탭에 표시됩니다.

인증서를 생성합니다

다른 곳에 붙여 넣을 인증서 텍스트를 생성합니다.

a. 인증서 생성 * 을 선택합니다.
b. 인증서 정보를 지정합니다.

   - * subject * (선택 사항): X.509 주체 또는 인증서 소유자의 고유 이름(DN).
   - 유효한 * 일 수 *: 생성된 인증서가 생성된 시점부터 생성된 유효 일 수입니다.
   - * 키 사용 확장 추가 *: 선택한 경우(기본값 및 권장) 키 사용 및 확장 키 사용 확장이 생성된 인증서에 추가됩니다.

     이러한 확장은 인증서에 포함된 키의 용도를 정의합니다.

     > 인증서에 이러한 확장자가 포함되어 있을 때 이전 클라이언트에 연결 문제가 발생하지 않는 한 이 확인란을 선택된 상태로 둡니다.

c. Generate * 를 선택합니다.
d. 인증서 메타데이터와 인증서 PEM을 표시하려면 * 클라이언트 인증서 세부 정보 * 를 선택합니다.

   > 대화 상자를 닫은 후에는 인증서 개인 키를 볼 수 없습니다. 키를 안전한 위치에 복사하거나 다운로드합니다.

   - 다른 곳에 붙여넣을 인증서 내용을 복사하려면 * 인증서 PEM * 복사 를 선택합니다.
   - 인증서 파일을 저장하려면 * 인증서 다운로드 * 를 선택합니다.

     인증서 파일 이름 및 다운로드 위치를 지정합니다. 파일을 확장자로 저장합니다 `.pem`.

예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

- 다른 곳에 붙여넣을 인증서 개인 키를 복사하려면 * 개인 키 복사 * 를 선택합니다.
- 개인 키를 파일로 저장하려면 * 개인 키 다운로드 * 를 선택합니다.

  개인 키 파일 이름과 다운로드 위치를 지정합니다.

e. Grid Manager에 인증서를 저장하려면 * Create * 를 선택합니다.

새 인증서가 클라이언트 탭에 나타납니다.

클라이언트 인증서를 다운로드하거나 복사합니다

다른 곳에서 사용할 클라이언트 인증서를 다운로드하거나 복사할 수 있습니다.

단계

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

인증서 파일을 다운로드합니다
인증서를 다운로드합니다 `.pem` 파일.

a. 인증서 다운로드 * 를 선택합니다.
b. 인증서 파일 이름 및 다운로드 위치를 지정합니다. 파일을 확장자로 저장합니다 `.pem`.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

인증서를 복사합니다
인증서 텍스트를 복사하여 다른 곳에 붙여 넣습니다.

a. 인증서 PEM 복사 * 를 선택합니다.
b. 복사한 인증서를 텍스트 편집기에 붙여 넣습니다.
c. 텍스트 파일을 확장자로 저장합니다 `.pem`.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

클라이언트 인증서를 제거합니다

더 이상 관리자 클라이언트 인증서가 필요하지 않으면 제거할 수 있습니다.

단계

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

2. 제거할 인증서를 선택합니다.
3. 삭제 * 를 선택한 다음 확인합니다.

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

인증서가 제거된 후에는 인증서를 사용한 클라이언트가 StorageGRID Prometheus 데이터베이스에 액세스하기 위해 새 클라이언트 인증서를 지정해야 합니다.

보안 설정을 구성합니다

TLS 및 SSH 정책을 관리합니다

TLS 및 SSH 정책은 클라이언트 응용 프로그램과 보안 TLS 연결을 설정하고 내부 StorageGRID 서비스에 대한 보안 SSH 연결을 설정하는 데 사용되는 프로토콜과 암호를 결정합니다.

보안 정책은 TLS 및 SSH가 이동 중인 데이터를 암호화하는 방법을 제어합니다. 일반적으로 시스템이 일반 조건 호환이거나 다른 암호를 사용해야 하는 경우가 아니면 최신 호환성(기본값) 정책을 사용합니다.

> 이러한 정책에서 암호를 사용하도록 일부 StorageGRID 서비스가 업데이트되지 않았습니다.

시작하기 전에

- 를 사용하여 그리드 관리자에 로그인했습니다 "지원되는 웹 브라우저".
- 을(를) 보유하고 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 활성 정책은 정책 타일에 녹색 확인 표시로 표시됩니다.

2. 타일을 검토하여 사용 가능한 정책에 대해 알아봅니다.

정책	설명
최신 호환성(기본값)	강력한 암호화가 필요하거나 특별한 요구 사항이 없는 경우 기본 정책을 사용합니다. 이 정책은 대부분의 TLS 및 SSH 클라이언트와 호환됩니다.
레거시 호환성	이전 클라이언트에 대한 추가 호환성 옵션이 필요한 경우 이 정책을 사용합니다. 이 정책의 추가 옵션을 사용하면 최신 호환성 정책보다 보안이 덜 강화될 수 있습니다.
일반 조건	일반 조건 인증이 필요한 경우 이 정책을 사용합니다.
FIPS 엄격한	일반 조건 인증이 필요하고 로드 밸런서 끝점, 테넌트 관리자 및 그리드 관리자에 대한 외부 클라이언트 연결에 NetApp 암호화 보안 모듈 3.0.8을 사용해야 하는 경우 이 정책을 사용합니다. 이 정책을 사용하면 성능이 저하될 수 있습니다. • 참고 *: 이 정책을 선택한 후에는 모든 노드가 있어야 합니다 "롤링 방식으로 재부팅했습니다" NetApp 암호화 보안 모듈 활성화 재부팅을 시작하고 모니터링하려면 * Maintenance * > * Rolling Reboot * 를 사용하십시오.
맞춤형	자신의 암호를 적용해야 하는 경우 사용자 지정 정책을 만듭니다.

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

   정책 타일에서 * 현재 정책 * 옆에 녹색 확인 표시가 나타납니다.

사용자 지정 보안 정책을 만듭니다

사용자 고유의 암호를 적용해야 하는 경우 사용자 지정 정책을 만들 수 있습니다.

단계

1. 만들려는 사용자 지정 정책과 가장 유사한 정책 타일에서 * 세부 정보 보기 * 를 선택합니다.
2. 클립보드로 복사 * 를 선택한 다음 * 취소 * 를 선택합니다.

3. 사용자 정의 정책 * 타일에서 * 구성 및 사용 * 을 선택합니다.
4. 복사한 JSON을 붙여 넣고 필요한 내용을 변경합니다.
5. Use policy * 를 선택합니다.

   사용자 지정 정책 타일의 * 현재 정책 * 옆에 녹색 확인 표시가 나타납니다.

6. 필요에 따라 * 구성 편집 * 을 선택하여 새 사용자 지정 정책을 더 많이 변경합니다.

일시적으로 기본 보안 정책으로 돌아갑니다

사용자 지정 보안 정책을 구성한 경우 구성된 TLS 정책이 과 호환되지 않는 경우 Grid Manager에 로그인하지 못할 수 있습니다 "구성된 서버 인증서입니다".

일시적으로 기본 보안 정책으로 되돌릴 수 있습니다.

단계

1. 관리자 노드에 로그인:
   a. 다음 명령을 입력합니다. `ssh admin@Admin_Node_IP`
   b. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.
   c. 루트로 전환하려면 다음 명령을 입력합니다. `su -`
   d. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.

      루트로 로그인하면 프롬프트가 에서 변경됩니다 `$` 를 선택합니다 `#`.

2. 다음 명령을 실행합니다.

   ```
   restore-default-cipher-configurations
   ```

3. 웹 브라우저에서 동일한 관리 노드의 그리드 관리자에 액세스합니다.
4. 의 단계를 따릅니다 보안 정책을 선택합니다 정책을 다시 구성합니다.

네트워크 및 개체 보안을 구성합니다

네트워크 및 개체 보안을 구성하여 저장된 개체를 암호화하고, 특정 S3 및 Swift 요청을 방지하거나, 스토리지 노드에 대한 클라이언트 연결이 HTTPS 대신 HTTP를 사용하도록 허용할 수 있습니다.

저장된 오브젝트 암호화

저장된 오브젝트 암호화를 통해 S3를 통해 수집된 모든 오브젝트 데이터를 암호화할 수 있습니다. 기본적으로 저장된 개체는 암호화되지 않지만 AES - 128 또는 AES - 256 암호화 알고리즘을 사용하여 개체를 암호화하도록 선택할 수 있습니다. 이 설정을 활성화하면 새로 수집된 모든 객체가 암호화되지만 기존 저장된 객체는 변경되지 않습니다. 암호화를 사용하지 않도록 설정하면 현재 암호화된 개체는 암호화된 상태로 유지되지만 새로 수집된 개체는 암호화되지 않습니다.

저장된 오브젝트 암호화 설정은 버킷 레벨 또는 오브젝트 레벨 암호화로 암호화되지 않은 S3 오브젝트에만 적용됩니다.

StorageGRID 암호화 방법에 대한 자세한 내용은 를 참조하십시오 "StorageGRID 암호화 방법을 검토합니다".

클라이언트 수정을 방지합니다

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

S3 REST API

- DeleteBucket 요청
- 기존 오브젝트의 데이터, 사용자 정의 메타데이터 또는 S3 오브젝트 태그 지정을 수정하는 요청

Swift REST API

- 컨테이너 요청을 삭제합니다
- 기존 객체 수정 요청. 예를 들어, 덮어쓰기, 삭제, 메타데이터 업데이트 등의 작업이 거부됩니다.

스토리지 노드 연결에 대해 **HTTP**를 설정합니다

기본적으로 클라이언트 애플리케이션은 스토리지 노드에 대한 직접 연결에 HTTPS 네트워크 프로토콜을 사용합니다. 비프로덕션 그리드를 테스트할 때와 같이 이러한 연결에 대해 HTTP를 선택적으로 활성화할 수 있습니다.

S3 및 Swift 클라이언트가 스토리지 노드에 직접 HTTP 연결을 해야 하는 경우에만 스토리지 노드 연결에 HTTP를 사용합니다. HTTPS 연결만 사용하는 클라이언트 또는 로드 밸런서 서비스에 연결된 클라이언트(에서 할 수 있기 때문에)에는 이 옵션을 사용할 필요가 없습니다 "각 로드 밸런서 엔드포인트를 구성합니다" HTTP 또는 HTTPS 사용).

을 참조하십시오 "요약: 클라이언트 연결을 위한 IP 주소 및 포트" HTTP 또는 HTTPS를 사용하여 스토리지 노드에 연결할 때 사용하는 S3 및 Swift 포트에 대해 알아봅니다.

옵션을 선택합니다

시작하기 전에

- 를 사용하여 그리드 관리자에 로그인했습니다 "지원되는 웹 브라우저".
- 루트 액세스 권한이 있습니다.

단계

1. 구성 * > * 보안 * > * 보안 설정 * 을 선택합니다.
2. Network and objects * 탭을 선택합니다.
3. 저장된 개체 암호화의 경우 저장된 개체를 암호화하지 않으려면 * 없음 * (기본값) 설정을 사용하거나 * AES-128 * 또는 * AES-256 * 을 선택하여 저장된 개체를 암호화합니다.
4. S3 및 Swift 클라이언트가 특정 요청을 하지 못하게 하려면 * 클라이언트 수정 방지 * 를 선택합니다(선택 사항).

> 이 설정을 변경하면 새 설정을 적용하는 데 약 1분이 걸립니다. 구성된 값이 성능 및 확장을 위해 캐싱됩니다.

5. 클라이언트가 스토리지 노드에 직접 접속하고 HTTP 연결을 사용하려는 경우 선택적으로 * 스토리지 노드 연결에 HTTP 사용 * 을 선택합니다.

> 요청이 암호화되지 않은 상태로 전송되므로 프로덕션 그리드에 대해 HTTP를 설정할 때는 주의해야 합니다.

6. 저장 * 을 선택합니다.

인터페이스 보안 설정을 변경합니다

인터페이스 보안 설정을 사용하면 사용자가 지정된 시간 이상 비활성 상태인 경우 로그아웃할지 여부 및 스택 추적이 API 오류 응답에 포함되는지 여부를 제어할 수 있습니다.

시작하기 전에

- 를 사용하여 그리드 관리자에 로그인했습니다 "지원되는 웹 브라우저".
- 있습니다 "루트 액세스 권한".

이 작업에 대해

보안 설정 * 페이지에는 * 브라우저 비활성 시간 제한 * 및 * 관리 API 스택 추적 * 설정이 포함됩니다.

브라우저 비활성 시간 초과

사용자가 로그아웃되기 전까지 사용자의 브라우저가 비활성화될 수 있는 시간을 나타냅니다. 기본값은 15분입니다.

브라우저 비활성 시간 초과는 다음과 같은 방법으로 제어됩니다.

- 시스템 보안을 위해 포함되어 있는 별도의 구성 불가능한 StorageGRID 타이머입니다. 각 사용자의 인증 토큰은 사용자가 로그인한 후 16시간 후에 만료됩니다. 사용자의 인증이 만료되면 브라우저 비활성 시간 초과가 비활성화되거나 브라우저 시간 초과 값에 도달하지 않은 경우에도 해당 사용자는 자동으로 로그아웃됩니다. 토큰을 갱신하려면 사용자가 다시 로그인해야 합니다.
- StorageGRID에 대해 SSO(Single Sign-On)가 활성화된 경우 ID 공급자에 대한 시간 제한 설정입니다.

  SSO가 활성화되어 있고 사용자의 브라우저가 시간 초과되면 사용자는 SSO 자격 증명을 다시 입력하여 StorageGRID에 다시 액세스해야 합니다. 을 참조하십시오 "Single Sign-On 구성".

관리 **API** 스택 추적

Grid Manager 및 Tenant Manager API 오류 응답에서 스택 추적이 반환되는지 여부를 제어합니다.

이 옵션은 기본적으로 비활성화되어 있지만 테스트 환경에서 이 기능을 사용할 수 있습니다. 일반적으로 API 오류가 발생할 때 내부 소프트웨어 세부 정보가 노출되지 않도록 프로덕션 환경에서 스택 추적을 비활성화해야 합니다.

단계

1. 구성 * > * 보안 * > * 보안 설정 * 을 선택합니다.
2. 인터페이스 * 탭을 선택합니다.
3. 브라우저 비활성 시간 초과 설정을 변경하려면:
   a. 아코디언을 확장합니다.
   b. 제한 시간을 변경하려면 60초에서 7일 사이의 값을 지정합니다. 기본 시간 제한은 15분입니다.
   c. 이 기능을 비활성화하려면 확인란을 선택 취소합니다.
   d. 저장 * 을 선택합니다.

      새 설정은 현재 로그인한 사용자에게는 영향을 주지 않습니다. 사용자는 다시 로그인하거나 브라우저를 새로 고쳐야 새 시간 초과 설정을 적용할 수 있습니다.
4. 관리 API 스택 추적 설정을 변경하려면 다음을 수행합니다.
   a. 아코디언을 확장합니다.
   b. Grid Manager 및 Tenant Manager API 오류 응답에서 스택 추적을 반환하려면 확인란을 선택합니다.

      API 오류가 발생할 때 내부 소프트웨어 세부 정보가 노출되지 않도록 프로덕션 환경에서 스택 추적을 비활성화하십시오.

   c. 저장 * 을 선택합니다.

키 관리 서버를 구성합니다

키 관리 서버 구성: 개요

특별히 구성된 어플라이언스 노드의 데이터를 보호하도록 하나 이상의 외부 키 관리 서버(KMS)를 구성할 수 있습니다.

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

KMS(키 관리 서버**)**란 무엇입니까**?**

KMS(Key Management Server)는 KMIP(Key Management Interoperability Protocol)를 사용하여 관련 StorageGRID 사이트의 StorageGRID 어플라이언스 노드에 암호화 키를 제공하는 외부 타사 시스템입니다.

하나 이상의 키 관리 서버를 사용하여 설치 중에 * 노드 암호화 * 설정이 활성화된 모든 StorageGRID 어플라이언스 노드에 대한 노드 암호화 키를 관리할 수 있습니다. 이러한 어플라이언스 노드에 키 관리 서버를 사용하면 어플라이언스를 데이터 센터에서 제거하더라도 데이터를 보호할 수 있습니다. 어플라이언스 볼륨이 암호화된 후에는 노드에서 KMS와 통신할 수 없는 한 어플라이언스의 데이터에 액세스할 수 없습니다.

> StorageGRID는 어플라이언스 노드를 암호화하고 해독하는 데 사용되는 외부 키를 생성하거나 관리하지 않습니다. 외부 키 관리 서버를 사용하여 StorageGRID 데이터를 보호하려는 경우 해당 서버를 설정하는 방법을 이해하고 암호화 키를 관리하는 방법을 이해해야 합니다. 주요 관리 작업을 수행하는 것은 이 지침의 범위를 벗어납니다. 도움이 필요한 경우 키 관리 서버 설명서를 참조하거나 기술 지원 부서에 문의하십시오.

KMS 및 어플라이언스 구성 개요

KMS(키 관리 서버)를 사용하여 어플라이언스 노드에서 StorageGRID 데이터를 보호하려면 먼저 하나 이상의 KMS 서버 설정 및 어플라이언스 노드에 대한 노드 암호화 활성화라는 두 가지 구성 작업을 완료해야 합니다. 이러한 두 구성 작업이 완료되면 키 관리 프로세스가 자동으로 수행됩니다.

이 순서도는 KMS를 사용하여 어플라이언스 노드의 StorageGRID 데이터를 보호하는 상위 단계를 보여 줍니다.

순서도는 KMS 설정 및 어플라이언스 설정이 병렬로 이루어지지만, 요구 사항에 따라 새 어플라이언스 노드에 대한 노드 암호화를 활성화하기 전이나 후에 키 관리 서버를 설정할 수 있습니다.

KMS(키 관리 서버**)** 설정

키 관리 서버를 설정하는 단계는 다음과 같습니다.

단계	을 참조하십시오
KMS 소프트웨어에 액세스하고 각 KMS 또는 KMS 클러스터에 StorageGRID용 클라이언트를 추가합니다.	"KMS에서 StorageGRID를 클라이언트로 구성합니다"
KMS에서 StorageGRID 클라이언트에 필요한 정보를 얻습니다.	"KMS에서 StorageGRID를 클라이언트로 구성합니다"
KMS를 Grid Manager에 추가하고, 단일 사이트 또는 기본 사이트 그룹에 할당하고, 필요한 인증서를 업로드하고, KMS 구성을 저장합니다.	"KMS(키 관리 서버) 추가"

제품을 설치합니다

KMS 사용을 위해 어플라이언스 노드를 설정하는 단계는 다음과 같습니다.

1. 어플라이언스 설치 시 하드웨어 구성 단계에서 StorageGRID 어플라이언스 설치 프로그램을 사용하여 어플라이언스에 대한 * 노드 암호화 * 설정을 활성화합니다.

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

2. StorageGRID 어플라이언스 설치 프로그램을 실행합니다. 설치 중에 각 어플라이언스 볼륨에 DEK(임의 데이터 암호화 키)가 다음과 같이 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 연결할 수 있을 때까지 DEK를 암호화하는 임시 키입니다.

3. 어플라이언스 노드를 StorageGRID에 추가합니다.

을 참조하십시오 "노드 암호화를 설정합니다" 를 참조하십시오.

키 관리 암호화 프로세스(자동으로 발생)

키 관리 암호화에는 자동으로 수행되는 다음과 같은 높은 수준의 단계가 포함됩니다.

1. 노드 암호화가 활성화된 어플라이언스를 그리드에 설치하는 경우 StorageGRID는 새 노드가 포함된 사이트에 대해 KMS 구성이 존재하는지 여부를 결정합니다.
   - KMS가 사이트에 대해 이미 구성된 경우 어플라이언스는 KMS 구성을 받습니다.
   - KMS가 사이트에 대해 아직 구성되지 않은 경우 사이트에 대해 KMS를 구성하고 어플라이언스가 KMS 구성을 받을 때까지 어플라이언스의 데이터는 임시 KK에 의해 계속 암호화됩니다.
2. 이 어플라이언스는 KMS 구성을 사용하여 KMS에 연결하고 암호화 키를 요청합니다.
3. KMS는 암호화 키를 어플라이언스에 보냅니다. KMS의 새 키는 임시 KEK를 대체하며, 이제 어플라이언스 볼륨의 DEK를 암호화하고 해독하는 데 사용됩니다.

> 암호화된 어플라이언스 노드가 구성된 KMS에 연결하기 전에 존재하는 모든 데이터는 임시 키로 암호화됩니다. 그러나 임시 키를 KMS 암호화 키로 교체할 때까지 어플라이언스 볼륨을 데이터 센터에서 제거하지 않도록 보호해서는 안 됩니다.

4. 제품의 전원이 켜져 있거나 재부팅된 경우 KMS에 다시 연결하여 키를 요청합니다. 휘발성 메모리에 저장된 키는 전원 손실이나 재부팅 시에도 계속 유지될 수 없습니다.

키 관리 서버 사용에 대한 고려 사항 및 요구 사항

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

지원되는 **KMIP** 버전은 무엇입니까**?**

StorageGRID는 KMIP 버전 1.4를 지원합니다.

"키 관리 상호 운용성 프로토콜 사양 버전 1.4"

네트워크 고려 사항은 무엇입니까**?**

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

노드 암호화를 사용하는 각 어플라이언스 노드에서 사이트에 대해 구성한 KMS 또는 KMS 클러스터에 대한 네트워크 액세스 권한이 있는지 확인해야 합니다.

지원되는 **TLS** 버전은 무엇입니까**?**

어플라이언스 노드와 구성된 KMS 간의 통신은 보안 TLS 연결을 사용합니다. StorageGRID는 KMS가 지원하는

내용과 KMS 클러스터에 KMIP를 연결할 때 TLS 1.2 또는 TLS 1.3 프로토콜을 지원할 수 있습니다 "TLS 및 SSH 정책" 를 사용하고 있습니다.

StorageGRID는 연결을 만들 때 KMS와 프로토콜 및 암호(TLS 1.2) 또는 암호 그룹(TLS 1.3)을 협상합니다. 사용할 수 있는 프로토콜 버전 및 암호화/암호 그룹을 보려면 를 참조하십시오 `tlsOutbound` 그리드의 활성 TLS 및 SSH 정책 섹션(* 구성 * > * 보안 * * * * 보안 설정 *)

어떤 어플라이언스가 지원됩니까?

KMS(키 관리 서버)를 사용하여 * 노드 암호화 * 설정이 활성화된 그리드에 있는 StorageGRID 어플라이언스의 암호화 키를 관리할 수 있습니다. 이 설정은 StorageGRID 어플라이언스 설치 프로그램을 사용하여 어플라이언스 설치의 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 KMS for StorageGRID 어플라이언스 및 어플라이언스 노드를 사용할 수 있습니다.

다음을 포함하여 소프트웨어 기반(비어플라이언스) 노드에 대해 구성된 KMS를 사용할 수 없습니다.

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

이러한 다른 플랫폼에 구축된 노드는 StorageGRID 외부의 데이터 저장소 또는 디스크 레벨에서 암호화를 사용할 수 있습니다.

키 관리 서버는 언제 구성해야 합니까?

새 설치의 경우 일반적으로 테넌트를 생성하기 전에 Grid Manager에서 하나 이상의 키 관리 서버를 설정해야 합니다. 이 순서를 사용하면 오브젝트 데이터가 노드에 저장되기 전에 노드가 보호됩니다.

어플라이언스 노드를 설치하기 전이나 설치한 후에 Grid Manager에서 키 관리 서버를 구성할 수 있습니다.

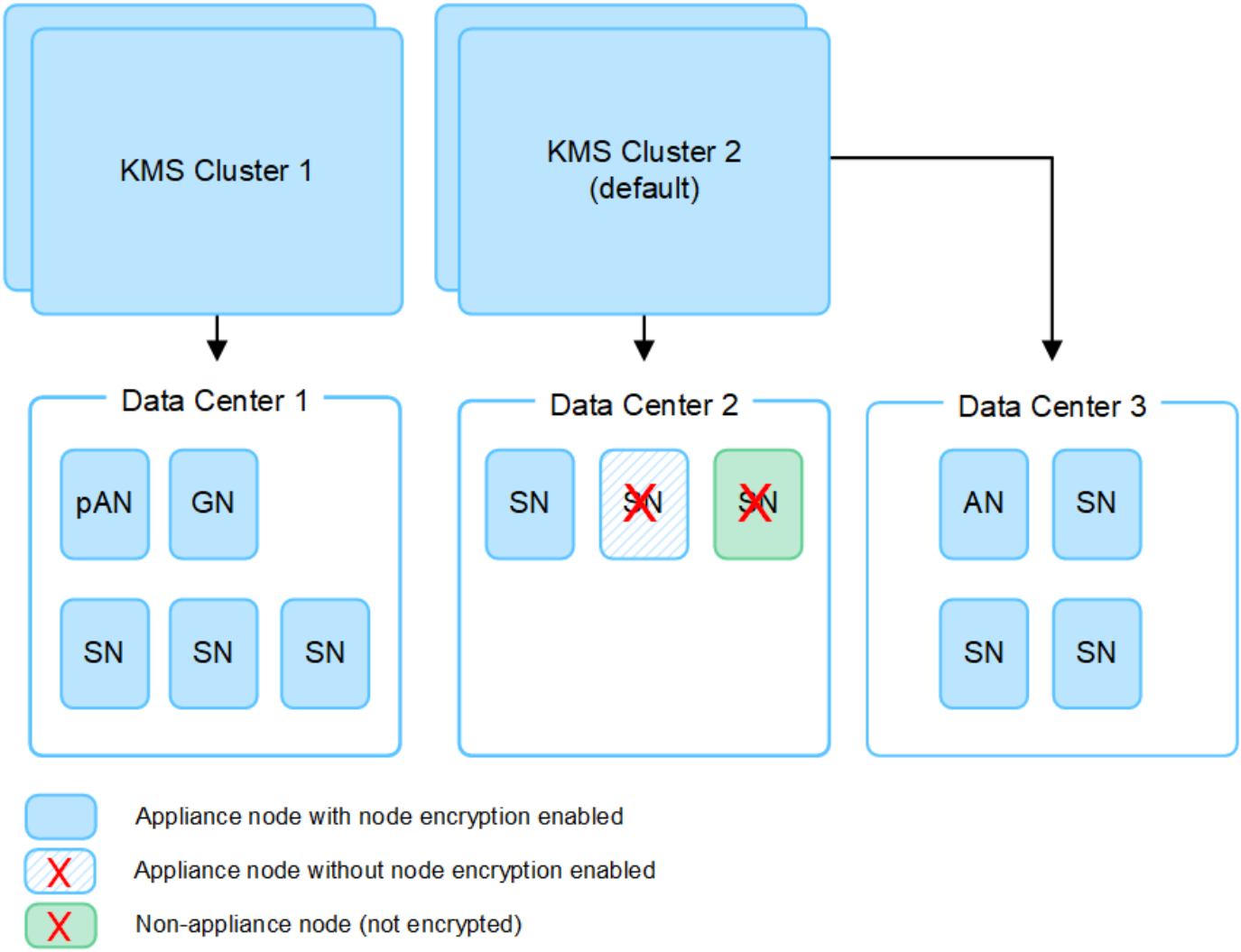
몇 개의 키 관리 서버가 필요합니까?

StorageGRID 시스템의 어플라이언스 노드에 암호화 키를 제공하도록 하나 이상의 외부 키 관리 서버를 구성할 수 있습니다. 각 KMS는 단일 사이트 또는 사이트 그룹의 StorageGRID 어플라이언스 노드에 단일 암호화 키를 제공합니다.

StorageGRID는 KMS 클러스터 사용을 지원합니다. 각 KMS 클러스터에는 구성 설정 및 암호화 키를 공유하는 여러 개의 복제된 키 관리 서버가 포함되어 있습니다. KMS 클러스터를 사용하여 키 관리를 수행하는 것이 좋습니다. KMS 클러스터는 고가용성 구성의 장애 조치 기능을 개선하므로 이 기능을 사용하는 것이 좋습니다.

예를 들어, StorageGRID 시스템에 데이터 센터 사이트가 3개 있다고 가정합니다. 다른 모든 사이트의 모든 어플라이언스 노드에 키를 제공하도록 하나의 KMS 클러스터를 구성하여 Data Center 1의 모든 어플라이언스 노드와 두 번째 KMS 클러스터에 키를 제공할 수 있습니다. 두 번째 KMS 클러스터를 추가하면 데이터 센터 2 및 데이터 센터 3에 대한 기본 KMS를 구성할 수 있습니다.

비어플라이언스 노드나 설치 중에 * 노드 암호화 * 설정이 활성화되지 않은 어플라이언스 노드에 대해 KMS를 사용할 수 없습니다.



키를 회전하면 어떻게 됩니까?

보안 모범 사례로서 정기적으로 수행해야 합니다 "암호화 키를 회전합니다" 구성된 각 KMS에서 사용됩니다.

새 키 버전을 사용할 수 있는 경우:

- KMS와 관련된 사이트 또는 사이트의 암호화된 어플라이언스 노드에 자동으로 배포됩니다. 키는 회전된 후 1시간 내에 분포되어야 합니다.
- 새 키 버전이 배포될 때 암호화된 어플라이언스 노드가 오프라인이면 재부팅되는 즉시 새 키가 노드에 수신됩니다.
- 새 키 버전을 사용하여 어플라이언스 볼륨을 암호화할 수 없는 경우 어플라이언스 노드에 대해 * KMS 암호화 키 회전 실패 * 경고가 트리거됩니다. 이 경고를 해결하려면 기술 지원 부서에 문의해야 할 수도 있습니다.

어플라이언스 노드를 암호화한 후 다시 사용할 수 있습니까?

암호화된 어플라이언스를 다른 StorageGRID 시스템에 설치해야 하는 경우 오브젝트 데이터를 다른 노드로 이동하려면 먼저 그리드 노드를 해제해야 합니다. 그런 다음 StorageGRID 어플라이언스 설치 프로그램을 사용하여 에 연결할 수 있습니다 "KMS 구성을 지웁니다". KMS 구성을 지우면 * 노드 암호화 * 설정이 비활성화되고 StorageGRID 사이트에 대한 어플라이언스 노드와 KMS 구성 간의 연결이 제거됩니다.

KMS 암호화 키에 액세스할 수 없으므로 어플라이언스에 남아 있는 데이터는 더 이상 액세스할 수 없으며 영구적으로 잠깁니다.

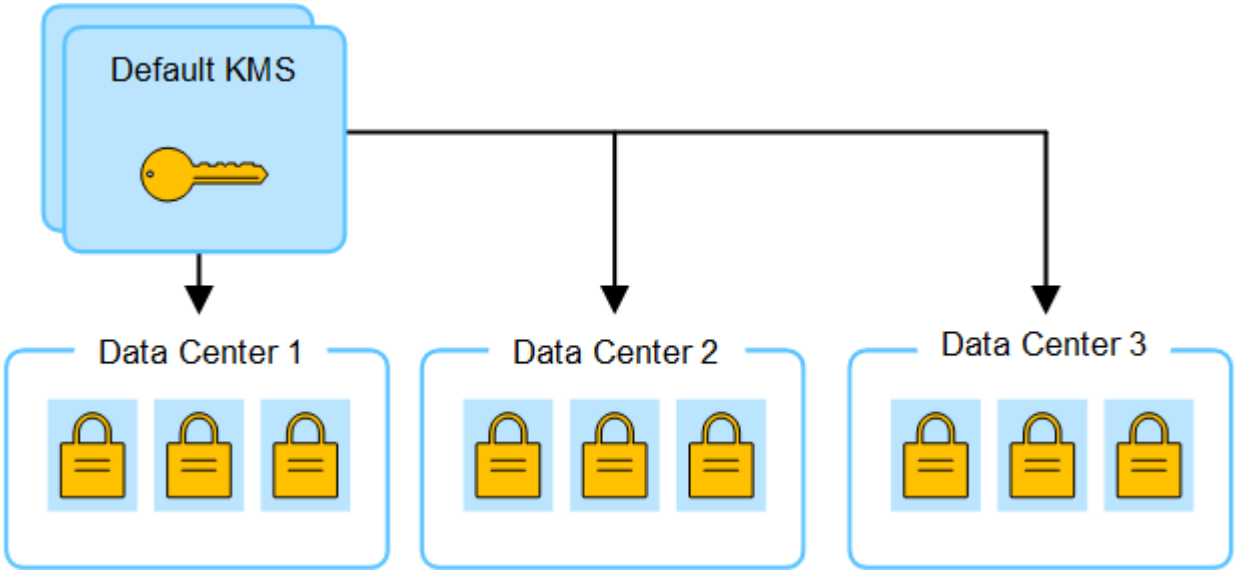
사이트의 **KMS**를 변경할 때의 고려 사항

각 KMS(Key Management Server) 또는 KMS 클러스터는 단일 사이트 또는 사이트 그룹의 모든 어플라이언스 노드에 암호화 키를 제공합니다. 사이트에 사용되는 KMS를 변경해야 하는 경우 암호화 키를 한 KMS에서 다른 KMS로 복사해야 할 수 있습니다.

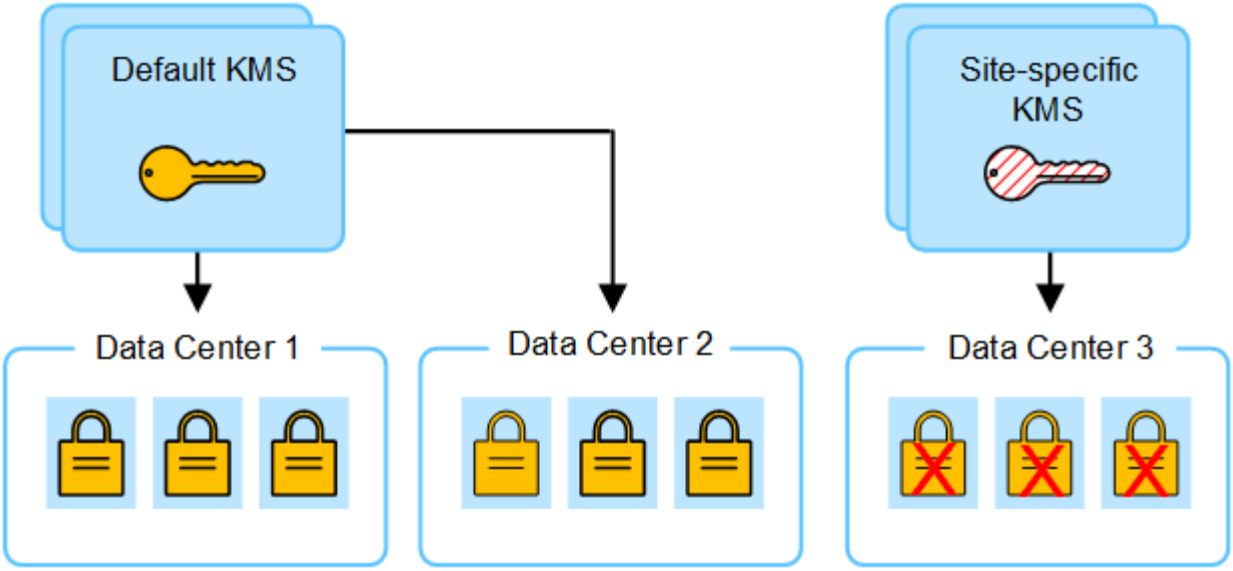
사이트에 사용되는 KMS를 변경하는 경우 해당 사이트에서 이전에 암호화된 어플라이언스 노드를 새 KMS에 저장된 키를 사용하여 해독할 수 있는지 확인해야 합니다. 경우에 따라 기존 KMS에서 새 KMS로 최신 버전의 암호화 키를 복사해야 할 수도 있습니다. KMS가 사이트에서 암호화된 어플라이언스 노드를 해독할 수 있는 올바른 키를 가지고 있는지 확인해야 합니다.

예를 들면 다음과 같습니다.

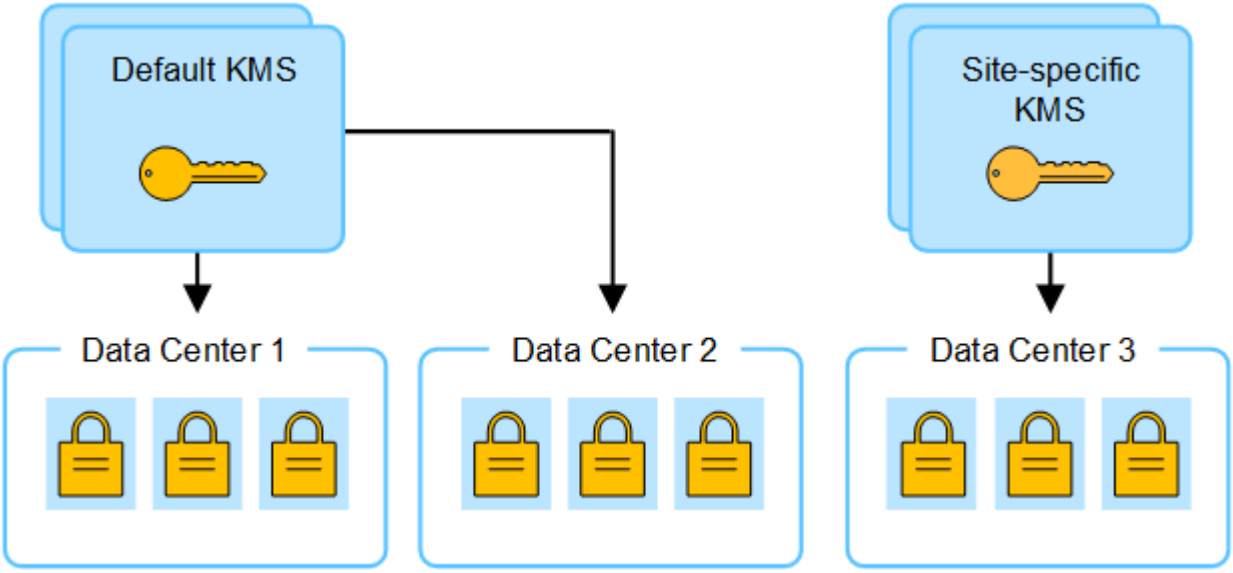
1. 처음에는 전용 KMS가 없는 모든 사이트에 적용되는 기본 KMS를 구성합니다.
2. KMS가 저장되면 * 노드 암호화 * 설정이 활성화된 모든 어플라이언스 노드가 KMS에 연결하여 암호화 키를 요청합니다. 이 키는 모든 사이트에서 어플라이언스 노드를 암호화하는 데 사용됩니다. 이러한 어플라이언스의 암호를 해독하는 데에도 이 동일한 키를 사용해야 합니다.



3. 한 사이트에 대해 사이트별 KMS를 추가하기로 결정합니다(그림의 데이터 센터 3). 그러나 어플라이언스 노드는 이미 암호화되어 있으므로 사이트별 KMS에 대한 구성을 저장하려고 하면 유효성 검사 오류가 발생합니다. 이 오류는 사이트별 KMS에 해당 사이트의 노드를 해독할 수 있는 올바른 키가 없기 때문에 발생합니다.



4. 이 문제를 해결하려면 기본 KMS에서 새 KMS로 암호화 키의 현재 버전을 복사합니다. (원칙적으로 원래 키를 동일한 별칭이 있는 새 키에 복사합니다. 원래 키는 새 키의 이전 버전이 됩니다.) 이제 사이트별 KMS에는 데이터 센터 3의 어플라이언스 노드를 해독하는 올바른 키가 있으므로 StorageGRID에 저장할 수 있습니다.



사이트에 사용되는 **KMS**를 변경하는 사용 사례

이 표에는 사이트에 대한 KMS를 변경하는 가장 일반적인 경우를 위한 필수 단계가 요약되어 있습니다.

사이트의 **KMS**를 변경하는 사용 사례	필요한 단계
하나 이상의 사이트별 KMS 항목이 있으며 이 중 하나를 기본 KMS로 사용하려고 합니다.	사이트별 KMS를 편집합니다. [에 대한 키 관리] 필드에서 * 다른 KMS에 의해 관리되지 않는 사이트(기본 KMS) * 를 선택합니다. 이제 사이트별 KMS가 기본 KMS로 사용됩니다. 이 내용은 전용 KMS가 없는 사이트에 적용됩니다. "KMS(키 관리 서버) 편집"

사이트의 **KMS**를 변경하는 사용 사례	필요한 단계
기본 KMS가 있으며 확장 시 새 사이트를 추가합니다. 새 사이트에 기본 KMS를 사용하지 않으려는 경우	1. 새 사이트의 어플라이언스 노드가 기본 KMS에 의해 이미 암호화된 경우 KMS 소프트웨어를 사용하여 기본 KMS에서 새 KMS로 암호화 키의 현재 버전을 복사합니다. 2. Grid Manager를 사용하여 새 KMS를 추가하고 사이트를 선택합니다. "KMS(키 관리 서버) 추가"
사이트의 KMS가 다른 서버를 사용하도록 해야 합니다.	1. 사이트의 어플라이언스 노드가 기존 KMS에 의해 이미 암호화된 경우 KMS 소프트웨어를 사용하여 기존 KMS에서 새 KMS로 암호화 키의 현재 버전을 복사합니다. 2. Grid Manager를 사용하여 기존 KMS 구성을 편집하고 새 호스트 이름 또는 IP 주소를 입력합니다. "KMS(키 관리 서버) 추가"

KMS에서 **StorageGRID**를 클라이언트로 구성합니다

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

> 이러한 지침은 Thales CipherTrust Manager 및 Hashicorp Vault에 적용됩니다. 지원되는 제품 및 버전 목록을 보려면 을 사용합니다 "NetApp 상호 운용성 매트릭스 툴(IMT)".

단계

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

   각 KMS는 단일 사이트 또는 사이트 그룹에서 StorageGRID 어플라이언스 노드에 대한 단일 암호화 키를 관리합니다.

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

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

   - StorageGRID에서 키를 생성하도록 합니다. 테스트 후 저장하면 메시지가 표시됩니다 "클라이언트 인증서를 업로드하는 중입니다".
3. 각 KMS 또는 KMS 클러스터에 대해 다음 정보를 기록합니다.

   KMS를 StorageGRID에 추가할 때 다음 정보가 필요합니다.

   - 각 서버의 호스트 이름 또는 IP 주소입니다.
   - KMS에서 KMIP 포트를 사용합니다.
   - KMS의 암호화 키에 대한 키 별칭입니다.
4. 각 KMS 또는 KMS 클러스터에 대해 CA(인증 기관)가 서명한 서버 인증서 또는 인증서 체인 순서에 따라 연결된

PEM 인코딩된 CA 인증서 파일이 들어 있는 인증서 번들을 받습니다.

서버 인증서를 사용하면 외부 KMS가 StorageGRID에 자신을 인증할 수 있습니다.

- 인증서는 PEM(Privacy Enhanced Mail) Base-64로 인코딩된 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, 일반적으로 포트 5696을 사용합니다.

5. 외부 KMS 및 클라이언트 인증서의 개인 키로 StorageGRID에 발급된 공용 클라이언트 인증서를 얻습니다.

   클라이언트 인증서를 사용하면 StorageGRID가 KMS에 대한 인증을 받을 수 있습니다.

KMS(키 관리 서버) 추가

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

시작하기 전에

- 을(를) 검토했습니다 "키 관리 서버 사용에 대한 고려 사항 및 요구 사항".
- 있습니다 "KMS에서 StorageGRID를 클라이언트로 구성했습니다"또한 각 KMS 또는 KMS 클러스터에 필요한 정보가 있습니다.
- 를 사용하여 그리드 관리자에 로그인했습니다 "지원되는 웹 브라우저".
- 을(를) 보유하고 있습니다 "루트 액세스 권한".

이 작업에 대해

가능하면 다른 KMS에서 관리하지 않는 모든 사이트에 적용되는 기본 KMS를 구성하기 전에 사이트별 키 관리 서버를 구성하십시오. 기본 KMS를 먼저 만들면 그리드의 모든 노드 암호화 어플라이언스는 기본 KMS로 암호화됩니다. 나중에 사이트별 KMS를 만들려면 먼저 기본 KMS에서 새 KMS로 암호화 키의 현재 버전을 복사해야 합니다. 을 참조하십시오 "사이트의 KMS를 변경할 때의 고려 사항" 를 참조하십시오.

1단계**: KMS** 세부 정보

KMS(Key Management Server 추가) 마법사의 1단계(KMS 세부 정보)에서 KMS 또는 KMS 클러스터에 대한 세부 정보를 제공합니다.

단계

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

   구성 세부 정보 탭이 선택된 키 관리 서버 페이지가 나타납니다.

2. Create * 를 선택합니다.

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

3. KMS에 구성한 KMS 및 StorageGRID 클라이언트에 대한 다음 정보를 입력합니다.

필드에 입력합니다	설명
KMS 이름	이 KMS를 식별하는 데 도움이 되는 설명 이름입니다. 1자에서 64자 사이여야 합니다.
키 이름	KMS에서 StorageGRID 클라이언트에 대한 정확한 키 별칭입니다. 1자에서 255자 사이여야 합니다. • 참고 *: KMS 제품을 사용하여 키를 만들지 않은 경우 StorageGRID에서 키를 만들라는 메시지가 표시됩니다.
의 키를 관리합니다	이 KMS와 관련된 StorageGRID 사이트입니다. 가능하면 다른 KMS에서 관리하지 않는 모든 사이트에 적용되는 기본 KMS를 구성하기 전에 사이트별 키 관리 서버를 구성해야 합니다. • 이 KMS가 특정 사이트의 어플라이언스 노드에 대한 암호화 키를 관리하는 경우 사이트를 선택합니다. • 전용 KMS가 없는 사이트와 후속 확장에 추가한 사이트에 적용되는 기본 KMS를 구성하려면 * 다른 KMS(기본 KMS)에서 관리하지 않는 사이트 * 를 선택합니다. ◦ 참고:* KMS 구성을 저장하면 검증 오류가 발생합니다. KMS 기본 KMS에 의해 이전에 암호화된 사이트를 선택했지만 새 KMS에 원본 암호화 키의 현재 버전을 제공하지 않은 경우 KMS 구성을 저장하면 오류가 발생합니다.
포트	KMS 서버가 KMIP(Key Management Interoperability Protocol) 통신에 사용하는 포트입니다. 기본값은 5696으로, KMIP 표준 포트입니다.
호스트 이름	KMS의 정규화된 도메인 이름 또는 IP 주소입니다. • 참고: * 서버 인증서의 주체 대체 이름(SAN) 필드에는 여기에 입력한 FQDN 또는 IP 주소가 포함되어야 합니다. 그렇지 않으면 StorageGRID는 KMS 또는 KMS 클러스터의 모든 서버에 연결할 수 없습니다.

4. KMS 클러스터를 구성하는 경우 * 다른 호스트 이름 추가 * 를 선택하여 클러스터의 각 서버에 대한 호스트 이름을 추가합니다.
5. Continue * 를 선택합니다.

2단계**:** 서버 인증서를 업로드합니다

키 관리 서버 추가 마법사의 2단계(서버 인증서 업로드)에서 KMS에 대한 서버 인증서(또는 인증서 번들)를 업로드합니다. 서버 인증서를 사용하면 외부 KMS가 StorageGRID에 자신을 인증할 수 있습니다.

단계

1. 2단계(서버 인증서 업로드) * 에서 저장된 서버 인증서 또는 인증서 번들의 위치를 찾습니다.

2. 인증서 파일을 업로드합니다.

   서버 인증서 메타데이터가 나타납니다.

   > 인증서 번들을 업로드한 경우 각 인증서의 메타데이터가 해당 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 사용하면 StorageGRID가 KMS에 대한 인증을 받을 수 있습니다.

단계

1. 3단계(클라이언트 인증서 업로드) * 에서 클라이언트 인증서 위치를 찾습니다.
2. 클라이언트 인증서 파일을 업로드합니다.

   클라이언트 인증서 메타데이터가 나타납니다.

3. 클라이언트 인증서의 개인 키 위치를 찾습니다.
4. 개인 키 파일을 업로드합니다.
5. 테스트 및 저장 * 을 선택합니다.

   키가 없으면 StorageGRID에서 키를 만들라는 메시지가 표시됩니다.

   키 관리 서버와 어플라이언스 노드 간의 연결은 테스트를 거칩니다. 모든 연결이 올바르고 KMS에서 올바른 키를 찾으면 키 관리 서버 페이지의 표에 새 키 관리 서버가 추가됩니다.

   > KMS를 추가한 직후 키 관리 서버 페이지의 인증서 상태는 알 수 없음으로 표시됩니다. 각 인증서의 실제 상태를 가져오는 데 30분 정도 StorageGRID 걸릴 수 있습니다. 현재 상태를 보려면 웹 브라우저를 새로 고쳐야 합니다.

6. 테스트 및 저장 * 을 선택할 때 오류 메시지가 나타나면 메시지 세부 정보를 검토한 다음 * 확인 * 을 선택합니다.

   예를 들어 연결 테스트에 실패한 경우 422:처리할 수 없는 엔터티 오류가 발생할 수 있습니다.

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

   > 강제 저장 * 을 선택하면 KMS 구성이 저장되지만 각 제품에서 해당 KMS로의 외부 연결은 테스트되지 않습니다. 구성에 문제가 있을 경우 해당 사이트에서 노드 암호화가 활성화된 어플라이언스 노드를 재부팅하지 못할 수 있습니다. 문제가 해결될 때까지 데이터에 액세스하지 못할 수 있습니다.

8. 확인 경고를 검토하고 구성을 강제 저장하려면 * OK * 를 선택합니다.

   KMS 구성은 저장되지만 KMS에 대한 연결은 테스트되지 않습니다.

KMS를 관리합니다

KMS(키 관리 서버) 관리에는 세부 정보 보기 또는 편집, 인증서 관리, 암호화된 노드 보기, KMS 제거 등이 포함됩니다.

시작하기 전에

- 를 사용하여 그리드 관리자에 로그인했습니다 "지원되는 웹 브라우저".
- 을(를) 보유하고 있습니다 "필수 액세스 권한".

KMS 세부 정보 보기

키 세부 정보, 서버 및 클라이언트 인증서의 현재 상태 등 StorageGRID 시스템의 각 KMS(키 관리 서버)에 대한 정보를 볼 수 있습니다.

단계

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

   키 관리 서버 페이지가 나타나고 다음 정보가 표시됩니다.

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

2. 특정 KMS에 대한 세부 정보를 보고 해당 KMS에 대한 작업을 수행하려면 KMS의 이름을 선택합니다. KMS의 세부 정보 페이지에는 다음 정보가 나열됩니다.

필드에 입력합니다	설명
의 키를 관리합니다	KMS와 관련된 StorageGRID 사이트 이 필드에는 특정 StorageGRID 사이트 또는 다른 KMS(기본 KMS)가 관리하지 않는 사이트의 이름이 표시됩니다.*
호스트 이름	KMS의 정규화된 도메인 이름 또는 IP 주소입니다. 두 개의 키 관리 서버로 구성된 클러스터가 있는 경우 두 서버의 정규화된 도메인 이름 또는 IP 주소가 나열됩니다. 클러스터에 키 관리 서버가 두 개 이상 있는 경우 첫 번째 KMS의 정규화된 도메인 이름 또는 IP 주소가 클러스터에 있는 추가 키 관리 서버의 수와 함께 나열됩니다. 예를 들면 다음과 같습니다. `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 선택합니다.

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

탭을 클릭합니다	필드에 입력합니다	설명
키 세부 정보	키 이름	KMS에서 StorageGRID 클라이언트의 키 별칭입니다.
키 UID	최신 버전의 키에 대한 고유 식별자입니다.	마지막 수정
키의 최신 버전 날짜 및 시간입니다.	서버 인증서	메타데이터
인증서의 메타데이터(예: 일련 번호, 만료 날짜 및 시간, 인증서 PEM)	인증서 PEM	인증서에 대한 PEM(개인 정보 보호 강화 메일) 파일의 내용입니다.
클라이언트 인증서	메타데이터	인증서의 메타데이터(예: 일련 번호, 만료 날짜 및 시간, 인증서 PEM)

4.] 조직의 보안 관행에 필요한 만큼 * Rotate key * 를 선택하거나 KMS 소프트웨어를 사용하여 새 버전의 키를 만듭니다.

   키 회전이 성공하면 키 UID 및 마지막으로 수정된 필드가 업데이트됩니다.

> KMS 소프트웨어를 사용하여 암호화 키를 회전하는 경우 마지막으로 사용한 키 버전에서 동일한 키의 새 버전으로 회전합니다. 완전히 다른 키로 회전하지 마십시오.
>
> KMS의 키 이름(별칭)을 변경하여 키를 회전하려고 하지 마십시오. StorageGRID를 사용하려면 KMS에서 동일한 키 별칭을 사용하여 이전에 사용한 모든 키 버전과 향후 모든 키 버전에 액세스할 수 있어야 합니다. 구성된 KMS의 키 별칭을 변경하면 StorageGRID에서 데이터의 암호를 해독하지 못할 수 있습니다.

인증서를 관리합니다

모든 서버 또는 클라이언트 인증서 문제를 즉시 해결합니다. 가능하면 만료되기 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 KMS에 대한 인증서 만료 값을 확인합니다.
3. KMS에 대한 인증서 만료가 알 수 없는 경우 최대 30분 정도 기다린 다음 웹 브라우저를 새로 고칩니다.
4. 인증서 만료 열에 인증서가 만료되었거나 만료가 임박했음을 나타내는 경우 KMS를 선택하여 KMS 세부 정보 페이지로 이동합니다.
   a. 서버 인증서 * 를 선택하고 "만료 날짜" 필드에 대한 값을 확인합니다.

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

c. 이 하위 단계를 반복하고 서버 인증서 대신 * 클라이언트 인증서 * 를 선택합니다.

5. KMS CA 인증서 만료 *, * KMS 클라이언트 인증서 만료 * 및 * KMS 서버 인증서 만료 * 알림이 트리거되면 각 경고에 대한 설명을 기록하고 권장 조치를 수행합니다.

> 인증서 만료에 대한 업데이트를 받는 데 30분 정도 걸릴 수 StorageGRID 있습니다. 현재 값을 보려면 웹 브라우저를 새로 고치십시오.

암호화된 노드를 봅니다

노드 암호화 * 설정이 활성화된 StorageGRID 시스템의 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 모든 키 관리 서버가 표시됩니다.

2. 페이지 상단에서 * 암호화된 노드 * 탭을 선택합니다.

   암호화된 노드 탭에는 * 노드 암호화 * 설정이 활성화된 StorageGRID 시스템의 어플라이언스 노드가 나열됩니다.

3. 각 어플라이언스 노드에 대해 표의 정보를 검토합니다.

열	설명
노드 이름	어플라이언스 노드의 이름입니다.
노드 유형입니다	노드 유형: 스토리지, 관리자 또는 게이트웨이
사이트	노드가 설치된 StorageGRID 사이트의 이름입니다.
KMS 이름	노드에 사용된 KMS의 설명 이름입니다. KMS가 나열되지 않으면 구성 세부 정보 탭을 선택하여 KMS를 추가합니다. "KMS(키 관리 서버) 추가"
키 UID	어플라이언스 노드에서 데이터를 암호화하고 해독하는 데 사용되는 암호화 키의 고유 ID입니다. 전체 키 UID를 보려면 텍스트를 선택합니다. 대시(--)는 어플라이언스 노드와 KMS 사이의 연결 문제로 인해 키 UID를 알 수 없음을 나타냅니다.

열	설명
상태	KMS와 어플라이언스 노드 간의 연결 상태입니다. 노드가 연결되어 있으면 타임스탬프가 30분마다 업데이트됩니다. KMS 구성이 변경된 후 연결 상태를 업데이트하는 데 몇 분 정도 걸릴 수 있습니다. • 참고: * 새 값을 보려면 웹 브라우저를 새로 고치십시오.

4. 상태 열에 KMS 문제가 표시되면 즉시 문제를 해결하십시오.

   KMS가 정상적으로 작동하는 동안 KMS*에 연결됨 상태로 표시됩니다. 노드가 그리드에서 연결이 끊어지면 노드 연결 상태가 표시됩니다(관리자 다운 또는 알 수 없음).

   다른 상태 메시지는 이름이 같은 StorageGRID 알림에 해당합니다.

   - KMS 구성을 로드하지 못했습니다
   - KMS 연결 오류입니다
   - KMS 암호화 키 이름을 찾을 수 없습니다
   - KMS 암호화 키 회전이 실패했습니다
   - 킬로미터 키가 어플라이언스 볼륨을 해독하지 못했습니다
   - KMS가 구성되지 않았습니다

   이러한 경고에 대해 권장되는 작업을 수행합니다.

   데이터를 완벽하게 보호하려면 모든 문제를 즉시 해결해야 합니다.

KMS를 편집합니다

예를 들어 인증서가 곧 만료될 경우 키 관리 서버의 구성을 편집해야 할 수 있습니다.

시작하기 전에

- KMS에 대해 선택한 사이트를 업데이트할 계획이라면 을 검토했습니다 "사이트의 KMS를 변경할 때의 고려 사항".
- 를 사용하여 그리드 관리자에 로그인했습니다 "지원되는 웹 브라우저".
- 을(를) 보유하고 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 * Actions * > * Edit * 를 선택합니다.

   KMS 세부 정보 페이지에서 KMS 이름을 선택하고 * 편집 * 을 선택하여 KMS를 편집할 수도 있습니다.

3. 선택적으로 키 관리 서버 편집 마법사의 * 1단계(KMS 세부 정보) * 에 있는 세부 정보를 업데이트합니다.

필드에 입력합니다	설명
KMS 이름	이 KMS를 식별하는 데 도움이 되는 설명 이름입니다. 1자에서 64자 사이여야 합니다.
키 이름	KMS에서 StorageGRID 클라이언트에 대한 정확한 키 별칭입니다. 1자에서 255자 사이여야 합니다. 키 이름은 드문 경우지만 편집하면 됩니다. 예를 들어, KMS에서 별칭의 이름이 바뀌거나 이전 키의 모든 버전이 새 별칭의 버전 기록으로 복사된 경우 키 이름을 편집해야 합니다.
의 키를 관리합니다	사이트별 KMS를 편집하고 있고 기본 KMS가 아직 없는 경우 선택적으로 * 다른 KMS(기본 KMS)에서 관리하지 않는 사이트 * 를 선택합니다. 이 항목을 선택하면 사이트별 KMS가 기본 KMS로 변환되며, 이 KMS는 전용 KMS가 없는 모든 사이트와 확장 시 추가된 사이트에 적용됩니다. • 참고: * 사이트별 KMS를 편집하는 경우 다른 사이트를 선택할 수 없습니다. 기본 KMS를 편집하는 경우 특정 사이트를 선택할 수 없습니다.
포트	KMS 서버가 KMIP(Key Management Interoperability Protocol) 통신에 사용하는 포트입니다. 기본값은 5696으로, KMIP 표준 포트입니다.
호스트 이름	KMS의 정규화된 도메인 이름 또는 IP 주소입니다. • 참고: * 서버 인증서의 주체 대체 이름(SAN) 필드에는 여기에 입력한 FQDN 또는 IP 주소가 포함되어야 합니다. 그렇지 않으면 StorageGRID는 KMS 또는 KMS 클러스터의 모든 서버에 연결할 수 없습니다.

4. KMS 클러스터를 구성하는 경우 * 다른 호스트 이름 추가 * 를 선택하여 클러스터의 각 서버에 대한 호스트 이름을 추가합니다.
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 업로드합니다.
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 업로드합니다.
9. 테스트 및 저장 * 을 선택합니다.

   영향을 받는 사이트에서 키 관리 서버와 모든 노드 암호화 어플라이언스 노드 간의 연결을 테스트합니다. 모든 노드 연결이 유효하고 KMS에서 올바른 키를 찾으면 키 관리 서버가 키 관리 서버 페이지의 테이블에 추가됩니다.

10. 오류 메시지가 나타나면 메시지 세부 정보를 검토하고 * OK * 를 선택합니다.

예를 들어, 이 KMS에 대해 선택한 사이트가 다른 KMS에 의해 이미 관리되고 있거나 연결 테스트에 실패한 경우 422:처리할 수 없는 엔터티 오류가 발생할 수 있습니다.

11. 연결 오류를 해결하기 전에 현재 설정을 저장해야 하는 경우 * 강제 저장 * 을 선택합니다.

> 강제 저장 * 을 선택하면 KMS 구성이 저장되지만 각 제품에서 해당 KMS로의 외부 연결은 테스트되지 않습니다. 구성에 문제가 있을 경우 해당 사이트에서 노드 암호화가 활성화된 어플라이언스 노드를 재부팅하지 못할 수 있습니다. 문제가 해결될 때까지 데이터에 액세스하지 못할 수 있습니다.

KMS 구성이 저장됩니다.

12. 확인 경고를 검토하고 구성을 강제 저장하려면 * OK * 를 선택합니다.

KMS 구성이 저장되지만 KMS에 대한 연결은 테스트되지 않습니다.

KMS(키 관리 서버**)** 제거

경우에 따라 키 관리 서버를 제거할 수 있습니다. 예를 들어 사이트를 해체한 경우 사이트별 KMS를 제거할 수 있습니다.

시작하기 전에

- 을(를) 검토했습니다 "키 관리 서버 사용에 대한 고려 사항 및 요구 사항".
- 를 사용하여 그리드 관리자에 로그인했습니다 "지원되는 웹 브라우저".
- 을(를) 보유하고 있습니다 "루트 액세스 권한".

이 작업에 대해

다음과 같은 경우 KMS를 제거할 수 있습니다.

- 사이트를 폐기했거나 사이트에 노드 암호화가 활성화된 어플라이언스 노드가 없는 경우 사이트별 KMS를 제거할 수 있습니다.
- 노드 암호화가 활성화된 어플라이언스 노드가 있는 각 사이트에 대해 사이트별 KMS가 이미 있는 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 * Actions * > * Remove * 를 선택합니다.

KMS 세부 정보 페이지에서 KMS 이름을 선택하고 * Remove * 를 선택하여 KMS를 제거할 수도 있습니다.

3. 다음 내용이 맞는지 확인합니다.
   - 노드 암호화가 활성화된 어플라이언스 노드가 없는 사이트에 대한 사이트별 KMS를 제거하고 있습니다.
   - 기본 KMS를 제거하고 있지만 노드 암호화를 사용하는 각 사이트에 대해 사이트별 KMS가 이미 있습니다.
4. 예 * 를 선택합니다.

KMS 구성이 제거되었습니다.

프록시 설정을 관리합니다

스토리지 프록시를 구성합니다

플랫폼 서비스 또는 클라우드 스토리지 풀을 사용하는 경우 스토리지 노드와 외부 S3 엔드포인트 간에 투명하지 않은 프록시를 구성할 수 있습니다. 예를 들어, 플랫폼 서비스 메시지를 인터넷의 끝점과 같은 외부 끝점으로 보내려면 투명하지 않은 프록시가 필요할 수 있습니다.

> 구성된 스토리지 프록시 설정은 Kafka 플랫폼 서비스 엔드포인트에 적용되지 않습니다.

시작하기 전에

- 있습니다 "특정 액세스 권한".
- 를 사용하여 그리드 관리자에 로그인했습니다 "지원되는 웹 브라우저".

이 작업에 대해

단일 스토리지 프록시에 대한 설정을 구성할 수 있습니다.

단계

1. 구성 * > * 보안 * > * 프록시 설정 * 을 선택합니다.
2. Storage * 탭에서 * Enable storage proxy * 확인란을 선택합니다.
3. 스토리지 프록시의 프로토콜을 선택합니다.
4. 프록시 서버의 호스트 이름 또는 IP 주소를 입력합니다.
5. 필요에 따라 프록시 서버에 연결하는 데 사용되는 포트를 입력합니다.

   프로토콜의 기본 포트(HTTP의 경우 80, SOCKS5의 경우 1080)를 사용하려면 이 필드를 비워 둡니다.

6. 저장 * 을 선택합니다.

   스토리지 프록시가 저장된 후 플랫폼 서비스 또는 클라우드 스토리지 풀의 새 엔드포인트를 구성하고 테스트할 수 있습니다.

   > 프록시 변경 사항이 적용되려면 최대 10분이 소요될 수 있습니다.

7. 프록시 서버의 설정을 확인하여 StorageGRID의 플랫폼 서비스 관련 메시지가 차단되지 않는지 확인합니다.
8. 스토리지 프록시를 비활성화해야 하는 경우 확인란을 선택 취소하고 * 저장 * 을 선택합니다.

관리자 프록시 설정을 구성합니다

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

AutoSupport에 대한 자세한 내용은 을 참조하십시오 "AutoSupport를 구성합니다".

시작하기 전에

- 있습니다 "특정 액세스 권한".
- 를 사용하여 그리드 관리자에 로그인했습니다 "지원되는 웹 브라우저".

이 작업에 대해

단일 관리자 프록시에 대한 설정을 구성할 수 있습니다.

단계

1. 구성 * > * 보안 * > * 프록시 설정 * 을 선택합니다.

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

2. 관리 * 탭을 선택합니다.
3. 관리자 프록시 사용 * 확인란을 선택합니다.
4. 프록시 서버의 호스트 이름 또는 IP 주소를 입력합니다.
5. 프록시 서버에 연결하는 데 사용되는 포트를 입력합니다.
6. 필요한 경우 프록시 서버의 사용자 이름과 암호를 입력합니다.

   프록시 서버에 사용자 이름 또는 암호가 필요하지 않은 경우 이 필드를 비워 둡니다.

7. 다음 중 하나를 선택합니다.

   - 관리자 프록시에 대한 연결을 보호하려면 * 인증서 확인 * 을 선택합니다. CA 번들을 업로드하여 관리 프록시 서버에서 제공하는 SSL 인증서의 신뢰성을 확인합니다.

     프록시 인증서가 확인된 경우 AutoSupport on Demand, StorageGRID를 통한 E-Series AutoSupport 및 StorageGRID 업그레이드 페이지의 업데이트 경로 확인이 작동하지 않습니다.

   CA 번들을 업로드하면 해당 메타데이터가 나타납니다.

   - 관리자 프록시 서버와 통신할 때 인증서의 유효성을 검사하지 않으려면 * 인증서 확인 안 함 * 을 선택합니다.

8. 저장 * 을 선택합니다.

   관리자 프록시가 저장된 후 관리 노드와 기술 지원 간의 프록시 서버가 구성됩니다.

   프록시 변경 사항이 적용되려면 최대 10분이 소요될 수 있습니다.

9. 관리자 프록시를 비활성화해야 하는 경우 * 관리자 프록시 사용 * 확인란의 선택을 취소한 다음 * 저장 * 을 선택합니다.

방화벽을 제어합니다

외부 방화벽에서 액세스를 제어합니다

외부 방화벽에서 특정 포트를 열거나 닫을 수 있습니다.

외부 방화벽에서 특정 포트를 열거나 닫아 StorageGRID 관리 노드의 사용자 인터페이스 및 API에 대한 액세스를

제어할 수 있습니다. 예를 들어, 테넌트가 다른 방법을 사용하여 시스템 액세스를 제어하는 것 외에도 방화벽에서 Grid Manager에 연결할 수 없도록 할 수 있습니다.

StorageGRID 내부 방화벽을 구성하려면 를 참조하십시오 "내부 방화벽을 구성합니다".

포트	설명	포트가 열려 있는 경우...
443	관리 노드의 기본 HTTPS 포트	웹 브라우저 및 관리 API 클라이언트는 Grid Manager, Grid Management API, Tenant Manager 및 Tenant Management API에 액세스할 수 있습니다. • 참고: * 포트 443은 일부 내부 트래픽에도 사용됩니다.
8443	관리 노드의 제한된 그리드 관리자 포트	• 웹 브라우저 및 관리 API 클라이언트는 HTTPS를 사용하여 그리드 관리자 및 그리드 관리 API에 액세스할 수 있습니다. • 웹 브라우저 및 관리 API 클라이언트는 테넌트 관리자 또는 테넌트 관리 API에 액세스할 수 없습니다. • 내부 콘텐츠 요청은 거부됩니다.
9443)을 참조하십시오	관리 노드의 제한된 테넌트 관리자 포트	• 웹 브라우저 및 관리 API 클라이언트는 HTTPS를 사용하여 테넌트 관리자 및 테넌트 관리 API에 액세스할 수 있습니다. • 웹 브라우저 및 관리 API 클라이언트는 그리드 관리자 또는 그리드 관리 API에 액세스할 수 없습니다. • 내부 콘텐츠 요청은 거부됩니다.

제한된 Grid Manager 또는 테넌트 관리자 포트에서는 SSO(Single Sign-On)를 사용할 수 없습니다. 사용자가 SSO(Single Sign-On)로 인증하도록 하려면 기본 HTTPS 포트(443)를 사용해야 합니다.

관련 정보

- "Grid Manager에 로그인합니다"
- "테넌트 계정을 생성합니다"
- "외부 통신"

내부 방화벽 제어를 관리합니다

StorageGRID에는 노드에 대한 네트워크 액세스를 제어할 수 있도록 함으로써 그리드의 보안을 강화하는 각 노드에 대한 내부 방화벽이 포함되어 있습니다. 방화벽을 사용하여 특정 그리드 구축에 필요한 포트를 제외한 모든 포트의 네트워크 액세스를 방지합니다. 방화벽 제어 페이지에서 변경한 구성은 각 노드에 배포됩니다.

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

- * 특별 권한 주소 목록 *: 이 탭을 사용하면 닫힌 포트에 대한 선택된 액세스를 허용할 수 있습니다. 외부 액세스 관리 탭을 사용하여 닫은 포트에 액세스할 수 있는 IP 주소 또는 서브넷을 CIDR 표시법으로 추가할 수 있습니다.

- * 외부 액세스 관리 *: 이 탭을 사용하여 기본적으로 열려 있는 포트를 닫거나 이전에 닫은 포트를 다시 열 수 있습니다.
- * 신뢰할 수 없는 클라이언트 네트워크 *: 노드가 클라이언트 네트워크의 인바운드 트래픽을 신뢰하는지 여부를 지정하려면 이 탭을 사용합니다.

  이 탭의 설정은 외부 액세스 관리 탭의 설정보다 우선합니다.

  - 신뢰할 수 없는 클라이언트 네트워크가 있는 노드는 해당 노드에 구성된 로드 밸런서 엔드포인트 포트(글로벌, 노드 인터페이스 및 노드 유형 바운드 엔드포인트)의 연결만 받아들입니다.
  - 부하 분산 장치 엔드포인트 포트 _ 는(는) 신뢰할 수 없는 클라이언트 네트워크에서 외부 네트워크 관리 탭의 설정에 관계없이 열려 있는 유일한 포트입니다.
  - 신뢰할 수 있는 경우 외부 액세스 관리 탭에서 열린 모든 포트와 클라이언트 네트워크에 열려 있는 모든 로드 밸런서 끝점에 액세스할 수 있습니다.

> 한 탭에서 설정한 내용은 다른 탭의 액세스 변경에 영향을 줄 수 있습니다. 모든 탭의 설정을 확인하여 네트워크가 예상한 대로 작동하는지 확인하십시오.

내부 방화벽 제어를 구성하려면 를 참조하십시오 "방화벽 제어를 구성합니다".

외부 방화벽 및 네트워크 보안에 대한 자세한 내용은 을 참조하십시오 "외부 방화벽에서 액세스를 제어합니다".

특별 권한 주소 목록 및 외부 액세스 관리 탭

특별 권한 주소 목록 탭을 사용하면 닫힌 그리드 포트에 대한 액세스 권한이 부여된 하나 이상의 IP 주소를 등록할 수 있습니다. 외부 액세스 관리 탭을 사용하면 선택한 외부 포트 또는 열려 있는 모든 외부 포트에 대한 외부 액세스를 닫을 수 있습니다(외부 포트는 기본적으로 비 그리드 노드가 액세스할 수 있는 포트입니다). 이러한 두 탭을 함께 사용하여 그리드에 필요한 정확한 네트워크 액세스를 사용자 지정할 수 있습니다.

> 권한이 있는 IP 주소는 기본적으로 내부 그리드 포트 액세스를 갖지 않습니다.

예 **1:** 유지 보수 작업에 점프 호스트를 사용합니다

네트워크 관리에 점프 호스트(보안 강화 호스트)를 사용하려는 경우를 가정해 보겠습니다. 다음과 같은 일반 단계를 사용할 수 있습니다.

1. 특별 권한 주소 목록 탭을 사용하여 점프 호스트의 IP 주소를 추가합니다.
2. 외부 액세스 관리 탭을 사용하여 모든 포트를 차단합니다.

> 포트 443 및 8443을 차단하기 전에 권한이 있는 IP 주소를 추가합니다. 사용자를 포함하여 현재 차단된 포트에 연결되어 있는 모든 사용자는 권한이 있는 주소 목록에 IP 주소가 추가되지 않으면 Grid Manager에 액세스할 수 없습니다.

구성을 저장하면 이동 호스트를 제외한 모든 호스트에 대해 그리드의 관리 노드에 있는 모든 외부 포트가 차단됩니다. 그런 다음 점프 호스트를 사용하여 그리드에 대한 유지 관리 작업을 보다 안전하게 수행할 수 있습니다.

예 **2:** 그리드 관리자 및 테넌트 관리자에 대한 액세스를 제한합니다

보안상의 이유로 Grid Manager 및 Tenant Manager(사전 설정 포트)에 대한 액세스를 제한하려는 경우를 가정해 보겠습니다. 다음과 같은 일반 단계를 사용할 수 있습니다.

1. 외부 액세스 관리 탭의 토글을 사용하여 포트 443을 차단합니다.
2. 외부 액세스 관리 탭의 토글을 사용하여 포트 8443에 대한 액세스를 허용합니다.
3. 포트 9443에 액세스할 수 있도록 하려면 Manage external access(외부 액세스 관리) 탭의 토글을 사용하십시오.

구성을 저장한 후 호스트는 포트 443에 액세스할 수 없지만 포트 8443을 통해 Grid Manager와 포트 9443을 통해 테넌트 관리자를 액세스할 수는 있습니다.

> 포트 443, 8443 및 9443 은 Grid Manager 및 Tenant Manager에 대해 사전 설정된 포트입니다. 특정 Grid Manager 또는 Tenant 관리자에 대한 액세스를 제한하도록 포트를 전환할 수 있습니다.

예 **3:** 민감한 포트를 잠급니다

중요한 포트와 해당 포트의 서비스(예: 포트 22의 SSH)를 잠그려고 한다고 가정합니다. 다음과 같은 일반 단계를 사용할 수 있습니다.

1. 특별 권한 주소 목록 탭을 사용하여 서비스에 액세스해야 하는 호스트에만 액세스 권한을 부여합니다.
2. 외부 액세스 관리 탭을 사용하여 모든 포트를 차단합니다.

> Grid Manager 및 Tenant Manager 액세스에 할당된 포트에 대한 액세스를 차단하기 전에 권한 있는 IP 주소를 추가합니다(사전 설정된 포트는 443 및 8443). 사용자를 포함하여 현재 차단된 포트에 연결되어 있는 모든 사용자는 권한이 있는 주소 목록에 IP 주소가 추가되지 않으면 Grid Manager에 액세스할 수 없습니다.

구성을 저장하면 권한이 있는 주소 목록의 호스트에서 포트 22 및 SSH 서비스를 사용할 수 있습니다. 다른 모든 호스트는 요청이 어떤 인터페이스에서 제공되든 서비스에 대한 액세스가 거부됩니다.

예 **4:** 사용하지 않는 서비스에 대한 액세스를 비활성화합니다

네트워크 수준에서는 사용하지 않을 일부 서비스를 사용하지 않도록 설정할 수 있습니다. 예를 들어, Swift 액세스를 제공하지 않으면 다음과 같은 일반 단계를 수행합니다.

1. 외부 액세스 관리 탭의 토글을 사용하여 포트 18083을 차단합니다.
2. 외부 액세스 관리 탭의 토글을 사용하여 포트 18085를 차단합니다.

구성을 저장한 후에는 스토리지 노드가 더 이상 Swift 연결을 허용하지 않지만, 차단되지 않은 포트에서 다른 서비스에 대한 액세스를 계속 허용합니다.

신뢰할 수 없는 클라이언트 네트워크 탭

클라이언트 네트워크를 사용하는 경우 명시적으로 구성된 끝점에서만 인바운드 클라이언트 트래픽을 허용하여 악의적인 공격으로부터 StorageGRID를 보호할 수 있습니다.

기본적으로 각 그리드 노드의 클라이언트 네트워크는 _ trusted _ 입니다. 즉, 기본적으로 StorageGRID는 모든 그리드 노드에 대한 인바운드 연결을 신뢰합니다 "사용 가능한 외부 포트".

각 노드의 클라이언트 네트워크가 _untrusted_로 지정함으로써 StorageGRID 시스템에 대한 악의적인 공격의 위협을 줄일 수 있습니다. 노드의 클라이언트 네트워크를 신뢰할 수 없는 경우 노드는 로드 밸런서 끝점으로 명시적으로 구성된 포트의 인바운드 연결만 허용합니다. 을 참조하십시오 "로드 밸런서 엔드포인트를 구성합니다" 및 "방화벽 제어를 구성합니다".

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

게이트웨이 노드가 HTTPS S3 요청을 제외한 클라이언트 네트워크의 모든 인바운드 트래픽을 거부하도록 한다고 가정합니다. 다음과 같은 일반 단계를 수행합니다.

1. 에서 "부하 분산 장치 엔드포인트" 페이지에서 포트 443에서 HTTPS를 통해 S3에 대한 로드 밸런서 끝점을 구성합니다.
2. 방화벽 제어 페이지에서 신뢰할 수 없음 을 선택하여 게이트웨이 노드의 클라이언트 네트워크를 신뢰할 수 없도록 지정합니다.

구성을 저장한 후 게이트웨이 노드의 클라이언트 네트워크의 모든 인바운드 트래픽은 포트 443 및 ICMP 에코(ping) 요청의 HTTPS S3 요청을 제외하고 삭제됩니다.

예 **2:** 스토리지 노드가 **S3** 플랫폼 서비스 요청을 전송합니다

스토리지 노드에서 아웃바운드 S3 플랫폼 서비스 트래픽을 활성화하되 클라이언트 네트워크의 해당 스토리지 노드에 대한 인바운드 연결을 차단하려는 경우를 가정해 봅니다. 이 일반 단계를 수행합니다.

- 방화벽 제어 페이지의 신뢰할 수 없는 클라이언트 네트워크 탭에서 스토리지 노드의 클라이언트 네트워크를 신뢰할 수 없음을 나타냅니다.

구성을 저장한 후 스토리지 노드는 더 이상 클라이언트 네트워크에서 들어오는 트래픽을 허용하지 않지만 구성된 플랫폼 서비스 대상에 대한 아웃바운드 요청은 계속 허용합니다.

예 **3:** 그리드 관리자에 대한 액세스를 서브넷으로 제한

특정 서브넷에서만 Grid Manager 액세스를 허용한다고 가정합니다. 다음 단계를 수행합니다.

1. 관리 노드의 클라이언트 네트워크를 서브넷에 연결합니다.
2. 신뢰할 수 없는 클라이언트 네트워크 탭을 사용하여 클라이언트 네트워크를 신뢰할 수 없음으로 구성합니다.
3. 관리 인터페이스 로드 밸런서 엔드포인트를 생성할 때 port를 입력하고 포트가 액세스할 관리 인터페이스를 선택합니다.
4. 신뢰할 수 없는 클라이언트 네트워크에 대해 * 예 * 를 선택합니다.
5. 외부 액세스 관리 탭을 사용하여 모든 외부 포트(해당 서브넷 외부의 호스트에 대해 설정된 권한이 있는 IP 주소 포함 또는 제외)를 차단합니다.

구성을 저장한 후에는 지정한 서브넷의 호스트만 Grid Manager에 액세스할 수 있습니다. 다른 호스트는 모두 차단됩니다.

내부 방화벽을 구성합니다

StorageGRID 노드의 특정 포트에 대한 네트워크 액세스를 제어하도록 StorageGRID 방화벽을 구성할 수 있습니다.

시작하기 전에

- 를 사용하여 그리드 관리자에 로그인했습니다 "지원되는 웹 브라우저".
- 있습니다 "특정 액세스 권한".
- 에서 정보를 검토했습니다 "방화벽 제어 관리" 및 "네트워킹 지침".

- 관리자 노드 또는 게이트웨이 노드가 명시적으로 구성된 끝점에서만 인바운드 트래픽을 수락하도록 하려면 로드 밸런서 끝점을 정의해야 합니다.

> 클라이언트 네트워크의 구성을 변경할 때 로드 밸런서 끝점이 구성되지 않은 경우 기존 클라이언트 연결이 실패할 수 있습니다.

이 작업에 대해

StorageGRID에는 그리드의 노드에서 일부 포트를 열거나 닫을 수 있도록 각 노드에 대한 내부 방화벽이 포함되어 있습니다. 방화벽 제어 탭을 사용하여 그리드 네트워크, 관리자 네트워크 및 클라이언트 네트워크에서 기본적으로 열려 있는 포트를 열거나 닫을 수 있습니다. 닫힌 그리드 포트에 액세스할 수 있는 권한이 있는 IP 주소 목록을 만들 수도 있습니다. 클라이언트 네트워크를 사용하는 경우 노드가 클라이언트 네트워크의 인바운드 트래픽을 신뢰하는지 여부를 지정하고 클라이언트 네트워크의 특정 포트에 대한 액세스를 구성할 수 있습니다.

그리드 외부의 IP 주소에 열려 있는 포트 수를 절대적으로 필요한 포트로만 제한하면 그리드의 보안이 향상됩니다. 세 개의 방화벽 제어 탭 각각에서 설정을 사용하여 필요한 포트만 열도록 합니다.

예를 포함한 방화벽 컨트롤 사용에 대한 자세한 내용은 을 참조하십시오 "방화벽 제어 관리".

외부 방화벽 및 네트워크 보안에 대한 자세한 내용은 을 참조하십시오 "외부 방화벽에서 액세스를 제어합니다".

방화벽 컨트롤에 액세스합니다

단계

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

   이 페이지의 세 가지 탭은 에 설명되어 있습니다 "방화벽 제어 관리".

2. 탭을 선택하여 방화벽 컨트롤을 구성합니다.

   이러한 탭은 순서에 상관없이 사용할 수 있습니다. 한 탭에서 설정한 구성은 다른 탭에서 수행할 수 있는 작업을 제한하지 않지만 한 탭에서 변경한 구성은 다른 탭에 구성된 포트의 동작을 변경할 수 있습니다.

특별 권한 주소 목록

특별 권한 주소 목록 탭을 사용하여 외부 액세스 관리 탭의 설정에 따라 기본적으로 닫히거나 닫힌 포트에 대한 호스트 액세스 권한을 부여할 수 있습니다.

권한이 있는 IP 주소 및 서브넷에는 기본적으로 내부 그리드 액세스가 없습니다. 또한 외부 액세스 관리 탭에서 차단된 경우에도 권한이 있는 주소 목록 탭에서 열린 로드 밸런서 끝점과 추가 포트에 액세스할 수 있습니다.

> 권한이 있는 주소 목록 탭의 설정은 신뢰할 수 없는 클라이언트 네트워크 탭의 설정을 재정의할 수 없습니다.

단계

1. 특별 권한 주소 목록 탭에서 닫힌 포트에 대한 액세스를 허용할 주소 또는 IP 서브넷을 입력합니다.
2. 선택적으로 * CIDR 표기법 * 으로 다른 IP 주소 또는 서브넷 추가 를 선택하여 권한이 있는 클라이언트를 추가합니다.

> 가능한 한 적은 수의 주소를 권한 있는 목록에 추가합니다.

3. 선택적으로 * 권한이 있는 IP 주소가 StorageGRID 내부 포트에 액세스하도록 허용 * 을 선택합니다. 을 참조하십시오 "StorageGRID 내부 포트".

> 이 옵션은 내부 서비스에 대한 일부 보호를 제거합니다. 가능한 경우 비활성화 상태로 둡니다.

4. 저장 * 을 선택합니다.

외부 액세스를 관리합니다

외부 액세스 관리 탭에서 포트가 닫힌 경우 권한이 있는 주소 목록에 IP 주소를 추가하지 않으면 비 그리드 IP 주소로 포트에 액세스할 수 없습니다. 기본적으로 열려 있는 포트만 닫을 수 있으며 닫은 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 경우 외부 액세스 관리 탭에 열려 있어도 클라이언트 네트워크에서 포트 SSH/22가 차단됩니다. 신뢰할 수 없는 클라이언트 네트워크 탭의 설정은 클라이언트 네트워크의 닫힌 포트(예: 443, 8443, 9443)를 재정의합니다.

단계

1. 외부 액세스 관리 * 를 선택합니다. 이 탭에는 그리드의 노드에 대해 모든 외부 포트(기본적으로 비 그리드 노드가 액세스할 수 있는 포트)가 포함된 테이블이 표시됩니다.
2. 다음 옵션을 사용하여 열고 닫을 포트를 구성합니다.
   - 각 포트 옆의 토글을 사용하여 선택한 포트를 열거나 닫습니다.
   - 표시된 모든 포트 열기 * 를 선택하여 표에 나열된 모든 포트를 엽니다.
   - 표에 나열된 모든 포트를 닫으려면 * 표시된 모든 포트 닫기 * 를 선택합니다.

> Grid Manager 포트 443 또는 8443을 닫으면 사용자를 포함하여 차단된 포트에 현재 연결되어 있는 모든 사용자는 권한이 있는 주소 목록에 IP 주소가 추가되지 않으면 Grid Manager에 액세스할 수 없습니다.

> 테이블 오른쪽에 있는 스크롤 막대를 사용하여 사용 가능한 모든 포트를 확인합니다. 검색 필드를 사용하여 포트 번호를 입력하여 외부 포트의 설정을 찾습니다. 일부 포트 번호를 입력할 수 있습니다. 예를 들어 * 2 * 를 입력하면 이름에 문자열 "2"가 포함된 모든 포트가 표시됩니다.

3. 저장 * 을 선택합니다

신뢰할 수 없는 클라이언트 네트워크

노드의 클라이언트 네트워크를 신뢰할 수 없는 경우 노드는 로드 밸런서 끝점으로 구성된 포트의 인바운드 트래픽만 허용하고 선택적으로 이 탭에서 선택하는 추가 포트만 허용합니다. 이 탭을 사용하여 확장에 추가된 새 노드의 기본 설정을 지정할 수도 있습니다.

> 로드 밸런서 끝점이 구성되지 않은 경우 기존 클라이언트 연결이 실패할 수 있습니다.

신뢰할 수 없는 클라이언트 네트워크* 탭에서 변경한 구성은 * 외부 액세스 관리 * 탭의 설정보다 우선합니다.

단계

1. 신뢰할 수 없는 클라이언트 네트워크 * 를 선택합니다.
2. 새 노드 기본값 설정 섹션에서 확장 절차에서 그리드에 새 노드를 추가할 때 기본 설정을 지정합니다.
   - * 신뢰 * (기본값): 확장 시 노드를 추가하면 해당 클라이언트 네트워크가 신뢰됩니다.
   - * 신뢰할 수 없음 *: 확장 시 노드가 추가되면 해당 클라이언트 네트워크를 신뢰할 수 없습니다.

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

     > 이 설정은 StorageGRID 시스템의 기존 노드에는 영향을 주지 않습니다.

3. 다음 옵션을 사용하여 명시적으로 구성된 로드 밸런싱 장치 엔드포인트 또는 추가 선택 포트에서만 클라이언트 연결을 허용할 노드를 선택합니다.
   - 표시된 노드에서 신뢰 해제 * 를 선택하여 테이블에 표시된 모든 노드를 신뢰할 수 없는 클라이언트 네트워크 목록에 추가합니다.
   - 표시된 노드의 신뢰 * 를 선택하여 신뢰할 수 없는 클라이언트 네트워크 목록에서 표에 표시된 모든 노드를 제거합니다.
   - 각 노드 옆의 토글을 사용하여 선택한 노드에 대해 클라이언트 네트워크를 신뢰할 수 있는 또는 신뢰할 수 없는 것으로 설정합니다.

     예를 들어 표시된 노드에서 * 언트러스트 * 를 선택하여 모든 노드를 신뢰할 수 없는 클라이언트 네트워크 목록에 추가한 다음 개별 노드 옆의 토글을 사용하여 해당 단일 노드를 신뢰할 수 있는 클라이언트 네트워크 목록에 추가할 수 있습니다.

     > 테이블 오른쪽에 있는 스크롤 막대를 사용하여 사용 가능한 모든 노드를 확인합니다. 검색 필드를 사용하여 노드 이름을 입력하여 노드 설정을 찾습니다. 부분 이름을 입력할 수 있습니다. 예를 들어 * GW * 를 입력하면 이름에 "GW" 문자열이 포함된 모든 노드가 표시됩니다.

4. 저장 * 을 선택합니다.

   새 방화벽 설정이 즉시 적용되고 적용됩니다. 로드 밸런서 끝점이 구성되지 않은 경우 기존 클라이언트 연결이 실패할 수 있습니다.