在身份服务引擎2.1及更高版本中配置SNMP CoA

目录

简介

本文档介绍使用简单网络管理协议(SNMP)的授权更改(CoA)功能。

先决条件

要求

Cisco 建议您了解以下主题：

- SNMP协议的基本知识
- 正则表达式的先验知识
- 思科身份服务引擎(ISE)的先验知识
- 身份服务引擎2.1。
- SNMP支持的交换机

使用的组件

本文档中的信息基于ISE版本2.1。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

这是ISE 2.1中引入的一项新功能。此功能补充了ISE中的另一个新功能，即ISE自身重定向，不依赖于网络设备。即使ISE直接向终端客户端发送重定向URL，在门户中进行身份验证后应使用不同策略应用终端以进行适当的网络访问。为此，在以前版本中，ISE发送了RADIUS CoA。某些网络设备不理解ISE发送的RADIUS CoA。由于SNMP几乎受所有网络接入设备(NAD)支持，因此使用SNMP的CoA在这种情况下成为可行选项。SNMP CoA由从ISE发送到NAD的SNMP SetRequest执行，以设置管理端口操作状态的某些对象标识符(OID)。

配置ISE

ISE上有两个设置需要配置才能使SNMP CoA工作。

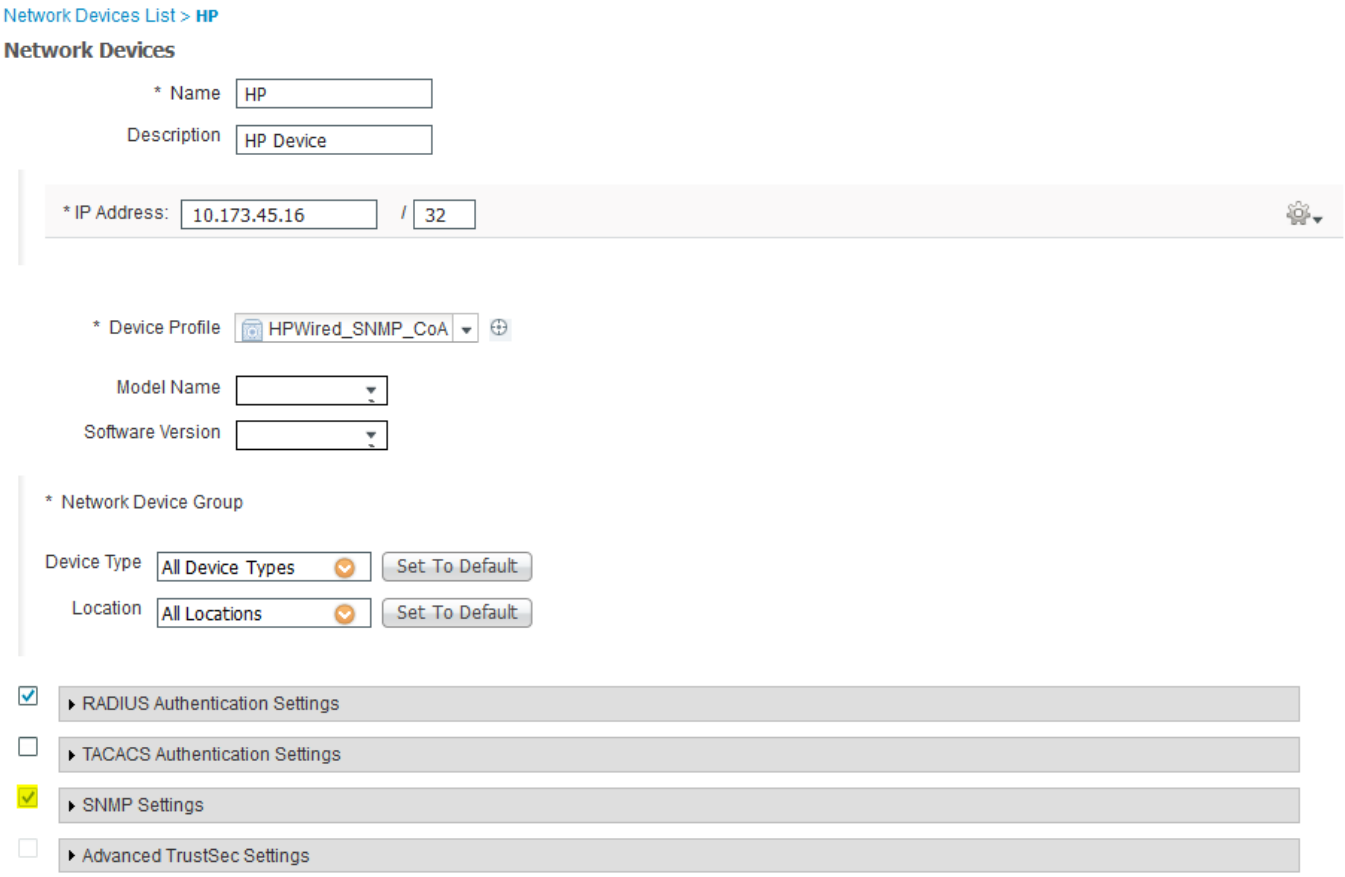
1. NAD的SNMP服务器设置。

2. NAD配置文件的SNMP CoA设置。

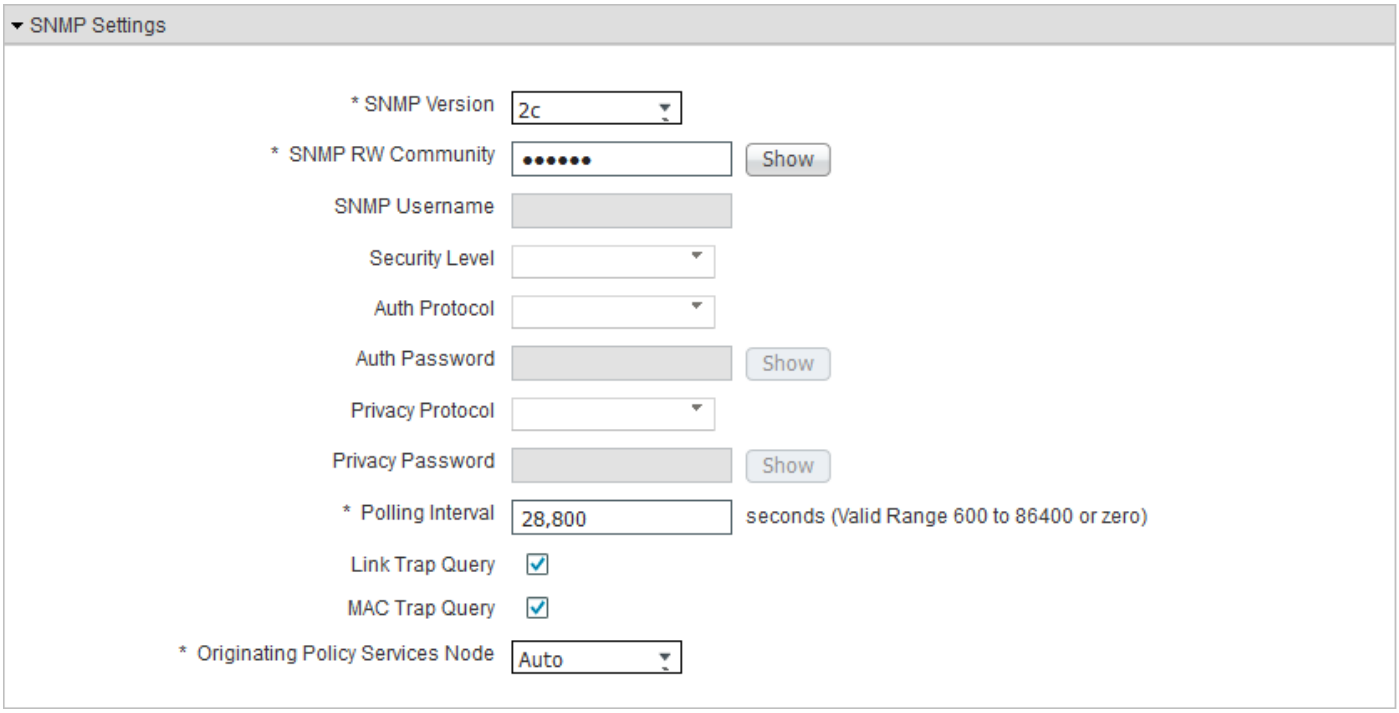
要在ISE上为NAD配置SNMP服务器设置，请导航**到Administration> Network Resources > Network Devices。**

配置NAD的SNMP设置

选择NAD。TACACS Authentication Settings下方将显示一个复选框，以便编辑SNMP Settings，如图所示。



根据要求填写设置。示例如图所示。

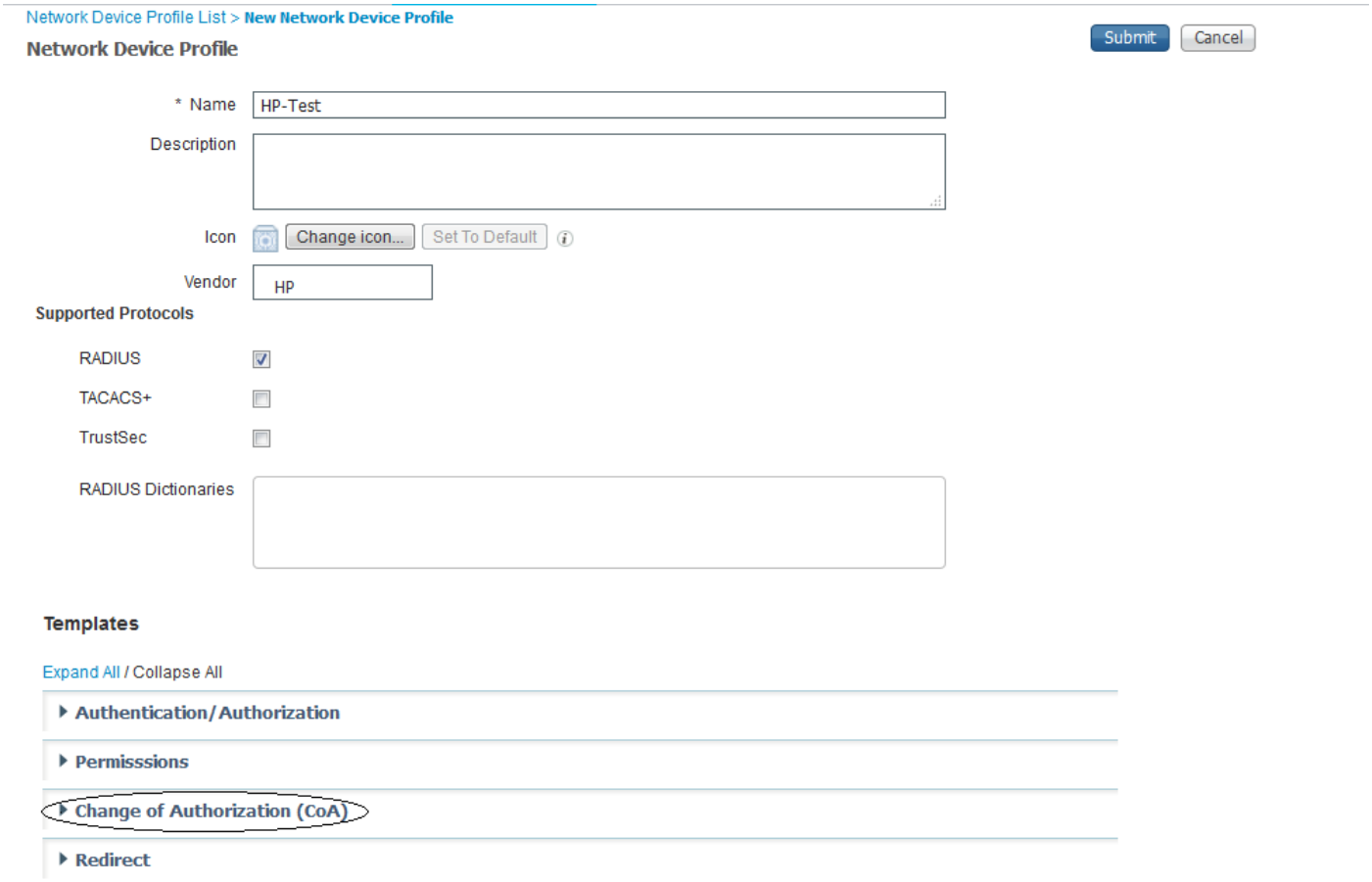


配置网络设备配置文件的SNMP CoA设置

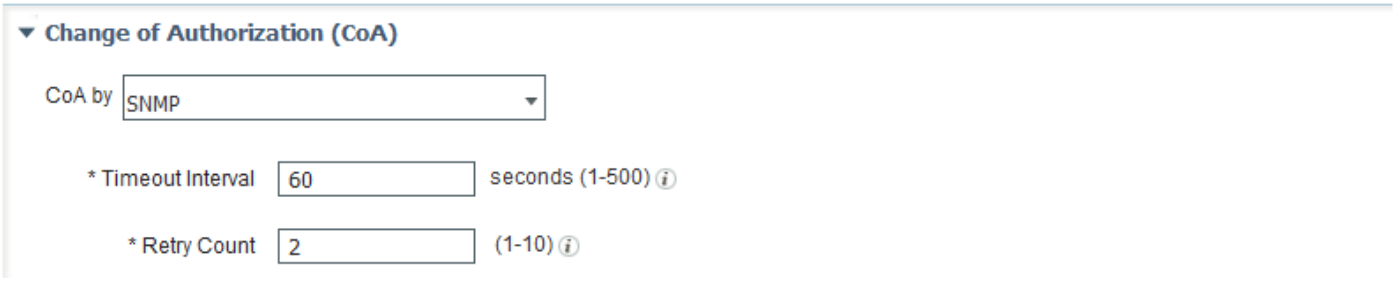
要配置网络设备配置文件的SNMP CoA设置，请导航至**Administration> Network Resources> Network Device Profiles**。

选择需要为其配置SNMP CoA的网络设备配置文件，然后展开“授权**更改”(Change of Authorization)**选项卡，如图所示。

注意：无法编辑默认网络设备配置文件的SNMP设置。



选择CoA类型作为**SNMP**并编辑SNMP超时和重试设置。这些设置可根据要求设置。本图显示了一个示例。

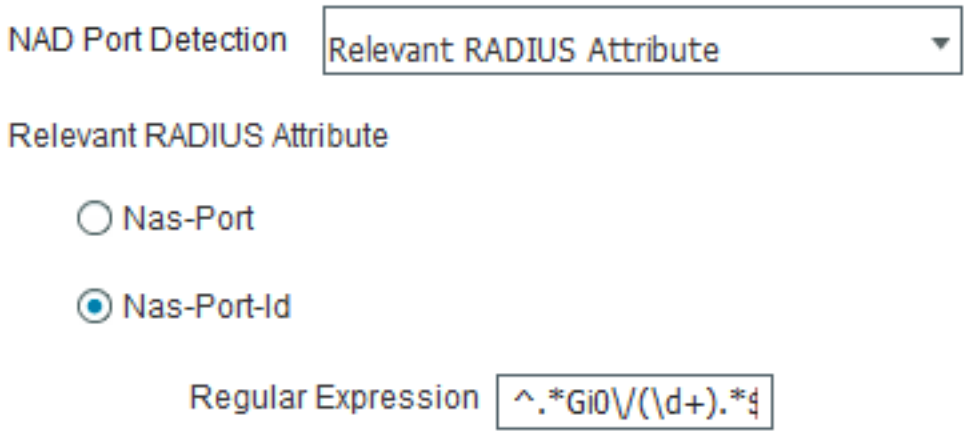


现在，配置NAD端口检测方法，ISE将通过此方法了解应为其设置OID的端口。目前，唯一可用的方法是从记帐信息中的相关RADIUS属性检索该信息。

提供此类信息的当前可用RADIUS属性是NAS端口和NAS端口ID。可以根据NAD支持的属性选择其中任何一个。大多数NAD都支持NAS端口ID。不同供应商有不同的方法来表示NAD上可用的接口。提取信息的标准方法可能不可能。因此，ISE中使用正则表达式来自定义要从NAS端口ID属性值匹配的字符串。此处提供了一个示例，以匹配Gi0/x形式的端口。

^.*Gi0\/(\d+)。*$

此表达式实质上表示(^)开始模式(.*)匹配任意字符(Gi0)匹配“Gi0”(\/)match“/”(\d+)匹配任意数字(.)匹配任意字符(*)(.*)匹配任意字符($)结束模式任意数目的实例。此示例可以如下图所示进行配置。



ISE支持的OID

默认情况下，ISE提供选项以配置三种类型的OID，以便对由NAS端口ID属性值标识的端口执行操作。

1.重新验证身份

2.端口退回

3.端口关闭

重新验证

大多数供应商使用的标准MIB可能不支持重新验证OID。此OID的信息可能因供应商而异。

> **注意：**如果任何设备开始支持OID，以根据MAC地址管理用户会话，则此选项可用于将来可能的增强。

端口退回

端口退回使用端口运行OID，它有两个值，一个用于关闭端口，另一个用于取消关闭端口。这些是大多数供应商使用的标准OID。

1.3.6.1.2.1.2.1.7.$port是OID

如果值设置为2，则端口将关闭；如果值设置为1，则端口将不关闭。

端口关闭

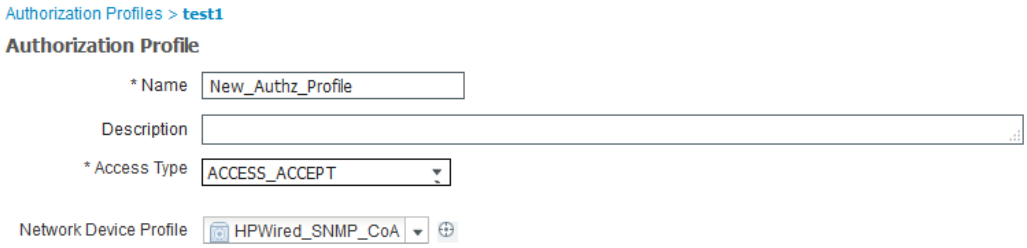
选择必须在该特定端口上执行的所需操作，如图所示。

警告：OID值的发送顺序非常重要。因为，OID值的设置顺序是在端口上执行操作的顺序。如果以相反的顺序（例如1和2）设置，则端口将首先取消关闭，然后关闭，这实际上是关闭端口。

将更改提交到设备配置文件。

此设备配置文件可用于任何要生效的授权配置文件。必须为终端执行的任何CoA操作都将作为SNMP SetRequest发送到交换机，并在终端所连接的端口上设置已配置的OID。以下是在授权配置文件中配置NAD配置文件的示例。

要创建新的授权策略或编辑已存在的授权策略，请导航至**Policy > Policy Elements > Results > Authorization > Authorization Profiles，如**图所示。



注意：交换机必须配置ISE作为SNMP服务器，并且应使用ISE上配置的同一社区字符串。交换机配置不在本文档的范围内。

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。