싱글 사인온(SSO) 사용

StorageGRID software

NetApp
July 23, 2026

목차

싱글 사인온(SSO) 사용

StorageGRID SSO에 대해 알아보십시오

싱글 사인온(SSO)이 활성화된 경우, 사용자는 조직에서 구현한 SSO 로그인 프로세스를 통해 자격 증명이 인증된 경우에만 Grid Manager, Tenant Manager, Grid Management API 또는 Tenant Management API에 액세스할 수 있습니다. 로컬 사용자는 StorageGRID에 로그인할 수 없습니다.

StorageGRID 시스템은 SAML 2.0(Security Assertion Markup Language 2.0) 표준을 사용한 단일 로그인(SSO)을 지원합니다.

SSO(Single Sign-On)를 활성화하기 전에 SSO가 활성화될 때 StorageGRID 로그인 및 로그아웃 프로세스에 어떤 영향을 미치는지 검토하십시오.

SSO가 활성화된 경우 로그인

SSO가 활성화된 상태에서 StorageGRID에 로그인하면 자격 증명을 확인하기 위해 조직의 SSO 페이지로 리디렉션됩니다.

단계

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

   StorageGRID 로그인 페이지가 나타납니다.

   - 이 브라우저에서 해당 URL에 처음 접속하는 경우 계정 ID를 입력하라는 메시지가 표시됩니다.
   - 이전에 그리드 관리자 또는 테넌트 관리자에 접속한 적이 있는 경우, 최근 계정을 선택하거나 계정 ID를 입력하라는 메시지가 표시됩니다.

   > StorageGRID 테넌트 계정의 전체 URL(즉, 정규화된 도메인 이름 또는 IP 주소 뒤에 `/?accountId=20-digit-account-id`)을 입력하면 StorageGRID 로그인 페이지가 표시되지 않습니다. 대신 조직의 SSO 로그인 페이지로 바로 리디렉션되며, 여기서 SSO 자격 증명으로 로그인하십시오할 수 있습니다.

2. Grid Manager 또는 테넌트 관리자 중 어느 쪽에 액세스할지 표시합니다.

   - 그리드 관리자에 액세스하려면 계정 **ID** 필드를 비워 두거나 계정 ID로 *0*을 입력하거나 최근 계정 목록에 *그리드 관리자*가 표시되면 해당 항목을 선택하십시오.
   - 테넌트 관리자에 액세스하려면 20자리 테넌트 계정 ID를 입력하거나 최근 계정 목록에 테넌트가 표시되는 경우 이름으로 테넌트를 선택하십시오.

3. *로그인*을 선택합니다

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

4. SSO 자격 증명으로 로그인하십시오.

   SSO 자격 증명이 올바른 경우:

a. ID 공급자(IdP)는 StorageGRID에 인증 응답을 제공합니다.

b. StorageGRID가 인증 응답을 검증합니다.

c. 응답이 유효하고 StorageGRID 액세스 권한이 있는 연합 그룹에 속해 있는 경우, 선택한 계정에 따라 Grid Manager 또는 Tenant Manager에 로그인됩니다.

> 서비스 계정에 액세스할 수 없는 경우에도 StorageGRID 액세스 권한이 있는 페더레이션 그룹에 속한 기존 사용자라면 로그인할 수 있습니다.

5. 적절한 권한이 있는 경우, 다른 관리 노드에 액세스하거나 Grid Manager 또는 Tenant Manager에 액세스할 수 있습니다.

   SSO 자격 증명을 다시 입력할 필요가 없습니다.

SSO가 활성화된 경우 로그아웃

StorageGRID에 SSO가 활성화된 경우, 로그아웃 시 발생하는 상황은 현재 로그인 상태와 로그아웃 위치에 따라 다릅니다.

단계

1. 사용자 인터페이스의 오른쪽 상단 모서리에서 로그아웃 링크를 찾습니다.
2. *로그아웃*을 선택합니다.

   StorageGRID 로그인 페이지가 나타납니다. 최근 계정 드롭다운이 업데이트되어 **Grid Manager** 또는 테넌트의 이름이 포함되므로 향후 이러한 사용자 인터페이스에 더 빠르게 액세스할 수 있습니다.

> 이 표는 단일 브라우저 세션을 사용하는 경우 로그아웃 시 발생하는 상황을 요약한 것입니다. 여러 브라우저 세션에서 StorageGRID에 로그인한 경우, 모든 브라우저 세션에서 개별적으로 로그아웃해야 합니다.

로그인되어 있는 경우...	그리고 로그아웃합니다...	로그아웃되었습니다...
하나 이상의 관리 노드에 있는 Grid Manager	모든 관리 노드의 Grid Manager	모든 관리 노드의 Grid Manager 참고: Entra ID를 SSO에 사용하는 경우 모든 관리자 노드에서 로그아웃하는 데 몇 분 정도 소요될 수 있습니다.
하나 이상의 관리 노드에 있는 테넌트 관리자	모든 관리 노드의 테넌트 관리자	모든 관리 노드의 테넌트 관리자
Grid Manager 및 Tenant Manager 모두	Grid Manager	그리드 관리자만 해당됩니다. SSO에서 로그아웃하려면 테넌트 관리자에서도 로그아웃해야 합니다.

StorageGRID SSO에 대한 요구 사항 및 고려 사항

StorageGRID 시스템에 대한 단일 로그인(SSO)을 활성화하기 전에 요구 사항 및 고려 사항을 검토하십시오.

ID 공급자 요구 사항

StorageGRID는 다음과 같은 SSO ID 공급자(IdP)를 지원합니다.

- Active Directory Federation Service(AD FS)
- Microsoft Entra ID
- PingFederate

SSO ID 공급자를 구성하기 전에 StorageGRID 시스템에 대한 ID 페더레이션을 구성해야 합니다. ID 페더레이션에 사용하는 LDAP 서비스 유형에 따라 구현할 수 있는 SSO 유형이 결정됩니다.

구성된 **LDAP** 서비스 유형	**SSO ID** 공급자 옵션
Active Directory	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

AD FS 요구사항

다음 AD FS 버전 중 하나를 사용할 수 있습니다.

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

> Windows Server 2016은 "KB3201845 업데이트" 또는 그 이상의 버전을 사용해야 합니다.

추가 요구 사항

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

Entra ID 관련 고려 사항

Entra ID를 SSO 유형으로 사용하고 사용자의 사용자 주체 이름이 sAMAccountName을 접두사로 사용하지 않는 경우, StorageGRID가 LDAP 서버와의 연결을 끊으면 로그인 문제가 발생할 수 있습니다. 사용자가 로그인할 수 있도록 하려면 LDAP 서버에 대한 연결을 복원해야 합니다.

서버 인증서 요구 사항

기본적으로 StorageGRID는 각 관리 노드에서 관리 인터페이스 인증서를 사용하여 Grid Manager, Tenant Manager, Grid Management API 및 Tenant Management API에 대한 액세스를 보호합니다. StorageGRID에 대한 신뢰 당사자 트러스트(AD FS), 엔터프라이즈 애플리케이션(Entra ID) 또는 서비스 공급자 연결(PingFederate)을 구성할 때 서버 인증서를 StorageGRID 요청에 대한 서명 인증서로 사용합니다.

아직 설치하지 않으셨다면 "관리 인터페이스에 대한 사용자 지정 인증서를 구성했습니다", 지금 바로 설치하십시오. 사용자 지정 서버 인증서를 설치하면 모든 관리 노드에서 사용되며, 모든 StorageGRID 신뢰 당사자 트러스트, 엔터프라이즈 애플리케이션 또는 SP 연결에서 사용할 수 있습니다.

> ⓘ 관리 노드의 기본 서버 인증서를 신뢰 당사자 트러스트, 엔터프라이즈 애플리케이션 또는 SP 연결에 사용하는 것은 권장되지 않습니다. 노드에 장애가 발생하여 복구하는 경우 새 기본 서버 인증서가 생성됩니다. 복구된 노드에 로그인하려면 먼저 신뢰 당사자 트러스트, 엔터프라이즈 애플리케이션 또는 SP 연결을 새 인증서로 업데이트해야 합니다.

관리자 노드의 서버 인증서는 해당 노드의 명령 셸에 로그인한 다음 `/var/local/mgmt-api` 디렉터리로 이동하면 확인할 수 있습니다. 사용자 지정 서버 인증서의 이름은 `custom-server.crt`입니다. 노드의 기본 서버 인증서의 이름은 `server.crt`입니다.

포트 요구 사항

제한된 Grid Manager 또는 Tenant Manager 포트에서는 싱글 사인온(SSO)을 사용할 수 없습니다. 사용자가 싱글 사인온으로 인증하도록 하려면 기본 HTTPS 포트(443)를 사용해야 합니다. "외부 방화벽에서 액세스 제어"을 참조하십시오.

연합 사용자가 **StorageGRID**에 로그인할 수 있는지 확인합니다

싱글 사인온(SSO)을 활성화하기 전에, 최소 한 명의 페더레이션 사용자가 기존 테넌트 계정에 대해 Grid Manager와 Tenant Manager에 로그인할 수 있는지 확인해야 합니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- "특정 액세스 권한"이(가) 있습니다.
- 이미 ID 페더레이션을 구성했습니다.

단계

1. 기존 테넌트 계정이 있는 경우, 어떤 테넌트도 자체 ID 소스를 사용하고 있지 않은지 확인하십시오.

   > SSO를 활성화하면 테넌트 관리자에 구성된 ID 소스가 그리드 관리자에 구성된 ID 소스로 재정의됩니다. 테넌트의 ID 소스에 속한 사용자는 그리드 관리자 ID 소스에 계정이 없는 경우 더 이상 로그인할 수 없습니다.

   a. 각 테넌트 계정에 대해 Tenant Manager에 로그인하십시오.
   b. 액세스 관리 > *ID 페더레이션*을 선택합니다.
   c. **ID** 페더레이션 사용 확인란이 선택되어 있지 않은지 확인하십시오.
   d. 그렇다면 이 테넌트 계정에 사용 중인 페더레이션 그룹이 더 이상 필요하지 않은지 확인하고 확인란을 선택

해제한 다음 *저장*을 선택하십시오.

2. 페더레이션 사용자가 Grid Manager에 액세스할 수 있는지 확인합니다.
   a. 그리드 관리자에서 구성 > 액세스 제어 > *관리자 그룹*을 선택합니다.
   b. Active Directory ID 소스에서 하나 이상의 페더레이션 그룹을 가져왔고 해당 그룹에 루트 액세스 권한이 할당되었는지 확인하십시오.
   c. 로그아웃합니다.
   d. 연합 그룹의 사용자로 그리드 관리자에 다시 로그인할 수 있는지 확인하십시오.
3. 기존 테넌트 계정이 있는 경우, 루트 액세스 권한이 있는 페더레이션 사용자가 로그인할 수 있는지 확인하십시오.
   a. 그리드 관리자에서 *테넌트*를 선택합니다.
   b. 테넌트 계정을 선택하고 작업 > *편집*을 선택합니다.
   c. 세부 정보 입력 탭에서 *계속*을 선택합니다.
   d. 자체 **ID** 소스 사용 확인란이 선택되어 있으면 선택을 해제하고 *저장*을 선택하십시오.

      테넌트 페이지가 나타납니다.

   e. 테넌트 계정을 선택하고 *로그인*을 선택한 다음 로컬 루트 사용자로 테넌트 계정에 로그인합니다.
   f. 테넌트 관리자에서 액세스 관리 > *그룹*을 선택합니다.
   g. 그리드 관리자의 페더레이션 그룹 중 하나 이상에 이 테넌트에 대한 루트 액세스 권한이 할당되어 있는지 확인합니다.
   h. 로그아웃합니다.
   i. 테넌트 연합 그룹의 사용자로 테넌트에 다시 로그인할 수 있는지 확인하십시오.

관련 정보

- "싱글 사인온(SSO)을 위한 요구 사항 및 고려 사항"
- "관리자 그룹 관리"
- "테넌트 계정 사용"

StorageGRID에서 SSO 구성

SSO 구성 마법사를 따라 샌드박스 모드로 들어가면 모든 StorageGRID 사용자에게 SSO를 활성화하기 전에 SSO를 구성하고 테스트할 수 있습니다. SSO가 활성화된 후에는 필요에 따라 샌드박스 모드로 돌아가 구성을 변경하거나 다시 테스트할 수 있습니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 다음이 있습니다. "루트 액세스 권한"
- StorageGRID 시스템에 대한 ID 페더레이션을 구성했습니다.
- ID 페더레이션 *LDAP 서비스 유형*의 경우, 사용하려는 SSO ID 공급자에 따라 Active Directory 또는 Entra ID를 선택했습니다.

구성된 **LDAP** 서비스 유형	**SSO ID** 공급자 옵션
Active Directory Federation Service(AD FS)	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

이 작업 정보

SSO가 활성화된 상태에서 사용자가 관리자 노드에 로그인하려고 하면 StorageGRID는 SSO ID 공급자에게 인증 요청을 보냅니다. 그러면 SSO ID 공급자는 인증 요청의 성공 여부를 나타내는 인증 응답을 StorageGRID로 다시 보냅니다. 요청이 성공한 경우:

- Active Directory 또는 PingFederate의 응답에는 사용자에 대한 범용 고유 식별자(UUID)가 포함됩니다.
- Entra ID의 응답에는 사용자 주체 이름(UPN)이 포함됩니다.

StorageGRID(서비스 제공업체)와 SSO ID 제공업체가 사용자 인증 요청에 대해 안전하게 통신할 수 있도록 하려면 다음 작업을 완료해야 합니다.

1. StorageGRID에서 설정을 구성합니다.
2. SSO ID 공급자 소프트웨어를 사용하여 각 관리 노드에 대한 신뢰 당사자 트러스트(AD FS), 엔터프라이즈 애플리케이션(Entra ID) 또는 서비스 공급자(PingFederate)를 생성합니다.
3. StorageGRID로 돌아가서 SSO를 활성화합니다.

샌드박스 모드를 사용하면 이러한 설정 변경 과정을 간편하게 수행하고 SSO를 활성화하기 전에 모든 설정을 테스트할 수 있습니다. 샌드박스 모드에서는 사용자가 SSO를 사용하여 로그인할 수 없습니다.

마법사에 액세스합니다

단계

1. * 구성 * > * 액세스 제어 * > * 싱글 사인온 * 을 선택합니다. 싱글 사인온 페이지가 나타납니다.

> SSO 설정 구성 버튼이 비활성화된 경우, ID 공급자를 페더레이션 ID 소스로 구성했는지 확인하십시오. 을(를) 참조하십시오."싱글 사인온(SSO)을 위한 요구 사항 및 고려 사항"

2. *SSO 설정 구성*을 선택합니다. ID 공급자 세부 정보 제공 페이지가 나타납니다.

ID 공급자 세부 정보 제공

단계

1. 드롭다운 목록에서 *SSO 유형*을 선택합니다.
2. SSO 유형으로 Active Directory를 선택한 경우, Active Directory Federation Service(AD FS)에 표시된 대로 ID 공급자의 *페더레이션 서비스 이름*을 정확하게 입력하십시오.

페더레이션 서비스 이름을 찾으려면 Windows Server Manager로 이동합니다. 도구 > *AD FS 관리*를 선택합니다. 작업 메뉴에서 *페더레이션 서비스 속성 편집*을 선택합니다. 페더레이션 서비스 이름은 두 번째 필드에 표시됩니다.

3. ID 공급자가 StorageGRID 요청에 대한 응답으로 SSO 구성 정보를 전송할 때 연결을 보호하는 데 사용할 TLS 인증서를 지정합니다.
   - 운영체제 **CA** 인증서 사용: 운영체제에 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 붙여넣으세요.
   - **TLS**를 사용하지 마십시오: 연결 보안을 위해 TLS 인증서를 사용하지 마십시오.

     CA 인증서를 변경한 경우 즉시 "관리 노드에서 mgmt-api 서비스를 재시작하십시오." Grid Manager에 대한 SSO가 성공적으로 작동하는지 테스트하십시오.
4. *계속*을 선택합니다. 신뢰 당사자 식별자 제공 페이지가 나타납니다.

신뢰 당사자 식별자 제공

1. 선택한 SSO 유형에 따라 '신뢰 당사자 식별자 제공' 페이지의 필드를 작성하십시오.

Active Directory

a. StorageGRID의 *Relying party identifier*를 지정합니다. 이 값은 AD FS에서 각 신뢰 당사자 트러스트에 사용할 이름을 제어합니다.

   - 예를 들어, 그리드에 관리 노드가 하나만 있고 향후 관리 노드를 추가할 계획이 없다면 `SG` 또는 `StorageGRID`를 입력하십시오.
   - 그리드에 관리자 노드가 두 개 이상 포함된 경우 식별자에 문자열 `[HOSTNAME]`을 포함하세요. 예를 들어, `SG-[HOSTNAME]`. 이 문자열을 포함하면 노드의 호스트 이름을 기반으로 그리드의 각 관리자 노드에 대한 신뢰 당사자 식별자를 보여주는 테이블이 생성됩니다.

   StorageGRID 시스템의 각 관리 노드에 대해 신뢰 당사자 트러스트를 생성해야 합니다. 각 관리 노드에 대한 신뢰 당사자 트러스트를 설정하면 사용자가 모든 관리 노드에 안전하게 로그인하고 로그아웃할 수 있습니다.

b. *저장 후 샌드박스 모드로 진입*을 선택합니다.

Entra ID

a. 엔터프라이즈 애플리케이션 섹션에서 StorageGRID의 *엔터프라이즈 애플리케이션 이름*을 지정합니다. 이 값은 Entra ID의 각 엔터프라이즈 애플리케이션에 사용할 이름을 제어합니다.

   - 예를 들어, 그리드에 관리 노드가 하나만 있고 향후 관리 노드를 추가할 계획이 없다면 `SG` 또는 `StorageGRID`를 입력하십시오.
   - 그리드에 관리 노드가 두 개 이상 포함된 경우 식별자에 `[HOSTNAME]` 문자열을 포함하십시오. 예를 들어, `SG-[HOSTNAME]`. 이 문자열을 포함하면 노드의 호스트 이름을 기반으로 시스템의 각 관리 노드에 대한 엔터프라이즈 애플리케이션 이름이 표시되는 표가 생성됩니다.

   StorageGRID 시스템의 각 관리 노드마다 엔터프라이즈 애플리케이션을 생성해야 합니다. 각 관리 노드에 엔터프라이즈 애플리케이션을 설치하면 사용자가 모든 관리 노드에 안전하게 로그인하고 로그아웃할 수 있습니다.

b. "Entra ID에서 엔터프라이즈 애플리케이션 생성"의 단계에 따라 표에 나열된 각 관리 노드에 대한 엔터프라이즈 애플리케이션을 생성하십시오.

c. Entra ID에서 각 엔터프라이즈 애플리케이션의 페더레이션 메타데이터 URL을 복사합니다. 그런 다음 이 URL을 StorageGRID의 해당 페더레이션 메타데이터 **URL** 필드에 붙여넣습니다.

d. 모든 관리 노드에 대한 페더레이션 메타데이터 URL을 복사하여 붙여넣은 후 *저장하고 샌드박스 모드로 진입*을 선택하십시오.

PingFederate

a. 서비스 제공업체(SP) 섹션에서 StorageGRID의 *SP 연결 ID*를 지정합니다. 이 값은 PingFederate에서 각 SP 연결에 사용하는 이름을 제어합니다.

   - 예를 들어, 그리드에 관리 노드가 하나만 있고 향후 관리 노드를 추가할 계획이 없다면 `SG` 또는 `StorageGRID`를 입력하십시오.
   - 그리드에 관리 노드가 두 개 이상 포함된 경우 식별자에 `[HOSTNAME]` 문자열을 포함하십시오. 예를 들어, `SG-[HOSTNAME]`. 이 문자열을 포함하면 노드의 호스트 이름을 기반으로 시스템의 각 관리 노드에 대한 SP 연결 ID를 보여주는 표가 생성됩니다.

StorageGRID 시스템의 각 관리 노드에 대해 SP 연결을 생성해야 합니다. 각 관리 노드에 SP 연결이 있으면 사용자가 모든 관리 노드에 안전하게 로그인하고 로그아웃할 수 있습니다.

b. 연합 메타데이터 **URL** 필드에 각 관리 노드에 대한 연합 메타데이터 URL을 지정하십시오.

   다음 형식을 사용하십시오.

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

c. *저장 후 샌드박스 모드로 진입*을 선택합니다.

신뢰 당사자 트러스트, 엔터프라이즈 애플리케이션 또는 **SP** 연결 구성

구성을 저장하고 샌드박스 모드로 전환하면 선택한 SSO 유형에 대한 구성을 완료하고 테스트할 수 있습니다.

StorageGRID는 필요한 기간 동안 샌드박스 모드를 유지할 수 있습니다. 단, 페더레이션 사용자 및 로컬 사용자만 로그인할 수 있습니다.

Active Directory

단계

1. Active Directory Federation Services(AD FS)로 이동합니다.
2. StorageGRID SSO 구성 페이지의 표에 표시된 각 신뢰 당사자 식별자를 사용하여 StorageGRID에 대한 하나 이상의 신뢰 당사자 트러스트를 생성합니다.

   표에 표시된 각 관리자 노드에 대해 하나의 트러스트를 생성해야 합니다.

   자세한 안내는 "AD FS에서 신뢰 당사자 트러스트 생성"을 참조하십시오.

Entra ID

단계

1. 현재 로그인한 관리자 노드의 싱글 사인온 페이지에서 SAML 메타데이터를 다운로드하고 저장하는 버튼을 선택합니다.
2. 그런 다음 그리드에 있는 다른 모든 관리 노드에 대해 이 단계를 반복하십시오.
   a. 노드에 로그인합니다.
   b. * 구성 * > * 액세스 제어 * > * 싱글 사인온 * 을 선택합니다.
   c. 해당 노드의 SAML 메타데이터를 다운로드하여 저장하십시오.
3. Azure 포털로 이동합니다.
4. "Entra ID에서 엔터프라이즈 애플리케이션 생성"의 단계에 따라 각 관리 노드에 대한 SAML 메타데이터 파일을 해당 Entra ID 엔터프라이즈 애플리케이션에 업로드합니다.

PingFederate

단계

1. 현재 로그인한 관리자 노드의 싱글 사인온 페이지에서 SAML 메타데이터를 다운로드하고 저장하는 버튼을 선택합니다.
2. 그런 다음 그리드에 있는 다른 모든 관리 노드에 대해 이 단계를 반복하십시오.
   a. 노드에 로그인합니다.
   b. * 구성 * > * 액세스 제어 * > * 싱글 사인온 * 을 선택합니다.
   c. 해당 노드의 SAML 메타데이터를 다운로드하여 저장하십시오.
3. PingFederate로 이동합니다.
4. "StorageGRID에 대한 하나 이상의 서비스 공급자(SP) 연결 생성". 각 관리 노드에 대한 SP 연결 ID(SSO 구성 페이지의 표에 표시됨)와 해당 관리 노드에 대해 다운로드한 SAML 메타데이터를 사용하십시오.

   표에 표시된 각 관리 노드에 대해 SP 연결을 하나씩 생성해야 합니다.

테스트 구성

StorageGRID 시스템 전체에 싱글 사인온(SSO) 사용을 적용하기 전에 각 관리 노드에 대해 싱글 사인온 및 싱글 로그아웃이 올바르게 구성되었는지 확인하십시오.

Active Directory

단계

1. SSO 구성 페이지에서 구성 마법사의 구성 테스트 단계에 있는 링크를 찾습니다.

   URL은 연합 서비스 이름 필드에 입력한 값에서 파생됩니다.

2. 링크를 선택하거나 URL을 복사하여 브라우저에 붙여넣어 ID 제공업체의 로그인 페이지에 접속하십시오.
3. SSO를 사용하여 StorageGRID에 로그인할 수 있는지 확인하려면 *다음 사이트 중 하나에 로그인*을 선택하고 기본 관리 노드에 대한 신뢰 당사자 식별자를 선택한 다음 *로그인*을 선택하십시오.
4. 연동 사용자 이름과 비밀번호를 입력하십시오.
   - SSO 로그인 및 로그아웃 작업이 성공하면 성공 메시지가 표시됩니다.
   - SSO 작업이 실패하면 오류 메시지가 표시됩니다. 문제를 해결하려면 브라우저의 쿠키를 삭제한 후 다시 시도하십시오.
5. 그리드의 각 관리 노드에 대해 SSO 연결을 확인하려면 이 단계를 반복하십시오.

Entra ID

단계

1. Azure 포털의 싱글 사인온 페이지로 이동합니다.
2. *이 애플리케이션 테스트*를 선택합니다.
3. 연합 사용자 자격 증명을 입력하십시오.
   - SSO 로그인 및 로그아웃 작업이 성공하면 성공 메시지가 표시됩니다.
   - SSO 작업이 실패하면 오류 메시지가 표시됩니다. 문제를 해결하려면 브라우저의 쿠키를 삭제한 후 다시 시도하십시오.
4. 그리드의 각 관리 노드에 대해 SSO 연결을 확인하려면 이 단계를 반복하십시오.

PingFederate

단계

1. SSO 구성 페이지에서 샌드박스 모드 메시지의 첫 번째 링크를 선택합니다.

   한 번에 하나의 링크만 선택하여 테스트하십시오.

2. 연합 사용자 자격 증명을 입력하십시오.
   - SSO 로그인 및 로그아웃 작업이 성공하면 성공 메시지가 표시됩니다.
   - SSO 작업이 실패하면 오류 메시지가 표시됩니다. 문제를 해결하려면 브라우저의 쿠키를 삭제한 후 다시 시도하십시오.
3. 그리드에 있는 각 관리 노드의 SSO 연결을 확인하려면 다음 링크를 선택하십시오.

   '페이지 만료' 메시지가 표시되면 브라우저에서 뒤로 버튼을 선택하고 자격 증명을 다시 제출하세요.

싱글 사인온 활성화

각 관리 노드에 SSO를 사용하여 로그인할 수 있음을 확인했으면 전체 StorageGRID 시스템에 대해 SSO를 활성화할 수 있습니다.

> SSO가 활성화되면 모든 사용자는 Grid Manager, Tenant Manager, Grid Management API 및 Tenant Management API에 액세스하려면 SSO를 사용해야 합니다. 로컬 사용자는 더 이상 StorageGRID에 액세스할 수 없습니다.

단계

1. SSO 구성 마법사의 테스트 구성 단계에서 *SSO 활성화*를 선택합니다.
2. 경고 메시지를 검토하고 *SSO 활성화*를 선택하십시오.

   싱글 사인온(SSO)이 활성화되었습니다. 싱글 사인온 페이지가 나타나고, 방금 구성한 SSO에 대한 세부 정보가 표시됩니다.

3. 구성을 편집하려면 *편집*을 선택합니다.
4. 싱글 사인온(SSO)을 비활성화하려면 *SSO 비활성화*를 선택합니다.

> Azure Portal을 사용하고 Entra ID에 액세스하는 데 사용하는 동일한 컴퓨터에서 StorageGRID에 액세스하는 경우, Azure Portal 사용자가 승인된 StorageGRID 사용자(StorageGRID로 가져온 페더레이션 그룹의 사용자)인지 확인하거나, StorageGRID에 로그인하기 전에 Azure Portal에서 로그아웃하십시오.

AD FS에서 StorageGRID에 대한 신뢰 당사자 트러스트 생성

시스템의 각 관리 노드에 대해 Active Directory Federation Services(AD FS)를 사용하여 신뢰 당사자 트러스트를 생성해야 합니다. PowerShell 명령을 사용하거나 StorageGRID에서 SAML 메타데이터를 가져오거나 데이터를 수동으로 입력하여 신뢰 당사자 트러스트를 생성할 수 있습니다.

시작하기 전에

- StorageGRID에 대해 Single Sign-On을 구성했으며 SSO 유형으로 *AD FS*를 선택했습니다.
- Grid Manager에 "샌드박스 모드에 진입했습니다."이(가) 있습니다.
- 시스템에 있는 각 관리 노드의 정규화된 도메인 이름(또는 IP 주소)과 신뢰 당사자 식별자를 알고 있습니다. 이러한 값은 StorageGRID SSO 구성 페이지의 관리 노드 세부 정보 테이블에서 찾을 수 있습니다.

> StorageGRID 시스템의 각 관리 노드에 대해 신뢰 당사자 트러스트를 생성해야 합니다. 각 관리 노드에 대한 신뢰 당사자 트러스트를 설정하면 사용자가 모든 관리 노드에 안전하게 로그인하고 로그아웃할 수 있습니다.

- AD FS에서 신뢰 당사자 트러스트를 생성해 본 경험이 있거나 Microsoft AD FS 설명서에 액세스할 수 있어야 합니다.
- 현재 AD FS 관리 스냅인을 사용 중이며 관리자 그룹에 속해 있습니다.
- 신뢰 당사자 트러스트를 수동으로 생성하는 경우 StorageGRID 관리 인터페이스에 업로드된 사용자 지정 인증서가 있거나 명령 셸에서 관리 노드에 로그인하는 방법을 알고 있어야 합니다.

이 작업 정보

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

Windows PowerShell을 사용하여 신뢰 당사자 트러스트 만들기

Windows PowerShell을 사용하여 하나 이상의 신뢰 당사자 트러스트를 신속하게 생성할 수 있습니다.

단계

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

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

   - `*Admin_Node_Identifier*`의 경우, Single Sign-on 페이지에 표시된 대로 관리자 노드의 신뢰 당사자 식별자(Relying Party Identifier)를 정확히 입력하십시오. 예를 들어, `SG-DC1-ADM1`입니다.
   - `*Admin_Node_FQDN*`에는 동일한 관리 노드의 정규화된 도메인 이름을 입력하십시오. (필요한 경우 노드의 IP 주소를 대신 사용할 수 있습니다. 단, 여기에 IP 주소를 입력하는 경우 해당 IP 주소가 변경되면 이 신뢰 당사자 트러스트를 업데이트하거나 다시 생성해야 합니다.)
3. Windows 서버 관리자에서 도구 > *AD FS 관리*를 선택합니다.

   AD FS 관리 툴이 나타납니다.
4. **AD FS** > *Relying Party Trusts*를 선택합니다.

   신뢰 당사자 트러스트 목록이 표시됩니다.
5. 새로 생성된 신뢰 당사자 트러스트에 액세스 제어 정책을 추가합니다.
   a. 방금 생성한 신뢰 당사자 트러스트를 찾으십시오.
   b. 트러스트를 마우스 오른쪽 버튼으로 클릭하고 *액세스 제어 정책 편집*을 선택합니다.
   c. 접근 제어 정책을 선택하십시오.
   d. *적용*을 선택하고 *확인*을 선택합니다.
6. 새로 생성된 신뢰 당사자 트러스트에 클레임 발급 정책을 추가합니다.
   a. 방금 생성한 신뢰 당사자 트러스트를 찾으십시오.
   b. 트러스트를 마우스 오른쪽 버튼으로 클릭하고 *클레임 발급 정책 편집*을 선택합니다.
   c. *규칙 추가*를 선택합니다.
   d. 규칙 템플릿 선택 페이지에서 목록에서 *LDAP 속성을 클레임으로 전송*을 선택하고 *다음*을 선택합니다.
   e. 규칙 구성 페이지에서 이 규칙에 대한 표시 이름을 입력합니다.

      예를 들어, **ObjectGUID to Name ID** 또는 **UPN to Name ID**.

   f. 속성 저장소로 *Active Directory*를 선택하십시오.

g. 매핑 테이블의 LDAP 속성 열에 *objectGUID*를 입력하거나 *User-Principal-Name*을 선택합니다.

h. 매핑 테이블의 나가는 클레임 유형 열에서 드롭다운 목록에서 *Name ID*를 선택합니다.

i. *마침*을 선택하고 *확인*을 선택합니다.

7. 메타데이터를 성공적으로 가져왔는지 확인하십시오.

a. 신뢰 당사자 트러스트를 마우스 오른쪽 버튼으로 클릭하여 속성을 엽니다.

b. 엔드포인트, 식별자, 서명 탭의 모든 필드가 채워져 있는지 확인하십시오.

메타데이터가 누락된 경우, 페더레이션 메타데이터 주소가 올바른지 확인하거나 값을 수동으로 입력하십시오.

8. StorageGRID 시스템의 모든 관리 노드에 대한 신뢰 당사자 트러스트를 구성하려면 이 단계를 반복하십시오.

9. 완료되면 StorageGRID로 돌아가서 "모든 신뢰 당사자 트러스트를 테스트합니다." 올바르게 구성되었는지 확인하십시오.

페더레이션 메타데이터를 가져와서 신뢰 당사자 트러스트 만들기

각 관리 노드의 SAML 메타데이터에 액세스하여 각 신뢰 당사자 트러스트에 대한 값을 가져올 수 있습니다.

단계

1. Windows 서버 관리자에서 *도구*를 선택한 다음 *AD FS 관리*를 선택합니다.

2. 작업에서 *Add Relying Party Trust*를 선택합니다.

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

4. *온라인 또는 로컬 네트워크에 게시된 신뢰 당사자에 대한 데이터 가져오기*를 선택하십시오.

5. *연합 메타데이터 주소(호스트 이름 또는 URL)*에 이 관리 노드의 SAML 메타데이터 위치를 입력합니다.

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

`_Admin_Node_FQDN_`에는 동일한 관리 노드의 정규화된 도메인 이름을 입력하십시오. (필요한 경우 노드의 IP 주소를 대신 사용할 수 있습니다. 단, 여기에 IP 주소를 입력하는 경우 해당 IP 주소가 변경되면 이 신뢰 당사자 트러스트를 업데이트하거나 다시 생성해야 합니다.)

6. 신뢰 당사자 트러스트 마법사를 완료하고, 신뢰 당사자 트러스트를 저장한 다음, 마법사를 닫으십시오.

표시 이름을 입력할 때는 그리드 관리자의 싱글 사인온 페이지에 표시된 관리자 노드의 신뢰 당사자 식별자(Relying Party Identifier)를 그대로 사용하십시오. 예를 들어, `SG-DC1-ADM1`입니다.

7. 클레임 규칙 추가:

a. 트러스트를 마우스 오른쪽 버튼으로 클릭하고 *클레임 발급 정책 편집*을 선택합니다.

b. *규칙 추가*를 선택합니다:

c. 규칙 템플릿 선택 페이지에서 목록에서 *LDAP 속성을 클레임으로 전송*을 선택하고 *다음*을 선택합니다.

d. 규칙 구성 페이지에서 이 규칙에 대한 표시 이름을 입력합니다.

예를 들어, **ObjectGUID to Name ID** 또는 **UPN to Name ID**.

e. 속성 저장소로 *Active Directory*를 선택하십시오.

f. 매핑 테이블의 LDAP 속성 열에 *objectGUID*를 입력하거나 *User-Principal-Name*을 선택합니다.

g. 매핑 테이블의 나가는 클레임 유형 열에서 드롭다운 목록에서 *Name ID*를 선택합니다.

h. *마침*을 선택하고 *확인*을 선택합니다.

8. 메타데이터를 성공적으로 가져왔는지 확인하십시오.

a. 신뢰 당사자 트러스트를 마우스 오른쪽 버튼으로 클릭하여 속성을 엽니다.

b. 엔드포인트, 식별자, 서명 탭의 모든 필드가 채워져 있는지 확인하십시오.

메타데이터가 누락된 경우, 페더레이션 메타데이터 주소가 올바른지 확인하거나 값을 수동으로 입력하십시오.

9. StorageGRID 시스템의 모든 관리 노드에 대한 신뢰 당사자 트러스트를 구성하려면 이 단계를 반복하십시오.

10. 완료되면 StorageGRID로 돌아가서 "모든 신뢰 당사자 트러스트를 테스트합니다." 올바르게 구성되었는지 확인하십시오.

신뢰 당사자 트러스트를 수동으로 생성합니다

신뢰 당사자 신탁에 대한 데이터를 가져오지 않으려면 값을 수동으로 입력할 수 있습니다.

단계

1. Windows 서버 관리자에서 *도구*를 선택한 다음 *AD FS 관리*를 선택합니다.

2. 작업에서 *Add Relying Party Trust*를 선택합니다.

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

4. *신뢰 당사자에 대한 데이터를 수동으로 입력하세요*를 선택하고 *다음*을 선택합니다.

5. 신뢰 당사자 트러스트 마법사를 완료합니다.

a. 이 관리자 노드에 표시할 이름을 입력하십시오.

일관성을 유지하기 위해 관리자 노드에 대한 신뢰 당사자 식별자(Relying Party Identifier)는 그리드 관리자의 싱글 사인온 페이지에 표시된 것과 정확히 동일하게 사용하십시오. 예를 들어, `SG-DC1-ADM1`.

b. 선택 사항인 토큰 암호화 인증서 구성 단계를 건너뜁니다.

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

d. 관리자 노드의 SAML 서비스 엔드포인트 URL을 입력하십시오.

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

> `_Admin_Node_FQDN_`에는 관리 노드의 정규화된 도메인 이름을 입력하십시오. (필요한 경우 노드의 `IP` 주소를 대신 사용할 수 있습니다. 단, 여기에 `IP` 주소를 입력하는 경우 해당 `IP` 주소가 변경되면 이 신뢰 당사자 트러스트를 업데이트하거나 다시 생성해야 합니다.)

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

Admin_Node_Identifier

`_Admin_Node_Identifier_`의 경우, Single Sign-on 페이지에 표시된 대로 관리자 노드의 신뢰 당사자 식별자(Relying Party Identifier)를 정확히 입력하십시오. 예를 들어, `SG-DC1-ADM1`입니다.

f. 설정을 검토하고, 신뢰 당사자 트러스트를 저장한 다음 마법사를 닫습니다.

청구 발행 정책 편집 대화 상자가 나타납니다.

대화 상자가 나타나지 않으면 해당 트러스트를 마우스 오른쪽 버튼으로 클릭하고 *클레임 발급 정책 편집*을 선택하십시오.

6. 클레임 규칙 마법사를 시작하려면 *규칙 추가*를 선택합니다.
   a. 규칙 템플릿 선택 페이지에서 목록에서 *LDAP 속성을 클레임으로 전송*을 선택하고 *다음*을 선택합니다.
   b. 규칙 구성 페이지에서 이 규칙에 대한 표시 이름을 입력합니다.

      예를 들어, **ObjectGUID to Name ID** 또는 **UPN to Name ID**.

   c. 속성 저장소로 *Active Directory*를 선택하십시오.
   d. 매핑 테이블의 LDAP 속성 열에 *objectGUID*를 입력하거나 *User-Principal-Name*을 선택합니다.
   e. 매핑 테이블의 나가는 클레임 유형 열에서 드롭다운 목록에서 *Name ID*를 선택합니다.
   f. *마침*을 선택하고 *확인*을 선택합니다.
7. 신뢰 당사자 트러스트를 마우스 오른쪽 버튼으로 클릭하여 속성을 엽니다.
8. 엔드포인트 탭에서 단일 로그아웃(SLO)용 엔드포인트를 구성합니다.
   a. *SAML 추가*를 선택합니다.
   b. 엔드포인트 유형 > *SAML 로그아웃*을 선택합니다.
   c. 바인딩 > *리디렉션*을 선택합니다.
   d. 신뢰할 수 있는 **URL** 필드에 이 관리자 노드에서 단일 로그아웃(SLO)에 사용되는 URL을 입력하십시오.

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

   에는 `*Admin_Node_FQDN*`관리 노드의 정규화된 도메인 이름을 입력하십시오. (필요한 경우 노드의 IP 주소를 대신 사용할 수 있습니다. 단, 여기에 IP 주소를 입력하는 경우 해당 IP 주소가 변경되면 이 신뢰 당사자 트러스트를 업데이트하거나 다시 생성해야 합니다.)

   a. *확인*을 선택합니다.
9. 서명 탭에서 이 신뢰 당사자 트러스트에 사용할 서명 인증서를 지정합니다.
   a. 사용자 지정 인증서를 추가합니다:
      - StorageGRID에 업로드한 사용자 지정 관리 인증서가 있는 경우 해당 인증서를 선택하십시오.

- 사용자 지정 인증서가 없는 경우 관리자 노드에 로그인하여 `/var/local/mgmt-api` 관리자 노드 디렉터리로 이동한 다음 `custom-server.crt` 인증서 파일을 추가하십시오.

> 관리자 노드의 기본 인증서 (`server.crt`를 사용하는 것은 권장되지 않습니다. 관리자 노드에 장애가 발생하면 노드를 복구할 때 기본 인증서가 다시 생성되며, 이때 신뢰 당사자 설정을 업데이트해야 합니다.

b. *적용*을 선택하고 *확인*을 선택합니다.

신뢰 당사자 속성이 저장되고 닫힙니다.

10. StorageGRID 시스템의 모든 관리 노드에 대한 신뢰 당사자 트러스트를 구성하려면 이 단계를 반복하십시오.
11. 완료되면 StorageGRID로 돌아가서 "모든 신뢰 당사자 트러스트를 테스트합니다." 올바르게 구성되었는지 확인하십시오.

Entra ID에서 StorageGRID용 엔터프라이즈 애플리케이션 생성

Entra ID를 사용하여 시스템의 각 관리 노드에 대한 엔터프라이즈 애플리케이션을 생성합니다.

시작하기 전에

- StorageGRID에 대한 Single Sign-On 구성을 시작했으며 SSO 유형으로 *Entra ID*를 선택했습니다.
- Grid Manager에 "샌드박스 모드에 진입했습니다."이(가) 있습니다.
- 시스템에는 각 관리 노드에 대한 *엔터프라이즈 애플리케이션 이름*이 있습니다. 이러한 값은 SSO 구성 페이지의 관리 노드 세부 정보 표에서 복사할 수 있습니다.

> StorageGRID 시스템의 각 관리 노드마다 엔터프라이즈 애플리케이션을 생성해야 합니다. 각 관리 노드에 엔터프라이즈 애플리케이션을 설치하면 사용자가 모든 관리 노드에 안전하게 로그인하고 로그아웃할 수 있습니다.

- Entra ID를 사용하여 엔터프라이즈 애플리케이션을 개발한 경험이 있으십니다.
- 귀하는 활성 구독이 있는 Entra ID 계정을 보유하고 있습니다.
- Entra ID 계정에는 글로벌 관리자, 클라우드 애플리케이션 관리자, 애플리케이션 관리자 또는 서비스 주체 소유자 중 하나의 역할이 있습니다.

Entra ID 액세스

단계

1. "Azure 포털"에 로그인합니다.
2. 다음으로 이동하세요. "Entra ID"
3. 선택 "기업용 애플리케이션"합니다.

엔터프라이즈 애플리케이션을 생성하고 StorageGRID SSO 구성을 저장합니다

StorageGRID에서 Entra ID에 대한 SSO 구성을 저장하려면 Entra ID를 사용하여 각 관리 노드에 대한 엔터프라이즈 애플리케이션을 생성해야 합니다. Entra ID에서 페더레이션 메타데이터 URL을 복사하여 SSO 구성 페이지의 해당

페더레이션 메타데이터 **URL** 필드에 붙여넣습니다.

단계

1. 각 관리 노드에 대해 다음 단계를 반복하십시오.
   a. Entra ID 엔터프라이즈 애플리케이션 창에서 *새 애플리케이션*을 선택합니다.
   b. *나만의 애플리케이션 만들기*를 선택합니다.
   c. 이름에는 SSO 구성 페이지의 관리자 노드 세부 정보 표에서 복사한 *엔터프라이즈 애플리케이션 이름*을 입력하십시오.
   d. 갤러리에서 찾을 수 없는 다른 애플리케이션 통합(비갤러리) 라디오 버튼을 선택된 상태로 두십시오.
   e. *생성*을 선택합니다.
   f. **2.** 싱글 사인온 설정 상자에서 시작하기 링크를 선택하거나 왼쪽 여백에서 싱글 사인온 링크를 선택하세요.
   g. **SAML** 상자를 선택합니다.
   h. *3단계 SAML 서명 인증서*에서 찾을 수 있는 *앱 페더레이션 메타데이터 URL*을 복사합니다.
   i. SSO 구성 페이지로 이동하여 사용한 엔터프라이즈 애플리케이션 이름*에 해당하는 **URL**을 *페더레이션 메타데이터 **URL** 필드에 붙여넣습니다.
2. 각 관리 노드에 대한 페더레이션 메타데이터 URL을 붙여넣고 SSO 구성에 필요한 다른 모든 변경 사항을 적용한 후 SSO 구성 페이지에서 *저장*을 선택하십시오.

모든 관리자 노드에 대한 **SAML** 메타데이터를 다운로드합니다**.**

SSO 구성이 저장되면 StorageGRID 시스템의 각 관리 노드에 대한 SAML 메타데이터 파일을 다운로드할 수 있습니다.

단계

1. 각 관리 노드에 대해 이 단계를 반복하십시오.
   a. 관리 노드에서 StorageGRID에 로그인합니다.
   b. * 구성 * > * 액세스 제어 * > * 싱글 사인온 * 을 선택합니다.
   c. 해당 관리 노드의 SAML 메타데이터를 다운로드하려면 버튼을 선택하십시오.
   d. Entra ID에 업로드할 파일을 저장합니다.

SAML 메타데이터를 각 엔터프라이즈 애플리케이션에 업로드합니다

각 StorageGRID 관리 노드에 대한 SAML 메타데이터 파일을 다운로드한 후 Entra ID에서 다음 단계를 수행하십시오.

단계

1. Azure 포털로 돌아가십시오.
2. 각 엔터프라이즈 애플리케이션에 대해 이 단계를 반복합니다.

   > 이전에 추가한 애플리케이션이 목록에 표시되려면 엔터프라이즈 애플리케이션 페이지를 새로고침해야 할 수 있습니다.

   a. 엔터프라이즈 애플리케이션의 속성 페이지로 이동합니다.
   b. *할당 필요*를 *아니요*로 설정합니다(할당을 별도로 구성하려는 경우는 제외).

c. 싱글 사인온 페이지로 이동합니다.

d. SAML 구성을 완료합니다.

e. 메타데이터 파일 업로드 버튼을 선택하고 해당 관리자 노드에 대해 다운로드한 SAML 메타데이터 파일을 선택하십시오.

f. 파일이 로드되면 *저장*을 선택한 다음 *X*를 선택하여 창을 닫습니다. 그러면 SAML을 사용한 싱글 사인온 설정 페이지로 돌아갑니다.

3. "각 애플리케이션을 테스트합니다.".

StorageGRID에 대한 PingFederate에서 서비스 공급자 연결 생성

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

시작하기 전에

- StorageGRID에 대한 Single Sign-On을 구성했으며 SSO 유형으로 *Ping Federate*를 선택했습니다.
- Grid Manager에 "샌드박스 모드에 진입했습니다."이(가) 있습니다.
- 시스템의 각 관리자 노드에 대한 *SP 연결 ID*가 있습니다. 이러한 값은 SSO 구성 페이지의 관리자 노드 세부 정보 테이블에서 확인할 수 있습니다.
- 시스템의 각 관리자 노드에 대한 *SAML 메타데이터*를 다운로드했습니다.
- PingFederate 서버에서 SP 연결을 생성해 본 경험이 있습니다.
- PingFederate 서버용 "관리자 참조 가이드"이(가) 있습니다. PingFederate 설명서에서 자세한 단계별 지침과 설명을 확인할 수 있습니다.
- PingFederate 서버용 "관리자 권한"이(가) 있습니다.

이 작업 정보

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

PingFederate에서 사전 요구 사항 완료

StorageGRID에 사용할 SP 연결을 생성하기 전에 PingFederate에서 필수 작업을 완료해야 합니다. SP 연결을 구성할 때 이러한 필수 작업에서 얻은 정보를 사용합니다.

데이터 저장소 생성

아직 데이터 저장소를 생성하지 않았다면 PingFederate를 AD FS LDAP 서버에 연결하는 데이터 저장소를 생성하십시오. StorageGRID에서 "ID 페더레이션 구성" 할 때 사용한 값을 사용하십시오.

- 유형: 디렉터리(LDAP)
- **LDAP** 유형: Active Directory
- 바이너리 속성 이름: LDAP 바이너리 속성 탭에 표시된 대로 *objectGUID*를 정확하게 입력하십시오.

암호 자격 증명 유효성 검사기 생성

아직 비밀번호 자격 증명 유효성 검사기를 만들지 않았다면 지금 만드세요.

- 유형: LDAP 사용자 이름 암호 자격 증명 유효성 검사기
- 데이터 저장소: 생성한 데이터 저장소를 선택합니다.
- 검색 기준: LDAP에서 정보를 입력하십시오(예: DC=saml,DC=sgws).
- 검색 필터: sAMAccountName=${username}
- 범위: 서브트리

IdP 어댑터 인스턴스 생성

아직 IdP 어댑터 인스턴스를 생성하지 않았다면 지금 생성하세요.

단계

1. 인증 > 통합 > *IdP 어댑터*로 이동합니다.
2. *새 인스턴스 생성*을 선택합니다.
3. 유형 탭에서 *HTML Form IdP Adapter*를 선택합니다.
4. IdP 어댑터 탭에서 *'Credential Validators'에 새 행 추가*를 선택합니다.
5. 생성한 비밀번호 자격 증명 유효성 검사기을 선택합니다.
6. 어댑터 속성 탭에서 가명*에 대해 *사용자 이름 속성을 선택합니다.
7. *저장*을 선택하세요.

서명 인증서를 생성하거나 가져옵니다**.**

아직 서명 인증서를 생성하거나 가져오지 않았다면 지금 생성하거나 가져오세요.

단계

1. 보안 > *서명 및 복호화 키 및 인증서*로 이동합니다.
2. 서명 인증서를 생성하거나 가져옵니다.

PingFederate에서 SP 연결 만들기

PingFederate에서 SP 연결을 생성할 때 관리 노드용으로 StorageGRID에서 다운로드한 SAML 메타데이터를 가져옵니다. 메타데이터 파일에는 필요한 여러 특정 값이 포함되어 있습니다.

StorageGRID 시스템의 각 관리 노드에 대해 SP 연결을 생성해야 사용자가 모든 노드에 안전하게 로그인하고 로그아웃할 수 있습니다. 이 지침에 따라 첫 번째 SP 연결을 생성하십시오. 그런 다음, 추가 SP 연결 생성으로 이동하여 필요한 추가 연결을 생성하십시오.

SP 연결 유형 선택

단계

1. 응용 프로그램 > 통합 > *SP 연결*로 이동하세요.

2. *연결 생성*을 선택합니다.
3. *이 연결에 템플릿을 사용하지 않음*을 선택합니다.
4. 브라우저 **SSO** 프로필 및 프로토콜로 *SAML 2.0*을 선택합니다.

SP 메타데이터 가져오기

단계

1. 메타데이터 가져오기 탭에서 *파일*을 선택합니다.
2. 관리 노드의 SSO 구성 페이지에서 다운로드한 SAML 메타데이터 파일을 선택하십시오.
3. 메타데이터 요약과 일반 정보 탭에 제공된 정보를 검토하십시오.

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

4. * 다음 * 을 선택합니다.

IdP 브라우저 **SSO** 구성

단계

1. 브라우저 SSO 탭에서 *브라우저 SSO 구성*을 선택합니다.
2. SAML 프로필 탭에서 **SP-initiated SSO**, **SP-initial SLO**, **IdP-initiated SSO** 및 **IdP-initiated SLO** 옵션을 선택합니다.
3. * 다음 * 을 선택합니다.
4. 어설션 수명 탭에서는 아무것도 변경하지 마십시오.
5. 어설션 생성 탭에서 *어설션 생성 구성*을 선택합니다.
   a. ID 매핑 탭에서 *표준*을 선택합니다.
   b. 속성 계약 탭에서 속성 계약으로 *SAML_SUBJECT*를 사용하고 가져온 지정되지 않은 이름 형식을 사용합니다.
6. 계약 연장의 경우, 사용하지 않는 `urn:oid`을(를) 제거하려면 *삭제*를 선택합니다.

맵 어댑터 인스턴스

단계

1. 인증 소스 매핑 탭에서 *새 어댑터 인스턴스 매핑*을 선택합니다.
2. 어댑터 인스턴스 탭에서 생성한 어댑터 인스턴스을 선택합니다.
3. 매핑 방법 탭에서 *데이터 저장소에서 추가 속성 검색*을 선택합니다.
4. 속성 소스 및 사용자 조회 탭에서 *속성 소스 추가*를 선택합니다.
5. 데이터 저장소 탭에서 설명을 입력하고 추가한 데이터 저장소을 선택합니다.
6. LDAP 디렉터리 검색 탭에서:
   - *기본 DN*을 입력하십시오. 이 값은 LDAP 서버에 대해 StorageGRID에 입력한 값과 정확히 일치해야 합니다.
   - 검색 범위에서 *하위 트리*를 선택합니다.

◦ 루트 객체 클래스의 경우, **objectGUID** 또는 **userPrincipalName** 속성 중 하나를 검색하여 추가하십시오.

7. LDAP 이진 속성 인코딩 유형 탭에서 **objectGUID** 속성에 대해 *Base64*를 선택합니다.
8. LDAP 필터 탭에서 *sAMAccountName=${username}*를 입력합니다.
9. 속성 계약 이행 탭에서 소스 드롭다운에서 **LDAP(속성)***을 선택하고 값 드롭다운에서 ***objectGUID** 또는 *userPrincipalName*을 선택합니다.
10. 속성 소스를 검토한 후 저장합니다.
11. Failsave Attribute Source 탭에서 *SSO 트랜잭션 취소*를 선택합니다.
12. 요약 내용을 검토하고 *완료*를 선택합니다.
13. *완료*를 선택합니다.

프로토콜 설정 구성

단계

1. **SP Connection** > **Browser SSO** > **Protocol Settings** 탭에서 *Configure Protocol Settings*를 선택합니다.
2. 어설션 소비자 서비스 URL 탭에서 StorageGRID SAML 메타데이터에서 가져온 기본값(바인딩의 경우 **POST** 및 엔드포인트 URL의 경우 `/api/saml-response`)을 그대로 사용하십시오.
3. SLO 서비스 URL 탭에서 StorageGRID SAML 메타데이터에서 가져온 기본값(바인딩의 경우 **REDIRECT**, 엔드포인트 URL의 경우 `/api/saml-logout`)을 그대로 사용하십시오.
4. 허용 가능한 SAML 바인딩 탭에서 *ARTIFACT*와 *SOAP*를 선택 해제하세요. *POST*와 *REDIRECT*만 필수입니다.
5. 서명 정책 탭에서 인증 요청에 서명 필수 및 항상 어설션에 서명 확인란을 선택된 상태로 둡니다.
6. 암호화 정책 탭에서 *없음*을 선택합니다.
7. 요약 내용을 검토하고 *완료*를 선택하여 프로토콜 설정을 저장하십시오.
8. 요약 내용을 검토하고 *완료*를 선택하여 브라우저 SSO 설정을 저장합니다.

자격 증명 구성

단계

1. SP 연결 탭에서 *자격 증명*을 선택합니다.
2. 자격 증명 탭에서 *자격 증명 구성*을 선택합니다.
3. 생성하거나 가져온 서명 인증서을(를) 선택합니다.
4. *다음*을 선택하여 *서명 확인 설정 관리*로 이동합니다.
   a. 신뢰 모델 탭에서 *고정되지 않음*을 선택합니다.
   b. 서명 확인 인증서 탭에서 StorageGRID SAML 메타데이터에서 가져온 서명 인증서 정보를 검토합니다.
5. 요약 화면을 검토하고 *저장*을 선택하여 SP 연결을 저장하십시오.

추가 **SP** 연결 생성

첫 번째 SP 연결을 복사하여 그리드의 각 관리 노드에 필요한 SP 연결을 생성할 수 있습니다. 각 복사본마다 새로운 메타데이터를 업로드합니다.

서로 다른 관리 노드에 대한 SP 연결은 파트너 엔티티 ID, 기본 URL, 연결 ID, 연결 이름, 서명 확인 및 SLO 응답 URL을 제외하고는 동일한 설정을 사용합니다.

단계

1. 추가 관리 노드마다 초기 SP 연결의 복사본을 만들려면 작업 > *복사*를 선택하십시오.
2. 복사본에 대한 연결 ID와 연결 이름을 입력하고 *저장*을 선택합니다.
3. 관리 노드에 해당하는 메타데이터 파일을 선택하십시오.
   a. 작업 > *메타데이터로 업데이트*를 선택합니다.
   b. *파일 선택*을 선택하고 메타데이터를 업로드합니다.
   c. * 다음 * 을 선택합니다.
   d. *저장*을 선택하세요.
4. 사용되지 않는 속성으로 인해 발생하는 오류를 해결하세요:
   a. 새 연결을 선택합니다.
   b. *브라우저 SSO 구성 > 어설션 생성 구성 > 속성 계약*을 선택하십시오.
   c. **urn:oid** 항목을 삭제합니다.
   d. *저장*을 선택하세요.

StorageGRID에서 SSO 비활성화

싱글 사인온(SSO) 기능을 더 이상 사용하지 않으려면 비활성화할 수 있습니다. ID 페더레이션을 비활성화하려면 먼저 싱글 사인온을 비활성화해야 합니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- "특정 액세스 권한"이(가) 있습니다.

단계

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

   싱글 사인온 페이지가 나타납니다.

2. *SSO 비활성화*를 선택합니다.
3. *예*를 선택합니다.

   로컬 사용자가 이제 로그인할 수 있다는 경고 메시지가 나타납니다.

다음에 StorageGRID에 로그인하면 StorageGRID 로그인 페이지가 나타나고 로컬 또는 페더레이션 StorageGRID 사용자의 사용자 이름과 암호를 입력해야 합니다.

StorageGRID 관리 노드에 대한 SSO를 일시적으로 비활성화했다가 다시 활성화합니다

싱글 사인온(SSO) 시스템에 장애가 발생하면 그리드 관리자에 로그인할 수 없습니다. 이 경우, 특정 관리 노드에 대해 SSO를 일시적으로 비활성화한 후 다시 활성화할 수 있습니다. SSO를 비활성화한 후 다시 활성화하려면 해당 노드의 명령 셸에 접속해야 합니다.

시작하기 전에

- "특정 액세스 권한"이(가) 있습니다.
- You have the `Passwords.txt` 파일을 가지고 계시네요.
- 로컬 루트 사용자의 암호를 알고 있습니다.

이 작업 정보

하나의 관리 노드에 대해 SSO를 비활성화한 후에는 로컬 루트 사용자로 Grid Manager에 로그인할 수 있습니다. StorageGRID 시스템의 보안을 유지하려면 로그아웃하는 즉시 노드의 명령 셸을 사용하여 관리 노드에서 SSO를 다시 활성화해야 합니다.

하나의 관리자 노드에 대해 SSO를 비활성화해도 그리드 내 다른 관리자 노드의 SSO 설정에는 영향을 미치지 않습니다. 그리드 관리자의 싱글 사인온 페이지에서 **SSO** 활성화 확인란은 선택된 상태로 유지되며, 기존 SSO 설정은 사용자가 업데이트하지 않는 한 그대로 유지됩니다.

단계

1. 관리자 노드에 로그인합니다.
   a. 다음 명령을 입력합니다. `ssh admin@Admin_Node_IP`
   b. `Passwords.txt` 파일에 나와 있는 비밀번호를 입력하십시오.
   c. 루트 권한으로 전환하려면 다음 명령을 입력하십시오. `su -`
   d. `Passwords.txt` 파일에 나와 있는 비밀번호를 입력하십시오.

      루트 계정으로 로그인하면 프롬프트가 `$`에서 `#`로 변경됩니다.

2. 다음 명령을 실행합니다.`disable-saml`

   해당 명령은 이 관리 노드에만 적용된다는 메시지가 표시됩니다.

3. SSO를 비활성화할 것인지 확인합니다.

   해당 노드에서 싱글 사인온(SSO)이 비활성화되었다는 메시지가 표시됩니다.

4. 웹 브라우저를 통해 동일한 관리 노드에서 그리드 관리자에 접속합니다.

   SSO가 비활성화되었으므로 이제 그리드 관리자 로그인 페이지가 표시됩니다.

5. 사용자 이름 root와 로컬 루트 사용자의 암호로 로그인합니다.
6. SSO 구성을 수정해야 하여 SSO를 일시적으로 비활성화한 경우:
   a. * 구성 * > * 액세스 제어 * > * 싱글 사인온 * 을 선택합니다.

b. 잘못되었거나 오래된 SSO 설정을 변경합니다.

c. *저장*을 선택하세요.

싱글 사인온 페이지에서 *저장*을 선택하면 전체 그리드에 대해 SSO가 자동으로 다시 활성화됩니다.

7. 다른 이유로 그리드 관리자에 액세스해야 해서 SSO를 일시적으로 비활성화한 경우:

a. 필요한 작업을 수행하십시오.

b. *로그아웃*을 선택하고 Grid Manager를 닫습니다.

c. 관리자 노드에서 SSO를 다시 활성화하십시오. 다음 단계 중 하나를 수행할 수 있습니다.

- 다음 명령을 실행합니다. `enable-saml`

해당 명령은 이 관리 노드에만 적용된다는 메시지가 표시됩니다.

SSO를 활성화할 것인지 확인합니다.

해당 노드에서 싱글 사인온(SSO)이 활성화되었다는 메시지가 표시됩니다.

- 그리드 노드를 재부팅하세요: `reboot`

8. 웹 브라우저를 통해 동일한 관리 노드에서 Grid Manager에 접속합니다.

9. StorageGRID 로그인 페이지가 나타나고 Grid Manager에 액세스하려면 SSO 자격 증명을 입력해야 하는지 확인하십시오.