配置ISE 2.4 pxGrid IND 1.6.1集成

目录

简介 先决条件 要求 使用的组件 配置 高级流程图 配置 步骤1.在ISE上配置终端自定义属性 步骤2.使用自定义属性配置分析器策略 步骤3.为分析实施启用自定义属性 步骤4.导出IND身份证书 步骤5.将IND身份证书上传到ISE受信任存储 步骤6.为IND生成证书 步骤7.下载PKCS12格式的证书链 步骤8.在IND上上传证书链 步骤9.在IND上配置策略服务器 步骤10.在IND上配置pxGrid集成 步骤11.批准ISE上的IND 步骤12.在IND上激活pxGrid服务 验证 ISE验证 IND验证 故障排除 IND上同步状态停滞在不同步状态 并非所有终端都与ISE共享 assetTag和AssetGroup在ISE上不可用

简介

本文档介绍如何配置和排除通过pxGrid(平台交换网格)的Identity Services Engine(ISE)2.4和 Industrial Network Director 1.6.1-4集成故障。 思科IND以pxGrid作为发布者注册,并将有关终端属 性的信息发布到IOTASSET词典的ISE。

先决条件

要求

Cisco 建议您具有以下主题的基础知识:

• 思科身份服务引擎

• 思科工业网络导向器

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 思科身份服务引擎版本2.4 p6
- 工业网络导向器1.6.1-4

配置

高级流程图



1. IND通过pxGrid版本2在ISE pxGrid节点上向ISE注册。来自IND(application.log)的相应日志:

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 **如日志所示,IND已注册assetTopic**

2. 启用pxgrid探测功能的ISE PSN可批量下载现有pxGrid资产(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][]
```

3.在IND上发现新终端(终端需要使用协议发现,否则终端不会被识别为pxGrid资产,不会通过 pxGrid与ISE共享)。

ll cisco	INDUSTRIAL NETWORK DIRECTOR	Operate	>	Inventory						
0verview	< Back						win2012.ex	ample.com		
							DEVICE OVI	ERVIEW		
					Name	win2012.example.com			Device Type	Server
					IP Address	10.62.145.72			Protoco	NetBIOS
					MAC Address	00:50:56:9c:3f:92			Group	Root
					Vendor	VMware			Connected to	
					pxGrid Asset	Yes			Tag(s	+

4. IND将此信息发布到ISE pxGrid节点

5.通过pxGrid探测功能的PSN接收此数据(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.使用正确的数据更新情景可视性

dei dei	ntity Services E	ngine	Home	▼Context Visibility	 Operations 	Policy	Administration	Work Centers
ndpoints	Users Net	work Devices	Applic	ation				
00:50):56:9C:3F:9 MAC Add Usernam Endpoint	2 C dress: 00:50: ne: t Profile: IOT_	56:9C:3F	92 2				
<u>ع</u> ے ۵	Applications	IP Address: 1 : Attributes	0.62.145.	Authentication T	hreats Vuln	erabilities		
Genera	I Attributes							
Descript	tion							
Static A	ssignment	false						
Endpoin	nt Policy	IOT_DE	/ICE2					
Static G	Froup Assignment	false						
Identity	Group Assignmer	nt Profiled						
Custom	n Attributes							
							7	Filter 👻 🌣 👻
	Attribute Nam	ne		Attribute Valu	le			
×	Attribute Name	9		Attribute Value	9			
	assetGroup			Root				
	LogicalProfile							
	assetTag			SEC_TAG2				
Other A	Attributes							
54101 /								

配置

注意:即使您只希望在情景可视性中了解assetGroup和assetTag,也需要步骤1 - 3

步骤1.在ISE上配置终端自定义属性

导航至**管理>身份管理>设置>终端自定义属性**。根据下图配置自定义属性(assetGroup和 assetTag)。

the intervices Engine Home		Home ► Conte	xt Visibility ► Operations	► Policy - Adm	inistration	Work Centers		
 System 	✓ Identity Management	Network Resources	bevice Portal Management	pxGrid Services	Feed Service	Threat Centric NAC		
Identities	Groups External Ide	entity Sources Identity	/ Source Sequences - Settings	3				
		9						
User Custom	Attributes	Endpoint Cu	stom Attributes					
User Authent	ication Settings							
Endpoint Pur	ge	Endpoint At	tributes (for reference)					
Endpoint Cus	tom Attributes	Mandatory	Attribute Name		Data Type	Ð		
			PostureApplicable		STRING			
			EndPointPolicy		STRING			
			AnomalousBehaviour		STRING			
			OperatingSystem		STRING			
			BYODRegistration		STRING			
			PortalUser		STRING			
			LastAUPAcceptanceHours		INT			
			LogicalProfile		STRING			
		Endpoint Cu	stom Attributes					
			Attribute name		Туре			
as		assetGroup		St	ring –	-		
		assetTag		St	ring 👻 –	- 0		
					Reset	Save		

步骤2.使用自定义属性配置分析器策略

导航至工**作中心>分析器>分析策略**。单击"Add"。配置分析器策略,类似于下图。

dentity Services Engine Home	Context Visibility Operations Policy Administration Work Centers
Network Access Guest Access TrustSec	BYOD Profiler Posture Posture Posture Posture Posture Posture Posture Posture
Overview Ext Id Sources Network Devices Endp	oint Classification Node Config Feeds + Manual Scans + Policy Elements Profiling Policies Policy Sets + Troubleshoot Reports + Settings Dictionaries
Profiling	Profiler Policy List > IOT_DEVICE1 Profiler Policy

步骤3.为分析实施启用自定义属性

导航至工**作中心>分析器>设置>分析器设置**。确保 为分析实施启用自定义属性 复选框。

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	vices Endpoint Classification Node Config Feeds > Manual Scans > Policy Elements Profiling Policies Policy Sets > Troubleshoot Reports - Settings Dictionaries
C Drofiles Settings	Profiler Configuration
Prolifer Seturigs	
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

步骤4.导出IND身份证书

导航至"**设置"> pxGrid**。单击"**Download** .pem IND certificate(下**载**.pem IND证书)"。此证书在 pxGrid注册期间使用,因此ISE应信任它。

.ılı.ılı. cısco	INDUSTRIAL NETWORK DIRECTOR	Settings > pxGrid	a	۰ 🌲	Ċ	9 ·	٤.
i⊟ Settings			pxGrid				
Trusted Certificates	Cisco Platform Exch Services Engine (IS	ange Grid (pxGrid) is an open, scal) pxGrid controller. This informatio	Jable 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 as on can then be loweraged by updream security systems to monitor security, detect threats, and set network policy. Learn more here.	ets discovered by	this system v	eith a Cisco Ide	ntity
	Download .pem	ND certificate					

步骤5.将IND身份证书上传到ISE受信任存储

导航到**管理>证书>证书管理>受信任证书**。单击"Import"。单击"浏**览"**,然后从步骤3中选择IND证书 。单击"提**交"**。

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	
System Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC	
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	(i)
OCSP Client Profile		J
Certificate Signing Requests	Trusted For: (j)	
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	

步骤6.为IND生成证书

IND不使用ISE CA颁发的客户端证书。相反,目标是填充IND受信任存储,因此当ISE发送其 pxGrid证书(在TLS交换期间)时,IND会信任它。

导航至Administration > pxGrid Services > Certificates。根据下图填充字段。CN字段是必填项,因 为ISE CA的目标是颁发身份证书。理想情况下,您应输入IND的FQDN,但由于IND未使用身份证书 ,因此CN字段值不重要。

dentity Services Engine Ho	ne	Policy ✓ Administration Work Centers	
System Identity Management Ne	twork Resources	pxGrid Services	
All Clients Web Clients Capabilities	Live Log Settings Certificates Per	missions	
Generate pxGrid Certificates			
I want to *	Generate a single certificate (without a certificate	ate 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	e file for both the certificate chain and key)	• 0
Certificate Password *	••••••		0
Confirm Password *	••••••		
		Reset Crea	te

步骤7.下载PKCS12格式的证书链

	Opening 1558534704560_cert.zip
You have cho	sen to open:
155853470	04560_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 aut	omatically for files like this from now on.
	Cancel

步骤8.在IND上上传证书链

导航至**Settings > pxGrid > Trusted Certificates**。单击"New(**新建)**"。输入名称(链将在IND上以此名称显示)。 密码是步骤1中的密码。

Upload Trusted Certificate			×						
Name*	IND								
Password									
Certificate *	Browse	C:\fakepath\ind.example.com_3.p12	×						
	Upload	Cancel							

步骤9.在IND上配置策略服务器

导航至**设置>策略服**务器,单击**新建**。输入ISE pxGrid节点的ISE FQDN和IP地址。

cisco NETWORK DIRECTOR	Settings > Policy Servers					۰ 🌲	Û
< Back to Servers				New Server			
	Protocols*						
	Host Name* ISE24-1ek.example.com	Ø	IP Address 10.62.145.140		Description		0
				Cancel Save			

步骤10.在IND上配置pxGrid集成

导航至**Settings > pxGrid**并启用pxGrid集成。单击切换按钮。输入节点名称,此主机名是ISE上 pxGrid客户端的名称。从Server 1字段的下拉菜单中选择之前配置的ISE。单击"**Register**(**注册)**"。

cisco	INDUSTRIAL NETWORK DIRECTOR	Settings > p	xGrid							۰ 🌲	Û	0 ·	1 -
i⊟ Setings						pxGri	d						
Trusted Certificates	Enable pxGrid- Settin	ngs											
	Download .pem II Connect Using ti Register a New N	IND certificate the Existing Node Node											
	ISE Server Node Name* IND			0	Server 1* ISE24-1ek.example.com			• 0	Server 2 Select a server				• 0
						Cancel F	Register						

注意:如果ISE上启用了Automatically approve new certificate-based accounts设置,则步骤 11 - 12可能会被忽略。

成功注册后,IND上会显示以下消息:

Message	×
pxGrid Node Approval Pending on the pxGrid Server	
ОК	

步骤11.批准ISE上的IND

导航至"管**理">"pxGrid服务">"所有客户端"**。打开"待审批总额(1)"下拉菜单。单击"**全部批准**"。

uluulu Identity Services Engine	ome	Operations Policy	✓ Administration → Wo	ork Centers
	letwork Resources	e Portal Management pxGrid S	ervices Feed Service	Threat Centric NAC
All Clients Web Clients Capabilitie	s Live Log Settings	Certificates Permissions		
🖌 Enable 🖉 Disable 😪 Approve 😝 Grou	ip 👎 Decline 🔞 Delete 👻	Sefresh Total Pending Approva	l(1) -	
Client Name	Client Description	Capi 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	

步骤12.在IND上激活pxGrid服务

导航至"**设置"> pxGrid**。单击"**激活**"。

cisco	INDUSTRIAL NETWORK DIRECTOR	Settings >	pxGrid				
:						pxGrid	
Trusted Certificates	Enable pxGrid- Actival	te					
	ISE Server						
	Download .pem	IND certificate					
	Node Name*			:	Server 1*		
	IND				ISE24-1ek.example.com		
						Disable Activate	

成功激活后,IND上显示以下消息:



验证

ISE验证

导航至"管**理">"pxGrid服务">"所有客户端"**。在"所有客户端"中,IND使用pxGrid版本2,IND客户端应显示为脱机(XMPP)。

cisco	Identity Services Engine	Home ▶ Cont	ext Visibility	Operations	Policy - Adm	inistration V	ork Centers	
Is Sys	tem Identity Management	Network Resource	es Device Port 	tal Management	pxGrid Services	Feed Service	Threat Centric NA	IC .
All C	lients Web Clients Capat	bilities Live Log	Settings Cer	tificates Perm	issions			
🖌 Enal	ble 🥝 Disable 🕜 Approve 😝	Group 👎 Decline 🌔	3 Delete 👻 🛞 Re	efresh Total Pend	ling Approval(0) 👻			
	Client Name	Client Description	on	Capabilities		Status		Client Group(s)
	ise-fanout-ise24-1ek			Capabilities(0	Pub, 0 Sub)	Online (XMPP)		Internal
	ise-pubsub-ise24-1ek Client Na	ame: Not Sortable		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)	Offline (XMPP)		

单击**Web客户端**,确认IND客户端的状态为ON,并且/topic/com.cisco.endint.asset是订用的一部分

cisco	Identity Services E	ngine Hom	ne F Conte	xt Visibility	 Operations 	Policy	- Administration	Work Cen	ters				
⊧ S	ystem 🔹 Identity Mar	agement + Net	work Resources	Devic	e Portal Managem	ent pxGrid \$	Services + Feed	Service + Three	eat Centric NAC				
All	Clients Web Clients	Capabilities	Live Log	Settings	Certificates	Permissions							
										Rows/Page 25	• 1 0	/1	Go 12 Total Rows
c	Refresh												Ŧ Filter
	Client Name	Connect T	To Ses	sion Id	Certificate	2	Subscriptions		Publications		IP Address	Status	Start time
×	Client Name		•								IP Address		•
	IND	ISE24-1ek	ISE2	24-1ek:181	CN=WIN20	12-AAA,					10.62.145.130	ON	2019-05-23 08:27
	ise-mnt-ise24-1ek	ISE24-1ek	ISE2	24-1ek:182	CN=ISE24-	1ek.exa	/topic/com.cisco	.ise.session.interr	nal		10.62.145.140	ON	2019-05-23 08:28
	ise-fanout-ise24-1ek	ISE24-1ek	ISE2	24-1ek:183	CN=ISE24-	1ek.exa	/topic/distribute	d	/topic/distribute	bd	10.62.145.140	ON	2019-05-23 08:28
	ise-admin-ise24-1ek	ISE24-1ek	ISE2	24-1ek:184	CN=ISE24-	1ek.exa	/topic/com.cisco	o.endpoint.asset			10.62.145.140	OFF 🕢	2019-05-23 08:28
	ise-mnt-ise24-2ek	ISE24-1ek	ISE2	24-1ek:185	No Certifica	ate	/topic/com.cisco	.ise.session.interr	nal /topic/com.cisc	o.ise.session.internal	10.62.145.141	OFF 🥥	2019-05-23 08:59
	ise-admin-ise24-2ek	ISE24-1ek	ISE2	24-1ek:188	No Certifica	ate					10.62.145.141	ON	2019-05-23 09:30
	ise-bridge-ise24-1ek	ISE24-1ek	ISE2	24-1ek:189	CN=ISE24-	1ek.exa					127.0.0.1	OFF 🧿	2019-05-23 09:30
	ise-fanout-ise24-1ek	ISE24-1ek	ISE2	24-1ek:190	CN=ISE24-	1ek.exa	/topic/wildcard				127.0.0.1	ON	2019-05-23 09:30
	ise-mnt-ise24-2ek	ISE24-1ek	ISE2	24-1ek:191	No Certifica	ate 💠	/topic/com.cisco	.ise.session.interr	nal /topic/com.cisc	o.ise.session.internal	10.62.145.141	ON	2019-05-23 09:43
	ise-admin-ise24-1ek	ISE24-1ek	ISE2	24-1ek:192	CN=ISE24-	1ek.exa	/topic/com.cisco	o.endpoint.asset			10.62.145.140	ON	2019-05-23 09:43
	ise-bridge-ise24-1ek	ISE24-1ek	ISE2	24-1ek:193	CN=ISE24-	1ek.exa					127.0.0.1	OFF 🕢	2019-05-23 10:04
	ise-bridge-ise24-1ek	ISE24-1ek	ISE2	24-1ek:194	CN=ISE24-	1ek.exa					127.0.0.1	ON	2019-05-23 10:09

IND验证

IND应转换到In Sync(正在同步)状态。如果ISE上的批量下载成功,如果不是IND将停滞在Out of Sync(不同步)状态,则完成此操作。

.ili.ili. cisco	INDUSTRIAL NETWORK DIRE	CTOR Settings > pxGrid						۰ 🌲	Û	•	1
≣≣ Settings				pxGrid							
Trusted Centricates	Cisco Pla Services	atorm Exchange Grid (pxGrid) is an open, scalable data-sharing and three Engine (ISE) pxGrid controller. This information can then be leveraged by	t control platform that allows upstream security systems	s seamless integration between multivendor identity, network, secur to monitor security, detect threats, and set network policy. Learn mo	ty and asset management systems. Enabling the f re here.	leature below activates t	he sharing of endpoint assets	discovered by	this system v	with a Cisco Ide	Intity
	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								

故障排除

IND上同步状态停滞在不同步状态

如果ISE上的批量下载成功,则会发生从不同步到不同步的转换。下面是IND application.log。

```
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必须能够解析由IND共享的IND主机名。否则,ISE无法批量下载,IND将永远不会转换到In Sync状态。如果批量下载失败(WIN2012-AAA无法由ISE解析),您可以在profiler.log中看到以下 异常。 要触发批量下载,可取消选中并检查PSN上的pxGrid探测功能。

```
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)
```

并非所有终端都与ISE共享

只有pxGrid资产标志为"是"(Yes)时,IND上的终端才与ISE共享,MAC地址也应可用,否则ISE没有 足够的数据来创建终端。

-ili-ili- cisco	INDUSTRIAL NETWORK DI	RECTOR	Operate >	Inventory						۵ 🌲	Û	0 ·	1 -
(Verview	< B4	ack					WIN2012-CHILD						
						1	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仅不可用,则在使用错误的TAG类型时可能会出现这种情况。更新终端时,需要使用 安全标记(而非常规标记)。

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

如果AssetTag和AssetGroup都不可用,则可能有多种原因

1.未使用自定义属性配置分析策略(请参阅文档配置部分的步骤1-3)

2.因CSCvn66106缺<u>陷</u>端点属性过滤器: 应禁用。否则,它会从分类器过滤自定义属性。在 profiler.log中可以看到以下日志。

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=Sec_TAG2}