

Configuración del dominio de autenticación TACACS+ en UCS Manager con el servidor ISE

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configuración](#)

[Configuración de TACACS+ en ISE](#)

[Configuración de TACACS+ en ISE](#)

[Configurar los atributos y las reglas en ISE](#)

[Configuración de TACACS+ en UCSM](#)

[Crear funciones para usuarios](#)

[Crear un proveedor TACACS+](#)

[Crear un grupo de proveedores TACACS+](#)

[Crear un dominio de autenticación](#)

[Troubleshoot](#)

[Problemas comunes de TACACS+ en UCSM](#)

[Revisión de UCSM](#)

[Problemas comunes de TACACS en ISE](#)

[Revisión de ISE](#)

[Información Relacionada](#)

Introducción

Este documento describe la configuración de la autenticación de Terminal Access Controller Access-Control System Plus (TACACS+) en Unified Compute System Manager (UCSM). TACACS+ es un protocolo de red que se utiliza para los servicios de autenticación, autorización y responsabilidad (AAA) , que proporciona un método centralizado para gestionar los dispositivos de acceso a la red (NAD) donde puede administrar y crear reglas a través de un servidor, en este caso práctico estamos utilizando Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco UCS Manager (UCSM)
- Terminal Access Controller Access-Control System Plus (TACACS+)
- Identity Services Engine (ISE)

Componentes Utilizados

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

- UCSM 4.2(3d)
- Cisco Identity Services Engine (ISE) versión 3.2

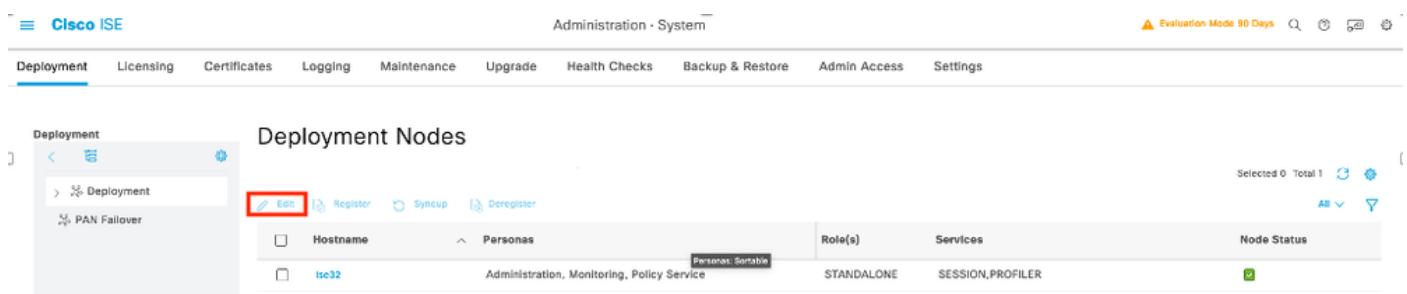
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender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

Configuración

Configuración de TACACS+ en ISE

Configuración de TACACS+ en ISE

Paso 1. La primera tarea es revisar si ISE tiene las capacidades correctas para manejar las autenticaciones TACACS+ para lo cual necesita verificar si dentro del Policy Service Node (PSN) desea que tenga la función de Device Admin Service, navegue por el menú Administration > System > Deployment, seleccione el nodo donde ISE realiza TACACS+ y luego seleccione el botón edit.



Paso 2. Desplácese hacia abajo hasta que vea la función correspondiente llamada Device Administration Service (observe que para habilitar esta función primero debe tener Policy Server Persona habilitado en el nodo y además tener licencias para TACACS+ disponibles en su implementación), seleccione esa casilla y luego guarde la configuración:

Cisco ISE Administration - System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

Other Monitoring Node

☐ Dedicated MNT

☒ Policy Service

☒ Enable Session Services

Include Node in Node Group

None

☒ Enable Profiling Service

☐ Enable Threat Centric NAC Service

☐ Enable SXP Service

☐ Enable Device Admin Service

☐ Enable Passive Identity Service

☐ pxGrid

Reset Save

Paso 3. Configure el Dispositivo de acceso a la red (NAD) que utiliza ISE como TACACS+ como servidor, navegue hasta el menú Administración > Recursos de red > Dispositivos de red y, a continuación, seleccione el botón +Agregar.

Cisco ISE Administration - Network Resources

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM

Network Devices

Default Device

Device Security Settings

Network Devices

Edit **+ Add** Duplicate Import Export Generate PAC Delete

Name	IP/Mask	Profile Name	Location	Type	Description
No data available					

Paso 4. En esta sección configure :

- Un nombre para que UCSM sea el cliente TACACS+.
- Las direcciones IP que utiliza UCSM para enviar solicitudes a ISE.
- TACACS+ Shared Secret (Clave secreta compartida de TACACS+). Se trata de la contraseña que se debe utilizar para cifrar los paquetes entre UCSM e ISE.

Cisco ISE Administration - Network Resources

Network Devices | Network Device Groups | Network Device Profiles | External RADIUS Servers | RADIUS Server Sequences | NAC Managers | External MDM | pxGrid Direct Connectors | Location Services

Network Devices List > USCM

Network Devices

Name USCM

Description

IP Address * IP: 10.31.123.9 / 32

IP Address * IP: 10.31.123.8 / 32

Device Profile Cisco

Model Name

Software Version

Network Device Group

Location All Locations [Set To Default](#)

IPSEC No [Set To Default](#)

Device Type All Device Types [Set To Default](#)

☐ RADIUS Authentication Settings

☒ TACACS Authentication Settings

Shared Secret [Show](#) [Retire](#)

☐ Enable Single Connect Mode

☒ Legacy Cisco Device



Nota: Para una configuración de clúster, agregue las direcciones IP del puerto de administración para ambas fabric interconectadas. Esta configuración garantiza que los usuarios remotos puedan seguir iniciando sesión si falla la primera fabric interconectada y el sistema conmuta por error a la segunda fabric interconectada. Todas las solicitudes de inicio de sesión se originan en estas direcciones IP, no en la dirección IP virtual que utiliza Cisco UCS Manager.

Configurar los atributos y las reglas en ISE

Paso 1. Cree un perfil TACACS+, navegue hasta el menú Centros de trabajo > Administración de dispositivos > Elementos de política > Resultados > Perfiles TACACS y, a continuación, seleccione Agregar

Cisco ISE Work Centers - Device Administration

Overview | Identities | User Identity Groups | Ext Id Sources | Network Resources | **Policy Elements** | Device Admin Policy Sets | Reports | Settings

TACACS Profiles

[Add](#) [Duplicate](#) [Trash](#) [Edit](#)

Name	Type	Description
Default Shell Profile	Shell	Default Shell Profile

Paso 2. En esta sección configure el perfil con un nombre y en la sección Atributos

personalizados, seleccione Agregar , luego cree un atributo de la característica OBLIGATORIO , denomínelo como cisco-av-pair y en el valor seleccione uno de los roles disponibles dentro de UCSM e ingrese que como un rol de shell, en este ejemplo está usando el rol admin y la entrada seleccionada debe ser shell:roles="admin", como se muestra aquí,

Cisco ISE Work Centers · Device Administration

Overview Identities User Identity Groups Ext Id Sources Network Resources **Policy Elements** Device Admin Policy Sets Reports Settings

Conditions >

Network Conditions >

Results ▾

Allowed Protocols

TACACS Command Sets

TACACS Profiles

Name

UCSM PROFILE ADMIN

Description

Task Attribute View

Raw View

Common Tasks

Common Task Type Shell ▾

☐ Default Privilege (Select 0 to 15)

☐ Maximum Privilege (Select 0 to 15)

☐ Access Control List

☐ Auto Command

☐ No Escape (Select true or false)

☐ Timeout Minutes (0-9999)

☐ Idle Time Minutes (0-9999)

Custom Attributes

Add

Trash ▾

Edit

⚙️

<input type="checkbox"/> Type	Name	Value
<input type="checkbox"/> MANDATORY	cisco-av-pair	shell:roles="admin"

Cancel

Save

En el mismo menú, si selecciona la Vista sin procesar para el perfil TACACS, puede verificar la configuración correspondiente del atributo que se enviará a través de ISE.

Cisco ISE

Work Centers · Device Administration

OverviewIdentitiesUser Identity GroupsExt Id SourcesNetwork ResourcesPolicy ElementsDevice Admin Policy SetsReportsSettings

Conditions>Network Conditions>Results▼Allowed ProtocolsTACACS Command SetsTACACS Profiles

TACACS Profiles > UCSM PROFILE ADMIN

TACACS Profile

NameUCSM PROFILE ADMIN

Description

Task Attribute ViewRaw View

Profile Attributes

cisco-av-pair=shell:roles=" admin"

CancelSave



Nota: El nombre del par cisco-av es la cadena que proporciona el ID de atributo para el proveedor TACACS+.

Paso 3. Seleccione en la marca y guarde su configuración.

Paso 4. Crear un conjunto de políticas de administración de dispositivos para su UCSM, navegue por el menú Centros de trabajo > Administración de dispositivos > Conjuntos de políticas de administración de dispositivos, luego desde un conjunto de políticas existente seleccione el icono de engranaje para luego seleccionar Insertar nueva fila

Cisco ISE

Work Centers · Device Administration

Evaluation Mode 89 Days

OverviewIdentitiesUser Identity GroupsExt Id SourcesNetwork ResourcesPolicy ElementsDevice Admin Policy SetsReportsSettings

Policy Sets

ResetReset Policyset HitcountsSave

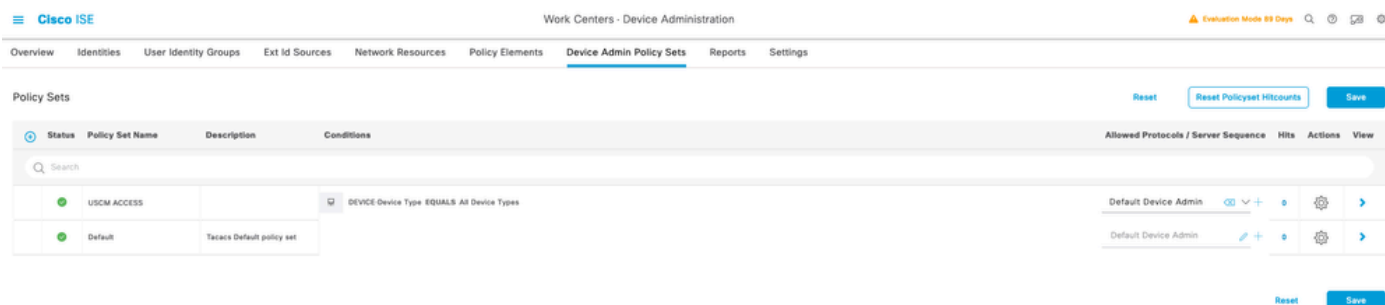
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
Default	Tacacs Default policy set						

Default Device Admin

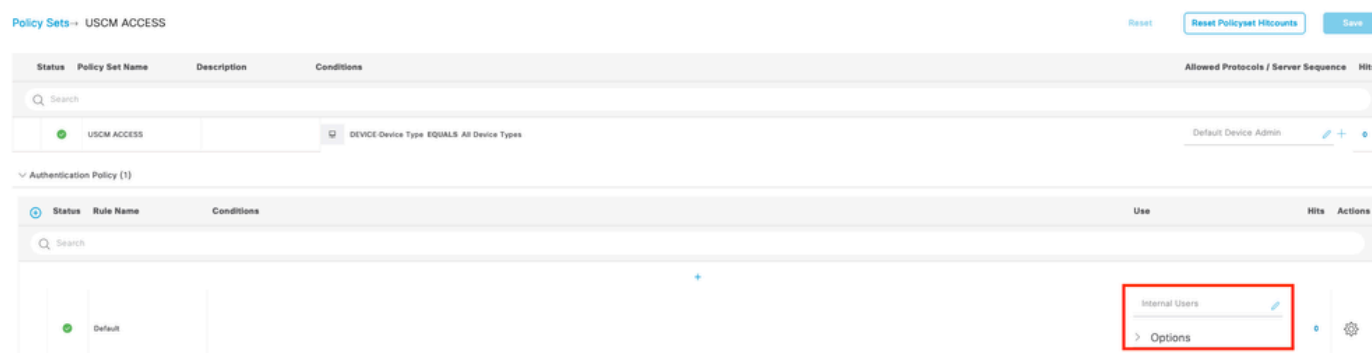
Insert new row above

ResetSave

Paso 5. Asigne un nombre a este nuevo conjunto de políticas, agregue condiciones en función de las características de las autenticaciones TACACS+ que se están realizando desde el servidor UCSM y seleccione como Protocolos permitidos > Administrador de dispositivos predeterminado, guarde su configuración.

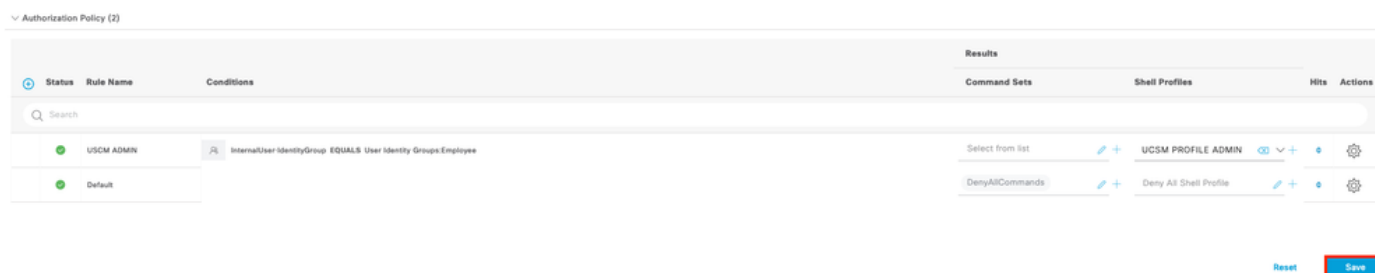


Paso 6. Seleccione en la opción > view y seleccione en la sección Authentication Policy, el origen de identidad externo desde el que ISE consulta el nombre de usuario y las credenciales que se introducen en UCSM; en este ejemplo, las credenciales corresponden a los usuarios internos almacenados en ISE.



Paso 7. Desplácese hacia abajo hasta la sección denominada Authorization Policy hasta la política Default, seleccione el icono de engranaje y luego inserte una regla.

Paso 8. Asigne un nombre a la nueva regla de autorización, agregue condiciones relativas al usuario que ya se han autenticado como pertenencia a un grupo y, en la sección Perfiles de shell, agregue el perfil TACACS que configuró anteriormente y guarde la configuración.



Configuración de TACACS+ en UCSM

Inicie sesión Cisco UCS Manager en la GUI con un usuario con privilegios de administrador.

Crear funciones para usuarios

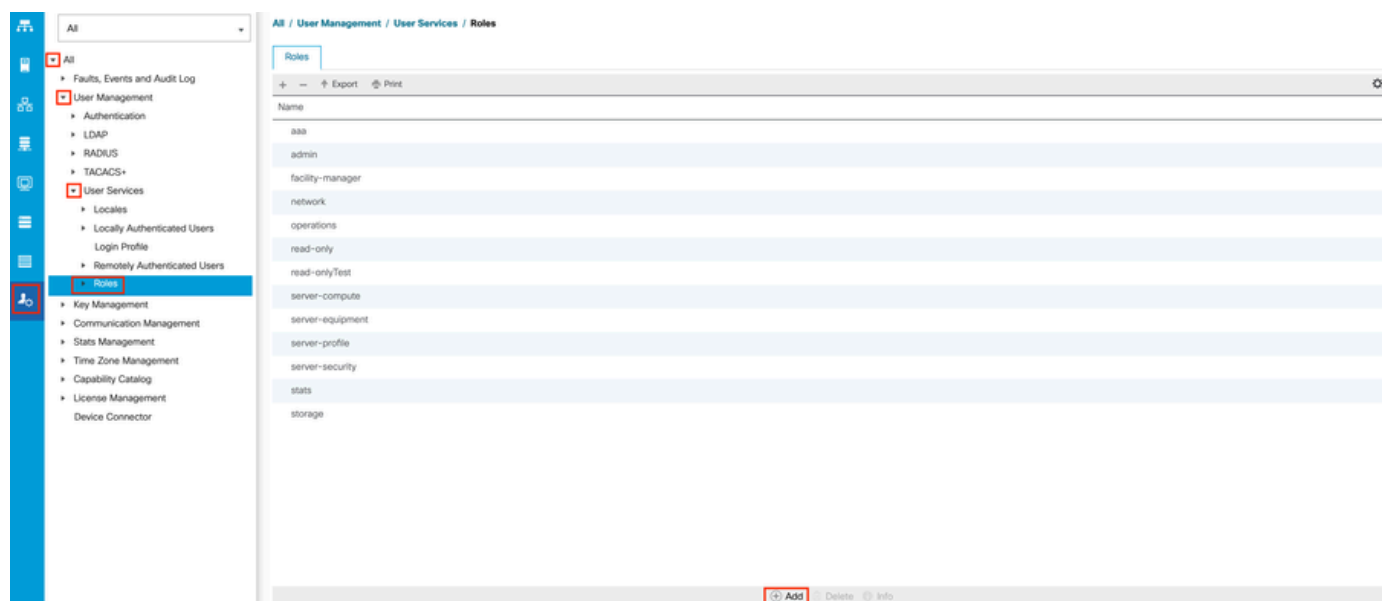
Paso 1. En el panel de navegación, seleccione la ficha Admin.

Paso 2. En la pestaña Admin, expanda All > User Management > User Services > Roles.

Paso 3. En el panel, seleccione la ficha General.

Paso 4. Seleccione Agregar para roles personalizados. Este ejemplo utiliza Roles predeterminados.

Paso 5. Verifique las coincidencias del rol de nombre con el nombre configurado previamente en el perfil TACACS+.



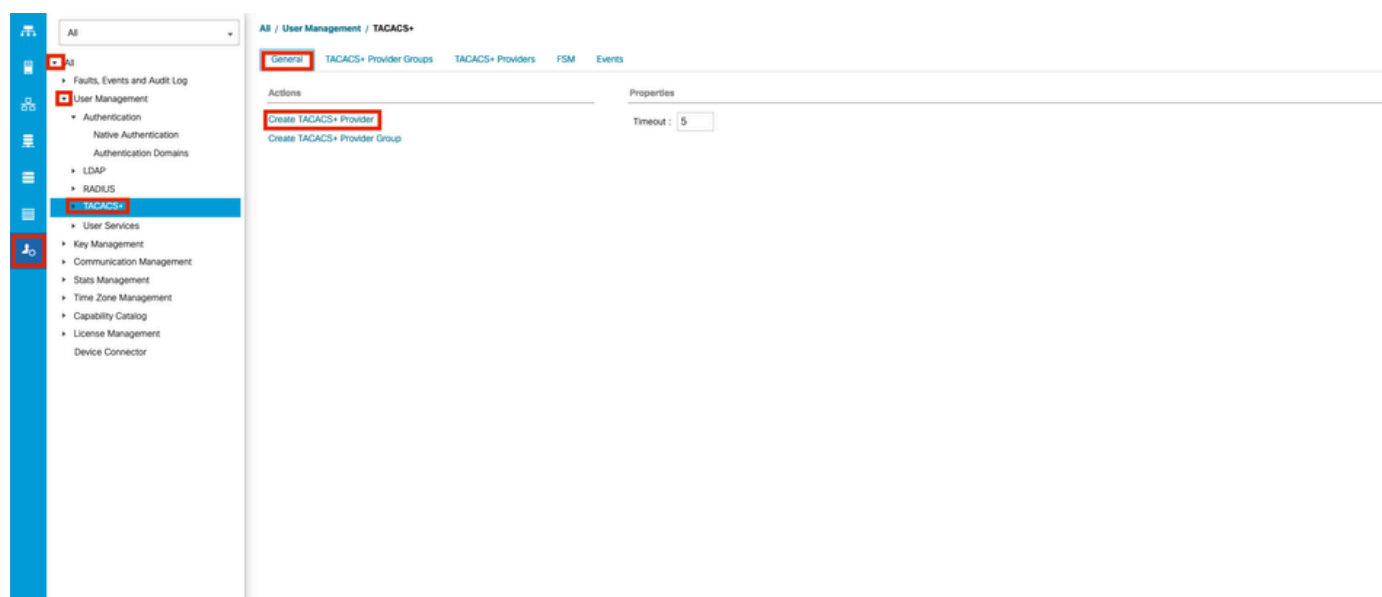
Crear un proveedor TACACS+

Paso 1. En el panel de navegación, seleccione la ficha Admin.

Paso 2. En la pestaña Admin, expanda All > User Management > TACACS+.

Paso 3. En el panel, seleccione la pestaña que General desee.

Paso 4. En la acción del área, seleccione Create TACACS+ Provider.

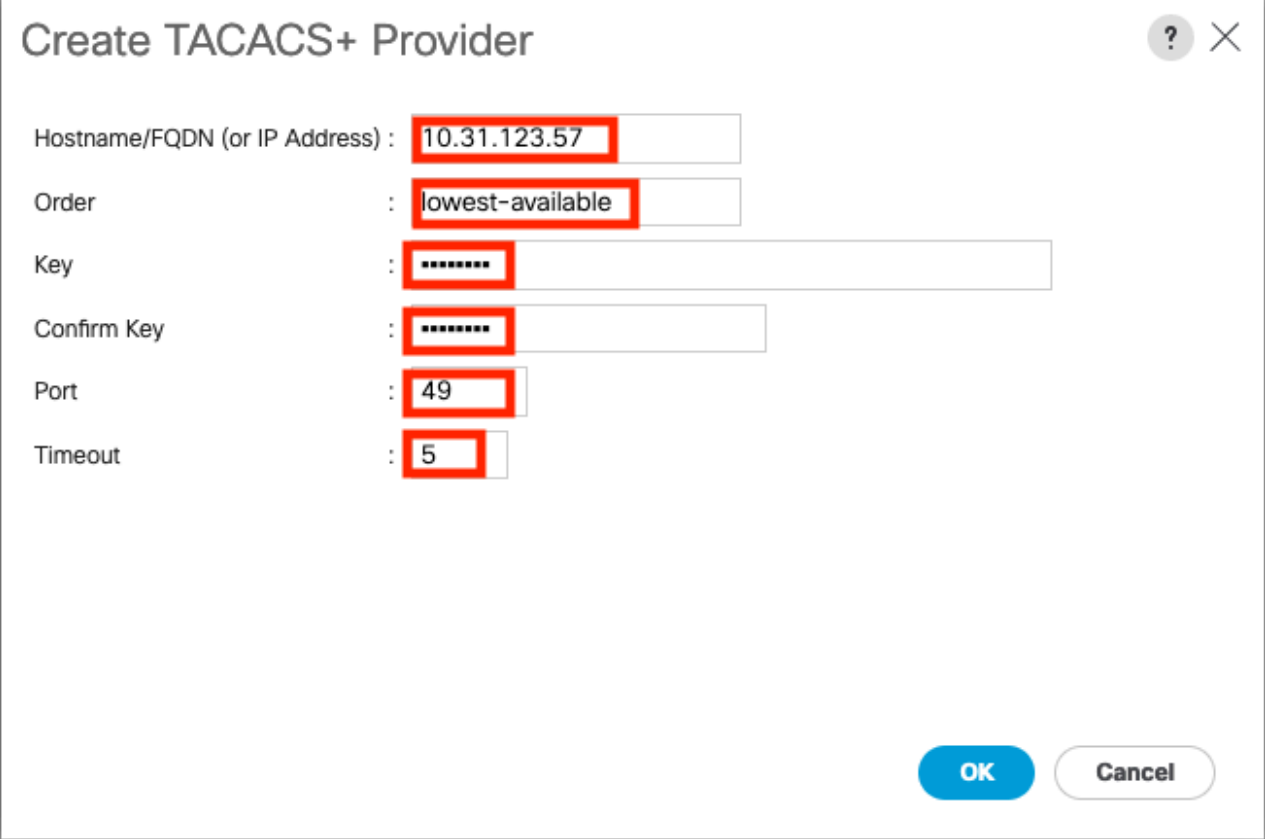


Paso 5. En la asistencia de Create TACACS+ Provider, introduzca la información correspondiente.

- En el campo Hostname, escriba la dirección IP o el nombre de host del servidor TACACS+.
- En el campo Pedido, el orden en el que Cisco UCS utiliza este proveedor para autenticar a los usuarios.

Introduzca un número entero entre 1 y 16, o bien introduzca el número más bajo disponible o 0 (cero) si desea que Cisco UCS asigne el siguiente pedido disponible en función de los otros proveedores definidos en esta instancia de Cisco UCS.

- En el campo Key, la clave de cifrado SSL para la base de datos.
- En el campo Confirm Key, la clave de cifrado SSL se repite con fines de confirmación.
- En el campo Puerto, el puerto a través del cual Cisco UCS se comunica con la base de datos TACACS+ (puerto predeterminado 49).
- En el campo Tiempo de espera, el tiempo en segundos que el sistema emplea para intentar contactar con la base de datos TACACS+ antes de que se agote el tiempo de espera.



Create TACACS+ Provider

Hostname/FQDN (or IP Address) : 10.31.123.57

Order : lowest-available

Key : *****

Confirm Key : *****

Port : 49

Timeout : 5

OK Cancel

Paso 6. Seleccione Aceptar.



Nota: Si utiliza un nombre de host en lugar de una dirección IP, debe configurar un servidor DNS en Cisco UCS Manager.

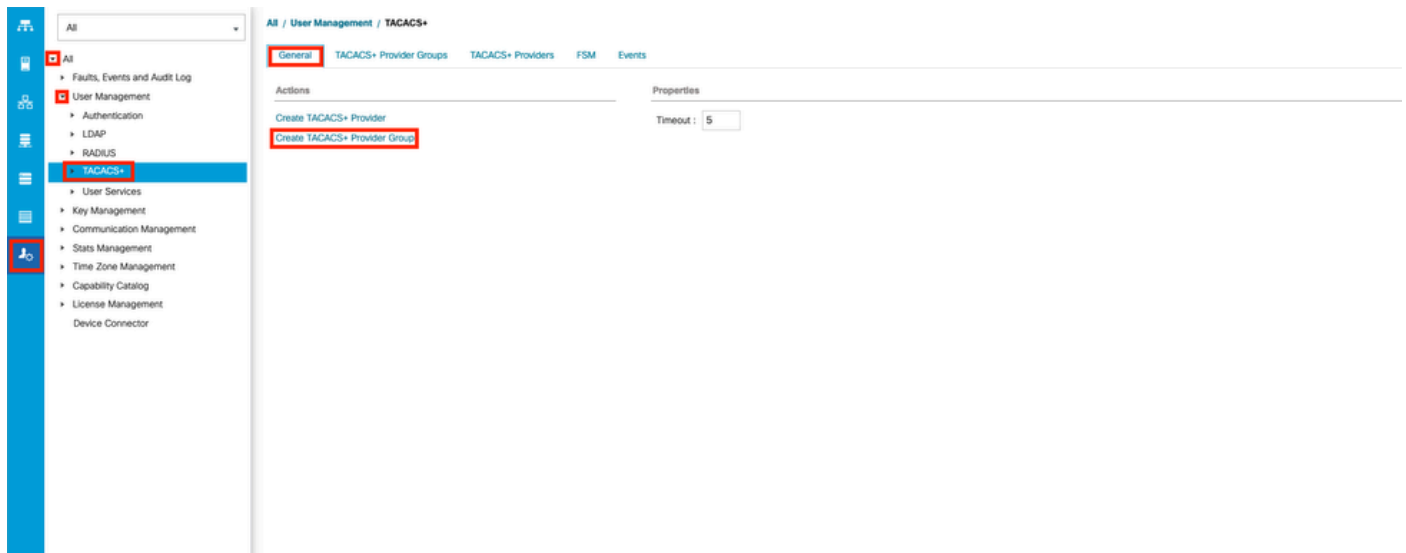
Crear un grupo de proveedores TACACS+

Paso 1. En **Navigation** el panel, seleccione la **Admin** ficha.

Paso 2. En **Admin** la ficha, expanda **All > User Management > TACACS+**.

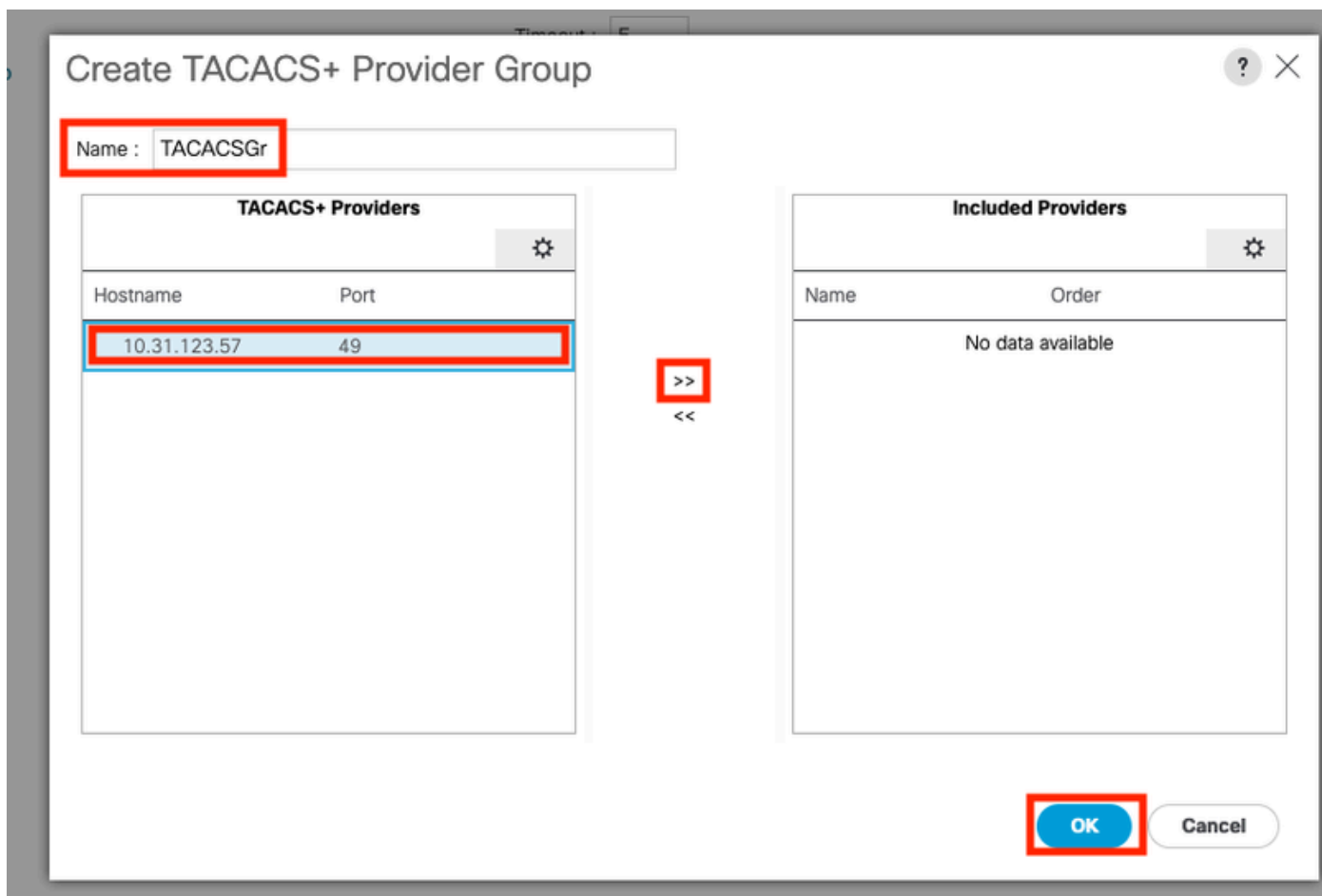
Paso 3. En **Work** el panel, seleccione la **General** pestaña.

Paso 4. En **Actions** el área, **Create TACACS+ Provider** seleccione **Grupo**.



Paso 5. En el cuadro de diálogo **Crear grupo de proveedores de TACACS+**, ingrese la información solicitada.

- En el campo **Nombre**, introduzca un nombre único para el grupo.
- En la tabla **Proveedores TACACS+**, elija los proveedores que se incluirán en el grupo.
- Seleccione el botón **>>** para agregar los proveedores a la tabla **Proveedores incluidos**.



Paso 6. Seleccione Aceptar.

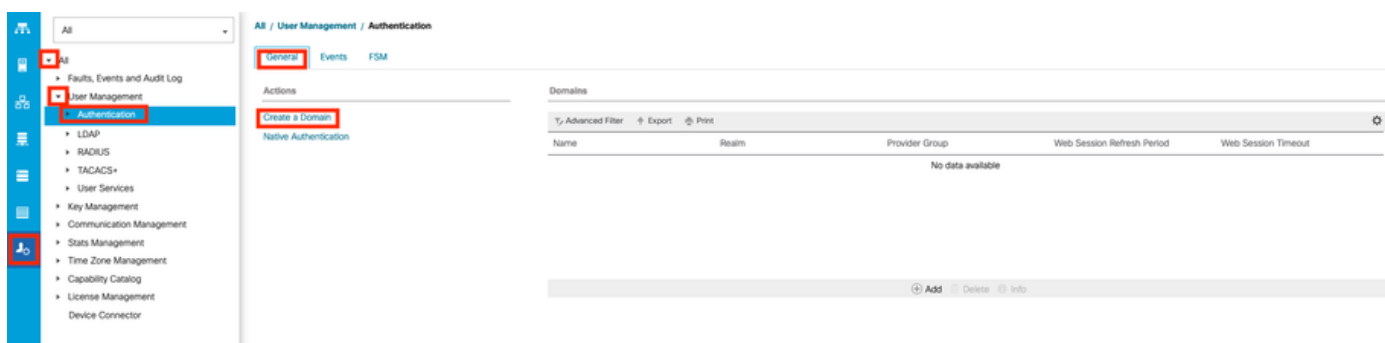
Crear un dominio de autenticación

Paso 1. En el Navigation panel, seleccione la Admin pestaña.

Paso 2. En la Admin ficha, expanda All > User Management > Authentication

Paso 3. EnWorkel panel, seleccione la General pestaña.

Paso 4. EnActionsel área, seleccioneCreate a Domain.



Paso 5. En el cuadro de diálogo Crear dominio, ingrese la información solicitada.

- En el campo Nombre, introduzca un nombre único para el dominio.
- En el rango, seleccione la opción Tacacs.

- En la lista desplegable Grupo de Proveedores, seleccione el grupo de proveedores TACACS+ creado anteriormente y seleccione Aceptar

Create a Domain

Name : TACACS

Web Session Refresh Period (sec) : 600

Web Session Timeout (sec) : 7200

Realm : ☐ Local ☐ Radius ☒ Tacacs ☐ Ldap

Provider Group : TACACSGr

Two Factor Authentication : ☐

OK Cancel

Troubleshoot

Problemas comunes de TACACS+ en UCSM

- Clave incorrecta o caracteres no válidos.
- Puerto Incorrecto.
- No hay comunicación con nuestro proveedor debido a una regla de firewall o proxy.
- FSM no es el 100%.

Verifique la configuración de UCSM TACACS+:

Debe asegurarse de que UCSM haya implementado la configuración. Para comprobar que el estado de la máquina de estado finito (FSM) aparece como 100% completado.

Verifique la configuración desde la línea de comandos de UCSM

```
<#root>
```

```
UCS-A#
```

```
scope security
```

```
UCS-A /security #
```

```
scope tacacs
```

UCS-A /security/tacacs #

show configuration

```
UCS-AS-MXC-P25-02-A# scope security
UCS-AS-MXC-P25-02-A /security # scope tacacs
UCS-AS-MXC-P25-02-A /security/tacacs # show configuration
scope tacacs
    enter auth-server-group TACACSGr
        enter server-ref 10.31.123.57
            set order 1
        exit
    exit
enter server 10.31.123.57
    set order 1
    set port 49
    set timeout 5
!    set key
    exit
    set timeout 5
exit
```

<#root>

UCS-A /security/tacacs #

show fsm status

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

FSM 1:
  Status: Nop
  Previous Status: Update Ep Success
  Timestamp: 2023-06-24T20:54:05.021
  Try: 0
  Progress (%): 100
  Current Task:
```

Verifique la configuración de Tacacs desde el NXOS:

<#root>

UCS-A#

connect nxos

UCS-A(nx-os)#

show tacacs-server

UCS-A(nx-os)#

show tacacs-server groups

```
[UCS-AS-MXC-P25-02-A# connect nxos
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2023, 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-A(nx-os)# show tacacs-server
timeout value:5
deadtime value:0
source interface:any available
Global Test Username:test
Global Test Password:*****
total number of servers:1

following TACACS+ servers are configured:
  10.31.123.57:
    available on port:49
    TACACS+ shared secret:*****
    timeout:5
[UCS-AS-MXC-P25-02-A(nx-os)# show tacacs-server groups
total number of groups:2

following TACACS+ server groups are configured:
  group tacacs:
    server 10.31.123.57 on port 49
    deadtime is 0
    vrf is management
  group TACACSGr:
    server 10.31.123.57 on port 49
    deadtime is 0
    vrf is management
```

Para probar la autenticación de NX-OS, utilice el `test aaa` comando (solo disponible en NX-OS).

Valide la configuración de su servidor:

<#root>

UCS-A(nx-os)#

test aaa server tacacs+

<TACACS+-server-IP-address or FQDN> <username> <password>

```
UCS-AS-MXC-P25-02-A# connect nxos
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2023, 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/librarv.txt.
UCS-AS-MXC-P25-02-A(nx-os)# test aaa server tacacs+ 10.31.123.57 operator Cisc0123
```

Revisión de UCSM

Verificación de disponibilidad

<#root>

UCS-A#

connect local-mgmt

UCS-A(local-mgmt)#

ping

<TACACS+-server-IP-address or FQDN>

```

UCS-AS-MXC-P25-02-A# connect local-mgmt
pCisco 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-A(local-mgmt)# ping 10.31.123.57
PING 10.31.123.57 (10.31.123.57) from 10.31.123.8 : 56(84) bytes of data.
64 bytes from 10.31.123.57: icmp_seq=1 ttl=64 time=0.347 ms
64 bytes from 10.31.123.57: icmp_seq=2 ttl=64 time=0.309 ms

```

Verificación de puertos

<#root>

UCS-A#

connect local-mgmt

UCS-A(local-mgmt)#

telnet

<TACACS+-server-IP-address or FQDN> <Port>

```

UCS-AS-MXC-P25-02-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-A(local-mgmt)# telnet 10.31.123.57 49
Trying 10.31.123.57...
Connected to 10.31.123.57.
Escape character is '^]'.

```

El método más efectivo para ver errores es habilitar la depuración de NXOS, con esta salida puede ver los grupos, la conexión y el mensaje de error que causa la mala comunicación.

- Abra una sesión SSH en UCSM e inicie sesión con cualquier usuario con privilegios con permisos de administrador (preferiblemente un usuario local), cambie al contexto de la CLI de NX-OS e inicie el monitor de terminal.


```
<#root>
```

```
UCS-A#
```

```
connect nxos
```

```
UCS-A(nx-os)#
```

```
terminal monitor
```

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

```
<#root>
```

```
UCS-A(nx-os)#
```

```
debug aaa all
```

```
UCS-A(nx-os)#
```

```
debug aaa aaa-request
```

```
UCS-A(nx-os)#
```

```
debug tacacs+ aaa-request
```

```
UCS-A(nx-os)#
```

```
debug tacacs+ aaa-request-lowlevel
```

```
UCS-A(nx-os)#
```

```
debug tacacs+ all
```

```

UCS-AS-MXC-P25-02-A# connect nxos
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2023, 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-A(nx-os)# terminal monitor
UCS-AS-MXC-P25-02-A(nx-os)# debug tacacs+ all
2023 Jun 26 04:42:22.104286 tacacs: event_loop(): calling process_rd_fd_set
2023 Jun 26 04:42:22.104311 tacacs: process_rd_fd_set: calling callback for fd 6
2023 Jun 26 04:42:22.104341 tacacs: fsrv didnt consume 182 opcode
2023 Jun 26 04:42:22.104994 tacacs: mts_message_handler: sdwrap_process_msg
2023 Jun 26 04:42:22.105011 tacacs: process_rd_fd_set: callback returned for fd 6
UCS-AS-MXC-P25-02-A(nx-os)# debug aaa all

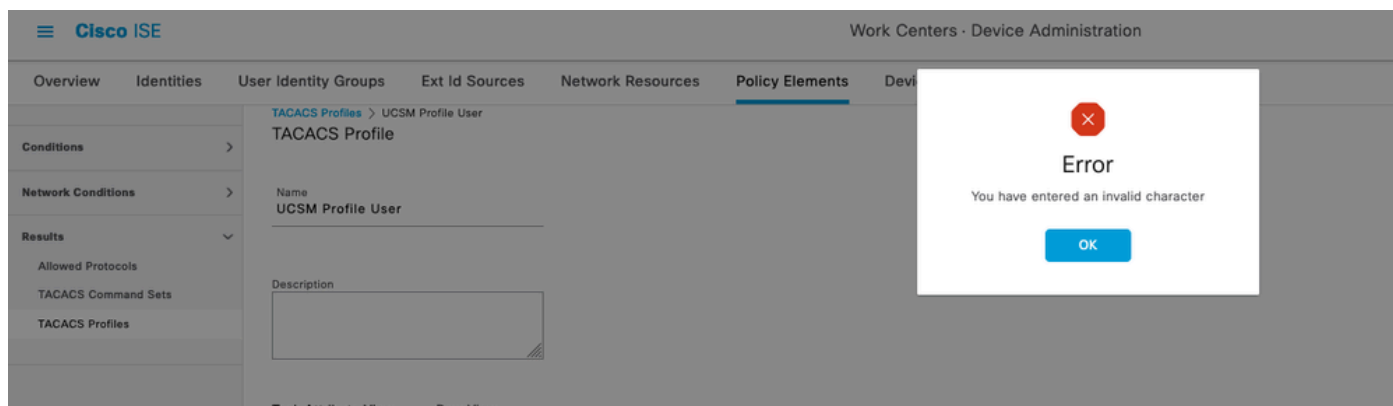
```

- Ahora abra una nueva sesión GUI o CLI e intente iniciar sesión como usuario remoto (TACACS+).
- Una vez que haya recibido un mensaje de error de inicio de sesión, desactive los debugs que cierran la sesión o con este comando.

```
UCS-A(nx-os)# undebug all
```

Problemas comunes de TACAC en ISE

- En ISE, este comportamiento se muestra al intentar configurar un perfil tacacs en los atributos necesarios para que UCSM asigne los roles correspondientes a admin o a cualquier otro rol. Seleccione en el botón save (guardar) y verá este comportamiento:



Este error se debe al siguiente bug <https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwc91917> ,

por favor asegúrese de que tiene donde se ha solucionado este defecto.

Revisión de ISE

Paso 1. Revise si el servicio TACACS+ se está ejecutando, esto se puede registrar:

- GUI: Revise si tiene el nodo enumerado con el servicio DEVICE ADMIN en Administration > System > Deployment.
- CLI: Ejecute el comando show ports | incluir 49 para confirmar que hay conexiones en el puerto TCP que pertenecen a TACACS+

```
<#root>
```

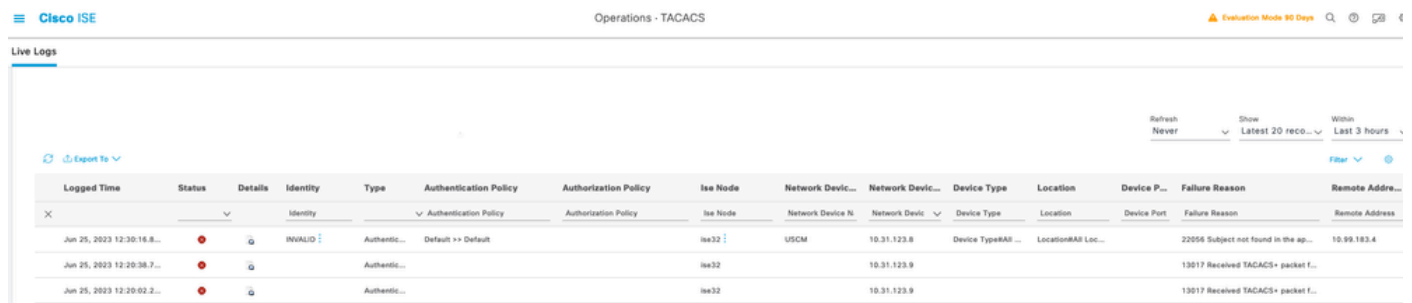
```
ise32/admin#
```

```
show ports | include 49
```

```
tcp: 169.254.4.1:49, 169.254.2.1:49, 169.254.4.1:49, 10.31.123.57:49
```

Paso 2. Confirme si hay registros de vida relacionados con intentos de autenticación TACACS+ : esto se puede verificar en el menú Operaciones > TACACS > Live logs ,

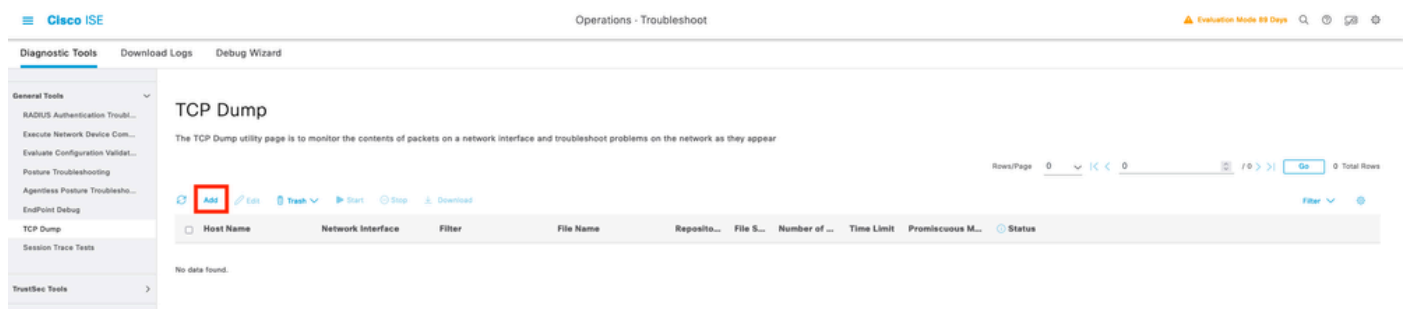
Dependiendo del motivo del fallo, puede ajustar la configuración o abordar la causa del fallo.



The screenshot shows the 'Live Logs' page in Cisco ISE. The table displays authentication attempts with columns for Logged Time, Status, Details, Identity, Type, Authentication Policy, Authorization Policy, Ise Node, Network Device, Device Type, Location, Device Port, Failure Reason, and Remote Address. The first row shows a failed attempt with status 'INVALID' and failure reason '22058 Subject not found in the ap...'. The second row shows a successful attempt with status 'Authenticated' and failure reason '13017 Received TACACS+ packet f...'. The third row shows another successful attempt with status 'Authenticated' and failure reason '13017 Received TACACS+ packet f...'.

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device	Network Device	Device Type	Location	Device P...	Failure Reason	Remote Address
Jun 25, 2023 12:30:16.8...	INVALID		INVALID	Authentic...	Default >> Default	Authorization Policy	ise32	USCM	10.31.123.8	Device TypeRAI...	LocationRAI Loc...		22058 Subject not found in the ap...	10.99.183.4
Jun 25, 2023 12:20:38.7...	Authenticated			Authentic...			ise32		10.31.123.9				13017 Received TACACS+ packet f...	
Jun 25, 2023 12:20:02.2...	Authenticated			Authentic...			ise32		10.31.123.9				13017 Received TACACS+ packet f...	

Paso 3. En caso de que no vea ningún livelog, proceda a tomar una captura de paquetes navegue hasta el menú Operaciones > Troubleshooting > Herramientas de diagnóstico > Herramientas generales > TCP Dump , seleccione on add



The screenshot shows the 'TCP Dump' configuration page in Cisco ISE. The page has a sidebar with 'Diagnostic Tools' and 'Download Logs'. The main area is titled 'TCP Dump' and contains a table for configuring the dump. The table has columns for Host Name, Network Interface, Filter, File Name, Repository, File S..., Number of ..., Time Limit, Promiscuous M..., and Status. The 'Add' button is highlighted with a red box.

Host Name	Network Interface	Filter	File Name	Repository	File S...	Number of ...	Time Limit	Promiscuous M...	Status
No data found.									

Seleccione el nodo de Servicio de políticas desde el que UCSM envía la autenticación y, a continuación, en los filtros, proceda a introducir ip host X.X.X.X correspondiente a la IP de UCSM

desde la que se envía la autenticación, asigne un nombre a la captura y desplácese hacia abajo para guardarla, ejecute la captura e inicie sesión desde UCSM .

Cisco ISE Operations - Troubleshoot

Diagnostic Tools Download Logs Debug Wizard

General Tools

- RADIUS Authentication Troubl...
- Execute Network Device Com...
- Evaluate Configuration Validat...
- Posture Troubleshooting
- Agentless Posture Troublesho...
- EndPoint Debug

TCP Dump

Session Trace Tests

TrustSec Tools

TCP Dump > New

Add TCP Dump

Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.

Host Name*
ise32

Network Interface*
GigabitEthernet 0 [Up, Running]

Filter
ip host 10.31.123.7
E.g: ip host 10.77.122.123 and not 10.177.122.119

File Name
taccap

Repository

File Size
10 Mb

Limit to
1 File(s)

Time Limit
5 Minute(s)

☐ Promiscuous Mode

Cancel Save **Save and Run**

Paso 4. Habilite el componente Runtime-AAA en debug dentro de PSN desde donde se realiza la autenticación en Operaciones > Troubleshooting > Debug Wizard > Debug log configuration, seleccione el nodo PSN , luego seleccione next en edit button .

Cisco ISE Operations - Troubleshoot

Diagnostic Tools Download Logs **Debug Wizard**

Debug Profile Configuration

Debug Log Configuration


Node List

Edit Reset to Default

Node Name	Replication Role
ise32	STANDALONE

Busque el componente runtime-AAA y cambie su nivel a debug para luego reproducir el problema

otra vez, y proceda a analizar los registros .



Operations · Troubleshoot

Diagnostic ToolsDownload LogsDebug Wizard

Debug Profile Configuration
Debug Log Configuration

Node List > ise32.example.com

Debug Level Configuration

 Edit  Reset to Default

	Component Name	Log Level	Description	Log file Name
	runtime-AAA	×		
<input type="radio"/>	runtime-AAA	DEBUG	AAA runtime messages (prrt)	prrt-server.log



Nota: Para obtener más información, consulte el vídeo en el canal de Cisco Youtube How to Enable Debugs on ISE 3.x Versions <https://www.youtube.com/watch?v=E3USz8B76c8>

Información Relacionada

[Guía de administración de Cisco UCS Manager](#)

[Guía de configuración de Cisco UCS CIMC TACACS+](#)

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).