인증서를 관리합니다

StorageGRID

NetApp
April 10, 2024

목차

인증서를 관리합니다

보안 인증서 정보

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 시스템 강화 지침 서버 인증서용.
- StorageGRID는 CA의 인증서를 단일 파일(CA 인증서 번들이라고 함)로 번들링하는 것을 지원합니다.

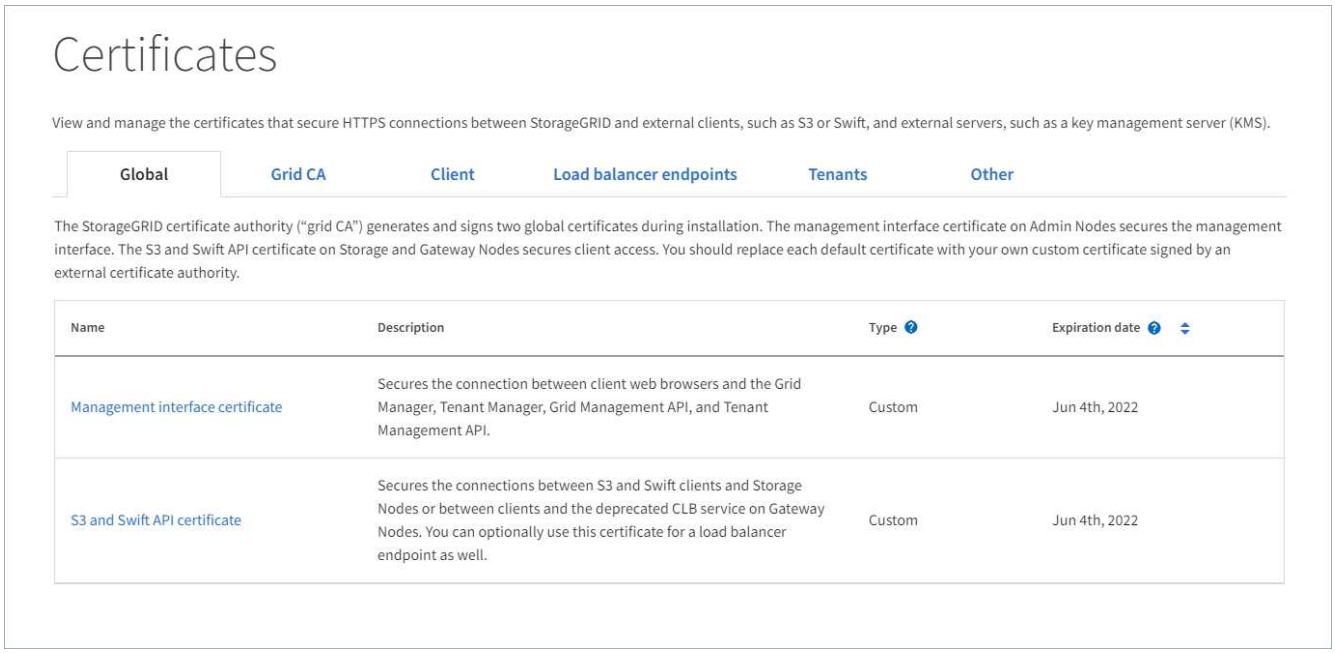
> StorageGRID에는 모든 그리드에서 동일한 운영 체제 CA 인증서도 포함됩니다. 프로덕션 환경에서는 운영 체제 CA 인증서 대신 외부 인증 기관에서 서명한 사용자 지정 인증서를 지정해야 합니다.

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.

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



2. 인증서 페이지에서 탭을 선택하여 각 인증서 범주에 대한 정보를 확인하고 인증서 설정에 액세스합니다. 적절한 권한이 있는 경우에만 탭에 액세스할 수 있습니다.
   - * 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 + 그리드 보안을 강화하기 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, CLB 서비스(더 이상 사용되지 않음) 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 다운로드합니다하지만 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 인증서업로드하거나 생성한 경우 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.

- 끝점 이름을 선택하여 인증서 세부 정보를 비롯하여 로드 밸런서 끝점에 대한 정보가 있는 브라우저 탭을 엽니다.
- 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.

- ID 페더레이션 인증서
- 클라우드 스토리지 풀 인증서
- KMS(키 관리 서버) 인증서
- SSO(Single Sign-On) 인증서
- 이메일 경고 알림 인증서
- 외부 syslog 서버 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.

> 적절한 권한이 있는 경우에만 다른 인증서에 대한 정보를 보고 액세스할 수 있습니다.

다음을 수행할 수 있습니다.

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

보안 인증서 세부 정보입니다

각 보안 인증서 유형은 아래에 설명되어 있으며 구현 지침이 포함된 문서에 대한 링크를 제공합니다.

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	게이트웨이 노드의 더 이상 사용되지 않는 CLB(Connection Load Balancer) 서비스와 로드 밸런서 엔드포인트(선택 사항)에 대한 스토리지 노드에 대한 보안 S3 또는 Swift 클라이언트 연결을 인증합니다.	• 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

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

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

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

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

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

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 * 를 선택한 다음 * 외부 syslog 서버 구성 * 을 선택합니다	외부 syslog 서버를 구성합니다

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.

StorageGRID가 REST API에 대한 클라이언트 연결을 보호하는 방법에 대한 자세한 내용은 을 참조하십시오 S3을 사용합니다 또는 Swift를 사용합니다.

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 파일('.key')입니다.

     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. 확장자가 '.pem'인 파일을 저장합니다.

   예를 들어, 'toragegrid_certificate.pem'

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

d. 저장 * 을 선택합니다. + 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.

   - * 도메인 이름 *: 인증서에 포함할 하나 이상의 정규화된 도메인 이름입니다. 여러 도메인 이름을 나타내는 와일드카드로 * 를 사용합니다.
   - * IP *: 인증서에 포함할 하나 이상의 IP 주소입니다.
   - * subject *: X.509 주체 또는 인증서 소유자의 고유 이름(DN)
   - * 일 유효 *: 인증서 만료 후 일 수입니다.

c. Generate * 를 선택합니다.

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

- 인증서 파일을 저장하려면 * 인증서 다운로드 * 를 선택합니다.

  인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자가 '.pem'인 파일을 저장합니다.

  예를 들어, 'toragegrid_certificate.pem'

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

e. 저장 * 을 선택합니다. + 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. + 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.

필요한 것

- 특정 액세스 권한이 있습니다.
- "passwords.txt" 파일이 있습니다.

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. 'ssh admin@primary_Admin_Node_IP' 명령어를 입력한다
b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
c. 루트로 전환하려면 다음 명령을 입력합니다
d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

3. 자체 서명된 새 인증서를 사용하여 StorageGRID를 구성합니다.

   '$sudo make-certificate—domain_wildcard-admin-node-FQDN_—type management'

   - '- 도메인'의 경우 와일드카드를 사용하여 모든 관리 노드의 정규화된 도메인 이름을 나타냅니다. 예를 들어, '*.ui.storagegrid.example.com'은 ' admin1.ui.storagegrid.example.com ' 및 ' admin2.ui.storagegrid.example.com ' 을 나타내는 * 와일드카드를 사용합니다.
   - 그리드 관리자 및 테넌트 관리자가 사용하는 관리 인터페이스 인증서를 구성하려면 '--type'을 '관리'로 설정합니다.
   - 기본적으로 생성된 인증서는 1년(365일) 동안 유효하며 만료되기 전에 다시 만들어야 합니다. '--days' 인증서를 사용하여 기본 유효 기간을 재정의할 수 있습니다.

     > 인증서의 유효 기간은 make-certificate를 실행하면 시작됩니다. 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 번들 '.pem' 파일을 다운로드합니다. 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. 확장자가 '.pem'인 파일을 저장합니다.

   예를 들어, 'toragegrid_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 확장자 '.pem'으로 저장합니다.

   예를 들어, 'toragegrid_certificate.pem'

S3 및 **Swift API** 인증서를 구성합니다

스토리지 노드에 대한 S3 또는 Swift 클라이언트 연결에 사용되는 서버 인증서, 게이트웨이 노드의 더 이상 사용되지 않는 CLB(Connection Load Balancer) 서비스 또는 밸런서 엔드포인트를 로드하기 위해 서버 인증서를 교체하거나 복원할 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 파일('.key')입니다.

     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. 확장자가 '.pem'인 파일을 저장합니다.

   예를 들어, 'toragegrid_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.

   - * 도메인 이름 *: 인증서에 포함할 하나 이상의 정규화된 도메인 이름입니다. 여러 도메인 이름을 나타내는 와일드카드로 * 를 사용합니다.
   - * IP *: 인증서에 포함할 하나 이상의 IP 주소입니다.
   - * subject *: X.509 주체 또는 인증서 소유자의 고유 이름(DN)
   - * 일 유효 *: 인증서 만료 후 일 수입니다.

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. 확장자가 '.pem'인 파일을 저장합니다.

예를 들어, 'toragegrid_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. + 필요에 따라 인증서 PEM을 다운로드하거나 복사할 수 있습니다.

기본 **S3** 및 **Swift API** 인증서를 복원합니다

스토리지 노드에 대한 S3 및 Swift 클라이언트 연결에 대해 기본 S3 및 Swift API 인증서를 사용하고 게이트웨이 노드에서 더 이상 사용되지 않는 CLB 서비스로 되돌릴 수 있습니다. 그러나 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 연결과 게이트웨이 노드의 더 이상 사용되지 않는 CLB 서비스에 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 번들 '.pem' 파일을 다운로드합니다. 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. 확장자가 '.pem'인 파일을 저장합니다.

   예를 들어, 'toragegrid_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 확장자 '.pem'으로 저장합니다.

   예를 들어, 'toragegrid_certificate.pem'

관련 정보

- S3을 사용합니다
- Swift를 사용합니다
- S3 API 엔드포인트 도메인 이름을 구성합니다

Grid CA 인증서를 복사합니다

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

필요한 것

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

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

인증서 '.pem' 파일을 다운로드합니다.

a. 인증서 다운로드 * 를 선택합니다.
b. 인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자가 '.pem'인 파일을 저장합니다.

   예를 들어, 'toragegrid_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 확장자 '.pem'으로 저장합니다.

   예를 들어, 'toragegrid_certificate.pem'

FabricPool용 StorageGRID 인증서를 구성합니다

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

필요한 것

- 특정 액세스 권한이 있습니다.
- 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.

> 게이트웨이 노드의 별도의 CLB(연결 로드 밸런서) 서비스는 더 이상 사용되지 않으며 FabricPool와 함께 사용하지 않는 것이 좋습니다.

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.

에 대한 정보를 참조하십시오 일반 보안 인증서 사용 및 사용자 지정 서버 인증서를 구성하는 중입니다.

> 실패한 서버 인증서로 인해 작업이 중단되지 않도록 하려면 이 서버 인증서가 곧 만료될 때 인증서 페이지 * 알림에 구성된 * 클라이언트 인증서 만료가 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.

필요한 것

- 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

시나리오에 따라 클라이언트 인증서를 추가합니다.

- 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. 최소 1자 이상 32자 이하의 인증서 이름을 입력하십시오.
4. 외부 모니터링 도구를 사용하여 Prometheus 메트릭에 액세스하려면 * Prometheus * 를 선택합니다.
5. 인증서 종류 * 섹션에서 관리 인터페이스 인증서 '.pem' 파일을 업로드합니다.
   a. 인증서 업로드 * 를 선택한 다음 * 계속 * 을 선택합니다.
   b. 관리 인터페이스 인증서 파일('.pem')을 업로드합니다.
      - 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.
6. 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.

      예: "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.

  f. 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.

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. 최소 1자 이상 32자 이하의 인증서 이름을 입력하십시오.
5. 외부 모니터링 도구를 사용하여 Prometheus 메트릭에 액세스하려면 * Prometheus * 를 선택합니다.
6. 인증서 유형 * 섹션에서 클라이언트 인증서, 개인 키 및 CA 번들 '.pem' 파일을 업로드합니다.
   a. 인증서 업로드 * 를 선택한 다음 * 계속 * 을 선택합니다.
   b. 클라이언트 인증서, 개인 키 및 CA 번들 파일('.pem')을 업로드합니다.
      - 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. 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.

      예: "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.

f. 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.

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. 최소 1자 이상 32자 이하의 인증서 이름을 입력하십시오.
4. 외부 모니터링 도구를 사용하여 Prometheus 메트릭에 액세스하려면 * Prometheus * 를 선택합니다.
5. 인증서 유형 * 섹션에서 * 인증서 생성 * 을 선택합니다.
6. 인증서 정보를 지정합니다.
   - * 도메인 이름 *: 인증서에 포함할 관리자 노드의 정규화된 도메인 이름 하나 이상. 여러 도메인 이름을 나타내는 와일드카드로 * 를 사용합니다.
   - * IP *: 인증서에 포함할 하나 이상의 관리 노드 IP 주소입니다.
   - * subject *: X.509 주체 또는 인증서 소유자의 고유 이름(DN)
7. Generate * 를 선택합니다.
8. [[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. 확장자가 '.pem'인 파일을 저장합니다.

   예를 들어, 'toragegrid_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.

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

   새 인증서가 클라이언트 탭에 나타납니다.

10. 그리드 관리자에서 * 구성 * > * 보안 * > * 인증서 * 를 선택한 다음 * 글로벌 * 탭을 선택합니다.
11. Management Interface certificate * 를 선택합니다.
12. 사용자 정의 인증서 사용 * 을 선택합니다.
13. 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 파일('.pem')을 업로드합니다.
    c. Grid Manager에 인증서를 저장하려면 * Create * 를 선택합니다.

       새 인증서가 클라이언트 탭에 나타납니다.

14. 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.

       예: "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 및 클라이언트 인증서 모두에 대한 관리 인터페이스 클라이언트 인증서
       - 클라이언트 키에 대한 개인 키입니다
    e. * ServerName *: 관리 노드의 도메인 이름을 입력합니다.

       servername은 관리 인터페이스 인증서에 표시된 도메인 이름과 일치해야 합니다.

    f. 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. 최소 1자 이상 32자 이하의 인증서 이름을 입력하십시오.
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 이름('.pem')을 업로드합니다.

   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. 확장자가 '.pem'인 파일을 저장합니다.

   예를 들어, 'toragegrid_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.
   - * 도메인 이름 *: 인증서에 포함할 하나 이상의 정규화된 도메인 이름입니다. 여러 도메인 이름을 나타내는 와일드카드로 * 를 사용합니다.
   - * IP *: 인증서에 포함할 하나 이상의 IP 주소입니다.
   - * subject *: X.509 주체 또는 인증서 소유자의 고유 이름(DN)
   - * 일 유효 *: 인증서 만료 후 일 수입니다.
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. 확장자가 '.pem'인 파일을 저장합니다.

   예를 들어, 'toragegrid_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

인증서 '.pem' 파일을 다운로드합니다.

a. 인증서 다운로드 * 를 선택합니다.
b. 인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자가 '.pem'인 파일을 저장합니다.

   예를 들어, 'toragegrid_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 확장자 '.pem'으로 저장합니다.

   예를 들어, 'toragegrid_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.