StorageGRID에 대한 관리자 액세스 제어

StorageGRID 11.5

NetApp
April 11, 2024

목차

StorageGRID에 대한 관리자 액세스 제어

방화벽 포트를 열거나 닫거나, 관리 그룹 및 사용자를 관리하고, SSO(Single Sign-On)를 구성하고, StorageGRID 메트릭에 대한 안전한 외부 액세스를 허용하는 클라이언트 인증서를 제공하여 StorageGRID 시스템에 대한 관리자 액세스를 제어할 수 있습니다.

- "방화벽을 통한 액세스 제어"
- "ID 페더레이션 사용"
- "관리 그룹 관리"
- "로컬 사용자 관리"
- "StorageGRID용 SSO(Single Sign-On) 사용"
- "관리자 클라이언트 인증서를 구성하는 중입니다"

방화벽을 통한 액세스 제어

방화벽을 통해 액세스를 제어하려면 외부 방화벽에서 특정 포트를 열거나 닫습니다.

외부 방화벽에서 액세스 제어

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.

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.

포트	설명	포트가 열려 있는 경우...
9443	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"

"StorageGRID에서 SSO를 사용하지 않는 경우 테넌트 계정 생성"

"요약: 클라이언트 연결을 위한 IP 주소 및 포트"

"신뢰할 수 없는 클라이언트 네트워크 관리"

"Ubuntu 또는 Debian을 설치합니다"

"VMware를 설치합니다"

"Red Hat Enterprise Linux 또는 CentOS를 설치합니다"

ID 페더레이션 사용

ID 페더레이션을 사용하면 그룹 및 사용자를 더 빠르게 설정할 수 있으며, 사용자는 익숙한 자격 증명을 사용하여 StorageGRID에 로그인할 수 있습니다.

ID 페더레이션을 구성하는 중입니다

관리 그룹 및 사용자를 Active Directory, OpenLDAP 또는 Oracle Directory Server와 같은 다른 시스템에서 관리하도록 하려면 ID 페더레이션을 구성할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.
- SSO(Single Sign-On)를 사용하려는 경우 통합 ID 소스로 Active Directory를 사용하고 ID 공급자로 AD FS를 사용해야 합니다. Single Sign-On 사용 요건 참조
- ID 공급자로 Active Directory, OpenLDAP 또는 Oracle Directory Server를 사용하고 있어야 합니다.

목록에 없는 LDAP v3 서비스를 사용하려면 기술 지원 부서에 문의해야 합니다.

- LDAP 서버와의 통신에 TLS(Transport Layer Security)를 사용하려는 경우 ID 공급자는 TLS 1.2 또는 1.3을 사용해야 합니다.

이 작업에 대해

다음과 같은 유형의 통합 그룹을 가져오려면 그리드 관리자의 ID 소스를 구성해야 합니다.

- 관리 그룹. 관리자 그룹의 사용자는 그룹에 할당된 관리 권한에 따라 Grid Manager에 로그인하여 작업을 수행할 수 있습니다.
- 자신의 ID 소스를 사용하지 않는 테넌트의 테넌트 사용자 그룹 테넌트 그룹의 사용자는 테넌트 관리자의 그룹에 할당된 권한을 기반으로 테넌트 관리자에 로그인하여 작업을 수행할 수 있습니다.

단계

1. Configuration * > * Access Control * > * Identity Federation * 을 선택합니다.
2. ID 페더레이션 사용 * 을 선택합니다.

   LDAP 서버 구성 필드가 나타납니다.

3. LDAP 서비스 유형 섹션에서 구성할 LDAP 서비스 유형을 선택합니다.

   Active Directory *, * OpenLDAP * 또는 * 기타 * 를 선택할 수 있습니다.

   OpenLDAP * 를 선택한 경우 OpenLDAP 서버를 구성해야 합니다. OpenLDAP 서버 구성 지침을 참조하십시오.

   Oracle Directory Server를 사용하는 LDAP 서버의 값을 구성하려면 * 기타 * 를 선택합니다.

4. 기타 * 를 선택한 경우 LDAP 속성 섹션의 필드를 작성합니다.
   - * 사용자 고유 이름 *: LDAP 사용자의 고유 식별자가 포함된 속성의 이름입니다. 이 속성은 과 같습니다 `sAMAccountName` Active Directory 및 의 경우 `uid` OpenLDAP의 경우. Oracle Directory Server를 구성하는 경우 를 입력합니다 `uid`.
   - * 사용자 UUID *: LDAP 사용자의 영구 고유 식별자가 포함된 특성의 이름입니다. 이 속성은 과 같습니다 `objectGUID` Active Directory 및 의 경우 `entryUUID` OpenLDAP의 경우. Oracle Directory Server를 구성하는 경우 를 입력합니다 `nsuniqueid`. 지정된 속성에 대한 각 사용자의 값은 16바이트 또는 문자열 형식의 32자리 16진수 숫자여야 하며, 하이픈은 무시됩니다.
   - * 그룹 고유 이름 *: LDAP 그룹의 고유 식별자가 포함된 속성의 이름입니다. 이 속성은 과 같습니다 `sAMAccountName` Active Directory 및 의 경우 `cn` OpenLDAP의 경우. Oracle Directory Server를 구성하는 경우 를 입력합니다 `cn`.
   - * 그룹 UUID *: LDAP 그룹의 영구 고유 식별자가 포함된 특성의 이름입니다. 이 속성은 과 같습니다 `objectGUID` Active Directory 및 의 경우 `entryUUID` OpenLDAP의 경우. Oracle Directory Server를 구성하는 경우 를 입력합니다 `nsuniqueid`. 지정된 속성에 대한 각 그룹의 값은 16바이트 또는 문자열 형식의 32자리 16진수 숫자여야 하며, 하이픈은 무시됩니다.
5. LDAP 서버 구성 섹션에서 필요한 LDAP 서버 및 네트워크 연결 정보를 입력합니다.
   - * 호스트 이름 *: LDAP 서버의 서버 호스트 이름 또는 IP 주소입니다.
   - * 포트 *: LDAP 서버에 연결하는 데 사용되는 포트입니다.

STARTTLS의 기본 포트는 389이고 LDAPS의 기본 포트는 636입니다. 그러나 방화벽이 올바르게 구성된 경우 모든 포트를 사용할 수 있습니다.

- * 사용자 이름 *: LDAP 서버에 연결할 사용자의 DN(고유 이름)의 전체 경로입니다.

  Active Directory의 경우 아래쪽 로그온 이름 또는 사용자 기본 이름을 지정할 수도 있습니다.

  지정된 사용자는 그룹 및 사용자를 나열하고 다음 속성에 액세스할 수 있는 권한이 있어야 합니다.

  - `sAMAccountName` 또는 `uid`
  - `objectGUID`, `entryUUID`, 또는 `nsuniqueid`
  - `cn`
  - `memberOf` 또는 `isMemberOf`

- * 암호 *: 사용자 이름과 연결된 암호입니다.
- * Group base DN *: 그룹을 검색할 LDAP 하위 트리에 대한 DN(고유 이름)의 전체 경로입니다. Active Directory 예제(아래)에서 고유 이름이 기본 DN(DC=StorageGrid, DC=example, DC=com)과 관련된 모든 그룹을 통합 그룹으로 사용할 수 있습니다.

  그룹 고유 이름 * 값은 * 그룹 기본 DN * 내에서 고유해야 합니다.

- * 사용자 기본 DN *: 사용자를 검색할 LDAP 하위 트리의 고유 이름(DN)의 전체 경로입니다.

  사용자 고유 이름 * 값은 * 사용자 기본 DN * 내에서 고유해야 합니다.

6. TLS(Transport Layer Security) * 섹션에서 보안 설정을 선택합니다.
   - * STARTTLS 사용(권장) *: STARTTLS를 사용하여 LDAP 서버와의 통신을 보호합니다. 이 옵션을 선택하는 것이 좋습니다.
   - * LDAPS * 사용: LDAPS(LDAP over SSL) 옵션은 TLS를 사용하여 LDAP 서버에 연결합니다. 이 옵션은 호환성을 위해 지원됩니다.
   - * TLS * 사용 안 함: StorageGRID 시스템과 LDAP 서버 간의 네트워크 트래픽은 보호되지 않습니다.

     Active Directory 서버가 LDAP 서명을 적용하는 경우 * TLS 사용 안 함 * 옵션을 사용할 수 없습니다. STARTTLS 또는 LDAPS를 사용해야 합니다.

7. STARTTLS 또는 LDAPS를 선택한 경우 연결 보안에 사용되는 인증서를 선택합니다.
   - * 운영 체제 CA 인증서 사용 *: 운영 체제에 설치된 기본 CA 인증서를 사용하여 연결을 보호합니다.
   - * 사용자 지정 CA 인증서 사용 *: 사용자 지정 보안 인증서를 사용합니다.

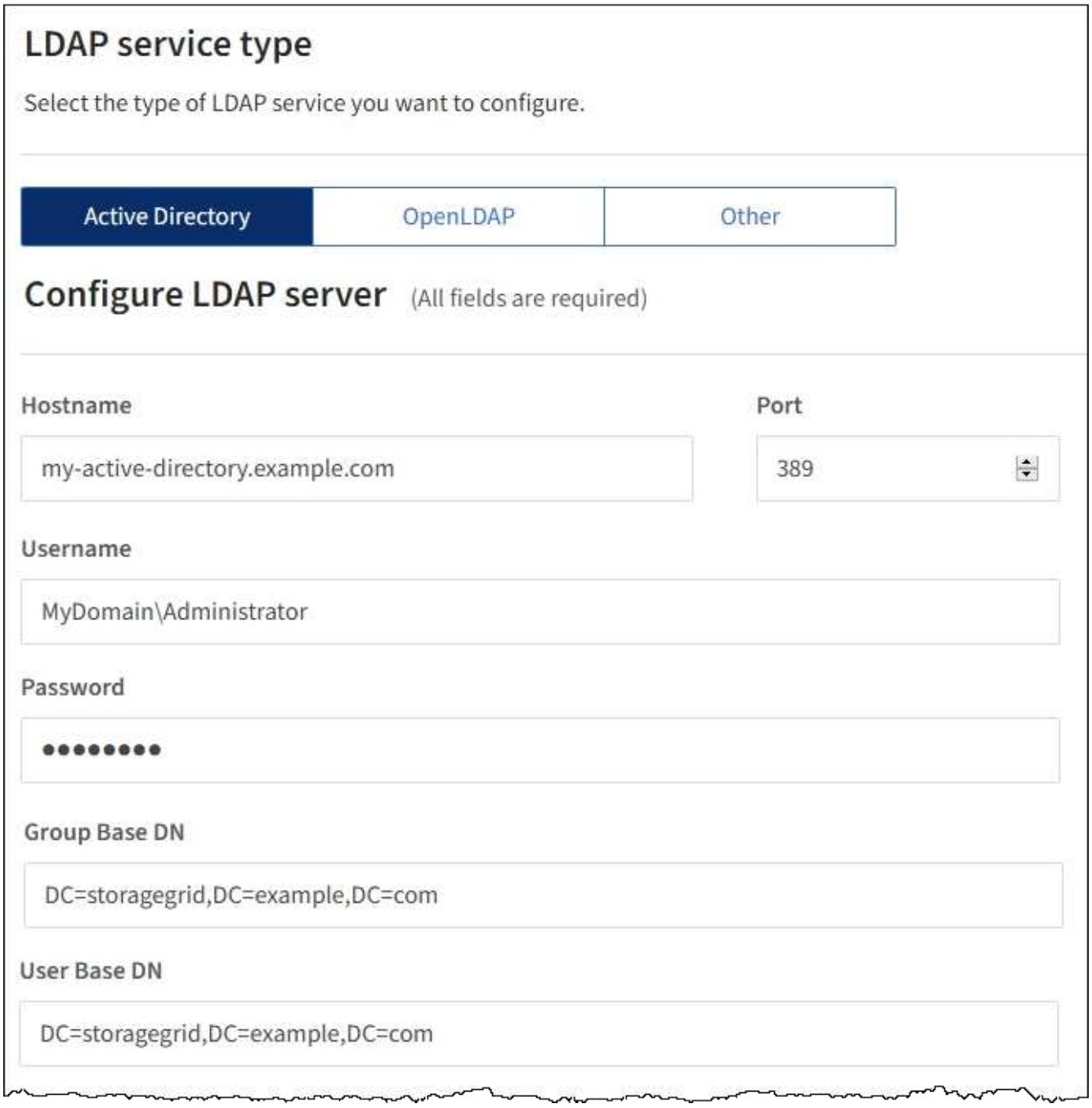
     이 설정을 선택한 경우 사용자 지정 보안 인증서를 복사하여 CA 인증서 텍스트 상자에 붙여 넣습니다.

8. 선택적으로 * 연결 테스트 * 를 선택하여 LDAP 서버에 대한 연결 설정을 확인합니다.

   연결이 유효한 경우 페이지의 오른쪽 상단에 확인 메시지가 나타납니다.

9. 연결이 유효하면 * 저장 * 을 선택합니다.

   다음 스크린샷은 Active Directory를 사용하는 LDAP 서버의 구성 값 예를 보여 줍니다.



관련 정보

"발신 TLS 연결에 지원되는 암호"

"Single Sign-On 사용에 대한 요구 사항"

"테넌트 계정을 생성하는 중입니다"

"테넌트 계정을 사용합니다"

OpenLDAP 서버 구성 지침

OpenLDAP 서버를 ID 페더레이션에 사용하려면 OpenLDAP 서버에서 특정 설정을 구성해야 합니다.

MemberOf 및 구체화 오버레이

MemberOf 및 구체화 오버레이를 활성화해야 합니다. 자세한 내용은 OpenLDAP용 관리자 안내서 에서 역방향 그룹 구성원 유지 관리 지침을 참조하십시오.

인덱싱

지정된 인덱스 키워드를 사용하여 다음 OpenLDAP 속성을 구성해야 합니다.

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

또한 최적의 성능을 위해 사용자 이름 도움말에 언급된 필드를 인덱싱해야 합니다.

OpenLDAP용 관리자 안내서 에서 역방향 그룹 구성원 유지 관리에 대한 정보를 참조하십시오.

관련 정보

"OpenLDAP 설명서: 버전 2.4 관리자 가이드"

ID 소스와 동기화 수행

StorageGRID 시스템은 ID 소스에서 페더레이션 그룹과 사용자를 정기적으로 동기화합니다. 사용자 권한을 최대한 빨리 설정하거나 제한하려는 경우 동기화를 강제로 시작할 수 있습니다.

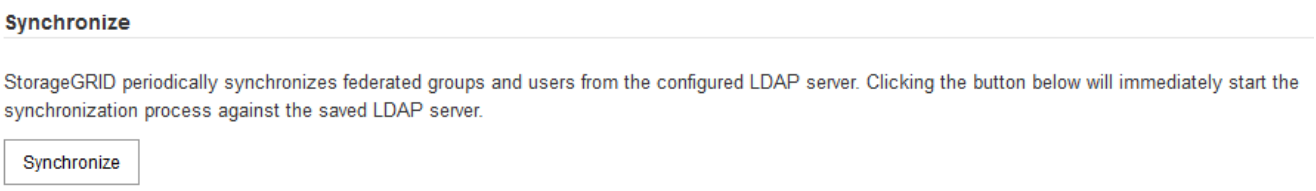
필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.
- ID 소스를 활성화해야 합니다.

단계

1. Configuration * > * Access Control * > * Identity Federation * 을 선택합니다.

   ID 페더레이션 페이지가 나타납니다. 동기화 * 버튼은 페이지 하단에 있습니다.

2. 동기화 * 를 클릭합니다.

   동기화가 성공적으로 시작되었다는 확인 메시지가 표시됩니다. 동기화 프로세스는 환경에 따라 다소 시간이 걸릴 수

있습니다.

ID 소스에서 페더레이션 그룹과 사용자를 동기화하는 데 문제가 있는 경우 * ID 페더레이션 동기화 실패 * 경고가 트리거됩니다.

ID 페더레이션을 사용하지 않도록 설정합니다

그룹 및 사용자에 대한 ID 페더레이션을 일시적으로 또는 영구적으로 비활성화할 수 있습니다. ID 페더레이션을 사용하지 않도록 설정하면 StorageGRID와 ID 소스 간에 통신이 이루어지지 않습니다. 그러나 구성한 설정은 그대로 유지되므로 나중에 ID 페더레이션을 쉽게 다시 사용할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

ID 페더레이션을 사용하지 않도록 설정하기 전에 다음 사항을 확인해야 합니다.

- 페더레이션 사용자는 로그인할 수 없습니다.
- 현재 로그인한 페더레이션 사용자는 세션이 만료될 때까지 StorageGRID 시스템에 대한 액세스 권한을 유지하지만 세션이 만료된 후에는 로그인할 수 없습니다.
- StorageGRID 시스템과 ID 소스 간의 동기화는 수행되지 않으며 동기화되지 않은 계정에 대해 알림 또는 경보가 발생하지 않습니다.
- SSO(Single Sign-On)가 * Enabled * 또는 * Sandbox Mode * 로 설정된 경우 * Enable Identity Federation *(ID 페더레이션 사용 *) 확인란이 비활성화됩니다. ID 페더레이션을 비활성화하려면 Single Sign-On 페이지의 SSO 상태가 * 사용 안 함 * 이어야 합니다.

단계

1. Configuration * > * Access Control * > * Identity Federation * 을 선택합니다.
2. ID 페더레이션 사용 * 확인란의 선택을 취소합니다.
3. 저장 * 을 클릭합니다.

관련 정보

"SSO(Single Sign-On) 비활성화"

관리 그룹 관리

관리자 그룹을 만들어 하나 이상의 관리자 사용자에 대한 보안 권한을 관리할 수 있습니다. StorageGRID 시스템에 대한 액세스 권한을 부여하려면 사용자가 그룹에 속해야 합니다.

관리 그룹 생성 중

관리자 그룹을 사용하면 그리드 관리자 및 그리드 관리 API에서 어떤 기능과 작업에 액세스할 수 있는지 확인할 수 있습니다.

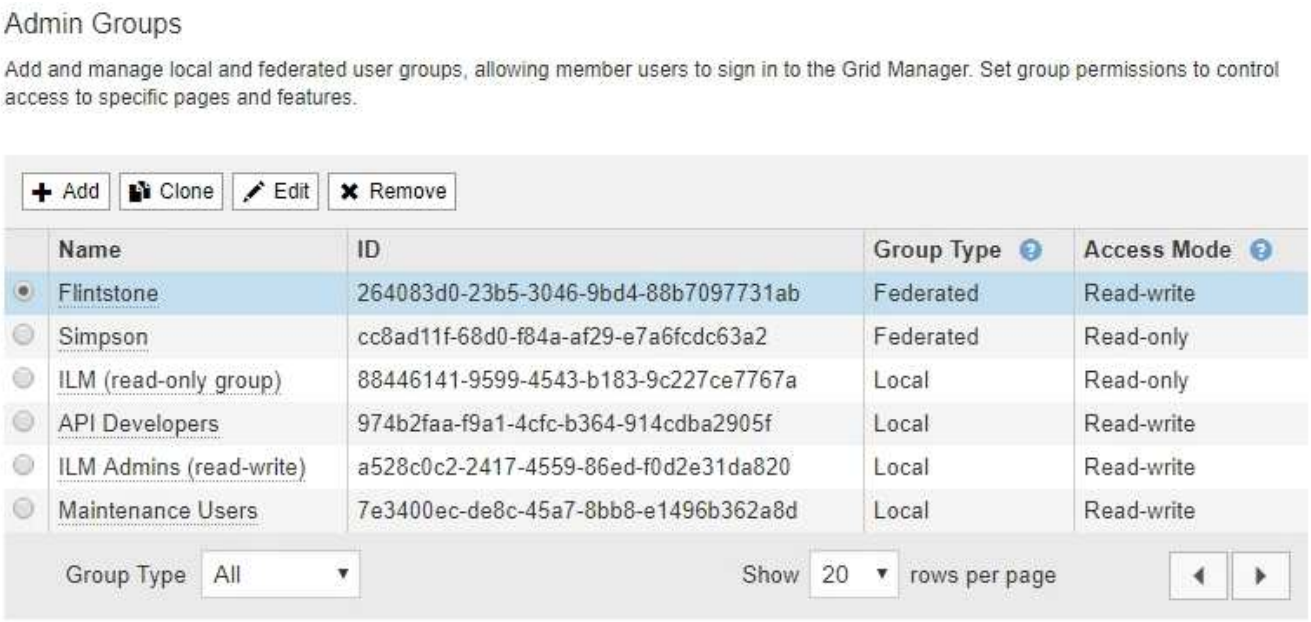
필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.
- 통합 그룹을 가져오려면 ID 페더레이션을 구성해야 하며 통합 그룹은 구성된 ID 소스에 이미 있어야 합니다.

단계

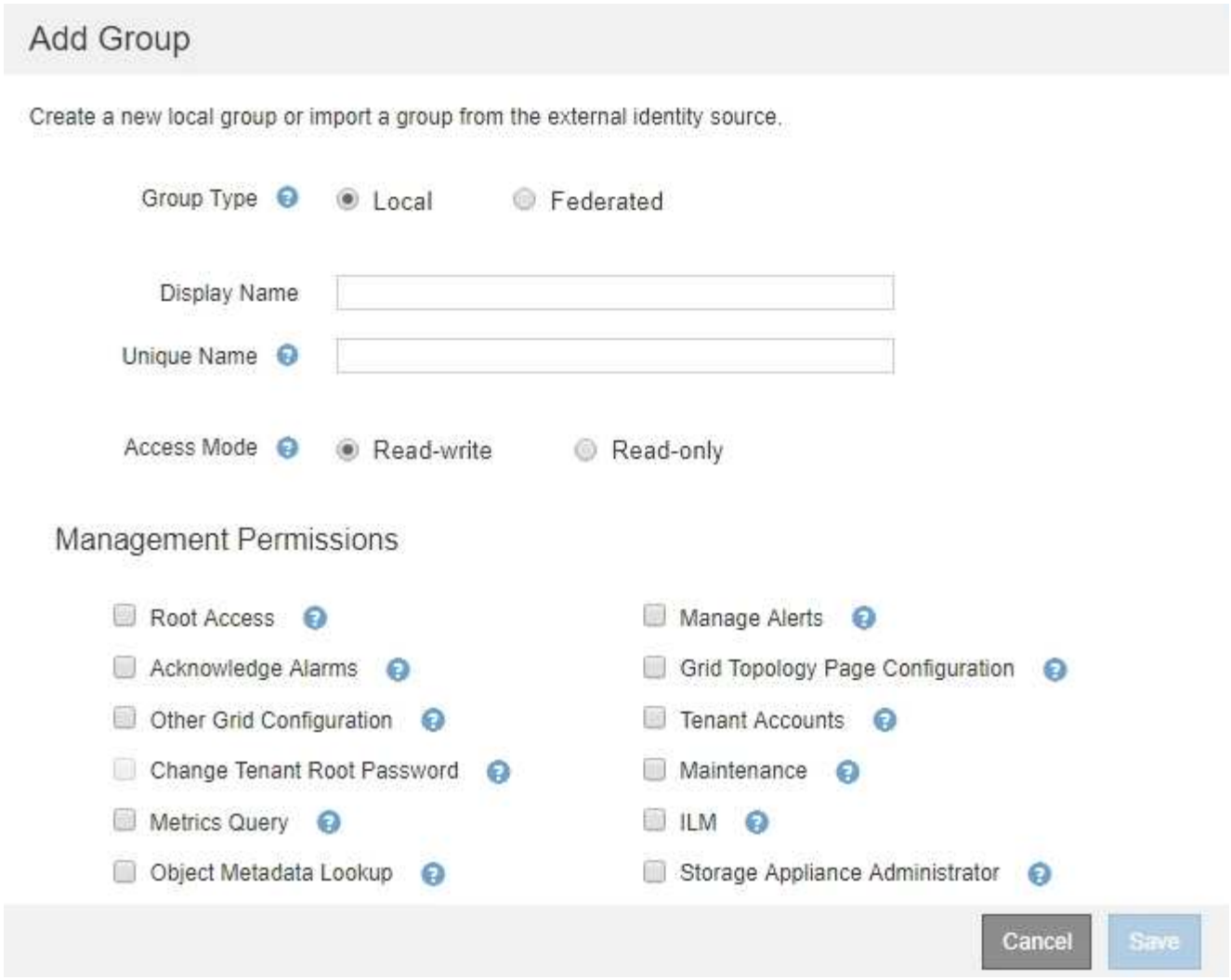
1. Configuration * * * Access Control * * Admin Groups * 를 선택합니다.

   관리 그룹 페이지가 나타나고 기존 관리 그룹이 나열됩니다.



2. 추가 * 를 선택합니다.

   그룹 추가 대화 상자가 나타납니다.



3. 그룹 유형 에서 StorageGRID 내에서만 사용할 그룹을 만들려면 * 로컬 * 을 선택하고, ID 소스에서 그룹을 가져오려면 * 통합 * 을 선택합니다.
4. Local * 을 선택한 경우 그룹의 표시 이름을 입력합니다. 표시 이름은 그리드 관리자에 나타나는 이름입니다. 예를 들어, "유지 보수 사용자" 또는 ""ILM 관리자""가 있습니다.
5. 그룹의 고유한 이름을 입력합니다.
   - * 로컬 *: 원하는 고유한 이름을 입력합니다. 예: ""ILM 관리자""""
   - * Federated *: 구성된 ID 소스에 표시된 대로 그룹의 이름을 정확하게 입력합니다.
6. 액세스 모드 * 의 경우 그룹의 사용자가 그리드 관리자 및 그리드 관리 API에서 설정을 변경하고 작업을 수행할 수 있는지 또는 설정과 기능만 볼 수 있는지 여부를 선택합니다.
   - * 읽기-쓰기 * (기본값): 사용자는 설정을 변경하고 관리 권한에서 허용하는 작업을 수행할 수 있습니다.
   - * 읽기 전용 *: 사용자는 설정 및 기능만 볼 수 있습니다. 그리드 관리자 또는 그리드 관리 API에서 어떠한 변경이나 작업도 수행할 수 없습니다. 로컬 읽기 전용 사용자는 자신의 암호를 변경할 수 있습니다.

> ⓘ 사용자가 여러 그룹에 속해 있고 모든 그룹이 * 읽기 전용 * 으로 설정된 경우 사용자는 선택된 모든 설정 및 기능에 대한 읽기 전용 액세스 권한을 갖게 됩니다.

7. 하나 이상의 관리 권한을 선택합니다.

각 그룹에 적어도 하나의 권한을 할당해야 합니다. 그렇지 않으면 그룹에 속한 사용자가 StorageGRID에 로그인할 수 없습니다.

8. 저장 * 을 선택합니다.

   새 그룹이 생성됩니다. 로컬 그룹인 경우 하나 이상의 사용자를 추가할 수 있습니다. 통합 그룹인 경우 ID 소스는 그룹에 속한 사용자를 관리합니다.

관련 정보

"로컬 사용자 관리"

관리자 그룹 권한

관리자 사용자 그룹을 만들 때 그리드 관리자의 특정 기능에 대한 액세스를 제어하는 권한을 하나 이상 선택합니다. 그런 다음 각 사용자를 이러한 관리 그룹 중 하나 이상에 할당하여 사용자가 수행할 수 있는 작업을 결정할 수 있습니다.

각 그룹에 적어도 하나의 권한을 할당해야 합니다. 그렇지 않으면 해당 그룹에 속한 사용자가 Grid Manager에 로그인할 수 없습니다.

기본적으로 하나 이상의 사용 권한이 있는 그룹에 속한 사용자는 다음 작업을 수행할 수 있습니다.

- Grid Manager에 로그인합니다
- 대시보드 보기
- 노드 페이지를 봅니다
- 그리드 토폴로지를 모니터링합니다
- 현재 및 해결된 경고를 봅니다
- 현재 및 과거 알람 보기(레거시 시스템)
- 자신의 암호 변경(로컬 사용자만 해당)
- 구성 및 유지 관리 페이지에서 특정 정보를 봅니다

다음 섹션에서는 관리자 그룹을 만들거나 편집할 때 할당할 수 있는 권한에 대해 설명합니다. 명시적으로 언급되지 않은 기능을 사용하려면 루트 액세스 권한이 필요합니다.

루트 액세스

이 권한은 모든 그리드 관리 기능에 대한 액세스를 제공합니다.

알림 관리

이 권한은 알림 관리 옵션에 대한 액세스를 제공합니다. 사용자는 이 권한을 가지고 있어야 Silence, 경고 알림 및 경고 규칙을 관리할 수 있습니다.

알람 확인(레거시 시스템)

이 권한을 통해 알람(레거시 시스템)을 확인하고 이에 대응할 수 있습니다. 로그인한 모든 사용자는 현재 및 과거 알람을 볼 수 있습니다.

사용자가 그리드 토폴로지를 모니터링하고 알람을 확인하려면 이 권한을 할당해야 합니다.

그리드 토폴로지 페이지 구성

이 권한을 통해 다음 메뉴 옵션에 액세스할 수 있습니다.

- 지원 * * 도구 * 그리드 토폴로지 * 의 페이지에서 사용할 수 있는 구성 탭.
- * 노드 * * 이벤트 * 탭에서 이벤트 카운트 * 링크를 재설정합니다.

기타 그리드 구성

이 권한은 추가 그리드 구성 옵션에 대한 액세스를 제공합니다.

이러한 추가 옵션을 보려면 그리드 토폴로지 페이지 구성 권한도 있어야 합니다.

- 알람 * (레거시 시스템):
  - 전체 알람
  - 레거시 이메일 설정
- * ILM *:
  - 스토리지 풀
  - 보관 등급
- * 구성 * * 네트워크 설정 *
  - 링크 비용
- * 구성 * * 시스템 설정 *:
  - 표시 옵션
  - 그리드 옵션
  - 스토리지 옵션
- * 구성 * * 모니터링 *:
  - 이벤트
- * 지원 *:
  - AutoSupport

테넌트 계정

이 권한은 * Tenants * * * Tenant Accounts * 페이지에 대한 액세스를 제공합니다.

Grid Management API 버전 1(더 이상 사용되지 않음)에서는 이 권한을 사용하여 테넌트 그룹 정책을 관리하고, Swift 관리자 암호를 재설정하고, 루트 사용자 S3 액세스 키를 관리합니다.

테넌트 루트 암호를 변경합니다

이 권한은 테넌트 계정 페이지의 * 루트 암호 변경 * 옵션에 대한 액세스를 제공하므로 테넌트의 로컬 루트 사용자에 대한 암호를 변경할 수 있는 사용자를 제어할 수 있습니다. 이 권한이 없는 사용자는 * 루트 암호 변경 * 옵션을 볼 수 없습니다.

이 권한을 할당하려면 먼저 그룹에 테넌트 계정 권한을 할당해야 합니다.

유지 관리

이 권한을 통해 다음 메뉴 옵션에 액세스할 수 있습니다.

- * 구성 * * 시스템 설정 *:
  - 도메인 이름 *
  - 서버 인증서 *
- * 구성 * * 모니터링 *:
  - 감사 *
- * 구성 * * 액세스 제어 *:
  - 그리드 암호
- * 유지보수 * * 유지보수 태스크 *
  - 서비스 해제
  - 확장
  - 복구
- * 유지보수 * * 네트워크 *:
  - DNS 서버 *
  - 그리드 네트워크 *
  - NTP 서버 *
- * 유지보수 * * 시스템 *:
  - 라이센스 *
  - 복구 패키지
  - 소프트웨어 업데이트
- * 지원 * * 툴 *:
  - 로그
- 유지 관리 권한이 없는 사용자는 별표가 표시된 페이지를 볼 수는 있지만 편집할 수는 없습니다.

메트릭 쿼리

이 권한은 * 지원 * * 도구 * 메트릭 * 페이지에 대한 액세스를 제공합니다. 이 권한은 또한 Grid Management API의 * Metrics * 섹션을 사용하여 맞춤형 Prometheus 메트릭 쿼리에 대한 액세스를 제공합니다.

ILM을 참조하십시오

이 권한은 다음 * ILM * 메뉴 옵션에 대한 액세스를 제공합니다.

- * 삭제 코딩 *
- * 규칙 *

- * 정책 *
- * 지역 *

ILM * * * 스토리지 풀 * 및 * ILM * * 스토리지 등급 * 메뉴 옵션에 대한 액세스는 다른 그리드 구성 및 그리드 토폴로지 페이지 구성 권한에 의해 제어됩니다.

개체 메타데이터 조회

이 권한은 * ILM * * 개체 메타데이터 조회 * 메뉴 옵션에 대한 액세스를 제공합니다.

스토리지 어플라이언스 관리자

이 권한은 그리드 관리자를 통해 스토리지 어플라이언스에서 E-Series SANtricity System Manager에 대한 액세스를 제공합니다.

사용 권한과 액세스 모드 간의 상호 작용

모든 권한에 대해 그룹의 액세스 모드 설정은 사용자가 설정을 변경하고 작업을 수행할 수 있는지 또는 관련 설정과 기능만 볼 수 있는지 여부를 결정합니다. 사용자가 여러 그룹에 속해 있고 모든 그룹이 * 읽기 전용 * 으로 설정된 경우 사용자는 선택된 모든 설정 및 기능에 대한 읽기 전용 액세스 권한을 갖게 됩니다.

Grid Management API에서 기능 비활성화

그리드 관리 API를 사용하여 StorageGRID 시스템의 특정 기능을 완전히 비활성화할 수 있습니다. 기능이 비활성화되면 해당 기능과 관련된 작업을 수행할 수 있는 권한을 아무도 할당할 수 없습니다.

이 작업에 대해

비활성화된 기능 시스템을 사용하면 StorageGRID 시스템의 특정 기능에 액세스하지 못하게 할 수 있습니다. 루트 액세스 권한이 있는 관리자 그룹에 속한 루트 사용자나 사용자가 해당 기능을 사용할 수 없도록 하는 유일한 방법은 기능을 비활성화하는 것입니다.

이 기능이 어떻게 유용한지 이해하려면 다음 시나리오를 고려해 보십시오.

_Company A는 테넌트 계정을 생성하여 StorageGRID 시스템의 스토리지 용량을 임대하는 서비스 공급자입니다. 회사 A는 임차자의 객체 보안을 보호하기 위해 계정이 배포된 후 자신의 직원이 테넌트 계정에 액세스할 수 없도록 하려고 합니다. _

_회사 A는 그리드 관리 API에서 기능 비활성화 시스템을 사용하여 이 목표를 달성할 수 있습니다. 그리드 관리자(UI 및 API 모두)에서 * 테넌트 루트 암호 변경 * 기능을 완전히 비활성화함으로써 회사 A는 루트 액세스 권한이 있는 그룹에 속하는 루트 사용자 및 루트 사용자를 포함한 관리자 사용자가 테넌트 계정의 루트 사용자에 대한 암호를 변경할 수 없도록 할 수 있습니다

비활성화된 피처를 다시 활성화합니다

기본적으로 그리드 관리 API를 사용하여 비활성화된 기능을 다시 활성화할 수 있습니다. 그러나 비활성화된 피처가 다시 활성화되지 않도록 하려면 * activateFeatures * 기능 자체를 비활성화할 수 있습니다.

activateFeatures * 기능은 다시 활성화할 수 없습니다. 이 기능을 비활성화하려는 경우 비활성화된 다른 모든 기능을 다시 활성화할 수 있는 기능이 영구적으로 손실됩니다. 손실된 기능을 복원하려면 기술 지원 부서에 문의해야 합니다.

자세한 내용은 S3 또는 Swift 클라이언트 애플리케이션 구현 지침을 참조하십시오.

단계

1. Grid Management API에 대한 Swagger 문서에 액세스합니다.
2. 기능 비활성화 끝점을 찾습니다.
3. 테넌트 루트 암호 변경 * 과 같은 기능을 비활성화하려면 다음과 같이 API로 본문을 보냅니다.

```
{ "grid": {"changeTenantRootPassword": true} }
```

요청이 완료되면 테넌트 루트 암호 변경 기능이 비활성화됩니다. 테넌트 루트 암호 변경 관리 권한이 사용자 인터페이스에 더 이상 나타나지 않으며 테넌트의 루트 암호를 변경하려고 시도하는 모든 API 요청이 "'403 사용 금지'"로 실패합니다.

4. 모든 기능을 다시 활성화하려면 다음과 같이 API로 본문을 보내십시오.

```
{ "grid": null }
```

이 요청이 완료되면 테넌트 루트 암호 변경 기능을 포함한 모든 기능이 다시 활성화됩니다. 이제 사용자 인터페이스에 테넌트 루트 암호 변경 관리 권한이 표시되며, 사용자에게 루트 액세스 또는 테넌트 루트 암호 변경 관리 권한이 있는 경우 테넌트의 루트 암호를 변경하려고 시도하는 모든 API 요청이 성공합니다.

> 이전 예에서는 _ALL_DEACTED 피처가 재활성화됩니다. 비활성화된 상태로 유지되어야 하는 다른 기능이 비활성화된 경우, PUT 요청에 명시적으로 지정해야 합니다. 예를 들어, Change Tenant Root Password 기능을 다시 활성화하고 Alarm Acknowledgement 기능을 계속 비활성화하려면 다음 Put 요청을 보냅니다.

```
{ "grid": { "alarmAcknowledgment": true } }
```

관련 정보

"Grid Management API 사용"

관리 그룹 수정

admin 그룹을 수정하여 그룹과 연결된 권한을 변경할 수 있습니다. 로컬 관리자 그룹의 경우 표시 이름을 업데이트할 수도 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

단계

1. Configuration * * * Access Control * * Admin Groups * 를 선택합니다.
2. 그룹을 선택합니다.

시스템에 20개 이상의 항목이 포함된 경우 각 페이지에 한 번에 표시되는 행 수를 지정할 수 있습니다. 그런 다음 브라우저의 찾기 기능을 사용하여 현재 표시된 행에서 특정 항목을 검색할 수 있습니다.

3. 편집 * 을 클릭합니다.
4. 또는 로컬 그룹의 경우 사용자에게 표시할 그룹 이름(예: " 유지보수 사용자")을 입력합니다.

   내부 그룹 이름인 고유한 이름은 변경할 수 없습니다.

5. 선택적으로 그룹의 액세스 모드를 변경합니다.
   - * 읽기-쓰기 * (기본값): 사용자는 설정을 변경하고 관리 권한에서 허용하는 작업을 수행할 수 있습니다.
   - * 읽기 전용 *: 사용자는 설정 및 기능만 볼 수 있습니다. 그리드 관리자 또는 그리드 관리 API에서 어떠한 변경이나 작업도 수행할 수 없습니다. 로컬 읽기 전용 사용자는 자신의 암호를 변경할 수 있습니다.

   > 사용자가 여러 그룹에 속해 있고 모든 그룹이 * 읽기 전용 * 으로 설정된 경우 사용자는 선택된 모든 설정 및 기능에 대한 읽기 전용 액세스 권한을 갖게 됩니다.

6. 필요에 따라 그룹 권한을 추가하거나 제거합니다.

   관리자 그룹 권한에 대한 정보를 봅니다.

7. 저장 * 을 선택합니다.

관련 정보

관리자 그룹 권한

관리 그룹 삭제

시스템에서 그룹을 제거하고 그룹과 관련된 모든 권한을 제거하려면 관리자 그룹을 삭제할 수 있습니다. admin 그룹을 삭제하면 그룹에서 모든 admin 사용자가 제거되지만 admin 사용자는 삭제되지 않습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

그룹을 삭제하면 다른 그룹에 의해 권한을 부여하지 않는 한 해당 그룹에 할당된 사용자는 그리드 관리자에 대한 모든 액세스 권한을 잃게 됩니다.

단계

1. Configuration * * * Access Control * * Admin Groups * 를 선택합니다.
2. 그룹 이름을 선택합니다.

   시스템에 20개 이상의 항목이 포함된 경우 각 페이지에 한 번에 표시되는 행 수를 지정할 수 있습니다. 그런 다음 브라우저의 찾기 기능을 사용하여 현재 표시된 행에서 특정 항목을 검색할 수 있습니다.

3. 제거 * 를 선택합니다.
4. OK * 를 선택합니다.

로컬 사용자 관리

로컬 사용자를 만들고 로컬 관리자 그룹에 할당하여 이러한 사용자가 액세스할 수 있는 그리드 관리자 기능을 결정할 수 있습니다.

Grid Manager에는 ""root""라는 이름의 미리 정의된 로컬 사용자가 하나 있습니다. 로컬 사용자를 추가 및 제거할 수는 있지만 루트 사용자는 제거할 수 없습니다.

SSO(Single Sign-On)가 활성화된 경우 로컬 사용자는 StorageGRID에 로그인할 수 없습니다.

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

로컬 사용자 생성

로컬 관리자 그룹을 생성한 경우 하나 이상의 로컬 사용자를 생성하고 각 사용자를 하나 이상의 그룹에 할당할 수 있습니다. 그룹의 권한은 사용자가 액세스할 수 있는 Grid Manager 기능을 제어합니다.

이 작업에 대해

로컬 사용자만 생성할 수 있으며 이러한 사용자는 로컬 관리자 그룹에만 할당할 수 있습니다. 통합 사용자 및 통합 그룹은 외부 ID 소스를 사용하여 관리됩니다.

단계

1. Configuration * > * Access Control * > * Admin Users * 를 선택합니다.
2. Create * 를 클릭합니다.
3. 사용자의 표시 이름, 고유 이름 및 암호를 입력합니다.
4. 액세스 권한을 제어하는 하나 이상의 그룹에 사용자를 할당합니다.

   그룹 이름 목록은 그룹 테이블에서 생성됩니다.

5. 저장 * 을 클릭합니다.

관련 정보

"관리 그룹 관리"

로컬 사용자 계정 수정

로컬 관리자 사용자 계정을 수정하여 사용자의 표시 이름 또는 그룹 구성원을 업데이트할 수 있습니다. 또한 사용자가 일시적으로 시스템에 액세스하지 못하도록 할 수도 있습니다.

이 작업에 대해

로컬 사용자만 편집할 수 있습니다. 통합 사용자 세부 정보는 외부 ID 소스와 자동으로 동기화됩니다.

단계

1. Configuration * > * Access Control * > * Admin Users * 를 선택합니다.
2. 편집할 사용자를 선택합니다.

시스템에 20개 이상의 항목이 포함된 경우 각 페이지에 한 번에 표시되는 행 수를 지정할 수 있습니다. 그런 다음 브라우저의 찾기 기능을 사용하여 현재 표시된 행에서 특정 항목을 검색할 수 있습니다.

3. 편집 * 을 클릭합니다.
4. 필요에 따라 이름 또는 그룹 구성원을 변경합니다.
5. 선택적으로 사용자가 시스템에 일시적으로 액세스하지 못하게 하려면 * 액세스 거부 * 를 선택합니다.
6. 저장 * 을 클릭합니다.

다음 번에 사용자가 로그아웃한 다음 그리드 관리자에 다시 로그인할 때 새 설정이 적용됩니다.

로컬 사용자 계정을 삭제하는 중입니다

더 이상 Grid Manager에 액세스할 필요가 없는 로컬 사용자의 계정을 삭제할 수 있습니다.

단계

1. Configuration * > * Access Control * > * Admin Users * 를 선택합니다.
2. 삭제할 로컬 사용자를 선택합니다.

사전 정의된 루트 로컬 사용자는 삭제할 수 없습니다.

시스템에 20개 이상의 항목이 포함된 경우 각 페이지에 한 번에 표시되는 행 수를 지정할 수 있습니다. 그런 다음 브라우저의 찾기 기능을 사용하여 현재 표시된 행에서 특정 항목을 검색할 수 있습니다.

3. 제거 * 를 클릭합니다.
4. 확인 * 을 클릭합니다.

로컬 사용자 암호 변경

로컬 사용자는 Grid Manager 배너의 * Change Password * 옵션을 사용하여 자신의 암호를 변경할 수 있습니다. 또한 관리자 사용자 페이지에 액세스할 수 있는 사용자는 다른 로컬 사용자의 암호를 변경할 수 있습니다.

이 작업에 대해

로컬 사용자의 암호만 변경할 수 있습니다. 통합 사용자는 외부 ID 원본에서 자신의 암호를 변경해야 합니다.

단계

1. Configuration * > * Access Control * > * Admin Users * 를 선택합니다.
2. 사용자 페이지에서 사용자를 선택합니다.

시스템에 20개 이상의 항목이 포함된 경우 각 페이지에 한 번에 표시되는 행 수를 지정할 수 있습니다. 그런 다음 브라우저의 찾기 기능을 사용하여 현재 표시된 행에서 특정 항목을 검색할 수 있습니다.

3. 암호 변경 * 을 클릭합니다.
4. 암호를 입력 및 확인하고 * 저장 * 을 클릭합니다.

StorageGRID용 SSO(Single Sign-On) 사용

StorageGRID 시스템은 SAML 2.0(Security Assertion Markup Language 2.0) 표준을 사용하여 SSO(Single Sign-On)를 지원합니다. SSO가 활성화된 경우 모든 사용자는 Grid Manager, Tenant Manager, Grid Management API 또는 Tenant Management API에 액세스하기 전에 외부 ID 공급자에 의해 인증되어야 합니다. 로컬 사용자는 StorageGRID에 로그인할 수 없습니다.

- "Single Sign-On의 작동 방식"
- "Single Sign-On 사용에 대한 요구 사항"
- "Single Sign-On 구성"

Single Sign-On의 작동 방식

SSO(Single Sign-On)를 활성화하기 전에 SSO를 사용할 때 StorageGRID 로그인 및 로그아웃 프로세스가 어떻게 영향을 받는지 검토하십시오.

SSO가 활성화되어 있을 때 로그인합니다

SSO가 활성화되어 있고 StorageGRID에 로그인하면 조직의 SSO 페이지로 리디렉션되어 자격 증명을 검증합니다.

단계

1. 웹 브라우저에 StorageGRID 관리 노드의 정규화된 도메인 이름 또는 IP 주소를 입력합니다.

   StorageGRID 로그인 페이지가 나타납니다.

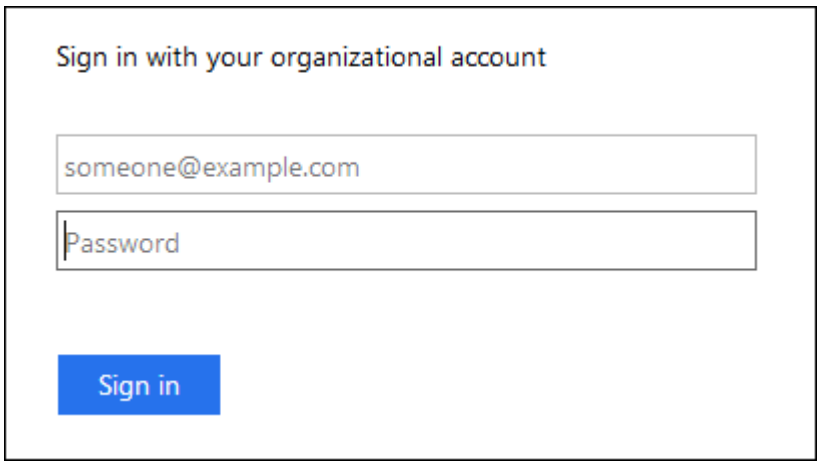
   - 이 브라우저에서 URL에 처음 액세스한 경우 계정 ID를 입력하라는 메시지가 표시됩니다.

   - 이전에 Grid Manager 또는 Tenant Manager에 액세스한 경우, 최근 계정을 선택하거나 계정 ID를 입력하라는 메시지가 나타납니다.

테넌트 계정의 전체 URL(즉, 정규화된 도메인 이름 또는 IP 주소 뒤에 오는)을 입력하면 StorageGRID 로그인 페이지가 표시되지 않습니다 `/?accountId=20-digit-account-id`)를 클릭합니다. 대신 조직의 SSO 로그인 페이지로 즉시 리디렉션됩니다. 여기에서 해당 페이지로 이동할 수 있습니다 SSO 자격 증명으로 로그인합니다.

2. 그리드 관리자 또는 테넌트 관리자에 액세스할지 여부를 지정합니다.
   - Grid Manager에 액세스하려면 **Account ID** 필드를 비워 두고 계정 ID로 * 0 * 을 입력하거나, 최근 계정 목록에 * Grid Manager * 를 선택합니다.
   - Tenant Manager에 액세스하려면 20자리 테넌트 계정 ID를 입력하거나 최근 계정 목록에 나타나는 경우 이름으로 Tenant를 선택합니다.
3. 로그인 * 을 클릭합니다

   StorageGRID가 조직의 SSO 로그인 페이지로 리디렉션합니다. 예를 들면 다음과 같습니다.



4. SSO 자격 증명으로 로그인합니다.

   SSO 자격 증명이 올바른 경우:

   a. IDP(Identity Provider)는 StorageGRID에 인증 응답을 제공합니다.
   b. StorageGRID는 인증 응답을 검증합니다.
   c. 응답이 유효하고 적절한 액세스 권한이 있는 통합 그룹에 속해 있는 경우 선택한 계정에 따라 Grid Manager

또는 Tenant Manager에 로그인됩니다.

5. 필요한 경우 다른 관리 노드에 액세스하거나 적절한 권한이 있는 경우 그리드 관리자 또는 테넌트 관리자에 액세스합니다.

   SSO 자격 증명을 다시 입력하지 않아도 됩니다.

SSO가 활성화된 경우 로그아웃합니다

StorageGRID에 대해 SSO가 활성화된 경우 로그아웃할 때 발생하는 작업은 로그인한 대상 및 로그아웃 위치에 따라 달라집니다.

단계

1. 사용자 인터페이스의 오른쪽 상단 모서리에 있는 * 로그아웃 * 링크를 찾습니다.
2. 로그아웃 * 을 클릭합니다.

   StorageGRID 로그인 페이지가 나타납니다. 최근 계정 * 드롭다운은 * 그리드 관리자 * 또는 테넌트 이름을 포함하도록 업데이트되므로 나중에 이러한 사용자 인터페이스에 보다 빠르게 액세스할 수 있습니다.

에 로그인한 경우...	에서 로그아웃합니다.	에서 로그아웃되었습니다...
하나 이상의 관리 노드에서 그리드 관리자	모든 관리 노드의 그리드 관리자	모든 관리 노드의 그리드 관리자
하나 이상의 관리 노드에서 테넌트 관리자	모든 관리 노드의 테넌트 관리자	모든 관리 노드의 테넌트 관리자
Grid Manager와 Tenant Manager 모두	그리드 관리자	그리드 관리자 전용. SSO에서 로그아웃하려면 테넌트 관리자에서 로그아웃해야 합니다.

> 이 표에는 단일 브라우저 세션을 사용하는 경우 로그아웃할 때 발생하는 동작이 요약되어 있습니다. 여러 브라우저 세션에서 StorageGRID에 로그인한 경우 모든 브라우저 세션에서 별도로 로그아웃해야 합니다.

Single Sign-On 사용에 대한 요구 사항

StorageGRID 시스템에 대해 SSO(Single Sign-On)를 활성화하기 전에 이 섹션의 요구 사항을 검토하십시오.

> 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.

ID 공급자 요구 사항

SSO의 ID 공급자(IDP)는 다음 요구 사항을 충족해야 합니다.

- 다음 AD FS(Active Directory Federation Service) 버전 중 하나:

- AD FS 4.0, Windows Server 2016에 포함되어 있습니다

  Windows Server 2016에서 을 사용해야 합니다 "KB3201845 업데이트"또는 그 이상.

- AD FS 3.0, Windows Server 2012 R2 업데이트 이상에 포함되어 있습니다.

- TLS(전송 계층 보안) 1.2 또는 1.3
- Microsoft .NET Framework 버전 3.5.1 이상

서버 인증서 요구 사항

StorageGRID는 각 관리 노드의 관리 인터페이스 서버 인증서를 사용하여 그리드 관리자, 테넌트 관리자, 그리드 관리 API 및 테넌트 관리 API에 대한 액세스를 보호합니다. AD FS에서 StorageGRID에 대한 SSO 기반 당사자 트러스트를 구성하는 경우 서버 인증서를 AD FS에 대한 StorageGRID 요청에 대한 서명 인증서로 사용합니다.

관리 인터페이스에 대한 사용자 지정 서버 인증서를 아직 설치하지 않았다면 지금 설치해야 합니다. 사용자 지정 서버 인증서를 설치하면 모든 관리 노드에 사용되며 모든 StorageGRID 사용 상대 트러스트에 사용할 수 있습니다.

AD FS 기반 당사자 신뢰에서 관리 노드의 기본 서버 인증서를 사용하는 것은 권장되지 않습니다. 노드가 실패하고 복구되면 새로운 기본 서버 인증서가 생성됩니다. 복구된 노드에 로그인하려면 먼저 AD FS의 기반 당사자 신뢰를 새 인증서로 업데이트해야 합니다.

노드의 명령 셸에 로그인하고 로 이동하여 관리 노드의 서버 인증서에 액세스할 수 있습니다 `/var/local/mgmt-api` 디렉토리. 사용자 지정 서버 인증서의 이름이 지정됩니다 `custom-server.crt`. 노드의 기본 서버 인증서 이름은 입니다 `server.crt`.

관련 정보

"방화벽을 통한 액세스 제어"

"Grid Manager 및 테넌트 관리자에 대한 사용자 지정 서버 인증서 구성"

Single Sign-On 구성

SSO(Single Sign-On)가 활성화된 경우 사용자는 조직에서 구현한 SSO 로그인 프로세스를 사용하여 자격 증명이 승인된 경우에만 Grid Manager, Tenant Manager, Grid Management API 또는 Tenant Management API에 액세스할 수 있습니다.

- "페더레이션 사용자가 로그인할 수 있는지 확인합니다"
- "sandbox 모드 사용"
- "AD FS에서 기반 당사자 신뢰를 생성합니다"
- "신뢰할 수 있는 당사자 신뢰 테스트"
- "SSO(Single Sign-On) 활성화"
- "SSO(Single Sign-On) 비활성화"
- "하나의 관리 노드에 대해 SSO(Single Sign-On)를 일시적으로 비활성화 및 다시 활성화합니다"

SSO(Single Sign-On)를 활성화하기 전에 하나 이상의 통합 사용자가 Grid Manager에 로그인하고 기존 테넌트 계정에 대한 테넌트 관리자에 로그인할 수 있는지 확인해야 합니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.
- 통합 ID 소스로 Active Directory를 사용하고 ID 공급자로 AD FS를 사용하고 있습니다.

  "Single Sign-On 사용에 대한 요구 사항"

단계

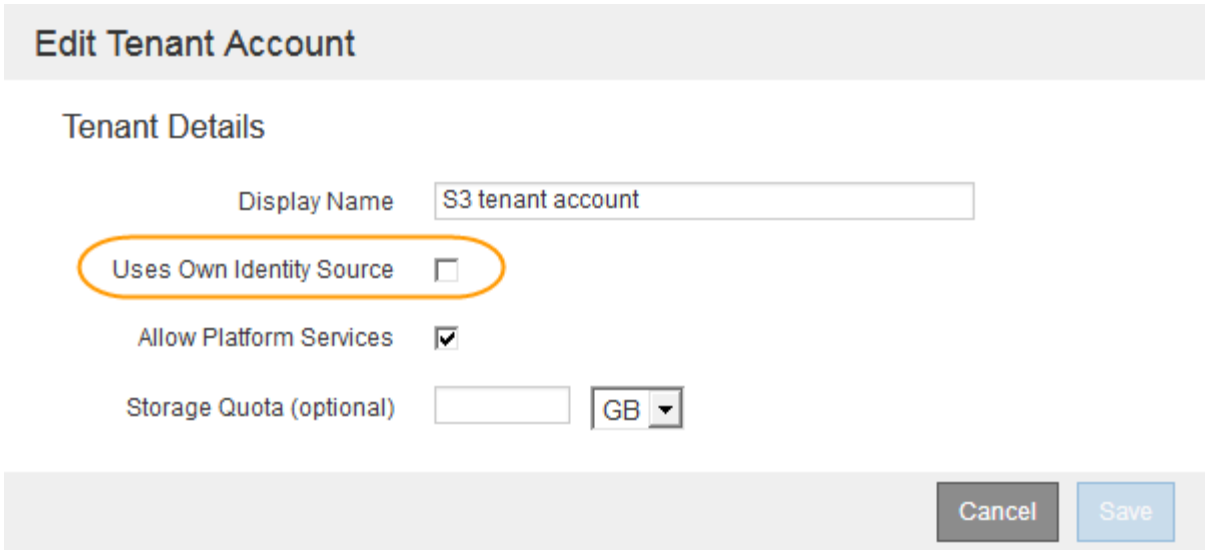
1. 기존 테넌트 계정이 있는 경우 해당 테넌트가 자신의 ID 소스를 사용하고 있지 않은지 확인합니다.

   SSO를 활성화하면 테넌트 관리자에 구성된 ID 소스가 그리드 관리자에 구성된 ID 소스에 의해 재정의됩니다. 테넌트의 ID 소스에 속하는 사용자는 Grid Manager ID 소스의 계정이 없으면 더 이상 로그인할 수 없습니다.

   a. 각 테넌트 계정의 테넌트 관리자에 로그인합니다.
   b. 액세스 제어 * > * ID 페더레이션 * 을 선택합니다.
   c. ID 페더레이션 사용 * 확인란이 선택되지 않았는지 확인합니다.
   d. 이 경우 이 테넌트 계정에 사용 중인 모든 통합 그룹이 더 이상 필요하지 않은지 확인하고 확인란의 선택을 취소하고 * Save * 를 클릭합니다.

2. 통합 사용자가 Grid Manager에 액세스할 수 있는지 확인합니다.
   a. Grid Manager에서 * 구성 * > * 액세스 제어 * > * 관리 그룹 * 을 선택합니다.
   b. Active Directory ID 소스에서 하나 이상의 통합 그룹을 가져오고 루트 액세스 권한이 할당되었는지 확인합니다.
   c. 로그아웃합니다.
   d. 통합 그룹의 사용자로 그리드 관리자에 다시 로그인할 수 있는지 확인합니다.

3. 기존 테넌트 계정이 있는 경우 루트 액세스 권한이 있는 페더레이션 사용자가 로그인할 수 있는지 확인합니다.
   a. Grid Manager에서 * Tenants * 를 선택합니다.
   b. 테넌트 계정을 선택하고 * 계정 편집 * 을 클릭합니다.
   c. [고유 ID 소스 사용] * 확인란을 선택한 경우 상자의 선택을 취소하고 [저장]을 클릭합니다.



테넌트 계정 페이지가 나타납니다.

a. 테넌트 계정을 선택하고 * 로그인 * 을 클릭한 다음 테넌트 계정에 로컬 루트 사용자로 로그인합니다.
b. 테넌트 관리자에서 * 액세스 제어 * > * 그룹 * 을 클릭합니다.
c. Grid Manager에서 하나 이상의 통합 그룹에 이 테넌트에 대한 루트 액세스 권한이 할당되었는지 확인합니다.
d. 로그아웃합니다.
e. 통합 그룹의 사용자로 테넌트에 다시 로그인할 수 있는지 확인합니다.

관련 정보

"Single Sign-On 사용에 대한 요구 사항"

"관리 그룹 관리"

"테넌트 계정을 사용합니다"

sandbox 모드 사용

StorageGRID 사용자에 대해 SSO(Single Sign-On)를 적용하기 전에 샌드박스 모드를 사용하여 AD FS(Active Directory Federation Services) 기반 당사자 트러스트를 구성 및 테스트할 수 있습니다. SSO를 사용하도록 설정한 후 샌드박스 모드를 다시 활성화하여 새로운 신뢰할 수 있는 기존 및 기존의 트러스트를 구성하거나 테스트할 수 있습니다. sandbox 모드를 다시 활성화하면 StorageGRID 사용자에 대해 SSO가 일시적으로 비활성화됩니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

SSO가 활성화되어 있고 사용자가 관리자 노드에 로그인을 시도하면 StorageGRID는 AD FS에 인증 요청을 보냅니다. 그런 다음 AD FS는 인증 요청을 성공했는지 여부를 나타내는 인증 응답을 StorageGRID로 다시 보냅니다. 요청에 성공하려면 사용자의 UUID(Universally Unique Identifier)가 응답에 포함됩니다.

StorageGRID(서비스 공급자) 및 AD FS(ID 공급자)가 사용자 인증 요청에 대해 안전하게 통신할 수 있도록 하려면 StorageGRID에서 특정 설정을 구성해야 합니다. 그런 다음 AD FS를 사용하여 모든 관리 노드에 대한 신뢰할 수 있는 상대 트러스트를 만들어야 합니다. 마지막으로 StorageGRID로 돌아가서 SSO를 활성화해야 합니다.

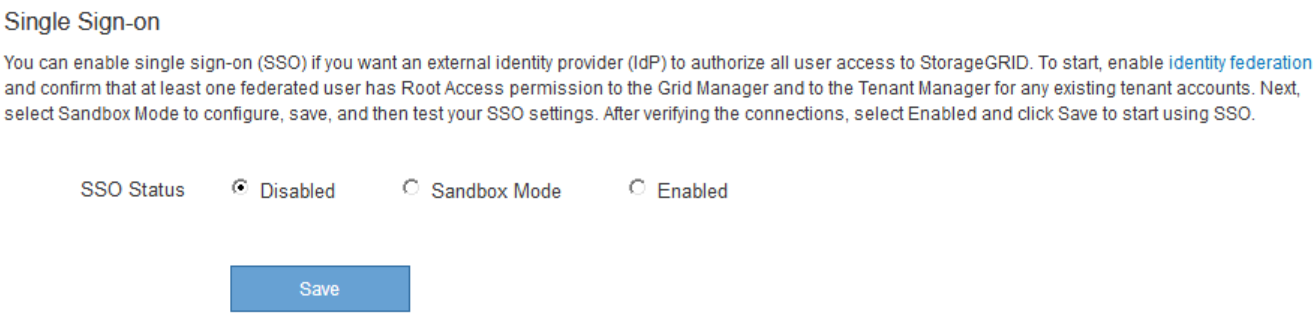
sandbox 모드를 사용하면 SSO를 활성화하기 전에 이 전면과 후면을 간편하게 구성하고 모든 설정을 테스트할 수 있습니다.

sandbox 모드를 사용하는 것이 좋지만 반드시 필요한 것은 아닙니다. StorageGRID에서 SSO를 구성한 직후 AD FS 기반 당사자 트러스트를 생성할 준비가 되었으면 또한 각 관리 노드에 대해 SSO 및 단일 로그아웃(SLO) 프로세스를 테스트할 필요가 없습니다. * Enabled * 를 클릭하고 StorageGRID 설정을 입력한 다음 AD FS의 각 관리 노드에 대한 신뢰할 수 있는 파티 트러스트 를 생성한 다음 * Save * 를 클릭하여 SSO를 활성화합니다.

단계

1. Configuration * * * Access Control * * Single Sign-On * 을 선택합니다.

   단일 사인온 페이지가 나타나고 * 비활성화 * 옵션이 선택됩니다.



   SSO 상태 옵션이 나타나지 않으면 Active Directory를 통합 ID 소스로 구성했는지 확인합니다. Single Sign-On 사용 요건 참조

2. Sandbox 모드 * 옵션을 선택합니다.

   ID 공급자 및 공급자 설정이 나타납니다. ID 공급자 섹션에서 * 서비스 유형 * 필드는 읽기 전용입니다. 사용 중인 ID 페더레이션 서비스 유형(예: Active Directory)이 표시됩니다.

3. ID 공급자 섹션에서 다음을 수행합니다.

   a. AD FS에 표시되는 대로 페더레이션 서비스 이름을 입력합니다.

      페더레이션 서비스 이름을 찾으려면 Windows Server Manager로 이동합니다. Tools * * * AD FS Management * 를 선택합니다. 작업 메뉴에서 * 페더레이션 서비스 속성 편집 * 을 선택합니다. 두 번째 필드에 페더레이션 서비스 이름이 표시됩니다.

   b. ID 공급자가 StorageGRID 요청에 대한 응답으로 SSO 구성 정보를 보낼 때 TLS(전송 계층 보안)를 사용하여 연결을 보호할지 여부를 지정합니다.

      - * 운영 체제 CA 인증서 사용 *: 운영 체제에 설치된 기본 CA 인증서를 사용하여 연결을 보호합니다.
      - * 사용자 지정 CA 인증서 사용 *: 사용자 지정 CA 인증서를 사용하여 연결을 보호합니다.

        이 설정을 선택한 경우 인증서를 복사하여 * CA 인증서 * 텍스트 상자에 붙여 넣습니다.

- * TLS * 사용 안 함: TLS 인증서를 사용하여 연결을 보호하지 마십시오.

4. 신뢰할 수 있는 당사자 섹션에서 신뢰할 수 있는 상대 트러스트를 구성할 때 StorageGRID 관리 노드에 사용할 신뢰할 수 있는 당사자 식별자를 지정합니다.

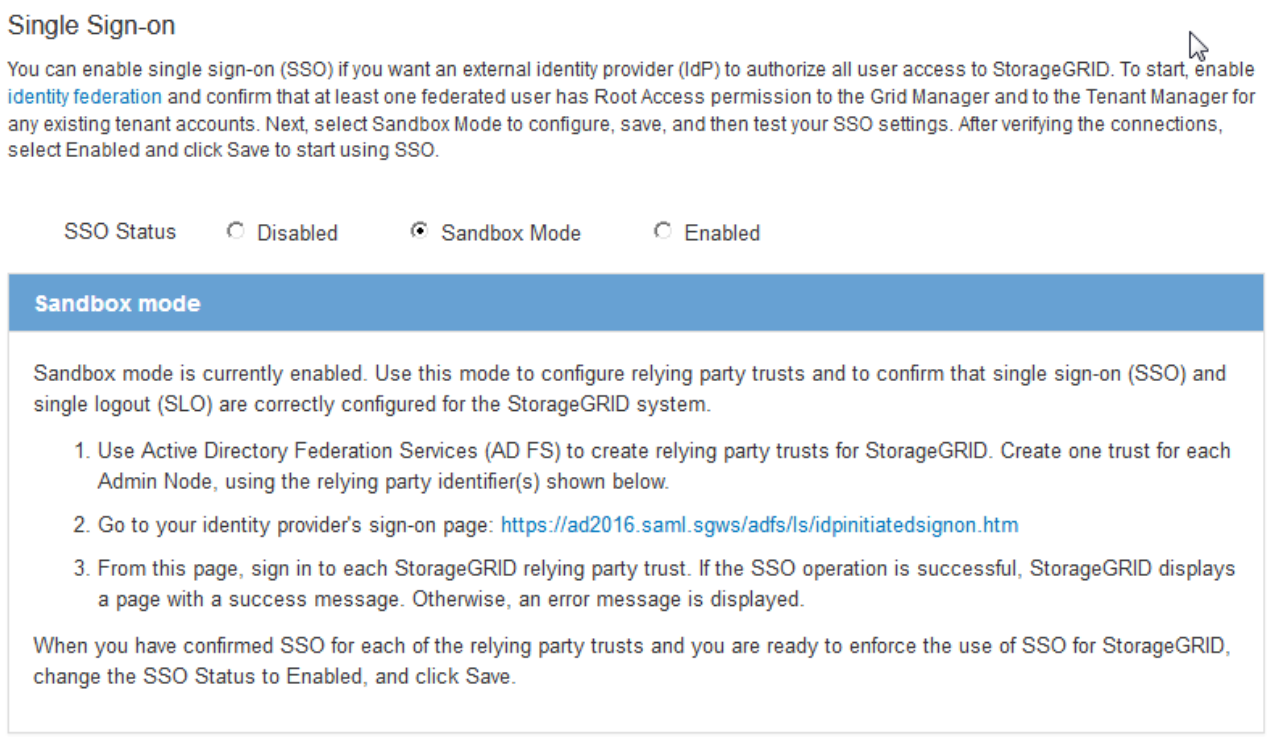
   - 예를 들어 그리드에 관리 노드가 하나뿐이고 나중에 관리 노드를 더 추가할 예정이 없는 경우 를 입력합니다 `SG` 또는 `StorageGRID`.
   - 그리드에 둘 이상의 관리 노드가 포함된 경우 문자열을 포함합니다 `[HOSTNAME]` 를 입력합니다. 예를 들면, 다음과 같습니다. `SG-[HOSTNAME]`. 이렇게 하면 노드의 호스트 이름을 기반으로 각 관리 노드에 대한 기반 당사자 식별자가 포함된 테이블이 생성됩니다. +참고: StorageGRID 시스템의 각 관리 노드에 대한 신뢰할 수 있는 상대 신뢰를 만들어야 합니다. 각 관리 노드에 대한 신뢰할 수 있는 당사자 덕분에 사용자는 모든 관리 노드에 안전하게 로그인할 수 있습니다.

5. 저장 * 을 클릭합니다.

   - 몇 초 동안 * Save * (저장 *) 버튼에 녹색 확인 표시가 나타납니다.

   - Sandbox 모드 확인 알림이 나타나고 Sandbox 모드가 이제 활성화되었음을 확인합니다. AD FS를 사용하는 동안 이 모드를 사용하여 각 관리 노드에 대한 의존적인 당사자 신뢰를 구성하고 SSO(Single Sign-In) 및 SLO(Single Logout) 프로세스를 테스트할 수 있습니다.



관련 정보

"Single Sign-On 사용에 대한 요구 사항"

AD FS에서 기반 당사자 신뢰를 생성합니다

AD FS(Active Directory Federation Services)를 사용하여 시스템의 각 관리 노드에 대한 기반

당사자 신뢰를 만들어야 합니다. PowerShell 명령을 사용하거나, StorageGRID에서 SAML 메타데이터를 가져오거나, 데이터를 수동으로 입력하여 의존할 수 있는 회사 트러스트를 만들 수 있습니다.

Windows PowerShell을 사용하여 신뢰할 수 있는 사용자 신뢰 생성

Windows PowerShell을 사용하여 하나 이상의 신뢰할 수 있는 파티 트러스트를 빠르게 만들 수 있습니다.

필요한 것

- StorageGRID에서 SSO를 구성했으며 시스템의 각 관리 노드에 대한 정규화된 도메인 이름(또는 IP 주소)과 관련 당사자 식별자를 알고 있습니다.

> StorageGRID 시스템의 각 관리 노드에 대한 신뢰할 수 있는 상대 신뢰를 만들어야 합니다. 각 관리 노드에 대한 신뢰할 수 있는 당사자 덕분에 사용자는 모든 관리 노드에 안전하게 로그인할 수 있습니다.

- AD FS에서 기반 당사자 트러스트를 만드는 경험이 있거나 Microsoft AD FS 문서에 액세스할 수 있습니다.
- AD FS 관리 스냅인을 사용하고 있으며 사용자는 Administrators 그룹에 속해 있습니다.

이 작업에 대해

이러한 지침은 Windows Server 2016에 포함된 AD FS 4.0에 적용됩니다. Windows 2012 R2에 포함된 AD FS 3.0을 사용하는 경우 절차에 약간의 차이가 있습니다. 질문이 있는 경우 Microsoft AD FS 설명서를 참조하십시오.

단계

1. Windows 시작 메뉴에서 PowerShell 아이콘을 마우스 오른쪽 단추로 클릭하고 * 관리자 권한으로 실행 * 을 선택합니다.
2. PowerShell 명령 프롬프트에서 다음 명령을 입력합니다.

   ```
   Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL
   "https://Admin_Node_FQDN/api/saml-metadata"
   ```

   - 용 `Admin_Node_Identifier`에서 관리 노드에 대한 기반 당사자 식별자를 단일 사인온 페이지에 표시된 대로 정확하게 입력합니다. 예를 들면, 다음과 같습니다. `SG-DC1-ADM1`.
   - 용 `Admin_Node_FQDN`에서 동일한 관리 노드에 대해 정규화된 도메인 이름을 입력합니다. (필요한 경우 노드의 IP 주소를 대신 사용할 수 있습니다. 그러나 여기에 IP 주소를 입력한 경우에는 해당 IP 주소가 변경될 경우 이 신뢰할 수 있는 사용자 신뢰를 업데이트하거나 다시 만들어야 합니다.)
3. Windows Server Manager에서 * Tools * > * AD FS Management * 를 선택합니다.

   AD FS 관리 도구가 나타납니다.
4. AD FS * > * 기반 당사자 신뢰 * 를 선택합니다.

   신뢰할 수 있는 당사자 목록이 나타납니다.
5. 새로 만든 신뢰할 수 있는 상대 신뢰에 액세스 제어 정책 추가:
   a. 방금 만든 신뢰할 수 있는 상대자를 찾습니다.
   b. 트러스트를 마우스 오른쪽 단추로 클릭하고 * 액세스 제어 정책 편집 * 을 선택합니다.

c. 액세스 제어 정책을 선택합니다.

d. 적용 * 을 클릭하고 * 확인 * 을 클릭합니다

6. 새로 생성된 신뢰할 수 있는 당사자 신탁에 클레임 발급 정책 추가:

a. 방금 만든 신뢰할 수 있는 상대자를 찾습니다.

b. 신뢰를 마우스 오른쪽 버튼으로 클릭하고 * 클레임 발급 정책 편집 * 을 선택합니다.

c. 규칙 추가 * 를 클릭합니다.

d. 규칙 템플릿 선택 페이지의 목록에서 * 청구로 LDAP 속성 보내기 * 를 선택하고 * 다음 * 을 클릭합니다.

e. 규칙 구성 페이지에서 이 규칙의 표시 이름을 입력합니다.

예를 들어, 이름 ID*에 대한 * objectGUID.

f. 특성 저장소의 경우 * Active Directory * 를 선택합니다.

g. 매핑 테이블의 LDAP 속성 열에 * objectGUID * 를 입력합니다.

h. 매핑 테이블의 발신 클레임 유형 열에서 드롭다운 목록에서 * 이름 ID * 를 선택합니다.

i. 마침 * 을 클릭하고 * 확인 * 을 클릭합니다.

7. 메타데이터를 성공적으로 가져왔는지 확인합니다.

a. 신뢰할 수 있는 상대 신뢰를 마우스 오른쪽 단추로 클릭하여 속성을 엽니다.

b. Endpoints *, * Identifiers * 및 * Signature * 탭의 필드가 채워져 있는지 확인합니다.

메타데이터가 누락된 경우 페더레이션 메타데이터 주소가 올바른지 확인하거나 값을 수동으로 입력합니다.

8. 이 단계를 반복하여 StorageGRID 시스템의 모든 관리 노드에 대한 신뢰할 수 있는 상대 트러스트를 구성합니다.

9. 완료되면 StorageGRID 및 로 돌아갑니다 "모든 신뢰할 수 있는 당사자 테스트" 올바르게 구성되었는지 확인합니다.

페더레이션 메타데이터를 가져와 사용 가능한 상대 신뢰 만들기

각 관리 노드에 대한 SAML 메타데이터에 액세스하여 각 의존자 신뢰의 값을 가져올 수 있습니다.

필요한 것

- StorageGRID에서 SSO를 구성했으며 시스템의 각 관리 노드에 대한 정규화된 도메인 이름(또는 IP 주소)과 관련 당사자 식별자를 알고 있습니다.

> StorageGRID 시스템의 각 관리 노드에 대한 신뢰할 수 있는 상대 신뢰를 만들어야 합니다. 각 관리 노드에 대한 신뢰할 수 있는 당사자 덕분에 사용자는 모든 관리 노드에 안전하게 로그인할 수 있습니다.

- AD FS에서 기반 당사자 트러스트를 만드는 경험이 있거나 Microsoft AD FS 문서에 액세스할 수 있습니다.
- AD FS 관리 스냅인을 사용하고 있으며 사용자는 Administrators 그룹에 속해 있습니다.

이 작업에 대해

이러한 지침은 Windows Server 2016에 포함된 AD FS 4.0에 적용됩니다. Windows 2012 R2에 포함된 AD FS 3.0을 사용하는 경우 절차에 약간의 차이가 있습니다. 질문이 있는 경우 Microsoft AD FS 설명서를 참조하십시오.

단계

1. Windows Server Manager에서 * Tools * 를 클릭한 다음 * AD FS Management * 를 선택합니다.
2. 작업에서 * 신뢰할 수 있는 당사자 신뢰 추가 * 를 클릭합니다.
3. 시작 페이지에서 * 클레임 인식 * 을 선택하고 * 시작 * 을 클릭합니다.
4. 온라인 또는 로컬 네트워크에 게시된 의존자에 대한 데이터 가져오기 * 를 선택합니다.
5. Federation 메타데이터 주소(호스트 이름 또는 URL) * 에 이 관리 노드에 대한 SAML 메타데이터의 위치를 입력합니다.

   `https://Admin_Node_FQDN/api/saml-metadata`

   용 `Admin_Node_FQDN`에서 동일한 관리 노드에 대해 정규화된 도메인 이름을 입력합니다. (필요한 경우 노드의 IP 주소를 대신 사용할 수 있습니다. 그러나 여기에 IP 주소를 입력한 경우에는 해당 IP 주소가 변경될 경우 이 신뢰할 수 있는 사용자 신뢰를 업데이트하거나 다시 만들어야 합니다.)

6. 신뢰할 수 있는 당사자 신뢰 마법사를 완료하고 신뢰할 수 있는 상대 신뢰를 저장한 다음 마법사를 닫습니다.

   표시 이름을 입력할 때 그리드 관리자의 단일 사인온 페이지에 나타나는 것과 동일하게 관리 노드에 대한 기반 당사자 식별자를 사용합니다. 예를 들면, 다음과 같습니다. `SG-DC1-ADM1`.

7. 청구 규칙 추가:
   a. 신뢰를 마우스 오른쪽 버튼으로 클릭하고 * 클레임 발급 정책 편집 * 을 선택합니다.
   b. 규칙 추가 * 를 클릭합니다.
   c. 규칙 템플릿 선택 페이지의 목록에서 * 청구로 LDAP 속성 보내기 * 를 선택하고 * 다음 * 을 클릭합니다.
   d. 규칙 구성 페이지에서 이 규칙의 표시 이름을 입력합니다.

      예를 들어, 이름 ID*에 대한 * objectGUID.

   e. 특성 저장소의 경우 * Active Directory * 를 선택합니다.
   f. 매핑 테이블의 LDAP 속성 열에 * objectGUID * 를 입력합니다.
   g. 매핑 테이블의 발신 클레임 유형 열에서 드롭다운 목록에서 * 이름 ID * 를 선택합니다.
   h. 마침 * 을 클릭하고 * 확인 * 을 클릭합니다.
8. 메타데이터를 성공적으로 가져왔는지 확인합니다.
   a. 신뢰할 수 있는 상대 신뢰를 마우스 오른쪽 단추로 클릭하여 속성을 엽니다.
   b. Endpoints *, * Identifiers * 및 * Signature * 탭의 필드가 채워져 있는지 확인합니다.

      메타데이터가 누락된 경우 페더레이션 메타데이터 주소가 올바른지 확인하거나 값을 수동으로 입력합니다.

9. 이 단계를 반복하여 StorageGRID 시스템의 모든 관리 노드에 대한 신뢰할 수 있는 상대 트러스트를 구성합니다.
10. 완료되면 StorageGRID 및 로 돌아갑니다 "모든 신뢰할 수 있는 당사자 테스트" 올바르게 구성되었는지 확인합니다.

수동으로 신뢰할 수 있는 상대 만들기

의존 파트 트러스트의 데이터를 불러오지 않도록 선택하면 값을 직접 입력할 수 있습니다.

필요한 것

- StorageGRID에서 SSO를 구성했으며 시스템의 각 관리 노드에 대한 정규화된 도메인 이름(또는 IP 주소)과 관련 당사자 식별자를 알고 있습니다.

> StorageGRID 시스템의 각 관리 노드에 대한 신뢰할 수 있는 상대 신뢰를 만들어야 합니다. 각 관리 노드에 대한 신뢰할 수 있는 당사자 덕분에 사용자는 모든 관리 노드에 안전하게 로그인할 수 있습니다.

- StorageGRID 관리 인터페이스를 위해 업로드된 사용자 지정 인증서가 있거나 명령 셸에서 관리자 노드에 로그인하는 방법을 알고 있습니다.
- AD FS에서 기반 당사자 트러스트를 만드는 경험이 있거나 Microsoft AD FS 문서에 액세스할 수 있습니다.
- AD FS 관리 스냅인을 사용하고 있으며 사용자는 Administrators 그룹에 속해 있습니다.

이 작업에 대해

이러한 지침은 Windows Server 2016에 포함된 AD FS 4.0에 적용됩니다. Windows 2012 R2에 포함된 AD FS 3.0을 사용하는 경우 절차에 약간의 차이가 있습니다. 질문이 있는 경우 Microsoft AD FS 설명서를 참조하십시오.

단계

1. Windows Server Manager에서 * Tools * 를 클릭한 다음 * AD FS Management * 를 선택합니다.
2. 작업에서 * 신뢰할 수 있는 당사자 신뢰 추가 * 를 클릭합니다.
3. 시작 페이지에서 * 클레임 인식 * 을 선택하고 * 시작 * 을 클릭합니다.
4. [의지하는 사용자에 대한 데이터 입력]을 선택하고 * [다음]을 클릭합니다.
5. 신뢰할 수 있는 당사자 신뢰 마법사를 완료합니다.

   a. 이 관리 노드의 표시 이름을 입력합니다.

      일관성을 위해 그리드 관리자의 단일 사인온 페이지에 표시되는 것과 동일하게 관리자 노드에 대한 기반 당사자 식별자를 사용합니다. 예를 들면, 다음과 같습니다. `SG-DC1-ADM1`.

   b. 선택적 토큰 암호화 인증서를 구성하려면 단계를 건너뜁니다.

   c. URL 구성 페이지에서 SAML 2.0 WebSSO 프로토콜 * 지원 활성화 확인란을 선택합니다.

   d. 관리 노드에 대한 SAML 서비스 끝점 URL을 입력합니다.

      `https://Admin_Node_FQDN/api/saml-response`

      용 `*Admin_Node_FQDN*`에서 관리자 노드의 정규화된 도메인 이름을 입력합니다. (필요한 경우 노드의 IP 주소를 대신 사용할 수 있습니다. 그러나 여기에 IP 주소를 입력한 경우에는 해당 IP 주소가 변경될 경우 이 신뢰할 수 있는 사용자 신뢰를 업데이트하거나 다시 만들어야 합니다.)

   e. 식별자 구성 페이지에서 동일한 관리 노드에 대한 기반 당사자 식별자를 지정합니다.

      Admin_Node_Identifier

      용 *Admin_Node_Identifier*`에서 관리 노드에 대한 기반 당사자 식별자를 단일 사인온 페이지에 표시된 대로 정확하게 입력합니다. 예를 들면, 다음과 같습니다. `SG-DC1-ADM1`.

   f. 설정을 검토하고 신뢰할 수 있는 상대 신뢰를 저장한 다음 마법사를 닫습니다.

청구 발급 정책 편집 대화 상자가 나타납니다.

> 대화 상자가 나타나지 않으면 트러스트를 마우스 오른쪽 단추로 클릭하고 * 클레임 발급 정책 편집 * 을 선택합니다.

6. 클레임 규칙 마법사를 시작하려면 * 규칙 추가 * 를 클릭합니다.
   a. 규칙 템플릿 선택 페이지의 목록에서 * 청구로 LDAP 속성 보내기 * 를 선택하고 * 다음 * 을 클릭합니다.
   b. 규칙 구성 페이지에서 이 규칙의 표시 이름을 입력합니다.

      예를 들어, 이름 ID*에 대한 * objectGUID.

   c. 특성 저장소의 경우 * Active Directory * 를 선택합니다.
   d. 매핑 테이블의 LDAP 속성 열에 * objectGUID * 를 입력합니다.
   e. 매핑 테이블의 발신 클레임 유형 열에서 드롭다운 목록에서 * 이름 ID * 를 선택합니다.
   f. 마침 * 을 클릭하고 * 확인 * 을 클릭합니다.
7. 신뢰할 수 있는 상대 신뢰를 마우스 오른쪽 단추로 클릭하여 속성을 엽니다.
8. 엔드포인트 * 탭에서 단일 로그아웃(SLO)에 대한 엔드포인트를 구성합니다.
   a. SAML 추가 * 를 클릭합니다.
   b. Endpoint Type * > * SAML Logout * 을 선택합니다.
   c. Binding * > * Redirect * 를 선택합니다.
   d. 신뢰할 수 있는 URL * 필드에 이 관리 노드에서 단일 로그아웃(SLO)에 사용되는 URL을 입력합니다.

      `https://Admin_Node_FQDN/api/saml-logout`

   용 `*Admin_Node_FQDN*`에서 관리자 노드의 정규화된 도메인 이름을 입력합니다. (필요한 경우 노드의 IP 주소를 대신 사용할 수 있습니다. 그러나 여기에 IP 주소를 입력한 경우에는 해당 IP 주소가 변경될 경우 이 신뢰할 수 있는 사용자 신뢰를 업데이트하거나 다시 만들어야 합니다.)

   a. 확인 * 을 클릭합니다.
9. 서명* 탭에서 이 신뢰할 수 있는 당사자 트러스트의 서명 인증서를 지정합니다.
   a. 사용자 지정 인증서 추가:
      - StorageGRID에 업로드한 사용자 지정 관리 인증서가 있는 경우 해당 인증서를 선택합니다.
      - 사용자 지정 인증서가 없는 경우 관리 노드에 로그인하고 로 이동합니다 `/var/local/mgmt-api` Admin Node의 디렉토리로 이동한 후 를 추가합니다 `custom-server.crt` 인증서 파일.
        - 참고: * 관리자 노드의 기본 인증서 사용 (`server.crt`)는 권장되지 않습니다. 관리자 노드에 장애가 발생하면 노드를 복구할 때 기본 인증서가 다시 생성되고, 신뢰할 수 있는 상대 트러스트를 업데이트해야 합니다.
   b. 적용 * 을 클릭하고 * 확인 * 을 클릭합니다.

      종속된 당사자 속성이 저장되고 닫힙니다.

10. 이 단계를 반복하여 StorageGRID 시스템의 모든 관리 노드에 대한 신뢰할 수 있는 상대 트러스트를 구성합니다.

11. 완료되면 StorageGRID 및 로 돌아갑니다 "모든 신뢰할 수 있는 당사자 테스트" 올바르게 구성되었는지 확인합니다.

신뢰할 수 있는 당사자 신뢰 테스트

StorageGRID에 SSO(Single Sign-On)를 사용하도록 강제하기 전에 SSO(Single Sign-On)와 SLO(Single Logout)가 올바르게 구성되었는지 확인합니다. 각 관리 노드에 대해 종속된 당사자 신뢰를 생성한 경우 각 관리 노드에 대해 SSO 및 SLO를 사용할 수 있는지 확인합니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.
- AD FS에서 하나 이상의 기반 당사자 트러스트를 구성했습니다.

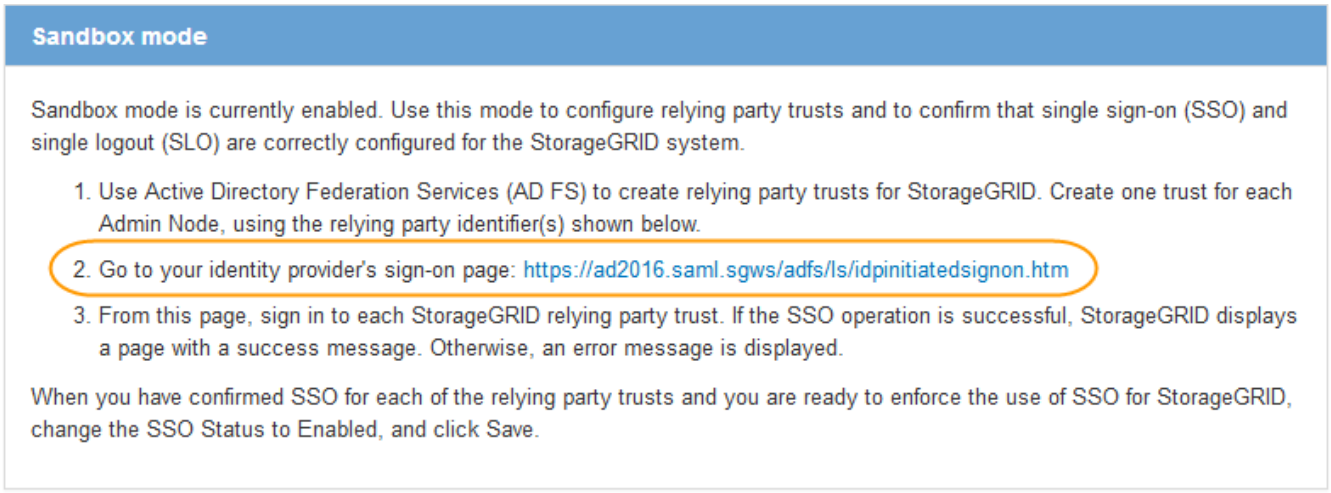
단계

1. Configuration * * * Access Control * * Single Sign-On * 을 선택합니다.

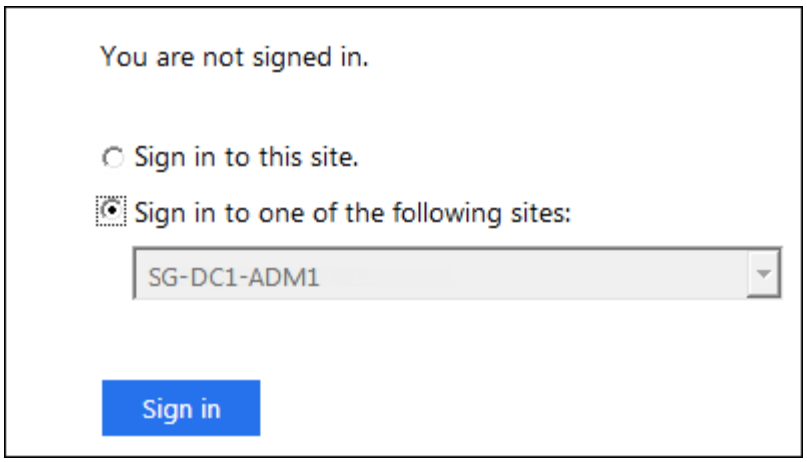
   단일 사인온 페이지가 나타나고 * Sandbox 모드 * 옵션이 선택됩니다.

2. sandbox 모드에 대한 지침에서 ID 공급자의 로그인 페이지에 대한 링크를 찾습니다.

   URL은 * Federated Service Name * 필드에 입력한 값에서 파생됩니다.



3. ID 공급자의 로그인 페이지에 액세스하려면 링크를 클릭하거나 URL을 복사하여 브라우저에 붙여 넣으십시오.
4. SSO를 사용하여 StorageGRID에 로그인할 수 있는지 확인하려면 * 다음 사이트 중 하나에 로그인 * 을 선택하고 기본 관리자 노드에 대한 보조 당사자 식별자를 선택한 다음 * 로그인 * 을 클릭합니다.



사용자 이름과 암호를 입력하라는 메시지가 표시됩니다.

5. 통합 사용자 이름과 암호를 입력합니다.
   - SSO 로그인 및 로그아웃 작업이 성공하면 성공 메시지가 나타납니다.

     ✔ Single sign-on authentication and logout test completed successfully.

   - SSO 작업이 실패하면 오류 메시지가 나타납니다. 문제를 해결하고 브라우저의 쿠키를 삭제한 후 다시 시도하십시오.
6. 이전 단계를 반복하여 다른 관리 노드에 로그인할 수 있는지 확인합니다.

   모든 SSO 로그인 및 로그아웃 작업이 성공하면 SSO를 활성화할 수 있습니다.

SSO(Single Sign-On) 활성화

sandbox 모드를 사용하여 모든 StorageGRID 기반 당사자 트러스트를 테스트한 후에는 SSO(Single Sign-On)를 사용할 수 있습니다.

필요한 것

- ID 소스에서 하나 이상의 통합 그룹을 가져오고 그룹에 할당된 루트 액세스 관리 권한을 가져와야 합니다. 하나 이상의 통합 사용자가 그리드 관리자 및 기존 테넌트 계정에 대한 테넌트 관리자에 대한 루트 액세스 권한을 가지고 있는지 확인해야 합니다.
- 샌드박스 모드를 사용하여 모든 신뢰할 수 있는 파티 트러스트를 수행해야 합니다.

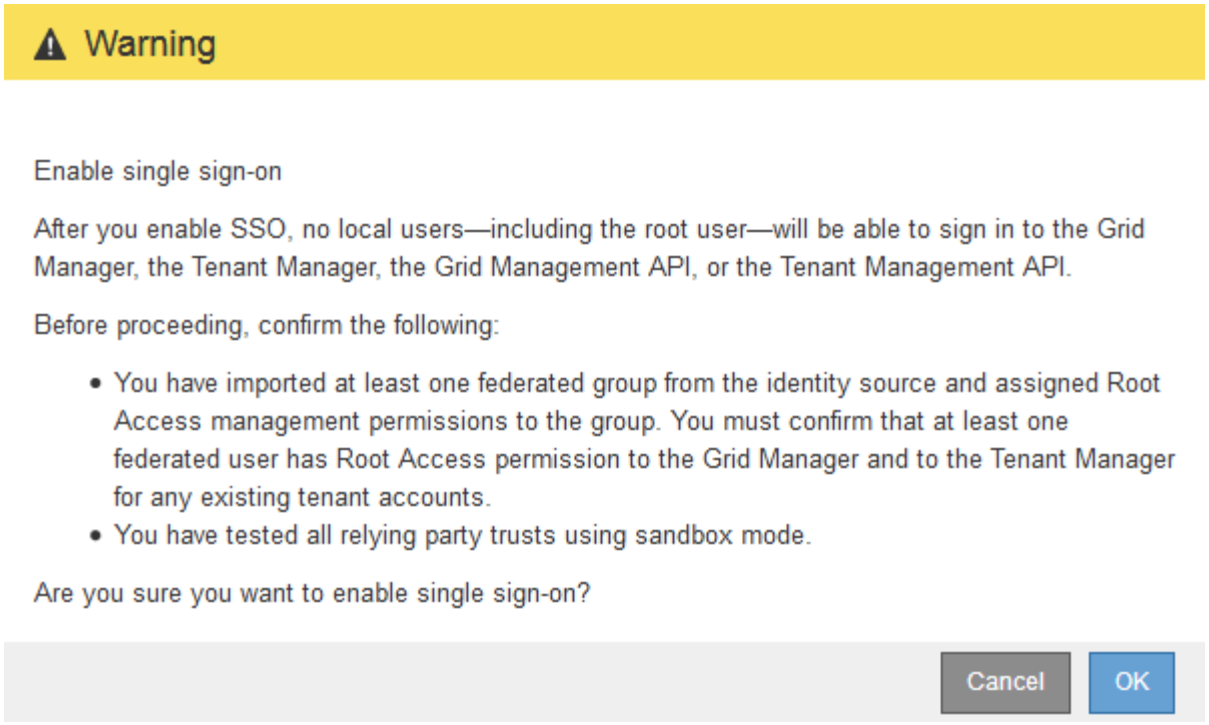
단계

1. Configuration * * * Access Control * * Single Sign-On * 을 선택합니다.

   단일 사인온 페이지가 * Sandbox 모드 * 가 선택된 상태로 나타납니다.

2. SSO 상태를 * Enabled * 로 변경합니다.
3. 저장 * 을 클릭합니다.

   경고 메시지가 나타납니다.



4. 경고를 검토하고 * OK * 를 클릭합니다.

   이제 SSO(Single Sign-On)가 활성화됩니다.

> 모든 사용자는 SSO를 사용하여 Grid Manager, Tenant Manager, Grid Management API 및 Tenant Management API에 액세스해야 합니다. 로컬 사용자는 더 이상 StorageGRID에 액세스할 수 없습니다.

SSO(Single Sign-On) 비활성화

이 기능을 더 이상 사용하지 않으려면 SSO(Single Sign-On)를 사용하지 않도록 설정할 수 있습니다. ID 페더레이션을 비활성화하려면 먼저 SSO(Single Sign-On)를 비활성화해야 합니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

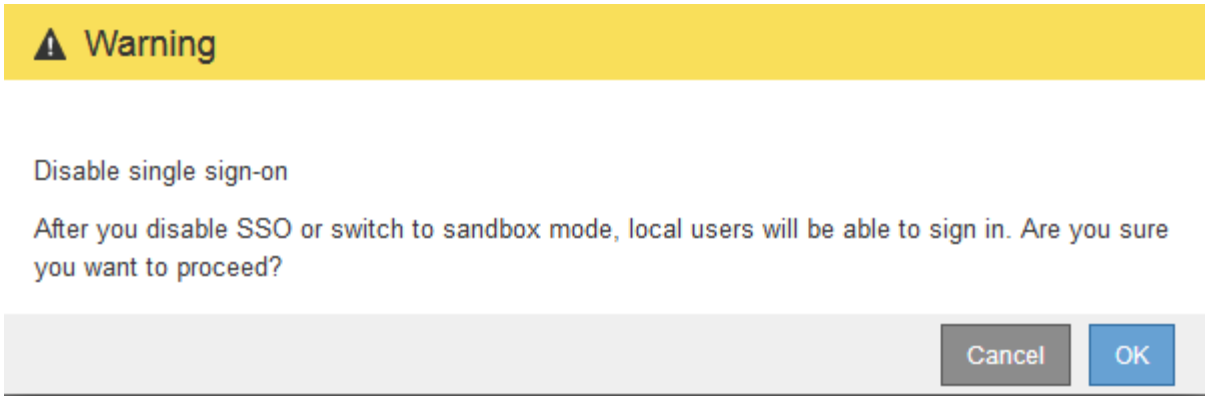
단계

1. Configuration * * * Access Control * * Single Sign-On * 을 선택합니다.

   단일 사인온 페이지가 나타납니다.

2. 사용 안 함 * 옵션을 선택합니다.
3. 저장 * 을 클릭합니다.

   로컬 사용자가 로그인할 수 있음을 나타내는 경고 메시지가 나타납니다.



4. 확인 * 을 클릭합니다.

   다음에 StorageGRID에 로그인할 때 StorageGRID 로그인 페이지가 나타나고 로컬 또는 통합 StorageGRID 사용자의 사용자 이름과 암호를 입력해야 합니다.

하나의 관리 노드에 대해 **SSO(Single Sign-On)**를 일시적으로 비활성화 및 다시 활성화합니다

SSO(Single Sign-On) 시스템이 다운되면 Grid Manager에 로그인하지 못할 수 있습니다. 이 경우 한 관리 노드에 대해 SSO를 일시적으로 비활성화 및 다시 활성화할 수 있습니다. SSO를 사용하지 않도록 설정한 다음 다시 사용하도록 설정하려면 노드의 명령 셸에 액세스해야 합니다.

필요한 것

- 특정 액세스 권한이 있어야 합니다.
- 에 가 있어야 합니다 `Passwords.txt` 파일.
- 로컬 루트 사용자의 암호를 알아야 합니다.

이 작업에 대해

한 관리 노드에 대해 SSO를 비활성화한 후 그리드 관리자에 로컬 루트 사용자로 로그인할 수 있습니다. StorageGRID 시스템을 보호하려면 로그아웃하는 즉시 노드의 명령 셸을 사용하여 관리자 노드에서 SSO를 다시 활성화해야 합니다.

> 한 관리 노드에 대해 SSO를 비활성화해도 그리드의 다른 관리 노드에 대한 SSO 설정에는 영향을 주지 않습니다. Grid Manager의 Single Sign-On 페이지에 있는 * Enable SSO * (SSO * 활성화) 확인란은 선택된 상태로 남아 있으며, 기존 SSO 설정은 모두 업데이트하지 않는 한 유지됩니다.

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.`disable-saml`

명령이 이 관리 노드에만 적용된다는 메시지가 표시됩니다.

3. SSO를 비활성화할지 확인합니다.

   노드에서 SSO(Single Sign-On)가 비활성화되었다는 메시지가 표시됩니다.

4. 웹 브라우저에서 동일한 관리 노드의 그리드 관리자에 액세스합니다.

   이제 SSO가 비활성화되어 Grid Manager 로그인 페이지가 표시됩니다.

5. 사용자 이름 루트와 로컬 루트 사용자 암호를 사용하여 로그인합니다.
6. SSO 구성을 수정해야 하므로 SSO를 일시적으로 비활성화한 경우:
   a. Configuration * * * Access Control * * Single Sign-On * 을 선택합니다.
   b. 잘못된 또는 오래된 SSO 설정을 변경합니다.
   c. 저장 * 을 클릭합니다.

      단일 사인온 페이지에서 * 저장 * 을 클릭하면 전체 그리드에 대한 SSO가 자동으로 다시 활성화됩니다.

7. 다른 이유로 인해 그리드 관리자에 액세스해야 하기 때문에 SSO를 일시적으로 비활성화한 경우:
   a. 수행해야 할 작업 또는 작업을 모두 수행합니다.
   b. 로그아웃 * 을 클릭하고 그리드 관리자를 닫습니다.
   c. 관리자 노드에서 SSO를 다시 활성화합니다. 다음 단계 중 하나를 수행할 수 있습니다.

      - 다음 명령을 실행합니다. `enable-saml`

        명령이 이 관리 노드에만 적용된다는 메시지가 표시됩니다.

      SSO를 활성화할지 확인합니다.

   노드에서 Single Sign-On이 설정되었음을 나타내는 메시지가 표시됩니다.

      ◦ 그리드 노드를 재부팅합니다. `reboot`

8. 웹 브라우저에서 동일한 관리 노드에서 그리드 관리자에 액세스합니다.
9. StorageGRID 로그인 페이지가 나타나고 그리드 관리자에 액세스하려면 SSO 자격 증명을 입력해야 합니다.

관련 정보

"Single Sign-On 구성"

관리자 클라이언트 인증서를 구성하는 중입니다

클라이언트 인증서를 사용하여 권한이 있는 외부 클라이언트가 StorageGRID Prometheus 데이터베이스에 액세스할 수 있도록 허용할 수 있습니다. 클라이언트 인증서는 외부 도구를 사용하여 StorageGRID를 모니터링하는 안전한 방법을 제공합니다.

외부 모니터링 도구를 사용하여 StorageGRID에 액세스해야 하는 경우 그리드 관리자를 사용하여 클라이언트 인증서를

업로드하거나 생성하고 인증서 정보를 외부 도구에 복사해야 합니다.

관리자 클라이언트 인증서를 추가하는 중입니다

클라이언트 인증서를 추가하려면 고유한 인증서를 제공하거나 Grid Manager를 사용하여 인증서를 생성할 수 있습니다.

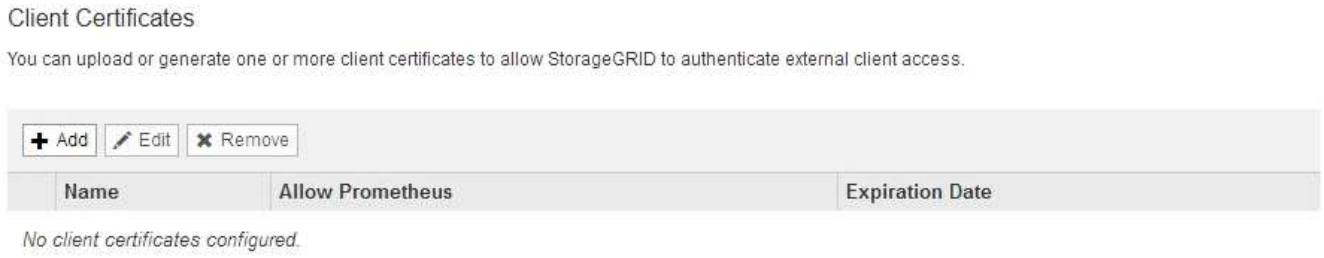
필요한 것

- 루트 액세스 권한이 있어야 합니다.
- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 관리 노드의 IP 주소 또는 도메인 이름을 알아야 합니다.
- StorageGRID 관리 인터페이스 서버 인증서를 구성하고 해당 CA 번들을 가지고 있어야 합니다
- 인증서를 업로드하려면 인증서의 공개 키와 개인 키를 로컬 컴퓨터에서 사용할 수 있어야 합니다.

단계

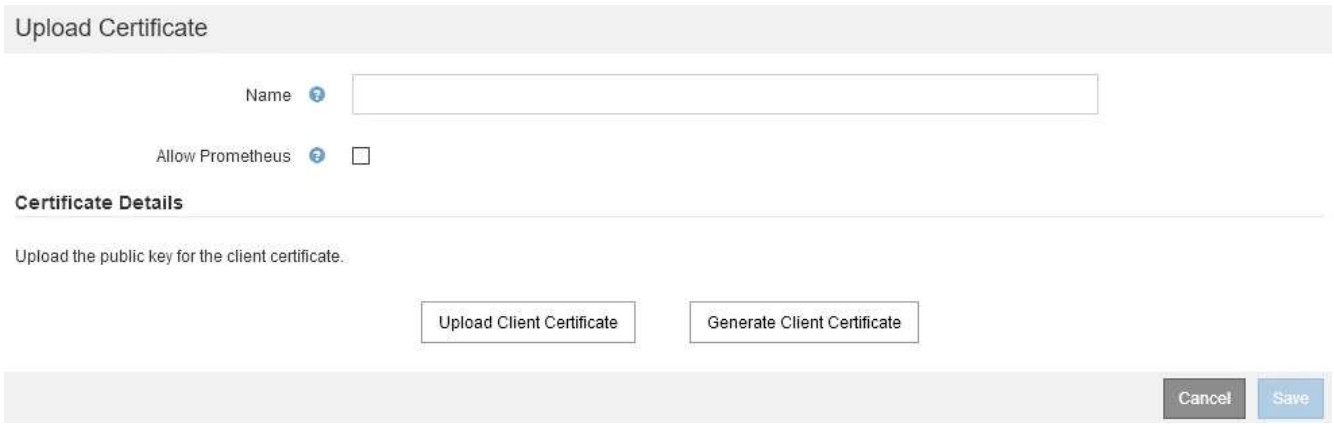
1. 그리드 관리자에서 * 구성 * > * 액세스 제어 * > * 클라이언트 인증서 * 를 선택합니다.

   클라이언트 인증서 페이지가 나타납니다.



2. 추가 * 를 선택합니다.

   인증서 업로드 페이지가 나타납니다.



3. 인증서의 이름을 1자에서 32자 사이로 입력합니다.
4. 외부 모니터링 도구를 사용하여 Prometheus 메트릭에 액세스하려면 * Prometheus * 허용 확인란을 선택합니다.
5. 인증서 업로드 또는 생성:
   a. 인증서를 업로드하려면 으로 이동합니다 여기.

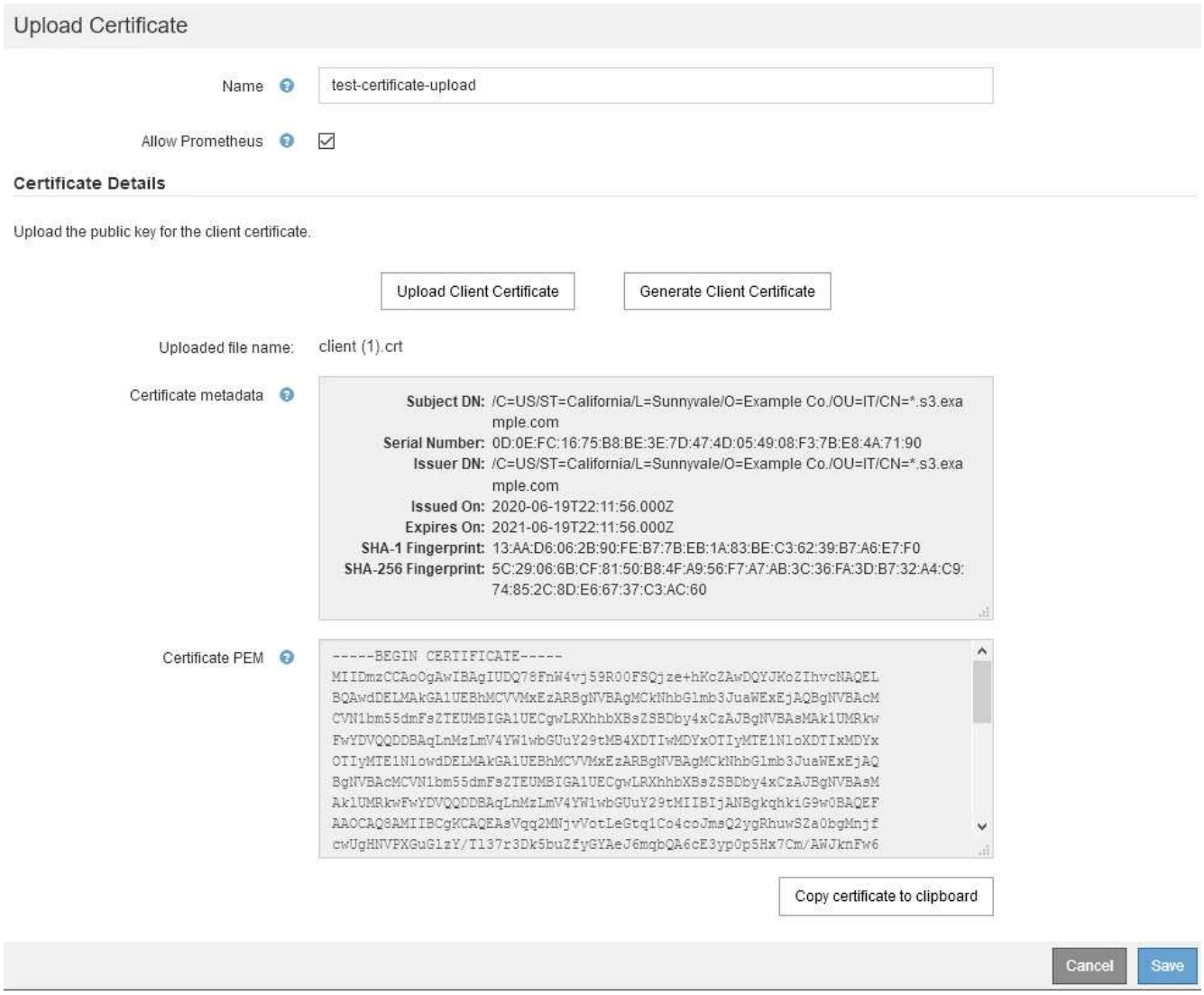
b. 인증서를 생성하려면 으로 이동합니다 여기.

6. 인증서를 업로드하려면

a. 클라이언트 인증서 업로드 * 를 선택합니다.

b. 인증서의 공개 키를 찾습니다.

인증서의 공개 키를 업로드하면 * 인증서 메타데이터 * 및 * 인증서 PEM * 필드가 채워집니다.



a. 클립보드로 인증서 복사 * 를 선택하고 외부 모니터링 도구에 인증서를 붙여 넣습니다.

b. 편집 도구를 사용하여 개인 키를 복사하여 외부 모니터링 도구에 붙여 넣습니다.

c. 인증서를 Grid Manager에 저장하려면 * 저장 * 을 선택합니다.

7. 인증서를 생성하려면:

a. 클라이언트 인증서 생성 * 을 선택합니다.

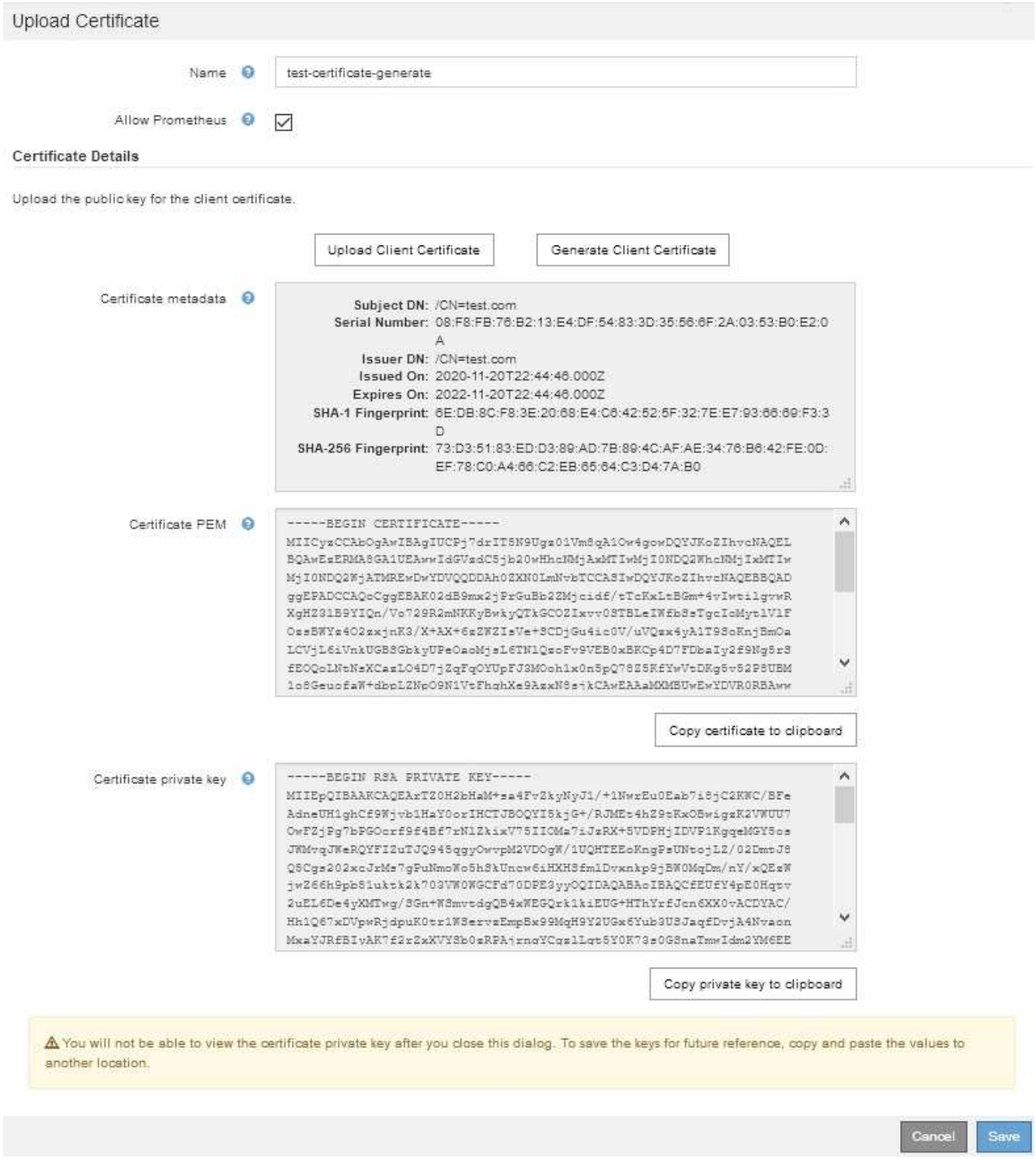
b. 관리자 노드의 도메인 이름 또는 IP 주소를 입력합니다.

c. 선택적으로 DN(고유 이름)이라고도 하는 X.509 제목을 입력하여 인증서를 소유한 관리자를 식별합니다.

d. 원하는 경우 인증서가 유효한 일 수를 선택합니다. 기본값은 730일입니다.

e. Generate * 를 선택합니다.

인증서 메타데이터 *, * 인증서 PEM * 및 * 인증서 개인 키 * 필드가 채워집니다.



a. 클립보드로 인증서 복사 * 를 선택하고 외부 모니터링 도구에 인증서를 붙여 넣습니다.

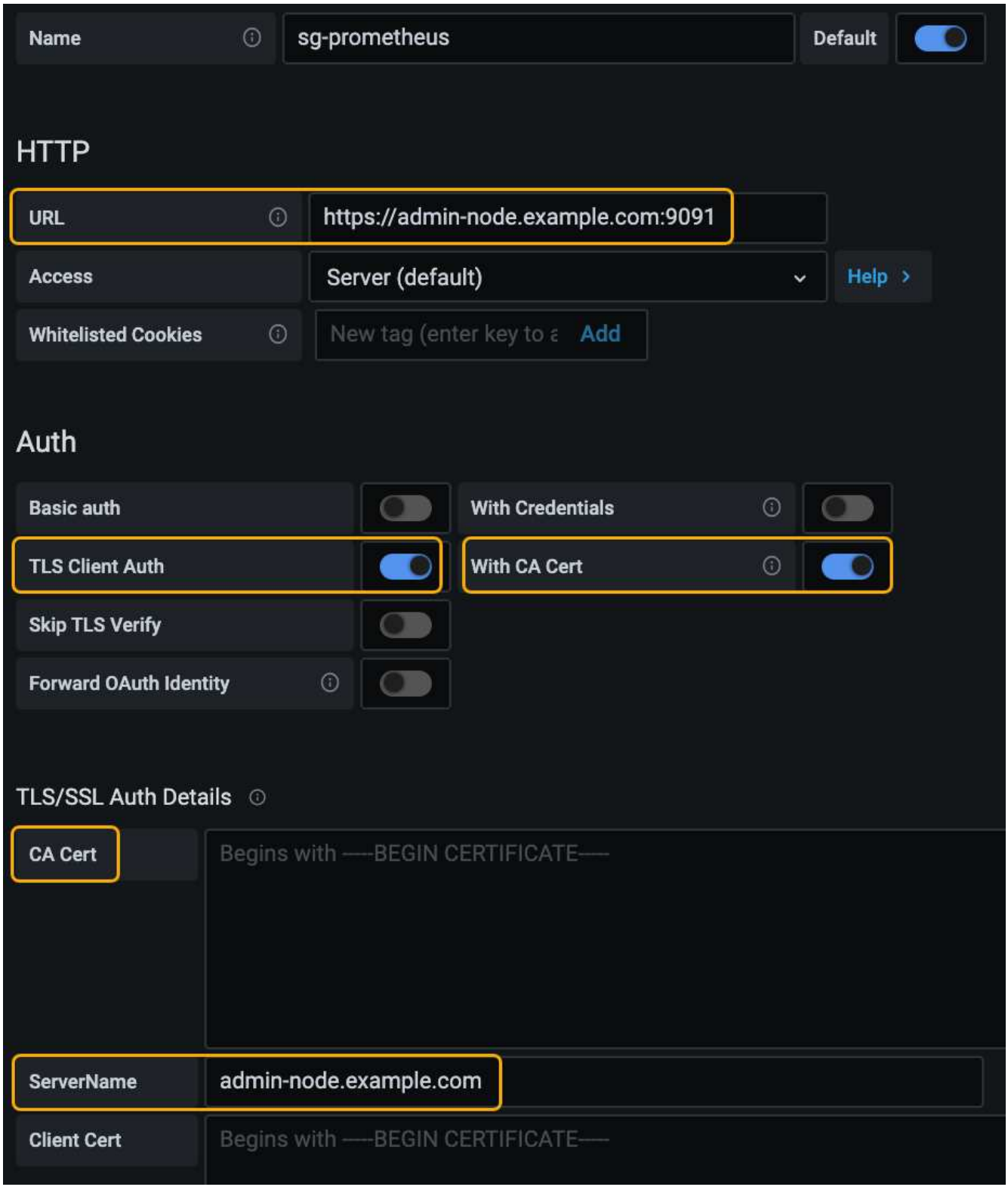
b. Copy private key to clipboard * 를 선택하고 키를 외부 모니터링 도구에 붙여 넣습니다.

대화 상자를 닫은 후에는 개인 키를 볼 수 없습니다. 키를 안전한 위치에 복사합니다.

c. 인증서를 Grid Manager에 저장하려면 * 저장 * 을 선택합니다.

8. Grafana와 같은 외부 모니터링 도구에서 다음 설정을 구성합니다.

Grafana 예제는 다음 스크린샷에 나와 있습니다.



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. 관리 인터페이스 서버 인증서 또는 CA 번들을 TLS/SSL 인증 세부 정보 아래의 **CA Cert**에 복사하여 붙여 넣습니다.

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

   servername은 관리 인터페이스 서버 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 StorageGRID 모니터링 및 문제 해결 지침을 참조하십시오.

관련 정보

"StorageGRID 보안 인증서 사용"

"Grid Manager 및 테넌트 관리자에 대한 사용자 지정 서버 인증서 구성"

"모니터링 및 문제 해결"

관리자 클라이언트 인증서를 편집하는 중입니다

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

필요한 것

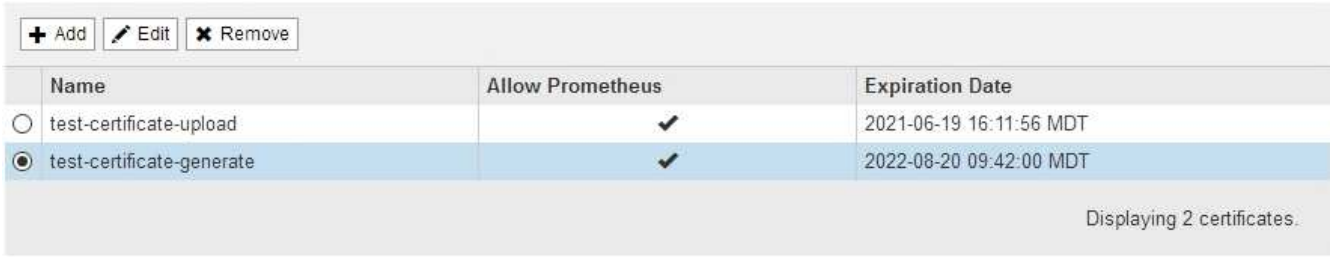
- 루트 액세스 권한이 있어야 합니다.
- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 관리 노드의 IP 주소 또는 도메인 이름을 알아야 합니다.
- 새 인증서 및 개인 키를 업로드하려면 로컬 컴퓨터에서 사용할 수 있어야 합니다.

단계

1. 구성 * > * 액세스 제어 * > * 클라이언트 인증서 * 를 선택합니다.

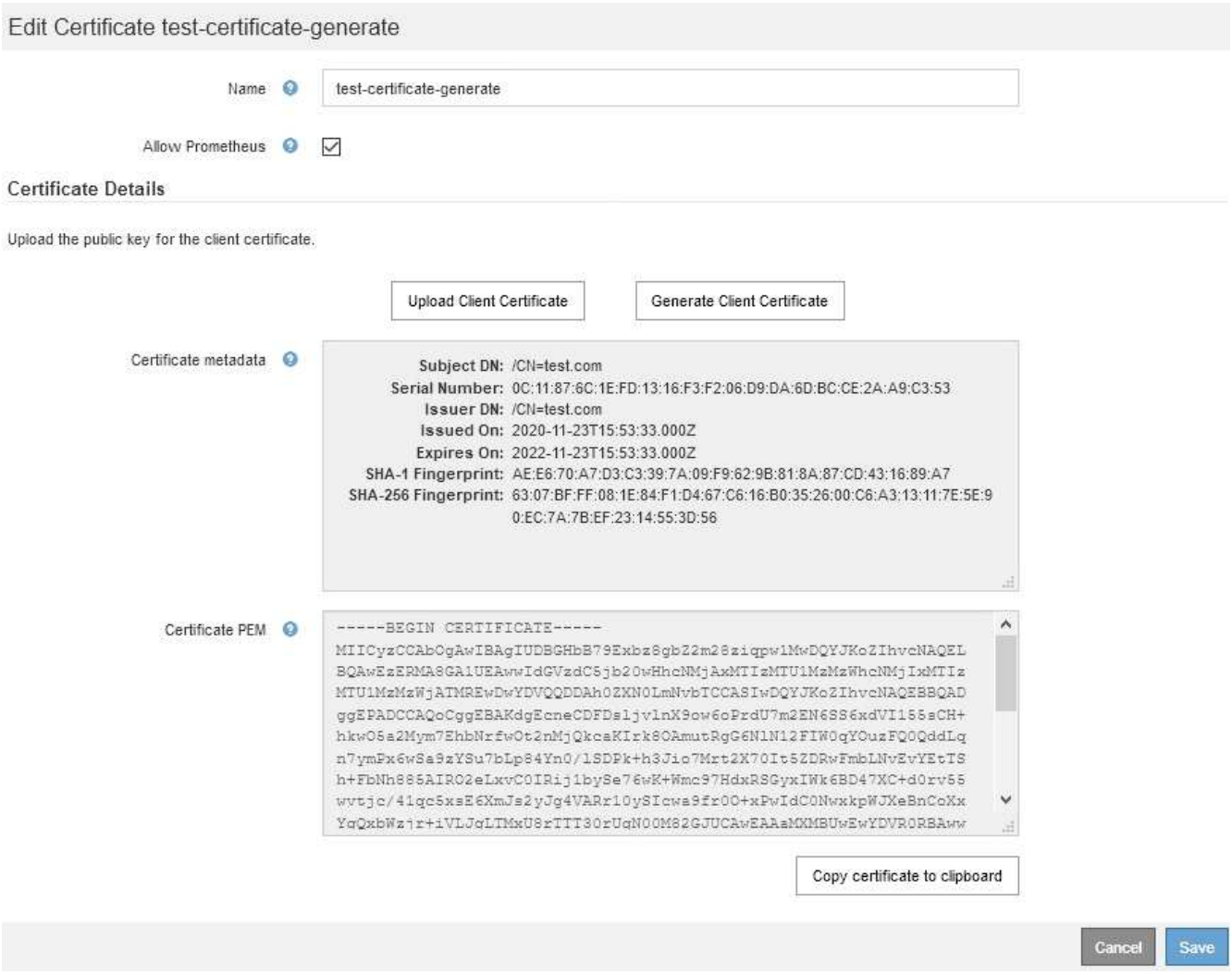
   클라이언트 인증서 페이지가 나타납니다. 기존 인증서가 나열됩니다.

   인증서 만료 날짜가 표에 나열되어 있습니다. 인증서가 곧 만료되거나 이미 만료된 경우 테이블에 메시지가 나타나고 경고가 트리거됩니다.



2. 편집할 인증서 왼쪽에 있는 라디오 단추를 선택합니다.
3. 편집 * 을 선택합니다.

   인증서 편집 대화 상자가 나타납니다.



4. 원하는 대로 인증서를 변경합니다.
5. 인증서를 Grid Manager에 저장하려면 * 저장 * 을 선택합니다.
6. 새 인증서를 업로드한 경우:
   a. 외부 모니터링 도구에 인증서를 붙여넣으려면 * 클립보드로 인증서 복사 * 를 선택합니다.
   b. 편집 도구를 사용하여 새 개인 키를 복사하여 외부 모니터링 도구에 붙여 넣습니다.
   c. 외부 모니터링 도구에서 인증서와 개인 키를 저장하고 테스트합니다.

7. 새 인증서를 생성한 경우:
   a. 외부 모니터링 도구에 인증서를 붙여넣으려면 * 클립보드로 인증서 복사 * 를 선택합니다.
   b. 인증서를 외부 모니터링 도구에 붙여넣으려면 * 클립보드로 개인 키 복사 * 를 선택합니다.

      대화 상자를 닫은 후에는 개인 키를 보거나 복사할 수 없습니다. 키를 안전한 위치에 복사합니다.

   c. 외부 모니터링 도구에서 인증서와 개인 키를 저장하고 테스트합니다.

관리자 클라이언트 인증서를 제거하는 중입니다

인증서가 더 이상 필요하지 않으면 제거할 수 있습니다.

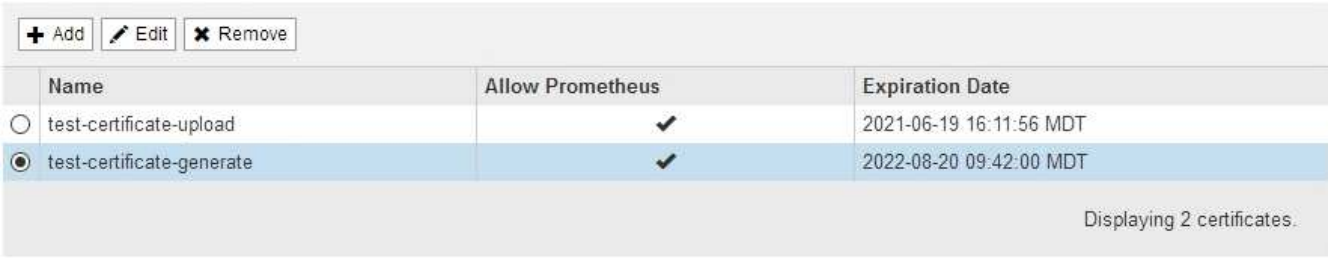
필요한 것

- 루트 액세스 권한이 있어야 합니다.
- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.

단계

1. 구성 * > * 액세스 제어 * > * 클라이언트 인증서 * 를 선택합니다.

   클라이언트 인증서 페이지가 나타납니다. 기존 인증서가 나열됩니다.



2. 제거할 인증서 왼쪽에 있는 라디오 단추를 선택합니다.
3. 제거 * 를 선택합니다.

   확인 대화 상자가 나타납니다.

4. OK * 를 선택합니다.

   인증서가 제거됩니다.