Configurer le domaine d'authentification TACACS+ sur UCS Manager avec le serveur ISE

Table des matières

Introduction

Ce document décrit la configuration de l'authentification TACACS+ (Terminal Access Controller Access-Control System Plus) sur Unified Compute System Manager (UCSM). TACACS+ est un protocole réseau utilisé pour les services d'authentification, d'autorisation et de responsabilité (AAA) , il fournit une méthode centralisée pour gérer les périphériques d'accès réseau (NAD) où vous pouvez administrer et créer des règles via un serveur. Dans ce scénario d'utilisation, nous utilisons Identity Services Engine (ISE).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco UCS Manager (UCSM)

- Système de contrôle d'accès TACACS+ (Terminal Access Controller Access-Control System Plus)
- Moteur du service de vérification des identités (ISE)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

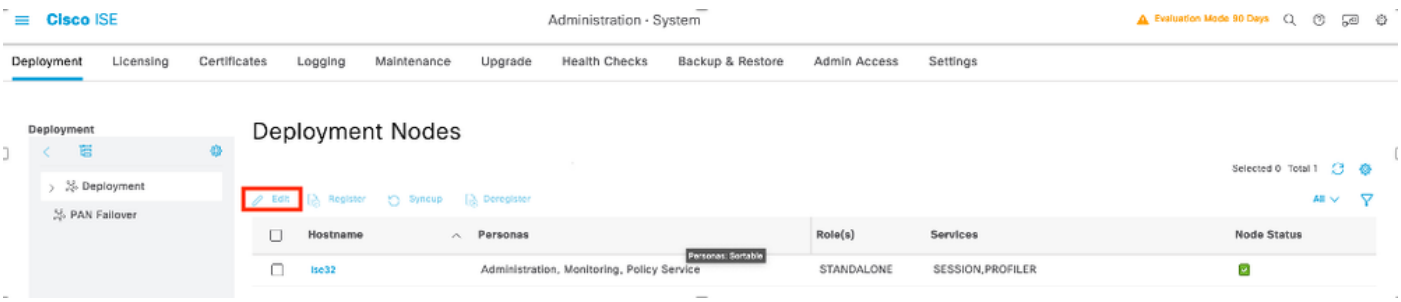
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configuration

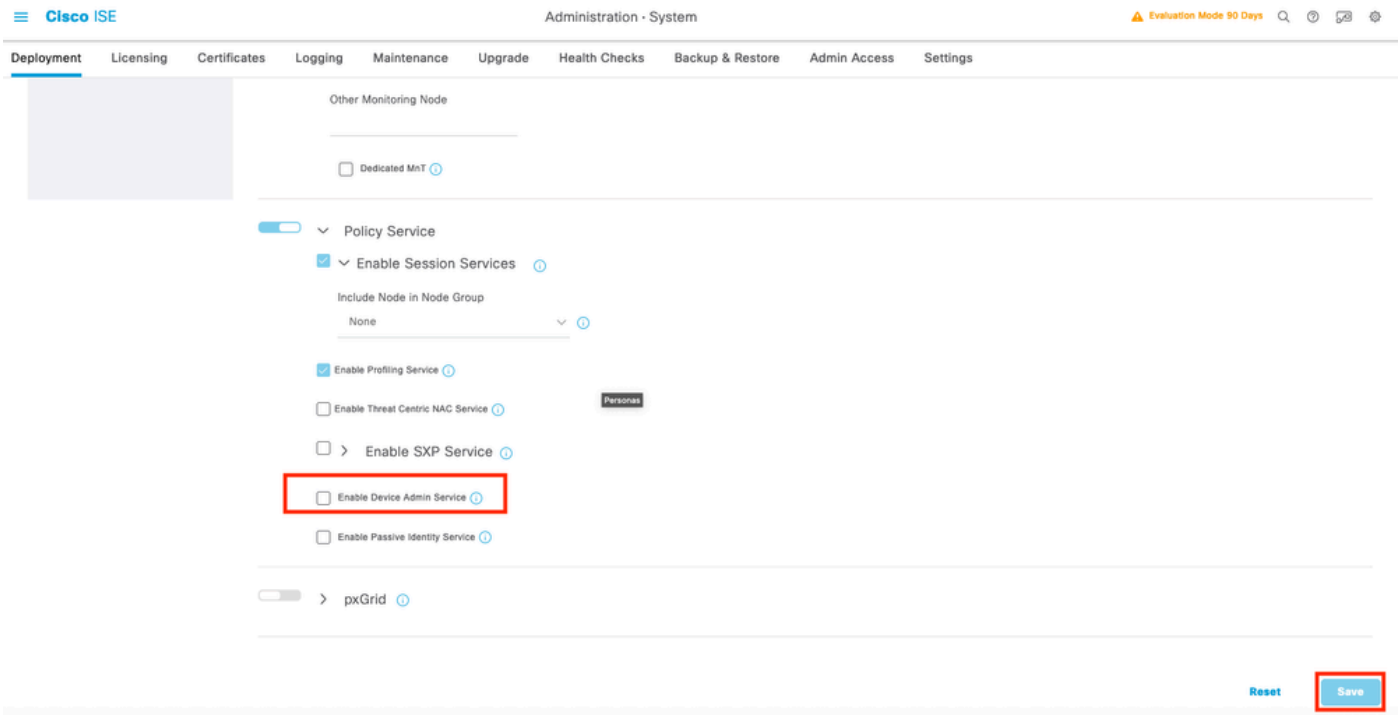
Configuration de TACACS+ sur ISE

Configuration de TACACS+ sur ISE

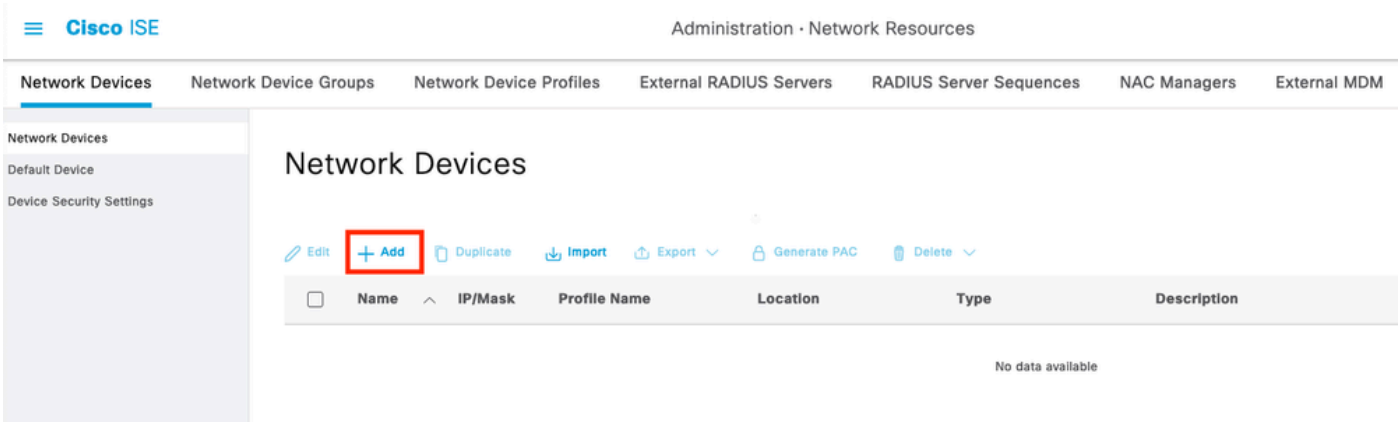
Étape 1. La première tâche consiste à vérifier si l'ISE dispose des capacités correctes pour gérer les authentifications TACACS+, afin que vous ayez besoin de vérifier si, dans le noeud Service de stratégie (PSN) souhaité, vous disposez de la fonctionnalité Device Admin Service, naviguez dans le menu Administration > System > Deployment, sélectionnez le noeud où l'ISE exécute TACACS+, puis sélectionnez le bouton edit.



Étape 2. Faites défiler la page vers le bas jusqu’à ce que vous voyiez la fonctionnalité correspondante appelée Device Administration Service (notez que pour que cette fonctionnalité soit activée, vous devez d’abord activer le personnage Policy Server sur le noeud et disposer en outre de licences pour TACACS+ dans votre déploiement), cochez cette case, puis enregistrez la configuration :

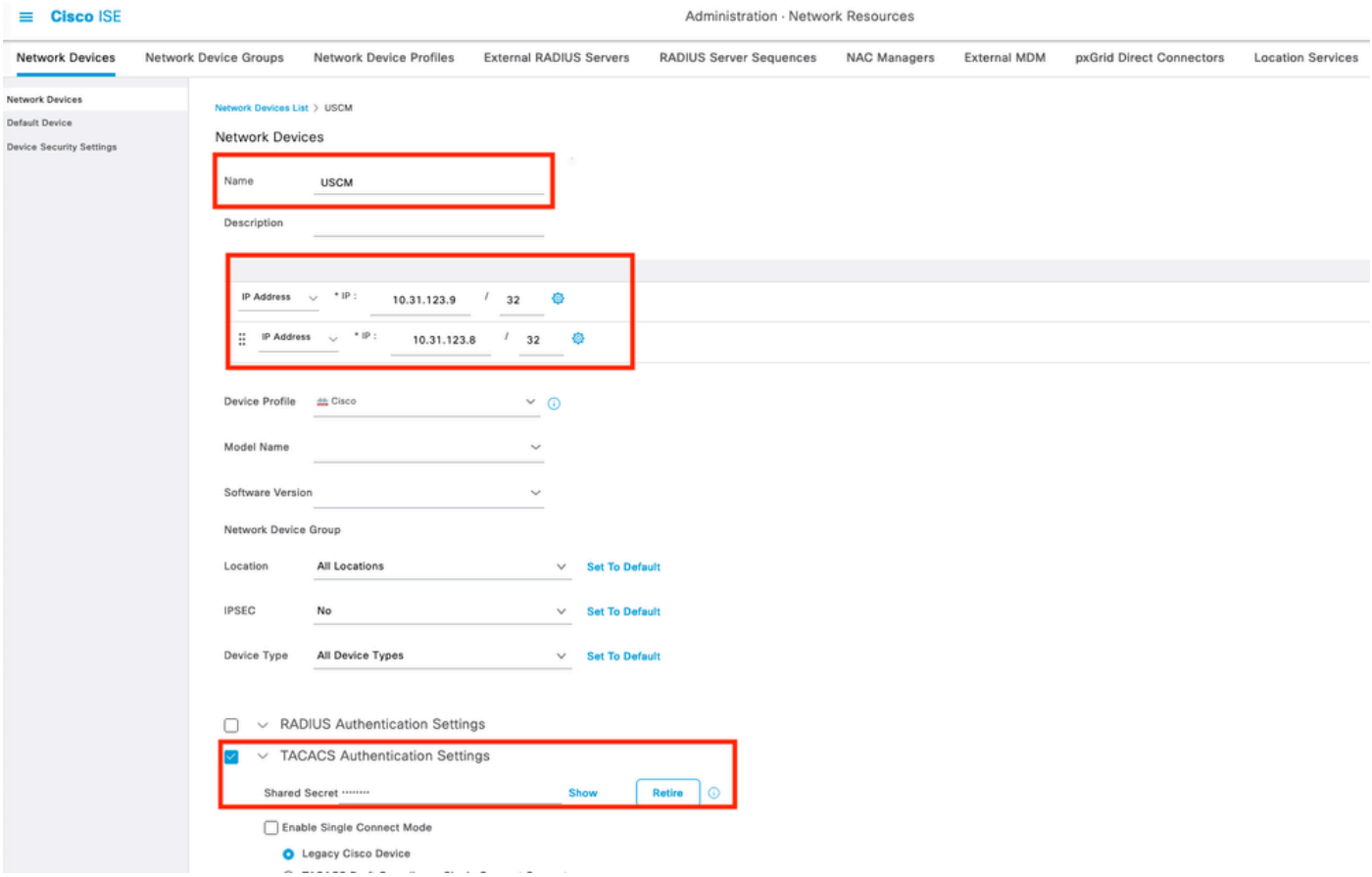


Étape 3. Configurez le périphérique d'accès réseau (NAD) qui utilise l'ISE comme serveur TACACS+, accédez au menu Administration > Network Resources > Network Devices puis sélectionnez le bouton +Add.



Étape 4. Dans cette section, configurez :

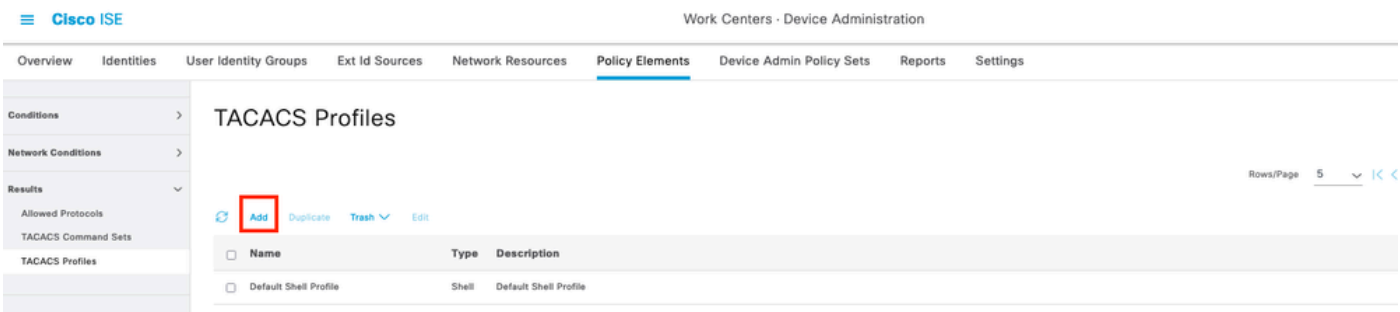
- Un nom pour le client UCSM qui sera le client TACACS+.
- Adresses IP utilisées par UCSM pour envoyer une requête à ISE.
- TACACS+ Shared Secret, mot de passe à utiliser pour chiffrer les paquets entre UCSM et ISE



Remarque : Pour une configuration de cluster, ajoutez les adresses IP du port de gestion pour les deux interconnexions de fabric. Cette configuration permet aux utilisateurs distants de continuer à se connecter en cas de défaillance de la première interconnexion de fabric et de basculement du système vers la seconde interconnexion de fabric. Toutes les demandes de connexion proviennent de ces adresses IP, et non de l'adresse IP virtuelle utilisée par Cisco UCS Manager.

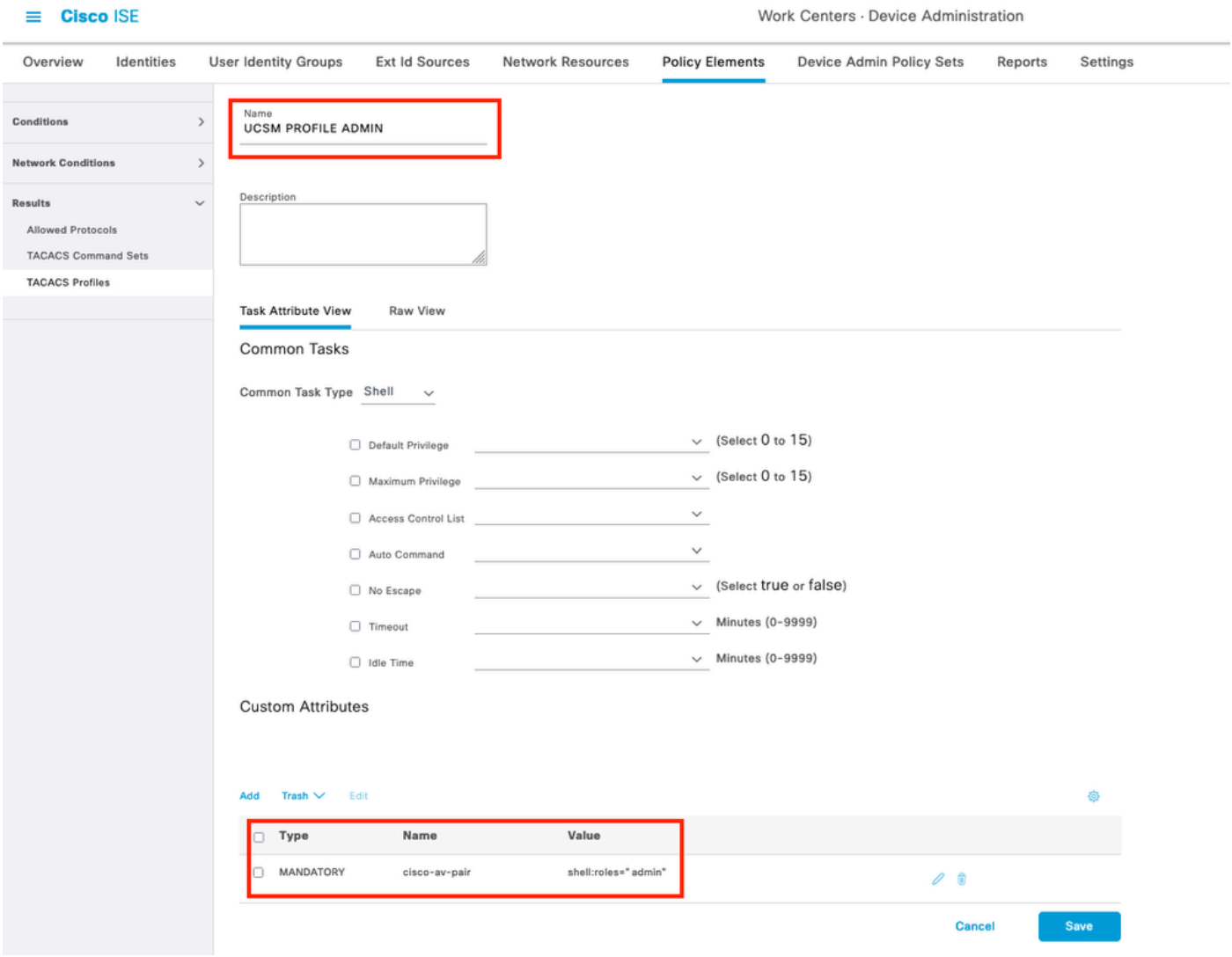
Configurer les attributs et les règles sur ISE

Étape 1. Créez un profil TACACS+, accédez au menu Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles , puis sélectionnez Add

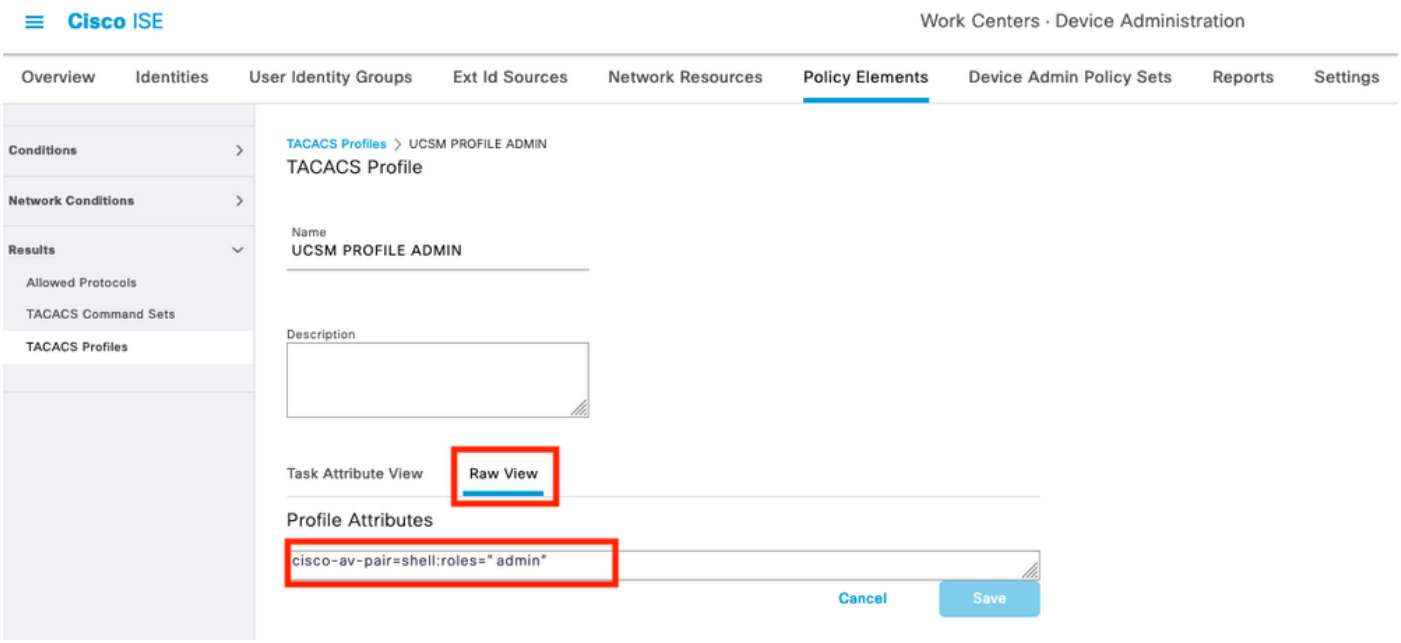


Étape 2. Dans cette section, configurez le profil avec un nom et dans la section Attributs personnalisés, sélectionnez Add , créez ensuite un attribut one de la caractéristique

OBLIGATOIRE , nommez-le comme cisco-av-pair et dans la valeur sélectionnez l'un des rôles disponibles dans le UCSM et entrez que comme un rôle shell, dans cet exemple, il utilise le rôle admin et l'entrée sélectionnée doit être shell : roles="admin" comme indiqué ici,



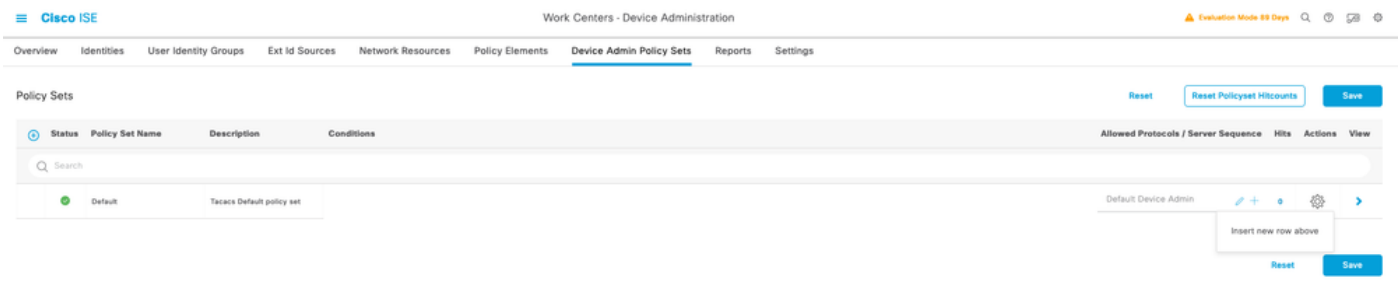
Dans le même menu si vous sélectionnez la vue brute pour le profil TACACS, vous pouvez vérifier la configuration correspondante de l'attribut qui doit être envoyé par ISE.



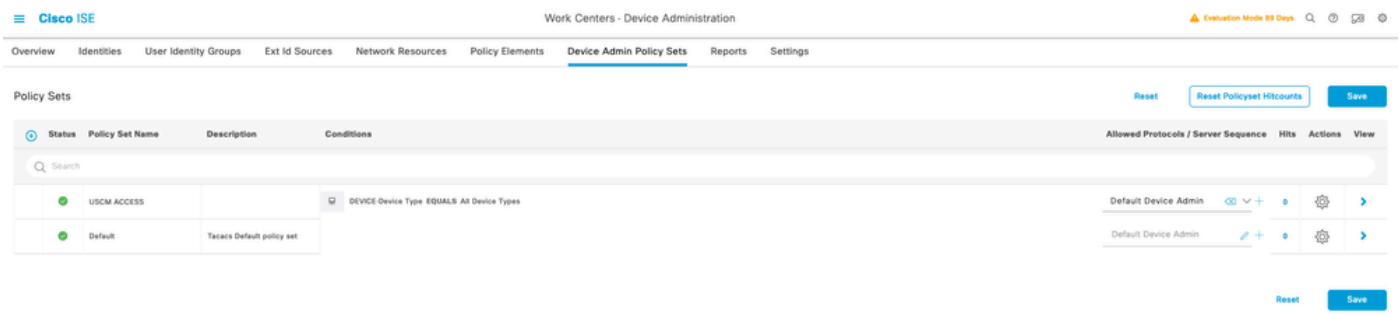
Remarque : Le nom cisco-av-pair est la chaîne qui fournit l'ID d'attribut pour le fournisseur TACACS+.

Étape 3. Sélectionnez cette option et enregistrez votre configuration.

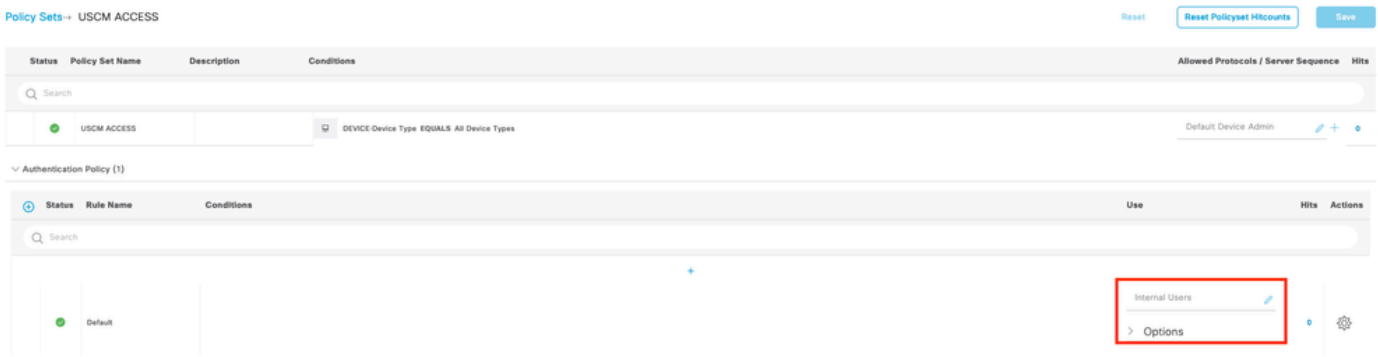
Étape 4 : création d'un ensemble de stratégies d'administration de périphériques à utiliser pour votre UCSM, naviguez dans le menu Work Centers > Device Administration > Device Admin Policy Sets, puis à partir d'un ensemble de stratégies existant, sélectionnez l'icône d'engrenage pour ensuite sélectionner Insert new row



Étape 5. Nommez ce nouvel ensemble de stratégies, ajoutez des conditions en fonction des caractéristiques des authentifications TACACS+ en cours à partir du serveur UCSM et sélectionnez Allowed Protocols > Default Device Admin, enregistrez votre configuration.

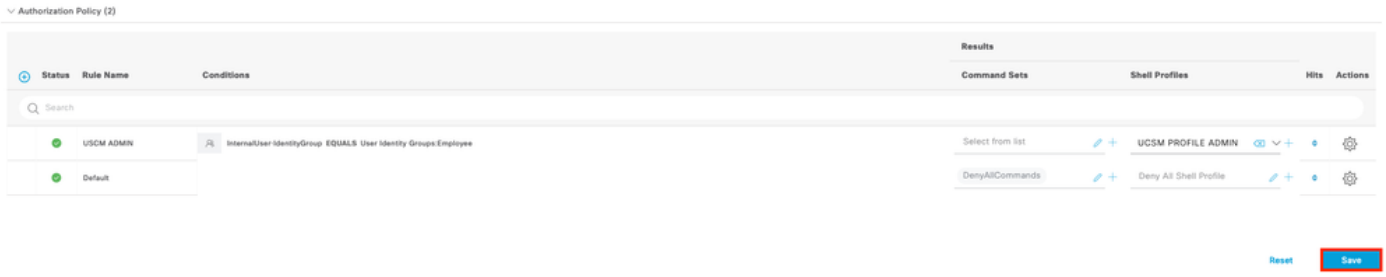


Étape 6. Sélectionnez dans l'option > view et sélectionnez dans la section Authentication Policy, la source d'identité externe à partir de laquelle l'ISE interroge le nom d'utilisateur et les informations d'identification qui sont entrées dans l'UCSM. Dans cet exemple, les informations d'identification correspondent aux utilisateurs internes stockés dans l'ISE.



Étape 7. Faites défiler la page jusqu'à la section intitulée Authorization Policy jusqu'à la politique Default, sélectionnez l'icône du rapport, puis insérez une règle.

Étape 8. Attribuez un nom à la nouvelle règle d'autorisation, ajoutez des conditions concernant l'utilisateur qui sont déjà authentifiées en tant qu'appartenance à un groupe et, dans la section Profils Shell, ajoutez le profil TACACS que vous avez configuré précédemment, enregistrez la configuration.



Configuration de TACACS+ sur UCSM

Connectez-vous **Cisco UCS Manager**à l'interface utilisateur graphique avec un utilisateur disposant de privilèges administrateur.

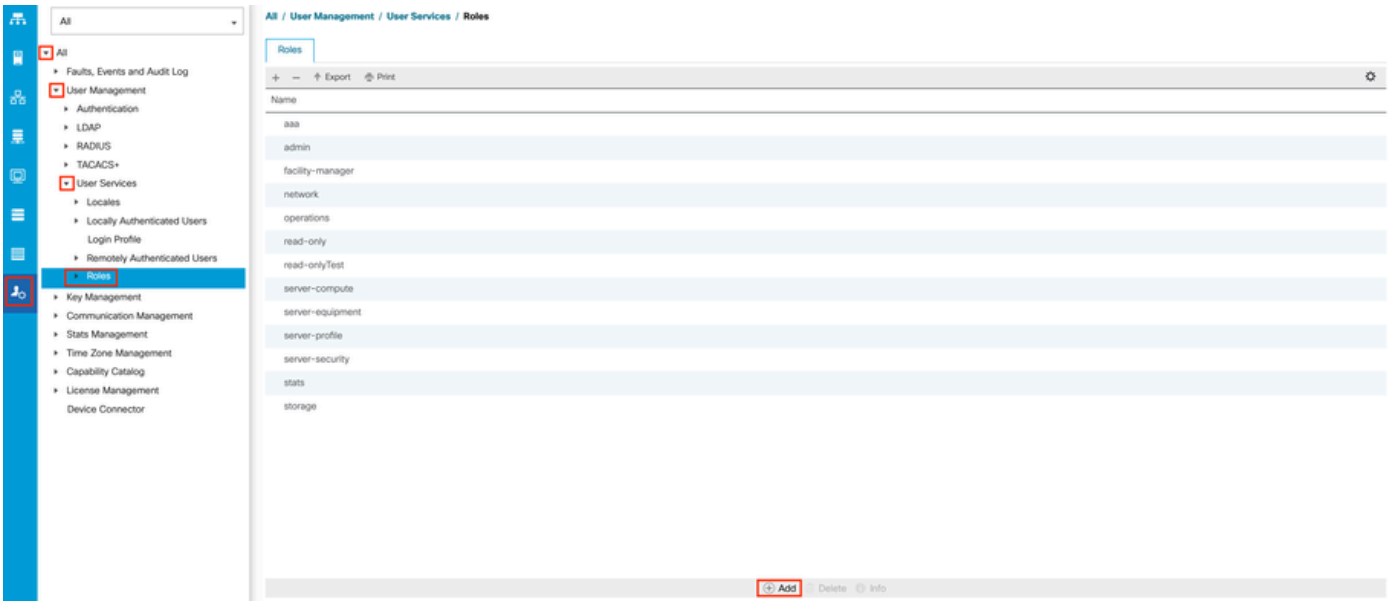
Créer des rôles pour les utilisateurs

Étape 1. Dans le volet de navigation, sélectionnez l'onglet Admin.
Étape 2. Dans l'onglet Admin, développez All > User Management > User Services > Roles.

Étape 3. Dans**Work**le volet, sélectionnez**General**l'onglet.

Étape 4. Sélectionnez Ajouter pour les rôles personnalisés. Cet exemple utilise les rôles par défaut.

Étape 5. Vérifiez que le rôle de nom correspond au nom configuré précédemment sur le profil TACACS.

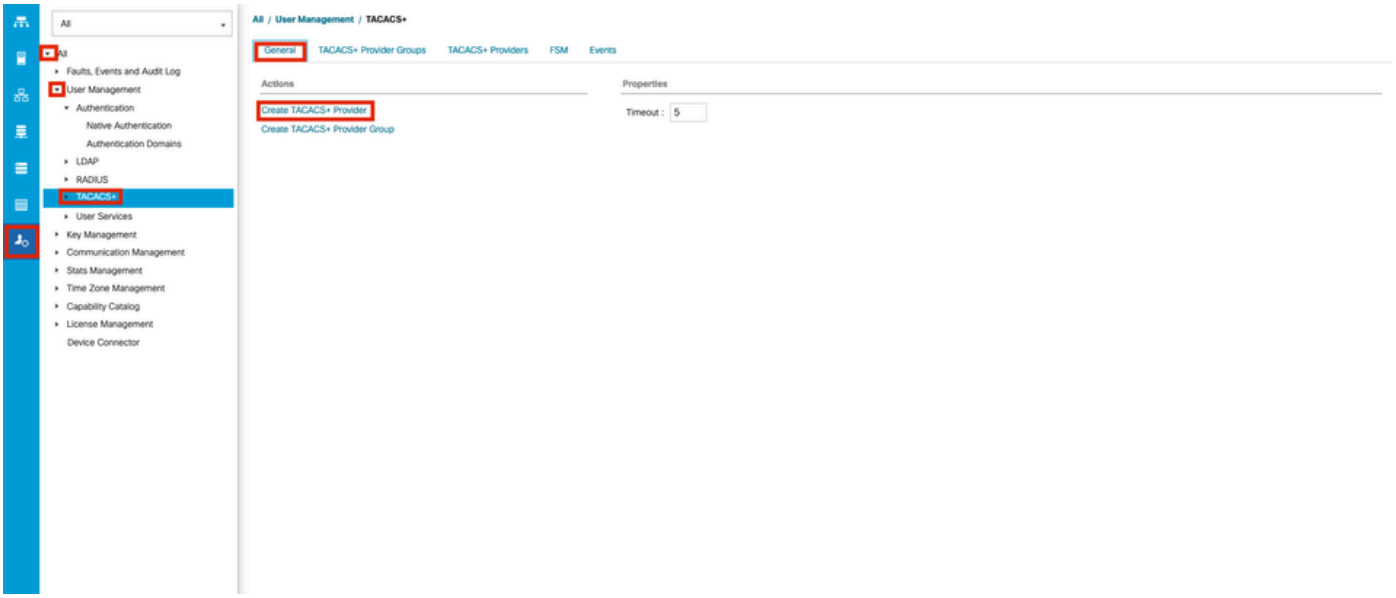


Créer un fournisseur TACACS+

Étape 1. Dans le volet de navigation, sélectionnez l'onglet Admin.
Étape 2. Dans l'onglet Admin, développez All > User Management > TACACS+.

Étape 3. Dans**Work**le volet, sélectionnez**General** l'onglet.

Étape 4. Dans**Actions**la zone, sélectionnez**Create TACACS+ Provider.**



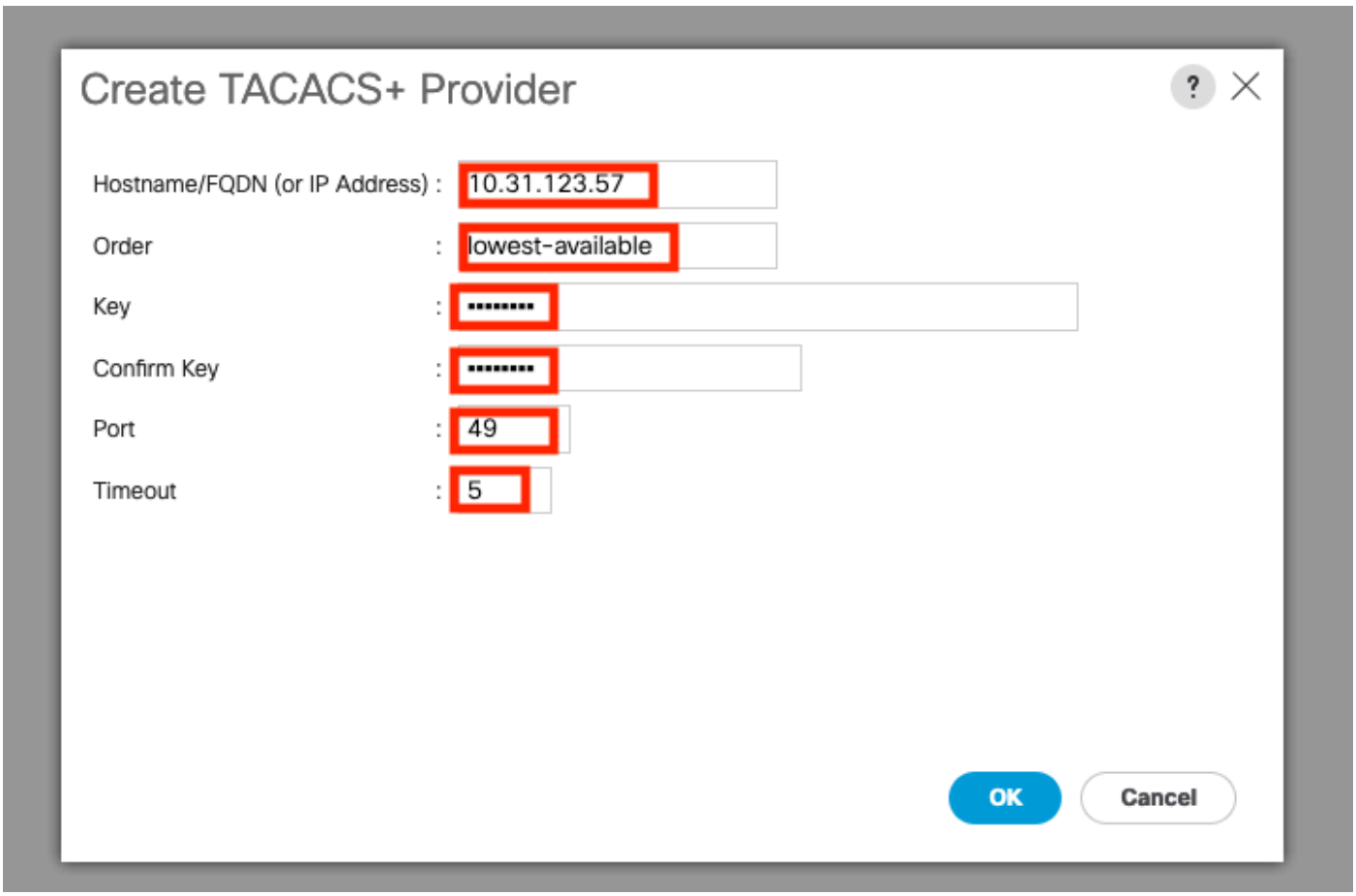
Étape 5. Dans**Create TACACS+ Provider**l'Assistant, entrez les informations appropriées.

- Dans le champ Hostname, saisissez l'adresse IP ou le nom d'hôte du serveur TACACS+.
- Dans le champ Order, Ordre dans lequel Cisco UCS utilise ce fournisseur pour authentifier les utilisateurs.

  Entrez un nombre entier compris entre 1 et 16, ou entrez le plus faible disponible ou 0 (zéro)

si vous souhaitez que Cisco UCS attribue la commande disponible suivante en fonction des autres fournisseurs définis dans cette instance Cisco UCS.

- Dans le champ Key, saisissez la clé de cryptage SSL de la base de données.
- Dans le champ Confirm Key, la clé de cryptage SSL est répétée à des fins de confirmation.
- Dans le champ Port, Port par lequel Cisco UCS communique avec la base de données TACACS+ (port 49 par défaut).
- Dans le champ Timeout, Durée en secondes que le système passe à essayer de contacter la base de données TACACS+ avant qu'elle n'expire.



Étape 6. Sélectionnez Ok.

Remarque : Si vous utilisez un nom d'hôte plutôt qu'une adresse IP, vous devez configurer un serveur DNS dans Cisco UCS Manager.

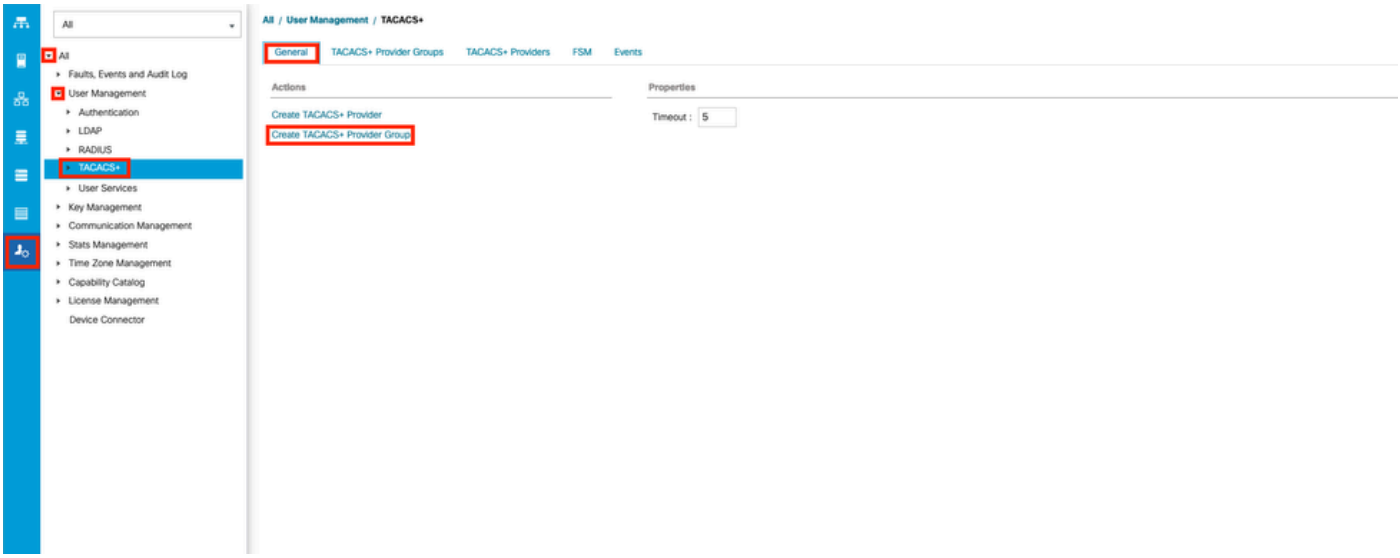
Créer un groupe de fournisseurs TACAC+

Étape 1.Dans**Navigation**le volet, sélectionnez l' **Admin**onglet.

Étape 2. Dans**Admin**l'onglet, développez **All** > **User Management** > **TACACS+**.

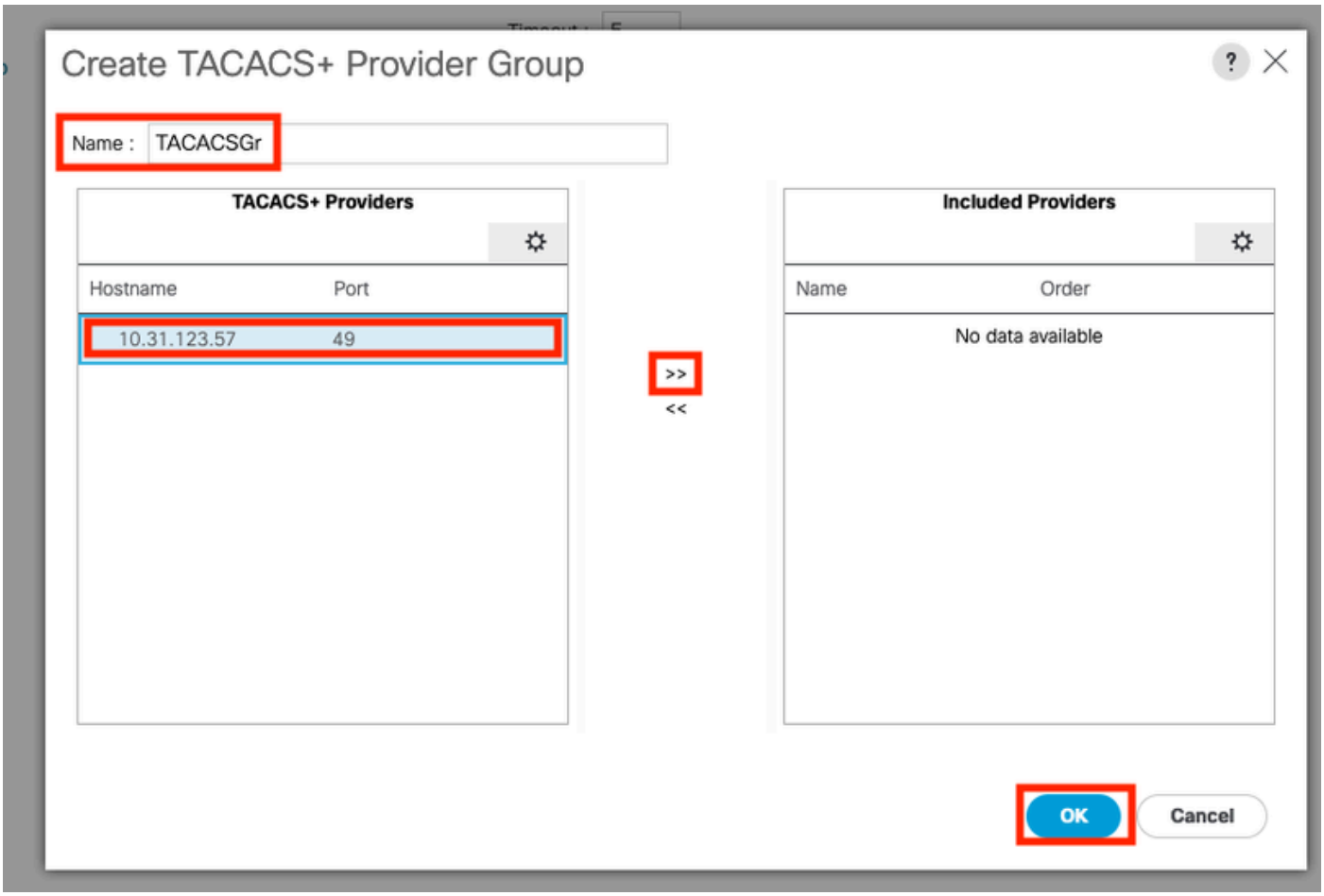
Étape 3. Dans**Work**le volet, sélectionnez l' **General**onglet.

Étape 4. Dans**Actions**la zone, Create TACACS+ Providersélectionnez**Groupe**.



Étape 5. Dans la boîte de dialogue Créer un groupe de fournisseurs TACACS+, entrez les informations requises.

- Dans le champ Nom, entrez un nom unique pour le groupe.
- Dans le tableau Fournisseurs TACACS+, sélectionnez les fournisseurs à inclure dans le groupe.
- Cliquez sur le bouton >> pour ajouter les fournisseurs au tableau Fournisseurs inclus.



Étape 6. Sélectionnez Ok.

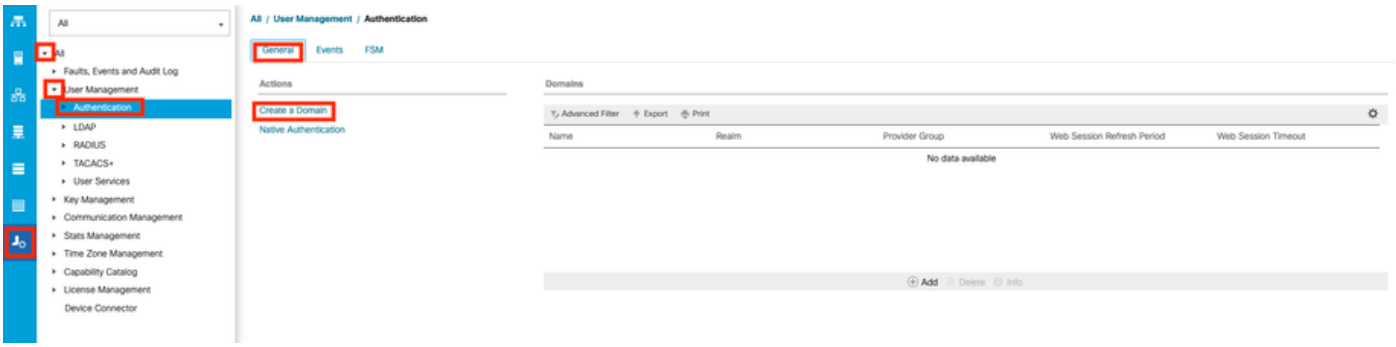
Créer un domaine d'authentification

Étape 1. Dans le **Navigation** volet, sélectionnez l' **Admin**onglet.

Étape 2. Dans l' **Admin**onglet, développez **All** > **User Management** > **Authentication**

Étape 3. Dans**Work**le volet, sélectionnez l' **General**onglet.

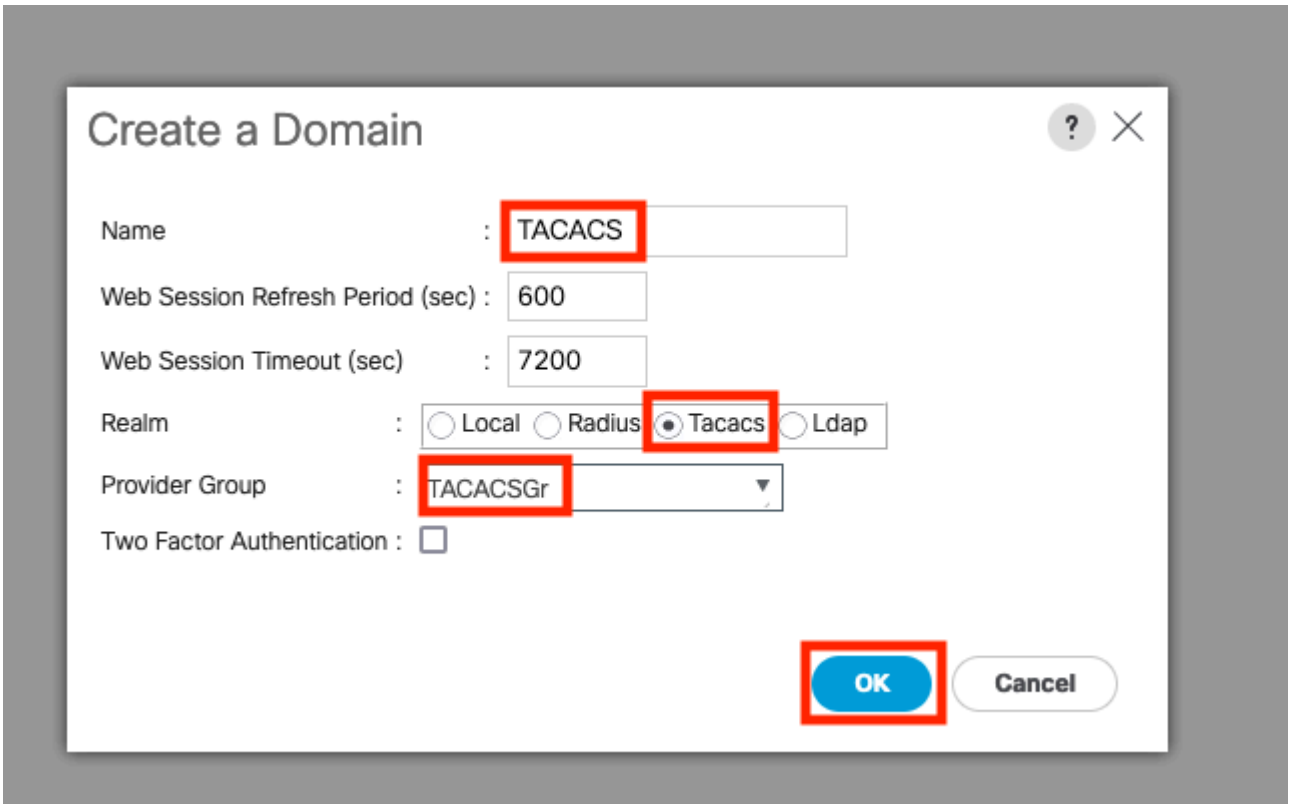
Étape 4. Dans**Actions**la zone, sélectionnez**Create a Domain.**



Étape 5. Dans la boîte de dialogue Créer un domaine, entrez les informations requises.

- Dans le champ Nom, entrez un nom unique pour le domaine.
- Dans le domaine, sélectionnez l'option Tacacs.

- Dans la liste déroulante Groupe de fournisseurs, sélectionnez le groupe de fournisseurs TACACS+ précédemment créé et cliquez sur OK



Dépannage

Problèmes courants de TACACS+ sur UCSM

- Clé incorrecte ou caractères non valides.
- Port incorrect.
- Aucune communication avec notre fournisseur en raison d'une règle de pare-feu ou de proxy.
- FSM n'est pas à 100 %.

Vérification de la configuration UCSM TACACS+ :

Vous devez vous assurer que l'UCSM a mis en oeuvre la configuration en vérifiant que l'état de la Finite State Machine (FSM) est indiqué comme 100% terminé.

Vérification de la configuration à partir de la ligne de commande 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:
```

Vérifiez la configuration de Tacacs à partir de NXOS :

<#root>

UCS-A#

connect nxos

UCS-A(nx-os)#

show tacacs-server

UCS-A(nx-os)#

show tacacs-server groups

```
[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)# show tacacs-server
timeout value:5
deadtime value:0
source interface:any available
Global Test Username:test
Global Test Password:*******
total number of servers:1

following TACACS+ servers are configured:
        10.31.123.57:
                available on port:49
                TACACS+ shared secret:********
                timeout:5
[UCS-AS-MXC-P25-02-A(nx-os)# show tacacs-server groups
total number of groups:2

following TACACS+ server groups are configured:
        group tacacs:
                server 10.31.123.57 on port 49
                deadtime is 0
                vrf is management
        group TACACSGr:
                server 10.31.123.57 on port 49
                deadtime is 0
                vrf is management
```

Afin de tester l'authentification à partir de NX-OS, utilisez**test aaa**la commande (disponible uniquement à partir de NXOS).

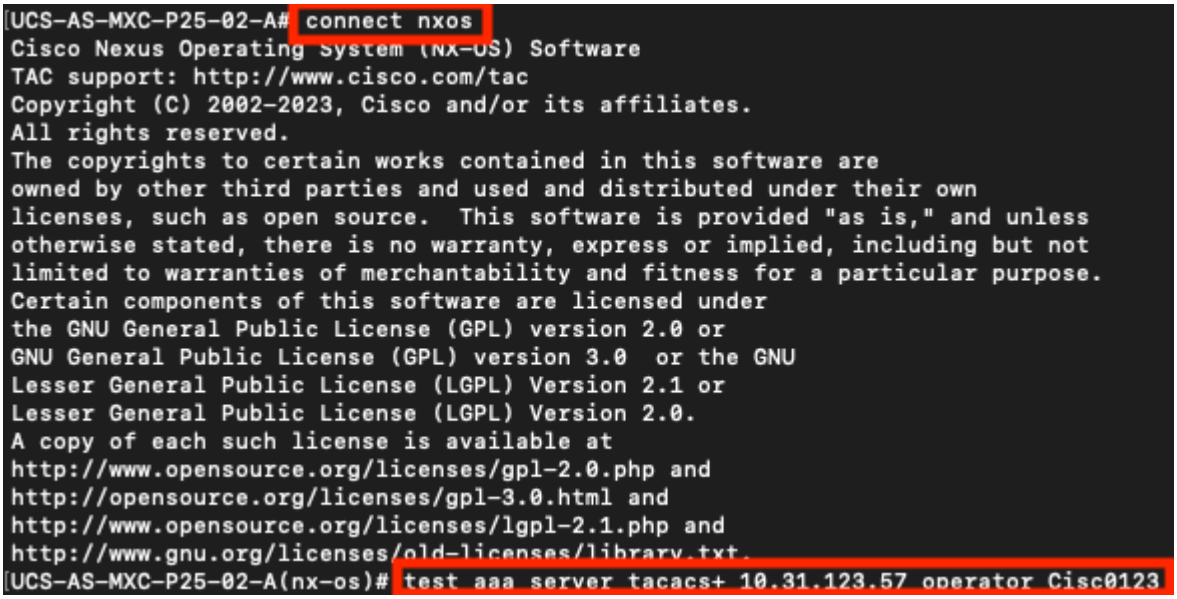
Validez la configuration de votre serveur :

<#root>

UCS-A(nx-os)#

test aaa server tacacs+

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



Révision UCSM

Vérification de l'accessibilité

<#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
```

Vérification du port

<#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 '^]'.
```

La méthode la plus efficace pour voir les erreurs est d'activer le débogage NXOS, avec ce résultat, vous pouvez voir les groupes, la connexion et le message d'erreur qui provoque une mauvaise communication.

- Ouvrez une session SSH sur UCSM et connectez-vous avec n'importe quel utilisateur disposant d'autorisations d'administrateur (de préférence un utilisateur local), passez au contexte CLI de NX-OS et démarrez le moniteur de terminal.

<#root>

UCS-A#

connect nxos

UCS-A(nx-os)#

terminal monitor

- Activez les indicateurs de débogage et vérifiez le résultat de la session SSH dans le fichier journal.

<#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

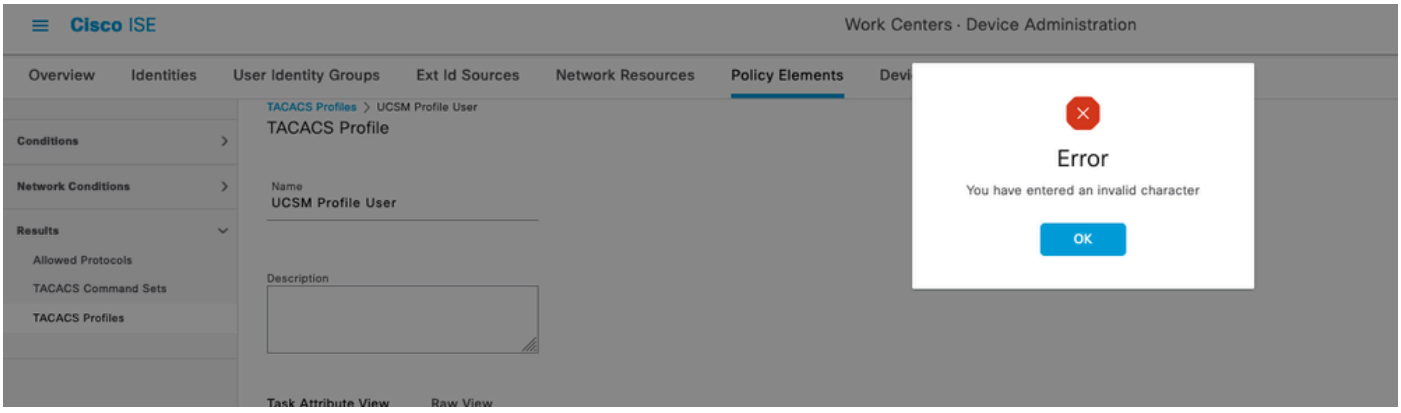
```
UCS-AS-MXC-P25-02-A# connect nxos
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2023, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and 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
```

- Ouvrez une nouvelle session GUI ou CLI et essayez de vous connecter en tant qu'utilisateur distant (TACACS+).
- Une fois que vous avez reçu un message d'échec de connexion, désactivez les débogages fermant la session ou avec cette commande.

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

Problèmes courants des TACAC sur ISE

- Dans ISE, ce comportement s'affiche lors de la tentative de configuration du profil tacacs dans les attributs nécessaires à UCSM pour attribuer les rôles correspondants pour admin ou tout autre rôle, sélectionnez sur le bouton d'enregistrement et ce comportement s'affiche :



Cette erreur est due au bogue suivant : https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwc91917, veuillez vous assurer que vous avez bien l'endroit où ce défaut a été corrigé.

Évaluation ISE

Étape 1. Vérifiez si la facilité de maintenance TACACS+ est en cours d'exécution. Vous pouvez l'intégrer :

- IUG: Vérifiez si le noeud est répertorié avec le service DEVICE ADMIN dans Administration > System > Deployment.
- CLI : Exécutez la commande show ports | inclure 49 pour confirmer que le port TCP contient des connexions appartenant à TACACS+

<#root>

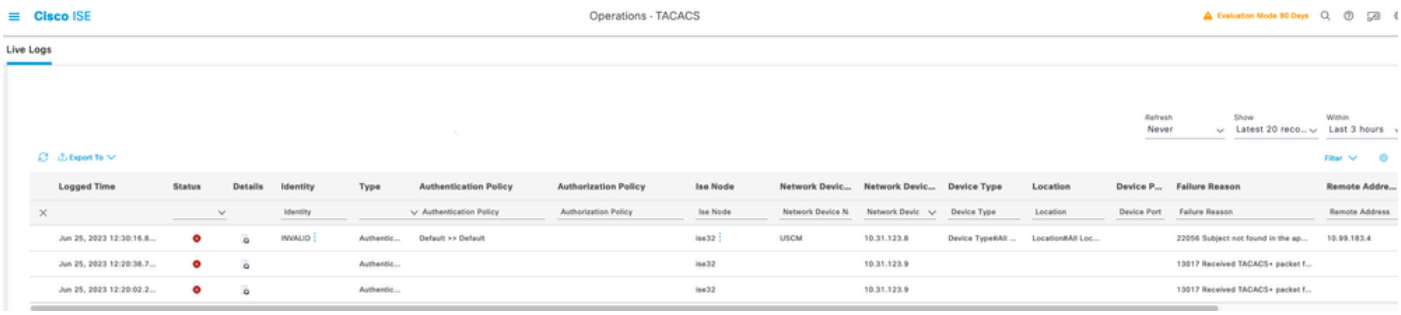
```
ise32/admin#
```

show ports | include 49

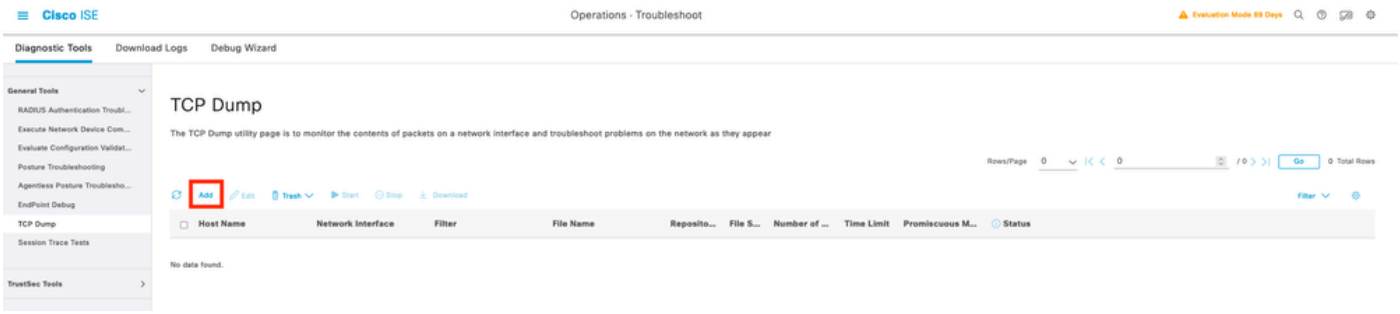
```
tcp: 169.254.4.1:49, 169.254.2.1:49, 169.254.4.1:49, 10.31.123.57:49
```

Étape 2. Vérifiez s'il existe des journaux en direct concernant les tentatives d'authentification TACACS+ : vous pouvez le vérifier dans le menu Operations > TACACS > Live logs ,

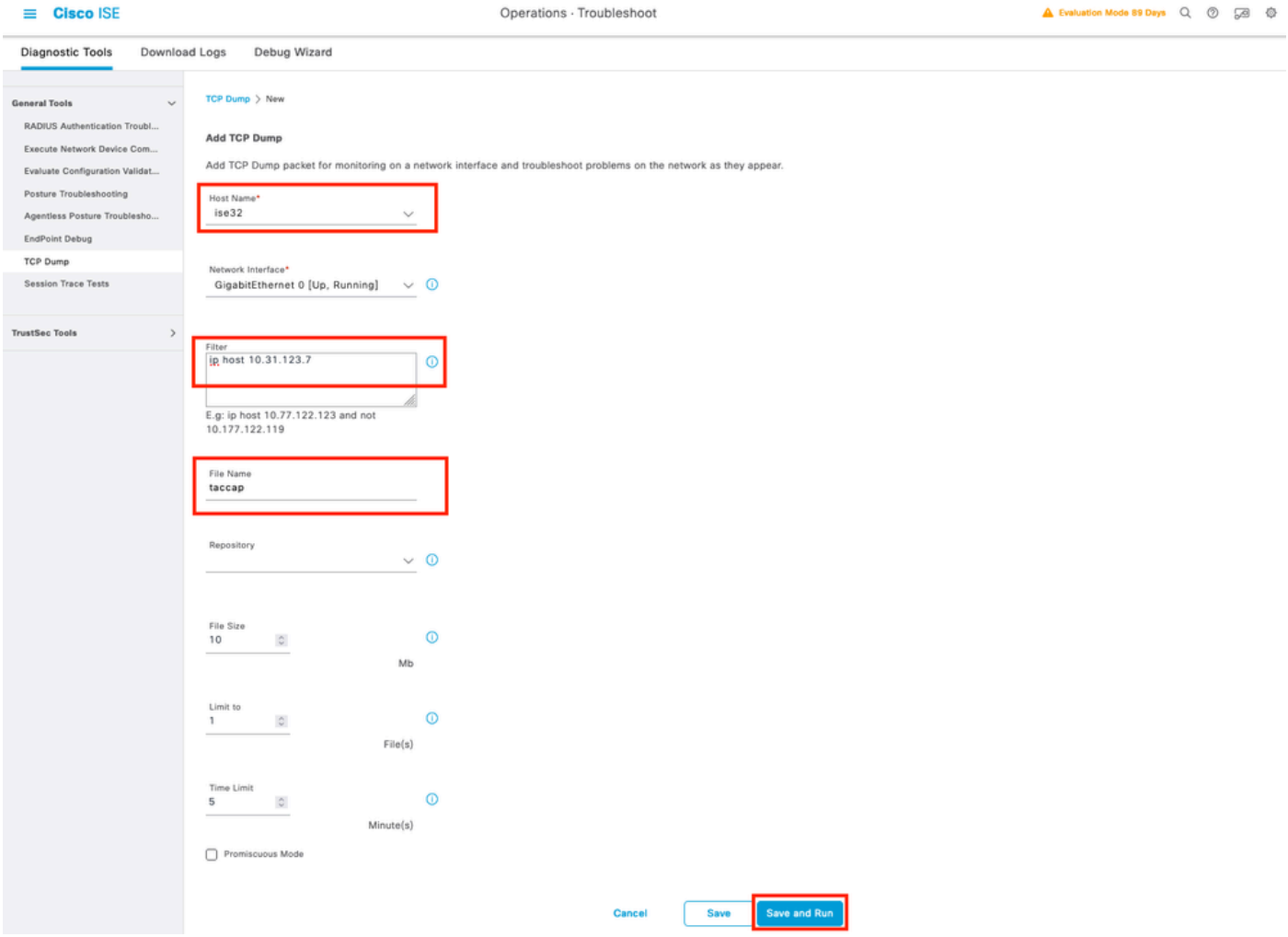
En fonction de la raison de l'échec, vous pouvez ajuster votre configuration ou résoudre la cause de l'échec.



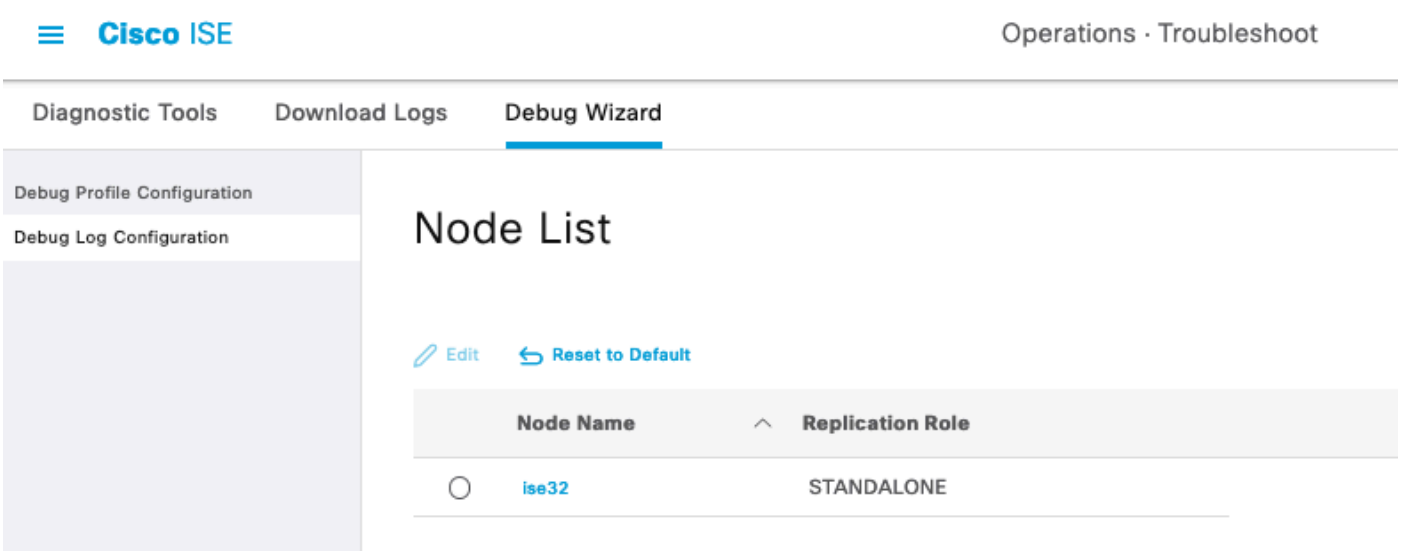
Étape 3. Si vous ne voyez pas de journal en direct, passez à une capture de paquets. Naviguez jusqu'au menu Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump , sélectionnez on add



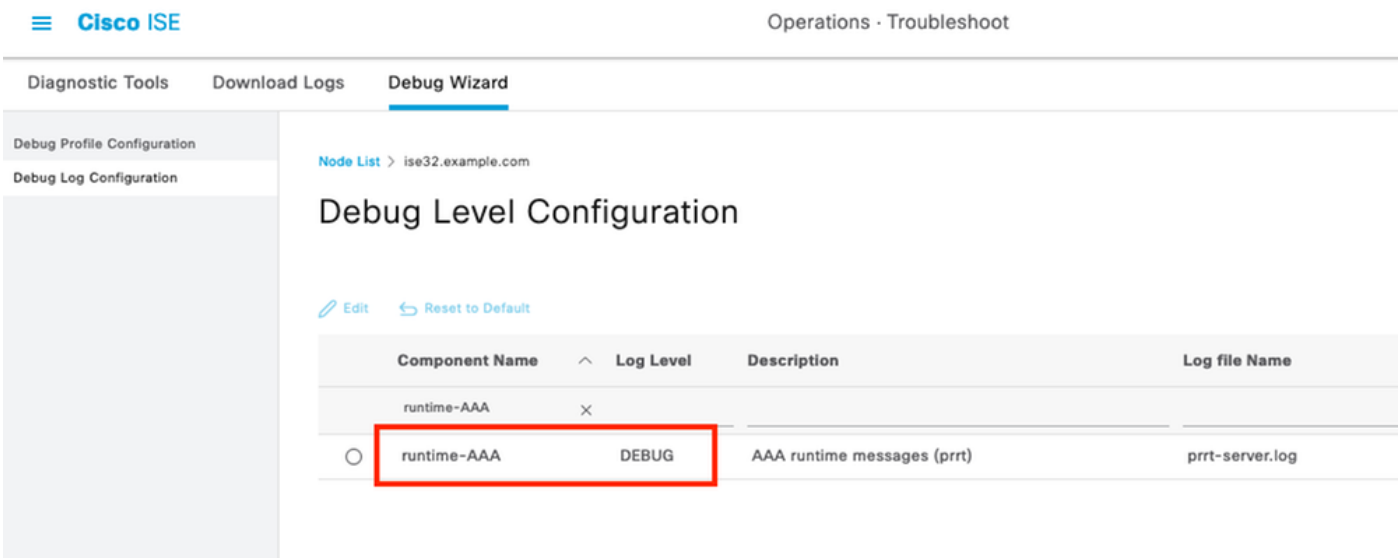
Sélectionnez le noeud Service de stratégie à partir duquel l'UCSM envoie l'authentification, puis dans les filtres, entrez ip host X.X.X.X correspondant à l'IP de l'UCSM à partir duquel l'authentification est envoyée, nommez la capture et faites défiler vers le bas pour enregistrer, exécuter la capture et vous connecter à partir de l'UCSM .



Étape 4. Activez le composant runtime-AAA dans debug dans le PSN à partir de l'endroit où l'authentification est effectuée dans Operations > Troubleshoot > Debug Wizard > Debug log configuration, sélectionnez PSN node , sélectionnez ensuite next in edit button .



Recherchez le composant runtime-AAA et modifiez son niveau en debug pour reproduire le problème à nouveau, puis analysez les journaux .



Remarque : Pour plus d'informations, reportez-vous à la vidéo de la chaîne Cisco Youtube How to Enable Deugs on ISE 3.x Versions https://www.youtube.com/watch?v=E3USz8B76c8 .

Informations connexes

Guide d'administration de Cisco UCS Manager

Guide de configuration de Cisco UCS CIMC TACACS+

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.