Configuration de la connexion administrateur basée sur RADIUS sur le commutateur Arista

Table des matières

Introduction

Ce document décrit comment configurer Cisco Identity Services Engine (ISE) pour authentifier les connexions administrateur sur les commutateurs Arista à l'aide de RADIUS.

Conditions préalables

Exigences

Avant de continuer, assurez-vous que :

- Cisco ISE (version 3.x recommandée) est installé et opérationnel.
- Commutateur Arista exécutant EOS avec prise en charge RADIUS.
- Active Directory (AD) ou base de données utilisateur interne configurée dans ISE.

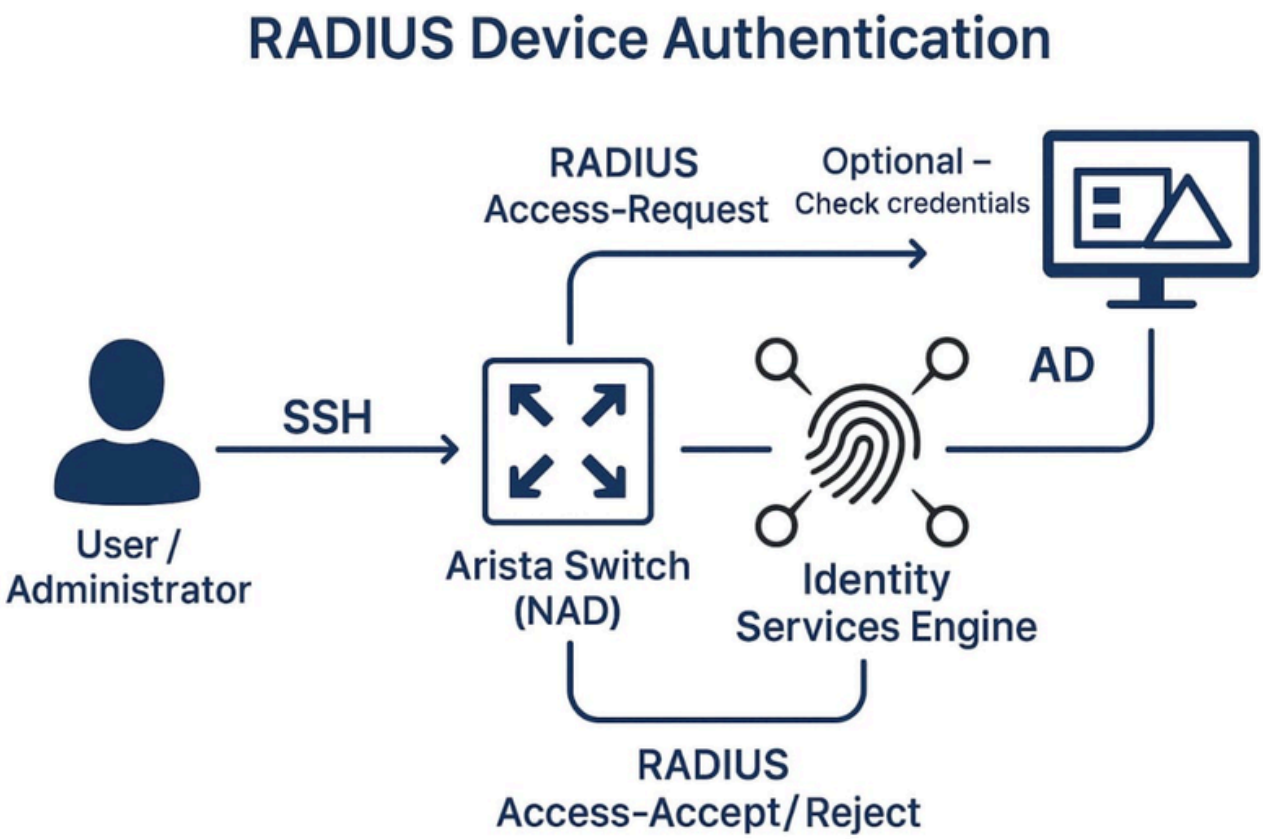
Composants utilisés

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



Voici un schéma de réseau illustrant l'authentification de périphérique RADIUS pour un commutateur Arista utilisant Cisco ISE, avec Active Directory (AD) comme source

d'authentification facultative.

Le schéma comprend :

- Commutateur Arista (faisant office de périphérique d'accès réseau, NAD)
- Cisco ISE (en tant que serveur RADIUS)
- Active Directory (AD) [Facultatif] (utilisé pour la vérification d'identité)
- Utilisateur/Administrateur (qui se connecte via SSH)

Configurer

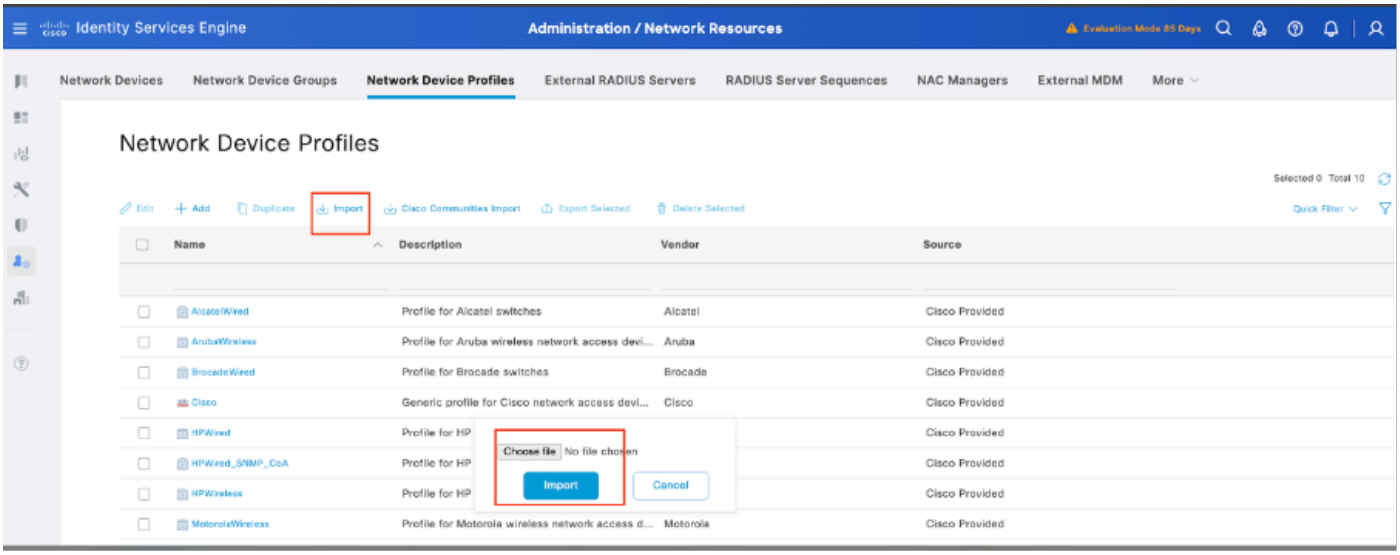
Configuration de Cisco ISE

Étape 1. 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

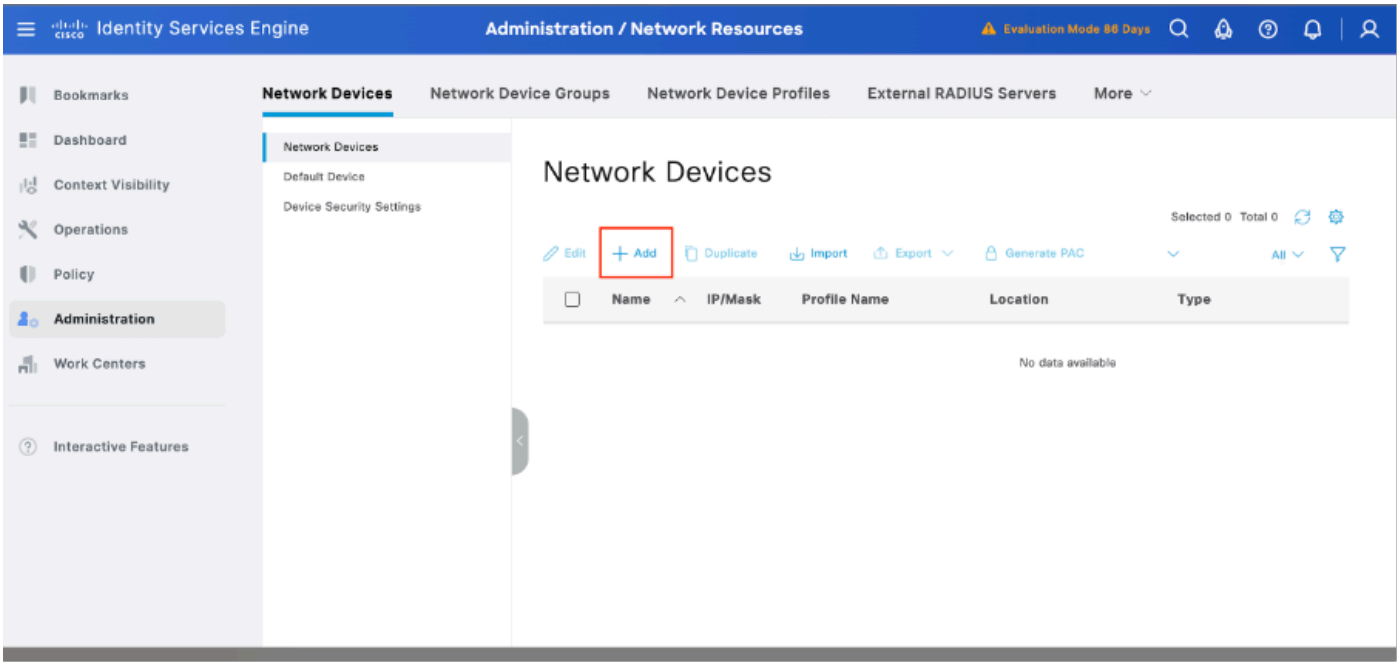
Voici les étapes à suivre pour importer le profil NAD Arista dans Cisco ISE :

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.



Étape 2. Ajouter un commutateur Arista en tant que périphérique réseau

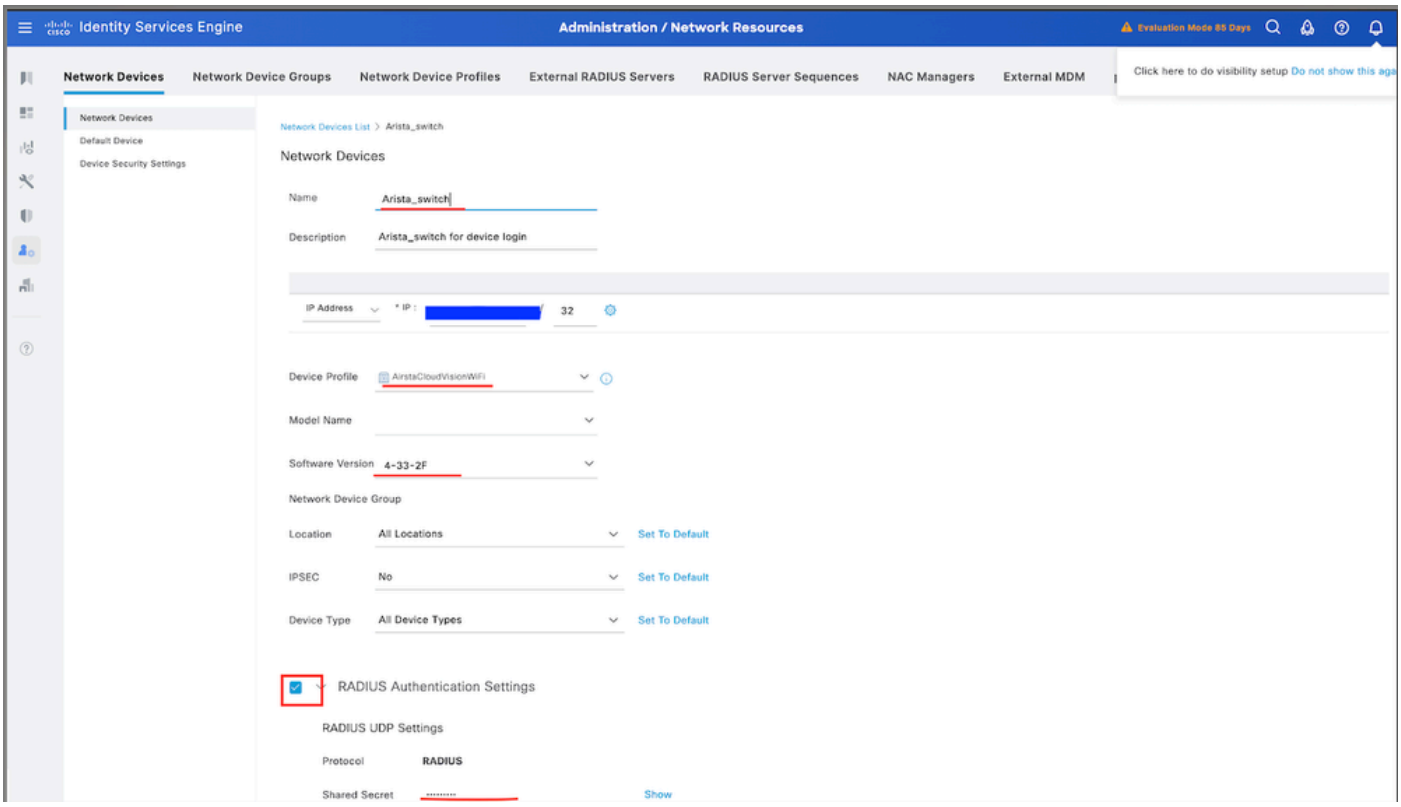
1. Accédez à Administration > Network Resources > Network Devices > +Add.



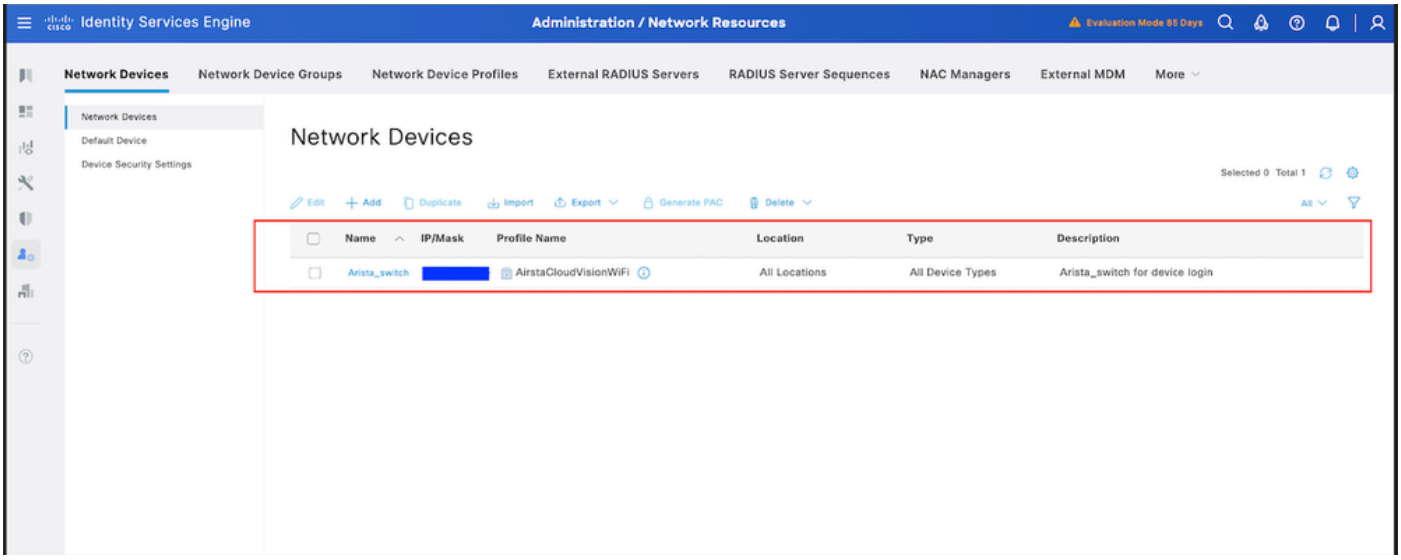
2. Cliquez sur Ajouter et entrez les informations suivantes :

1. Name : Arista-Switch
2. Adresse IP: <IP du commutateur>
3. Type de périphérique : Choisir un autre câblé
4. Profil de périphérique réseau : sélectionnez AirstaCloudVisionWiFi.
5. Paramètres d'authentification RADIUS :
    1. Activer l'authentification RADIUS
    2. Entrez le secret partagé (il doit correspondre à la configuration du commutateur).

3. Cliquez sur Enregistrer.

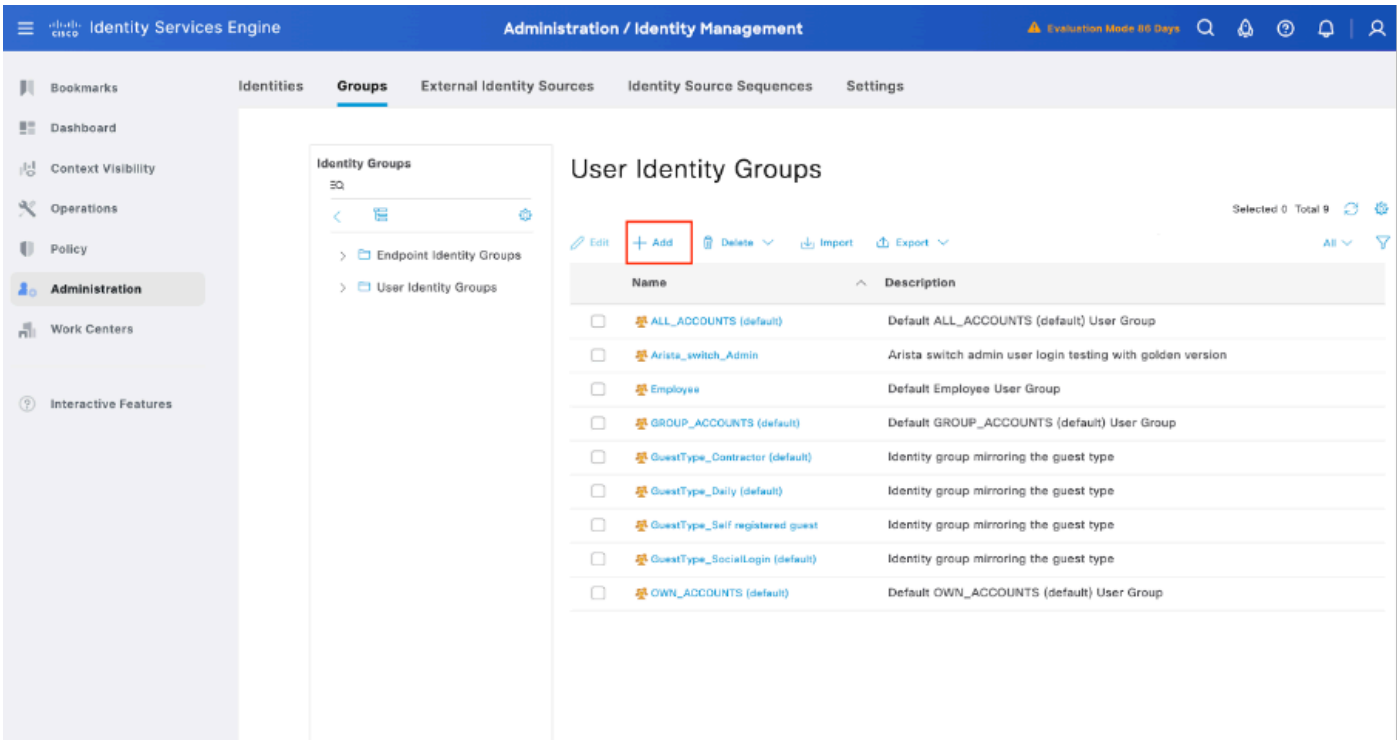


Étape 3. Vérifiez que le nouveau périphérique est affiché sous Périphériques réseau



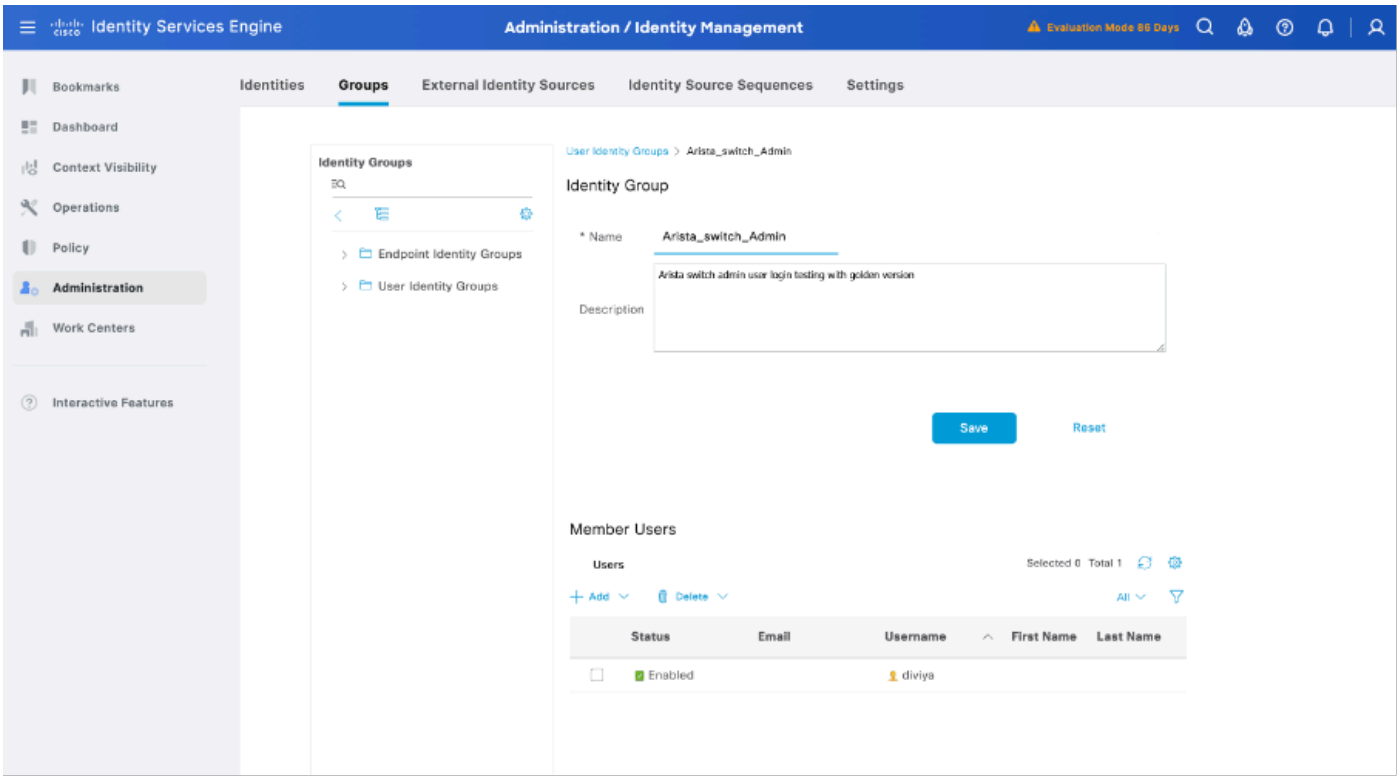
Étape 4. Créer les groupes d'identités utilisateur requis

Accédez à Administration > Identity Management > Groups > User Identity Groups > + Add:



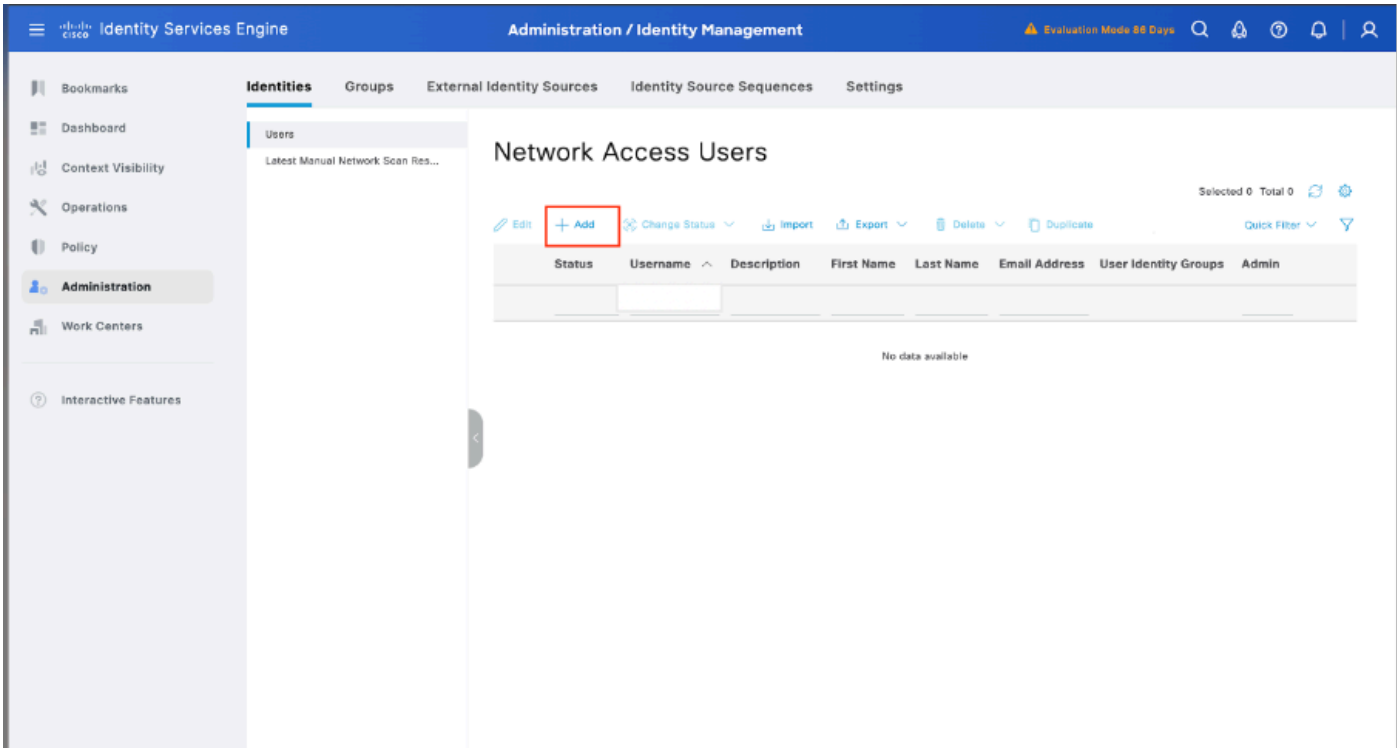
Étape 5. Définir un nom pour le groupe d'identités d'utilisateur Admin

Cliquez sur Submit afin d'enregistrer la configuration :

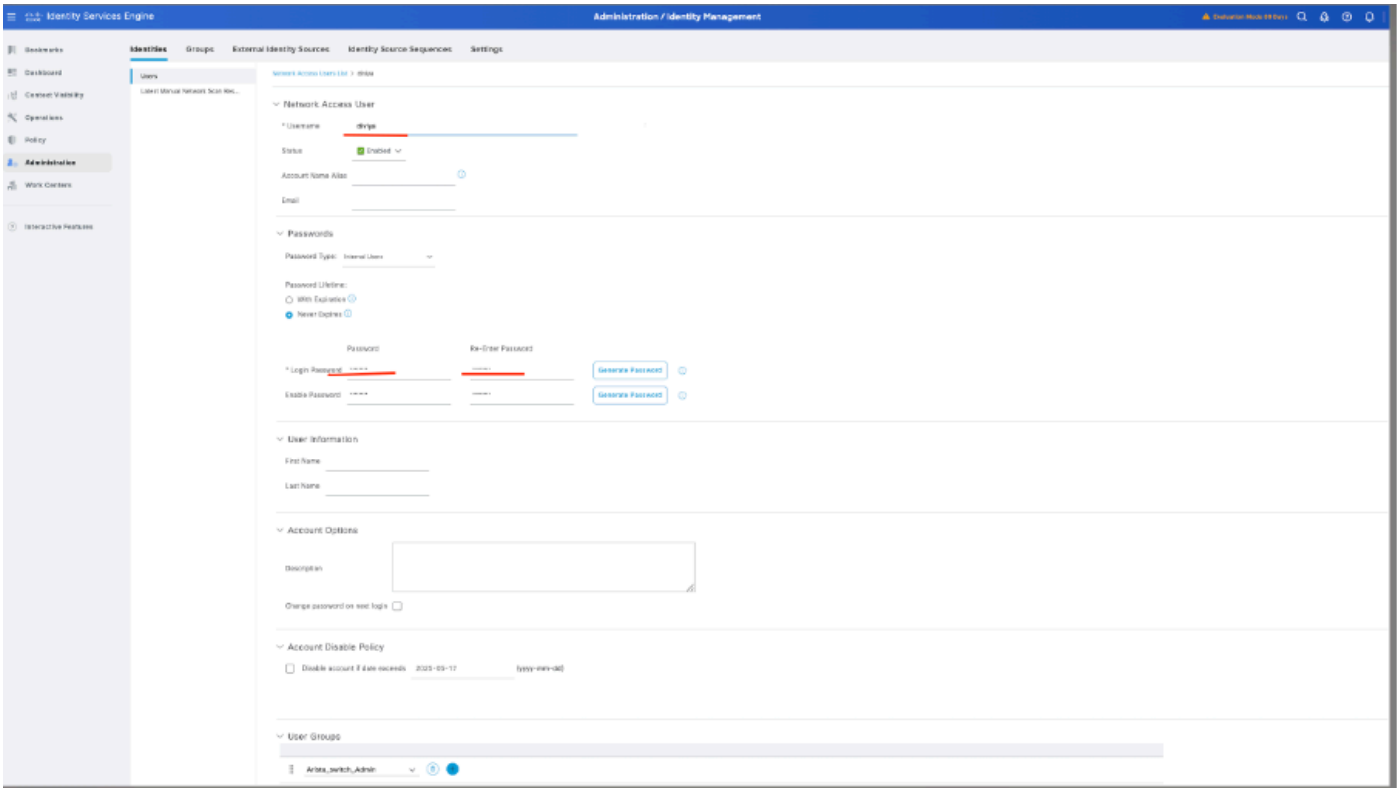


Étape 6. Créer les utilisateurs locaux et les ajouter à leur groupe de correspondants

Accédez à Administration > Gestion des identités > Identités > + Ajouter :



6.1. Ajouter l'utilisateur avec des droits d'administrateur. Définissez un nom, un mot de passe et attribuez-le à Arista_switch_Admin, faites défiler vers le bas et cliquez sur Submit pour enregistrer les modifications.

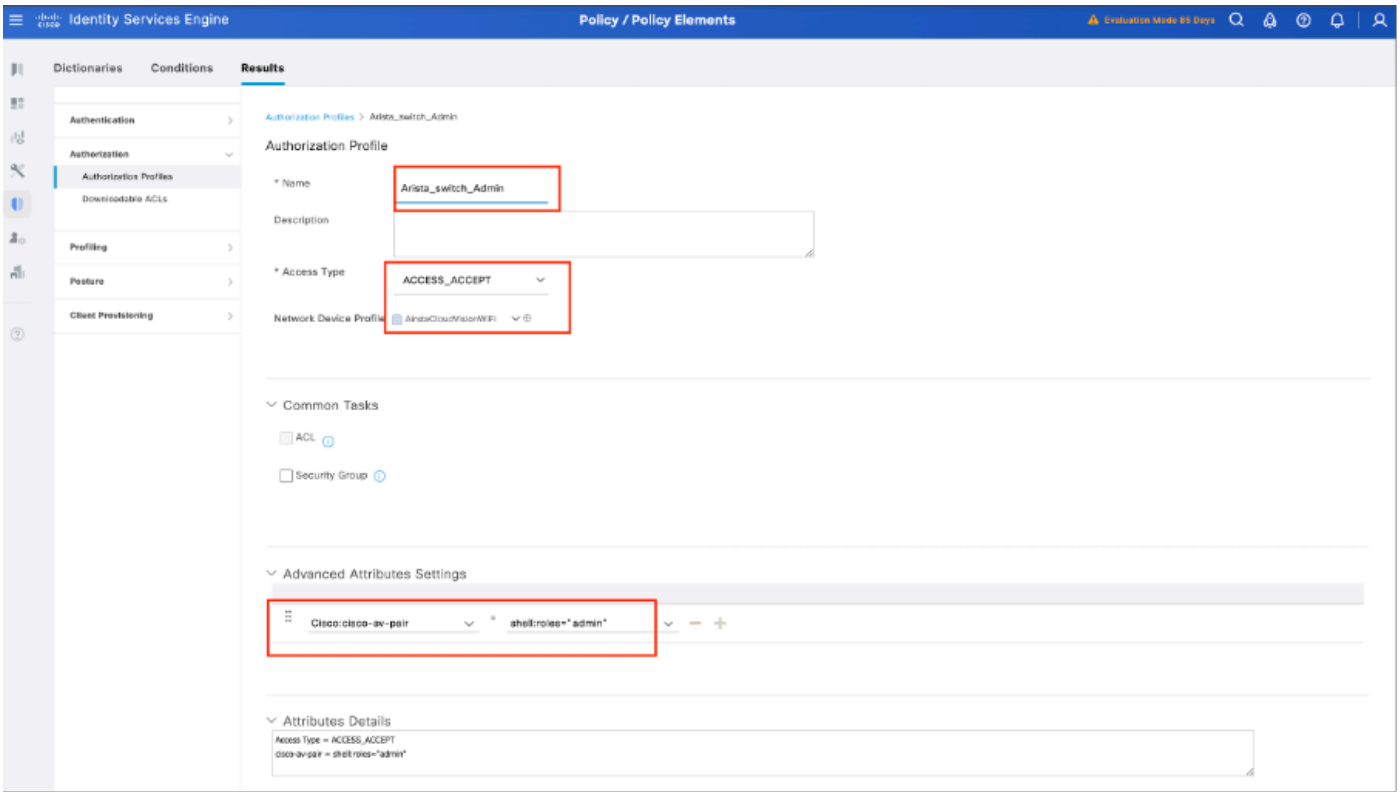


Étape 7. Créer le profil d'autorisation pour l'utilisateur Admin

Accédez à Policy > Policy Elements > Results > Authorization > Authorization Profiles > +Add.

Définissez un nom pour le profil d'autorisation, laissez le type d'accès comme ACCESS_ACCEPT

et sous Advanced Attributes Settings ajoutez cisco-av-pair=shell : roles="admin" avec et cliquez sur Submit.



Étape 8. Créer un jeu de stratégies correspondant à l'adresse IP du commutateur Arista

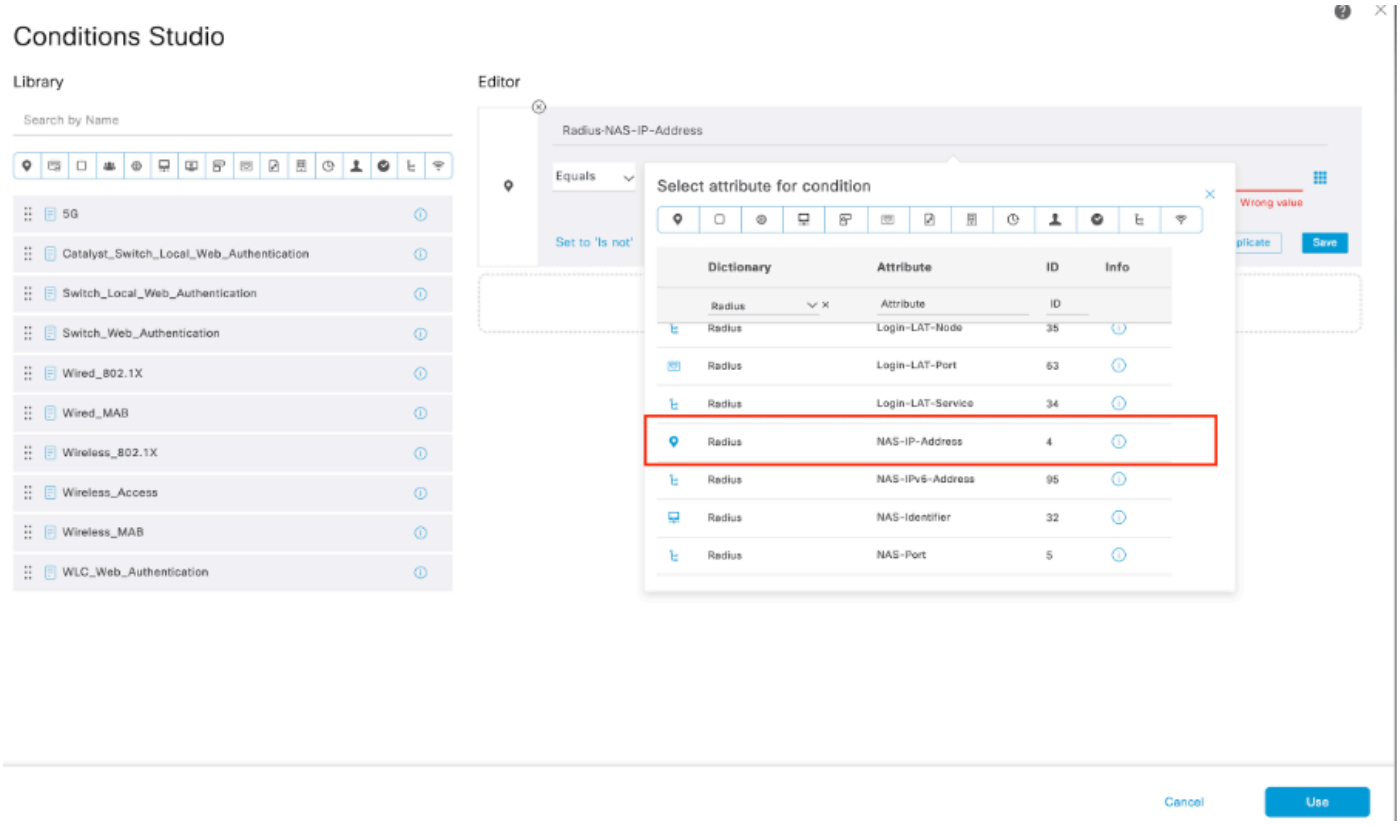
Cela permet d'empêcher d'autres périphériques d'accorder l'accès aux utilisateurs.

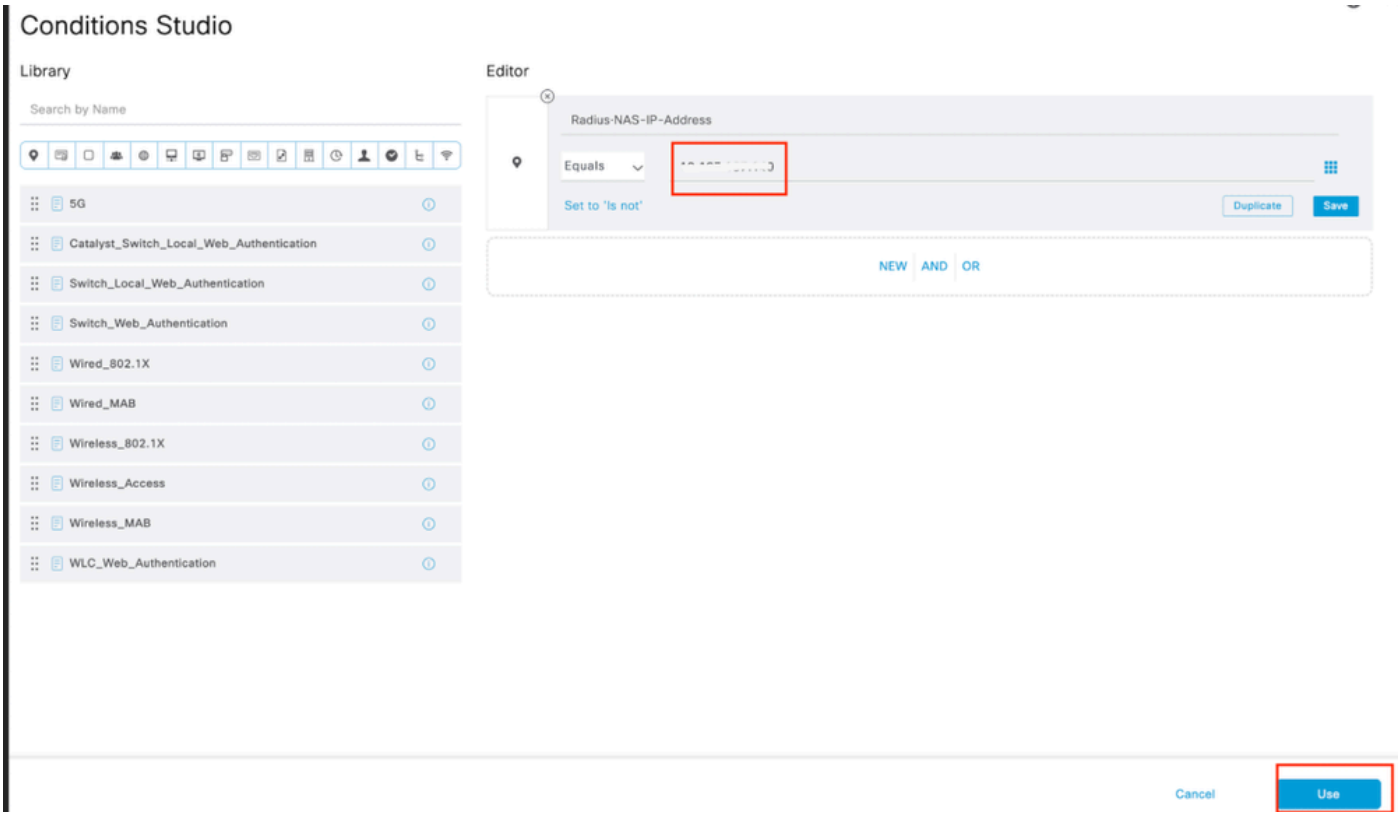
Accédez à Policy > Policy Sets > Add icon sign dans l'angle supérieur gauche.

8.1 Une nouvelle ligne est placée en haut de vos ensembles de stratégies. Cliquez sur l'icône Ajouter pour configurer une nouvelle condition.

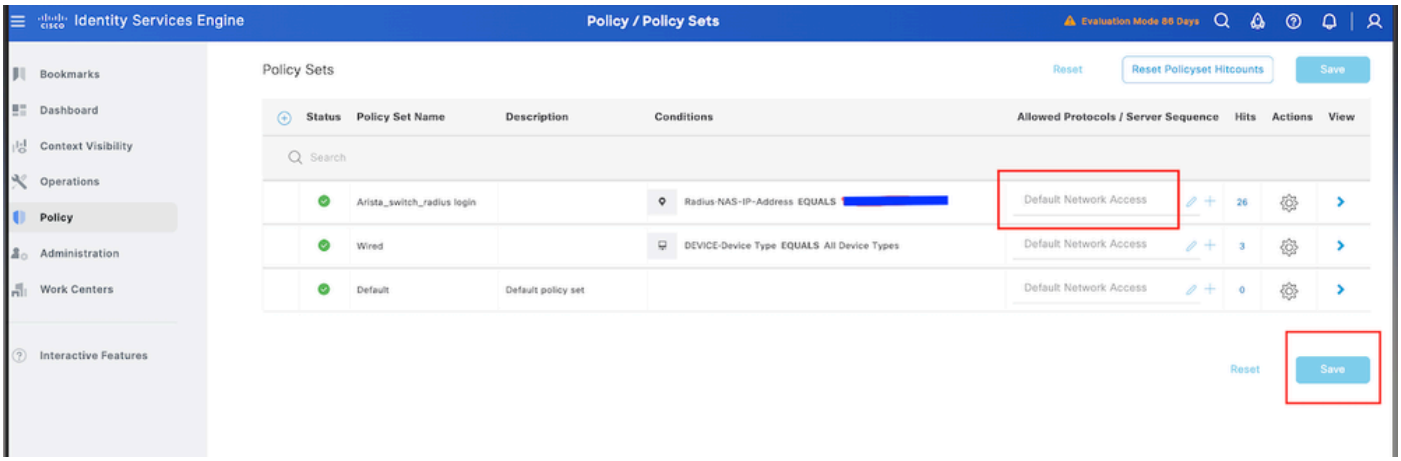
8.2 Ajoutez une condition supérieure pour l'attribut RADIUS NAS-IP-Address correspondant à

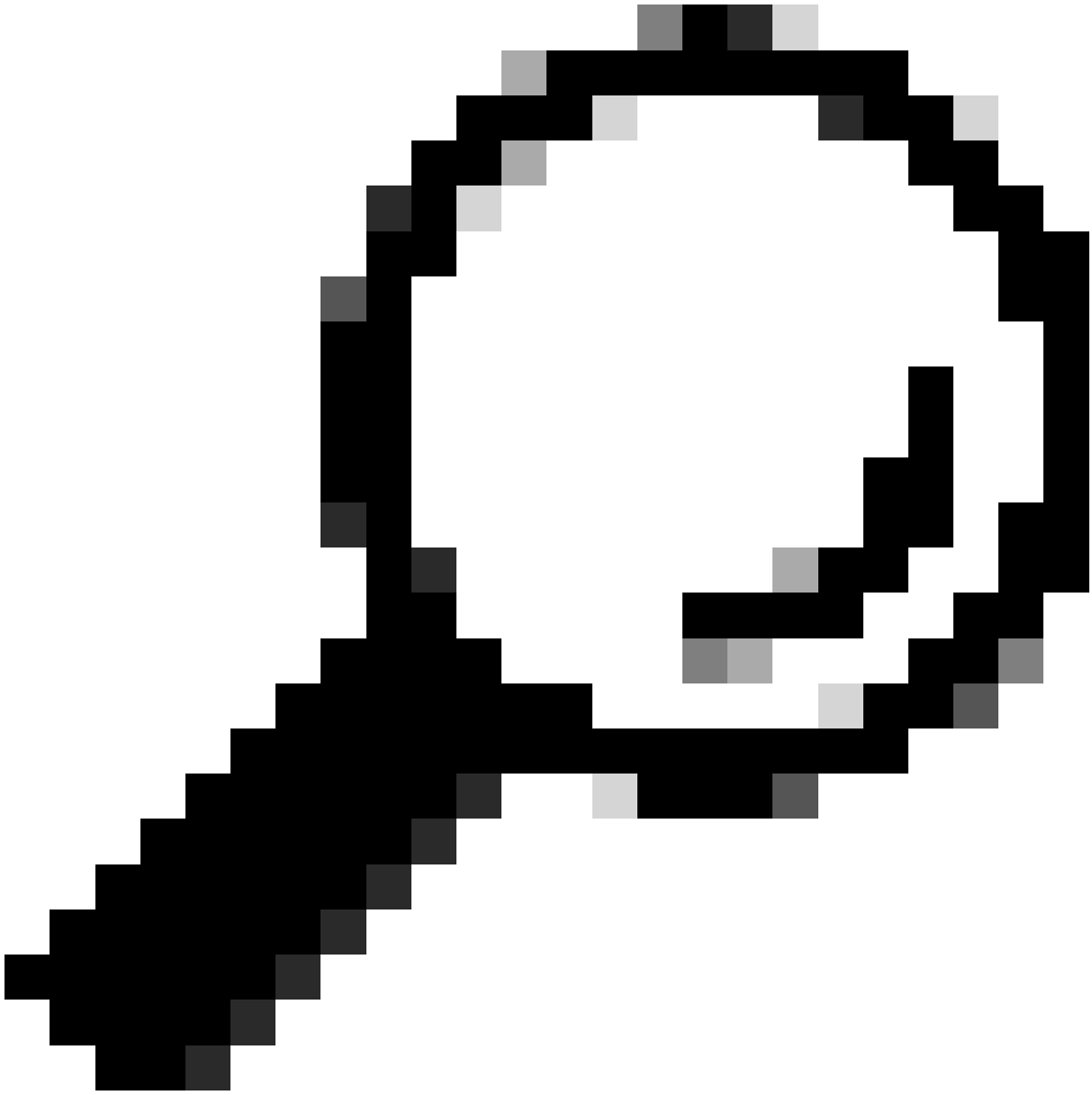
l'adresse IP du commutateur Arista, puis cliquez sur Use.





8.3 Une fois terminé, cliquez sur Save :

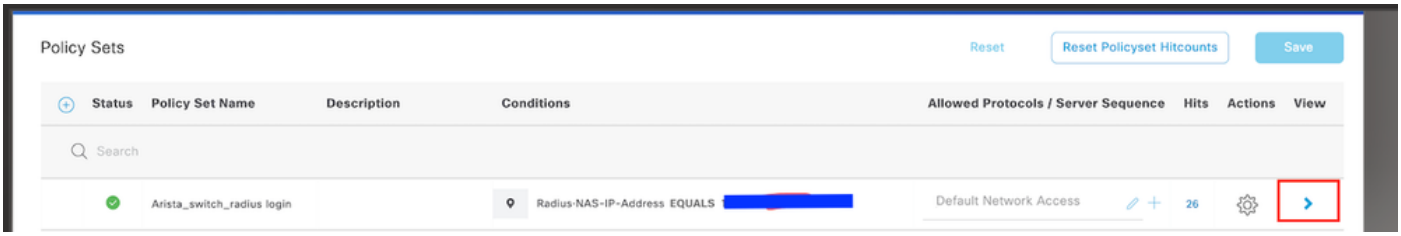




Conseil : Pour cet exercice, nous avons autorisé la liste des protocoles d'accès réseau par défaut. Vous pouvez créer une nouvelle liste et la réduire si nécessaire.

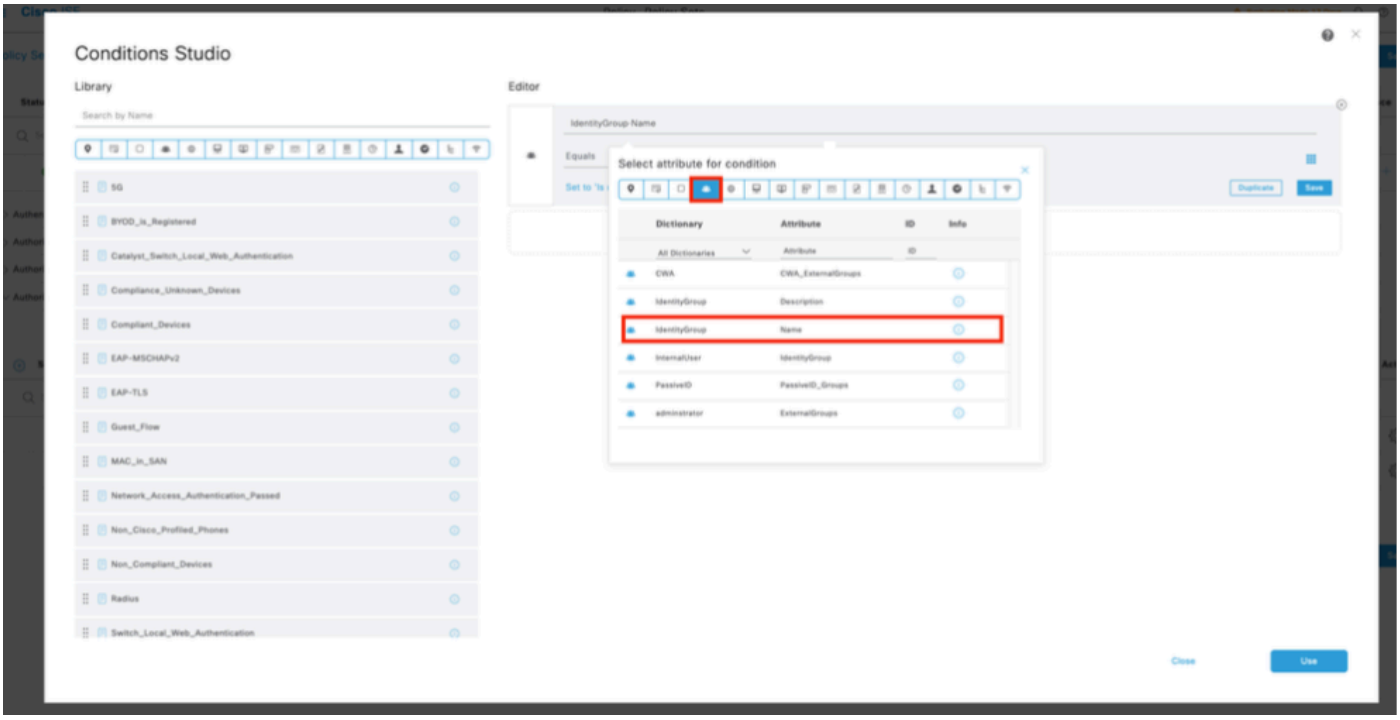
Étape 9. Afficher le nouvel ensemble de stratégies

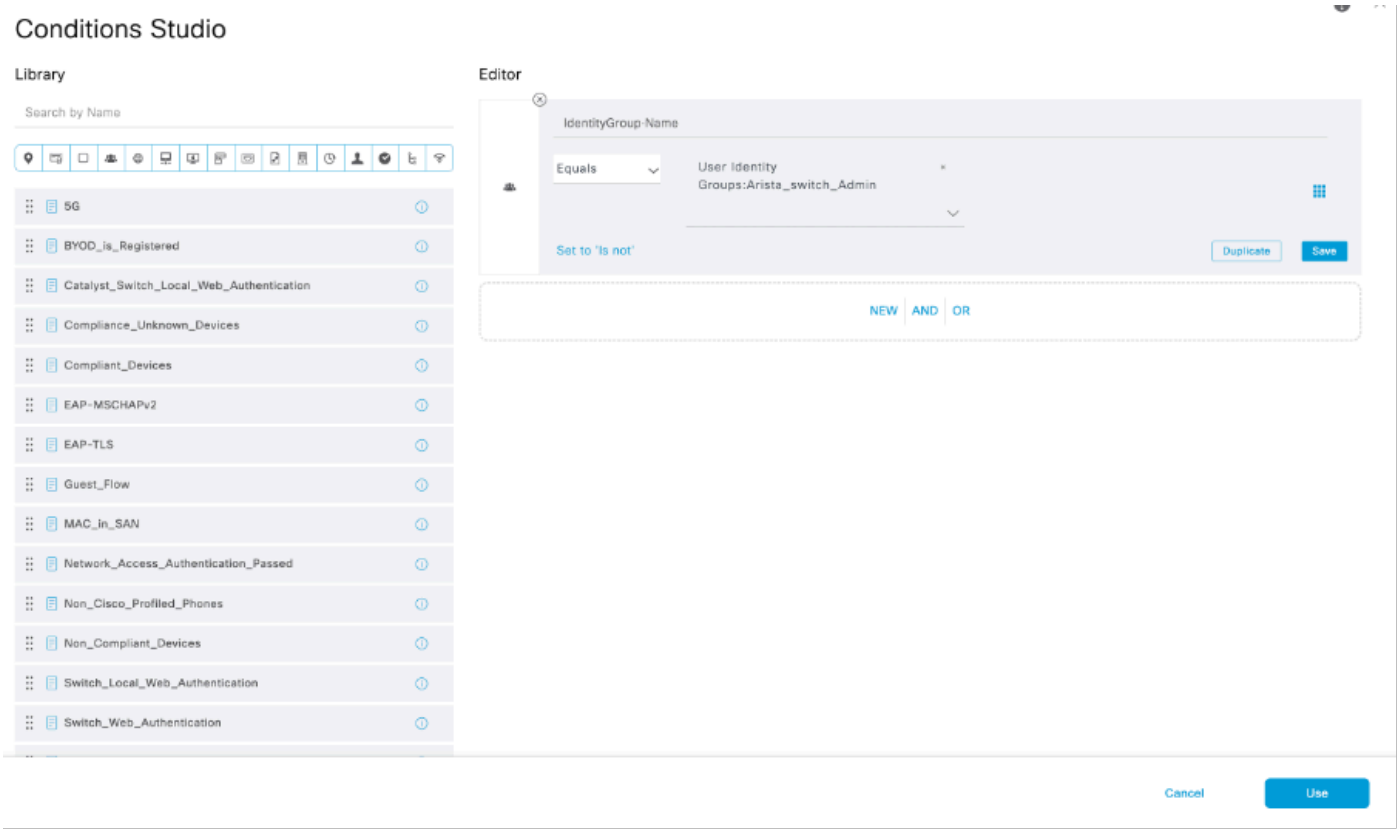
Cliquez sur l'icône > située à la fin de la ligne :



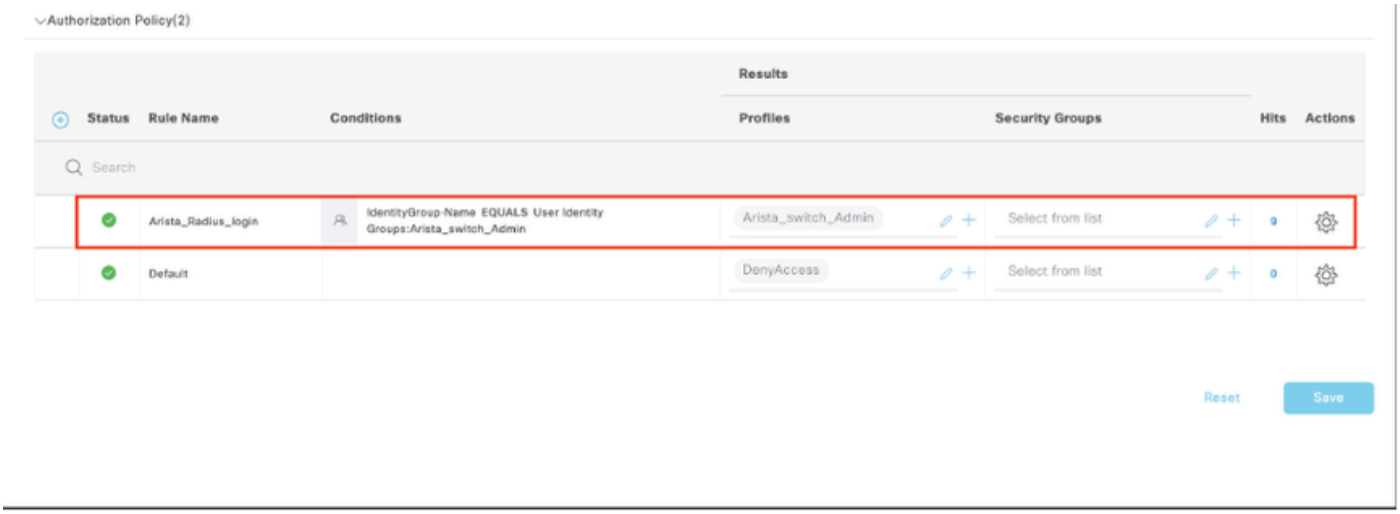
9.1 Développez le menu Authorization Policy et cliquez sur (+) pour ajouter une nouvelle condition.

9.2 Définir les conditions pour faire correspondre le groupe d'identité du dictionnaire avec le nom d'attribut et les groupes d'identité de l'utilisateur : Arista_switch_Admin (nom du groupe créé à l'étape 7) et cliquez sur Use.





9.3 Validez que la nouvelle condition est configurée dans la stratégie d'autorisation, puis ajoutez un profil utilisateur sous Profils :



Configuration du commutateur Arista

Étape 1 : activation de l'authentification RADIUS

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

configurer

!

radius-server host <ISE-IP> key <RADIUS-SECRET>

radius-server timeout 5

radius-server retransmit 3

radius-server deadtime 30

!

serveur de groupe aaa radius ISE

  serveur <ISE-IP>

!

aaa authentication login default group ISE local

aaa authorization exec default group ISE local

aaa accounting exec default start-stop group ISE

aaa accounting commands 15 default start-stop group ISE

aaa accounting system default start-stop group ISE

!

tranche

Étape 2 : enregistrement de la configuration

Pour conserver les paramètres lors des redémarrages :

mémoire d'écriture

ou

copy running-config startup-config

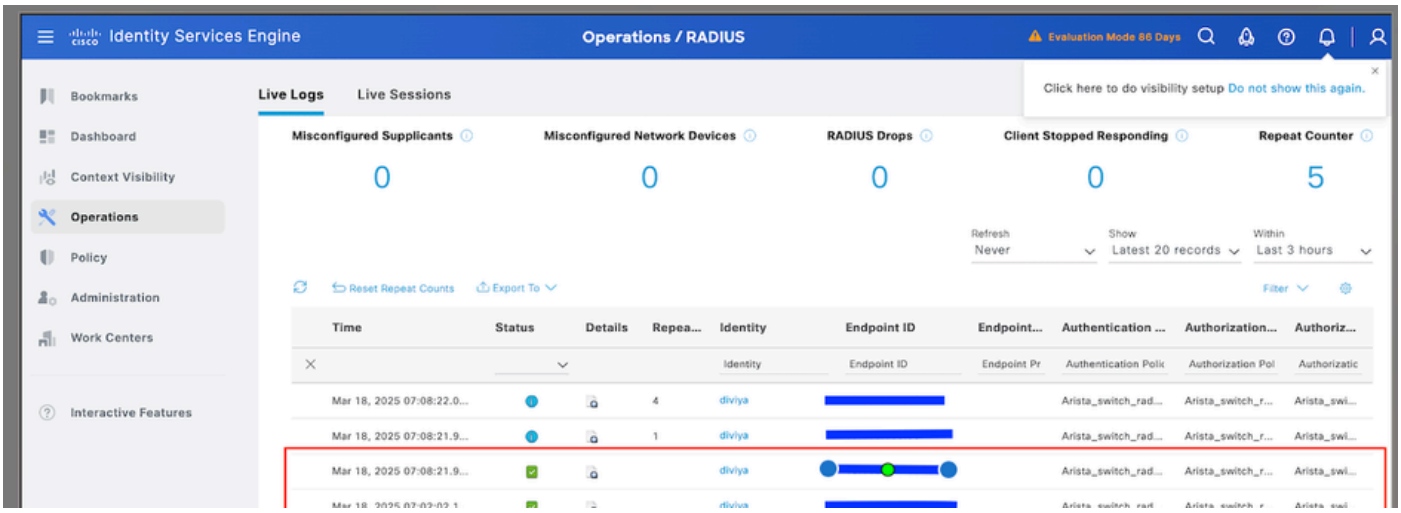
Vérifier

Évaluation ISE

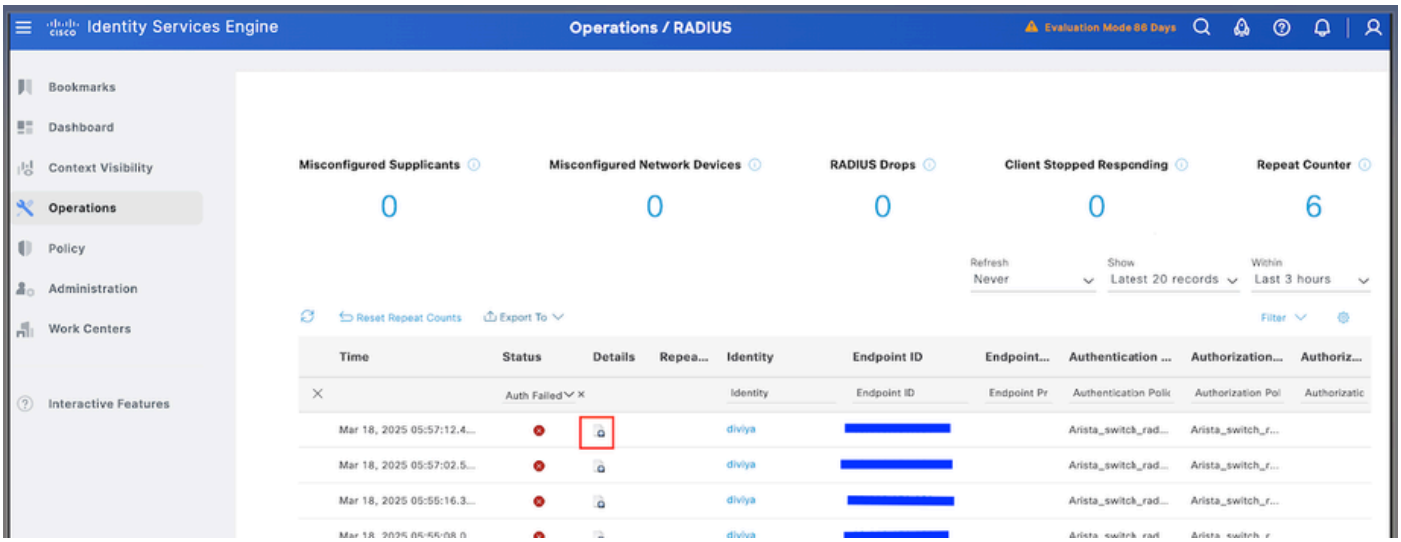
1. Essayez de vous connecter au commutateur Arista à l'aide des nouvelles informations d'identification Radius :

    1.1 Accédez à Operations > Radius > Live logs.

    1.2 Les informations affichées indiquent si un utilisateur a réussi à se connecter.



2. Pour l'état Échec, vérifiez les détails de la session :

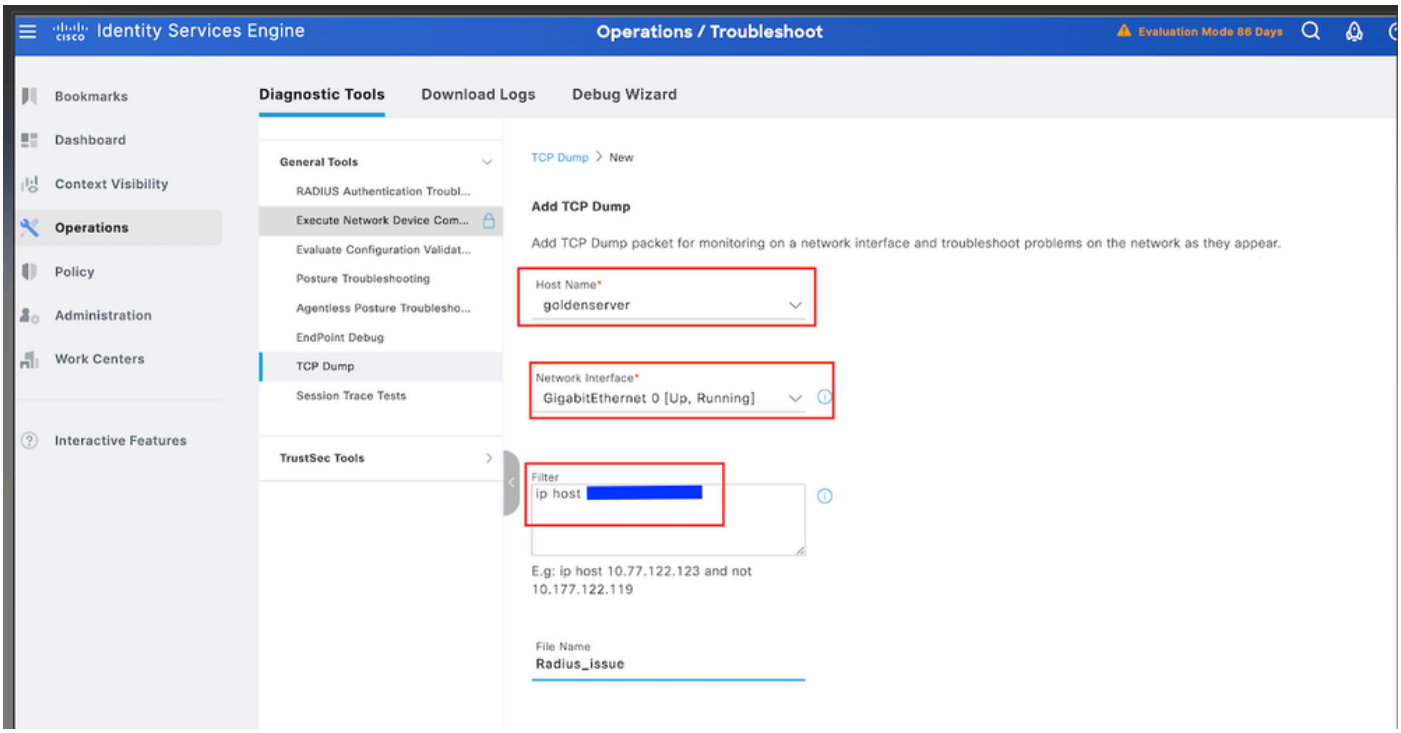


3. Pour les demandes qui n'apparaissent pas dans les journaux Radius Live , vérifiez si la demande UDP atteint le noeud ISE par le biais d'une capture de paquets.

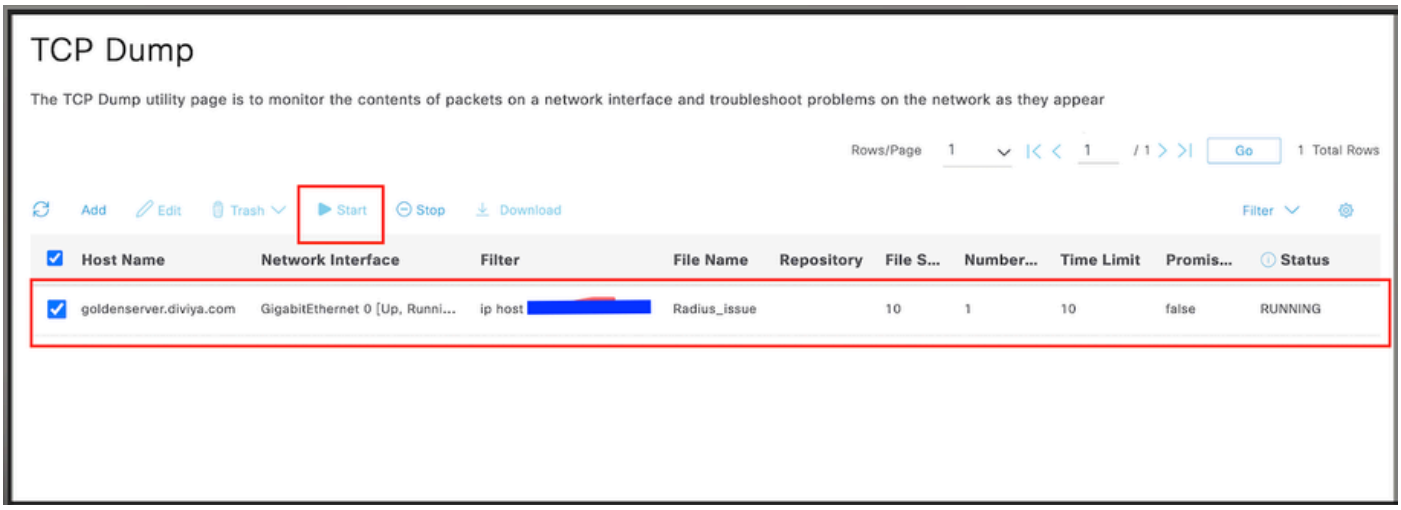
3.1. Accédez à Operations > Troubleshoot > Diagnostic Tools > TCP dump.

3.2. Ajoutez une nouvelle capture et téléchargez le fichier sur votre ordinateur local afin de vérifier si les paquets UDP arrivent sur le noeud ISE.

3.3. Remplissez les informations demandées, faites défiler la page vers le bas et cliquez sur Save.



3.4. Sélectionnez et commencez la capture.



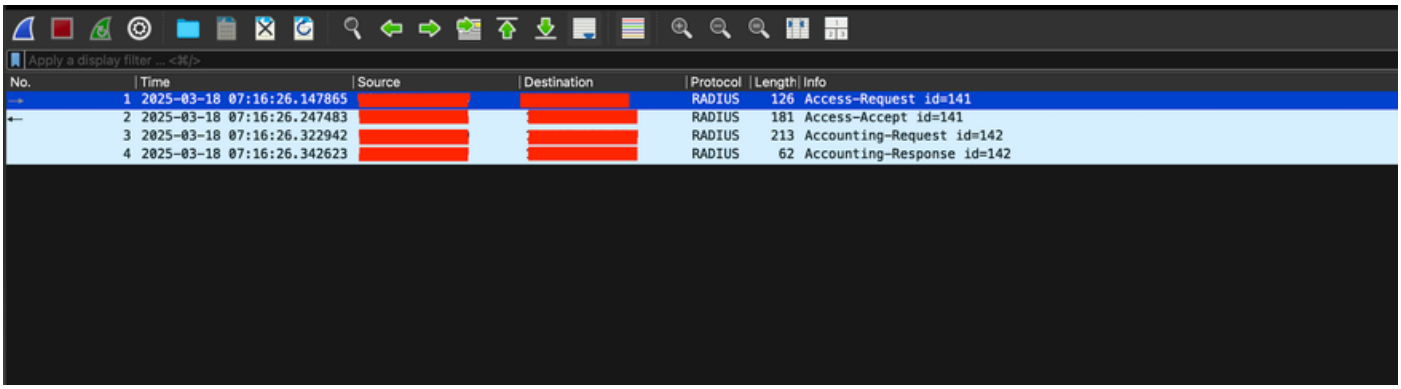
3.5. Tentative de connexion au commutateur Arista pendant l'exécution de la capture ISE.

3.6. Arrêtez le vidage TCP dans ISE et téléchargez le fichier sur un ordinateur local.

3.7. Examiner la sortie du trafic.

Résultat attendu :

Paquet n° 1. Demande du commutateur Arista au serveur ISE via le port 1812 (RADIUS).
Paquet no2. Réponse du serveur ISE acceptant la requête initiale.



Dépannage

Scénario 1. « Demande 5405 RADIUS abandonnée »

Problème

Ce scénario implique le dépannage d'une erreur « Demande RADIUS 5405 abandonnée » avec la raison « 11007 Impossible de localiser le périphérique réseau ou le client AAA » dans Cisco ISE lorsqu'un périphérique réseau (tel qu'un commutateur Arista) tente de s'authentifier.

Causes possibles

- Cisco Identity Services Engine (ISE) ne peut pas identifier le commutateur Arista, car son adresse IP ne figure pas parmi les périphériques réseau connus.
- La requête RADIUS provient d'une adresse IP qu'ISE ne reconnaît pas comme périphérique réseau ou client AAA valide.
- Il peut y avoir une incohérence dans la configuration entre le commutateur et l'ISE (par exemple, une adresse IP incorrecte ou un secret partagé).

Solution

- Ajoutez le commutateur à la liste Cisco ISE des périphériques réseau avec l'adresse IP correcte.
- Vérifiez que l'adresse IP et le secret partagé configurés dans ISE correspondent exactement à ce qui est défini sur le commutateur.
- Une fois corrigée, la demande RADIUS doit être correctement reconnue et traitée.

Scénario 2 : le commutateur Arista ne parvient pas à basculer pour sauvegarder le PSN ISE

Problème

Un commutateur Arista est configuré pour utiliser Cisco ISE pour l'authentification RADIUS. Lorsque le noeud de service de stratégie ISE principal (PSN) devient indisponible, le commutateur ne bascule pas automatiquement vers un PSN de secours. Par conséquent, les journaux d'authentification apparaissent uniquement à partir du PSN ISE principal, et il n'y a aucun journal du PSN secondaire/de sauvegarde lorsque le PSN principal est en panne.

Causes possibles

- La configuration du serveur RADIUS du commutateur Arista pointe uniquement vers le noeud ISE principal, de sorte que les serveurs de sauvegarde ne sont pas utilisés.
- La priorité du serveur RADIUS n'est pas correctement définie ou l'IP ISE de sauvegarde est manquante dans la configuration.
- Le délai d'attente et les paramètres de retransmission sur le commutateur sont définis trop bas, ce qui empêche un retour réussi vers le PSN de sauvegarde.
- Le commutateur utilise un nom de domaine complet (FQDN) pour le PSN, mais la résolution DNS ne renvoie pas tous les enregistrements A, ce qui entraîne uniquement le contact avec le serveur principal.

Solution

- Assurez-vous que plusieurs IP PSN ISE sont entrées dans la configuration du groupe de serveurs RADIUS du commutateur. Cela permet au commutateur d'utiliser le PSN ISE de secours si le principal est inaccessible.

  Exemple de configuration :

  ```
  radius-server host <ISE1-IP> key <secret>

  radius-server host <ISE2-IP> key <secret>
  ```

- Vérifiez que les valeurs de priorité, de délai d'attente et de retransmission du serveur RADIUS sont correctement configurées pour un basculement fiable.
- Si vous utilisez des FQDN, vérifiez les paramètres DNS et la résolution pour vous assurer que toutes les adresses IP PSN sont renvoyées et utilisées par le commutateur.

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.