# 在Catalyst 9800 WLC上配置本地EAP身份驗證

目錄 簡介 必要條件 需求 <u>採用元件</u> 設定 網路圖表 <u>主本地EAP配置</u> 步驟 1.本地EAP配置檔案 步驟 2.AAA認證方法 步驟 3.配置AAA授權方法 步驟 4.配置本地高級方法 步驟 5.設定WLAN 步驟 6.建立一個或多個使用者 步驟7.建立策略配置檔案。建立策略標籤以將此WLAN配置檔案對映到策略配置檔案 步驟 8.將策略標籤部署到接入點。 驗證 疑難排解 由於密碼錯誤而無法連線的客戶端示例

<u>失敗時的跟蹤</u>

# 簡介

本檔案介紹Catalyst 9800 WLC(無線LAN控制器)上的本地EAP的組態。

## 必要條件

### 需求

本檔案介紹Catalyst 9800 WLC上本地EAP(可擴充驗證通訊協定)的組態;即WLC執行為無線使 用者端的RADIUS驗證伺服器。

本檔案假設您熟悉9800 WLC上的WLAN基本組態,且僅專注於WLC作為無線使用者端的本地 EAP伺服器運作。

### 採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

16.12.1s版上的Catalyst 9800

設定

網路圖表



主本地EAP配置

步驟 1.本地EAP配置檔案

在9800 Web UI中轉至Configuration > Security > Local EAP。



```
選擇Add
```

輸入配置檔名稱。

由於安全性較差,LEAP完全不被建議使用。其他3種EAP方法中的任何一種都需要您配置信任點。 這是因為作為驗證者的9800必須傳送憑證讓使用者端信任它。

使用者端不信任WLC預設憑證,因此您需要在使用者端停用伺服器憑證驗證(不建議),或在9800 WLC上安裝使用者端信任的憑證信任點(或手動匯入使用者端信任儲存區中)。

Create Local EAP Profiles		×
Profile Name*	mylocaleap	
LEAP		
EAP-FAST		
EAP-TLS		
PEAP		
Trustpoint Name	admincert	,
Cancel		Apply to Device

CLI:

(config)#eap profile mylocapeap (config-eap-profile)#method peap (config-eap-profile)#pki-trustpoint admincert

步驟 2.AAA認證方法

您需要配置本地點的AAA dot1x方法,以便使用使用者的本地資料庫(但可以使用外部LDAP查詢 ,例如)。

前往Configuration > Security > AAA,然後前往AAA method list索引標籤以進行驗證。選擇Add。

選擇「dot1x」型別和本地組型別。

Configuration • > 5	Security + > AAA													
+ AAA Wizerd														
Servers / Groups	AAA Method List	AAA Adva	nced											
Authentication					_									
Authorization			- + 4	d × Dele	te									
Accounting				Name		Туре	< Group Type	~	Group1	Group2	v Group3	~	Group4	~
				default		dot1x	local		N/A	N/A	N/A		N/A	
			н	1 = =	10 • items per p	oge								1 - 1 of 1 items

步驟 3.配置AAA授權方法

轉到Authorization子頁籤,並建立用於鍵入credential-download的新方法並將其指向本地。

對網路授權型別執行相同操作

CLI:

```
(config)#aaa new-model
(config)#aaa authentication dot1x default local
(config)#aaa authorization credential-download default local
(config)#aaa local authentication default authorization default
(config)#aaa authorization network default local
```

步驟 4.配置本地高級方法

轉到AAA advanced選項卡。

Configuration - > Security - > AAA

定義本地身份驗證和授權方法。由於此示例使用了「預設」憑證下載和「預設」dot1x方法,您需要 在此為本地身份驗證和授權下拉框設定預設值。

如果已定義命名方法,請在下拉選單中選擇「方法清單」,然後使用另一個欄位輸入方法名稱。

+ AAA Wizard					
Servers / Groups	AAA Method List	AAA Advanced			
Global Config		Local Authe	entication	Default	•
RADIUS Fallback		Local Author	orization	Default	•
Attribute List Name	Ð	Radius Sen	ver Load Balance	DISABLED	
Device Authentica	tion	Interim Upo	late		
AP Policy		Show Adva	Inced Settings >>>		
Password Policy					
AAA Interface					

CLI:

aaa local authentication default authorization default

步驟 5.設定WLAN

然後,您可以根據上一步中定義的本地EAP配置檔案和AAA身份驗證方法配置WLAN的802.1x安全 性。

轉至Configuration > Tags and Profiles > WLANs > + Add >

提供SSID和配置檔名稱。

預設情況下, Dot1x security在第2層下處於選中狀態。

在AAA下,選擇Local EAP Authentication,並從下拉選單中選擇Local EAP profile和AAA Authentication list。

dit WLAN	١				
General	Security	Advanced			
Layer <sup>2</sup>	Layer3	AAA			
Layer 2 Se	curity Mode		WPA + WPA2 V	Fast Transition	Adaptive Enabled
MAC Filteri	ng			Over the DS	
Protected	l Manageme	ent Frame		Reassociation Timeout	20
				MPSK Configuration	
PMF			Disabled 🔻	MPSK	
WPA Para	ameters				
WPA Policy	/				
WPA2 Polic	су				
WPA2 Enci	ryption		AES(CCMP128)		
			CCMP256		
			GCMP128		
			GCMP256		
Auth Key N	lgmt		✓ 802.1x		
			PSK		
			CCKM		
			FT + 802.1x		
			FT + PSK		
			802.1x-SHA256		
			PSK-SHA256		

# Edit WLAN General Security Advanced Layer2 Layer3 AAA Authentication List default Local EAP Authentication EAP Profile Name mylocaleap

(config)#wlan localpeapssid 1 localpeapssid (config-wlan)#security dot1x authentication-list default (config-wlan)#local-auth mylocaleap

步驟 6.建立一個或多個使用者

在CLI中,使用者必須是network-user型別。以下是在CLI中建立的使用者範例:

(config)#user-name 1xuser creation-time 1572730075 description 1xuser password 0 Cisco123 type network-user description 1xuser

在CLI中建立後,此使用者在Web UI中可見,但如果在Web UI中建立,則沒有方法使其自16.12起 成為network-user

步驟 7.建立策略配置檔案。建立策略標籤以將此WLAN配置檔案對映到策略配置檔案

轉到Configuration > Tags and profiles > Policy

為WLAN建立策略配置檔案。

### 此範例顯示flexconnect本機交換,但vlan 1468上發生中央驗證情況,但這取決於您的網路。

Edit Poli	cy Profile						x
Geheral	Access Policies	QOS and AVC	Mobility	Advanced			
	A Configurin	g in enabled state will re	sult in loss of c	connectivity fo	or clients associated with thi	s profile.	
Name	e*	leap		WLAN	Switching Policy		
Desc	ription	Enter Description		Central	Switching	DISABLED	
Statu	IS	ENABLED		Central	Authentication	ENABLED	
Pass	ive Client	DISABLED		Central	DHCP	ENABLED	
Encry	vpted Traffic Analytics	DISABLED		Central	Association	ENABLED	
CTS	Policy			Flex NA	AT/PAT	DISABLED	
Inline	Tagging						
SGA	CL Enforcement						
Defa	ult SGT	2-65519					

### 轉至Configuration > Tags and profiles > Tags

### 將WLAN分配給標籤內的策略配置檔案。

Configuration - > Tags & Profiles - > Tags		Edit Policy Tag		×
Policy Site RF AP		A Changes m	ay result in loss of connectivity for some clients that are	e associated to APs with this Policy Tag.
C Ad C Deep		Name*	default-policy-tag	
Policy Tag Name	<ul> <li>Description</li> </ul>	Description	default policy-tag	
default-policy-tag	default policy-tag	VIAN-POLK	CY Mans: 1	
H + 1 + H 10 + Rems per page		- HEATFOLK	or mapa. T	
		+ Add X Delete		
		WLAN Profile	<ul> <li>Policy Prof</li> </ul>	die v
		ndarchis_leap	leap	
		× < 1 × ×	10 v items per page	1 - 1 of 1 items
		> RLAN-POLIC	CY Maps: 0	

### 步驟 8.將策略標籤部署到接入點。

在這種情況下,對於單個AP,可以直接在AP上分配標籤。

轉至Configuration > Wireless >Access points,然後選擇要配置的AP。

確保分配的標籤是您配置的標籤。

驗證

主要配置行如下所示:

aaa new-model aaa authentication dot1x default local aaa authorization credential-download default local aaa local authentication default authorization default eap profile mylocaleap method peap pki-trustpoint admincert user-name 1xuser creation-time 1572730075 description 1xuser password 0 Cisco123 type network-user description 1xuser wlan ndarchis\_leap 1 ndarchis\_leap local-auth mylocaleap security dot1x authentication-list default no shutdown

### 疑難排解

請注意,Cisco IOS® XE 16.12及更早版本僅支援TLS 1.0進行本地EAP身份驗證,如果客戶端越來 越普遍地僅支援TLS 1.2,則可能會造成問題。Cisco IOS® XE 17.1及更高版本支援TLS 1.2和TLS 1.0。

若要對連線有問題的特定客戶端進行故障排除,請使用RadioActive Tracing。轉至故障排除> RadioActive Trace,新增客戶端MAC地址。

選擇開始以啟用該客戶端的跟蹤。

Troubleshooting - > Radioactive Trace		
Conditional Debug Global State: Started		
+ Add × Delete Start Stop		
MAC/IP Address	Trace file	
e836.171f.a162	debugTrace_e836.171f.a162.txt 📩	► Generate
I I I I I I I I I I I I I I I I I I I		1 - 1 of 1 items

### 重現問題後,可以選擇Generate按鈕以生成包含調試輸出的檔案。

由於密碼錯誤而無法連線的客戶端示例

2019/10/30 14:54:00.781 {wncd\_x\_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap\_90000004] Sen

2019/10/30	14:54:00.781	{wncd_x_R0-0}{2}:	[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30	14:54:00.784	{wncd_x_R0-0}{2}:	[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec
2019/10/30	14:54:00.784	{wncd_x_R0-0}{2}:	[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30	14:54:00.785	{wncd_x_R0-0}{2}:	[caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG:
2019/10/30	14:54:00.788	{wncd_x_R0-0}{2}:	[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sen
2019/10/30	14:54:00.788	{wncd_x_R0-0}{2}:	[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30	14:54:00.791	{wncd_x_R0-0}{2}:	[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec
2019/10/30	14:54:00.791	{wncd_x_R0-0}{2}:	[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30	14:54:00.791	{wncd_x_R0-0}{2}:	[caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG:
2019/10/30	14:54:00.792	{wncd_x_R0-0}{2}:	[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sen
2019/10/30	14:54:00.792	{wncd_x_R0-0}{2}:	[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30	14:54:00.795	{wncd_x_R0-0}{2}:	[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec
2019/10/30	14:54:00.795	{wncd_x_R0-0}{2}:	[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30	14:54:00.795	{wncd_x_R0-0}{2}:	<pre>[caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG:</pre>
2019/10/30	14:54:00.796	{wncd_x_R0-0}{2}:	[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sen
2019/10/30	14:54:00.796	{wncd_x_R0-0}{2}:	[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30	14:54:00.804	{wncd_x_R0-0}{2}:	[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec
2019/10/30	14:54:00.804	{wncd_x_R0-0}{2}:	[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30	14:54:00.804	{wncd_x_R0-0}{2}:	[caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG:
2019/10/30	14:54:00.805	{wncd_x_R0-0}{2}:	[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sen
2019/10/30	14:54:00.805	{wncd_x_R0-0}{2}:	[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30	14:54:00.808	{wncd_x_R0-0}{2}:	[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec
2019/10/30	14:54:00.808	{wncd_x_R0-0}{2}:	[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30	14:54:00.808	{wncd_x_R0-0}{2}:	<pre>[caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG:</pre>
2019/10/30	14:54:00.808	{wncd_x_R0-0}{2}:	[eap] [23294]: (info): FAST: EAP_FAIL from inner method MSCHAP
2019/10/30	14:54:00.808	{wncd_x_R0-0}{2}:	[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sen
2019/10/30	14:54:00.808	{wncd_x_R0-0}{2}:	[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30	14:54:00.811	{wncd_x_R0-0}{2}:	[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec
2019/10/30	14:54:00.811	{wncd_x_R0-0}{2}:	[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30	14:54:00.811	{wncd_x_R0-0}{2}:	[caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG:
2019/10/30	14:54:00.812	{wncd_x_R0-0}{2}:	[eap-auth] [23294]: (info): FAIL for EAP method name: EAP-FAS
2019/10/30	14:54:00.812	{wncd_x_R0-0}{2}:	[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rai
2019/10/30	14:54:00.813	{wncd_x_R0-0}{2}:	[errmsg] [23294]: (note): %DOT1X-5-FAIL: Authentication faile
2019/10/30	14:54:00.813	{wncd_x_R0-0}{2}:	[auth-mgr] [23294]: (info): [e836.171f.a162:capwap_90000004]

### 失敗時的跟蹤

即使未啟用調試,也可以使用trace-on-failure命令檢查給定mac地址的故障事件清單。

在下一個示例中,AAA方法最初不存在(AAA伺服器關閉事件),幾分鐘後客戶端使用了錯誤的憑 據。

在Cisco IOS® XE 17.1及更高版本中,命令是show logging trace-on-failure summary(16.12及之 前版本),且是show logging profile wireless(filter mac <mac>)trace-on-failure (Cisco IOS XE 17.1及更高版本中)。17.1及更高版本允許您過濾客戶端MAC地址,這一點沒有技術區別。

Nico9800#show logging profile wireless filter mac e836.171f.a162 trace-on-failure
Displaying logs from the last 0 days, 0 hours, 10 minutes, 0 seconds
executing cmd on chassis 2 ...
sending cmd to chassis 1 ...
Collecting files on current[1] chassis.
# of files collected = 30
Collecting files on current[2] chassis.
# of files collected = 30
Collecting files from chassis 1.

Time	UUID	Log	
2019/10/30 14:51:04.4	438 0x0	SANET_AUTHC_FAILURE - AAA Server Down username , audit session <sup>.</sup>	id
2019/10/30 14:58:04.4	424 0x0	e836.171f.a162	N p

### 關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。