在AP上配置802.1X,以使用LSC进行PEAP或 EAP-TLS

目录	
先决条件	
<u>要求</u>	
使用的组件	
<u>背景信息</u>	
网络图	
配置	
Windows Server 2016 SCEP CA	
配置证书模板和注册表	
<u>在9800上配置LSC</u>	
<u>AP LSC GUI配置步骤</u>	
<u>AP LSC CLI配置步骤</u>	
AP LSC验证	
排除LSC调配故障	
使用LSC的AP有线802.1X身份验证	
<u>AP有线802.1x身份验证配置步骤</u>	
<u>AP有线802.1x身份验证GUI配置</u>	
<u>AP有线802.1x身份验证CLI配置</u>	
<u>AP有线802.1x身份验证交换机配置</u>	
RADIUS服务器证书安装	
<u>AP有线802.1x身份验证验证</u>	
<u>802.1X身份验证故障排除</u>	
相关信息	

简介

本文档介绍如何使用802.1X PEAP或EAP-TLS方法对交换机端口上的思科接入点进行身份验证。

先决条件

要求

Cisco 建议您了解以下主题:

- 无线控制器
- 访问点

- 交换机
- ISE服务器
- 认证中心.

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 无线控制器:运行17.09.02的C9800-40-K9
- 接入点:C9117AXI-D
- 交换机:运行17.06.04的C9200L-24P-4G
- AAA服务器:运行3.1.0.518的ISE-VM-K9
- 证书颁发机构: Windows Server 2016

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

如果您希望接入点(AP)使用802.1X通过交换机端口进行身份验证,默认情况下,它们使用不需要证书的EAP-FAST身份验证协议。如果希望AP使用PEAP-mschapv2方法(在AP端使用凭证,但在RADIUS端使用证书)或EAP-TLS方法(在两端使用证书),则必须先配置LSC。这是将受信任/根证书调配到接入点的唯一方法(对于EAP-TLS,也是设备证书)。AP无法执行PEAP并忽略服务器端验证。本文档首先介绍如何配置LSC,然后介绍如何配置802.1X。

如果您希望PKI提供更好的安全性、控制您的证书颁发机构(CA),并在生成的证书上定义策略、限制和使用,请使用LSC。

使用LSC时,控制器会获得CA颁发的证书。AP不直接与CA服务器通信,但WLC代表加入的AP请 求证书。必须在控制器上配置CA服务器详细信息且必须可访问。

控制器使用简单证书注册协议(SCEP)将设备上生成的certReq转发到CA,并再次使用SCEP从CA获 取签名证书。

SCEP是PKI客户端和CA服务器用于支持证书注册和撤销的证书管理协议。它广泛用于思科,并且 受许多CA服务器的支持。在SCEP中,HTTP用作PKI消息的传输协议。SCEP 的主要目标是向网络 设备安全地颁发证书。

网络图





主要需要配置两项:SCEP CA和9800 WLC。

Windows Server 2016 SCEP CA

本文档介绍用于实验的Windows Server SCEP CA的基本安装。实际的生产级Windows CA必须安 全且适当地配置,才能进行企业运营。本部分旨在帮助您在实验室中进行测试,并从使此配置有效 所需的设置中获得灵感。以下是步骤:

步骤1.安装全新的Windows Server 2016桌面体验。

步骤2.确保您的服务器配置了静态IP地址。

第3步:安装新的角色和服务,从Active Directory域服务和DNS服务器开始。

r Se	rver Manager			- 0 ×
	Add Roles and Features Wizard		- 🗆 X	age Tools View Help
	Select server roles		DESTINATION SERVER WIN-3E2O2T1QD0U	
i	Before You Begin	Select one or more roles to install on the selected server.		
	Installation Type Server Selection Server Roles Peatures DNS Server AD DS Confirmation Results	Roles Active Directory Certificate Services Active Directory Pomain Services Active Directory Federation Services Active Directory Federation Services Active Directory Lightweight Directory Services Active Directory Rights Management Services Device Health Attestation DHCP Server Fax Server Pile and Storage Services (1 of 12 installed) Host Guardian Service Hyper-V MultiPoint Services Network Policy and Access Services Print and Document Services Remote Desktop Services Volume Activation Services Web Server (IIS) Windows Deployment Services	Description 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
2		< Previous Next :	> Install Cancel	
		Events 1 Events Performance 5 Service BPA results Perform BPA results BPA results	es mance sults	1

Active Directory安装

🝙 Se	erver Manager								- 0	\times
a	ᡖ Add Roles and Features Wizard	1		-		×	200	Tools	View	Help
	Installation progr	ess		DESTINA WIN-3	ATION SER E2O2T1Q	IVER DOU	uge -			^
	Before You Begin	view installation progress								
	Server Selection	Feature installation								
	Server Roles	Configuration required. Installation su	cceeded on WIN-3E2O2T1QD0U.							
ΪĘ	Features DNS Server AD DS Confirmation Results	Active Directory Domain Services Additional steps are required to make th 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	is machine a domain controller. ler Windows PowerShell rrupting running tasks. View task pro n the command bar, and then Task D	ogress or etails.	open thi	\$			Hide	2
		Export configuration settings								
		< Pri	evious Next > Cla	ose	Canc	el				
		Events	Events							
		Services	Services							
		Performance	Performance							
		BPA results	BPA results							
										~

AD安装结束

第4步:完成后,点击Promote this server to a domain controller上的控制面板。

🚘 Server Manager			– 0 ×
Server M	lanager • Dashboard	• 🥲 🍢 Manage	Tools View Help
Dashboard	WELCOME TO SERVER MANAGE	Post-deployment Configuration Configuration required for Active Directory Domain	
Local Server All Servers	1 C	Services at WIN-3E2O2T1QD0U Promote this server to a domain controller	
DNS	QUICK START	Feature installation	
File and Storage Services	3	Configuration required. Installation succeeded on WIN-3E2O2T1QD0U. Add Roles and Features	
	WHAT'S NEW 4	Task Details	
	E	Connect this converte cloud convices	

配置AD服务

步骤5.创建新林并选择域名。

	-					
re-	Se	rve	r M	an	ag	er

(📥 Active Directory Domain Service	es Configuration Wizard				-		\times
	Active Directory Domain Service	Es Configuration Wizard iguration Select the deployment ope Add a domain controlle Add a new domain to a Add a new forest Specify the domain information Root domain name:	ration r to an existin n existing fore ation for this o	g domain est operation mydomain.loca		TA WIN-3	RGET SEI	X RVER 2DOU
		More about deployment co	onfigurations					
		Fuents	< Pre	vious Next >	Insta		Cance	el

选择林名称

步骤6.将证书服务角色添加到服务器:

📥 Server Manager						-	- () ×
Ser	ver Manager • Das	hboard •	B	🏲	Manage	Tools	View	Help
 Dashboard Local Server 	WELCOME TO SEE	RVER MANAGER						
All Servers	🔁 Add Roles and Features Wizard				-		×	
DNS	Select server role	S		WIN	DESTIN 3E2O2T1QD0U.n	ATION SERV nydomain.lo	ER cəl	
	Before You Begin Installation Type Server Selection Server Roles	Select one or more roles to install on the selected server. Roles Roles Rotive Directory Certificate Services Active Directory Domain Services (Installed)	^	Description Active Dir (AD CS) is	on ectory Certific used to creat	ate Service	:s	
	Features AD CS Role Services Confirmation	Active Directory Federation Services Active Directory Lightweight Directory Services Active Directory Rights Management Services Device Health Attestation DHCP Server DNS Server (Installed)		certification role service and mana variety of	on authorities tes that allow y ge certificates applications.	and relate ou to issu used in a	d e	de

添加证书服务

🚔 Server Manager					- 0	\times
Ser Ser	ver Manager • Dash	board • (🔊 🚩 Manage	e Tools	View	Help
DashboardLocal Server	WELCOME TO SERV	/ER MANAGER				_
All Servers	📥 Add Roles and Features Wizard		-	- 🗆	×	
 AD DS DNS File and Storage Ser 	Select role services	Solart the role convicer to install for Active Directory Contificat	DE: WIN-3E202T1QD	TINATION SERVI 0U.mydomain.loo	ER cal	
	Before You Begin	Select the role services to install for Active Directory Certificat	te Services			
	Installation Type	Role services	Description			
	Server Selection Server Roles Features	Certification Authority Certificate Enrollment Policy Web Service Certificate Enrollment Web Service Certification Authority Web Enrollment	Certification Authori to issue and manage Multiple CAs can be public key infrastruc	rtification Authority (CA) is used issue and manage certificates. Iltiple CAs can be linked to forn blic key infrastructure.		
	AD CS Role Services	e Services Network Device Enrollment Service Online Responder				
	Confirmation Results					

仅添加证书颁发机构

步骤7.完成后,配置证书颁发机构。

🚖 Server	Manager			-	đΧ
\mathbf{E}	AD CS Configuration		×	age Tools Vi	ew Help
III Dat	Role Services		DESTINATION SERVER WIN-3E2O2T1QD0U.mydomain.local		
All 🖬	Credentials	Select Role Services to configure		- 🗆 🗙	
🖳 AD	Role Services				
i∎i AD	Setup Type	Certification Authority		DESTINATION SERVER QD0U.mydomain.local	
🔒 DN	CA Type	Online Responder			
File File	Private Key	Network Device Enrollment Service			
	Cryptography	Certificate Enrollment Web Service			
	CA Name	Certificate Enrollment Policy Web Service			
	Validity Period			main.local.	
	Certificate Database				
	Confirmation			n the destination	ide
	Progress				
	Results				
		More about AD CS Server Roles			
		< Previous 1	Next > Configure Cancel	ess or open this	

第8步:选择企业CA。



企业CA

步骤9.使其成为根CA。自Cisco IOS XE 17.6起,LSC支持从属CA。

Manager		_	đ	×
AD CS Configuration		age Tools	View I	Help
CA Type Credentials Role Services	DESTINATION SERVER WIN-3E2O2TIQD0U.mydomain.local Specify the type of the CA	- 0	×	
Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	 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. Root CA Root CA Root CAs are the first and may be the only CAs configured in a PKI hierarchy. Subordinate CA Subordinate CA Subordinate CA receives a certificate to issue certificates by the CA above them in the hierarchy.	n the destination	ide	
	More about CA Type < Previous Next > Configure Cancel Image again by clicking Notifications in the command bar, and then Task Device Export configuration settings < Previous Next > Close	ess or open this tails.		
	AD CS Configuration CA Type Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Ab CS Configuration AD CS Configuration CA Type Credentials Role Services Setup Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results Progress Results Configure Private Kay Configure Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results Configure Private Kay Configure Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results Configure Private Key Configure Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results Configure Private Key Configure Private Key Configure Confi	Ab CS Configuration	Aba do Configuration

选择根CA

让用于CA的帐户成为IIS_IUSRS组的一部分非常重要。在本示例中,使用管理员帐户并转到Active Directory用户和计算机菜单,将管理员用户添加到IIS_IUSRS组。

📥 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>? X 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	? X 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

将管理员帐户添加到IIS_USER组

第10步:在正确的IIS组中拥有用户后,添加角色和服务。然后将Online Responder和NDES服务添 加到您的证书颁发机构。

o ×



安装NDES和在线响应程序服务

📥 Server Manager

步骤11.完成后,配置这些服务。



安装在线响应器和NDES服务

步骤12.系统会提示您选择服务帐户。这是您之前添加到IIS_IUSRS组的帐户。



选择已添加到IIS组的用户

步骤13.这足以执行SCEP操作,但为了实现802.1X身份验证,您还需要在RADIUS服务器上安装证书。因此,为方便起见,请安装和配置Web注册服务,以便在Windows Server上轻松复制和粘贴 ISE证书请求。



安装Web注册服务

AD CS Configuration			_		\times
Role Services		WIN-	DESTINA 3E2O2T1QD0U.my	TION SER	VER ocal
Credentials Role Services Confirmation Progress Results	Select Role Services to configure Certification Authority Certification Authority Web Enrollment Conline Responder Network Device Enrollment Service Certificate Enrollment Web Service Certificate Enrollment Policy Web Service More about AD CS Server Roles				
-	< Previous	Next >	Configure	Cance	el 🛛

配置web注册服务

步骤 14您可以通过访问<u>http://<serverip>/certsrv/mscep/mscep.dll</u>验证SCEP服务是否正常运行:

0	Netw	ork Dev	vice Enrollment Servic 🗙	+	_		X	
←	\rightarrow	C	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门户验证

步骤 15

默认情况下,Windows Server在注册到Microsoft SCEP(MSCEP)之前使用动态质询密码对客户端和 终端请求进行身份验证。这需要管理员帐户浏览到Web GUI,为每个请求生成按需密码(密码必须 包含在请求中)。控制器不能将此密码包含在发送给服务器的请求中。要删除此功能,需要修改 NDES服务器上的注册表项:

打开注册表编辑器,在开始菜单中搜索Regedit。

导航到计算机> HKEY_LOCAL_MACHINE >软件> Microsoft >加密> MSCEP >强制密码

将EnforcePassword值更改为0。如果已经是0,则保留原样。

۲. Electric de la construcción de la const		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

设置Enforcepassword值

配置证书模板和注册表

证书及其关联密钥可在多个场景中使用,用于由CA服务器内的应用策略定义的不同目的。应用策略 存储在证书的Extended Key Usage(EKU)字段中。验证器会分析此字段,以验证客户端是否将其用 于预期目的。要确保将正确的应用策略集成到WLC和AP证书,请创建正确的证书模板并将其映射到 NDES注册表:

步骤1:导航到开始>管理工具>证书颁发机构。

第二步:展开CA服务器文件夹树,右键单击证书模板文件夹并选择管理。

第三步:右键单击Users证书模板,然后在上下文菜单中选择Duplicate Template。

第四步:导航到General选项卡,根据需要更改模板名称和有效期,保留所有其它选项未选中。

🗥 注意:修改有效期时,请确保有效期不超过证书颁发机构的根证书有效期。

Properties of New Template

X

Subject Name	Sen	ver	Issuance R	equirements
Superseded Templa	ites	Exte	nsions	Security
Compatibility General	Request	Handling	Cryptography	Key Attestation
Template display name:				
9800-LSC				
Template name:				
9800-LSC				
Validity period:	_	Renewa	period:	
2 years 🗸	1	6	weeks 🗸	
	_			
Publish certificate in	Active Dir	rectory		
Do not automatic	cally reenro	oll if a dupli	cate certificate e	xists in Active
Directory				
ОК	(Cancel	Apply	Help

第五步:导航到Subject Name选项卡,确保选择了请求中的Supply。系统将显示一个弹出窗口,指示用户不需要管理员批准即可获得证书签名,请选择OK。

Properties of New Template									
Compatibility General Request Handling Cryptography Key Attestation									
Supersed	ded Templa	tes	Exte	nsions	Security				
Subject Name Server Issuance Requirements									
Use subject information from existing certificates for autoenrollment renewal requests (*)									
 Build from this Active Directory information Select this option to enforce consistency among subject names and to simplify certificate administration. 									

在请求中提供

第六步:导航到Extensions选项卡,然后选择Application Policies选项,然后选择Edit...按钮。确保 Application Policies窗口中的Client Authentication;否则,选择Add并添加它。

Properties of New Template								
Compatibility	General	Request	Handling	Cryptography	Key Attestation			
Subject N	Subject Name Server Issuance Requirements							
Supersec	ded Templa	tes	Exte	nsions	Security			
To modify an extension, select it, and then click Edit.								
Extensions included in this template:								
Edit Application Policies Extension								
An application policy defines how a certificate can be used.								
Application policies: Client Authentication Encrypting File System Secure Email								

验证扩展

步骤 7.导航到Security选项卡,确保在Windows Server中启用SCEP服务的步骤6中定义的服务帐户 具有模板的完全控制权限,然后选择Apply和OK。

Properties of New Template

X

ompatibility	General	Request	Handling	Cryptography	Key Attestation				
Subject N	Vame	Serv	rer	Issuance R	equirements				
Superse	ded Templa	ites	Exte	ensions	Security				
Group or user names:									
& Authen	ticated Use	115							
Administrator									
Domain Admins (CHUU-DOMAIN Domain Admins)									
Se Domain	1 Users (CH	UU-DOMA	(IN\Domai	in Users)					
Senterpr	ise Admins	(CHUU-DC)MAIN\En	nterprise Admins))				
			Г		-				
			L	Add	Remove				
Parmiesione	for Adminiet	rator		Allow	Decy				
ennissions		Jaw			Deny				
Full Contro	ol			<u> </u>					
Read				~					
Write				✓					
Enroll				✓					
Autoenrol				~					
For special p	ermissions	or advanc/	ed settings	s, click	Advanced				
Advanced.					Autoriced				
					_				

步骤 9选择以前创建的证书模板(在本示例中为9800-LSC),然后选择OK。

💊 注意:由于需要跨所有服务器复制新创建的证书模板,因此在多台服务器部署中列出该模板可 能需要较长时间。

	Enable Certificate Templates	
elect one Certificate Template to lote: If a certificate template that of formation about this template has If of the certificate templates in the 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 unti been replicated to all domain controllers. e organization may not be available to your CA. <u>ificate Template Concepts.</u>	I
Name	Intended Purpose	~
9800-LSC	Client Authentication, Secure Email, Encrypting File System	
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	
Exchange Signature Only	Secure Email	
Exchange User	Secure Email	
IPSec	IP security IKE intermediate	
Key Recovery Agent	Key Recovery Agent	
OCSP Resnanse Signing	OCSP Signing	~
	OK Car	ncel

选择模板

新证书模板现在在Certificate Templates文件夹内容中列出。

🧔 certsrv - [Cer	tification Authority (Local)\CHUU-WIN	112-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 Client Authentication Client Authentication Server Authentication Server Authentication Server Authentication Microsoft Trust List Signing, Encrypting	

选择LSC

步骤 10返回Registry Editor窗口,导航到Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP。

步骤 11编辑EncryptionTemplate、GeneralPurposeTemplate和SignatureTemplate注册表,使其指 向新创建的证书模板。



更改注册表中的模板

步骤 12重新启动NDES服务器,返回证书颁发机构窗口,选择服务器名称,然后依次选择停止和播 放按钮。

۵ د	certsrv - [Certification Authority (Local)\CHU	JU-WIN12-CA]	_ 🗆 X
File Action View Help	Þ 8		
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中为AP配置LSC的序列步骤。

- 1. 创建RSA密钥。此密钥稍后用于PKI信任点。
- 2. 创建信任点并映射创建的RSA密钥。
- 3. 为AP启用LSC调配并映射信任点。
 - 1. 为所有加入的AP启用LSC。
 - 2. 通过调配列表为选定AP启用LSC。
- 4. 更改无线管理信任点并指向LSC信任点。

AP LSC GUI配置步骤

第1步:导航到Configuration > Security > PKI Management > Key Pair Generation。

- 1. 点击add并为其指定相关名称。
- 2. 添加RSA密钥大小。
- 3. 密钥可导出选项是可选的。只有在您想将密钥导出为开箱即用时,才需要此密钥。
- 4. 选择生成

Monitoring + Add Configuration × Administration × Administration × Bloo-40.cisco.com RSA No 2 zeroize Key Name × Y Type Exportable Zeroize Key Name* AP-SCEP TP-self-signed-2147029136 RSA 9800-40.cisco.com RSA 9800-40.cisco.com RSA Victorial Cisco_locom RSA No 2 zer Modulus Size* 2048 Cisco_IDEVID_SUDI RSA Cisco_IDEVID_SUDI_LEGACY RSA No 2 zer Key Exportable* ✓ Key 4 1 No 2 zer Xey Exportable* ✓	Dashboard	Trustpoints CA Server Key Pair Generation Add Certificate Trustpool					
Communication Key Name F	Monitoring	+ Add	Key T	Key T			
Administration 9800-40.cisco.com RSA No Image: Second Seco	Configuration >	TD_colf_clanad_2147020126	DSA	No.	Key Name*	AP-SCEP	
Licensing TP-self-signed- 2147029136.server RSA No Image: Constraint of the server of the ser	Administration	9800-40.cisco.com	RSA	No a Ze	Key Type*	● RSA Key ○ EC Key	
CISCO_IDEVID_SUDI RSA No Image: Cisco_IDEVID_SUDI_LEGACY Troubleshooting CISCO_IDEVID_SUDI_LEGACY RSA No Image: Cisco_IDEVID_SUDI_LEGACY Image: Im	Licensing	TP-self-signed- 2147029136.server	RSA	No 🗎 Ze	Modulus Size*	2048	
CISCO_IDEVID_SUDI_LEGACY_RSA No Image: Zerr Key Exportable* Image: Image		CISCO_IDEVID_SUDI	RSA	No 🗎 Ze	ine ine cite		
H H I ⊨ H I0 - 1 - 5 of 5 items Cancel	Troubleshooting	CISCO_IDEVID_SUDI_LEGAC	Y RSA	No 🗎 Ze	Key Exportable*		
		H 4 1 F H	10 🗸	1 - 5 of 5 items	D Cancel	✓ Generate	
					_		

第二步:导航至Configuration > Security > PKI Management > Trustpoints

- 1. 点击add并为其指定相关名称。
- 2. 输入注册URL(此处的URL为<u>http://10.106.35.61:80/certsrv/mscep/mscep.dll</u>)和其余详细信息。
- 3. 选择在步骤1中创建的RSA密钥对。
- 4. 单击Authenticate。
- 5. 点击enroll trustpoint并输入密码。
- 6. 单击Apply to Device。

Q Search Menu Items	Configuration - > Set	curity * > 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

第3步:导航到配置>无线>接入点。向下滚动并选择LSC Provision。

- 1. 将状态选择为已启用。这将为连接到此WLC的所有AP启用LSC。
- 2. 选择我们在步骤2中创建的信任点名称。

根据需要填写其余详细信息。

Q. Search Meniu Items	Configuration * > Wireless * > Access Points				
are Dashboard	 All Access Points 				
\bigcirc Monitoring \rightarrow	Total APs : 1		Misconfigured AP Tag : 0 C	Ps Country Code : 0 LSC Failback : 0	Select an Action
Configuration	AP Name : AP Model :	Admin : Slots : Status Up Time : IP Address	Base Radio MAC Ethernet MAC	AP Power Derate	i Operation i Config Status Status
(Ô) Administration →	AP0CD0-F89A-46E0 🔥 💓 C9117AXI-D	2 0 days 0 hrs 26 mins 42 secs 10.105.101.160	3 d0ec.3579.0300 0cd0.189a.46e	O Local Yes	Registered Healths
C Licensing	H 4 1 H H 10 V			1	- 1 of 1 access points
💥 Troubleshooting	> 6 GHz Radios				
	> 5 GHz Radios				
	> 2.4 GHz Radios				
	> Dual-Band Radios				
	> Country				
	✓ LSC Provision				
	Status	Enabled •	Subject Name Parameters	8	Apply
	Trustpoint Name	Access_Point-MS.# •	Country IN	i i	
	Number of Join Attempts	3	State K/	Α.	
	Key Size	2048 ¥	City Be	engaluru	
	Certificate chain status	Not Available	Organization TA	AC	
	Number of certificates on chain	0			

启用LSC后,AP将通过WLC下载证书并重新启动。在AP控制台会话中,您会看到类似于此代码片 段的内容。

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

第4步:启用LSC后,您可以更改无线管理证书以匹配LSC信任点。这会使AP加入其LSC证书,并 且WLC使用其LSC证书进行AP加入。如果您唯一感兴趣的是对AP进行802.1X身份验证,则这是可 选步骤。

- 1. 转至Configuration > Interface > Wireless, 然后单击Management Interface。
- 2. 更改Trustpoint以匹配我们在步骤2中创建的信任点。

LSC GUI配置部分到此结束。AP现在必须能够使用LSC证书加入WLC。

Q. Search Menu Items	Configuration * > Interfa	ace* > Wireless				Edit Management Interface	×
_	+ Add × Delete					A Changing the interface or t	rustpoint will cause APs to disconnect and disrupt clients.
Dashboard	Interface Name	▼ Interface Type	Y VLAN ID	Y IP Address	Y IP Netmask		
Monitoring →	Vian101	Management	101	10.105.101.160	255.255.255	Interface	Vlan101 • (i)
	H 4 1 P H	10 🔻				Trustpoint	Access_Point-MS # ¥
ି ମିଧି Administration 🔉						There is no trustpoint configured on the cor	ntroller. CISCO_DEVD_SUDI is used as the default trustpoint.
M Licensing						NAT IPv4/IPv6 Server Address	0.0.0.0
(C) Licensing							
X Troubleshooting							
						D Cancel	Update & Apply to Device

AP LSC CLI配置步骤

1.使用此命令创建RSA密钥。

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.创建PKI信任点并映射RSA密钥对。输入注册URL和其余详细信息。

```
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,O=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>命令对PKI信任点进行身份验证并将其注册到CA服务器。 在密码提示符下输入密码。

```
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证书配置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.更改无线管理信任点,使其与上面创建的信任点匹配。

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

AP LSC验证

在WLC上运行这些命令以验证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
AD LCC suthentication state	CARLAR DTLC

重新加载AP后,登录到AP CLI并运行这些命令以验证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:
```

APOCOD.F89A.46E0#sho crypto in LSC LSC: Enabled APOCOD.F89A.45E0#sho capwap cli config in lsc AP lsc enable : 1 AP lsc reboot cnt : 0 AP lsc reboot cnt : 0 AP lsc mode : 0x1 AP lsc dtls fallback state : 0 AP lsc dtls fallback state : 0 AP lsc dtls fallback state : 0 AP lsc dtls fallback state : 0
AP0CD0.F89A.46E0#sho dtls connections
Number of DTLS connection = 1
<pre>[ClientIP]:ClientPort <=> [ServerIP]:ServerPort Ciphersuit Version</pre>
[10.105.101.168]:5256 <=> [10.105.101.160]:5246 0xc02f 1.2

Current connection certificate issuer name: sumans-lab-ca

排除LSC调配故障

您可以从WLC或AP上行链路交换机端口获取EPC捕获,以验证AP用于形成CAPWAP隧道的证书。 从PCAP验证DTLS隧道是否已成功建立。



可以在AP和WLC上运行DTLS调试以了解证书问题。

使用LSC的AP有线802.1X身份验证

AP配置为使用相同的LSC证书对自身进行身份验证。AP充当802.1X请求方,并由交换机针对ISE服 务器进行身份验证。ISE服务器与后端的AD通信。



注意:在AP上行链路交换机端口上启用dot1x身份验证后,AP在通过身份验证之前无法转 发或接收任何流量。要恢复身份验证不成功的AP并获得AP访问权限,请在AP有线交换机 端口上禁用dot1x auth。

EAP-TLS身份验证工作流程和消息交换



AP有线802.1x身份验证配置步骤

- 1. 启用dot1x port auth和CAPWAP DTLS并选择EAP类型。
- 2. 为AP创建dot1x凭证。
- 3. 在交换机端口上启用dot1x。
- 4. 在RADIUS服务器上安装受信任证书。

AP有线802.1x身份验证GUI配置

- 1. 导航到AP加入配置文件,然后点击配置文件。
 - 1. 点击AP > General。选择EAP类型和AP授权类型作为"CAPWAP DTLS + dot1x port auth"。
 - 2. 导航到Management > Credentials并为AP dot1x auth创建用户名和密码。

Cisco Ca	talyst 9800-40 Wireless Controller		Welcome admin 🛛 🛠 🌾 🛕 🖺 🏟 🗐 📿	Search APs and Clents Q
Q. Search Manu Items	Configuration * > Tags & Profiles * > AP Join		Edit AP Join Profile General Client CAPWAP AP Management Si	x iecurity ICap QoS
Dashboard Monitoring	AP Join Profile Name	▼ Des	General Power Management Hyperlocation AP Statis	Client Statistics Reporting Internal
	APG_test tootSte		Switch Flag	5 GHz (soc) 90
{⊙} Administration → (©) Licensing	APG_3rd-Fir-APs APG_4th-Fir-APs		Power Injector State Power Injector Type Unknown	2.4 GHz (sec) 90 Extended Module
💥 Troubleshooting	APG_00+Fr-APs APG_70+Fr-APs APG_80+Fr-APs		AP EAP Auth Configuration	Enable Mesh
Walk Me Through 2	APG_11th-Fir-APs APG_12th-Fir-APs APG_12th-Fir-APs		EAP Type EAP-TLS v AP Authorization Type CAPVAP DTLS + DDTs. CAPVAP DTLS +	Profile Name default-mesh-pro • Clear
	H < 1 2 3 → H 10 v		DOTTx port auth CAPWAP DTLS Dottx port auth	
			"D Cancel	🗄 Update & Apply to Device

Cisco Cat	alyst 9800-40 Wireless Controller	Welcome admin 🖌 🌾 🋕 🖹 💠 🔞 🕢 🎜 🔯 State Als and Cherry 🔾 🛛 🖀 Feedback) 🖉
Q. Search Menu Items	Configuration * > Tags & Profiles * > AP Join	Edit AP Join Profile *
Dashboard	+ Add × Delate	General Cilent CAPWAP AP Management Security ICap QoS Device User Credentials CDP Interface
O Hardenter	AP Join Profile Name	T Des
(1) Monitoring	ep-euth	Lot ix crecentais
🗞 Configuration 💦 🔸	APG_test	Dot1x Username ap-wired-user
() Administration >	testSite APG_3rd-Fir-APs	Dot1x Password
C Licensing	APG_4th-Fir-APs	Dot1x Pasoword Type clear •
Y Troubleshooting	APG_6th-Fir-APs	
~	APG_7th-Fir-APs	
	APG_8th-Fir-APs	
	APG_11th-Fir-APs	
Walk Me Through >	APG_12th-Fir-APs	
	H K 1 2 3 F H 10 F	
		Cancel

AP有线802.1x身份验证CLI配置

使用以下命令从CLI为AP启用dot1x。这仅对使用特定加入配置文件的AP启用有线身份验证。

#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有线802.1x身份验证交换机配置

此交换机配置在实验室中用于启用AP有线身份验证。您可以根据设计采用不同的配置。

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服务器证书安装

身份验证发生在AP(充当请求方)和RADIUS服务器之间。双方必须相互信任对方证书。使AP信任 RADIUS服务器证书的唯一方法是使RADIUS服务器使用由也颁发AP证书的SCEP CA颁发的证书。

在ISE中,转至管理>证书>生成证书签名请求

生成CSR并使用ISE节点的信息填充字段。

Administration - System

Deployment Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings
Certificate Management System Certificates	Certificate Signing Request Certificate types will require different extended key usages. The list below outlines which extended key usages are required for each certificate type:
Trusted Certificates	ISE Identity Certificates:
OCSP Client Profile	Multi-Use (Admin, EAP, Portal, pxGrid) - Client and Server Authentication
Certificate Signing Requests	Admin - Server Authentication EAP Authentication EAP Authentication
Certificate Periodic Check Se	DTLS Authentication - Server Authentication
	Portal - Server Authentication
Certificate Authority >	pxGrid - Client and Server Authentication
	SAML - SAML Signing Certificate Kennes in Generation - Generate a Similar Certificate or pageste a brand page Massaning Certificate
	tot Messaging service - Generate a signing Germicate or generate a brano new Messaging Certificate. Data Connect Certificate - Connect Oracle Database
	ISE Certificate Authority Certificates:
	ISE Root CA - This is not a signing request, but an ability to generate a brand new Root CA certificate for the ISE CA functionality.
	ISE Intermediate CA - This is an Intermediate CA Signing Request.
	Renew ISE OCSP Responder Certificates - This is not a signing request, but an ability to renew the OCSP responder certificate that is signed by the ISE Root CA/ISE Intermediate CA.
	Usage
	Certificate(s) will be used for EAP Authentication
	Allow Wildcard Certificates 🗌 🕠
	Node(s)
	Generate CSR's for these Nodes:
	Node CSR Friendly Name
	ISE99 ISE99#EAP Authentication
	Subject
	Common Name (CN) FQONS
	Organizational Unit (OU)
	Organization (O)
	City (L)
	State (ST)

生成后,您可以导出它并将其复制粘贴为文本。

导航到您的Windows CA IP地址并将/certsrv/添加到URL

单击Request a certificate

$\leftarrow \ \ \rightarrow$	C A Non sécurisé 192.168.1.98/certsrv/
Microsoft A	tive Directory Certificate Services – mydomain-WIN-3E2O2T1QD0U-CA
Welcome	
Use this W	b 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 als	so 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>

单击Submit a certificate request by using a base-64

Microsoft Active Directory Certificate Services -- mydomain-WIN-3E202T1QD0U-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.

将CSR文本粘贴到文本框中。选择Web服务器证书模板。

← 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: (No templates found!) >
Additional Attributes:

然后,您可以通过返回到Certificate Signing Request菜单并单击Bind certificate,在ISE上安装此证书。然后,您可以上传从Windows C获取的证书。

■ Cisco ISE	E 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 Certificate Periodic Check Se	A Certificate signing kequests (CSHs) must be sent to and signed by an external authority. Click "export" to download one or more CSHs so that they may be signed by an external authority. After a request has been signed, click this list.			
	Q View 🖞 Export 🌐 Delete Bind Certificate			
Certificate Authority >	Erriendly Name Certificate Subject Key Length Portal gro Timestamp \wedge Host			
	ISE99#EAP Authentication CN≈ISE99.mydomain.local 4096 Mon, 30 Oct 2023 ISE99			

AP有线802.1x身份验证验证

通过控制台访问AP并运行命令:

#show ap authentication status

未启用AP身份验证:

APOCD0.F89A.46E8#sho ap authentication status AP dot1x feature is disabled. APOCD0.F89A.40E8#

启用AP身份验证后来自AP的控制台日志:

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已成功通过身份验证:



WLC验证:



身份验证成功后的交换机端口接口状态:

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

 Interface
 MAC Address
 Method
 Domain
 Status Fg
 Session ID

 Gi1/0/2
 0cd0.f89a.46e0
 dot1x
 DATA
 Auth
 9765690A20000005CCEED0FBF

以下是指示身份验证成功的AP控制台日志示例:

```
[*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身份验证故障排除

对AP上行链路执行PCAP并验证radius身份验证。以下是成功身份验证的片段。

47907:47:17.192983 Cisco_9a:46:e0 Nearest-non-TP. EAP Response, Identity[Packet size limited during capture]	
ATE ATE <td></td>	
47907:47:17.256975 Cisco_9a:46:e0 Nearest-non-TP EAP Response, TLS EAP (EAP-TLS)[Packet size limited during capture]	
47907:47:17.267976 Cisco_9a:46:e0 Nearest-non-TP EAP Response, TLS EAP (EAP-TLS)[Packet size limited during capture]	
47907:47:17.274979 Cisco_9a:46:e0 Nearest-non-TP EAP Response, TLS EAP (EAP-TLS)[Packet size limited during capture]	
078L 8110/11/2/7802 38.180.54.18 181.103 181.2 20081 AccessDatiente Doc 4/ 4 79 07:47:17.311980 Cisco_9a:46:e0 Nearestnon-TP EAP Response, TLS EAP (EAP-TLS)	
47907:47:17.318968 Cisco_9a:46:e0 Nearest-non-TP EAP Response, TLS EAP (EAP-TLS)	
2 479. 07:47:17.324980 Cisco 9a:46:e0 Nearest-non-TP_ TLSV1.2 Encrypted Handshake Message, Encrypted Handshake Message, Change Cipher Spec. 2 479. 07:47:17.324980 Cisco 9a:46:e0 Nearest-non-TP_ TLSV1.2 Encrypted Handshake Message, Encrypted Handshake Message, Change Cipher Spec.	Encrypted Handshake Ne
4 479. 07:47:17.34296 (Sice.09:46:06) NearConnorTP. EAP Response, TIS EAP (EAP-TLS) [Packet size limited during capture]	

TCPdump从ISE收集捕获身份验证。



如果在身份验证期间发现问题,则需要从AP有线上行链路和ISE端同时捕获数据包。

AP的debug命令:

#debug ap authentication packet

相关信息

- <u>思科技术支持和下载</u>
- <u>在具有AireOS的AP上配置802.1X</u>
- <u>LSC 9800配置指南</u>
- <u>9800的LSC配置示例</u>
- <u>在9800上为AP配置802.1X</u>

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。