SSO(Single Sign-On) 사용

StorageGRID software

NetApp
January 15, 2026

목차

SSO(Single Sign-On) 사용

SSO 작동 방식

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

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 처음으로 URL에 접속하는 경우 계정 ID를 입력하라는 메시지가 표시됩니다.
   - 이전에 Grid Manager나 Tenant Manager에 접속한 적이 있는 경우 최근 계정을 선택하거나 계정 ID를 입력하라는 메시지가 표시됩니다.

   > ⓘ 테넌트 계정에 대한 전체 URL(즉, 정규화된 도메인 이름 또는 IP 주소 다음에 가 오는 경우)을 입력하면 StorageGRID 로그인 페이지가 표시되지 않습니다 `/?accountId=20-digit-account-id`. 대신 조직의 SSO 로그인 페이지로 바로 리디렉션됩니다SSO 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.

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.

> 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.

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 Entra ID를 사용하는 경우 모든 관리 노드에서 로그아웃하는 데 몇 분이 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.

SSO에 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)
- 마이크로소프트 엔트라 ID
- 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	• Active Directory를 클릭합니다 • 엔트라 ID • PingFederate(PingFederate)
엔트라 ID	엔트라 ID

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 2016은, 이상을 사용해야 "KB3201845 업데이트" 합니다.

추가 요구 사항

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

Entra ID에 대한 고려 사항

SSO 유형으로 Entra ID를 사용하고 사용자의 사용자 주체 이름이 접두사로 sAMAccountName을 사용하지 않는 경우 StorageGRID LDAP 서버와 연결이 끊어지면 로그인 문제가 발생할 수 있습니다. 사용자가 로그인할 수 있도록 하려면 LDAP 서버에 대한 연결을 복원해야 합니다.

서버 인증서 요구 사항

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

아직 하지 않았다면 "관리 인터페이스에 대한 사용자 지정 인증서를 구성했습니다"지금 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 디렉터리로 이동하여 관리자 노드의 서버 인증서에 액세스할 수 `/var/local/mgmt-api` 있습니다. 사용자 지정 서버 인증서의 이름은 `custom-server.crt`입니다. 노드의 기본 서버 인증서 이름은 `server.crt`입니다.

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 "외부 방화벽에서 액세스를 제어합니다"참조하십시오.

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

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"
- 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. 그리드 관리자에서 구성 > 액세스 제어 > *관리자 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. 그리드 관리자에서 *테넌트*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.

   e. 테넌트 계정을 선택하고 * 로그인 * 을 선택한 다음 테넌트 계정에 로컬 루트 사용자로 로그인합니다.
   f. 테넌트 관리자에서 액세스 관리 > *그룹*을 선택합니다.
   g. Grid Manager에서 하나 이상의 통합 그룹에 이 테넌트에 대한 루트 액세스 권한이 할당되었는지 확인합니다.
   h. 로그아웃합니다.
   i. 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"

SSO 구성

SSO 구성 마법사를 따라 샌드박스 모드로 들어가서 모든 StorageGRID 사용자에 대해 SSO(단일 로그인)를 활성화하기 전에 SSO를 구성하고 테스트할 수 있습니다. SSO가 활성화된 후 구성을 변경하거나 다시 테스트해야 할 때 샌드박스 모드로 돌아갈 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "루트 액세스 권한"있습니다.
- StorageGRID 시스템에 대해 ID 페더레이션을 구성했습니다.
- ID 페더레이션 *LDAP 서비스 유형*의 경우, 사용하려는 SSO ID 공급자에 따라 Active Directory 또는 Entra ID를 선택했습니다.

구성된 **LDAP** 서비스 유형입니다	**SSO ID** 공급자에 대한 옵션
AD FS(Active Directory Federation Service)	• Active Directory를 클릭합니다 • 엔트라 ID • PingFederate(PingFederate)
엔트라 ID	엔트라 ID

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.
- Entra ID의 응답에는 UPN(사용자 주체 이름)이 포함되어 있습니다.

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

1. StorageGRID 에서 설정을 구성합니다.
2. SSO ID 공급자의 소프트웨어를 사용하여 각 관리 노드에 대한 신뢰 당사자 신뢰(AD FS), 엔터프라이즈 애플리케이션(Entra ID) 또는 서비스 공급자(PingFederate)를 만듭니다.
3. SSO를 활성화하려면 StorageGRID 로 돌아가세요.

샌드박스 모드를 사용하면 이러한 왕복 구성을 쉽게 수행하고 SSO를 활성화하기 전에 모든 설정을 테스트할 수 있습니다. 샌드박스 모드를 사용하는 경우 사용자는 SSO를 사용하여 로그인할 수 없습니다.

마법사에 액세스합니다

단계

1. 구성 > 액세스 제어 > *단일 로그인*을 선택합니다. Single Sign-On 페이지가 나타납니다.

> SSO 설정 구성 버튼이 비활성화된 경우 ID 공급자를 페더레이션 ID 소스로 구성했는지 확인하세요. "SSO(Single Sign-On)에 대한 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 ID 공급자에 대한 *페더레이션 서비스 이름*을 Active Directory 페더레이션 서비스(AD FS)에 표시된 대로 정확하게 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.

3. 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.

     CA 인증서를 변경하는 경우 즉시 "관리 노드에서 mgmt-API 서비스를 다시 시작합니다"그리드 관리자에서 성공적인 SSO를 테스트합니다.
4. *계속*을 선택하세요. 신뢰 당사자 식별자 제공 페이지가 나타납니다.

신뢰하는 당사자 식별자 제공

1. 선택한 SSO 유형에 따라 신뢰 당사자 식별자 제공 페이지에서 필드를 완성합니다.

Active Directory를 클릭합니다

a. StorageGRID 에 대한 *신뢰 당사자 식별자*를 지정합니다. 이 값은 AD FS에서 각 신뢰 당사자 신뢰에 사용하는 이름을 제어합니다.

   - 예를 들어 그리드에 관리자 노드가 하나만 있고 앞으로 관리자 노드를 더 추가할 계획이 없는 경우 또는 `StorageGRID` 를 입력합니다. `SG`
   - 그리드에 두 개 이상의 관리 노드가 포함된 경우 다음 문자열을 포함합니다. `[HOSTNAME]` 식별자에서. 예를 들어, `SG-[HOSTNAME]` . 이 문자열을 포함하면 노드의 호스트 이름을 기반으로 그리드의 각 관리 노드에 대한 신뢰 당사자 식별자를 보여주는 표가 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.

b. *저장하고 샌드박스 모드로 들어가기*를 선택하세요.

엔트라 **ID**

a. 엔터프라이즈 애플리케이션 섹션에서 StorageGRID 에 대한 *엔터프라이즈 애플리케이션 이름*을 지정합니다. 이 값은 Entra ID에서 각 엔터프라이즈 애플리케이션에 사용하는 이름을 제어합니다.

   - 예를 들어 그리드에 관리자 노드가 하나만 있고 앞으로 관리자 노드를 더 추가할 계획이 없는 경우 또는 `StorageGRID` 를 입력합니다. `SG`
   - 그리드에 두 개 이상의 관리 노드가 포함된 경우 다음 문자열을 포함합니다. `[HOSTNAME]` 식별자에서. 예를 들어, `SG-[HOSTNAME]` . 이 문자열을 포함하면 노드의 호스트 이름을 기반으로 시스템의 각 관리 노드에 대한 엔터프라이즈 애플리케이션 이름을 보여주는 표가 생성됩니다.

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

b. 다음 단계를 따르세요"Entra ID에서 엔터프라이즈 애플리케이션 만들기" 표에 나열된 각 관리 노드에 대한 엔터프라이즈 애플리케이션을 생성합니다.

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

d. 모든 관리 노드에 대한 페더레이션 메타데이터 URL을 복사하여 붙여넣은 후 *저장 및 샌드박스 모드 전환*을 선택합니다.

PingFederate(PingFederate)

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

   - 예를 들어 그리드에 관리자 노드가 하나만 있고 앞으로 관리자 노드를 더 추가할 계획이 없는 경우 또는 `StorageGRID` 를 입력합니다. `SG`
   - 그리드에 두 개 이상의 관리 노드가 포함된 경우 다음 문자열을 포함합니다. `[HOSTNAME]` 식별자에서. 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 접속을 생성해야 합니다. 각 관리 노드에 대해 SP를 연결하면 사용자가 관리자 노드에 안전하게 로그인할 수 있습니다.

b. 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>
```

c. *저장하고 샌드박스 모드로 들어가기*를 선택하세요.

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

구성을 저장하고 샌드박스 모드로 들어간 후, 선택한 SSO 유형에 대한 구성을 완료하고 테스트할 수 있습니다.

StorageGRID 필요한 만큼 샌드박스 모드를 유지할 수 있습니다. 하지만 연합 사용자와 로컬 사용자만 로그인할 수 있습니다.

Active Directory를 클릭합니다

단계

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

   테이블에 표시된 각 관리 노드에 대해 하나의 신뢰를 만들어야 합니다.

   자세한 내용은 을 "AD FS에서 기반 당사자 트러스트를 생성합니다"참조하십시오.

엔트라 **ID**

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 로그인*을 선택합니다.
   c. 해당 노드에 대한 SAML 메타데이터를 다운로드하고 저장합니다.
3. Azure Portal로 이동합니다.
4. 다음 단계를 따르세요"Entra ID에서 엔터프라이즈 애플리케이션 만들기" 각 관리 노드의 SAML 메타데이터 파일을 해당 Entra ID 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 로그인*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 노드의 SP 연결 ID(SSO 구성 페이지의 표에 표시됨)와 해당 관리 노드에 대해 다운로드한 SAML 메타데이터를 사용합니다.

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

테스트 구성

StorageGRID 시스템 전체에 대해 단일 로그인 사용을 강제로 적용하기 전에 각 관리 노드에 대해 단일 로그인 및 단일 로그아웃이 올바르게 구성되었는지 확인하세요.

Active Directory를 클릭합니다

단계

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

   URL은 * 페더레이션 서비스 이름 * 필드에 입력한 값에서 파생됩니다.

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

엔트라 **ID**

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

   링크를 한 번에 하나씩 선택하여 테스트합니다.

2. 통합 사용자의 자격 증명을 입력합니다.
   - SSO 로그인 및 로그아웃 작업이 성공하면 성공 메시지가 나타납니다.
   - 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. SSO 구성 마법사의 테스트 구성 단계에서 *SSO 사용*을 선택합니다.
2. 경고 메시지를 검토하고 *SSO 사용*을 선택하세요.

   이제 Single Sign-On이 활성화되었습니다. Single Sign-On 페이지가 나타나고 방금 구성한 SSO에 대한 세부 정보가 포함됩니다.

3. 구성을 편집하려면 *편집*을 선택하세요.
4. Single Sign-On을 비활성화하려면 *SSO 비활성화*를 선택하세요.

Azure Portal을 사용하고 Entra ID에 액세스하는 데 사용하는 것과 동일한 컴퓨터에서 StorageGRID에 액세스하는 경우 Azure Portal 사용자가 권한이 있는 StorageGRID 사용자(StorageGRID 로 가져온 페더레이션 그룹의 사용자)인지 확인하거나 StorageGRID 에 로그인을 시도하기 전에 Azure Portal에서 로그아웃하세요.

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.
- 당신은 가지고있다"샌드박스 모드로 들어갔습니다" 그리드 관리자에서.
- 시스템의 각 관리 노드에 대한 정규화된 도메인 이름(또는 IP 주소)과 신뢰 당사자 식별자를 알고 있습니다. 이러한 값은 StorageGRID SSO 구성 페이지의 관리 노드 세부 정보 표에서 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"
   ```

   - 의 경우 *Admin_Node_Identifier* 단일 사인온 페이지에 표시된 대로 관리자 노드의 종속 당사자 식별자를 입력합니다. `SG-DC1-ADM1`예를 들어,
   - 의 경우 *Admin_Node_FQDN* 동일한 관리자 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 * objectGUID를 이름 ID * 로, * UPN을 이름 ID * 로 지정합니다.
   f. 특성 저장소의 경우 * Active Directory * 를 선택합니다.

g. Mapping 테이블의 LDAP Attribute 열에서 * objectGUID * 를 입력하거나 * User-Principal-Name * 을 선택합니다.

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. 완료되면 StorageGRID 로 돌아가서"모든 신뢰 당사자 트러스트를 테스트합니다" 올바르게 구성되었는지 확인하세요.

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`

의 경우 *Admin_Node_FQDN* 동일한 관리자 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. `SG-DC1-ADM1`예를 들어,

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 * objectGUID를 이름 ID * 로, * UPN을 이름 ID * 로 지정합니다.

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

f. Mapping 테이블의 LDAP Attribute 열에서 * objectGUID * 를 입력하거나 * User-Principal-Name * 을 선택합니다.

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. 완료되면 StorageGRID 로 돌아가서"모든 신뢰 당사자 트러스트를 테스트합니다" 올바르게 구성되었는지 확인하세요.

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. `SG-DC1-ADM1`예를 들어,

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`

의 경우 *Admin_Node_FQDN* 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

의 경우 *Admin_Node_Identifier* 단일 사인온 페이지에 표시된 대로 관리자 노드의 종속 당사자 식별자를 입력합니다. `SG-DC1-ADM1`예를 들어,

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 * objectGUID를 이름 ID * 로, * UPN을 이름 ID * 로 지정합니다.

   c. 특성 저장소의 경우 * Active Directory * 를 선택합니다.
   d. Mapping 테이블의 LDAP Attribute 열에서 * objectGUID * 를 입력하거나 * User-Principal-Name * 을 선택합니다.
   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`

   의 경우 *Admin_Node_FQDN* 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 관리자 노드에 로그인하고 관리자 노드의 디렉터리로 이동하여 `/var/local/mgmt-api` 인증서 파일을 추가합니다 `custom-server.crt`.

관리자 노드의 기본 인증서 (`server.crt`사용)은 사용하지 않는 것이 좋습니다. 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. 완료되면 StorageGRID 로 돌아가서"모든 신뢰 당사자 트러스트를 테스트합니다" 올바르게 구성되었는지 확인하세요.

Entra ID에서 엔터프라이즈 애플리케이션 만들기

Entra ID를 사용하면 시스템의 각 관리 노드에 대한 엔터프라이즈 애플리케이션을 만들 수 있습니다.

시작하기 전에

- StorageGRID 에 대한 단일 로그인 구성을 시작했으며 SSO 유형으로 *Entra ID*를 선택했습니다.
- 당신은 가지고있다"샌드박스 모드로 들어갔습니다" 그리드 관리자에서.
- 시스템의 각 관리 노드에는 *엔터프라이즈 애플리케이션 이름*이 있습니다. SSO 구성 페이지의 관리 노드 세부 정보 표에서 이러한 값을 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.

- Entra ID에서 엔터프라이즈 애플리케이션을 만든 경험이 있습니다.
- 활성화된 구독이 있는 Entra ID 계정이 있습니다.
- Entra ID 계정에는 글로벌 관리자, 클라우드 애플리케이션 관리자, 애플리케이션 관리자 또는 서비스 주체 소유자라는 역할 중 하나가 있습니다.

엔트라 ID 접속

단계

1. 에 "Azure 포털"로그인합니다.
2. 로 이동 "엔트라 ID" .
3. 을 "엔터프라이즈 애플리케이션"선택합니다.

엔터프라이즈 애플리케이션을 생성하고 StorageGRID SSO 구성을 저장합니다

StorageGRID 에서 Entra ID에 대한 SSO 구성을 저장하려면 Entra ID를 사용하여 각 관리 노드에 대한 엔터프라이즈 애플리케이션을 만들어야 합니다. Entra ID에서 페더레이션 메타데이터 URL을 복사하여 SSO 구성 페이지의 해당 페더레이션 메타데이터 **URL** 필드에 붙여넣습니다.

단계

1. 각 관리 노드에 대해 다음 단계를 반복합니다.
   a. Entra ID Enterprise 애플리케이션 창에서 *새 애플리케이션*을 선택합니다.
   b. 사용자 정의 응용 프로그램 만들기 * 를 선택합니다.
   c. 이름에는 SSO 구성 페이지의 관리 노드 세부 정보 표에서 복사한 *엔터프라이즈 애플리케이션 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. 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 모든 변경을 한 후 SSO 구성 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 로그인*을 선택합니다.
   c. 버튼을 선택하여 해당 Admin Node에 대한 SAML 메타데이터를 다운로드합니다.
   d. Entra ID에 업로드할 파일을 저장합니다.

각 엔터프라이즈 애플리케이션에 **SAML** 메타데이터를 업로드합니다

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

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. "각 응용 프로그램을 테스트하세요" .

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.
- 당신은 가지고있다"샌드박스 모드로 들어갔습니다" 그리드 관리자에서.
- 시스템의 각 관리 노드에는 * SP 연결 ID*가 있습니다. 이러한 값은 SSO 구성 페이지의 관리 노드 세부 정보 표에서 찾을 수 있습니다.
- 시스템의 각 관리 노드에 대해 * SAML 메타데이터 * 를 다운로드했습니다.
- PingFederate Server에서 SP 연결을 생성하는 경험이 있습니다.
- PingFederate Server용 이 "관리자 참조 안내서"있습니다. PingFederate 설명서는 자세한 단계별 지침과 설명을 제공합니다.
- 당신은 가지고있다"관리자 권한" PingFederate 서버용.

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. StorageGRID에서 사용한 값을 "ID 페더레이션을 구성하는 중입니다"사용합니다.

- * 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. 선택하세요암호 자격 증명 유효성 검사기가 있습니다 당신이 창조했습니다.
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 추가 SP 접속을 생성합니다 이동하여 필요한 추가 연결을 만듭니다.

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. 관리 노드의 SSO 구성 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 **SSO**를 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 사용하지 않는 를 제거합니다 `urn:oid`.

어댑터 인스턴스를 매핑합니다

단계

1. 인증 소스 매핑 탭에서 * 새 어댑터 인스턴스 매핑 * 을 선택합니다.
2. 어댑터 인스턴스 탭에서 작성한 을 어댑터 인스턴스선택합니다.
3. 매핑 방법 탭에서 * 데이터 저장소에서 추가 특성 검색 * 을 선택합니다.
4. 특성 원본 및 사용자 조회 탭에서 * 특성 원본 추가 * 를 선택합니다.
5. 데이터 저장소 탭에서 설명을 입력하고 추가한 을 데이터 저장소선택합니다.
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 * 또는 * userPrincipalName * 속성 중 하나를 검색하여 추가합니다.

7. LDAP 바이너리 특성 인코딩 형식 탭에서 * objectGUID * 특성에 대해 * Base64 * 를 선택합니다.
8. LDAP 필터 탭에서 * sAMAccountName=${username} * 을 입력합니다.
9. 특성 계약 이행 탭의 소스 드롭다운에서 * LDAP (attribute) * 를 선택하고 값 드롭다운에서 * objectGUID * 또는 * userPrincipalName * 을 선택합니다.
10. 특성 소스를 검토한 후 저장합니다.
11. Failsave 특성 소스 탭에서 * SSO 트랜잭션 중단 * 을 선택합니다.
12. 요약을 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. 어설션 소비자 서비스 URL 탭에서 StorageGRID SAML 메타데이터(* 바인딩 및 끝점 URL의 경우 * POST *)에서 가져온 기본값을 수락합니다. `/api/saml-response`
3. SLO 서비스 URL 탭에서 StorageGRID SAML 메타데이터(* 바인딩 및 끝점 URL의 경우 * 리디렉션 *)에서 가져온 기본값을 그대로 `/api/saml-logout` 사용합니다.
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. 선택하세요서명 인증서 귀하가 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 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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"

단계

1. 구성 > 액세스 제어 > *단일 로그인*을 선택합니다.

   단일 사인온 페이지가 나타납니다.

2. *SSO 비활성화*를 선택하세요.
3. 예 * 를 선택합니다.

   로컬 사용자가 로그인할 수 있음을 나타내는 경고 메시지가 나타납니다.

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

한 관리 노드에 대해 SSO를 일시적으로 비활성화하고 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

- 있습니다. "특정 액세스 권한"
- `Passwords.txt`파일이 있습니다.
- 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. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

      루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

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 로그인*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

상표 정보