将ISE与Prime基础设施集成以实现终端可视性

目录

简介

本文档介绍如何将ISE与Prime基础设施集成，以获得经过身份验证的终端的可视性。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科ISE。
- Cisco Prime基础设施。
- 终端根据ISE进行身份验证的无线或有线AAA流。
- 交换机和WLC等NAD（网络接入设备）上的SNMP配置。

使用的组件

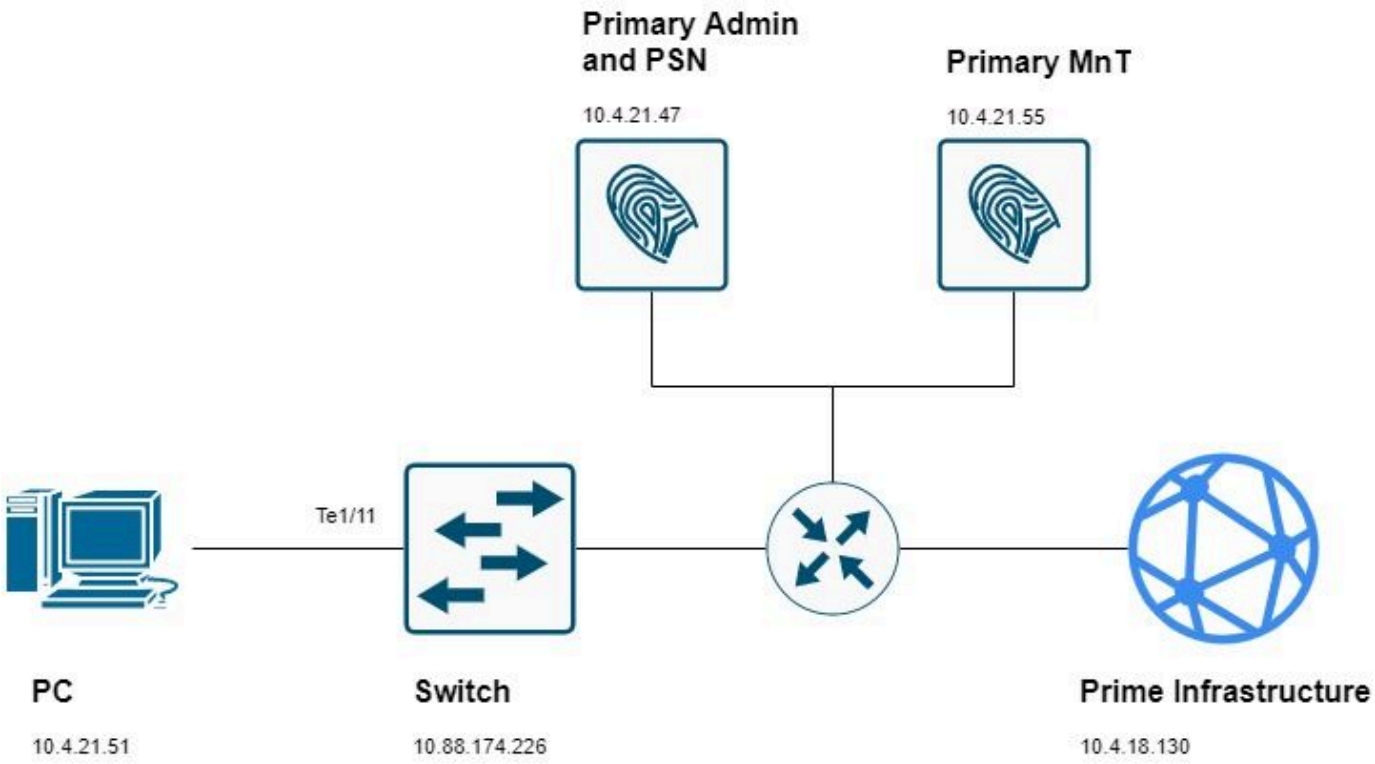
本文档中的信息基于以下软件和硬件版本：

- ISE 3.1部署。
- 思科Prime基础设施3.8。
- 运行Cisco IOS® 15.5的C6816-X-LE。
- Windows 10计算机。

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

网络图



配置

交换机配置

1.配置网络接入设备(NAD)以对ISE进行AAA身份验证。在本指南中，您将使用此配置：

```
aaa new-model

radius server ise31
 address ipv4 10.4.21.47 auth-port 1812 acct-port 1813
 key Cisc0123

aaa server radius dynamic-author
 client 10.4.21.47 server-key Cisc0123

aaa group server radius ISE
 server name ise31

aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa accounting dot1x default start-stop group ISE
```

```
dot1x system-auth-control
```

2.在交换机中配置Device Tracking:

```
device-tracking policy DT1
 tracking enable

device-tracking tracking auto-source
```

3.为dot1x身份验证配置switchport并将设备跟踪策略附加到该端口：

```
interface TenGigabitEthernet1/11
 device-tracking attach-policy DT1
 authentication host-mode multi-domain
 authentication order dot1x mab webauth
 authentication priority dot1x mab webauth
 authentication port-control auto
 mab
 dot1x pae authenticator
```

4.配置RO SNMP社区和SNMP陷阱以满足您的网络要求（或者，您可以配置RW社区）：

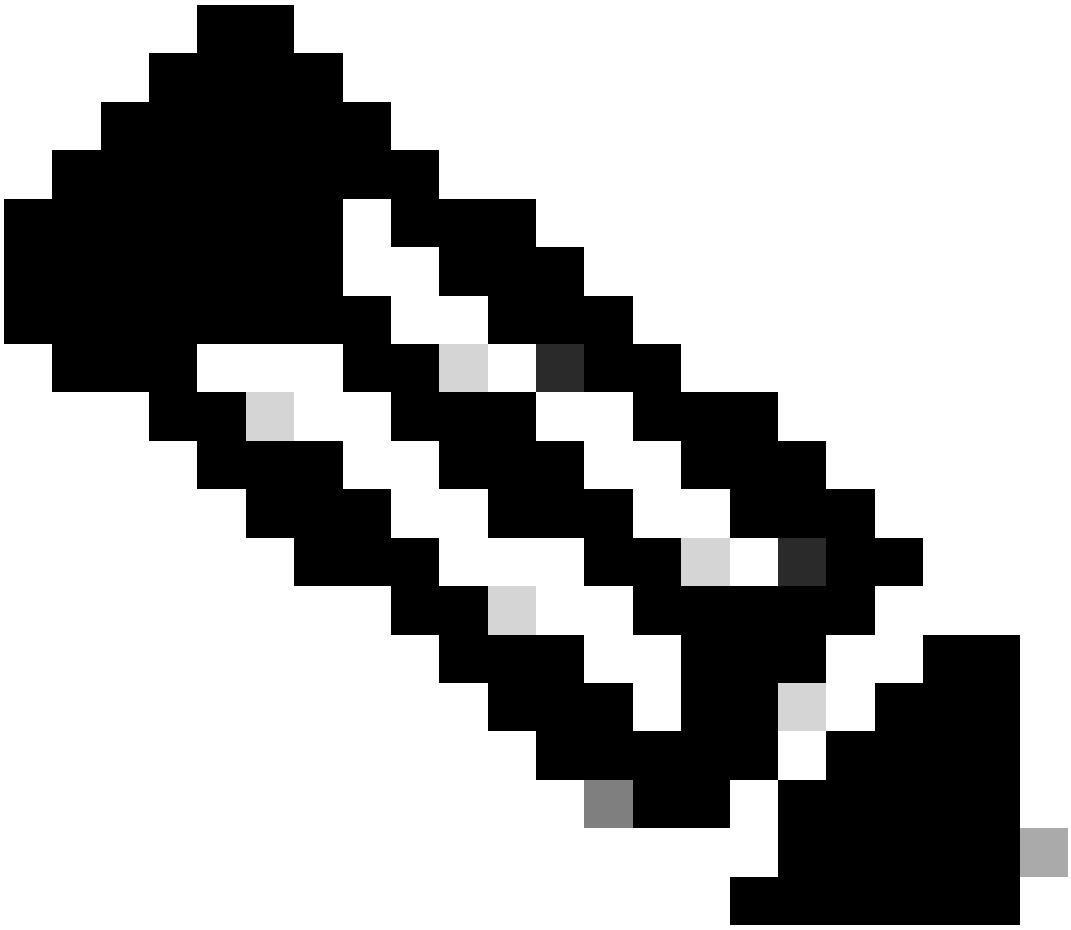
```
snmp-server community public RO
snmp-server community private RW
snmp-server trap-source TenGigabitEthernet1/16
snmp-server source-interface informs TenGigabitEthernet1/16
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps aaa_server
snmp-server enable traps trustsec authz-file-error
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps port-security
snmp-server enable traps event-manager
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold
snmp-server host 10.4.18.130 version 2c public udp-port 161
```

5.配置Telnet或SSH访问，以便Prime可以管理设备：

```
username admin password 0 cisco!123
aaa authentication login default local

line vty 0 4
 transport input ssh
 login authentication default
```

6.（可选）对于SSH连接，需要RSA密钥。如果NAD没有NAD，请使用以下步骤生成它。

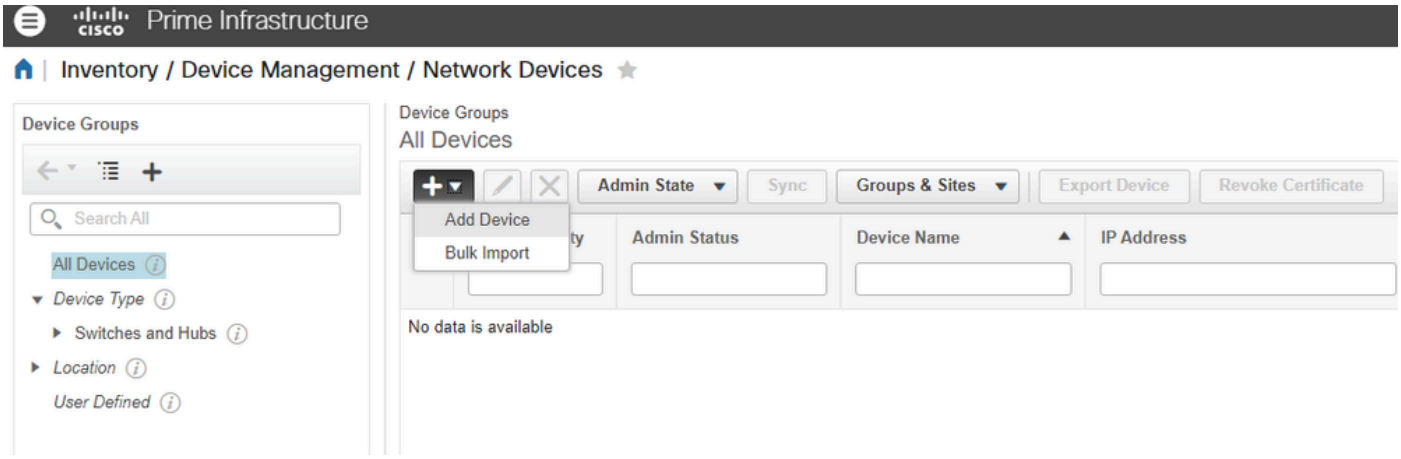


注意：某些设备在生成RSA之前需要已配置的域。检查您的设备是否配置了域，以便不覆盖现有域。

```
ip domain-name cisco.com
crypto key generate rsa
```

Cisco Prime基础设施配置

7.在资产>设备管理>网络设备>加号(+)>添加设备中添加网络设备：



要完成库存，必须填写以下字段：

对于有线设备：

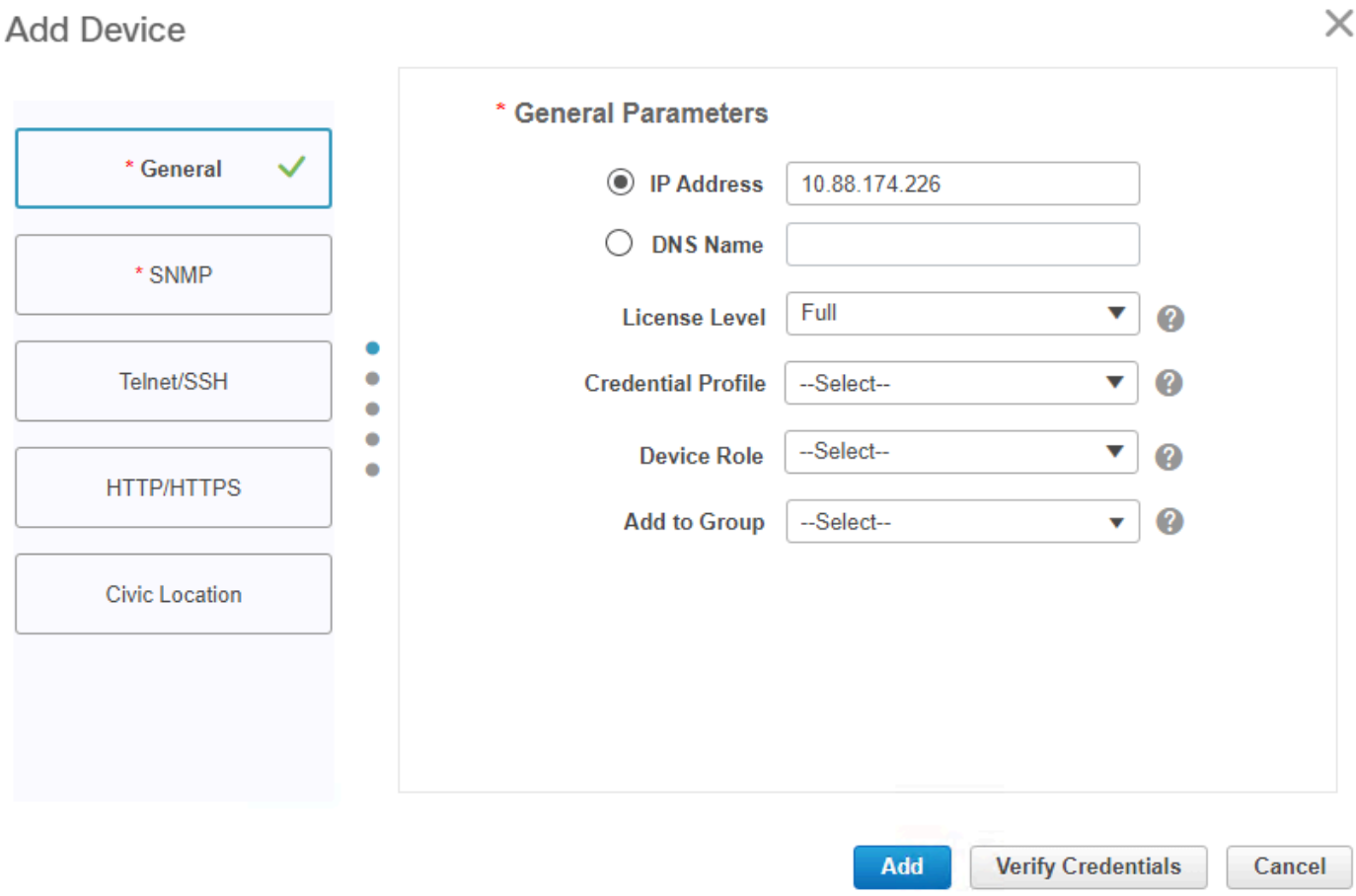
- 一般：IP或DNS。
- SNMP ：需要RO社区 — 确保也在交换机/WLC中对其进行配置。
- Telnet/SSH:执行模式和启用模式凭证。

对于WLC:

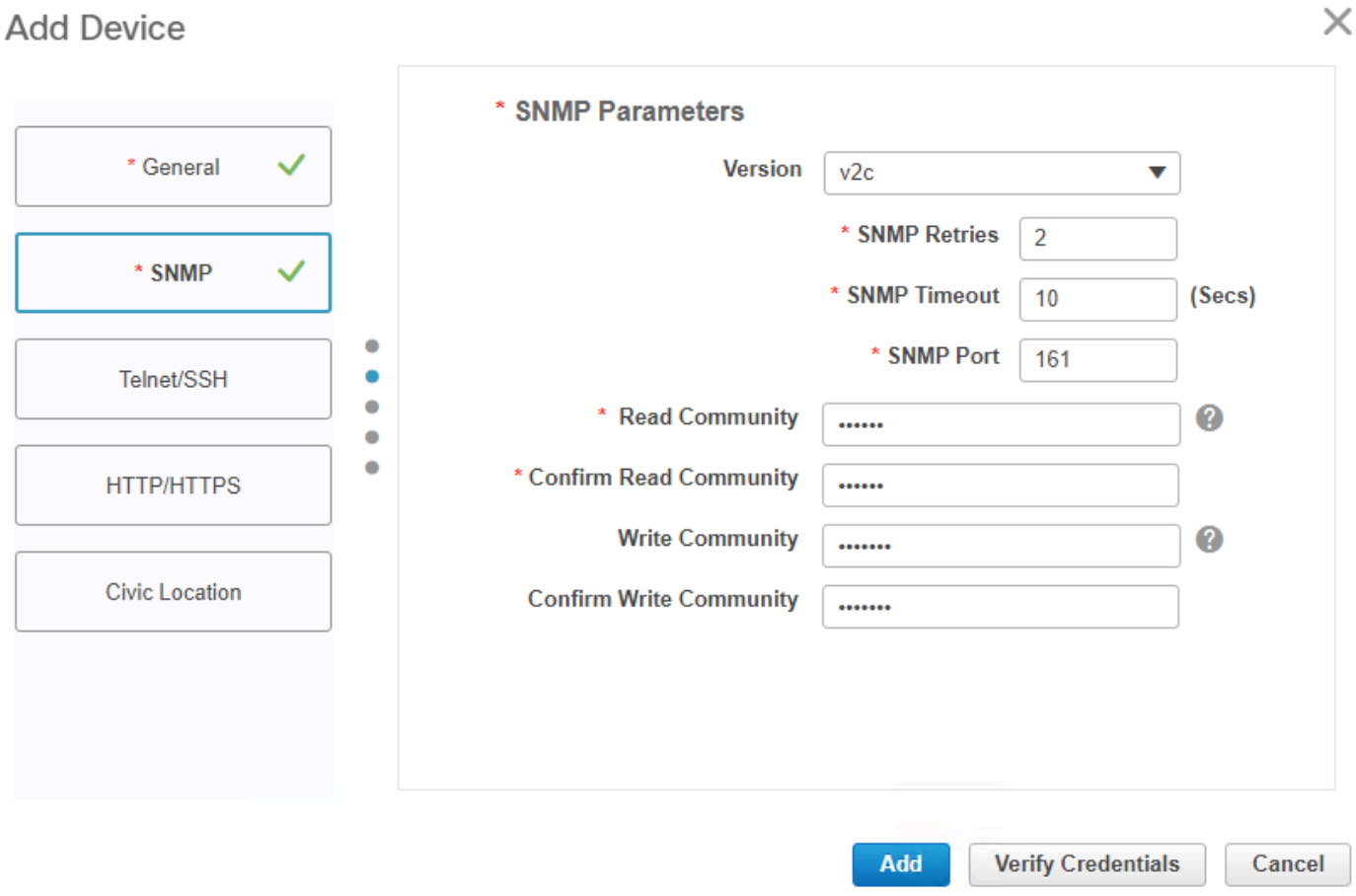
- 一般：IP或DNS。
- SNMP ：需要RO社区 — 确保也在交换机/WLC中对其进行配置。

在本指南中，您将使用Cisco交换机：

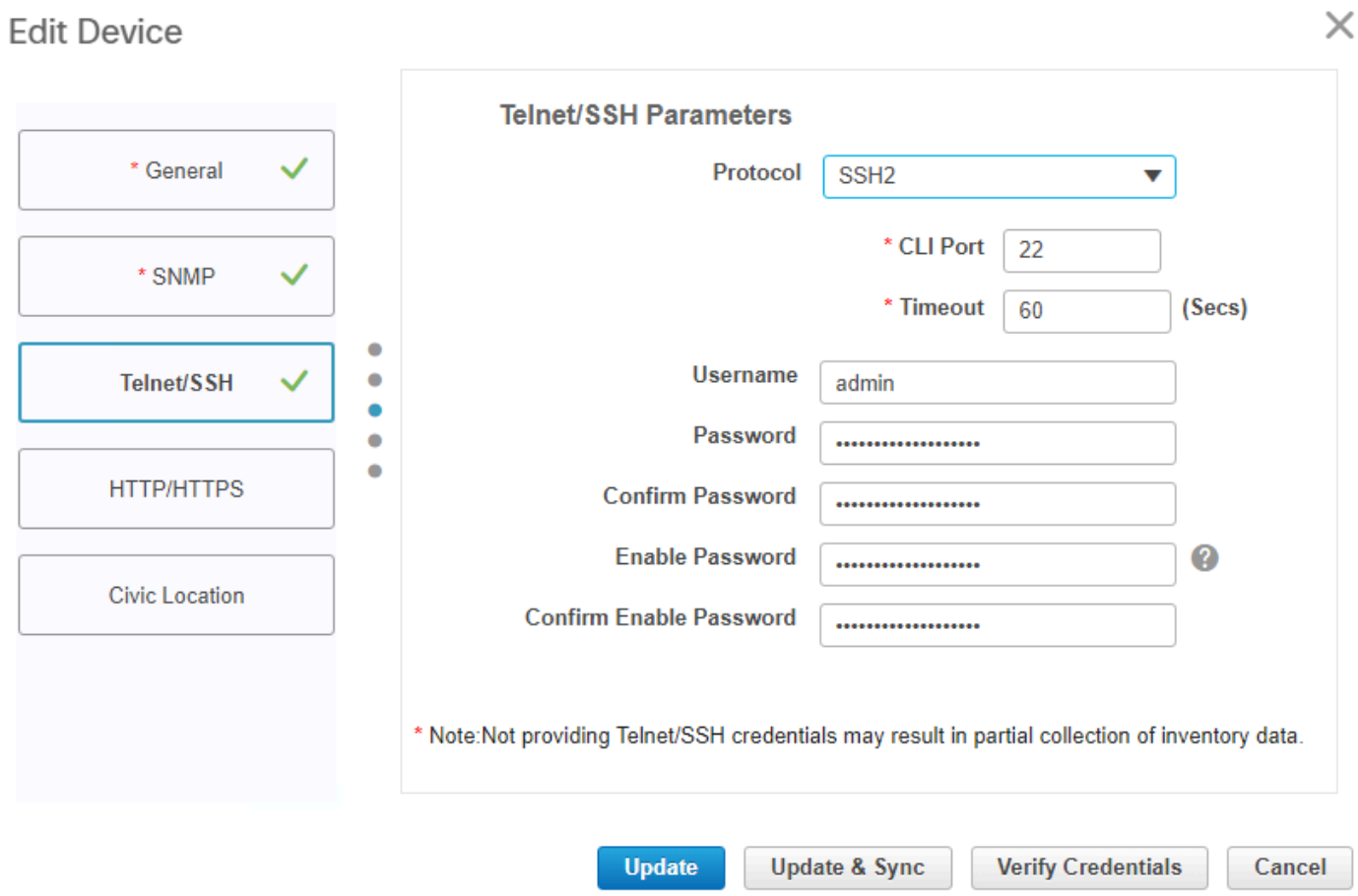
i.常规部分：


Add Device
* General
* SNMP
Telnet/SSH
HTTP/HTTPS
Civic Location
* General Parameters
IP Address
10.88.174.226
DNS Name
License Level
Full
Credential Profile
--Select--
Device Role
--Select--
Add to Group
--Select--
Add
Verify Credentials
Cancel

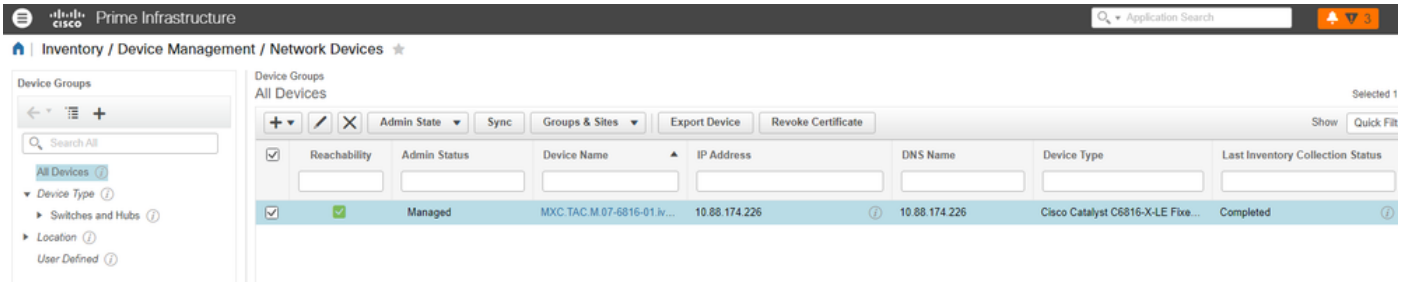
二、SNMP 部分:


Add Device
* General
* SNMP
Telnet/SSH
HTTP/HTTPS
Civic Location
* SNMP Parameters
Version
v2c
* SNMP Retries
2
* SNMP Timeout
10
(Secs)
* SNMP Port
161
* Read Community
* Confirm Read Community
Write Community
Confirm Write Community
Add
Verify Credentials
Cancel

三。Telnet/SSH部分：



8.完成所有必填字段后，确保Reachability和Collection Status分别为Green和Completed:

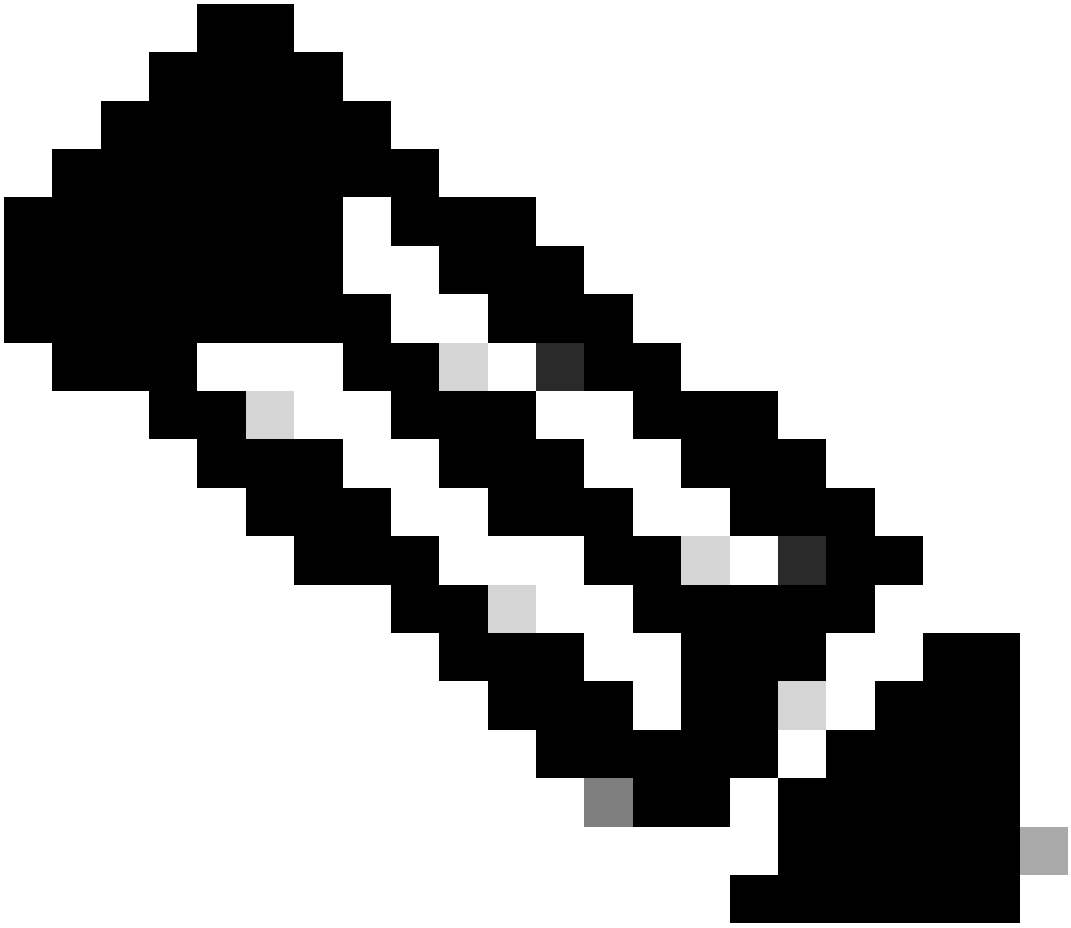


9.将Prime与ISE集成。

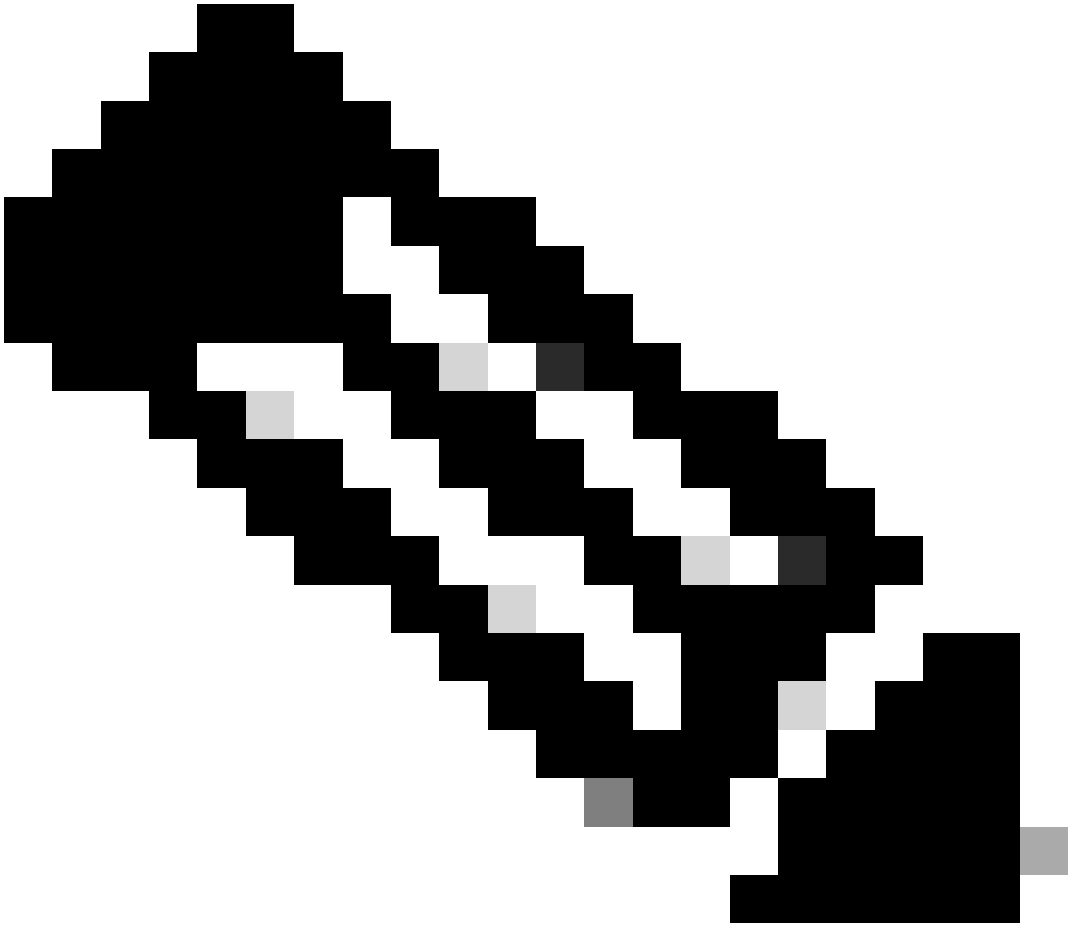
i.导航到Administration > Servers > ISE Servers。

二、在下拉菜单中，选择Add ISE Server，然后单击Go:

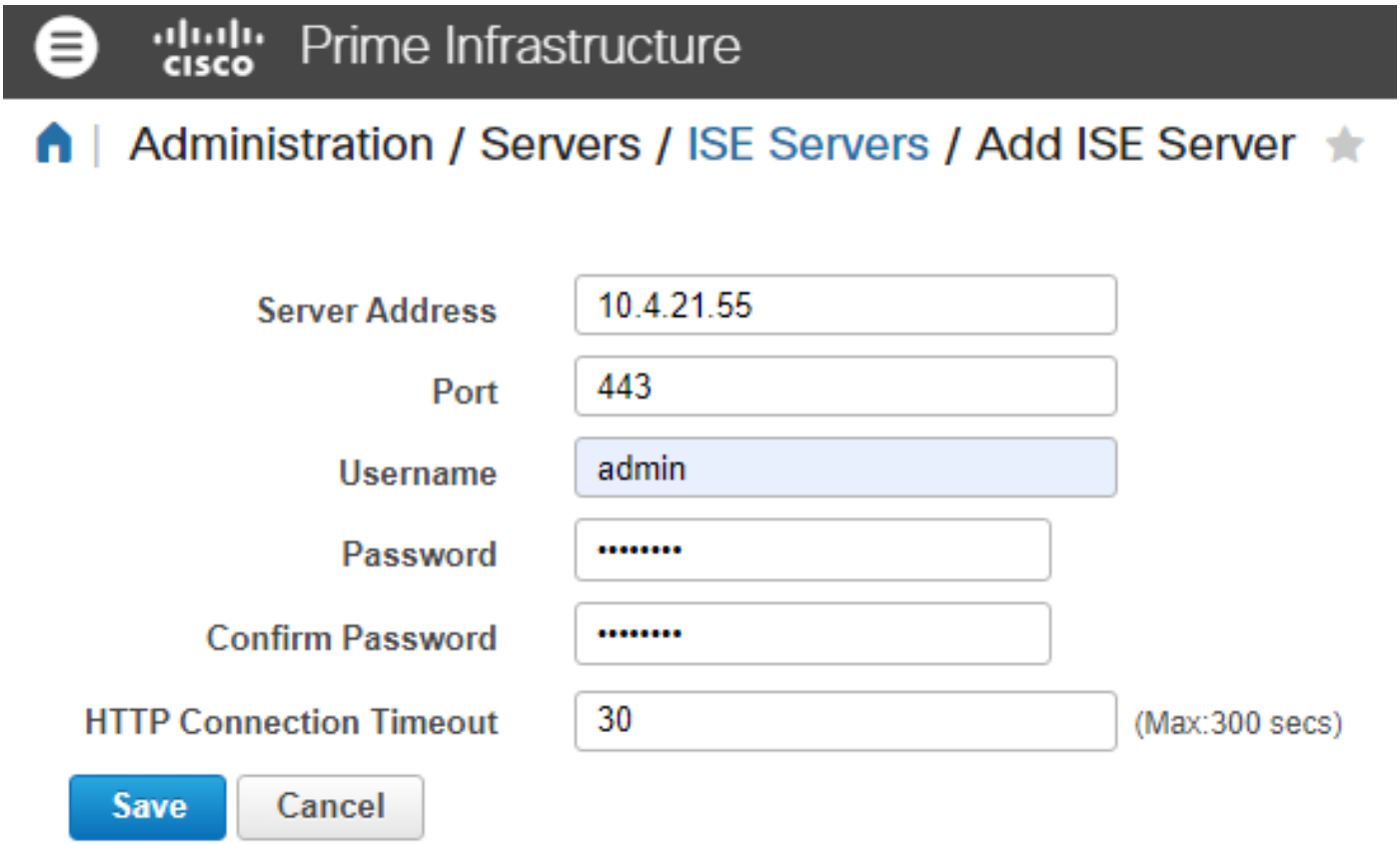
三。填写所有字段，然后单击Save。



注意：必须针对主要和辅助（如果适用）监控ISE节点建立连接。



注意：默认端口设置为443，但您可以使用ISE中的任何其他打开的端口建立连接。



四。导航回ISE服务器页面。服务器状态显示可访问且角色显示（独立、主[MnT]或辅助[MnT]）：

终端配置

10.终端必须配置为执行dot1x(RFC 3850)身份验证。这可以通过配置思科网络访问管理器(NAM)或利用操作系统本地请求方来实现。关于此配置，有很多指南，因此本指南中不包括这些步骤。

验证

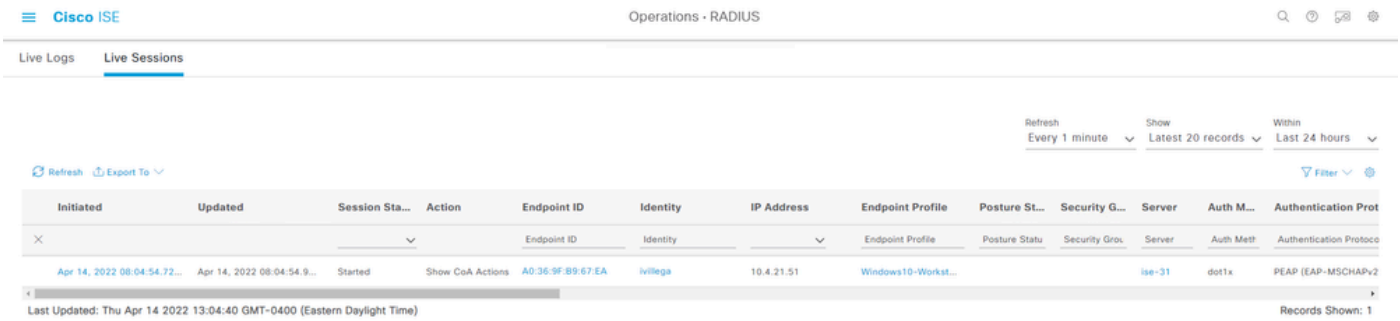
验证ISE

ISE收到来自NAD的RADIUS请求并成功对用户进行身份验证。

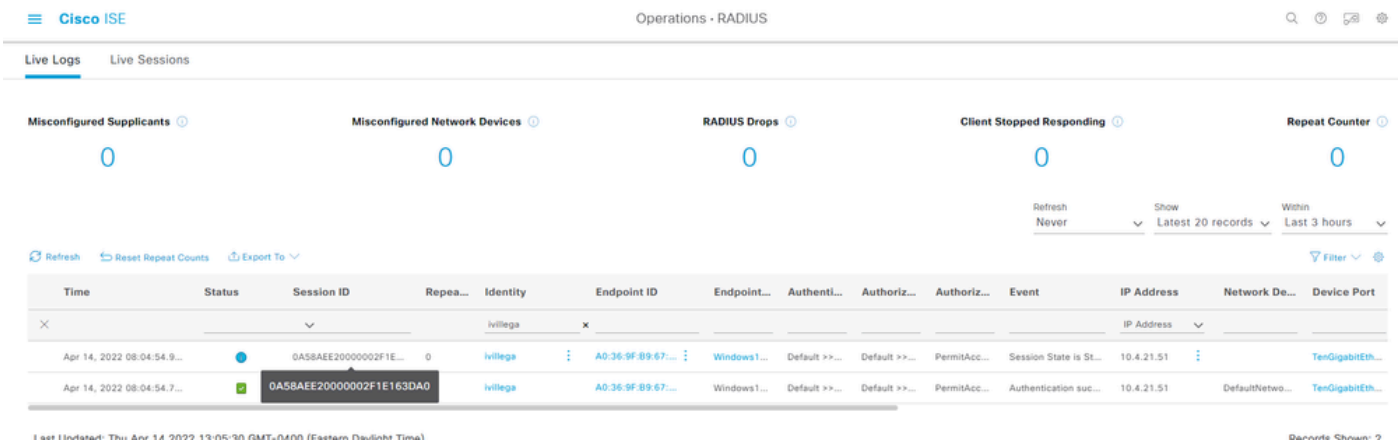
在ISE > Administration > Network Resources > Network Devices中添加并配置NAD。

1.导航到操作> RADIUS >实时会话。

确保用户实时会话已在此页面中列出。会话信息与Prime基础设施共享。



2. 在操作> RADIUS >实时日志中检查会话ID:



检验NAD

3.检查NAD中的会话详细信息。会话ID与ISE中的会话ID匹配：

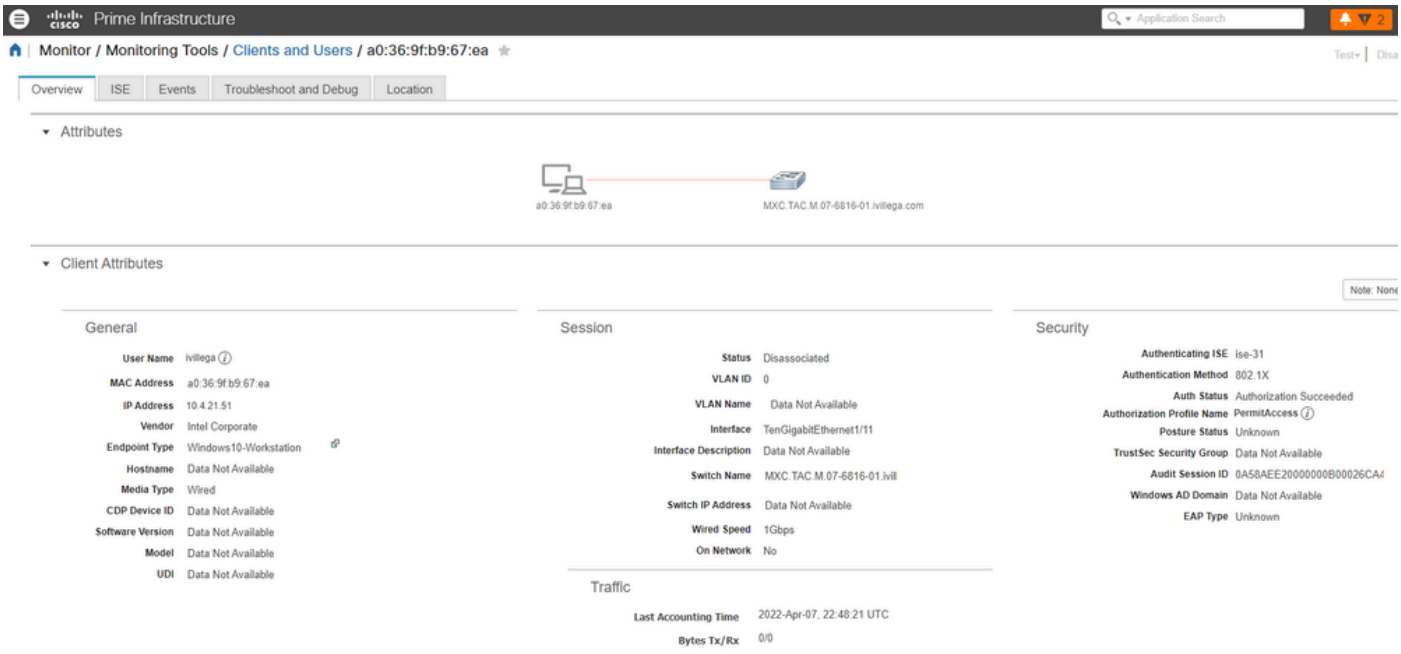
```
MXC.TAC.M.07-6816-01#show authentication session int Te1/11 detail
        Interface: TenGigabitEthernet1/11
      MAC Address: a036.9fb9.67ea
     IPv6 Address: Unknown
     IPv4 Address: 10.4.21.51
        User-Name: ivillega
           Status: Authorized
           Domain: DATA
   Oper host mode: multi-domain
 Oper control dir: both
  Session timeout: N/A
Common Session ID: 0A58AEE20000002F1E163DA0
  Acct Session ID: 0x00000023
           Handle: 0xD9000001
   Current Policy: POLICY_Te1/11

Method status list:
        Method      State
        dot1x       Authc Success
```

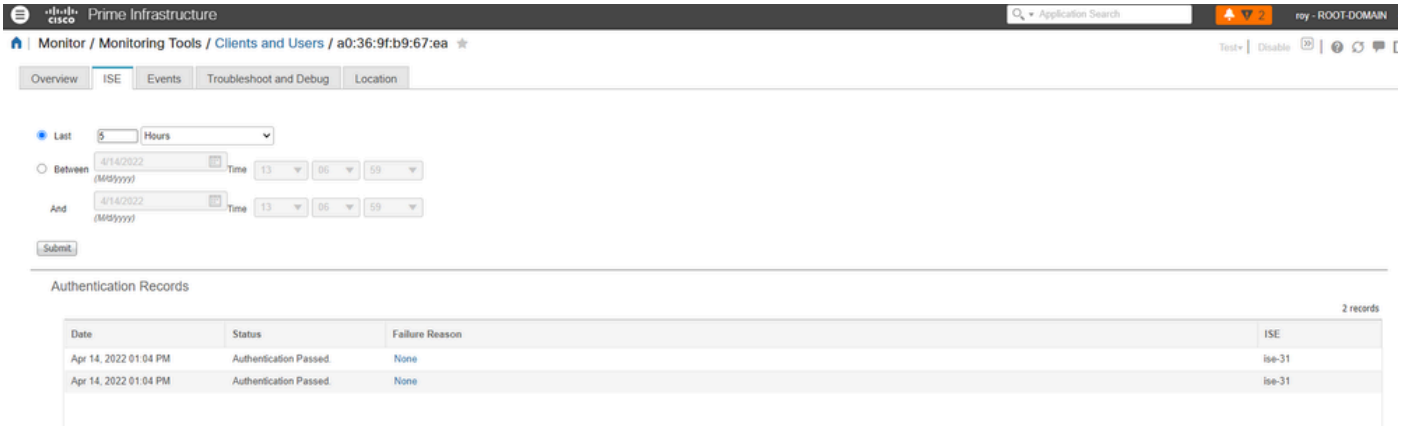
检验Prime基础设施

4.定位至监控>监控工具>客户端和用户。显示终端的MAC地址：

5.如果单击它，您会看到用户会话详细信息和ISE服务器信息：



6.还有一个标记为ISE的选项卡用于检索此特定终端的会话事件。您可以选择Prime基础设施用于从ISE获取事件的时间范围：



故障排除

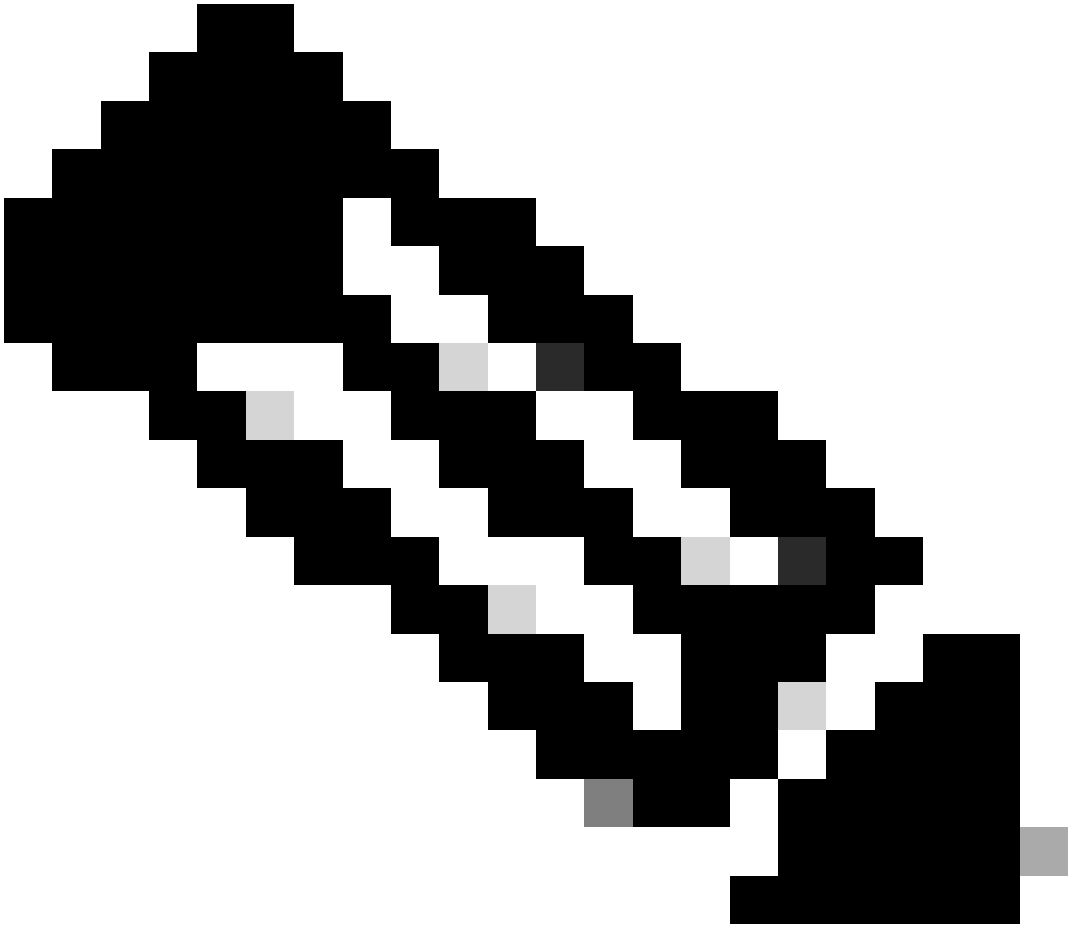
1.使用ping测试ISE和Prime基础设施之间的连接。如果没有连接，您可以使用ISE或PI的跟踪路由查找问题。

2.检查步骤9中配置的端口是否在ISE MnT节点中打开（默认端口为443）：

```
ise-31-1/admin# show ports | include :443
     tcp: 0.0.0.0:80, 0.0.0.0:19444, 0.0.0.0:19001, 0.0.0.0:443
```

如果输出中列出端口，则表示ISE MnT已打开端口。

如果没有输出或未列出端口，则表示ISE MnT已关闭该端口。在这种情况下，您可以尝试使用其他端口或通过ISE团队打开TAC案例，以检查端口未打开的原因。



注意：ISE MnT节点仅使用某些端口，无法打开ISE MnT节点中未在ISE安装指南“端口参考”部分列出的端口。

3.使用来自Prime基础设施的Telnet测试步骤9中配置的端口：

```
prime-testcom/admin# telnet 10.4.21.55 port 443
Trying 10.4.21.55...
```

```
Connected to 10.4.21.55.
```

如果telnet测试的输出为Connected to <ISE MnT IP/FQDN>，则表示测试成功。

如果telnet测试的输出停滞在Trying <ISE MnT IP/FQDN>，则表示测试失败。这可能与中间网络设备中的ACL或与防火墙规则相关。

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）。