配置ISE 2.4和FMC 6.2.3 pxGrid整合

目錄

簡介 必要條件 需求 採用元件 配置ISE 步驟1.啟用pxGrid服務 步驟2.配置ISE以批准所有pxGrid基於證書的帳戶 步驟3.匯出ISE MNT管理員證書和pxGrid CA證書 配置FMC 步驟4.向FMC新增新領域 步驟5.生成FMC CA證書 步驟6.使用OpenSSL從產生的憑證中提取憑證和私密金鑰 步驟7.將證書安裝到FMC 步驟8.將FMC證書匯入ISE 步驟9.在FMC上配置pxGrid連線 驗證 在ISE中驗證 在FMC中驗證 疑難排解

簡介

本文檔介紹整合ISE pxGrid版本2.4和FMC版本6.2.3的配置流程。

必要條件

需求

思科建議您瞭解以下主題:

- ISE 2.4
- FMC 6.2.3
- Active Directory/輕量目錄訪問協定(LDAP)

採用元件

本文中的資訊係根據以下軟體和硬體版本:

• 獨立ISE 2.4

- FMCv 6.2.3
- Active Directory 2012R2
- •身分識別服務引擎(ISE)pxGrid版本2.4
- Firepower管理中心(FMC)版本6.2.3

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。

配置ISE

步驟1.啟用pxGrid服務

1. 登入ISE管理員GUI,導航至**管理>部署。**

2.選擇要用於pxGrid角色的ISE節點。



3.啟用pxGrid服務,然後按一下Save,如下圖所示。

Deployment	Deployment Nodes List > tim24adm
()E (2)	Edit Node
Arrow Deployment Arrow PAN Failover	General Settings Profiling Configuration
	Hostname
	FQDN
	IP Address
	Node Type Identity Services Engine (ISE)
	Role STANDALONE Make Primary
	Administration
	V Monitoring
	Role PRIMARY
	Other Monitoring Node
	Policy Service
	Enable Session Services (i)
	Include Node in Node Group None (i)
	Enable Profiling Service (j)
	Enable Threat Centric NAC Service (j)
	Enable SXP Service (i)
	Enable Device Admin Service (j)
	Enable Passive Identity Service (i)
	pxGrid 🕡
	Save Reset

4.驗證pxGrid服務是否從CLI運行。

注意:如果使用多個pxGrid節點,該過程最多需要5分鐘時間,pxGrid服務才能完全啟動並確 定高可用性(HA)狀態。

5.通過SSH進入ISE pxGrid節點CLI並檢查應用狀態。

show application status ise | in pxGrid
pxGrid Infrastructure Service running 24062
pxGrid Publisher Subscriber Service running 24366
pxGrid Connection Manager running 24323
pxGrid Controller running 24404
#

6.訪問ISE管理員GUI並驗證服務是否線上且正常運行。導航到管理> pxGrid服務。

7.在頁面底部, ISE顯示Connected to pxGrid <pxGrid node FQDN>。

dentity Services Engine	Home Home	Operations Policy Admin	istration Work Centers				License Warning 🔺 🔍 🐵 🔿 🔿	
System Identity Management	ent	e Portal Management pxGrid Services	Feed Service Threat Centric N	AC .			Click here to do wireless setup and visibility setup Do not show this again. $ imes$	
All Clients Web Clients Clapabilities Live Log Settings Certificates Permissions								
√ Enable Ø Disable Ø Approv	ve 😝 Group 👎 Decline 🔞 Delete	 Refresh Total Pending Approval(0) 	•				1-7 of 7 Show 25 y per page Page 1 🗘	
Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log		
ise-mnt-tim24adm		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate	View		
Ise-fanout-tim24adm		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View		
Ise-pubsub-tim24adm		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View		
ise-bridge-tim24adm		Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate	View		
Ise-admin-tim24adm		Capabilities(4 Pub, 2 Sub)	Online (XMPP)	Internal	Certificate	View		
Iseagent-firepower-20762a	2982d	Capabilities(0 Pub, 6 Sub)	Online (XMPP)		Certificate	View		
☐ ▶ firesightisetest-firepower-2	0762a	Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate	View		

步驟2.配置ISE以批准所有pxGrid基於證書的帳戶

1.導航到管理> pxGrid服務>設定。

2.選中覈取方塊:「自動批准基於證書的新帳戶」,然後按一下儲存。

cise	Identity Services Engine	Home Conte	xt Visibility	s Policy	 Administration 	Work Centers
•	System Identity Management	Network Resources	Device Portal Manage	ment pxGrid Se	rvices + Feed Se	rvice + Threat Centric NAC
A	Il Clients Web Clients Capa	bilities Live Log	Settings Certificates	Permissions		
	PxGrid Settings					
	 Automatically approve new cer Allow password based account 	tificate-based accounts creation				
	Use Default Save					
	Test					
Con	nected to pxGrid tim24adm.rtpaaa.n	et				

注意:如果未啟用此選項,管理員必須手動批准與ISE的FMC連線。

步驟3.匯出ISE MNT管理員證書和pxGrid CA證書

1.定位至管理>證書>系統證書。

2.如果未在「主要管理」節點上啟用,請展開「主要監視(MNT)」節點。

3.使用Used-By "Admin"欄位選擇證書。

注意:本指南使用管理員使用的預設ISE自簽名證書。如果您使用證書頒發機構(CA)簽名的管理員證書,請匯出在ISE MNT節點上簽名的管理員證書的根CA。

4.按一下**匯出**。

5.選擇匯出證書和私鑰的選項。

6.設定加密金鑰。

7. Export和Save檔案,如下圖所示。

dentity Services Engine	Home + Context Visibility + Operations +	Policy Administration	Work Centers				License Warning 📥 🔍 🔍 🔘 🔘	
System Hontity Management	Network Resources	pxGrid Services + Feed Service	te + Threat Centric NAC					
Deployment Licensing - Certificates	s + Logging + Maintenance Upgrade + Back	up & Restore + Admin Access	+ Settings					
0	-							
* Certificate Management	System Certificates 🛕 For disaster recovery it	is recommended to experience	ate and private key pairs of all system	n certificates.				
System Certificates	📝 Edit. 🕂 Generate Self Signed Certificate 🔒	- Import 🕃 Export 🗶 Del	iete 🔎 View					
Trusted Certificates	Friendly Name	Used By Po	artal group tag	Issued To	Issued By	Valid From	Expiration Date	
OCSP Client Profile	▼ tim24adm							
Certificate Signing Requests Certificate Periodic Check Setti	OU+Certificate Services System Certificate e.CN+tim24adm.rtpaaa.net#Certificate Se rvices Endpoint Sub CA - tim24adm#0000	pxGrid				Thu, 29 Mar 2018	Thu, 30 Mar 2028 🕑	
Certificate Authority	OverSAML Self-signed sami server certificate - CN+SAML Sm24ar/m rtnaaa net	SAML				Fri, 30 Mar 2018	Sat, 30 Mar 2019 🛃	
	Default self-signed server certificate	EAP Authentication, Admin, Del	fault Portal Certificate Group 👔			Fri, 30 Mar 2018	Sat, 30 Mar 2019 🛃	
Export Cer	tificate 'Default	self-signe	ad server o	ertificate	r		×	
			○ Export	Certificate (Dnly			
			Export	Certificate a	and Private Key			
	*Private Ke	y Password	•••••					
	*Confirr	n Password	•••••					
Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private key.								
						E	cport Cancel	

9.返回ISE系統證書螢幕。

10.使用「使用者」列中的「pxGrid」用法確定證書上的「頒發者」欄位。

註:在舊版ISE中,這是一個自簽名證書,但自2.2起,預設情況下此證書由內部ISE CA鏈頒 發。

11.選擇「Certificate」,然後按一下**View**,如下圖所示。

dealer Identity Services Engine	Home + Context Visibility + Operations	Policy Administration	Work Centers			Liten	ie Warning 📥 🔍 0 O	0	
* System + Identity Management	Network Resources	pxGrid Services	ervice + Threat Centric NAC						
Deplayment Liconsing -Contributes + Logging + Maintenance Upgrade + Backup & Restore + Admin Access + Settings									
Certificate Management	System Certificates 🛕 For disaster recovery	it is recommended to export cer	rtificate and private key pairs of all system ce	rtificates.					
System Certificates	🖌 Edit. 🕂 Generate Self Signed Certificate	🕂 Import 🕃 Export 🗙	Delete View						
Trusted Certificates	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date		
OCSP Client Profile	▼ tim24adm								
Certificate Signing Requests	OU=Certificate Services System Certificate e,CN=tim24adm.rtpaaa.net#Certificate Se	oxOrid				Thu, 29 Mar 2018	Thu, 30 Mar 2028 🛃		
Certificate Periodic Check Set5	 Nices Endpoint Sub CA - tm24admil0000 1 					-			
Certificate Authority	 Default self-signed sami server certificate CN=SAML_tim24adm.rtpasa.net 	SAML				Fri, 30 Mar 2018	Sat, 30 Mar 2019 🛃		
	 Default self-signed server certificate 	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group ④			Fri, 30 Mar 2018	Sat, 30 Mar 2019 🗾		

12.確定頂級(根)證書。在本例中為「Certificate Services Root CA - tim24adm」。

13.關閉「certificate view(證書檢視)」視窗,如下圖所示。



Close

14.展開ISE證書頒發機構選單。

15.選擇證書頒發機構證書。

16.選擇已識別的根證書,然後按一下**匯出。**然後儲存pxGrid根CA證書,如下圖所示。

dentity Services Engine	Home	Context Visibility Operation	ns → Policy ▼A	dministration + Work Centers					License Warning 🔺	s o o o
System Identity Management	Network	Resources	ement pxGrid Service	s + Feed Service + Threat Cent	ric NAC					
Deployment Licensing Certificates	s + Lo	gging Maintenance Upgrade	 Backup & Restore 	Admin Access Settings						
• •										
Certificate Management	CAC	ertificates								
- Certificate Authority	1	idit 👍 Import 🕃 Export 🗙	Delete 🔎 View 🔮	Refresh						
Outpring A		Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiration Status
Charles	🔻 tin	124adm								
Issued Certificates	0	Certificate Services Endpoint Sub CA - tim24adm#000003	Enabled	Infrastructure,Endpoints	32 D2 72 55 A9 7D 40 13 8F 2A EF CF 0D 1C 41 AB	Certificate Services Endpoint Sub	Certificate Services Node CA -	Thu, 29 Mar 2018	Thu, 30 Mar 2028	1
Certificate Authority Certificates		Certificate Services Root CA - tim24adm#00001	Enabled	Infrastructure,Endpoints	36 67 74 15 A6 A8 4F EB B7 46 1 E7 37 1A AB 88	Certificate Services Root CA - tim24adm	Certificate Services Root CA - tim24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2028	
Certificate Templates	0	Certificate Services Node CA - tim24adm#00002	Enabled	Infrastructure,Endpoints	30 1A 22 E7 AA E5 45 35 8C 65 7B EE 53 09 34 3E	tim24adm	tim24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2028	
External CA Settings		Certificate Services OCSP Responder - tim24adm#00004	Enabled	Infrastructure,Endpoints	74 C2 35 B8 32 6A 40 0F AC C8 D0 B9 51 DC 07 7D	Certificate Services OCSP Responder - tim24adm	Certificate Services Node CA - tim24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2023	

配置FMC

步驟4.向FMC新增新領域

1. 訪問FMC GUI並導航至System > Integration > Realms。

2. 按一下 New Realm ,如下圖所示。									
Overview Analysis Policies Devices Objects AMP Intelligence						Deploy	🖉 🌒 System	n Help v	admin v
	Configuration	Users	Domains	Integration	Updates	Licenses v	Vath v M	tonitoring •	Tools •
Cisco CSI Realms Identity Sources eStreamer Host Input Client Smart Software Satellite									
							🥖 Compare	realms	lew realm

3.填寫表單並按一下「測試Active Directory(AD)加入」按鈕。

注意:AD加入使用者名稱必須採用使用者主體名稱(UPN)格式,否則測試失敗。

4.如果測試AD加入成功,請按一下確定。

Add New Realm				?	×
Name *	ISEpxGrid	••••			
Description	Realm for use with pxGrid				
Туре *	AD	~			
AD Primary Domain *			ex: domain.com		
AD Join Username			ex: user@domain		
AD Join Password		••••	Test AD Join		
Directory Username *	admin		ex: user@domain		
Directory Password *		••••			
Base DN *	CN=Users,DN=rtpaaa,DN=net		ex: ou=user,dc=cisco,dc=com		
Group DN *	DN=rtpaaa,DN=net		ex: ou=group,dc=cisco,dc=com		
Group Attribute	Member	~			
* Required Field					
			OK Cancel		

5.按一下Directory頁籤,然後按一下Add directory,如下圖所示。

Overview Analysis Policies Devices Objects AMP Intelligence						Deploy	🖉 🛇 Syr	stem Help +	admin v
	Configuration	Users	Domains	Integration	Updates	Licenses •	Health +	Monitoring •	Tools •
Enter Turscion Directory Realm Configuration User Download								Save .	Cancel
								0 ^	dd directory

6.配置IP/主機名並測試連線。

注意:如果測試失敗,請在「領域配置」頁籤上驗證憑據。

7.按一下**確定**。

Edit directory		? ×
Hostname / IP Address		
Port	389	
Encryption	🔵 STARTTLS 📉 LDAPS 💽 None	
SSL Certificate	✓ ⊙	
	ОК Теst	Cancel
Status		
(i) Test	connection succeeded	
	ОК	
8.按一下 User Downlo	ad頁籤。	
LAB	Configuration Users Domains Integration Updates Licens	as v Health v Monitoring v Tools v

9.如果尚未選擇,請啟用使用者和組下載

10.按一下「立即下載」

Directory Realm Configuration User Downloa

LAB

LAB Enter Descri	ption]
Directory	Realm Configuration	User Download	
Downloa Begin autor	nd users and groups matic download at 8 V load Now	PM V America/New York	Repeat Every 24 ¥ Hours

11.填寫清單後,新增所需的組,然後選擇Add to Include。

12.儲存領**域配置**。

Overview Analysis Policies Devices Objects AMP In	ntelligence				Deploy O System Help + admin +
			Configuration Users	Domains Integration	Updates Licenses + Health + Monitoring + Tools +
	-				
LAB	-				Tou have unsaved changes To Save Cancel
Enter Description					
Directory Realm Configuration User Download					
Download users and groups					
Benin automatic download at a w say w America/New York Renas	t Every Da W Hours				
when the second se	a cruf 24 · main				
Available Groups C		Groups to Include (35)		Groups to Exclude (0)	
0 Search by name		📌 NetOps	8	None	
A NetCos		SQLServer2005SQLBrowserUserSRTPAAA-DC2	8		
SOLServer2005SOLBrowserUserSRTPAAA-DC2		Administrators &	8		
A WSUS Administrators		A Enterprise Read-only Domain Controllers	8		
B Enterprise Read-only Domain Controllers		🝰 DnsUpdateProxy	8		
A DosUpdateProxy		👍 jhoehn-group	8		
A thoshs-aroup		A Denied RODC Password Replication Group	8		
Denied RODC Password Replication Group		🝰 Domain Admins	8		
Domain Admins		🝰 Child	8		
A Child		🝰 DnsAdmins	8		
A DosAdmins		a Lester\Made\Me\Do\It	8		
A Lester/Made/Me\Do\Jt		🝰 Group Policy Creator Owners	8		
A Group Policy Creator Owners		₫ INE	8		
A INE		🔶 🍰 Domain Users	8		
A Domain Users		A ChadTest	8		
🝰 ChadTest		- A Read-only Domain Controllers	8		
A Read-only Domain Controllers	Include	AAS and IAS Servers	8		
ARAS and IAS Servers	Add to	Cert Publishers	8		
🝰 Cert Publishers	Exclude	🔄 💣 Schema Admins	8		
🝰 Schema Admins		A WSUS Reporters	8		
A WSUS Reporters		af Parent	8		
🔗 Parent		at ISE Admins	8		
🝰 ISE Admins		WinRMRemoteWMIUsers	8		
A WinAMRemoteWMIUsers		Allowed RODC Password Replication Group	8		
Allowed RODC Password Replication Group		2 TimSponsors	8		
A TimSponsors		# AllowedVPN	8		
🝰 AllowedVPN		Enterprise Admins	3		
💣 Enterprise Admins		2 test-users	8		
🝰 test-users		at sponsors	3		
a sponsors		MerpubraryUpdaters	8		
A HelpLibraryUpdaters		Protected Users	8		
Protected Users		Pompio Computers	8		
Domain Guests		Domain Computers	0		
Domain Computers		contain controllers	8.0		
Domain Controllers		Enter User Inclusion	Add	Enter User Exclusion	Add
A Charactele Descrite Casterline					

13.啟用「領域狀態」。

Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence									Deploy	🕘 🔍 Sy	stem Help	• admin •
										Configuration	Users	Domains	Integration	Updates	Licenses +	Health •	Monitoring	g • Tools •
Cisco CSI	Realms	Identit	y Sources	eStream	r H	fost Input Client	Smart Software Satellite											
																Com	pare realms	O New realm
Name								Description	Domain	Туре		Base DN	Group	DN	Group Atte	libute	State	
LAB									Global	AD		DC=rtpaaa,DC=	net CN=U	sers,DC=rtpaaa	,DC+ member			± 🥒 🐚 🗊

步驟5.生成FMC CA證書

1.導覽至**對象>對象管理>內部CA**,如下圖所示。

Overview Analysis Polici	es Devices Objects AMP Intelligence			Deploy 🔺 Syst	tem Help v a	dmin v
Object Management Intro	sion Rules			Add Network •	🔍 Filter	_
Retwork	Name	Value	Туре		Override	
JP Port			Control of		~	
S Interface	ary .		0.00	P	^	
Application Filters	any-ipv4		Netw	ork	×	
S VLAN Tag	any-ipv6 Host Dv4-Benchmark-Tests Netw	Host		×		
URL Contraction		ork	×			
Time Range	IPv4-Link-Local		Netw	ork	×	
\$ Variable Set	IPv4-Multicast		Netw	ork	×	
 Security Intelligence Network Lists and Feeds 	IPv4-Private-10.0.0.0-8		Netw	ork	×	
DNS Lists and Feeds	IPv4-Private-172.16.0.0-12 N IPv4-Private-192.168.0.0-16 N IPv4-Private-AR-MPC1918 O	ork	×			
URL Lists and Feeds		Netw	ork	x		
File List		Group	p	×		
Distinguished Name	IPv4-IPv4-Mapped		Netw	ork	×	
Cibject Groups	IPv6-Link-Local		Netw	ork	×	
a PKI	1Pv6-Private-Unique-Local-Addresses		Netw	ork	×	
Trusted CAs	IPv6-to-IPv4-Relay-Anycast		Netw	ork	×	
External Certs Internal Certs Cert Enrollment Internal CA Groups Internal CA Groups Internal CA Groups Internal Cert Groups External Cert Groups						

2.按一下**生成CA**。

3.填寫該表單並按一下Generate self-signed CA。

Name				Value	
Ģ	Generate Internal Certificate	Authority	? ×]	
	Name:	LabFP623	B		
	Country Name (two-letter code):	US			
	State or Province:	NC			
	Locality or City:	RTP			
	Organization:	Cisco			
	Organizational Unit (Department):	TAC			
	Common Name:				

4.生成完成後,按一下生成的CA證書右側的鉛筆,如下圖所示。

Overview	Analysis	Policies	Devices	Objects	AMP Intelligence	De	ploy 🛕 System H	elp + admin +
Object Man	agement	Intrusion	Rules					
						Cenerate CA	O Import CA	
Network		N	ame			Value		
Port Interface	,	u	bFP623			CN+LabFP623.rtpaaa.net, ORG+Cisco, OU=TAG	., C=US	/ 8

5.按一下「Download」。

Name:	LabFP623		
4 Subje	ect:		
Co	ommon Name:		
Or	rganization: Cisco		
Or	ganization Unit: TAC		
Issue	r:		
Co	ommon Name:		
Or	rganization: Cisco		
Or	ganization Unit: TAC		
Not V	alid Before:		
Ma	ay 15 18:13:52 2018 GMT		
Not V	alid After:		
Ma	ay 12 18:13:52 2028 GMT		
Serial	Number:		
a	2:1e:98:52:be:2f:b8:98		
Certif	icate Fingerprint:		
C7	2:D7:99:F3:EE:41:5C:7B:36:91:40:04:F7:1D:22:4C:60:C2:3C:9C		
Public	: Key Fingerprint:		
b5	1aabcb2cb25e922fdf6c0088771fca794897a1		
Dow	nload	OK	Capcel

6.配置並確認加密密碼,然後按一下OK。

7.將公鑰加密標準(PKCS)p12檔案儲存到本地檔案系統。

步驟6.使用OpenSSL從產生的憑證中提取憑證和私密金鑰

此操作在FMC的根目錄上或在任何支援OpenSSL命令的客戶端上完成。此示例使用標準的Linux shell。

1.使用openssl從p12檔案中提取憑證(CER)和私鑰(PVK)。

2.提取CER檔案,然後配置FMC上證書生成的證書匯出金鑰。

~\$ openssl pkcsl2 -nokeys -clcerts -in <filename.pl2> -out <filename.cer>
Password:
Last login: Tue May 15 18:46:41 UTC 2018
Enter Import Password:
MAC verified OK
3.提取PVK檔案,配置證書匯出金鑰,然後設定新的PEM密碼短語並進行確認。

~\$ openssl pkcs12 -nocerts -in <filename.p12> -out <filename.pvk>
Password: Last login: Tue May 15 18:46:41 UTC 2018 Enter Import Password: MAC verified OK
4.下一步需要使用PEM短語。

步驟7.將證書安裝到FMC

1.導航到對象>對象管理> PKI >內部證書。

2.按一下「Add Internal Cert」,如下圖所示。

Overview Analysis	Policies Devices Ob	ects AMP Intelligence				Deploy 📀	System Help +	admin v
Object Management	Intrusion Rules							
								-
						Add Internal Cert	Sector Filter	-
Retwork	Name				Value			
JP Port								0 -
4 Interface	TIMPP623				CN=1imPP623.rtpasa.net, OkG-	-CISCO, OU=TAC, C=US		00
n Tunnel Zone								
Application Filters								
🛞 VLAN Tag								
G URL								
Geolocation								
Time Range								
\$ Variable Set								
 Security Intelligence 								
Network Lists and	Feeds							
ONS Lists and Feet	ds							
URL Lists and Feed	ds							
Sinkhole								
C File List								
Opher Suite List								
Distinguished Name								
Individual Objects								
Cobject Groups								
a 🔑 PKI								
Internal CAs								
Trusted CAs								
External Certs								
Internal Certs								
Cert Enrollment								
Thermal CA Groups	a							
Trusted CA Groups								
Enternal Cert Group	(pa							
Excernal Cert Grou	100							

3.配置內部證書的名稱。

4.瀏覽到CER檔案的位置並將其選中。填寫「Certificate Data」後,選擇第二個。

5.瀏覽選項並選擇PVK檔案。

6.刪除PVK部分中的任何前導「Bag attributes」和所有尾隨值。PVK以-----BEGIN ENCRYPTED PRIVATE KEY(開始加密私鑰)開頭,以-----END ENCRYPTED PRIVATE KEY(結束加密私鑰)結束。

註:如果PVK文本的前導和尾隨連字元之外有任何字元,則無法按一下**OK**。

7. 選中Encrypted框並配置在步驟6匯出PVK時建立的密碼。

8.按一下**確定**。

Add Known Internal Certificate

Name: TZfpcert
Certificate Data or, choose a file: Browse
BEGIN CERTIFICATE MIIDfTCCAmWgAwIBAgIJAKIemFK+L7iYMA0GCSqGSIb3DQEBCwUAMGQxCzAJBgNV BAYTAIVTMQswCQYDVQQIDAJOQzEMMAoGA1UEBwwDUIRQMQ4wDAYDVQQKDAVDaXNj bzEMMAoGA1UECwwDVEFDMRwwGgYDVQQDDBNMYWJGUDYyMy5ydHBhYWEubmV0MB4X DTE4MDUxNTE4MTM1MIoXDTI4MDUxMjE4MTM1MIowZDELMAkGA1UEBhMCVVMxCzAJ BgNVBAgMAk5DMQwwCgYDVQQHDANSVFAxDjAMBgNVBAoMBUNpc2NvMQwwCgYDVQQL DANUQUMxHDAaBgNVBAMME0xhYkZQNjIzLnJ0cGFhYS5uZXQwggEiMA0GCSqGSIb3 DQEBAQUAA4IBDwAwggEKAoIBAQDMjtS5IUIFiZkZK/TSGtkOCmuivTK5kk1WzAy6 D7Gm/c69cXw/VfIPWnSBzhEkiRTyspmTMdyf/4TJvUmUH60h108/8dZeqJOzbjon
Bag Attributes Ioowse IocalKeyID: C7 D7 99 F3 EE 41 5C 7B 36 91 40 04 F7 1D 22 4C 60 C2 3C 9C Key Attributes: <no attributes=""> MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQI5uV3MsiHZsICAggA MBQGCCqGSIb3DQMHBAhgGVm1+xHLIASCBMjjJxkffXUNUcdB22smybvWotwbcRrt xL0qjEStmwuyExVp+TWC3AyIJN1DE7/rRssjRAqsnSOxIvDGmg0dVsvnbbqZwjFP 74POu/O2Vy99iFoVgW2q9DyXyL/h64TH9CZtwLKIOGOeEunNKpamDnpfyN8QC4DC fXvNZ9/NG4HrEcFmnnij0EwJ0QT8Jn5gAUj+AIPMe32zPqwoccRNYrRXMVM9+Jwp</no>
C Encrypted, and the password is:
OK Cancel
cfCJU2QGI4jT0SorN4u2Lk+S+Qd1s7Ii2wIQMWKPI2R9UGv1tyM6HTPCGoCo6VDI acClCUAsecVrYY081GKTVVJ3bWgWfPtR3OH12YCA2whcCKcG50MByB4tjhHN036q O/g= END_ENCRYPTED_PRIVATE_KEY ← DELETE
Encrypted, and the password is:
OK Cancel

步驟8.將FMC證書匯入ISE

1.訪問ISE GUI並導航到管理>系統>證書>受信任證書。

2.按一下**匯入**。

dentity Services Engine	Home + Context Visibility + Operations + Polic	• Administra	tion + Work Centers						L	icense Warning 🔺 🔗	
System + Identity Management	Network Resources Device Portal Management pxG	rid Services + F	eed Service + Threat Cer	tric NAC							
Deployment Licensing - Certificate	es + Logging + Maintenance Upgrade + Backup &	Restore + Admi	n Access + Settings								
0											
Certificate Management	Trusted Certificat										
System Certificates	/Edit -Import @Export X Delete PView								5	ihow All	- 8
Trusted Certificates	Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiration Status		
OCSP Client Profile	Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 89	Baltimore CyberTrust Ro	Baltimore CyberTrust Ro	Fri, 12 May 2000	Mon, 12 May 2025	.		
Certificate Signing Requests	Cisco CA Manufacturing	Disabled	Endpoints Infrastructure	6A 69 67 B3 00 00	Cisco Manufacturing CA	Cisco Root CA 2048	Fri, 10 Jun 2005	Mon, 14 May 2029			
Certificate Periodic Check Setti	Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure	02	Cisco Manufacturing CA	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037	2		
Certificate Authority	Cisco Root CA 2048	Disabled	Infrastructure Endpoints	SF F8 78 28 28 54	Cisco Root CA 2048	Cisco Root CA 2048	Fri, 14 May 2004	Mon, 14 May 2029			
	Cisco Root CA M2	Enabled	Endpoints Infrastructure	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037			
	Default self-signed server certificate	Enabled	Endpoints Infrastructure	5A BE 7E D8 00 00	tim24adm.rtpaaa.net	tim24adm.rtpaaa.net	Fri, 30 Mar 2018	Sat, 30 Mar 2019			
	DigiCert root CA	Enabled	Endpoints Infrastructure	02 AC 5C 26 6A 08	DigiCert High Assurance	DigiCert High Assurance	Thu, 9 Nov 2006	Sun, 9 Nov 2031			
	DigiCert SHA2 High Assurance Server CA	Enabled	Endpoints Infrastructure	04 E1 E7 A4 DC SC	DigiCert SHA2 High Ass	DigiCert High Assurance.	Tue, 22 Oct 2013	Sun, 22 Oct 2028			
	DST Root CA X3 Certificate Authority	Enabled	Cisco Services	44 AF B0 80 D6 A3	DST Root CA X3	DST Root CA X3	Sat, 30 Sep 2000	Thu, 30 Sep 2021	2		
	HydrantID SSL ICA G2	Enabled	Cisco Services	75 17 16 77 83 D0	HydrantID SSL ICA G2	QuoVadis Root CA 2	Tue, 17 Dec 2013	Sun, 17 Dec 2023	1		
	QuoVadis Root CA 2	Enabled	Cisco Services	05 09	QuoVadis Root CA 2	QuoVadis Root CA 2	Fri, 24 Nov 2006	Mon, 24 Nov 2031	1		
	Thawte Primary Root CA	Enabled	Cisco Services	34 4E D5 57 20 D5	thawte Primary Root CA	thawte Primary Root CA	Thu, 16 Nov 2006	Wed, 16 Jul 2036	2		
	TimFP623	Enabled	Infrastructure Endpoints	BE F9 42 3D 25 AS	TimFP623.rtpaaa.net	TimFP623.rtpaaa.net	Tue, 15 May 2018	Fri, 12 May 2028	2		
	VertSign Class 3 Public Primary Certification Authority	Enabled	Cisco Services	18 DA D1 9E 26 7D	VeriSign Class 3 Public	VeriSign Class 3 Public	Tue, 7 Nov 2006	Wed, 16 Jul 2036	2		
	VeriSign Class 3 Secure Server CA - G3	Enabled	Cisco Services	6E CC 7A A5 A7 03	VeriSign Class 3 Secure	VeriSign Class 3 Public	Sun, 7 Feb 2010	Fri, 7 Feb 2020			

3.按一下Choose File,然後從本地系統中選擇FMC CER檔案。

可選:配置友好名稱。

4.檢查ISE內的Trust身份驗證。

可選:配置說明。

5.按一下「Submit」,如下圖所示。

Import a new Certificate into the Certificate Store

* Certificate File	Choose File TZfpcert.cer	
Friendly Name		(i)
\ \	Trusted For: 🥡	
	✓ Trust for authentication within ISE	
	Trust for client authentication and Syslog	
	Trust for authentication of Cisco Services	
	Validate Certificate Extensions	
Description		
	Submit Cancel	

步驟9.在FMC上配置pxGrid連線

1.導覽至System > Integration > Identity Sources,如下圖所示。

Overview Analysis Policies Devices Objects AMP Intelligence					Deploy	ି 🧟 🎙	ystem Help v	admin v
	Configuration	Users	Domains Integration	Updates	Licenses •	ealth •	Monitoring •	Tools •
Cisco CSI Realms Identity Sources eStreamer Host Input Client Smart Software Satellite								
2.按一下ISE。								
3. 能直ISE pxGrld即點的IP地址或土機名。								
▲選擇∞vCrid伺肥哭CAナ側的」								
4.选择PXGIIU们版品CAU则的+。								

5.命名伺服器CA檔案,然後瀏覽到步驟3中收集的pxGrid根簽名CA。然後按一下Save。

6.選擇MNT Server CA右側的+。

7.命名伺服器CA檔案,然後瀏覽到步驟3中收集的Admin證書。然後按一下Save。

8.從下拉選單中選擇FMC CER檔案。

Identity Sources			
Service Type	None Identity Services Engine	User Agent	
Primary Host Name/IP Address *	<ise address="" ip="" node="" pxgrid=""></ise>	8	
Secondary Host Name/IP Address			
pxGrid Server CA *	ISE24InternalRoot	•	\odot
MNT Server CA *	ISE24SelfSigned	~	
FMC Server Certificate *	TimFP623	*	0
ISE Network Filter			ex. 10.89.31.0/24, 192.168.8.0/24,
* Required Field	Test		

9.按一下**測試**。

10.如果測試成功,請按一下確定,然後按一下螢幕右上角的儲存。

Status



注意:運行兩個ISE pxGrid節點時,一個主機顯示成功(Success)和一個主機顯示失敗 (Failure)是正常現象,因為pxGrid一次只在一個ISE節點上主動運行。這取決於配置哪個主主 機可能會顯示Failure,哪個輔助主機可能會顯示Success。這取決於ISE中的哪個節點是活動 的pxGrid節點。

驗證

在ISE中驗證

1.開啟ISE GUI並導航到管理> pxGrid服務。

如果成功,客戶端清單中將列出兩個firepower連線。一個用於實際FMC(iseagent-hostname-33bytes),另一個用於測試裝置(firesightistest-hostname-33bytes)。

-dade case	Identity Services Engine	Home + Context Visibility	Operations Policy Adm	inistration + Work Centers				License Warning 🔺 🔍 🤤 😋	o 0
+ Syt	stem + Identity Management	Network Resources Pevic	e Portal Management pxGrid Services	+ Feed Service + Threat Cen	tric NAC				
AI C	lients Web Clients Cap	abilities Live Log Settings	Certificates Permissions						
√tre	able 🙆 Disable 🕝 Approve	😝 Group 📫 Decline 🔞 Delete	 Refresh Total Pending Approval(0) 	*				1-7 of 7 Show 25 + per page Page	1 🗘
	Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log		
			Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate	Vew		
			Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View		
			Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	Vew		
			Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate	View		
			Casabilities(4 Pub. 2 Sub)	Online (XMPP)	Internal	Certificate	Vew		
			Capabilities(0 Pub, 6 Sub)	Online (XMPP)		Certificate	View		
			Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate	View		
					(C)				

iseagent-firepower連線顯示六(6)個子並線上顯示。

firesightistestest-firepower連線顯示零(0)個子網,並且顯示為離線。

iseagent-firepower客戶端的展開檢視顯示六個訂閱。

 iseagent-firepower-20762a2982d 	Ca	pabilities(0 Pub, 6 Sub)	Online (XMPP)		Certificate	View		
	Cap	ability Detail			1 - 6 of 6	Show 25 - per page	a Page 1	\$
		Capability Name	Capability Version	Messaging Role	Message Filter			
	0	AdaptiveNetworkControl	1.0	Sub				
	0	Core	1.0	Sub				
	0	EndpointProfileMetaData	1.0	Sub				
	0	EndpointProtectionService	1.0	Sub				
	0	SessionDirectory	1.0	Sub				
	0	TrustSecMetaData	1.0	Sub				

註:由於Cisco錯誤<u>IDCSCvo75376</u>存在主機名限制,批次下載失敗。FMC上的測試按鈕顯示 連線故障。這會影響2.3p6、2.4p6和2.6。當前建議運行2.3補丁5或2.4補丁5,直到發佈正式 補丁。

在FMC中驗證

1.開啟FMC GUI並導航至分析>使用者>活動會話。

通過ISE中的會話目錄功能發佈的所有Active Sessions都顯示在FMC上的Active Sessions表中。

C	Overview Analysis Policies Devices Objects AMP Intelligence Depicy @ System Help + admin +															
C	ontext Exp	lorer Connection	s • Intrusions •	Files • Hosts •	Users + Active Sessi	Vulnerabilities	Correlation •	Custom •	Lookup •	Search						
													Bookmark This Pa	ige Report De	signer Dashboard View Bookm	arks Search •
Active Sessions																
							Info No devices reg <u>Click here to re</u>	istered. egister a devic	<u>e.</u>	×						
Table View of Active Sessions > Active Sessions																
Search Constraints (<u>ddt, Search</u>) Disabled Column												Disabled Columns				
Jump to •																
1		Login Time ×	Last Seen ×	User ×	Authe	ntication Type × C	Ourrent IP ×	Realm ×	Username ×	First Name >	Last Name ×	E-Mail ×	Department ×	Phone ×	Discovery.Application ×	Device ×
	¥ 0 7	018-05-15 13:26:21	2018-05-15 13:27:36	xiao yao (LAB\xia	wao.LDAP) Passive	Authentication	1	LAB					users (rtoaaa)		LDAP	fireqower
	4 D 2	018-05-15 12:35:54	2018-05-15 12:35:54	admin admin (LA	Bladmin, LDAP) Passive	Authentication	1	LAB					users (rtoaaa)		LDAP	fireqower
	š 🗆 2	018-05-15 11:27:14	2018-05-15 11:27:14	tom (LAB\tom, L	DAP) Passive	Authentication	1	LAB					users (rtoaaa)		LDAP	firecower
	4 🗆 2	018-05-15 11:20:30	2018-05-15 11:20:30	lark kent (LAB)a	uperman_LDAP) Passive	Authentication	1	LAB					users (rtoaaa)		LDAP	firequier
1	I< < Page	1 of 1 >> Display	ing rows 1-4 of 4 rows													
	View View All	Logout)													

在FMC CLI sudo模式下,「adi_cli session」顯示從ISE傳送到FMC的使用者會話資訊。

ssh admin@<FMC IP ADDRESS>
Password:
Last login: Tue May 15 19:03:01 UTC 2018 from dhcp-172-18-250-115.cisco.com on ssh
Last login: Wed May 16 16:28:50 2018 from dhcp-172-18-250-115.cisco.com

Copyright 2004-2018, Cisco and/or its affiliates. All rights reserved. Cisco is a registered trademark of Cisco Systems, Inc. All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.2.3 (build 13) Cisco Firepower Management Center for VMWare v6.2.3 (build 83)

admin@firepower:~\$ sudo -i Password: Last login: Wed May 16 16:01:01 UTC 2018 on cron root@firepower:~# adi_cli session

received user session: username tom, ip ::ffff:172.18.250.148, location_ip ::ffff:10.36.150.11, realm_id 2, domain rtpaaa.net, type Add, identity Passive. received user session: username xiayao, ip ::ffff:10.36.148.98, location_ip ::, realm_id 2, domain rtpaaa.net, type Add, identity Passive. received user session: username admin, ip ::ffff:10.36.150.24, location_ip ::, realm_id 2, domain rtpaaa.net, type Add, identity Passive. received user session: username administrator, ip ::ffff:172.18.124.200, location_ip ::, realm_id 2, domain rtpaaa.net, type Add, identity Passive.

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

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)。