

配置ISE 2.7 pxGrid CCV 3.1.0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](#)

- [1.在一個PSN上啟用pxGrid探測](#)
- [2.在ISE上配置終端自定義屬性](#)
- [3.使用自定義屬性配置Profiler策略](#)
- [4.啟用用於分析實施的自定義屬性](#)
- [5.配置pxGrid客戶端的自動審批](#)
- [6.匯出CCV證書](#)
- [7.將CCV身份證書上傳到ISE受信任庫](#)
- [8.生成CCV證書](#)
- [9.下載PKCS12格式的證書鏈](#)
- [10.在CCV上配置ISE整合詳細資訊](#)
- [11.上傳CCV證書鏈並啟動整合](#)

[驗證](#)

[CCV整合驗證](#)

[ISE整合驗證](#)

[驗證CCV組更改](#)

[疑難排解](#)

[在ISE上啟用調試](#)

[在CCV上啟用調試](#)

[批次下載失敗](#)

[並非所有終端都在ISE上建立](#)

[AssetGroup在ISE上不可用](#)

[終端組更新未反映在ISE上](#)

[從CCV中刪除組不是從ISE中刪除組](#)

[CCV從Web客戶端斷開](#)

[ISE與CCV TrustSec整合使用案例](#)

[拓撲和流](#)

[設定](#)

- [1.在ISE上配置可擴展組標籤](#)
- [2.使用組2的自定義屬性配置分析器策略](#)
- [3.配置授權策略以根據ISE上的終端身份組分配SGT](#)

[驗證](#)

- [1.終端基於CCV組1進行身份驗證](#)
- [2.管理員更改組](#)

簡介

本檔案介紹如何透過平台Exchange Grid v2(pxGrid)設定身分識別服務引擎(ISE)2.7與思科網路願景(CCV)3.1.0的整合以及疑難排解。CCV向pxGrid v2註冊為發佈者，並將終端屬性資訊發佈到ISE以獲取IOTASSET字典。

必要條件

需求

思科建議您瞭解以下主題的基本知識：

- ISE
- 思科網路願景

採用元件

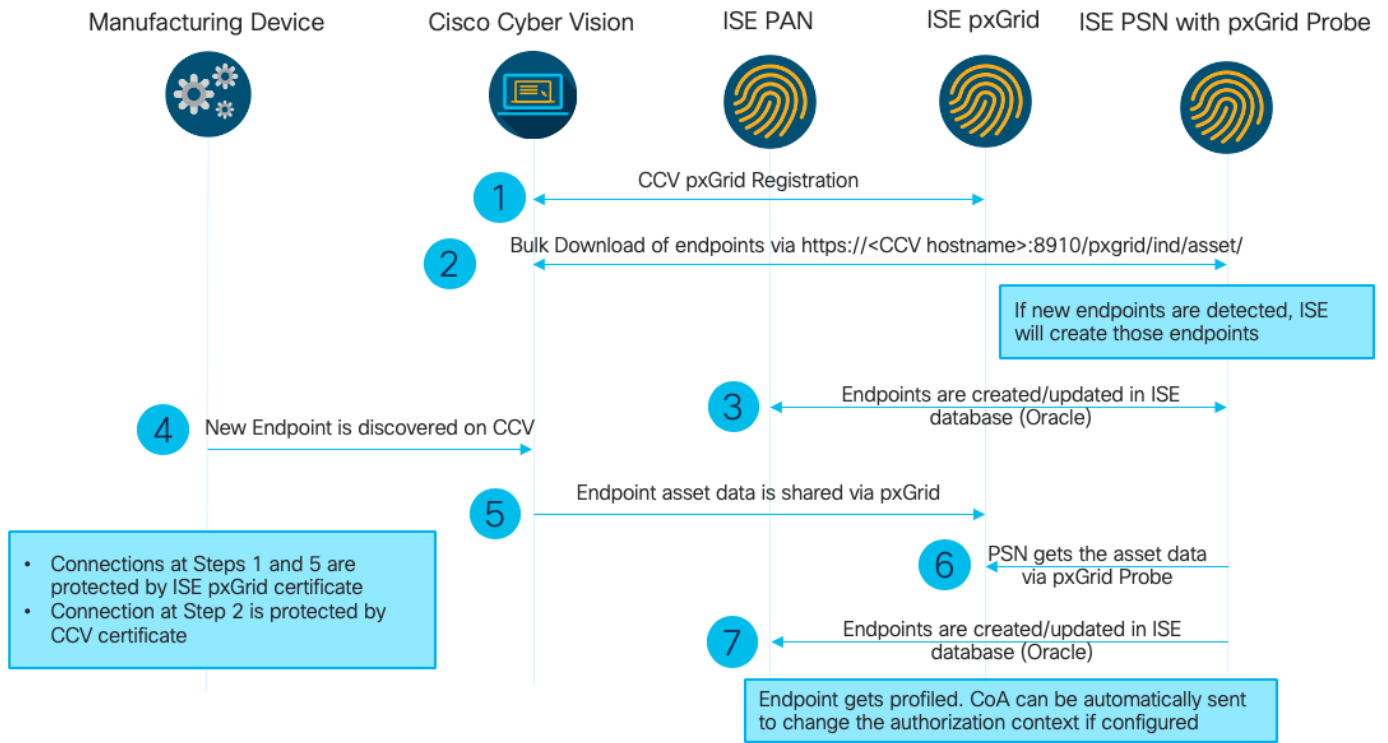
本檔案中的資訊是根據以下軟體和硬體版本：

- Cisco ISE版本2.7補丁1
- 思科網路願景版本3.1.0
- 工業乙太網路交換器IE-4000-4TC4G-E(含15.2(6)E)

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。

設定

高級流程圖



此ISE部署用於設定。

Deployment Nodes

| <input type="checkbox"/> Edit <input type="checkbox"/> Register <input type="checkbox"/> Syncup <input type="checkbox"/> Deregister | | | |
|---|--|----------------|------------------|
| Hostname | Personas | Role(s) | Services |
| <input type="checkbox"/> ISE27-1ek | Administration, Monitoring, Policy Service, pxGrid | PRI(A), PRI(M) | ALL |
| <input type="checkbox"/> ISE27-2ek | Administration, Monitoring, Policy Service | SEC(A), SEC(M) | SESSION,PROFILER |

ISE 2.7-1ek是主管理節點(PAN)節點和pxGrid節點。

ISE 2.7-2ek是啟用pxGrid探測的策略服務節點(PSN)。

以下是與上述圖對應的步驟。

1. CCV通過pxGrid版本2註冊到ISE上的assetTopic。來自CCV的相應日誌：

附註：若要檢視CCV上的pxGrid日誌，請發出以下命令**journalctl -u pxgrid-agent**。

```

root@center:~# journalctl -u pxgrid-agent -f
Jun 24 13:31:03 center pxgrid-agent-start.sh[1310]: pxgrid-agent RPC server listening to:
'/tmp/pxgrid-agent.sock' [caller=main.go:102]
Jun 24 13:31:03 center pxgrid-agent-start.sh[1310]: pxgrid-agent Request
path=/pxgrid/control/AccountActivate body={}
[caller=control.go:127]
Jun 24 13:31:03 center pxgrid-agent-start.sh[1310]: pxgrid-agent Account activated
[caller=pxgrid.go:76]
Jun 24 13:31:03 center pxgrid-agent-start.sh[1310]: pxgrid-agent Request
path=/pxgrid/control/ServiceRegister
body={"name":"com.cisco.endpoint.asset","properties":{"assetTopic":"/topic/com.cisco.endpoint.as
set
  
```

```
Jun 24 13:31:03 center pxgrid-agent-start.sh[1310]: pxgrid-agent Service registered, ID:
4b9af94b-9255-46df-b5ef-24bdbba99f3a
[caller=pxgrid.go:94]
Jun 24 13:31:03 center pxgrid-agent-start.sh[1310]: pxgrid-agent Request
path=/pxgrid/control/ServiceLookup
body={"name":"com.cisco.ise.pubsub"} [caller=control.go:127]
Jun 24 13:31:03 center pxgrid-agent-start.sh[1310]: pxgrid-agent Request
path=/pxgrid/control/AccessSecret
body={"peerNodeName":"com.cisco.ise.pubsub"} [caller=control.go:127]
Jun 24 13:31:03 center pxgrid-agent-start.sh[1310]: pxgrid-agent Websocket connect
url=wss://ISE27-1ek.example.com:8910/pxgrid/ise/pubsub [caller=endpoint.go:102]
Jun 24 13:31:03 center pxgrid-agent-start.sh[1310]: pxgrid-agent STOMP CONNECT host=10.48.17.86
[caller=endpoint.go:111]
Jun 24 13:33:27 center pxgrid-agent-start.sh[1310]: pxgrid-agent API: getSyncStatus
[caller=sync_status.go:34]
Jun 24 13:33:28 center pxgrid-agent-start.sh[1310]: pxgrid-agent Cyber Vision is in sync with
ISE [caller=assets.go:67]
Jun 24 13:36:03 center pxgrid-agent-start.sh[1310]: pxgrid-agent Request
path=/pxgrid/control/ServiceReregister
body={"id":"4b9af94b-9255-46df-b5ef-24bdbba99f3a"} [caller=control.go:127]
```

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

```
2020-06-24 13:41:37,091 DEBUG [ProfilerINDSubscriberPoller-56-thread-1][
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::- Looking for new publishers ...
2020-06-24 13:41:37,104 DEBUG [ProfilerINDSubscriberPoller-56-thread-1][
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::- Existing services are:
[Service [name=com.cisco.endpoint.asset, nodeName=cv-jens,
properties={assetTopic=/topic/com.cisco.endpoint.asset,
restBaseUrl=https://Center:8910/pxgrid/ind/asset/,
wsPubsubService=com.cisco.ise.pubsub}]]
2020-06-24 13:41:37,104 INFO [ProfilerINDSubscriberPoller-56-thread-1][
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::- New services are: []
2020-06-24 13:41:37,114 INFO [ProfilerINDSubscriberPoller-56-thread-1][
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::- NODENAME:cv-jens
2020-06-24 13:41:37,114 INFO [ProfilerINDSubscriberPoller-56-thread-1][
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::- REQUEST
BODY{"offset":"0","limit":"500"}
2020-06-24 13:41:37,158 INFO [ProfilerINDSubscriberPoller-56-thread-1][
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::- Response status={}200
2020-06-24 13:41:37,159 INFO [ProfilerINDSubscriberPoller-56-thread-1][
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::- Content: {OUT_OF_SYNC}
2020-06-24 13:41:37,159 INFO [ProfilerINDSubscriberPoller-56-thread-1][
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::- Status is :{OUT_OF_SYNC}
2020-06-24 13:41:37,159 DEBUG [ProfilerINDSubscriberPoller-56-thread-1][
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::-
Static set after adding new services: [Service [name=com.cisco.endpoint.asset,
nodeName=cv-jens, properties={assetTopic=/topic/com.cisco.endpoint.asset,
restBaseUrl=https://Center:8910/pxgrid/ind/asset/, wsPubsubService=com.cisco.ise.pubsub}]]
2020-06-24 13:41:37,169 INFO [ProfilerINDSubscriberBulkRequestPool-77-thread-1][
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::- NODENAME:cv-jens
2020-06-24 13:41:37,169 INFO [ProfilerINDSubscriberBulkRequestPool-77-thread-1][
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::- REQUEST
BODY{"offset":"0","limit":"500"}
2020-06-24 13:41:37,600 INFO [ProfilerINDSubscriberBulkRequestPool-77-thread-1][
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::- Response status={}200
2020-06-24 13:41:37,604 INFO [ProfilerINDSubscriberBulkRequestPool-77-thread-1][
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::- Content:
{"assets":[{"assetId":"88666e21-6eba-5c1e-b6a9-930c6076119d","assetName":"Xerox
0:0:0","assetIpAddress":"","
"assetMacAddress":"00:00:00:00:00:00","assetVendor":"XEROX
```

3. 端點將新增到PSN並啟用pxGrid探測，並且PSN將持續事件傳送到PAN以儲存這些端點

(profiler.log)。在ISE上建立的終端可以在情景可視性下的終端詳細資訊中檢視。

```
2020-06-24 13:41:37,677 DEBUG [ProfilerINDSubscriberBulkRequestPool-77-thread-1][  
cisco.profiler.infrastructure.probemgr.INDSubscriber -:::- mac address is :28:63:36:1e:10:05ip  
address is :192.168.105.150  
2020-06-24 13:41:37,677 DEBUG [ProfilerINDSubscriberBulkRequestPool-77-thread-1][  
cisco.profiler.infrastructure.probemgr.INDSubscriber -:::- sending endpoint to  
forwarder{"assetId":  
"01c8f9dd-8538-5eac-a924-d6382ce3df2d", "assetName": "Siemens  
192.168.105.150", "assetIpAddress": "192.168.105.150",  
"assetMacAddress": "28:63:36:1e:10:05", "assetVendor": "Siemens  
AG", "assetProductId": "", "assetSerialNumber": "",  
"assetDeviceType": "", "assetSwRevision": "", "assetHwRevision": "", "assetProtocol": "ARP,  
S7Plus", "assetCustomAttributes": [],  
"assetConnectedLinks": []}  
2020-06-24 13:41:37,677 INFO [ProfilerINDSubscriberBulkRequestPool-77-thread-1][  
cisco.profiler.infrastructure.probemgr.Forwarder -:::- Forwarder Mac 28:63:36:1E:10:05  
MessageCode null epSource pxGrid Probe  
2020-06-24 13:41:37,677 DEBUG [ProfilerINDSubscriberBulkRequestPool-77-thread-1][  
cisco.profiler.infrastructure.probemgr.INDSubscriber -:::- Endpoint is  
processedEndPoint[id=<null>, name=<null>]  
MAC: 28:63:36:1E:10:05  
Attribute:BYODRegistration value:Unknown  
Attribute:DeviceRegistrationStatus value:NotRegistered  
Attribute:EndPointPolicy value:Unknown  
Attribute:EndPointPolicyID value:  
Attribute:EndPointSource value:pxGrid Probe  
Attribute:MACAddress value:28:63:36:1E:10:05  
Attribute:MatchedPolicy value:Unknown  
Attribute:MatchedPolicyID value:  
Attribute:NmapSubnetScanID value:0  
Attribute:OUI value:Siemens AG  
Attribute:PolicyVersion value:0  
Attribute:PortalUser value:  
Attribute:PostureApplicable value:Yes  
Attribute:StaticAssignment value:false  
Attribute:StaticGroupAssignment value:false  
Attribute:Total Certainty Factor value:0  
Attribute:assetDeviceType value:  
Attribute:assetHwRevision value:  
Attribute:assetId value:01c8f9dd-8538-5eac-a924-d6382ce3df2d  
Attribute:assetIpAddress value:192.168.105.150  
Attribute:assetMacAddress value:28:63:36:1e:10:05  
Attribute:assetName value:Siemens 192.168.105.150  
Attribute:assetProductId value:  
Attribute:assetProtocol value:ARP, S7Plus  
Attribute:assetSerialNumber value:  
Attribute:assetSwRevision value:  
Attribute:assetVendor value:Siemens AG  
Attribute:ip value:192.168.105.150  
Attribute:SkipProfiling value:false
```

4.將終端放入組後，CCV通過埠8910傳送STOMP消息，以使用自定義屬性中的組資料更新終端。
來自CCV的相應日誌：

```
root@center:~# journalctl -u pxgrid-agent -f  
Jun 24 14:32:04 center pxgrid-agent-start.sh[1216]: pxgrid-agent STOMP SEND  
destination=/topic/com.cisco.endpoint.asset  
body={"opType": "UPDATE", "asset": {"assetId": "ce01ade2-eb6f-53c8-a646-9661b10c976e",  
"assetName": "Cisco  
a0:3a:59", "assetIpAddress": "", "assetMacAddress": "00:f2:8b:a0:3a:59", "assetVendor": "Cisco
```

```
Systems, Inc",
"assetProductId":"","assetSerialNumber":"","assetDeviceType":"","assetSwRevision":"","assetHwRevision":"","assetProtocol":"","
"assetCustomAttributes": [{"key": "assetGroup", "value": "Group1"}], {"key": "assetCCVGrp", "value": "Group1"}],
"assetConnectedLinks": []}] [caller=endpoint.go:118]
```

5. PxGrid節點接收STOMP更新並將此消息轉發給所有訂戶，其中包含已啟用pxGrid探測功能的PSN。pxGrid節點上的pxgrid-server.log。

```
2020-06-24 14:40:13,765 TRACE [Thread-1631][] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -
::::-
stomp=SEND:{content-length=453, destination=/topic/com.cisco.endpoint.asset}
2020-06-24 14:40:13,766 TRACE [Thread-1631][] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -
::::-
session [2b,cv-jens,OPEN] is permitted (cached) to send to
topic=/topic/com.cisco.endpoint.asset:
2020-06-24 14:40:13,766 TRACE [Thread-1631][]
cpm.pxgridwebapp.ws.pubsub.SubscriptionThreadedDistributor -::::-
Distributing stomp frame from=[2b,cv-jens,OPEN], topic=/topic/com.cisco.endpoint.asset,
true:true
2020-06-24 14:40:13,766 TRACE [Thread-1631][]
cpm.pxgridwebapp.ws.pubsub.SubscriptionThreadedDistributor -::::-
Distributing stomp frame from=[2b,cv-jens,OPEN],
topic=/topic/com.cisco.endpoint.asset,to=[19,ise-admin-ise27-2ek,OPEN]
2020-06-24 14:40:13,766 TRACE [Thread-1631][]
cpm.pxgridwebapp.ws.pubsub.SubscriptionThreadedDistributor -::::-
Distributing stomp frame from=[2b,cv-jens,OPEN], topic=/topic/wildcard,to=[2a,ise-fanout-ise27-
1ek,OPEN]
```

6.啟用了pxGrid探測的PSN作為資產主題上的訂閱伺服器，接收來自pxGrid節點的消息並更新終端(profiler.log)。在ISE上更新的終端可以在情景可視性下的終端詳細資訊中檢視。

```
2020-06-24 14:40:13,767 DEBUG [Grizzly(2)][]
cisco.profiler.infrastructure.probemgr.INDSsubscriber -::::-
Parsing push notification response: {"opType": "UPDATE", "asset": {"assetId": "ce01ade2-eb6f-53c8-
a646-9661b10c976e",
"assetName": "Cisco
a0:3a:59", "assetIpAddress": "", "assetMacAddress": "00:f2:8b:a0:3a:59", "assetVendor": "Cisco
Systems, Inc",
"assetProductId": "", "assetSerialNumber": "", "assetDeviceType": "", "assetSwRevision": "", "assetHwRevision": "",
"assetProtocol": "", "assetCustomAttributes": [{"key": "assetGroup", "value": "Group1"}], {"key": "assetC
CVGrp", "value": "Group1"}],
"assetConnectedLinks": []}]
2020-06-24 14:40:13,767 DEBUG [Grizzly(2)][]
cisco.profiler.infrastructure.probemgr.INDSsubscriber -::::-
sending endpoint to forwarder{"assetId": "ce01ade2-eb6f-53c8-a646-
9661b10c976e", "assetName": "Cisco a0:3a:59", "assetIpAddress": "",
"assetMacAddress": "00:f2:8b:a0:3a:59", "assetVendor": "Cisco Systems,
Inc", "assetProductId": "", "assetSerialNumber": "",
"assetDeviceType": "", "assetSwRevision": "", "assetHwRevision": "", "assetProtocol": "",
"assetCustomAttributes": [{"key": "assetGroup", "value": "Group1"}], {"key": "assetCCVGrp", "value": "Gro
up1"}], "assetConnectedLinks": []}]
2020-06-24 14:40:13,768 INFO [Grizzly(2)][] cisco.profiler.infrastructure.probemgr.Forwarder -
::::-
Forwarder Mac 00:F2:8B:A0:3A:59 MessageCode null epSource pxGrid Probe
2020-06-24 14:40:13,768 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.probemgr.ForwarderHelper -:
00:F2:8B:A0:3A:59:87026690-b628-11ea-bdb7-82edacd9a457:ProfilerCollection:- sequencing Radius
message for mac = 00:F2:8B:A0:3A:59
2020-06-24 14:40:13,768 INFO [forwarder-9][] cisco.profiler.infrastructure.probemgr.Forwarder -:
```

```

00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:ProfilerCollection:-
Processing endpoint:00:F2:8B:A0:3A:59 MessageCode null epSource pxGrid Probe
2020-06-24 14:40:13,768 DEBUG [forwarder-9][] com.cisco.profiler.im.EndPoint -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:ProfilerCollection:-
filtered custom attributes are:{assetGroup=Group1, assetCCVGrp=Group1}
2020-06-24 14:40:13,768 DEBUG [forwarder-9][] cisco.profiler.infrastructure.probemgr.Forwarder -
:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:ProfilerCollection:- Radius
Filtering:00:F2:8B:A0:3A:59
2020-06-24 14:40:13,768 DEBUG [forwarder-9][] cisco.profiler.infrastructure.probemgr.Forwarder -
:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:ProfilerCollection:- Endpoint
Attributes:EndPoint[id=<null>,name=<null>]
MAC: 00:F2:8B:A0:3A:59
Attribute:2309ae60-693d-11ea-9cbe-02251d8f7c49 value:Group1
Attribute:BYODRegistration value:Unknown
Attribute:DeviceRegistrationStatus value:NotRegistered
Attribute:EndPointProfilerServer value:ISE27-2ek.example.com
Attribute:EndPointSource value:pxGrid Probe
Attribute:MACAddress value:00:F2:8B:A0:3A:59
Attribute:NmapSubnetScanID value:0
Attribute:OUI value:Cisco Systems, Inc
Attribute:PolicyVersion value:0
Attribute:PortalUser value:
Attribute:PostureApplicable value:Yes
Attribute:assetDeviceType value:
Attribute:assetGroup value:Group1
Attribute:assetHwRevision value:
Attribute:assetId value:ce0lade2-eb6f-53c8-a646-9661b10c976e
Attribute:assetIpAddress value:
Attribute:assetMacAddress value:00:f2:8b:a0:3a:59
Attribute:assetName value:Cisco a0:3a:59
Attribute:assetProductId value:
Attribute:assetProtocol value:
Attribute:assetSerialNumber value:
Attribute:assetSwRevision value:
Attribute:assetVendor value:Cisco Systems, Inc
Attribute:SkipProfiling value:false

```

7.啟用了pxGrid探測功能的PSN將重新分析終端，因為匹配了新策略(profiler.log)。

```

2020-06-24 14:40:13,773 INFO [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Classify Mac
00:F2:8B:A0:3A:59 MessageCode null epSource pxGrid Probe
2020-06-24 14:40:13,777 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Policy Cisco-Device matched
00:F2:8B:A0:3A:59 (certainty 10)
2020-06-24 14:40:13,777 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Policy ekorneyc_ASSET_Group1
matched 00:F2:8B:A0:3A:59 (certainty 20)
2020-06-24 14:40:13,778 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- After analyzing policy
hierarchy: Endpoint:
00:F2:8B:A0:3A:59 EndpointPolicy:ekorneyc_ASSET_Group1 for:20 ExceptionRuleMatched:false
2020-06-24 14:40:13,778 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Endpoint 00:F2:8B:A0:3A:59
Matched Policy Changed.
2020-06-24 14:40:13,778 DEBUG [forwarder-9][]

```

```
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Endpoint 00:F2:8B:A0:3A:59
IdentityGroup Changed.
2020-06-24 14:40:13,778 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Setting identity group ID on
endpoint
00:F2:8B:A0:3A:59 - 91b0fd10-a181-11ea-ala3-fe7d097d8c61
2020-06-24 14:40:13,778 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Calling end point cache with
profiled end point
00:F2:8B:A0:3A:59, policy ekorneyc_ASSET_Group1, matched policy ekorneyc_ASSET_Group1
2020-06-24 14:40:13,778 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Sending event to persist end
point
00:F2:8B:A0:3A:59, and ep message code = null
2020-06-24 14:40:13,778 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Endpoint 00:F2:8B:A0:3A:59
IdentityGroup / Logical Profile Changed. Issuing a Conditional CoA
```

組態

附註：即使您想要僅檢視assetGroup和情景可視性，也需執行步驟1 - 4。

1. 在一個PSN上啟用pxGrid探測

導航到管理>系統>部署，選擇具有PSN角色的ISE節點。切換到Profiling Configuration頁籤。確保pxGrid探測器已啟用。

Deployment

- Deployment
- PAN Failover

Deployment Nodes List > ISE27-2ek

Edit Node

General Settings | **Profiling Configuration**

- ▶ NETFLOW
- ▶ DHCP
- ▶ DHCPSPAN
- ▶ HTTP
- ▶ RADIUS
- ▶ Network Scan (NMAP)
- ▶ DNS
- ▶ SNMPQUERY
- ▶ SNMPTRAP
- ▶ Active Directory
- ▼ pxGrid

Description: The PXgrid probe to fetch attributes of MAC or IP-Address as a subscriber from PXGrid Queue

2.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**。根據此圖配置自定義屬性(assetGroup)。CCV 3.1.0僅支援自定義資產組屬性。

Identity 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

Identities Groups External Identity Sources Identity Source Sequences Settings

User Custom Attributes
User Authentication Settings
Endpoint Purge
Endpoint Custom Attributes

Endpoint Custom Attributes

Endpoint Attributes (for reference)

| Mandatory | Attribute Name | Data Type |
|-----------|------------------------|-----------|
| | PostureApplicable | STRING |
| | LogicalProfile | STRING |
| | EndPointPolicy | STRING |
| | AnomalousBehaviour | STRING |
| | OperatingSystem | STRING |
| | BYODRegistration | STRING |
| | PortalUser | STRING |
| | LastAUPAcceptanceHours | INT |

Endpoint Custom Attributes

Attribute Name:

Type: - +

3. 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」。配置類似於此映像的Profiler策略。此策略中使用的條件表達式為CUSTOMATTRIBUTE:assetGroup EQUALS Group1。

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Profiling

Profiler Policy List > ekorneyc_ASSET_Group1

Profiler Policy

* Name: Description:

Policy Enabled:

* Minimum Certainty Factor: (Valid Range 1 to 65535)

* Exception Action:

* Network Scan (NMAP) Action:

Create an Identity Group for the policy: Yes, create matching Identity Group
 No, use existing Identity Group hierarchy

* Parent Policy:

* Associated CoA Type:

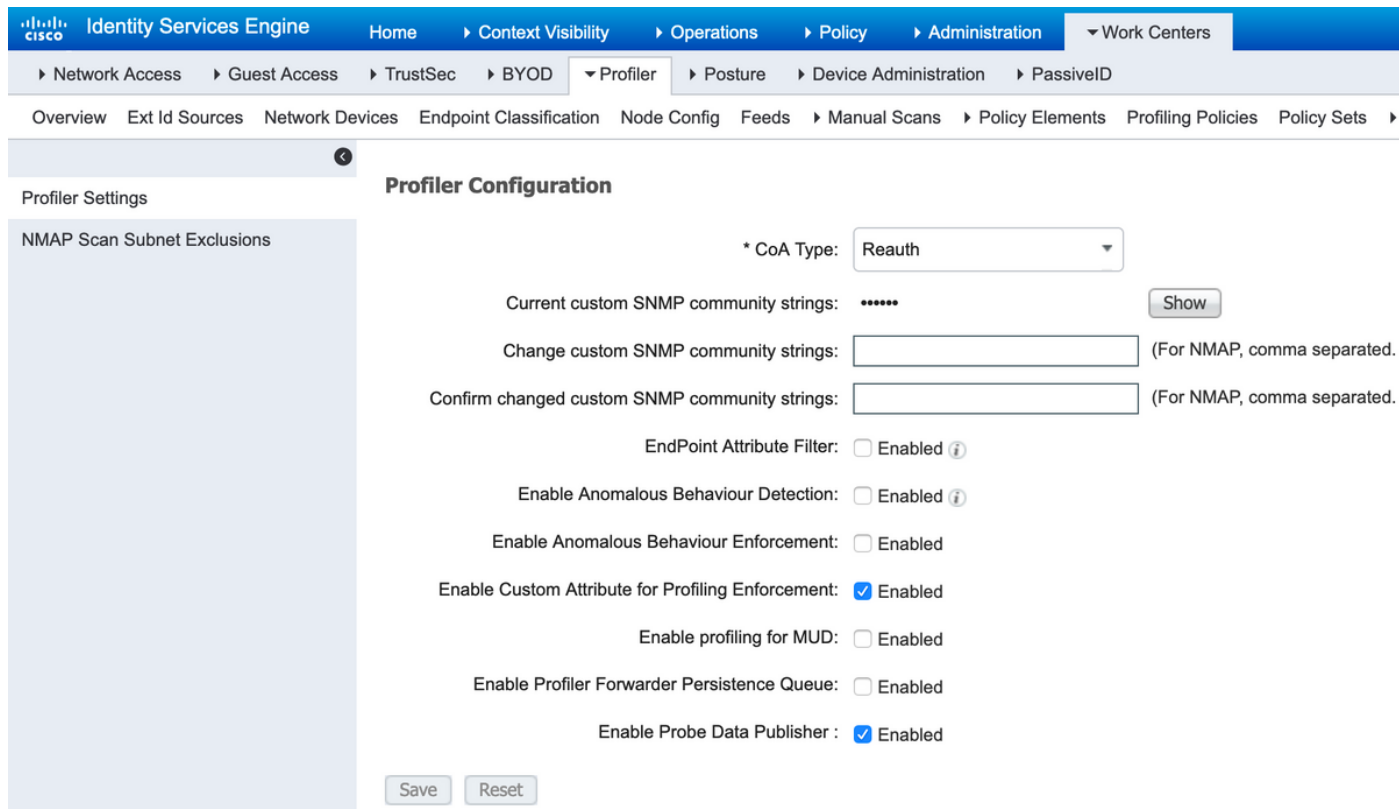
System Type: Administrator Created

Rules

If Condition: Then:

4. 啟用用於分析實施的自定義屬性

導航到工作中心(Work Centers)> Profiler(Profiler)>分析策略(Profiling Policies)。按一下「Add」。配置類似於此映像的Profiler策略。確保啟用分析實施的自定義屬性。



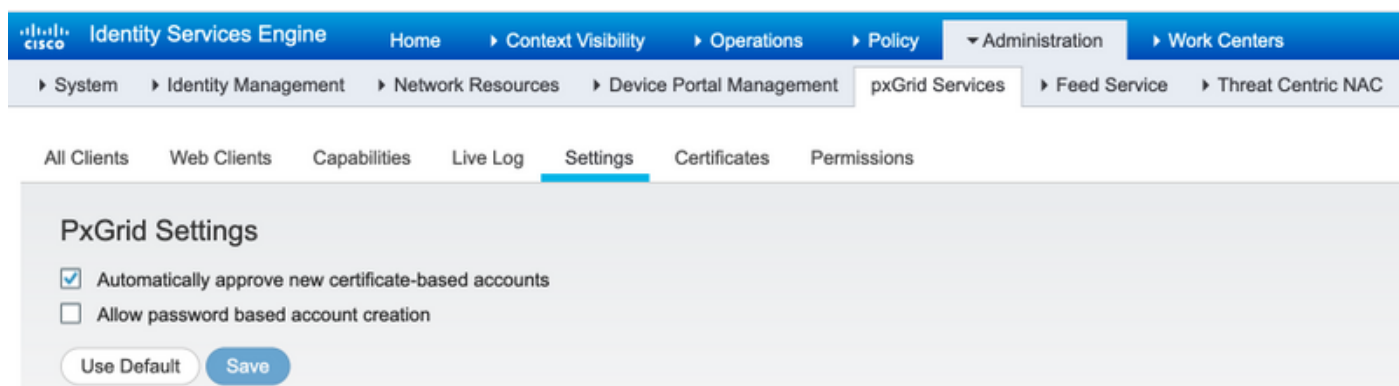
The screenshot shows the 'Profiler Configuration' page in the Cisco Identity Services Engine. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Profiler > Posture > Device Administration > PassiveID. The left sidebar contains 'Profiler Settings' and 'NMAP Scan Subnet Exclusions'. The main content area has the following settings:

- * CoA Type: Reauth (dropdown)
- Current custom SNMP community strings: ***** (with a 'Show' button)
- Change custom SNMP community strings: [text input] (For NMAP, comma separated.)
- Confirm changed custom SNMP community strings: [text input] (For NMAP, comma separated.)
- EndPoint Attribute Filter: Enabled ⓘ
- Enable Anomalous Behaviour Detection: Enabled ⓘ
- Enable Anomalous Behaviour Enforcement: Enabled
- Enable Custom Attribute for Profiling Enforcement: Enabled
- Enable profiling for MUD: Enabled
- Enable Profiler Forwarder Persistence Queue: Enabled
- Enable Probe Data Publisher: Enabled

At the bottom, there are 'Save' and 'Reset' buttons.

5. 配置pxGrid客戶端的自動審批

導航到管理> pxGrid服務>設定。選擇Automatically approve new certificate-based accounts，然後按一下Save。此步驟可確保整合完成後，您無需批准CCV。



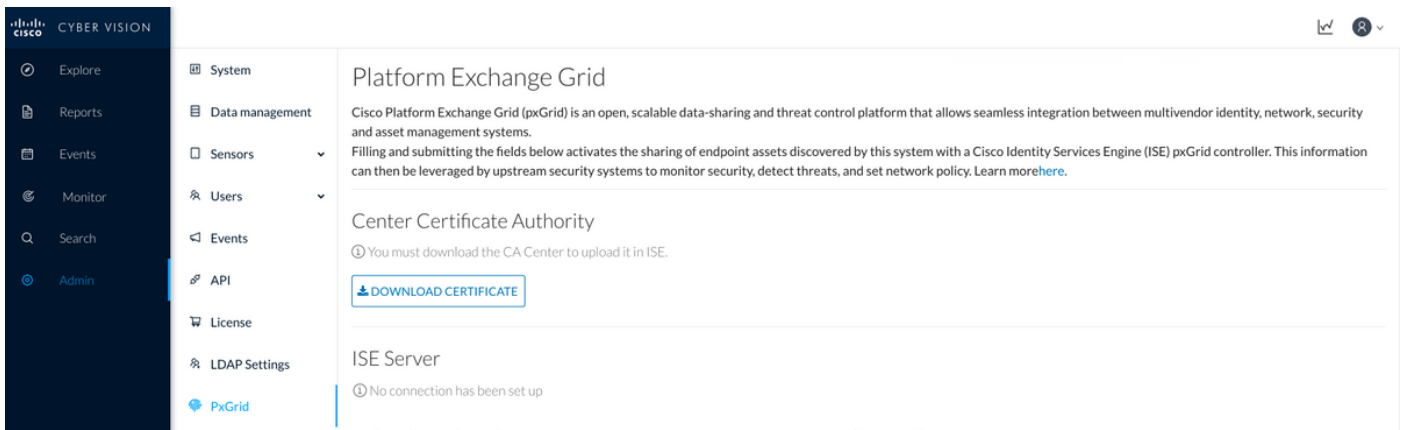
The screenshot shows the 'PxGrid Settings' page in the Cisco Identity Services Engine. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > pxGrid Services > Feed Service > Threat Centric NAC. The left sidebar contains 'All Clients', 'Web Clients', 'Capabilities', 'Live Log', 'Settings', 'Certificates', and 'Permissions'. The main content area has the following settings:

- Automatically approve new certificate-based accounts
- Allow password based account creation

At the bottom, there are 'Use Default' and 'Save' buttons.

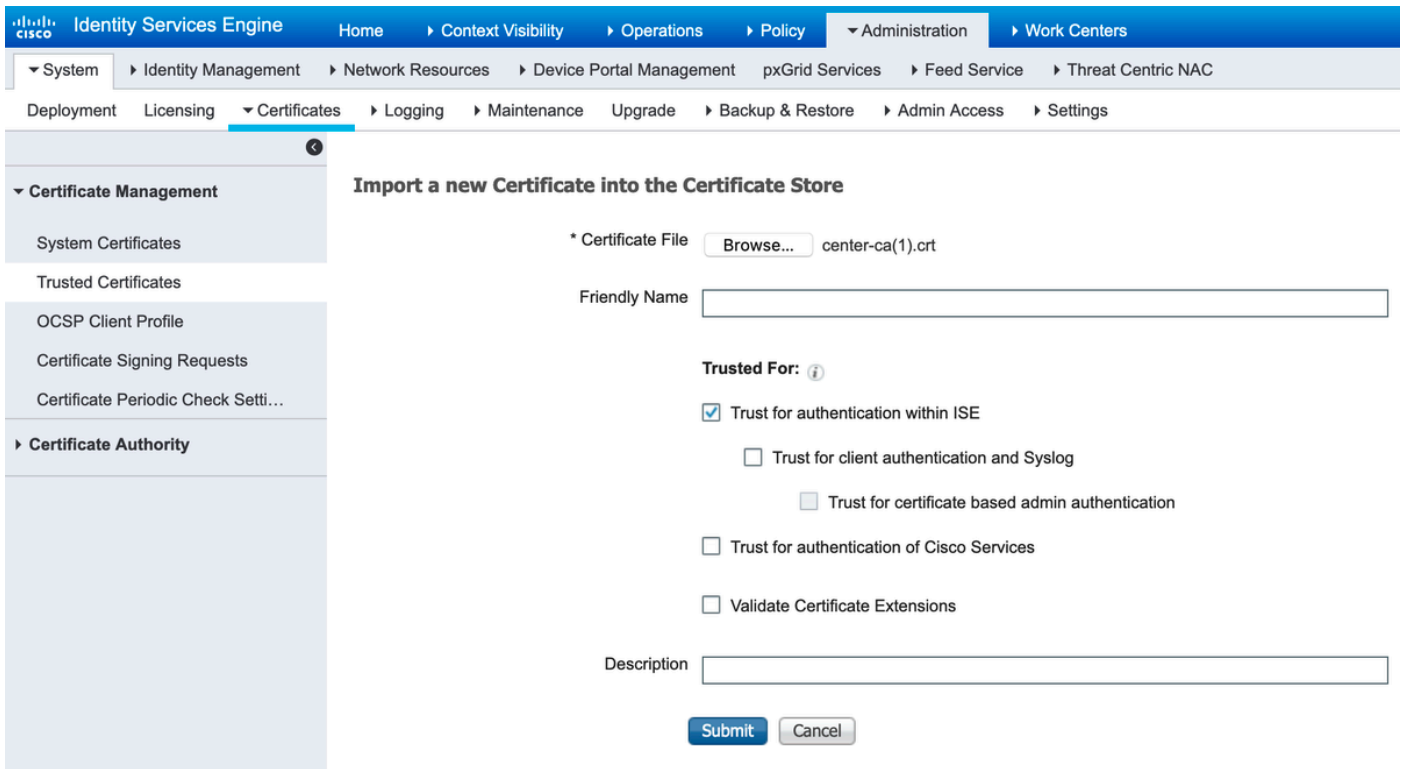
6. 匯出CCV證書

導覽至Admin > pxGrid。按一下「DOWNLOAD CERTIFICATE」。此證書在pxGrid註冊期間使用，因此ISE應信任它。



7. 將CCV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5中選擇CCV證書。按一下**Submit**。



8. 生成CCV證書

在pxGrid整合和更新期間，CCV需要客戶端證書。它應該由ISE內部CA使用**PxGrid_Certificate_Template**頒發。

導航到**管理> pxGrid服務>證書**。根據此影象填充欄位。公用名(CN)欄位是必填欄位，因為ISE CA的目標是頒發身份證書。您應輸入CCV的主機名，CN欄位值至關重要。若要檢查CCV的主機名，請發出**hostname**命令。選擇**PKCS12**作為**Certificate Download Format**。

```
root@center:~# hostname
center
root@center:~#
```

Identity 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

All Clients Web Clients Capabilities Live Log Settings Certificates Permissions

Generate pxGrid Certificates

I want to *

Common Name (CN) *

Description

Certificate Template [pxGrid_Certificate_Template](#) ⓘ

Subject Alternative Name (SAN) - +

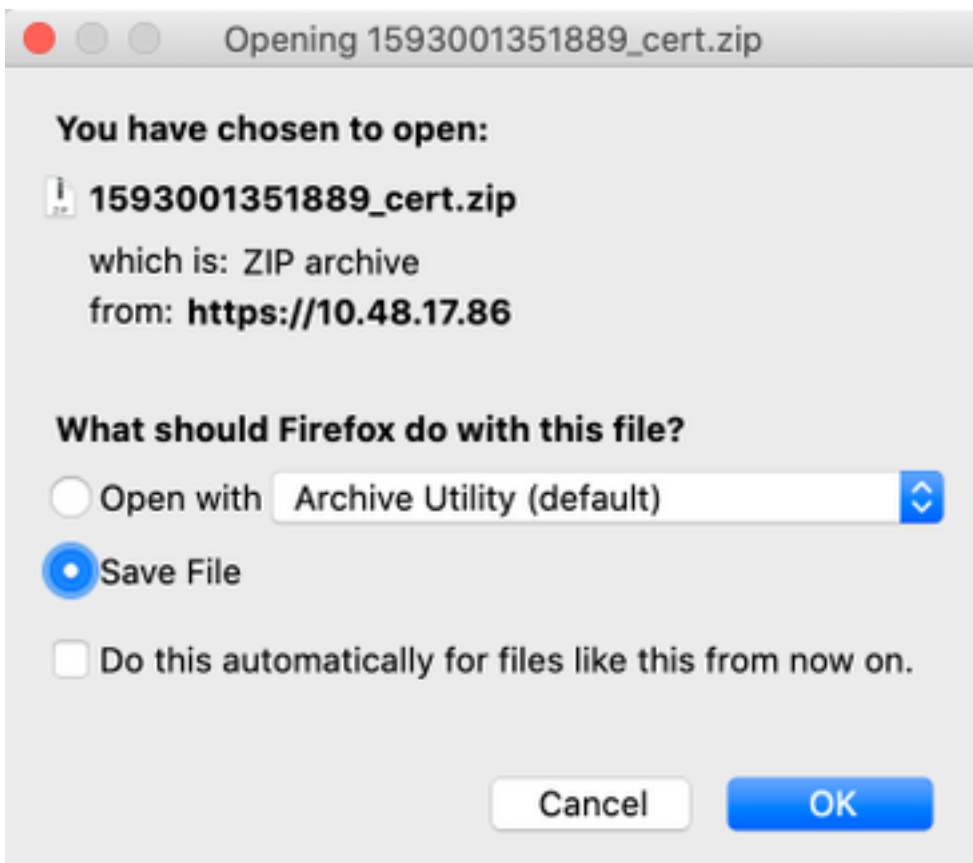
Certificate Download Format * ⓘ

Certificate Password * ⓘ

Confirm Password *

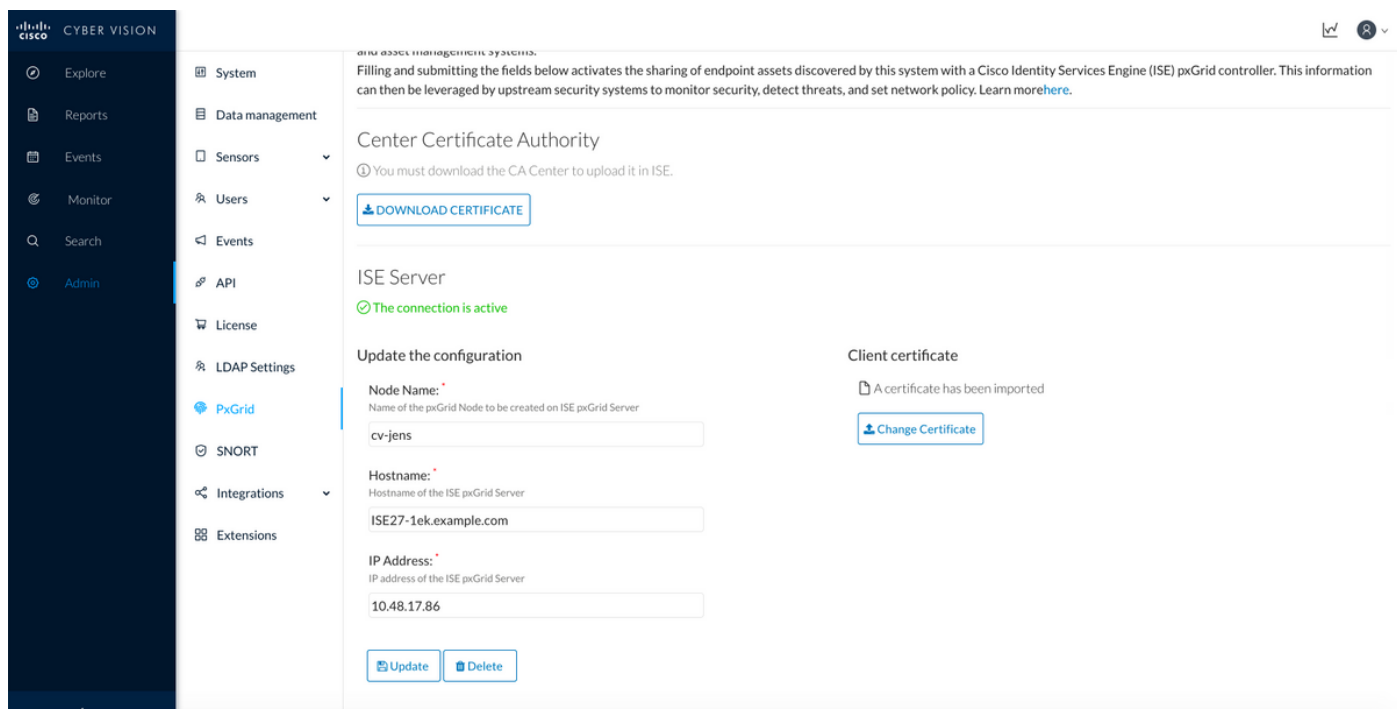
9. 下載PKCS12格式的證書鍵

當您以PKCS12格式安裝證書時，在CCV上安裝了CCV身份證書ISE內部CA鍵，以確保從ISE啟動pxGrid通訊時CCV信任ISE，例如pxGrid keepalive消息。



10. 在CCV上配置ISE整合詳細資訊

導覽至Admin > pxGrid。配置節點名稱，此名稱將在ISE上顯示為客戶端名稱，位於管理> pxGrid服務> Web客戶端。配置ISE pxGrid節點的主機名和IP地址。確保CCV可以解析ISE FQDN。



11.上傳CCV證書鍵並啟動整合

導覽至Admin > pxGrid。按一下「Change Certificate」。從步驟8-9中選擇ISE CA頒發的證書。從步驟8輸入密碼，然後按一下OK。

Do you want to enter a password?

.....

Ok

Cancel

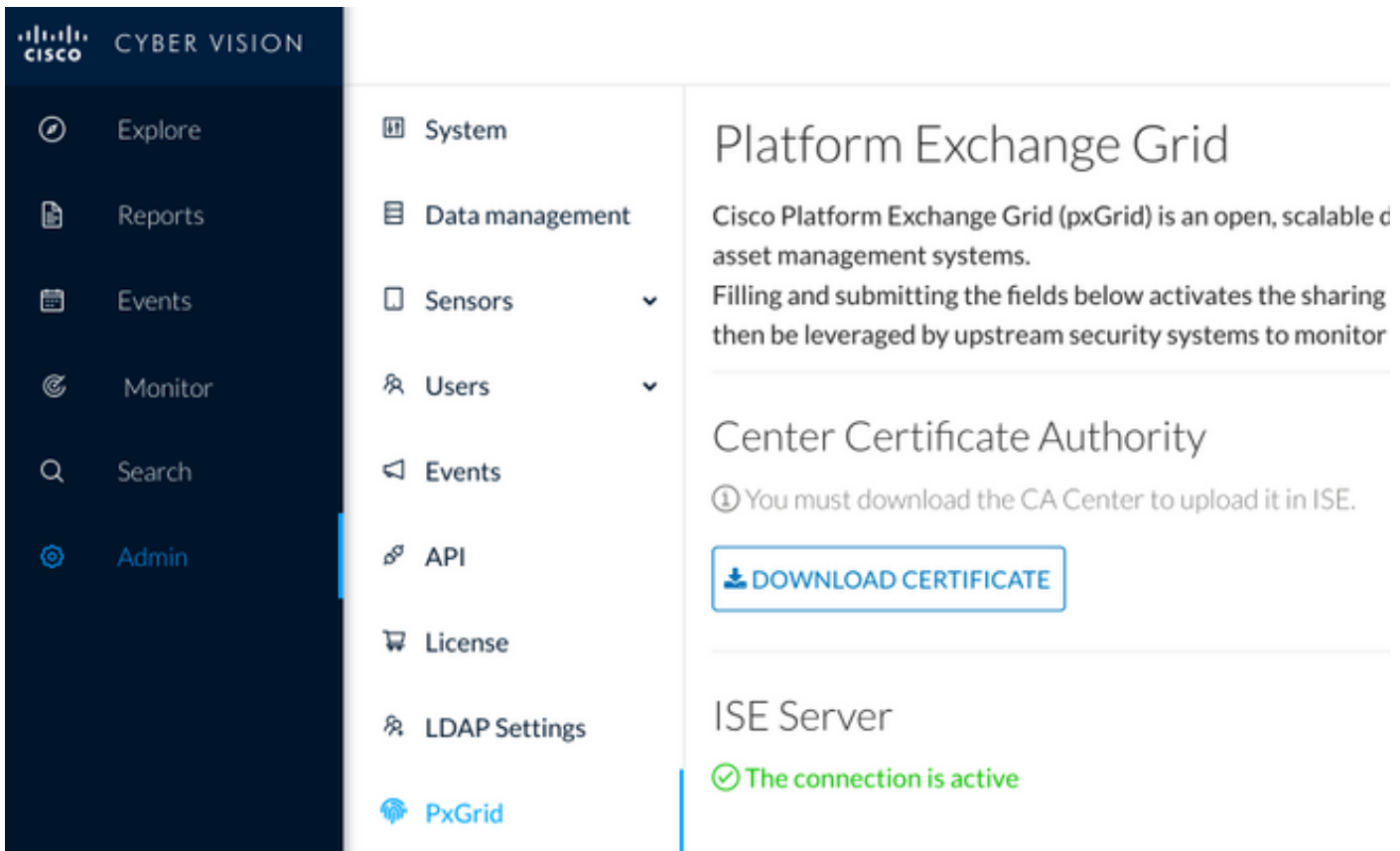
點選更新，這將觸發實際的CCV - ISE整合。

驗證

使用本節內容，確認您的組態是否正常運作。

CCV整合驗證

整合完成後，您可以通過導航到Admin > pxGrid來確認整合是否成功。您應該會看到ISE伺服器下的連線處於活動狀態消息。



ISE整合驗證

導航到管理> pxGrid服務> Web客戶端。確認CCV客戶端(cv-jens)的狀態為ON。

附註：在All Clients選單中，CCV pxGrid客戶端的狀態應該顯示為Offline，因為它只顯示pxGrid v1狀態。

| Client Name | Connect To | Session Id | Certificate | Subscriptions | Publications | IP Address | Status | Start time | Duration... |
|----------------------|------------|--------------|-------------------|----------------------------|----------------------------|--------------|--------|-------------------------|-------------|
| ise-fanout-ise27-1ek | ISE27-1ek | ISE27-1ek:15 | CN=ISE27-1ek.e... | /topic/distributed | /topic/distributed | 10.48.17.86 | ON | 2020-06-24 09:56:50 UTC | 00:04:37:18 |
| ise-bridge-ise27-1ek | ISE27-1ek | ISE27-1ek:23 | CN=ISE27-1ek.e... | | /topic/com.cisco.ise.co... | 127.0.0.1 | ON | 2020-06-24 10:06:52 UTC | 00:04:27:16 |
| ise-mnt-ise27-2ek | ISE27-1ek | ISE27-1ek:24 | No Certificate | /topic/com.cisco.ise.se... | /topic/com.cisco.ise.se... | 10.48.17.88 | ON | 2020-06-24 10:18:25 UTC | 00:04:15:43 |
| ise-admin-ise27-2ek | ISE27-1ek | ISE27-1ek:25 | No Certificate | /topic/com.cisco.endpo... | | 10.48.17.88 | ON | 2020-06-24 10:18:26 UTC | 00:04:15:43 |
| ise-admin-ise27-1ek | ISE27-1ek | ISE27-1ek:34 | CN=ISE27-1ek.e... | | /topic/com.cisco.ise.en... | 10.48.17.86 | OFF | 2020-06-24 12:09:50 UTC | 00:02:19:00 |
| ise-fanout-ise27-1ek | ISE27-1ek | ISE27-1ek:37 | CN=ISE27-1ek.e... | /topic/wildcard | | 127.0.0.1 | OFF | 2020-06-24 13:02:51 UTC | 00:01:08:00 |
| cv-jens | ISE27-1ek | ISE27-1ek:38 | CN=center | | | 10.48.43.241 | ON | 2020-06-24 13:39:12 UTC | 00:00:54:56 |
| ise-mnt-ise27-1ek | ISE27-1ek | ISE27-1ek:39 | CN=ISE27-1ek.e... | /topic/com.cisco.ise.se... | | 10.48.17.86 | ON | 2020-06-24 13:53:51 UTC | 00:00:40:17 |
| ise-fanout-ise27-1ek | ISE27-1ek | ISE27-1ek:40 | CN=ISE27-1ek.e... | /topic/wildcard | | 127.0.0.1 | OFF | 2020-06-24 14:11:51 UTC | 00:00:18:00 |
| ise-admin-ise27-1ek | ISE27-1ek | ISE27-1ek:41 | CN=ISE27-1ek.e... | | | 10.48.17.86 | ON | 2020-06-24 14:29:51 UTC | 00:00:04:17 |
| ise-fanout-ise27-1ek | ISE27-1ek | ISE27-1ek:42 | CN=ISE27-1ek.e... | /topic/wildcard | | 127.0.0.1 | ON | 2020-06-24 14:30:51 UTC | 00:00:03:17 |

附註：由於CSCvt78208，您將不會立即看到具有/topic/com.cisco.ise.endpoint.asset的CCV，它僅在首次發佈時顯示。

驗證CCV組更改

導航到瀏覽>所有資料>元件清單。按一下其中一個「Components (元件)」並將其新增到組中。

The screenshot shows the Cisco Cyber Vision interface. On the left is a navigation menu with options like Explore, Reports, Events, Monitor, Search, and Admin. The main area displays a list of 5 components. The component 'Cisco a0:3a:59' is highlighted. A modal window is open for this component, showing its details: IP: -, MAC: 00:f2:8b:a0:3a:59, and Properties: vendor-name: Cisco Systems, Inc, name: Cisco a0:3a:59, mac: 00:f2:8b:a0:3a:59. A 'Component' panel on the right shows options to 'Add to group', 'Create a new group', and lists existing groups: Group1 and Group2. Below the modal, there are summary cards for Flow (1), Events (3), Vulnerability (-), Credential (-), and Variable (-).

| Component | Group | First activity | Last activity | IP | MAC |
|--|-------|-----------------------------|----------------------------|-----------------|--------------------|
| KJK_IE4000_10.KJK_IE4000_10 00:f6:63:4d:d6:85 | - | Jun 24, 2020 12:37:49 PM | Jun 24, 2020 4:27:19 PM | - | 00:f6:63:4d:d6:85 |
| 01:00:0c:00:00:00 | - | May 11, 2020 6:44:15 PM | Jun 24, 2020 4:27:19 PM | - | 01:00:0c:00:00:00 |
| 01:00:0c:cccc:cccc | - | Mar 13, 2020 1:52:23 PM | Jun 24, 2020 4:27:19 PM | - | 01:00:0c:cccc:cccc |
| 255.255.255.255 | - | Mar 13, 2020 1:52:09 PM | Jun 24, 2020 4:25:45 PM | 255.255.255.255 | ff:ff:ff:ff:ff:ff |
| Cisco a0:3a:59 | - | Jun 24, 2020 2:47:34 PM | Jun 24, 2020 4:25:45 PM | - | 00:f2:8b:a0:3a:59 |

驗證/topic/com.cisco.ise.endpoint.asset現在已列為針對CCV的發佈。

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The main area displays a table of client sessions. The table has columns for Client Name, Connect To, Session Id, Certificate, Subscriptions, Publications, IP Address, Status, Start time, and Duration. The table is filtered by 'Client Name' and 'IP Address'. The table shows 15 rows of data, including sessions for 'ise-fanout-ise27-1ek', 'ise-bridge-ise27-1ek', 'ise-mnt-ise27-2ek', 'ise-admin-ise27-2ek', 'ise-mnt-ise27-1ek', 'ise-admin-ise27-1ek', 'ise-fanout-ise27-1ek', 'cv-jens', 'ise-fanout-ise27-1ek', 'ise-mnt-ise27-1ek', 'ise-fanout-ise27-1ek', 'ise-fanout-ise27-1ek', 'ise-fanout-ise27-1ek', 'ise-fanout-ise27-1ek', and 'ise-mnt-ise27-2ek'.

| Client Name | Connect To | Session Id | Certificate | Subscriptions | Publications | IP Address | Status | Start time | Duratio... |
|----------------------|------------|--------------|-------------------|--------------------------------------|---------------------------------------|--------------|--------|-------------------------|-------------|
| ise-fanout-ise27-1ek | ISE27-1ek | ISE27-1ek:15 | CN=ISE27-1ek.e... | /topic/distributed | /topic/distributed | 10.48.17.86 | OFF | 2020-06-24 09:58:50 UTC | 00:04:57:00 |
| ise-bridge-ise27-1ek | ISE27-1ek | ISE27-1ek:23 | CN=ISE27-1ek.e... | /topic/com.cisco.ise.config.profiler | /topic/com.cisco.ise.config.profiler | 127.0.0.1 | ON | 2020-06-24 10:06:52 UTC | 00:05:03:05 |
| ise-mnt-ise27-2ek | ISE27-1ek | ISE27-1ek:24 | No Certificate | /topic/com.cisco.ise.se... | /topic/com.cisco.ise.session.internal | 10.48.17.88 | OFF | 2020-06-24 10:18:25 UTC | 00:04:42:00 |
| ise-admin-ise27-2ek | ISE27-1ek | ISE27-1ek:25 | No Certificate | /topic/com.cisco.endpo... | /topic/com.cisco.endpo... | 10.48.17.88 | ON | 2020-06-24 10:18:26 UTC | 00:04:51:31 |
| ise-mnt-ise27-1ek | ISE27-1ek | ISE27-1ek:39 | CN=ISE27-1ek.e... | /topic/com.cisco.ise.se... | /topic/com.cisco.ise.se... | 10.48.17.86 | OFF | 2020-06-24 13:53:51 UTC | 00:00:58:00 |
| ise-admin-ise27-1ek | ISE27-1ek | ISE27-1ek:41 | CN=ISE27-1ek.e... | /topic/com.cisco.ise.endpoint | /topic/com.cisco.ise.endpoint | 10.48.17.86 | ON | 2020-06-24 14:29:51 UTC | 00:00:40:06 |
| ise-fanout-ise27-1ek | ISE27-1ek | ISE27-1ek:42 | CN=ISE27-1ek.e... | /topic/wildcard | /topic/wildcard | 127.0.0.1 | OFF | 2020-06-24 14:30:51 UTC | 00:00:14:00 |
| cv-jens | ISE27-1ek | ISE27-1ek:43 | CN=center | /topic/com.cisco.endpoint.asset | /topic/com.cisco.endpoint.asset | 10.48.43.241 | ON | 2020-06-24 14:38:47 UTC | 00:00:31:10 |
| ise-fanout-ise27-1ek | ISE27-1ek | ISE27-1ek:44 | CN=ISE27-1ek.e... | /topic/wildcard | /topic/wildcard | 127.0.0.1 | OFF | 2020-06-24 14:45:52 UTC | 00:00:11:00 |
| ise-mnt-ise27-1ek | ISE27-1ek | ISE27-1ek:45 | CN=ISE27-1ek.e... | /topic/com.cisco.ise.se... | /topic/com.cisco.ise.se... | 10.48.17.86 | OFF | 2020-06-24 14:52:51 UTC | 00:00:17:00 |
| ise-fanout-ise27-1ek | ISE27-1ek | ISE27-1ek:46 | CN=ISE27-1ek.e... | /topic/distributed | /topic/distributed | 10.48.17.86 | OFF | 2020-06-24 14:53:53 UTC | 00:00:02:00 |
| ise-fanout-ise27-1ek | ISE27-1ek | ISE27-1ek:47 | CN=ISE27-1ek.e... | /topic/distributed | /topic/distributed | 10.48.17.86 | ON | 2020-06-24 14:55:53 UTC | 00:00:14:03 |
| ise-fanout-ise27-1ek | ISE27-1ek | ISE27-1ek:48 | CN=ISE27-1ek.e... | /topic/wildcard | /topic/wildcard | 127.0.0.1 | ON | 2020-06-24 14:57:52 UTC | 00:00:12:05 |
| ise-mnt-ise27-2ek | ISE27-1ek | ISE27-1ek:49 | No Certificate | /topic/com.cisco.ise.se... | /topic/com.cisco.ise.session.internal | 10.48.17.88 | ON | 2020-06-24 15:01:26 UTC | 00:00:08:31 |

確認通過CCV分配的Group1反映在ISE上，並通過導航到Context Visibility > Endpoints使分析策略生效。選擇在上一步中更新的端點。切換到屬性頁籤。自定義屬性部分應反映新配置的組。

Filters: *00:F2:8B:A0:3A:59

Endpoints > 00:F2:8B:A0:3A:59

00:F2:8B:A0:3A:59 [Refresh] [Edit] [Close]



MAC Address: 00:F2:8B:A0:3A:59
Username:
Endpoint Profile: ekorneyc_ASSET_Group1
Current IP Address:
Location:

Applications Attributes Authentication Threats Vulnerabilities

General Attributes

Description

Static Assignment false
Endpoint Policy ekorneyc_ASSET_Group1
Static Group Assignment false
Identity Group Assignment ekorneyc_ASSET_Group1

Custom Attributes

Filter [Settings]

| | Attribute String | Attribute Value |
|---|------------------|-----------------|
| x | Attribute String | Attribute Value |
| | assetGroup | Group1 |

「其他屬性」部分列出了從CCV接收的所有其他資產屬性。

Other Attributes

| | |
|--------------------------|--------------------------------------|
| BYODRegistration | Unknown |
| DeviceRegistrationStatus | NotRegistered |
| ElapsedDays | 0 |
| EndPointPolicy | ekorneyc_ASSET_Group1 |
| EndPointProfilerServer | ISE27-2ek.example.com |
| EndPointSource | pxGrid Probe |
| EndPointVersion | 14 |
| IdentityGroup | ekorneyc_ASSET_Group1 |
| InactiveDays | 0 |
| MACAddress | 00:F2:8B:A0:3A:59 |
| MatchedPolicy | ekorneyc_ASSET_Group1 |
| OUI | Cisco Systems, Inc |
| PolicyVersion | 9 |
| PostureApplicable | Yes |
| StaticAssignment | false |
| StaticGroupAssignment | false |
| Total Certainty Factor | 20 |
| assetId | ce01ade2-eb6f-53c8-a646-9661b10c976e |
| assetMacAddress | 00:f2:8b:a0:3a:59 |
| assetName | Cisco a0:3a:59 |
| assetVendor | Cisco Systems, Inc |

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

在ISE上啟用調試

要在ISE上啟用調試，請導航到**Administration > System > Logging > Debug Log Configuration**。將日誌級別設定為以下值：

| 《女神異聞錄》 PAN (可選) 已啟用pxGrid探測功能的 PSN | 元件名稱 探查器 | 日誌級別 調試 | 要檢查的檔案 profiler.log |
|--|-------------|------------|------------------------|
| PxGrid | 探查器 | 調試 | profiler.log |
| | pxgrid | 追蹤 | pxgrid-server.log |

在CCV上啟用調試

要在CCV上啟用調試，請執行以下操作：

- 使用 `touch /data/etc/sbs/pxgrid-agent.conf` 命令建立檔案 `/data/etc/sbs/pxgrid-agent.conf`
- 使用 `vi` 編輯器和 `vi /data/etc/sbs/pxgrid-agent.conf` 命令，將此內容貼上到 `pxgrid-agent.conf` 檔案中

```
# /data/etc/sbs/pxgrid-agent.conf
```

```
base:
```

```
loglevel: debug
```

- 通過運行 `systemctl restart pxgrid-agent` 命令重新啟動 `pxgrid-agent`
- 使用 `journalctl -u pxgrid-agent` 命令檢視日志

批次下載失敗

CCV在整合期間向ISE發佈批次下載URL。啟用了pxGrid探測的ISE PSN使用此URL執行批次下載。確保：

- 從ISE的角度可以正確解析URL中的主機名
- 允許從埠8910上的PSN到CCV的通訊

啟用pxGrid探測的PSN上的 `profiler.log`:

```
INFO [ProfilerINDSubscriberPoller-58-thread-1][[]
cisco.profiler.infrastructure.probemgr.INDSubscriber -:::- New services are:
[Service [name=com.cisco.endpoint.asset, nodeName=cv-jens4,
properties={assetTopic=/topic/com.cisco.endpoint.asset,
restBaseUrl=https://Center:8910/pxgrid/ind/asset/, wsPubsubService=com.cisco.ise.pubsub}]]
```

由於 [CSCvt75422](#)，批次下載可能會失敗，您應該在ISE上的 `profiler.log` 中看到此錯誤以確認它。缺陷在CCV 3.1.0中修復。

```
2020-04-09 10:47:22,832 ERROR [ProfilerINDSubscriberBulkRequestPool-212-thread-1][[]
cisco.profiler.infrastructure.probemgr.INDSubscriber
-:::- ProfilerError while sending bulkrequest to cv-jens4:This is not a JSON Object.
java.lang.IllegalStateException: This is not a JSON Object.
at com.google.gson.JsonElement.getAsJsonObject(JsonElement.java:83)
at
com.cisco.profiler.infrastructure.probemgr.INDSubscriber.parseJsonBulkResponse(INDSubscriber.java:161)
at
com.cisco.profiler.infrastructure.probemgr.INDSubscriber$BulkRequestWorkerThread.run(INDSubscriber.java:532)
at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149)
at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624)
at java.lang.Thread.run(Thread.java:748)
```

並非所有終端都在ISE上建立

CCV上的某些終端可能附加了太多的屬性，因此ISE資料庫將無法處理它。如果您在ISE的 `profiler.log` 中看到這些錯誤，可以確認。

```
2020-05-29 00:01:25,228 ERROR [admin-http-pool1][[] com.cisco.profiler.api.EDFEndPointHandler -
:::-
Failed to create endpoint 00:06:F6:2A:C4:2B ORA-12899:
value too large for column "CEPM"."EDF_EP_MASTER"."EDF_ENDPOINTIP" (actual:660, maximum: 100)
2020-05-29 00:01:25,229 ERROR [admin-http-pool1][[] com.cisco.profiler.api.EDFEndPointHandler -
```

::::-

Unable to create the endpoint.:ORA-12899:

value too large for column "CEPM"."EDF_EP_MASTER"."EDF_ENDPOINTIP" (actual: 660, maximum: 100)

com.cisco.epm.edf2.exceptions.EDF2SQLException: ORA-12899:

value too large for column "CEPM"."EDF_EP_MASTER"."EDF_ENDPOINTIP" (actual: 660, maximum: 100)

AssetGroup在ISE上不可用

如果AssetGroup在ISE上不可用，則很可能未使用自定義屬性配置分析策略（請參閱文檔配置部分中的步驟2-4.）。即使對於情景可視性，僅用於顯示組屬性，步驟2-4中的分析策略和其他設定也是必需的。

終端組更新未反映在ISE上

由於[CSCvu80175.CCV](#)不會將終端更新發佈到ISE，直到CCV在整合後立即重新啟動。作為解決方法完成整合後，您可以重新啟動CCV。

從CCV中刪除組不是從ISE中刪除組

之所以會出現此問題，是因為CCV [CSCvu47880上的已知缺陷](#)。在從CCV中刪除組期間傳送的pxGrid更新與預期格式不同，因此不會刪除組。

CCV從Web客戶端斷開

出現此問題的原因是ISE [CSCvu4780](#)上的已知缺陷，在該缺陷中，客戶端轉換為OFF狀態，然後從Web客戶端完全刪除。此問題在ISE的2.6補丁7和2.7補丁2中已解決。

如果您在ISE的pxgrid-server.log中看到以下錯誤，可以確認此錯誤：

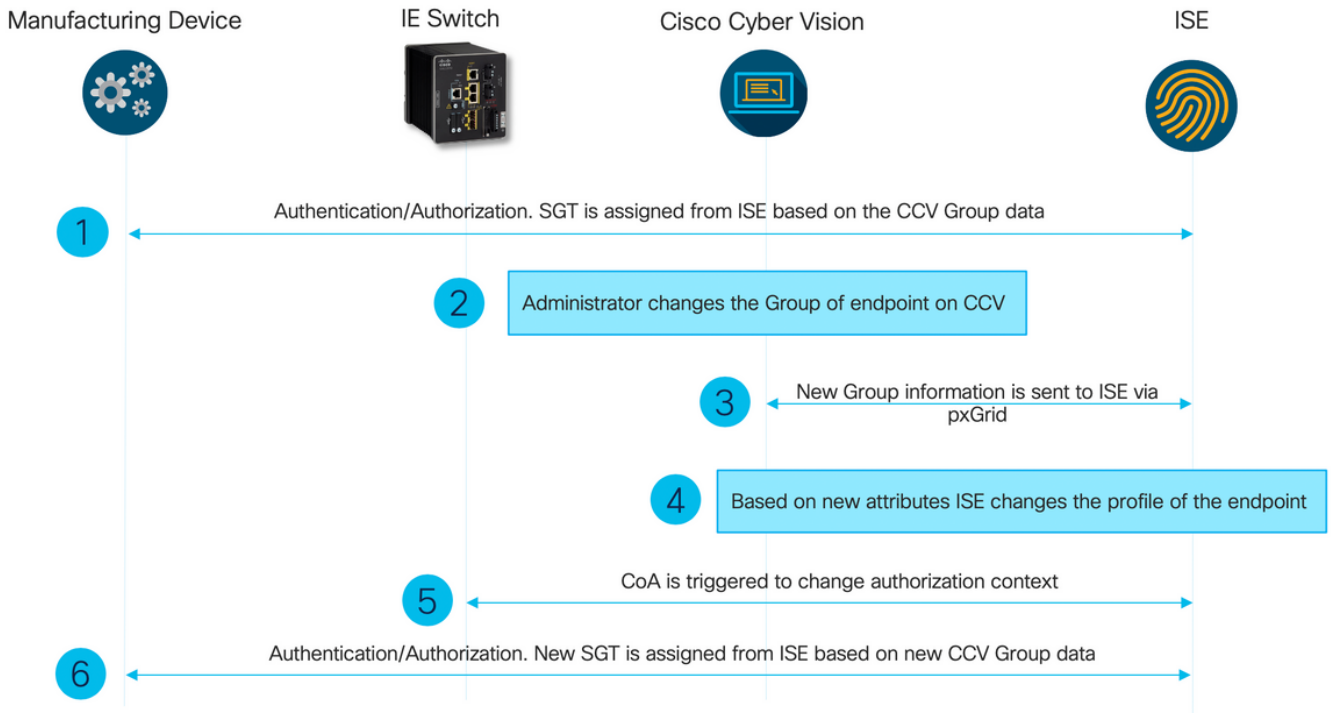
```
2020-06-26 09:42:28,772 DEBUG [Pxgrid-SessionManager-LookupAccountsTask][  
cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -::::-  
onClose: session=[14f,CLOSED], sessionInfo=WSSessionInfo [id=336, nodeName=cv-jens,  
addr=10.48.43.241, sessionId=14f, status=OFF,  
creationTime=2020-06-26 08:19:28.726, closeTime=2020-06-26 09:42:28.772,  
reason=VIOLATED_POLICY:Did not receive a pong: too slow ...,  
subscriptions=[], publications=[/topic/com.cisco.endpoint.asset]]
```

ISE與CCV TrustSec整合使用案例

此配置顯示了當TrustSec到位時ISE與CCV的整合如何有利於端到端安全性。這只是整合完成之後如何使用整合的其中一個示例。

附註：TrustSec交換機配置說明不在本文的討論範圍之內，但可以在附錄中找到。

拓撲和流



設定

1. 在ISE上配置可擴展組標籤

為了達到前面提到的使用案例，TrustSec標籤的IOT_Group1_Asset和IOT_Group2_Asset被手動配置為分別將組1 CCV資產與組2區分開來。導航到工作中心> TrustSec > 元件>安全組。按一下Add。名稱SGT，如下圖所示。

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Components TrustSec Policy Policy Sets SXP Troubleshoot Reports Settings

Security Groups

IP SGT Static Mapping

Security Group ACLs

Network Devices

Trustsec Servers

Security Groups

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

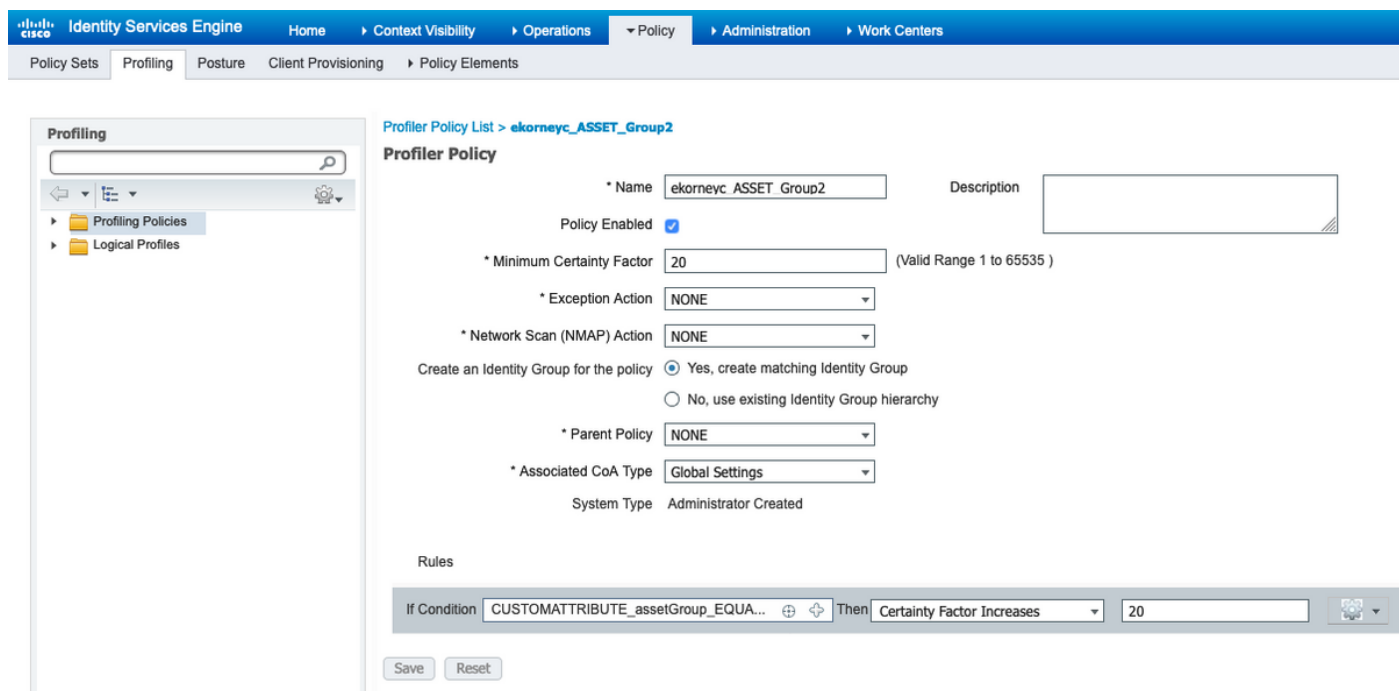
Edit
 Add
 Import
 Export
 Trash
 Push
 Verify Deploy

| <input type="checkbox"/> | Icon | Name | SGT (Dec / Hex) | Description | Learned from |
|--------------------------|------|---------------------|-----------------|------------------------------------|--------------|
| <input type="checkbox"/> | | Auditors | 9/0009 | Auditor Security Group | |
| <input type="checkbox"/> | | BYOD | 15/000F | BYOD Security Group | |
| <input type="checkbox"/> | | Contractors | 5/0005 | Contractor Security Group | |
| <input type="checkbox"/> | | Developers | 8/0008 | Developer Security Group | |
| <input type="checkbox"/> | | Development_Servers | 12/000C | Development Servers Security Group | |
| <input type="checkbox"/> | | Employees | 4/0004 | Employee Security Group | |
| <input type="checkbox"/> | | Guests | 6/0006 | Guest Security Group | |
| <input type="checkbox"/> | | IOT_Group1_Asset | 16/0010 | | |
| <input type="checkbox"/> | | IOT_Group2_Asset | 17/0011 | | |

2. 使用組2的自定義屬性配置分析器策略

附註：在本文檔的第一部分中的步驟3中完成了組1的配置分析。

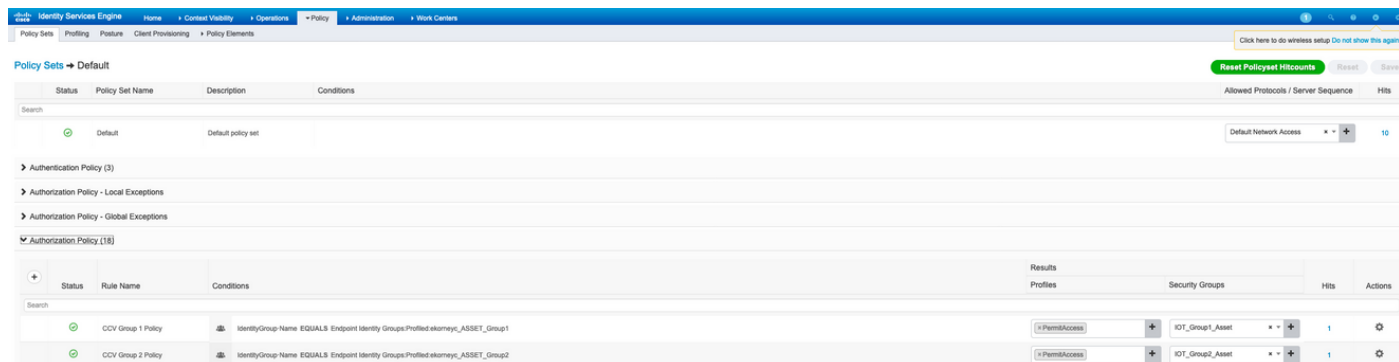
導航到工作中心(Work Centers)> Profiler(Profiler)>分析策略(Profiling Policies)。按一下「Add」。配置類似於此映像的Profiler策略。此策略中使用的條件表達式為CUSTOMATTRIBUTE:assetGroup EQUALS Group2。



3.配置授權策略以根據ISE上的終端身份組分配SGT

導航到Policy > Policy Sets。選擇Policy Set並根據此映像配置Authorization Policies。請注意，因此會分配步驟1中配置的SGT。

| 規則名稱 | 狀況 | 配置檔案 | 安全組 |
|----------|---|--------------|------------------|
| CCV組1策略 | IdentityGroup-Name EQUALS Endpoint Identity Groups:Profiled:ekorneyc_ ASSET_Group1 | PermitAccess | IOT_Group1_Asset |
| CCV第2組策略 | IdentityGroup-Name EQUALS Endpoint Identity Groups:Profiled:ekorneyc_ ASSET_Group2 | PermitAccess | IOT_Group2_Asset |



驗證

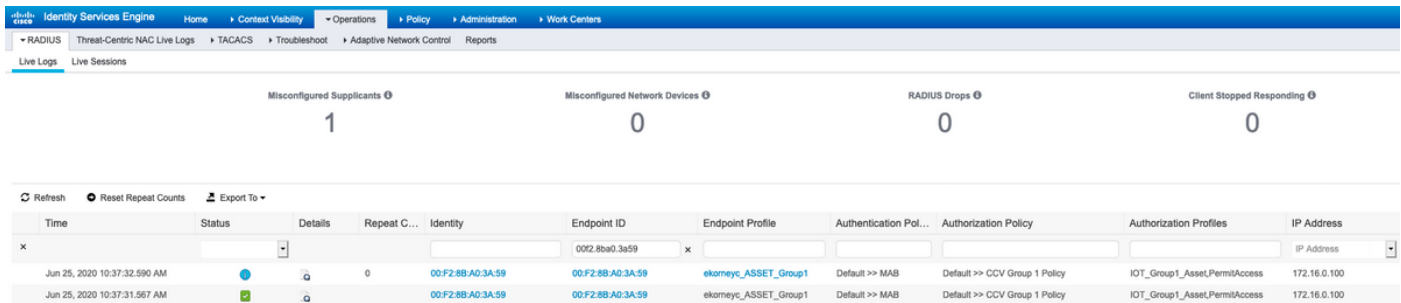
使用本節內容，確認您的組態是否正常運作。

1. 終端基於CCV組1進行身份驗證

在Switch上，您可以看到環境資料包括SGT的16-54:IOT_Group1_Asset和17-54:IOT_Group2_Asset。

```
KJK_IE4000_10#show cts environment-data
CTS Environment Data
=====
Current state = COMPLETE
Last status = Successful
Local Device SGT:
SGT tag = 0-00:Unknown
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
*Server: 10.48.17.86, port 1812, A-ID 11A2F46141F0DC8F082EFBC4C49D217E
Status = ALIVE
auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Multicast Group SGT Table:
Security Group Name Table:
0-54:Unknown
2-54:TrustSec_Devices
3-54:Network_Services
4-54:Employees
5-54:Contractors
6-54:Guests
7-54:Production_Users
8-54:Developers
9-54:Auditors
10-54:Point_of_Sale_Systems
11-54:Production_Servers
12-54:Development_Servers
13-54:Test_Servers
14-54:PCI_Servers
15-54:BYOD
    16-54:IOT_Group1_Asset
    17-54:IOT_Group2_Asset
255-54:Quarantined_Systems
Environment Data Lifetime = 86400 secs
Last update time = 16:39:44 UTC Wed Jun 13 2035
Env-data expires in 0:23:59:53 (dd:hr:mm:sec)
Env-data refreshes in 0:23:59:53 (dd:hr:mm:sec)
Cache data applied = NONE
State Machine is running
KJK_IE4000_10#
```

端點進行身份驗證，因此**匹配CCV Group 1策略**，分配SGT IOT_Group1_Asset。



The screenshot shows the Identity Services Engine (ISE) Live Sessions interface. At the top, there are summary statistics: Misconfigured Supplicants (1), Misconfigured Network Devices (0), RADIUS Drops (0), and Client Stopped Responding (0). Below this is a table of active sessions. The table has columns for Time, Status, Details, Repeat Counts, Identity, Endpoint ID, Endpoint Profile, Authentication Policy, Authorization Policy, Authorization Profiles, and IP Address. Two sessions are listed, both with a status of 'Success' and occurring at 10:37:32.590 AM and 10:37:31.567 AM on Jun 25, 2020. Both sessions are for endpoint 00F2:8B:A0:3A:59 and are associated with the 'ekomeyc_ASSET_Group1' profile. The authentication policy is 'Default >> MAB' and the authorization policy is 'Default >> CCV Group 1 Policy'. The authorization profiles are 'IOT_Group1_AssetPermitAccess' and the IP address is 172.16.0.100.

| Time | Status | Details | Repeat C... | Identity | Endpoint ID | Endpoint Profile | Authentication Pol... | Authorization Policy | Authorization Profiles | IP Address |
|------------------------------|---------|---------|-------------|------------------|------------------|----------------------|-----------------------|-------------------------------|------------------------------|--------------|
| Jun 25, 2020 10:37:32.590 AM | Success | | 0 | 00F2:8B:A0:3A:59 | 00F2:8B:A0:3A:59 | ekomeyc_ASSET_Group1 | Default >> MAB | Default >> CCV Group 1 Policy | IOT_Group1_AssetPermitAccess | 172.16.0.100 |
| Jun 25, 2020 10:37:31.567 AM | Success | | | 00F2:8B:A0:3A:59 | 00F2:8B:A0:3A:59 | ekomeyc_ASSET_Group1 | Default >> MAB | Default >> CCV Group 1 Policy | IOT_Group1_AssetPermitAccess | 172.16.0.100 |

Switch show authentication sessions interface fa1/7 detail 確認已成功應用Access-Accept資料。

KJK_IE4000_10#show authentication sessions interface fal/7 detail

Interface: FastEthernet1/7

MAC Address: 00f2.8ba0.3a59

IPv6 Address: Unknown

IPv4 Address: 172.16.0.100

User-Name: 00-F2-8B-A0-3A-59

Status: Authorized

Domain: DATA

Oper host mode: single-host

Oper control dir: both

Session timeout: N/A

Restart timeout: N/A

Periodic Acct timeout: N/A

Session Uptime: 128s

Common Session ID: 0A302BFD0000001B02BE1E9C

Acct Session ID: 0x00000010

Handle: 0x58000003

Current Policy: POLICY_Fal/7

Local Policies:

Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Security Policy: Should Secure

Security Status: Link Unsecure

Server Policies:

SGT Value: 16

Method status list:

Method State

mab Authc Success

KJK_IE4000_10#

2.管理員更改組

導覽至Search。貼上終端的Mac地址，按一下該地址並將其新增到組2。

附註：在CCV上，您不能一次將組從1更改為2。因此，您應該首先從組中刪除端點，然後分配組2。

The screenshot shows the Cisco Cyber Vision (CCV) interface. On the left is a dark navigation sidebar with options: Explore, Reports, Events, Monitor, Search, and Admin. The main content area displays a search result for a component named 'Cisco a0:3a:59'. The component details include IP: -, MAC: 00:f2:8b:a0:3a:59, and a '2 results' indicator. A dropdown menu is open over the component, showing options: 'Create a new group', 'Group1', and 'Group2'. The 'Group2' option is selected. Below the component details, there are sections for 'Properties' and 'Tags'. The 'Properties' section shows 'vendor-name: Cisco Systems, Inc' and 'name: Cisco a0:3a:59'. The 'Tags' section shows 'No tags found'.

3-6.終端組更改對CCV的影響

步驟4、5和6將反映在此影像中。由於分析，終端將身份組更改為ekorneyc_ASSET_Group2（如步驟4所示），導致ISE將CoA傳送到交換機（步驟5），最後終端重新身份驗證（步驟6）。

| Time | Status | Details | Repeat ... | Identity | Endpoint ID | Endpoint Profile | Authentication Pol... | Authorization Policy | Authorization Profiles | IP Address | Network Device | Device Port | Identity Group |
|------------------------------|------------|---------|------------|-----------------|-----------------|-----------------------|-----------------------|-------------------------------|------------------------------|--------------|----------------|-----------------|-----------------------|
| Jun 25, 2020 10:43:00:411 AM | Authorized | | 0 | 00F28B-A0-3A-59 | 00F28B-A0-3A-59 | ekorneyc_ASSET_Group2 | Default >> MAB | Default >> CCV Group 2 Policy | IOT_Group2_AssetPermitAccess | 172.16.0.100 | | FastEthernet1/7 | ekorneyc_ASSET_Group2 |
| Jun 25, 2020 10:42:59:503 AM | Authorized | | 0 | 00F28B-A0-3A-59 | 00F28B-A0-3A-59 | ekorneyc_ASSET_Group2 | Default >> MAB | Default >> CCV Group 2 Policy | IOT_Group2_AssetPermitAccess | 172.16.0.100 | E-4000 | FastEthernet1/7 | ekorneyc_ASSET_Group2 |
| Jun 25, 2020 10:42:59:482 AM | Authorized | | 0 | 00F28B-A0-3A-59 | 00F28B-A0-3A-59 | ekorneyc_ASSET_Group1 | Default >> MAB | Default >> CCV Group 1 Policy | IOT_Group1_AssetPermitAccess | 172.16.0.100 | E-4000 | FastEthernet1/7 | ekorneyc_ASSET_Group1 |
| Jun 25, 2020 10:37:31:567 AM | Authorized | | 0 | 00F28B-A0-3A-59 | 00F28B-A0-3A-59 | ekorneyc_ASSET_Group1 | Default >> MAB | Default >> CCV Group 1 Policy | IOT_Group1_AssetPermitAccess | 172.16.0.100 | E-4000 | FastEthernet1/7 | ekorneyc_ASSET_Group1 |

Switch show authentication sessions interface fa1/7 detail 確認已分配新的SGT。

```
KJK_IE4000_10#show authentication sessions interface fa1/7 detail
Interface: FastEthernet1/7
MAC Address: 00f2.8ba0.3a59
IPv6 Address: Unknown
IPv4 Address: 172.16.0.100
User-Name: 00-F2-8B-A0-3A-59
Status: Authorized
Domain: DATA
Oper host mode: single-host
Oper control dir: both
Session timeout: N/A
Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 664s
Common Session ID: 0A302BFD0000001B02BE1E9C
Acct Session ID: 0x00000010
Handle: 0x58000003
Current Policy: POLICY_Fa1/7

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
Security Policy: Should Secure
Security Status: Link Unsecure

Server Policies:
SGT Value: 17

Method status list:
Method State
```

mab Authc Success

KJK_IE4000_10#

附錄

交換機TrustSec相關配置

附註：Cts credentials不是運行配置的一部分，應在特權執行模式下使用cts credentials id <id> password <password>命令進行配置。

aaa new-model

```
!  
aaa group server radius ISE  
server name ISE-1  
!  
aaa authentication dot1x default group ISE  
aaa authorization network default group ISE  
aaa authorization network ISE group ISE  
aaa accounting dot1x default start-stop group ISE  
!  
dot1x system-auth-control  
!  
aaa server radius dynamic-author  
client 10.48.17.86  
server-key cisco  
!  
aaa session-id common  
!  
cts authorization list ISE  
cts role-based enforcement  
!  
interface FastEthernet1/7  
description --- ekorneyc TEST machine ---  
switchport access vlan 10  
switchport mode access  
authentication port-control auto  
mab  
!  
radius server ISE-1  
address ipv4 10.48.17.86 auth-port 1645 acct-port 1646  
pac key cisco  
!  
end
```

KJK_IE4000_10#