使用ISE和Catalyst 9800无线局域网控制器配置动态VLAN分配

目录

简介 要求 使<u>用的组件</u> 背景信息 使用 RADIUS 服务器执行动态 VLAN 分配 配置 网络图 配置步骤 思科ISE配置 步骤1.在Cisco ISE服务器上将Catalyst WLC配置为AAA客户端 步骤2.在思科ISE上配置内部用户 步骤3.配置用于动态VLAN分配的RADIUS(IETF)属性 为多个 VLAN 配置交换机 Catalyst 9800 WLC配置 步骤1.使用身份验证服务器的详细信息配置WLC 步骤2.配置VLAN 步骤3.配置WLAN(SSID) 步骤4.配置策略配置文件 步骤5.配置策略标记 步骤6.将策略标记分配给AP 验证 故障排除 相关信息

简介

本文档介绍动态VLAN分配的概念,以及如何配置Catalyst 9800无线LAN控制器(WLC)和思科身份服 务引擎(ISE)来分配无线LAN(WLAN),以便为无线客户端完成此操作。

要求

Cisco 建议您了解以下主题:

- •了解WLC和轻量接入点(LAP)的基本知识。
- •了解AAA服务器(如ISE)的功能知识。
- 深入了解无线网络和无线安全问题。
- •了解动态VLAN分配的功能知识。
- •了解无线接入点控制和调配(CAPWAP)的基本知识。

使用的组件

本文档中的信息基于以下软件和硬件版本:

- •运行固件版本16.12.4a的Cisco Catalyst 9800 WLC(Catalyst 9800-CL)。
- Cisco 2800系列LAP在本地模式下。
- 本地Windows 10请求方。
- •运行版本2.7的思科身份服务引擎(ISE)。
- •运行固件版本16.9.6的Cisco 3850系列交换机。

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。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

背景信息

使用 RADIUS 服务器执行动态 VLAN 分配

在大多数无线局域网(WLAN)系统中,每个WLAN都有一个静态策略,该策略适用于与服务集标识符 (SSID)关联的所有客户端。 虽然此方法功能强大,但它有其局限性,因为它要求客户端与不同的 SSID关联,以继承不同的QoS和安全策略。

然而,Cisco WLAN 解决方案支持网络标识。这允许网络通告单个SSID,并允许特定用户根据用户 凭证继承不同的QoS或安全策略。

动态 VLAN 分配便是一项这样的功能,它根据无线用户提供的凭证将该用户置于特定 VLAN 中。将 用户分配到特定VLAN的任务由RADIUS身份验证服务器(如Cisco ISE)处理。例如,利用此任务 可使无线主机能够在园区网络中移动时保持位于同一 VLAN 中。

因此,当客户端尝试关联到向控制器注册的LAP时,WLC会将用户的凭证传递到RADIUS服务器进 行验证。成功执行身份验证后,RADIUS 服务器便会将某些 Internet 工程任务组 (IETF) 属性传递给 用户。这些RADIUS属性决定必须分配给无线客户端的VLAN ID。客户端的SSID无关紧要,因为用 户始终被分配到此预定VLAN ID。

用于 VLAN ID 分配的 RADIUS 用户属性包括:

- IETF 64 (隧道类型)— 将此项设置为 VLAN。
- IETF 65(隧道介质类型) 将此值设置为802。
- IETF 81(隧道专用组 ID)— 将此项设置为 VLAN ID。

VLAN ID为12位,值介于1和4094之间(含1和4094)。由于隧道专用组 ID 属于字符串类型(如用 于 IEEE 802.1X 的 <u>RFC2868 中所定义),因此,VLAN ID 整数值被编码为字符串。</u>发送这些隧道 属性时,必须在Tag字段中输入它们。

配置

本部分提供有关如何配置本文档所述功能的信息。

网络图

本文档使用以下网络设置:



下面是此图中使用的组件的配置详细信息:

- •思科ISE(RADIUS)服务器的IP地址是10.10.1.24。
- WLC 的管理接口地址为 10.10.1.17。
- •控制器上的内部 DHCP 服务器用于将 IP 地址分配给无线客户端。
- •本文档使用802.1x和PEAP作为安全机制。
- VLAN102用于此配置。用户名jonathga-102配置为由RADIUS服务器放入VLAN102。

配置步骤

此配置分为三类:

- 思科ISE配置。
- 为多个 VLAN 配置交换机.
- Catalyst 9800 WLC配置。

思科ISE配置

此配置要求执行下列步骤:

- 将Catalyst WLC配置为Cisco ISE服务器上的AAA客户端。
- 在思科ISE上配置内部用户。
- •在Cisco ISE上配置用于动态VLAN分配的RADIUS(IETF)属性。

步骤1.在Cisco ISE服务器上将Catalyst WLC配置为AAA客户端

此过程说明如何将WLC添加为ISE服务器上的AAA客户端,以便WLC将用户凭证传递给ISE。

请完成以下步骤:

1. 从ISE GUI导航至 Administration > Network Resources > Network Devices选择 Add。

2. 使用WLC管理IP地址和WLC和ISE之间的RADIUS共享密钥完成配置,如图所示:

cisco lidentity oervices Engine	Home	 Context 	Visibility	Operations	Policy	 Administration 	 Work Centers 	
System Identity Management	- Network	Resources	Device Po	rtal Management	pxGrid Se	rvices Feed S	ervice	NAC
Network Devices Network Device (Groups	Network Devic	ce Profiles	External RADIUS	Servers R	ADIUS Server Sequ	uences NAC Managers	External MD
Network Devices	Netwo	rk Devices Lis	it > New Netw	ork Device				
Default Devices	Netw	ork Device	es			_		
Delault Device			* Na	me WLC-C980	0-CL			
Device Security Settings			Descript	ion vWLC-980	0			
	I	IP Address	▼ *IP	10.10.1.17			/ 32	
			* Device Pro	file ditto Cisco	• ⊕			
			Model Na	me	*			
			Software Vers	ion	*			
		Network Dev	ice Group					
		Location [All Locations	0 s	et To Default)		
		IPSEC [No	📀 🕓	et To Default			
	0	evice Type	WLC	📀 💽	et To Default)		
	_							
			authentication \$	Settings				
		RADIUS	UDP Settings					
					Pro	tocol RADIUS		
					* Shared Se	ecret •••••	Show	N
				Use Sec	ond Shared Se	ecret 🗌 🔅		
							Show	N
					CoA	Port 1700	Set	To Default

此过程说明如何在思科ISE的内部用户数据库上添加用户。

请完成以下步骤:

- 1. 从ISE GUI导航至 Administration > Identity Management > Identities 选择 Add。
- 2. 使用用户名、密码和用户组完成配置,如图所示:

ultulu cisco	Ident	ity Servic	es Engine	Home	Context Visib	ility 🕨 Opera	tions P	olicy 🗸	dministration	Work Centers
► Sys	stem	◄ Identity	Management	Network	Resources F	evice Portal Mar	nagement p	xGrid Service	es 🔹 🕨 Feed Se	rvice
✓Ider	ntities	Groups	External Iden	tity Sources	Identity Source	Sequences	Settings			
			G	Networ	k Access Users Li	st > New Networ	k Access User	r		
Users				▼ Ne	twork Access	Jser				
Latest I	Manual	Network S	Scan Results	* Na Sta	ame jonathga-10 atus 🔽 Enable	02 ed 👻				
				E	nail					
				▼ P	asswords					
				Pa	ssword Type:	Internal Users		•		
					F	assword		Re-En	ter Password	
				*L	ogin Password	•••••		•••••	•••	Generate Password (i)
				En	able Password	•••••		•••••	•••	Generate Password (i)
				• 0	ser informatio					
				Fir	st Name					
				La	st Name					
				– A	ccount Option	5				
						Description				
				Cr	ange password o	n next login 🛛				
				▼ A	ccount Disable	Policy				
					Disable accoun	t if date exceeds	2021-05-18	}	(ууу	y-mm-dd)
				v 0	ser Groups					
				≣ ∨	LAN102	0) — +			
				Sub	mit Cancel					

步骤3.配置用于动态VLAN分配的RADIUS(IETF)属性

此过程说明如何为无线用户创建授权配置文件和身份验证策略。

请完成以下步骤:

- 1. 从ISE GUI导航至 Policy > Policy Elements > Results > Authorization > Authorization profiles 选择 Add 创建 新配置文件。
- 2. 使用相应组的VLAN信息完成授权配置文件配置。此图显示 jonathga-VLAN-102 组配置设置。

cisco	Identit	y Services Engir	le Home	Context Visibility	 Operations 	▼ Policy	Administration	Work Centers	
Poli	cy Sets	Profiling Postu	re Client Provis	ioning Policy Ele	ments				
Dict	ionaries	Conditions	• Results						
			O Authori	zation Profiles > jonal	thga-VLAN-102				
▶ Aut	henticati	on	Autho	orization Profile	-				
▼ Aut	horizatio	n		* Name	jonathga-VLAN-102]		
Au	thorizatio	n Profiles		Description	Dynamic-Vlan-Asign	ment			
Do	wnloadab	ole ACLs		Access Type	ACCESS_ACCEPT	7			
+ Pro	filing		Netw	ork Device Profile	🟥 Cisco 💌 🕀				
Pos	sture			Service Template					
♦ Clie	ent Provis	sioning		Track Movement					
			Pass	ive Identity Tracking	(i)				
			▼ Co	mmon Tasks					
			0	DACL Name					
			0	ACL (Filter-ID)					
			•	Security Group					_
				VLAN	Ta	ag ID 1	Edit Tag	ID/Name 102	
			_						
			▼ Ad	lvanced Attributes	s Settings				
			Se	lect an item	😒 =		0	- +	
			▼ At	tributes Details					
			Acce Tunr Tunr Tunr	ss Type = ACCESS_AC hel-Private-Group-ID = hel-Type = 1:13 hel-Medium-Type = 1:	CCEPT = 1:102 6				
			Save	Reset					

配置授权配置文件后,需要为无线用户创建身份验证策略。您可以使用 Custom 策略或修改 Default 策略集。在本例中,创建了自定义配置文件。

3. 导航至 Policy > Policy Sets 选择 Add 要创建新策略,如图所示:

cisco	Identity	Services Engine	Home	Context Visibility	 Operations 	▼Policy	Administration	Work Centers			Q,	0	• •	
Policy	Sets F	Profiling Posture	Client Provision	ing + Policy Elem	ents									
Policy	/ Sets										F	Reset	Save	
+	Statu	s Policy Set Nar	ne	Description		Condition	าร		Allowed Protocols / Serve	er Sequence	Hits	Actions	View	
Searc	:h													
1	\odot	Jonathga-Policy		Dynamic-Vlan-As	signment	₽ D T)	EVICE-Device Type EC /pes#WLC	QUALS All Device	Default Network Access	× • +		٥	>	
✓ Auther	ntication P	olicy (2)												
(+)	Status	Rule Name	Condit	ions						Use				
Search														
										Inte	ernal Users		* *	
	ø	wireless-dot1x		Wireless_802.1X						>	Options			-
										-	Liser ID O	ineras.		5
	\odot	Default								~!!	User_ID_SI	lores		
										>	Options			

现在,您需要为用户创建授权策略,以便根据组成员身份分配相应的授权配置文件。

5. 打开 Authorization policy 部分并创建策略以满足该要求,如图所示:

					Results				
T	Status	Rule Name	Conditi	ns	Profiles	Security Groups	Hits	Actions	
Search									
	0	VLAN-102	AND	InternalUser identityGroup EQUALS User identity Groups:VLAN102 Vireless_802.1X	×jonathga-VLAN-102	Select from list 💌 🕇	0	٥	
	0	VLAN-105	AND	InternalUser identityGroup EQUALS User identity Groups VLAN105 Wireless_802.1X	×jonathga-VLAN-105	Select from list	0	٥	
	0	Default			* DenyAccess	Select from list	0	٥	

为多个 VLAN 配置交换机

要允许多个VLAN通过交换机,您需要发出以下命令来配置连接到控制器的交换机端口:

Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk encapsulation dot1q

注意:默认情况下,大多数交换机都允许在该交换机上通过中继端口创建的所有 VLAN。如果 有线网络连接到交换机,则可以将此相同配置应用于连接到有线网络的交换机端口。这样将在 位于有线网络和无线网络中的相同 VLAN 之间实现通信。

Catalyst 9800 WLC配置

此配置要求执行下列步骤:

- 用身份验证服务器的详细信息配置 WLC.
- 配置VLAN。
- 配置WLAN(SSID)。
- 配置策略配置文件。

- 配置策略标记。
- 将策略标记分配给AP。

步骤1.使用身份验证服务器的详细信息配置WLC

必须配置WLC,以便它能够与RADIUS服务器通信以验证客户端。

请完成以下步骤:

1. 从控制器GUI导航至 Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add 并输入 RADIUS服务器信息,如图所示:

Q Search Menu Items	Authe	ntication A	uthorizatior	and Account	ting	
🚃 Dashboard	+ 4	AA Wizard				
Monitoring	>	AAA Method List		Servers / Groups		AAA Advanced
Real Configuration	› 📑	Add				
() Administration	> RA	DIUS				
💥 Troubleshootin	g ta	CACS+	_	Servers	Server G	iroups
	10	٨D		Name	×.	Address
Create AAA Radius Server		_				×
Name*	Cisco-ISE		Support for CoA		ENABLED	(i)
Server Address*	10.10.1.24		CoA Server Key	Туре	Clear Text	¥
PAC Key	0		CoA Server Key	i		
Кеу Туре	Clear Text 🔻		Confirm CoA Ser	ver Key		
Key* 🛈			Automate Tester		D	
Confirm Key*						
Auth Port	1812					
Acct Port	1813					
Server Timeout (seconds)	1-1000]				
Retry Count	0-100]				
Cancel						Apply to Device

2. 要将RADIUS服务器添加到RADIUS组,请导航至 Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add 如图所示:

Create AAA Radius Server Group

Name*	ISE-SERVER		
Group Type	RADIUS		
MAC-Delimiter	none 🔻		
MAC-Filtering	none 🔻		
Dead-Time (mins)	5		
Load Balance	DISABLED		
Source Interface VLAN ID	none 🔻		
Available Servers	Assigne	d Servers	
server-2019	Cisco-ISE	*	 <
Cancel			Apply to Device

3. 要创建身份验证方法列表,请导航至 Configuration > Security > AAA > AAA Method List > Authentication > + Add 如图所示:



×

Quick Setup: AAA Authentication

Method List Name*	ISE-SERVER		
Туре*	dot1x •		
Group Type	group 🔹 🤅		
Fallback to local	0		
Available Server Groups	Assign	ed Server Groups	
radius Idap tacacs+ radgrp_SykesLab server2019 tacacgrp_SykesLab	> ISE-SERVER		
Cancel			Apply to Device

步骤2.配置VLAN

此步骤说明如何在Catalyst 9800 WLC上配置VLAN。如本文档中上文所述,WLC 中也必须具有在 RADIUS 服务器的 Tunnel-Private-Group ID 属性下指定的 VLAN ID。

在本例中,用户jonathga-102使用 Tunnel-Private-Group ID of 102 (VLAN =102) 在RADIUS服务器上。

1. 导航至 Configuration > Layer2 > VLAN > VLAN > + Add 如图所示:

Q Search Menu Items	
Dashboard SVI VLAN	VLAN Group
Monitoring > + Add × Delete	
Configuration > VLAN ID	~ Name
(☉) Administration →	defau
	VLAN
Troubleshooting	VLAN
2602	VLAN

2. 输入所需信息,如图所示:

STEALE VEAN							^
Create a single VLAN							
VLAN ID*	102						
Name			١				
State	ACTIVATED						
IGMP Snooping	DISAB	LED					
ARP Broadcast	DISAB	LED					
Port Members				Q Search			
	Available (2)		Associated	(0)			
	Gi1	>			Î		
	Gi2	÷					
			No Assoc	iated Members			
					*		
O Create a range of VLAN	ls						
VLAN Range*	· .	(Ex:5-7	7)				
Cancel					L	Apply to De	vice

注意:如果不指定名称,VLAN将自动获得VLANXXX的名称,其中XXXX是VLAN ID。

对所有需要的VLAN重复步骤1和2,完成后,您可以继续步骤3。

3. 验证数据接口中是否允许VLAN。 如果您正在使用端口通道,请导航至 Configuration > Interface > Logical > PortChannel name > General。如果您看到它配置为 Allowed VLAN = All 配置完成。如果您看 到 Allowed VLAN = VLANs IDs,添加所需的VLAN,然后选择 Update & Apply to Device。如果没有使用 端口通道,请导航至 Configuration > Interface > Ethernet > Interface Name > General。如果您看到它配置 为 Allowed VLAN = All 配置完成。如果您看到 Allowed VLAN = VLANs IDs,添加所需的VLAN,然后选 择 Update & Apply to Device。

如果使用All或特定VLAN ID,此图像显示与接口设置相关的配置。

General	Advanced	
Interface		GigabitEthernet3
Description		(1-200 Characters)
Admin Status		UP
Port Fast		disable 🔹
Enable Layer	3 Address	DISABLED
Switchport Mo	ode	trunk 🔹
Allowed Vlan		 All Vlan IDs
Native Vlan		•

.

General Advanced	
Interface	GigabitEthernet1
Description	(1-200 Characters)
Speed	1000 🔻
Admin Status	UP 💽
Enable Layer 3 Address	DISABLED
Switchport Mode	trunk 🔻
Allowed Vlan	O All O Vlan IDs
Vlan IDs	551,102,105 (e.g. 1,2,4,6-10)
Native Vlan	551 🔻

步骤3.配置WLAN(SSID)

此过程说明如何在 WLC 中配置 WLAN。

请完成以下步骤:

1. 以创建WLAN。导航至 Configuration > Wireless > WLANs > + Add 并根据需要配置网络,如图所示:

Q Search Menu Items	WIRELESS NETWORKS	
Dashboard	+ Add X Delete	
Monitoring >	Name	≪ 1
	wob-anch	5

2. 输入WLAN信息,如图所示:

WLAN			
eral Security	Advanced		
Profile Name*	Dinamyc-VLAN	Radio Policy All 🔻	
6SID*	Dinamyc-VLAN	Broadcast SSID	
WLAN ID*	6		
Status			

Cancel	Apply to Device

3. 导航至 Security 选项卡,然后选择所需的安全方法。在本例中,WPA2 + 802.1x如图所示:

Add WLAN				×
General	Security	Advanced		Ť.
Layer2	Layer3	AAA		
Layer 2 Security Mode	WPA + WPA2 ¥	Fast Transition	Adaptive Enab 👻	
MAC Fitering		Over the DS		
Protected Management Frame		Reassociation Timeout	20	
PMF	Disabled •			ł
WPA Parameters				
WPA Poinv				
"D Cancel			Save & Apply to Devic	

Add WLAN		¢
PMF	Disabled v	
WPA Parameters		
WPA Policy		
WPA2 Policy	\checkmark	
WPA2 Encryption	AES(CCMP128) CCMP256 GCMP128 GCMP256 G	
Auth Key Mgmt	802.1x v	
ບ Cancel	Save & Apply to Device	

发件人Security > AAA 选项卡,从 Configure the WLC with the Details of the Authentication Server 部分,如图所示:

Add WLAN	Add WLAN				
General	Security	Advanced			
Layer2	Layer3	ΑΑΑ			
Authenti	cation List				
Local EA	AP Authenticat	tion 🖸			

Cancel

Apply to Device

步骤4.配置策略配置文件

此过程说明如何在WLC中配置策略配置文件。

请完成以下步骤:

1. 导航至 Configuration > Tags & Profiles > Policy Profile 配置 default-policy-profile 或创建新映像,如图所

示:	_		
Q Search Menu Items	Policy Profile		
B Dashboard	+ Add X Delete		
Monitoring >	Policy Profile Name	< Description	
Configuration >	default-policy-profile	default policy profile	
ි Administration >	4 4 1 ⊨ ⊨ 10 v ite	ms per page	
Edit Policy Profile General Acces	s Policies QOS and AVC	Mobility Advanced	
🛦 Con	figuring in enabled state will result in loss of	connectivity for clients associated with this profil	e.
Name*	default-policy-profile	WLAN Switching Policy]
Description	default policy profile	Central Switching	
Status		Central Authentication	
Passive Client	DISABLED	Central DHCP	
Encrypted Traffic Analytic	DISABLED	Central Association Enable	
CTS Policy		Flex NAT/PAT	
Inline Tagging			
SGACL Enforcement			

2. 从 Access Policies 选项卡分配无线客户端在默认情况下连接到此WLAN时分配到的VLAN,如图 所示:

2-65519

Default SGT

Edit Policy Profile						
General Access Policies	QOS and AVC	Mobility	Ad	vanced		
WLAN Local Profiling		V	WLAN ACL			
HTTP TLV Caching		IF	Pv4 ACL	Search or Select	•	
RADIUS Profiling		IF	Pv6 ACL	Search or Select	•	
DHCP TLV Caching			URL Filters			
Local Subscriber Policy Name	Search or Select 🔹	P	Pre Auth	Search or Select		
VLAN			Poet Auth	Search or Select		
VLAN/VLAN Group	VLAN2602 •		OSC AUT		•	
Multicast VLAN	Enter Multicast VLAN					

注意:在提供的示例中,RADIUS服务器的工作是在身份验证成功后将无线客户端分配给特定 VLAN,因此策略配置文件上配置的VLAN可以是黑洞VLAN,RADIUS服务器会覆盖此映射 ,并将通过该WLAN的用户分配给RADIUS服务器中用户Tunnel-Group-Private-ID字段下指定 的VLAN。

3. 从 Advance 选项卡 Allow AAA Override 复选框以覆盖WLC配置,当RADIUS服务器返回将客户端 置于正确VLAN所需的属性时,如图所示:

General A	ccess Policies	QOS and AVC	Mobility	Advanced			
WLAN Timeout				Fabric Profile		Search or Select	٣
Session Timeout	(sec)	1800		Umbrella Parameter Map		Not Configured	•
dle Timeout (sec	:)	300		mDNS Service Policy		default-mdns-servic	•
dle Threshold (b	ytes)	0	1	,			Clea
Night Exclusion	Timoout (eac)	× 60	7	WLAN Flex Poli	су		
Silent Exclusion	nneour (sec)	60		VLAN Central Sw	itching	9	
DHCP				Solit MAC ACL		Search or Select	•
Pv4 DHCP Requ	ired						
HCP Server IP	Address		7	Air Time Fairnes	ss Pol	licies	
			_	2.4 GHz Policy		Search or Select	•
ow more >>>				5 GHz Policy		Search or Select	
AAA Policy							
Allow AAA Overr	ide						
NAC State							
Policy Name		default-aaa-policy 🗙	•				

步骤5.配置策略标记

此过程说明如何在WLC中配置策略标记。

请完成以下步骤:

<u>1. 导航至 Configuration ></u> Tags & Profiles > Tags > Policy 如图所示,如果需要,添加一个新的:

Q Search Menu Items		Manage Tags	
Dashboard		Policy Site RF AP	
Monitoring	>	+ Add	
🔾 Configuration	>	Policy Tag Name	< Description
বি Administration	>	central-anchor	
~		default-policy-tag	default policy-tag
X Troubleshooting		< < 1 ► ► 10 ▼ items per page	

2. 将名称添加到策略标记并选择 +Add,如图所示:

ŀ	Add Policy Tag				×
	Name*	Dynamic-VLAN			
	Description	Enter Description			
	VULAN-POLICY	/ Maps: 0			
	+ Add × Dele	ete			
	WLAN Profile		T	Policy Profile	Ŧ
	H	10 🔻 items per page	9		No items to display

3. 将WLAN配置文件链接到所需的策略配置文件,如图所示:

Add Policy Tag			×
Name*	Dynamic-VLAN		
Description	Enter Description		
VILAN-POLICY	(Maps: 0		
+ Add × Dele	ete		
WLAN Profile		Policy Profile	T
⊌ ∢ 0 ► №	10 🔻 items per page		No items to display
Map WLAN and Pol	icy		
WLAN Profile*	Dinamyc-VLAN 🗸	Policy Profile*	default-policy-profil 🔻
		· ·	

Add Policy Tag				×
Name*	Dynamic-VLAN			
Description	Enter Description			
WLAN-POLICY + Add × Delete	/ Maps: 1			
WLAN Profile		~	Policy Profile	×.
Dinamyc-VLAN			default-policy-profile	
	10 🔻 items per page			1 - 1 of 1 items
RLAN-POLICY	Maps: 0			
Cancel				

步骤6.将策略标记分配给AP

此过程说明如何在WLC中配置策略标记。

请完成以下步骤:

1. 导航至 Configuration > Wireless > Access Points > AP Name > General Tags 分配相关策略标记,然后选择 Update & Apply to Device 如图所示:

Edit AP			×
General Interfaces	High Availability Inve	entory ICap Advanced	
General		Version	
AP Name*	AP2802I-B-K9	Primary Software Version	16.12.4.31
Location*	default location	Predownloaded Status	N/A
Base Radio MAC	10b3.d677.a8c0	Predownloaded Version	N/A
Ethernet MAC	084f.a9a2.8ed4	Next Retry Time	N/A
Admin Status	ENABLED	Boot Version	1.1.2.4
AP Mode	Local	IOS Version	16.12.4.31
Operation Status	Registered	Mini IOS Version	0.0.0.0
Fabric Status	Disabled	IP Config	
LED State	ENABLED	CAPWAP Preferred Mode IPv	4
LED Brightness Level	8 🔻	DHCP IPv4 Address 10.	10.102.101
CleanAir <u>NSI Key</u>		Static IP (IPv4/IPv6)	
Tags		Time Statistics	
Policy	Dynamic-VLAN 🔻	Up Time	0 days 0 hrs 4 mins 52 secs
Site	default-site-tag	Controller Association Latency	1 min 36 secs
Cancel			Update & Apply to Device

警告:请注意,当AP上的策略标记更改时,它会丢弃与WLC的关联并重新加入。

验证

使用本部分可确认配置能否正常运行。

测试与Windows 10和本地请求方的连接,当系统提示您输入用户名和密码后,输入ISE上映射到 VLAN的用户信息。

在上一个示例中,请注意jonathga-102已分配给RADIUS服务器中指定的VLAN102。本示例使用此 用户名接收身份验证,并由RADIUS服务器分配给VLAN:

完成身份验证后,您需要根据发送的RADIUS属性验证是否将客户端分配到正确的VLAN。完成以下 步骤以完成此任务:

1. 从控制器GUI导航至 Monitoring > Wireless > Clients > Select the client MAC address > General > Security

Information 并查找VLAN字段,如图所示:

Monitoring >> Wireless >> Clients	Client		
	360 View General QOS Statist	ics ATF Statistics	
Clients Sleeping Clients Excluded Clients	Client Properties AP Properties	Security Information	
× Delete	IIF ID	0x9000008	
	Authorized	TRUE	
Total Client(s) in the Network: 1	Common Session ID	33020A0A0000003	
Number of Client(s) selected: 0	Acct Session ID	0x00000000	
	Auth Method Status List		
	Method	Dot1x	
b88a.6010.3c60 💥 10.10.102.121 fe80::d8a2:dc93:3758:&	SM State	AUTHENTICATED	
i 🚽 🚽 1 🕨 10 🔻 items per page	SM Bend State	IDLE	
	Protocol Map	0x000001 (OUI)	
	Local Policies		
	Service Template	wlan_svc_default-	
	Absolute Timer	1800	
	Server Policies		
	VLAN	102	
	Resultant Policies		
	VLAN Name	VLAN0102	
	VLAN	102	

在此窗口中,您可以观察到此客户端根据RADIUS服务器上配置的RADIUS属性分配给 VLAN102。在CLI中,您可以使用 show wireless client summary detail 要查看与图中所示相同的信 息

·										
Catalyst-C980 Number of Cli	0-CL≸show wireless client summan ents: 1	y detail								
MAC Address BSSID	SSID Auth Method	AP Name Created	Connected	State Protocol Ch	IP Addres annel Width	s SGI NSS Rate	CAP	Username	Device-type	VLAN
10000-00 10.3c6 1001-00	0 Dinamyc-VLAN 0 [802.1x]	AIR-AP2802I-A 05	-K9 06	Run 11n(2.4) 1	10.10.105 20/20	.200 Y/Y 1/1 24.0	Е	jonathga-1	Intel-Device	105
Catalyst-C980 Number of Cli	0-CL∯show wireless client summan ents: 1	y detail								
MAC Address BSSID	SSID Auth Method	AP Name Created	Connected	State Protocol Ch	IP Addres annel Width	SGI NSS Rate	CAP	Username	Device-type	VLAN

2. 可以启用 Radioactive traces 确保RADIUS属性成功传输到WLC。为此,请执行以下步骤: 从控 制器GUI导航至 Troubleshooting > Radioactive Trace > +Add。输入无线客户端的Mac地址。选择 Start。将客户端与WLAN连接。导航至 Stop > Generate > Choose 10 minutes > Apply to Device > Select the trace file to download the log。

跟踪输出的这一部分确保RADIUS属性成功传输:

.

```
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Received from id
1812/60 10.10.1.24:0, Access-Accept, len 352
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: authenticator e5 5e
58 fa da 0a c7 55 - 53 55 7d 43 97 5a 8b 17
```

2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: User-Name 13 "jonathga-102" [1] 2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: State [24] 40 ... 2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Class 54 ... [25] 2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): 01: 2021/03/21 22:22:45.236 {wncd x R0-0}{1}: [radius] [25253]: (info): RADIUS: Tunnel-Type [64] 6 VLAN [13] 2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): 01: 2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Tunnel-Medium-Type 6 ALL 802 [65] [6] 2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: EAP-Message [79] б... 2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Message-18 ... Authenticator[80] 2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): 01: 2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Tunnel-Private-Group-Id[81] 6 "102" 2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: EAP-Key-Name [102] 67 * 2021/03/21 22:22:45.237 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: MS-MPPE-Send-Key 52 [16] 2021/03/21 22:22:45.237 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: MS-MPPE-Recv-Key [17] 52 * 2021/03/21 22:22:45.238 {wncd_x_R0-0}{1}: [eap-auth] [25253]: (info): SUCCESS for EAP method name: PEAP on handle 0x0C000008 2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [Applied attribute username 0 "jonathga-102"] : 2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [Applied attribute class 0 43 41 43 53 3a 33 33 30 32 30 41 30 41 30 30 30 30 30 30 33 35 35 36 : 45 32 32 31 36 42 3a 49 53 45 2d 32 2f 33 39 33 33 36 36 38 37 32 2f 31 31 32 36 34 30] 2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [Applied attribute tunnel-type 1 13 [vlan]] : 2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [Applied attribute : tunnel-medium-type 1 6 [ALL_802]] 2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [Applied attribute :tunnel-private-group-id 1 "102"] 2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [Applied attribute timeout 0 1800 (0x708)] $\label{eq:loss} \end{tabular} $$ 2021/03/21 \ 22:22:46.700 \ \{wncd_x_R0-0\} \end{tabular} $$ auth-mgr-feat_wireless] \ [25253]: (info): $$ (in$ [0000.0000.0000:unknown] AAA override is enabled under policy profile

故障排除

目前没有针对此配置的故障排除信息。

相关信息

• 最终用户指南