使用OpenSSL為IND和ISE pxGrid整合建立 SAN證書

目錄

簡介

本文檔介紹如何為Industrial Network Director(IND)和Identity Services Engine之間的pxGrid整合建 立SAN證書。

背景資訊

在Cisco ISE中為pxGrid使用建立證書時,無法將伺服器短主機名輸入到ISE GUI中,因為ISE僅允 許FQDN或IP地址。

若要建立包含主機名和FQDN的證書,必須在ISE之外建立證書請求檔案。可以使用OpenSSL建立 證書簽名請求(CSR)以及使用者替代名稱(SAN)欄位條目。

本文檔不包括在IND伺服器和ISE伺服器之間啟用pxGrid通訊的全面步驟。 在配置pxGrid並確認需 要伺服器主機名後,可以使用這些步驟。 如果在ISE探查器日誌檔案中發現此錯誤,通訊需要主機 名證書。

Unable to get sync statusjava.security.cert.CertificateException: No subject alternative DNS name match

有關使用pxGrid通訊的IND初始部署步驟,請訪問

https://www.cisco.com/c/dam/en/us/td/docs/switches/ind/install/IND_PxGrid_Registration_Guide_Final.pdf

需要的應用程式

- Cisco Industrial Network Director(IND)
- 思科身分識別服務引擎(ISE)
- OpenSSL
 - 在多數現代Linux版本以及MacOS中,OpenSSL包是預設安裝的。如果您發現命令不可用,請使用作業系統的軟體包管理應用程式安裝OpenSSL。
 - ◎ 有關OpenSSL for Windows的資訊,請訪問<u>https://wiki.openssl.org/index.php/Binaries</u>

其他資訊

就本檔案而言,使用下列詳細資訊:

- IND伺服器主機名: rch-mas-ind
- FQDN:rch-mas-ind.cisco.com
- OpenSSL配置: rch-mas-ind.reg
- 證書請求檔名: rch-mas-ind.csr
- 私鑰檔名:rch-mas-ind.pem
- 證書檔名: rch-mas-ind.cer

流程步驟

建立證書CSR

- 1. 在安裝了OpenSSL的系統上,為OpenSSL選項(包括SAN資訊)建立一個請求文本檔案。
 - 大多數「_default」欄位是可選的,因為可以在步驟10中運行OpenSSL命令時輸入答 #2。
 - SAN詳細資訊(DNS.1、DNS.2)是必需的,必須包括DNS短主機名以及伺服器的FQDN。 如果需要,可以使用DNS.3、DNS.4等新增其他DNS名稱。
 - 請求檔案文本檔案示例:

[req]

distinguished_name =名稱 req_extensions = v3_req

[名稱]

countryName =國家/地區名稱(2個字母代碼) countryName_default =美國 stateOrProvinceName =州或省名稱(全稱) stateOrProvinceName_default = TX localityName =城市 localityName_default = Cisco Lab organizationalUnitName =組織單位名稱(例如IT) organizationalUnitName_default = TAC commonName =公用名(例如,您的姓名) commonName max = 64 commonName default = rch-mas-ind.cisco.com emailAddress =電子郵件地址 emailAddress max = 40 [v3 reg] keyUsage = keyEncipherment, dataEncipherment extendedKeyUsage = serverAuth, clientAuth subjectAltName = @alt names [alt_names] DNS.1 = rch-mas-ind DNS.2 = rch-mas-ind.cisco.com

檔案。

指令:

openssl req -newkey rsa:2048 -keyout <server>.pem -out <server>.csr -config <server>.req

- 出現提示時, 輸入您選擇的密碼。 請務必記住此密碼, 如同在後續步驟中使用。

You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. Country Name (2 letter code) [US]: State or Province Name (Full Name) [TX]: City [Cisco Lab]: Organizational Unit Name (eg, IT) [TAC]: Common Name (eg, YOUR name) [rch-mas-ind.cisco.com]: Email Address []:

- 3. 如果需要,請驗證CSR檔案資訊。對於SAN證書,請檢查「x509v3 Subject Alternative
 - Name」(x509v3主題備用名稱),如本螢幕快照中突出顯示。
 - 命令列:

openssl req -in <server>.csr -noout -text



 4. 在文本編輯器中開啟CSR檔案。 出於安全原因,示例螢幕截圖不完整且經過編輯。 實際產生 的CSR檔案包含更多行。 -----BEGIN CERTIFICATE REQUEST-----MIIDMDCCAhgCAQAwfzELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAlRYMRIwEAYDVQQH DAlDaXNjbyBMYWIxDDAKBgNVBAsMA1RBQzEeMBwGA1UEAwwVcmNoLW1hcy1pbmQu Y21zY28uY29tMSEwHwYJKoZIhvcNAQkBFhJ3aXJhbnNvbUBjaXNjby5jb20wggEi MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDVkRpj307uFPRm2IboESQRqxRC NJ2n8bHzRxOwg4cePcUwu1m9E9Y45r1wG4NTmvylIn7AL4KwdTHdT9JDDiThInQS L6agDTXLhfe4R08Wrz3RbS3MBP/i1dxo8U+YmuHOUkVVS290D532DGj3uf8zye2D @iPa3xRQqggCBJ2H/99Y0XnFxj48PUqOGcLDFjaf3FhpRXa750em0FuBVG8k3BOW AAGgbDBqBgkqhkiG9w0BCQ4xXTBbMAsGA1UdDwQEAwIEMDAdBgNVHSUEFjAUBggr BgEFBQcDAQYIKwYBBQUHAwIwLQYDVR0RBCYwJIILcmNoLW1hcy1pbmSCFXJjaC1t YXMtaW5kLmNpc2NvLmNvbTANBgkqhkiG9w0BAQsFAAOCAQEAm1c4E6VKFZHnvGO+ krmNXv9nFq4PBz1x1RDsfdt9u0cVQo6EgJw+gBeI5FqQdsURLq12sZhdFXSaGY1h d4jeQq3aSB6UaOsDHRUeh7Bo069Q6QOLuQOowaDY9dK0Fy2CiqMLcUokb52h6SPv Af9qdA==

-----END CERTIFICATE REQUEST-----

5. 將私鑰檔案(<server>.pem)複製到PC,就像在後續步驟中所使用的一樣。

使用思科ISE生成證書,使用建立的CSR檔案資訊

在ISE GUI中:

- 1. 刪除現有的pxGrid客戶端。
 - 導航到Administration > pxGrid Services > All Clients。
 - 查詢並選擇現有的客戶機主機名(如果列出),
 - 如果找到並選定,請按一下「刪除」按鈕,然後選擇「刪除選定項」。根據需要進行確認。

2. 建立新證書。

- 按一下pxGrid服務頁面上的「證書」(Certificates)頁籤。
- 選擇選項:
 - 。「我想」:

"生成單個證書(包含證書簽名請求)"

。"證書簽名請求詳細資訊:

。從文字編輯器複製/貼上CSR詳細資訊。務必包括BEGIN和END行。

。"證書下載格式"

。"隱私增強型電子郵件(PEM)格式的證書,PKCS8 PEM格式的金鑰。"

- 輸入證書密碼並加以確認。
- 按一下「建立」按鈕。

Hentity Services Engine H	me Context Visibility Operations Policy Administration Work Centers
System → Identity Management → N	etwork Resources
All Clients Web Clients Capabilitie	s Live.Log Settings Certificates Permissions
Generate pxGrid Certificates	
I want to *	Generate a single certificate (with certificate signing request)
Certificate Signing Request Details *	BEGIN CERTIFICATE REQUEST MIIDMDCCAhgCAQAwtzELMAkGA1UEBhMCV/ItxCzAJBgNVBAgMAIRYINRiwEAYDVQQH
	DAIDaXNjbyBMYWbDDAKBgNVBASMA1RBQ2EeMBwGA1UEAwwVcmNoLW1hcy1pc2Uu yobygou/yobM85wAaw/ IKa2IbwAkACkREh 12ay IbbeAkAk IBia/Milw5k2ObwaaEi
Description	
Certificate Template	pxGrid_Certificate_Template
Subject Alternative Name (SAN)	· • • - +
Certificate Download Format*	Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain v
Certificate Password *	
Confirm Password *	
	Reset Create

- 這會建立和下載包含憑證檔案以及憑證鏈結的其他檔案的ZIP檔案。開啟ZIP並解 壓縮憑證。
 - ◎ 檔名通常為<IND server fqdn>.cer
 - ◎ 在ISE的某些版本中,檔名是<IND fqdn>_<IND短名稱>.cer

將新證書匯入到IND伺服器,並將其啟用以供pxGrid使用

在IND GUI中:

- 1. 禁用pxGrid服務,以便可以匯入新證書並將其設定為活動證書。
 - 導航到Settings > pxGrid。
 - 按一下可禁用pxGrid。

CISCO NETWORK DIRECTOR	Settings	>	pxGrid	
Cisco Platform Exchange Grid (px0 Identity Services Engine (ISE) pxGr	Grid) is an open, id controller. Thi	scala s infor	ble data-sharir mation can the	ng ai en be
Download .pem IND certificate	9			
Disable pxGrid Of Enable	e pxGrid			

2. 將新證書匯入系統證書。

- 導覽至Settings > Certificate Management。
- 按一下「System Certificates(系統證書)」
- 按一下「Add Certificate」。
- 輸入證書名稱。
- 按一下「Certificate」左邊的「Browse」,然後找到新的證書檔案。
- 按一下「Certificate」左邊的「Browse」,然後找到建立CSR時儲存的私鑰。
- 輸入之前使用OpenSSL建立私鑰和CSR時使用的密碼。
- 按一下「上傳」。

tetter.	NOISE NOTICE	Station Section	gn) Certificate Man	agement				
		AND CANTRALING & Contribution	ter(n)					
Π_{0}	0	Rate	leased to	All Syden Certificate			х.	
(arthore	0	poped	Oversity these does not course	Sata*	poper-location 2023			58.96
121	0	time-and	01-001-040-000-04-04-04-04-04-04-04-04-04-04-0	Certificate*	Reveal Computers was related and and			5810
	0	reprises	O-Case Systems, Direkti Opp	Private Key	Breete Champalitebras ad per-		0	0136
				Pataword	I	•	۰	
					Uptrail Canad			

- 3. 將新證書匯入為受信任的證書。
 - 導航到Settings > Certificate Management,點選Trusted Certificates。

- 按一下「Add Certificate」。
- 輸入證書名稱;該名稱必須不同於系統證書上使用的名稱。
- 按一下「Certificate」左側的「Browse」,然後找到新的證書檔案。
- 密碼欄位可以留空。
- 按一下「上傳」。

dada (Constant Constant	temoga > Certificate Man	aponent			
		Add Cardinana 1 Gard	Sficetw(x)				
Π_{0}	0	Natio	tenueri To	Add Trunked Certificate		×	No.
Contribution of	0	10,00,00	On-Deco Lonsing Red Dub-Deco	Same *	pagest tracked 2023		-01-30 Sec.40 47
100	0	Respondence for	On-Detailings, D-Detailings, Du-On	Carlificate"	Breese Characteristics can be been set on		
				Pressouri		•	
					Ushell Canol		
			Ð				

- 4. 設定pxGrid以使用新證書。
 - 導航到Settings(設定) > Certificate Management(證書管理),按一下Settings(設定)。
 - 如果尚未完成,請選擇「pxGrid」下的「CA證書」。
 - 選擇在證書匯入期間建立的系統證書名稱。
 - 按一下「儲存」。

在ISE伺服器中啟用並註冊pxGrid

在IND GUI中:

- 1. 導航到Settings > pxGrid。
- 2. 按一下滑塊以啟用pxGrid。
- 如果這不是第一次在該IND伺服器上向ISE註冊pxGrid,請選擇「使用現有節點連線」。
 自動填充IND節點和ISE伺服器資訊。
- 4. 要註冊新的IND伺服器以使用pxGrid,如果需要,請選擇「註冊新節點」。 輸入IND節 點名稱,並根據需要選擇ISE伺服器。
 - 如果ISE伺服器未列在伺服器1或伺服器2的下拉選項中,則可以使用Settings > Policy Server將其新增為新的pxGrid伺服器

AR PROPERTY	Settings) gallest				0	۰
bran pord Select	5					
(contrast period) calified						
C Connectificing the Encloy In Propose of Real Parks	-					
rill herver						
Tests (Sector)		factor 11		Server 2		
chese relations		 In the second second 		band a same		*
		Canad	Experime			

5. 點選註冊(Register)。確認資訊會顯示在螢幕上。

Message		×
pxGrid Node successfully	registered	
	ок	

在ISE伺服器中批准註冊請求

在ISE GUI中:

1. 導航到Administration > pxGrid Services > All Clients。 待批准請求顯示為「待批准總數(1)」

2. 點選「待批准總數(1)」,然後選擇「全部批准」。

-de-de- cisco Identity Services Engine Home + Context Visibility	Operations Policy Adr	ministration • Work Centers			
System Hentity Management Network Resources Device Performance	ortal Management pxGrid Services	Feed Service Threat Centrie	NAC		
All Clients Web Clients Capabilities Live Log Settings (Certificates Permissions				
🖋 Enable 🥝 Disable 🙄 Approve 😝 Group 🌻 Decline 🚱 Delete 🗸 🛞 Ra	efresh Total Pending Approval(1) +				
Client Name Description	Cap Approve All	Status	Client Group(s)	Auth Method	Log
ise-bridge-rch-mas-ise	Capadiaties(U Pub, 4 Sub)	Online (XMPP)	Internal	Certificate	View
ise-mnt-rch-mas-ise	Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate	View
ise-admin-rch-mas-ise	Capabilities(5 Pub, 2 Sub)	Online (XMPP)	Internal	Certificate	View
ise-fanout-rch-mas-ise	Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View
Ise-pubsub-rch-mas-ise	Capabilities(0 Pub, 0 Sub)	Offine (XMPP)		Certificate	View
rch-mas-ind.cisco.com	Capabilities(0 Pub, 0 Sub)	Pending		Certificate	View

3. 在顯示的彈出視窗中,按一下「全部批准」。



	Client Name	Description	Cap Approve All	Status	Client Group(s)	Auth Method	Log
□ ▶	ise-bridge-rch-mas-ise		Capabilloes(U PUD, 4 SUD)	Online (XMPP)	Internal	Certificate	View
□ ►	ise-mnt-rch-mas-ise		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate	View
□ ►	ise-admin-rch-mas-ise		Capabilities(S Pub, 2 Sub)	Online (XMPP)	Internal	Certificate	View
□ ►	ise-fanout-rch-mas-ise		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View
	ise-pubsub-rch-mas-ise		Capabilities(0 Pub, 0 Sub)	Offine (XMPP)		Certificate	View
	rch-mas-ind.cisco.com		Capabilities(0 Pub, 0 Sub)	Pending		Certificate	View

在IND伺服器中啟用pxGrid服務

在IND GUI中:

- 1. 導航到Settings > pxGrid。
- 2. 按一下「啟用」。

erver	
nisad peri IND certificate	
ana"	Server 1*
has-ise (isco com	nch-mas-ise coico com

3. 確認資訊會顯示在螢幕上。



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)。