在Arista交换机上配置基于RADIUS的管理员登录

目录

简介

本文档介绍如何配置思科身份服务引擎(ISE)以使用RADIUS对Arista交换机上的管理员登录进行身份验证。

先决条件

要求

在继续操作之前，请确保：

- 思科ISE（推荐版本3.x）已安装且运行正常。
- 运行EOS并支持RADIUS的Arista交换机。
- ISE中配置的Active Directory(AD)或内部用户数据库。

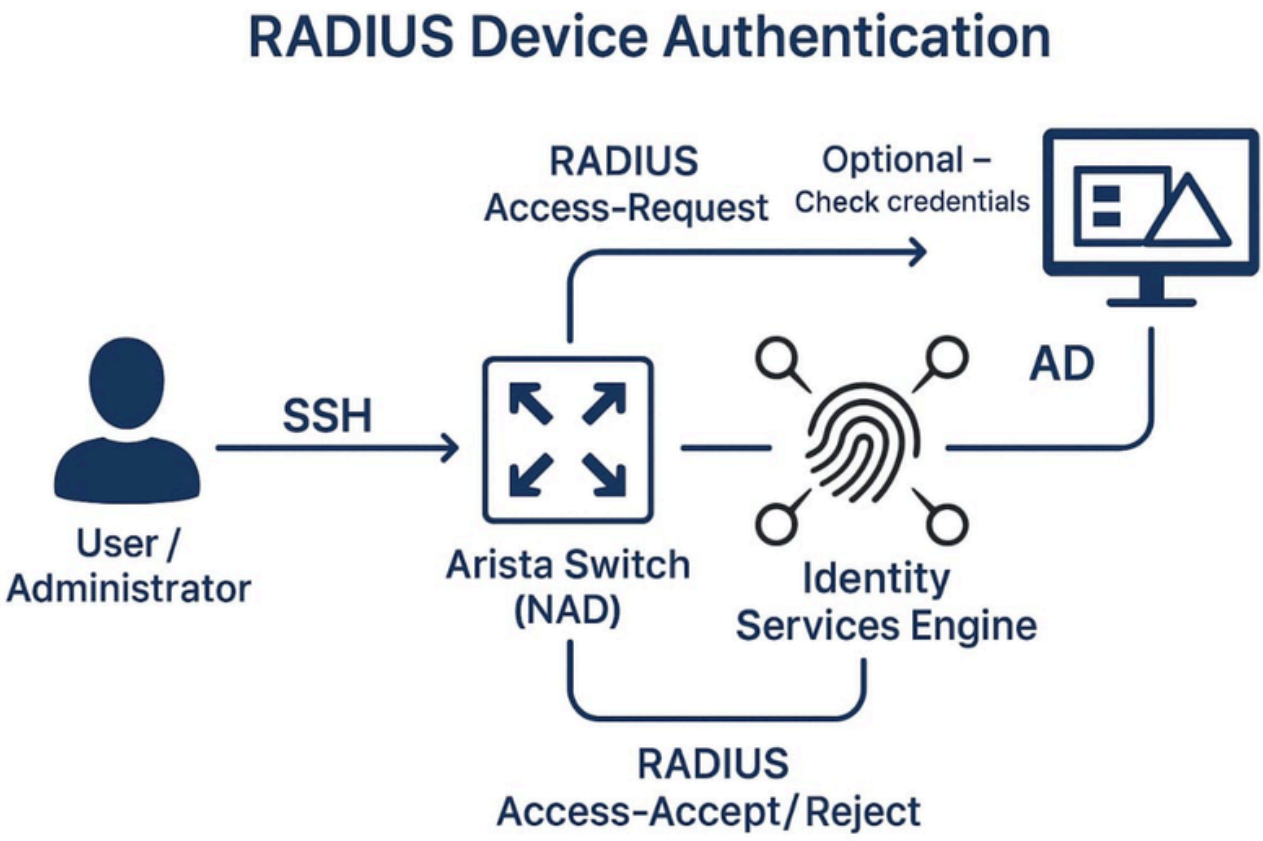
使用的组件

本文档中的信息基于以下软件和硬件版本：

- Arista交换机软件映像版本：4.33.2F
- 思科身份服务引擎(ISE)版本3.3补丁4

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。

网络图



以下网络图展示使用Cisco ISE对Arista交换机进行基于RADIUS的设备身份验证，并将Active Directory(AD)作为可选身份验证源。

该图包括：

- Arista交换机（用作网络接入设备，NAD）
- 思科ISE（充当RADIUS服务器）

- Active Directory(AD)[可选]（用于身份验证）
- 用户/管理员（通过SSH登录）

配置

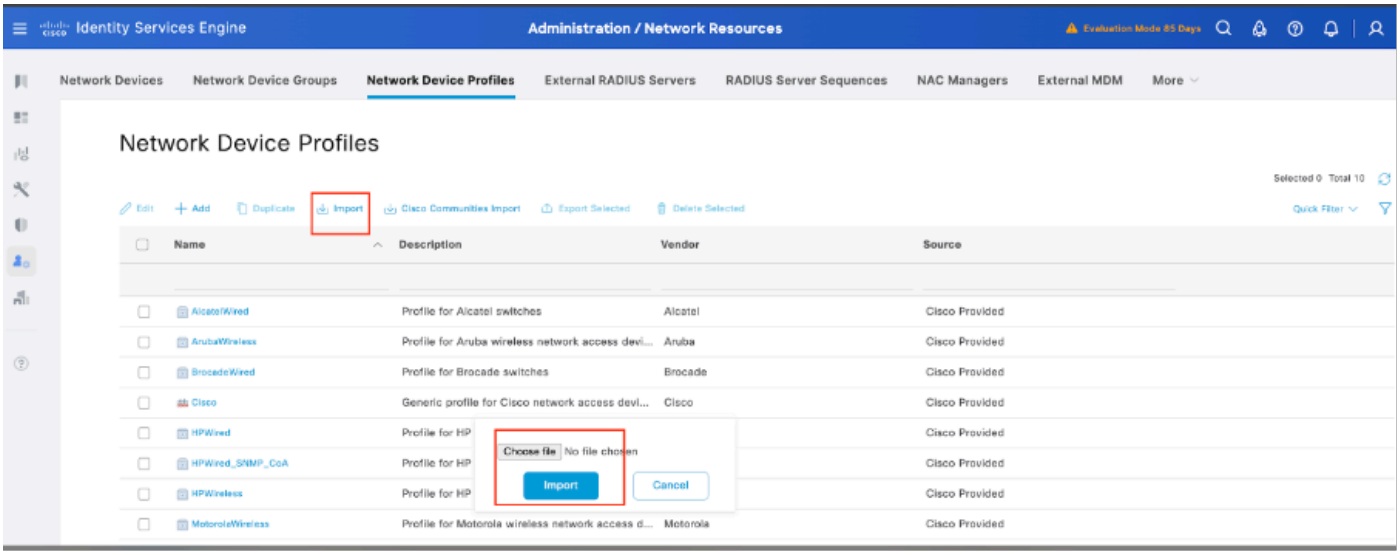
配置Cisco ISE

步骤1：获取思科ISE的Arista网络设备配置文件

思科社区已共享Arista设备的专用NAD配置文件。此配置文件以及必要的字典文件，可以在Arista CloudVision WiFi Dictionary and NAD Profile for ISE Integration文章中找到。将此配置文件下载并导入到ISE设置有助于更顺利的集成。

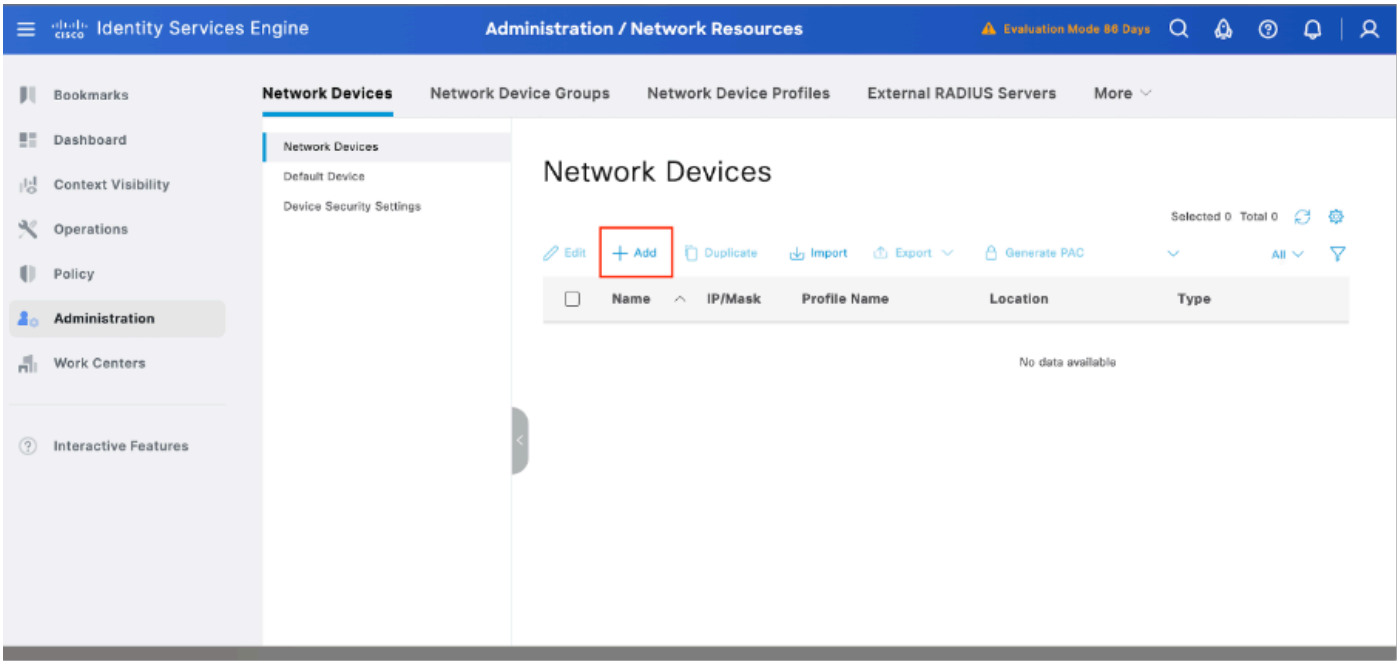
以下是将Arista NAD配置文件导入思科ISE的步骤：

1. 下载配置文件：
    - 从上面提供的思科社区链接获取Arista NAD配置文件。思科社区。
2. 访问Cisco ISE:
    - 登录到您的Cisco ISE管理控制台。
3. 导入NAD配置文件：
    - 导航到管理>网络资源>网络设备配置文件。
    - 单击Import按钮。
    - 上传下载的Arista NAD配置文件。



Step 2. 添加Arista交换机作为网络设备

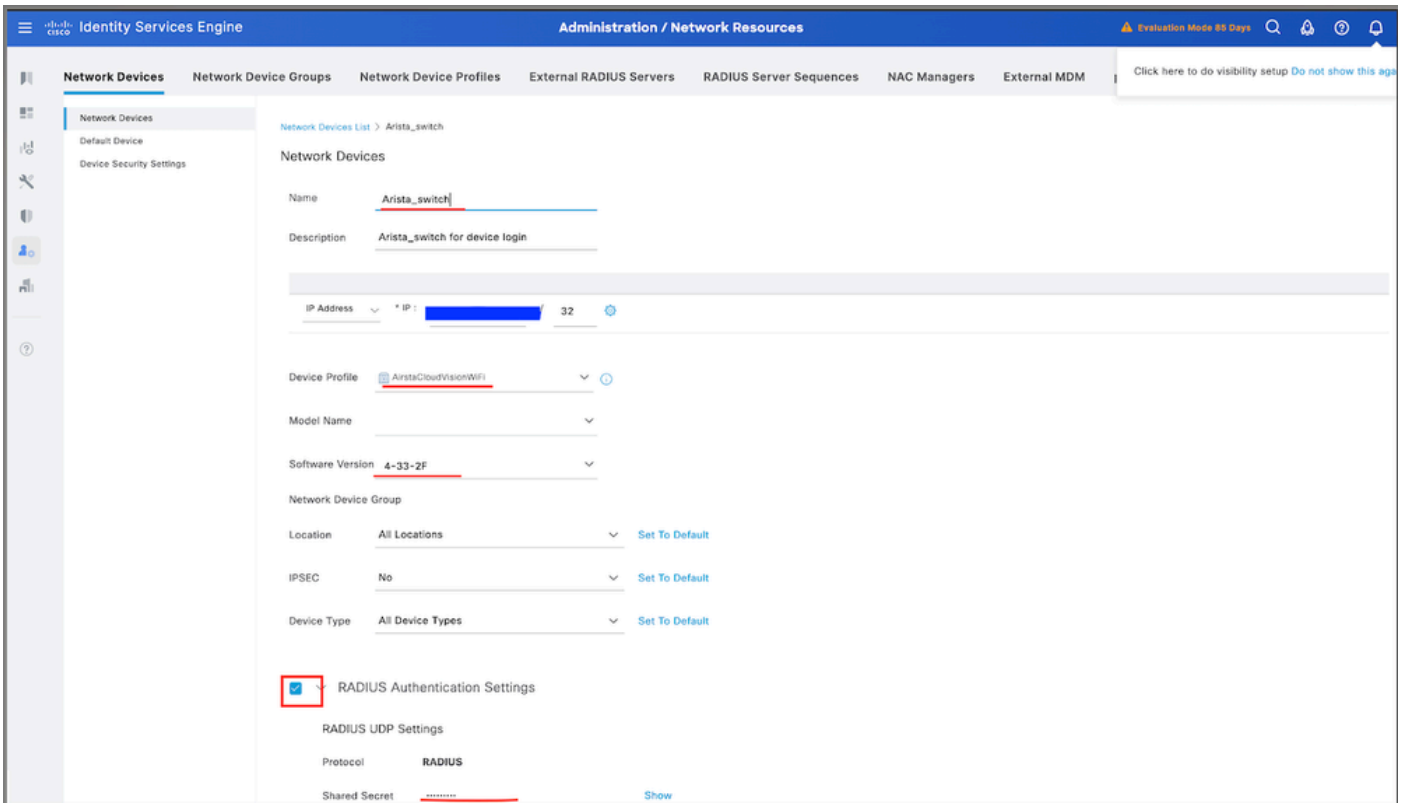
1. 导航到管理>网络资源>网络设备> +添加。



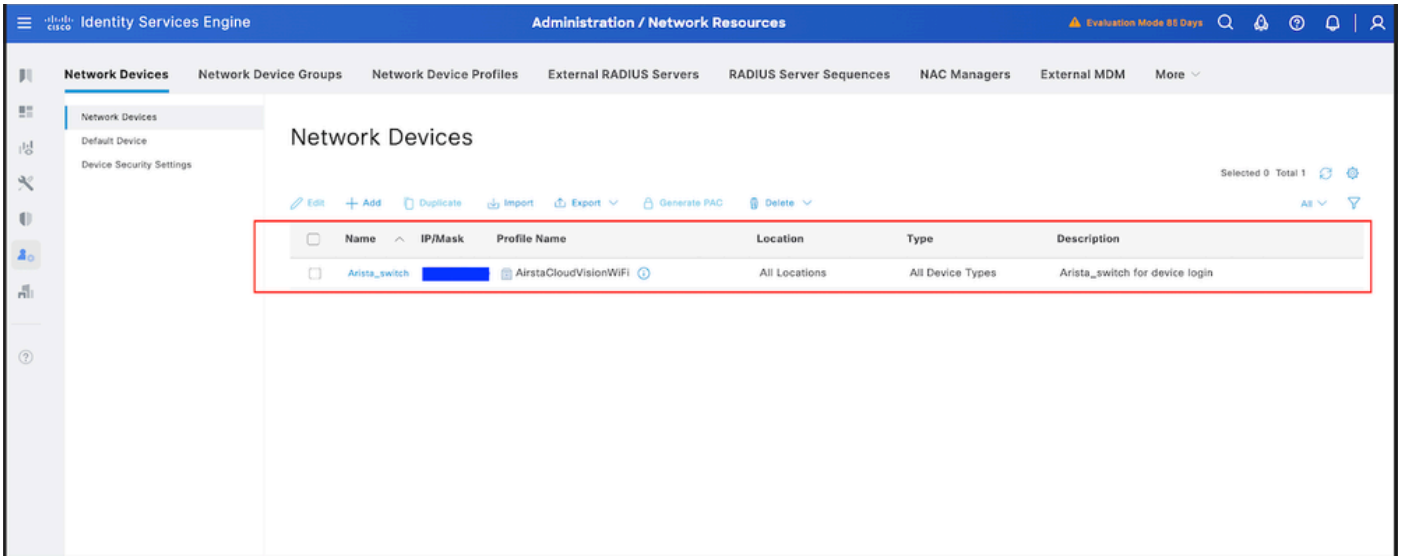
2.单击Add并输入以下详细信息：

1. 名称：Arista-Switch
2. IP Address:<Switch-IP>
3. 设备类型：选择其他有线
4. 网络设备配置文件:选择AirstaCloudVisionWiFi。
5. RADIUS身份验证设置:
    1. 启用RADIUS身份验证
    2. 输入Shared Secret（必须与交换机配置匹配）。

3.单击保存。

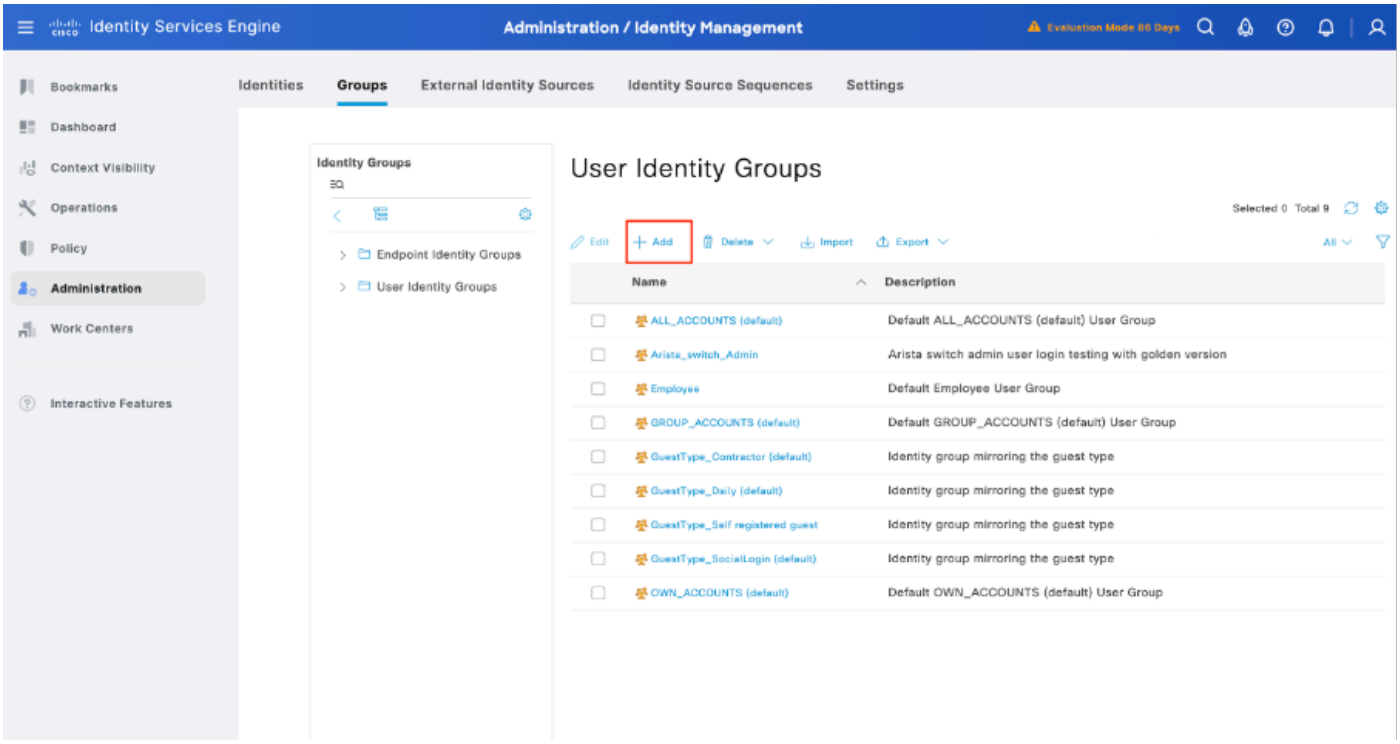


第 3 步： 验证“Network Devices（网络设备）”下显示的新设备



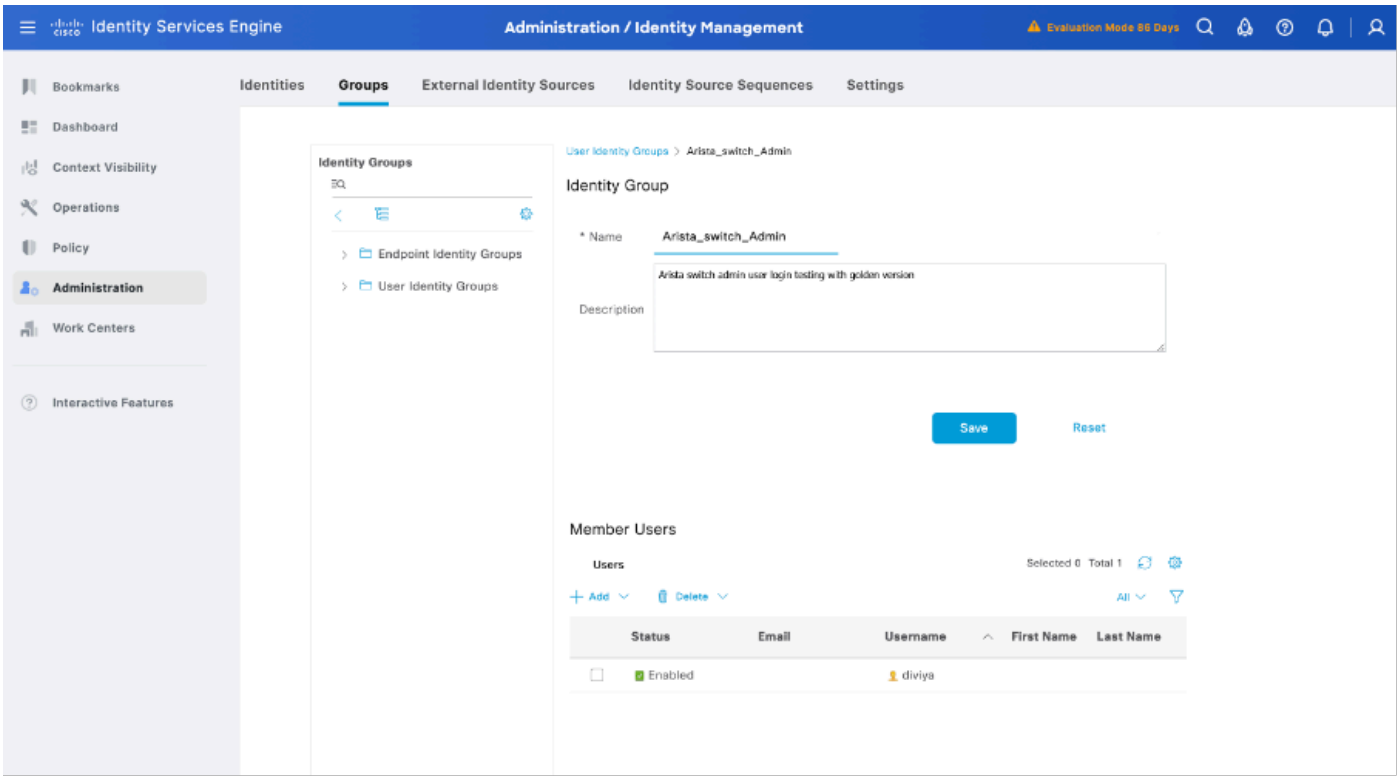
第 4 步： 创建所需的用户身份组

导航到管理>身份管理>组>用户身份组> +添加:



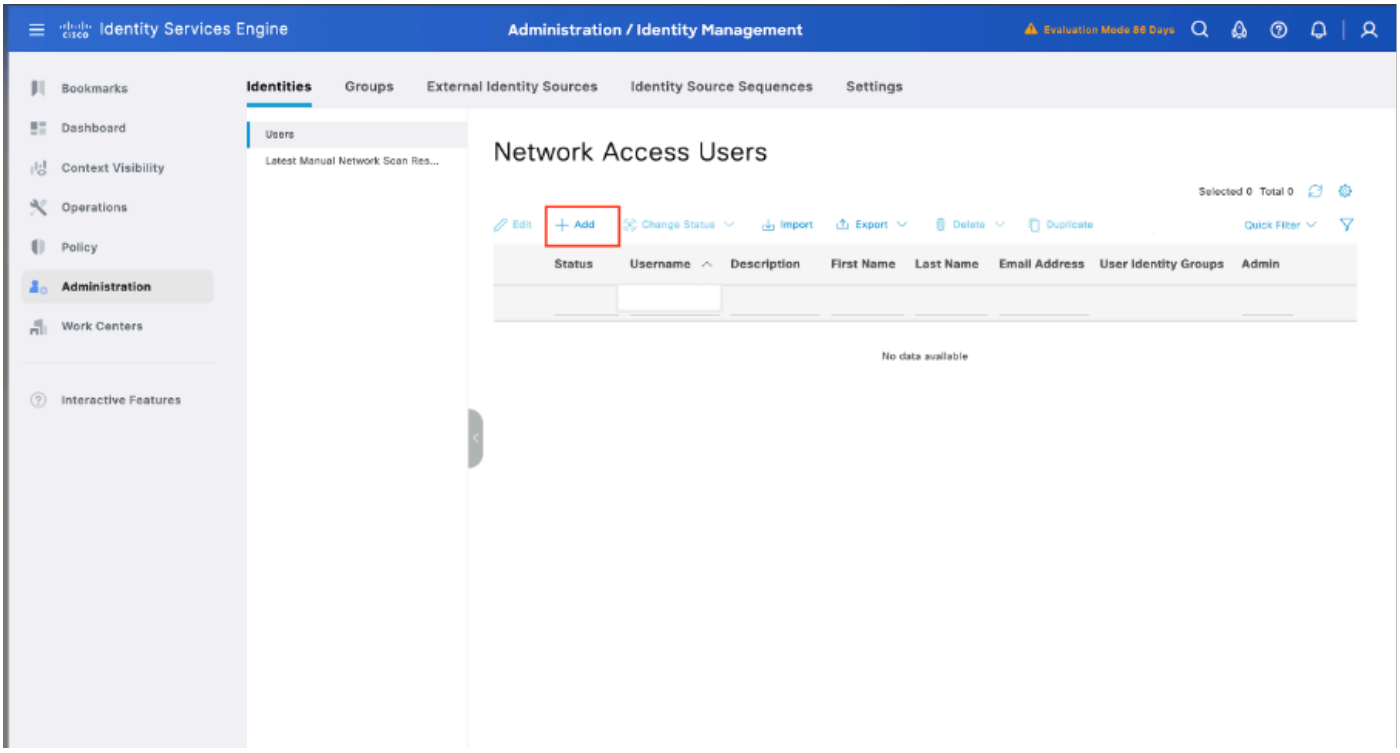
第 5 步： 设置管理员用户身份组的名称

单击Submit以保存配置：

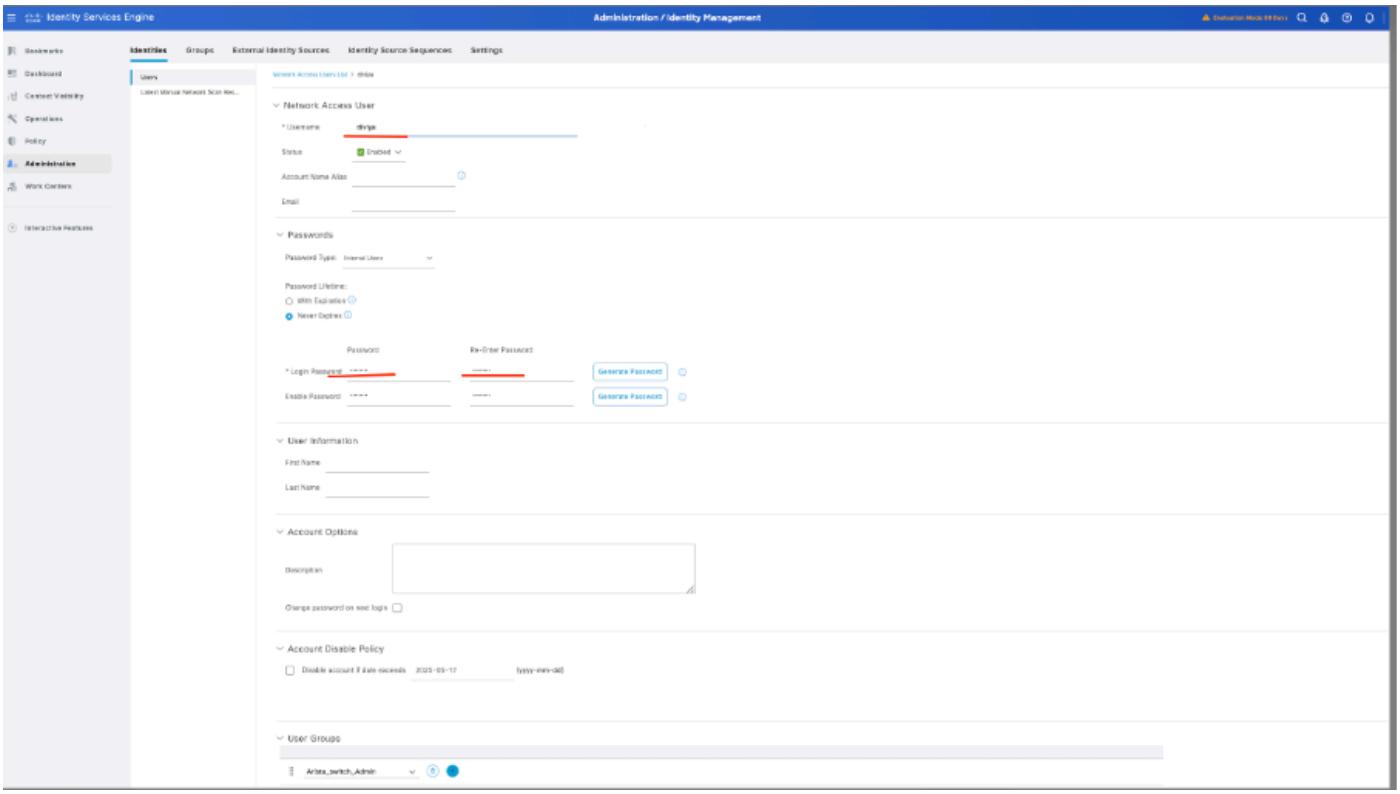


第六步： 创建本地用户并将他们添加到其往来行组

导航到管理>身份管理>身份> +添加:



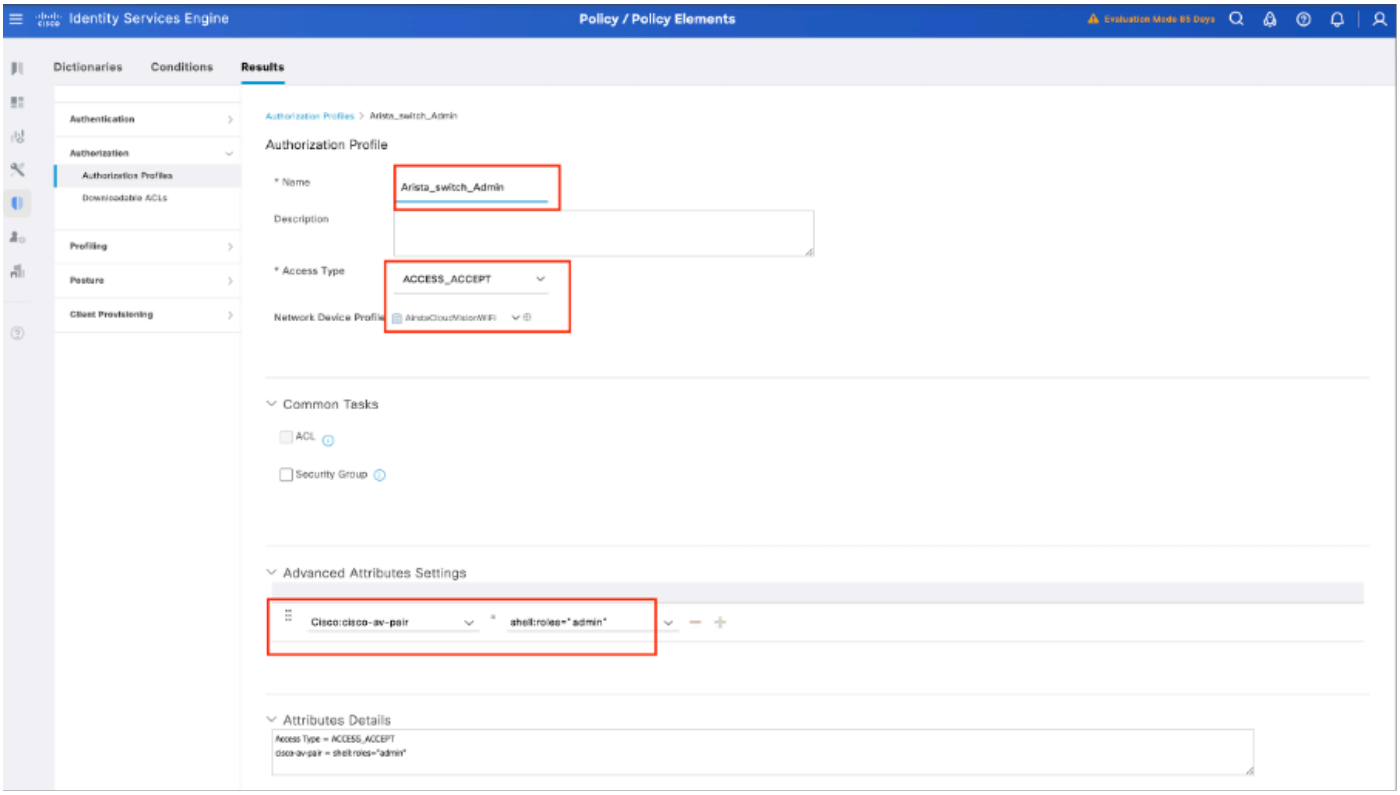
6.1.添加具有管理员权限的用户。设置名称、密码并将其分配给Arista_switch_Admin，向下滚动并单击Submit以保存更改。



第 7 步： 为管理员用户创建授权配置文件

导航到Policy > Policy Elements > Results > Authorization > Authorization Profiles > +Add。

定义授权配置文件的名称，将Access Type保留为ACCESS_ACCEPT，然后在Advanced Attributes Settings下添加cisco-av-pair=shell:roles="admin"，然后单击Submit。



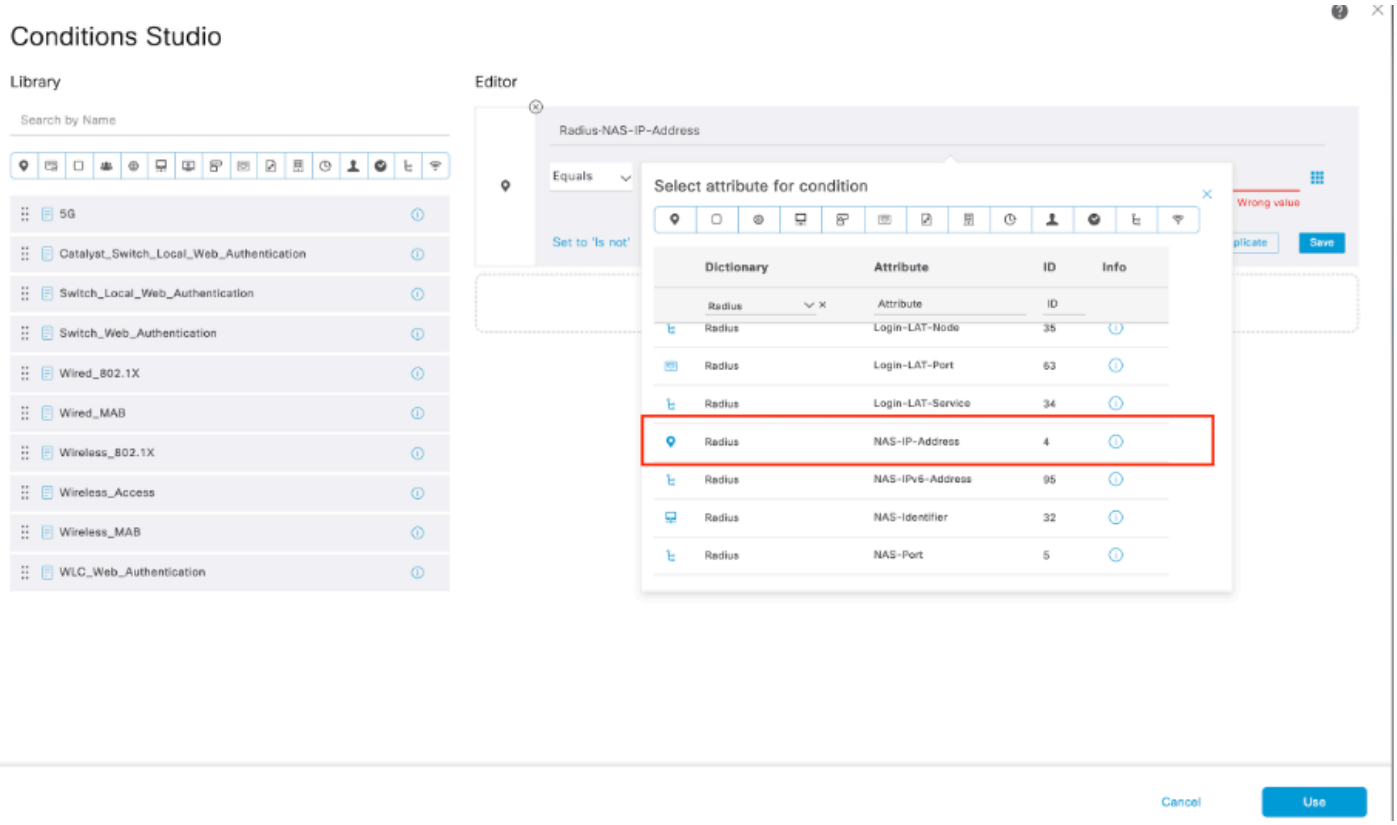
步骤 8 创建与Arista交换机IP地址匹配的策略集

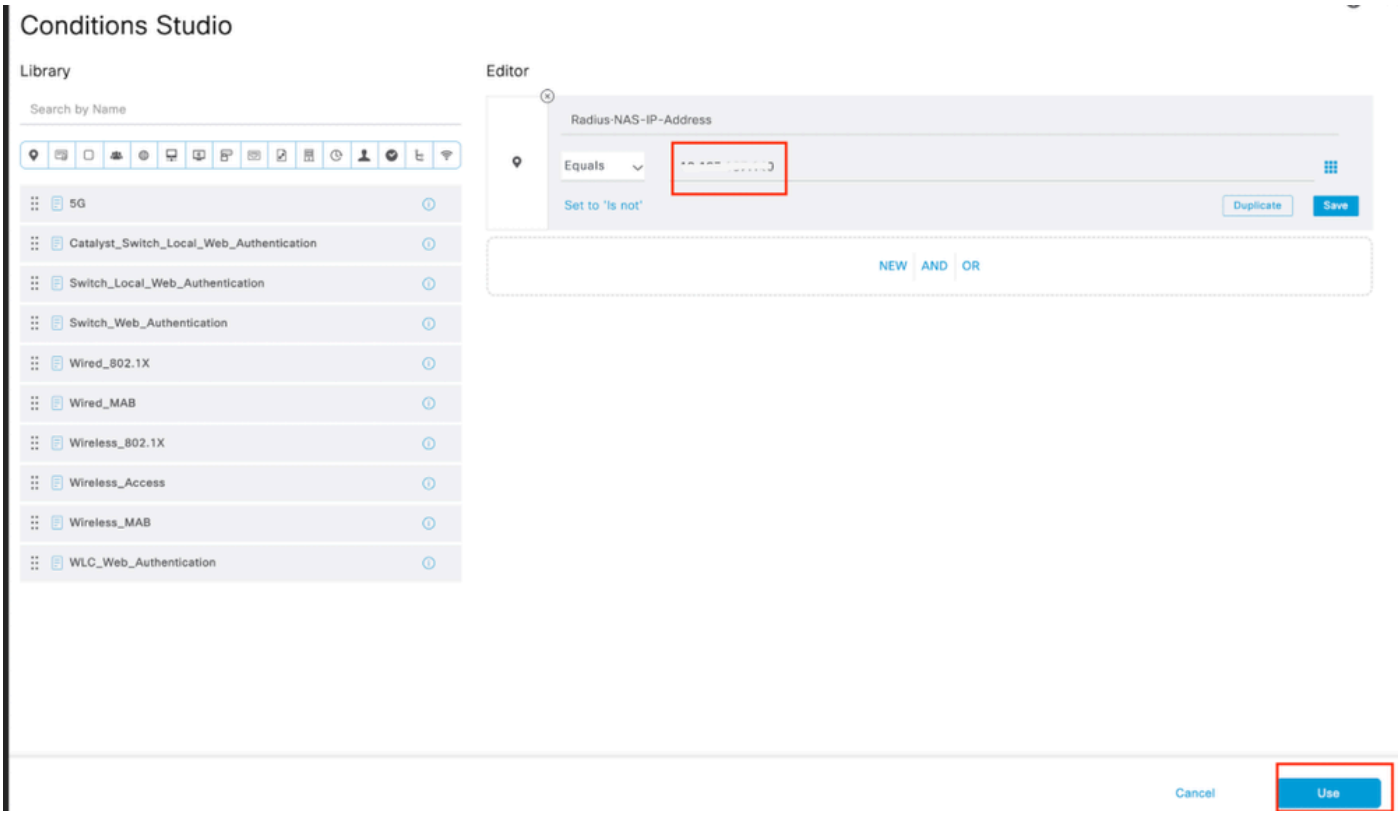
这是为了防止其他设备向用户授予访问权限。

导航到Policy > Policy Sets >Add图标，图标位于左上角。

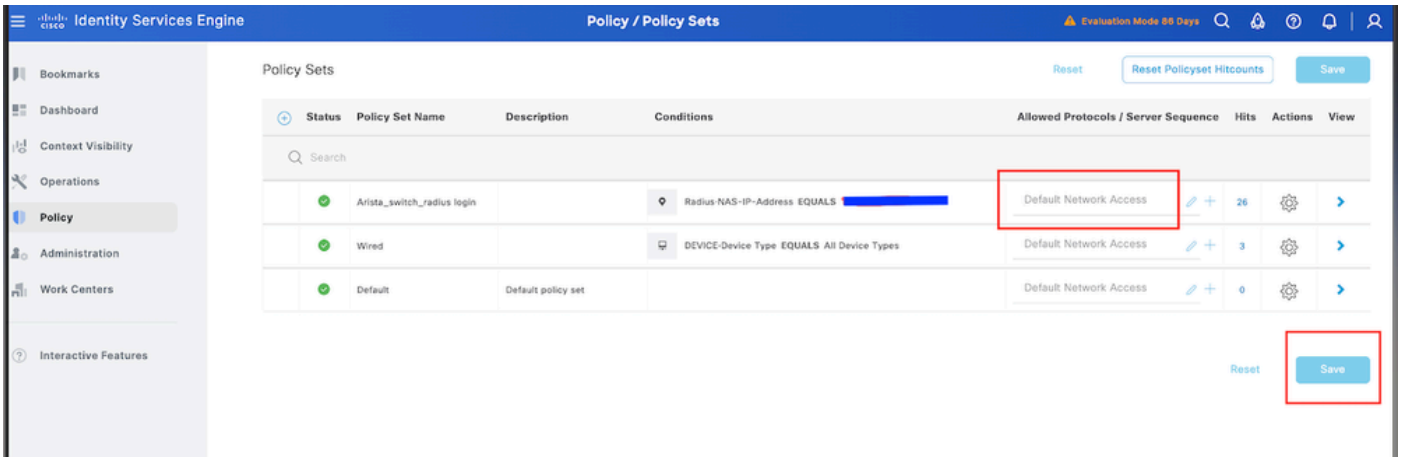
8.1新行位于策略集的顶部。单击Add图标配置新条件。

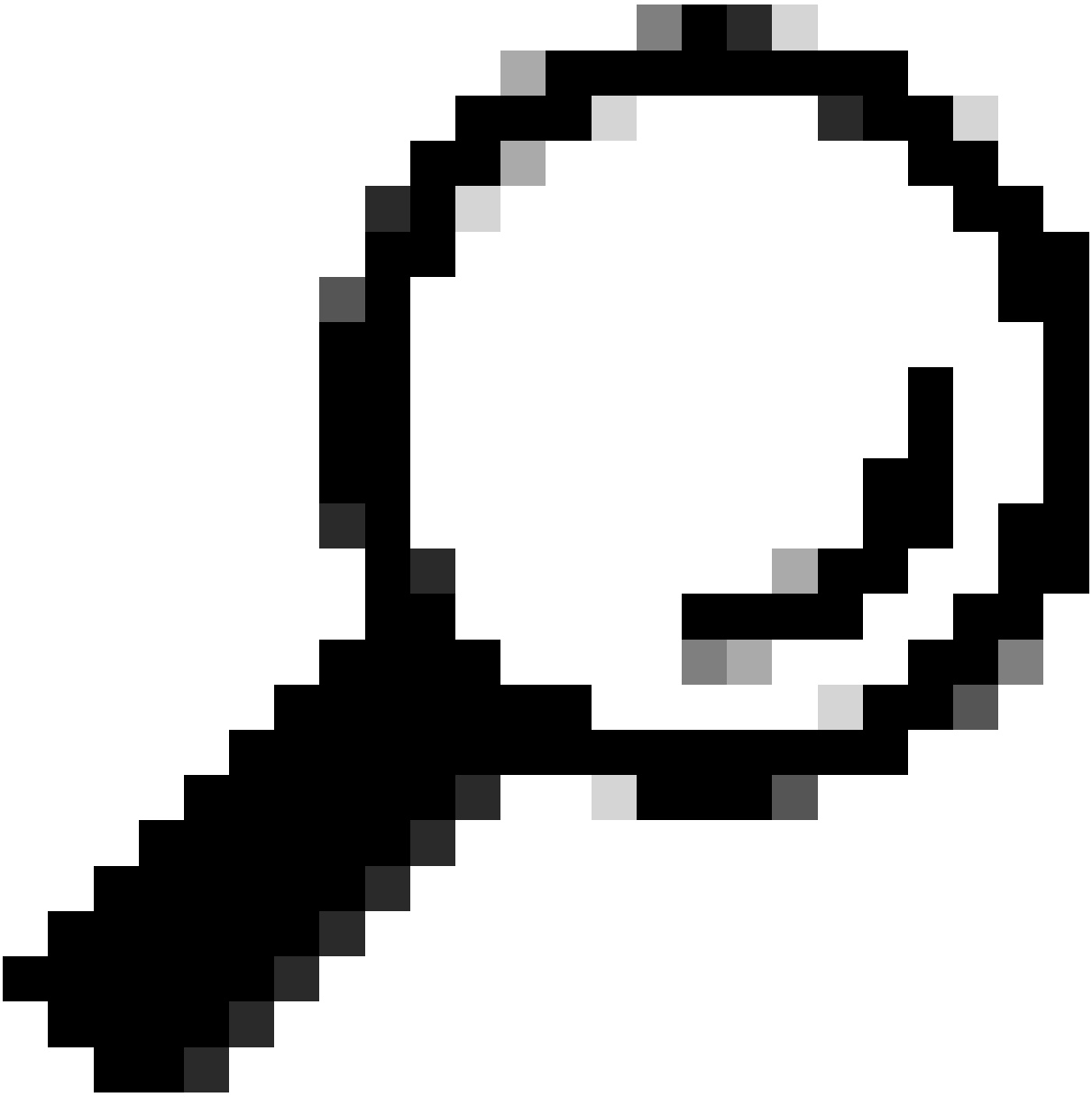
8.2为与Arista交换机IP地址匹配的RADIUS NAS-IP-Address属性添加顶部条件，然后单击Use。





8.3完成后，单击Save:

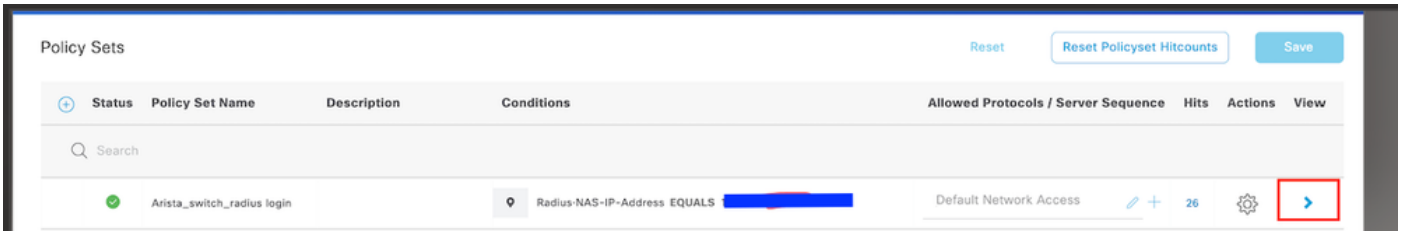




提示：在本练习中，我们允许使用Default Network Access Protocols列表。您可以创建新列表并根据需要缩小其范围。

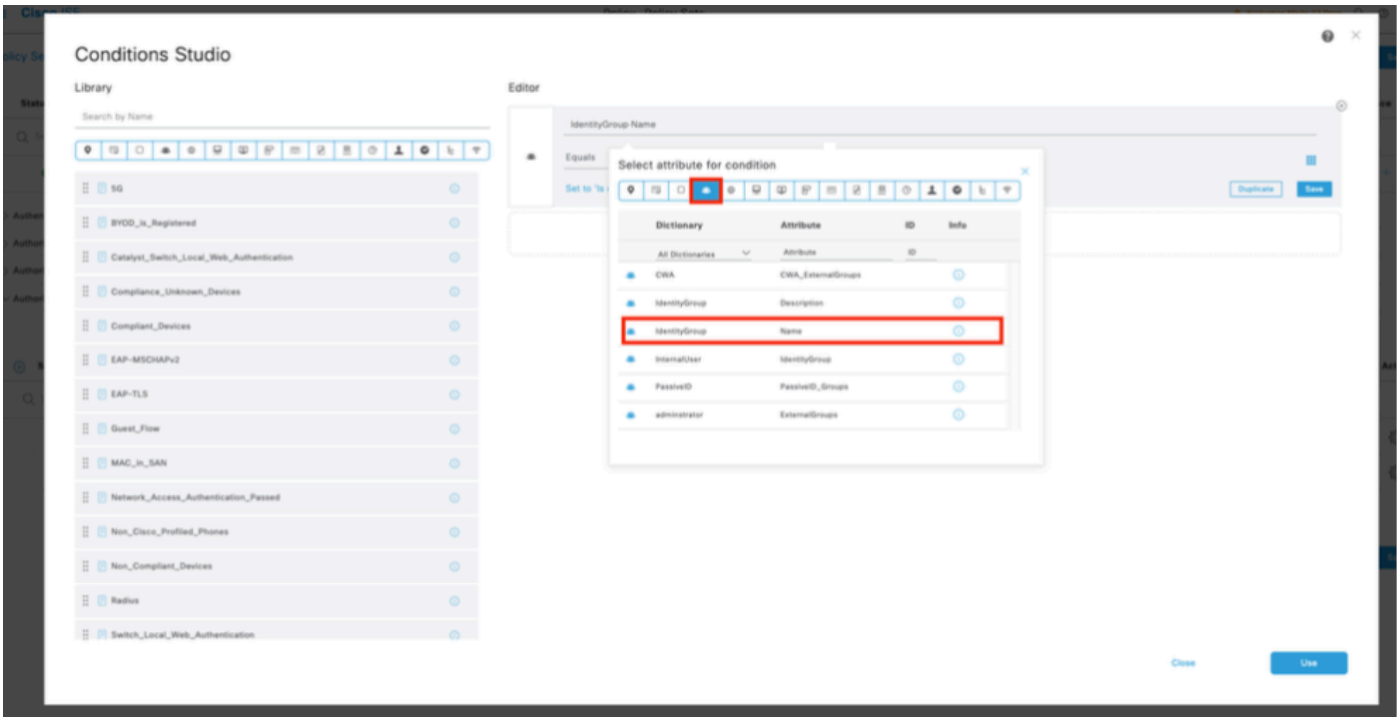
步骤 9 查看新策略集

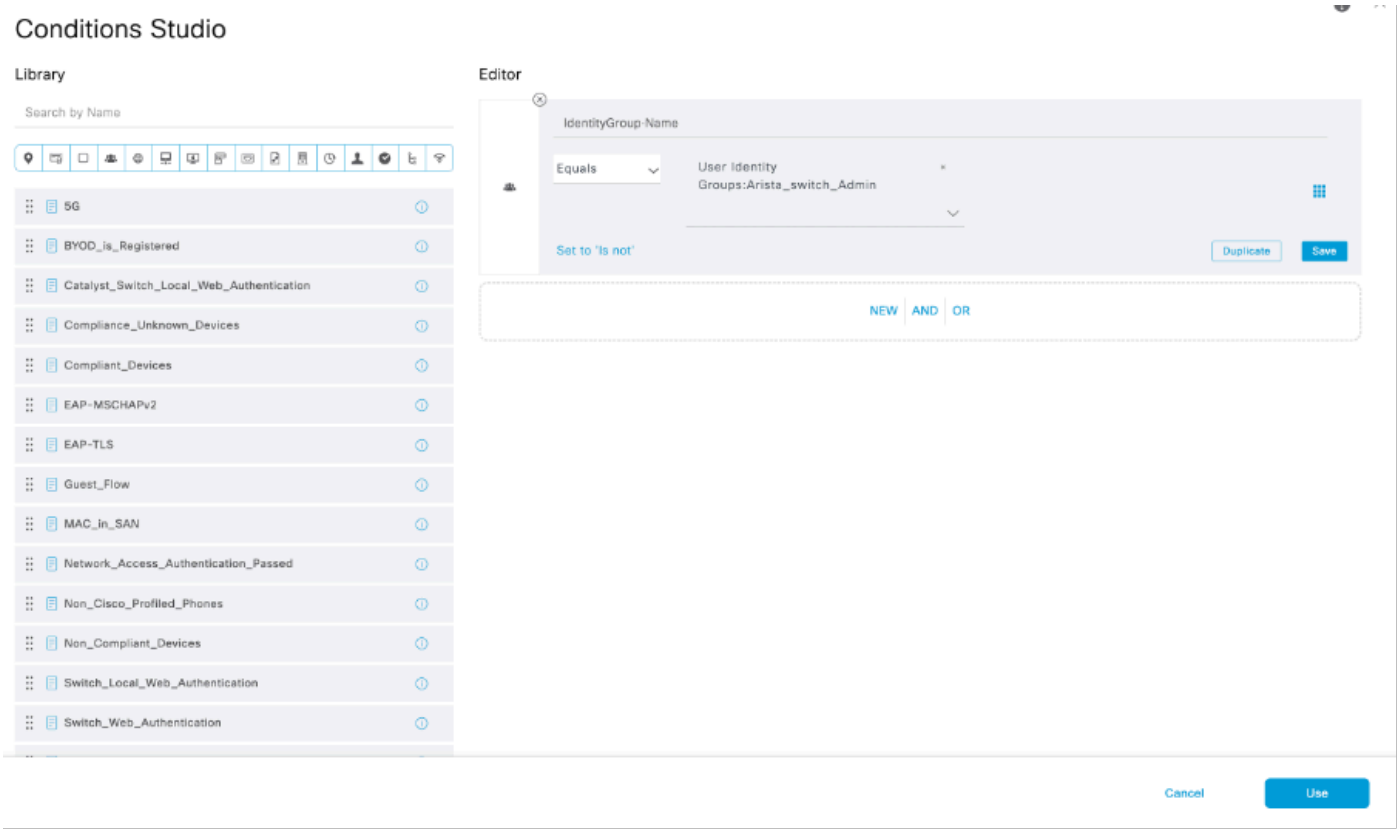
点击位于行尾的>图标：



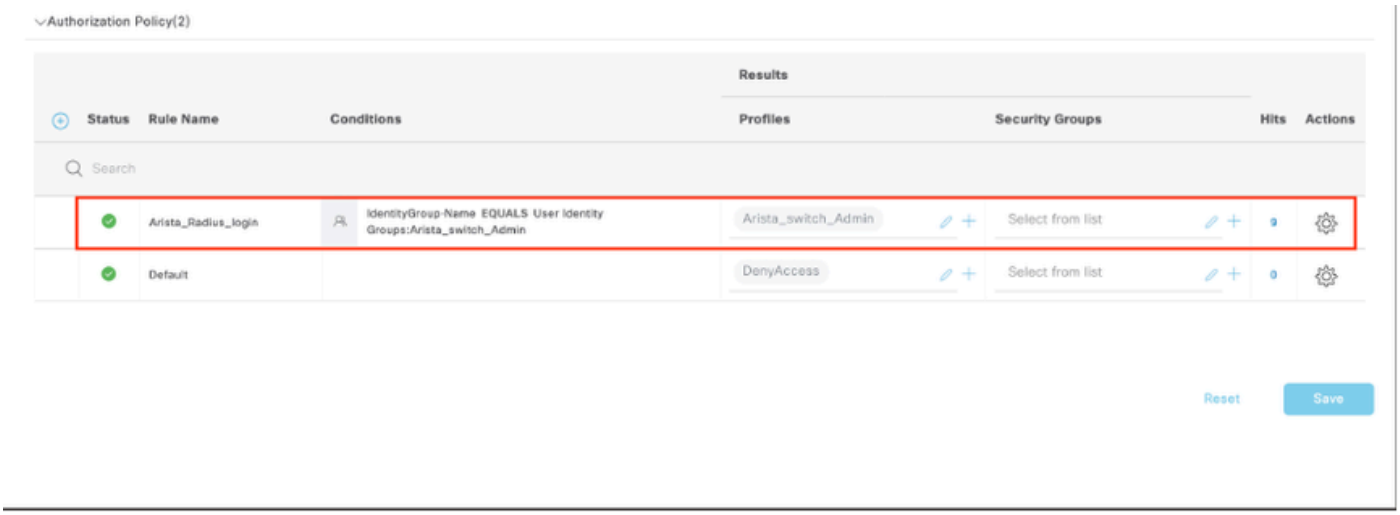
9.1展开Authorization Policy菜单，然后单击(+)添加新条件。

9.2设置条件以匹配Dictionary Identity Group with Attribute Name Equals User Identity Groups:Arista_switch_Admin(在步骤7中创建的组名称)，然后点击使用。





9.3验证在授权策略中配置的新条件，然后在配置文件下添加用户配置文件



配置Arista交换机

步骤1.启用RADIUS身份验证

登录到Arista交换机并进入配置模式：

配置

!

radius-server host <ISE-IP> key <RADIUS-SECRET>

radius-server timeout 5

radius-server retransmit 3

radius-server deadtime 30

!

aaa group server radius ISE

服务器<ISE-IP>

!

aaa authentication login default group ISE local

aaa authorization exec default group ISE local

aaa accounting exec default start-stop group ISE

aaa accounting commands 15 default start-stop group ISE

aaa accounting system default start-stop group ISE

!

结束

步骤2.保存配置

要在重新启动后保留设置，请执行以下操作：

写存储器

或

copy running-config startup-config

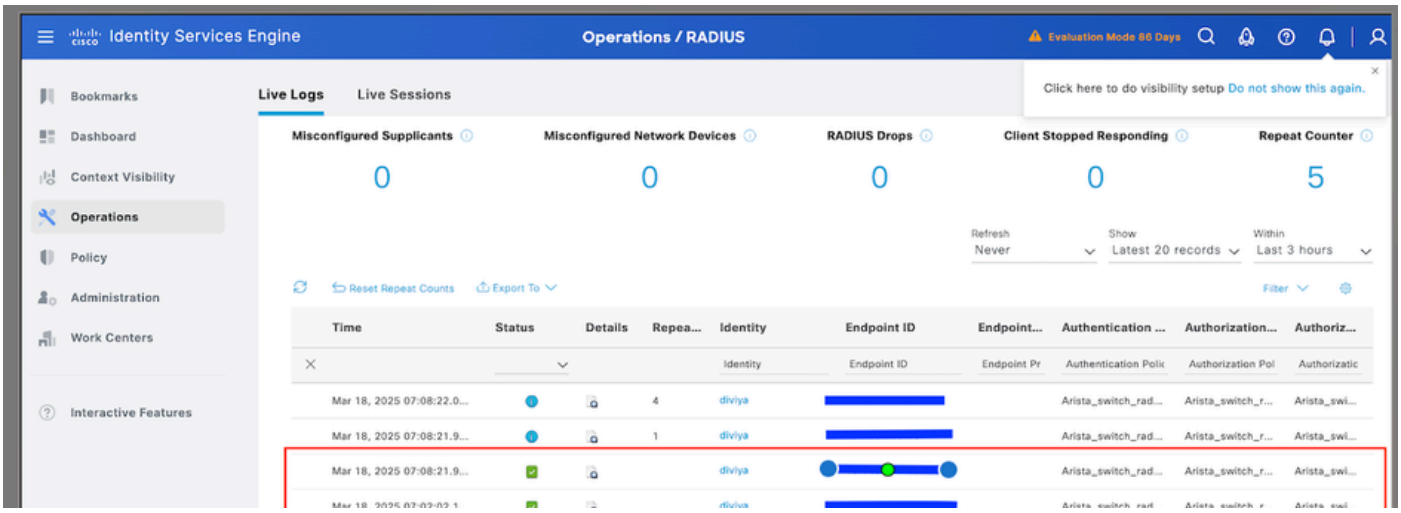
验证

ISE审核

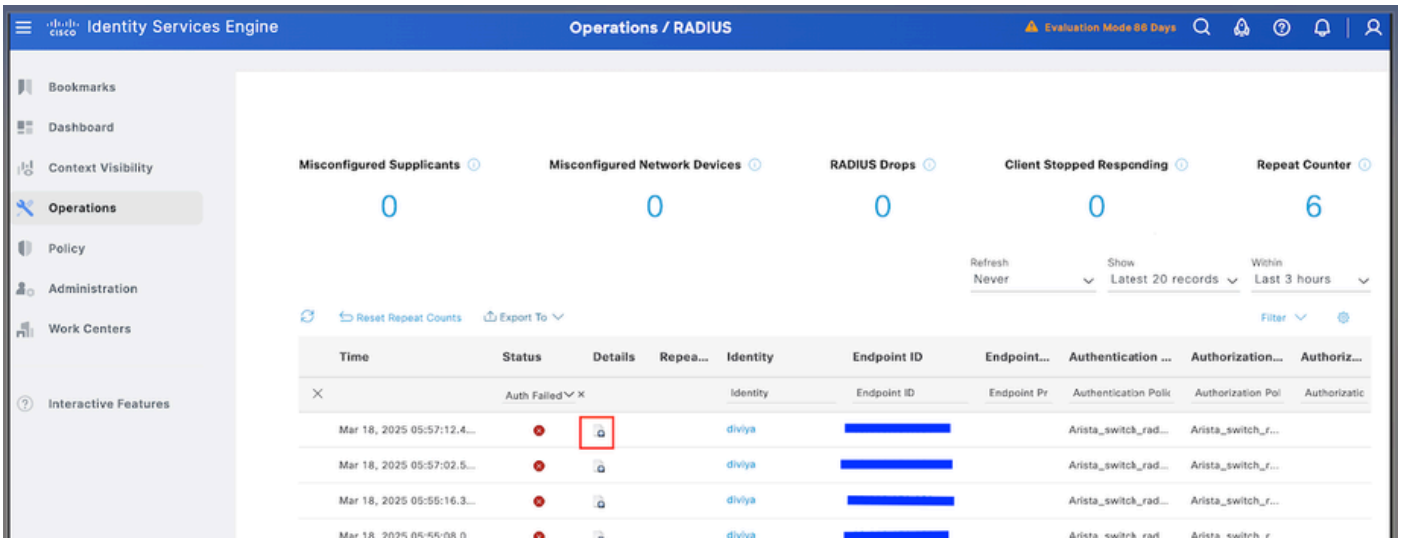
1.尝试使用新的Radius凭证登录Arista交换机：

1.1导航到操作> Radius >实时日志。

1.2显示的信息显示用户是否成功登录。



2.对于失败状态，请查看会话详细信息：

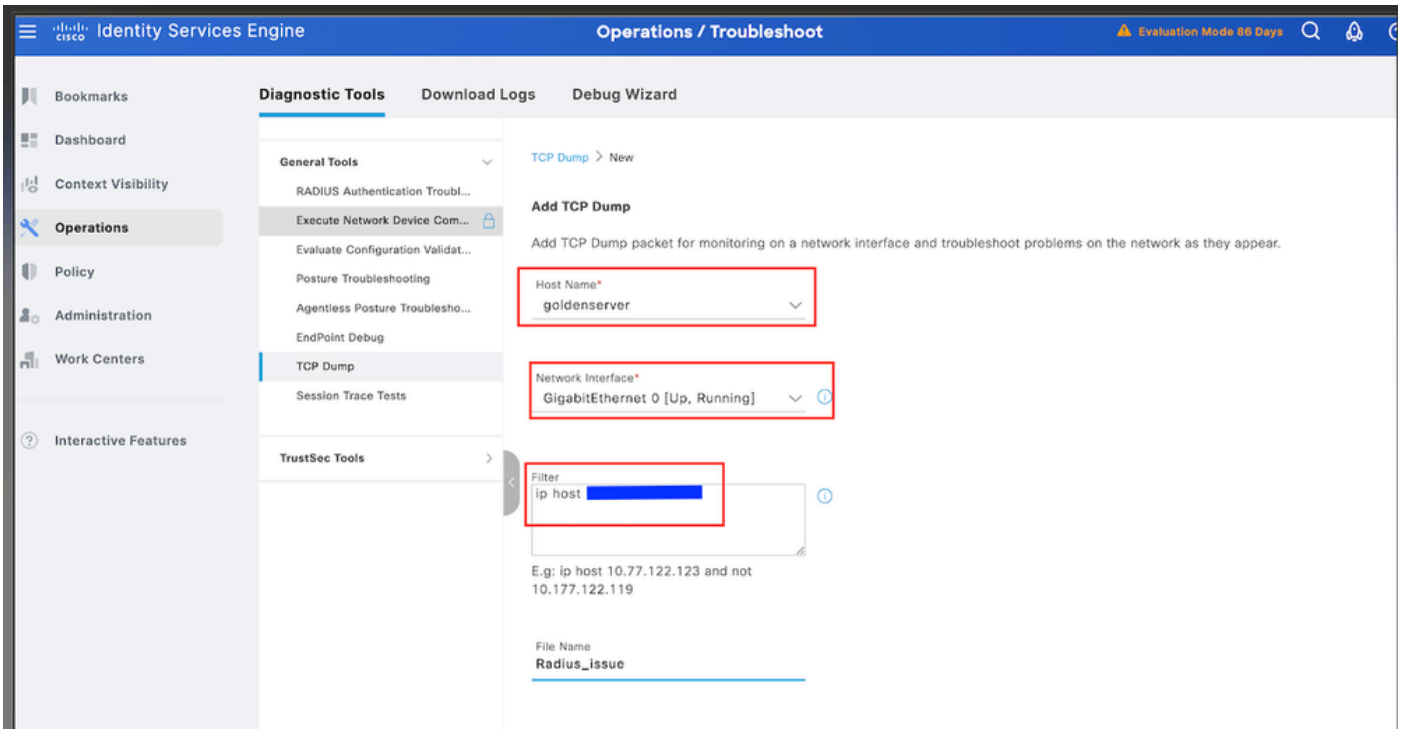


3.对于未显示在Radius Live日志中的请求，请查看UDP请求是否通过数据包捕获到达ISE节点。

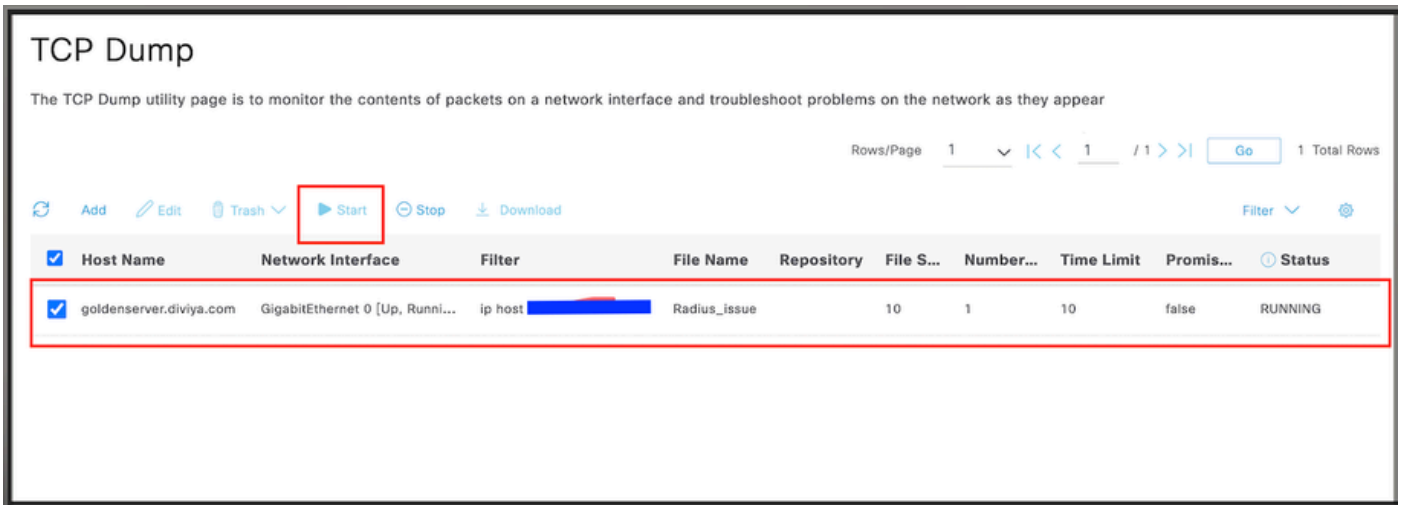
3.1.导航到操作>故障排除>诊断工具> TCP转储。

3.2.添加新的捕获并将文件下载到本地计算机，以查看UDP数据包是否到达ISE节点。

3.3.填写请求的信息，向下滚动并点击保存。



3.4.选择并启动捕获。



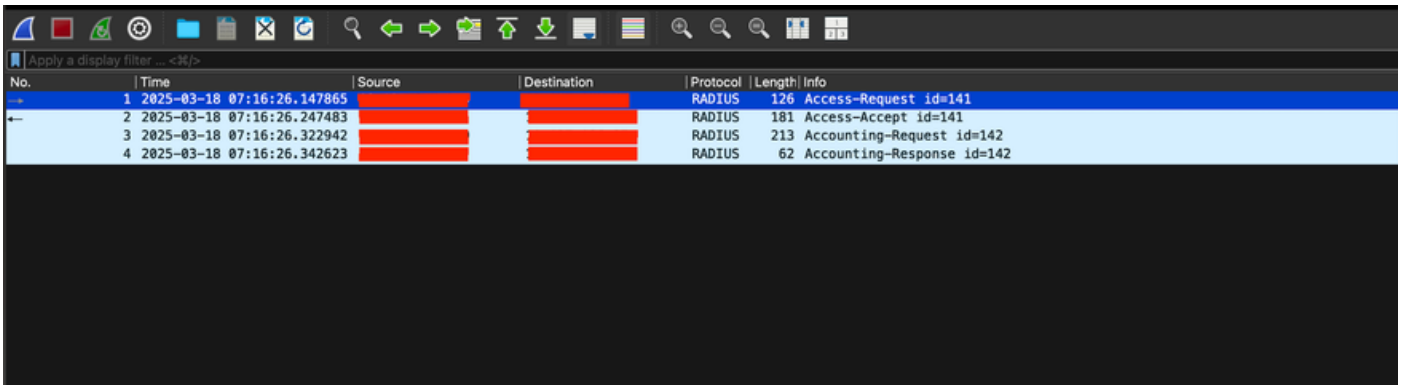
3.5.尝试在ISE捕获运行时登录到Arista交换机。

3.6.停止ISE中的TCP转储并将文件下载到本地计算机。

3.7.检查流量输出。

预期输出：

数据包No1。从Arista交换机通过端口1812(RADIUS)向ISE服务器发出的请求。
数据包No2。ISE服务器应答接受初始请求。



故障排除

场景1.“5405 RADIUS请求已丢弃”

问题

此场景涉及排除在网络设备（例如Arista交换机）尝试进行身份验证时在Cisco ISE中出现“5405 RADIUS Request dropped”错误，原因为“11007 Could not locate Network Device or AAA Client”。

可能的原因

- 思科身份服务引擎(ISE)无法识别Arista交换机，因为其IP地址未在已知网络设备中列出。
- RADIUS请求来自ISE无法识别为有效网络设备或AAA客户端的IP地址。
- 交换机和ISE之间的配置可能不匹配（例如IP或共享密钥不正确）。

解决方案

- 将交换机添加到具有正确IP地址的网络设备的Cisco ISE列表。
- 验证ISE中配置的IP地址和共享密钥与交换机上的设置完全匹配。
- 更正后，必须正确识别并处理RADIUS请求。

场景2:Arista交换机无法故障切换到备份ISE PSN

问题

Arista交换机配置为使用Cisco ISE进行RADIUS身份验证。当主ISE策略服务节点(PSN)不可用时，交换机不会自动故障切换到备用PSN。因此，身份验证日志仅显示在主ISE PSN中，当主设备关闭时，从辅助/备用PSN中没有任何日志。

可能的原因

- Arista交换机的RADIUS服务器配置仅指向主ISE节点，因此不使用备份服务器。

- 未正确设置RADIUS服务器优先级，或者配置中缺少备份ISE IP。
- 交换机上的超时和重传设置设置过低，导致无法成功回退到备用PSN。
- 交换机将FQDN用于PSN，但DNS解析不会返回所有A记录，导致只与主服务器联系。

解决方案

- 确保在交换机的RADIUS服务器组配置中输入多个ISE PSN IP。这样，如果主设备无法访问，交换机可以使用备份ISE PSN。

  配置示例:

  ```
  radius-server host <ISE1-IP> key <secret>

  radius-server host <ISE2-IP> key <secret>
  ```

- 验证RADIUS服务器优先级、超时和重传值是否已正确配置，以实现可靠的故障切换。
- 如果使用FQDN，请检查DNS设置和解析，以确保交换机返回和使用所有PSN IP地址。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。