在带有ISE的Arista交换机上配置TACACS+身份验证

目录

简介

先决条件

使用的组件

网络图

配置

- ISE上的TACACS+配置
- 配置Arista交换机
  - 步骤1.启用TACACS+身份验证
  - 步骤2.保存配置

验证

- ISE审核

故障排除

- 问题 1
  - 可能的原因
- 问题 2
  - 可能的原因
  - 解决方案

简介

本文档介绍如何将Cisco ISE TACACS+与Arista交换机集成以实现集中式AAA管理员访问。

先决条件

Cisco 建议您了解以下主题：

- Cisco ISE和TACACS+协议。
- Arista交换机

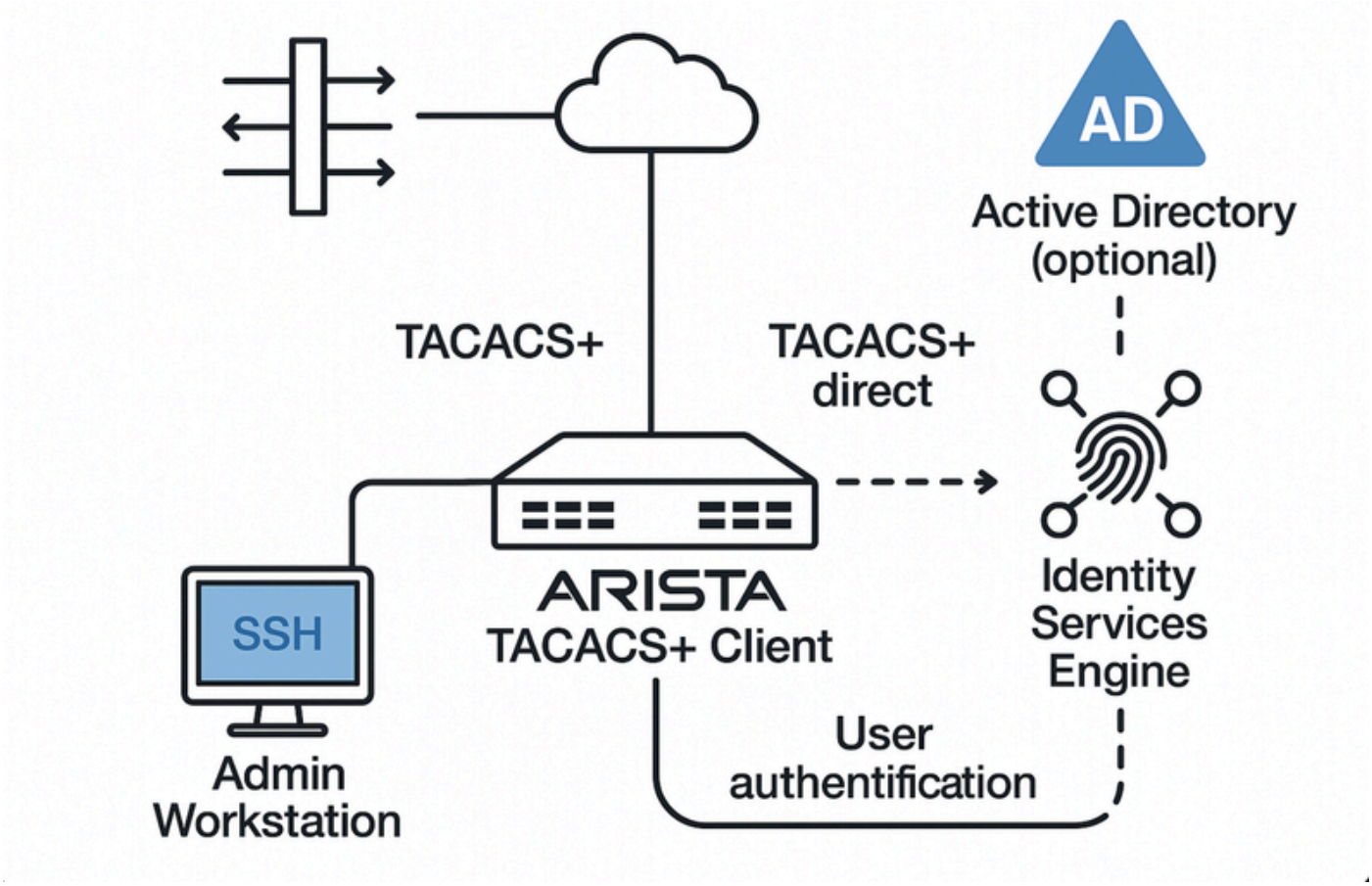
使用的组件

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，请确保您了解任何命令的潜在影响

网络图

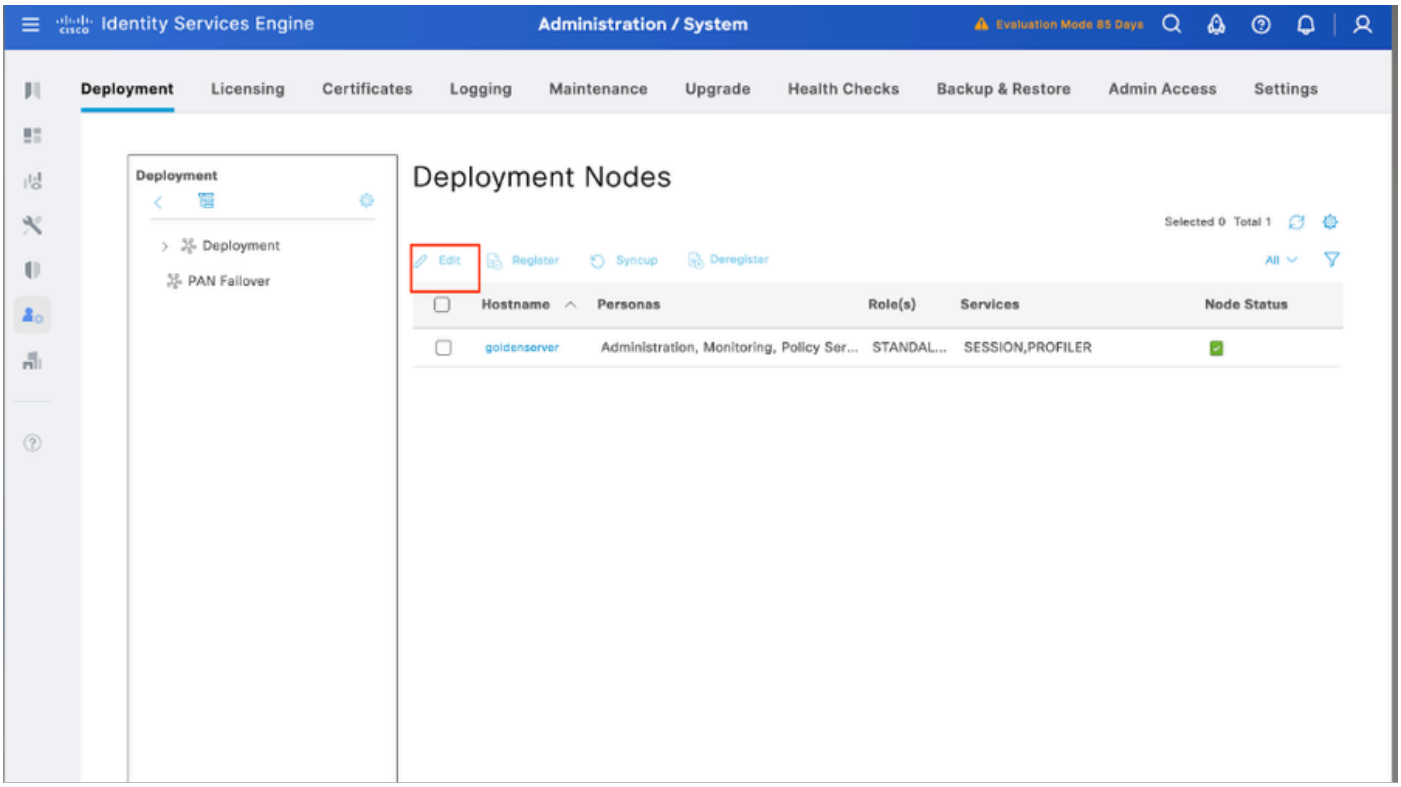


配置

ISE上的TACACS+配置

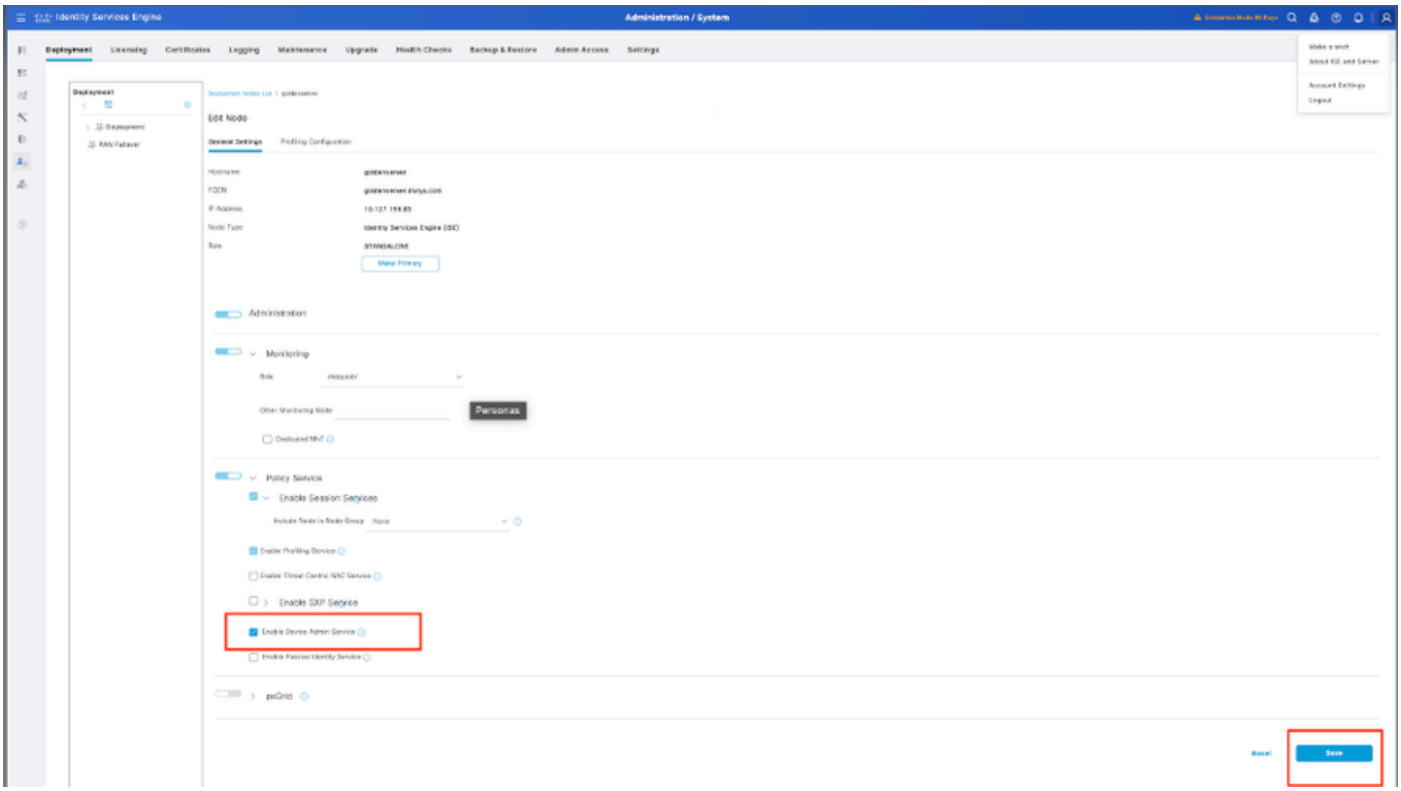
步骤1.初始步骤是验证思科ISE是否具有处理TACACS+身份验证的必要功能。为此，请确认所需的策略服务节点(PSN)已启用设备管理服务功能。

导航到Administration > System > Deployment，选择ISE处理TACACS+身份验证的相应节点，然后单击Edit查看其配置。



步骤2.向下滚动以查找Device Administration Service功能。请注意，启用此功能需要策略服务角色在节点上处于活动状态，并且部署中需要可用的TACACS+许可证。

选中此复选框可启用该功能，然后保存配置。



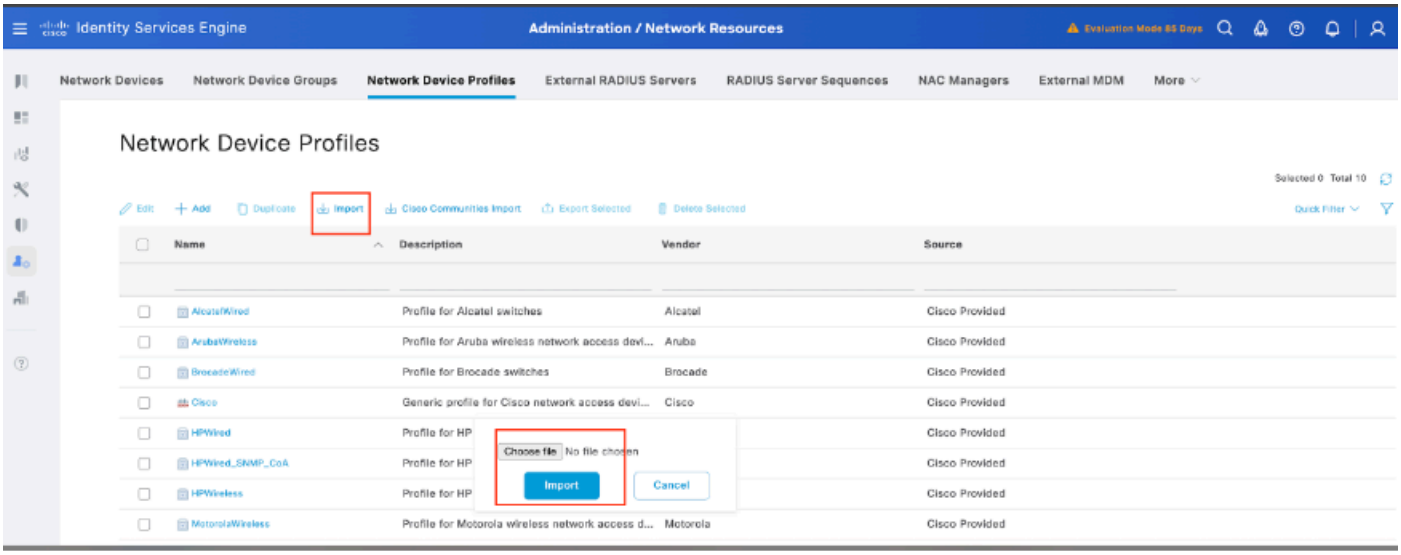
步骤3.获取思科ISE的Arista网络设备配置文件。

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

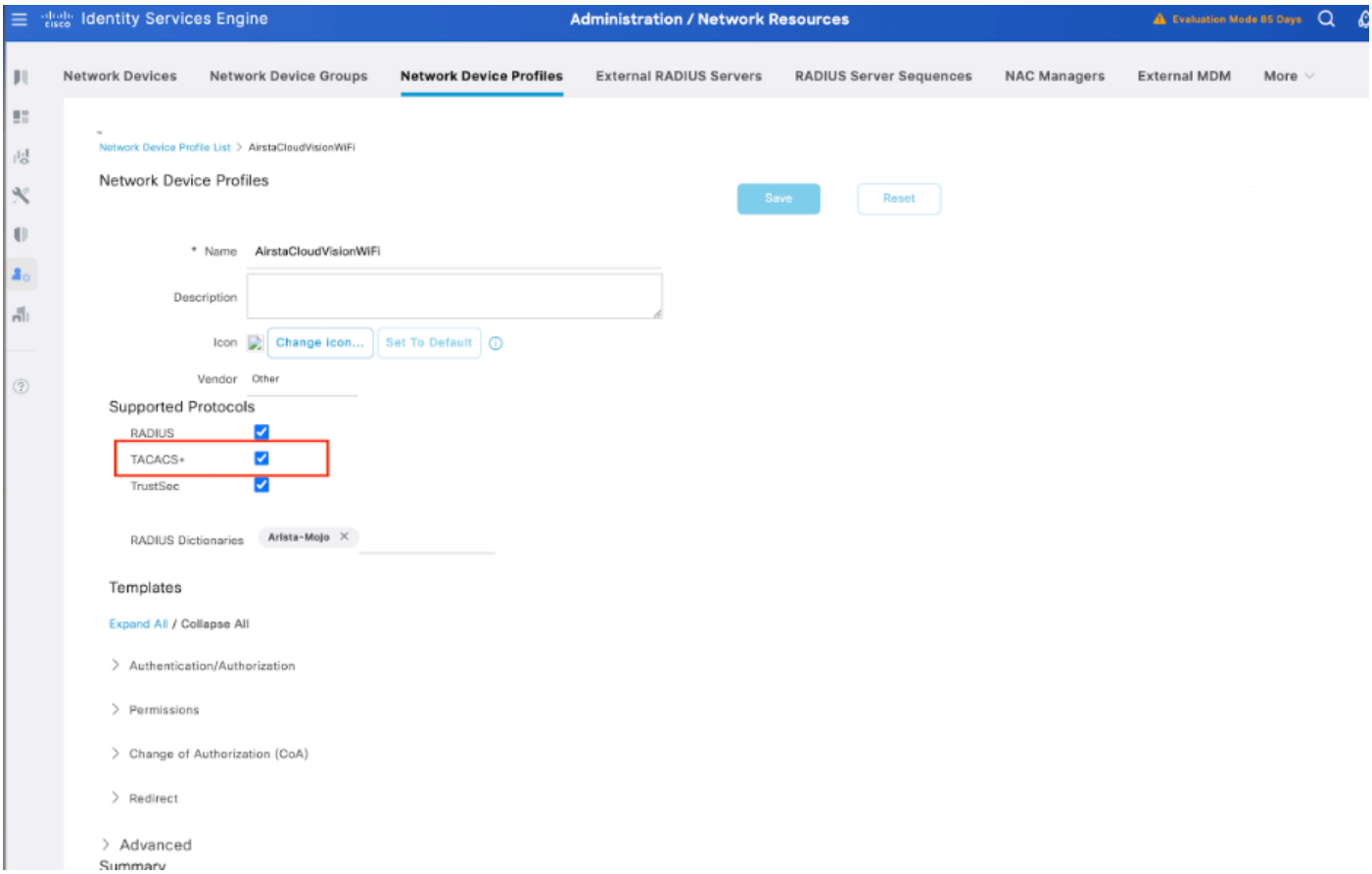
CloudVision WiFi Dictionary and NAD Profile for ISE Integration文章中找到。将此配置文件下载并导入到ISE设置有助于更顺利的集成。

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。
    - 点击Import按钮。
    - 上传下载的Arista NAD配置文件。

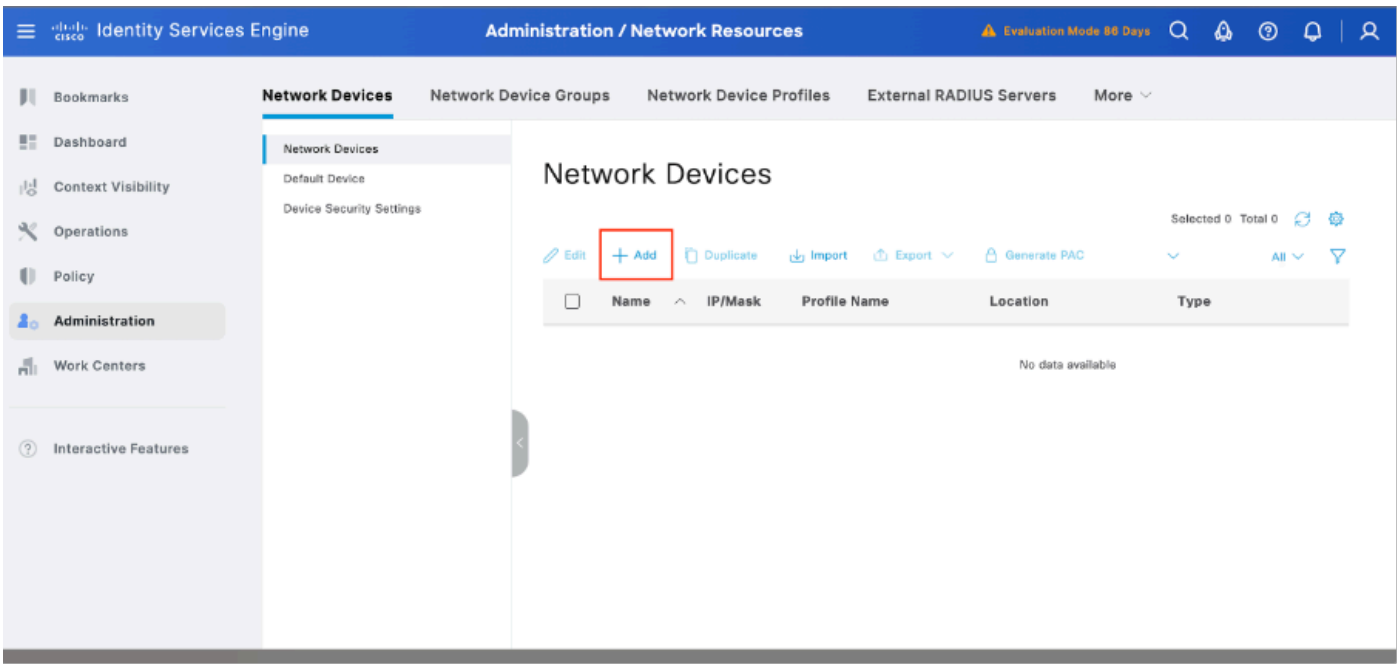


上传完成后，导航到Edit选项并启用TACACS+作为受支持的协议。



步骤 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:

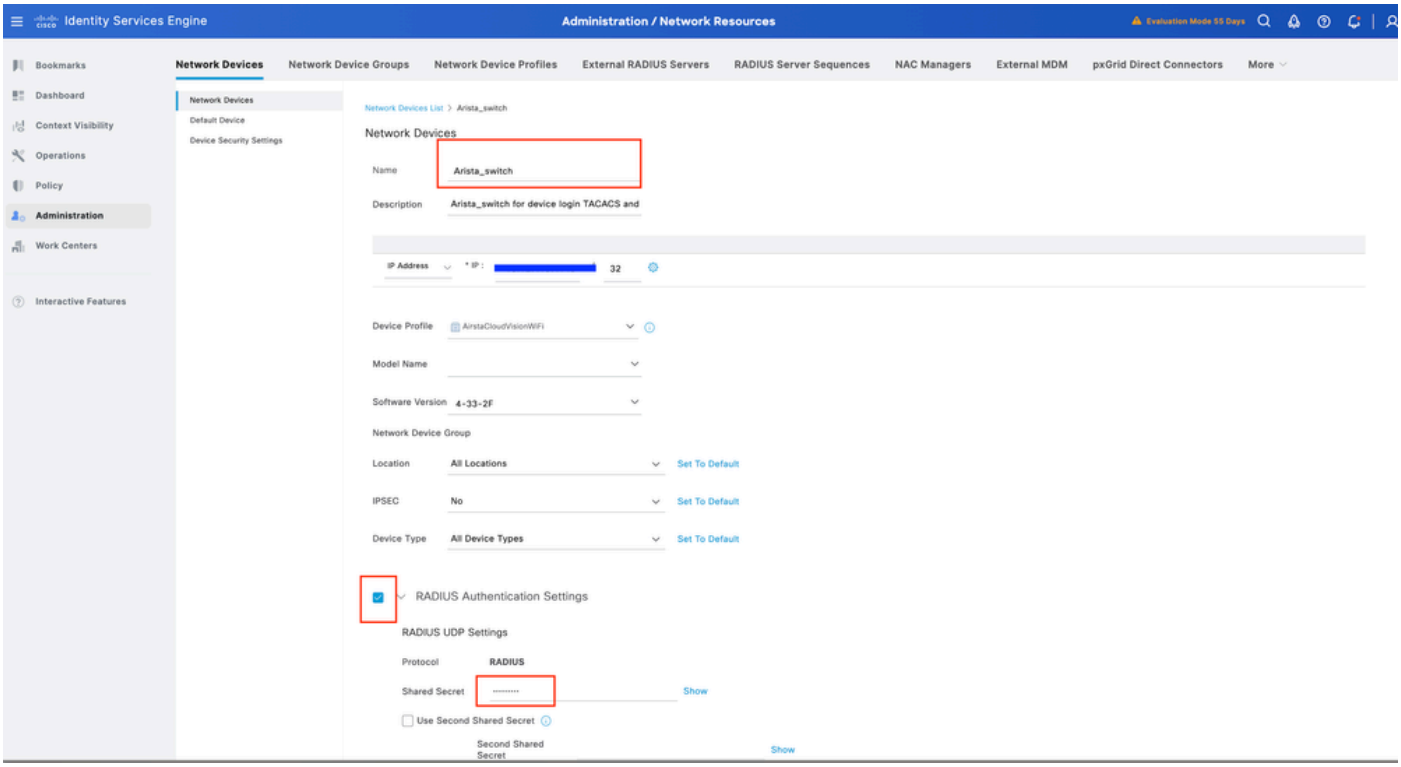


2.单击Add并输入以下详细信息：

- IP Address:<Switch-IP>
- 设备类型：选择其他有线
- 网络设备配置文件:选择AirstaCloudVisionWiFi。

- RADIUS身份验证设置:
  - 启用RADIUS身份验证。
  - 输入Shared Secret（必须与交换机配置匹配）。

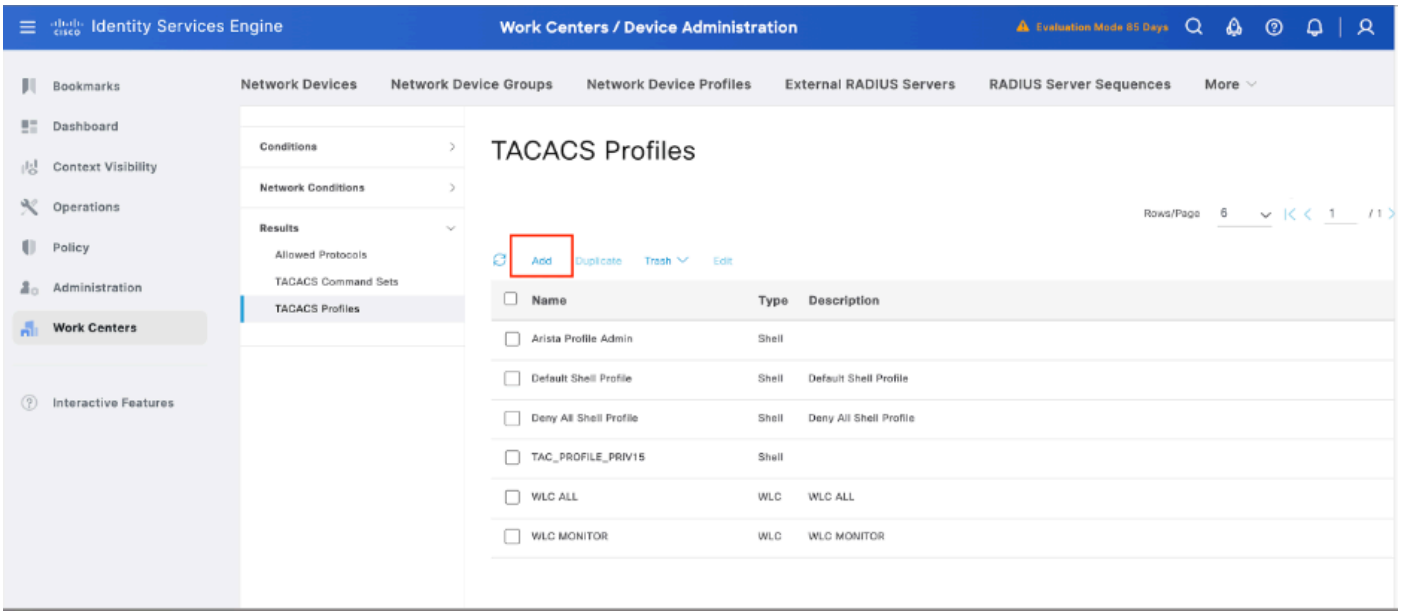
3.单击Save:



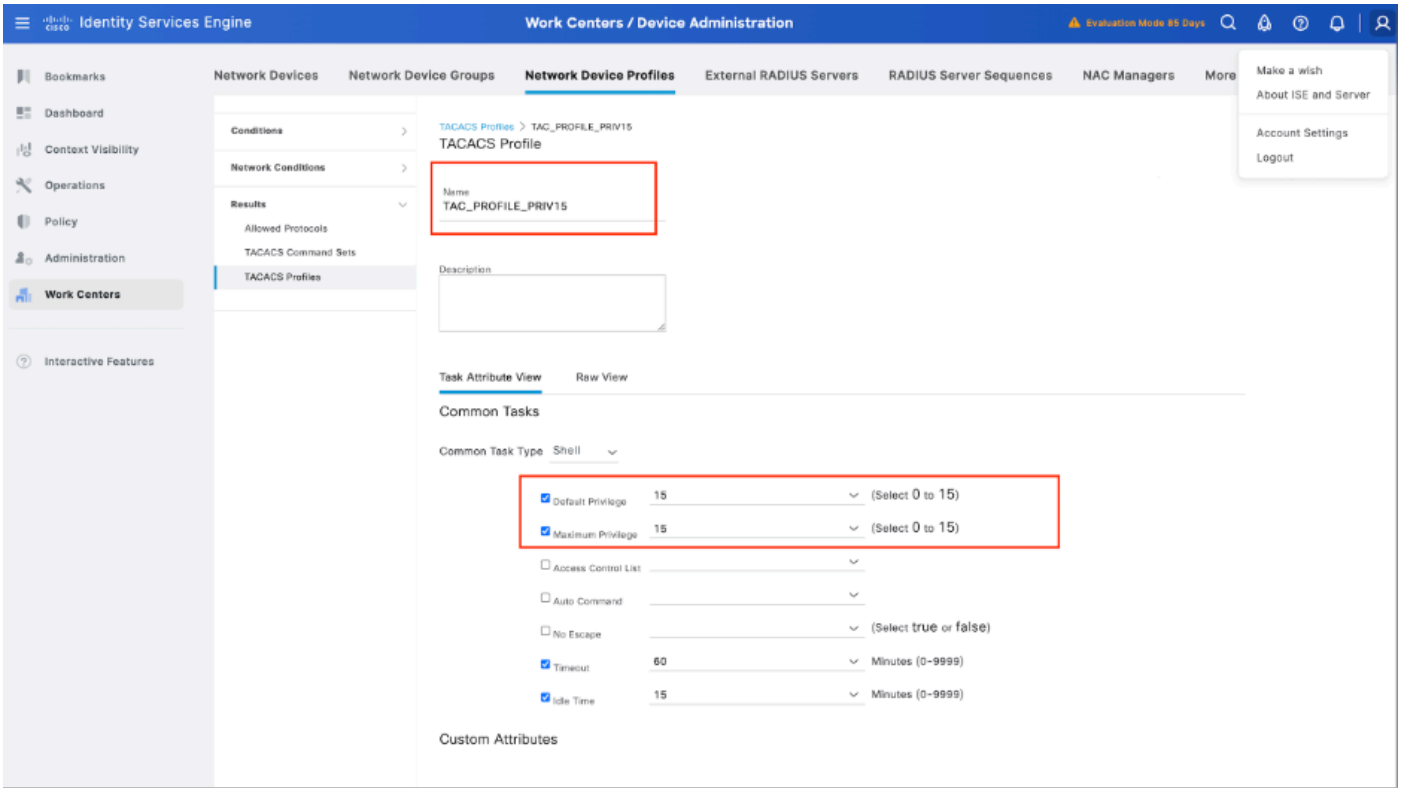
步骤3.在Network Devices:

步骤4.配置TACACS配置文件。

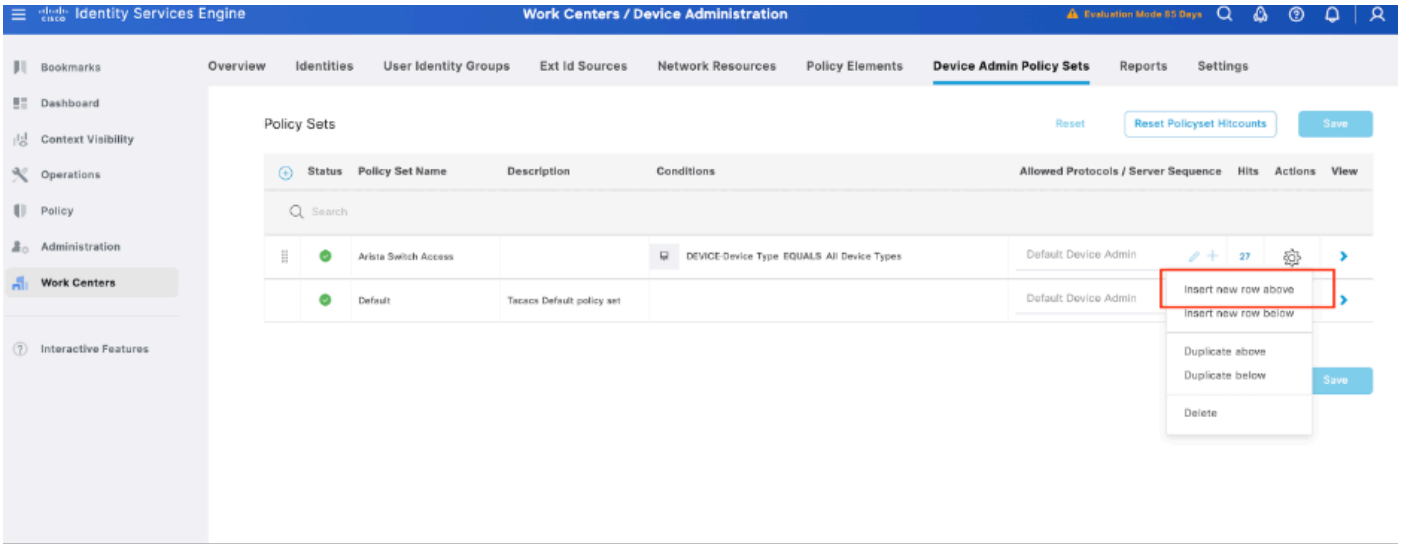
创建TACACS配置文件，导航到菜单Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles，然后选择Add:



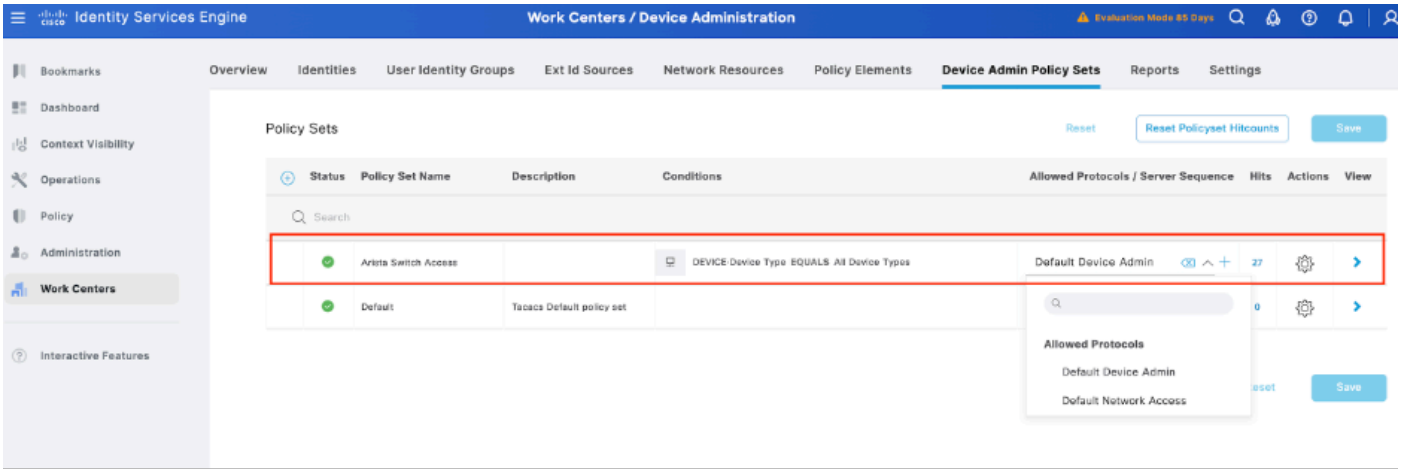
输入名称，选中Default Privilege复选框，并将值设置为15。此外，选择Maximum Privilege，将其值设置为15，然后单击Submit:



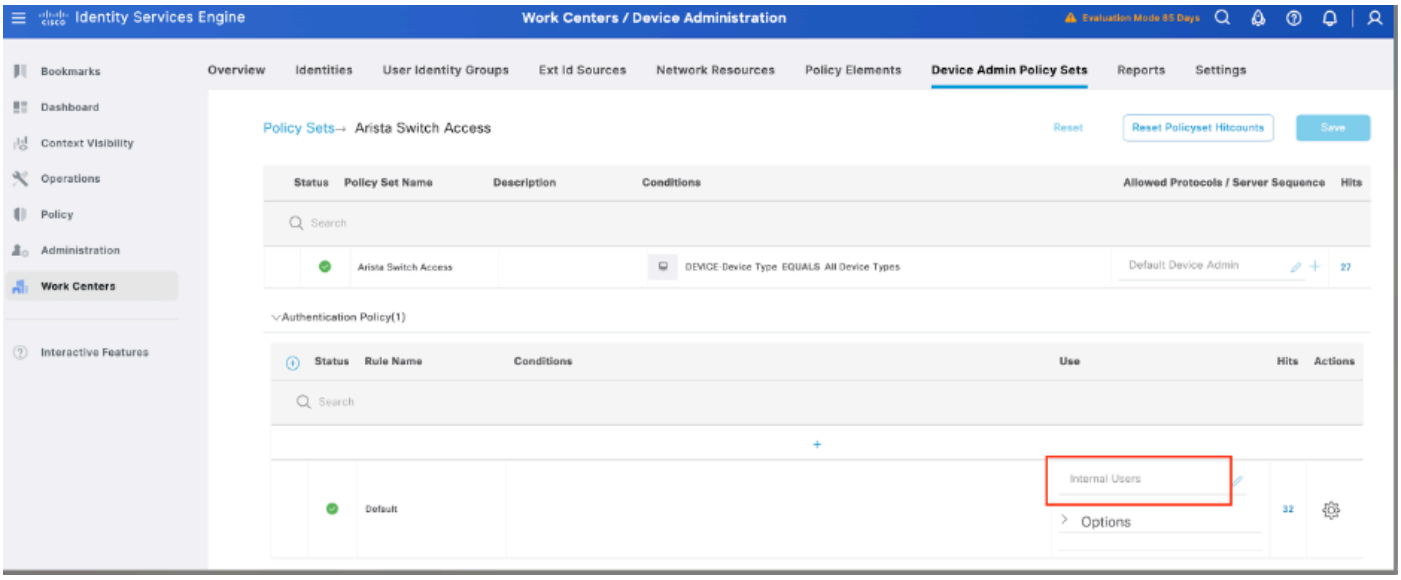
第5步：创建用于Arista交换机的设备管理策略集，导航到菜单Work Centers > Device Administration > Device Admin Policy Sets，然后从现有策略集中选择齿轮图标，然后选择上面的Insert new row。



第6步：命名此新的策略集，根据Arista交换机正在进行中的TACACS+身份验证的特征添加条件，并选择Allowed Protocols > Default Device Admin，保存配置。



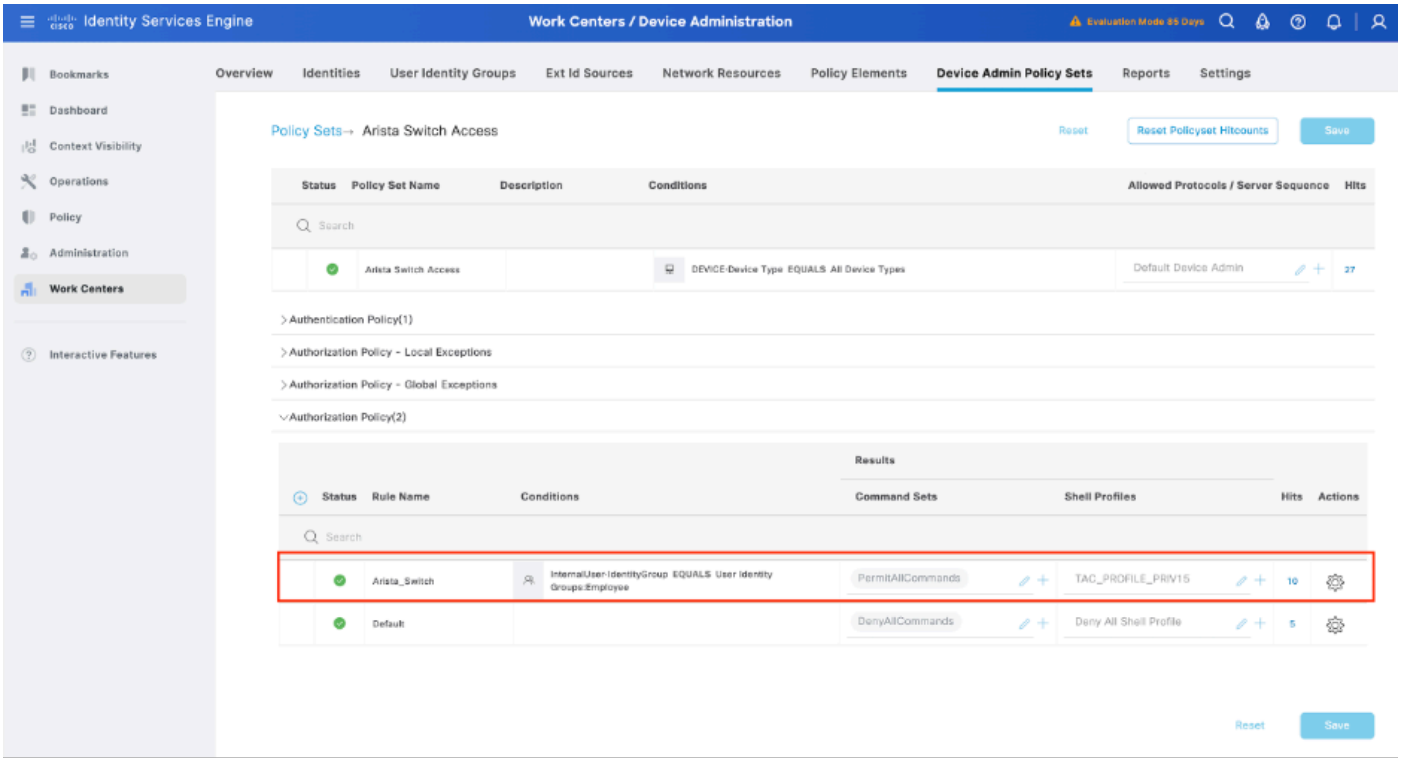
第7步：在 > view选项中选择，然后在身份验证策略部分中，选择Cisco ISE用于在Arista交换机上查询身份验证的用户名和凭据的外部身份源。在本示例中，凭证对应于ISE中存储的内部用户。



步骤8.向下滚动至名为Authorization Policy到Default policy的部分，选择齿轮图标，然后在上面插

入一个规则。

第9步：命名新的授权规则，添加与已通过身份验证的用户有关的条件作为组成员身份，并在外壳配置文件部分添加您之前配置的TACACS配置文件，保存配置。



配置Arista交换机

步骤1.启用TACACS+身份验证

登录到Arista交换机并进入配置模式：

配置

!

tacacs-server host <ISE-IP> key <TACACS-SECRET>

!

aaa group server tacacs+ ISE_TACACS

服务器<ISE-IP>

!

aaa authentication login default group ISE_TACACS local

aaa authorization exec default group ISE_TACACS local

aaa accounting commands 15 default start-stop group ISE_TACACS

!

结束

步骤2.保存配置

要在重新启动后保留配置，请执行以下操作：

写入内存数量

或者

copy running-config startup-config

验证

ISE审核

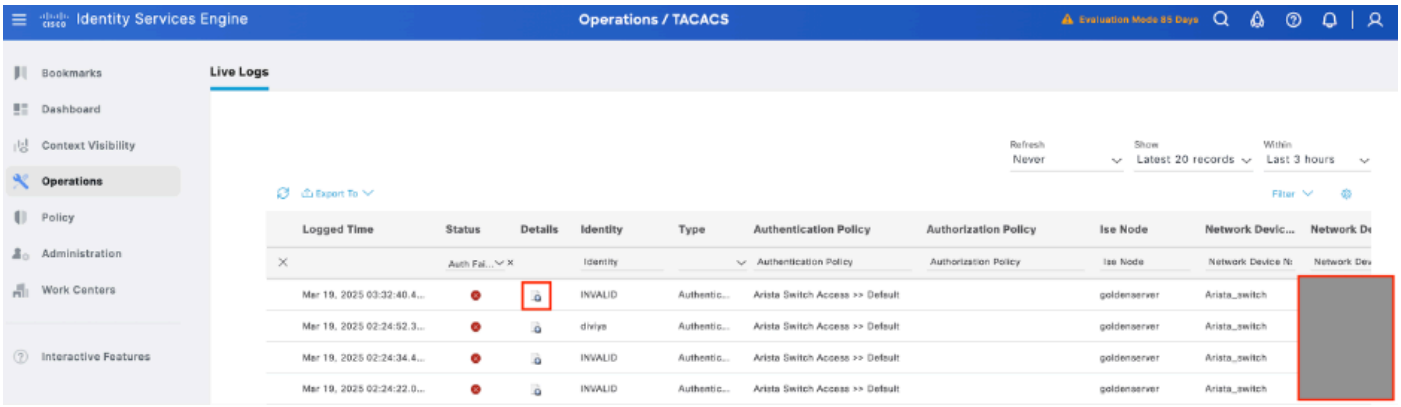
步骤1.检查TACACS+可维护性是否正在运行，可以将其检入：

- GUI:如果节点列在服务DEVICE ADMIN in > System > Deployment，请进行检查。
- CLI：运行命令show ports | include 49以确认TCP端口中存在属于TACACS+的连接

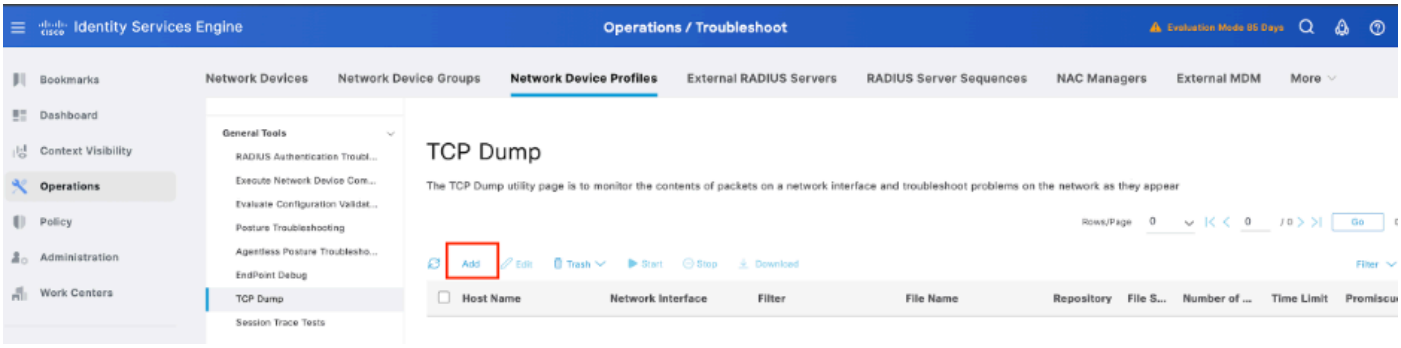
```
goldenserver/admin#show ports | include 49
tcp: [redacted]
```

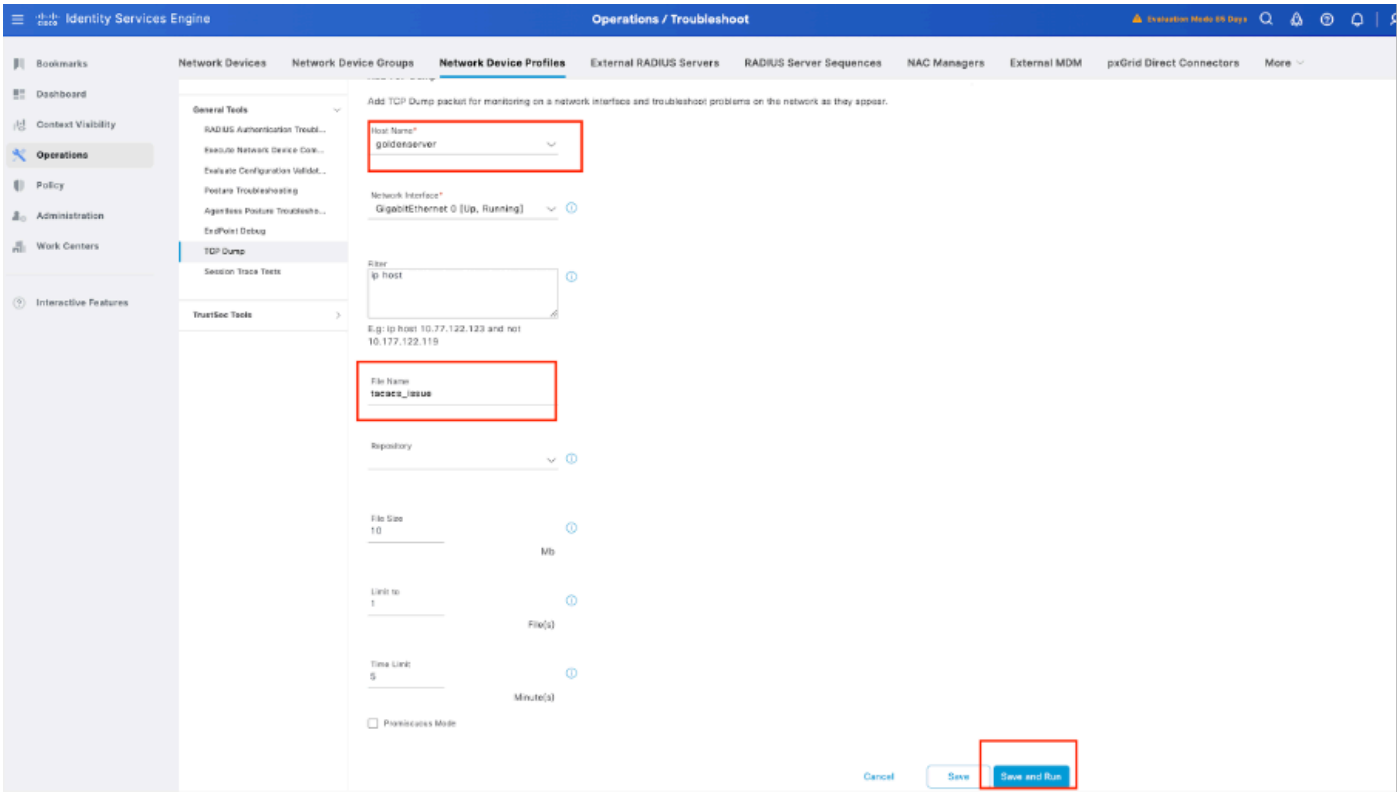
步骤2.确认是否存在有关TACACS+身份验证尝试的实时日志：可以在Operations > TACACS > Live logs菜单中进行检查。

根据故障原因，您可以调整配置或解决故障原因。

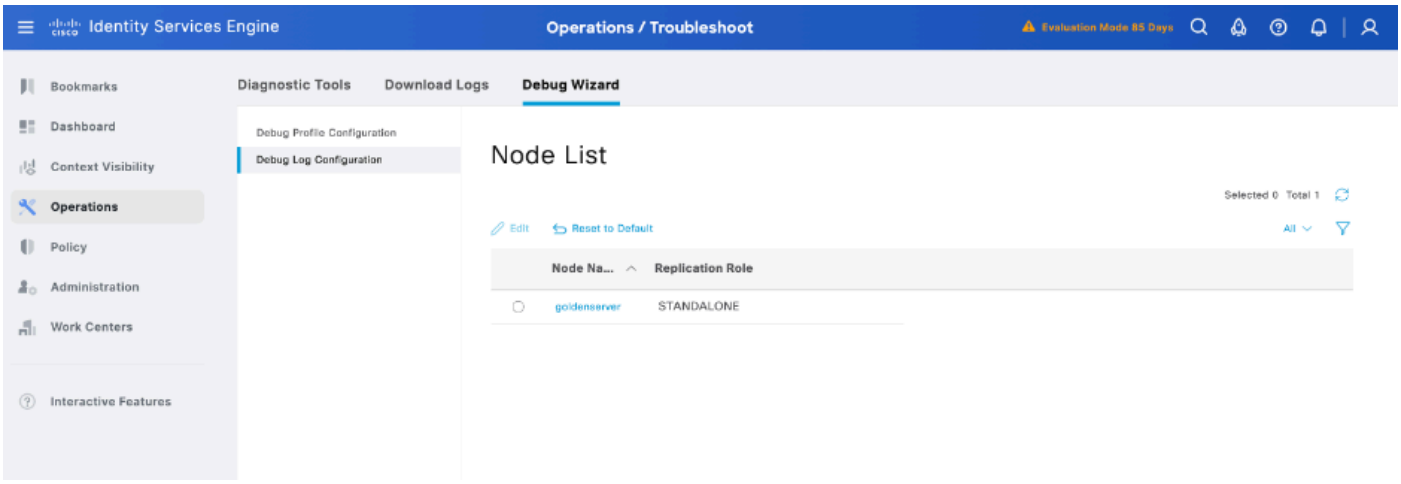


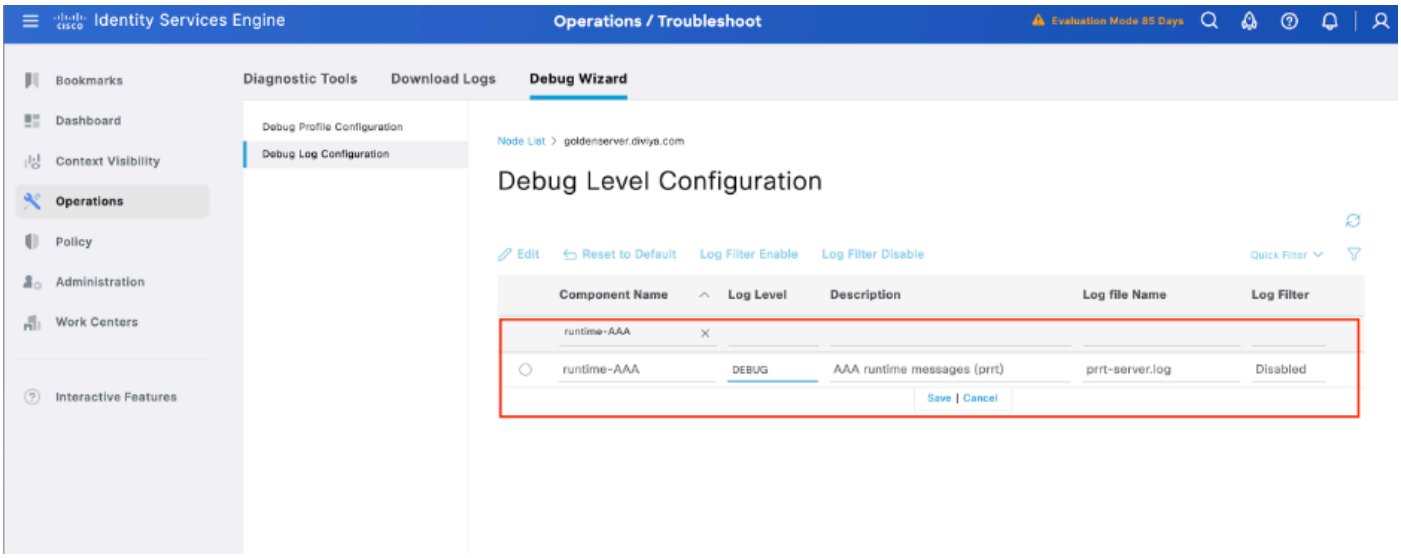
步骤3.如果您看不到任何实时日志，则继续捕获数据包。导航到菜单Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump，选择Add:





第4步：在操作>故障排除>调试向导>调试日志配置中执行身份验证的PSN内的调试中启用组件runtime-AAA，选择PSN节点，然后选择编辑按钮：





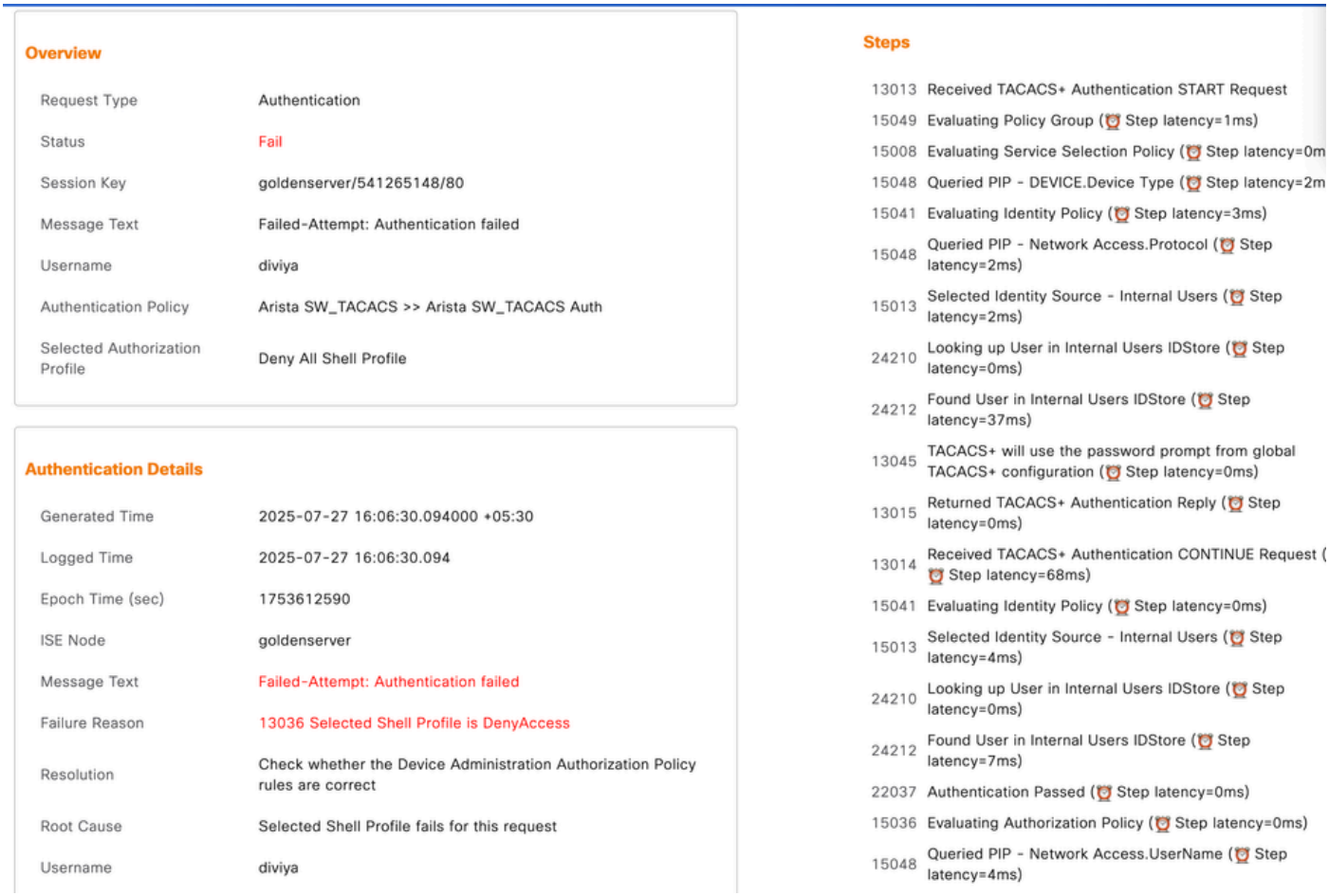
确定运行时AAA组件，将其日志记录级别设置为debug，重现问题，并分析日志以进一步进行调查。

故障排除

问题 1

思科ISE和Arista交换机（或任何网络设备）之间的TACACS+身份验证失败，并显示以下错误消息：

"所13036外壳配置文件为DenyAccess"



思科ISE中的错误“13036 Selected Shell Profile is DenyAccess”通常意味着在TACACS+设备管理尝试期间，授权策略与设置为DenyAccess的外壳配置文件匹配。这通常不是外壳配置文件本身配置错误的结果，而是表明配置的授权规则均未与传入的用户属性（如组成员身份、设备类型或位置）匹配。 因此，ISE会退回到默认规则或显式拒绝规则，导致访问被拒绝。

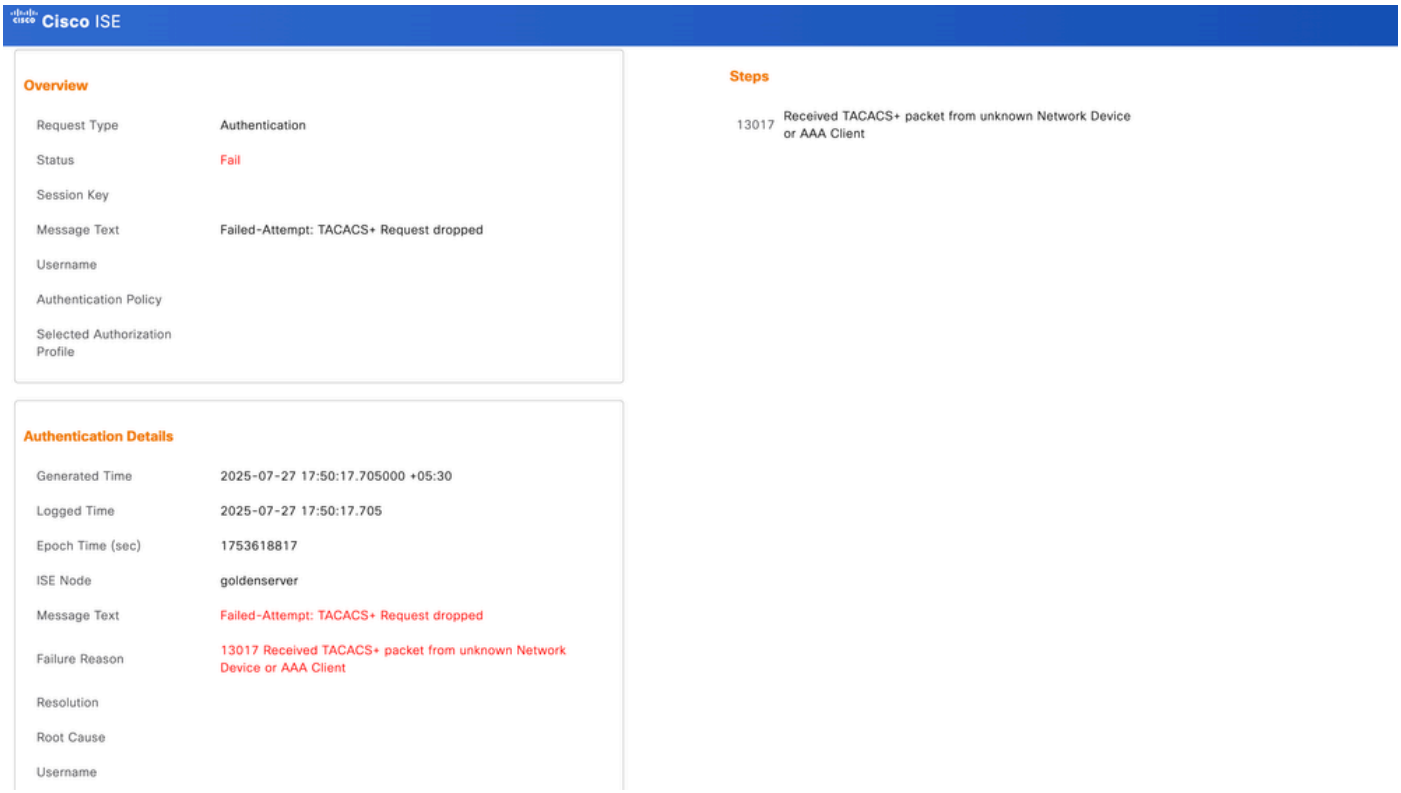
可能的原因

- 检查ISE中的授权策略规则。确认用户或设备与分配预期外壳配置文件的正确规则（例如允许适当访问的规则）匹配。
- 确保AD或内部用户组映射正确并且策略条件（如用户组成员资格、设备类型和协议）被准确指定。
- 使用ISE实时日志和失败尝试的详细信息，确切了解匹配的规则及其原因。

问题 2

思科ISE和Arista交换机（或任何网络设备）之间的TACACS+身份验证失败，并显示以下错误消息：

"已13017未知网络设备或AAA客户端收到TACACS+数据包"



可能的原因

- 最常见的原因是交换机的IP地址未添加为ISE中的网络设备（在Administration > Network Resources > Network Devices下）。
- 确保IP地址或范围与Arista交换机用于发送TACACS+数据包的源IP完全匹配。
- 如果您的交换机使用管理接口，请确认其确切的IP（不仅是子网/范围）已添加到ISE中。

解决方案

- 在ISE GUI中转至Administration > Network Resources > Network Devices。
- 验证Arista交换机上的确切源IP地址是否正用于TACACS+通信（通常为管理接口IP）。
- 指定共享密钥（必须与Arista交换机上的设置匹配）。

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）。