ID 페더레이션 사용

StorageGRID 11.5

NetApp
April 11, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/storagegrid-115/tenant/guidelines-for-configuring-openldap-server.html on April 11, 2024. Always check docs.netapp.com for the latest.

목차

ID 페더레이션 사용

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

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

통합 ID 소스 구성

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

필요한 것

- 지원되는 브라우저를 사용하여 테넌트 관리자에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.
- ID 공급자로 Active Directory, OpenLDAP 또는 Oracle Directory Server를 사용하고 있어야 합니다. 목록에 없는 LDAP v3 서비스를 사용하려면 기술 지원 부서에 문의해야 합니다.
- LDAP 서버와의 통신에 TLS(Transport Layer Security)를 사용하려는 경우 ID 공급자는 TLS 1.2 또는 1.3을 사용해야 합니다.

이 작업에 대해

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

> This tenant account uses the LDAP server that is configured for the Grid Manager. Contact the grid administrator for information or to change this setting.

단계

1. 액세스 관리 * > * ID 페더레이션 * 을 선택합니다.
2. ID 페더레이션 사용 * 을 선택합니다.
3. LDAP 서비스 유형 섹션에서 * Active Directory *, * OpenLDAP * 또는 * 기타 * 를 선택합니다.

   OpenLDAP * 를 선택한 경우 OpenLDAP 서버를 구성합니다. OpenLDAP 서버 구성 지침을 참조하십시오.

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

4. 기타 * 를 선택한 경우 LDAP 속성 섹션의 필드를 작성합니다.
   - * 사용자 고유 이름 *: LDAP 사용자의 고유 식별자가 포함된 속성의 이름입니다. 이 속성은 과 같습니다 `sAMAccountName` Active Directory 및 의 경우 `uid` OpenLDAP의 경우. Oracle Directory Server를 구성하는 경우 를 입력합니다 `uid`.

- * 사용자 UUID *: LDAP 사용자의 영구 고유 식별자가 포함된 특성의 이름입니다. 이 속성은 과 같습니다 `objectGUID` Active Directory 및 의 경우 `entryUUID` OpenLDAP의 경우. Oracle Directory Server를 구성하는 경우 를 입력합니다 `nsuniqueid`. 지정된 속성에 대한 각 사용자의 값은 16바이트 또는 문자열 형식의 32자리 16진수 숫자여야 하며, 하이픈은 무시됩니다.
- * 그룹 고유 이름 *: LDAP 그룹의 고유 식별자가 포함된 속성의 이름입니다. 이 속성은 과 같습니다 `sAMAccountName` Active Directory 및 의 경우 `cn` OpenLDAP의 경우. Oracle Directory Server를 구성하는 경우 를 입력합니다 `cn`.
- * 그룹 UUID *: LDAP 그룹의 영구 고유 식별자가 포함된 특성의 이름입니다. 이 속성은 과 같습니다 `objectGUID` Active Directory 및 의 경우 `entryUUID` OpenLDAP의 경우. Oracle Directory Server를 구성하는 경우 를 입력합니다 `nsuniqueid`. 지정된 속성에 대한 각 그룹의 값은 16바이트 또는 문자열 형식의 32자리 16진수 숫자여야 하며, 하이픈은 무시됩니다.

5. LDAP 서버 구성 섹션에서 필요한 LDAP 서버 및 네트워크 연결 정보를 입력합니다.
   - * 호스트 이름 *: LDAP 서버의 서버 호스트 이름 또는 IP 주소입니다.
   - * 포트 *: LDAP 서버에 연결하는 데 사용되는 포트입니다. STARTTLS의 기본 포트는 389이고 LDAPS의 기본 포트는 636입니다. 그러나 방화벽이 올바르게 구성된 경우 모든 포트를 사용할 수 있습니다.
   - * 사용자 이름 *: LDAP 서버에 연결할 사용자의 DN(고유 이름)의 전체 경로입니다. Active Directory의 경우 아래쪽 로그온 이름 또는 사용자 기본 이름을 지정할 수도 있습니다.

     지정된 사용자는 그룹 및 사용자를 나열하고 다음 속성에 액세스할 수 있는 권한이 있어야 합니다.

     - `sAMAccountName` 또는 `uid`
     - `objectGUID`, `entryUUID`, 또는 `nsuniqueid`
     - `cn`
     - `memberOf` 또는 `isMemberOf`
   - * 암호 *: 사용자 이름과 연결된 암호입니다.
   - * Group base DN *: 그룹을 검색할 LDAP 하위 트리에 대한 DN(고유 이름)의 전체 경로입니다. Active Directory 예제(아래)에서 고유 이름이 기본 DN(DC=StorageGrid, DC=example, DC=com)과 관련된 모든 그룹을 통합 그룹으로 사용할 수 있습니다.

     그룹 고유 이름 * 값은 * 그룹 기본 DN * 내에서 고유해야 합니다.
   - * 사용자 기본 DN *: 사용자를 검색할 LDAP 하위 트리의 고유 이름(DN)의 전체 경로입니다.

     사용자 고유 이름 * 값은 * 사용자 기본 DN * 내에서 고유해야 합니다.

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

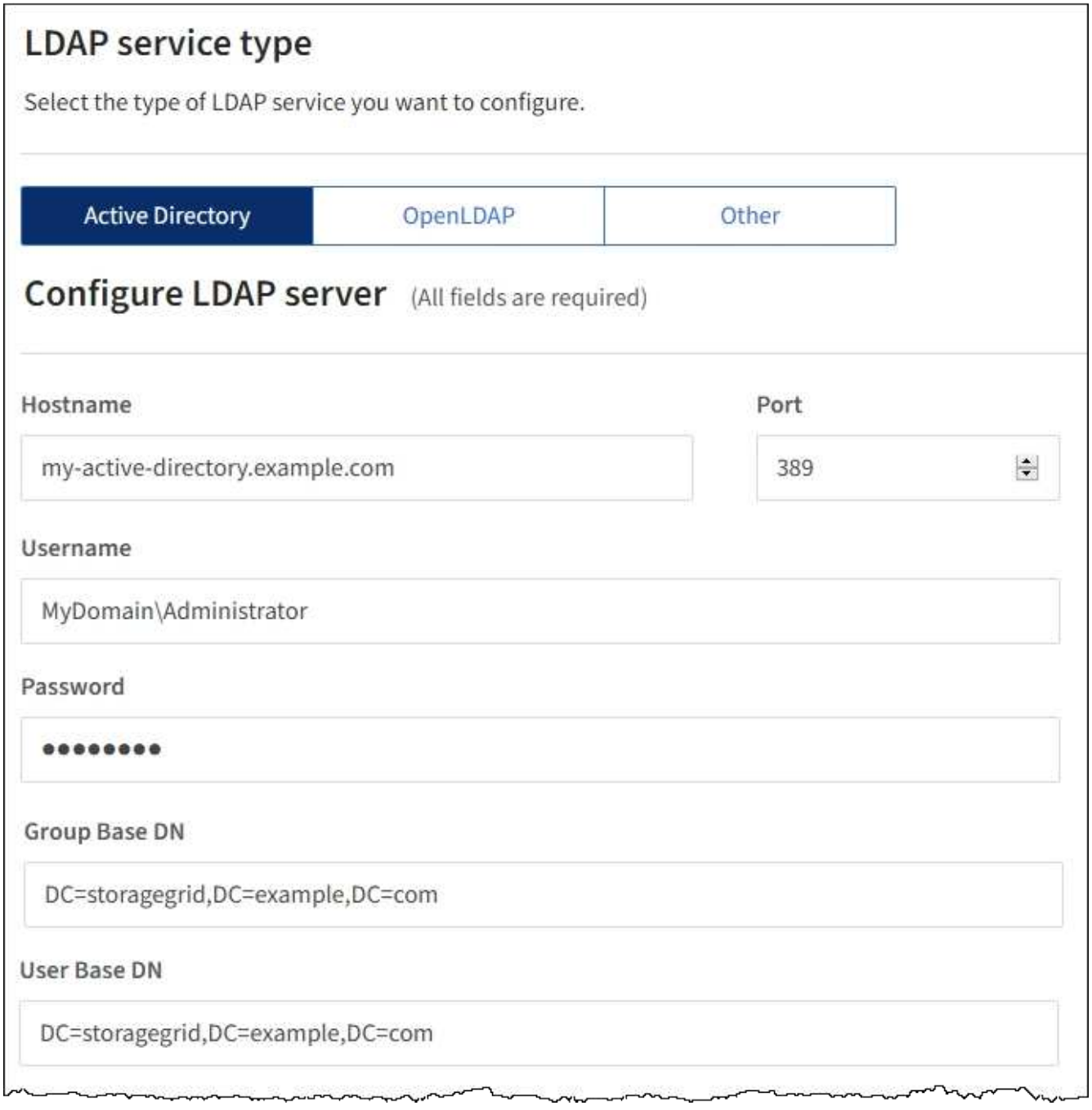
     Active Directory 서버가 LDAP 서명을 적용하는 경우에는 이 옵션이 지원되지 않습니다. STARTTLS 또는 LDAPS를 사용해야 합니다.

7. STARTTLS 또는 LDAPS를 선택한 경우 연결 보안에 사용되는 인증서를 선택합니다.
   - * 운영 체제 CA 인증서 사용 *: 운영 체제에 설치된 기본 CA 인증서를 사용하여 연결을 보호합니다.
   - * 사용자 지정 CA 인증서 사용 *: 사용자 지정 보안 인증서를 사용합니다.

     이 설정을 선택한 경우 사용자 지정 보안 인증서를 복사하여 CA 인증서 텍스트 상자에 붙여 넣습니다.
8. LDAP 서버에 대한 연결 설정을 확인하려면 * 연결 테스트 * 를 선택합니다.

   연결이 유효한 경우 페이지의 오른쪽 상단에 확인 메시지가 나타납니다.
9. 연결이 유효하면 * 저장 * 을 선택합니다.

   다음 스크린샷은 Active Directory를 사용하는 LDAP 서버의 구성 값 예를 보여 줍니다.



관련 정보

"테넌트 관리 권한"

"OpenLDAP 서버 구성 지침"

OpenLDAP 서버 구성 지침

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

MemberOf 및 구체화 오버레이

MemberOf 및 구체화 오버레이를 활성화해야 합니다. 자세한 내용은 OpenLDAP용 관리자 안내서 에서 역방향 그룹 구성원 유지 관리 지침을 참조하십시오.

인덱싱

지정된 인덱스 키워드를 사용하여 다음 OpenLDAP 속성을 구성해야 합니다.

```
olcDbIndex: objectClass eq
olcDbIndex: uid eq,pres,sub
olcDbIndex: cn eq,pres,sub
olcDbIndex: entryUUID eq
```

또한 최적의 성능을 위해 사용자 이름 도움말에 언급된 필드를 인덱싱해야 합니다.

OpenLDAP용 관리자 안내서 에서 역방향 그룹 구성원 유지 관리에 대한 정보를 참조하십시오.

ID 소스와 동기화 수행

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

필요한 것

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

단계

1. 액세스 관리 * > * ID 페더레이션 * 을 선택합니다.

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

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

2. 동기화 서버 * 를 선택합니다.

   동기화가 성공적으로 시작되었음을 나타내는 확인 메시지가 표시됩니다.

관련 정보

"테넌트 관리 권한"

ID 페더레이션을 사용하지 않도록 설정합니다

이 테넌트에 대해 ID 페더레이션 서비스를 구성한 경우 테넌트 그룹 및 사용자에 대한 ID 페더레이션을 일시적으로 또는 영구적으로 비활성화할 수 있습니다. ID 페더레이션을 비활성화하면 StorageGRID 시스템과 ID 소스 간에 통신이 이루어지지 않습니다. 그러나 구성한 설정은 그대로 유지되므로 나중에 ID 페더레이션을 쉽게 다시 활성화할 수 있습니다.

필요한 것

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

이 작업에 대해

ID 페더레이션을 사용하지 않도록 설정하기 전에 다음 사항을 확인해야 합니다.

- 페더레이션 사용자는 로그인할 수 없습니다.
- 현재 로그인한 페더레이션 사용자는 세션이 만료될 때까지 테넌트 계정에 대한 액세스 권한을 유지하지만 세션이 만료된 후에는 로그인할 수 없습니다.
- StorageGRID 시스템과 ID 소스 간의 동기화는 수행되지 않습니다.

단계

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

관련 정보

"테넌트 관리 권한"

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄됨 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 라이센스와 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 라이센스도 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 라이센스를 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 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

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