Single Sign-On 구성

StorageGRID 11.5

NetApp
April 11, 2024

목차

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"

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.

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.

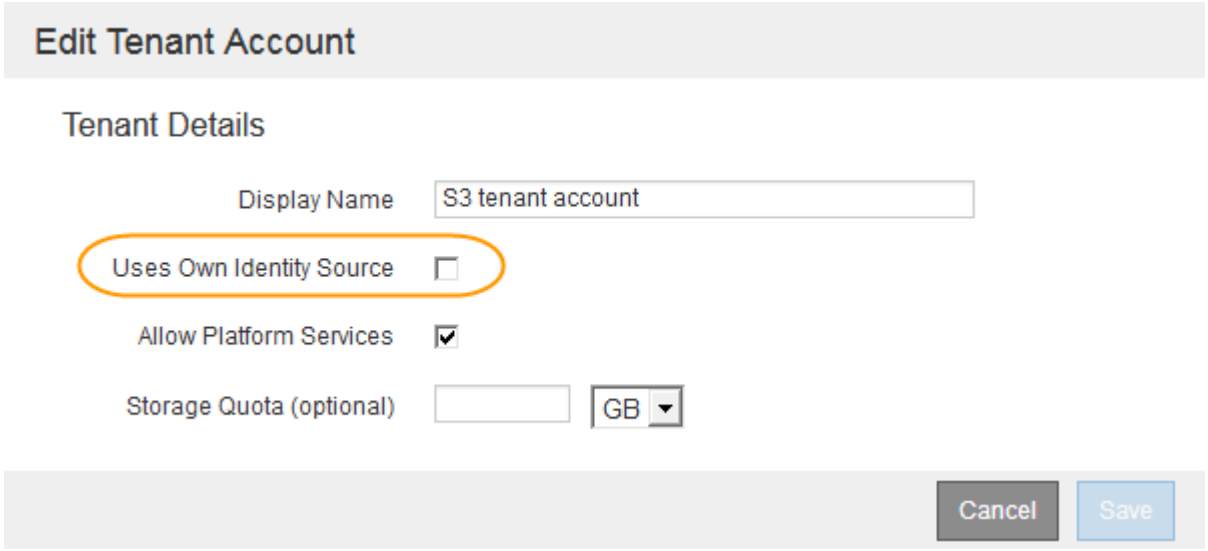
d. 통합 그룹의 사용자로 그리드 관리자에 다시 로그인할 수 있는지 확인합니다.

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.

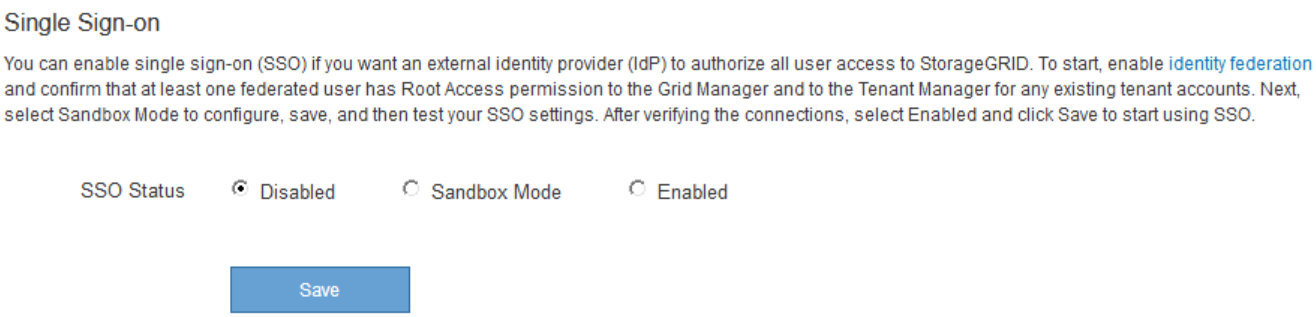
sandbox 모드를 사용하면 SSO를 활성화하기 전에 이 전면과 후면을 간편하게 구성하고 모든 설정을 테스트할 수 있습니다.

> 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`.

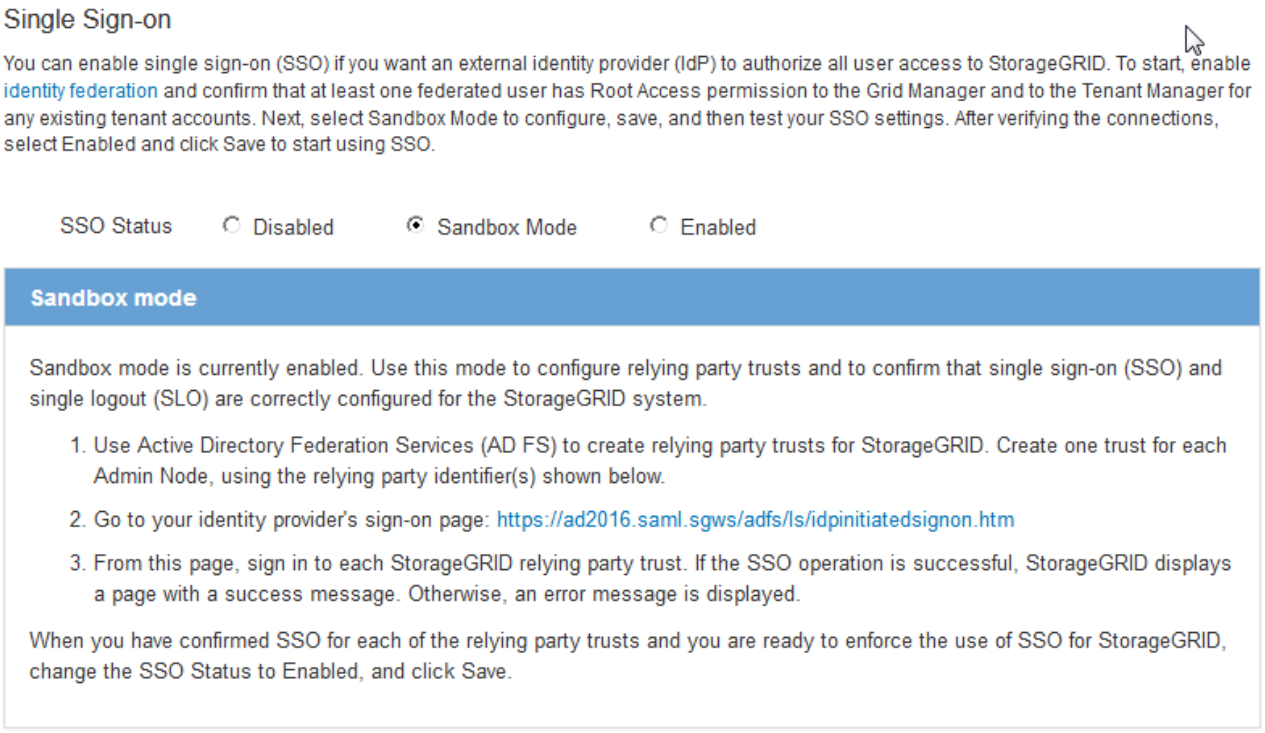
   ◦ 그리드에 둘 이상의 관리 노드가 포함된 경우 문자열을 포함합니다 `[HOSTNAME]` 를 입력합니다. 예를 들면, 다음과 같습니다. `SG-[HOSTNAME]`. 이렇게 하면 노드의 호스트 이름을 기반으로 각 관리 노드에 대한 기반 당사자 식별자가 포함된 테이블이 생성됩니다. +참고: StorageGRID 시스템의 각 관리 노드에 대한 신뢰할 수 있는 상대 신뢰를 만들어야 합니다. 각 관리 노드에 대한 신뢰할 수 있는 당사자 덕분에 사용자는 모든 관리 노드에 안전하게 로그인할 수 있습니다.

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.

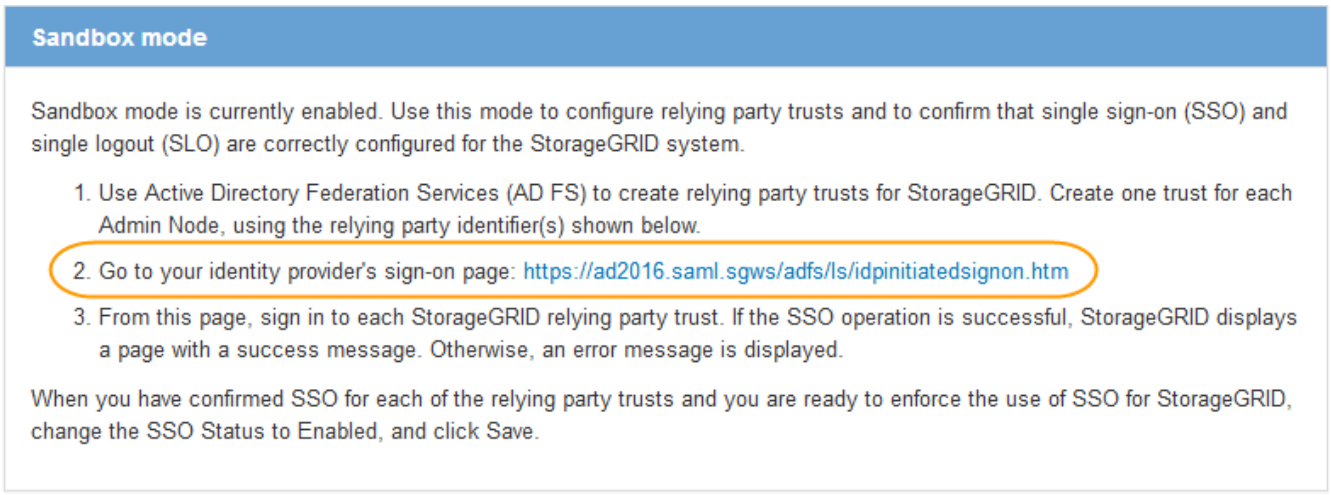
단계

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

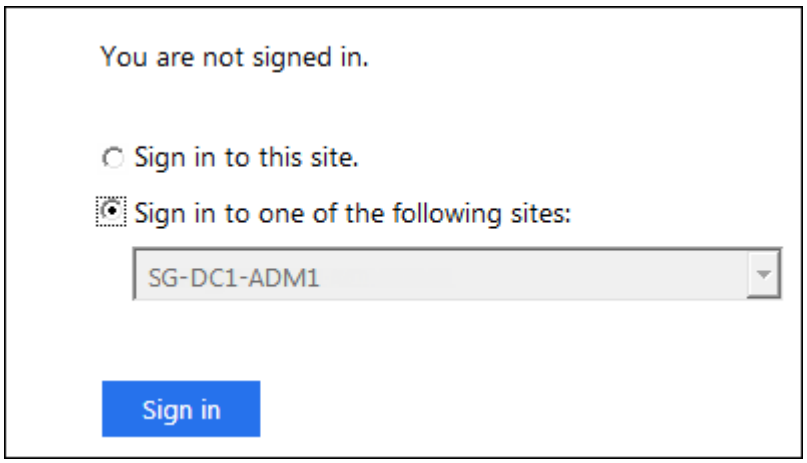
   단일 사인온 페이지가 나타나고 * Sandbox 모드 * 옵션이 선택됩니다.

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

   URL은 * Federated Service Name * 필드에 입력한 값에서 파생됩니다.

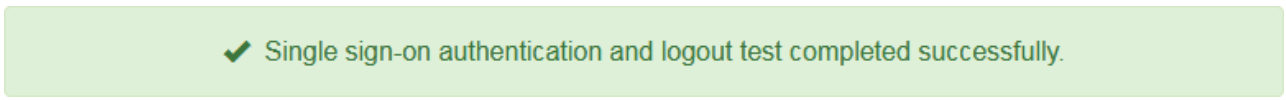


3. ID 공급자의 로그인 페이지에 액세스하려면 링크를 클릭하거나 URL을 복사하여 브라우저에 붙여 넣으십시오.
4. SSO를 사용하여 StorageGRID에 로그인할 수 있는지 확인하려면 * 다음 사이트 중 하나에 로그인 * 을 선택하고 기본 관리자 노드에 대한 보조 당사자 식별자를 선택한 다음 * 로그인 * 을 클릭합니다.



   사용자 이름과 암호를 입력하라는 메시지가 표시됩니다.

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



   - 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.

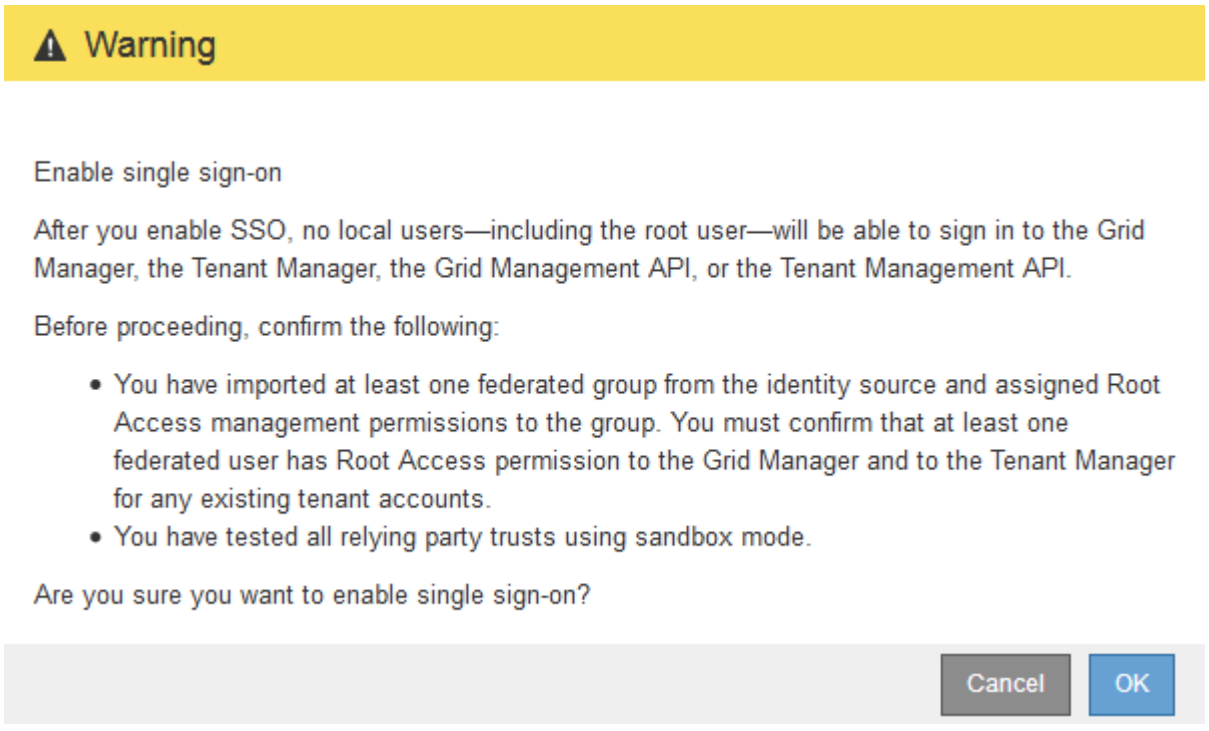
단계

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.

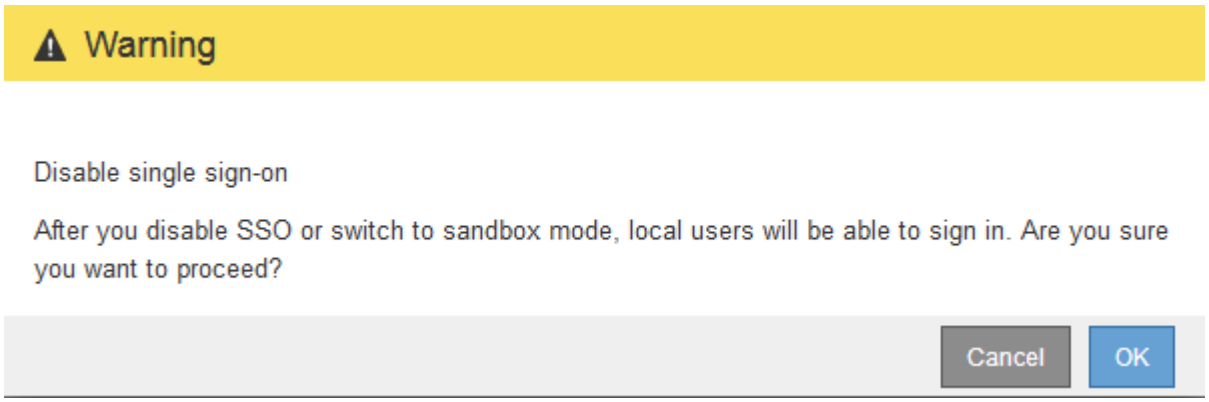
단계

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"