使用ISE千兆乙太網1介面配置TACACS+

目錄

簡介

本檔案介紹使用Gigabit乙太網路1介面的ISE TACACS+組態，其中路由器和交換器擔任網路裝置。

背景資訊

思科ISE支援最多6個乙太網介面。它只能有三個繫結：bond 0、bond 1和bond 2。您不能更改屬於繫結的介面或更改介面在繫結中的角色。

必要條件

需求

思科建議您瞭解以下主題：

- 基本網路知識
- 思科身份識別服務引擎。

採用元件

本文件中的資訊是以下列硬體與軟體版本為依據：

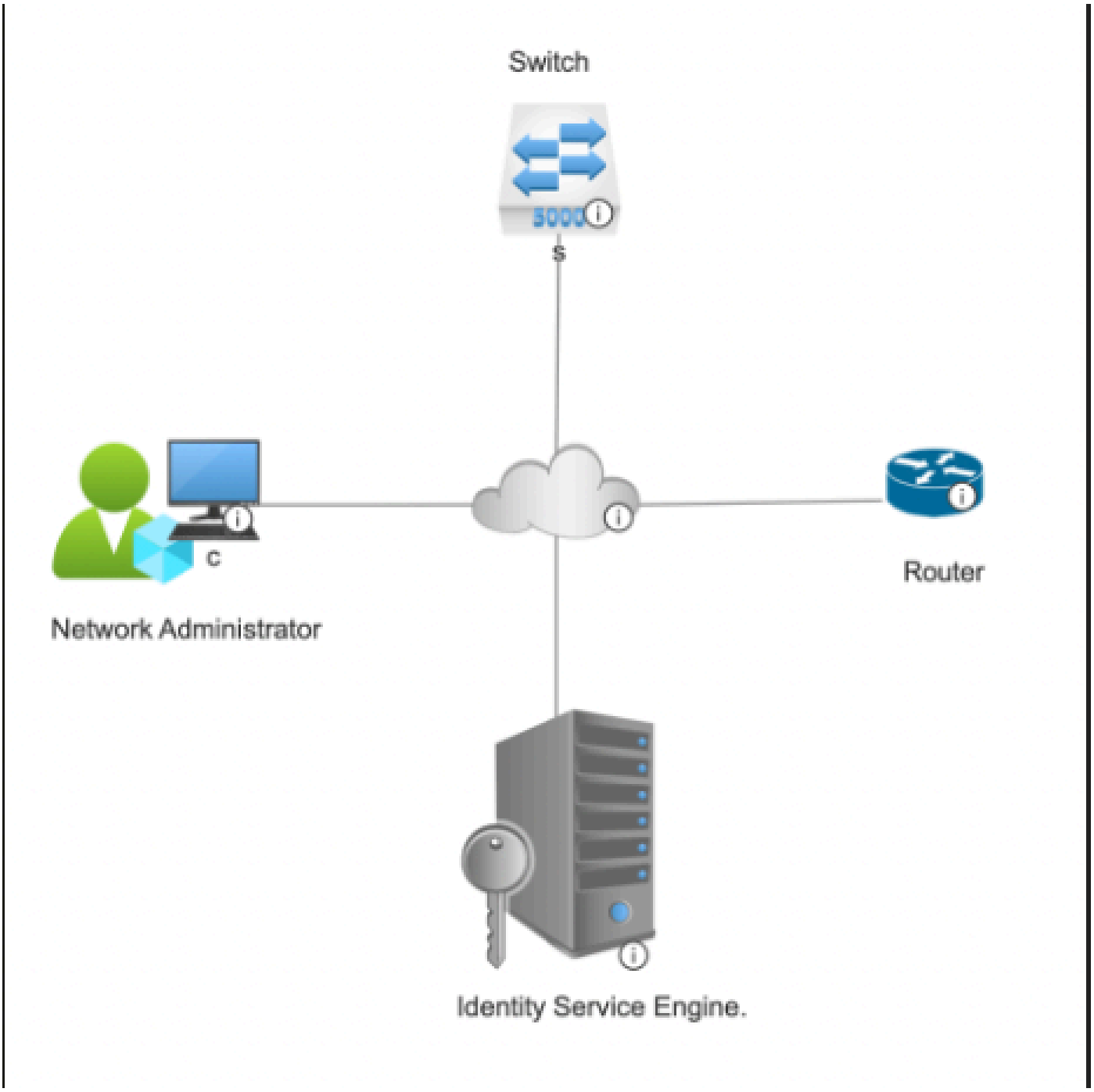
- 思科身分識別服務引擎v3.3
- Cisco IOS®軟體版本17.x
- Cisco C9200交換器。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

組態的目的是：為TACACS+配置ISE的Gigabit乙太網1，並使用ISE作為身份驗證伺服器的TACACS+驗證交換機和路由器。

網路圖表

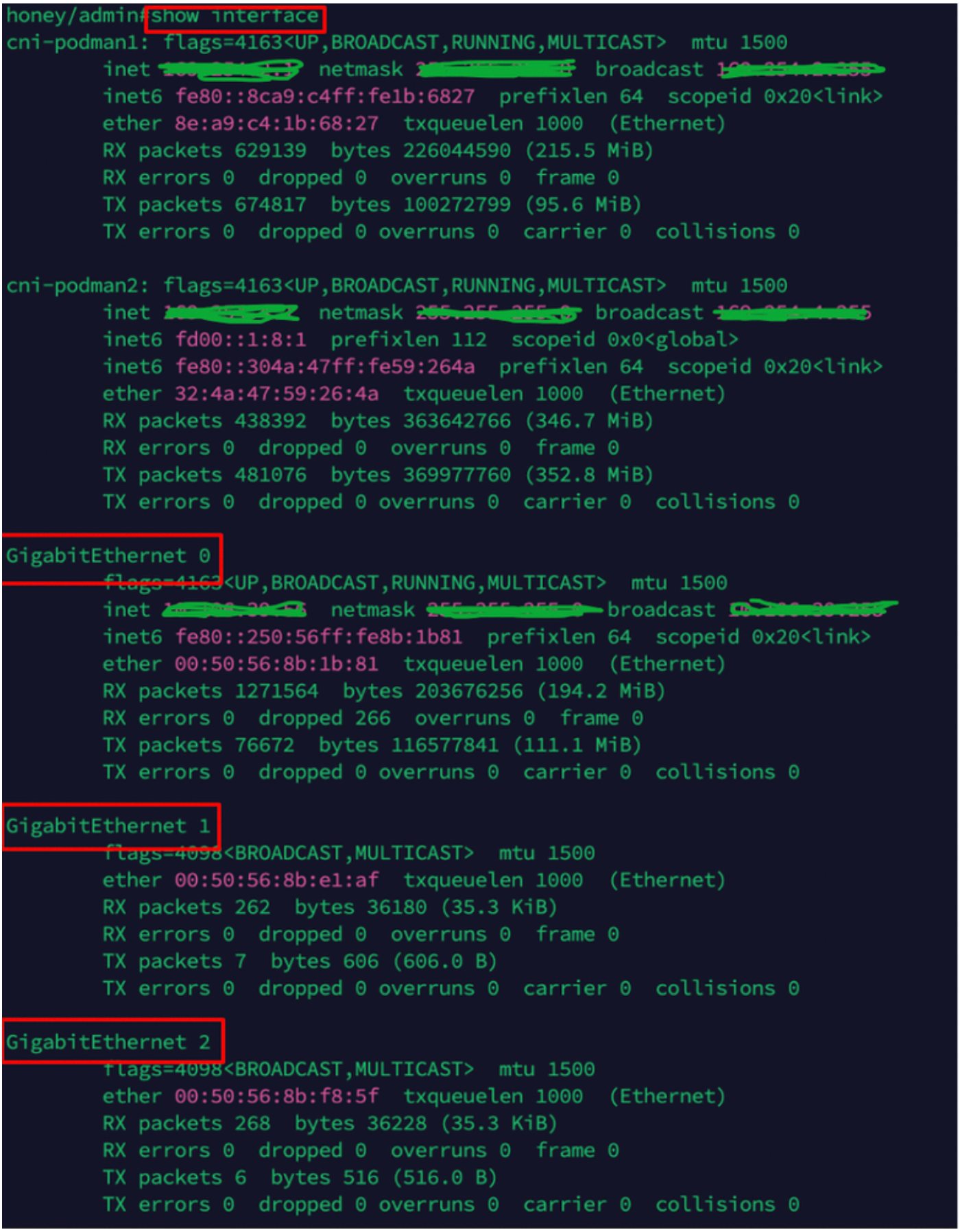


網路拓撲

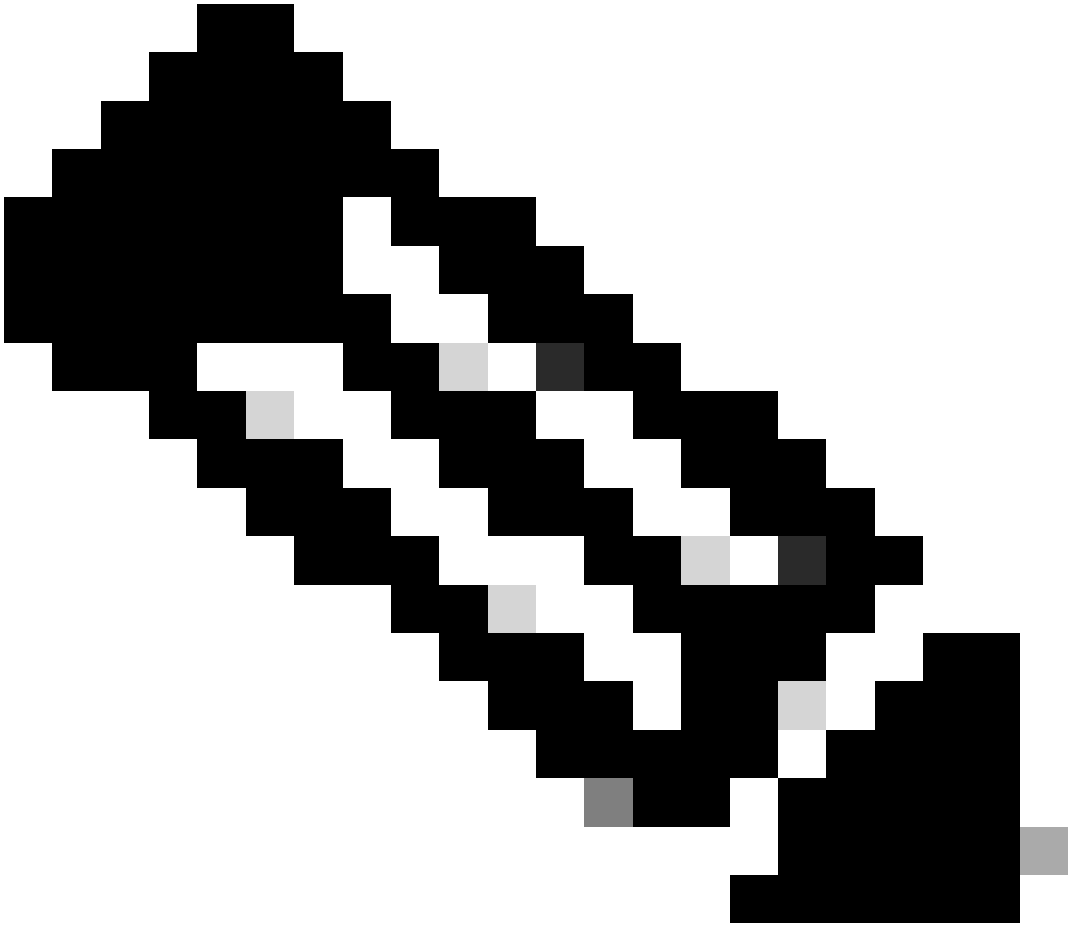
為TACACS+設定身分識別服務引擎

配置ISE中千兆乙太網1介面的IP地址

1. 登入啟用裝置管理的ISE PSN節點的CLI，並使用show interface命令驗證可用介面：


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

驗證ISE中的介面



附註：在此配置中，ISE中僅配置三個介面，重點是Gigabit Ethernet 1介面。可使用相同的過程為所有介面配置IP地址。預設情況下，ISE最多支援六個千兆乙太網介面。

2.從同一PSN節點的CLI中，使用以下命令為Gigabit Ethernet 1介面分配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地址可能導致ise服務重新啟動

是否繼續更改IP地址？

繼續？[是，否]是

3.執行步驟2會使ISE節點服務重新啟動。要驗證ISE服務的狀態，請運行show application status ise命令，並確保服務的狀態正在按照以下螢幕截圖運行：

```
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服務狀態驗證

4.使用show interface命令檢驗Gig1介面的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
```

從CLI驗證ISE Gig2介面IP地址

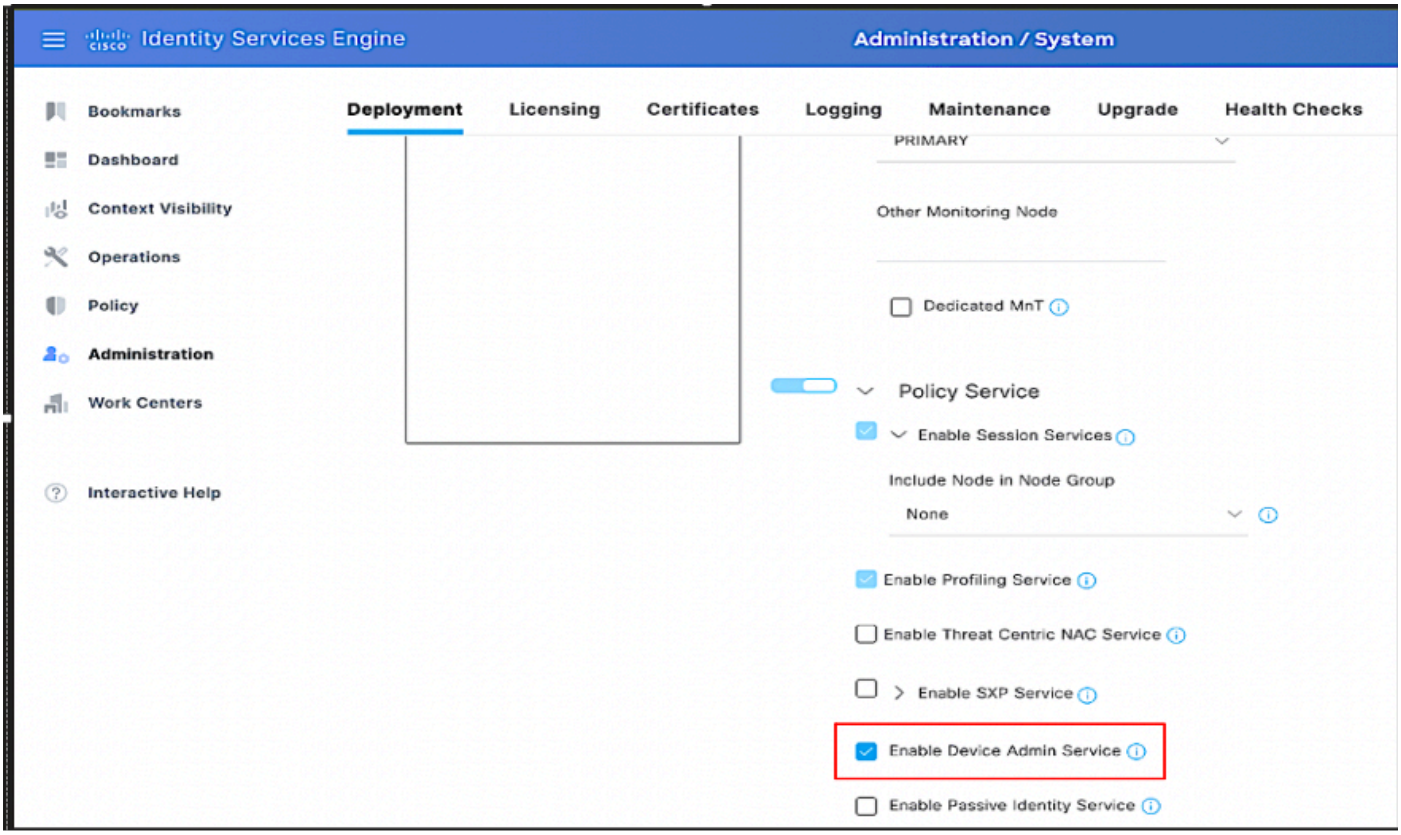
5.使用show ports檢驗ISE節點中埠49的允許量 | inc 49命令：

```
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,
```

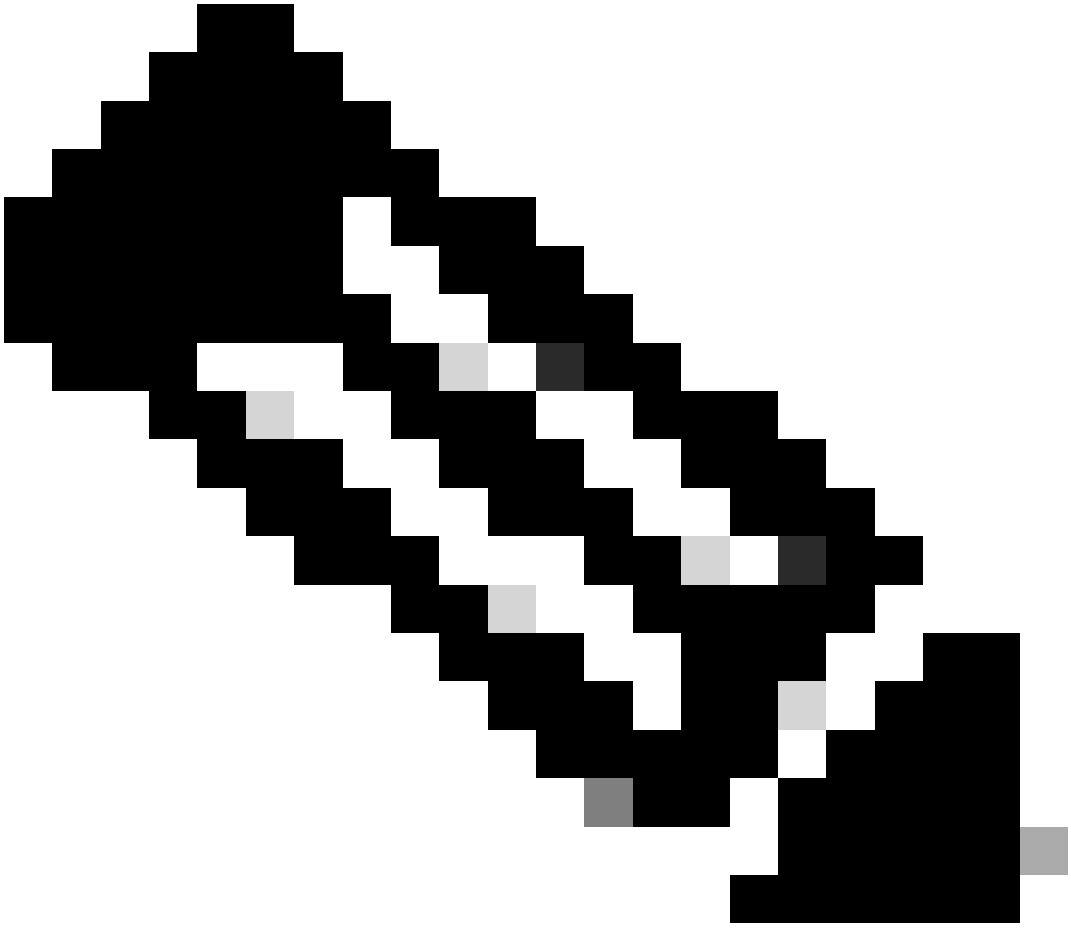
驗證ISE中的埠49允許

在ISE中啟用裝置管理

導航到ISE >管理>部署>選擇PSN節點的GUI，然後選中啟用裝置管理服務:



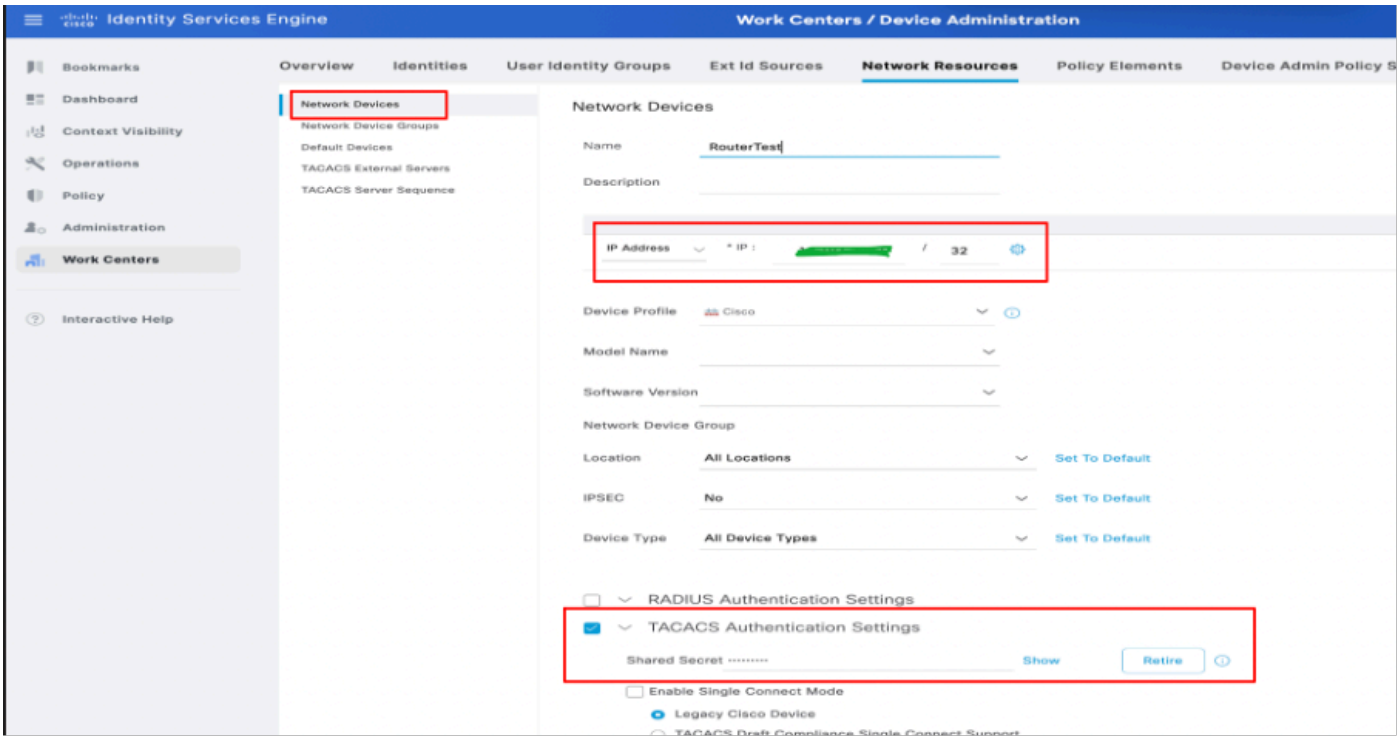
在ISE中啟用裝置管理服務



附註：要啟用Device Admin服務，需要裝置管理許可證。

在ISE中新增網路裝置

1.定位至工作中心>裝置管理>網路資源>網路裝置。按一下「新增」。提供名稱、IP地址。選中TACACS+身份驗證設定覈取方塊並提供共用金鑰。



在ISE中配置網路裝置

2.按照上述步驟新增TACACS身份驗證所需的所有網路裝置。

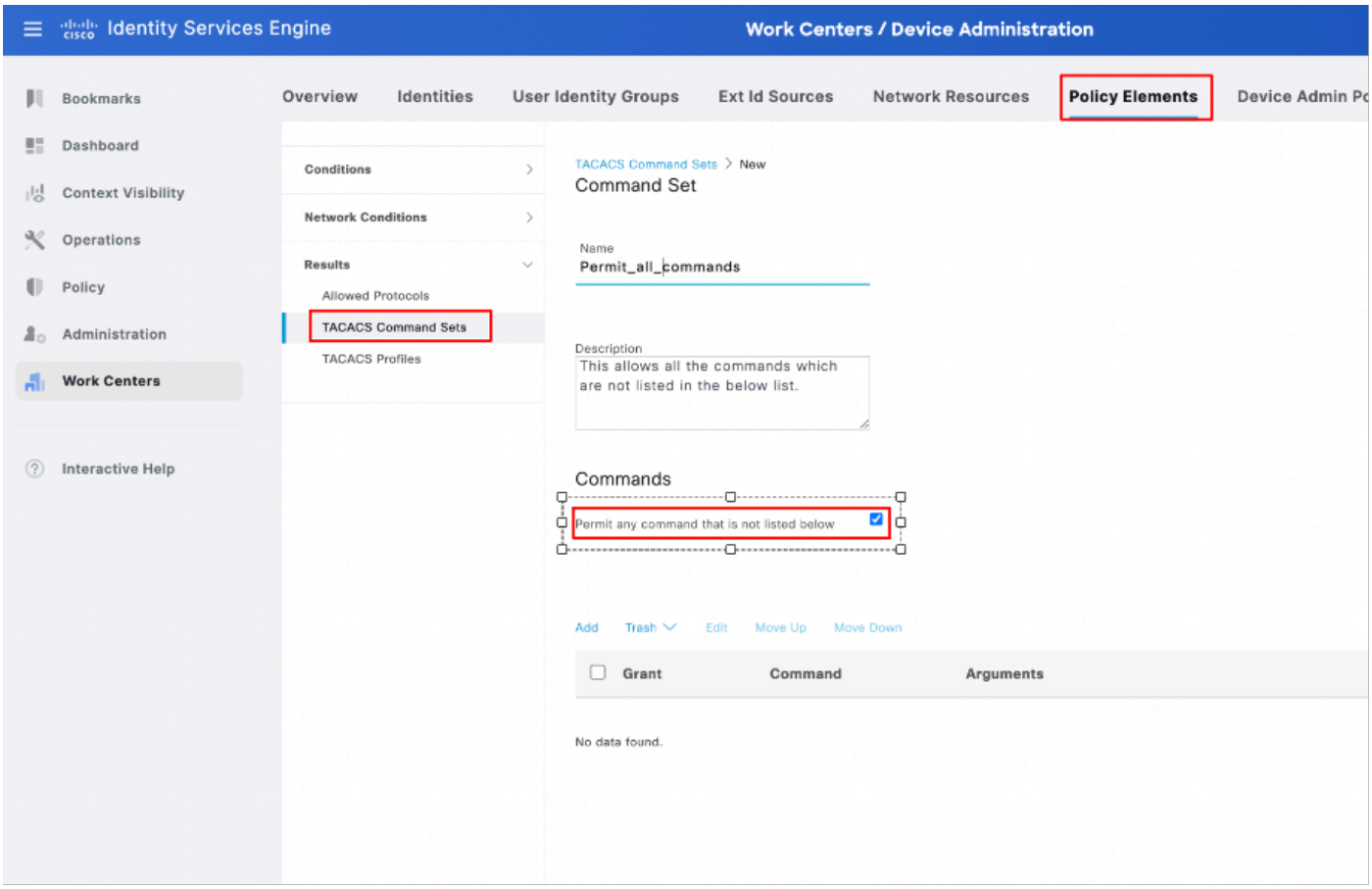
配置TACACS+命令集

為此演示配置了兩個命令集：

Permit_all_commands分配給使用者admin並允許裝置上的所有命令。

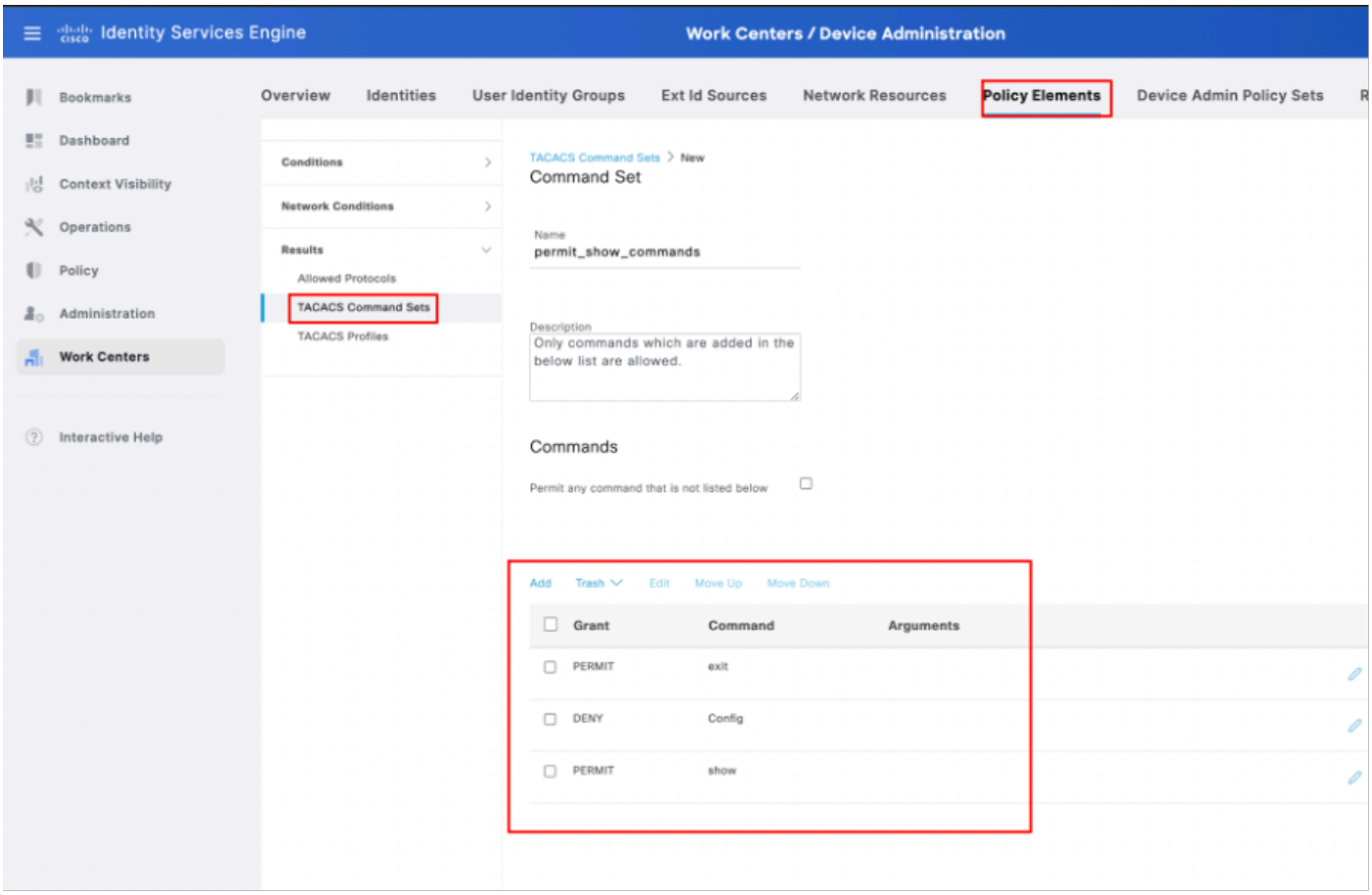
permit_show_commands，分配給使用者並僅允許show命令

1. 導航到工作中心>裝置管理>策略結果> TACACS命令集。按一下Add。提供名稱PermitAllCommands，然後選擇Permit any命令覈取方塊（未列出）。按一下Submit（提交）。



在ISE中配置命令集

2.導航到工作中心(Work Centers)>裝置管理(Device Administration)>策略結果(Policy Results)>TACACS命令集(TACACS Command Sets)。單擊「新增」(Add)。提供名稱PermitShowCommands，按一下「新增」(Add),最後按一下permit show和exit命令。預設情況下，如果引數留空，則包括所有引數。按一下Submit（提交）。

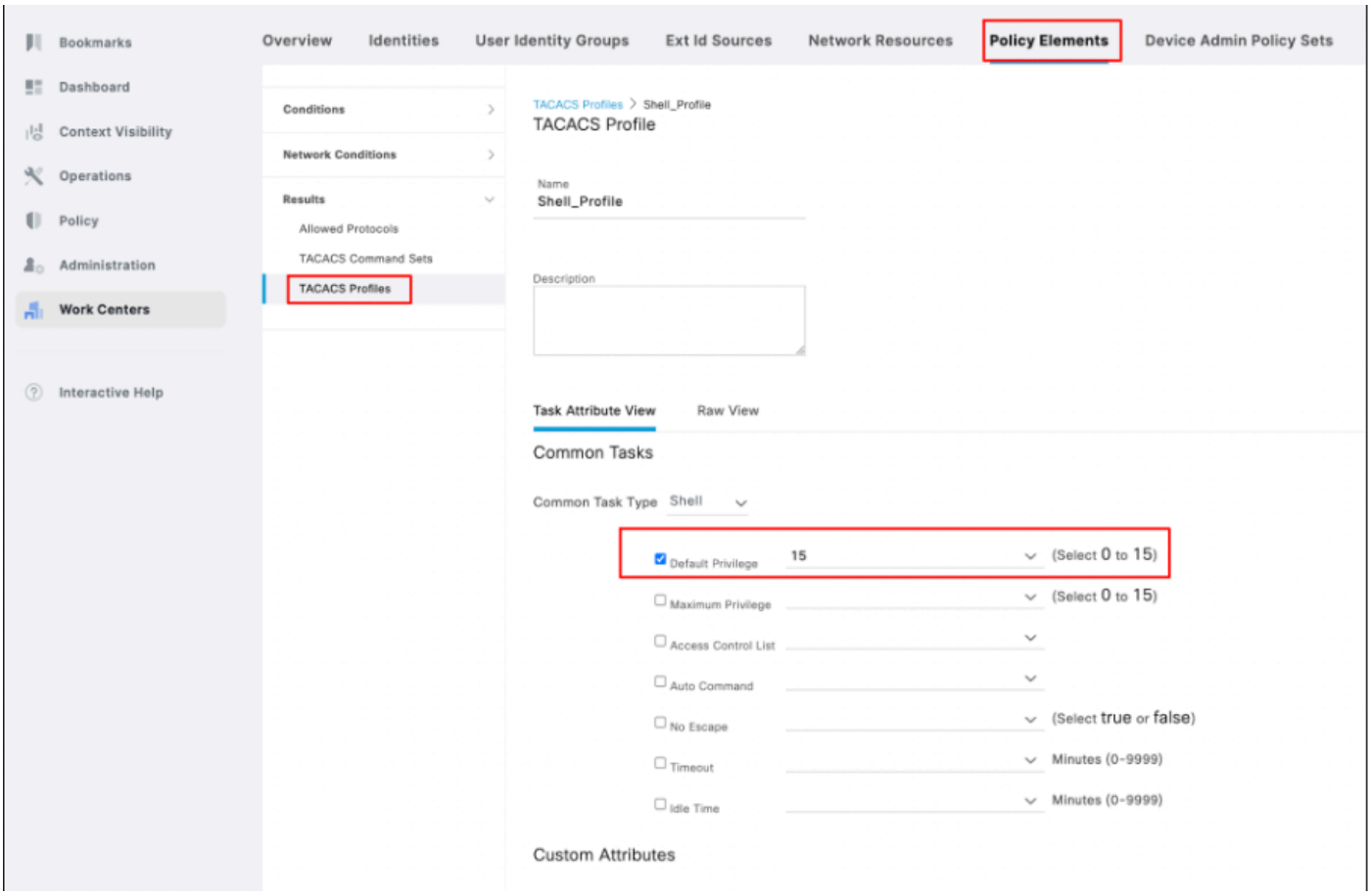


在ISE中配置permit_show_commands

設定TACACS+設定檔

配置單個TACACS+配置檔案，並通過命令集執行命令授權。

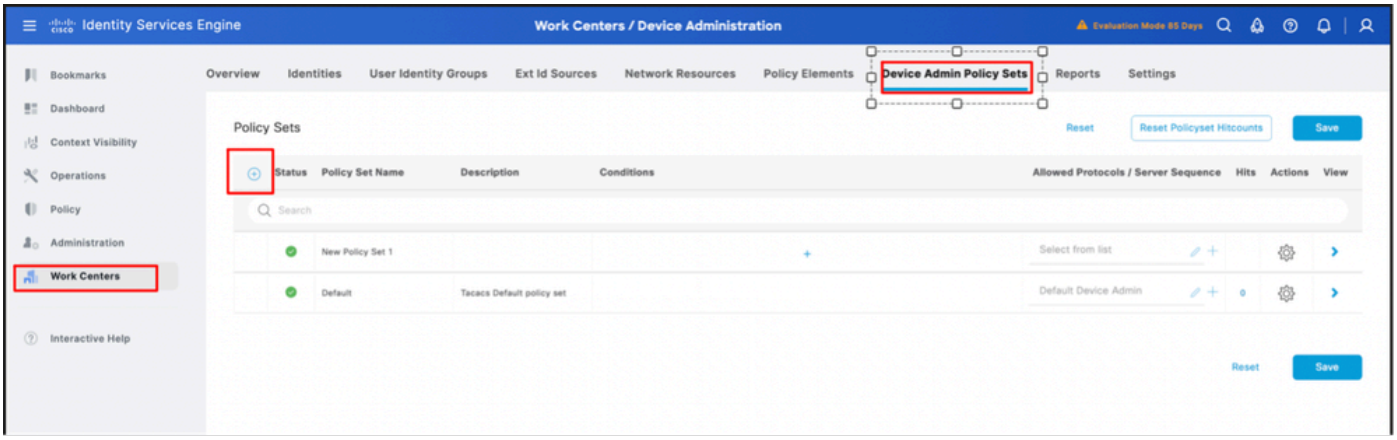
要配置TACACS+配置檔案，請導航至工作中心 > 裝置管理 > 策略結果 > TACACS配置檔案。按一下Add，為Shell配置檔案提供名稱，選中Default Privilege覈取方塊，然後輸入值15。最後，按一下Submit。



在ISE中配置TACACS配置檔案

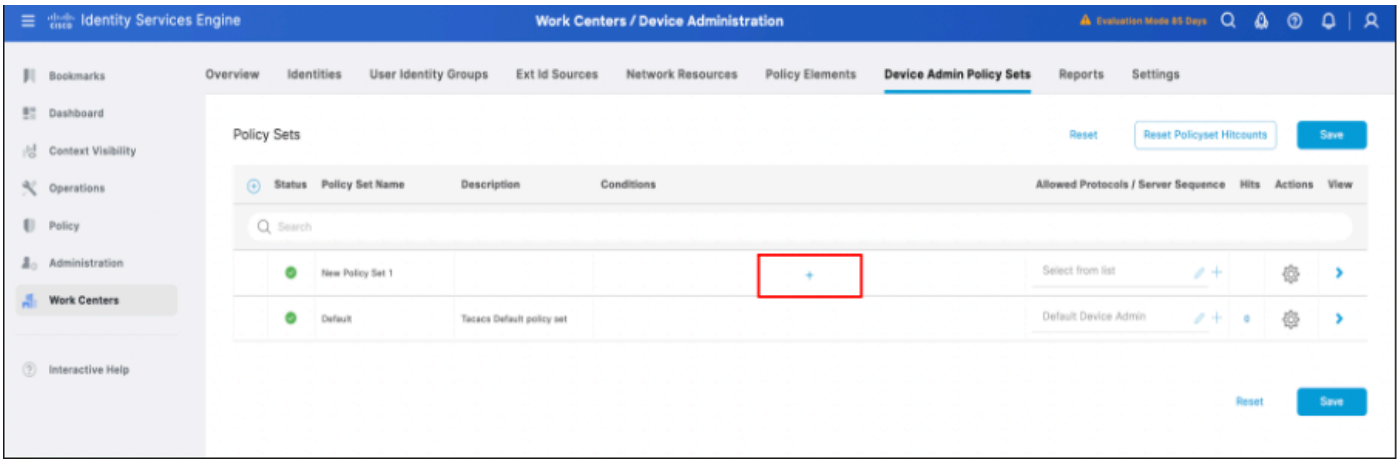
設定TACACS+驗證和授權設定檔

1.登入到ISE PAN GUI -> Administration -> Work Centers -> Device administration -> Device admin策略集。按一下+(plus)圖示建立新策略。在這種情況下，策略集命名為New Policy set 1。



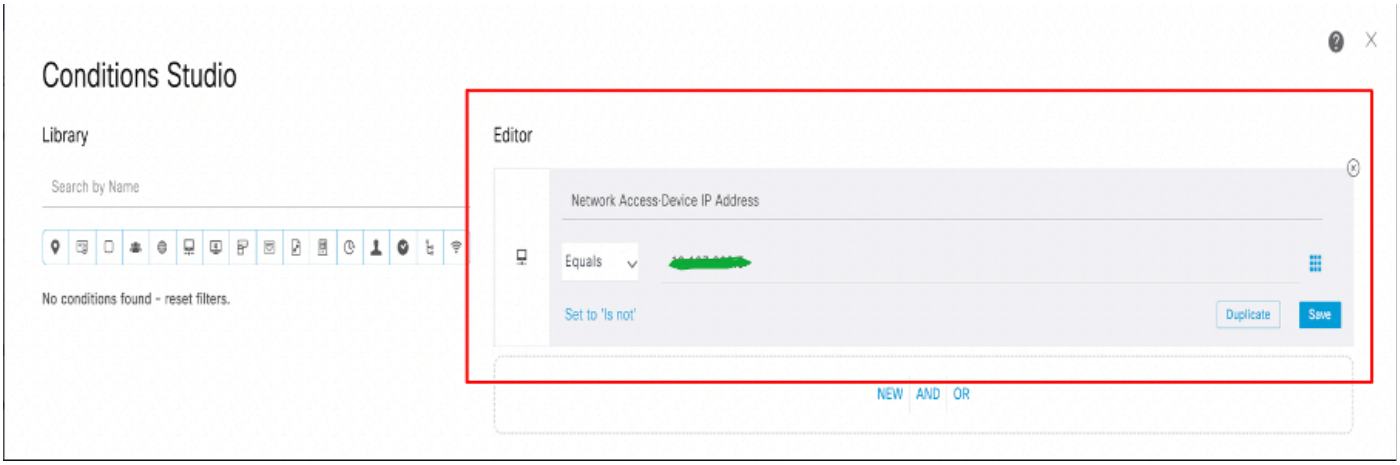
在ISE中配置策略集

2.在儲存策略集之前，需要配置條件，如本螢幕截圖所示。按一下+(plus)圖示配置策略集的條件。

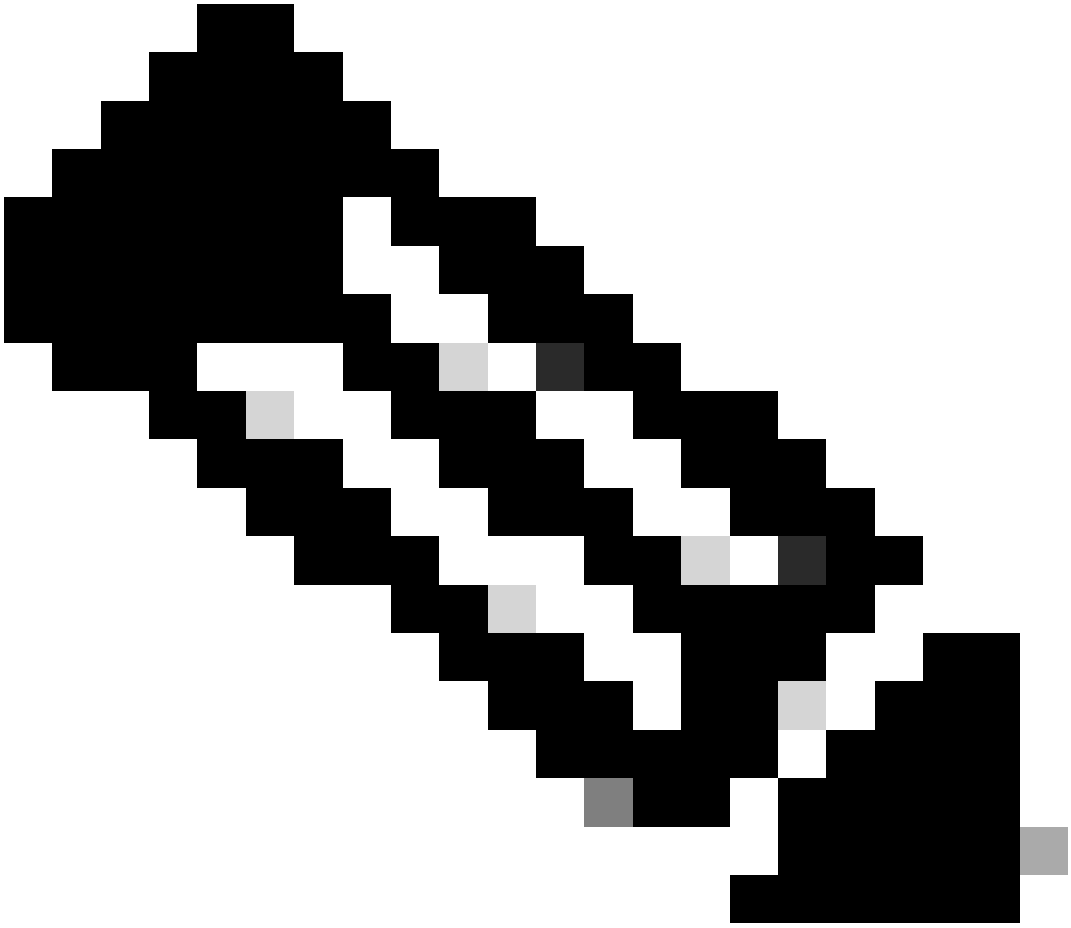


在ISE中配置策略集條件

3.按一下步驟2中提到的+（加）圖示後，將開啟「條件工作室」對話方塊。在此，配置所需的條件。使用新條件或現有條件儲存條件，然後滾動。按一下「use」。

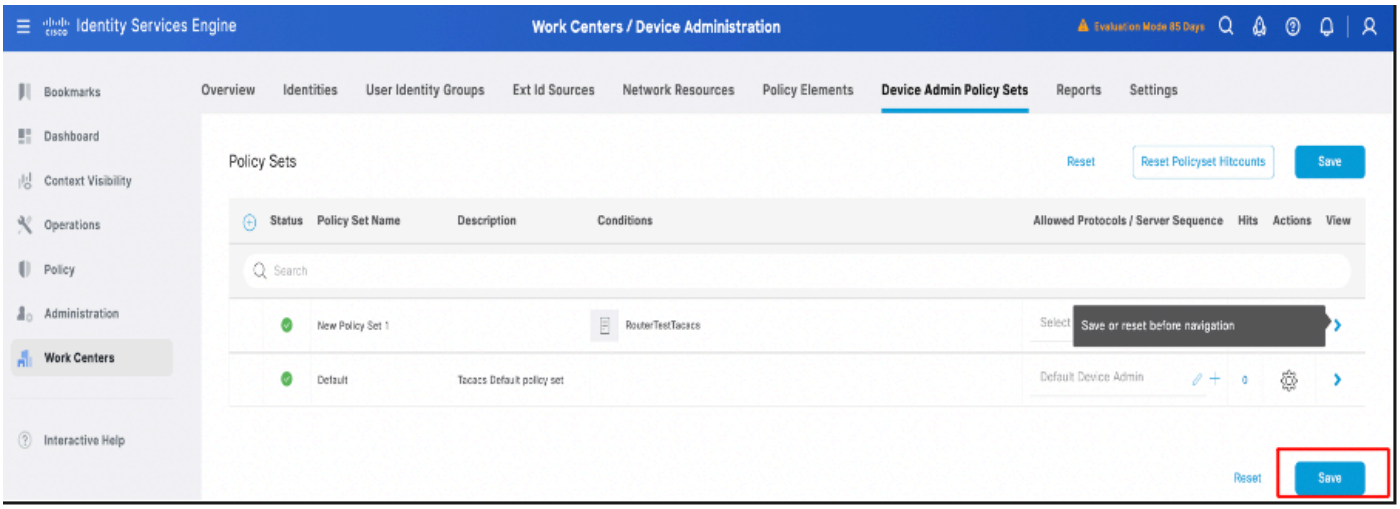


在ISE中配置策略集條件



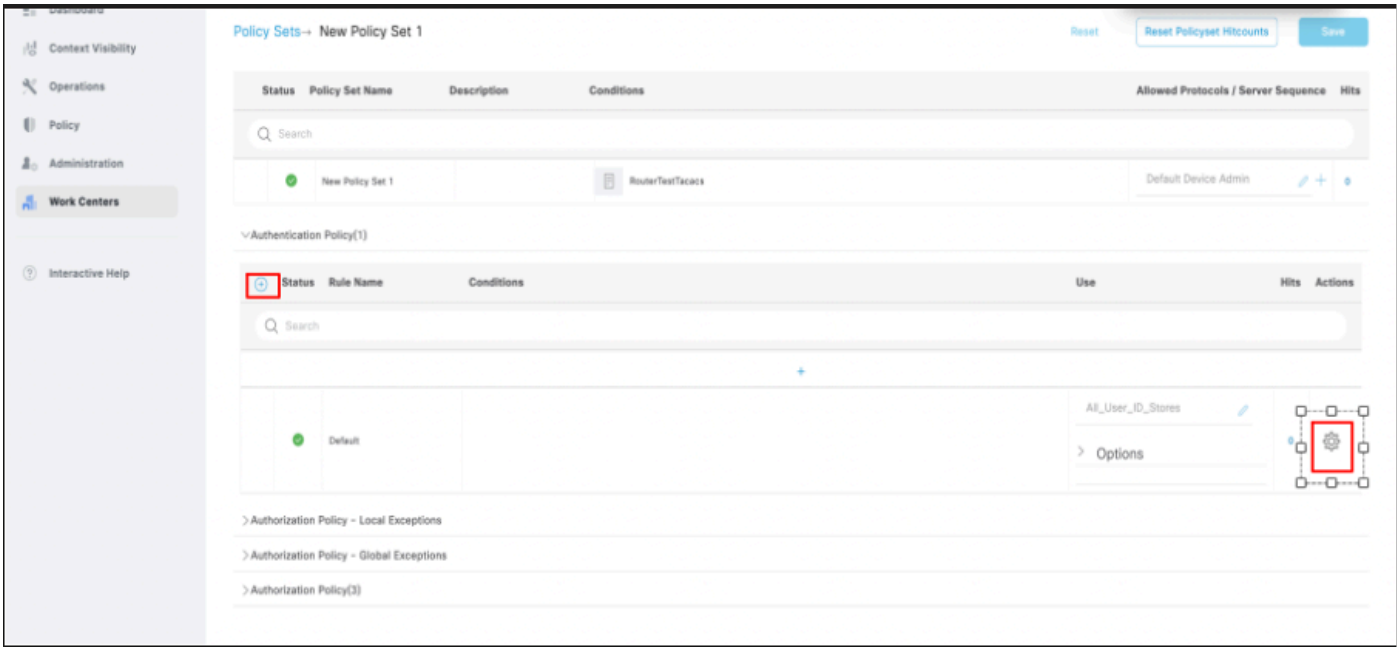
附註：對於本文檔來說，這些條件與網路裝置IP相匹配。但是，條件可能因部署要求而有所不同。

4.配置並儲存條件後，將允許的協定配置為Default device admin。儲存通過按一下選項Save建立的策略集。

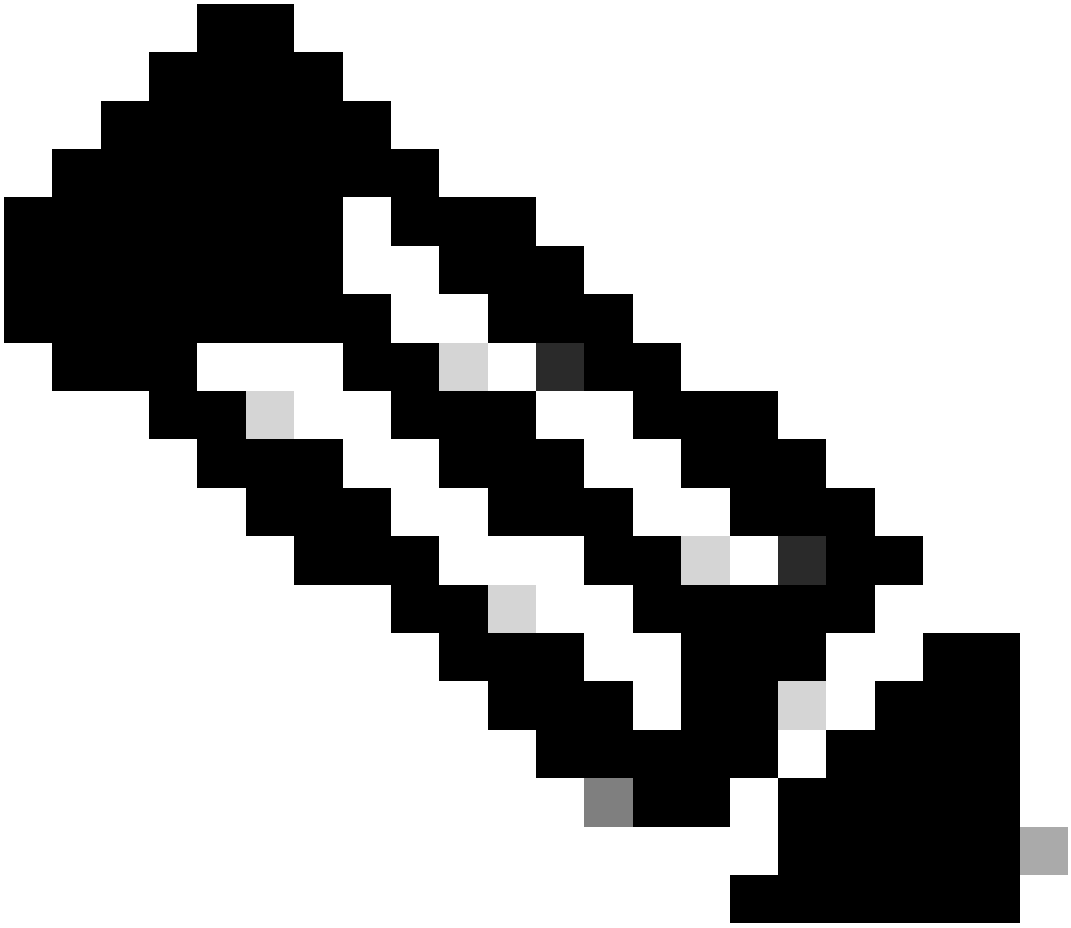


策略集配置確認。

5.展開New Policy set -> Authentication Policy(1)->按一下+(plus)圖示或按一下gear Icon，然後按一下Insert new row about來建立新的身份驗證策略。

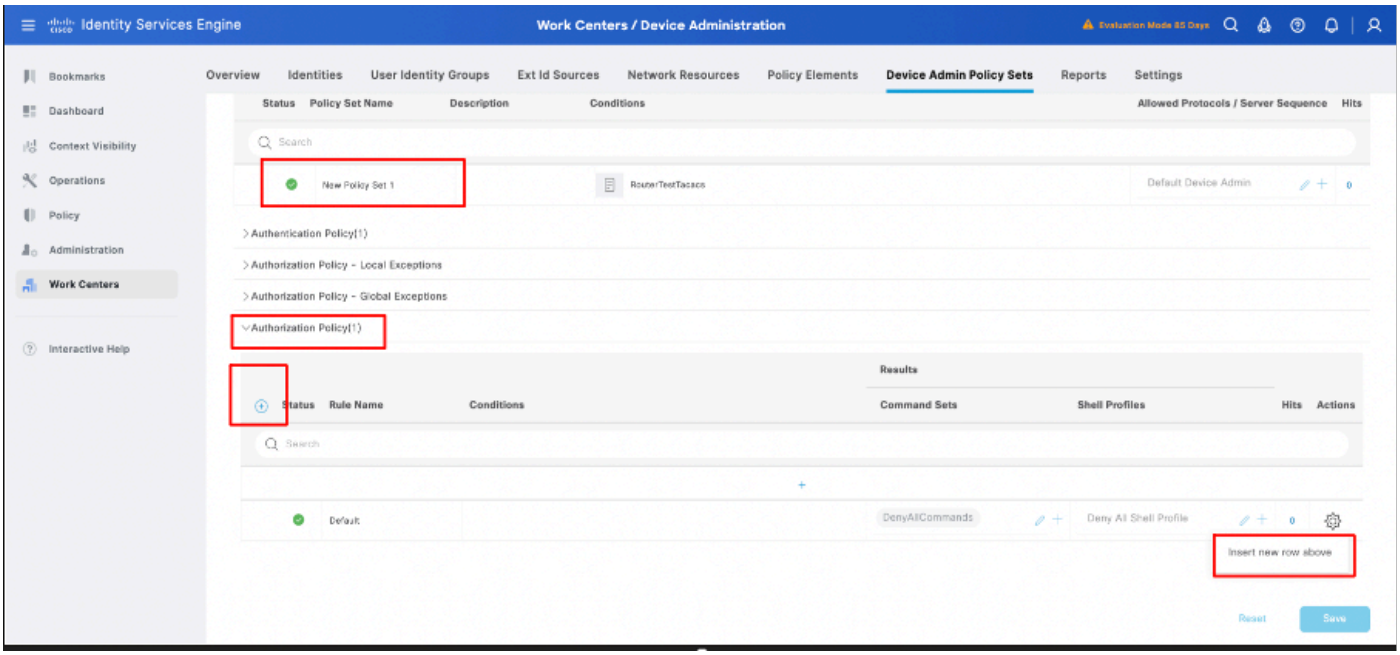


在策略集中配置身份驗證策略。



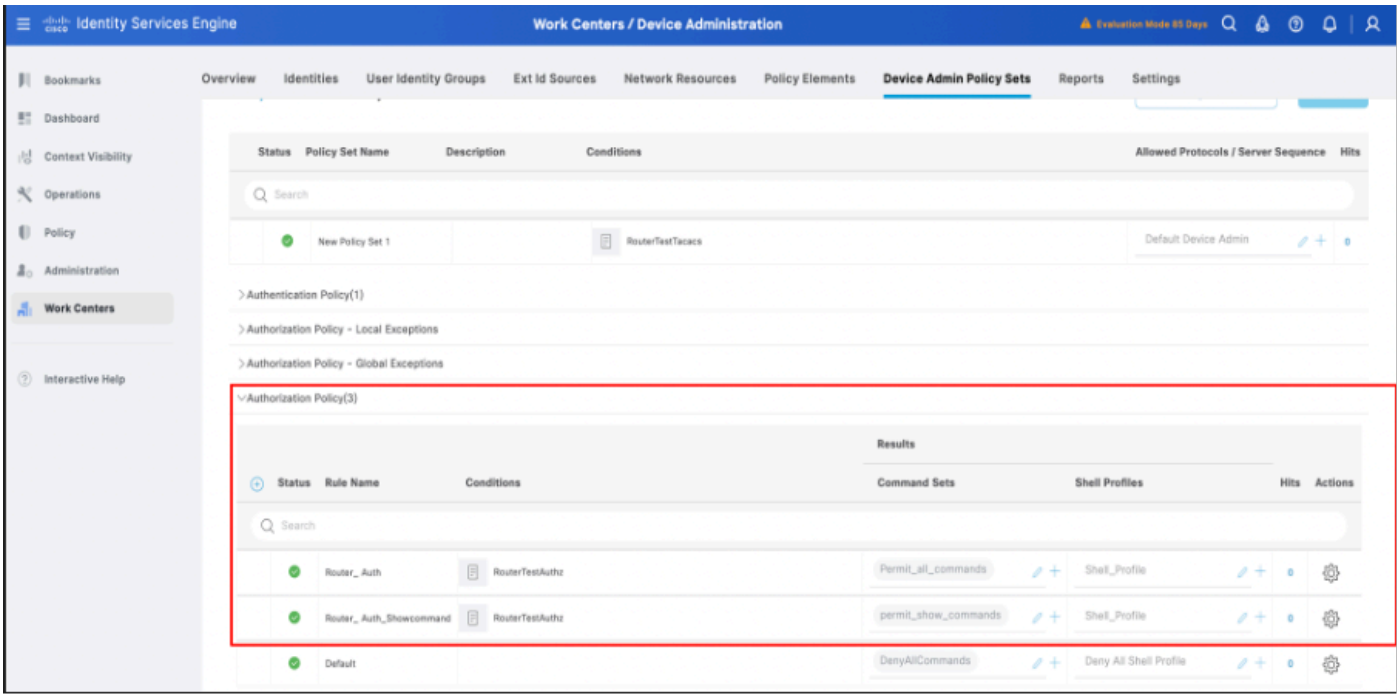
附註：在本演示中，使用帶有All_User_ID_Stores的預設身份驗證策略集。但是，可以根據部署要求自定義身份儲存庫的使用。

6.展開New Policy set -> Authorization Policy(1)。 按一下+（加）圖示或按一下齒輪圖示。然後，在上面插入新行以建立授權策略。

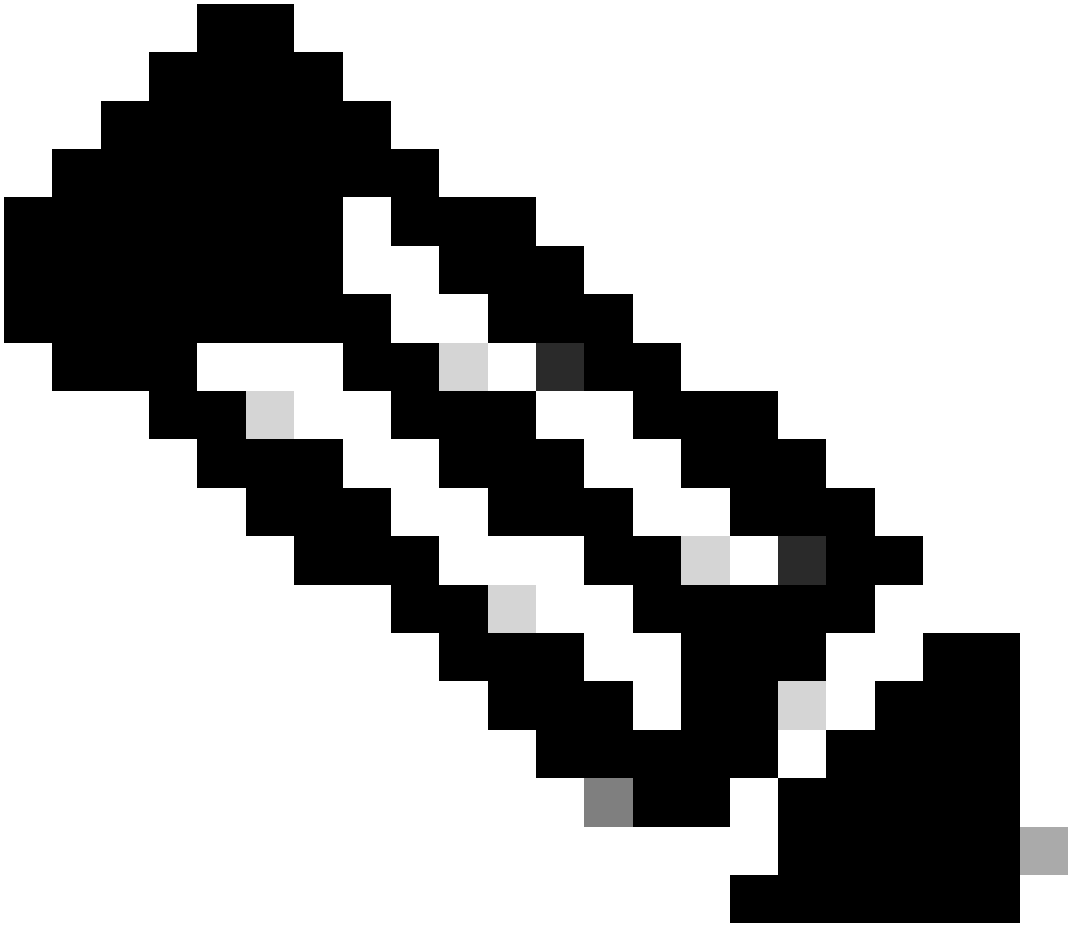


授權策略的配置

7.使用對映到授權策略的條件、命令集和外殼配置檔案配置授權策略。



在ISE中完成授權策略的配置

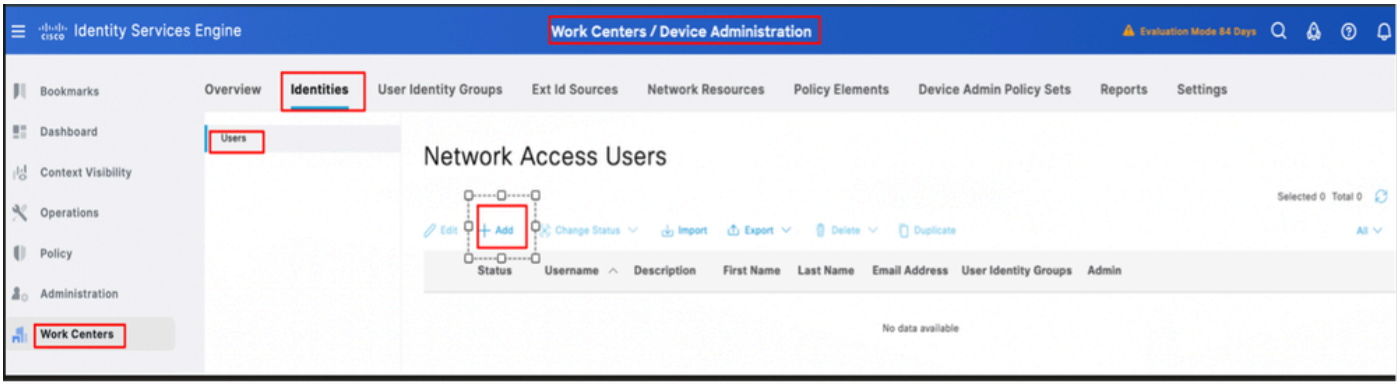


附註：所配置的條件取決於實驗環境，並可根據部署要求進行配置。

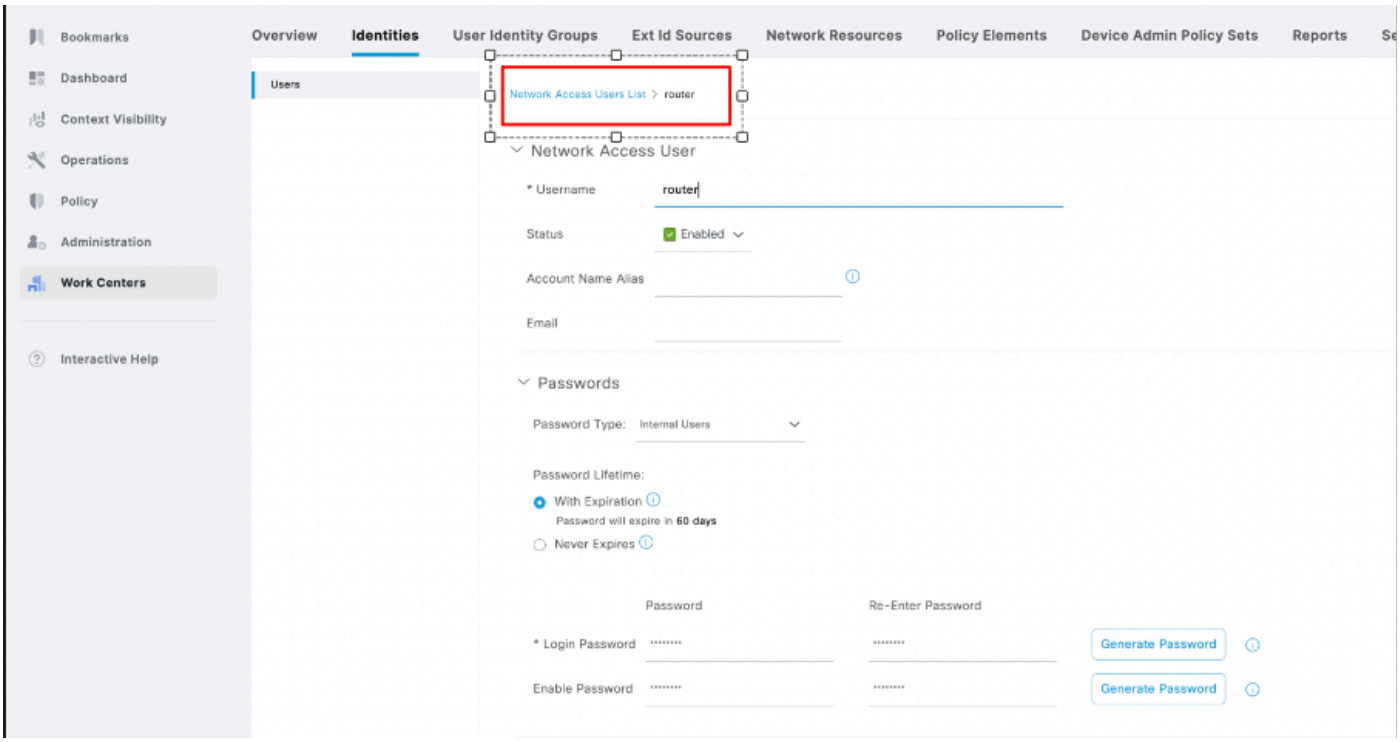
8.按照前6步為交換機或用於TACACS+的任何其它網路裝置配置策略集。

在ISE中為需要的TACACS身份驗證配置網路訪問使用者

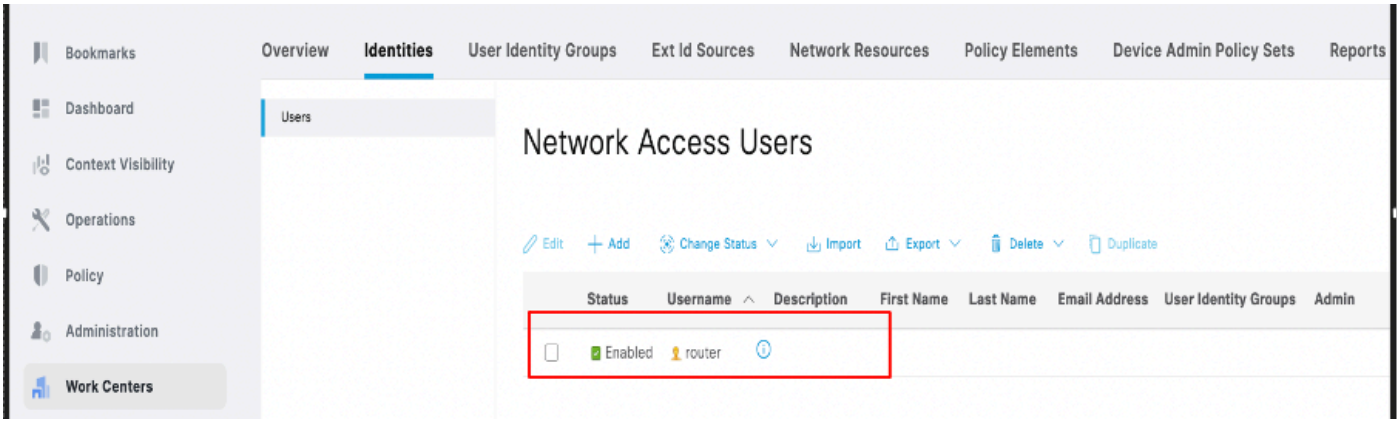
1. 導航至工作中心 — >裝置管理 — >身份 — >使用者。按一下+(plus)圖示以建立新使用者。



2.提供以展開Username和Password詳細資訊，將使用者對映到使用者身份組（可選），然後按一下Submit。



3.在工作中心 — >身份 — >使用者 — >網路訪問使用者中提交使用者名稱配置後，將對該使用者進行可見配置和啟用。



為TACACS+配置路由器

為TACACS+身份驗證和授權配置Cisco IOS路由器

1. 登入到路由器的CLI並運行這些命令以在路由器中配置TACACS。

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

ASR1001-X(config)#aaa session-id common。-在NAD中啟用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伺服器的IP地址> . — ISE介面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 name 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(config)#exit

2.儲存路由器TACACS+配置後，使用show run aaa命令驗證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伺服器ise1

address ipv4 <TACACS伺服器的IP地址>

主要XXXXX

!

!

aaa群組伺服器tacacs+ isegroup

伺服器名稱ise1

ip vrf forwarding Mgmt-intf

ip tacacs source-interface GigabitEthernet1

!

!

!

aaa new-model

aaa session-id common

!

!

為TACACS+設定交換器

設定交換器以進行TACACS+驗證和授權

1. 登入到交換機的CLI並運行這些命令以在交換機中配置TACACS。

C9200L-48P-4X#configure t

輸入配置命令，每行一個。 以CNTL/Z結束。

C9200L-48P-4X(config)#aaa新型號。— 啟用NAD中的aaa所需的命令

C9200L-48P-4X(config)#aaa session-id common。 — 在NAD中啟用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)i伺#tacacs器ise1

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

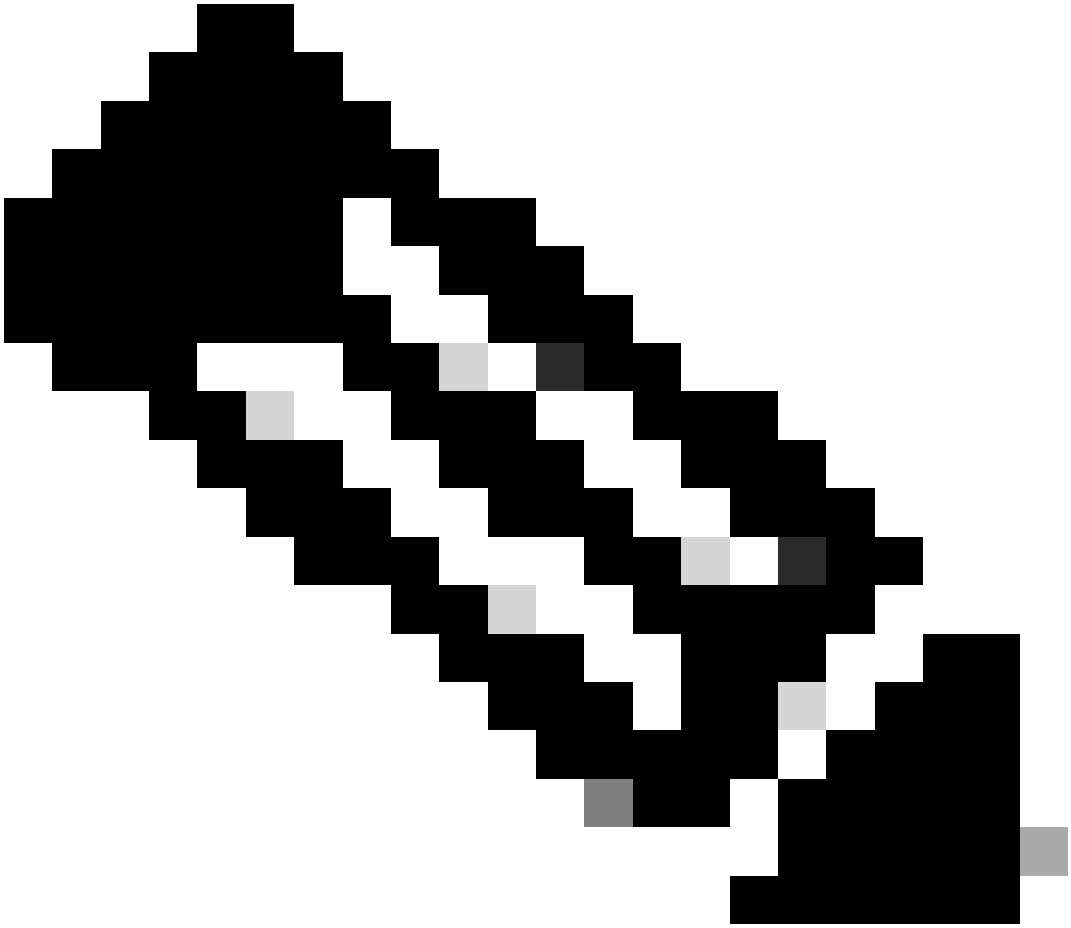
C9200L-48P-4X(config-server-tacacs)#key XXXXX

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

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

C9200L-48P-4X(config)#exit

C9200L-48P-4X#wr記憶體



附註：在NAD TACACS+組態中，tacacs+ 是可以根據部署要求自定義的群組。

2.儲存交換器TACACS+組態後，使用show run aaa 指令驗證TACACS+組態。

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伺服器ise1

 address ipv4 <TACACS伺服器的IP地址>

 主要XXXXX

!

!

aaa群組伺服器tacacs+ isegroup

 伺服器名稱ise1

!

!

!

aaa new-model

aaa session-id common

!

!
```

驗證

從路由器驗證

在路由器的CLI上，使用test aaa group tacacsgroupname username password new 命令針對具有Gigabit Ethernet 1介面的ISE驗證TACACS+。

以下是Router & ISE的輸出示例：

從路由器驗證埠49:

```
ASR1001-X#telnet ISE Gig 1介面IP 49

正在嘗試ISE GIg 1介面IP， 49..未解決
```

ASR1001-X#test aaa group isegroup router XXXX全新

正在傳送密碼

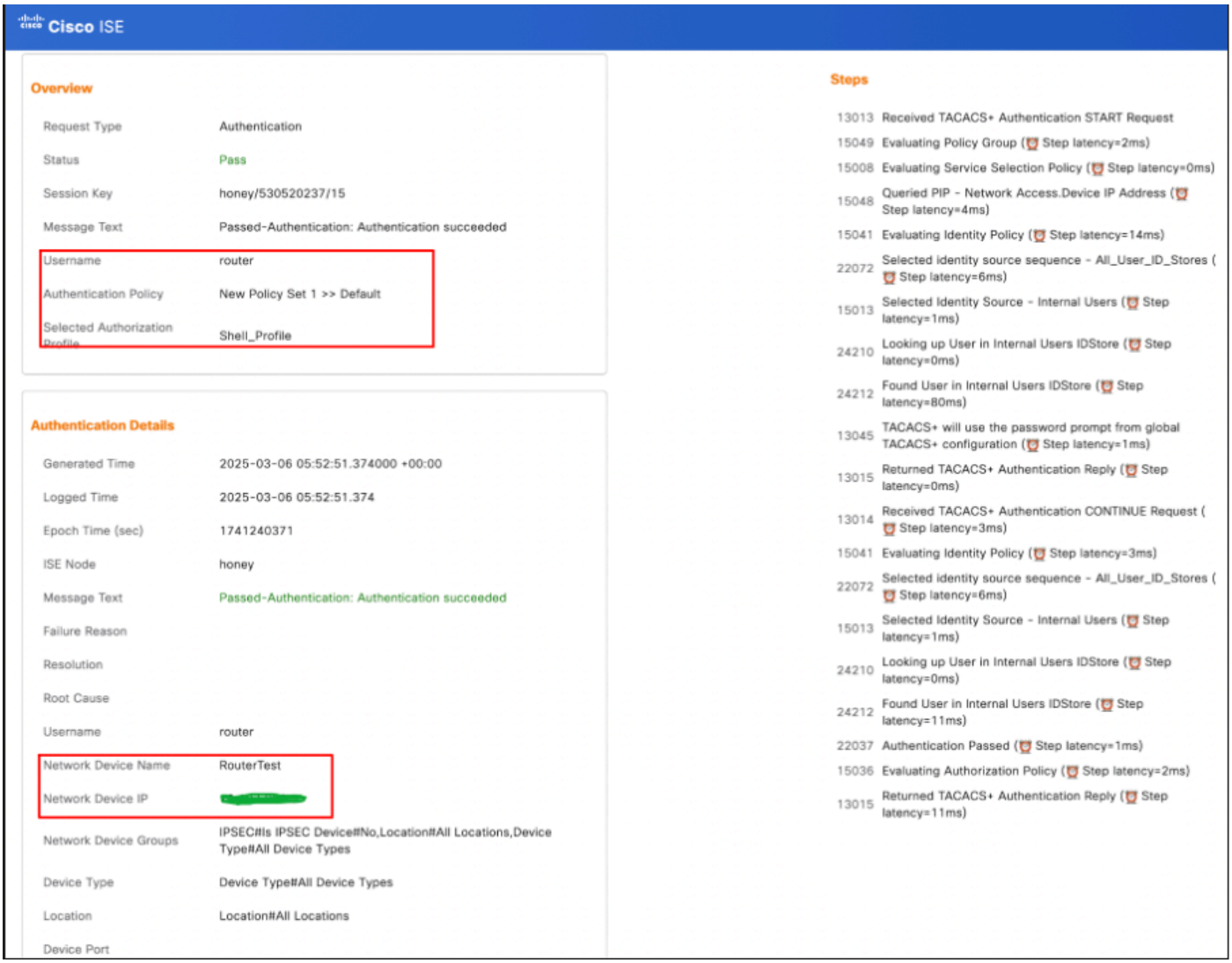
使用者已成功通過身份驗證

使用者屬性

使用者名稱0 "router"

reply-message 0 "Password:"

要從ISE進行驗證，請登入到GUI -> Operations -> TACACS live logs，然後在Network Device Details欄位中使用路由器IP進行過濾。



來自ISE的TACACS即時日誌 — 路由器驗證。

驗證交換機

在交換機的CLI中，使用test aaa group tacacsgroupname username password newn 命令，使用Gigabit Ethernet 1介面驗證TACACS+針對ISE的身份驗證：

以下是交換機和ISE的輸出示例。

從交換機驗證埠49:

C9200L-48P# telnet ISE Gig1介面IP 49

正在嘗試ISE Gig1介面IP，49...未解決

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

正在傳送密碼

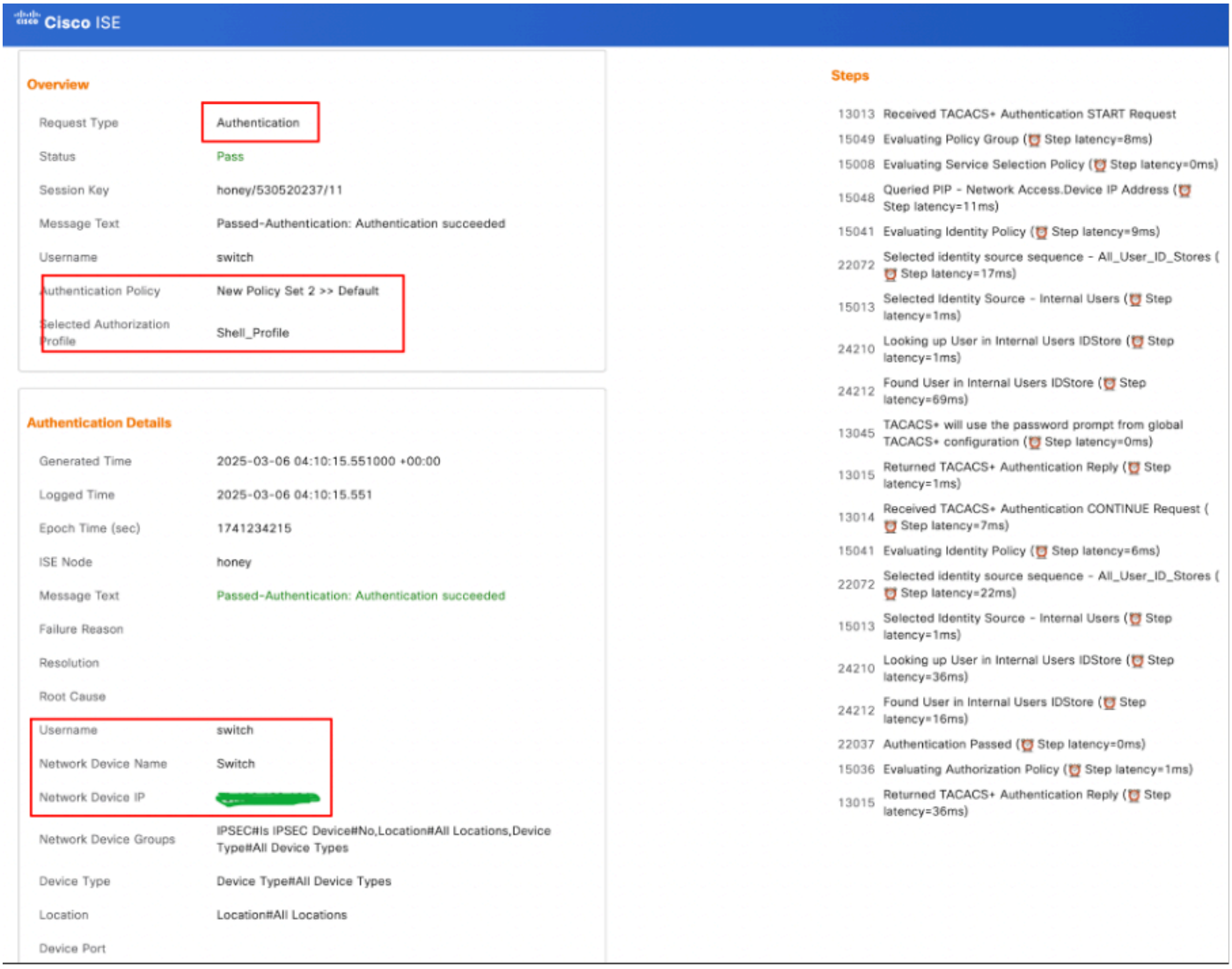
使用者已成功通過身份驗證

使用者屬性

使用者名稱0 "switch"

reply-message 0 "Password:"

要從ISE進行驗證，請登入到GUI -> Operations -> TACACS live logs，然後在Network Device Details欄位中使用交換機IP進行過濾。



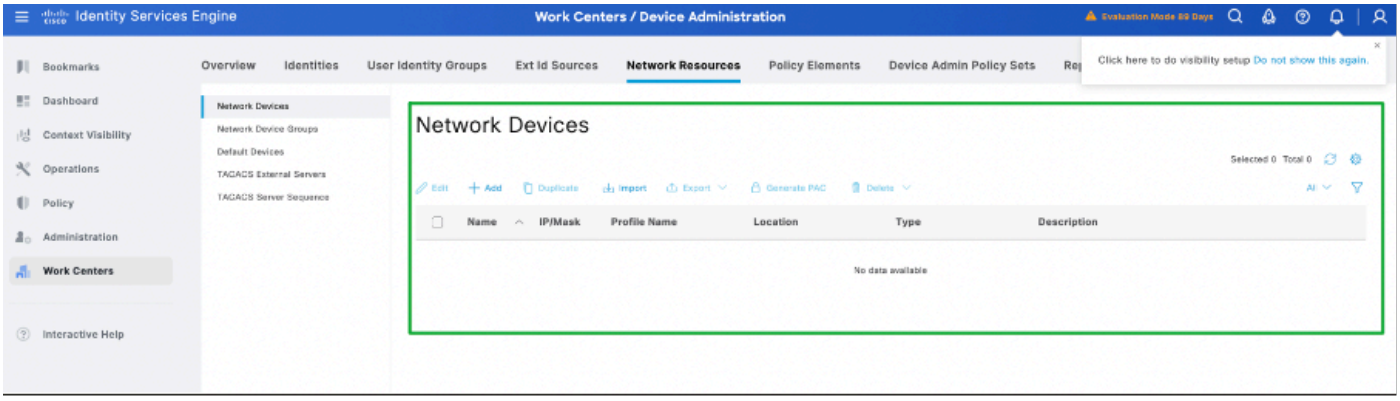
來自ISE的TACACS即時日誌 — 交換機驗證。

疑難排解

本節討論發現的一些與TACACS+驗證相關的常見問題。

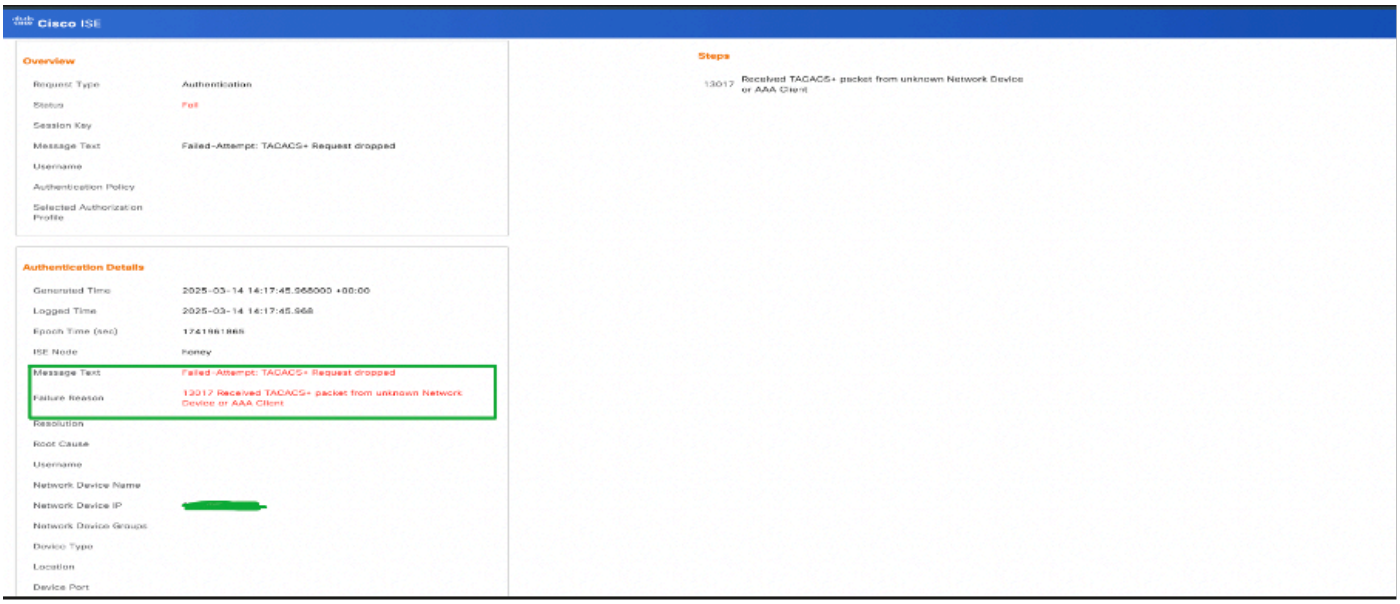
案例 1:TACACS+驗證失敗，顯示「Error:13017收到來自未知網路裝置或AAA客戶端」的TACACS+資料包。

當網路裝置未新增為ISE中的網路資源時，會出現此情況。如本螢幕截圖所示，交換機不會新增到ISE的網路資源中。



故障排除場景 — 網路裝置未新增到ISE。

現在，當您從交換機/網路裝置測試身份驗證時，資料包按預期到達ISE。但是，驗證失敗，並出現錯誤「Error:13017收到來自未知網路裝置或AAA客戶端」的TACACS+資料包，如下螢幕截圖所示：



TACACS即時日誌 — 網路裝置未新增到ISE時失敗。

從網路裝置（交換機）進行驗證

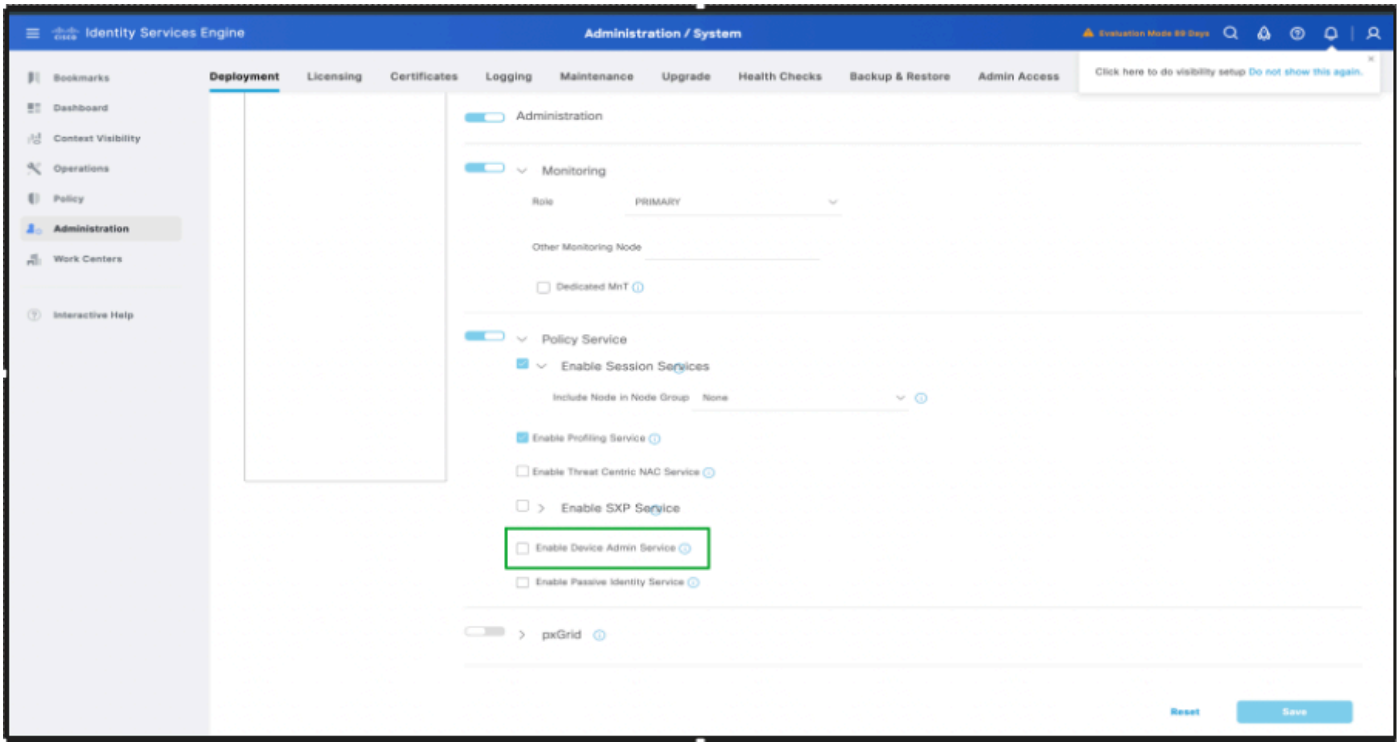
Switch#test aaa group isegroup switch XXXXXX new
使用者已拒絕

解決方案：驗證交換機/路由器/網路裝置是否新增為ISE中的網路裝置。如果未新增裝置，請將網路裝置新增到ISE的網路裝置清單。

案例 2: ISE會在沒有任何資訊的情況下以靜默方式丟棄TACACS+資料包。

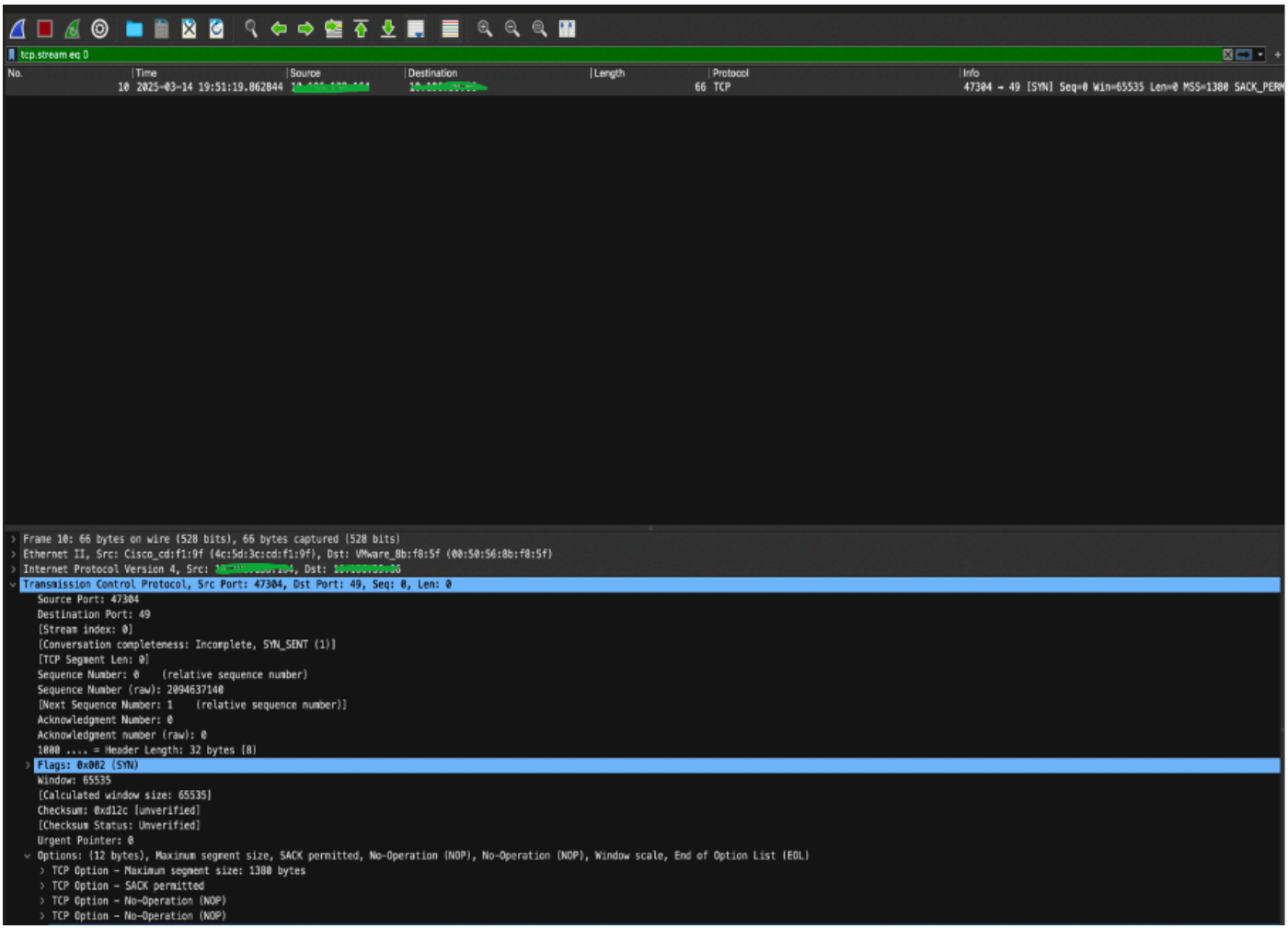
當ISE中禁用裝置管理服務時，會出現此情況。在此場景中，ISE丟棄資料包，並且即使正在從新增到ISE網路資源的網路裝置啟動身份驗證，也不會看到即時日誌。

如本螢幕截圖所示，在ISE中禁用裝置管理。



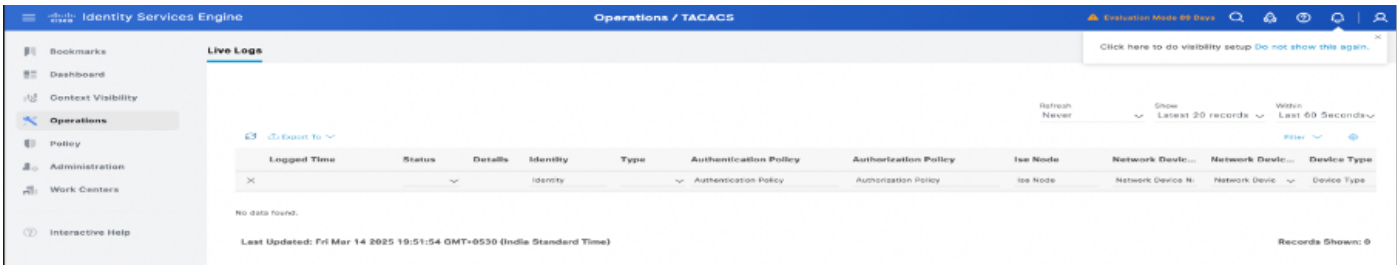
場景，ISE中未啟用裝置管理。

當使用者從網路裝置發起身份驗證時，ISE會在即時日誌中沒有任何資訊的情況下以靜默方式丟棄資料包，並且ISE不會響應網路裝置傳送的Syn資料包，以完成TACACS身份驗證過程。請參閱以下螢幕截圖：



ISE在TACACS期間以靜默方式丟棄資料包

ISE在身份驗證期間不顯示即時日誌。



無TACACS即時日誌 — 從ISE驗證

從網路裝置（交換機）進行驗證

Switch#
Switch#test aaa group isegroup switch XXXX new
使用者已拒絕
Switch#
*2014年3月14日13:54:28.14:T+:版本192(0xC0)，型別1，序列1，加密1,SC 0
*2014年3月14日13:54:28.14:T+:session_id 10158877(0x9B031D), dlen 14(0xE)
*2014年3月14日13:54:28.14:T+:type:AUTHEN/START， priv_lvl:15 action:LOGIN ascii
*2014年3月14日13:54:28.14:T+:svc:LOGIN user_len:6 port_len:0(0x0)raddr_len:0(0x0)data_len:0
*2014年3月14日13:54:28.14:T+:使用者： 交換器
*2014年3月14日13:54:28.14:T+:連接埠：
*2014年3月14日13:54:28.14:T+:rem_addr:
*2014年3月14日13:54:28.14:T+:資料：
*2014年3月14日13:54:28.14:T+:End Packet

解決方案：在ISE中啟用裝置管理。

參考

- 疑難排解TACACS驗證問題
- 思科身份服務引擎管理員指南3.3版
- 適用於TACACS伺服器的VRF

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。