Autenticação do Administrador do Lobby de Controladoras Wireless LAN via servidor RADIUS

Contents

Introduction Prerequisites Requirements Componentes Utilizados Conventions Informações de Apoio Configuraç Configurações Configurações Configuração de WLC Configuração de servidor RADIUS Verificar Troubleshoot Informações Relacionadas

Introduction

Este documento explica as etapas de configuração envolvidas para autenticar um administrador de lobby do controlador de LAN sem fio (WLC) com um servidor RADIUS.

Prerequisites

Requirements

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Conhecimento de como configurar parâmetros básicos em WLCs
- Conhecimento de como configurar um servidor RADIUS, como o Cisco Secure ACS
- Conhecimento dos usuários convidados na WLC

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

• Controlador de LAN sem fio Cisco 4400 que executa a versão 7.0.216.0

 Um Cisco Secure ACS que executa o software versão 4.1 e é usado como um servidor RADIUS nesta configuração.

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.

Conventions

Consulte as <u>Convenções de Dicas Técnicas da Cisco para obter mais informações sobre</u> <u>convenções de documentos.</u>

Informações de Apoio

Um administrador de lobby, também conhecido como embaixador de lobby de uma WLC, pode criar e gerenciar contas de usuário convidado no Wireless LAN Controller (WLC). O embaixador do lobby tem privilégios de configuração limitados e pode acessar apenas as páginas da Web usadas para gerenciar as contas de convidado. O embaixador do lobby pode especificar o tempo durante o qual as contas de usuário convidado permanecem ativas. Depois que o tempo especificado expirar, as contas de usuário convidado expirarão automaticamente.

Consulte o <u>Guia de implantação: Cisco Guest Access Usando o Cisco Wireless LAN Controller</u> para obter mais informações sobre os usuários convidados.

Para criar uma conta de usuário convidado no WLC, você precisa fazer login no controlador como um administrador de lobby. Este documento explica como um usuário é autenticado na WLC como administrador de lobby com base nos atributos retornados pelo servidor RADIUS.

Observação: a autenticação de administrador de lobby também pode ser executada com base na conta de administrador de lobby configurada localmente na WLC. Consulte <u>Criação de uma Conta</u> <u>de Embaixador de Lobby</u> para obter informações sobre como criar uma conta de administrador de lobby localmente em um controlador.

Configurar

Nesta seção, você recebe as informações sobre como configurar o WLC e o Cisco Secure ACS para o propósito descrito neste documento.

Configurações

Este documento utiliza as seguintes configurações:

- O endereço IP da interface de gerenciamento da WLC é 10.77.244.212/27.
- O endereço IP do servidor RADIUS é 10.77.244.197/27.
- A chave secreta compartilhada usada no access point (AP) e no servidor RADIUS é cisco123.
- O nome de usuário e a senha do administrador de lobby configurados no servidor RADIUS são ambos lobbyadmin.

No exemplo de configuração neste documento, qualquer usuário que faça login no controlador com nome de usuário e senha como lobbyadmin recebe a função de administrador de lobby.

Configuração de WLC

Antes de iniciar a configuração de WLC necessária, verifique se a sua controladora executa a versão 4.0.206.0 ou posterior. Isso ocorre devido à ID de bug da Cisco <u>CSCsg89868</u> (somente clientes <u>registrados</u>) na qual a interface da Web do controlador exibe páginas da Web incorretas para o usuário LobbyAdmin quando o nome de usuário é armazenado em um banco de dados RADIUS. O LobbyAdmin é apresentado com a interface ReadOnly em vez da interface LobbyAdmin.

Esse bug foi resolvido na versão 4.0.206.0 da WLC. Portanto, certifique-se de que a versão do controlador seja 4.0.206.0 ou posterior. Consulte <u>Atualização de software do controlador de LAN</u> <u>sem fio (WLC)</u> para obter instruções sobre como atualizar seu controlador para a versão apropriada.

Para executar a autenticação de gerenciamento do controlador com o servidor RADIUS, verifique se o sinalizador **Admin-auth-via-RADIUS** está ativado no controlador. Isso pode ser verificado na saída do comando **show radius summary**.

A primeira etapa é configurar as informações do servidor RADIUS no controlador e estabelecer a acessibilidade da camada 3 entre o controlador e o servidor RADIUS.

Configurar informações do servidor RADIUS no controlador

Conclua estes passos para configurar a WLC com detalhes sobre o ACS:

 Na GUI do WLC, escolha a guia Security e configure o endereço IP e o segredo compartilhado do servidor ACS.Esse segredo compartilhado precisa ser o mesmo no ACS para que a WLC se comunique com o ACS.Observação: o segredo compartilhado ACS diferencia maiúsculas de minúsculas. Portanto, certifique-se de inserir as informações secretas compartilhadas corretamente.Esta figura mostra um

exemplo:							
cisco	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Security	RADIUS Authentic	ation Servers	s > New				
▼ AAA General ▼ RADIUS	Server Index (Priorit) Server IP Address	0	2 2	7			
Authentication Accounting	Shared Secret Forma	, .	ASCII 🗸				
Fallback TACACS+	Shared Secret						
LDAP	Confirm Shared Secr	et	•••••				
MAC Filtering Disebled Clients	Key Wrap	Ē] (Designed f	or FIPS custor	ners and requires	a key wrap comp	pliant RAE
User Login Policies AP Policies	Port Number		1812				
Password Policies	Server Status		Enabled 💌				
Local EAP	Support for RFC 3576	ē.	Enabled 💌				
Priority Order	Server Timeout		2 seconds				
▶ Certificate	Network User		Enable				
Access Control Lists	Management		Enable	- T			
Wireless Protection Policies	IPSec		Enable				

2. Marque a caixa de seleção **Management** para permitir que o ACS gerencie os usuários da WLC, como mostrado na figura na etapa 1. Em seguida, clique em **Aplicar**.

3. Verifique a alcançabilidade da Camada 3 entre o controlador e o servidor RADIUS configurado com a ajuda do comando ping. Essa opção de ping também está disponível na página de servidor RADIUS configurada na GUI da WLC na guia Security>RADIUS Authentication.Este diagrama mostra uma resposta de ping bem-sucedida do servidor RADIUS. Portanto, a acessibilidade da camada 3 está disponível entre o controlador e o servidor

RADIL	JS.	

cisco	MONITOR	WLANS C	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	нецр	EEEDBACK
Security	RADIUS	Authenticat	ion Serve	rs		G)			
▼ AAA General ▼ RADIUS Authentication Accounting Fallback	Call Sta Use AES MAC De	tion ID Type Å : Key Wrap limiter	IP Addres	ss 💌 ed far FIPS custom	iers and rec	uires a key wrap c	ampliant RADIU	S server)	i.
LDAP Local Net Users	Network User	Management	Server Index	Server Address	i Port	IPSec	Adm	in Statu	s
Disabled Clients		v	1	10.78.177.16	1812	Disabled	Enab	led	
User Login Policies AP Policies Password Policies	V	V	2	10.77.244.197	1812	Disabled	Eneb	led	

Configuração de servidor RADIUS

Conclua as etapas nestas seções para configurar o servidor RADIUS:

- 1. Adicione a WLC como um cliente AAA ao servidor RADIUS
- 2. <u>Configurar o atributo de tipo de serviço IETF RADIUS apropriado para um administrador de</u> <u>lobby</u>

Adicione a WLC como um cliente AAA ao servidor RADIUS

Conclua estes passos para adicionar a WLC como um cliente AAA no servidor RADIUS. Como mencionado anteriormente, este documento usa o ACS como o servidor RADIUS. Você pode usar qualquer servidor RADIUS para esta configuração.

Conclua estes passos para adicionar a WLC como um cliente AAA no ACS:

- 1. Na GUI do ACS, escolha a guia **Network Configuration**.
- 2. Em AAA Clients, clique em Add Entry.
- 3. Na janela Add AAA Client (Adicionar cliente AAA), digite o nome do host WLC, o endereço IP da WLC e uma chave secreta compartilhada. Veja o diagrama de exemplo na etapa 5.
- 4. No menu suspenso Authenticate Using (Autenticar usando), escolha RADIUS (Cisco Aironet).
- 5. Clique em **Enviar + Reiniciar** para salvar a configuração.



Network Configuration

Add AAA Client

AAA Client Hostname	WLC2
AAA Client IP Address	10.77.244.212
Shared Secret	cisco123
RADIUS Key Wrap Key Encryption Key Message Authenticator Cod Key Input Format	le Key C ASCII @ Hexadecimal
Authenticate Using	RADJUS (Cisco Airanet)
Single Connect TACACS+	- AAA Client (Record stop in accounting on failure)
□ Log Update/Watchdog P	ackets from this AAA Client
E Log RADIUS Tunneling P	ackets from this AAA Client
IT Replace RADIUS Port inf	o with Usemame from this AAA Client
- Match Framed-IP-Addres	s with user IP address for accounting packets from this A

Configurar o atributo de tipo de serviço IETF RADIUS apropriado para um administrador de lobby

Para autenticar um usuário de gerenciamento de um controlador como administrador de lobby através do servidor RADIUS, você deve adicionar o usuário ao banco de dados RADIUS com o atributo IETF RADIUS Service-Type definido como **Callback Administrative**. Este atributo atribui ao usuário específico a função de administrador de lobby em um controlador.

Este documento mostra o exemplo de usuário lobbyadmin como administrador de lobby. Para configurar esse usuário, faça o seguinte no ACS:

- 1. Na GUI do ACS, escolha a guia User Setup.
- 2. Digite o nome de usuário a ser adicionado ao ACS conforme mostrado nesta janela de exemplo:

CISCO SYSTEMS	User Setup
اللانية مناللاتية -	Select
User Setup	
Group Setup	User: lobbyadmin
Shared Profile Components	Find Add/Edit
Network Configuration	
System Configuration	List users beginning with letter/number:
Configuration	NOPOBSTUVWXYZ Q123456789
Administration Control	List all users
External User Databases	Remove Dynamic Users
Doog Posture Validation	

- 3. Clique em Adicionar/Editar para ir para a página Editar usuário.
- 4. Na página User Edit, forneça os detalhes do nome real, da descrição e da senha desse usuário.Neste exemplo, o nome de usuário e a senha usados são ambos lobbyadmin.

User Setup



ser	User: lobby	yadmin (New User)
roup	ΠA	ccount Disabled
ed Profile ponents	Supplem	entary User Info
tion Re	al Name Lob	by Admin
De	scription Lob	by Admin
n		
	U	ser Setup 📑
	Password Authentica	tion:
		ACS Internal Database 💌
	CiscoSecu CHAP/ARAP, if the	re PAP (Also used for CHAP/MS- Separate field is not checked.)
	Password	
	Confirm Password	•••••
	□ Separate (CHAP/N	IS-CHAP/ARAP)
	Password	
	Confirm Password	2
ļ	When a token server supplying a separate card user allows CHA	I is used for authentication, CHAP password for a token P authentication. This is Submit Cancel

- 5. Role para baixo até a configuração IETF RADIUS Attributes e marque a caixa de seleção Service-Type Attribute.
- 6. Escolha **Callback Administrative** no menu suspenso Service-Type (Tipo de serviço) e clique em **Submit (Enviar)**.Este é o atributo que atribui a este usuário a função de administrador de lobby.

	Account Disable				
User Setup	• Never				
Group Setup	C Disable account if:				
Shared Profile Components	Date exceeds:				
		Sep - 25 2011			
Configuration	Eailed attempts exceed				
System	E Compositione				
Configuration	p	evenes filles o			
Interface Configuration	Failed attempts since last	t successful login: U			
Administration	Reset current failed at	tempts count on submit			
Control					
External User Databases					
Posture Validation	IETF RA	ADIUS Attributes			
Network Access Profiles	☐ [006] Service-Type				
Deserteend	10 AL 1995	Callback Administrative			

Às vezes, esse atributo Service-Type não fica visível nas configurações do usuário. Nesses casos, faça o seguinte para torná-lo visível:Na GUI do ACS, escolha **Interface Configuration** > **RADIUS (IETF)** para habilitar os atributos IETF na janela User Configuration.Isso exibe a página Configurações do RADIUS (IETF).Na página Configurações de RADIUS (IETF), você pode ativar o atributo IETF que precisa estar visível nas configurações de usuário ou grupo. Para esta configuração, marque **Service-Type** para a coluna User (Usuário) e clique em **Submit (Enviar)**.Esta janela mostra um exemplo:

LISCO SYSTEMS

Interface Configuration

an Tana
User Sotup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Configuration
Administration Control
Databases
Posture Validation
Network Access Profiles
Reports and Activity
Documentation
cx

RADIUS (IETF)

User	Group
N	₽ [006] Service-Type
	[007] Framed-Protocol [007] [] [] [] [] [] []] [[]
	🖻 [009] Framed-IP-Netmask
	[010] Framed-Routing
	🖻 [011] Filter-Id
	[012] Framed-MTU [012] [
	[013] Framed-Compression
	[014] Login-IP-Host [014] [014] [014] [
	[015] Login-Service [[[[
	🛙 [016] Login-TCP-Port
	[018] Reply-Message [018] Reply-Message []]
	🖻 [020] Callback-Id
	[022] Framed-Route [022] [
	[023] Framed-IPX-Network
	[024] State [024] [[[[
	[025] Class [[[[
	[027] Session-Timeout [027] Session-Timeout S
	🗹 [028] Idle-Timeout
	[029] Termination-Action
	🖻 [033] Proxy-State
	[034] Login-LAT-Service
	[035] Login-LAT-Node
Г	Submit Cancel

Observação: este exemplo especifica a autenticação por usuário. Você também pode executar a autenticação com base no grupo ao qual um usuário específico pertence. Nesses casos, marque a caixa de seleção **Grupo** para que este atributo fique visível em Configurações de grupo. **Observação:** também, se a autenticação for em grupo, você precisará atribuir usuários a um grupo específico e configurar os atributos IETF da configuração do grupo para fornecer privilégios de acesso aos usuários desse grupo. Consulte <u>Gerenciamento de grupos de usuários</u> para obter informações detalhadas sobre como configurar e gerenciar grupos.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Para verificar se sua configuração funciona corretamente, acesse a WLC através do modo GUI (HTTP/HTTPS).

Observação: um embaixador do lobby não pode acessar a interface CLI do controlador e, portanto, pode criar contas de usuário convidado somente na GUI do controlador.

Quando o prompt de login for exibido, digite o nome de usuário e a senha configurados no ACS. Se as configurações estiverem corretas, você será autenticado com êxito na WLC como **administrador de lobby**. Este exemplo mostra como a GUI de um administrador de lobby cuida da autenticação bem-sucedida:



Observação: você pode ver que um administrador de lobby não tem outra opção além do gerenciamento de usuários convidados.

Para verificá-lo a partir do modo CLI, faça Telnet no controlador como um administrador de leitura/gravação. Emita o comando **debug aaa all enable** na CLI do controlador.

(Cisco Controller) >debug aaa all enable (Cisco Controller) > *aaaQueueReader: Aug 26 18:07:35.072: ReProcessAuthentication previous proto 28, next proto 20001 *aaaQueueReader: Aug 26 18:07:35.072: AuthenticationRequest: 0x3081f7dc *aaaQueueReader: Aug 26 18:07:35.072: proxyState.....00:00:00:40: 00:00-00:00 *aaaQueueReader: Aug 26 18:07:35.072: Packet contains 5 AVPs (not shown) *aaaQueueReader: Aug 26 18:07:35.072: apfVapRadiusInfoGet: WLAN(0) dynamic int attributes srcAddr: 0x0, gw:0x0, mask:0x0, vlan:0, dpPort:0, srcPort:0 *aaaQueueReader: Aug 26 18:07:35.073: 00:00:00:40:00:00 Successful transmission of Authentication Packet (id 39) to 10.77.244.212:1812, proxy state 00:00:00:40:00:00-00:01 .'.G......... *aaaQueueReader: Aug 26 18:07:35.073: 00000010: 00 00 00 00 01 0c 6c 6f 62 62 79 61 64 6d 69 6elobbvadmin *aaaQueueReader: Aug 26 18:07:35.073: 00000020: 02 12 5f 5b 5c 12 c5 c8 52 d3 3f 4f 4f 8e 9d 38 .._[\...R.?00..8 *aaaQueueReader: Aug 26 18:07:35.073: 00000030: 42 91 06 06 00 00 07 04 06 0a 4e b1 1a 20 09 B....N....

```
*aaaQueueReader: Aug 26 18:07:35.073: 00000040: 57 4c 43 34 34 30 30 WLC4400
*radiusTransportThread: Aug 26 18:07:35.080: 00000000: 02 27 00 40 7e 04 6d 533d ed 79 9c b6 99
d1
£8
   .'.@~.mS=.y....
*radiusTransportThread: Aug 26 18:07:35.080: 00000010: d0 5a 8f 4f 08 06 ff ffff ff 06 06 00 00
00
0b
   .Z.O.....
*radiusTransportThread: Aug 26 18:07:35.080: 00000020: 19 20 43 41 43 53 3a 302f 61 65 32 36 2f
61
34
   ..CACS:0/ae26/a4
*radiusTransportThread: Aug 26 18:07:35.080: 00000030: 65 62 31 31 61 2f 6c 6f62 62 79 61 64 6d
69
6e eb11a/lobbyadmin
*radiusTransportThread: Aug 26 18:07:35.080: ****Enter processIncomingMessages: response code=2
*radiusTransportThread: Aug 26 18:07:35.080: ****Enter processRadiusResponse: response code=2
*radiusTransportThread: Aug 26 18:07:35.080: 00:00:00:40:00:00 Access-Accept received from
RADIUS
server 10.77.244.212 for mobile 00:00:00:40:00:00 receiveId = 0
*radiusTransportThread: Aug 26 18:07:35.080: AuthorizationResponse: 0x13c73d50
*radiusTransportThread: Aug 26 18:07:35.080:
                                        structureSize.....118
*radiusTransportThread: Aug 26 18:07:35.080:
                                         resultCode.....0
*radiusTransportThread: Aug 26 18:07:35.080:
protocolUsed.....0x00000001
*radiusTransportThread: Aug 26 18:07:35.080:
proxyState.....00:00:00:40:00:00-00:00
*radiusTransportThread: Aug 26 18:07:35.080: Packet contains 3 AVPs:
*radiusTransportThread: Aug 26 18:07:35.080:
                                            AVP[01] Framed-IP-
*radiusTransportThread: Aug 26 18:07:35.080:
                                            AVP[02] Service-
*radiusTransportThread: Aug 26 18:07:35.080:
                                           AVP[03]
Class......
CACS:0/ae26/a4eb11a/lobbyadmin (30 bytes)
*emWeb: Aug 26 18:07:35.084: Authentication succeeded for lobbyadmin
```

Nas informações destacadas nesta saída, você pode ver que o atributo de tipo de serviço 11 (Callback Administrative) é passado para o controlador a partir do servidor ACS e o usuário está conectado como administrador de lobby.

Esses comandos podem ser de ajuda adicional:

- debug aaa details enable
- debug aaa events enable
- debug aaa packets enable

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

Troubleshoot

Quando você faz login em um controlador com privilégios de embaixador do lobby, não é possível criar uma conta de usuário convidado com um valor de tempo de vida "0", que é uma conta que nunca expira. Nessas situações, você recebe a mensagem de erro Lifetime value cannot be 0.

Isso se deve à ID de bug da Cisco <u>CSCsf32392</u> (somente clientes <u>registrados</u>), que é encontrada principalmente na versão 4.0 da WLC. Este bug foi resolvido na versão 4.1 do WLC.

Informações Relacionadas

- Autenticação de servidor RADIUS de usuários de gerenciamento no exemplo de configuração do controlador
- <u>Configuração TACACS+ da Cisco Unified Wireless Network</u>
- Versão 4.0 do Guia de configuração do controlador de LAN sem fio da Cisco Gerenciamento de contas de usuários
- Exemplo de configuração de ACLs em Wireless LAN Controller
- Perguntas frequentes sobre o Wireless LAN Controller (WLC)
- <u>ACLs em Wireless LAN Controllers: Regras, limitações e exemplos</u>
- Exemplo de configuração de autenticação de web externa com Wireless LAN Controllers
- Exemplo de configuração de autenticação da Web para o controlador da LAN sem fio
- WLAN de convidado e WLAN interna usando o exemplo de configuração de WLCs
- <u>Suporte Técnico e Documentação Cisco Systems</u>