在带有ISE服务器的UCS Manager上配置TACACS+身份验证域

目录

简介

本文档介绍在统一计算系统管理器(UCSM)上配置增强型终端访问控制器访问控制系统(TACACS+)身份验证。TACACS+是用于身份验证、授权和责任服务(AAA)的网络协议，它提供了一种集中管理网络访问设备(NAD)的方法，您可以在其中通过服务器管理和创建规则，在此使用案例场景中，我们使用的是身份服务引擎(ISE)。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco UCS Manager(UCSM)
- 增强型终端访问控制器访问控制系统(TACACS+)
- 身份服务引擎 (ISE)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- UCSM 4.2(3d)
- 思科身份服务引擎(ISE)版本3.2

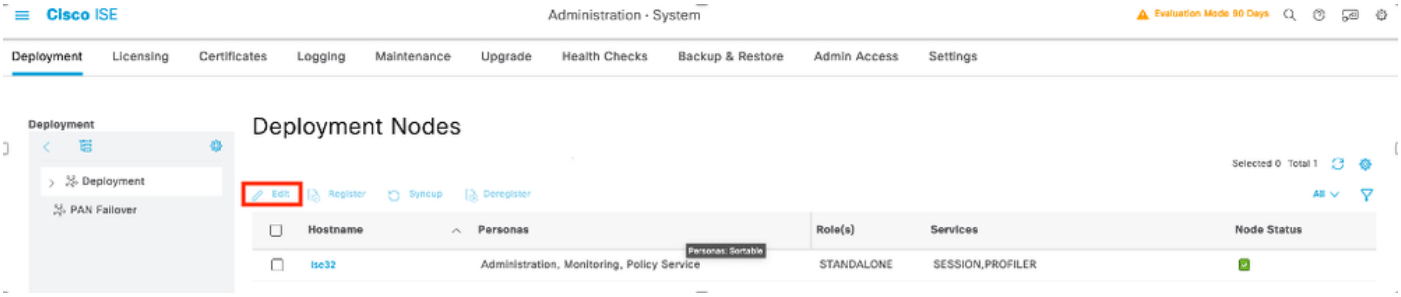
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

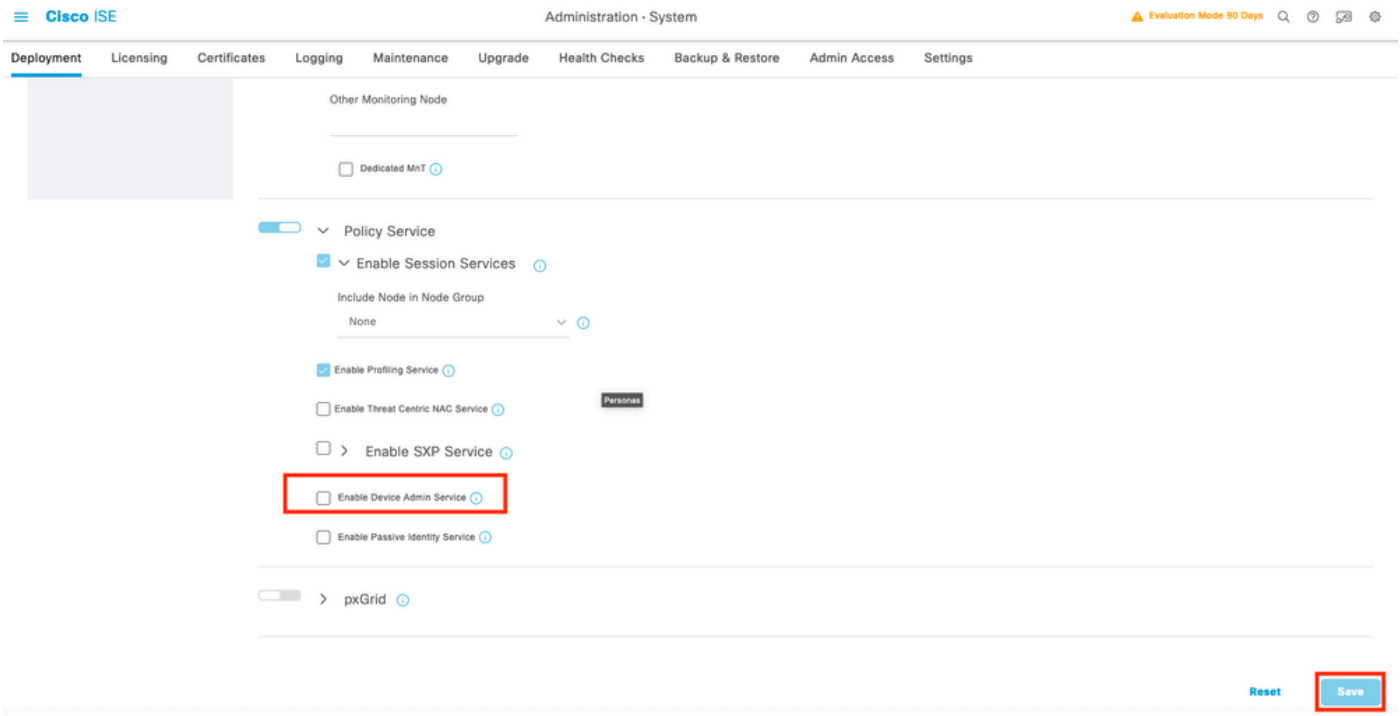
ISE上的TACACS+配置

在ISE上设置TACACS+

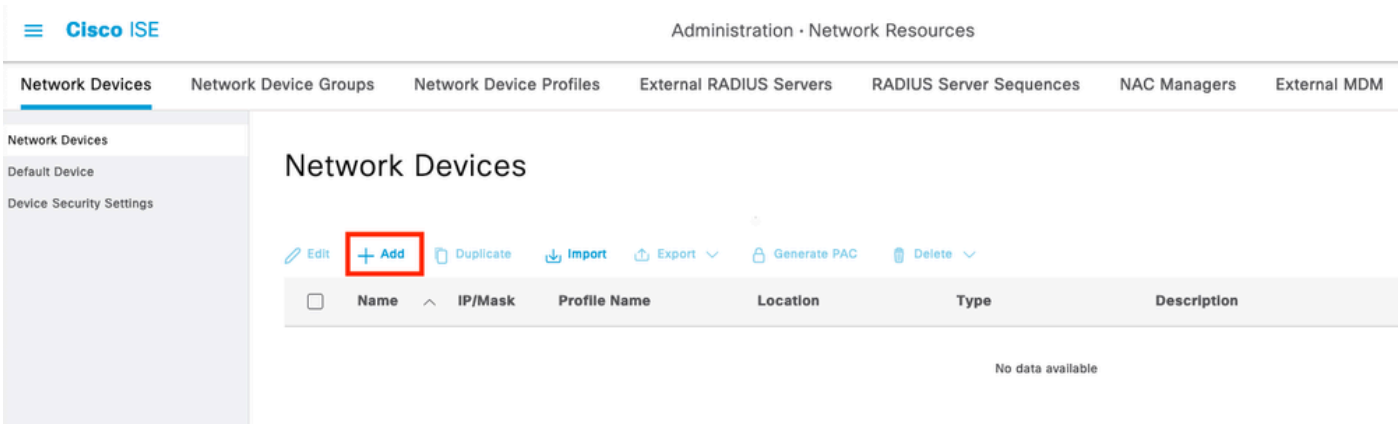
第1步：第一项任务是检查ISE是否具有处理TACACS+身份验证的正确功能，以便您需要在策略服务节点(PSN)中检查是否具有设备管理服务的功能，浏览菜单Administration > System > Deployment，选择ISE执行TACACS+的节点，然后选择按钮编辑。



第2步：向下滚动，直到您看到相应的功能Device Administration Service（注意，要启用此功能，您首先需要在节点上启用策略服务器角色，并且部署中提供TACACS+许可证），选中该复选框，然后保存配置：

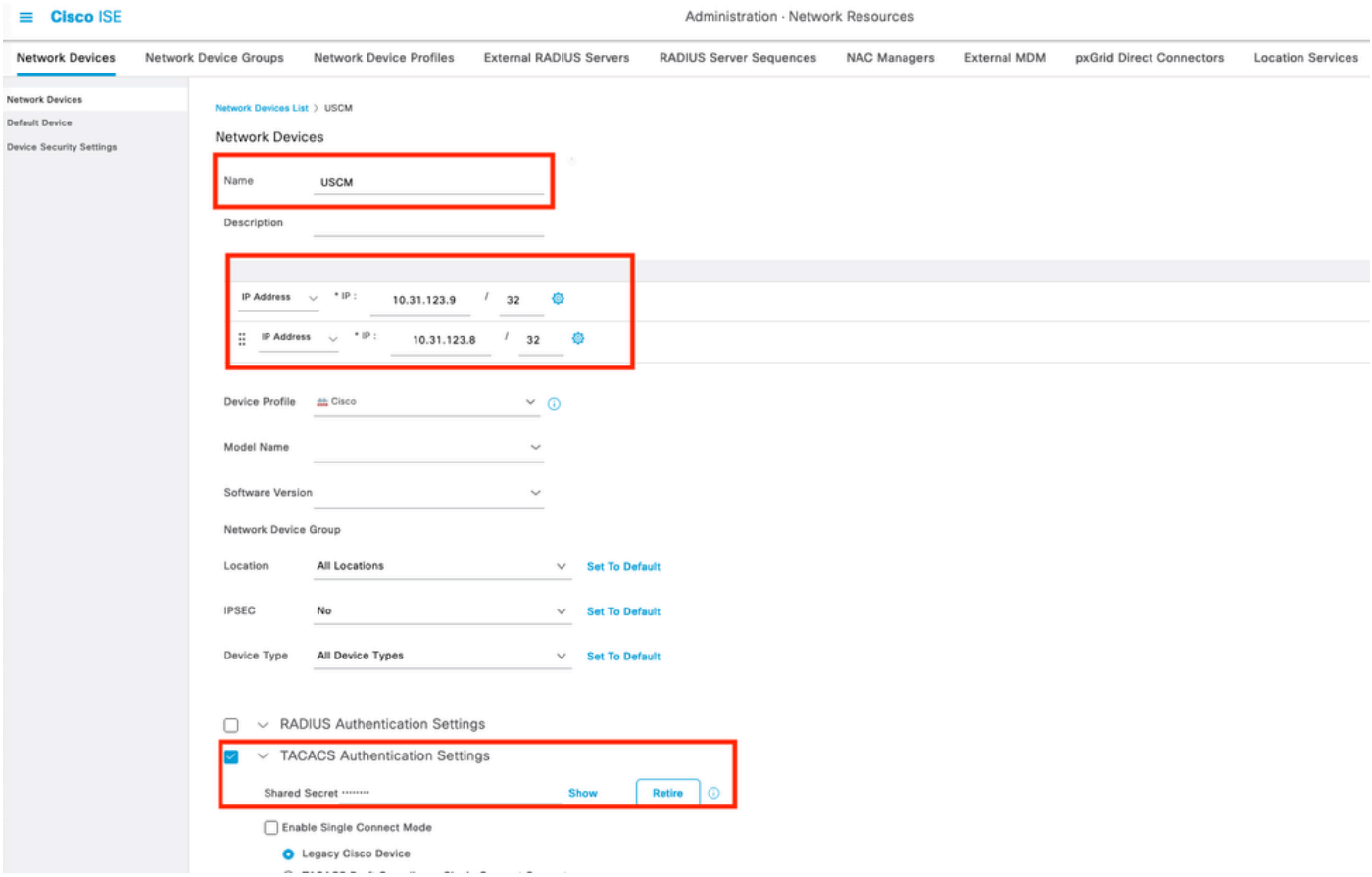


第3步。配置将ISE用作TACACS+作为服务器的网络接入设备(NAD)，导航到菜单Administration > Network Resources > Network Devices，然后选择按钮+Add。



第4步。在本节中，配置：

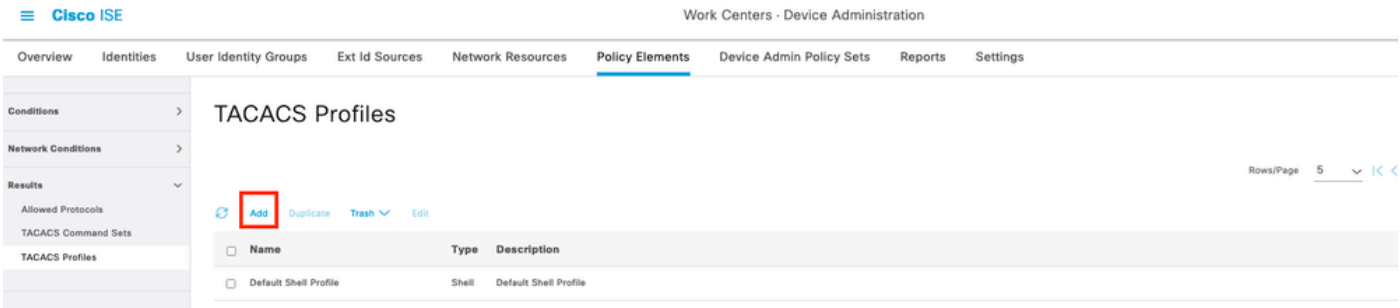
- 要作为TACACS+客户端的UCSM的名称。
- UCSM用于向ISE发送请求的IP地址。
- TACACS+共享密钥，这是用于加密UCSM和ISE之间的数据包的密码



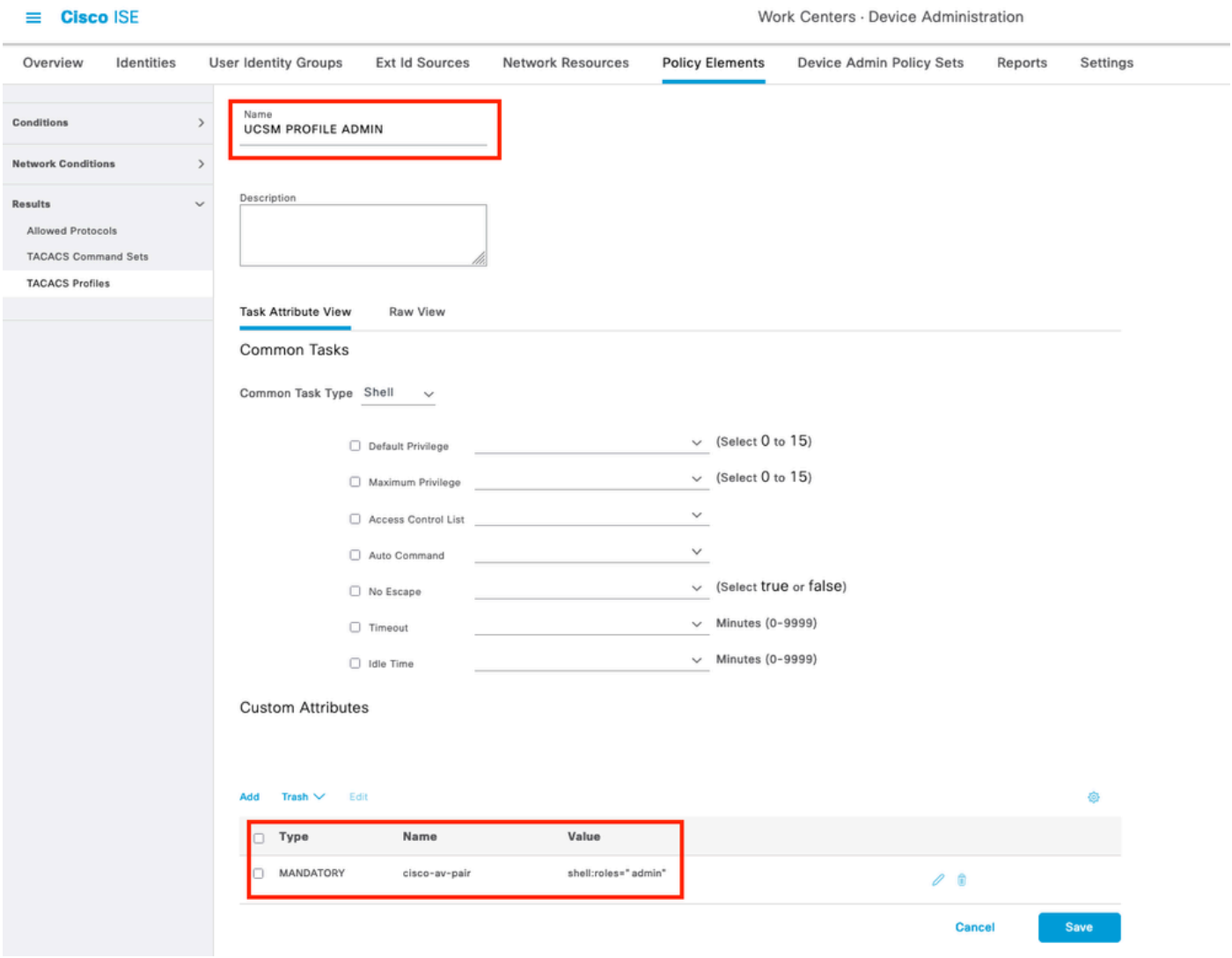
注意：对于集群配置，请为两个交换矩阵互联添加管理端口IP地址。此配置可确保在第一交换矩阵互联发生故障且系统故障切换到第二交换矩阵互联时，远程用户可以继续登录。所有登录请求均源自这些IP地址，而不是Cisco UCS Manager使用的虚拟IP地址。

在ISE上配置属性和规则

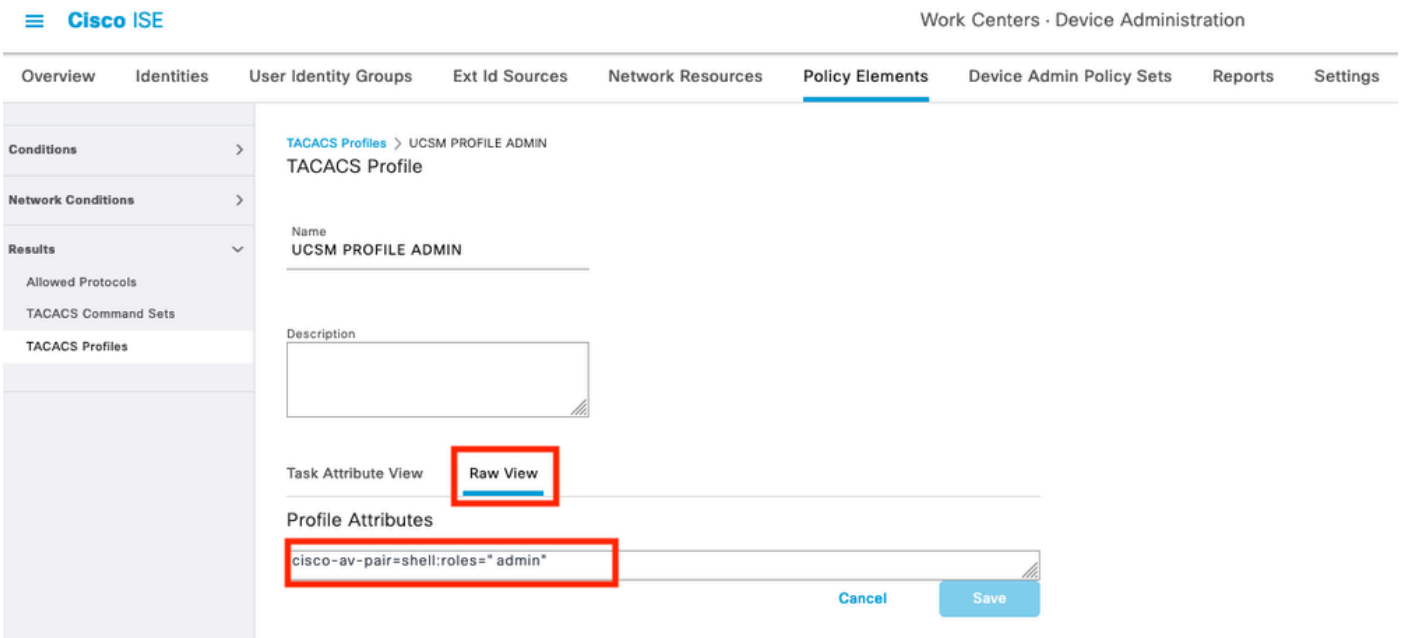
第1步：创建TACACS+配置文件，导航到菜单Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles，然后选择Add



第2。在此部分中，使用名称配置配置文件，并在Custom Attributes部分中，选择Add，然后创建一个特性MANDATORY的属性，将其命名为cisco-av-pair，在值中选择一个可用于UCSM的角色并输入该角色作为shell角色，在本示例中，它使用角色admin，并且选择的输入需要是shell:roles="admin"，如下所示，



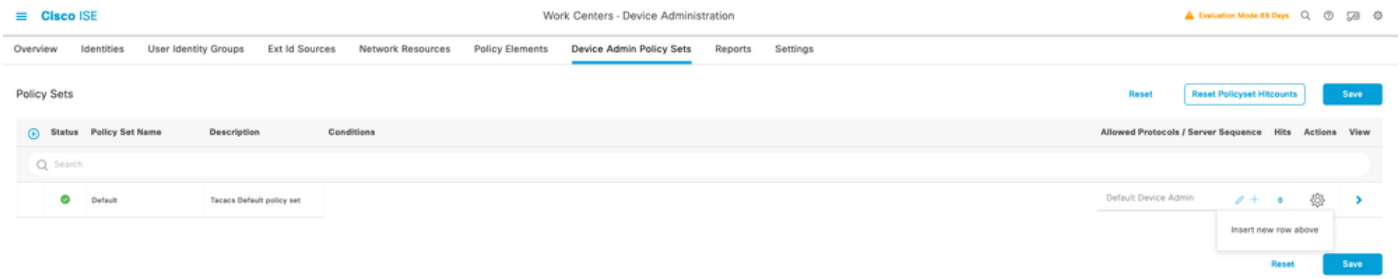
在同一菜单中，如果您为TACACS配置文件选择Raw View，则可以验证通过ISE发送的属性的相应配置。



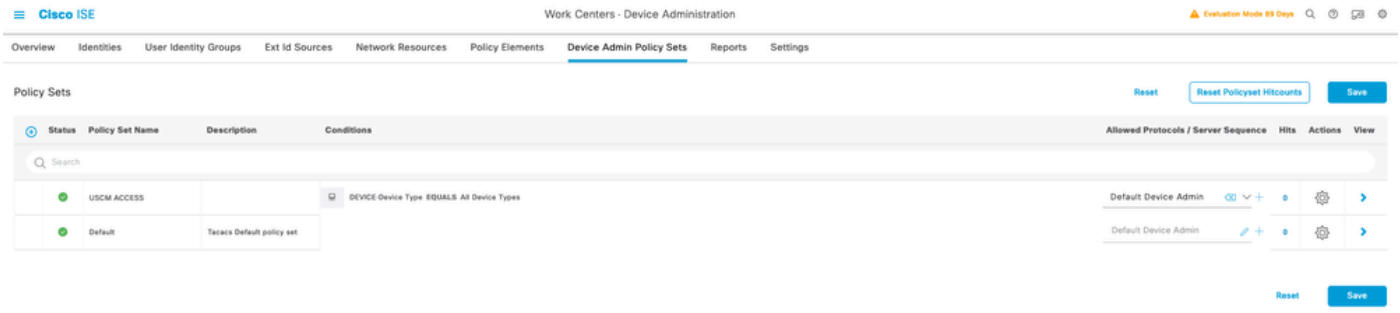
注意：cisco-av-pair name是为TACACS+提供程序提供属性ID的字符串。

第3步。选中并保存配置。

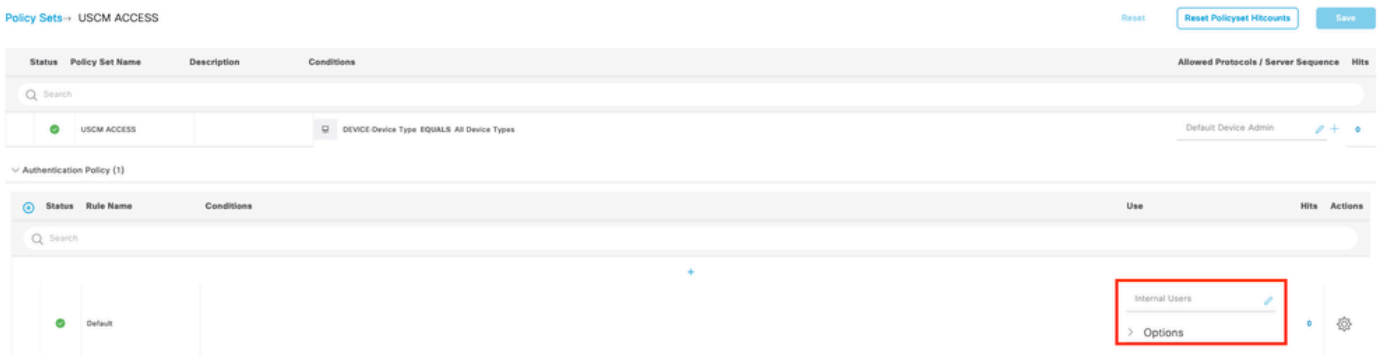
第4步：创建用于UCSM的Device Admin Policy Set，导航菜单Work Centers > Device Administration > Device Admin Policy Sets，然后从现有策略集中选择齿轮图标，然后选择Insert new row



第5步：命名此新的Policy Set，根据从UCSM服务器进行中的TACACS+身份验证的特征添加条件，并选择Allowed Protocols > Default Device Admin，保存配置。

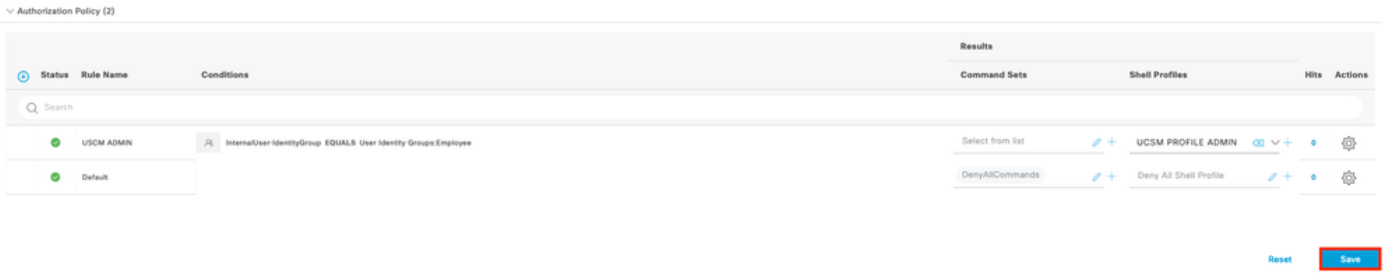


第6步：在>view选项中选择，并在Authentication Policy部分中选择ISE从中查询输入到UCSM的用户名和凭据的外部身份源，在本示例中，凭据对应于ISE中存储的内部用户。



步骤7.下滚至名为Authorization Policy的部分直到Default policy，选择齿轮图标，然后插入一个规则。

第8步：命名新的授权规则，添加与已通过身份验证的用户相关的条件作为组成员身份，并在Shell Profiles部分添加您以前配置的TACACS配置文件，保存配置。



UCSM上的TACACS+配置

使用Cisco UCS Manager具有管理员权限的用户登录GUI。

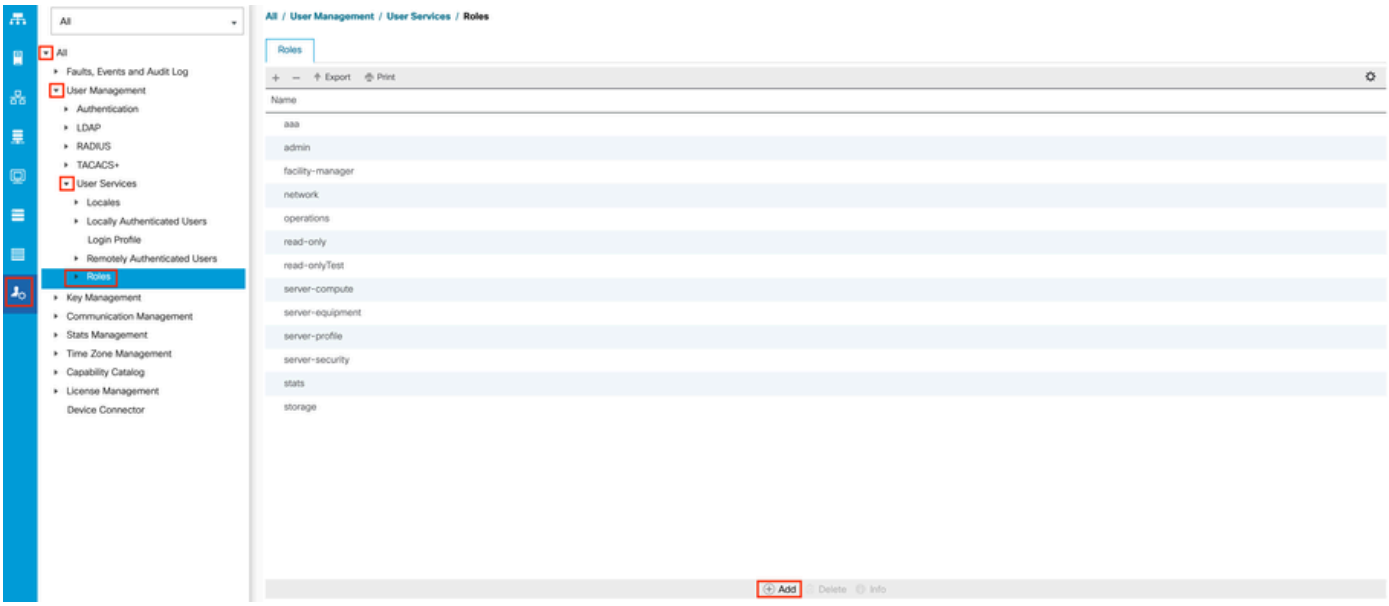
为用户创建角色

第1步：在“导航”(Navigation)窗格中，选择管理员选项卡。
第2步：在Admin选项卡上，展开All > User Management >User Services > Roles。

步骤3.在窗Work格中，选择选General项卡。

步骤4.为自定义角色选择Add。此示例使用默认角色。

步骤5.检验名称角色是否与之前在TACACS配置文件中配置的名称相匹配。

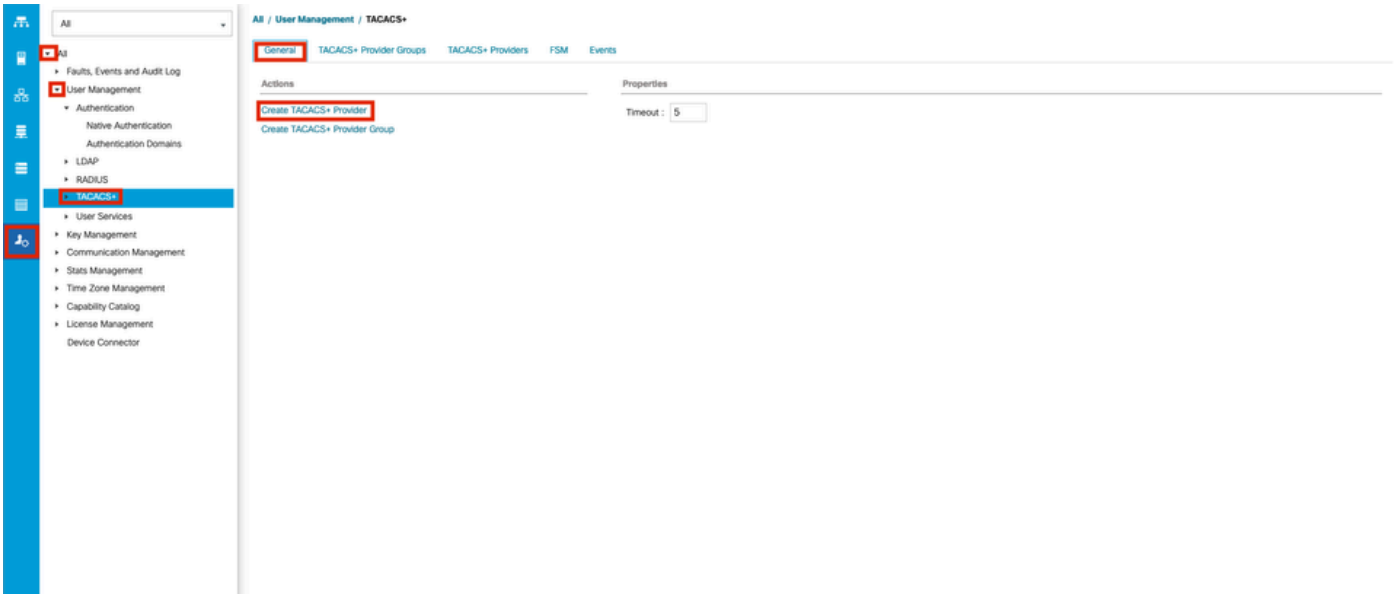


创建TACACS+提供程序

第1步：在“导航”(Navigation)窗格中，选择管理员选项卡。
第2步：在Admin选项卡上，展开All > User Management > TACACS+。

步骤3.在窗Work格中，选择选项卡General。

步骤4.在区域Actions中，选择Create TACACS+ Provider.



步骤5.在向**Create TACACS+ Provider**导中输入适当的信息。

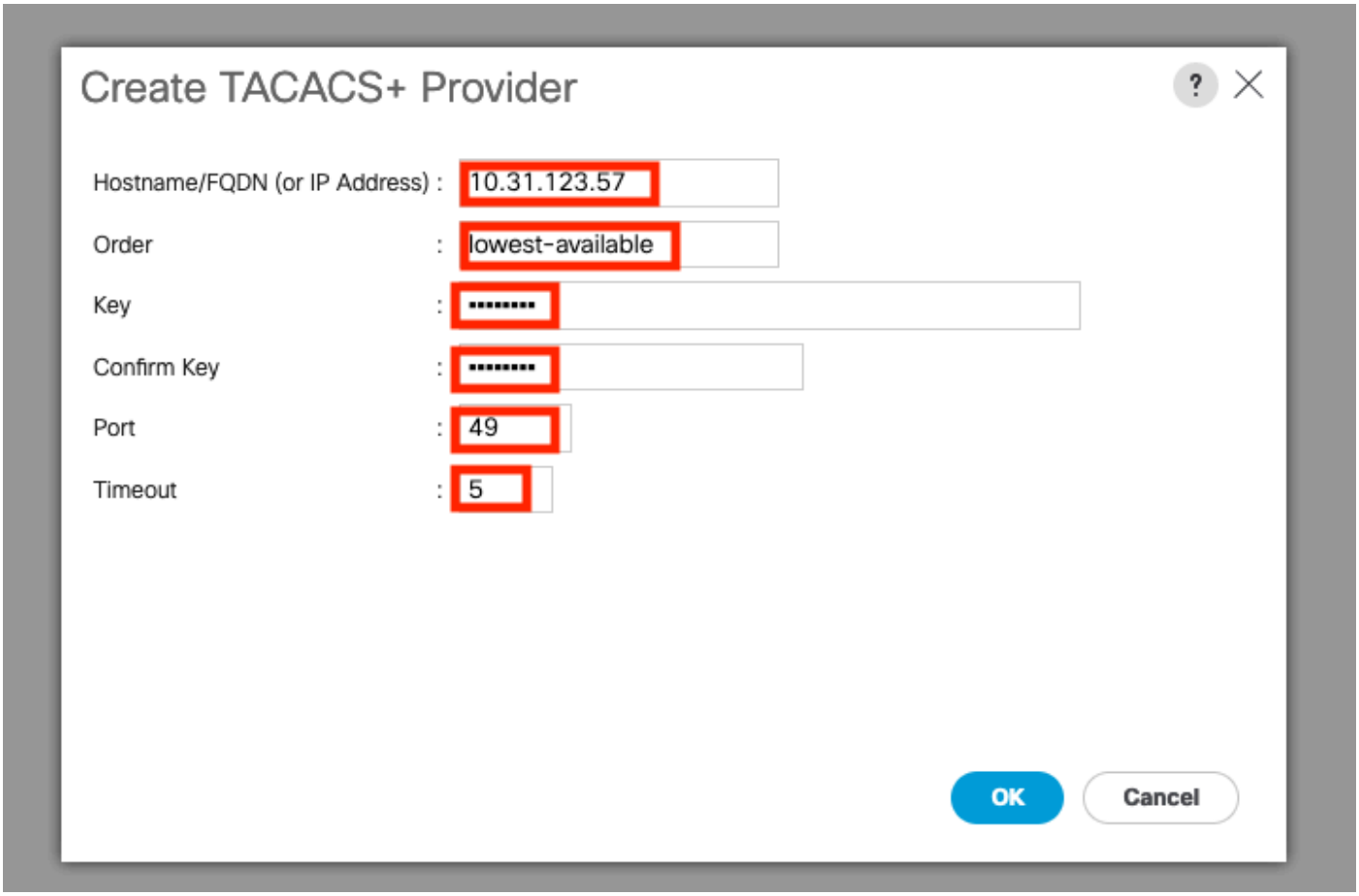
- 在Hostname字段中，键入TACACS+服务器的IP地址或主机名。
- 在Order字段中，Cisco UCS使用此提供商对用户进行身份验证的顺序。

  输入介于1和16之间的整数，或者输入可用最小的或0（零）（如果您希望Cisco UCS根据此Cisco UCS实例中定义的其他提供商分配下一个可用订单）。

- 在Key字段中，输入数据库的SSL加密密钥。

- 在Confirm Key字段中，为确认目的重复的SSL加密密钥。
- 在Port字段中，Cisco UCS与TACACS+数据库（端口49默认端口）通信的端口。

- 在Timeout字段中，系统在超时之前尝试联系TACACS+数据库所花费的时间（以秒为单位）。



步骤6.选择确定。

注意：如果使用主机名而不是IP地址，则必须在Cisco UCS Manager中配置DNS服务器。

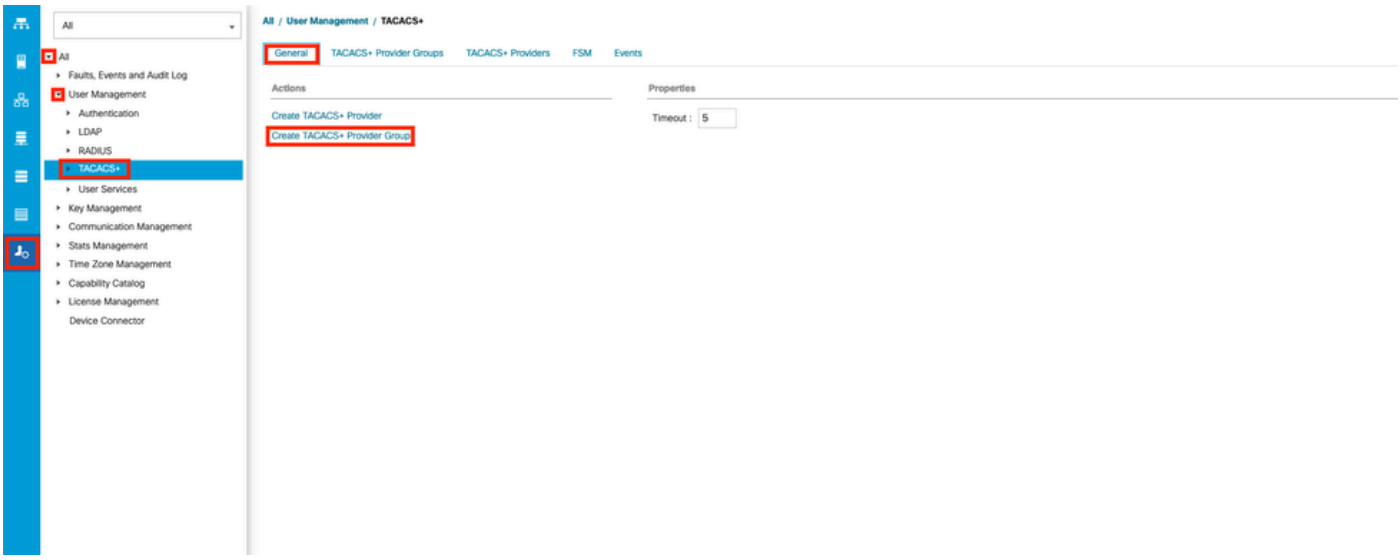
创建TACAC+提供程序组

步骤1.在窗**Navigation**格中，选择选项**Admin**卡。

步骤2.在选项**Admin**卡上，展开**All > User Management > TACACS+**。

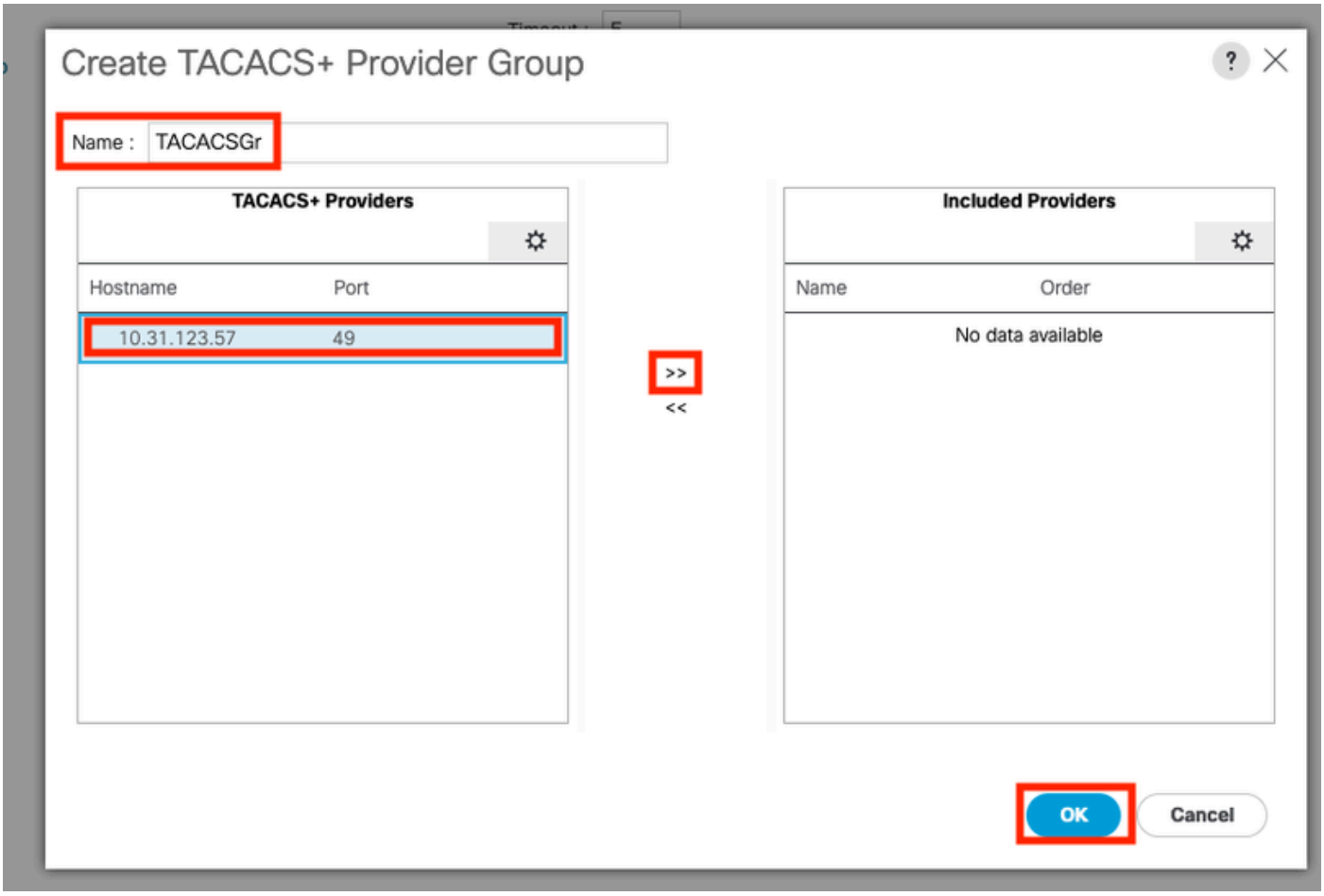
步骤3.在窗**Work**格中，选择选项**General**卡。

步骤4.在区**Actions**域中，选Create TACACS+ Provider择Group。



第5步：在创建TACACS+提供程序组对话框中，输入请求的信息。

- 在名称字段中，输入组的唯一名称。
- 在TACACS+ Providers表中，选择要包含在组中的提供程序。
- 选择>>按钮将提供程序添加到包含的提供程序表。



步骤6.选择确定。

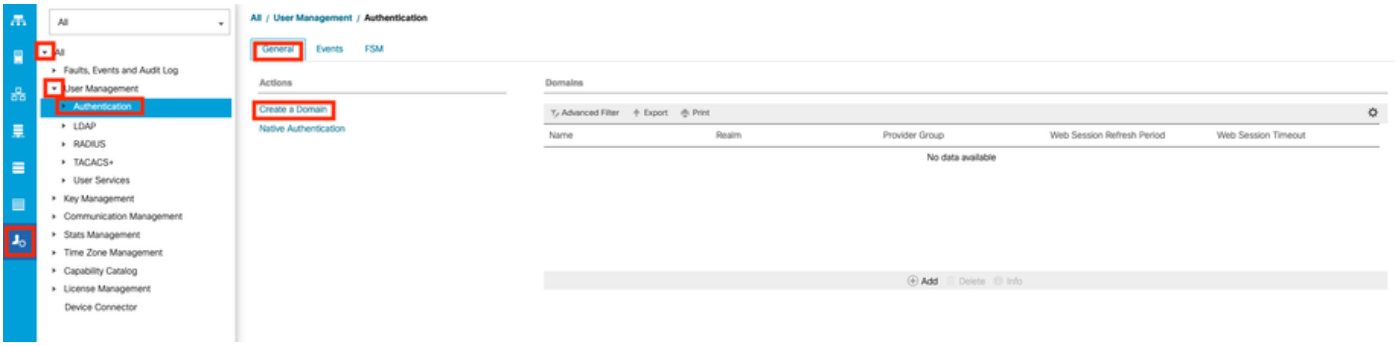
创建身份验证域

步骤1.在窗Navigation格中，选择选项Admin卡。

步骤2.在选项卡Admin上，展开 All > User Management > Authentication

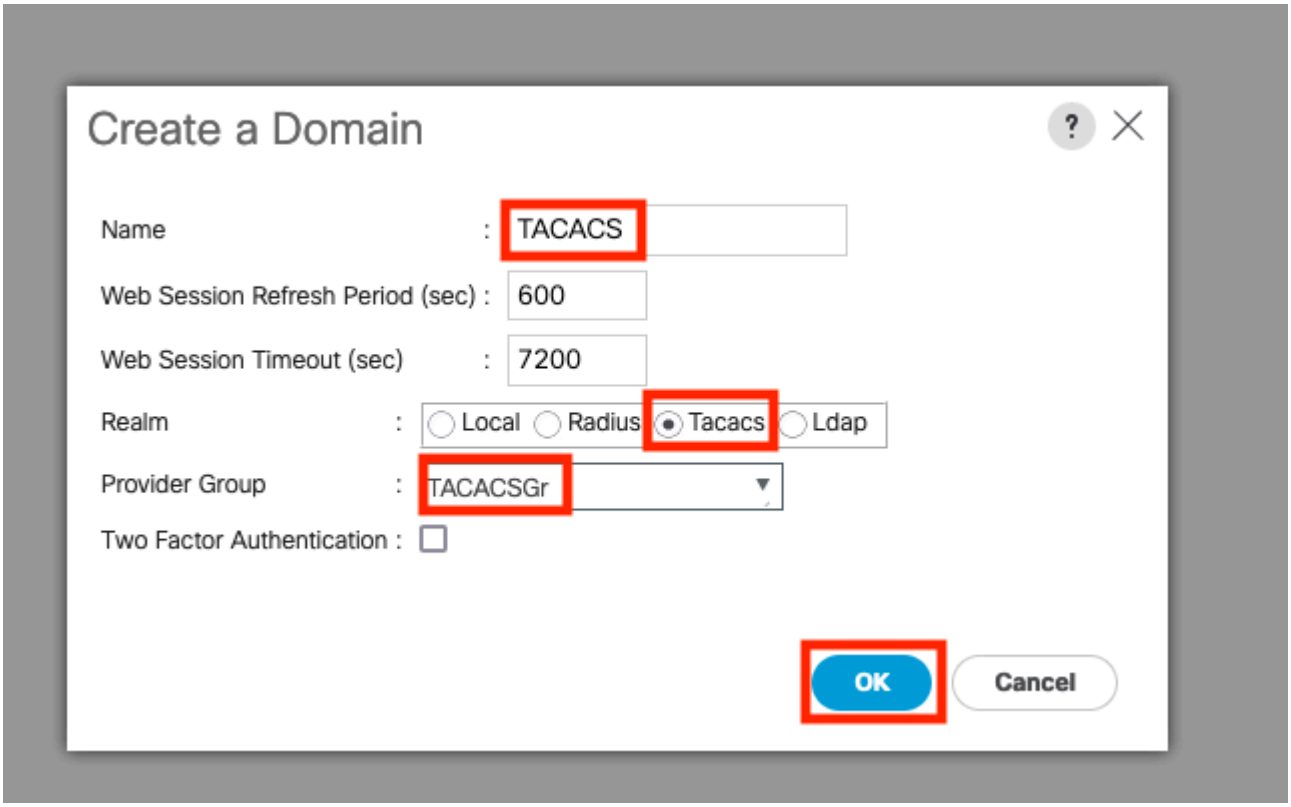
步骤3.在窗Work格中，选择选项General卡。

步骤4.在区Actions域中，选择Create a Domain.



步骤5.在Create Domain对话框中，输入请求的信息。

- 在名称字段中，输入域的唯一名称。
- 在Realm中，选择Tacacs选项。
- 从Provider Group下拉列表中，选择以前创建的TACACS+提供程序组，然后选择OK



故障排除

UCSM上的常见TACACS+问题

- 密钥错误或字符无效。
- 端口错误.
- 由于防火墙或代理规则，无法与提供商通信。
- FSM不是100%。

验证UCSM TACACS+配置：

您必须确保UCSM已实施配置检查，有限状态机(FSM)的状态显示为100%完成。

从UCSM命令行验证配置

<#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:
```

从NXOS验证Tacacs配置：

<#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
```

要测试来自NX-OS的身份验证，请使用**test aaa**命令（仅适用于NXOS）。

验证服务器配置：

<#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
```

UCSM审核

可达性验证

<#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
```

端口验证

<#root>

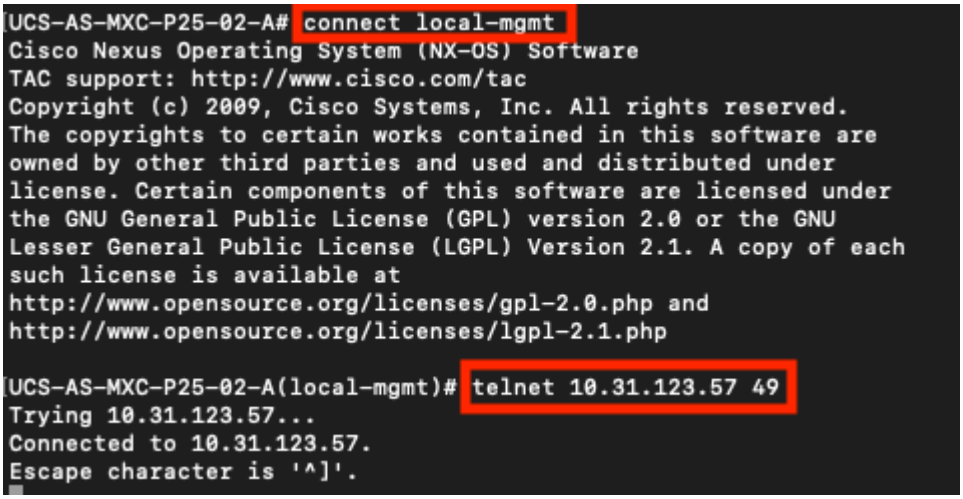
UCS-A#

connect local-mgmt

UCS-A(local-mgmt)#

telnet

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



查看错误的最有效方法是启用NXOS调试，通过此输出，您可以看到导致通信错误的组、连接和错误消息。

- 打开到UCSM的SSH会话，使用具有管理员权限的任何特权用户（最好是本地用户）登录，转到NX-OS CLI上下文并启动终端监控。

<#root>

UCS-A#

connect nxos

UCS-A(nx-os)#

terminal monitor

- 启用调试标志，并验证到日志文件的SSH会话输出。

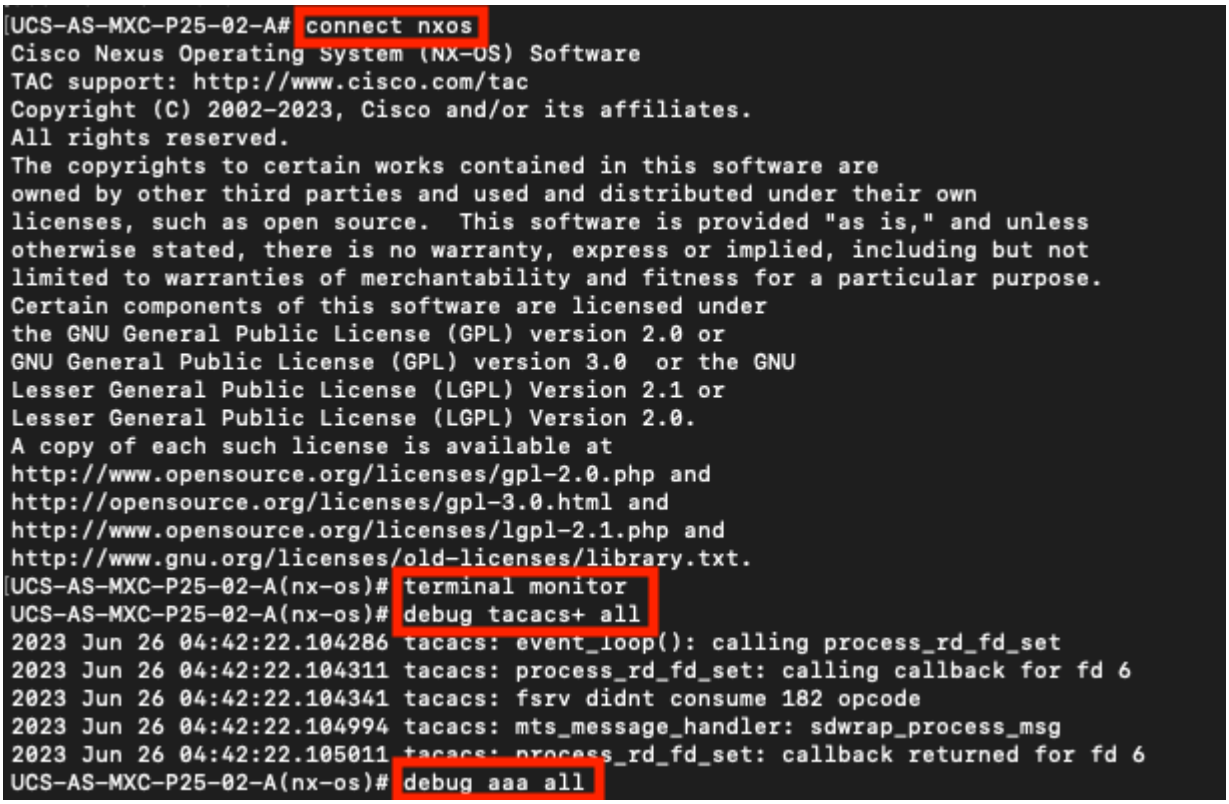
<#root>

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
```



- 现在打开新的GUI或CLI会话，并尝试以远程用户(TACACS+)身份登录。
- 收到登录失败消息后，请关闭关闭会话或使用此命令的调试。

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

ISE上的常见TACAC问题

- 在ISE中，在尝试在UCSM分配管理员或任何其他角色的相应角色所需的属性中配置tacacs配置文件时，会显示此行为，在“保存”(save)按钮上选择，并看到此行为：

此错误是由以下Bug https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwc91917引起的，请确保您具有解决此缺陷的位置。

ISE审核

步骤1.检查TACACS+可维护性是否正在运行，可以将其检入：

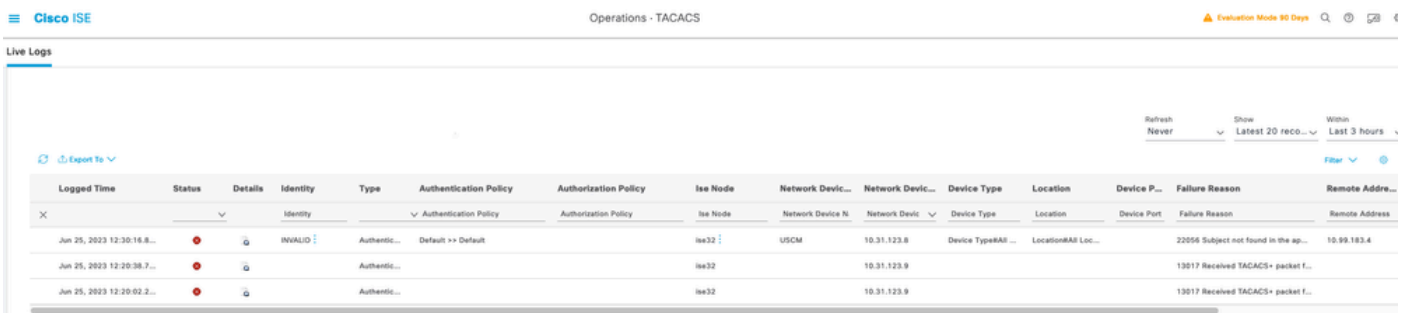
- GUI:查看您是否已在Administration > System > Deployment中列出服务DEVICE ADMIN的节点。
- CLI：运行命令show ports | include 49以确认TCP端口中存在属于TACACS+的连接

<#root>

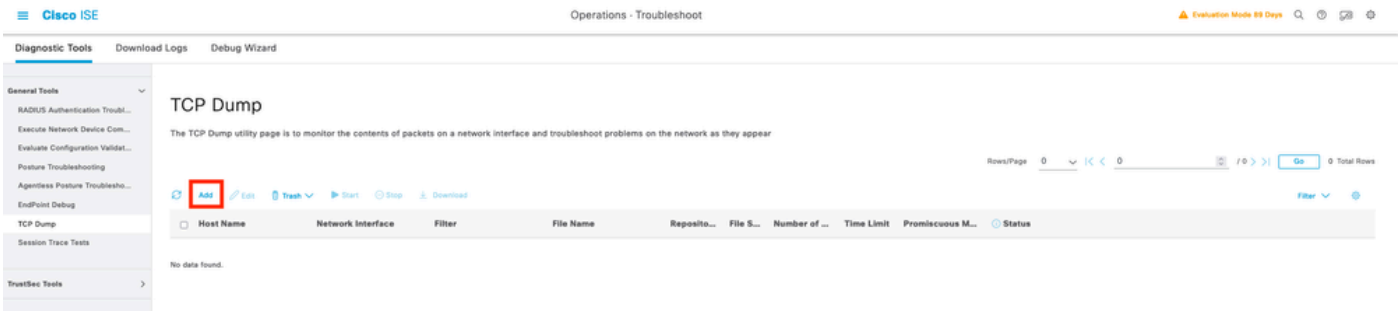
```
ise32/admin#
show ports | include 49

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

步骤2.确认是否存在有关TACACS+身份验证尝试的实时日志：可以在Operations > TACACS > Live logs菜单中进行检查。

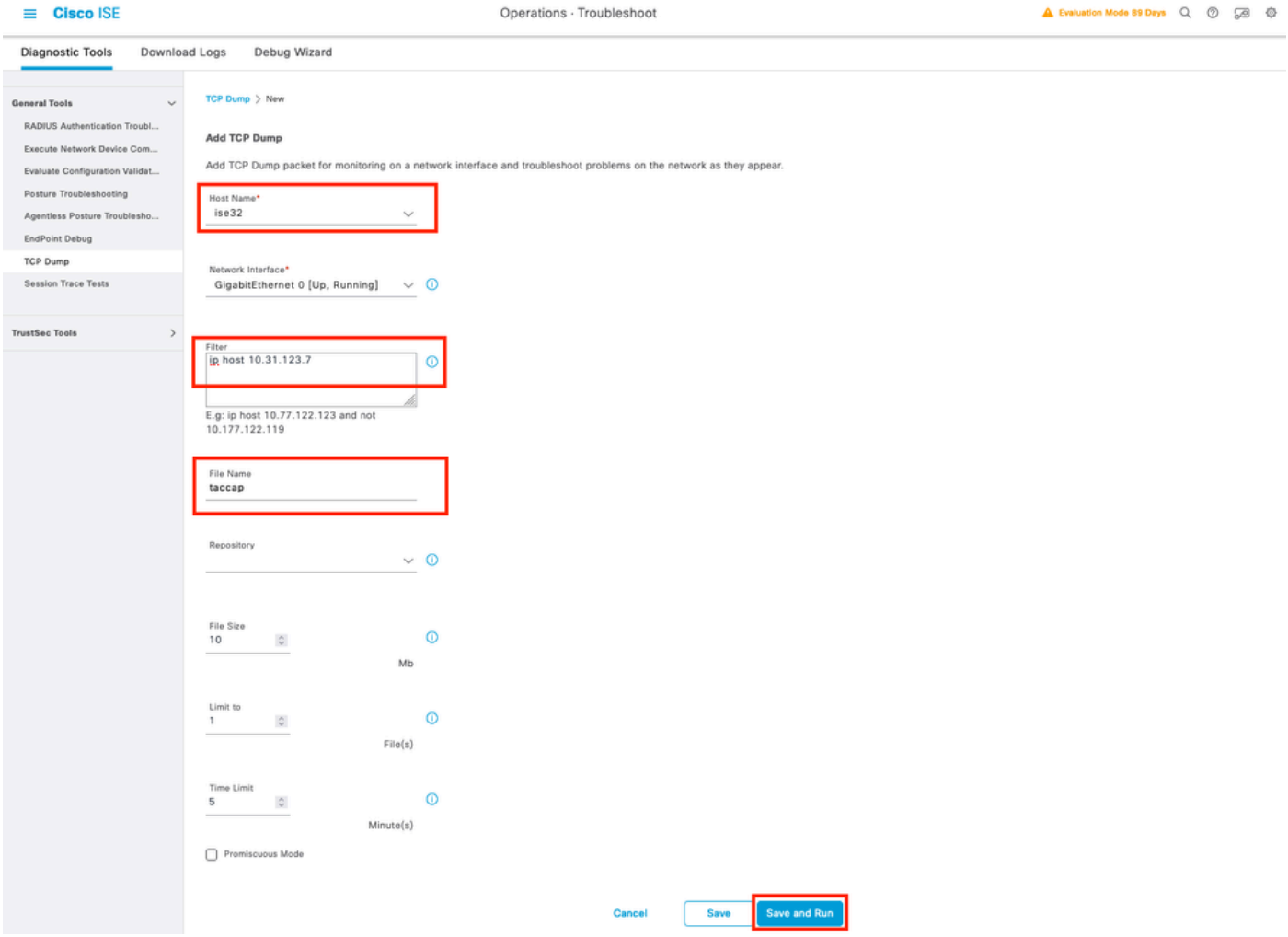
根据故障原因，您可以调整配置或解决故障原因。



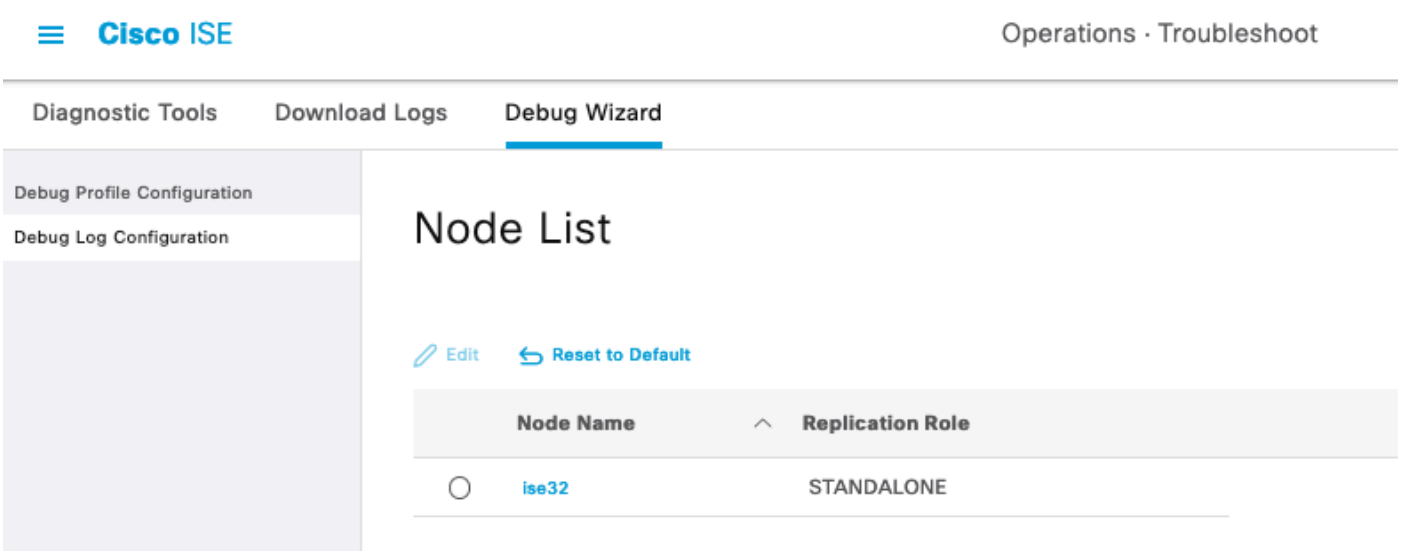
步骤3.如果看不到任何实时日志，请继续捕获数据包，导航到菜单Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump，选择on add



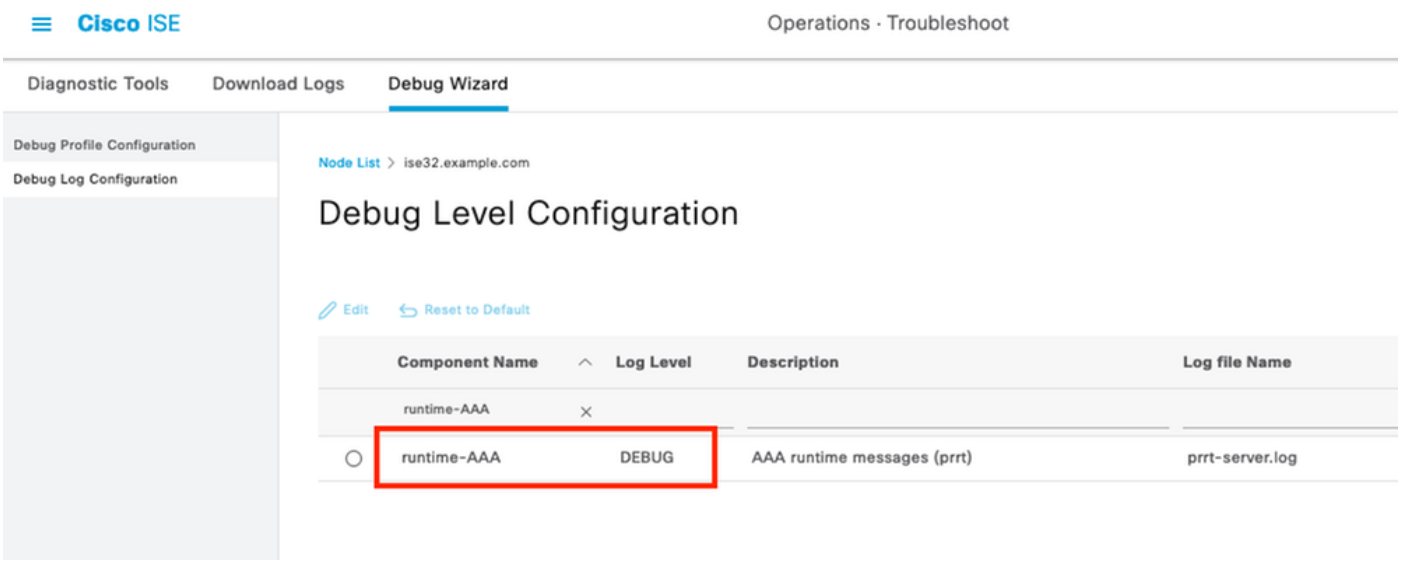
选择UCSM从中发送身份验证的策略服务节点，然后在过滤器中继续输入ip host X.X.X.X（与从中发送身份验证的UCSM的IP对应），命名捕获并向下滚动以保存，运行捕获并从UCSM登录。



第4步：在Operations > Troubleshoot > Debug Wizard > Debug log configuration中执行身份验证的PSN中的debug中启用组件runtime-AAA，选择PSN节点，然后选择edit按钮中的next。



查找组件runtime-AAA并将其级别更改为debug，然后再次重现问题，然后继续分析日志。



注意：有关详细信息，请参阅Cisco Youtube的频道How to Enable Debugs on ISE 3.x Versions https://www.youtube.com/watch?v=E3USz8B76c8中的视频。

相关信息

Cisco UCS Manager管理指南

Cisco UCS CIMC配置指南TACACS+

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。