在Catalyst 9800上使用锚点配置中央Web身份验 证

目录

简介 先决条件 要求 使用的组件 配置锚定到另一个Catalyst 9800的Catalyst 9800 网络图 在两台9800上配置AAA 在WLC上配置WLAN 在外部WLC上创建策略配置文件和策略标记 在锚点WLC上创建策略配置文件 在两个9800上重定向ACL配置 配置ISE 配置锚定到AireOS WLC的Catalyst 9800 Catalyst 9800外部配置 锚点AireOS WLC上的AAA配置 AireOS WLC上的WLAN配置 在AireOS WLC上重定向ACL 配置ISE 当AireOS WLC是外部WLC,而Catalyst 9800是锚时,配置的差异 验证 故障排除 Catalyst 9800故障排除信息 客户端详细信息 嵌入式数据包捕获 RadioActive跟踪 AireOS故障排除信息 客户端详细信息 从CLI调试 参考

简介

本文档介绍如何在Catalyst 9800上配置并排除中心Web身份验证(CWA)的故障,该CWA指向另一个 无线LAN控制器(WLC)作为移动锚点,使用AireOS或另一个9800 WLC覆盖目标。

先决条件

建议您对9800 WLC、AireOS WLC和思科ISE有基本了解。假设在启动CWA锚点配置之前,您已在 两个WLC之间建立移动隧道。这不在此配置示例的范围内。如果您需要帮助,请参阅标题为"<u>在</u> <u>Catalyst 9800控制器上构建移动隧道"的文档</u>。

使用的组件

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。

9800 17.2.1

5520 8.5.164 IRCM映像

ISE 2.4

配置锚定到另一个Catalyst 9800的Catalyst 9800

网络图



在两台9800上配置AAA

在锚点和外部,您需要先添加RADIUS服务器并确保已启用CoA。这可以在菜单中完成 Configuration>Security>AAA>Servers/Groups>Servers>单击Add按钮。

Cisco Cata	alyst 9800-L Wireless Controller		Welcome admin Last login Fri, May 15 2020 16:56:51
Q Search Menu Items	Configuration > Security > AAA	J	
🚃 Dashboard	+ AAA Wizard		
Monitoring >	Servers / Groups AAA Method Lis	t AAA Advanced	
	+ Add × Delete		
	RADIUS	Servers Server Groups	
C Licensing	TACACS+		
	LDAP	Name	Auth Port
M Housicshooung	Create AAA Radius Server		×
	Name*	CLUS-Server	
	Server Address*	XXXX	
	PAC Key		
	Кеу Туре	Clear Text 🔹	
	Key*		
	Confirm Key*		
	Auth Port	1812	
	Acct Port	1813	
	Server Timeout (seconds)	1-1000	
	Retry Count	0-100	
	Support for CoA	ENABLED	
	Cancel		Apply to Device

您现在需要创建一个服务器组,并将刚配置的服务器放入该组。此操作在此**处完成** Configuration>Security>AAA>Servers/Groups>Server Groups>+Add。

Cisco Cata	alyst 9800-L Wireless Co	ontroller	
Q Search Menu Items	Configuration > Security	y* > AAA	
📻 Dashboard	+ AAA Wizard		
G Monitoring	Servers / Groups AAA	Method List AAA Advanced	
Configuration	+ Add × Delete		
Administration	RADIUS	Servers Server Groups	
© Licensing	TACACS+	Name	
💥 Troubleshooting	LDAP Create AAA Radius Sen/	er Group	× ser
	Create AAA Radius Serve		
	Name*	CLUS-Server-Group	
	Group Type	RADIUS	
	MAC-Delimiter	none 🔻	
	MAC-Filtering	none	
	Dead-Time (mins)	1-1440	
	Available Servers	Assigned Servers	
		CLUS-Server	
	Cancel		Apply to Device

现在,创建一个**授权**方法列表(CWA不需要身份验证方法列表),其中类型为network,组类型为group。将上一操作中的 服务器组添加到此方法列表。

此配置在此处完成Configuration>Security>AAA>Servers/AAA Method List>Authorization>+Add

Cisco Catal	yst 9800-L Wirele	ess Controller			
Q Search Menu Items	Configuration > S	Security * > AAA			
📻 Dashboard	+ AAA Wizard				
Monitoring >	Servers / Groups	AAA Method List	AAA Advanced		
Configuration	Authentication				
Administration	Authorization	Ľ	+ Add X D		
© Licensing	Accounting Quick Setup: AAA	Authorization	Name	√ Туре	Group Type
X Troubleshooting	Method List Name*	CLUS-Au	thZ-Meth-List		
	Туре*	network	•		
	Group Type	group	•		
	Fallback to local				
	Authenticated				
	Available Server Groups	3	Assigned Server Group	ps	
	radius Idap	*	CLUS-Server-G	iroup 🔺	~
	tacacs+ ISE1	<			^
		»			▼
		*		-	<u>×</u>
	Cancel				Apply to Device

(可选)使用与授权方法列表相同的服务器组创建记帐方法列表。可以在此处创建记帐列表 Configuration>Security>AAA>Servers/AAA Method List>Accounting>+Add

¢	cisco	Cisco Cata	alyst 9800-L Wirele	ess Controller					
٩	Search Menu I	tems	Configuration > S	ecurity > AAA					
	Dashboard		+ AAA Wizard						
G	Monitoring		Servers / Groups	AAA Method List	AAA Advanced	I			
Z			Authentication	ſ					
	Administratio	on 🔉	Authorization		-+ Add		Turpe		Group1
C	Licensing		Quick Setup: AAA	Accounting	Name	*.	Туре	*	×
X	Troubleshoo	oting	Method List Name*	CLUS-	Acct-Meth-List				
			Type*	identity	•				
			Available Server Groups		Assigned Server G	roups			
			radius Idap tacacs+ ISE1		CLUS-Ser	ver-Group	•	× × ×	
			Cancel					Apply to	Device

在WLC上配置WLAN

在两个WLC上创建和配置WLAN。两个WLAN上的WLAN应匹配。安全类型应为mac过滤,应应用 上一步的授权方法列表。此配置在**Configuration>Tags & Profiles>WLANs>+Add下完成**

Cisco Cata	alyst 9800-L Wireless	Controller			
Q Search Menu Items	Configuration > Tag	s & Profiles * > WLANs			
Dashboard	+ Add × Dele				
G Monitoring	Number of WLANs selected	:0			
Configuration	Add WLAN	e	✓ ID		~ X
	General Security	Advanced			
C Licensing	Profile Name*	CLUS-WLAN-Name	Radio Policy	All)
X Troubleshooting	SSID*	CLUS-SSID	Broadcast SSID	ENABLED	
	WLAN ID*	2			
	Status	ENABLED			
	Cancel				Apply to Device

Cisco Cata	alyst 9800-L Wireless Controller	
Q Search Menu Items	Configuration * > Tags & Profiles * > WLANs	
Dashboard	+ Add × Delete Enable WLAN Disable WLAN	
Monitoring >	Number of WLANs selected : 0	
	Add WLAN	×
	General Security Advanced	
C Licensing	Layer2 Layer3 AAA	
X Troubleshooting	Layer 2 Security Mode None Lobby Admin Access	
	MAC Filtering Over the DS	
	OWE Transition Mode Reassociation Timeout 20	
	Authorization List*	
	Cancel	

在外部WLC上创建策略配置文件和策略标记

转到外部WLC Web UI。

要创建策略配置文件,请转到Configuration>Tags & Profiles>Policy>+Add

锚定时,必须使用中央交换。

Cisco Cataly	st 9800-L Wireless Contr	roller		
Q Search Menu Items	Configuration • > Tags & Pro	files > Policy		
🔜 Dashboard	+ Add × Delete			
Monitoring >	Status v Policy Profile I	Name		 Description
A	dd Policy Profile			×
Configuration >	General Access Policies	QOS and AVC Mobility	Advanced	
Administration				
C Licensing	A Configurin	ig in enabled state will result in loss o	of connectivity for clients associated with	this profile.
X Troubleshooting	Name*	CLUS-Policy-Profile	WLAN Switching Policy	
	Description	Policy Profile for CLUS	Central Switching	
	Status		Central Authentication	
	Passive Client	DISABLED	Central DHCP	
	Encrypted Traffic Analytics	DISABLED	Central Association	
	CTS Policy		Flex NAT/PAT	DISABLED
	Inline Tagging			
	SGACL Enforcement			
	Default SGT	2-65519		
	Cancel			Apply to Device

在"高级"选项卡上,AAA覆盖和RADIUS NAC对于CWA是必需的。如果选择创建会计方法列表,您 也可以在此处应用该会计方法列表。

Q Search Menu Items	ration * > Tags & Pro	ofiles > Policy				
📰 Dashboard 🛛 🕂 🗛	dd X Delete					
C Monitoring	Status V Policy Profile	Name			~	Description
Add Poli	cy Profile					×
General	Access Policies	QOS and AVC	Mobility Ad	vanced		
(O) Administration > WLAN	Timeout			Fabric Profile	Search or Select	V
C Licensing Session	Timeout (sec)	1800		mDNS Service Policy	Search or Select	•
M Troubleshooting	neout (sec)	300		Hotspot Server	Search or Select	•
Idle Thr	eshold (bytes)	0		User Private Network	c	
Client E.	xclusion Timeout (sec)	60		Status		
Guest L	AN Session Timeout			Drop Unicast		
DHCP				Umbrella		
IPv4 DH	ICP Required			Umbrella Parameter Map	Not Configured	▼ Clear
DHCP S	Server IP Address			Flex DHCP Option for DNS	ENABLED	
AAA Po	olicy			DNS Traffic Redirect	IGNORE	
Allow A	AA Override			WLAN Flex Policy		
NAC Sta	ate			VLAN Central Switching	g 🔲	
NAC Ty	rpe	RADIUS	•	Split MAC ACL	Search or Select	•
Policy N	lame	default-aaa-policy >	•	Air Time Fairness Pol	licies	
Account	ting List	CLUS-Acct-Meth-	ē 🗸	2.4 GHz Policy	Search or Select	•

在"移动"选项卡**上,不**选中"导出锚点"复选框,而是将锚点WLC添加到锚点列表。确保点击"应用到 设备"。 提醒一下,这假定您已在两个控制器之间建立移动隧道

Cisco Cata	lyst 9800-L Wireless Conti	roller		
Q. Search Monultome	Configuration * > Tags & Pro	Nes * > Policy		
Dashboard	+ Add × Delete			
Monitoring	Add Policy Profile			×
Configuration	General Access Policies	QOS and AVC Mobility	Advanced	
Administration >	Mobility Anchors			
C Licensing	Export Anchor			
Troubleshooting	Static IP Mobility Adding Mobility Anchors will cause the disable and may result in loss of com Drag and Drop/double click/click or	DISABLED a enabled WLANs to momentarily ectivity for some clients. In the arrow to add/remove Anchor	ra	
	Available (0)	Selected (1)		
	Anchor IP	Anchor IP	Anchor Priority	
	No anchors available	192.168.160.	18 Primary (1)	• *
	To Cancel			Apply to Device

要使AP使用此策略配置文件,您需要创建策略标记并将其应用到您希望使用的AP。

要创建策略标记,请转至Configuration>Tags & Profiles>Tags?Policy>+Add

Cisco Cata	alyst 9800-L Wireles	ss Controller		
Q Search Menu Items	Configuration > Ta	ags & Profiles > Tags		
🚃 Dashboard	Policy Site F	RF AP		
Monitoring >	+ Add ×			
Configuration	Policy Tag Na	ime		
	Add Policy Tag			×
C Administration >	Name*	CLUS-Policy-Tag		
C Licensing	Description	Policy Tag for CLUS		
X Troubleshooting	VUAN-POLIC	Y Maps: 0		
	+ Add × De	lete		
	WLAN Profile		V Policy Profile	~
		10 🔻 items per page		No items to display
	Map WLAN and Pol	licy		
	WLAN Profile*	CLUS-WLAN-Name 🔻	Policy Profile*	CLUS-Policy-Profile
		×		
	RLAN-POLICY	′ Maps: 0		
	Cancel			Apply to Device

要同时将其添加到多个AP,请转至**Configuration>Wireless Setup>Advanced>Start Now**。点击"标 记AP"旁的项目符号栏,将标记添加到您选择的AP。

¢	alialia cisco	Cisco Cata	alyst 9800-L Wire	eless Controller								
٩	Search Menu Ite	ms	Configuration * >	Wireless Setup *	> Ad	vance	d					
	Dashboard		Start			*	+	- Tag APs				
	Monitoring			Tags & Profiles			Numb Selec	per of APs: 3 ted Number of APs: 3				
Z			0	WLAN Profile				AP Name v	AP Model ~	AP MAC ~	AP ~ Mode	AS
	Administratio		0	Policy Profile				Jays2800	AIR-AP2802I- B-K9	002a.10f3.6b60	Local	E
~ ~			0	Policy Tag 🛛 🥥				Jays3800	AIR-AP3802I- B-K9	70b3.1755.0520	Local	E
G	Licensing							AP0062.ec20.122c	AIR-CAP2702I- B-K9	cc16.7e6c.3cf0	Local	D
X	Troubleshoot		0	AP Join Profile			M	∢ 1 ▶	10 🔻 items per j			
			0	Flex Profile			Tag	APs			3	¢
				Site Tag			Та	igs				
			9				Po	licy CLUS	-Policy-Tag 🗸			
			0	RF Profile			Sit	e Searc	h or Select 🔻			
			0	RF Tag 🛛 🥏			RF	Searc	h or Select 🔻			
				Apply			Ch	anging AP Tag(s) will	cause associated A	P(s) to reconnect		
			6	Tag APs	Þ)	0	Cancel			to Device)
			Done									

在锚点WLC上创建策略配置文件

转到锚点WLC Web UI。在锚点9800上的Policy Profile(策略配置文件)下**Configuration(配置)> Tags & Profiles(标记 和配置文件)> Tags(标记)> Policy(策略)>+Add(添加)**。确保这与在外部创建的策略配置文件匹配,但移动选项卡 和记帐列表除外。

在此,您不添加锚点,但是您确实选中了"导出锚点"复选框。请勿在此处添加会计列表。提醒一下,这假定您已在两个控 制器之间建立移动隧道

注意:没有理由将此配置文件与策略标记中的WLAN关联。如果您这样做,会造成问题。如果要对此WLC上的AP使用相同 的WLAN,请为其创建另一个策略配置文件。

Cisco Catalyst 9800-L Wireless Controller								
Q Search Menu Items Configuration * > Tags & Profiles * >	Policy							
Dashboard + Add × Delete								
Monitoring Add Policy Profile		×						
General Access Policies QOS and Configuration	d AVC Mobility Advanced							
Administration Mobility Anchors								
C Licensing								
X Troubleshooting Adding Mobility Anchors will cause the enabled V disable and may result in loss of connectivity for Drag and Drop/double click/click on the arrow	Static IP Mobility DISABLED Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.							
Available (1)	Selected (0)							
Anchor IP	Anchor IP Anchor Priority	_						
▲ 192.168.160.16	Anchors not assigned							
Cancel		Apply to Device						

在两个9800上重定向ACL配置

接下来,您需要在两个9800上创建重定向ACL配置。外部上的条目无关紧要,因为它将是将ACL应用于流量的锚点WLC。 唯一的要求是它在那里,并有一些入口。锚点上的条目必须"拒绝"访问端口8443上的ISE,并"允许"其他所有内容。此 ACL仅应用于从客户端"传入"的流量,因此不需要返回流量的规则。DHCP和DNS将在ACL中没有条目时通过。

Cisco Cata	alyst 9800-L Wireless Co	ontroller			Welcome admin
Q Search Menu Items	Configuration > Security	· > ACL			
Dashboard	+ Add × Delete Add ACL Setup	Associate Interfaces			×
Monitoring >	ACL Name*	CLUS-ACL	ACL Type	IPv4 Extended	
Configuration	Rules				
Administration	Sequence*		Action	permit 🔻	
© Licensing	Source Type	any 🔻			
💥 Troubleshooting	Destination Type	any 🔻			
	Protocol	ahp 🔻			
	Log	0	DSCP	None	
	+ Add × Delete				
	Sequence ~ Action	 Source < Source < Wildcard 	Destination V IP Vildcard V	Protocol v Port	Destination ~ Port DSCP ~ Log ~
	10 deny	any	192.168.160.99	tcp None	eq 8443 None Disabled
	100 permit	any	any	ip None	None None Disabled
		10 🔻 items per page			1 - 2 of 2 items
	Cancel				Apply to Device

配置ISE

最后一步是为CWA配置ISE。此门户有大量选项,但此示例将坚持基本操作,并使用默认自注册访 客门户。

在ISE上,您需要创建授权配置文件、使用身份验证策略设置的策略和使用授权配置文件的授权策略,将9800(外部)作为网络设备添加到ISE,并创建用户名和密码以登录网络。

要创建授权配置文件,请转到Policy>Policy Elements>Authorization>Results>Authorization Profiles>,然后单击Add。确保返回的访问类型为"access_accept",然后设置要发回的AVP(属性 — 值对)。对于CWA,重定向ACL和重定向URL是必需的,但您也可以发送回VLAN ID和会话超时 等内容。ACL名称必须与外部和锚点9800上重定向ACL的名称匹配。

$\epsilon \rightarrow C$ A Not secure 19	2.168.160.99/admin/#policy/policy_elements/policy_elements_permissions/policy_elements_permissions_authorization/policy_elements_permissions/policy_elements_permissions_authorization/policy_elements_permissions/policy_elements_permissions/policy_elements_permissions/policy_elements_permissions_authorization/policy_elements_permissions/policy_elements_permissions/policy_elements_permissions/policy_elements_permissions/policy_elements_permissions/policy_elements_permissions_authorization/policy_elements_permissions/pol
dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture Cl	ent Provisioning Policy Elements
Dictionaries Conditions Result	
Authentication Authorization Authorization Profiles Downloadable ACLs Profiling Posture Client Provisioning	Authorization Profiles > test Authorization Profile * Name CLUS-AuthZ-Profile-ISE Description * Access Type ACCESS_ACCEPT Network Device Profile Gence Cisco
	Passive identity fracking () Common Tasks Voice Domain Permission Web Redirection (CWA, MDM, NSP, CPP) () Centralized Web Auth (cv) ACL CLUS-ACL Value Self-Registered Guest Portal (cv)

然后,您需要配置一种方法,将刚创建的授权配置文件应用到通过CWA的客户端。为此,一种方法 是创建策略集,在使用MAB时绕过身份验证,并在使用在被叫站ID中发送的SSID时应用授权配置文 件。同样,有很多方法可以做到这一点,所以如果你需要更具体或更安全的东西,那么,这只是最 简单的方法。

要创建策略集,请转至**Policy>Policy Sets**,然后按屏幕左侧的+按钮。将新策略集命名,并确保其 设置为"默认网络访问"或允许MAB的"处理主机查找"的任何允许的协议列表(以检查允许的协议列表 ,请转至Policy>Policy Elements>Results>Authentication>Allowed Protocols)。 现在,在您创建

的新策略集中间点击该+号。

ultrute identity Services Engine Home + Context Visibility + Operations	Policy Administration Work Centers	License Warning 🔺 🔍 🔍 🔘 🔿
Policy Sets Profiling Posture Client Provisioning + Policy Elements		Click here to do visibility setup Do not show this again.
Policy Sets		ResetAll Hitcounts Reset Save
+ Status Policy Set Name Description	Conditions	Allowed Protocols / Server Sequence Hits Actions View
Search		
O <u>CLUS-CWA-Policy-Set</u>	+	Default Network Access 🔹 🕈 🔶 🗲
Default Default Default		Default Network Access * * + 0 🌣 🕨
		Reset Save

对于每次在ISE中使用MAB时的此策略集,它将通过此策略集。之后,您可以对被叫站ID制定匹配 的授权策略,以便根据所使用的WLAN应用不同的结果。此流程可以定制,您可以进行许多匹配。

Library	E	ditor		
mab ♥ 및 □ ▲ ● 무 및 문 ፬ 2 1		Wireless_MAB Set to 'Is not'		<i>(</i>)
Wired_MAB	٦			
Wireless_MAB	(i)		+ New AND OR	

在策略集内,创建策略。身份验证策略在MAB上可以再次匹配,但您需要更改ID存储以使用"内部终 端",并需要更改选项以继续进行身份验证失败和找不到用户。

Polcy Sets Profiling Posture Client Provisioning + Polcy Elements	Click here to do visibility setup Do not show this again.	×
Policy Sets → CLUS-CWA-Policy-Set	ResetAll Hitcounts Reset Save	e
Status Policy Set Name Description Conditions	Allowed Protocols / Server Sequence Hit	ts
Beach		
CLUS-CWA-Policy-Set	Default Network Access * * + 0)
▼ Authentication Policy (2)		
+ Status Rule Name Conditions	Use Hits Action	15
Cause MAR Condition	Internal Endpoints	
⊘ Default	Al_User_ID_Stores * * > Options 0	
Authorization Policy - Local Exceptions		
Authorization Policy - Global Exceptions		
Authorization Policy (1)		

设置身份验证策略后,您需要在授权策略中创建两个规则。此策略读起来像ACL,因此顺序需要在 顶部设置身份验证后规则,在底部设置身份验证前规则。后身份验证规则将匹配已通过访客流的用 户。也就是说,如果他们已经登录,他们会遵守这条规则,然后停止。如果他们尚未登录,则继续 从列表中按下预身份验证规则获取重定向。最好将授权策略规则与以SSID结尾的被叫站点ID进行匹 配,以便仅命中配置为这样做的WLAN。

Policy	Sets +	CLUS-CWA-Policy-Set							ResetAll Hitcou	ants
	Status	Policy Set Name	Descrip	otion	Con	ditions			Allowed Protocols	s / Server 8
Search										
	0	CLUS-CWA-Policy-Set				Wireless_MAB			Default Network A	ccess
> Auth	nentication	n Policy (2)								
> Auth	orization	Policy - Local Exceptions								
> Auth	orization	Policy - Global Exceptions								
∨ Auth	norization	Policy (4)								
+ Searc	Status	Rule Name	Cond	itions			Results Profiles	Se	ecurity Groups	
ſ	0	Post-CWA	AND	E Network Acces	s-UseCa Station-I	ISE EQUALS Quest Flow D ENDS_WITH CLUS-SSID	CLUS-Post-Auth	+	Select from list	- +
	Ø	MAB on WLAN	AND	Radius-Called	Station-I	D ENDS_WITH CLUS-SSID	CLUS-Auth2-Profile-ISE	+	Select from list	• +
	Ø	Flex AuthZ	₽	Radius Called-Station-II	ENDS	WITH FLEX-CWA	CLUS-Flex_CWA	+	Select from list	- +
	ø	Default					× DenyAccess	+ :	Select from list	• +

配置策略集后,您需要向ISE告知9800(外部),以便ISE信任它作为身份验证器。这可以在 Admin>Network Resources>**Network Device>**+中完成。您需要为其命名,设置IP地址(在本例中 为整个管理子网),启用RADIUS,并设置共享密钥。ISE上的共享密钥必须与9800上的共享密钥 匹配,否则此过程将失败。添加配置后,按"提交"按钮保存配置。

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	
System Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC	
Network Devices Network Device	Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services	
Network Device Default Device Device Security Settings	Network Devices List > JAysNet Network Devices Name CLUS_Net-Device Description	
	IP Address IP: 192.168.160.0 (24)	
	* Device Profile 🗰 Cisco 💌 🕀 Model Name 🔍 Software Version 🖳	
	Location All Locations Set To Default	
	IPSEC No Set To Default	
	All Device Type All Device Types	
	RADIUS Authentication Settings	
	RADIUS UDP Settings	
	Protocol RADIUS Shared Secret Show Show	
	CoA Port 1700 Set To Default	
	RADIUS DTLS Settings (j)	

最后,您需要将客户端将要输入的用户名和密码添加到登录页面,以验证他们应该具有网络访问权限。这在Admin>Identity Management>**Identity>Users>+Add下完成,并**确保在添加后点击提交。 与ISE的其他所有功能一样,这是可定制的,不必是本地存储的用户,但是,这是最简单的配置。

cisco lo	dentity Service	s Engine	Home +	Context Visibility	 Operations 	Policy	✓ Admini	istration 🔷 Wo	rk Centers	
Syste	em 🔽 Identity I	Vanagement	Network Reso	ources + Devic	e Portal Manageme	ent pxGrid	Services	Feed Service	Threat Centric NAC	
✓Identit	ties Groups	External Identit	y Sources Id	lentity Source Se	quences • Settin	gs				
		G	Maharah							
Users]		Network Acc	ess Users List >	New Network Acce	ss User				
Latest Ma	anual Network So	an Results	• Netwo	TR ALLESS USE	<u> </u>					
			* Name	CLUS-User	<u> </u>					
			Status	Enabled •						
			Email							
			▼ Pass	words						
			Passwo	ord Type: Inter	nal Users	•				
				Pass	word		Re-Enter Pa	assword		
			* Login	Password			•••••		Generate Password	1
			Enable	Password		`			Generate Password	i
			▼ User	Information						
			First Na	ame						
			Last Na	ame						
			▼ Acco	unt Options						
				Des	cription					
			Change	e password on ne	kt login					
			Accord	unt Disable Po	licy					
			🗆 Di	sable account if d	ate exceeds 2020)-07-17		(yyyy-mm-do	1)	
			▼ User	Groups						
			Select	an item	0 -					
			Submit	Cancel						

配置锚定到AireOS WLC的Catalyst 9800



Catalyst 9800外部配置

按照与前面讨论的步骤操作,跳过"在锚点WLC上创建策略配置文件"部分。

锚点AireOS WLC上的AAA配置

通过转到Security>AAA>RADIUS>Authentication>New,将服务器**添加到WLC中**。添加服务器IP地 址、共享密钥和CoA支持。

ı. cısco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MANAGEMENT COMMAND	s help	EEEDBACK	Sage Configuration Ping Logout Befree A Hom
Security	RADIUS Authentication Serve	175			Apply New
AAA General Catherine Constance Fallback DNS DNS	Auth Called Station ID Type AP a Use AES Key Wrap C (Ore MAC Delimiter Hype Framed MTU 100 Network Tunnel User Management Proxy	LC Address: SSID upned for FIPS customers and requires a key wrap compliant RA ten Server Server Index Address(Ipv4/Ipv6) Port IPSec Sta	DUS server) nin tus		
cisco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MANAGEMENT COMMAND	s held	<u>FEEDBACK</u>	Sage Configuration Bing Logout Befree A Hom
Security	RADIUS Authentication Serve	rs > New			< Back Apply
AAA General General Accounting Accounting Pallback DMS DMS DMS DMS DMS DMS Local Net Vern MAC/Fitning Vert Login Pholose I Local EAP Advanced EAP I Advanced EAP Derivity Order Derivity Order Control Lists Witneless Protection Pholes I Witneless Protection I Web Auth	Server Index (Priority) Server Index (Priority) Shared Secret Format Shared Secret Apply Cisco ISE Default settings Key Wrap Port Number Server Status Support for CoA Server Timeout Network User Hanagement Retransmit Timeout Turnel Proxy PAC Provisioning IPSec	v 152.166.160.99 AGCT Cosigned for FIPS customers and requires a key wrap co Cosigned ov Crabled v Crabled v S seconds S secon	mpliant RADIU	5 server)	

AireOS WLC上的WLAN配置

要创建WLAN,请转至WLANs>Create New>Go。

配置配置文件名称、WLAN ID和SSID,然后点击"应用"。

،،ا،،،ا،، cısco			WIRELESS SECU	RITY M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	
WLANs	WLANs							
VLANS	Current Filter:	None	[Change Filter] [Clea	r Filter]				Create New 🗸 Go
Advanced	U WLAN ID	Type Profile Name W	LAN SSID Admin S	atus Security Policies				
IIIIIII CISCO MONITOR	WLANS CONTROLLER V	WIRELESS SECURITY MANAGEM	ENT COMMANDS HELP EF	EDBACK				Saye Configuration Eing Logout Befresh
WLANs WLANs	New							< Back Apply
✓ WLANS WLANS Advanced Type Profile N SSID ID	me CLUS-WI CLUS-SS 1	▼] VLAN-Name SSDI						

这会将您带到WLAN配置。在"常规"选项卡上,如果您不打算将ISE配置为在AVP中发送接口,您可 以添加希望客户端使用的接口。然后转到**Security>Layer2**选项卡,匹配您在9800上使用的"Layer 2 Security"配置并启用"MAC Filtering"。



现在转到Security>**AAA Servers**选项卡,将ISE服务器设置为"Authentication Servers"。 **请勿为**"记 帐服务器"设置任何内容。 取消选中"启用"(Enable)复选框以进行记账。

ahaha		Sage Configurate	ion Eing	Logout Befres
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMEN	AT COMMANDS HELP EEEDBACK		🔒 Home
WLANs	WLANs > Edit 'CLUS-WLAN-Name'		< Back	Apply
VILANS	General Security QoS Policy-Mapping Advanced			
Advanced	Layer 2 Layer 3 AAA Servers			^
	Select AAA servers below to override use of default servers on this WLAN RADIUS Server RADIUS Server Overantia interfaceBeabled Apply Caco ISE Default SettingBeabled Server 3 MoneBeabled Server 4 NoneBeabled RADIUS Server 6 NoneBeabled	9 9 9 9 9	Î	

在WLAN配置中,切换到"高级"选项卡并启用"允许AAA覆盖",并将"NAC状态"更改为"ISE NAC"

սիսիս					Logout Befresh
CISCO	MONITOR WLANS CONTROLLER W	IRELESS SECURITY MANAGEMENT COMMANDS	HELP FEEDBACK		A Home
WLANs	WLANs > Edit 'CLUS-WLAN-Nam	re"		< 8ack	Αρρίγ
VLANS	General Security QoS Po	licy-Mapping Advanced			
viLos	Allow AAA Override Coverage Hole Detection Enable Session Timeout Ainonet IE Diagnostic Channel M Override Interface ACL Lawey? Adl URL ACL P2P Blocking Action	C traited C traited C traited C traited C traited D traited	DHCP DHCP Server DHCP Addr. Assignment Required OFAP Split Tunnel Protection (IFP) MPP Client Protection (I Optional Optional Optional Optional Optional Optional Optional Optional Optional Optional Optional Optional Optional Optional Optional		Î
	Client Exclusion * Maximum Allowed Clients [#] Static IP Tunneling [#] Wi-R Direct Clients Policy Maximum Allowed Clients Per AP Radio Cliear HotSpot Configuration		DTHP Period (in beacon intervals) 802.11a/n (1 - 255) 802.11b/g/n (1 - 255) FAC NAC State Load Balancing and Band Select		

最后一件事就是把它固定在自己身上。为此,请返回WLANs页面,将鼠标悬停在WLAN>Mobility Anchors右侧的蓝色框上。将"交换机IP地址(锚点)"设置为本地,然后按"移动锚点创建"按钮。然 后,它应显示优先级为0的本地锚点。

،،ا،،،ا،، cısco		MONITOR	<u>W</u> LANs	CONTROLLE	R WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK	_		
WLANs		WLANs											
VLANs		Current Filt	ter: No	one	[Change Filt	er] [Clear Filter	1				Create New	♥ Go]
Advanced		U WLAN I	ID Type	Pro	ile Name		WLAN SS	ID		Admin Status	Security Policies		
			WLAN	N CLU	S-WLAN-Name		CLUS-SSIC)		Enabled	MAC Filtering		Pamara
													Mobility Anchors
													S02.110 Foreign Many
													Service
													Advertisements Hotspot 2.0
WLANs	Mobility	Anchors											< Back
* WLANS													
WLANs Advanced	WLAN SS	ID CLUS-SSID											
	Switch IP local	Address (Anchor)								Up Data Path	Control Path up	O	
	Mobility	Anchor Create											
	Switch I	P Address (And	nor) [192.168.160.18 ¥									
	Driority		ſ	19									
	-nonty-		U.										
	Foot Not	es											

在AireOS WLC上重定向ACL

这是AireOS WLC上需要的最终配置。要创建重定向ACL,请转到**Security>Access Control** Lists>Access Control Lists>New。输入ACL名称(这必须与AVP中发送的内容匹配)并点击"应用 "。

uluulu cisco	sonitor wilang controller wireless security management commands help eeedback	ve Configuration Bing Logout Befresh n Home
Security	Access Control Lists > New	< Back Apply
✓ AAA General ✓ RADIUS Authentication Accounting Falback DNS Downloaded AVP ► TACACS+	Access Control List Name (LUS-ACL) ACL Type	

现在,单击您刚创建的ACL的名称。单击"添加新规则"按钮。与9800控制器不同,在AireOS WLC上,您为允许到达ISE的流量配置允许语句,而无需重定向。 默认情况下允许DHCP和DNS。

ılıılı cısco	MONI	TOR	WLAN		۲ ۱	WIRELESS	SECURIT		MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK		Sa <u>v</u> e Co	nfiguration	<u>P</u> ing	Logout <u>R</u> efr
Security	Acc	ess C	ontrol	Lists > Edit											< Back	A	dd New Rule
AAA General RADIUS	Gene	eral															
Authentication Accounting Fallback DNS	Acces Deny	s List N Counte	ame rs	CLUS-ACL 5													
Downloaded AVP	Seq	Actio	on S	ource IP/Mask		Destina	tion IP/Ma	sk	Protocol	Source Por	t	Dest Port	DSCP	Direction	Number	of Hits	
LDAP Local Net Users	Ŧ	Perm	it 0	.0.0.0 .0.0.0	/	192.168	.160.99	/	тср	Any		8443	Any	Any	273		
MAC Filtering Disabled Clients User Login Policies	2	Perm	it 1 2	92.168.160.99 55.255.255.255	/	0.0.0.0 0.0.0.0		/	ТСР	8443		Any	Any	Any	566		
AP Policies Password Policies																	
Local EAP																	
Advanced EAP																	
Priority Order																	
Certificate																	
▼ Access Control Lists																	



Access Control Lists CPU Access Control

CWAISE

ISE9800ISE

Policy>Policy Elements>Authorization>Results>Authorization Profiles>+Add"access_accept"AVP — CWAACLURLVLAN ID ACLWLCACL

🗧 🔶 C 🔺 Not secure | 192.168.160.99/admin/#policy/policy_elements/policy_elements_permissions/policy_elements_permissions/authorization/policy_element

Identity Services Engine	Home	Operations	- Policy	Administration	• Work Centers	
Policy Sets Profiling Posture Cl	lient Provisioning 🔽 Policy Elem	ients				
Dictionaries + Conditions - Result	IS					
Authentication	Authorization Profiles > test					
- Authorization	* Name	CLUS-AuthZ-Profile-IS	E]		
Authorization Profiles Downloadable ACLs	* Access Type	ACCESS_ACCEPT	×)		A
▶ Profiling	Network Device Profile	🗱 Cisco 🔻 🕀				
▶ Posture	Service Template	0				
Client Provisioning	Track Movement					
	Passive Identity Tracking	1				
	▼ Common Tasks					
	Voice Domain Permissio	on				
	Web Redirection (CWA)	, MDM, NSP, CPP) (D			
	Centralized Web Auth	•	ACL	CLUS-ACL	Val	lue Self-Registered Guest Portal (c 🗸

CWAMABIDSSID

Policy>Policy Set+""MAB""Policy>Policy Elements>Results>Authentication>Allowed Protocols +

utude Identity Services Engine Home + Context Visibility + Op	rations Policy + Administration + Work Centers	License Warning 🔺 🔍 😐 🔿 🔿
Policy Sets Profiling Posture Client Provisioning + Policy Elements		Click here to do visibility setup Do not show this again.
Policy Sets		ResetAll Hitcounts Reset Save
+ Status Policy Set Name Description	Conditions	Allowed Protocols / Server Sequence Hits Actions View
Search		
O CLUS CWA-Policy-Set	+	Default Network Access 🔹 👻 +
Default Default Default		Default Network Access ** + 0 🗘 🕨

ISEMABIDWLAN



MABID""

Policy Sets Profiling Posture Client Provisioning + Policy Elements		Click here to do visibility setup Do not show this again.	×
Policy Sets → CLUS-CWA-Policy-Set		ResetAll Hitcounts Reset S	Save
Status Policy Set Name Description	Conditions	Allowed Protocols / Server Sequence	Hits
Search			
CLUS-CWA-Policy-Set	Wireless_MAB	Default Network Access 🔹 👻 🛨	0
▲ Authentication Policy (2)			
+ Status Rule Name Conditions		Use Hits Act	tions
CUUS MAB Condition		Internat Endpoints	¢
Default		All_User_JD_Stores * * Options	¢
Authorization Policy - Local Exceptions Authorization Policy - Clobal Exceptions			
Authorization Policy (1)			

ACLSSIDIDWLAN

Policy Sets + CLUS-CWA-Policy-Set

Policy	Sets +	CLUS-GWA-Policy-Set								ResetAll H	itcounts
	Status	Policy Set Name	Descrip	otion	Con	ditions				Allowed Prot	ocols / Server S
Search											
	0	CLUS-CWA-Policy-Set				Wireless_MAB				Default Netw	ork Access
> Auth	entication	Policy (2)									
> Auth	orization	Policy - Local Exceptions									
> Auth	orization	Policy - Global Exceptions									
✓ Auth	orization	Policy (4)									
٠	Status	Rule Name	Condi	itions				Results Profiles	S	ecurity Groups	
Searc	h										
	Ø	Post-CWA	AND	B Network Access Image: Called Control Radius Called Control	s-UseCa Station-	se EQUALS Guest Flow D ENDS_WITH CLUS-SSID		CLUS-Post-Auth	+	Select from list	• +
	ø	MAB on WLAN	AND	Radius-Called	Station-	D ENDS_WITH CLUS-SSID		CLUS-AuthZ-Profile-ISE	+	Select from list	• +
	0	Flex AuthZ	₽	Radius Called-Station-II	ENDS	WITH FLEX-CWA		× CLUS-Flex_CWA	+	Select from list	- +
	0	Default						× DenyAccess	+	Select from list	- +

ISE9800ISEAdmin>Network Resources>Network Device>+.IPRADIUSISE9800""

dentity Services Engine	Home Context Vis	ibility	Policy Adn	ninistration 🔷 W	/ork Centers		
System Identity Management	• Network Resources	Device Portal Management	pxGrid Services	Feed Service	Threat Centric N	IAC	
Network Devices Network Device Gi	roups Network Device	Profiles External RADIUS	Servers RADIUS	Server Sequences	NAC Managers	External MDM	Location Services
Network Devices Network Devices Default Device Device Security Settings	Network Devices List > Network Devices List > IP Address IP Address * Network Device Location All IPSEC No Device Type All IV RADIUS Auth RADIUS UD RADIUS UD	Profiles External RADIUS JAysNet * Name CLUX Description * IP : 192.168.160 * Device Profile @@ C Model Name Software Version Group Locations Si Device Types Si use Seco LS Settings	Servers RADIUS	RADIUS () () () () () () () () () ()	24	External MDM	Location Services
	1000301	La serunda (I)					

Admin>Identity Management>Identity>Users>+Add ISE

cisco	Identity	Service	s Engine	Home	Context Visibilit	y I Operatio	ns + Policy	✓ Adminis	stration > We	ork Centers
► Sys	stem [Identity I 	/lanagement	Network F	esources 🔹 🕨 De	vice Portal Manag	ement pxGrid S	Services •	Feed Service	Threat Centric NAC
▼Ide	entities	Groups	External Identi	ty Sources	Identity Source S	Sequences 🔹 🕨 S	ettings			
Users Latest	Manual N	Groups	External Identi	ty Sources Network Net Net Net Stat Em Pas (* Lo	Identity Source S Access Users List work Access User Ine CLUS-User US CLUS-User US Enabled ail sswords sword Type: In Pa gin Password •	Sequences > S > New Network / ser ternal Users ssword	Access User	Re-Enter Pa:	ssword	Generate Password (j)
				Ena	ble Password					Generate Password (i)
				▼ Us	er Information					
				Firs	t Name					
				Las	t Name					
				▼ Ac	count Options					
					D	escription				
				Cha	inge password on	next login 🛛				
				▼ Ac	count Disable I	Policy				
					Disable account i	f date exceeds	2020-07-17		(yyyy-mm-d	ld)
				▼ Us	er Groups					
				ii Se	lect an item	0				
				Subm	it Cancel					

当AireOS WLC是外部WLC,而Catalyst 9800是锚时,配置的差异

如果希望AireOs WLC成为外部控制器,则配置与之前相同,只有两个差异。

- 1. AAA记帐从不在锚点上完成,因此9800将没有记帐方法列表,并且AireOS WLC将启用记帐并 指向ISE。
- 2. AireOS需要定位于9800,而不是自身。在策略配置文件中,9800不会选择锚点,但会选中"导 出锚点"框。
- 3. 请注意,当AireOS WLC将客户端导出到9800时,它只发送WLAN配置文件名称(WLAN Profile Name)。因此,9800将将从AireOS发送的WLAN配置文件名称应用到WLAN配置文件名称和策 略配置文件名称。也就是说,当从AireOS WLC锚定到9800 WLC时,两个WLC上的WLAN配 置文件名称和9800上的策略配置文件名称必须全部匹配。

验证

要验证9800 WLC上的配置,请运行以下命令

Show Run | section aaa|radius

• WLAN

Show wlan id <wlan id>

•策略配置文件

Show wireless profile policy detailed <profile name>

• 策略标记

Show wireless tag policy detailed <policy tag name>

ACL

Show IP access-list <ACL name>

• 验证移动是否与锚点一起启用

Show wireless mobility summary 要验证AireOS WLC上的配置,请运行以下命令

AAA

Show radius summary 注意:RFC3576是CoA配置

• WLAN

Show WLAN <wlan id>

ACL

Show acl detailed <acl name>

• 验证移动性是否与外部

Show mobility summary

故障排除

根据客户端在进程中停止的点,故障排除看起来有所不同。例如,如果WLC从ISE在MAB上未收到 响应,则客户端将停滞在"Policy Manager State:关联",不会导出到锚点。在这种情况下,您只能对 外部进行故障排除,并可以收集RA跟踪和WLC和ISE之间流量的数据包捕获。另一个示例是MAB已 成功通过,但客户端未收到重定向。在这种情况下,您需要确保外国用户在AVP中收到重定向并将 其应用到客户端。您还需要检查锚点,以确保客户端具有正确的ACL。此故障排除范围不在此技术 文档的设计范围内(查看有关通用客户端故障排除指南的参考信息)。

有关9800 WLC上CWA故障排除的更多帮助,请参阅Cisco Live!演示DGTL-TSENT-404

Catalyst 9800故障排除信息

客户端详细信息

show wireless client mac-address 您应查看"策略管理器状态"、"会话管理器>身份验证方法"、"移动角色"。

您还可以在GUI中的Monitoring>Clients下找到此信息

嵌入式数据包捕获

命令从CLI启动#monitor capture <capture name>,然后在此之后显示选项。

在GUI中,转到Troubleshoot>Packet Capture>+Add

RadioActive跟踪

从CLI

debug wireless mac/ip

使用命令的no形式将其停止。这将记录到名为"ra_trace"的bootflash中的文件,然后记录客户端的 MAC或IP地址以及日期和时间。

在GUI中,转到Troubleshoot>Rabitic Trace>+Add。添加客户端的mac或ip地址,点击apply,然后 点击start。在您完成该过程几次后,停止跟踪,生成日志并将其下载到您的设备。

AireOS故障排除信息

客户端详细信息

在CLI中显示客户端详细信息

从GUI Monitor>Clients

从CLI调试

Debug client

Debug mobility handoff

Debug mobility config



使用9800控制器构建移动隧道

9800上的无线调试和日志收集