



StorageGRID에 대한 액세스를 제어합니다

StorageGRID 11.7

NetApp
April 12, 2024

목차

StorageGRID에 대한 액세스를 제어합니다	1
Control StorageGRID 액세스: 개요	1
프로비저닝 암호를 변경합니다	2
노드 콘솔 암호를 변경합니다	2
ID 페더레이션을 사용합니다	4
관리 그룹을 관리합니다	9
관리자 그룹 권한	12
사용자 관리	16
SSO(Single Sign-On) 사용	19

StorageGRID에 대한 액세스를 제어합니다

Control StorageGRID 액세스: 개요

그룹 및 사용자를 만들거나 가져오고 각 그룹에 권한을 할당하여 StorageGRID에 액세스할 수 있는 사용자와 사용자가 수행할 수 있는 작업을 제어할 수 있습니다. 선택적으로 SSO(Single Sign-On)를 활성화하고, 클라이언트 인증서를 생성하고, 그리드 암호를 변경할 수 있습니다.

그리드 관리자에 대한 액세스를 제어합니다

ID 페더레이션 서비스에서 그룹과 사용자를 가져오거나 로컬 그룹 및 로컬 사용자를 설정하여 Grid Manager 및 Grid Management API에 액세스할 수 있는 사용자를 결정합니다.

사용 ["ID 제휴"](#) 설정을 구성합니다 ["그룹"](#) 및 ["사용자"](#) 또한 사용자는 익숙한 자격 증명을 사용하여 StorageGRID에 더 빠르게 로그인할 수 있습니다. Active Directory, OpenLDAP 또는 Oracle Directory Server를 사용하는 경우 ID 페더레이션을 구성할 수 있습니다.



다른 LDAP v3 서비스를 사용하려면 기술 지원 부서에 문의하십시오.

다른 작업을 할당하여 각 사용자가 수행할 수 있는 작업을 결정합니다 ["권한"](#) 확인할 수 있습니다. 예를 들어 한 그룹의 사용자가 ILM 규칙 및 다른 그룹의 사용자를 관리하여 유지 관리 작업을 수행할 수 있도록 할 수 있습니다. 시스템에 액세스하려면 사용자가 하나 이상의 그룹에 속해 있어야 합니다.

선택적으로 그룹을 읽기 전용으로 구성할 수 있습니다. 읽기 전용 그룹의 사용자는 설정과 기능만 볼 수 있습니다. 그리드 관리자 또는 그리드 관리 API에서 어떠한 변경이나 작업도 수행할 수 없습니다.

SSO(Single Sign-On)를 활성화합니다

StorageGRID 시스템은 SAML 2.0(Security Assertion Markup Language 2.0) 표준을 사용하여 SSO(Single Sign-On)를 지원합니다. 먼저 해 ["SSO를 구성하고 사용하도록 설정합니다"](#) 모든 사용자는 그리드 관리자, 테넌트 관리자, 그리드 관리 API 또는 테넌트 관리 API에 액세스하기 전에 외부 ID 공급자에 의해 인증되어야 합니다. 로컬 사용자는 StorageGRID에 로그인할 수 없습니다.

프로비저닝 암호를 변경합니다

프로비저닝 암호는 많은 설치 및 유지 관리 절차와 StorageGRID 복구 패키지 다운로드에 필요합니다. 또한 StorageGRID 시스템에 대한 그리드 토폴로지 정보와 암호화 키의 백업을 다운로드하려면 암호문도 필요합니다. 가능합니다 ["암호를 변경합니다"](#) 필요에 따라.

노드 콘솔 암호를 변경합니다

그리드의 각 노드에는 고유한 노드 콘솔 암호가 있습니다. 이 암호는 SSH를 사용하여 노드에 `"admin"`으로 로그인하거나 VM/물리적 콘솔 연결의 루트 사용자에게 로그인해야 합니다. 필요에 따라 할 수 있습니다 ["노드 콘솔 암호를 변경합니다"](#) 각 노드에 대해.

프로비저닝 암호를 변경합니다

StorageGRID 프로비저닝 암호를 변경하려면 다음 절차를 따르십시오. 복구, 확장 및 유지 보수 절차에 필요한 암호 문구입니다. 또한 그리드 토폴로지 정보, 그리드 노드 콘솔 암호 및 StorageGRID 시스템용 암호화 키가 포함된 복구 패키지 백업을 다운로드하려면 암호문이 필요합니다.

시작하기 전에

- 를 사용하여 그리드 관리자에 로그인했습니다 "[지원되는 웹 브라우저](#)".
- 유지 관리 또는 루트 액세스 권한이 있습니다.
- 현재 프로비저닝 암호가 있습니다.

이 작업에 대해

프로비저닝 암호는 많은 설치 및 유지 관리 절차와 에 필요합니다 "[복구 패키지 다운로드 중](#)". 프로비저닝 암호가 에 나와 있지 않습니다 Passwords.txt 파일. 프로비저닝 암호를 문서화하고 안전한 장소에 보관해야 합니다.

단계

1. 구성 * > * 액세스 제어 * > * 그리드 비밀번호 * 를 선택합니다.
2. 프로비저닝 암호 변경 * 에서 * 변경 * 을 선택합니다
3. 현재 프로비저닝 암호를 입력합니다.
4. 새 암호를 입력합니다. 암호는 8자 이상 32자 이하여야 합니다. 암호는 대/소문자를 구분합니다.
5. 새 프로비저닝 암호를 안전한 위치에 저장합니다. 설치, 확장 및 유지보수 절차에 필요합니다.
6. 새 암호를 다시 입력하고 * Save * 를 선택합니다.

프로비저닝 암호 변경이 완료되면 녹색 성공 배너가 표시됩니다.



Provisioning passphrase successfully changed. Go to the [Recovery Package](#) to download a new Recovery Package.

7. 복구 패키지 * 를 선택합니다.
8. 새 프로비저닝 암호를 입력하여 새 복구 패키지를 다운로드합니다.



프로비저닝 암호를 변경한 후에는 즉시 새 복구 패키지를 다운로드해야 합니다. 복구 패키지 파일을 사용하면 오류가 발생할 경우 시스템을 복원할 수 있습니다.

노드 콘솔 암호를 변경합니다

그리드의 각 노드에는 노드에 로그인해야 하는 고유한 노드 콘솔 암호가 있습니다. 다음 단계를 사용하여 그리드의 각 노드에 대한 고유한 노드 콘솔 암호를 변경합니다.

시작하기 전에

- 를 사용하여 그리드 관리자에 로그인했습니다 "[지원되는 웹 브라우저](#)".
- 유지 관리 또는 루트 액세스 권한이 있습니다.

- 현재 프로비저닝 암호가 있습니다.

이 작업에 대해

노드 콘솔 암호를 사용하여 SSH를 사용하여 노드에 "admin"으로 로그인하거나 VM/물리적 콘솔 연결의 루트 사용자에게 로그인할 수 있습니다. 노드 콘솔 암호 변경 프로세스에서는 그리드의 각 노드에 대해 새 암호를 생성하고 암호를 업데이트된 에 저장합니다 Passwords.txt 파일을 복구 패키지에 저장합니다. 암호는 Passwords.txt 파일의 암호 열에 나열됩니다.



노드 간 통신에 사용되는 SSH 키에 대해 별도의 SSH 액세스 암호가 있습니다. 이 절차에서는 SSH 액세스 암호를 변경하지 않습니다.

마법사에 액세스합니다

단계

1. 구성 * > * 액세스 제어 * > * 그리드 비밀번호 * 를 선택합니다.
2. 노드 콘솔 암호 변경 * 에서 * 변경 * 을 선택합니다.

프로비저닝 암호를 입력합니다

단계

1. 그리드의 프로비저닝 암호를 입력합니다.
2. Continue * 를 선택합니다.

현재 복구 패키지를 다운로드합니다

노드 콘솔 암호를 변경하기 전에 현재 복구 패키지를 다운로드하십시오. 노드에 대한 암호 변경 프로세스가 실패할 경우 이 파일의 암호를 사용할 수 있습니다.

단계

1. 복구 패키지 다운로드 * 를 선택합니다.
2. 복구 패키지 파일을 복사합니다 (.zip)를 사용하여 두 개의 안전하고 서로 다른 위치에 안전하게 보관합니다.



복구 패키지 파일은 StorageGRID 시스템에서 데이터를 가져오는 데 사용할 수 있는 암호화 키 및 암호가 포함되어 있으므로 안전하게 보호해야 합니다.

3. Continue * 를 선택합니다.
4. 확인 대화 상자가 나타나면 노드 콘솔 암호 변경을 시작할 준비가 되었으면 * 예 * 를 선택합니다.

이 프로세스가 시작된 후에는 취소할 수 없습니다.

노드 콘솔 암호를 변경합니다

노드 콘솔 암호 프로세스가 시작되면 새 암호를 포함하는 새 복구 패키지가 생성됩니다. 그런 다음 각 노드에서 암호가 업데이트됩니다.

단계

1. 새 복구 패키지가 생성될 때까지 기다립니다. 몇 분 정도 걸릴 수 있습니다.
2. 새 복구 패키지 다운로드 * 를 선택합니다.
3. 다운로드가 완료되면 다음을 수행합니다.
 - a. 를 엽니다 .zip 파일.
 - b. 를 포함하여 콘텐츠에 액세스할 수 있는지 확인합니다 Passwords.txt 새 노드 콘솔 암호가 들어 있는 파일입니다.
 - c. 새 복구 패키지 파일을 복사합니다 (.zip)를 사용하여 두 개의 안전하고 서로 다른 위치에 안전하게 보관합니다.



이전 복구 패키지를 덮어쓰지 마십시오.

복구 패키지 파일은 StorageGRID 시스템에서 데이터를 가져오는 데 사용할 수 있는 암호화 키 및 암호가 포함되어 있으므로 안전하게 보호해야 합니다.

4. 새 복구 패키지를 다운로드하고 콘텐츠를 확인했음을 나타내려면 확인란을 선택합니다.
5. 노드 콘솔 암호 변경 * 을 선택하고 모든 노드가 새 암호로 업데이트될 때까지 기다립니다. 이 작업은 몇 분 정도 걸릴 수 있습니다.

모든 노드에 대한 암호가 변경되면 녹색 성공 배너가 나타납니다. 다음 단계로 이동합니다.

업데이트 프로세스 중에 오류가 발생하면 배너 메시지에 암호가 변경되지 않은 노드 수가 표시됩니다. 암호가 변경되지 않은 노드에서 프로세스가 자동으로 다시 시도됩니다. 일부 노드의 암호를 변경하지 않고 프로세스가 종료되면 * Retry * (재시도 *) 버튼이 나타납니다.

하나 이상의 노드에 대한 암호 업데이트가 실패한 경우:

- a. 표에 나열된 오류 메시지를 검토합니다.
- b. 문제를 해결합니다.
- c. 재시도 * 를 선택합니다.



다시 시도하면 이전 암호 변경 시도 중에 실패한 노드의 노드 콘솔 암호만 변경됩니다.

6. 모든 노드에 대해 노드 콘솔 암호를 변경한 후 을 삭제합니다 [처음 다운로드한 복구 패키지](#)입니다.
7. 필요에 따라 * 복구 패키지 * 링크를 사용하여 새 복구 패키지의 추가 복사본을 다운로드합니다.

ID 페더레이션을 사용합니다

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

Grid Manager의 ID 페더레이션을 구성합니다

Active Directory, Azure Active Directory(Azure AD), OpenLDAP 또는 Oracle Directory Server와 같은 다른 시스템에서 관리 그룹 및 사용자를 관리하려는 경우 Grid Manager에서 ID 페더레이션을 구성할 수 있습니다.

시작하기 전에

- 를 사용하여 그리드 관리자에 로그인했습니다 ["지원되는 웹 브라우저"](#).
- 특정 액세스 권한이 있습니다.
- Active Directory, Azure AD, OpenLDAP 또는 Oracle Directory Server를 ID 공급자로 사용하고 있습니다.



목록에 없는 LDAP v3 서비스를 사용하려면 기술 지원 부서에 문의하십시오.

- OpenLDAP를 사용하려면 OpenLDAP 서버를 구성해야 합니다. 을 참조하십시오 [OpenLDAP 서버 구성 지침](#).
- SSO(Single Sign-On)를 사용하려는 경우 을 검토했습니다 ["SSO\(Single Sign-On\)에 대한 요구 사항 및 고려 사항"](#).
- LDAP 서버와의 통신에 TLS(Transport Layer Security)를 사용하려는 경우 ID 공급자는 TLS 1.2 또는 1.3을 사용합니다. 을 참조하십시오 ["발신 TLS 연결에 지원되는 암호"](#).

이 작업에 대해

Active Directory, Azure AD, OpenLDAP 또는 Oracle Directory Server와 같은 다른 시스템에서 그룹을 가져오려면 Grid Manager의 ID 소스를 구성할 수 있습니다. 다음 유형의 그룹을 가져올 수 있습니다.

- 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. 을 참조하십시오 ["테넌트 계정을 생성합니다"](#) 및 ["테넌트 계정을 사용합니다"](#) 를 참조하십시오.

구성을 입력합니다

단계

1. 구성 * > * 액세스 제어 * > * ID 페더레이션 * 을 선택합니다.
2. ID 페더레이션 사용 * 을 선택합니다.
3. LDAP 서비스 유형 섹션에서 구성할 LDAP 서비스 유형을 선택합니다.

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory	Azure	OpenLDAP	Other
------------------	-------	----------	-------

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

4. 기타 * 를 선택한 경우 LDAP 속성 섹션의 필드를 작성합니다. 그렇지 않으면 다음 단계로 이동합니다.
 - * 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. 모든 LDAP 서비스 유형에 대해 LDAP 서버 구성 섹션에 필요한 LDAP 서버 및 네트워크 연결 정보를 입력합니다.

- * 호스트 이름 *: LDAP 서버의 FQDN(정규화된 도메인 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 로그인 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
- * Active Directory *: objectSid, primaryGroupID, userAccountControl, 및 userPrincipalName
- * Azure *: accountEnabled 및 userPrincipalName

- * 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.

- * 사용자 이름 형식 바인딩 * (선택 사항): 패턴을 자동으로 확인할 수 없는 경우 StorageGRID에서 기본 사용자 이름 패턴을 사용해야 합니다.

StorageGRID가 서비스 계정에 바인딩할 수 없는 경우 사용자가 로그인할 수 있으므로 * 사용자 이름 형식 바인딩 * 을 제공하는 것이 좋습니다.

다음 패턴 중 하나를 입력합니다.

- * UserPrincipalName 패턴(Active Directory 및 Azure) *: [USERNAME]@example.com
- * 하위 수준 로그온 이름 패턴(Active Directory 및 Azure) *: example\[USERNAME]
- * 고유 이름 패턴 *: CN=[USERNAME],CN=Users,DC=example,DC=com

[UserName] * 을 서면 그대로 포함합니다.

6. TLS(전송 계층 보안) 섹션에서 보안 설정을 선택합니다.

- * STARTTLS 사용 *: STARTTLS를 사용하여 LDAP 서버와의 통신 보안을 설정합니다. 이 옵션은 Active Directory, OpenLDAP 또는 기타 에 대해 권장되지만 Azure에서는 지원되지 않습니다.
- * LDAPS * 사용: LDAPS(LDAP over SSL) 옵션은 TLS를 사용하여 LDAP 서버에 연결합니다. Azure의 경우 이 옵션을 선택해야 합니다.
- * TLS * 사용 안 함: StorageGRID 시스템과 LDAP 서버 간의 네트워크 트래픽은 보호되지 않습니다. 이 옵션은 Azure에서 지원되지 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 그리드 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.

연결을 테스트하고 구성을 저장합니다

모든 값을 입력한 후 구성을 저장하기 전에 연결을 테스트해야 합니다. StorageGRID는 LDAP 서버에 대한 연결 설정과 바인딩 사용자 이름 형식(제공한 경우)을 확인합니다.

단계

1. Test connection * 을 선택합니다.
2. 바인딩 사용자 이름 형식을 제공하지 않은 경우:
 - 연결 설정이 유효하면 "Test connection successful(연결 테스트 성공)" 메시지가 나타납니다. Save * 를 선택하여 설정을 저장합니다.
 - 연결 설정이 잘못된 경우 ""테스트 연결을 설정할 수 없습니다"" 메시지가 나타납니다. 닫기 * 를 선택합니다. 그런 다음 문제를 해결하고 연결을 다시 테스트합니다.
3. 바인딩 사용자 이름 형식을 제공한 경우 유효한 통합 사용자의 사용자 이름과 암호를 입력합니다.

예를 들어 사용자 이름과 암호를 입력합니다. @ 또는 / 같은 특수 문자를 사용자 이름에 포함하지 마십시오.

Test Connection ✕

To test the connection and the bind username format, enter the username and password of a federated user. For example, enter your own federated username and password. The test values are not saved.

Test username

The username of a federated user.

Test password

Cancel
Test Connection

- 연결 설정이 유효하면 "Test connection successful(연결 테스트 성공)" 메시지가 나타납니다. Save * 를 선택하여 설정을 저장합니다.
- 연결 설정, 바인딩 사용자 이름 형식 또는 테스트 사용자 이름과 암호가 올바르지 않으면 오류 메시지가 나타납니다. 모든 문제를 해결하고 연결을 다시 테스트합니다.

ID 소스와 강제로 동기화합니다

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

단계

1. ID 페더레이션 페이지로 이동합니다.
2. 페이지 맨 위에서 * 서버 동기화 * 를 선택합니다.

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 비활성화합니다

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 구성된 설정은 그대로 유지되므로 나중에 ID 페더레이션을 쉽게 다시 사용할 수 있습니다.

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 * 확인란이 비활성화됩니다. ID 페더레이션을 비활성화하려면 Single Sign-On 페이지의 SSO 상태가 * 사용 안 함 * 이어야 합니다. 을 참조하십시오 ["SSO\(Single Sign-On\)를 비활성화합니다"](#).

단계

1. ID 페더레이션 페이지로 이동합니다.
2. ID 페더레이션 사용 * 확인란의 선택을 취소합니다.

OpenLDAP 서버 구성 지침

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



ActiveDirectory 또는 Azure가 아닌 ID 소스의 경우 StorageGRID는 외부에서 비활성화된 사용자에게 대한 S3 액세스를 자동으로 차단하지 않습니다. S3 액세스를 차단하려면 사용자의 S3 키를 삭제하거나 모든 그룹에서 사용자를 제거합니다.

MemberOf 및 구체화 오버레이

MemberOf 및 구체화 오버레이를 활성화해야 합니다. 자세한 내용은 의 역방향 그룹 구성원 유지 관리 지침을 참조하십시오 <http://www.openldap.org/doc/admin24/index.html>["OpenLDAP 설명서: 버전 2.4 관리자 가이드"].

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.

에서 역방향 그룹 구성원 유지 관리에 대한 정보를

참조하십시오 <http://www.openldap.org/doc/admin24/index.html>["OpenLDAP 설명서: 버전 2.4 관리자 가이드"].

관리 그룹을 관리합니다

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

시작하기 전에

- 를 사용하여 그리드 관리자에 로그인했습니다 ["지원되는 웹 브라우저"](#).
- 특정 액세스 권한이 있습니다.
- 통합 그룹을 가져오려는 경우 ID 페더레이션을 구성하고 통합 그룹이 이미 구성된 ID 소스에 있습니다.

관리자 그룹을 생성합니다

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

마법사에 액세스합니다

단계

1. 구성 * > * 액세스 제어 * > * 관리 그룹 * 을 선택합니다.
2. Create group * 을 선택합니다.

그룹 유형을 선택합니다

로컬 그룹을 생성하거나 통합 그룹을 가져올 수 있습니다.

- 로컬 사용자에게 권한을 할당하려면 로컬 그룹을 만듭니다.
- 통합 그룹을 생성하여 ID 소스에서 사용자를 가져옵니다.

로컬 그룹

단계

1. 로컬 그룹 * 을 선택합니다.
2. 나중에 필요에 따라 업데이트할 수 있는 그룹의 표시 이름을 입력합니다. 예를 들어, "유지 보수 사용자" 또는 ""ILM 관리자""가 있습니다.
3. 나중에 업데이트할 수 없는 그룹의 고유 이름을 입력합니다.
4. Continue * 를 선택합니다.

통합 그룹

단계

1. 페더레이션 그룹 * 을 선택합니다.
2. 구성된 ID 소스에 표시된 대로 가져올 그룹의 이름을 정확하게 입력합니다.
 - Active Directory 및 Azure의 경우 sAMAccountName을 사용합니다.
 - OpenLDAP의 경우 CN(일반 이름)을 사용합니다.
 - 다른 LDAP의 경우 LDAP 서버에 적절한 고유한 이름을 사용합니다.
3. Continue * 를 선택합니다.

그룹 권한을 관리합니다

단계

1. 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.

2. 하나 이상의 를 선택합니다 "관리자 그룹 권한".

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

3. 로컬 그룹을 만드는 경우 * 계속 * 을 선택합니다. 통합 그룹을 만드는 경우 * 그룹 생성 * 및 * 마침 * 을 선택합니다.

사용자 추가(로컬 그룹만 해당)

단계

1. 필요에 따라 이 그룹에 대해 하나 이상의 로컬 사용자를 선택합니다.


아직 로컬 사용자를 만들지 않은 경우 사용자를 추가하지 않고 그룹을 저장할 수 있습니다. 사용자 페이지에서 이 그룹을 사용자에게 추가할 수 있습니다. 을 참조하십시오 "사용자 관리" 를 참조하십시오.

2. Create group * 과 * Finish * 를 선택합니다.

관리 그룹을 보고 편집합니다

기존 그룹에 대한 세부 정보를 보거나 그룹을 수정하거나 그룹을 복제할 수 있습니다.

- 모든 그룹의 기본 정보를 보려면 그룹 페이지의 표를 검토하십시오.
- 특정 그룹에 대한 모든 세부 정보를 보거나 그룹을 편집하려면 * 작업 * 메뉴 또는 세부 정보 페이지를 사용하십시오.

작업	작업 메뉴	세부 정보 페이지
그룹 세부 정보를 봅니다	a. 그룹의 확인란을 선택합니다. b. Actions * > * View group details * 를 선택합니다.	테이블에서 그룹 이름을 선택합니다.
표시 이름 편집(로컬 그룹만 해당)	a. 그룹의 확인란을 선택합니다. b. Actions * > * Edit group name * 을 선택합니다. c. 새 이름을 입력합니다. d. 변경 내용 저장 * 을 선택합니다.	a. 세부 정보를 표시할 그룹 이름을 선택합니다. b. 편집 아이콘을 선택합니다  . c. 새 이름을 입력합니다. d. 변경 내용 저장 * 을 선택합니다.

작업	작업 메뉴	세부 정보 페이지
액세스 모드 또는 권한을 편집합니다	a. 그룹의 확인란을 선택합니다. b. Actions * > * View group details * 를 선택합니다. c. 선택적으로 그룹의 액세스 모드를 변경합니다. d. 필요에 따라 를 선택하거나 선택 취소합니다 "관리자 그룹 권한". e. 변경 내용 저장 * 을 선택합니다.	a. 세부 정보를 표시할 그룹 이름을 선택합니다. b. 선택적으로 그룹의 액세스 모드를 변경합니다. c. 필요에 따라 를 선택하거나 선택 취소합니다 "관리자 그룹 권한". d. 변경 내용 저장 * 을 선택합니다.

그룹을 복제합니다

단계

1. 그룹의 확인란을 선택합니다.
2. Actions * > * Duplicate group * 을 선택합니다.
3. 복제 그룹 마법사를 완료합니다.

그룹을 삭제합니다

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

단계

1. 그룹 페이지에서 제거할 각 그룹에 대한 확인란을 선택합니다.
2. Actions * > * Delete group * 을 선택합니다.
3. 그룹 삭제 * 를 선택합니다.

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 Manager 또는 Grid Management API에 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 페이지에 제공된 특정 정보를 봅니다

사용 권한과 액세스 모드 간의 상호 작용

모든 권한에 대해 그룹의 * 액세스 모드 * 설정은 사용자가 설정을 변경하고 작업을 수행할 수 있는지 또는 관련 설정 및 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.

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.

알람 확인(레거시)

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.

테넌트 루트 암호를 변경합니다

이 권한은 테넌트 페이지의 * 루트 암호 변경 * 옵션에 대한 액세스를 제공하므로 테넌트의 로컬 루트 사용자의 암호를 변경할 수 있는 사용자를 제어할 수 있습니다. 이 권한은 S3 키 가져오기 기능이 활성화된 경우 S3 키를 마이그레이션하는 데도 사용됩니다. 이 권한이 없는 사용자는 * 루트 암호 변경 * 옵션을 볼 수 없습니다.



루트 암호 변경 * 옵션이 포함된 테넌트 페이지에 대한 액세스 권한을 부여하려면 * 테넌트 계정 * 권한도 할당합니다.

그리드 토폴로지 페이지 구성

이 권한은 * 지원 * > * 도구 * > * 그리드 토폴로지 * 페이지의 구성 탭에 대한 액세스를 제공합니다.

ILM을 참조하십시오

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

- 규칙
- 정책
- 삭제 코딩

- 지역
- 지원합니다



사용자는 * 기타 그리드 구성 * 및 * 그리드 토폴로지 페이지 구성 * 권한이 있어야 스토리지 등급을 관리할 수 있습니다.

유지 관리

다음 옵션을 사용하려면 사용자에게 유지 관리 권한이 있어야 합니다.

- * 구성 * > * 액세스 제어 *:
 - 그리드 암호
- * 구성 * > * 네트워크 *:
 - S3 끝점 도메인 이름
- * 유지보수 * > * 작업 *:
 - 서비스 해제
 - 확장
 - 개체 존재 여부 검사
 - 복구
- * 유지보수 * > * 시스템 *:
 - 복구 패키지
 - 소프트웨어 업데이트
- 지원 * > * 툴 *:
 - 로그

유지 관리 권한이 없는 사용자는 다음 페이지를 볼 수 있지만 편집할 수는 없습니다.

- * 유지보수 * > * 네트워크 *:
 - DNS 서버
 - 그리드 네트워크
 - NTP 서버
- * 유지보수 * > * 시스템 *:
 - 라이선스
- * 구성 * > * 네트워크 *:
 - S3 끝점 도메인 이름
- * 구성 * > * 보안 *:
 - 인증서
- * 구성 * > * 모니터링 *:

- 감사 및 syslog 서버

알림을 관리합니다

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

메트릭 쿼리

이 권한은 다음에 대한 액세스를 제공합니다.

- 지원 * > * 도구 * > * 메트릭 * 페이지
- Grid Management API의 * Metrics * 섹션을 사용하여 맞춤형 Prometheus 메트릭 쿼리를 수행합니다
- 메트릭이 포함된 Grid Manager 대시보드 카드

개체 메타데이터 조회

이 권한은 * ILM * > * 개체 메타데이터 조회 * 페이지에 대한 액세스를 제공합니다.

기타 그리드 구성

이 권한은 추가 그리드 구성 옵션에 대한 액세스를 제공합니다.



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

- * ILM *:
 - 보관 등급
- * 구성 * > * 시스템 *:
 - 스토리지 옵션
- 지원 * > * 알람(레거시) *:
 - 사용자 지정 이벤트
 - 전체 알람
 - 레거시 전자 메일 설정
- 지원 * > * 기타 *:
 - 링크 비용

스토리지 어플라이언스 관리자

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

테넌트 계정

이 권한은 다음 기능을 제공합니다.

- 테넌트 페이지에 액세스하여 테넌트 계정을 생성, 편집 및 제거할 수 있습니다
- 기존 트래픽 분류 정책을 봅니다
- 테넌트 세부 정보가 포함된 Grid Manager 대시보드 카드를 봅니다

사용자 관리

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

시작하기 전에

- 를 사용하여 그리드 관리자에 로그인했습니다 "[지원되는 웹 브라우저](#)".
- 특정 액세스 권한이 있습니다.

로컬 사용자를 생성합니다

하나 이상의 로컬 사용자를 생성하고 각 사용자를 하나 이상의 로컬 그룹에 할당할 수 있습니다. 그룹의 권한은 사용자가 액세스할 수 있는 Grid Manager 및 Grid Management API 기능을 제어합니다.

로컬 사용자만 생성할 수 있습니다. 외부 ID 소스를 사용하여 연결된 사용자 및 그룹을 관리합니다.

Grid Manager에는 ""root""라는 이름의 미리 정의된 로컬 사용자가 하나 있습니다. 루트 사용자를 제거할 수 없습니다.



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

마법사에 액세스합니다

단계

1. 구성 * > * 액세스 제어 * > * 관리자 사용자 * 를 선택합니다.
2. 사용자 생성 * 을 선택합니다.

사용자 자격 증명을 입력합니다

단계

1. 사용자의 전체 이름, 고유한 사용자 이름 및 암호를 입력합니다.
2. 이 사용자가 그리드 관리자 또는 그리드 관리 API에 액세스할 수 없는 경우 * 예 * 를 선택합니다(선택 사항).
3. Continue * 를 선택합니다.

그룹에 할당합니다

단계

1. 필요에 따라 사용자를 하나 이상의 그룹에 할당하여 사용자의 권한을 결정합니다.

아직 그룹을 만들지 않은 경우 그룹을 선택하지 않고 사용자를 저장할 수 있습니다. 이 사용자를 그룹 페이지의 그룹에 추가할 수 있습니다.

사용자가 여러 그룹에 속한 경우 권한은 누적됩니다. 을 참조하십시오 "[관리 그룹을 관리합니다](#)" 를 참조하십시오.

2. Create user * 를 선택하고 * Finish * 를 선택합니다.

로컬 사용자를 보고 편집합니다

기존 로컬 및 통합 사용자에 대한 세부 정보를 볼 수 있습니다. 로컬 사용자를 수정하여 사용자의 전체 이름, 암호 또는 그룹 구성원을 변경할 수 있습니다. 사용자가 그리드 관리자 및 그리드 관리 API에 일시적으로 액세스하지 못하도록 할 수도 있습니다.


로컬 사용자만 편집할 수 있습니다. 외부 ID 소스를 사용하여 페더레이션 사용자를 관리합니다.

- 모든 로컬 및 통합 사용자에 대한 기본 정보를 보려면 사용자 페이지의 표를 검토하십시오.
- 특정 사용자의 모든 세부 정보를 보거나, 로컬 사용자를 편집하거나, 로컬 사용자 암호를 변경하려면 * 작업 * 메뉴 또는 세부 정보 페이지를 사용하십시오.

다음에 사용자가 로그아웃한 다음 다시 그리드 관리자에 로그인할 때 모든 편집 내용이 적용됩니다.



로컬 사용자는 Grid Manager 배너에 있는 * 암호 변경 * 옵션을 사용하여 자신의 암호를 변경할 수 있습니다.

작업	작업 메뉴	세부 정보 페이지
사용자 세부 정보를 봅니다	<ol style="list-style-type: none"> 사용자의 확인란을 선택합니다. Actions * > * View user details * 를 선택합니다. 	테이블에서 사용자 이름을 선택합니다.
전체 이름 편집(로컬 사용자만 해당)	<ol style="list-style-type: none"> 사용자의 확인란을 선택합니다. 작업 * > * 전체 이름 편집 * 을 선택합니다. 새 이름을 입력합니다. 변경 내용 저장 * 을 선택합니다. 	<ol style="list-style-type: none"> 사용자 이름을 선택하여 세부 정보를 표시합니다. 편집 아이콘을 선택합니다 . 새 이름을 입력합니다. 변경 내용 저장 * 을 선택합니다.
StorageGRID 액세스를 거부하거나 허용합니다	<ol style="list-style-type: none"> 사용자의 확인란을 선택합니다. Actions * > * View user details * 를 선택합니다. 액세스 탭을 선택합니다. 사용자가 그리드 관리자 또는 그리드 관리 API에 로그인하지 못하도록 하려면 * 예 * 를 선택하고, 사용자가 로그인할 수 있도록 하려면 * 아니요 * 를 선택합니다. 변경 내용 저장 * 을 선택합니다. 	<ol style="list-style-type: none"> 사용자 이름을 선택하여 세부 정보를 표시합니다. 액세스 탭을 선택합니다. 사용자가 그리드 관리자 또는 그리드 관리 API에 로그인하지 못하도록 하려면 * 예 * 를 선택하고, 사용자가 로그인할 수 있도록 하려면 * 아니요 * 를 선택합니다. 변경 내용 저장 * 을 선택합니다.

작업	작업 메뉴	세부 정보 페이지
암호 변경(로컬 사용자만 해당)	<ul style="list-style-type: none"> a. 사용자의 확인란을 선택합니다. b. Actions * > * View user details * 를 선택합니다. c. 암호 탭을 선택합니다. d. 새 암호를 입력합니다. e. 암호 변경 * 을 선택합니다. 	<ul style="list-style-type: none"> a. 사용자 이름을 선택하여 세부 정보를 표시합니다. b. 암호 탭을 선택합니다. c. 새 암호를 입력합니다. d. 암호 변경 * 을 선택합니다.
그룹 변경(로컬 사용자만 해당)	<ul style="list-style-type: none"> a. 사용자의 확인란을 선택합니다. b. Actions * > * View user details * 를 선택합니다. c. 그룹 탭을 선택합니다. d. 필요에 따라 그룹 이름 뒤에 있는 링크를 선택하여 새 브라우저 탭에서 그룹의 세부 정보를 봅니다. e. 다른 그룹을 선택하려면 * Edit groups * 를 선택합니다. f. 변경 내용 저장 * 을 선택합니다. 	<ul style="list-style-type: none"> a. 사용자 이름을 선택하여 세부 정보를 표시합니다. b. 그룹 탭을 선택합니다. c. 필요에 따라 그룹 이름 뒤에 있는 링크를 선택하여 새 브라우저 탭에서 그룹의 세부 정보를 봅니다. d. 다른 그룹을 선택하려면 * Edit groups * 를 선택합니다. e. 변경 내용 저장 * 을 선택합니다.

사용자를 복제합니다

기존 사용자를 복제하여 동일한 권한을 가진 새 사용자를 만들 수 있습니다.

단계

1. 사용자의 확인란을 선택합니다.
2. Actions * > * Duplicate user * 를 선택합니다.
3. 사용자 복제 마법사를 완료합니다.

사용자를 삭제합니다

로컬 사용자를 삭제하여 해당 사용자를 시스템에서 영구적으로 제거할 수 있습니다.



루트 사용자는 삭제할 수 없습니다.

단계

1. 사용자 페이지에서 제거할 각 사용자에 대한 확인란을 선택합니다.
2. Actions * > * Delete user * 를 선택합니다.
3. 사용자 삭제 * 를 선택합니다.

SSO(Single Sign-On) 사용

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. 로컬 사용자는 StorageGRID에 로그인할 수 없습니다.

Single Sign-On의 작동 방식

StorageGRID 시스템은 SAML 2.0(Security Assertion Markup Language 2.0) 표준을 사용하여 SSO(Single Sign-On)를 지원합니다.

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

SSO가 활성화되면 로그인하십시오

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.

NetApp StorageGRID[®]

Sign in

Account

Sign in

[NetApp support](#) | [NetApp.com](#)

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

NetApp StorageGRID[®]

Tenant Manager

Recent

Account

Sign in

[NetApp support](#) | [NetApp.com](#)



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 선택합니다

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

The screenshot shows a login interface titled "Sign in with your organizational account". It contains two input fields: the first is for an email address, with the placeholder text "someone@example.com"; the second is for a password, with the placeholder text "Password". Below the fields is a blue button labeled "Sign in".

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 StorageGRID 액세스 권한이 있는 통합 그룹에 속해 있는 경우 선택한 계정에 따라 그리드 관리자 또는 테넌트 관리자에 로그인됩니다.



서비스 계정에 액세스할 수 없는 경우 StorageGRID 액세스 권한이 있는 통합 그룹에 속한 기존 사용자라면 계속 로그인할 수 있습니다.

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 활성화되면 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 선택합니다.

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 • 참고: * SSO에 Azure를 사용하는 경우 모든 관리 노드에서 로그아웃하는 데 몇 분 정도 걸릴 수 있습니다.
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.

SSO(Single Sign-On)에 대한 요구 사항 및 고려 사항

StorageGRID 시스템에 대해 SSO(Single Sign-On)를 활성화하기 전에 요구 사항 및 고려 사항을 검토하십시오.

ID 공급자 요구 사항

StorageGRID는 다음 SSO ID 공급자(IDP)를 지원합니다.

- AD FS(Active Directory Federation Service)
- Azure Active Directory(Azure AD)
- PingFederate(PingFederate)

SSO ID 공급자를 구성하려면 먼저 StorageGRID 시스템에 대한 ID 페더레이션을 구성해야 합니다. ID 페더레이션에 사용하는 LDAP 서비스 유형은 구현할 수 있는 SSO 유형을 제어합니다.

구성된 LDAP 서비스 유형입니다	SSO ID 공급자에 대한 옵션
Active Directory를 클릭합니다	<ul style="list-style-type: none"> • Active Directory를 클릭합니다 • Azure를 지원합니다 • PingFederate(PingFederate)
Azure를 지원합니다	Azure를 지원합니다

AD FS 요구 사항

다음 버전의 AD FS를 사용할 수 있습니다.

- Windows Server 2022 AD FS
- Windows Server 2019 AD FS
- Windows Server 2016 AD FS



Windows Server 2016에서 을 사용해야 합니다 "[KB3201845 업데이트](#)" 또는 그 이상.

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

추가 요구 사항

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

Azure 고려 사항

Azure를 SSO 유형으로 사용하고 sAMAccountName을 접두사로 사용하지 않는 사용자 기본 이름이 있는 경우 StorageGRID와 LDAP 서버 간의 연결이 끊어지면 로그인 문제가 발생할 수 있습니다. 사용자가 로그인할 수 있도록 하려면 LDAP 서버에 대한 연결을 복원해야 합니다.

서버 인증서 요구 사항

기본적으로 StorageGRID는 각 관리 노드의 관리 인터페이스 인증서를 사용하여 그리드 관리자, 테넌트 관리자, 그리드 관리 API 및 테넌트 관리 API에 대한 액세스를 보호합니다. AD FS(사용자 트러스트), Azure(엔터프라이즈 응용 프로그램) 또는 StorageGRID에 대한 서비스 공급자 연결(PingFederate)을 구성하는 경우 서버 인증서를 StorageGRID 요청에 대한 서명 인증서로 사용합니다.

아직 등록하지 않은 경우 "[관리 인터페이스에 대한 사용자 지정 인증서를 구성했습니다](#)"이제 그렇게 해야 합니다. 사용자 지정 서버 인증서는 모든 관리 노드에 사용되며 모든 StorageGRID 신뢰할 수 있는 당사자, 엔터프라이즈 응용 프로그램 또는 SP 연결에서 사용할 수 있습니다.



사용 중인 신뢰, 엔터프라이즈 응용 프로그램 또는 SP 연결에서 관리 노드의 기본 서버 인증서를 사용하는 것은 권장되지 않습니다. 노드가 실패하고 복구되면 새로운 기본 서버 인증서가 생성됩니다. 복구된 노드에 로그인하려면 먼저 신뢰할 수 있는 당사자 신뢰, 엔터프라이즈 애플리케이션 또는 SP 연결을 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 `server.crt`.

포트 요구 사항

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. 을 참조하십시오 ["외부 방화벽에서 액세스를 제어합니다"](#).

페더레이션 사용자가 로그인할 수 있는지 확인합니다

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.

시작하기 전에

- 를 사용하여 그리드 관리자에 로그인했습니다 ["지원되는 웹 브라우저"](#).
- 특정 액세스 권한이 있습니다.
- ID 페더레이션을 이미 구성했습니다.

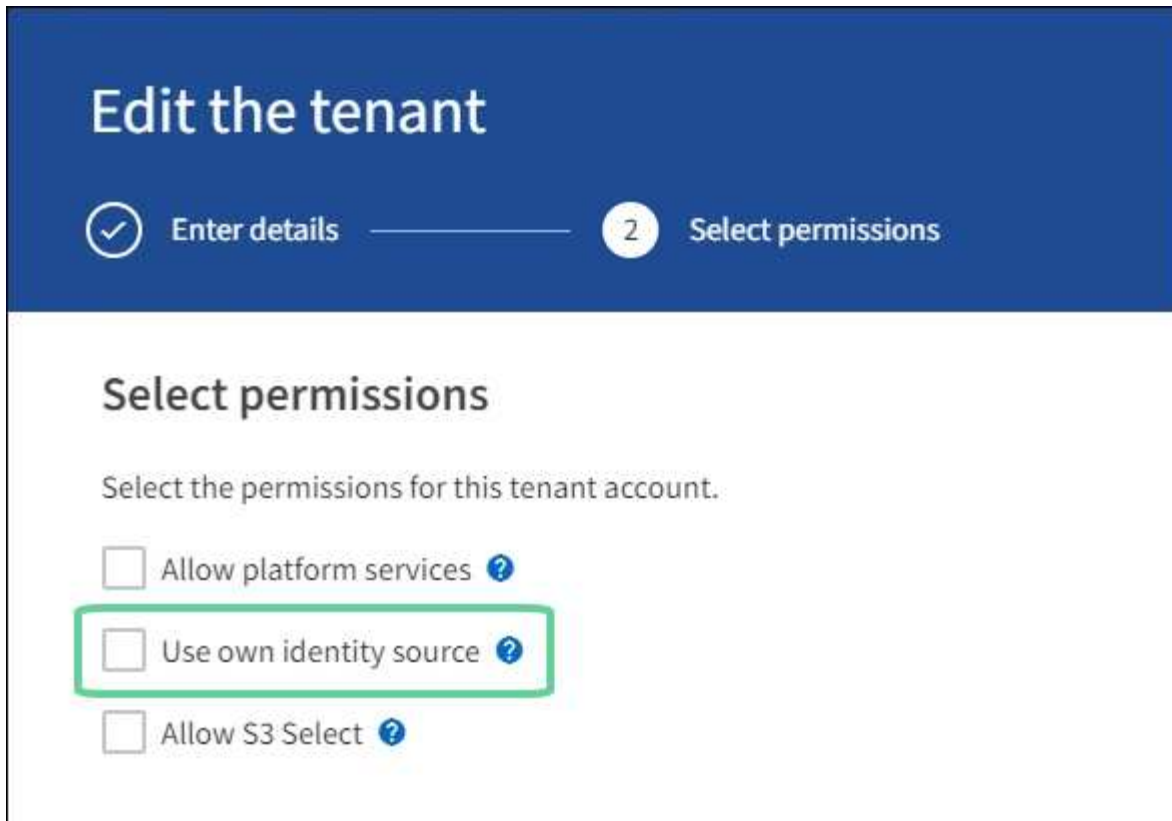
단계

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 관리 * > * 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 확인란을 선택 취소하고 * Save * 를 선택합니다.
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 * 작업 * > * 편집 * 을 선택합니다.
 - c. 세부 정보 입력 탭에서 * 계속 * 을 선택합니다.
 - d. Use own identity source * (고유 ID 소스 사용 *) 확인란을 선택한 경우, 상자의 선택을 취소하고 * Save * (저장 *)를 선택합니다.



테넌트 페이지가 나타납니다.

- 테넌트 계정을 선택하고 * 로그인 * 을 선택한 다음 테넌트 계정에 로컬 루트 사용자로 로그인합니다.
- 테넌트 관리자에서 * 액세스 관리 * > * 그룹 * 을 선택합니다.
- Grid Manager에서 하나 이상의 통합 그룹에 이 테넌트에 대한 루트 액세스 권한이 할당되었는지 확인합니다.
- 로그아웃합니다.
- 통합 그룹의 사용자로 테넌트에 다시 로그인할 수 있는지 확인합니다.

관련 정보

- ["SSO\(Single Sign-On\)에 대한 요구 사항 및 고려 사항"](#)
- ["관리 그룹을 관리합니다"](#)
- ["테넌트 계정을 사용합니다"](#)

sandbox 모드를 사용합니다

sandbox 모드를 사용하면 모든 StorageGRID 사용자가 SSO(Single Sign-On)를 사용하도록 설정하기 전에 이를 구성하고 테스트할 수 있습니다. SSO가 활성화된 후에는 구성을 변경하거나 다시 테스트해야 할 때마다 샌드박스 모드로 돌아갈 수 있습니다.

시작하기 전에

- 를 사용하여 그리드 관리자에 로그인했습니다 ["지원되는 웹 브라우저"](#).
- 루트 액세스 권한이 있습니다.
- StorageGRID 시스템에 대해 ID 페더레이션을 구성했습니다.

- ID 페더레이션 * LDAP 서비스 유형 * 의 경우 사용하려는 SSO ID 공급자에 따라 Active Directory 또는 Azure를 선택했습니다.

구성된 LDAP 서비스 유형입니다	SSO ID 공급자에 대한 옵션
Active Directory를 클릭합니다	<ul style="list-style-type: none"> • Active Directory를 클릭합니다 • Azure를 지원합니다 • PingFederate(PingFederate)
Azure를 지원합니다	Azure를 지원합니다

이 작업에 대해

SSO가 활성화되어 있고 사용자가 관리자 노드에 로그인을 시도하면 StorageGRID는 인증 요청을 SSO ID 공급자에 보냅니다. 또한 SSO ID 공급자는 인증 요청이 성공했는지 여부를 나타내는 인증 응답을 StorageGRID로 다시 보냅니다. 성공적인 요청의 경우:

- Active Directory 또는 PingFederate의 응답에는 사용자의 UUID(Universally Unique Identifier)가 포함됩니다.
- Azure의 응답에는 UPN(User Principal Name)이 포함됩니다.

StorageGRID(서비스 공급자)와 SSO ID 공급자가 사용자 인증 요청에 대해 안전하게 통신할 수 있도록 하려면 StorageGRID에서 특정 설정을 구성해야 합니다. 그런 다음 SSO ID 공급자의 소프트웨어를 사용하여 각 관리 노드에 대한 기반 AD FS(파티 트러스트), Azure(엔터프라이즈 애플리케이션) 또는 서비스 공급자(PingFederate)를 만들어야 합니다. 마지막으로 StorageGRID로 돌아가서 SSO를 활성화해야 합니다.

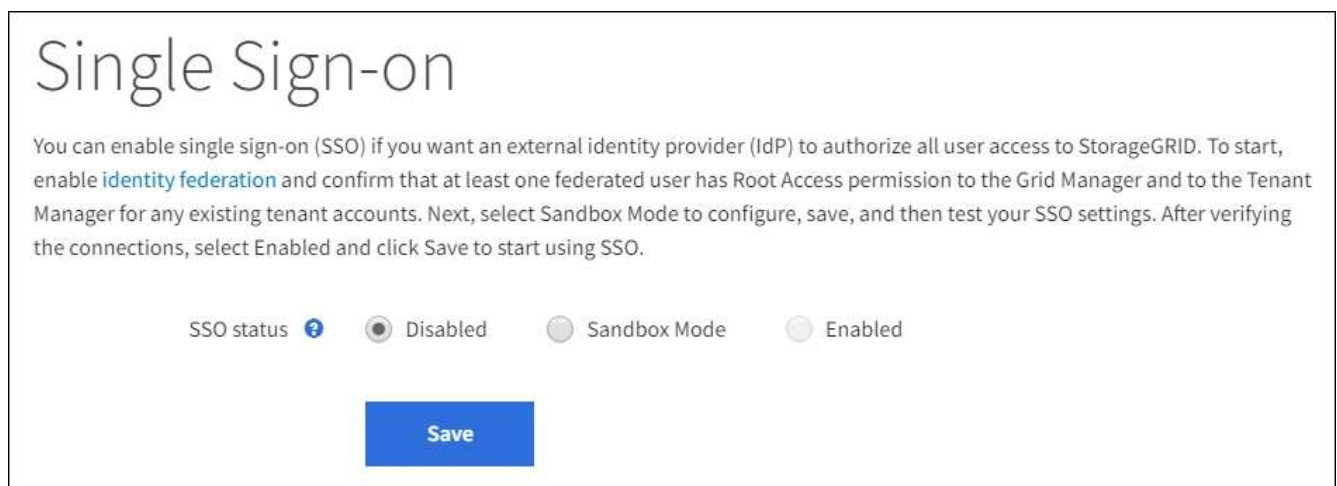
sandbox 모드를 사용하면 SSO를 활성화하기 전에 이 전면과 후면을 간편하게 구성하고 모든 설정을 테스트할 수 있습니다. 샌드박스 모드를 사용하는 경우 사용자는 SSO를 사용하여 로그인할 수 없습니다.

sandbox 모드에 액세스합니다

단계

1. 구성 * > * 액세스 제어 * > * 단일 사인온 * 을 선택합니다.

단일 사인온 페이지가 나타나고 * 비활성화 * 옵션이 선택됩니다.





SSO 상태 옵션이 나타나지 않으면 ID 공급자를 통합 ID 소스로 구성했는지 확인합니다. 을 참조하십시오 "[SSO\(Single Sign-On\)에 대한 요구 사항 및 고려 사항](#)".

2. Sandbox 모드 * 를 선택합니다.

ID 공급자 섹션이 나타납니다.

ID 공급자 세부 정보를 입력합니다

단계

1. 드롭다운 목록에서 * SSO 유형 * 을 선택합니다.
2. 선택한 SSO 유형에 따라 ID 공급자 섹션의 필드를 작성합니다.

Active Directory를 클릭합니다

1. AD FS(Active Directory Federation Service)에 표시되는 것과 동일하게 ID 공급자에 대한 * 페더레이션 서비스 이름 * 을 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.

2. ID 공급자가 StorageGRID 요청에 대한 응답으로 SSO 구성 정보를 보낼 때 연결을 보호하는 데 사용할 TLS 인증서를 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 사용자 지정 인증서의 텍스트를 복사하여 * CA 인증서 * 텍스트 상자에 붙여 넣습니다.

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

3. StorageGRID에 대한 * 사용 당사자 식별자 * 를 관련 당사자 섹션에서 지정합니다. 이 값은 AD FS의 각 기반 당사자 신뢰에 사용하는 이름을 제어합니다.

- 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]. 그러면 노드의 호스트 이름을 기반으로 시스템의 각 관리 노드에 대한 기반 당사자 식별자가 표시되는 테이블이 생성됩니다.



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.

4. 저장 * 을 선택합니다.

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



Azure를 지원합니다

1. ID 공급자가 StorageGRID 요청에 대한 응답으로 SSO 구성 정보를 보낼 때 연결을 보호하는 데 사용할 TLS 인증서를 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 사용자 지정 인증서의 텍스트를 복사하여 * CA 인증서 * 텍스트 상자에 붙여 넣습니다.

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

2. 엔터프라이즈 응용 프로그램 섹션에서 StorageGRID의 * 엔터프라이즈 응용 프로그램 이름 * 을 지정합니다. 이 값은 Azure AD의 각 엔터프라이즈 애플리케이션에 사용하는 이름을 제어합니다.

◦ 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 시스템의 각 관리 노드에 대한 엔터프라이즈 애플리케이션 이름을 표시하는 테이블이 생성됩니다.



StorageGRID 시스템의 각 관리 노드에 대해 엔터프라이즈 애플리케이션을 만들어야 합니다. 각 관리 노드에 엔터프라이즈 애플리케이션을 사용하면 사용자가 관리자 노드에 안전하게 로그인할 수 있습니다.

3. 의 단계를 따릅니다 "Azure AD에서 엔터프라이즈 애플리케이션을 생성합니다" 테이블에 나열된 각 관리 노드에 대해 엔터프라이즈 애플리케이션을 생성합니다.

4. Azure AD에서 각 엔터프라이즈 애플리케이션의 연합 메타데이터 URL을 복사합니다. 그런 다음 이 URL을 StorageGRID의 해당 * 페더레이션 메타데이터 URL * 필드에 붙여 넣습니다.

5. 모든 관리 노드에 대한 통합 메타데이터 URL을 복사하여 붙여넣은 후 * 저장 * 을 선택합니다.

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



PingFederate(PingFederate)

1. ID 공급자가 StorageGRID 요청에 대한 응답으로 SSO 구성 정보를 보낼 때 연결을 보호하는 데 사용할 TLS 인증서를 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 사용자 지정 인증서의 텍스트를 복사하여 * CA 인증서 * 텍스트 상자에 붙여 넣습니다.

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

2. 서비스 공급자(SP) 섹션에서 StorageGRID에 대한 * SP 접속 ID * 를 지정합니다. 이 값은 PingFederate의 각 SP 연결에 사용할 이름을 제어합니다.

◦ 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]. 그러면 노드의 호스트 이름을 기준으로 시스템의 각 관리 노드에 대한 SP 접속 ID가 표시되는 테이블이 생성됩니다.



StorageGRID 시스템의 각 관리 노드에 대해 SP 접속을 생성해야 합니다. 각 관리 노드에 대해 SP를 연결하면 사용자가 관리자 노드에 안전하게 로그인할 수 있습니다.

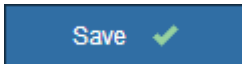
3. Federation metadata URL * 필드에서 각 관리 노드에 대한 페더레이션 메타데이터 URL을 지정합니다.

다음 형식을 사용합니다.

```
https://<Federation Service
Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP Connection
ID>
```

4. 저장 * 을 선택합니다.

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



신뢰할 수 있는 파티 트러스트, 엔터프라이즈 애플리케이션 또는 **SP** 연결을 구성합니다

구성이 저장되면 Sandbox 모드 확인 알림이 나타납니다. 이 알림은 이제 sandbox 모드가 활성화되었음을 확인하고 개요 지침을 제공합니다.

StorageGRID는 필요한 경우 샌드박스 모드로 유지될 수 있습니다. 그러나 단일 사인온 페이지에서 * Sandbox 모드 * 를 선택하면 모든 StorageGRID 사용자에게 대해 SSO가 비활성화됩니다. 로컬 사용자만 로그인할 수 있습니다.

다음 단계에 따라 사용자 트러스트(Active Directory), 엔터프라이즈 응용 프로그램(Azure) 완료 또는 SP 연결(PingFederate)을 구성합니다.

Active Directory를 클릭합니다

단계

1. AD FS(Active Directory Federation Services)로 이동합니다.
2. StorageGRID 단일 사인온 페이지의 표에 표시된 각 기반 당사자 식별자를 사용하여 StorageGRID에 대한 하나 이상의 신뢰할 수 있는 상대 트러스트를 만듭니다.

테이블에 표시된 각 관리 노드에 대해 하나의 신뢰를 만들어야 합니다.

자세한 내용은 를 참조하십시오 ["AD FS에서 기반 당사자 트러스트를 생성합니다"](#).

Azure를 지원합니다

단계

1. 현재 로그인한 Admin Node의 Single Sign-On 페이지에서 SAML 메타데이터를 다운로드하고 저장할 버튼을 선택합니다.
2. 그리드에서 다른 관리 노드에 대해 다음 단계를 반복합니다.
 - a. 노드에 로그인합니다.
 - b. 구성 * > * 액세스 제어 * > * 단일 사인온 * 을 선택합니다.
 - c. 해당 노드에 대한 SAML 메타데이터를 다운로드하고 저장합니다.
3. Azure Portal로 이동합니다.
4. 의 단계를 따릅니다 ["Azure AD에서 엔터프라이즈 애플리케이션을 생성합니다"](#) 각 관리 노드에 대한 SAML 메타데이터 파일을 해당 Azure 엔터프라이즈 애플리케이션에 업로드합니다.

PingFederate(PingFederate)

단계

1. 현재 로그인한 Admin Node의 Single Sign-On 페이지에서 SAML 메타데이터를 다운로드하고 저장할 버튼을 선택합니다.
2. 그리드에서 다른 관리 노드에 대해 다음 단계를 반복합니다.
 - a. 노드에 로그인합니다.
 - b. 구성 * > * 액세스 제어 * > * 단일 사인온 * 을 선택합니다.
 - c. 해당 노드에 대한 SAML 메타데이터를 다운로드하고 저장합니다.
3. PingFederate로 이동합니다.
4. ["StorageGRID에 대한 SP\(서비스 공급자\) 연결을 하나 이상 생성합니다"](#). 각 관리 노드에 대해 SP 연결 ID(StorageGRID 단일 사인온 페이지의 표에 표시됨)와 해당 관리 노드에 대해 다운로드한 SAML 메타데이터를 사용합니다.

표에 표시된 각 관리 노드에 대해 하나의 SP 접속을 생성해야 합니다.

SSO 연결을 테스트합니다

전체 StorageGRID 시스템에 대해 SSO(Single Sign-On)를 사용하기 전에 각 관리 노드에 대해 SSO(Single Sign-On)와 단일 로그아웃이 올바르게 구성되어 있는지 확인해야 합니다.

Active Directory를 클릭합니다

단계

1. StorageGRID 단일 사인온 페이지의 Sandbox 모드 메시지에서 링크를 찾습니다.

URL은 * 페더레이션 서비스 이름 * 필드에 입력한 값에서 파생됩니다.

Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
2. Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm>
3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

2. ID 공급자의 로그인 페이지에 액세스하려면 링크를 선택하거나 URL을 복사하여 브라우저에 붙여 넣으십시오.
3. 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 선택합니다.

You are not signed in.

Sign in to this site.

Sign in to one of the following sites:

SG-DC1-ADM1

4. 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.
5. 이 단계를 반복하여 그리드의 각 관리 노드에 대한 SSO 연결을 확인합니다.

Azure를 지원합니다

단계

1. Azure 포털의 Single Sign-On 페이지로 이동합니다.
2. 이 응용 프로그램 테스트 * 를 선택합니다.
3. 통합 사용자의 자격 증명을 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.
4. 이 단계를 반복하여 그리드의 각 관리 노드에 대한 SSO 연결을 확인합니다.

PingFederate(PingFederate)

단계

1. StorageGRID 단일 사인온 페이지에서 Sandbox 모드 메시지의 첫 번째 링크를 선택합니다.

링크를 한 번에 하나씩 선택하여 테스트합니다.

Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure service provider (SP) connections and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Ping Federate to create SP connections for StorageGRID. Create one SP connection for each Admin Node, using the relying party identifier(s) shown below.
2. Test SSO and SLO by selecting the link for each Admin Node:
 - [https://\[redacted\]/idp/startSSO.ping?PartnerSpld=SG-DC1-ADM1-106-69](https://[redacted]/idp/startSSO.ping?PartnerSpld=SG-DC1-ADM1-106-69)
 - [https://\[redacted\]/idp/startSSO.ping?PartnerSpld=SG-DC2-ADM1-106-73](https://[redacted]/idp/startSSO.ping?PartnerSpld=SG-DC2-ADM1-106-73)
3. StorageGRID displays a success or error message for each test.

When you have confirmed SSO for each SP connection and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and select **Save**.

2. 통합 사용자의 자격 증명을 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.
3. 다음 링크를 선택하여 그리드의 각 관리 노드에 대한 SSO 연결을 확인합니다.

페이지 만료 메시지가 표시되면 브라우저에서 * 뒤로 * 버튼을 선택하고 자격 증명을 다시 제출하십시오.

SSO(Single Sign-On)를 활성화합니다

SSO를 사용하여 각 관리 노드에 로그인할 수 있는지 확인한 후 전체 StorageGRID 시스템에 대해 SSO를 활성화할 수 있습니다.



SSO가 활성화된 경우 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.

단계

1. 구성 * > * 액세스 제어 * > * 단일 사인온 * 을 선택합니다.
2. SSO 상태를 * Enabled * 로 변경합니다.
3. 저장 * 을 선택합니다.
4. 경고 메시지를 검토하고 * OK * 를 선택합니다.

이제 SSO(Single Sign-On)가 활성화됩니다.



Azure 포털을 사용 중이고 Azure에 액세스하는 데 사용하는 컴퓨터에서 StorageGRID에 액세스하는 경우 Azure Portal 사용자가 승인된 StorageGRID 사용자인지 확인합니다(StorageGRID로 가져온 통합 그룹의 사용자). 또는 StorageGRID에 로그인하기 전에 Azure 포털에서 로그아웃합니다.

AD FS에서 기반 당사자 트러스트를 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.

시작하기 전에

- StorageGRID에 대해 Single Sign-On을 구성하고 SSO 유형으로 * AD FS * 를 선택했습니다.
- * Sandbox 모드 * 는 Grid Manager의 Single Sign-On 페이지에서 선택됩니다. 을 참조하십시오 "[sandbox 모드를 사용합니다](#)".
- 시스템의 각 관리 노드에 대한 정규화된 도메인 이름(또는 IP 주소)과 관련 당사자 식별자를 알고 있습니다. 이러한 값은 StorageGRID 단일 사인온 페이지의 관리 노드 세부 정보 테이블에서 찾을 수 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.
- 수동으로 신뢰할 수 있는 상대 신뢰를 만드는 경우 StorageGRID 관리 인터페이스에 대해 업로드된 사용자 지정 인증서가 있거나 명령 셸에서 관리 노드에 로그인하는 방법을 알고 있어야 합니다.

이 작업에 대해

이 지침은 Windows Server 2016 AD FS에 적용됩니다. 다른 버전의 AD FS를 사용하는 경우 절차에 약간의 차이가 있을 수 있습니다. 질문이 있는 경우 Microsoft AD FS 설명서를 참조하십시오.

Windows PowerShell을 사용하여 신뢰할 수 있는 사용자 신뢰를 만듭니다

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

단계

1. Windows 시작 메뉴에서 PowerShell 아이콘을 마우스 오른쪽 버튼으로 선택하고 * 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_Identifer``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. Apply * 를 선택하고 * OK * 를 선택합니다

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

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. 작업을 마치면 StorageGRID로 돌아가 모든 신뢰할 수 있는 상대 트러스트를 테스트하여 올바르게 구성되었는지 확인합니다. 을 참조하십시오 **"Sandbox 모드를 사용합니다"** 를 참조하십시오.

페더레이션 메타데이터를 가져와 사용 상대 신뢰를 만듭니다

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

단계

1. Windows Server Manager에서 * Tools * 를 선택한 다음 * AD FS Management * 를 선택합니다.

2. 작업에서 * 신뢰할 수 있는 당사자 신뢰 추가 * 를 선택합니다.

3. 시작 페이지에서 * 클레임 인식 * 을 선택하고 * 시작 * 을 선택합니다.

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 * 선택:

c. 규칙 템플릿 선택 페이지의 목록에서 * 청구로 LDAP 속성 보내기 * 를 선택하고 * 다음 * 을 선택합니다.

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 선택하고 * 확인 * 을 선택합니다.
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. 작업을 마치면 StorageGRID로 돌아가 모든 신뢰할 수 있는 상대 트러스트를 테스트하여 올바르게 구성되었는지 확인합니다. 을 참조하십시오 "[Sandbox 모드를 사용합니다](#)" 를 참조하십시오.

수동으로 신뢰할 수 있는 상대 신뢰를 만듭니다

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

단계

1. Windows Server Manager에서 * Tools * 를 선택한 다음 * AD FS Management * 를 선택합니다.
2. 작업에서 * 신뢰할 수 있는 당사자 신뢰 추가 * 를 선택합니다.
3. 시작 페이지에서 * 클레임 인식 * 을 선택하고 * 시작 * 을 선택합니다.
4. [의지하는 자에 대한 데이터 입력]을 선택하고 * [다음]을 선택합니다.
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 건너뛵니다.
- 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 선택합니다.

a. 규칙 템플릿 선택 페이지의 목록에서 *청구로 LDAP 속성 보내기* 를 선택하고 *다음* 을 선택합니다.

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 선택하고 *확인* 을 선택합니다.

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 선택합니다.

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. OK* 를 선택합니다.

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. Apply* 를 선택하고 * OK* 를 선택합니다.

종속된 당사자 속성이 저장되고 닫힙니다.

10. 이 단계를 반복하여 StorageGRID 시스템의 모든 관리 노드에 대한 신뢰할 수 있는 상대 트러스트를 구성합니다.
11. 작업을 마치면 StorageGRID로 돌아가 모든 신뢰할 수 있는 상대 트러스트를 테스트하여 올바르게 구성되었는지 확인합니다. 을 참조하십시오 ["sandbox 모드를 사용합니다"](#) 를 참조하십시오.

Azure AD에서 엔터프라이즈 애플리케이션을 생성합니다

Azure AD를 사용하여 시스템의 각 관리 노드에 대한 엔터프라이즈 애플리케이션을 생성합니다.

시작하기 전에

- StorageGRID에 대한 SSO(Single Sign-On) 구성을 시작했으며 SSO 유형으로 * Azure * 를 선택했습니다.
- * Sandbox 모드 * 는 Grid Manager의 Single Sign-On 페이지에서 선택됩니다. 을 참조하십시오 ["sandbox 모드를 사용합니다"](#).
- 시스템의 각 관리 노드에 대해 * 엔터프라이즈 애플리케이션 이름 * 이 있습니다. 이러한 값은 StorageGRID 단일 사인온 페이지의 관리 노드 세부 정보 테이블에서 복사할 수 있습니다.



StorageGRID 시스템의 각 관리 노드에 대해 엔터프라이즈 애플리케이션을 만들어야 합니다. 각 관리 노드에 엔터프라이즈 애플리케이션을 사용하면 사용자가 관리자 노드에 안전하게 로그인할 수 있습니다.

- Azure Active Directory에서 엔터프라이즈 응용 프로그램을 만든 경험이 있습니다.
- Azure 계정에 활성 구독이 있습니다.
- Azure 계정에는 글로벌 관리자, 클라우드 응용 프로그램 관리자, 응용 프로그램 관리자 또는 서비스 보안 주체의 소유자인 다음 역할 중 하나가 있습니다.

Azure AD에 액세스합니다

단계

1. 에 로그인합니다 ["Azure 포털"](#).
2. 로 이동합니다 ["Azure Active Directory를 클릭합니다"](#).
3. 를 선택합니다 ["엔터프라이즈 애플리케이션"](#).

엔터프라이즈 애플리케이션을 생성하고 **StorageGRID SSO** 구성을 저장합니다

StorageGRID에서 Azure에 대한 SSO 구성을 저장하려면 Azure를 사용하여 각 관리 노드에 대한 엔터프라이즈 애플리케이션을 만들어야 합니다. Azure에서 페더레이션 메타데이터 URL을 복사하여 StorageGRID 단일 사인온 페이지의 해당 * 페더레이션 메타데이터 URL * 필드에 붙여 넣습니다.

단계

1. 각 관리 노드에 대해 다음 단계를 반복합니다.
 - a. Azure Enterprise 응용 프로그램 창에서 * 새 응용 프로그램 * 을 선택합니다.
 - b. 사용자 정의 응용 프로그램 만들기 * 를 선택합니다.
 - c. 이름으로 StorageGRID 단일 사인온 페이지의 관리 노드 세부 정보 테이블에서 복사한 * 엔터프라이즈 응용 프로그램 이름 * 을 입력합니다.
 - d. 갤러리에서 찾을 수 없는 * 다른 응용 프로그램 통합(갤러리 외) * 라디오 버튼을 선택된 상태로 둡니다.

- e. Create * 를 선택합니다.
 - f. 2에서 * 시작하기 * 링크를 선택합니다. Single Sign On * 상자를 설정하거나 왼쪽 여백에서 * Single Sign-On * 링크를 선택합니다.
 - g. SAML * 상자를 선택합니다.
 - h. 앱 페더레이션 메타데이터 URL * 을 복사합니다. * 3단계 SAML 서명 인증서 * 에서 찾을 수 있습니다.
 - i. StorageGRID 단일 사인온 페이지로 이동하여 사용한 * 엔터프라이즈 응용 프로그램 이름 * 에 해당하는 * 통합 메타데이터 URL * 필드에 URL을 붙여 넣습니다.
2. 각 관리 노드에 대한 페더레이션 메타데이터 URL을 붙여 넣고 SSO 구성에 필요한 다른 모든 변경 사항을 적용한 후 StorageGRID 단일 사인온 페이지에서 * 저장 * 을 선택합니다.

모든 관리 노드에 대해 **SAML** 메타데이터를 다운로드합니다

SSO 구성을 저장한 후 StorageGRID 시스템의 각 관리 노드에 대해 SAML 메타데이터 파일을 다운로드할 수 있습니다.

단계

1. 각 관리 노드에 대해 이 단계를 반복합니다.
 - a. 관리자 노드에서 StorageGRID에 로그인합니다.
 - b. 구성 * > * 액세스 제어 * > * 단일 사인온 * 을 선택합니다.
 - c. 버튼을 선택하여 해당 Admin Node에 대한 SAML 메타데이터를 다운로드합니다.
 - d. Azure AD에 업로드할 파일을 저장합니다.

각 엔터프라이즈 애플리케이션에 **SAML** 메타데이터를 업로드합니다

각 StorageGRID 관리 노드에 대해 SAML 메타데이터 파일을 다운로드한 후 Azure AD에서 다음 단계를 수행하십시오.

단계

1. Azure 포털로 돌아갑니다.
2. 각 엔터프라이즈 애플리케이션에 대해 다음 단계를 반복합니다.



이전에 목록에 추가한 응용 프로그램을 보려면 엔터프라이즈 응용 프로그램 페이지를 새로 고쳐야 할 수 있습니다.

- a. 엔터프라이즈 애플리케이션의 속성 페이지로 이동합니다.
 - b. 할당 필요 * 를 * 아니오 * 로 설정합니다(할당을 별도로 구성하지 않는 경우).
 - c. Single Sign-On 페이지로 이동합니다.
 - d. SAML 구성을 완료합니다.
 - e. Upload metadata file * 버튼을 선택하고 해당 Admin Node에 대해 다운로드한 SAML 메타데이터 파일을 선택합니다.
 - f. 파일을 로드한 후 * Save * 를 선택하고 * X * 를 선택하여 창을 닫습니다. SAML로 단일 사인온 설정 페이지로 돌아갑니다.
3. 의 단계를 따릅니다 "**sandbox 모드를 사용합니다**" 각 응용 프로그램을 테스트합니다.

PingFederate에서 서비스 공급자(SP) 연결을 생성합니다

PingFederate를 사용하여 시스템의 각 관리 노드에 대한 서비스 공급자(SP) 연결을 만듭니다. 프로세스 속도를 높이기 위해 StorageGRID에서 SAML 메타데이터를 가져옵니다.

시작하기 전에

- StorageGRID에 대한 SSO(Single Sign-On)를 구성하고 SSO 유형으로 * Ping 남부연합을 선택했습니다.
- * Sandbox 모드 * 는 Grid Manager의 Single Sign-On 페이지에서 선택됩니다. 을 참조하십시오 "[sandbox 모드를 사용합니다](#)".
- 시스템의 각 관리 노드에 대해 * SP 접속 ID * 가 있습니다. 이러한 값은 StorageGRID 단일 사인온 페이지의 관리 노드 세부 정보 테이블에서 찾을 수 있습니다.
- 시스템의 각 관리 노드에 대해 * SAML 메타데이터 * 를 다운로드했습니다.
- PingFederate Server에서 SP 연결을 생성하는 경험이 있습니다.
- 을(를) 보유하고 있습니다<https://docs.pingidentity.com/bundle/pingfederate-103/page/kfj1564002962494.html>["관리자 참조 안내서"] PingFederate Server의 경우 PingFederate 설명서는 자세한 단계별 지침과 설명을 제공합니다.
- PingFederate Server에 대한 관리자 권한이 있습니다.

이 작업에 대해

이 지침은 PingFederate Server 버전 10.3을 StorageGRID의 SSO 공급자로 구성하는 방법을 요약합니다. 다른 버전의 PingFederate를 사용하는 경우 이 지침을 조정해야 할 수 있습니다. 릴리스에 대한 자세한 지침은 PingFederate Server 설명서를 참조하십시오.

PingFederate에서 필수 구성 요소를 완료합니다

StorageGRID에 사용할 SP 연결을 생성하려면 PingFederate에서 사전 요구 작업을 완료해야 합니다. SP 접속을 구성할 때 이러한 사전 요구 사항의 정보를 사용합니다.

데이터 저장소 생성

아직 연결하지 않은 경우 데이터 저장소를 생성하여 PingFederate를 AD FS LDAP 서버에 연결합니다. 사용 시 사용한 값을 사용합니다 "[ID 페더레이션을 구성하는 중입니다](#)" StorageGRID에서

- * 유형 *: 디렉토리(LDAP)
- * LDAP 유형 *: Active Directory
- * 바이너리 특성 이름 *: LDAP 바이너리 특성 탭의 * objectGUID * 를 그림과 같이 정확하게 입력합니다.

암호 자격 증명 유효성 검사기 **[[암호 유효성 검사기]]** 만들기

아직 설치하지 않은 경우 암호 자격 증명 유효성 검사기를 만듭니다.

- * 유형 *: LDAP 사용자 이름 암호 자격 증명 검사기
- * 데이터 저장소 *: 만든 데이터 저장소를 선택합니다.
- * 검색 기준 *: LDAP의 정보를 입력합니다(예: DC=SAML, DC=SGWs).
- * 검색 필터 *: sAMAccountName=\${username}

- * 범위 *: 하위 트리

IDP 어댑터 인스턴스 만들기

아직 IDP 어댑터 인스턴스를 만들지 않은 경우 생성합니다.

단계

1. 인증 * > * 통합 * > * IDP 어댑터 * 로 이동합니다.
2. 새 인스턴스 만들기 * 를 선택합니다.
3. 유형 탭에서 * HTML 양식 IDP 어댑터 * 를 선택합니다.
4. IDP Adapter 탭에서 * Add a new row to 'Credential Validators' * 를 선택합니다.
5. 를 선택합니다 [암호 자격 증명 유효성 검사기가 있습니다](#) 을(를) 만들었습니다.
6. 어댑터 특성 탭에서 * 가명 * 에 대한 * 사용자 이름 * 속성을 선택합니다.
7. 저장 * 을 선택합니다.

서명 인증서 만들기 또는 가져오기

서명 인증서를 아직 만들지 않은 경우 서명 인증서를 만들거나 가져옵니다.

단계

1. 보안 * > * 서명 및 암호 해독 키 및 인증서 * 로 이동합니다.
2. 서명 인증서를 만들거나 가져옵니다.

PingFederate에서 SP 접속을 생성합니다

PingFederate에서 SP 연결을 생성할 때 StorageGRID에서 다운로드한 SAML 메타데이터를 관리자 노드에 대해 가져옵니다. 메타데이터 파일에는 필요한 많은 특정 값이 들어 있습니다.



사용자가 모든 노드에 안전하게 로그인할 수 있도록 StorageGRID 시스템의 각 관리 노드에 대해 SP 접속을 생성해야 합니다. 이 지침에 따라 첫 번째 SP 접속을 생성합니다. 그런 다음 로 이동합니다 [추가 SP 접속을 생성합니다](#) 필요한 추가 연결을 생성합니다.

SP 접속 유형을 선택합니다

단계

1. 응용 프로그램 * > * 통합 * > * SP 연결 * 으로 이동합니다.
2. Create Connection * 을 선택합니다.
3. 이 연결에 템플릿을 사용하지 않음 * 을 선택합니다.
4. 프로토콜로 * Browser SSO Profiles * 및 * SAML 2.0 * 을 선택합니다.

SP 메타데이터를 가져옵니다

단계

1. 메타데이터 가져오기 탭에서 * 파일 * 을 선택합니다.
2. 관리자 노드의 StorageGRID Single Sign-On 페이지에서 다운로드한 SAML 메타데이터 파일을 선택합니다.

3. 메타데이터 요약 및 일반 정보 탭에 제공된 정보를 검토합니다.

파트너의 엔티티 ID와 연결 이름은 StorageGRID SP 연결 ID로 설정됩니다. (예: 10.96.105.200-DC1-ADM1-105-200). 기본 URL은 StorageGRID 관리 노드의 IP입니다.

4. 다음 * 을 선택합니다.

IDP 브라우저 SSO를 구성합니다

단계

1. Browser SSO(브라우저 SSO) 탭에서 * Configure Browser SSO *(브라우저 SSO * 구성) 를 선택합니다.
2. SAML 프로필 탭에서 * SP 시작 SSO *, * SP 초기 SLO *, * IDP 시작 SSO * 및 * IDP 시작 SLO * 옵션을 선택합니다.
3. 다음 * 을 선택합니다.
4. 어설션 수명 탭에서 변경하지 않습니다.
5. 어설션 작성 탭에서 * 어설션 작성 설정 * 을 선택합니다.
 - a. ID 매핑 탭에서 * 표준 * 을 선택합니다.
 - b. [속성 계약] 탭에서 [속성 계약] 및 가져온 지정되지 않은 이름 형식으로 * SAML_subject * 를 사용합니다.
6. 계약 연장 에서 * 삭제 * 를 선택하여 를 제거합니다 urn:oid, 사용되지 않습니다.

어댑터 인스턴스를 매핑합니다

단계

1. 인증 소스 매핑 탭에서 * 새 어댑터 인스턴스 매핑 * 을 선택합니다.
2. 어댑터 인스턴스 탭에서 를 선택합니다 어댑터 인스턴스 을(를) 만들었습니다.
3. 매핑 방법 탭에서 * 데이터 저장소에서 추가 특성 검색 * 을 선택합니다.
4. 특성 원본 및 사용자 조회 탭에서 * 특성 원본 추가 * 를 선택합니다.
5. Data Store(데이터 저장소) 탭에서 설명을 입력하고 를 선택합니다 데이터 저장소 을(를) 추가했습니다.
6. LDAP 디렉토리 검색 탭에서 다음을 수행합니다.
 - 기본 DN * 을 입력합니다. 이 값은 LDAP 서버에 대해 StorageGRID에 입력한 값과 정확히 일치해야 합니다.
 - 검색 범위 에서 * 하위 트리 * 를 선택합니다.
 - 루트 개체 클래스의 경우 * objectGUID * 특성을 검색하여 추가합니다.
7. LDAP 바이너리 특성 인코딩 형식 탭에서 * objectGUID * 특성에 대해 * Base64 * 를 선택합니다.
8. LDAP 필터 탭에서 * sAMAccountName=\${username} * 을 입력합니다.
9. [속성 계약 이행] 탭의 [소스] 드롭다운에서 * LDAP(속성) * 를 선택하고 값 드롭다운에서 * objectGUID * 를 선택합니다.
10. 특성 소스를 검토한 후 저장합니다.
11. Failsave 특성 소스 탭에서 * SSO 트랜잭션 중단 * 을 선택합니다.
12. 요약 검토하고 * 완료 * 를 선택합니다.
13. 완료 * 를 선택합니다.

프로토콜 설정을 구성합니다

단계

1. SP Connection * > * Browser SSO * > * Protocol Settings * 탭에서 * Configure Protocol Settings * 를 선택합니다.
2. Assertion Consumer Service URL 탭에서 StorageGRID SAML 메타데이터(* 바인딩 및 의 경우 POST*)에서 가져온 기본값을 그대로 사용합니다 /api/saml-response 엔드포인트 URL).
3. SLO 서비스 URL 탭에서 StorageGRID SAML 메타데이터에서 가져온 기본값을 그대로 사용합니다(바인딩 및 의 경우 * redirect *) /api/saml-logout 엔드포인트 URL의 경우.
4. 허용 가능한 SAML 바인딩 탭에서 * Artifact * 및 * SOAP * 를 지웁니다. POST * 및 * REDIRECT * 만 필요합니다.
5. 서명 정책 탭에서 * Authn 요청 서명 필요 * 및 * 항상 설정 서명 * 확인란을 선택된 상태로 둡니다.
6. 암호화 정책 탭에서 * 없음 * 을 선택합니다.
7. 요약을 검토하고 * Done * (완료 *)을 선택하여 프로토콜 설정을 저장합니다.
8. 요약을 검토하고 * 완료 * 를 선택하여 브라우저 SSO 설정을 저장합니다.

자격 증명을 구성합니다

단계

1. SP 연결 탭에서 * 자격 증명 * 을 선택합니다.
2. 자격 증명 탭에서 * 자격 증명 구성 * 을 선택합니다.
3. 를 선택합니다 **서명 인증서** 만들거나 가져왔습니다.
4. 다음 * 을 선택하여 * 서명 확인 설정 관리 * 로 이동합니다.
 - a. 보안 모델 탭에서 * 앵커 지정되지 않음 * 을 선택합니다.
 - b. 서명 확인 인증서 탭에서 StorageGRID SAML 메타데이터에서 가져온 서명 인증서 정보를 검토합니다.
5. 요약 화면을 검토하고 * 저장 * 을 선택하여 SP 접속을 저장합니다.

추가 SP 접속을 생성합니다

첫 번째 SP 접속을 복제하여 그리드의 각 관리 노드에 필요한 SP 접속을 생성할 수 있습니다. 각 복사본에 대한 새 메타데이터를 업로드합니다.



파트너의 엔티티 ID, 기본 URL, 연결 ID, 연결 이름, 서명 확인을 제외하고 서로 다른 관리 노드의 SP 연결은 동일한 설정을 사용합니다. SLO 응답 URL이 있습니다.

단계

1. 각 추가 관리 노드에 대한 초기 SP 연결의 복제본을 생성하려면 * Action * > * Copy * 를 선택합니다.
2. 복사본의 연결 ID와 연결 이름을 입력하고 * 저장 * 을 선택합니다.
3. 관리 노드에 해당하는 메타데이터 파일을 선택합니다.
 - a. 작업 * > * 메타데이터 업데이트 * 를 선택합니다.
 - b. 파일 선택 * 을 선택하고 메타데이터를 업로드합니다.

- c. 다음 * 을 선택합니다.
 - d. 저장 * 을 선택합니다.
4. 미사용 속성으로 인한 오류를 해결합니다.
- a. 새 연결을 선택합니다.
 - b. Configure Browser SSO > Configure Assertion Creation > Attribute Contract * 를 선택합니다.
 - c. urn:OID*에 대한 항목을 삭제합니다.
 - d. 저장 * 을 선택합니다.

SSO(Single Sign-On)를 비활성화합니다

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.

시작하기 전에

- 를 사용하여 그리드 관리자에 로그인했습니다 "[지원되는 웹 브라우저](#)".
- 특정 액세스 권한이 있습니다.

단계

1. 구성 * > * 액세스 제어 * > * 단일 사인온 * 을 선택합니다.

단일 사인온 페이지가 나타납니다.

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

로컬 사용자가 로그인할 수 있음을 나타내는 경고 메시지가 나타납니다.

4. OK * 를 선택합니다.

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.

시작하기 전에

- 특정 액세스 권한이 있습니다.
- 을(를) 보유하고 있습니다 Passwords.txt 파일.
- 로컬 루트 사용자의 암호를 알고 있습니다.

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 * 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. 구성 `>` `>` * 액세스 제어 * `>` * 단일 사인온 * 을 선택합니다.
- b. 잘못된 또는 오래된 SSO 설정을 변경합니다.
- c. 저장 * 을 선택합니다.

단일 사인온 페이지에서 * 저장 * 을 선택하면 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 선택하고 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.

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.