테넌트 사용자에 대한 시스템 액세스 관리

StorageGRID 11.5

NetApp
April 11, 2024

목차

테넌트 사용자에 대한 시스템 액세스 관리 1
ID 페더레이션 사용 1
그룹 관리 6
로컬 사용자 관리 19

테넌트 사용자에 대한 시스템 액세스 관리

통합 ID 소스에서 그룹을 가져오고 관리 권한을 할당하여 테넌트 계정에 대한 액세스 권한을 사용자에게 부여합니다. 전체 StorageGRID 시스템에 SSO(Single Sign-On)가 적용되지 않는 한 로컬 테넌트 그룹 및 사용자를 생성할 수도 있습니다.

- "ID 페더레이션 사용"
- "그룹 관리"
- "로컬 사용자 관리"

ID 페더레이션 사용

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

- "통합 ID 소스 구성"
- "ID 소스와 동기화 수행"
- "ID 페더레이션을 사용하지 않도록 설정합니다"

통합 ID 소스 구성

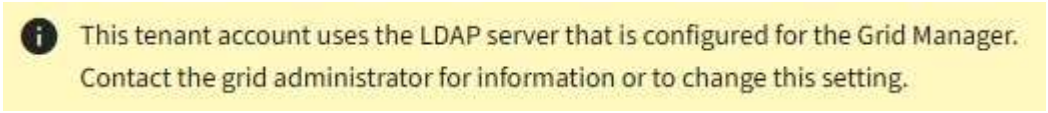
테넌트 그룹 및 사용자를 Active Directory, OpenLDAP 또는 Oracle Directory Server와 같은 다른 시스템에서 관리하도록 하려면 ID 페더레이션을 구성할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 테넌트 관리자에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.
- 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

테넌트의 ID 페더레이션 서비스를 구성할 수 있는지 여부는 테넌트 계정 설정 방법에 따라 달라집니다. 테넌트가 Grid Manager용으로 구성된 ID 페더레이션 서비스를 공유할 수 있습니다. ID 페더레이션 페이지에 액세스할 때 이 메시지가 표시되면 이 테넌트에 대해 별도의 통합 ID 소스를 구성할 수 없습니다.



단계

1. 액세스 관리 * > * ID 페더레이션 * 을 선택합니다.
2. ID 페더레이션 사용 * 을 선택합니다.

3. LDAP 서비스 유형 섹션에서 * Active Directory *, * OpenLDAP * 또는 * 기타 * 를 선택합니다.

   OpenLDAP * 를 선택한 경우 OpenLDAP 서버를 구성합니다. 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.

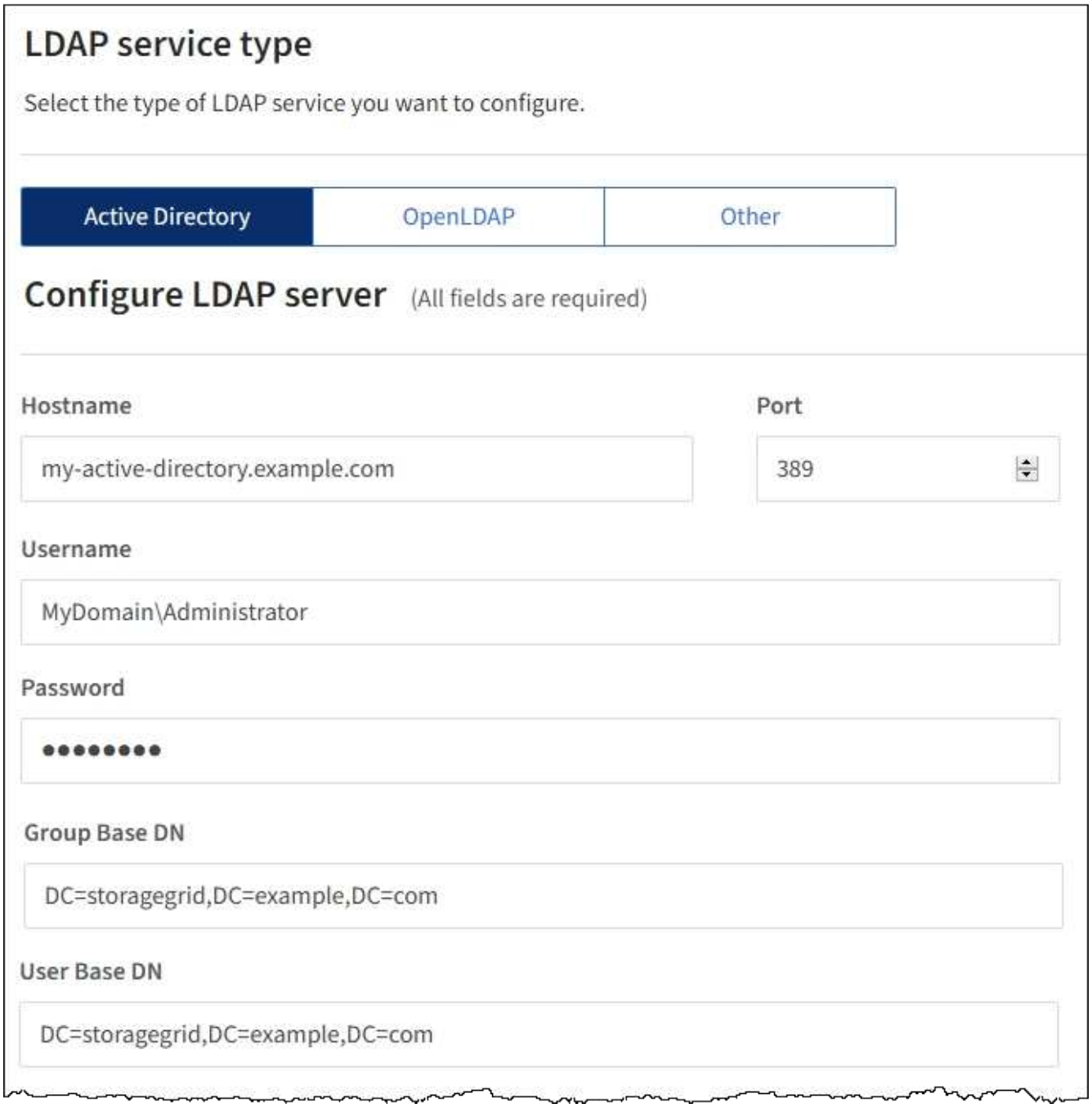
6. TLS(Transport Layer Security) * 섹션에서 보안 설정을 선택합니다.
   - * STARTTLS 사용(권장) *: STARTTLS를 사용하여 LDAP 서버와의 통신을 보호합니다. 이 옵션을 선택하는 것이 좋습니다.
   - * LDAPS * 사용: LDAPS(LDAP over SSL) 옵션은 TLS를 사용하여 LDAP 서버에 연결합니다. 이 옵션은 호환성을 위해 지원됩니다.
   - * TLS * 사용 안 함: StorageGRID 시스템과 LDAP 서버 간의 네트워크 트래픽은 보호되지 않습니다.

     Active Directory 서버가 LDAP 서명을 적용하는 경우에는 이 옵션이 지원되지 않습니다. 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. LDAP 서버에 대한 연결 설정을 확인하려면 * 연결 테스트 * 를 선택합니다.

   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

"테넌트 관리 권한"

"OpenLDAP 서버 구성 지침"

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.

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 테넌트 관리자에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.
- 저장된 ID 소스를 활성화해야 합니다.

단계

1. 액세스 관리 * > * ID 페더레이션 * 을 선택합니다.

   ID 페더레이션 페이지가 나타납니다. 동기화 서버 * 버튼은 페이지 오른쪽 상단에 있습니다.

   > 저장된 ID 소스가 활성화되어 있지 않으면 * 동기화 서버 * 버튼이 활성화되지 않습니다.

2. 동기화 서버 * 를 선택합니다.

   동기화가 성공적으로 시작되었음을 나타내는 확인 메시지가 표시됩니다.

관련 정보

"테넌트 관리 권한"

ID 페더레이션을 사용하지 않도록 설정합니다

이 테넌트에 대해 ID 페더레이션 서비스를 구성한 경우 테넌트 그룹 및 사용자에 대한 ID 페더레이션을 일시적으로 또는 영구적으로 비활성화할 수 있습니다. ID 페더레이션을

비활성화하면 StorageGRID 시스템과 ID 소스 간에 통신이 이루어지지 않습니다. 그러나 구성한 설정은 그대로 유지되므로 나중에 ID 페더레이션을 쉽게 다시 활성화할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 테넌트 관리자에 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 테넌트 계정에 대한 액세스 권한을 유지하지만 세션이 만료된 후에는 로그인할 수 없습니다.
- StorageGRID 시스템과 ID 소스 간의 동기화는 수행되지 않습니다.

단계

1. 액세스 관리 * > * ID 페더레이션 * 을 선택합니다.
2. ID 페더레이션 사용 * 확인란의 선택을 취소합니다.
3. 저장 * 을 선택합니다.

관련 정보

"테넌트 관리 권한"

그룹 관리

테넌트 사용자가 수행할 수 있는 작업을 제어하기 위해 사용자 그룹에 권한을 할당합니다. Active Directory 또는 OpenLDAP와 같은 ID 소스에서 통합 그룹을 가져오거나 로컬 그룹을 생성할 수 있습니다.

StorageGRID 시스템에 SSO(Single Sign-On)가 설정되어 있으면 그룹 사용 권한에 따라 S3 및 Swift 리소스에 액세스할 수 있지만 로컬 사용자는 테넌트 관리자에 로그인할 수 없습니다.

테넌트 관리 권한

테넌트 그룹을 생성하기 전에 해당 그룹에 할당할 권한을 고려하십시오. 테넌트 관리 권한은 사용자가 테넌트 관리자 또는 테넌트 관리 API를 사용하여 수행할 수 있는 작업을 결정합니다. 사용자는 하나 이상의 그룹에 속할 수 있습니다. 사용자가 여러 그룹에 속한 경우 권한은 누적됩니다.

테넌트 관리자에 로그인하거나 테넌트 관리 API를 사용하려면 사용자가 하나 이상의 권한이 있는 그룹에 속해야 합니다. 로그인할 수 있는 모든 사용자는 다음 작업을 수행할 수 있습니다.

- 대시보드 보기
- 자신의 암호 변경(로컬 사용자의 경우)

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 전용으로 설정되어 있는 경우 사용자는 선택한 모든 설정 및 기능에 대해 읽기 전용 권한을 갖게 됩니다.

그룹에 다음 권한을 할당할 수 있습니다. S3 테넌트와 Swift 테넌트는 다른 그룹 권한을 가집니다. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

권한	설명
루트 액세스	테넌트 관리자 및 테넌트 관리 API에 대한 전체 액세스를 제공합니다. • 참고: * Swift 사용자는 테넌트 계정에 로그인하려면 루트 액세스 권한이 있어야 합니다.
관리자	Swift 테넌트만 해당. 이 테넌트 계정에 대한 Swift 컨테이너 및 객체에 대한 전체 액세스를 제공합니다 • 참고: * Swift 사용자는 Swift REST API를 사용하여 모든 작업을 수행하려면 Swift 관리자 권한이 있어야 합니다.
자신의 S3 자격 증명을 관리합니다	S3 테넌트만 해당. 사용자가 자신의 S3 액세스 키를 생성하고 제거할 수 있습니다. 이 권한이 없는 사용자는 * storage(S3) * > * My S3 access keys * 메뉴 옵션을 볼 수 없습니다.
모든 버킷 관리	• S3 테넌트: 사용자가 테넌트 관리자 및 테넌트 관리 API를 사용하여 S3 버킷을 생성 및 삭제하고 S3 버킷 또는 그룹 정책에 관계없이 테넌트 계정의 모든 S3 버킷을 관리할 수 있습니다. 이 권한이 없는 사용자는 * Bucket * 메뉴 옵션을 볼 수 없습니다. • Swift 테넌트: Swift 사용자가 테넌트 관리 API를 사용하여 Swift 컨테이너의 정합성 수준을 제어할 수 있습니다. • 참고: * 테넌트 관리 API에서 Swift 그룹에만 모든 버킷 관리 권한을 할당할 수 있습니다. 테넌트 관리자를 사용하여 Swift 그룹에 이 권한을 할당할 수 없습니다.
엔드포인트 관리	S3 테넌트만 해당. 테넌트 관리자 또는 테넌트 관리 API를 사용하여 StorageGRID 플랫폼 서비스의 대상으로 사용되는 엔드포인트를 생성하거나 편집할 수 있습니다. 이 권한이 없는 사용자는 * 플랫폼 서비스 끝점 * 메뉴 옵션을 볼 수 없습니다.

관련 정보

"S3을 사용합니다"

"Swift를 사용합니다"

S3 테넌트에 대한 그룹 생성 중

통합 그룹을 가져오거나 로컬 그룹을 생성하여 S3 사용자 그룹에 대한 권한을 관리할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 테넌트 관리자에 로그인해야 합니다.
- 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다.
- 통합 그룹을 가져오려는 경우 ID 페더레이션을 구성하고 통합 그룹이 이미 구성된 ID 소스에 있습니다.

단계

1. 액세스 관리 * > * 그룹 * 을 선택합니다.

2. Create group * 을 선택합니다.
3. 로컬 그룹을 생성하려면 * Local group * 탭을 선택하고, 이전에 구성된 ID 소스에서 그룹을 가져오려면 * Federated group * 탭을 선택합니다.

   StorageGRID 시스템에서 SSO(Single Sign-On)를 사용하는 경우 로컬 그룹에 속한 사용자는 그룹 권한에 따라 클라이언트 애플리케이션을 사용하여 테넌트의 리소스를 관리할 수 있지만 테넌트 관리자에 로그인할 수 없습니다.

4. 그룹의 이름을 입력합니다.
   - * 로컬 그룹 *: 표시 이름과 고유 이름을 모두 입력합니다. 나중에 표시 이름을 편집할 수 있습니다.
   - * 페더레이션 그룹 *: 고유한 이름을 입력합니다. Active Directory의 경우 고유한 이름은 에 연결된 이름입니다 `sAMAccountName` 속성. OpenLDAP의 경우 고유한 이름은 에 연결된 이름입니다 `uid` 속성.
5. Continue * 를 선택합니다.
6. 액세스 모드를 선택합니다. 사용자가 여러 그룹에 속해 있고 모든 그룹이 읽기 전용으로 설정되어 있는 경우 사용자는 선택한 모든 설정 및 기능에 대해 읽기 전용 권한을 갖게 됩니다.
   - * 읽기-쓰기 * (기본값): 사용자는 테넌트 관리자에 로그인하여 테넌트 구성을 관리할 수 있습니다.
   - * 읽기 전용 *: 사용자는 설정 및 기능만 볼 수 있습니다. 테넌트 관리자 또는 테넌트 관리 API에서 작업을 변경하거나 수행할 수 없습니다. 로컬 읽기 전용 사용자는 자신의 암호를 변경할 수 있습니다.
7. 이 그룹에 대한 그룹 권한을 선택합니다.

테넌트 관리 권한에 대한 정보를 참조하십시오.

8. Continue * 를 선택합니다.
9. 그룹 정책을 선택하여 이 그룹의 구성원이 가질 S3 액세스 권한을 결정합니다.
   - * S3 액세스 없음 *: 기본값. 이 그룹의 사용자는 버킷 정책을 통해 액세스가 부여되지 않는 한 S3 리소스에 액세스할 수 없습니다. 이 옵션을 선택하면 루트 사용자만 기본적으로 S3 리소스에 액세스할 수 있습니다.
   - * 읽기 전용 액세스 *: 이 그룹의 사용자는 S3 리소스에 대한 읽기 전용 액세스 권한을 가집니다. 예를 들어 이 그룹의 사용자는 개체를 나열하고 개체 데이터, 메타데이터 및 태그를 읽을 수 있습니다. 이 옵션을 선택하면 읽기 전용 그룹 정책의 JSON 문자열이 텍스트 상자에 나타납니다. 이 문자열은 편집할 수 없습니다.
   - * 전체 액세스 *: 이 그룹의 사용자는 버킷을 포함하여 S3 리소스에 대한 모든 액세스 권한을 가집니다. 이 옵션을 선택하면 전체 액세스 그룹 정책의 JSON 문자열이 텍스트 상자에 나타납니다. 이 문자열은 편집할 수 없습니다.
   - * 사용자 정의 *: 그룹의 사용자에게는 텍스트 상자에 지정한 사용 권한이 부여됩니다. 언어 구문 및 예제를 비롯한 그룹 정책에 대한 자세한 내용은 S3 클라이언트 애플리케이션 구현 지침을 참조하십시오.
10. 사용자 정의 * 를 선택한 경우 그룹 정책을 입력합니다. 각 그룹 정책은 크기 제한이 5,120바이트입니다. 올바른 JSON 형식 문자열을 입력해야 합니다.

    이 예제에서 그룹 구성원은 지정된 버킷의 사용자 이름(키 접두사)과 일치하는 폴더만 나열하고 액세스할 수 있습니다. 이러한 폴더의 개인 정보를 확인할 때는 다른 그룹 정책 및 버킷 정책의 액세스 권한을 고려해야 합니다.

11. 통합 그룹을 생성하는지 또는 로컬 그룹을 생성하는지에 따라 표시되는 버튼을 선택합니다.
    - 통합 그룹: * 그룹 생성 *
    - 로컬 그룹: * 계속 *

로컬 그룹을 만드는 경우 * Continue * 를 선택하면 4단계(사용자 추가)가 나타납니다. 이 단계는 통합 그룹에 대해서는 나타나지 않습니다.

12. 그룹에 추가할 각 사용자에 대한 확인란을 선택한 다음 * 그룹 생성 * 을 선택합니다.

    필요에 따라 사용자를 추가하지 않고 그룹을 저장할 수 있습니다. 나중에 그룹에 사용자를 추가하거나 새 사용자를 추가할 때 그룹을 선택할 수 있습니다.

13. 마침 * 을 선택합니다.

    생성한 그룹이 그룹 목록에 나타납니다. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

관련 정보

"테넌트 관리 권한"

"S3을 사용합니다"

Swift 테넌트에 대한 그룹을 생성하는 중입니다

통합 그룹을 가져오거나 로컬 그룹을 생성하여 Swift 테넌트 계정에 대한 액세스 권한을 관리할 수 있습니다. 하나 이상의 그룹에 Swift 관리자 권한이 있어야 합니다. 이 권한은 Swift 테넌트 계정의 컨테이너 및 개체를 관리하는 데 필요합니다.

필요한 것

- 지원되는 브라우저를 사용하여 테넌트 관리자에 로그인해야 합니다.
- 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다.
- 통합 그룹을 가져오려는 경우 ID 페더레이션을 구성하고 통합 그룹이 이미 구성된 ID 소스에 있습니다.

단계

1. 액세스 관리 * > * 그룹 * 을 선택합니다.

2. Create group * 을 선택합니다.
3. 로컬 그룹을 생성하려면 * Local group * 탭을 선택하고, 이전에 구성된 ID 소스에서 그룹을 가져오려면 * Federated group * 탭을 선택합니다.

   StorageGRID 시스템에서 SSO(Single Sign-On)를 사용하는 경우 로컬 그룹에 속한 사용자는 그룹 권한에 따라 클라이언트 애플리케이션을 사용하여 테넌트의 리소스를 관리할 수 있지만 테넌트 관리자에 로그인할 수 없습니다.

4. 그룹의 이름을 입력합니다.
   - * 로컬 그룹 *: 표시 이름과 고유 이름을 모두 입력합니다. 나중에 표시 이름을 편집할 수 있습니다.
   - * 페더레이션 그룹 *: 고유한 이름을 입력합니다. Active Directory의 경우 고유한 이름은 에 연결된 이름입니다 `sAMAccountName` 속성. OpenLDAP의 경우 고유한 이름은 에 연결된 이름입니다 `uid` 속성.
5. Continue * 를 선택합니다.
6. 액세스 모드를 선택합니다. 사용자가 여러 그룹에 속해 있고 모든 그룹이 읽기 전용으로 설정되어 있는 경우 사용자는 선택한 모든 설정 및 기능에 대해 읽기 전용 권한을 갖게 됩니다.
   - * 읽기-쓰기 * (기본값): 사용자는 테넌트 관리자에 로그인하여 테넌트 구성을 관리할 수 있습니다.
   - * 읽기 전용 *: 사용자는 설정 및 기능만 볼 수 있습니다. 테넌트 관리자 또는 테넌트 관리 API에서 작업을 변경하거나 수행할 수 없습니다. 로컬 읽기 전용 사용자는 자신의 암호를 변경할 수 있습니다.
7. 그룹 권한을 설정합니다.
   - 사용자가 테넌트 관리자 또는 테넌트 관리 API에 로그인해야 하는 경우 * Root Access * 확인란을 선택합니다. (기본값)
   - 사용자가 테넌트 관리자 또는 테넌트 관리 API에 액세스할 필요가 없는 경우 * Root Access * (루트 액세스 *) 확인란의 선택을 취소합니다. 예를 들어, 테넌트에 액세스할 필요가 없는 응용 프로그램의 확인란을 선택 취소합니다. 그런 다음 이러한 사용자가 컨테이너 및 개체를 관리할 수 있도록 * Swift 관리자 * 권한을 할당합니다.
8. Continue * 를 선택합니다.
9. 사용자가 Swift REST API를 사용할 수 있어야 하는 경우 * Swift administrator * 확인란을 선택합니다.

Swift 사용자는 테넌트 관리자에 액세스하려면 루트 액세스 권한이 있어야 합니다. 그러나 루트 액세스 권한은 사용자가 Swift REST API에 인증하여 컨테이너를 생성하고 객체를 수집하는 것을 허용하지 않습니다. 사용자는 Swift REST API에 인증할 수 있는 Swift 관리자 권한이 있어야 합니다.

10. 통합 그룹을 생성하는지 또는 로컬 그룹을 생성하는지에 따라 표시되는 버튼을 선택합니다.
    - 통합 그룹: * 그룹 생성 *
    - 로컬 그룹: * 계속 *

      로컬 그룹을 만드는 경우 * Continue * 를 선택하면 4단계(사용자 추가)가 나타납니다. 이 단계는 통합 그룹에 대해서는 나타나지 않습니다.

11. 그룹에 추가할 각 사용자에 대한 확인란을 선택한 다음 * 그룹 생성 * 을 선택합니다.

    필요에 따라 사용자를 추가하지 않고 그룹을 저장할 수 있습니다. 나중에 그룹에 사용자를 추가하거나 새 사용자를 만들 때 그룹을 선택할 수 있습니다.

12. 마침 * 을 선택합니다.

    생성한 그룹이 그룹 목록에 나타납니다. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

관련 정보

"테넌트 관리 권한"

"Swift를 사용합니다"

그룹 세부 정보 보기 및 편집

그룹의 세부 정보를 볼 때 그룹의 표시 이름, 사용 권한, 정책 및 그룹에 속한 사용자를 변경할 수 있습니다.

필요한 것

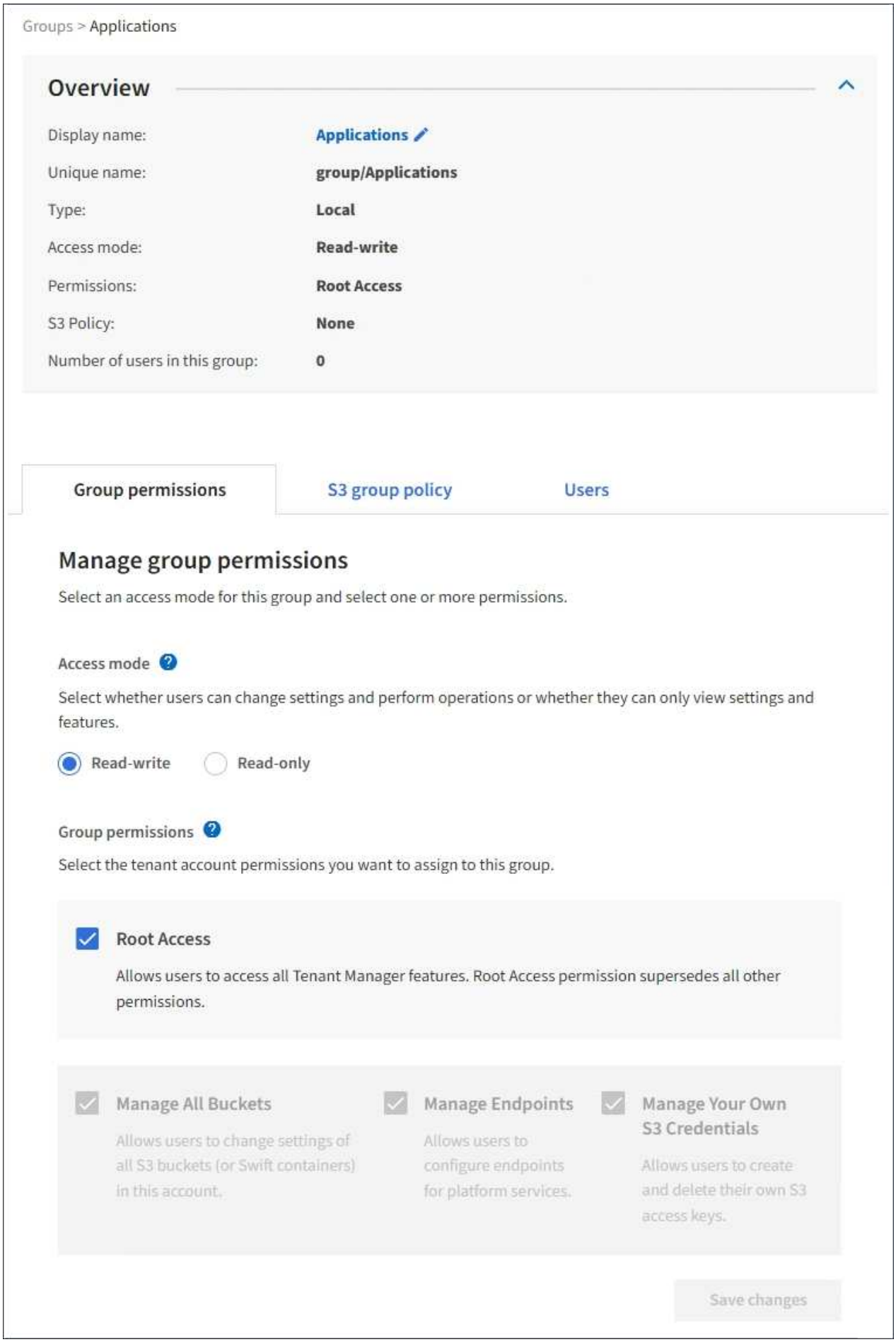
- 지원되는 브라우저를 사용하여 테넌트 관리자에 로그인해야 합니다.
- 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다.

단계

1. 액세스 관리 * > * 그룹 * 을 선택합니다.
2. 세부 정보를 보거나 편집할 그룹의 이름을 선택합니다.

   또는 * Actions * > * View group details * 를 선택할 수 있습니다.

   그룹 세부 정보 페이지가 나타납니다. 다음 예에서는 S3 그룹 세부 정보 페이지를 보여 줍니다.


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. 필요에 따라 그룹 설정을 변경합니다.

   변경 내용을 저장하려면 각 섹션을 변경한 후 * 변경 사항 저장 * 을 선택합니다. 변경 내용이 저장되면 페이지의 오른쪽 상단에 확인 메시지가 나타납니다.

   a. 선택적으로 표시 이름 또는 편집 아이콘을 선택합니다 표시 이름을 업데이트합니다.

      그룹의 고유한 이름은 변경할 수 없습니다. 통합 그룹의 표시 이름은 편집할 수 없습니다.

   b. 필요에 따라 사용 권한을 업데이트합니다.

   c. 그룹 정책의 경우 S3 또는 Swift 테넌트를 적절하게 변경합니다.

      - S3 테넌트의 그룹을 편집하는 경우 선택적으로 다른 S3 그룹 정책을 선택합니다. 사용자 지정 S3 정책을 선택한 경우 필요에 따라 JSON 문자열을 업데이트합니다.
      - Swift 테넌트의 그룹을 편집하는 경우, 필요에 따라 * Swift 관리자 * 확인란을 선택하거나 선택 취소합니다.

        Swift 관리자 권한에 대한 자세한 내용은 Swift 테넌트에 대한 그룹 생성 지침을 참조하십시오.

   d. 필요에 따라 사용자를 추가 또는 제거합니다.

4. 변경한 각 섹션에 대해 * 변경 사항 저장 * 을 선택했는지 확인합니다.

   캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

관련 정보

"S3 테넌트에 대한 그룹 생성 중"

"Swift 테넌트에 대한 그룹을 생성하는 중입니다"

로컬 그룹에 사용자 추가

필요에 따라 로컬 그룹에 사용자를 추가할 수 있습니다.

필요한 것

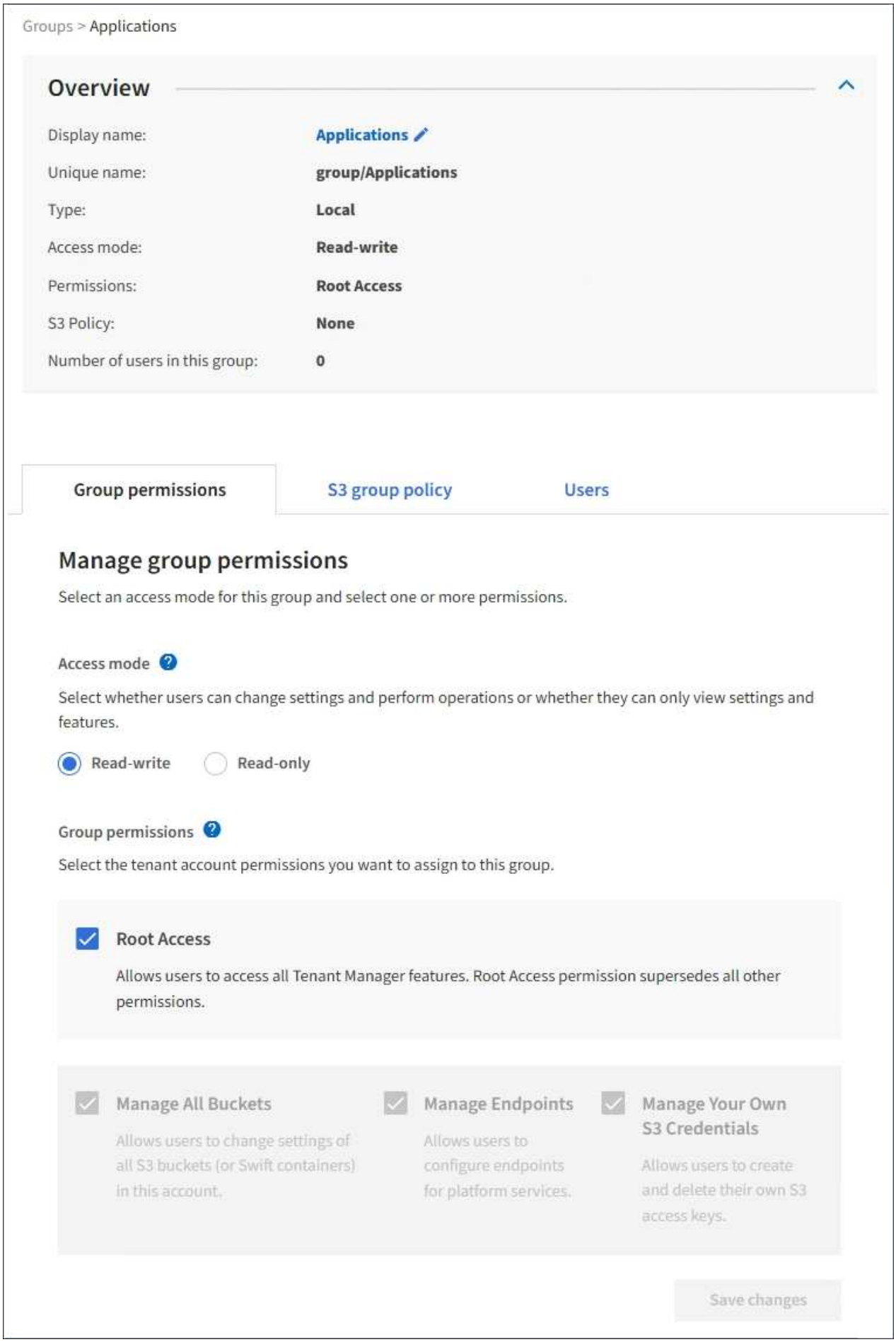
- 지원되는 브라우저를 사용하여 테넌트 관리자에 로그인해야 합니다.
- 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다.

단계

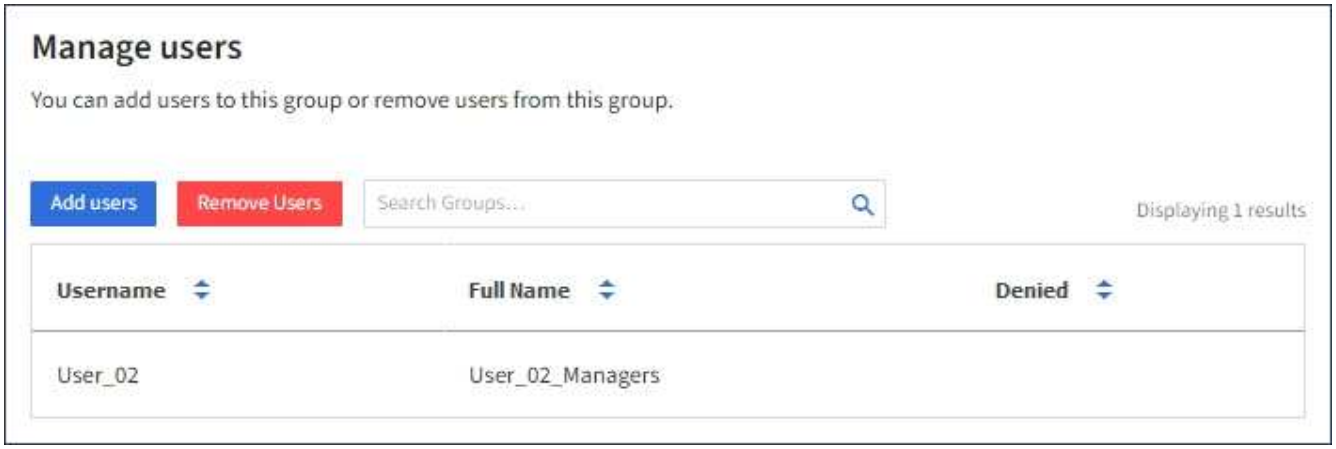
1. 액세스 관리 * > * 그룹 * 을 선택합니다.
2. 사용자를 추가할 로컬 그룹의 이름을 선택합니다.

   또는 * Actions * > * View group details * 를 선택할 수 있습니다.

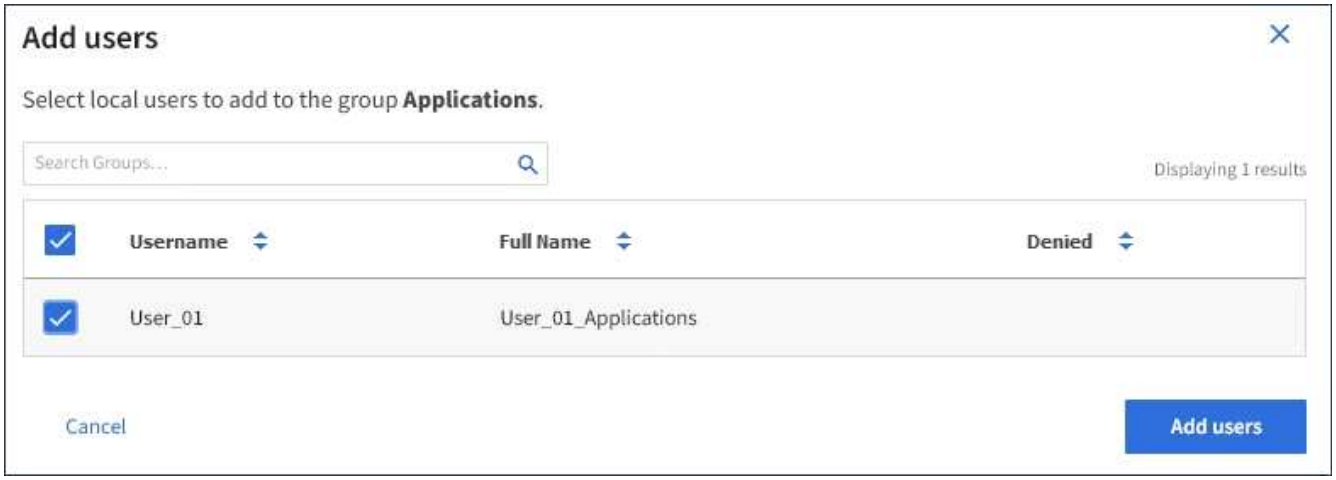
   그룹 세부 정보 페이지가 나타납니다.


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. 사용자 관리 * 를 선택한 다음 * 사용자 추가 * 를 선택합니다.



4. 그룹에 추가할 사용자를 선택한 다음 * 사용자 추가 * 를 선택합니다.



페이지의 오른쪽 상단에 확인 메시지가 나타납니다. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

그룹 이름 편집

그룹의 표시 이름을 편집할 수 있습니다. 그룹의 고유한 이름은 편집할 수 없습니다.

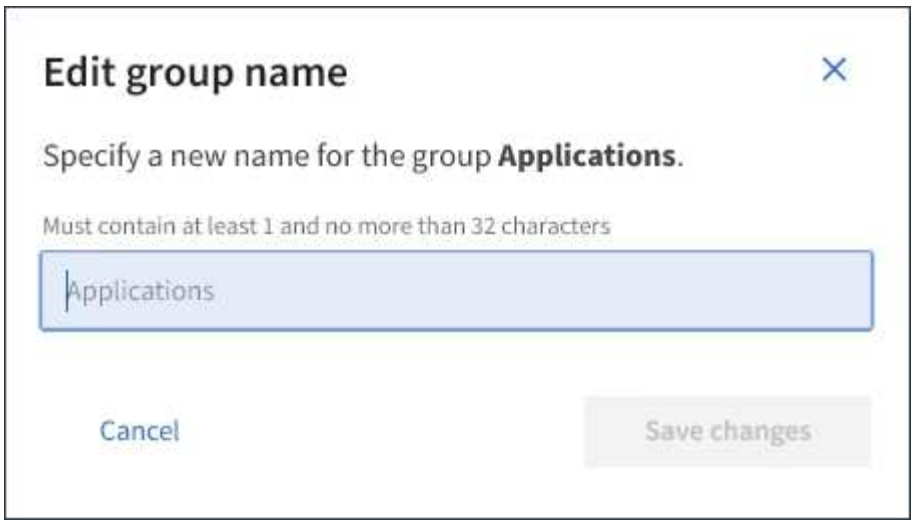
필요한 것

- 지원되는 브라우저를 사용하여 테넌트 관리자에 로그인해야 합니다.
- 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다.

단계

1. 액세스 관리 * > * 그룹 * 을 선택합니다.
2. 표시 이름을 편집할 그룹의 확인란을 선택합니다.
3. Actions * > * Edit group name * 을 선택합니다.

   Edit group name(그룹 이름 편집) 대화 상자가 나타납니다.



4. 로컬 그룹을 편집하는 경우 필요에 따라 표시 이름을 업데이트합니다.

   그룹의 고유한 이름은 변경할 수 없습니다. 통합 그룹의 표시 이름은 편집할 수 없습니다.

5. 변경 내용 저장 * 을 선택합니다.

   페이지의 오른쪽 상단에 확인 메시지가 나타납니다. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

관련 정보

"테넌트 관리 권한"

그룹 복제

기존 그룹을 복제하면 새 그룹을 더 빠르게 만들 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 테넌트 관리자에 로그인해야 합니다.
- 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다.

단계

1. 액세스 관리 * > * 그룹 * 을 선택합니다.
2. 복제할 그룹의 확인란을 선택합니다.
3. Duplicate group * 을 선택합니다. 그룹을 생성하는 방법에 대한 자세한 내용은 S3 테넌트 또는 Swift 테넌트용 그룹을 생성하는 지침을 참조하십시오.
4. 로컬 그룹을 생성하려면 * Local group * 탭을 선택하고, 이전에 구성된 ID 소스에서 그룹을 가져오려면 * Federated group * 탭을 선택합니다.

   StorageGRID 시스템에서 SSO(Single Sign-On)를 사용하는 경우 로컬 그룹에 속한 사용자는 그룹 권한에 따라 클라이언트 애플리케이션을 사용하여 테넌트의 리소스를 관리할 수 있지만 테넌트 관리자에 로그인할 수 없습니다.

5. 그룹의 이름을 입력합니다.

◦ * 로컬 그룹 *: 표시 이름과 고유 이름을 모두 입력합니다. 나중에 표시 이름을 편집할 수 있습니다.

◦ * 페더레이션 그룹 *: 고유한 이름을 입력합니다. Active Directory의 경우 고유한 이름은 에 연결된 이름입니다 `sAMAccountName` 속성. OpenLDAP의 경우 고유한 이름은 에 연결된 이름입니다 `uid` 속성.

6. Continue * 를 선택합니다.
7. 필요에 따라 이 그룹에 대한 권한을 수정합니다.
8. Continue * 를 선택합니다.
9. 필요에 따라 S3 테넌트에 대한 그룹을 복제할 경우 * S3 정책 추가 * 라디오 버튼에서 다른 정책을 선택할 수도 있습니다. 사용자 지정 정책을 선택한 경우 필요에 따라 JSON 문자열을 업데이트합니다.
10. Create group * 을 선택합니다.

관련 정보

"S3 테넌트에 대한 그룹 생성 중"

"Swift 테넌트에 대한 그룹을 생성하는 중입니다"

"테넌트 관리 권한"

그룹을 삭제하는 중입니다

시스템에서 그룹을 삭제할 수 있습니다. 해당 그룹에만 속하는 사용자는 더 이상 테넌트 관리자에 로그인하거나 테넌트 계정을 사용할 수 없습니다.

필요한 것

- 지원되는 브라우저를 사용하여 테넌트 관리자에 로그인해야 합니다.
- 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다.

단계

1. 액세스 관리 * > * 그룹 * 을 선택합니다.

2. 삭제할 그룹의 확인란을 선택합니다.
3. Actions * > * Delete group * 을 선택합니다.

   확인 메시지가 나타납니다.

4. 확인 메시지에 표시된 그룹을 삭제하려면 * Delete group * 을 선택합니다.

   페이지의 오른쪽 상단에 확인 메시지가 나타납니다. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

관련 정보

"테넌트 관리 권한"

로컬 사용자 관리

로컬 사용자를 만들고 로컬 그룹에 할당하여 사용자가 액세스할 수 있는 기능을 결정할 수 있습니다. Tenant Manager에는 ""root""라는 이름의 미리 정의된 로컬 사용자가 한 명 있습니다. 로컬 사용자를 추가 및 제거할 수는 있지만 루트 사용자는 제거할 수 없습니다.

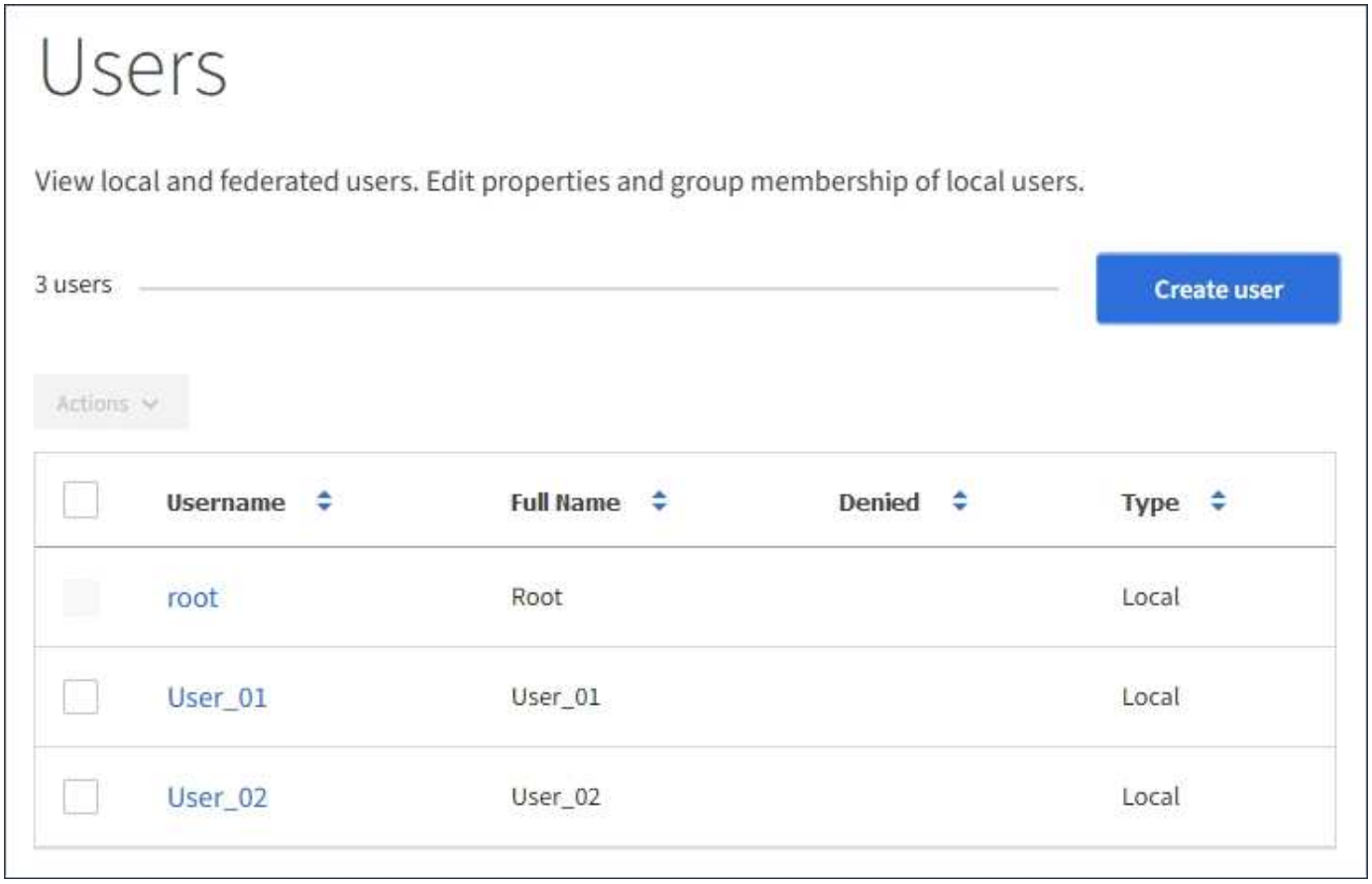
필요한 것

- 지원되는 브라우저를 사용하여 테넌트 관리자에 로그인해야 합니다.
- 루트 액세스 권한이 있는 읽기-쓰기 사용자 그룹에 속해야 합니다.

> StorageGRID 시스템에서 SSO(Single Sign-On)가 활성화된 경우 그룹 사용 권한에 따라 S3 또는 Swift 클라이언트 애플리케이션을 사용하여 테넌트의 리소스에 액세스할 수 있지만 로컬 사용자는 테넌트 관리자 또는 테넌트 관리 API에 로그인할 수 없습니다.

사용자 페이지에 액세스

액세스 관리 * > * 사용자 * 를 선택합니다.



로컬 사용자 생성 중

로컬 사용자를 만들고 하나 이상의 로컬 그룹에 할당하여 액세스 권한을 제어할 수 있습니다.

그룹에 속하지 않은 S3 사용자는 관리 권한이나 S3 그룹 정책이 적용되지 않습니다. 이러한 사용자는 버킷 정책을 통해 S3 버킷 액세스가 부여될 수 있습니다.

그룹에 속하지 않는 Swift 사용자는 관리 권한이나 Swift 컨테이너 액세스 권한이 없습니다.

단계

1. 사용자 생성 * 을 선택합니다.
2. 다음 필드를 작성합니다.
   - * 전체 이름 *: 이 사용자의 전체 이름(예: 사용자의 이름 및 성 또는 응용 프로그램 이름)입니다.
   - * 사용자 이름 *: 이 사용자가 로그인하는 데 사용할 이름입니다. 사용자 이름은 고유해야 하며 변경할 수 없습니다.
   - * 암호 * : 사용자가 로그인할 때 사용하는 암호입니다.
   - * 암호 확인 *: 암호 필드에 입력한 것과 동일한 암호를 입력합니다.
   - * 액세스 거부 *: * 예 * 를 선택하면 사용자가 하나 이상의 그룹에 속해 있더라도 이 사용자는 테넌트 계정에 로그인할 수 없습니다.

예를 들어 이 기능을 사용하여 사용자의 로그인 기능을 일시적으로 중단할 수 있습니다.

3. Continue * 를 선택합니다.
4. 사용자를 하나 이상의 로컬 그룹에 할당합니다.

   그룹에 속하지 않은 사용자에게는 관리 권한이 없습니다. 권한은 누적됩니다. 사용자는 자신이 속한 모든 그룹에 대한 모든 권한을 갖게 됩니다.

5. 사용자 생성 * 을 선택합니다.

   캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

사용자 세부 정보 편집

사용자의 세부 정보를 편집할 때 사용자의 전체 이름과 암호를 변경하고, 사용자를 다른 그룹에 추가하고, 사용자가 테넌트에 액세스하지 못하도록 할 수 있습니다.

단계

1. 사용자 목록에서 세부 정보를 보거나 편집할 사용자의 이름을 선택합니다.

   또는 사용자의 확인란을 선택한 다음 * Actions * > * View user details * 를 선택합니다.

2. 필요에 따라 사용자 설정을 변경합니다.
   a. 필요에 따라 전체 이름 또는 편집 아이콘을 선택하여 사용자의 전체 이름을 변경합니다 개요 섹션.

      사용자 이름은 변경할 수 없습니다.

   b. 암호 * 탭에서 필요에 따라 사용자 암호를 변경합니다.
   c. Access * 탭에서 사용자가 로그인(* 아니요 * 선택)하거나 사용자가 필요에 따라 로그인하지 못하도록 합니다(* 예 * 선택).
   d. 그룹 * 탭에서 사용자를 그룹에 추가하거나 필요에 따라 그룹에서 사용자를 제거합니다.
   e. 각 섹션에 필요한 경우 * 변경 사항 저장 * 을 선택합니다.

      캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

로컬 사용자 복제

로컬 사용자를 복제하면 새 사용자를 보다 빠르게 만들 수 있습니다.

단계

1. 사용자 목록에서 복제할 사용자를 선택합니다.
2. 사용자 복제 * 를 선택합니다.
3. 새 사용자에 대해 다음 필드를 수정합니다.
   - * 전체 이름 *: 이 사용자의 전체 이름(예: 사용자의 이름 및 성 또는 응용 프로그램 이름)입니다.
   - * 사용자 이름 *: 이 사용자가 로그인하는 데 사용할 이름입니다. 사용자 이름은 고유해야 하며 변경할 수 없습니다.

- * 암호 * : 사용자가 로그인할 때 사용하는 암호입니다.
- * 암호 확인 *: 암호 필드에 입력한 것과 동일한 암호를 입력합니다.
- * 액세스 거부 *: * 예 * 를 선택하면 사용자가 하나 이상의 그룹에 속해 있더라도 이 사용자는 테넌트 계정에 로그인할 수 없습니다.

  예를 들어 이 기능을 사용하여 사용자의 로그인 기능을 일시적으로 중단할 수 있습니다.

4. Continue * 를 선택합니다.
5. 하나 이상의 로컬 그룹을 선택합니다.

   그룹에 속하지 않은 사용자에게는 관리 권한이 없습니다. 권한은 누적됩니다. 사용자는 자신이 속한 모든 그룹에 대한 모든 권한을 갖게 됩니다.

6. 사용자 생성 * 을 선택합니다.

   캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

로컬 사용자를 삭제하는 중입니다

StorageGRID 테넌트 계정에 더 이상 액세스할 필요가 없는 로컬 사용자를 영구적으로 삭제할 수 있습니다.

테넌트 관리자를 사용하여 로컬 사용자는 삭제할 수 있지만 페더레이션 사용자는 삭제할 수 없습니다. 통합 사용자를 삭제하려면 통합 ID 소스를 사용해야 합니다.

단계

1. 사용자 목록에서 삭제할 로컬 사용자의 확인란을 선택합니다.
2. Actions * > * Delete user * 를 선택합니다.
3. 확인 대화 상자에서 * 사용자 삭제 * 를 선택하여 시스템에서 사용자를 삭제할 것인지 확인합니다.

   캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

관련 정보

"테넌트 관리 권한"