SNMP CoA configureren in Identity Services Engine 2.1 en hoger

Inhoud

Inleiding

In dit document wordt de optie Automation (CoA) gewijzigd met behulp van Simple Network Management Protocol (SNMP).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van SNMP-protocol
- Voorafgaande kennis van reguliere expressies
- Voorafgaande kennis van Cisco Identity Services Engine (ISE)
- Identity Services Engine 2.1.
- SNMP-ondersteunde switches

Gebruikte componenten

De informatie in dit document is gebaseerd op ISE versie 2.1.

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Dit is een nieuwe functie die in ISE 2.1 is geïntroduceerd. Deze functie vult een andere nieuwe functie in ISE, namelijk, omleiding door ISE zelf en is niet afhankelijk van Network Devices. Zelfs als ISE direct een URL naar de eindclient verstuurt, zou het eindpunt met verschillend beleid na de authenticatie in het portaal voor geëigende netwerktoegang moeten worden toegepast. Om dit te laten gebeuren, in vorige versies, stuurde ISE een RADIUS CoA. Sommige netwerkapparaten begrijpen geen RADIUS CoA die door ISE wordt verstuurd. Aangezien SNMP wordt ondersteund door vrijwel alle Network Access Devices (NAD's), is CoA dat SNMP gebruikt in zo'n scenario een levensvatbare optie geworden. Een SNMP CoA wordt uitgevoerd door een SNMP SetApplication van ISE naar een NAD verzonden om bepaalde Objectidentificatoren (OIDs) in te stellen die de operationele status van een haven beheren.

ISE configureren

Er zijn twee instellingen op ISE die moeten worden geconfigureerd voor het SNMP CoA.

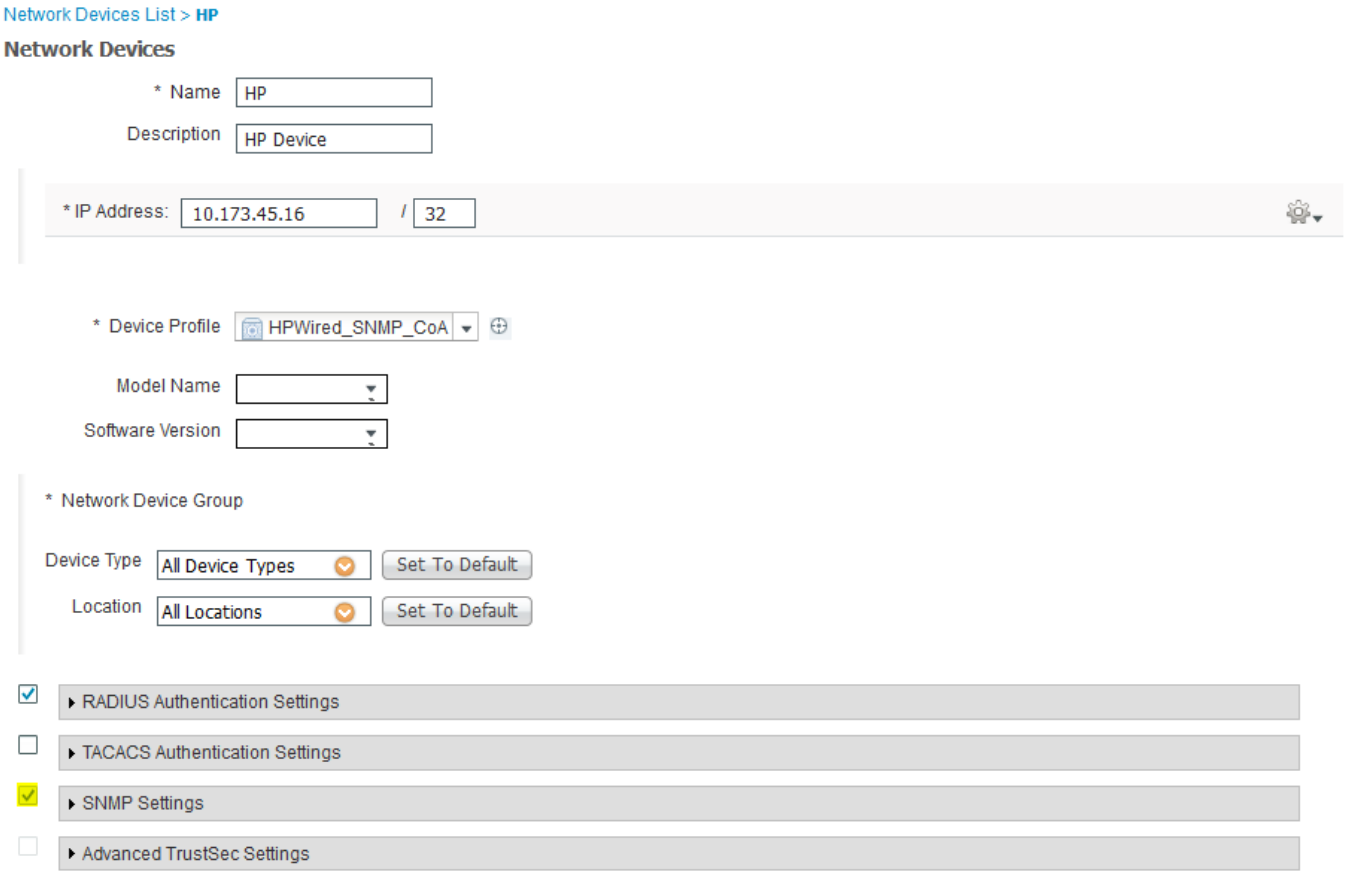
1. SNMP-serverinstellingen van een NAD.

2. SNMP CoA-instellingen van een NAD-profiel.

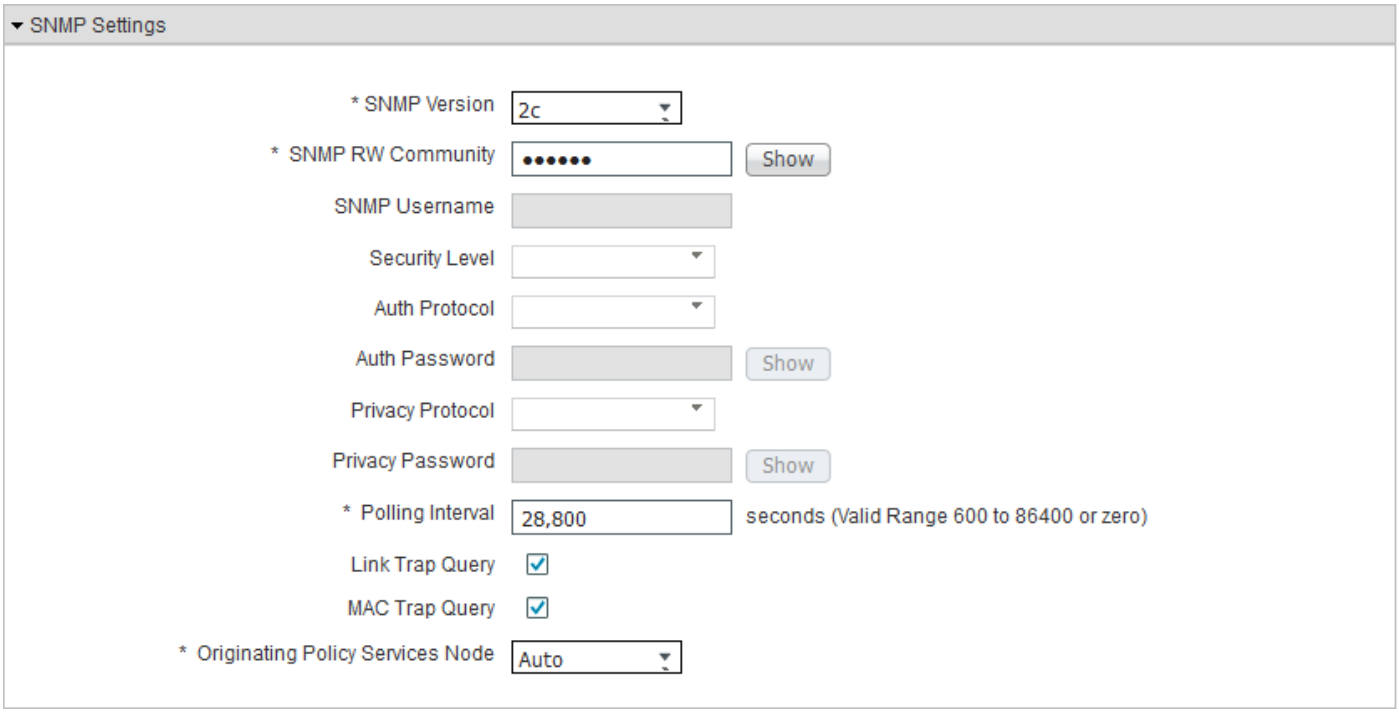
Om SNMP serverinstellingen op ISE voor een NAD te configureren navigeer naar **Netwerkbronnen > Netwerkapparaten.**

SNMP-instellingen voor NAD configureren

Selecteer een NAD. Onder de TACACS-verificatie-instellingen is een selectieteken beschikbaar om de SNMP-instellingen te bewerken zoals in de afbeelding.



Populeer de instellingen volgens de vereiste. In de afbeelding wordt een voorbeeld getoond.

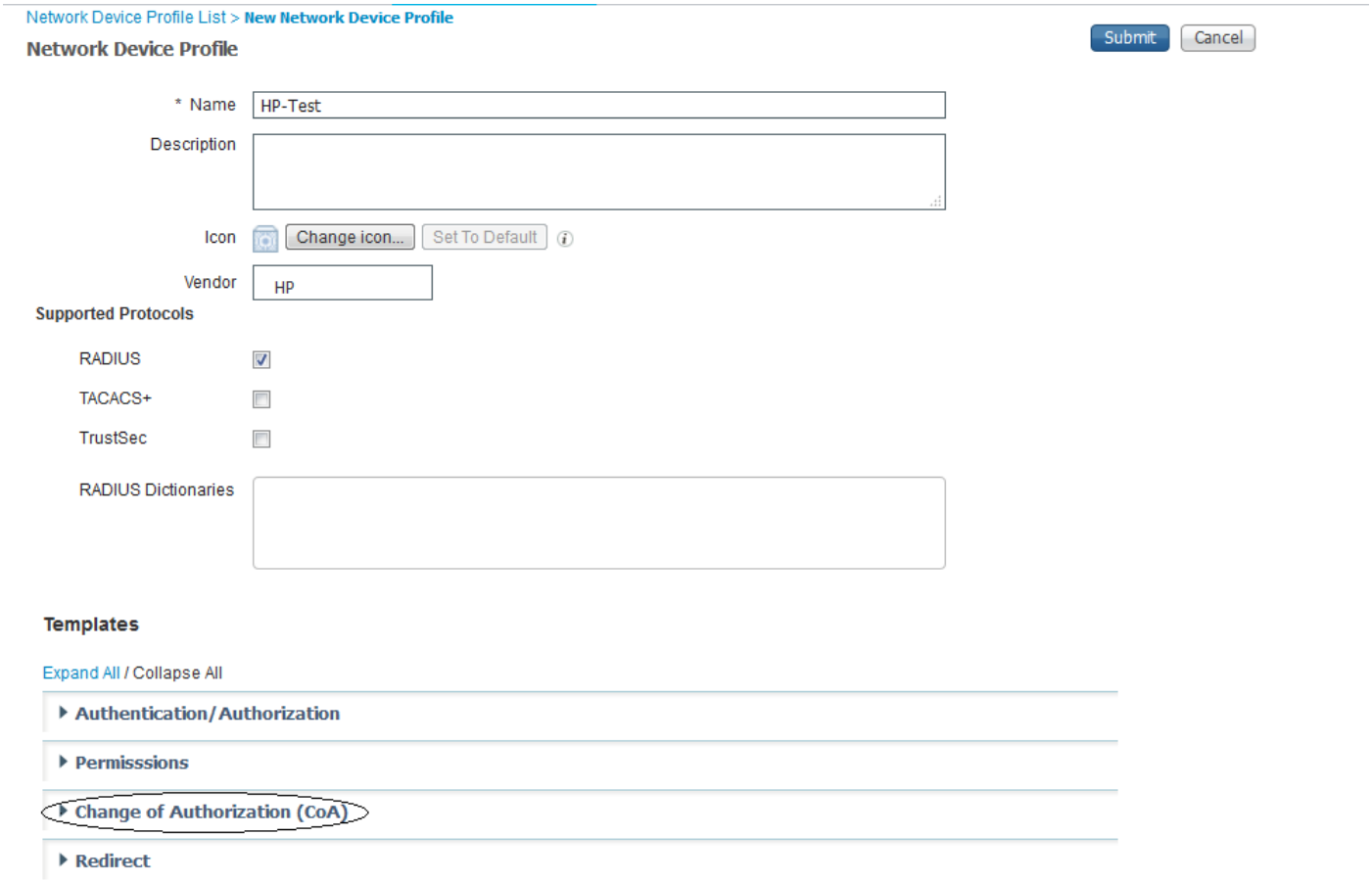


SNMP CoA-instellingen van netwerkapparaatprofiel configureren

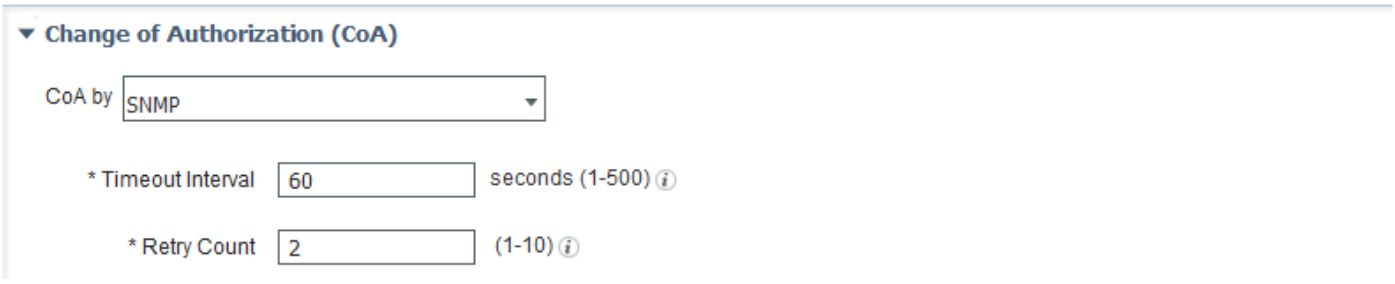
Om de SNMP CoA-instellingen te configureren voor een netwerkapparaatprofiel, dient u te navigeren naar **Netwerkprofielen** van **> Netwerkbronnen>.**

Selecteer het profiel van het netwerkapparaat waarvoor SNMP CoA moet worden geconfigureerd en breid **het** tabblad **Wijzigen van** de **autorisatie uit** zoals in de afbeelding.

Opmerking: SNMP-instellingen van standaard netwerkapparaatprofielen kunnen niet worden bewerkt.



Selecteer het CoA-type als **SNMP** en bewerk de instellingen voor de SNMP-tijdelijke oplossing en opnieuw proberen. Deze instellingen kunnen worden ingesteld naar wens. In deze afbeelding wordt een voorbeeld getoond.

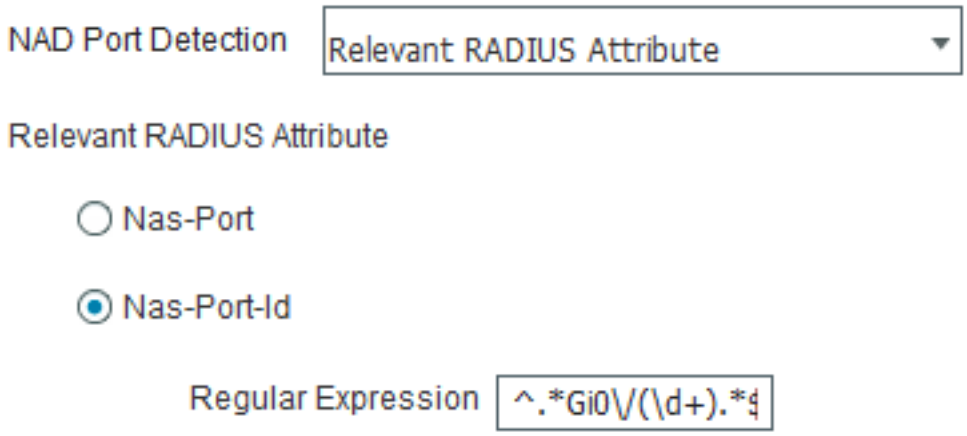


Stel nu de NAD Port Detectiemethode in waarmee ISE de poort weet waarvoor de OIDs moeten worden ingesteld. Tot nu toe is de enige beschikbare methode om die informatie uit de desbetreffende RADIUS-eigenschap van de boekhoudkundige informatie op te halen.

De huidige beschikbare RADIUS-kenmerken die dergelijke informatie geven, zijn NAS-poorts en NAS-Port-ID. Elk van deze kenmerken kan worden gekozen op basis van de door de NAD ondersteunde eigenschap. De meeste NAD's ondersteunen NAS-Port-ID. Verschillende verkopers hebben verschillende manieren om de interfaces beschikbaar op de NAD weer te geven. Een standaardmanier om de informatie op te vragen is misschien niet mogelijk. Daarom worden in ISE reguliere expressies gebruikt om de string die gecompenseerd moet worden van de waarde van de NAS-Port-ID eigenschap aan te passen. Hier wordt een voorbeeld gegeven om de havens aan te passen die in de vorm van Gi0/x zijn.

^.*i0\/(\d+)*$

Deze expressie betekent in wezen (^)start patroon (.*) overeenkomend met elk aantal gevallen van een charecter (Gi0) match 'Gi0' (\/)match '/' (\d+) overeenkomend met een of meer dan één gevallen van een cijferig (.) overeenkomend met een charecter (*) (.*) gelijk aan elk aantal gevallen van een charecter ($)einde patroon. Dit voorbeeld kan worden ingesteld zoals in deze afbeelding.



OID's ondersteund door ISE

Standaard biedt ISE opties om drie typen OID's te configureren om een bewerking uit te voeren op de poorten die worden geïdentificeerd door de waarde van de NAS-Port-ID.

1. Reecht

2. Poortsprong

3. Poortsluiting

reauthentiseren

Mogelijk wordt OID niet herecht ondersteund in standaard MIB's die door de meeste verkopers worden gebruikt. De informatie over deze OID kan van verkoper tot verkoper verschillen.

> Opmerking: Deze optie is beschikbaar voor mogelijke toekomstige verbetering als een apparaat een OID begint te ondersteunen om gebruikerssessies te beheren op basis van MAC-Address.

Poortbout

Poortbounce gebruikt een operationele OID van de haven die twee waarden heeft, de ene voor het afsluiten van de haven en de andere voor het afsluiten van de haven. Dit zijn standaard OID's die door de meeste verkopers worden gebruikt.

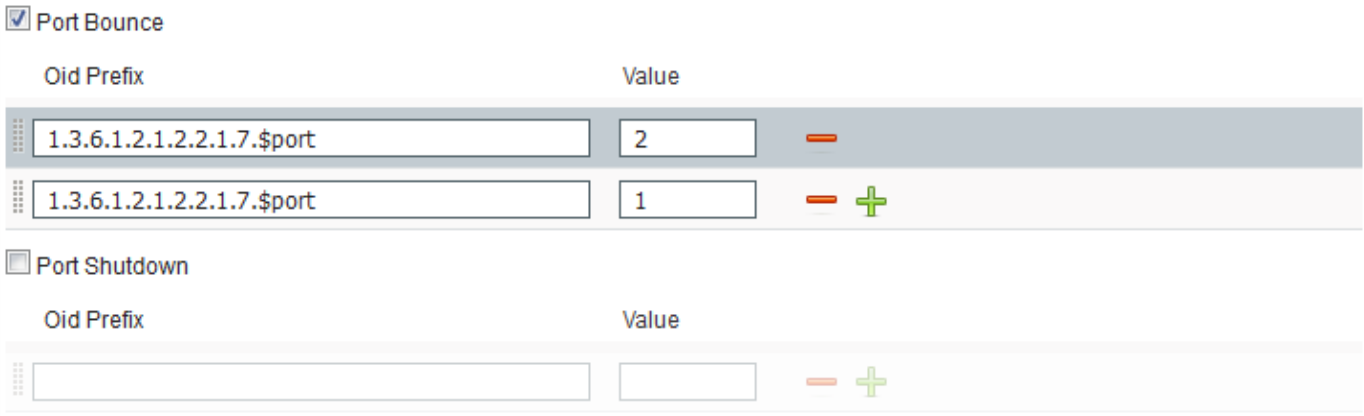
1.3.6.1.2.1.2.2.1.7.$port is de OID

Als de waarde op 2 is ingesteld, wordt de poort afgesloten en als de waarde op 1 is ingesteld,

wordt de poort niet gesloten.

Poortsluiting

Selecteer de gewenste bewerking die op die specifieke poort moet worden uitgevoerd zoals in de afbeelding.

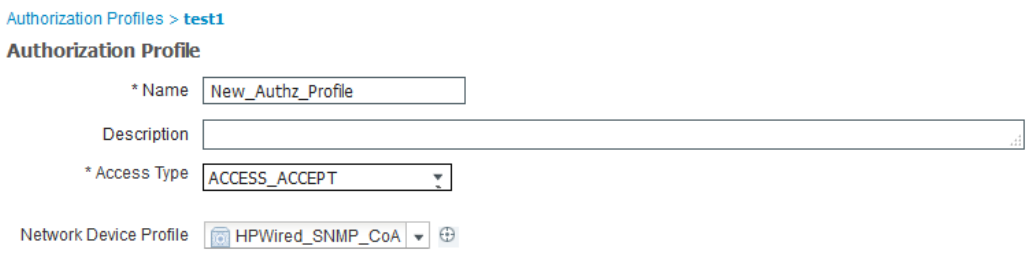


> **Voorzichtig:** De volgorde waarin de OID-waarden worden verzonden is erg belangrijk. Omdat, de volgorde waarin de OID waarden worden ingesteld de volgorde is waarin de bewerkingen op de poort worden uitgevoerd. Als ze in omgekeerde volgorde worden ingesteld, zeg 1 en dan 2, dan zou eerst een haven worden afgesloten en dan afsluiten, wat in feite de haven sluit.

Breng de wijzigingen in het apparaatprofiel in.

Dit profiel van het hulpmiddel kan worden gebruikt in elk vergunningprofiel dat in werking moet worden gesteld. Elke CoA-handeling die voor een eindpunt moet worden uitgevoerd, wordt als SNMP SetApplication naar de switch gestuurd met de geconfigureerde OIDs die op de poort worden ingesteld waarop het eindpunt is aangesloten. Hier is een voorbeeld om het NAD-profiel in het autorisatieprofiel te configureren.

Om een nieuw vergunningsbeleid te creëren of om het reeds bestaande te bewerken, navigeer aan **Beleid > Elementen van het Beleid > Resultaten > Vergunning > Profielen van de Vergunning** zoals in de afbeelding getoond.



> Opmerking: De switch moet met ISE als SNMP Server worden geconfigureerd en dezelfde community-string gebruiken die op ISE is geconfigureerd. De configuratie van de switch is niet binnen het bereik van dit document.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.