在AP上為PEAP或使用LSC的EAP-TLS配置 802.1X

目錄
<u>必要條件</u>
採用元件
<u>背景資訊</u>
網路圖表
設定
Windows Server 2016 SCEP CA
<u>配置證書模板和登錄檔</u>
<u>在9800上配置LSC</u>
AP LSC GUI配置步驟
AP LSC CLI配置步驟
AP LSC驗證
排除LSC調配故障
<u>使用LSC的AP有線802.1X身份驗證</u>
AP有線802.1x身份驗證配置步驟
AP有線802.1x身份驗證GUI配置
<u>AP有線802.1x身份驗證CLI配置</u>
AP有線802.1x身份驗證交換機配置
RADIUS伺服器憑證安裝
AP有線802.1x驗證驗證
<u>802.1X身份驗證故障排除</u>

簡介

本文檔介紹如何使用802.1X PEAP或EAP-TLS方法對交換機埠上的思科接入點進行身份驗證。

必要條件

需求

思科建議您瞭解以下主題:

- 無線控制器
- 存取點

- 交換器
- ISE伺服器
- 證書頒發機構。

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- 無線控制器:運行17.09.02的C9800-40-K9
- 接入點: C9117AXI-D
- 交換機:運行17.06.04的C9200L-24P-4G
- AAA伺服器:運行3.1.0.518的ISE-VM-K9
- 證書頒發機構: Windows Server 2016

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。

背景資訊

如果您希望存取點(AP)使用802.1X驗證其交換器連線埠,預設情況下,它們會使用不需要憑證的 EAP-FAST驗證通訊協定。如果您希望AP使用PEAP-mschapv2方法(在AP端使用憑證,但在 RADIUS端使用證書)或EAP-TLS方法(在兩端使用證書),您必須首先配置LSC。這是將受信任 /根證書調配到接入點的唯一方法(在EAP-TLS的情況下也是裝置證書)。AP無法執行PEAP並忽略 伺服器端驗證。本文檔首先介紹配置LSC,然後介紹配置802.1X端。

如果您希望PKI提供更好的安全性、控制證書頒發機構(CA)並在生成的證書上定義策略、限制和使用,請使用LSC。

若使用LSC,控制器會取得由CA頒發的憑證。AP不與CA伺服器直接通訊,但WLC代表加入的 AP請求證書。CA伺服器詳細資訊必須在控制器上配置並且必須可訪問。

控制器使用Simple Certificate Enrollment Protocol(SCEP)將裝置上生成的certReq轉發到CA,並再 次使用SCEP從CA獲取已簽名的證書。

SCEP是PKI客戶端和CA伺服器用於支援證書註冊和撤銷的證書管理協定。它廣泛使用在Cisco中 ,並且受許多CA伺服器的支援。在SCEP中,HTTP用作PKI消息的傳輸協定。SCEP的主要目標是 向網路裝置安全頒發證書。

網路圖表



設定

主要需要設定兩個專案:SCEP CA和9800 WLC。

Windows Server 2016 SCEP CA

本文檔介紹用於實驗的Windows Server SCEP CA的基本安裝。對於企業運營,必須安全且適當地 配置實際的生產級Windows CA。本節旨在幫助您在實驗室中對其進行測試,並從使此配置正常工 作所需的設定中獲得靈感。以下是步驟:

步驟1.安裝全新的Windows Server 2016案頭體驗。

步驟2.確保您的伺服器配置了靜態IP地址。

步驟3.安裝新的角色和服務,從Active Directory域服務和DNS伺服器開始。

🚖 Se	rver Manager			- 0 ×
<	🚵 Add Roles and Features Wizard		- 🗆 ×	age Tools View Help
	Select server roles		DESTINATION SERVER WIN-3E202T1QD0U	
i	Before You Begin	Select one or more roles to install on the selected server.		
	Installation Type	Roles	Description	
Ϊŝ	Server Selection Server Roles Features DNS Server AD DS Confirmation Results	 Active Directory Certificate Services Active Directory Domain Services Active Directory Federation Services Active Directory Rights Management Services Active Directory Rights Management Services Device Health Attestation DHCP Server DNS Server Fax Server Pile and Storage Services (1 of 12 installed) Host Guardian Services NultiPoint Services Print and Document Services Remote Access Remote Access Remote Desktop Services Volume Activation Services Web Server (IIS) Windows Deployment Services 	Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.	Hide
es.		< Previous Next	> Install Cancel	
		Events 1 Events Performance 5 Service BPA results Performance 1	es mance	
		BPA re	10/19/2022 11/26 AM	

Active Directory安裝

🝙 Se	erver Manager								- 0	\times
	🚡 Add Roles and Features Wizard			-		×	200	Tools	View	Help
	Installation progre	ESS View installation progress		DESTINA WIN-3	ATION SER E2O2T1Q	VER DOU		IOOIS	view	
5-3	Installation Type	 Feature installation 								
ا و ا م	Server Selection	Configuration required. Installation s	ucceeded on WIN-3E2O2T1QD0U.							
1	Features DNS Server AD DS Confirmation Results	Active Directory Domain Services Additional steps are required to make the Promote this server to a domain control DNS Server Group Policy Management Remote Server Administration Tools Role Administration Tools DNS Server Tools AD DS and AD LDS Tools Active Directory module for AD DS Tools You can close this wizard without int page again by clicking Notifications Export configuration settings	his machine a domain controller. Iller or Windows PowerShell errupting running tasks. View task pro in the command bar, and then Task Di	gress or otalis.	open thi	∧			Hide	2
		< P	revious Next > Clo	se	Canc	el				
		Events Services Performance BPA results	Events Services Performance BPA results				_			

AD安裝結束

步驟4.完成後,在「Promote this server to a domain controller(將此伺服器升級為域控制器)」上 按一下控制面板中的按鈕。

🚘 Server Manager			– 0 ×
Server M	1anager • Dashboard	- 🕲 🍢 Mai	anage Tools View Help
🛄 Dashboard	WELCOME TO SERVER MANAGE	Post-deployment Configuration Configuration Provide Configuration Provide Configuration	
Local Server All Servers		Services at WIN-3E2O2T1QDOU Promote this server to a domain controller	
i∎i AD DS	QUICK START	Feature installation	
■File and Storage Services ▷	3	Configuration required. Installation succeeded on WIN-3E2O2T1QD0U.	
	WHAT'S NEW 4	Task Details	
	E	Connect this converte cloud convices	

配置AD服務

步驟5.建立新林並選擇域名。

	-					
re-	Se	rve	r M	an	ag	er

(📥 Active Directory Domain Service	🛓 Active Directory Domain Services Configuration Wizard									
	Active Directory Domain Service	Select the deployment ope Add a domain controlle Add a new domain to a Add a new forest Specify the domain informa Root domain name:	ration r to an existing n existing forest ation for this op n	domain eration nydomain.loca		TA WIN-3	RGET SEL	X RVER QDOU			
		Function	< Previ	ous Next >	Insta	ill	Cance	el			
		Events		Evente							

選擇林名稱

步驟6.將Certificate Services角色新增到伺服器:

👝 Server Manager						-	- (J X
Ser Ser	ver Manager • Das	hboard -	· ③	I 🏲	Manage	Tools	View	Help
DashboardLocal Server	WELCOME TO SE	RVER MANAGER						
All Servers	Add Roles and Features Wizard				-		×	
AD DS	Solact conver role	c			DESTIN	IATION SERV	'ER	
File and Storage Set	r Select server role	5		WIN	1-3E2O2T1QD0U.r	nydomain.lo	cal	
	Before You Begin	Select one or more roles to install on the selected server.						
	Installation Type	Roles		Descript	ion			
	Server Selection Server Roles Features AD CS Role Services Confirmation	Active Directory Certificate Services Active Directory Domain Services (Installed) Active Directory Pederation Services Active Directory Lightweight Directory Services Active Directory Rights Management Services Device Health Attestation DHCP Server DNS Server (Installed)	^	Active Di (AD CS) i certificat role serv and man variety o	irectory Certific is used to creat ion authorities ices that allow age certificates f applications.	ate Service e and relate you to issu s used in a	es d le	de

🚔 Server Manager					-	- 6	i ×
Ser Ser	ver Manager • Dash	board •	☺ 🚩 м	lanage	Tools	View	Help
 Dashboard Local Server 	WELCOME TO SERV	/ER MANAGER					
All Servers	📥 Add Roles and Features Wizard			-		×	
 AD DS DNS File and Storage Ser 	Select role services	S Select the role services to install for Active Directory Certific	WIN-3E202	DESTINAT 2T1QD0U.myd	'ION SERVI domain.loc	ER tal	
	Installation Type	Role services	Description				
	Server Selection Server Roles Features AD CS Role Services Confirmation Results	Certification Authority Certificate Enrollment Policy Web Service Certificate Enrollment Web Service Certification Authority Web Enrollment Network Device Enrollment Service Online Responder	Certification Au to issue and m Multiple CAs ca public key infra	uthority (CA anage certi an be linked astructure.	l) is used ficates. d to form	na ic	le

僅新增證書頒發機構

步驟7.完成之後,配置證書頒發機構。

🚖 Server I	Manager				_	- 6) ×
\mathbf{E}	AD CS Configuration		-	▼ □ ×	age Tools	View	Help
III Da:	Role Services		DESTINATIO WIN-3E2O2TIQD0U.mydo	N SERVER main.local			
	Credentials Dele Cervices	Select Role Services to configure			- 0	×	
■。AD ■ AD ● DN ■ File	Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	 Certification Authority Certification Authority Web Enrollment Online Responder Network Device Enrollment Service Certificate Enrollment Web Service Certificate Enrollment Policy Web Service 			DESTINATION SERVE QD0U.mydomain.loc main.local.	R al	Je
		More about AD CS Server Roles					
		< Previous	Next > Configure	Cancel	ess or open this		

步驟8.選擇企業CA。



企業CA

步驟9.使其成為根CA。自Cisco IOS XE 17.6以來,LSC支援從屬CA。

🚖 Server I	Manager		_				
\mathbf{E}	AD CS Configuration		age Tools V	iew Help			
Da:	СА Туре	DESTINATION SERVER WIN-3E2O2T1QD0U.mydomain.local					
M AD M AD M DN File	Creventians Role Services Setup Type CA Type Private Key	When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.	DESTINATION SERVER QD0U.mydomain.local				
	Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Cryptography Root CA Root CAs are the first and may be the only CAs configured in a PKI hierarchy. Subordinate CA Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy. Orgress sults					
		Previous Next > Configure Cancel page again by clicking Notifications in the command bar, and then Task De Export configuration settings	ess or open this tails.				

選擇根CA

請務必將用於CA的帳戶設為IIS_IUSRS組的一部分。在本示例中,您使用管理員帳戶並轉到Active Directory使用者和電腦選單,將管理員使用者新增到IIS_IUSRS組中。

📥 Server Manager								- 0	\times
<u>ج</u> ے۔ Se	erver Manag	er • Dashbo	ard			· ③ 🖡	Manage Too	ls View I	Help
Image: Dashbor Image: Local Sector Image: All Server AD CS Image: AD CS <t< td=""><td>ve Directory Users and ction View Help Pre Directory Users and C aved Queries nydomain.local Builtin Computers Domain Controllers ForeignSecurityPrinc Managed Service Ac Users</td><td>Administrator Properti Remote control General Address Member Of Member of: Name Administrators Domain Admins Domain Users Enterprise Admins Group Policy Cre IIS_IUSRS Schema Admins Add F Primary group: Doc Set Primary Group OP</td><td>es Remote Desktop Account Profile Dial-in E Active Directory Dom mydomain Jocal/Built mydomain Jocal/User mydomain Jocal/User mydomain Jocal/User mydomain Jocal/User mydomain Jocal/User mydomain Jocal/User mydomain Jocal/User mydomain Jocal/User main Users There is no need You have Macinto applications. C</td><td>Services Profile Telephones invironment ain Services Folder s s s s to change Primary g sh clients or POSIX Apply </td><td>? × COM+ Organization Sessions proup unless compliant Help Next > Ults</td><td>Configure</td><td>× ¢</td><td>Hide</td><td></td></t<>	ve Directory Users and ction View Help Pre Directory Users and C aved Queries nydomain.local Builtin Computers Domain Controllers ForeignSecurityPrinc Managed Service Ac Users	Administrator Properti Remote control General Address Member Of Member of: Name Administrators Domain Admins Domain Users Enterprise Admins Group Policy Cre IIS_IUSRS Schema Admins Add F Primary group: Doc Set Primary Group OP	es Remote Desktop Account Profile Dial-in E Active Directory Dom mydomain Jocal/Built mydomain Jocal/User mydomain Jocal/User mydomain Jocal/User mydomain Jocal/User mydomain Jocal/User mydomain Jocal/User mydomain Jocal/User mydomain Jocal/User main Users There is no need You have Macinto applications. C	Services Profile Telephones invironment ain Services Folder s s s s to change Primary g sh clients or POSIX Apply	? × COM+ Organization Sessions proup unless compliant Help Next > Ults	Configure	× ¢	Hide	
:	🩋 🖬 🖥						^ फ़ॄ 4 <mark>∞</mark> 8	NG 10:47 PM EFR 10/19/2023	2

將管理員帳戶新增到IIS_USER組

步驟10.在正確的IIS組中擁有使用者後,新增角色和服務。然後將Online Responder和NDES服務新 增到您的認證機構。

o ×



安裝NDES和線上響應程式服務

📥 Server Manager

步驟11.完成後,配置這些服務。



安裝線上響應程式和NDES服務

步驟12.系統提示您選擇服務帳戶。這是您以前新增到IIS_IUSRS組的帳戶。



選擇已新增到IIS組的使用者

步驟13。這足以執行SCEP操作,但為了實現802.1X驗證,您還需要在RADIUS伺服器上安裝憑證 。因此,為方便起見,請安裝和配置Web註冊服務,以便在Windows伺服器上輕鬆複製和貼上 ISE證書請求。



安裝Web註冊服務

AD CS Configuration			_		×
Role Services		WIN-3	DESTINA BE2O2T1QD0U.my	ION SERV	/ER ocal
Credentials Role Services Confirmation Progress Results	 Select Role Services to configure Certification Authority Certification Authority Web Enrollment Online Responder Network Device Enrollment Service Certificate Enrollment Web Service Certificate Enrollment Policy Web Service 				
	More about AD CS Server Roles				
-	< Previous	Next >	Configure	Cancel	I

配置web註冊服務

步驟 14.您可以訪問<u>http://<serverip>/certsrv/mscep/mscep.dll</u> ,驗證SCEP<u>服務是否正常運行:</u>

0	Netwo	ork Dev	vice Enrollment Servic 🗙	+	_		X	
\leftarrow	\rightarrow	G	O No seguro 172	.16.80.8/certsrv/mscep/mscep.dll	☆	۲	:	
Network Device Enrollment Service								
Network Device Enrollment Service allows you to obtain certificates for routers or other network devices								

This URL is used by network devices to submit certificate requests.

To obtain an enrollment challenge password, go to the admin URL. By default, the admin URL is <u>http://Chuu-Win12/CertSrv/mscep_admin</u>

For more information see Using Network Device Enrollment Service.

using the Simple Certificate Enrollment Protocol (SCEP).

SCEP入口驗證

步驟 15.

預設情況下,Windows Server在Microsoft SCEP(MSCEP)註冊之前使用動態質詢密碼對客戶端和終 端請求進行身份驗證。這需要管理員帳戶瀏覽到Web GUI為每個請求生成按需密碼(密碼必須包含 在請求中)。控制器不能將此密碼包含在傳送給伺服器的請求中。要刪除此功能,需要修改 NDES伺服器上的登錄檔項:

開啟登錄檔編輯器,在開始選單中搜尋Regedit。

導航到Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP > EnforcePassword

將EnforcePassword值更改為0。如果它已經是0,則保留原樣。

۲. Contraction (Contraction)		Registry Editor		_ 🗆 X
File Edit View Favorites Help				
- MSCEP	^	Name	Туре	Data
— 📜 САТуре		(Default)	REG SZ	(value not set)
		8 EnforcePassword	REG_DWORD	0x00000000 (0)
EnforcePassword		(- · · · · · · · · · · · · · · · · · ·		
- OID	≡			
- Protect	_			
- Providers				
- Services				
Data Accord				
DataAccess				
Device Association Framework				
Dfra				2
DES				
DHCPMibAgent				
DirectDraw				
DirectInput				
DirectPlay8				
DirectPlayNATHelp	$\overline{}$			
<		<	111	>
Computer\HKEY_LOCAL_MACHINE\S	OFT	WARE\Microsoft\Crypt	ography\MSCEP\Enfor	cePassword

設定Enforcepassword值

配置證書模板和登錄檔

證書及其關聯金鑰可以在CA伺服器內的應用程式策略所定義的多個場景中用於不同的用途。應用策略儲存在證書的Extended Key Usage(EKU)欄位中。驗證器會分析此欄位,以驗證客戶端是否將其用於預期目的。要確保將正確的應用程式策略整合到WLC和AP證書,請建立正確的證書模板並將其對映到NDES登錄檔:

步驟 1.導航到開始>管理工具>證書頒發機構。

步驟 2.展開「CA伺服器」資料夾樹,按一下右鍵Certificate Templates資料夾並選擇Manage。

步驟 3.按一下右鍵Users證書模板,然後在上下文選單中選擇Duplicate Template。

步驟 4.定位至常規標籤,根據需要更改模板名稱和有效期,保留所有其它選項未選定。

⚠️ 注意:修改有效期時,請確保有效期不超過證書頒發機構的根證書有效性。

Properties of New Template

X

Subject Name	Sen	ver	Issuance R	equirements
Superseded Templa	tes	Exte	nsions	Security
Compatibility General	Request	Handling	Cryptography	Key Attestation
Template display name: 9800-LSC				
Template name:				
0000 200				
Validity period:] Active Dir	Renewa 6	veeks v	
Do not automatic Directory	ally reenro	oll if a dupli	cate certificate e	xists in Active
ОК	(Cancel	Apply	Help

步驟 5.定位至主題名稱標籤,確保已選擇請求中的「供應」。系統將顯示一個彈出視窗,指示使用 者不需要管理員批准即可簽署其證書,請選擇OK。

Properties of New Template								
Compatibility	General	Request	Handling	Cryptography	Key Attestation			
Supersec	ded Templa	ites	Extensions		Security			
Subject N	lame	Sen	ver	Issuance R	equirements			
Supply in	the reques	st.						
Supply in Use a renew	the reques subject info wal request	t mation fro s (*)	om existing	certificates for a	utoenrollment			

在請求中提供

步驟 6.導航到Extensions頁籤,然後選擇Application Policies選項,然後選擇Edit...按鈕。確保 Application Policies視窗中的Client Authentication;否則,選擇Add並新增它。

	Pro	perties	of New	Template	X			
Compatibility	General	Request	Handling	Cryptography	Key Attestation			
Subject N	lame	Ser	ver Issuance R		Requirements			
Supersec	ded Templa	tes	Exte	nsions	Security			
To modify an	To modify an extension, select it, and then click Edit.							
Extensions included in this template:								
Edit /	Applicati	on Poli	cies Exte	nsion X				
An application policy defines how a certificate can be used.								
Application p Client Author Encrypting Secure Ema	Application policies: Client Authentication Encrypting File System Secure Email							

驗證擴展

步驟 7.導航到Security選項卡,確保在Windows伺服器中啟用SCEP服務的步驟6中定義的服務帳戶 具有模板的完全控制許可權,然後選擇Apply和OK。

Properties of New Template

X

	Ciciliciai	Request	Handling	Cryptography	Key Attestation			
Subject I	Name	Sen	/er	Issuance R	equirements			
Superse	ded Templa	ates	Exte	insions	Security			
Group or use	er names:							
& Authen	ticated Use	118						
Administrator								
Se Domain	n Admins (C	HUU-DON	AIN\Dom	ain Admins)				
Se Domain	n Users (CH	IUU-DOM/	AIN\Domai	n Users)				
Enterpr	rise Admins	(CHUU-DO	JMAIN\En	terprise Admins)				
				Add	Permana			
				A00	Nemove			
Permiseione	for Administ	trator		Allow	Deov			
Cimissions		(I GLOI			Ceny			
				J				
Full Contro	ol			•				
Full Contro Read	ol			 ✓ 				
Full Contro Read Write	ol			✓ ✓				
Full Contro Read Write Enroll	ol			 <td></td>				
Full Contro Read Write Enroll Autoenrol	ol I			 <				
Full Contro Read Write Enroll Autoenrol	I			 <				
Full Contro Read Write Enroll Autoenrol	I							
Full Contro Read Write Enroll Autoenrol	I							
Full Contro Read Write Enroll Autoenrol	ol I Dermissions	or advanc	ed settings	s, click				
Full Contro Read Write Enroll Autoenrol	ol I	or advanc	ed settings	s, click	Advanced			
Full Contro Read Write Enroll Autoenrol	ol I	or advanc	ed settings	s, click	Advanced			
Full Contro Read Write Enroll Autoenrol	ol I	or advanc	ed settings	s, click	Advanced			
Full Contro Read Write Enroll Autoenrol	ol	or advanc	ed settings	s, click	Advanced			

步驟 8.返回證書頒發機構視窗,按一下右鍵Certificate Templates資料夾,然後選擇New > Certificate Template to Issue。

步驟 9.選擇以前建立的證書模板(在此示例中為9800-LSC),然後選擇OK。

注意:由於需要在所有伺服器上複製新建立的證書模板,因此在多台伺服器部署中列出該模板 可能需要較長時間。

3	Enable Certificate Templates	X
Select one Certificate Template to Note: If a certificate template that information about this template has All of the certificate templates in th For more information, see <u>Cert</u>	enable on this Certification Authority. was recently created does not appear on this list, you may need to wait until been replicated to all domain controllers. e organization may not be available to your CA. <u>ifficate Template Concepts.</u>	
Name	Intended Purpose	~
@ 9800-LSC	Client Authentication, Secure Email, Encrypting File System	
R CA Exchange	Private Key Archival	
Code Signing	Code Signing	=
Cross Certification Authority	<al></al>	
Enrollment Agent	Certificate Request Agent	
Enrollment Agent (Computer)	Certificate Request Agent	
Rechange Signature Only	Secure Email	
Exchange User	Secure Email	
IPSec	IP security IKE intermediate	
Key Recovery Agent	Key Recovery Agent	
OCSP Response Signing	OCSP Signing	~
	OK Cano	;el

選擇模板

新證書模板現在列在Certificate Templates檔案夾內容中。

🧔 certsrv - [Cer	tification Authority (Local)\CHUU-WIN	N12-CA\Certificate Templates]	X
File Action View Help			
🗢 🏟 🖄 🙆 😫			
Certification Authority (Local) CHUU-WIN12-CA Revoked Certificates Pending Requests Failed Requests Certificate Templates	Name Image: Second Se	Intended Purpose Client Authentication, Secure Email, En Client Authentication Certificate Request Agent IP security IKE intermediate Certificate Request Agent Directory Service Email Replication Client Authentication, Server Authentic Client Authentication, Server Authentic File Recovery Encrypting File System Client Authentication, Server Authentic Server Authentication Client Authentication, Server Authentic Server Authentication Client Authentication, Server Authentic Encrypting File System, Secure Email, Cl <all> Microsoft Trust List Signing, Encrypting</all>	

選擇LSC

步驟 10.返回Registry Editor視窗並導航到Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP。

步驟 11.編輯EncryptionTemplate、GeneralPurposeTemplate和SignatureTemplate登錄檔,使其指向新建立的證書模板。

۲. Electric de la construcción de la const	Registry Editor		_ D X
File Edit View Favorites Help			
File Edit View Favorites Help Image: Defaults Image: Defaults Image: Defaults Image: Defaults Image: Defaults Image: Defaults Image: Defaults Image: Defaults Image: Defaults Image: Defaults Image: Defaults Image: Defaults Image: Defaults Image: Defaults Image: Defaults Image: Defaults Image: Defaults Image: Defaults Image: Defaults Image: Defaults Image: Defaults Image: Defaults Image: Defaults Image: Defaults Image: Defaults Image: Defaults Image: D	Name (Default) (Defa	Type REG_SZ REG_SZ REG_SZ REG_SZ	Data (value not set) 9800-LSC 9800-LSC 9800-LSC
DFS DFS DHCPMibAgent DirectDraw DirectInput	<	111	>
Computer\HKEY_LOCAL_MACHINE\SOFT	WARE\Microsoft\Crypt	ography\MSCEP	.4

在登錄檔中更改模板

步驟 12.重新啟動NDES伺服器,返回到Certification Authority 視窗,選擇伺服器名稱,然後依次選 擇Stop 和Play 按鈕。

ia)	certsrv - [Certification Authority (Local)\CH	JU-WIN12-CA]	_ 🗆 X
File Action View Help 	▶ ■		
CHUU-WIN12-CA Revoked Certificates Issued Certificates Pending Requests Failed Requests Certificate Templates	Name Revoked Certificates Issued Certificates Pending Requests Failed Requests Certificate Templates		

在9800上配置LSC

以下是在WLC中為AP配置LSC的序列步驟。

- 1. 建立RSA金鑰。此金鑰稍後用於PKI信任點。
- 2. 建立信任點並對映建立的RSA金鑰。
- 3. 為AP啟用LSC調配並對映信任點。
 - 1. 為所有加入的AP啟用LSC。
 - 2. 通過預配清單為選定的AP啟用LSC。
- 4. 更改無線管理信任點並指向LSC信任點。

AP LSC GUI配置步驟

步驟1.導覽至Configuration > Security > PKI Management > Key Pair Generation。

- 1. 點選add並為其指定相關名稱。
- 2. 新增RSA金鑰大小。
- 3. 可匯出金鑰選項是可選的。只有在您想將金鑰從盒子中匯出時才需要這樣做。
- 4. 選擇生成

Dashboard	1	Trustpoints CA Server	Key Pair	Generation Add Ce	ertificate Trustp	bool
Monitoring	>	+ Add	Key Type	Key Y Exportable Zeroize		
Comgulation	í.	TP-self-signed-2147029136	RSA	No 🛱 Zer	Key Name*	AP-SCEP
Administration	>	9800-40.cisco.com	RSA	No 🔒 Zer	Key Type*	● RSA Key ○ EC Key
Licensing		TP-self-signed- 2147029136.server	RSA	No 🗎 Zer	Modulus Size*	2048
		CISCO_IDEVID_SUDI	RSA	No 🗎 Zer		
Troubleshooting		CISCO_IDEVID_SUDI_LEGACY	RSA	No 🗎 Zer	Key Exportable*	
		н н 1 н н	10 🗸	1 - 5 of 5 items	Cancel	✓ Generate

步驟 2.導航至Configuration > Security > PKI Management > Trustpoints

- 1. 點選add並為其指定相關名稱。
- 2. 輸入註冊URL(此處的URL為<u>http://10.106.35.61:80/certsrv/mscep/mscep.dll</u>)及其餘詳細資訊。
- 3. 選擇在步驟1中建立的RSA金鑰對。
- 4. 按一下「Authenticate」。
- 5. 點選註冊信任點並輸入密碼。
- 6. 按一下Apply to Device(應用到裝置)。

Q Search Menu Items	Configuration • > Security • > PKI Management							
🚍 Dashboard	Add Trustpoint			×				
	Label*	Access_Point-MS-CA	Enrollment Type	SCEP O Terminal				
(Monitoring >	Subject Name							
Configuration >	Country Code	IN	State	КА				
Administration	Location	Bengaluru	Domain Name	TAC-LAB.cisco.local				
© Licensing	Organization	TAC	Email Address	mail@tac-lab.local				
X Troubleshooting	Enrollment URL	/certsrv/mscep/mscep.dll	Authenticate					
	Key Generated		Available RSA Keypairs	AP-SCEP 🔻				
	Enroll Trustpoint							
	Password*							
	Re-Enter Password*							
	Cancel			Apply to Device				

步驟3.導覽至Configuration > Wireless > Access Points。向下滾動並選擇LSC Provision。

- 1. 將狀態選擇為已啟用。這會為連線到此WLC的所有AP啟用LSC。
- 2. 選擇我們在步驟2中建立的信任點名稱。

根據需要填寫其餘詳細資訊。

Q. Search Menu Items	Configuration * > Wireless * > Access Points			
and Dashboard	 All Access Points 			
	Total APs : 1		Misconfigured APs Tag : 0 Country Cor	de : 0 LSC Failback : 0 Select an Action 👻
Configuration	AP Name E AP Model	Admin : Slots : Status Up Time : IP Address	Base Radio MAC : Ethernet MAC :	AP i Power Denate i Operation i Config Mode Capable Status Status
(O) Administration >	AP0CD0-F89A-46E0 4 2 C9117AXI-D	2 O days 0 hrs 26 10.105.101.168 mins 42 secs	d0ec.3579.0300 0cd0.189a.46e0	Local Yes Registered Healthy
C Licensing	H 4 1 F H 10 -			1 - 1 of 1 access points 👌
X Troubleshooting	> 6 GHz Radios			
	> 5 GHz Radios			
	> 2.4 GHz Radios			
	> Dual-Band Radios			
	> Country			
	 LSC Provision 			
	Status	Enabled •	Subject Name Parameters	B) Apply
	Trustpoint Name	Access_Point-MS.# +	Country IN	
	Number of Join Attempts	3	State KA	
	Key Size	2048 •	City Bengaluru	
	Certificate chain status	Not Available	Organization TAC	
	Number of certificates on chain	0	-	

啟用LSC後,AP會通過WLC下載證書並重新啟動。在AP控制檯會話中,您會看到類似以下代碼片 段的內容。

-		
[*09/25/2023]	10:03:28.0993]	
[*09/25/2023 1	10:03:28.7016]	
[+09/25/2023 1	10:03:28.7663]	writing new private key to '/tmp/lsc/priv_key'
[+09/25/2023]	10:03:28.7666]	
[*09/25/2023 1	10:03:28.9212]	LSC_ENABLE: saving ROOT_CERT_
[+09/25/2023 1	10:03:28.9212]	
[+09/25/2023 1	10:03:28.9293]	LSC_ENABLE: saving DEVICE_CERT
[+09/25/2023 1	10:03:28.9293]	
[+09/25/2023 1	10:03:28.9635]	LSC certs and private key verified
[+09/25/2023 1	10:03:28.9635]	
[+09/25/2023 1	10:03:29.4997]	LSC private key written to hardware TAM
[+09/25/2023 1	10:03:29.4997]	
[*09/25/2023 1	10:03:29.5526]	A[09/25/2023 10:03:29.6099] audit_printk_skb: 12 callbacks suppressed

步驟4.啟用LSC後,可以更改無線管理證書以匹配LSC信任點。這會使AP加入其LSC證書,並且 WLC使用其LSC證書加入AP。如果您唯一感興趣的是對AP進行802.1X身份驗證,則這是可選步驟 。

- 1. 前往Configuration > Interface > Wireless,然後按一下Management Interface。
- 2. 更改Trustpoint以匹配我們在步驟2中建立的信任點。

LSC GUI配置部分到此結束。AP現在必須能夠使用LSC證書加入WLC。

Q. Search Menu Items	Configuration * > Interface * > Wireless Edit Management Interface *
-	Add > Delete Changing the interface or trustpoint will cause APs to disconnect and disrupt clients.
Dashboard	Interface Name 🝸 Interface Type 🍸 VLAN ID 🍸 IP Address 🍸 IP Netmask
	Vian101 Management 101 10.105.101.160 255.255.255
Configuration →	H < 1 > H 10 v
() Administration >	There is no interpoint configured on the controller. CASCO_UTEVID_SUDT is used as the debut thistpoint.
C) Licensing	NAT IPv4/IPv6 Server Address 0.0.0.0
NB Tour biostration	
Troubleshooting	
	D Cancel

AP LSC CLI配置步驟

1.使用此命令建立RSA金鑰。

9800-40(config)#crypto key generate rsa general-keys modulus 2048 label AP-SCEP

% You already have RSA keys defined named AP-SCEP. % They will be replaced % The key modulus size is 2048 bits % Generating 2048 bit RSA keys, keys will be non-exportable... [OK] (elapsed time was 0 seconds) Sep 27 05:08:13.144: %CRYPTO_ENGINE-5-KEY_DELETED: A key named AP-SCEP has been removed from key storag Sep 27 05:08:13.753: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named AP-SCEP has been generated or imported

2.建立PKI信任點並對映RSA金鑰對。輸入註冊URL及其餘詳細資訊。

```
9800-40(config)#crypto pki trustpoint Access_Point-MS-CA
9800-40(ca-trustpoint)#enrollment url http://10.106.35.61:80/certsrv/mscep/mscep.dll
9800-40(ca-trustpoint)#subject-name C=IN,L=Bengaluru,ST=KA,0=TAC,CN=TAC-LAB.cisco.local,E=mail@tac-lab.
9800-40(ca-trustpoint)#rsakeypair AP-SCEP
9800-40(ca-trustpoint)#revocation none
9800-40(ca-trustpoint)#exit
```

3.使用crypto pki authenticate <trustpoint>命令向CA伺服器驗證並註冊PKI信任點。在密碼提示中輸 入密碼。

```
9800-40(config)#crypto pki authenticate Access_Point-MS-CA
Certificate has the following attributes:
Fingerprint MD5: C44D21AA 9B489622 4BF548E1 707F9B3B
Fingerprint SHA1: D2DE6E8C BA665DEB B202ED70 899FDB05 94996ED2
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
9800-40(config)#crypto pki enroll Access_Point-MS-CA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password:
Sep 26 01:25:00.880: %PKI-6-CERT_ENROLL_MANUAL: Manual enrollment for trustpoint Access_Point-MS-CA
Re-enter password:
% The subject name in the certificate will include: C=IN,L=Bengaluru,ST=KA,O=TAC,CN=TAC-LAB.cisco.local
% The subject name in the certificate will include: 9800-40.cisco.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: TTM244909MX
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose Access_Point-MS-CA' commandwill show the fingerprint.
Sep 26 01:25:15.062: %PKI-6-CSR_FINGERPRINT:
CSR Fingerprint MD5 : B3D551528B97DA5415052474E7880667
CSR Fingerprint SHA1: D426CE9B095E1B856848895DC14F997BA79F9005
CSR Fingerprint SHA2: B8CEE743549E3DD7C8FA816E97F2746AB48EE6311F38F0B8F4D01017D8081525
Sep 26 01:25:15.062: CRYPTO_PKI: Certificate Request Fingerprint MD5 :B3D55152 8B97DA54 15052474 E78806
Sep 26 01:25:15.062: CRYPTO_PKI: Certificate Request Fingerprint SHA1 :D426CE9B 095E1B85 6848895D C14F9
Sep 26 01:25:15.063: CRYPTO_PKI: Certificate Request Fingerprint SHA2 :B8CEE743 549E3DD7 C8FA816E 97F27
Sep 26 01:25:30.239: %PKI-6-CERT_INSTALL: An ID certificate has been installed under
Trustpoint : Access_Point-MS-CA
Issuer-name : cn=sumans-lab-ca,dc=sumans,dc=tac-lab,dc=com
Subject-name : e=mail@tac-lab.local,cn=TAC-LAB.cisco.local,o=TAC,l=Bengaluru,st=KA,c=IN,hostname=9800-4
Serial-number: 5C000001400DD405D77E6FE7F00000000014
End-date : 2024-09-25T06:45:15Z
9800-40(config)#
```

4.使用LSC證書配置AP加入。

9800-40(config)#ap lsc-provision join-attempt 10 9800-40(config)#ap lsc-provision subject-name-parameter country IN state KA city Bengaluru domain TAC-L 9800-40(config)#ap lsc-provision key-size 2048 9800-40(config)#ap lsc-provision trustpoint Access_Point-MS-CA 9800-40(config)#ap lsc-provision In Non-WLANCC mode APs will be provisioning with RSA certificates with specified key-size configuration Are you sure you want to continue? (y/n): y

5.更改無線管理信任點,使其與上面建立的信任點匹配。

9800-40(config)#wireless management trustpoint Access_Point-MS-CA

AP LSC驗證

在WLC上運行這些命令以驗證LSC。

#show wireless management trustpoint
#show ap lsc-provision summary
#show ap name < AP NAME > config general | be Certificate



9800-40#sho ap name AP0CD0.F8	89A.46E0 config general begin Certificate
AP Certificate type	: Locally Significant Certificate
AP Certificate Expiry-time	: 09/25/2024 06:48:23
AP Certificate issuer common-	-name : sumans-lab-ca
AP Certificate Policy	: Default
AP CAPWAP-DTLS LSC Status	
Certificate status	: Available
LSC fallback status	: No
Issuer certificate hash	: 611255bc69f565af537be59297f453593e432e1b
Certificate expiry time	: 09/25/2024 06:48:23
AP 802.1x LSC Status	
Certificate status	: Not Available
AB 100 authorities the	CANAD DTLC

重新載入AP後,登入到AP CLI並運行這些命令以驗證LSC配置。

#show crypto | be LSC
#show capwap cli config | in lsc
#show dtls connection

```
APOCD0.F89A.46E0#sho crypto | be LSC
LSC: Enabled
                          --- Device Certificate ---
Certificate:
   Data:
       Version: 3 (0x2)
      Serial Number:
           5c:00:00:00:18:18:14:ed:da:85:f9:bf:d1:00:00:00:00:00:18
       Signature Algorithm: sha256WithRSAEncryption
       Issuer: DC = com, DC = tac-lab, DC = sumans, CN = sumans-lab-ca
       Validity
           Not Before: Sep 28 04:15:28 2023 GMT
           Not After : Sep 27 04:15:28 2024 GMT
       Subject: C = IN, ST = KA, L = Bengaluru, O = TAC, CN = ap1g6-0CD0F89A46E0, emailAddress = mail@tac-lab.local
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
               RSA Public-Key: (2048 bit)
               Modulus:
```

	AP0CD0.F89A.46E0#sho crypto	in LSC
ľ	LSC: Enabled	
	AP@CD@.F89A.46E@#sho capwap cl	l <u>i confia i</u> n lsc
	AP lsc enable	: 1
	AP lsc reboot cnt	: 0
l	AP lsc max num of retry	: 10
l	AP lsc mode	: 0×1
l	AP lsc dtls fallback state	: 0
l	AP0CD0.F89A.46E0#	
l	Read timed out	
U		

AP0CD0.F89A.46E0#sho dtls connections

Number of DTLS connection = 1

[ClientIP]:ClientPort <=> [ServerIP]:ServerPort Ciphersuit Version

[10.105.101.168]:5256 <=> [10.105.101.160]:5246 0xc02f 1.2

Current connection certificate issuer name: sumans-lab-ca

排除LSC調配故障

您可以從WLC或AP上行鏈路交換機埠獲取EPC捕獲,以驗證AP用於形成CAPWAP隧道的證書。從 PCAP驗證是否成功構建DTLS隧道。



可以在AP和WLC上運行DTLS調試以瞭解證書問題。

AP配置為使用相同的LSC證書進行身份驗證。AP充當802.1X請求方,並由交換機針對ISE伺服器進 行身份驗證。ISE伺服器與後端的AD通訊。



註:一旦在AP上行鏈路交換機埠上啟用dot1x身份驗證,AP將無法轉發或接收任何流量 ,直到身份驗證通過。要恢復身份驗證失敗的AP並獲得AP訪問許可權,請禁用AP有線交 換機埠上的dot1x auth。

EAP-TLS身份驗證工作流程和消息交換



AP有線802.1x身份驗證配置步驟

- 1. 啟用dot1x port auth和CAPWAP DTLS,然後選擇EAP型別。
- 2. 為AP建立dot1x憑據。
- 3. 在交換機埠上啟用dot1x。
- 4. 在RADIUS伺服器上安裝受信任的證書。

AP有線802.1x身份驗證GUI配置

- 1. 導航到AP加入配置檔案,然後按一下該配置檔案。
 - 1. 按一下AP > General。選擇EAP型別和AP授權型別作為「CAPWAP DTLS + dot1x port auth」。
 - 2. 導航到Management > Credentials,然後為AP dot1x auth建立使用者名稱和密碼。

Cisco Cat	talyst 9800-40 Wireless Controller		Welcome admin 🛛 🛠 🤻 🛕 🖺 🏟 🔞 📿 Search	APs and Clients Q
Q. Search Manu Items	Configuration * > Tags & Profiles * > AP Join		Edit AP Join Profile General Clent CAPWAP AP Management Security	x ICap QoS
Dashboard	AP Join Profile Name	T Des	General Power Management Hyperlocation AP Statistics Power Over Ethernet Clies	nt Statistics Reporting Interval
Configuration	APQ_test tonSto APQ_stor-Fir-APs		Switch Flag 5 GH Power Injector State 2.4 0	z (sec) 90 Hz (sec) 90
Clicensing Troubleshooting	APG_db-FF-APs APG_db-FF-APs APG_fb-FF-APs APG_7b-FF-APs		Power Injector Type Unknown Exte Injector Switch MAC 0000.0000 Enable	nded Module
	APG_BUH-Fir-APs APG_110+-Fir-APs APG_110+-Fir-APs		AP EAP Auth Configuration Mes EAP Type EAP-TLS Profil AP Authorization Type CAPNAP DTLS + DOTe.	h e Name default-mesh-pro v @ Clear
Work Me Through 1	APO_1200+PH-APs H ← 1 2 3 → ₩ 10 -		CAPVAP DTLS + DOT's port auth CAPVAP DTLS Dot's port auth	
			"D Cancel	👸 Update & Apply to Device

Cisco Cat	talyst 9800-40 Wireless Controller	Welcome admin 🛛 🏘 🌾 🛕 🖹 🌣 🔞 🕢 🎜 Estato Alls and Clares 🔍 🛛 🖀 Feedback, 🖍 🚱
Q. Search Menu Items	Configuration * > Tags & Profiles * > AP Join	Edit AP Join Profile x
Dashboard	+ Add X Delete	General Client CAPWAP AP Management Security ICap QoS
	AP Join Profile Name	Y Des
Monitoring >	ap-auth	Dot1x Credentials
🔾 Configuration 🔹	APG_test	Dot1x Username ap-wired-user
(C) Administration	testSite	Dot1x Password
	APG_3rd-Fir-APs APG_4th-Fir-APs	Dot1x Password Type elear •
	APG_0th-Fk-APs	
Troubleshooting	APG_7th-Fk-APs	
	APG_8th-Fir-APs	
	APG_11th-Fir-APs	
And the Parcel of	APG_12th-Fir-APs	
	H 4 1 2 3 + H 10 -	
		Cancel

AP有線802.1x身份驗證CLI配置

使用以下命令從CLI為AP啟用dot1x。這僅對使用特定加入配置檔案的AP啟用有線身份驗證。

#ap profile ap-auth
#dot1x eap-type eap-tls
#dot1x lsc-ap-auth-state both
#dot1x username ap-wired-user password 0 cisco!123

AP有線802.1x身份驗證交換機配置

本實驗使用交換機配置來啟用AP有線身份驗證。您可以根據設計採用不同的配置。

aaa new-model dot1x system-auth-control aaa authentication dot1x default group radius aaa authorization network default group radius radius server ISE address ipv4 10.106.34.170 auth-port 1812 acct-port 1813 key cisco!123 interface GigabitEthernet1/0/2 description "AP-UPLINK-PORT-AUTH-ENABLED" switchport access vlan 101 switchport mode access authentication host-mode multi-host authentication order dot1x authentication priority dot1x authentication port-control auto dot1x pae authenticator end

RADIUS伺服器憑證安裝

驗證發生在AP(充當請求方)和RADIUS伺服器之間。兩者必須信任彼此的證書。使AP信任 RADIUS伺服器證書的唯一方法是使RADIUS伺服器使用由也頒發AP證書的SCEP CA頒發的證書。

在ISE中,轉至管理>證書>生成證書簽名請求

生成CSR並使用ISE節點的資訊填充欄位。

■ Cisco ISE

Administration · System

Deployment Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings
Deployment Licensing Certificate Management ~ System Certificates ~ Trusted Certificates ~ OCSP Client Profile ~ Certificate Signing Requests ~ Certificate Periodic Check Se ~	Certified use Andmanno Upgrad Health Order Backup & R. Beston Admin Acces Settings
	Certificate(s) will be used for EAP Authentication
	Node(s)
	Generate CSR's for these Nodes:
	Node CSR Friendly Name
	SE99 ISE99/IEAP Authentication
	Subject
	Common Name (CN) FFQDNS O
	Organizational Unit (OU)
	Organization (O)
	City (L)
	State (ST)

生成後,可以匯出它並將其複製貼上為文本。

導航到您的Windows CA IP地址並將/certsrv/新增到URL

按一下「Request a certificate」

← → C ▲ Non sécurisé | 192.168.1.98/certsrv/
 Microsoft Active Directory Certificate Services - mydomain-WIN-3E2O2T1QD0U-CA
 Welcome
 Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task: <u>Request a certificate</u> <u>View the status of a pending certificate request</u> <u>Download a CA certificate, certificate chain, or CRL</u>

按一下Submit a certificate request by using a base-64

Microsoft Active Directory Certificate Services -- mydomain-WIN-3E2O2T1QD0U-CA

Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to: Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file,

在文本框中貼上CSR文本。選擇Web伺服器證書模板。

← C ▲ Non sécurisé 192.168.1.98/certsrv/certrqxt.asp
Microsoft Active Directory Certificate Services - mydomain-WIN-3E202T1QD0U-CA
Submit a Certificate Request or Renewal Request
To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.
Saved Request: Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):
Certificate Template:
Additional Attributes:

然後,通過返回到Certificate Signing Request選單並按一下Bind certificate,可以在ISE上安裝此證 書。然後,您可以上傳從Windows C獲得的證書。

≡ Cisco ISE	Administration - System			
Deployment Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings			
Certificate Management ~ System Certificates	Certificate Signing Requests			
Trusted Certificates OCSP Client Profile	Generate Certificate Signing Requests (CSR)			
Certificate Signing Requests	A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click this list.			
Certificate Periodic Check Se	Q View 🖞 Export 📋 Delete Bind Certificate			
Certificate Authority >	Erriendly Name Certificate Subject Key Length Portal gro Timestamp Abox			
	ISE99#EAP Authentication CN=ISE99.mydomain.local 4096 Mon, 30 Oct 2023 ISE99			

AP有線802.1x驗證驗證

通過控制檯訪問AP並運行命令:

#show ap authentication status

未啟用AP身份驗證:

A<u>POCD0.F89A.46E8≇sho ap authenticat</u>ion status AP <mark>dot1x</mark> feature is disabled. IPOCD0.F89A.40E0#

啟用ap auth後從AP記錄控制檯日誌:

AP0CD0.F89A.46E0#[*09/26/2023 08:57:40.9154] [*09/26/2023 08:57:40.9154] Restart for both CAPWAP DTLS & 802.1X LSC mode [*09/26/2023 08:57:40.9719] AP Rebooting: Reset Reason - LSC mode ALL

AP已成功通過身份驗證:



WLC驗證:



成功身份驗證後的交換機埠介面狀態:

 Switch#sho authentication sessions interface gigabitEthernet 1/0/2

 Interface
 MAC Address
 Method
 Domain
 Status Fg
 Session ID

 Gi1/0/2
 0cd0.f89a.45e0
 dot1x
 DATA
 Auth
 9765690A0000005CCEED0FBF

以下是指示身份驗證成功的AP控制檯日誌示例:

```
[*09/26/2023 07:33:57.5512] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5513] hostapd:EAP: Status notification: started (param=)
[*09/26/2023 07:33:57.5513] hostapd:EAP: EAP-Request Identity
[*09/26/2023 07:33:57.5633] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5634] hostapd:EAP: Status notification: accept proposed method (param=TLS)
[*09/26/2023 07:33:57.5673] hostapd:dot1x: CTRL-EVENT-EAP-METHOD EAP vendor 0 method 13 (TLS) selected
[*09/26/2023 07:33:57.5907] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5977] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6045] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6126] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6137] hostapd:dot1x: CTRL-EVENT-EAP-PEER-CERT depth=1 subject='/DC=com/DC=tac-lab
[*09/26/2023 07:33:57.6145] hostapd:dot1x: CTRL-EVENT-EAP-PEER-CERT depth=0 subject='/C=IN/ST=KA/L=BLR/
[*09/26/2023 07:33:57.6151] hostapd:EAP: Status notification: remote certificate verification (param=su
[*09/26/2023 07:33:57.6539] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6601] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6773] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.7812] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.7812] hostapd:EAP: Status notification: completion (param=success)
[*09/26/2023 07:33:57.7812] hostapd:dot1x: CTRL-EVENT-EAP-SUCCESS EAP authentication completed successf
[*09/26/2023 07:33:57.7813] hostapd:dot1x: State: ASSOCIATED -> COMPLETED
[*09/26/2023 07:33:57.7813] hostapd:dot1x: CTRL-EVENT-CONNECTED - Connection to 01:80:c2:00:00:03 comp]
```

802.1X身份驗證故障排除

在AP上行鏈路上執行PCAP並驗證radius身份驗證。以下是成功驗證的片段。

	479	07:47:17.192983	Cisco_9a:46:e0	Nearest-non-TP_	EAP	Response, Identity[Packet size limited during capture]	
	479	07:47:17.201985 07:47:17.205983	18.100.34.178 Cisco 9a:46:e8	10.105.101.151 Nearest-pon-TP_	RADIUS 1812 55431 TLSv1.2	Access-Challenge 104149 Encrypted Handshake Message	
	479	07:47:17.253984	10.186.34.170	10.105.101.151	MOIUS 1812 55431	Access-Onlinear to 200	-
	479	07:47:17.256975	C1sco_9a:46:e0	Nearest-non-TP	EAP RADIUS 1812 55431	Response, TLS EAP (EAP-TLS)[Packet size Limited during capture]	
	479	07:47:17.267976	Cisco_9a:46:e0	Nearest-non-TP_	EAP	Response, TLS EAP (EAP-TLS)[Packet size limited during capture]	
	479	07:47:17.274979	Cisco_9a:46:e0	Nearest-non-TP_	EAP	Response, TLS EAP (EAP-TLS)[Packet size limited during capture]	
	479	07:47:17.277985 07:47:17.311988	10.106.34.170 Cisco 9a:46:e8	10.105.101.151 Nearest-pop-TP-	RADIUS 1812 55431	Access-Challenge id=247 Response, TLS FAP (FAP-TLS)	
Ť	479	67:47:17.314978	10.186.34.178	18.185.181.151	RADIUS 1812 55431	Reservation (see a second	
٠	479	07:47:17.318968	Cisco_9a:46:e0	Nearest-non-TP_	EAP RADIUS 1812 55431	Response, TLS EAP (EAP-TLS)	
+	479	07:47:17.324980	Cisco_9a:46:e0	Nearest-non-TP_	TLSv1.2	Encrypted Handshake Message, Encrypted Handshake Message, Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Me	
	479	07:47:17.342969	Cisco_9a:46:e0	Nearest-non-TP.	EAP 1812 55931	Response, TLS EAP (EAP-TLS)[Packet size limited during capture]	
	479	07:47:17.376979	10.106.34.170	10.105.101.151	RADIUS 1812 55431	Access-Accept id=251	_

TCPdump收集來自ISE的身份驗證。



如果在身份驗證期間發現問題,則需要從AP有線上行鏈路和ISE端同時捕獲資料包。

AP的Debug命令:

#debug ap authentication packet

相關資訊

- <u>思科技術支援與下載</u>
- <u>使用AireOS在AP上配置802.1X</u>
- <u>適用於LSC的9800組態設定指南</u>
- <u>9800的LSC配置示例</u>
- <u>為9800上的AP配置802.1X</u>

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)。