

Configurar LDAP no UCS Manager

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Criar um domínio de autenticação local](#)

[Criar um provedor LDAP](#)

[Configuração de regra de grupo LDAP](#)

[Criar um grupo de provedores LDAP](#)

[Criar um mapa de grupo LDAP](#)

[Criar um domínio de autenticação LDAP](#)

[Verificar](#)

[Problemas comuns de LDAP.](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve a configuração para acesso de servidor remoto com o protocolo LDAP em NOSSO Unified Computing System Manager Domain (UCSM).

Prerequisites

Requirements

A Cisco recomenda o conhecimento destes tópicos:

- **Unified Computing System Manager Domain (UCSM)**
- Autenticação local e remota
- **Lightweight Directory Access Protocol (LDAP)**
- **Microsoft Active Directory (MS-AD)**

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver

ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Lightweight Directory Access Protocol (LDAP) é um dos principais protocolos desenvolvidos para serviços de diretório que gerenciam com segurança os usuários e seus direitos de acesso aos recursos de TI.

A maioria dos serviços de diretório ainda usa LDAP hoje, embora também possam usar protocolos adicionais como Kerberos, SAML, RADIUS, SMB, Oauth e outros.

Configurar

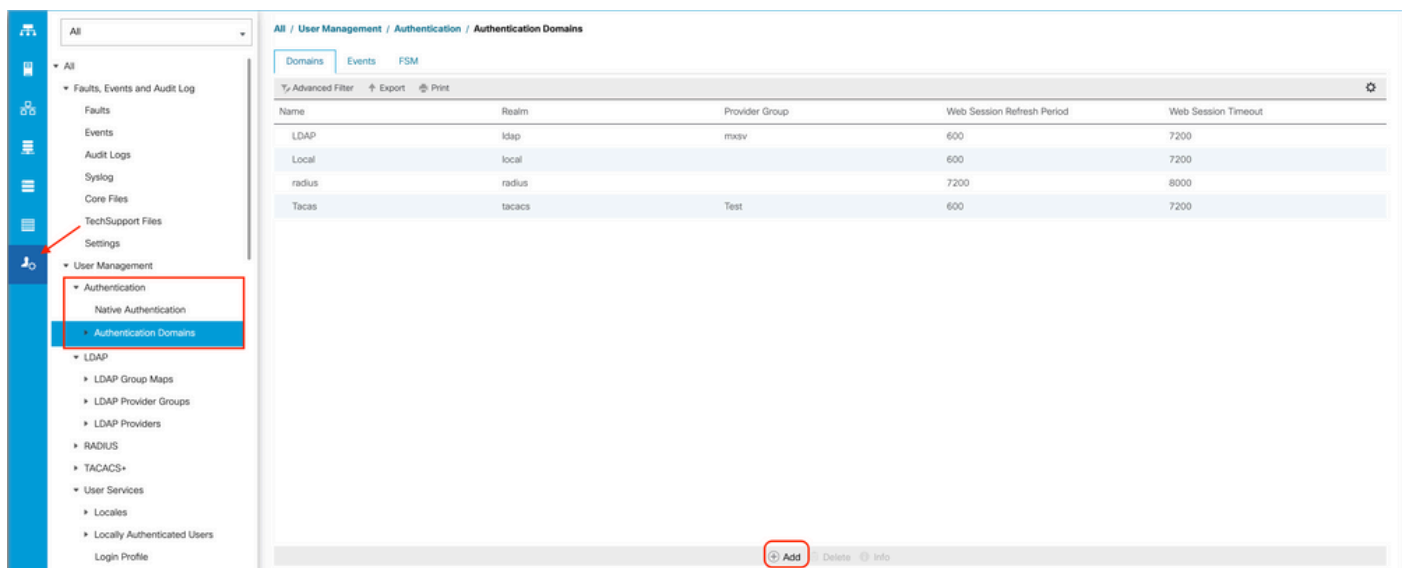
Antes de Começar

Faça login no Cisco UCS Manager GUI como um usuário administrativo.

Criar um domínio de autenticação local

Etapa 1. No Navigation clique no botão Admin guia.

Etapa 2. No Admin, expandir All > User Management > Authentication



The screenshot shows the Cisco UCS Manager GUI. On the left is a navigation menu with a tree structure. The 'Authentication Domains' option is highlighted with a red box. On the right, the 'Authentication Domains' table is displayed with the following data:

Name	Realm	Provider Group	Web Session Refresh Period	Web Session Timeout
LDAP	ldap	mxsv	600	7200
Local	local		600	7200
radius	radius		7200	8000
Tacacs	tacacs	Test	600	7200

At the bottom of the table, there is an 'Add' button circled in red.

Etapa 3. Clique com o botão direito do mouse **Authentication Domains** e selecione **Create a Domain**.

Etapa 4. Para a **Name** campo, tipo **Local**.

Etapa 5. Para a **Realm**, clique no botão **Local** botão de opção.

General	Events
<p>Actions</p> <p>Delete</p>	
<p>Properties</p> <p>Name : Local</p> <p>Web Session Refresh Period (sec) : 600</p> <p>Web Session Timeout (sec) : 7200</p> <p>Realm : <input checked="" type="radio"/> Local <input type="radio"/> Radius <input type="radio"/> Tacacs <input type="radio"/> Ldap</p>	
<p>OK Apply Cancel Help</p>	

Etapa 6. Clique em ok.

Criar um provedor LDAP

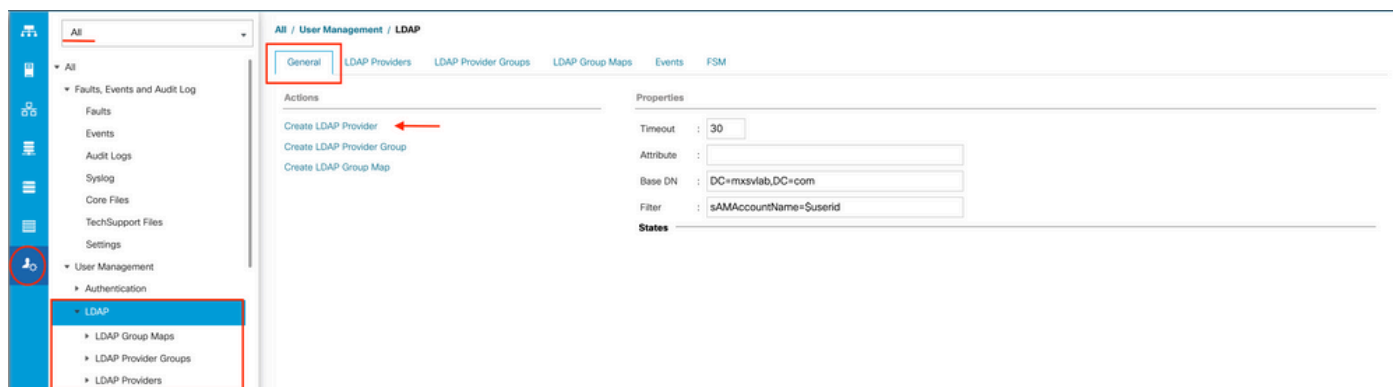
Este exemplo de configuração não inclui etapas para configurar LDAP com SSL.

Etapa 1. No Navigation clique no botão Admin guia.

Etapa 2. No Admin , expandir All > User Management > LDAP.

Etapa 3. No Work clique no botão General guia.

Etapa 4. No Actions , clique em Create LDAP Provider



Etapa 5. No Create LDAP Provider do assistente, insira as informações apropriadas:

- No Hostnamedigite o endereço IP ou o nome de host do servidor do AD.
- No Order , aceite o lowest-available padrão.
- No BindDN , copie e cole o BindDN da sua configuração do AD.

Para esta configuração de exemplo, o valor BindDN é **CN=ucsbind,OU=CiscoUCS,DC=mxsvlab,DC=com.**

- No **BaseDN** , copie e cole o BaseDN da sua configuração do AD.

Para esta configuração de exemplo, o valor de BaseDN é **DC=mxsvlab,DC=com**.

- Deixe o **Enable SSL** caixa de seleção desmarcada.
- No **Port** aceite o padrão 389.
- No **Filter** , copie e cole o atributo de filtro da sua configuração do AD.

O Cisco UCS usa o valor de filtro para determinar se o nome de usuário (fornecido na tela de logon pelo **Cisco UCS Manager**) está em AD.

Para esta configuração de exemplo, o valor do filtro é **sAMAccountName=\$userid**, onde \$userid é o user name para entrar no **Cisco UCS Manager** tela de login.

- Deixe o **Attribute** campo em branco.
- No **Password** digite a senha da conta ucsbind configurada no AD.

Se você precisar voltar para a **Create LDAP Provider wizard** para redefinir a senha, não fique alarmado se o campo password estiver em branco.

O **Set: yes** que aparece ao lado do campo de senha indica que uma senha foi definida.

- No **Confirm Password** digite novamente a senha da conta ucsbind configurada no AD.
- No **Timeout** , aceite o 30 padrão.
- No **Vendor** selecione o botão de opção **MS-AD** para Microsoft Active Directory.

Create LDAP Provider

1 Create LDAP Provider

2 LDAP Group Rule

Hostname/FQDN (or IP Address) : 10.31.123.60

Order : lowest-available

Bind DN : CN=ucsbind,OU=CiscoUCS,DC=mxsvlab,DC=com

Base DN : DC=mxsvlab,DC=com

Port : 389

Enable SSL :

Filter : sAMAccountName=\$userid

Attribute :

Password :

Confirm Password :

Timeout : 30

Vendor : Open Ldap MS AD

< Prev Next > Finish Cancel

Etapa 6. Clique em **Next**

Configuração de regra de grupo LDAP

Passo 1. Na guia LDAP Group Rule do assistente, preencha os próximos campos:

- Para a **Group Authentication** clique no botão **Enable** botão de opção.
- Para a **Group Recursion** clique no botão **Recursive** botão de opção. Isso permite que o sistema continue a pesquisa, nível por nível, até encontrar um usuário.

Se a **Group Recursion** está definido como **Non-Recursive**, ele limita o UCS a uma pesquisa de primeiro nível, mesmo que a pesquisa não localize um usuário qualificado.

- No **Target Attribute** , aceite o **memberOf** padrão.

The screenshot shows the 'Create LDAP Provider' wizard. On the left, a blue sidebar indicates the current step is '2 LDAP Group Rule'. The main panel is titled 'Create LDAP Provider' and contains the following configuration options:

- Group Authorization :** Disable Enable
- Group Recursion :** Non Recursive Recursive
- Target Attribute :** memberOf
- Use Primary Group :**

At the bottom of the wizard, there are four buttons: '< Prev', 'Next >', 'Finish', and 'Cancel'.

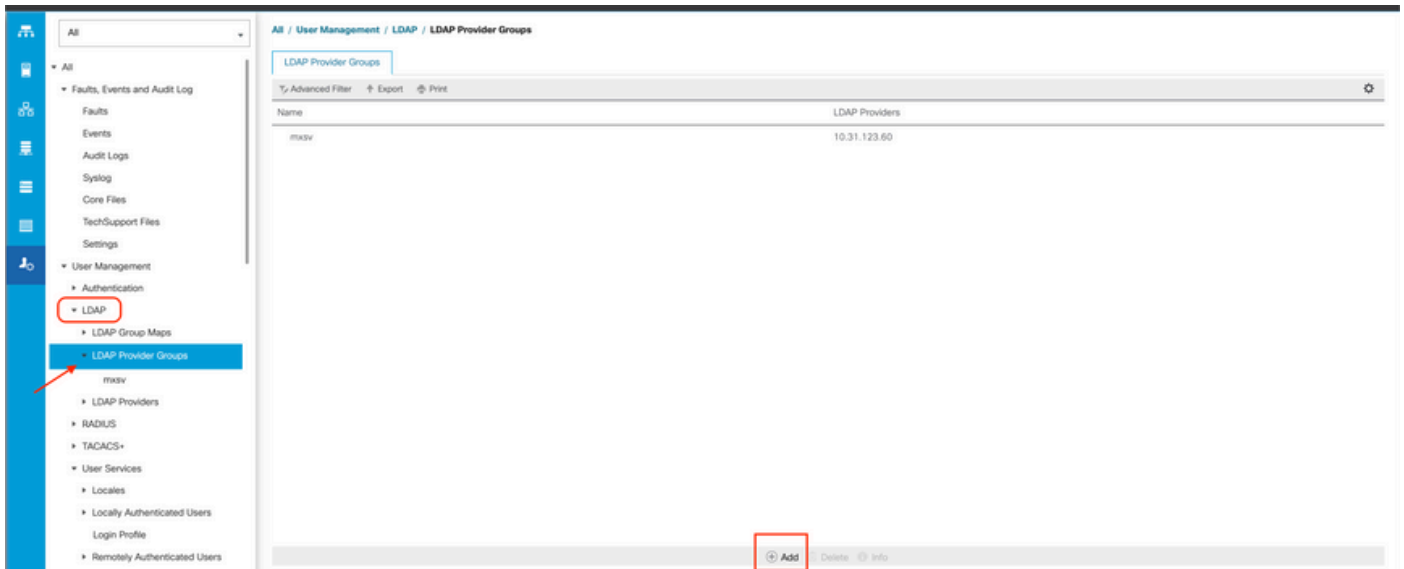
Etapa 2. Clique em **Finish**.

Note: Em um cenário real, você provavelmente teria vários provedores LDAP. Para vários provedores LDAP, você deve repetir as etapas para configurar a Regra de grupo LDAP para cada provedor LDAP. No entanto, nesta configuração de exemplo, há apenas um provedor LDAP, portanto isso não é necessário.

O endereço IP do servidor do AD é exibido no painel de navegação em **LDAP>Provedores LDAP**.

Criar um grupo de provedores LDAP

Etapa 1. No painel de Navegação, clique com o botão direito do mouse em **LDAP Provider Groups** e selecione **Create LDAP Provider Group**.



Etapa 2. No **Create LDAP Provider Group**, preencha as informações adequadamente:

- No **Name** insira um nome exclusivo para o grupo, como **LDAP Providers**.
- No **LDAP Providers** selecione o endereço IP do servidor AD.
- Clique no botão **>>** para adicionar o servidor AD ao seu **Included Providers** tabela.

Create LDAP Provider Group

Name : mxsv

LDAP Providers		
Hostname	Bind DN	Port
10.31.123....	CN=ucsbind,...	389

>>
<<

Included Providers	
Name	Order
No data available	

OK Cancel

Etapa 3. Clique em **OK**.

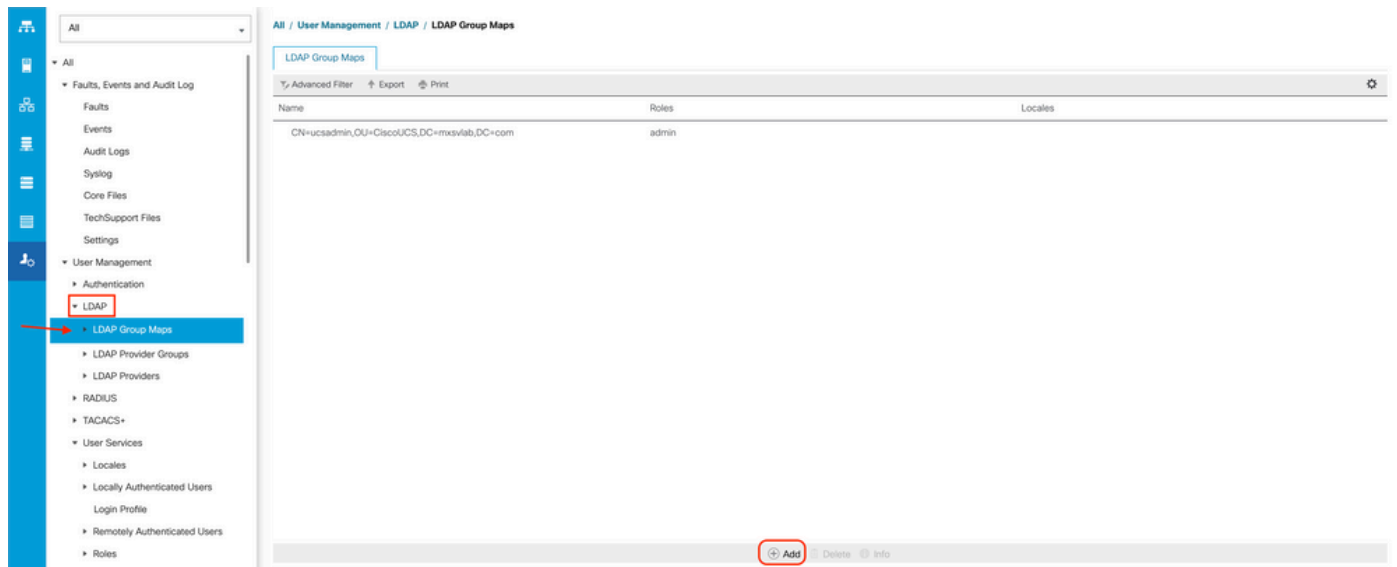
Seu grupo de provedores aparece no **LDAP Provider Groups** pasta.

Criar um mapa de grupo LDAP

Etapa 1. No painel de navegação, clique no botão Adminguia.

Etapa 2. No Admin , expandir All > User Management > LDAP.

Etapa 3. No painel Trabalho, clique em Criar LDAP Group Map.



Etapa 4. No Create LDAP Group Map , preencha as informações adequadamente:

- No **LDAP Group DN** , copie e cole o valor que você tem na seção de configuração do servidor AD para seu grupo LDAP.

O valor DN do grupo LDAP solicitado nesta etapa mapeia para o nome distinto de cada um dos grupos criados no AD em Grupos UCS.

Por esse motivo, o valor DN do grupo inserido no Cisco UCS Manager deve corresponder exatamente ao valor DN do grupo no servidor AD.

Nesta configuração de exemplo, esse valor é **CN=ucsadmin,OU=CiscoUCS,DC=sampldesign,DC=com.**

- No **Roles** , clique no botão Admin e clique em OK.

Clique na caixa de seleção de uma função para indicar que você deseja atribuir privilégios de administrador a todos os usuários incluídos no mapa de grupos.

Create LDAP Group Map



LDAP Group DN : CN=ucsadmin,OU=CiscoUCS,DC=mxsvlab,DC=com

Roles

- aaa
- admin ←
- facility-manager
- network
- OnlyKVM
- operations
- read-only
- server-compute
- server-equipment
- server-profile
- server-security
- stats
- storage

Locales

- JaviTest
- JosueLoc
- Test

OK

Cancel

Etapa 5. Crie novos mapas de grupo LDAP (use as informações gravadas anteriormente no AD) para cada uma das funções restantes no servidor AD que você deseja testar.

Próximo: Crie seu domínio de autenticação LDAP.

Criar um domínio de autenticação LDAP

Etapa 1. Na guia Admin , expandir All > User Management > Authentication

Etapa 2. Clique com o botão direito do mouse **Autenticação** Authentication Domains e **selecione** Create a Domain.

Navigation menu items:

- All
- Faults, Events and Audit Log
 - Faults
 - Events
 - Audit Logs
 - Systemlog
 - Core Files
 - TechSupport Files
 - Settings
- User Management
 - Authentication
 - Native Authentication
 - Authentication Domains**
 - LDAP
 - LDAP Group Maps
 - LDAP Provider Groups
 - LDAP Providers
 - RADIUS
 - TACACS+
 - User Services
 - Locales
 - Locally Authenticated Users
 - Login Profile

Name	Realm	Provider Group	Web Session Refresh Period	Web Session Timeout
LDAP	ldap	mxsv	600	7200
Local	local		600	7200
radius	radius		7200	8000
Tacacs	tacacs	Test	600	7200

Buttons: Add, Delete, Info

Etapa 3. Na Create a Domain preencha o seguinte:

- No **Name** digite um nome para o seu domínio, como LDAP.
- No **Realm** clique no botão Ldap botão de opção.
- Nos **Provider Group** , selecione a LDAP Provider Group criado anteriormente e clique em **OK**.

Properties for: LDAP

General | Events

Actions

Delete

Properties

Name : **LDAP**

Web Session Refresh Period (sec) : 600

Web Session Timeout (sec) : 7200

Realm : Local Radius Tacacs Ldap

Provider Group : mxsv

Buttons: OK, Apply, Cancel, Help

O domínio de autenticação aparece em Authentication Domains.

Verificar

Ping para LDAP Provider IP ou 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
```

Para testar a autenticação do NX-OS, use o comando `test aaa` (disponível somente no NXOS).

Validamos a configuração do nosso servidor:

```
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
```

Problemas comuns de LDAP.

- Configuração básica.
- Senha incorreta ou caracteres inválidos.
- Porta ou campo Filter errado.

- Não há comunicação com nosso provedor devido a uma regra de Firewall ou Proxy.
- FSM não é 100%.
- Problemas de certificado.

Troubleshoot

Verificar configuração LDAP do UCSM:

Você deve garantir que o UCSM implementou a configuração com êxito, pois o status do Finite State Machine (FSM) é mostrado como 100% concluído.

Para verificar a configuração a partir da linha de comando de nosso UCSM:

```
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
```

```
[UCS-AS-MXC-P25-02-B-A /security/ldap # show fsm status
```

```
FSM 1:  
  Status: Nop  
  Previous Status: Update Ep Success  
  Timestamp: 2022-08-10T00:08:55.329  
  Try: 0  
  Progress (%): 100  
  Current Task:
```

Para verificar a configuração do NXOS:

```
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

```

O método mais eficaz para ver erros é ativar nossa depuração, com essa saída podemos ver os

grupos, a conexão e a mensagem de erro que impede a comunicação.

- Abra uma sessão SSH para FI e faça login como um usuário local, altere para o contexto CLI do NX-OS e inicie o monitor de terminal.

```
ucs # connect nxos
```

```
ucs(nxos)# terminal monitor
```

- Habilite sinalizadores de depuração e verifique a saída da sessão SSH para o arquivo de log.

```
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 ←
```

- Agora, abra uma nova sessão de GUI ou CLI e tente fazer login como um usuário remoto (LDAP).
- Após receber uma mensagem de falha de login, desative as depurações.

Informações Relacionadas

- [Suporte Técnico e Documentação - Cisco Systems](#)

- [Configuração de exemplo UCSM LDAP](#)
- [Guia de configuração da GUI do Cisco UCS C Series](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.