인증서 관리

StorageGRID software

NetApp
July 23, 2026

목차

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.

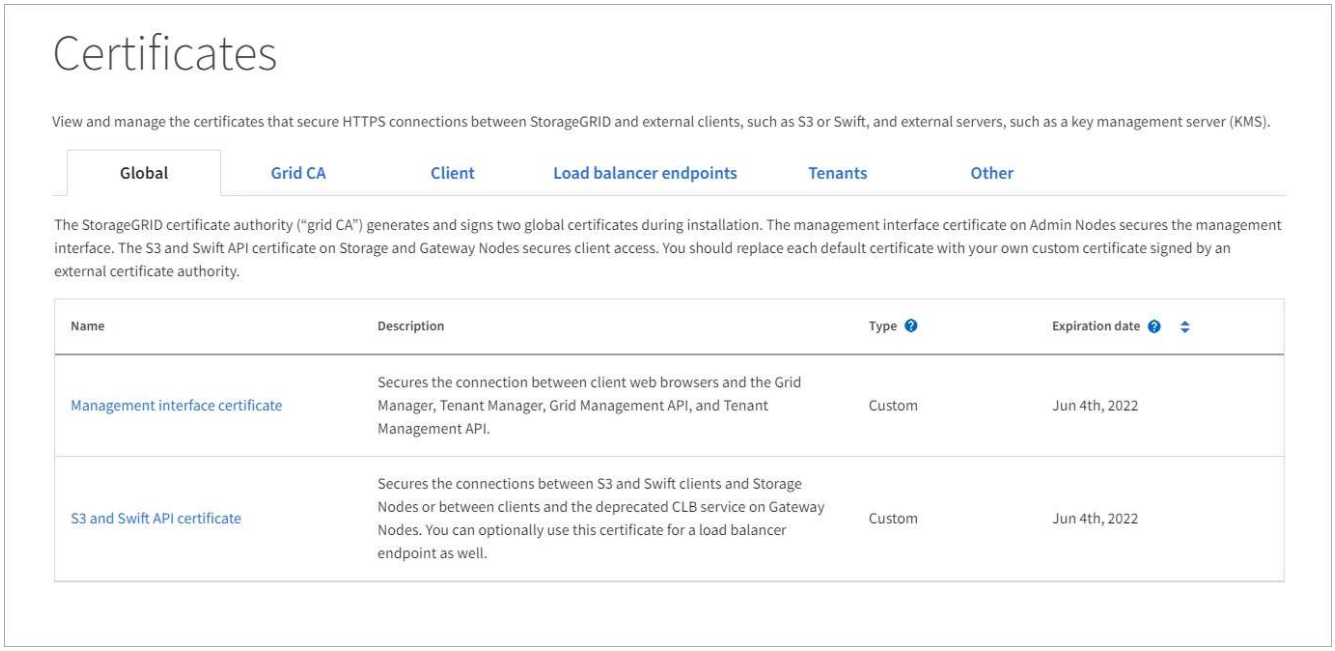
서버 및 클라이언트 인증서 유형의 변형은 여러 가지 방식으로 구현됩니다. 시스템을 구성하기 전에 특정 StorageGRID 구성에 필요한 모든 인증서를 준비해야 합니다.

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.