使用ISE千兆以太网1接口配置TACACS+

目录

简介

本文档介绍带有千兆以太网1接口的ISE TACACS+配置，其中路由器和交换机用作网络设备。

背景信息

思科ISE支持最多6个以太网接口。它只能有三个绑定：bond 0、bond 1和bond 2。您不能更改属于绑定的接口或更改绑定中接口的角色。

先决条件

要求

思科建议您了解以下主题：

- 基本网络知识
- 思科身份服务引擎。

使用的组件

本文档中的信息基于下列硬件和软件版本：

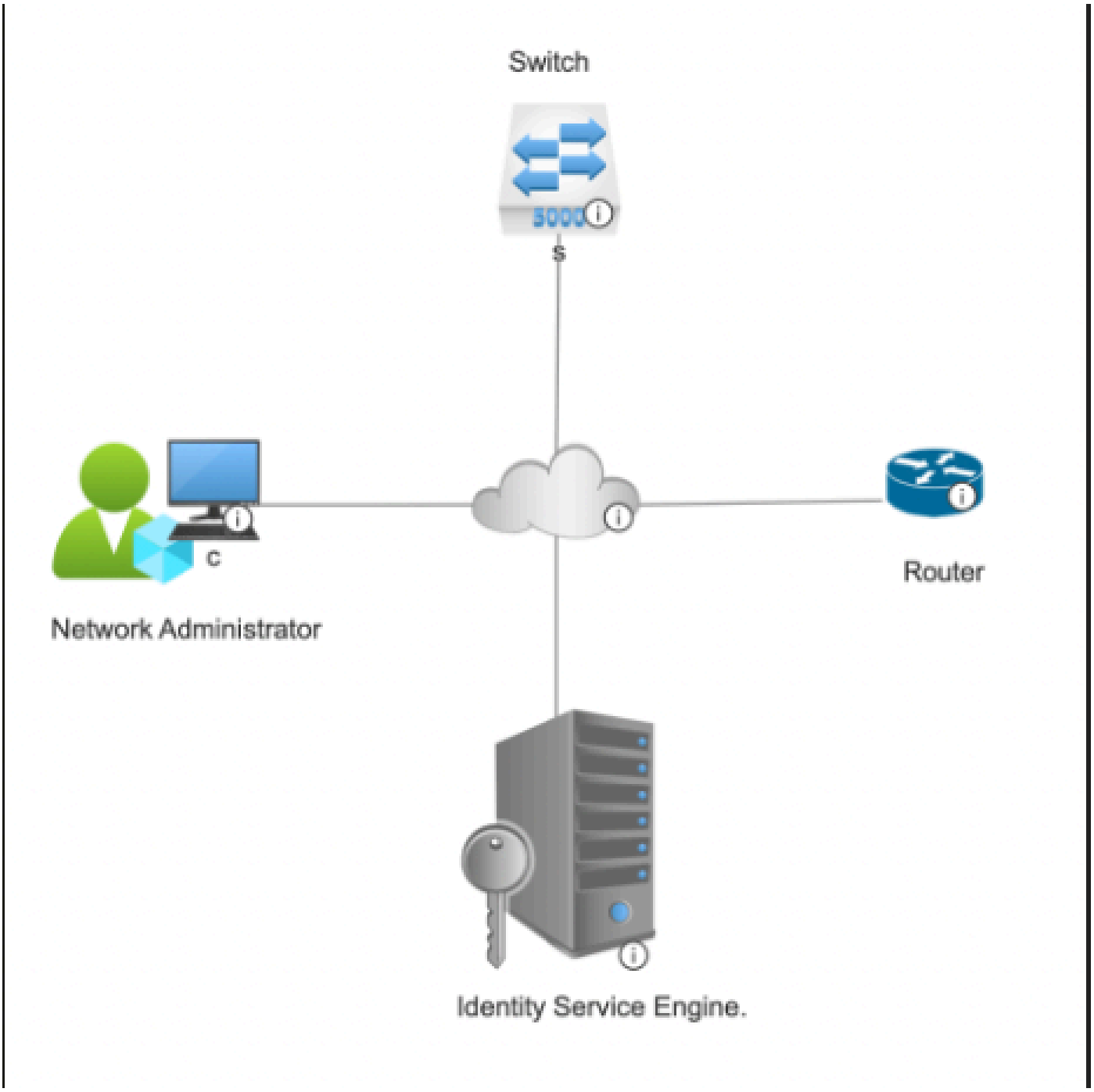
- 思科身份服务引擎v3.3
- 思科IOS®软件版本17.x
- Cisco C9200交换机。

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

配置的目的是：为TACACS+配置ISE的千兆以太网1，并使用TACACS+和ISE作为身份验证服务器对交换机和路由器进行身份验证。

网络图

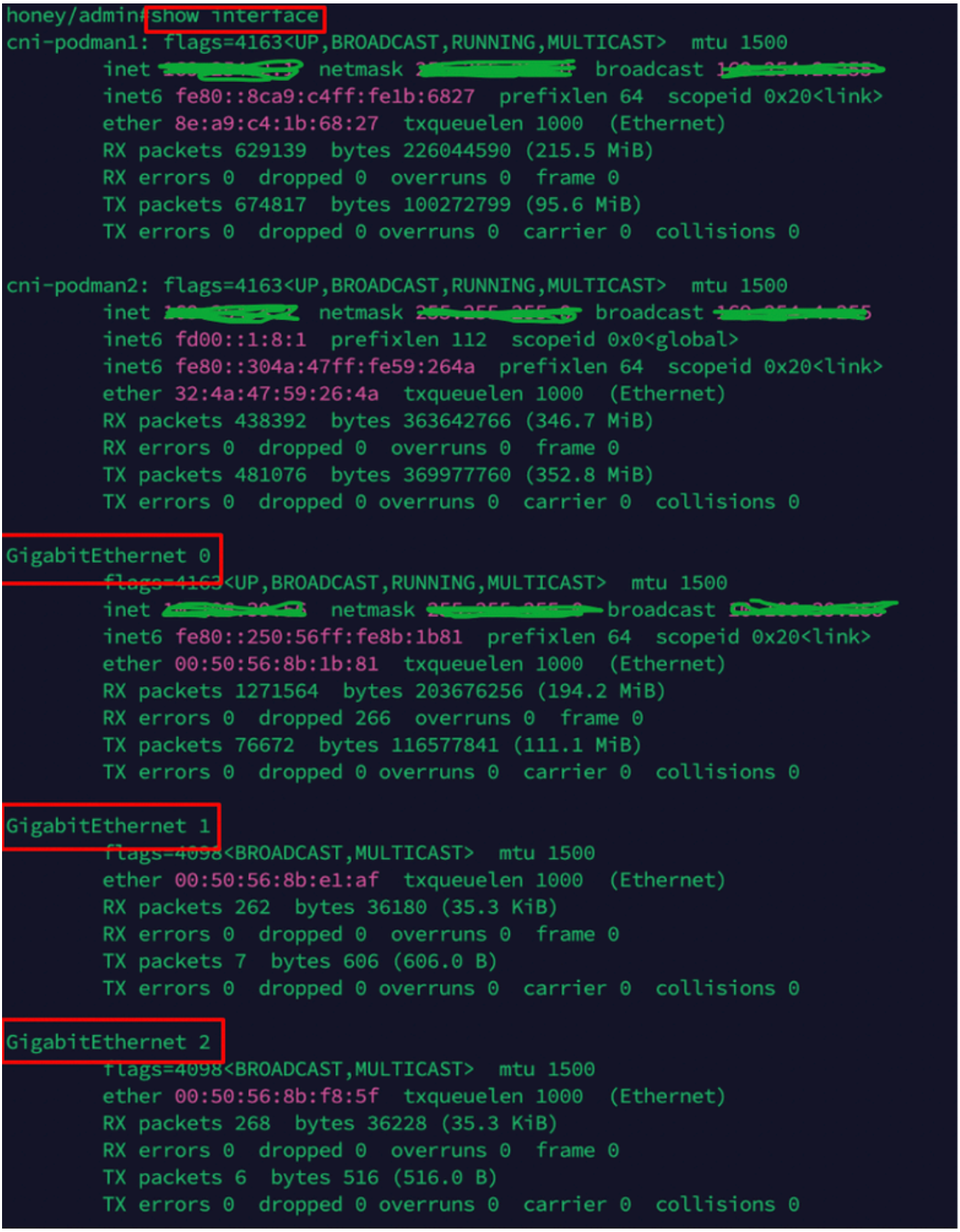


网络拓扑

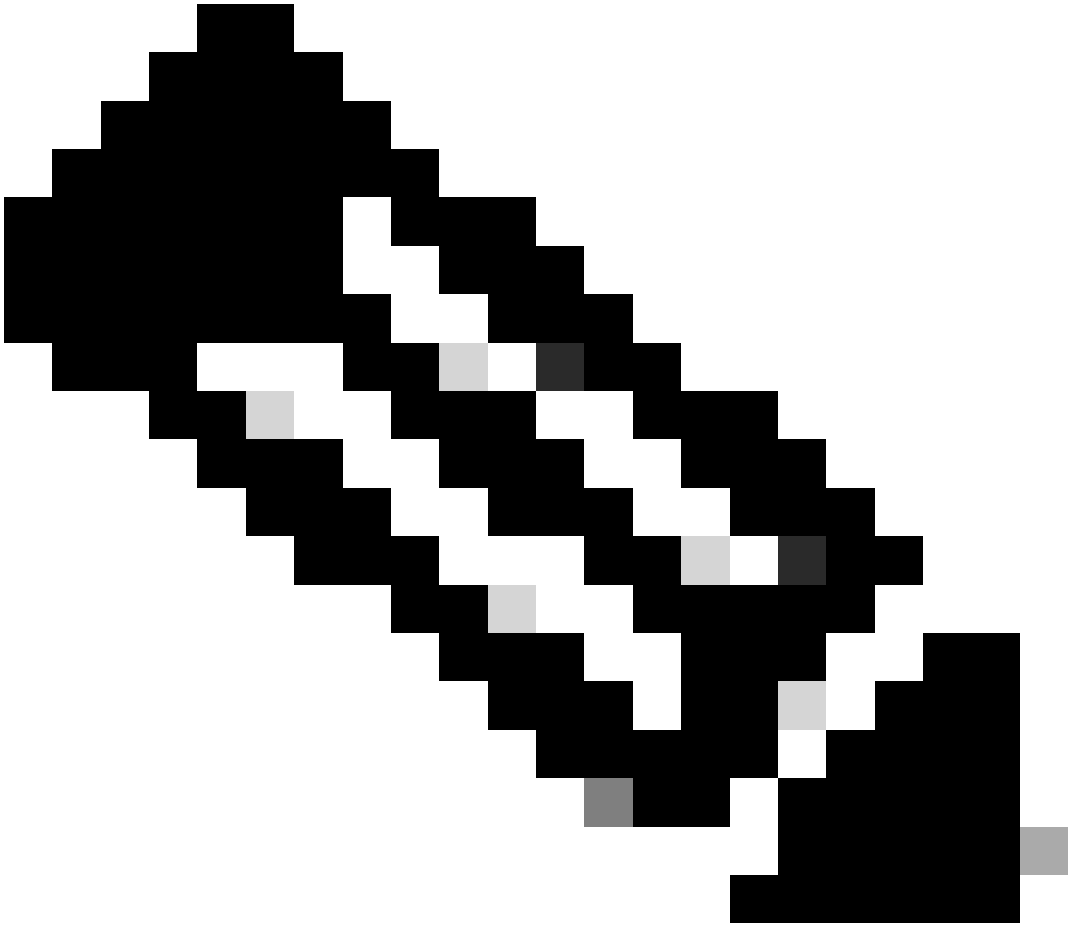
为TACACS+配置身份服务引擎

在ISE中配置千兆以太网1接口的IP地址

1. 登录启用设备管理员的ISE PSN节点的CLI，并使用show interface命令验证可用接口：


honey/admin#show interface
cni-podman1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet [redacted] netmask [redacted] broadcast [redacted]
inet6 fe80::8ca9:c4ff:fe1b:6827 prefixlen 64 scopeid 0x20<link>
ether 8e:a9:c4:1b:68:27 txqueuelen 1000 (Ethernet)
RX packets 629139 bytes 226044590 (215.5 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 674817 bytes 100272799 (95.6 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
cni-podman2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet [redacted] netmask [redacted] broadcast [redacted]
inet6 fd00::1:8:1 prefixlen 112 scopeid 0x0<global>
inet6 fe80::304a:47ff:fe59:264a prefixlen 64 scopeid 0x20<link>
ether 32:4a:47:59:26:4a txqueuelen 1000 (Ethernet)
RX packets 438392 bytes 363642766 (346.7 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 481076 bytes 369977760 (352.8 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
GigabitEthernet 0
flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet [redacted] netmask [redacted] broadcast [redacted]
inet6 fe80::250:56ff:fe8b:1b81 prefixlen 64 scopeid 0x20<link>
ether 00:50:56:8b:1b:81 txqueuelen 1000 (Ethernet)
RX packets 1271564 bytes 203676256 (194.2 MiB)
RX errors 0 dropped 266 overruns 0 frame 0
TX packets 76672 bytes 116577841 (111.1 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
GigabitEthernet 1
flags=4098<BROADCAST,MULTICAST> mtu 1500
ether 00:50:56:8b:e1:af txqueuelen 1000 (Ethernet)
RX packets 262 bytes 36180 (35.3 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 7 bytes 606 (606.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
GigabitEthernet 2
flags=4098<BROADCAST,MULTICAST> mtu 1500
ether 00:50:56:8b:f8:5f txqueuelen 1000 (Ethernet)
RX packets 268 bytes 36228 (35.3 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 6 bytes 516 (516.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

验证ISE中的接口



注意：在此配置中，ISE中仅配置三个接口，重点是Gigabit Ethernet 1接口。相同的步骤可用于配置所有接口的IP地址。默认情况下，ISE最多支持六个千兆以太网接口。

2.从同一PSN节点的CLI中，使用以下命令为千兆以太网1接口分配IP地址：

hostnameofise#configure t

hostnameofise/admin(config)#interface Gigabit Ethernet 1

hostnameofise/admin(config-GigabitEthernet-1)# <ip address> <subnet netmask> %更改IP地址可能导致ise服务重新启动

是否继续更改IP地址？

是否继续？[是，否]是

3.执行步骤2会使ISE节点服务重新启动。要验证ISE服务的状态，请运行show application status ise命令，并确保服务的状态正在按照以下屏幕截图运行：

```
honey/admin#show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          1739169
Database Server                        running          102 PROCESSES
Application Server                     running          1755746
Profiler Database                      running          1746379
ISE Indexing Engine                    running          1757121
AD Connector                           running          1759148
M&T Session Database                   running          1752122
M&T Log Processor                      running          1755926
Certificate Authority Service          running          1759026
EST Service                            running          1786647
SXP Engine Service                     disabled
TC-NAC Service                         disabled
PassiveID WMI Service                  disabled
PassiveID Syslog Service               disabled
PassiveID API Service                  disabled
PassiveID Agent Service                disabled
PassiveID Endpoint Service             disabled
PassiveID SPAN Service                 disabled
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
ISE Messaging Service                  running          1743222
ISE API Gateway Database Service       running          1745409
ISE API Gateway Service                running          1750887
ISE pxGrid Direct Service              running          1874179
Segmentation Policy Service            disabled
REST Auth Service                      disabled
SSE Connector                          disabled
Hermes (pxGrid Cloud Agent)            disabled
McTrust (Meraki Sync Service)          disabled
ISE Node Exporter                      running          1760519
ISE Prometheus Service                 running          1762540
ISE Grafana Service                    running          1765779
ISE MNT LogAnalytics Elasticsearch     running          1768218
ISE Logstash Service                   running          1773207
ISE Kibana Service                     running          1774914
ISE Native IPSec Service               running          1779658
MFC Profiler                           running          1932013
```

ISE服务状态验证

4.使用show interface命令检验Gig1接口的IP地址：

五

```
honey/admin#show interface
cni-podman1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::8ca9:c4ff:fe1b:6827  prefixlen 64  scopeid 0x20<link>
        ether 8e:a9:c4:1b:68:27  txqueuelen 1000  (Ethernet)
        RX packets 633876  bytes 228753800 (218.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 680052  bytes 102100762 (97.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

cni-podman2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fd00::1:8:1  prefixlen 112  scopeid 0x0<global>
        inet6 fe80::304a:47ff:fe59:264a  prefixlen 64  scopeid 0x20<link>
        ether 32:4a:47:59:26:4a  txqueuelen 1000  (Ethernet)
        RX packets 503576  bytes 516105026 (492.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 595701  bytes 383404526 (365.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 0
        flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::250:56ff:fe8b:1b81  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:8b:1b:81  txqueuelen 1000  (Ethernet)
        RX packets 1387052  bytes 213478717 (203.5 MiB)
        RX errors 0  dropped 266  overruns 0  frame 0
        TX packets 136494  bytes 261900250 (249.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 1
        flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::250:56ff:fe8b:e1af  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:8b:e1:af  txqueuelen 1000  (Ethernet)
        RX packets 5165  bytes 1072036 (1.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 2260 (2.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

从CLI验证ISE Gig2接口IP地址

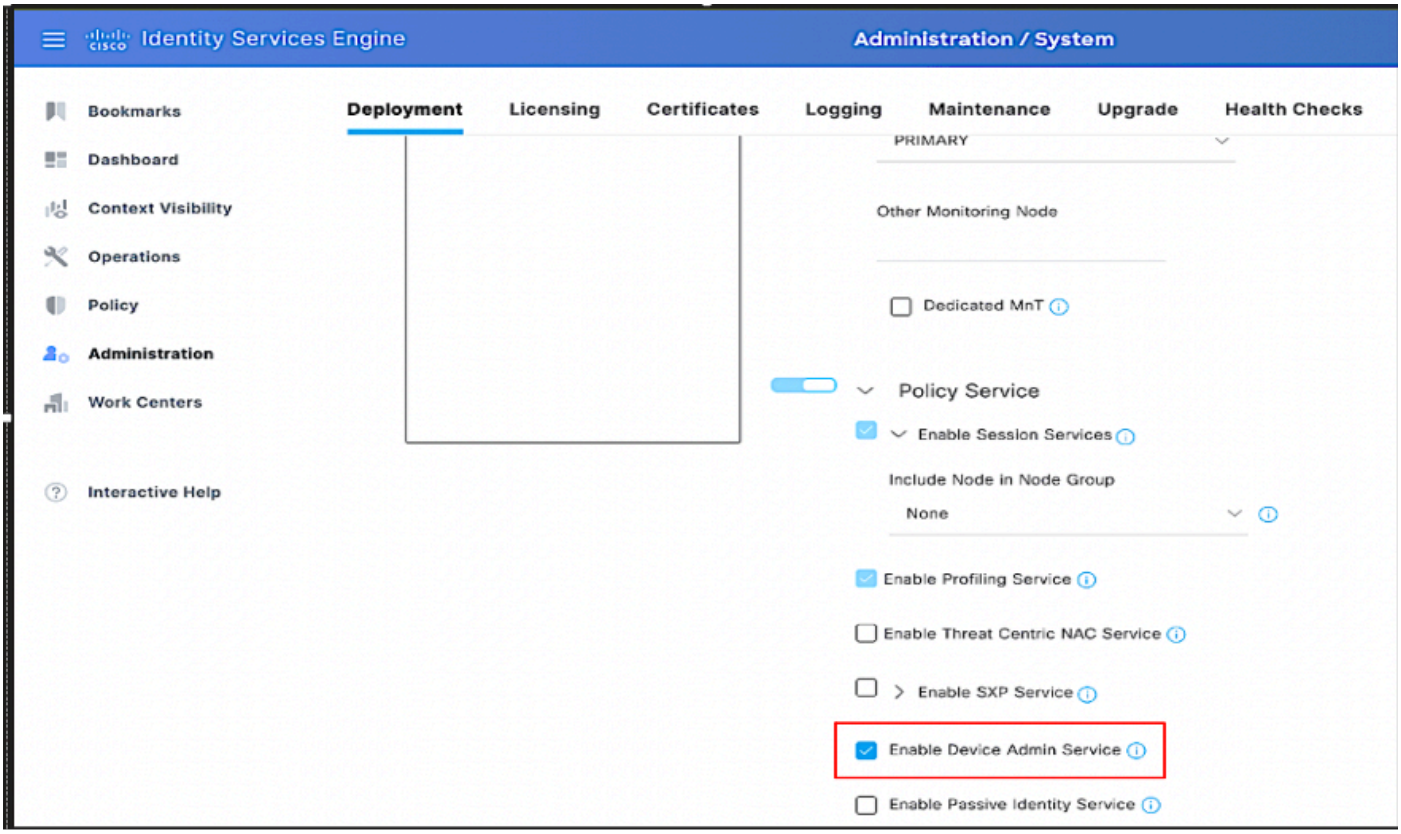
5.使用show ports检验ISE节点中允许使用的端口49 | inc 49命令：

```
honey/admin#show ports | include 49
        tcp: 127.0.0.1:8888, 169.254.4.1:49, 169.254.2.1:49, [redacted]:49, [redacted]:49,
```

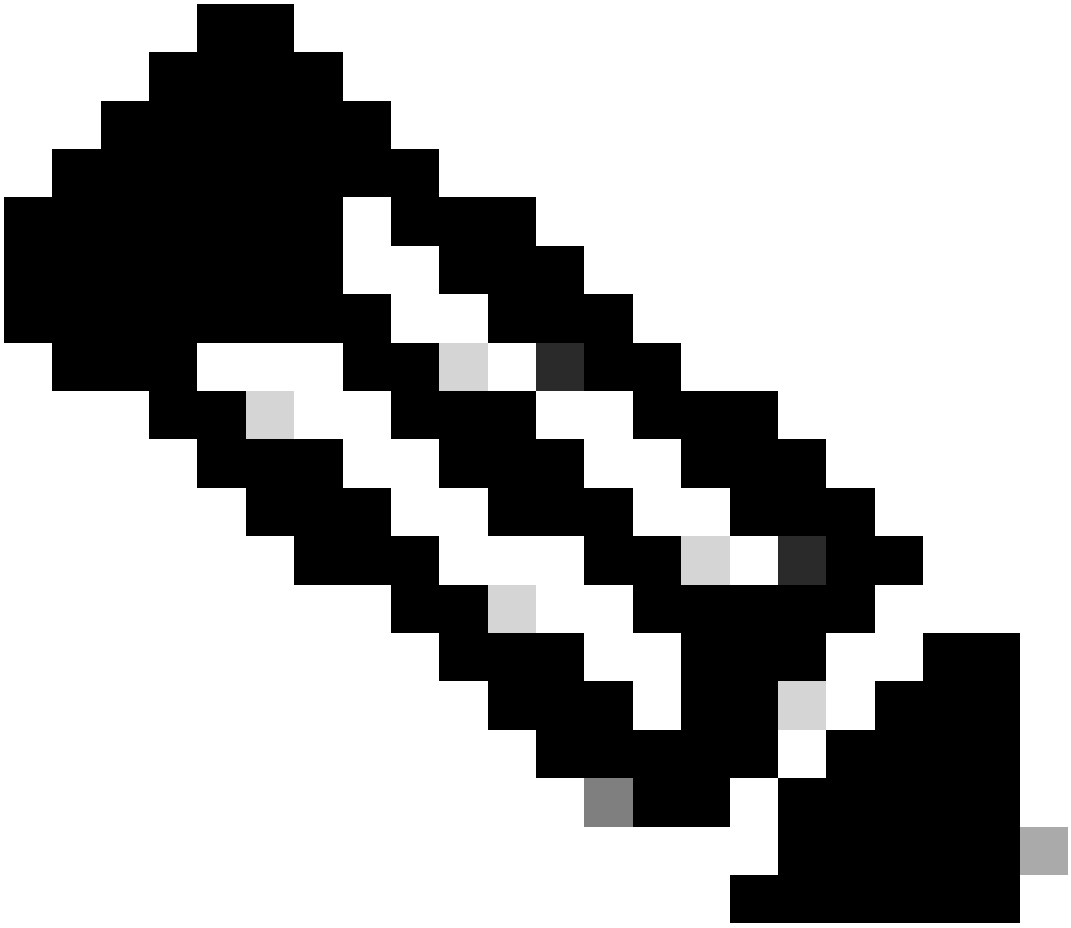
在ISE中验证端口49允许

在ISE中启用设备管理

导航到ISE > Administration > Deployment > Select the PSN node，然后选中Enable Device admin service:



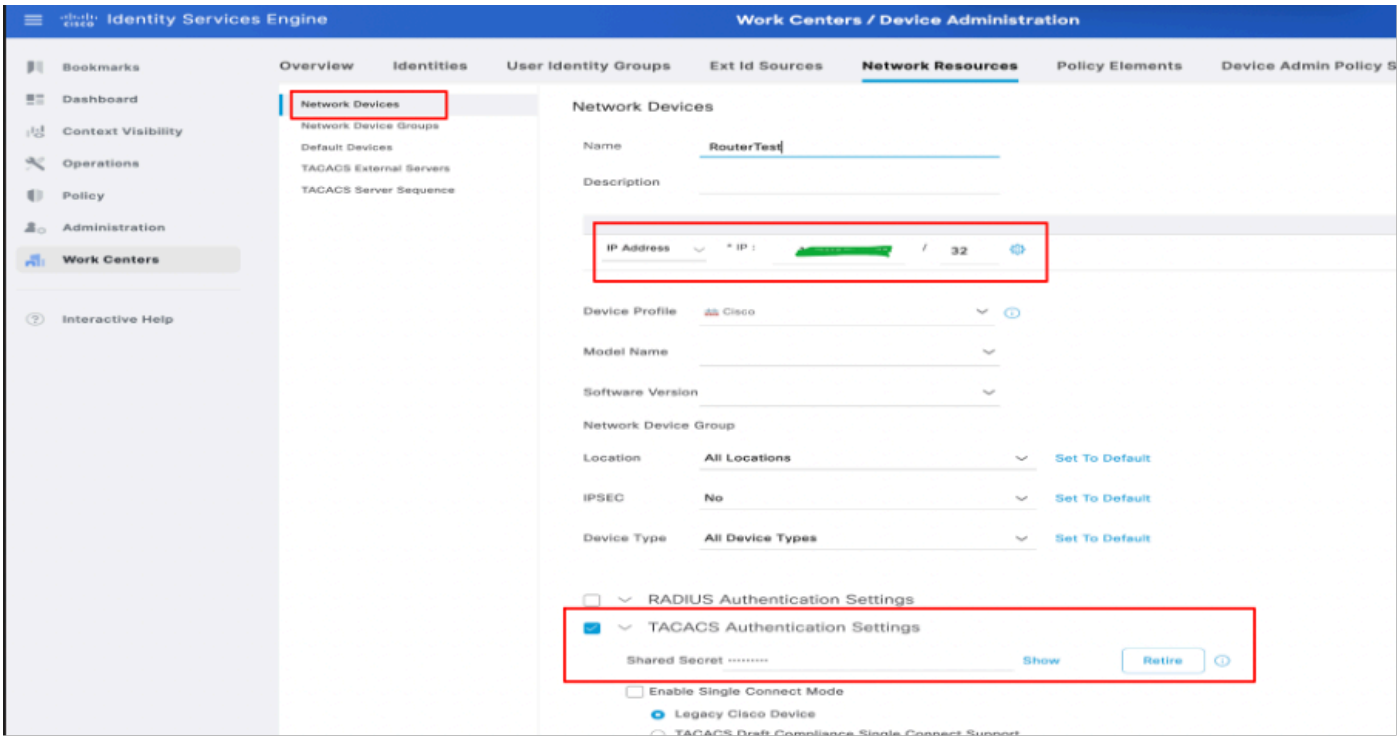
在ISE中启用设备管理服务



注意：要启用设备管理服务，需要设备管理许可证。

在ISE中添加网络设备

1.定位至工作中心>设备管理>网络资源>网络设备。单击 Add。提供名称、IP地址。选中TACACS+ Authentication Settings复选框并提供共享密钥。



在ISE中配置网络设备

2.按照上述步骤添加TACACS身份验证所需的所有网络设备。

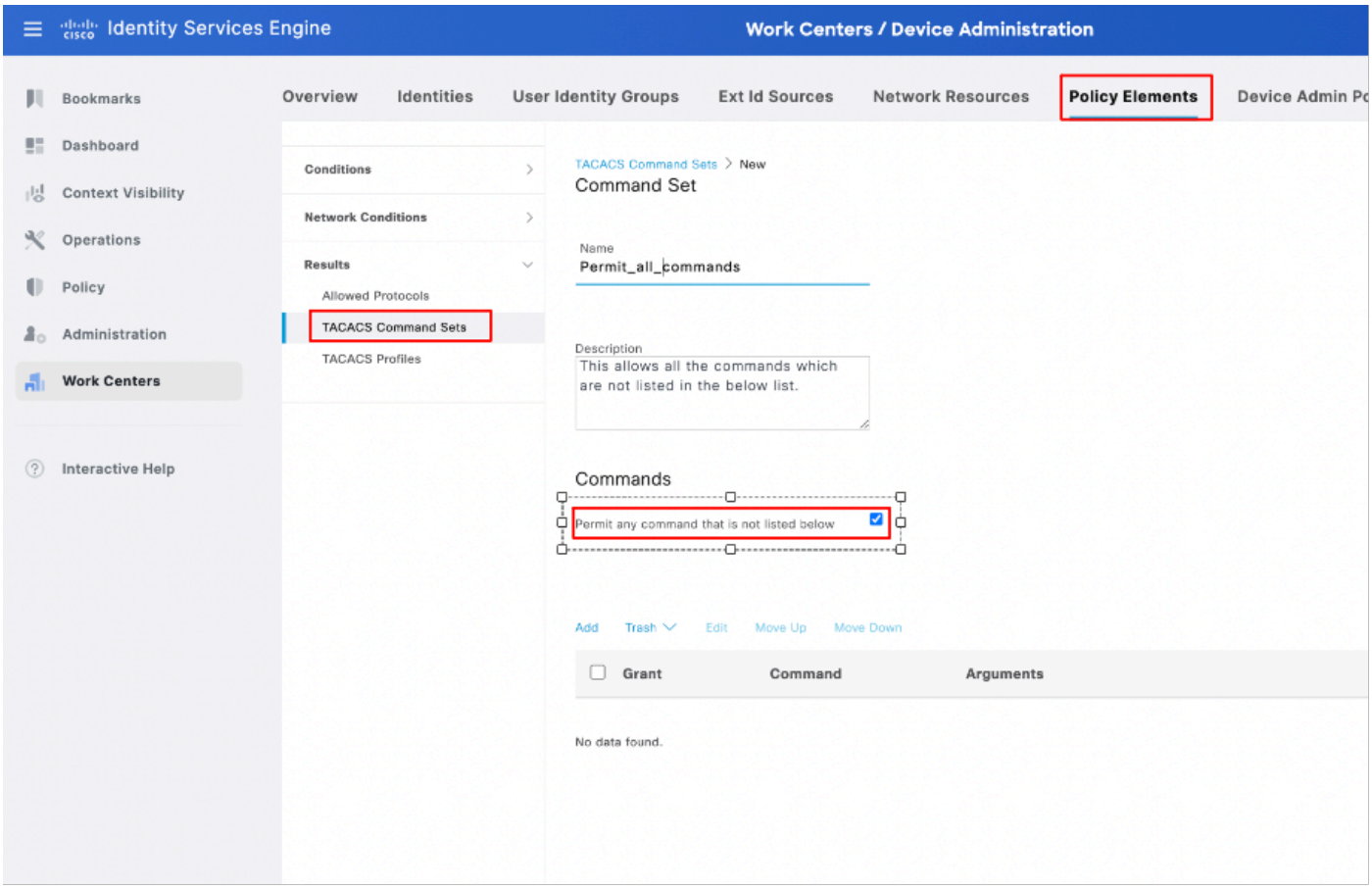
配置TACACS+命令集

本演示配置了两个命令集：

Permit_all_commands分配给用户admin并允许设备上的所有命令。

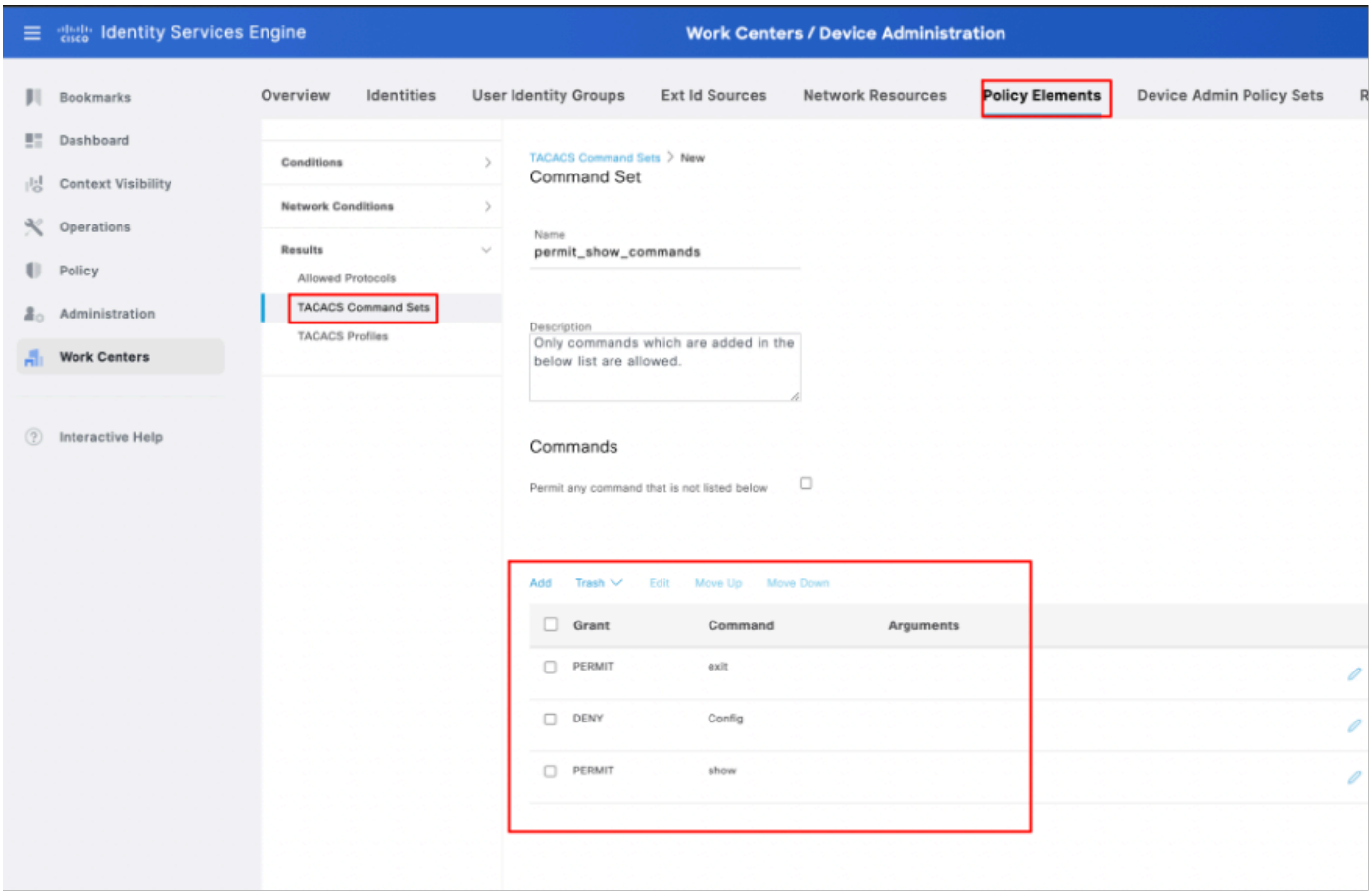
permit_show_commands，分配给用户并仅允许show命令

1. 导航到工作中心>设备管理>策略结果> TACACS命令集。单击Add.提供名称PermitAllCommands，然后选择Permit any command复选框（未列出）。单击 submit。



在ISE中配置命令集

2.定位至“工作中心”>“设备管理”>“策略结果”>“TACACS命令集”。单击“添加”。提供名称PermitShowCommands，单击“添加”，最后单击permit show和exit命令。默认情况下，如果参数留空，则包含所有参数。单击 submit。

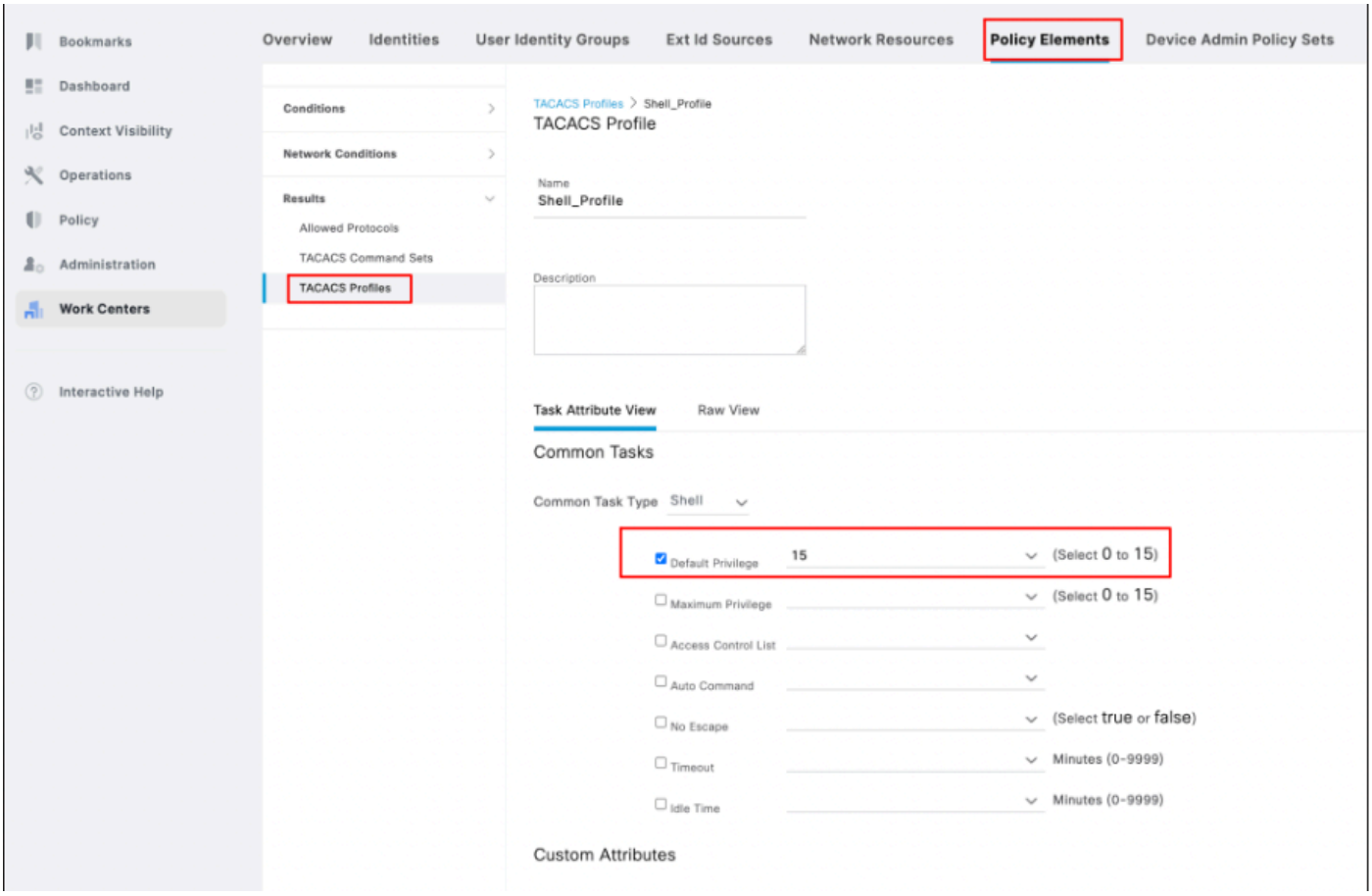


在ISE中配置permit_show_commands

配置TACACS+配置文件

配置单个TACACS+配置文件，并通过命令集执行命令授权。

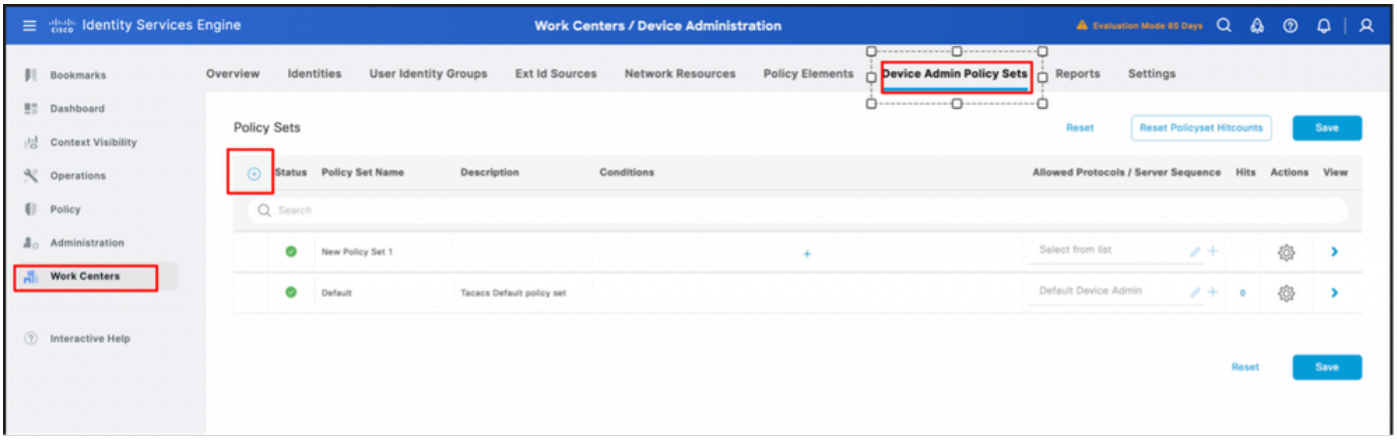
要配置TACACS+配置文件，请导航到工作中心 > 设备管理 > 策略结果 > TACACS配置文件。单击Add，为外壳配置文件提供名称，选中Default Privilege复选框，然后输入值15。最后，单击Submit。



在ISE中配置TACACS配置文件

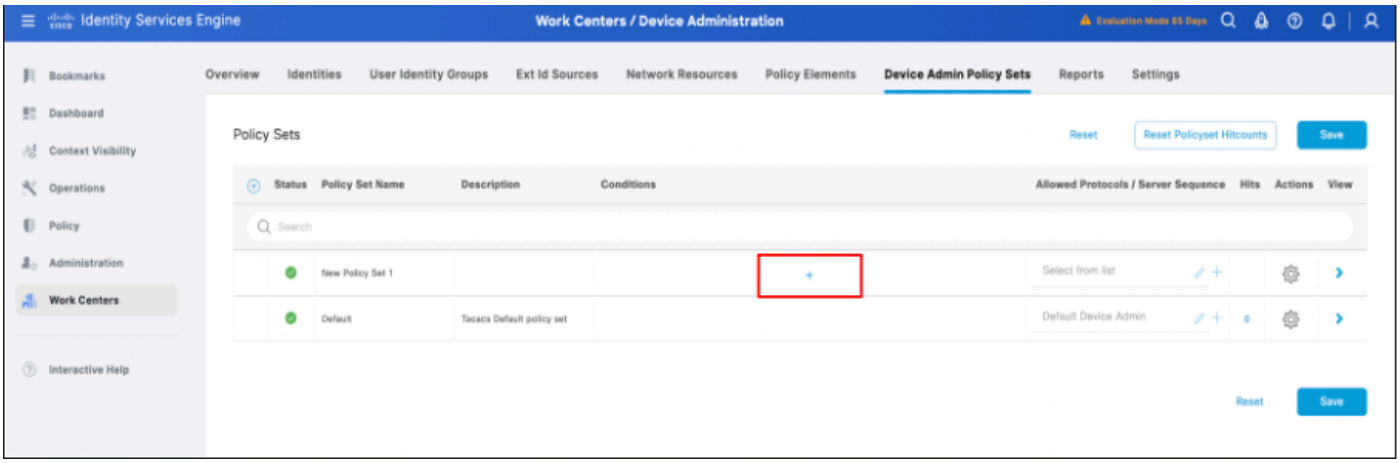
配置TACACS+身份验证和授权配置文件

1.登录到ISE PAN GUI -> Administration -> Work Centers -> Device administration -> Device admin policy sets。点击+（加）图标创建新策略。在本例中，策略集命名为New Policy set 1。



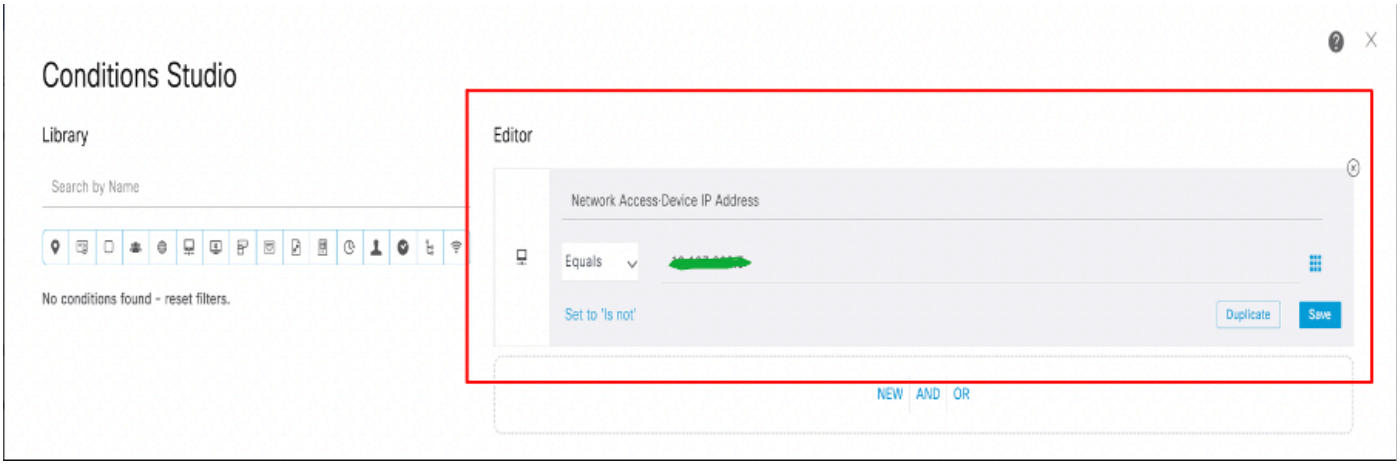
在ISE中配置策略集

2.在保存策略集之前，需要配置条件，如本屏幕截图所示。点击+（加）图标配置策略集的条件。

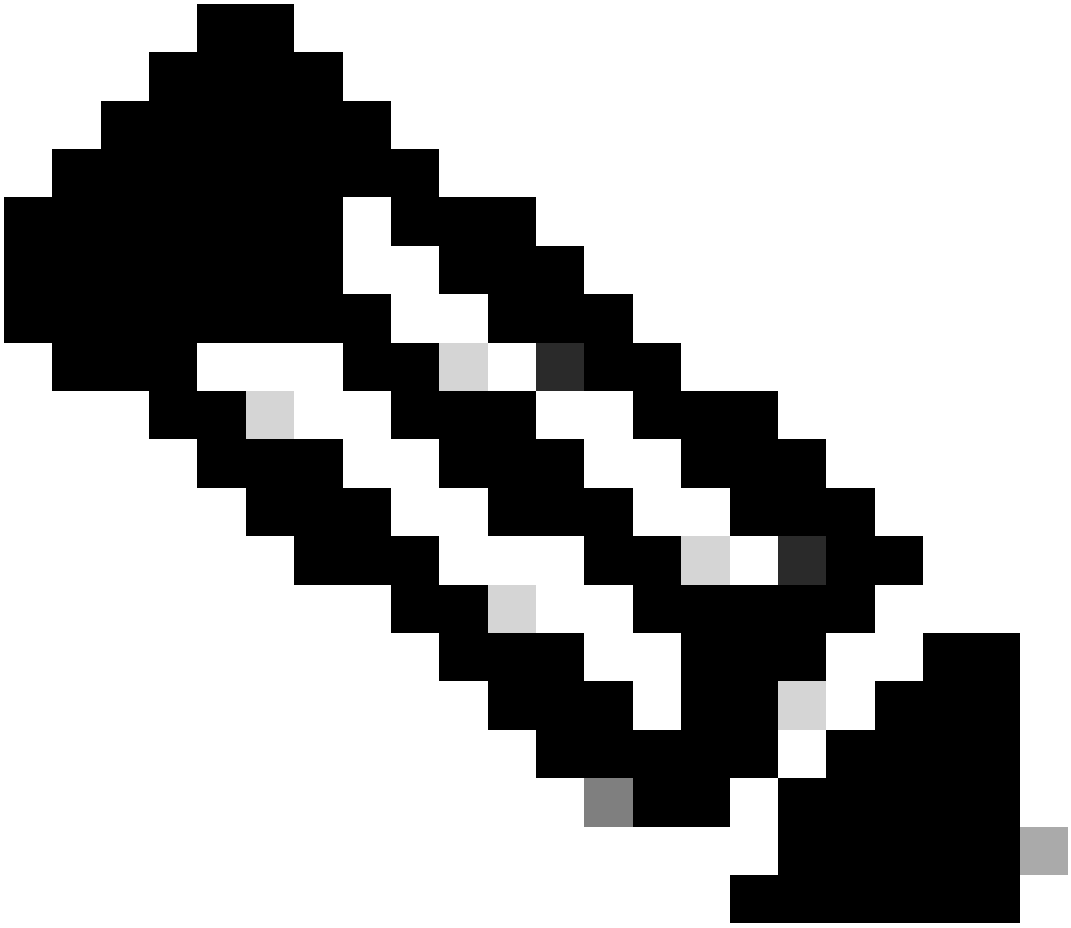


在ISE中配置策略集条件

3.单击第2步中提到的+（加号）图标后，将打开“条件工作室”对话框。在此，配置所需的条件。将条件保存为新条件或现有条件，然后滚动。单击use。

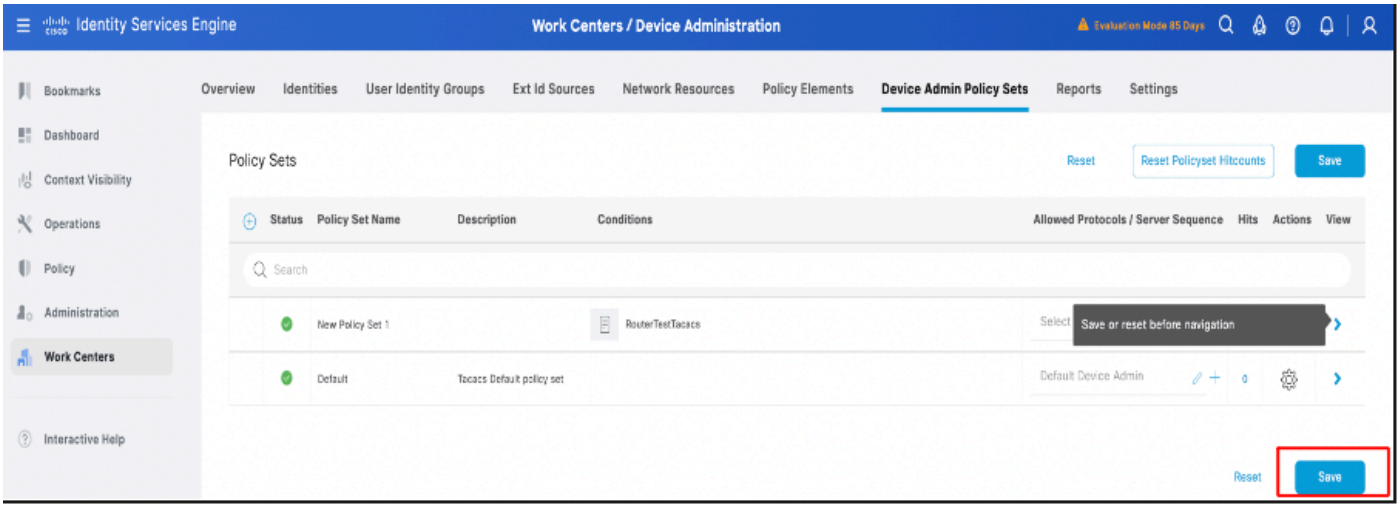


在ISE中配置策略集条件



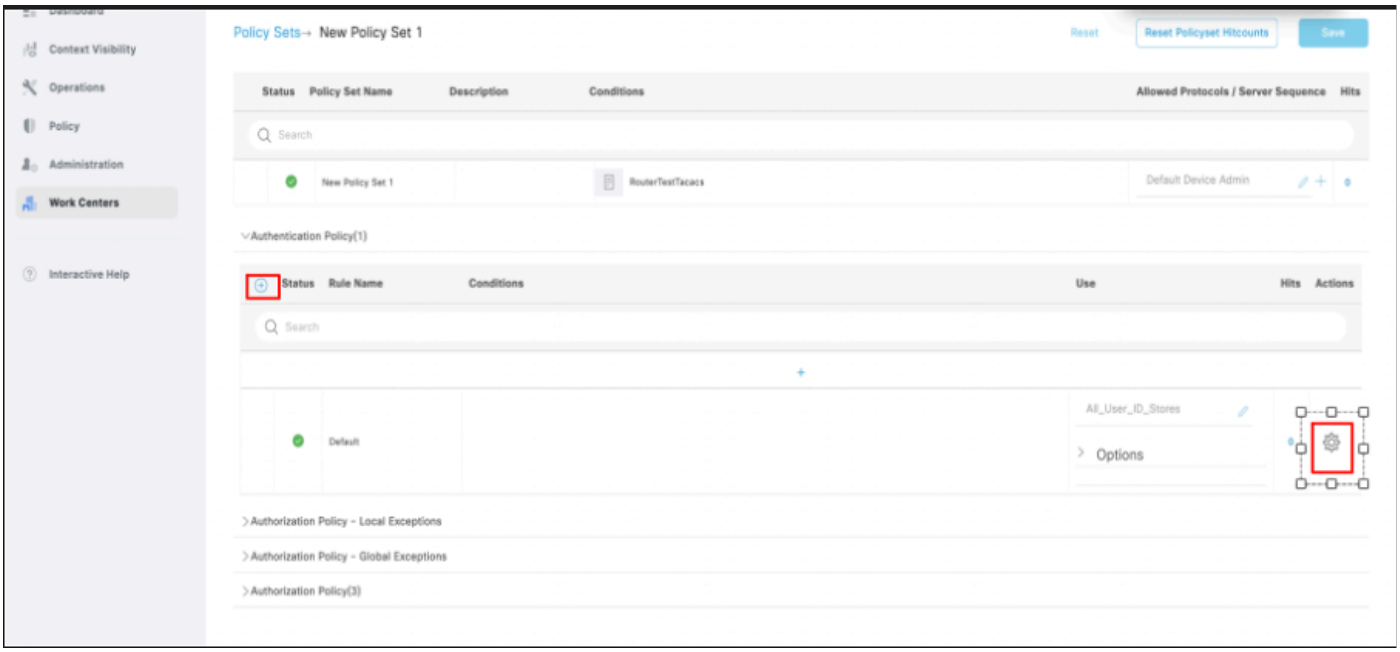
注意：对于此文档，条件与网络设备IP匹配。但是，条件可能因部署要求而异。

4.配置并保存条件后，将允许的协议配置为Default device admin。通过单击Save选项保存创建的策略集。

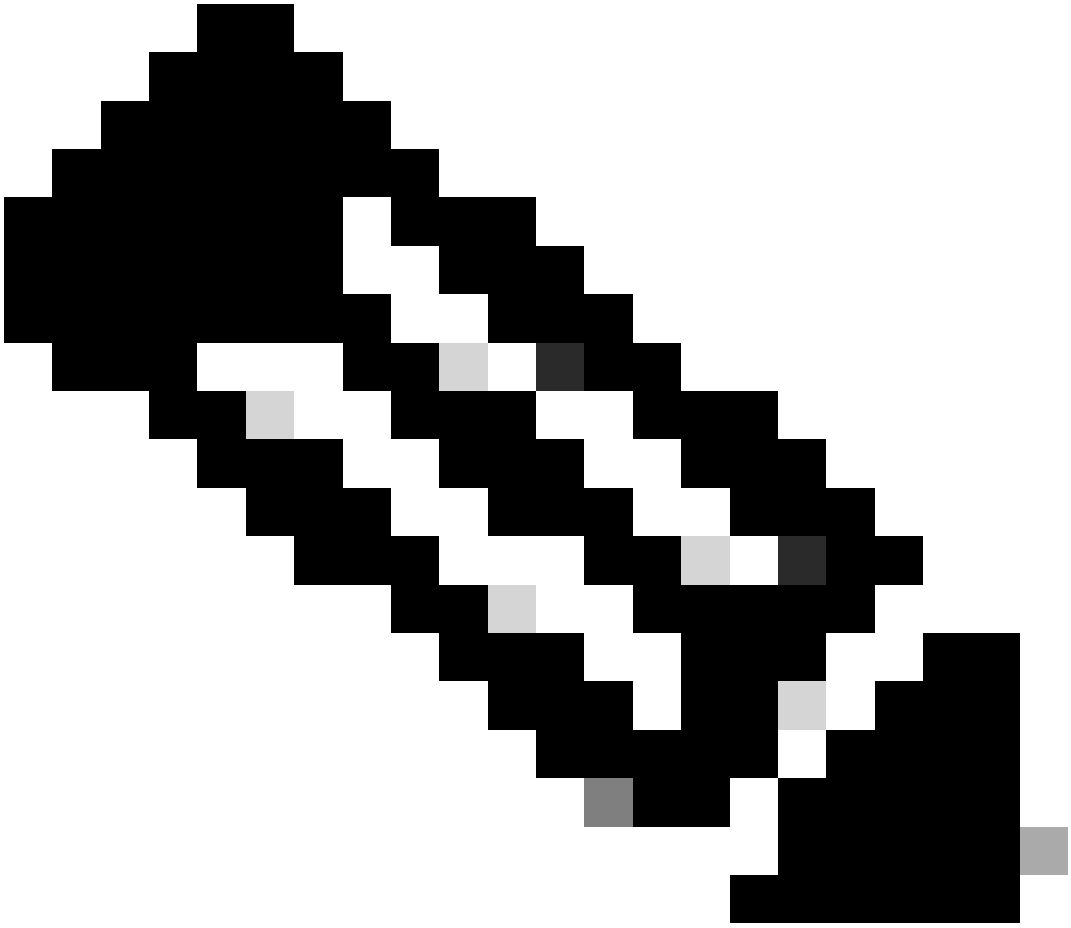


策略集配置确认。

5.展开New Policy set -> Authentication Policy(1) ->单击+（加号）图标或单击gear Icon，然后单击Insert new row above，创建新的身份验证策略。

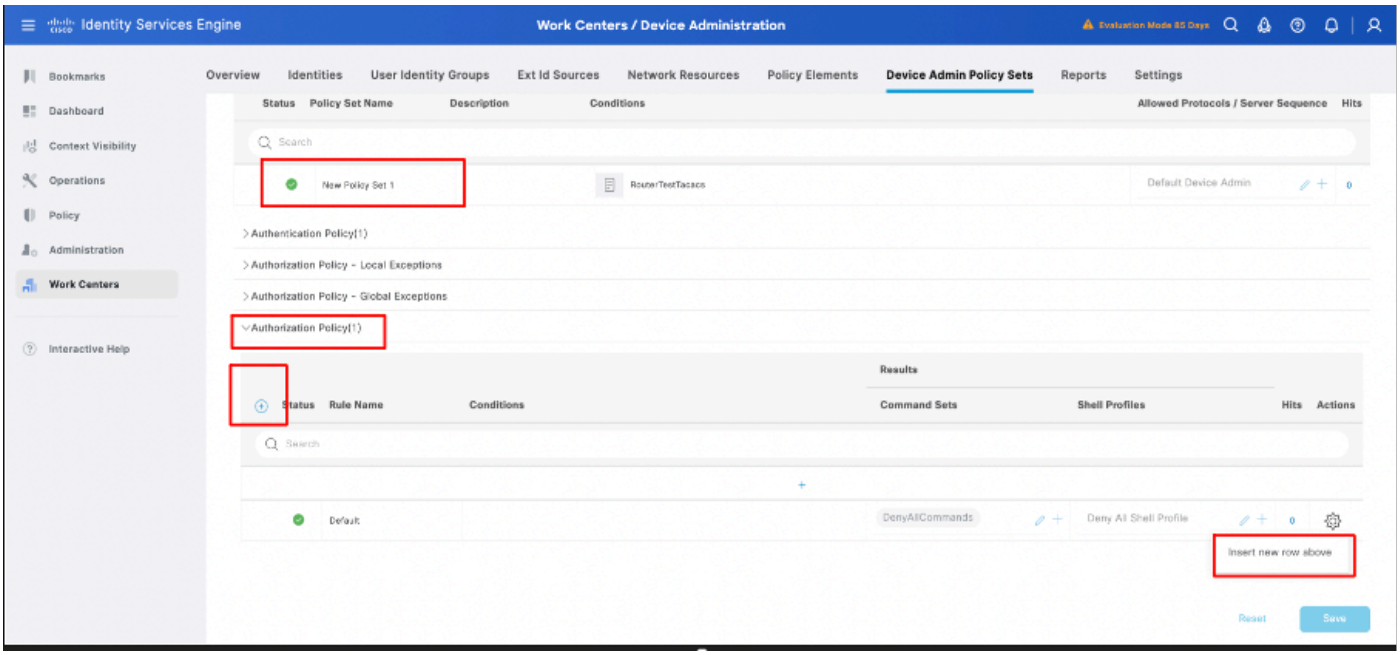


在策略集中配置身份验证策略。



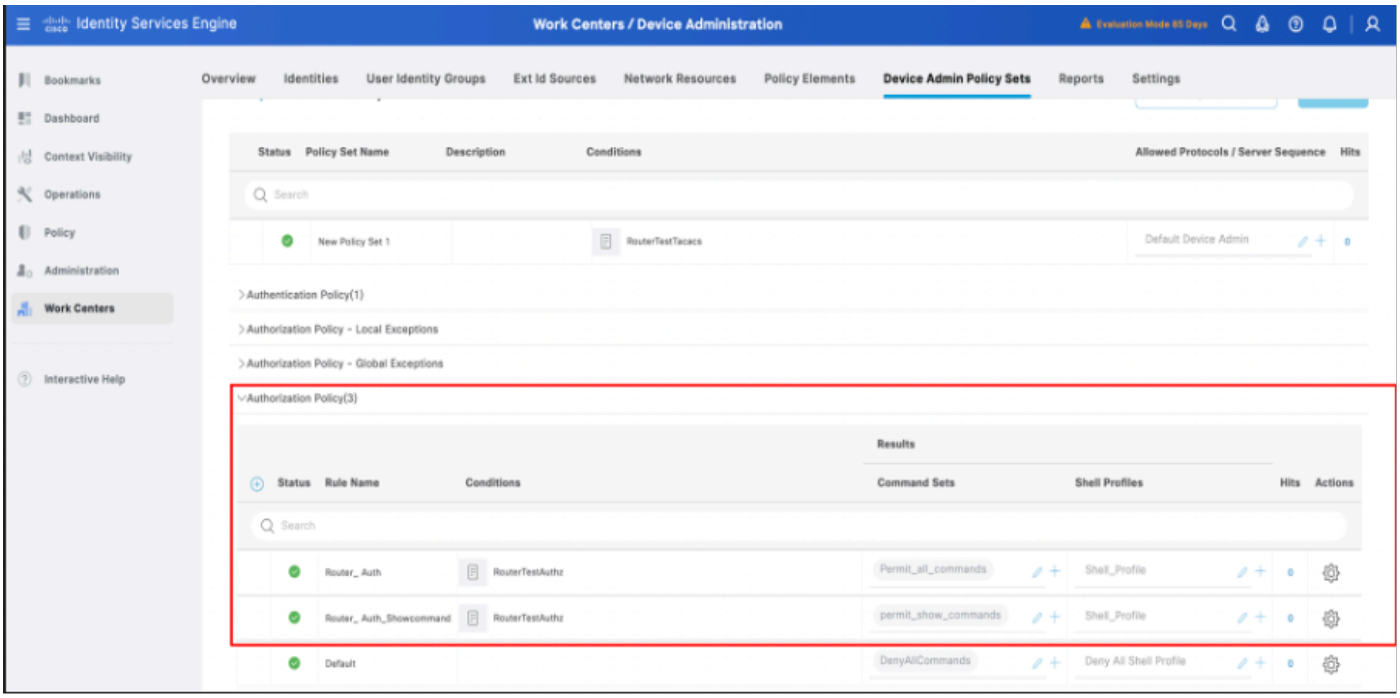
注意：在本演示中，使用默认身份验证策略集All_User_ID_Stores。但是，身份存储库的使用可根据部署要求进行自定义。

6.展开New Policy set -> Authorization Policy(1)。 点击+(加号)图标或点击齿轮图标。然后，在上面插入新行以创建授权策略。

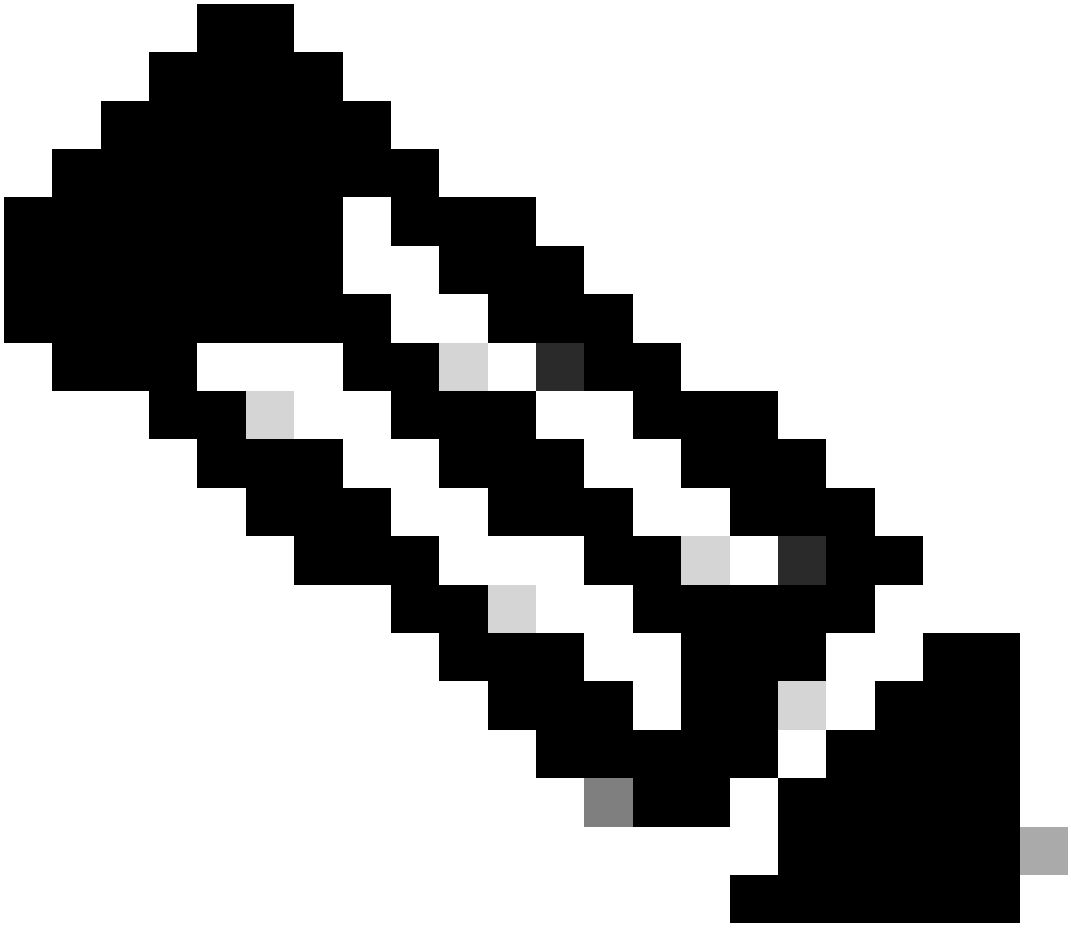


授权策略的配置

7.使用映射到授权策略的条件、命令集和外壳配置文件配置授权策略。



在ISE中完成授权策略的配置

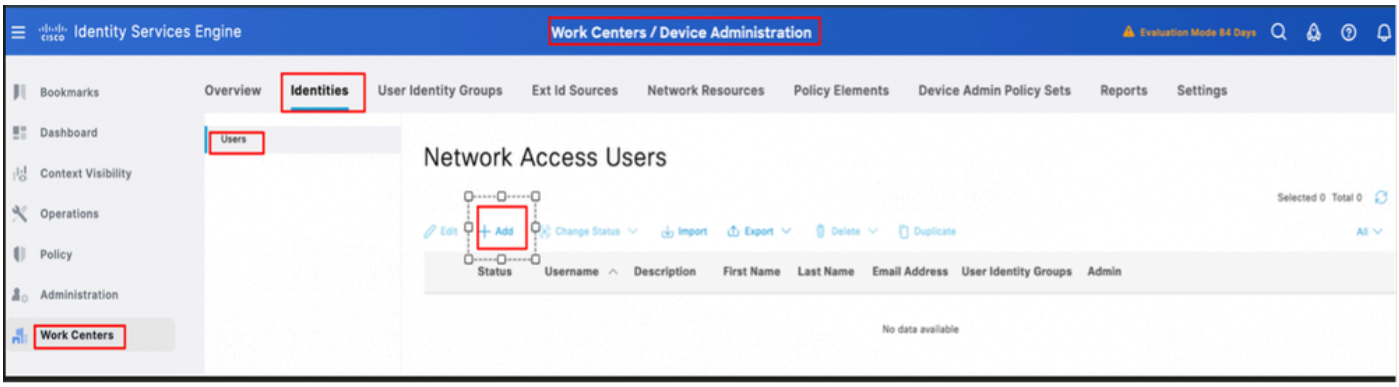


注意：配置的条件取决于实验环境，并可根据部署要求进行配置。

8.按照前6步为交换机或用于TACACS+的任何其他网络设备配置策略集。

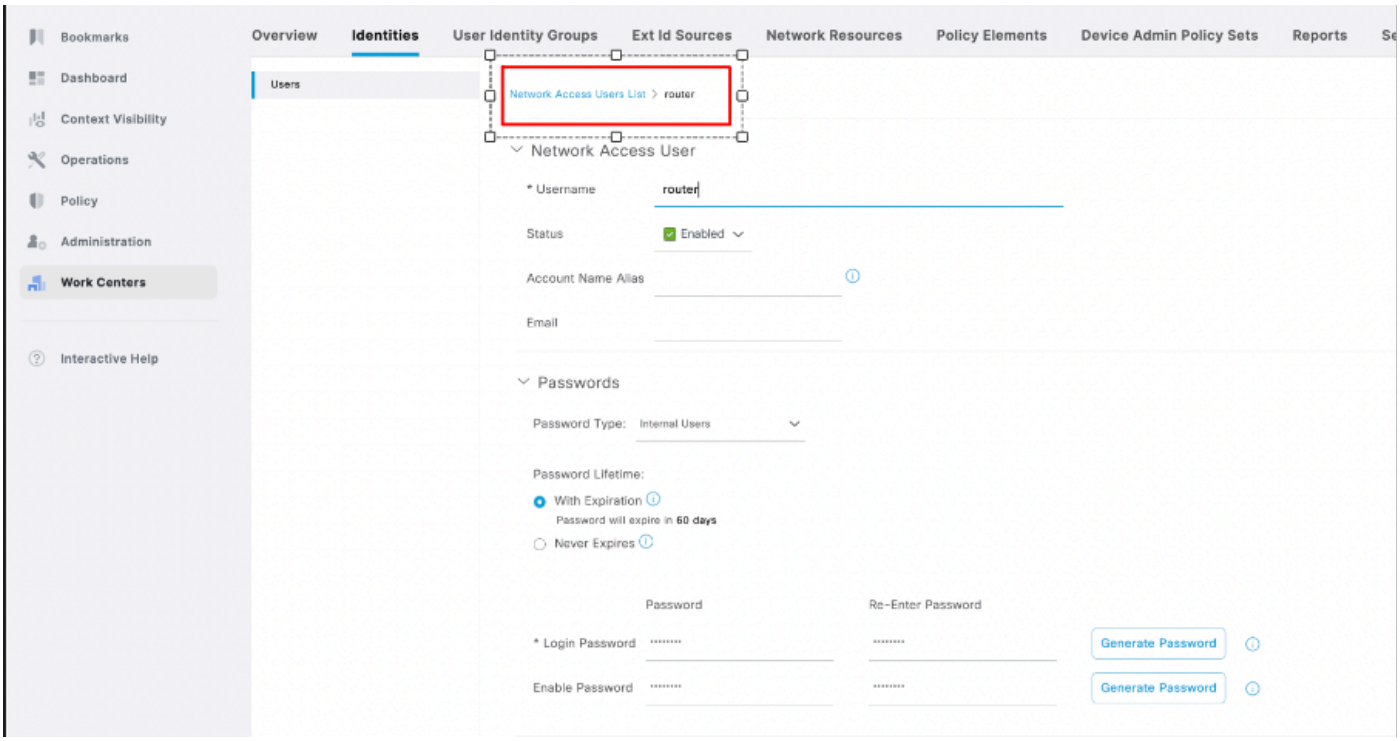
在ISE中为NAD的TACACS身份验证配置网络访问用户

1. 导航到Workcenters -> Device Administration -> Identities -> Users。点击+(plus)图标以创建新用户。



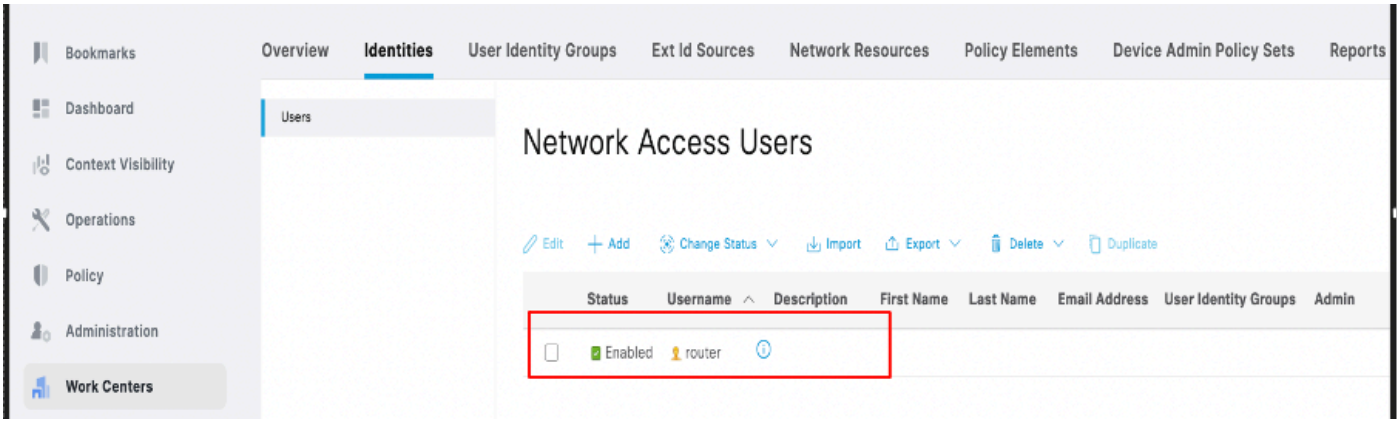
在ISE中配置网络访问用户

2.提供以展开用户名和密码详细信息，将用户映射到用户身份组（可选），然后单击提交。



配置网络访问用户 — 继续

3.在Work Centers -> Identities -> Users -> Network Access users中提交用户名配置后，用户将被可视地配置并启用。



确认网络访问用户配置。

为TACACS+配置路由器

为TACACS+身份验证和授权配置Cisco IOS路由器

1. 登录到路由器的CLI并运行这些命令以在路由器中配置TACACS。

ASR1001-X(config)#aaa new-model — 在NAD中启用aaa所需的命令

ASR1001-X(config)#aaa session-id common。 — 在NAD中启用aaa所需的命令。

ASR1001-X(config)#aaa authentication login default group tacacs+ local

ASR1001-X(config)#aaa authorization exec default group tacacs+

ASR1001-X(config)#aaa authorization network list1 group tacacs+

ASR1001-X(config)#tacacs server ise1

ASR1001-X(config-server-tacacs)#address ipv4 <TACACS服务器的IP地址> . — ISE接口G1 IP地址。

ASR1001-X(config-server-tacacs)# key XXXXX

ASR1001-X(config)# aaa group server tacacs+ isegroup

ASR1001-X(config-sg-tacacs+)#server称ise1

ASR1001-X(config-sg-tacacs+)#ip vrf forwarding Mgmt-intf

ASR1001-X(config-sg-tacacs+)#ip tacacs source-interface GigabitEthernet0

ASR1001-X(config-sg-tacacs+)#ip tacacs source-interface GigabitEthernet1

ASR1001-X（配置）#exit

2.保存路由器TACACS+配置后，使用show run aaa命令验证TACACS+配置。

ASR1001-X#show run aaa

!

aaa authentication login default group isegroup local

aaa authorization exec default group isegroup

aaa authorization network list1 group isegroup

username admin password 0 XXXXXXX

!

```
tacacs服务器ise1
 address ipv4 <TACACS服务器的IP地址>
 密钥XXXXX
!
!
aaa group server tacacs+ isegroup
 服务器名称ise1
 ip vrf forwarding Mgmt-intf
 ip tacacs source-interface GigabitEthernet1
!
!
!
aaa new-model
aaa session-id common
!
!
```

为TACACS+配置交换机

为TACACS+身份验证和授权配置交换机

1. 登录到交换机的CLI并运行这些命令以在交换机中配置TACACS。

```
C9200L-48P-4X#configure t
输入配置命令，每行一条。 以 CNTL/Z 结束。
C9200L-48P-4X(config)#aaa新型号。 — 在NAD中启用aaa所需的命令
C9200L-48P-4X(config)#aaa session-id common。 — 在NAD中启用aaa所需的命令。
C9200L-48P-4X(config)#aaa authentication login default group isegroup local
C9200L-48P-4X(config)#aaa authorization exec default group isegroup
C9200L-48P-4X(config)#aaa authorization network list1 group isegroup
```

C9200L-48P-4X(config)#tacacs server ise1

C9200L-48P-4X(config-server-tacacs)#address ipv4 <TACACS服务器的IP地址> — ISE接口G1 IP地址。

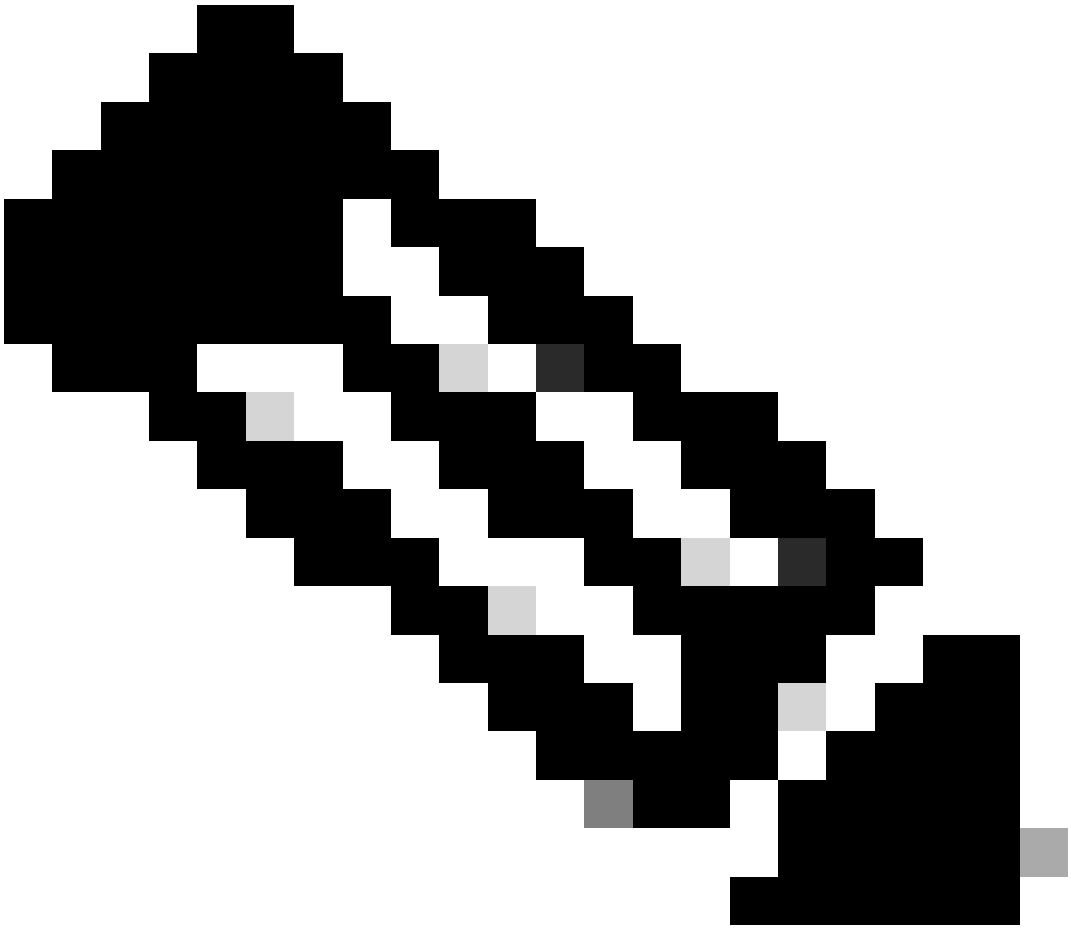
C9200L-48P-4X(config-server-tacacs)#key XXXXX

C9200L-48P(config)#aaa group server tacacs+ isegroup

C9200L-48P(config-sg-tacacs+)#server称ise1

C9200L-48P-4X（配置）#exit

C9200L-48P-4X#wr mem



注意：在需要TACACS+配置中，tacacs+ 是可以根据部署要求自定义的组。

2.保存交换机TACACS+配置后，使用show run aaa命令检验TACACS+配置。

```
C9200L-48P#show run aaa
!
aaa authentication login default group isegroup local
aaa authorization exec default group isegroup
aaa authorization network list1 group isegroup
username admin password 0 XXXXX
!
!
tacacs服务器ise1
 address ipv4 <TACACS服务器的IP地址>
 密钥XXXXX
!
!
aaa group server tacacs+ isegroup
 服务器名称ise1
!
!
!
aaa new-model
aaa session-id common
!
!
```

确认

从路由器验证

在路由器的CLI中，使用test aaa group tacacsgroupname username password new命令针对具有千兆以太网1接口的ISE验证TACACS+。

以下是路由器和ISE的输出示例：

从路由器验证端口49:

ASR1001-X#telnet ISE千兆1接口IP 49

正在尝试ISE GIg 1接口IP， 49..Open（未解决）

ASR1001-X#test aaa group isegroup router XXXX新

正在发送密码

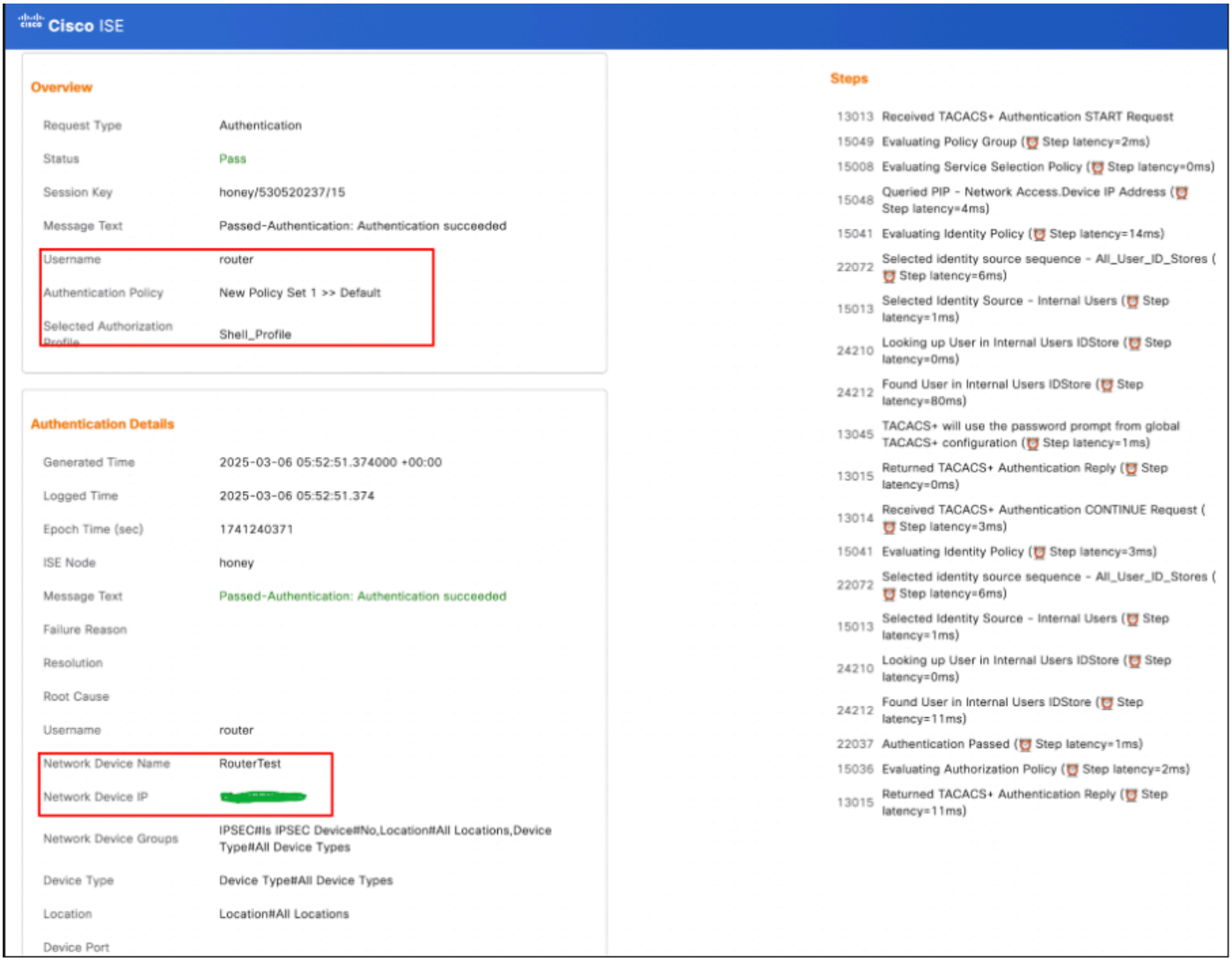
用户已成功通过身份验证

用户属性

用户名0 "router"

reply-message 0 "密码："

要从ISE进行验证，请登录GUI -> Operations -> TACACS live logs，然后在Network Device Details字段中使用路由器IP进行过滤。



来自ISE的TACACS实时日志 — 路由器验证。

交换机验证

在交换机的CLI中，使用test aaa group tacacsgroupname username password newn命令验证针对千兆以太网1接口的ISE的TACACS+身份验证：

以下是交换机和ISE的输出示例。

从交换机验证端口49:

C9200L-48P# telnet ISE Gig1接口IP 49

正在尝试ISE Gig1接口IP， 49..Open（未解决）

C9200L-48P#test aaa group isegroup switch XXXX新

正在发送密码

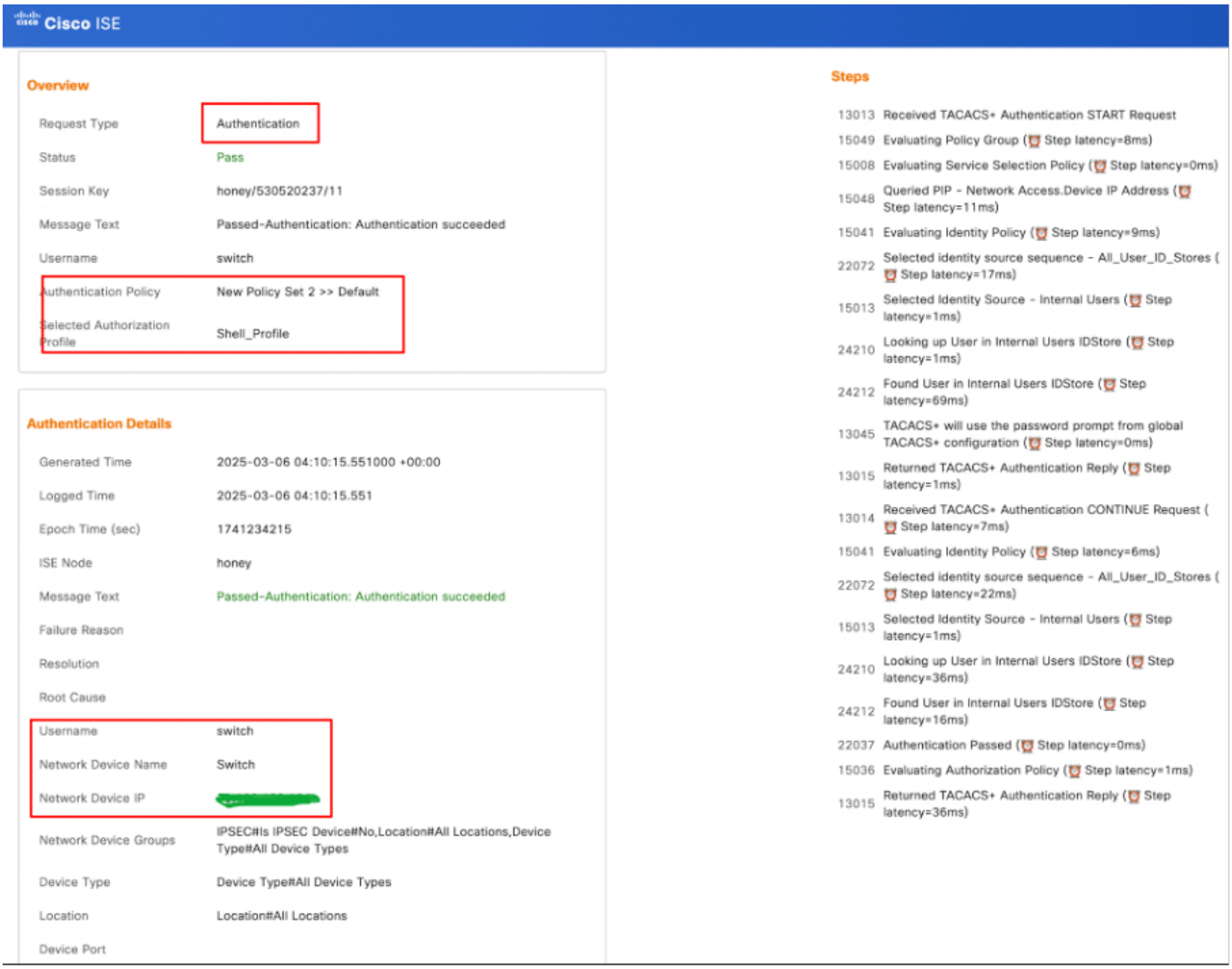
用户已成功通过身份验证

用户属性

username 0 "switch"

reply-message 0 "密码："

要从ISE进行验证，请登录GUI -> Operations -> TACACS live logs，然后在Network Device Details字段中使用交换机IP进行过滤。



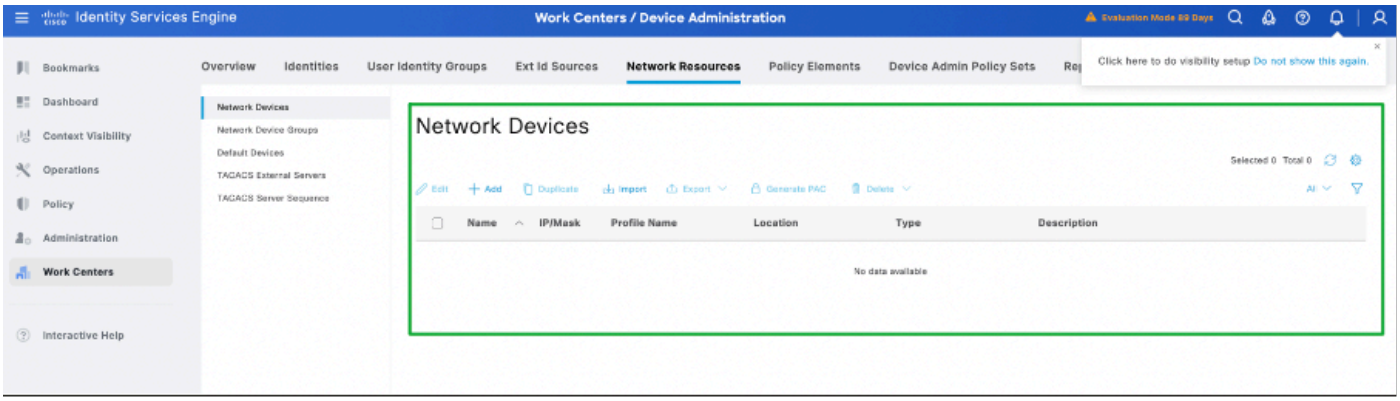
来自ISE的TACACS实时日志 — 交换机验证。

故障排除

本部分讨论发现的一些与TACACS+身份验证相关的常见问题。

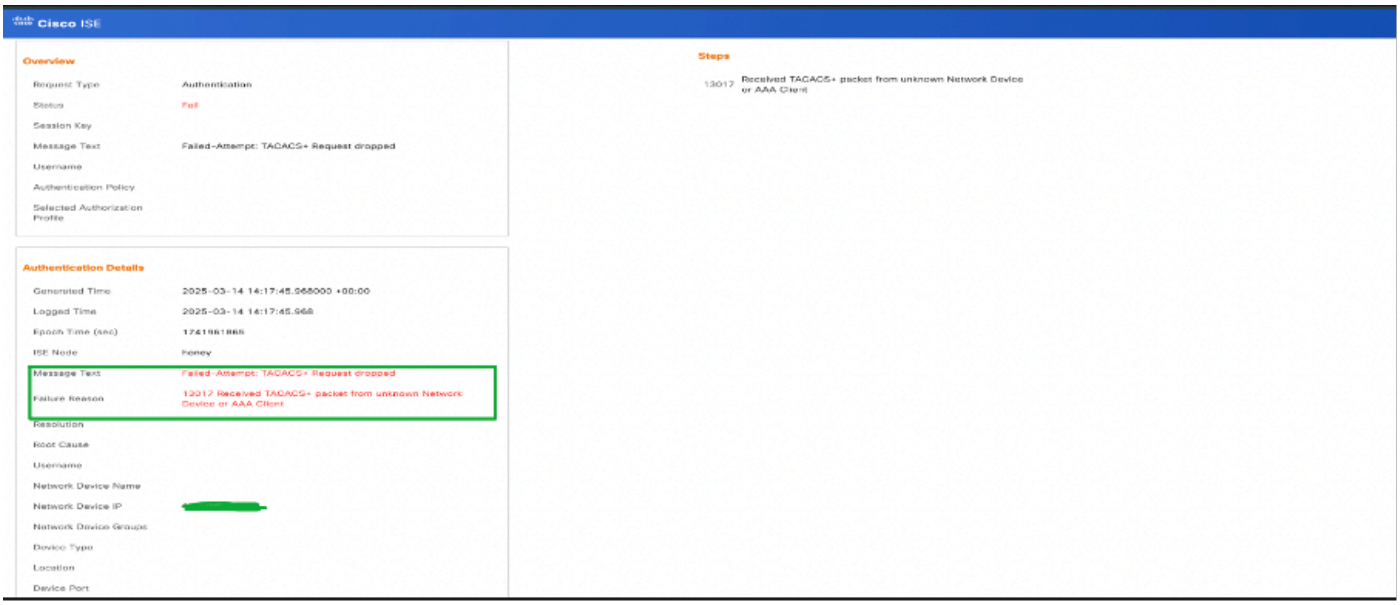
情形 1：TACACS+身份验证失败，显示“错误：13017收到来自未知网络设备或AAA客户端”的TACACS+数据包。

当网络设备未添加为ISE中的网络资源时，会出现此情况。如本屏幕截图所示，交换机不会添加到ISE的网络资源中。



故障排除场景 — 网络设备未添加到ISE。

现在，当您从交换机/网络设备测试身份验证时，数据包按预期到达ISE。但是，身份验证失败，错误为“Error :13017收到来自未知网络设备或AAA客户端”的TACACS+数据包，如下屏幕截图所示：



TACACS实时日志 — 网络设备未添加到ISE时失败。

从网络设备（交换机）进行验证

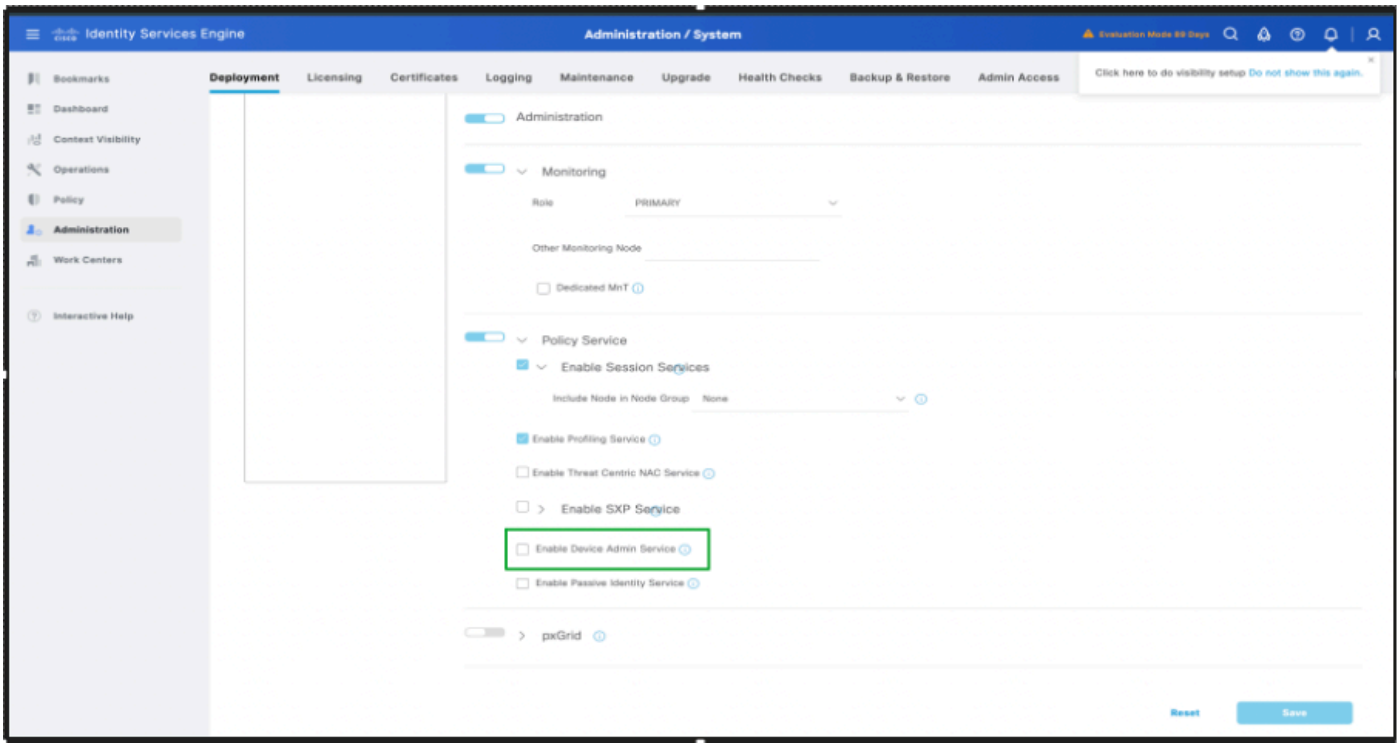
Switch#test aaa group isegroup switch XXXXXX new
用户被拒绝

解决方案：验证交换机/路由器/网络设备是否添加为ISE中的网络设备。如果未添加设备，请将网络设备添加到ISE的网络设备列表。

方案 2： ISE会在没有任何信息的情况下以静默方式丢弃TACACS+数据包。

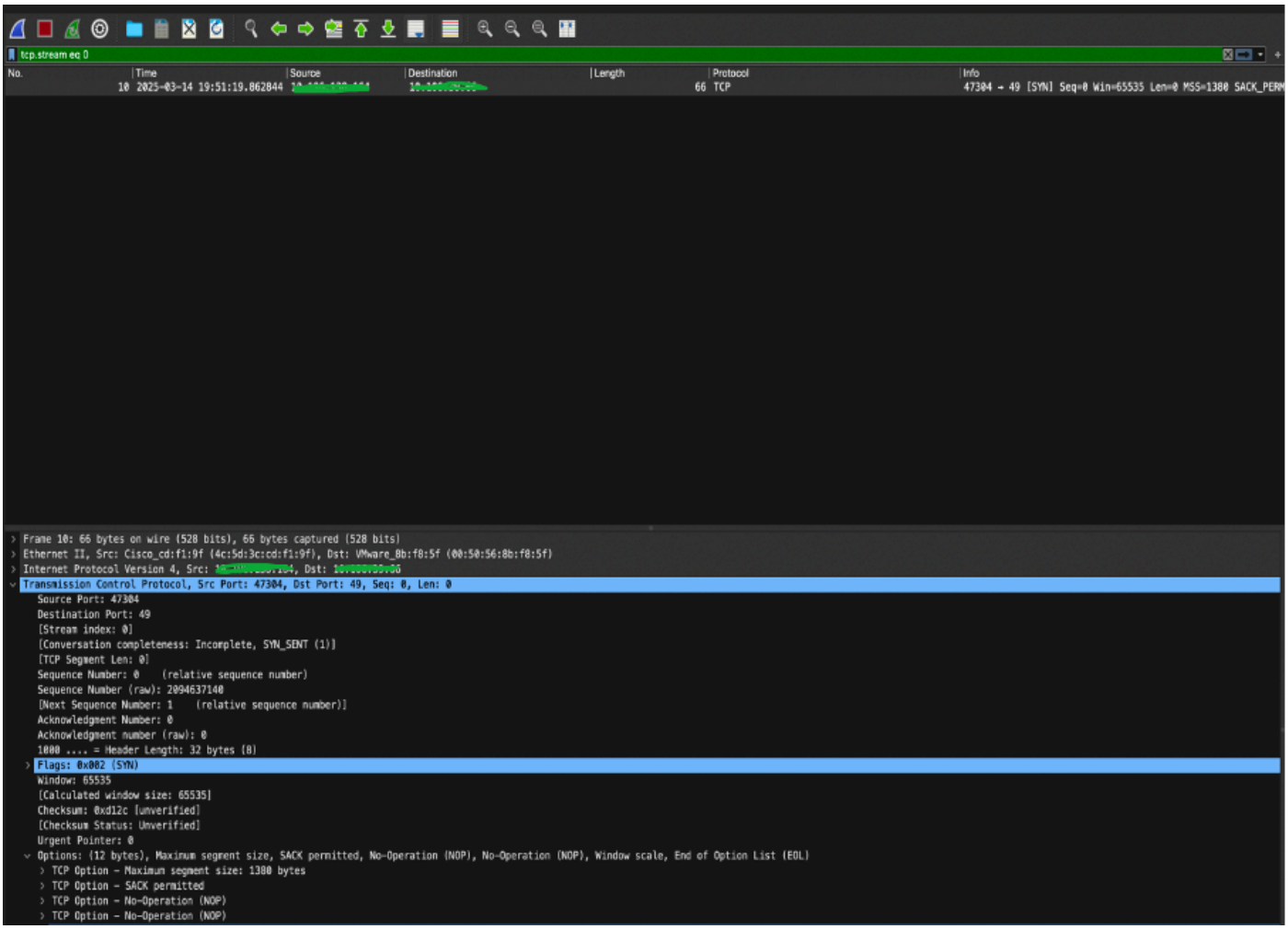
在ISE中禁用设备管理服务时会出现此情况。在这种情况下，ISE会丢弃数据包，并且不会看到实时日志，即使身份验证是从添加到ISE网络资源的网络设备发起的。

如此屏幕截图所示，在ISE中禁用设备管理。



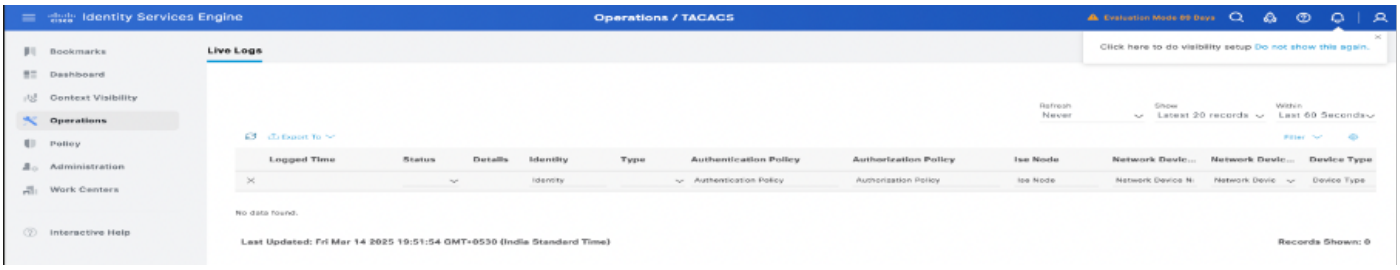
场景，ISE中未启用设备管理。

当用户从网络设备启动身份验证时，ISE会在实时日志中无任何信息的情况下以静默方式丢弃数据包，并且ISE不会响应网络设备发送的Syn数据包，以完成TACACS身份验证过程。请参阅以下屏幕截图：



ISE在TACACS期间以静默方式丢弃数据包

ISE在身份验证期间不显示实时日志。



无TACACS实时日志 — 从ISE验证

从网络设备（交换机）进行验证

Switch#
Switch#test aaa group isegroup switch XXXX new
用户被拒绝
Switch#
*Mar 14 13:54:28.144:T+:版本192(0xC0)，类型1，序列1，加密1,SC 0
*Mar 14 13:54:28.144:T+:session_id 10158877(0x9B031D),dlen 14(0xE)
*Mar 14 13:54:28.144:T+:类型：AUTHEN/START，priv_lvl:15操作：LOGIN ascii
*Mar 14 13:54:28.144:T+:svc:LOGIN user_len:6 port_len:0(0x0)raddr_len:0(0x0)data_len:0
*Mar 14 13:54:28.144:T+:用户名： 交换机
*Mar 14 13:54:28.144:T+:端口：
*Mar 14 13:54:28.144:T+:rem_addr:
*Mar 14 13:54:28.144:T+: 数据：
*Mar 14 13:54:28.144:T+:结束数据包

解决方案：在ISE中启用设备管理。

参考

- 排除TACACS身份验证问题
- 思科身份服务引擎管理员指南，版本3.3
- 用于TACACS服务器的VRF

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）。