陈斌A 2007-01-14 发表

## CAMS与AD配合做域统一认证的典型配置

## 一、组网需求:

支持802.1X的交换机; CAMS服务器; Microsoft Active Directory; iNode客户端。

### 二、组网图:

*服务器名称:	192. 168. 1. 11	* 服务器版本:	3	
* 服务器IP地址:	192. 168. 1. 11	* 端口:	389	
* 服务器类型:	通用LDAP服务器 🗸			
* Base DN:	ou=121, dc=h3c, dc=com			
* 自动连接间隔时长	5 分钟	☑ 是否连通服务器	1	
* 管理员DN:	cn=chenning, ou=ywrj, ou=121, dc=h3c, dc=com			
管理员密码:	•••••	* 是否需要实时认证:	否	
* 用户名属性名称:	saMAccountName	* 用户密码属性名称:	userPassword	
备份服务器IP地址		☑ 启用主服务器	□ 启用备份服务器	
🗌 从备份服务器自	动切换回主服务器	切换间隔时间:	24	

#### 设备说明:

NAS: S3952 CAMS V2.1 R0121SP1 Microsoft Active Directory 5.2 iNode V2.4-R0213

#### 三、配置步骤:

前提条件是CAMS, AD, NAS, User均路由可达。 NAS可以采用802.1X认证或者Portal认证, 这里已 802.1X认证为例。 1. 配置NAS # 配置Radius服务器 [S3952]radius scheme h3c [S3952-radius-h3c]server-type huawei [S3952-radius-h3c]primary authentication 192.168.1.12 1812 [S3952-radius-h3c]primary accounting 192.168.1.12 1813 [S3952-radius-h3c]primary accounting 192.168.1.12 1813 [S3952-radius-h3c]key authentication test [S3952-radius-h3c]key accounting test [S3952-radius-h3c]user-name-format without-domain

## # 配置认证域

[S3952]domain h3c [S3952-domain-h3c]radius-scheme h3c [S3952]domain default enable h3c

## # 配置VLAN

[S3952]Vlan 2 [S3952-vlan2]Port interface GigabitEthernet1/1/1 to GigabitEthernet1/1/4 [S3952]Interface vlan 2 \管理Vlan [S3952-Interface-vlan-2]ip add 192.168.1.99 255.255.255.0 [S3952]Interface vlan 1 \用户Vlan [S3952-Interface-vlan-1]ip add 192.168.0.1 255.255.255.0

# # 启动802.1X认证 [S3952] dot1x [S3952] dot1x authentication-method pap [S3952] dot1x interface Ethernet 1/0/1 to Ethernet 1/0/48

注: 这里只是列出了802.1X的所有必须的配置,还有一些高级选项可以自行配置,如 version check, accounting on等。

2. 配置CAMS

1). 配置接入设备参数:系统管理>>系统配置>>接入设备配置

这里必须将NAS的上行端口(靠近CAMS的端口)地址添加到起始地址和结束地址之 间。共享密钥和端口必须与设备的配置一致。

修议 12月前日 - 11月1月1日	出账   缴资   省停   黑名里 B.p.ik.A.   總券过录   计试去取自由	見以付資交型   強制下线   在 :   空会日本	鐵删除   时间科	信 铜尸	部助   ₩ 므 。	
(写)高思   上州998日   7	1/1914年   3000 旧水   以证大败口志				帐亏: ISY	
		帐号用户信息				
基本信息:					打印	
帐号 名	fsy	帐号类型	预付费中	预付费帐号		
胀号状态	正常	帐号余额	0.00 元	0.00 元		
用户姓名	fen	证件号码				
自用密码控制策略	否	下次登录须修改密码	否	否		
联系方式	fen	Enail地址	Email地址 fsy@aaa.bbb.ccc			
创建时间	2007-01-14	帐号失效时间	不限			
设备IP地址		端口号				
/LAN ID		是否绑定多IP、MAC地址	否			
用户IP地址		阿卡MAC地址	网卡MAC地址			
在线数量限制	1	最大闲置时长	最大闲置时长不限			
在线状态	不在线	修改密码/充值 不限				
登录提示信息						
LDAP服务器认证(LDAP服务器中存在此帐号)		服务器名称	1212			
<b>戸由法的服</b> 条信負・						
服务名	服务描述	计费策	146	服务后缀	详细信息	
(W		不计费	····		查询	

2). 配置LDAP服务器: 组件管理>>LDAP组件>>LDAP服务器管理

这里的Base DN就是指所要同步AD中目录的范围,即CAMS只同步该Base DN路径下 (包含所有子目录)的所有用户。若Base DN设置为根域h3c.com则会同步该AD中的 所有用户。

管理员DN指具有查询权限的AD中的用户,可以与Base DN不在同一目录。

管理员DN和BaseDN的命名规则为:从左到右,依次从最小子目录到根目录,中间用 逗号隔开。根目录前缀为dc=,原始目录(如users)和用户名(chenning)前缀为cn =,新建的目录前缀为ou=,用户名前缀。

对于AD服务器,用户名属性建议修改为saMAccountName

Internet 协议 (TCP/IP)	属性 ? 🔀
常规	
如果网络支持此功能,则可以系 您需要从网络系统管理员处获?	朱取自动指派的 IP 设置。否则, 最适当的 IP 设置。
○ 自动获得 IP 地址 (2) → 使用下面的 IP 地址 (S):	
IP 地址 (I):	192 .168 . 0 . 23
子网掩码 (U):	255 . 255 . 255 . 0
默认网关 @):	192 .168 . 0 . 1
○ 自动获得 DMS 服务器地址 ○ 使用下面的 DMS 服务器地	: (E) : 址 (E) :
首选 DNS 服务器 (P):	192 .168 . 1 . 11
备用 DNS 服务器(A):	
	高级(火)
	确定 取消

3). 同步测试:在LDAP服务器管理中选择建立的LADP服务器,点击行末的<同步>, 若设置正确,会出现同步成功的提示。



4). 配置LDAP同步配置:组件管理>>LDAP组件>>LDAP同步配置>>增加
 出现如下的配置选项,选择LDAP服务器,配置过滤条件。对于AD,建议过滤条件配置为:(&(distinguishedName=\*)(userPrincipalName=\*))。该过滤条件的意含义是选出
 同时具有distinguishedName和userPrincipalName属性的用户。



点击下一步选择个列的属性,建议如下图配置,再选择相关的服务和计费方式。由于 AD中的用户密码加密不可逆,不能同步到CAMS中,用户每次都会到AD中认证,所 以这里的CAMS本地密码可以任意设置。



5). 同步用户:在LDAP同步配置中选择同步配置,点击行尾的<同步>,则CAMS系统 会自动同步AD中的所有Base DN中的用户到CAMS中。若同步成功会会出现"同步LAD P服务器用户成功"的提示。



同步成切后会在这里的<同步用户管理>和用户管理>>账号用户中反现 LDAP用户。 至此,CAMS与AD同步完成,用户可以采用同步过来的用户进行LDAP认证。若需要 进行域统一认证,还需进行如下两步配置: 3. 配置客户端 1). 在iNode客户端中点击<新建>创建域统一认证了连接 🛃 iNode 智能客户端 文件(E) 操作(E) 信息(I) 视图(V) 帮助(H) 🎻 新建 🕌 删除 🛛 🥝 连接 💽 断开 🍈 🔦 属性 📃 安全 🔼 🥝 E 2 2 2 我的802.1x \*域统一认证 连接 帐户 EAD 连接操作 创建一个新的连接 🔼 最新安全检查结果 客户端配置选项 🥝 启动此连接 运行方式 日志级别 更改此连接的设置 🕌 删除此连接 启动方式 ☑ 启动域统一认证 (0) 启用域统一认证功能需要一个域统一认证连接, 如果您还没有创建这样的连接,请在下次登录域之前 创建它。 其它操作 1 配置客户端运行方式 E @ 查看帮助 窗口最小化一 连接信息 \$ ▼客户端启动后窗口最小化() 认证协议:802.1x 连接创建时间: 2007-1-14 19:59 确定 取消 \*域统一认证帐户 上网计时000:00:00 断开 2) 选择基本的认证方式,本例中为802.1X认证,再选择<域统一认证连接> LDAP组件 >> LDAP同步配置 >> 修改配置 修改配置 登录信息 \*帐号名: 用户密码: 不从LDAP服务器同步 ~ sallAccountname 用户密码: 密码确认: \* 用户姓名: 证件号码: di spl ayName × 联系方式: Y Email地址: userFrincipalName v nane \* 帐号类型: 预付费帐号 × 不从LDAP服务器同步 \* 預付金額: v 元 不从LDAP服务器同步 帐号失效时间: \* 不限 端口号: 设备IP地址: \*

۷ 修改密码/充值: 网卡MAC地址: \* 不限 v 在线数量限制: 最大闲置时长: 分钟 不从LDAP服务器同步 脊录提示信息: ~ 服务信息 选择 服务名称 服务描述 计费策略 服务后缀 不计费

用户IP地址:

3) 然后会在iNode中发现新的域统一认证连接,再在操作>>配置客户端运行方式中选 择启动域统一认证。



4. 配置用户电脑

VLAN ID:

1) 设置PC的网络连接,配置正确的DNS服务器。本例中DNS服务器和AD在同一台服 务器上。

系统管理 >> 系统配	置 >> 接入设备配置 >> 増加酯	置項			
		增加配	置项		
	* 初始IP地址:	192.168.1.9	9		
	结束IP地址:				
	* 共享密钥:	test			
	* 业务类型:	LAN接入业务	×		
	*端口列表:	1812, 1813			
	* 协议类型:	扩展协议	~		
	* RADIUS 报文类型:	标准报文	~		
			#094		
		NHAC IGE	U LAUT		
2) 将PC加入	、域: 在我的电脑:	>>属性>>计算	机名>>更改中的	输入域名,再辅	入域管理员
的用户名和额	密码, 用户就可以	加入到域中了。	2		
	LI	AP同步配置(1213	) 所同步的用户管	理	
	帐号名:		Email地址	:	
	用户状态:不限	~		查询	
	增加删除	全选 清	除重置	返回帮助	
	共有 2 条记录, 15 💌	条记录/页.	第1页/共1页	《 上一页 下一页 》	
帐号名 🗘	帐号类型 🔶	用户姓名	Enail地址	同步时间 🔶	用户状态 鈫
fsy	预付费帐号 	fen	fsy@h3c.com	2007-01-14 19:33:18	存在
bin	顶竹货帐亏	chen	bine h3c.com	2007-01-14 19:33:18	伊住
<b>四、预期效</b> 在PC登陆系	<b>果:</b> 统时,使用之前的	训建的域用户并	选择登陆到域		
新建连	接向导				
洗搔	车接类型				26
l	五五一五 五名用户连接和域统	认证连接无需配置	置协议属性		
C	普通连接(B) 您将需要一个用户。	名和密码来创建新	的连接。		
(	医名用户连接(A) 匿名用户连接没有: 匿名用户连接。	对应的用户名和密	冯,直接使用默认	的配置来创建一个	
G	● 類弦一认证连接( 在登录Windows域之 用户名和密码直接)	D) 前首先进行身份认 面过操作系统的登	证,通过认证后您 录界面获得。	才可以登录域。	
		<上─步®)	下步(10)>〕 [ ]	完成 (2) 🗌 🗌 取	消
占土确中后	今左丞吐容口的		计标志 1	正 建空注"的地	

点击确定后,会在登陆窗口的右侧出现"正在进行域统一认证,请等待"的提示,之后 成功登陆。若在CAMS中配置了EAD检查,则登陆到系统后,iNode还会对系统进行安 全检查,并采取相关策略。

# 五、配置关键点:

- 1. NAS上802.1x的认证模式必须为pap。
- 2. CAMS的服务和NAS中配置的默认域都必须采用AD中域的NetBIOS名称,默认情况下是域的第一部分,例如h3c.com,则如上两处都应设置为h3c。