

iMC UAM MsChapV2 LDAP认证的典型配置

一、组网需求:

安装有iNode的客户端通过接入设备连接至iMC:

1. 接入设备将客户端发出的认证请求报文发往UAM, UAM根据用户帐号查得该用户需要进行MsChapV2 LDAP认证;
2. UAM为该用户提交一个请求报文给mschapv2server.exe进程, 后者再转交给域控服务器;
3. 域控服务器根据用户信息决定用户是否能认证通过, 然后再将认证结果经由mschapv2server.exe进程返回给UAM;
4. UAM将认证结果通过接入设备返回给客户端。

说明: MsChapV2 LDAP认证方式是从iMC UAM 3.60-E6209才有的新特性。

二、组网图:

UAM MsChapV2 LDAP认证组网如图2-1所示



图2-1

三、配置步骤:

1. 接入设备配置

(1): 配置各接口IP地址 (略)

(2): 配置radius方案为h3c

```
[sw] radius scheme h3c
[sw-radius-h3c] server-type extended
[sw-radius-h3c] primary authentication 10.2.0.2 1812
[sw-radius-h3c] primary accounting 10.2.0.2 1813
[sw-radius-h3c] key authentication simple h3c
[sw-radius-h3c] key accounting simple h3c
[sw-radius-h3c] user-name-format with-domain
```

(3): 配置domain为dot1x引用方案h3c

```
[sw] domain dot1x
[sw-isp-dot1x] authentication lan-access radius-scheme h3
[sw-isp-dot1x] authorization lan-access radius-scheme h3c
[sw-isp-dot1x] accounting lan-access radius-scheme h3c
```

(4): 开启全局dot1x特性, 目前证书认证只能与802.1x配合

```
[sw] dot1x
```

(5): 配置dot1x的认证模式为eap类型

```
[sw] dot1x authentication-method eap
```

(6): 开启接口的dot1x特性

```
[sw-GigabitEthernet2/0/3] dot1x
```

2.iMC侧配置:

(1): 由于采用PEAP证书认证, 所以服务器侧必须安装根证书和服务器证书, 客户端验证服务器的话, 需要安装根证书, 否则不需要安装任何证书。本案例客户端不验证服务器;

将从CA服务器中下载的根证书和服务器证书导入到iMC中(下载过程略):

业务-用户接入管理-业务参数配置-证书配置-动作, 如图3-1所示;

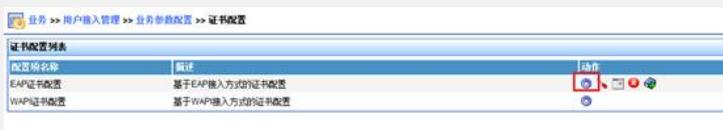


图3-1

点击浏览, 找到根证书文件, 然后点击下一步, 如图3-2所示;

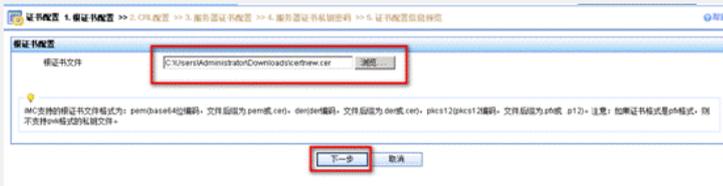


图3-2

保持默认值, 点击下一步, 如图3-3;



图3-3

如图3-4所示点击浏览, 找到从IE里面导出的服务器证书(与根证书同一CA机构颁发), 勾选服务器证书和私钥在同一文件, 单击下一步;



图3-4

输入之前创建的私钥密码;



图3-5

点击确定, 至此我们在iMC侧导入了根证书和服务器证书, iMC具有了证书认证的能力, 如图3-6所示;



图3-6

(2): 新建服务chapv2ldap, 后缀为之前新建的域dot1x, 认证类型选择EAP-PEAP认证, 点击确定, 如图3-7所示;

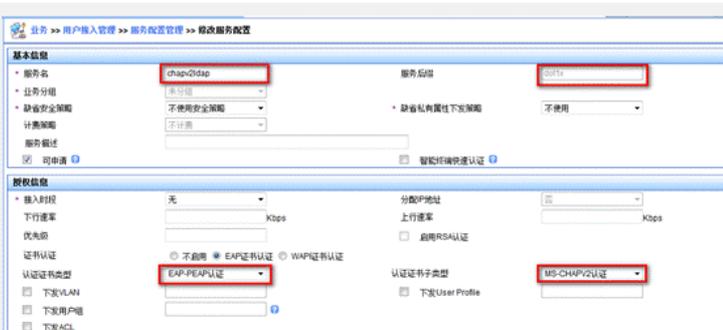


图3-7

(3): 在LDAP服务器上(同IMC服务器)新建虚拟计算机, 依次点击;



图3-8

输入新建计算机名称h3c, 点击确定, 如图3-9所示;

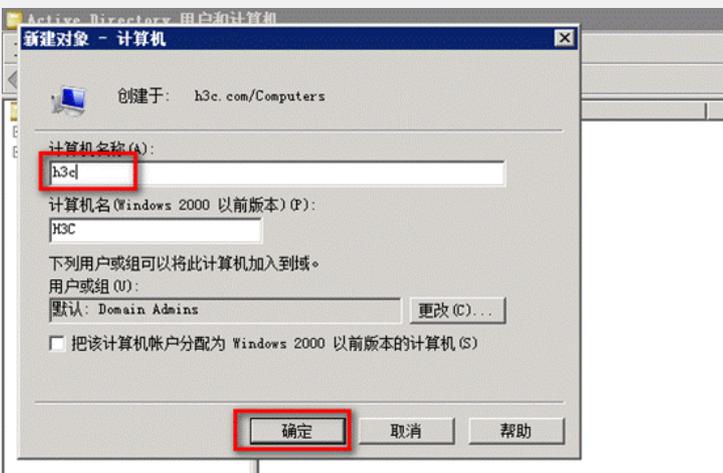


图3-9

为新建的虚拟计算机设置密码, 需要运行一个脚本程序——ModiComputerAccountPass.vbs, 该脚本程序从PEAP认证域配置界面下载获得, 先下载到本地, 使用文本编辑器打开该文件, 将CN=testAccount,CN=Computers, DC= CONTOSO,DC=COM替换为虚拟计算机帐号DN, 本例中DN为CN=h3c, CN= Computers,DC=h3c,DC=com, 将IMC123替换为虚拟计算机密码“q1w2e3R4”;



图3-10

(4): 在LDAP服务器中新建组织单元haha如图3-11依次点击;

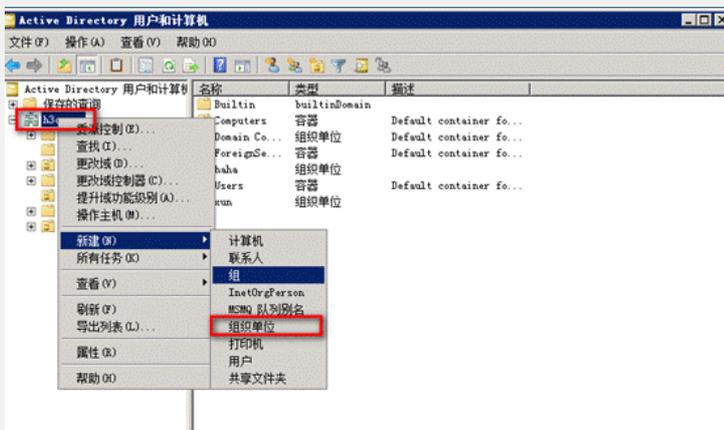


图3-11

(5): 在组织单元haha里面新建三个用户“x111”、“x112”、“x113”，并为其设置LDAP密码，勾选密码永不过期（新建用户时会自动提示创建密码）；

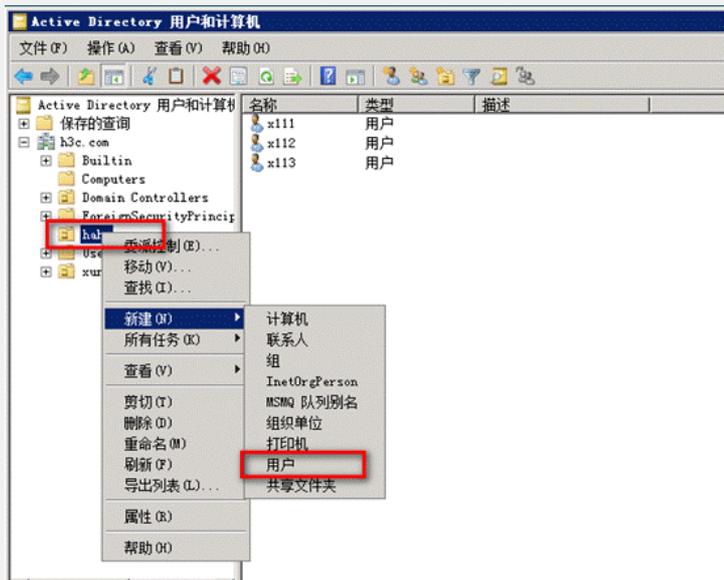


图3-12

效果如图3-13所示；

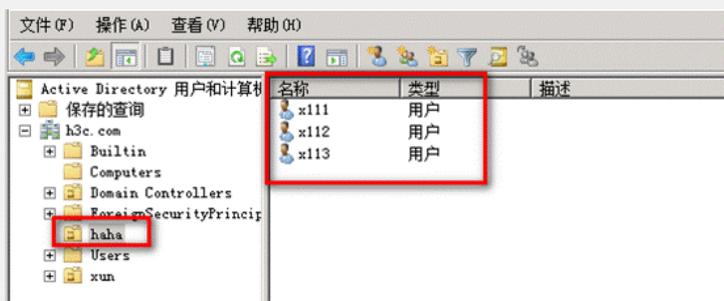


图3-13

(6): iMC中LDAP配置，业务-用户接入管理-LDAP业务管理-服务器配置，其中Base DN为获取用户数据的范围；对于LDAP服务器来说，管理员DN确定为图3-14所示；其他选项意义分别为：

服务器类型:分为通用LDAP服务器和微软活动目录。前者表示所有符合LDAP标准的服务器，后者专指Microsoft Windows活动目录；

服务器同步方式:当“服务器类型”设置为通用LDAP服务器时，该参数只能设置为手工指定；当“服务器类型”设置为微软活动目录时，该参数可以设置为手工指定或基于AD组；

手工指定:为LDAP服务器配置同步策略时，可以为绑定用户指定服务；

基于AD组:为LDAP服务器配置同步策略时，只能为LDAP组指定服务，根据绑定用户所属的LDAP组自动为用户分配服务。

LDAP服务器信息

基本信息

- 服务器名称: 10.2.0.2
- 服务器IP地址: 10.2.0.2
- 服务器类型: 微软活动目录
- 实时认证: 是
- 连接超时时间: 30 秒
- 用户分组: 手工指定
- 业务分组: 未分组

服务器信息

- 服务器版本: 3
- 端口: 389
- 服务器同步方式: 手工指定
- 连接超时时间: 1分钟
- 同步超时时间: 0 秒

高级信息

- Base DN: ou=haha,dc=h3c,dc=com
- 管理员DN: cn=admin,dc=h3c,dc=com
- 管理员密码: *****
- 用户名属性名称: sAMAccountName
- 用户密码属性名称: []

图3-14

配置完后点击检测，看到如图3-15提示说明配置成功，然后点击确定；

业务 >> 用户接入管理 >> LDAP业务管理 >> 服务器配置 >> 修改LDAP服务器信息

当前的配置正确，能与LDAP服务器“10.2.0.2”连接成功。

LDAP服务器信息

基本信息

- 服务器名称: 10.2.0.2
- 服务器IP地址: 10.2.0.2
- 服务器类型: 微软活动目录
- 实时认证: 是
- 连接超时时间: 30 秒
- 用户分组: 手工指定
- 业务分组: 未分组

服务器信息

- 服务器版本: 3
- 端口: 389
- 服务器同步方式: 手工指定
- 连接超时时间: 1分钟
- 同步超时时间: 0 秒

高级信息

- Base DN: ou=haha,dc=h3c,dc=com
- 管理员DN: cn=admin,dc=h3c,dc=com
- 管理员密码: *****
- 用户名属性名称: sAMAccountName
- 用户密码属性名称: []

图3-15

LDAP同步策略配置；

业务 >> 用户接入管理 >> LDAP业务管理 >> 同步策略配置 >> 修改LDAP同步策略

修改LDAP同步策略

基本信息

- 同步策略名称: chapv2ldap
- 服务器名称: 10.2.0.2
- 业务分组: 未分组
- Base DN: ou=haha,dc=h3c,dc=com
- 子BaseDN: ou=haha,dc=h3c,dc=com
- 过滤条件: (&(objectclass=user)(sAMAccountName=*))
- 状态: 有效

同步的用户类型

- 接入用户
- 设备管理用户

同步选项

- 自动同步
- 按需同步
- 新增用户及其接入帐号
- 为已存在用户新增接入帐号
- 仅同步当前节点下的用户

下一步 取消

图3-16

如果在LDAP配置了telephonenumber和mail，则选择从LDAP导入，当从LDAP服务器同步过来的用户和LDAP解除绑定关系后，认证时将使用图3-17配置的密码“h3c”。

修改LDAP同步策略

基本信息

- 用户姓名: cn
- 证件号码: sAMAccountName
- 通讯地址: 不从LDAP服务器同步
- 电话: telephonenumber
- 电子邮件: mail
- 用户分组: 未分组

接入信息

- 帐号名: sAMAccountName
- 帐号类型: 预付费帐号
- 预付金额: 0 元
- 失效日期: 不从LDAP服务器同步
- 密码: 不从LDAP服务器同步
- 密码: h3c
- 自助充值: 允许
- 最大闲置时长: 不从LDAP服务器同步
- 在线数量限制: 不从LDAP服务器同步
- 智能终端最大绑定数: 不从LDAP服务器同步
- 登录提示信息: 不从LDAP服务器同步

接入设备绑定信息

- 设备IP地址: 不从LDAP服务器同步
- 端口号: 不从LDAP服务器同步
- VLAN ID/内层VLAN ID: 不从LDAP服务器同步

图3-17

勾选之前创建的服务，点击完成；



图3-18

(7): PEAP认证域控配置, 业务-用户接入管理-业务参数配置;



图3-19

此处注意点较多:

- 1): 域控服务器全名为安装域控服务器PC的全名, 具体可通过单击我的电脑-右键-属性-查看;
- 2): 虚拟计算机名称和之前新建的保持一致;
- 3): 虚拟计算机密码为之前为虚拟计算机新建的密码。



图3-20

至此, iMC侧的配置全部完成, 接下来配置客户端。

3. iNode客户端配置:

- 1): 新建802.1x连接 (证书认证唯一支持);



图3-21

2) 选择证书认证里面的PEAP认证, 如图3-22所示, 安全密码为LDAP里面创建用户时设置的密码, 由于客户端不需要验证服务器, 所以不选择验证服务器证书, 当客户端安装有根证书时, 可勾选此项。

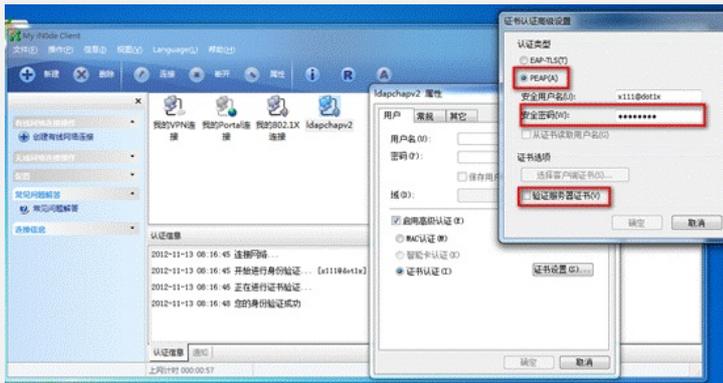


图3-22

配置完成后, 发起连接, 可以成功认证, 如上图3-22所示。

4. 配置关键点:

- 1) 该认证方式只能与802.1x配合, 不支持Portal认证方式;
- 2) 导入iMC的根证书和服务器证书为同一CA机构颁发; 服务器证书需先安装到IE里面, 导出后才能导入iMC中;
- 3) PEAP域控配置里面IP只能填写实际IP地址, 不能填写127.0.0.1;
- 4) iNode客户端认证时, 输入的密码为LDAP中为用户创建的密码, 解除绑定关系后使用iMC中创建的密码h3c;
- 5) 客户端认证时尽量不要携带前缀;
- 6) 有时PC认证不成功, 在配置正确时, 可以将域控服务器的类型选择为2003或以前, 此时可以解决问题。