配置ISE 2.7 pxGrid CCV 3.1.0集成

目录

简介

本文档介绍如何配置和排除身份服务引擎(ISE)2.7与Cisco Cyber Vision(CCV)3.1.0在Platform Exchange Grid v2(pxGrid)上的集成故障。CCV以pxGrid v2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：

- ISE
- 思科网络愿景

使用的组件

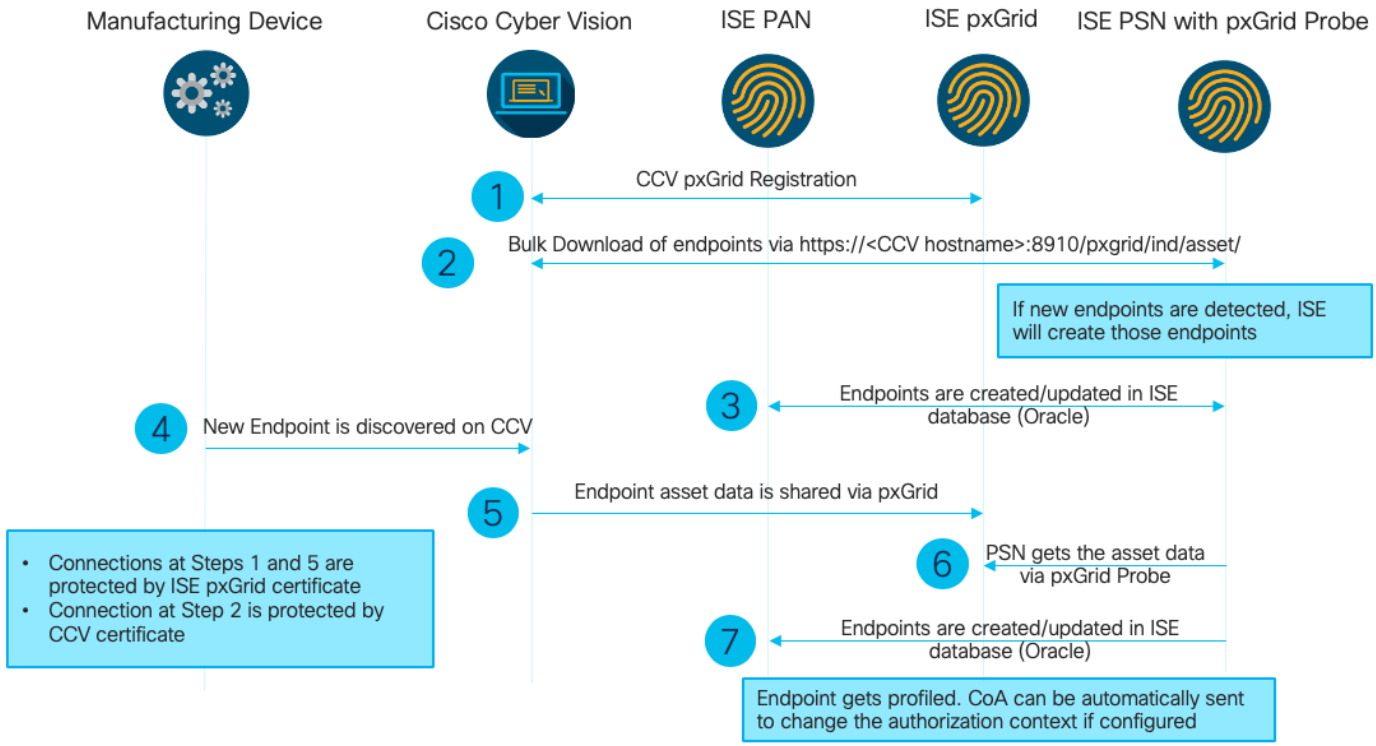
本文档中的信息基于下列软件和硬件版本：

- 思科ISE版本2.7补丁1
- 思科网络愿景版本3.1.0
- 工业以太网交换机IE-4000-4TC4G-E，带软件15.2(6)E

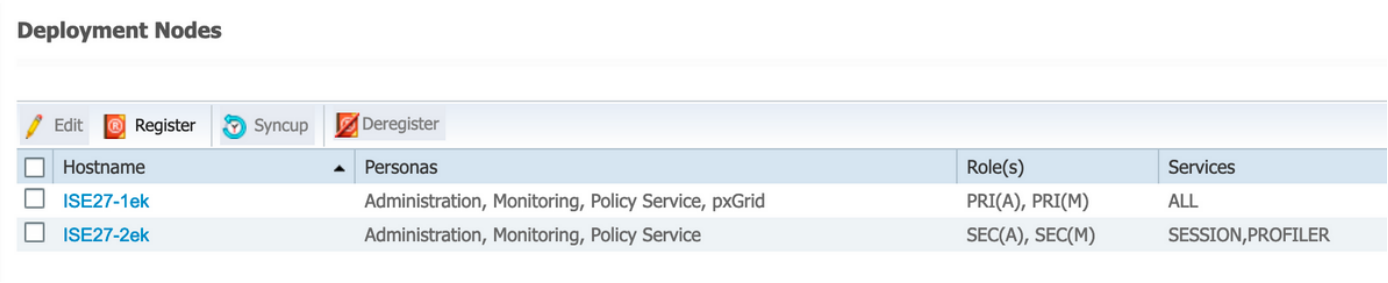
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

高级流程图



此ISE部署用于设置。



ISE 2.7-1ek是主管理节点(PAN)节点和pxGrid节点。

ISE 2.7-2ek是启用pxGrid探测的策略服务节点(PSN)。

以下是与前面提到的图表对应的步骤。

1. CCV通过pxGrid版本2注册到assetISE上的主题。CCV的相应日志：

注意：要查看CCV上的pxGrid日志，请发出以**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.启用pxGrid探测功能的ISE PSN可批量下载现有pxGrid资产(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.在启用pxGrid探测功能的情况下，终端会添加到PSN，PSN会向PAN发送持久事件以保存这些终

端(profiler.log)。 在ISE上创建的终端可在情景可视性下的终端详细信息中查看。

```
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
proccessedEndPoint[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.将终端放入组后，CCV通过端口8910发送STOMP消息，以使用自定义属性中的组数据更新终端。来自CCV的相应日志：

```
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":"","assetHwRev
ision":"","assetProtocol":"",
"assetCustomAttributes":[{"key":"assetGroup","value":"Group1"},{"key":"assetCCVGrp","value":"Gro
up1"}],
"assetConnectedLinks":[]}} [caller=endpoint.go:118]
```

5. PxGrid节点接收STOMP更新并将此消息转发给所有用户，它包括启用pxGrid探测功能的PSN。**pxgrid节点上的**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.启用pxGrid探测功能的PSN是资产主题的订用者，它从pxGrid节点接收消息并更新终端(**profiler.log**)。 可在情景可视性下的终端详细信息中查看ISE上更新的终端。

```
2020-06-24 14:40:13,767 DEBUG [Grizzly(2)][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::::-
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":"","assetHwRev
ision":"",
"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.INDSubscriber -::::-
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:ce01ade2-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.启用了pxGrid探测功能的PSN将重新分析终端，作为匹配的新策略(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][]
```

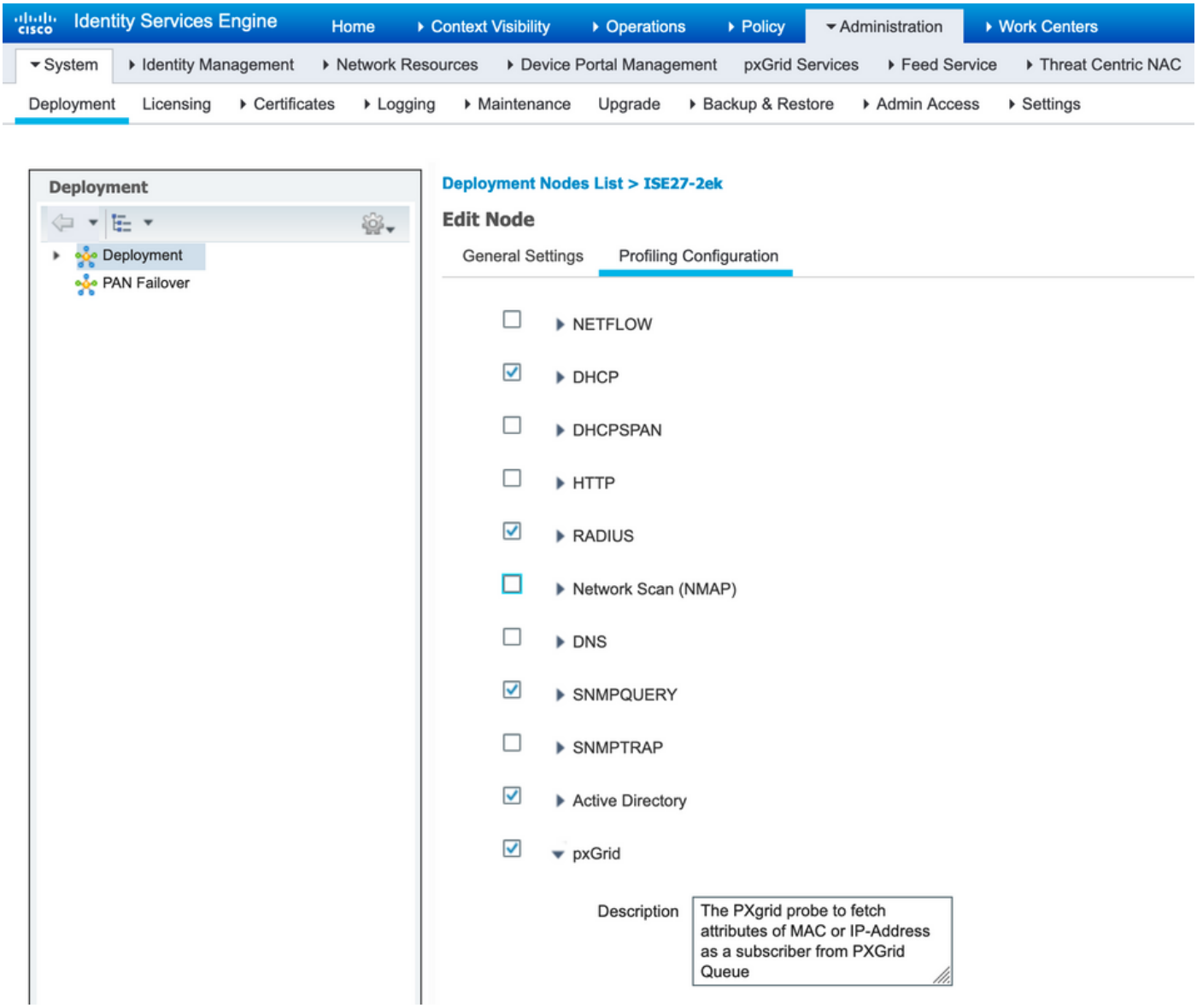
```
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Endpoint 00:F2:8B:A0:3A:59
IdentityGroup Changed.
2020-06-24 14:40:13,778 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- Setting identity group ID on
endpoint
00:F2:8B:A0:3A:59 - 91b0fd10-a181-11ea-a1a3-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
```

配置

注意：即使您只想了解资产组和情景可视性，也需要步骤1 - 4。

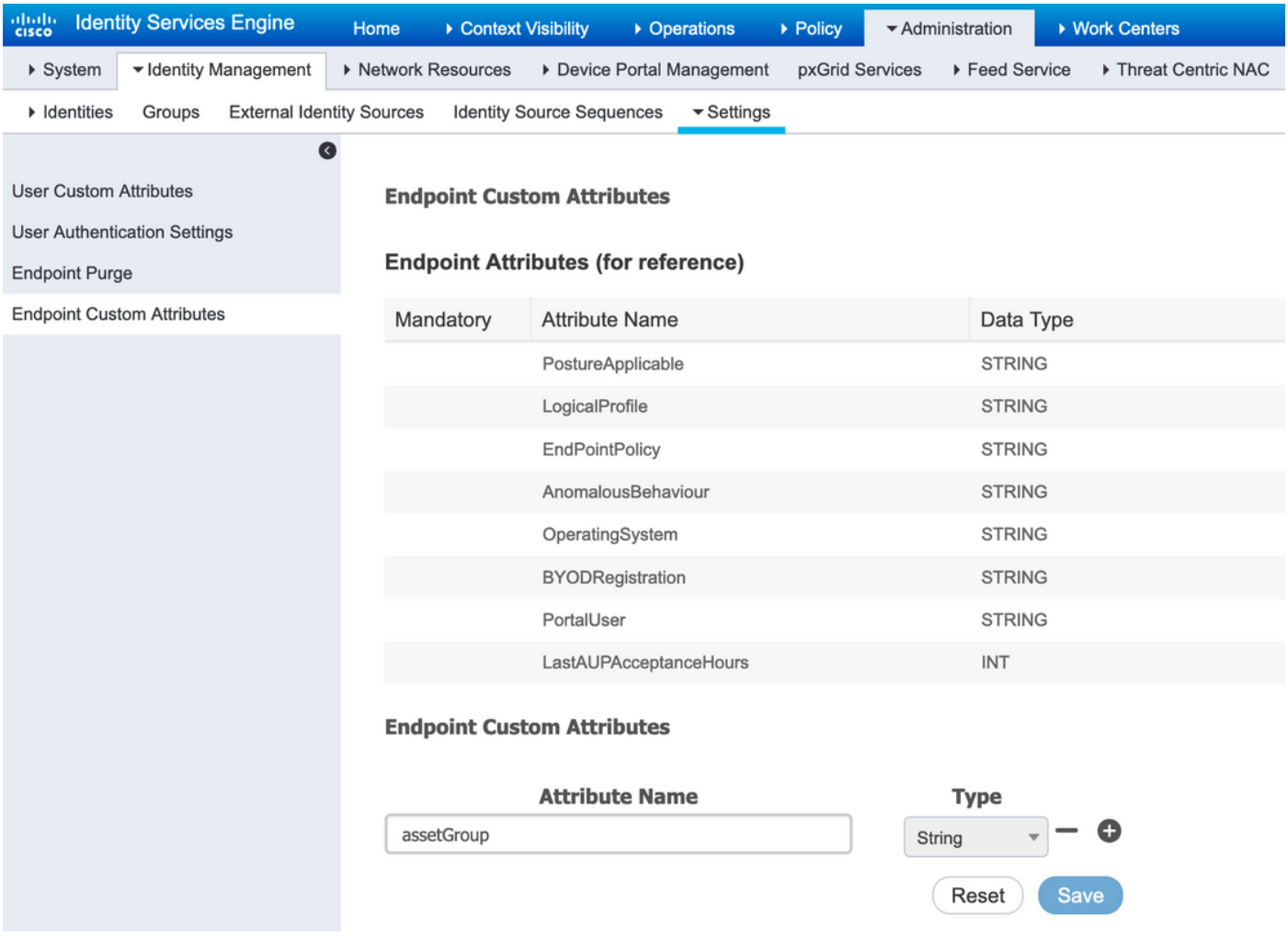
1.在其中一个PSN上启用pxGrid探测功能

导航至**管理>系统>部署**，选择具有PSN角色的ISE节点。切换到分析**配置选**项卡。确保已**启**用pxGrid探测。



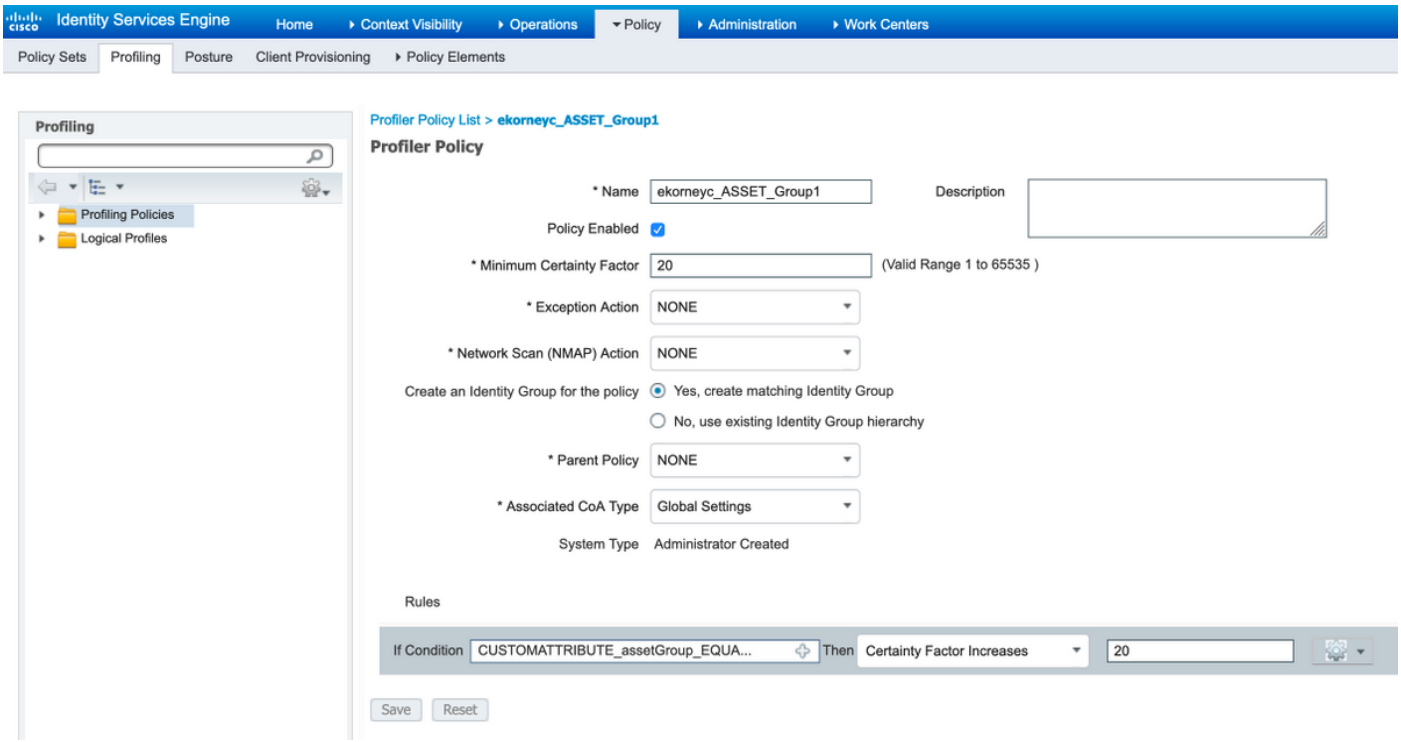
2.在ISE上配置终端自定义属性

导航至**管理>身份管理>设置>终端自定义属性**。根据此映像配置自定义属性(assetGroup)。CCV 3.1.0仅支持自定义**资产组**属性。



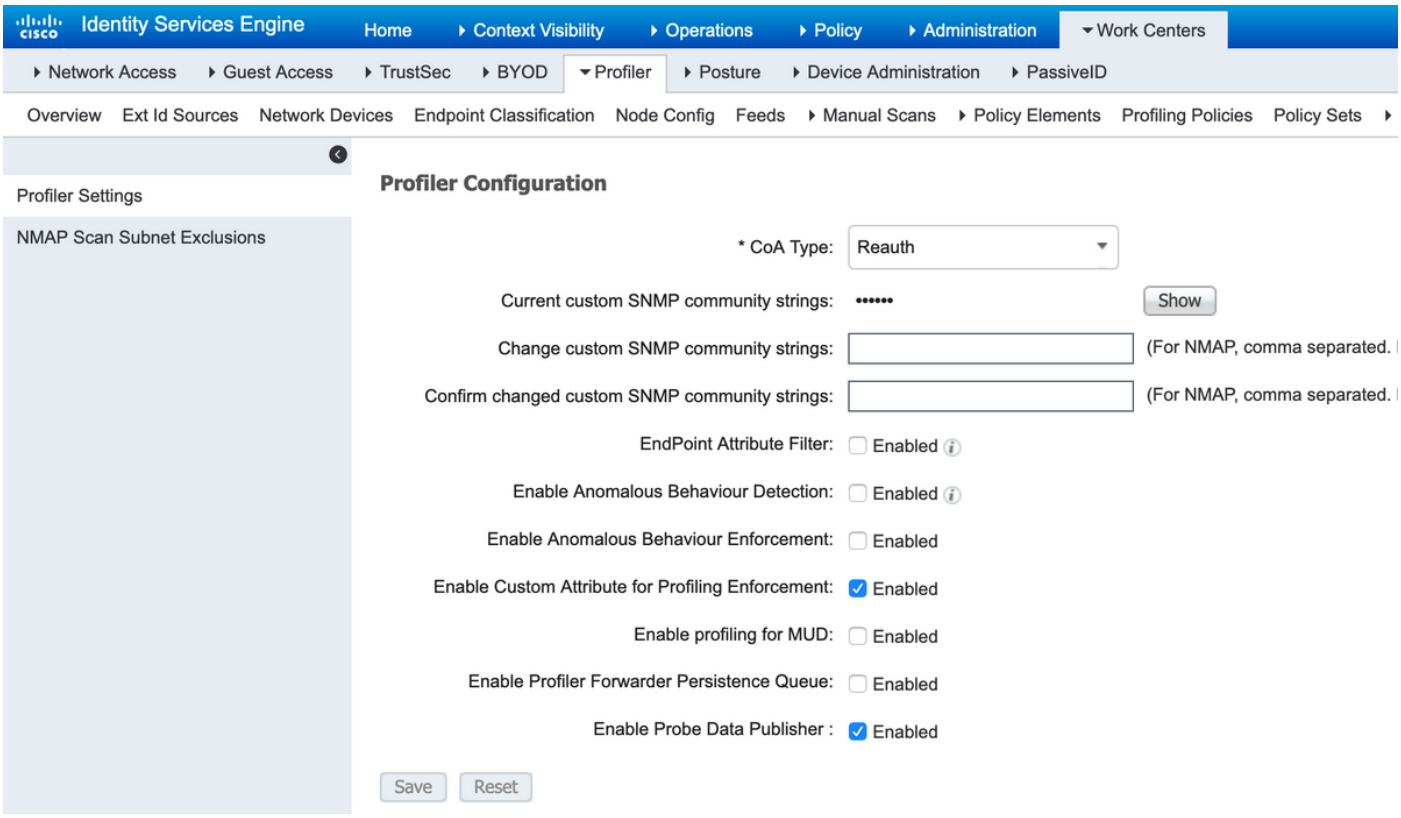
3.使用自定义属性配置分析器策略

导航至工**作中心>分析器>分析策略**。单击“Add”。配置与此映像类似的分析器策略。此策略中使用的条件表达式**是CUSTOMATTRIBUTE:assetGroup EQUALS Group1。**



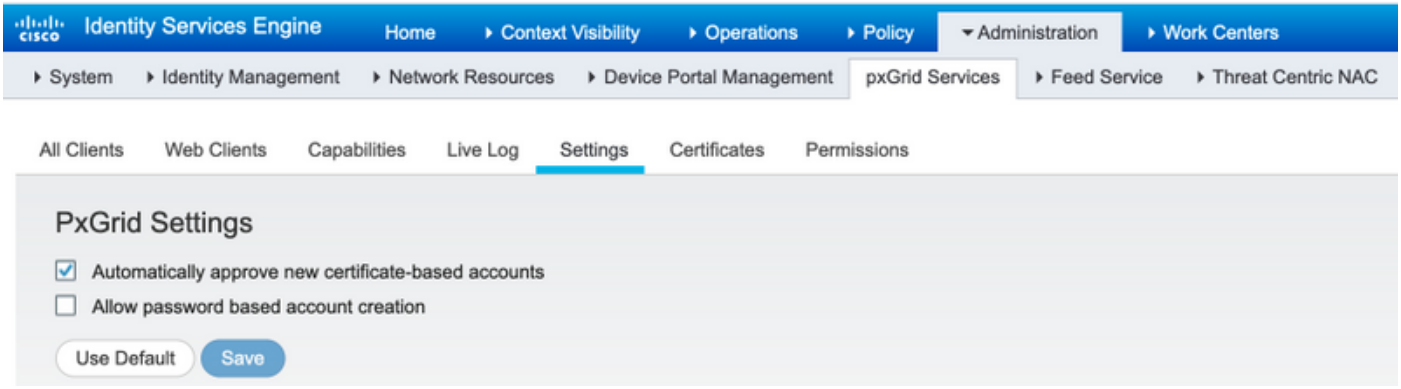
4.为分析实施启用自定义属性

导航至工**作中心>分析器>分析策略**。单击“**Add**”。配置与此映像类似的分析器策略。确保**已启用为分析实施启**用自定义属性。



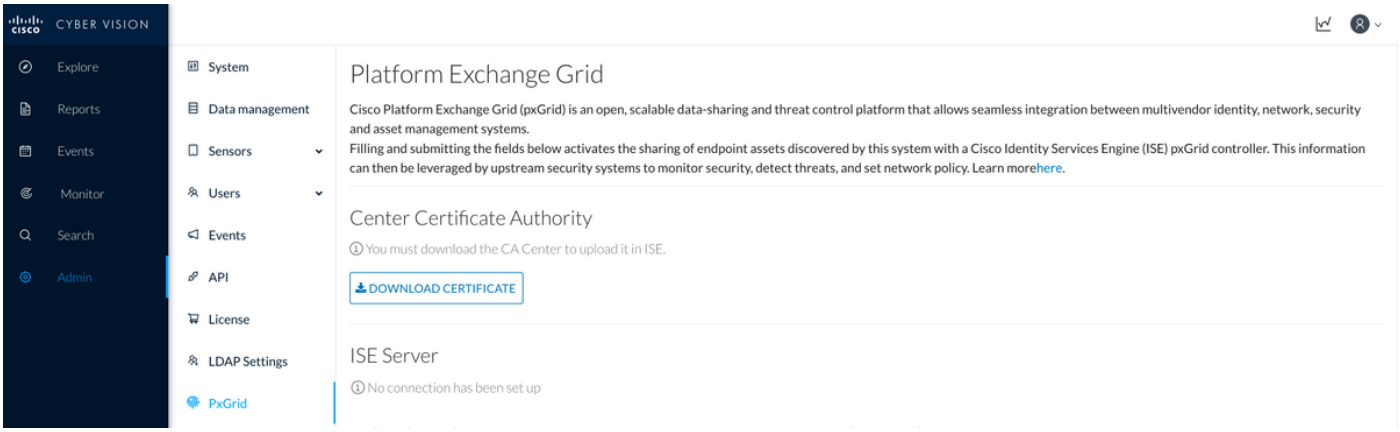
5.配置pxGrid客户端的自动审批

导航至“**管理**”>“**pxGrid服务**”>“**设置**”。选择**自动批准新的基于证书的帐户**，然后单**击保存**。此步骤可确保在集成完成后，您无需批准CCV。



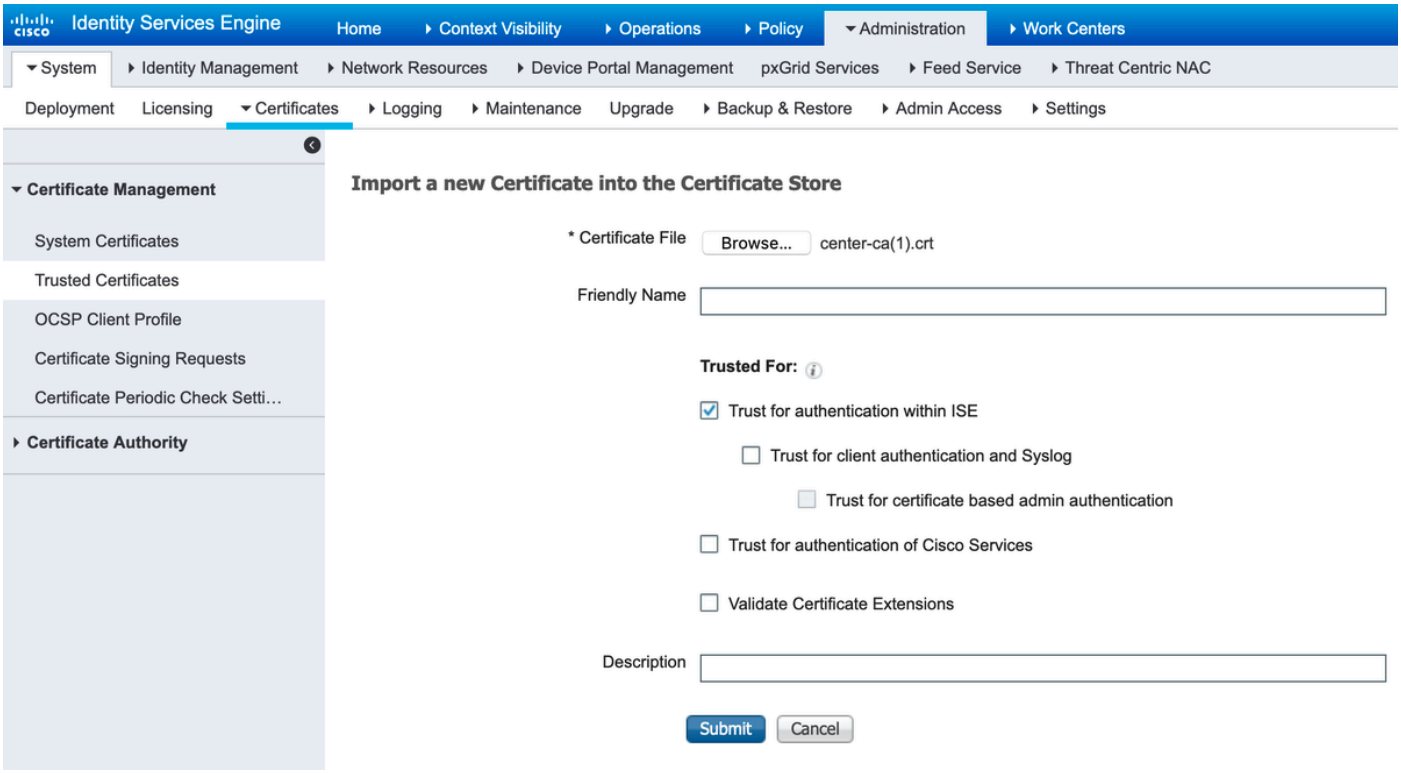
6.导出CCV证书

导航至**Admin > pxGrid**。单击“**DOWNLOAD CERTIFICATE（下载证书）**”。此证书在pxGrid注册期间使用，因此ISE应信任它。



7.将CCV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5中选择CCV证书。单击“提**交”**。

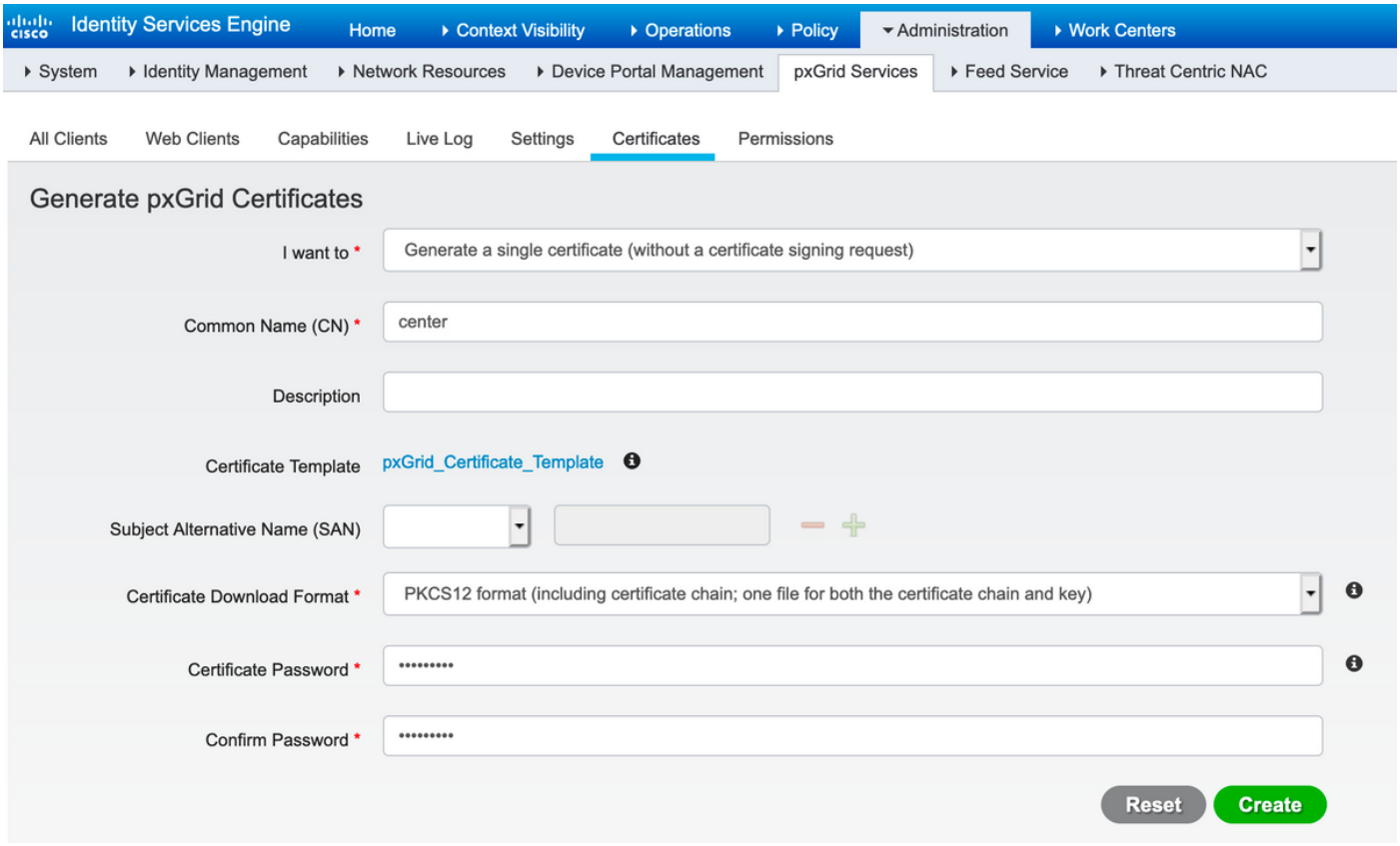


8.生成CCV证书

在pxGrid集成和更新期间，CCV需要客户端证书。它应由ISE内部CA使用PxGrid_Certificate_**Template颁发**。

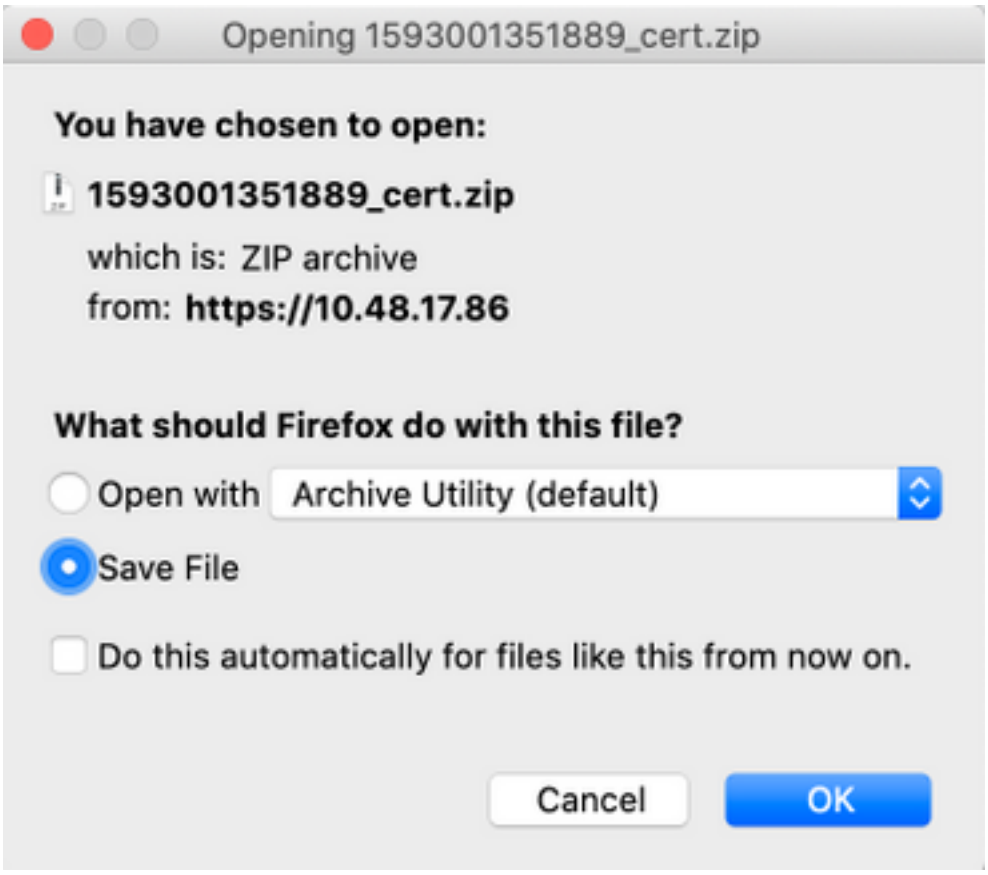
导航至**Administration > pxGrid Services > Certificates**。根据此图像填充字段。公用名(CN)字段是必填项，因为ISE CA的目标是颁发身份证书。您应输入CCV的主机名，CN字段值至关重要。要检查CCV的主机名，请发出**hostname**命令。选择PKCS12作**为Certificate Download Format。**

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



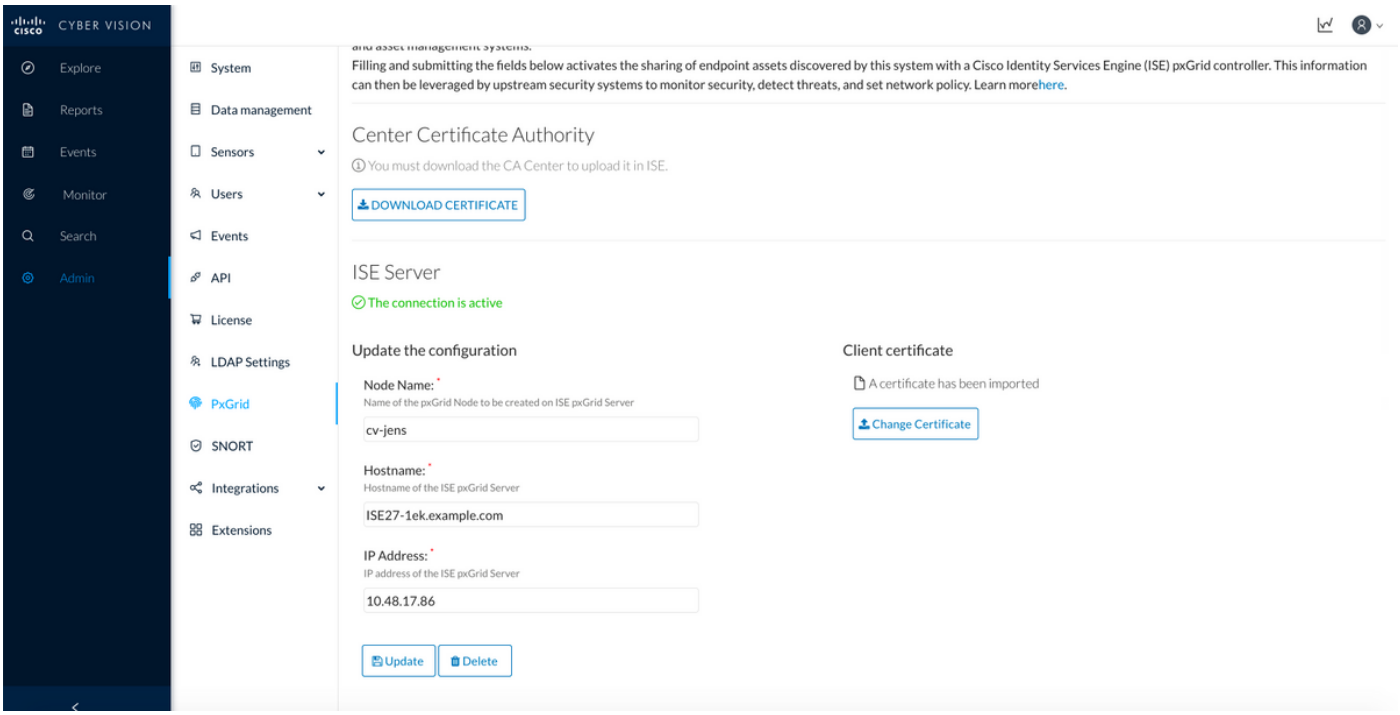
9.下载PKCS12格式的证书链

当您以PKCS12格式安装证书时，CCV上会安装CCV身份证书ISE内部CA链，以确保当从ISE发起pxGrid通信时，CCV信任ISE，例如pxGrid keepalive消息。



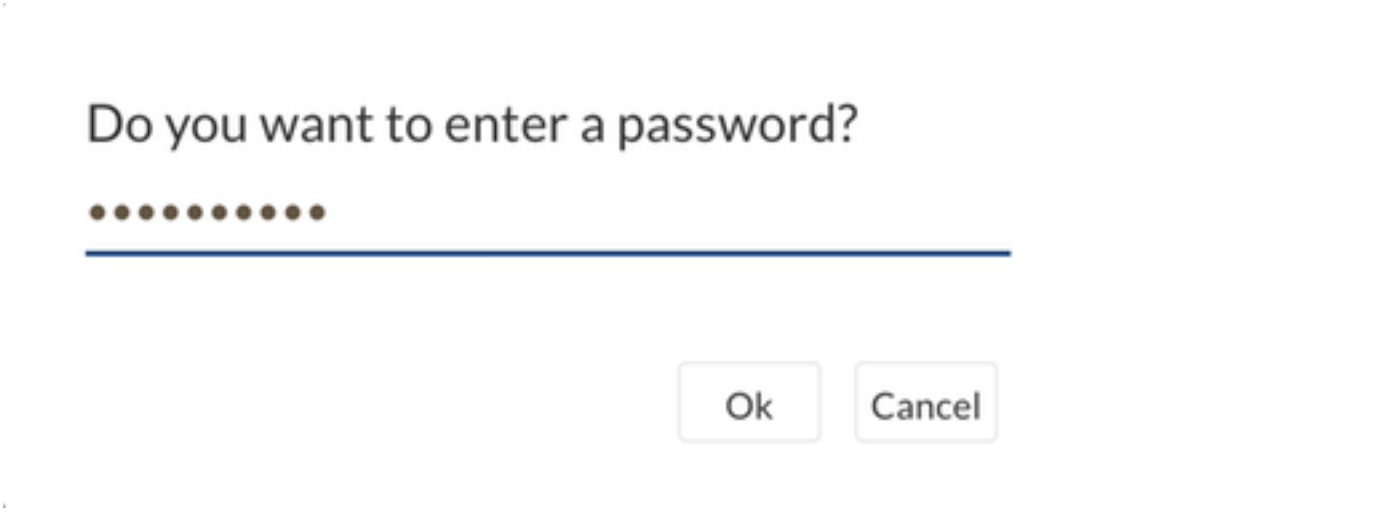
10.在CCV上配置ISE集成详细信息

导航至**Admin > pxGrid**。配置节点名称，此名称将在ISE上显示为Administration > pxGrid Services > Web Clients**中的Client Name。配置ISE pxGrid节点的主机名**和IP地址。确保CCV可以解析ISE FQDN。



11.在CCV上传证书链并启动集成

导航至**Admin > pxGrid**。单击“**Change Certificate**”。从步骤8-9中选择由ISE CA颁发的证书。输入步骤8中的密码，然后单击**OK**。



单击**Update**，触发实际CCV - ISE集成。

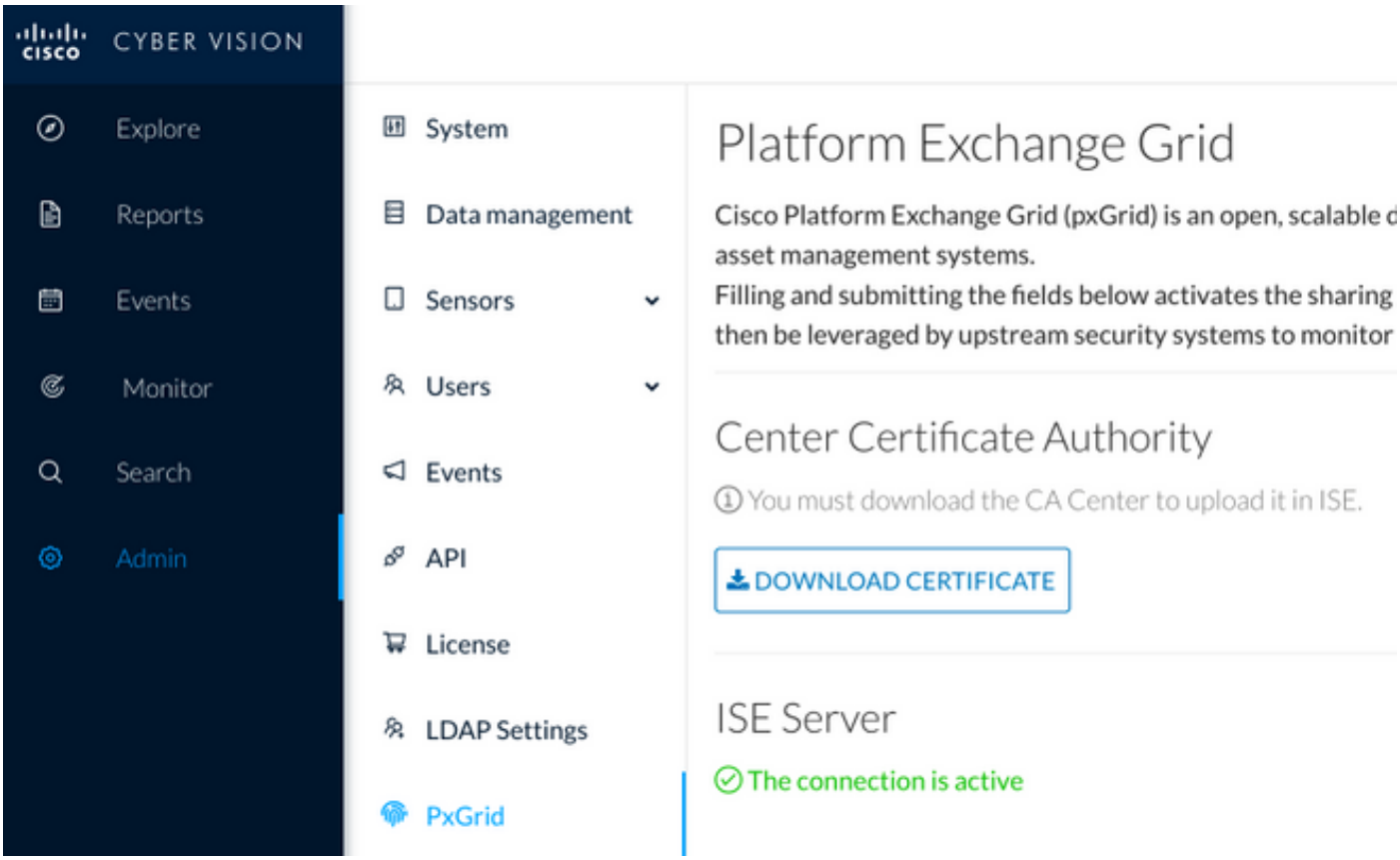
验证

使用本部分可确认配置能否正常运行。

CCV集成验证

完成集成后，您可以导航到Admin > pxGrid**来确认其成功**。您应该在ISE**服务器下看到连**接处于活动

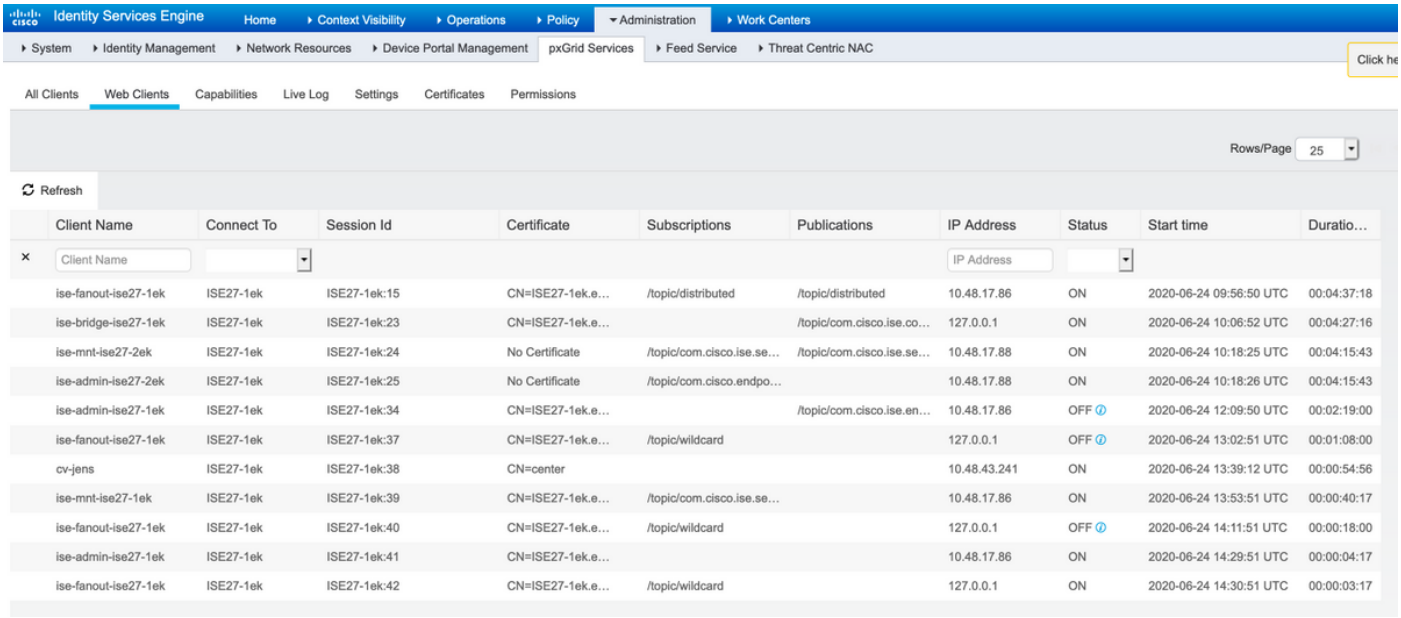
状态消息。



ISE集成验证

导航至**Administration > pxGrid Services > Web Clients**。确认CCV客户端(cv-jens)的状态为**ON**。

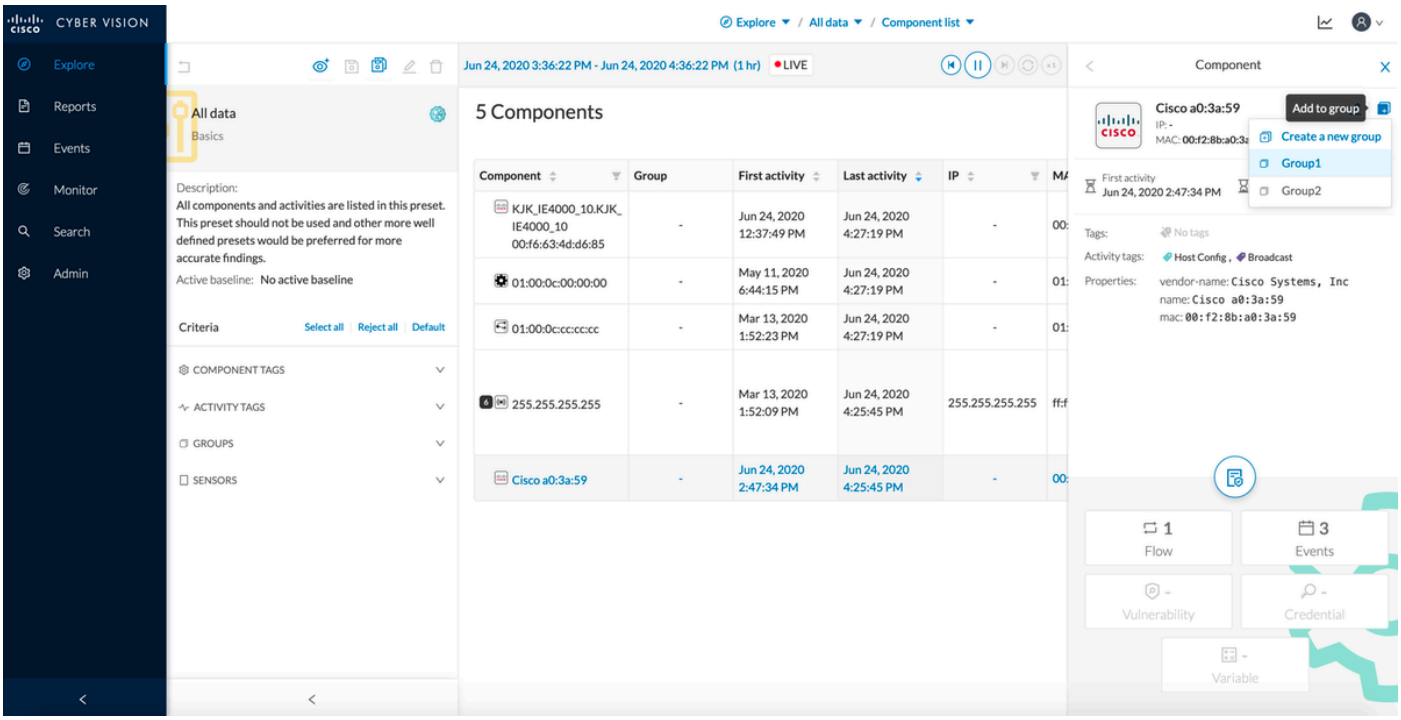
> **注意**：在“所有客户端”菜单中，CCV pxGrid客户端的状态应显示为**脱机**，因为它只显示pxGrid v1状态。



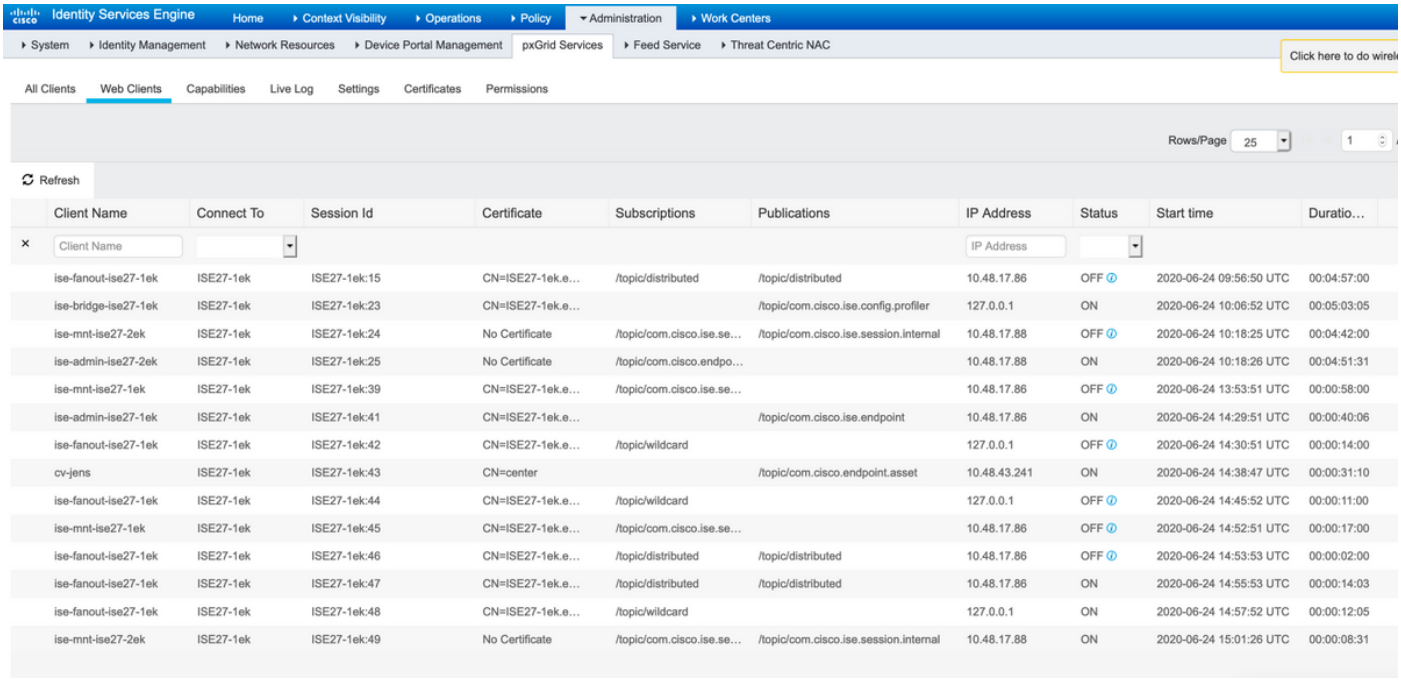
> **注意**：由于CSCvt78208，您不会立即看到CCV有**/topic/com.cisco.ise.endpoint.asset，它仅在首次发布时显示。**

验证CCV组更改

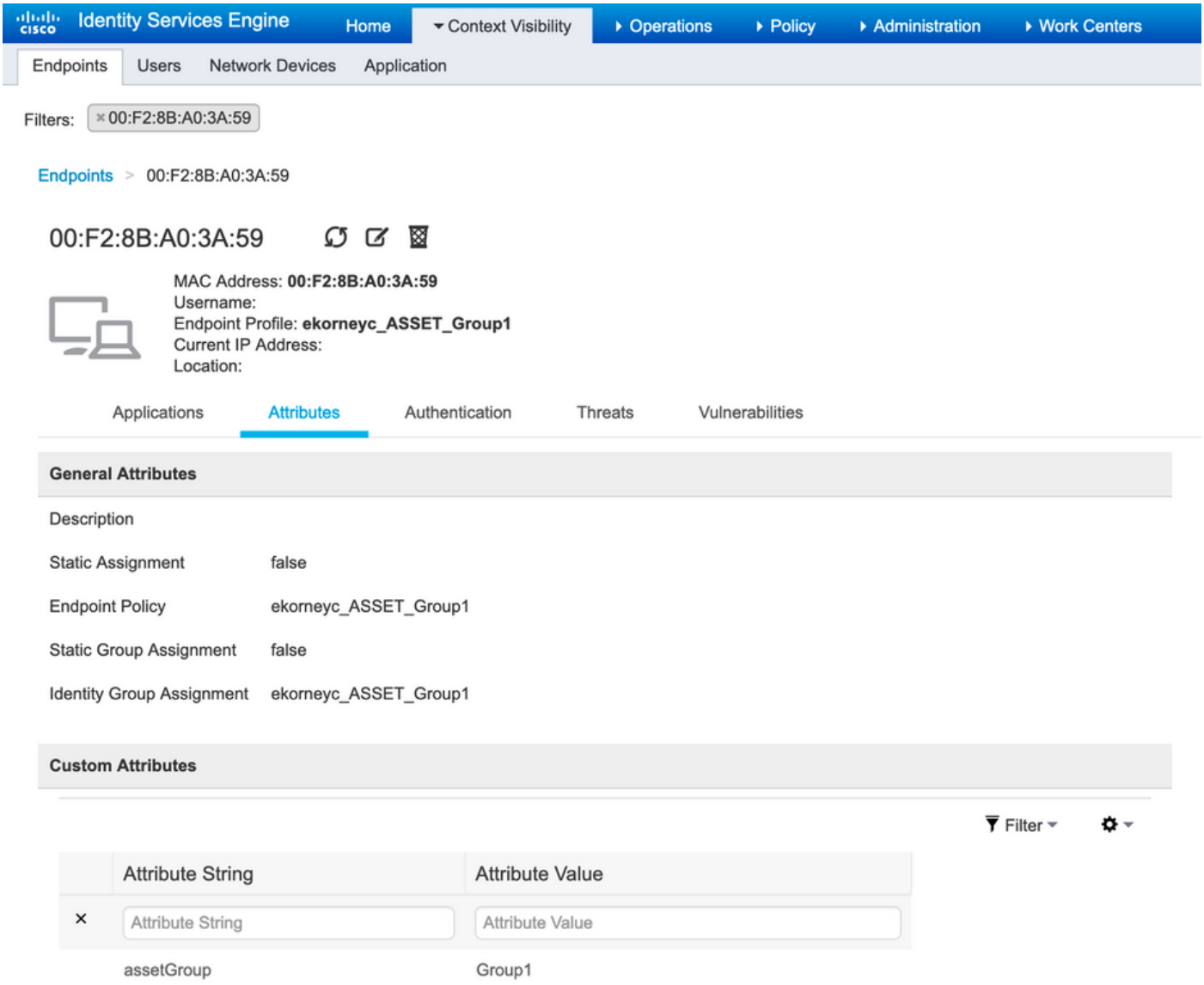
导航至“浏**览”>“所有数据”>“组件列表**”。单击其中一个“组件”(Components),**然后将**其添加到“组”(Group)。



验证/topic/com.cisco.**ise.endpoint.asset现**在是否列为针对CCV的发布。



确认通过CCV分配的组1反映在ISE上，并通过导航到Context Visibility > Endpoints来**分析策略生效**。选择上一步中更新的终端。切换到属性选项卡。自定义属性部分应反映新配置的组。



“其他属性”部分列出从CCV接收的所有其他资产属性。

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

故障排除

本部分提供的信息可用于对配置进行故障排除。

在ISE上启用调试

要在ISE上启用调试，请导航至**Administration > System > Logging > Debug Log Configuration**。将日志级别设置为：

角色	组件名称	日志级别	要检查的文件
PAN（可选）	分析器	调试	profiler.log
启用pxGrid探测功能的PSN	分析器	调试	profiler.log
PxGrid	pxgrid	跟踪	pxgrid-server.log

在CCV上启用调试

要在CCV上启用调试，请执行以下操作：

- 使用touch /data/etc/sbs/pxgrid-agent.conf命**令创**建文**件/data/etc/sbs/pxgrid-agent.conf**。

- 使用vi编辑器和vi /data/etc/sbs/pxgrid-agent.conf命令将此内容粘贴到pxgrid-agent.conf文件中

```
# /data/etc/sbs/pxgrid-agent.conf
base:
loglevel: debug
```

- 通过运行systemctl restart pxgrid-agent命令重新启动pxgrid-agent。
- 使用journalctl -u pxgrid-agent命令查看日志

批量下载失败

CCV在集成期间将批量下载URL发布到ISE。启用pxGrid探测功能的ISE PSN使用此URL执行批量下载。请确保：

- URL中的主机名可从ISE角度正确解析
- 允许从端口8910上的PSN到CCV的通信

启用pxGrid探测功能的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}]]
```

由于CSCvt75422，批量下载可能失败，您应在ISE上的Profiler.log中看到此错误以确认。缺陷在CCV 3.1.0中已修复。

```
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.jav
a:161)
at
com.cisco.profiler.infrastructure.probemgr.INDSubscriber$BulkRequestWorkerThread.run(INDSubscrib
er.java:532)
at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149)
at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624)
at java.lang.Thread.run(Thread.java:748)
```

并非所有终端都在ISE上创建

CCV上的某些终端可能附加了太多属性，因此ISE数据库将无法处理该属性。如果在ISE上的profiler.log中看到这些错误，可以确认它。

```
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)
```

资产组在ISE上不可用

如果AssetGroup在ISE上不可用，则很可能分析策略未使用自定义属性进行配置（请参阅文档配置部分的步骤2-4）。 即使对于情景可视性，仅要显示组属性、分析策略和步骤2-4中的其他设置也是必需的。

终端组更新未反映在ISE上

由于CSCvu80175，在集成后CCV立即重新启动之前，CCV不会将终端更新发布到ISE。在完成集成后，您可以重新启动CCV作为解决方法。

从CCV删除组不是从ISE删除

此问题是由于CCV CSCvu47880上的已知缺陷而发生的。从CCV删除组期间发送的pxGrid更新格式与预期格式不同，因此不会删除组。

CCV从Web客户端断开

出现此问题是由于ISE CSCvu47880上的已知缺陷，在该缺陷中，客户端转换到关闭状态，然后从Web客户端完全删除。此问题在ISE的2.6补丁7和2.7补丁2中解决。

如果在ISE上的pxgrid-server.log中看到**以下错误，您可以**确认它：

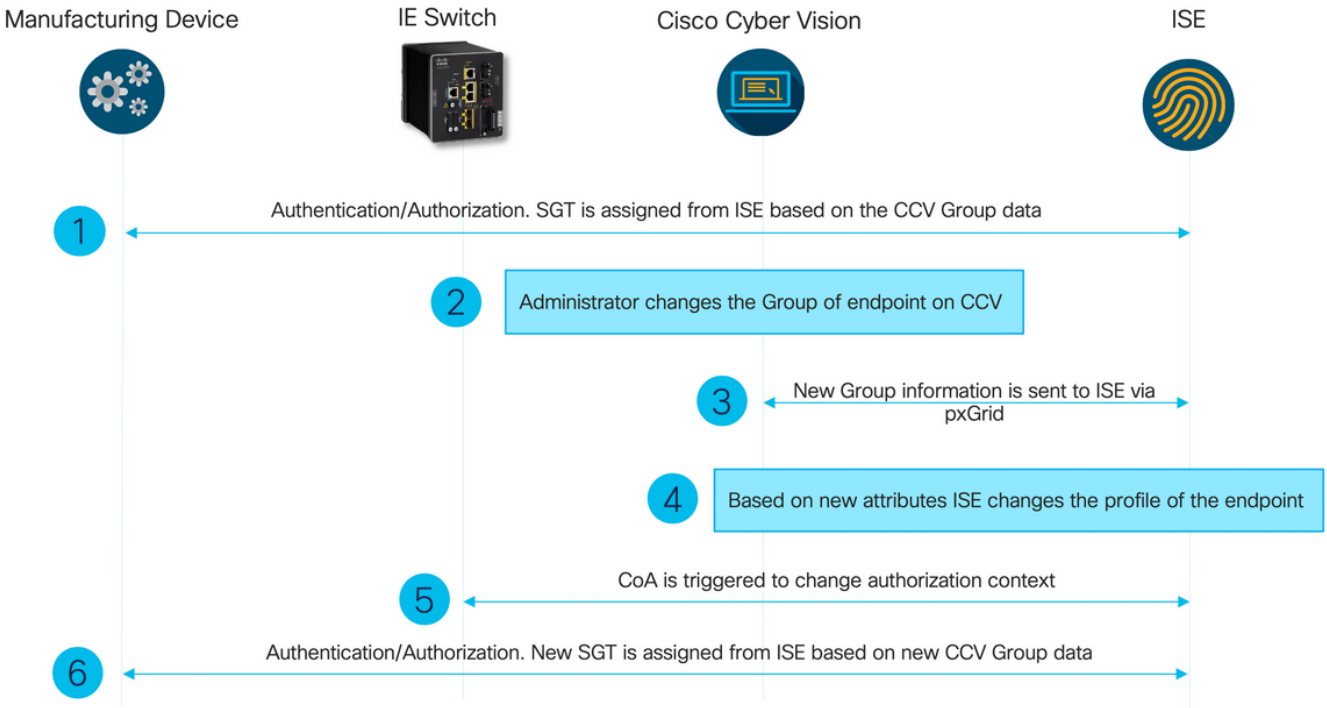
```
2020-06-26 09:42:28,772 DEBUG [Pxgrid-SessionManager-LookupAccountsTask][]
cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -::::-
onClose: session=[14f,CLOSED], sessionInfo=WSSessionInfo [id=336, nodeName=cv-jens,
addr=10.48.43.241, sessionID=14f, status=OFF,
creationTime=2020-06-26 08:19:28.726, 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与CCV TrustSec集成使用案例

此配置显示当TrustSec部署时，ISE与CCV的集成如何使安全端到端受益。这只是集成完成后如何使用集成的示例之一。

> **注意**：TrustSec交换机配置说明不在本文的范围内，但可以在附录中找到。

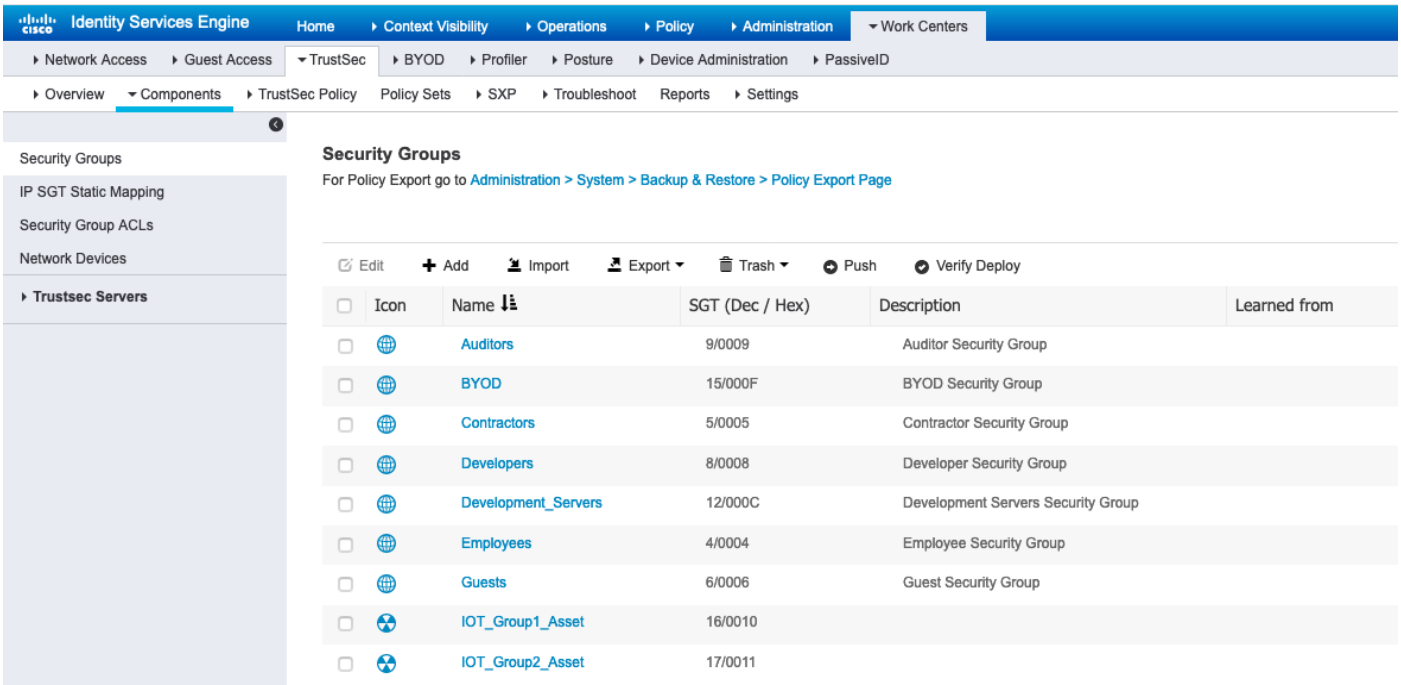
拓扑和流



配置

1.在ISE上配置可扩展组标记

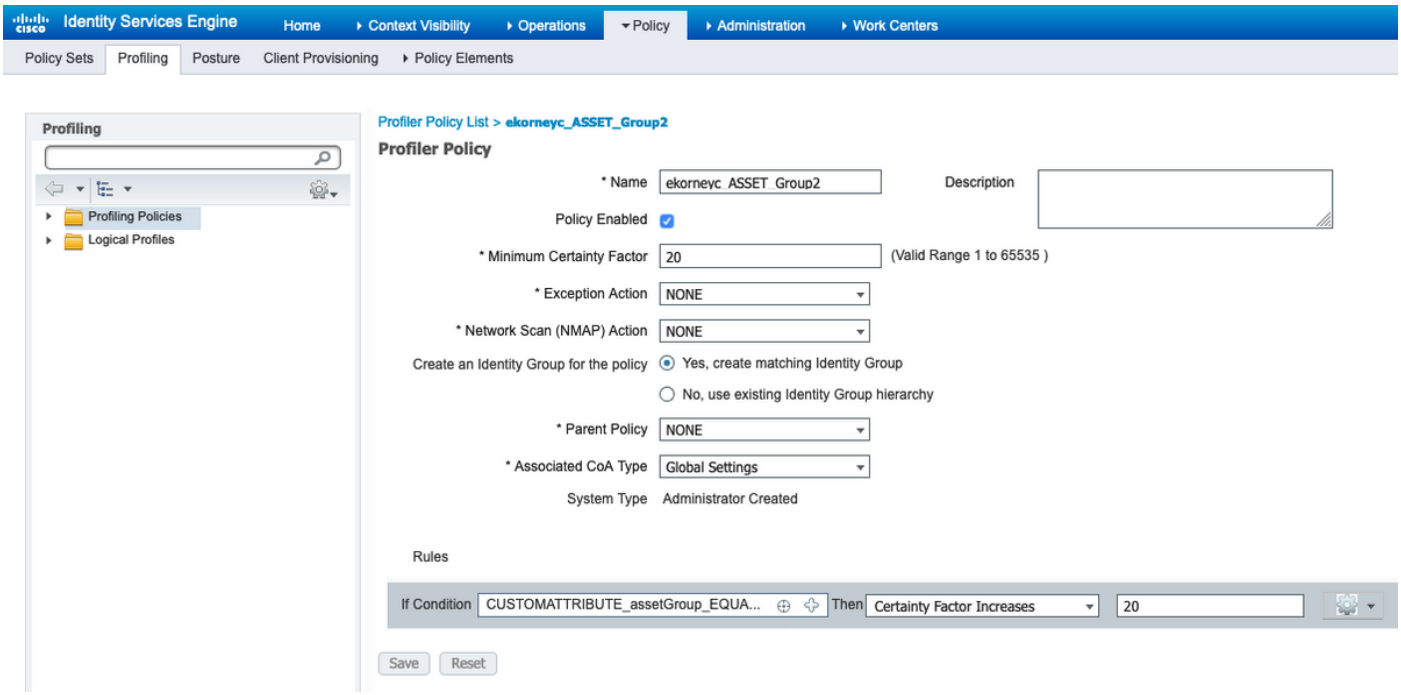
为了实现上述使用案例，手动配置TrustSec标记的IOT_Group1_Asset和IOT_Group2_Asset，以区分组1 CCV资产和组2。导航至工**作中心> TrustSec >组件>安全组**。单击“**添加”。**如图所示命名SGT。



2.使用组2的自定义属性配置分析器策略

注意：第1组的分析配置在文档第一部分的步骤3中完成。

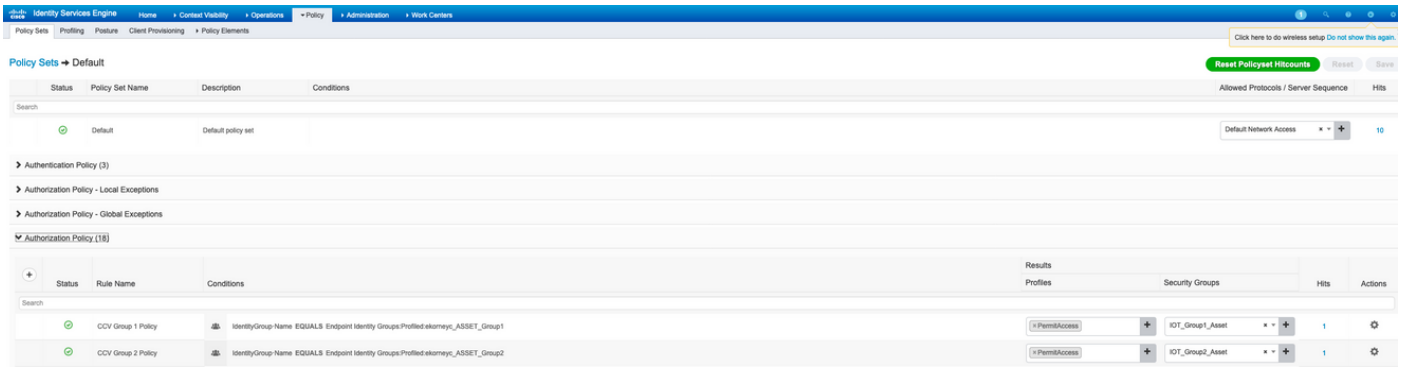
导航至工**作中心>分析器>分析策略**。单击“Add”。配置与此映像类似的分析器策略。此策略中使用的条件表达式**是CUSTOMATTRIBUTE:assetGroup EQUALS Group2。**



3.配置授权策略以根据ISE上的终端身份组分配SGT

导航至**策略>策略集**。选择**策略集**并根据**此映**像配置授权策略。请注意，因此，将分配步骤1中配置的SGT。

规则名称	条件	配置文件	安全组
CCV组1策略	IdentityGroup·Name EQUALS终端身份组：Profiled:ekorneyc_ASSET_Group1	允许访问	IOT_Group1_Asset
CCV组2策略	IdentityGroup·Name EQUALS终端身份组：Profiled:ekorneyc_ASSET_Group2	允许访问	IOT_Group2_Asset



验证

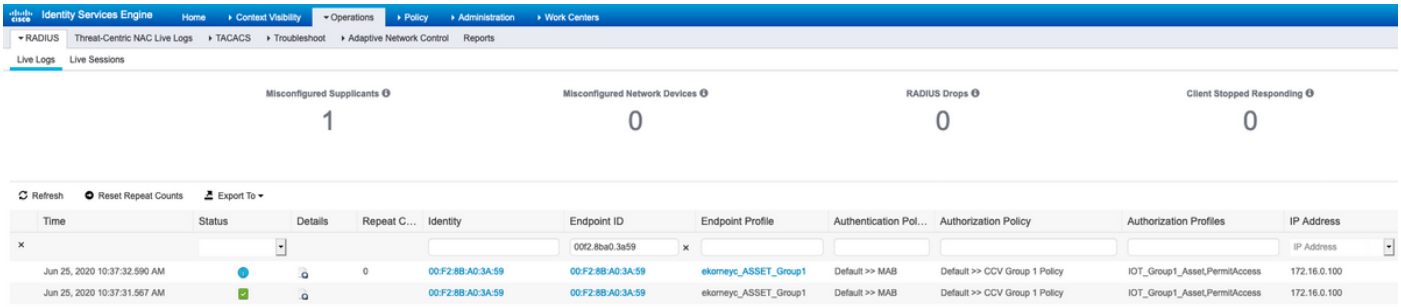
使用本部分可确认配置能否正常运行。

1.终端根据CCV组1进行身份验证

在交换机上，您可以看到环境数据包括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#
```

终端进行身份验证，因此，CCV组1策略匹配，SGT IOT_Group1_Asset被分配。



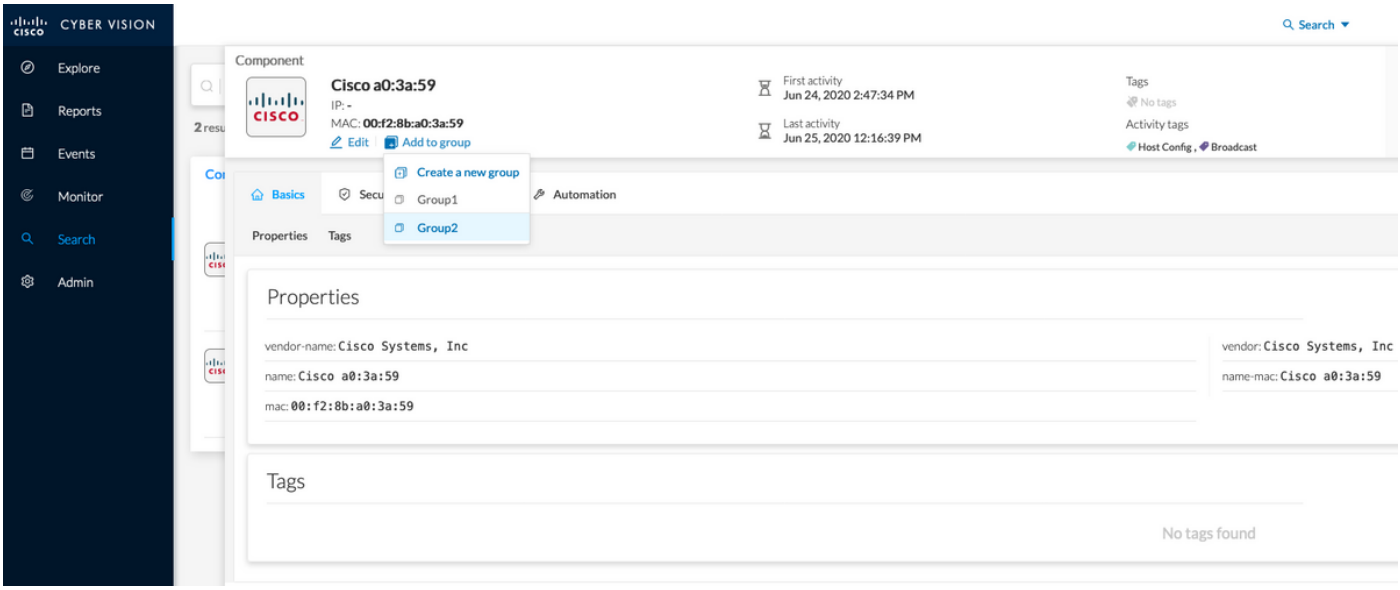
交换机show authentication sessions interface fa1/7 detail确认Access-Accept数据已成功应用。

```
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: 128s
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: 16

Method status list:
Method State

mab Authc Success

KJK_IE4000_10#
```

2.管理员更改组

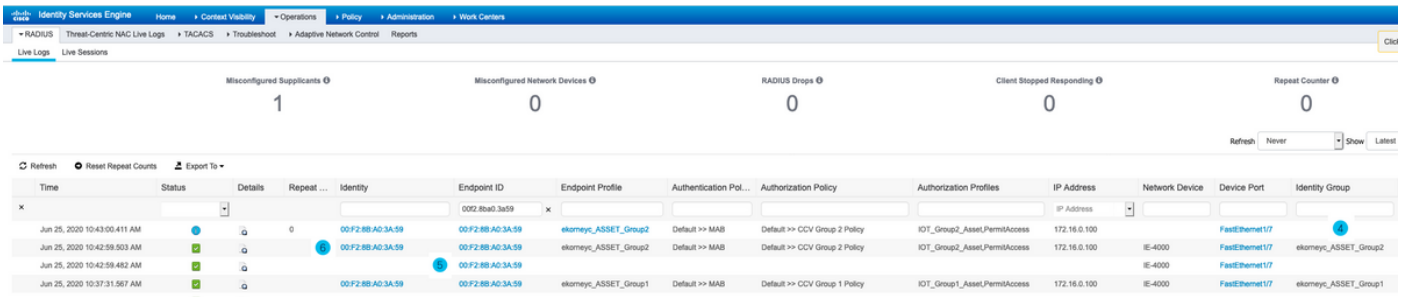
导航至**搜索**。粘贴终端的Mac地址，单击该地址并**将其**添加到组2。

> **注意**：在CCV上，您不能一次将组从1更改为2。因此，您应首先从组中删除终端，然后分配组2。



3-6.终端组更改对CCV的影响

步骤4.、5.和6.反映在此图中。由于分析，终端将身份组更改为步骤4中所示的ekorneyc_ASSET_Group2，这导致ISE将CoA发送到交换机（步骤5），最后终端重新身份验证（步骤6）。



交换机**show authentication sessions interface fa1/7 detail**确认已分配新的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#
```

Appendix

交换机TrustSec相关配置

> **注意**：Cts凭证不属于running-config，应在特权执行模式下使用**cts credentials id <id> password <password>**命令进行配置。

```
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#
```