使用ISE服务器在CIMC上配置TACACS+身份验证

目录

简介

本文档介绍在思科集成管理控制器(CIMC)上配置终端访问控制器访问控制系统Plus(TACACS+)身份验证。

TACACS+通常用于使用中央服务器对网络设备进行身份验证。自版本4.1(3b)以来，思科IMC支持TACACS+身份验证。CIMC上的TACACS+支持可简化对设备具有访问权限的多个用户帐户的管理工作。此功能有助于定期更改用户凭证和远程管理用户帐户。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科集成管理控制器(CIMC)
- 增强型终端访问控制器访问控制系统(TACACS+)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- UCSC-C220-M4S
- CIMC版本：4.1(3b)
- 思科身份服务引擎(ISE)版本3.0.0.458

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。

配置

TACACS+服务器端权限关联配置

根据为该用户配置的**cisco-av-pair值**计算用户的权限级别。需**要在TACACS+服**务器上为创建cisco-av-pair，并且用户不能使用任何默认的TACACS+属性。cisco-av-pair属性支持如下所示**的三个语**法

对于管**理员**权限：

```
cisco-av-pair=shell:roles="admin"
```

对于用**户**权限：

```
cisco-av-pair=shell:roles="user"
```

对于**只读权**限：

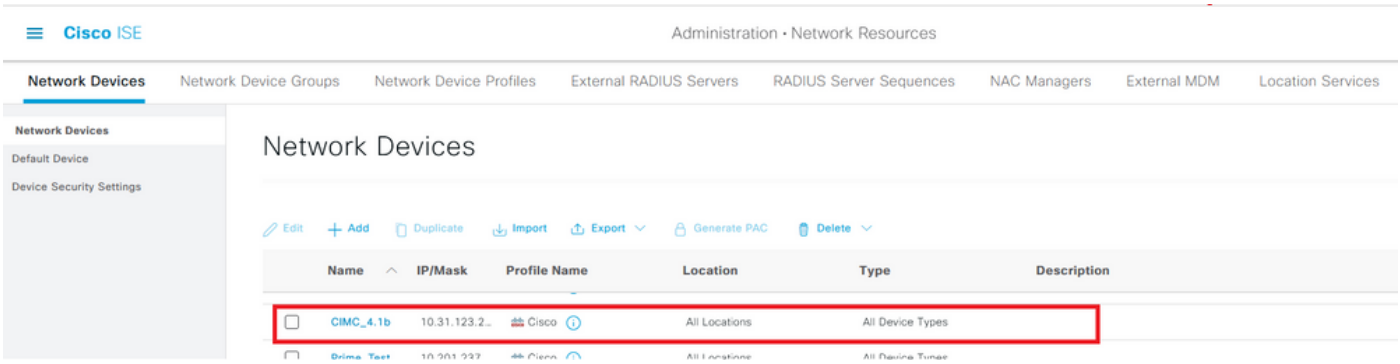
```
cisco-av-pair=shell:roles="read-only"
```

要支持其他设备，如果需要添加其他角色，则可以用逗号作为分隔符添加这些角色。例如，UCSM支持**aaa**，因此可**以配置shell:roles="admin，aaa"**,CIMC接受此格式。

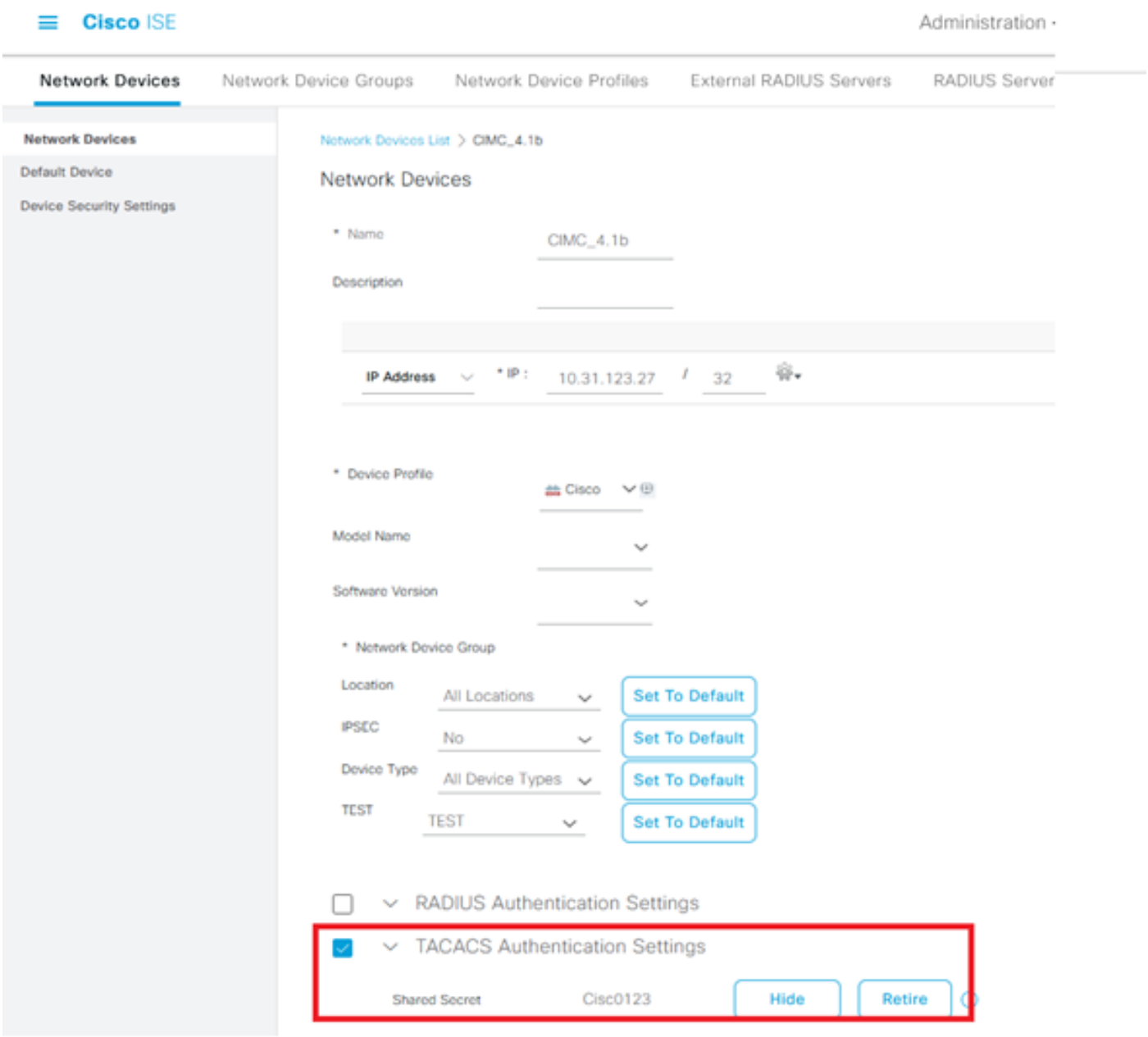
注意：如**果TACACS+服**务器上未配置cisco-av-pair，则具有该服务器的用**户具有只读**权限。

ISE配置要求

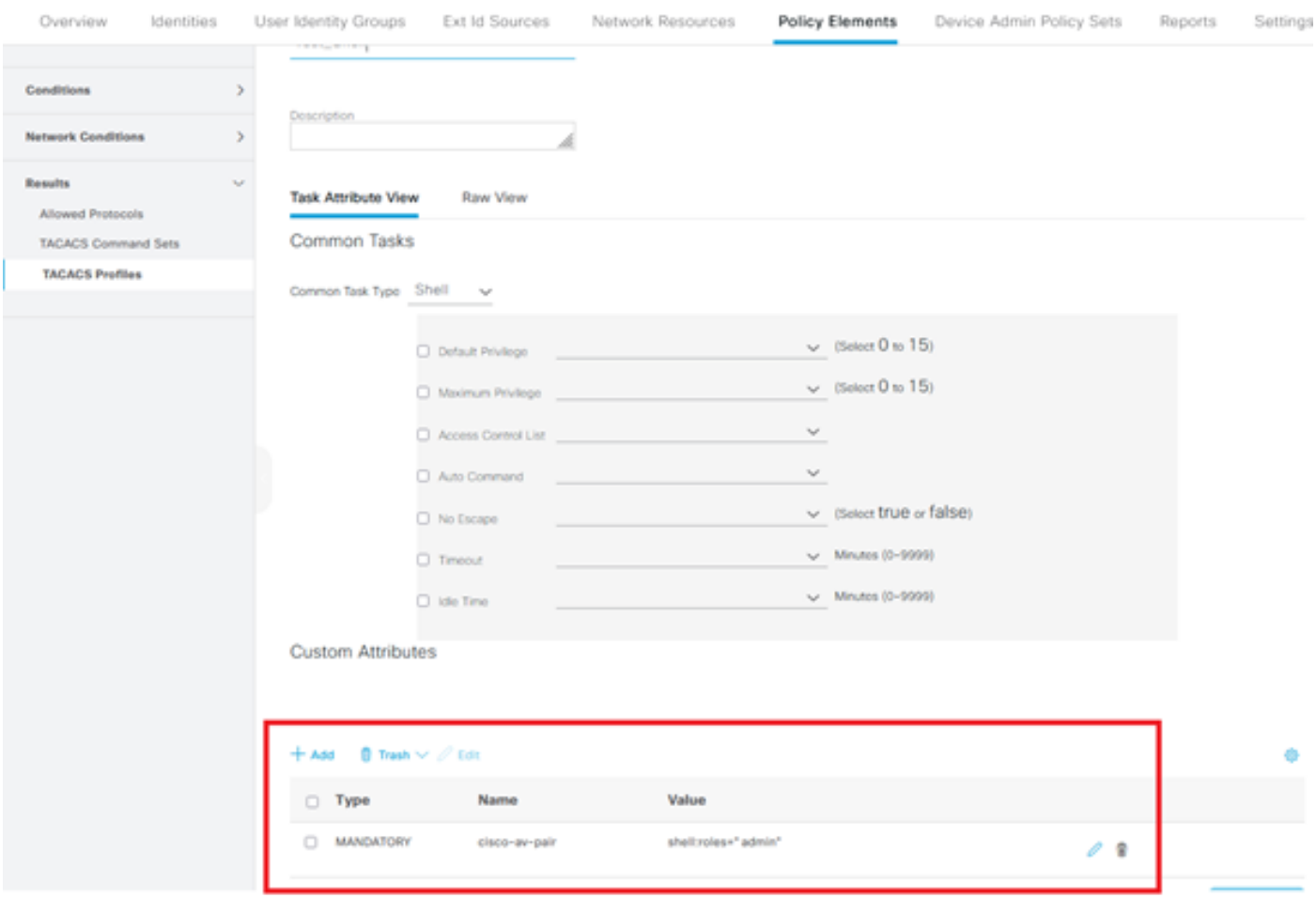
ISE网络设备上必须允许服务器的管理IP。



要在CIMC上输入的共享密钥密码。



具有管理员**权限的具有cisco-av-pair属**性的外壳配置文件。

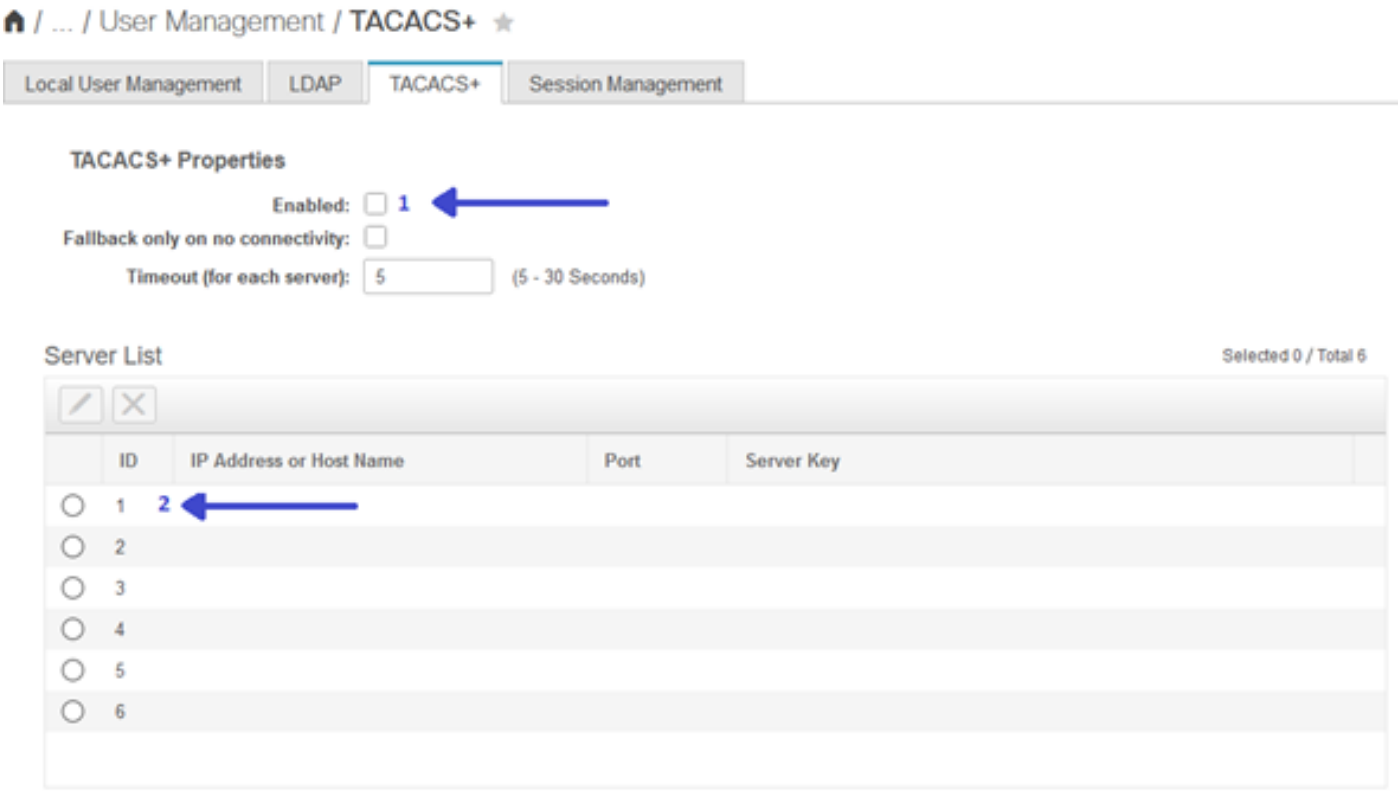


CIMC上的TACACS+配置

步骤1.导航至Admin > User Management > TACACS+

步骤2.选中复选框以启用TACACS+

步骤3.可以在表中指定的6行中的任一行添加新服务器。单击该行或选择该行，然后单击表顶部的编辑按钮，如下图所示。

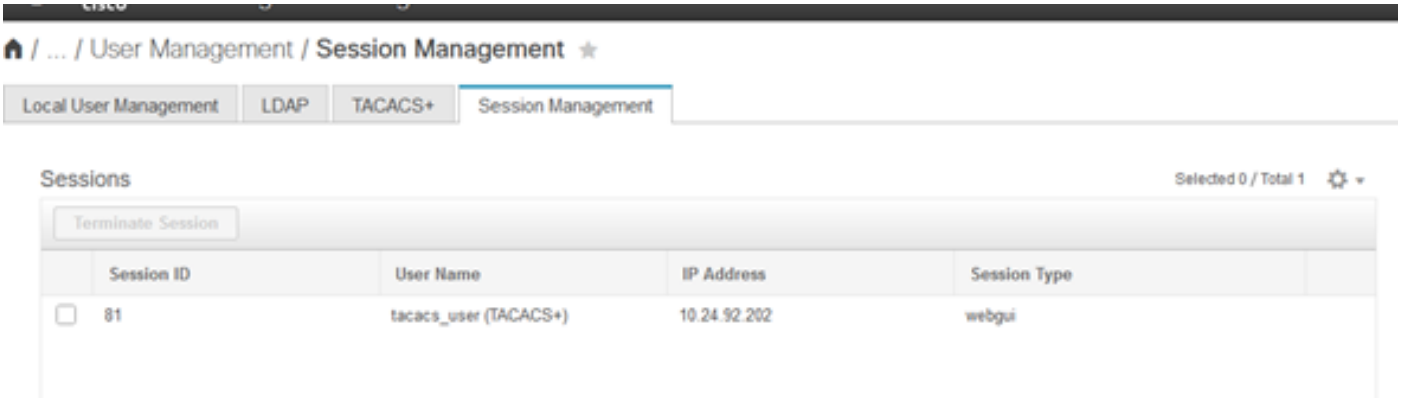


注意：如果用户已启用TACACS+回退而无连接选项，CIMC强制必须始终将第一个身份验证优先级设置为TACACS+，否则回退配置可能变得无关。

步骤4.填写IP地址或主机名、端口和服务器密钥/共享密钥并**保存**配置。

Cisco IMC最多支持六台TACACS+远程服务器。用户成功通过身份验证后，用户名将附加(TACACS+)。

这也显示在会话管理中



验证

- 在CIMC上最多可配置6台TACACS+服务器。
- 与服务器关联的密钥最长可包含64个字符。
- 超时可以配置为5到30秒（计算为与LDAP一致的最大180秒）。
- 如果TACACS+服务器需要使用服务名来创建**cisco-av-pair**，则用户需要使用**Log in** 作为服务名。
- 不支持修改配置。

从CIMC中的CLI验证配置

- 验证TACACS+是否已启用。

```
C220-WZP22460WCD# scope tacacs+
C220-WZP22460WCD /tacacs+ # show detail
TACACS+ Settings:
Enabled: yes
Fallback only on no connectivity: no
Timeout(for each server): 5
```

- 验证每台服务器的配置详细信息。

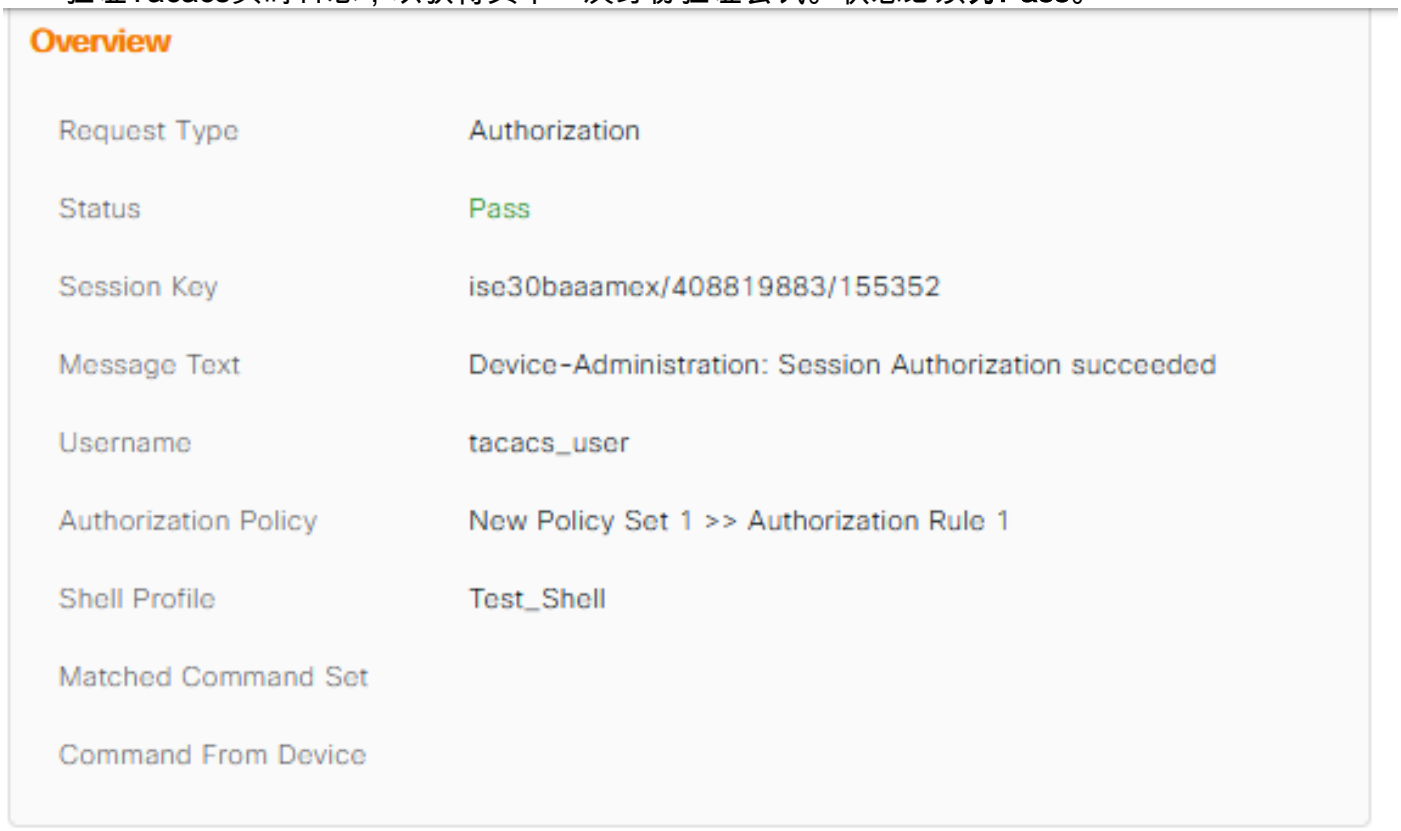
```
C220-WZP22460WCD /tacacs+ # scope tacacs-server 1
C220-WZP22460WCD /tacacs+/tacacs-server # show detail
Server Id 1:
Server IP address/Hostname: 10.31.126.220
Server Key: ******
Server Port: 49
```

故障排除

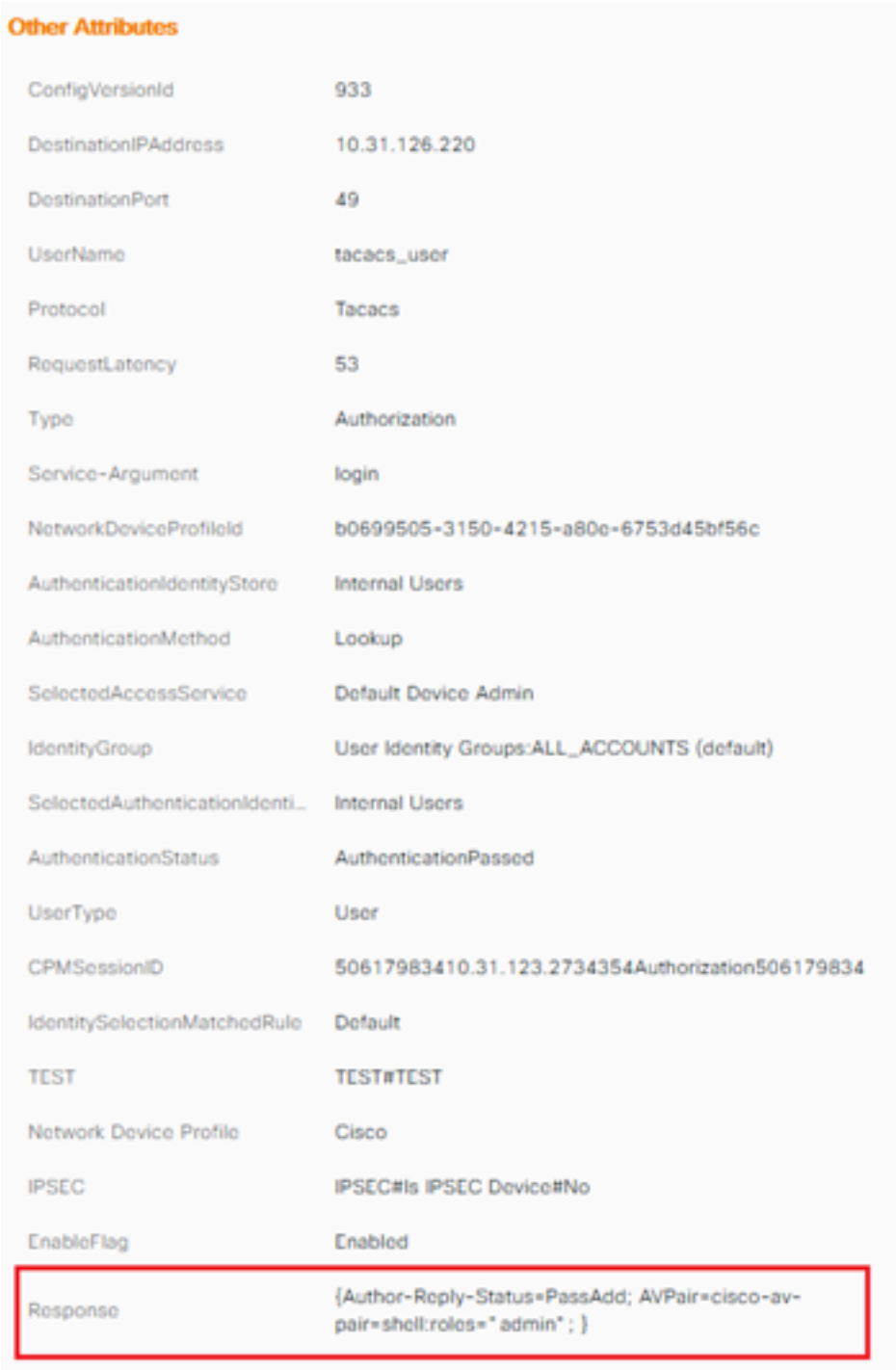
- 确保TACACS+服务器IP可从CIMC访问，并且端口配置正确。
- 确保在**TACACS+服务器**上正确配置了cisco-av-pair。
- 检查TACACS+服务器是否可达（IP和端口）。
- 确保密钥或凭证与TACACS+服务器上配置的密钥或凭证匹配。
- 如果您可以使用TACACS+登录，但只具**有只读权**限，请验证cisco-av-pair在TACACS+服务器上是否具有正确的语法。

ISE故障排除

- 验证Tacacs实时日志，以获得其中一次身份验证尝试。状态必须**为Pass**。



- 验证响应是否配置**了正确的cisco-av**-pair属性。



相关信息

- [TACACS+身份验证Cisco UCS-C]
- [技术支持和文档 - Cisco Systems]
- [配置ISE 2.0:基于AD组成员身份的IOS TACACS+身份验证和命令授权]