

Configuración de LDAP en UCS Manager

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Crear un dominio de autenticación local](#)

[Crear un proveedor LDAP](#)

[Configuración de regla de grupo LDAP](#)

[Crear un grupo de proveedores LDAP](#)

[Crear un mapa de grupo LDAP](#)

[Crear un dominio de autenticación LDAP](#)

[Verificación](#)

[Problemas comunes de LDAP.](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe la configuración para el acceso al servidor remoto con el protocolo LDAP en nuestro Unified Computing System Manager Domain (UCSM).

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

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

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Lightweight Directory Access Protocol (LDAP) es uno de los protocolos principales desarrollados para los servicios de directorio que gestiona de forma segura a los usuarios y sus derechos de acceso a los recursos de TI.

La mayoría de los servicios de directorio todavía utilizan LDAP en la actualidad, aunque también pueden utilizar protocolos adicionales como Kerberos, SAML, RADIUS, SMB, Oauth y otros.

Configurar

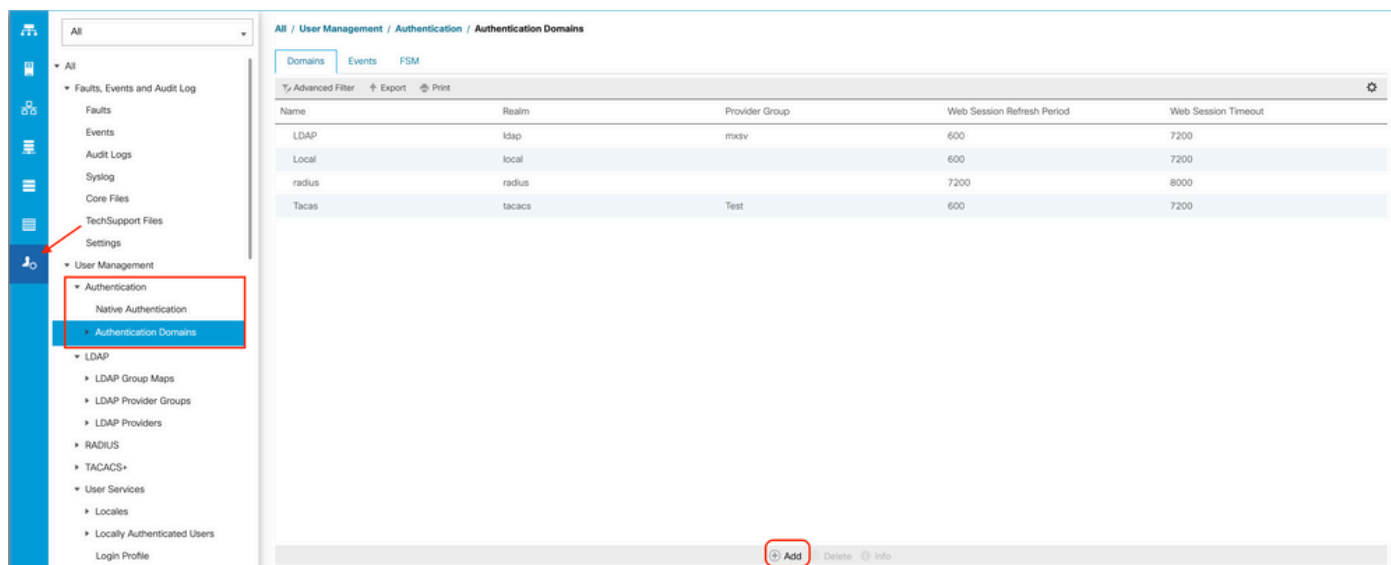
Antes de comenzar

Inicie sesión en **Cisco UCS Manager GUI** como usuario administrativo.

Crear un dominio de autenticación local

Paso 1. En el **Navigation** haga clic en el botón **Admin** ficha.

Paso 2. En el **Admin** ficha, 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' item is highlighted with a red box. On the right, the 'Authentication Domains' page is displayed, showing a table with columns: Name, Realm, Provider Group, Web Session Refresh Period, and Web Session Timeout. The table contains four rows: LDAP, Local, radius, and Tacacs. At the bottom of the table, there is an 'Add' button circled in red.

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

Paso 3. Clic con el botón derecho **Authentication Domains** y seleccione **Create a Domain**.

Paso 4. Para el **Name** campo, tipo **Local**.

Paso 5. Para el **Realm**, haga clic en el botón **Local** botón de opción.

General	Events
<p>Actions</p> <p>Delete</p>	<p>Properties</p> <p>Name : Local</p> <p>Web Session Refresh Period (sec) : <input type="text" value="600"/></p> <p>Web Session Timeout (sec) : <input type="text" value="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>	

Paso 6. Haga clic en ok.

Crear un proveedor LDAP

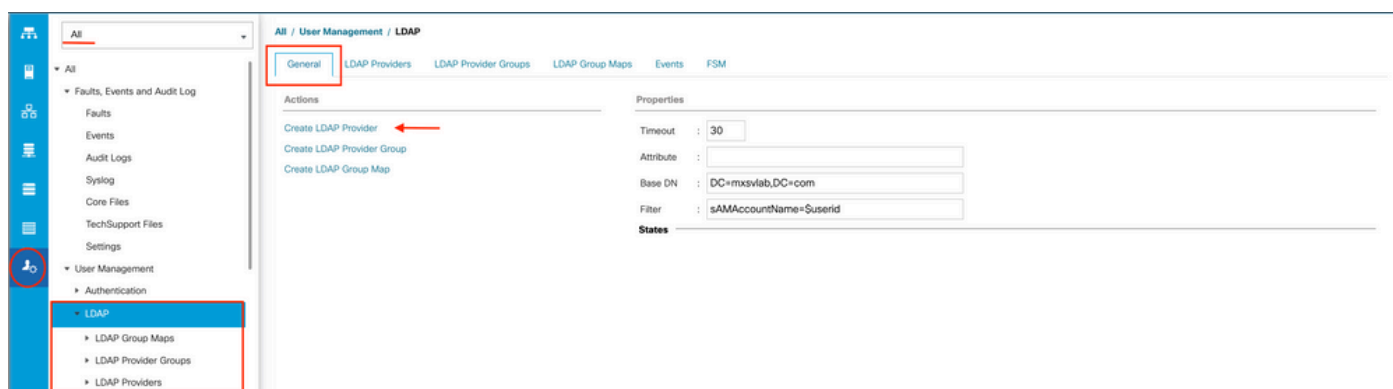
Este ejemplo de configuración no incluye los pasos para configurar LDAP con SSL.

Paso 1. En el Navigation haga clic en el botón Admin ficha.

Paso 2. En el Admin ficha, expandir All > User Management > LDAP.

Paso 3. En el work haga clic en el botón General ficha.

Paso 4. En el Actions área, haga clic en Create LDAP Provider



Paso 5. En el Create LDAP Provider del asistente, introduzca la información correspondiente:

- En el **Hostname** escriba la dirección IP o el nombre de host del servidor de AD.
- En el **Order**, acepte el **lowest-available** predeterminado.
- En el **BindDN** copie y pegue el DN de enlace de la configuración de AD.

Para esta configuración de ejemplo, el valor de BindDN es **CN=ucsbind,OU=CiscoUCS,DC=mxsvlab,DC=com**.

- En el **BaseDN** copie y pegue el DN base de la configuración de AD.

Para esta configuración de ejemplo, el valor BaseDN es **DC=mxsvlab,DC=com**.

- Deje el **Enable SSL** casilla de verificación desactivada.
- En el **Port** , acepte el valor predeterminado 389.
- En el **Filter** copie y pegue el atributo de filtro de la configuración de AD.

Cisco UCS utiliza el valor de filtro para determinar si el nombre de usuario (proporcionado en la pantalla de inicio de sesión por **Cisco UCS Manager**) está en AD.

Para esta configuración de ejemplo, el valor del filtro es **sAMAccountName=\$userid**, donde \$userid es el user name para introducir en el **Cisco UCS Manager** pantalla de inicio de sesión

- Deje el **Attribute** campo en blanco.
- En el **Password** escriba la contraseña de la cuenta ucsbind configurada en AD.

Si necesita volver a la página **Create LDAP Provider wizard** para restablecer la contraseña, no se alarme si el campo de contraseña está vacío.

Set: yes mensaje que aparece junto al campo contraseña indica que se ha establecido una contraseña.

- En el **Confirm Password** , vuelva a escribir la contraseña de la cuenta ucsbind configurada en AD.
- En el **Timeout** , acepte el 30 por defecto.
- En el **Vendor** , seleccione el botón de opción de **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

Paso 6. Haga clic en Next

Configuración de regla de grupo LDAP

Paso 1. En elLDAP Group Rule del asistente, rellene los campos siguientes:

- Para el Group Authentication haga clic en el campo Enable botón de opción.
- Para el Group Recursion haga clic en el campo Recursive botón de opción. Esto permite al sistema continuar la búsqueda hacia abajo, nivel por nivel, hasta que encuentre un usuario.

Si Group Recursion se establece en Non-RecursiveAdemás, limita UCS a una búsqueda del primer nivel, incluso si la búsqueda no encuentra un usuario cualificado.

- En el Target Attribute , acepte elmemberOf predeterminado.

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 shows the following configuration:

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

At the bottom, there are four buttons: '< Prev', 'Next >', 'Finish' (highlighted in blue), and 'Cancel'. A red arrow points to the 'memberOf' text in the Target Attribute field.

Paso 2. Haga clic en Finish.

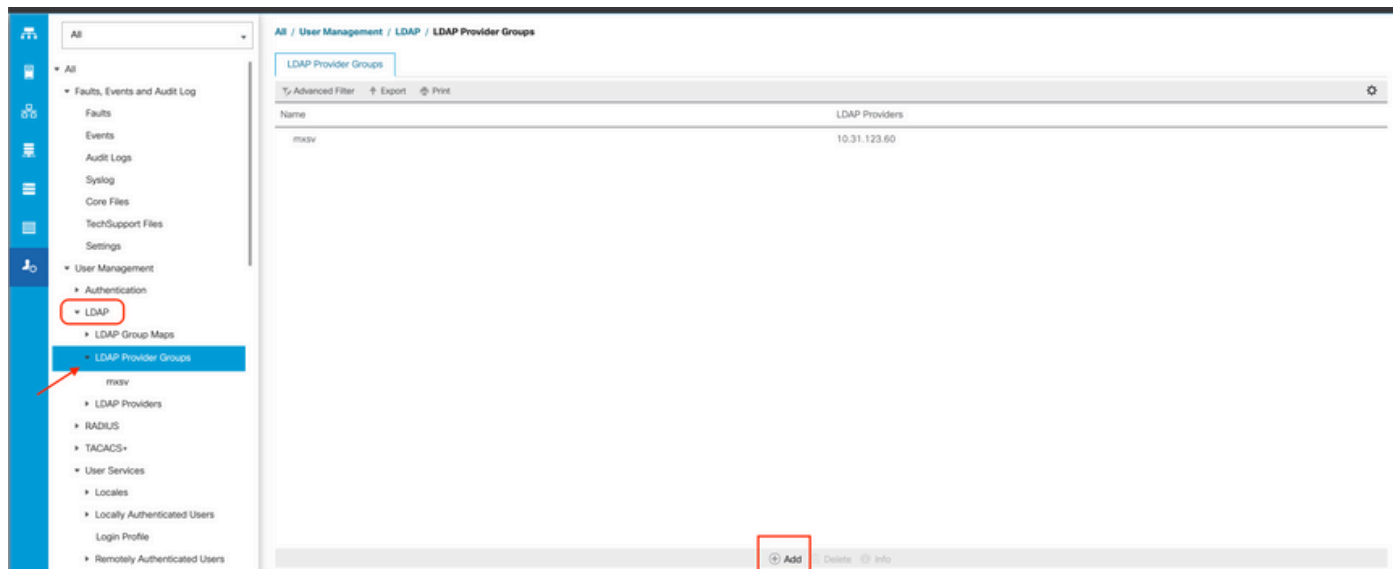
Nota: En un escenario real, lo más probable es que tenga varios proveedores LDAP. Para varios proveedores LDAP, debe repetir los pasos para configurar la regla de grupo LDAP para cada proveedor LDAP. Sin embargo, en esta configuración de ejemplo, sólo hay un proveedor LDAP, por lo que esto no es necesario.

La dirección IP del servidor AD se muestra en el panel de navegación bajoLDAP>Proveedores

LDAP.

Crear un grupo de proveedores LDAP

Paso 1. En el panel de navegación, haga clic con el botón derecho del ratón **LDAP Provider Groups** y seleccione **Create LDAP Provider Group**.



Paso 2. En el **Create LDAP Provider Group**, rellene la información de forma adecuada:

- En el **Name** introduzca un nombre único para el grupo, como **LDAP Providers**.
- En el **LDAP Providers**, elija la dirección IP del servidor AD.
- Haga clic en el botón **>>** para agregar el servidor de AD a su **Included Providers** tabla.

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

Paso 3. Click OK.

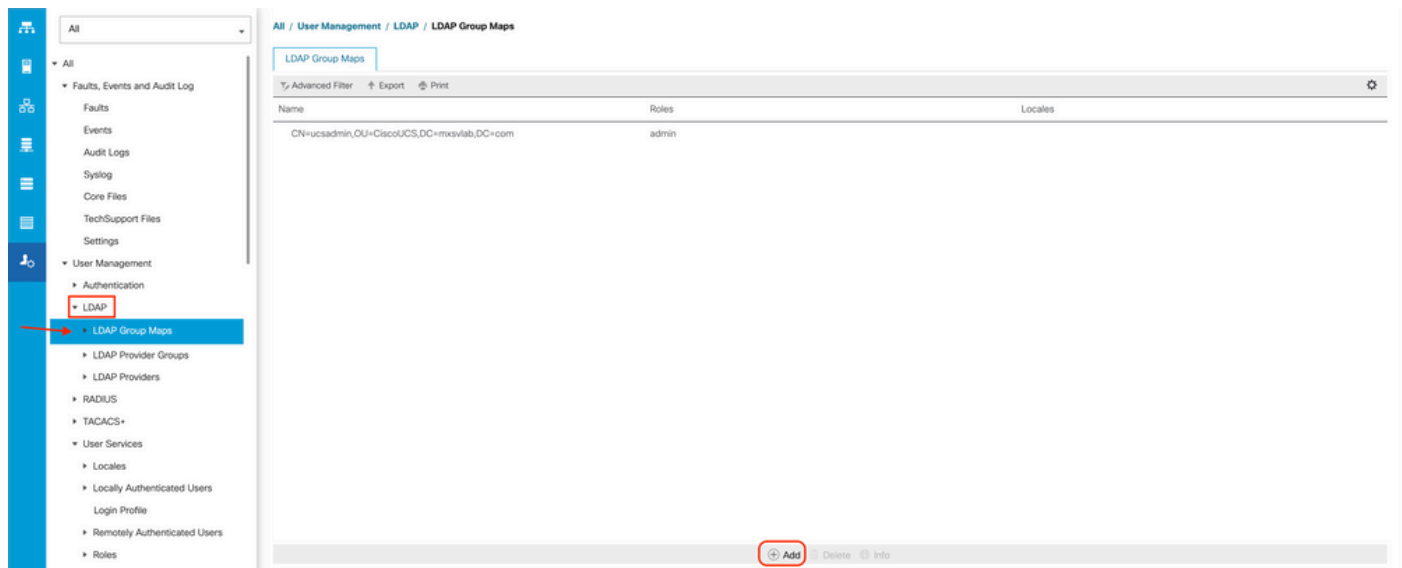
El grupo de proveedores aparece en el **LDAP Provider Groups** carpeta.

Crear un mapa de grupo LDAP

Paso 1. En el panel de navegación, haga clic en el botón **Admin** ficha.

Paso 2. En el **Admin** ficha, expandir **All > User Management > LDAP**.

Paso 3. En el panel de trabajo, haga clic en **Crear LDAP Group Map**.



Paso 4. En el **Create LDAP Group Map** , rellene la información de forma adecuada:

- En el **LDAP Group DN** copie y pegue el valor que tiene en la sección de configuración del servidor AD para su grupo LDAP.

El valor de DN de grupo LDAP solicitado en este paso se asigna al nombre distinguido de cada uno de los grupos que creó en AD en Grupos UCS.

Por este motivo, el valor de DN de grupo introducido en Cisco UCS Manager debe coincidir exactamente con el valor de DN de grupo del servidor AD.

En esta configuración de ejemplo, este valor es
CN=ucsadmin,OU=CiscoUCS,DC=sampldesign,DC=com.

- En el **Roles** haga clic en el botón **Admin** y haga clic en **Aceptar**.

Haga clic en la casilla de verificación de un rol para indicar que desea asignar privilegios de administrador a todos los usuarios incluidos en el mapa de grupo.

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

Paso 5. Cree nuevos mapas de grupo LDAP (utilice la información que registró anteriormente en AD) para cada uno de los roles restantes del servidor AD que desee probar.

Siguiente: Cree su dominio de autenticación LDAP.

Crear un dominio de autenticación LDAP

Paso 1. En el Admin ficha, expandir **All > User Management > Authentication**

Paso 2. Clic con el botón derecho **Autenticación Authentication Domains** y **seleccione** Create a Domain.

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

Paso 3. En el Create a Domain , complete el siguiente cuadro:

- En el **Name** , escriba un nombre para el dominio, como LDAP.
- En el **Realm** haga clic en el botón **Ldap** botón de opción.
- Desde **Provider Group** lista desplegable, seleccione la **LDAP Provider Group** creado anteriormente y haga clic en **Aceptar**.

Properties for: LDAP ✕

General

Events

Actions	Properties
Delete	<p>Name : LDAP</p> <p>Web Session Refresh Period (sec) : <input style="width: 80px;" type="text" value="600"/></p> <p>Web Session Timeout (sec) : <input style="width: 80px;" type="text" value="7200"/></p> <p>Realm : <input type="radio"/> Local <input type="radio"/> Radius <input type="radio"/> Tacacs <input checked="" type="radio"/> Ldap</p> <p>Provider Group : <input style="width: 150px;" type="text" value="mxsv"/></p>

El dominio de autenticación aparece en **Authentication Domains**.

Verificación

Enviar ping a LDAP Provider IP o 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 probar la autenticación de NX-OS, utilice el `test aaa` (solo disponible desde NXOS).

Validamos la configuración de nuestro 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 comunes de LDAP.

- Configuración Básica.
- Contraseña incorrecta o caracteres no válidos.
- Puerto o campo de filtro incorrecto.

- No hay comunicación con nuestro proveedor debido a una regla de firewall o proxy.
- FSM no es el 100%.
- Problemas de certificado.

Troubleshoot

Verifique la configuración LDAP de UCSM:

Debe asegurarse de que UCSM ha implementado la configuración correctamente debido al estado del Finite State Machine (FSM) se muestra como 100% completado.

Para verificar la configuración desde la línea de comandos de nuestro 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 la configuración desde 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

```

El método más efectivo para ver los errores es habilitar nuestra depuración, con esta salida

podemos ver los grupos, la conexión y el mensaje de error que impide la comunicación.

- Abra una sesión SSH en FI e inicie sesión como usuario local y cambie al contexto CLI de NX-OS e inicie el monitor de terminal.

```
ucs # connect nxos
```

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

- Habilite los indicadores de depuración y verifique el resultado de la sesión SSH en el archivo de registro.

```
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
```

- Ahora abra una nueva sesión GUI o CLI e intente iniciar sesión como un usuario remoto (LDAP).
- Una vez que haya recibido un mensaje de error de inicio de sesión, desactive las depuraciones.

Información Relacionada

- [Soporte Técnico y Documentación - Cisco Systems](#)
- [Ejemplo de configuración de UCSM LDAP](#)
- [Guía de configuración de la GUI de Cisco UCS C Series](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).