UCS Manager에서 LDAP 구성

목차

소개

이 문서에서는 의 LDAP 프로토콜을 통한 원격 서버 액세스를 위한 컨피그레이션에 대해 설명합니다. **Unified Computing System Manager Domain (UCSM).**

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- **Unified Computing System Manager Domain (UCSM)**
- 로컬 및 원격 인증
- **Lightweight Directory Access Protocol (LDAP)**
- **Microsoft Active Directory (MS-AD)**

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- **Cisco UCS 6454 Fabric Interconnect**
- UCSM 버전 4.0(4k)
- **Microsoft Active Directory (MS-AD)**

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든

명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

Lightweight Directory Access Protocol (LDAP) 는 사용자와 IT 리소스에 대한 액세스 권한을 안전하게 관리하는 디렉토리 서비스를 위해 개발된 핵심 프로토콜 중 하나입니다.

대부분의 디렉토리 서비스는 Kerberos, SAML, RADIUS, SMB, Oauth 등과 같은 추가 프로토콜을 사용할 수도 있지만 현재 여전히 LDAP를 사용합니다.

구성

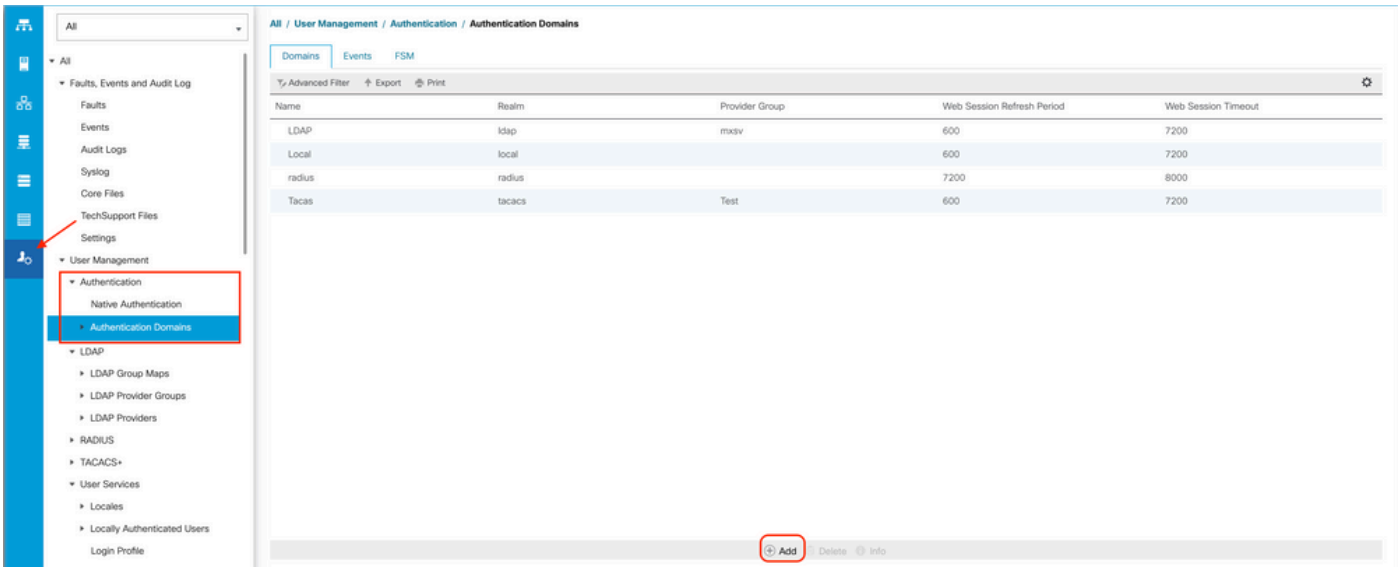
시작하기 전에

로그인**Cisco UCS Manager** GUI관리할 수 있습니다.

로컬 인증 도메인 생성

1단계. 의 **Navigation** 창에서 **Admin** 탭을 클릭합니다.

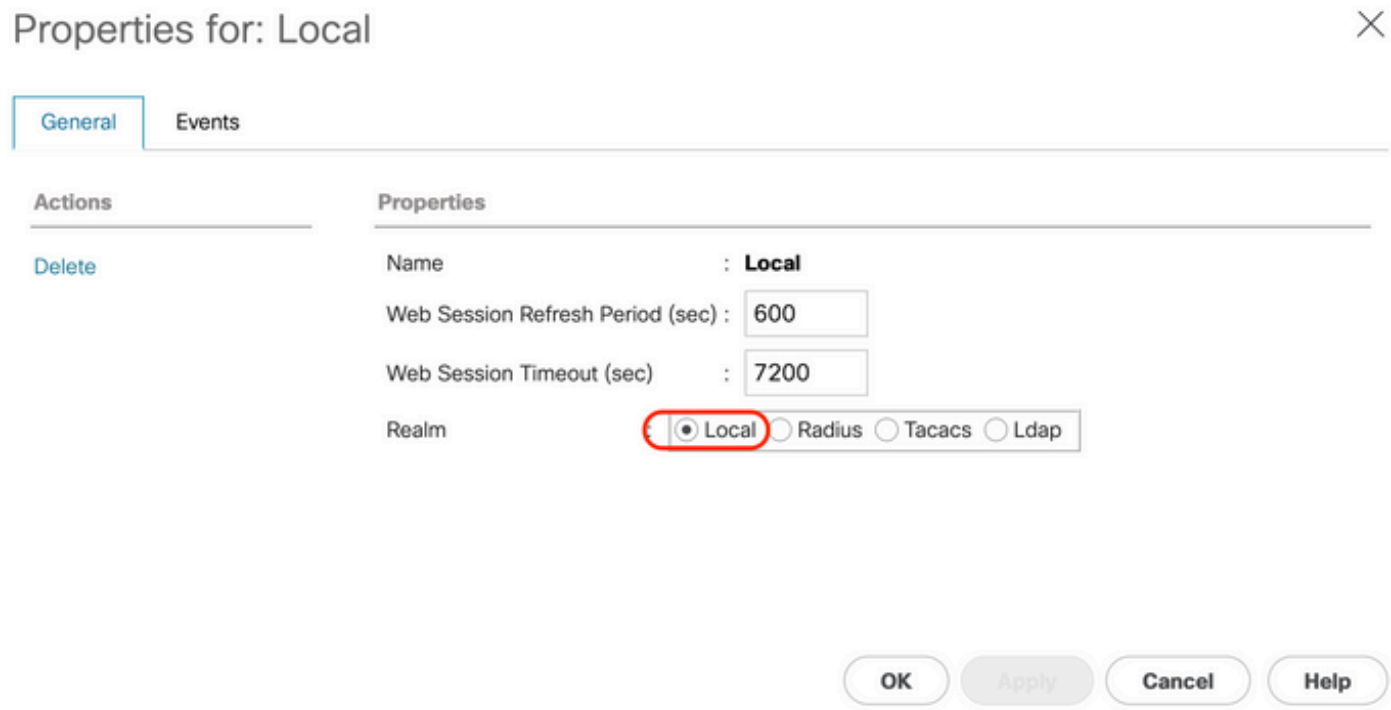
2단계. 에 **Admin** 탭, 확장 **All > User Management > Authentication**



3단계. 마우스 오른쪽 단추 클릭 **Authentication Domains** 및 선택 **Create a Domain.**

4단계. 의 경우 **Name** 필드, 유형 **Local.**

5단계. 의 경우 **Realm**을 클릭하고 **Local** 라디오 버튼.



6단계. 클릭 **OK**.

LDAP 제공자 생성

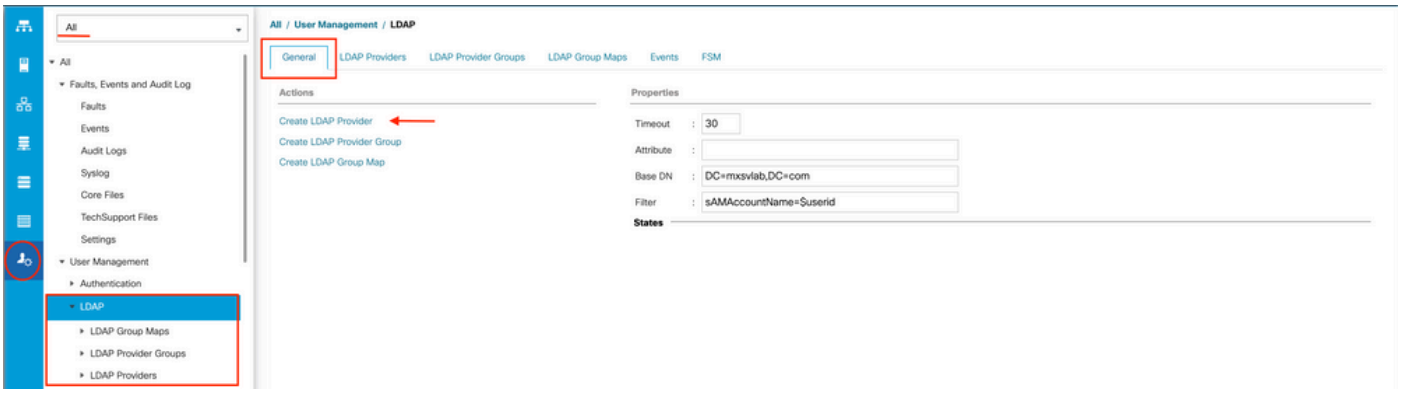
이 샘플 컨피그레이션에는 SSL을 사용하여 LDAP를 구성하는 단계가 포함되어 있지 않습니다.

1단계.의 **Navigation** 창에서 **Admin** 탭을 클릭합니다.

2단계. 에 **Admin** 탭, 확장 **All > User Management > LDAP.**

3단계. 의 **Work** 창에서 **General** 탭을 클릭합니다.

4단계. 의 **Actions** 영역을 클릭하고 **Create LDAP Provider**



5단계. 의 **Create LDAP Provider** 마법사 페이지에서 적절한 정보를 입력합니다.

- 의 **Hostname**필드에 AD 서버의 IP 주소 또는 호스트 이름을 입력합니다.
- 의 **Order** 필드, 수락 **lowest-available** 기본값.
- 의 **BindDN** 필드를 클릭하고 AD 컨피그레이션에서 BindDN을 복사하여 붙여넣습니다.

이 샘플 컨피그레이션의 경우 BindDN 값은 **CN=ucsbind,OU=CiscoUCS,DC=mxsvlab,DC=com**입니다.

- 의 **BaseDN** 필드를 클릭하고 AD 컨피그레이션에서 BaseDN을 복사하여 붙여넣습니다.

이 샘플 컨피그레이션의 경우 BaseDN 값은 **DC=mxsvlab,DC=com입니다.**

- 에서 나가십시오. **Enable SSL** 확인란을 선택하지 않았습니다.
- 의 **Port** 필드에 389 기본값을 적용합니다.
- 의 **Filter** 필드, AD 컨피그레이션에서 필터 특성을 복사하여 붙여넣습니다.

Cisco UCS는 필터 값을 사용하여 사용자 이름(로그온 화면에서 제공)이 **Cisco UCS Manager**)이(가) AD에 있습니다.

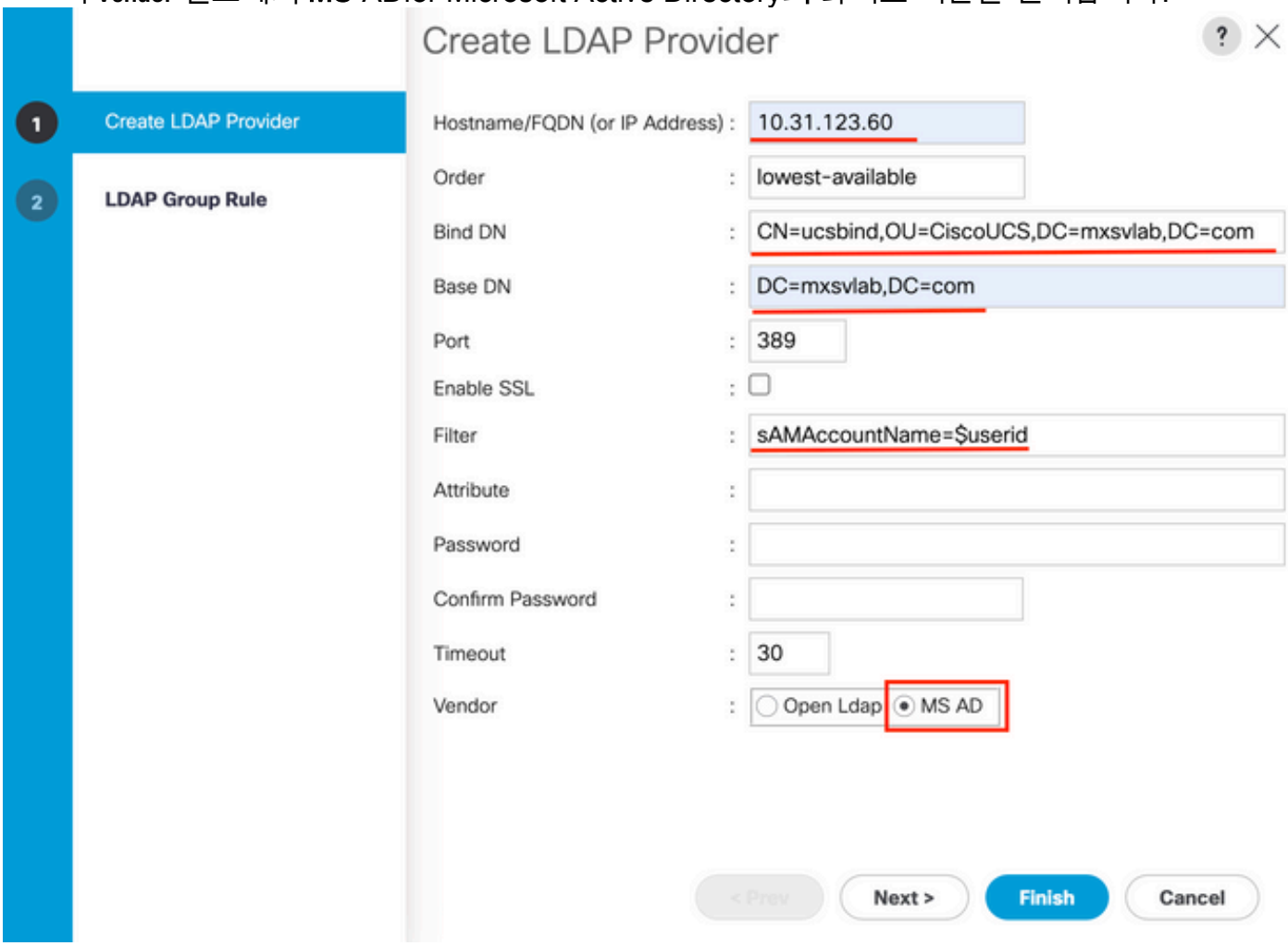
이 샘플 컨피그레이션의 경우 필터 값은 **sAMAccountName=$userid**입니다. 여기서 $userid는 **user name** 를 입력하여 **Cisco UCS Manager** 로그인 화면.

- 에서 나가십시오. **Attribute** 필드가 비어 있습니다.
- 의 **Password** 필드에 AD에 구성된 ucsbind 계정의 비밀번호를 입력합니다.

Firepower Threat Defense의 **Create LDAP Provider wizard** 비밀번호를 재설정하려면 비밀번호 필드가 비어 있으면 경계하지 마십시오.

이 **Set: yes** password(비밀번호) 필드 옆에 표시되는 메시지는 비밀번호가 설정되었음을 나타냅니다 .

- 의 **Confirm Password** 필드에 AD에 구성된 ucsbind 계정의 비밀번호를 다시 입력합니다.
- 의 **Timeout** 필드, 수락 기본값 30입니다.
- 의 **Vendor** 필드에서 **MS-ADfor Microsoft Active Directory의** 라디오 버튼을 선택합니다.



6단계. 클릭 **Next**

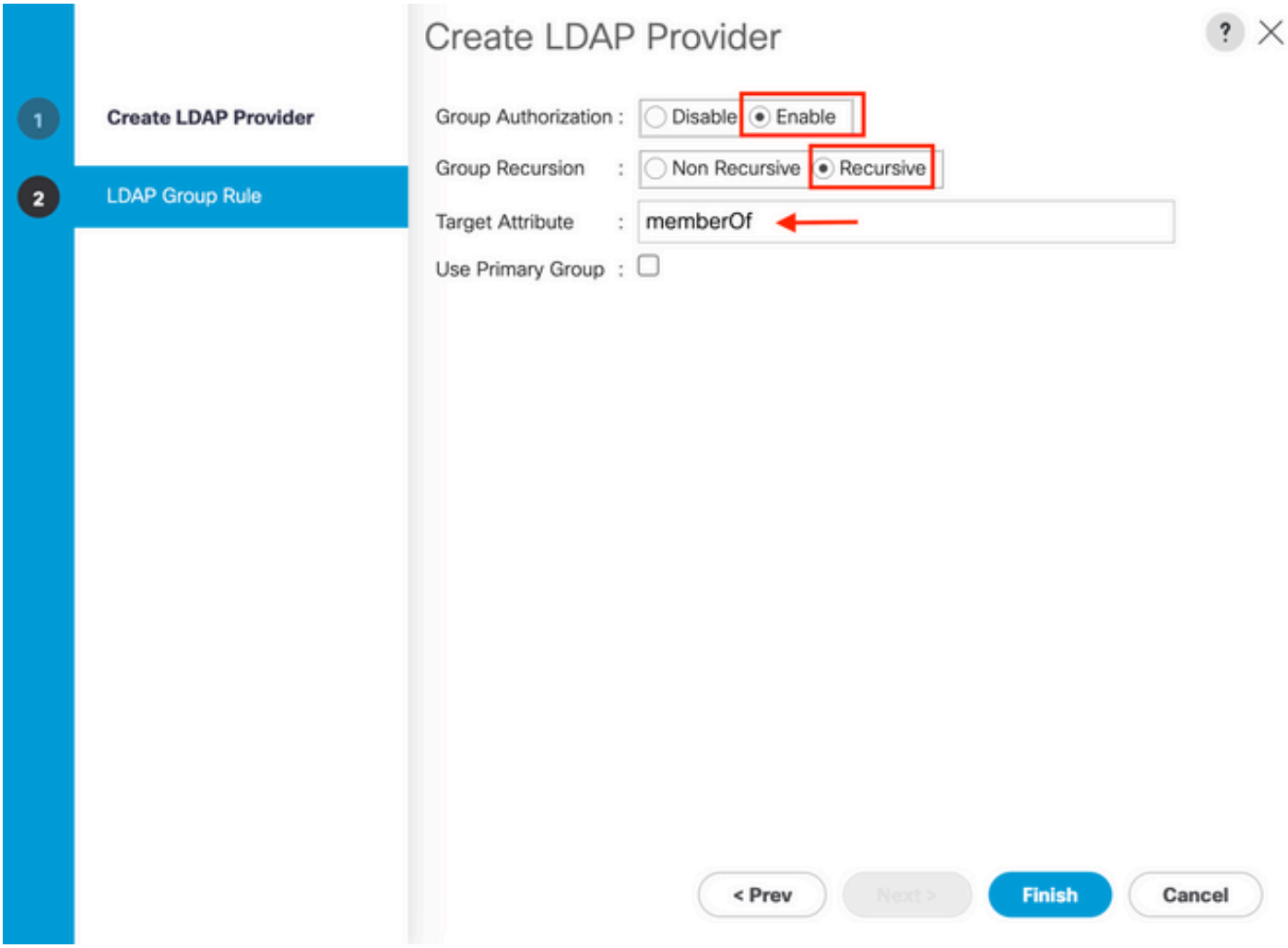
LDAP 그룹 규칙 컨피그레이션

1단계. 에**LDAP Group Rule** 마법사 페이지에서 다음 필드를 완료합니다.

- 의 경우 **Group Authentication** 필드를 클릭하고 **Enable** 라디오 버튼.
- 의 경우 **Group Recursion** 필드를 클릭하고 **Recursive** 라디오 버튼. 이렇게 하면 시스템에서 사용자를 찾을 때까지 수준별로 검색을 계속 아래로 진행할 수 있습니다.

이 **Group Recursion** 다음으로 설정됨 **Non-Recursive**에서는 UCS를 첫 번째 레벨의 검색으로 제한합니다. 단, 검색에서 적격 사용자를 찾을 수는 없습니다.

- 의 **Target Attribute** 필드, 수락**memberOf** 기본값.



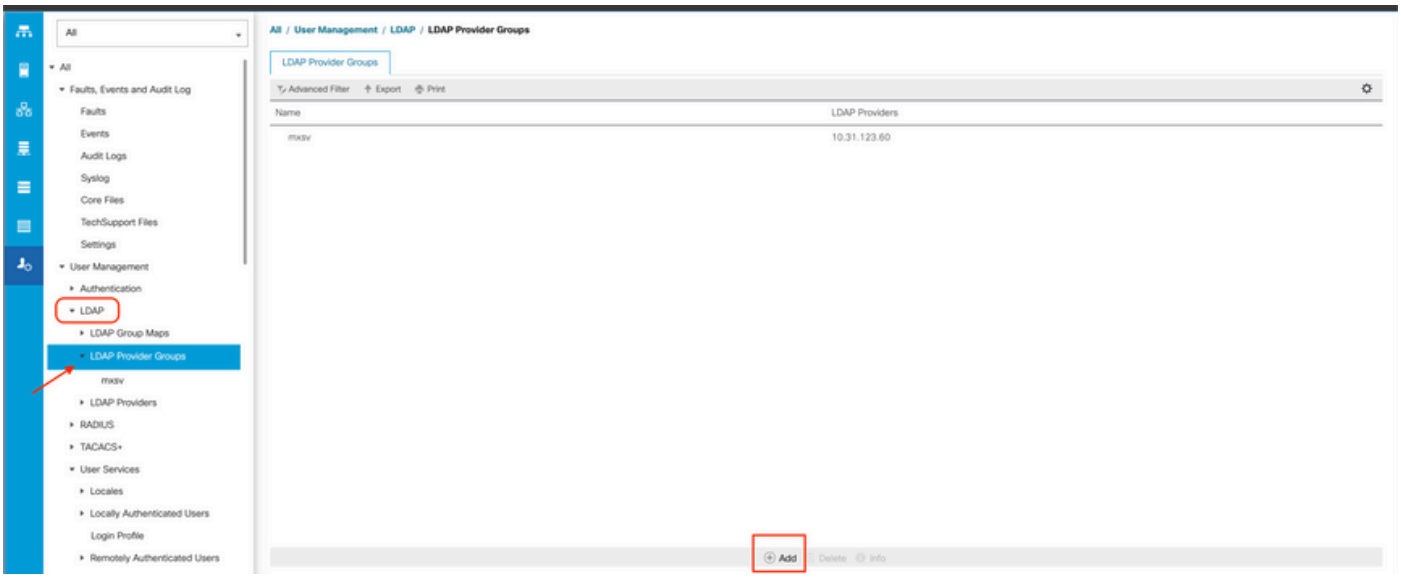
2단계. 클릭 **Finish**.

> **참고**: 실제 시나리오에서는 여러 LDAP 제공자가 있을 가능성이 높습니다. 여러 LDAP 제공자의 경우 각 LDAP 제공자에 대해 LDAP 그룹 규칙을 구성하는 단계를 반복합니다. 그러나 이 샘플 컨피그레이션에는 LDAP 제공자가 하나만 있으므로 이 작업은 필요하지 않습니다.

AD 서버의 IP 주소는 Navigation(탐색) 창의 LDAP>**LDAP Providers(LDAP 제공자)** 아래**에 표시됩니다**.

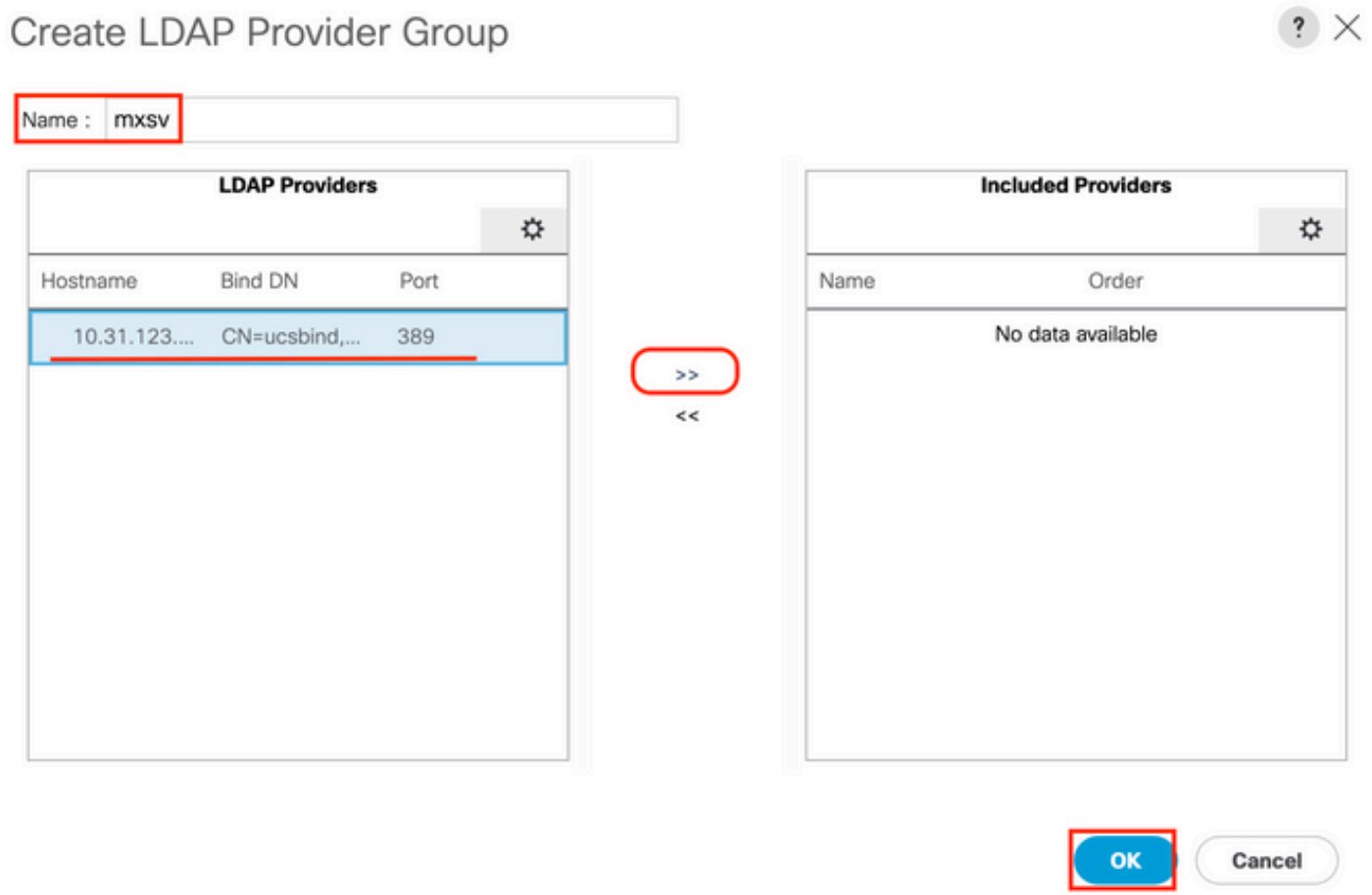
LDAP 제공자 그룹 생성

1단계. Navigation(탐색) 창에서 마우스 오른쪽 단추를 클릭합니다. **LDAP Provider Groups** 및 선택 **Create LDAP Provider Group**.



2단계. 의 **Create LDAP Provider Group** 대화 상자에서 정보를 적절히 채웁니다.

- 의 **Name** 필드에 다음과 같은 그룹의 고유한 이름을 입력합니다. **LDAP Providers.**
- 의 **LDAP Providers** 테이블에서 AD 서버의 IP 주소를 선택합니다.
- **>> 버튼을 클릭하여 AD 서버를 Included Providers 테이블.**



3단계. OK(확인)를 클릭합니다.

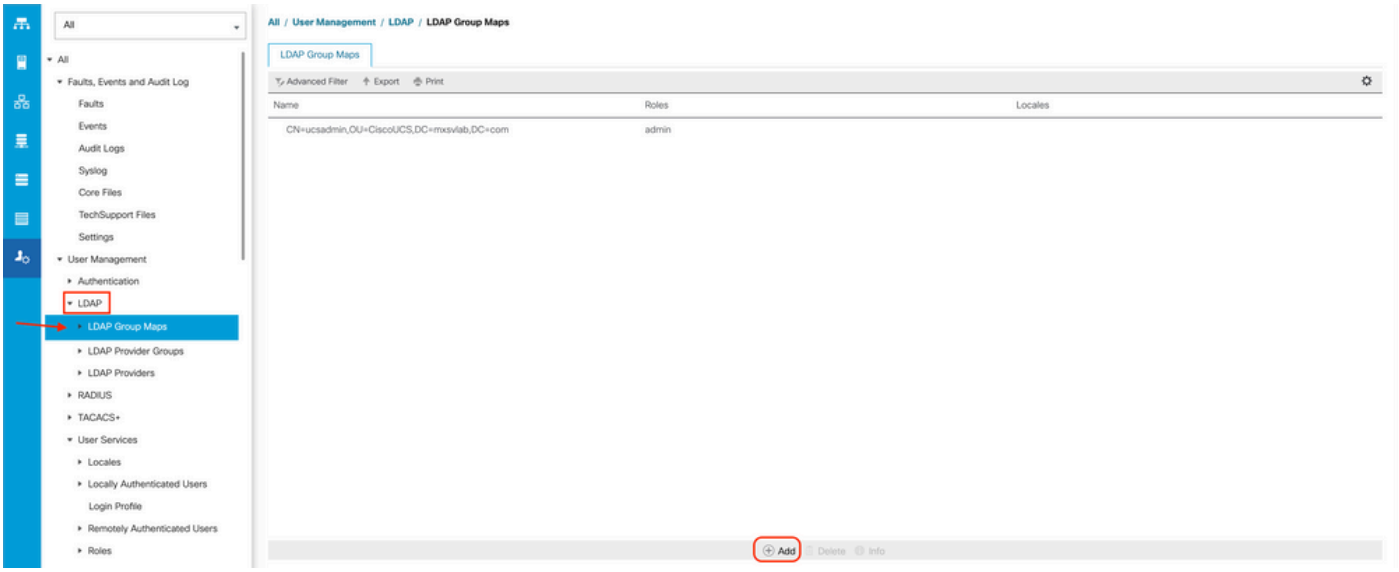
제공 기관 그룹이 **LDAP Provider Groups** 폴더.

LDAP 그룹 맵 생성

1단계. 탐색 창에서 **Admin**탭을 클릭합니다.

2단계. 에 **Admin** 탭, 확장 **All > User Management > LDAP.**

3단계. 작업 창에서 만들기를 클릭합니다 **LDAP Group Map.**



4단계. 의 **Create LDAP Group Map** 대화 상자에서 정보를 적절히 채웁니다.

- 의 **LDAP Group DN** 필드에 LDAP 그룹의 AD 서버 컨피그레이션 섹션에 있는 값을 복사하여 붙여 넣습니다.

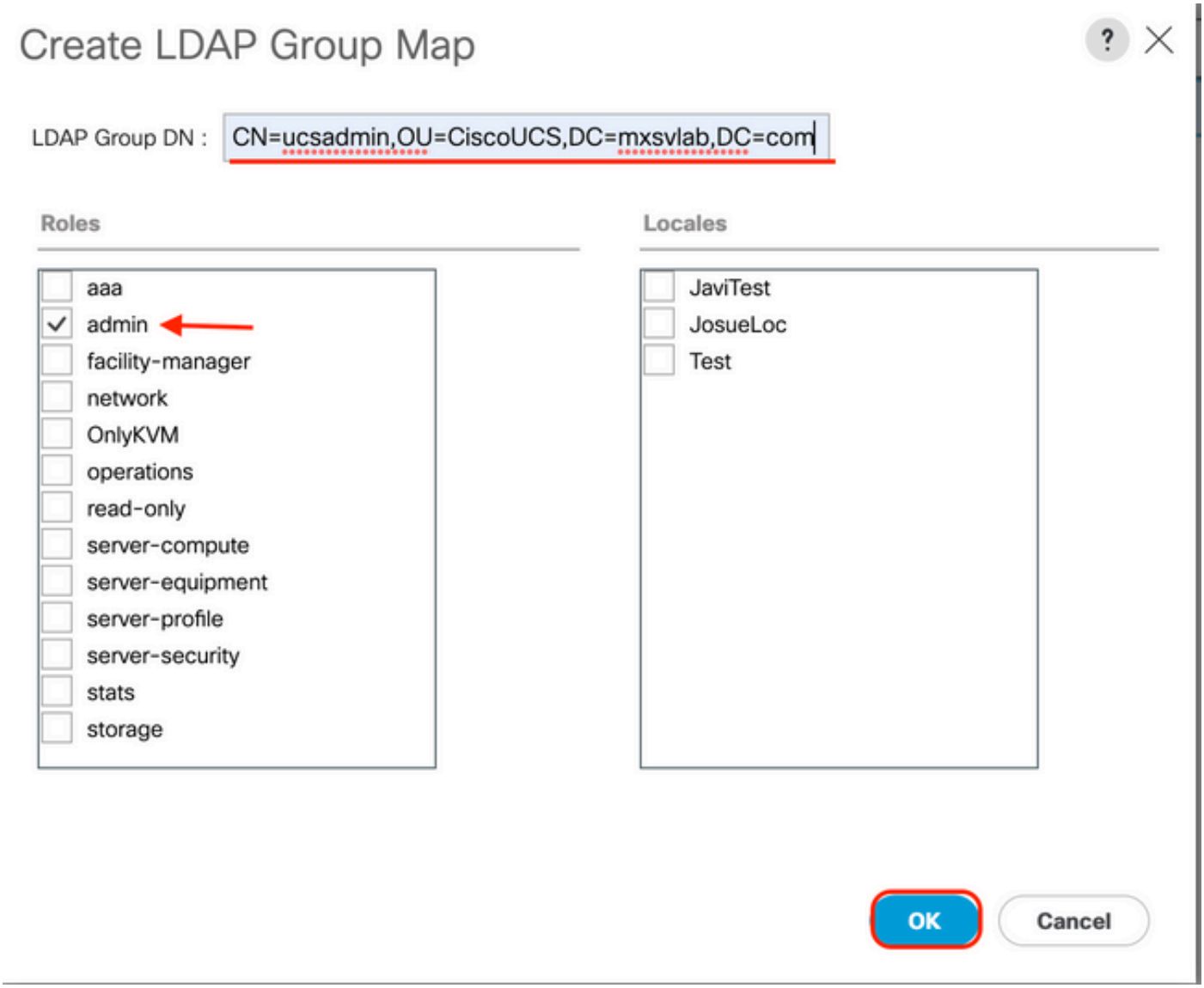
이 단계에서 요청된 LDAP 그룹 DN 값은 UCS Groups(UCS 그룹) 아래의 AD에서 생성한 각 그룹의 DN에 매핑됩니다.

따라서 Cisco UCS Manager에 입력한 그룹 DN 값은 AD 서버의 그룹 DN 값과 정확하게 일치해야 합니다.

이 샘플 컨피그레이션에서 이 값은 **CN=ucsadmin,OU=CiscoUCS,DC=sampledesign,DC=com입니다.**

- 의 **Roles** 표를 클릭하고 **Admin** 확인란을 선택하고 확인을 **클릭합니다.**

그룹 맵에 포함된 모든 사용자에게 관리자 권한을 지정하려는 역할을 나타내는 역할의 확인란을 클릭합니다.



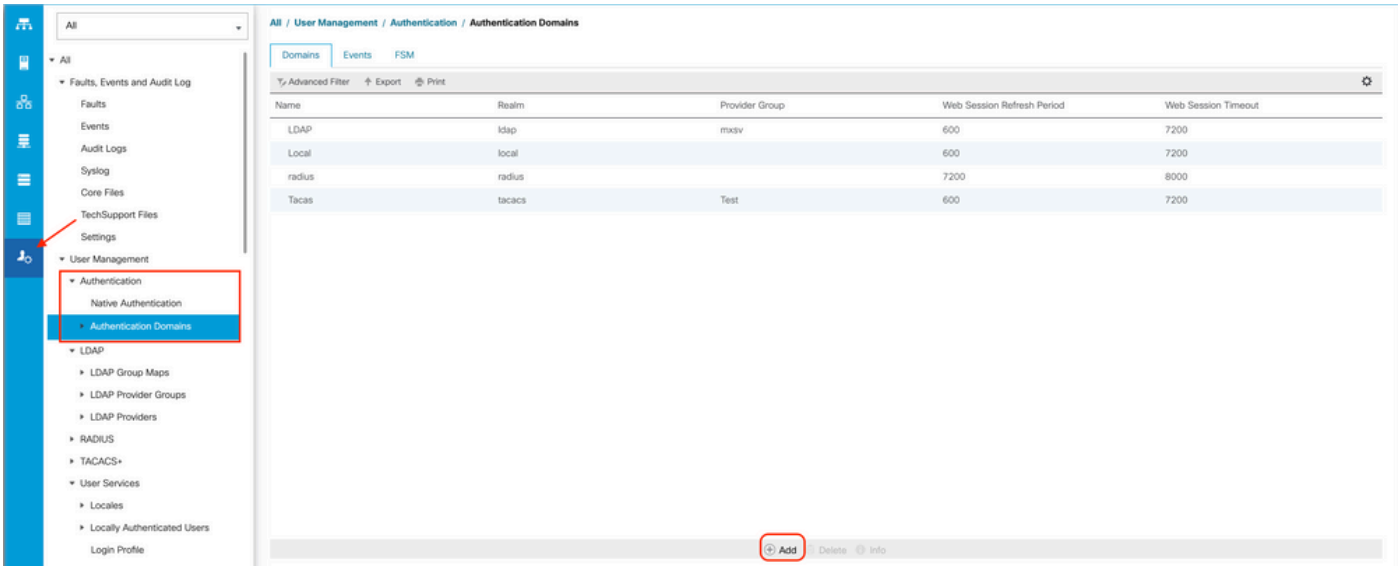
5단계. 테스트할 AD 서버의 각 나머지 역할에 대해 새 LDAP 그룹 맵을 만듭니다(AD에서 이전에 기록한 정보 사용).

다음: LDAP 인증 도메인을 생성합니다.

LDAP 인증 도메인 생성

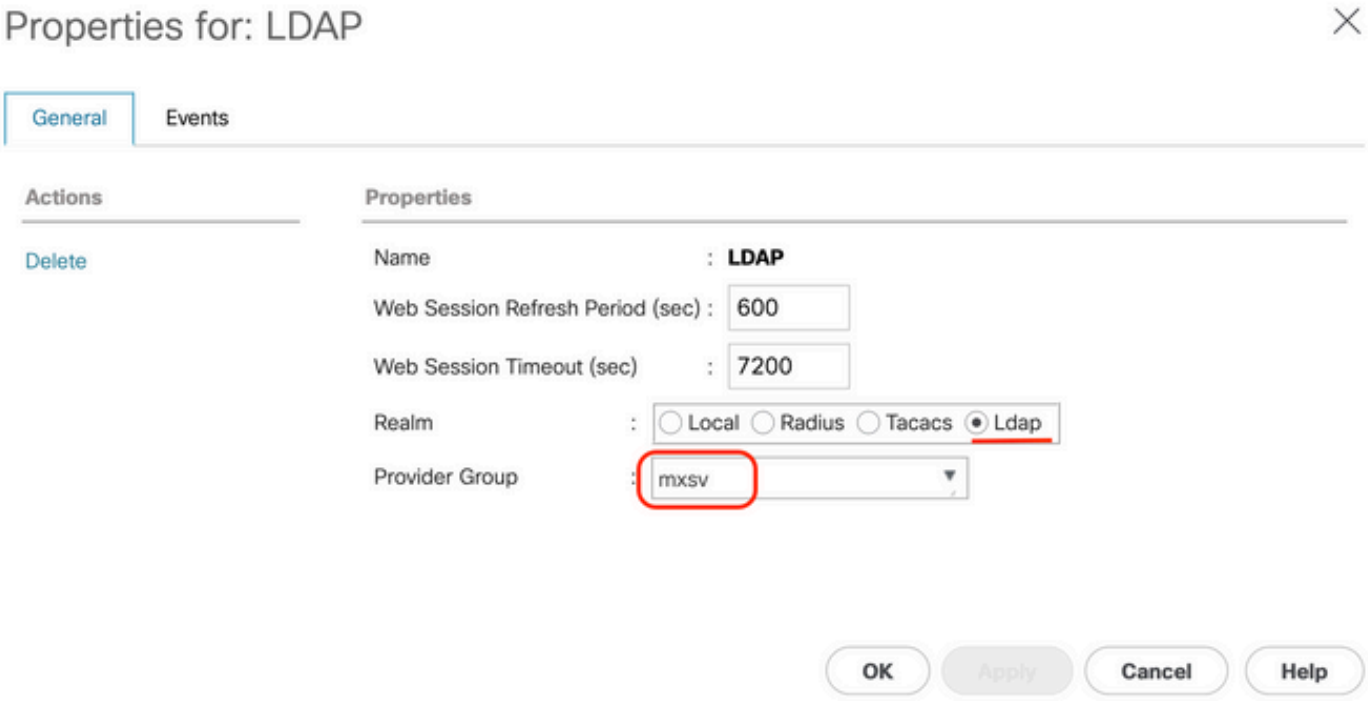
1단계. 에 관리자 탭, 확장 **All > User Management > Authentication**

2단계. 마우스 오른쪽 단추 클릭 **인증** Authentication Domains **및 선택** Create a Domain.



3단계.nbsp(&n)**Create a Domain** 대화 상자에서 다음을 완료합니다.

- 의 **Name** 필드에 도메인의 이름(예: LDAP)을 입력합니다.
- 의 **Realm** 영역을 클릭하고 **Ldap** 라디오 버튼.
- 에서 **Provider Group** 드롭다운 목록에서 **LDAP Provider Group** 이전에 생성한 후 확인을 **클릭합니다**.



인증 도메인이 아래에 나타납니다. **Authentication Domains.**

다음을 확인합니다.

Ping 대상 **LDAP Provider IP** 또는 **FQDN**:

```
UCS-AS-MXC-P25-02-B-A# connect local-mgmt
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

UCS-AS-MXC-P25-02-B-A(local-mgmt)# ping 10.31.123.60
PING 10.31.123.60 (10.31.123.60) from 10.31.123.8 : 56(84) bytes of data.
64 bytes from 10.31.123.60: icmp_seq=1 ttl=128 time=0.302 ms
64 bytes from 10.31.123.60: icmp_seq=2 ttl=128 time=0.347 ms
64 bytes from 10.31.123.60: icmp_seq=3 ttl=128 time=0.408 ms
```

NX-OS에서 인증을 테스트하려면 **test aaa** 명령(NXOS에서만 사용 가능).

서버의 구성을 확인합니다.

```
ucs(nxos)# test aaa server ldap <LDAP-server-IP-address or FQDN> <username> <password>
```

```
UCS-AS-MXC-P25-02-B-A# connect nxos
 Bad terminal type: "xterm-256color". Will assume vt100.
 Cisco Nexus Operating System (NX-OS) Software
 TAC support: http://www.cisco.com/tac
 Copyright (C) 2002-2020, Cisco and/or its affiliates.
 All rights reserved.
 The copyrights to certain works contained in this software are
 owned by other third parties and used and distributed under their own
 licenses, such as open source.  This software is provided "as is," and unless
 otherwise stated, there is no warranty, express or implied, including but not
 limited to warranties of merchantability and fitness for a particular purpose.
 Certain components of this software are licensed under
 the GNU General Public License (GPL) version 2.0 or
 GNU General Public License (GPL) version 3.0  or the GNU
 Lesser General Public License (LGPL) Version 2.1 or
 Lesser General Public License (LGPL) Version 2.0.
 A copy of each such license is available at
 http://www.opensource.org/licenses/gpl-2.0.php and
 http://opensource.org/licenses/gpl-3.0.html and
 http://www.opensource.org/licenses/lgpl-2.1.php and
 http://www.gnu.org/licenses/old-licenses/library.txt.
UCS-AS-MXC-P25-02-B-A(nx-os)# test aaa server ldap 10.31.123.60 admin Cisco123
```

일반적인 LDAP 문제.

- 기본 설정.
- 잘못된 암호 또는 잘못된 문자입니다.
- 잘못된 포트 또는 필터 필드

- 방화벽 또는 프록시 규칙으로 인해 공급자와 통신하지 않습니다.
- FSM은 100%가 아닙니다.
- 인증서 문제.

문제 해결

UCSM LDAP 컨피그레이션 확인:

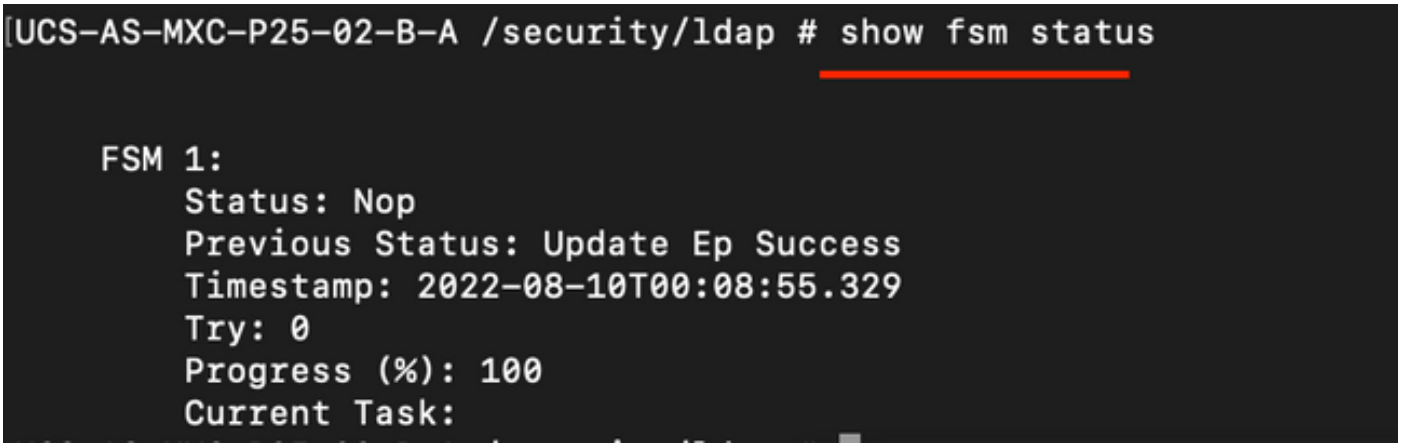
의 상태가 다음과 같으므로 UCSM에서 컨피그레이션을 성공적으로 구현했는지 확인해야 합니다 **Finite State Machine (FSM)** 100% 완료로 표시됩니다.

UCSM의 명령줄에서 컨피그레이션을 확인하려면

```
ucs # scope security
ucs /security# scope ldap
ucs /security/ldap# show configuration
```

```
UCS-AS-MXC-P25-02-B-A /security # scope security
UCS-AS-MXC-P25-02-B-A /security # scope security
UCS-AS-MXC-P25-02-B-A /security # scope ldap
UCS-AS-MXC-P25-02-B-A /security/ldap # show configuration
  scope ldap
      enter auth-server-group mxsv
          enter server-ref 10.31.123.60
              set order 1
          exit
      exit
      enter ldap-group "CN=ucsadmin,OU=CiscoUCS,DC=mxsvlab,DC=com"
      exit
      enter server 10.31.123.60
          enter ldap-group-rule
              set authorization enable
              set member-of-attribute memberOf
              set traversal recursive
              set use-primary-group no
          exit
          set attribute ""
          set basedn "DC=mxsvlab,DC=com"
          set binddn "CN=ucsbind,OU=CiscoUCS,DC=mxsvlab,DC=com"
          set filter ""
          set order 1
          set port 389
          set ssl no
          set timeout 30
          set vendor ms-ad
  !       set password
      exit
      set attribute ""
      set basedn "DC=mxsvlab,DC=com"
      set filter sAMAccountName=$userid
      set timeout 30
  exit
UCS-AS-MXC-P25-02-B-A /security/ldap #
```

```
ucs /security/ldap# show fsm status
```



NXOS에서 컨피그레이션을 확인하려면

```
ucs# connect nxos
ucs(nxos)# show ldap-server
ucs(nxos)# show ldap-server groups
```

```
UCS-AS-MXC-P25-02-B-A# connect nxos
Bad terminal type: "xterm-256color". Will assume vt100.
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source.  This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
UCS-AS-MXC-P25-02-B-A(nx-os)# show ldap-server
     timeout : 30
        port : 0
      baseDN : DC=mxsvlab,DC=com
user profile attribute :
search filter : sAMAccountName=$userid
  use groups : 0
recurse groups : 0
group attribute : memberOf
    group map CN=ucsadmin,OU=CiscoUCS,DC=mxsvlab,DC=com:
        roles: admin
        locales:
total number of servers : 1

following LDAP servers are configured:
    10.31.123.60:
        timeout: 30    port: 389    rootDN: CN=ucsbind,OU=CiscoUCS,DC=mxsvlab,DC=com
        enable-ssl: false
        baseDN: DC=mxsvlab,DC=com
        user profile attribute:
        search filter:
        use groups: true
        recurse groups: true
        group attribute: memberOf
        vendor: MS AD
UCS-AS-MXC-P25-02-B-A(nx-os)# show ldap-server groups
total number of groups: 2

following LDAP server groups are configured:
    group ldap:
        baseDN:
        user profile attribute:
        search filter:
        group membership attribute:
        server: 10.31.123.60 port: 389 timeout: 30
    group mxsv:
        baseDN:
        user profile attribute:
        search filter:
        group membership attribute:
        server: 10.31.123.60 port: 389 timeout: 30
```

오류를 확인하는 가장 효과적인 방법은 디버그를 활성화하는 것입니다. 이 출력으로 그룹, 연결 및

통신을 방지하는 오류 메시지를 볼 수 있습니다.

- FI에 대한 SSH 세션을 열고 로컬 사용자로 로그인한 다음 NX-OS CLI 컨텍스트로 변경하고 터미널 모니터를 시작합니다.

```
 ucs # connect nxos

ucs(nxos)# terminal monitor
```

- 디버그 플래그를 활성화하고 로그 파일에 대한 SSH 세션 출력을 확인합니다.

```
 ucs(nxos)# debug aaa all <<< not required, incase of debugging authentication problems

ucs(nxos)# debug aaa aaa-requests

ucs(nxos)# debug ldap all <<< not required, incase of debugging authentication problems.

ucs(nxos)# debug ldap aaa-request-lowlevel

ucs(nxos)# debug ldap aaa-request
```

```
UCS-AS-MXC-P25-02-B-A# connect nxos
Bad terminal type: "xterm-256color". Will assume vt100.
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source.  This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
UCS-AS-MXC-P25-02-B-A(nx-os)# terminal monitor
UCS-AS-MXC-P25-02-B-A(nx-os)# debug ldap all
UCS-AS-MXC-P25-02-B-A(nx-os)# debug aaa all
```

- 이제 새 GUI 또는 CLI 세션을 열고 원격(LDAP) 사용자로 로그인을 시도합니다.
- 로그인 실패 메시지가 표시되면 디버그를 끕니다.

관련 정보

- [기술 지원 및 문서 – Cisco Systems]

- UCSM LDAP 샘플 컨피그레이션
- Cisco UCS C Series GUI 컨피그레이션 가이드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.