Configurar o domínio de autenticação TACACS+ no UCS Manager com o servidor ISE

Contents

Introdução

Este documento descreve a configuração da autenticação do Terminal Access Controller Access-Control System Plus (TACACS+) no Unified Compute System Manager (UCSM). O TACACS+ é um protocolo de rede usado para serviços de Autenticação, Autorização e Responsabilidade (AAA) , que fornece um método centralizado para gerenciar Dispositivos de Acesso à Rede (NAD), onde você pode administrar e criar regras através de um servidor, neste cenário de caso de uso, estamos usando o Identity Services Engine (ISE).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

Componentes Utilizados

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

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

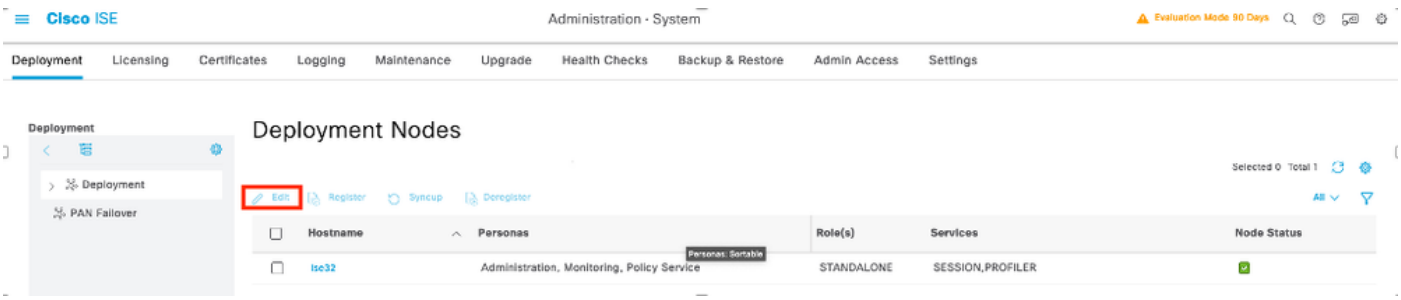
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configuração

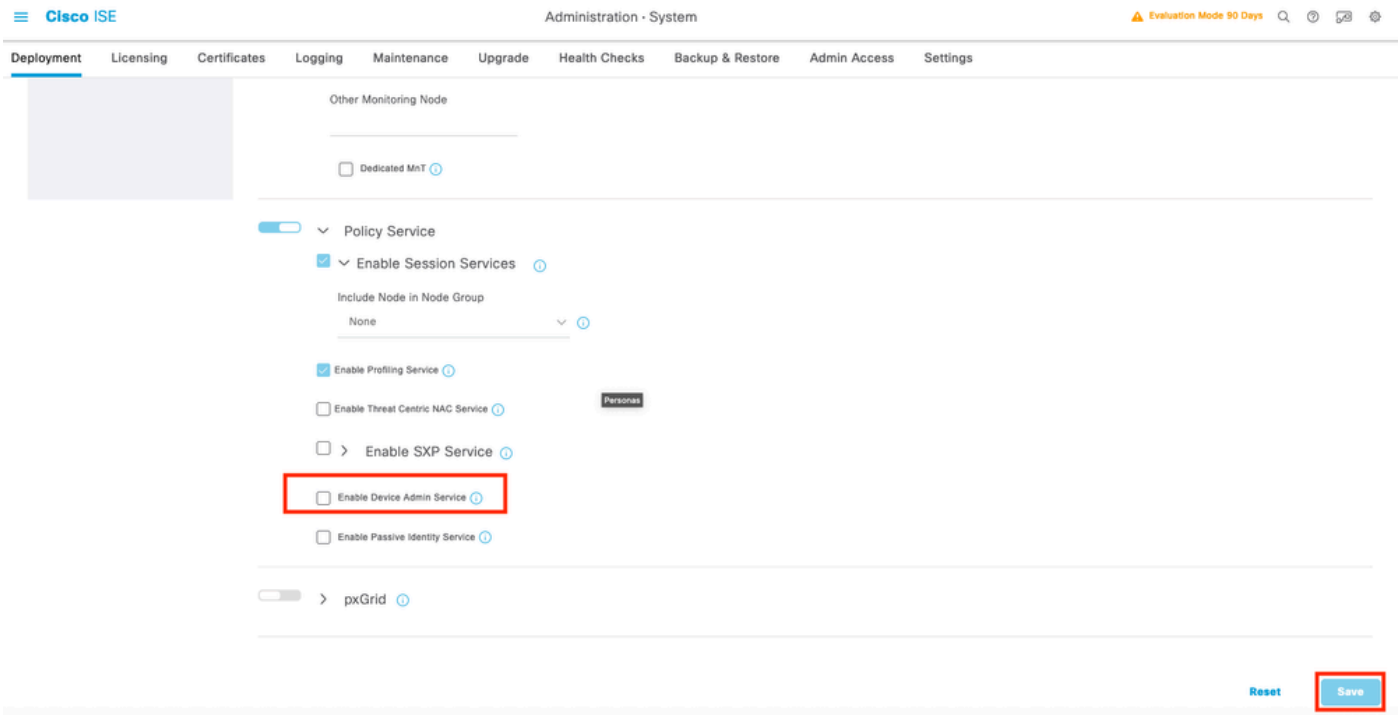
Configuração TACACS+ no ISE

Configuração de TACACS+ no ISE

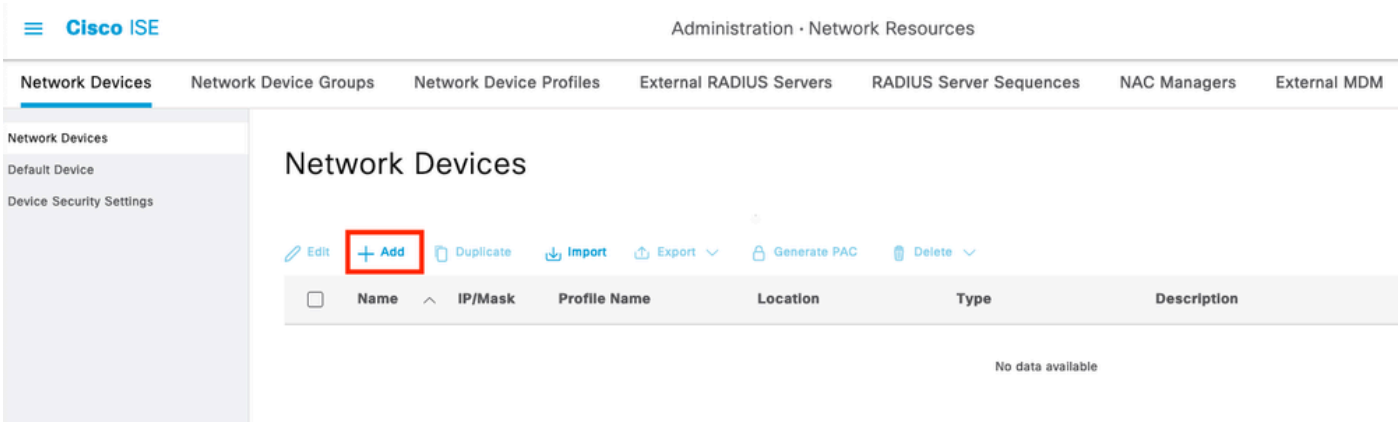
Etapa 1. A primeira tarefa é revisar se o ISE tem os recursos corretos para lidar com autenticações TACACS+ para tal você precisa verificar se dentro do Policy Service Node (PSN) desejado você tem o recurso para Device Admin Service, navegue através do menu Administração > Sistema > Implantação, selecione o nó onde o ISE executa TACACS+ e, em seguida, selecione o botão editar.



Etapa 2. Role para baixo até ver o recurso correspondente chamado Device Administration Service (observe que, para que esse recurso seja habilitado, você precisa primeiro ter o Policy Server persona habilitado no nó e, além disso, ter licenças para TACACS+ disponíveis em sua implantação), marque essa caixa de seleção e salve a configuração:

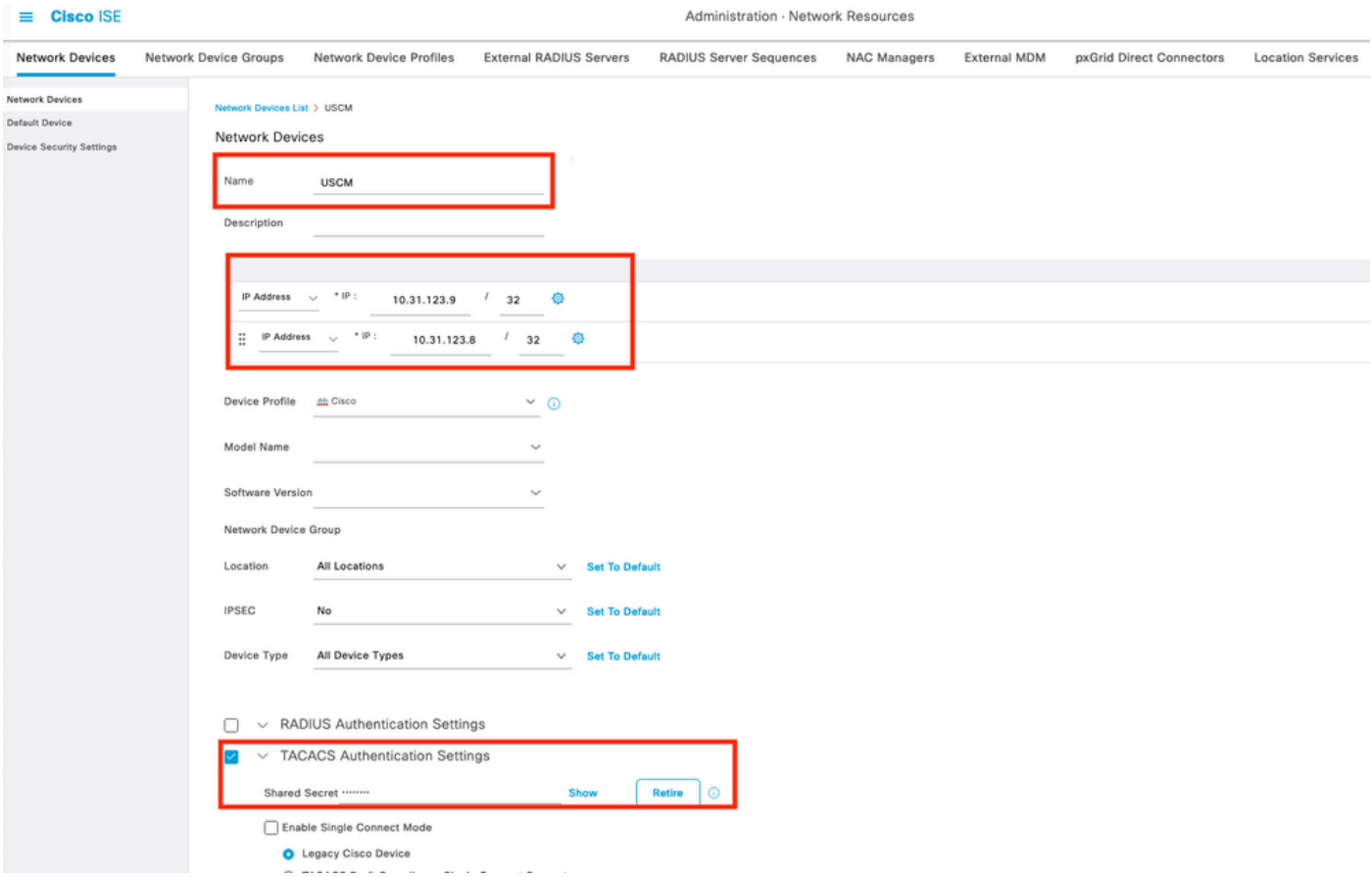


Etapa 3. Configure o dispositivo de acesso à rede (NAD) que usa o ISE como TACACS+ como servidor, navegue até o menu Administração > Recursos de rede > Dispositivos de rede e selecione o botão +Adicionar.



Etapa 4. Nesta seção, configure :

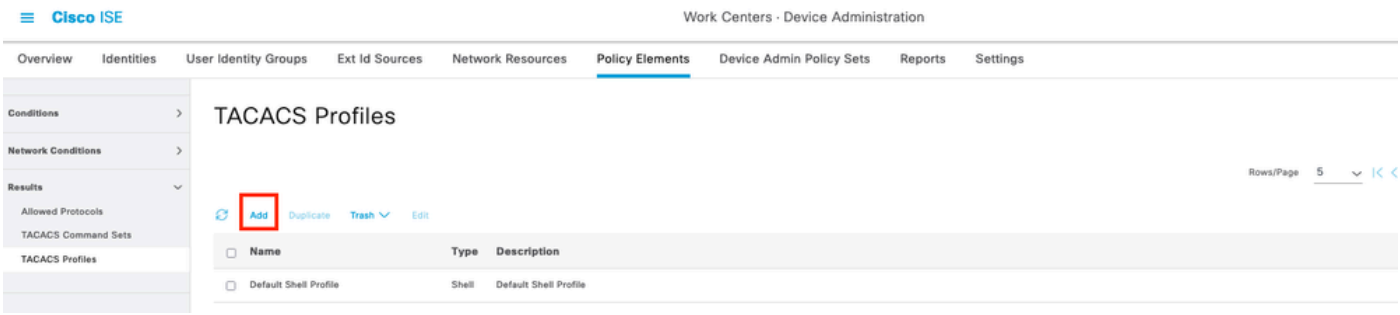
- Um nome para que o UCSM seja o cliente TACACS+.
- Os endereços IP que o UCSM usa para enviar solicitações ao ISE.
- Segredo compartilhado TACACS+, esta é a senha que deve ser usada para criptografar os pacotes entre o UCSM e o ISE



Note: Para uma configuração de cluster, adicione os endereços IP da porta de gerenciamento para ambas as interconexões de estrutura. Essa configuração garante que os usuários remotos possam continuar a fazer login se a primeira interconexão de estrutura falhar e o sistema falhar na segunda interconexão de estrutura. Todas as solicitações de login são originadas desses endereços IP, não do endereço IP virtual usado pelo Cisco UCS Manager.

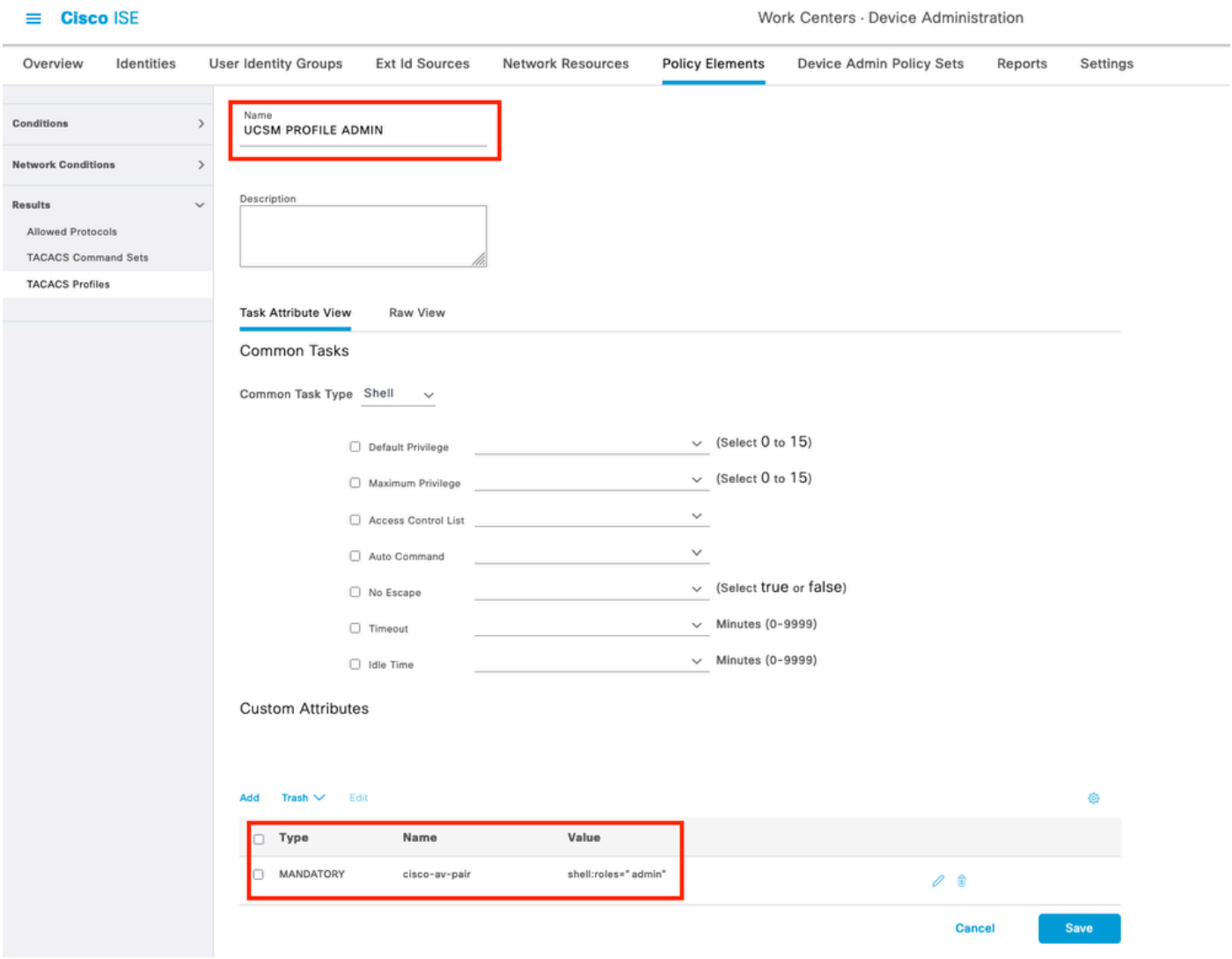
Configurar os atributos e as regras no ISE

Etapa 1. Crie um perfil TACACS+, navegue até o menu Centros de trabalho > Administração de dispositivo > Elementos de política > Resultados > Perfis TACACS e selecione Adicionar

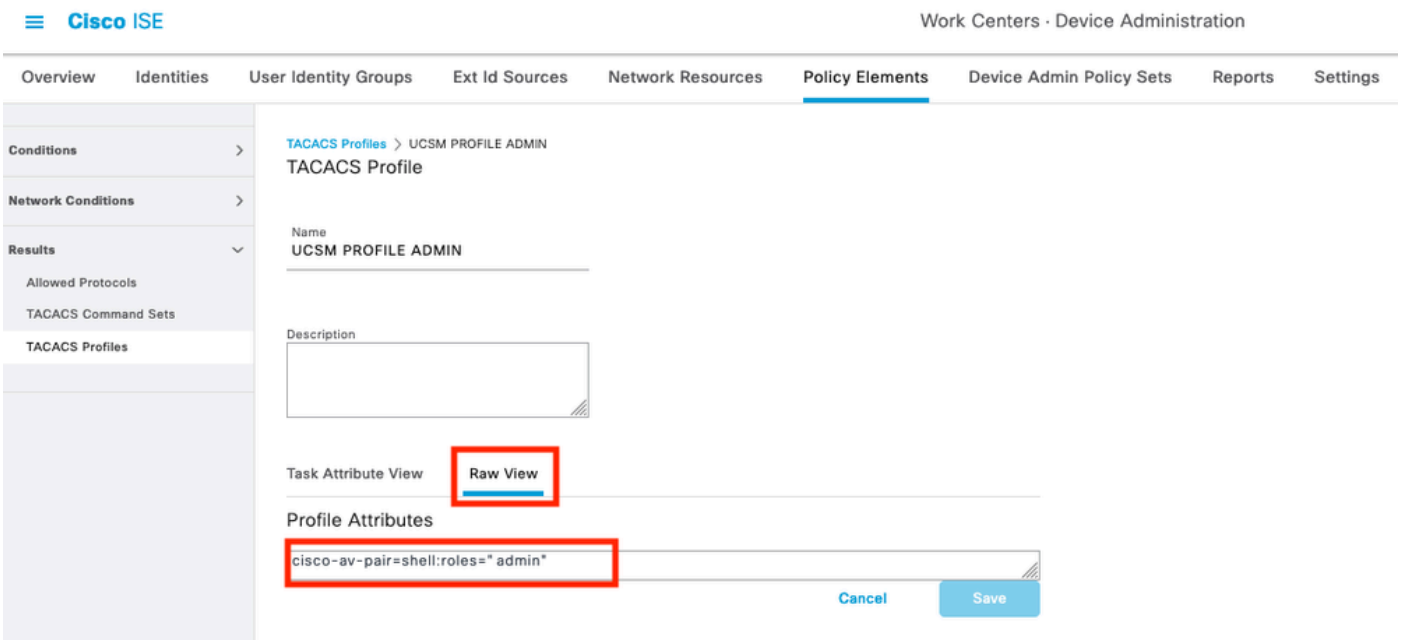


Etapa 2. Nesta seção, configure o perfil com um nome e, na seção Custom Attributes, selecione Add , em seguida, crie um atributo da característica MANDATORY , nomeie-o como cisco-av-pair

e, no valor, selecione uma das funções disponíveis no UCSM e insira como uma função de shell; neste exemplo, ele está usando a função admin e a entrada selecionada precisa ser shell:roles="admin" como mostrado aqui,



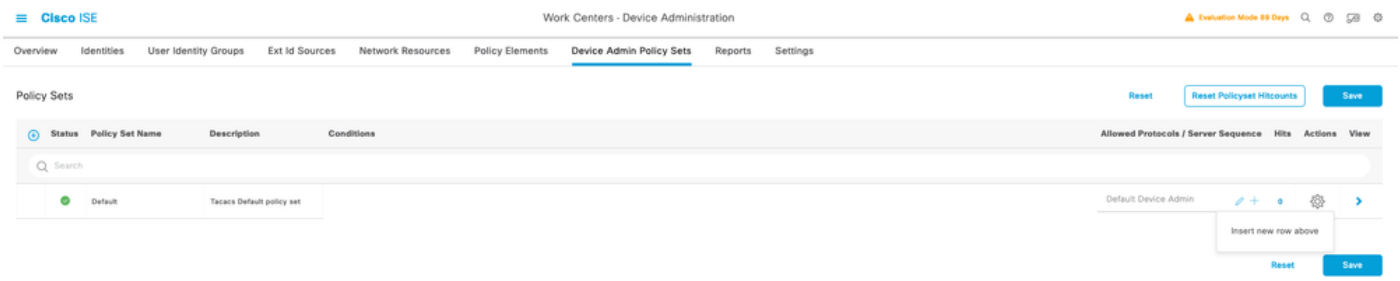
No mesmo menu, se você selecionar a visualização bruta para o perfil TACACS, você pode verificar a configuração correspondente do atributo que deve ser enviado através do ISE.



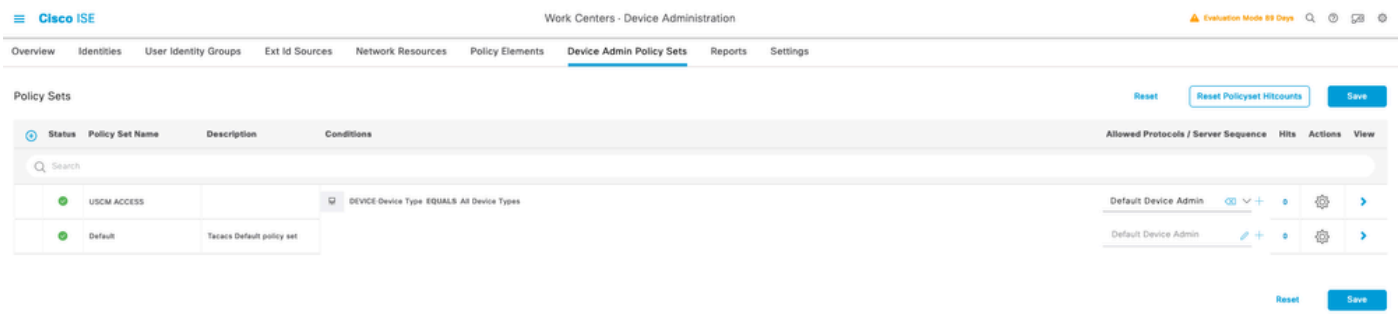
Note: O nome cisco-av-pair é a string que fornece a ID de atributo para o provedor TACACS+.

Etapa 3. Selecione na opção e salve sua configuração.

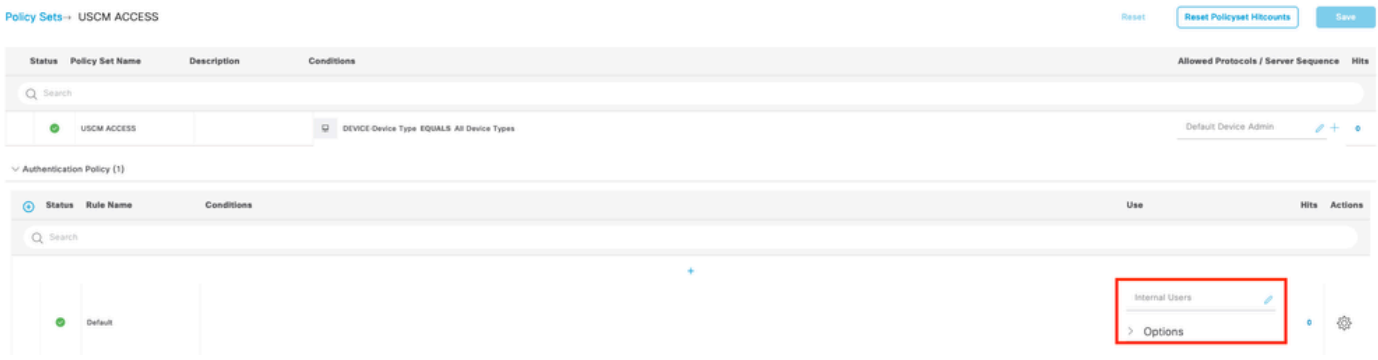
Etapa 4. Crie um Device Admin Policy Set a ser usado para o seu UCSM, navegue no menu Work Centers > Device Administration > Device Admin Policy Sets e, em seguida, em um conjunto de políticas existente, selecione o ícone de engrenagem para, em seguida, selecione Insert nova linha



Etapa 5. Nomeie este novo conjunto de políticas, adicione condições dependendo das características das autenticações TACACS+ que estão em andamento no servidor UCSM e selecione como Allowed Protocols > Default Device Admin, save sua configuração.

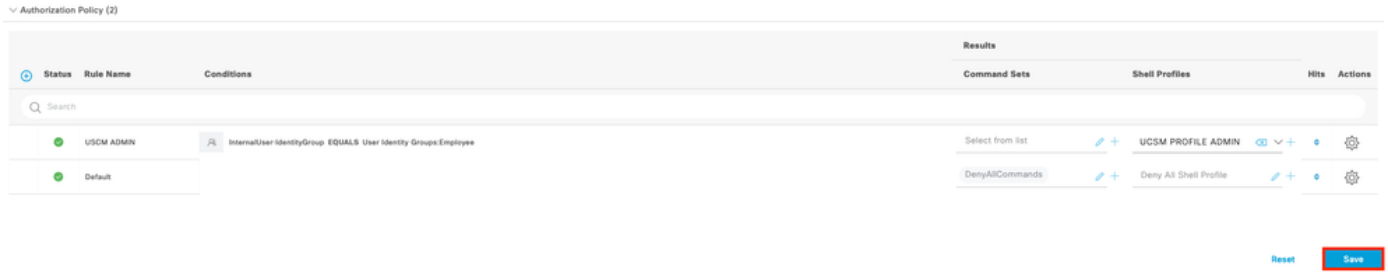


Etapa 6. Selecione na opção > exibir e selecione na seção Authentication Policy, a fonte de identidade externa de onde o ISE consulta o nome de usuário e as credenciais que são inseridas no UCSM, neste exemplo, as credenciais correspondem aos usuários internos armazenados no ISE.



Etapa 7. Role para baixo até a seção Authorization Policy até a Default policy, selecione o ícone de engrenagem e insira uma regra.

Etapa 8. Nomeie a nova Regra de Autorização, adicione condições referentes ao usuário que já está autenticado como membro do grupo e, na seção Perfis de shell, adicione o perfil TACACS que você configurou anteriormente, salve a configuração.



Configuração TACACS+ em UCSM

Faça login **Cisco UCS Manager**na GUI com um usuário com privilégios de administrador.

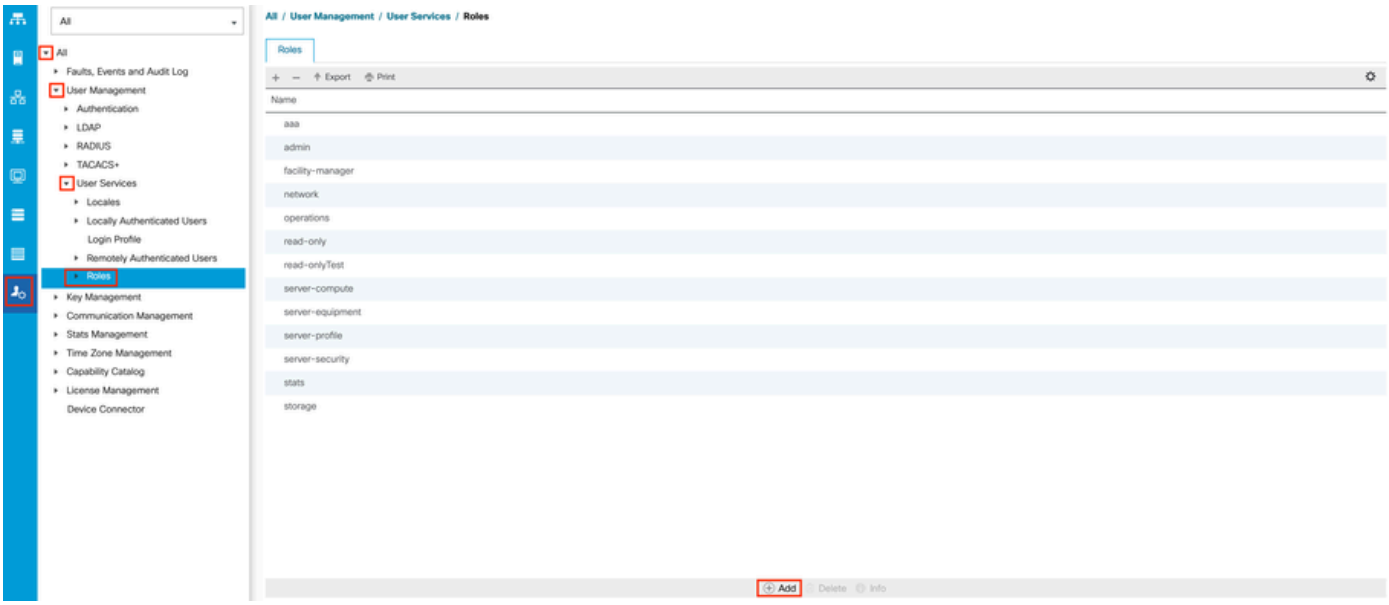
Criar funções para usuários

Etapa 1. No painel Navegação, selecione a guia Admin.
Etapa 2. Na guia Admin, expanda All > User Management >User Services > Roles.

Etapa 3. No**Work**painel, selecione**General**a guia.

Etapa 4. Selecione Add para funções personalizadas. Este exemplo usa Funções padrão.

Etapa 5. Verificar se a função de nome corresponde ao nome configurado anteriormente no perfil TACACS.

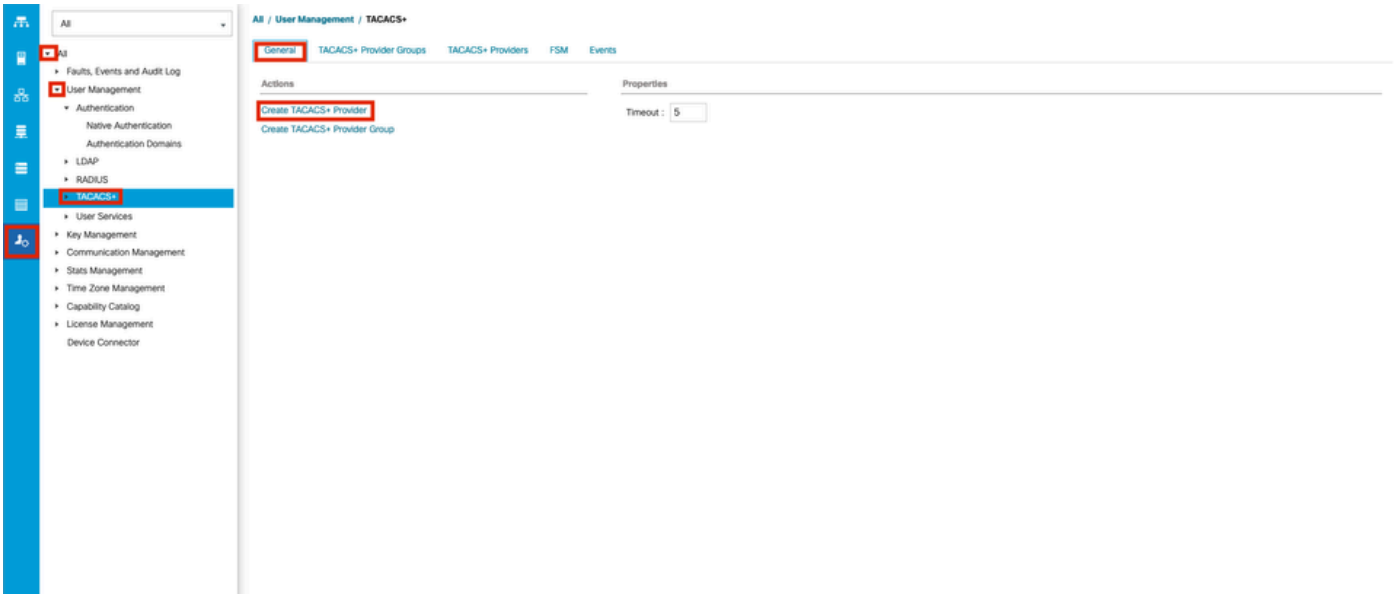


Criar um provedor TACACS+

Etapa 1. No painel Navegação, selecione a guia Admin.
Etapa 2. Na guia Admin, expanda All > User Management > TACACS+.

Etapa 3. No**Work**painel, selecione a guia .**General**.

Etapa 4. Na**Actions**área, selecione**Create TACACS+ Provider.**



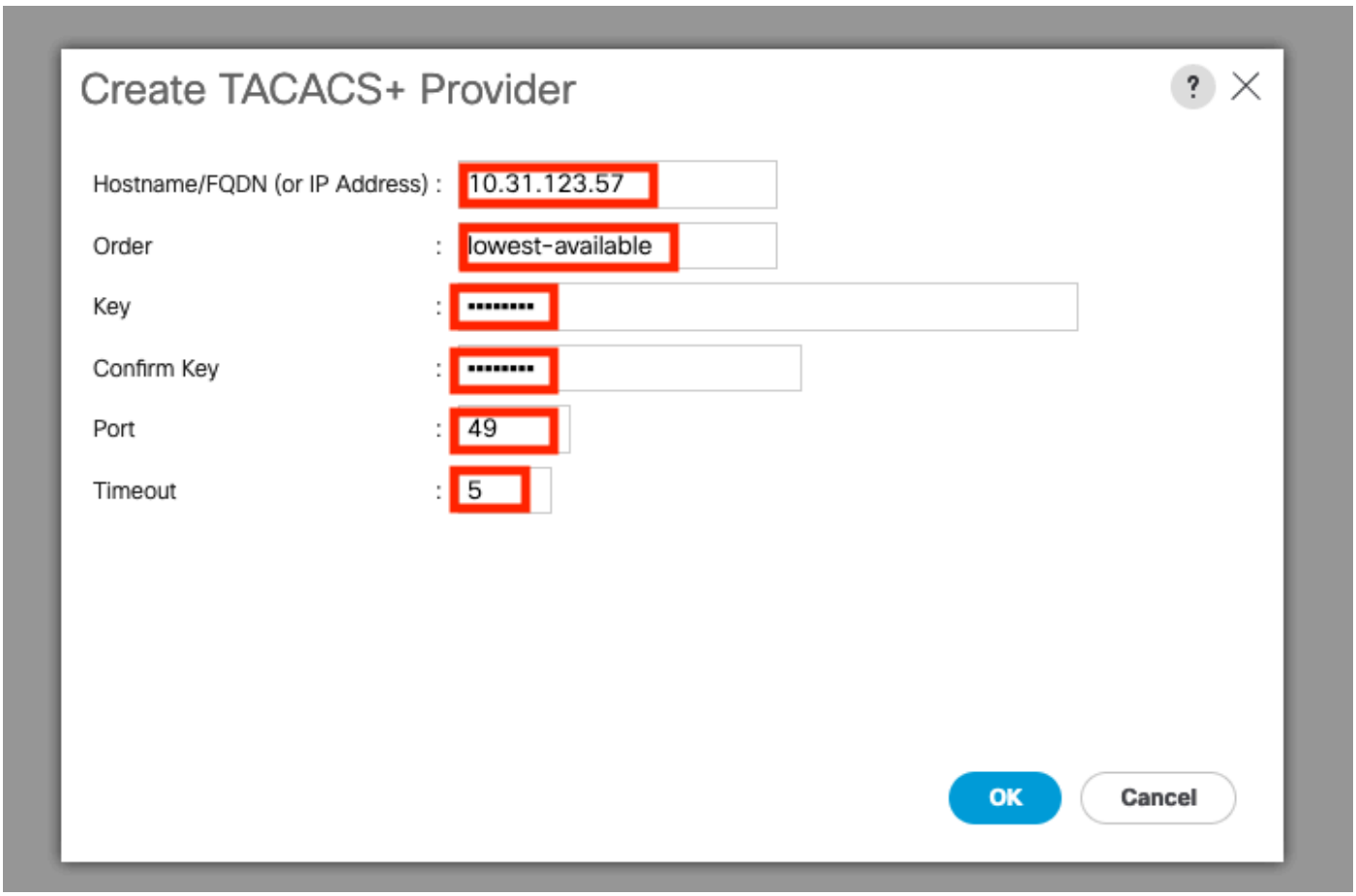
Etapa 5. No**Create TACACS+ Provider**assistente, insira as informações apropriadas.

- No campo Hostname, digite o endereço IP ou o nome de host do servidor TACACS+.
- No campo Pedido, A ordem na qual o Cisco UCS usa esse provedor para autenticar usuários.

  Insira um número inteiro entre 1 e 16, ou insira o menor disponível ou 0 (zero) se quiser que

o Cisco UCS atribua o próximo pedido disponível com base nos outros provedores definidos nesta instância do Cisco UCS.

- No campo Key, a chave de criptografia SSL do banco de dados.
- No campo Confirm Key, a chave de criptografia SSL é repetida para fins de confirmação.
- No campo Port, a porta pela qual o Cisco UCS se comunica com o banco de dados TACACS+ (porta padrão 49 da porta).
- No campo Timeout, o tempo em segundos que o sistema gasta tentando contatar o banco de dados TACACS+ antes que ele expire.



Etapa 6. Selecione Ok.

Note: Se você usar um nome de host em vez de um endereço IP, deverá configurar um servidor DNS no Cisco UCS Manager.

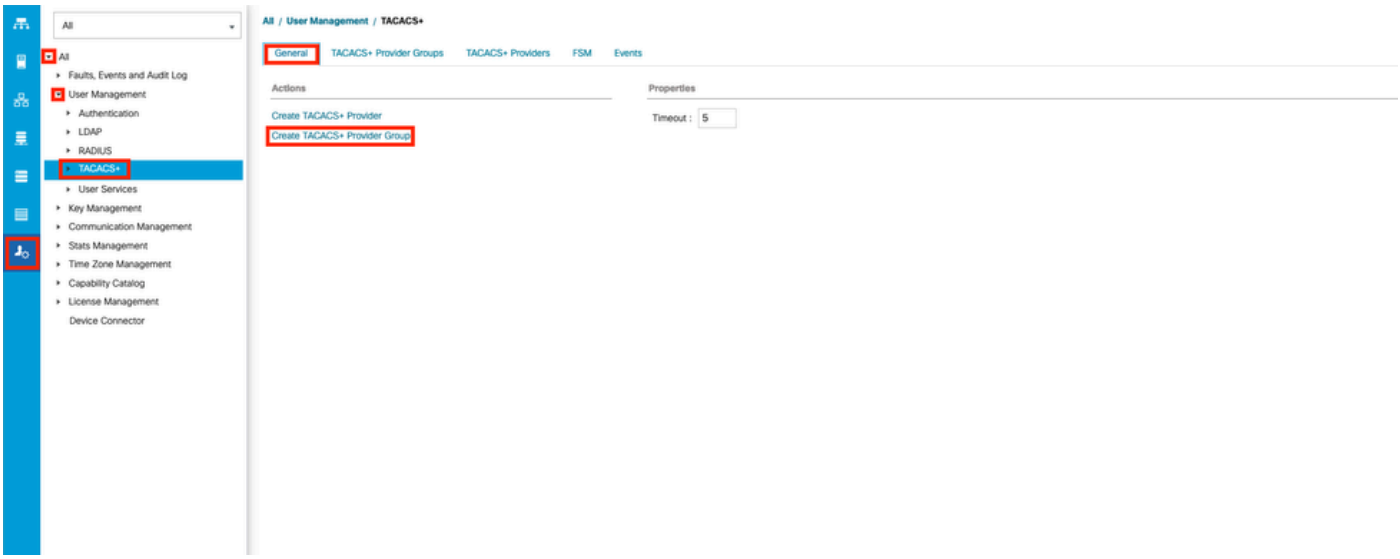
Criar um grupo de provedores TACAC+

Etapa 1.No**Navigation**painel, selecione a **Admin** guia.

Etapa 2. Na**Admin**guia, expanda **All** > **User Management** > **TACACS+**.

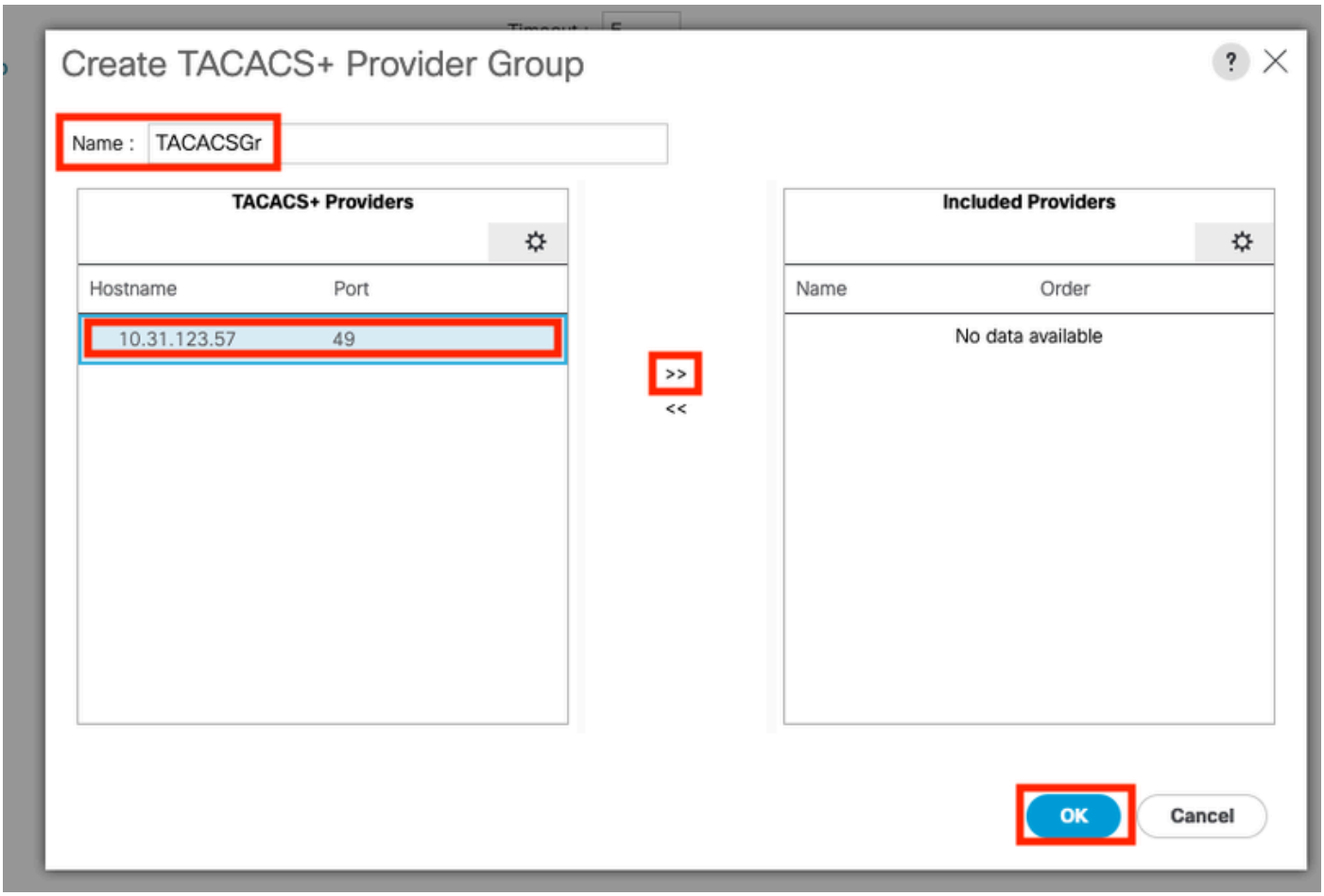
Etapa 3. No**Work**painel, selecione a **General** guia.

Etapa 4. Na**Actions**área, Create TACACS+ ProviderselecioneGroup.



Etapa 5. Na caixa de diálogo Create TACACS+ Provider Group, digite as informações solicitadas.

- No campo Nome, insira um nome exclusivo para o grupo.
- Na tabela Provedores TACACS+, escolha os provedores a serem incluídos no grupo.
- Selecione o botão >> para adicionar os provedores à tabela Provedores Incluídos.



Etapa 6. Selecione Ok.

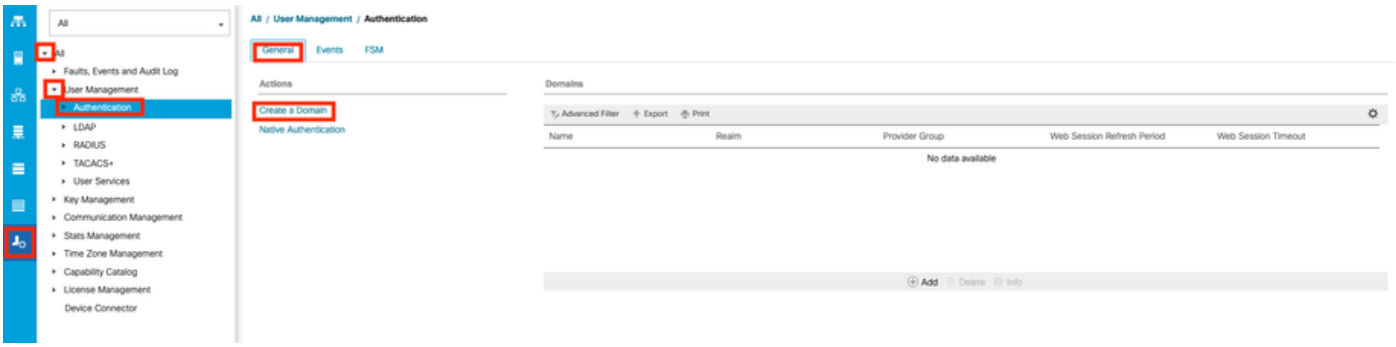
Criar um domínio de autenticação

Etapa 1. No **Navigation** painel, selecione a **Admin** guia.

Etapa 2. Na **Admin** guia, expanda **All** > **User Management** > **Authentication**

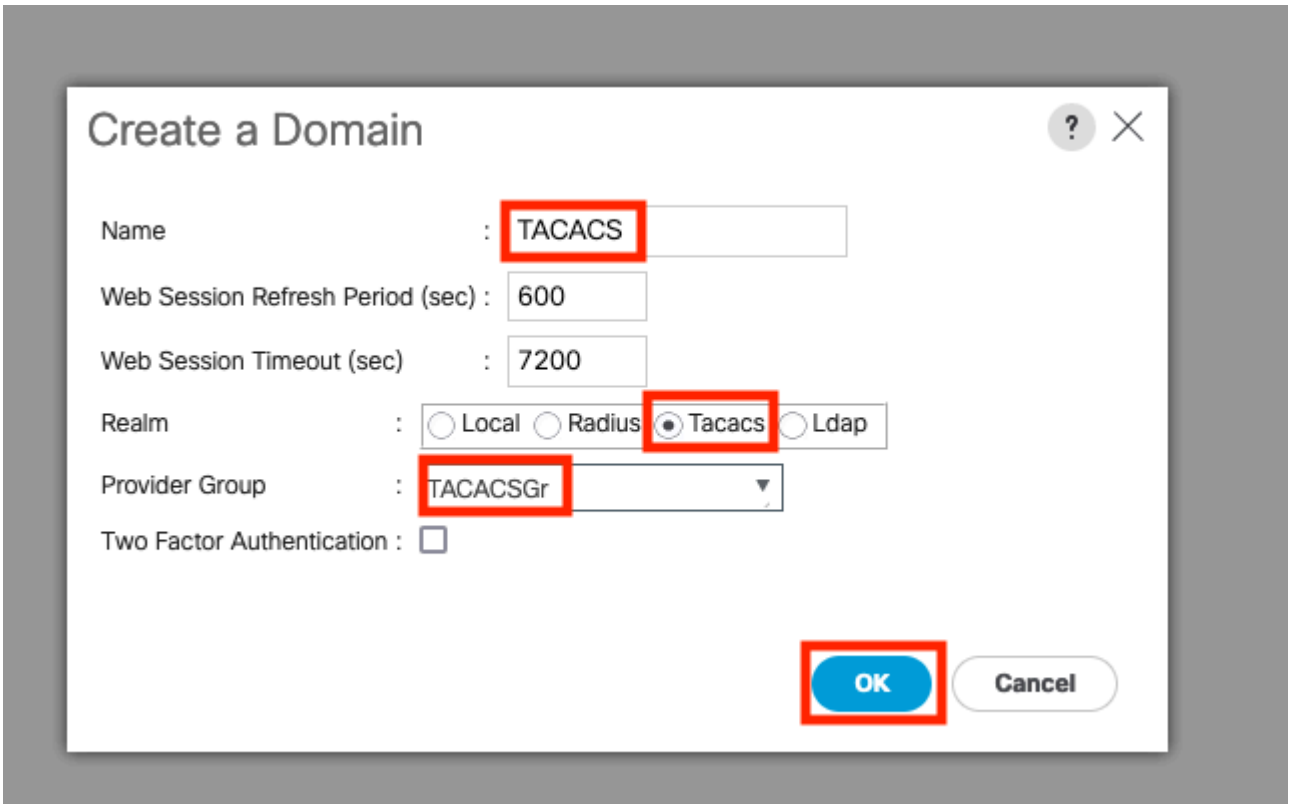
Etapa 3. No**Work**painel, selecione a **General** guia.

Etapa 4. Na**Actions**área, selecione**Create a Domain.**



Etapa 5. Na caixa de diálogo Create Domain, digite as informações solicitadas.

- No campo Nome, insira um nome exclusivo para o domínio.
- No Realm, selecione a opção Tacacs.
- Na lista suspensa Grupo do provedor, selecione o grupo do provedor TACACS+ criado anteriormente e selecione OK



Troubleshooting

Problemas comuns de TACACS+ no UCSM

- Chave incorreta ou caracteres inválidos.
- Porta Errada.
- Não há comunicação com nosso provedor devido a uma regra de Firewall ou Proxy.
- FSM não é 100%.

Verifique a configuração UCSM TACACS+:

Você deve garantir que o UCSM implementou a configuração, verificando se o status da Máquina de Estado Finito (FSM) é mostrado como 100% concluído.

Verifique a configuração a partir da linha de comando do 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 a configuração Tacacs do NXOS:

<#root>

UCS-A#

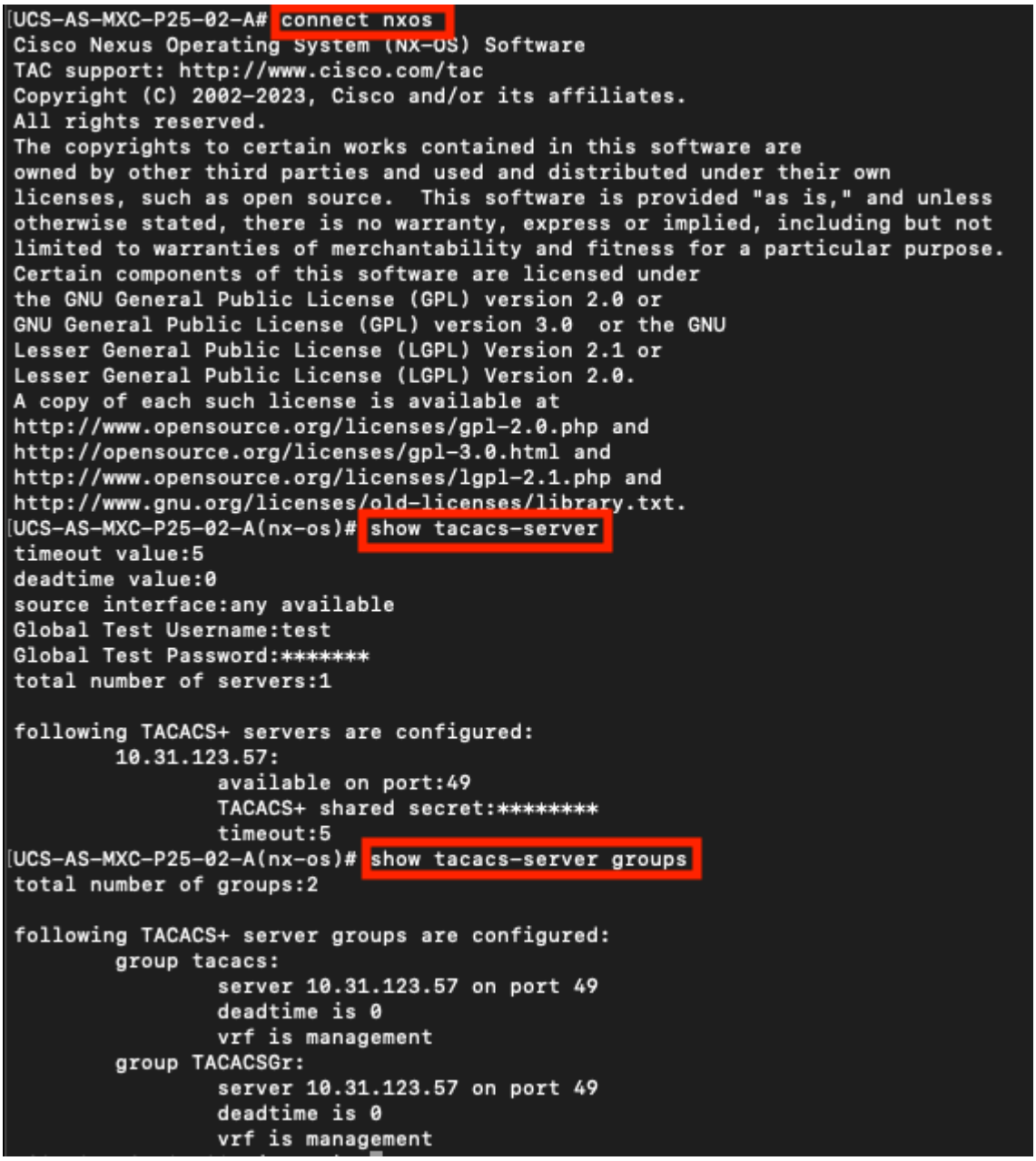
connect nxos

UCS-A(nx-os)#

show tacacs-server

UCS-A(nx-os)#

show tacacs-server groups



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

Valide a configuração do nosso 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/library.txt.
UCS-AS-MXC-P25-02-A(nx-os)# test aaa server tacacs+ 10.31.123.57 operator Cisc0123
```

Revisão do UCSM

Verificação de acessibilidade

<#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
```

Verificação de porta

<#root>

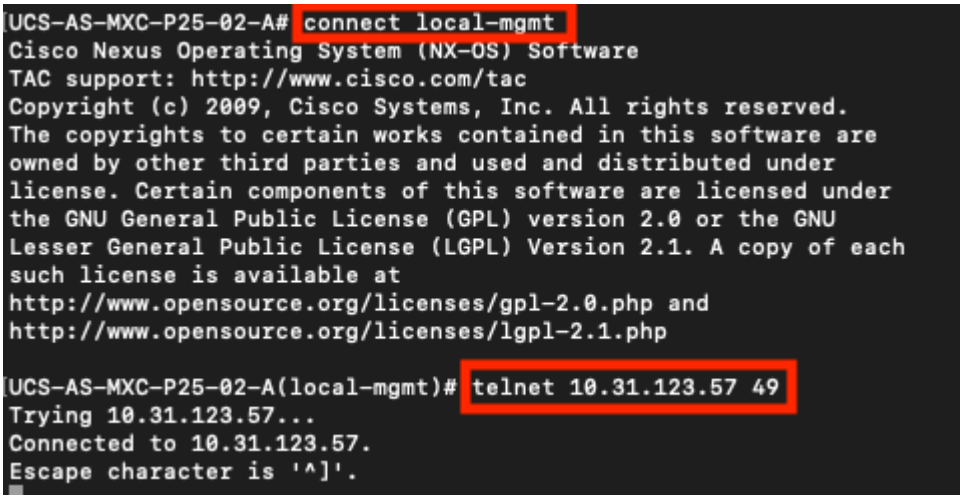
UCS-A#

connect local-mgmt

UCS-A(local-mgmt)#

telnet

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



O método mais eficaz para ver erros é habilitar a depuração do NXOS. Com essa saída, você pode ver os grupos, a conexão e a mensagem de erro que causa problemas de comunicação.

- Abra uma sessão SSH para o UCSM e faça login com qualquer usuário privilegiado com permissões de administrador (preferencialmente um usuário local), altere para o contexto CLI do NX-OS e inicie o monitor de terminal.

<#root>

UCS-A#

connect nxos

UCS-A(nx-os)#

terminal monitor

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

<#root>

UCS-A(nx-os)#

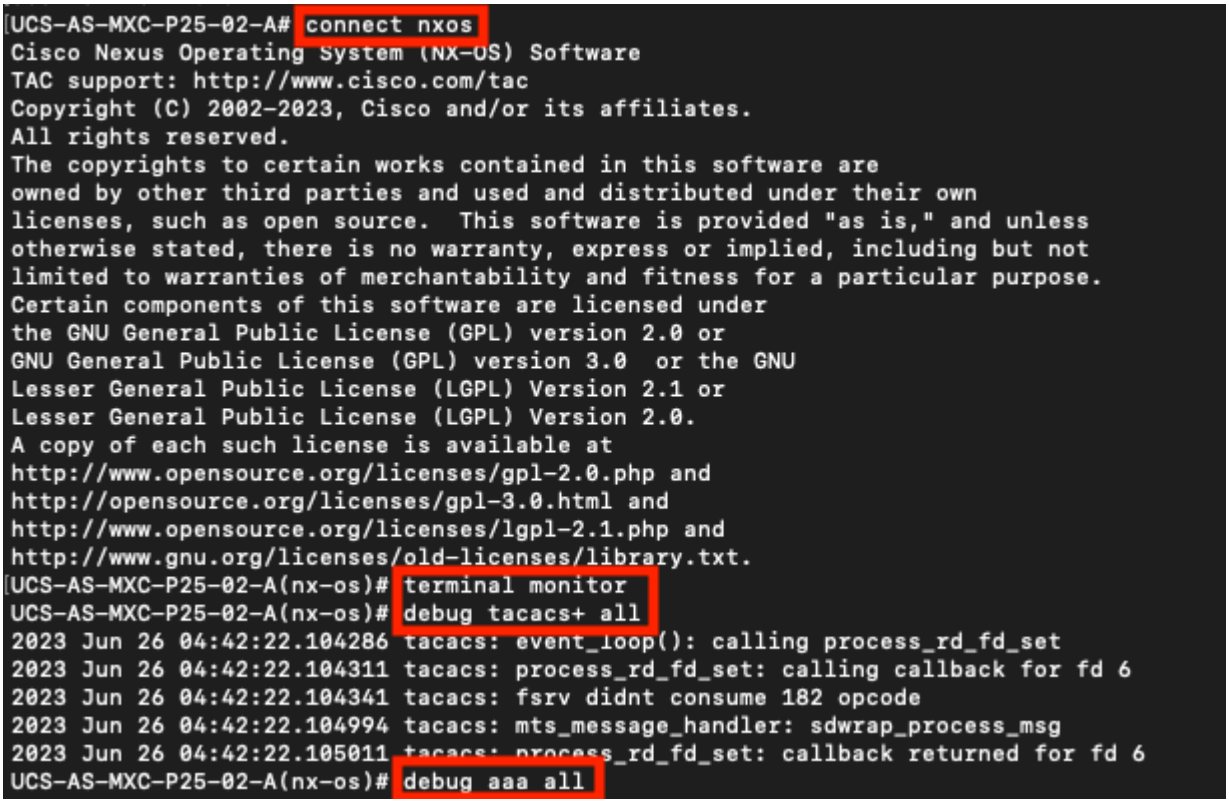
debug aaa all

```
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
```

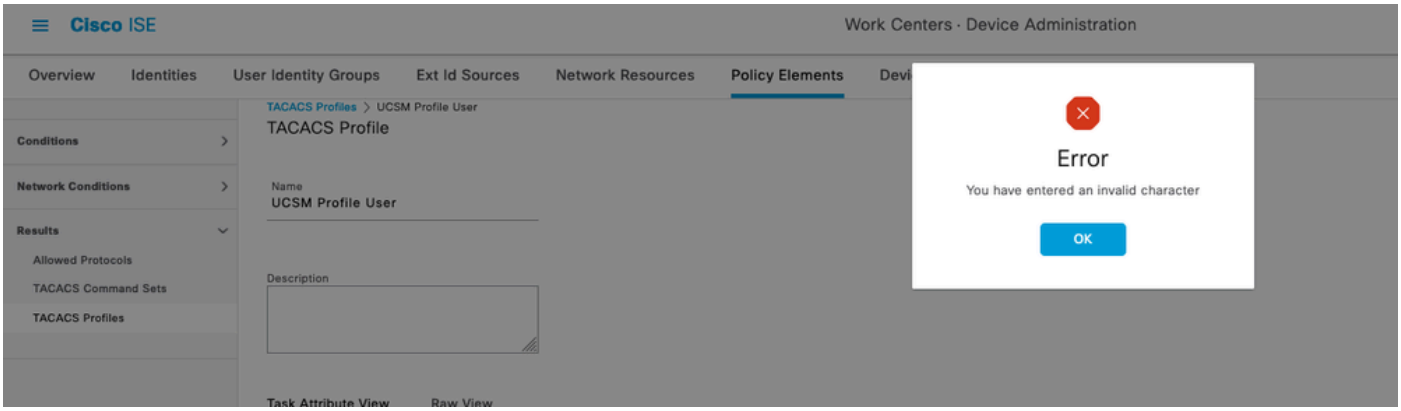


- Agora, abra uma nova sessão de GUI ou CLI e tente fazer login como um usuário remoto (TACACS+).
- Assim que você receber uma mensagem de falha de login, desative as depurações que fecham a sessão ou com esse comando.

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

Problemas comuns de TACACs no ISE

- No ISE, esse comportamento é exibido ao tentar configurar um perfil tacacs nos atributos necessários para que o UCSM atribua as funções correspondentes para admin ou qualquer outra função, selecione no botão salvar e esse comportamento é visto:



Este erro é devido ao seguinte bug https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwc91917 , certifique-se de que você tenha onde este defeito foi solucionado.

Revisão do ISE

Etapa 1. Revise se a capacidade de serviço TACACS+ está em execução, isso pode ser verificado em:

- GUI: Verifique se você tem o nó listado com o serviço DEVICE ADMIN em Administração > Sistema > Implantação.
- CLI: Execute o comando show ports | incluir 49 para confirmar que há conexões na porta TCP que pertencem ao TACACS+

<#root>

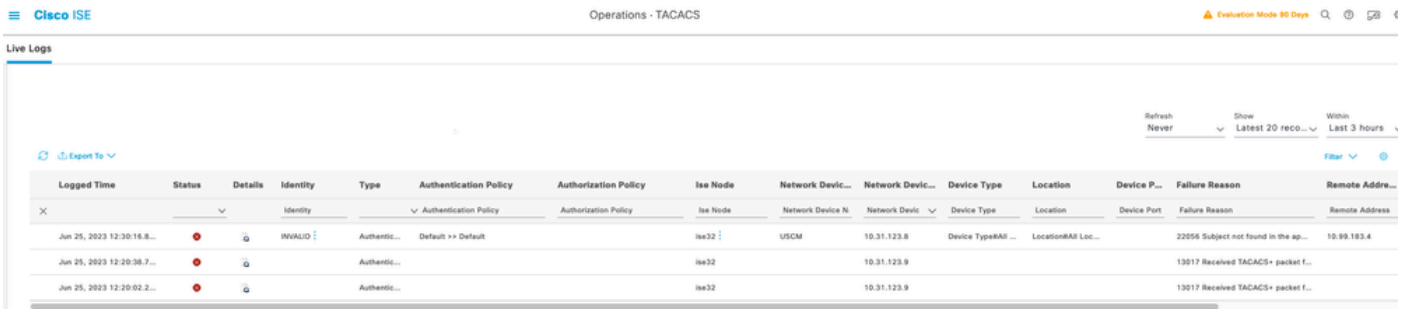
```
ise32/admin#
```

```
show ports | include 49
```

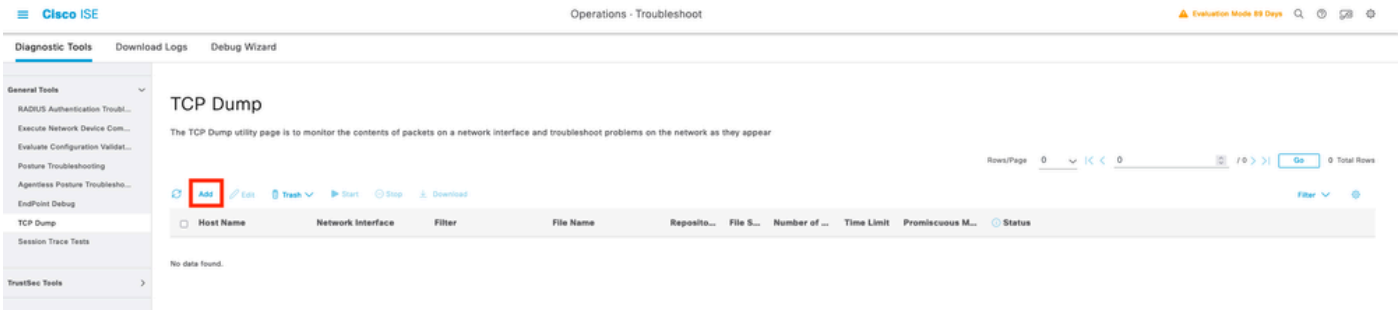
```
tcp: 169.254.4.1:49, 169.254.2.1:49, 169.254.4.1:49, 10.31.123.57:49
```

Etapa 2. Confirme se há registros em tempo real referentes a tentativas de autenticação TACACS+ : isso pode ser verificado no menu Operations > TACACS > Live logs ,

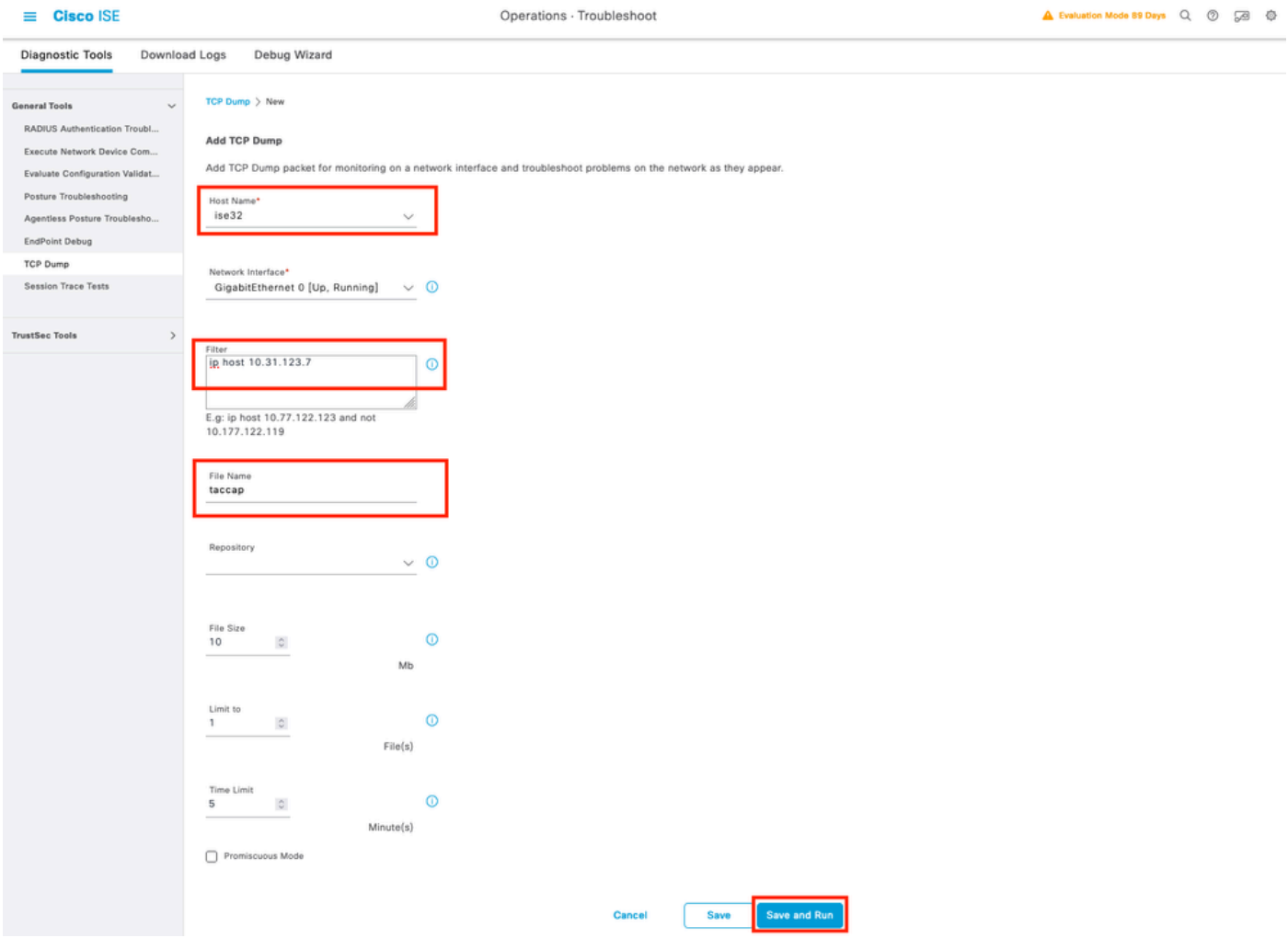
Dependendo do motivo da falha, você pode ajustar sua configuração ou tratar da causa da falha.



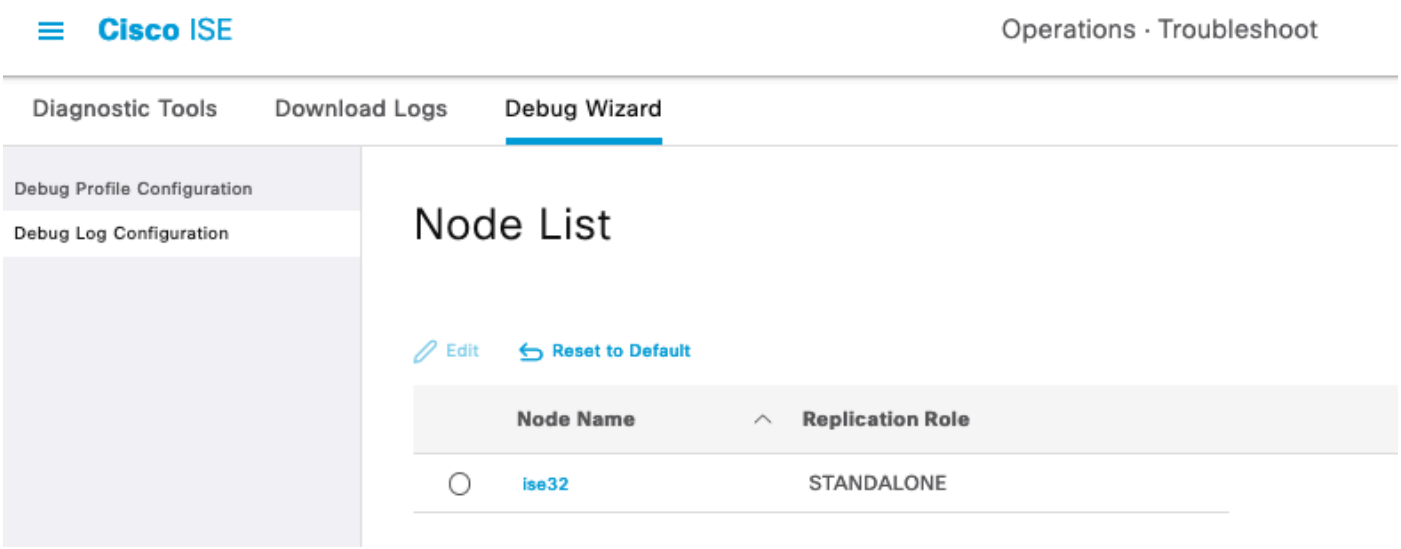
Etapa 3. Caso você não veja nenhum ciclo de vida, continue para fazer uma captura de pacote, navegue até o menu Operações > Solução de problemas > Ferramentas de diagnóstico > Ferramentas gerais > Despejo TCP , selecione em adicionar



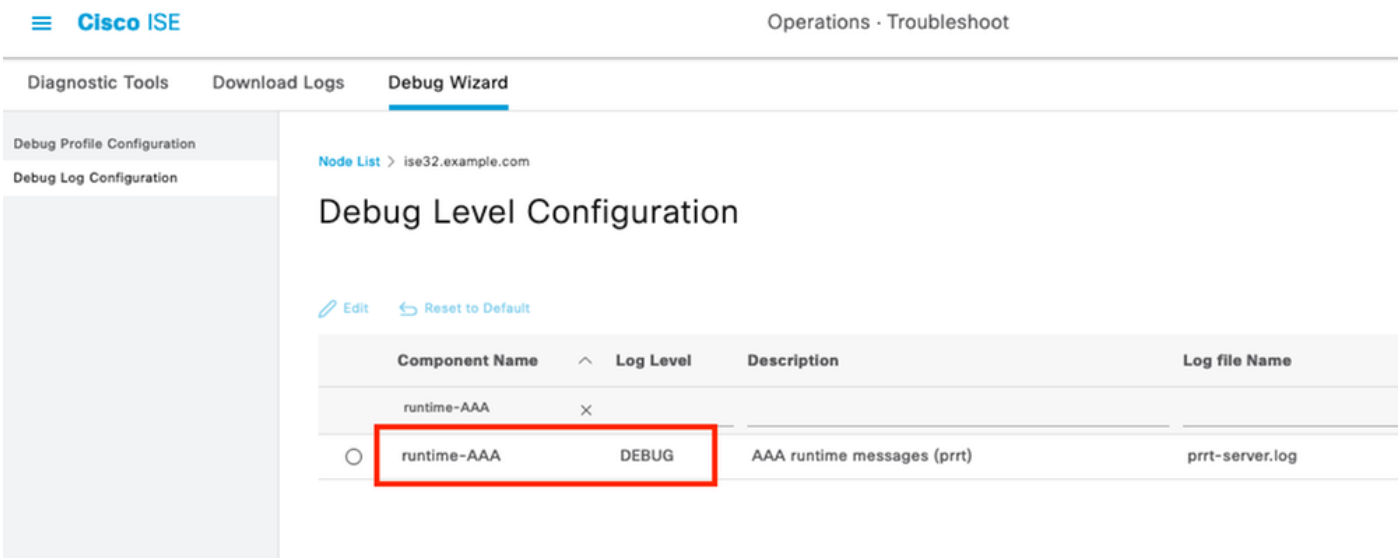
Selecione o nó Policy Service de onde o UCSM está enviando a autenticação e, em seguida, nos filtros, prossiga para a entrada do host IP X.X.X.X correspondente ao IP do UCSM de onde a autenticação está sendo enviada, nomeie a captura e role para baixo para salvar, execute a captura e faça login a partir do UCSM .



Etapa 4. Ative o componente runtime-AAA na depuração dentro do PSN de onde a autenticação está sendo executada em Operações > Solução de problemas > Assistente de depuração > Configuração do log de depuração, selecione o nó PSN e, em seguida, selecione avançar no botão de edição .



Procure o componente runtime-AAA e altere seu nível para debug para, em seguida, reproduzir o problema novamente e continue a analisar os logs .



Note: Para obter mais informações, consulte o vídeo no canal do Cisco Youtube Como habilitar depurações em versões do ISE 3.x https://www.youtube.com/watch?v=E3USz8B76c8 .

Informações Relacionadas

Guia de gerenciamento de administração do Cisco UCS Manager

Guia de configuração do Cisco UCS CIMC TACACS+

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.