# 通过Microsoft NPS对AireOS WLC的管理访问

### 目录

<u>简介</u> <u>先决条件</u> <u>要求</u> <u>使用的组件</u> <u>背景信息</u> 配置 WLC 配置 <u>Microsoft NPS配置</u> <u>验证</u> 故障排除

## 简介

本文档介绍如何通过Microsoft网络策略服务器(NPS)为AireOS WLC GUI和CLI配置管理访问。

## 先决条件

### 要求

Cisco 建议您了解以下主题:

- •无线安全解决方案知识
- AAA和RADIUS概念
- Microsoft Server 2012基础知识
- 安装Microsoft NPS和Active Directory(AD)

#### 使用的组件

本文档中提供的信息基于以下软件和硬件组件。

- 8.8.120.0上的AireOS控制器(5520)
- Microsoft Server 2012

**注意:**本文档旨在向读者提供Microsoft服务器上WLC管理访问所需配置的示例。本文档中介 绍的Microsoft Windows服务器配置已在实验室中测试,并发现可以按预期工作。如果配置有 问题,请联系Microsoft获取帮助。思科技术支持中心(TAC)不支持Microsoft Windows服务器 配置。Microsoft Windows 2012安装和配置指南可在Microsoft技术网上找到。

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。

## 背景信息

当访问WLC CLI/GUI时,系统会提示用户输入凭证以成功登录。凭证可以针对本地数据库或外部 AAA服务器进行验证。在本文档中,Microsoft NPS用作外部身份验证服务器。

### 配置

在本示例中,在AAA(NPS)viz上配置了两个用户。loginuser和adminuser。loginuser只具有只读访问权限,而adminuser被授予完全访问权限。

#### WLC 配置

步骤1.在控制器上添加RADIUS服务器。导航至**Security > RADIUS > Authentication**。单击**New**以 添加服务器。确保**management**选项已启用,以便此服务器可用于管理访问,如此图所示。

cisco		<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	Sa EEEDB
Security	RADIUS	Authenti	cation Server	rs > Edit					
<ul> <li>AAA         <ul> <li>General</li> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> <li>Auth Cached Users</li> <li>Fallback</li> <li>DNS</li> <li>Downloaded AVP</li> </ul> </li> <li>TTACACS+         <ul> <li>LDAP</li> <li>Local Net Users</li> <li>MAC Filtering</li> <li>Disabled Clients</li> <li>User Login Policies</li> <li>AP Policies</li> <li>Password Policies</li> </ul> </li> <li>Local EAP         <ul> <li>Advanced EAP</li> <li>Priority Order</li> <li>Certificate</li> <li>Access Control Lists</li> <li>Wireless Protection</li> <li>Policies</li> <li>Web Auth</li> <li>TrustSec</li> <li>Local Policies</li> </ul> </li> </ul>	Server In Server Ad Shared Si Shared Si Confirm S Key Wrap Apply Cis Apply Cis Port Num Server St Support f Server Til Network I Managem Tunnel Pin Realm Lis PAC Provi IPSec Cisco ACA	Authenti dex ddress(Ipv4 ecret Forma ecret Shared Secr bar co ISE Defa co ACA Def ber atus for CoA meout User sent sent Retrans oxy & isioning	/Ipv6) at ret ault settings ault settings	2 10.106.33.39 ASCII ©  (Designed fo 0 1812 Enabled © 5 secon ✓ Enable 5 secon Enable Enable Enable	e FIPS custom ds	ers and requires a i	œy wrap complia	nt RADIU	S server;
h Advanced									

步骤2.导航至"安**全">"优先级订单">"管理用户**"。确保RADIUS被选作身份验证类型之一。

MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT
Priority O	rder > N	/lanagement L	Jser		
Authentica	ition				
Not U	sed		Order U	sed for Authe	ntication
TACACS	+	>		RADIUS LOCAL	Up
		<			Down

**注意:**如果选择RADIUS作为身份验证顺序中的第一个优先级,则仅当RADIUS服务器无法访问时,本地凭证才用于身份验证。如果选择RADIUS作为第二优先级,则首先根据本地数据库验证RADIUS凭证,然后根据已配置的RADIUS服务器检查。

#### Microsoft NPS配置

步骤1.打开Microsoft NPS服务器。右键单击"Radius Clients(**Radius客户端)**"。单击**New**将WLC添加为RADIUS客户端。

输入所需的详细信息。请确保在添加RADIUS服务器时共享密钥与控制器上配置的密钥相同。

<b></b>	WLC Properties X	x
File Action View Help File Action View Help Policies	WLC Properties       ×         Settings       Advanced         Image: Select an existing template:       v         Name and Address       Friendly name:         WLC       Address (IP or DNS):         Image: WLC       Verfy         Shared Secret       Select an existing Shared Secrets template:         None       v         To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.         Image: Manual       Generate         Shared secret:       Image: Manual	x
< III >	OK Cancel Apply	

步骤2.导航至Policies > Connection Request Policies。右键点击以添加新策略,如图所示。

•	Cisco WLC Properties
File Action View Help	Overview Conditions Settings
🗢 🔿 🙎 🖬 📓 🖬	Policy name: Osco WLC
<ul> <li>NPS (Local)</li> <li>RADIUS Clients and Servers</li> <li>RADIUS Clients</li> <li>Remote RADIUS Server</li> <li>Policies</li> <li>Connection Request Po</li> <li>Network Policies</li> <li>Health Policies</li> <li>Network Access Protection</li> </ul>	Policy State If enabled, NPS evaluates this policy while processing connection requests. If disabled, NPS does not evalue this policy. ✓ Policy enabled Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but nether is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.
👂 🚮 System Health Validato	Type of network access server:
<ul> <li>Bernediation Server Gro</li> <li>▲ Accounting</li> <li>▶ ➡ Templates Management</li> </ul>	Vendor specific:
< III >	OK Cancel Apply

步骤3.在"条件**"选**项卡下,**选择NAS**标识符作为新条件。出现提示时,输入控制器的主机名作为值 ,如图所示。

	Cisco WLC Properties	x
Overview Conditions Settings	15	
Configure the conditions for this If conditions match the connect connection request, NPS skips	s network policy. ction request, NPS uses this policy to authorize the connection request. If conditions do not match the s this policy and evaluates other policies, if additional policies are configured.	
Condition	Value	1
NAS Identifier	Cisco-WLC	
Condition description: The NAS Identifier condition spi syntax to specify NAS names.	pecifies a character string that is the name of the network access server (NAS). You can use pattern matching	
	Add Edit Remove	]
	OK Cancel App	у

步骤4.导航至Policies > Network Policies。右键单击以添加新策略。在本示例中,策略名为Cisco WLC RW,这意味着策略用于提供完全(读写)访问。确保策略配置如下所示。

0	Cisco WLC RW Properties	×
File Action View Help File Action View Help NPS (Local) A RADIUS Clients and Servers RADIUS Clients Remote RADIUS Server Policies Connection Request Po Network Policies Health Policies Network Access Protection Accounting Methods Management	Cisco WLC RW Properties         Overview       Conditions       Constraints       Settings         Policy name:       Disco WLC RW         Policy State       If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.         If enabled       Access Permission         If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. What is access permission?         Image: The Connection request matches this policy.	
Templates Management	<ul> <li>● Grant access. Grant access if the connection request matches this policy.</li> <li>○ Deny access. Deny access if the connection request matches this policy.</li> <li>✓ Ignore user account dial-in properties.</li> <li>If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts.</li> <li>Network connection method</li> <li>Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but nether is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.</li> <li>● Type of network access server:</li> <li>Unspecified</li> <li>✓</li> <li>○ Vendor specific:</li> <li>10  </li> </ul>	
× · · · · · · · · · · · · · · · · · · ·	OK Cancel Appl	y .

步骤5.在"条件"选**项卡**下,单击"**添加"**。选择用**户组**,然后单**击添**加,如图所示。

				Cisco V	VLC RW Pro	perties				2
Overview	Conditions	Constraints	Settings							
Configure	the condition	is for this netv	ork policy							
If condition	ns match the n request, N	connection r PS skips this p	equest, NP policy and (	S uses this policy evaluates other po	to authorize the blicies, if addition	connection al policies a	n request. If co are configured.	nditions do not matc	h the	
				Se	lect condition	on				x
Select	a condition, a	nd then click	Add.							
Group	S									^
10	Windows The Windo groups.	Groups ws Groups o	ondition sp	ecifies that the c	onnecting user	or compute	er must belong	to one of the selec	ted	=
1	The Machine	ne Groups co	ndition sp	ecifies that the co	onnecting comp	uter must b	belong to one o	of the selected group	ps.	
HCAP	The User (	ips àroups condit	ion specif	ies that the conne	ecting user mus	t belong to	one of the sel	ected groups.		
	Location ( The HCAP required to network ac	Groups Location Gro match this p cess servers	ups condi blicy. The (NASs). S	tion specifies the HCAP protocol is See your NAS do	Host Credentia used for comm cumentation bef	I Authoriza nunication ore using t	ation Protocol ( between NPS a his condition.	(HCAP) location gro and some third part	oups y	~
								Add	Cancel	
							Add	Edit	Remove	•

步骤6.在显示的对**话框中**单击"添加组"。在显示**的"**选择组"窗口中,选择所需**的对象类型**和**位置,并 输入所需的对象名称,如图所示。** 

	Cisco WLC RW	Propertie	s		
)v	User Groups	x			
C If	Specify the group membership required to match this policy.		on reque	st. If conditions do not match the	
	Groups		are con	tigured.	x
					~
			iter must	elong to one of the selected	
	Add Groups Remove		belong	to one of the selected groups.	
ŀ	OK C Select Group	ancel	o one of	the selected groups.	
Г	Select this object type:			col (HCAP) location groups	
	Group	Object T	ypes	NPS and some third party tion.	_
	From this location:				*
	Enter the object name to select (examples):	Locatio	ons	Add Cancel	
	Domain Admins	Check N	lames	Edt Remove	
	Advanced OK	Ca	ncel		

如果添加正确,应如下所示。

				Cisc	o WLC R	W Prop	perties	5						X
Overview	Conditions	Constraints	Settings											
Configure If conditio connectio	the condition ns match the in request, N	to for this ne connection PS skips this	twork policy. request, NP policy and e	S uses this po evaluates oth	olicy to auth er policies, i	norize the of additional	connect al policie	ion requ is are co	est. If con nfigured.	dtions	do not m	natch th	ne	
Con	dition		/alue											
🚜 Use	r Groups	1	WLANLSC\0	Domain Admin	15									
Condition	description:													
The User	Groups cond	ltion specifie	es that the co	onnecting use	er must belo	ng to one	of the s	elected (	groups. \dd		Edit		Remove	
									OK		Can	ncel	A	oply

**注意:**要查找位置和对象名称的详细信息,请打开Active Directory并查找所需的用户名。在本示例中,**域管理**员由获得完全访问权限的用户组成。**adminuser**是此对象名称的一部分。

	Ac	tive Directory Use	rs and Con	nputers			-	x
File Action View Help Active Directory Users and Com Active Directory Users and Com Saved Queries Wanlsc.com Builtin Computers Domain Controllers ForeignSecurityPrincipals Managed Service Accour Users	Admi Name Admi Admi Admi Admi Allow Anan AP US AR US AP US AC Contr AC Contr AC Contr AC Contr AC Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma	Remote control Member Of General Address Admin Use First name: Last name: Display name: Description: Office:	rs and Con Admin Us Remote D Dial-in Account er User Admin User	er Prope Desktop Sen Envir Profile	erties vices Profile onment   Telephones	COM+ Sessions Organization		×
< III >	B Doma Doma Doma Emple Enter; Group Coup Login RAS a RAS a Read-	Office: Telephone number: E-mail: Web page:	K C	ancel	Apply	Other Other		<ul> <li></li> </ul>

	Active	Directory	Users an	nd Compute	rs	
File Action View Help		Admin U	ser Prop	erties	?	x
Active Directory Users and Saved Queries Saved Qu	Remote control         General       Address         Member Of         Member of:         Name         Domain Admins	Remote I Account Dial-in Active Direct wlanisc.com/ Remove	Desktop Se Profile ory Domain Users	change Primary ( clients or POSI)	COM- Organizat Sessions	
	C	K	Cancel	Apply	Help	

步骤7.在"约束"**选项卡**下,导航至"**身份验证方**法",并确**保仅选**中未加密的身份验证。

	Cisco WLC RW Properties
Overview       Conditions       Constraints       Setting         Configure the constraints for this network polification set not matched by the constraints:       Constraints         Constraints:       Constraints         Constraints:       Constraints         Muthentication Methods       Idle Timeout         Session Timeout       Called Station ID         Pay and time restrictions       NAS Port Type	Cisco WLC RW Properties  Cisco WLC RW Properties Cisco WLC RW Properti
	Add       Edt       Remove         Less secure authentication methods:       Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)         User can change password after it has expired         Microsoft Encrypted Authentication (MS-CHAP)         User can change password after it has expired         Encrypted authentication (CHAP)         Vencrypted authentication (PAP, SPAP)         Allow clients to connect without negotiating an authentication method         Perform machine health check only         OK       Cancel

步骤8.在"设置"**选项卡**下,导航**至"RADIUS属性">"标准"**。单击Add以添加新属性Service-Type。从 下拉菜单中,选择Administrative以提供对映射到此策略的用户的完全访问权限。单击应用保存更改 ,如图所示。

conditions and constraints m ettings:	natch the connection request and the policy grants access, settings are applied.	
RADIUS Attributes	Attribute Information	nd
Standard Vendor Specific	Attribute name: Service-Type	9
Network Access Protection	Attribute number: 6	
Extended State	Attribute format: Enumerator	P
Multilink and Bandwid Allocation Protocol (B	Attribute Value: Commonly used for Dial-Up or VPN	
P Filters	<pre></pre>	
Encryption	O Commonly used for 802.1x	
🔏 IP Settings	<none></none>	
	Others	
	Administrative v	
	OK Cancel	

**注意:**如果要为特定用户提供只读访问权限,请从下拉列表中选择NAS-Prompt。在本示例中 ,创建另一个名**为Cisco WLC RO的**策略,以在域用户对象名下为用户提供**只读**访问权限。

	Cisco WLC RO Properties
Overview Conditions Constr	aints Settings
Configure the conditions for thi If conditions match the connec connection request, NPS skips	s network policy. tion request, NPS uses this policy to authorize the connection request. If conditions do not match the this policy and evaluates other policies, if additional policies are configured.
Condition	Value
all User Groups	WLANLSC\Domain Users
Condition description: The User Groups condition spe	ecifies that the connecting user must belong to one of the selected groups.
	OK Cancel Apply

	Cisco WLC RO Properties	)
verview Conditions Constr Configure the settings for this r If conditions and constraints m	aints Settings etwork policy. atch the connection request and the policy grants access, settings are applied.	
RADIUS Attributes	Attribute Information Attribute, and ADIUS clerts. See	
Vendor Specific Network Access Protection NAP Enforcement	Service-Type Attribute number: 6	
Extended State Routing and Remote Acc Acc Multilink and Bandwid	Attribute format: Enumerator Attribute Value:	
Allocation Protocol (B P IP Filters Encryption	Commonly used for Dial-Up or VPN Conne> Commonly used for 802.1x	
R Settings	<pre> v  • Others</pre>	
	NAS Prompt V OK Cancel	
	OK Cancel &	ply

### 验证

1.使用**登录**用户凭据时,不允许用户在控制器上配置任何更改。



General	Security	QoS	Policy-Mapping	Advanced		
Profile Name		tes	tr			
Туре		WL	AN			
SSID		tes	t2			
Status	Status		Enabled			
Security	Policies					
						inges.)
		Autho	rization Failed No su	fficient privileges		
Radio Pol	icy	riatilo		noiont privilogeo		
Interface,	/Interface Gro					
Multicast	Vlan Feature				Close	
Broadcas	t SSID	0	Lilavicu			
NAS-ID		nor	ne			

#### 从debug aaa all enable中,您可以看到授权响应中service-type属性的值为7,与NAS提示符对应。

```
*aaaQueueReader: Dec 07 22:20:14.664: 30:01:00:00:00:00 Successful transmission of
Authentication Packet (pktId 14) to 10.106.33.39:1812 from server queue 0, proxy state
30:01:00:00:00:00-00:00
*aaaQueueReader: Dec 07 22:20:14.664: 00000000: 01 0e 00 48 47 f8 f3 5c 58 46 98 ff 8e f8 20 7a
....HG...\XF.....z
*aaaQueueReader: Dec 07 22:20:14.664: 00000010: f6 a1 f1 d1 01 0b 6c 6f 67 69 6e 75 73 65 72 02
....loginuser.
*aaaQueueReader: Dec 07 22:20:14.664: 00000020: 12 c2 34 69 d8 72 fd 0c 85 aa af 5c bd 76 96 eb
..4i.r....\.v..
*aaaQueueReader: Dec 07 22:20:14.664: 00000030: 60 06 06 00 00 00 07 04 06 0a 6a 24 31 20 0b 43
`....j$1..C
*aaaQueueReader: Dec 07 22:20:14.664: 00000040: 69 73 63 6f 2d 57 4c 43 isco-WLC
*radiusTransportThread: Dec 07 22:20:14.668: 30:01:00:00:00:00 Access-Accept received from
RADIUS server 10.106.33.39 (qid:0) with port:1812, pktId:14
*radiusTransportThread: Dec 07 22:20:14.668: AuthorizationResponse: 0xa3d3fb25a0
*radiusTransportThread: Dec 07 22:20:14.668: RadiusIndexSet(1), Index(1)
*radiusTransportThread: Dec 07 22:20:14.668:
protocolUsed......0x00000001
*radiusTransportThread: Dec 07 22:20:14.668:
*radiusTransportThread: Dec 07 22:20:14.668: Packet contains 2 AVPs:
*radiusTransportThread: Dec 07 22:20:14.668: AVP[01] Service-
*radiusTransportThread: Dec 07 22:20:14.668: AVP[02]
Class.....DATA (44 bytes)
2.使用adminuser凭据时,用户应具有服务类型值6的完全访问权限,该值与管理相对应。
```



\*aaaQueueReader: Dec 07 22:14:27.439: AuthenticationRequest: 0x7fba240c2f00 \*aaaQueueReader: Dec 07 22:14:27.439: proxyState.....2E:01:00:00:00:00-00:00 \*aaaQueueReader: Dec 07 22:14:27.439: Packet contains 5 AVPs: \*aaaQueueReader: Dec 07 22:14:27.439: AVP[01] User-Name......adminuser (9 bytes) \*aaaQueueReader: Dec 07 22:14:27.439: AVP[04] Nas-Ip-\*aaaQueueReader: Dec 07 22:14:27.439: AVP[05] NAS-Identifier.....Cisco-WLC (9 bytes) : : \*radiusTransportThread: Dec 07 22:14:27.442: 2e:01:00:00:00 Access-Accept received from RADIUS server 10.106.33.39 (qid:0) with port:1812, pktId:13 \*radiusTransportThread: Dec 07 22:14:27.442: AuthorizationResponse: 0xa3d3fb25a0 \*radiusTransportThread: Dec 07 22:14:27.442: protocolUsed.....0x0000001 \*radiusTransportThread: Dec 07 22:14:27.442: proxyState.....2E:01:00:00:00:00-00:00 \*radiusTransportThread: Dec 07 22:14:27.442: AVP[01] Service-**Type.....0x00000006 (6)** (4 bytes) \*radiusTransportThread: Dec 07 22:14:27.442: AVP[02] Class.....DATA (44 bytes)

### 故障排除

要排除通过NPS对WLC的管理访问故障,请运行debug aaa all enable命令。

1.此处显示了使用不正确凭据时的日志。

```
*aaaQueueReader: Dec 07 22:36:39.753: 32:01:00:00:00:00 Successful transmission of
Authentication Packet (pktId 15) to 10.106.33.39:1812 from server queue 0, proxy state
32:01:00:00:00-00:00
*aaaQueueReader: Dec 07 22:36:39.753: 00000000: 01 0f 00 48 b7 e4 16 4d cc 78 05 32 26 4c ec 8d
....H....M.x.2&L..
*aaaQueueReader: Dec 07 22:36:39.753: 00000010: c7 a0 5b 72 01 0b 6c 6f 67 69 6e 75 73 65 72 02
..[r..loginuser.
*aaaQueueReader: Dec 07 22:36:39.753: 00000020: 12 03 a7 37 d4 c0 16 13 fc 73 70 df 1f de e3 e4
....7.....sp.....
*aaaQueueReader: Dec 07 22:36:39.753: 00000030: 32 06 06 00 00 07 04 06 0a 6a 24 31 20 0b 43
2....j$1..C
*aaaQueueReader: Dec 07 22:36:39.753: 00000040: 69 73 63 6f 2d 57 4c 43 isco-WLC
*aaaQueueReader: Dec 07 22:36:39.753: 32:01:00:00:00:00 User entry not found in the Local FileDB
for the client.
*radiusTransportThread: Dec 07 22:36:39.763: 32:01:00:00:00:00 Counted 0 AVPs (processed 20
bytes, left 0)
*radiusTransportThread: Dec 07 22:36:39.763: 32:01:00:00:00 Access-Reject received from
RADIUS server 10.106.33.39 (qid:0) with port:1812, pktId:15
```

#### 2.当service-type与Administrative(value=6)或NAS-prompt(value=7)以外的值一起使用时,如下所示 。在这种情况下,即使身份验证成功,登录也会失败。

```
*aaaQueueReader: Dec 07 22:46:31.849: AuthenticationRequest: 0x7fba240c56a8
*aaaQueueReader: Dec 07 22:46:31.849: Callback.....0xa3c13ccb70
*aaaQueueReader: Dec 07 22:46:31.849:
*aaaQueueReader: Dec 07 22:46:31.849: Packet contains 5 AVPs:
(9 bytes)
*aaaQueueReader: Dec 07 22:46:31.849: AVP[03] Service-
Type.....0x00000007 (7) (4 bytes)
*aaaQueueReader: Dec 07 22:46:31.849: AVP[04] Nas-Ip-
*aaaQueueReader: Dec 07 22:46:31.849: AVP[05] NAS-Identifier.....Cisco-WLC
(9 bytes)
:
*radiusTransportThread: Dec 07 22:46:31.853: AuthorizationResponse: 0xa3d3fb25a0
*radiusTransportThread: Dec 07 22:46:31.853: RadiusIndexSet(1), Index(1)
*radiusTransportThread: Dec 07 22:46:31.853: resultCode.....0
*radiusTransportThread: Dec 07 22:46:31.853:
protocolUsed.....0x0000001
*radiusTransportThread: Dec 07 22:46:31.853: Packet contains 2 AVPs:
*radiusTransportThread: Dec 07 22:46:31.853: AVP[01] Service-
Type.....0x00000001 (1) (4 bytes)
*radiusTransportThread: Dec 07 22:46:31.853: AVP[02]
Class.....DATA (44 bytes)
*emWeb: Dec 07 22:46:31.853: Authentication succeeded for adminuser
```