서버 인증서를 구성합니다

StorageGRID 11.7

NetApp
April 12, 2024

목차

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 REST API에 대한 클라이언트 연결을 보호하는 방법에 대한 자세한 내용은 을 참조하십시오 "S3 REST API에 대한 보안을 구성합니다" 또는 "Swift REST API에 대한 보안을 구성합니다".

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. + 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 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 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.

시작하기 전에

- 특정 액세스 권한이 있습니다.
- 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. + 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".
- 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

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

- 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".

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.