Configurer la CoA SNMP dans Identity Services Engine 2.1 et versions ultérieures

Contenu

Introduction

Ce document décrit la fonctionnalité de modification d'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 :

- Connaissances de base du protocole SNMP
- Connaissance préalable des expressions régulières
- Connaissance préalable de Cisco Identity Service Engine (ISE)
- Identity Service Engine 2.1.
- Commutateurs SNMP pris en charge

Components Used

Les informations de ce document sont basées sur ISE version 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.

Informations générales

Il s'agit d'une nouvelle fonctionnalité introduite dans ISE 2.1. Cette fonctionnalité complète une autre nouvelle fonctionnalité de ISE viz., la redirection par ISE elle-même et ne dépend pas des périphériques réseau. Même si ISE envoie une URL de redirection directement au client final, le point de terminaison doit être appliqué avec une politique différente après l'authentification dans le portail pour un accès réseau approprié. Pour cela, dans les versions précédentes, ISE a envoyé une CoA RADIUS. Certains périphériques réseau ne comprennent pas la CoA RADIUS envoyée par ISE. Puisque SNMP est pris en charge par presque tous les périphériques d'accès réseau (NAD), CoA qui utilise SNMP est devenu une option viable dans un tel scénario. Une CoA SNMP est exécutée par une requête SetRequest SNMP envoyée par ISE à un NAD afin de définir certains OID (Object Identifoers) qui gèrent l'état opérationnel d'un port.

Configurer ISE

Il existe deux paramètres sur ISE qui doivent être configurés pour que la CoA SNMP fonctionne.

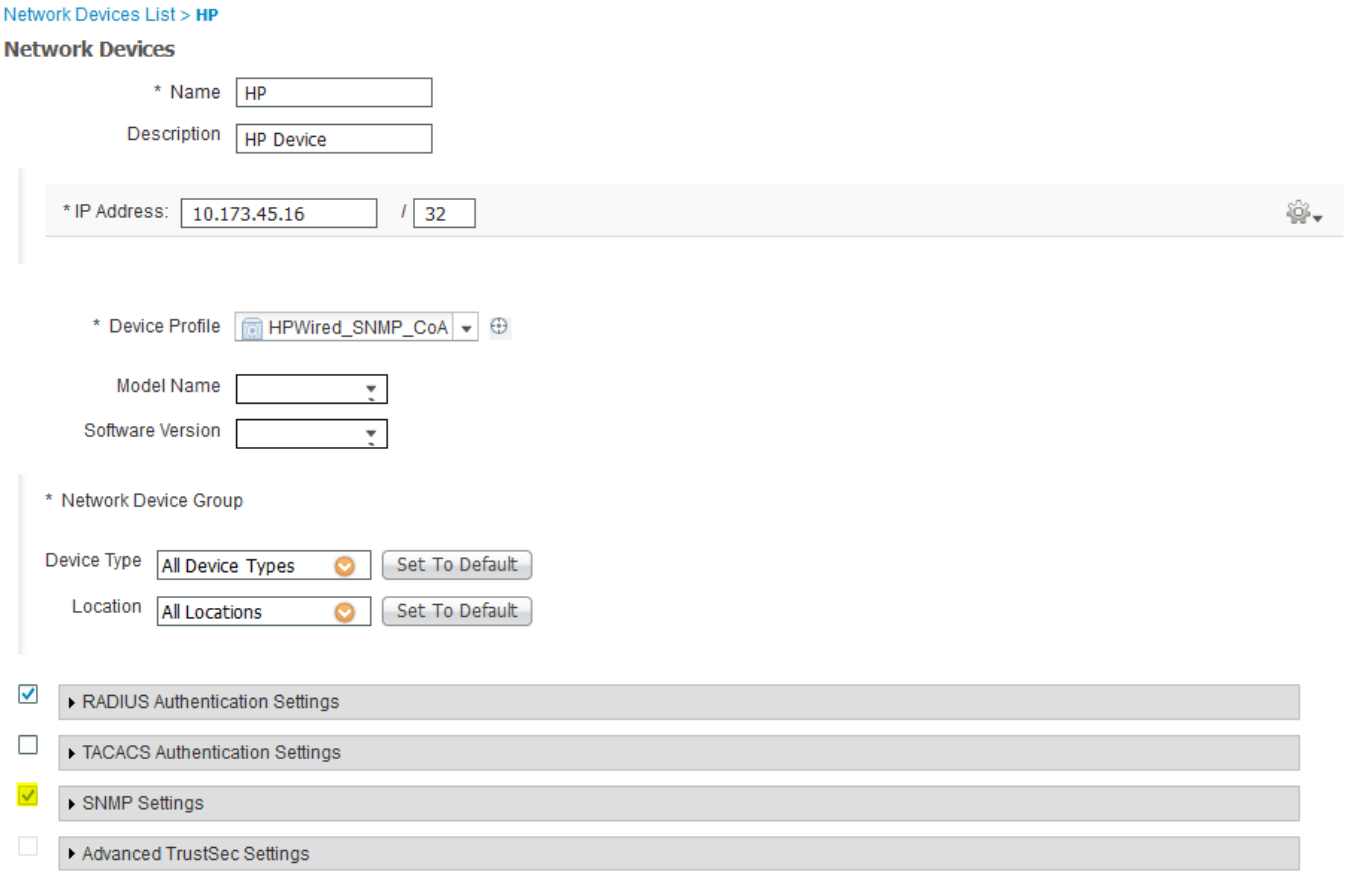
1. Paramètres du serveur SNMP d'une NAD.

2. Paramètres de CoA SNMP d'un profil NAD.

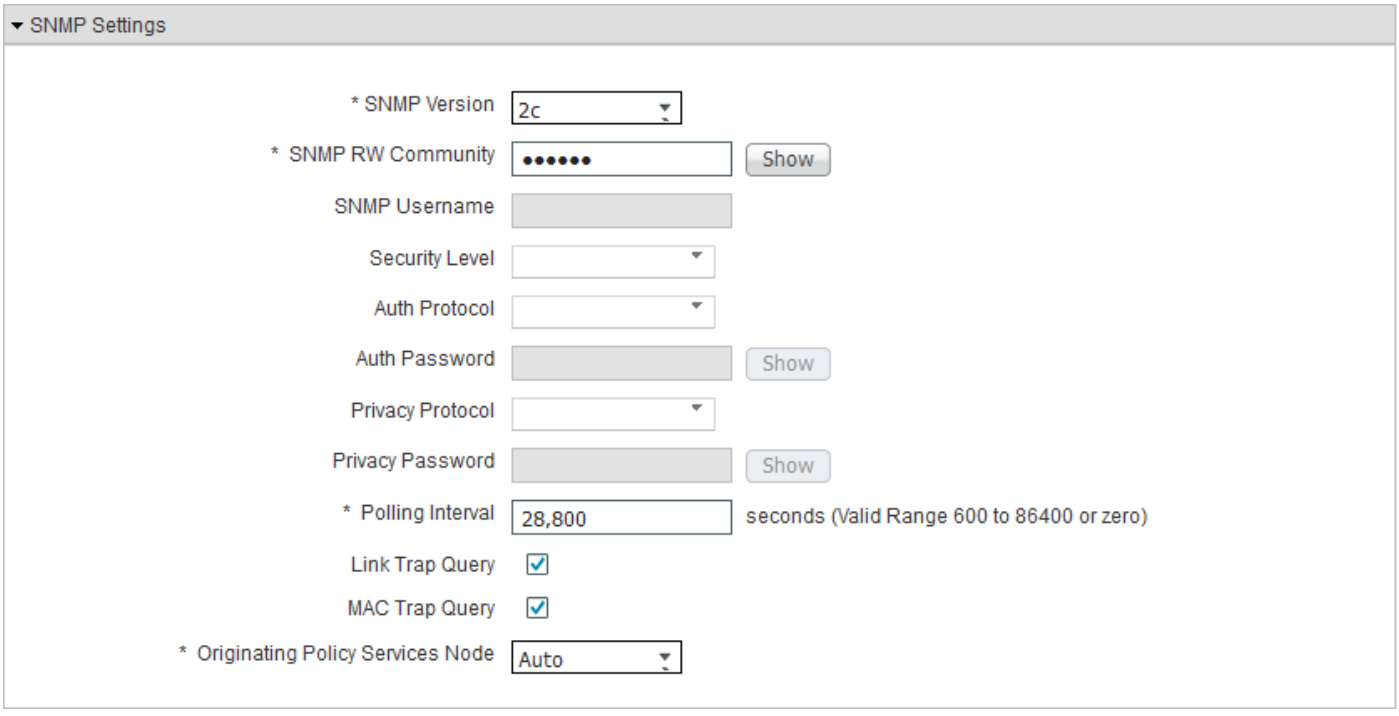
Afin de configurer les paramètres du serveur SNMP sur ISE pour un NAD, accédez à **Administration > Network Resources > Network Devices.**

Configuration des paramètres SNMP de NAD

Sélectionnez un NAD. Une case à cocher sera disponible sous les paramètres d'authentification TACACS afin de modifier les paramètres SNMP comme indiqué dans l'image.



Remplissez les paramètres en fonction des besoins. Un exemple est présenté dans l'image.

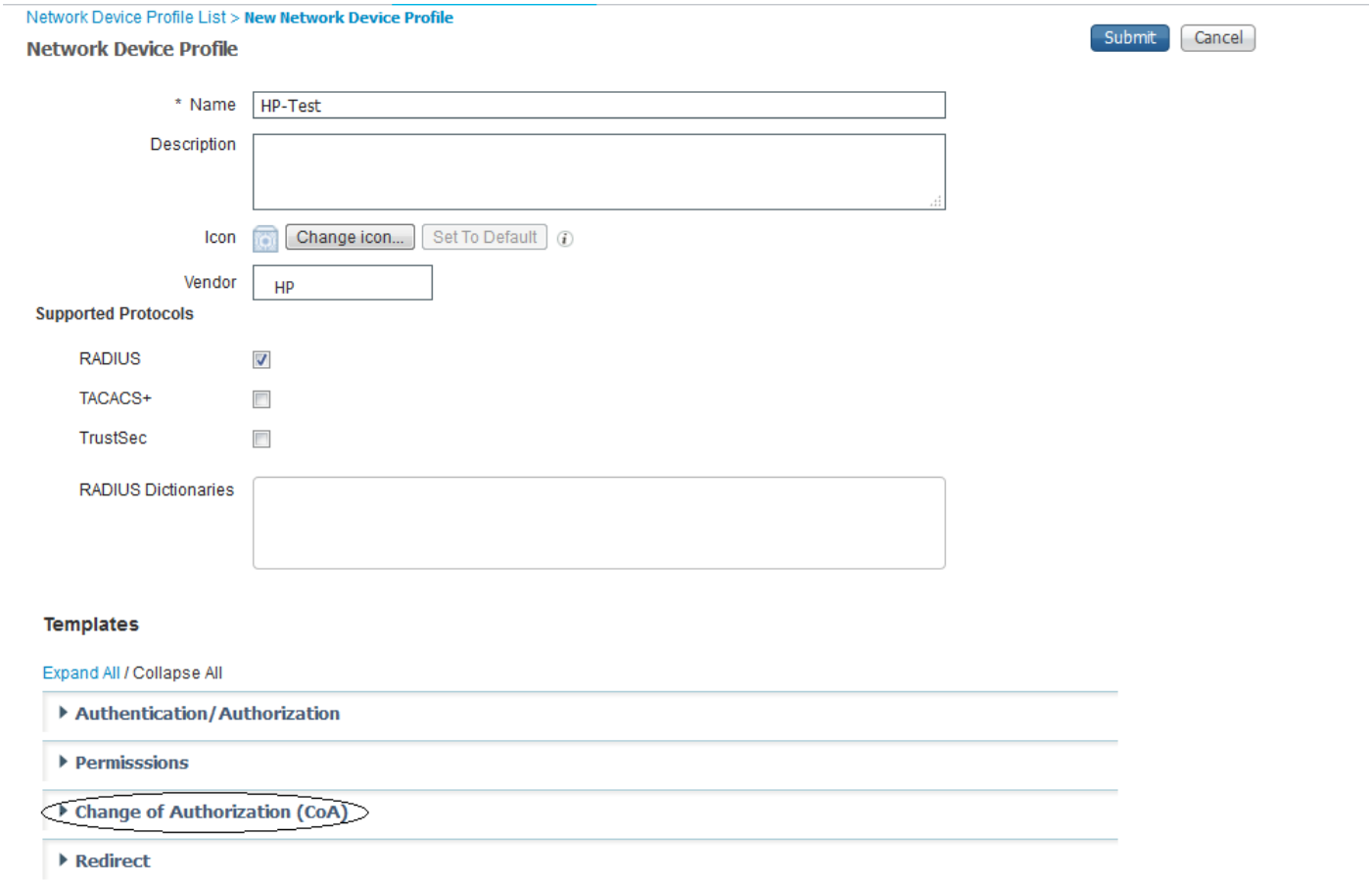


Configurer les paramètres de CoA SNMP du profil de périphérique réseau

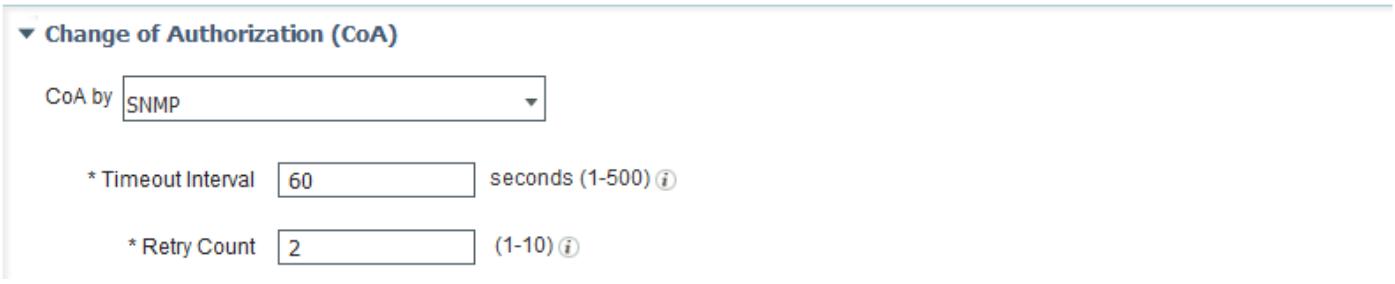
Afin de configurer les paramètres de CoA SNMP pour un profil de périphérique réseau, accédez à **Administration > Network Resources > Network Device Profiles.**

Sélectionnez le profil de périphérique réseau pour lequel la CoA SNMP doit être configurée et développez l'onglet **Modification de l'autorisation** comme illustré dans l'image.

Note: Impossible de modifier les paramètres SNMP des profils de périphérique réseau par défaut.



Sélectionnez le type CoA **SNMP** et modifiez les paramètres de temporisation et de nouvelle tentative SNMP. Ces paramètres peuvent être définis en fonction des besoins. Un exemple est présenté dans cette image.

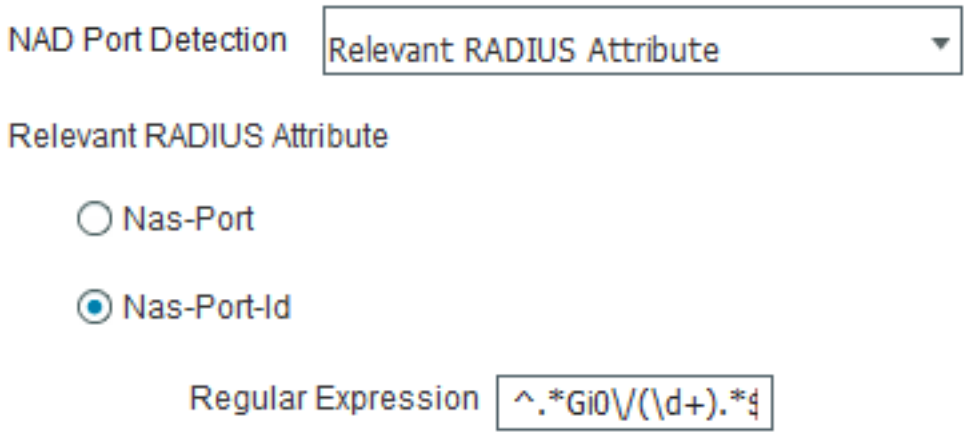


Maintenant, configurez la méthode NAD Port Detection par laquelle ISE connaîtrait le port pour lequel les OID doivent être définis. À ce jour, la seule méthode disponible est de récupérer ces informations de l'attribut RADIUS approprié à partir des informations de comptabilité.

Les attributs RADIUS disponibles actuels qui fournissent ces informations sont NAS-Port et NAS-Port-Id. N'importe lequel d'entre eux peut être choisi en fonction de l'attribut pris en charge par la NAD. La plupart des NAD prennent en charge NAS-Port-Id. Différents fournisseurs proposent différentes manières de représenter les interfaces disponibles sur la NAD. Il n'est peut-être pas possible d'extraire l'information de manière standard. Par conséquent, des expressions régulières sont utilisées dans ISE pour personnaliser les chaînes à associer à partir de la valeur d'attribut NAS-Port-Id. Un exemple est donné ici afin de faire correspondre les ports qui sont sous la forme de Gi0/x.

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

Cette expression signifie essentiellement que (^)start pattern (.*)match n'importe quel nombre d'instances d'un caractère (Gi0)match 'Gi0' (\/)match '/' (\d+)match une ou plusieurs instances d'un chiffre (.)match any charecter (*) (.*)match n'importe quel nombre d'instances d'un modèle de fin de caractère ($). Cet exemple peut être configuré comme illustré dans cette image.



OID pris en charge par ISE

Par défaut, ISE fournit des options afin de configurer trois types d'OID afin d'effectuer une opération sur les ports identifiés par la valeur d'attribut NAS-Port-Id.

1. Réauthentifier

2. Rebondissement du port

3. Arrêt du port

Réauthentifier

La réauthentification de l'OID peut ne pas être prise en charge dans les MIB standard utilisées par la plupart des fournisseurs. Les informations de cet OID peuvent varier d'un fournisseur à l'autre.

> **Note**: Cette option est fournie pour une éventuelle amélioration future si un périphérique commence à prendre en charge un OID pour gérer les sessions utilisateur en fonction de l'adresse MAC.

Rebondissement du port

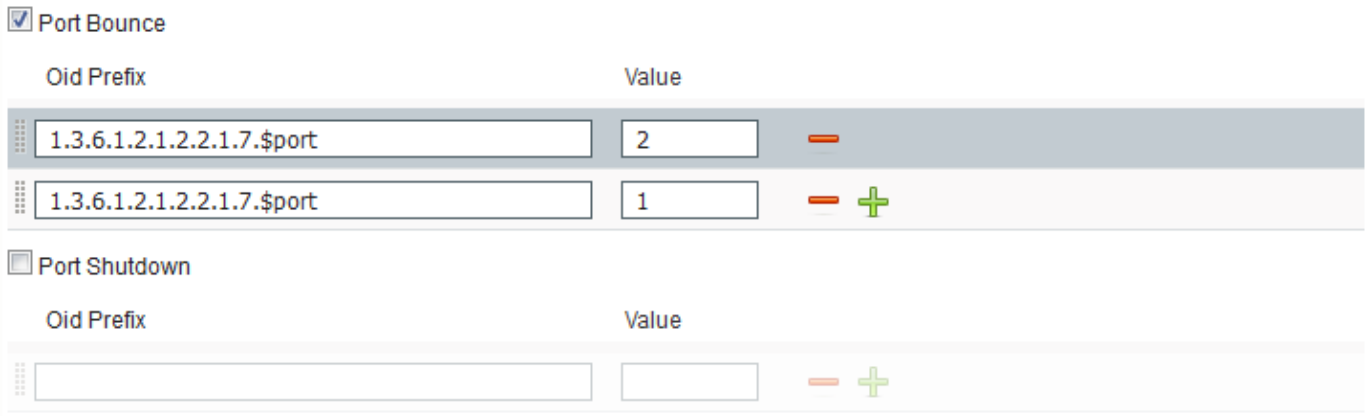
Le renvoi de port utilise un OID opérationnel de port qui a deux valeurs, l'une pour arrêter le port et l'autre pour annuler l'arrêt du port. Il s'agit d'OID standard utilisés par la plupart des fournisseurs.

1.3.6.1.2.1.2.2.1.7.$port est l'OID

Si la valeur est définie sur 2, le port est arrêté et si la valeur est définie sur 1, le port est désactivé.

Arrêt du port

Sélectionnez l'opération souhaitée qui doit être effectuée sur ce port spécifique, comme indiqué dans l'image.

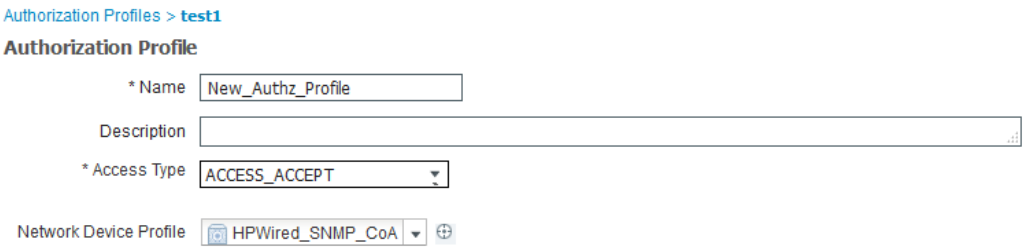


> **Attention** : L'ordre dans lequel les valeurs OID sont envoyées est très important. Parce que, l'ordre dans lequel les valeurs OID sont définies est l'ordre dans lequel les opérations sont effectuées sur le port. S'ils sont définis dans un ordre inverse, disons 1 et 2, un port serait d'abord désactivé, puis arrêté, ce qui est essentiellement en train d'arrêter le port.

Envoyez les modifications au profil du périphérique.

Ce profil de périphérique peut être utilisé dans n'importe quel profil d'autorisation à prendre en compte. Toute opération CoA qui doit être effectuée pour un point de terminaison sera envoyée en tant que SNMP SetRequest au commutateur avec les OID configurés à définir sur le port sur lequel le point de terminaison est connecté. Voici un exemple afin de configurer le profil NAD dans le profil d'autorisation.

Pour créer une nouvelle stratégie d'autorisation ou pour modifier celle qui existe déjà, accédez à **Stratégie > Éléments de stratégie > Résultats > Autorisation > Profils d'autorisation** comme indiqué dans l'image.



> **Note**: Le commutateur doit être configuré avec ISE comme serveur SNMP et utiliser la même chaîne de communauté que celle configurée sur ISE. La configuration du commutateur n'est pas comprise dans ce document.

Vérification

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

Dépannage

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