Configurez le CoA SNMP dans le Cisco Identity Services Engine 2.1 et en haut

Contenu

Introduction

Ce document décrit la modification de la caractéristique de l'autorisation (CoA) avec l'utilisation du Protocole SNMP (Simple Network Management Protocol).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de base de SNMP Protocol
- Connaissance préalable des expressions régulières
- Connaissance préalable de l'engine de gestion d'identité de Cisco (ISE)
- Engine 2.1 de gestion d'identité.
- Commutateurs pris en charge par SNMP

[Composants utilisés](#)

Les informations dans ce document sont basées sur la version 2.1 ISE.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un

environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

Informations générales

C'est une nouvelle fonctionnalité introduite dans ISE 2.1. Cette caractéristique complimente une autre nouvelle caractéristique dans ISE à savoir, redirection par ISE elle-même et ne dépend pas des périphériques de réseau. Même si ISE envoie un URL de redirection directement au client d'extrémité, le point final devrait être appliqué avec la stratégie différente après l'authentification dans le portail pour l'accès au réseau approprié. Pour que ceci se produise, dans les versions préalables, ISE a envoyé un CoA de RAYON. Certains des périphériques de réseau ne comprennent pas un CoA de RAYON envoyé par ISE. Puisque le SNMP est pris en charge par presque tous les périphériques d'accès au réseau (NADs), le CoA qui utilise le SNMP est devenu une alternative viable dans un tel scénario. Un CoA SNMP est exécuté par un SNMP SetRequest envoyé d'ISE à un NAD afin de placer certain objet Identifoers (OID) qui gèrent l'état opérationnel d'un port.

Configurez ISE

Il y a deux configurations sur ISE qui doivent être configurés pour que le CoA SNMP fonctionne.

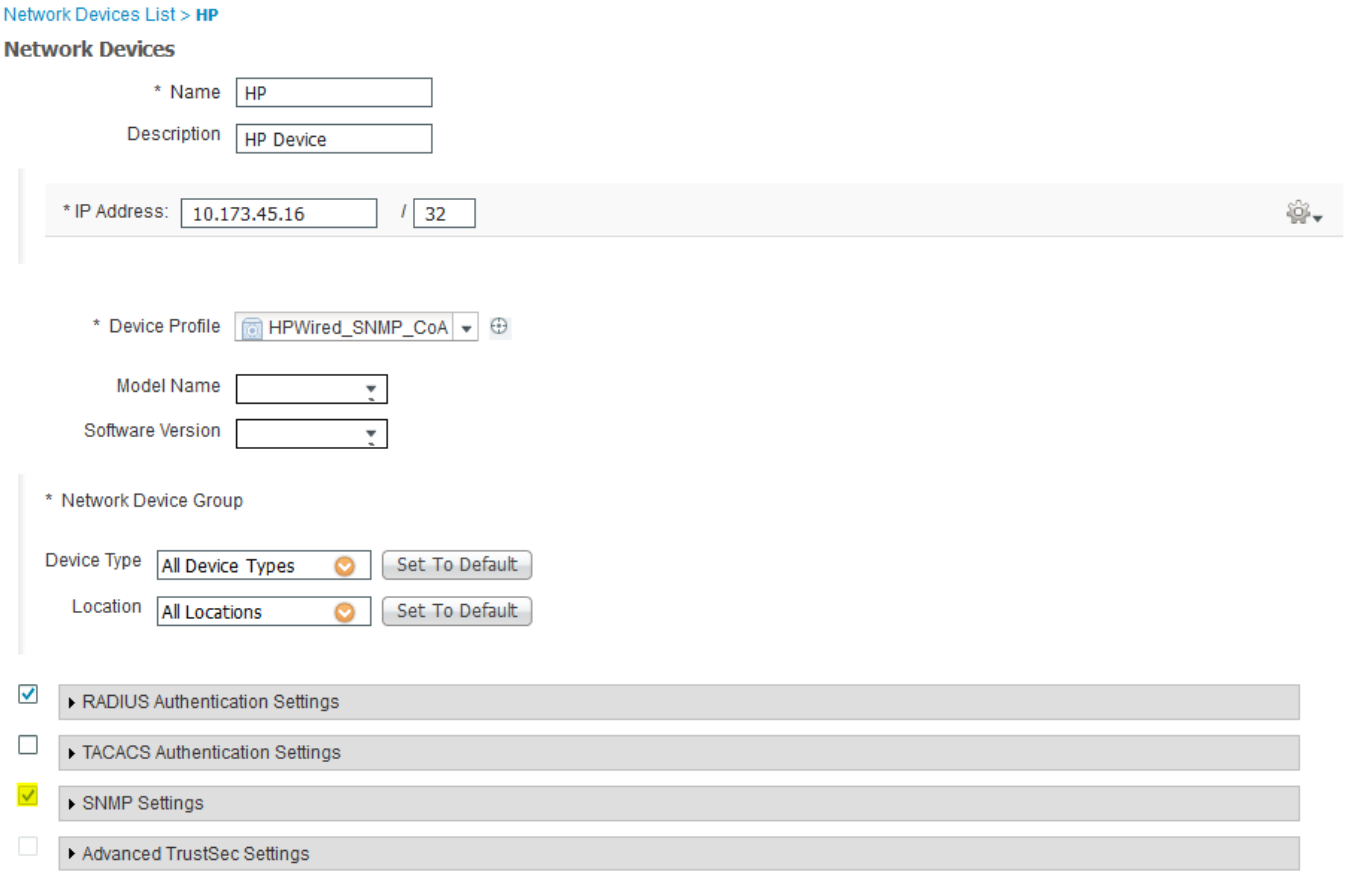
1. Configurations de serveur SNMP d'un NAD.

2. Configurations CoA SNMP d'un profil NAD.

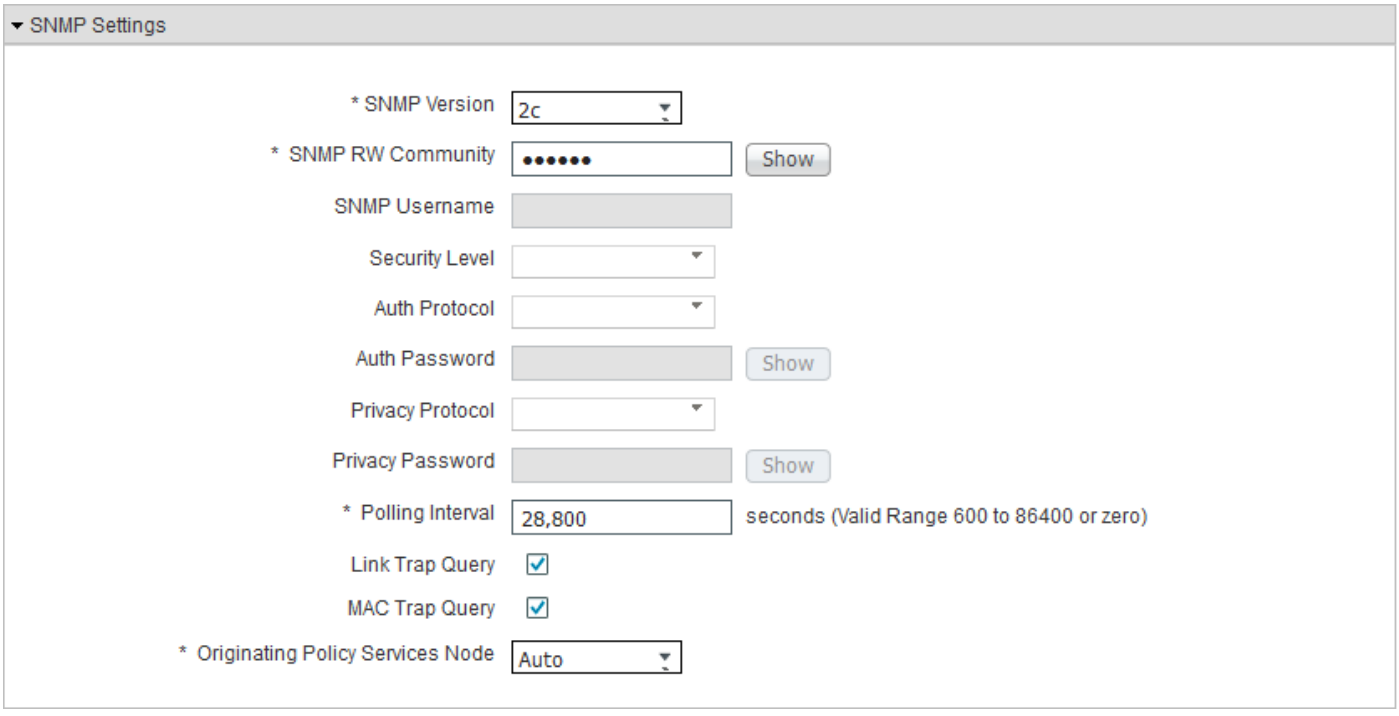
Afin de configurer des configurations de serveur SNMP sur ISE pour un NAD, naviguez vers des **ressources de réseau en Administration> > des périphériques de réseau.**

Configurez les configurations SNMP du NAD

Sélectionnez un NAD. Une case à cocher sera disponible sous les configurations d'authentification TACACS afin d'éditer les configurations SNMP suivant les indications de l'image.



Remplissez configurations selon la condition requise. Un exemple est affiché dans l'image.

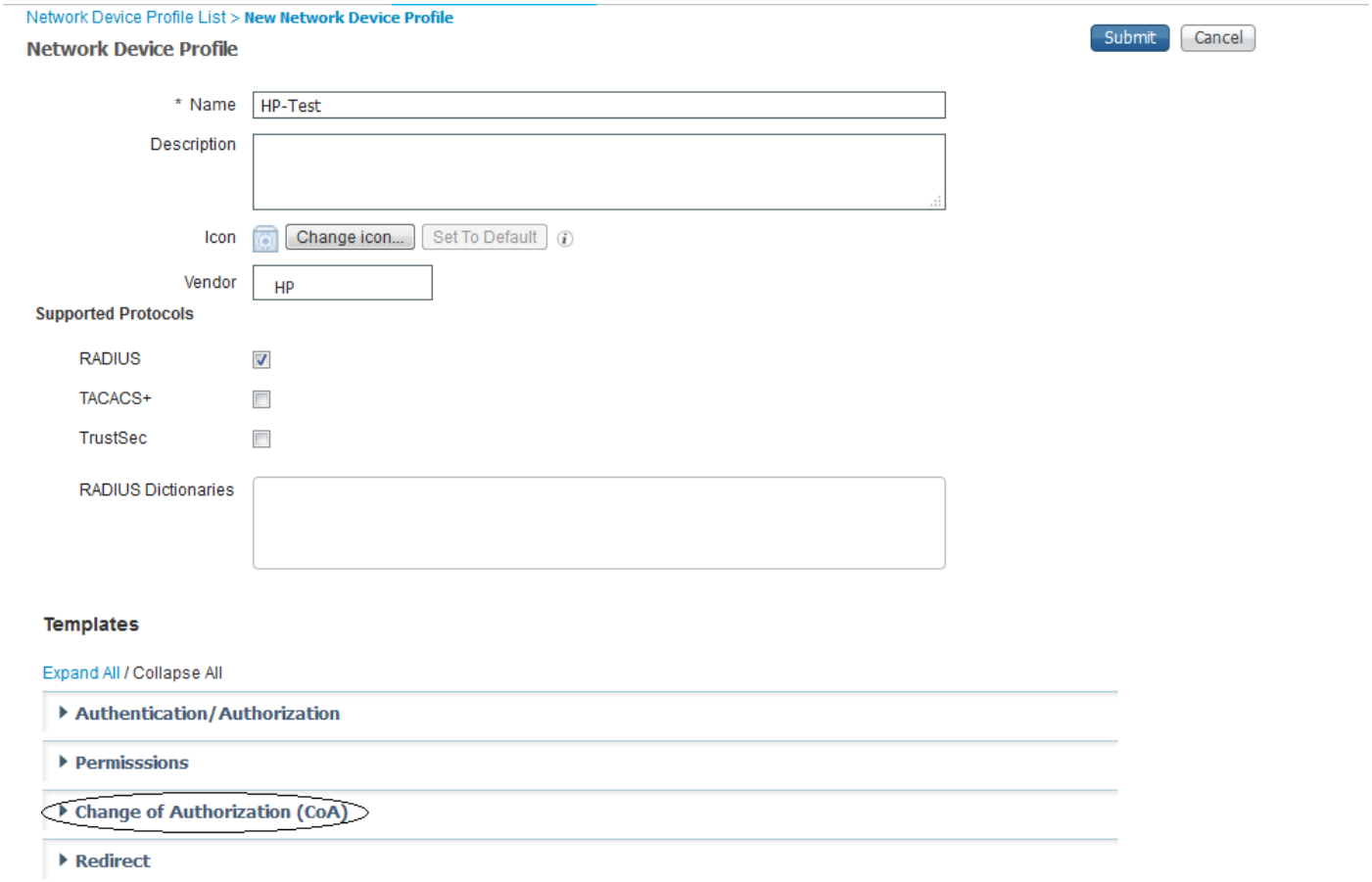


Configurez les configurations CoA SNMP du profil de périphérique de réseau

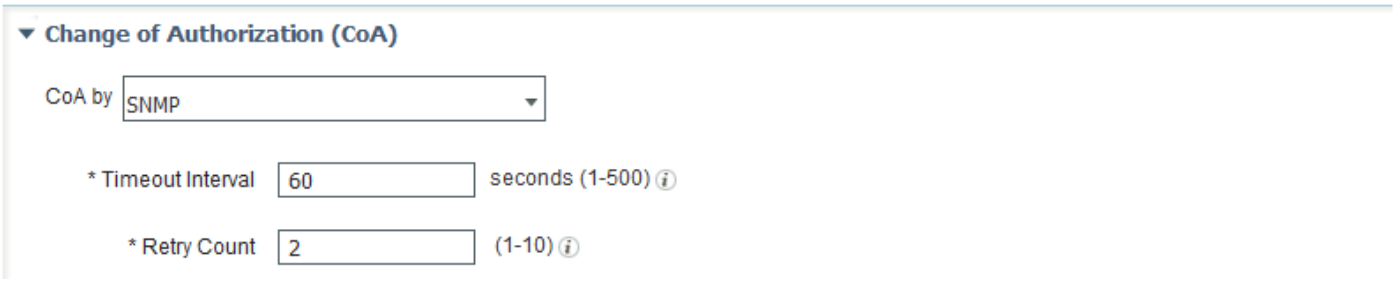
Afin de configurer les configurations CoA SNMP pour un profil de périphérique de réseau, naviguez vers des **profils de périphérique de réseau de Resources> de réseau d'Administration>.**

Sélectionnez le profil de périphérique de réseau pour lequel le CoA SNMP doit être configuré et développez la **modification de l'**onglet d'**autorisation** suivant les indications de l'image.

Note: Des configurations SNMP des profils de périphérique par défaut de réseau ne peuvent pas être éditées.



Sélectionnez le type CoA comme **SNMP** et éditez le délai d'attente SNMP et relancez les configurations. Ces configurations peuvent être placées selon la condition requise. Un exemple est affiché dans cette image.

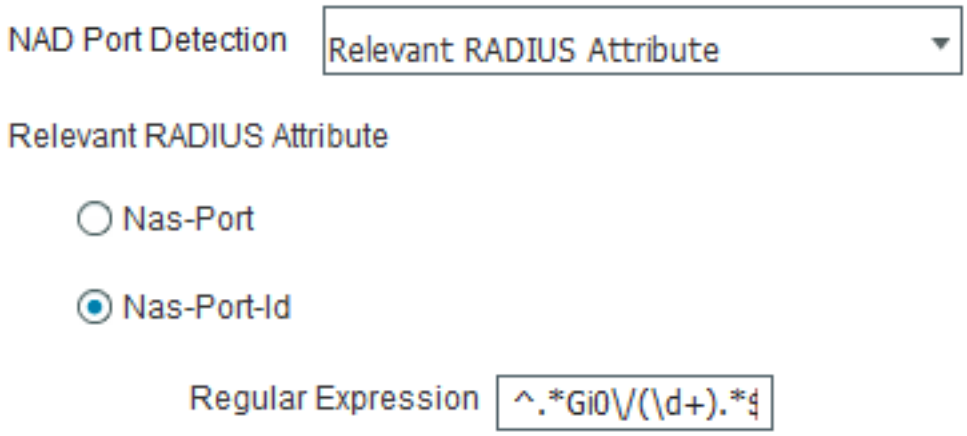


Maintenant, configurez la méthode de dépistage de port NAD par laquelle ISE connaîtrait le port pour lequel les OID devraient être placés. Dorénavant, la seule méthode disponible est de récupérer ces informations de l'attribut RADIUS approprié de l'information de comptabilité.

Les attributs RADIUS disponibles en cours qui fournissent une telle informations sont Nas-port et Nas-Port-id. Des n'importe quels d'entre eux peuvent être choisis ont basé sur l'attribut pris en charge par le NAD. La majeure partie du NADs prend en charge le Nas-Port-id. Les différents constructeurs ont différentes manières de représenter les interfaces disponibles sur le NAD. Une méthode standard d'extraire les informations ne pourrait pas être possible. Par conséquent des expressions régulières sont utilisées dans ISE à la coutume les chaînes à apparier de la valeur d'attribut de Nas-Port-id. Un exemple est donné ici afin d'apparier les ports qui sont sous forme de Gi0/x.

^.*Gi0\/(\d+).*$

Cette expression signifie essentiellement le modèle de début (de ^) (. *) correspondance un certain nombre d'exemples de tout caractère match " (Gi0)match 'Gi0 (\/)/ » (\ d+) correspondance un ou plusieurs qu'une cite de n'importe quel caractère de match any de chiffre (.) (*) (. *) correspondance un certain nombre d'exemples de tout modèle d'extrémité du caractère ($). Cet exemple peut être configuré suivant les indications de cette image.



OID pris en charge par ISE

Par défaut, ISE fournit des options afin de configurer trois types d'OID afin d'exécuter une exécution sur les ports identifiés par la valeur d'attribut de Nas-Port-id.

1. Authentifiez à nouveau

2. Rebond de port

3. Arrêt de port

Authentifiez à nouveau

Authentifiez à nouveau l'OID ne pourrait pas être pris en charge dans le MIB standard utilisé par la plupart des constructeurs. Les informations de cet OID pourraient varier du constructeur au constructeur.

> **Note**: Cette option est donnée pour la future amélioration possible si tous les débuts de périphérique de prendre en charge un OID pour gérer des sessions d'utilisateur basées sur le mac-address.

Rebond de port

Le rebond de port utilise un port OID opérationnel qui a deux valeurs, une pour fermer le port et les autres pour Unshutting le port. Ce sont des OID standard utilisés par la plupart des constructeurs.

1.3.6.1.2.1.2.2.1.7.$port est l'OID

Si la valeur est placée à 2, le port est arrêt et si la valeur est placée à 1, le port est unshut.

Arrêt de port

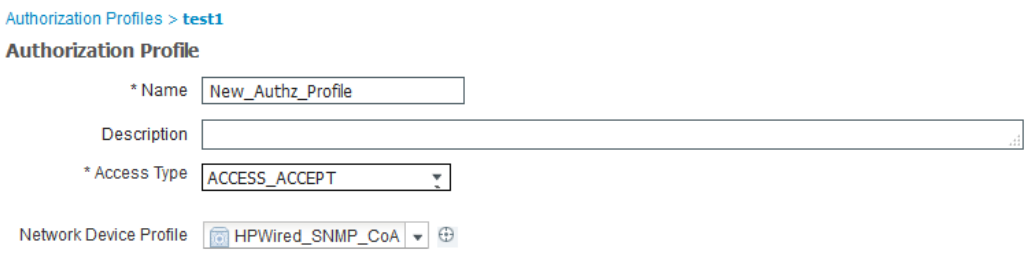
Sélectionnez l'exécution désirée qui doit être exécutée sur ce port spécifique suivant les indications de l'image.

> **Attention** : La commande dans laquelle l'OID évalue sont envoyées est très importante. Puisque, la commande dans laquelle l'OID évalue sont réglée est la commande dans laquelle les exécutions sont exécutées sur le port. S'ils sont placés dans un ordre inverse, dites 1 et puis 2, un port d'abord et puis serait unshut l'arrêt qui essentiellement arrête le port.

Soumettez les modifications au profil de périphérique.

Ce profil de périphérique peut être utilisé dans n'importe quel profil d'autorisation à prendre dans l'affect. N'importe quelle exécution CoA qui doit être exécutée pour un point final sera envoyée comme SNMP SetRequest au commutateur avec les OID configurés à placer sur le port sur lequel le point final est connecté. Voici un exemple afin de configurer le profil NAD dans le profil d'autorisation.

Pour créer une nouvelle stratégie d'autorisation ou éditer celui qui existe déjà, naviguez vers la **stratégie > les éléments de stratégie > les résultats > l'autorisation > les profils d'autorisation** suivant les indications de l'image.



> **Note**: Le commutateur doit être configuré avec ISE en tant que serveur SNMP et devrait utiliser la même chaîne de la communauté qui est configurée sur ISE. La configuration du commutateur est hors de portée de ce document.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.