配置ISE 2.4 pxGrid IND 1.6.1整合

目錄

簡介 必要條件 需求 採用元件 設定 高級流程圖 組態 步驟1.在ISE上配置終端自定義屬性 步驟2.使用自定義屬性配置Profiler策略 步驟3. 啟用用於分析實施的自定義屬性 步驟4.匯出IND身份證書 步驟5.將IND身份證書上傳到ISE受信任庫 步驟6.為IND生成證書 步驟7.下載PKCS12格式的證書鏈 步驟8.在IND上傳憑證鏈結 步驟9.在IND上配置策略伺服器 步驟10.在IND上配置pxGrid整合 步驟11.在ISE上批准IND 步驟12.在IND上啟用pxGrid服務 驗證 ISE驗證 IND驗證 疑難排解 IND上的同步狀態停滯在「不同步」狀態 並非所有終端都與ISE共用 assetTag和AssetGroup在ISE上不可用

簡介

本文檔介紹如何配置身份服務引擎(ISE)2.4和工業網路導向器1.6.1-4通過pxGrid(平台交換網格)的整合並對其進行故障排除。 Cisco IND在pxGrid中註冊為發佈者,並將終端屬性資訊發佈到ISE for IOTASSET Dictionary。

必要條件

需求

思科建議您瞭解以下主題的基本知識:

• 思科身分識別服務引擎

Cisco Industrial Network Director

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- •思科身分識別服務引擎版本2.4 p6
- •工業網路導向器1.6.1-4

設定

高級流程圖



1. IND通過ISE pxGrid節點上的pxGrid版本2向ISE註冊。來自IND(application.log)的對應日誌:

2019-05-22 14:31:17,770:INFO:qtp281049997-52711:PxgridPublisher:: Connect start 2019-05-22 14:31:17,770:INFO:qtp281049997-52711:PxgridPublisher:: Hostname:WIN2012-AAA IpAddress:10.62.145.130 2019-05-22 14:31:17,770:INFO:qtp281049997-52711:PxgridPublisher:: pxGrid RestBaseUrl:https://WIN2012-AAA:8910/pxgrid/ind/asset/ 2019-05-22 14:31:17,770:INFO:qtp281049997-52711:PxgridController:: Send Request ServiceRegister invoked with pxGridServer(s) [ISE24-1ek.example.com] 2019-05-22 14:31:17,770:INFO:qtp281049997-52711:PxgridController:: Sending ServiceRegister request to pxGridServer ISE24-lek.example.com 2019-05-22 14:31:17,786:INFO:qtp281049997-52711:PxgridController:: Request={"name":"com.cisco.endpoint.asset","properties":{"wsPubsubService":"com.cisco.ise.pubsub ", "restBaseUrl": "https://WIN2012-AAA:8910/pxgrid/ind/asset/","assetTopic":"/topic/com.cisco.endpoint.asset"}} 2019-05-22 14:31:17,911:INFO:qtp281049997-52711:PxgridController:: Response={"id":"76d4abaf-9efd-4c68-a046-79e049564902", "reregisterTimeMillis": "300000"} 2019-05-22 14:31:17,911:INFO:qtp281049997-52711:PxgridController:: Send Request ServiceLookup invoked with pxGridServer(s) [ISE24-lek.example.com] 2019-05-22 14:31:17,911:INFO:qtp281049997-52711:PxgridController:: Sending ServiceLookup request to pxGridServer ISE24-lek.example.com 2019-05-22 14:31:17,911:INFO:qtp281049997-52711:PxgridController::

Request={"name":"com.cisco.ise.pubsub"} 2019-05-22 14:31:17,911:INFO:qtp281049997-52711:PxgridController:: Response={"services":[{"name":"com.cisco.ise.pubsub","nodeName":"ise-pubsub-ise24lek","properties":{"wsUrl":"wss://ISE24-lek.example.com:8910/pxgrid/ise/pubsub"}}] 2019-05-22 14:31:17,911:INFO:qtp281049997-52711:PxgridPublisher:: wsUrl=wss://ISE24lek.example.com:8910/pxgrid/ise/pubsub 2019-05-22 14:31:17,911:INFO:qtp281049997-52711:PxgridController:: Send Request AccessSecret invoked with pxGridServer(s) [ISE24-lek.example.com] 2019-05-22 14:31:17,911:INFO:qtp281049997-52711:PxgridController:: Sending AccessSecret request to pxGridServer ISE24-lek.example.com 2019-05-22 14:31:17,926:INFO:qtp281049997-52711:PxgridController:: Request={"peerNodeName":"isepubsub-ise24-lek"} 2019-05-22 14:31:17,926:INFO:qtp281049997-52711:PxgridController:: Access Secret recieved 2019-05-22 14:31:17,926:INFO:qtp281049997-52711:PxgridController:: Client created **如目誌所示,IND已註冊assetTopic**

2. 啟用了pxgrid探測的ISE PSN批次下載現有的pxGrid資產(profiler.log):

```
2019-05-22 14:39:25,817 INFO [ProfilerINDSubscriberPoller-56-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- New services are: [Service
[name=com.cisco.endpoint.asset, nodeName=ind2, properties={wsPubsubService=com.cisco.ise.pubsub,
restBaseUrl=https://WIN2012-AAA:8910/pxgrid/ind/asset/,
assetTopic=/topic/com.cisco.endpoint.asset}]]
2019-05-22 14:39:26,011 INFO [ProfilerINDSubscriberPoller-56-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- NODENAME:ind2
2019-05-22 14:39:26,011 INFO [ProfilerINDSubscriberPoller-56-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- REQUEST
BODY{ "offset": "0", "limit": "500" }
2019-05-22 14:39:26,046 INFO [ProfilerINDSubscriberPoller-56-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Response status={}200
2019-05-22 14:39:26,046 INFO [ProfilerINDSubscriberPoller-56-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Content: "OUT_OF_SYNC"
2019-05-22 14:39:26,047 INFO [ProfilerINDSubscriberPoller-56-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Status is :"OUT_OF_SYNC"
2019-05-22 14:39:26,047 DEBUG [ProfilerINDSubscriberPoller-56-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Static set after adding new services:
[Service [name=com.cisco.endpoint.asset, nodeName=ind,
properties={wsPubsubService=com.cisco.ise.pubsub, restBaseUrl=https://WIN2012-
AAA:8910/pxgrid/ind/asset/, assetTopic=/topic/com.cisco.endpoint.asset}], Service
[name=com.cisco.endpoint.asset, nodeName=ind2, properties={wsPubsubService=com.cisco.ise.pubsub,
restBaseUrl=https://WIN2012-AAA:8910/pxgrid/ind/asset/,
assetTopic=/topic/com.cisco.endpoint.asset}]]
2019-05-22 14:39:26,052 INFO [ProfilerINDSubscriberBulkRequestPool-80-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- NODENAME:ind2
2019-05-22 14:39:26,052 INFO [ProfilerINDSubscriberBulkRequestPool-80-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- REQUEST
BODY{ "offset": "0", "limit": "500" }
2019-05-22 14:39:26,111 INFO [ProfilerINDSubscriberBulkRequestPool-80-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Response status={}200
2019-05-22 14:39:26,111 INFO [ProfilerINDSubscriberBulkRequestPool-80-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Content:
{"assets":[{"assetId":"100","assetName":"WIN2012-
CHILD", "assetIpAddress": "10.62.145.131", "assetMacAddress": "00:50:56:b6:46:87", "assetVendor": "VMw
are", "assetProductId":"Unknown", "assetSerialNumber":"", "assetDeviceType":"Server", "assetSwRevisi
on":"", "assetHwRevision":"", "assetProtocol":"NetBIOS", "assetConnectedLinks":[], "assetCustomAttri
butes":[{"key":"assetGroup","value":"Root"}, {"key":"assetTag","value":"SEC_TAG2"}]}, {"assetId":"
101", "assetName": "win2012.example.com", "assetIpAddress": "10.62.145.72", "assetMacAddress": "00:50:
56:9c:3f:92", "assetVendor": "VMware", "assetProductId": "Unknown", "assetSerialNumber": "", "assetDevi
ceType":"Server","assetSwRevision":"","assetHwRevision":"","assetProtocol":"NetBIOS","assetConne
ctedLinks":[],"assetCustomAttributes":[{"key":"assetGroup","value":"Root"},{"key":"assetTag","va
lue":""}]}]
2019-05-22 14:39:26,111 DEBUG [ProfilerINDSubscriberBulkRequestPool-80-thread-1][]
```

cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Parsing bulk response
{"assets":[{"assetId":"100","assetName":"WIN2012CHILD","assetIpAddress":"10.62.145.131","assetMacAddress":"00:50:56:b6:46:87","assetVendor":"VMw
are","assetProductId":"Unknown","assetSerialNumber":"","assetDeviceType":"Server","assetSwRevisi
on":"","assetHwRevision":"","assetProtocol":"NetBIOS","assetConnectedLinks":[],"assetCustomAttri
butes":[{"key":"assetGroup","value":"Root"},{"key":"assetTag","value":"Server","assetId":"00:50:
56:9c:3f:92","assetVendor":"VMware","assetProductId":"Unknown","assetSerialNumber":"","assetProtocol":"NetBIOS","assetProtocol":"NetBIOS","assetProtocol":"10.62.145.72","assetMacAddress":"00:50:
56:9c:3f:92","assetVendor":"VMware","assetProductId":"Unknown","assetSerialNumber":"","assetDeviceType":"Server","assetCustomAttributes":[["ukuy":"assetVendor":"VMware","assetProductId":"Unknown","assetSerialNumber":"","assetCustomAttributes":"10.62.145.72","assetMacAddress":"00:50:
56:9c:3f:92","assetVendor":"VMware","assetProductId":"Unknown","assetSerialNumber":"","assetDeviceType":"Server","assetSwRevision":"","assetHwRevision":"","assetProtocol":"NetBIOS","assetConne
ctedLinks":[],"assetCustomAttributes":[{"key":"assetGroup","value":"Root"},{"key":"assetTag","value":"","assetTag","value":"","assetTag","value":"","assetTag","value":"","assetTag","value":"","assetTag","value":"","assetTag","value":"","assetTag","value":"","assetTag","value":"","assetTag","value":"","assetTag","value":"","assetTag","value":"","assetTag","value":"","assetTag","value":","assetTag","value":","assetTag","value":","assetTag","value":","assetTag","value":","assetTag","value":",","assetTag","value":",","assetTag","value":",","assetTag","value":",","assetTag","value":",","assetTag","value":",","assetTag","value":",","assetTag","value":",",","assetTag","value":",",","assetTag","value":",",","assetTag","value":",",","assetTag","value":",",","assetTag","value":",",","assetTag","value":",",",","assetTag",",",",",",",",",,",,",,",,",,

3.在IND上發現新終結點(需要使用協定發現終結點,否則終結點未標識為pxGrid資產,並且未通過 pxGrid與ISE共用)。

.ılı.ılı. cısco	INDUSTRIAL NETWORK DIRECTOR	Operate	> Inve	entory							
Overview	< Back						win20	012.example.com			
							DEVIC	CE OVERVIEW			
					Name	win2012.example.com			Dev	ісе Туре	Server
					IP Address	10.62.145.72				Protocol	NetBIOS
				MA	AC Address	00:50:56:9c:3f:92				Group	Root
					Vendor	VMware			Conr	ected to	
				p	xGrid Asset	Yes				Tag(s)	+

4. IND將此資訊發佈到ISE pxGrid節點

5. PSN通過pxGrid探測接收此資料(profiler.log):

```
2019-05-22 15:20:40,616 DEBUG [Grizzly(2)][]
```

```
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Parsing push notification response:
{"asset":{"assetId":"101","assetName":"win2012.example.com","assetIpAddress":"10.62.145.72","ass
etMacAddress":"00:50:56:9c:3f:92","assetVendor":"VMware","assetProductId":"Unknown","assetSerial
Number":"", "assetDeviceType": "Server", "assetSwRevision":"", "assetHwRevision":"", "assetProtocol":
"NetBIOS", "assetConnectedLinks":[], "assetCustomAttributes":[{"key": "assetGroup", "value": "Root"},
{ "key": "assetTag", "value": "SEC_TAG2" } ] }, "opType": "UPDATE" }
2019-05-22 15:20:40,616 DEBUG [Grizzly(2)][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- sending endpoint to
forwarder{"assetId":"101","assetName":"win2012.example.com","assetIpAddress":"10.62.145.72","ass
etMacAddress":"00:50:56:9c:3f:92", "assetVendor":"VMware", "assetProductId":"Unknown", "assetSerial
Number":"", "assetDeviceType": "Server", "assetSwRevision":"", "assetHwRevision":"", "assetProtocol":
"NetBIOS", "assetConnectedLinks":[], "assetCustomAttributes":[{"key": "assetGroup", "value": "Root"},
{"key":"assetTag","value":"SEC_TAG2"}]
2019-05-22 15:20:40,617 INFO [Grizzly(2)][] cisco.profiler.infrastructure.probemgr.Forwarder -
::- Forwarder Mac 00:50:56:9C:3F:92 MessageCode null epSource PXGRIDPROBE
2019-05-22 15:20:40,617 DEBUG [forwarder-2][]
cisco.profiler.infrastructure.probemgr.ForwarderHelper -: ProfilerCollection:- sequencing Radius
message for mac = 00:50:56:9C:3F:92
2019-05-22 15:20:40,617 DEBUG [forwarder-2][] cisco.profiler.infrastructure.probemgr.Forwarder -
:ProfilerCollection:- Processing endpoint:00:50:56:9C:3F:92
2019-05-22 15:20:40,618 DEBUG [forwarder-2][] com.cisco.profiler.im.EndPoint -
:ProfilerCollection:- filtered custom attributes are:{assetGroup=Root, assetTag=SEC_TAG2}
2019-05-22 15:20:40,618 DEBUG [forwarder-2][] cisco.profiler.infrastructure.probemgr.Forwarder -
:ProfilerCollection:- Filtering:00:50:56:9C:3F:92
2019-05-22 15:20:40,618 DEBUG [forwarder-2][] cisco.profiler.infrastructure.probemgr.Forwarder -
:ProfilerCollection: - Endpoint Attributes: EndPoint[id=<null>, name=<null>]
```

MAC: 00:50:56:9C:3F:92 Attribute:BYODRegistration value:Unknown Attribute:DeviceRegistrationStatus value:NotRegistered Attribute:EndPointProfilerServer value:ISE24-1ek.example.com Attribute:EndPointSource value:PXGRIDPROBE Attribute:MACAddress value:00:50:56:9C:3F:92 Attribute:NmapSubnetScanID value:0 Attribute:OUI value:VMware, Inc. Attribute:PolicyVersion value:0 Attribute:PortalUser value: Attribute:PostureApplicable value:Yes Attribute:assetDeviceType value:Server Attribute:assetGroup value:Root Attribute:assetHwRevision value: Attribute:assetId value:101 Attribute:assetIpAddress value:10.62.145.72 Attribute:assetMacAddress value:00:50:56:9c:3f:92 Attribute:assetName value:win2012.example.com Attribute:assetProductId value:Unknown Attribute:assetProtocol value:NetBIOS Attribute:assetSerialNumber value: Attribute:assetSwRevision value: Attribute:assetTag value:SEC_TAG2 Attribute:assetVendor value:VMware Attribute:b310a420-78a5-11e9-a189-9ac8f4107843 value:Root Attribute:b8e73d50-78a5-11e9-a189-9ac8f4107843 value:SEC_TAG2 Attribute: ip value: 10.62.145.72 Attribute:SkipProfiling value:false 6.使用正確資料更新情景可視性

Endpoints Users Network Devices Application 00:50:56:9C:3F:92 Image: Comparison of the compariso
00:50:56:9C:3F:92 Image: Construction MAC Address: 00:50:56:9C:3F:92 Username: Endpoint Profile: IOT_DEVICE2 Current IP Address: 10.62.145.72 Location: Image: Construction Image: Co
Cocation: Location: Applications Attributes Authentication Threats Vulnerabilities General Attributes Description Static Assignment false
General Attributes Description Static Assignment false
Description Static Assignment false
Static Assignment false
Endpoint Policy IOT_DEVICE2
Static Group Assignment false
Identity Group Assignment Profiled
Custom Attributes
Tilter - 🌣
Attribute Name Attribute Value
× Attribute Name Attribute Value
assetGroup Root
LogicalProfile
assetTag SEC_TAG2
Other Attributes

組態

附註:即使您希望在情景可視性中僅能看到assetGroup和assetTag,也需要步驟1-3

步驟1.在ISE上配置終端自定義屬性

導航到**管理>身份管理>設定>端點自定義屬性**。根據以下影象配置自定義屬性(assetGroup和 assetTag)。

cisco Ident	tity Services Engine	Home ► Cont	ext Visibility	 Operations 	Policy	- Administration			
 System 	- Identity Management	Network Resource	s Device	Portal Management	pxGrid S	ervices + Feed S	ervice		
Identities	Groups External Ide	ntity Sources Identi	y Source Sequ	ences - Settings					
	(3							
User Custom	Attributes	Endpoint C	ustom Attril	outes					
User Authenti	cation Settings								
Endpoint Purg	ge	Endpoint A	ttributes (fo	or reference)					
Endpoint Cus	tom Attributes	Mandatory	Attribute	Name		Data	Туре		
			PostureA	oplicable		STRI	NG		
			EndPoint	Policy		STRING			
			AnomalousBehaviour			STRING			
			OperatingSystem			STRING			
			BYODRe	gistration		STRI	NG		
			PortalUse	r		STRI	NG		
			LastAUPA	cceptanceHours		INT			
			LogicalPr	ofile		STRI	NG		
		Endpoint C	ustom Attril	outes					
			Attribut	e name		Туре			
		assetGroup				String	_		
		assetTag				String	- •		
						Reset Save			

步驟2.使用自定義屬性配置Profiler策略

導航到工**作中心(Work Centers)> Profiler(Profiler)>分析策略(Profiling Policies)**。按一下「Add」。 配置探查器策略,如下圖所示。

dentity Services Engine	Home	 Context Visit 	bility 🕨	Operations	Policy A	dministration	Work Centers					
Network Access Guest Access	TrustSec	BYOD	✓ Profiler	 Posture 	Device Administr	ration + Passivell	D					
Overview Ext Id Sources Network De	vices End	point Classificat	ion Node	Config Feeds	Manual Scans	 Policy Elements 	Profiling Policies	Policy Sets	 Troubleshoot 	Reports	 Settings 	Dictionaries

Profiling	Profiler Policy List > IOT_DEVICE1
٩	Profiler Policy
(-) + E +	*Name IOT_DEVICE1 Description
Profiling Policies	Policy Enabled
Logical Profiles	* Minimum Certainty Factor 20 (Valid Range 1 to 65535)
	* Exception Action NONE
	* Network Scan (NMAP) Action NONE
	Create an Identity Group for the policy O Yes, create matching Identity Group
	No, use existing Identity Group hierarchy
	Parent Policy NONE
	* Associated CoA Type Global Settings
	System Type Administrator Created
	Rules
	If Condition CUSTOMATTRIBUTE_assetTag_EQUALS Certainty Factor Increases V 20
	Save Rese Condition Name Expression CUSTOMATTRIB O EQUALS SEC_TAG1

步驟3.啟用用於分析實施的自定義屬性

導航到**工作中心> Profiler > Settings > Profiler Settings**。確保 **啟用分析強制的自定義屬性** 覈取方塊 已選中。

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Network Access Guest Access	TrustSec → BYOD ▼Profiler → Posture → Device Administration → PassiveID
Overview Ext Id Sources Network De	wices Endpoint Classification Node Config Feeds + Manual Scans + Policy Elements Profiling Policies Policy Sets + Troubleshoot Reports - Settings Dictionaries
Profiler Settings	Profiler Configuration
NMAP Scan Subnet Exclusions	* CoA Type: Reauth *
	Current custom SNMP community strings: •••••• Show
	Change custom SNMP community strings: (For NMAP, comma separated. Field will be cleared on successful saved change.)
	Confirm changed custom SNMP community strings: (For NMAP, comma separated. Field will be cleared on successful saved change.)
	EndPoint Attribute Filter: Denabled
	Enable Anomalous Behaviour Detection: Detection: Enabled ()
	Enable Anomalous Behaviour Enforcement: 🗌 Enabled
	Enable Custom Attribute for Profiling Enforcement: 🥑 Enabled
	Save Reset

步驟4.匯出IND身份證書

導覽至**Settings > pxGrid**。按一下「**Download .pem IND certificate**」。此證書在pxGrid註冊期間使 用,因此ISE應信任它。

-ili-ili- cisco	INDUSTRIAL Network Director	Setting	• >	pxGrid	▲ • □ • ⊥ •			
i⊟ Settings					pxGrid			
Trusted Certificates	Cisco Platform Exchange Grid (pxGrid) is an open, scalable data-sharing and threat control platform that allows seamless integration between multivendor identity, network, security and asset management systems. Enabling the feature below activates the sharing of endpoint assets discovered by this system with Services Engine (ISE) pxGrid controller. This information can then be leveraged by upstream security systems to monitor security, detect threats, and set network policy. Learn more here.							
	Download .p	em IND certificate						

步驟5.將IND身份證書上傳到ISE受信任庫

導航到**管理>證書>證書管理>受信任證書**。按一下Import。按一下Browse,然後從步驟3中選擇 IND證書。按一下Submit。

ululu Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers						
✓ System → Identity Management	Network Resources						
Deployment Licensing - Certificate	s Logging Maintenance Upgrade Backup & Restore Admin Access Settings						
0							
- Certificate Management	Import a new Certificate into the Certificate Store						
System Certificates	* Certificate File Browse ind(1).pem						
Trusted Certificates	Friendly Name						
OCSP Client Profile							
Certificate Signing Requests	Trusted For: 🕧						
Certificate Periodic Check Setti	✓ Trust for authentication within ISE						
Certificate Authority	Trust for client authentication and Syslog						
	Trust for authentication of Cisco Services						
	Validate Certificate Extensions						
	Description						
	Submit Cancel						

步驟6.為IND生成證書

IND不使用ISE CA頒發的客戶端證書。相反,目標是填充IND受信任儲存,因此ISE傳送其pxGrid證 書時(在TLS交換期間),它受IND信任。

導航到**管理> pxGrid服務>證書**。根據以下影象填充欄位。CN欄位是必填欄位,因為ISE CA的目標 是頒發身份證書。理想情況下,應輸入IND的FQDN,但由於身份證書不被IND使用,因此CN欄位 值不重要。

Horisco Identity Services Engine Ho	me Context Visibility Operations Policy Administration Work Centers	
System Identity Management Ne	twork Resources	
All Clients Web Clients Capabilities	Live Log Settings Certificates Permissions	
Generate pxGrid Certificates		
I want to *	Generate a single certificate (without a certificate signing request)	•
Common Name (CN) *	ind.example.com	
Description		
Certificate Template	PxGrid_Certificate_Template	
Subject Alternative Name (SAN)		
Certificate Download Format *	PKCS12 format (including certificate chain; one file for both the certificate chain and key)	• 0
Certificate Password *		0
Confirm Password *		
Commit assword		
	Reset Create	

步驟7.下載PKCS12格式的證書鏈

• • •	Opening 1558534704560_cert.zip								
You have cho	sen to open:								
155853470	1558534704560_cert.zip								
which is: ZI from: https	P archive ://10.62.145.140								
What should Firefox do with this file?									
Open with	Archive Utility (default)								
 Save File 									
Do this automatically for files like this from now on.									
	Cancel OK								

步驟8.在IND上傳憑證鏈結

導航到**設定> pxGrid >受信任證書**。按一下**New**。輸入Name(在IND上可以看到帶有此名稱的鏈)。 密碼是步驟1中的密碼。

Upload Trusted Certificate			×					
Name* IND								
Password								
Certificate •	Browse	C:\fakepath\ind.example.com_ 3.p12	×					
	Upload	Cancel						

步驟9.在IND上配置策略伺服器

導航到**設定>策略伺服器**,按一下**新建**。輸入ISE pxGrid節點的ISE FQDN和IP地址。

cisco NETWORK DIRECTOR	Settings > Policy Servers					۵ 🌲	Û
< Back to Servers				New Server			
P	rotocols*						
H (lost Name* ISE24-1ek.example.com	0	IP Address 10.62.145.140		Description		0
				Cancel Save			

步驟10.在IND上配置pxGrid整合

導航到**設定> pxGrid**並啟用pxGrid整合。按一下切換按鈕。輸入節點名稱,此主機名稱是ISE上的 pxGrid客戶端的名稱。從伺服器1欄位的下拉選單中選擇之前配置的ISE。按一下「**Register**」。

cisco	INDUSTRIAL NETWORK DIRECTOR	Settings > pxGrid						۹ 🌲	Û	? •	1 ·
i⊟ Setings					pxGrid						
E Trusted Certificates	Enable pxGrid- Settin	gs									
	Download .pem II Connect Using the Register a New N	ND certificate he Existing Node lode									
	ISE Server			Server 1*		Server 2					
	IND		0	ISE24-1ek.example.com		• O Selec	t a server				• 0
					Cancel Register						

附註:如果在ISE上啟用自動批准基於證書的新帳戶設定,則忽略步驟11-12。

成功註冊後,IND上顯示以下消息:

Message		×
pxGrid Node Approval Pending o	on the pxGrid Server	
	ОК	

導航到**管理> pxGrid服務>所有客戶端**。開啟「等待批准的總數(1)」下拉選單。按一下「Approve All」。

tisce Identity Services Engine Home → Context Visit	ility ► Operations ► Policy - Add	ministration Work Centers									
System Identity Management Network Resources	Device Portal Management pxGrid Services	Feed Service Threat Centric NAC									
All Clients Web Clients Capabilities Live Log Settings Certificates Permissions											
🖋 Enable 🖉 Disable 😪 Approve 😝 Group 👎 Decline 😵 Delete	➡ Stress Total Pending Approval(1) ▼										
Client Name Client Description	Cap. Approve All	Status Client Group(s)									
□ ▶ ise-fanout-ise24-1ek	Capabilities(0 Pub, 0 Sub)	Online (XMPP) Internal									
□ ► ise-pubsub-ise24-1ek	Capabilities(0 Pub, 0 Sub)	Online (XMPP) Internal									
□ ► ise-pubsub-ise24-2ek	Capabilities(0 Pub, 0 Sub)	Online (XMPP) Internal									
□ ► ise-fanout-ise24-2ek	Capabilities(0 Pub, 0 Sub)	Online (XMPP) Internal									
□ ► ise-admin-ise24-3ek	Capabilities(0 Pub, 0 Sub)	Online (XMPP) Internal									
□ ► ise-mnt-ise24-2ek	Capabilities(2 Pub, 1 Sub)	Online (XMPP) Internal									
□ ▶ ise-mnt-ise24-1ek	Capabilities(2 Pub, 1 Sub)	Online (XMPP) Internal									
□ ► ise-bridge-ise24-1ek	Capabilities(0 Pub, 4 Sub)	Online (XMPP) Internal									
□ ► ise-admin-ise24-1ek	Capabilities(5 Pub, 2 Sub)	Online (XMPP) Internal									
□ ► ise-admin-ise24-2ek	Capabilities(1 Pub, 1 Sub)	Online (XMPP) Internal									
□ ▶ ind	Capabilities(0 Pub, 0 Sub)	Pending									

步驟12.在IND上啟用pxGrid服務

導覽至Settings > pxGrid。按一下「Activate」。

Enable pxGrid- Activate ISE Server Download .pem IND certificate Node Name* Server 1* ISE24-1ek.example.com		pxGrid
Enable pxGrid- Activate ISE Server Download .pem IND certificate Node Name* Server 1* IND		
ISE Server Download .pem IND certificate Node Name* Server 1* IND ISE24-1ek.example.com	Enable pxGrid- Activate	
ISE Server Download .pem IND certificate Node Name* Server 1* IND ISE24-1ek.example.com		
Download .pem IND certificate Node Name* Server 1* IND ISE24-1ek.example.com		
Download .pem IND certificate Node Name* Server 1* IND ISE24-1ek.example.com	ISE SELVER	
Node Name* Server 1* IND ISE24-1ek.example.com	Download .pem IND certificate	
Node Name* Server 1* IND ISE24-1ek.example.com		
IND ISE24-1ek.example.com	Node Name*	Server 1*
	IND	ISE24-1ek.example.com
Disable Activate		Disable Activate
Disable Activate		Disable Activate

成功啟用後,IND上顯示以下消息:



驗證

ISE驗證

導航到**管理> pxGrid服務>所有客戶端**。在All Clients中,IND會將IND客戶端視為 Offline(XMPP),IND使用pxGrid版本2。

cisco	Identity Services Engine	Home 🕨 C	ontext Visibility	 Operation 	ns	- Administration	Work Centers	
 Syst 	tem Identity Management	Network Resource	urces + Devic	e Portal Mana	ement pxGrid S	Services Feed Se	ervice + Threat Centric N	AC
All CI	ients Web Clients Capa	abilities Live Log	g Settings	Certificates	Permissions			
🖌 Enat	ole 🧭 Disable 😪 Approve 🗧) Group 👎 Decline	😧 Delete 👻	😵 Refresh	otal Pending Approv	val(0) 💌		
	Client Name	Client Descr	iption	Сара	bilities	Status		Client Group(s)
►►	ise-fanout-ise24-1ek			Сара	pilities(0 Pub, 0 Su	b) Online (XMPP)	Internal
►►	ise-pubsub-ise24-1ek Client N	lame: Not Sortable		Сара	pilities(0 Pub, 0 Su	b) Online (XMPP)	Internal
	ise-pubsub-ise24-2ek			Сара	pilities(0 Pub, 0 Su	b) Online (XMPP)	Internal
	ise-fanout-ise24-2ek			Сара	pilities(0 Pub, 0 Su	b) Online (XMPP)	Internal
	ise-admin-ise24-3ek			Сара	pilities(0 Pub, 0 Su	b) Online (XMPP)	Internal
	ise-mnt-ise24-2ek			Сара	pilities(2 Pub, 1 Su	b) Online (XMPP)	Internal
	ise-mnt-ise24-1ek			Сара	pilities(2 Pub, 1 Su	b) Online (XMPP)	Internal
	ise-bridge-ise24-1ek			Сара	pilities(0 Pub, 4 Su	b) Online (XMPP)	Internal
	ise-admin-ise24-1ek			Capa	pilities(5 Pub, 2 Su	b) Online (XMPP)	Internal
	ise-admin-ise24-2ek			Capa	pilities(1 Pub, 1 Su	b) Online (XMPP)	Internal
	ind			Capa	pilities(0 Pub, 0 Su	b) Offline (XMPP)	

按一下**Web Clients**,確認IND客戶端的狀態為ON,並且/topic/com.cisco.endoint.asset是 Subscriptions的一部分。

cisco	Identi	ty Services Engli	ne Home	Cont	ext Visibility	 Operations 	Policy	- Administration	 Work Centers 					
▶ Sy	stem	 Identity Manager 	ment + Netwo	rk Resource	s Devic	e Portal Managem	ent pxGrid S	Services + Feed Se	rvice + Threat Cer	ntric NAC				
All	Clients	Web Clients	Capabilities	Live Log	Settings	Certificates	Permissions							
										R	ows/Page 25	1	/1 = = (Go 12 Total Rows
C F	Refresh													Ţ Filter - ¢ -
	Clien	t Name	Connect To	Se	ssion Id	Certificate	•	Subscriptions		Publications		IP Address	Status	Start time
×	Clien	it Name		•								IP Address		•
	IND		ISE24-1ek	ISE	24-1ek:181	CN=WIN20)12-AAA,					10.62.145.130	ON	2019-05-23 08:27
	ise-m	nt-ise24-1ek	ISE24-1ek	ISE	24-1ek:182	CN=ISE24	-1ek.exa	/topic/com.cisco.is	e.session.internal			10.62.145.140	ON	2019-05-23 08:28
	ise-far	nout-ise24-1ek	ISE24-1ek	ISE	24-1ek:183	CN=ISE24	-1ek.exa	/topic/distributed		/topic/distributed		10.62.145.140	ON	2019-05-23 08:28
	ise-ad	Imin-ise24-1ek	ISE24-1ek	ISE	24-1ek:184	CN=ISE24	-1ek.exa	/topic/com.cisco.ei	ndpoint.asset			10.62.145.140	OFF 🥥	2019-05-23 08:28
	ise-m	nt-ise24-2ek	ISE24-1ek	ISE	24-1ek:185	No Certifica	ate	/topic/com.cisco.is	e.session.internal	/topic/com.cisco.ise.	session.internal	10.62.145.141	OFF 🥥	2019-05-23 08:59
	ise-ad	lmin-ise24-2ek	ISE24-1ek	ISE	24-1ek:188	No Certifica	ate					10.62.145.141	ON	2019-05-23 09:30
	ise-bri	idge-ise24-1ek	ISE24-1ek	ISE	24-1ek:189	CN=ISE24	-1ek.exa					127.0.0.1	OFF 🧿	2019-05-23 09:30
	ise-far	nout-ise24-1ek	ISE24-1ek	ISE	24-1ek:190	CN=ISE24	-1ek.exa	/topic/wildcard				127.0.0.1	ON	2019-05-23 09:30
	ise-m	nt-ise24-2ek	ISE24-1ek	ISE	24-1ek:191	No Certifica	ate 💠	/topic/com.cisco.is	e.session.internal	/topic/com.cisco.ise.	session.internal	10.62.145.141	ON	2019-05-23 09:43
	ise-ad	Imin-ise24-1ek	ISE24-1ek	ISE	24-1ek:192	CN=ISE24	-1ek.exa	/topic/com.cisco.ei	ndpoint.asset			10.62.145.140	ON	2019-05-23 09:43
	ise-bri	idge-ise24-1ek	ISE24-1ek	ISE	24-1ek:193	CN=ISE24	-1ek.exa					127.0.0.1	OFF 🧿	2019-05-23 10:04
	ise-bri	idge-ise24-1ek	ISE24-1ek	ISE	24-1ek:194	CN=ISE24	-1ek.exa					127.0.0.1	ON	2019-05-23 10:09

IND驗證

IND應轉換為「同步」狀態。如果ISE上的批次下載成功,則完成,如果不是IND將停滯在「不同步」狀態。

.ili.ili. cisco	INDUSTRIAL NETWORK DIRE	CTOR Settings > pxGrid						۰ 🌲	Û	•	1			
Elittings				pxGrid										
Trusted Centricates	Cisco Pla Services	Cisco Platform Exchange Grid (pxGrid) is an open, scalable data-sharing and threat control platform that allows seamless integration between multivendor identity, network, security and asset management systems. Enabling the feature below activates the sharing of endpoint assets discovered by this system with a Cisco Identity Services Engine (ISE) pxGrid controller. This information can then be leveraged by upstream socurity systems to monitor socurity, detect threats, and set network policy. Learn more here.												
	Down	load .pem IND certificate												
)												
	ISE	Server												
	Node	Name*		Server 1*	Se	erver 2								
	INC			ISE24-1ek.example.com										
	-													
	Stat	istics												
		Sync. Status	In Sync		Last Sync.	Status Probe Time	2019-05-23 10:19:16							
		Number of Assets Shared via Last Bulk Request	2		Last	Bulk Request Time	2019-05-23 08:29:14							
		Last Update Operation	Update			Last Update Time	2019-05-22 20:17:36							
	-	Total pxGrid Asset Count	2											

疑難排解

IND上的同步狀態停滯在「不同步」狀態

如果在ISE上成功進行批次下載,則會發生從不同步到同步的轉換。IND application.log(位於下方)。

2019-05-22 22:09:06,902:INFO:qtp281049997-53444:PxgridConfigMgr:: Pxgrid Statistics Start:: Bulk Request : bulkReqAssetCount:2 add: false 2019-05-22 22:09:06,902:INFO:qtp281049997-53444:PxgridConfigMgr:: Pxgrid Statistics updated:: Bulk Request : AssetCount:2 2019-05-22 22:09:06,902:INFO:qtp281049997-53444:PxgridConfigMgr:: Sync Status transition to IN_SYNC

2019-05-22 22:09:06,918:INFO:qtp281049997-53444:PxGridServiceRestController:: getAssets Completed

ISE能夠解析IND共用的IND主機名至關重要。否則ISE無法執行批次下載,並且IND永遠不會轉換到 「同步」狀態。如果批次下載失敗(WIN2012-AAA無法由ISE解決),您可在profiler.log中看到以 下異常。 要觸發批次下載,可以取消選中並檢查PSN上的pxGrid探測器。

```
2019-04-30 13:59:50,708 INFO [ProfilerINDSubscriberPoller-60-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- New services are: []
2019-04-30 13:59:50,714 INFO [ProfilerINDSubscriberPoller-60-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- NODENAME:ind
2019-04-30 13:59:50,714 INFO [ProfilerINDSubscriberPoller-60-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- REQUEST
BODY{ "offset": "0", "limit": "500" }
2019-04-30 13:59:50,716 ERROR [ProfilerINDSubscriberPoller-60-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Unable to get sync statusWIN2012-
AAA:WIN2012-AAA
java.net.UnknownHostException: WIN2012-AAA
at java.net.AbstractPlainSocketImpl.connect(AbstractPlainSocketImpl.java:184)
at java.net.SocksSocketImpl.connect(SocksSocketImpl.java:392)
at java.net.Socket.connect(Socket.java:589)
at sun.security.ssl.SSLSocketImpl.connect(SSLSocketImpl.java:673)
at sun.security.ssl.BaseSSLSocketImpl.connect(BaseSSLSocketImpl.java:173)
at sun.net.NetworkClient.doConnect(NetworkClient.java:180)
at sun.net.www.http.HttpClient.openServer(HttpClient.java:463)
at sun.net.www.http.HttpClient.openServer(HttpClient.java:558)
at sun.net.www.protocol.https.HttpsClient.<init>(HttpsClient.java:264)
at sun.net.www.protocol.https.HttpsClient.New(HttpsClient.java:367)
at
sun.net.www.protocol.https.AbstractDelegateHttpsURLConnection.getNewHttpClient(AbstractDelegateH
ttpsURLConnection.java:191)
at sun.net.www.protocol.http.HttpURLConnection.plainConnect0(HttpURLConnection.java:1156)
at sun.net.www.protocol.http.HttpURLConnection.plainConnect(HttpURLConnection.java:1050)
at
sun.net.www.protocol.https.AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLCo
nnection.java:177)
at sun.net.www.protocol.http.HttpURLConnection.getOutputStream0(HttpURLConnection.java:1334)
at sun.net.www.protocol.http.HttpURLConnection.getOutputStream(HttpURLConnection.java:1309)
at
sun.net.www.protocol.https.HttpsURLConnectionImpl.getOutputStream(HttpsURLConnectionImpl.java:25
9)
at com.cisco.profiler.infrastructure.probemgr.INDSubscriber.getRequest(INDSubscriber.java:362)
at com.cisco.profiler.infrastructure.probemgr.INDSubscriber.isInSync(INDSubscriber.java:500)
at
com.cisco.profiler.infrastructure.probemgr.INDSubscriber.populateIOTServiceList(INDSubscriber.ja
va:462)
at
com.cisco.profiler.infrastructure.probemgr.INDSubscriber$WorkerThread.run(INDSubscriber.java:441
)
at java.util.concurrent.Executors$RunnableAdapter.call(Executors.java:511)
at java.util.concurrent.FutureTask.runAndReset(FutureTask.java:308)
at
java.util.concurrent.ScheduledThreadPoolExecutor$ScheduledFutureTask.access$301(ScheduledThreadP
oolExecutor.java:180)
at
java.util.concurrent.ScheduledThreadPoolExecutor$ScheduledFutureTask.run(ScheduledThreadPoolExec
utor.java:294)
at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149)
at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624)
at java.lang.Thread.run(Thread.java:748)
```

並非所有終端都與ISE共用

僅當pxGrid Asset標誌為Yes時,IND上的終端才與ISE共用,MAC地址也應可用,否則ISE沒有足 夠的資料建立終端。

-ili-ili- cisco	INDUSTRIAL NETWORK DIRECTOR	Operate > Inventory					۰ 🌲	Û	? -	٤
50 Overview	< Back			WIN2012-CHILD						
				DEVICE OVERVIEW						
		Name	WIN2012-CHILD		Device Type	Server				
		IP Address	10.62.145.131		Protocol	NetBIOS				
		MAC Address	00:50:56:b6:46:87		Group	Root				
		Vendor	VMware		Connected to					
		pxGrid Asset	Yes		Tag(s)	SEC_TAG2				

assetTag和AssetGroup在ISE上不可用

如果assetTag僅不可用,則可能會出現使用錯誤TAG型別的情況。更新端點時,需要使用安全標籤 (非常規標籤)。

Associated Device Tags		×
No Tags Associated with this device		
Add Regular Tag		
Select a tag	•	
Add Security Tag		
Select a tag SEC_TAG1 SEC_TAG2		

如果AssetTag和AssetGroup均不可用,則可能有多個原因

1.未使用自定義屬性配置分析策略(請參閱本文檔配置部分中的步驟1-3)

2.由於CSCvn<u>缺陷66106</u> 端點屬性篩選器: 應該禁用。否則,它會從分類器中過濾自定義屬性。在 profiler.log中可以看到以下日誌。

2019-05-22 11:20:11,796 DEBUG [PersistentWorker-8-18-thread-1][] com.cisco.profiler.im.EndPoint -:Profiling:- filtered custom attributes are:{assetGroup=Root, assetTag=SEC_TAG2, b310a420-78a5-11e9-a189-9ac8f4107843=Root, b8e73d50-78a5-11e9-a189-9ac8f4107843=SEC_TAG2}