Acesso de gerenciamento para WLC AireOS por meio do Microsoft NPS

Contents

Introduction Prerequisites Requirements Componentes Utilizados Informações de Apoio Configurações Configuração de WLC Configuração do Microsoft NPS Verificar Troubleshoot

Introduction

Este documento descreve como configurar o acesso de gerenciamento para a GUI e CLI do AireOS WLC através do Microsoft Network Policy Server (NPS).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento das soluções de segurança sem fio
- Conceitos de AAA e RADIUS
- Conhecimento básico do Microsoft Server 2012
- Instalação do Microsoft NPS e Ative Diretory (AD)

Componentes Utilizados

As informações fornecidas neste documento são baseadas nos seguintes componentes de software e hardware.

- Controladora AireOS (5520) em 8.8.120.0
- Microsoft Server 2012

Note: Este documento destina-se a dar aos leitores um exemplo da configuração necessária em um servidor Microsoft para acesso de gerenciamento WLC. A configuração do servidor Microsoft Windows apresentada neste documento foi testada no laboratório e foi encontrada para funcionar como esperado. Se tiver problemas com a configuração, entre em contato com a Microsoft para obter ajuda. O Cisco Technical Assistance Center (TAC) não oferece

suporte à configuração do servidor Microsoft Windows. Os guias de instalação e configuração do Microsoft Windows 2012 podem ser encontrados no Microsoft Tech Net.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informações de Apoio

Quando a CLI/GUI da WLC é acessada, o usuário é solicitado a inserir as credenciais para fazer login com êxito. As credenciais podem ser verificadas em um banco de dados local ou em um servidor AAA externo. Neste documento, o Microsoft NPS está sendo usado como o servidor de autenticação externa.

Configurações

Neste exemplo, dois usuários são configurados no AAA (NPS) viz. **loginuser** e **adminuser**. **loginuser** tem apenas o acesso somente leitura enquanto **adminuser** recebe acesso total.

Configuração de WLC

Etapa 1. Adicione o servidor RADIUS à controladora. Navegue até **Security > RADIUS > Authentication**. Clique em **Novo** para adicionar o servidor. Verifique se a opção **de gerenciamento** está habilitada para que esse servidor possa ser usado para acesso de gerenciamento, como mostrado nesta imagem.

cisco		<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	Sa EEEDB
Security	RADIUS	Authenti	ication Server	rs > Edit					
 AAA General RADIUS Authentication Accounting Auth Cached Users Fallback DNS Downloaded AVP TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies Local EAP Advanced EAP Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec Local Policies Umbrella 	Server In Server Ad Shared Si Shared Si Confirm S Key Wrap Apply Cis Apply Cis Port Num Server St Support fi Server Til Network I Managem Tunnel Pri Realm Lis PAC Provi IPSec Cisco AC/	dex dress(Ipv4 ecret Formi ecret Shared Secr o co ISE Defa co ACA Def ber atus for CoA meout User tent tent Retrans oxy a isioning	/Ipv6) at ret sult settings ault settings smit Timeout	2 10.106.33.39 ASCII © (Designed fo 0 1812 Enabled © 5 secon ✓ Enable 5 second Enable Enable	9 r FIPS custom ds	ers and requires a k	ey wrap complia	nt RADIU	S server;
Advanced									

Etapa 2. Navegue até **Segurança > Ordem de prioridade > Usuário de gerenciamento**. Verifique se RADIUS está selecionado como um dos tipos de autenticação.

MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT						
Priority C	Priority Order > Management User										
Authentic	ation										
Not I	Jsed		Order U	sed for Authe	entication						
TACACS	5+	>		RADIUS	Up						
		<			Down						

Note: Se RADIUS for selecionado como a primeira prioridade na ordem de autenticação, as credenciais locais serão usadas para autenticação somente se o servidor RADIUS estiver inacessível. Se RADIUS for selecionado como uma segunda prioridade, as credenciais RADIUS serão primeiro verificadas no banco de dados local e, em seguida, verificadas em relação aos servidores RADIUS configurados.

Configuração do Microsoft NPS

Etapa 1. Abra o servidor Microsoft NPS. Clique com o botão direito do mouse em Clientes Radius.

Clique em New para adicionar a WLC como o cliente RADIUS.

Insira os detalhes necessários. Certifique-se de que o segredo compartilhado seja o mesmo que o configurado na controladora enquanto o servidor RADIUS é adicionado.

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

Etapa 2. Navegue para **Políticas > Políticas de solicitação de conexão**. Clique com o botão direito do mouse para adicionar uma nova política, como mostrado na imagem.

•	Cisco WLC Properties	-
File Action View Help File Action View Help Provide the second	Overview Conditions Settings Policy name: Oteco WLC Proverview Policy name: Oteco WLC Policy state # enabled, NPS evaluates this policy while processing connection requests. If disabled, NPS does not evalue this policy. Policy enabled	
 Connection Request Po Connection Request Po Network Policies Health Policies Network Access Protection Network Access Protection Remediation Server Gro Accounting Templates Management 	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. Type of network access server: Unspecified Vendor specific: 10	
< III >	OK Cancel App	ły

Etapa 3. Na guia **Condições**, selecione **Identificador NAS** como a nova condição. Quando solicitado, insira o nome do host do controlador como o valor, como mostrado na imagem.

	Cisco WLC Properties	x
Overview Conditions Set	ttings	
Configure the conditions for If conditions match the con connection request, NPS s	r this network policy. Infection request, NPS uses this policy to authorize the connection request. If conditions do not match the kips this policy and evaluates other policies, if additional policies are configured.	
Condition	Value	
NAS Identifier	Cisco-WLC	
Condition description: The NAS Identifier condition syntax to specify NAS name	n specifies a character string that is the name of the network access server (NAS). You can use pattern matching es.	
	Add Edit Remove]
	OK Cancel Appl	y

Etapa 4. Navegue até **Políticas > Políticas de rede**. Clique com o botão direito do mouse para adicionar uma nova política. Neste exemplo, a política é denominada **Cisco WLC RW**, o que implica que a política é usada para fornecer acesso completo (leitura/gravação). Verifique se a política está configurada conforme mostrado aqui.

0	Cisco WLC RW Properties	×
File Action View Help File Action ACOUNTION File Action File Acti	Cisco WLC RW Properties Verview Conditions Constraints Settings Policy name: Policy State F enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy. Policy state F enabled Access Pemission 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? Grant access. Grant access if the connection request matches this policy. Policy and the policy grants access or deny access. Unhat is access of the connection request matches this policy. Policy and the policy grants access permission? Grant access. Grant access if the connection request matches this policy. Policy and the policy grants access, perform authorization with network policy only do net evaluate the dial-in properties of user accounts. 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 is an 802.1X authenticating switch or wireless access point, select Unspecified. Type of network access server: Dispecified V Vendor specific: Deny access server: Dispecified V Vendor specific: Deny access server: Dispecified V Vendor specific: Deny access server: Deny accesserve: Deny access server: Deny access server: Deny access serv	
< III >	OK Cancel Apply	,

Etapa 5. Na guia **Condições**, clique em **Adicionar**. Selecione os **grupos de usuários** e clique em **Adicionar**, como mostrado na imagem.

Overview	Conditions	Constraints	Settings									
Configure	the condition	ns for this net	vork policy.									
If condition connection	ns match the n request, N	Connection r PS skips this	equest, NP colicy and e	S uses this po avaluates othe	olicy to authors of the second s	orize the con additional p	nection re olicies are	equest. If cor configured.	nditions d	o not match	n the	
					Select c	ondition						x
Select	a condition, a	and then click	Add.									
Group	s											^
	Windows The Windo groups. Machine	Groups ws Groups c Groups	ondition sp	ecifies that t	he connecti	ng user or c	omputer	must belong	to one o	f the select	ted	=
	The Machi User Gro The User (ne Groups co ps Groups condi	ndition sp tion specifi	ecifies that th	e connectir	ng computer ser must be	must bel long to or	ong to one o ne of the sele	f the sele	ected group	15.	
	Location The HCAP required to network ac	Groups Location Gro match this p cess servers	ups condit olicy. The (NASs). S	tion specifies HCAP protoc See your NAS	the Host C ol is used fi documenta	redential Au or communi ation before	thorizatio cation be using this	on Protocol (ween NPS a condition.	HCAP) Id and some	ocation gro third party	ups /	~
										Add	Cance	4
								Add	Б	dit	Remov	/e

Etapa 6. Clique em **Adicionar grupos** na caixa de diálogo exibida. Na janela **Selecionar grupo** exibida, selecione o **tipo de objeto** e **local** desejados e insira o nome do objeto necessário, como mostrado na imagem.

	Cisco WLC RW Properties	X
Ov	User Groups 🗶	
Ci H	Specify the group membership required to match this policy. on request. If conditions do not match the	
	Groups are configured.	x
		~
	iter must belong to one of the selected	=
	Add Groups Remove : belong to one of the selected groups.	
	OK Cancel to one of the selected groups.	
	Select this object type: col (HCAP) location groups	
	Group Object Types NPS and some third party tion.	~
	From this location: wlanlsc.com Locations Add Cancel	
L	Enter the object name to select (examples): Domain Admins Check Names L Edit	,
	Advanced OK Cancel	

A condição, se adicionada corretamente, deve ser exibida como mostrado aqui.

				Cisc	to WLC F	RW Pro	pertie	s						
Overview	Conditions	Constraints	Settings											
Configure If conditio	the condition ons match the on request, N	ns for this network of the second sec	vork policy. equest, NP policy and e	S uses this p avaluates oth	olicy to aut her policies,	horize the if addition	connect nal policie	tion requ	uest. If cor onfigured.	nditions	do not	match t	the	
Con	dition	V	alue											
🚜 Use	r Groups	W	LANLSC\E	Domain Admir	ns									
Condition The User	description: Groups cond	ation specifies	that the co	nnecting us	er must bek	ong to on	e of the s	elected	groups.					
									Add		Edt		Remove	

Note: Para descobrir a localização e os detalhes do nome do objeto, abra o ative diretory e procure o nome de usuário desejado. Neste exemplo, os **Domain Admins** consistem em usuários que recebem acesso total. **adminuser** faz parte deste nome de objeto.

	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 Ar US AC ert P AC Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr Contr C	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		×
Image: Second		Office: Telephone number: E-mail: Web page:	K C	ancel	Apply	Other Other		

			Active [Directory	Users ar	nd Compute	ers	
File Act	ion View Hel	lp		Admin Us	ser Prop	erties	?	×
→ Ctive → Sav → ₩ wia → ₩ → ₩ → ₩ → ₩ → ₩ → ₩	Directory Users ar red Queries anlsc.com Builtin Computers Domain Controlle ForeignSecurityP Managed Service Users	nd Remote co General A Member of: Name Domain Ad	ntrol Address X	Remote Dial-in	Desktop Se Profile Env ory Domain Users	rvices Profile Telephones ironment	COM+ Organizat Sessions	ion ir ac rou rou rou rou rou s G re p istra
		Add Primary grou Set Prima	p: Do ny Group	emove main Admins There is n you have application	o need to Macintosh ns. Cancel	change Primary clients or POSI	group unless X-compliant	istra rou rou rou rou rou

Passo 7. Na guia **Restrições**, navegue para **Métodos de autenticação** e verifique se somente **a autenticação não criptografada** está marcada.

	Cisco WLC RW Properties
Overview Conditions Constraints Setting Configure the constraints for this network po If all constraints are not matched by the con Constraints: Constraints	Icy. nection request, network access is denied. Allow access only to those clients that authenticate with the specified methods.
Authentication Methods	EAP types are negotiated between NPS and the client in the order in which they are listed. EAP Types: Move Up Move Down
	Add Edit Remove Less secure authentication methods:
	Encrypted authentication (CHAP) Unencrypted authentication (PAP, SPAP) Allow clients to connect without negotiating an authentication method Perform machine health check only
	OK Cancel Apply

Etapa 8. Na guia **Settings**, navegue para **RADIUS Attributes > Standard**. Clique em **Add** para adicionar um novo atributo, **Service-Type**. No menu suspenso, selecione **Administrative** para fornecer acesso total aos usuários mapeados para essa política. Clique em Aplicar para salvar as alterações, conforme mostrado na imagem.

RADIUS Attributes Attribute Information Andard attribute, and ADIUS clients. See Standard Attribute name: Service-Type Attribute name: Service-Type Attribute name: Service-Type Network Access Protection Attribute number: 6 Attribute number: 6 Image: Comparison NAP Enforcement Attribute format: Enumerator Image: Comparison Image: Comparison	
Standard ADIUS clients. See Image: Service-Type Attribute name: Service-Type Network Access Protection Attribute number: 6 Image: NAP Enforcement Attribute format: Enumeration	
Vendor Specific Service-Type Network Access Protection Attribute number: NAP Enforcement 6 Extended State Attribute format:	
Network Access Protection Attribute number: NAP Enforcement 6 Extended State Attribute format:	
NAP Enforcement 6 Image: Extended State Attribute format:	
Extended State Attribute format:	
Routing and Remote Acc	
Multilink and Bandwid Attribute Value: Allocation Protocol (B O Commonly used for Dial-Up or VPN	
TP Filters	
Encryption O Commonly used for 802.1x	
IP Settings IP Settings	
(a) Other	
© Others	
Administrative V	
Administrative V	
Administrative V OK Cancel	
IP Settings <pre></pre>	

Note: Se desejar fornecer acesso somente leitura a usuários específicos, selecione NAS-Prompt na lista suspensa. Neste exemplo, outra política chamada **Cisco WLC RO** é criada para fornecer acesso somente leitura aos usuários sob o nome do objeto **Usuários de domínio**.

	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

Overview Conditions Constraints Settings Configure the settings for this network policy. # conditions and constraints match the connection request and the policy grants access, settings are appled. Settings: RADIUS Attributes Attribute Information Settings Attribute Information Attribute Information Attribute Information Attribute name: Service-Type Attribute format: Envort Access Protection NAP Enforcement Attribute format: Fourting and Renote Acc Attribute Value: Allocation Protocol (6) P IP Filters Encryption IP Settings Others NAS Prompt OK		Cisco WLC RO Properties	x
Configure the settings for this network policy. If conditions and constraints match the connection request and the policy grants access, settings are applied. Settings: CADIUS Attributes Attribute Information Image: Standard Image: Standard Attribute name: Service-Type andard attribute, and ADIUS clients. See Image: NAP Enforcement Image: Standard Attribute name: Service-Type andard attribute, and ADIUS clients. See Image: NAP Enforcement Image: Standard Attribute name: Service-Type andard attribute, and ADIUS clients. See Image: NAP Enforcement Image: Standard Attribute value: Commonly used for Dial-Up or VPN Image: Standard Image: Image: Standard Attribute Value: Commonly used for 802.1x Image: Standard Image: Image: Image: Image: Standard Image:	Overview Conditions Constr	aints Settings	
RADIUS Attributes Attribute Information Image: Construction of the structure of t	Configure the settings for this r If conditions and constraints m Settings:	etwork policy. atch the connection request and the policy grants access, settings are applied.	
Standard Attroute name: Service-Type Network Access Protection Attroute number: Service-Type NAP Enforcement Attroute number: Service and Remote Access Multilink and Bandwid Altroute Bandwid Altroute formonly used for Dial-Up or VPN Image: Commonly used for Dial-Up or VPN IP Filters Commonly used for 802.1x IP Settings Others NAS Prompt V OK Cancel	RADIUS Attributes	Attribute Information X and at the te and	-
Network Access Protech Attrbute number: Image: Strended State Attrbute format: Routing and Remote Acc Attrbute format: Image: Multilink and Bandwig Attrbute Value: Attrbute Value: Commonly used for Dial-Up or VPN Image: Protyption Commonly used for 802.1x Image: Protyption Commonly used for 802.1x Image: Protyption Others Image: NAS Prompt V OK Cancel	Standard	Atribute name: Service-Type	
Image: State Attribute format: Enumerator Multilink and Bandwid Allocation Protocol (B Encryption Attribute Value: Commonly used for Dial-Up or VPN IP Filters Image: Commonly used for 802.1x IP Settings Image: Commonly used for 802.1x IP	NAP Enforcement	Attribute number: 6	
Multilink and Bandwid Allocation Protocol (8 Prilers Attribute Value: Commonly used for Dial-Up or VPN Pilers Inone> IP Settings Commonly used for 802.1x IP Settings Inone> Others OK	Extended State	Attribute format: Enumerator	
	Multilink and Bandwid Allocation Protocol (B	Attribute Value: O Commonly used for Dial-Up or VPN	
Commonly used for 802.1x Conne> OK Cancel	TP Filters	<pre> v</pre>	
IP Settings Others NAS Prompt OK Cancel	Encryption	O Commonly used for 802.1x	
Others NAS Prompt OK Cancel	R IP Settings	<pre> v</pre>	
OK Cancel		Others	
OK Cancel		NAS Prompt v	
		OK Cancel	
		OK Crossel in	*

Verificar

1. Quando as credenciais **loginuser** são usadas, o usuário não tem permissão para configurar nenhuma alteração no controlador.



General	Security	QoS	Policy-Mapping	Advanced		
Profile Name		tes	tr			
Туре		WL	AN			
SSID		tes	t2			
Status						
Security	Policies					
,				inges.)		
		Autho	rization Failed No.cu	ufficient privileges		
Radio Pol	icy	Authorization Failed. No sufficient privileges				
Interface	/Interface Grou					
Multicast	Vlan Feature			Close		
Broadcas	t SSID	Litabled				
NAS-ID		nor	ne			

No **debug aaa all enable**, você pode ver que o valor do atributo service-type na resposta de autorização é 7, o que corresponde ao prompt do NAS.

```
*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
\dots HG. \backslash 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 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.....0x0000001
*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. Quando as credenciais **de administrador** são usadas, o usuário deve ter acesso total com o valor 6 **do tipo de serviço**, que corresponde ao **administrativo**.



```
*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.....0x00000001
*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)
```

Troubleshoot

Para solucionar problemas de acesso de gerenciamento à WLC através do NPS, execute o comando **debug aaa all enable**.

1. Os registros quando credenciais incorretas são usadas são mostrados aqui.

*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 32:01:00:00:00:00-00:00 *aaaQueueReader: Dec 07 22:36:39.753: 00000000: 01 0f 00 48 b7 e4 16 4d cc 78 05 32 26 4c ec 8dH....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 e47.....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: 32:01:00:00:00:00 Access-Reject received from

 Os registros quando service-type é usado com um valor diferente de Administrative (value=6) ou NAS-prompt (value=7) são mostrados da seguinte maneira. Nesse caso, o login falha mesmo se a autenticação for bem-sucedida.

```
*aaaQueueReader: Dec 07 22:46:31.849: AuthenticationRequest: 0x7fba240c56a8
*aaaQueueReader: Dec 07 22:46:31.849:
*aaaQueueReader: Dec 07 22:46:31.849: Packet contains 5 AVPs:
*aaaQueueReader: Dec 07 22:46:31.849: AVP[01] User-Name......adminuser
(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
```