Configurazione di TACACS+ con ISE Gigabit Ethernet 1 Interface

Sommario

Introduzione

In questo documento viene descritta la configurazione ISE TACACS+ con interfaccia Gigabit Ethernet 1 con router e switch che funzionano come dispositivi di rete.

Premesse

Cisco ISE supporta fino a 6 interfacce Ethernet. Può avere solo tre obbligazioni, obbligazione 0, obbligazione 1 e obbligazione 2. Non è possibile modificare le interfacce che fanno parte di

un'obbligazione o cambiare il ruolo dell'interfaccia in un'obbligazione.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di rete
- Cisco Identity Service Engine.

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni hardware e software:

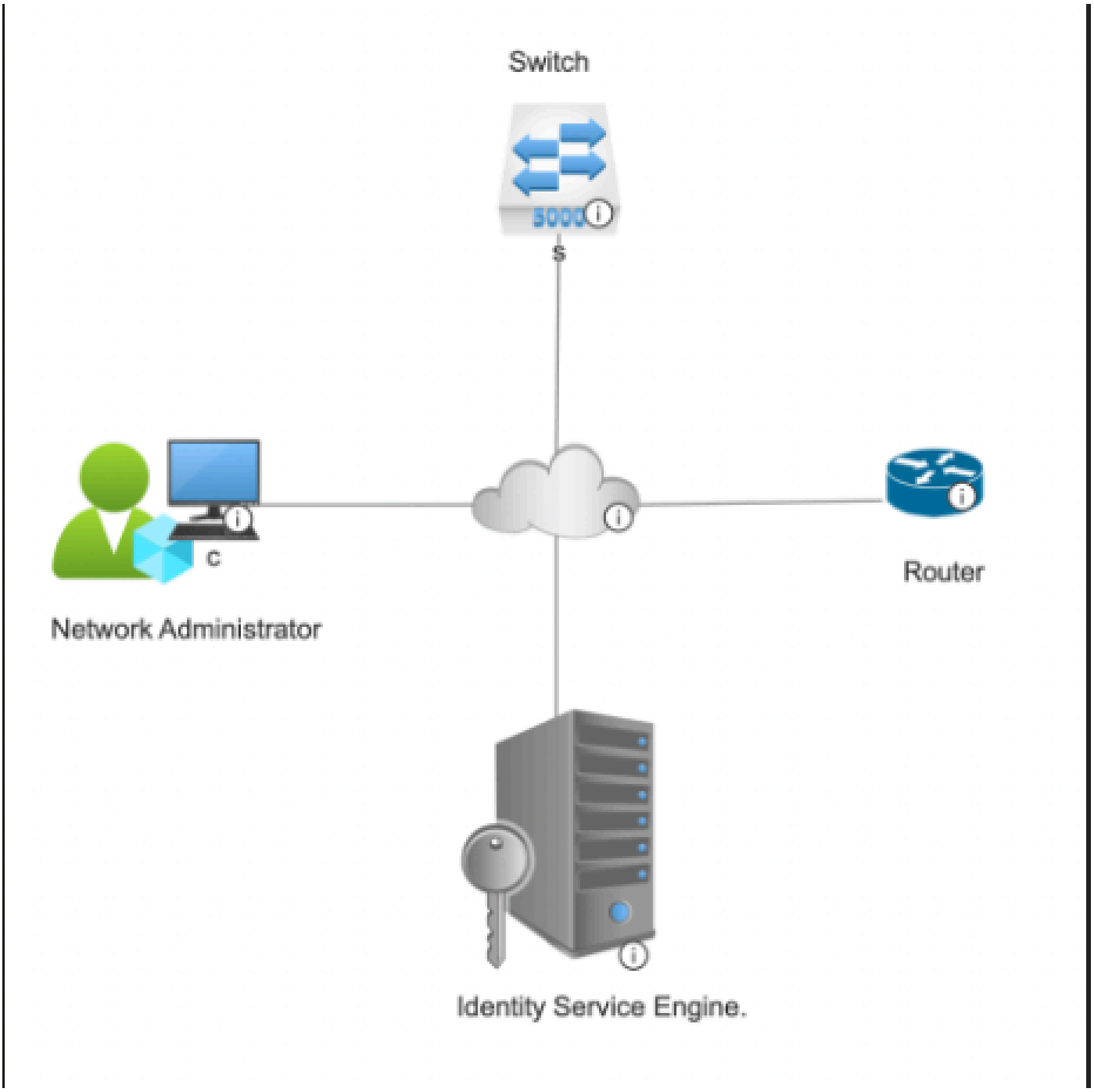
- Cisco Identity Service Engine v3.3
- Software Cisco IOS® versione 17.x
- Cisco C9200 switch.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Lo scopo della configurazione è: Configurare Gigabit Ethernet 1 di ISE per TACACS+ e autenticare switch e router con TACACS+ con ISE come server di autenticazione.

Esempio di rete

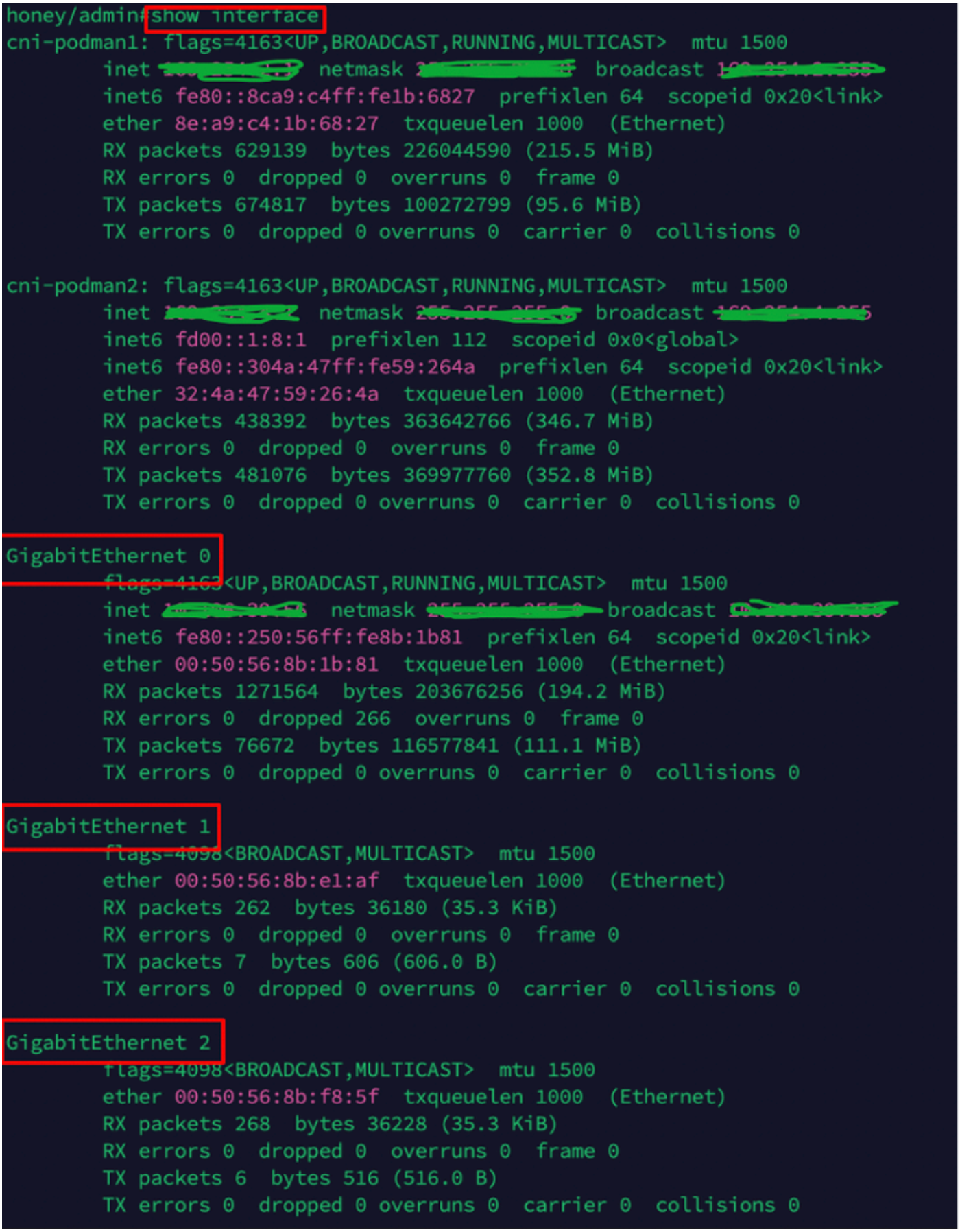


Topologia della rete

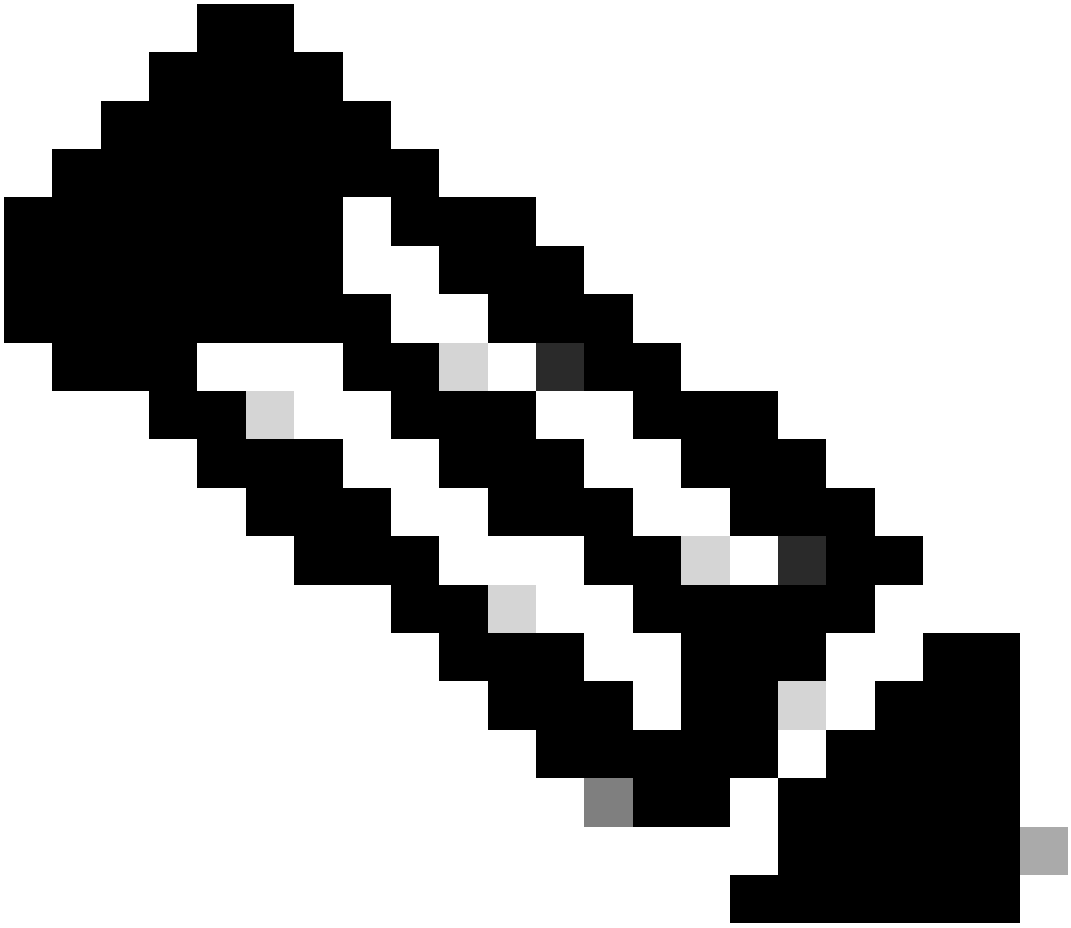
Configurazione di Identity Services Engine per TACACS+

Configurazione dell'indirizzo IP per l'interfaccia Gigabit Ethernet 1 in ISE

1. Accedere alla CLI del nodo PSN di ISE in cui è abilitato Device admin e verificare le interfacce disponibili con il comando show interface:



Verifica delle interfacce in ISE



Nota: In questa configurazione, solo tre interfacce sono configurate in ISE, con particolare attenzione all'interfaccia Gigabit Ethernet 1. La stessa procedura può essere applicata per configurare l'indirizzo IP di tutte le interfacce. Per impostazione predefinita, ISE supporta fino a sei interfacce Gigabit Ethernet.

---

2. Dalla CLI dello stesso nodo PSN, assegnare un indirizzo IP all'interfaccia Gigabit Ethernet 1 utilizzando questi comandi:

hostnameofise#configure t

hostnameofise/admin(config)#interface Gigabit Ethernet 1

hostnameofise/admin(config-GigabitEthernet-1)# <indirizzo ip> <subnet mask> % La modifica dell'indirizzo IP potrebbe causare il riavvio dei servizi ISE

Continuare con la modifica dell'indirizzo IP?

Procedere? [sì,no] sì

3. L'esecuzione del passaggio 2 comporta il riavvio dei servizi del nodo ISE. Per verificare lo stato dei servizi ISE, eseguire il comando show application status ise e verificare che lo stato dei servizi sia in esecuzione come mostrato in questa schermata:

```
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
```

Verifica dello stato del servizio ISE

4. Verificare l'indirizzo IP dell'interfaccia Gig1 con il comando show interface:

V

```
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
```

Verifica dell'indirizzo IP dell'interfaccia ISE Gig2 dalla CLI

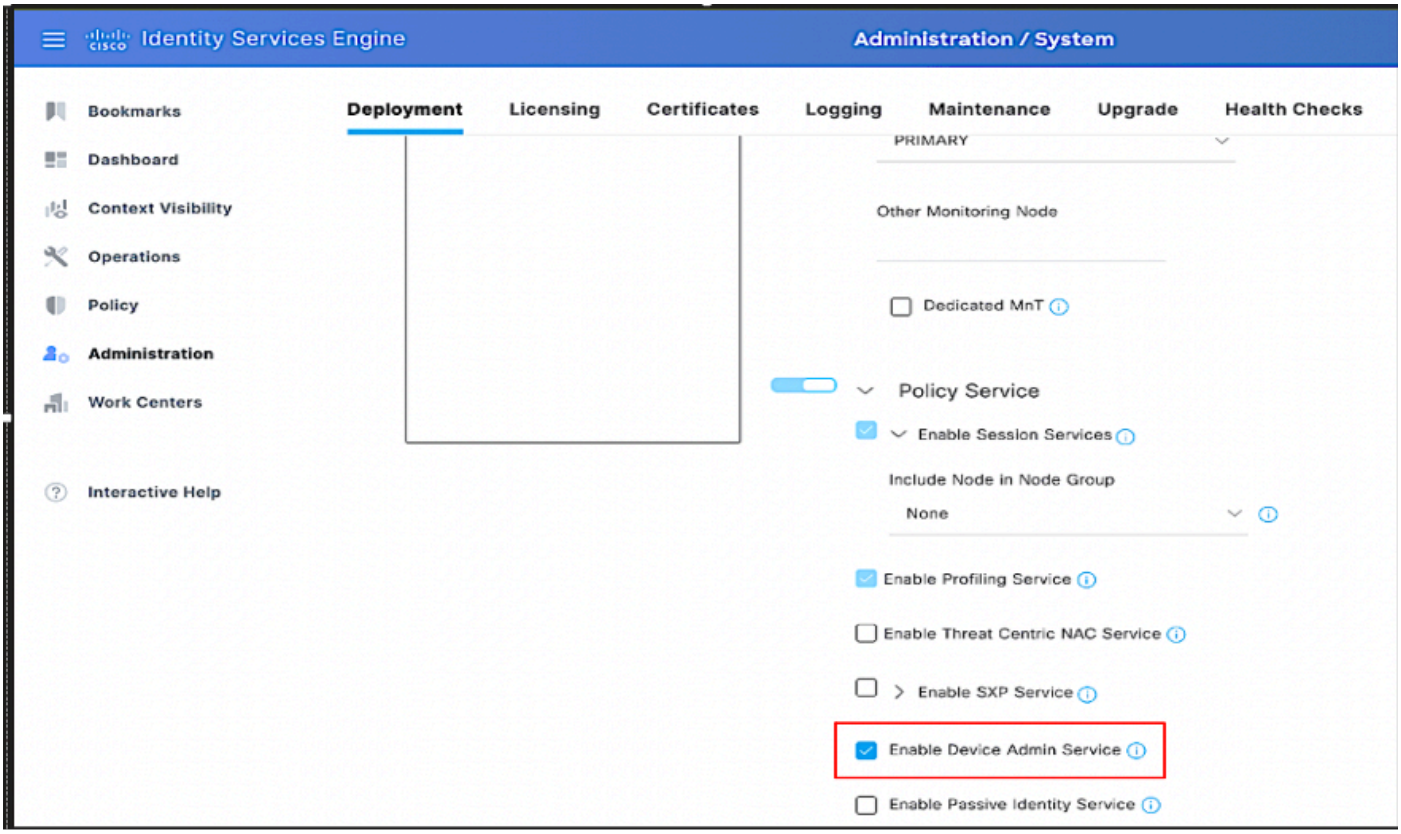
5. Verificare la tolleranza della porta 49 nel nodo ISE utilizzando il comando show ports | inc 49 comando:

```
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,
```

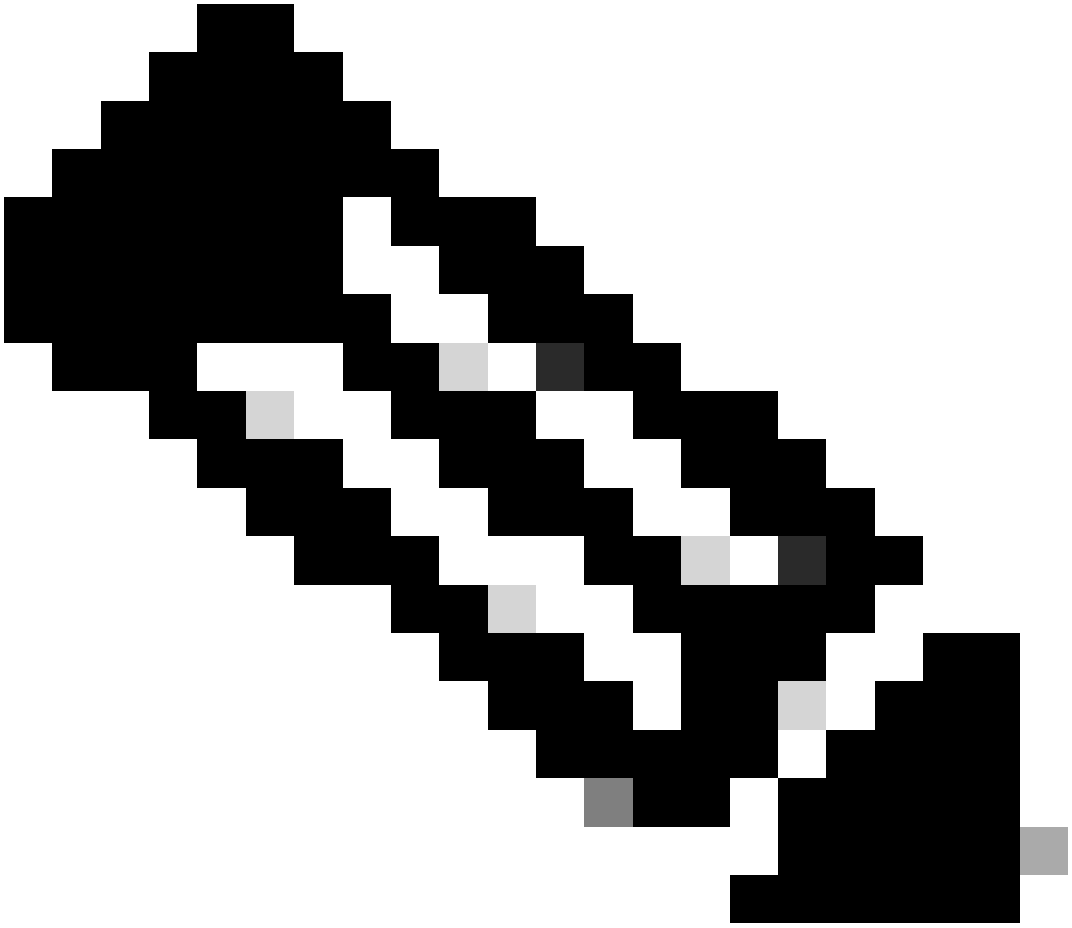
verifica della tolleranza per la porta 49 nell'ISE

Abilitare l'amministrazione dei dispositivi in ISE

Selezionare GUI di ISE > Amministrazione > Distribuzione > Selezionare il nodo PSN, quindi selezionare Abilita servizio di amministrazione dispositivi:



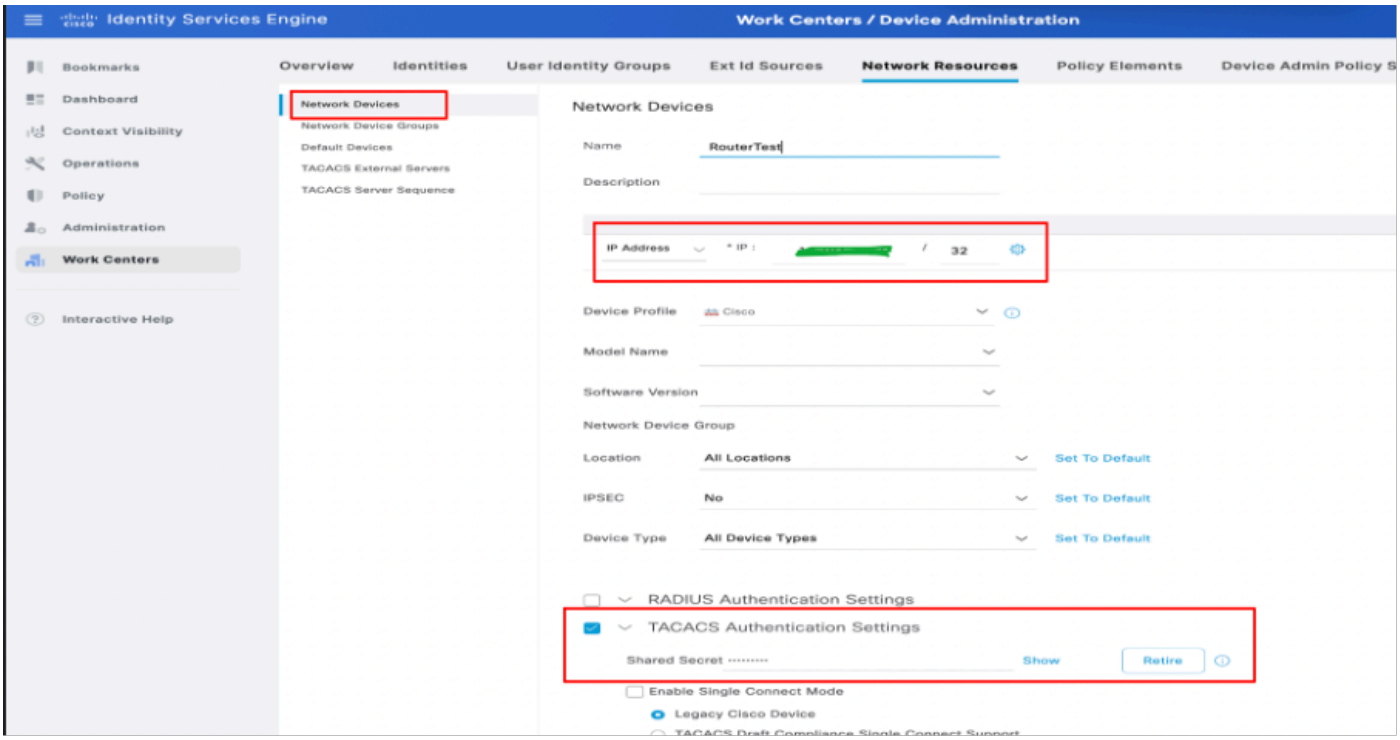
Abilitazione del servizio di amministrazione dei dispositivi in ISE



Nota: Per attivare il servizio Device Admin, è necessario disporre di una licenza di amministrazione del dispositivo.

Aggiungi un dispositivo di rete ad ISE

1. Passare a Centri di lavoro > Amministrazione dispositivi > Risorse di rete > Dispositivi di rete. Fare clic su Add. Fornire nome, indirizzo IP. Selezionare la casella di controllo TACACS+ Authentication Settings (Impostazioni autenticazione TACACS+) e fornire la chiave segreta condivisa.



Configurazione di un dispositivo di rete in ISE

2. Per aggiungere tutti i dispositivi di rete necessari per l'autenticazione TACACS, attenersi alla procedura descritta sopra.

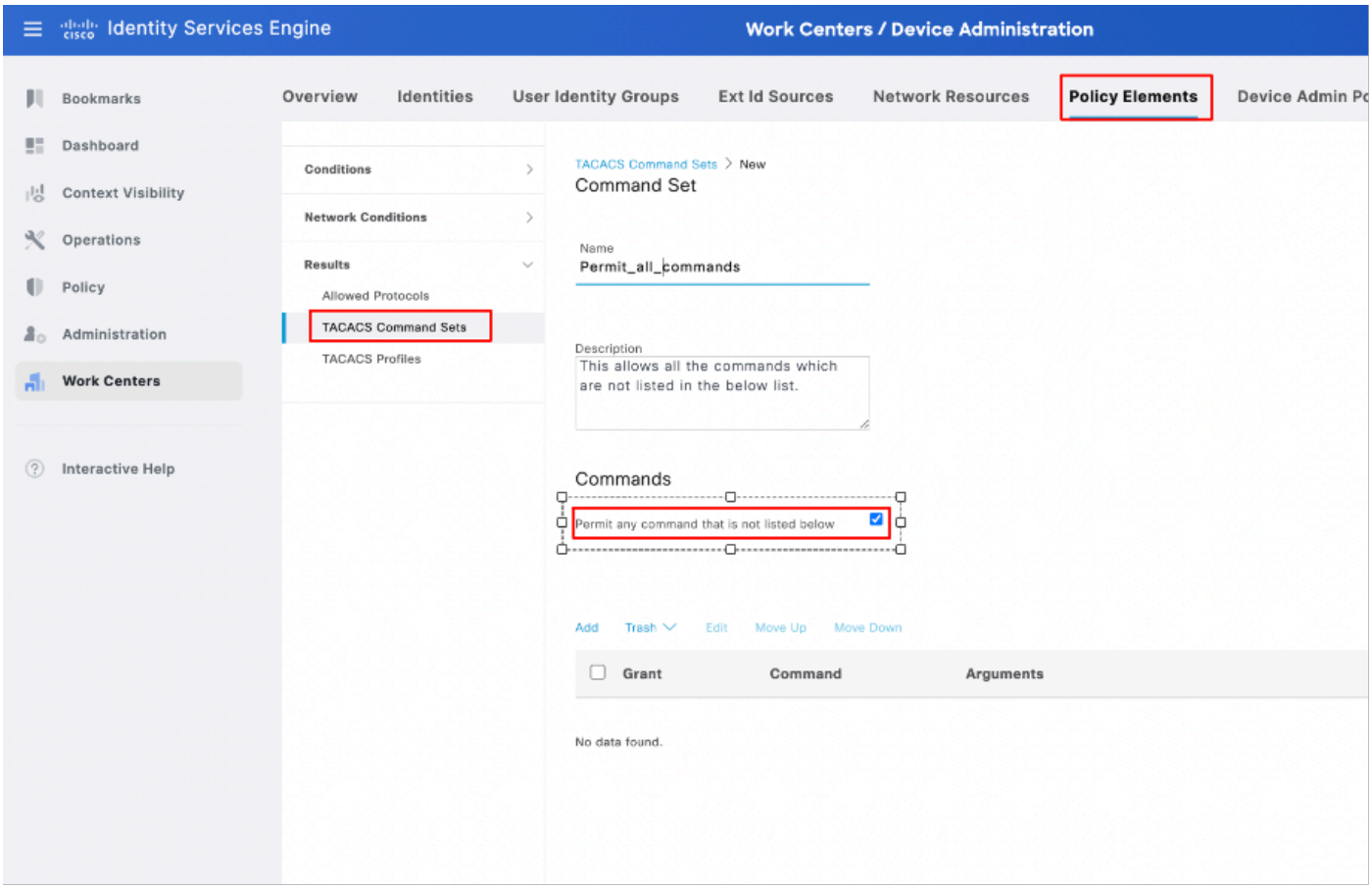
Configura set di comandi TACACS+

Per questa dimostrazione sono configurati due set di comandi:

Permit_all_commands, viene assegnato all'amministratore utenti e consente tutti i comandi sul dispositivo.

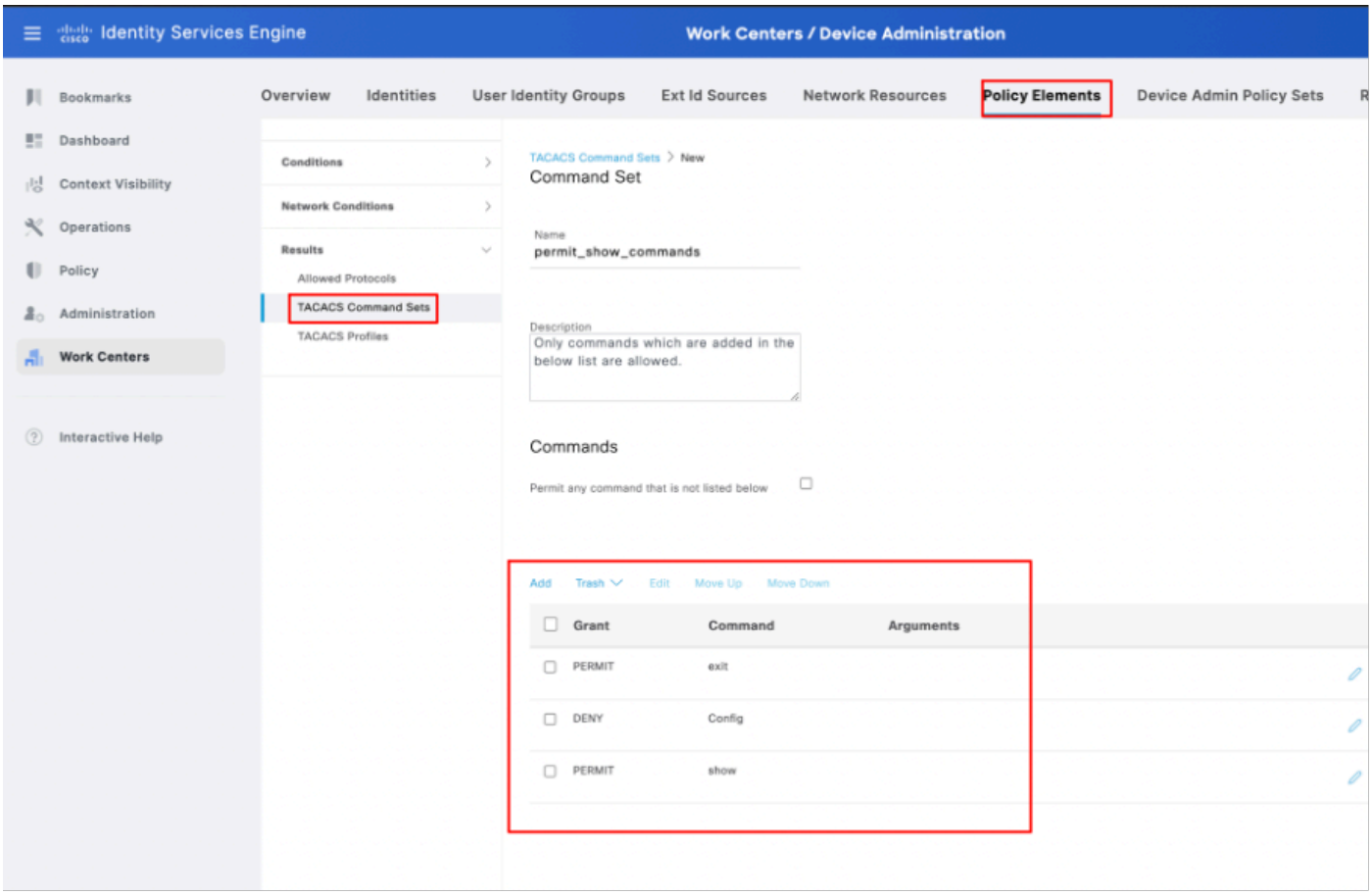
allow_show_commands, è assegnato a un utente e consente solo comandi show

1. Passare a Centri di lavoro > Amministrazione dispositivi > Risultati criteri > Set di comandi TACACS. Fare clic su Aggiungi. Specificare il nome PermitAllCommands, quindi scegliere la casella di controllo Permit any command non elencata. Fare clic su Invia.



Configurazione dei set di comandi in ISE

2. Passare a Centri di lavoro > Amministrazione dispositivi > Risultati dei criteri > Set di comandi TACACS. Fare clic su Aggiungi. Specificare il nome PermitShowCommands, fare clic su Aggiungi, quindi infine consentire i comandi show e exit. Per impostazione predefinita, se gli argomenti vengono lasciati vuoti, vengono inclusi tutti gli argomenti. Fare clic su Invia.

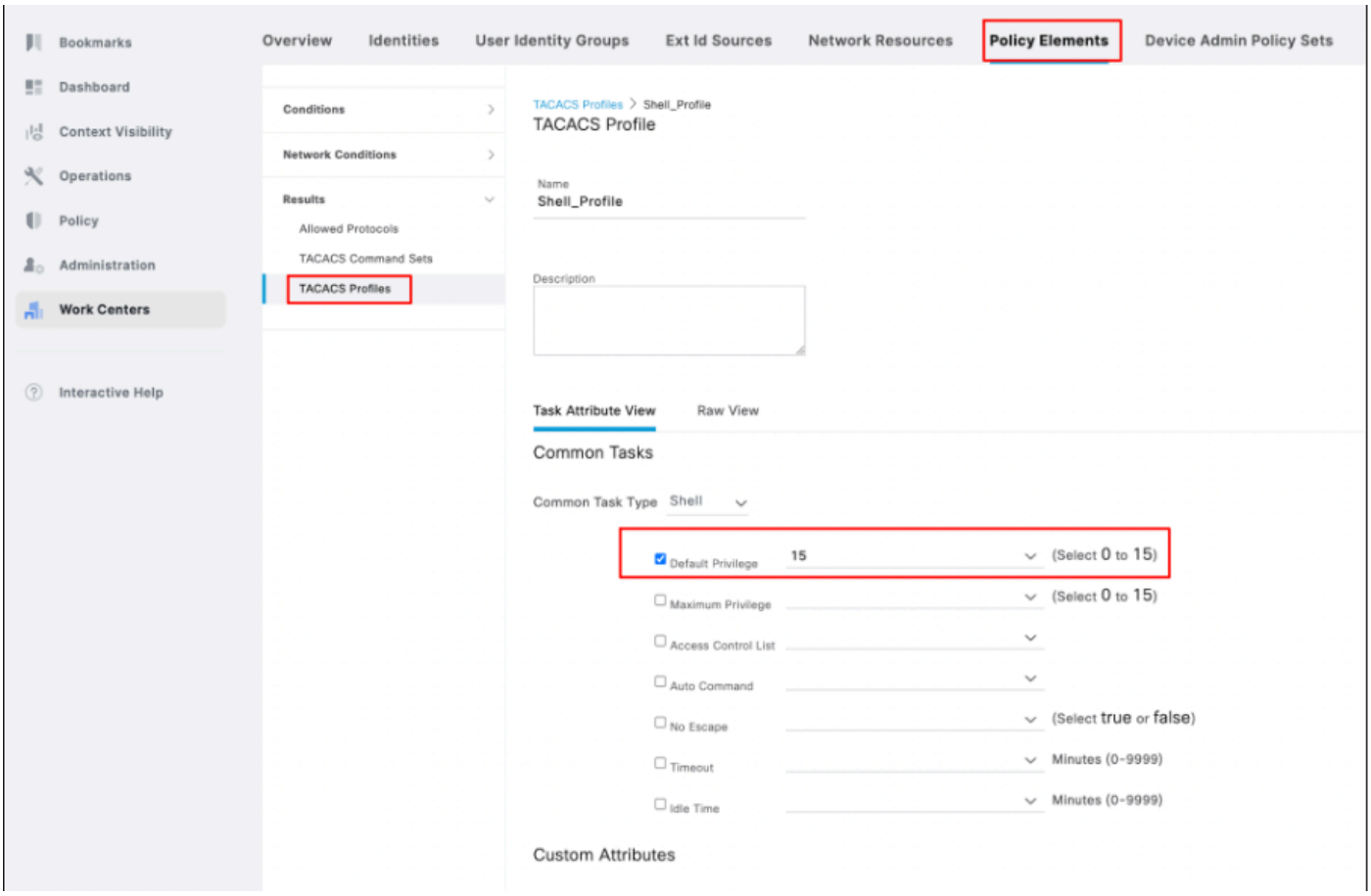


Configurazione di allow_show_commands in ISE

Configurazione del profilo TACACS+

È stato configurato un singolo profilo TACACS+ e l'autorizzazione del comando viene eseguita tramite set di comandi.

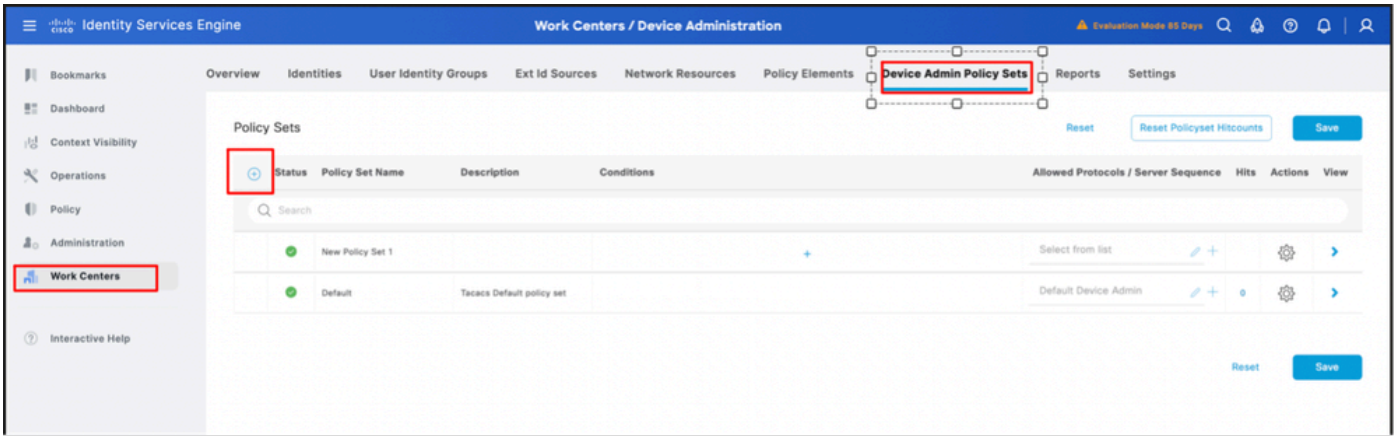
Per configurare un profilo TACACS+, selezionare Work Center > Device Administration > Policy Results > TACACS Profiles. Fare clic su Add (Aggiungi), fornire un nome per il profilo di shell, selezionare la casella di controllo Default Privilege (Privilegio predefinito) e immettere il valore 15. Infine, fare clic su Submit (Invia).



Configurazione del profilo TACACS in ISE

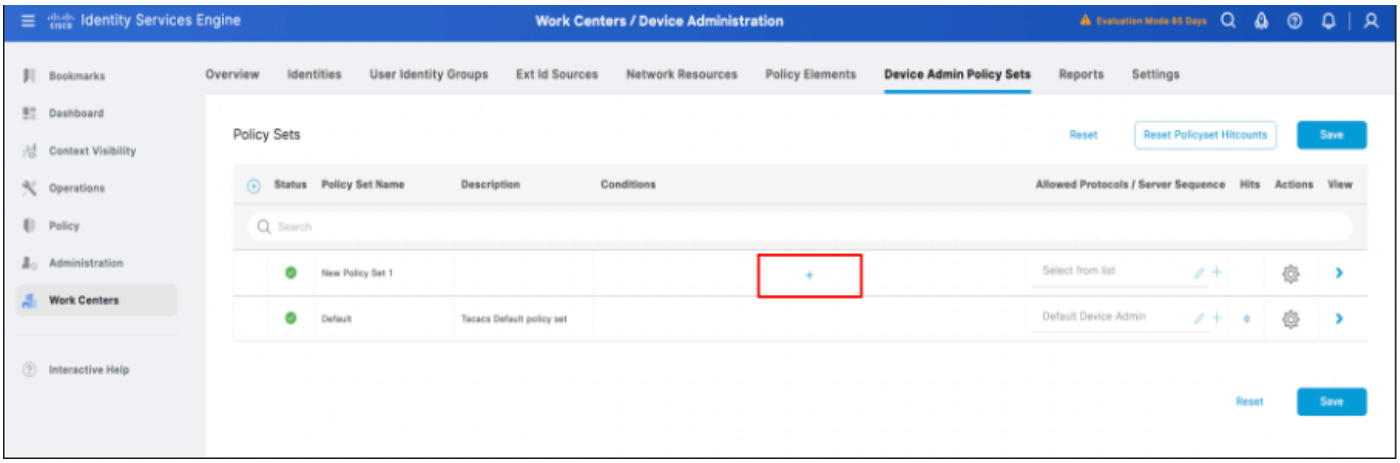
Configurazione del profilo di autenticazione e autorizzazione TACACS+

1. Accedere alla GUI ISE PAN -> Amministrazione -> Centri di lavoro -> Amministrazione dispositivi -> Set di criteri di amministrazione dispositivi. Fare clic sull'icona + (più) per creare un nuovo criterio. In questo caso, al set di criteri viene assegnato il nome Nuovo set di criteri 1.



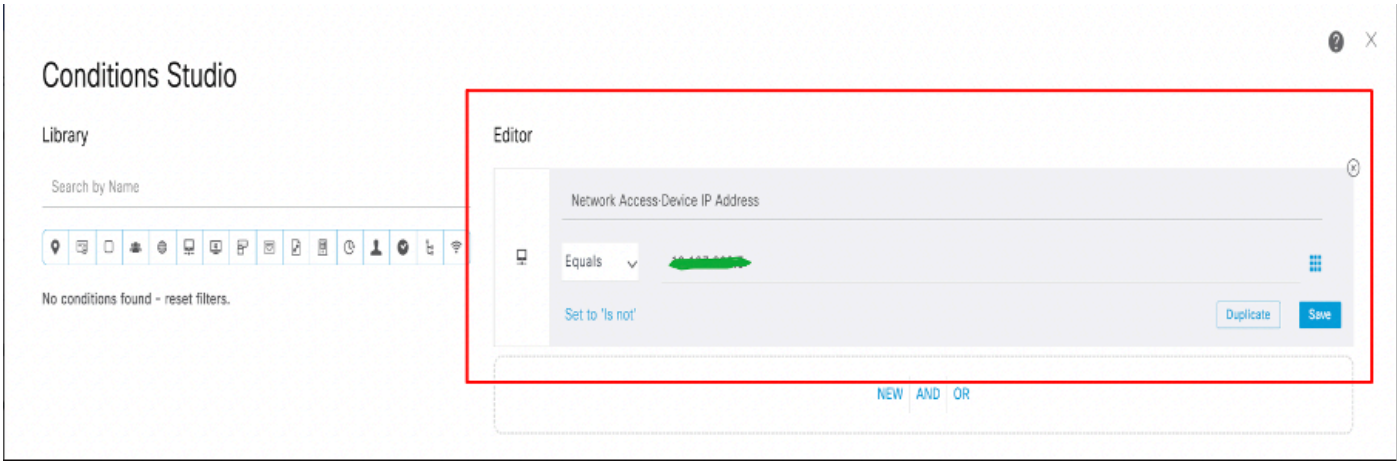
Configurazione della policy impostata in ISE

2. Prima di salvare il set di criteri, è necessario configurare le condizioni, come mostrato in questa schermata. Fare clic sull'icona + (più) per configurare le condizioni per il set di criteri.

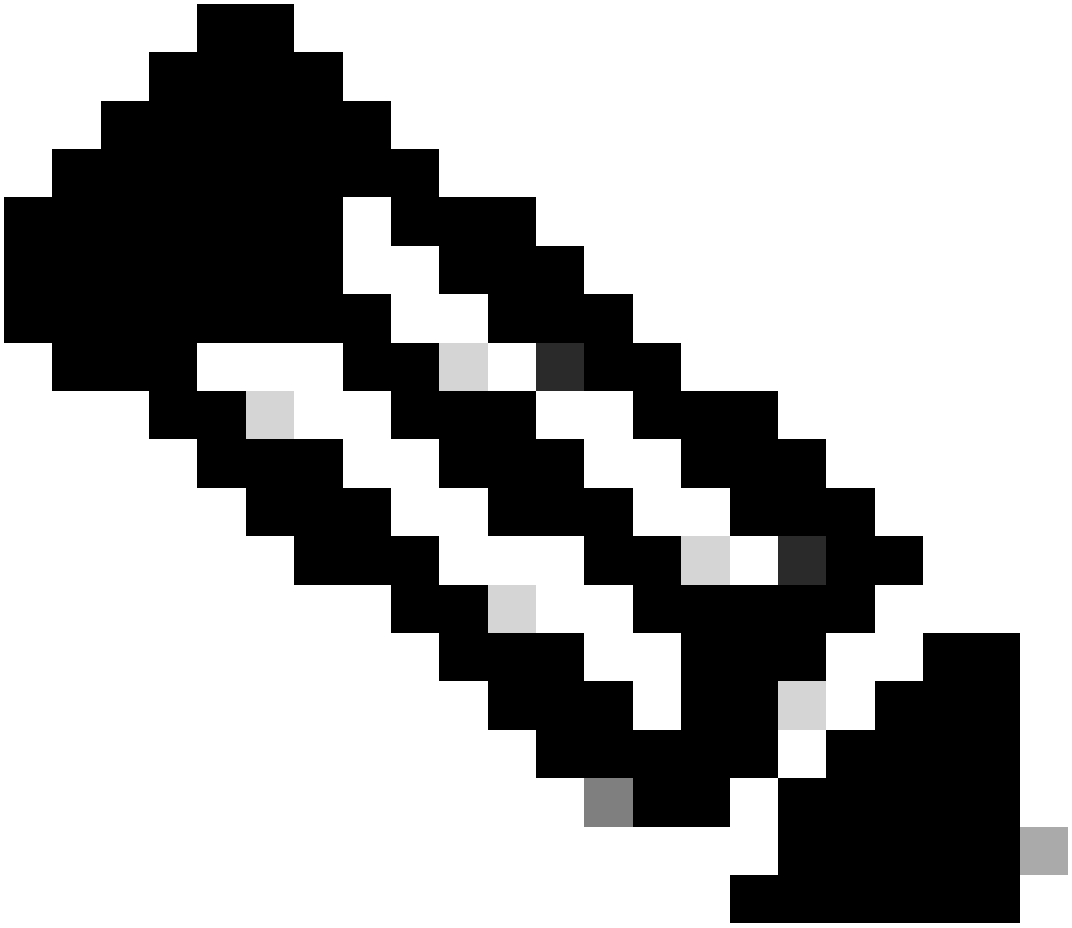


Configurazione delle condizioni per il set di criteri in ISE

3. Dopo aver fatto clic sull'icona + (più) come indicato al punto 2, viene visualizzata la finestra di dialogo Studio condizioni. Configurare le condizioni necessarie. Salvare la condizione con le condizioni nuove o esistenti, scorrere. Fare clic su Usa.

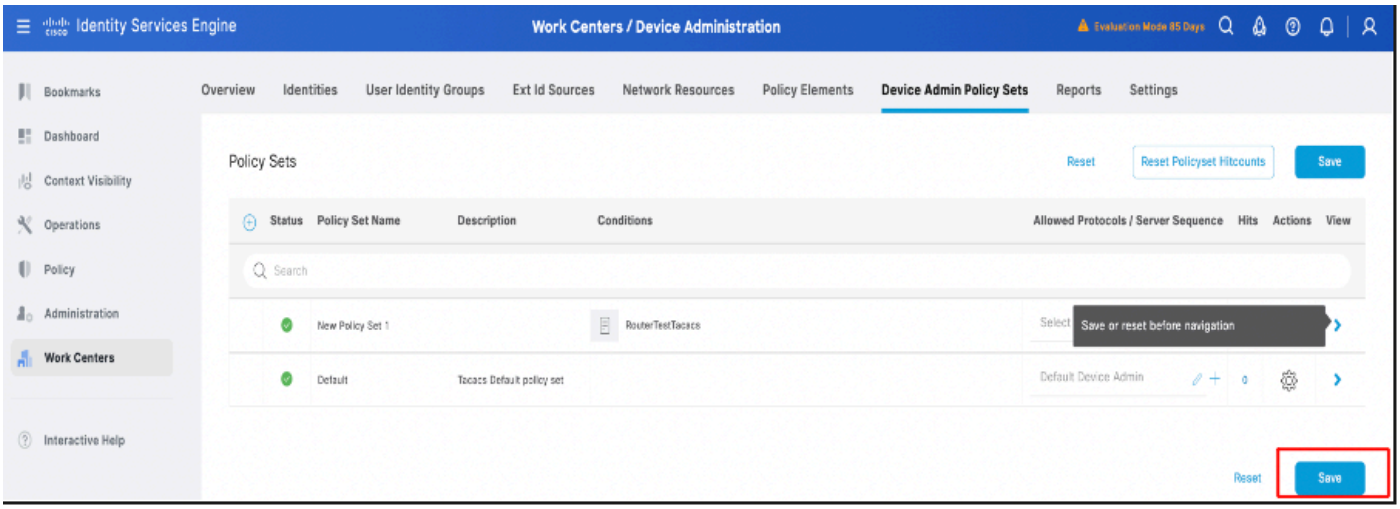


Configurazione delle condizioni per il set di criteri in ISE



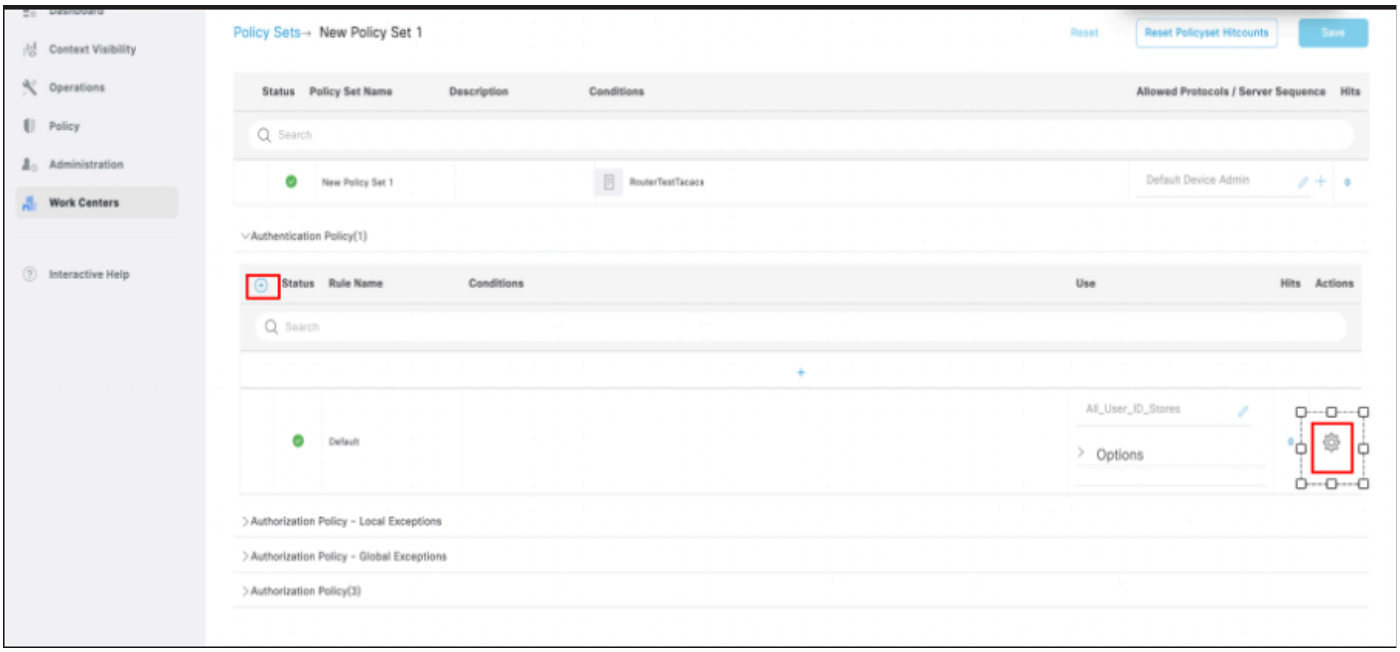
Nota: Per questa documentazione, le condizioni corrispondono all'indirizzo IP del dispositivo di rete. Le condizioni possono tuttavia variare in base ai requisiti di distribuzione.

4. Una volta configurate e salvate le condizioni, configurare i protocolli consentiti come amministratore predefinito del dispositivo. Salvare il set di criteri creato facendo clic sull'opzione Salva .

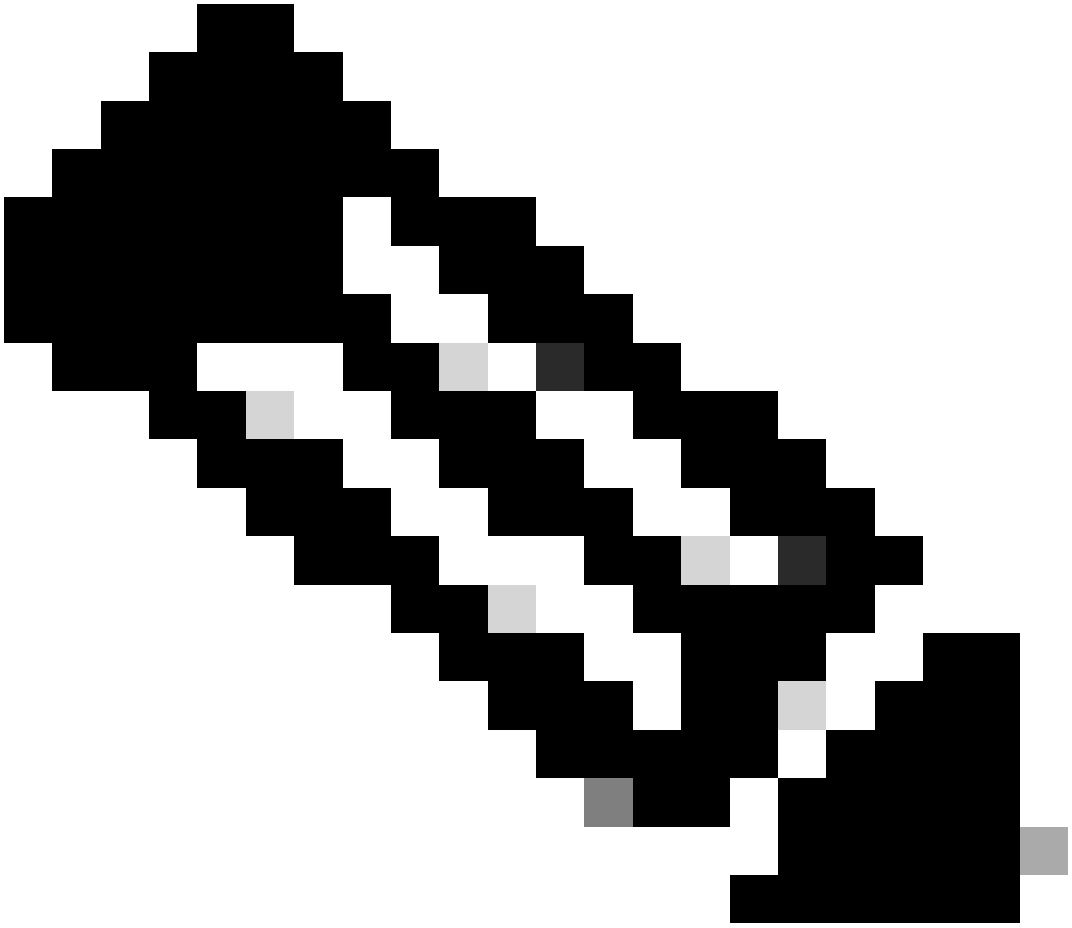


Conferma configurazione set di criteri.

5. Espandere il Nuovo set di criteri -> Criteri di autenticazione (1) -> Creare un nuovo criterio di autenticazione facendo clic sull'icona + (più) o facendo clic sull'icona a forma di ingranaggio, quindi inserire una nuova riga sopra.

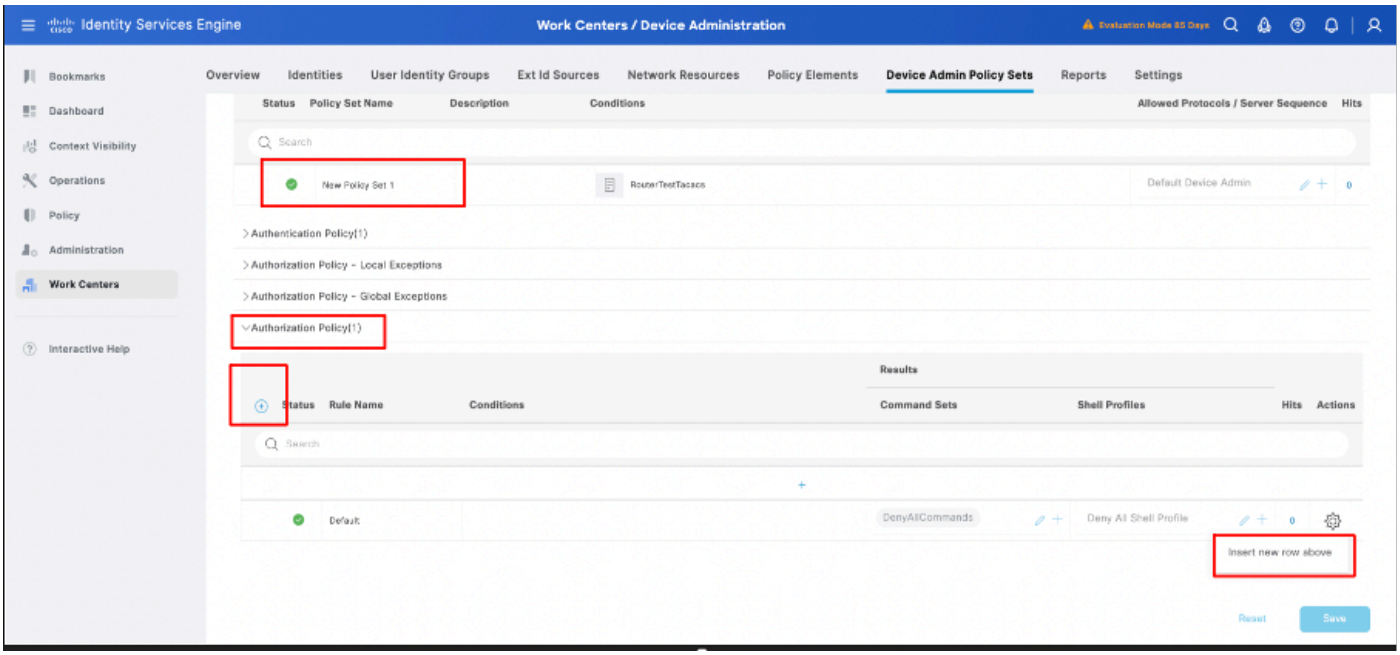


Configurazione dei criteri di autenticazione nel set di criteri.



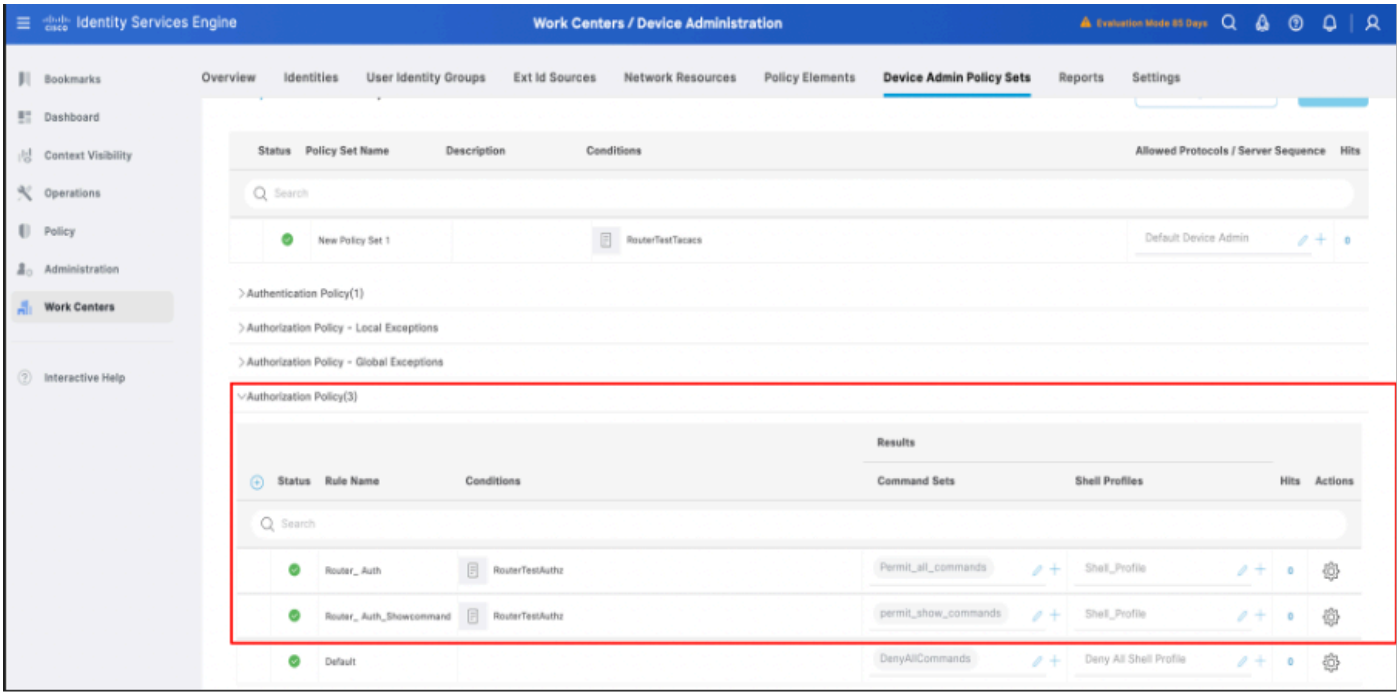
Nota: Per questa dimostrazione, viene utilizzato il criterio di autenticazione predefinito impostato con All_User_ID_Stores. Tuttavia, l'utilizzo degli archivi Identity è personalizzabile in base ai requisiti di distribuzione.

6. Espandere il nuovo set di criteri -> Criteri di autorizzazione (1). Fate clic sull'icona + (più) oppure sull'icona dell'ingranaggio. Quindi, inserire una nuova riga sopra per creare un criterio di autorizzazione.

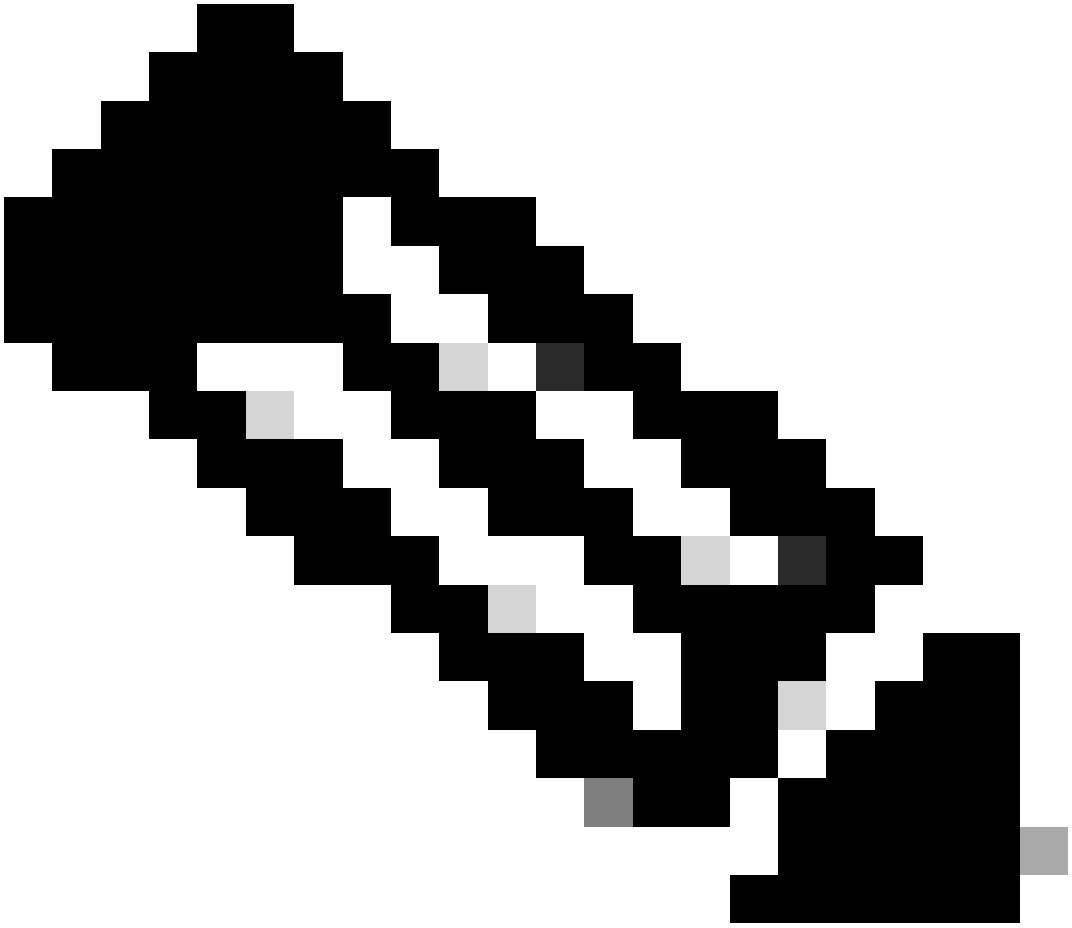


Configurazione dei criteri di autorizzazione

7. Configurare il criterio di autorizzazione con condizioni, set di comandi e profilo della shell mappati ai criteri di autorizzazione.



Configurazione completa dei criteri di autorizzazione in ISE



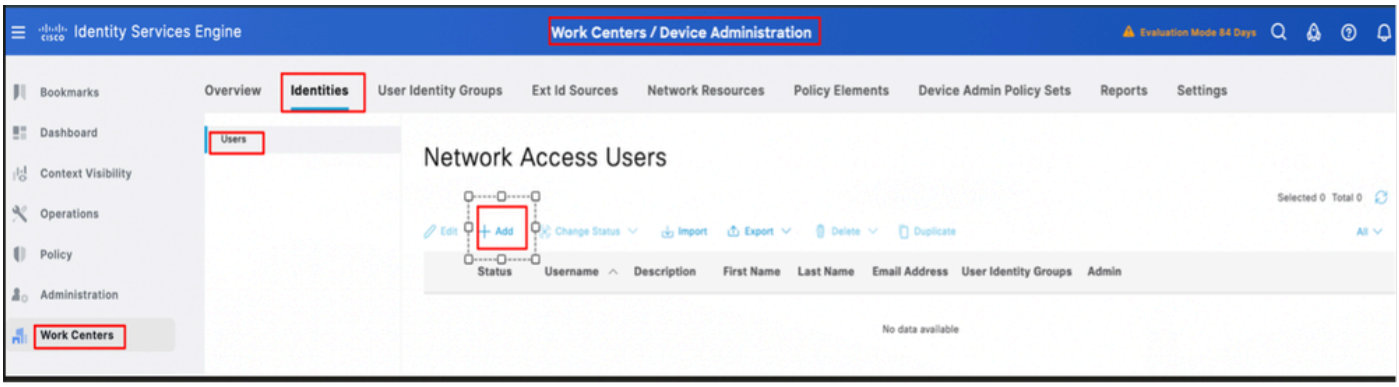
Nota: Le condizioni configurate sono conformi all'ambiente lab e possono essere configurate in base ai requisiti di installazione.

---

8. Seguire i primi 6 passaggi per configurare i set di criteri per lo switch o qualsiasi altro dispositivo di rete usato per TACACS+.

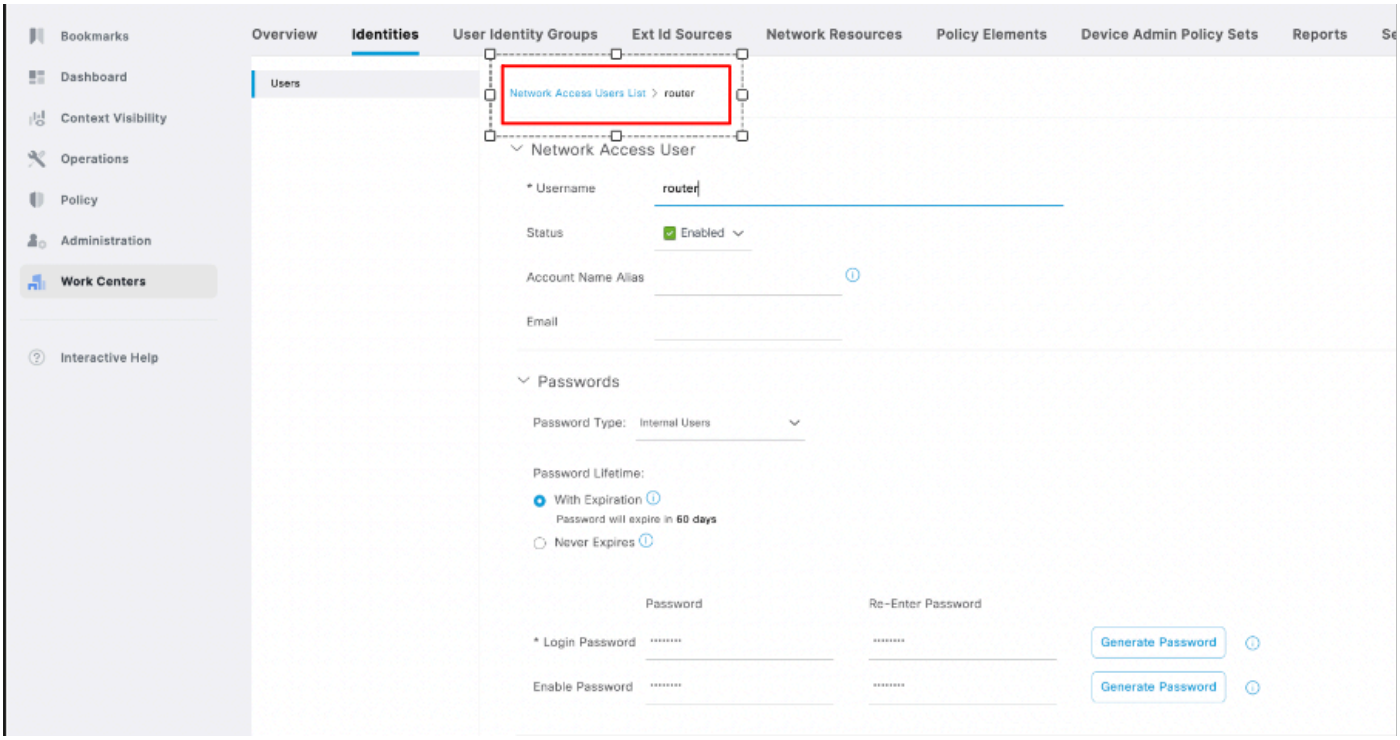
Configurazione degli utenti di Network Access per l'autenticazione TACACS di AD in ISE

1. Passare a Workcenter -> Amministrazione dispositivi -> Identità -> Utenti. Fare clic sull'icona +(più) per creare un nuovo utente.



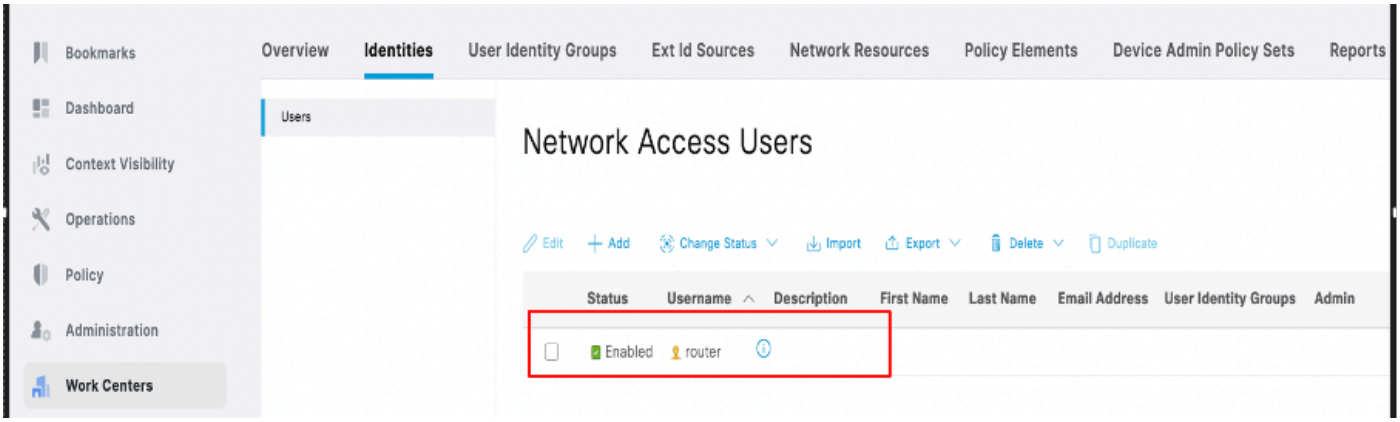
Configurare gli utenti di accesso alla rete in ISE

2. Fornire per espandere i dettagli del nome utente e della password, mappare l'utente a un gruppo di identità utente (facoltativo), quindi fare clic su Invia.



Configura utenti di accesso alla rete - Continua

3. Dopo aver sottomesso la configurazione del nome utente nei centri di lavoro -> Identità -> Utenti -> Utenti di accesso alla rete, l'utente viene configurato e abilitato in modo visibile.



Configurazione del router per TACACS+

Configurazione del router Cisco IOS per l'autenticazione e l'autorizzazione TACACS+

1. Accedere alla CLI del router ed eseguire questi comandi per configurare il TACACS nel router.

ASR1001-X(config)#aaa new-model — comando richiesto per abilitare aaa in NAD

ASR 1001-X(config)#aaa session-id comune. —Comando richiesto per abilitare aaa in NAD.

ASR 1001-X(config)#aaa authentication login gruppo predefinito tacacs+ local

ASR 1001-X(config)#aaa authorization exec gruppo predefinito tacacs+

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

ASR 1001-X(config)#tacacs server ise1

ASR1001-X(config-server-tacacs)#address ipv4 <indirizzo IP del server TACACS > . — Indirizzo IP dell'interfaccia ISE G1.

ASR 1001-X(config-server-tacacs)# chiave XXXXX

ASR 1001-X(config)# gruppo server aaa tacacs+ isegroup

ASR 1001-X(config-sg-tacacs+)#nome server ise1

ASR 1001-X(config-sg-tacacs+)#ip vrf forwarding Mgmt-intf

ASR 1001-X(config-sg-tacacs+)#ip tacacs source-interface Gigabit Ethernet0

ASR 1001-X(config-sg-tacacs+)#ip tacacs source-interface Gigabit Ethernet1

ASR 1001-X(config) #exit

2. Dopo aver salvato le configurazioni TACACS+ del router, verificare la configurazione TACACS+ utilizzando il comando show run aaa.

ASR 1001-X#show run aaa

!

autenticazione aaa gruppo predefinito isegroup locale

iegroup gruppo predefinito esecuzione autorizzazione aaa

gruppo isegroup elenco1 di reti di autorizzazione aaa

username admin password 0 XXXXXXX

!

tacacs server ise1

address ipv4 <indirizzo IP del server TACACS>

chiave XXXXX

!

!

gruppo server aaa tacacs+ isegroup

nome server ise1

ip vrf forwarding Mgmt-intf

ip tacacs source-interface Gigabit Ethernet1

!

!

!

aaa new-model

id sessione aaa comune

!

!

Configurazione dello switch per TACACS+

Configurazione dello switch per autenticazione e autorizzazione TACACS+

1. Accedere alla CLI dello switch ed eseguire questi comandi per configurare TACACS nello switch.

C9200L-48P-4X#configure t

Immettere i comandi di configurazione, uno per riga. Termina con CNTL/Z.

C9200L-48P-4X(config)#aaa new-model. — comando necessario per abilitare aaa in NAD

C9200L-48P-4X(config)#aaa session-id comune. — comando richiesto per abilitare aaa in NAD.

C9200L-48P-4X(config)#aaa authentication login default group isegroup local

C9200L-48P-4X(config)#aaa authorization exec gruppo isegroup predefinito

C9200L-48P-4X(config)#aaa authorization network list1 gruppo isegroup

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

C9200L-48P-4X(config-server-tacacs)#address ipv4 <indirizzo IP del server TACACS> — indirizzo IP dell'interfaccia ISE G1.

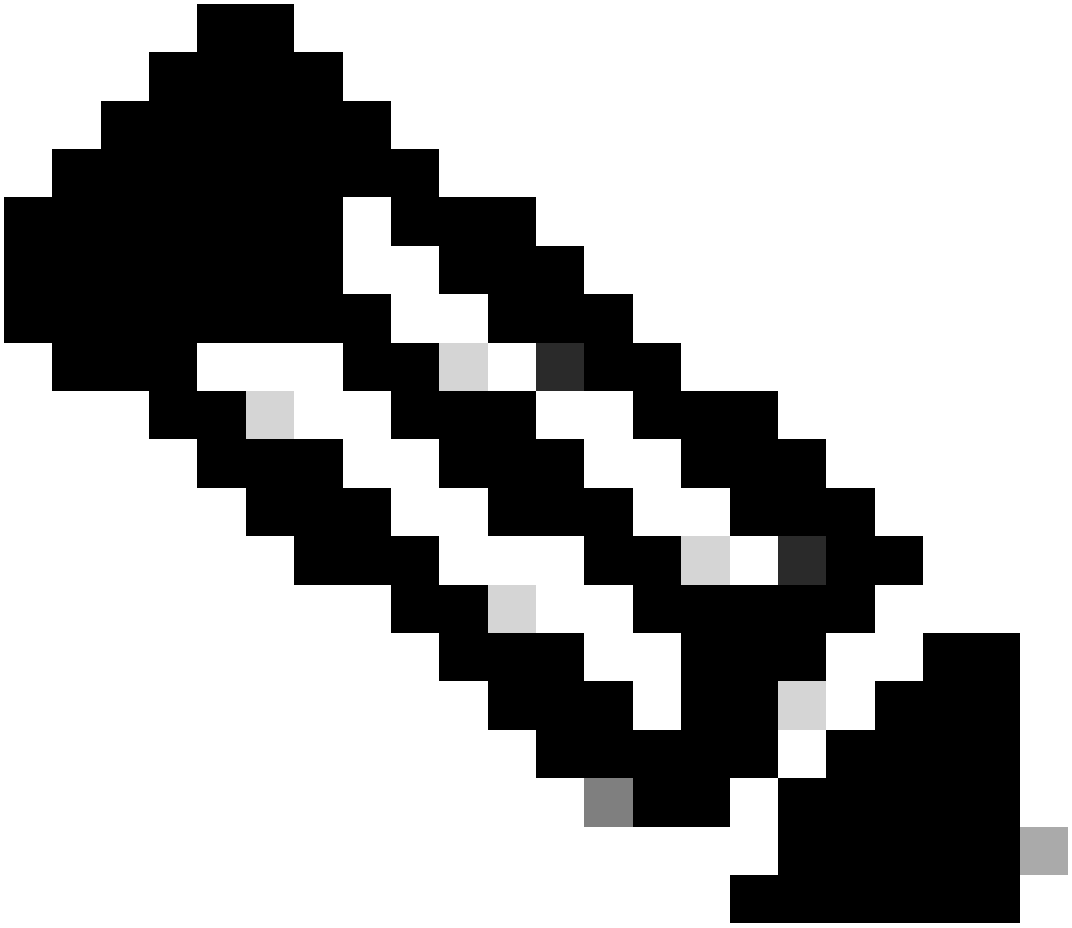
C9200L-48P-4X (config-server-tacacs)#key XXXXX

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

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

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

C9200L-48P-4X#wr mem



Nota: Nella configurazione NAD TACACS+, tacacs+ è il gruppo che può essere personalizzato in base ai requisiti di installazione.

---

2. Dopo aver salvato le configurazioni dello switch TACACS+, verificare la configurazione di TACACS+ utilizzando il comando show run aaa.

C9200L-48P#show run aaa

!

autenticazione aaa gruppo predefinito isegroup locale

iegroup gruppo predefinito esecuzione autorizzazione aaa

gruppo isegroup elenco1 di reti di autorizzazione aaa

username admin password 0 XXXXX

!

!

tacacs server ise1

address ipv4 <indirizzo IP del server TACACS>

chiave XXXXX

!

!

gruppo server aaa tacacs+ isegroup

nome server ise1

!

!

!

aaa new-model

id sessione aaa comune

!

!

Verifica

Verifica dal router

Dalla CLI del router, verificare l'autenticazione di TACACS+ sull'interfaccia ISE con Gigabit Ethernet 1 usando il comando test aaa group tacacsgroupname username password new.

Di seguito è riportato un esempio di output per Router e ISE:

Verifica della porta 49 dal router:

ASR 1001-X#telnet ISE Gig 1 interface IP 49

Sto provando ad ISE GIg 1 interface IP, 49... Open (Aperto)

ASR1001-X#test aaa group isegroup router XXXX nuovo

Password di invio

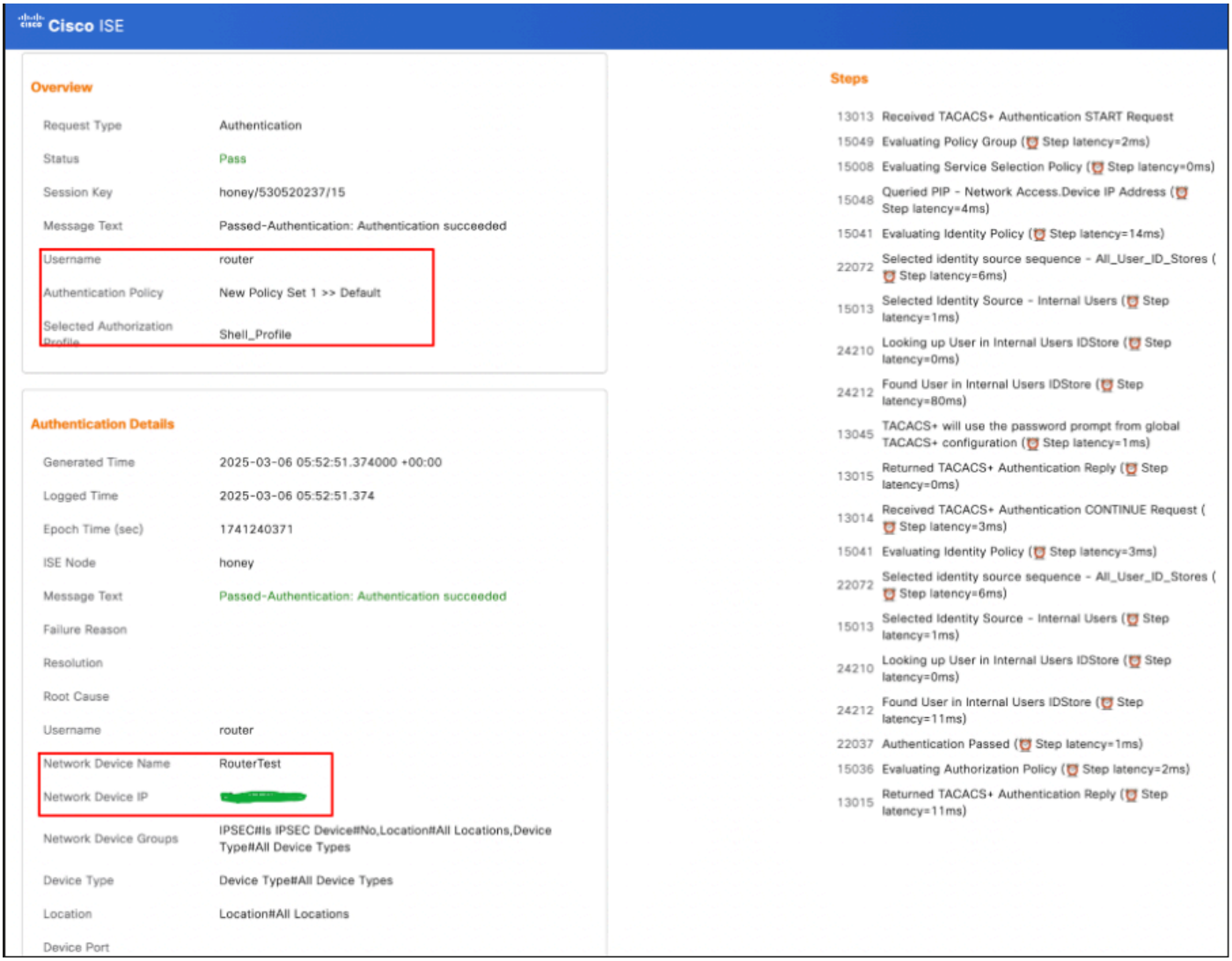
Autenticazione utente completata

ATTRIBUTI UTENTE

username 0 "router"

reply-message 0 "Password:"

Per la verifica da ISE, accedere alla GUI -> Operations -> TACACS live logs, quindi filtrare con il router IP nel campo Network Device Details (Dettagli dispositivo di rete).



Registri TACACS live da ISE - Verifica router.

Verifica dello switch

Dalla CLI dello switch, verificare l'autenticazione di TACACS+ con ISE sull'interfaccia Gigabit Ethernet 1 usando il comando test aaa group tacacsgroupname username password newn:

Di seguito vengono riportati alcuni esempi di output da switch e ISE.

Verifica della porta 49 dallo switch:

C9200L-48P# telnet ISE Gig1 interface IP 49

Sto provando ad ISE Gig1 interface IP, 49... Open (Aperto)

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

Password di invio

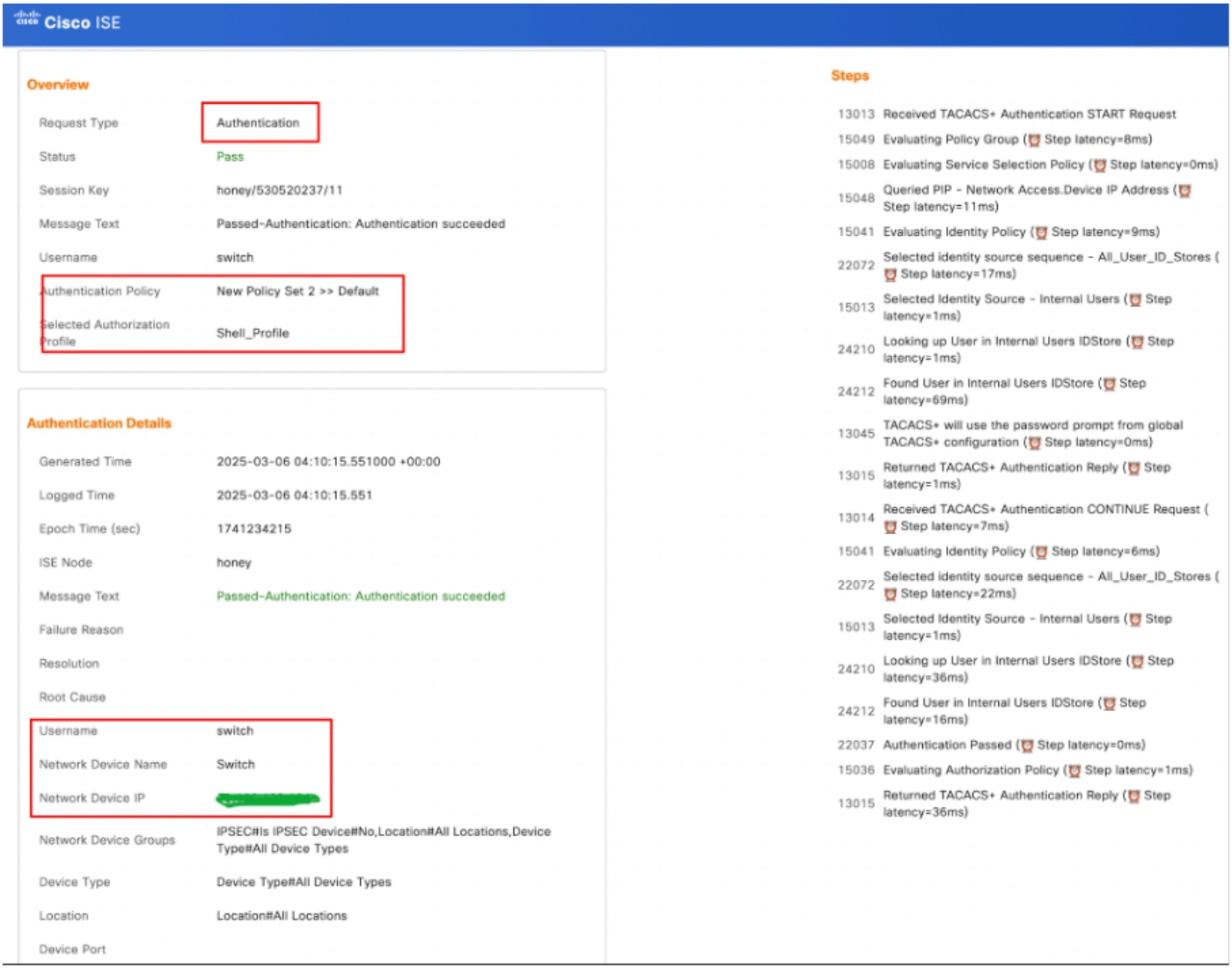
Autenticazione utente completata

ATTRIBUTI UTENTE

username 0 "switch"

reply-message 0 "Password:"

Per la verifica da ISE, accedere alla GUI -> Operations -> TACACS live logs, quindi filtrare con lo switch IP nel campo Network Device Details (Dettagli dispositivo di rete).



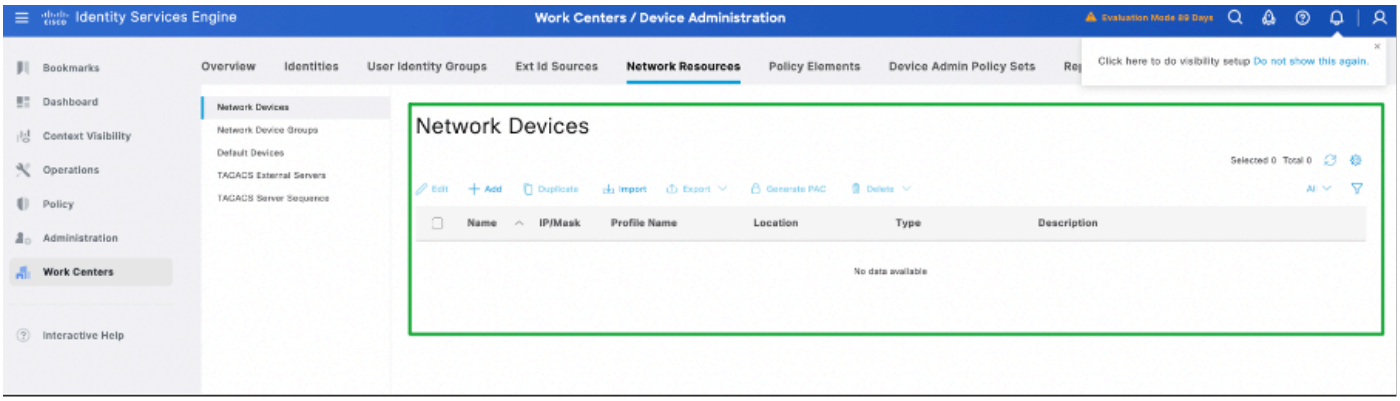
Registri TACACS live da ISE - Verifica switch.

Risoluzione dei problemi

In questa sezione vengono illustrati alcuni dei problemi più comuni riscontrati relativi alle autenticazioni TACACS+.

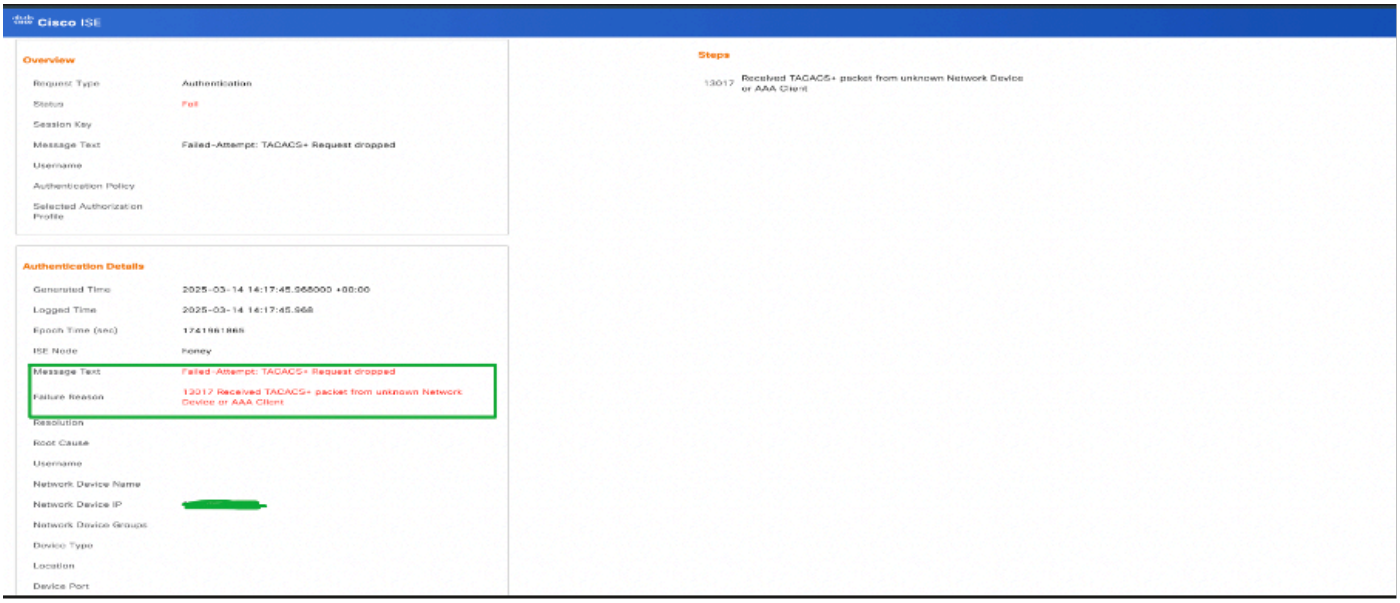
Scenario 1: L'autenticazione TACACS+ non riesce e viene restituito il messaggio di errore "Errore: 13017 Received TACACS+ packet from known Network Device or AAA Client" (Ricevuto pacchetto TACACS+ da dispositivo di rete o client AAA sconosciuto).

Questo scenario si verifica quando il dispositivo di rete non viene aggiunto come Risorse di rete in ISE. Come mostrato in questa schermata, lo switch non viene aggiunto nelle risorse di rete di ISE.



Scenario di risoluzione dei problemi - I dispositivi di rete non vengono aggiunti in ISE.

Ora, quando si testa l'autenticazione dallo switch o dal dispositivo di rete, il pacchetto raggiunge l'ISE come previsto. Tuttavia, l'autenticazione non riesce e viene visualizzato l'errore "Errore: 13017 Received TACACS+ packet from known Network Device or AAA Client" (Ricevuto pacchetto TACACS+ da dispositivo di rete o client AAA sconosciuto), come mostrato in questa schermata:



TACACS live logs: errore quando il dispositivo di rete non viene aggiunto all'ISE.

Verifica dal dispositivo di rete (switch)

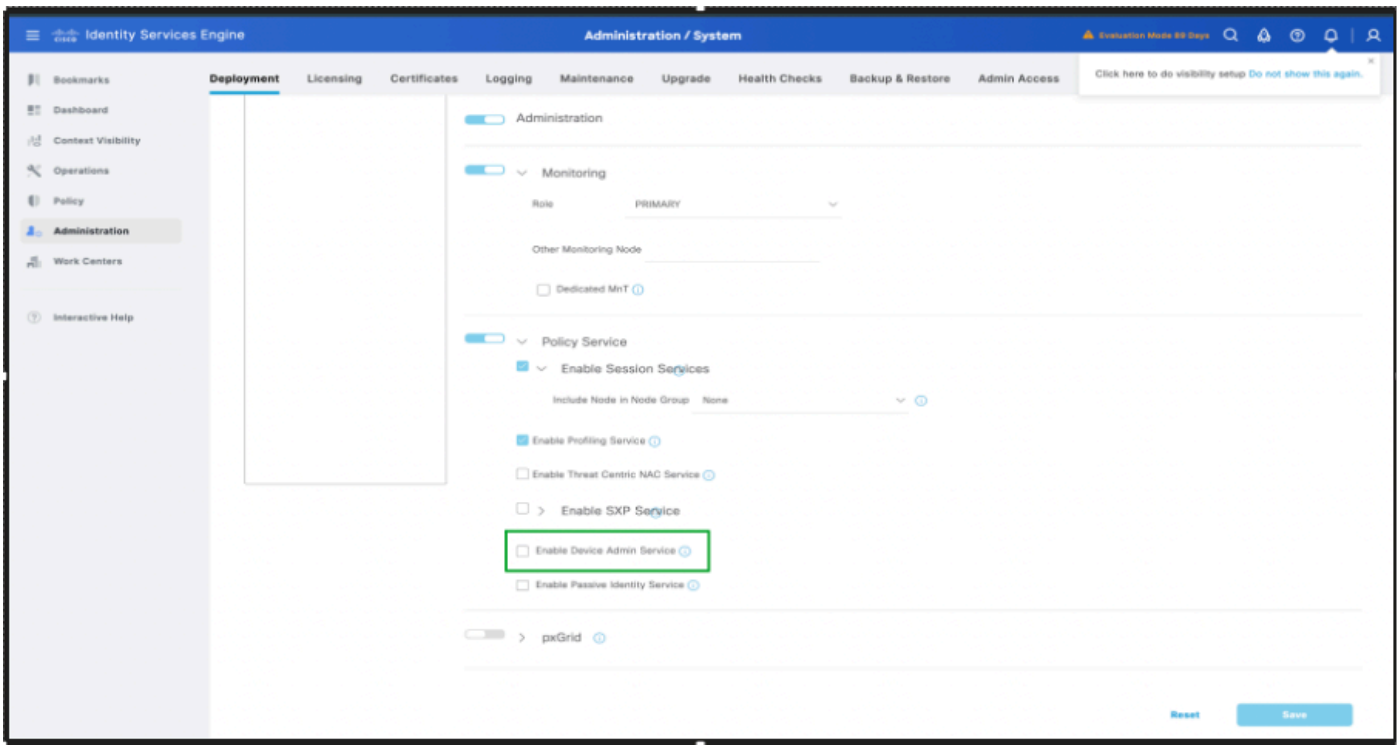
Switch#test aaa gruppo isegroup switch XXXXXX nuovo
Utente rifiutato

Soluzione: Verificare che lo switch, il router o il dispositivo di rete sia stato aggiunto come dispositivo di rete in ISE. Se la periferica non viene aggiunta, aggiungerla all'elenco delle periferiche di rete dell'ISE.

Scenario 2: ISE scarta il pacchetto TACACS+ in modo silenzioso senza alcuna informazione.

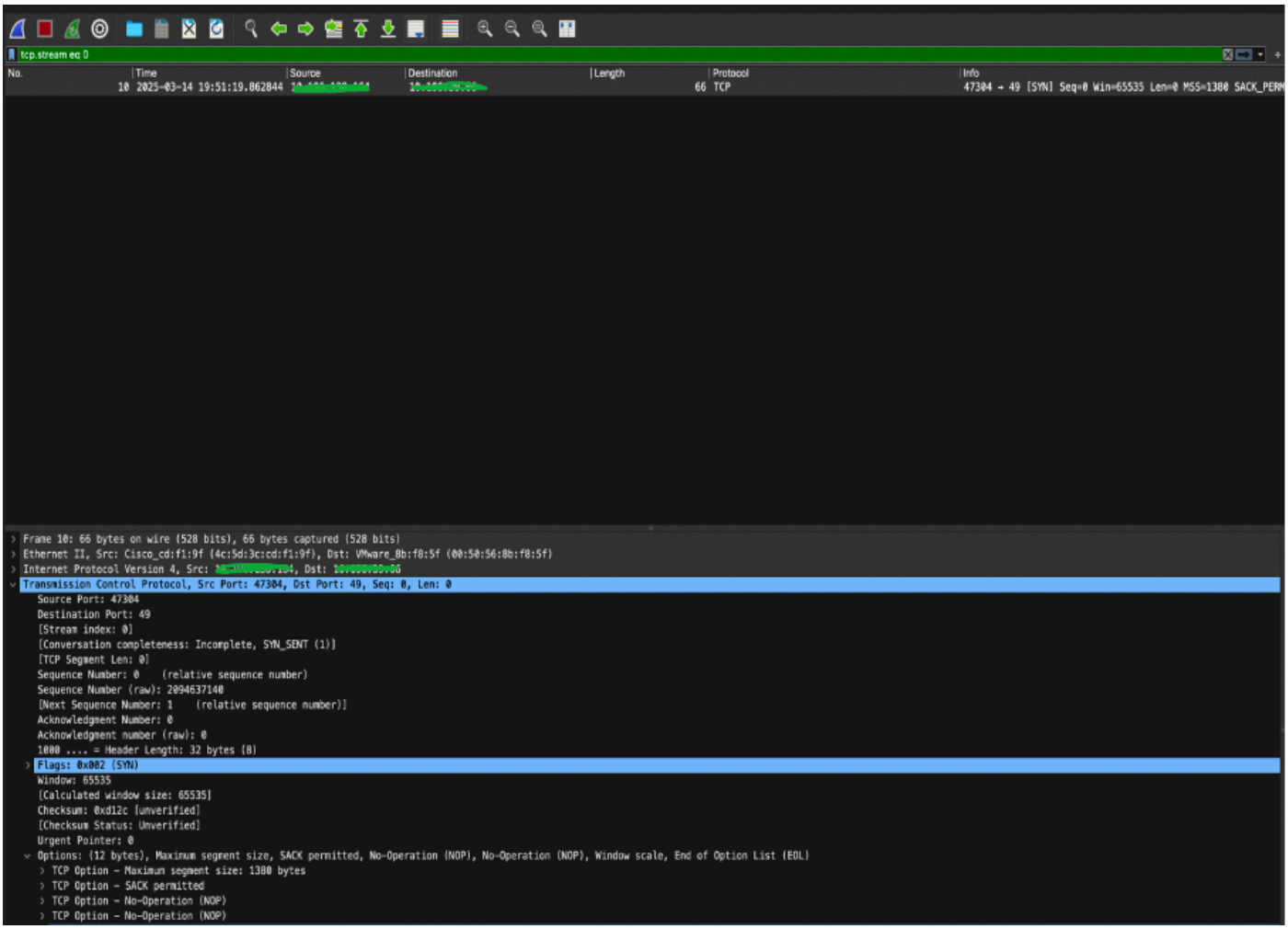
Questo scenario si verifica quando Device Administration Service viene disabilitato in ISE. In questo scenario, ISE scarta il pacchetto e non viene visualizzato alcun log live anche se l'autenticazione viene avviata dal dispositivo di rete che viene aggiunto alle Risorse di rete di ISE.

Come mostrato in questa schermata, Device Administration è disabilitato in ISE.



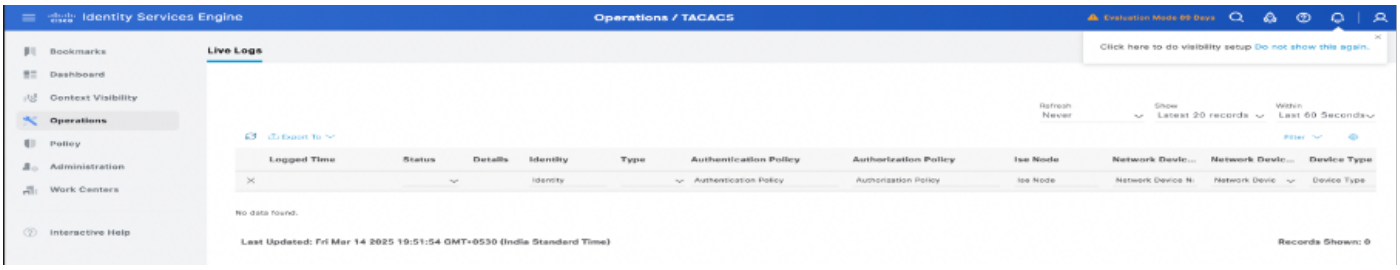
Scenario, l'amministrazione del dispositivo non è abilitata in ISE.

Quando un utente avvia l'autenticazione dal dispositivo di rete, ISE scarta automaticamente i pacchetti senza alcuna informazione nei log attivi e non risponde al pacchetto Syn inviato dal dispositivo di rete per completare il processo di autenticazione TACACS. Fare riferimento a questa schermata:



ISE - perdita di pacchetti in modo silenzioso durante TACACS

ISE: non visualizza alcun log live durante l'autenticazione.



Nessun log live TACACS - Verifica da ISE

Verifica dal dispositivo di rete (switch)

N. switch
Switch#test aaa gruppo isegroup switch XXXX nuovo
Utente rifiutato
N. switch
*14 mar 13:54:28.144: T+: Versione 192 (0xC0), tipo 1, sequenza 1, crittografia 1, SC 0
*14 mar 13:54:28.144: T+: session_id 10158877 (0x9B031D), dlen 14 (0xE)
*14 mar 13:54:28.144: T+: type:AUTHEN/START, priv_lvl:15, azione:LOGIN ascii
*14 mar 13:54:28.144: T+: svc:LOGIN user_len:6 port_len:0 (0x0) raddr_len:0 (0x0) data_len:0
*14 mar 13:54:28.144: T+: utente: switch
*14 mar 13:54:28.144: T+: port:
*14 mar 13:54:28.144: T+: indirizzo_rim:
*14 mar 13:54:28.144: T+: dati:
*14 mar 13:54:28.144: T+: Fine pacchetto

Soluzione: Abilitare l'amministrazione dei dispositivi in ISE.

Riferimento

- Risoluzione dei problemi di autenticazione TAC
- Guida dell'amministratore di Cisco Identity Services Engine, versione 3.3
- VRF per server TACACS

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).