在身份服務引擎2.1及更高版本中配置SNMP CoA

目錄

簡介

本檔案介紹使用簡單網路管理通訊協定(SNMP)的授權變更(CoA)功能。

必要條件

需求

思科建議您瞭解以下主題：

- SNMP協定基礎知識
- 正規表示式的先驗知識
- 預先瞭解思科身份服務引擎(ISE)
- 身分識別服務引擎2.1.
- SNMP支援的交換器

採用元件

本文檔中的資訊基於ISE版本2.1。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

這是ISE 2.1中引入的一項新功能。該功能補充了ISE中的另一項新功能，即由ISE本身重定向而不依賴於網路裝置。即使ISE將重定向URL直接傳送到終端客戶端，終端在門戶中的身份驗證之後應用不同的策略進行適當的網路訪問。為此，在以前的版本中，ISE傳送了RADIUS CoA。某些網路裝置無法識別ISE傳送的RADIUS CoA。由於幾乎所有的網路存取裝置(NAD)都支援SNMP，因此使用SNMP的CoA在此種情況下成為可行的選項。SNMP CoA由從ISE傳送到NAD的SNMP SetRequest執行，以設定管理埠運行狀態的特定對象識別符號(OID)。

配置ISE

ISE上有兩個設定需要配置才能使SNMP CoA正常工作。

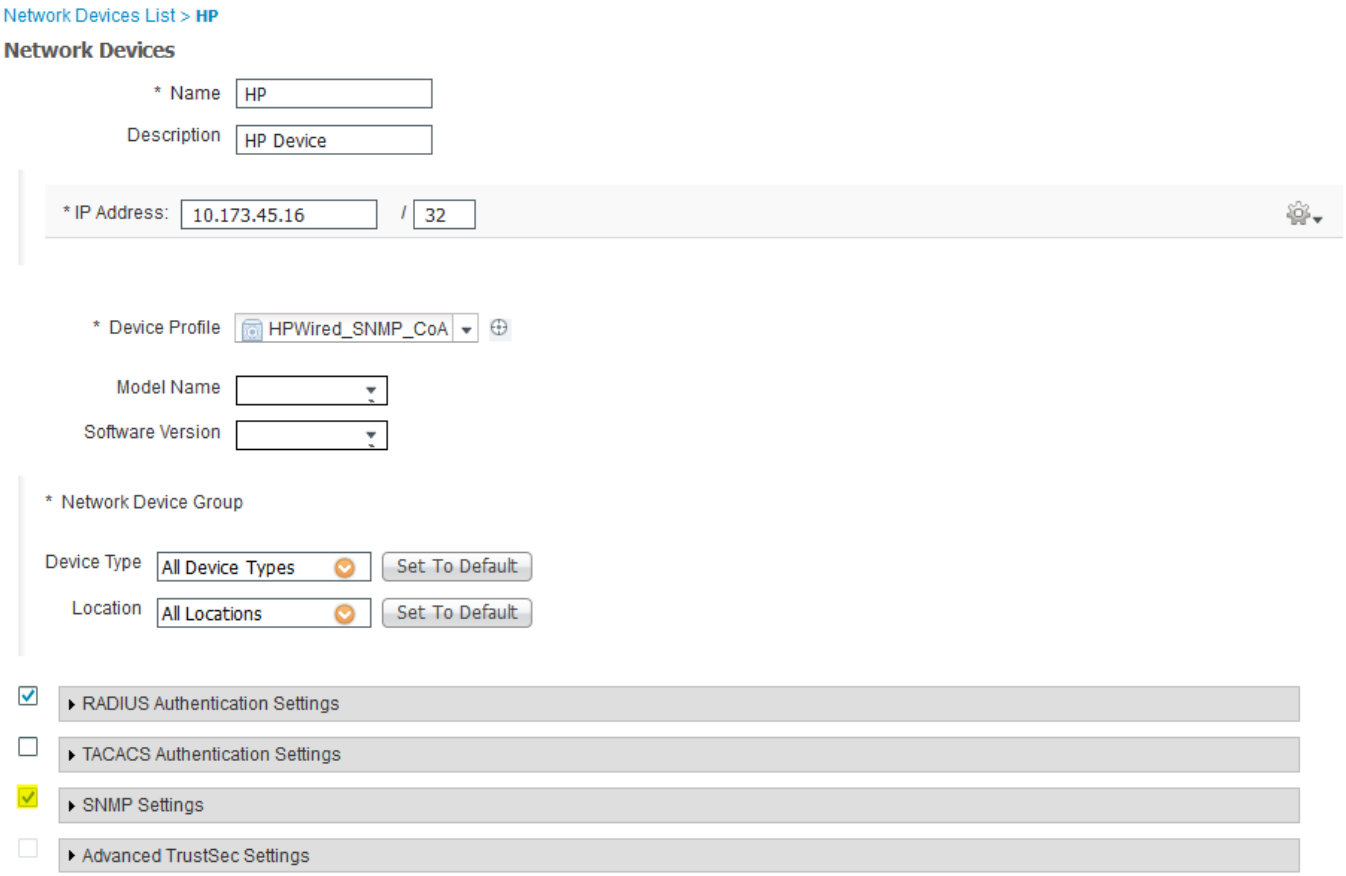
1. NAD的SNMP伺服器設定。

2. NAD配置檔案的SNMP CoA設定。

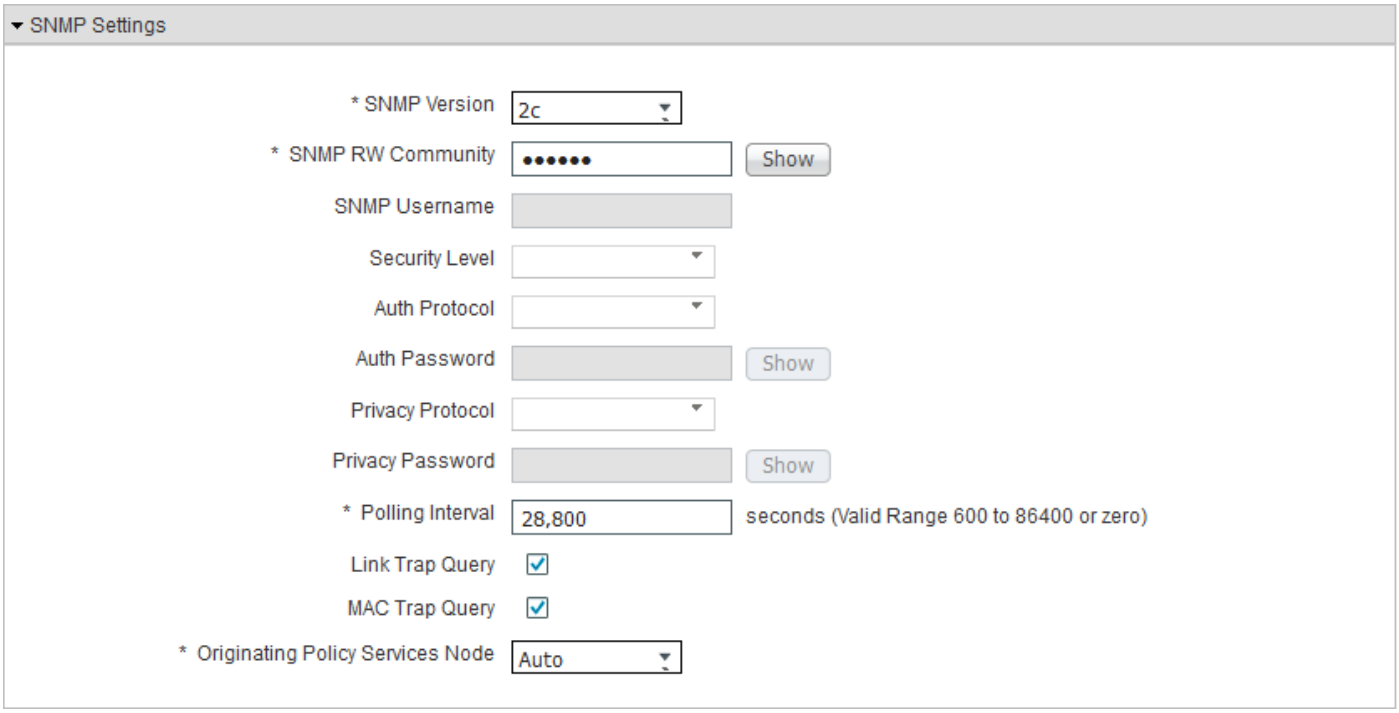
要在ISE上為NAD配置SNMP伺服器設定，請導航到**管理>網路資源>網路裝置。**

配置NAD的SNMP設定

選擇NAD。TACACS Authentication Settings下方將顯示一個覈取方塊，以便編輯SNMP設定，如下圖所示。



根據要求填充設定。圖中顯示了一個範例。

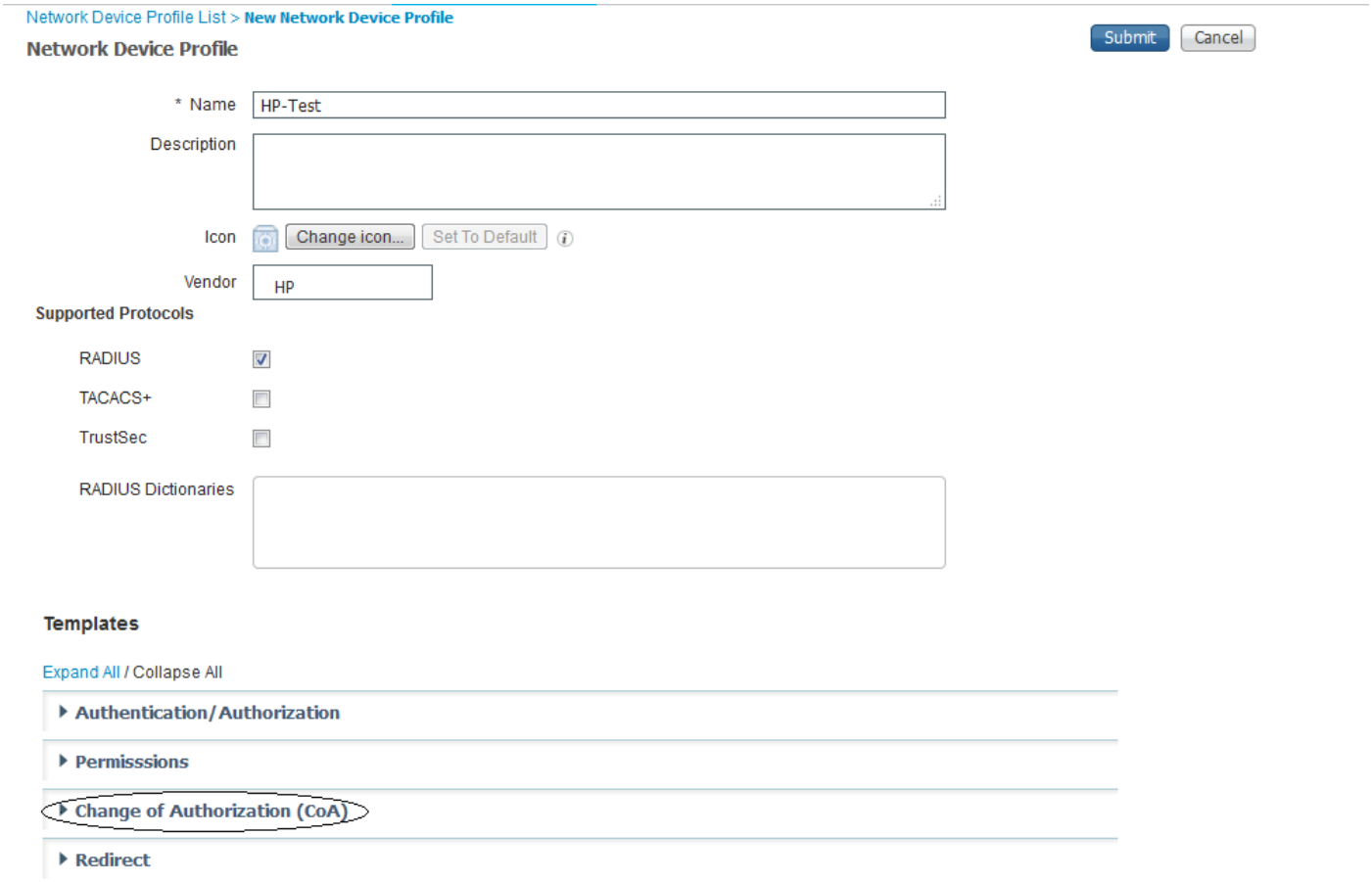


配置網路裝置配置檔案的SNMP CoA設定

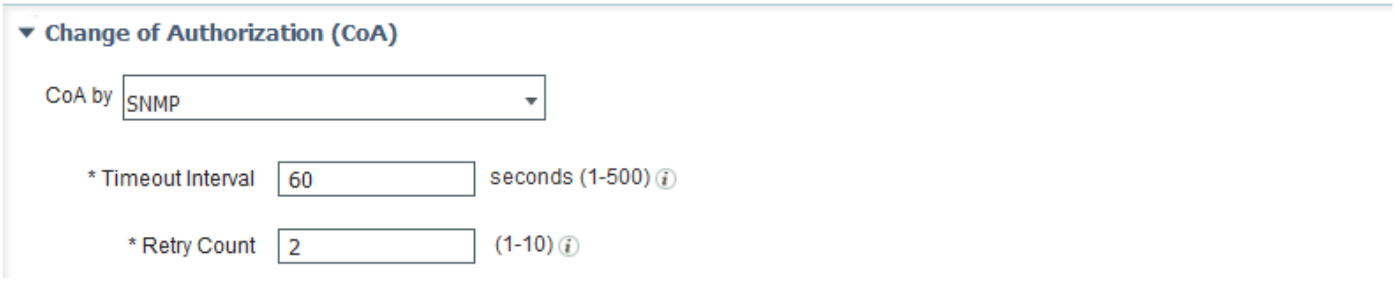
要為網路裝置配置檔案配置SNMP CoA設定，請導航至**管理>網路資源>網路裝置配置檔案。**

選擇需要為其配置SNMP CoA的網路裝置配置檔案，然後展開**Change of Authorization**頁籤，如下圖所示。

附註：無法編輯預設網路裝置配置檔案的SNMP設定。



選擇CoA型別為**SNMP**，並編輯SNMP超時和重試設定。可以根據需要設定這些設定。下圖顯示範例。

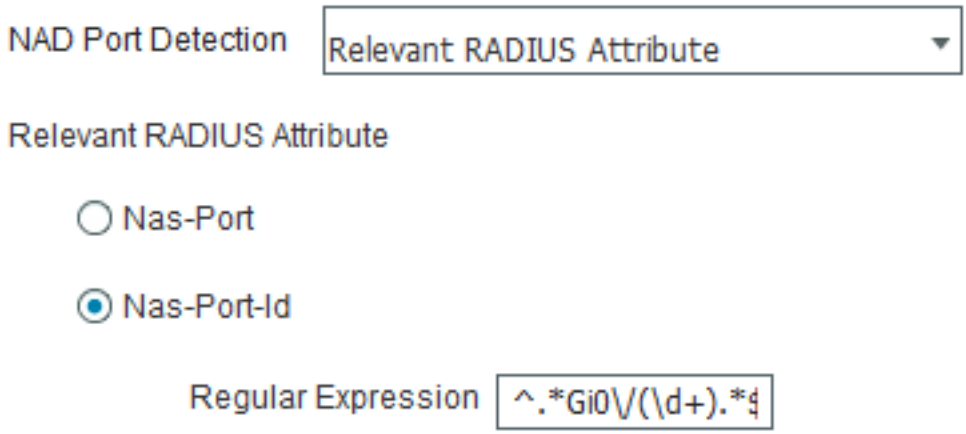


現在，配置NAD埠檢測方法，ISE通過該方法可以知道應為其設定OID的埠。目前，唯一可用的方法是從記帳資訊中的相關RADIUS屬性檢索該資訊。

提供此類資訊的當前可用RADIUS屬性是NAS-Port和NAS-Port-Id。可以根據NAD支援的屬性選擇其中的任意一個。大多數NAD都支援NAS埠ID。不同的供應商有不同的方式來表示NAD上的可用介面。提取資訊的標準方法可能無法實現。因此，在ISE中使用正規表示式來自定義要從NAS-Port-Id屬性值匹配的字串。這裡提供一個範例以比對以Gi0/x形式出現的連線埠。

^.*Gi0\/(\d+)。*$

此表達式實質上表示(^)start pattern(.*)匹配任意字元(Gi0)的任何數目的例項匹配「Gi0」(\/)match '/'(\d+)匹配任意數字(.)的一個或多個例項匹配任意字元(*)(.*)匹配任意字元($)end模式的任意數目的例項。此範例可如下圖所示。



ISE支援的OID

預設情況下，ISE提供選項來配置三種OID，以便對NAS-Port-Id屬性值標識的埠執行操作。

1.重新驗證

2.埠退回

3.埠關閉

重新驗證

大多數供應商使用的標準MIB可能不支援重新驗證OID。此OID的資訊可能因供應商而異。

> **附註**：如果任何裝置開始支援OID以基於MAC地址管理使用者會話，則提供此選項可增強未來的功能。

埠退回

埠反彈使用埠操作OID，該OID有兩個值，一個用於關閉埠，另一個用於取消關閉埠。這些是大多數供應商使用的標準OID。

1.3.6.1.2.1.2.2.1.7.$port是OID

如果值設定為2，則埠關閉；如果值設定為1，則埠不關閉。

連線埠關閉

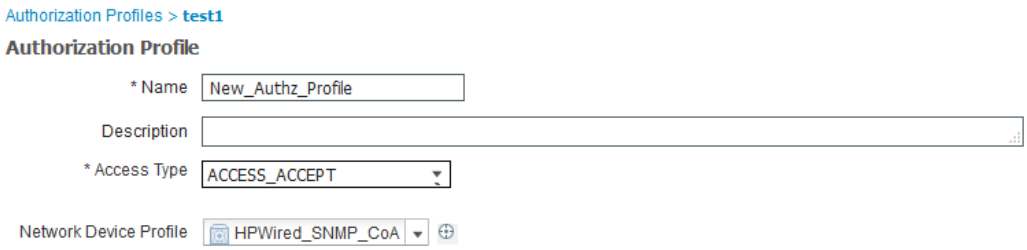
選擇必須在該特定埠上執行的所需操作，如下圖所示。

注意：OID值的傳送順序非常重要。因為，設定OID值的順序是在埠上執行操作的順序。如果埠按相反的順序設定，例如1和2，則埠將首先被取消關閉，然後關閉，這實際上就是關閉埠。

提交對裝置配置檔案的更改。

此裝置配置檔案可用於要生效的任何授權配置檔案。對終端必須執行的任何CoA操作都將作為SNMP SetRequest傳送到交換機，並且配置的OID將在終端連線的埠上設定。以下示例用於在授權配置檔案中配置NAD配置檔案。

若要建立新的授權策略或編輯已存在的授權策略，請導航至**Policy > Policy Elements > Results > Authorization > Authorization Profiles**，如下圖所示。



附註：交換機必須使用ISE配置為SNMP伺服器，並且應該使用在ISE上配置的相同社群字串。交換器的設定超出本檔案的範圍。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。