

の以上の SNMP CoA を Identity Services Engine 2.1 設定して下さい

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[ISE の設定](#)

[NAD の SNMP 設定を設定して下さい](#)

[ネットワークデバイス プロファイルの SNMP CoA 設定を設定して下さい](#)

[ISE によってサポートされる OID](#)

[再認証して下さい](#)

[ポート バウンス](#)

[ポート シャットダウン](#)

[確認](#)

[トラブルシューティング](#)

概要

この資料は簡易ネットワーク管理プロトコル (SNMP) の使用を用いる許可 (CoA) 機能の変更を説明したものです。

前提条件

要件

次の項目に関する知識が推奨されます。

- SNMP プロトコルの基本的な知識
- 正規表現の前ナレッジ
- Cisco 識別 サービス エンジン (ISE) の前ナレッジ
- 識別 サービス エンジン 2.1。
- SNMP はスイッチをサポートしました

使用するコンポーネント

この文書に記載されている情報は ISE バージョン 2.1 に基づいています。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメン

トで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

これは ISE 2.1 で導入される新しい機能です。この機能はすなわち ISE によって ISE、リダイレクション自体の別の新しい機能をほめ、ネットワークデバイスに左右されません。ISE が端クライアントにリダイレクション URL を直接送信しても、エンドポイントは適切なネットワークアクセスのためのポータル認証の後で別のポリシーと適用する必要があります。、前のバージョンで起こるこれのために ISE は RADIUS CoA を送信しました。いくつかのネットワークデバイスは ISE によって送信される RADIUS CoA を理解しません。SNMP がほとんどすべてのネットワークアクセスデバイス（NADs）によってサポートされるので、SNMP をなったそのような場合には可能なオプションに使用する CoA。SNMP CoA はある特定のオブジェクト Identifoers（OID）を設定するために ISE から NAD に送信される SNMP SetRequest によって実行されたポートの動作状態を管理する。

ISE の設定

SNMP CoA がはたらくことができるように行われる必要がある ISE に 2 つの設定があります。

1. NAD の SNMP サーバ設定。
2. NAD プロファイルの SNMP CoA 設定。

NAD のための ISE の SNMP サーバ設定を、ナビゲート **Administration > ネットワークリソース > ネットワークデバイス** に行うため。

NAD の SNMP 設定を設定して下さい

NAD を選択して下さい。チェックボックスはイメージに示すように SNMP 設定を編集して TACACS 認証設定の下に利用できます。

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

要件によって設定を読み込んで下さい。例はイメージで示されています。

▼ 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

ネットワークデバイス プロファイルの SNMP CoA 設定を設定して下さい

設定がネットワークデバイスのためにプロファイルしたり SNMP CoA を設定するために、**Administration> ネットワーク Resources> ネットワークデバイス プロファイル**にナビゲートして下さい。

SNMP CoA が設定される必要がある選択し、イメージに示すように許可タブの変更を拡張して下

さいネットワークデバイス プロファイルを。

注: デフォルトネットワーク デバイス プロファイルの SNMP 設定は編集することができません。

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

CoA 型を **SNMP** として選択し、SNMP タイムアウトを編集し、設定を再試行して下さい。これらの設定は要件によって行うことができます。例はこのイメージで示されています。

▼ Change of Authorization (CoA)

CoA by

* Timeout Interval seconds (1-500) ⓘ

* Retry Count (1-10) ⓘ

この場合、ISE が OID が設定する必要があるポートを知っている NAD ポート検出方法を設定して下さい。現在、唯一の利用可能な方式はアカウントリング 情報からの関連した RADIUS特性からその情報を検索することです。

そのような情報を与える現在の利用可能な RADIUS特性は Nas-port および Nas-port-id です。それらのどれでも NAD によってサポートされる属性に基づいていました選択することができます。NADs のほとんどは Nas-port-id をサポートします。異なるベンダーに NAD で利用可能なインターフェイスを表すさまざまな方法があります。情報を得る標準的な方法は可能性のあるではないかもしれません。それ故に正規表現はカスタムへの ISE で Nas-port-id 属性値から一致するべきストリング使用されます。例は Gi0/x の形にあるポートを一致するためにここに与えられます。

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

この式は本質的に (^) 開始パターンを意味します (.*) 文字の例の数一致する (Gi0)match 'Gi0 () Vあらゆるディジットの 1 例より一致/」 (\d+) 1つ以上を (。) 一致する文字を一致する (*) (.*) 文字 (\$) 端パターンの例の数一致する。この例はこのイメージに示すように設定することができます。

NAD Port Detection

Relevant RADIUS Attribute

Relevant RADIUS Attribute

Nas-Port

Nas-Port-Id

Regular Expression

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

ISE によってサポートされる OID

デフォルトで、ISE は Nas-port-id 属性値によって識別されるポートのオペレーションを行うために OID の 3 つの型を設定するためにオプションを提供します。

1. 再認証して下さい
2. ポート バウンス
3. ポート シャットダウン

再認証して下さい

OID をベンダーのほとんどが使用する標準MIB でサポートされないかもしれませんが再認証して下さい。この OID の情報はベンダーからベンダーに異なるかもしれません。

注: このオプションは可能性のある未来の機能拡張に MAC アドレスに基づいてユーザセッションを管理するためにどのデバイスでも OID をサポートし始める場合提供されます。

ポート バウンス

ポート バウンスはポートを停止するために 2 つの値があるポート操作上 OID を、1 つおよび Unshutting のための他の 1 ポート使用します。これらはベンダーのほとんどが使用する標準 OID です。

1.3.6.1.2.1.2.2.1.7.\$port は OID です

値が 2 に設定される場合、ポートは値が 1 に設定されれば、ポートです unshut シャットダウンされ。

ポート シャットダウン

イメージに示すようにその特定のポートで実行されたならない望ましい オペレーションを選択して下さい。

Port Bounce

Oid Prefix	Value	
<input type="text" value="1.3.6.1.2.1.2.2.1.7.\$port"/>	<input type="text" value="2"/>	—
<input type="text" value="1.3.6.1.2.1.2.2.1.7.\$port"/>	<input type="text" value="1"/>	— +

Port Shutdown

Oid Prefix	Value	
<input type="text"/>	<input type="text"/>	— +

注意：OID が評価する順序はです非常に重要送信 されます。、OID が評価する順序が一定であるオペレーションがポートで実行された順序であるので。次にそれらが逆順で設定される場合、1つおよび2つを言って下さい、ポートは本質的にポートをシャットダウンしている最初に unshut、次にシャットダウンします。

デバイス プロファイルへの変更を入れて下さい。

あらゆる許可プロファイルでこのデバイス プロファイルが影響に運ばれるのに使用することができます。エンドポイントのために実行されたならないエンドポイントが接続されるポートで設定されたOIDが設定されているとどのCoAオペレーションでもスイッチにSNMP SetRequestとして送信されます。例は許可プロファイルのNADプロファイルを設定するためにここにあります。

ポリシー > **ポリシー要素**に既に、ナビゲートがイメージに示すように存在して >> 許可 > 許可プロファイル起因すること新しい承認ポリシーを作成するか、または1つを編集するため。

Authorization Profiles > test1

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

注: スイッチはSNMPサーバでISEで設定する必要があり、ISEで設定される同じコミュニティストリングを使用する必要があります。スイッチの設定はこの資料の範囲からあります。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。