H3C 交换机与第三方认证服务器

对接操作指导

新华三技术有限公司
http://www.h3c.com

资料版本：6W102-20221229

环境保护

本产品符合关于环境保护方面的设计要求，产品的存放、使用和弃置应遵照相关国家法律、法规要求进行。

前 言

本文档主要介绍 H3C 交换机与第三方认证服务器的对接操作指导。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... }*	表示从多个选项中至少选取一个。
[x | y | ...]*	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

H3C 交换机

与 Aruba ClearPass 接入认证功能对接操作指导

目 录

1 简介

本文档介绍 H3C 交换机与 Aruba 的认证服务器软件 ClearPass 的接入认证功能对接配置，包括：

- MAC 地址认证对接配置举例
- 802.1X 认证对接配置举例
- Portal 认证对接配置举例
- 授权 VLAN 对接配置举例
- 授权 ACL 对接配置举例
- 授权 User-Profile 对接配置举例
- 授权 CAR 对接配置举例
- 重认证对接配置举例
- URL 重定向对接配置举例
- DAE 对接配置举例
- SSH 登录使用 HWTACACS 认证对接配置举例
- Login 登录使用 RADIUS 认证对接配置举例

说明

对接第三方认证服务器操作为交换机产品通用性内容，但部分接入认证功能在各产换机产品上存在支持差异。产品对各认证特性的支持情况请参考产品配置指导中安全分册的相关内容。

2 互通性分析

表1 接入认证互通性分析

H3C	Aruba ClearPass	互通结论
固定用户名和密码的MAC地址认证	CHAP认证	可以互通
MAC地址作为用户名密码进行认证	CHAP认证	可以互通
802.1X CHAP认证	CHAP认证	可以互通
802.1X PAP认证	PAP认证	可以互通
802.1X EAP认证	EAP-MD5认证	可以互通
802.1X EAP认证	证书认证	可以互通
Portal认证	CHAP认证	可以互通
授权VLAN	• 授权数字型 VLAN • 授权 VLAN 名称 • 授权 VLAN 组名 • 授权 Multi VLAN	可以互通

H3C	Aruba ClearPass	互通结论
	• 授权 Auto VLAN	
授权ACL	授权静态ACL	可以互通
授权User Profile	授权User Profile	可以互通
授权CAR属性	授权CAR	可以互通
重认证	• 会话超时后重认证 • 会话超时后强制下线 • 会话超时后根据周期重认证定时器的值重认证	可以互通
授权URL重定向	URL重定向	可以互通
DAE	• 强制下线（Disconnect Messages） • 关闭端口（CoA-Session termination by Disabling host port） • 重启端口（CoA-Session termination by bouncing host port）	可以互通
SSH用户的HWTACACS认证	-	可以互通
Login用户的RADIUS认证	-	可以互通

3 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

4 使用限制

本文档中 MAC 地址、802.1X 认证和 Portal 认证对接配置举例中，配置 ClearPass 时，配置文件中需要至少配置一个属性，否则配置文件会无法保存；若不使用配置文件，则用户认证上线时服务器端会报警告。

5 MAC 地址认证对接配置举例

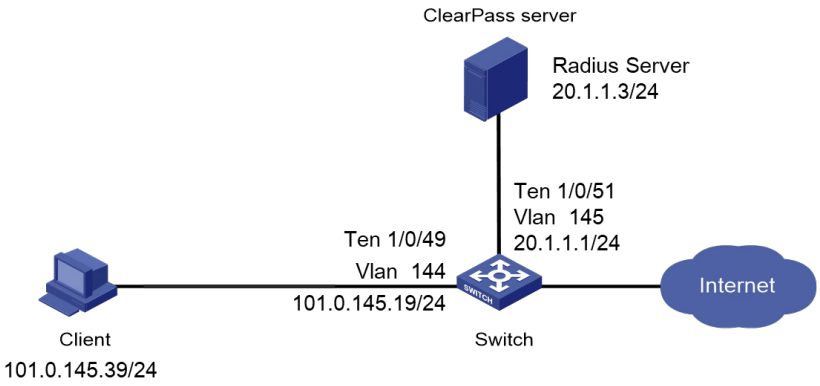
5.1 组网需求

如图 1 所示，Client 和 ClearPass 服务器通过 Switch 建立连接，设备管理员希望对 Client 进行 MAC 地址认证，以控制其对网络资源的访问，具体要求如下：

- 采用 ClearPass 作为 RADIUS 服务器。

- 配置 MAC 地址认证的用户名和密码。

图1 MAC 认证配置组网图



5.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch：S5130-HI，R3507P02
- Aruba 认证服务器：ClearPass CPPM V6.9.7

5.3 固定用户名密码的MAC地址认证配置步骤与验证

说明

本配置仅展示认证的相关配置，网络互通的相关配置略，请保证设备间能够互相访问。

5.3.1 配置 Switch

配置 RADIUS 方案。

```
<Device> system-view
[Device] radius scheme radius1
[Device-radius-radius1] primary authentication 20.1.1.3
[Device-radius-radius1] primary accounting 20.1.1.3
[Device-radius-radius1] key authentication simple 123456
[Device-radius-radius1] key accounting simple 123456
[Device-radius-radius1] user-name-format without-domain
[Device-radius-radius1] quit
```

配置 MAC 地址认证的认证方法为 CHAP。

```
[Device] mac-authentication authentication-method chap
```

创建 MAC 地址认证的域 mac-auth，并配置 ISP 域的 AAA 方法。

```
[Device] domain mac-auth
[Device-isp-mac-auth] authentication default radius-scheme radius1
[Device-isp-mac-auth] authorization default radius-scheme radius1
[Device-isp-mac-auth] accounting default radius-scheme radius1
```

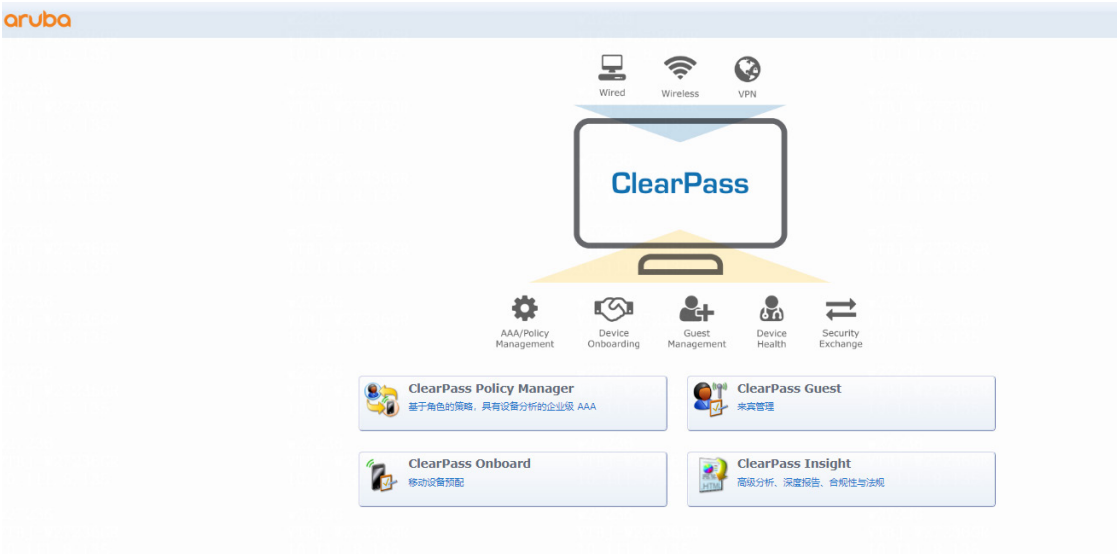
```
[Device-isp-mac-auth] quit
```
配置互通的 VLAN 和 VLAN 接口的 IP 地址。
```
[Device] vlan 144
[Device-vlan144] quit
[Device] interface Vlan-interface 144
[Device-Vlan-interface144] ip address 101.0.145.19 255.255.255.0
[Device-Vlan-interface144] quit
[Device] vlan 145
[Device-vlan145] quit
[Device] interface Vlan-interface 145
[Device-Vlan-interface145] ip address 20.1.1.1 255.255.255.0
[Device-Vlan-interface145] quit
```
将端口 XGE1/0/49 和 XGE1/0/51 加入到指定的 VLAN，并开启 MAC 地址认证功能。
```
[Device] interface Ten-GigabitEthernet 1/0/49
[Device-Ten-GigabitEthernet1/0/49] port access vlan 144
[Device-Ten-GigabitEthernet1/0/49] mac-authentication
[Device-Ten-GigabitEthernet1/0/49] quit
[Device] interface Ten-GigabitEthernet 1/0/51
[Device-Ten-GigabitEthernet1/0/51] port access vlan 145
[Device-Ten-GigabitEthernet1/0/51] quit
```
设置 mac-auth 为系统缺省的认证域。
```
[Device] domain default enable mac-auth
```
指定 MAC 地址认证用户的认证域 mac-auth。
```
[Device] mac-authentication domain mac-auth
```
配置 MAC 地址认证的定时器。
```
[Device] mac-authentication timer offline-detect 180
[Device] mac-authentication timer quiet 180
```
配置 MAC 地址认证使用固定用户名账号：用户名为 user，密码为明文 123456。
```
[Device] mac-authentication user-name-format fixed account user password simple 123456
```
开启全局 MAC 地址认证。
```
[Device] mac-authentication
```

5.3.2 配置 ClearPass

(1) 登录 ClearPass

在浏览器中输入 ClearPass 的管理 IP 地址，登录 ClearPass 的配置页面。

图2 登录 ClearPass



单击“ClearPass Policy Manager”，输入登录 ClearPass 服务器的用户名和密码（本例为 admin 和 Pass1234_），点击“登录”按钮进入认证配置页面。

图3 登录 ClearPass Policy Manager

(2) 添加用户

依次点击“配置 » 身份 » 本地用户 » 添加”，根据图 4 输入用户 ID 和密码。

a. “用户 ID”为设备上指定的 MAC 地址认证用户的用户名（本例为 user）

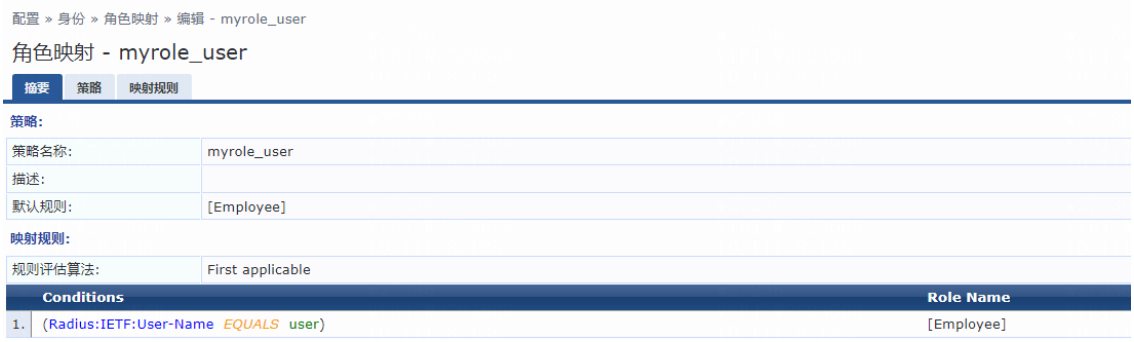
b. “密码”为设备上配置的 MAC 地址认证用户的密码（本例为 123456）

图4 添加用户

(3) 角色映射

根据图 5 添加角色映射。其中，添加“Conditions”时“User-Name”的值对应的是图 4 的“用户 ID”。

图5 添加角色映射



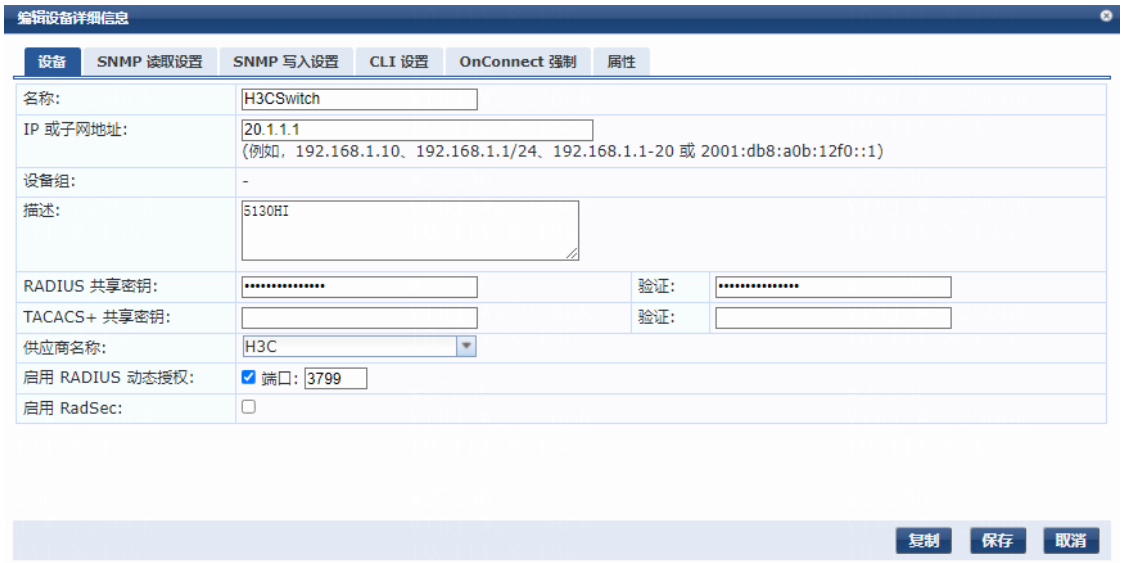
(4) 添加设备

依次点击“配置 » 网络 » 设备 » 添加”，根据图 6 添加设备。

a. “IP 或子网地址”请填写设备上与服务器接口可达的 IP 地址（本例为 20.1.1.1/24）

b. “RADIUS 共享密钥”需要与设备上配置的与 RADIUS 服务器交互的密钥相同（本例为 123456）

图6 添加设备



(5) 添加设备组

依次点击“配置 » 网络 » 设备组 » 添加”，根据图 7 添加设备组。

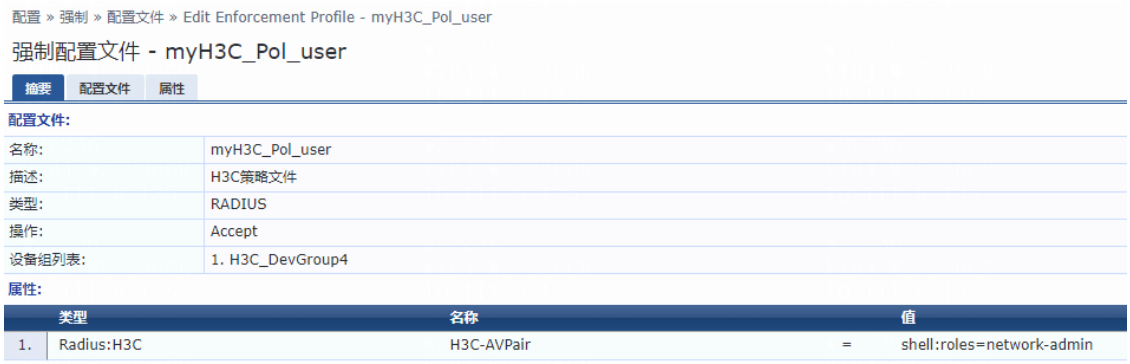
“子网”请填写设备上与服务器接口可达的 IP 地址（本例为 20.1.1.1/24）。

图7 添加设备组

(6) 添加配置文件

根据图 8 添加配置文件。此处的属性至少需指定一个，当前以赋予用户角色属性 network-admin 为例。

图8 添加配置文件



(7) 添加策略

根据图 9 添加策略。

a. 在添加策略时，“Conditions”中对应的“Actions”选择图 8 创建的配置文件。

b. 规则评估算法，根据需要选择选项中的一个即可。

图9 添加策略

(8) 添加服务

根据图 10 到图 13 添加服务中对应的各项。

a. 在图 10 中添加服务时，“类型”选择“RADIUS 强制（通用）”

b. 在图 12 中添加角色时，“角色映射策略”选择图 5 创建的角色映射

c. 在图 13 中添加强制时，“强制策略”选择在图 9 中创建的强制策略

图10 添加服务

图11 添加身份验证

分别点击“Select to Add”选择要使用的身份验证方法、身份验证源。

图12 添加角色

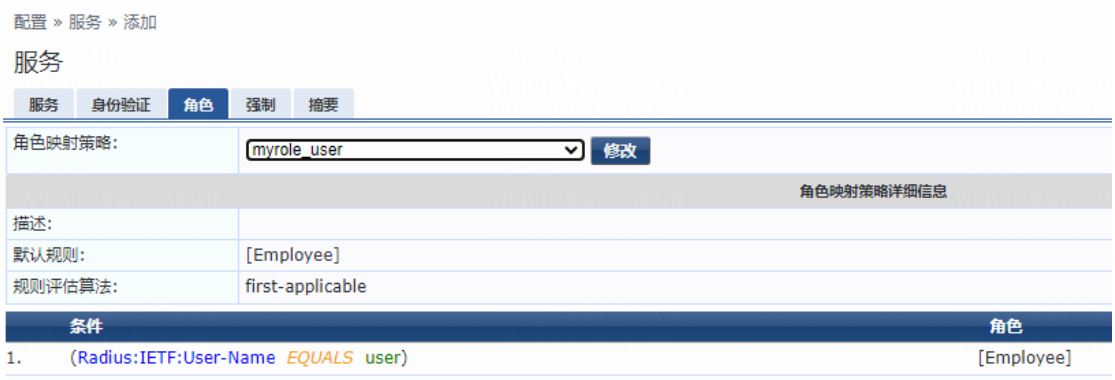


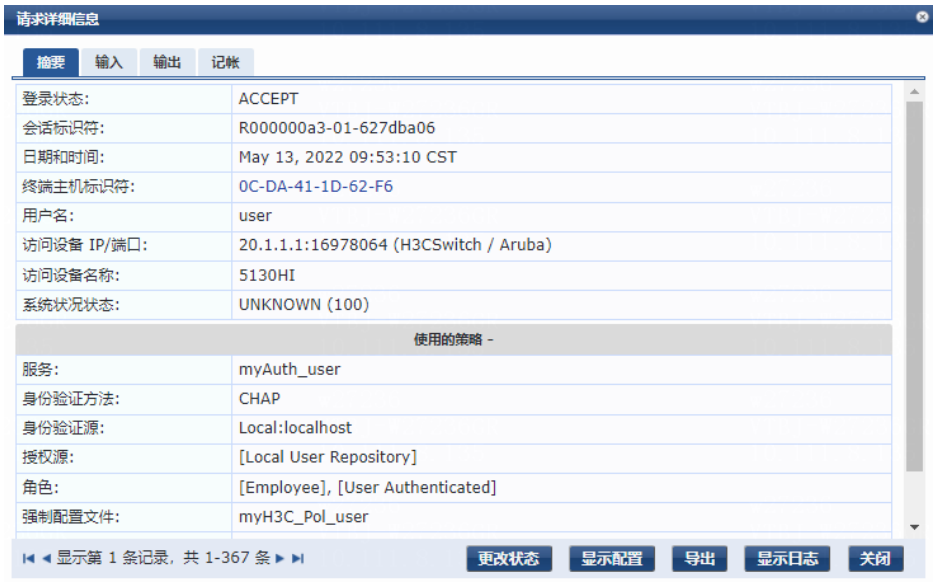
图13 添加强制

5.3.3 验证配置

(1) 在设备和服务器都配置好的情况下,在客户端利用 CMD 窗口 Ping 服务器即可完成用户上线。

(2) 用户上线后，可在服务器上查看到用户信息，点击“监视 » 实时监控 » 访问跟踪器”，选择用户上线记录点击（后续皆可通过该导航查看用户上线记录），如图 14。

图14 用户上线后服务器显示



(3) 用户上线后设备的显示信息

通过在设备上执行 **display mac-authentication connection** 可以看到上线用户的信息，其中 Username 为 MAC 地址认证的用户名 user。

```
[Device] display mac-authentication connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: user
User access state: Successful
Authentication domain: mac-auth
IPv4 address: 101.0.145.39
Initial VLAN: 144
Authorization untagged VLAN: N/A
Authorization tagged VLAN: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: N/A
Online from: 2022/05/13 09:53:10
Online duration: 0h 0m 5s
```

5.4 MAC地址作为用户名密码的MAC地址认证配置步骤与验证

说明

- 若采用 MAC 地址账号，则设备将检测到的用户 MAC 地址作为用户名和密码发送给 RADIUS 服务器进行验证。

5.4.1 配置 Switch

其它配置与“5.3.1 配置 Switch”相同，只需要将以下命令恢复缺省配置即可。

```
[Device] undo mac-authentication user-name-format
```

5.4.2 配置 ClearPass

需要注意以下几点，其它与“5.3.2 配置 ClearPass”配置相同。

(1) 添加用户

用户名和密码与客户端的 MAC 地址相同。

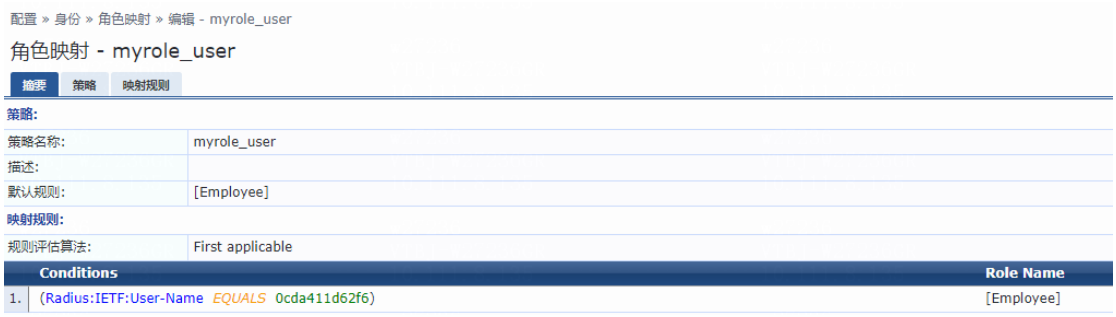
依次点击“配置 » 身份 » 本地用户 » 添加”，根据图 15 添加用户。

图15 添加用户

(2) 角色映射

需要将图 15 创建的角色映射中“Conditions”下的“User-Name”修改为用户的 MAC 地址。

图16 添加角色映射

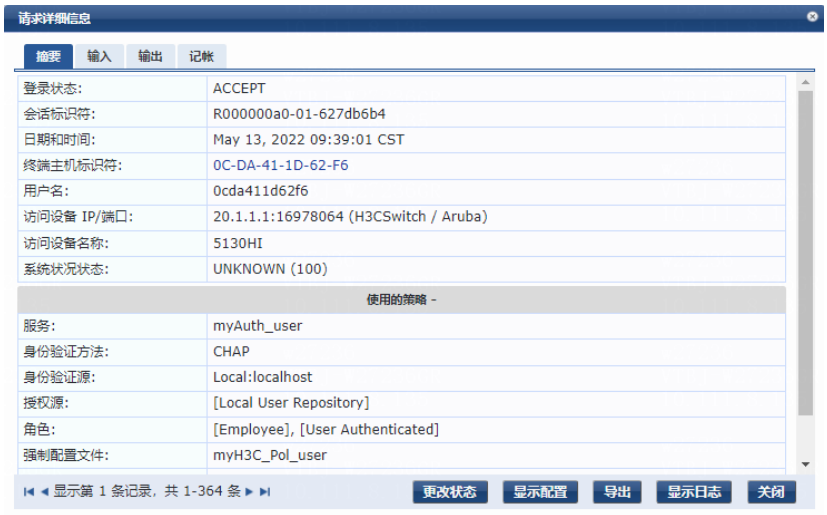


5.4.3 验证配置

(1) 在设备和服务器都配置好的情况下，在客户端利用 CMD 窗口 Ping 服务器即可完成用户上线。

(2) 用户上线后服务器显示如图 17。

图17 用户上线后服务器显示



(3) 用户上线后设备上的显示

通过在设备上执行 **display mac-authentication connection** 可以看到上线用户的信息，其中 Username 为用户的 MAC 地址。

```
[Device]display mac-authentication connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: 0cda411d62f6
User access state: Successful
Authentication domain: mac-auth
IPv4 address: 101.0.145.39
Initial VLAN: 144
```

```
Authorization untagged VLAN: N/A
Authorization tagged VLAN: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: N/A
Online from: 2022/05/13 09:39:01
Online duration: 0h 0m 6s
```

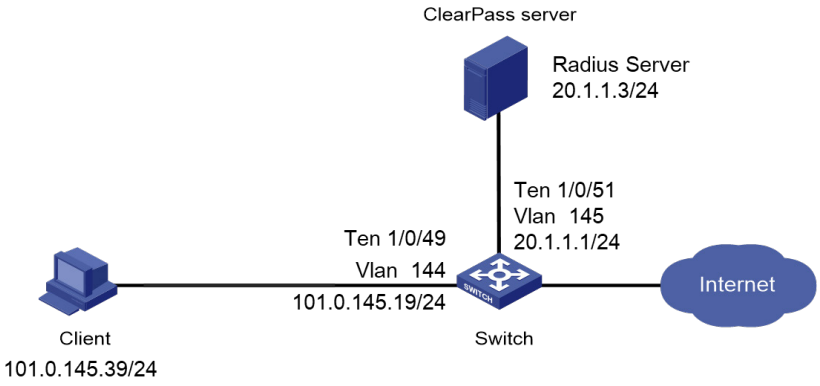
6 802.1X 认证对接配置举例

6.1 组网需求

如图 18 所示，Client 和 ClearPass 服务器通过 Switch 建立连接，设备管理员希望对 Client 进行 802.1X 认证，以控制其对网络资源的访问，具体要求如下：

- 采用 ClearPass 作为 RADIUS 服务器。
- 配置 PAP、CHAP、EAP-MD5、证书相关认证（EAP-TLS、EAP-PEAP、EAP-TTLS）方式。

图18 802.1X 认证配置组网图



6.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch：S5130-HI，R3507P02
- Aruba 认证服务器：ClearPass CPPM V6.9.7

6.3 802.1X CHAP配置步骤与验证

说明

本配置仅展示认证的相关配置，网络互通的相关配置略，请保证设备间能够互相访问。

6.3.1 配置 Switch

配置 RADIUS 方案。

```
<Device> system-view
[Device] radius scheme radius1
[Device-radius-radius1] primary authentication 20.1.1.3
[Device-radius-radius1] primary accounting 20.1.1.3
[Device-radius-radius1] key authentication simple 123456
[Device-radius-radius1] key accounting simple 123456
[Device-radius-radius1] user-name-format without-domain
[Device-radius-radius1] quit
```

配置 802.1x 认证的认证方法。

```
[Device] dot1x authentication-method CHAP
```

创建 802.1X 认证的域 bbb，配置 ISP 域的 AAA 方法。

```
[Device] domain bbb
[Device-isp-bbb] authentication default radius-scheme radius1
[Device-isp-bbb] authorization lan-access radius-scheme radius1 local
[Device-isp-bbb] accounting lan-access radius-scheme radius1 local
[Device-isp-bbb] quit
```

配置互通的 VLAN 和 VLAN 接口的 IP 地址。

```
[Device] vlan 144
[Device-vlan144]quit
[Device] interface Vlan-interface 144
[Device-Vlan-interface144] ip address 101.0.145.19 255.255.255.0
[Device-Vlan-interface144] quit
[Device] vlan 145
[Device-vlan145] quit
[Device] interface Vlan-interface 145
[Device-Vlan-interface145] ip address 20.1.1.1 255.255.255.0
[Device-Vlan-interface145] quit
```

将端口 XGE1/0/49 加入到指定 VLAN。

```
[Device]interface Ten-GigabitEthernet 1/0/49
[Device-Ten-GigabitEthernet1/0/49] port access vlan 144
```

开启端口的 802.1X 认证功能，并设置域 bbb 为 802.1X 强制认证域。

```
[Device-Ten-GigabitEthernet1/0/49] dot1x
[Device-Ten-GigabitEthernet1/0/49] dot1x mandatory-domain bbb
```

设置 802.1X 为端口控制方式。

```
[Device-Ten-GigabitEthernet1/0/49] dot1x port-method portbased
```

```
[Device-Ten-GigabitEthernet1/0/49] quit
```

将端口 XGE1/0/51 加入到指定 VLAN。

```
[Device] interface Ten-GigabitEthernet 1/0/51
[Device-Ten-GigabitEthernet1/0/51] port access vlan 145
[Device-Ten-GigabitEthernet1/0/51] quit
```

设置 bbb 为系统缺省的认证域。

```
[Device] domain default enable bbb
```

添加网络接入类本地用户，用户名为 user，密码为明文输入的 123456。（此处添加的本地用户的用户名和密码需要与远程服务器端配置的用户名和密码保持一致）

```
[Device] local-user user class network
[Device-luser-network-user] password simple 123456
[Device-luser-network-user] service-type lan-access
[Device-luser-network-user] quit
```

开启全局 802.1x 认证。

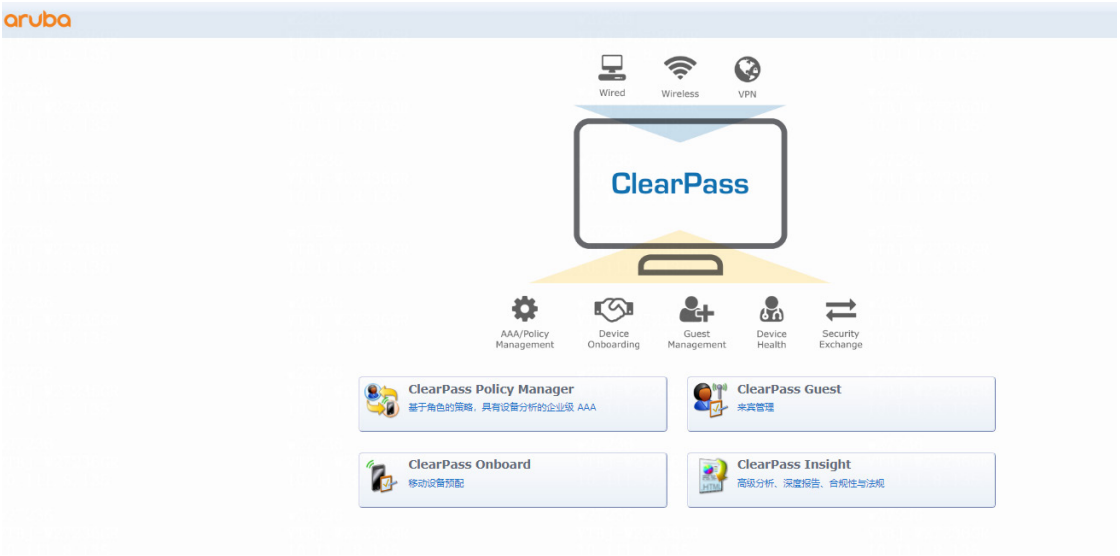
```
[Device] dot1x
```

6.3.2 配置 ClearPass

(1) 登录 ClearPass

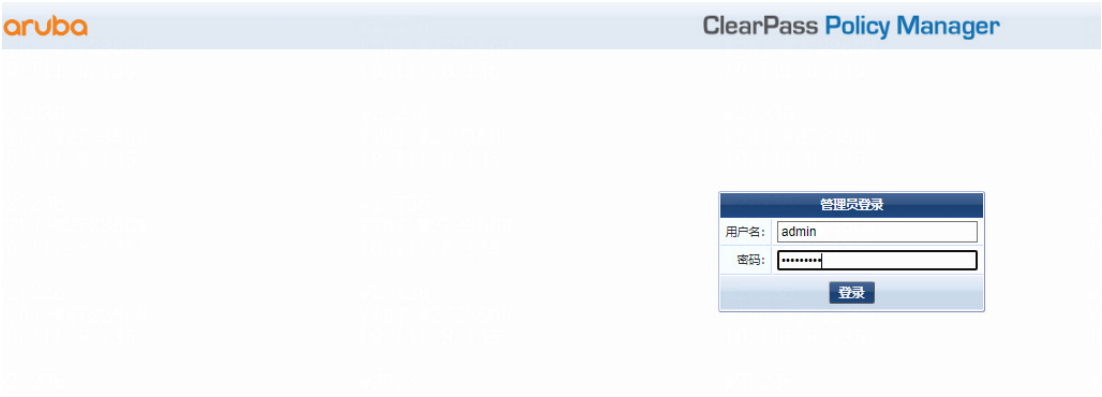
在浏览器中输入 ClearPass 的管理 IP 地址，登录 ClearPass 的配置页面。

图19 登录 ClearPass



单击“ClearPass Policy Manager”，输入登录 ClearPass 服务器的用户名和密码（本例为 admin 和 Pass1234_），点击“登录”按钮进入认证配置页面。

图20 登录 ClearPass Policy Manager



(2) 添加用户

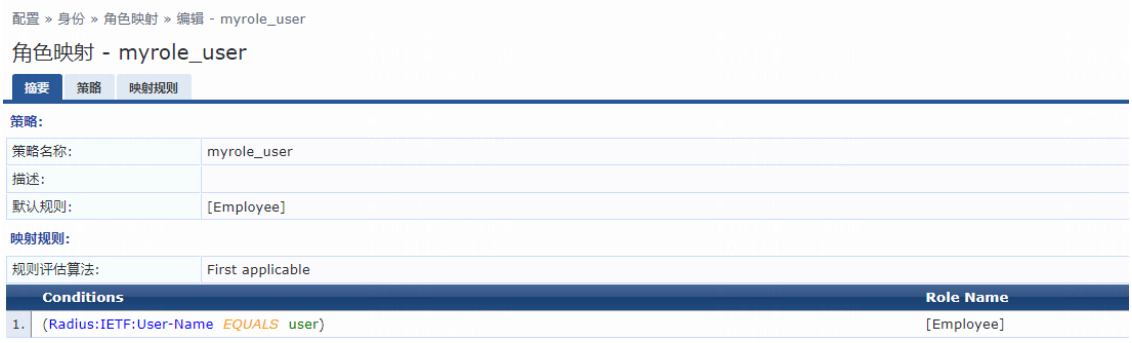
依次点击“配置 » 身份 » 本地用户 » 添加”，根据图 21 添加用户。

图21 添加用户

(3) 角色映射

根据图 22 添加角色映射。添加“Conditions”时“User-Name”的值对应的是图 21 添加的用户 ID。

图22 添加角色映射



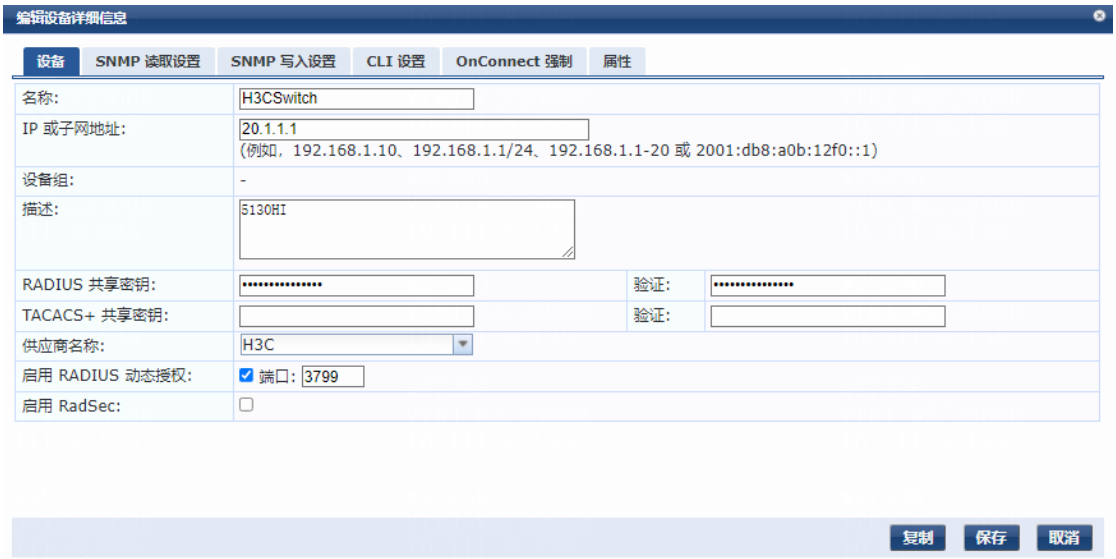
(4) 添加设备

依次点击“配置 » 网络 » 设备 » 添加”，根据图 23 添加设备。

a. “IP 或子网地址”填写设备上与服务器接口可达的 IP 地址（本例为 20.1.1.1/24）。

b. “RADIUS 共享密钥”需要与设备上配置的与 RADIUS 服务器交互的密钥相同（本例为 123456）

图23 添加设备



(5) 添加设备组

依次点击“配置 » 网络 » 设备组 » 添加”，根据图 24 添加设备组。

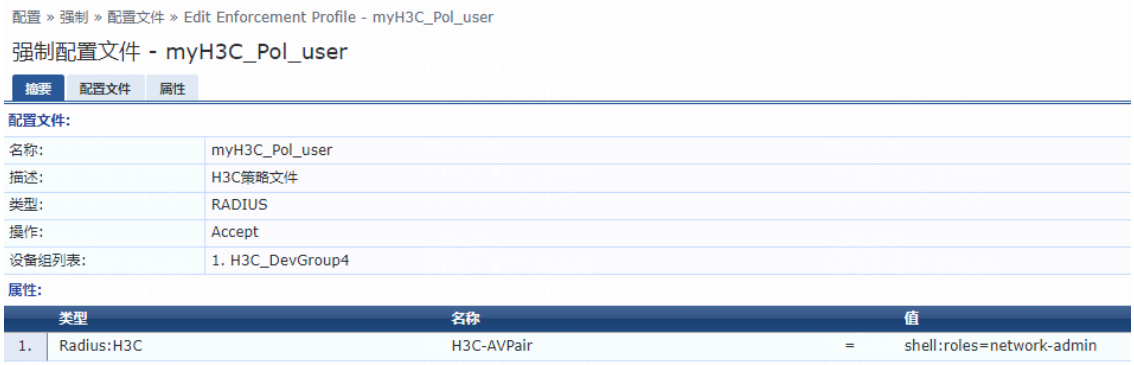
“子网”填写设备上与服务器接口可达的 IP 地址（本例为 20.1.1.1/24）。

图24 添加设备组

(6) 添加配置文件

根据图 25 添加配置文件。此处的属性至少指定一个，当前以赋予用户角色属性 network-admin 为例。

图25 添加配置文件



(7) 添加策略

根据图 26 添加策略。

a. 在添加策略时，“Conditions”中对应的“Actions”选择图 25 创建的配置文件。

b. 规则评估算法，根据需要选择选项中的一个即可。

图26 添加策略

(8) 添加服务

添加服务中对应的各项。

a. 在图 27 中添加服务时，“类型”选择 RADIUS 强制（通用）

b. 在图 25 中添加角色时，“角色映射”策略选择图 22 创建的角色映射

c. 在图 26 中添加强制时，“强制策略”选择在图 26 中创建的强制策略

图27 添加服务

图28 添加身份验证

分别点击“Select to Add”选择要使用的身份验证方法、身份验证源。

图29 添加角色

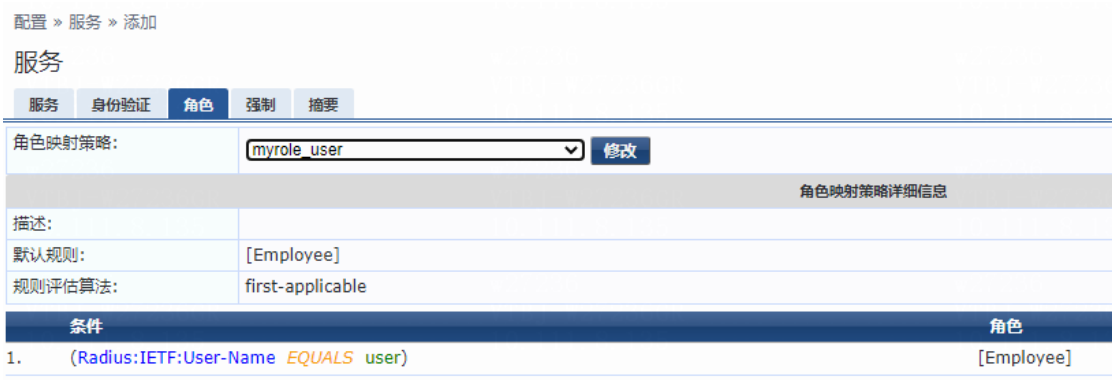


图30 添加强制

6.3.3 验证配置

(1) 在设备和服务器都配置好的情况下，在客户端使用 iNode 客户端，输入服务器上配置的用户名和密码即可完成用户上线。

图31 802.1X 客户端连接示意图

(2) 用户上线后服务器显示如图 32 所示。

图32 用户上线后服务器显示

(3) 用户上线后设备上的显示

在设备上通过 **display dot1x connection** 可以查看 802.1X 用户的信息，可其中 Username 为 802.1X 的用户名（本例为 user）。

```
[Device] display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: user
User access state: Successful
Authentication domain: bbb
Authentication method: CHAP
Initial VLAN: 144
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: N/A
Online from: 2022/05/11 18:21:58
Online duration: 0h 1m 22s
```

6.4 802.1X PAP认证配置步骤与验证

6.4.1 配置 Switch

设备上只需要将认证方式修改为 PAP，其它配置无需修改，请参考 6.3.1 配置 Switch。

```
[Device] dot1x authentication-method PAP
```

6.4.2 配置 ClearPass

服务器上只需要将“服务”中的“身份验证方式”修改为 PAP，其它配置无需修改，请参考 6.3.2 配置 ClearPass。

图33 修改身份验证方式

6.4.3 验证配置

(1) 在设备和服务器都配置好的情况下，在客户端使用 iNode 客户端，输入服务器上配置的用户名和密码即可完成用户上线。

(2) 用户上线后服务器显示如图 34 所示。

图34 用户上线后服务器显示

(3) 用户上线后设备显示

在设备上通过 **display dot1x connection** 可以查看 802.1X 用户的信息，可以看到上线用户的 Authentication method 已更改为 PAP。其余信息不变。

```
[Device]display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: user
User access state: Successful
Authentication domain: bbb
Authentication method: PAP
Initial VLAN: 144
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: N/A
Online from: 2022/05/11 18:23:06
Online duration: 0h 4m 28s
```

6.5 802.1X EAP MD5认证配置步骤与验证

6.5.1 配置 Switch

设备上只需要将认证方式修改为 EAP，其它配置无需修改，请参考 6.3.1 配置 Switch。

```
[Device] dot1x authentication-method EAP
```

6.5.2 配置 ClearPass

服务器上只需要将“服务”中的“身份验证方式”修改为 EAP-MD5 即可，其它配置无需修改，请参考 6.3.2 配置 ClearPass。

图35 修改身份验证方式

6.5.3 验证配置

(1) 在设备和服务器都配置好的情况下，在客户端使用 iNode 客户端，输入服务器上配置的用户名和密码即可完成用户上线。

(2) 用户上线后服务器显示如图 36。

图36 用户上线后服务器显示

(3) 用户上线后设备显示

在设备上通过 **display dot1x connection** 可以查看 802.1X 用户的信息，可其中 Username 为 802.1X 的用户名（本例为 user）。

```
[Device] display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: user
User access state: Successful
Authentication domain: bbb
Authentication method: EAP
Initial VLAN: 144
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: N/A
Online from: 2022/05/11 18:34:37
Online duration: 0h 0m 4s
```

6.6 802.1X证书认证配置步骤与验证

用户如需进行证书相关认证，需要先将相关证书（本例为：根证书、客户端证书以及服务器证书，如图 37，如需获取相关证书，请联系技术支持）分别导入 iNode 客户端以及服务器，并且在客户端上需选择相应的证书验证方式，同时设备以及服务器上也应选择相对应的认证方式，才可实现证书认证。

图37 三份证书

将根证书 certnew.cer 和客户端证书 jin.pfx 复制到 iNode 客户端文件中，双击打开，并进行后续安装。

6.6.1 客户端配置

(1) 导入根证书

图38 客户端导入根证书

点击“安装证书”，按照证书导入向导的步骤进行安装。

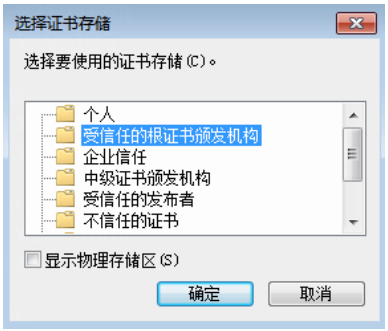
图39 证书安装向导一

点击“下一步”。

图40 证书安装向导二

选择“将所有的证书放入下列存储”点击“浏览”。

图41 选择证书存储

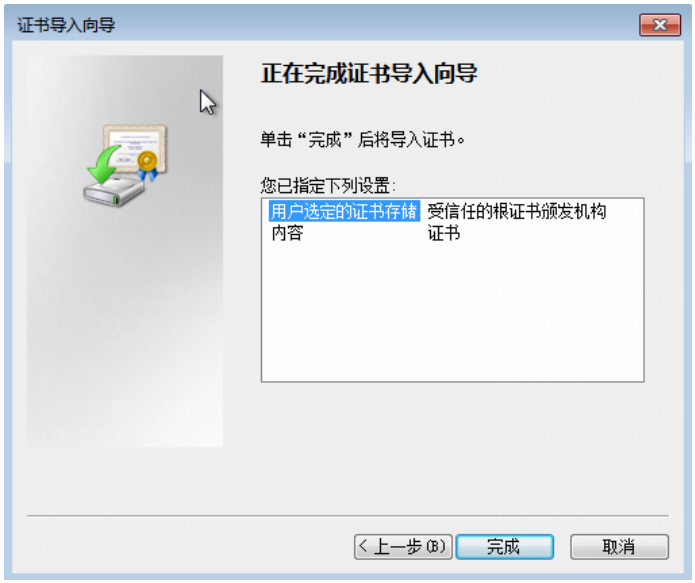


选择“受信任的根证书颁布机构”，点击“确定”。

图42 证书安装向导三

点击“下一步”。

图43 证书安装向导四



点击完成，即可完成根证书导入。

(2) 客户端证书导入

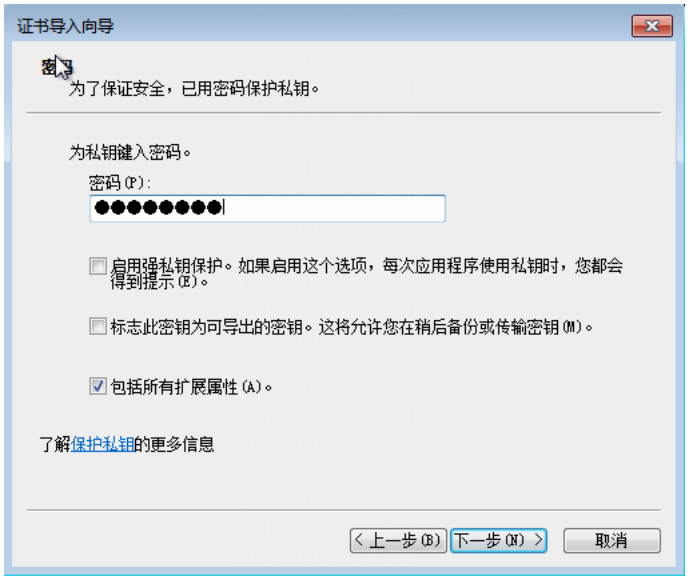
图44 客户端证书导入向导一

点击“下一步”。

图45 客户端证书导入向导二

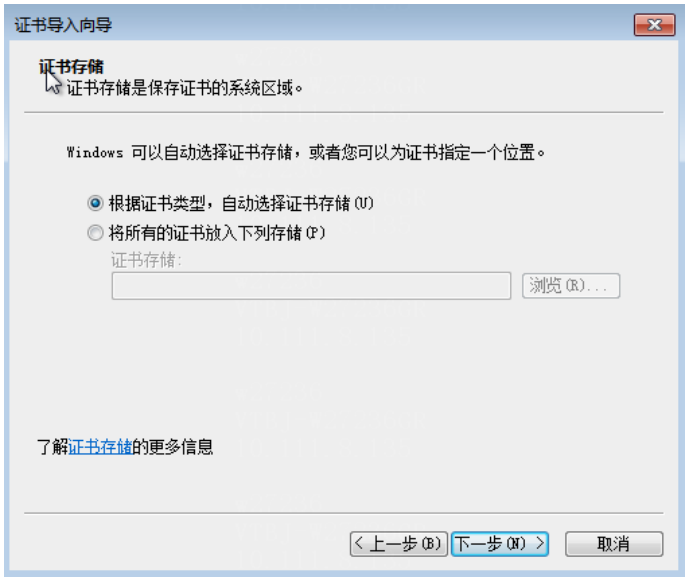
文件名按照默认，点击“下一步”。

图46 客户端证书导入向导三



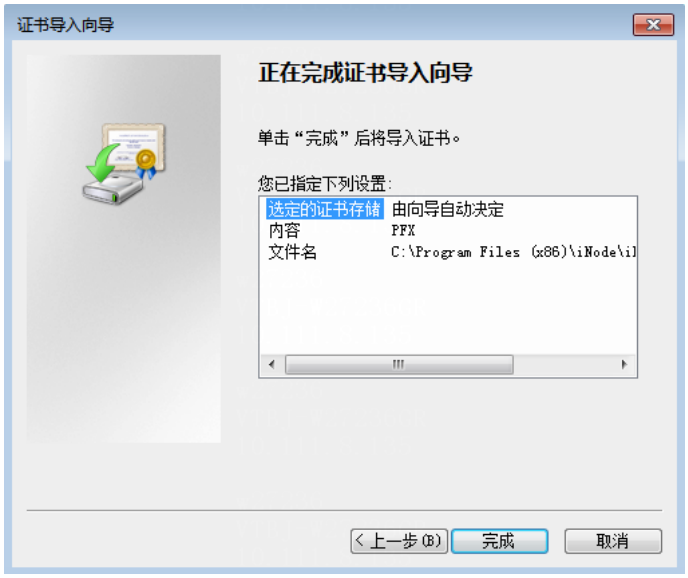
输入密码，密码为证书生成时的密码，点击“下一步”。

图47 客户端证书导入向导四



选择“根据证书类型，自动选择证书存储”，点击“下一步”。

图48 客户端证书导入向导五



点击完成，即可导入客户端证书。

(3) 客户端选择认证方式

图49 802.1X 客户端认证

在图 49 中点击“更多 » 属性”，进入“802.1X 认证”的属性页面。

在图 51 中点击“高级 » 启用高级认证 » 选择客户端证书”。

不同的认证方式对应选择的“认证类型”不同，EAP-TLS 和 EAP-PEAP 直接选择即可，EAP-TTLS 必须选择 EAP-TTLS 以及它的子类型 MS-CHAP-V2，如图 52。

图50 EAP-TLS 认证方式

图51 PEAP 认证方式

图52 EAP-TTLS 认证方式

点击“确定后”，进入“选择证书”页面（如图 53），选择之前导入的客户端证书，点击“确定”，完成客户端证书选择。

图53 选择客户端证书

6.6.2 配置 Switch

设备上只需要将认证方式修改为 EAP，其它配置无需修改。

```
[Device] dot1x authentication-method EAP
```

6.6.3 配置 ClearPass

服务器上的配置请参考 6.3.2 配置 ClearPass，并做如下补充：

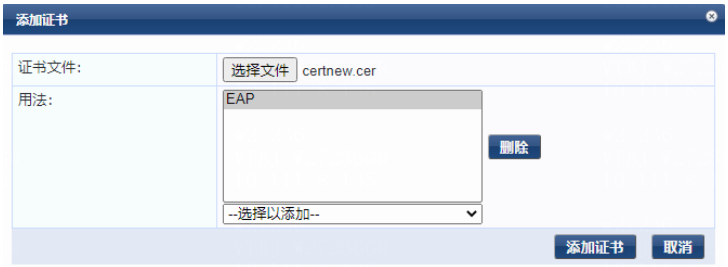
（1）导入根证书

在导航栏中选择“管理 » 证书 » 信任列表，添加根证书。

图54 导入根证书

如图 55“证书文件”选择根证书 certnew.cer，用法选择“EAP”，点击“添加证书”。

图55 添加证书



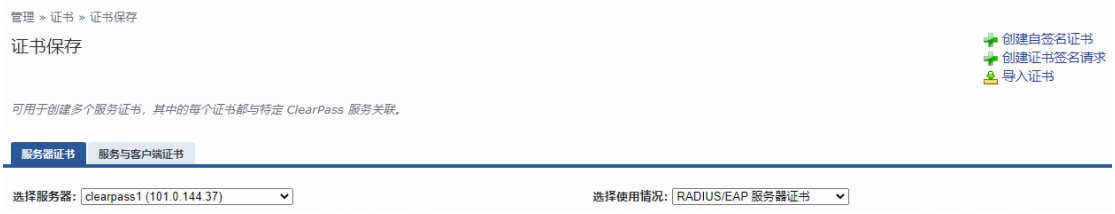
如图 56 查看证书信任列表，已成功导入根证书“CN=WINSERVER-KIM-CA”。

图56 查看导入的证书

（2）导入服务器证书

在导航栏中选择“管理 » 证书 » 信任列表，添加服务器证书。

图57 导入服务器证书



如图 58 证书类型选择“服务器证书”，上传方法按图 58 中选择，再点击选择文件，选择服务器证书 server.pfx，输入密码，点击“导入”。

图58 导入证书

可成功导入服务器证书，如图 59。

图59 查看导入的服务器证书

服务器上选择的认证方式需与客户端相对应。选择身份验证方法为 EAP-TLS，见图 60；选择身份验证方法为 EAP-PEAP，见图 61；选择身份验证方法为 EAP-TTLS，见图 62。

图60 选择身份验证方法 EAP-TLS

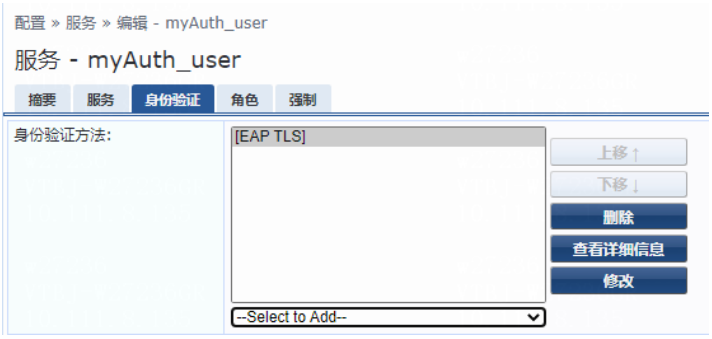


图61 选择身份验证方法为 EAP-PEAP

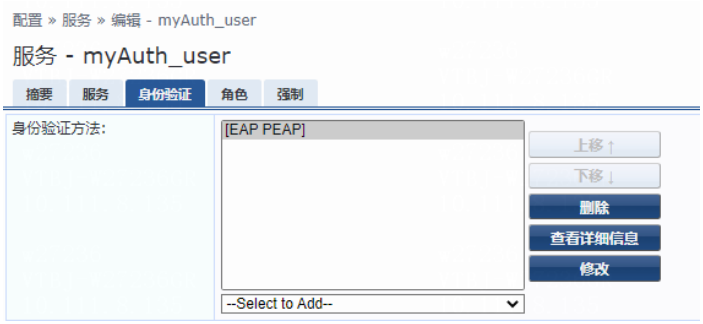
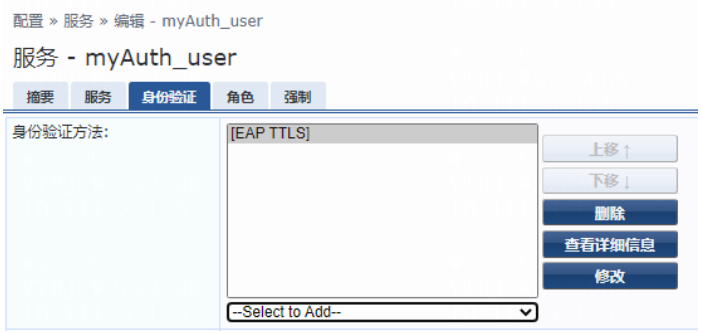


图62 选择身份验证方法为 EAP-TTLS



6.6.4 验证配置

(1) 用户在 iNode 客户端以及设备和服务器上完成配置后，在 iNode 客户端登录上线。

(2) 用户上线后服务器显示如图 63、图 64、图 65。

图63 EAP-TLS 认证方式上线后服务器显示

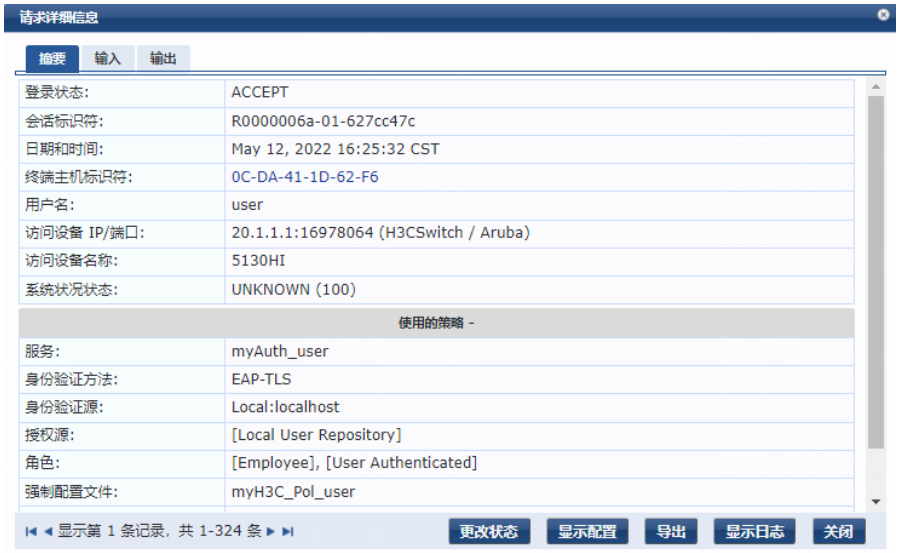


图64 EAP-PEAP 认证方式上线后服务器显示

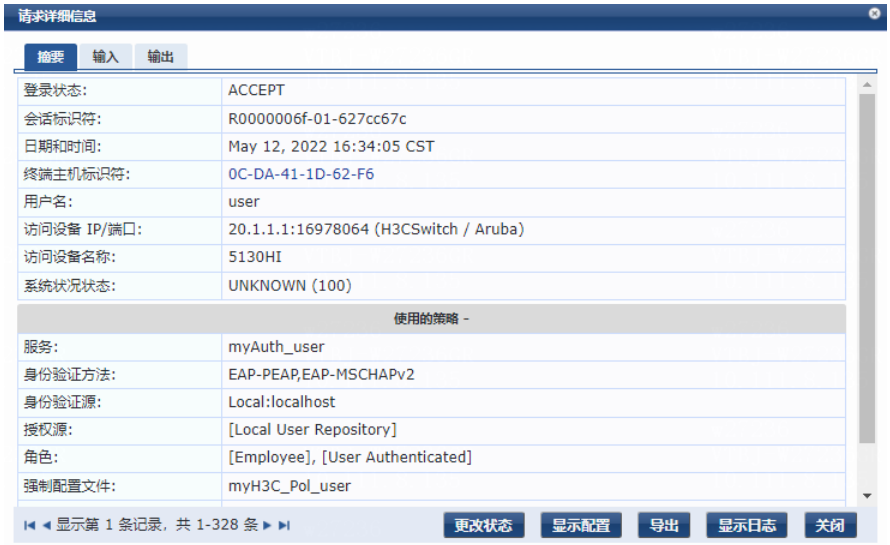
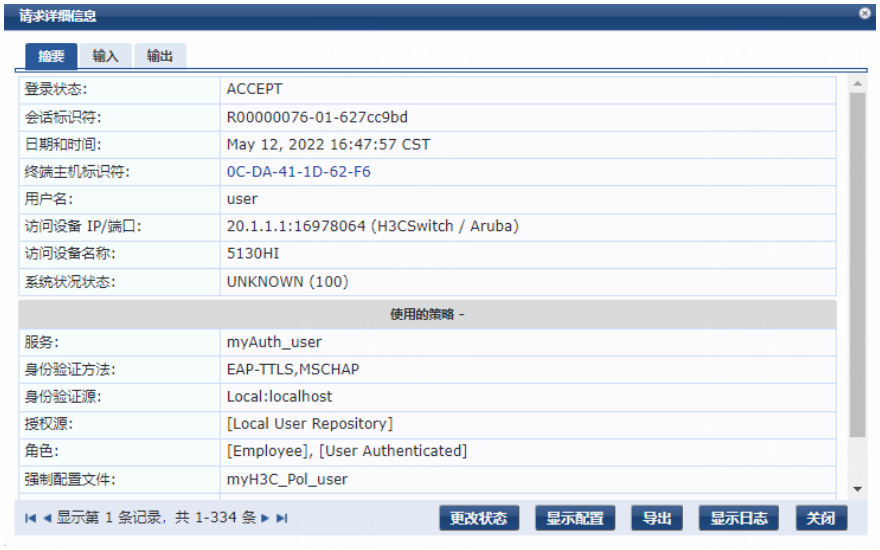


图65 EAP-TTLS 认证方式上线后服务器显示



(3) 用户线向后设备显示

在设备上通过 **display dot1x connection** 可以查看 802.1X 用户的信息，可其中 Username 为 802.1X 的用户名（本例为 user）。

```
[Device]display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: user
User access state: Successful
Authentication domain: bbb
Authentication method: EAP
Initial VLAN: 144
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: N/A
Online from: 2022/05/12 16:47:57
Online duration: 0h 0m 5s
```

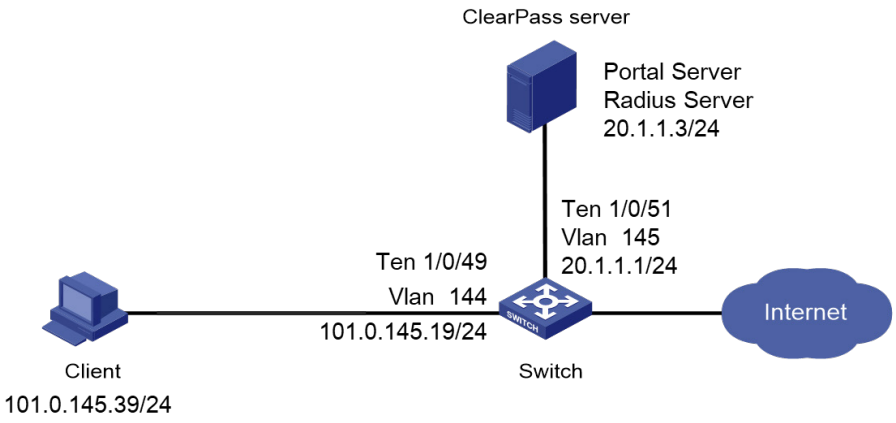
7 Portal 认证对接配置举例

7.1 组网需求

如图 66 所示，Client 和 ClearPass 服务器通过 Switch 建立连接，设备管理员希望对 Client 进行 Portal 认证，以控制其对网络资源的访问，具体要求如下：

- 采用 ClearPass 作为 RADIUS 服务器和 Portal 服务器。
- 用户采用直接方式的 Portal 认证。

图66 Portal 认证配置组网图



7.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch：S5130-HI，R3507P02
- Aruba 认证服务器：ClearPass CPPM V6.9.7

7.3 配置步骤

说明

本配置仅展示认证的相关配置，网络互通的相关配置略，请保证设备间能够互相访问。

7.3.1 配置 Switch

将配置 HTTPS 的安全证书使用 FTP 导入到设备上（如需获取相关证书，请联系技术支持）。

图67 HTTPS 安全证书

配置 RADIUS 方案。

```
<Device> system-view
[Device] radius scheme radius1
[Device-radius-radius1] primary authentication 20.1.1.3
[Device-radius-radius1] primary accounting 20.1.1.3
[Device-radius-radius1] key authentication simple 123456
[Device-radius-radius1] key accounting simple 123456
[Device-radius-radius1] user-name-format without-domain
[Device-radius-radius1] quit
```

创建 ISP 域“dm1”，并为该 ISP 域配置 AAA 认证/授权、计费方法为“”。

```
[Device] domain dm1
[Device-isp-dm1] authentication portal radius-scheme radius1
[Device-isp-dm1] authorization portal radius-scheme radius1
[Device-isp-dm1] accounting portal radius-scheme radius1
[Device-isp-dm1]quit
```

配置互通的 VLAN 和 VLAN 接口的 IP 地址。

```
[Device] vlan 144
[Device-vlan144] quit
[Device] interface Vlan-interface 144
[Device-Vlan-interface144] ip address 101.0.145.19 255.255.255.0
[Device-Vlan-interface144] portal apply web-server newpt
[Device-Vlan-interface144] portal bas-ip 101.0.145.19
[Device-Vlan-interface144]quit
[Device] vlan 145
[Device-vlan145] quit
[Device] interface Vlan-interface 145
[Device-Vlan-interface145] ip address 20.1.1.1 255.255.255.0
[Device-Vlan-interface145] quit
```

将端口 XGE1/0/49 和 XGE1/0/51 加入到指定的 VLAN。

```
[Device] interface Ten-GigabitEthernet 1/0/49
[Device-Ten-GigabitEthernet1/0/49] port access vlan 144
[Device-Ten-GigabitEthernet1/0/49] quit
[Device] interface Ten-GigabitEthernet 1/0/51
[Device-Ten-GigabitEthernet1/0/51] port access vlan 145
[Device-Ten-GigabitEthernet1/0/51] quit
```

配置 dm1 为缺省的 ISP 域。

```
[Device] domain default enable dm1
```

创建并进入 PKI 域 sslvpn，并指定证书申请所使用的 RSA 密钥对为 sslvpn，密钥用途为通用。

```
[Device] pki domain sslvpn
[Device-pki-domain-sslvpn] public-key rsa general name sslvpn
```

关闭 CRL 检查。

 注意

若开启了 CRL 检查，如果 PKI 域中不存在相应的 CRL、CRL 获取失败、或者 CRL 检查时发现待获取的证书已经吊销，则手动申请证书、获取证书的操作将会失败。

```
[Device-pki-domain-sslvpn] undo crl check enable
[Device-pki-domain-sslvpn] quit
```
将证书导入创建的域中，导入时需要的密码为创建证书时输入的密码。
```
[Device] pki import domain sslvpn pem ca filename cacert.crt
[Device] pki import domain sslvpn p12 local filename local.pfx
```
配置 HTTPS 服务器使用的 SSL 策略。
```
[Device] ssl server-policy 1
[Device-ssl-server-policy-1] pki-domain sslvpn
```
配置基于目的 IP 为 101.0.145.19 的免认证。
```
[Device] portal free-rule 2 destination ip 101.0.145.19 255.255.255.255
```
配置 Portal Web 服务器的 URL 地址。
```
[Device] portal web-server newpt
[Device-portal-websvr-newpt] url https://20.1.1.3/guest/h3c.php?_browser=1
[Device-portal-websvr-newpt] quit
```
配置 Portal 认证服务器。
```
[Device] portal server newpt
[Device-portal-server-newpt] ip 20.1.1.3 key simple 123456
[Device-portal-server-newpt] quit
```
进入本地 Portal Web 服务视图，并指定使用 HTTPS 协议和客户端交互认证信息。
```
[Device] portal local-web-server https ssl-server-policy 1 tcp-port 8443
[Device-portal-local-websvr-https] default-logon-page defaultfile.zip
[Device-portal-local-websvr-https] quit
```
开启 HTTPS 服务。
```
[Device] ip https enable
```

注意

配置 Portal Web 服务器的 URL 时，需选取 https 类型，因为 Aruba ClearPass 目前支持的是 https。

配置 Portal 直接认证。
```
[Device] interface Vlan-interface 144
[Device-Vlan-interface144] portal enable method direct
[Device-Vlan-interface144] quit
```

说明

- 用户可以采用直接认证或者可跨三层 Portal 认证方式上线，后者只需要修改设备上的 **portal enable method direct** 配置为 **portal enable method layer3** 即可，服务器和客户端无需改动。

7.3.2 配置 ClearPass

(1) 登录 Web 服务器

在游览器上登录服务器，点击“ClearPass 访客”。

图68 登录 ClearPass

(2) 创建 web 登录页

点击“主页 » 配置 » 页面 » Web 登录 » 新建 Web 登录页”。

图69 新建 Web 登录页

(3) 填写登录页内容

a. “提交 URL”必须与设备上 web-server 中配置的 URL 中的 http / https 的类型相同（具体参见 7.3.1 配置 Switch），因为当前设备会做二次检查，如不相同则无法通过

b. “提交方法”采用“POST”

c. URL 中填写的 IP 是设备上认证 VLAN 对应的 IP 地址（本例为：101.0.145.19）

d. “用户名字段、密码字段、额外字段”需按照当前格式填写，不做修改

e. “身份验证前检查”按照图 71 当前选项填写

f. 其它字段保持不变，点击“保存更改”

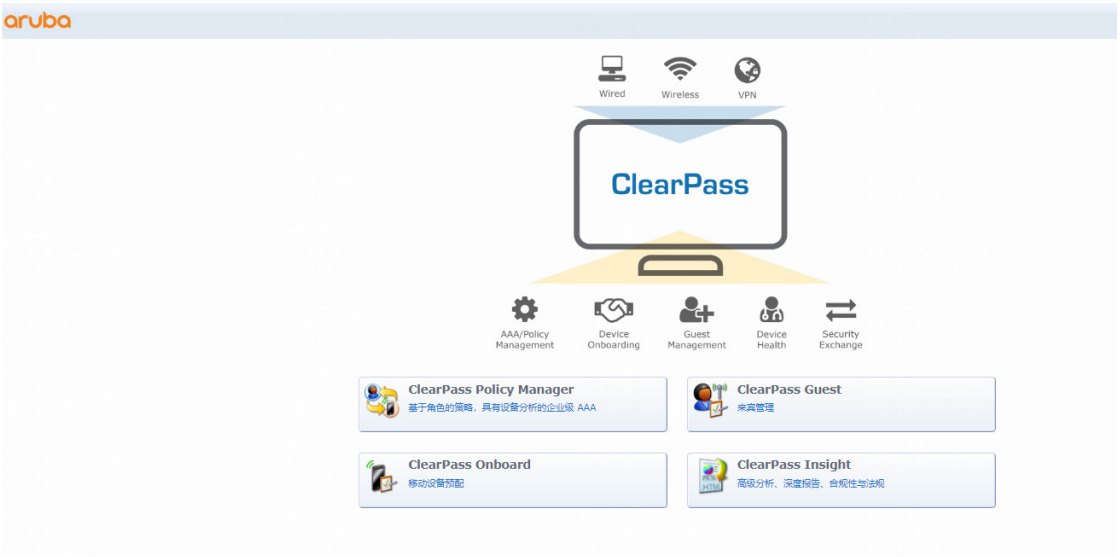
图70 Web 登录页填写示意一

图71 Web 登录页填写示意二

(4) 登录 ClearPass 策略服务器

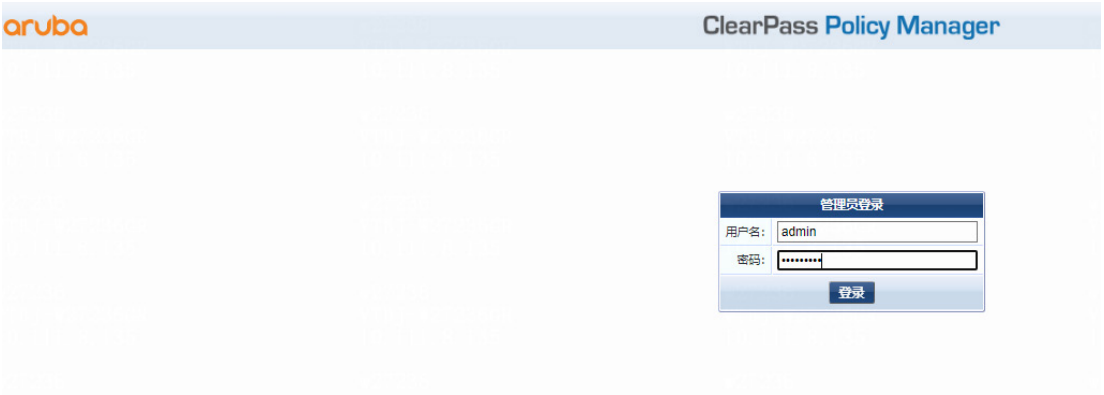
在浏览器中输入 ClearPass 的管理 IP 地址，登录页面后单击“ClearPass Policy Manager”，输入登录 ClearPass 服务器的用户名和密码进入认证配置页面。

图72 登录 ClearPass



单击“ClearPass Policy Manager”，输入登录 ClearPass 服务器的用户名和密码（本例为 admin 和 Pass1234_），点击“登录”按钮进入认证配置页面。

图73 登录 ClearPass Policy Manager



(5) 添加用户

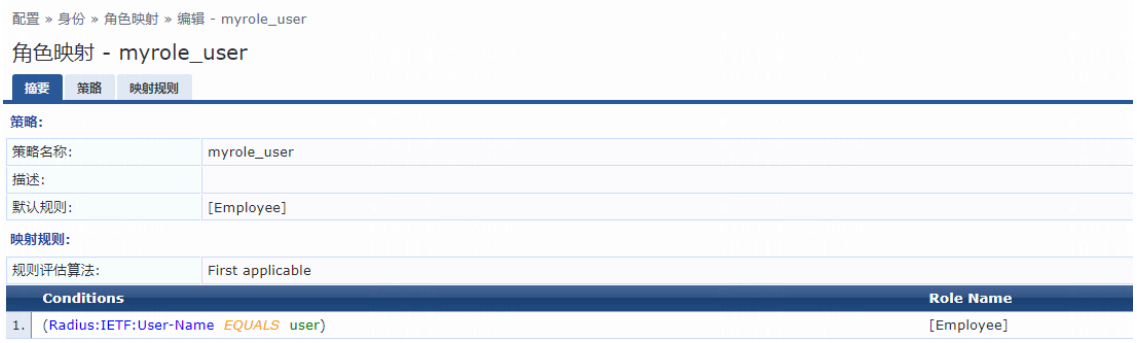
依次点击“配置 » 身份 » 本地用户 » 添加”，根据图 74 添加用户。

图74 添加用户

(6) 角色映射

根据图 75 添加角色映射，添加“Conditions”时“User-Name”的值对应的是图 74 添加的用户 ID。

图75 添加角色映射



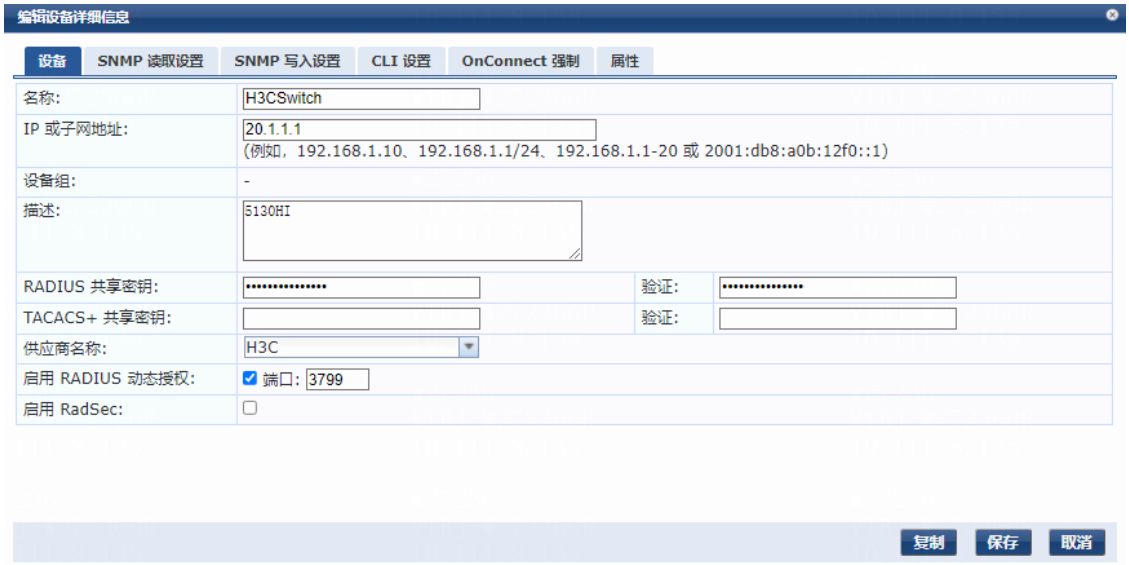
(7) 添加设备

依次点击“配置 » 网络 » 设备 » 添加”，根据图 76 添加设备

a. “IP 或子网地址”填写设备上与服务器接口可达的 IP 地址（本例为 20.1.1.1/24）

b. “RADIUS 共享密钥”需要与设备上配置的密钥相同

图76 添加设备



(8) 添加设备组

依次点击“配置 » 网络 » 设备组 » 添加”，根据图 77 添加设备组。

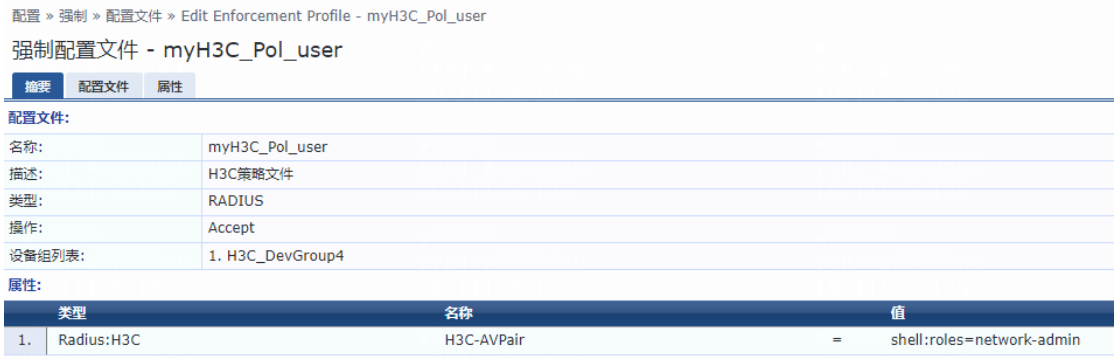
“子网”填写设备上与服务器接口可达的 IP 地址（本例为 20.1.1.1/24）

图77 添加设备组

(9) 添加配置文件

根据图 78 添加配置文件。此处的属性至少指定一个，当前以赋予用户角色属性 network-admin 为例。

图78 添加配置文件



(10) 添加策略

根据图 79 添加策略。

a. 在添加策略时，“Conditions”中对应的“Actions”选择图 78 创建的配置文件

b. 规则评估算法，根据需要选择选项中的一个即可

图79 添加策略

(11) 添加服务

添加服务中对应的各项。

a. 在图 80 中添加服务时，“类型”选择 RADIUS 强制（通用）

- NAS-Port-Type：NAS 认证用户的端口的物理类型，15 表示以太网
- Service-Type：用户申请认证的业务类型
- Framed-Protocol：用户 Frame 类型业务的封装协议

b. 在图 82 中添加角色时，“角色映射”策略选择图 75 创建的角色映射

c. 在图 83 中添加强制时，“强制策略”选择在图 78 中创建的强制策略

图80 添加服务

图81 添加身份验证

分别点击“Select to Add”选择要使用的身份验证方法、身份验证源。

图82 添加角色

图83 添加强制

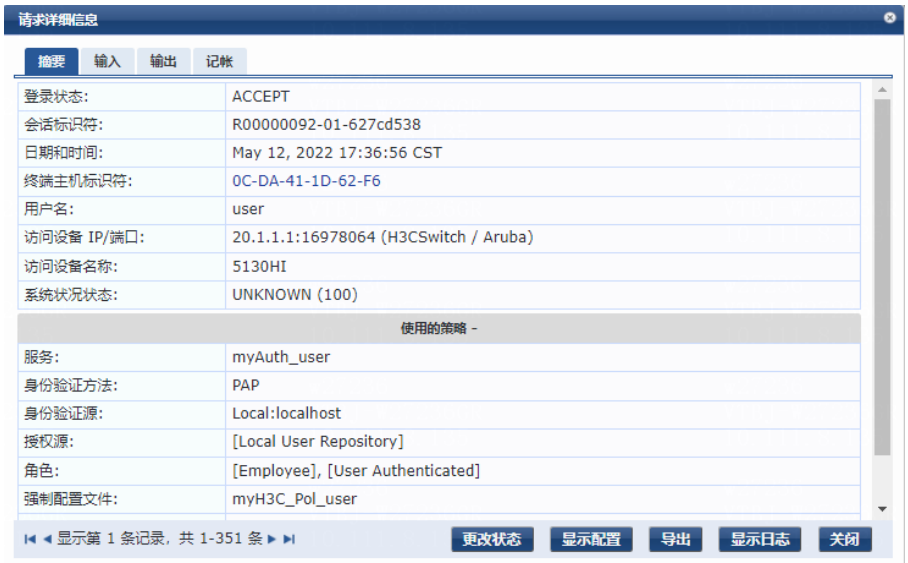
7.4 验证配置

(1) 用户在游览器上输入任意 IP，会被重定向到在服务器上配置的 Web 登陆页面，输入在服务器上配置的用户名和密码，点击登录。

图84 Web 登录页面

(2) 用户上线后服务器显示如图 85。

图85 用户上线后服务器显示



(3) 用户上线后设备显示信息

在设备上通过 **display portal user** 命令可以查看上线 Portal 用户的信息。其中 Username 字段显示为 Portal 用户的用户名 user。

```
[Device] display portal user all
Total portal users: 1
Username: user
  Portal server:
  State: Online
  VPN instance: N/A
  MAC             IP                   VLAN    Interface
  0cda-411d-62f6  101.0.145.39          144     Vlan-interface144
  Authorization information:
    DHCP IP pool: N/A
    User profile: N/A
    Session group profile: N/A
    ACL number: N/A
    Inbound CAR: N/A
Outbound CAR: N/A
```

8 授权 VLAN 对接配置举例

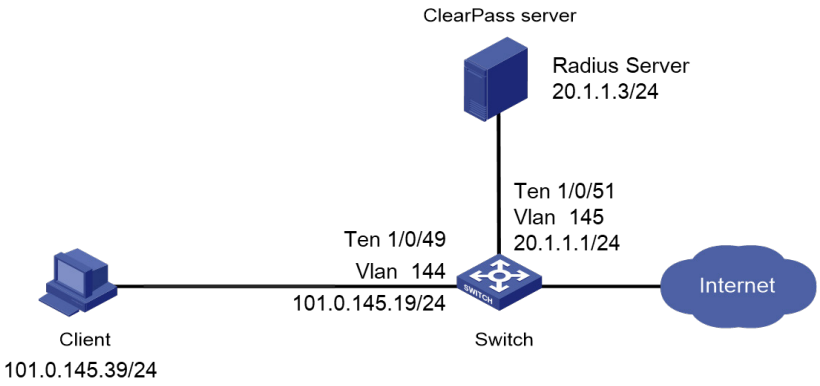
8.1 组网需求

如图 86 所示，Client 和 ClearPass 服务器通过 Switch 建立连接，设备管理员希望对 Client 进行 802.1X 认证或者 MAC 地址认证，以控制其对网络资源的访问，具体要求如下：

- 采用 ClearPass 作为 RADIUS 服务器。

- 通过 ClearPass 授权下发 VLAN，初始 VLAN 为 144。

图86 授权 VLAN 组网图



8.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch：S5130-HI，R3507P02
- Aruba 认证服务器：ClearPass CPPM V6.9.7

8.3 授权数字型VLAN配置步骤与验证

8.3.1 配置 Switch

MAC 地址认证用户，Swtich 上的配置请参考 5.3.1 配置 Switch。

802.1X 认证用户，Swtich 上的配置请参考 6.3.1 配置 Switch。

8.3.2 配置 ClearPass

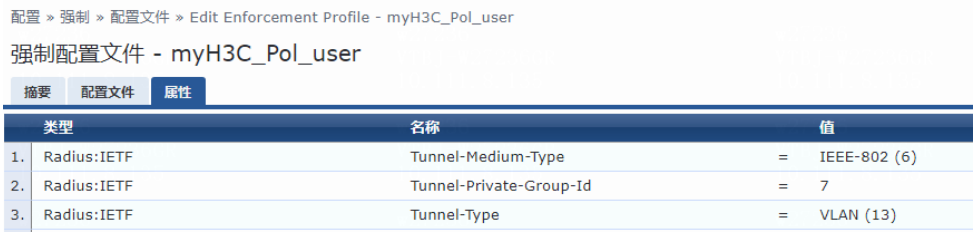
MAC 地址认证用户，服务器上的配置请参考 5.3.2 配置 ClearPass。

802.1X 认证用户，服务器上的配置请参考 6.3.2 配置 ClearPass。

只需将“配置文件”的“属性”参考图 87 修改即可。

- Tunnel-Medium-Type：创建隧道的传输层媒介类型，该属性值为 6 时表示 802 类型，可用于下发 VLAN。
- Tunnel-Private-Group-ID：隧道会话的组 ID，该属性在下发 VLAN 时用于携带下发的 VLAN ID（本例下发的 VLAN ID 为 7）。
- Tunnel-Type：使用的隧道协议，该属性值为 13 时表示下发 VLAN。

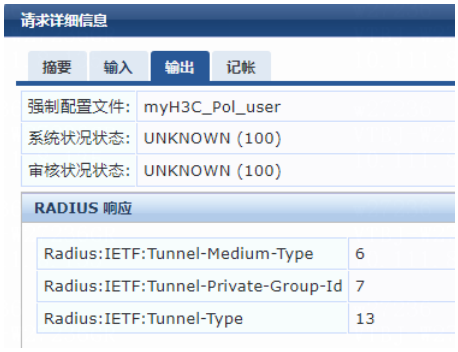
图87 配置文件



8.3.3 验证配置

(1) 用户上线后服务器显示如图 88。

图88 用户上线后服务器显示



(2) 用户上线后设备显示信息（以 802.1X 认证为例）

在设备上通过 **display dot1x connection** 命令可以查看上线 802.1X 用户的信息。其中 Authorization untagged VLAN:字段显示成功下发授权 VLAN 7。

```
[Device]display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: user
User access state: Successful
Authentication domain: bbb
Authentication method: EAP
Initial VLAN: 144
Authorization untagged VLAN: 7
Authorization tagged VLAN list: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: N/A
Online from: 2022/05/11 18:42:15
Online duration: 0h 0m 45s
```

(3) 用户上线后设备显示信息（以 MAC 地址认证为例）

在设备上通过 **display mac-authentication connection** 命令可以查看上线 MAC 地址认证用户的信息。其中 Authorization untagged VLAN:字段显示成功下发授权 VLAN 7。

```
[Device]display mac-authentication connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: user
User access state: Successful
Authentication domain: mac-auth
IPv4 address: 101.0.145.39
Initial VLAN: 144
Authorization untagged VLAN: 7
Authorization tagged VLAN: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: N/A
Online from: 2022/05/13 10:06:50
Online duration: 0h 0m 16s
```

8.4 授权VLAN名称配置步骤与验证

8.4.1 配置 Switch

MAC 地址认证用户，Swtich 上的配置请参考 5.3.1 配置 Switch。

802.1X 认证用户，Swtich 上的配置请参考 6.3.1 配置 Switch。

授权 VLAN 名称时，该 VLAN 必须在设备上已经创建，并且设置了 VLAN 名称。

```
[Device] vlan 8
[Device-vlan8] name vl
```

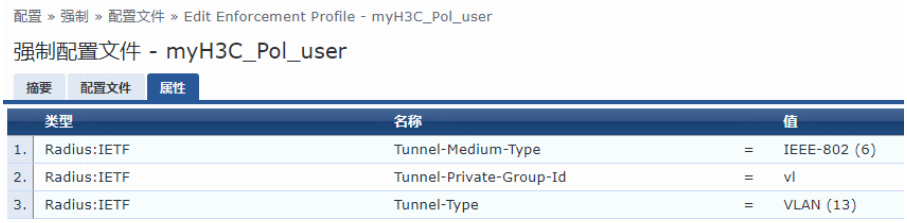
8.4.2 配置 ClearPass

MAC 地址认证用户，服务器上的配置请参考 5.3.2 配置 ClearPass。

802.1X 认证用户，服务器上的配置请参考 6.3.2 配置 ClearPass。

只需将“配置文件”的“属性”参考图 89 修改即可。

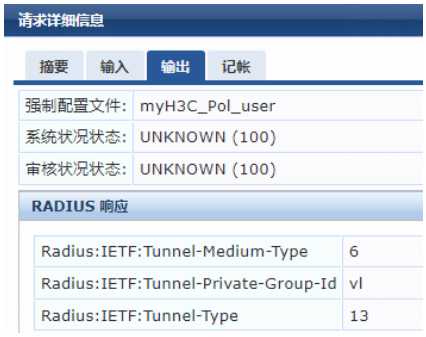
图89 配置文件



8.4.3 验证配置

(1) 用户上线后服务器显示如图 90。

图90 用户上线后服务器显示



(2) 用户上线后设备显示信息（以 802.1X 认证为例）

在设备上通过 **display dot1x connection** 命令可以查看上线 802.1X 用户的信息。其中 Authorization untagged VLAN:字段显示成功下发授权 VLAN 8（该 VLAN 名称为 vl）。

```
[Device] display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: user
User access state: Successful
Authentication domain: bbb
Authentication method: EAP
Initial VLAN: 144
Authorization untagged VLAN: 8
Authorization tagged VLAN list: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: N/A
```

```
Online from: 2022/05/11 18:52:05
Online duration: 0h 0m 11s
```

(3) 用户上线后设备显示信息（以 MAC 地址认证为例）

在设备上通过 **display mac-authentication connection** 命令可以查看上线 MAC 地址认证用户的信息。其中 Authorization untagged VLAN:字段显示成功下发授权 VLAN 8（该 VLAN 名称为 vl）。

```
[Device]display mac-authentication connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: user
User access state: Successful
Authentication domain: mac-auth
IPv4 address: 101.0.145.39
Initial VLAN: 144
Authorization untagged VLAN: 8
Authorization tagged VLAN: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: N/A
Online from: 2022/05/13 10:08:19
Online duration: 0h 0m 4s
```

8.5 授权VLAN组名配置步骤与验证

8.5.1 配置 Switch

MAC 地址认证用户，Swtich 上的配置请参考 5.3.1 配置 Switch。

802.1X 认证用户，Swtich 上的配置请参考 6.3.1 配置 Switch。

下发的 VLAN 组必须在设备上已经创建，会将该组 VLAN 组中 ID 最小的 VLAN 授权给当前的认证用户，且后续该端口上的认证用户均被加入该授权 VLAN。

```
[Device] vlan-group temp
[Device-vlan-group-temp] vlan-list 100 101 200 300
```

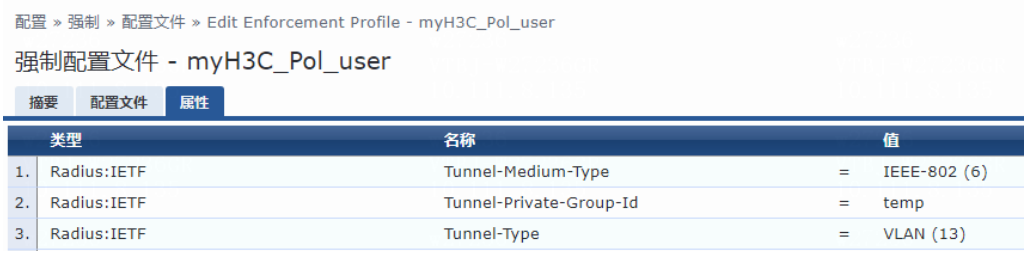
8.5.2 配置 ClearPass

MAC 地址认证用户，服务器上的配置请参考 5.3.2 配置 ClearPass。

802.1X 认证用户，服务器上的配置请参考 6.3.2 配置 ClearPass。

只需将“配置文件”的“属性”参考图 91 修改即可。

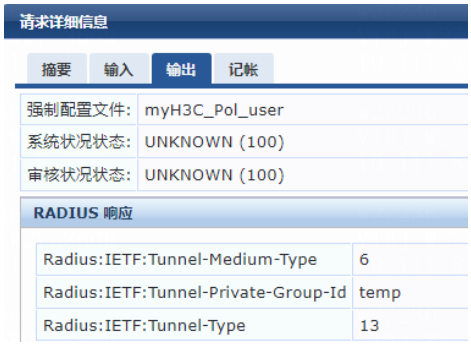
图91 配置文件



8.5.3 验证配置

(1) 用户上线后服务器显示如图 92。

图92 用户上线后服务器显示



(2) 用户上线后设备上显示信息（以 802.1X 认证为例）

在设备上通过 **display dot1x connection** 命令可以查看上线 802.1X 用户的信息。其中 Authorization untagged VLAN:字段显示成功下发授权 VLAN 100。

```
[Device]display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: user
User access state: Successful
Authentication domain: bbb
Authentication method: EAP
Initial VLAN: 144
Authorization untagged VLAN: 100
Authorization tagged VLAN list: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: N/A
```

```
Online from: 2022/05/11 18:59:08
Online duration: 0h 0m 8s
```

(3) 用户上线后设备显示信息（以 MAC 地址认证为例）

在设备上通过 **display mac-authentication connection** 命令可以查看上线 MAC 地址认证用户的信息。其中 Authorization untagged VLAN:字段显示成功下发授权 VLAN 100。

```
[Device]display mac-authentication connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: user
User access state: Successful
Authentication domain: mac-auth
IPv4 address: 101.0.145.39
Initial VLAN: 144
Authorization untagged VLAN: 100
Authorization tagged VLAN: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: N/A
Online from: 2022/05/13 10:09:19
Online duration: 0h 0m 1s
```

8.6 授权Multi VLAN配置步骤与验证

8.6.1 配置 Switch

MAC 地址认证用户，Swtich 上的配置请参考 5.3.1 配置 Switch。

802.1X 认证用户，Swtich 上的配置请参考 6.3.1 配置 Switch。

服务器授权多个 VLAN 名称时，所有 VLAN 必须在设备上均已经创建，并且均设置了 VLAN 名称。

```
[Device] vlan 100
[Device-vlan100] name v1
[Device-vlan100] quit
[Device] vlan 200
[Device-vlan200] name v2
[Device-vlan200] quit
```

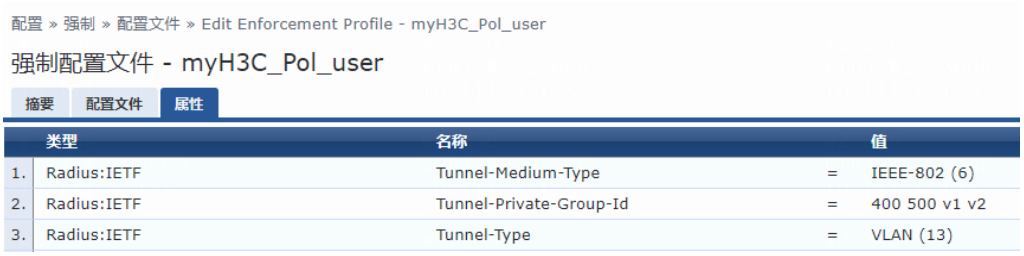
8.6.2 配置 ClearPass

MAC 地址认证用户，服务器上的配置请参考 5.3.2 配置 ClearPass。

802.1X 认证用户，服务器上的配置请参考 6.3.2 配置 ClearPass。

只需将“配置文件”的“属性”参考图 93 修改即可。

图93 配置文件



8.6.3 验证配置

(1) 用户上线后服务器显示如图 94。

图94 用户上线后服务器显示

(2) 用户上线后设备上显示信息（以 802.1X 认证为例）

在设备上通过 **display dot1x connection** 命令可以查看上线 802.1X 用户的信息。其中 Authorization untagged VLAN:字段显示成功下发授权 VLAN 100。

说明

若认证服务器下发的授权 VLAN 信息为一个包含若干 VLAN 编号以及若干 VLAN 名称的字符串，则设备首先将其解析为一组 VLAN ID，然后采用与解析一个 VLAN 组名相同的解析逻辑选择一个授权 VLAN。通常是按 VLAN ID 最小选择。

```
[Device]display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: user
User access state: Successful
Authentication domain: bbb
Authentication method: EAP
Initial VLAN: 144
Authorization untagged VLAN: 100
```

```
Authorization tagged VLAN list: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: N/A
Online from: 2022/05/11 19:07:58
Online duration: 0h 0m 14s
```

8.7 授权Auto VLAN规则1配置步骤与验证

说明

Auto VLAN 规则下，服务器下发的授权 VLAN 仅对端口链路类型为 Hybrid 或 Trunk，且 802.1X 接入控制方式为 Port-based 的端口有效。若端口链路类型为 access，则用户上线失败。

8.7.1 配置 Switch

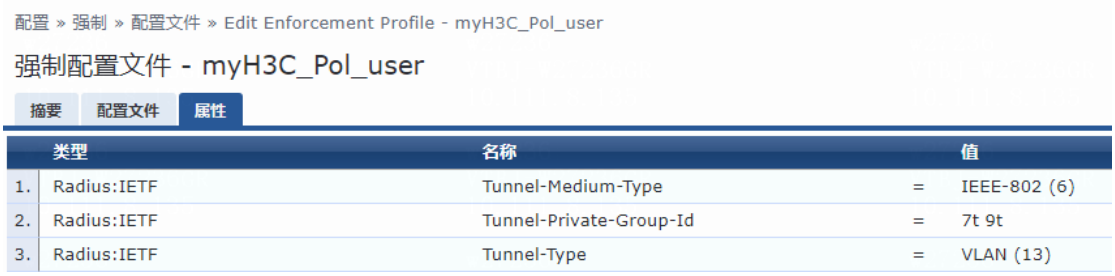
Swtich 上的配置请参考 6.3.1 配置 Switch。

8.7.2 配置 ClearPass

服务器上的配置请参考 6.3.2 配置 ClearPass。

只需将“配置文件”的“属性”参考图 95 修改即可。

图95 配置文件

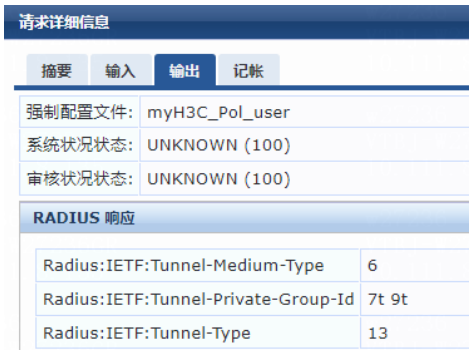


8.7.3 验证配置

用户使用 802.1X 认证方式上线。

(1) 用户上线后服务器显示如 8.7.3 (1)图 96。

图96 用户上线后服务器显示



(2) 用户上线后设备上信息

在设备上通过 **display dot1x connection** 命令可以查看上线 802.1X 用户的信息。其中 Authorization tagged VLAN 字段显示成功下发授权 VLAN 7 和 VLAN 9。不存在 untagged 的授权 VLAN，则不修改端口的缺省 VLAN。

```
[Device] display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: user
User access state: Successful
Authentication domain: bbb
Authentication method: EAP
Initial VLAN: 144
Authorization untagged VLAN: 144
Authorization tagged VLAN list: 7 9
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: N/A
Online from: 2022/05/12 09:57:20
Online duration: 0h 18m 37s
```

8.8 授权Auto VLAN规则2配置步骤与验证

8.8.1 配置 Switch

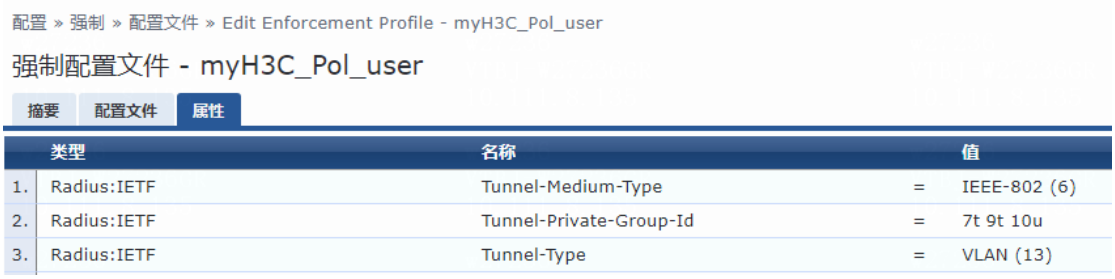
Swtich 上的配置请参考 6.3.1 配置 Switch。

8.8.2 配置 ClearPass

服务器上的配置请参考 6.3.2 配置 ClearPass。

只需将“配置文件”的“属性”参考图 97 修改即可。

图97 配置文件



8.8.3 验证配置

用户使用 802.1X 认证方式上线。

(1) 用户上线后服务器上显示如 8.8.3 (1)图 98。

图98 用户上线后服务器显示

(2) 用户上线后设备上显示信息

在设备上通过 **display dot1x connection** 命令可以查看上线 802.1X 用户的信息。其中 Authorization tagged VLAN 字段显示成功下发授权 VLAN 7 和 VLAN 9。存在 untagged 的授权 VLAN，端口的缺省 VLAN 将被修改为 untagged 的授权 VLAN。

```
[Device]display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: user
User access state: Successful
Authentication domain: bbb
Authentication method: EAP
Initial VLAN: 144
Authorization untagged VLAN: 10
Authorization tagged VLAN list: 7 9
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
```

```
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: N/A
Online from: 2022/05/12 10:21:00
Online duration: 0h 0m 3s
```

8.9 授权Auto VLAN规则3配置步骤与验证

8.9.1 配置 Switch

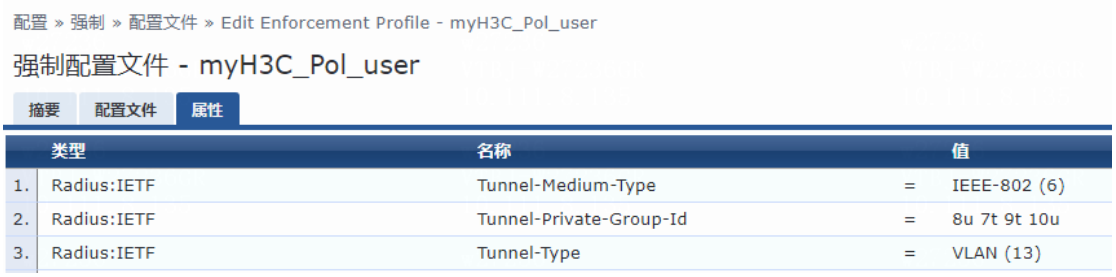
Swtich 上的配置请参考 6.3.1 配置 Switch。

8.9.2 配置 ClearPass

服务器上的配置请参考 6.3.2 配置 ClearPass。

只需将“配置文件”的“属性”参考图 99 修改即可。

图99 配置文件



8.9.3 验证配置

用户使用 802.1X 认证方式上线。

(1) 用户上线后服务器上显示如 8.9.3 (1)图 100。

图100 用户上线后服务器显示

(2) 用户上线后设备上显示

在设备上通过 **display dot1x connection** 命令可以查看上线 802.1X 用户的信息。其中 Authorization tagged VLAN 字段显示成功下发授权 VLAN 7、VLAN 9 和 VLAN 10。授权 VLAN 信息为一个包含若干个“VLAN ID+后缀”形式的字符串，则只有第一个不携带后缀或者携带 untagged 后缀的 VLAN 将被解析为唯一的 untagged 的授权 VLAN（本例为 VLAN 8），其余 VLAN 都被解析为 tagged 的授权 VLAN，端口的缺省 VLAN 将被修改为 untagged 的授权 VLAN。

```
[Device] display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: user
User access state: Successful
Authentication domain: bbb
Authentication method: EAP
Initial VLAN: 144
Authorization untagged VLAN: 8
Authorization tagged VLAN list: 7 9-10
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: N/A
Online from: 2022/05/12 10:26:36
Online duration: 0h 0m 4s
```

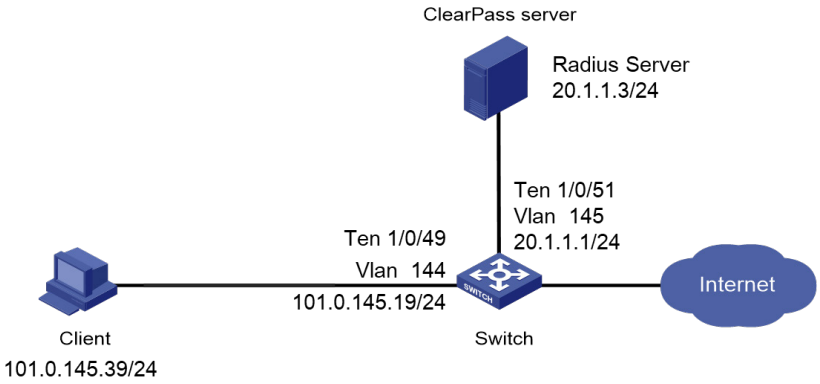
9 授权 ACL 对接配置举例

9.1 组网需求

如图 101 所示，Client 和 ClearPass 服务器通过 Switch 建立连接，设备管理员希望对 Client 进行 802.1X 认证或者 MAC 地址认证或 Portal 认证，以控制其对网络资源的访问，具体要求如下：

- 采用 ClearPass 作为 RADIUS 服务器。
- 通过 ClearPass 授权下发 ACL。

图101 授权 ACL 组网图



9.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch：S5130-HI，R3507P02
- Aruba 认证服务器：ClearPass CPPM V6.9.7

9.3 配置步骤

9.3.1 配置 Switch

MAC 地址认证用户，Swtich 上的配置请参考 5.3.1 配置 Switch。

802.1X 认证用户，Swtich 上的配置请参考 6.3.1 配置 Switch。

授权 ACL 名称时，该 ACL 必须在设备上已经创建才会生效。

在设备上创建 ACL，并配置规则。

```
[Device] acl advanced 3999
[Device-acl-ipv4-adv-3999] rule 0 permit ip source any
```

9.3.2 配置 ClearPass

MAC 地址认证用户，服务器上的配置请参考 5.3.2 配置 ClearPass。

802.1X 认证用户，服务器上的配置请参考 6.3.2 配置 ClearPass。

只需将“配置文件”的“属性”参考图 102 修改即可。

图102 配置文件

注：Filter-Id 取值为数字，则按照 ACL Number 处理，取值不全为数字，则按照 User Profile 处理。

9.4 验证配置

用户使用不同认证方式上线（MAC 地址认证、802.1X 认证、Portal 认证）。

(1) 用户上线后服务器上显示，图 78。

图103 用户上线后服务器显示

(2) 用户上线后设备上显示

可以看到服务器下发的 ACL 成功下发到设备上。

```
[Device]display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: user
User access state: Successful
Authentication domain: bbb
Authentication method: EAP
Initial VLAN: 144
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
Authorization ACL number/name: 3999
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: N/A
Online from: 2022/05/12 10:34:53
Online duration: 0h 0m 13s
```

10 授权 User-Profile 对接配置举例

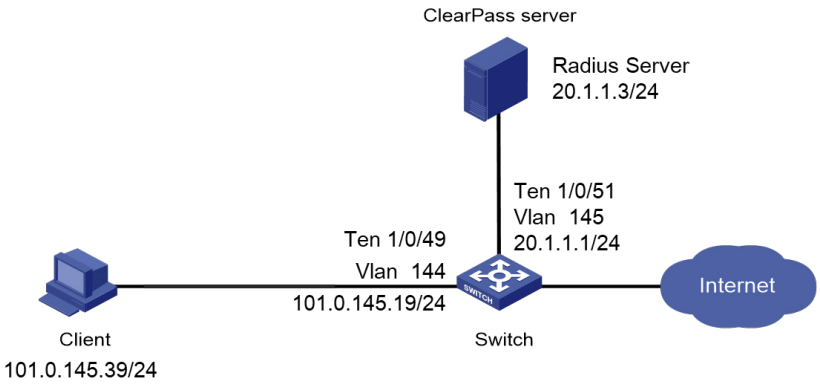
10.1 组网需求

如图 104 所示，Client 和 ClearPass 服务器通过 Switch 建立连接，设备管理员希望对 Client 进行 802.1X 认证或者 MAC 地址认证或 Portal 认证，以控制其对网络资源的访问，具体要求如下：

- 采用 ClearPass 作为 RADIUS 服务器。

- 通过 ClearPass 授权下发 User-Profile。

图104 授权 User-Profile 组网图



10.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch：S5130-HI，R3507P02
- Aruba 认证服务器：ClearPass CPPM V6.9.7

10.3 配置步骤

10.3.1 配置 Switch

802.1X 认证用户，Swtich 上的配置请参考 6.3.1 配置 Switch。

授权 User-Profile 名称时，该 User-Profile 必须在设备上已经创建才会生效。

创建对 User 的速率进行限制的 QoS 策略。

创建流分类 class，匹配所有报文。

```
[Device] traffic classifier class
[Device-classifier-class] if-match any
[Device-classifier-class] quit
```

创建流行为 for_ub，动作为流量监管，cir 为 10000kbps。

```
[Device] traffic behavior for_ub
[Device-behavior-for_ub] car cir 10000
[Device-behavior-for_ub] quit
```

创建 QoS 策略 for_ub，将流分类和流行为进行关联。

```
[Device] qos policy for_ub
[Device-qospolicy-for_ub] classifier class behavior for_ub
[Device-qospolicy-for_ub] quit
```

为 User 创建 User Profile，并应用 QoS 策略。

```
[Device] user-profile ub
[Device-user-profile-ub] qos apply policy for_ub inbound
[Device-user-profile-ub] quit
```

10.3.2 配置 ClearPass

802.1X 认证用户，服务器上的配置请参考 6.3.2 配置 ClearPass。

只需将“配置文件”的“属性”参考图 105 修改即可。

图105 配置文件

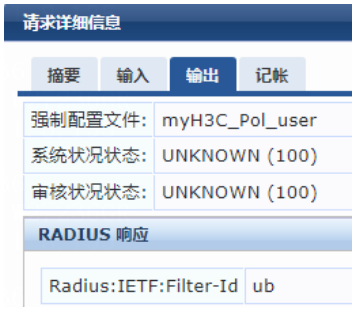
说明

Filter-Id 取值为数字，则按照 ACL Number 处理，取值不全为数字，则按照 User Profile 处理。

10.4 验证配置

(1) 用户上线后服务器上显示如图 106(1)图 106。

图106 用户上线后服务器显示



(2) 用户上线后设备上显示

在设备上通过 **display dot1x connection** 命令可以查看上线 802.1X 用户的信息。其中 Authorization user profile 字段显示成功下发名称为“ub”授权 User Profile。

```
[Device] display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: user
User access state: Successful
Authentication domain: bbb
Authentication method: EAP
Initial VLAN: 144
```

```
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: ub
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: N/A
Online from: 2022/05/12 10:52:34
Online duration: 0h 0m 4s
```

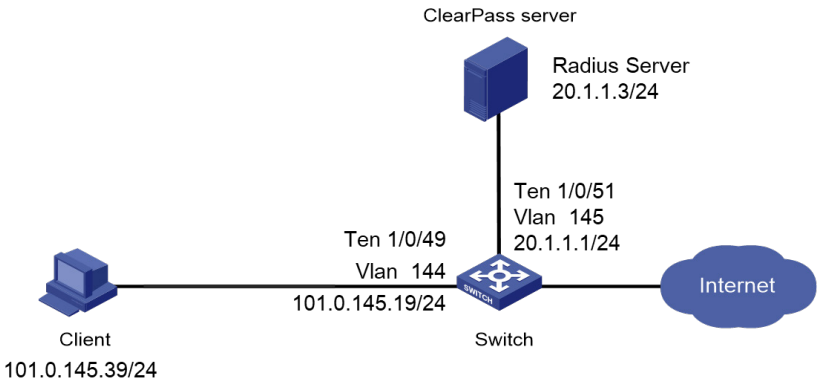
11 授权 CAR 对接配置举例

11.1 组网需求

如图 107 所示，Client 和 ClearPass 服务器通过 Switch 建立连接，设备管理员希望对 Client 进行 802.1X 认证或者 MAC 地址认证，以控制其对网络资源的访问，具体要求如下：

- 采用 ClearPass 作为 RADIUS 服务器。
- 通过 ClearPass 授权下发 CAR（Average input rate、Peak input rate、Average output rate、Peak output rate）。

图107 授权 CAR 组网图



11.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch：S5130-HI，R3507P02
- Aruba 认证服务器：ClearPass CPPM V6.9.7

11.3 配置步骤

11.3.1 配置 Switch

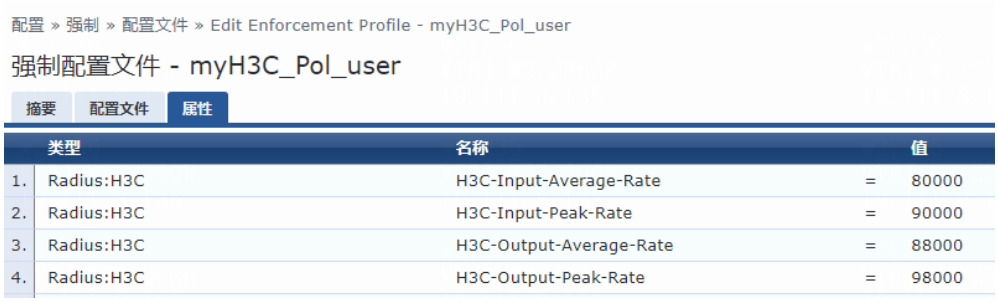
802.1X 认证用户，Swtich 上的配置请参考 6.3.1 配置 Switch。

11.3.2 配置 ClearPass

802.1X 认证用户，服务器上的配置请参考 6.3.2 配置 ClearPass。

只需将“配置文件”的“属性”参考图 108 修改即可。

图108 配置文件



	类型	名称		值
1.	Radius:H3C	H3C-Input-Average-Rate	=	80000
2.	Radius:H3C	H3C-Input-Peak-Rate	=	90000
3.	Radius:H3C	H3C-Output-Average-Rate	=	88000
4.	Radius:H3C	H3C-Output-Peak-Rate	=	98000

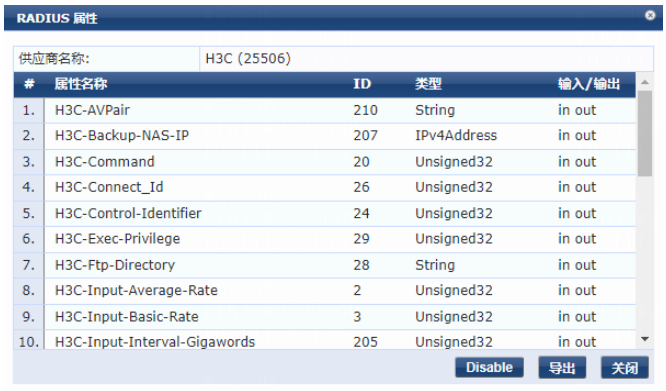
若服务器上没有 Output-Average-Rate 和 Output-Peak-Rate 需要自己在服务器的词典里添加，添加方式如下：

如图 109 所示，依次点击“管理 » 字典 » RADIUS » H3C”。

图109 RAIUS 字典项添加示意图一

#	供应商名称	供应商 ID	供应商前缀	已启用
41.	Extreme	1916	Extreme	false
42.	F5	3375	F5	false
43.	Fortinet	12356	Fortinet	false
44.	Foundry	1991	Foundry	false
45.	Freeswitch	27880	Freeswitch	false
46.	Gandalf	64	Gandalf	false
47.	Gemtek	10529	Gemtek	false
48.	H3C	25506	H3C	true

图110 RAIUS 字典项添加示意图二

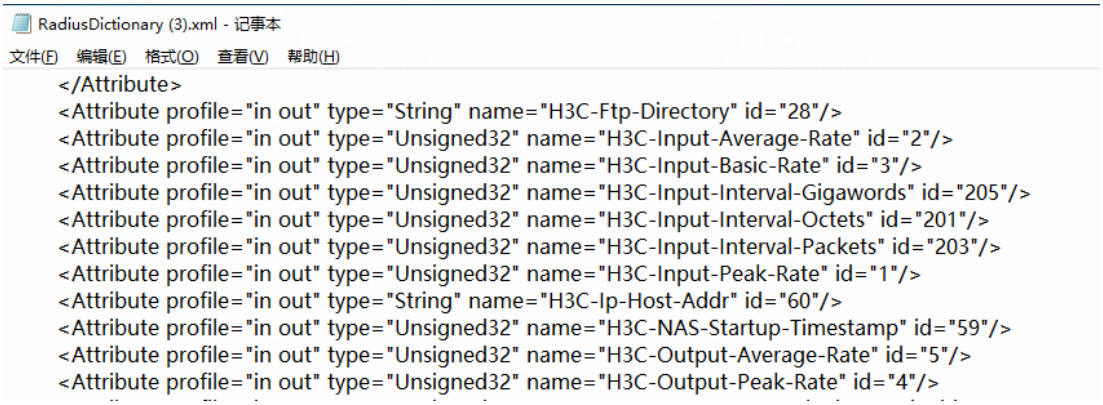


#	属性名称	ID	类型	输入/输出
1.	H3C-AVPair	210	String	in out
2.	H3C-Backup-NAS-IP	207	IPv4Address	in out
3.	H3C-Command	20	Unsigned32	in out
4.	H3C-Connect_Id	26	Unsigned32	in out
5.	H3C-Control-Identifier	24	Unsigned32	in out
6.	H3C-Exec-Privilege	29	Unsigned32	in out
7.	H3C-Ftp-Directory	28	String	in out
8.	H3C-Input-Average-Rate	2	Unsigned32	in out
9.	H3C-Input-Basic-Rate	3	Unsigned32	in out
10.	H3C-Input-Interval-Gigawords	205	Unsigned32	in out

点击“导出”按钮，将内容导出。

打开导出的文件，如图 111。

图111 导出后的文件



参照“Input-Average-Rate”和“Input-Peak-Rate”添加“Output-Average-Rate”和“Output-Peak-Rate”这两条属性，之后将该文件保存导入词典即可。

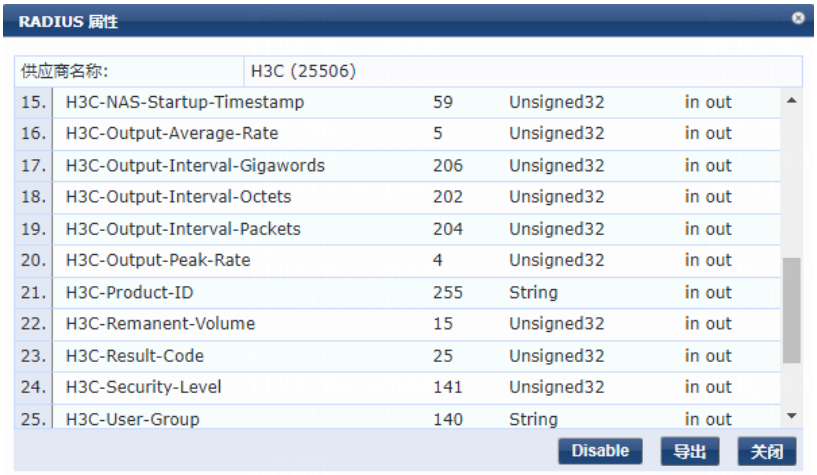
如图 112、图 113 所示，依次点击“管理 » 字典 » RADIUS » 导入”。

图112 导入修改后的文件示意图一

图113 导入修改后的文件示意图二

点击“导入”按钮后，如图 114 所示。

图114 导入成功

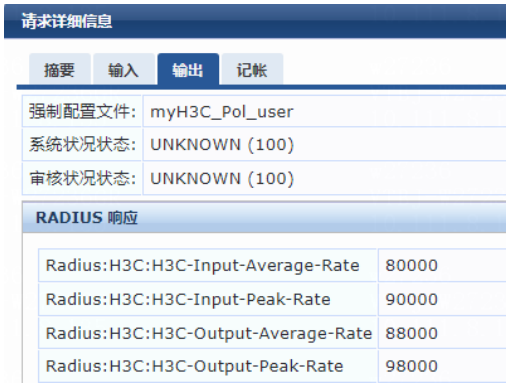


查看 H3C 词典，发现属性 Output-Average-Rate 和 Output-Peak-Rate 已经导入。

11.4 验证配置

(1) 用户上线后服务器上显示如图 115。

图115 用户上线后服务器显示



(2) 用户上线后设备上显示

在设备上通过 **display dot1x connection** 命令可以查看上线 802.1X 用户的信息。其中 Authorization CAR 字段显示成功下发授权 CAR。

```
[Device] display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: user
User access state: Successful
Authentication domain: bbb
Authentication method: EAP
Initial VLAN: 144
Authorization untagged VLAN: N/A
```

```
Authorization tagged VLAN list: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR:
  Average input rate: 80000 bps
  Peak input rate: 90000 bps
  Average output rate: 88000 bps
  Peak output rate: 98000 bps
Authorization URL: N/A
Termination action: Default
Session timeout period: N/A
Online from: 2022/05/12 10:43:24
Online duration: 0h 0m 4s
```

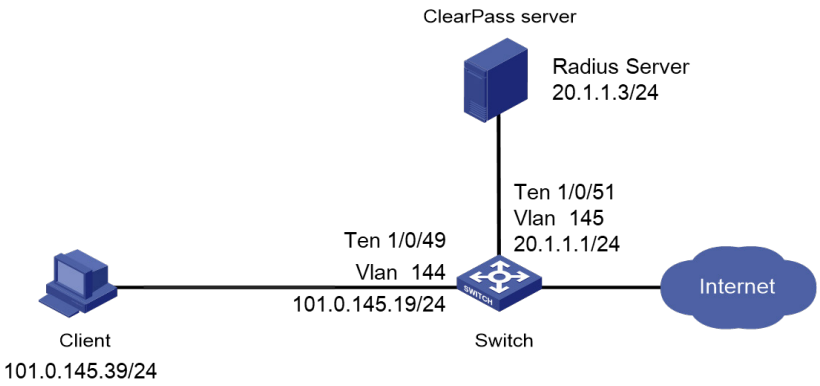
12 重认证对接配置举例

12.1 组网需求

如图 116 所示，Client 和 ClearPass 服务器通过 Switch 建立连接，设备管理员希望对 Client 进行 802.1X 认证或者 MAC 地址认证，以控制其对网络资源的访问，具体要求如下：

- 采用 ClearPass 作为 RADIUS 服务器。
- 通过 ClearPass 授权下发 Session-Timeout、Termination-Action。

图116 授权 Session-Timeout、Termination-Action 组网图



12.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch：S5130-HI，R3507P02
- Aruba 认证服务器：ClearPass CPPM V6.9.7

12.3 用户会话超时后重认证配置步骤与验证（一）

说明

当认证服务器下发了用户会话超时时长，且指定的会话终止动作（Termination-Action）为要求用户进行重认证 RADIUS-Request (1)，则无论设备上是否开启周期性重认证功能，端口都会在用户会话超时时长到达后对该用户发起重认证。

12.3.1 配置 Switch

MAC 地址认证用户，Swtich 上的配置请参考 5.3.1 配置 Switch。

802.1X 认证用户，Swtich 上的配置请参考 6.3.1 配置 Switch。

12.3.2 配置 ClearPass

MAC 地址认证用户，服务器上的配置请参考 5.3.2 配置 ClearPass。

802.1X 认证用户，服务器上的配置请参考 6.3.2 配置 ClearPass。

只需将“配置文件”的“属性”参考图 117 修改即可。

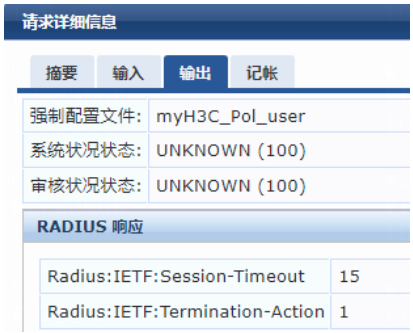
图117 配置文件

12.3.3 验证配置

用户使用不同认证方式上线（MAC 地址认证、802.1X 认证）。

(1) 用户上线后服务器上显示如图 118。

图118 用户上线后服务器显示



(2) 用户上线后设备上显示（以 802.1X 认证为例）

在设备上通过 **display dot1x connection** 命令可以查看上线 802.1X 用户的信息。Session timeout period 字段显示服务器下发的会话超时时长为 15 秒，该时间到达之后，用户所在的会话将会被删除，之后，对该用户所采取的动作为 Termination action 字段显示的 Radius-request，即：会话超时时长到达后，服务器要求 802.1X 用户进行重认证。

```
[Device] display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: user
User access state: Successful
Authentication domain: bbb
Authentication method: EAP
Initial VLAN: 144
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Radius-request
Session timeout period: 15 s
Online from: 2022/05/12 11:02:14
Online duration: 0h 0m 4s
```

(3) 用户上线后设备上显示（以 MAC 认证为例）

在设备上通过 **display mac-authentication connection** 命令可以查看上线 MAC 地址认证用户的信息。Session timeout period 字段显示服务器下发的会话超时时长为 15 秒，该时间到达之后，用户所在的会话将会被删除，之后，对该用户所采取的动作为 Termination action 字段显示的 Radius-request，即：会话超时时长到达后，服务器要求 802.1X 用户进行重认证。

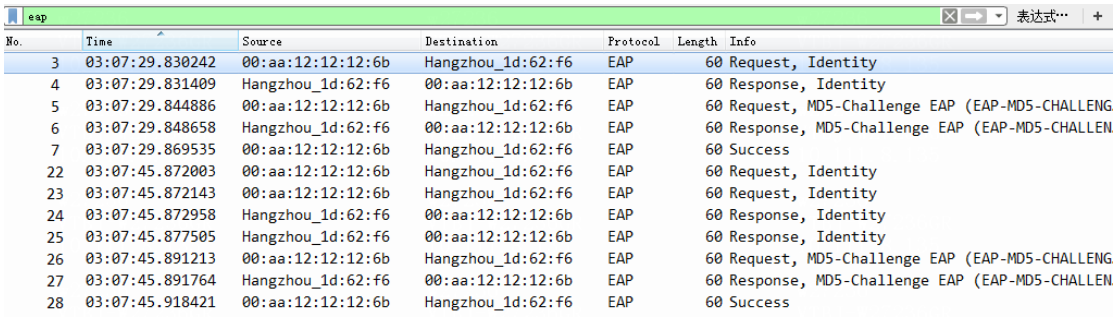
```
[Device] display mac-authentication connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: user
User access state: Successful
Authentication domain: mac-auth
IPv4 address: 101.0.145.39
Initial VLAN: 144
Authorization untagged VLAN: N/A
Authorization tagged VLAN: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
```

```
Authorization URL: N/A
Termination action: Radius-request
Session timeout period: 15 sec
Online from: 2022/05/13 11:20:20
Online duration: 0h 0m 4s
```

(4) 抓包查看用户重认证

对于 802.1X 认证，根据配置的用户会话超时时长，15 秒后用户需要重认证，并认证成功。

图119 报文捕获示意图一

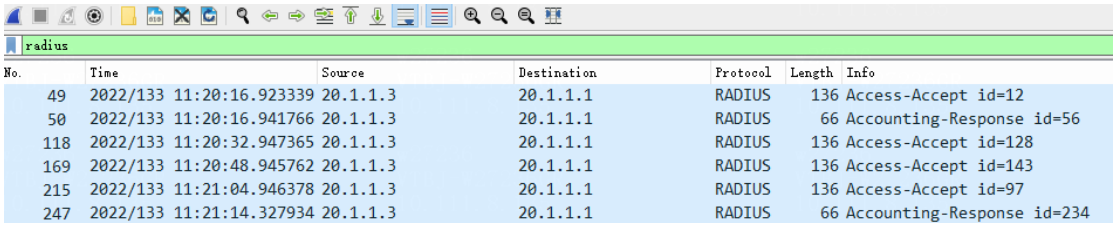


eap

No.	Time	Source	Destination	Protocol	Length	Info
3	03:07:29.830242	00:aa:12:12:12:6b	Hangzhou_1d:62:f6	EAP	60	Request, Identity
4	03:07:29.831409	Hangzhou_1d:62:f6	00:aa:12:12:12:6b	EAP	60	Response, Identity
5	03:07:29.844886	00:aa:12:12:12:6b	Hangzhou_1d:62:f6	EAP	60	Request, MD5-Challenge EAP (EAP-MD5-CHALLENG
6	03:07:29.848658	Hangzhou_1d:62:f6	00:aa:12:12:12:6b	EAP	60	Response, MD5-Challenge EAP (EAP-MD5-CHALLEN
7	03:07:29.869535	00:aa:12:12:12:6b	Hangzhou_1d:62:f6	EAP	60	Success
22	03:07:45.872003	00:aa:12:12:12:6b	Hangzhou_1d:62:f6	EAP	60	Request, Identity
23	03:07:45.872143	00:aa:12:12:12:6b	Hangzhou_1d:62:f6	EAP	60	Request, Identity
24	03:07:45.872958	Hangzhou_1d:62:f6	00:aa:12:12:12:6b	EAP	60	Response, Identity
25	03:07:45.877505	Hangzhou_1d:62:f6	00:aa:12:12:12:6b	EAP	60	Response, Identity
26	03:07:45.891213	00:aa:12:12:12:6b	Hangzhou_1d:62:f6	EAP	60	Request, MD5-Challenge EAP (EAP-MD5-CHALLENG
27	03:07:45.891764	Hangzhou_1d:62:f6	00:aa:12:12:12:6b	EAP	60	Response, MD5-Challenge EAP (EAP-MD5-CHALLEN
28	03:07:45.918421	00:aa:12:12:12:6b	Hangzhou_1d:62:f6	EAP	60	Success

对于 MAC 地址认证，根据配置的用户会话超时时长，15 秒后用户需要重认证，并认证成功。

图120 报文捕获示意图二



radius

No.	Time	Source	Destination	Protocol	Length	Info
49	2022/133 11:20:16.923339	20.1.1.3	20.1.1.1	RADIUS	136	Access-Accept id=12
50	2022/133 11:20:16.941766	20.1.1.3	20.1.1.1	RADIUS	66	Accounting-Response id=56
118	2022/133 11:20:32.947365	20.1.1.3	20.1.1.1	RADIUS	136	Access-Accept id=128
169	2022/133 11:20:48.945762	20.1.1.3	20.1.1.1	RADIUS	136	Access-Accept id=143
215	2022/133 11:21:04.946378	20.1.1.3	20.1.1.1	RADIUS	136	Access-Accept id=97
247	2022/133 11:21:14.327934	20.1.1.3	20.1.1.1	RADIUS	66	Accounting-Response id=234

12.4 用户会话超时后强制下线配置步骤与验证（一）

说明

当认证服务器下发了用户会话超时时长，且指定的会话终止动作（Termination-Action）为要求用户强制下线 Default (0)时，若设备上未开启周期性重认证功能，则端口会在用户会话超时时长到达后强制该用户下线。

12.4.1 配置 Switch

MAC 地址认证用户，Swtich 上的配置请参考 5.3.1 配置 Switch。

802.1X 认证用户，Swtich 上的配置请参考 6.3.1 配置 Switch。

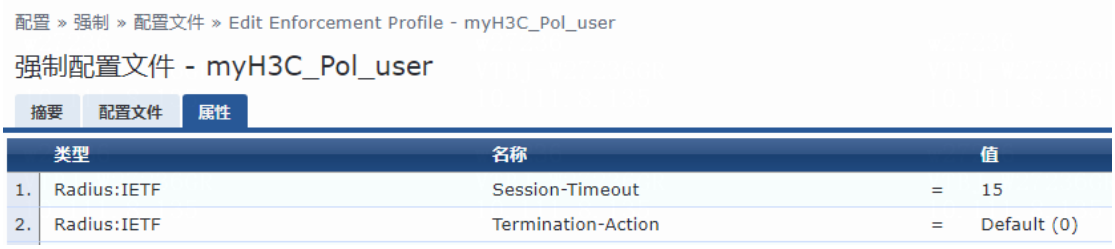
12.4.2 配置 ClearPass

MAC 地址认证用户，服务器上的配置请参考 5.3.2 配置 ClearPass。

802.1X 认证用户，服务器上的配置请参考 6.3.2 配置 ClearPass。

只需将“配置文件”的“属性”参考图 121 修改即可。

图121 配置文件



12.4.3 验证配置

用户使用不同认证方式上线（MAC 地址认证、802.1X 认证）。

(1) 用户上线后服务器上显示如图 122，15 秒后用户被强制下线，如图 123。

图122 用户上线后服务器显示

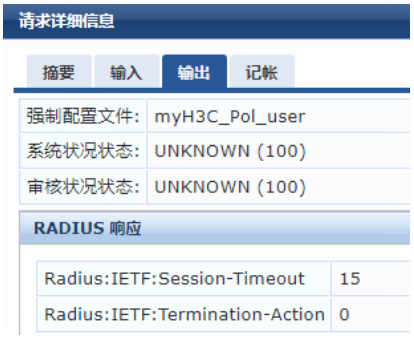
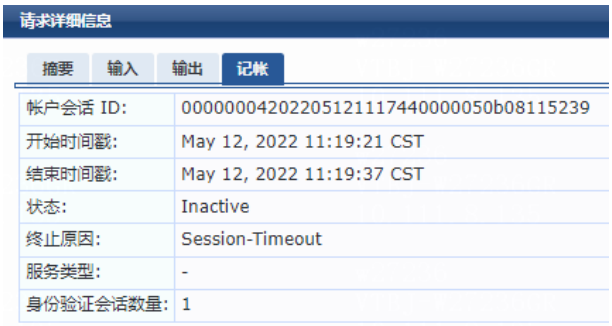


图123 用户被强制下线



(2) 用户上线后设备上显示（以 802.1X 认证为例）

在设备上通过 **display dot1x connection** 命令可以查看上线 802.1X 用户的信息。

Session timeout period 字段显示服务器下发的会话超时时长为 15 秒，该时间到达之后，用户

所在的会话将会被删除，之后，对该用户所采取的动作为 Termination action 字段显示的 Default，即：会话超时时长到达后，强制用户下线。

```
[Device]display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: user
User access state: Successful
Authentication domain: bbb
Authentication method: EAP
Initial VLAN: 144
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: 15 s
Online from: 2022/05/12 11:19:21
Online duration: 0h 0m 4s
```

(3) 用户上线后设备上显示（以 MAC 地址认证为例）

在设备上通过 **display mac-authentication connection** 命令可以查看上线 MAC 地址认证用户的信息。Session timeout period 字段显示服务器下发的会话超时时长为 15 秒，该时间到达之后，用户所在的会话将会被删除，之后，对该用户所采取的动作为 Termination action 字段显示的 Default，即：会话超时时长到达后，强制用户下线。

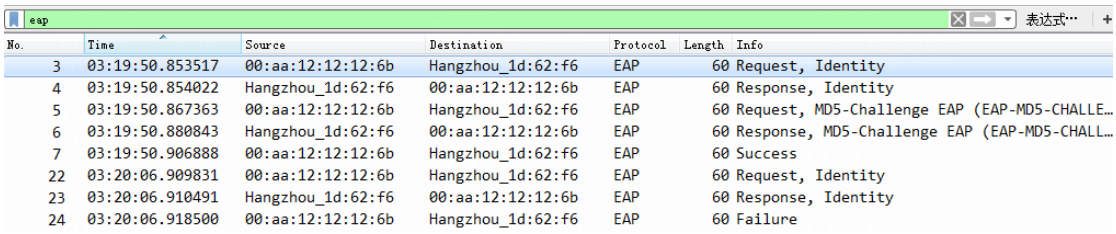
```
[Device] display mac-authentication connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: user
User access state: Successful
Authentication domain: mac-auth
IPv4 address: 101.0.145.39
Initial VLAN: 144
Authorization untagged VLAN: N/A
Authorization tagged VLAN: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: 15 sec
```

```
Online from: 2022/05/13 14:33:12
Online duration: 0h 0m 5s
```

(4) 抓包查看用户重认证

对于 802.1X 认证，根据配置的用户会话超时时长，15 秒后用户用户被强制下线。

图124 报文捕获示意图



eap 表达式…

No.	Time	Source	Destination	Protocol	Length	Info
3	03:19:50.853517	00:aa:12:12:12:6b	Hangzhou_1d:62:f6	EAP	60	Request, Identity
4	03:19:50.854022	Hangzhou_1d:62:f6	00:aa:12:12:12:6b	EAP	60	Response, Identity
5	03:19:50.867363	00:aa:12:12:12:6b	Hangzhou_1d:62:f6	EAP	60	Request, MD5-Challenge EAP (EAP-MD5-CHALLE…
6	03:19:50.880843	Hangzhou_1d:62:f6	00:aa:12:12:12:6b	EAP	60	Response, MD5-Challenge EAP (EAP-MD5-CHALL…
7	03:19:50.906888	00:aa:12:12:12:6b	Hangzhou_1d:62:f6	EAP	60	Success
22	03:20:06.909831	00:aa:12:12:12:6b	Hangzhou_1d:62:f6	EAP	60	Request, Identity
23	03:20:06.910491	Hangzhou_1d:62:f6	00:aa:12:12:12:6b	EAP	60	Response, Identity
24	03:20:06.918500	00:aa:12:12:12:6b	Hangzhou_1d:62:f6	EAP	60	Failure

12.5 用户会话超时后重认证配置步骤与验证（二）

说明

当认证服务器下发了用户会话超时时长，且指定的会话终止动作（Termination-Action）为要求用户强制下线 Default (0)，若设备上开启了周期性重认证功能，且设备上配置的重认证定时器值小于用户会话超时时长，则端口会以重认证定时器的值为周期向该端口在线用户发起重认证。

12.5.1 配置 Switch

802.1X 认证用户，Swtich 上的配置请参考 6.3.1 配置 Switch。

MAC 地址认证用户，Swtich 上的配置请参考 5.3.1 配置 Switch。

(1) 对于 802.1X 认证，设备上需要额外加上以下配置：

```
[Device]interface Ten-GigabitEthernet 1/0/49
[Device-Ten-GigabitEthernet1/0/49] dot1x re-authenticate
[Device-Ten-GigabitEthernet1/0/49] dot1x timer reauth-period 60
```

(2) 对于 MAC 地址认证，设备上需要额外加上以下配置：

```
[Device] mac-authentication timer reauth-period 60
[Device] interface Ten-GigabitEthernet 1/0/49
[Device-Ten-GigabitEthernet1/0/49] mac-authentication timer reauth-period 60
[Device-Ten-GigabitEthernet1/0/49] mac-authentication re-authenticate
[Device-Ten-GigabitEthernet1/0/49] quit
```

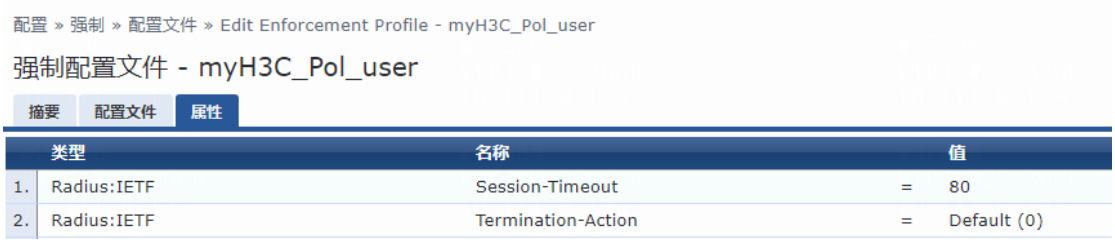
12.5.2 配置 ClearPass

MAC 地址认证用户，服务器上的配置请参考 5.3.2 配置 ClearPass。

802.1X 认证用户，服务器上的配置请参考 6.3.2 配置 ClearPass。

只需将“配置文件”的“属性”参考图 125 修改即可（注意：服务器上配置的会话超时时长为 80 秒，大于设备上配置的周期重认证定时器的时长）。

图125 配置文件

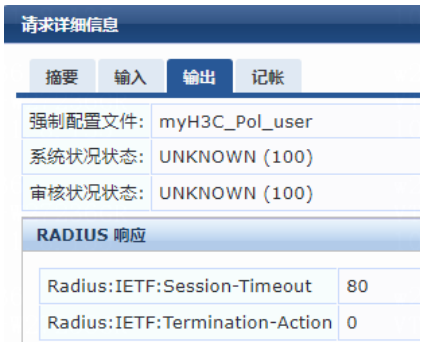


12.5.3 验证配置

用户使用不同认证方式上线（MAC 地址认证、802.1X 认证）。

(1) 用户上线后服务器上显示如图 126。

图126 用户上线后服务器显示



(2) 用户上线后设备上显示（以 802.1X 认证为例）

在设备上通过 **display dot1x connection** 命令可以查看上线 802.1X 用户的信息。Session timeout period 字段显示设备上配置的周期性重认证定时器的时长，到达该时长后，用户所在的会话将会被删除，之后，对该用户所采取的动作为 Termination action 字段显示的 Default，即用户强制下线。

```
[Device] display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: user
User access state: Successful
Authentication domain: bbb
Authentication method: EAP
Initial VLAN: 144
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
```

```
Authorization URL: N/A
Termination action: Default
Session timeout period: 80 s
Online from: 2022/05/12 11:24:50
Online duration: 0h 0m 11s
```

(3) 用户上线后设备上显示（以 MAC 地址认证为例）

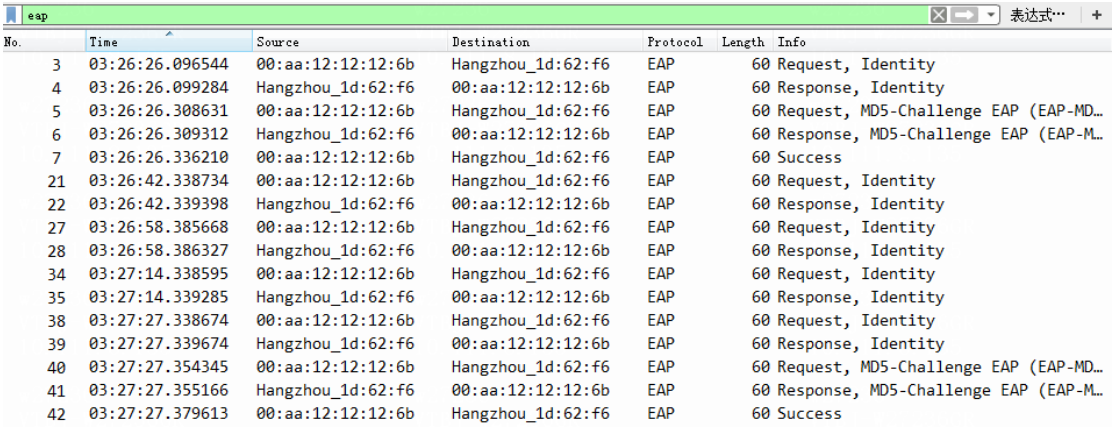
在设备上通过 **display mac-authentication connection** 命令可以查看上线 MAC 地址认证用户的信息。Session timeout period 字段显示设备上配置的周期性重认证定时器的时长，到达该时长后，用户所在的会话将会被删除，之后，对该用户所采取的动作为 Termination action 字段显示的 Default，即用户强制下线。

```
[Device] display mac-authentication connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: user
User access state: Successful
Authentication domain: mac-auth
IPv4 address: 101.0.145.39
Initial VLAN: 144
Authorization untagged VLAN: N/A
Authorization tagged VLAN: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: 80 sec
Online from: 2022/05/13 14:55:01
Online duration: 0h 0m 8s
```

(4) 抓包查看用户重认证

对于 802.1X 认证，端口会以重认证定时器的 60 秒为周期向该端口在线 802.1X 用户发起重认证，并且成功上线。

图127 报文捕获示意图一

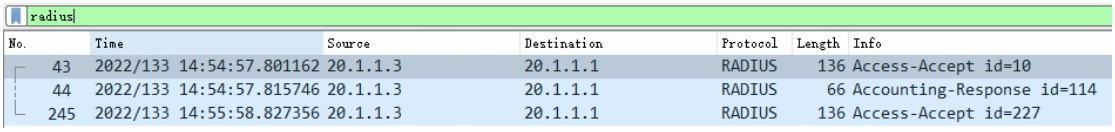


eap 表达式…

No.	Time	Source	Destination	Protocol	Length	Info
3	03:26:26.096544	00:aa:12:12:12:6b	Hangzhou_1d:62:f6	EAP	60	Request, Identity
4	03:26:26.099284	Hangzhou_1d:62:f6	00:aa:12:12:12:6b	EAP	60	Response, Identity
5	03:26:26.308631	00:aa:12:12:12:6b	Hangzhou_1d:62:f6	EAP	60	Request, MD5-Challenge EAP (EAP-MD…
6	03:26:26.309312	Hangzhou_1d:62:f6	00:aa:12:12:12:6b	EAP	60	Response, MD5-Challenge EAP (EAP-M…
7	03:26:26.336210	00:aa:12:12:12:6b	Hangzhou_1d:62:f6	EAP	60	Success
21	03:26:42.338734	00:aa:12:12:12:6b	Hangzhou_1d:62:f6	EAP	60	Request, Identity
22	03:26:42.339398	Hangzhou_1d:62:f6	00:aa:12:12:12:6b	EAP	60	Response, Identity
27	03:26:58.385668	00:aa:12:12:12:6b	Hangzhou_1d:62:f6	EAP	60	Request, Identity
28	03:26:58.386327	Hangzhou_1d:62:f6	00:aa:12:12:12:6b	EAP	60	Response, Identity
34	03:27:14.338595	00:aa:12:12:12:6b	Hangzhou_1d:62:f6	EAP	60	Request, Identity
35	03:27:14.339285	Hangzhou_1d:62:f6	00:aa:12:12:12:6b	EAP	60	Response, Identity
38	03:27:27.338674	00:aa:12:12:12:6b	Hangzhou_1d:62:f6	EAP	60	Request, Identity
39	03:27:27.339674	Hangzhou_1d:62:f6	00:aa:12:12:12:6b	EAP	60	Response, Identity
40	03:27:27.354345	00:aa:12:12:12:6b	Hangzhou_1d:62:f6	EAP	60	Request, MD5-Challenge EAP (EAP-MD…
41	03:27:27.355166	Hangzhou_1d:62:f6	00:aa:12:12:12:6b	EAP	60	Response, MD5-Challenge EAP (EAP-M…
42	03:27:27.379613	00:aa:12:12:12:6b	Hangzhou_1d:62:f6	EAP	60	Success

对于，MAC 地址认证，端口会以重认证定时器的 60 秒为周期向该端口在线用户发起重认证，并且成功上线。

图128 抓包报文捕获示意图二



radius

No.	Time	Source	Destination	Protocol	Length	Info
43	2022/133 14:54:57.801162	20.1.1.3	20.1.1.1	RADIUS	136	Access-Accept id=10
44	2022/133 14:54:57.815746	20.1.1.3	20.1.1.1	RADIUS	66	Accounting-Response id=114
245	2022/133 14:55:58.827356	20.1.1.3	20.1.1.1	RADIUS	136	Access-Accept id=227

12.6 用户会话超时后强制下线配置步骤与验证（二）

说明

当认证服务器下发了用户会话超时时长，且指定的会话终止动作（Termination-Action）为要求用户强制下线 Default (0)，若设备上配置的重认证定时器值大于等于用户会话超时时长，则端口会在用户会话超时时长到达后强制该用户下线。

12.6.1 配置 Switch

802.1X 认证用户，Swtich 上的配置请参考 6.3.1 配置 Switch。

MAC 地址认证用户，Swtich 上的配置请参考 5.3.1 配置 Switch。

(1) 对于 802.1X 认证，设备上需要额外加上以下配置：

```
[Device]interface Ten-GigabitEthernet 1/0/49
[Device-Ten-GigabitEthernet1/0/49] dot1x re-authenticate
[Device-Ten-GigabitEthernet1/0/49] dot1x timer reauth-period 60
```

(2) 对于 MAC 地址认证，设备上需要额外加上以下配置：

```
[Device] mac-authentication timer reauth-period 60
[Device] interface Ten-GigabitEthernet 1/0/49
[Device-Ten-GigabitEthernet1/0/49] mac-authentication timer reauth-period 60
```

```
[Device-Ten-GigabitEthernet1/0/49] mac-authentication re-authenticate
[Device-Ten-GigabitEthernet1/0/49]quit
```

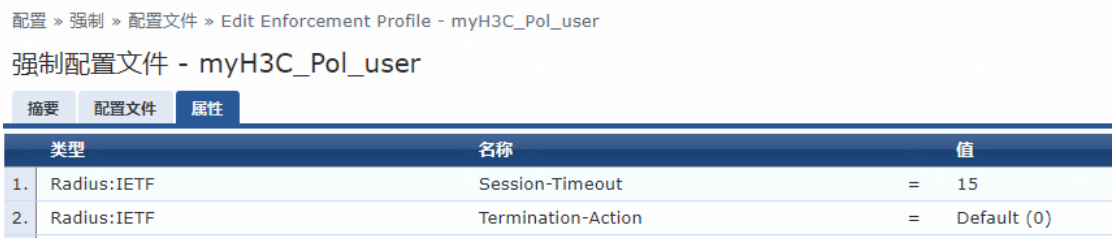
12.6.2 配置 ClearPass

MAC 地址认证用户，服务器上的配置请参考 5.3.2 配置 ClearPass。

802.1X 认证用户，服务器上的配置请参考 6.3.2 配置 ClearPass。

只需将“配置文件”的“属性”参考图 129 修改即可（注意：服务器上配置的会话超时时长为 15 秒，小于设备上配置的周期重认证定时器的时长）。

图129 配置文件



12.6.3 验证配置

用户使用不同认证方式上线（MAC 地址认证、802.1X 认证）。

(1) 用户上线后服务器上显示如图 130 和图 131。

图130 用户上线后服务器显示

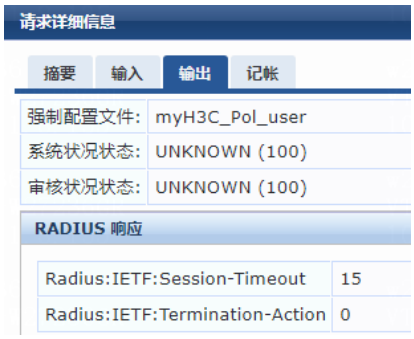
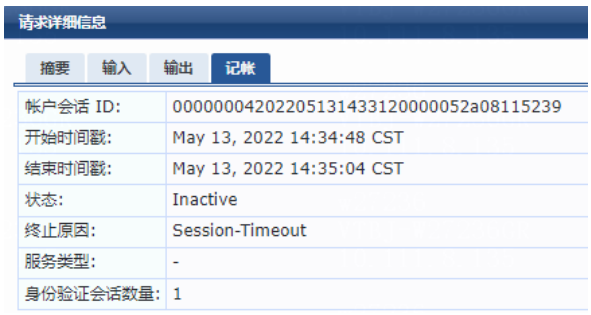


图131 用户被强制下线



(2) 用户上线后设备上显示（以 802.1X 认证为例）

在设备上通过 **display dot1x connection** 命令可以查看上线 802.1X 用户的信息。Session timeout period 字段显示会话超时时长，到达该时长后，用户所在的会话将会被删除，之后，对该用户所采取的动作为 Termination action 字段显示的 Default，即用户强制下线。

```
[Device]display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: user
User access state: Successful
Authentication domain: bbb
Authentication method: EAP
Initial VLAN: 144
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: 15 s
Online from: 2022/05/13 14:34:58
Online duration: 0h 0m 4s
```

(3) 用户上线后设备上显示（以 MAC 地址认证为例）

在设备上通过 **display mac-authentication connection** 命令可以查看上线 MAC 地址认证用户的信息。Session timeout period 字段显示会话超时时长，到达该时长后，用户所在的会话将会被删除，之后，对该用户所采取的动作为 Termination action 字段显示的 Default，即用户强制下线。

```
[Device]display mac-authentication connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: user
User access state: Successful
Authentication domain: mac-auth
IPv4 address: 101.0.145.39
Initial VLAN: 144
Authorization untagged VLAN: N/A
Authorization tagged VLAN: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
```

```
Session timeout period: 15 sec
Online from: 2022/05/13 14:59:25
Online duration: 0h 0m 5s
```

通过报文捕获，可以验证对于 802.1X 认证，根据配置的用户会话超时时长，15 秒后用户用户被强制下线。

12.7 服务器未配置会话超时重认证配置步骤与验证

说明

当认证服务器未下发用户会话超时时长时，是否对用户进行重认证，由设备上配置的重认证功能决定。

12.7.1 配置 Switch

802.1X 认证用户，Swtich 上的配置请参考 6.3.1 配置 Switch。

MAC 地址认证用户，Swtich 上的配置请参考 5.3.1 配置 Switch。

(1) 对于 802.1X 认证，设备上需要额外加上以下配置：

```
[Device] interface Ten-GigabitEthernet 1/0/49
[Device-Ten-GigabitEthernet1/0/49] dot1x re-authenticate
[Device-Ten-GigabitEthernet1/0/49] dot1x timer reauth-period 60
```

(2) 对于 MAC 地址认证，设备上需要额外加上以下配置：

```
[Device] mac-authentication timer reauth-period 60
[Device] interface Ten-GigabitEthernet 1/0/49
[Device-Ten-GigabitEthernet1/0/49] mac-authentication timer reauth-period 60
[Device-Ten-GigabitEthernet1/0/49] mac-authentication re-authenticate
[Device-Ten-GigabitEthernet1/0/49] quit
```

12.7.2 配置 ClearPass

MAC 地址认证用户，服务器上的配置请参考 5.3.2 配置 ClearPass。

802.1X 认证用户，服务器上的配置请参考 6.3.2 配置 ClearPass。

只需将“配置文件”的“属性”参考图 132 修改即可（注意：服务器上未配置会话超时时长）。

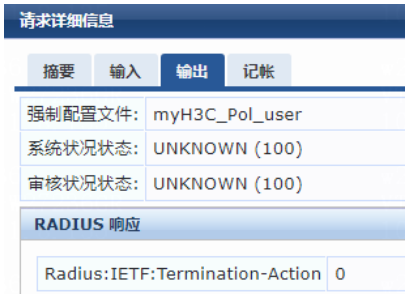
图132 配置文件

12.7.3 验证配置

用户使用不同认证方式上线（MAC 地址认证、802.1X 认证）。

(1) 用户上线后服务器上显示如图 133。

图133 用户上线后服务器显示



(2) 用户上线后设备上显示（以 802.1X 认证为例）

在设备上通过 **display dot1x connection** 命令可以查看上线 802.1X 用户的信息。Termination action 字段显示的 Default。

```
[Device] display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: user
User access state: Successful
Authentication domain: bbb
Authentication method: EAP
Initial VLAN: 144
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: N/A
Online from: 2022/05/12 14:09:59
Online duration: 0h 0m 5s
```

(3) 用户上线后设备上显示（以 MAC 地址认证为例）

在设备上通过 **display dot1x connection** 命令可以查看上线 MAC 地址认证用户的信息。Termination action 字段显示的 Default。

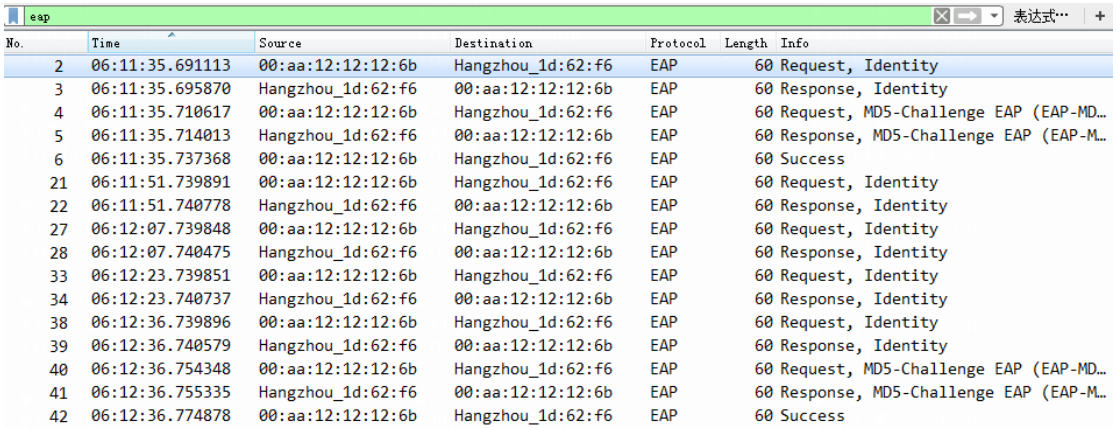
```
[Device]display mac-authentication connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
```

```
Username: user
User access state: Successful
Authentication domain: mac-auth
IPv6 address: FE80::5D79:AE17:4AEF:503A
Initial VLAN: 144
Authorization untagged VLAN: N/A
Authorization tagged VLAN: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: N/A
Online from: 2022/05/13 15:06:31
Online duration: 0h 0m 7s
```

(4) 抓包查看用户重认证

对于 802.1X 认证，端口会以重认证定时器的 60 秒为周期向该端口在线 802.1X 用户发起重认证，并且成功上线。

图134 报文捕获示意图



对于 MAC 地址认证，端口会以重认证定时器的 60 秒为周期向该端口在线用户发起重认证，并且成功上线。

图135 报文捕获示意图

radius

No.	Time	Source	Destination	Protocol	Length	Info
62	2022/133 15:06:27.192213	20.1.1.3	20.1.1.1	RADIUS	130	Access-Accept id=192
63	2022/133 15:06:27.206710	20.1.1.3	20.1.1.1	RADIUS	66	Accounting-Response id=254
268	2022/133 15:07:28.221788	20.1.1.3	20.1.1.1	RADIUS	130	Access-Accept id=38

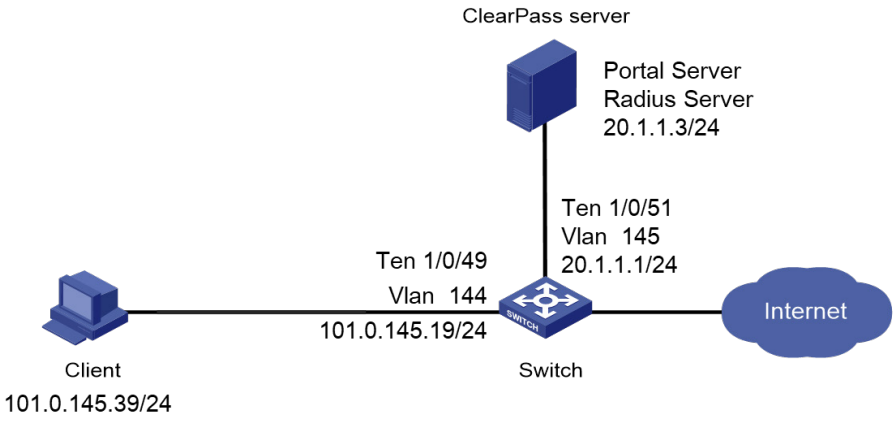
13 URL 重定向对接配置举例

13.1 组网需求

如图 136 所示，Client 和 ClearPass 服务器通过 Switch 建立连接，设备管理员希望对 Client 进行 802.1X 认证，以控制其对网络资源的访问，具体要求如下：

- 采用 ClearPass 作为 RADIUS 服务器和 Portal 服务器。
- 用户采用 802.1X 认证，服务器授权下发 URL 重定向。
- 802.1X 认证通过后，用户在客户端的游览器上输入任意 IP 地址会被重定向到 URL 中的 Web 页面。

图136 802.1X 认证配置组网图



13.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch：S5130-HI，R3507P02
- Aruba 认证服务器：ClearPass CPPM V6.9.7

13.3 配置步骤

说明

本配置仅展示认证的相关配置，网络互通的相关配置略，请保证设备间能够互相访问。

13.3.1 配置 Switch

#设备上配置一条 ACL 放行 URL 中的 IP 地址。并且该条 ACL 需要在服务器上下发。Swtich 上的其它配置请参考 6.3.1 配置 Switch。

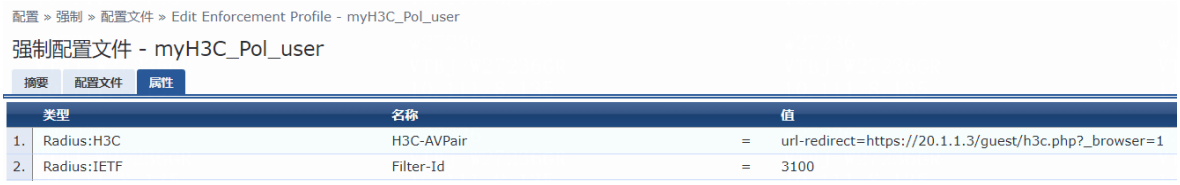
```
[Device] acl advanced 3100
[Device-acl-ipv4-adv-3100] rule 1 permit ip destination 20.1.1.3 0
```

13.3.2 配置 ClearPass

802.1X 认证用户，服务器上的配置请参考 6.3.2 配置 ClearPass。

只需将“配置文件”的“属性”参考图 137 修改即可。

图137 配置文件

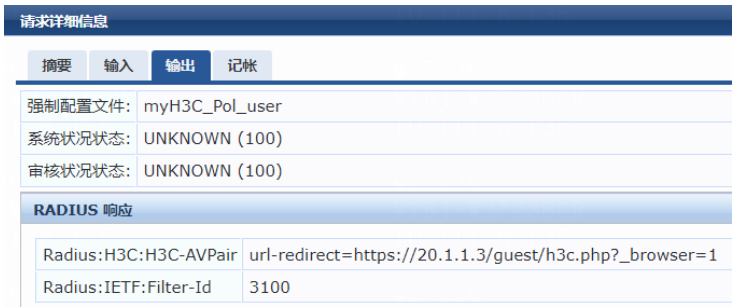


注：URL 中的 IP 地址为实际使用的 Portal 服务器的 IP 地址，本例中 IP 为 20.1.1.3。

13.4 验证配置

(1) 用户上线后服务器显示如图 138。

图138 用户上线后服务器输出显示



(2) 用户上线后设备显示

在设备上通过 **display dot1x connection** 命令可以查看上线 802.1X 用户的信息。

```
[Device]display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-62f6
Access interface: Ten-GigabitEthernet1/0/49
Username: user
User access state: Successful
Authentication domain: bbb
```

```
Authentication method: CHAP
Initial VLAN: 144
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
Authorization ACL number/name: 3100
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: https://20.1.1.3/guest/h3c.php?_browser=1
Termination action: Default
Session timeout period: N/A
Online from: 2022/05/27 11:16:21
Online duration: 0h 0m 4s
```

(3) 用户在客户端的游览器上输入任意 IP 地址，会被重定向到 URL 中的 Web 页面。

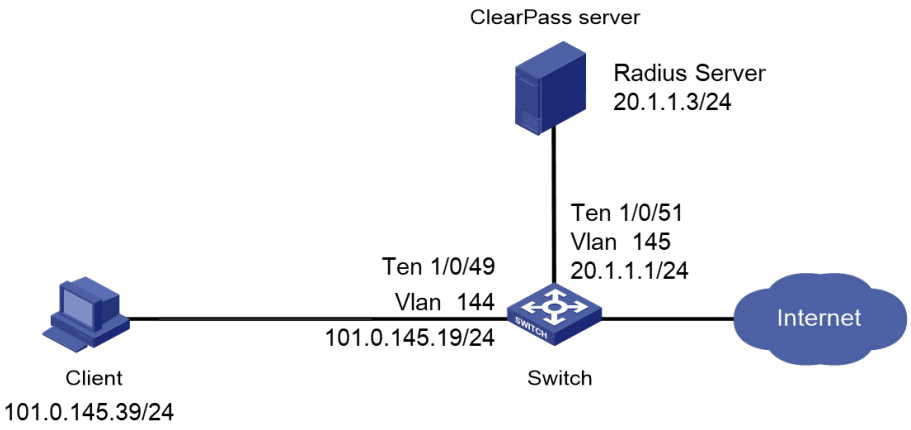
14 DAE 对接配置举例

14.1 组网需求

如图 139 示，Client 和 ClearPass 服务器通过 Switch 建立连接，设备管理员希望对 Client 进行认证（以 802.1X 认证为例），以控制其对网络资源的访问，具体要求如下：

- 采用 ClearPass 作为 RADIUS 服务器。
- 通过 ClearPass 下发 DAE 请求。

图139 组网图



14.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch：S5130-HI，R3507P02
- Aruba 认证服务器：ClearPass CPPM V6.9.7

14.3 强制下线（Disconnect Messages）配置步骤与验证

14.3.1 配置 Switch

Swtich 上的基础配置请参考 6.3.1 配置 Switch。

设备上需要额外增加如下配置。

开启 RADIUS DAE 服务，并进入 RADIUS DAE 服务器视图。

```
[Device] radius dynamic-author server
```

指定 RADIUS DAE 客户端，此 IP 是 AAA 服务器的 IP，密钥是服务器上配置的 radius 共享密钥。

```
[Device-radius-da-server] client ip 20.1.1.3 key simple 123456
[Device-radius-da-server] quit
```

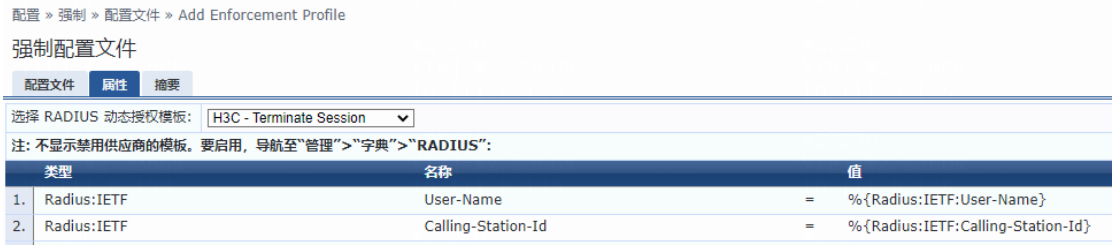
14.3.2 配置 ClearPass

服务器上的配置请参考 6.3.2 配置 ClearPass。并参考图 140、图 141 补充配置。

图140 配置文件

图141 添加属性

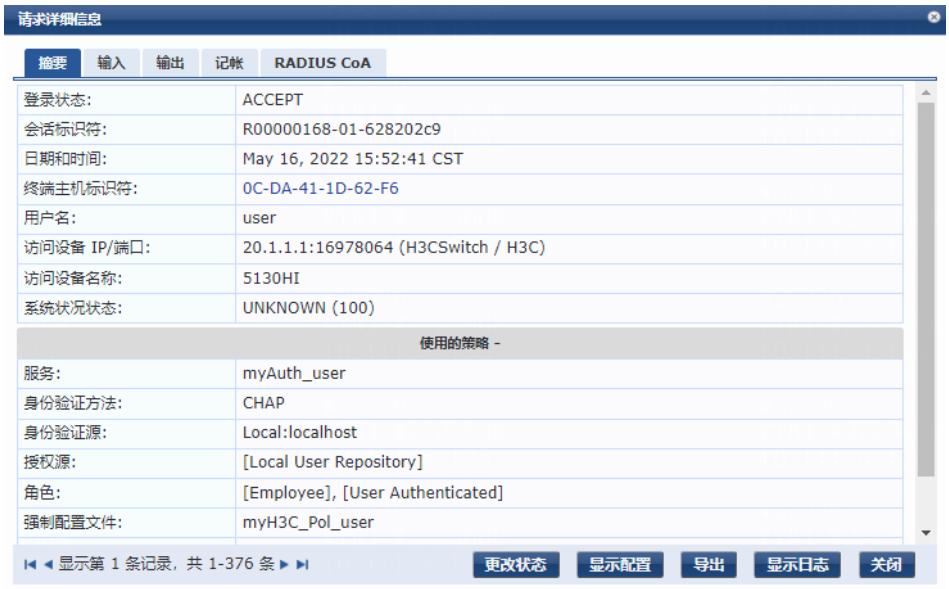
根据需求选择“H3C-Terminate Session”的 Radius 动态授权模板。



14.3.3 验证配置

(1) 用户上线后服务器上显示如图 142。

图142 用户上线后服务器显示



(2) 在 DAE 客户端（ClearPass）上发送 DAE 请求

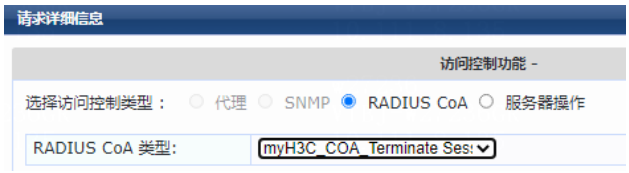
用户上线后，点击图 142 中的“更改状态”按钮。

a. “选择访问控制类型”为“RADIUS CoA”

b. “RADIUS CoA 类型”选择在图 140 中创建的配置文件

c. 点击“提交”按钮

图143 发送 DAE 请求



(3) 用户下线后服务器显示

图144 RADIUS CoA 显示

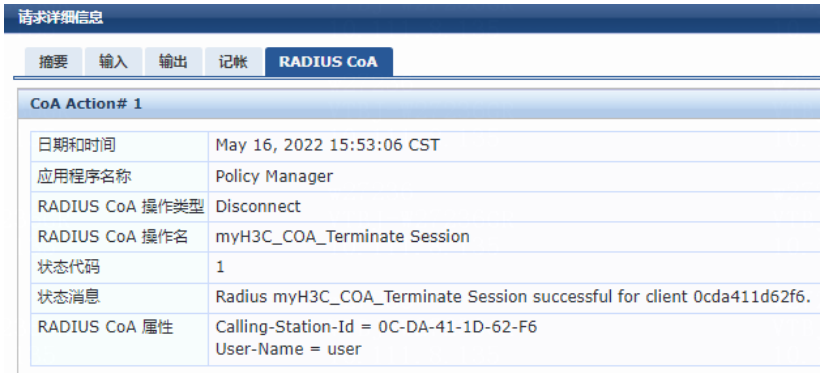
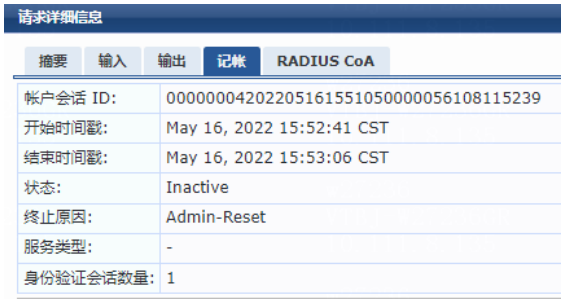


图145 用户强制下线



14.4 关闭端口（Disabling Host Port）的配置步骤与验证

14.4.1 配置 Switch

Swtich 上的基础配置请参考 6.3.1 配置 Switch。

设备上需要额外增加如下配置。

开启 RADIUS DAE 服务，并进入 RADIUS DAE 服务器视图。

```
[Device] radius dynamic-author server
```

指定 RADIUS DAE 客户端，此 IP 是 AAA 服务器的 IP，密钥是服务器上配置的 radius 共享密钥

```
[Device-radius-da-server] client ip 20.1.1.3 key simple 123456
[Device-radius-da-server] quit
```

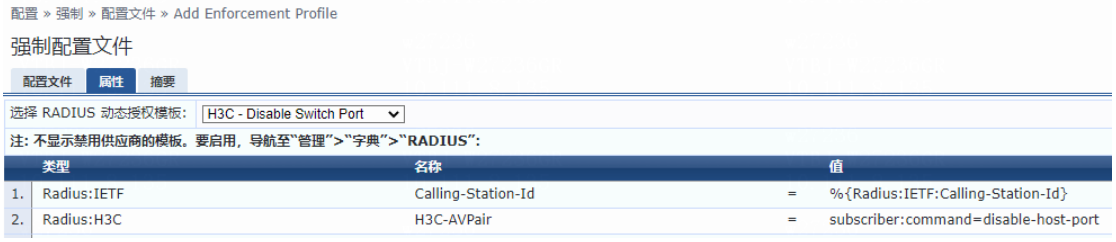
14.4.2 配置 ClearPass

服务器上的配置请参考 6.3.2 配置 ClearPass。并参考图 146、图 147 补充配置。

图146 配置文件

图147 添加属性

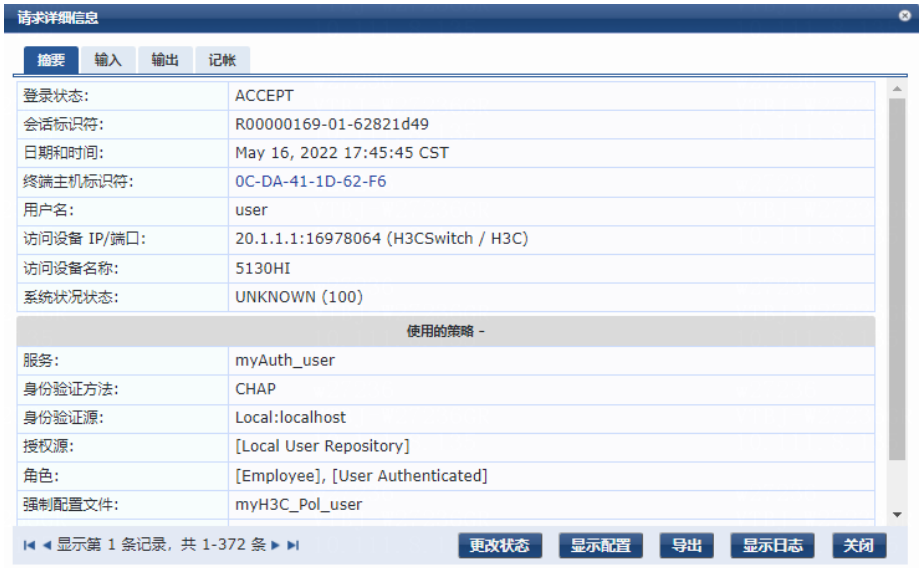
根据需求选择“H3C-Disable Switch Port”的 Radius 动态授权模板。



14.4.3 验证配置

(1) 用户上线后服务器上显示如图 148。

图148 用户上线后服务器显示



(2) 在 DAE 客户端（ClearPass）上发送 DAE 请求

用户上线后，点击 图 148 中的“更改状态”。

a. “选择访问控制类型为“RADIUS CoA”

b. “RADIUS CoA 类型”选择在图 146 中创建的配置文件

c. 点击“提交”

图149 发送 DAE 请求

(3) 用户强制下线后服务器上显示。

图150 RADIUS CoA 显示

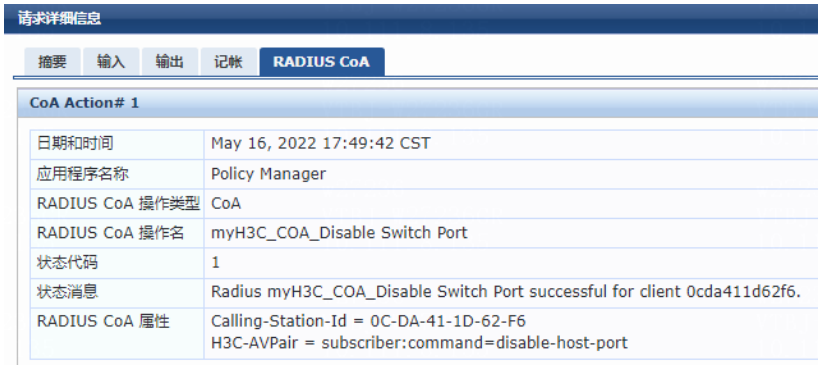
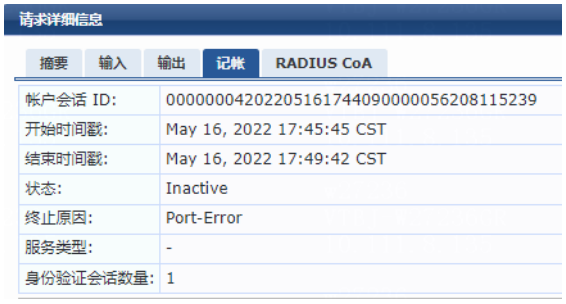


图151 用户下线



14.5 重启端口（Bouncing Host Port）的配置步骤与验证

14.5.1 配置 Switch

Swtich 上的基础配置请参考 6.3.1 配置 Switch。

设备上需要额外增加如下配置。

开启 RADIUS DAE 服务，并进入 RADIUS DAE 服务器视图。

```
[Device] radius dynamic-author server
```

指定 RADIUS DAE 客户端，此 IP 是 AAA 服务器的 IP，密钥是服务器上配置的 radius 共享密钥

```
[Device-radius-da-server] client ip 20.1.1.3 key simple 123456
[Device-radius-da-server] quit
```

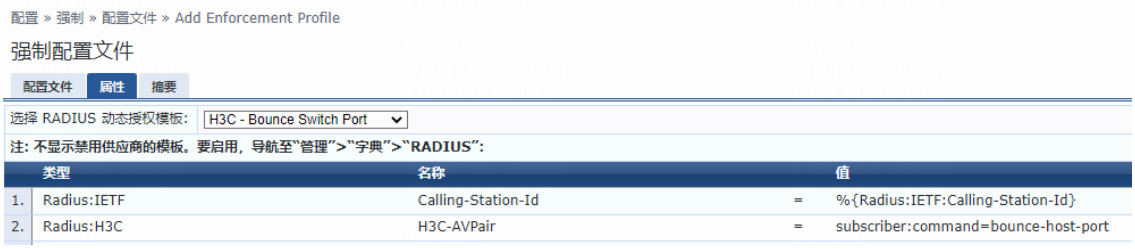
14.5.2 配置 ClearPass

服务器上的配置请参考 6.3.2 配置 ClearPass。并参考图 152、图 153 补充配置。

图152 配置文件

图153 添加属性

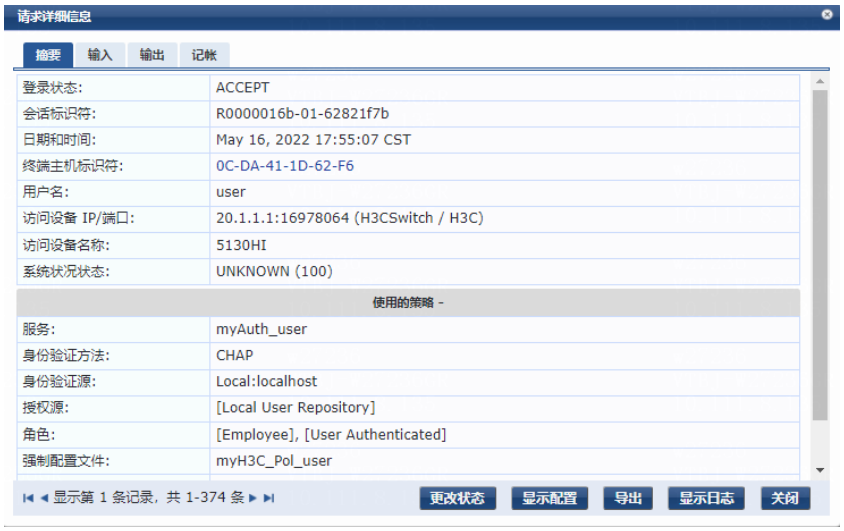
根据需求选择“H3C-Bounce Switch Port”的 Radius 动态授权模板。



14.5.3 验证配置

(1) 用户上线后服务器上显示如图 154。

图154 用户上线后服务器显示



(2) 在 DAE 客户端（ClearPass）上发送 DAE 请求

用户上线后，点击图 154 中的“更改状态”。

a. “选择访问控制类型”为“RADIUS CoA”

b. “RADIUS CoA 类型”选择在图 152 创建的配置文件

c. 点击“提交”

图155 发送 DAE 请求

(3) 用户下线后服务器上的显示如图 156、图 157。

图156 RADIUS CoA 显示

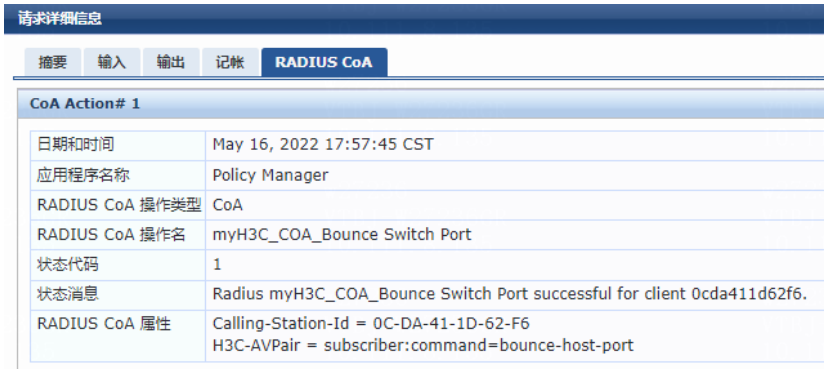
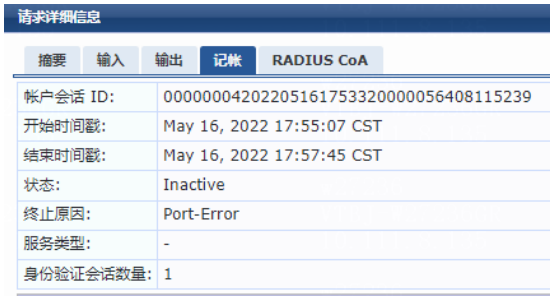


图157 用户下线



(4) 端口重启后用户重新上线如图 158、图 159。

图158 用户重新上线

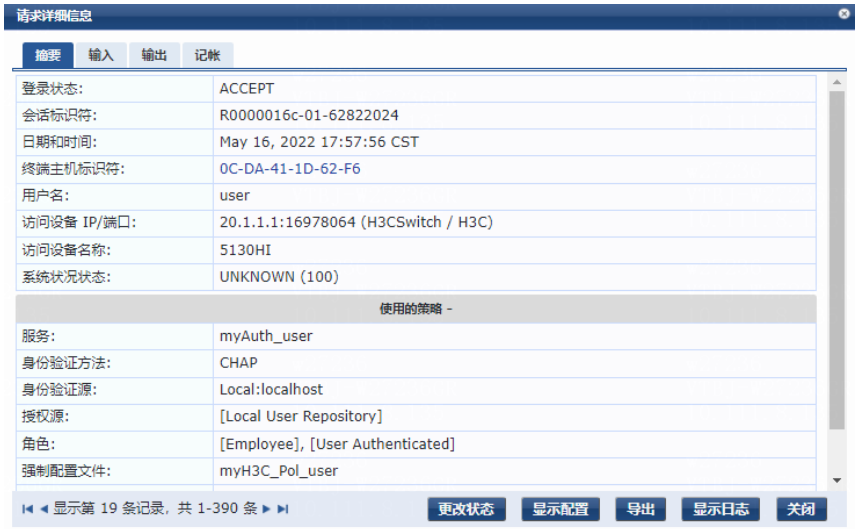
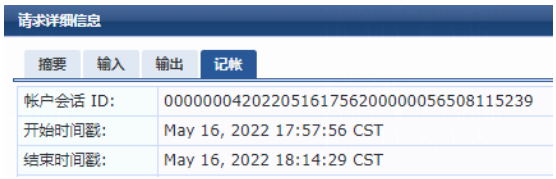


图159 重新上线会话改变

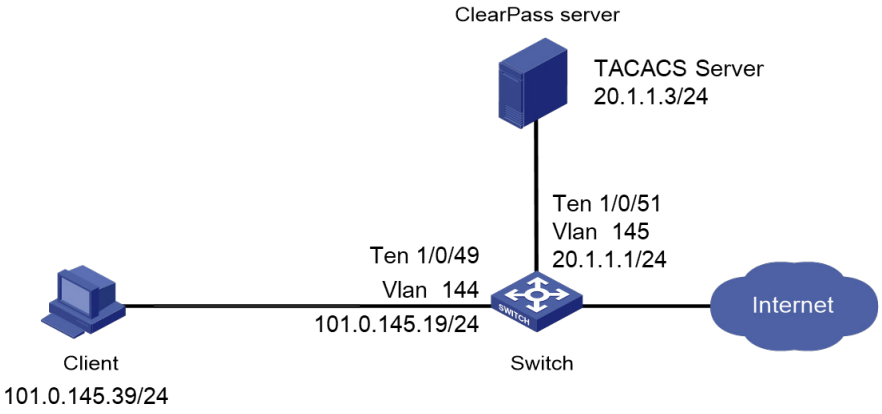


15 SSH 登录使用 HWTACACS 认证对接操作举例

15.1 组网需求

如图 160 所示，设备管理员希望 PC 使用 SSH 登录 Switch 时，通过使用 ClearPass 服务器进行远程 TACACS 认证，登录 Switch 后，验证为 network-admin 用户角色。

图160 认证组网图



15.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch：S5130-HI，R3507P02
- Aruba 认证服务器：ClearPass CPPM V6.9.7

15.3 配置步骤

15.3.1 配置 Switch

创建 HWTACACS 方案 tac。

```
<Device> system-view
[Device] hwtacacs scheme tac
[Device-hwtacacs-tac] primary authentication 20.1.1.3
[Device-hwtacacs-tac] primary accounting 20.1.1.3
[Device-hwtacacs-tac] key authentication simple 123456
[Device-hwtacacs-tac] key accounting simple 123456
[Device-hwtacacs-tac] user-name-format without-domain
[Device-hwtacacs-tac] quit
```

创建 ISP 域 tac，为 login 用户配置 AAA 认证方法为 TACACS 认证/授权/计费。

```
[Device] domain tac
[Device-isp-tac] authentication login hwtacacs-scheme tac
[Device-isp-tac] authorization login hwtacacs-scheme tac
[Device-isp-tac] accounting login hwtacacs-scheme tac
[Device-isp-tac] quit
```

配置 ISP 域 tac 为缺省域。

```
[Device] domain default enable tac
```

创建本地 RSA 及 DSA 密钥对。

```
[Device] public-key local create rsa
[Device] public-key local create dsa
```

开启 SSH 服务器功能。

```
[Device] ssh server enable
```

开启缺省用户角色授权功能，使得认证通过后的 SSH 用户具有缺省的用户角色 network- admin。

```
[Device] role default-role enable network-admin
```

设置 SSH 用户登录用户线的认证方式为 AAA 认证。

```
[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
[Device-line-vty0-63] quit
```

配置互通的 VLAN 和 VLAN 接口 IP 地址。

```
[Device] vlan 144
[Device-vlan144] quit
[Device] interface Vlan-interface 144
[Device-Vlan-interface144] ip address 101.0.145.19 255.255.255.0
[Device-Vlan-interface144] quit
[Device] vlan 145
```

```
[Device-vlan145] quit
[Device] interface Vlan-interface 145
[Device-Vlan-interface145] ip address 20.1.1.1 255.255.255.0
[Device-Vlan-interface145] quit
```

将端口 XGE1/0/49 和 XGE1/0/51 加入到指定的 VLAN。

```
[Device] interface Ten-GigabitEthernet 1/0/49
[Device-Ten-GigabitEthernet1/0/49] port access vlan 144
[Device-Ten-GigabitEthernet1/0/49] quit
[Device] interface Ten-GigabitEthernet 1/0/51
[Device-Ten-GigabitEthernet1/0/51] port access vlan 145
[Device-Ten-GigabitEthernet1/0/51] quit
```

15.3.2 配置 ClearPass

(1) 添加用户

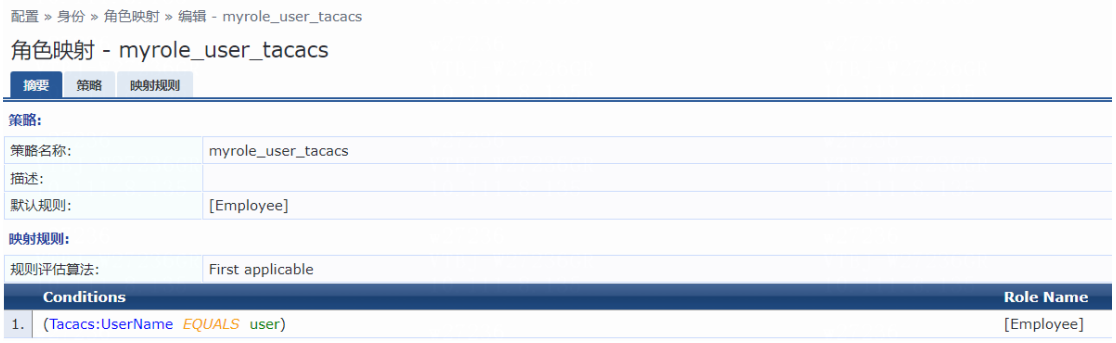
依次点击“配置 » 身份 » 本地用户 » 添加”，根据图 161 添加用户。

图161 添加用户

(2) 角色映射

根据图 162 添加角色映射，添加“Conditions”时 User-Name 的值对应的是图 161 添加的用户 ID

图162 添加角色映射



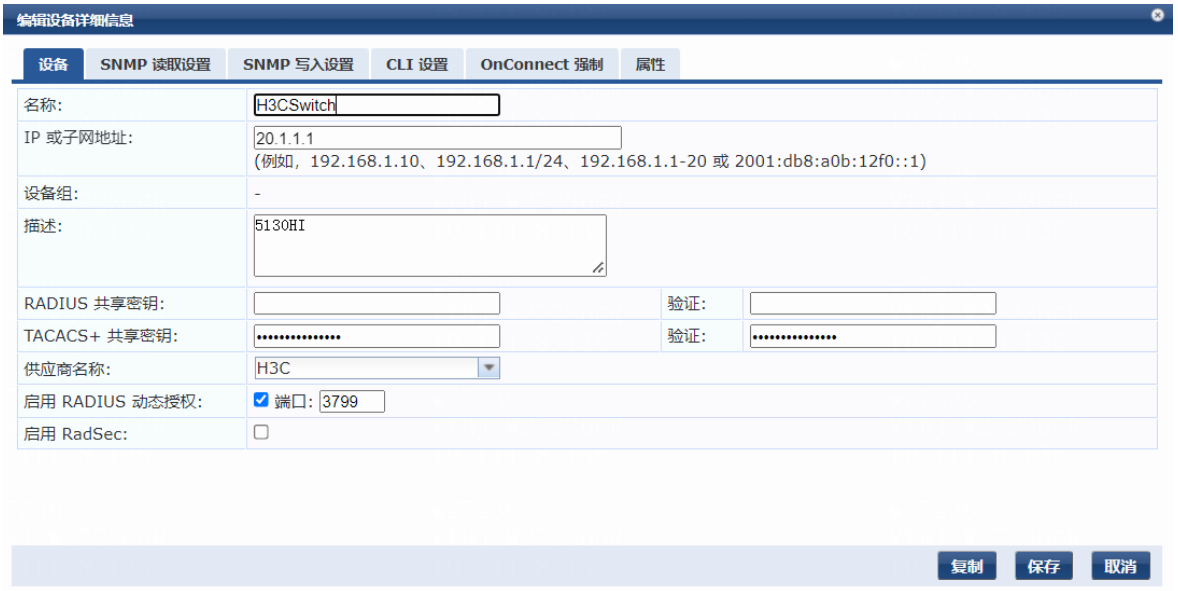
(3) 添加设备

依次点击“配置 » 网络 » 设备 » 添加”，根据图 163 添加设备。

a. “IP 或子网地址”填写设备上与服务器接口可达的 IP 地址（本例为 20.1.1.1/24）

b. “TACACS+共享密钥”需要与设备上配置的密钥相同

图163 添加设备



(4) 添加设备组

依次点击“配置 » 网络 » 设备组 » 添加”，根据图 164 添加设备组。“子网”填写设备上与服务器接口可达的 IP 地址（本例为 20.1.1.1/24）

图164 添加设备组

(5) 添加配置文件

根据图 165 添加配置文件。

图165 添加配置文件

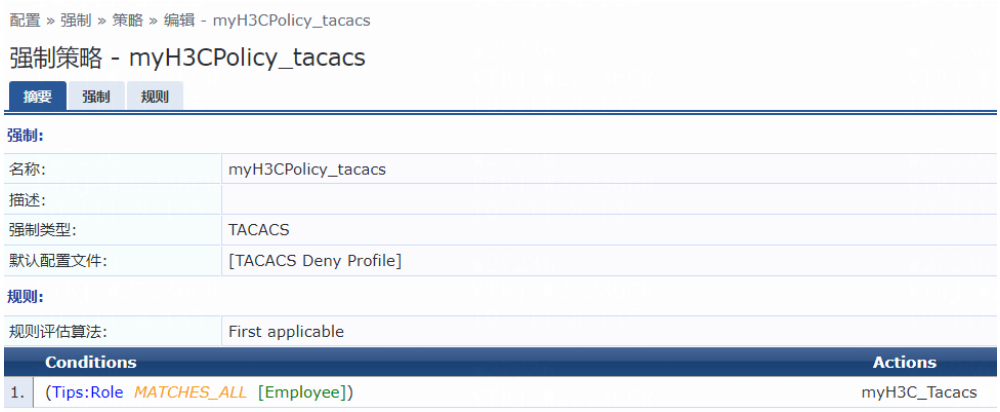
(6) 添加策略

根据图 166 添加策略。

a. 在添加策略时，“Conditions”中对应的“Actions”选择图 165 创建的配置文件即可

b. 规则评估算法，根据需要选择选项中的一个即可

图166 添加策略



(7) 添加服务

添加服务中对应的各项。

a. 在图 167 中添加服务时，类型选择“TACACS+ 强制”

b. 在图 169 中添加角色时，角色映射策略选择图 116 创建的角色映射

c. 在图 170 中添加强制时，强制策略选择在图 120 中创建的强制策略

图167 添加服务

图168 添加身份验证

图169 添加角色

图170 添加强制

15.4 验证配置

(1) 用户使用 Putty 软件，打开安装好的 Putty 软件。参考图 171，根据以下步骤登录。

a. 点击“Session”

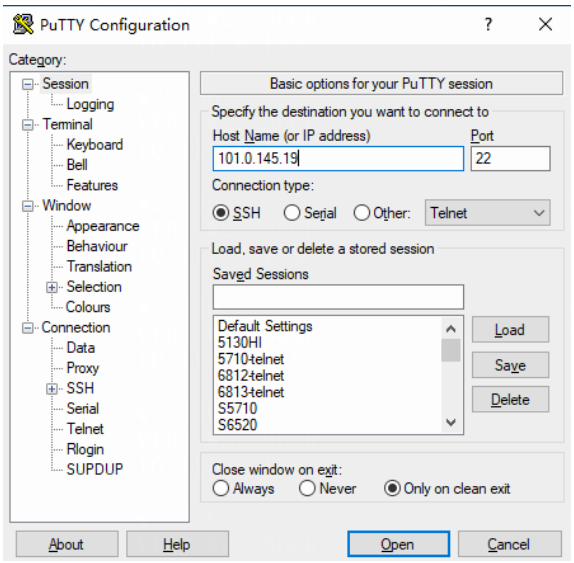
b. “Connection type” 选择为“SSH”

c. 输入 IP address，此 IP 为设备上与客户端互通的 IP（该组网中 IP 为 101.0.145.19）

d. “Port”使用默认的“22”

e. 点击“Open”。

图171 Putty 界面 SSH 登录

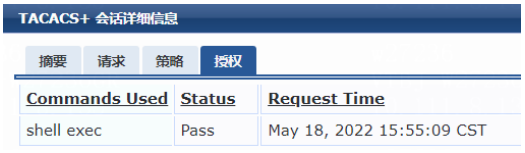


(2) 用户上线后服务器显示如图 172、图 173、图 174。

图172 用户上线后服务器显示一

图173 用户上线后服务器显示二

图174 用户上线后服务器显示三



(3) 用户上线

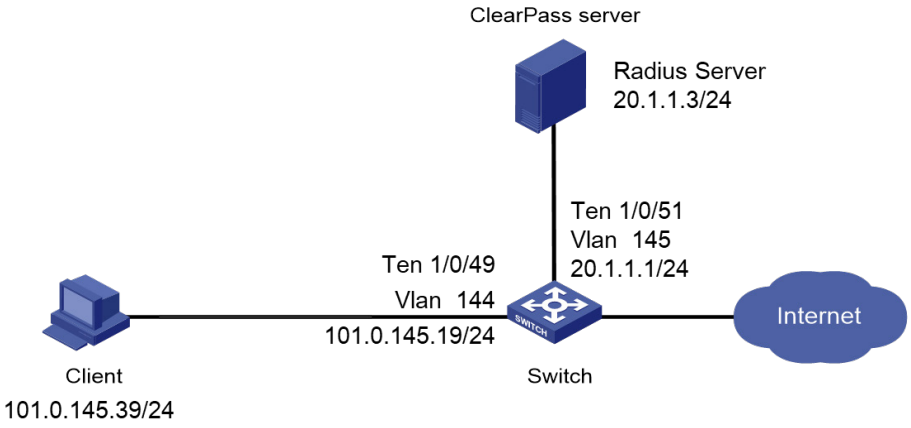
输入服务器上创建的用户名“user”和密码“123456”，点击“回车键”即可登录设备。

16 Login 用户登录使用 Radius 认证对接操作举例

16.1 组网需求

如图 175 所示，设备管理员希望使用 SSH、Telnet 或 Console 口登录 Switch 时，通过使用 ClearPass 服务器进行远程 RADIUS 认证，登录 Switch 后，验证为 network-admin 用户角色。

图175 Login 用户登录组网图



16.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch：S5130-HI，R3507P02
- Aruba 认证服务器：ClearPass CPPM V6.9.7

16.3 配置步骤

16.3.1 配置 Switch

1. SSH 登录方式

创建 RADIUS 方案 radius1。

```
<Device> system-view
[Device] radius scheme radius1
[Device-radius-radius1] primary authentication 20.1.1.3
[Device-radius-radius1] primary accounting 20.1.1.3
[Device-radius-radius1] key authentication simple 123456
[Device-radius-radius1] key accounting simple 123456
[Device-radius-radius1] user-name-format without-domain
[Device-radius-radius1] quit
```

创建 ISP 域 123，为 login 用户配置 AAA 认证方法为 RADIUS 认证/授权/计费。

```
[Device] domain 123
```

```
[Device-isp-123] authentication login radius-scheme radius1
[Device-isp-123] authorization login radius-scheme radius1
[Device-isp-123] accounting login radius-scheme radius1
[Device-isp-123] quit
```

配置 ISP 域 123 为缺省域。

```
[Device] domain default enable 123
```

创建本地 RSA 及 DSA 密钥对。

```
[Device] public-key local create rsa
[Device] public-key local create dsa
```

开启 SSH 服务器功能。

```
[Device] ssh server enable
```

设置用户登录用户线的认证方式为 AAA 认证。

```
[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
[Device-line-vty0-63] quit
```

配置互通的 VLAN 和 VLAN 接口的 IP 地址。

```
[Device] vlan 144
[Device-vlan144] quit
[Device] interface Vlan-interface 144
[Device-Vlan-interface144] ip address 101.0.145.19 255.255.255.0
[Device-Vlan-interface144] quit
[Device] vlan 145
[Device-vlan145] quit
[Device] interface Vlan-interface 145
[Device-Vlan-interface145] ip address 20.1.1.1 255.255.255.0
[Device-Vlan-interface145] quit
```

将端口 XGE1/0/49 和 XGE1/0/51 加入指定的 VLAN。

```
[Device] interface Ten-GigabitEthernet 1/0/49
[Device-Ten-GigabitEthernet1/0/49] port access vlan 144
[Device-Ten-GigabitEthernet1/0/49] quit
[Device] interface Ten-GigabitEthernet 1/0/51
[Device-Ten-GigabitEthernet1/0/51] port access vlan 145
[Device-Ten-GigabitEthernet1/0/51] quit
```

2. Telnet 登录方式

配置与 16.3.1 1. SSH 登录方式基本相同，只需在设备上额外加以下配置即可。

开启 Telnet 服务器功能。

```
[Device] telnet server enable
```

3. Console 口登录方式

配置与 16.3.1 1. SSH 登录方式基本相同，只需在设备上额外加以下配置即可。

```
[Device] line aux 0
[Device-line-aux0] authentication-mode scheme
[Device-line-aux0] quit
```

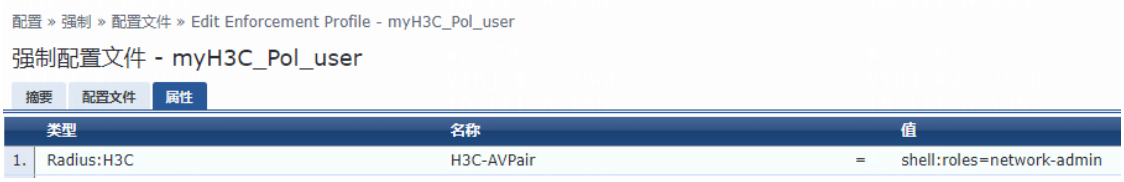
16.3.2 配置 ClearPass

服务器上的配置请参考 6.3.2 配置 ClearPass。

只需将“配置文件”的“属性”参考图 176 修改即可。

需要注意的是：这里的“user role”必须与设备上对应，在设备系统视图使用 **display role** 命令行来查看支持的角色。（本例中配置为 network-admin）

图176 配置文件



16.4 验证配置

16.4.1 SSH/Telnet 登录方式

(1) 用户使用 Putty 软件，打开安装好的 Putty 软件。参考图 132、图 133，根据以下步骤登录。

a. 点击“Session”

b. “Connection type” 选择为“SSH”（若为 Telnet 则选择“Telnet”）

c. 输入 IP address，此 IP 为设备上与客户端互通的 IP（该组网中 IP 为 101.0.145.19）

d. “Port”使用默认的“22” （若为 Telnet 则使用“23”）

e. 点击“Open”。

图177 Putty 界面 SSH 登录

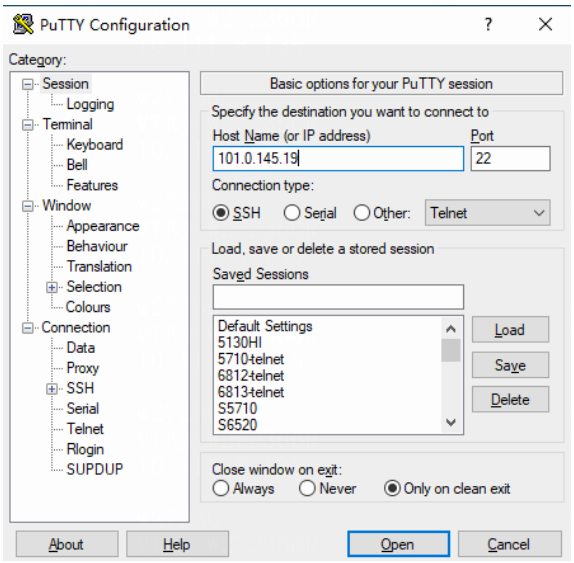
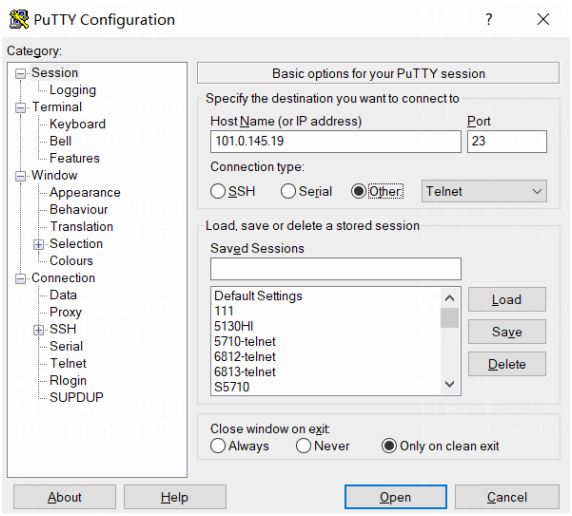
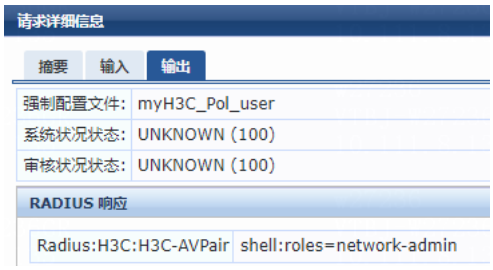


图178 Putty 界面 Telnet 登录



(2) 用户上线后服务器显示如图 179。

图179 用户上线后服务器显示



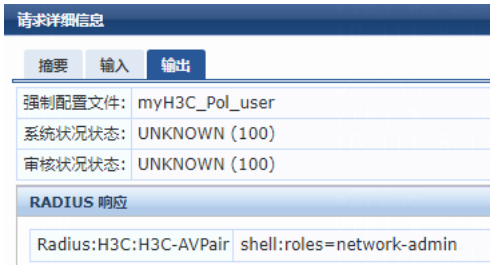
(3) 用户上线后客户端显示

输入服务器上创建的用户名“user”和密码“123456”，回车后即可登录。

16.4.2 Console 口登录方式

(1) 用户使用使用 Console 口登录设备，上线后服务器显示如图 180。

图180 用户上线后服务器显示



(2) 用户上线后客户端显示

输入服务器上创建的用户名“user”和密码“123456”，回车后即可登录。

H3C 交换机

与 Windows Server 2016-NPS 接入认证功能对接操作指导

目 录

1 简介

本文档介绍 H3C 交换机与 Windows 的认证服务器软件 Windows Server 2016-NPS 的接入认证功能对接配置，包括：

- MAC 地址认证对接配置举例
- 802.1X 认证对接配置举例

- Portal 认证对接配置举例
- 授权 VLAN 对接配置举例
- 授权 ACL 对接配置举例
- 授权 User-Profile 对接配置举例

说明

对接第三方认证服务器操作为交换机产品通用性内容，但部分接入认证功能在各产换机产品上存在支持差异。产品对各认证特性的支持情况请参考产品配置指导中安全分册的相关内容。

2 互通性分析

表2-1 接入认证互通性分析

H3C	Windows Server 2016-NPS	互通结论
固定用户名和密码的MAC地址认证	CHAP认证	可以互通
MAC地址作为用户名密码进行认证	CHAP认证	可以互通
802.1X CHAP认证	CHAP认证	可以互通
802.1X PAP认证	PAP认证	可以互通
802.1X EAP认证	EAP-PEAP认证	可以互通
本地Portal+LDAP认证	CHAP认证	可以互通
授权 VLAN	• 授权数字型 VLAN • 授权 VLAN 名称 • 授权 VLAN 组名 • 授权 Multi VLAN • 授权 Auto VLAN	可以互通
授权ACL	授权静态ACL	可以互通
授权User Profile	授权User Profile	可以互通

3 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

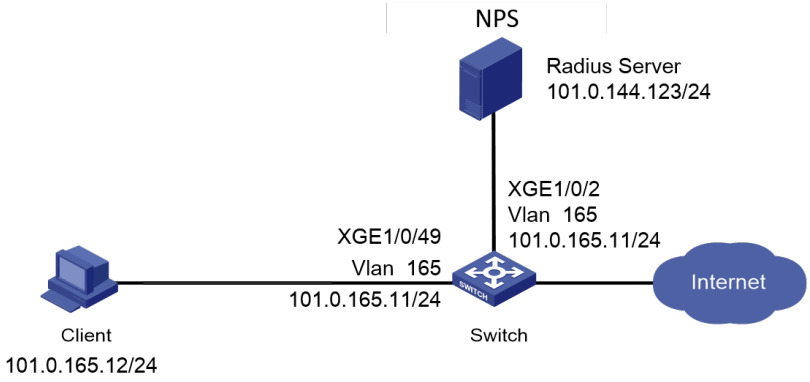
4 MAC 地址认证对接配置举例

4.1 组网需求

如图 4-1 所示，Client 和 Windows Server 2016-NPS 服务器通过 Switch 建立连接，设备管理员希望对 Client 进行 MAC 地址认证，以控制其对网络资源的访问，具体要求如下：

- 采用 Windows Server 2016-NPS 作为 RADIUS 服务器。
- 配置 MAC 地址认证的用户名和密码。

图4-1 MAC 认证配置组网图



4.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch： S5560X-54C-PWR-EI，Version 7.1.070
- 认证服务器：Windows Server 2016-NPS

4.3 固定用户名密码的MAC地址认证配置步骤与验证

说明

本配置仅展示认证的相关配置，网络互通的相关配置略，请保证设备间能够互相访问。

4.3.1 配置 Switch

配置 RADIUS 方案。

```
<Switch> system-view
[Switch] radius scheme radius1
[Switch-radius-radius1] primary authentication 101.0.144.123
[Switch-radius-radius1] primary accounting 101.0.144.123
[Switch-radius-radius1] key authentication simple admin
[Switch-radius-radius1] key accounting simple admin
[Switch-radius-radius1] user-name-format without-domain
[Switch-radius-radius1] quit
```

配置 MAC 地址认证的认证方法为 CHAP。

```
[Switch] mac-authentication authentication-method chap
```

创建 MAC 地址认证的域 mac-auth，并配置 ISP 域的 AAA 方法。

```
[Switch] domain mac-auth
[Switch-isp-mac-auth] authentication default radius-scheme radius1
[Switch-isp-mac-auth] authorization default radius-scheme radius1
[Switch-isp-mac-auth] accounting default radius-scheme radius1
[Switch-isp-mac-auth] quit
```

配置互通的 VLAN 和 VLAN 接口的 IP 地址。

```
[Switch] vlan 165
[Switch-vlan165] quit
[Switch] interface Vlan-interface 165
[Switch-Vlan-interface165] ip address 101.0.165.11 255.255.255.0
[Switch-Vlan-interface165] quit
```

将端口 XGE1/0/49 加入到指定 VLAN，并开启 MAC 地址认证功能。

```
[Switch]interface Ten-GigabitEthernet 1/0/49
[Switch-Ten-GigabitEthernet1/0/49] port access vlan 165
[Switch-Ten-GigabitEthernet1/0/49] mac-authentication
[Switch-Ten-GigabitEthernet1/0/49] quit
```

设置 mac-auth 为系统缺省的认证域。

```
[Switch] domain default enable mac-auth
```

指定 MAC 地址认证用户的认证域 mac-auth。

```
[Switch] mac-authentication domain mac-auth
```

配置 MAC 地址认证的定时器。

```
[Switch] mac-authentication timer offline-detect 180
[Switch] mac-authentication timer quiet 180
```

配置 MAC 地址认证使用固定用户名账号：用户名为 user，密码为明文 123456。

```
[Switch] mac-authentication user-name-format fixed account user password simple 123456
```

开启全局 MAC 地址认证。

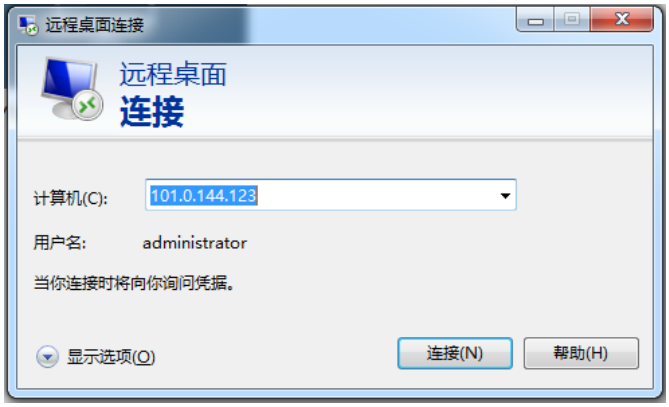
```
[Switch] mac-authentication
```

4.3.2 配置 Windows Server 2016-NPS

(1) 登录 Windows Server 2016-NPS

在远程桌面连接中输入 Windows Server 2016-NPS 的管理 IP 地址（本例为 101.0.144.123），登录 Windows Server 2016-NPS 的桌面。

图4-2 远程桌面连接



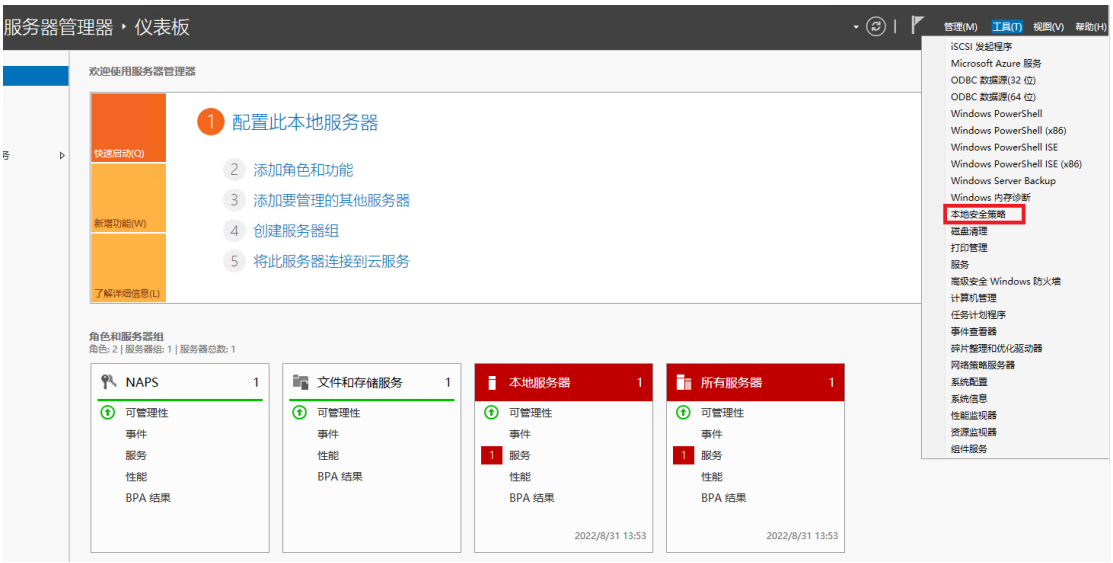
#输入登录 Windows Server 2016-NPS 服务器的用户名和密码（本例为 Administrator 和 admin@123456），点击“确定”按钮进入 NPS 远程桌面。

图4-3 输入登录用户名密码

(2) 配置本地安全策略

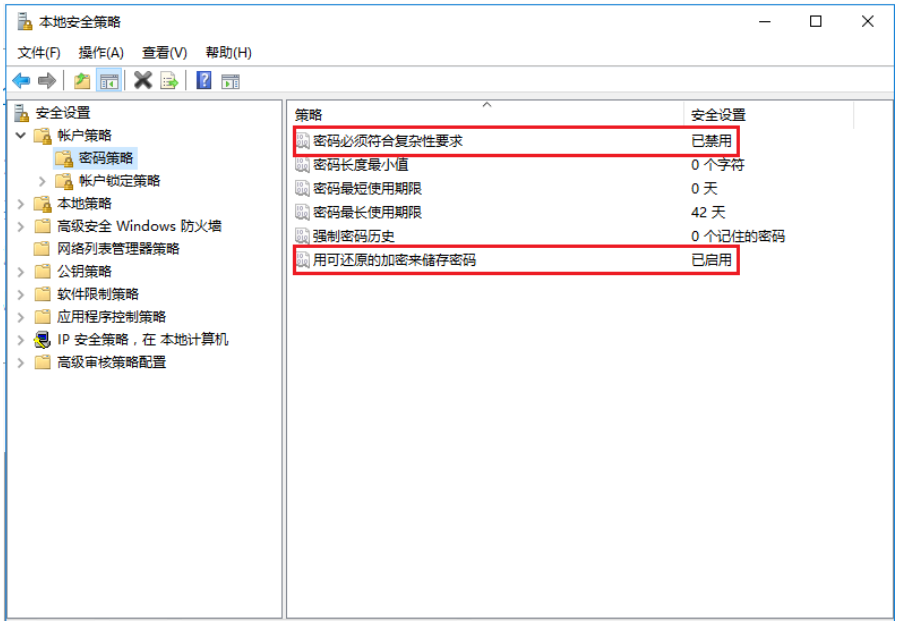
登录 NPS 后，在“服务器管理器”界面，依次点击“工具 » 本地安全策略”（如图 4-4 所示）。

图4-4 配置本地安全策略



在本地安全策略配置的左侧导航中，选择“密码策略”，设置“密码必须符合复杂性要求”为已禁用；设置“用可还原的加密来储存密码”为已启用。配置完成后，如图 4-5 所示。

图4-5 配置密码策略



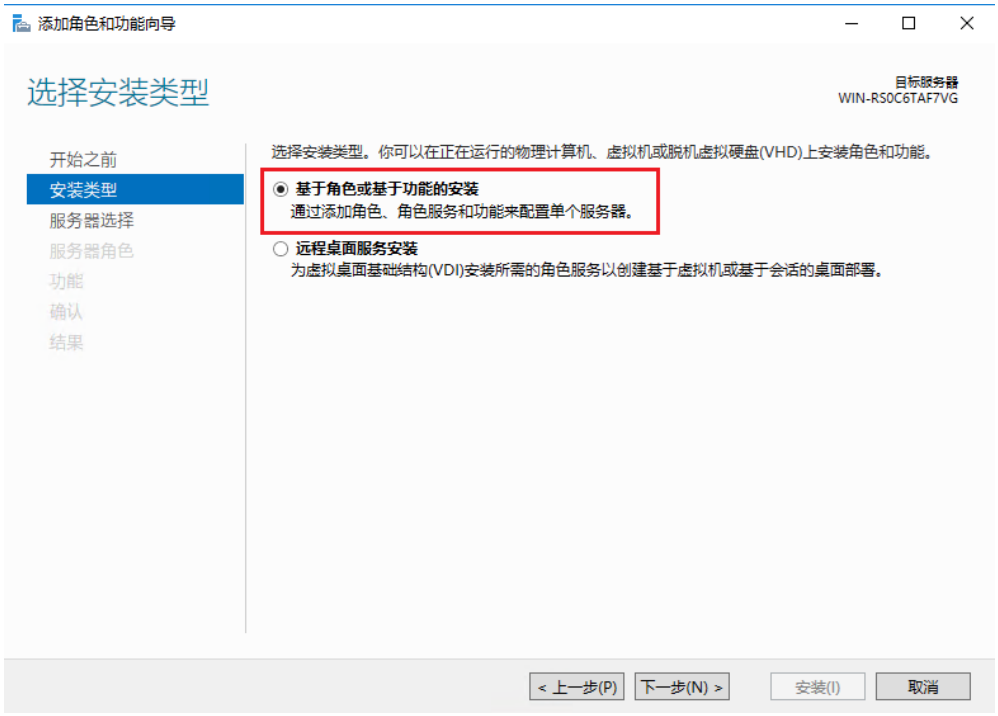
(3) 添加网络策略服务器

在“服务器管理器-仪表板”界面，依次点击“管理 » 添加角色和功能”（如图 4-6 所示），为服务器添加角色和功能。

图4-6 添加角色和功能

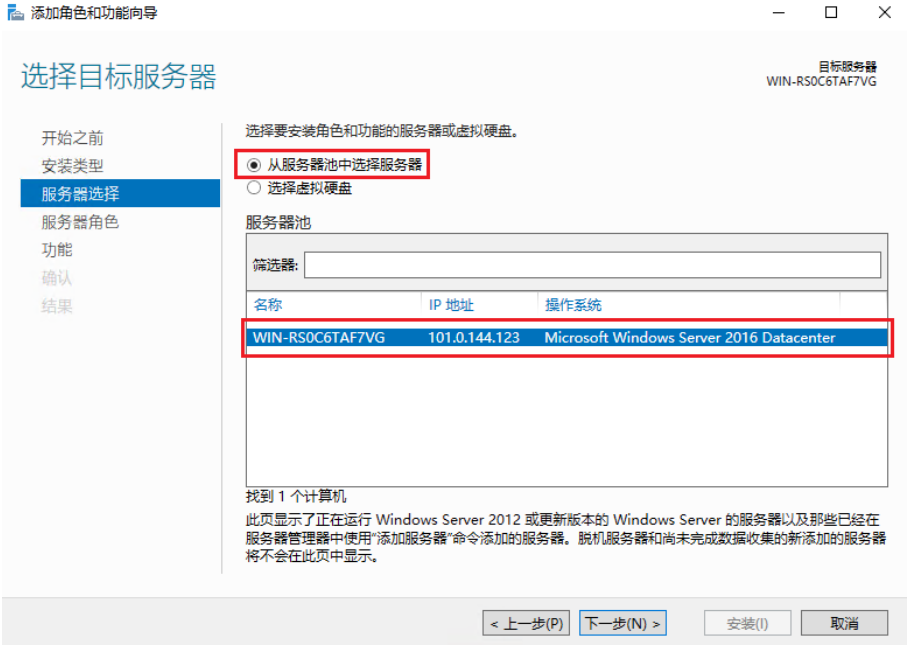
在左侧导航中，选择“安装类型”，选择“基于角色或基于功能的安装”（如图 4-7 所示）。

图4-7 选择安装类型



点击<下一步>，进入“服务器选择”配置，选择“从服务器池中选择服务器”（如图 4-8 所示），此处选择的服务器为远程登录的 NPS 服务器。

图4-8 选择目标服务器



点击<下一步>，进入“服务器角色”配置，勾选“网络策略和访问服务”（如图 4-9 所示），并点击<下一步>，按提示完成安装。

图4-9 选择服务器角色

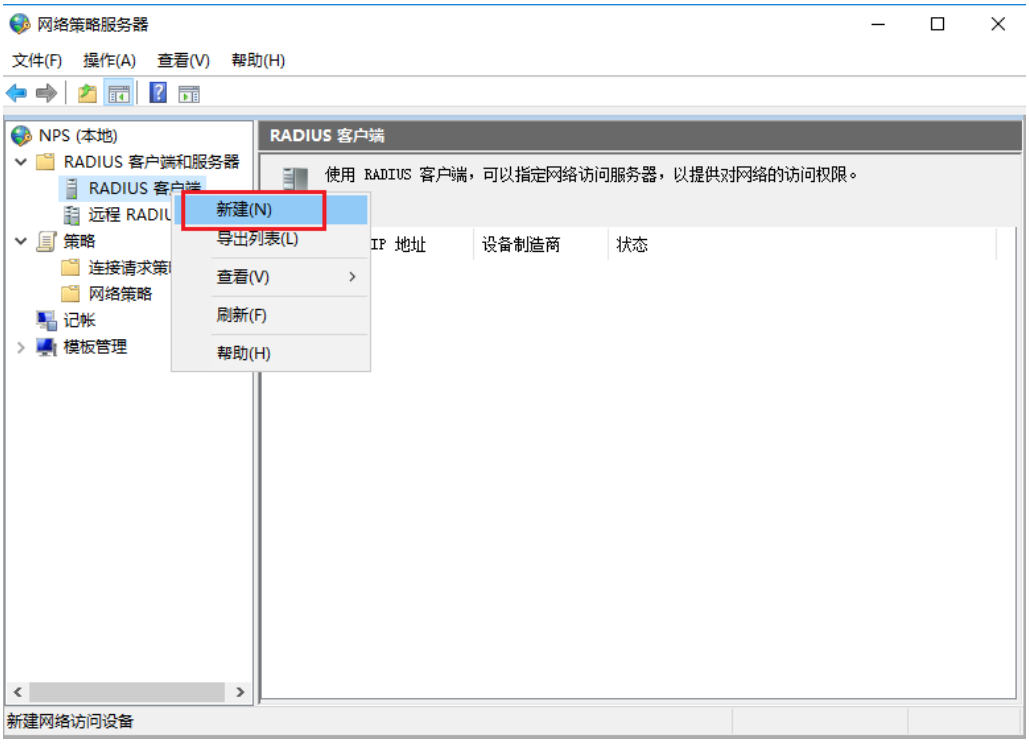
(4) 配置 RADIUS 客户端

在“服务器管理器-仪表板”界面，依次点击“工具 » 网络策略服务器”。

图4-10 打开网络策略服务器

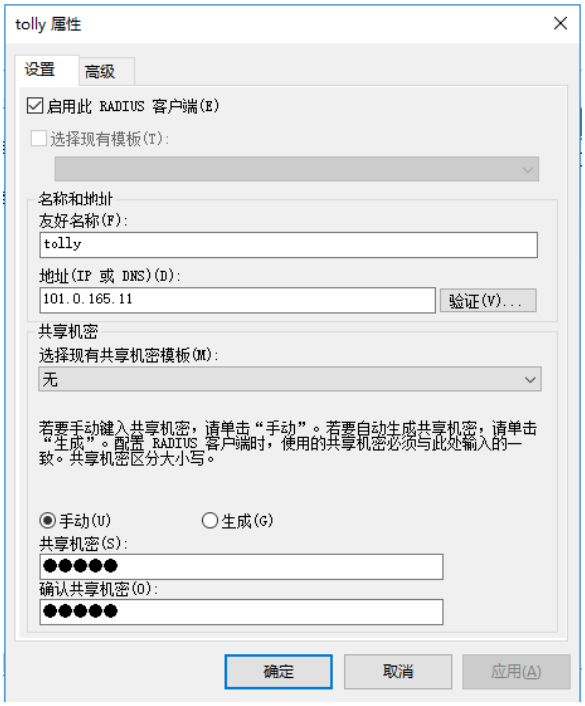
选择“RADIUS 客户端”，右键点击新建。

图4-11 新建 RADIUS 客户端



在弹窗中配置RADIUS客户端的属性，包括名称和IP地址，注意“共享机密”需要与Switch上的配置保持一致。

图4-12 配置 RADIUS 客户端属性



点击<确定>，完成 RADIUS 客户端配置。

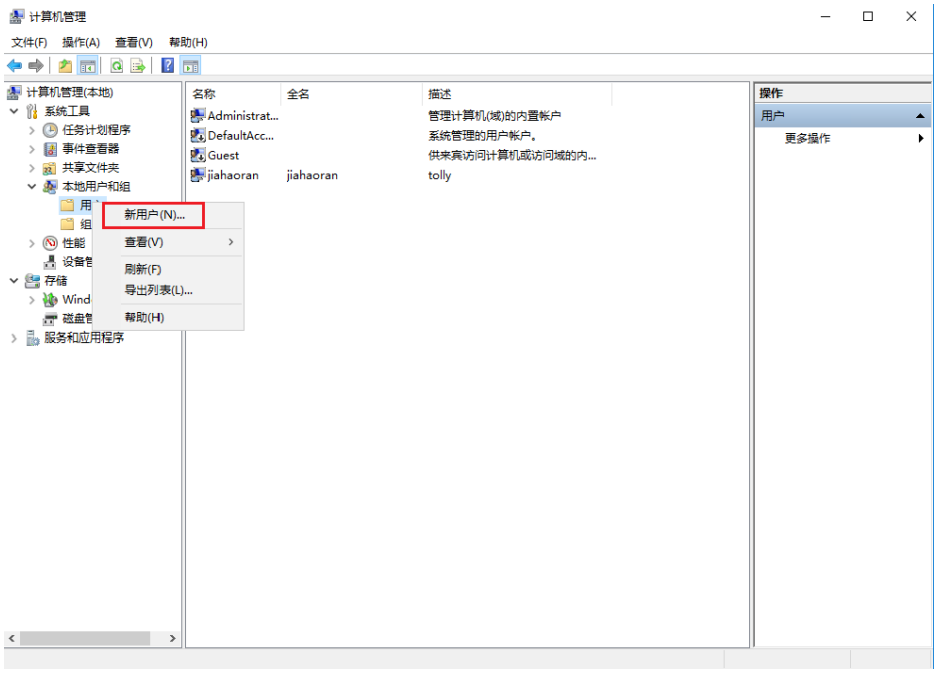
(5) 添加用户

在“服务器管理器-仪表板”界面，依次点击“工具 » 计算机管理”。

图4-13 打开计算机管理

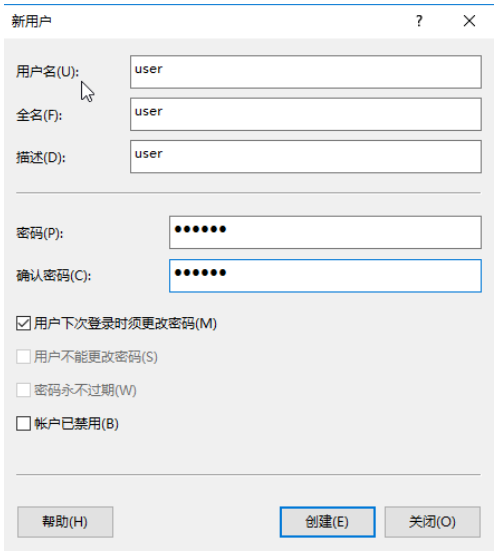
在“计算机管理”中，选中“用户”，右键选择“新用户”。

图4-14 添加新用户



创建的新用户应该与 Switch 上配置的固定用户名的 MAC 地址认证用户账号相同，本例用户名为“user”，密码为“123456”。点击<创建>。

图4-15 配置新用户



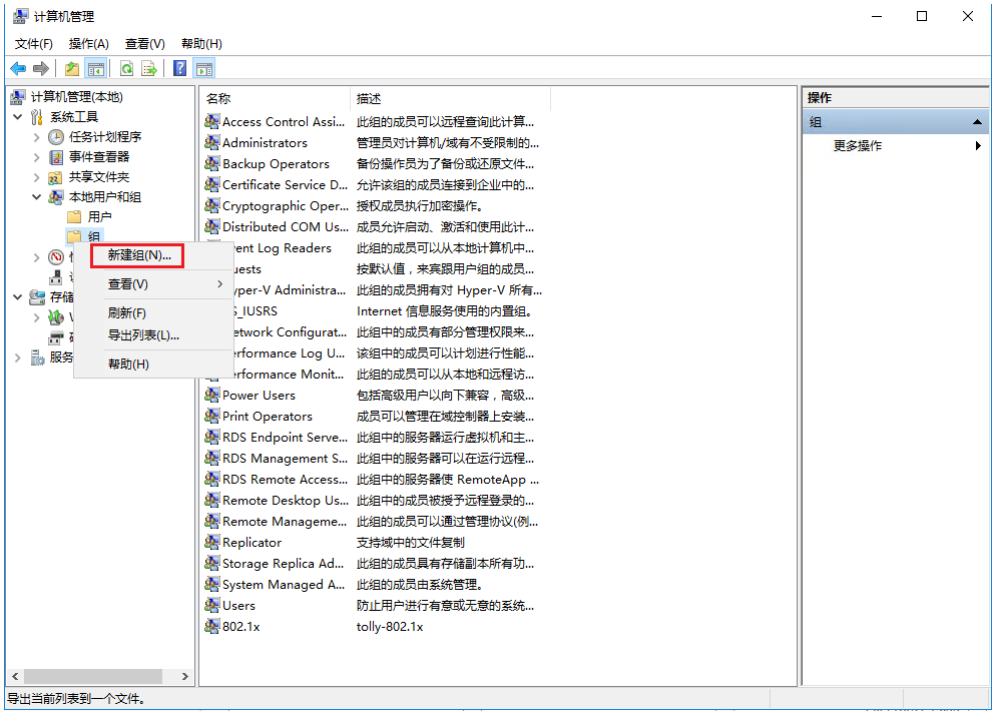
在“计算机管理”中，选中刚创建的用户“user”，配置该用户的属性。在“拨入”页签中，选择网络访问权限为“允许访问”。点击<确定>完成配置。

图4-16 配置用户接入属性的网络访问权限为允许访问

(6) 添加组

在“计算机管理”中，选择“组”，右键选择“新建组”。

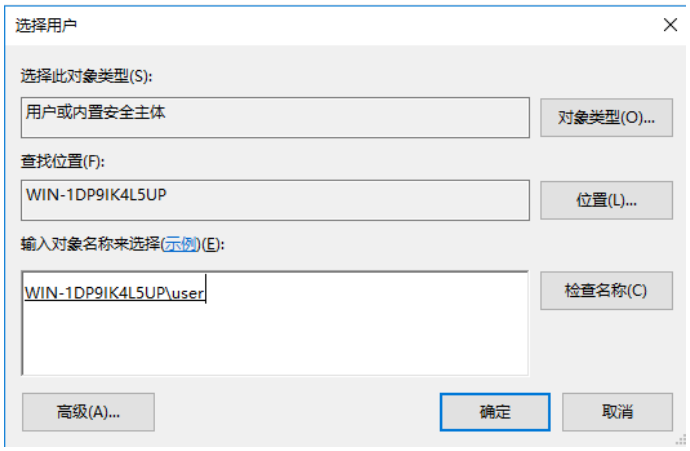
图4-17 新建组



在弹窗中设置组名，本例为“group1”，并添加组成员，这里需要把用户“user”添加为成员。点击<创建>，完成组的创建。

图4-18 配置组名

图4-19 添加组成员



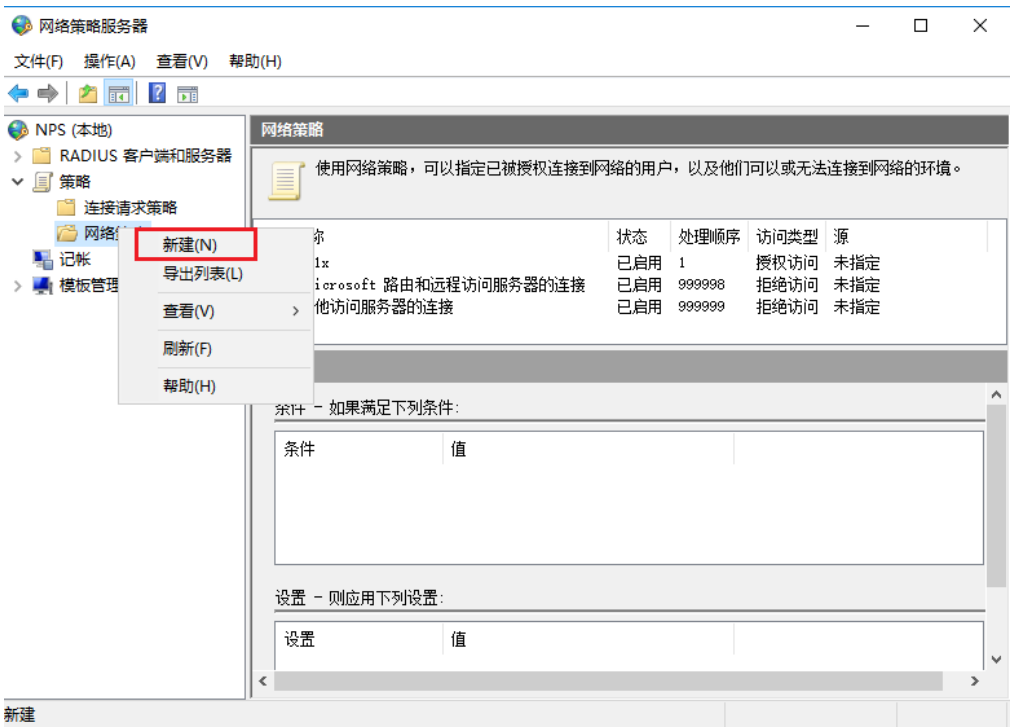
(7) 添加策略

在“服务器管理器-仪表板”界面，依次点击“工具 » 网络策略服务器”。

图4-20 打开网络策略服务器

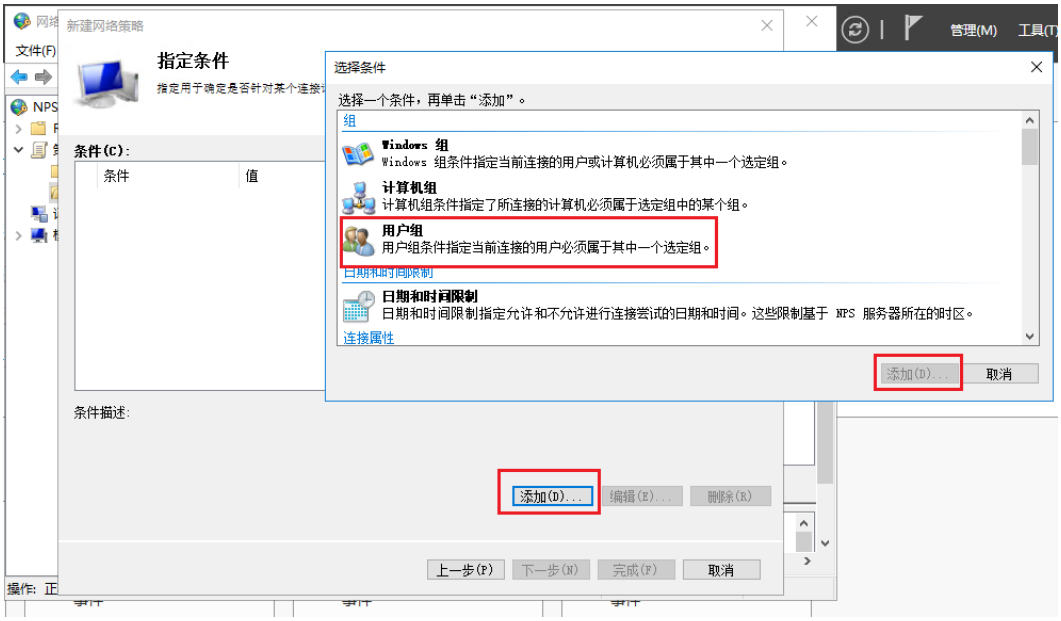
在“网络策略服务器”中，选择“网络策略”，右键选择“新建”，可添加一个新的网络策略。

图4-21 新建网络策略



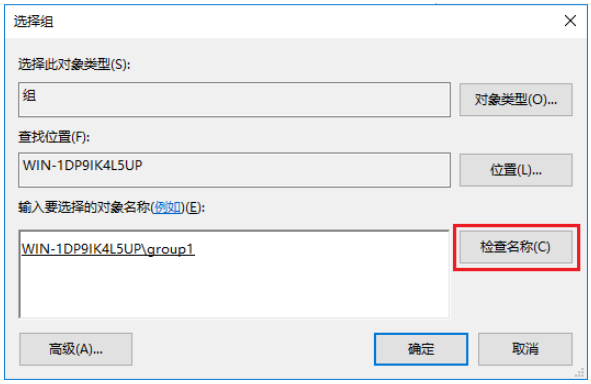
在新建的网络策略中，点击<添加>按钮，在弹窗中选择“用户组”，点击<添加>按钮。

图4-22 添加用户组



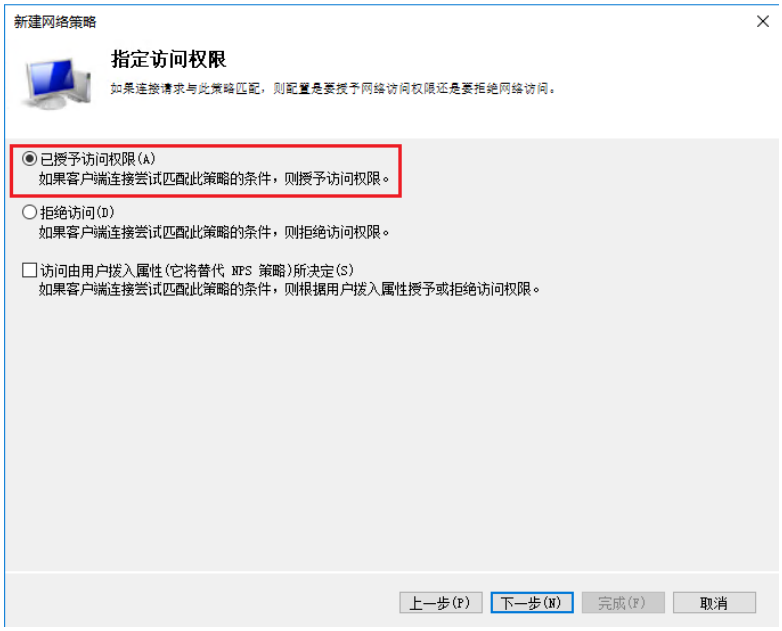
在“选择组”配置中的“输入要选择的对象名称”中输入组名（本例为 group1），点击<检查名称>，将联想出“WIN-RS0C6TAF7VG\group1”，点击<确定>完成配置。

图4-23 组配置



指定访问权限保持默认配置“已授予访问权限”，点击<下一步>。

图4-24 指定访问权限



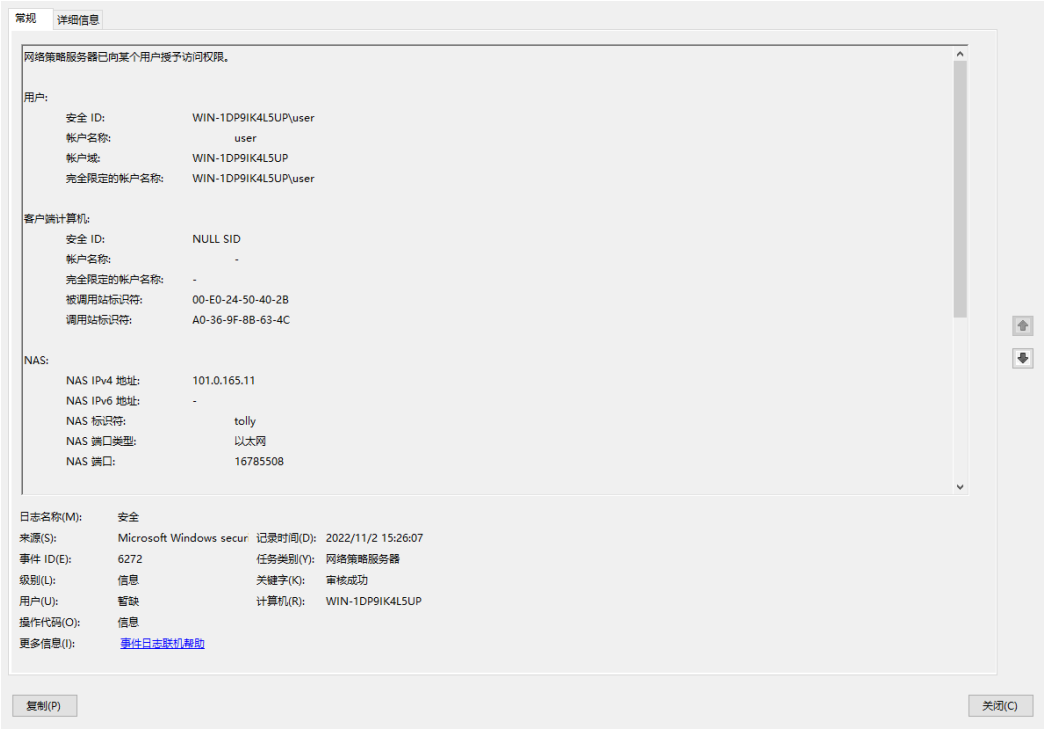
在“配置身份验证方法”步骤中，勾选“加密的身份验证”，点击<下一步>，完成配置。

4.3.3 验证配置

(1) 完成设备和服务器的配置后，MAC 地址认证用户 Ping 服务器即可完成上线。

(2) 用户上线后，服务器可显示用户的相关信息，具体参见图 4-25。

图4-25 用户上线验证



(3) 用户上线后，通过在设备上执行 **display mac-authentication connection** 可以看到上线用户的信息，对于固定用户名密码的 MAC 地址认证用户，Username 字段为 Switch 上配置的固定用户名 user。

```
<Switch> display  mac-authentication connection
Total connections: 1
Slot ID: 1
User MAC address: a036-9f8b-634c
Access interface: GigabitEthernet1/0/2
Username: user
User access state: Successful
Authentication domain: mac-auth
IPv4 address: 101.0.165.12
IPv4 address source: User packet
Initial VLAN: 165
Authorization untagged VLAN: N/A
Authorization tagged VLAN: N/A
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Authorization IPv6 URL: N/A
Authorization temporary redirect: Disabled
```

```
    Start accounting: Successful
    Real-time accounting-update failures: 0
    Termination action: Default
    Session timeout period: N/A
    Offline detection: 300 sec (command-configured)
    Online from: 2013/01/08 02:47:40
    Online duration: 0h 26m 8s
    Port-down keep online: Disabled (offline)
```

4.3.4 配置文件

```
#
 mac-authentication
 mac-authentication domain mac-auth
mac-authentication user-name-format fixed account user password cipher
$c$3$2HmbYwuGcvFCwTALdWqK5AzOvn2w5SY=
 mac-authentication authentication-method chap
#
domain mac-auth
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 accounting lan-access radius-scheme radius1
#
radius scheme radius1
 primary authentication 101.0.144.123
 primary accounting 101.0.144.123
 key authentication cipher $c$3$9jjl0lp5VA/WXEw065ZIT7j4AIN88XTF
 key accounting cipher $c$3$fk1zm9nf2IFMdk+I7hGsyBcsAwqLobi7
 user-name-format without-domain
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 165
 mac-authentication
#
```

4.4 MAC地址作为用户名密码的MAC地址认证配置步骤与验证

说明

若采用 MAC 地址账号，则设备将检测到的用户 MAC 地址作为用户名和密码发送给 RADIUS 服务器进行验证。

4.4.1 配置 Switch

其它配置与“4.3.1 配置 Switch”相同，只需要将以下命令恢复缺省配置即可。

```
[Switch] undo mac-authentication user-name-format
```

4.4.2 配置 Windows Server 2016-NPS

除以下用户和组的配置有修改外，其它与“4.3.2 配置 Windows Server 2016-NPS”配置相同。

本例采用 MAC 地址作为用户名和密码，因此服务器上添加的用户和密码，均为 MAC 地址认证用户的 MAC 地址。

在“服务器管理器-仪表板”界面，依次点击“工具 » 计算机管理 »本地用户和组”，根据图 4-26、图 4-27、图 4-28 和图 4-29 添加新用户和组。

图4-26 添加用户

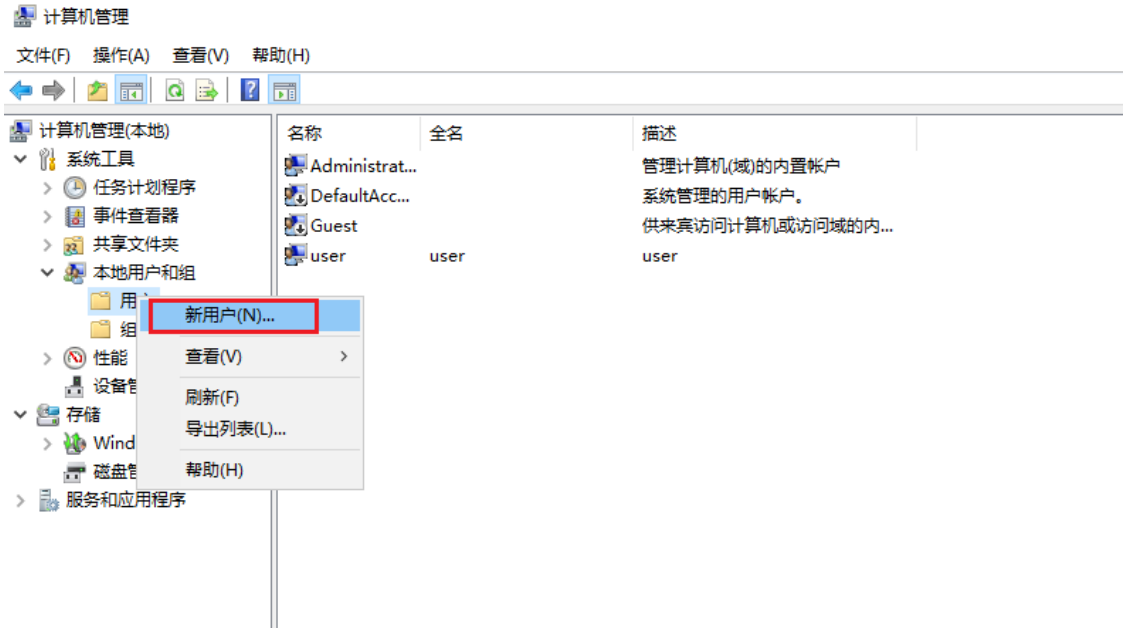
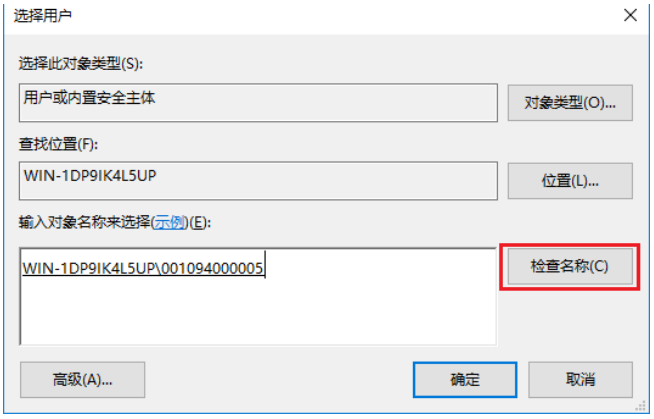


图4-27 输入用户名和密码

图4-28 添加用户组

图4-29 添加组用户



4.4.3 验证配置

(1) 完成设备和服务器的配置后，MAC 地址认证用户 Ping 服务器即可完成上线。

(2) 用户上线后，服务器可显示用户的相关信息，具体参见图 4-30。

图4-30 用户上线验证

(3) 用户上线后，通过在设备上执行 **display mac-authentication connection** 可以看到上线用户的信息，其中 Username 字段为用户的 MAC 地址。

```
[Switch] display  mac-authentication connection
Total connections: 1
Slot ID: 1
User MAC address: 0010-9400-0005
Access interface: GigabitEthernet1/0/2
Username: 001094000005
User access state: Successful
Authentication domain: mac-auth
IPv4 address: 101.0.165.12
IPv4 address source: User packet
Initial VLAN: 165
Authorization untagged VLAN: N/A
Authorization tagged VLAN: N/A
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Authorization IPv6 URL: N/A
Authorization temporary redirect: Disabled
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: N/A
```

```
    Offline detection: 300 sec (command-configured)
    Online from: 2013/01/08 05:10:17
    Online duration: 0h 0m 16s
    Port-down keep online: Disabled (offline)
```

4.4.4 配置文件

```
#
 mac-authentication
 mac-authentication domain mac-auth
mac-authentication user-name-format mac-address without-hyphen uppercase
 mac-authentication authentication-method chap
#
domain mac-auth
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 accounting lan-access radius-scheme radius1
#
radius scheme radius1
 primary authentication 101.0.144.123
 primary accounting 101.0.144.123
 key authentication cipher $c$3$9jjl0lp5VA/WXEw065ZIT7j4AIN88XTF
 key accounting cipher $c$3$fk1zm9nf2IFMdk+I7hGsyBcsAwqLobi7
 user-name-format without-domain
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 165
 mac-authentication
#
```

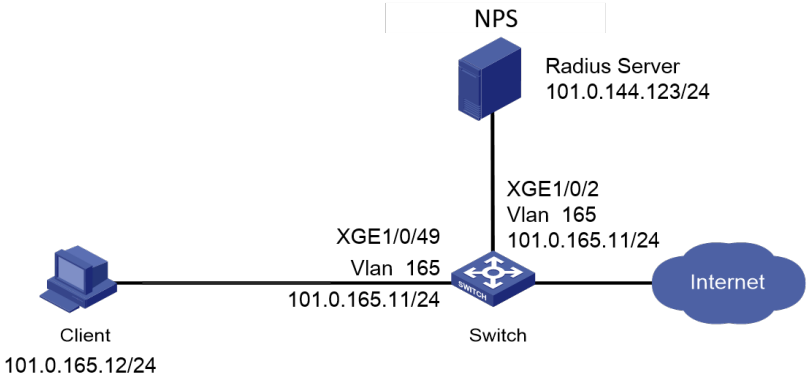
5 802.1X 认证对接配置举例

5.1 组网需求

如图 5-1 所示，Client 和 Windows Server 2016-NPS 服务器通过 Switch 建立连接，设备管理员希望对 Client 进行 802.1X 认证，以控制其对网络资源的访问，具体要求如下：

- 采用 Windows Server 2016-NPS 作为 RADIUS 服务器。
- 配置 PAP、CHAP、证书相关认证（EAP-PEAP）方式。

图5-1 802.1X 认证配置组网图



5.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch： S5560X-54C-PWR-EI，Version 7.1.070
- 认证服务器：Windows Server 2016-NPS

5.3 802.1X CHAP配置步骤与验证

说明

本配置仅展示认证的相关配置，网络互通的相关配置略，请保证设备间能够互相访问。

5.3.1 配置 Switch

配置 RADIUS 方案。

```
<Switch> system-view
[Switch] radius scheme radius1
[Switch-radius-radius1] primary authentication 101.0.144.123
[Switch-radius-radius1] primary accounting 101.0.144.123
[Switch-radius-radius1] key authentication simple admin
[Switch-radius-radius1] key accounting simple admin
[Switch-radius-radius1] user-name-format without-domain
[Switch-radius-radius1] quit
```

配置 802.1x 认证的认证方法。

```
[Switch] dot1x authentication-method CHAP
```

创建 802.1X 认证的域 domain1，配置 ISP 域的 AAA 方法。

```
[Switch] domain domain1
[Switch-isp-domain1] authentication default radius-scheme radius1
[Switch-isp-domain1] authorization lan-access radius-scheme radius1
[Switch-isp-domain1] accounting lan-access radius-scheme radius1
```

```
[Switch-isp-domain1] quit
```
配置互通的 VLAN 和 VLAN 接口的 IP 地址。
```
[Switch] vlan 165
[Switch-vlan165] quit
[Switch] interface Vlan-interface 165
[Switch-Vlan-interface165] ip address 101.0.165.11 255.255.255.0
[Switch-Vlan-interface165] quit
```
将端口 XGE1/0/49 加入到指定 VLAN。
```
[Switch]interface Ten-GigabitEthernet 1/0/49
[Switch-Ten-GigabitEthernet1/0/49] port access vlan 165
```
开启端口的 802.1X 认证功能，并设置域 domain1 为 802.1X 强制认证域。
```
[Switch-Ten-GigabitEthernet1/0/49] dot1x
[Switch-Ten-GigabitEthernet1/0/49] dot1x mandatory-domain domain1
```
设置 802.1X 为端口控制方式。
```
[Switch-Ten-GigabitEthernet1/0/49] dot1x port-method portbased
[Switch-Ten-GigabitEthernet1/0/49] quit
```
将端口 XGE1/0/2 加入到指定 VLAN。
```
[Switch] interface Ten-GigabitEthernet 1/0/2
[Switch-Ten-GigabitEthernet1/0/2] port access vlan 165
[Switch-Ten-GigabitEthernet1/0/2] quit
```
设置 domain1 为系统缺省的认证域。
```
[Switch] domain default enable domain1
```
开启全局 802.1x 认证。
```
[Switch] dot1x
```

5.3.2 配置 Windows Server 2016-NPS

需要注意：除了添加的新用户，需要 802.1X 用户的用户名和密码保持一致外，其它与“4.3.2 配置 Windows Server 2016-NPS”配置相同。

在“服务器管理器-仪表板”界面，依次点击“工具 » 计算机管理 » 本地用户和组”，如图 5-2 添加新用户。

图5-2 添加新用户

5.3.3 验证配置

(1) 在设备和服务器都配置好的情况下，在客户端使用 iNode 客户端，输入服务器上配置的用户名和密码即可完成用户上线。

图5-3 802.1X 客户端接入

图5-4 802.1X 客户端连接成功

(2) 用户上线后服务器显示如图 5-5 所示。

图5-5 802.1X 用户接入成功

(3) 用户上线后，通过 **display dot1x connection** 可以查看 802.1X 用户的信息，可其中 Username 字段为 802.1X 的用户名（本例为 user）。

```
[Switch] display  dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: a036-9f8b-634c
Access interface: GigabitEthernet1/0/2
Username: user
User access state: Successful
Authentication domain: domain1
EAP packet identifier: 2
Authentication method: CHAP
AAA authentication method: RADIUS
Initial VLAN: 165
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Authorization IPv6 URL: N/A
Authorization temporary redirect: Disabled
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
```

```
    Session timeout period: N/A
    Online from: 2013/01/03 08:22:24
    Online duration: 0h 0m 35s
```

5.3.4 配置文件

```
#
 dot1x
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 1 100 165 untagged
 port hybrid pvid vlan 165
undo dot1x handshake
 dot1x mandatory-domain domain1
 undo dot1x multicast-trigger
 dot1x port-method portbased
#
domain domain1
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 accounting lan-access radius-scheme radius1
#
radius scheme radius1
 primary authentication 101.0.144.123
 primary accounting 101.0.144.123
 key authentication cipher $c$3$9jjl0lp5VA/WXEw065ZIT7j4AIN88XTF
 key accounting cipher $c$3$fk1zm9nf2IFMdk+I7hGsyBcsAwqLobi7
 user-name-format without-domain
#
```

5.4 802.1X PAP认证配置步骤与验证

5.4.1 配置 Switch

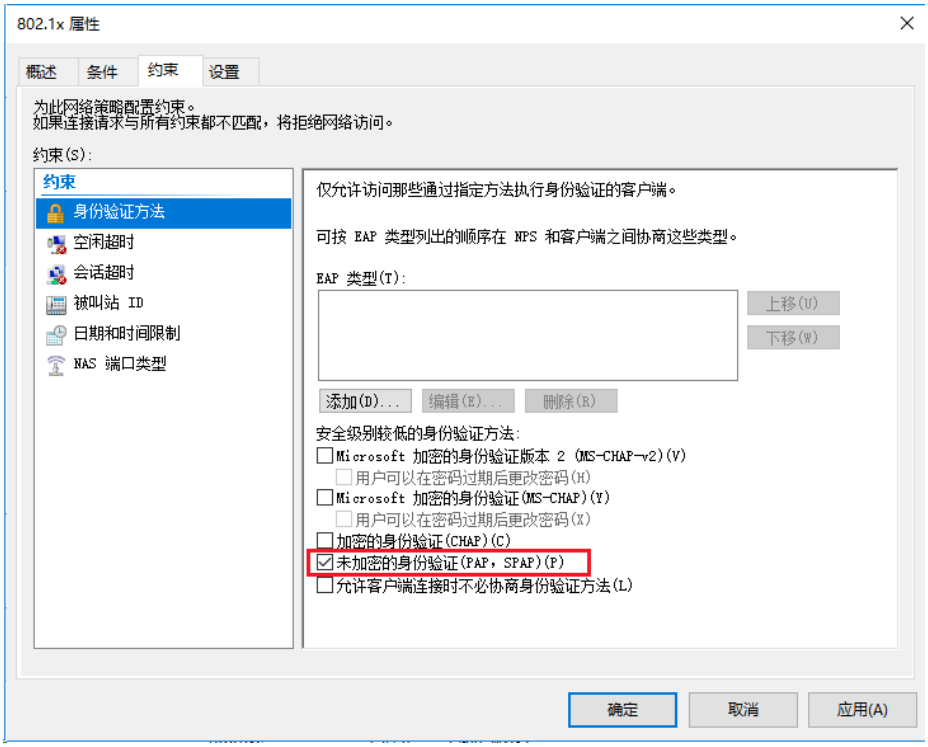
设备上只需要将认证方式修改为 PAP，其它配置无需修改，请参考 5.3.1 配置 Switch。

```
[Switch] dot1x authentication-method PAP
```

5.4.2 配置 Windows Server 2016-NPS

根据图 5-6 所示，服务器上只需要将“服务”中的“身份验证方式”选择为“未加密的身份验证（PAP，SPAP）（P）”，其它配置无需修改，请参考 5.3.2 配置 Windows Server 2016-NPS。

图5-6 修改身份验证方式

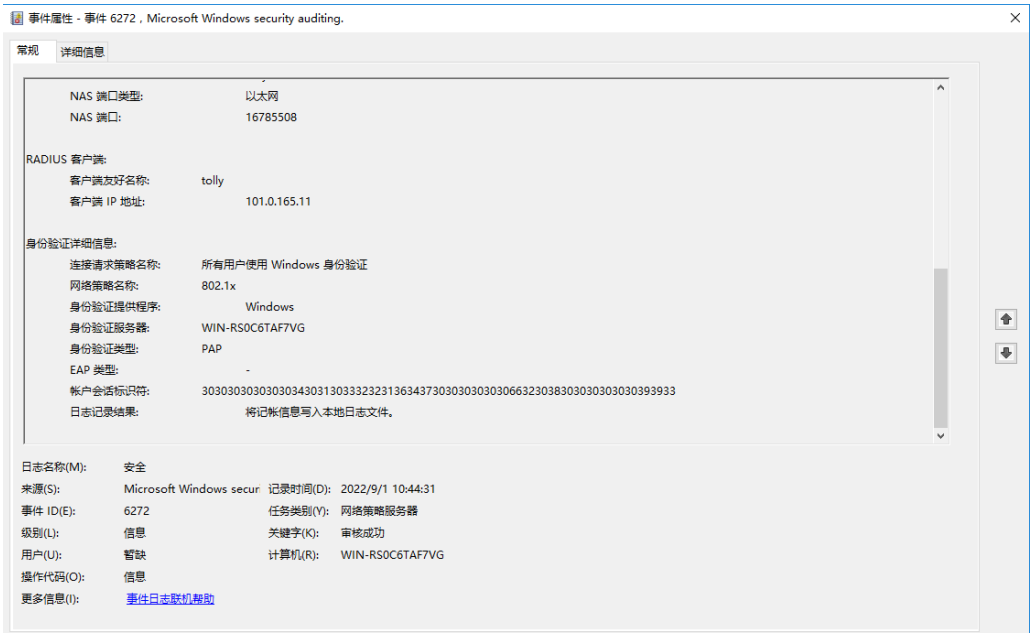


5.4.3 验证配置

(1) 在设备和服务器都配置好的情况下，在客户端使用 iNode 客户端，输入服务器上配置的用户名和密码即可完成用户上线。

(2) 用户上线后服务器显示如图 5-7 所示。

图5-7 认证成功后服务器显示



(3) 用户上线后，在设备上通过 **display dot1x connection** 可以查看 802.1X 用户的信息，可以看到上线用户的 Authentication method 字段已更改为 PAP。其余信息不变。

```
[Switch] display  dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: a036-9f8b-634c
Access interface: GigabitEthernet1/0/2
Username: user
User access state: Successful
Authentication domain: domain1
EAP packet identifier: 2
Authentication method: PAP
AAA authentication method: RADIUS
Initial VLAN: 165
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Authorization IPv6 URL: N/A
Authorization temporary redirect: Disabled
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
```

```
      Session timeout period: N/A
      Online from: 2013/01/03 08:25:51
      Online duration: 0h 0m 8s
```

5.4.4 配置文件

```
#
 dot1x
dot1x authentication-method pap
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 1 100 165 untagged
 port hybrid pvid vlan 165
undo dot1x handshake
 dot1x mandatory-domain domain1
 undo dot1x multicast-trigger
 dot1x port-method portbased
#
domain domain1
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 accounting lan-access radius-scheme radius1
#
radius scheme radius1
 primary authentication 101.0.144.123
 primary accounting 101.0.144.123
 key authentication cipher $c$3$9jjl0lp5VA/WXEw065ZIT7j4AIN88XTF
 key accounting cipher $c$3$fk1zm9nf2IFMdk+I7hGsyBcsAwqLobi7
 user-name-format without-domain
#
```

5.5 802.1X EAP-PEAP认证配置步骤与验证

5.5.1 配置 Switch

设备上只需要将认证方式修改为 EAP，其它配置无需修改，请参考 5.3.1 配置 Switch。

```
[Switch] dot1x authentication-method EAP
```

5.5.2 配置 Windows Server 2016-NPS

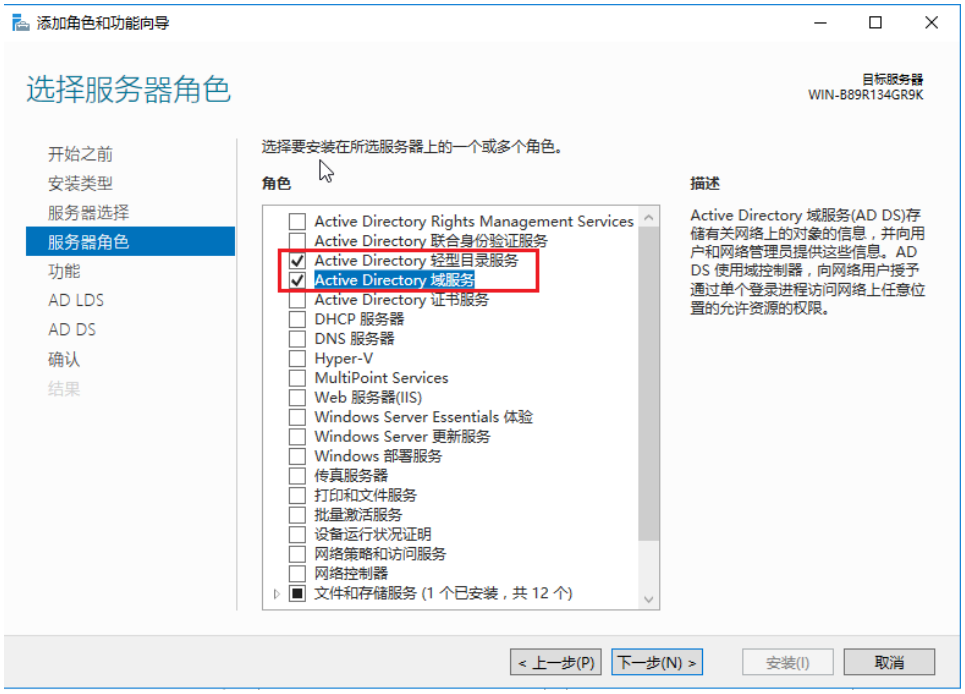
服务器上只需要修改如下配置，其余通用配置请参考 5.3.2 配置 Windows Server 2016-NPS。

(1) 配置 AD 域控用户管理

a. AD 域安装

根据图 5-8 所示，在“添加角色和功能向导”界面，点击“服务器角色”，勾选角色下的“Active Directory 轻型目录服务”和“Active Directory 域服务”，之后连续点击<下一步>，等待安装成功后关闭向导。

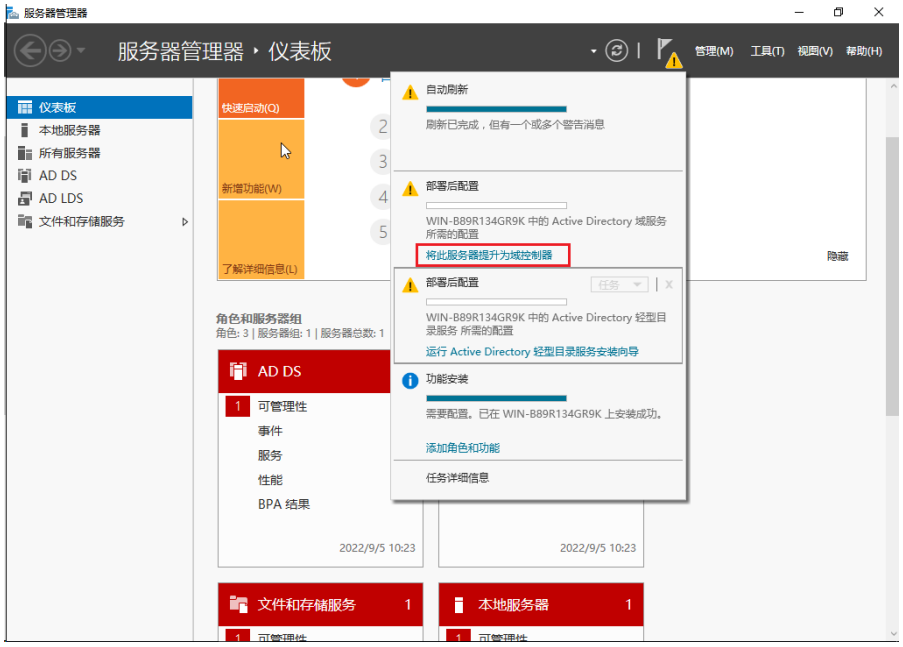
图5-8 选择服务器角色



b. 配置 AD 域控

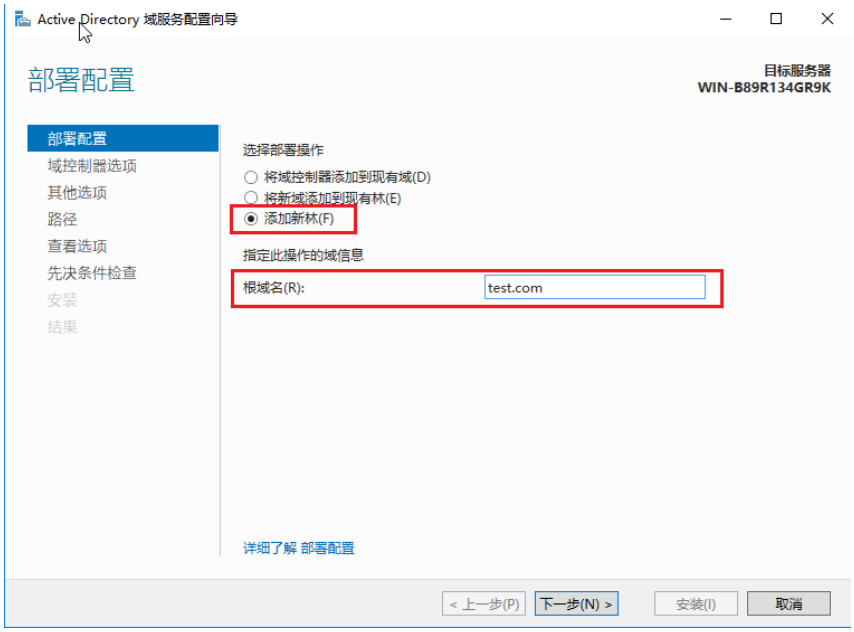
如图 5-9 所示，在“服务器管理器-仪表板”界面，依次点击“管理»将此服务器提升为域控制器”。

图5-9 将服务器提升为域控制器



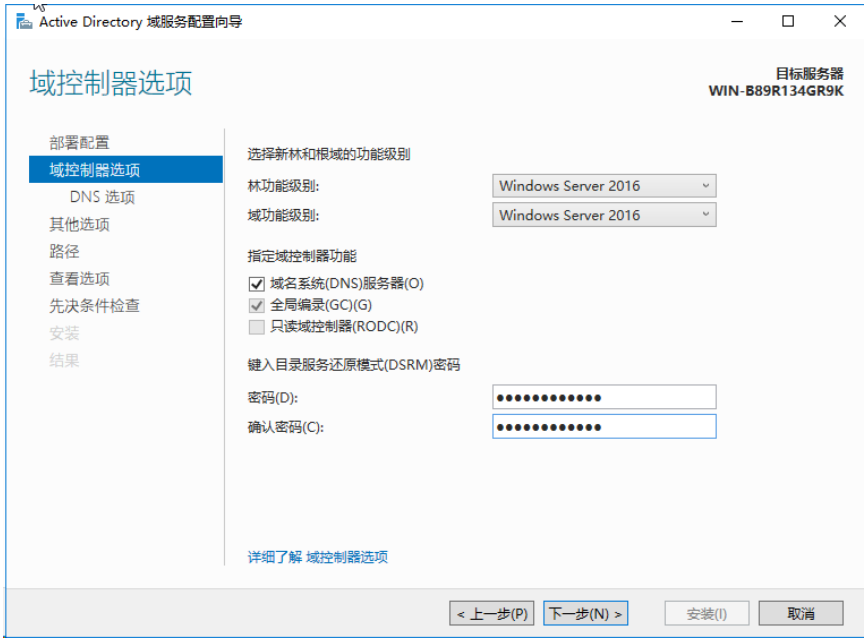
跳转到“Active Directory 域服务配置向导”界面后，点击左侧菜单中的“部署配置”页签，选择部署操作为“添加新林”并在下方输入“根域名”。

图5-10 部署配置



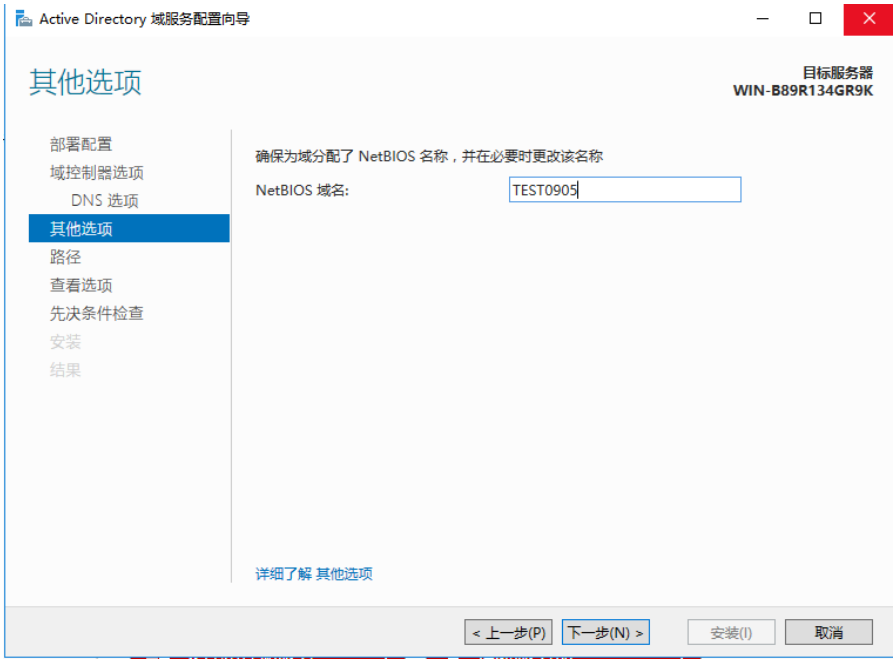
点击左侧菜单中的“域控制器选项”页签，在右侧输入 DSRM 密码。（“DNS 选项页”可忽略）

图5-11 配置域控制器选项



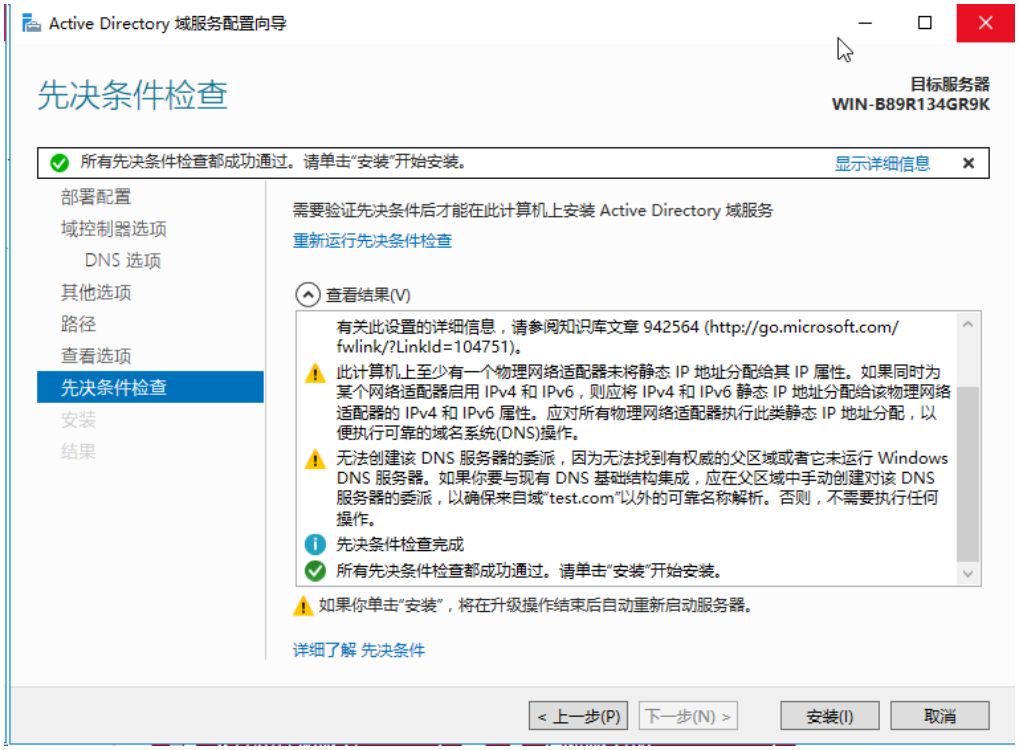
点击左侧菜单中的“其他选项”页签，输入 NetBIOS 域名。需要注意的是，此处请务必记录下域名，后续升级为域控服务器后需登录此域。

图5-12 配置其他选项



之后连续点击<下一步>，直到“先决条件检查”页签，此处需显示“所有先决条件检查都成功通过”，点击“安装”即可。然后等待安装完成，自动重新启动服务器。

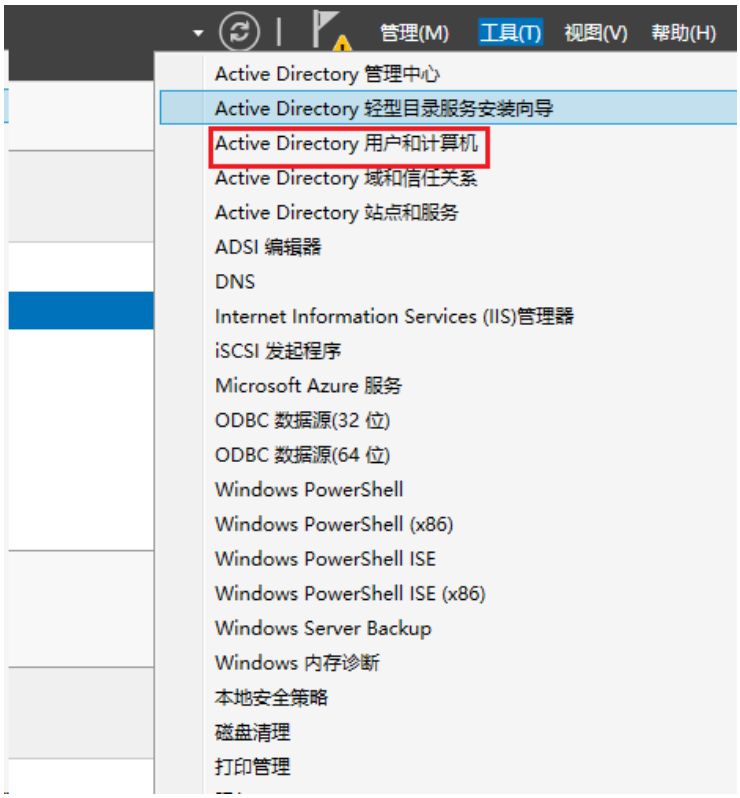
图5-13 先决条件检查



c. 创建 AD 用户

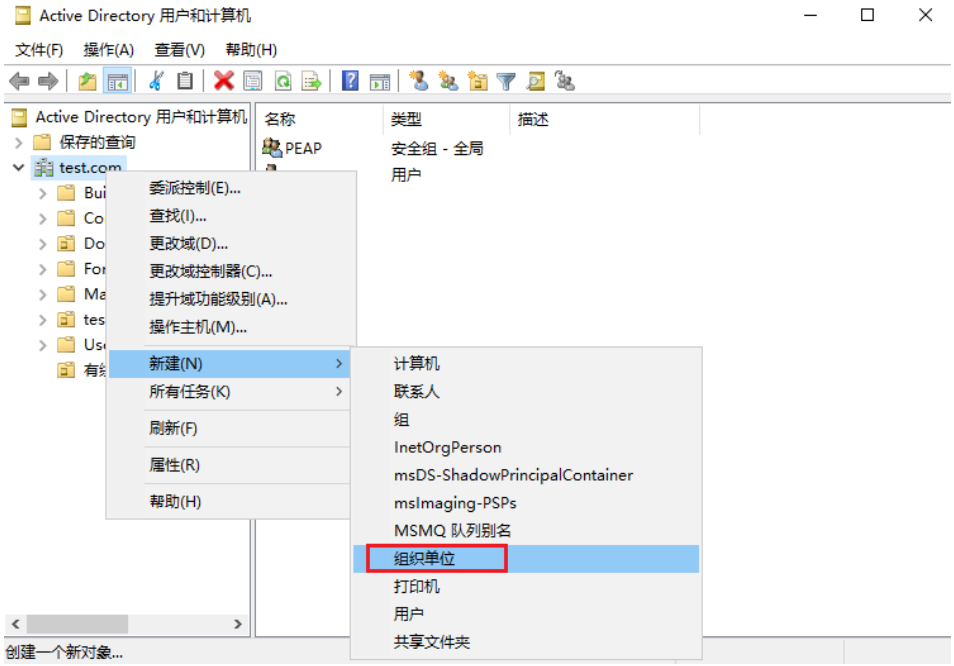
如图 5-14 所示，在“服务器管理器-仪表板”界面，依次点击“工具 » Active Directory 用户和计算机”，打开 AD 用户和计算机界面。

图5-14 打开 AD 用户和计算机界面



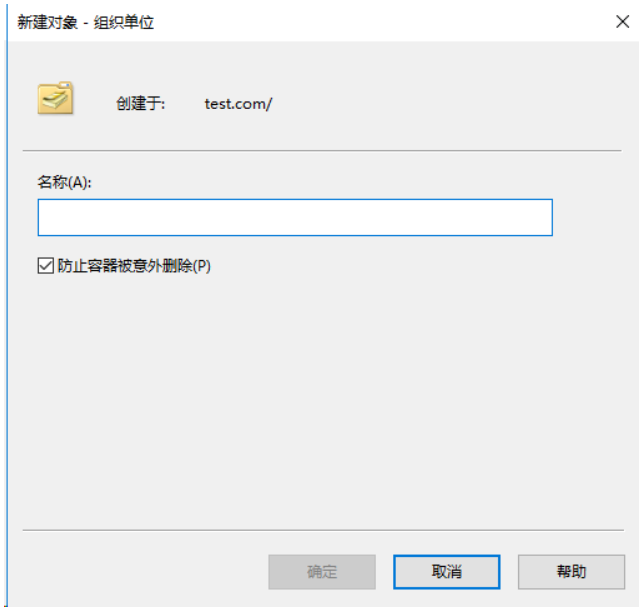
在弹窗页面中选择左侧根域名并点击鼠标右键，依次选择“新建 » 组织单位”。

图5-15 创建组织单位



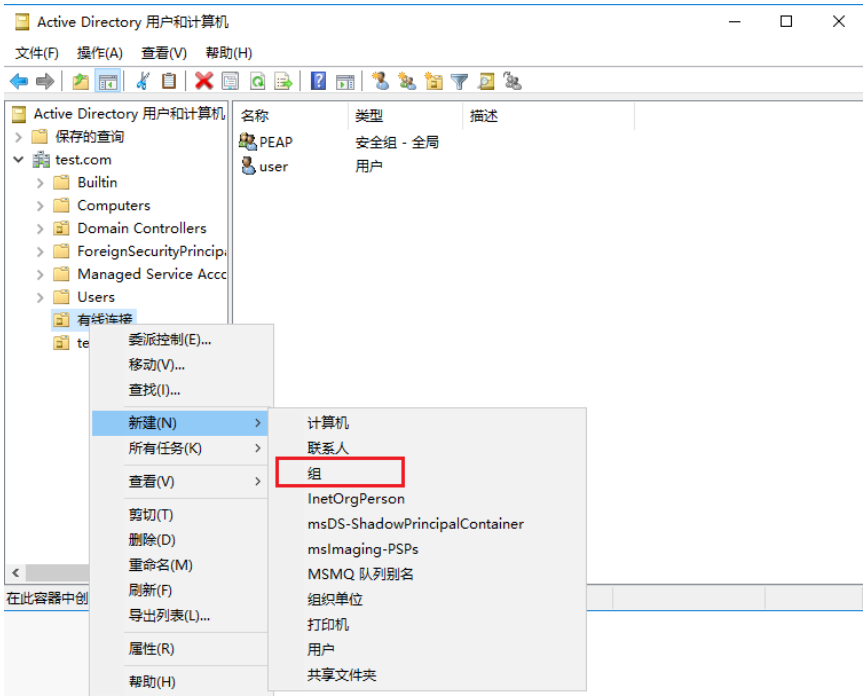
在弹窗页面中，输入组织单位名称，点击<确定>。

图5-16 输入组织单位名称



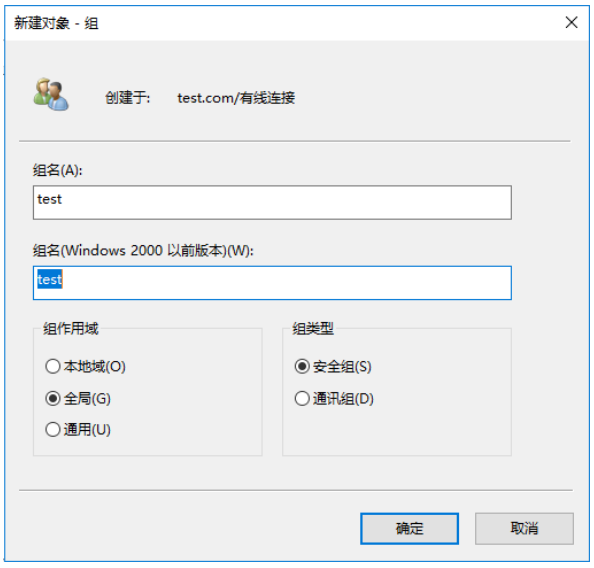
选择新建好的“组织单位”并点击右键，依次选择“新建 » 组”。

图5-17 新建组



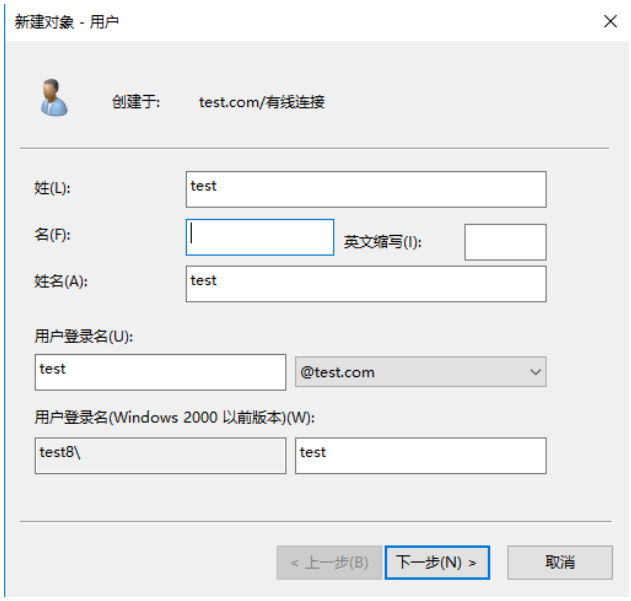
在弹窗页面中，输入“组名”，选择“组作用域”、“组类型”，点击<确定>。

图5-18 输入组名



选择新建好的“组织单位”并点击右键，依次选择“新建»用户”，如图 5-19 所示，输入用户姓名、用户登录名等信息。

图5-19 新建用户

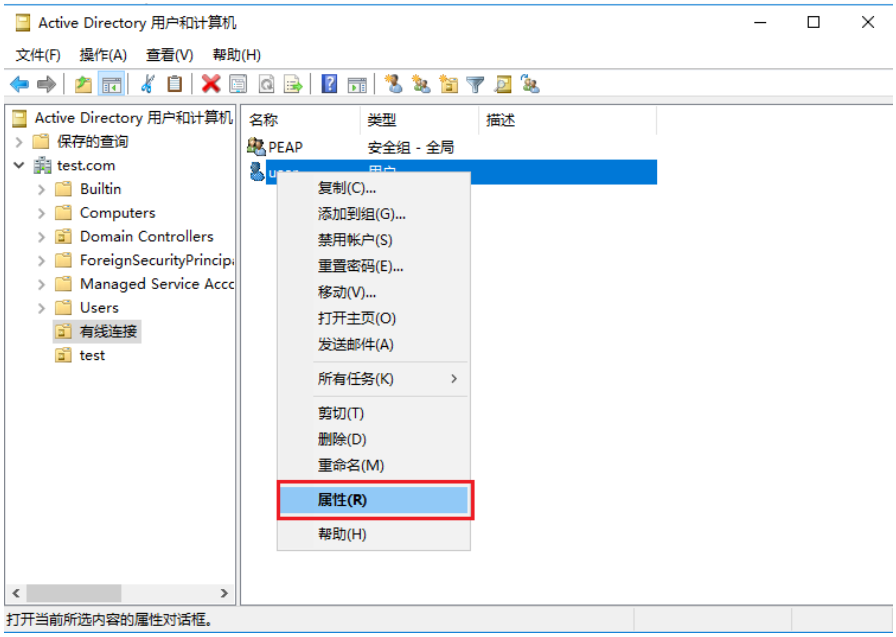


点击<下一步>，配置用户密码并确认密码。需要注意的是，务必记录密码，以免后续登录时遗忘。

图5-20 配置新建用户的密码

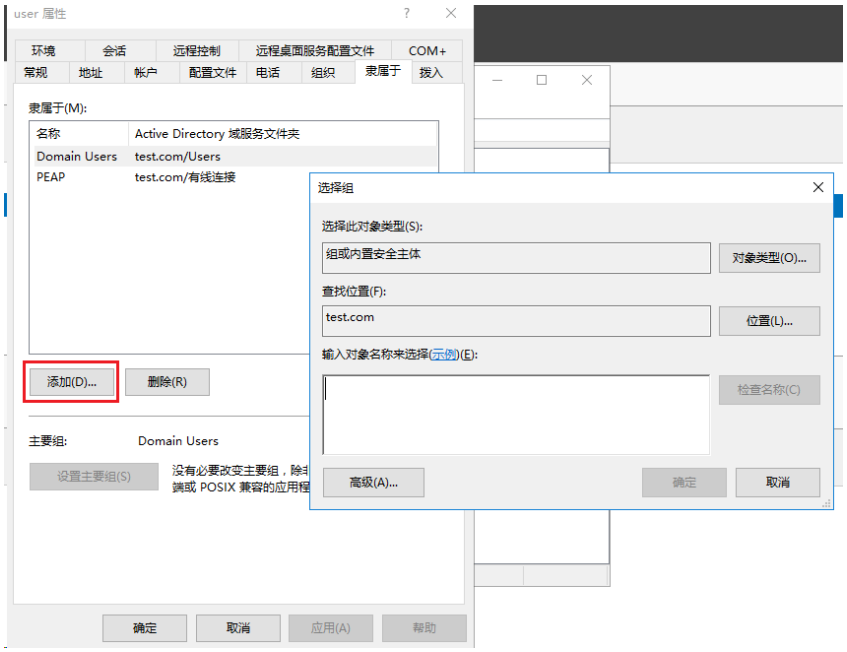
选择新建的用户，右键选择“属性”。

图5-21 打开新建用户的属性页面



在弹窗页面中，点击“隶属于”页签，点击下方<添加>，在弹窗中选择组，点击<确定>。

图5-22 在属性页面的隶属于页面中添加组

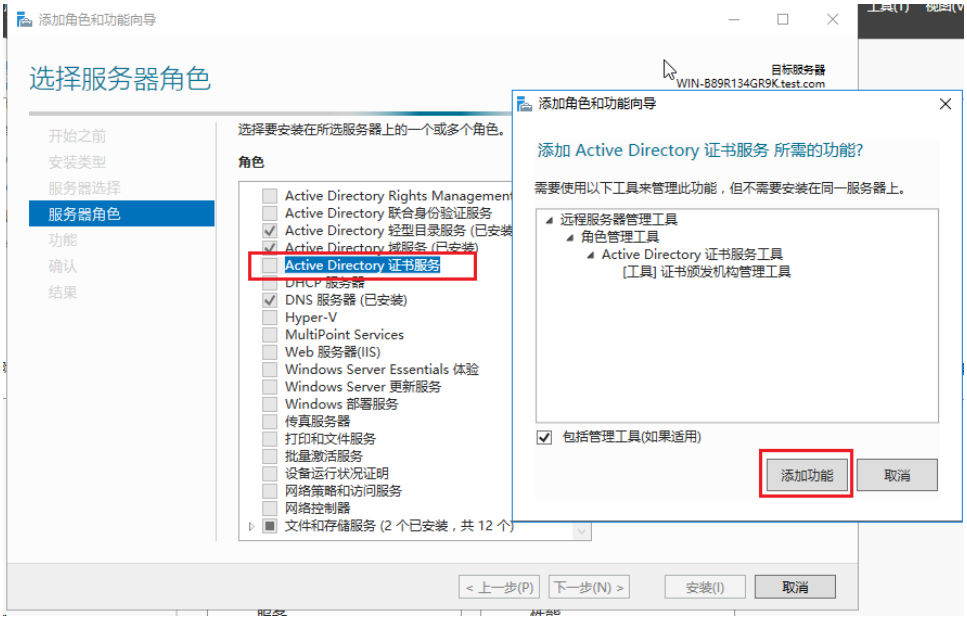


(2) Radius 安装

a. 安装 AD 证书

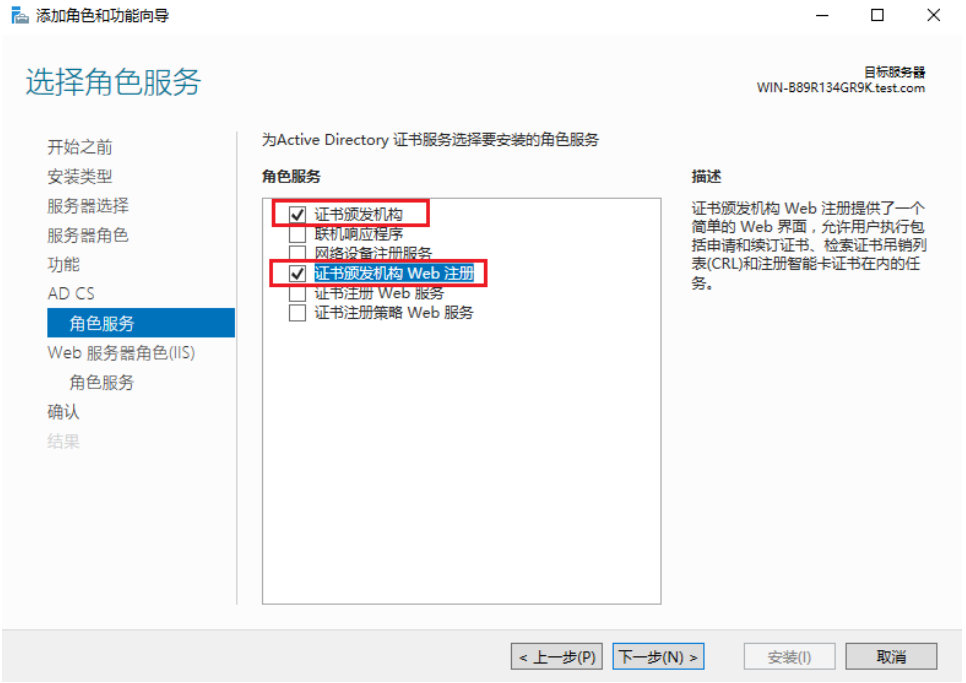
如图 5-23 所示，在“添加角色和功能向导”界面，选择左侧的“服务器角色”，勾选“Active Directory 证书服务”，并在弹窗页面点击<添加功能>。

图5-23 AD 证书服务



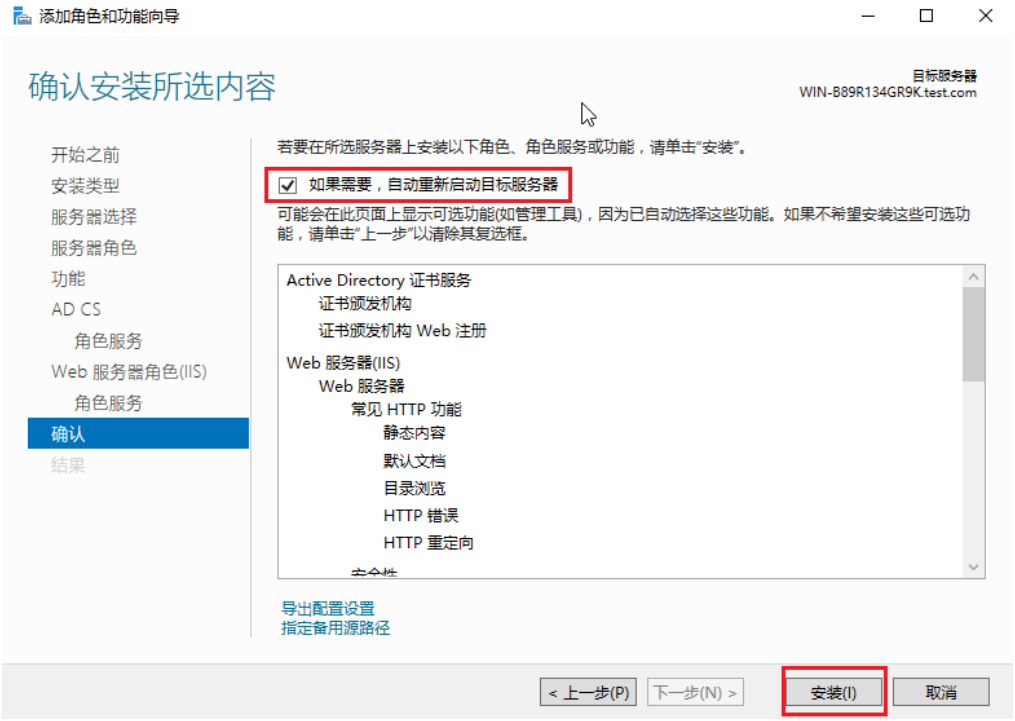
在“添加角色和功能向导”界面，选择左侧的“AD CS » 角色服务”，勾选“证书颁发机构”和“证书颁发机构 Web 注册”，之后一直点击<下一步>即可。

图5-24 配置角色服务



直至“确认”页时，勾选“如果需要，自动重新启动目标服务器”，点击<安装>，完成 AD 证书的安装。

图5-25 确认页面



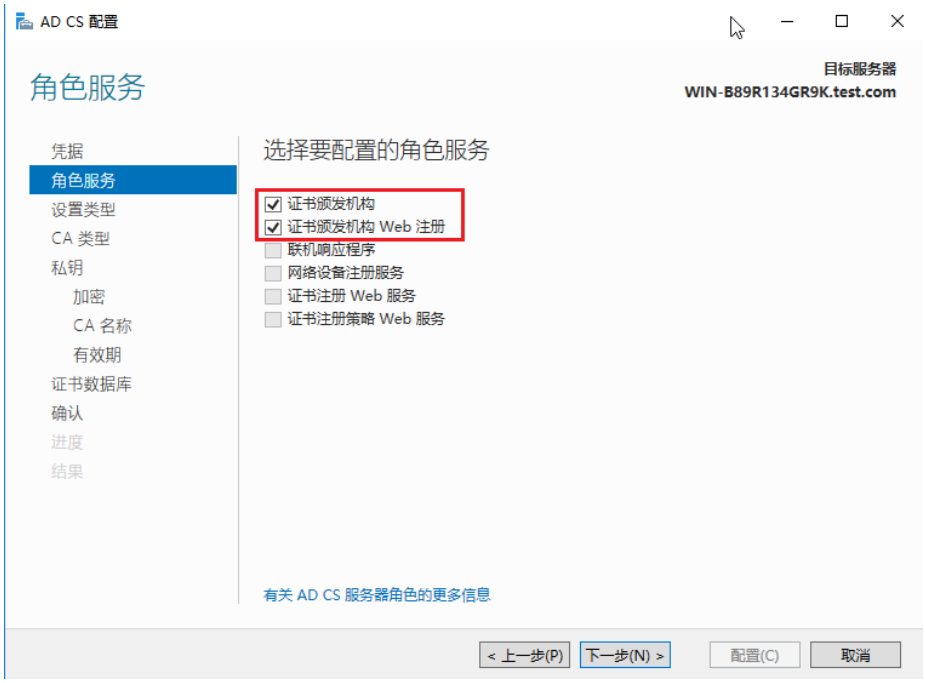
b. 配置 AD 证书

如图 5-26 所示，在“服务器管理器-仪表板”界面，依次点击“管理 » 配置目标服务器上的 Active Directory 证书服务”。

图5-26 配置目标服务器上的 Active Directory 证书服务

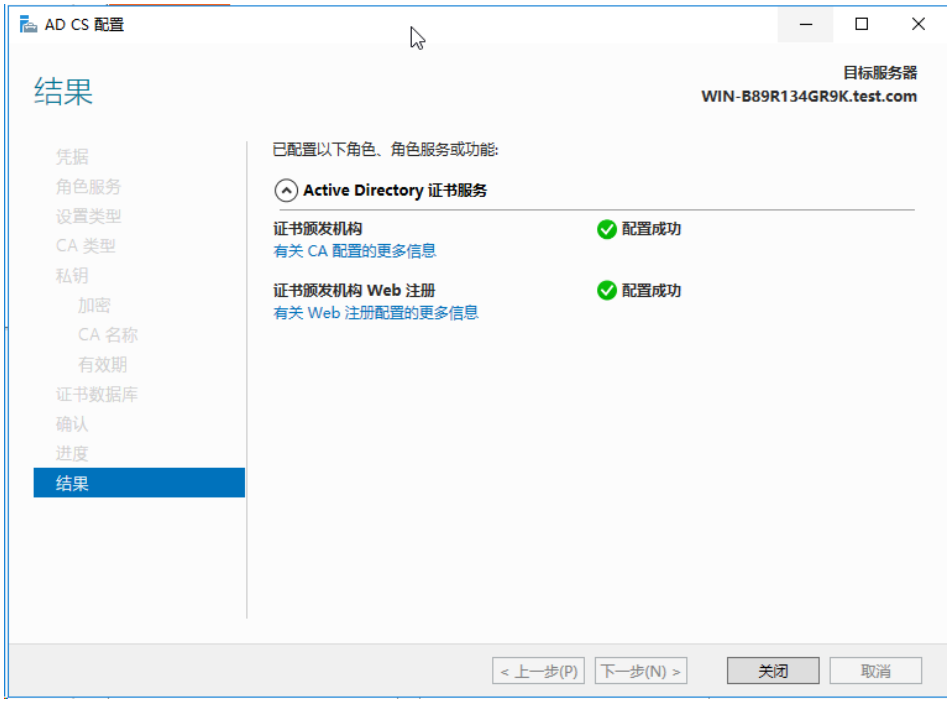
在弹窗页面左侧选择“角色服务”，并勾选“证书颁发机构”和“证书颁发机构 Web 注册”。

图5-27 配置角色服务



后续页面一直点击<下一步>，直至最终显示配置成功，如图 5-28 所示。

图5-28 配置成功页面



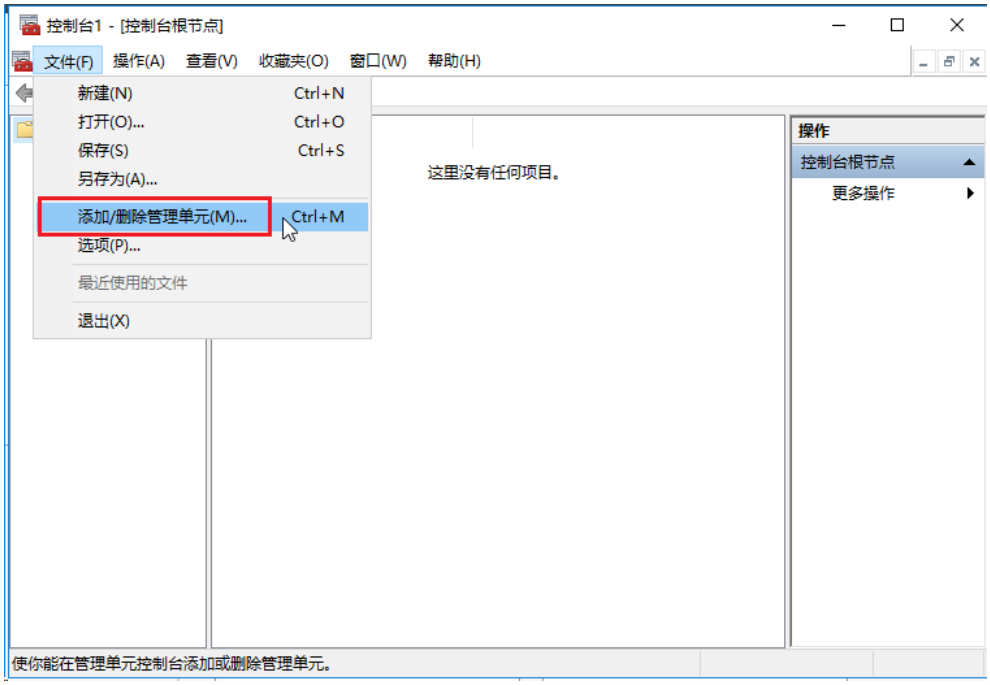
c. 申请 CA 证书

通过搜索栏打开 mmc。

图5-29 打开 mmc

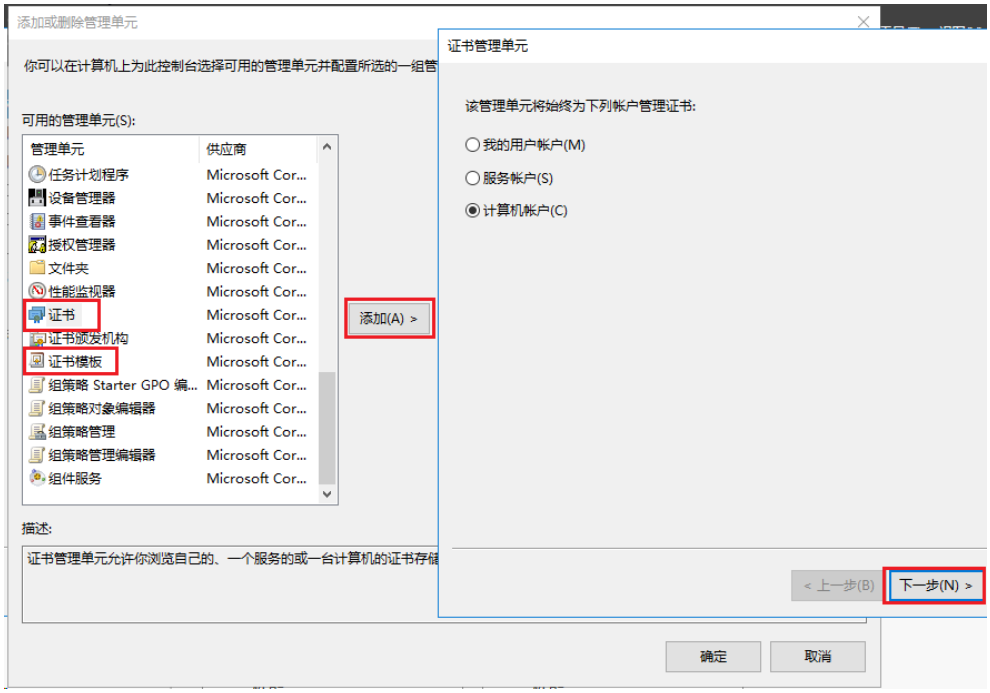
在“控制台”界面，依次点击“文件 » 添加/删除管理单元”。

图5-30 添加/删除管理单元



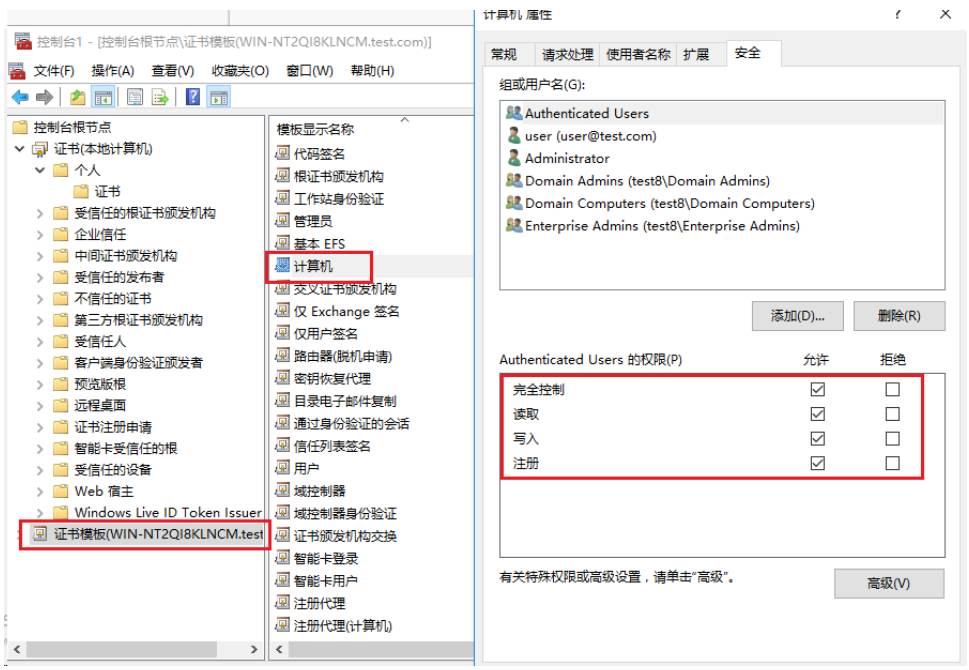
将弹窗界面左侧的“证书”和“证书模板”两个管理单元添加到控制台，依次点击<下一步>。

图5-31 添加证书、证书模板两个管理单元



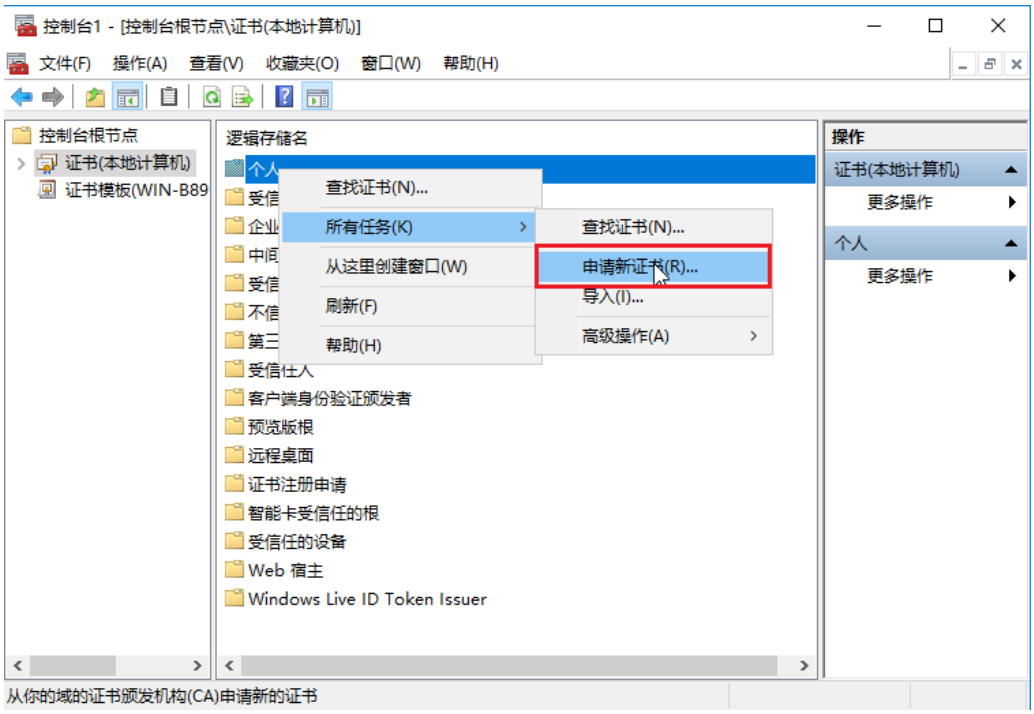
在“证书模板”管理单元选择“计算机 ”并点击右键，在“计算机 属性”弹窗页面选择“安全”页签，将登录计算机的 Administrator 加入其中，并勾选“完全控制”权限。

图5-32 修改证书模板页面



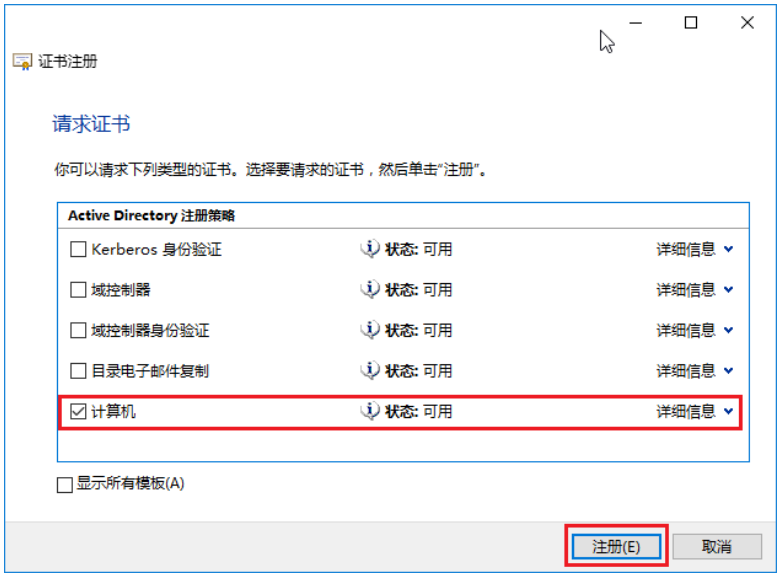
在“证书”管理单元选择“个人”并点击右键，依次点击“所有任务 » 申请根证书”。

图5-33 申请根证书



在弹窗页面勾选“计算机”注册策略，点击<注册>，完成证书注册。

图5-34 勾选注册策略



d. 安装 NPS

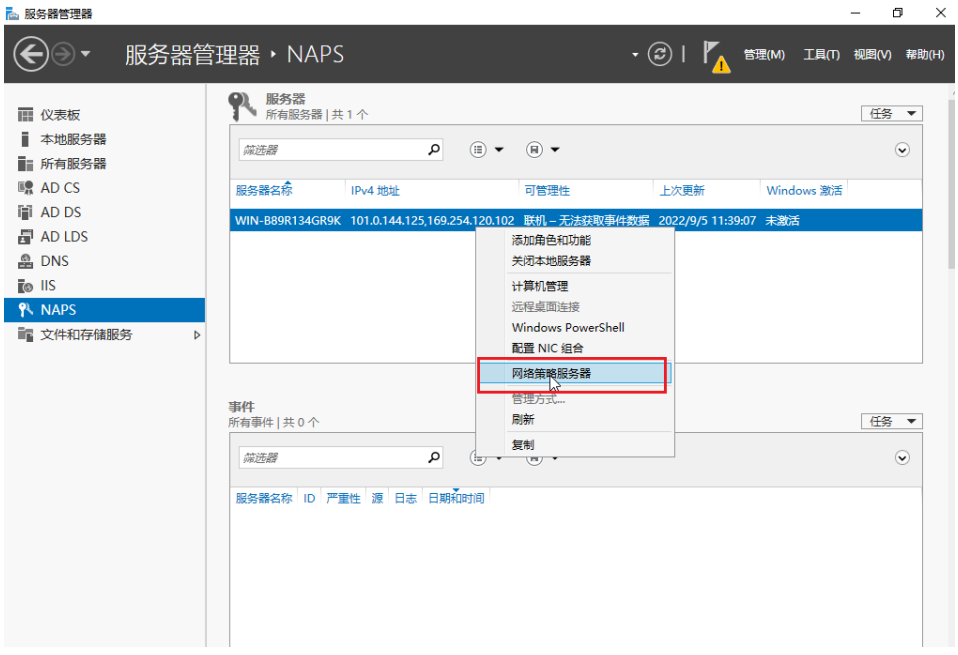
在“服务器管理器-仪表板”界面，点击右上角的“管理”菜单，并选择“添加角色和功能”，在弹窗页面左侧选择“服务器角色”，勾选“网络策略和访问服务”。后续一直点击<下一步>，直至“确认”页签时，勾选“如果需要，自动重新启动目标服务器”，点击<确认>，等待安装成功。

图5-35 选择服务器角色

e. 配置 NPS

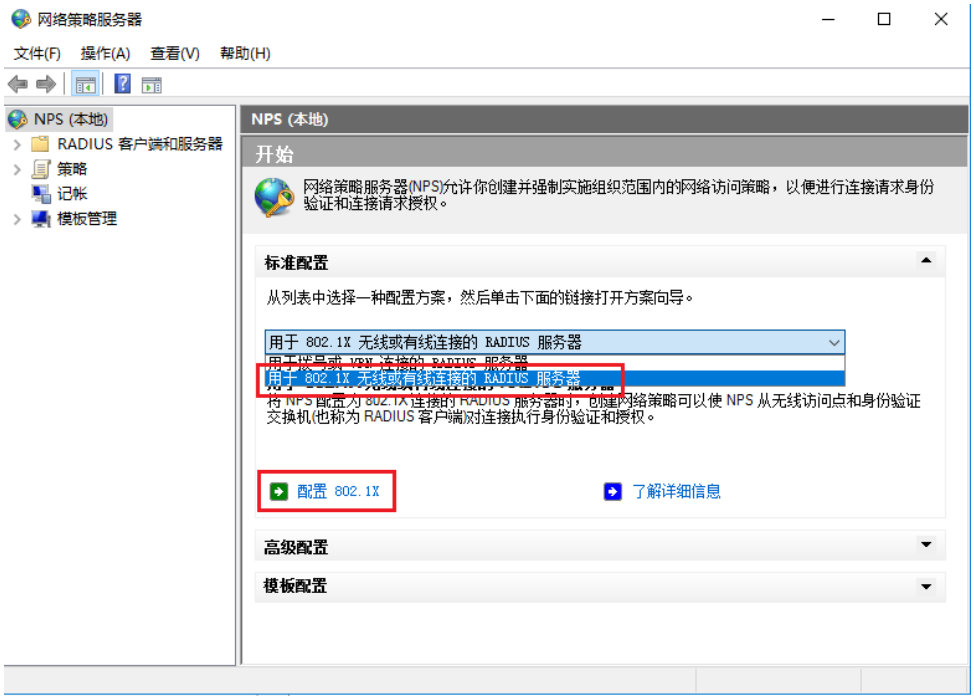
在“服务器管理器-NAPS”界面，选中服务器，右键选择“网络策略服务器”。

图5-36 打开网络策略服务器



在弹窗页面右侧“标准配置”列表中，选择“用于 802.1X 无线或有线连接的 RADIUS 服务器”，点击“配置 802.1x”。

图5-37 创建 802.1x 有线连接



在“配置 802.1X”页面，输入连接名称，点击<下一步>。

图5-38 配置 802.1X 连接名称

点击右侧<添加>。

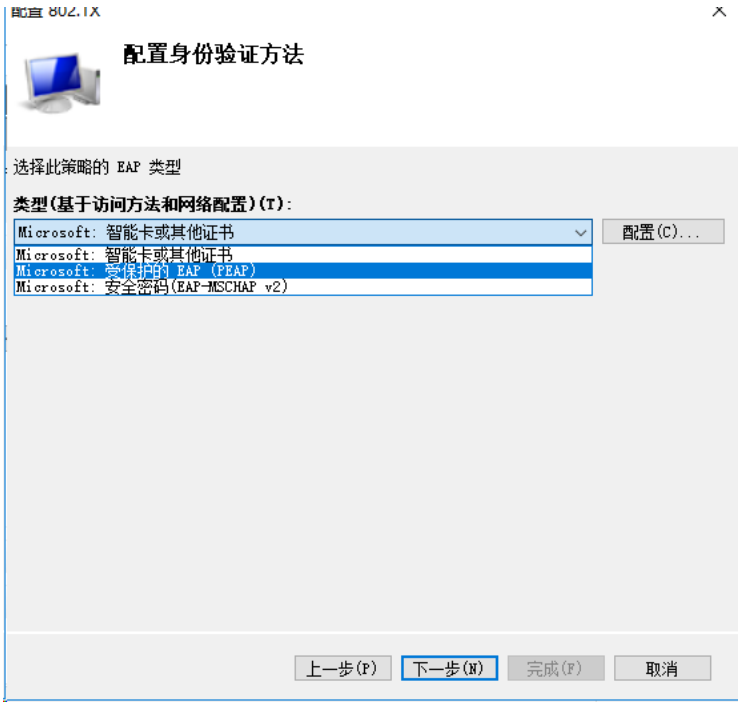
图5-39 选择 radius 客户端

在弹窗页面中输入“名称和地址”、“共享机密”等信息，点击<确定>，完成 RADIUS 客户端的新建。

图5-40 配置 RADIUS 客户端

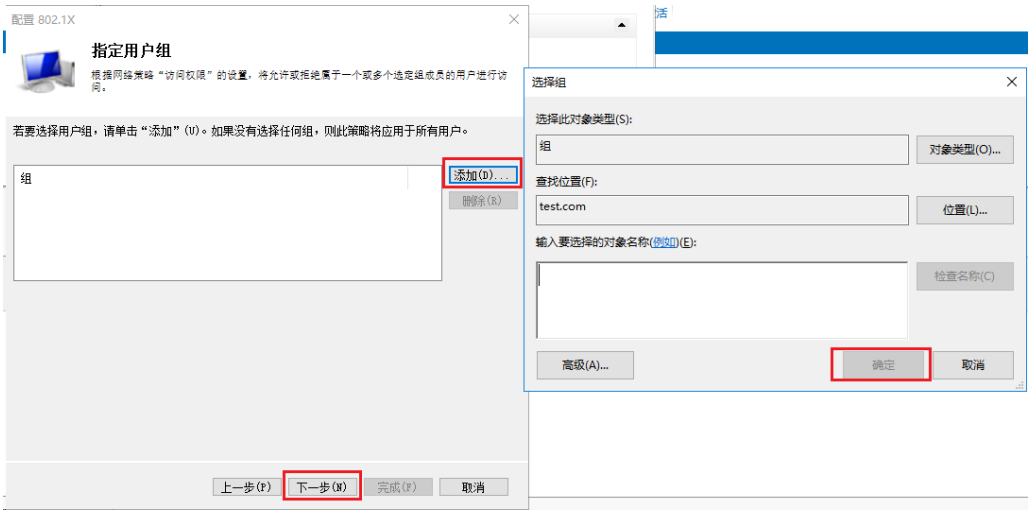
点击<下一步>，选择“Microsoft：受保护的 EAP（PEAP）”策略，完成身份验证方法的配置。

图5-41 配置身份验证方法



点击<下一步>，点击右侧的<添加>，在弹窗页面中选择组并点击<确定>，即完成指定用户组。之后一直点击<下一步>完成配置。

图5-42 指定用户组



f. 注册 AD 服务器

在“网络策略服务器”页面中，选中“NPS（本地）”，右键选择“在 Active Directory 中注册服务器”，完成 AD 服务器的的注册。

图5-43 注册服务器

5.5.3 验证配置

(1) 在设备和服务器都配置好的情况下，在 PC 使用有线网卡登录

(2) 用户上线后服务器显示如图 5-44。

图5-44 用户上线后服务器显示

SubjectUserSid S-1-5-21-3522783572-2637291755-2670974682-1105
SubjectUserName user
SubjectDomainName TEST8
FullyQualifiedSubjectUserName TEST8\user
SubjectMachineSID S-1-0-0
SubjectMachineName -
FullyQualifiedSubjectMachineName -
CalledStationID 00-E0-24-50-40-2B
CallingStationID A0-36-9F-8B-63-4C
NASIPv4Address 101.0.165.11
NASIPv6Address -
NASIdentifier tolly
NASPortType 以太网
NASPort 16785508
ClientName tolly
ClientIPAddress 101.0.165.11
ProxyPolicyName 安全有线(以太网)连接
NetworkPolicyName 安全有线(以太网)连接
AuthenticationProvider Windows
AuthenticationServer WIN-NT2QI8KLNCM.test.com
AuthenticationType PEAP
EAPType Microsoft: 安全密码(EAP-MSCHAP v2)
AccountSessionIdentifier 3030303030303034303130373230323433313030303030313837303830303030303039393 3
LoggingResult 将记帐信息写入本地日志文件。

(3) 用户上线后，在设备上通过 **display dot1x connection** 可以查看 802.1X 用户的信息，可其中 Username 为 802.1X 的用户名（本例为 user）。

```
<Switch> display  dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: a036-9f8b-634c
Access interface: GigabitEthernet1/0/2
Username: user
User access state: Successful
Authentication domain: eap
EAP packet identifier: 11
Authentication method: EAP
AAA authentication method: RADIUS
Initial VLAN: 165
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Authorization IPv6 URL: N/A
Authorization temporary redirect: Disabled
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: N/A
Online from: 2013/01/07 20:24:31
Online duration: 0h 0m 14s
```

5.5.4 配置文件

```
#
 dot1x
dot1x authentication-method peap
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 1 100 165 untagged
 port hybrid pvid vlan 165
undo dot1x handshake
 dot1x mandatory-domain domain1
 undo dot1x multicast-trigger
 dot1x port-method portbased
#
```

```
domain domain1
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 accounting lan-access radius-scheme radius1
#
radius scheme radius1
 primary authentication 101.0.144.123
 primary accounting 101.0.144.123
 key authentication cipher $c$3$9jjl0lp5VA/WXEw065ZIT7j4AIN88XTF
 key accounting cipher $c$3$fk1zm9nf2IFMdk+I7hGsyBcsAwqLobi7
 user-name-format without-domain
#
```

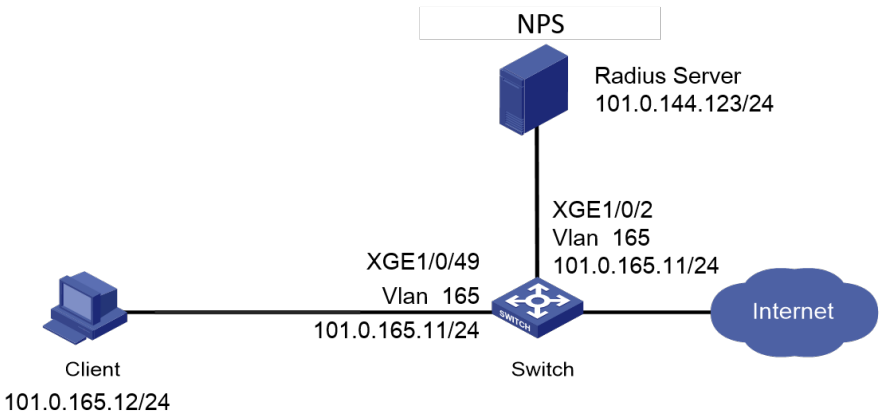
6 Portal 认证对接配置举例——本地 portal+LDAP 认证

6.1 组网需求

如图 6-1 所示，Client 和 Windows Server 2016-NPS 服务器通过 Switch 建立连接，设备管理员希望对 Client 进行 Portal 认证，以控制其对网络资源的访问，具体要求如下：

- 采用 Windows Server 2016-NPS 作为 LDAP 服务器。
- 用户采用直接方式的 Portal 认证。

图6-1 Portal 认证配置组网图



6.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch： S5560X-54C-PWR-EI，Version 7.1.070
- 认证服务器：Windows Server 2016-NPS

6.3 配置步骤

说明

本配置仅展示认证的相关配置，网络互通的相关配置略，请保证设备间能够互相访问。

6.3.1 配置 Switch

进入本地 Portal Web 服务视图，并指定使用 HTTPS 协议和客户端交互认证信息。

```
<Switch> system-view
[Switch] portal local-web-server http tcp-port 2331
[Switch-portal-local-websvr-http] quit
```

配置 Portal Web 服务器的 URL 地址。

```
[Switch] portal web-server newpt
[Switch-portal-websvr-newpt] url http://101.0.165.11:2331/portal
[Switch-portal-websvr-newpt] quit
```

配置 LDAP 服务器 ccc。

```
[Switch] ldap server ccc
[Switch-ldap-server-ccc] login-dn cn=administrator,cn=users,dc=test,dc=com
[Switch-ldap-server-ccc] search-base-dn dc=test,dc=com
[Switch-ldap-server-ccc] ip 101.0.144.124
[Switch-ldap-server-ccc] login-password cipher 123456
[Switch-ldap-server-ccc] quit
```

创建 LDAP 方案 ldap1。

```
[Switch] ldap scheme ldap1
[Switch-ldap-ldap1] authentication-server ccc
[Switch-ldap-ldap1] quit
```

配置互通的 VLAN 和 VLAN 接口的 IP 地址。

```
[Switch] vlan 165
[Switch-vlan165] quit
[Switch] interface Vlan-interface 165
[Switch-Vlan-interface165] ip address 101.0.165.11 255.255.255.0
[Switch-Vlan-interface165] portal apply web-server newpt
[Switch-Vlan-interface165] quit
```

将端口 XGE1/0/47 和 GE1/0/2 加入到指定的 VLAN。

```
[Switch] interface Ten-GigabitEthernet 1/0/47
[Switch-Ten-GigabitEthernet1/0/47] port access vlan 165
[Switch-Ten-GigabitEthernet1/0/47] quit
[Switch] interface Ten-GigabitEthernet 1/0/2
[Switch-Ten-GigabitEthernet1/0/2] port access vlan 165
[Switch-Ten-GigabitEthernet1/0/2] quit
```

配置 domain1 域。

```
[switch] domain domain1
[switch-isp-domain1] authentication portal ldap-scheme ldap1
```

```
[switch-isp-domain1] authentication portal none
[switch-isp-domain1] accounting portal none
[switch-isp-domain1] quit
```

配置 domain1 为缺省的 ISP 域。

```
[Switch] domain default enable domain1
```

配置 Portal 直接认证。

```
[Switch] interface Vlan-interface 165
[Switch-Vlan-interface165] portal enable method direct
[Switch-Vlan-interface165] quit
```

说明

用户可以采用直接认证或者可跨三层 Portal 认证方式上线，后者只需要修改设备上的 **portal enable method direct** 配置为 **portal enable method layer3** 即可，服务器和客户端无需改动。

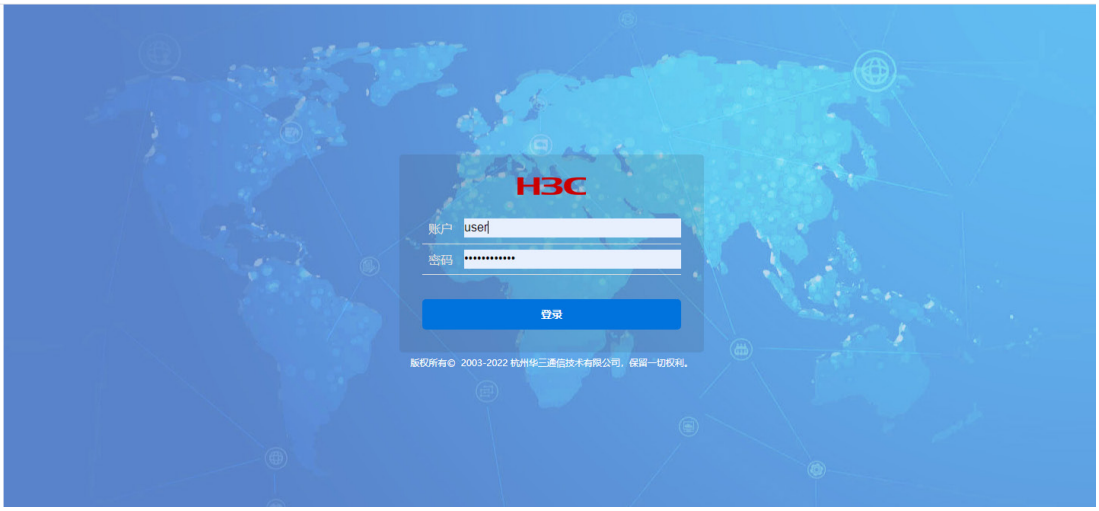
6.3.2 配置 Windows Server 2016-NPS

服务器上的配置请参考 5.5.2 配置 Windows Server 2016-NPS。

6.4 验证配置

(1) 用户在浏览器上输入本地认证 IP 地址，回车后会跳转到登录页面，请根据图 6-2 所示，输入账户名和密码。

图6-2 Web 登录页面



页面显示登录成功。

图6-3 登录成功

(2) 用户上线后服务器显示如图 6-4。

图6-4 用户上线后服务器显示

(3) 用户上线后，在设备上通过 **display portal user** 命令可以查看上线 Portal 用户的信息。其中 Username 字段显示为 Portal 用户的用户名 user。

```
<Switch> display  portal user all
Total portal users: 1
Username: user
```

```
Portal server:
State: Online
VPN instance: N/A
MAC             IP                   VLAN    Interface
a036-9f8b-634c  101.0.165.12         165     Vlan-interface165
Authorization information:
  DHCP IP pool: N/A
  User profile: N/A
  Session group profile: N/A
  ACL number: N/A
  Inbound CAR: N/A
  Outbound CAR: N/A
```

6.5 配置文件

```
#
interface Vlan-interface165
 ip address 101.0.165.11 255.255.255.0
 portal enable method direct
 portal apply web-server newpt
#
domain ldap
 authentication portal ldap-scheme ldap
 authorization portal none
 accounting portal none
#
ldap scheme ldap
 authentication-server ldap
#
ldap server ldap
 login-dn cn=administrator,cn=users,dc=test,dc=com
 search-base-dn dc=test,dc=com
 ip 101.0.144.124
 login-password cipher $c$3$MU1UdAnLgSFni5hERPL15CYR7NsHW6RkErhr3bQuNA==
#
portal web-server newpt
 url http://101.0.165.11:2331/portal
#
portal local-web-server http
 default-logon-page en.zip
 tcp-port 2331
#
```

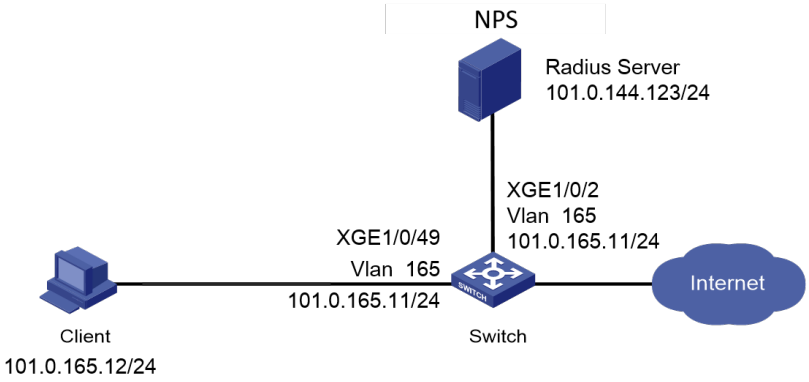
7 授权 VLAN 对接配置举例

7.1 组网需求

如图 7-1 所示，Client 和 Windows Server 2016-NPS 服务器通过 Switch 建立连接，设备管理员希望对 Client 进行 802.1X 认证或者 MAC 地址认证，以控制其对网络资源的访问，具体要求如下：

- 采用 Windows Server 2016-NPS 作为 RADIUS 服务器。
- 通过 Windows Server 2016-NPS 授权下发 VLAN，初始 VLAN 为 144。

图7-1 授权 VLAN 组网图



7.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch： S5560X-54C-PWR-EI，Version 7.1.070
- 认证服务器：Windows Server 2016-NPS

7.3 授权数字型VLAN配置步骤与验证

7.3.1 配置 Switch

- 若采用 MAC 地址认证，Swtich 上的配置请参考 4.3.1 配置 Switch。
- 若采用 802.1X 认证，Swtich 上的配置请参考 5.3.1 配置 Switch。

7.3.2 配置 Windows Server 2016-NPS

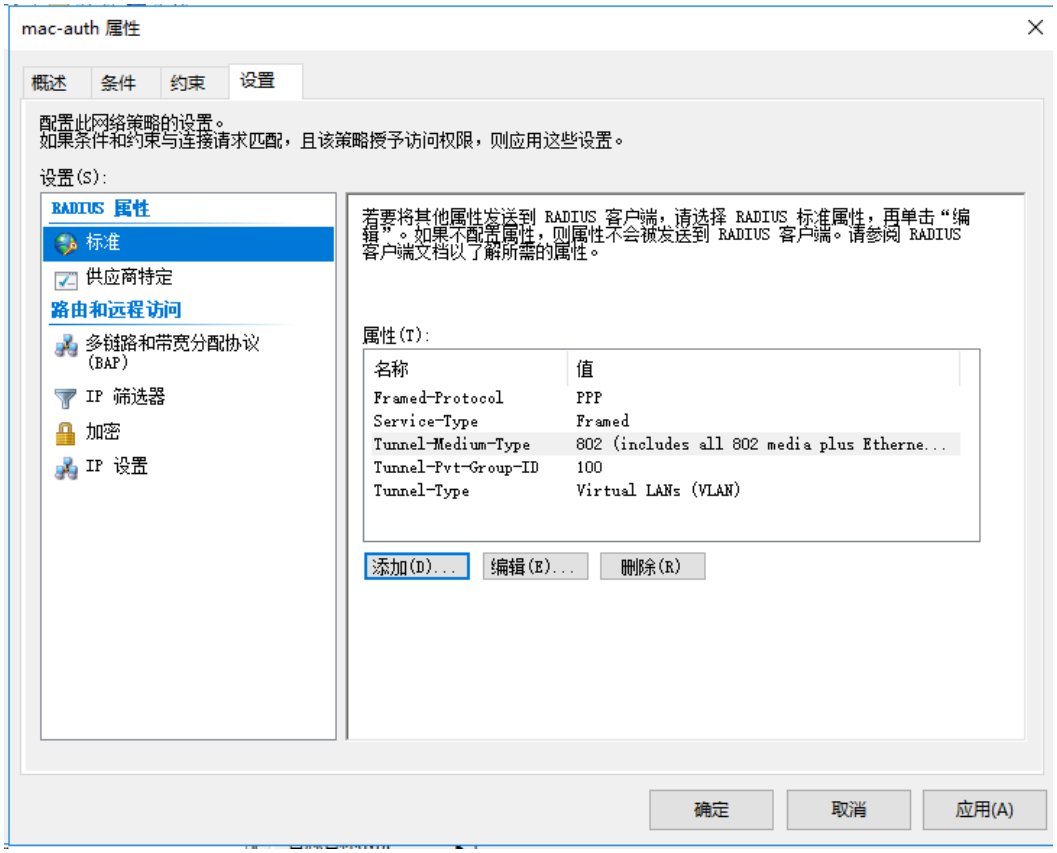
(1) 服务器上的通用配置。

- 若采用 MAC 地址认证，服务器上的配置请参考 4.3.2 配置 Windows Server 2016-NPS。
- 若采用 802.1X 认证，服务器上的配置请参考 5.3.2 配置 Windows Server 2016-NPS。

(2) 只需将“配置文件”的“属性”参考图 7-2 修改即可。

- Tunnel-Medium-Type：创建隧道的传输层媒介类型，该属性值为 6 时表示 802 类型，可用于下发 VLAN。
- Tunnel-Private-Group-ID：隧道会话的组 ID，该属性在下发 VLAN 时用于携带下发的 VLAN ID（本例下发的 VLAN ID 为 100）。
- Tunnel-Type：使用的隧道协议，该属性值为 13 时表示下发 VLAN。

图7-2 配置文件



7.3.3 验证配置

(1) 用户上线后服务器显示如图 7-3。

图7-3 用户上线后服务器显示

(2) 以 802.1X 认证为例，用户上线后，在设备上通过 **display dot1x connection** 命令可以查看上线 802.1X 用户的信息。其中 Authorization untagged VLAN 字段显示成功下发授权 VLAN100。

```
<Switch> display  dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: a036-9f8b-634c
Access interface: GigabitEthernet1/0/2
Username: user
User access state: Successful
Authentication domain: domain1
EAP packet identifier: 2
Authentication method: CHAP
AAA authentication method: RADIUS
Initial VLAN: 165
Authorization untagged VLAN: 100
Authorization tagged VLAN list: N/A
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Authorization IPv6 URL: N/A
Authorization temporary redirect: Disabled
```

```
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: N/A
Online from: 2013/01/08 06:52:03
Online duration: 0h 0m 14s
```

以 MAC 地址认证为例，用户上线后，在设备上通过 **display mac-authentication connection** 命令可以查看上线 MAC 地址认证用户的信息。其中 Authorization untagged VLAN 字段显示成功下发授权 VLAN 100。

```
[[Switch]display  mac-authentication  connection
Total connections: 1
Slot ID: 1
User MAC address: 0010-9400-0005
Access interface: GigabitEthernet1/0/2
Username: 001094000005
User access state: Successful
Authentication domain: domain1
IPv4 address: 192.85.1.2
IPv4 address source: User packet
Initial VLAN: 165
Authorization untagged VLAN: 100
Authorization tagged VLAN: N/A
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Authorization IPv6 URL: N/A
Authorization temporary redirect: Disabled
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: N/A
Offline detection: 300 sec (command-configured)
Online from: 2013/01/08 06:25:15
Online duration: 0h 0m 8s
Port-down keep online: Disabled (offline)
```

7.3.4 配置文件

```
#
 dot1x
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type hybrid
```

```
 port hybrid vlan 1 100 165 untagged
 port hybrid pvid vlan 165
undo dot1x handshake
 dot1x mandatory-domain domain1
 undo dot1x multicast-trigger
 dot1x port-method portbased
#
domain domain1
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 accounting lan-access radius-scheme radius1
#
radius scheme radius1
 primary authentication 101.0.144.123
 primary accounting 101.0.144.123
 key authentication cipher $c$3$9jjl0lp5VA/WXEw065ZIT7j4AIN88XTF
 key accounting cipher $c$3$fk1zm9nf2IFMdk+I7hGsyBcsAwqLobi7
 user-name-format without-domain
#
```

7.4 授权VLAN名称配置步骤与验证

7.4.1 配置 Switch

(1) Swtich 上的配置。

- 若采用 MAC 地址认证，Swtich 上的配置请参考 4.3.1 配置 Switch。
- 若采用 802.1X 认证用户，Swtich 上的配置请参考 5.3.1 配置 Switch。

(2) 授权 VLAN 名称时，该 VLAN 必须在设备上已经创建，并且设置了 VLAN 名称。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] name tolly
```

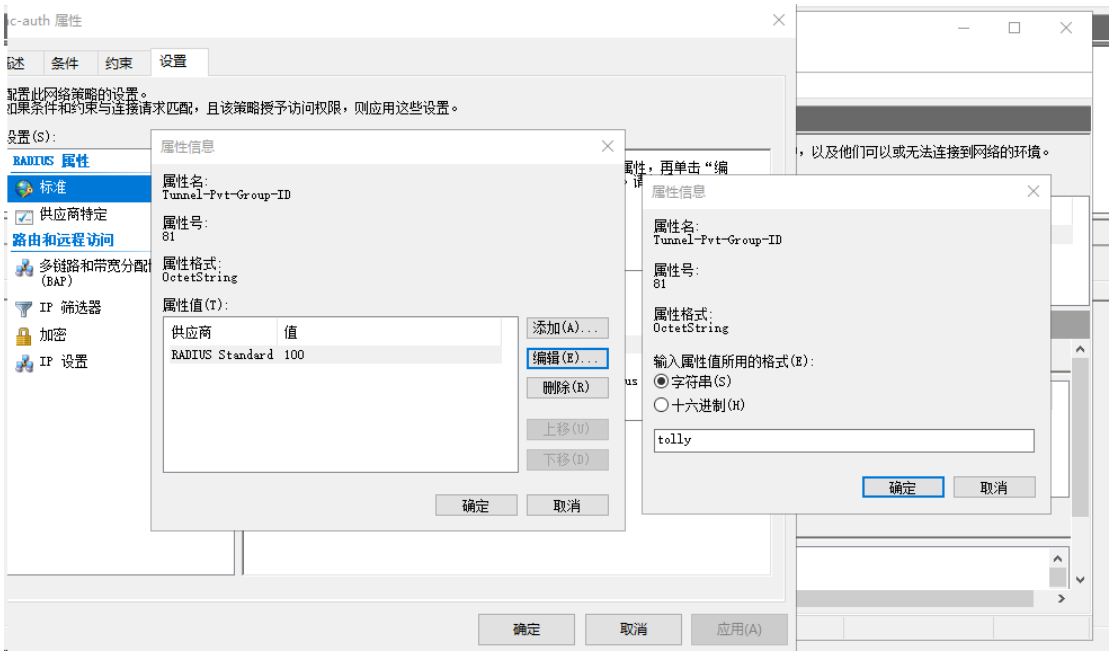
7.4.2 配置 Windows Server 2016-NPS

(1) 服务器上的通用配置。

- 若采用 MAC 地址认证，服务器上的配置请参考 4.3.2 配置 Windows Server 2016-NPS。
- 若采用 802.1X 认证，服务器上的配置请参考 5.3.2 配置 Windows Server 2016-NPS。

(2) 只需将“网络策略”的“属性”参考图 7-4 修改即可。

图7-4 配置文件



7.4.3 验证配置

(1) 用户上线后服务器显示如图 7-5。

图7-5 用户上线后服务器显示

(2) 以 802.1X 认证为例，用户上线后，在设备上通过 **display dot1x connection** 命令可以查看上线 802.1X 用户的信息。其中 Authorization untagged VLAN 字段显示成功下发授权 VLAN100（该 VLAN 名称为 tolly）。

```
[Switch]display  dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: a036-9f8b-634c
Access interface: GigabitEthernet1/0/2
Username: user
User access state: Successful
Authentication domain: domain1
EAP packet identifier: 2
Authentication method: CHAP
AAA authentication method: RADIUS
Initial VLAN: 165
Authorization untagged VLAN: 100
Authorization tagged VLAN list: N/A
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Authorization IPv6 URL: N/A
Authorization temporary redirect: Disabled
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: N/A
Online from: 2013/01/08 06:55:46
Online duration: 0h 0m 9s
```

(3) 以 MAC 地址认证为例，用户上线后，在设备上通过 **display mac-authentication connection** 命令可以查看上线 MAC 地址认证用户的信息。其中 Authorization untagged VLAN 字段显示成功下发授权 VLAN100（该 VLAN 名称为 tolly）。

```
[Switch]display  mac-authentication connection
Total connections: 1
Slot ID: 1
User MAC address: 0010-9400-0005
Access interface: GigabitEthernet1/0/2
Username: 001094000005
User access state: Successful
Authentication domain: domain1
IPv4 address: 192.85.1.2
IPv4 address source: User packet
Initial VLAN: 165
Authorization untagged VLAN: 100
```

```
Authorization tagged VLAN: N/A
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Authorization IPv6 URL: N/A
Authorization temporary redirect: Disabled
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: N/A
Offline detection: 300 sec (command-configured)
Online from: 2013/01/08 06:57:21
Online duration: 0h 0m 9s
Port-down keep online: Disabled (offline)
```

7.4.4 配置文件

```
#
 dot1x
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 1 100 165 untagged
 port hybrid pvid vlan 165
 undo dot1x handshake
 dot1x mandatory-domain domain1
 undo dot1x multicast-trigger
 dot1x port-method portbased
#
domain domain1
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 accounting lan-access radius-scheme radius1
#
radius scheme radius1
 primary authentication 101.0.144.123
 primary accounting 101.0.144.123
 key authentication cipher $c$3$9jjl0lp5VA/WXEw065ZIT7j4AIN88XTF
 key accounting cipher $c$3$fk1zm9nf2IFMdk+I7hGsyBcsAwqLobi7
 user-name-format without-domain
#
```

7.5 授权VLAN组名配置步骤与验证

7.5.1 配置 Switch

(1) Swtich 上的配置

- 若采用 MAC 地址认证，Swtich 上的配置请参考 4.3.1 配置 Switch。
- 若采用 802.1X 认证，Swtich 上的配置请参考 5.3.1 配置 Switch。

(2) 下发的 VLAN 组必须在设备上已经创建，会将该组 VLAN 组中 ID 最小的 VLAN 授权给当前的认证用户，且后续该端口上的认证用户均被加入该授权 VLAN。

```
<Switch> system-view
[Switch] vlan-group temp
[Switch-vlan-group-temp] vlan-list 100 200 300
```

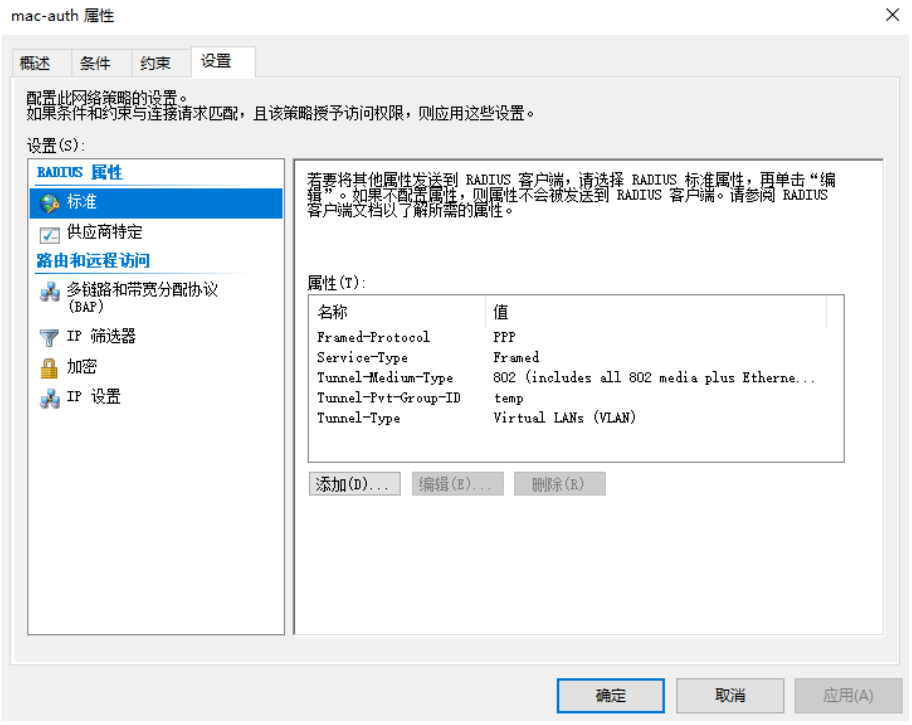
7.5.2 配置 Windows Server 2016-NPS

(1) 服务器上的通用配置。

- 若采用 MAC 地址认证，服务器上的配置请参考 4.3.2 配置 Windows Server 2016-NPS。
- 若采用 802.1X 认证，服务器上的配置请参考 5.3.2 配置 Windows Server 2016-NPS。

(2) 只需将“网络策略”的“属性”参考图 7-6 修改即可。

图7-6 配置文件



7.5.3 验证配置

(1) 用户上线后服务器显示如图 7-7。

图7-7 用户上线后服务器显示

(2) 以 802.1X 认证为例，用户上线后，在设备上通过 **display dot1x connection** 命令可以查看上线 802.1X 用户的信息。其中 Authorization untagged VLAN 字段显示成功下发授权 VLAN 100。

```
<Switch> display  dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: a036-9f8b-634c
Access interface: GigabitEthernet1/0/2
Username: user
User access state: Successful
Authentication domain: domain1
EAP packet identifier: 2
Authentication method: CHAP
AAA authentication method: RADIUS
Initial VLAN: 165
Authorization untagged VLAN: 100
Authorization tagged VLAN list: N/A
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Authorization IPv6 URL: N/A
Authorization temporary redirect: Disabled
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: N/A
Online from: 2013/01/08 07:03:17
Online duration: 0h 0m 12s
```

以 MAC 地址认证为例，用户上线后，在设备上通过 **display mac-authentication connection** 命令可以查看上线 MAC 地址认证用户的信息。其中 Authorization untagged VLAN 字段显示成功下发授权 VLAN 100。

```
<Switch> display  mac-authentication  connection
Total connections: 1
Slot ID: 1
User MAC address: 0010-9400-0005
Access interface: GigabitEthernet1/0/2
Username: 001094000005
User access state: Successful
Authentication domain: domain1
IPv4 address: 192.85.1.2
IPv4 address source: User packet
Initial VLAN: 165
Authorization untagged VLAN: 100
Authorization tagged VLAN: N/A
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Authorization IPv6 URL: N/A
Authorization temporary redirect: Disabled
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: N/A
Offline detection: 300 sec (command-configured)
Online from: 2013/01/08 06:57:21
Online duration: 0h 10m 12s
Port-down keep online: Disabled (offline)
```

7.5.4 配置文件

```
#
 dot1x
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 1 100 165 untagged
 port hybrid pvid vlan 165
undo dot1x handshake
 dot1x mandatory-domain domain1
 undo dot1x multicast-trigger
 dot1x port-method portbased
```

```
#
domain domain1
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 accounting lan-access radius-scheme radius1
#
radius scheme radius1
 primary authentication 101.0.144.123
 primary accounting 101.0.144.123
 key authentication cipher $c$3$9jjl0lp5VA/WXEw065ZIT7j4AIN88XTF
 key accounting cipher $c$3$fk1zm9nf2IFMdk+I7hGsyBcsAwqLobi7
 user-name-format without-domain
#
```

7.6 授权Multi VLAN配置步骤与验证

7.6.1 配置 Switch

(1) Swtich 上的配置。

- 若采用 MAC 地址认证，Swtich 上的配置请参考 4.3.1 配置 Switch。
- 若采用 802.1X 认证，Swtich 上的配置请参考 5.3.1 配置 Switch。

(2) 服务器授权多个 VLAN 名称时，所有 VLAN 必须在设备上均已经创建，并且均设置了 VLAN 名称。

```
[Switch] vlan 100
[Switch-vlan100] name tolly1
[Switch-vlan100] quit
[Switch] vlan 200
[Switch-vlan200] name tolly2
[Switch-vlan200] quit
```

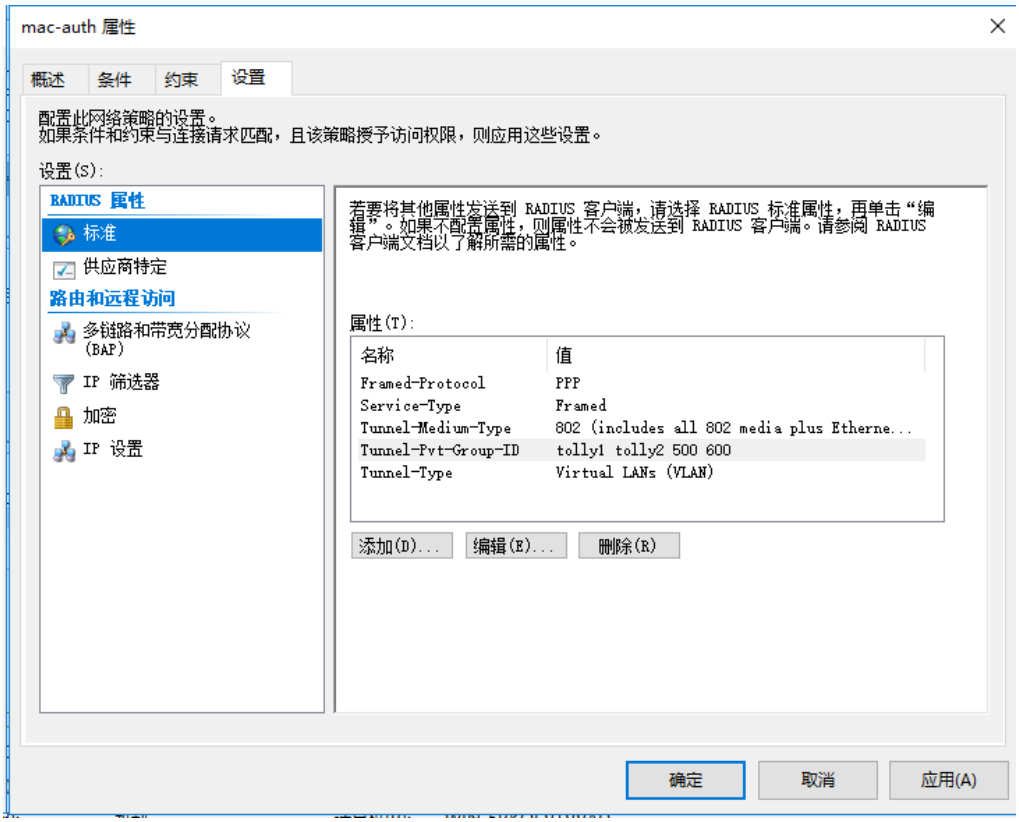
7.6.2 配置 Windows Server 2016-NPS

(1) 服务器上的配置。

- 若采用 MAC 地址认证，服务器上的配置请参考 4.3.2 配置 Windows Server 2016-NPS。
- 若采用 802.1X 认证，服务器上的配置请参考 5.3.2 配置 Windows Server 2016-NPS。

(2) 只需将“网络策略”的“属性”参考图 7-8 修改即可。

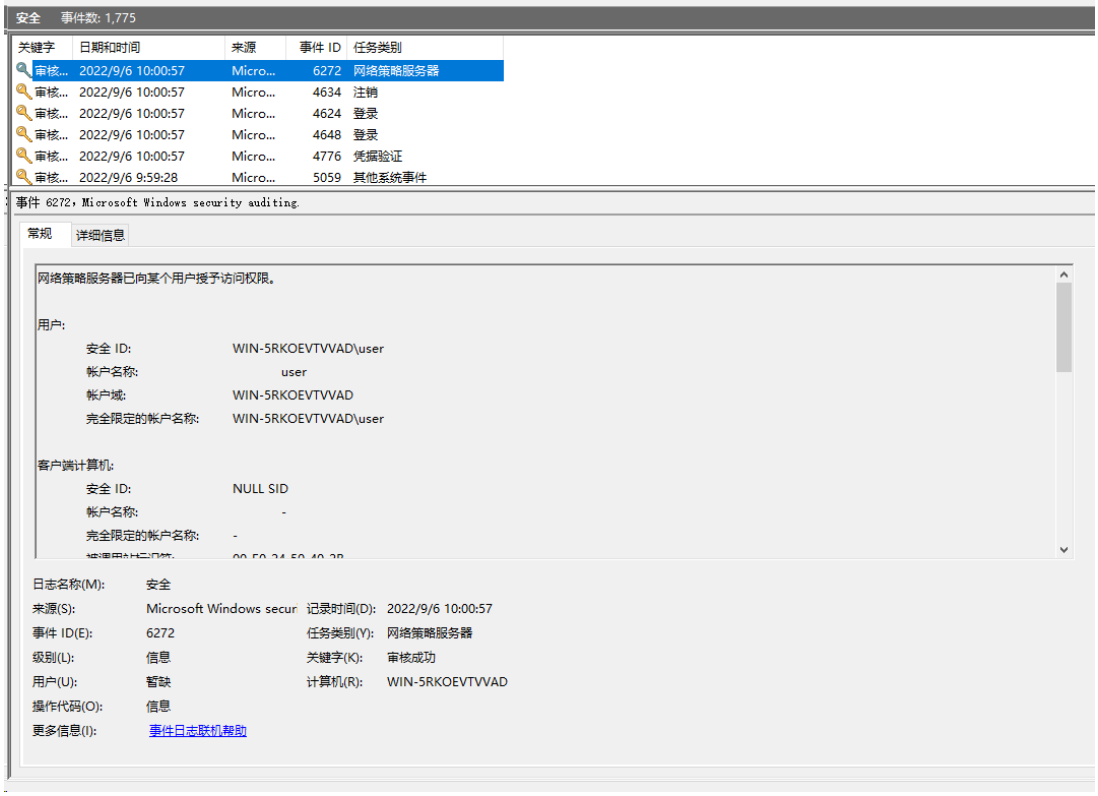
图7-8 配置文件



7.6.3 验证配置

(1) 用户上线后服务器显示如图 7-9。

图7-9 用户上线后服务器显示



(2) 以 802.1X 认证为例，用户上线后，在设备上通过 **display dot1x connection** 命令可以查看上线 802.1X 用户的信息。其中 Authorization untagged VLAN 字段显示成功下发授权 VLAN 100。

说明

若认证服务器下发的授权 VLAN 信息为一个包含若干 VLAN 编号以及若干 VLAN 名称的字符串，则设备首先将其解析为一组 VLAN ID，然后采用与解析一个 VLAN 组名相同的解析逻辑选择一个授权 VLAN。通常是按 VLAN ID 最小选择。

```
<Switch> display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: a036-9f8b-634c
Access interface: GigabitEthernet1/0/2
Username: user
User access state: Successful
Authentication domain: domain1
EAP packet identifier: 2
Authentication method: CHAP
AAA authentication method: RADIUS
Initial VLAN: 165
Authorization untagged VLAN: 100
```

```
     Authorization tagged VLAN list: N/A
     Authorization VSI: N/A
     Authorization microsegment ID: N/A
     Authorization ACL number/name: N/A
     Authorization dynamic ACL name: N/A
     Authorization user profile: N/A
     Authorization CAR: N/A
     Authorization URL: N/A
     Authorization IPv6 URL: N/A
     Authorization temporary redirect: Disabled
     Start accounting: Successful
     Real-time accounting-update failures: 0
     Termination action: Default
     Session timeout period: N/A
     Online from: 2013/01/08 21:33:14
     Online duration: 0h 0m 12s
```

7.6.4 配置文件

```
#
 dot1x
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 1 100 165 untagged
 port hybrid pvid vlan 165
undo dot1x handshake
 dot1x mandatory-domain domain1
 undo dot1x multicast-trigger
 dot1x port-method portbased
#
domain domain1
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 accounting lan-access radius-scheme radius1
#
radius scheme radius1
 primary authentication 101.0.144.123
 primary accounting 101.0.144.123
 key authentication cipher $c$3$9jjl0lp5VA/WXEw065ZIT7j4AIN88XTF
 key accounting cipher $c$3$fk1zm9nf2IFMdk+I7hGsyBcsAwqLobi7
 user-name-format without-domain
#
```

7.7 授权Auto VLAN规则1配置步骤与验证

说明

Auto VLAN 规则下，服务器下发的授权 VLAN 仅对端口链路类型为 Hybrid 或 Trunk，且 802.1X 接入控制方式为 Port-based 的端口有效。若端口链路类型为 access，则用户上线失败。

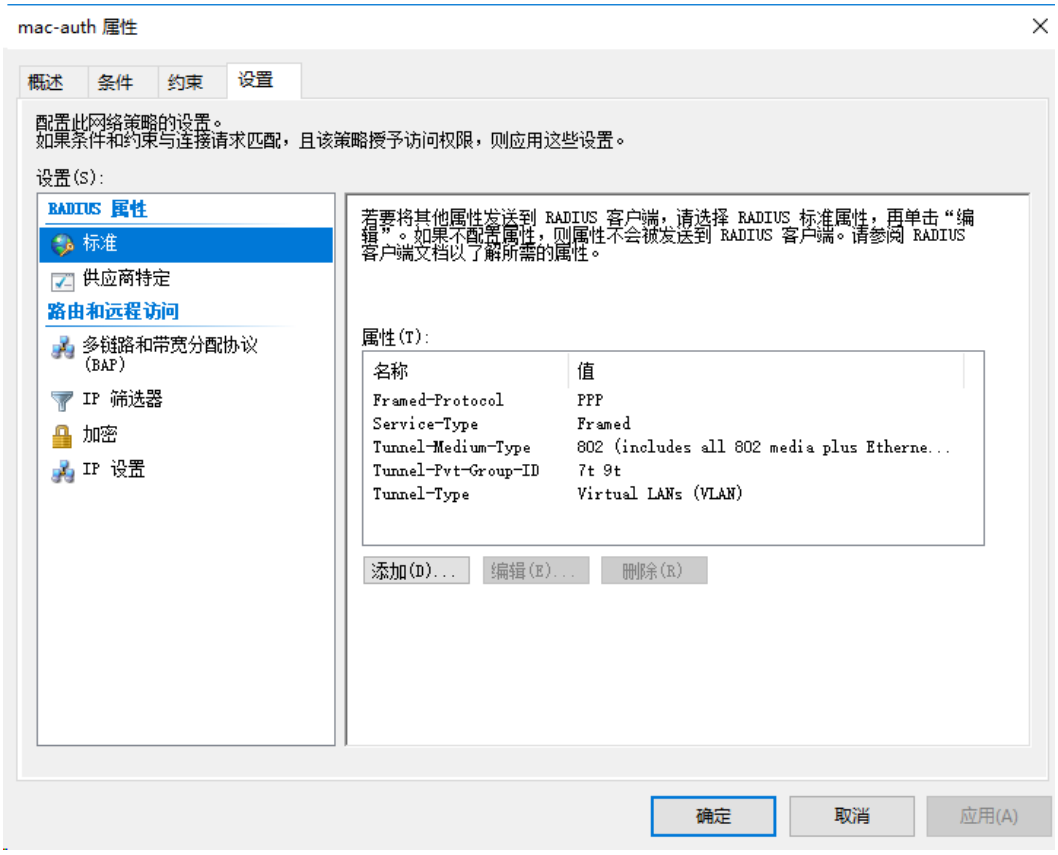
7.7.1 配置 Switch

Swtich 上的配置请参考 5.3.1 配置 Switch。

7.7.2 配置 Windows Server 2016-NPS

服务器上的配置请参考 5.3.2 配置 Windows Server 2016-NPS。只需将“网络策略”的“属性”参考图 7-10 修改即可。

图7-10 配置文件



7.7.3 验证配置

用户使用 802.1X 认证方式上线。

(1) 用户上线后服务器显示如图 7-11。

图7-11 用户上线后服务器显示

(2) 用户上线后，在设备上通过 **display dot1x connection** 命令可以查看上线 802.1X 用户的信息。其中 Authorization tagged VLAN 字段显示成功下发授权 VLAN 7 和 VLAN 9。不存在 untagged 的授权 VLAN，则不修改端口的缺省 VLAN。

```
<Switch> display  dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: a036-9f8b-634c
Access interface: GigabitEthernet1/0/2
Username: user
User access state: Successful
Authentication domain: domain1
EAP packet identifier: 2
Authentication method: CHAP
AAA authentication method: RADIUS
Initial VLAN: 165
Authorization untagged VLAN: 100
Authorization tagged VLAN list: 7 9
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
```

```
    Authorization user profile: N/A
    Authorization CAR: N/A
    Authorization URL: N/A
    Authorization IPv6 URL: N/A
    Authorization temporary redirect: Disabled
    Start accounting: Successful
    Real-time accounting-update failures: 0
    Termination action: Default
    Session timeout period: N/A
    Online from: 2013/01/08 07:15:29
    Online duration: 0h 0m 10s
```

7.7.4 配置文件

```
#
 dot1x
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 1 100 165 untagged
 port hybrid pvid vlan 165
undo dot1x handshake
 dot1x mandatory-domain domain1
 undo dot1x multicast-trigger
 dot1x port-method portbased
#
domain domain1
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 accounting lan-access radius-scheme radius1
#
radius scheme radius1
 primary authentication 101.0.144.123
 primary accounting 101.0.144.123
 key authentication cipher $c$3$9jjl0lp5VA/WXEw065ZIT7j4AIN88XTF
 key accounting cipher $c$3$fk1zm9nf2IFMdk+I7hGsyBcsAwqLobi7
 user-name-format without-domain
#
```

7.8 授权Auto VLAN规则2配置步骤与验证

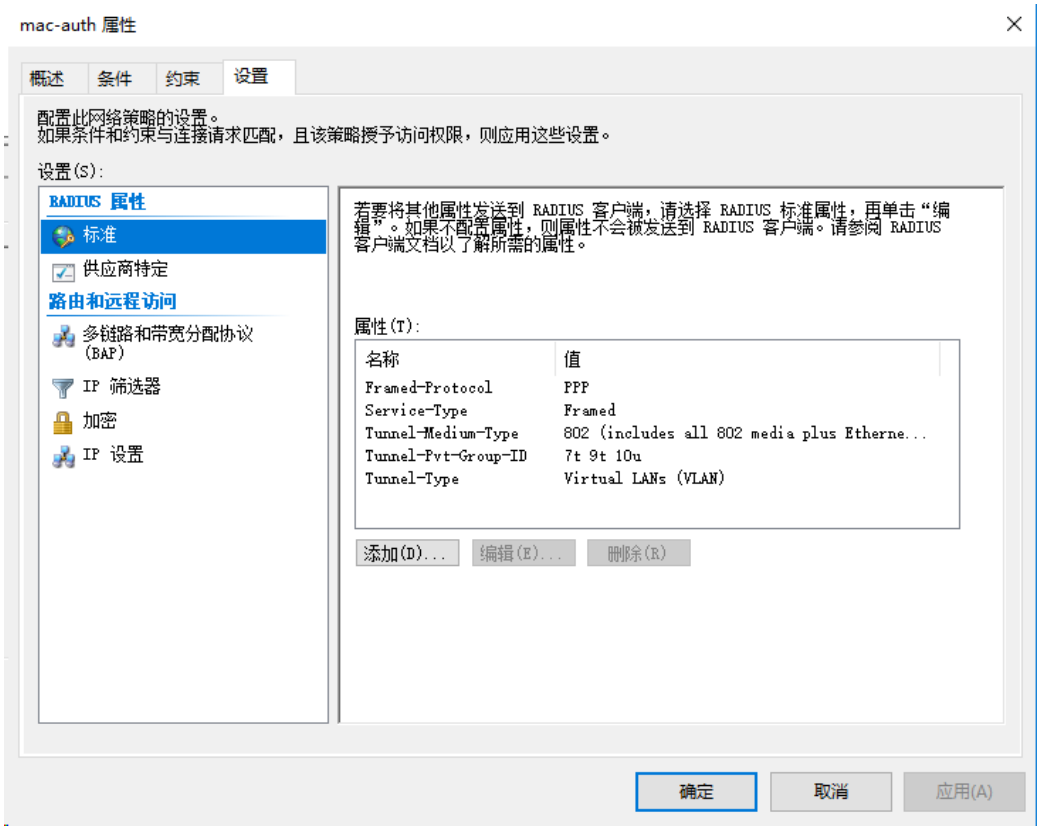
7.8.1 配置 Switch

Swtich 上的配置请参考 5.3.1 配置 Switch。

7.8.2 配置 Windows Server 2016-NPS

服务器上的配置请参考 5.3.2 配置 Windows Server 2016-NPS。只需将“网络策略”的“属性”参考图 7-12 修改即可。

图7-12 配置文件

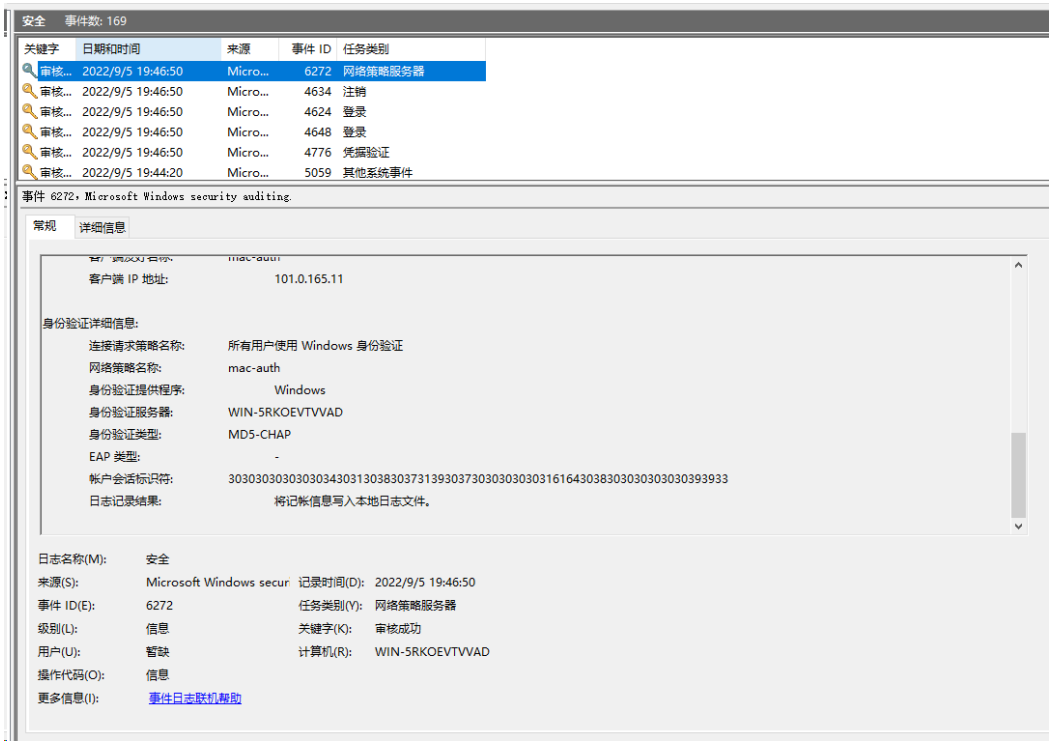


7.8.3 验证配置

用户使用 802.1X 认证方式上线。

(1) 用户上线后服务器上显示如图 7-13。

图7-13 用户上线后服务器显示



(2) 用户上线后，在设备上通过 **display dot1x connection** 命令可以查看上线 802.1X 用户的信息。其中 Authorization tagged VLAN 字段显示成功下发授权 VLAN 7 和 VLAN 9。存在 untagged 的授权 VLAN，端口的缺省 VLAN 将被修改为 untagged 的授权 VLAN。

```
<Switch> display  dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: a036-9f8b-634c
Access interface: GigabitEthernet1/0/2
Username: user
User access state: Successful
Authentication domain: domain1
EAP packet identifier: 2
Authentication method: CHAP
AAA authentication method: RADIUS
Initial VLAN: 165
Authorization untagged VLAN: 10
Authorization tagged VLAN list: 7 9
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Authorization IPv6 URL: N/A
```

```
    Authorization temporary redirect: Disabled
    Start accounting: Successful
    Real-time accounting-update failures: 0
    Termination action: Default
    Session timeout period: N/A
    Online from: 2013/01/08 07:19:07
    Online duration: 0h 0m 10s
```

7.8.4 配置文件

```
#
 dot1x
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 1 100 165 untagged
 port hybrid pvid vlan 165
undo dot1x handshake
 dot1x mandatory-domain domain1
 undo dot1x multicast-trigger
 dot1x port-method portbased
#
domain domain1
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 accounting lan-access radius-scheme radius1
#
radius scheme radius1
 primary authentication 101.0.144.123
 primary accounting 101.0.144.123
 key authentication cipher $c$3$9jjl0lp5VA/WXEw065ZIT7j4AIN88XTF
 key accounting cipher $c$3$fk1zm9nf2IFMdk+I7hGsyBcsAwqLobi7
 user-name-format without-domain
#
```

7.9 授权Auto VLAN规则3配置步骤与验证

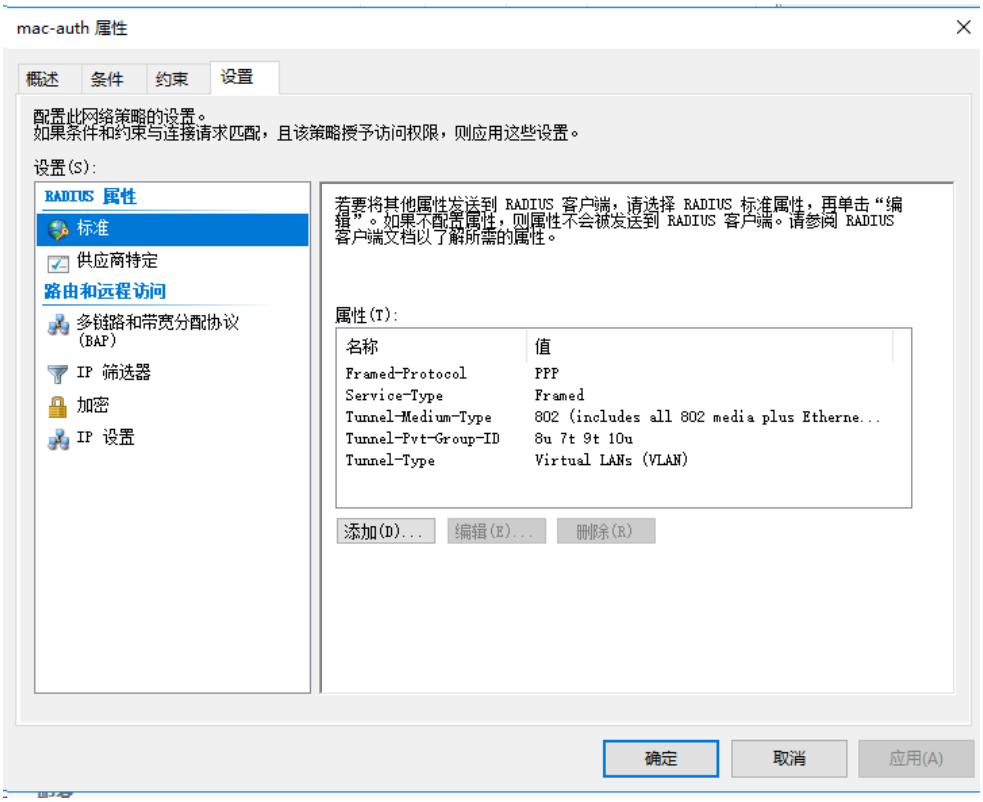
7.9.1 配置 Switch

Swtich 上的配置请参考 5.3.1 配置 Switch。

7.9.2 配置 Windows Server 2016-NPS

服务器上的配置请参考 5.3.2 配置 Windows Server 2016-NPS。只需将“配置文件”的“属性”参考图 7-14 修改即可。

图7-14 配置文件

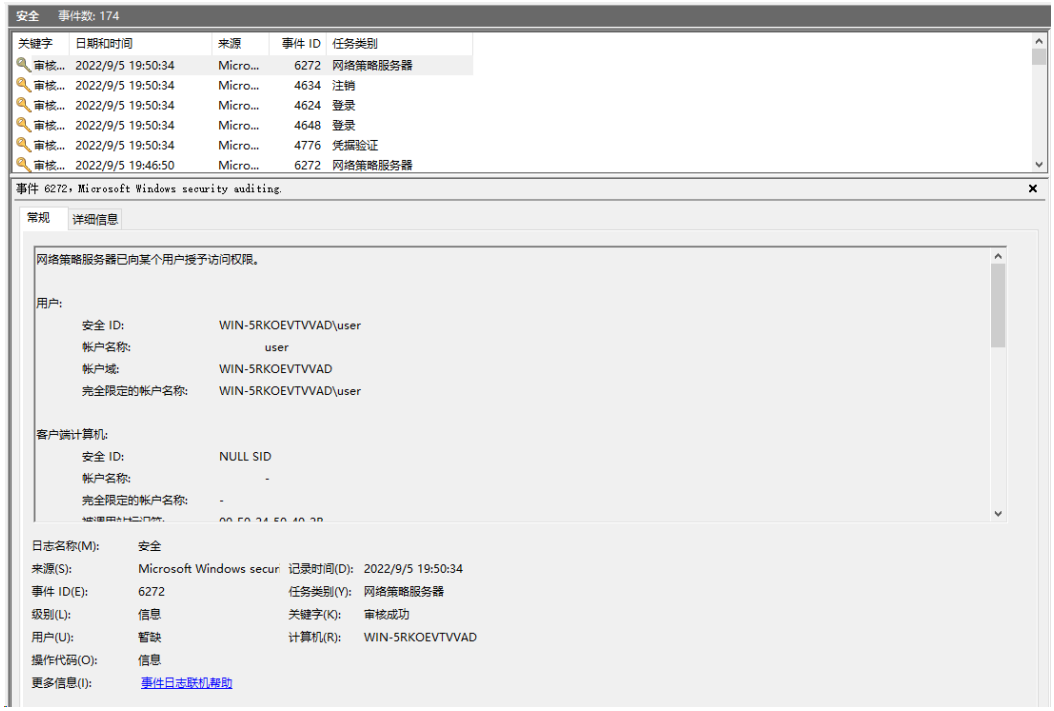


7.9.3 验证配置

用户使用 802.1X 认证方式上线。

(1) 用户上线后服务器上显示如图 7-15。

图7-15 用户上线后服务器显示



(2) 用户上线后，在设备上通过 **display dot1x connection** 命令可以查看上线 802.1X 用户的信息。其中 Authorization tagged VLAN 字段显示成功下发授权 VLAN 7、VLAN 9 和 VLAN 10。授权 VLAN 信息为一个包含若干个“VLAN ID+后缀”形式的字符串，则只有第一个不携带后缀或者携带 untagged 后缀的 VLAN 将被解析为唯一的 untagged 的授权 VLAN（本例为 VLAN 8），其余 VLAN 都被解析为 tagged 的授权 VLAN，端口的缺省 VLAN 将被修改为 untagged 的授权 VLAN。

```
[Switch]display  dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: a036-9f8b-634c
Access interface: GigabitEthernet1/0/2
Username: user
User access state: Successful
Authentication domain: domain1
EAP packet identifier: 2
Authentication method: CHAP
AAA authentication method: RADIUS
Initial VLAN: 165
Authorization untagged VLAN: 8
Authorization tagged VLAN list: 7 9-10
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
```

```
    Authorization CAR: N/A
    Authorization URL: N/A
    Authorization IPv6 URL: N/A
    Authorization temporary redirect: Disabled
    Start accounting: Successful
    Real-time accounting-update failures: 0
    Termination action: Default
    Session timeout period: N/A
    Online from: 2013/01/08 07:22:52
    Online duration: 0h 0m 48s
```

7.9.4 配置文件

```
#
 dot1x
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 1 100 165 untagged
 port hybrid pvid vlan 165
undo dot1x handshake
 dot1x mandatory-domain domain1
 undo dot1x multicast-trigger
 dot1x port-method portbased
#
domain domain1
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 accounting lan-access radius-scheme radius1
#
radius scheme radius1
 primary authentication 101.0.144.123
 primary accounting 101.0.144.123
 key authentication cipher $c$3$9jjl0lp5VA/WXEw065ZIT7j4AIN88XTF
 key accounting cipher $c$3$fk1zm9nf2IFMdk+I7hGsyBcsAwqLobi7
 user-name-format without-domain
#
```

8 授权 ACL 对接配置举例

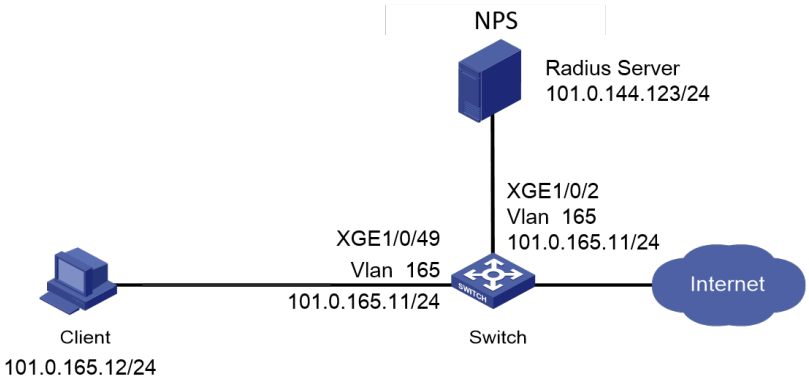
8.1 组网需求

如图 8-1 所示，Client 和 Windows Server 2016-NPS 服务器通过 Switch 建立连接，设备管理员希望对 Client 进行 802.1X 认证或者 MAC 地址认证，以控制其对网络资源的访问，具体要求如下：

- 采用 Windows Server 2016-NPS 作为 RADIUS 服务器。

- 通过 Windows Server 2016-NPS 授权下发 ACL。

图8-1 授权 ACL 组网图



8.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch： S5560X-54C-PWR-EI，Version 7.1.070
- 认证服务器：Windows Server 2016-NPS

8.3 配置步骤

8.3.1 配置 Switch

(1) Swtich 上的配置。

- 若采用 MAC 地址认证，Swtich 上的配置请参考 4.3.1 配置 Switch。
- 若采用 802.1X 认证，Swtich 上的配置请参考 5.3.1 配置 Switch。

(2) 授权 ACL 名称时，该 ACL 必须在设备上已经创建才会生效。

在设备上创建 ACL，并配置规则。

```
<Switch> system-view
[Switch] acl advanced 3001
[Switch-acl-ipv4-adv-3001] rule 0 permit ip source any
```

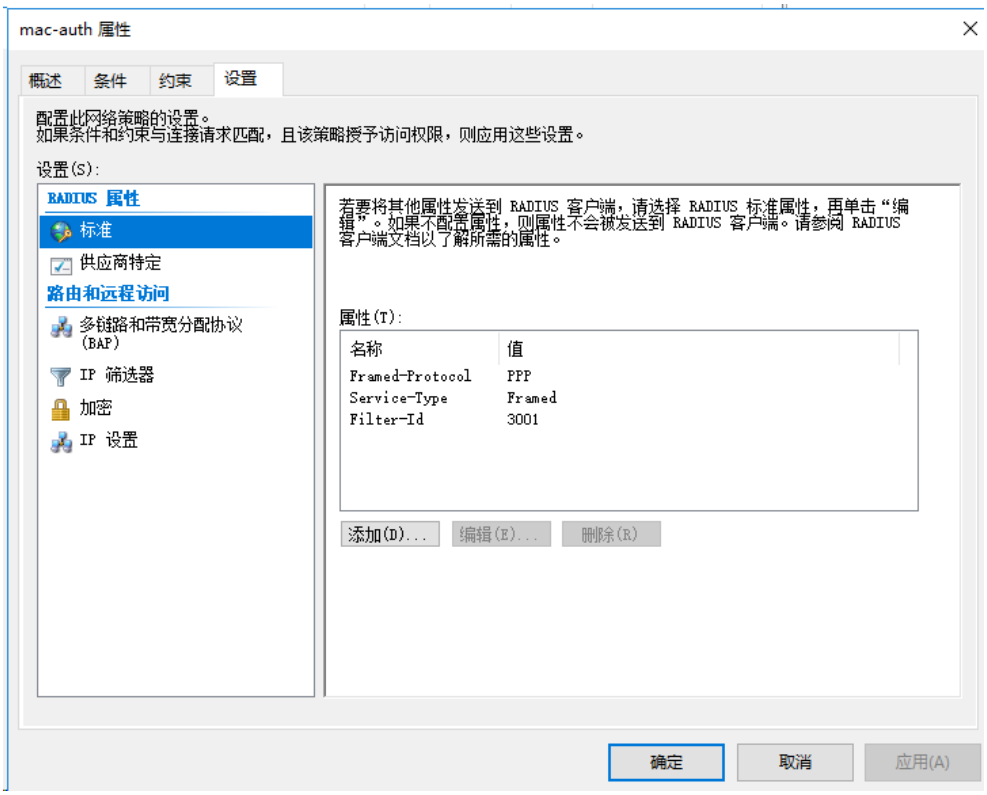
8.3.2 配置 Windows Server 2016-NPS

(1) 服务器上的配置。

- 若采用 MAC 地址认证，服务器上的配置请参考 4.3.2 配置 Windows Server 2016-NPS。
- 若采用 802.1X 认证，服务器上的配置请参考 5.3.2 配置 Windows Server 2016-NPS。

(2) 只需将“配置文件”的“属性”参考图 8-2 修改即可。

图8-2 配置文件



说明

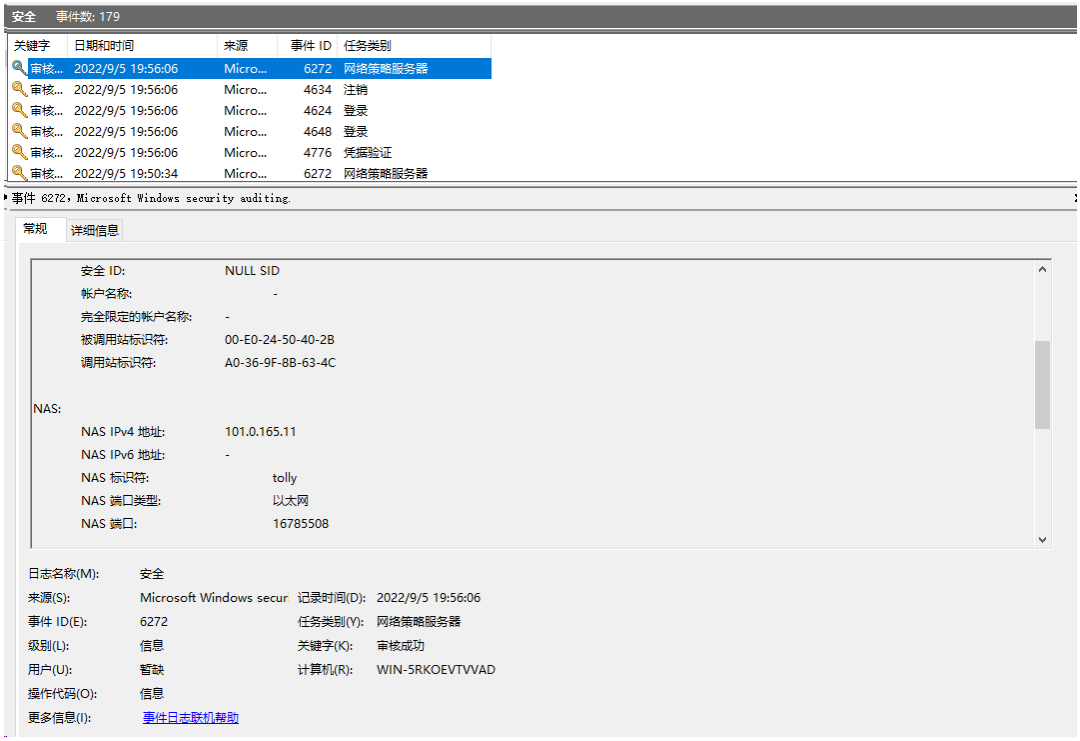
Filter-Id 取值为数字，则按照 ACL Number 处理，取值不全为数字，则按照 User Profile 处理。

8.4 验证配置

以用户使用 802.1X 认证方式上线为例。

(1) 用户上线后服务器上显示如图 8-3。

图8-3 用户上线后服务器显示



(2) 用户上线后，在设备上通过 **display dot1x connection** 命令查看上线 802.1X 用户的信息，可以看到服务器下发的 ACL 成功下发到设备上。

```
<Switch> display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: a036-9f8b-634c
Access interface: GigabitEthernet1/0/2
Username: user
User access state: Successful
Authentication domain: domain1
EAP packet identifier: 2
Authentication method: CHAP
AAA authentication method: RADIUS
Initial VLAN: 165
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: 3001
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Authorization IPv6 URL: N/A
Authorization temporary redirect: Disabled
```

```
    Start accounting: Successful
    Real-time accounting-update failures: 0
    Termination action: Default
    Session timeout period: N/A
    Online from: 2013/01/08 07:28:24
    Online duration: 0h 0m 12s
```

8.5 配置文件

```
#
 dot1x
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 1 100 165 untagged
 port hybrid pvid vlan 165
undo dot1x handshake
 dot1x mandatory-domain domain1
 undo dot1x multicast-trigger
 dot1x port-method portbased
#
domain domain1
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 accounting lan-access radius-scheme radius1
#
radius scheme radius1
 primary authentication 101.0.144.123
 primary accounting 101.0.144.123
 key authentication cipher $c$3$9jjl0lp5VA/WXEw065ZIT7j4AIN88XTF
 key accounting cipher $c$3$fk1zm9nf2IFMdk+I7hGsyBcsAwqLobi7
 user-name-format without-domain
#
```

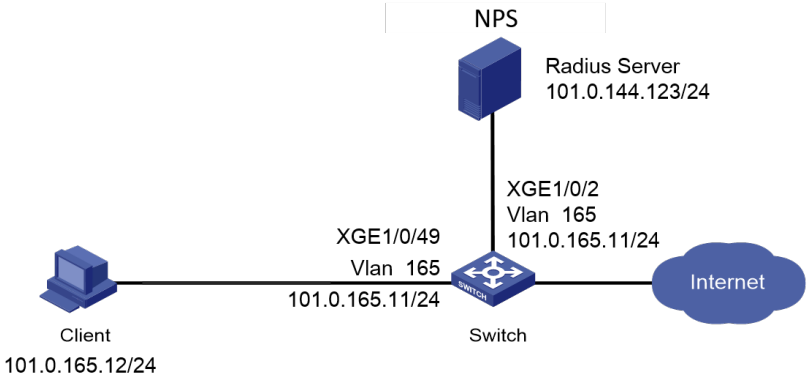
9 授权 User-Profile 对接配置举例

9.1 组网需求

如图 9-1 所示，Client 和 Windows Server 2016-NPS 服务器通过 Switch 建立连接，设备管理员希望对 Client 进行 802.1X 认证或者 MAC 地址认证，以控制其对网络资源的访问，具体要求如下：

- 采用 Windows Server 2016-NPS 作为 RADIUS 服务器。
- 通过 Windows Server 2016-NPS 授权下发 User-Profile。

图9-1 授权 User-Profile 组网图



9.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch： S5560X-54C-PWR-EI，Version 7.1.070
- 认证服务器：Windows Server 2016-NPS

9.3 配置步骤

9.3.1 配置 Switch

(1) Swtich 上的配置。

- 若采用 MAC 地址认证，Swtich 上的配置请参考 4.3.1 配置 Switch。
- 若采用 802.1X 认证，Swtich 上的配置请参考 5.3.1 配置 Switch。

(2) 授权 User-Profile 名称时，该 User-Profile 必须在设备上已经创建才会生效。

为 User 创建 User Profile，并创建 qos car。

```
<Switch> system-view
[Switch] user-profile test
[Switch-user-profile-test]qos  car inbound any  cir 100000
[Switch-user-profile-test] quit
```

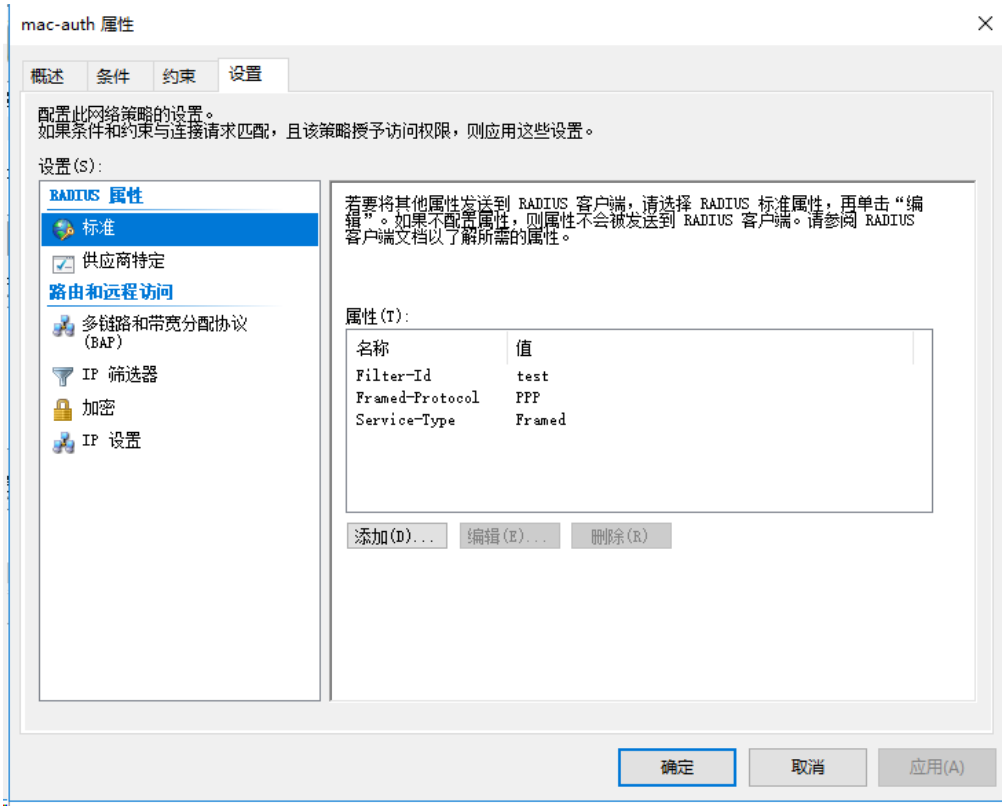
9.3.2 配置 Windows Server 2016-NPS

(1) 服务器上的配置。

- 若采用 MAC 地址认证，服务器上的配置请参考 4.3.2 配置 Windows Server 2016-NPS。
- 若采用 802.1X 认证，服务器上的配置请参考 5.3.2 配置 Windows Server 2016-NPS。

(2) 只需将“网络策略”的“属性”参考图 9-2 修改即可。

图9-2 配置文件



说明

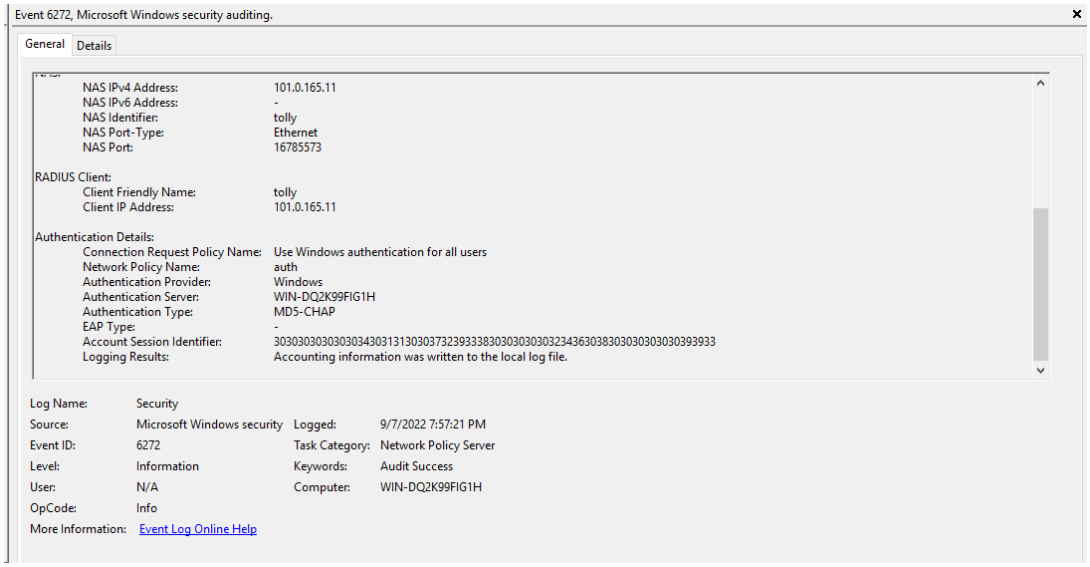
Filter-Id 取值为数字，则按照 ACL Number 处理，取值不全为数字，则按照 User Profile 处理。

9.4 验证配置

以用户使用 802.1X 认证方式上线为例。

(1) 用户上线后服务器上显示如图 9-3。

图9-3 用户上线后服务器显示



(2) 用户上线后，在设备上通过 **display dot1x connection** 命令可以查看上线 802.1X 用户的信息。其中 Authorization user profile 字段显示成功下发名称为 test 的授权 User Profile。

```
<Switch> display  dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: a036-9f8b-634c
Access interface: GigabitEthernet1/0/2
Username: user
User access state: Successful
Authentication domain: domain1
EAP packet identifier: 2
Authentication method: CHAP
AAA authentication method: RADIUS
Initial VLAN: 165
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: test
Authorization CAR: N/A
Authorization URL: N/A
Authorization IPv6 URL: N/A
Authorization temporary redirect: Disabled
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: N/A
```

```
    Online from: 2013/01/10 07:29:38
    Online duration: 0h 0m 50s
```

9.5 配置文件

```
#
 dot1x
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 1 100 165 untagged
 port hybrid pvid vlan 165
undo dot1x handshake
 dot1x mandatory-domain domain1
 undo dot1x multicast-trigger
 dot1x port-method portbased
#
domain domain1
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 accounting lan-access radius-scheme radius1
#
radius scheme radius1
 primary authentication 101.0.144.123
 primary accounting 101.0.144.123
 key authentication cipher $c$3$9jjl0lp5VA/WXEw065ZIT7j4AIN88XTF
 key accounting cipher $c$3$fk1zm9nf2IFMdk+I7hGsyBcsAwqLobi7
 user-name-format without-domain
#
```

H3C 交换机

与 Cisco ISE 功能对接操作指导

目 录

1 简介

本文档介绍 H3C 交换机与 Cisco 的认证服务器软件 ISE 的接入认证功能对接配置，包括：

- 802.1X 认证对接配置举例
- MAC 地址认证对接配置举例
- Portal 认证对接配置举例
- 授权 VLAN 对接配置举例
- 授权静态 ACL 对接配置举例
- 授权动态 ACL 对接配置举例
- 授权 CAR 对接配置举例
- 授权 User-Profile 对接配置举例
- 授权 CAR 对接配置举例
- 重认证对接配置举例
- URL 重定向对接配置举例
- DAE 对接配置举例
- SSH 登录使用 HWTACACS 认证对接配置举例
- 使用 LDAP 账户认证对接配置举例
- 终端识别 Profiling 对接配置举例
- 终端安全 Posture Assessment 对接配置举例

说明

对接第三方认证服务器操作为交换机产品通用性内容，但部分接入认证功能在各交换机产品上存在支持差异。产品对各认证特性的支持情况请参考产品配置指导中安全分册的相关内容。

2 互通性分析

表2-1 接入认证互通性分析

H3C	Cisco ISE	互通结论
802.1X CHAP认证	CHAP认证	可以互通
802.1X PAP认证	PAP认证	可以互通
802.1X EAP认证	EAP-MD5认证	可以互通
802.1X EAP认证	EAP-PEAP/TTLS认证	可以互通
802.1X EAP认证	EAP-TLS认证	可以互通

H3C	Cisco ISE	互通结论
802.1X EAP认证	EAP-FAST认证	可以互通
MAC地址认证	MAC地址认证	可以互通
Portal认证	CWA认证	可以互通
授权VLAN	授权VLAN	可以互通
授权ACL	授权静态ACL	可以互通
授权ACL	授权动态ACL	可以互通
授权CAR属性	授权CAR	可以互通
授权URL重定向	URL重定向	可以互通
DAE	重认证	可以互通
SSH用户的HWTACACS认证	HWTACACS认证	可以互通
使用LDAP账户认证	LDAP账户认证	可以互通
-	终端识别Profiling	可以互通
-	终端安全Posture Assessment	可以互通

3 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

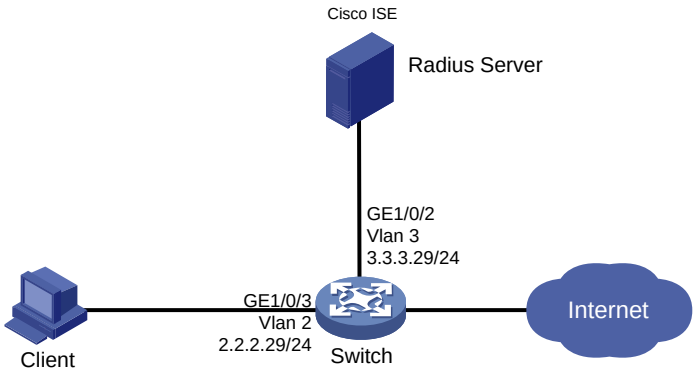
4 802.1X 认证对接配置举例

4.1 组网需求

如图 4-1 所示，Client 和 ISE 服务器通过 Switch 建立连接，设备管理员希望对 Client 进行 802.1X 认证，以控制其对网络资源的访问，具体要求如下：

- 采用 Cisco ISE 作为 RADIUS 服务器。
- 配置 PAP、CHAP、EAP-MD5、EAP-TLS、EAP-PEAP、EAP-TTLS 方式。

图4-1 802.1X 认证配置组网图



4.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch：S5560X-R6618P27
- 认证服务器: Cisco ISE V2.4.0.357 patch 8
- 系统：Windows 10 21H2
- 认证客户端：iNode PC 7.3 (E513)
- 认证客户端：Cisco anyconnect 4.8.03052

4.3 802.1X CHAP配置步骤与验证

说明

本配置仅展示认证的相关配置，网络互通的相关配置略，请保证设备间能够互相访问。

4.3.1 配置 Switch

配置互通的 VLAN 和 VLAN 接口的 IP 地址。

```
<Switch> system-view
[Switch] vlan 2
[Switch-vlan2] quit
[Switch] interface Vlan-interface 2
[Switch-Vlan-interface2] ip address 2.2.2.29 255.255.255.0
[Switch-Vlan-interface2] quit
[Switch] vlan 3
[Switch-vlan3] quit
[Switch] interface Vlan-interface 3
[Switch-Vlan-interface3] ip address 3.3.3.29 255.255.255.0
[Switch-Vlan-interface3] quit
```

将端口 GE1/0/2 加入到指定 VLAN。

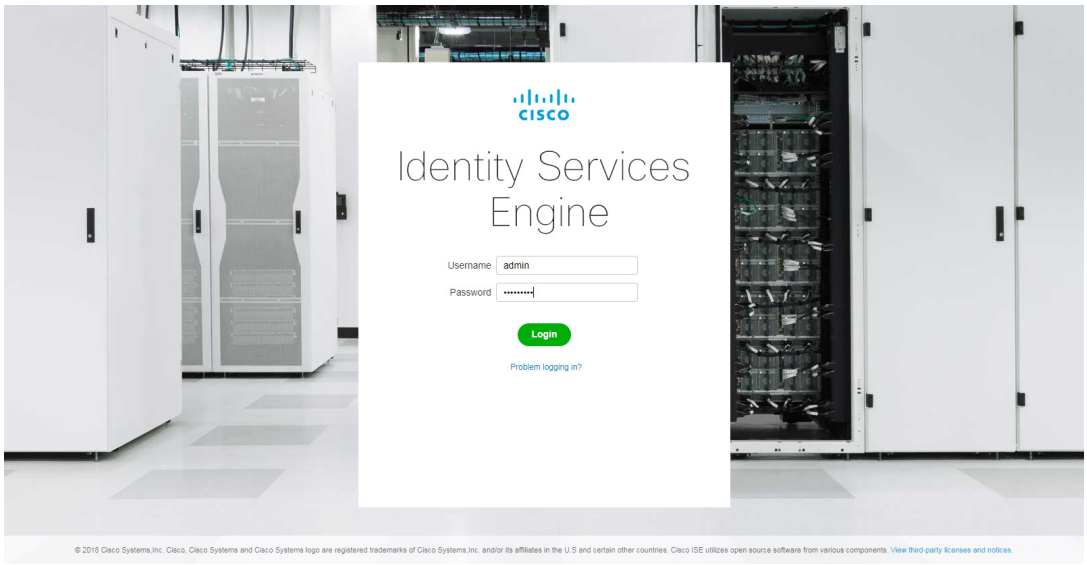
```
[Switch] interface GigabitEthernet 1/0/2
[Switch-GigabitEthernet1/0/2] port switchcess vlan 3
[Switch-GigabitEthernet1/0/2] quit
```
开启全局 802.1x 认证。
```
[Switch] dot1x
```
配置 802.1x 认证的认证方法为 CHAP。
```
[Switch] dot1x authentication-method CHAP
```
配置 RADIUS 方案。
```
<Switch> system-view
[Switch] radius scheme ise
```
配置 RADIUS 服务器地址和密钥，此密钥与 ISE 服务器的配置一致
```
[Switch-radius-ise] primary authentication 3.3.3.24 key simple expert
[Switch-radius-ise] primary accounting 3.3.3.24 key simple expert
[Switch-radius-ise] user-name-format keep-original
[Switch-radius-ise] quit
```
创建 802.1X 认证的域 test.com，配置 ISP 域的 AAA 方法。
```
[Switch] domain test.com
[Switch-isp-test.com] authentication default radius-scheme ise
[Switch-isp-test.com] authorization default radius-scheme ise
[Switch-isp-test.com] accounting default radius-scheme ise
[Switch-isp-test.com] quit
```
将端口 GE1/0/3 加入到指定 VLAN。
```
[Switch]interface Ten-GigabitEthernet 1/0/3
[Switch-GigabitEthernet1/0/3] port switchcess vlan 2
```
开启端口的 802.1X 认证功能，并设置域 test.com 为 802.1X 强制认证域。
```
[Switch-GigabitEthernet1/0/3] dot1x
[Switch-GigabitEthernet1/0/3] dot1x mandatory-domain test.com
```

4.3.2 配置 ISE

(1) 登录 ISE

在浏览器中输入 ISE 的管理 IP 地址，输入用户名密码，登录 ISE 页面。

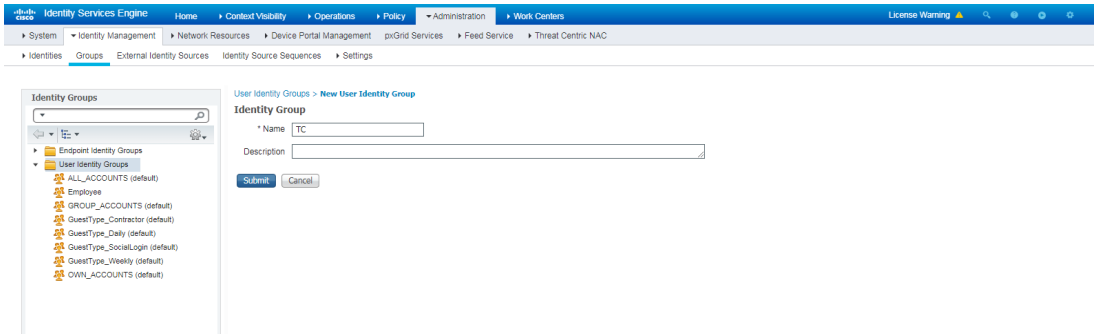
图4-2 登录 ISE



(2) 创建用户组和用户账号

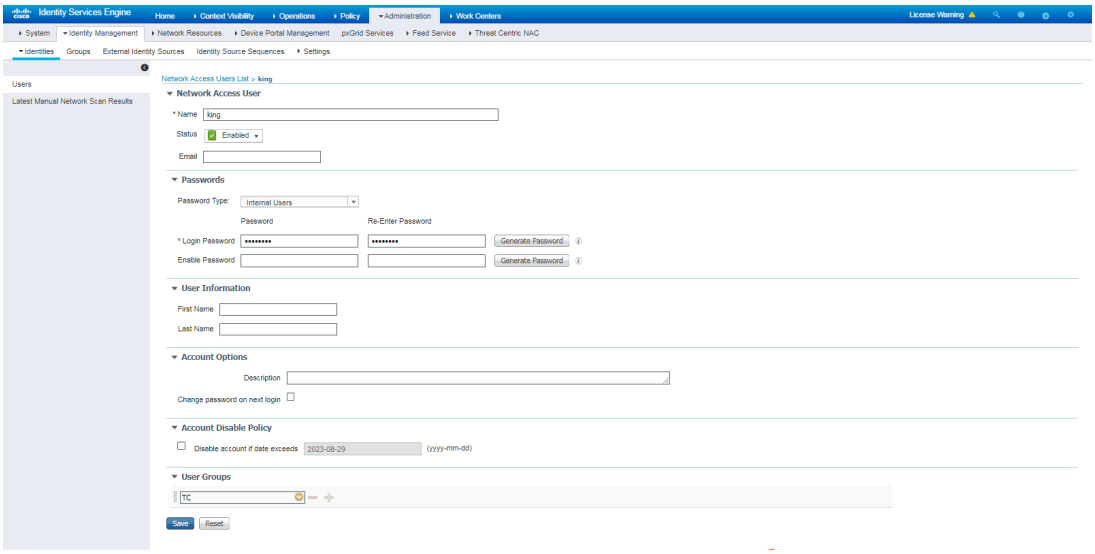
创建用户组：选择[Administration/Identity Management/Groups/User Identity Groups]选项，点击<Add>按钮，创建名称为 TC 的新用户组。

图4-3 创建用户组



创建用户账号：选择[Administration/Identity Management/Identities/Users]选项，点击<Add>按钮，创建名称为 king 的新帐号，配置密码为 king，绑定用户组 TC。

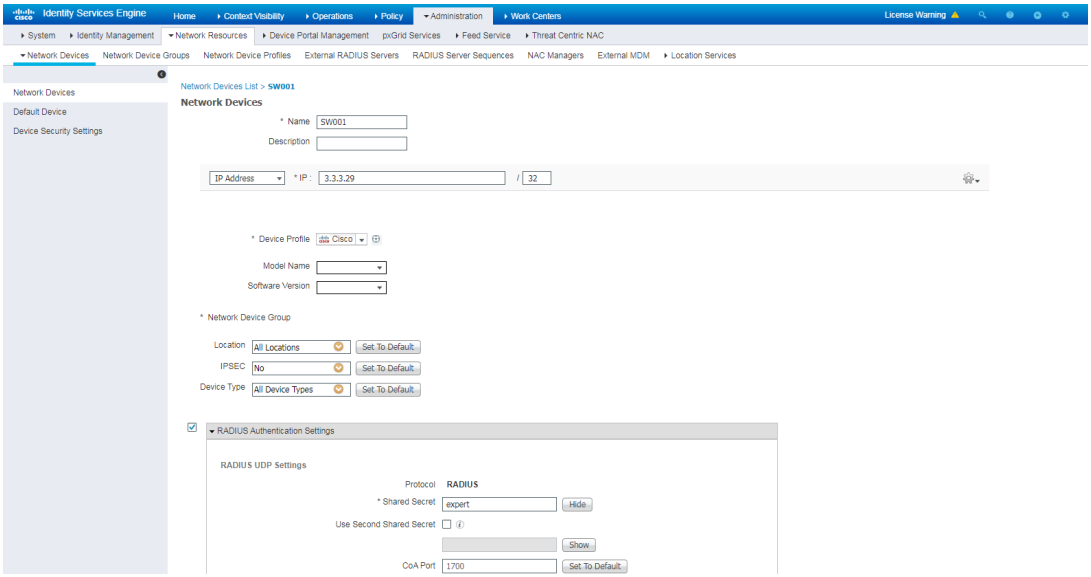
图4-4 创建用户账号



(3) 添加 Switch 设备

在页面上方导航栏中选择[Administration/Network Resources/Network Devices]选项，点击<Add>按钮添加名称为 SW001 的新设备，配置 IP 地址为 3.3.3.29，与 switch 指定的 NAS-IP 保持一致，配置密码 expert，与设备上配置的与 RADIUS 服务器交互的密钥相同。

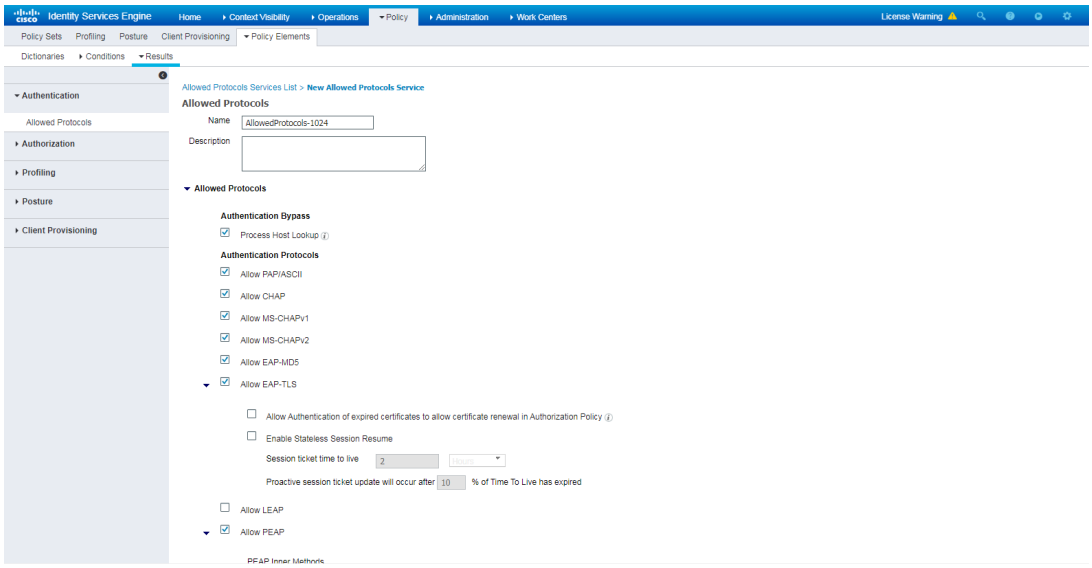
图4-5 添加 Switch



(4) 配置认证协议

在页面上方导航栏中选择[Policy/Policy Elements/Results/Authentication/Allowed Protocols]选项，新建名称为 AllowedProtocols-1024 的认证协议服务，确认勾选 Allow CHAP 选项。

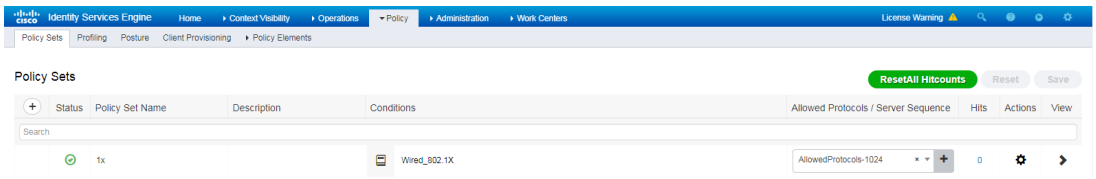
图4-6 新建认证协议服务



(5) 配置认证和授权策略

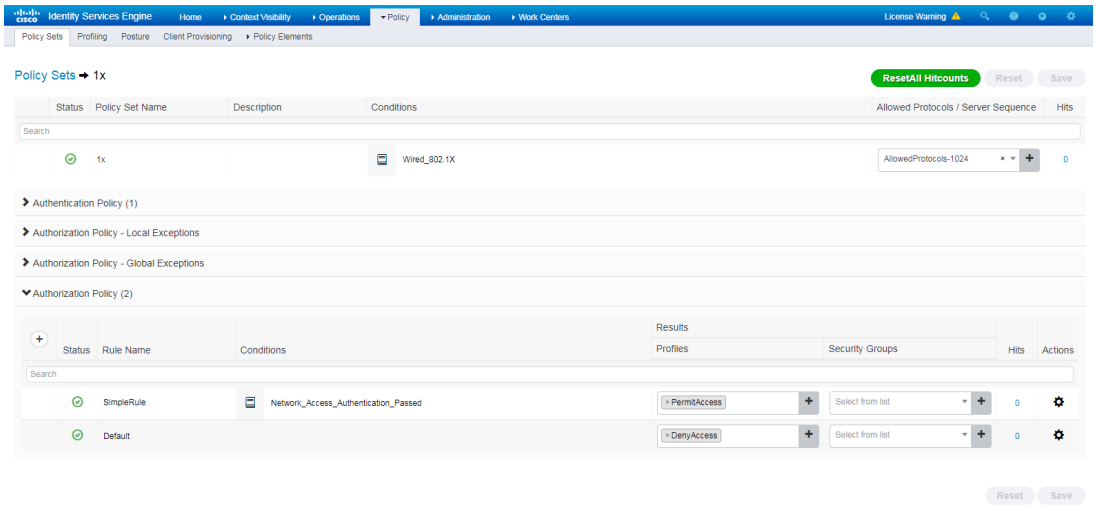
配置认证和授权策略：在页面上方导航栏中选择[Policy/Policy Sets]选项，点击 Policy Sets 下方的<+>按钮，配置名称 1x 的认证和授权策略，并在 Conditions 栏中选择“Wired_Dot1x”，在 Allowed Protocols/Server Sequence 栏中选择 Default Network Access。

图4-7 配置认证和授权策略 1



点击上图“1x”后的<View>按钮，在 Authorization Policy 栏中新增一个名称为 SimpleRule 的授权策略，在 Result Pofiles 栏中选择选择“PermitAccess”。

图4-8 配置认证和授权策略 2

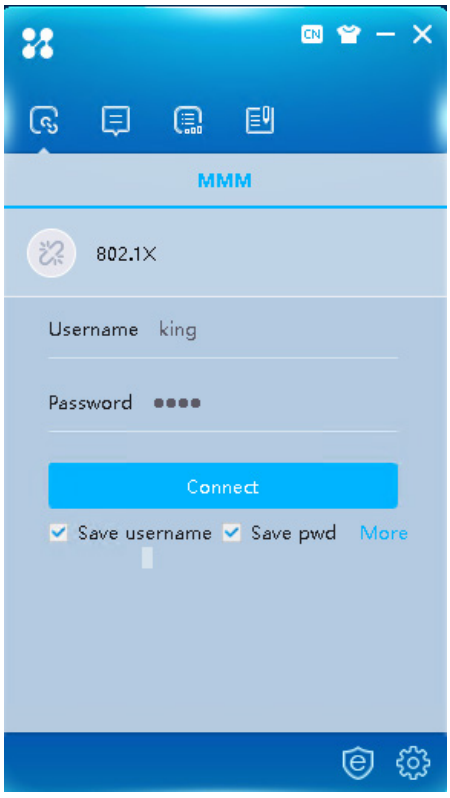


4.3.3 验证配置

(1) Windows 上 iNode 连接情况

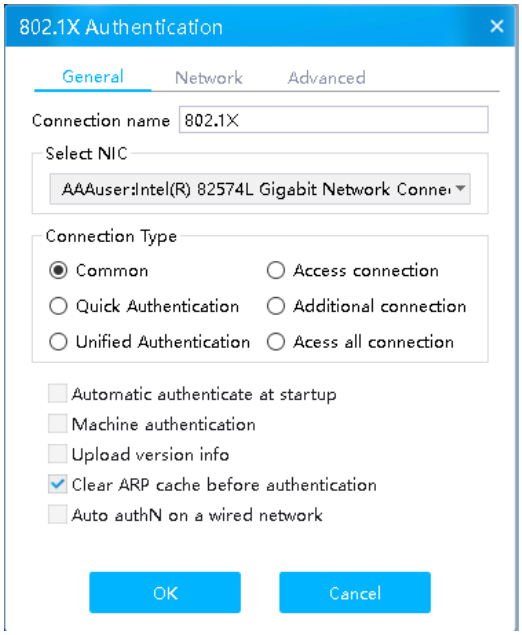
点击“More”，进入 802.1X 认证的属性页面。

图4-9 iNode 连接页面



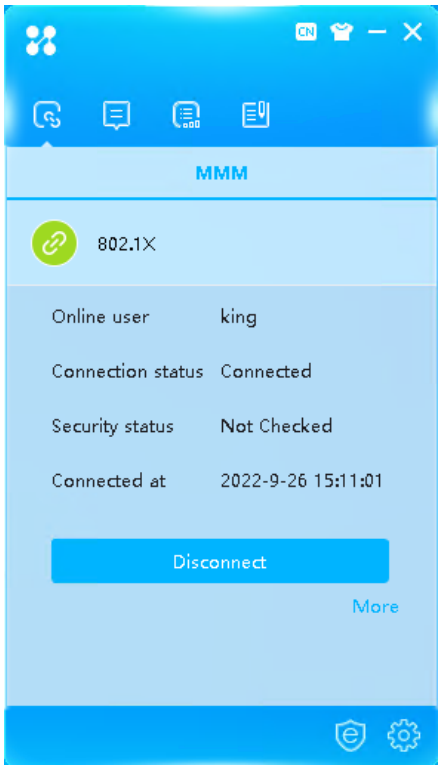
建议取消勾选“Upload version info”，点击<OK>。

图4-10 配置连接信息



输入服务器上配置的用户名和密码即可完成用户上线。

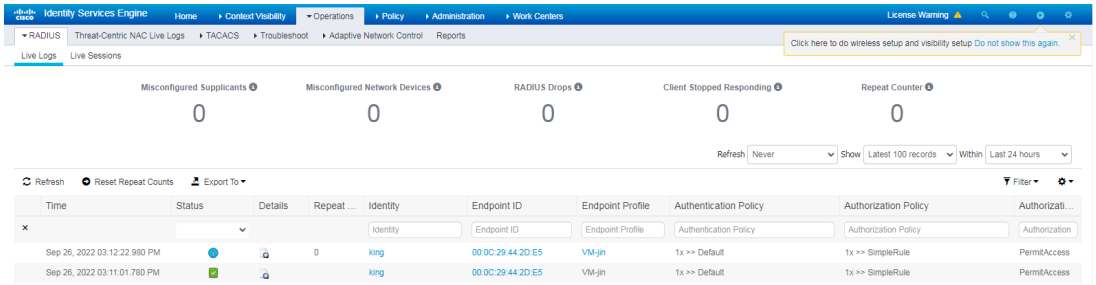
图4-11 iNode 802.1X 连接成功



(2) 服务器显示情况

在页面上方导航栏中选择[Operations/RADIUS]，用户可以查看终端上线的 Live Logs 和 Live Sessions。

图4-12 查看终端上线的 Live Logs



点击 Details 栏按钮，查看 Authentication Details，可以看到 Authentication Protocol 为 CHAP/MD5 等相关信息。

图4-13 查看 Live Logs 的 Details

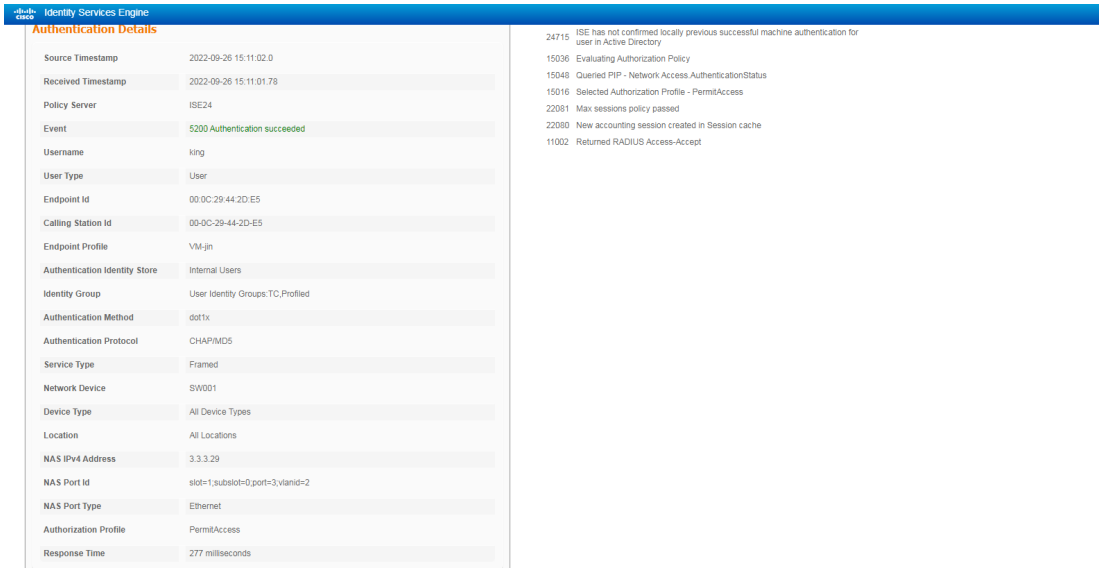
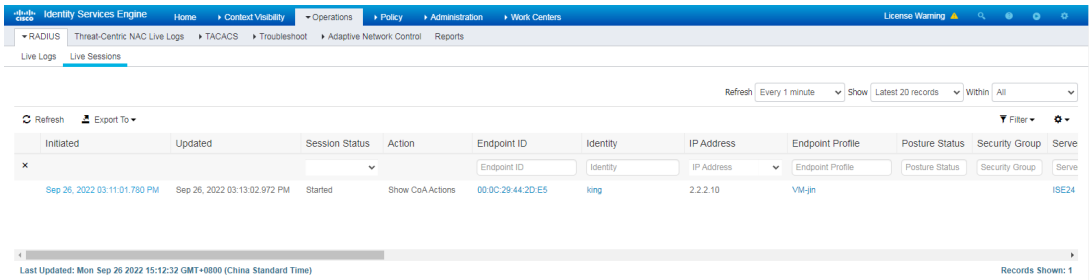


图4-14 查看终端上线的 Live Sessions



(3) 设备上的显示情况

在设备上通过 **display dot1x connection** 可以查看 802.1X 用户的信息，可其中 Username 为 802.1X 的用户名（本例为 king）。

```
<Switch> display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 000c-2944-2de5
Access interface: GigabitEthernet1/0/3
Username: king
User access state: Successful
Authentication domain: ise
IPv4 address: 2.2.2.10
IPv4 address source: IP Source Guard
EAP packet identifier: 2
Authentication method: CHAP
AAA authentication method: RADIUS
Initial VLAN: 2
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Authorization IPv6 URL: N/A
Authorization temporary redirect: Disabled
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: N/A
Online from: 2022/09/26 15:09:04
Online duration: 0h 7m 55s
```

4.3.4 配置文件

```
#
 dot1x
 dot1x authentication-method chap
#
vlan 1
#
vlan 2
 description toClients
 arp snooping enable
#
vlan 3
 description toAAAserver
```

```
#
interface Vlan-interface1
#
interface Vlan-interface2
 description toClients
 ip address 2.2.2.29 255.255.255.0
#
interface Vlan-interface3
 description toAAAservers
 ip address 3.3.3.29 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 2
 dot1x
#
radius scheme ise
 primary authentication 3.3.3.24 key cipher $c$3$2oLOvHdRilTBlb6n1yh3/MoXN8z/RMbctQ==
 primary accounting 3.3.3.24 key cipher $c$3$fAhWH/rHm9hCcPq2PBWQa54YG9xKuQ1P0w==
 timer realtime-accounting 20 second
user-name-format keep-original
#
#
domain test.com
 authentication default radius-scheme ise
 authorization default radius-scheme ise
 accounting default radius-scheme ise
#
```

4.4 802.1X PAP认证配置步骤与验证

4.4.1 配置 Switch

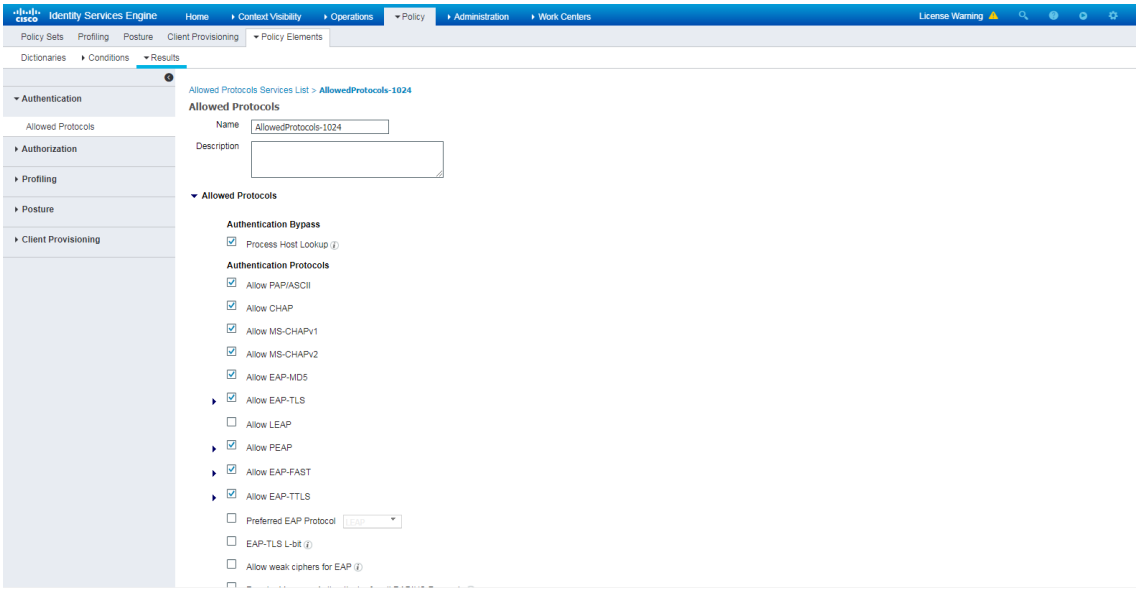
设备上只需要将认证方式修改为 PAP，其它配置无需修改，具体请参考 4.3.1 配置 Switch。

```
[Switch] dot1x authentication-method PAP
```

4.4.2 配置 ISE

服务器上确认 Allowed Protocols 勾选 Allow PAP/ASCII，具体请参考 4.3.2 配置 ISE。

图4-15 确认勾选 Allow PAP/ASCII

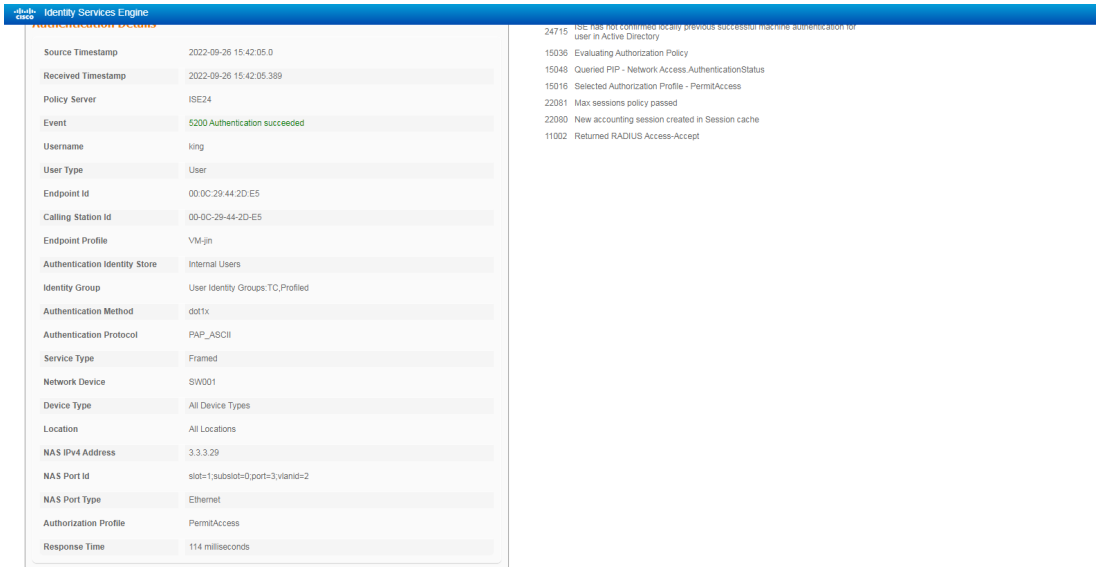


4.4.3 验证配置

(1) 在设备和服务器都配置好的情况下，在客户端使用 iNode 客户端，输入服务器上配置的用户名和密码即可完成用户上线。

(2) 用户上线后服务器显示如图 4-16 所示。

图4-16 用户上线后服务器显示



(3) 用户上线后设备显示

在设备上通过 **display dot1x connection** 可以查看 802.1X 用户的信息，可以看到上线用户的 Authentication methodzi 字段已更改为 PAP。其余信息不变。

```
<Switch> display dot1x connection
```

```
Total connections: 1
Slot ID: 1
User MAC address: 000c-2944-2de5
Access interface: GigabitEthernet1/0/3
Username: king
User access state: Successful
Authentication domain: ise
IPv4 address: 2.2.2.10
IPv4 address source: IP Source Guard
EAP packet identifier: 2
Authentication method: PAP
AAA authentication method: RADIUS
Initial VLAN: 2
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Authorization IPv6 URL: N/A
Authorization temporary redirect: Disabled
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: N/A
Online from: 2022/09/26 15:40:08
Online duration: 0h 1m 16s
```

4.4.4 配置文件

```
#
 dot1x
 dot1x authentication-method pap
#
vlan 1
#
vlan 2
 description toClients
 arp snooping enable
#
vlan 3
 description toAAAserver
#
interface Vlan-interface1
#
interface Vlan-interface2
```

```
 description toClients
 ip address 2.2.2.29 255.255.255.0
#
interface Vlan-interface3
 description toAAAservers
 ip address 3.3.3.29 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 2
 dot1x
#
radius scheme ise
 primary authentication 3.3.3.24 key cipher $c$3$2oLOvHdRilTBlb6n1yh3/MoXN8z/RMbctQ==
 primary accounting 3.3.3.24 key cipher $c$3$fAhWH/rHm9hCcPq2PBWQa54YG9xKuQ1P0w==
 timer realtime-accounting 20 second
 user-name-format keep-original
#
#
domain test.com
 authentication default radius-scheme ise
 authorization default radius-scheme ise
 accounting default radius-scheme ise
#
```

4.5 802.1X EAP-MD5认证配置步骤与验证

4.5.1 配置 Switch

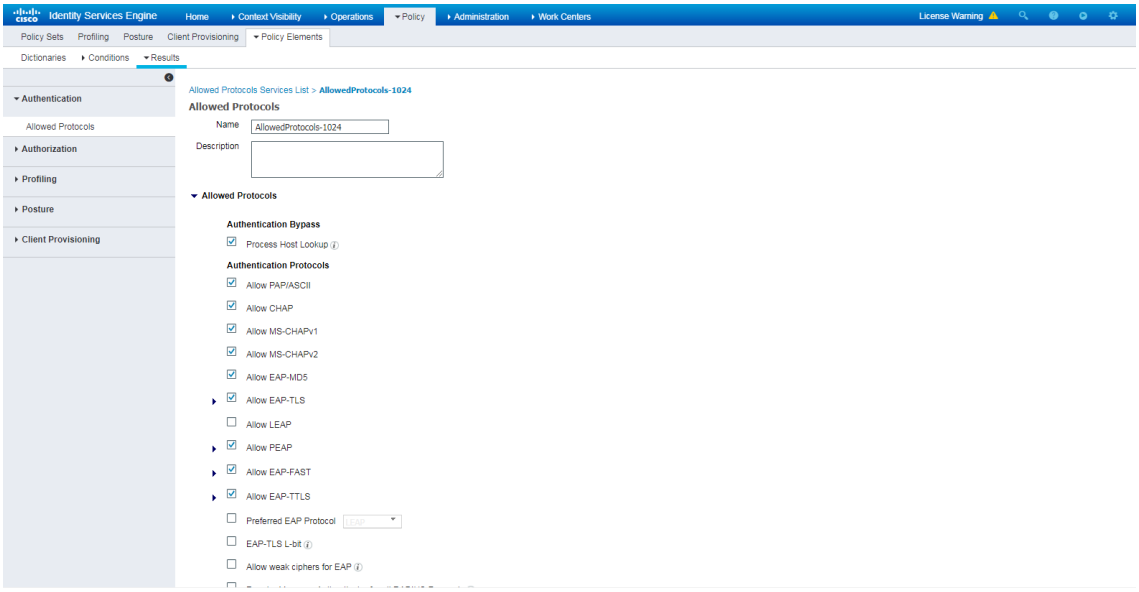
设备上只需要将认证方式修改为 EAP，其它配置无需修改，具体请参考 4.3.1 配置 Switch。

```
[Switch] dot1x authentication-method EAP
```

4.5.2 配置 ISE

服务器上确认 Allowed Protocols 勾选 Allow EAP-MD5，具体请参考 4.3.2 配置 ISE。

图4-17 确认勾选 Allow EAP-MD5

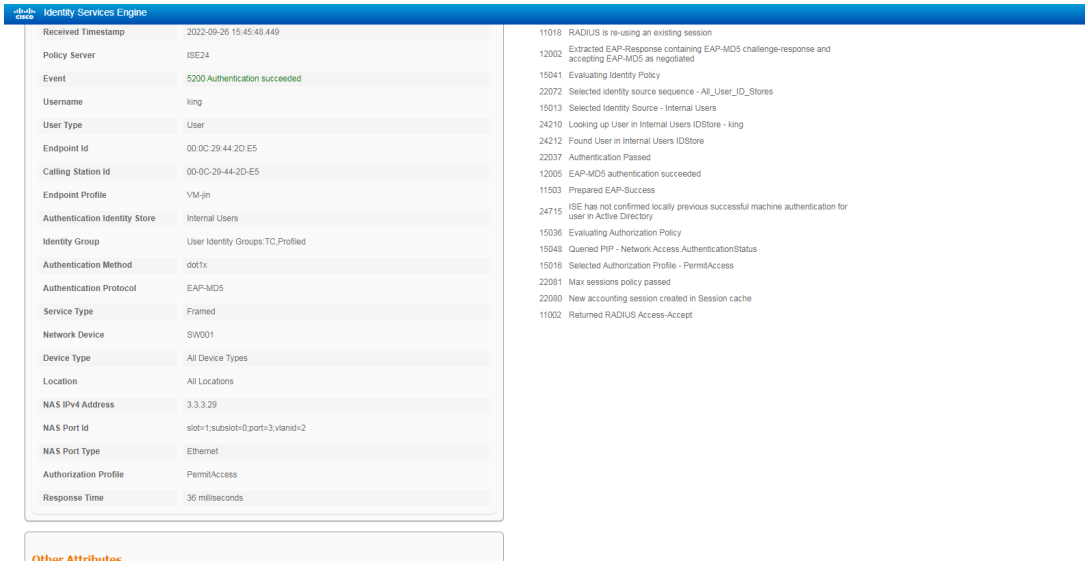


4.5.3 验证配置

(1) 在设备和服务器都配置好的情况下，在客户端使用 iNode 客户端，输入服务器上配置的用户名和密码即可完成用户上线。

(2) 用户上线后服务器显示如图 4-18。

图4-18 用户上线后服务器显示



(3) 用户上线后设备显示

在设备上通过 **display dot1x connection** 可以查看 802.1X 用户的信息，可其中 Username 为 802.1X 的用户名（本例为 king）。

```
<Switch> display dot1x connection
```

```
Total connections: 1
Slot ID: 1
User MAC address: 000c-2944-2de5
Access interface: GigabitEthernet1/0/3
Username: king
User access state: Successful
Authentication domain: ise
IPv4 address: 2.2.2.10
IPv4 address source: IP Source Guard
EAP packet identifier: 108
Authentication method: EAP
AAA authentication method: RADIUS
Initial VLAN: 2
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Authorization IPv6 URL: N/A
Authorization temporary redirect: Disabled
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: N/A
Online from: 2022/09/26 15:43:51
Online duration: 0h 0m 8s
```

4.5.4 配置文件

```
#
 dot1x
 dot1x authentication-method eap
#
vlan 1
#
vlan 2
 description toClients
 arp snooping enable
#
vlan 3
 description toAAAserver
#
interface Vlan-interface1
#
interface Vlan-interface2
```

```
 description toClients
 ip address 2.2.2.29 255.255.255.0
#
interface Vlan-interface3
 description toAAAservers
 ip address 3.3.3.29 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 2
 dot1x
#
radius scheme ise
 primary authentication 3.3.3.24 key cipher $c$3$2oLOvHdRilTBlb6n1yh3/MoXN8z/RMbctQ==
 primary accounting 3.3.3.24 key cipher $c$3$fAhWH/rHm9hCcPq2PBWQa54YG9xKuQ1P0w==
 timer realtime-accounting 20 second
 user-name-format keep-original
#
#
domain test.com
 authentication default radius-scheme ise
 authorization default radius-scheme ise
 accounting default radius-scheme ise
#
```

4.6 802.1X EAP-PEAP/TTLS认证配置步骤与验证

下述配置以不要求客户端证书，服务器端使用了 ISE 自带的自签名证书来举例。

4.6.1 配置 Switch

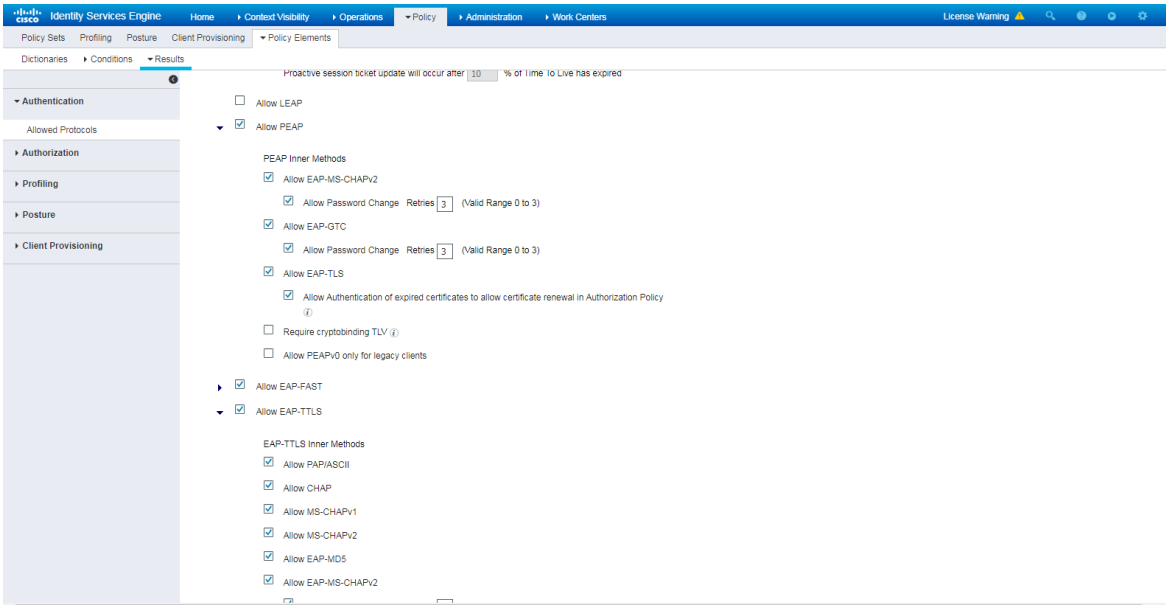
设备上确认认证方式配置为 EAP，其它配置无需修改，具体请参考 4.3.1 配置 Switch。

```
[Switch] dot1x authentication-method EAP
```

4.6.2 配置 ISE

服务器上确认使用的 Allowed Protocols 勾选 Allow PEAP/Allow EAP-TTLS 相关选项，具体请参考 4.3.2 配置 ISE。

图4-19 确认勾选 Allow PEAP/Allow EAP-TTLS 相关选项

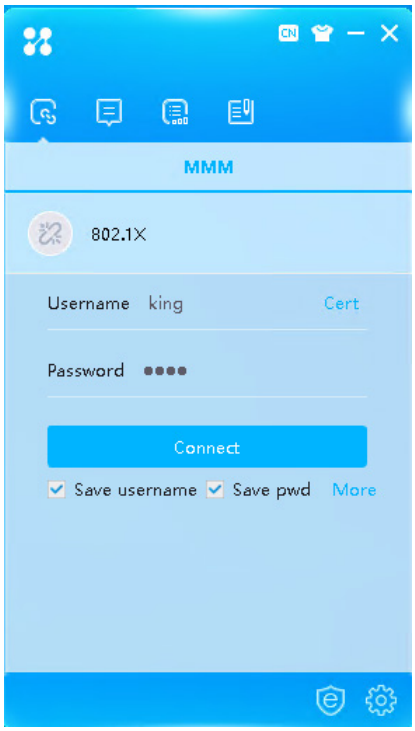


4.6.3 验证配置

(1) iNode 配置及显示情况

点击“More”，进入 802.1X 认证的属性页面。

图4-20 802.1X 客户端认证



认证类型“Authentication Type”勾选“PEAP”或“EAP-TTLS”，点击<OK>。

图4-21 勾选认证方式为 PEAP

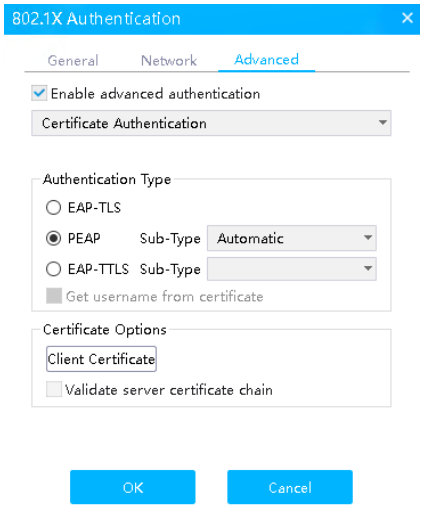
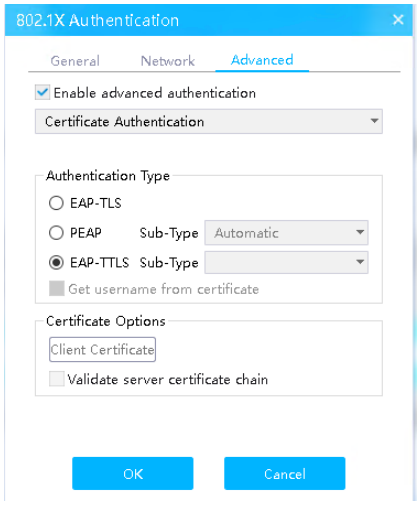


图4-22 勾选认证方式为 EAP-TTLS



认证通过后，显示效果跟其他 EAP 认证方式相同。

(2) 用户上线后服务器显示如图 4-23、图 4-24。

图4-23 认证方式为 PEAP 时用户上线后服务器显示

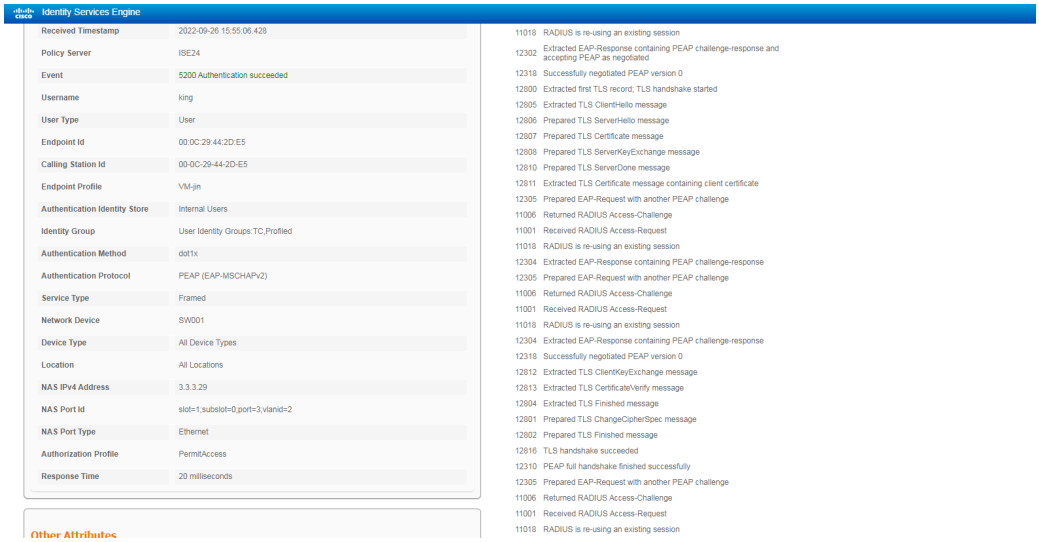
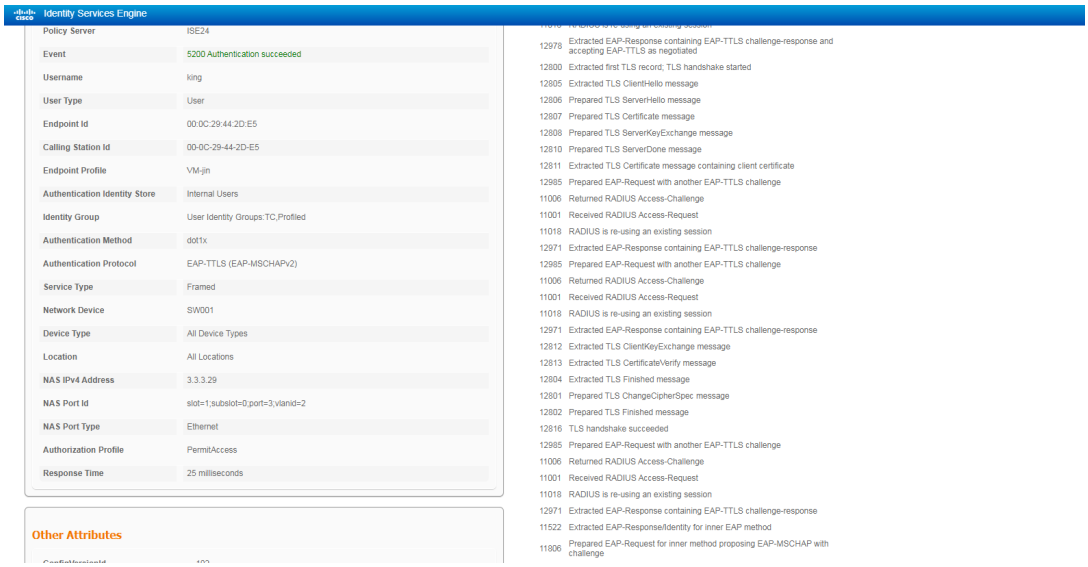


图4-24 认证方式为 EAP-TTLS 时用户上线后服务器显示



(3) 用户上线后设备显示

在设备上通过 **display dot1x connection** 可以查看 802.1X 用户的信息，可其中 Username 为 802.1X 的用户名（本例为 king）。

```
<Switch> display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 000c-2944-2de5
Access interface: GigabitEthernet1/0/3
Username: king
User access state: Successful
Authentication domain: ise
```

```
      IPv4 address: 2.2.2.10
      IPv4 address source: IP Source Guard
      EAP packet identifier: 108
      Authentication method: EAP
      AAA authentication method: RADIUS
      Initial VLAN: 2
      Authorization untagged VLAN: N/A
      Authorization tagged VLAN list: N/A
      Authorization VSI: N/A
      Authorization microsegment ID: N/A
      Authorization ACL number/name: N/A
      Authorization dynamic ACL name: N/A
      Authorization user profile: N/A
      Authorization CAR: N/A
      Authorization URL: N/A
      Authorization IPv6 URL: N/A
      Authorization temporary redirect: Disabled
      Start accounting: Successful
      Real-time accounting-update failures: 0
      Termination action: Default
      Session timeout period: N/A
      Online from: 2022/09/26 15:43:51
      Online duration: 0h 0m 8s
```

4.6.4 配置文件

```
#
 dot1x
 dot1x authentication-method eap
#
vlan 1
#
vlan 2
 description toClients
 arp snooping enable
#
vlan 3
 description toAAAserver
#
interface Vlan-interface1
#
interface Vlan-interface2
 description toClients
 ip address 2.2.2.29 255.255.255.0
#
interface Vlan-interface3
 description toAAAservers
 ip address 3.3.3.29 255.255.255.0
#
```

```
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 2
 dot1x
#
radius scheme ise
 primary authentication 3.3.3.24 key cipher $c$3$2oLOvHdRilTBlb6n1yh3/MoXN8z/RMbctQ==
 primary accounting 3.3.3.24 key cipher $c$3$fAhWH/rHm9hCcPq2PBWQa54YG9xKuQ1P0w==
 timer realtime-accounting 20 second
 user-name-format keep-original
#
#
domain test.com
 authentication default radius-scheme ise
 authorization default radius-scheme ise
 accounting default radius-scheme ise
#
```

4.7 802.1X EAP-TLS认证配置步骤与验证

本文档以 Windows Server 作为第三方 CA 来签发证书为例，Windows Server 及 CA 服务等安装配置请参考其他文档。

4.7.1 配置 Switch

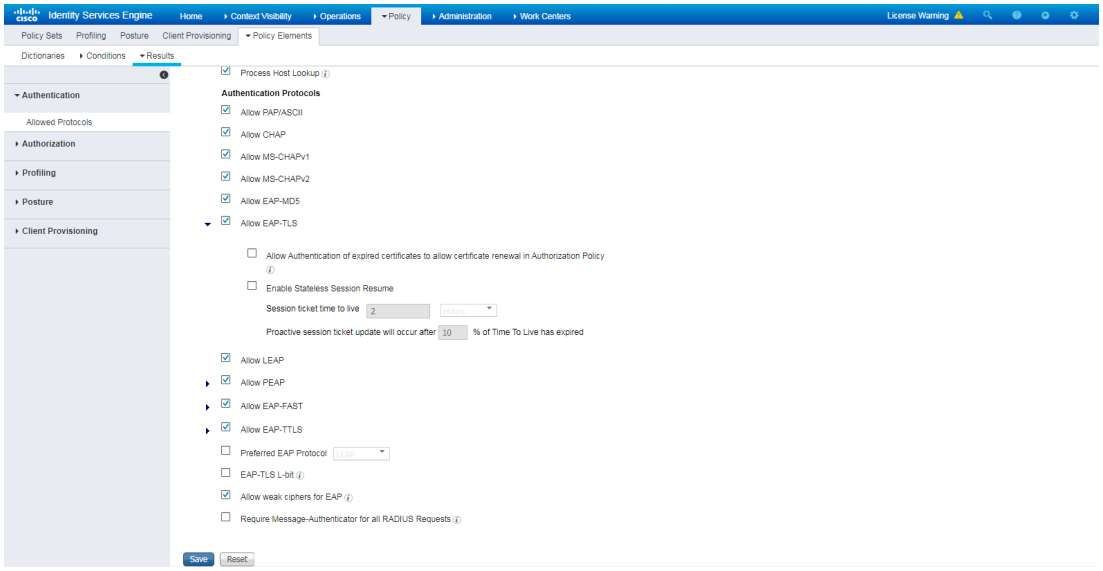
设备上确认认证方式为 EAP，其它配置无需修改，具体请参考 4.3.1 配置 Switch。

```
[Switch] dot1x authentication-method EAP
```

4.7.2 配置 ISE

(1) 服务器上确认 Allowed Protocols 勾选 Allow EAP-TLS，服务器上的其他配置请参考 4.3.2 配置 ISE。

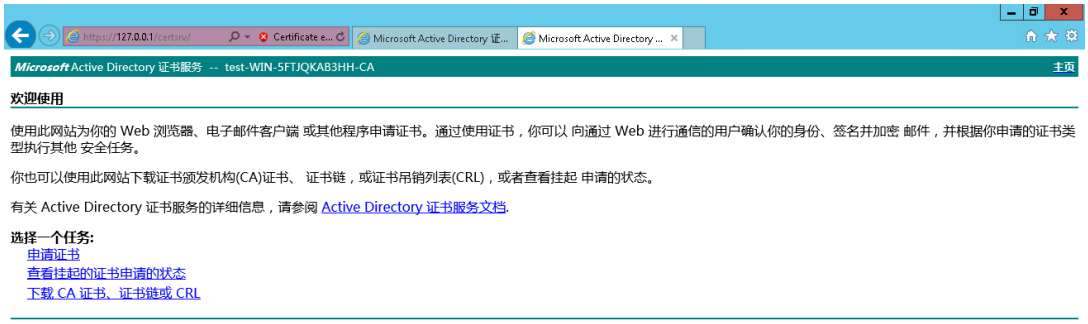
图4-25 确认勾选 Allow EAP-TLS



(2) 下载并安装根证书

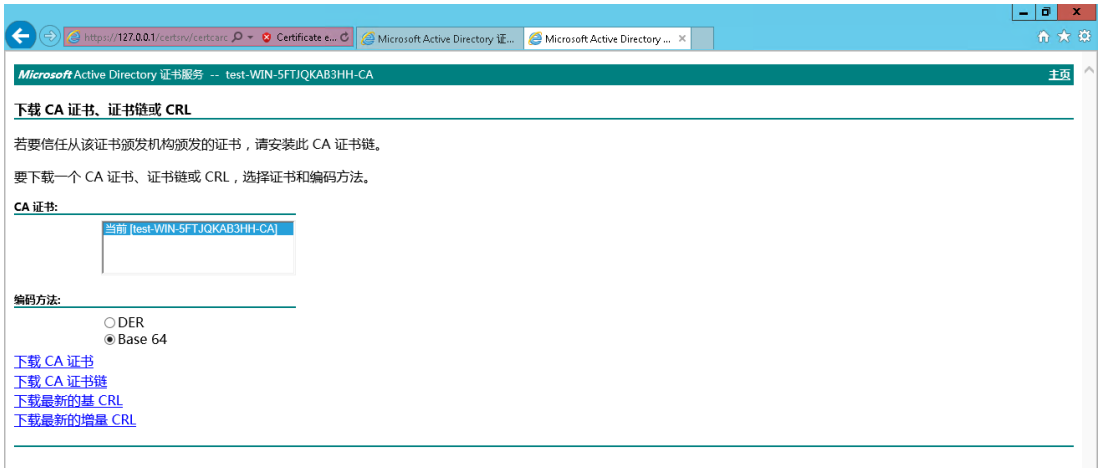
打开 Windows Server 证书服务 Web 界面，并点击“下载 CA 证书、证书链或 CRL”。Windows server 证书服务的具体安装配置请参考 Windows server 相关文档。

图4-26 下载 CA 证书、证书链或 CRL



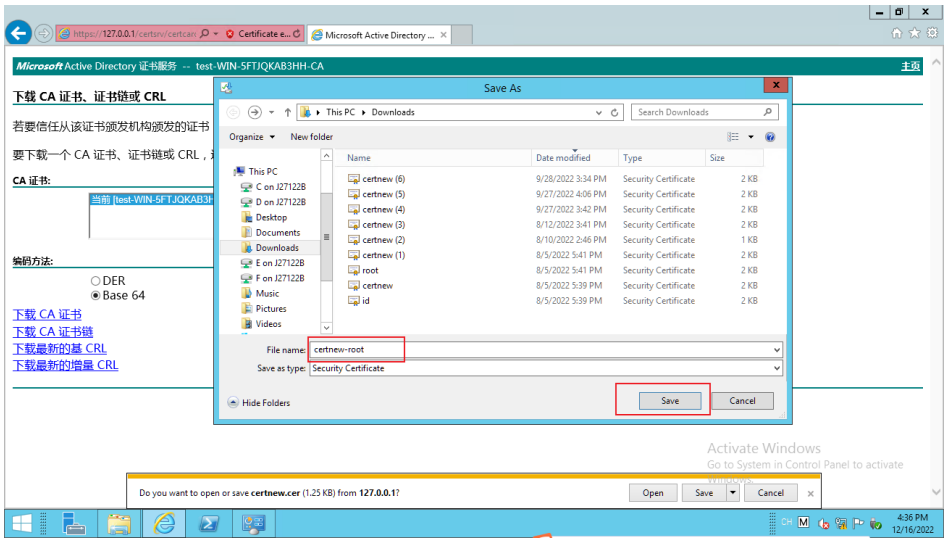
点击“下载 CA 证书”。

图4-27 下载 CA 证书



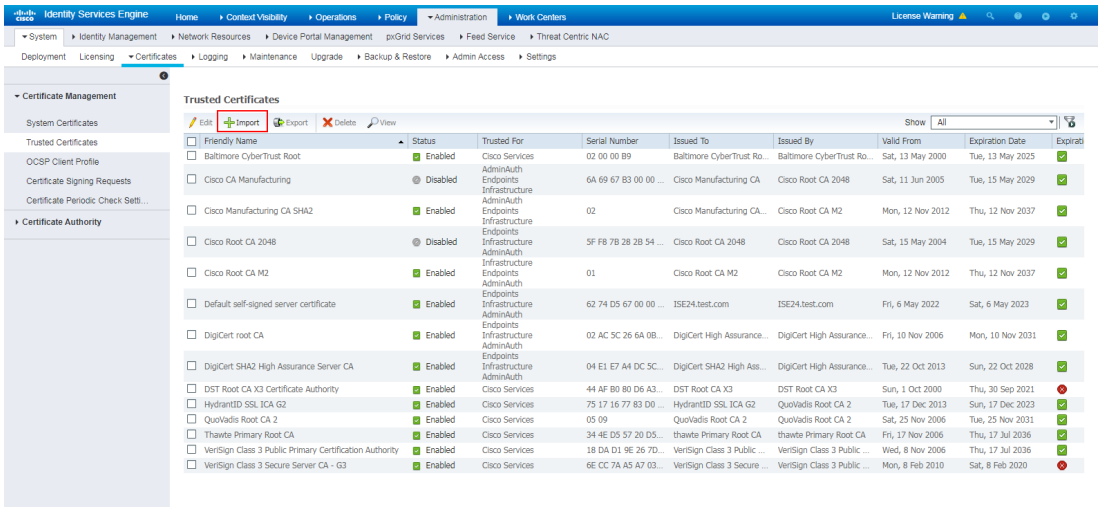
将证书命令为 certnew-root.cer。

图4-28 命名下载的证书



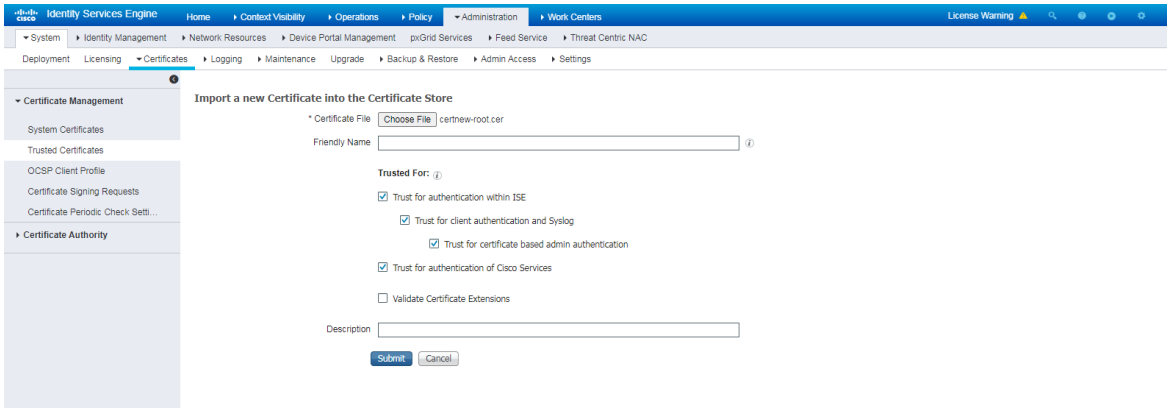
登录 ISE 页面，在页面上方导航栏中选择[Administration/System/Certificates/Certificate Management/Trusted Certificates]选项，点击“Import”，添加证书。

图4-29 打开添加证书页面



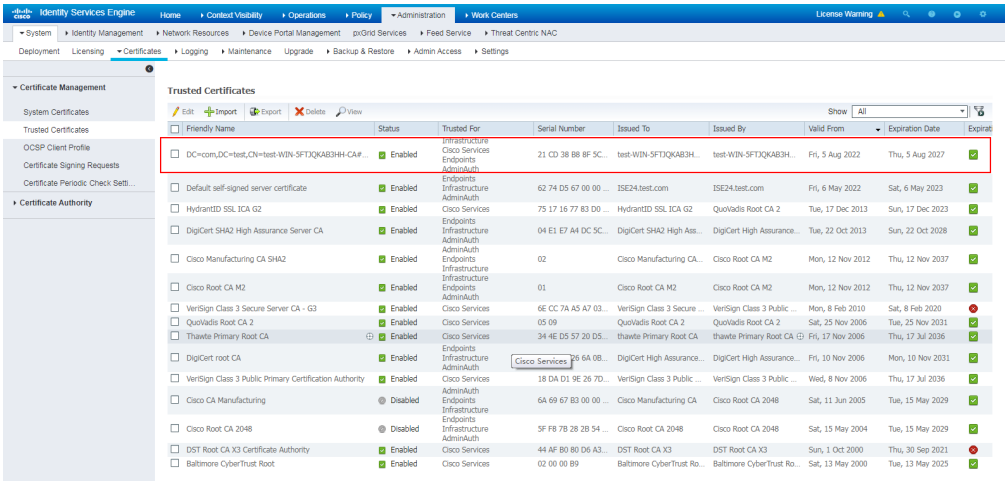
点击<Choose File>选择并上传刚下载的根证书，并点击<Submit>确认。

图4-30 选择并上传刚下载的根证书



可以看到刚上传的根证书如下图列表中红框所示。

图4-31 查看导入的根证书



(3) 申请并安装个人证书

在 ISE 页面上方导航栏中选择[Administration/System/Certificates/Certificate Management/Certificate Siging Requests]选项，按照如下步骤，生成 CSR。

图4-32 选择 multi-use，并补充其他信息

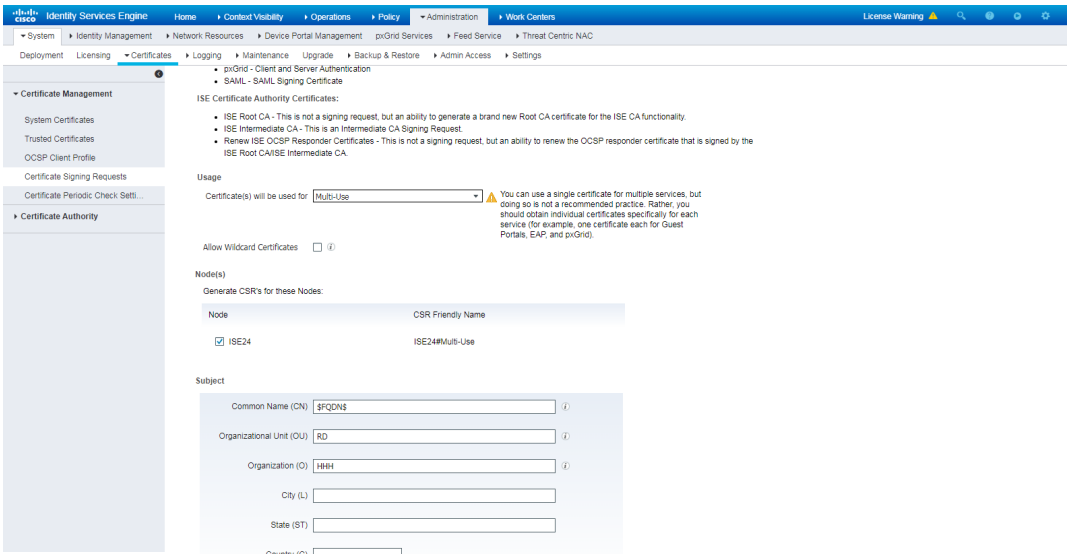


图4-33 页面底端点击 Generate

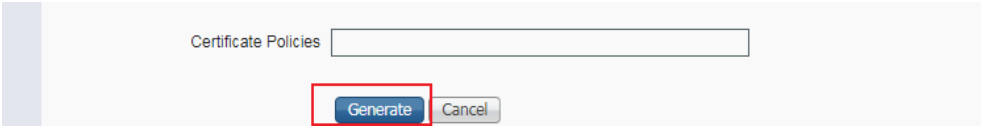
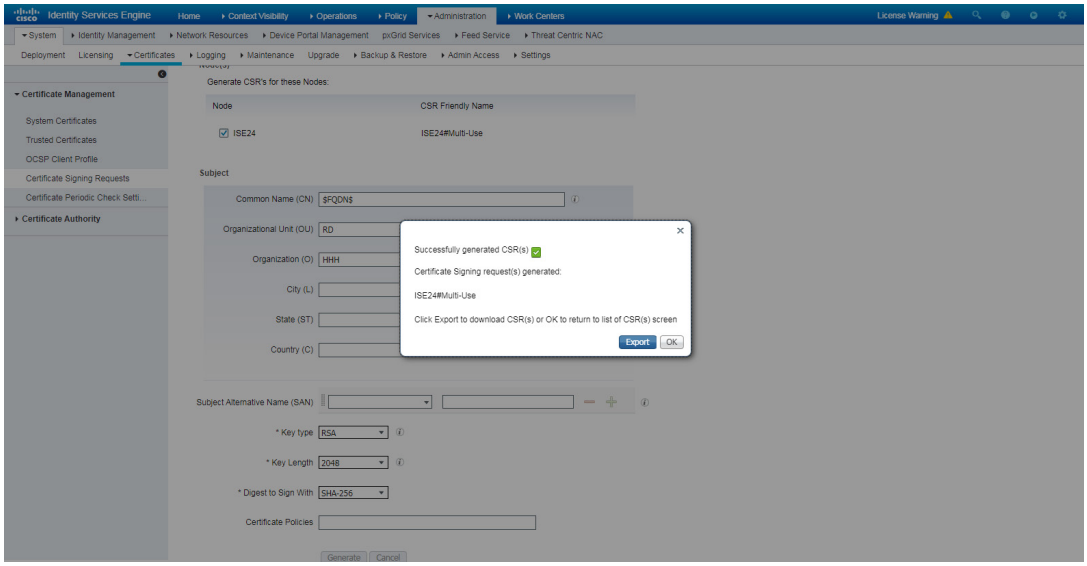


图4-34 点击 Export



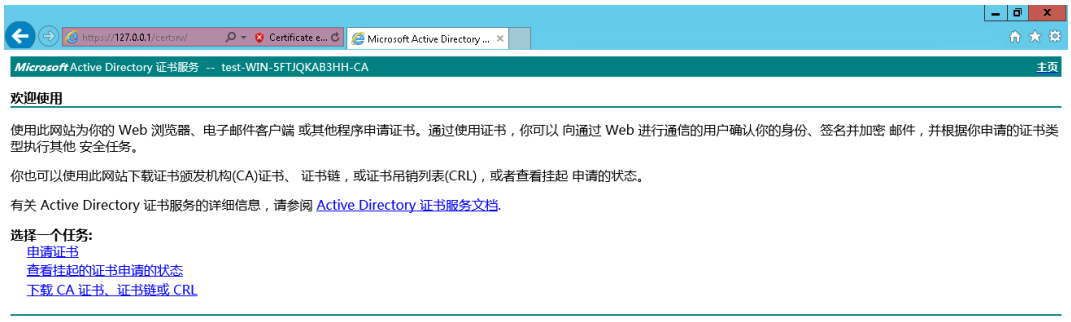
点击弹窗中的<Export>生成文件 ISE24MultiUse.pem，打开如下，复制全部内容。

图4-35 生成证书文件

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC6DCCAdACAQAwNDEXMBUGA1UEAxMOSVNFMjQudGVzdC5jb20xCzAJBgNVBAsT
AlJEMQwwCgYDVQQKEwNISEgwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQCuRjv3GeXTF8OgYj2JPT8iO6X7BUZodFGVsdVJ2+CUEXEMxAAnpXaMh8vVyqfm
mp8OjqZ60FG/AeyLNAVMAYLS5wE88xodpMmRPv8w1U1z0E7tUMvGAogTadme0Tt9
ne4my9LWMvCnsDMkPf7k+cnt1hQD+3hNZvY+BW8eykMimCTunQBdWWB4TKOv8Qvo
WDFLL3GsM/NAcjE+l6Tleq/m+8gaXEzjHq1W13d7V7UF3uK7HhiKW/Iw8o9JUpes
kaYV6oeHrxz8bQuwIuzdPBAjWY2/yfdopSrBKkv/BzAOXt/pjaaiFdECgkT9bxl0
Z9Na/2/L4jxRDfk9QYdlk7z3AgMBAAGgbzBtBgkqhkiG9w0BCQ4xYDBeMAsGA1Ud
DwQEAwIF4DAdBgNVHQ4EFgQU2jmj7l5rSw0yVb/vlWAYkK/YBwkwHQYDVR0lBBYw
FAYIKwYBBQUHAwEGCCsGAQUFBwMCMBEGCWCGSAGG+EIBAQQEAwIGQDANBgkqhkiG
9w0BAQsFAAOCAQEAUYeu6Zsg0lUaworPMjz85iVDeal8jiQrhn+MvNbs0YxtJwS2
JlA7yCf4dsOm06Zb7mLrQqLxrVs4eitqcoVICfQ5uIUxI2r+4USWYAnzFRiKoldS
G7mvBWoe7xOYB7OMyNI0E2i2YLujdBbgZmwPdyWXaCgKRVneI431vAjh6s58ZRMM
OtGNFBzIDKWXsXswHDeRCTtj7XbQVA7K5Ur0kJdWoTOMCCQoaoSjsPZ/vvWsmQIr
drJKxrt7XKqCHMOjay7tgwLXpXF9HWVy3DJ22F6umRJM3JpyeqPYUR/OoqUmEeDU
tf/GBCDaz6ZXxoxujT4jj6+V7jPZxzh0mmsOsQ==
-----END CERTIFICATE REQUEST-----
```

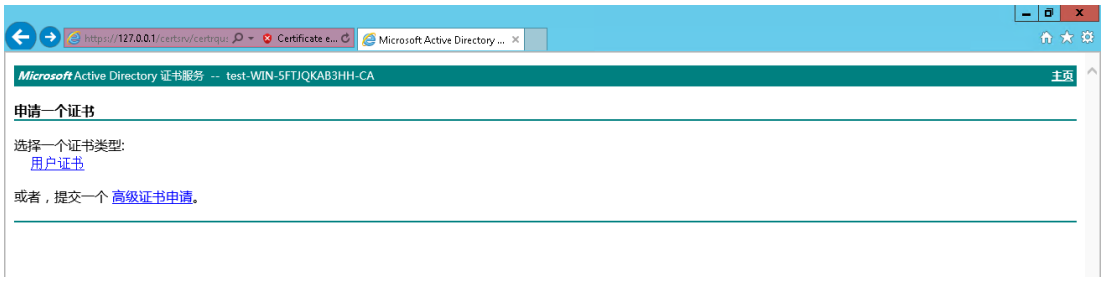
打开 Windows Server 证书服务 Web 界面，点击“申请证书”。

图4-36 申请证书



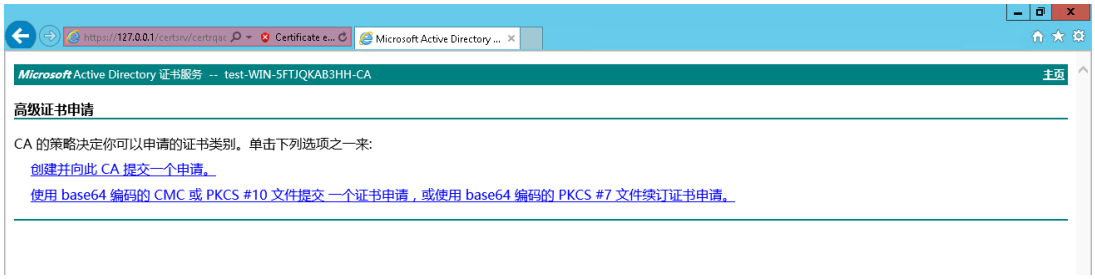
点击“高级证书申请”。

图4-37 申请高级证书



点击“使用 base64 编码的 CMC 或 PKCS #10 文件提交一个证书申请，或使用 base64 编码的 PKCS #7 文件续订证书申请”。

图4-38 申请证书类别

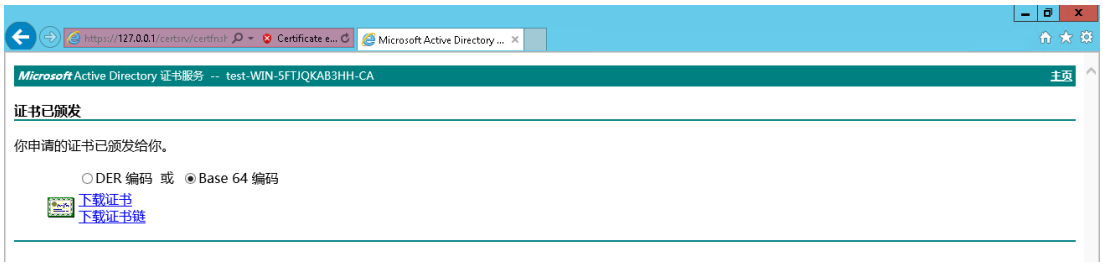


将刚复制的证书文件的内容粘贴到“保存的申请”下侧框内，选择“证书模板”，并点击<提交>。

图4-39 提交一个证书申请

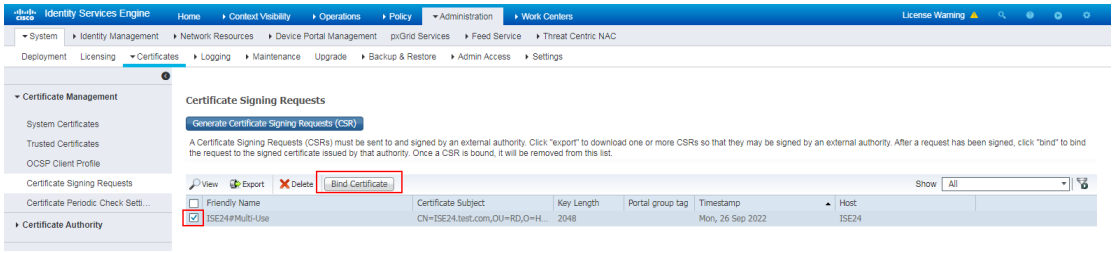
选择“Base 64 编码”，点击“下载证书”，并重命名为 certnew-server.cer。

图4-40 下载证书



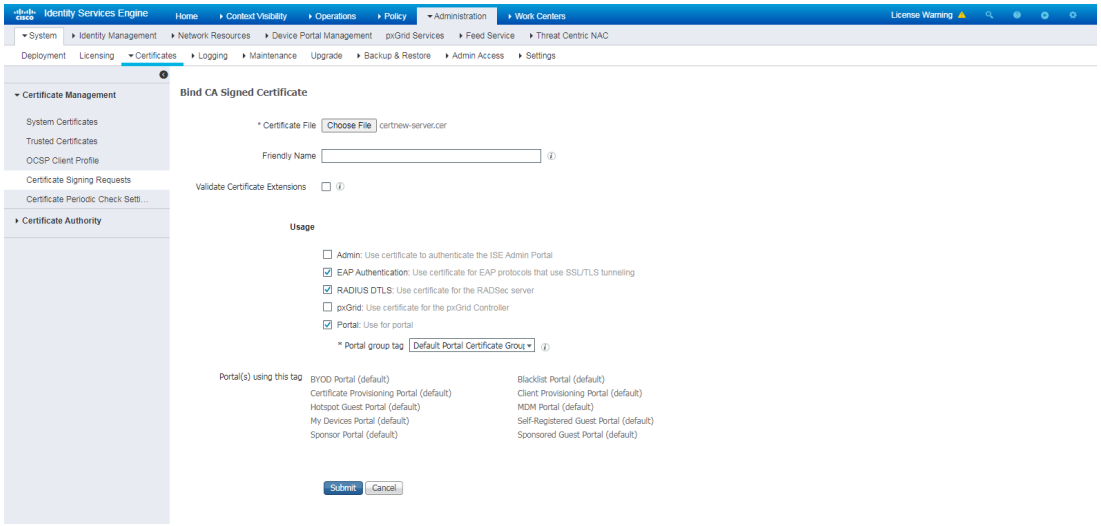
在 ISE 页面上方导航栏中选择[Administration/System/Certificates/Certificate Management/Certificate Siging Requests]选项，勾选刚才创建的 CSR，点击<Bind Certificate>绑定证书。

图4-41 绑定证书



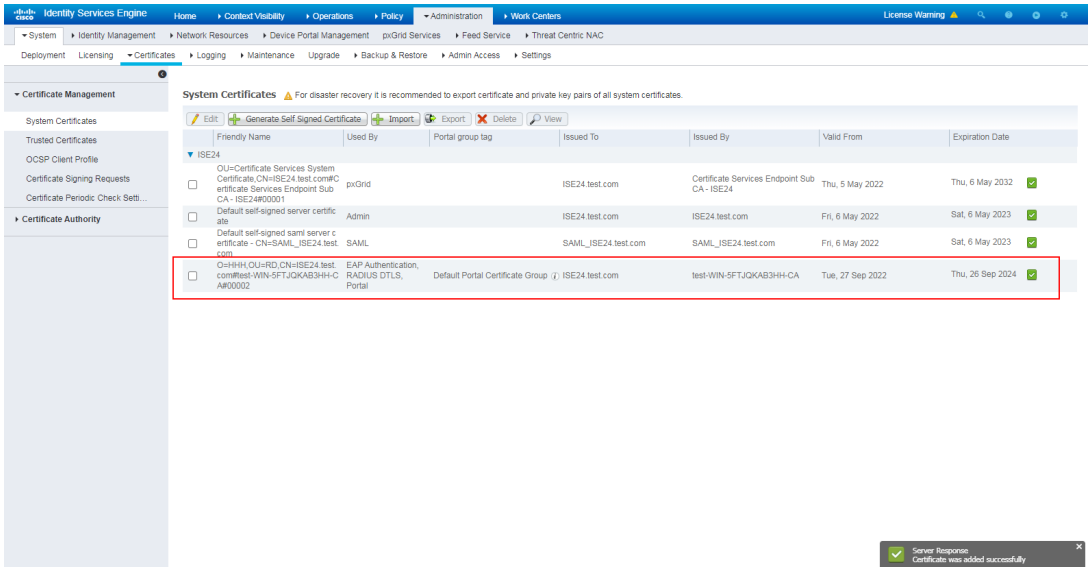
选择并上传之前下载的个人证书 certnew-server.cer，如图勾选“EAP Authentication”等，并点击<Submit>确认。

图4-42 选择并上传之前下载的个人证书



可以看到刚导入的个人证书如下图列表中的红框。

图4-43 查看导入的认证证书

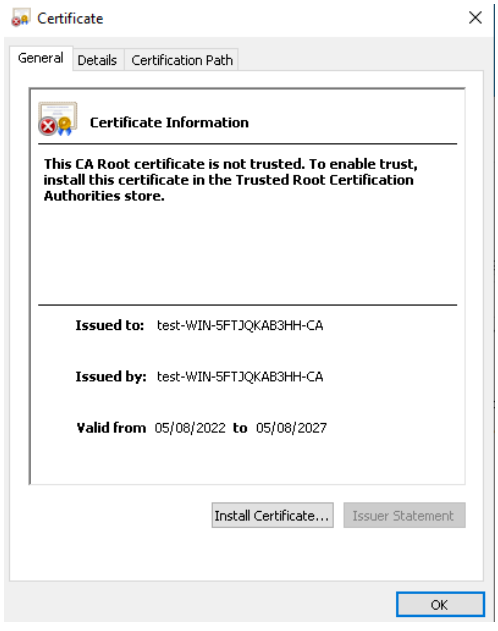


4.7.3 配置 Windows 客户端

(1) 安装根证书

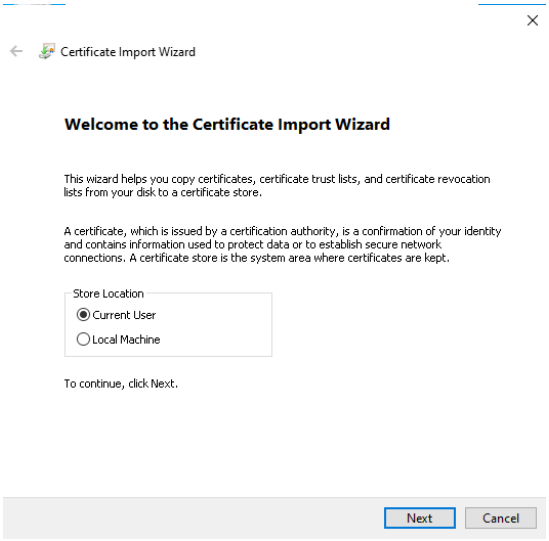
在 Windows 客户端中双击打开上一节下载的根证书 certnew-root.cer，点击<Install Certificate>安装证书。

图4-44 安装证书



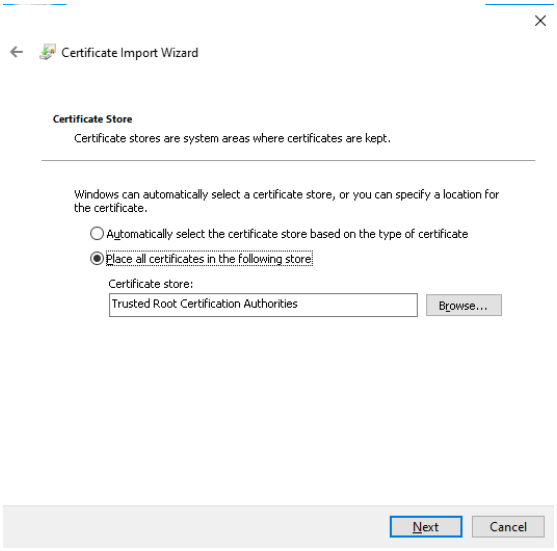
在向导页面中选择“Current User”，并点击<Next>。

图4-45 选择 Current User



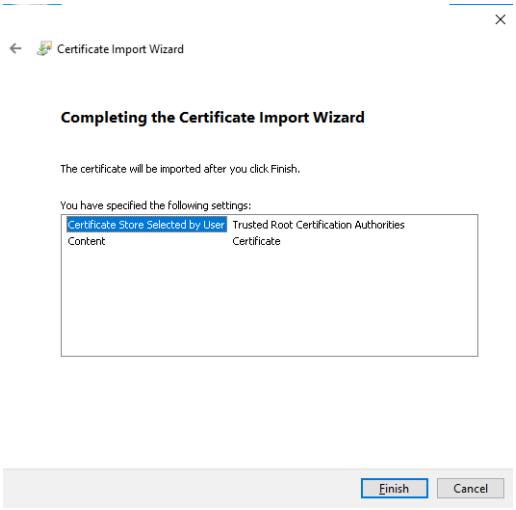
勾选“Place all cerfiticates in the following store”，并在“Cerfiticates store”中选择“Trusted Root Certification Authorities”， 点击<Next>。

图4-46 选择 Trusted Root Certification Authorities



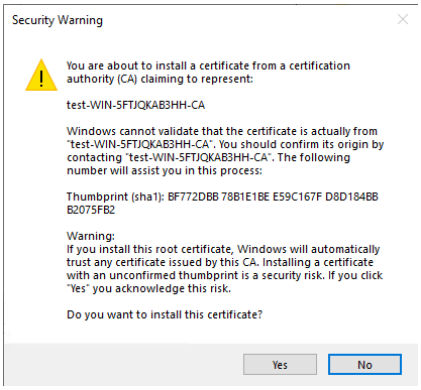
点击<Finish>。

图4-47 完成导入



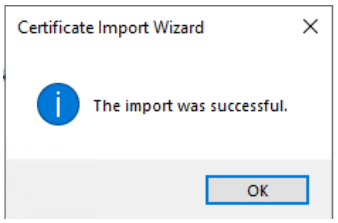
弹窗安全警告中选择<Yes>。

图4-48 安全警告



导入成功。

图4-49 导入证书成功



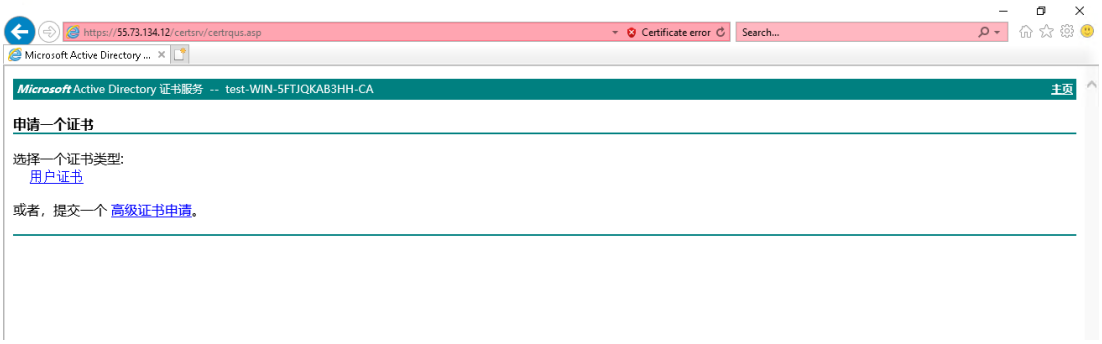
(2) 申请并安装用户证书

在 Windows 客户端上用 IE 浏览器打开 Windows Server CA 证书服务网址 https://IP/certsrv，点击“申请证书”。

图4-50 申请证书

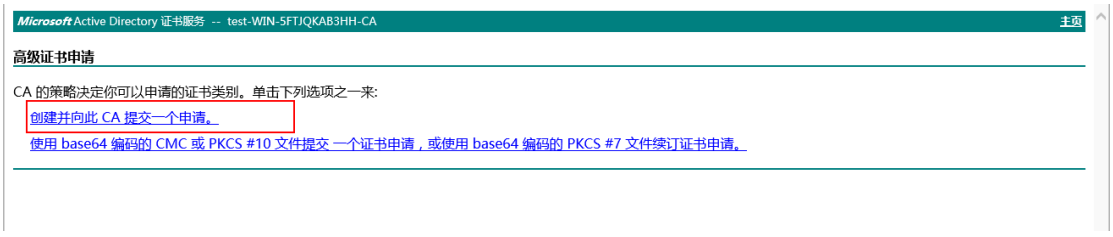
点击“高级证书申请”。

图4-51 提交高级证书申请



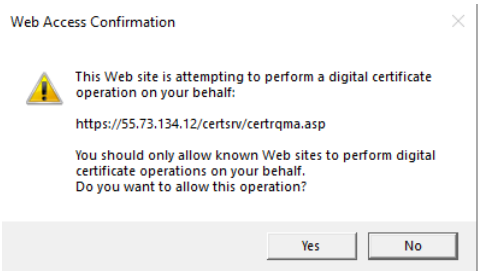
点击“创建并向此 CA 提交一个申请”。

图4-52 申请证书类别



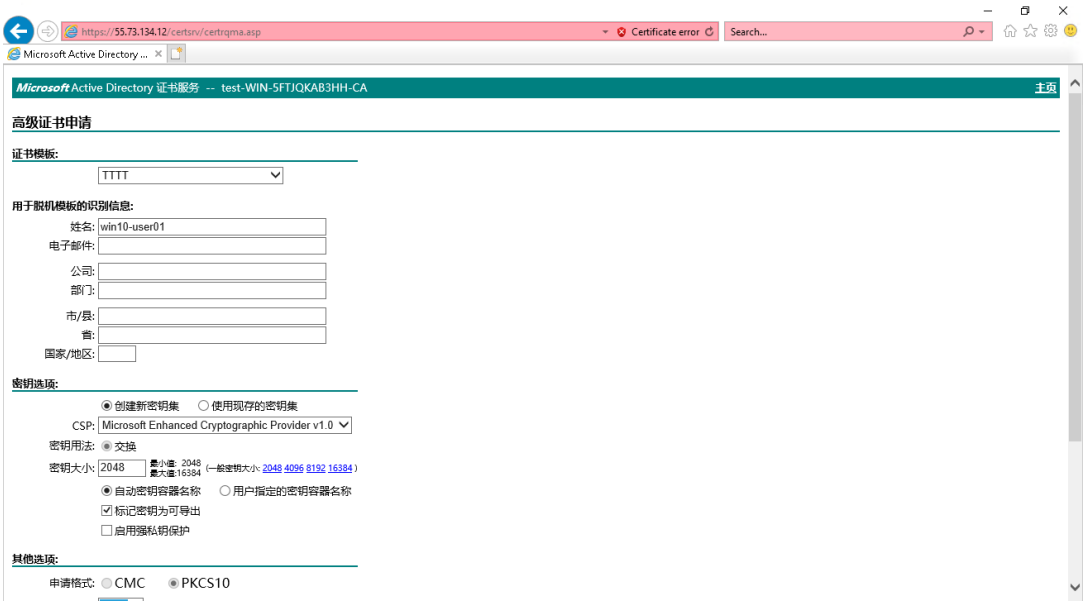
在弹窗中点击<Yes>。

图4-53 弹窗确认



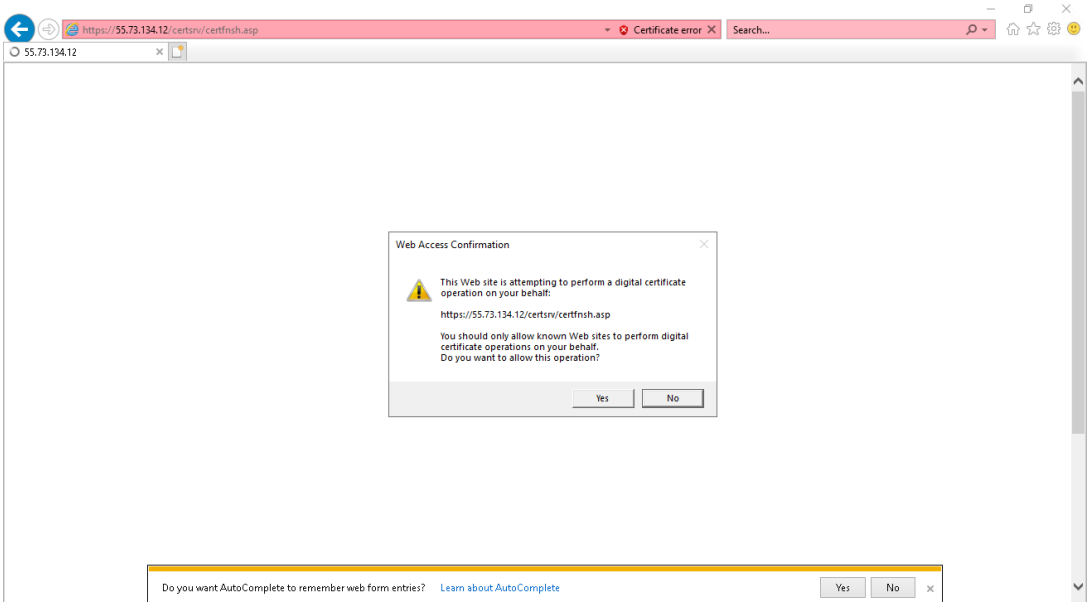
填写相关信息，并提交。

图4-54 高级证书申请



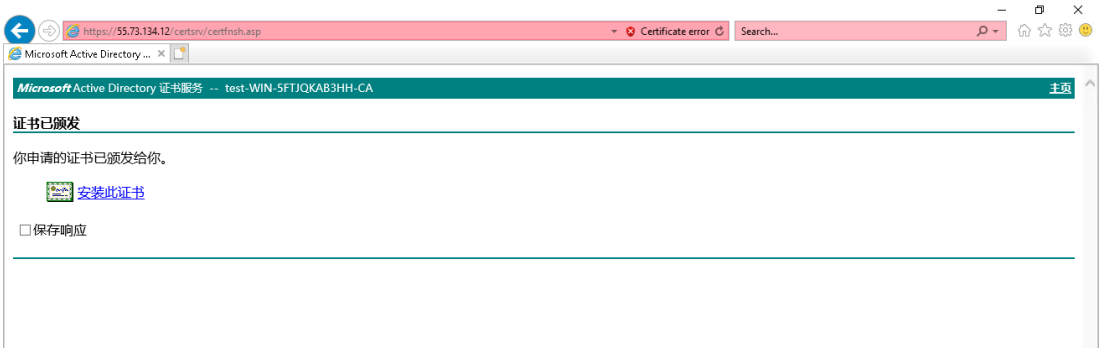
在弹窗中点击<Yes>。

图4-55 弹窗确认



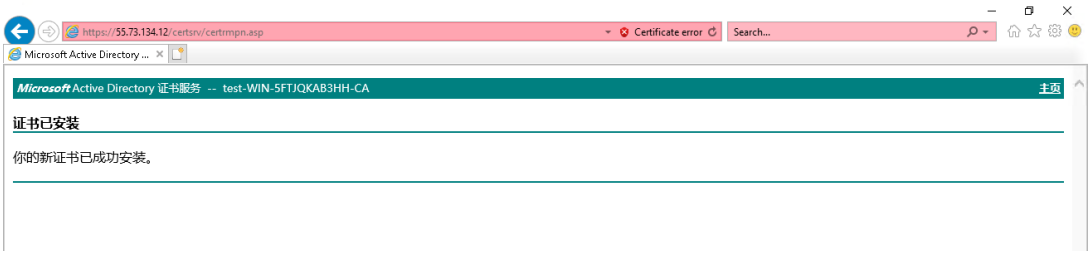
点击“安装此证书”。

图4-56 安装证书



证书安装成功。

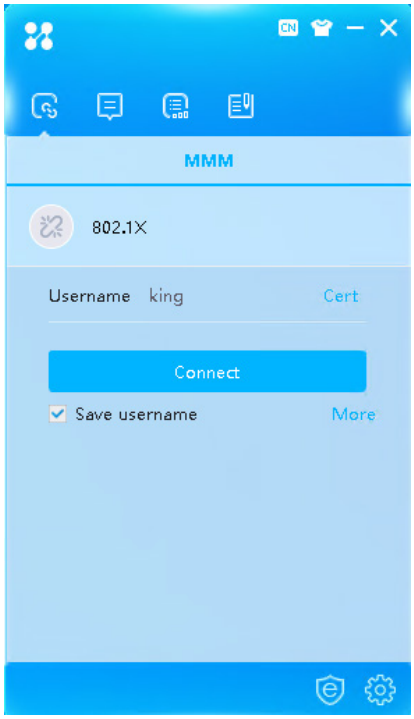
图4-57 成功安装证书



(3) 选择 iNode 客户端认证方式

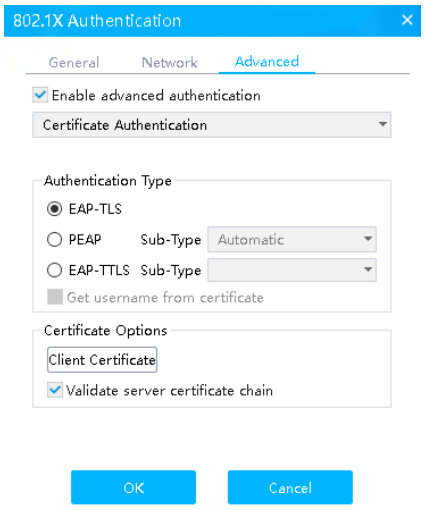
点击“More”，进入 802.1X 认证的属性页面。

图4-58 802.1X 客户端认证



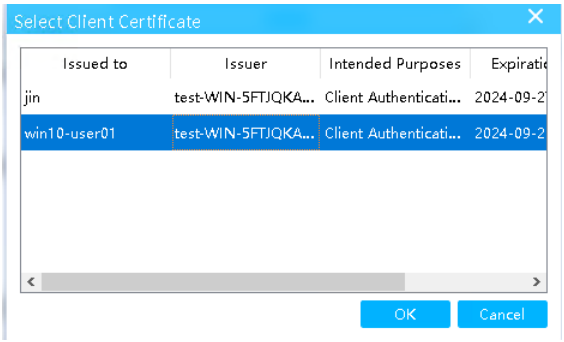
点击“Advanced”页签勾选“Enable advanced authentication”，选择“Authentication Type”为“EAP-TLS”，选择“Certificate Options”为“Client Certificate”。

图4-59 选择 EAP-TLS 认证方式



进入“Select Client Certificate”页面，选择之前导入的客户端证书，点击“OK”，完成客户端证书选择。

图4-60 选择客户端证书

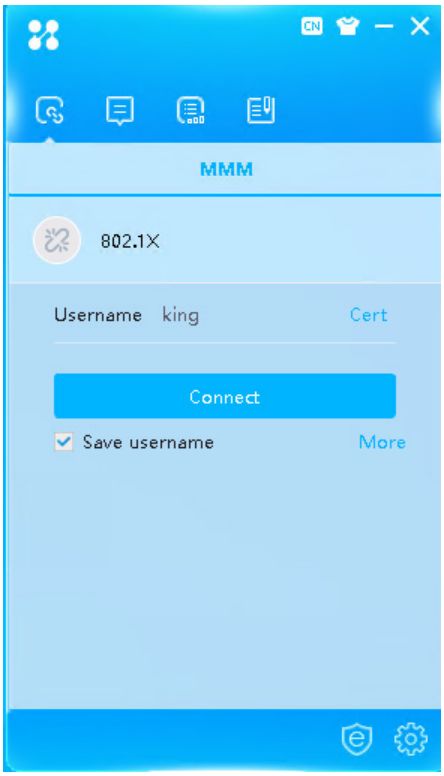


4.7.4 验证配置

(1) iNode 客户端登录上线

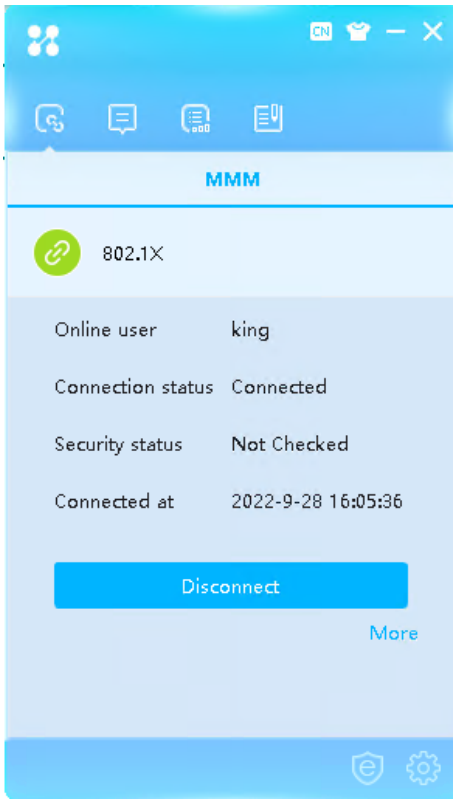
点击<Connect>，发起 802.1X 认证。

图4-61 点击 connect



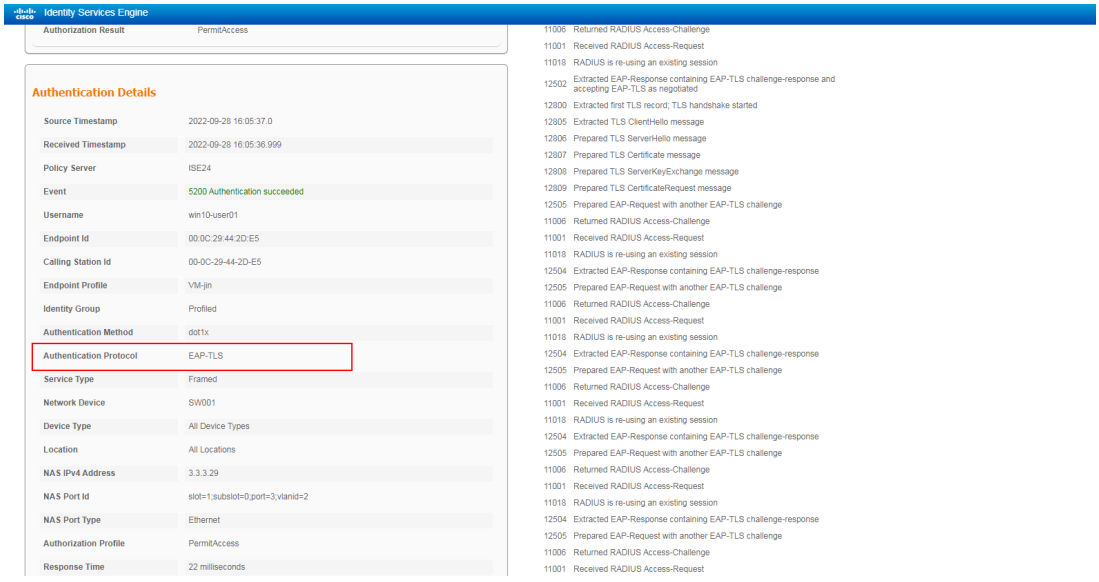
用户上线成功。

图4-62 上线成功



(2) 用户上线后服务器显示

图4-63 EAP-TLS 认证方式上线后服务器显示



(3) 用户上线后设备显示

在设备上通过 **`display dot1x connection`** 可以查看 802.1X 用户的信息，可其中 Username 为 802.1X 的用户名（本例为 king）。

```
<Switch> display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 000c-2944-2de5
Access interface: GigabitEthernet1/0/3
Username: king
User access state: Successful
Authentication domain: ise
IPv4 address: 2.2.2.10
IPv4 address source: IP Source Guard
EAP packet identifier: 227
Authentication method: EAP
AAA authentication method: RADIUS
Initial VLAN: 2
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Authorization IPv6 URL: N/A
Authorization temporary redirect: Disabled
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: N/A
Online from: 2022/09/28 15:17:15
Online duration: 0h 0m 7s
```

4.7.5 配置文件

```
#
 dot1x
 dot1x authentication-method eap
#
vlan 1
#
vlan 2
 description toClients
 arp snooping enable
#
vlan 3
 description toAAAserver
#
interface Vlan-interface1
#
```

```
interface Vlan-interface2
 description toClients
 ip address 2.2.2.29 255.255.255.0
#
interface Vlan-interface3
 description toAAAservers
 ip address 3.3.3.29 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 2
 dot1x
#
radius scheme ise
 primary authentication 3.3.3.24 key cipher $c$3$2oLOvHdRilTBlb6n1yh3/MoXN8z/RMbctQ==
 primary accounting 3.3.3.24 key cipher $c$3$fAhWH/rHm9hCcPq2PBWQa54YG9xKuQ1P0w==
 timer realtime-accounting 20 second
 user-name-format keep-original
#
#
domain test.com
 authentication default radius-scheme ise
 authorization default radius-scheme ise
 accounting default radius-scheme ise
#
```

4.8 802.1X EAP-FAST认证配置步骤与验证

4.8.1 配置 Switch

设备上确认认证方式为 EAP。

```
[Switch] dot1x authentication-method EAP
```

建议在交换机连接客户端的对应接口上关闭 802.1X 的组播触发功能和在线用户握手功能。

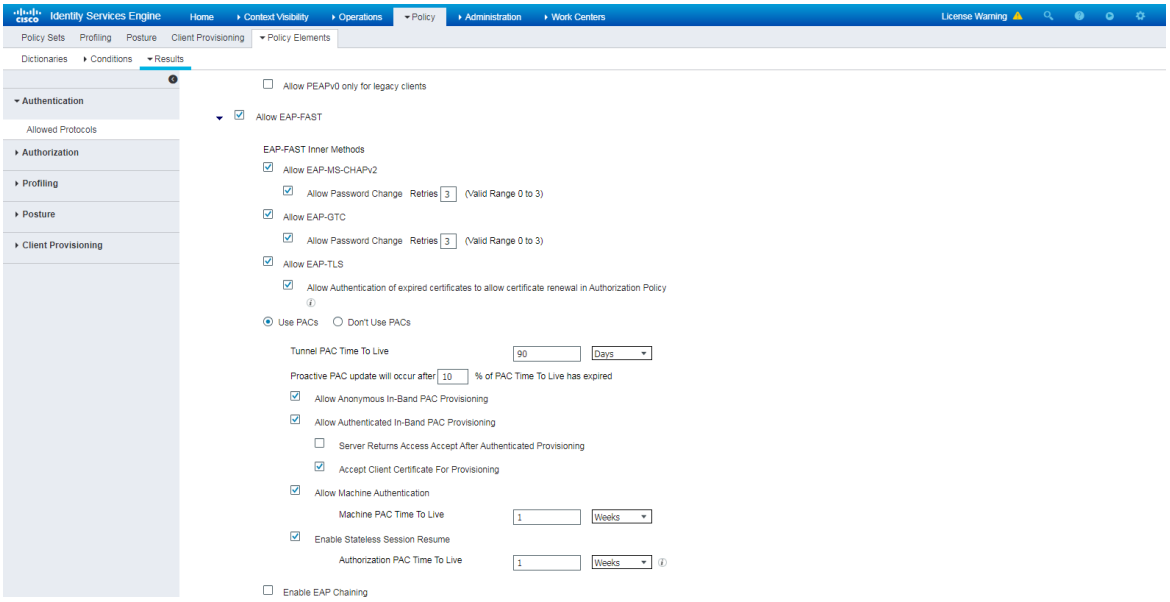
```
[Switch-GigabitEthernet1/0/3]undo dot1x handshake
[Switch-GigabitEthernet1/0/3]undo dot1x multicast-trigger
```

其它配置无需修改，具体请参考 4.3.1 配置 Switch。

4.8.2 配置 ISE

服务器上确认 Allowed Protocols 勾选 Allow EAP-FAST 相关选项，请参考 4.3.2 配置 ISE。

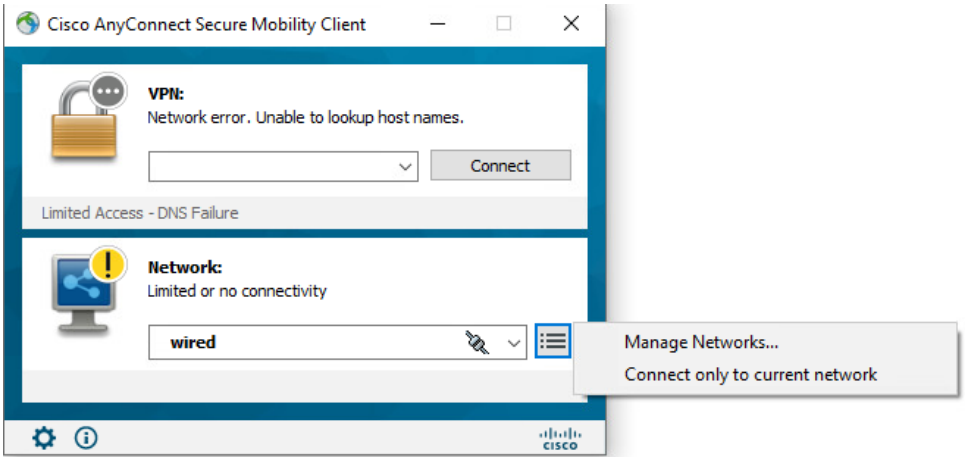
图4-64 确认勾选 Allow EAP-FAST 相关选项



4.8.3 配置 Cisco AnyConnect 客户端

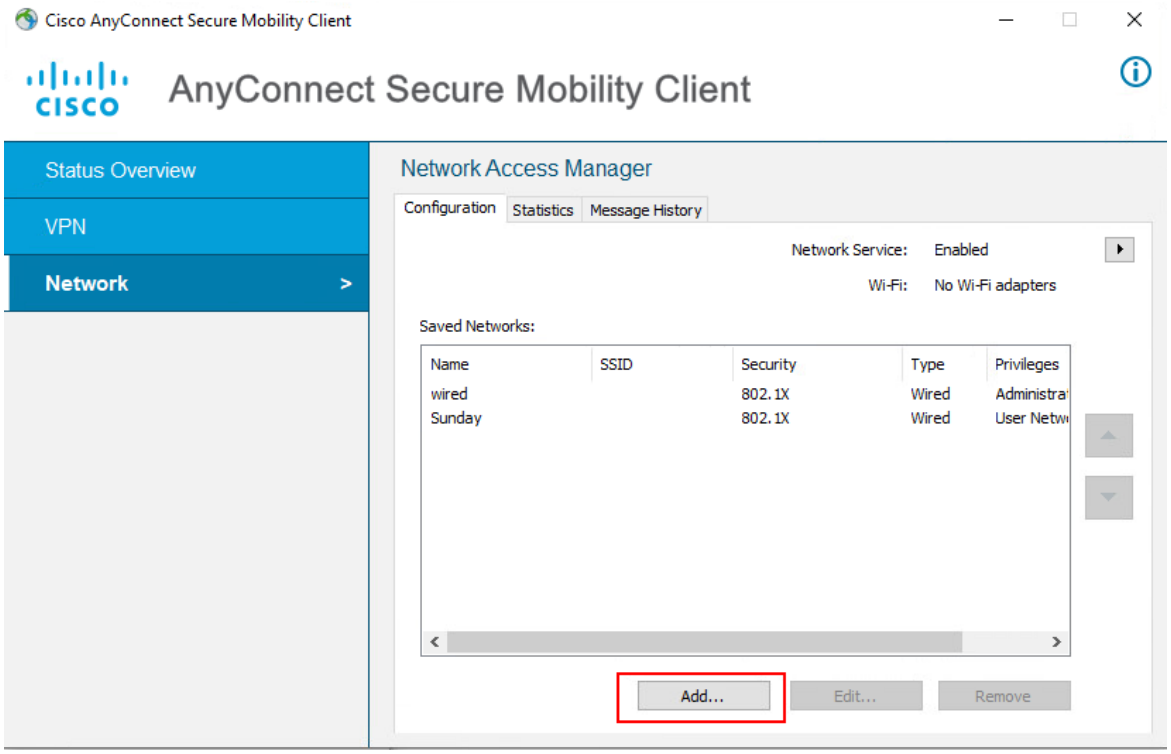
以 predeploy 或者 webdeploy 方式安装 Cisco AnyConnect 客户端，webdeploy 方式可以参考下图中选中“Network”为“wired”，并选择“Manage Networks”。

图4-65 选择有线连接



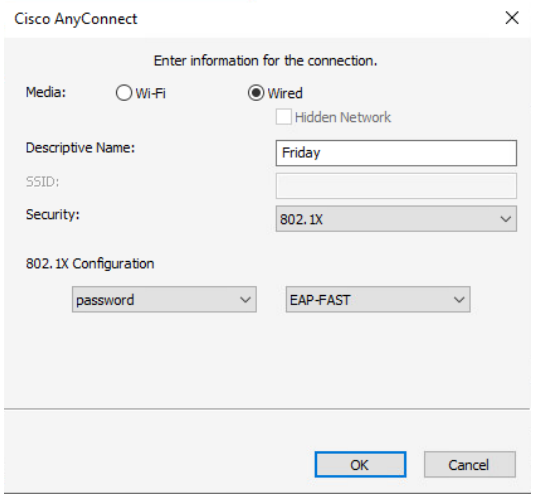
弹窗中点击<Add>。

图4-66 添加 Cisco AnyConnect 客户端



弹窗中填写相关信息。

图4-67 配置 Cisco AnyConnect 客户端

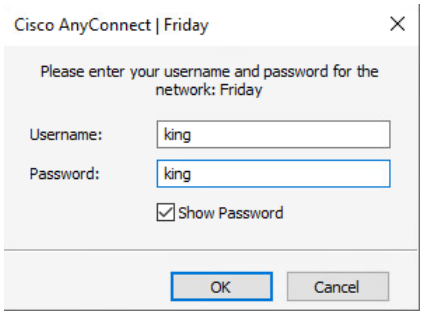


4.8.4 验证配置

(1) 客户端连接

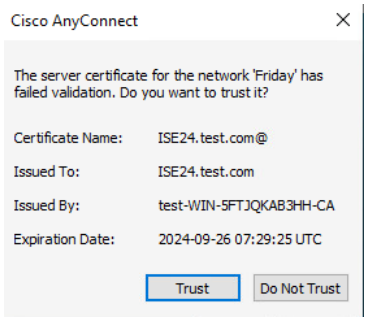
连接之前创建的 network，填写用户名密码，点击<OK>。

图4-68 客户端发起连接



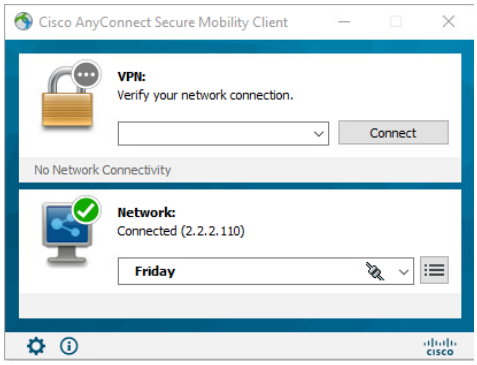
弹窗中点击<Trust>。

图4-69 弹窗选择信任



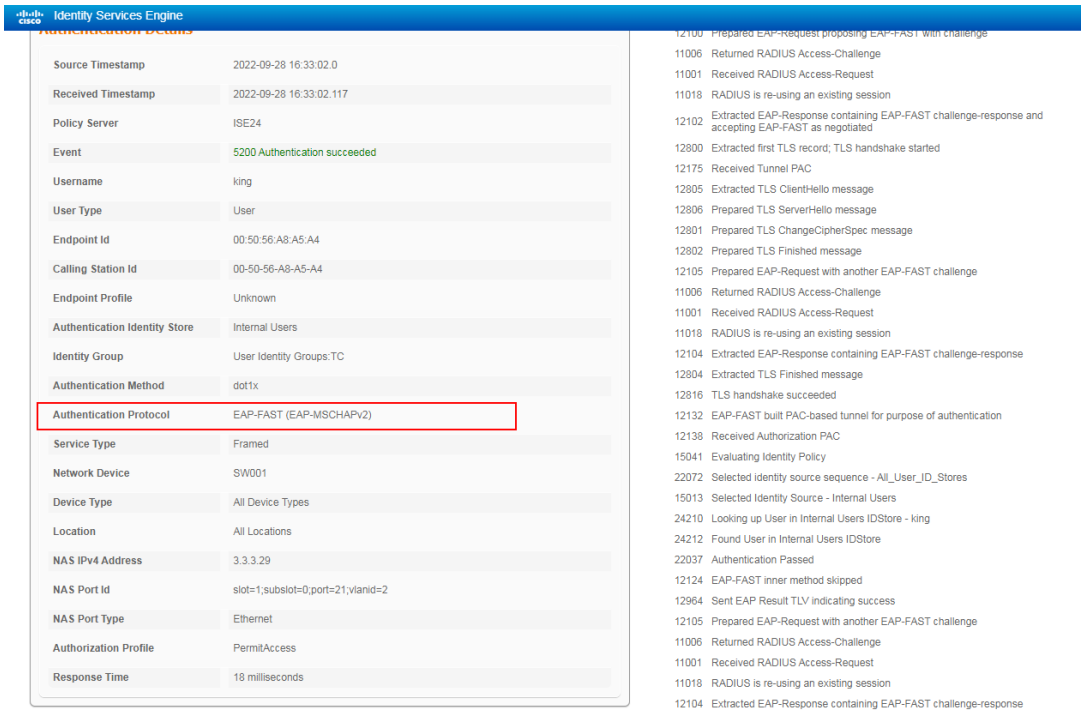
连接成功。

图4-70 成功连接



(2) 用户上线后服务器显示情况

图4-71 用户上线后服务器显示



(3) 用户上线后设备显示

在设备上通过 **display dot1x connection** 可以查看 802.1X 用户的信息，可其中 Username 为 802.1X 的用户名（本例为 king）。

```
<Switch> display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 000c-2944-2de5
Access interface: GigabitEthernet1/0/3
Username: king
User access state: Successful
Authentication domain: ise
IPv4 address: 2.2.2.10
IPv4 address source: IP Source Guard
EAP packet identifier: 227
Authentication method: EAP
AAA authentication method: RADIUS
Initial VLAN: 2
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
```

```
     Authorization IPv6 URL: N/A
     Authorization temporary redirect: Disabled
     Start accounting: Successful
     Real-time accounting-update failures: 0
     Termination action: Default
     Session timeout period: N/A
     Online from: 2022/09/28 15:17:15
     Online duration: 0h 0m 7s
```

4.8.5 配置文件

```
#
 dot1x
 dot1x authentication-method eap
#
vlan 1
#
vlan 2
 description toClients
 arp snooping enable
#
vlan 3
 description toAAAserver
#
interface Vlan-interface1
#
interface Vlan-interface2
 description toClients
 ip address 2.2.2.29 255.255.255.0
#
interface Vlan-interface3
 description toAAAservers
 ip address 3.3.3.29 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 2
 dot1x
 undo dot1x handshake
 undo dot1x multicast-trigger
#
#
radius scheme ise
 primary authentication 3.3.3.24 key cipher $c$3$2oLOvHdRilTBlb6n1yh3/MoXN8z/RMbctQ==
 primary accounting 3.3.3.24 key cipher $c$3$fAhWH/rHm9hCcPq2PBWQa54YG9xKuQ1P0w==
```

```
 timer realtime-accounting 20 second
 user-name-format keep-original
#
#
domain test.com
 authentication default radius-scheme ise
 authorization default radius-scheme ise
 accounting default radius-scheme ise
#
```

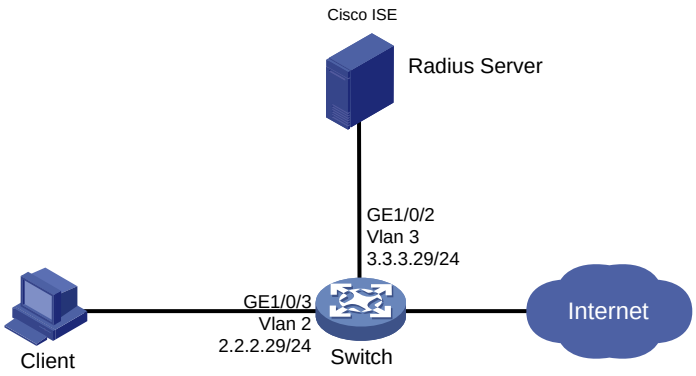
5 MAC 地址认证对接配置举例

5.1 组网需求

如图 5-1 所示，Client 和 ISE 服务器通过 Switch 建立连接，设备管理员希望对 Client 进行 MAC 地址认证，以控制其对网络资源的访问，具体要求如下：

- 采用 Cisco ISE 作为 RADIUS 服务器。
- 配置 MAC 地址认证的用户名和密码。

图5-1 MAC 认证配置组网图



5.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch：S5560X-R6618P27
- 认证服务器: Cisco ISE V2.4.0.357 patch 8
- 系统：Windows 10 21H2
- 认证客户端：iNode PC 7.3 (E513)

5.3 MAC地址认证配置步骤与验证

说明

本配置仅展示认证的相关配置，网络互通的相关配置略，请保证设备间能够互相访问。

5.3.1 配置 Switch

将端口 GE1/0/3 加入到指定的 VLAN，并开启 MAC 地址认证功能。

```
[Switch-GigabitEthernet1/0/3] port access vlan 2
[Switch-GigabitEthernet1/0/3] MAC-authentication
[Switch-GigabitEthernet1/0/3] quit
```

指定 MAC 地址认证用户的认证域 test.com。

```
[Switch] MAC-authentication domain test.com
```

配置 MAC 地址认证所使用的的用户名密码格式，ise 上所加的用户需与此处保持一致。缺省情况下，使用用户的 MAC 地址作为用户名与密码，其中字母为小写，且不带连字符。

```
[Switch] mac-authentication user-name-format mac-address with-hyphen uppercase
```

开启全局 MAC 地址认证，缺省情况下，设备采用 PAP 认证方法进行 MAC 地址认证。

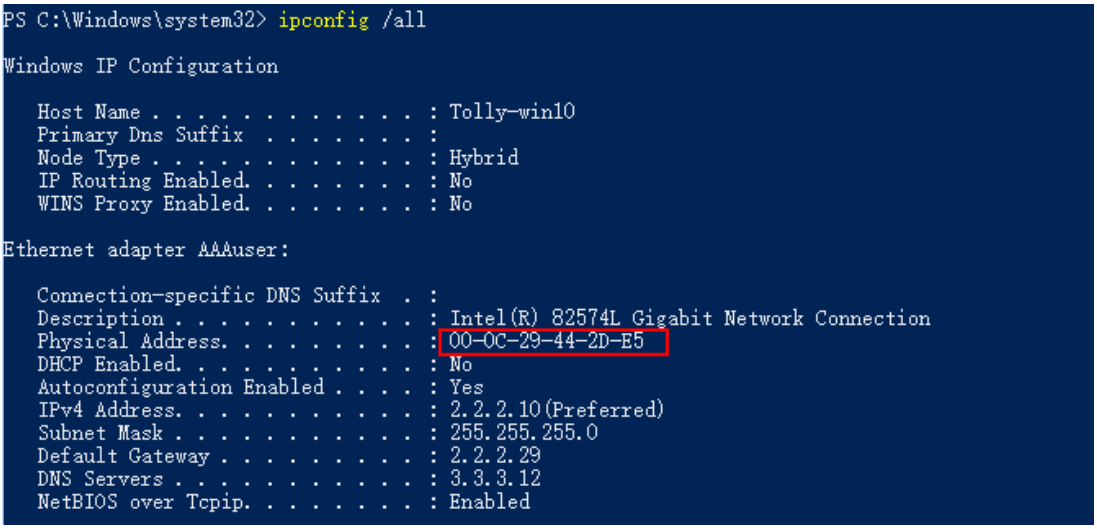
```
[Switch] MAC-authentication
```

5.3.2 配置 ISE

(1) 查看终端信息

查看终端 Windows 连接交换机的物理口的 MAC 地址。

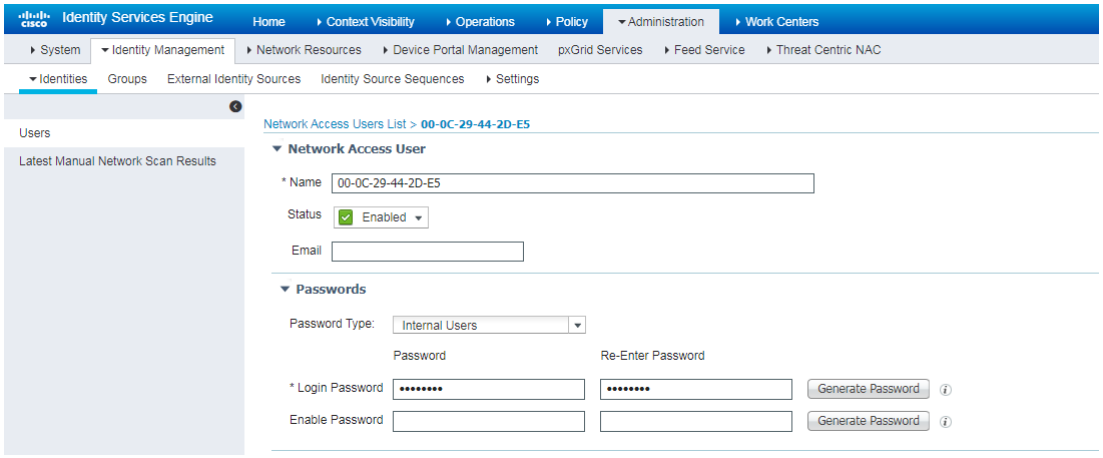
图5-2 查看终端 mac 地址



(2) 创建用户账号

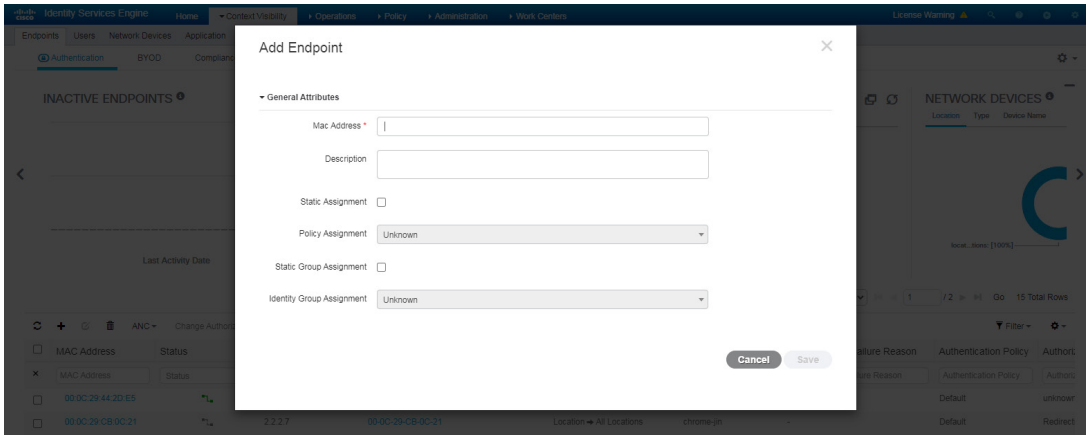
在ISE页面上方导航栏中选择[Administration/Identity Management/Identities/Users]选项，点击<Add>按钮，创建名称为 00-0C-29-44-2D-E5 的用户账号，配置密码为 00-0C-29-44-2D-E5。

图5-3 创建用户



注意，也可以在 Endpoint 中添加需要认证的终端，本文档不以此种情况举例，可参考下图。

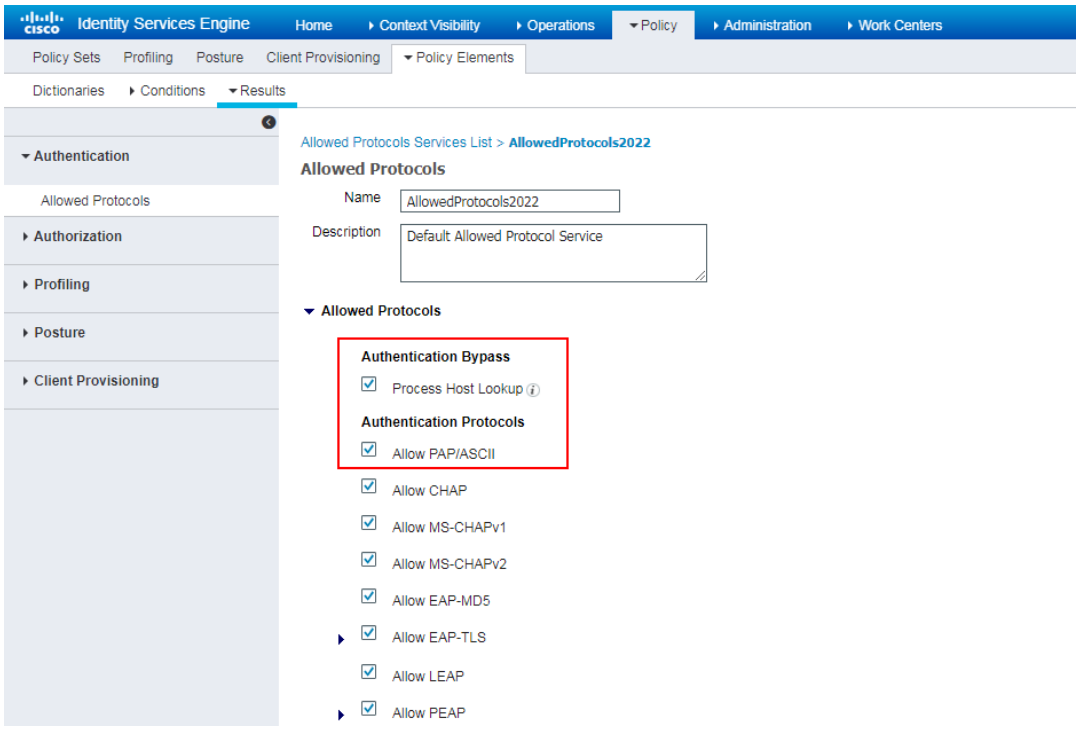
图5-4 Add Endpoint



(3) 配置认证协议

在 ISE 页面上方导航栏中选择[Policy/Policy Elements/Results/Authentication/Allowed Protocols]选项，新建名称为 AllowedProtocols2022 的 allowed protocols。在 Authentication Bypass 栏中勾选 Process Host Lookup 选项，在 Authentication Protocols 栏中确认勾选 PAP/ASCII 选项。

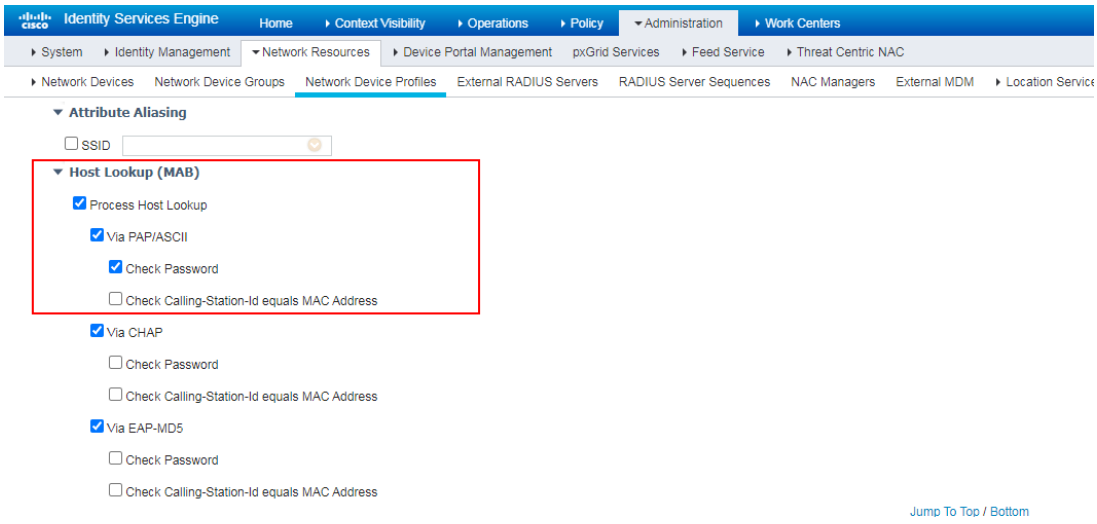
图5-5 配置认证协议



(4) 配置 Network Switch Profile

复制 Cisco Network Switch Profiles，并参考下图修改，勾选 Check Password 提升安全性。

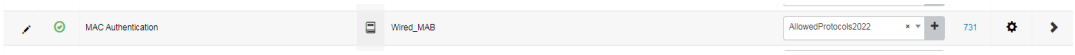
图5-6 配置 Network Switch Profile



(5) 配置认证和授权策略

在 ISE 页面上方导航栏中选择[Policy/Policy Sets]选项，点击 Policy Sets 下方的<+>按钮，配置名称 MAC Authentication 的认证和授权策略，并配置 Conditions 为 Wired_MAB。

图5-7 新建认证和授权策略

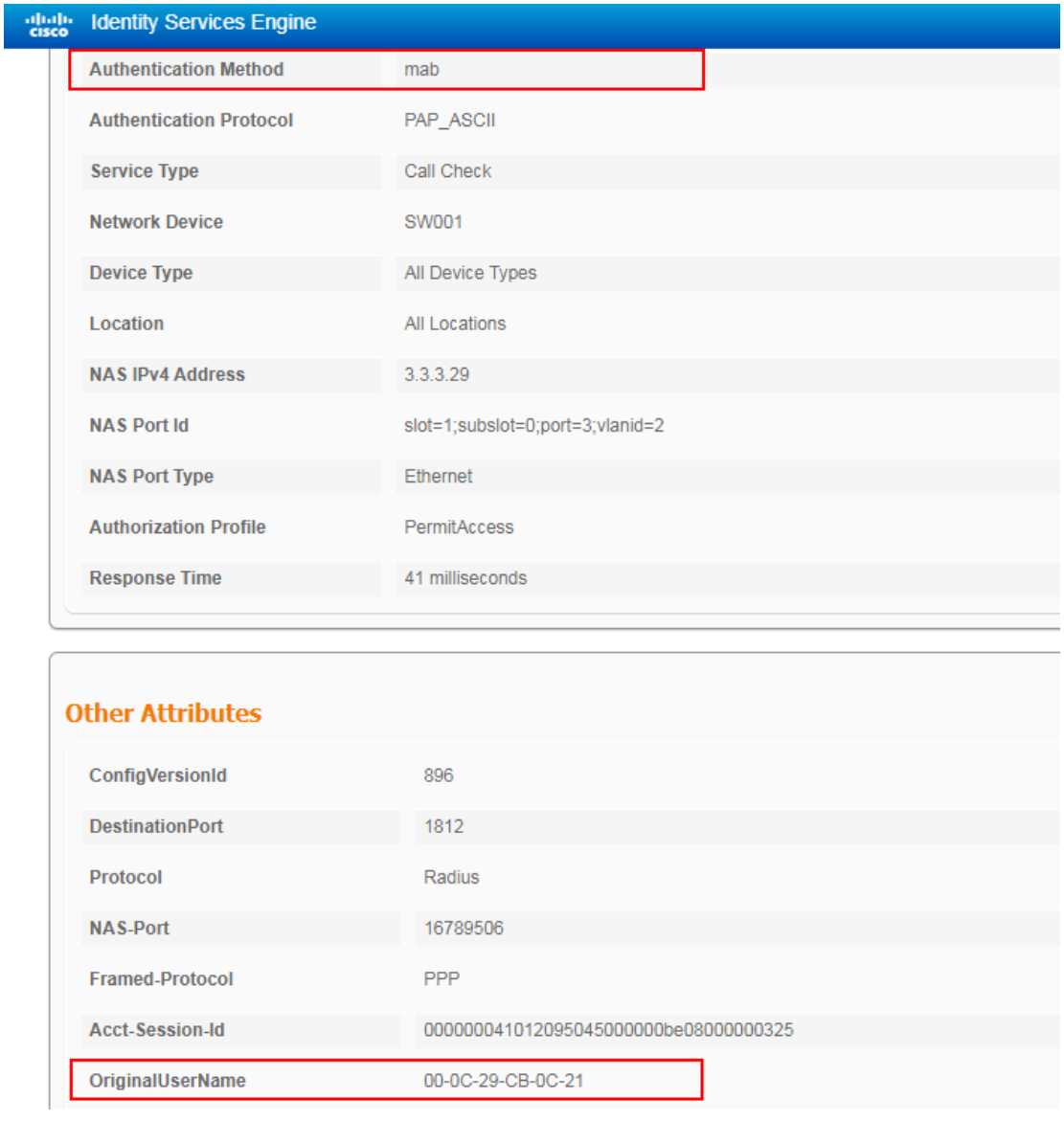


5.3.3 验证配置

(1) 用户上线后服务器显示情况

在设备和服务器都配置好的情况下，在客户端 Ping 服务器即可完成用户上线。

图5-8 用户上线后服务器显示



(2) 用户上线后设备的显示信息

通过在设备上执行 **display mac-authentication connection** 可以看到上线用户的信息。

```
<Switch> display mac-authentication connection
Total connections: 1
Slot ID: 1
User MAC address: 000c-2944-2de5
Access interface: GigabitEthernet1/0/3
Username: 00-0C-29-44-2D-E5
User access state: Successful
Authentication domain: test.com
IPv4 address: 2.2.2.10
IPv4 address source: IP Source Guard
Initial VLAN: 2
Authorization untagged VLAN: N/A
Authorization tagged VLAN: N/A
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Authorization IPv6 URL: N/A
Authorization temporary redirect: Disabled
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: N/A
Offline detection: 300 sec (command-configured)
Online from: 2022/10/12 17:48:35
Online duration: 0h 8m 9s
Port-down keep online: Disabled (offline)
```

5.4 配置文件

```
#
 mac-authentication domain test.com
 mac-authentication user-name-format mac-address with-hyphen uppercase
#
#
vlan 2
 description toClients
 arp snooping enable
#
vlan 3
 description toAAAserver
#
interface Vlan-interface2
 description toClients
 ip address 2.2.2.29 255.255.255.0
```

```
#
interface Vlan-interface3
 description toAAAservers
 ip address 3.3.3.29 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 2
MAC-authentication
#
radius scheme ise
 primary authentication 3.3.3.24 key cipher $c$3$2oLOvHdRilTBlb6n1yh3/MoXN8z/RMbctQ==
 primary accounting 3.3.3.24 key cipher $c$3$fAhWH/rHm9hCcPq2PBWQa54YG9xKuQ1P0w==
 user-name-format keep-original
#
#
domain test.com
 authentication default radius-scheme ise
 authorization default radius-scheme ise
 accounting default radius-scheme ise
#
```

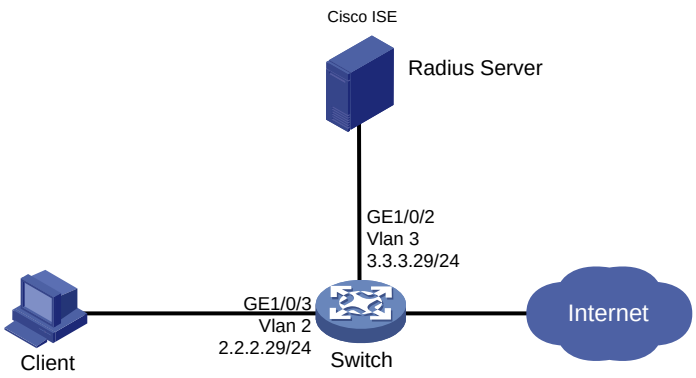
6 Portal 认证对接配置举例

以 CWA(Centralized Web Authentication)为例。

6.1 组网需求

如图 6-1 所示，Client 和 ISE 服务器通过 Switch 建立连接，设备管理员希望对 Client 进行 Portal 认证，以控制其对网络资源的访问，具体要求：采用 ISE 作为 RADIUS 服务器和 Portal 服务器。

图6-1 Portal 认证配置组网图



6.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch：S5560X-R6618P27
- 认证服务器: Cisco ISE V2.4.0.357 patch 8
- 系统：Windows 10 21H2
- 认证客户端：iNode PC 7.3 (E513)

6.3 配置步骤

说明

本配置仅展示认证的相关配置，网络互通的相关配置略，请保证设备间能够互相访问。

6.3.1 配置 Switch

配置 ACL，使得终端只能访问 CWA、DNS 服务器等必要地址。

```
[Switch]acl number 3000
[Switch-acl-ipv4-adv-3000]dis th
#
acl advanced 3000
 rule 0 permit ip destination 3.3.3.24 0
 rule 2 permit ip destination 3.3.3.12 0
 rule 6 permit ip destination 2.2.2.0 0.0.0.255
#
Return
```

CWA 以 MAC 地址认证为基础，相关内容请参考 MAC 地址认证相关章节。

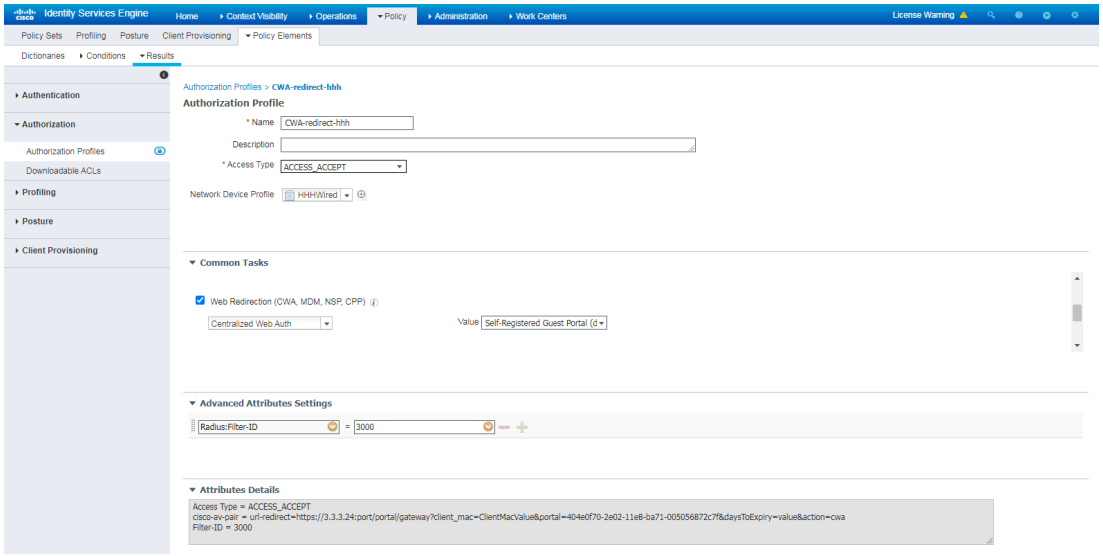
6.3.2 配置 ISE

CWA 以 MAC 地址认证为基础，相关内容请参考 MAC 地址认证相关章节。

(1) 创建 Authorization Profile

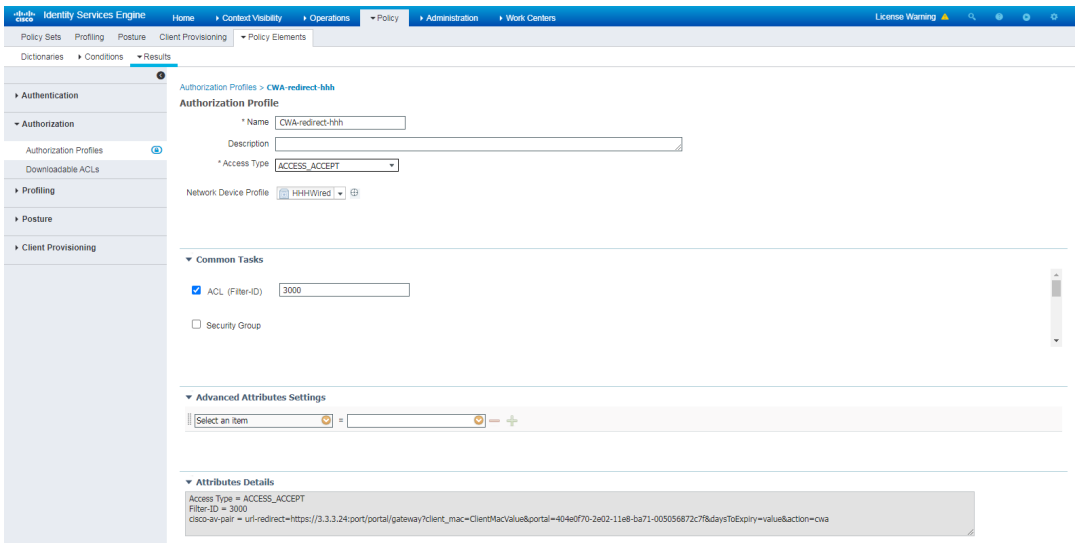
在 ISE 页面上方导航栏中选择[Policy/Policy Elements/Results/Authorization/Authorization Profiles]选项，新建 Authorization Profile，命名为 CWA-redirect-hhh，勾选 Web Redirection (CWA, MDM, NSP, CPP)，选择 Centralized Web Auth。

图6-2 新建 Authorization Profile



勾选并填入将与终端关联的 ACL 3000。

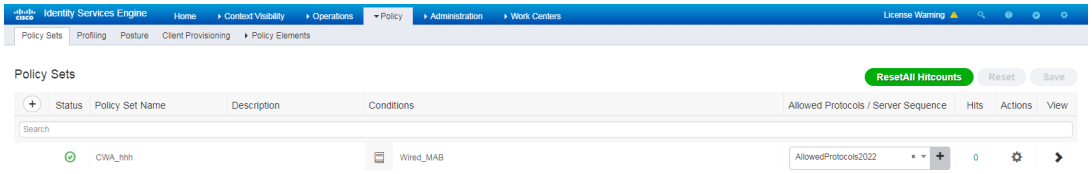
图6-3 填写 ACL



(2) 创建 Policy Set

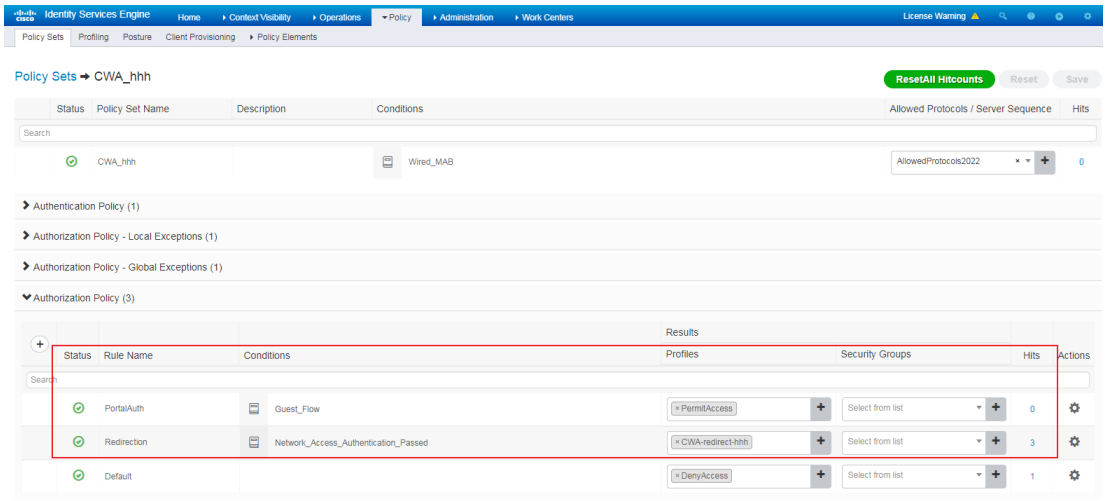
在 ISE 页面上方导航栏中选择[Policy/Policy Sets]选项，新建一个 Policy Set 命名为 CWA_hhh，Conditions 选择 Wired_MAB。

图6-4 创建 Policy Set



点击 Authorization Policy 下方的<＋>按钮，新建 2 个 Authorization Policy，Redirection 用于终端打开页面重定向到 CWA 页面，PortalAuth 用于在 CWA 页面输入用户名密码，认证通过后，拿到新的授权。

图6-5 新建 Authorization Policy

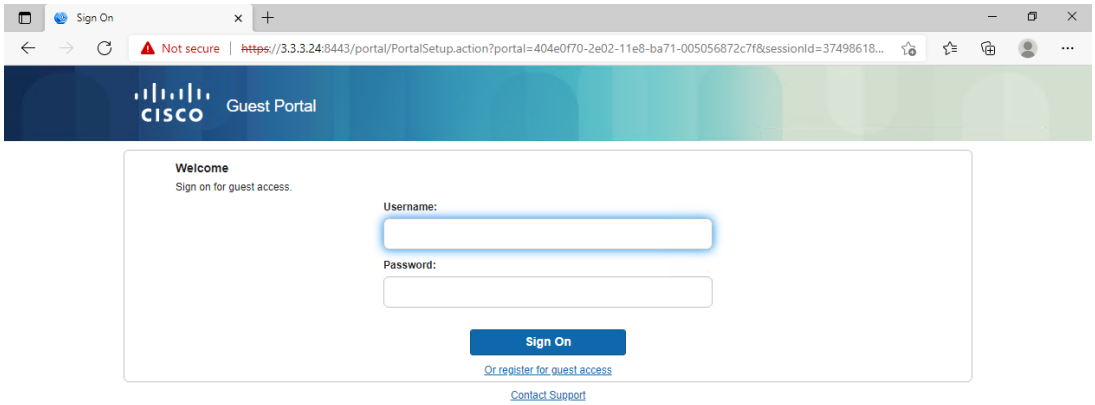


6.3.3 效果展示

(1) 重定向到 CWA 页面

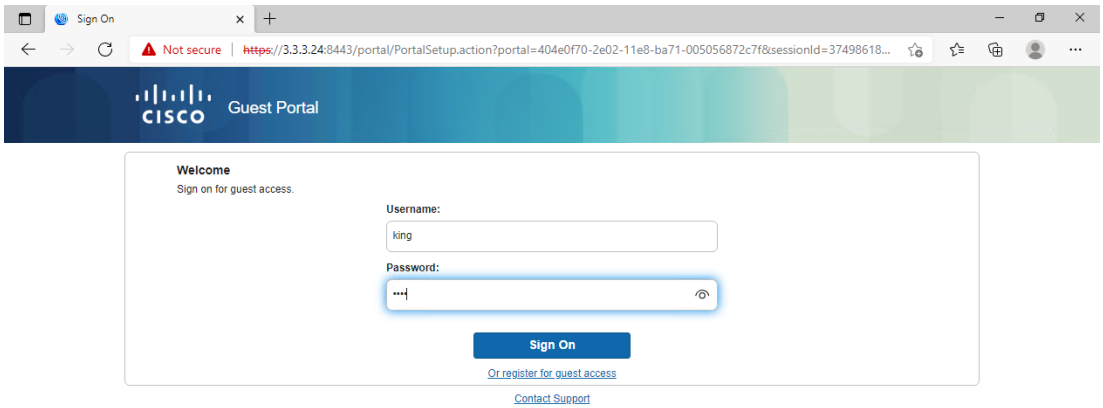
终端打开浏览器，随机访问页面，被重定向到 CWA 页面。

图6-6 重定向到 CWA 页面



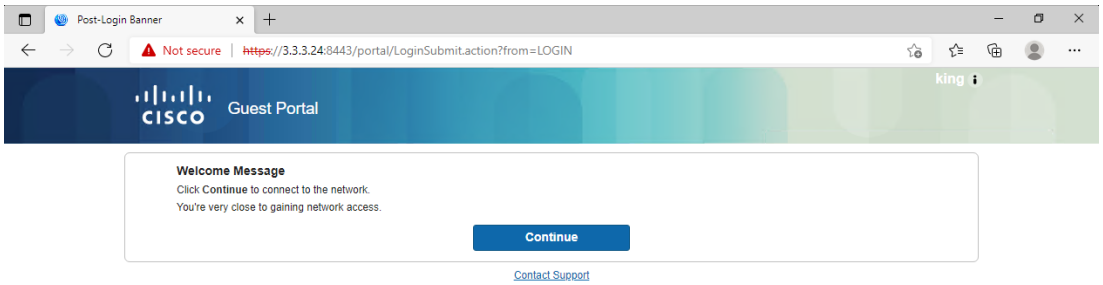
输入用户名密码，点击<Sign On>。

图6-7 输入用户名密码



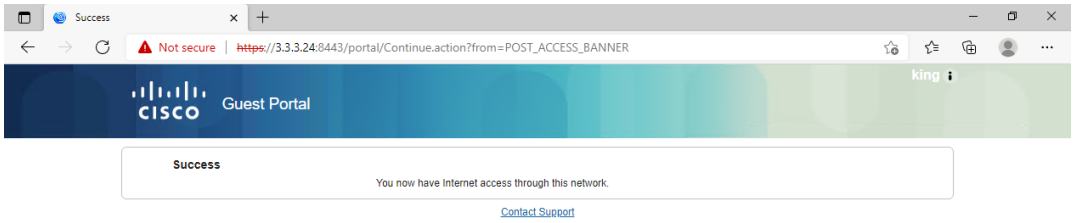
点击<Continue>。

图6-8 点击继续



(2) 通过认证

图6-9 通过认证



(3) 交换机上显示情况

交换机上 **display mac-authentication connection** 可以看到 ISE 下发的授权情况，上面的连接为之前已经通过 CWA 页面认证的连接，没有特殊的网络限制。下面的连接为另一个终端，在 CWA 认证前，通过 MAC 地址认证，拿到了 CWA 页面及 ACL 授权。

图6-10 交换机上显示

```
[Device]dis mac-authentication connection
Total connections: 2
Slot ID: 1
User MAC address: 000c-295b-8151
Access interface: GigabitEthernet1/0/21
Username: 00-0C-29-5B-81-51
User access state: Successful
Authentication domain: test.com
IPv4 address: 2.2.2.2
IPv4 address source: IP Source Guard
Initial VLAN: 2
Authorization untagged VLAN: N/A
Authorization tagged VLAN: N/A
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Authorization IPv6 URL: N/A
Authorization temporary redirect: Disabled
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: N/A
Offline detection: 300 sec (command-configured)
Online from: 2022/11/11 16:14:48
Online duration: 0h 3m 40s
Port-down keep online: Disabled (offline)

Slot ID: 1
User MAC address: 000c-29af-5a33
Access interface: GigabitEthernet1/0/21
Username: 00-0C-29-AF-5A-33
User access state: Successful
Authentication domain: test.com
IPv4 address: 2.2.2.111
IPv4 address source: IP Source Guard
Initial VLAN: 2
Authorization untagged VLAN: N/A
Authorization tagged VLAN: N/A
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: 3000
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: https://3.3.3.24:8443/portal/gateway?client_mac=00-0C-29-AF-5A-33&portal=404e0f70-2e02-11e8-ba71-005056872c7f&action=cwa&token=54248765
7bb909e6355fc2c50d5e16ae
Authorization IPv6 URL: N/A
Authorization temporary redirect: Disabled
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: N/A
Offline detection: 300 sec (command-configured)
Online from: 2022/11/11 16:11:55
Online duration: 0h 6m 33s
```

(4) ISE 上显示情况

ISE 上日志可以看到，终端通过 MAC 地址认证拿到 CWA-redirect-hhh 授权，在 CWA 页面认证通过后，ISE 下发 COA 重认证，而后拿到 PermitAccess 授权。

图6-11 ISE 日志显示

6.4 配置文件

```
#
 mac-authentication domain test.com
 mac-authentication user-name-format mac-address with-hyphen uppercase
#
#
vlan 2
 description toClients
 arp snooping enable
#
vlan 3
 description toAAAserver
#
```

```
interface Vlan-interface2
 description toClients
 ip address 2.2.2.29 255.255.255.0
#
interface Vlan-interface3
 description toAAAservers
 ip address 3.3.3.29 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 2
MAC-authentication
#
radius scheme ise
 primary authentication 3.3.3.24 key cipher $c$3$2oLOvHdRilTBlb6n1yh3/MoXN8z/RMbctQ==
 primary accounting 3.3.3.24 key cipher $c$3$fAhWH/rHm9hCcPq2PBWQa54YG9xKuQ1P0w==
 user-name-format keep-original
#
#
domain test.com
 authentication default radius-scheme ise
 authorization default radius-scheme ise
 accounting default radius-scheme ise
#
```

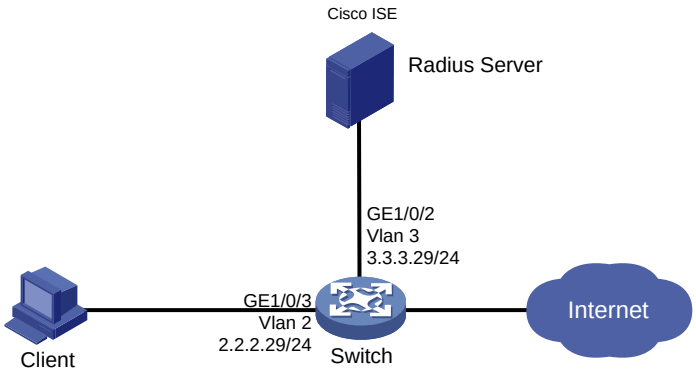
7 授权 VLAN 对接配置举例

7.1 组网需求

如图 7-1 所示，Client 和 ISE 服务器通过 Switch 建立连接，设备管理员希望对 Client 进行 802.1X 认证或者 MAC 地址认证，以控制其对网络资源的访问，具体要求如下：

- 采用 Cisco ISE 作为 RADIUS 服务器。
- 通过 ISE 授权下发 VLAN，初始 VLAN 为 100，目标授权 VLAN 2。

图7-1 授权 VLAN 组网图



7.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch：S5560X-R6618P27
- 认证服务器: Cisco ISE V2.4.0.357 patch 8
- 系统：Windows 10 21H2
- 认证客户端：iNode PC 7.3 (E513)

7.3 授权VLAN配置步骤与验证

7.3.1 配置 Switch

MAC 地址认证用户，Swtich 上的配置请参考 5.3.1 配置 Switch。

802.1X 认证用户，Swtich 上的配置请参考 4.3.1 配置 Switch。

为验证效果，可以配置 DHCP 服务器。

7.3.2 配置 ISE

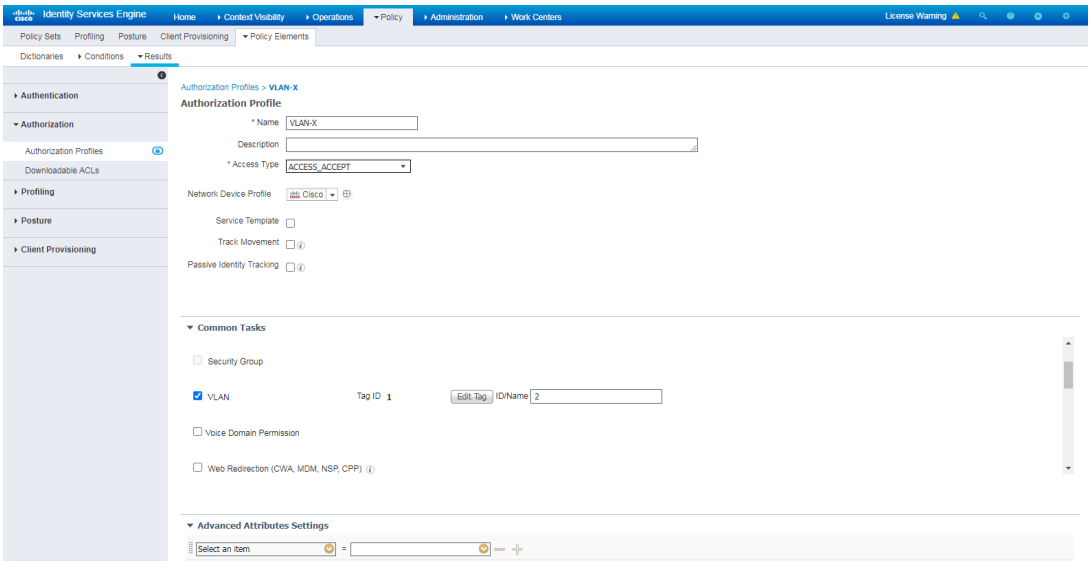
MAC 地址认证用户，服务器上的配置请参考 5.3.2 配置 ISE。

802.1X 认证用户，服务器上的配置请参考 4.3.2 配置 ISE。

(1) 配置 Authorization Profile

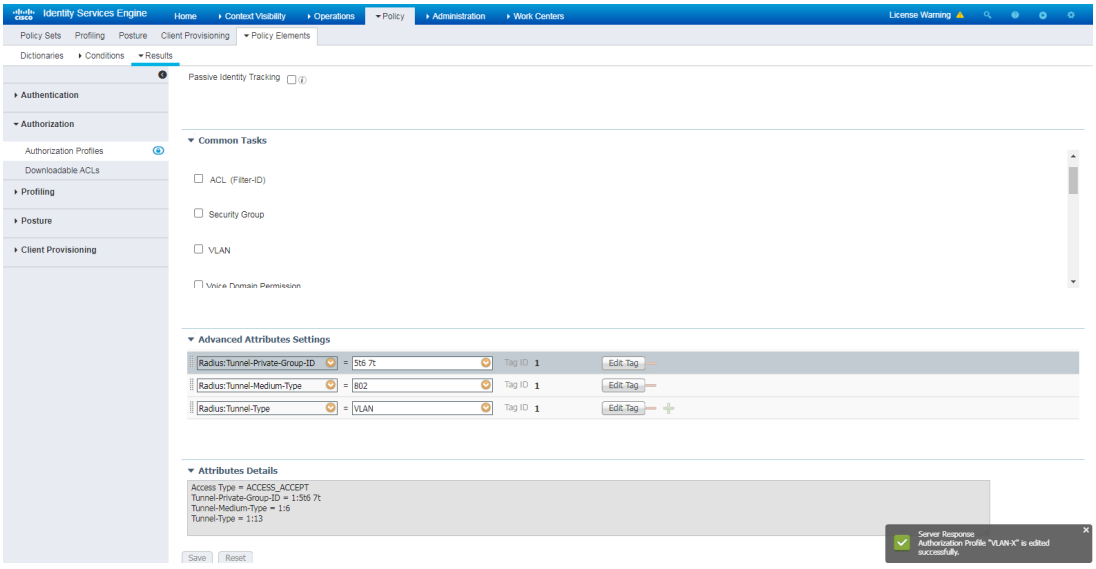
在 ISE 页面上选择[Policy/Policy Elements/Results/Authorization/Authorization Profiles]选项，点击<Add>按钮，在 Authorization Profile 栏中配置名称为 VLAN-X，在 Network Switch Profile 下拉框中选择跟 Network Switchs 中添加的交换机相同的类型，在 Common Tasks 栏中勾选 VLAN 属性并输入 VLAN 编号 2。

图7-2 配置授权 VLAN



注意，如果需要下发 VLAN 格式中需要包含空格的话，在 Common Tasks 的 vlan 中填入网页会报错，可以在 Advanced Attributes Settings 中选择对应字段填入，参考下图。VLAN 格式的具体规则请参考产品文档。文档后续配置还是以 vlan2 为例。

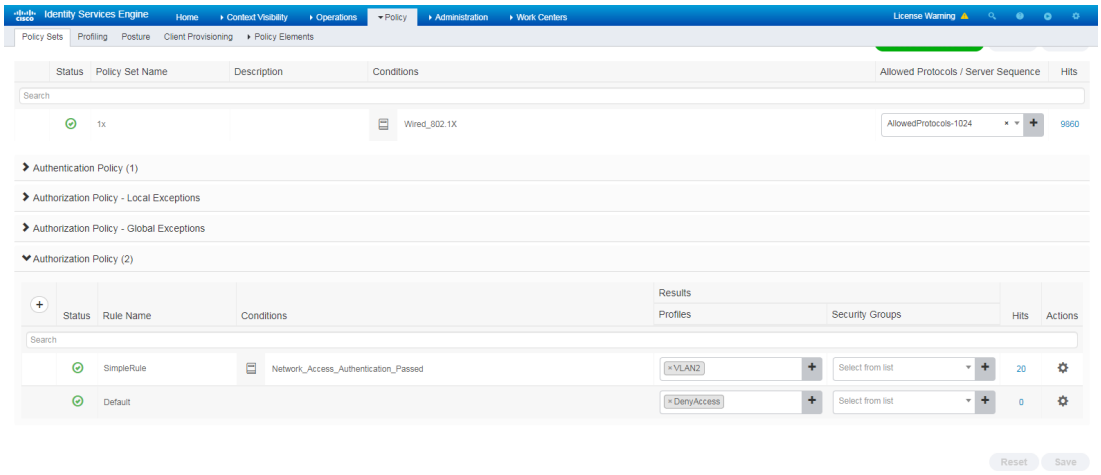
图7-3 在 Advanced Attributes Settings 中填入 VLAN 信息



(2) 配置认证和授权策略

在 ISE 页面上选择[Policy/Policy Sets]选项，在对应的 Result Pofiles 栏中选择“VLAN2”。

图7-4 配置认证和授权策略



7.3.3 验证配置

(1) 服务器端显示

在页面上方导航栏中选择[Operations/RADIUS]，用户可以查看终端上线的 Live Logs 和 Live Sessions 等信息。

图7-5 用户上线后服务器显示 1

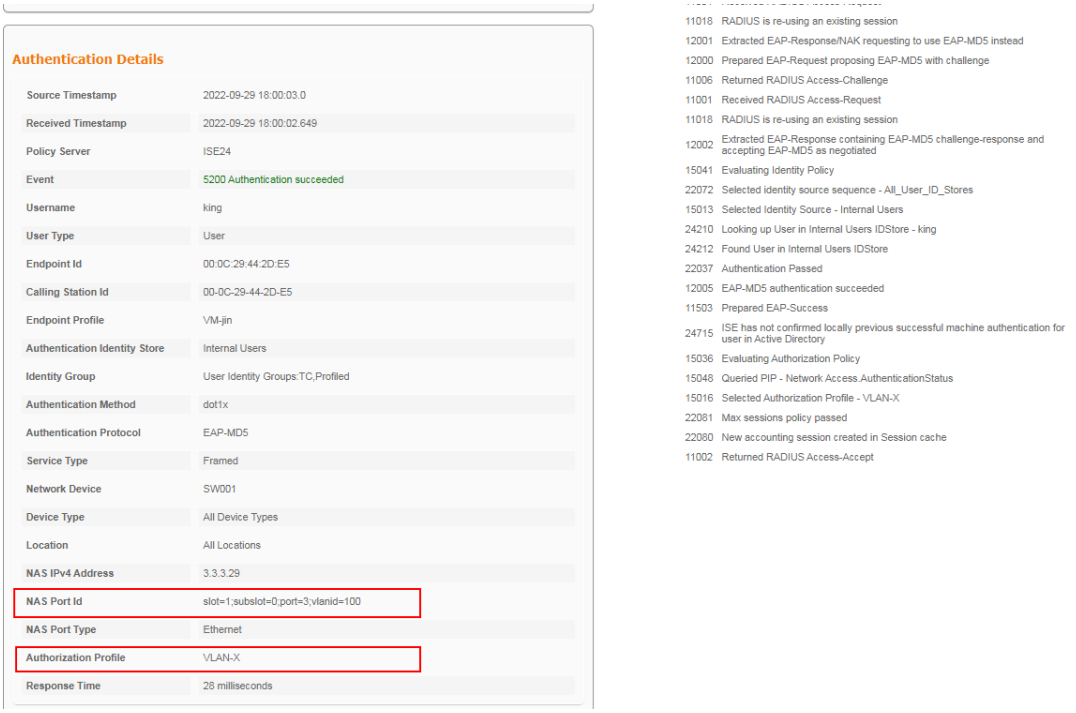
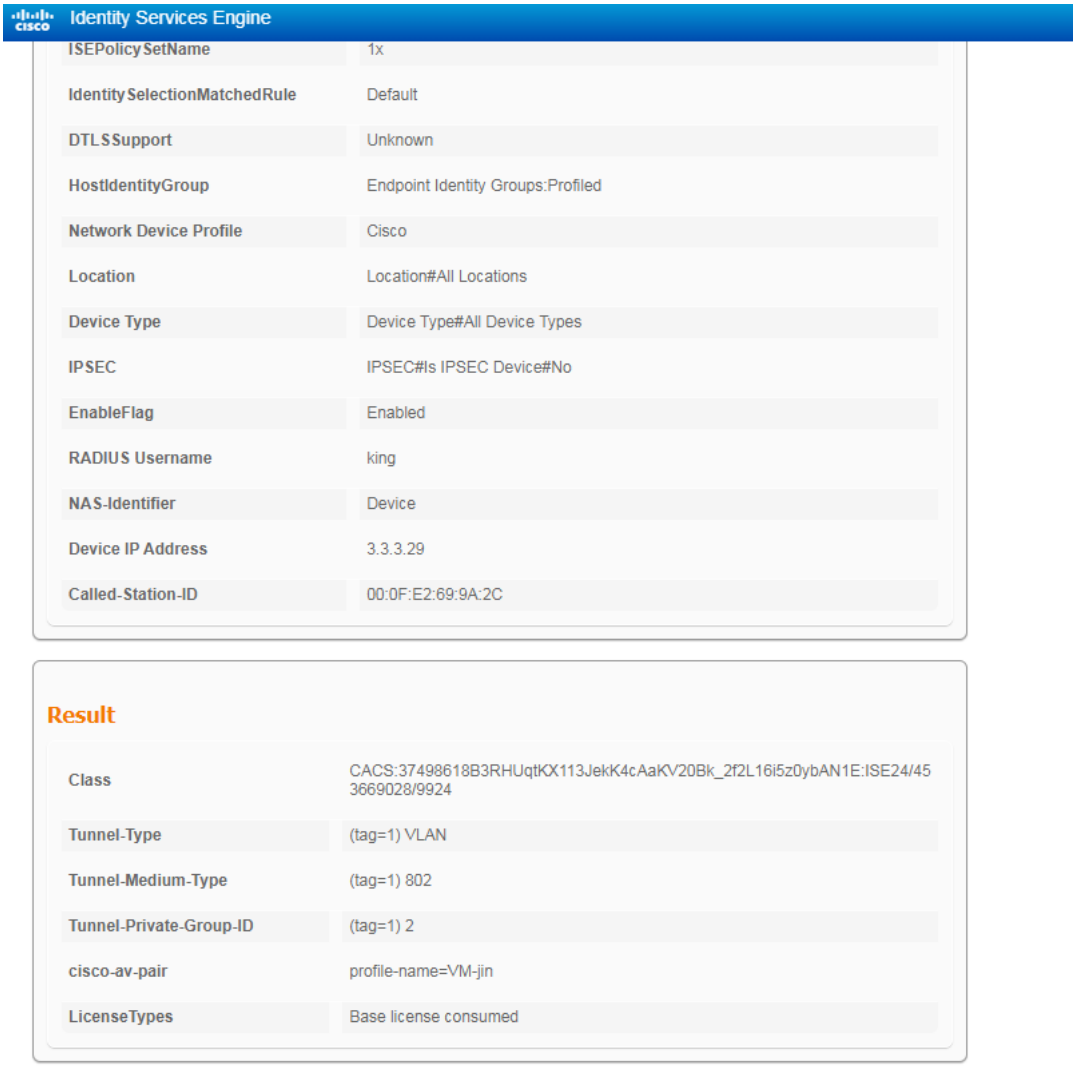


图7-6 用户上线后服务器显示 2



(2) 设备端显示（以 802.1X 认证为例）

在设备上通过 **display dot1x connection** 命令可以查看上线 802.1X 用户的信息。其中 Authorization untagged VLAN 字段显示成功下发的授权 VLAN。

```
<Switch> display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 000c-2944-2de5
Access interface: GigabitEthernet1/0/3
Username: king
User access state: Successful
Authentication domain: test.com
IPv4 address: 2.2.2.18
IPv4 address source: IP Source Guard
EAP packet identifier: 108
Authentication method: EAP
```

```
AAA authentication method: RADIUS
Initial VLAN: 100
Authorization untagged VLAN: 2
Authorization tagged VLAN list: N/A
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Authorization IPv6 URL: N/A
Authorization temporary redirect: Disabled
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: N/A
Online from: 2022/09/29 17:58:14
Online duration: 0h 4m 6s
```

(3) 连通性验证

授权成功，终端加入到 vlan2，通过 DHCP 拿到 IP 地址。显示如下：

```
Ethernet adapter AAAuser:
   Connection-specific DNS Suffix    :
   Description                       : Intel(R) 82574L Gigabit Network Connection
   Physical Address                  : 00-0C-29-44-2D-E5
   DHCP Enabled                      : Yes
   Autoconfiguration Enabled         : Yes
   IPv4 Address                      : 2.2.2.18(Preferred)
   Subnet Mask                       : 255.255.255.0
   Lease Obtained                    : 30 September 2022 17:00:41
   Lease Expires                     : 10 October 2022 17:00:40
   Default Gateway                   : 2.2.2.29
   DHCP Server                       : 2.2.2.29
   DNS Servers                       : 3.3.3.12
   NetBIOS over Tcpip                : Enabled
```

并可以跟跟其他系统正常联通。

```
PS C:\Windows\system32> tracert 3.3.3.24

Tracing route to 3.3.3.24 over a maximum of 30 hops

  1     1 ms     1 ms     1 ms  2.2.2.29
  2     1 ms    <1 ms    <1 ms  3.3.3.24
```

7.4 配置文件

```
#
```

```
 dot1x
 dot1x authentication-method eap
#
vlan 1
#
vlan 2
 description toClients
 arp snooping enable
#
vlan 3
 description toAAAserver
#
interface Vlan-interface1
#
interface Vlan-interface2
 description toClients
 ip address 2.2.2.29 255.255.255.0
#
interface Vlan-interface3
 description toAAAservers
 ip address 3.3.3.29 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 2
 dot1x
#
radius scheme ise
 primary authentication 3.3.3.24 key cipher $c$3$2oLOvHdRilTBlb6n1yh3/MoXN8z/RMbctQ==
 primary accounting 3.3.3.24 key cipher $c$3$fAhWH/rHm9hCcPq2PBWQa54YG9xKuQ1P0w==
 timer realtime-accounting 20 second
 user-name-format keep-original
#
#
domain test.com
 authentication default radius-scheme ise
 authorization default radius-scheme ise
 accounting default radius-scheme ise
#
 dhcp enable
 dhcp server forbidden-ip 2.2.2.29
#
dhcp server ip-pool Pool1
 gateway-list 2.2.2.29
```

```
 network 2.2.2.0 mask 255.255.255.0
 dns-list 3.3.3.12
 expired day 10
#
```

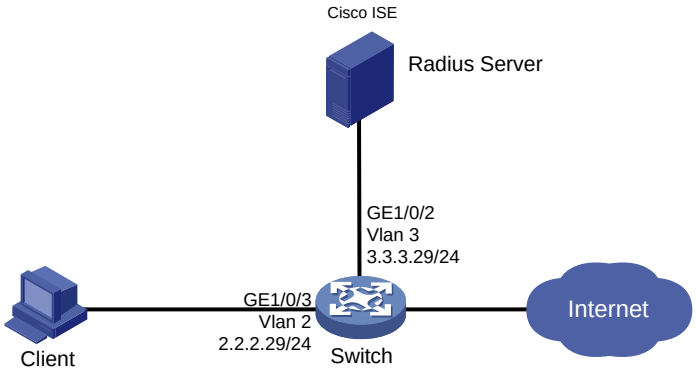
8 授权静态 ACL 对接配置举例

8.1 组网需求

如图 8-1 所示，Client 和 ISE 服务器通过 Switch 建立连接，设备管理员希望对 Client 进行 802.1X 认证或者 MAC 地址认证或 Portal 认证，以控制其对网络资源的访问，具体要求如下：

- 采用 Cisco ISE 作为 RADIUS 服务器。
- 通过 ISE 授权下发 ACL 编号。

图8-1 授权 ACL 组网图



8.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch：S5560X-R6618P27
- 认证服务器: Cisco ISE V2.4.0.357 patch 8
- 系统：Windows 10 21H2
- 认证客户端：iNode PC 7.3 (E513)

8.3 配置步骤

8.3.1 配置 Switch

MAC 地址认证用户，Swtich 上的配置请参考 5.3.1 配置 Switch。

802.1X 认证用户，Swtich 上的配置请参考 4.3.1 配置 Switch。

授权静态 ACL 时，该 ACL 必须在设备上已经创建才会生效。

在设备上创建 ACL，并配置规则。

```
[Switch] acl advanced 3200
[Switch-acl-ipv4-adv-3200] rule 0 deny ip destination 3.3.3.12 0
```

8.3.2 配置 ISE

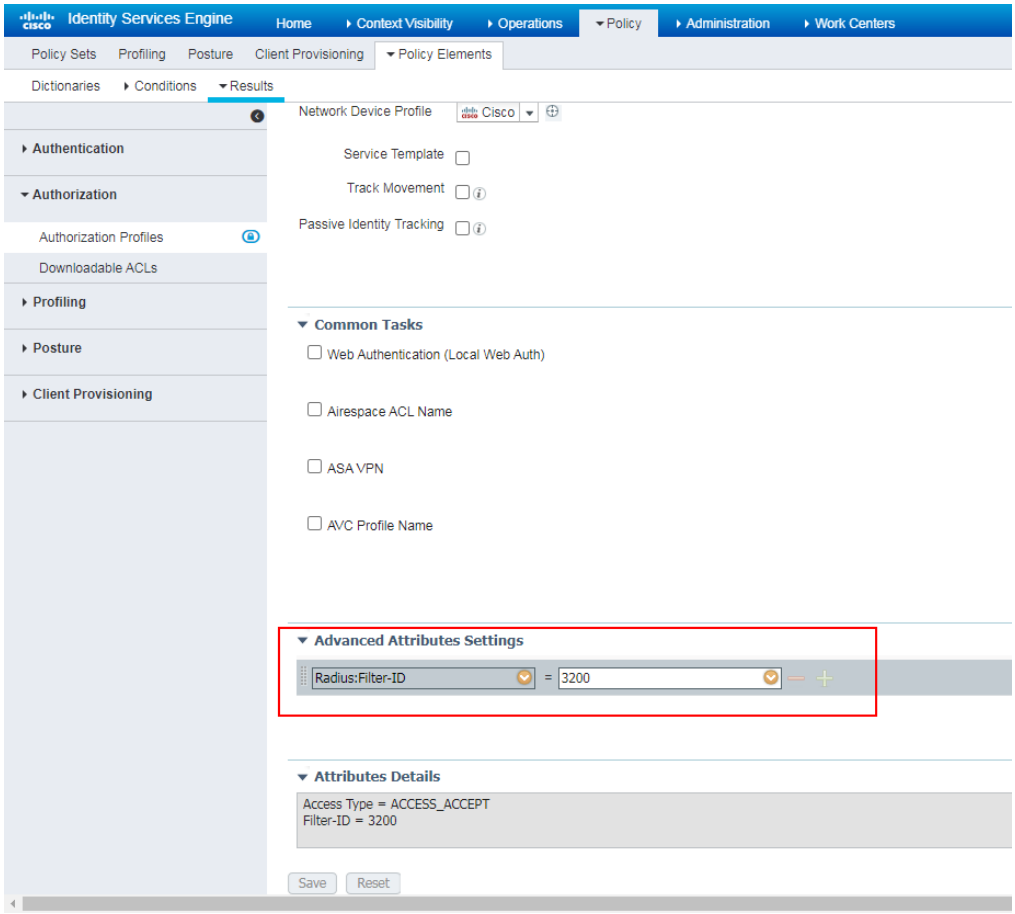
MAC 地址认证用户，服务器上的配置请参考 5.3.2 配置 ISE。

802.1X 认证用户，服务器上的配置请参考 4.3.2 配置 ISE。

(1) 配置 Authorization Profile

在 ISE 页面上选择[Policy/Policy Elements/Results/Authorization/Authorization Profiles]选项，点击<Add>按钮，在 Authorization Profile 栏中配置名称为 Dynamic_ACL ID，在 Network Switch Profile 下拉框中选择跟 Network Switchs 中添加的交换机相同的类型，在 Advanced Attributes Settings 中添加 Filter-ID 为 3200。

图8-2 在 Advanced Attributes Settings 中填入 Filter-ID 信息

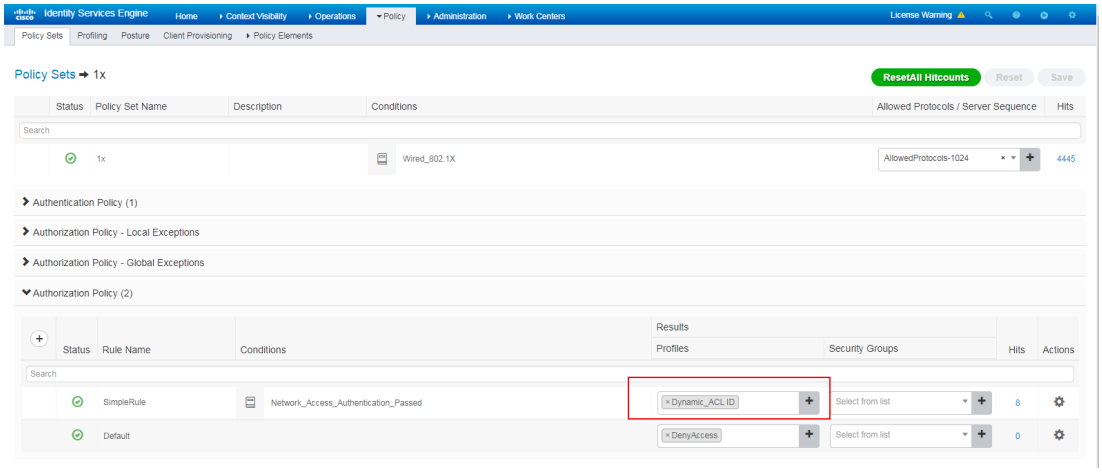


注：Filter-ID 取值为数字，则按照 ACL Number 处理，取值不全为数字，则按照 User Profile 处理。

(2) 配置 Policy

在 ISE 页面上选择[Policy/Policy Sets]选项，在相应的 policy 中修改 Results Profiles 为刚创建的 Dynamic_ACL ID。

图8-3 修改 Policy

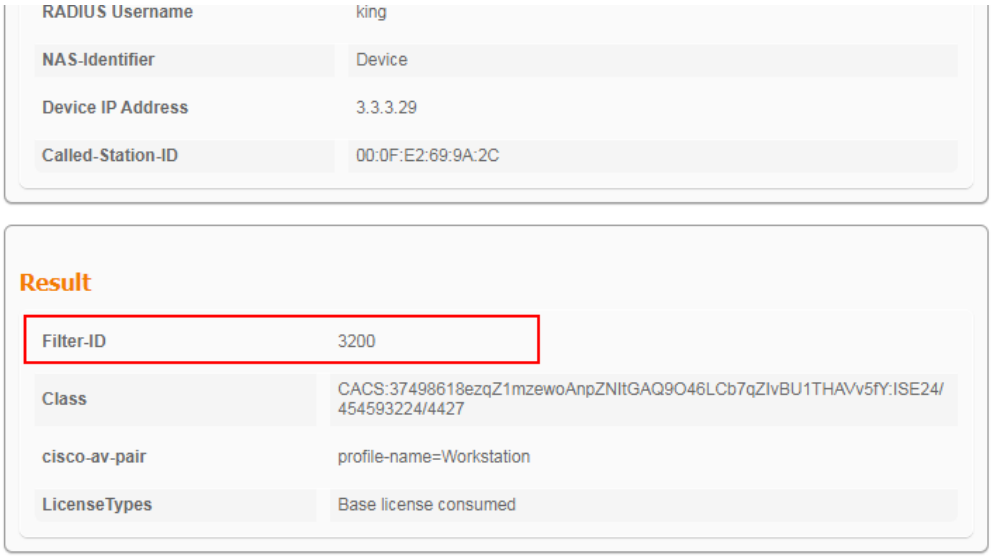


8.4 验证配置

用户使用不同认证方式上线（MAC 地址认证、802.1X 认证、Portal 认证）。

(1) 用户上线后服务器上显示。

图8-4 用户上线后服务器显示



(2) 用户上线后设备上显示

可以看到服务器下发的 ACL 成功下发到设备上。

```
<Switch> display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 000c-2944-2de5
Access interface: GigabitEthernet1/0/3
Username: king
```

```
     User access state: Successful
     Authentication domain: test.com
     IPv4 address: 2.2.2.1
     IPv4 address source: IP Source Guard
     EAP packet identifier: 100
     Authentication method: EAP
     AAA authentication method: RADIUS
     Initial VLAN: 2
     Authorization untagged VLAN: N/A
     Authorization tagged VLAN list: N/A
     Authorization VSI: N/A
     Authorization microsegment ID: N/A
     Authorization ACL number/name: 3200
     Authorization dynamic ACL name: N/A
     Authorization user profile: N/A
     Authorization CAR: N/A
     Authorization URL: N/A
     Authorization IPv6 URL: N/A
     Authorization temporary redirect: Disabled
     Start accounting: Successful
     Real-time accounting-update failures: 0
     Termination action: Default
     Session timeout period: N/A
     Online from: 2021/01/08 16:21:32
     Online duration: 0h 6m 51s
```

8.5 配置文件

```
#
 dot1x
 dot1x authentication-method eap
#
vlan 1
#
vlan 2
 description toClients
 arp snooping enable
#
vlan 3
 description toAAAserver
#
interface Vlan-interface1
#
interface Vlan-interface2
 description toClients
 ip address 2.2.2.29 255.255.255.0
#
interface Vlan-interface3
```

```
 description toAAAservers
 ip address 3.3.3.29 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 2
 dot1x
#
radius scheme ise
 primary authentication 3.3.3.24 key cipher $c$3$2oLOvHdRilTBlb6n1yh3/MoXN8z/RMbctQ==
 primary accounting 3.3.3.24 key cipher $c$3$fAhWH/rHm9hCcPq2PBWQa54YG9xKuQ1P0w==
 timer realtime-accounting 20 second
 user-name-format keep-original
#
#
domain test.com
 authentication default radius-scheme ise
 authorization default radius-scheme ise
 accounting default radius-scheme ise
#
```

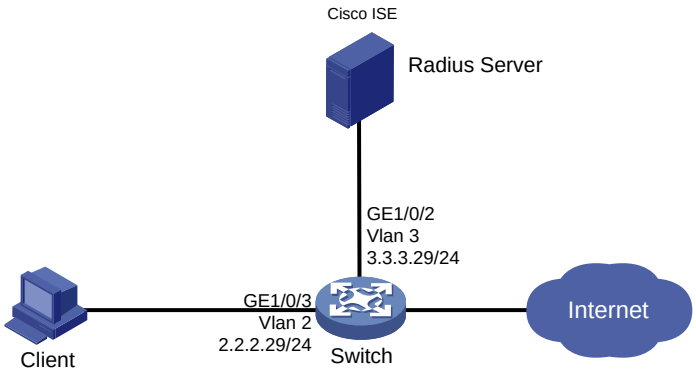
9 授权动态 ACL 对接配置举例

9.1 组网需求

如图 9-1 所示，Client 和 ISE 服务器通过 Switch 建立连接，设备管理员希望对 Client 进行 802.1X 认证或者 MAC 地址认证或 Portal 认证，以控制其对网络资源的访问，具体要求如下：

- 采用 Cisco ISE 作为 RADIUS 服务器。
- 通过 ISE 授权下发动态 ACL 信息。

图9-1 授权 ACL 组网图



9.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch：S5560X-R6618P27
- 认证服务器: Cisco ISE V2.4.0.357 patch 8
- 系统：Windows 10 21H2
- 认证客户端：iNode PC 7.3 (E513)

9.3 配置步骤

9.3.1 配置 Switch

MAC 地址认证用户，Swtich 上的配置请参考 5.3.1 配置 Switch。

802.1X 认证用户，Swtich 上的配置请参考 4.3.1 配置 Switch。

9.3.2 配置 ISE

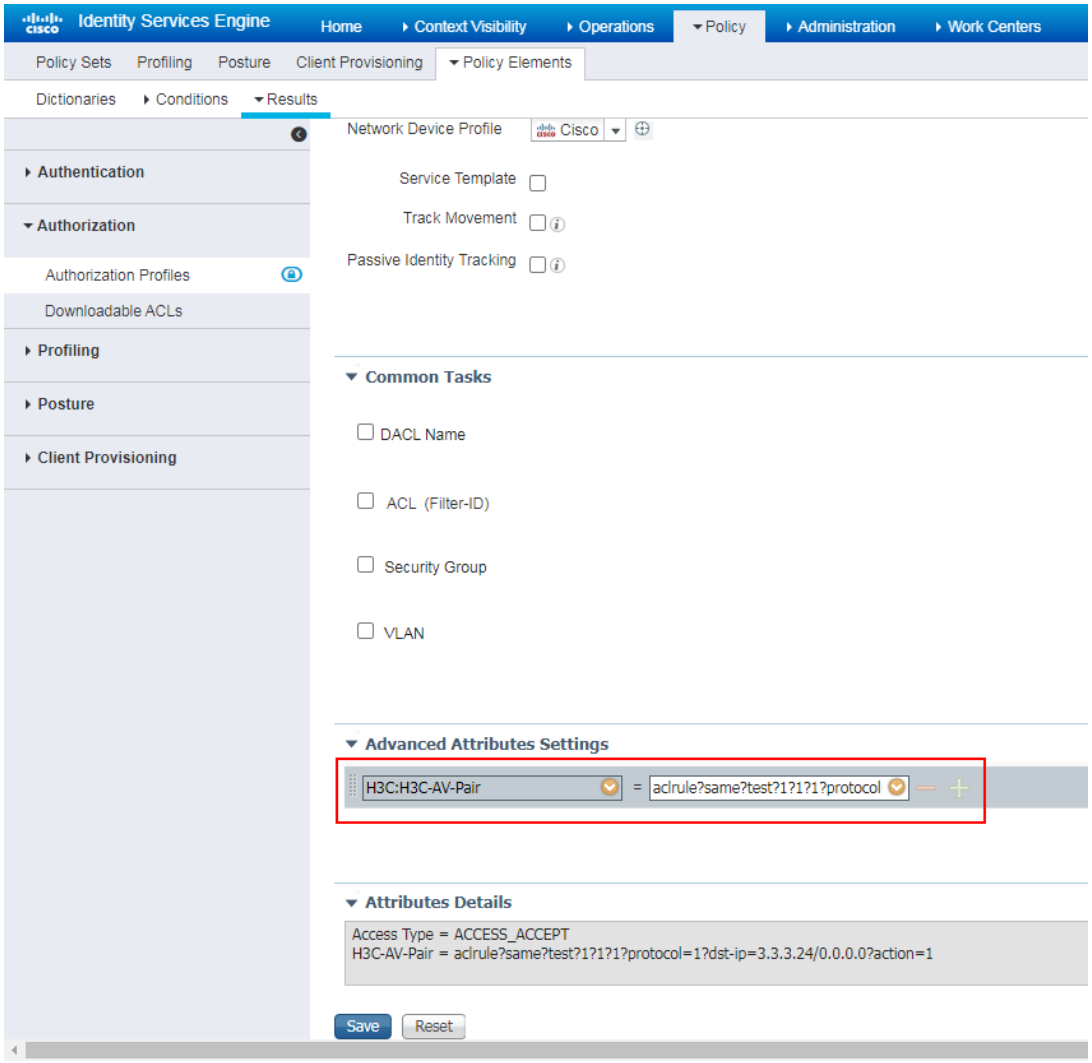
MAC 地址认证用户，服务器上的配置请参考 5.3.2 配置 ISE。

802.1X 认证用户，服务器上的配置请参考 4.3.2 配置 ISE。

(1) 配置 Authorization Profile

在 ISE 页面上选择[Policy/Policy Elements/Results/Authorization/Authorization Profiles]选项，点击<Add>按钮，在 Authorization Profile 栏中配置名称为 Downloadable_ACL，在 Network Switch Profile 下拉框中选择跟 Network Switchs 中添加的交换机相同的类型，在 Advanced Attributes Settings 中添加 H3C-AV-Pair，并填入 aclrule?same?test?1?1?1?protocol=1?dst-ip=3.3.3.24/0.0.0.0?action=1，ACL 具体格式说明请参考相关产品文档。

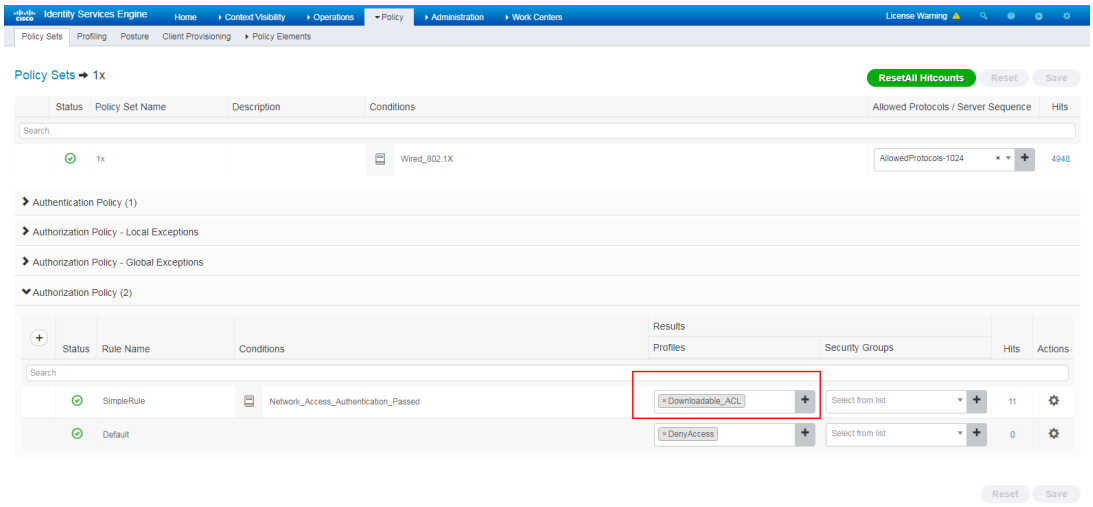
图9-2 在 Advanced Attributes Settings 中填入



(2) 配置 Policy

在 ISE 页面上选择[Policy/Policy Sets]选项，在相应的 policy 中修改 Results Profiles 为刚创建的 Downloadable_ACL

图9-3 修改 Policy

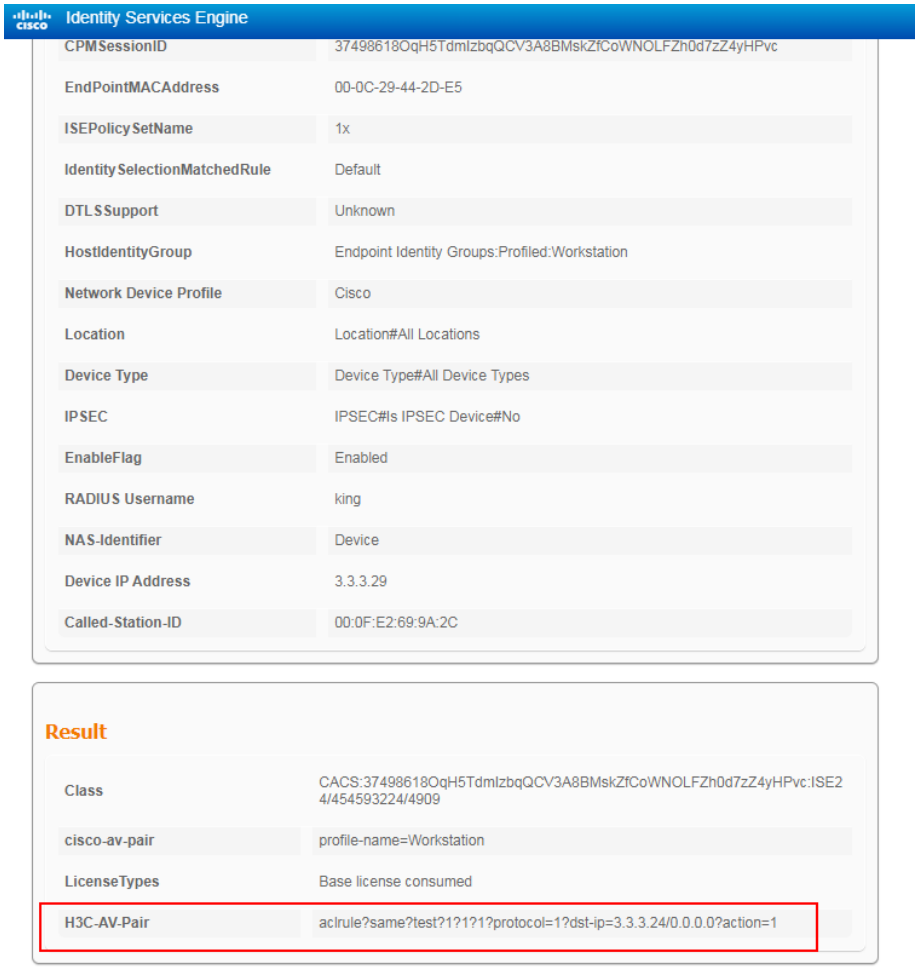


9.4 验证配置

用户使用不同认证方式上线（MAC 地址认证、802.1X 认证、Portal 认证）。

(1) 用户上线后服务器上显示。

图9-4 用户上线后服务器显示



(2) 用户上线后设备上显示

可以看到服务器下发的 ACL 成功下发到设备上。

```
<Switch> display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 000c-2944-2de5
Access interface: GigabitEthernet1/0/3
Username: king
User access state: Successful
Authentication domain: test.com
IPv4 address: 2.2.2.1
IPv4 address source: IP Source Guard
EAP packet identifier: 217
Authentication method: EAP
AAA authentication method: RADIUS
Initial VLAN: 2
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
```

```
    Authorization VSI: N/A
    Authorization microsegment ID: N/A
    Authorization ACL number/name: N/A
    Authorization dynamic ACL name: test
    Authorization user profile: N/A
    Authorization CAR: N/A
    Authorization URL: N/A
    Authorization IPv6 URL: N/A
    Authorization temporary redirect: Disabled
    Start accounting: Successful
    Real-time accounting-update failures: 0
    Termination action: Default
    Session timeout period: N/A
    Online from: 2021/01/08 18:59:52
    Online duration: 0h 7m 56s

    <Switch> display acl name test
    Advanced IPv4 ACL named test, 1 rule,
    This is a dynamic advanced IPv4 ACL
    ACL's step is 5, start ID is 0
     rule 1 deny ip destination 3.3.3.24 0 (Dynamic)
```

9.5 配置文件

```
#
 dot1x
 dot1x authentication-method eap
#
vlan 1
#
vlan 2
 description toClients
 arp snooping enable
#
vlan 3
 description toAAAserver
#
interface Vlan-interface1
#
interface Vlan-interface2
 description toClients
 ip address 2.2.2.29 255.255.255.0
#
interface Vlan-interface3
 description toAAAservers
 ip address 3.3.3.29 255.255.255.0
#
interface GigabitEthernet1/0/2
```

```
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 2
 dot1x
#
radius scheme ise
 primary authentication 3.3.3.24 key cipher $c$3$2oLOvHdRilTBlb6n1yh3/MoXN8z/RMbctQ==
 primary accounting 3.3.3.24 key cipher $c$3$fAhWH/rHm9hCcPq2PBWQa54YG9xKuQ1P0w==
 timer realtime-accounting 20 second
 user-name-format keep-original
#
#
domain test.com
 authentication default radius-scheme ise
 authorization default radius-scheme ise
 accounting default radius-scheme ise
#
```

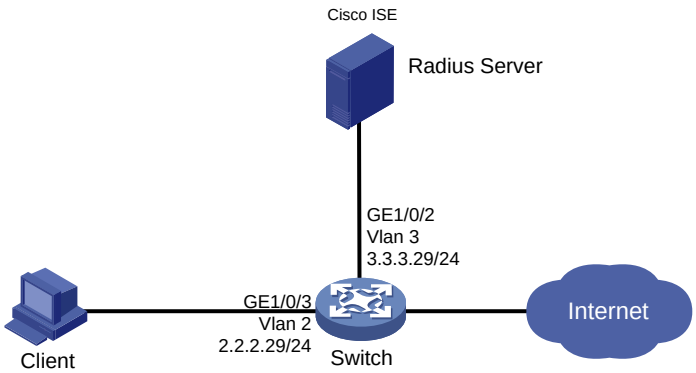
10 授权 CAR 对接配置举例

10.1 组网需求

如图 10-1 所示，Client 和 ISE 服务器通过 Switch 建立连接，设备管理员希望对 Client 进行 802.1X 认证或者 MAC 地址认证，以控制其对网络资源的访问，具体要求如下：

- 采用 Cisco ISE 作为 RADIUS 服务器。
- 通过 ISE 授权下发 CAR（Average input rate、Peak input rate、Average output rate、Peak output rate）。

图10-1 授权 CAR 组网图



10.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch：S5560X-R6618P27
- 认证服务器: Cisco ISE V2.4.0.357 patch 8
- 系统：Windows 10 21H2
- 认证客户端：iNode PC 7.3 (E513)

10.3 配置步骤

10.3.1 配置 Switch

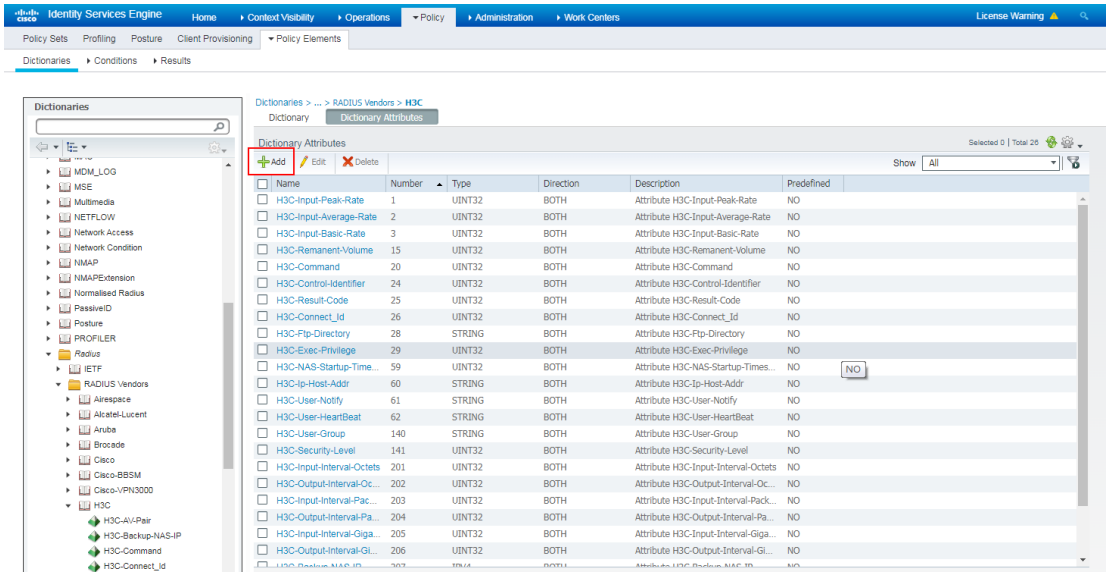
802.1X 认证用户，Swtich 上的配置请参考 4.3.1 配置 Switch。

10.3.2 配置 ISE

(1) 添加字典

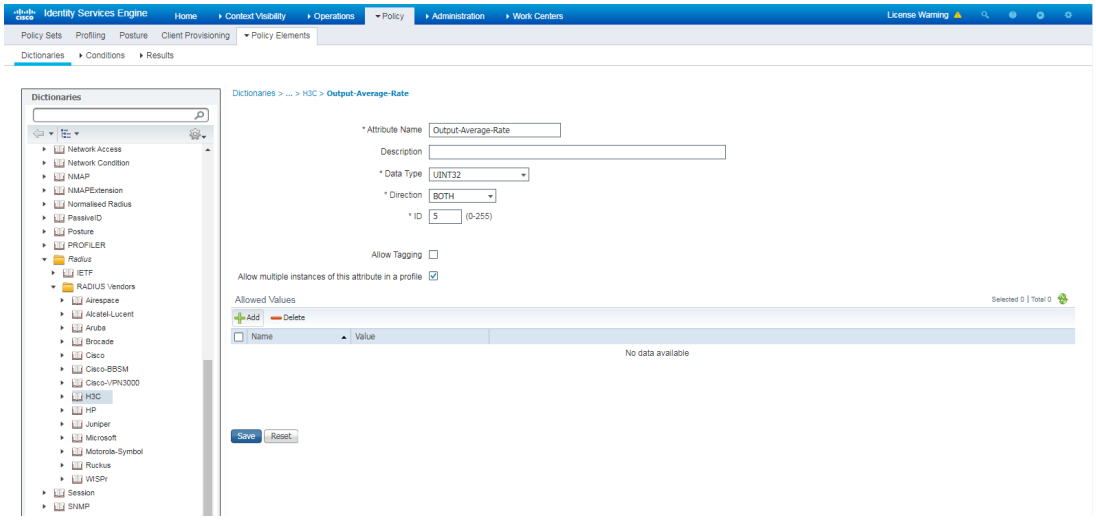
在 ISE 页面上选择[Policy/Policy Elements/Dictionaries]选项，依次选择“Dictionaries > RADIUS > RADIUS Vendors > H3C”，点击“Add”。

图10-2 添加字典



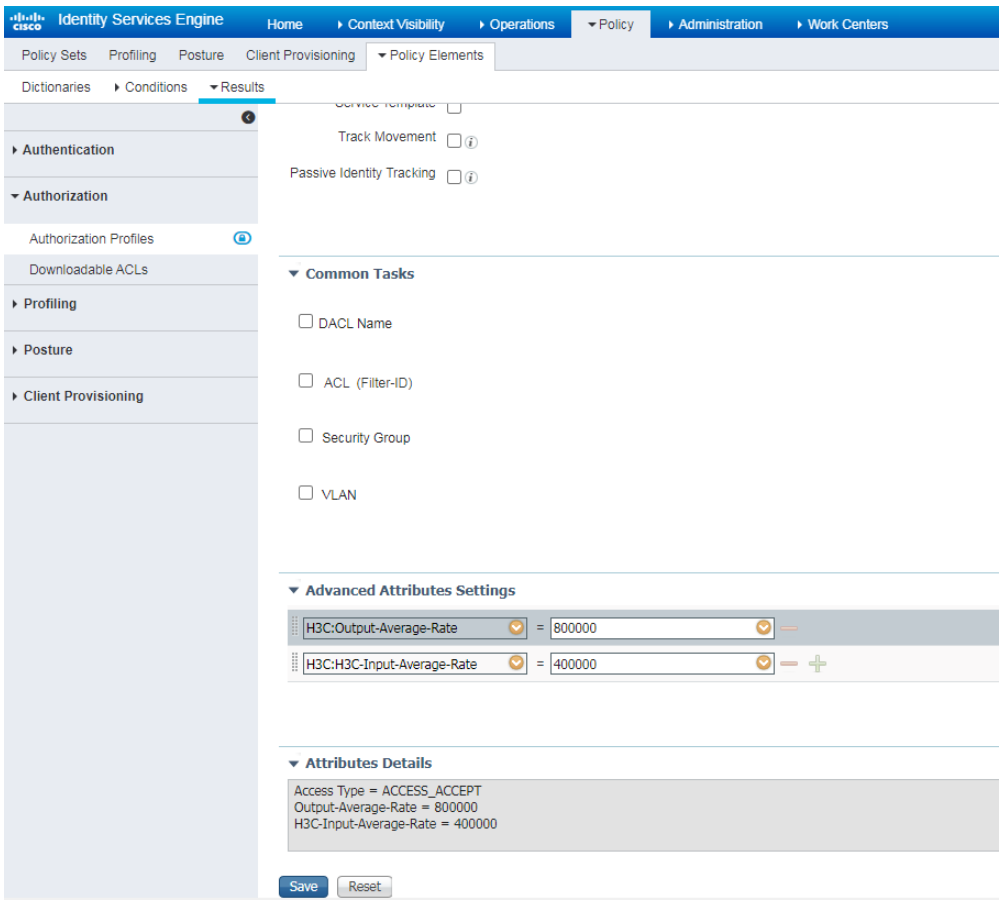
配置 Output-Average-Rate，Data Type 选择 UINT32。

图10-3 配置 Output-Average-Rate



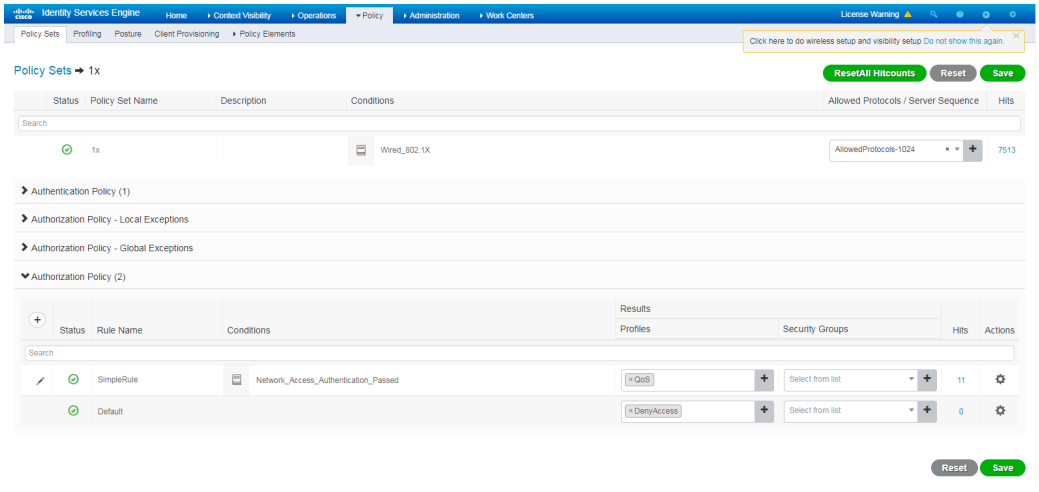
创建名为 Qos 的 authorization profile，在 Advanced Attributes Settings 中选择 H3C-Out-Average-Rate 和 H3C-H3C-Input-Average-Rate，并填入相应的数值。

图10-4 配置 authorization profile



在 Policy 中选择之前创建的 authorization profile。

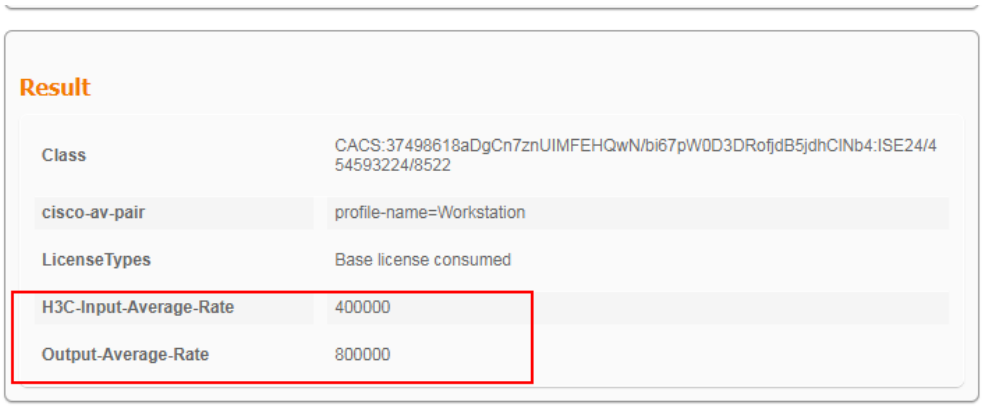
图10-5 配置 policy set



10.4 验证配置

(1) 用户上线后服务器上显示如图 10-6。

图10-6 用户上线后服务器显示



(2) 用户上线后设备上显示

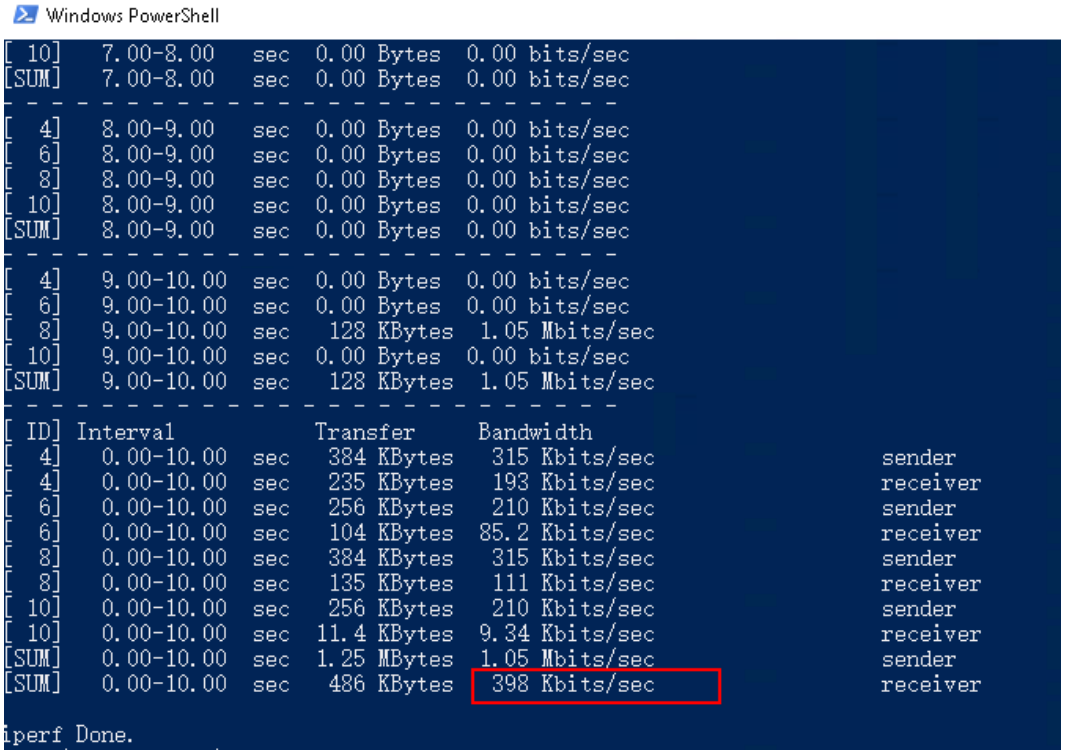
在设备上通过 **display dot1x connection** 命令可以查看上线 802.1X 用户的信息。其中 Authorization CAR 字段显示成功下发授权 CAR。

```
<Switch> display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 000c-2944-2de5
Access interface: GigabitEthernet1/0/3
Username: king
User access state: Successful
```

```
Authentication domain: test.com
IPv4 address: 2.2.2.1
IPv4 address source: IP Source Guard
EAP packet identifier: 16
Authentication method: EAP
AAA authentication method: RADIUS
Initial VLAN: 2
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR:
  Average input rate: 400000 bps
  Peak input rate: 400000 bps
  Average output rate: 800000 bps
  Peak output rate: 800000 bps
Authorization URL: N/A
Authorization IPv6 URL: N/A
Authorization temporary redirect: Disabled
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: N/A
Online from: 2021/01/09 14:24:42
Online duration: 1h 8m 46s
```

通过的终端 Windows10 使用 iperf 验证 input 限速效果。

图10-7 input 限速效果



10.5 配置文件

```
#
 dot1x
 dot1x authentication-method eap
#
vlan 1
#
vlan 2
 description toClients
 arp snooping enable
#
vlan 3
 description toAAAserver
#
interface Vlan-interface1
#
interface Vlan-interface2
 description toClients
 ip address 2.2.2.29 255.255.255.0
#
interface Vlan-interface3
 description toAAAservers
 ip address 3.3.3.29 255.255.255.0
```

```
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 2
 dot1x
#
radius scheme ise
 primary authentication 3.3.3.24 key cipher $c$3$2oLOvHdRilTBlb6n1yh3/MoXN8z/RMbctQ==
 primary accounting 3.3.3.24 key cipher $c$3$fAhWH/rHm9hCcPq2PBWQa54YG9xKuQ1P0w==
 timer realtime-accounting 20 second
 user-name-format keep-original
#
#
domain test.com
 authentication default radius-scheme ise
 authorization default radius-scheme ise
 accounting default radius-scheme ise
#
```

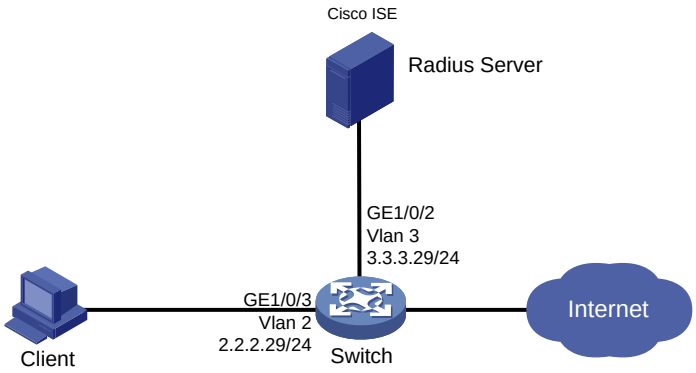
11 URL 重定向对接配置举例

11.1 组网需求

如图 11-1 所示，Client 和 ISE 服务器通过 Switch 建立连接，设备管理员希望对 Client 进行 802.1X 认证，以控制其对网络资源的访问，具体要求如下：

- 采用 ISE 作为 RADIUS 服务器和 Portal 服务器。
- 用户采用 802.1X 认证，服务器授权下发 URL 重定向。
- 802.1X 认证通过后，用户在客户端的游览器上输入任意 IP 地址会被重定向到 URL 中的 Web 页面。

图11-1 URL 重定向对接配置组网图



11.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch：S5560X-R6618P27
- 认证服务器: Cisco ISE V2.4.0.357 patch 8
- 系统：Windows 10 21H2
- 认证客户端：iNode PC 7.3 (E513)

11.3 配置步骤

说明

本配置仅展示认证的相关配置，网络互通的相关配置略，请保证设备间能够互相访问。

11.3.1 配置 Switch

#设备上配置一条 ACL 放行 URL 中的 IP 地址。并且该条 ACL 需要在服务器上下发。Swtich 上的其它配置请参考 4.3.1 配置 Switch。

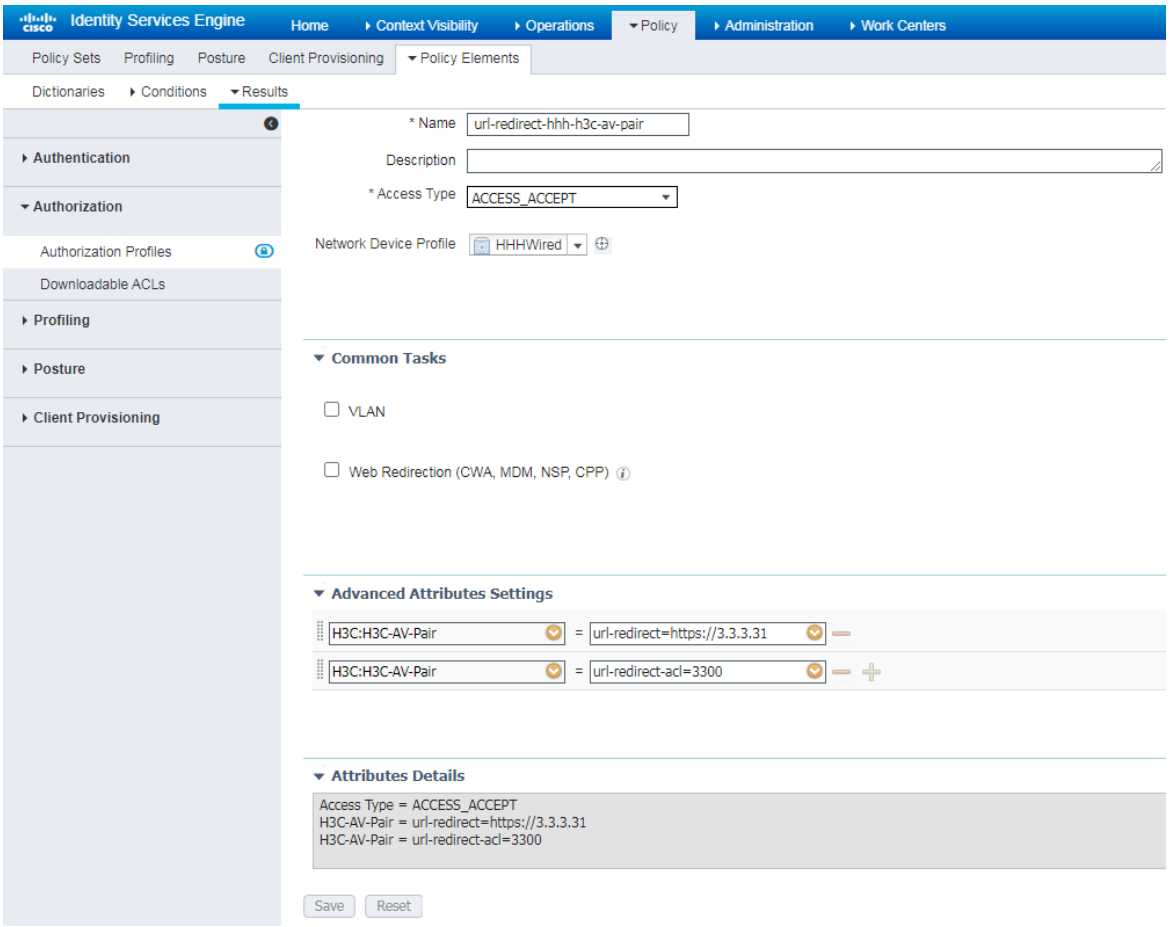
```
[Switch] acl advanced 3300
[Switch-acl-ipv4-adv-3100] rule 1 permit ip destination 3.3.3.31 0
```

11.3.2 配置 ISE

802.1X 认证用户，服务器上的配置请参考 4.3.2 配置 ISE。

只需将“配置文件”的“属性”参考下图修改即可。

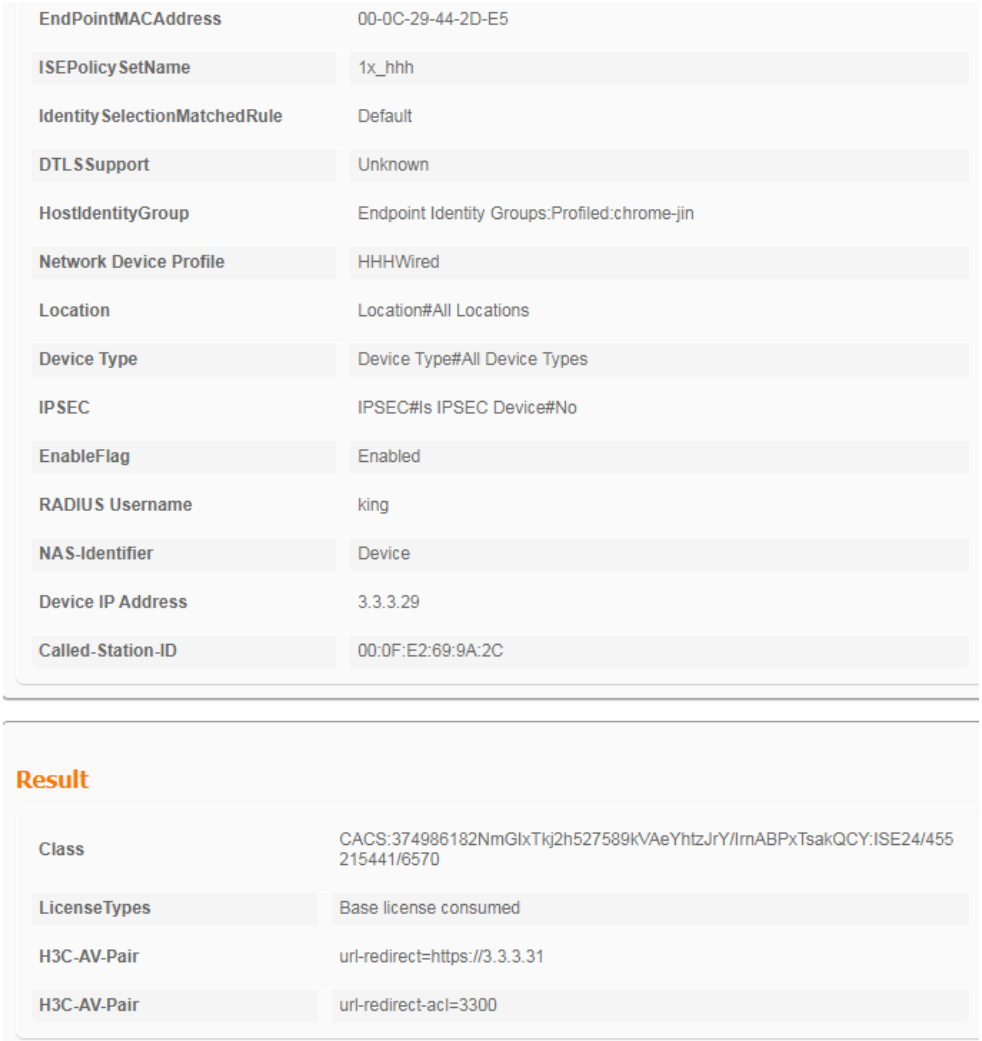
图11-2 创建 Authorization Profile



11.4 验证配置

(1) 用户上线后服务器显示

图11-3 用户上线后服务器输出显示



EndPointMACAddress	00-0C-29-44-2D-E5
ISEPolicySetName	1x_hhh
IdentitySelectionMatchedRule	Default
DTLSSupport	Unknown
HostIdentityGroup	Endpoint Identity Groups:Profiled:chrome-jin
Network Device Profile	HHHWired
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
EnableFlag	Enabled
RADIUS Username	king
NAS-Identifier	Device
Device IP Address	3.3.3.29
Called-Station-ID	00:0F:E2:69:9A:2C

Result

Class	CACS:374986182NmGlxTkj2h527589kVAeYhtzJrY/IrnABPxTsakQCY:ISE24/455215441/6570
LicenseTypes	Base license consumed
H3C-AV-Pair	url-redirect=https://3.3.3.31
H3C-AV-Pair	url-redirect-acl=3300

(2) 用户上线后设备显示

在设备上通过 **display dot1x connection** 命令可以查看上线 802.1X 用户的信息。

```
<Switch> display dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 000c-2944-2de5
Access interface: GigabitEthernet1/0/3
Username: king
User access state: Successful
Authentication domain: test.com
IPv4 address: 2.2.2.10
IPv4 address source: IP Source Guard
EAP packet identifier: 117
Authentication method: CHAP
AAA authentication method: RADIUS
Initial VLAN: 2
Authorization untagged VLAN: N/A
```

```
Authorization tagged VLAN list: N/A
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: 3300
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: https://3.3.3.31
Authorization IPv6 URL: N/A
Authorization temporary redirect: Disabled
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: N/A
Online from: 2022/10/18 14:40:26
Online duration: 1h 39m 14s
```

用户在客户端的游览器上输入任意 IP 地址，会被重定向到 URL 中的 Web 页面。

11.5 配置文件

```
#
 dot1x
 dot1x authentication-method eap
#
vlan 1
#
vlan 2
 description toClients
 arp snooping enable
#
vlan 3
 description toAAAserver
#
interface Vlan-interface1
#
interface Vlan-interface2
 description toClients
 ip address 2.2.2.29 255.255.255.0
#
interface Vlan-interface3
 description toAAAservers
 ip address 3.3.3.29 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/3
```

```
 port link-mode bridge
 port access vlan 2
 dot1x
#
radius scheme ise
 primary authentication 3.3.3.24 key cipher $c$3$2oLOvHdRilTBlb6n1yh3/MoXN8z/RMbctQ==
 primary accounting 3.3.3.24 key cipher $c$3$fAhWH/rHm9hCcPq2PBWQa54YG9xKuQ1P0w==
 timer realtime-accounting 20 second
 user-name-format keep-original
#
#
domain test.com
 authentication default radius-scheme ise
 authorization default radius-scheme ise
 accounting default radius-scheme ise
#
```

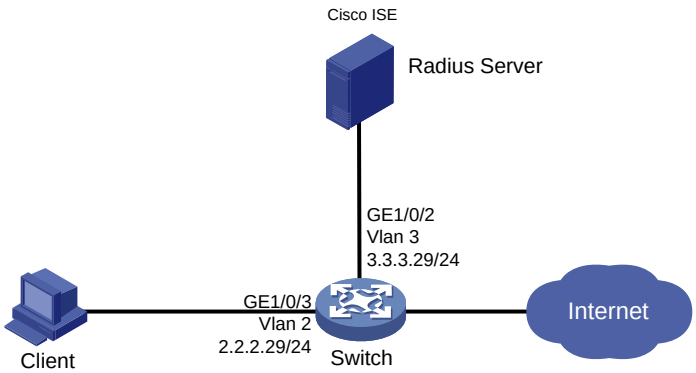
12 DAE 对接配置举例

12.1 组网需求

如图 12-1 示，Client 和 ISE 服务器通过 Switch 建立连接，设备管理员希望对 Client 进行认证（以 802.1X 认证为例），以控制其对网络资源的访问，具体要求如下：

- 采用 Cisco ISE 作为 RADIUS 服务器。
- 通过 ISE 下发 DAE 请求。

图12-1 DAE 对接配置组网图



12.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch：S5560X-R6618P27
- 认证服务器: Cisco ISE V2.4.0.357 patch 8

- 系统：Windows 10 21H2
- 认证客户端：iNode PC 7.3 (E513)

12.3 配置Switch

Swtich 上的基础配置请参考 4.3.1 配置 Switch。

设备上需要额外增加如下配置。

开启 RADIUS DAE 服务，并进入 RADIUS DAE 服务器视图。

```
[Switch] radius dynamic-author server
```

指定 RADIUS DAE 客户端，此 IP 是 AAA 服务器的 IP，密钥是服务器上配置的 radius 共享密钥，port 缺省为 3799。

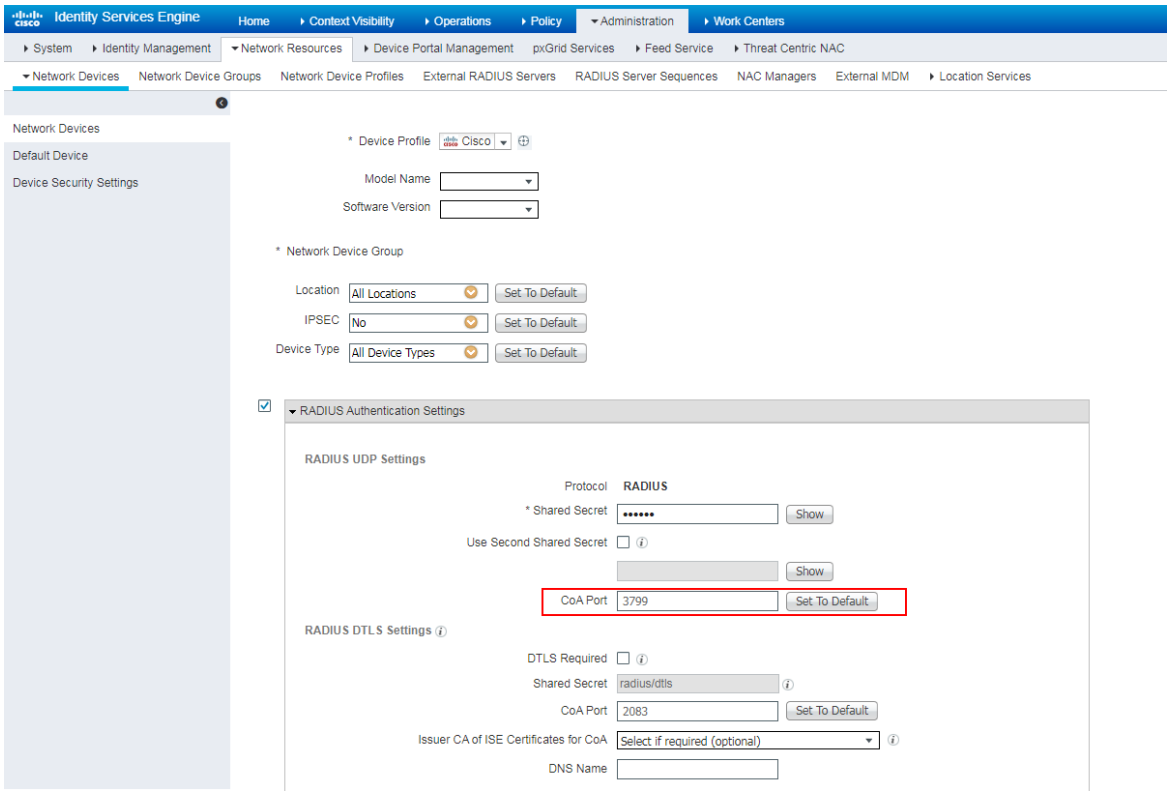
```
[Switch-radius-da-server] client ip 3.3.3.24 key simple expert
[Switch-radius-da-server] quit
```

12.4 配置ISE

服务器上的配置请参考 4.3.2 配置 ISE，并参考下图补充配置。

在 ISE 页面上选择[Administration/Network Resources/Network Devices/Network Devices]选项，确认 ISE 所添加的设备的 CoA Port 跟设备上的一致。

图12-2 确认 Network Switchs CoA Port



12.5 验证配置

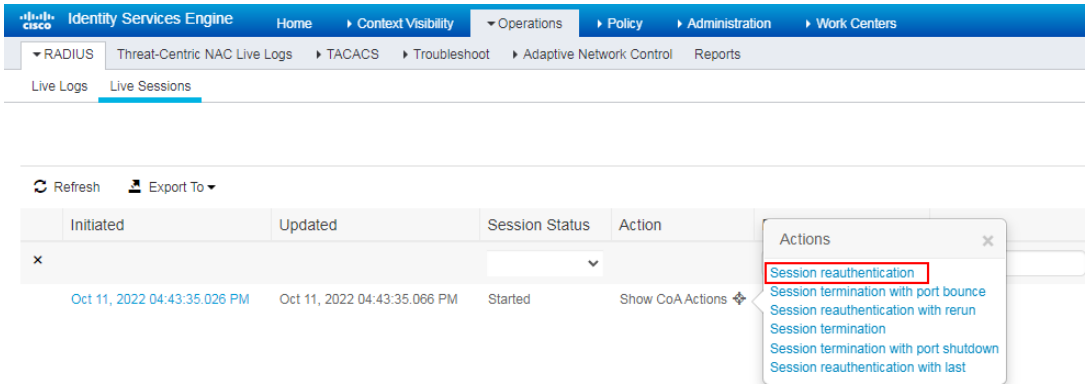
12.5.1 重认证

(1) ISE 上触发重认证

使用 802.1X 认证 PAP/CHAP 上线，在 Live Sessions 中点击 Show CoA Actions 后边的标志，选择 Session reauthentication。

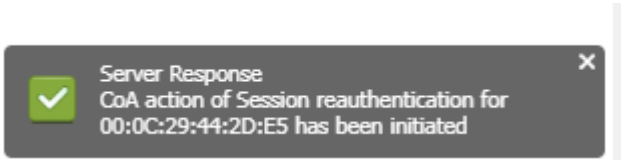
同样可以选择 Session termination with port bounce、Session termination with port shutdown、Session termination 来触发其他功能，本文档不再赘述。

图12-3 选择 Session reauthentication



点击后页面右下角提示如下。

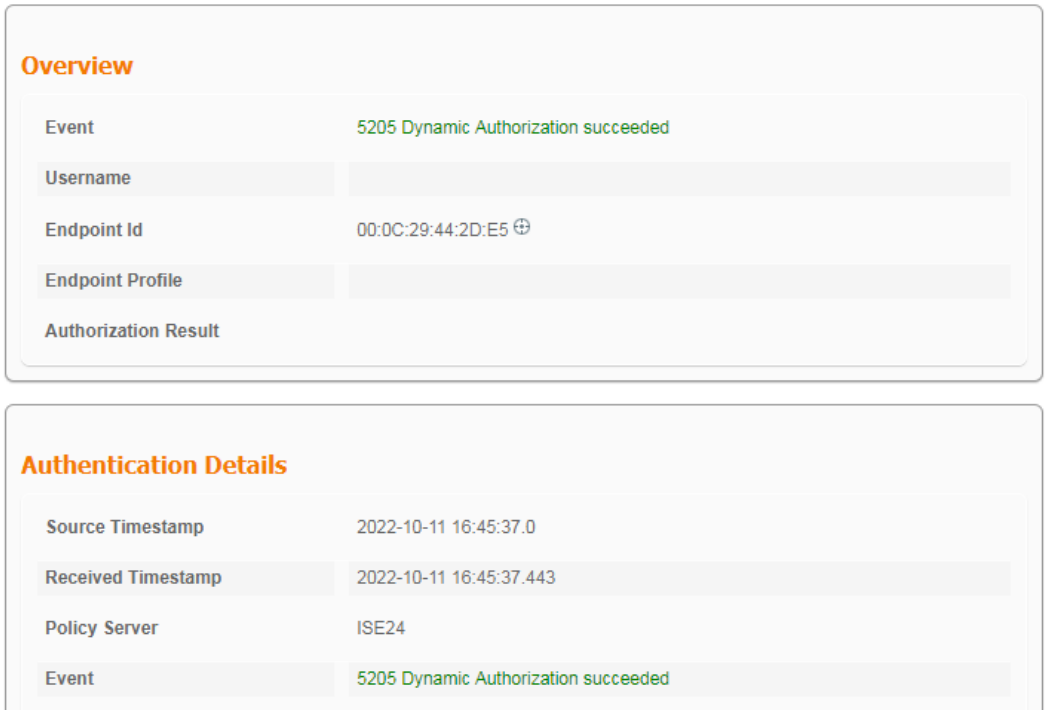
图12-4 点击后右下角提示



(2) ISE 上日志

Live Logs 可以看到下发成功的日志。

表12-1 Live Logs 日志



12.6 配置文件

```
#
 dot1x
 dot1x authentication-method eap
#
vlan 1
#
vlan 2
 description toClients
 arp snooping enable
#
vlan 3
 description toAAAserver
#
interface Vlan-interface1
#
interface Vlan-interface2
 description toClients
 ip address 2.2.2.29 255.255.255.0
#
interface Vlan-interface3
 description toAAAservers
 ip address 3.3.3.29 255.255.255.0
#
```

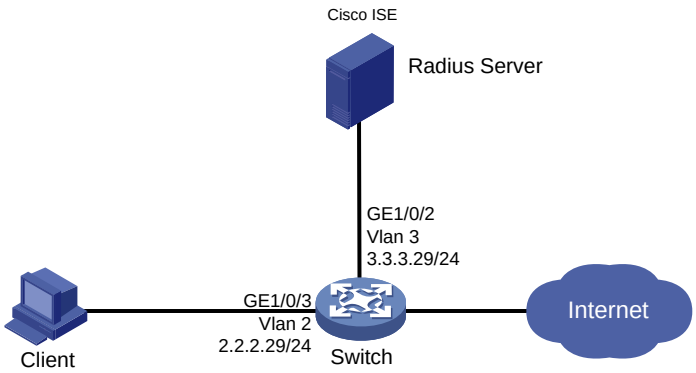
```
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 2
 dot1x
#
radius scheme ise
 primary authentication 3.3.3.24 key cipher $c$3$2oLOvHdRilTBlb6n1yh3/MoXN8z/RMbctQ==
 primary accounting 3.3.3.24 key cipher $c$3$fAhWH/rHm9hCcPq2PBWQa54YG9xKuQ1P0w==
 timer realtime-accounting 20 second
 user-name-format keep-original
#
#
domain test.com
 authentication default radius-scheme ise
 authorization default radius-scheme ise
 accounting default radius-scheme ise
#
```

13 SSH 登录时使用 HWTACACS 认证对接操作举例

13.1 组网需求

如图 13-1 所示，设备管理员希望 PC 使用 SSH 登录 Switch 时，通过使用 ISE 服务器进行远程 HWTACACS 认证，登录 Switch 后，验证为 level-15 用户角色，并且使 level-15 用户角色执行 **display cpu-usage** 命令无效。

图13-1 HWTACACS 认证组网图



13.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch：S5560X-R6618P27
- 认证服务器: Cisco ISE V2.4.0.357 patch 8
- 系统：Windows 10 21H2
- 认证客户端：iNode PC 7.3 (E513)

13.3 配置步骤

说明

本配置仅展示认证的相关配置，网络互通的相关配置略，请保证设备间能够互相访问。

13.3.1 配置 Switch

(1) 配置 HWTACACS 方案

创建名称为 ise 的 HWTACACS 方案并进入该方案视图。

```
<Switch> system-view
[Switch] hwtacacs scheme ise
```

配置认证/计费服务器 IP 地址为 3.3.3.24，认证/授权、计费报文的共享密钥为 expert。

```
[Switch-hwtacacs-ise] primary authorization 3.3.3.24 key simple expert
[Switch-hwtacacs-ise] primary authentication 3.3.3.24 key simple expert
[Switch-hwtacacs-ise] primary accounting 3.3.3.24 key simple expert
```

配置发送给 HWTACACS 服务器的用户名不携带 ISP 域名。

```
[Switch-radius-ise] user-name-format keep-original
```

(2) 配置 ISP 域

创建并进入名称为 ise 的 ISP 域。并将认证、授权和计费的方式配置为使用 HWTACACS 方案 ise。

```
[Switch] domain ise
[Switch-isp-ise] authentication login hwtacacs-scheme ise
[Switch-isp-ise] authorization login hwtacacs-scheme ise
[Switch-isp-ise] accounting login none
[Switch-isp-ise] authorization command hwtacacs-scheme ise
[Switch-isp-ise] accounting command hwtacacs-scheme ise
[Switch-isp-ise] quit
```

配置系统缺省的 ISP 域 ise，所有接入用户共用此缺省域的认证和计费方法。若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方法。

```
[Switch] domain default enable ise
```

(3) 配置 SSH 认证

生成 RSA 密钥对。

```
[Switch] public-key local create rsa
The range of public key modulus is (512 ~ 4096).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
```

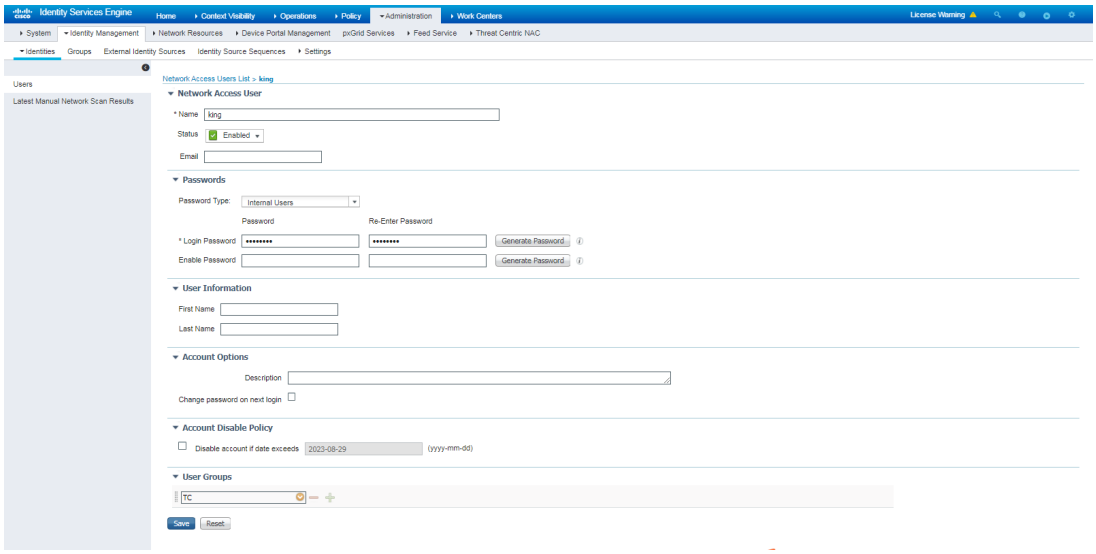
```
...
Create the key pair successfully.
```
生成 DSA 密钥对。
```
[Switch] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
........
Create the key pair successfully.
```
使能 SSH 服务器功能。
```
[Switch] ssh server enable
```
设置 SSH 客户端登录用户界面的认证方式为 scheme，并使能命令行授权功能、命令行审计功能。
```
[Switch] line vty 0 63
[Switch-line-vty0-63] authentication-mode scheme
[Switch-line-vty0-63] command authorization
[Switch-line-vty0-63] command accounting
[Switch-line-vty0-63] quit
```
使能缺省用户角色授权功能
```
[Switch] role default-role enable
```

13.3.2 配置 ISE 服务器

(1) 创建用户账号

在页面上方导航栏中选择[Work Centers/Switch Administration/Identities/Users]选项，点击<Add>按钮，创建名称为 king 的新帐号，配置密码为 king。

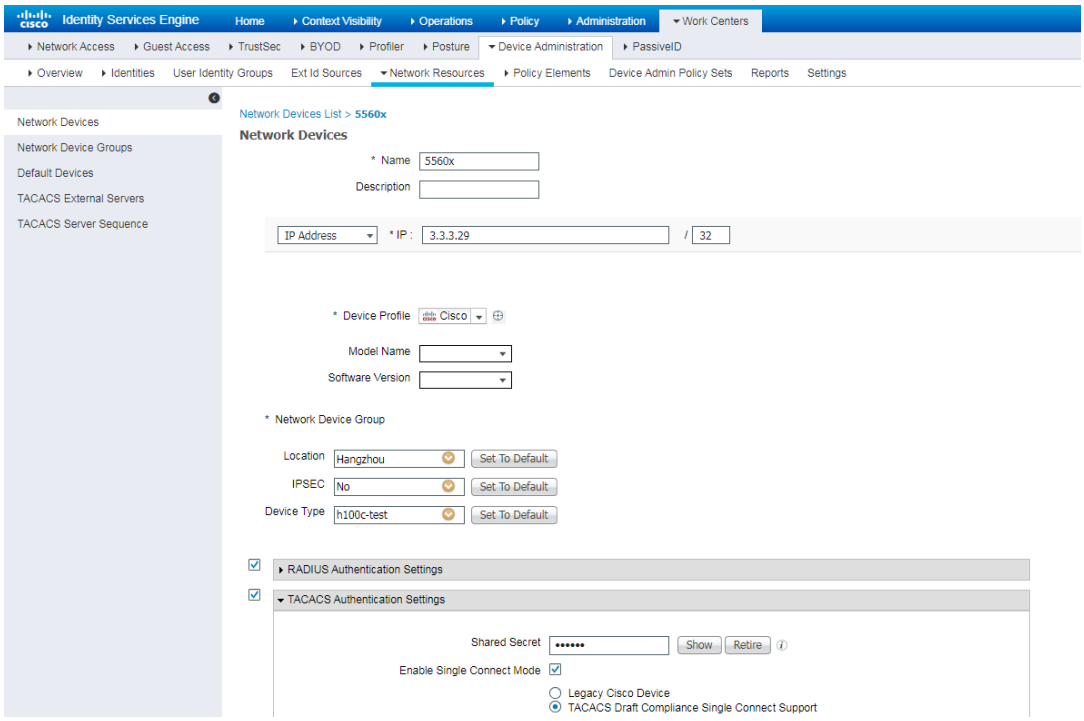
图13-2 创建用户账号



(2) 添加 Switch 设备

在页面上方导航栏中选择[Switch Administration/Network Resources/Network Switchs]选项，点击<Add>按钮，添加名称为 5560x 的新设备，配置 IP 地址为 3.3.3.29，勾选 TACACS Authentication Settings 栏，配置密码 expert。

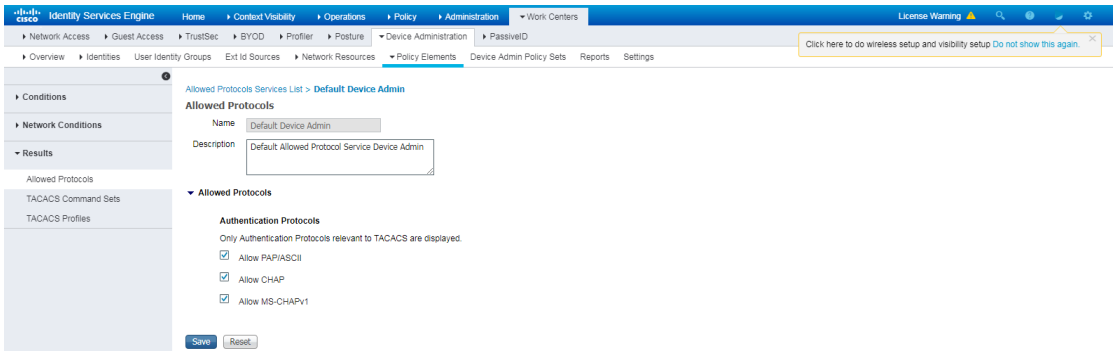
图13-3 添加 Switch 设备



(3) 配置认证协议

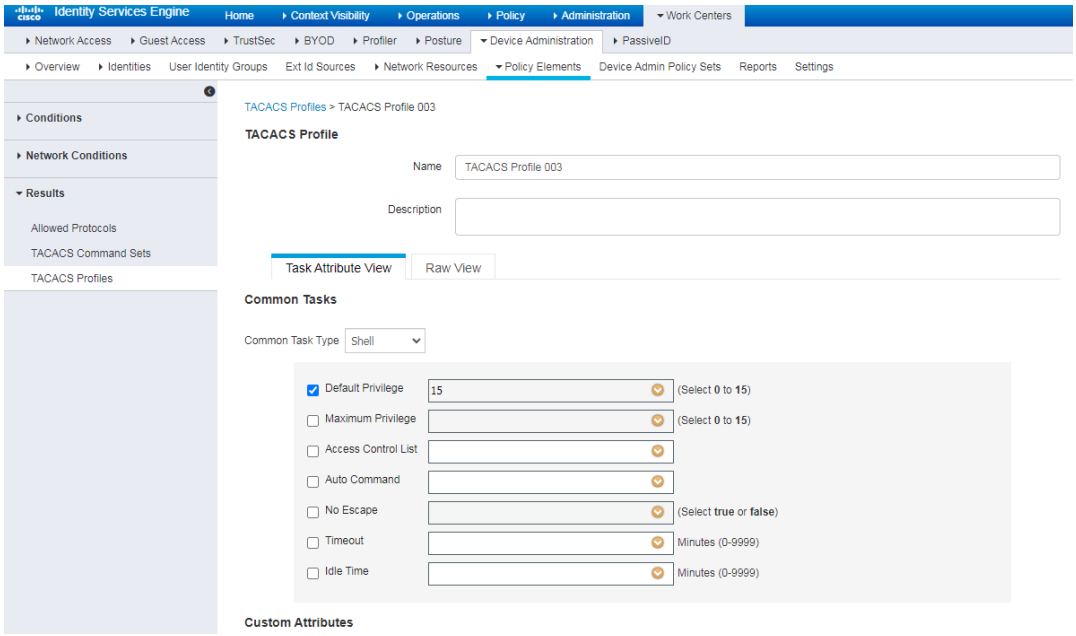
配置认证协议：在页面上方导航栏中选择[Switch Administration/Policy Elements/Results/Allowed Protocols]选项，确认默认的策略“Default Switch Admin”协议勾选情况。

图13-4 配置认证协议



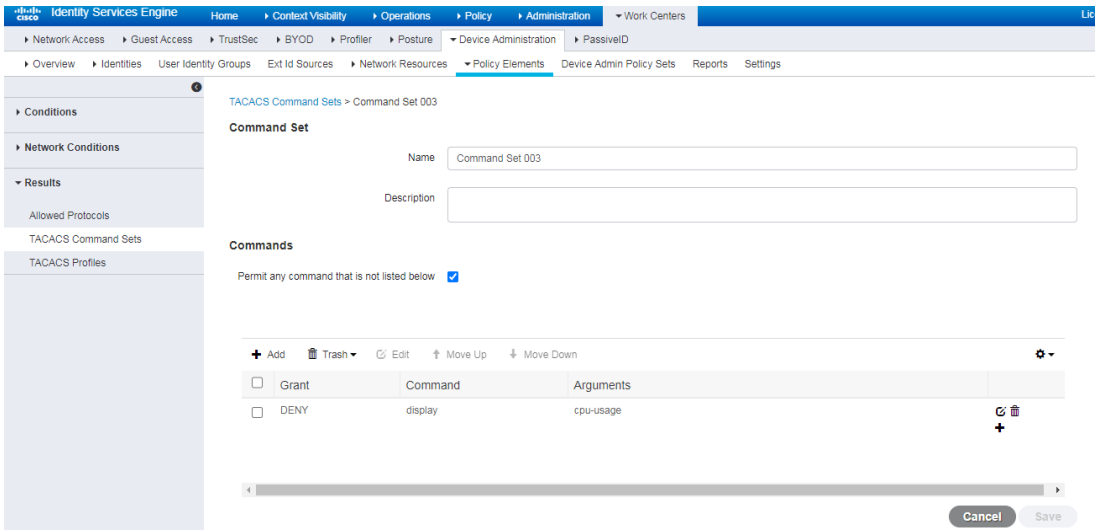
配置 TACACS 授权用户角色：在页面上方导航栏中选择[Switch Administration/Policy Elements/Results/TACACS Profiles]选项，点击<Add>按钮，新建名称为名称为 TACACSProfile1 的命令集，配置 Default Privilege 为 level15。

图13-5 配置授权用户角色



配置 TACACS 授权命令行集合：在页面上方导航栏中选择[Switch Administration/Policy Elements/Results/TACACS Command Sets]选项，点击<Add>按钮新建名称为 CommandSet1 的命令集，配置不允许执行命令 **`display cpu-usage`**；在 Commands 栏中勾选 Permit any commandthat is mot listed below，允许执行其他命令。

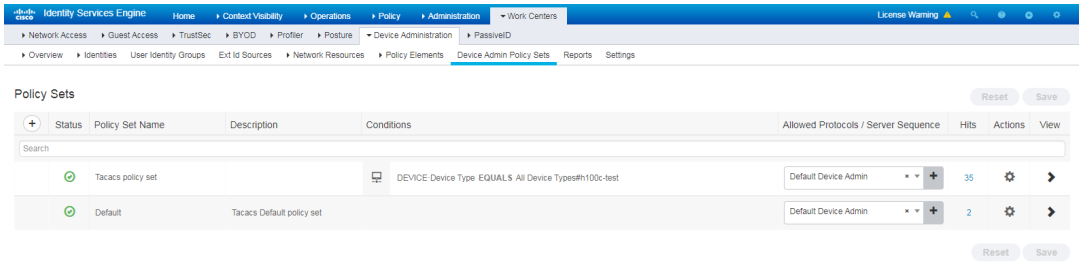
图13-6 配置授权命令行集合



(4) 配置认证和授权策略

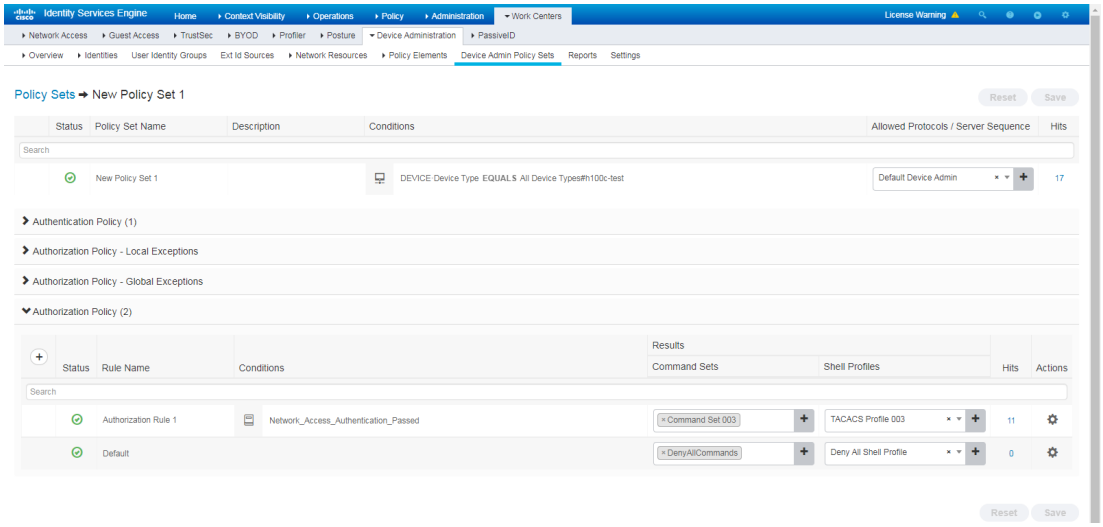
新建认证策略：在页面上方导航栏中选择[Switch Administration/Switch Admin Policy Sets]选项，点击<＋>按钮新建。

图13-7 新建认证策略



设置认证策略和授权策略：点击上图认证策略 a 后面的<View>按钮，在 Authorization Policy 中新建，并指定授权策略下发 TACACS 角色和 TACACS 命令集。

图13-8 设置认证策略和授权策略

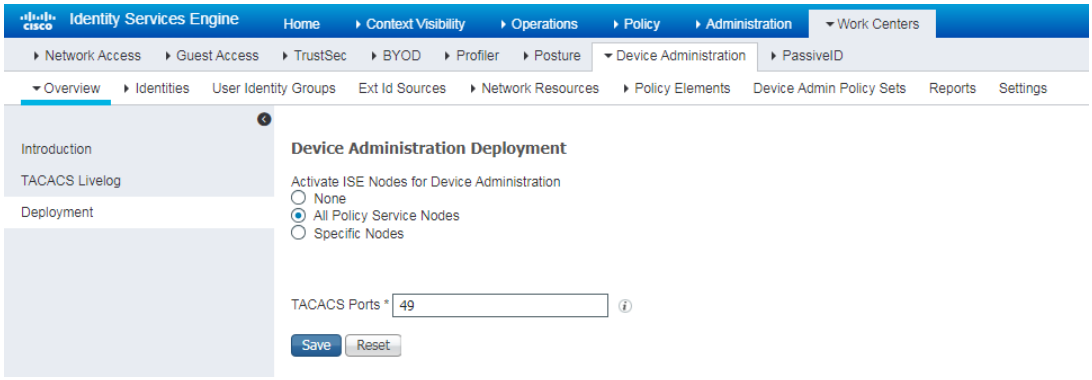


(5) 开启设备管理服务

To activate ISE Nodes for Switch Administration，

选择[Work Centers/Switch Administration/Overview/ Deployment] 选项，确认选中了需要的 node

图13-9 Deployment 页面



13.4 验证配置

13.4.1 配置 SSH 客户端

说明

SSH 客户端软件有很多，例如 PuTTY、OpenSSH 等。本文中仅以客户端软件 PuTTY0.76 为例，说明 Stelnet 客户端的配置方法。

安装 PuTTY 0.76 软件。

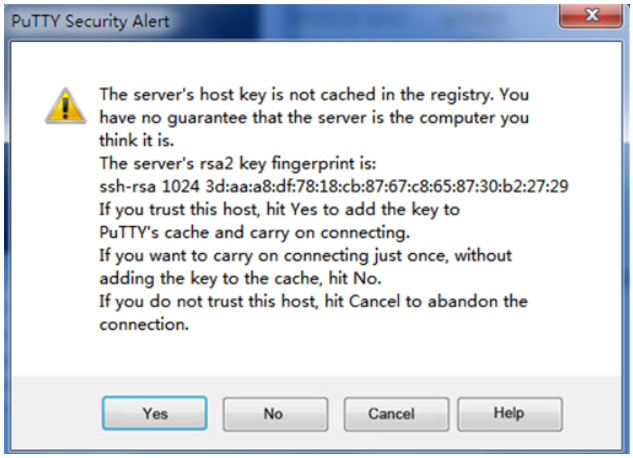
打开 PuTTY.exe 程序，点击“Session”功能区：

- 在“Host Name（or IP address）”文本框中输入 SSH 服务器的 IP 地址。
- 在“Port”文本框中输入 SSH 协议端口号 22。
- 在“Connection type”区域选择 SSH 协议。

单击<Open>按钮。

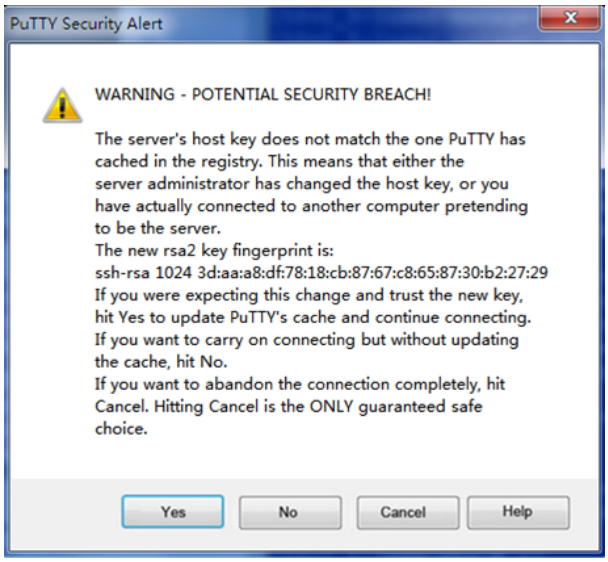
如果弹出图 13-10 所示“PuTTY Security Alert”对话框，请根据实际情况做出选择。本例中选择信任该服务器，则单击“Yes”按钮。

图13-10 SSH 客户端登录界面（一）



如果弹出图 13-11 所示“PuTTY Security Alert”对话框，请根据实际情况做出选择。本例中选择信任该主机密钥，则单击“Yes”按钮。

图13-11 SSH 客户端登录界面（二）



在如下登录界面中输入用户名“king”和密码“king”，即可成功登录设备。

```
login as: king
king@55.73.134.29's password:
******************************************************************************
* Copyright (c) 2004-2021 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************
<Switch>
```

13.4.2 验证授权命令

角色 15 允许访问的命令，比如 **display memory** 可以正常访问；deny 的命令 **display cpu-usage** 无法访问，提示 Permission denied。

```
[Switch]display memory
Memory statistics are measured in KB:
Slot 1:
             Total      Used      Free    Shared   Buffers    Cached   FreeRatio
Mem:       2036432    785096   1251336         0      1472    258008       62.0%
-/+ Buffers/Cache:    525616   1510816
Swap:            0         0         0
LowMem:    1651408    400692   1250716        --        --        --       75.7%
HighMem:    385024    384404       620        --        --        --        0.2%

[Switch]display cpu-usage
Permission denied.
```

输入 **display users** 可以看到目前登录的用户角色为 level-15。

```
[Switch]display users
```

```
  Idx   Line      Idle        Time                Pid      Type
+ 10    VTY 0     00:00:00    Oct 17 20:11:40     105288   SSH

Following are more details.
VTY 0    :
        User name: king
        User role list: level-15
        Location: 55.73.134.88
```

13.4.3 查看服务器端相关日志

选择页面上方的[Work Centers/Switch Administration/Overview/TACACA Livelog]中可以看到认证相关的日志。

图13-12 TACACA Livelog

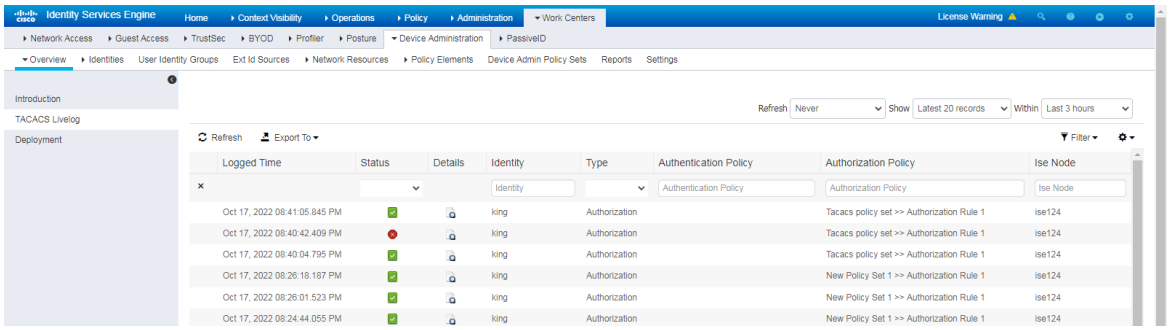
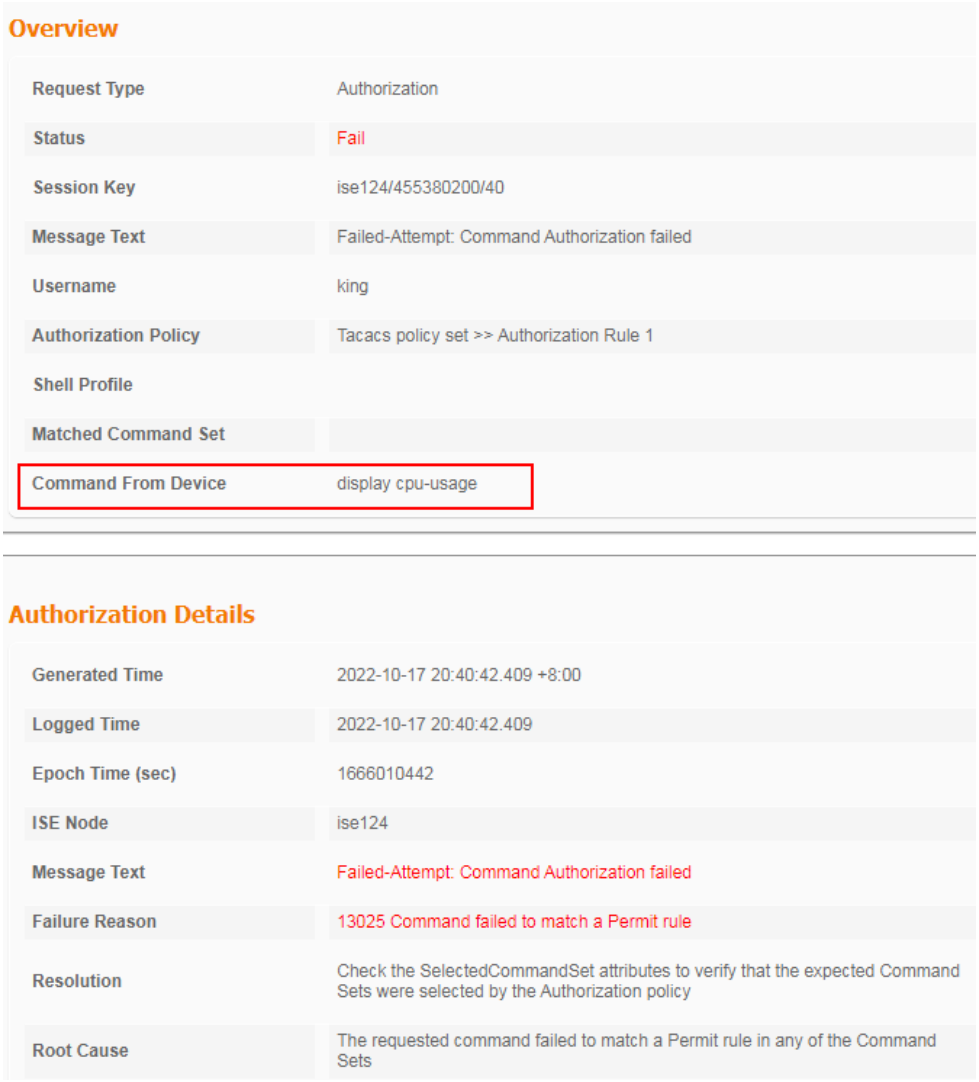


图13-13 设备输入 display cpu-usage 命令被阻止



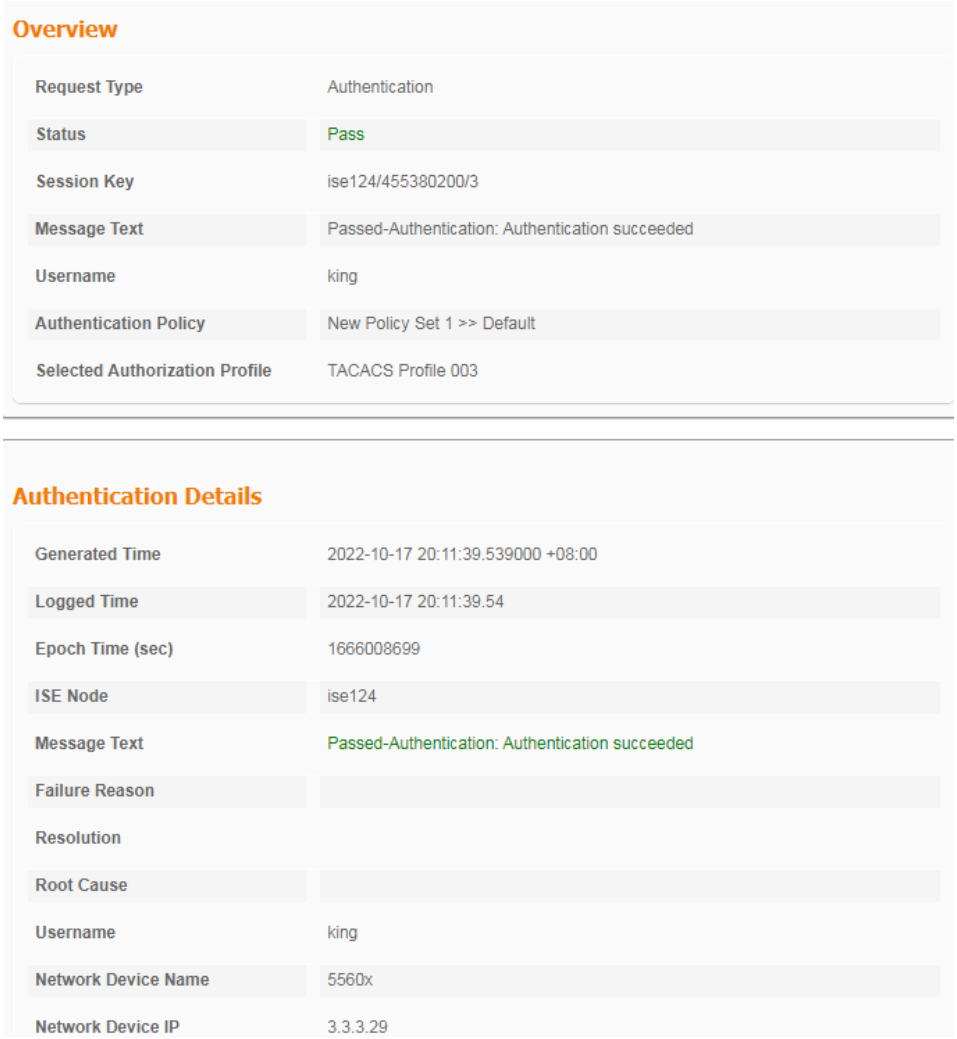
Overview

Request Type	Authorization
Status	Fail
Session Key	ise124/455380200/40
Message Text	Failed-Attempt: Command Authorization failed
Username	king
Authorization Policy	Tacacs policy set >> Authorization Rule 1
Shell Profile	
Matched Command Set	
Command From Device	display cpu-usage

Authorization Details

Generated Time	2022-10-17 20:40:42.409 +8:00
Logged Time	2022-10-17 20:40:42.409
Epoch Time (sec)	1666010442
ISE Node	ise124
Message Text	Failed-Attempt: Command Authorization failed
Failure Reason	13025 Command failed to match a Permit rule
Resolution	Check the SelectedCommandSet attributes to verify that the expected Command Sets were selected by the Authorization policy
Root Cause	The requested command failed to match a Permit rule in any of the Command Sets

图13-14 TACACS 登录成功



13.5 配置文件

```
#
hwtacacs scheme ise
primary authentication 3.3.3.24 key cipher $c$3$wUwB4o8ka2I7ajzobLbwHsYtDKub7VhEdA==
 primary authorization 3.3.3.24 key cipher $c$3$/Eh17X/LhZiOsed29CU4/fKGEtpwjCT6Pg==
 primary accounting 3.3.3.24 key cipher $c$3$SkVBs/z9WNAvWzgTNx1mZSs0reEKR+7EOQ==
 user-name-format without-domain
#
domain ise
 authentication login hwtacacs-scheme ise
 authorization login hwtacacs-scheme ise
 accounting login none
 authorization command hwtacacs-scheme ise
 accounting command hwtacacs-scheme ise
#
```

```
public-key local create rsa
#
public-key local create dsa
#
ssh server enable
#
role default-role enable
#
line vty 0 31
 authentication-mode scheme
 command authorization
 command accounting
#
```

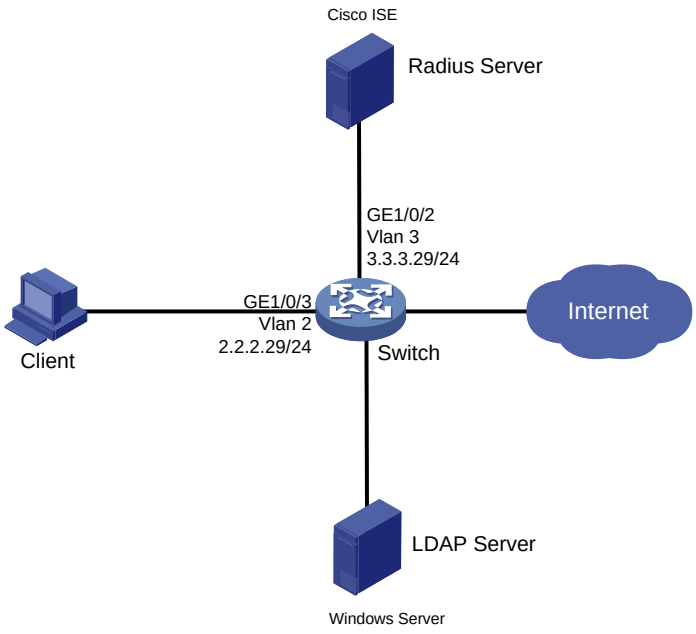
14 使用 LDAP 账户认证对接配置举例

14.1 组网需求

如图 14-1 所示，Client 和 ISE 服务器及 LDAP 服务器（Windows Server）通过 Switch 建立连接，设备管理员希望对 Client 进行 802.1X 认证，以控制其对网络资源的访问，具体要求如下：

- 采用 Cisco ISE 作为 RADIUS 服务器。
- 采用 Windows Server 中的用户名密码。

图14-1 LDAP 认证配置组网图



14.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch：S5560X-R6618P27
- 认证服务器: Cisco ISE V2.4.0.357 patch 8
- 系统：Windows 10 21H2
- 认证客户端：iNode PC 7.3 (E513)

  LDAP 服务器：Windows Server 2012R2

14.3 认证配置步骤与验证

说明

本配置仅展示认证的相关配置，网络互通的相关配置略，请保证设备间能够互相访问。

14.3.1 配置 Switch

设备上确认认证方式配置为 EAP，后续以认证方式 PEAP (EAP-GTC)举例，其他配置请参考 4.3.1 配置 Switch。

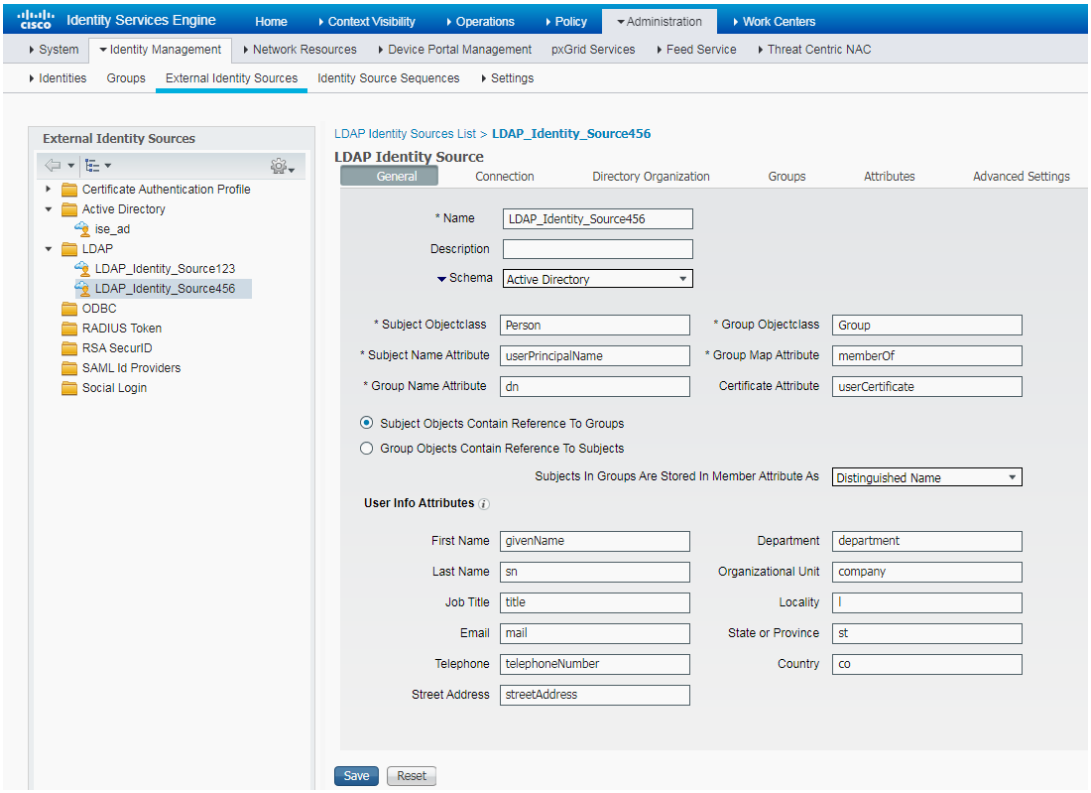
```
[Switch] dot1x authentication-method EAP
```

14.3.2 配置 ISE

(1) 新建 External Identity Sources

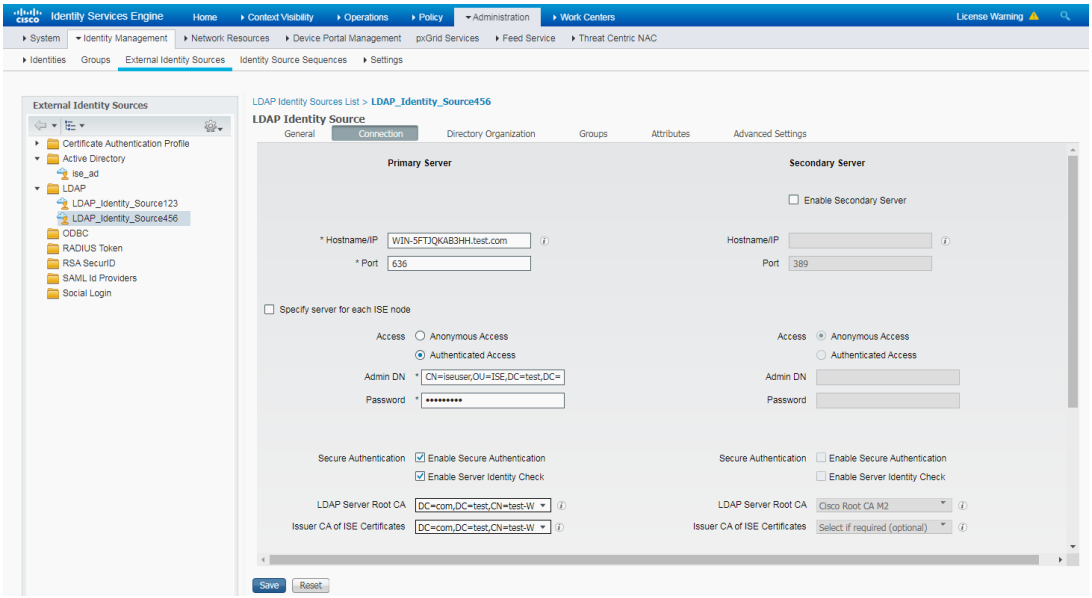
在页面上方导航栏中选择[Administration/Identity Management/ External Identity Sources/LDAP]选项，点击<Add>按钮，创建名称为 LDAP_Identity_Source456 的 LDAP Identity Source。

图14-2 新建 External Identity Sources



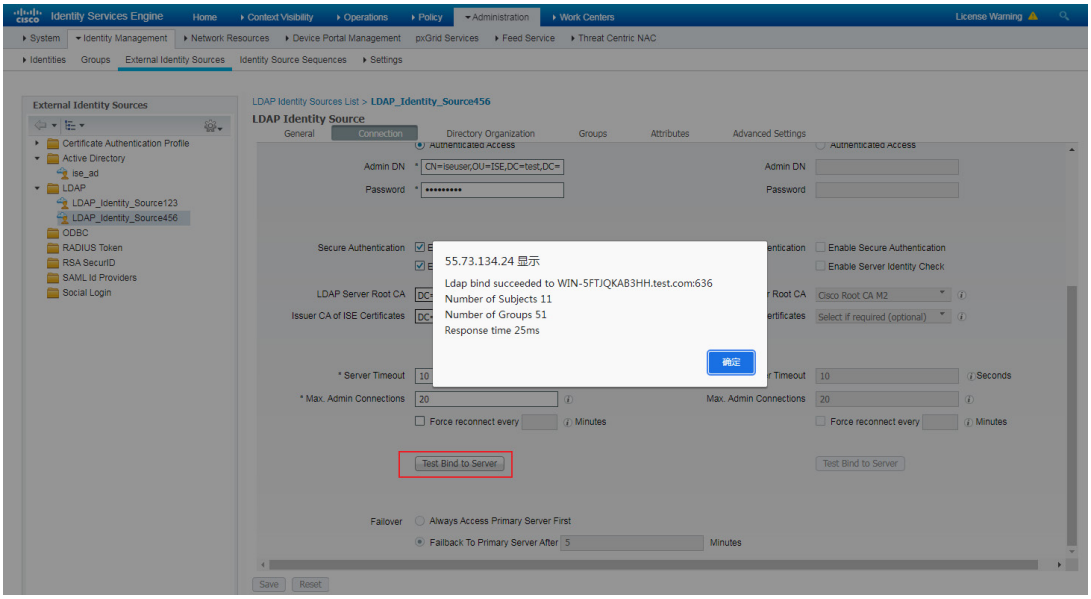
为保证安全性，以 LDAPS 方式连接 LDAP server 举例，在 Connection 标签页，填入 ldap server 的 Hostname/IP，LDAPS 端口号为 636，若以 LDAP 方式连接，端口号为 389。在 ldap server 获取其他参数填入其他位置，具体请参考 Windows Server 相关手册。

图14-3 修改 Connection 标签页参数



点击<Test Bind to Server>，可以看到已经成功连接上。

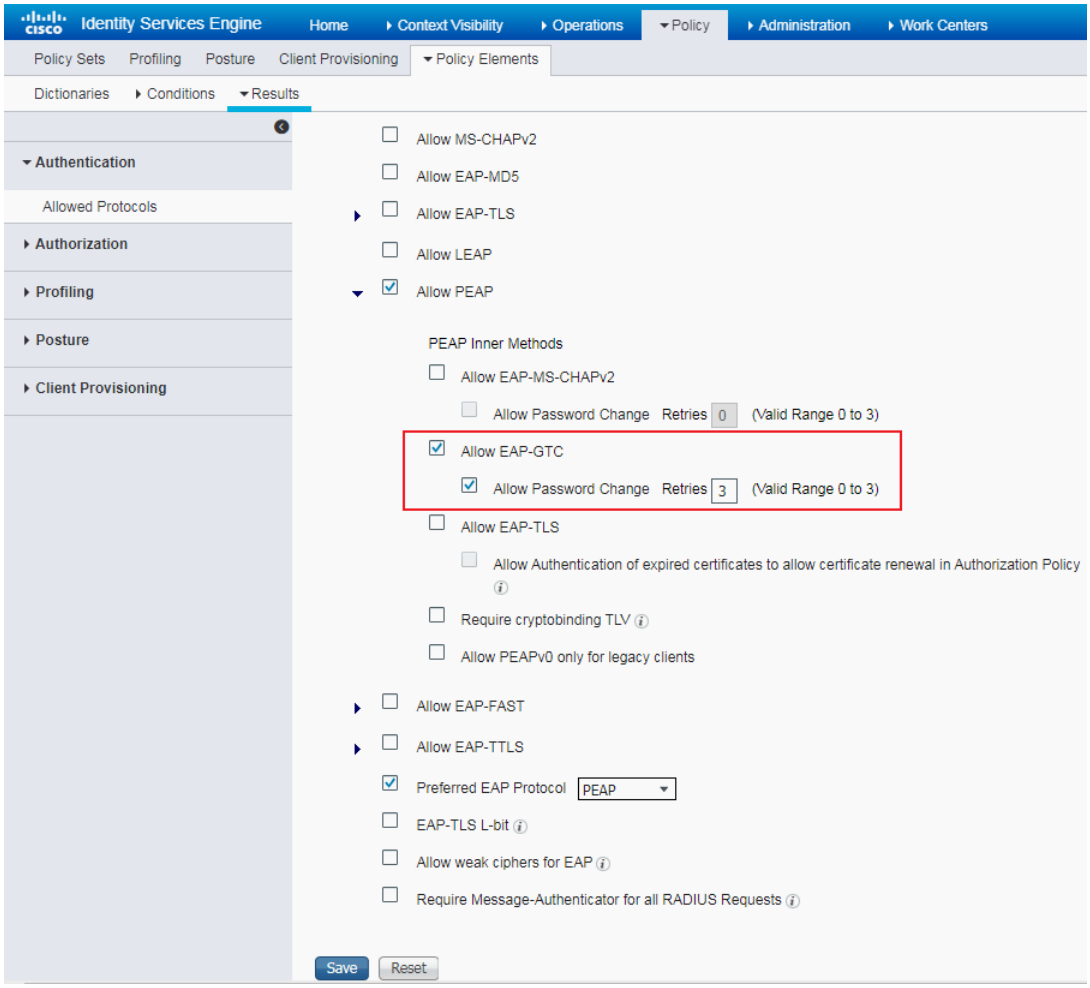
图14-4 连接成功



(2) 配置认证协议

在页面上方导航栏中选择[Policy/Policy Elements/Results/Authentication/Allowed Protocols]选项，新建名称为 1x_EAP-PEAP-GTC，并确保勾选 EAP-GTC。

图14-5 配置认证协议



(3) 配置认证和授权策略

在页面上方导航栏中选择[Policy/Policy Sets]选项，点击 Policy Sets 下方的<+>按钮，配置名称 1x-id through LDAPS 的认证和授权策略。

图14-6 图 1-18 新建 Policy

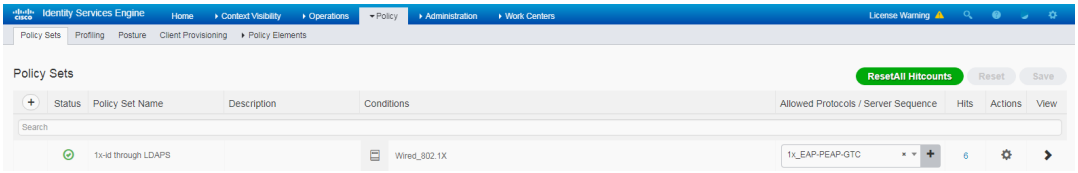
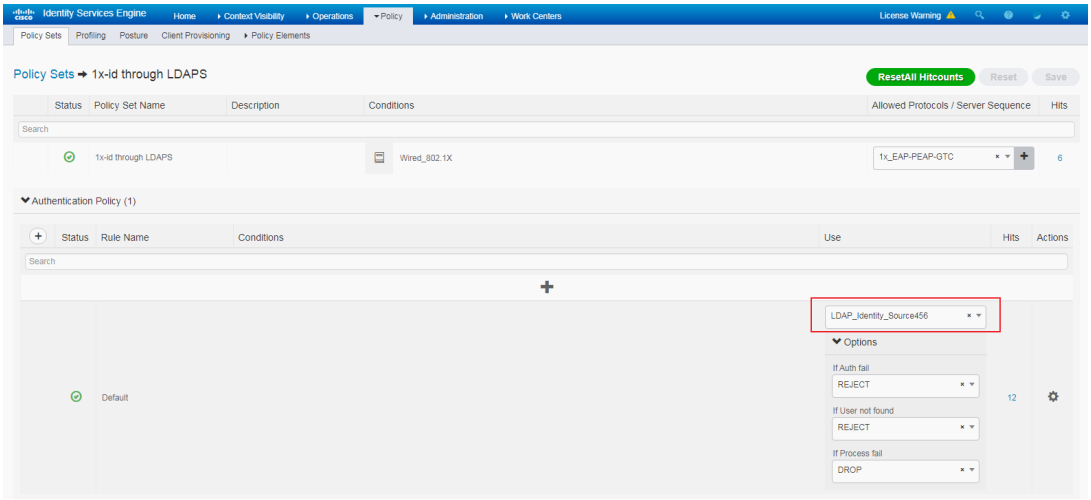


图14-7 Use LDAP_Identity_Source456

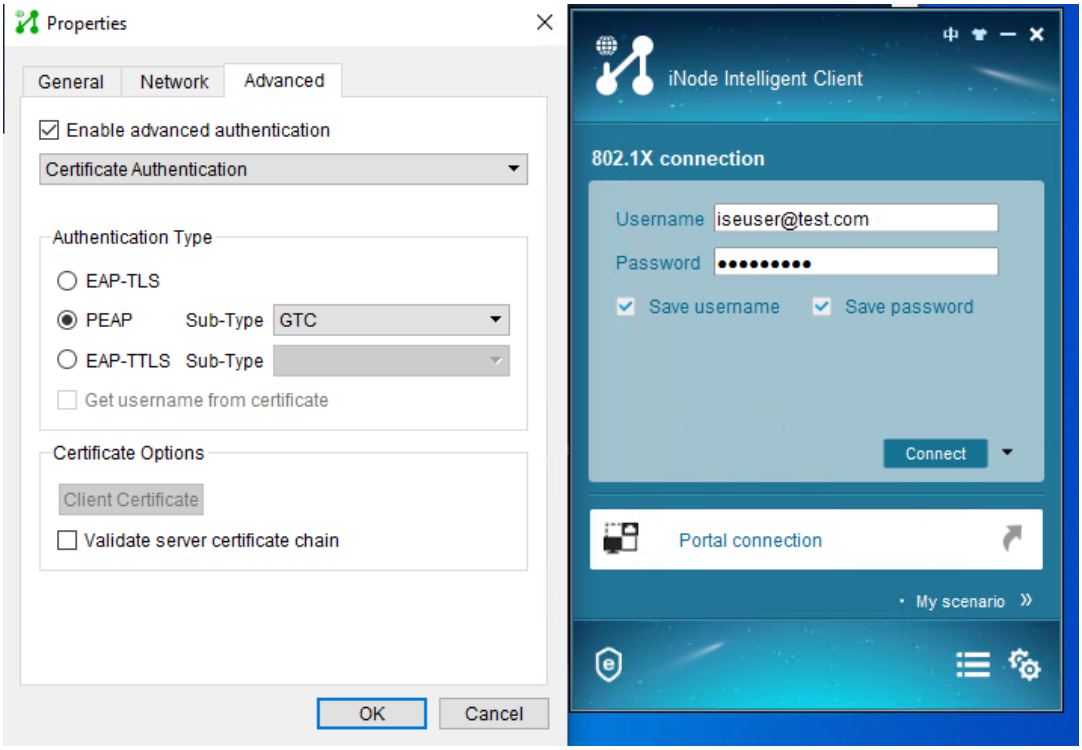


14.3.3 验证配置

(1) Windows 客户端上使用 iNode 登录

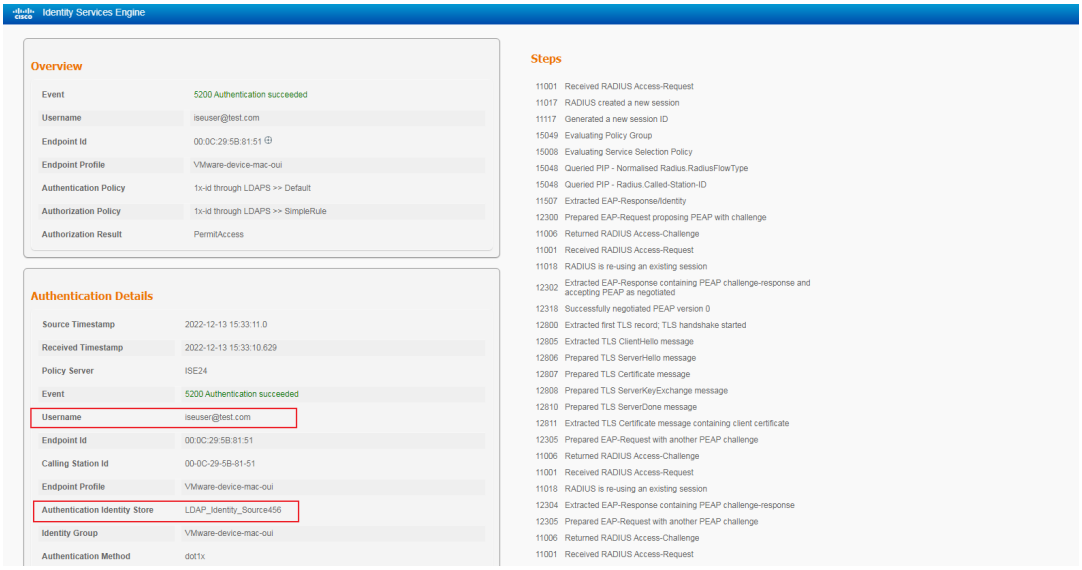
在 iNode 填入已经在 Windows Server 已经创建好的用户名密码，在 Properties 中选择 Authentication Type 为 PEAP，Sub-Type 为 GTC。

图14-8 iNode 登录



(2) 用户上线后服务器日志显示

图14-9 用户上线后服务器日志显示



(3) 用户上线后设备的显示信息

通过在设备上执行 **display dot1x connection** 可以看到上线用户的信息。

```
<Switch> display dot1x connection
Total connections: 1
Slot ID: 1
```

```
User MAC address: 000c-295b-8151
Access interface: GigabitEthernet1/0/21
Username: iseuser@test.com
User access state: Successful
Authentication domain: test.com
IPv4 address: 2.2.2.2
IPv4 address source: IP Source Guard
EAP packet identifier: 200
Authentication method: EAP
AAA authentication method: RADIUS
Initial VLAN: 2
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Authorization IPv6 URL: N/A
Authorization temporary redirect: Disabled
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: N/A
Online from: 2022/12/13 15:33:10
Online duration: 0h 1m 17s
```

14.4 配置文件

```
#
 dot1x
 dot1x authentication-method eap
#
vlan 1
#
vlan 2
 description toClients
 arp snooping enable
#
vlan 3
 description toAAAserver
#
interface Vlan-interface1
#
interface Vlan-interface2
 description toClients
```

```
 ip address 2.2.2.29 255.255.255.0
#
interface Vlan-interface3
 description toAAAservers
 ip address 3.3.3.29 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 2
 dot1x
#
radius scheme ise
 primary authentication 3.3.3.24 key cipher $c$3$2oLOvHdRilTBlb6n1yh3/MoXN8z/RMbctQ==
 primary accounting 3.3.3.24 key cipher $c$3$fAhWH/rHm9hCcPq2PBWQa54YG9xKuQ1P0w==
 timer realtime-accounting 20 second
 user-name-format keep-original
#
#
domain test.com
 authentication default radius-scheme ise
 authorization default radius-scheme ise
 accounting default radius-scheme ise
#
```

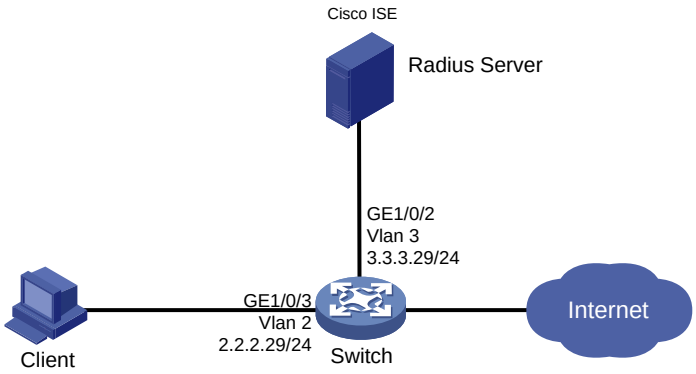
15 终端识别 Profiling 对接配置举例

通过 SNMP+LLDP 识别终端配置举例。

15.1 组网需求

如图 15-1 所示，Client 和 ISE 服务器通过 Switch 建立连接，设备管理员希望对 Client 进行终端识别。

图15-1 终端识别 Profiling 对接配置组网图



15.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch：S5560X-R6618P27
- 认证服务器: Cisco ISE V2.4.0.357 patch 8
- 系统：Windows 10 21H2
- 认证客户端：iNode PC 7.3 (E513)

15.3 配置步骤

说明

本配置仅展示终端识别相关配置，网络互通或者认证的相关配置略，请保证设备间能够互相访问。

15.3.1 配置 Switch

创建 SNMP 团体并配置设备支持的 SNMP 版本，Swtich 上的其他配置请参考 4.3.1 配置 Switch。

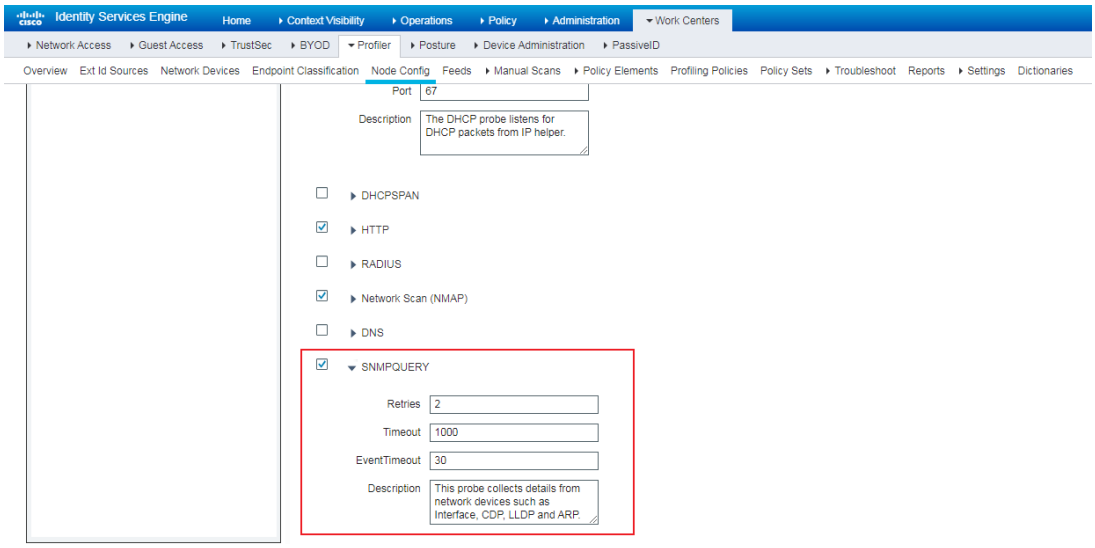
```
[Switch] snmp-agent community read simple public
[Switch] snmp-agent sys-info version all
```

15.3.2 配置 ISE

(1) 配置探针

在页面上方导航栏中选择[Work Centers/Profiler/Node Config/Profiling Configuraton]选项，打开相关的属性探针，打开 SNMPQUERY。

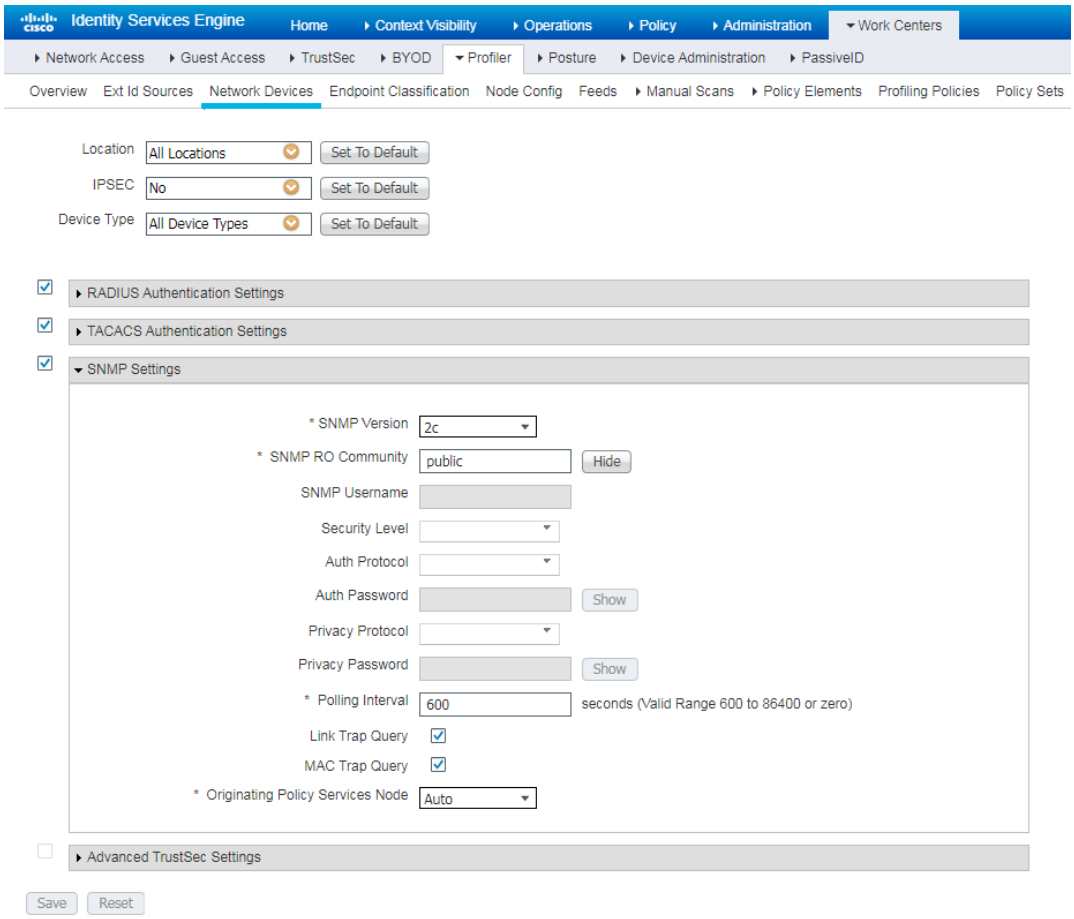
图15-2 配置探针



(2) 配置 SNMP

在页面上方导航栏中选择[Work Centers/Profiler/Network Devices]选项，选中对应的交换机，在 SNMP Settings 填写相关配置，保证 ISE 能够获取交换机 SNMP 信息。

图15-3 填写 SNMP Settings



15.4 Windows上配置

15.4.1 安装 lldp 相关模块

Win10 上在线或离线安装 lldp 相关模块，确保 Windows 能够发出 lldp 报文，并被交换机接收。

以离线安装为例，下载 WindowsTH-RSAT_WS2016-x64.msu（https://download.microsoft.com/download/1/D/8/1D8B5022-5477-4B9A-8104-6A71FF9D98AB/WindowsTH-RSAT_WS2016-x64.msu），以文件放到 C:\Downloads 为例。

管理员权限打开 cmd，输入如下命令：

MKDIR C:\Downloads\RSAT

MKDIR C:\Downloads\RSAT\x64

expand -f:* C:\Downloads\WindowsTH-RSAT_WS2016-x64.msu C:\Downloads\RSAT\x64

进入 C:\Downloads\RSAT\x64，并输入命令 Dism.exe /Online /Add-Package /PackagePath:".\WindowsTH-KB2693643-x64.cab"，等待安装成功。

15.4.2 打开 lldp 并验证效果

在 CMD 中输入命令，打开 lldp，Enable-NetLldpAgent -NetAdapterName "AAAuser"

图15-4 Win10（vmware 虚拟机）发出 lldp 报文

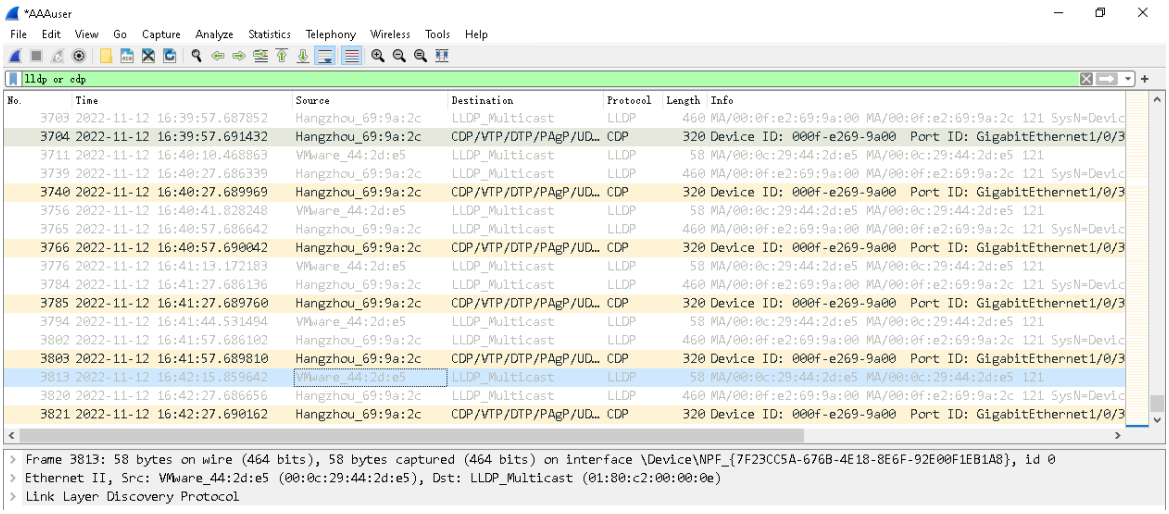


图15-5 交换机上收集到相关 lldp 信息

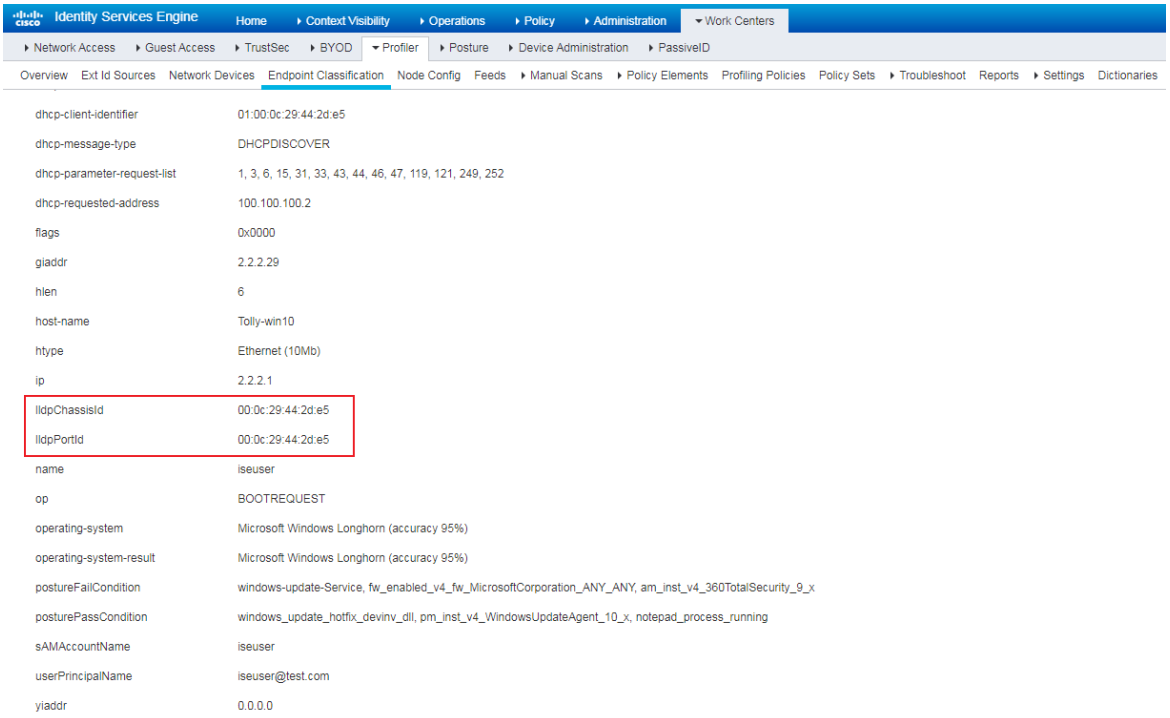
```
[Device]display lldp neighbor-information list
Chassis ID : * -- -- Nearest nontpmr bridge neighbor
             # -- -- Nearest customer bridge neighbor
             Default -- -- Nearest bridge neighbor
Local Interface Chassis ID      Port ID                 System Name
GE1/0/2         ISE24           eth1                    -
GE1/0/2         esxi67.test.com vmnic1                  -
GE1/0/3         000c-2944-2de5  000c-2944-2de5          -
GE1/0/3         esxi67.test.com vmnic2                  -
GE1/0/21        00dd-b690-f913  00dd-b690-f913          -
GE1/0/21        localhost       vmnic6                  -
GE1/0/22        00dd-b690-f912  00dd-b690-f912          -
GE1/0/22        ise31           eth1                    -
GE1/0/22        localhost       vmnic5                  -
MGE0/0/0        703a-a66c-f036  GigabitEthernet1/0/36   T-002011
```

15.5 Profile相关配置

15.5.1 查看 lldp 信息

之前配置 SNMP 章节可以看到最小间隔 10 分钟，等待后，在 endpoint classification 中找到对应的 endpoint，点击查看信息，可以看到已经关联了 lldp 信息。

图15-6 Endpoint 展示 lldp 信息

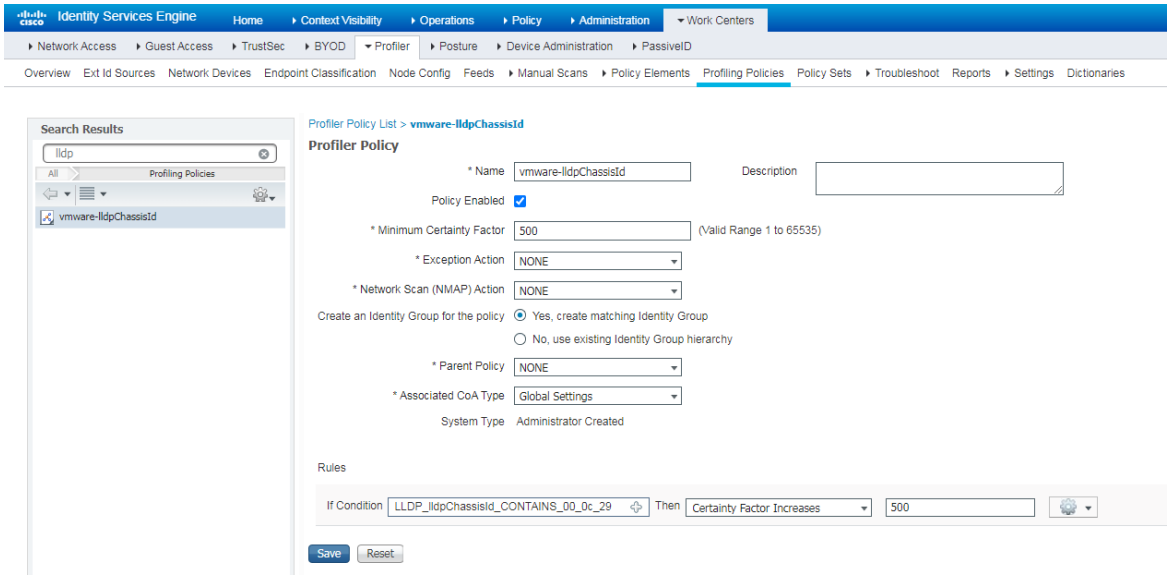


15.5.2 创建 Profiling Policy

创建 Profiling Policy，如果 endpoint 的 lldpChassisId 字段包含 00:0c:29 字段的话，就将 Certainty Factor 增加 500，最小满足 500，也即只要 endpoint 满足这个条件，就把他们划到一个组。

注意，如果 endpoint 可以匹配其他 Profiler Policy，并且 Certainty Factor 比这个 500 高的话，endpoint 最终最终会显示最高 Certainty Factor 的 Profiling Policy。

图15-7 新建 Profiling Policy



15.6 效果展示

图15-8 Endpoint Profile 显示 vmware-lldpChassisId

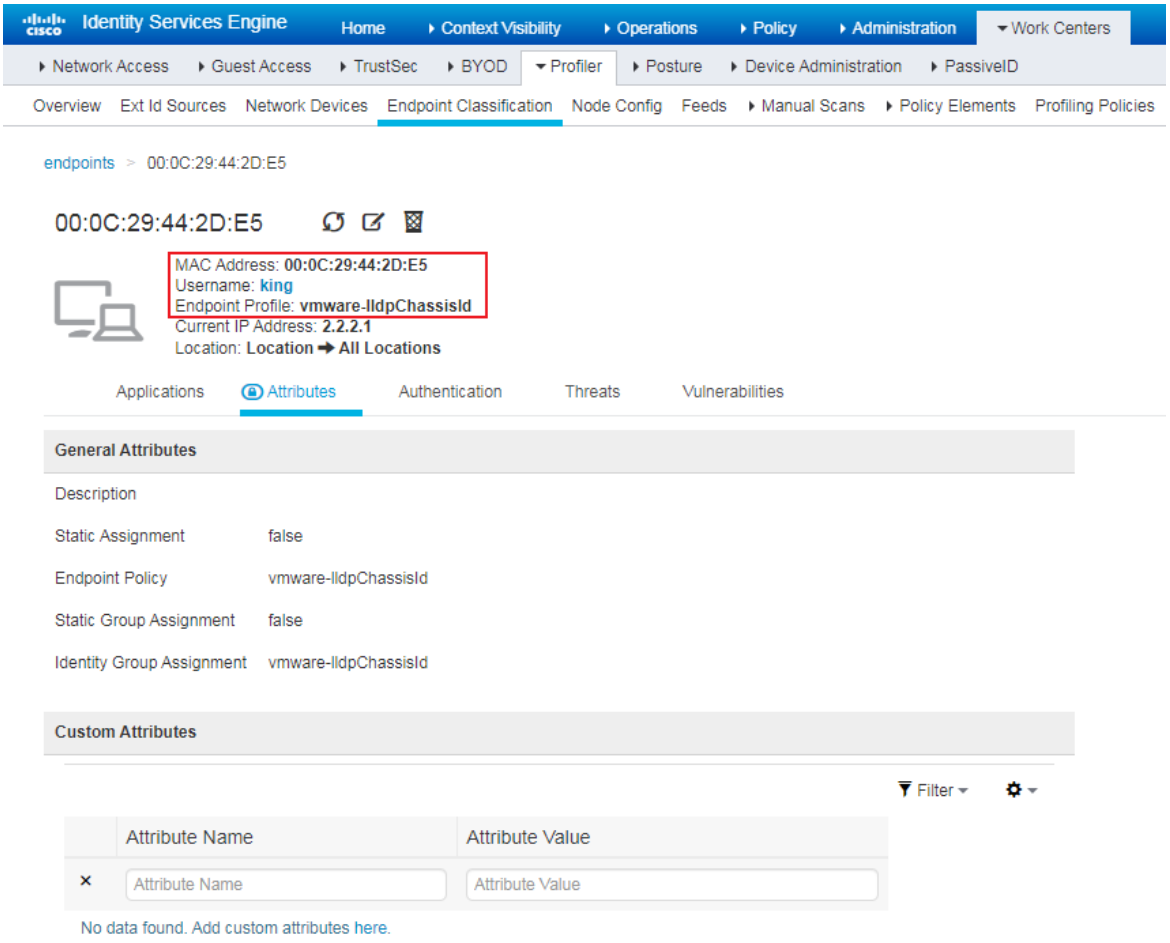
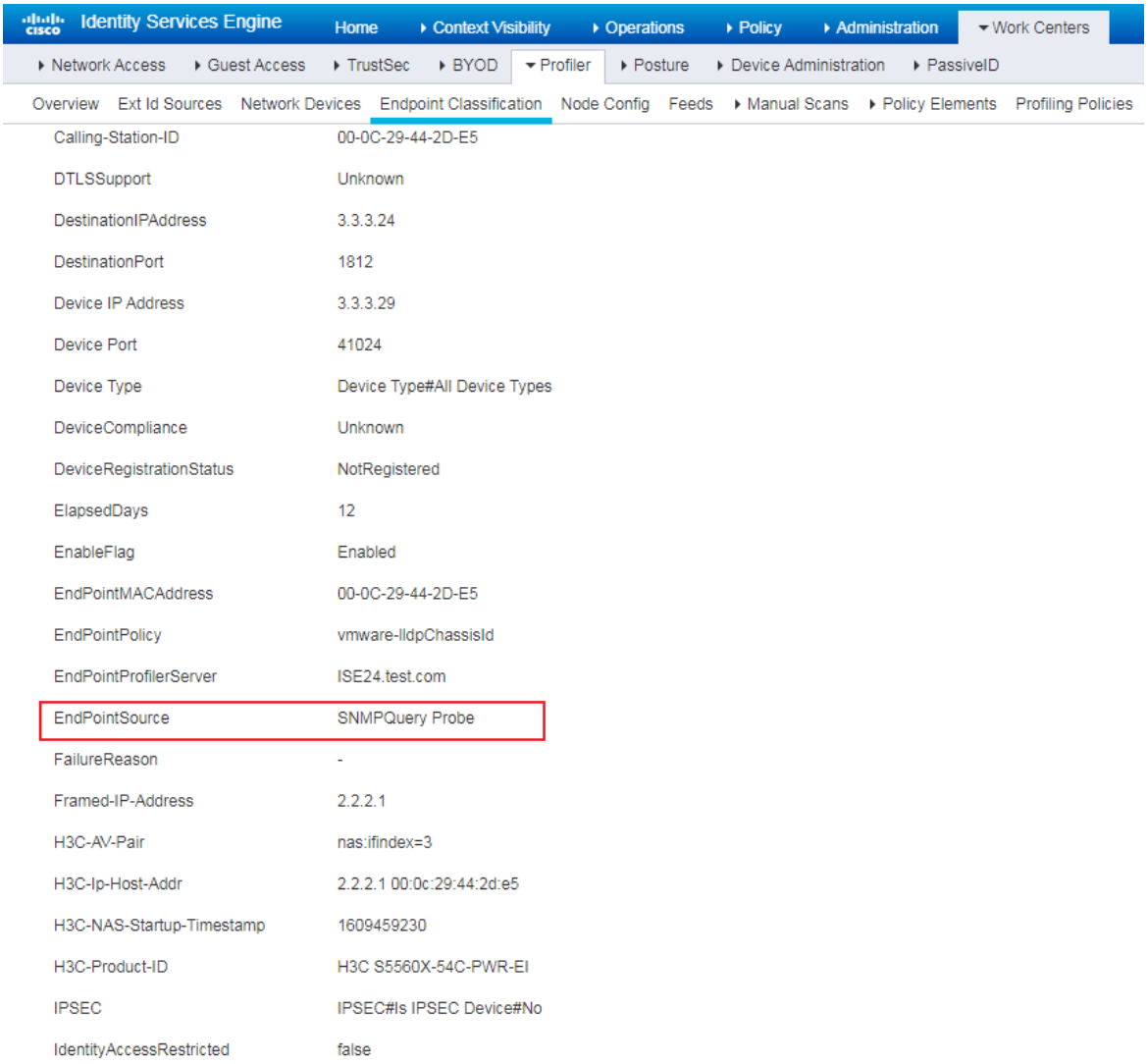


图15-9 EndPointSource 显示为 SNMPQuery Probe



15.7 配置文件

```
#
 snmp-agent
 snmp-agent community read cipher $c$3$KaeEzejbDaABoVp8gpCZyK8F7+BvOlj2jQ==
 snmp-agent sys-info version all
#
```

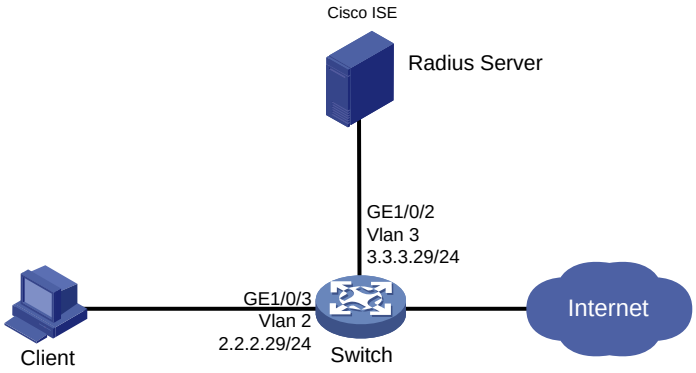
其他配置请参考相应的认证方式。

16 终端安全 Posture Assessment 对接配置举例

16.1 组网需求

如图 16-1 所示，Client 和 ISE 服务器通过 Switch 建立连接，设备管理员希望对 Client 进行 Posture Assessment

图16-1 终端安全 Posture Assessment 对接配置组网图



16.2 使用版本

本配置举例所使用的设备型号及版本信息如下：

- Switch：S5560X-R6618P27
- 认证服务器: Cisco ISE V2.4.0.357 patch 8
- 系统：Windows 10 21H2
- 认证客户端：iNode PC 7.3 (E513)

16.3 配置步骤

说明

本配置仅展示终端安全的相关配置，网络互通的相关配置略，请保证设备间能够互相访问。

16.3.1 配置 Switch

本举例以 802.1X 环境为例，Swtich 上的配置请参考 4.3.1 配置 Switch。

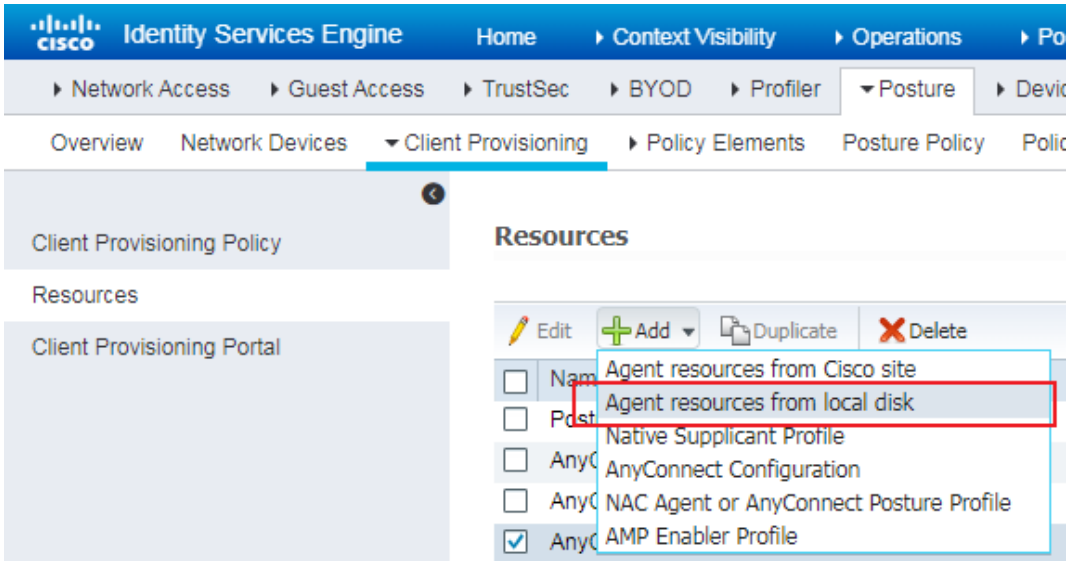
16.3.2 配置 ISE

(1) 上传 Client provision 所需资源

在页面上方导航栏中选择[Work Centers/Posture/Client Provisioning/Resources]选项，点击“Add”，选择 Agent resources from local disk 上传电脑本地文件，如果 ise 服务器可以连接互联网的话，也可以选择 from cisco site。

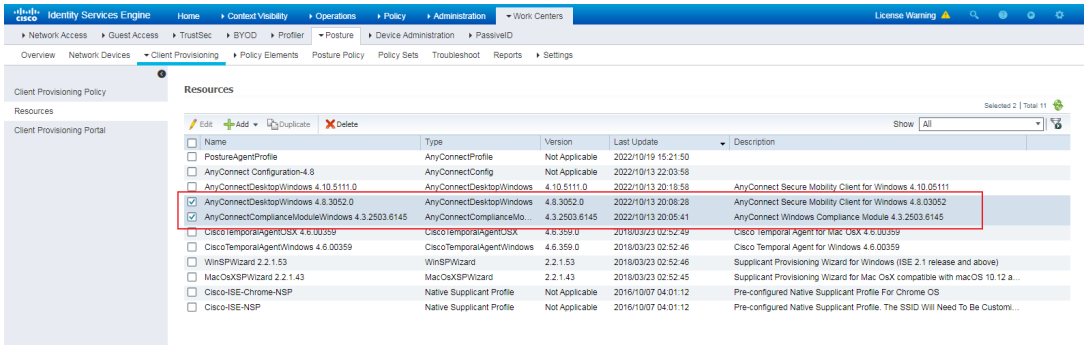
相关文件可通过 CISCO 网站等方式获取。

图16-2 上传文件



所上传的文件如红框所示

图16-3 已上传文件的展示

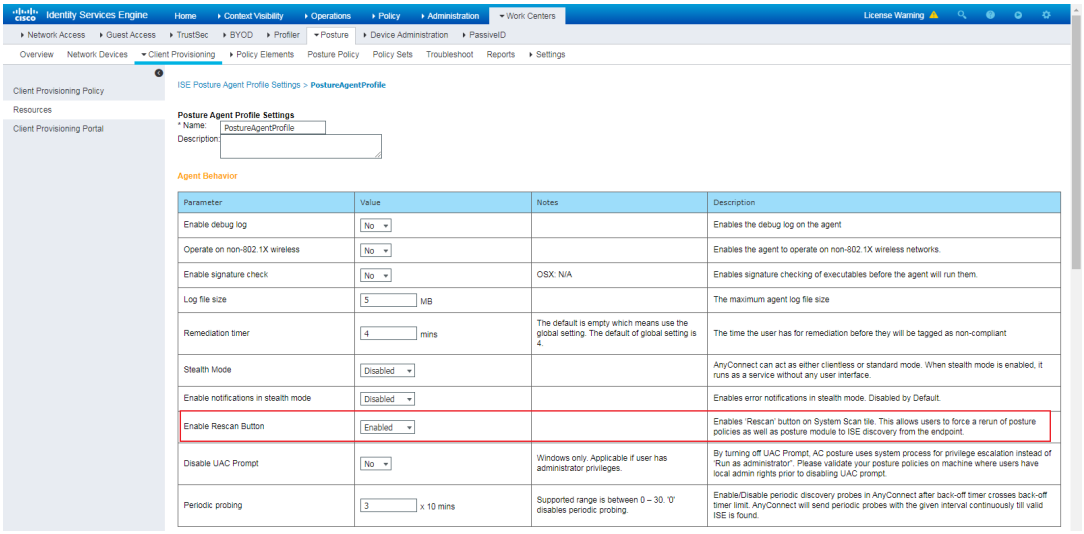


(2) 创建 Posture Agent Profile Settings

在页面上方导航栏中选择[Work Centers/Posture/Client Provisioning/Resources]选项，新建 Posture Agent Profile Settings，并命名为 PostureAgentProfile。

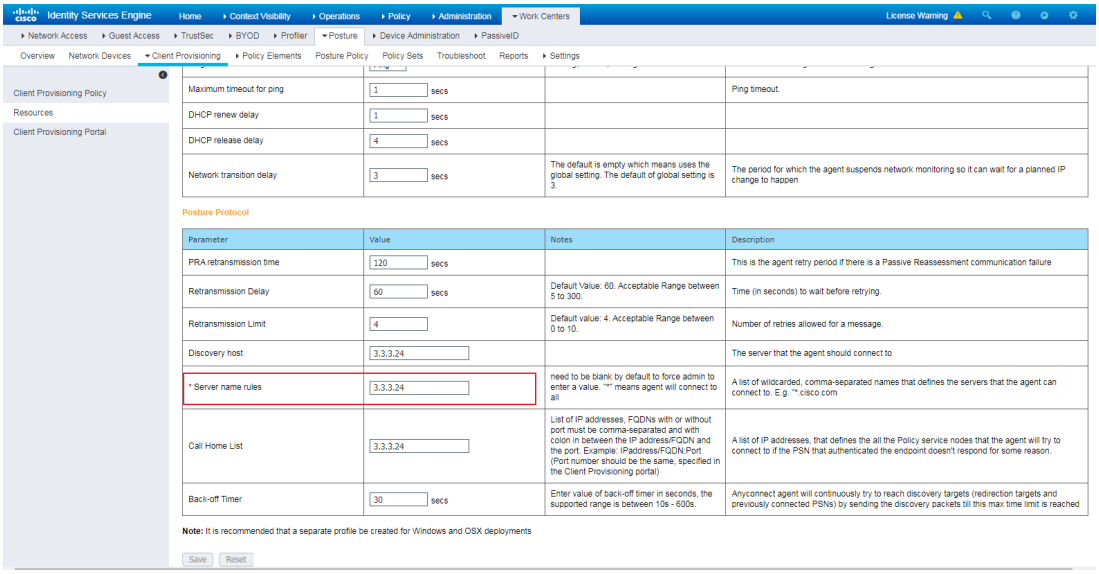
为方便调试，可以使能 Enable Rescan Button 选项。这个配置是下发给 anyconnect 作为配置文件使用的。

图16-4 新建 Posture Agent Profile Settings



注意填写标星的选项，本例中填了 ISE 的 IP 地址。

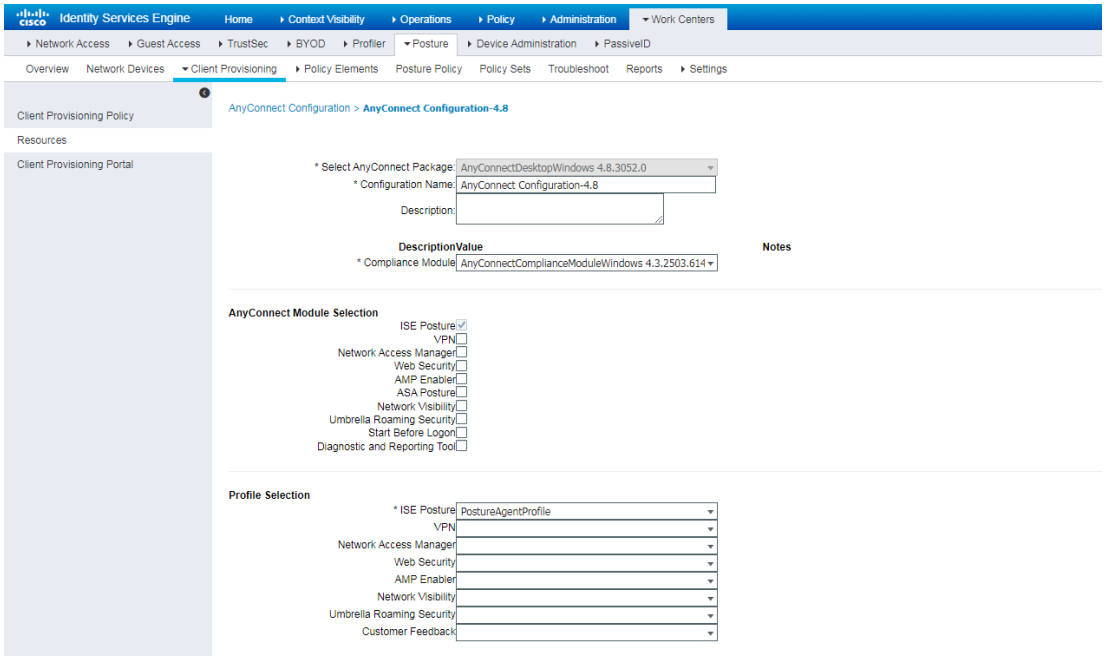
图16-5 填写标星的选项



(3) 创建 AnyConnect Configuration

新建 AnyConnect Configuration，命名为 AnyConnect Configuration-4.8，* ISE Posture 中关联前边创建的 PostureAgentProfile，Compliance Module 关联上传的文件 AnyConnectComplianceModuleWindows 4.3.2503.6145。

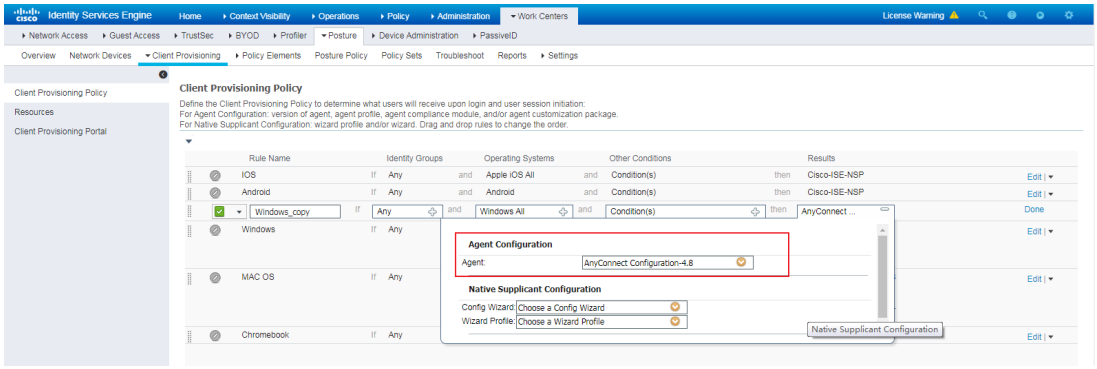
图16-6 AnyConnect Configuration 相关配置



(4) 创建 Client Provisioning Policy

在页面上方导航栏中选择[Work Centers/Posture/Client Provisioning/Client Provisioning Policy]选项，选择之前创建的 AnyConnect Configuration-4.8。

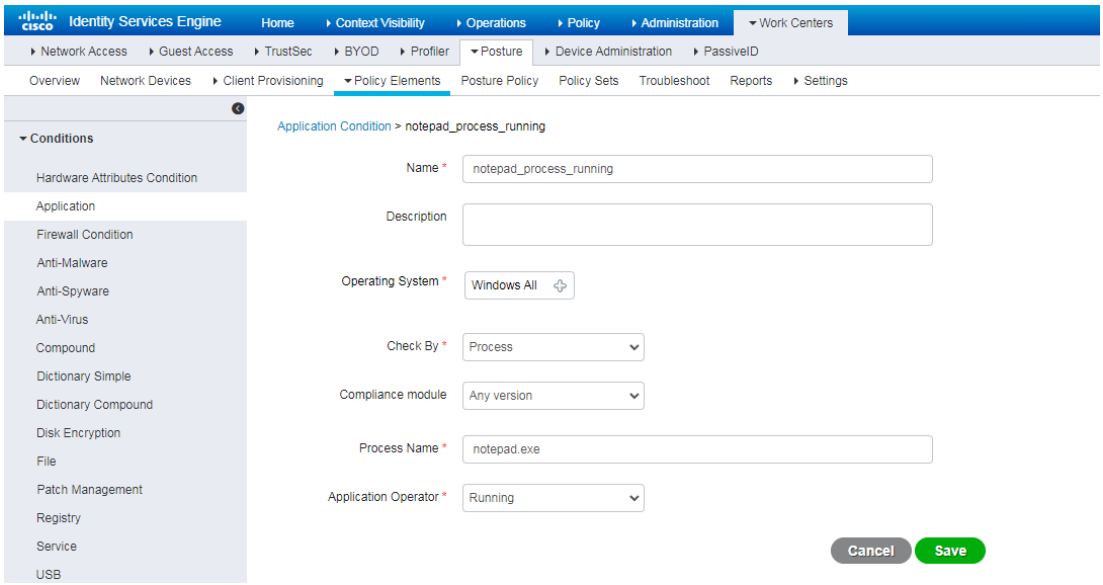
图16-7 新建 Client Provisioning Policy



(5) 创建 posture policy element

在页面上方导航栏中选择[Work Centers/Posture/Policy Elements/Condition/Application]选项，以检测 notepad 是否运行为例，在 application 中新建，并命名为 notepad_process_running。

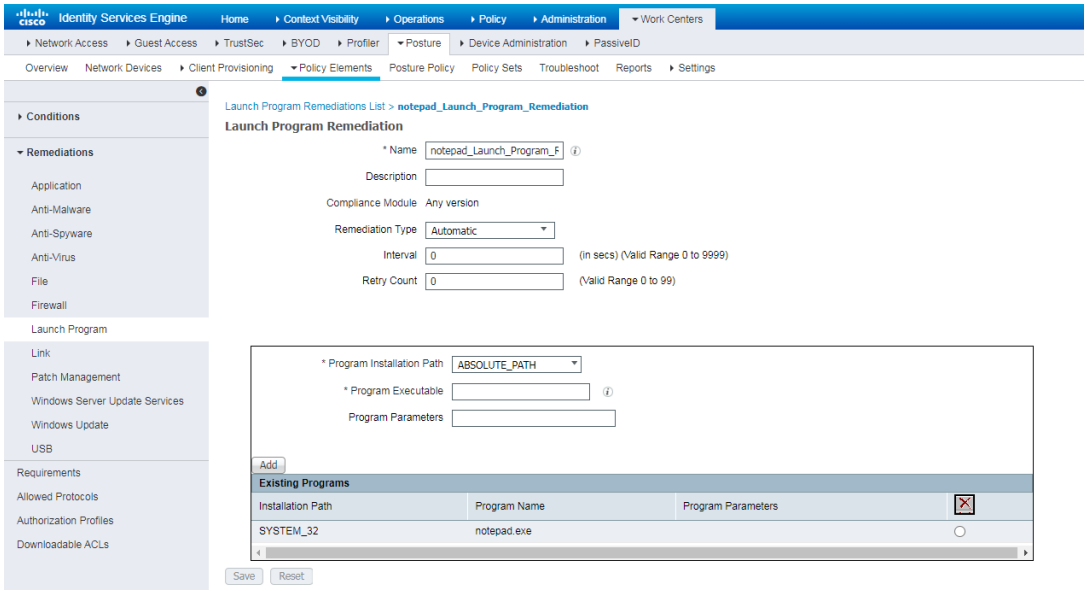
图16-8 新建 Application Condition



(6) 创建 Remediation

在页面上方导航栏中选择[Work Centers/Posture/Policy Elements/Remediations/Launch Program]选项，在 Launch Program Remediations 中新建并命名为 notepad_Launch_Program_Remediation。

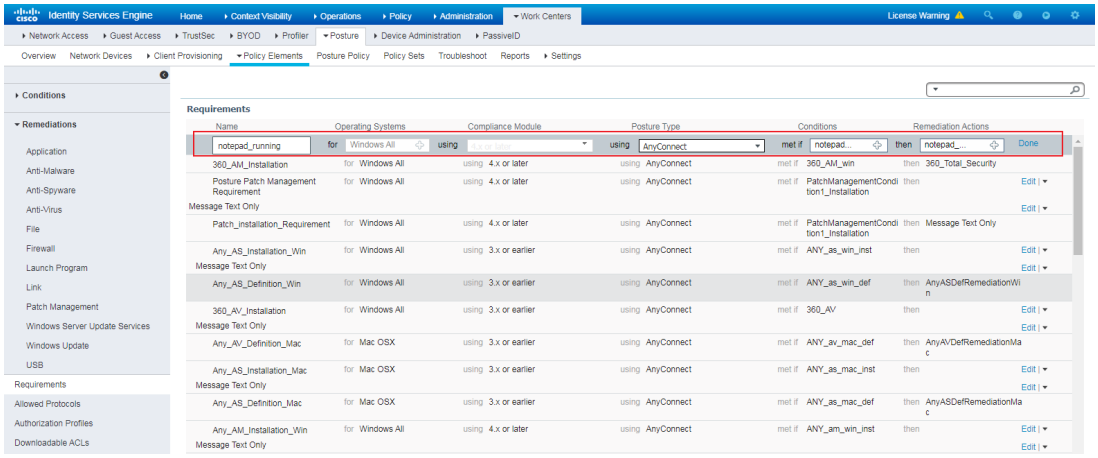
图16-9 新建 Remediation



(7) 创建 Requirement

在页面上方导航栏中选择[Work Centers/Posture/Policy Elements/Remediations/Requirements]选项，创建 Requirement 关联上之前创建的 condition 及 Remediation。

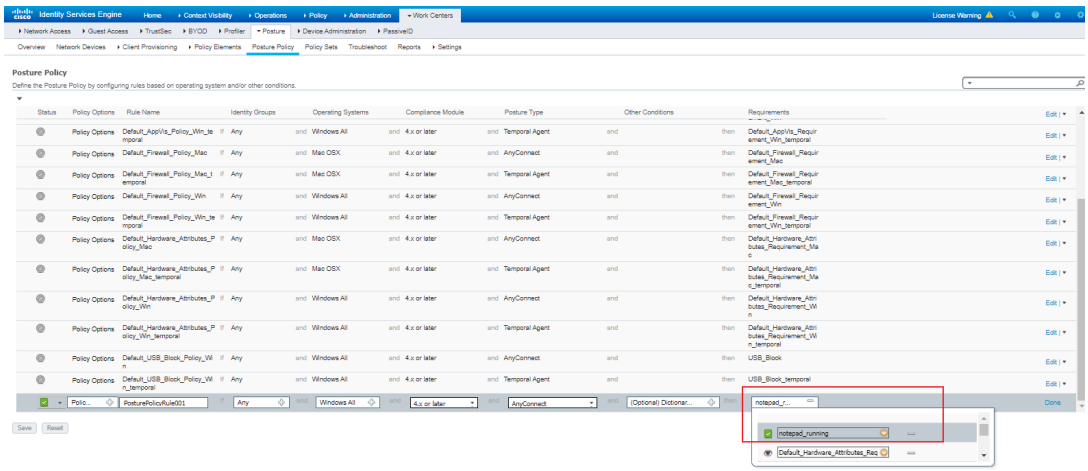
图16-10 新建 Requirement



(8) 创建 Posture Policy

在页面上方导航栏中选择[Work Centers/Posture/Posture Policy]选项，新建 Posture Policy，因为之前上传了 AnyConnectComplianceModuleWindows 4.3.2503.6145，这儿 Compliance Module 选择 4.x or later，Other Conditions 选上之前创建的 notepad_running。

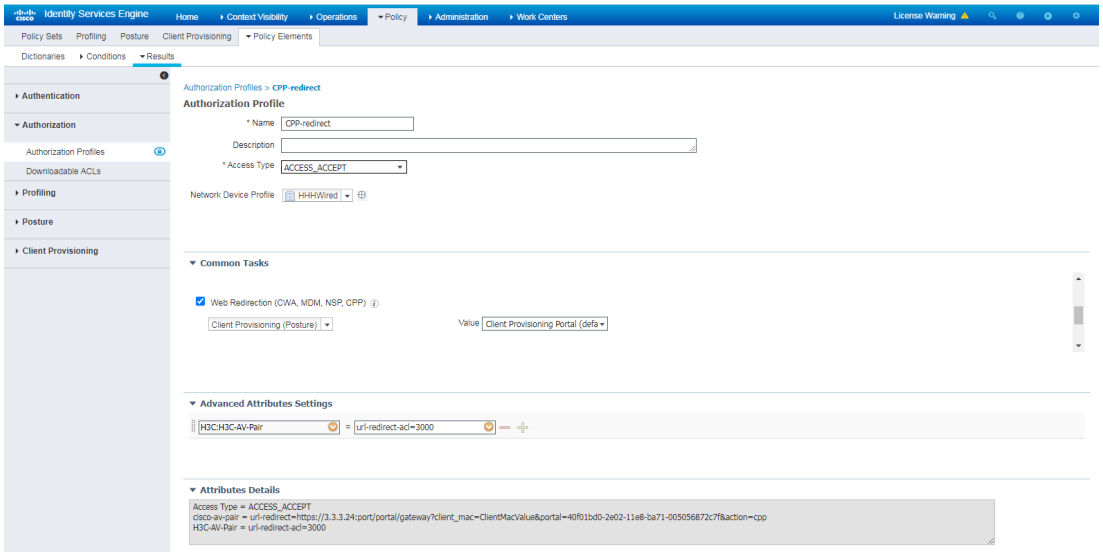
图16-11 创建 Posture Policy



(9) 创建 Authorization Profile

在页面上方导航栏中选择[Policy/Policy Elements/Results/Authorization/Authorization Profiles]选项，新建 1 个 Authorization Profile 用于 Client provision，也就是终端在合规状态未知或者不合规的时候，将终端的网页访问重定向到 cpp 页面，用于下载 anyconnect 客户端。如下图，命名为 CPP-redirect，并关联上 ACL，使得终端可以访问 cpp 页面。

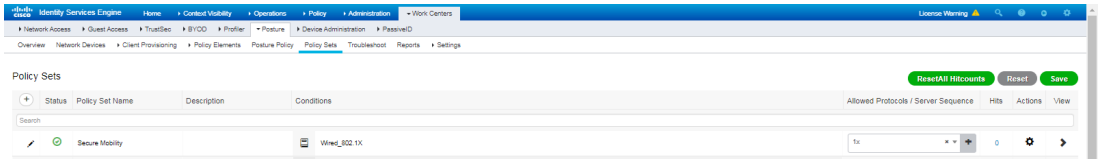
图16-12 新建 Authorization Profile



(10) 创建 Policy Set

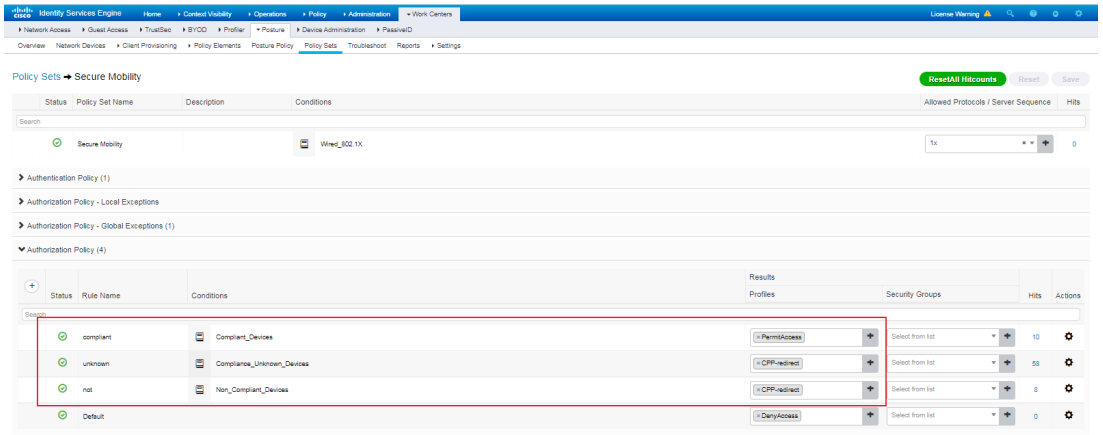
在页面上方导航栏中选择[Work Centers/Posture/Policy Sets]选项，新建 Policy Set，并命名为 Secure Mobility。

图16-13 新建 Policy Set



新建 3 个 Authorization Policy，使得合规状态未知及不合规状态下只能访问 cpp 页面，合规状态下授予 permitaccess 完全访问的权限。

图16-14 新建 Authorization Policy



16.4 效果展示

16.4.1 Client Provisioning

终端连接成功 802.1X，浏览器访问随机页面跳转到 Client Provisioning Portal。

图16-15 Client Provisioning Portal

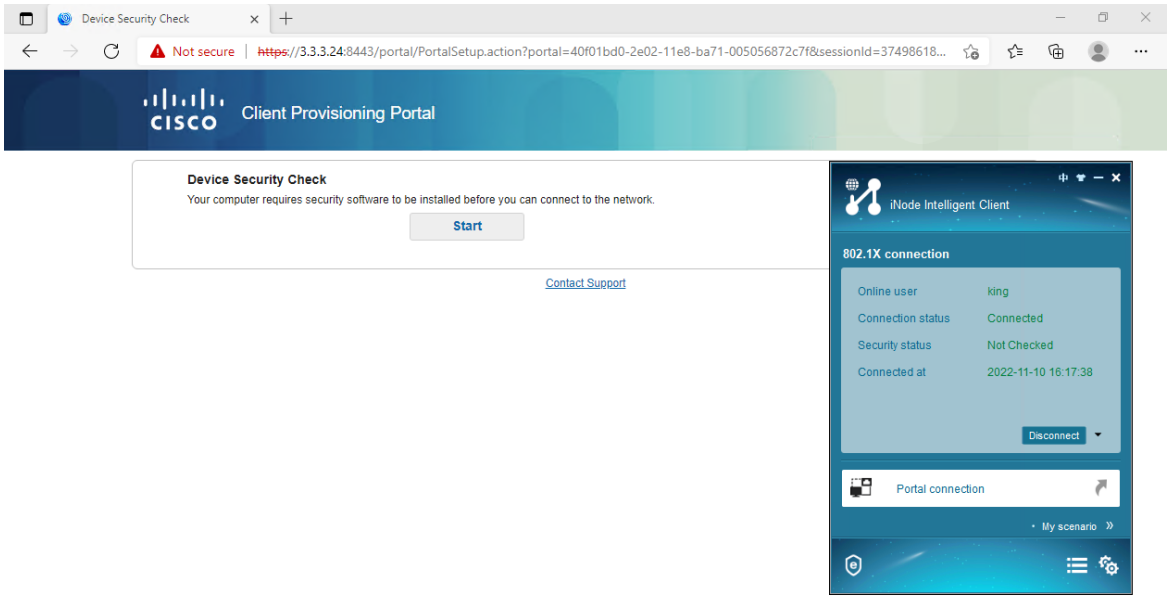


图16-16 Click start and wait a while

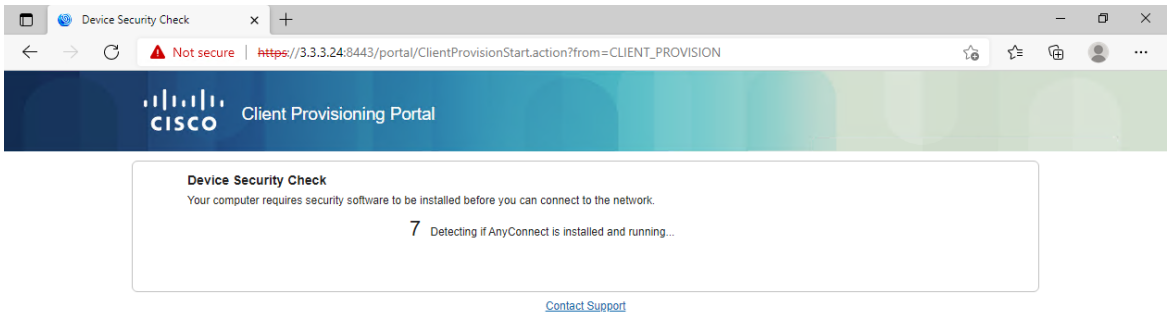


图16-17 点击 Click here to download and install AnyConnect

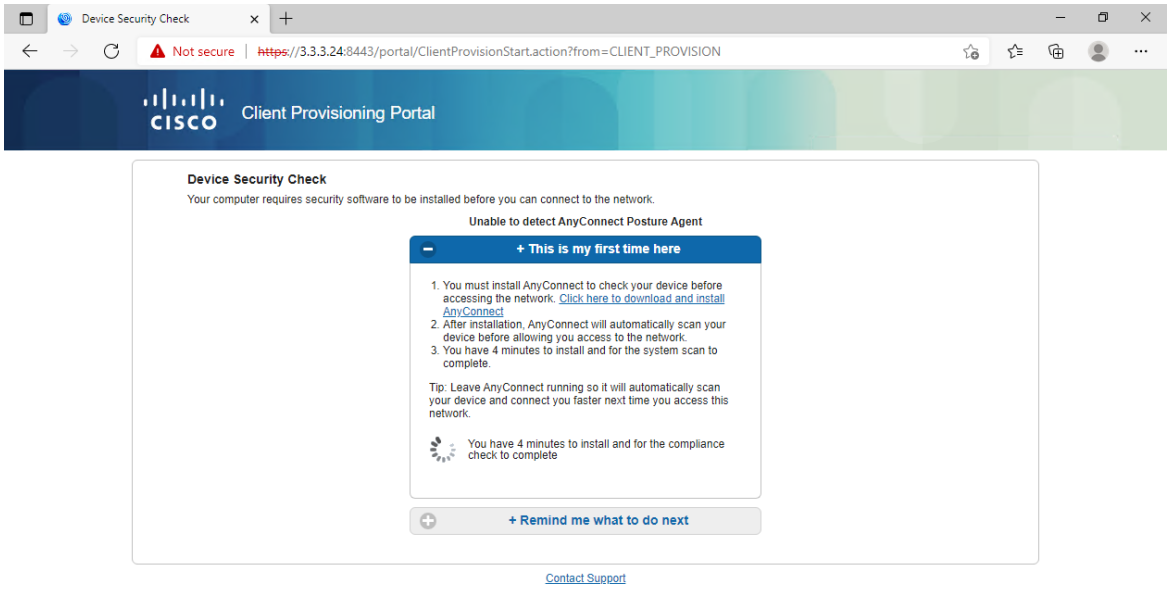


图16-18 下载软件包并打开

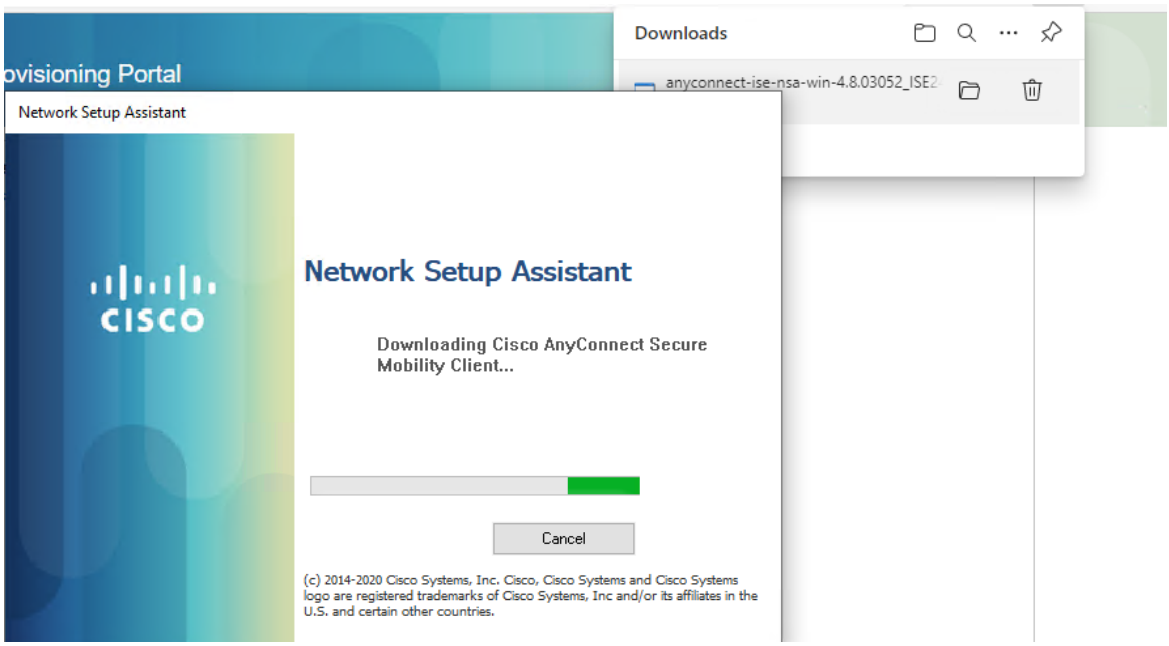
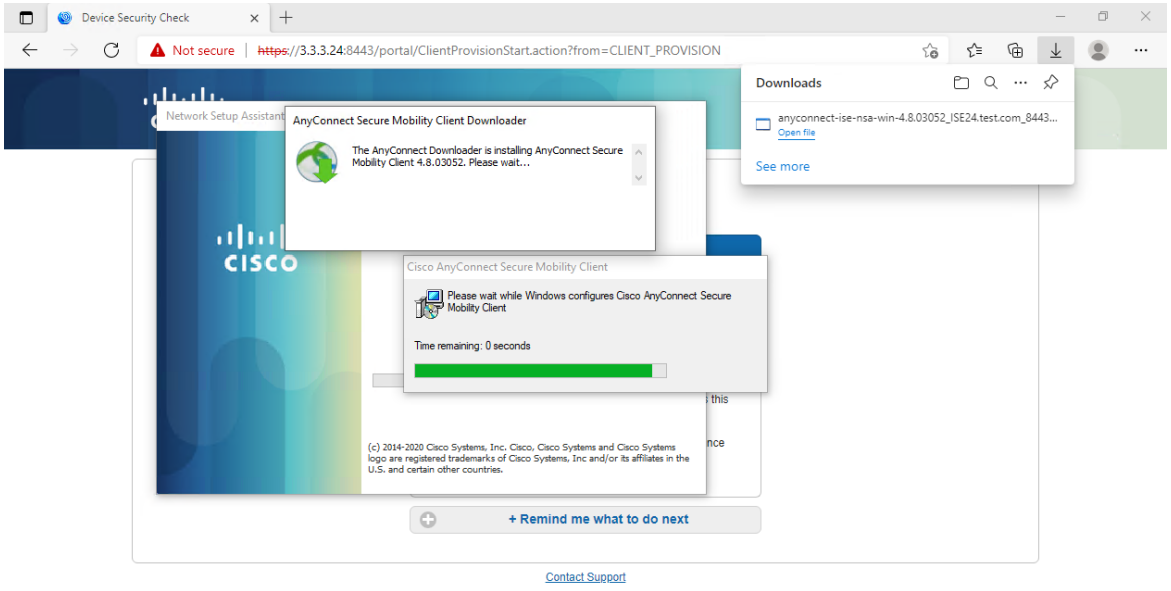


图16-19 Connect anyway

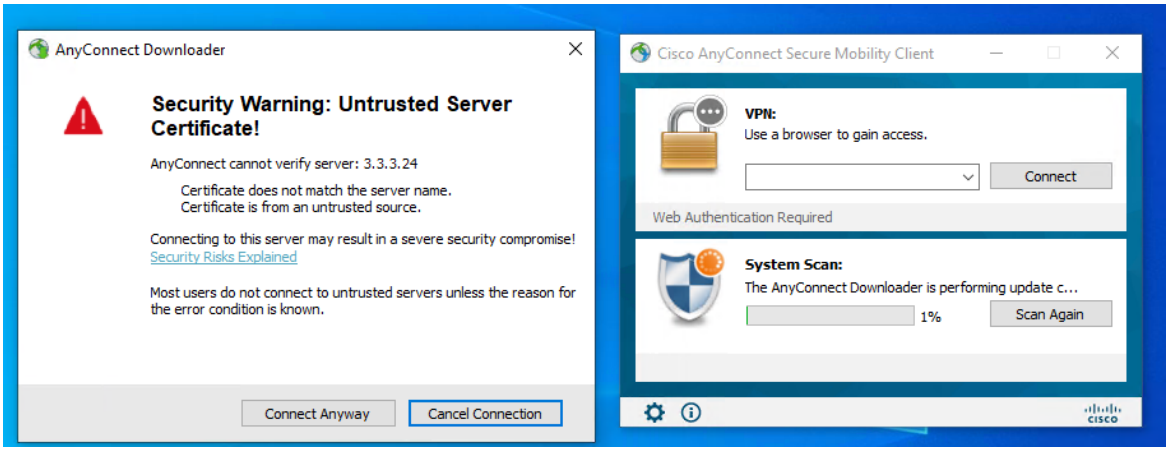
图16-20 等待安装成功



16.4.2 Posture Assessment

安装成功后自动运行，点击 Connect anyway。

图16-21 点击 Connect anyway



根据之前 Posture Policy 等配置，Anyconnect 在检测到 notepad.exe 没打开的情况下，会自动打开 notepad.exe。配置的其他 optional 检测项可以选择<Skip All>。

图16-22 自动打开 notepad.Exe

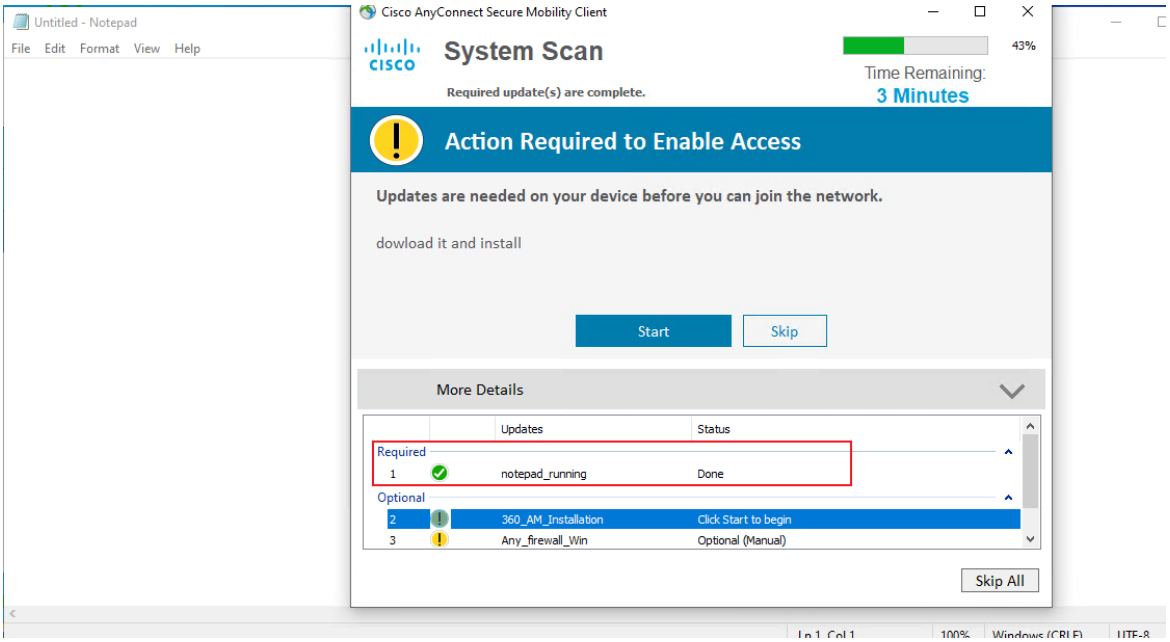


图16-23 anyconnect 检测为 compliant

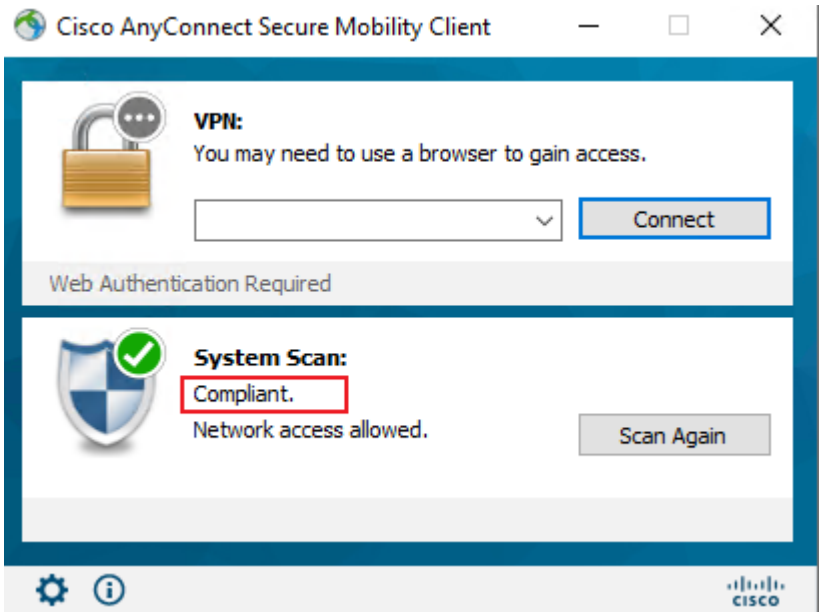
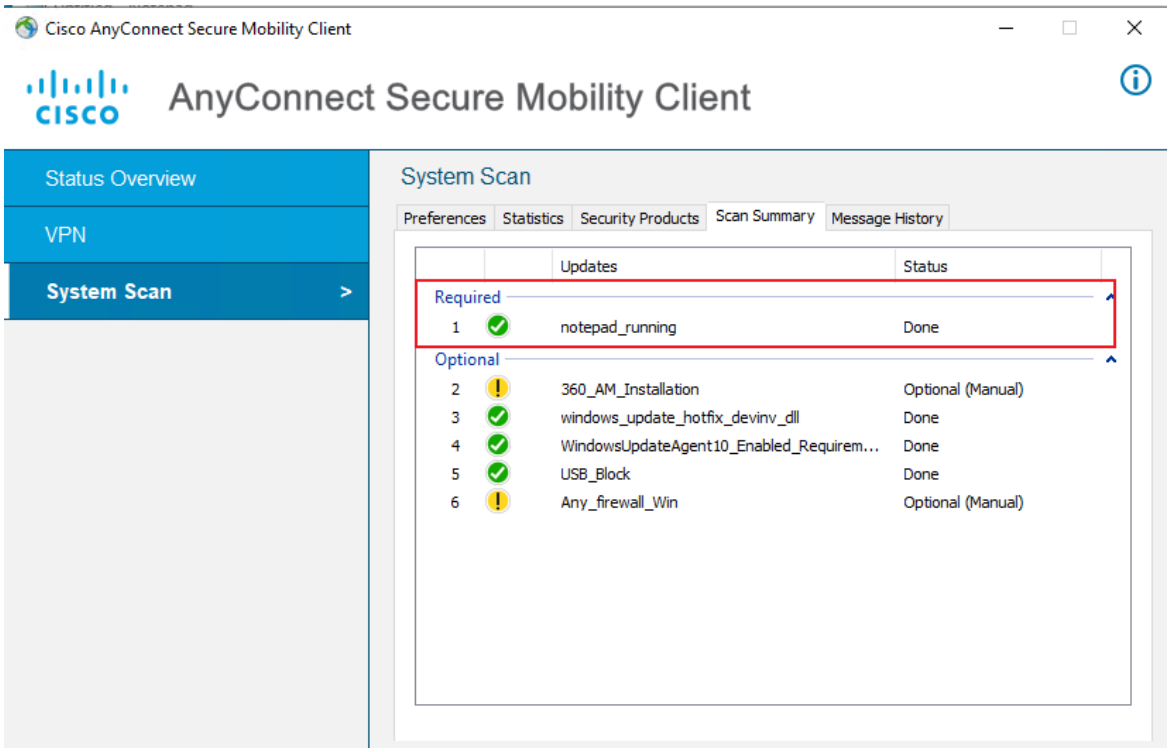


图16-24 Anyconnect scan summary



回顾 ISE 上的日志，可以看到终端一开始拿到 Secure Mobility >> unknown 的授权 CPP-redirect，在终端安装成功 anyconnect 并检测通过后，ISE 自动下发 coa 重认证，因为此时终端已是合规状态，终端拿到了 Secure Mobility >> compliant 下的授权。

图16-25 Live logs

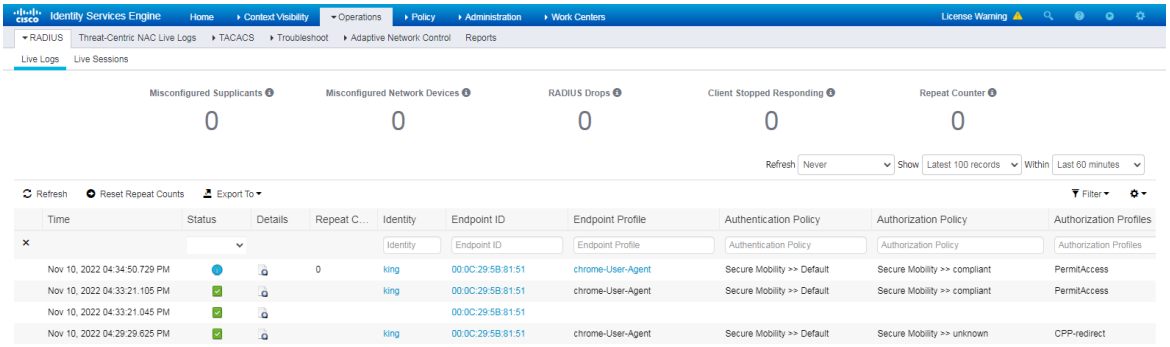
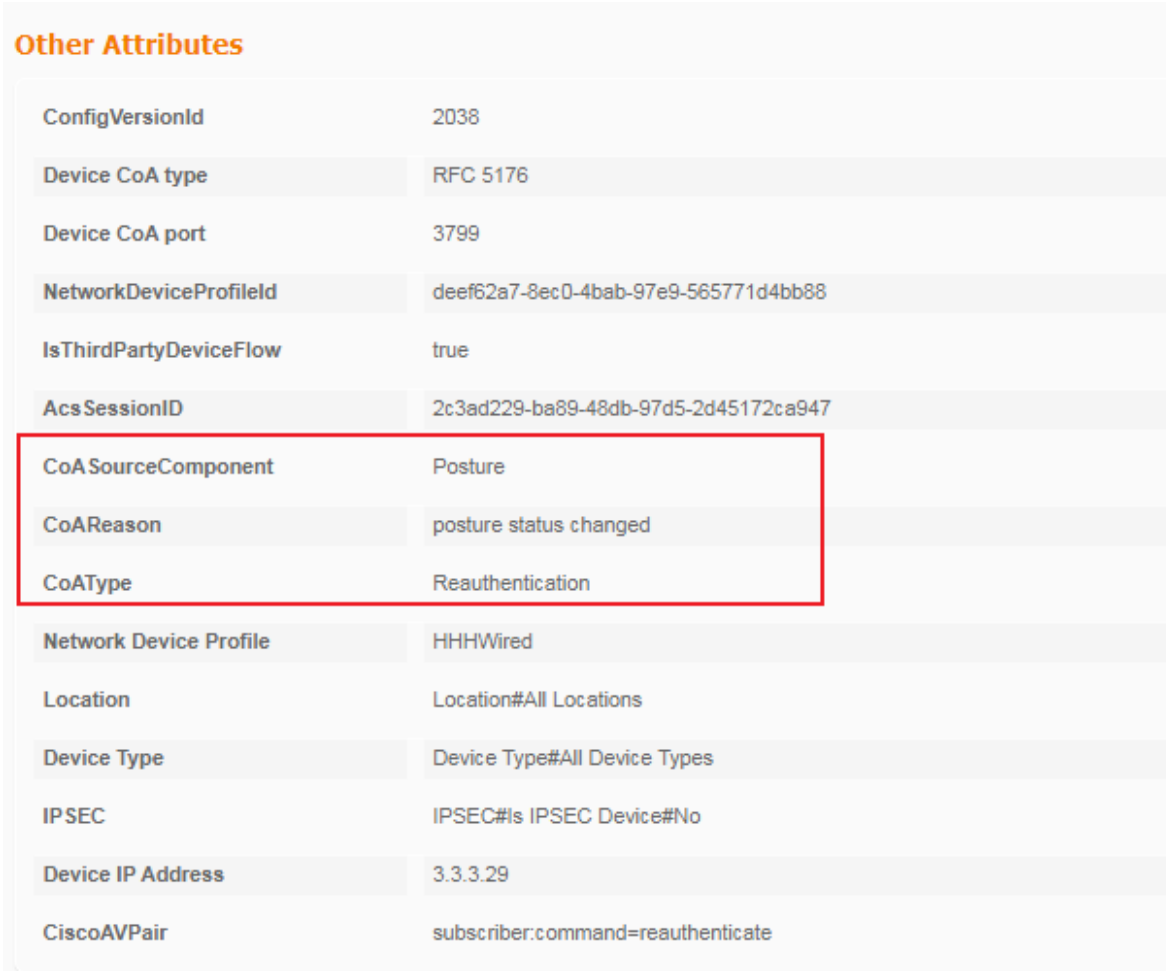


图16-26 posture status changed 触发 Reauthentication



16.5 配置文件

```
#
 dot1x
 dot1x authentication-method eap
```

```
#
vlan 1
#
vlan 2
 description toClients
 arp snooping enable
#
vlan 3
 description toAAAserver
#
interface Vlan-interface1
#
interface Vlan-interface2
 description toClients
 ip address 2.2.2.29 255.255.255.0
#
interface Vlan-interface3
 description toAAAservers
 ip address 3.3.3.29 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 2
 dot1x
#
radius scheme ise
 primary authentication 3.3.3.24 key cipher $c$3$2oLOvHdRilTBlb6n1yh3/MoXN8z/RMbctQ==
 primary accounting 3.3.3.24 key cipher $c$3$fAhWH/rHm9hCcPq2PBWQa54YG9xKuQ1P0w==
 timer realtime-accounting 20 second
 user-name-format keep-original
#
#
domain test.com
 authentication default radius-scheme ise
 authorization default radius-scheme ise
 accounting default radius-scheme ise
#
```