# Configuration de l'authentification TACACS+ sur le commutateur Arista avec ISE

## Table des matières



## Introduction

Ce document décrit comment intégrer Cisco ISE TACACS+ avec un commutateur Arista pour un AAA centralisé d'accès administrateur.

## Conditions préalables

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco ISE et le protocole TACACS+.
- commutateurs Arista

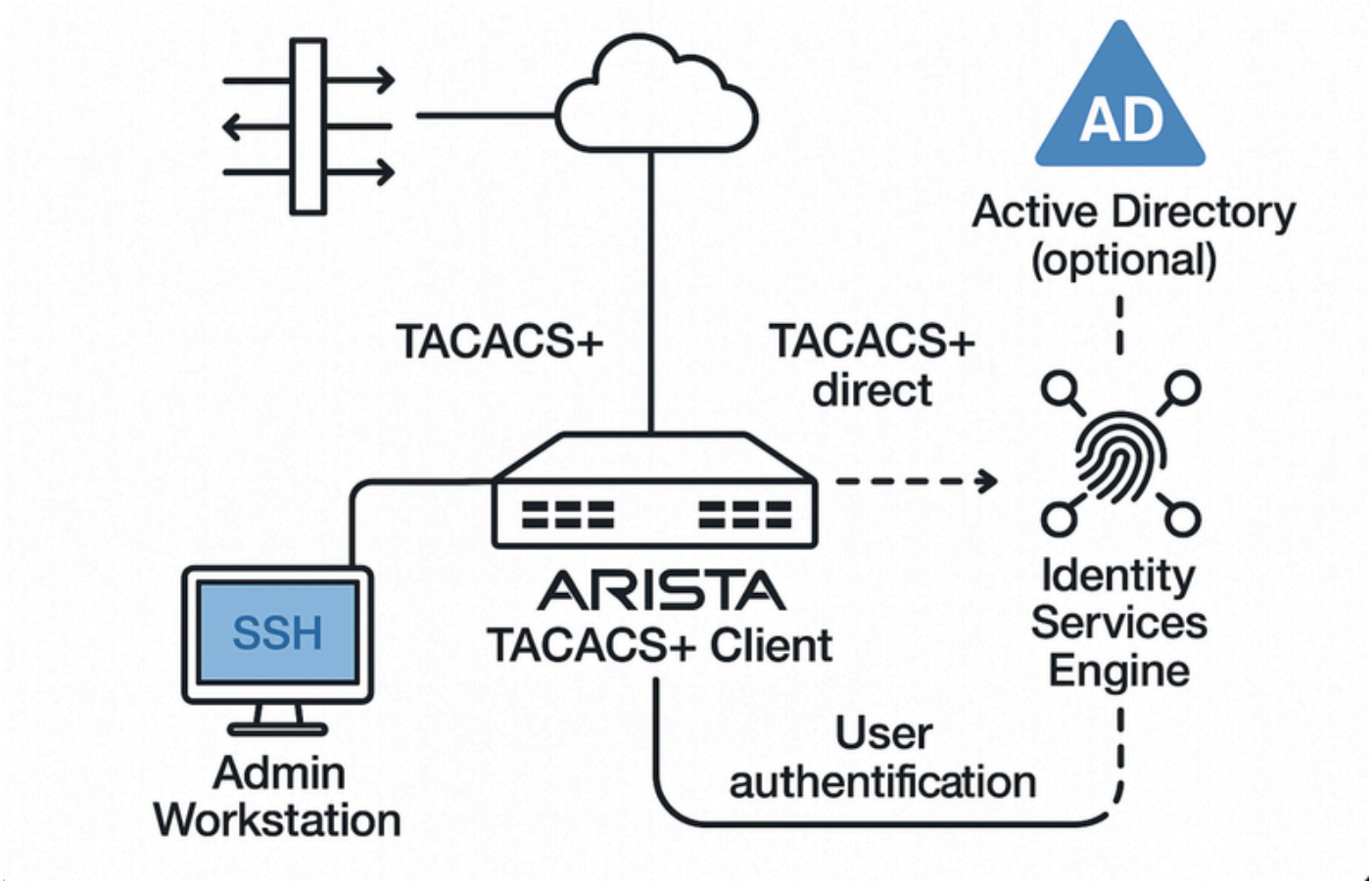
## Composants utilisés

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

- Version de l'image logicielle du commutateur Arista : 4,33,2 F
- Cisco Identity Services Engine (ISE) version 3.3 Patch 4

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

## Diagramme du réseau

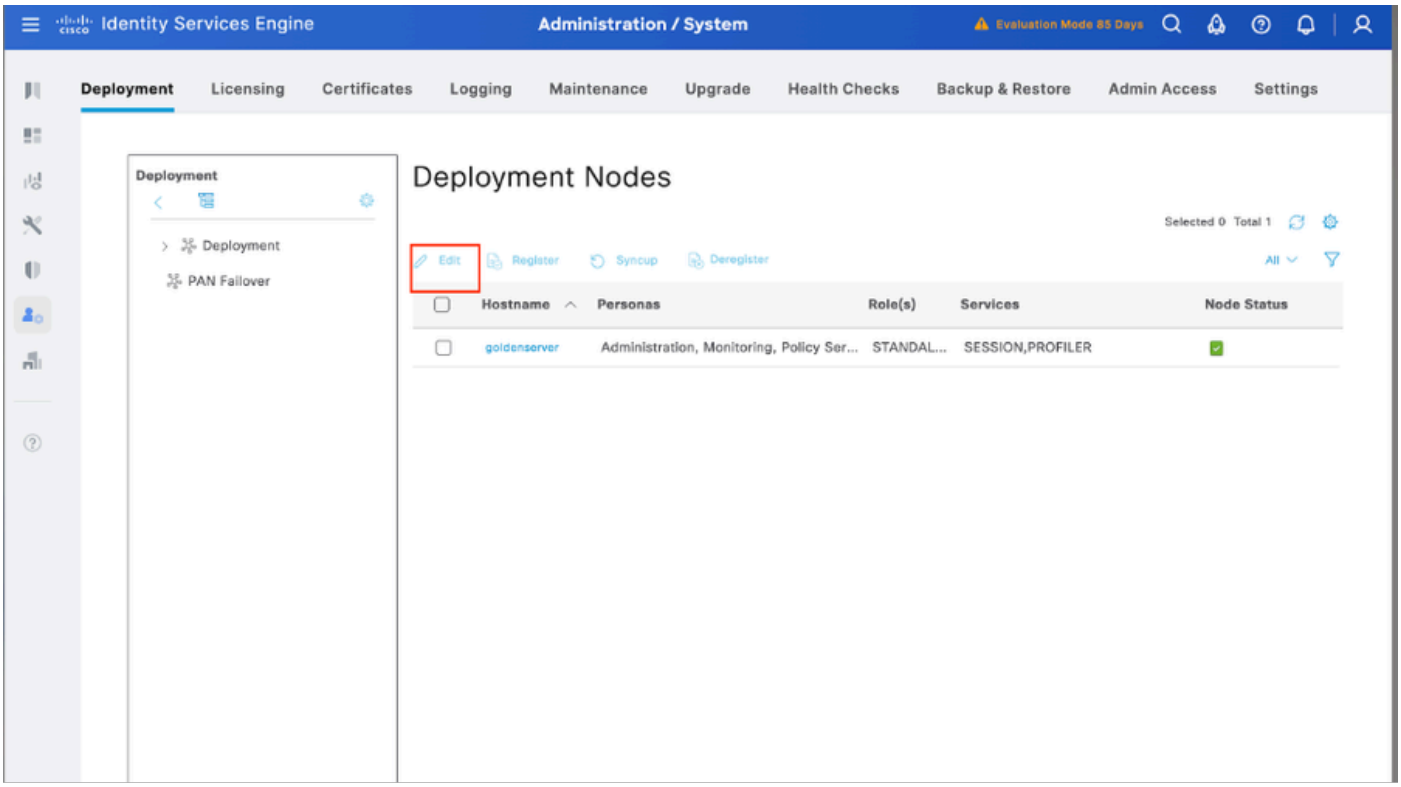



## Configurations

### Configuration de TACACS+ sur ISE

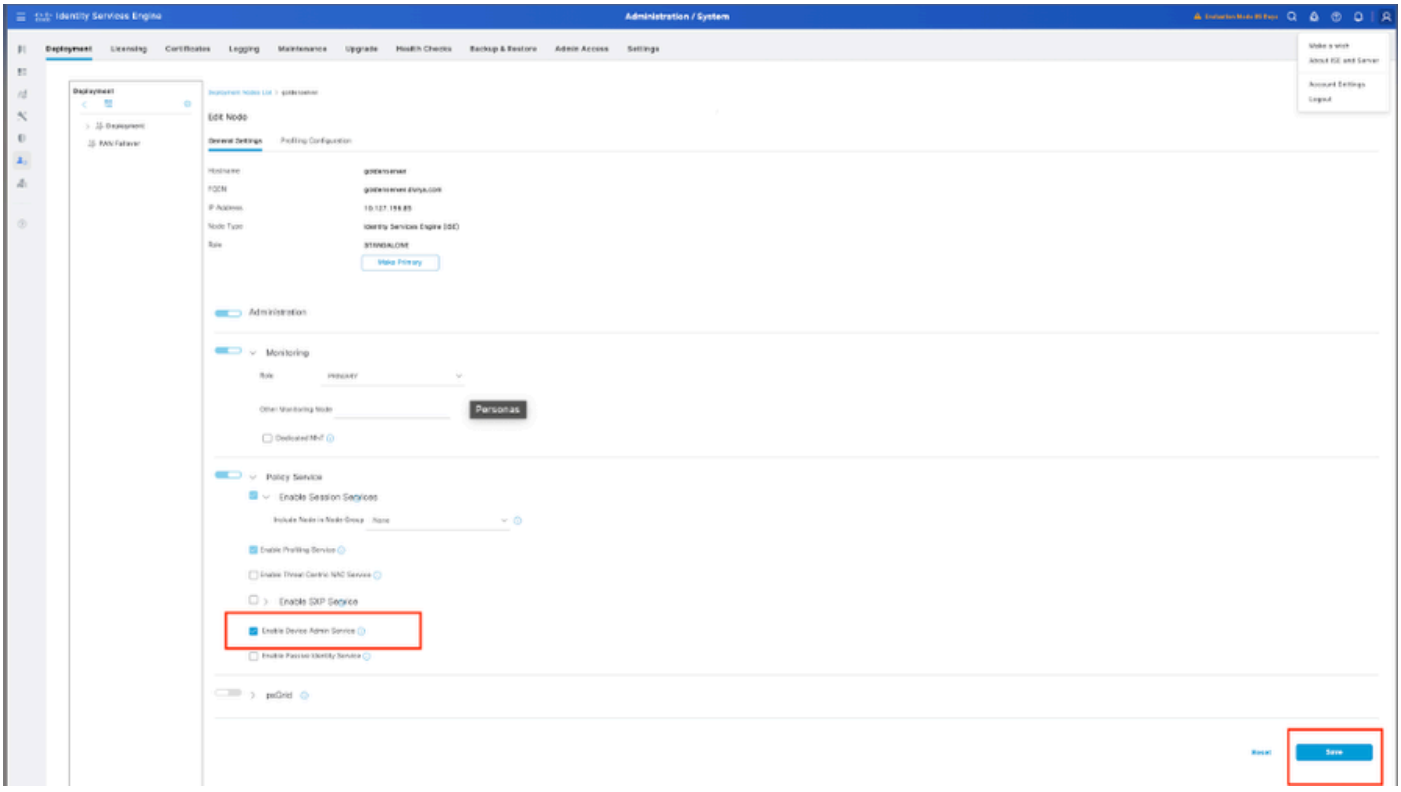
Étape 1. L'étape initiale consiste à vérifier si Cisco ISE dispose des capacités nécessaires pour gérer l'authentification TACACS+. Pour ce faire, vérifiez que la fonctionnalité Device Admin Service est activée sur le noeud Service de stratégie (PSN) souhaité.

Accédez à Administration > System > Deployment, sélectionnez le noeud approprié où ISE traite l'authentification TACACS+, et cliquez sur Edit pour revoir sa configuration.




Étape 2. Faites défiler la page vers le bas pour localiser la fonction Device Administration Service. Notez que l'activation de cette fonctionnalité nécessite que le personnel Policy Service soit actif sur le noeud, ainsi que les licences TACACS+ disponibles dans le déploiement.

Cochez la case pour activer la fonction, puis enregistrez la configuration.

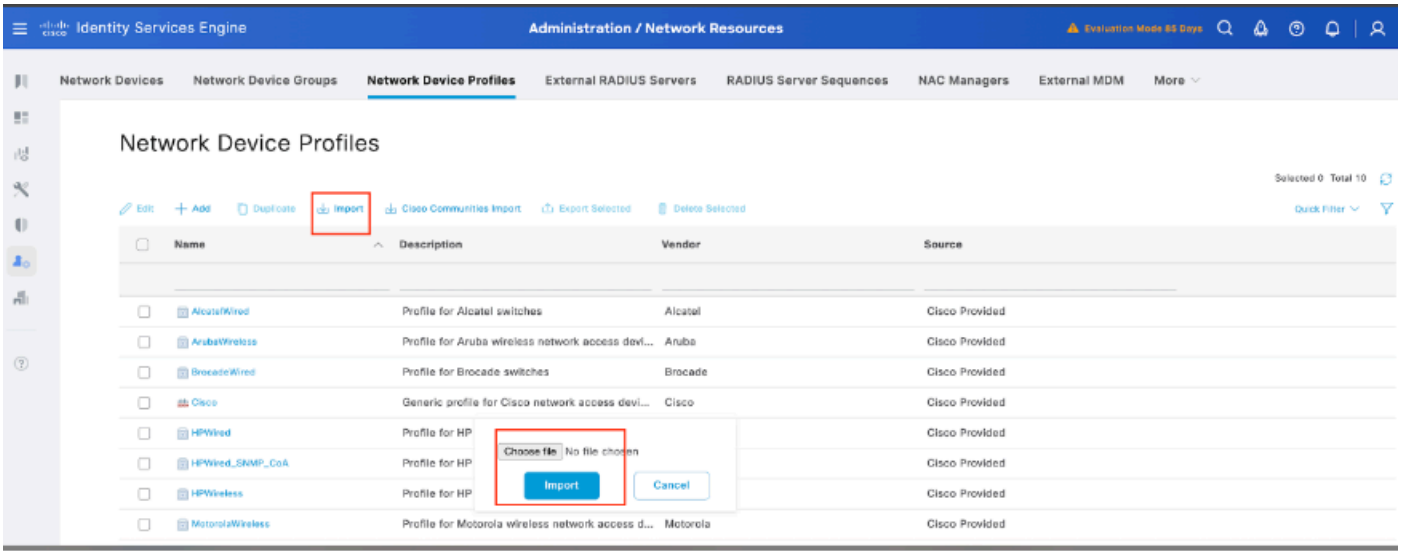



Étape 3. Obtention du profil de périphérique réseau Arista pour Cisco ISE

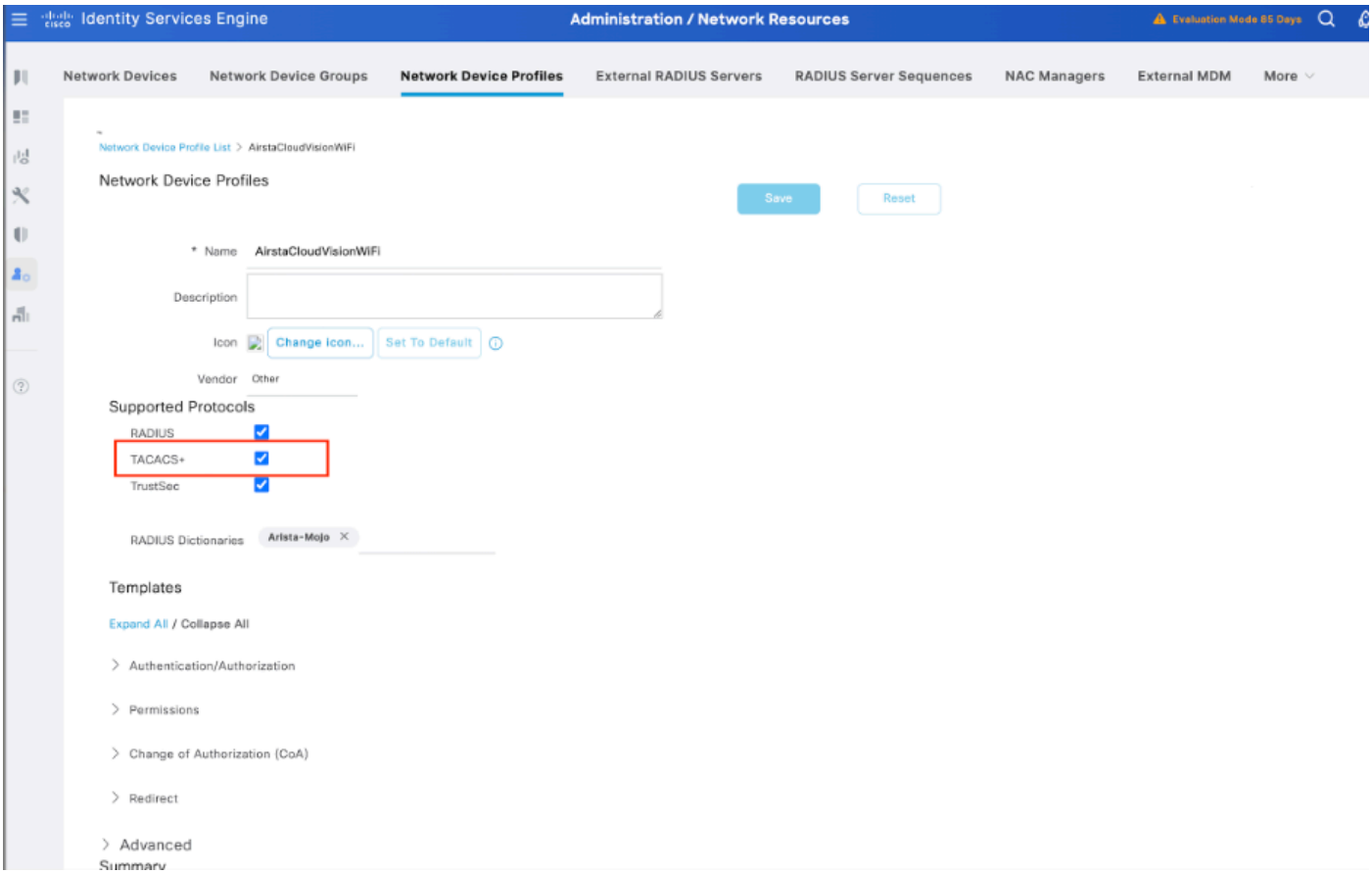
La communauté Cisco a partagé un profil NAD dédié pour les périphériques Arista. Ce profil, ainsi que les fichiers de dictionnaire nécessaires, se trouvent dans l'article Arista CloudVision WiFi Dictionary and NAD Profile for ISE Integration. Le téléchargement et l'importation de ce profil dans votre configuration ISE facilitent l'intégration

Étapes d'importation du profil NAD Arista dans Cisco ISE :

1. Téléchargez le profil :
    - Obtenez le profil NAD Arista à partir du lien Communauté Cisco fourni ci-dessus. Communauté Cisco
2. Accédez à Cisco ISE :
    - Connectez-vous à votre console d'administration Cisco ISE
3. Importer le profil NAD :
    - Accédez à Administration > Network Resources > Network Device Profiles.
    - Cliquez sur le bouton Importer
    - Téléchargez le fichier de profil Arista NAD.

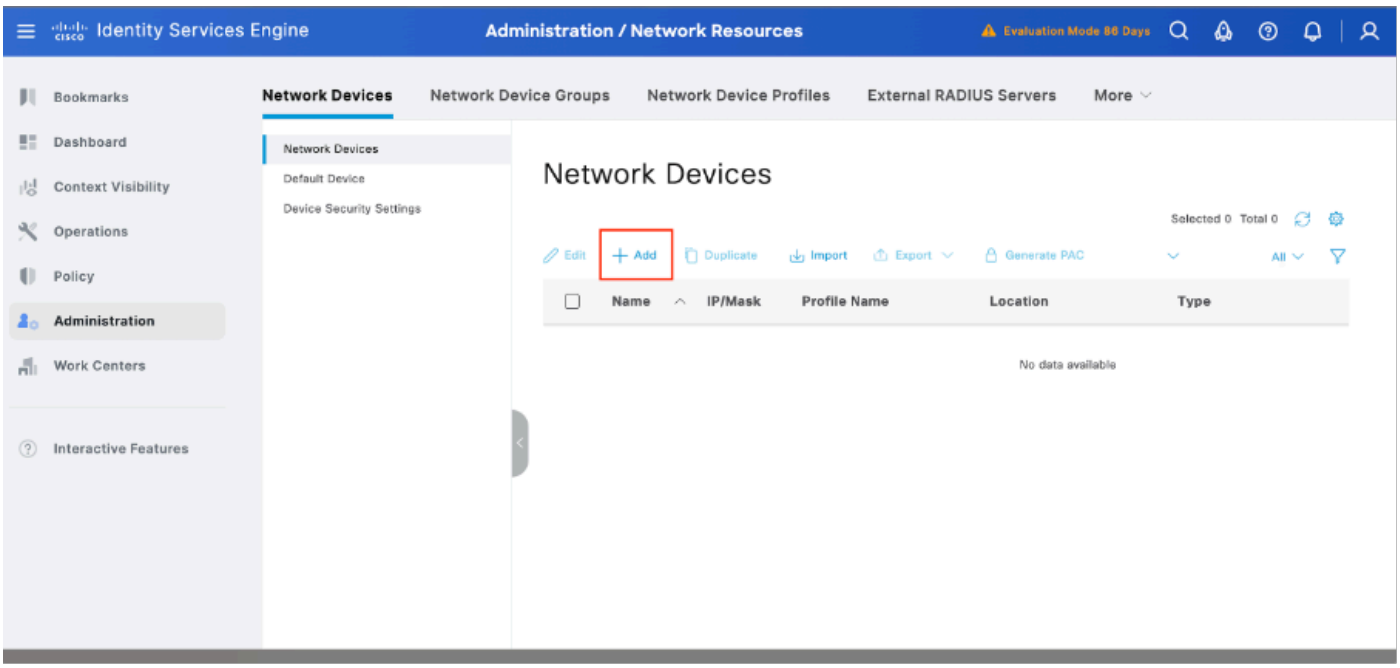



Une fois le téléchargement terminé, accédez à l'option Edit et activez TACACS+ comme protocole pris en charge.




Étape 2 : Ajoutez un commutateur Arista en tant que périphérique réseau.

1. Accédez à Administration > Network Resources > Network Devices > +Add:

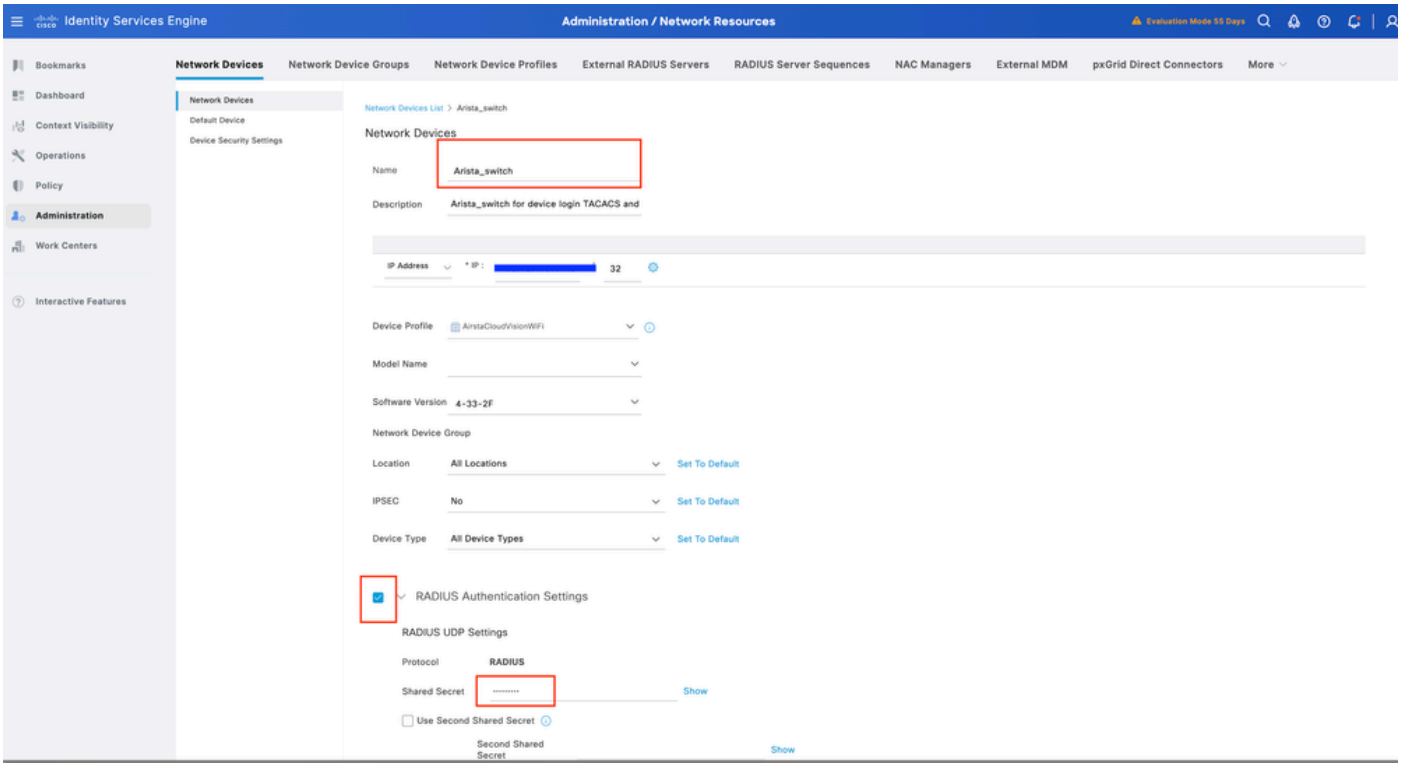



2.Cliquez sur Add et entrez ces détails :

- Adresse IP: <IP du commutateur>
- Type de périphérique : Choisir un autre câblé
- Profil de périphérique réseau : sélectionnez AirstaCloudVisionWiFi.

- Paramètres d'authentification RADIUS :
  - Activez l'authentification RADIUS.
  - Entrez le secret partagé (il doit correspondre à la configuration du commutateur).

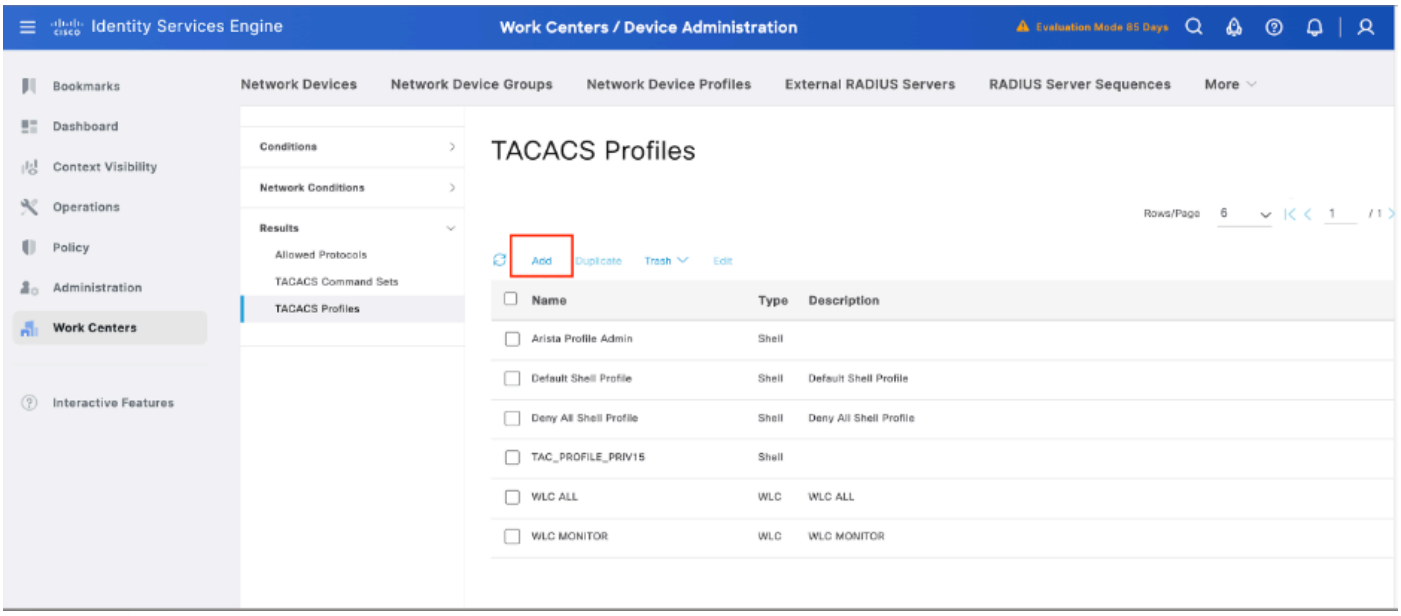
3. Cliquez sur Enregistrer :



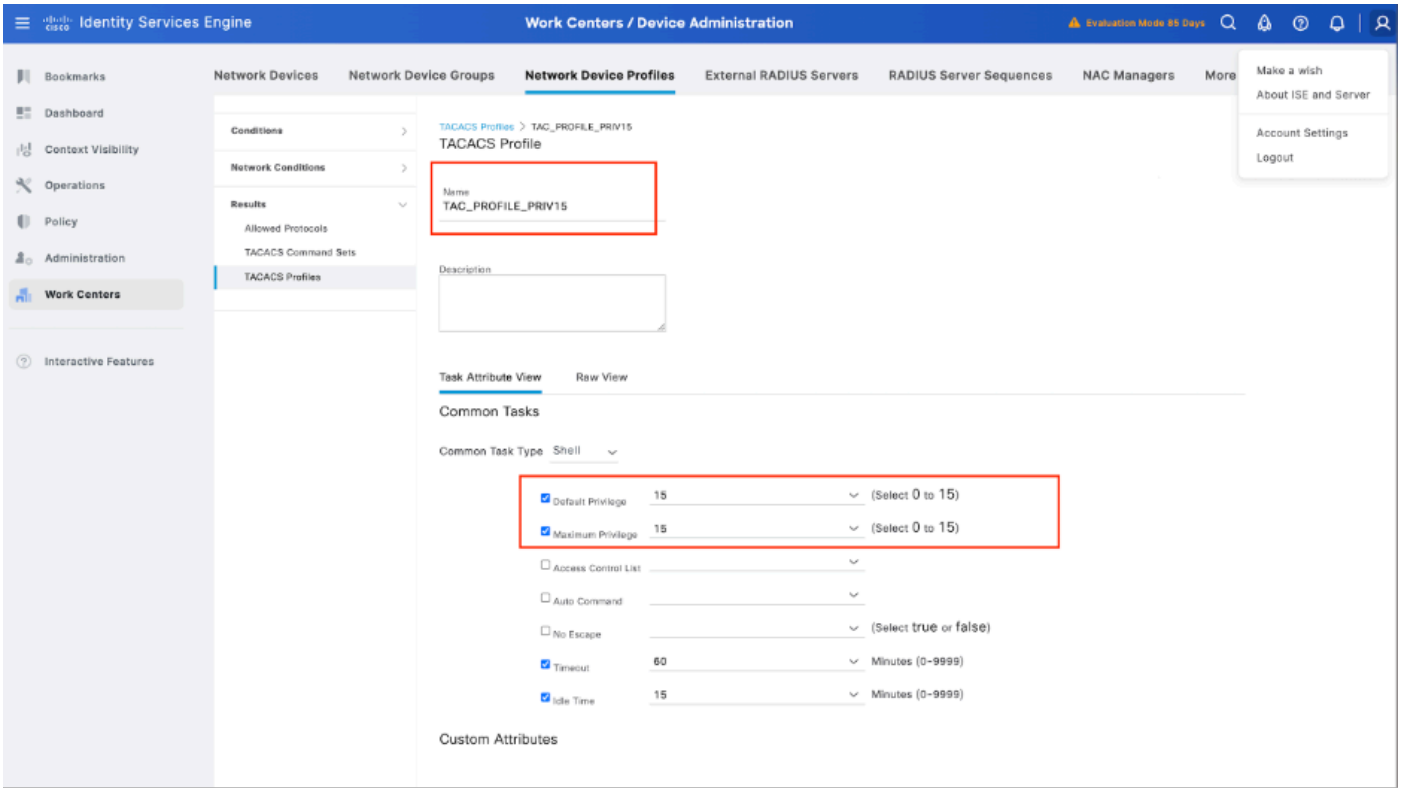

Étape 3. Validez le nouveau périphérique comme indiqué sous Network Devices :


Étape 4 : configuration du profil TACACS

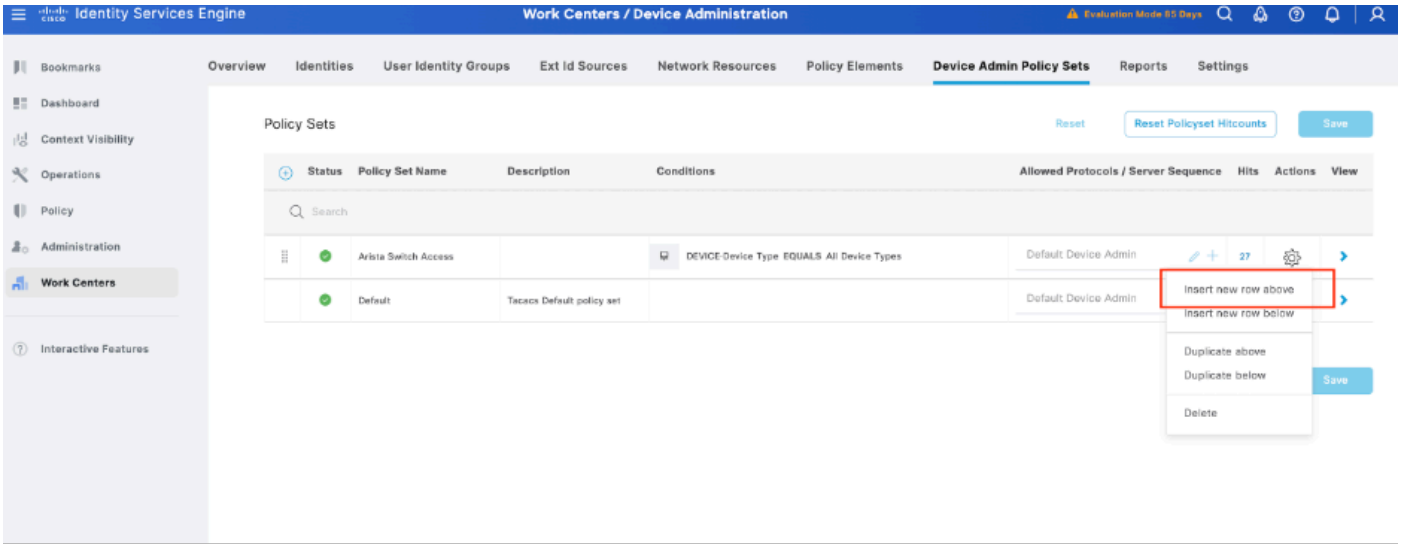
Créez un profil TACACS, accédez au menu Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles, puis sélectionnez Add :



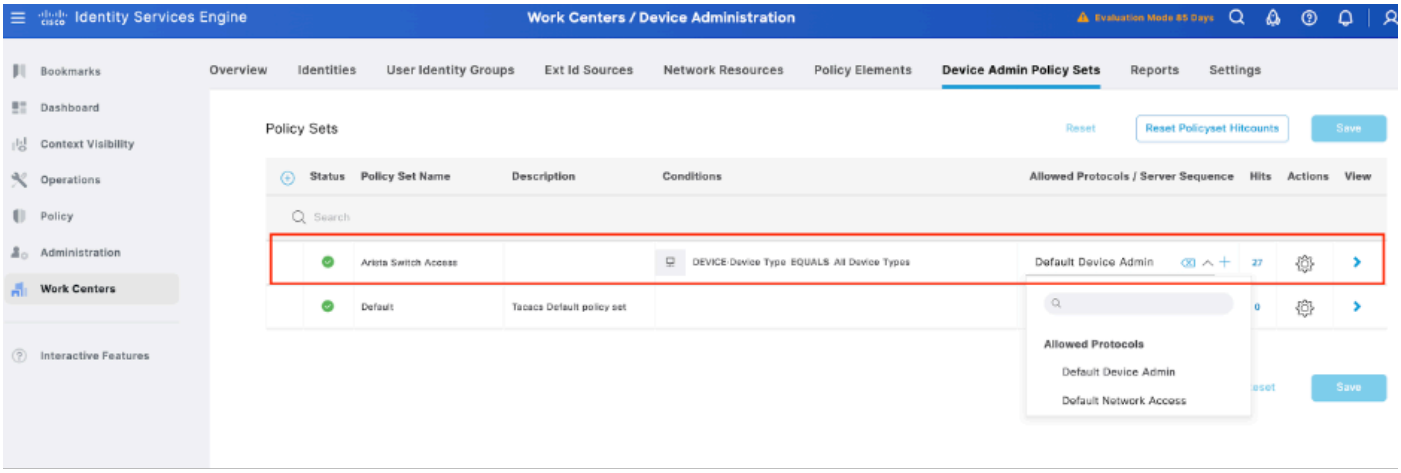

Saisissez un nom, cochez la case Privilège par défaut et définissez la valeur sur 15. En outre, sélectionnez Privilège maximal, définissez sa valeur sur 15, puis cliquez sur Soumettre :



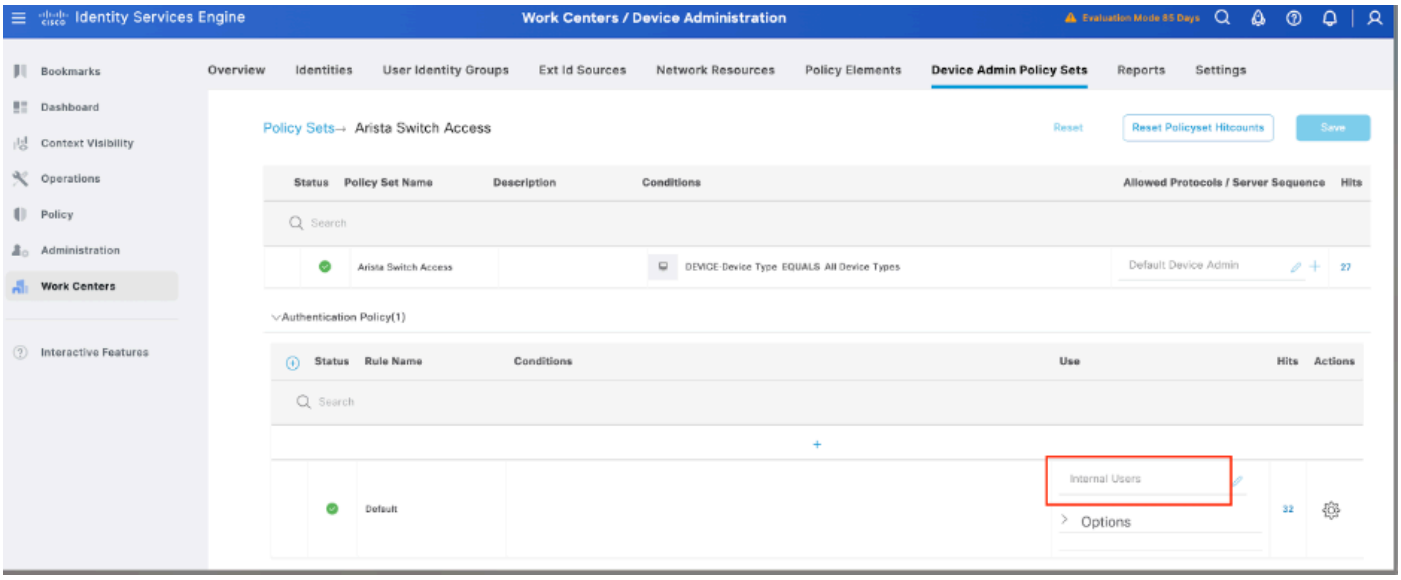

Étape 5. Créez un ensemble de stratégies d'administration de périphériques à utiliser pour votre commutateur Arista, accédez au menu Work Centers > Device Administration > Device Admin Policy Sets, puis, à partir d'un ensemble de stratégies existant, sélectionnez l'icône d'engrenage pour ensuite sélectionner Insert new row above.




Étape 6. Nommez ce nouvel ensemble de stratégies, ajoutez des conditions en fonction des caractéristiques des authentifications TACACS+ en cours à partir du commutateur Arista, et sélectionnez Allowed Protocols > Default Device Admin, enregistrez votre configuration.

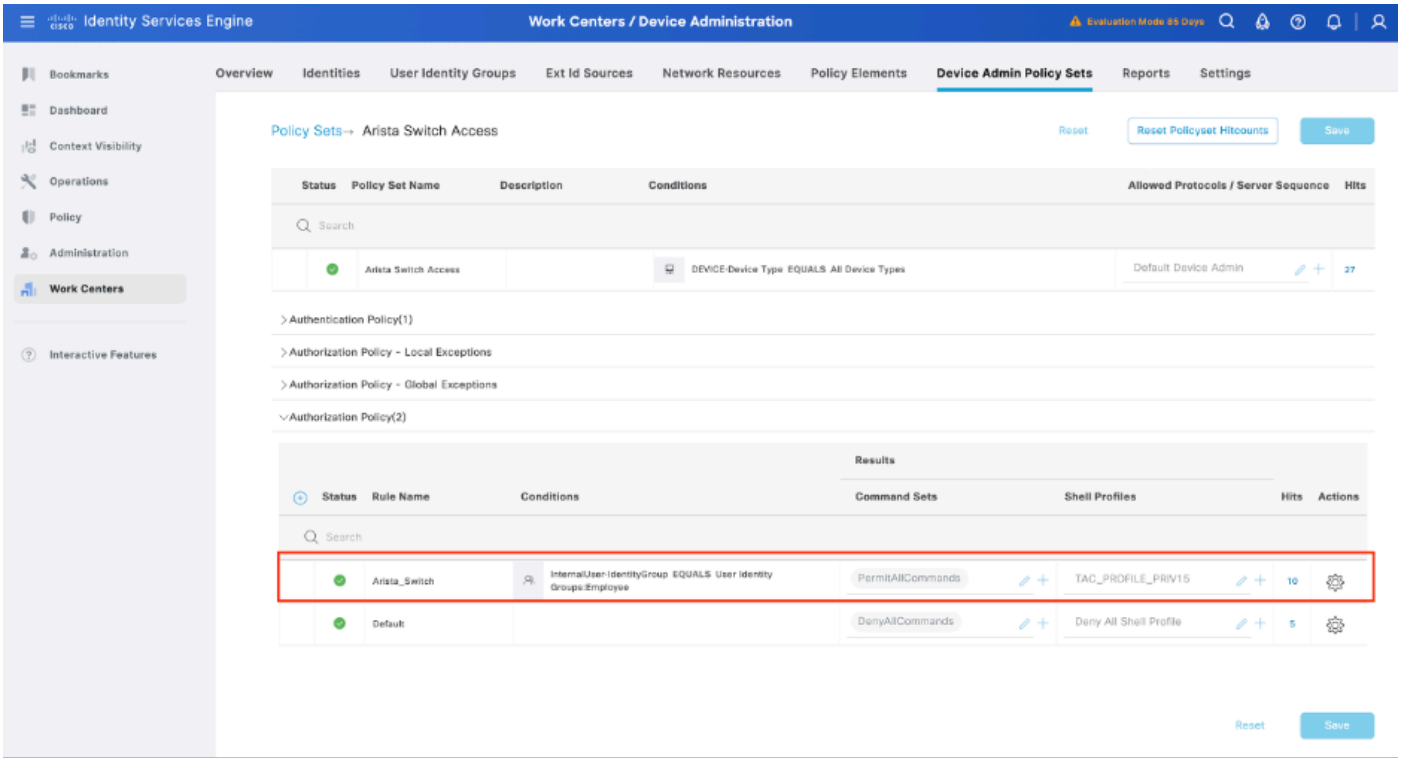



Étape 7. Sélectionnez l'option > view, puis dans la section Authentication Policy, sélectionnez la source d'identité externe que Cisco ISE utilise pour interroger le nom d'utilisateur et les informations d'identification pour l'authentification sur le commutateur Arista. Dans cet exemple, les informations d'identification correspondent aux utilisateurs internes stockés dans ISE.




Étape 8. Faites défiler la page jusqu'à la section intitulée Authorization Policy to Default policy, sélectionnez l'icône du rapport, puis insérez une règle ci-dessus.

Étape 9. Attribuez un nom à la nouvelle règle d'autorisation, ajoutez des conditions concernant l'utilisateur qui est déjà authentifié 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 du commutateur Arista

Étape 1 : activation de l'authentification TACACS+

Connectez-vous au commutateur Arista et passez en mode de configuration :

configurer

!

tacacs-server host <ISE-IP> key <TACACS-SECRET>

!

aaa group server tacacs+ ISE_TACACS

  serveur <ISE-IP>

!

aaa authentication login default group ISE_TACACS local

aaa authorization exec default group ISE_TACACS local

aaa accounting commands 15 default start-stop group ISE_TACACS

!

Tranche

Étape 2 : enregistrement de la configuration

Pour conserver la configuration lors des redémarrages :

# mémoire d'écriture

OU

# copy running-config startup-config

# Vérifier

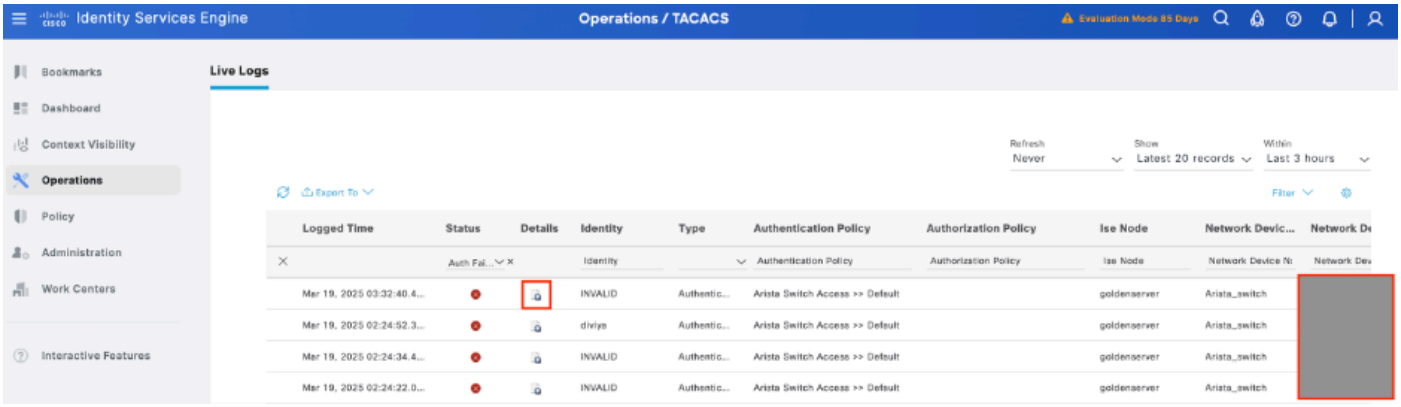
## Évaluation ISE

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

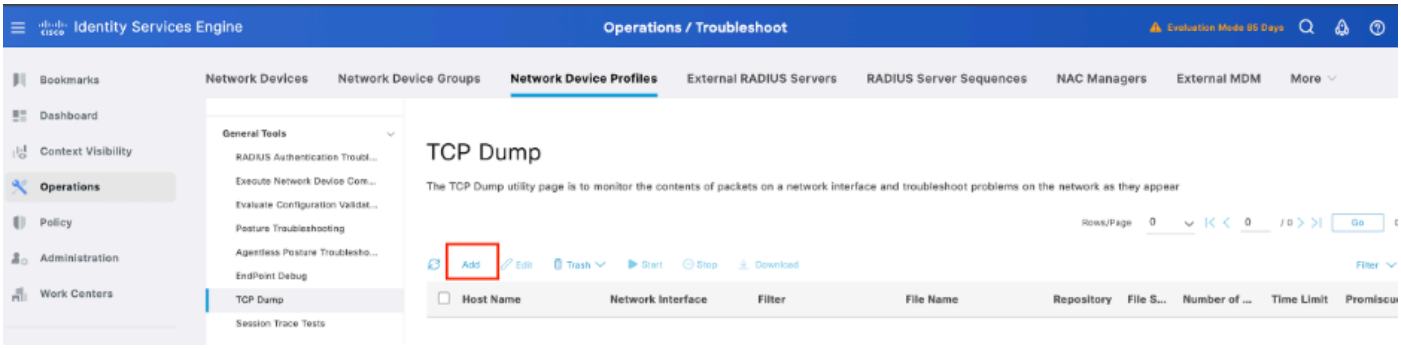
- IUG: Vérifiez si le noeud est répertorié avec le service DEVICE ADMIN dans > System > Deployment.
- CLI : Exécutez la commande show ports | inclure 49 pour confirmer que le port TCP contient des connexions appartenant à TACACS+

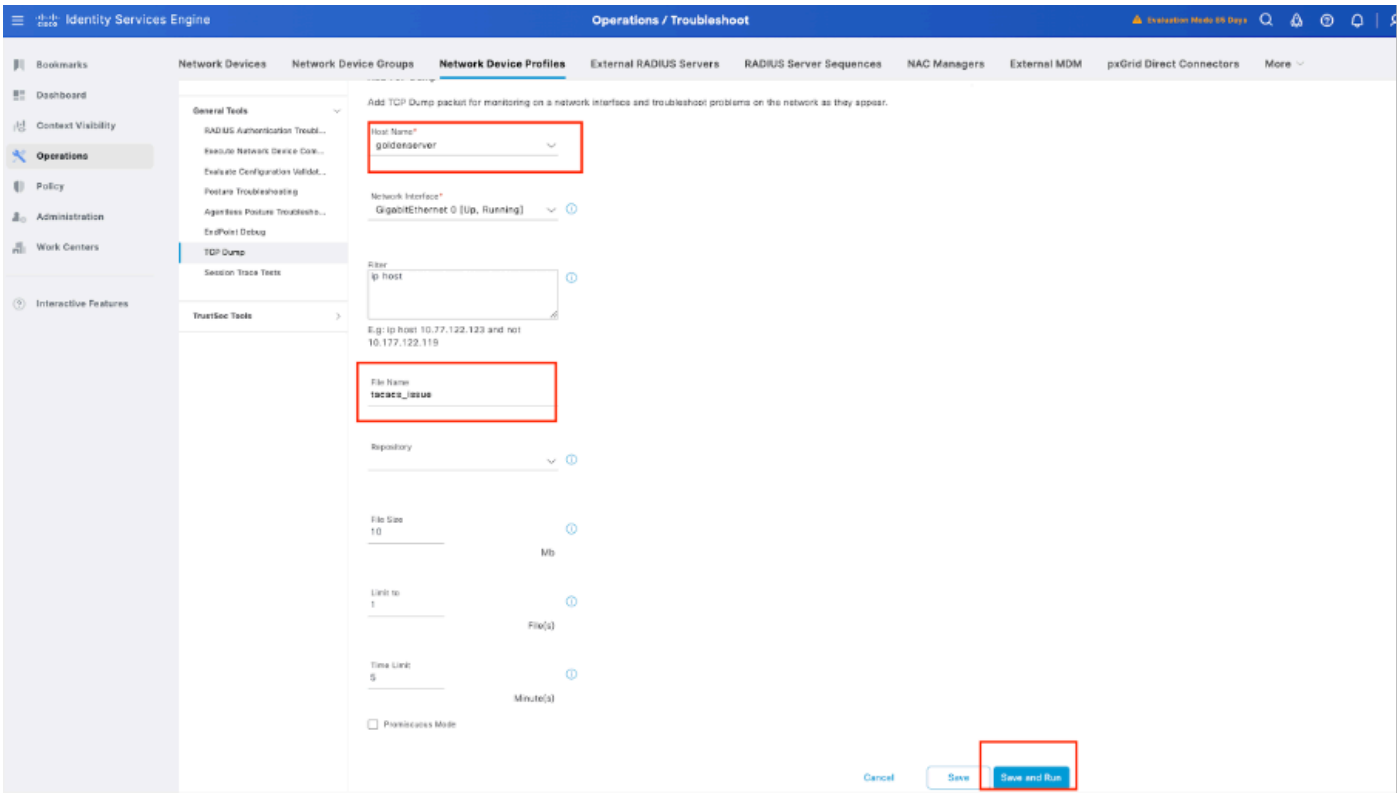
Étape 2. Vérifier s'il existe des journaux en direct concernant les tentatives d'authentification TACACS+ : vous pouvez le vérifier dans le menu Operations > TACACS > Live logs,

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

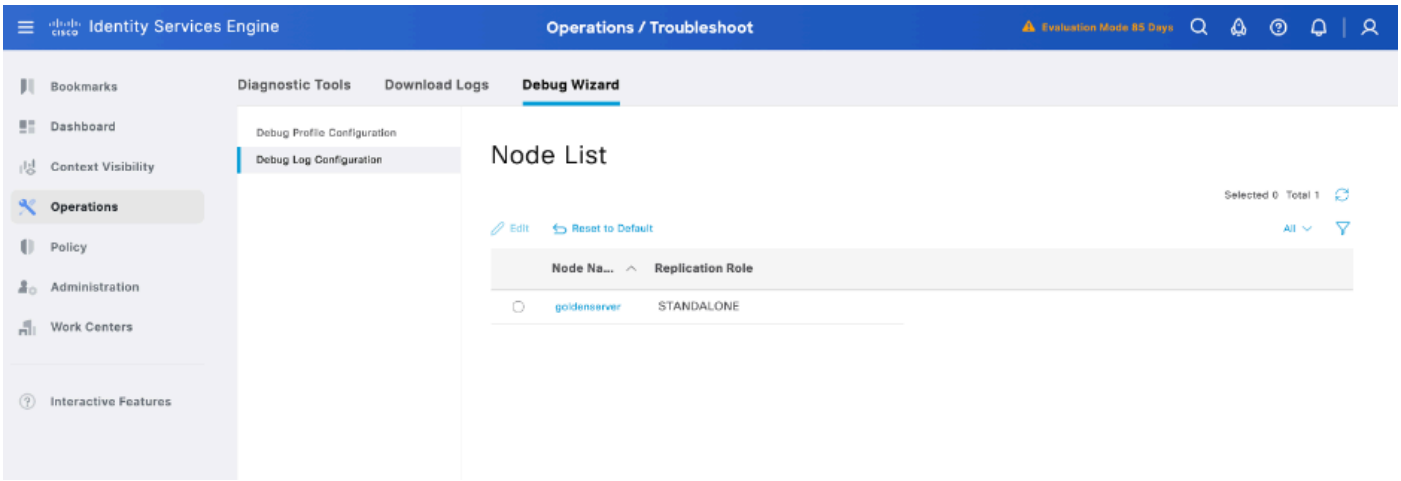


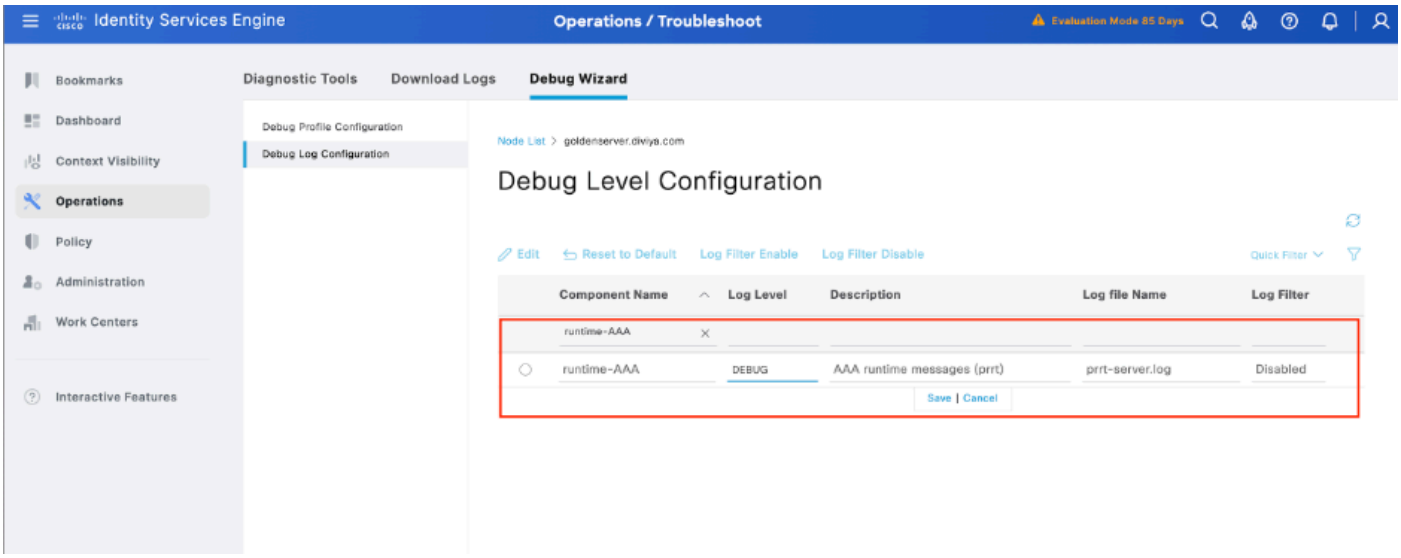

Étape 3. Si vous ne voyez pas de journal en direct, passez à la capture de paquets. Accédez au menu Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump , sélectionnez Add:






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, puis sélectionnez le bouton Edit :





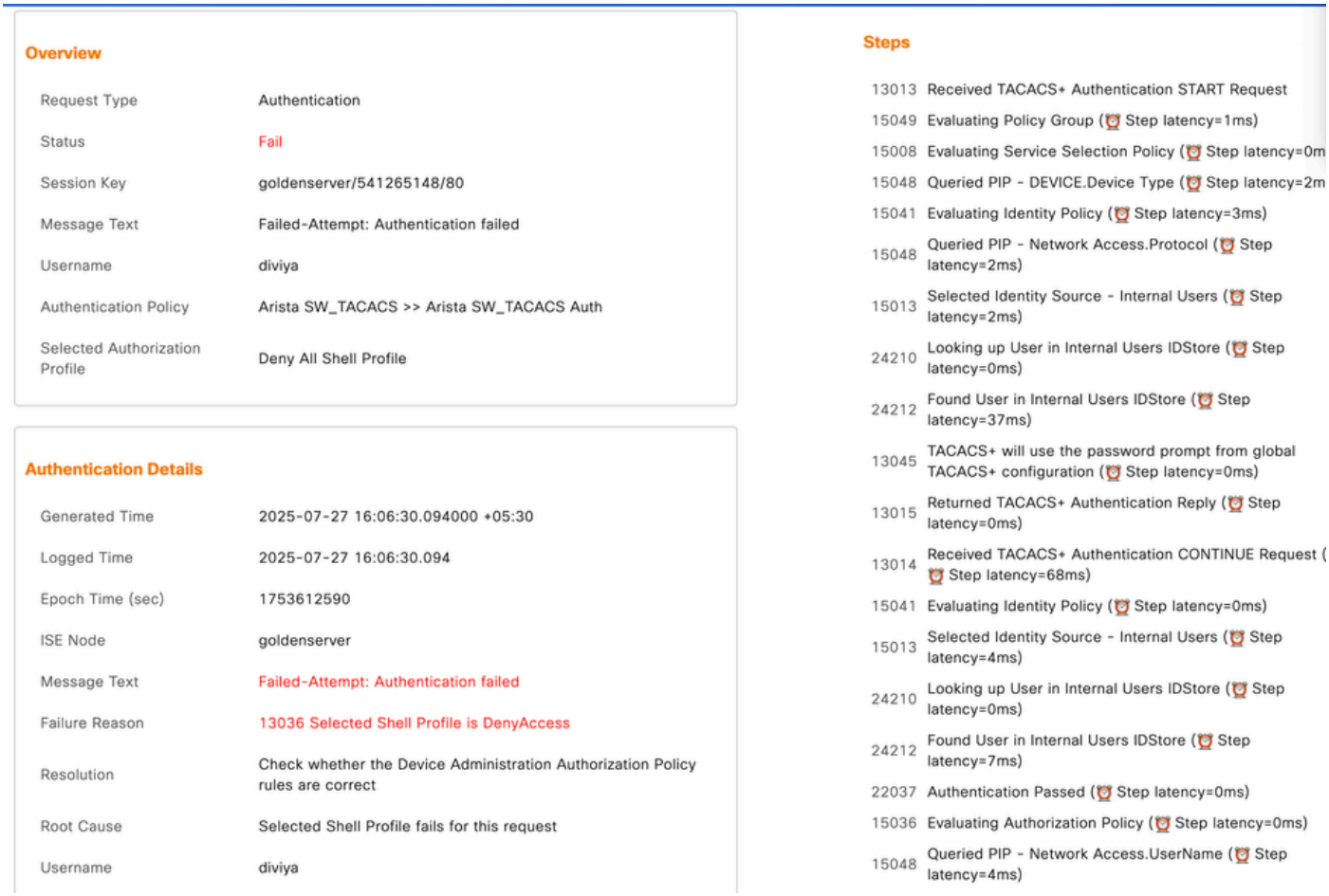

Identifiez le composant runtime-AAA, définissez son niveau de journalisation sur debug, reproduisez le problème et analysez les journaux pour une enquête plus approfondie.

# Dépannage

## Problème 1

L'authentification TACACS+ entre Cisco ISE et le commutateur Arista (ou tout périphérique réseau) échoue avec le message d'erreur suivant :

"Le profil d'interpréteur de commandes 13036 sélectionné est DenyAccess"



**Overview**

| | |
|---|---|
| Request Type | Authentication |
| Status | Fail |
| Session Key | goldenserver/541265148/80 |
| Message Text | Failed-Attempt: Authentication failed |
| Username | diviya |
| Authentication Policy | Arista SW_TACACS >> Arista SW_TACACS Auth |
| Selected Authorization Profile | Deny All Shell Profile |

**Authentication Details**

| | |
|---|---|
| Generated Time | 2025-07-27 16:06:30.094000 +05:30 |
| Logged Time | 2025-07-27 16:06:30.094 |
| Epoch Time (sec) | 1753612590 |
| ISE Node | goldenserver |
| Message Text | Failed-Attempt: Authentication failed |
| Failure Reason | 13036 Selected Shell Profile is DenyAccess |
| Resolution | Check whether the Device Administration Authorization Policy rules are correct |
| Root Cause | Selected Shell Profile fails for this request |
| Username | diviya |

**Steps**

| | |
|---|---|
| 13013 | Received TACACS+ Authentication START Request |
| 15049 | Evaluating Policy Group (Step latency=1ms) |
| 15008 | Evaluating Service Selection Policy (Step latency=0m |
| 15048 | Queried PIP - DEVICE.Device Type (Step latency=2m |
| 15041 | Evaluating Identity Policy (Step latency=3ms) |
| 15048 | Queried PIP - Network Access.Protocol (Step latency=2ms) |
| 15013 | Selected Identity Source - Internal Users (Step latency=2ms) |
| 24210 | Looking up User in Internal Users IDStore (Step latency=0ms) |
| 24212 | Found User in Internal Users IDStore (Step latency=37ms) |
| 13045 | TACACS+ will use the password prompt from global TACACS+ configuration (Step latency=0ms) |
| 13015 | Returned TACACS+ Authentication Reply (Step latency=0ms) |
| 13014 | Received TACACS+ Authentication CONTINUE Request ( Step latency=68ms) |
| 15041 | Evaluating Identity Policy (Step latency=0ms) |
| 15013 | Selected Identity Source - Internal Users (Step latency=4ms) |
| 24210 | Looking up User in Internal Users IDStore (Step latency=0ms) |
| 24212 | Found User in Internal Users IDStore (Step latency=7ms) |
| 22037 | Authentication Passed (Step latency=0ms) |
| 15036 | Evaluating Authorization Policy (Step latency=0ms) |
| 15048 | Queried PIP - Network Access.UserName (Step latency=4ms) |

L'erreur « 13036 Selected Shell Profile is DenyAccess » dans Cisco ISE signifie typiquement que pendant une tentative d'administration de périphérique TACACS+, la stratégie d'autorisation correspondait à un profil d'interpréteur de commandes défini sur DenyAccess.Ce n'est généralement pas le résultat d'un profil d'interpréteur de commandes mal configuré lui-même, mais indique plutôt qu'aucune des règles d'autorisation configurées ne correspondait aux attributs d'utilisateur entrant (tels que l'appartenance à un groupe, le type de périphérique ou l'emplacement). Par conséquent, ISE revient à une règle par défaut ou à une règle de refus explicite, ce qui entraîne le refus de l'accès.

Causes possibles

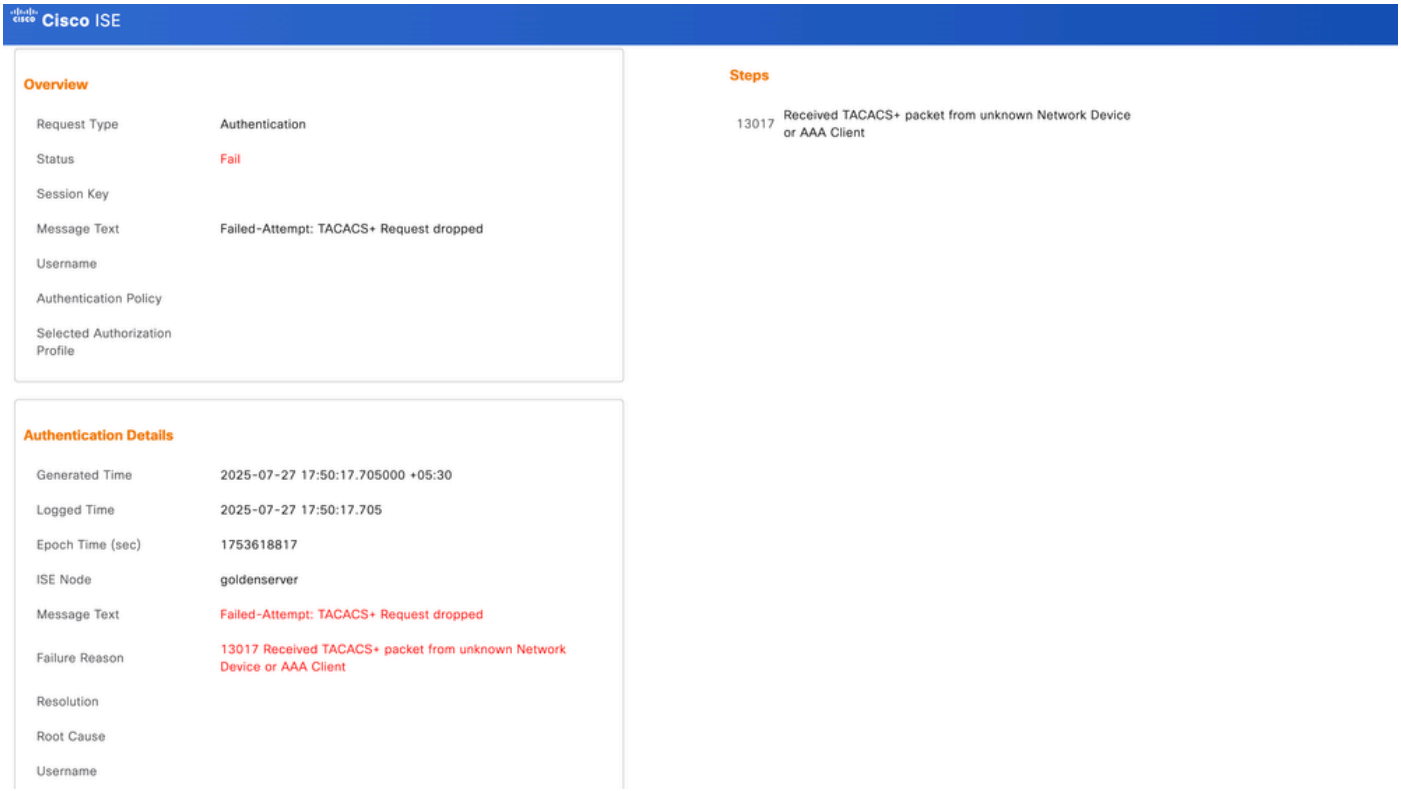
- Examinez les règles de stratégie d'autorisation dans ISE. Vérifiez que l'utilisateur ou le périphérique correspond à la règle qui attribue le profil d'environnement souhaité, par exemple celle qui autorise un accès approprié.
- Assurez-vous que le mappage AD ou de groupe d'utilisateurs interne est correct et que les conditions de stratégie, telles que l'appartenance à un groupe d'utilisateurs, le type de périphérique et le protocole, sont spécifiées avec précision.
- Utilisez les journaux en direct ISE et les détails de l'échec de la tentative pour voir exactement quelle règle correspond et pourquoi.

## Problème 2

L'authentification TACACS+ entre Cisco ISE et le commutateur Arista (ou tout périphérique

réseau) échoue avec le message d'erreur suivant :

"13017 Paquet TACACS+ reçu d'un périphérique réseau inconnu ou d'un client AAA"




Causes possibles

- La raison la plus courante est que l'adresse IP du commutateur n'est pas ajoutée en tant que périphérique réseau dans ISE (sous Administration > Network Resources > Network Devices).
- Assurez-vous que l'adresse IP ou la plage correspond exactement à l'adresse IP source utilisée par le commutateur Arista pour envoyer des paquets TACACS+.
- Si votre commutateur utilise une interface de gestion, vérifiez que son adresse IP exacte (et pas seulement un sous-réseau/une plage) est ajoutée dans ISE.

Solution

- Accédez à Administration > Network Resources > Network Devices dans l'interface utilisateur graphique ISE.
- Vérifiez si l'adresse IP source exacte sur le commutateur Arista est utilisée pour la communication TACACS+ (le plus souvent l'adresse IP de l'interface de gestion).
- Spécifiez le secret partagé (il doit correspondre à celui défini sur le commutateur Arista).

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.