

Configurazione di SNMP CoA in Identity Services Engine 2.1 e versioni successive

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurare ISE](#)

[Configurazione delle impostazioni SNMP di NAD](#)

[Configurazione delle impostazioni CoA SNMP del profilo del dispositivo di rete](#)

[OID supportati da ISE](#)

[Riautentica](#)

[Rimbalzo porta](#)

[Port-shutdown](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

Questo documento descrive la funzione Cambia autorizzazione (CoA) con l'uso del protocollo SNMP (Simple Network Management Protocol).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base del protocollo SNMP
- Conoscenza delle espressioni regolari
- Conoscenza precedente di Cisco Identity Service Engine (ISE)
- Identity Service Engine 2.1.1
- Switch supportati da SNMP

Componenti usati

Il riferimento delle informazioni contenute in questo documento è ISE versione 2.1.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Questa nuova funzionalità, introdotta ad ISE 2.1, completa un'altra nuova funzionalità di ISE, il reindirizzamento da parte di ISE e non dipende dai dispositivi di rete. Anche se ISE invia un URL di reindirizzamento direttamente al client finale, l'endpoint deve essere applicato con criteri diversi dopo l'autenticazione nel portale per consentire l'accesso alla rete appropriato. Nelle versioni precedenti, ISE ha inviato una CoA RADIUS. Alcuni dispositivi di rete non sono in grado di interpretare una richiesta RADIUS CoA inviata da ISE. Poiché il protocollo SNMP è supportato da quasi tutti i dispositivi di accesso alla rete (NAD), in uno scenario di questo tipo la CoA che utilizza il protocollo SNMP è diventata un'opzione praticabile. Una CoA SNMP viene eseguita da una SetRequest SNMP inviata da ISE a un NAD per impostare determinati Object Identifier (OID) che gestiscono lo stato operativo di una porta.

Configurare ISE

Per il corretto funzionamento del protocollo SNMP CoA, è necessario configurare due impostazioni su ISE.

1. Impostazioni del server SNMP di un NAD.
2. Impostazioni di SNMP CoA di un profilo NAD.

Per configurare le impostazioni del server SNMP su ISE per un server NAD, selezionare **Amministrazione > Risorse di rete > Dispositivi di rete**.

Configurazione delle impostazioni SNMP di NAD

Selezionare un NAD. Sotto le impostazioni di autenticazione TACACS sarà disponibile una casella di controllo per modificare le impostazioni SNMP, come mostrato nell'immagine.

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

Popolare le impostazioni secondo il requisito. Nell'immagine viene visualizzato un esempio.

▼ 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

Configurazione delle impostazioni CoA SNMP del profilo del dispositivo di rete

Per configurare le impostazioni di CoA SNMP per un profilo di dispositivo di rete, selezionare **Amministrazione > Risorse di rete > Profili dispositivi di rete**.

Selezionare il profilo del dispositivo di rete per il quale configurare SNMP CoA ed espandere la scheda **Modifica di autorizzazione** come mostrato nell'immagine.

Nota: Non è possibile modificare le impostazioni SNMP dei profili dei dispositivi di rete predefiniti.

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

Submit Cancel

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

Selezionare il tipo CoA come **SNMP** e modificare le impostazioni SNMP Timeout and Retry. Queste impostazioni possono essere configurate in base ai requisiti. L'immagine mostra un esempio.

▼ Change of Authorization (CoA)

CoA by

* Timeout Interval seconds (1-500)

* Retry Count (1-10)

A questo punto, configurare il metodo di rilevamento della porta AND in base al quale ISE potrebbe conoscere la porta per la quale impostare gli OID. L'unico metodo attualmente disponibile consiste nel recuperare tali informazioni dall'attributo RADIUS pertinente dalle informazioni di accounting.

Gli attributi RADIUS attualmente disponibili che forniscono tali informazioni sono NAS-Port e NAS-Port-Id. È possibile scegliere uno di questi attributi in base all'attributo supportato da NAD. La maggior parte dei NAD supporta NAS-Port-Id. I diversi fornitori possono rappresentare in modi diversi le interfacce disponibili nel NAD. Un metodo standard per estrarre le informazioni potrebbe non essere possibile. Pertanto, le espressioni regolari vengono utilizzate in ISE per personalizzare le stringhe da associare dal valore dell'attributo NAS-Port-Id. Di seguito viene riportato un esempio per individuare le porte nella forma Gi0/x.

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

L'espressione indica essenzialmente (^)start pattern (.)match any number of instance of any charecter (Gi0)match 'Gi0' (V)match '/' (\d+)match one or more once of any digit (.)match any charecter (*) (.*).match any number of instance of any charecter (\$)end pattern. Questo esempio può essere configurato come mostrato nell'immagine.

NAD Port Detection

Relevant RADIUS Attribute

Relevant RADIUS Attribute

Nas-Port

Nas-Port-Id

Regular Expression

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

OID supportati da ISE

Per impostazione predefinita, ISE offre opzioni che consentono di configurare tre tipi di OID per eseguire un'operazione sulle porte identificate dal valore dell'attributo NAS-Port-Id.

1. Riautentica
2. Rimbalzo della porta
3. Arresto della porta

Riautentica

OID di riautenticazione potrebbe non essere supportato nei MIB standard utilizzati dalla maggior parte dei fornitori. Le informazioni di questo OID potrebbero variare da fornitore a fornitore.

Nota: Questa opzione viene fornita per un possibile miglioramento futuro se un dispositivo inizia a supportare un OID per gestire le sessioni utente in base all'indirizzo MAC.

Rimbalzo porta

Port-bounce utilizza un OID operativo di porta con due valori, uno per l'arresto della porta e l'altro per l'annullamento dell'arresto della porta. Si tratta di OID standard utilizzati dalla maggior parte dei fornitori.

1.3.6.1.2.1.2.2.1.7.\$port è l'OID

Se il valore è impostato su 2, la porta viene chiusa e se il valore è impostato su 1, la porta viene chiusa.

Port-shutdown

Selezionare l'operazione desiderata da eseguire sulla porta specifica, come mostrato nell'immagine.

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	
		- +

Attenzione: L'ordine in cui vengono inviati i valori OID è molto importante. Infatti, l'ordine in cui vengono impostati i valori OID è l'ordine in cui vengono eseguite le operazioni sulla porta. Se sono impostate in ordine inverso, ad esempio 1 e 2, una porta verrà prima disattivata e quindi chiusa e la porta verrà chiusa.

Inviare le modifiche al profilo del dispositivo.

Questo profilo di dispositivo può essere utilizzato in qualsiasi profilo di autorizzazione. Qualsiasi operazione CoA da eseguire su un endpoint verrà inviata come SNMP SetRequest allo switch con gli OID configurati da impostare sulla porta a cui è connesso l'endpoint. Di seguito è riportato un esempio per configurare il profilo NAD in Profilo di autorizzazione.

Per creare un nuovo criterio di autorizzazione o modificare quello esistente, selezionare **Criterio > Elementi criterio > Risultati > Autorizzazione > Profili di autorizzazione**, come mostrato nell'immagine.

Authorization Profiles > test1

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Nota: Lo switch deve essere configurato con ISE come server SNMP e deve utilizzare la stessa stringa della community configurata su ISE. La configurazione dello switch non rientra nell'ambito di questo documento.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.