

Configurar o CoA SNMP no 2.1 do Identity Services Engine e acima

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar o ISE](#)

[Configurar ajustes SNMP do NAD](#)

[Configurar ajustes CoA SNMP do perfil do dispositivo de rede](#)

[OID apoiados pelo ISE](#)

[Reauthenticate](#)

[Mova o salto](#)

[Parada de porta](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento descreve a mudança da característica da autorização (CoA) com o uso do Simple Network Management Protocol (SNMP).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico do protocolo de SNMP
- Conhecimento prévio das expressões regulares
- Conhecimento prévio do motor do serviço da identidade de Cisco (ISE)
- 2.1 do motor do serviço da identidade.
- O SNMP apoiou o Switches

Componentes Utilizados

A informação neste documento é baseada na versão 2.1 ISE.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de

laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se sua rede está viva, assegure-se de que você compreenda o impacto potencial do comando any.

Informações de Apoio

Este é uns novos recursos introduzidos no 2.1 ISE. Esta característica felicita uns outros novos recursos no ISE a saber, na reorientação pelo ISE própria e não depende dos dispositivos de rede. Mesmo se o ISE envia uma reorientação URL diretamente ao cliente da extremidade, o valor-limite deve ser aplicado com política diferente após a autenticação no portal para o acesso de rede apropriado. Para que isto aconteça, nas versões anterior, o ISE enviou um CoA do RAIO. Alguns dos dispositivos de rede não compreendem um CoA do RAIO enviado pelo ISE. Desde que o SNMP é apoiado por quase todos os dispositivos do acesso de rede (NADs), o CoA que usa o SNMP se transformou uma opção viável em tal encenação. Um CoA SNMP é executado por um SetRequest SNMP enviado do ISE a um NAD a fim ajustar determinado objeto Identifoers (OID) que controlam o status operacional de uma porta.

Configurar o ISE

Há dois ajustes no ISE que precisam de ser configurados para que o CoA SNMP trabalhe.

1. Ajustes do servidor SNMP de um NAD.
2. Ajustes CoA SNMP de um perfil NAD.

A fim configurar ajustes do servidor SNMP no ISE para um NAD, navegue aos **recursos de rede de Administration** > > **aos dispositivos de rede**.

Configurar ajustes SNMP do NAD

Selecione um NAD. Uma caixa de seleção estará disponível debaixo dos ajustes da autenticação TACACS a fim editar os ajustes SNMP segundo as indicações da imagem.

Network Devices

* Name

Description

* IP Address: /



* Device Profile

Model Name

Software Version

* Network Device Group

Device Type

Location

- ▶ RADIUS Authentication Settings
- ▶ TACACS Authentication Settings
- ▶ SNMP Settings
- ▶ Advanced TrustSec Settings

Povoe os ajustes conforme a exigência. Um exemplo é mostrado na imagem.

▼ SNMP Settings

* SNMP Version

* SNMP RW Community

SNMP Username

Security Level

Auth Protocol

Auth Password

Privacy Protocol

Privacy Password

* Polling Interval seconds (Valid Range 600 to 86400 or zero)

Link Trap Query

MAC Trap Query

* Originating Policy Services Node

Configurar ajustes CoA SNMP do perfil do dispositivo de rede

A fim configurar o CoA que SNMP os ajustes para um dispositivo de rede perfilam, navegam aos perfis do dispositivo de rede de Resources> da rede de Administration>.

Selecione o perfil do dispositivo de rede para que o CoA SNMP precisa de ser configurado e expanda a **mudança da aba da autorização** segundo as indicações da imagem.

Note: Os ajustes SNMP de perfis de dispositivo da rede padrão não podem ser editados.

Network Device Profile List > **New Network Device Profile**

Network Device Profile

* Name

Description

Icon ⓘ

Vendor

Supported Protocols

RADIUS

TACACS+

TrustSec

RADIUS Dictionaries

Templates

[Expand All / Collapse All](#)

- ▶ Authentication/Authorization
- ▶ Permissions
- ▶ **Change of Authorization (CoA)**
- ▶ Redirect

Selecione o tipo CoA como o **SNMP** e edite o snmp timeout e experimente de novo ajustes. Estes ajustes podem ser ajustados conforme a exigência. Um exemplo é mostrado nesta imagem.

▼ **Change of Authorization (CoA)**

CoA by

* Timeout Interval seconds (1-500) ⓘ

* Retry Count (1-10) ⓘ

Agora, configurar o método de detecção da porta NAD por que o ISE conhecerá a porta para a qual os OID devem ser ajustados. A partir de agora, o único método disponível é recuperar essa informação do atributo RADIUS relevante da informação de contabilidade.

Os atributos RADIUS disponíveis atuais que dão tal informação são NAS-porta e nas-port-id. Qualquer deles pode ser escolhido baseado no atributo apoiado pelo NAD. A maioria dos NADs apoiam o nas-port-id. Os vendedores diferentes têm maneiras diferentes de representar as relações disponíveis no NAD. Uma maneira padrão extrair a informação não pôde ser possível. Daqui as expressões regulares são usadas no ISE ao costume as cordas a ser combinadas do valor de atributo do nas-port-id. Um exemplo é dado aqui a fim combinar as portas que são sob a forma de Gi0/x.

`^.*Gi0V(\d+).*`

Esta expressão significa essencialmente o teste padrão do começo (do ^) (. *) fósforo algum número de exemplos de algum carácter (“do fósforo Gi0)match 'Gi0 (V)'" (\ d+) fósforo uns ou vários do que um cita como exemplo de todo o fósforo do dígito (.) qualquer carácter (*) (. *) fósforo algum número de exemplos de algum teste padrão da extremidade do carácter (\$). Este exemplo pode ser configurado segundo as indicações desta imagem.

NAD Port Detection

Relevant RADIUS Attribute

Relevant RADIUS Attribute

Nas-Port

Nas-Port-Id

Regular Expression

`^.*Gi0V(\d+).*$`

OID apoiados pelo ISE

À revelia, o ISE fornece opções a fim configurar três tipos de OID a fim executar uma operação nas portas identificadas pelo valor de atributo do nas-port-id.

1. Reauthenticate
2. Mova o salto
3. Parada de porta

Reauthenticate

Reauthenticate o OID não pôde ser apoiado nos MIB padrão usados pela maioria dos vendedores. A informação deste OID pôde variar do vendedor ao vendedor.

Note: Esta opção está fornecida para o aprimoramento futuro possível se qualquer dispositivo começa apoiar um OID para controlar as sessões do usuário baseadas no endereço MAC.

Salto da porta

O salto da porta usa uma porta OID operacional que tenha dois valores, um fechando a porta para baixo e outro para Unshutting a porta. Estes são o padrão OID usado pela maioria dos vendedores.

1.3.6.1.2.1.2.2.1.7.\$port é o OID

Se o valor é ajustado a 2, a porta é parada programada e se o valor é ajustado a 1, a porta é unshut.

Parada de porta

Selecione a operação desejada que tem que ser executada nessa porta específica segundo as indicações da imagem.

Port Bounce

Oid Prefix	Value	
1.3.6.1.2.1.2.2.1.7.\$port	2	-
1.3.6.1.2.1.2.2.1.7.\$port	1	- +

Port Shutdown

Oid Prefix	Value	
		- +

Caution: A ordem em que o OID avalia é enviada é muito importante. Porque, a ordem em que o OID avalia é ajustada é a ordem em que as operações são executadas na porta. Se são ajustados em uma ordem reversa, diga 1 e então 2, uma porta seria unshut primeiramente e então a parada programada que essencialmente está fechando a porta.

Submeta as mudanças ao perfil de dispositivo.

Este perfil de dispositivo pode ser usado em todo o perfil da autorização a ser tomado na influência. Toda a operação CoA que tiver que ser executada para um valor-limite será enviada como um SetRequest SNMP ao interruptor com os OID configurados a ser ajustados na porta em que o valor-limite é conectado. Está aqui um exemplo a fim configurar o perfil NAD no perfil da autorização.

Para criar uma política nova da autorização ou editar esse que já existe, navegue à **política > aos elementos da política > aos resultados > à autorização > aos perfis da autorização** segundo as indicações da imagem.

Authorization Profiles > test1

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Note: O interruptor deve ser configurado com o ISE como o servidor SNMP e deve usar o mesmo string de comunidade que é configurado no ISE. A configuração do interruptor é fora do espaço deste documento.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.