H3C 无线控制器

与 LDAP 服务器配合进行本地 Portal 认证典型配置举例 (V7)

资料版本：6W100-20191125

目 录

1 简介

本文档介绍在无线控制器上配置本地 Portal 服务器，通过 LDAP 协议将 AC 设备解析出的用户名和密码传到 LDAP 服务器上的对无线用户进行认证的典型配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的无线控制器和接入点产品，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，请参考相关产品手册，或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。

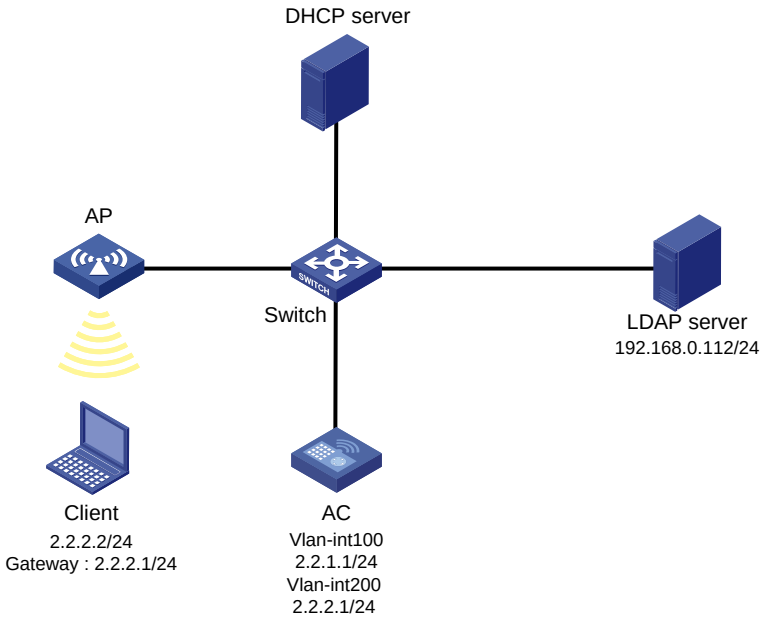
本文档假设您已了解 AAA、Portal、WLAN 特性。

3 配置举例

3.1 组网需求

如图 1 所示组网，AP 和 Client 通过 DHCP 服务器获取 IP 地址，要求：配置 AC 对无线用户进行本地 Portal 认证，并采用 LDAP 服务器对用户进行远程 AAA 认证。

图1 本地 Portal 服务器与 LDAP 服务器组合认证组网图



3.2 配置注意事项

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- 如果本地 Portal Web 服务器提供的缺省认证页面文件需要更新，需要 undo default-logon-page 后重新配置，否则新页面不会生效。
- 配置路由，保证启动 Portal 之前各设备之间的路由可达。
- 请提前编辑好认证页面，保存为 abc.zip，并上传到 AC 存储介质的根目录

3.3 配置步骤

3.3.1 配置AC

(1) 配置 AC 接口

创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AP 将获取该 IP 地址与 AC 建立 CAPWAP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 2.2.1.1 24
[AC-Vlan-interface100] quit
```

创建 VLAN 200 及其对应的 VLAN 接口，并为该接口配置 IP 地址。Client 将使用该 VLAN 接入无线网络。

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 2.2.2.1 24
[AC-Vlan-interface200] quit
```

配置 AC 与 Switch 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，允许 VLAN 100、VLAN 200 通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

(2) 配置 LDAP 方案

创建 LDAP 服务器 ldap，并进入 LDAP 服务器视图。

```
[AC] ldap server ldap
```

配置具有管理员权限的用户 DN。

```
[AC-ldap-server-ldap] login-dn cn=administrator,cn=users,dc=myias,dc=com
```

配置查询用户的起始目录。

```
[AC-ldap-server-ldap] search-base-dn dc=myias,dc=com
```

配置 LDAP 认证服务器的 IP 地址。

```
[AC-ldap-server-ldap] ip 192.168.0.112
```

配置具有管理员权限的用户密码。

```
[AC-ldap-server-ldap] login-password simple 123456
[AC-ldap-server-ldap] quit
```

创建 LDAP 方案 ldap，并进入 LDAP 方案视图。

```
[AC] ldap scheme ldap
```

配置 LDAP 认证服务器。

```
[AC-ldap-ldap] authentication-server ldap
[AC-ldap-ldap] quit
```

创建 ISP 域 ldap，并进入 ISP 域视图。

```
[AC] domain ldap
```

为 Portal 用户配置 AAA 认证方法为 LDAP 认证、不授权、不计费。

```
[AC-isp-ldap]authentication portal ldap-scheme ldap
[AC-isp-ldap] authorization portal none
[AC-isp-ldap] accounting portal none
```

指定 ISP 域 ldap 下的用户闲置切断时间为 15 分钟，闲置切断时间内产生的流量为 1024 字节。

```
[AC-isp-ldap] authorization-attribute idle-cut 15 1024
[AC-isp-ldap] quit
```

(3) 配置 Portal 认证

配置 Portal Web 服务器的 URL 为 http://2.2.2.1 /portal。

```
[AC] portal web-server newpt
[AC-portal-websvr-newpt] url http://2.2.2.1/portal
[AC-portal-websvr-newpt] quit
```

创建本地 Portal Web 服务器，进入本地 Portal Web 服务器视图，并指定使用 HTTP 协议和客户端交互认证信息。

```
[AC] portal local-web-server http
```

配置本地 Portal Web 服务器提供的缺省认证页面文件为 abc.zip（设备的存储介质的根目录下必须已存在该认证页面文件，否则功能不生效）。

```
[AC–portal-local-websvr-http] default-logon-page abc.zip
[AC–portal-local-websvr-http] quit
```

(4) 配置无线服务

创建无线服务模板 st1，并进入无线服务模板视图。

```
[AC] wlan service-template st1
```

配置 SSID 为 service。

```
[AC-wlan-st-st1] ssid service
```

配置无线服务模板 VLAN 为 200。

```
[AC-wlan-st-st1] vlan 200
```

使能直接方式的 Portal 认证。

```
[AC-wlan-st-st1] portal enable method direct
```

配置接入的 Portal 用户使用认证域为 ldap。

```
[AC-wlan-st-st1] portal domain ldap
```

在服务模板上引用名称为 newpt 的 Portal Web 服务器作为用户认证时使用的 Web 服务器。

```
[AC-wlan-st-st1] portal apply web-server newpt
```

使能无线服务模板。

```
[AC-wlan-st-st1] service-template enable
[AC-wlan-st-st1] quit
```

创建 AP，配置 AP 名称为 officeap，型号名称选择 WA2620E-AGN，并配置其序列号。

```
[AC] wlan ap officeap model WA2620E-AGN
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
```

进入 radio 2 射频视图。

```
[AC-wlan-ap-officeap] radio 2
```

将无线服务模板 st1 绑定到 AP 的 radio 2，并开启射频。

```
[AC-wlan-ap-officeap-radio-2] service-template st1
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] quit
[AC-wlan-ap-officeap] quit
```

3.3.2 Switch的配置

创建 VLAN 100，用于转发 AC 和 AP 间 CAPWAP 隧道内的流量。

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

创建 VLAN 200，用于转发 Client 无线报文。

```
[Switch] vlan 200
[Switch-vlan200] quit
```

配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，允许 VLAN 100 和 VLAN 200 通过。

```
[Switch] interface gigabitethernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit
```

配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

3.3.3 配置LDAP服务器

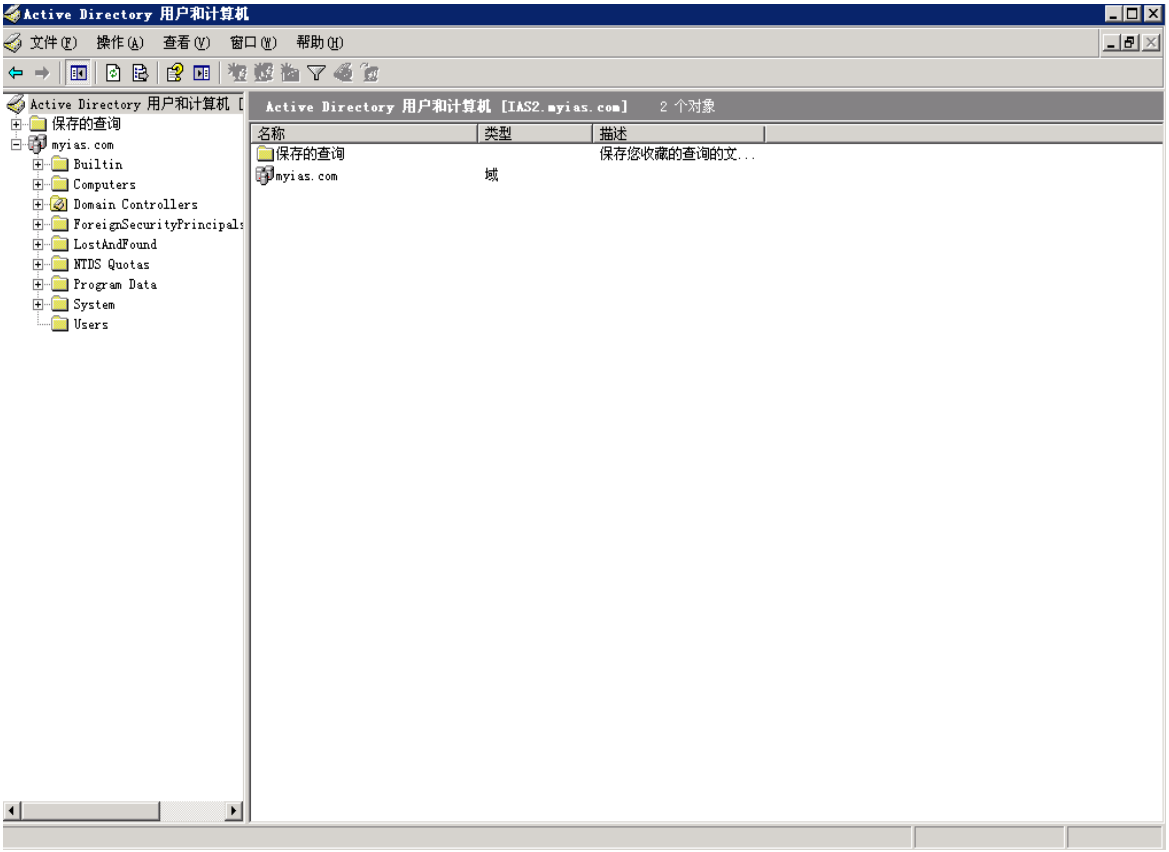
说明

本文以 Microsoft Windows 2003 Server 的 Active Directory 为例，说明该例中 LDAP 服务器的基本配置。

(1) 添加用户 aa

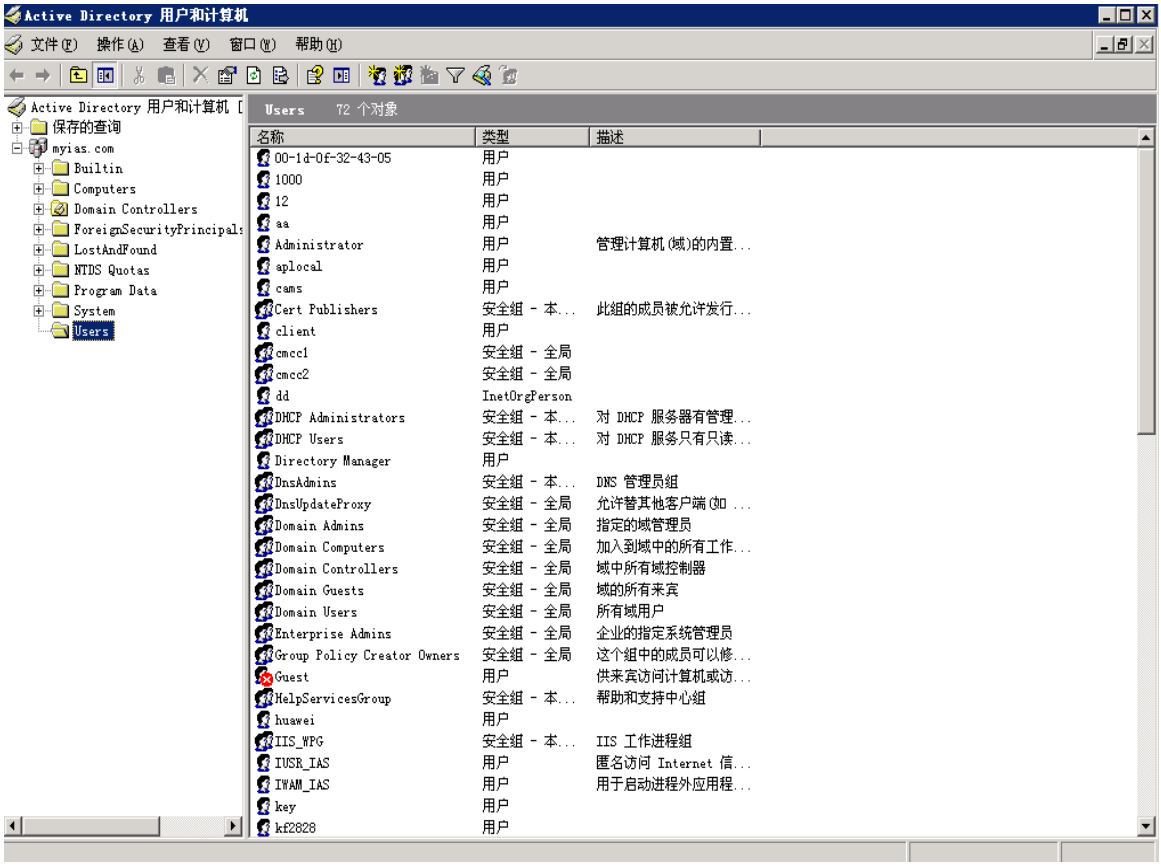
在 LDAP 服务器上，选择[开始/管理工具]中的[Active Directory 用户和计算机]，打开 Active Directory 用户管理界面。

图2 打开 Active Directory 用户管理界面



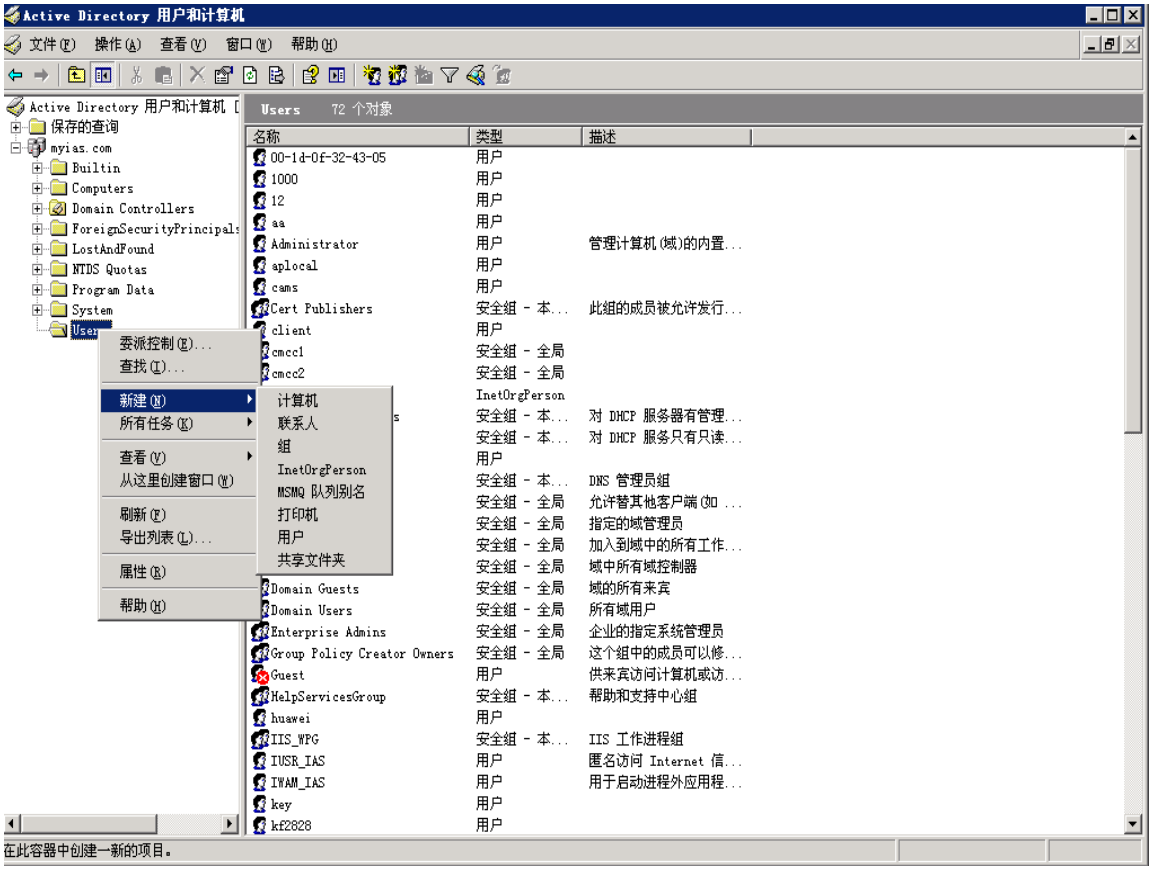
在 Active Directory 用户管理界面的左侧导航树中，点击 myias.com 节点下的<Users>按钮。

图3 添加用户



右键单击“Users”，选择[新建/用户]，打开“新建对象-用户”对话框。

图4 新建用户

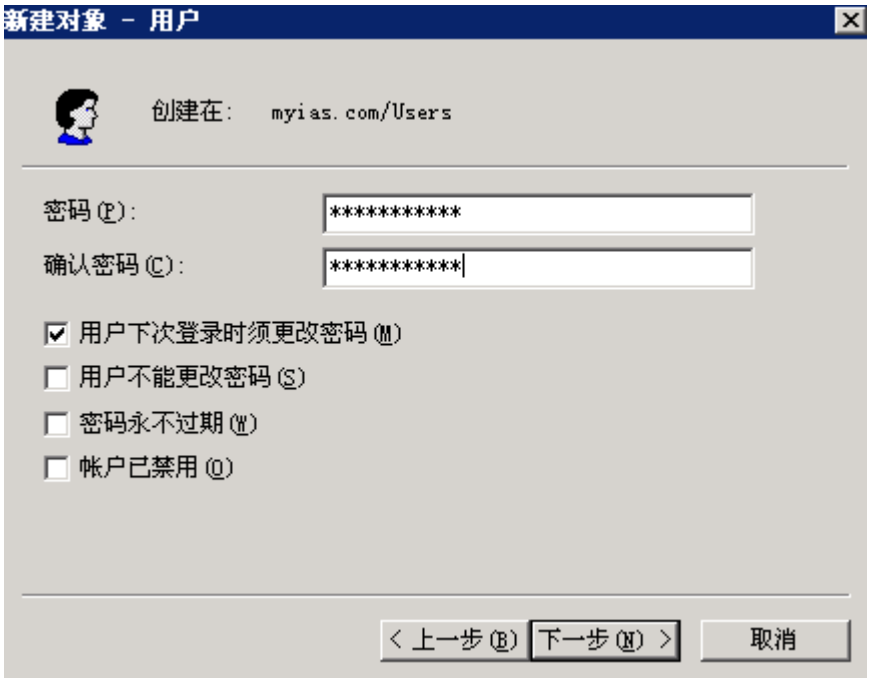


在对话框中输入用户信息和用户登录名 aa，并单击<下一步>按钮。

图5 新建用户 aa

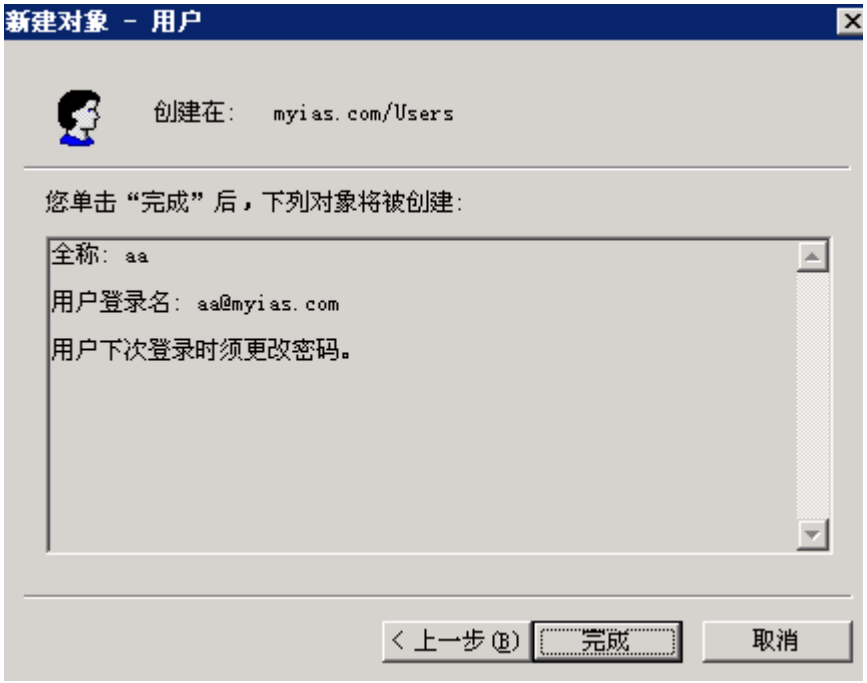
在弹出的对话框内输入密码，并确认密码，然后单击<下一步>按钮。

图6 设置用户密码



完成新建用户。

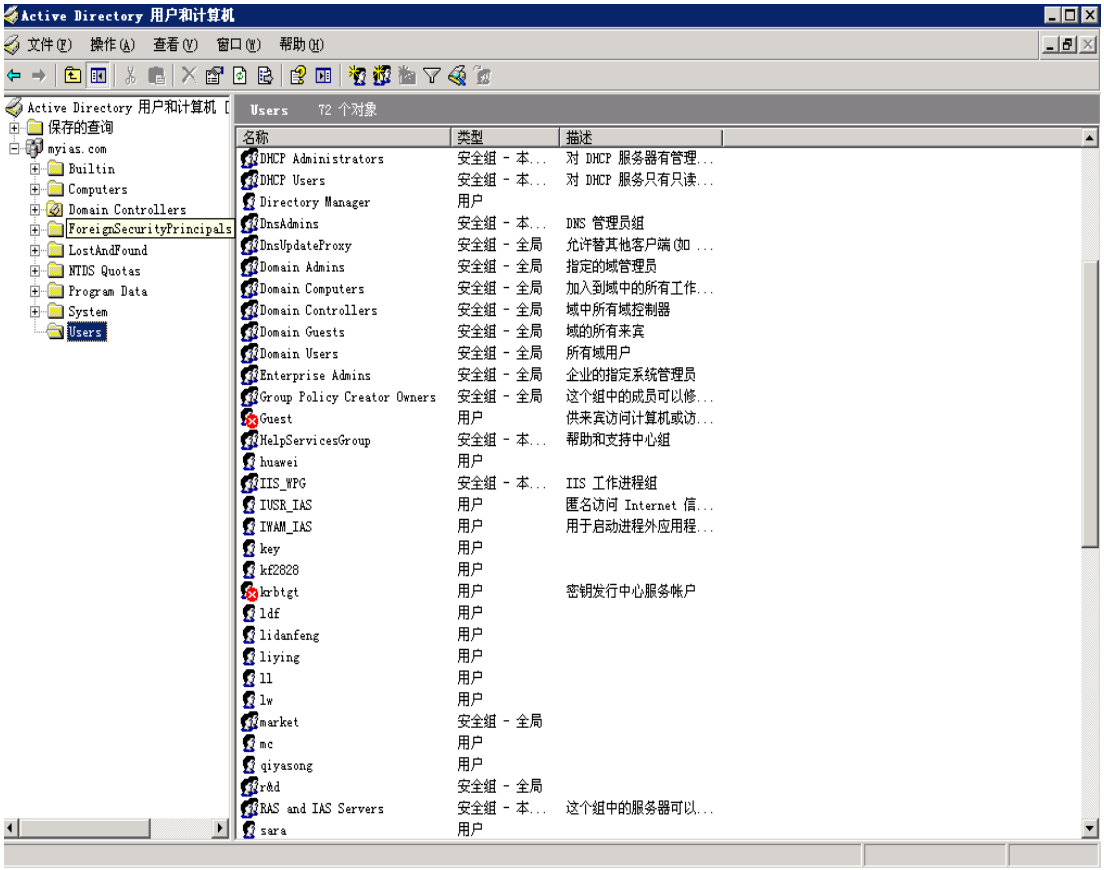
图7 完成新建用户



(2) 将用户 aa 加入 Users 组

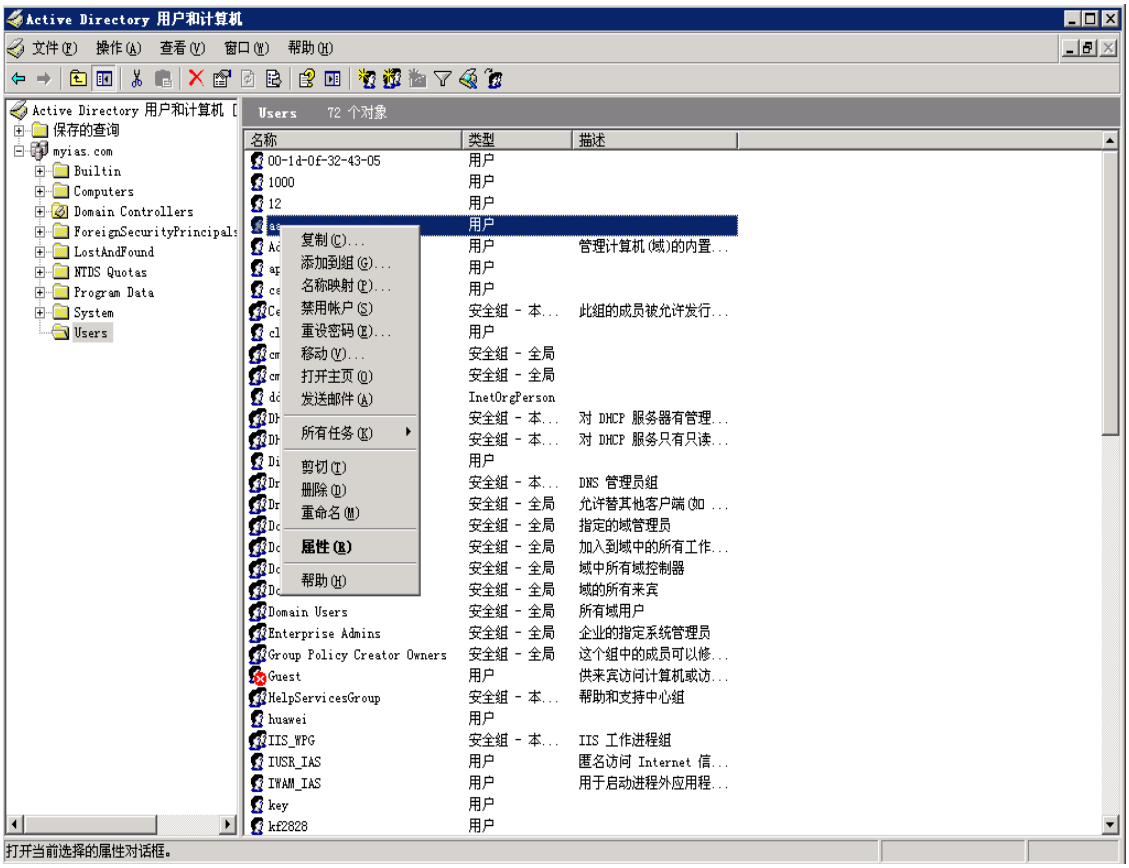
在 Active Directory 用户管理界面的左侧导航树中，单击 myias.com 节点下的“Users”按钮。

图8 将用户加入组



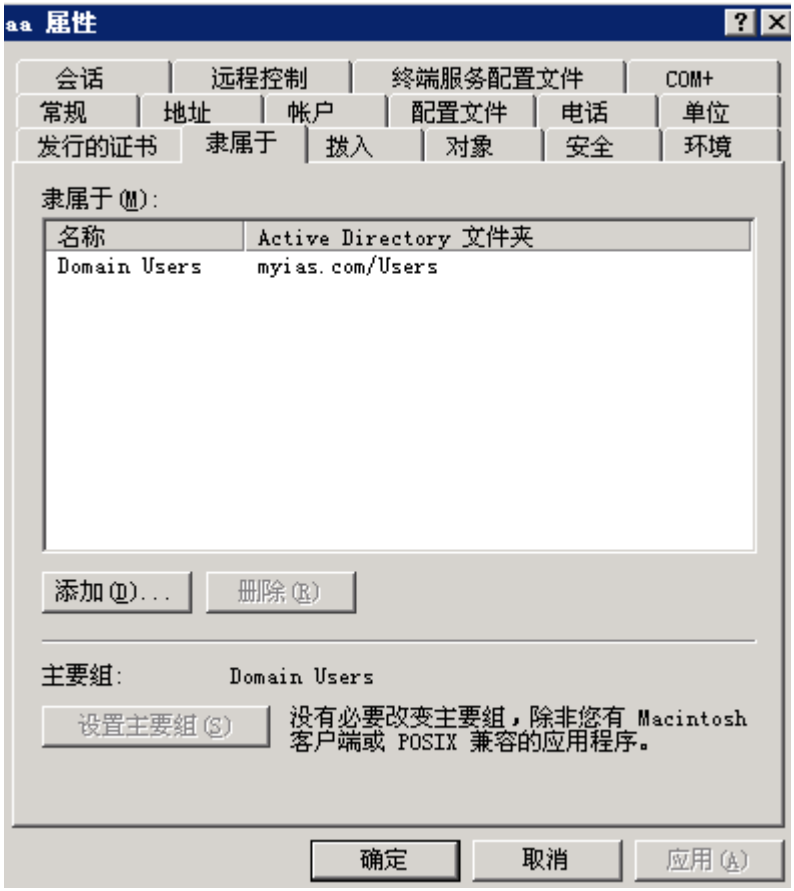
在右侧的 Users 信息框中右键单击用户 aa，选择“属性”项。

图9 选择用户



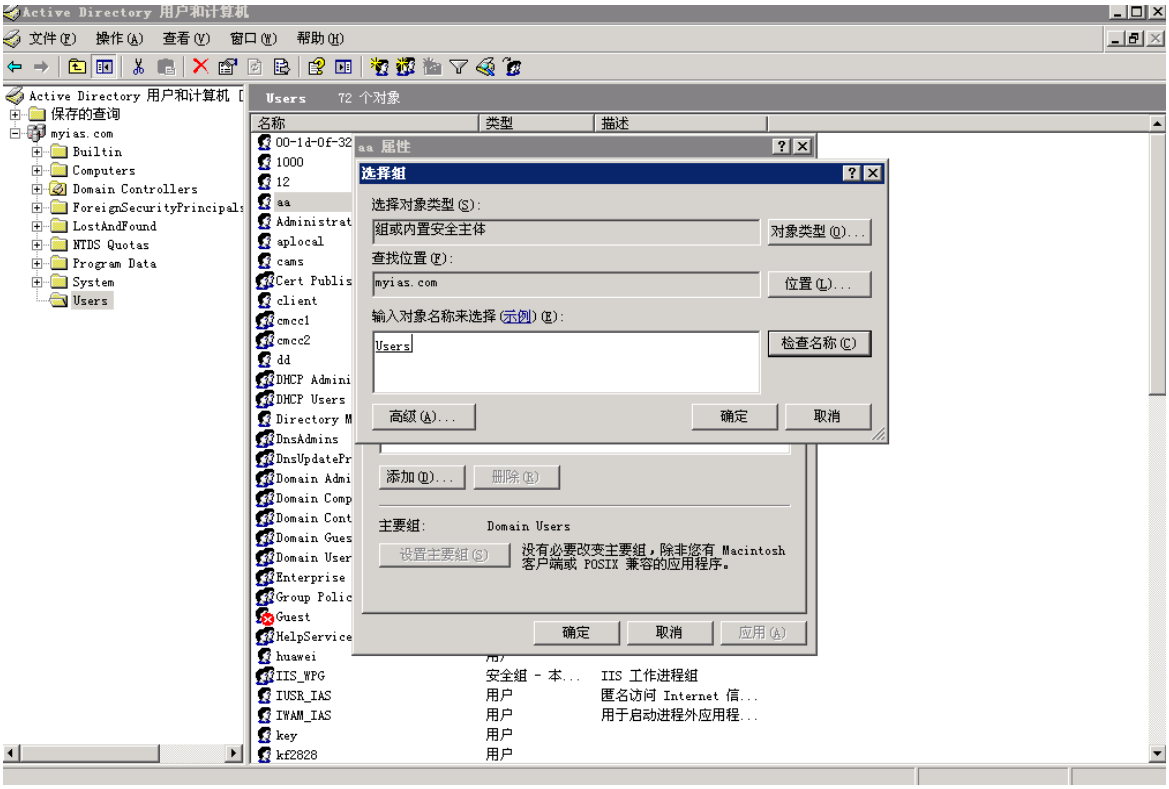
选择“隶属于”页签，并单击<添加(D)...>按钮。

图10 修改用户属性



在弹出的[选择组]对话框中的可编辑区域框中输入对象名称“Users”，单击<确定>，完成用户 aa 添加到 Users 组。

图11 添加用户 aa 到用户组 Users



完成用户 aa 的添加之后，还需要配置管理员用户 administrator 的密码。

- 在右侧的 Users 信息框中右键单击管理员用户 administrator，选择“设置密码(S)...”项；
- 在弹出的密码添加对话框中设置管理员密码。

3.4 验证配置

打开无线客户端上的 IE 浏览器，输入任意的 IP 地址，按回车，网页会自动跳转到 Portal 认证页面，输入用户名：aa，密码:123456，单击 logon 按钮，认证成功。

用户通过认证后，在 AC 上使用命令 **display portal user all** 可以查看到有 Portal 用户在线。

```
<AC> display portal user all
 Index:17
 State:ONLINE
 SubState:NONE
 ACL:3777
 Work-mode:stand-alone
 MAC              IP               Vlan    Interface
 --------------------------------------------------------------------------
 2477-0341-f118   2.2.2.2          200      Vlan-interface200
 Total 1 user(s) matched, 1 listed.
```

3.5 配置文件

- AC：

```
#
vlan 100
#
vlan 200
#
wlan service-template st1
 ssid service
 vlan 200
 portal enable method direct
 portal domain ldap
 portal apply web-server newpt
 service-template enable
#
interface Vlan-interface100
 ip address 2.2.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 2.2.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 200
#
ldap server ldap
 login-dn cn=administrator,cn=users,dc=myias,dc=com
 search-base-dn dc=myias,dc=com
 ip 192.168.0.112
 login-password cipher $c$3$CEz2vKCnA2/51D8rFc/+nTNtOx8Gan+81Q==
#
ldap scheme ldap
 authentication-server ldap
#
domain ldap
 authorization-attribute idle-cut 15 1024
 authentication portal ldap-scheme ldap
 authorization portal none
 accounting portal none
#
portal web-server newpt
 url http://2.2.2.1/portal
#
portal local-web-server http
 default-logon-page abc.zip
#
wlan ap officeap model WA2620E-AGN
```

```
 serial-id 21023529G007C000020
 radio 2
  radio enable
  service-template st1
#
```

- Switch：

```
#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
 poe enable
#
```

4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“用户接入与认证配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“用户接入与认证命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“WLAN 接入配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 接入命令参考”。