Portal 张轩玮 2018-11-27 发表

组网及说明

1 配置需求或说明

1.1 适用产品系列

本案例适用于WAC380、WAC381、MSG系列的AC。

1.2 配置需求及实现的效果

无线电脑连接SSID:service后,无线电脑自动获取192.168.100.0/24网段ip,网关vlan100的ip地址:19 2.168.100.1/24,想要实现对无线用户的统一管理及认证功能。现已有LDAP服务器

(192.168.16.222/24) 提供认证服务,WAC380使能本地portal服务器功能,并作为无线网络的网关设备。通过Web页面输入aa /123456这组账号密码进行认证登录,LDAP服务器对用户进行身份认证,以达到对用户访问进行控制的目的。

2 组网图



配置步骤

1 配置步骤

1.1 在AC上配置相关VLAN及对应虚接口的地址 提示: ap注册和无线配置详细步骤参考《2.2.05 WAC380系列产品AP二层注册、无线加密配置方法(命令行版)》 在AC上配置相关VLAN及对应虚接口的地址,并放通对应接口。 创建VLAN100及其对应的VLAN接口,并为该接口配置IP地址。开启dhcp服务,Client使用该VLAN 接入无线网络 system-view [H3C] vlan 100 [H3C-vlan100] quit [H3C] interface vlan-interface 100 [H3C-Vlan-interface100] ip address 192.168.100.1 24 [H3C-Vlan-interface100] quit #开启DHCP服务器功能 [H3C]dhcp enable #配置地址池vlan100,分配192.168.100.0/24网段 [H3C]dhcp server ip-pool vlan100 [H3C-dhcp-pool-1]network 192.168.100.0 mask 255.255.255.0 #分配网关和DNS服务器地址, 网关是192.168.100.1, DNS服务器是114.114.114.114。 [H3C-dhcp-pool-1]gateway-list 192.168.100.1 [H3C-dhcp-pool-1]dns-list 114.114.114.114 [H3C-dhcp-pool-1]quit

1.2 配置LDAP方案
创建LDAP服务器Idap,并进入LDAP服务器视图。
[H3C] Idap server Idap
配置具有管理员权限的用户DN。
[H3C-Idap-server-Idap] login-dn cn=administrator,cn=users,dc=myias,dc=com
配置查询用户的起始目录。
[H3C-Idap-server-Idap] search-base-dn dc=myias,dc=com
配置LDAP认证服务器的IP地址。
[H3C-Idap-server-Idap] ip 192.168.16.222
配置具有管理员权限的用户密码。

[H3C-Idap-server-Idap] login-password simple 123456

创建LDAP方案Idap,并进入LDAP方案视图。 [H3C] Idap scheme Idap # 配置LDAP认证服务器。 [H3C-Idap-Idap] authentication-server Idap

1.3 创建ISP域Idap
 # 创建ISP域Idap,并进入ISP域视图。
 [H3C] domain Idap
 # 为Portal用户配置AAA认证方法为LDAP认证、不授权、不计费。
 [H3C-isp-Idap]authentication portal Idap-scheme Idap
 [H3C-isp-Idap] authorization portal none
 [H3C-isp-Idap] accounting portal none
 # 指定ISP域Idap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。
 [H3C-isp-Idap] authorization-attribute idle-cut 15 1024

1.4 配置Portal认证
配置PortalWeb服务器的URL为http://192.168.100.1 /portal。
[H3C] portal web-server newpt
[H3C-portal-websvr-newpt] url http://192.168.100.1/portal
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。
[H3C] portal local-web-server http
#配置本地Portal Web服务器提供认证页面文件为xxx.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)。
提示:设备自带压缩包defaultfile.zip,也可以使用该压缩包。
[H3C-portal-local-websvr-http] default-logon-page xxx.zip
[H3C-portal-local-websvr-http] quit

1.5 配置无线服务

[H3C] wlan service-template st1 [H3C-wlan-st-st1] ssid service [H3C-wlan-st-st1] vlan 100 # 使能直接方式的Portal认证。 [H3C-wlan-st-st1] portal enable method direct # 配置接入的Portal用户使用认证域为Idap。 [H3C-wlan-st-st1] portal domain Idap # 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。 [H3C-wlan-st-st1] portal apply web-server newpt # 使能无线服务模板。 [H3C-wlan-st-st1] service-template enable # 配置AP [H3C] wlan ap officeap model WA2620E-AGN [H3C-wlan-ap-officeap] serial-id 21023529G007C000020 [H3C-wlan-ap-officeap] radio 2 [H3C-wlan-ap-officeap-radio-2] service-template st1 [H3C-wlan-ap-officeap-radio-2] radio enable

1.6 配置LDAP服务器
 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。

1.6.1 添加用户aa
 # 在LDAP服务器上,选择[开始/管理工具]中的[H3Ctive Directory用户和计算机],打开Active Direct ory用户管理界面。
 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"节点下的按钮。 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。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。 新建用户aa

±π.).			
200).	*	本 分物层 (1)。	
]a	英文編与しい	
生名(人):	aa		
用户登录名(1)	:		
aa		@myias.com 💌	
用户登录名 (Wi	ndows 2000 l	以前版本)(2):	
HALYC/		99	

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。 设置用户密码:123456

密码(2):	*****
确认密码 (C):	*****
▼ 用户下次登录时	须更改密码 (11)
用户不能更改密	
密码永不过期 (D
一帐户已禁用(0)	

完成新建用户。 完成新建用户



1.6.2 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。 将用户加入组

SActive Directory 用户和计算机				_ D X
文件(E) 操作(A) 查看(E) 窗口	(1) 有助(1)			_[#] ×
		A 80		
		1.12		
Active Directory 用户和計算机 [Fsers 记 个对象			
20	8称	英型		
G D bullets	DHEP Administrators	安全组 - 本	对 DHCP 服务器有管理	
E Constant	DHCP Users	安全组 - 本	对 DHDP 服务只有只读	
R 20 Dennis Controllers	Directory Manager	月户		
R Terrai e Carrity Principal a	DasAleins	安全组 - 本	185 管理员组	
8 I tertin Hand	DasUpdateFroxy	安全组 - 全局	尤许替其他客户端 (如	
R R R R R	Donain Advins	安全组 - 全局	教定的城管理员	
Porran Data	Bonain Cosputers	安全组 - 全局	加入到贼中的所有工作	
8- System	Domain Controllers	安全領 - 全局	城中所省城控制器	
Uters	Domain Guests	安全道 - 全局	域的所有来宽	
	Donain Bars	安全領 - 全局	所有城田户	
	Tatararis, Linias	安全街 - 全島	今後の地定支持教育局	
	Gram Raline Creator Denor	安全街 - 全县	这个组成的成品可以依	
	Grant County Creator Veners	BP	在本方法设计管部式法	
	Wale from the form	C+# - *	新研究教育中心的	
1	ana post vice on our	80	8W/W/W/277712/18	
	TTTC INC.	Red . *	THE TREAM	
	1112 110	3318 * 4		
	TICK IAS	80	ECOP Internet G.	
	TIME INS	HP RC	用于启动进程对应用程	
	, key	HP RP		
	2 kf2838	用户	2101 (T + 110 K + +	
1	arbigt	用户	密钥女行中心服务物户	
	5 14f	月户		
	lideofeng	月户		
	liying	用户		
	F 11	月户		
	1 lw	月户		
1	aurket.	安全组 - 全局		
1	nc	用户		
	giyatong	月户		
	. ad	安全组 - 全局		
	DRAS and IAS Servers	安全祖 - 本	这个细中的服务器可以	
	C INCA	月户		

在右侧的Users信息框中右键单击用户aa,选择"属性"项。 选择用户

交 文件(1) 操作(1) 查看(1) 智口	1 图 帮助图			
⊳ → 🖻 🖩 👗 🛱 🗙 😭	3 🗟 🕄 🖬 💆 🏙 🗸	a 🕫		
	20 #B 00 20 #B 00 20 #D 00 <th></th> <th>単位 常常計算机の約00内置 対 DIGT 服务場省管理 対 DIGT 服务場省管理 対 DIGT 服务場省管理 対 DIGT 服务場省管理 対 DIGT 服务場省管理 対 DIGT 服务場省管理 対 DIGT 服务場合管理 対 DIGT 服务者管理 対 DIGT RES 指示: DIGT RES</th> <th></th>		単位 常常計算机の約00内置 対 DIGT 服务場省管理 対 DIGT 服务場省管理 対 DIGT 服务場省管理 対 DIGT 服务場省管理 対 DIGT 服务場省管理 対 DIGT 服务場省管理 対 DIGT 服务場合管理 対 DIGT 服务者管理 対 DIGT RES 指示: DIGT RES	
	Goroup Policy Creator Owners Weest MalpServicesGroup Anavei	安全道 - 全局 用户 安全道 - 本 用户	这个组中的成员可以修 供来发访问计算机成访 帮助和支持中心组	
	THIS_WE INCE_IAS INAM_IAS INAY	安全组 - 本 用户 用户 用户	IIS 工作进程组 置名访问 Internet 值 用于启动进程外应用程	

#选择"隶属于"页签,并单击"添加(D)…"按钮。

[唐士 (M): 名称	Active Directory 文件事
Domain Users	myias.com/Users
泰加 (1)	重勝(医)
泰加 @)	田時(臣)

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。 添加用户aa到用户组Users

Attra Directory 用户的计算机 Constant 22 个分類 Constant Con	文件(1) 操作(1) 查看(1) 查看(1) 单	® Ø 3 ⊡ 10 ∰ 10 ≪ (1) m	_18)
	Antire Burstop AD-26(1924, [True Delives Develop AD-26(1924, [Delives Cases of the Constant of the Consta	22 小方法 22	

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)…" ·在弹出的密码添加对话框中设置管理员密码。

1.7 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。 通过执行以下显示命令查看WAC上生成的Portal在线用户信息。 dis portal user all Username: aa AP name: 586a-b1fa-8380 Radio ID: 1 SSID: service Portal server: newpt State: Online VPN instance: N/A MAC IP VLAN Interface b841-a468-d9bd 192.168.100.7 100 WLAN-BSS1/0/5

配置关键点