WLC和NAC访客服务器(NGS)集成指南

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> <u>使用的组件</u> <u>规则</u> <u>背景信息</u> 配置无线 LAN 控制器 (WLC) <u>初始化</u> <u>Cisco NAC Guest Server</u> <u>相关信息</u>

<u>简介</u>

本文档提供了集成 NAC Guest Server 和无线 LAN 控制器的指南。

<u>先决条件</u>

<u>要求</u>

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本:

- Cisco 无线 LAN 控制器 (WLC) 4.2.61.0
- 带有 IOS® 12.2(25)SEE2 版的 Catalyst 3560
- Cisco ADU 4.0.0.279 版
- NAC Guest Server 1.0 版

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

<u>规则</u>

有关文档规则的详细信息,请参阅 <u>Cisco 技术提示规则。</u>

<u>背景信息</u>

Cisco NAC Guest Server 是为来宾、访客、承包商、顾问或客户提供临时网络访问权的完整配置和 报告系统。Guest Server 与 Cisco NAC Appliance 或 Cisco 无线 LAN 控制器配合工作,后者为访 客访问提供捕获式门户和实施点。

Cisco NAC Guest Server 允许拥有权限的任何用户轻松地创建临时访客帐户和邀请访客。Cisco NAC Guest Server 对邀请人(创建访客帐户的用户)执行完整的身份验证,并允许邀请人通过打印 输出、电子邮件或 SMS 将帐户详细信息提供给访客。系统会存储从创建用户帐户到访客访问网络 的完整体验以进行审计和报告。

在创建访客帐户时,系统会在 Cisco NAC Appliance Manager (Clean Access Manager) 中配置它 们,或将它们存储在 Cisco NAC Guest Server 上的内置数据库中。当您使用 Guest Server 的内置 数据库时,外部网络接入设备(例如 Cisco 无线 LAN 控制器)可以利用远程身份验证拨入用户服务 (RADIUS) 协议根据 Guest Server 对用户进行身份验证。

在创建帐户时,Cisco NAC Guest Server 会为访客帐户配置指定的有效期。在帐户过期后,Guest Server 将直接从 Cisco NAC Appliance Manager 中删除帐户,或发送 RADIUS 消息来通知网络接入设备 (NAD) 帐户剩余的有效时间长度,在该时间长度后,NAD 必须删除用户。

Cisco NAC Guest Server 提供了重要的访客网络访问记帐,方法是合并从创建访客帐户到访客使用 帐户的整个审计跟踪过程,以便可以通过中心管理界面执行报告。

访客访问概念

Cisco NAC Guest Server 利用许多术语来解释提供访客访问所需的组件。

来宾用户

访客用户是需要用户帐户来访问网络的人。

发起人

邀请人是创建访客用户帐户的人。此人通常是提供网络访问的组织的员工。邀请人可以是承担某些 工作职责的特定个人,也可以是可以根据企业目录(例如 Microsoft Active Directory (AD))进行身 份验证的任何员工。

网络实施设备

这些设备是提供网络访问的网络基础设施组件。另外,网络实施设备将访客用户推送到捕获式门户 ,他们可以在其中输入其访客帐户详细信息。当访客输入其临时用户名和密码时,网络实施设备将 根据 Guest Server 所创建的访客帐户来检查这些凭证。

Guest Server

这是 Cisco NAC Guest Server,它将所有访客访问连接在一起。访客服务器将这些链接在一起:创 建访客帐户的发起人、传递到访客的帐户详细信息、针对网络实施设备的访客身份验证,以及访客 的网络实施设备与访客服务器的验证。另外,Cisco NAC Guest Server 合并网络实施设备中的记帐 信息以提供单点访客访问报告。

在 CCO 中提供了有关 NGS 的详细文档。

http://www.cisco.com/en/US/docs/security/nac/guestserver/configuration_guide/10/nacguestserver/ .html



<u> 配置无线 LAN 控制器 (WLC)</u>

请按照以下步骤配置 WLC:

- 1. 初始化控制器和接入点。
- 2. 配置控制器接口。
- 3. 配置 RADIUS。
- 4. 配置 WLAN 设置。

<u>初始化</u>

对于初始配置,请使用控制台连接(例如 HyperTerminal)并按照设置提示来填充登录和接口信息 。**reset system 命令也可启动这些提示。**

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_44:36:c3]: WLC
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): admin
Service Interface IP Address Configuration [none][DHCP]: <ENTER>
Enable Link Aggregation (LAG) [yes][NO]:no
Management Interface IP Address: 10.10.51.2
Management Interface Default Router: 10.10.51.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 2]: 1
```

Management Interface DHCP Server IP Address: 10.10.51.1 AP Transport Mode [layer2][LAYER3]: layer3 AP Manager Interface IP Address: 10.10.51.3 AP-Manager is on Management subnet, using same values AP Manager Interface DHCP Server (10.10.5<X>.1):<ENTER> Virtual Gateway IP Address: 1.1.1.1 Mobility/RF Group Name: mobile-1 Enable Symmetric Mobility Tunneling: No Network Name (SSID): wireless-1 Allow Static IP Addresses [YES] [no]: <ENTER> Configure a RADIUS Server now? [YES][no]:<ENTER> Enter the RADIUS Server's Address: 10.1.1.12 Enter the RADIUS Server's Port [1812]:<ENTER> Enter the RADIUS Server's Secret: cisco Enter Country Code (enter 'help' for a list of countries) [US]:<ENTER> Enable 802.11b Network [YES][no]:<ENTER> Enable 802.11a Network [YES] [no]:<ENTER> Enable 802.11g Network [YES] [no]:<ENTER> Enable Auto-RF [YES] [no]:<ENTER> Configure a NTP server now? [YES][no]: no Configure the system time now? [YES][no]: yes Enter the date in MM/DD/YY format: mm/dd/yy Enter the time in HH:MM:SS format: hh:mm:ss

Cisco NAC Guest Server

Cisco NAC Guest Server 是为客户端(例如访客、承包商等)提供临时网络访问的配置和报告解决 方案。Cisco NAC Guest Server 与 Cisco 统一无线网络或 Cisco NAC Appliance 解决方案配合工作 。本文档指导您完成将 Cisco NAC Guest Server 与 Cisco WLC 集成的步骤,这将可以创建访客用 户帐户并验证访客的临时网络访问。

按照以下步骤完成集成:

 在 WLC 中添加 Cisco NAC Guest Server 作为身份验证服务器。浏览到您的 WLC(https://10.10.51.2, admin/admin)来执行以下配置。选择 Security > RADIUS > Authentication。

 cisco		<u>w</u> lans <u>c</u>	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	RADIUS	Authentica	ation Serve	rs					
General RADIUS	Call Stat	ion ID Type	IP Address						
Authentication Accounting Fallback TACACS+	Network	Management	Server t Index	Server Addres	is Port	uires a key wrap (Sec	Admin Status	
LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	<u>v</u>	<u> </u>	1	10.1.1.12	1812	Die	abled	Enabled	

选择 New。添加 Cisco NAC Guest Server 的 IP 地址 (10.1.1.14)。添加共享密钥。确认共享 密钥。

uluulu cisco	MONITOR WLANS CONTROL	LLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security	RADIUS Authentication S	ervers > New
AAA General RADIUS	Server Index (Priority)	2 •
Authentication Accounting	Server IPAddress	10.1.1.14
Fallback TACACS+	Shared Secret Format	ASCII -
LDAP Local Net Users	Shared Secret	•••••
Disabled Clients User Login Policies	Confirm Shared Secret	*****
AP Policies	Key Wrap	(Designed for FIPS customers and requires a key wrap compliant RADIUS server)
 Priority Order 	Port Number	1812
Access Control Lists	Server Status	Enabled T
Wireless Protection Policies	Support for RFC 3576	Enabled •
Web Auth	Server Timeout	2 seconds
Advanced	Network User	Exchine .
	Network User	r Enable
	Management	🔽 Enable
	IPSec	Enable

选择 Apply。

սիսիս cisco	MONITOR	WLANS C	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	RADIUS	Authentica	tion Serv	ers					
 AAA General RADIUS Authentication Accounting Fallback 	Call Stat Use AES Network	ion ID Type Key Wrap	IP Addres	s	ners and req	uires a key wrap c	ompliant RADIU	S server)	
FIACACS+	User	Management	Index	Server Addres	s Port	IP	Sec	Admin Status	
LDAP Local Net Users	4	v	1	10.1.1.12	1812	Dis	abled	Enabled	
MAC Filtering Disabled Clients User Login Policies	4	v	2	10.1.1.14	1812	Dis	abled	Enabled	

2. 在 WLC 中添加 Cisco NAC Guest Server 作为记帐服务器。选择 Security > RADIUS

>Accounting. Sage Configuration Eng | Logout | Befresh CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP Apphy Nem... Security RADIUS Accounting Servers Apphy Nem... * AAA General * RADIUS Accounting * TACACS+ Local Net Users Network User Server Index Server Address Port IPSec Admin Status * TACACS+ Local Net Users MAC Filtering Disabled Clents User Login Pasicies AP Policies Network User Server Address Port IPSec Admin Status

选择 New。添加 Cisco NAC Guest Server 的 IP 地址 (10.1.1.14)。添加共享密钥。确认共享 密钥。

، را، را، cısco	MONITOR WLANS CO	NTROLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	нецр
Security	RADIUS Accounting	Servers > New				
AAA General RADIUS Authentication Accounting	Server Index (Priority) Server IPAddress	2 •				
Fallback TACACS+	Shared Secret Format	ASCII ·				
LDAP Local Net Users MAC Filtering	Shared Secret	*****				
Disabled Clients User Login Policies AP Policies	Confirm Shared Secret	•••••		1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-		
Local EAP	Port Number	1813				
Priority Order	Server Status	Enabled 💌				
Access Control Lists	Server Timeout	2 seconds				
 Wireless Protection Policies 	Network User	E Enable				
Web Auth	Hetwork User	r chable				
Advanced	IPSec	Enable				

选择 Apply。

սիսիս cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECU	RITY M <u>a</u> n	AGEMENT	COMMANDS	HELP
Security	RADIUS A	Accounti	ng Servers						
▼ AAA General	Network User	Server	Server /	Address	Port	IPSec	A	dmin atus	
+ RADIUS	~	1	10.1.1.1	2	1813	Disabled	Er	abled	3
Accounting	V	2	10.1.1.1	4	1813	Disabled	Er	abled	3
Authentication Accounting Fallback	۷ ۲	1	10.1.1.1	4	1813	Disabled	Er	abled	3

3. 修改 WLAN(无线 x)以使用 NAC Guest Server。编辑 WLAN(无线 x)。选择 Security 选 项卡。将第 2 层安全更改为 None,并将第 3 层安全更改为使用 Web Authentication。

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
CISCO WLANS WLANS MLANS Advanced	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP WLANS > Edit General Security QoS Advanced Layer 2 Layer 3 AAA Servers Layer 3 Security None Web Policy 2 Authentication Passthrough Conditional Web Redirect Preauthentication ACL None Over-ride Global Config Enable

选择"Security"选项卡下的 AAA Servers。在"Server 1"框下,选择 RADIUS server (10.1.1.14)。在"Server 1"框下,选择 Accounting Server (10.1.1.14)。

ı. cısco	MONITOR MLA	NS CONTROLLER	WIREL	ESS SECURITY	MANAGEMENT	COMMANDS HEL	,	Saye Confi
WLANs	WLANs > Edit							
- WLANs	General 5	ecurity QoS	Advan	iced				
WLANs	Layer 2	Layer 3 AAA	Servers					
	Select AAA se Radius Serve	ervers below to ov ers Authentication Sec	erride use wers A	on this WLAN	LDAP Server Server 1	s None		
			P	Enabled		Server 2	None	•
	Server 1	1P:10.1.1.14, Port:	1812 -	IP:10.1.1.14, Port:18	13 -	Server 3	None	•
	Server 2	None		None	•			
	Server 3	None	•	None	*			
	Local EAP Au	thentication						
	Local EAP	Authentication	nabled					

选择 Advanced 选项卡。启用 Allow AAA Override。这允许从 NAC Guest 设备设置每客户端 会话超时。

MONITOR WLANS CONTROLLER WIRELESS SECURITY MAN	Sage Config AGEMENT COMMANDS HELP
General Security QoS Advanced Allow AAA Override Enabled H-REAP Local Switching Enabled Enabled Enabled Enabled Enabled Disanostic Channel Enabled IPv6 Enable Override Interface ACL P2P Blocking Action Client Exclusion Enabled Fenabled Fenabled Timeout Value (secs) 	DHCP DHCP Server DHCP Addr. Assignment Required Management Frame Protection (MFP) Infrastructure MFP Protection MFP Client Protection DTIM Period (in beacon intervals) 802.11a/n (1 - 255) 1
	MONITOR WLANS CONTROLLER WIRELESS SECURITY MAN WLANS > Edit General Security QoS Advanced Allow AAA Override Imabled H-REAP Local Switching Enabled Enable Session Timeout [1800] Session Timeout (secs) Aironet IE Diagnostic Channel Enabled IPv6 Enable Override Interface ACL P3P Blocking Action Disabled Client Exclusion f Imabled Senabled Senabled Timeout Value (secs) Senabled

注意:在SSID上启用AAA override时,NGS上的访客用户的剩余寿命将作为访客用户登录时的会话超时推送到WLC。选择 Apply 来保存您的 WLAN 配置。

cisco		WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP		
WLANs	WLANs >	Edit								
VLANS	General	Securi	ty QoS	Advanced						
Advanced	Profile N	lame	wireles	s-1						
	SSID		wireles	s-1						
	Status		🗹 Ena	✓ Enabled						
	Security Policies		Web-/ (Modific	Web-Auth (Modifications done under security tab will appear after applying the cha						
	Radio Po Interfac Broadca	olicy e st SSID	All manag F Enab	ement 💌						

4. 验证是否在 Cisco NAC Guest Server 中将控制器添加为 Radius 客户端。浏览到 NAC Guest Server (https://10.1.1.14/admin) 来执行以下配置。**注:如**果您在URL中指定/admin,您将看 到"管理"(Administration)页面。



© Cisco 2007 Version 1.0.0

System Log

重新启动 Radius 服务以使更改生效。选择 **Radius Clients**。选择"Restart Radius"框中的 **Restart。**

cisco	Radius Clients
Main Home/Summary Logout	- Radius Clients
Authentication Local Users AD Authentication Admin Accounts User Groups	WIC
Guest Policy Username Policy Password Policy	
vices NAC Appliance Radius Clients Email Settings SMS Settings	Add Radius Edit Radius Delete Radius
er Interface emplates tapping	If any changes are made to the radius clients please click the Restart Radius button to apply them. Restart
erver Network Settings Date/Time Settings SSL Settings System Log	
isco 2007 Version	1.0.0

5. 在 Cisco NAC Guest Server 中创建本地用户,即,Lobby Ambassador。选择 Local Users。 选择 Add User。注意:您必须填写所有字段。输入名字:lobby。输入姓氏:Ambassador。 输入用户名:lobby。输入密码:密码。保留组为 Default。输入电子邮件地址 :lobby@xyz.com。选择 Add User。

I.

Main Homa/Summary Logout Local User Accounts can create guest user accounts. Authentication Local Users AD Authentication Admin Accounts User Groups First Name: jobby Last Name: jobby Guest Policy Username Policy Password Policy Password Policy Repeat Password; Devices NAC Appliance Radius Cients Email Settings SMS Settings Group: DEFAULT User Interface Templass Mapping	cisco	Add a Local User Account	
Home/Summary Logout First Name: obby Authentication Local Users AD Authentication Admin Accounts User Groups Deloy Password Policy Password Policy Password Policy Devices NAC Appliance Radius Clients Email Address: obby@xyz.com Email Address: obby@xyz.com SMS Settings SMS Settings Date/Time Settings SSL Settings SSL Settings SSL Settings SSL Settings SSL Settings	Main	- Local User Accounts can create gues	st user accounts.
Authentication Last Name: Ambassador Local Users AD Authentication AD Authentication Username: lobby User Groups Password: "****** Guest Policy Repeat Password: "****** Username Policy Group: DEFAULT Password Policy Group: DEFAULT NAC Appliance Email Address: lobby@xyz.com Redius Clients Email Address: lobby@xyz.com Email Settings Add User SMS Settings Add User Server Network Settings Network Settings System Log	Home/Summary Logout	First Name:	lobby
AD Authentication Admin Accounts User Groups Guest Policy Username Policy Password Policy Password Policy Password Policy Devices NAC Appliance RAdius Citents Email Settings SMS Settings SMS Settings Sature Interface Templetes Mapping Server Network Settings SSL Settings System Log O Cisco 2007 Version 1.0.0	Authentication Local Users	Last Name:	Ambassador
User Groups Guest Policy Usemame Policy Password Policy Password Policy Devices NAC Appliance Radius Clients Email Settings SMS Settings User Interface Templates Mapping Server Network Settings SSL Setting SSL Setting SSL Sett	AD Authentication Admin Accounts	Username:	lobby
Guest Policy Repeat Password: Username Policy Group: Devices NAC Appliance NAC Appliance Email Address: Devices Iobby@xyz.com Email Settings Add User SMS Settings Add User Vaser Interface Add User Templates Add User Network Settings Sstreer Network Settings Sst. Settings SSL Settings System Log	User Groups	Password:	
Devices Group: DEFAULT NAC Appliance Email Address: Jobby@xyz.com Email Settings Add User SMS Settings Add User User Interface Add User Templates Mapping Server Network Settings Satisfies Satisfies Viser Interface Settings Server Network Settings Satisfies Settings System Log O Cisco 2007 Version 1.0.0	Guest Policy Username Policy Password Policy	Repeat Password:	
Proc. Appliance Radius Clients Email Address: lobby@syz.com User Interface Templates Mapping Server Network Settings Date/Time Settings SSL Settings SSL Settings System Log	Devices	Group:	DEFAULT
Add User Reset Form Templates Mapping Server Network Settings Data/Time Settings SSL Settings System Log © Cisco 2007 Version 1.0.0	Radius Clients Email Settings SMS Settings	Email Address:	lobby@xyz.com
Server Network Settings Date/Time Settings SSL Settings System Log	User Interface Templates Mapping		Add User Reset Form
© Cisco 2007 Version 1.0.0	Server Network Settings Date/Time Settings SSL Settings System Log		
	© Cisco 2007 Version	1.0.0	

6. 作为本地用户登录并创建访客帐户。浏览到 NAC Guest Server (https://10.1.1.14),使用您在 步骤 5 中创建的用户名/密码登录,然后执行以下配置

:



Cisco 2007

7. 连接到访客 WLAN 并作为访客用户登录。将您的无线客户端连接到访客 WLAN (无线 x)。 打开 Web 浏览器以重定向到 Web-Auth 登录页。注意:或者,键入https://1.1.1.1/login.html以 重定向到"登录"页面。输入您在步骤 6 中创建的访客用户名。输入在步骤 6 中自动生成的密码 。通过 Telnet 登录到 WLC 并使用 show client detail 命令验证是否设置了会话超时。当会话 超时到期时,访客客户端将断开连接,并且您的 ping 将停止。

(Cisco Controller) >show client detail 80:13:e8:b7	2:5e:dd
Client MAC Address	00:13:e8:b7:5e:dd
Client Username	podx@cisco.com
AP MAC Address	00:17:df:a6:e5:f0
Client State	Associated
Vireless LAN Id	1
BSSID	00:17:df:a6:e5:ff
Channel	68
IP Address	10.1.1.22
Association Id	1
Authentication Algorithm	Open System
Reason Code	0
Status Code	0
Session Timeout	59
Client CCX version	4
Client E2E version	1
Mirroring	Disabled
QoS Level	Silver
Diff Serv Code Point (DSCP)	disabled
882.1P Priority Tag	disabled
WMM Support	Enabled
U-APSD Support	Disabled
Mobility State	Local
More or (q)uit	
(Cisco Controller) >	

注意:要设置从无线LAN控制器(WLC)到NAC访客服务器(NGS)的Web身份验证,您需要对Web身 份验证属性使用PAP模式身份验证。如果 Web 身份验证策略设置为 CHAP,则身份验证将失败 ,因为 NGS 不支持 CHAP。

相关信息

- Cisco NAC Appliance Clean Access Manager 安装和配置指南, 4.1(3) 版
- Cisco NAC Appliance 交换机和无线 LAN 控制器支持
- Cisco 无线 LAN 控制器配置指南 7.0.116.0 版
- <u>(视频)Cisco 身份服务引擎 (ISE) 和无线 LAN 控制器 (WLC) 的集成</u>
- NAC(Clean Access): 配置访客访问
- •部署指南:使用思科无线局域网控制器的思科访客接入,版本4.1
- <u>技术支持和文档 Cisco Systems</u>

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。