

Configurazione del ruolo TACACS personalizzato per Nexus 9K con ISE 3.2

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Passaggio 1: configurare Nexus 9000](#)

[Passaggio 2. Configura Identity Service Engine 3.2](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

Questo documento descrive come configurare un ruolo Nexus personalizzato per TACACS tramite CLI su NK9.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- TACACS+
- ISE 3.2

Componenti usati

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

- Cisco Nexus 9000, file di immagine NXOS: bootflash:///nxos.9.3.5.bin
- Identity Service Engine versione 3.2

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.

Premesse

Requisiti per le licenze:

Cisco NX-OS - TACACS+ non richiede licenza.

Cisco Identity Service Engine - Per le nuove installazioni ISE, si ha una licenza con un periodo di valutazione di 90 giorni che ha accesso a tutte le funzionalità ISE, se non si dispone di una licenza di valutazione, per usare la funzione ISE TACACS è necessaria una licenza Device Admin per il Policy Server Node che esegue l'autenticazione.

Dopo l'autenticazione dell'utente Admin/Help Desk sul dispositivo Nexus, ISE restituisce il ruolo della shell Nexus desiderato.

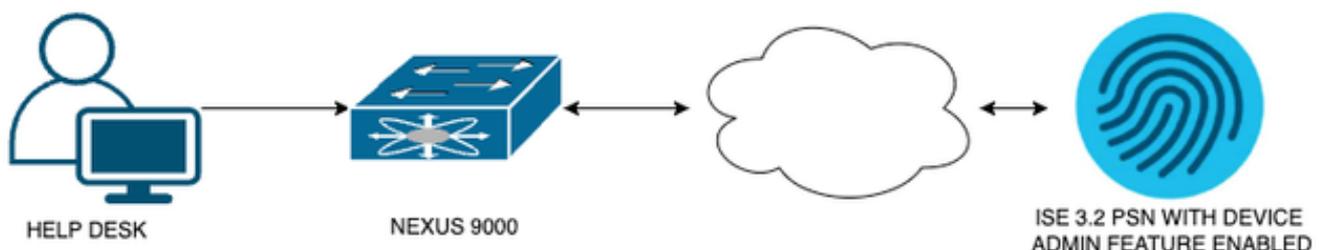
L'utente assegnato con questo ruolo può eseguire la risoluzione dei problemi di base e riavviare alcune porte.

La sessione TACACS che ottiene il ruolo Nexus deve essere in grado di utilizzare ed eseguire solo i comandi e le azioni seguenti:

- Accesso per configurare il terminale in modo che esegua SOLO le interfacce chiusa e non chiusa da 1/1-1/21 e 1/25-1/30
- SSH
- SSH6
- telnet
- Telnet 6
- Traceroute
- Traceroute6
- Ping
- Ping6
- Abilita

Configurazione

Esempio di rete



Passaggio 1: configurare Nexus 9000

1. Configurazione AAA.



Avviso: dopo aver abilitato l'autenticazione TACACS, il dispositivo Nexus cessa di utilizzare l'autenticazione locale e inizia a utilizzare l'autenticazione basata sul server AAA.

```
Nexus9000(config)# feature tacacs+
Nexus9000(config)# tacacs-server host <Your ISE IP> key 0 Nexus3xample
Nexus9000(config)# tacacs-server key 0 "Nexus3xample"
Nexus9000(config)# aaa group server tacacs+ IsePsnServers
Nexus9000(config-tacacs+)# server <Your ISE IP>
Nexus9000(config)# aaa authentication login default group IsePsnServers local
```

2. Configurare il ruolo personalizzato con i requisiti specificati.

```
Nexus9000(config)# role name helpdesk
Nexus9000(config-role)# description Can perform basic Troubleshooting and bounce certain ports
Nexus9000(config-role)# rule 1 permit read
Nexus9000(config-role)# rule 2 permit command enable *
Nexus9000(config-role)# rule 3 permit command ssh *
Nexus9000(config-role)# rule 4 permit command ssh6 *
Nexus9000(config-role)# rule 5 permit command ping *
Nexus9000(config-role)# rule 6 permit command ping6 *
Nexus9000(config-role)# rule 7 permit command telnet *
Nexus9000(config-role)# rule 8 permit command traceroute *
Nexus9000(config-role)# rule 9 permit command traceroute6 *
Nexus9000(config-role)# rule 10 permit command telnet6 *
Nexus9000(config-role)# rule 11 permit command config t ; interface * ; shutdown
Nexus9000(config-role)# rule 12 permit command config t ; interface * ; no shutdown
```

```
vlan policy deny
interface policy deny
```

```
Nexus9000(config-role-interface)# permit interface Ethernet1/1
Nexus9000(config-role-interface)# permit interface Ethernet1/2
Nexus9000(config-role-interface)# permit interface Ethernet1/3
Nexus9000(config-role-interface)# permit interface Ethernet1/4
Nexus9000(config-role-interface)# permit interface Ethernet1/5
Nexus9000(config-role-interface)# permit interface Ethernet1/6
Nexus9000(config-role-interface)# permit interface Ethernet1/7
Nexus9000(config-role-interface)# permit interface Ethernet1/8
Nexus9000(config-role-interface)# permit interface Ethernet1/8
Nexus9000(config-role-interface)# permit interface Ethernet1/9
Nexus9000(config-role-interface)# permit interface Ethernet1/10
Nexus9000(config-role-interface)# permit interface Ethernet1/11
Nexus9000(config-role-interface)# permit interface Ethernet1/12
Nexus9000(config-role-interface)# permit interface Ethernet1/13
Nexus9000(config-role-interface)# permit interface Ethernet1/14
Nexus9000(config-role-interface)# permit interface Ethernet1/15
Nexus9000(config-role-interface)# permit interface Ethernet1/16
Nexus9000(config-role-interface)# permit interface Ethernet1/17
Nexus9000(config-role-interface)# permit interface Ethernet1/18
Nexus9000(config-role-interface)# permit interface Ethernet1/19
Nexus9000(config-role-interface)# permit interface Ethernet1/20
Nexus9000(config-role-interface)# permit interface Ethernet1/21
Nexus9000(config-role-interface)# permit interface Ethernet1/22
Nexus9000(config-role-interface)# permit interface Ethernet1/25
Nexus9000(config-role-interface)# permit interface Ethernet1/26
Nexus9000(config-role-interface)# permit interface Ethernet1/27
Nexus9000(config-role-interface)# permit interface Ethernet1/28
Nexus9000(config-role-interface)# permit interface Ethernet1/29
Nexus9000(config-role-interface)# permit interface Ethernet1/30
```

```
Nexus9000# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
```

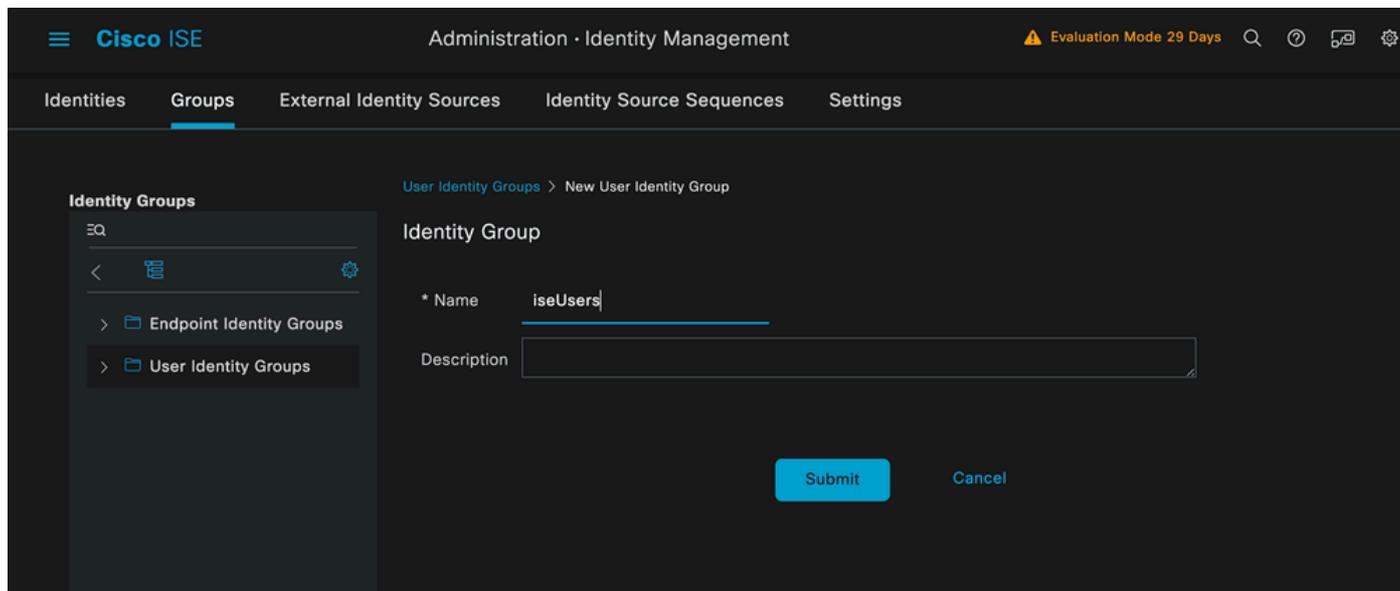
Copy complete.

Passaggio 2. Configura Identity Service Engine 3.2

1. Configurare l'identità utilizzata durante la sessione TACACS di Nexus.

Viene utilizzata l'autenticazione ISE locale.

Passare alla scheda Amministrazione > Gestione delle identità > Gruppi e creare il gruppo di cui l'utente deve far parte. Il gruppo di identità creato per questa dimostrazione è iseUsers.

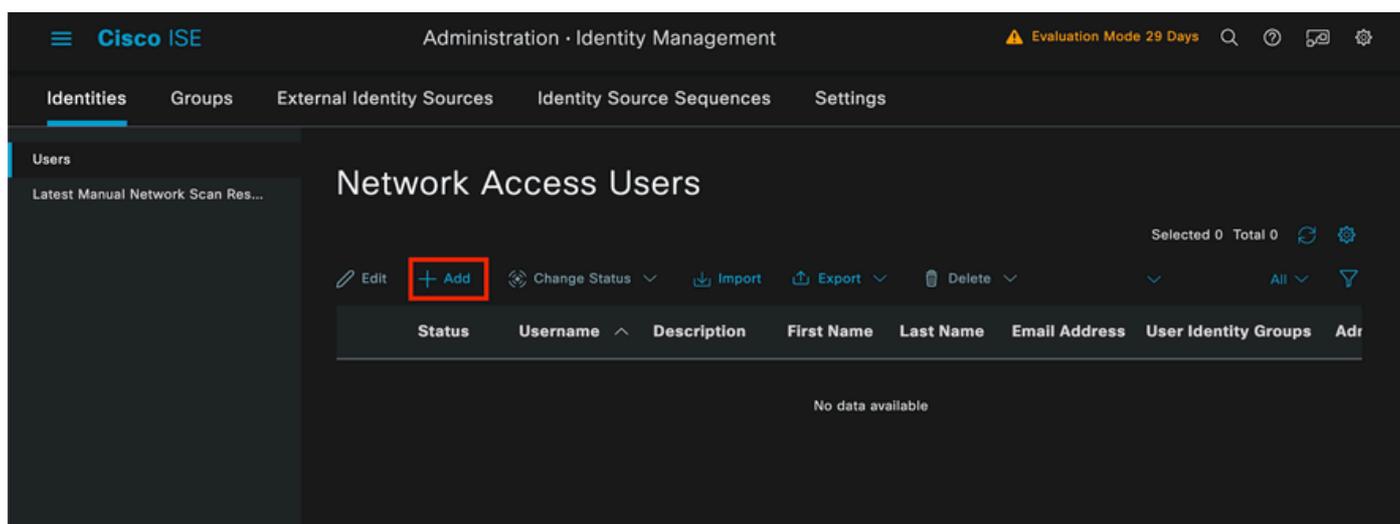


Creazione di un gruppo di utenti

Fare clic sul pulsante Invia.

Passare quindi a Amministrazione > Gestione delle identità > scheda Identità.

Premere il pulsante Add.



Creazione utente

Nei campi obbligatori, a partire dal nome dell'utente, nell'esempio viene utilizzato il nome utente iseischool.

Network Access User

* Username

Status Enabled

Account Name Alias

Email

Denominazione dell'utente e creazione

Il passo successivo è quello di assegnare una password al nome utente creato, VainillaISE97 è la password utilizzata in questa dimostrazione.

Passwords

Password Type:

Password Lifetime:

- With Expiration
Password will expire in 60 days
- Never Expires

Password

Re-Enter Password

* Login Password

Generate Password ⓘ

Enable Password

Generate Password ⓘ

Assegnazione password

Infine, assegnare l'utente al gruppo creato in precedenza, in questo caso iseUsers.

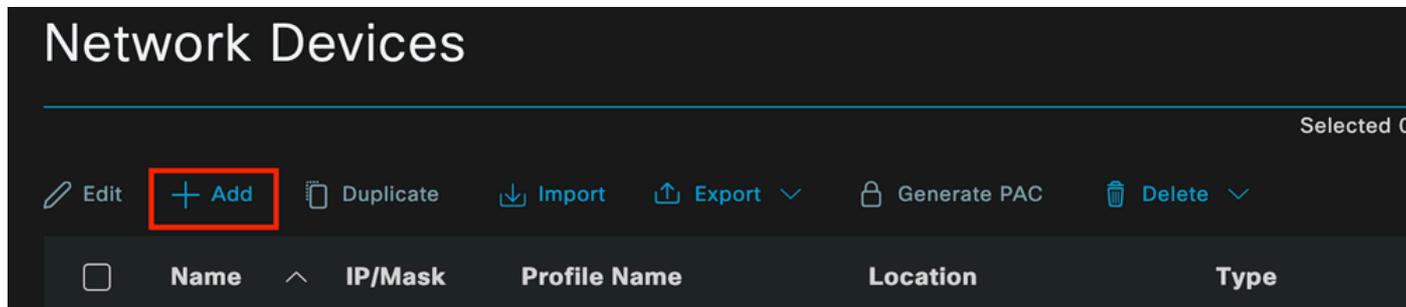
User Groups

Assegnazione gruppo

2. Configurare e aggiungere il dispositivo di rete.

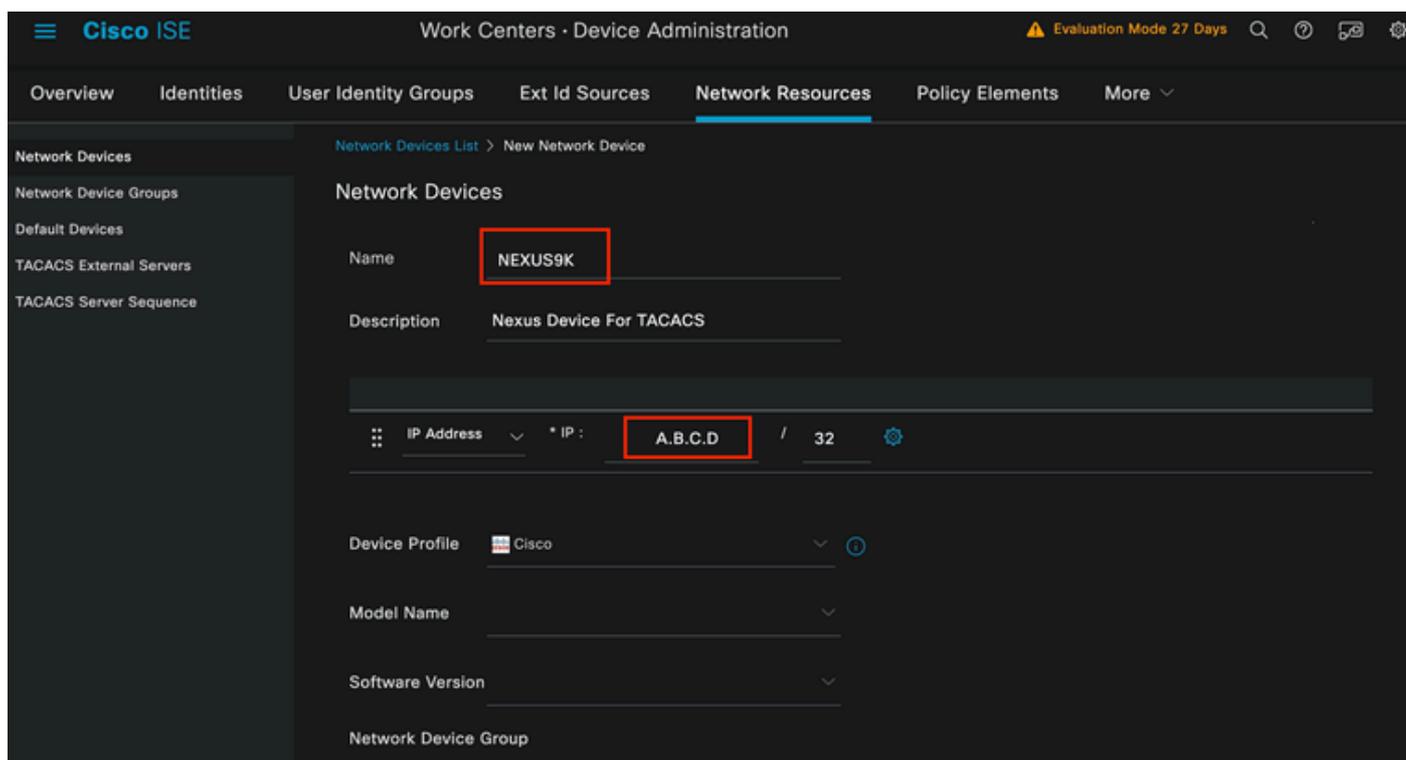
Aggiungere il dispositivo NEXUS 9000 ad ISE Administration > Network Resources > Network Devices

Per iniziare, fare clic sul pulsante Add (Aggiungi).



Pagina Dispositivo di accesso alla rete

Immettere i valori nel modulo, assegnare un nome al NAD che si sta creando e un indirizzo IP da cui il NAD contatta ISE per la conversazione TACACS.



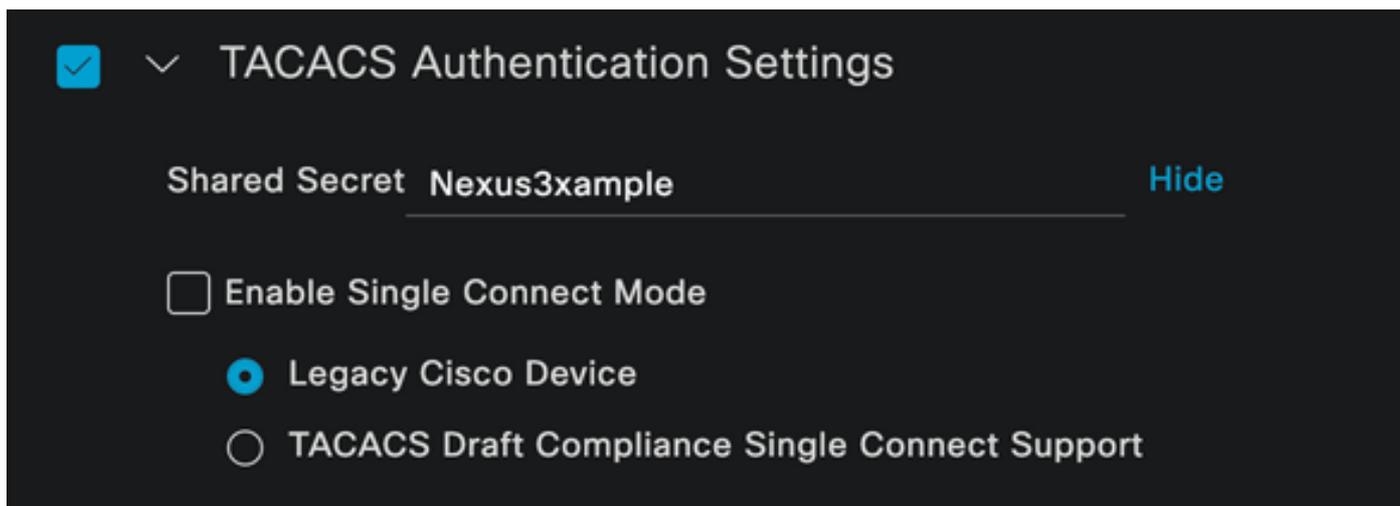
Configura dispositivo di rete

Le opzioni dell'elenco a discesa possono essere lasciate in bianco e possono essere omesse. Tali opzioni consentono di classificare i NAD in base alla posizione, al tipo di dispositivo, alla versione e quindi di modificare il flusso di autenticazione in base a questi filtri.

In Amministrazione > Risorse di rete > Dispositivi di rete > Utente e > Impostazioni di autenticazione TACACS.

Aggiungere il segreto condiviso utilizzato nella configurazione NAD per questa dimostrazione. In

questa dimostrazione viene utilizzato Nexus3xample.



Sezione di configurazione TACACS

Salvare le modifiche facendo clic sul pulsante Invia.

3. Configurazione TACACS su ISE.

Verificare che nel PSN configurato in Nexus 9k sia abilitata l'opzione Device Admin.



Nota: l'abilitazione del servizio Device Admin NON determina il riavvio di ISE.



Enable Device Admin Service



Controllo funzionalità PSN Device Admin

È possibile selezionare nel menu ISE Amministrazione > Sistema > Distribuzione > PSN > Sezione Policy Server > Abilita servizi di amministrazione dispositivi.

- Creare un profilo TACACS che restituisca l'helpdesk del ruolo al dispositivo Nexus se l'autenticazione ha esito positivo.

Dal menu ISE, selezionare Workcenter > Device Administration > Policy Elements > Results >

TACACS Profiles e fare clic sul pulsante Add.

The screenshot shows the Cisco ISE interface for TACACS Profiles. The breadcrumb trail is "TACACS Profiles > New". The page title is "TACACS Profile". The "Name" field contains "Nexus Helpdesk". The "Description" field contains "This TACACS profile will be sent if the user is part of the helpdesk team group". The "Add" button is highlighted with a red box.

Profilo TACACS

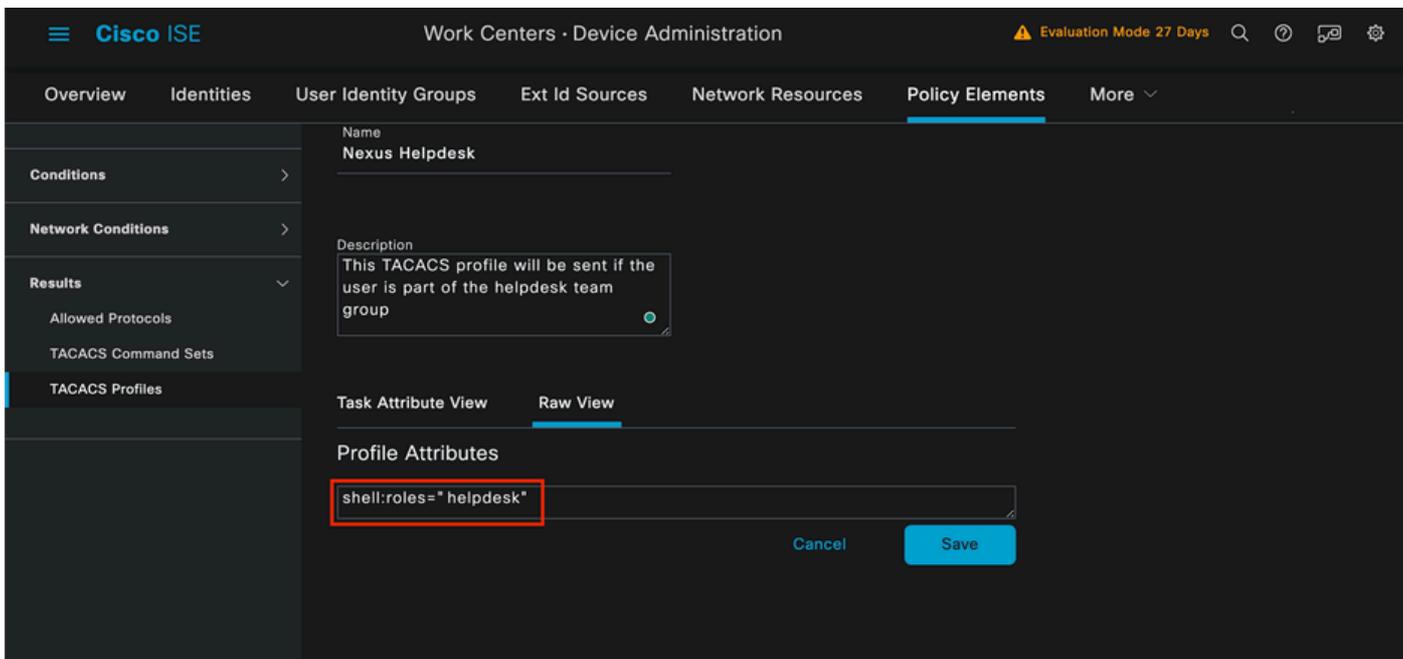
Assegnare un nome e facoltativamente una descrizione.

The screenshot shows the Cisco ISE interface for TACACS Profile configuration. The breadcrumb trail is "TACACS Profiles > New". The page title is "TACACS Profile". The "Name" field contains "Nexus Helpdesk". The "Description" field contains "This TACACS profile will be sent if the user is part of the helpdesk team group".

Denominazione profilo TACACS

Ignorare la sezione Visualizzazione attributi task e passare alla sezione Visualizzazione non elaborata.

E immettere il valore shell:roles="helpdesk".



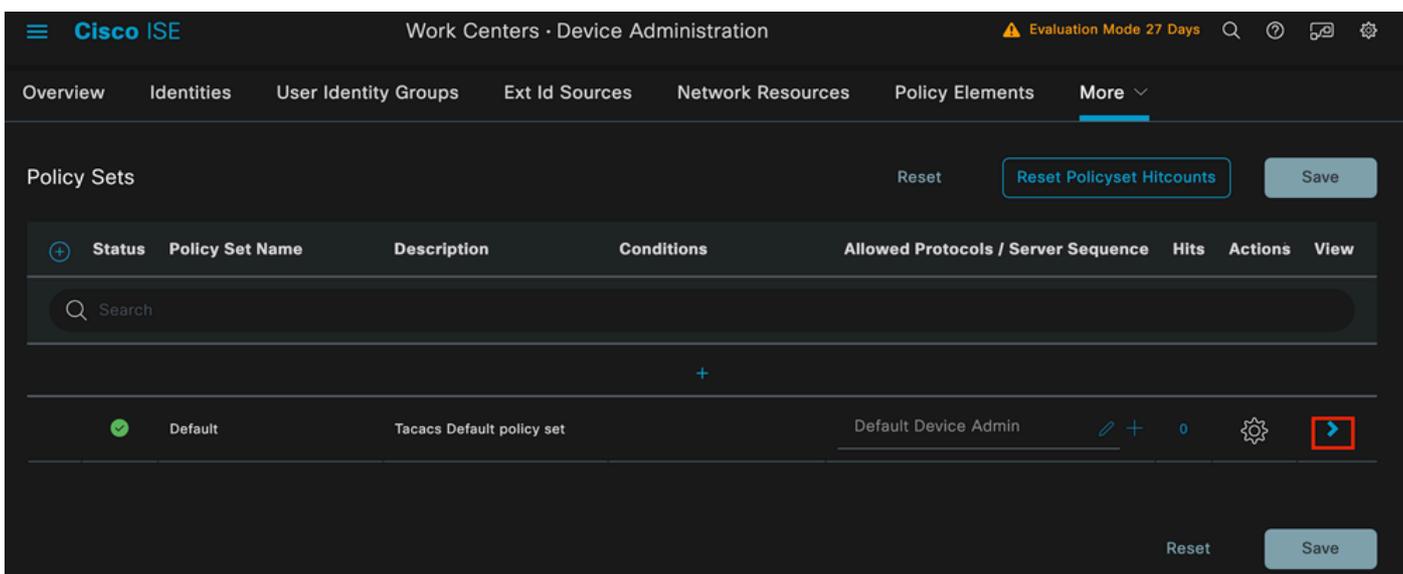
Aggiunta dell'attributo del profilo

Configurare il set di criteri che include il criterio di autenticazione e il criterio di autorizzazione.

Dal menu ISE accedere a Centri di lavoro > Amministrazione dispositivi > Set di criteri di amministrazione dispositivi.

A scopo dimostrativo, viene utilizzato il set di criteri predefinito. È tuttavia possibile creare un altro set di criteri, con condizioni che soddisfino scenari specifici.

Fare clic sulla freccia alla fine della riga.



Pagina Set di criteri di amministrazione del dispositivo

All'interno della configurazione del set di criteri, scorrere verso il basso ed espandere la sezione Criteri di autenticazione.

Fare clic sull'icona Aggiungi.

Per questo esempio di configurazione, il valore Name è Internal Authentication e la condizione scelta è Network Device (Nexus) IP (sostituto di A.B.C.D.). I criteri di autenticazione utilizzano l'archivio identità degli utenti interni.

The screenshot shows the Cisco ISE Work Centers - Device Administration interface. The top navigation bar includes 'Overview', 'Identities', 'User Identity Groups', 'Ext Id Sources', 'Network Resources', 'Policy Elements', and 'More'. A search bar is present below the navigation. The main content area displays a table of authentication rules. The 'Internal Authentication' rule is highlighted with a red box. Its condition is 'Network Access-Device IP Address EQUALS A.B.C.D', also highlighted with a red box. To the right, the 'Internal Users' identity source is selected, and its options are visible: 'If Auth fail' (REJECT), 'If User not found' (REJECT), and 'If Process fail' (DROP). The 'Default' rule is also visible at the bottom left.

Criterio di autenticazione

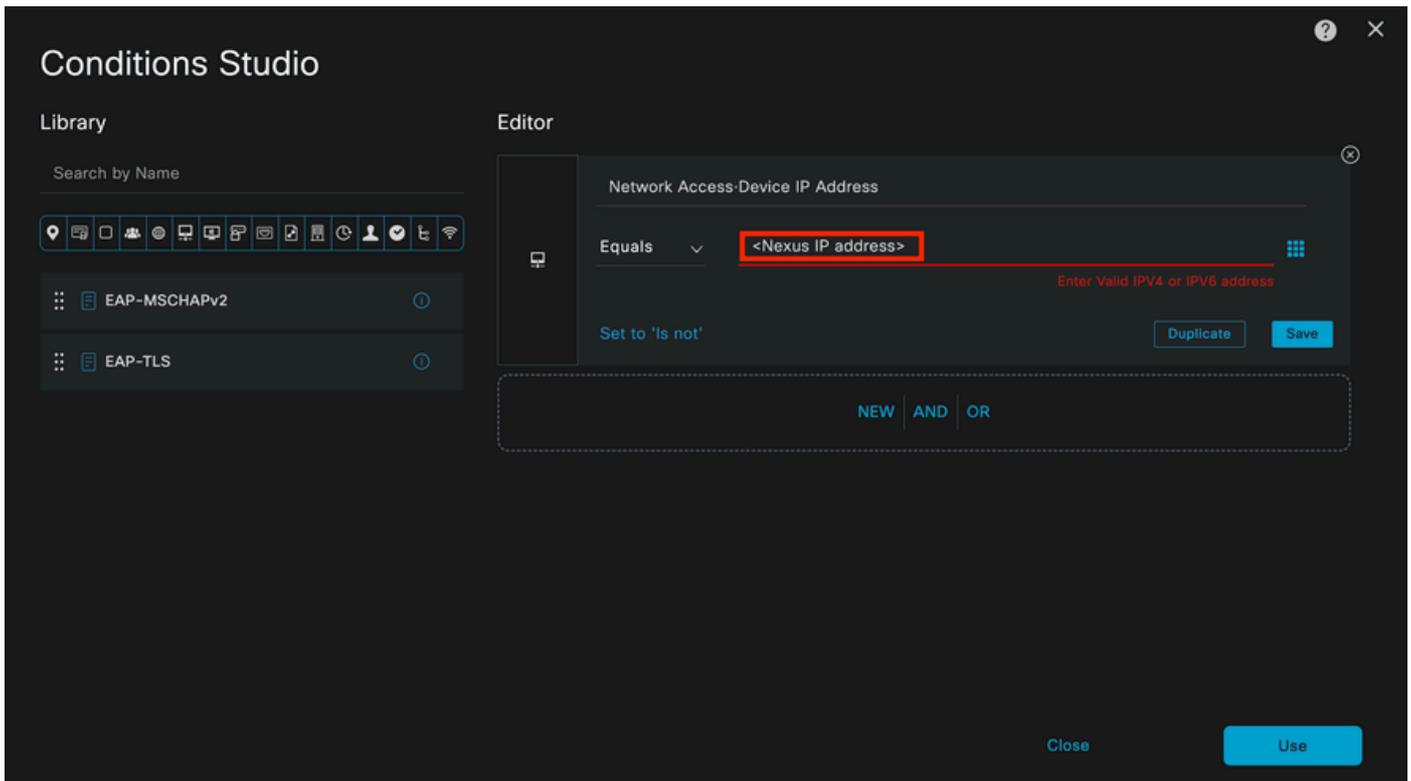
Di seguito viene riportata la configurazione della condizione.

Selezionare Accesso di rete > Attributo dizionario indirizzo IP dispositivo.

The screenshot shows the Conditions Studio interface. The 'Library' pane on the left contains 'EAP-MSCHAPv2' and 'EAP-TLS'. The 'Editor' pane shows the condition 'Network Access-Device IP Address'. A 'Select attribute for condition' dialog is open, displaying a table of attributes. The 'Network Access' dictionary and 'Device IP Address' attribute are highlighted with a red box. The 'Use' button is visible at the bottom right of the dialog.

Dictionary	Attribute	ID	Info
All Dictionaries	Attribute	ID	
DEVICE	Device Type		
DEVICE	Model Name		
DEVICE	Network Device Profile		
DEVICE	Software Version		
Network Access	Device IP Address		
Network Access	NetworkDeviceName		

Sostituire il commento <Nexus IP address> con l'indirizzo IP corretto.



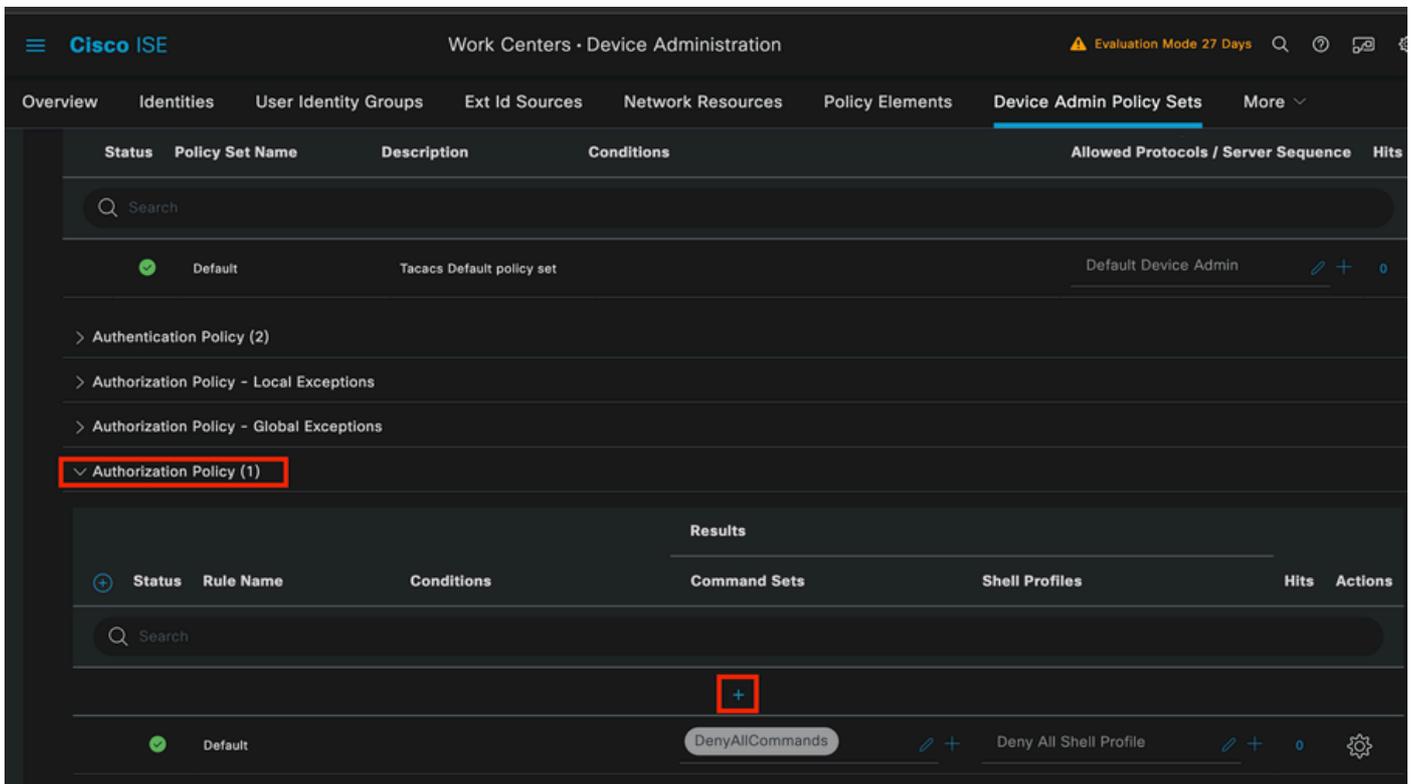
Aggiunta del filtro IP

Fare clic sul pulsante Use (Usa).

Questa condizione viene soddisfatta solo dal dispositivo Nexus configurato. Tuttavia, se lo scopo è abilitare questa condizione per una grande quantità di dispositivi, è necessario considerare una condizione diversa.

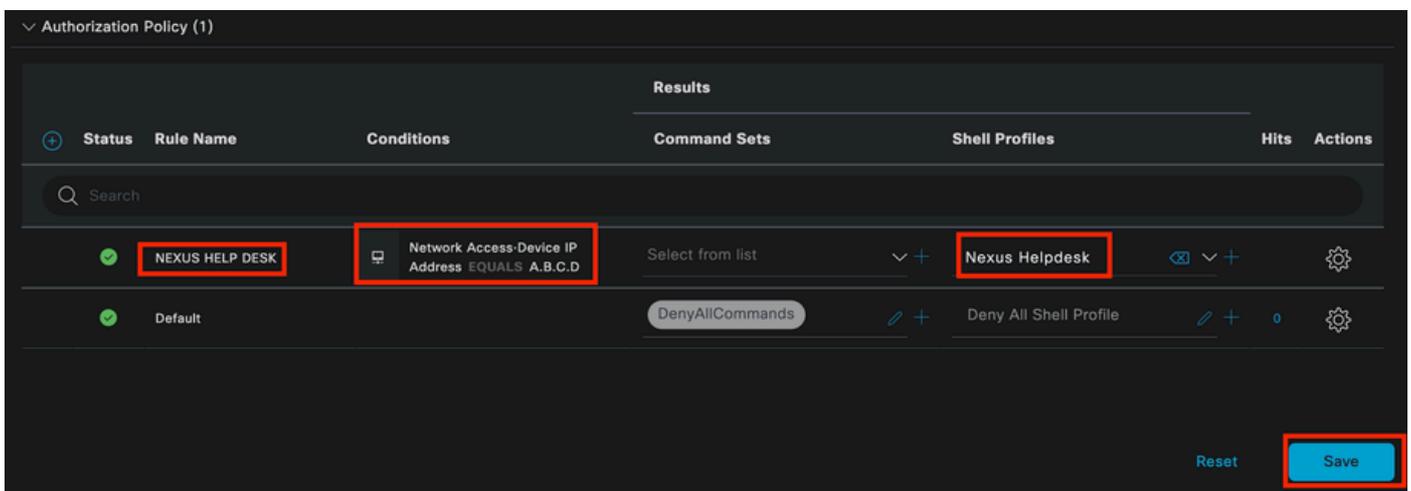
Passare quindi alla sezione Criteri di autorizzazione ed espanderla.

Fare clic sull'icona + (più).



Sezione Criteri di autorizzazione

In questo esempio NEXUS HELP DESK è stato utilizzato come nome del criterio di autorizzazione.



Studio condizioni per i criteri di autorizzazione

La stessa condizione configurata nei criteri di autenticazione viene utilizzata per i criteri di autorizzazione.

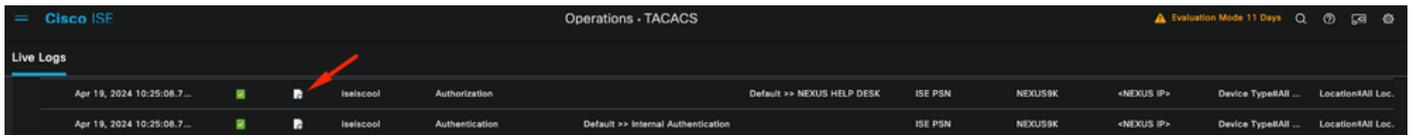
Nella colonna Profili shell, il profilo configurato prima della selezione di Nexus Helpdesk.

Infine, fare clic sul pulsante Salva.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Dalla GUI di ISE, selezionare Operations > TACACS > Live Logs, identificare il record che corrisponde al nome utente usato e fare clic sul log dettagliato dell'evento Authorization.



Log TACACS Live

Tra i dettagli inclusi in questo report, è disponibile la sezione Response, in cui è possibile verificare in che modo ISE ha restituito il valore shell:roles="helpdesk"

Response

```
{Author-Reply-Status=PassRepl;  
AVPair=shell:roles=" helpdesk" ; }
```

Risposta dettagli registro dinamico

Sul dispositivo Nexus:

```
Nexus9000 login: iseiscool  
Password: VainillaISE97
```

```
Nexus9000# conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Nexus9000(config)# interface ethernet 1/23  
% Interface permission denied
```

```
Nexus9000(config)# ?  
  interface  Configure interfaces  
  show      Show running system information  
  end       Go to exec mode  
  exit      Exit from command interpreter
```

```
Nexus9000(config)# role name test  
% Permission denied for the role
```

```
Nexus9000(config)#
```

```
Nexus9000(config)# interface loopback 0  
% Interface permission denied
```

```
Nexus9000(config)#  
Nexus9000# conf t
```

```
Nexus9000(config)# interface ethernet 1/5  
Notice that only the commands allowed are listed.  
Nexus9000(config-if)# ?
```

```
no      Negate a command or set its defaults  
show    Show running system information  
shutdown Enable/disable an interface  
end     Go to exec mode  
exit    Exit from command interpreter
```

```
Nexus9000(config-if)# cdp
Nexus9000(config-if)# cdp enable
% Permission denied for the role
Nexus9000(config-if)#
```

Risoluzione dei problemi

- Verificare che l'ISE sia raggiungibile dal dispositivo Nexus. Nexus9000# ping <Your ISE IP>
PING <IP ISE> (56 byte di dati)
64 byte da <IP ISE> : icmp_seq=0 ttl=59 time=1,22 ms
64 byte da <Your ISE IP> : icmp_seq=1 ttl=59 time=0.739 ms
64 byte da <Your ISE IP> : icmp_seq=2 ttl=59 time=0.686 ms
64 byte da <Your ISE IP> : icmp_seq=3 ttl=59 time=0.71 ms
64 byte da <Your ISE IP> : icmp_seq=4 ttl=59 time=0.72 ms
- Verificare che la porta 49 sia aperta tra ISE e il dispositivo Nexus.
Nexus 9000# telnet <Your ISE IP> 49
Tentativo di esecuzione di <Your ISE IP> in corso...
Connesso a <IP ISE> .
Il carattere di escape è '^'.
- Utilizzare i seguenti debug:

```
debug tacacs+ all
```

```
Nexus 9000#
```

```
Nexus9000# 2024 Apr 19 22:50:44.199329 tacacs: event_loop(): chiamata process_rd_fd_set
2024 Apr 19 22:50:44.19935 tacacs: process_rd_fd_set: richiamata per fd 6
2024 Apr 19 22:50:44.199392 tacacs: fsrv non ha consumato 8421 codice operativo
2024 Apr 19 22:50:44.19406 tacacs: process_implicit_cfs_session_start: immissione...
2024 Apr 19 22:50:44.199414 tacacs: process_implicit_cfs_session_start: uscita in corso. La
distribuzione è disabilitata
2024 Apr 19 22:50:44.199424 tacacs: process_aaa_tplus_request: immissione per id sessione aaa
0
2024 Apr 19 22:50:44.199438 tacacs: process_aaa_tplus_request:Controllo dello stato della porta
mgmt0 con servergroup lsePsnServers
2024 Apr 19 22:50:44.19451 tacacs: tacacs_global_config(4220): immissione...
2024 Apr 19 22:50:44.19466 tacacs: tacacs_global_config(4577): GET_REQ...
2024 Apr 19 22:50:44.208027 tacacs: tacacs_global_config(4701): recuperato il valore restituito
dalla configurazione del protocollo globale operazione:SUCCESS
2024 Apr 19 22:50:44.208045 tacacs: tacacs_global_config(4716): REQ:num server 0
2024 Apr 19 22:50:44.208054 tacacs: tacacs_global_config: REQ:num gruppo 1
2024 Apr 19 22:50:44.208062 tacacs: tacacs_global_config: REQ:num timeout 5
2024 Apr 19 22:50:44.208070 tacacs: tacacs_global_config: REQ:num deadtime 0
2024 Apr 19 22:50:44.208078 tacacs: tacacs_global_config: REQ:num tipo_crittografia 7
2024 Apr 19 22:50:44.208086 tacacs: tacacs_global_config: restituzione 0
2024 Apr 19 22:50:44.208098 tacacs: process_aaa_tplus_request:group_info è popolato in
aaa_req, quindi Using servergroup lsePsnServers
```

2024 Apr 19 22:50:44.208108 tacacs: tacacs_servergroup_config: immissione per il gruppo di server, indice 0

2024 Apr 19 22:50:44.208117 tacacs: tacacs_servergroup_config: GETNEXT_REQ per il gruppo di server di protocollo index:0 nome:

2024 Apr 19 22:50:44.208148 tacacs: tacacs_pss2_move2key: rcode = 40480003 syserr2str = nessuna chiave pss

2024 Apr 19 22:50:44.208160 tacacs: tacacs_pss2_move2key: chiamata pss2_getkey

2024 Apr 19 22:50:44.208171 tacacs: tacacs_servergroup_config: GETNEXT_REQ ha ottenuto il gruppo di server di protocollo indice:2 nome:IsePsnServers

2024 Apr 19 22:50:44.208184 tacacs: tacacs_servergroup_config: recuperato il valore restituito dal gruppo di protocolli operazione:SUCCESS

2024 Apr 19 22:50:44.208194 tacacs: tacacs_servergroup_config: restituzione valore 0 per il gruppo di server di protocollo:IsePsnServers

2024 Apr 19 22:50:44.208210 tacacs: process_aaa_tplus_request: trovato gruppo IsePsnServers. Il valore vrf corrispondente è predefinito, source-intf è 0

2024 Apr 19 22:50:44.208224 tacacs: process_aaa_tplus_request: controllo di mgmt0 vrf:management rispetto a vrf:default del gruppo richiesto

2024 Apr 19 22:50:44.208256 tacacs: process_aaa_tplus_request:mgmt_if 83886080

2024 Apr 19 22:50:44.208272 tacacs: process_aaa_tplus_request:global_src_intf : 0, src_intf locale è 0 e vrf_name è il valore predefinito

2024 Apr 19 22:50:44.208286 tacacs: create_tplus_req_state_machine(902): immissione per id sessione aaa 0

2024 Apr 19 22:50:44.208295 tacacs: conteggio macchina a stati 0

2024 Apr 19 22:50:44.208307 tacacs: init_tplus_req_state_machine: immissione per id sessione aaa 0

2024 Apr 19 22:50:44.208317 tacacs: init_tplus_req_state_machine(1298):tplus_ctx è NULL dovrebbe essere se autore e test

2024 Apr 19 22:50:44.208327 tacacs: tacacs_servergroup_config: immissione per il gruppo di server IsePsnServers, indice 0

2024 Apr 19 22:50:44.208339 tacacs: tacacs_servergroup_config: GET_REQ per il gruppo di server di protocollo indice:0 nome:IsePsnServers

2024 Apr 19 22:50:44.208357 tacacs: find_tacacs_servergroup: immissione per il gruppo di server IsePsnServers

2024 Apr 19 22:50:44.208372 tacacs: tacacs_pss2_move2key: rcode = 0 syserr2str = SUCCESS

2024 Apr 19 22:50:44.208382 tacacs: find_tacacs_servergroup: uscita per il gruppo di server Indice IsePsnServers è 2

2024 Apr 19 22:50:44.208401 tacacs: tacacs_servergroup_config: GET_REQ: errore find_tacacs_servergroup 0 per il gruppo di server di protocollo IsePsnServers

2024 Apr 19 22:50:44.208420 tacacs: tacacs_pss2_move2key: rcode = 0 syserr2str = SUCCESS

2024 Apr 19 22:50:44.20843 tacacs: tacacs_servergroup_config: GET_REQ ha ottenuto il protocollo gruppo di server indice:2 nome:IsePsnServers

2024 A2024 Apr 19 22:52024 Apr 19 22:52024 Apr 19 22:5
Nexus 9000#

- Eseguire un'acquisizione del pacchetto (per visualizzare i dettagli del pacchetto, è necessario modificare le preferenze Wireshark TACACS+ e aggiornare la chiave condivisa

utilizzata da Nexus e ISE)

```
No. | Time | Sc | De | Protocol | Length | Info
---|---|---|---|---|---|---
66 22:25:08.757401 ... .. TACACS+ 107 R: Authorization

> Transmission Control Protocol, Src Port: 49, Dst Port: 58863, Seq: 1, Ack: 90, Len: 41
  TACACS+
    Major version: TACACS+
    Minor version: 0
    Type: Authorization (2)
    Sequence number: 2
    > Flags: 0x00 (Encrypted payload, Multiple Connections)
    Session ID: 1136115821
    Packet length: 29
    Encrypted Reply
    v Decrypted Reply
      Auth Status: PASS_REPL (0x02)
      Server Msg length: 0
      Data length: 0
      Arg count: 1
      Arg[0] length: 22
      Arg[0] value: shell:roles="helpdesk"
```

Pacchetto di autorizzazione TACACS

- Verificare che la chiave condivisa sia la stessa sul lato ISE e Nexus. Questa condizione può essere verificata anche in Wireshark.

TACACS+

```
Major version: TACACS+
Minor version: 1
Type: Authentication (1)
Sequence number: 1
Flags: 0x00 (Encrypted payload, Multiple Connections)
Session ID: 232251350
Packet length: 43
Encrypted Request
Decrypted Request
  Action: Inbound Login (1)
  Privilege Level: 1
  Authentication type: PAP (2)
  Service: Login (1)
  User len: 9
  User: iseiscool
  Port len: 1
  Port: 0
  Remaddr len: 12
  Remote Address: [REDACTED]
  Password Length: 13
  Password: VainillaISE97
```

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).