Configurazione del dominio di autenticazione TACACS+ su UCS Manager con ISE Server

Sommario

Introduzione

In questo documento viene descritta la configurazione dell'autenticazione TACACS+ (Terminal Access Controller Access-Control System Plus) su Unified Compute System Manager (UCSM). TACACS+ è un protocollo di rete utilizzato per i servizi di autenticazione, autorizzazione e responsabilità (AAA) e fornisce un metodo centralizzato per gestire i dispositivi di accesso alla rete (NAD) tramite i quali è possibile amministrare e creare regole tramite un server. In questo scenario di utilizzo viene utilizzato Identity Services Engine (ISE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco UCS Manager (UCSM)
- Access-Control System Plus di Terminal Access Controller (TACACS+)
- Identity Services Engine (ISE)

Componenti usati

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

- UCSM 4.2(3d)
- Cisco Identity Services Engine (ISE) versione 3.2

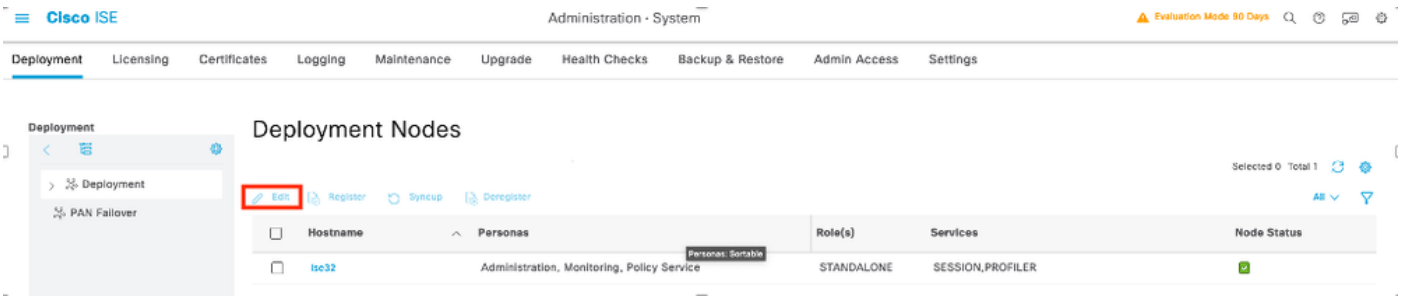
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Configurazione

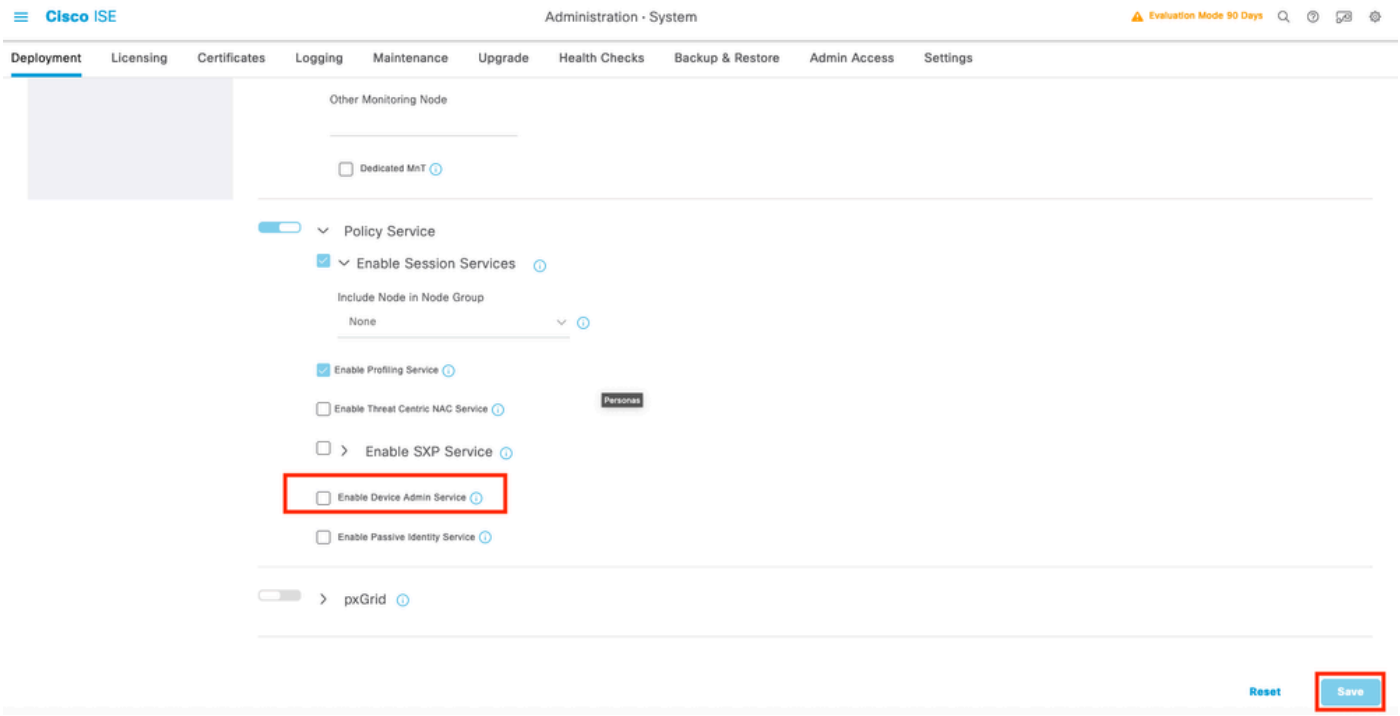
Configurazione TACACS+ su ISE

Configurazione di TACACS+ su ISE

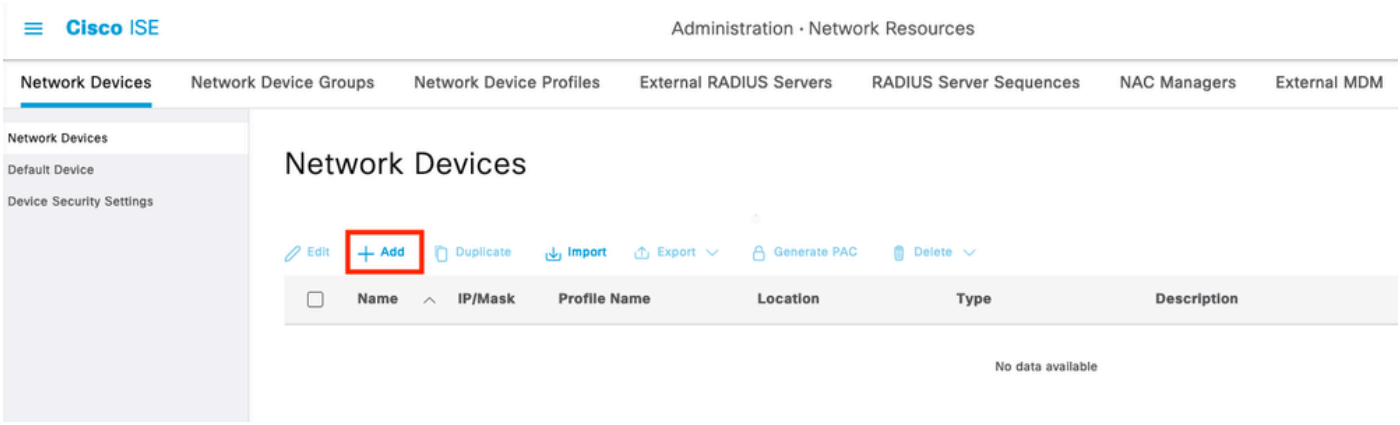
Passaggio 1. La prima attività consiste nel verificare se l'ISE dispone delle funzionalità corrette per gestire le autenticazioni TACACS+. Per questo motivo, è necessario controllare se all'interno del Policy Service Node (PSN) si desidera disporre della funzionalità per il Device Admin Service, cercare nel menu Amministrazione > Sistema > Distribuzione, selezionare il nodo in cui l'ISE esegue TACACS+ e quindi selezionare il pulsante edit.



Passaggio 2. Scorrere verso il basso fino a visualizzare la funzionalità corrispondente denominata Device Administration Service (si noti che per abilitare questa funzionalità è necessario che sul nodo sia abilitata la persona di Policy Server e che nella distribuzione siano disponibili le licenze per TACACS+), selezionare la casella di controllo e salvare la configurazione:

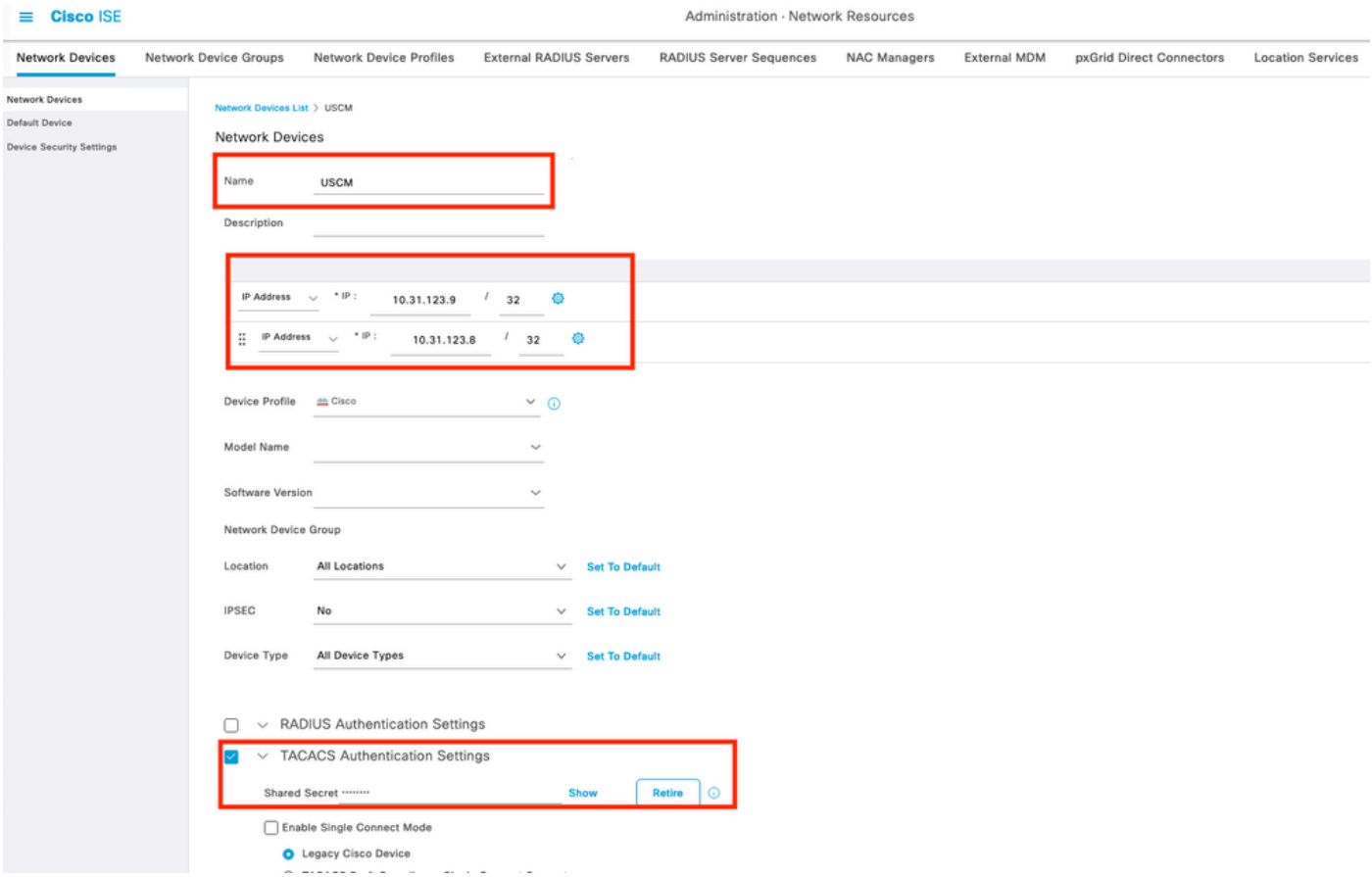


Passaggio 3. Configurare il dispositivo di accesso alla rete (NAD) che usa ISE come TACACS+ come server, selezionare il menu Amministrazione > Risorse di rete > Dispositivi di rete, quindi fare clic sul pulsante +Aggiungi.



Passaggio 4. In questa sezione configurare:

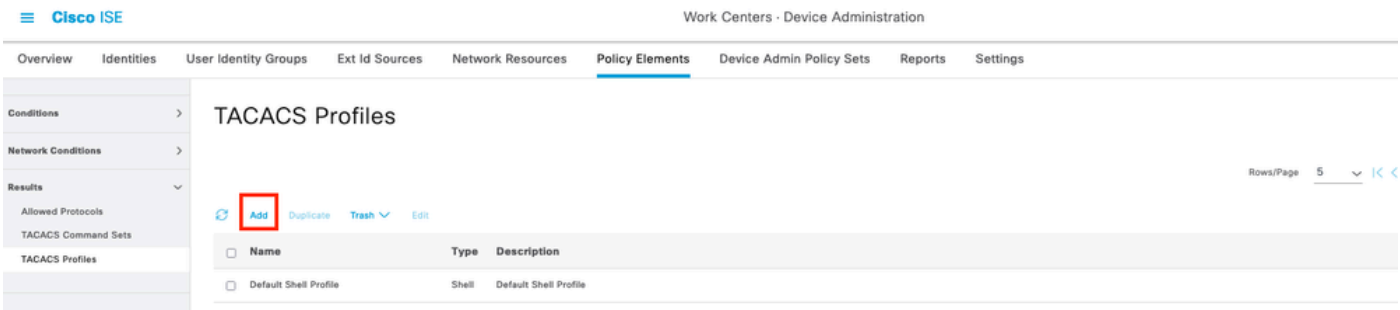
- Un nome che indica che l'UCSM deve essere il client TACACS+.
- Gli indirizzi IP che il modulo UCSM utilizza per inviare la richiesta ad ISE.
- TACACS+ Shared Secret, è la password che deve essere utilizzata per crittografare i pacchetti tra UCSM e ISE



Nota: Per una configurazione cluster, aggiungere gli indirizzi IP della porta di gestione per entrambe le interconnessioni fabric. Questa configurazione garantisce che gli utenti remoti possano continuare ad eseguire l'accesso se la prima interconnessione fabric non riesce e il sistema esegue il failover sulla seconda interconnessione fabric. Tutte le richieste di accesso hanno origine da questi indirizzi IP, non dall'indirizzo IP virtuale utilizzato da Cisco UCS Manager.

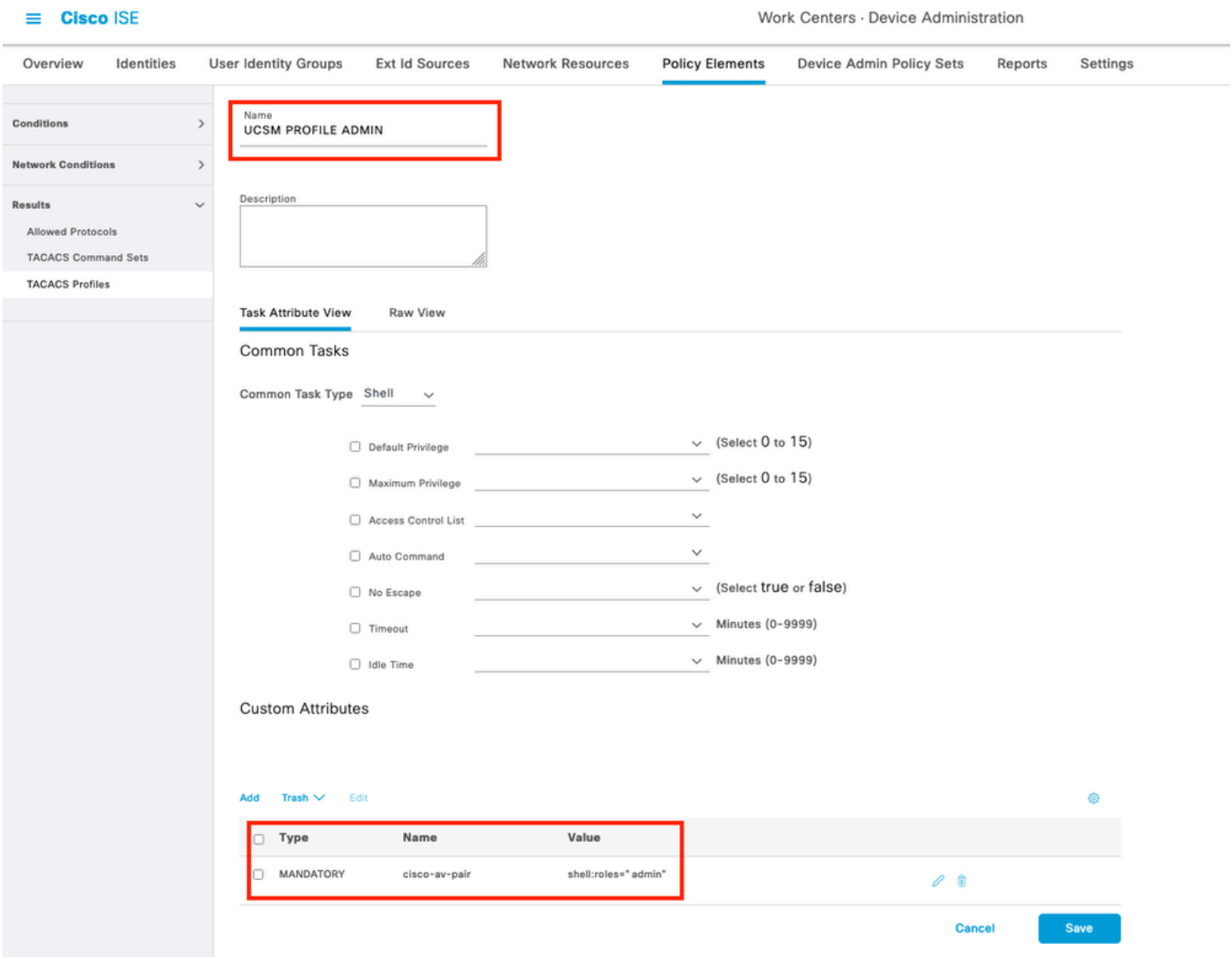
Configurazione di attributi e regole su ISE

Passaggio 1. Creare un profilo TACACS+, selezionare il menu Centri di lavoro > Amministrazione dispositivi > Elementi dei criteri > Risultati > Profili TACACS , quindi selezionare Aggiungi

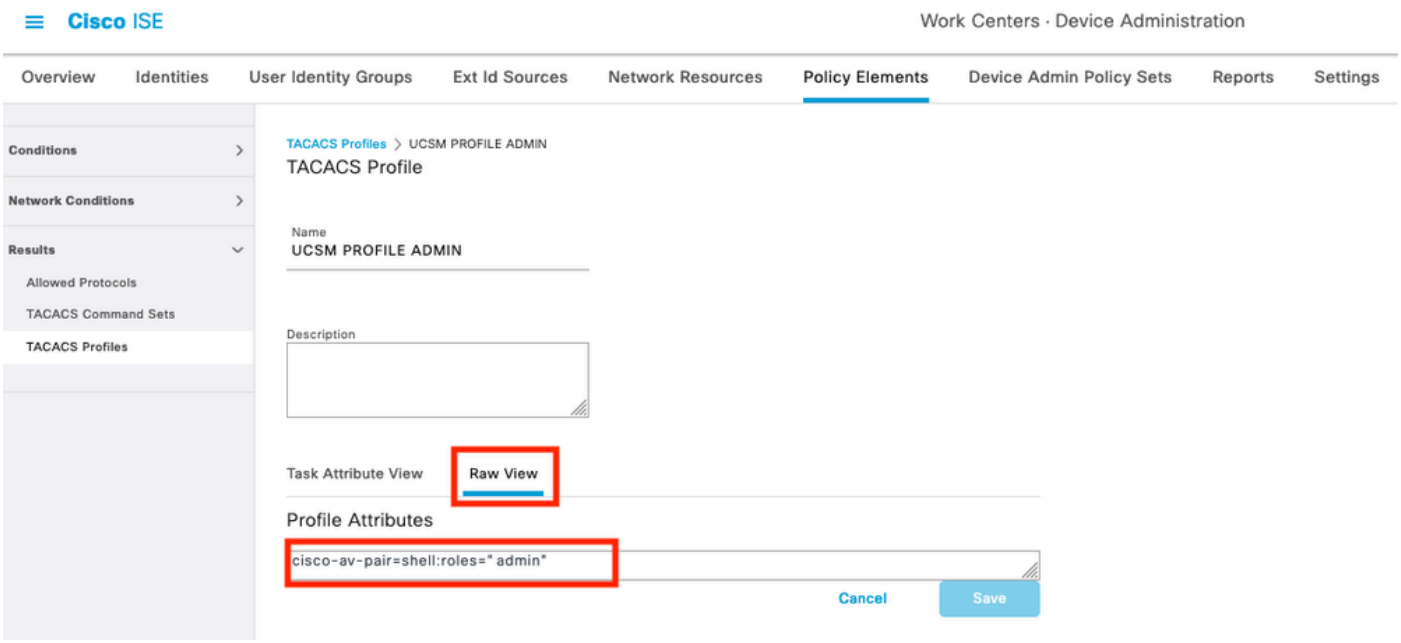


Passaggio 2. In questa sezione configurare il profilo con un nome e nella sezione Attributi personalizzati selezionare Add, quindi creare un attributo di caratteristica MANDATORY,

denominarlo cisco-av-pair e nel valore selezionare uno dei ruoli disponibili all'interno di UCSM e immettere che come ruolo della shell, in questo esempio viene utilizzato il ruolo admin e l'input selezionato deve essere shell:roles="admin" come mostrato di seguito,



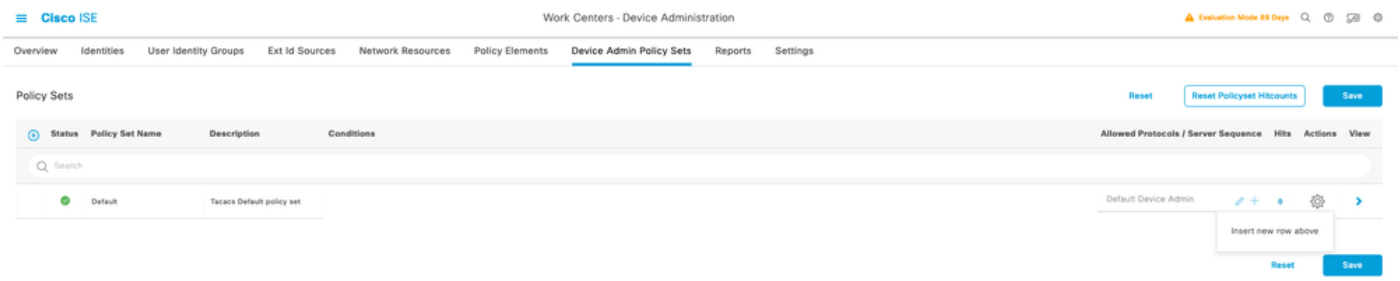
Nello stesso menu, se si seleziona Raw View per il profilo TACACS, è possibile verificare la configurazione corrispondente dell'attributo da inviare tramite ISE.



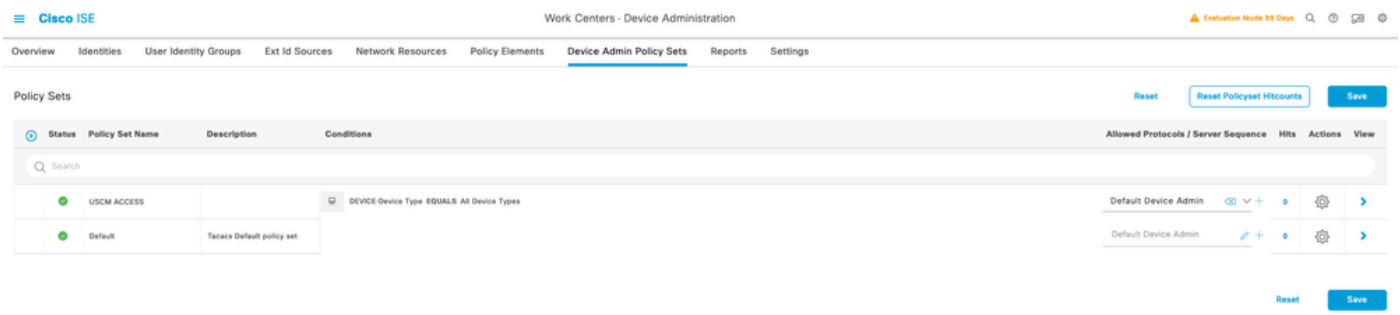
Nota: Il nome della coppia cisco-av è la stringa che fornisce l'ID attributo per il provider TACACS+.

Passaggio 3. Selezionare la casella di spunta e salvare la configurazione.

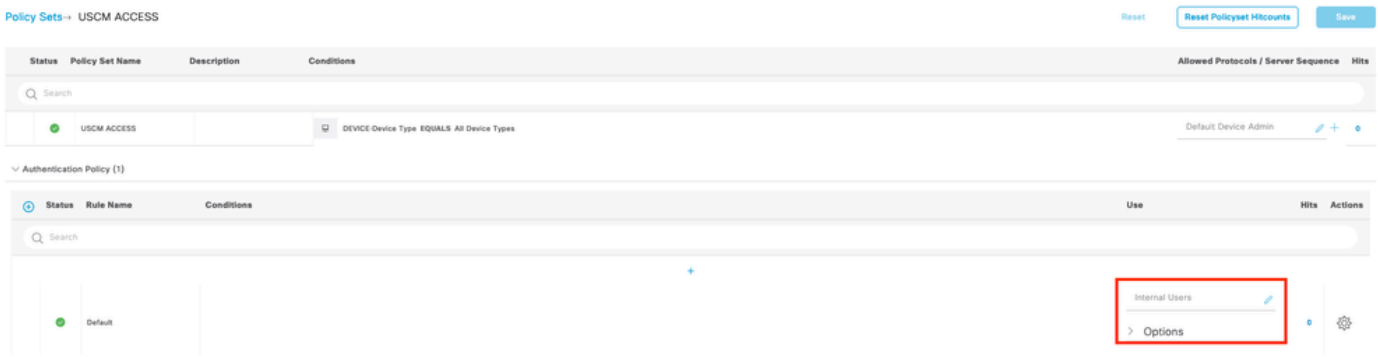
Passaggio 4. Creare un set di criteri di amministrazione dei dispositivi da utilizzare per il modulo UCSM, selezionare il menu Centri di lavoro > Amministrazione dispositivi > Set di criteri di amministrazione dei dispositivi, quindi da un set di criteri esistente selezionare l'icona degli ingranaggi e selezionare Inserisci nuova riga



Passaggio 5. Assegnare un nome al nuovo set di criteri, aggiungere le condizioni in base alle caratteristiche delle autenticazioni TACACS+ in corso sul server UCSM e selezionare Protocolli consentiti > Amministratore predefinito del dispositivo, quindi salvare la configurazione.

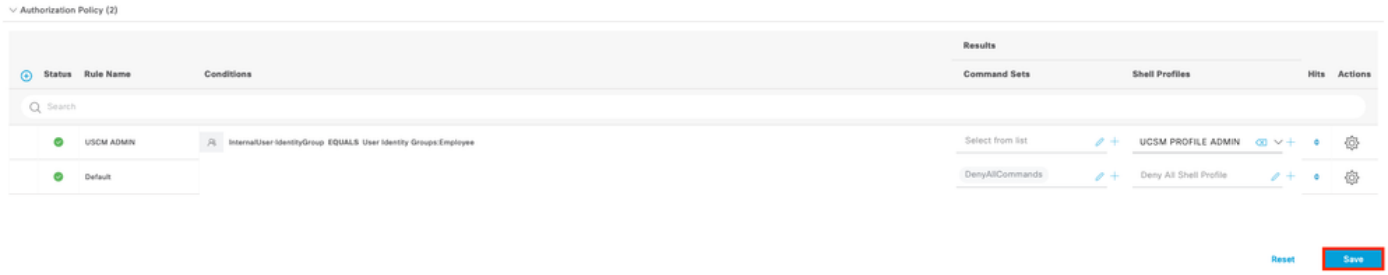


Passaggio 6. Selezionare nell'opzione >view e selezionare nella sezione Authentication Policy (Criteri di autenticazione) l'origine dell'identità esterna da cui ISE richiede il nome utente e le credenziali immesse nell'UCSM. In questo esempio, le credenziali corrispondono agli utenti interni memorizzati in ISE.



Passaggio 7. Scorrere verso il basso fino alla sezione Criteri di autorizzazione fino al criterio Predefinito, selezionare l'icona di ingranaggio, quindi inserire una regola.

Passaggio 8. Assegnare un nome alla nuova regola di autorizzazione, aggiungere le condizioni relative all'utente già autenticato come appartenenza al gruppo e, nella sezione Profili shell, aggiungere il profilo TACACS configurato in precedenza, salvare la configurazione.



Configurazione TACACS+ su UCSM

Accedere **Cisco UCS Manager**alla GUI con un utente con privilegi di amministratore.

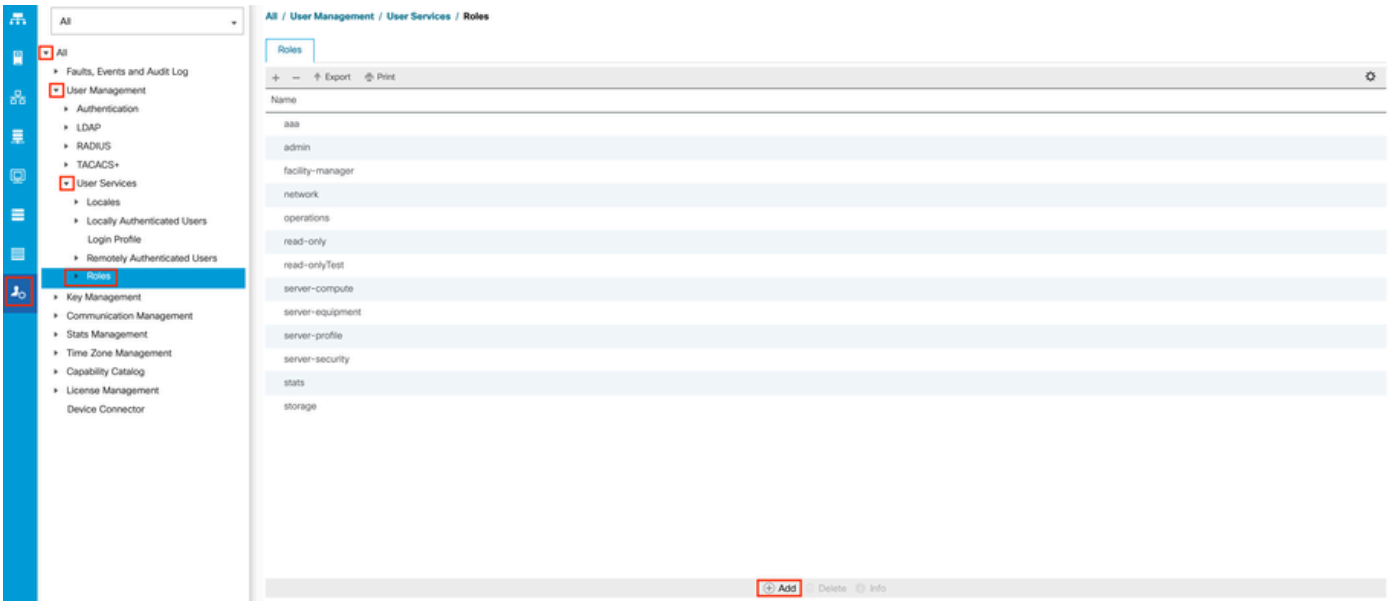
Creazione di ruoli per gli utenti

Passaggio 1. Nel riquadro di spostamento, selezionare la scheda Amministrazione.
Passaggio 2. Nella scheda Amministrazione, espandere Tutto > Gestione utenti > Servizi utente > Ruoli.

Passaggio 3. Nel riquadro**Work**selezionare**General**la scheda.

Passaggio 4. Selezionare Aggiungi per i ruoli personalizzati. In questo esempio si utilizzano i ruoli predefiniti.

Passaggio 5. Verificare che il nome del ruolo corrisponda al nome configurato in precedenza nel profilo TACACS.

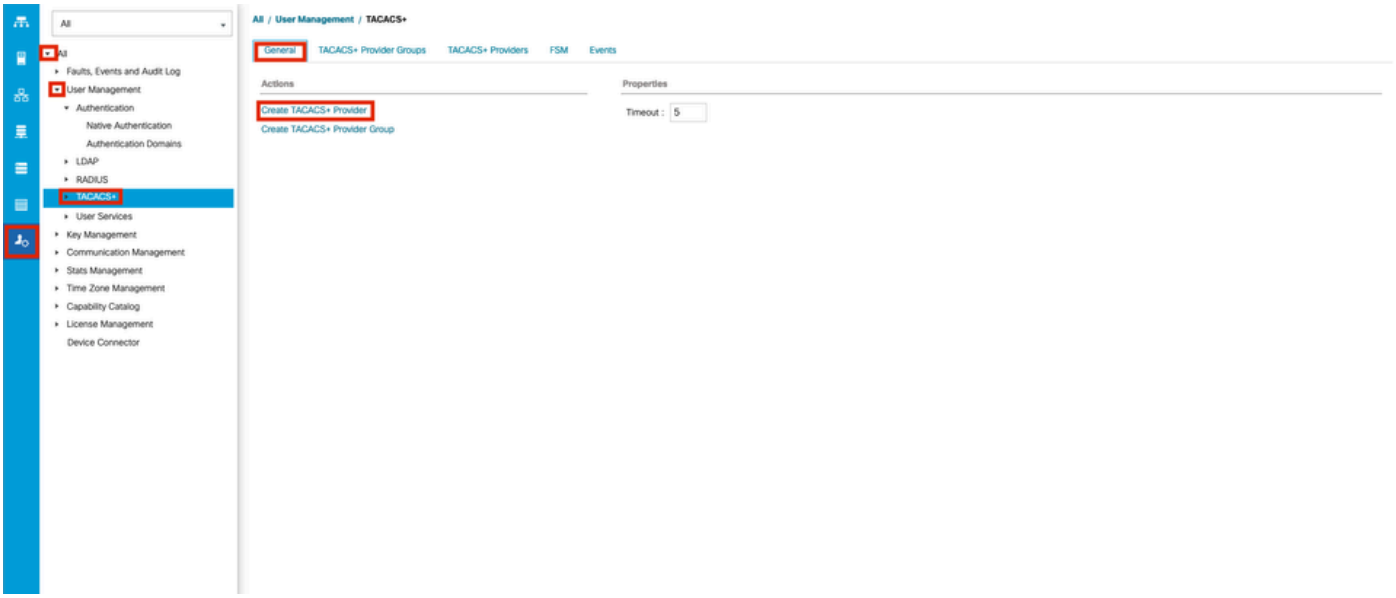


Crea un provider TACACS+

Passaggio 1. Nel riquadro di spostamento, selezionare la scheda Amministrazione.
Passaggio 2. Nella scheda Admin, espandere All > User Management > TACACS+.

Passaggio 3. Nel riquadro**Work**selezionare la scheda corrispondente**General**.

Passaggio 4. Nell'**Actions**area, selezionare**Create TACACS+ Provider.**

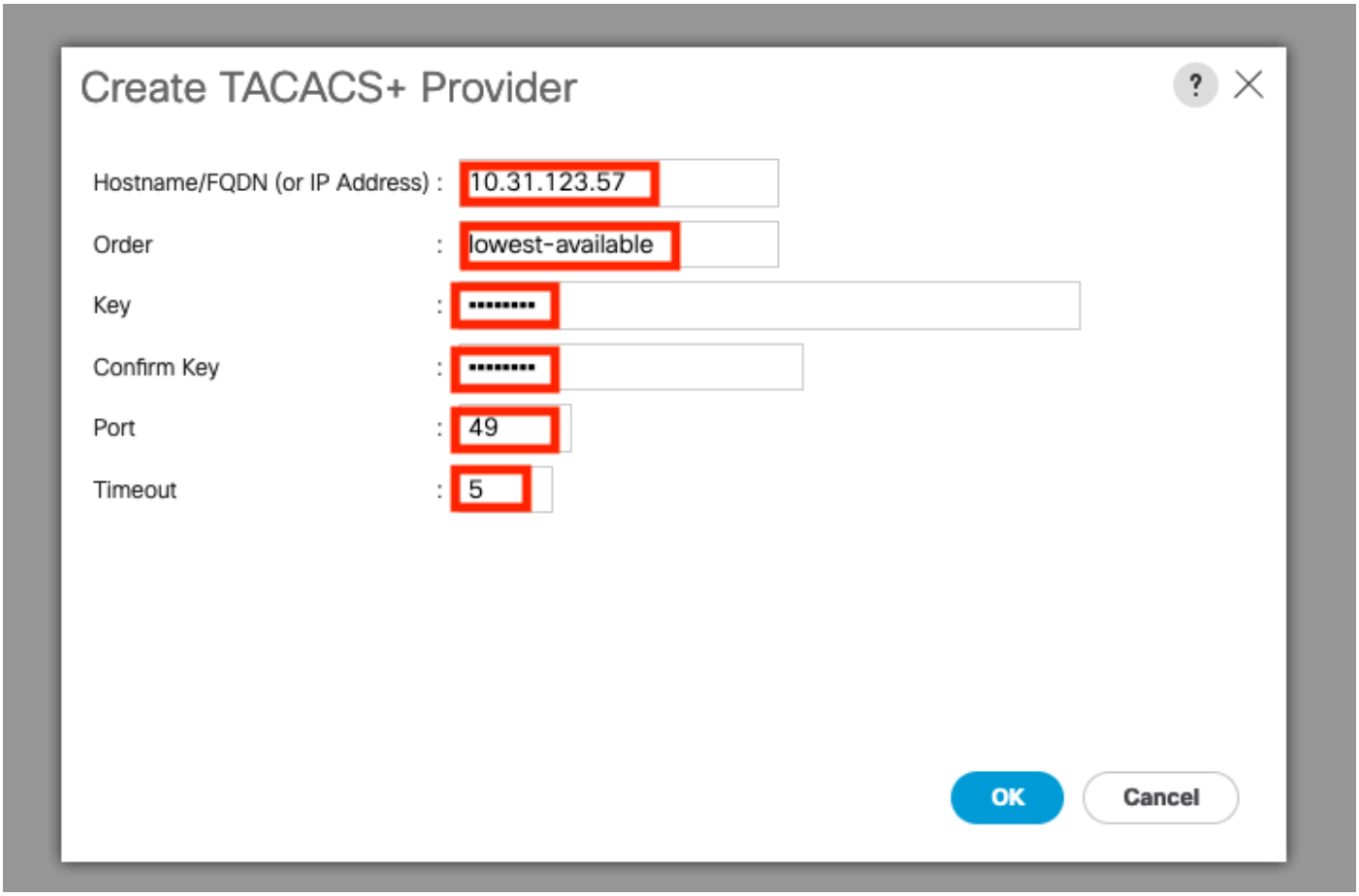


Passaggio 5. Nella procedura guidata**Create TACACS+ Provider**immettere le informazioni appropriate.

- Nel campo Hostname (Nome host), digitare l'indirizzo IP o il nome host del server TACACS+.
- Nel campo Order (Ordine), viene visualizzato l'ordine in cui Cisco UCS utilizza questo provider per autenticare gli utenti.

Immettere un numero intero compreso tra 1 e 16 oppure immettere il valore minimo disponibile o 0 (zero) se si desidera che Cisco UCS assegni il successivo ordine disponibile in base agli altri provider definiti in questa istanza di Cisco UCS.

- Nel campo Chiave, la chiave di crittografia SSL per il database.
- Nel campo Confirm Key (Conferma chiave), viene ripetuta la chiave di crittografia SSL per la conferma.
- Nel campo Port (Porta), indica la porta attraverso cui Cisco UCS comunica con il database TACACS+ (porta 49, porta predefinita).
- Nel campo Timeout, indica il tempo in secondi impiegato dal sistema per tentare di contattare il database TACACS+ prima del timeout.



Passaggio 6. Selezionare Ok.

Nota: Se si utilizza un nome host anziché un indirizzo IP, è necessario configurare un server DNS in Cisco UCS Manager.

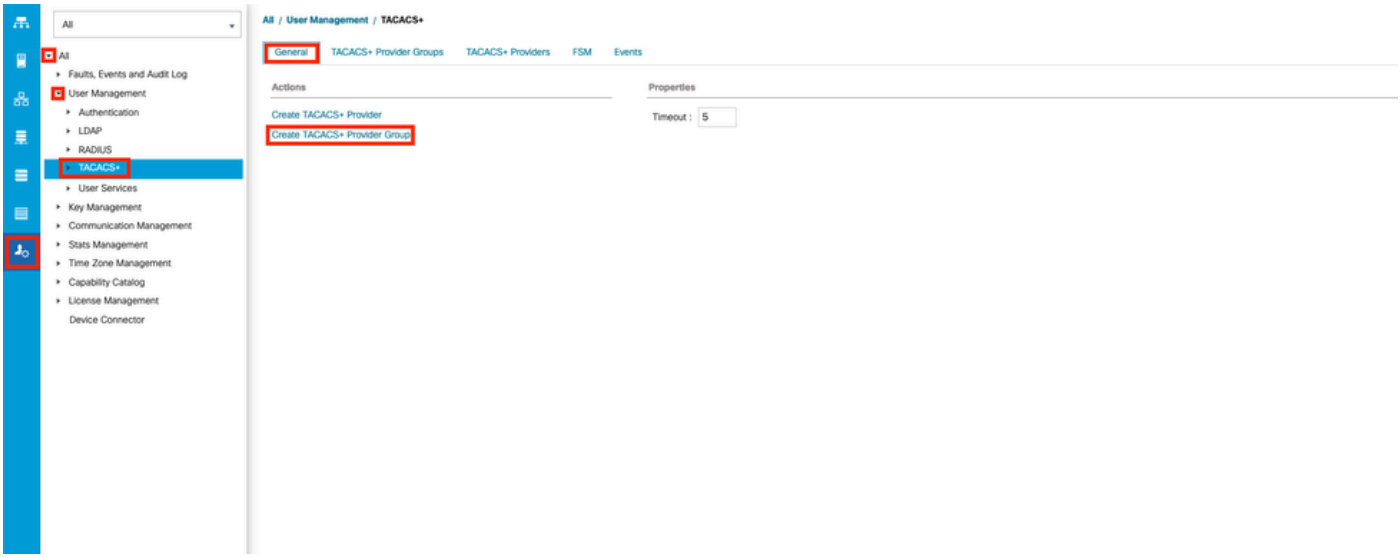
Crea un gruppo di provider TACAC+

Passaggio 1.Nel**Navigation**riquadro, selezionare la **Admin** scheda.

Passaggio 2. Espandere**Admin**la scheda **All** > **User Management** > **TACACS+**.

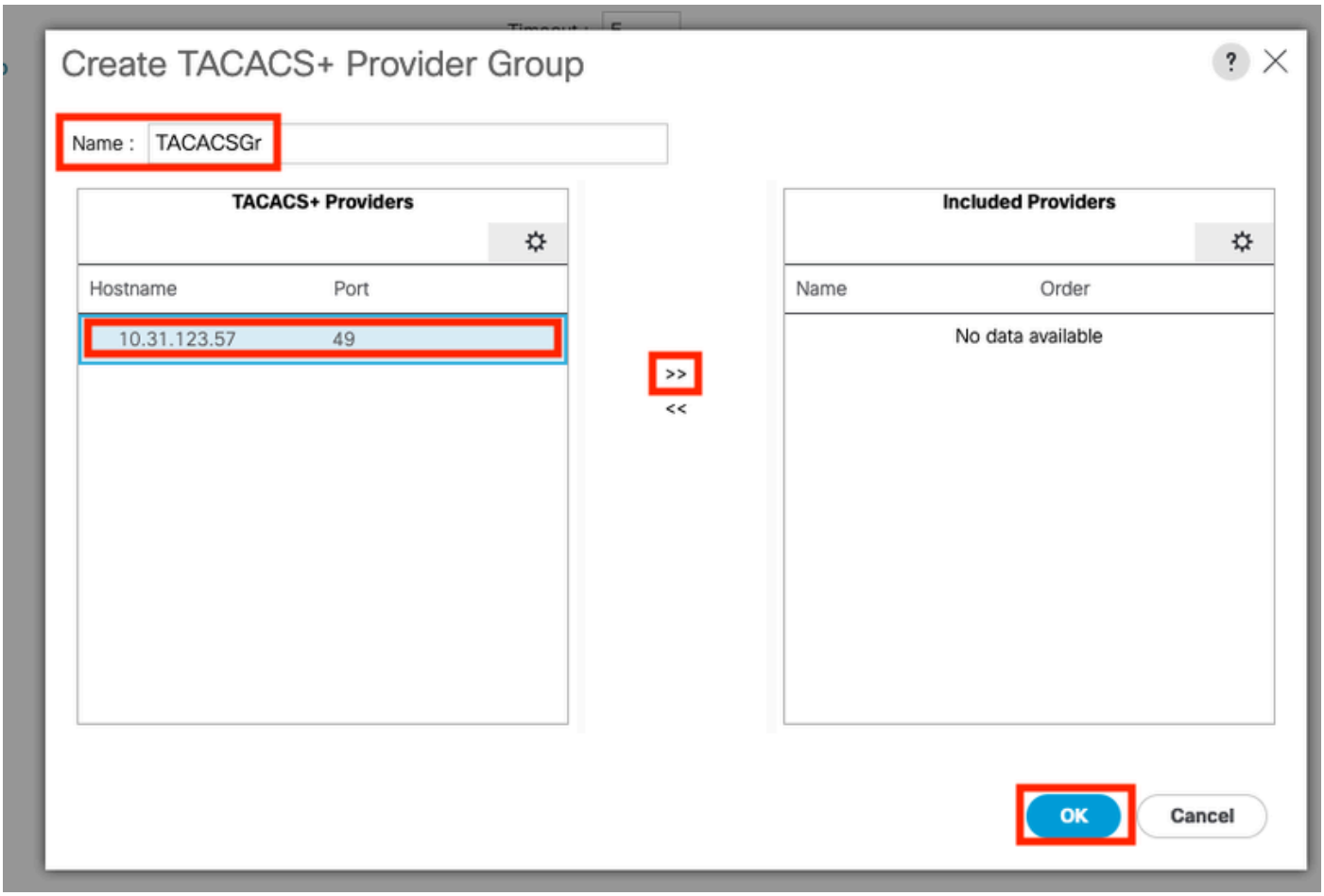
Passaggio 3. Nel riquadro**Work**selezionare la **General** scheda.

Passaggio 4. Nell'area, **Actions**Create TACACS+ Providerselezionare Gruppo.



Passaggio 5. Nella finestra di dialogo Crea gruppo di provider TACACS+, immettere le informazioni richieste.

- Nel campo Nome, immettere un nome univoco per il gruppo.
- Nella tabella Provider TACACS+, scegliere i provider da includere nel gruppo.
- Selezionare il pulsante >> per aggiungere i provider alla tabella Provider inclusi.



Passaggio 6. Selezionare Ok.

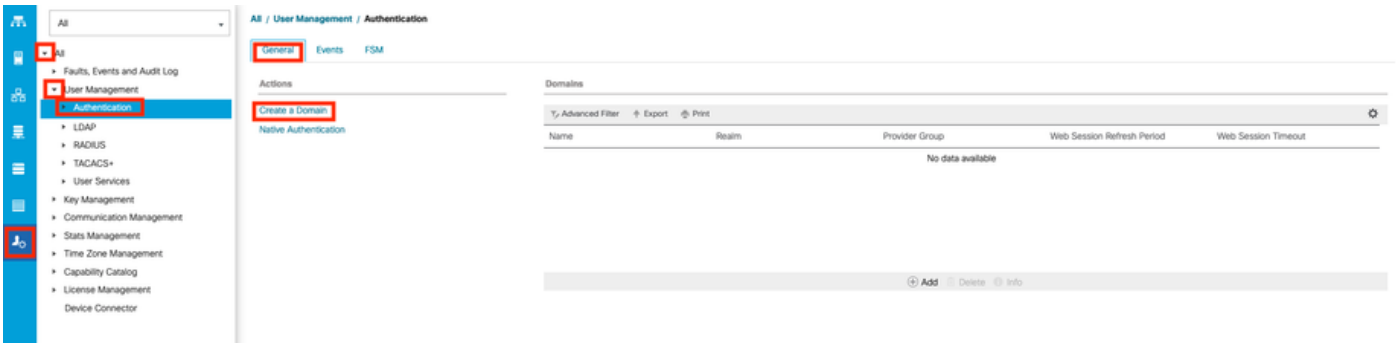
Crea un dominio di autenticazione

Passaggio 1. Nel **Navigation** riquadro, selezionare la **Admin** scheda.

Passaggio 2. Nella **Admin** scheda espandere **All** > **User Management** > **Authentication**

Passaggio 3. Nel riquadro**Work**selezionare la **General** scheda.

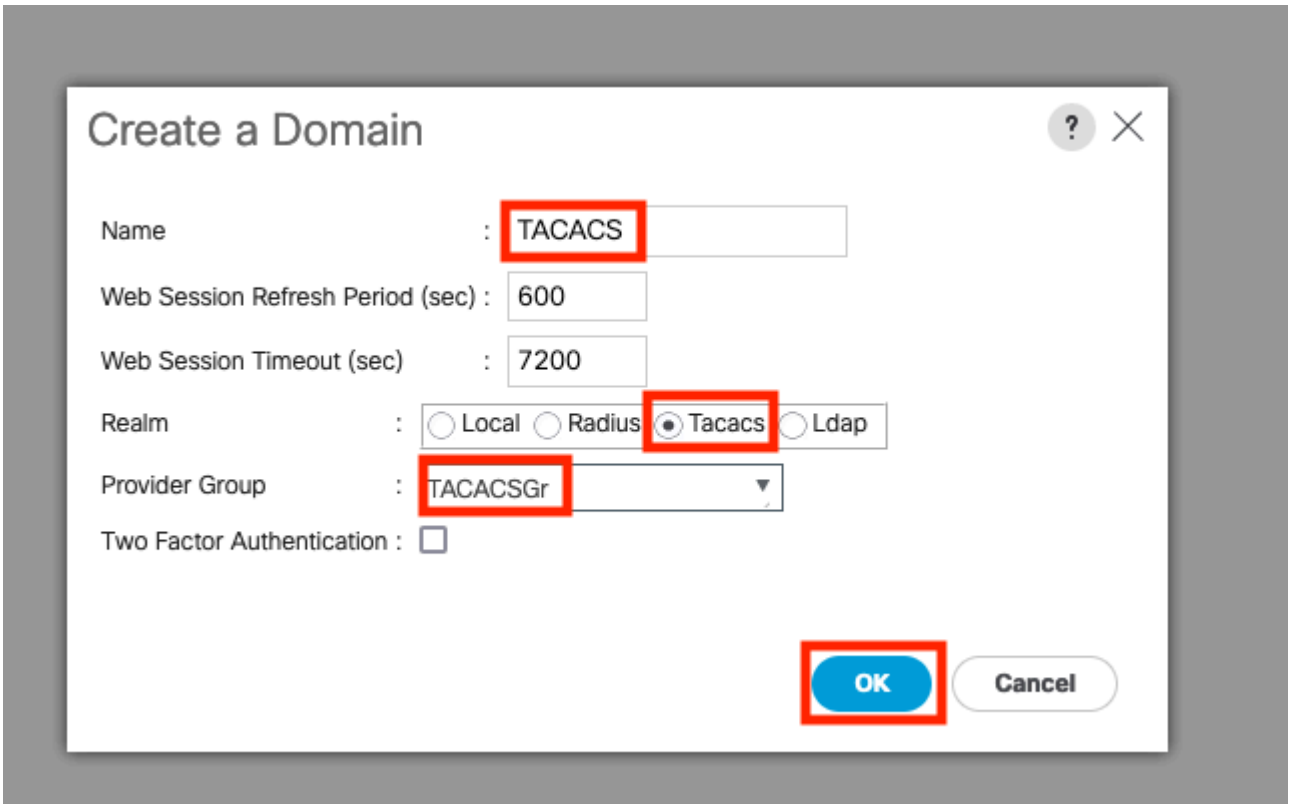
Passaggio 4. Nell'**Actions**area, selezionare**Create a Domain.**



Passaggio 5. Nella finestra di dialogo Crea dominio, immettere le informazioni richieste.

- Nel campo Nome, immettere un nome univoco per il dominio.
- Nel realm, selezionate l'opzione TACACS.

- Dall'elenco a discesa Provider Group (Gruppo provider), selezionare il gruppo di provider TACACS+ creato in precedenza e selezionare OK



Risoluzione dei problemi

Problemi comuni di TACACS+ sull'UCSM

- Chiave o caratteri non validi.
- Porta errata.
- Nessuna comunicazione con il provider a causa di una regola del firewall o del proxy.
- Gli FSM non sono al 100%.

Verificare la configurazione UCSM TACACS+:

È necessario verificare che il modulo UCSM abbia implementato la configurazione controllando che lo stato della macchina a stati finiti (FSM) venga visualizzato come completato al 100%.

Verificare la configurazione dalla riga di comando di UCSM

<#root>

```
UCS-A#
scope security

UCS-A /security #
scope tacacs
```

UCS-A /security/tacacs #

show configuration

```
UCS-AS-MXC-P25-02-A# scope security
UCS-AS-MXC-P25-02-A /security # scope tacacs
UCS-AS-MXC-P25-02-A /security/tacacs # show configuration
 scope tacacs
     enter auth-server-group TACACSGr
         enter server-ref 10.31.123.57
             set order 1
         exit
     exit
     enter server 10.31.123.57
         set order 1
         set port 49
         set timeout 5
 !       set key
     exit
     set timeout 5
 exit
```

<#root>

UCS-A /security/tacacs #

show fsm status

```
UCS-AS-MXC-P25-02-A /security/tacacs # show fsm status

    FSM 1:
        Status: Nop
        Previous Status: Update Ep Success
        Timestamp: 2023-06-24T20:54:05.021
        Try: 0
        Progress (%): 100
        Current Task:
```

Verificare la configurazione di Tacacs da NXOS:

<#root>

UCS-A#

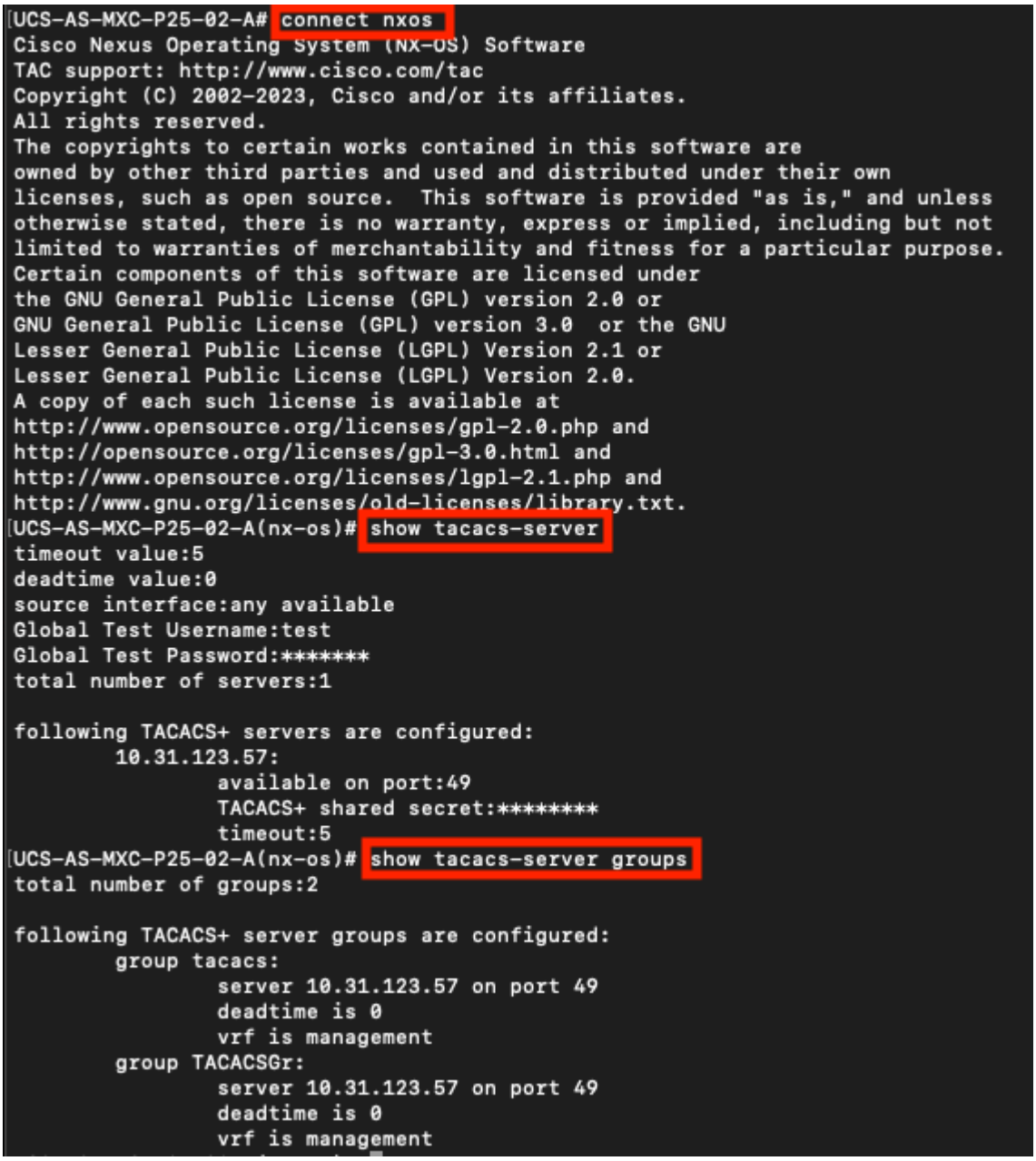
connect nxos

UCS-A(nx-os)#

show tacacs-server

UCS-A(nx-os)#

show tacacs-server groups



Per verificare l'autenticazione da NX-OS, utilizzare**test aaa**il comando (disponibile solo da NXOS).

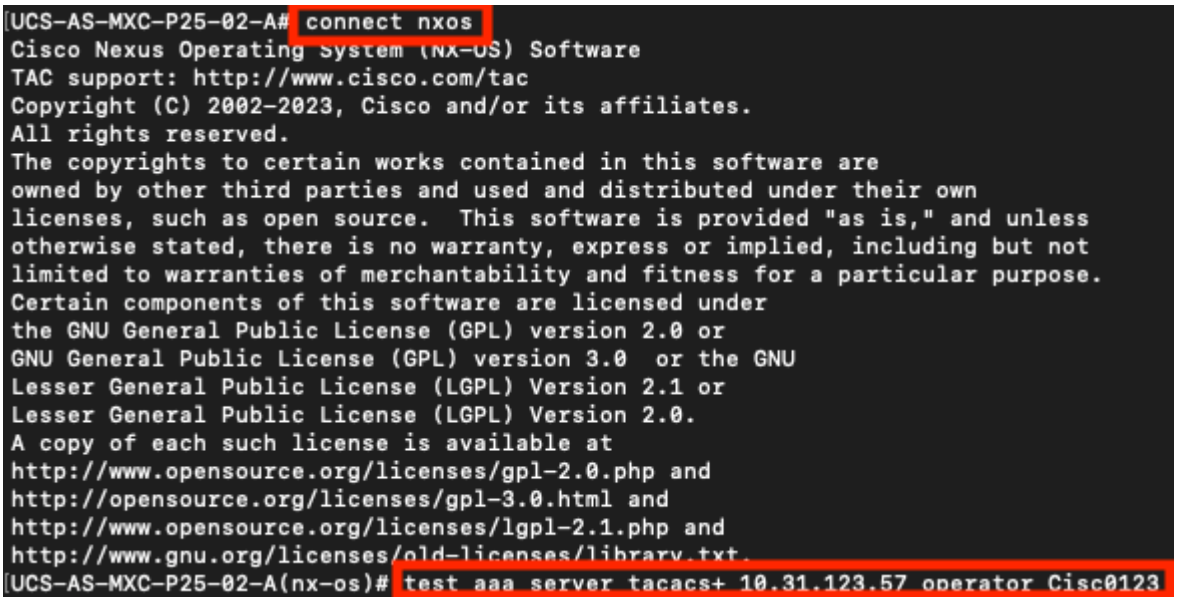
Convalidare la configurazione del server:

<#root>

UCS-A(nx-os)#

test aaa server tacacs+

<TACACS+-server-IP-address or FQDN> <username> <password>



Revisione UCSM

Verifica della raggiungibilità

<#root>

UCS-A#

connect local-mgmt

UCS-A(local-mgmt)#

ping

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

```
UCS-AS-MXC-P25-02-A# connect local-mgmt
pCisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

UCS-AS-MXC-P25-02-A(local-mgmt)# ping 10.31.123.57
PING 10.31.123.57 (10.31.123.57) from 10.31.123.8 : 56(84) bytes of data.
64 bytes from 10.31.123.57: icmp_seq=1 ttl=64 time=0.347 ms
64 bytes from 10.31.123.57: icmp_seq=2 ttl=64 time=0.309 ms
```

Verifica porta

<#root>

UCS-A#

connect local-mgmt

UCS-A(local-mgmt)#

telnet

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

```
UCS-AS-MXC-P25-02-A# connect local-mgmt
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

UCS-AS-MXC-P25-02-A(local-mgmt)# telnet 10.31.123.57 49
Trying 10.31.123.57...
Connected to 10.31.123.57.
Escape character is '^]'.
```

Il metodo più efficace per visualizzare gli errori consiste nell'attivare il debug NXOS, che consente di visualizzare i gruppi, la connessione e il messaggio di errore che causa la mancata comunicazione.

- Aprire una sessione SSH su UCSM e accedere con qualsiasi utente con privilegi amministrativi (preferibilmente un utente locale), passare al contesto CLI di NX-OS e avviare terminal monitor.

<#root>

```
UCS-A#
connect nxos

UCS-A(nx-os)#
terminal monitor
```

- Abilitare i flag di debug e verificare l'output della sessione SSH nel file di log.

<#root>

```
UCS-A(nx-os)#
debug aaa all

UCS-A(nx-os)#
debug aaa aaa-request

UCS-A(nx-os)#
debug tacacs+ aaa-request

UCS-A(nx-os)#
debug tacacs+ aaa-request-lowlevel

UCS-A(nx-os)#
debug tacacs+ all
```

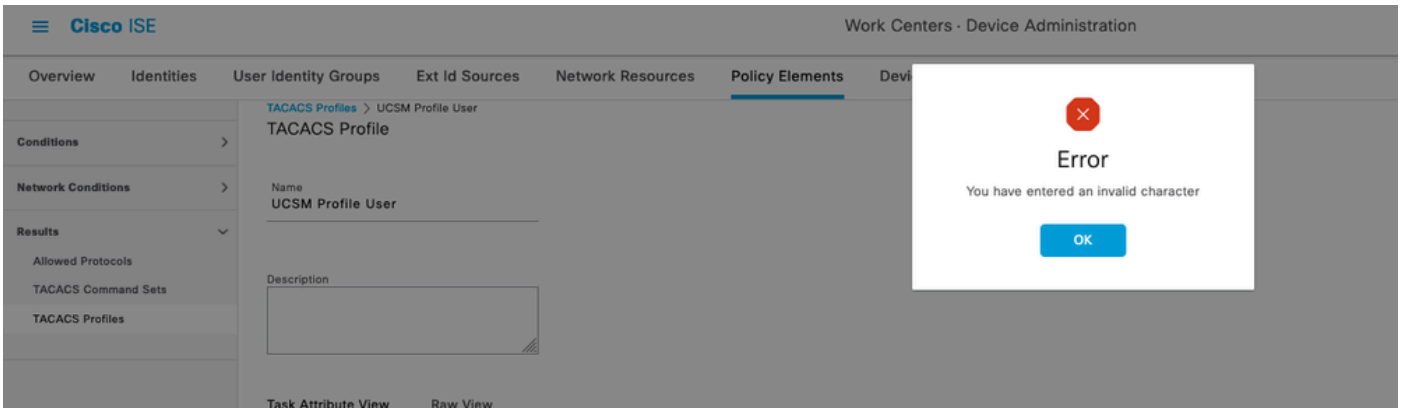
```
UCS-AS-MXC-P25-02-A# connect nxos
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2023, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source.  This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
UCS-AS-MXC-P25-02-A(nx-os)# terminal monitor
UCS-AS-MXC-P25-02-A(nx-os)# debug tacacs+ all
2023 Jun 26 04:42:22.104286 tacacs: event_loop(): calling process_rd_fd_set
2023 Jun 26 04:42:22.104311 tacacs: process_rd_fd_set: calling callback for fd 6
2023 Jun 26 04:42:22.104341 tacacs: fsrv didnt consume 182 opcode
2023 Jun 26 04:42:22.104994 tacacs: mts_message_handler: sdwrap_process_msg
2023 Jun 26 04:42:22.105011 tacacs: process_rd_fd_set: callback returned for fd 6
UCS-AS-MXC-P25-02-A(nx-os)# debug aaa all
```

- Aprire una nuova sessione della GUI o della CLI e tentare di accedere come utente remoto (TACACS+).
- Dopo aver ricevuto un messaggio di accesso non riuscito, disattivare i debug chiudendo la sessione o con questo comando.

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

Problemi comuni di TACAC sull'ISE

- All'interno di ISE, questo comportamento viene visualizzato quando si cerca di configurare un profilo tacacs negli attributi necessari a UCSM per assegnare i ruoli corrispondenti per l'amministratore o qualsiasi altro ruolo, selezionare il pulsante Save (Salva) e questo comportamento è visibile:



Questo errore è dovuto al seguente bug https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwc91917 , accertarsi di aver individuato la causa a cui è stato risolto.

Recensione ISE

Passaggio 1. Verificare che il servizio TACACS+ sia in esecuzione e che sia possibile archiviarlo:

- GUI: Verificare se il nodo è elencato con il servizio DEVICE ADMIN in Amministrazione > Sistema > Distribuzione.
- CLI: Eseguire il comando show ports | includere 49 per confermare che la porta TCP contiene connessioni che appartengono a TACACS+

<#root>

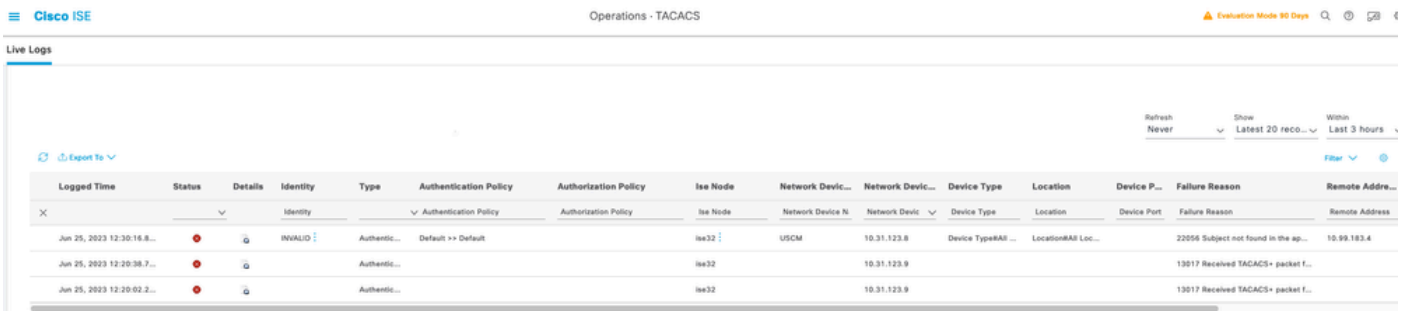
```
ise32/admin#
```

```
show ports | include 49
```

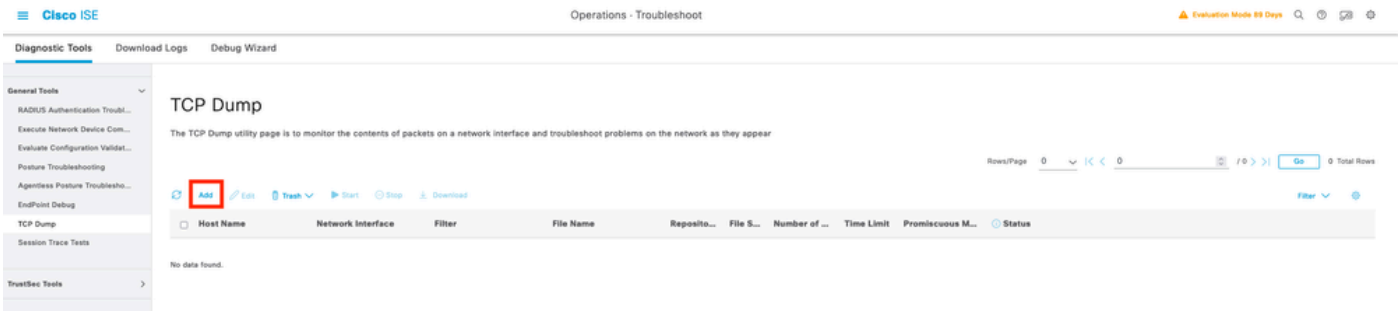
```
tcp: 169.254.4.1:49, 169.254.2.1:49, 169.254.4.1:49, 10.31.123.57:49
```

Passaggio 2. Conferma se sono presenti registri attivi relativi ai tentativi di autenticazione TACACS+: è possibile controllare questa impostazione nel menu Operazioni > TACACS > Live logs ,

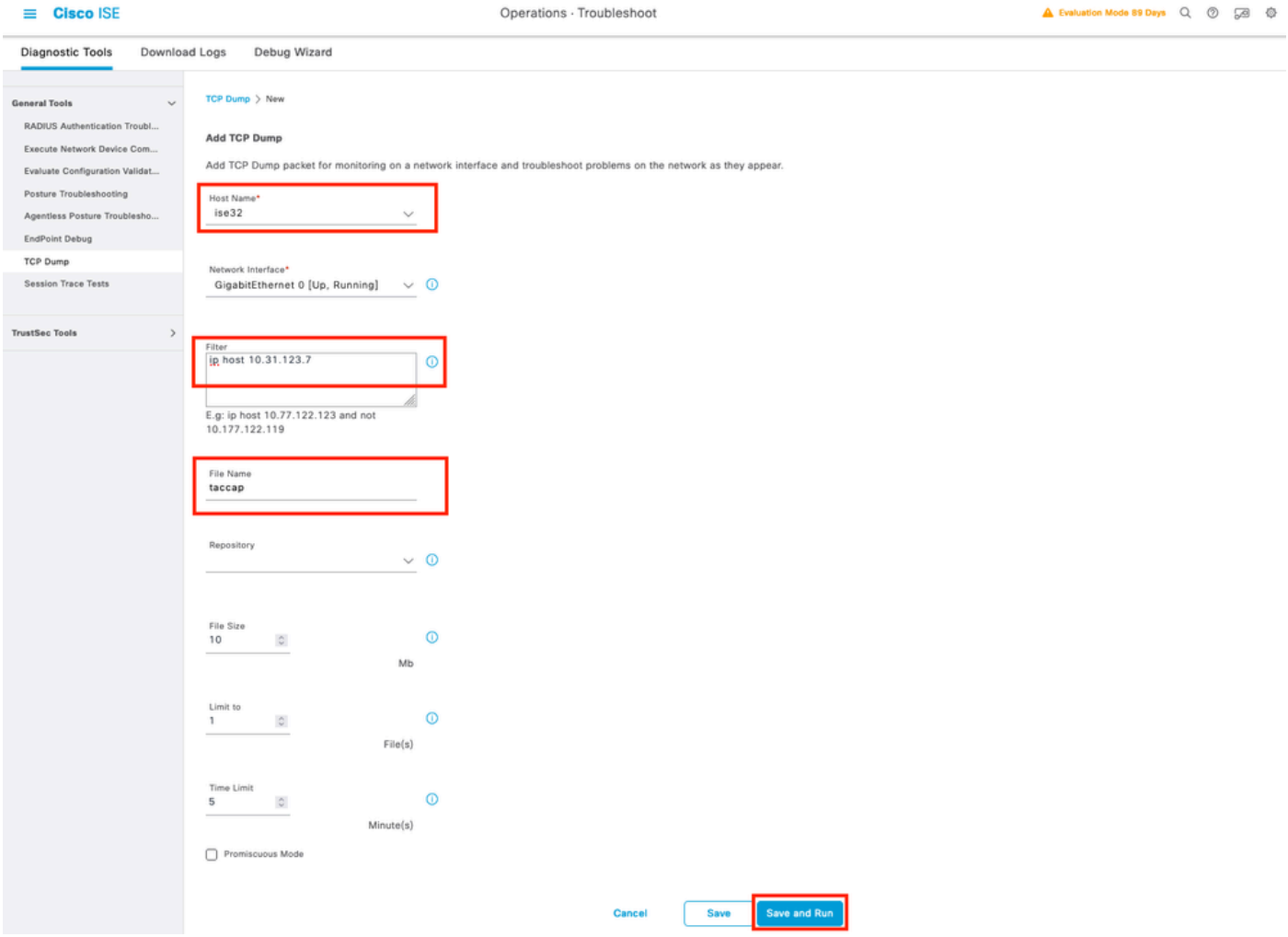
A seconda del motivo dell'errore, è possibile modificare la configurazione o risolvere la causa dell'errore.



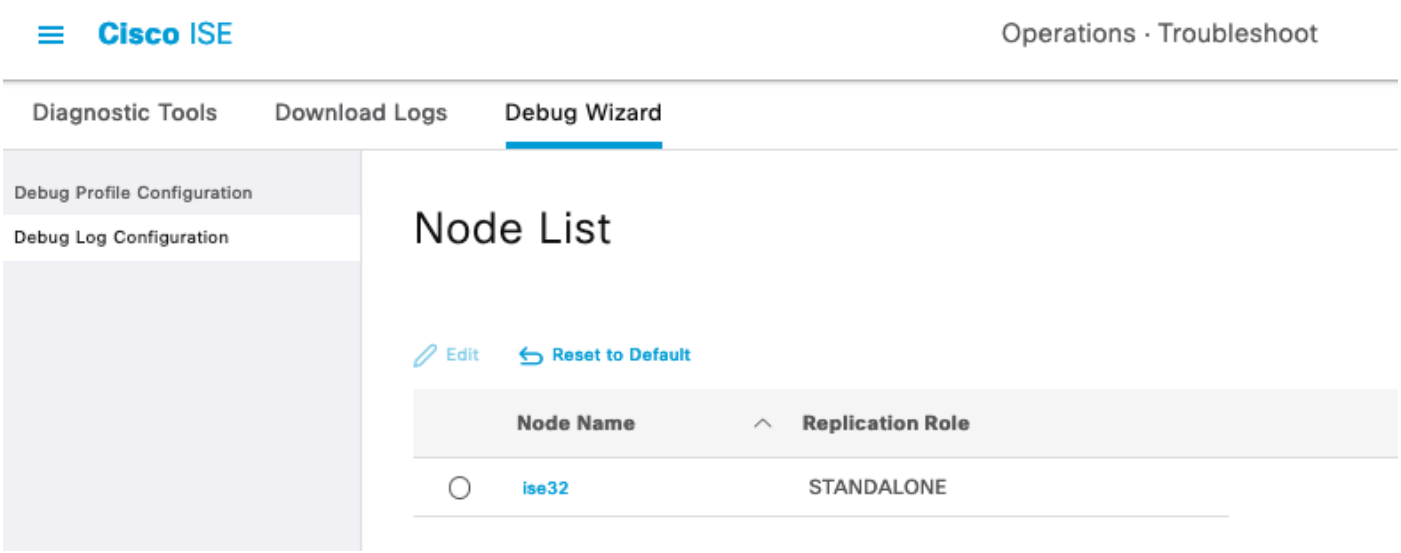
Passaggio 3. Se non viene visualizzato alcun catalogo, procedere con l'acquisizione di un pacchetto. Passare al menu Operazioni > Risoluzione dei problemi > Strumenti di diagnostica > Strumenti generali > TCP Dump , selezionare Aggiungi



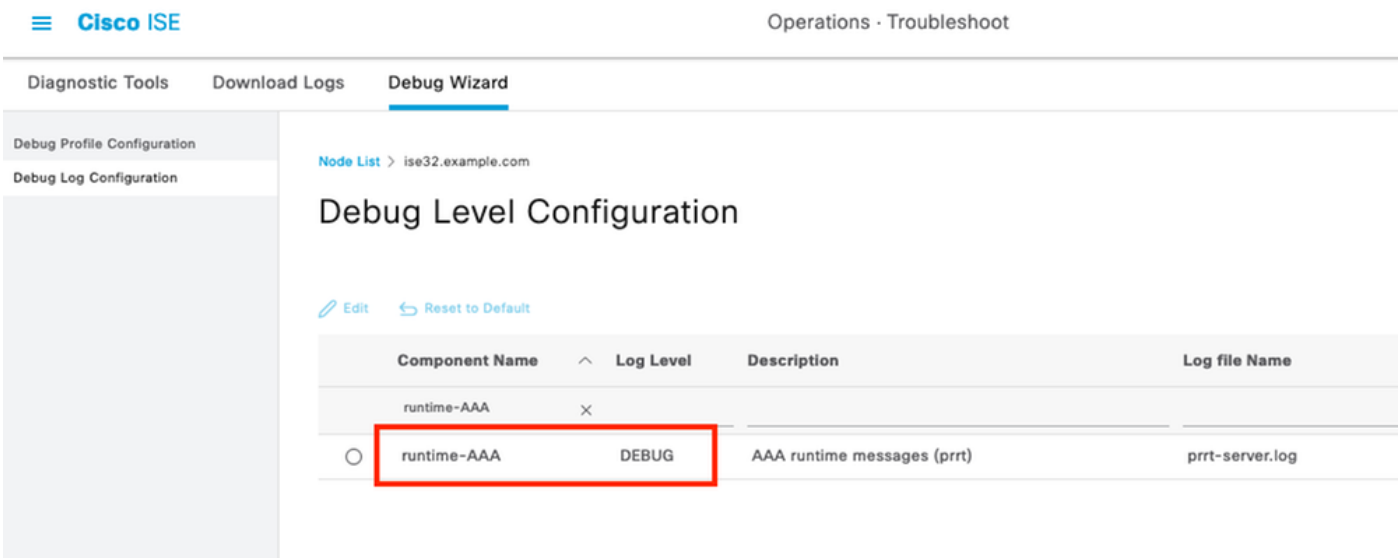
Selezionare il nodo del servizio criteri da cui il modulo UCSM sta inviando l'autenticazione, quindi nei filtri procedere all'input dell'host IP X.X.X corrispondente all'indirizzo IP del modulo UCSM dal quale viene inviata l'autenticazione, assegnare un nome all'acquisizione e scorrere verso il basso per salvare, eseguire l'acquisizione e accedere dal modulo UCSM.



Passaggio 4. Abilitare il componente runtime-AAA nel debug all'interno del PSN da cui viene eseguita l'autenticazione in Operazioni > Risoluzione dei problemi > Procedura guidata debug > Configurazione del registro di debug, selezionare il nodo PSN, selezionare quindi avanti nel pulsante Modifica.



Cercare il componente runtime-AAA e modificarne il livello per eseguire il debug, quindi riprodurre nuovamente il problema e procedere all'analisi dei log.



Nota: Per ulteriori informazioni, fare riferimento al video nel canale di Cisco Youtube "How to Enable Debug on ISE 3.x Versions https://www.youtube.com/watch?v=E3USz8B76c8" (Come abilitare i debug sulle versioni ISE 3.x).

Informazioni correlate

Guida all'amministrazione di Cisco UCS Manager

Guida alla configurazione di Cisco UCS CIMC 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).