Configuration de l'authentification utilisateur basée sur Radius et TACACS

Table des matières

Introduction

Ce document décrit comment configurer l'authentification et l'autorisation des utilisateurs basées sur Radius et TACACS pour vEdge et les contrôleurs avec ISE.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Pour les besoins de la démonstration, la version 2.6 d'ISE est utilisée. vEdge-cloud et les contrôleurs exécutant 19.2.1

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.

Configurer

Le logiciel Viptela fournit trois noms de groupes d'utilisateurs fixes : basic, netadmin, et operator. Vous devez affecter l'utilisateur à au moins un groupe. L'utilisateur TACACS/Radius par défaut est automatiquement placé dans le groupe de base.

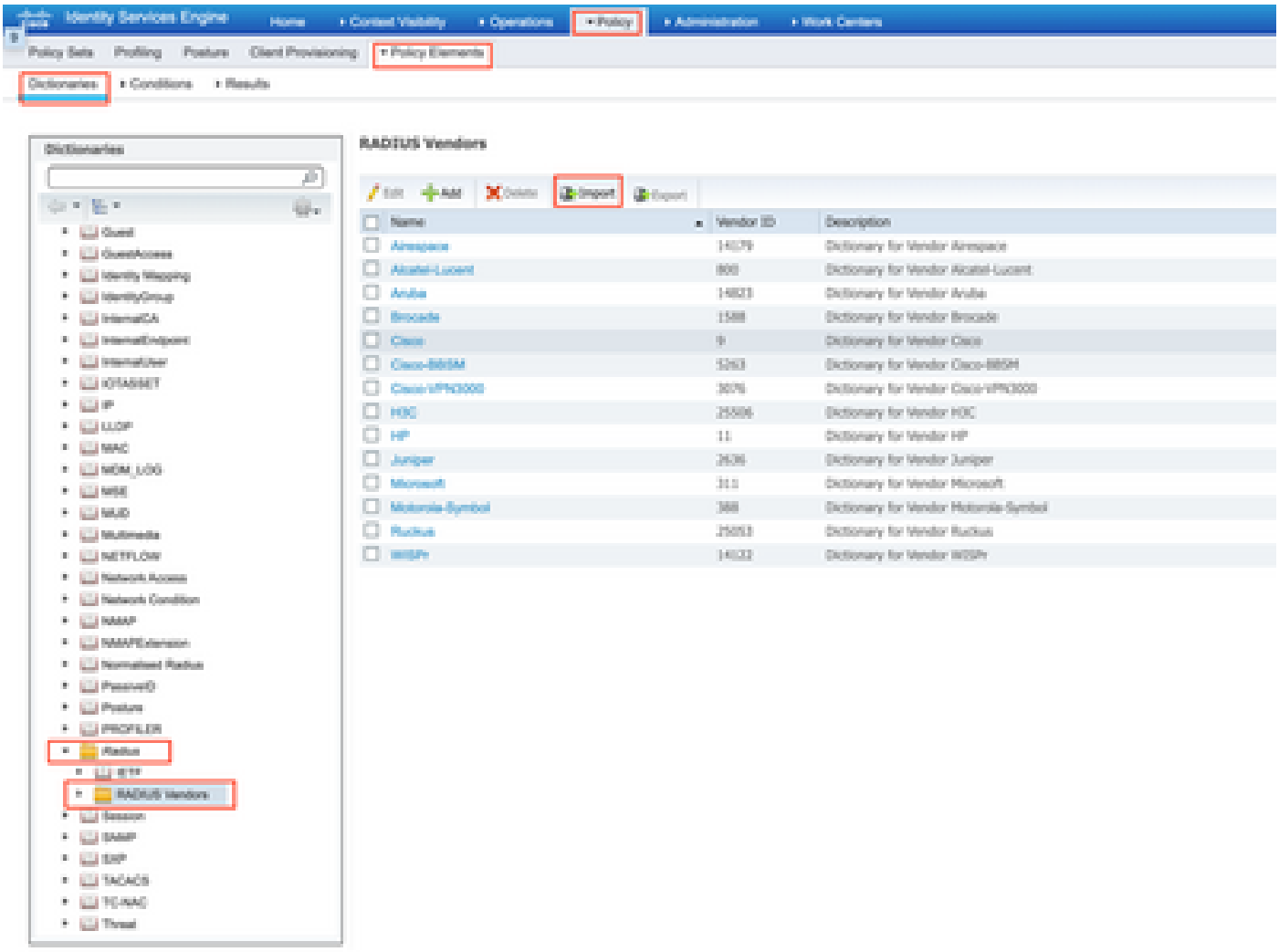
Authentification et autorisation utilisateur basées sur Radius pour vEdge et les

contrôleurs

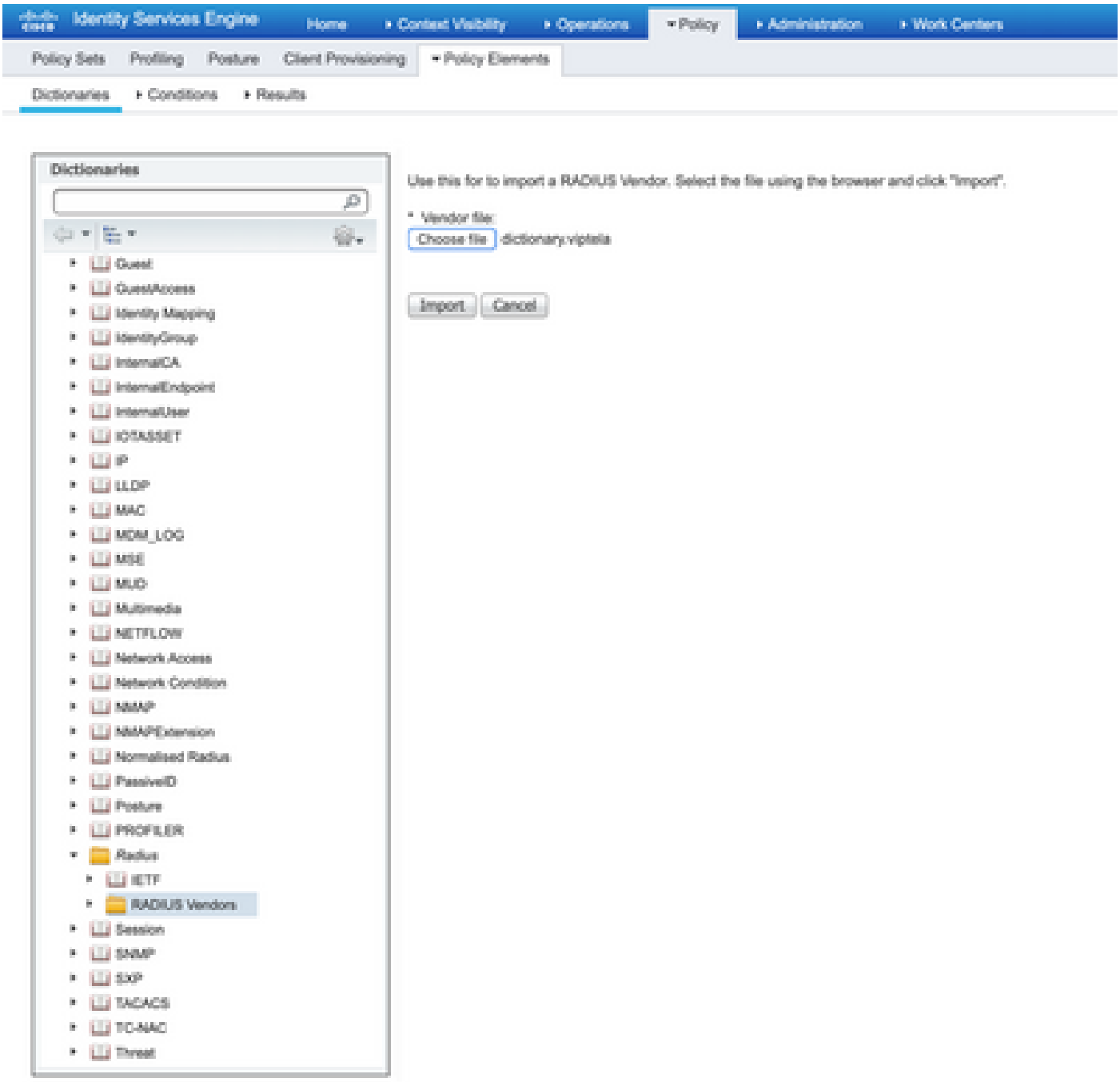
Étape 1. Créez un dictionnaire de rayons Viptela pour ISE. Pour ce faire, créez un fichier texte avec le contenu suivant :

```
# -*- text -*-
#
#  dictionary.viptela
#
#
# Version:      $Id$
#

VENDOR          Viptela                         41916

BEGIN-VENDOR    Viptela

ATTRIBUTE       Viptela-Group-Name              1    string
```

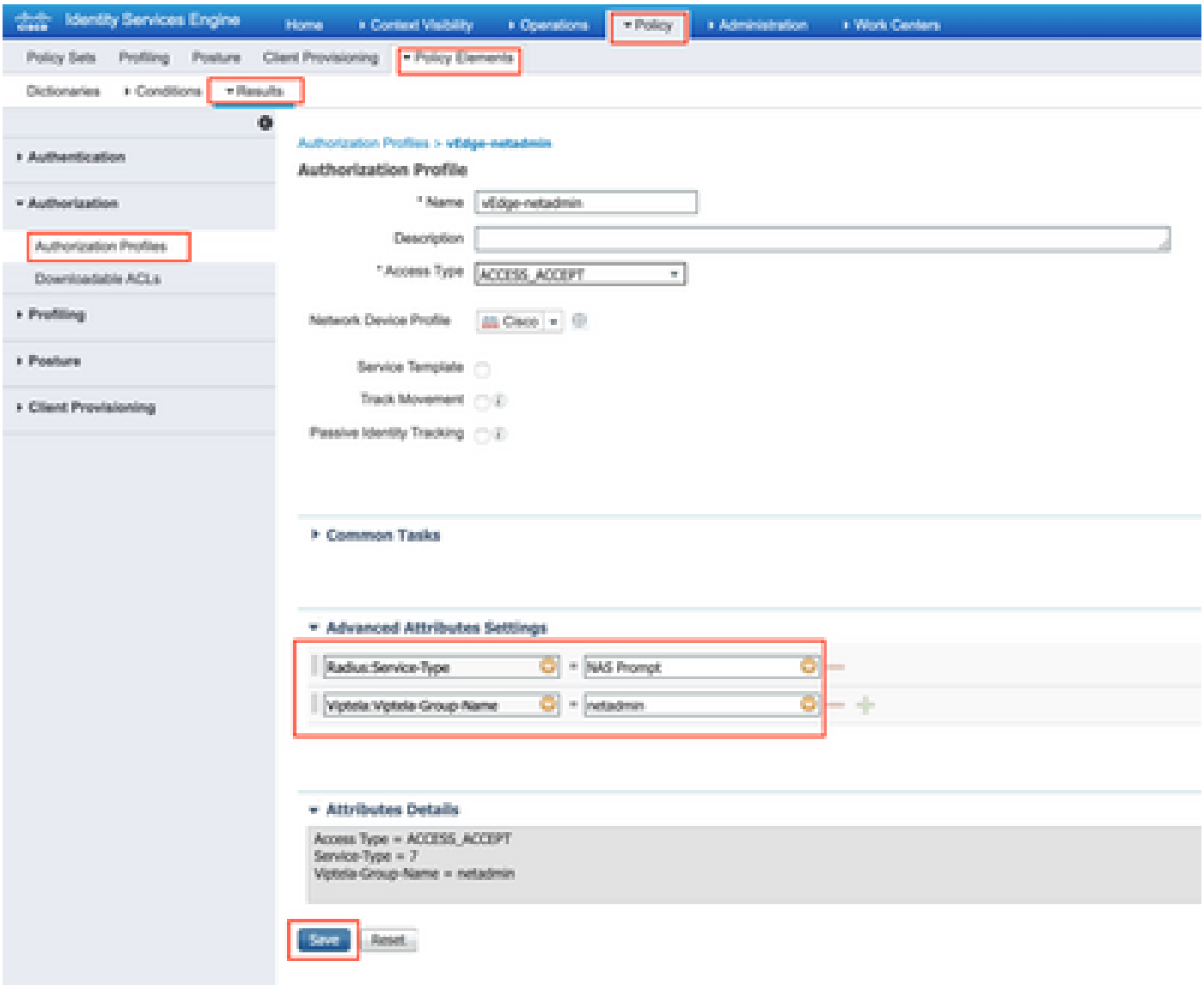
Étape 2. Téléchargez le dictionnaire vers ISE. Pour cela, accédez à Policy > Policy Elements > Dictionaries. Dans la liste des dictionnaires, accédez à Radius > Fournisseurs Radius, puis cliquez sur Importer comme indiqué.



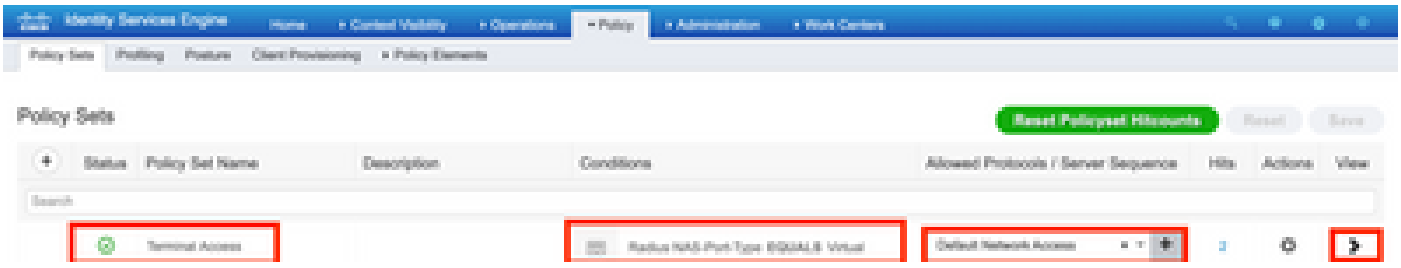
Téléchargez le fichier que vous avez créé à l'étape 1.



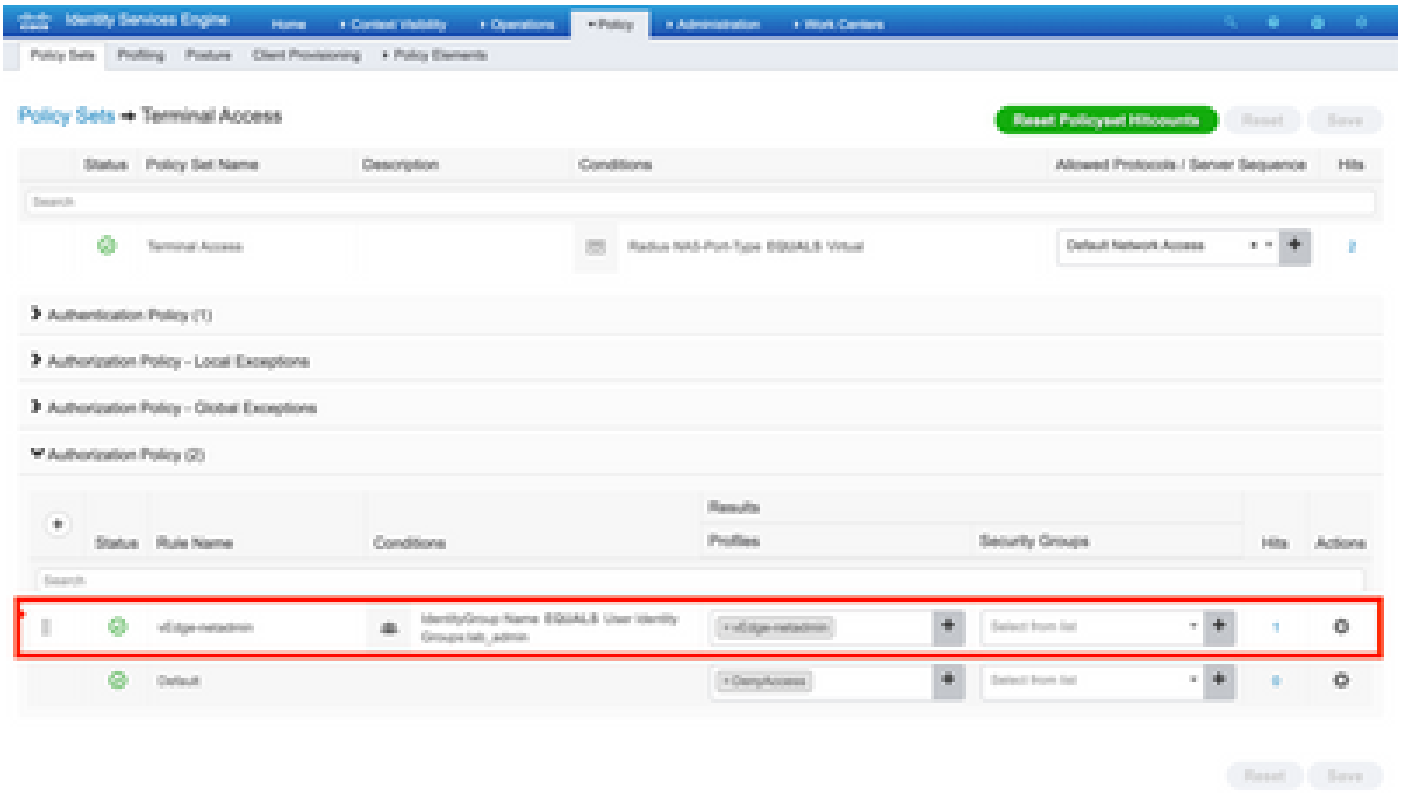
Étape 3. Créer un profil d'autorisation. Dans cette étape, le profil d'autorisation Radius attribue, par exemple, le niveau de privilège netadmin à un utilisateur authentifié. Pour cela, accédez à Policy > Policy Elements > Authorization Profiles et spécifiez deux attributs avancés comme indiqué dans l'image.



Étape 4. En fonction de votre configuration réelle, votre jeu de stratégies peut avoir un aspect différent. Pour les besoins de la démonstration dans cet article, l'entrée de stratégie appelée Terminal Access est créée comme illustré dans l'image.

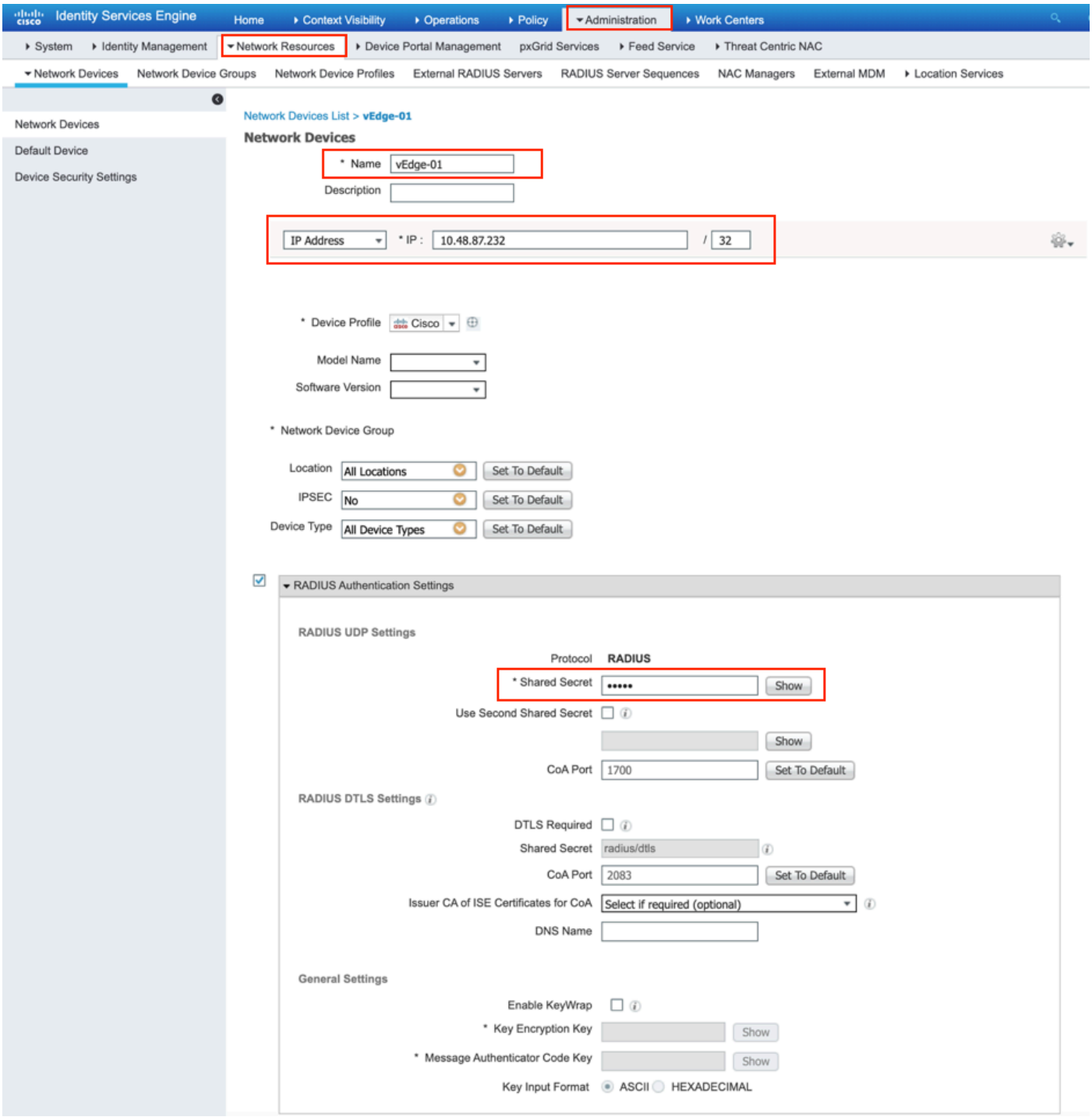


Cliquez sur > et l'écran suivant apparaît comme illustré dans l'image.



Cette stratégie correspond au groupe d'utilisateurs lab_admin et attribue un profil d'autorisation créé à l'étape 3.

Étape 5. Définissez NAS (routeur ou contrôleur vEdge) comme indiqué dans l'image.



Étape 6. Configurez vEdge/Controller.

```
system
 aaa
  auth-order       radius local
  radius
  server 10.48.87.210
   vpn 512
   key cisco
  exit
 !
!
```

Étape 7. Vérification . Connectez-vous à vEdge et assurez-vous que le groupe netadmin est attribué à l'utilisateur distant.

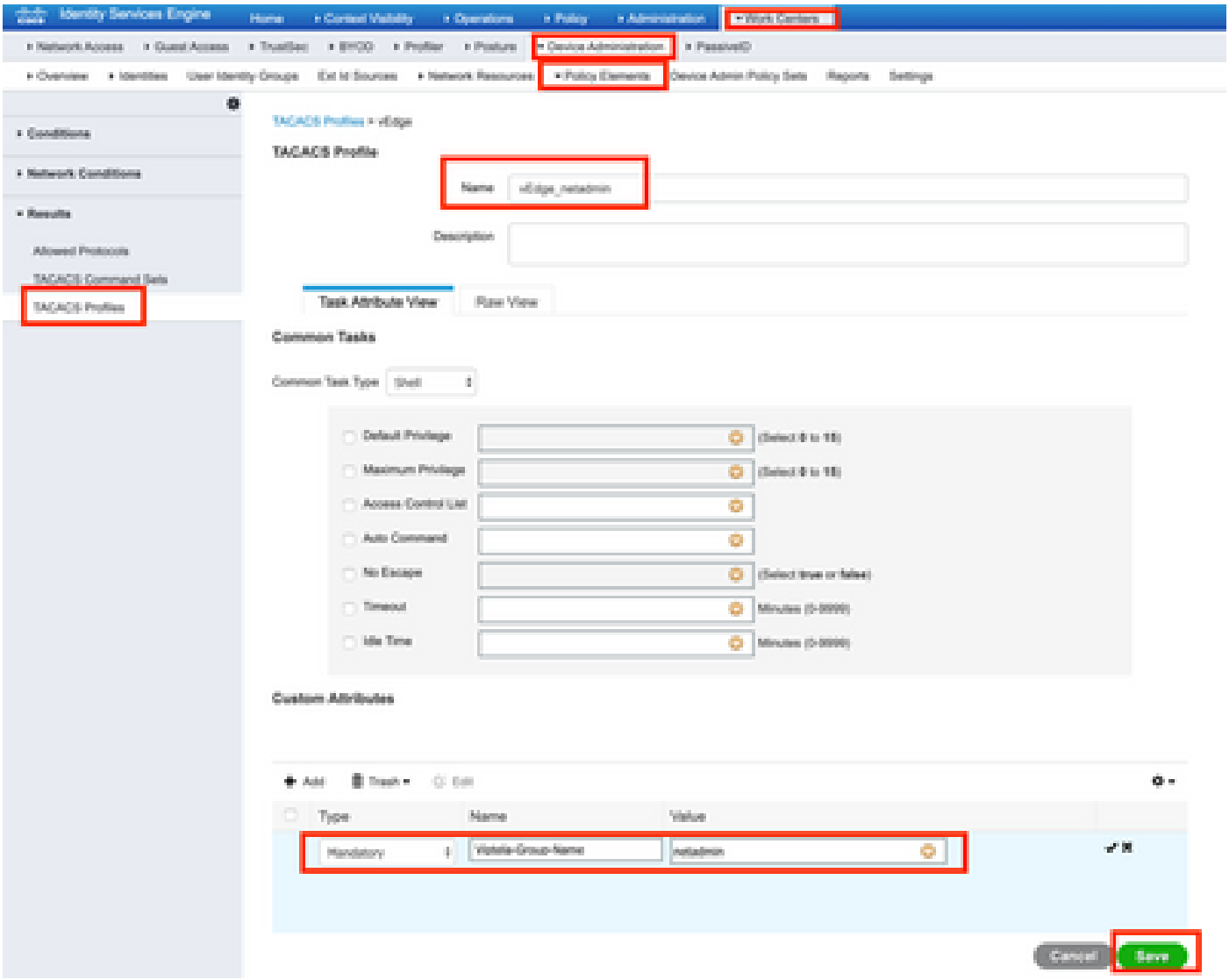
```
vEdgeCloud1# show users

                                                    AUTH
SESSION  USER      CONTEXT  FROM          PROTO  GROUP      LOGIN TIME
-------------------------------------------------------------------------------------
33472    ekhabaro  cli      10.149.4.155  ssh    netadmin   2020-03-09T18:39:40+00:00
```

Authentification et autorisation des utilisateurs basées sur TACACS pour vEdge et les contrôleurs

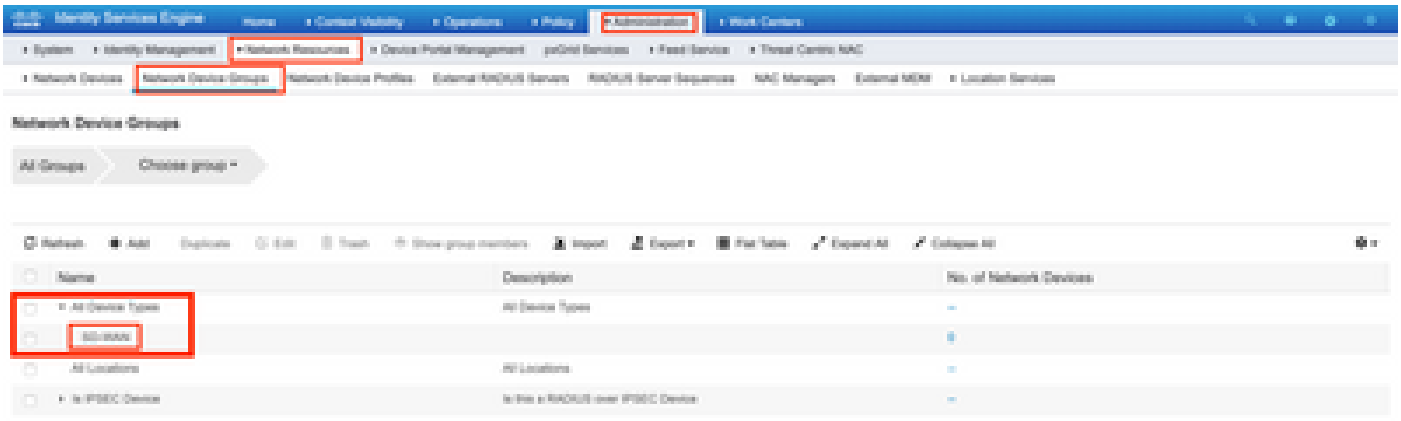
Étape 1. Créez un profil TACACS. Dans cette étape, le profil TACACS créé est affecté, par exemple, au niveau de privilège netadmin à un utilisateur authentifié.

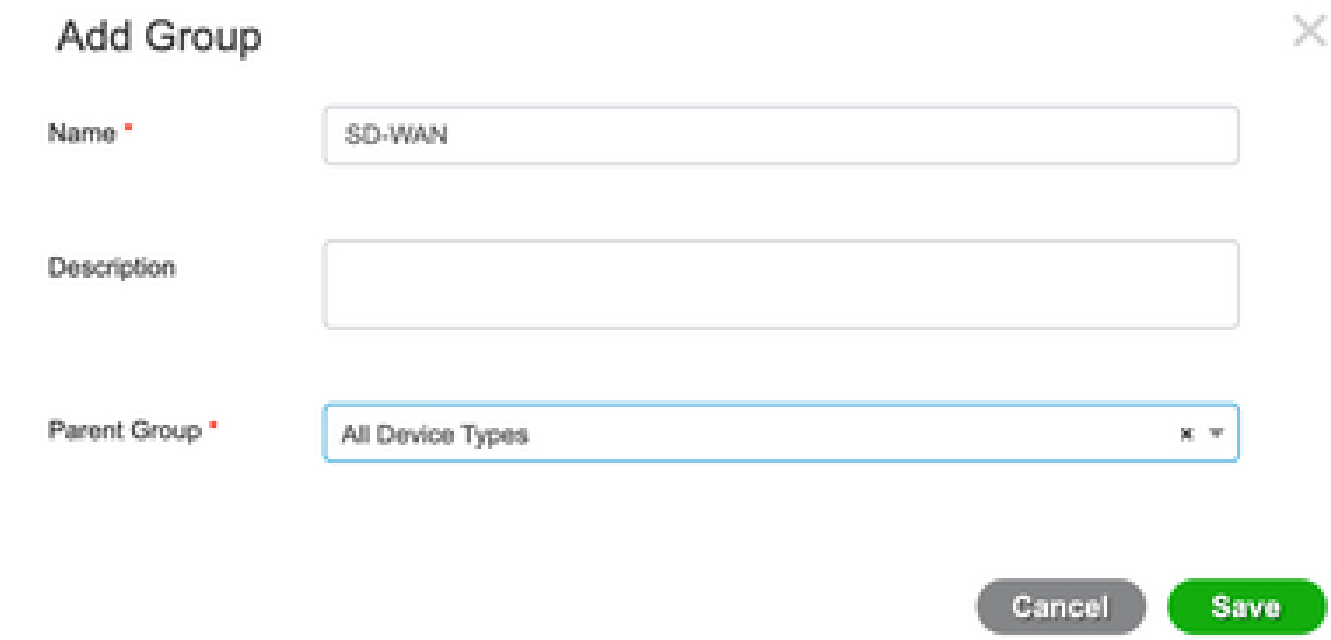
- Sélectionnez Obligatoire dans la section Attribut personnalisé pour ajouter l'attribut comme suit :

Type	Nom	Valeur
Obligatoire	Nom-Groupe-Viptela	netadmin

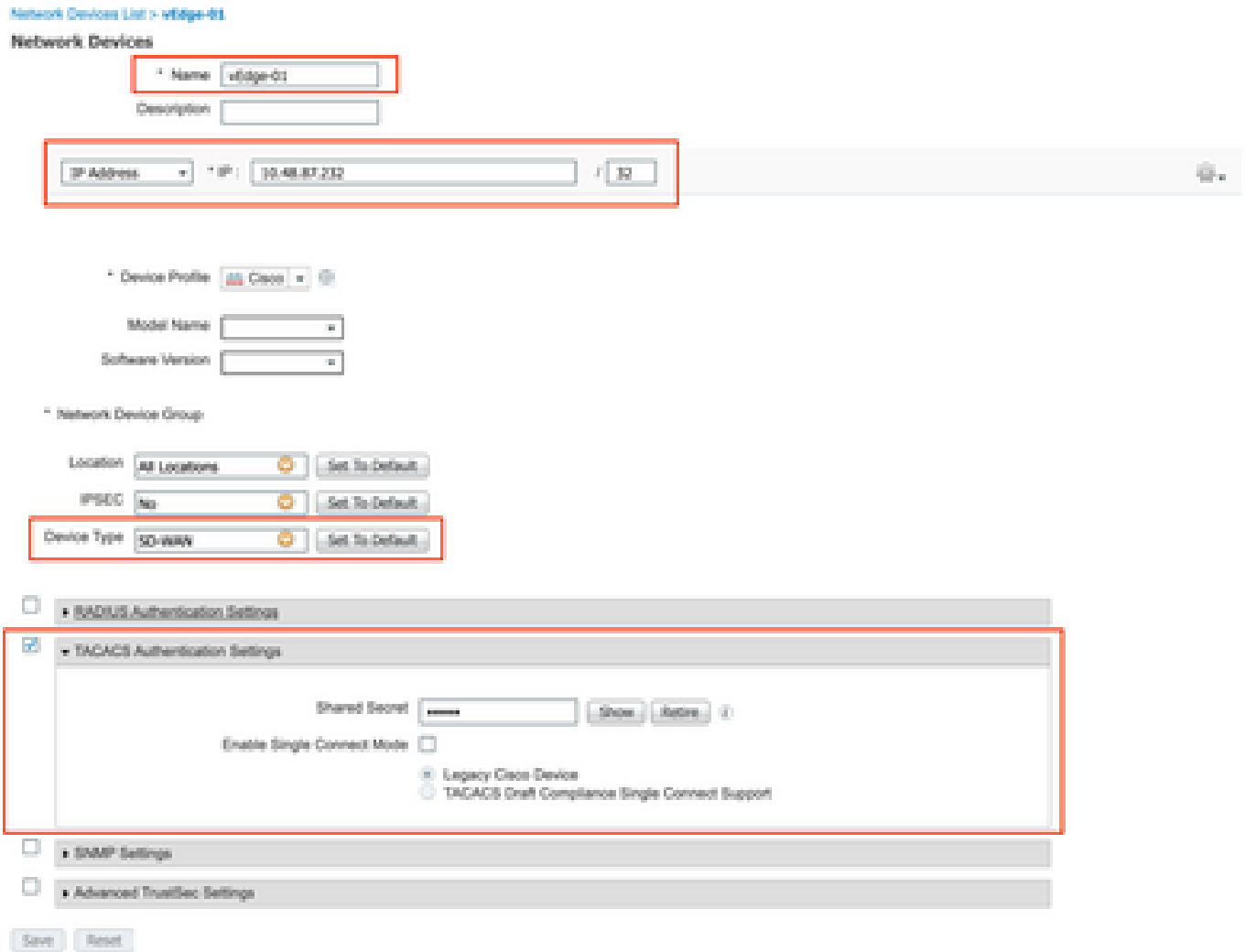


Étape 2. Créez un groupe de périphériques pour SD-WAN.



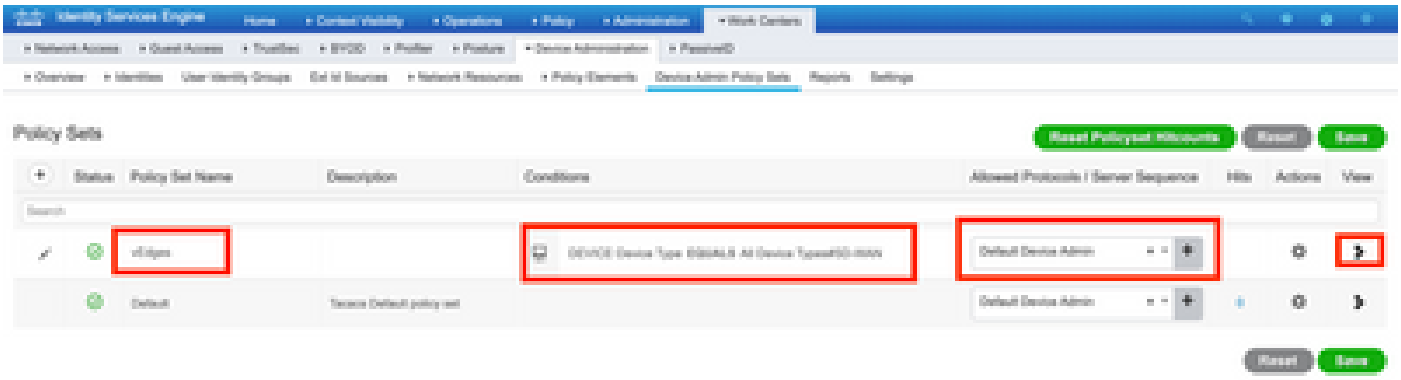


Étape 3. Configurez le périphérique et attribuez-le au groupe de périphériques SD-WAN :

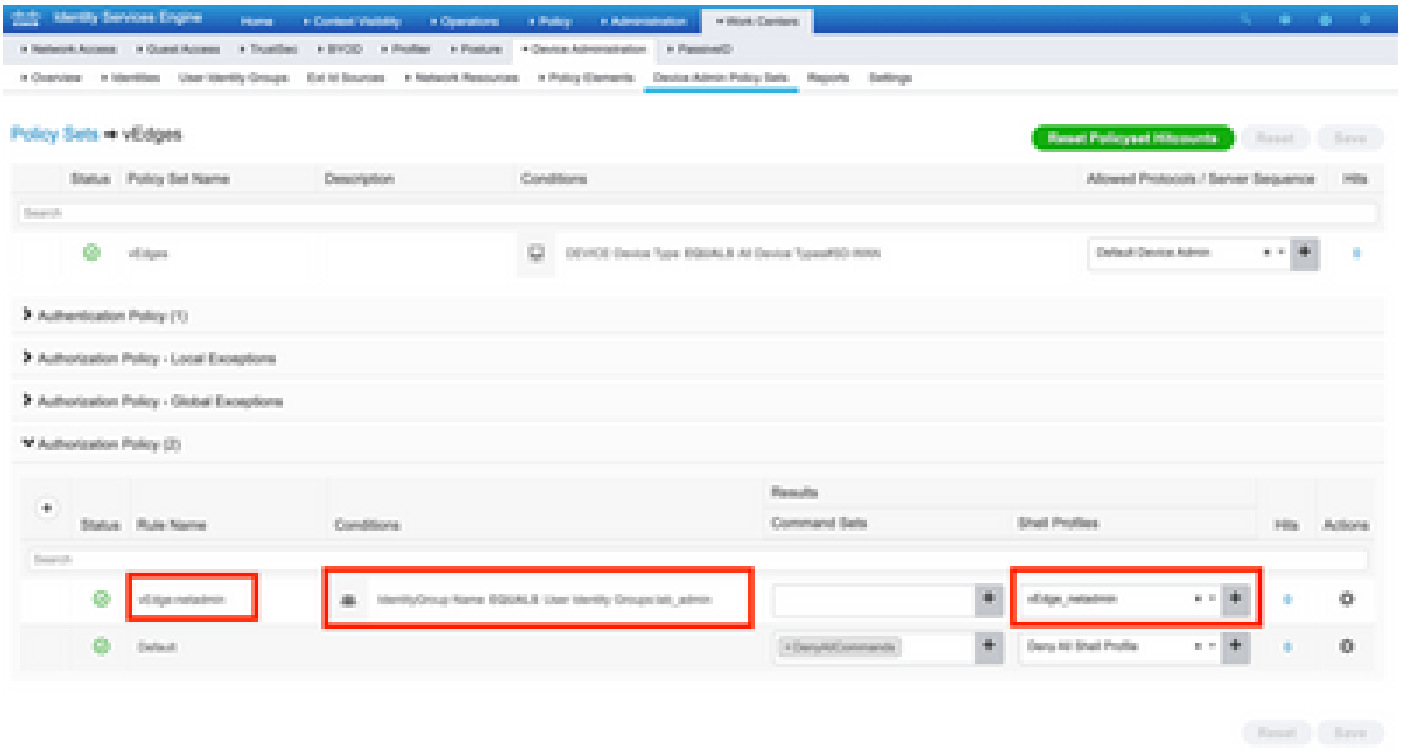


Étape 4. Définissez la politique d'administration des périphériques.

En fonction de votre configuration réelle, votre jeu de stratégies peut avoir un aspect différent. Pour les besoins de la démonstration dans ce document, la politique est créée.



Cliquez sur > et l'écran suivant apparaît comme illustré dans cette image. Cette stratégie correspond en fonction du type de périphérique nommé SD-WAN et attribue le profil Shell qui est créé à l'étape 1.



Étape 5. Configurer vEdge :

```
system
 aaa
  auth-order tacacs local
 !
 tacacs
  server 10.48.87.210
   vpn 512
   key cisco
  exit
 !
!
```

Étape 6. Vérification . Connectez-vous à vEdge et assurez-vous que le groupe netadmin est attribué à l'utilisateur distant :

```
vEdgeCloud1# show users

                                                  AUTH
SESSION  USER      CONTEXT  FROM          PROTO  GROUP      LOGIN TIME
-------------------------------------------------------------------------------
33472    ekhabaro  cli      10.149.4.155  ssh    netadmin   2020-03-09T18:39:40+00:00
```

Informations connexes

- Guide de déploiement prescriptif de Cisco ISE Device Administration : https://community.cisco.com/t5/security-documents/cisco-ise-device-administration-prescriptive-deployment-guide/ta-p/3738365#toc-hId-298630973
- Configuration de l'accès et de l'authentification des utilisateurs : https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/02System_and_Interface

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.