Configuration de l'intégration ISE 2.7 pxGrid CCV 3.1.0

Contenu

Introduction

Ce document décrit comment configurer et dépanner l'intégration d'ISE (Identity Services Engine) 2.7 avec Cisco Cyber Vision (CCV) 3.1.0 sur Platform Exchange Grid v2 (pxGrid). CCV est enregistré auprès de pxGrid v2 en tant qu'éditeur et publie des informations sur les attributs des points de terminaison dans ISE pour IOTASSET Dictionary.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- ISE
- Cisco Cyber Vision

Components Used

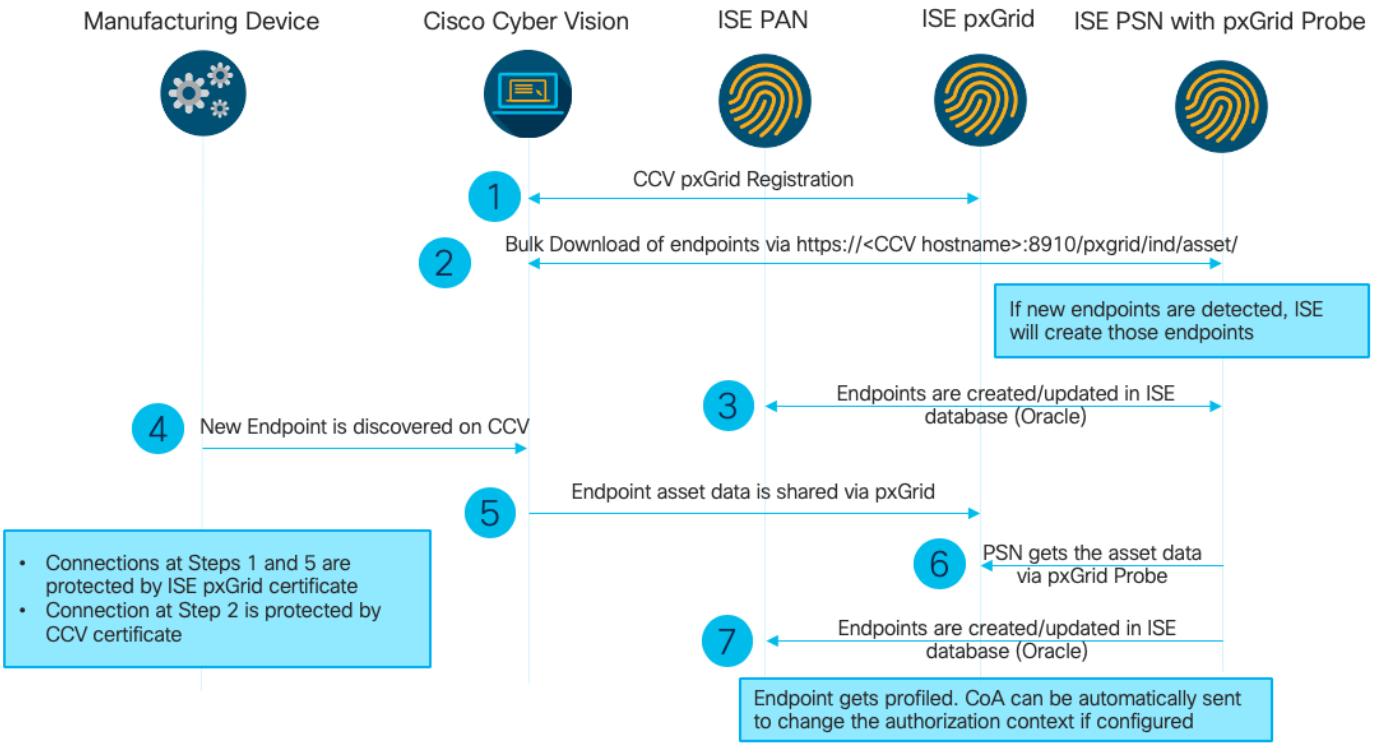
Les informations de ce document sont basées sur les versions logicielles et matérielles suivantes :

- Correctif 1 de Cisco ISE version 2.7
- Cisco Cybervision version 3.1.0
- Commutateur Ethernet industriel IE-4000-4TC4G-E avec logiciel 15.2(6)E

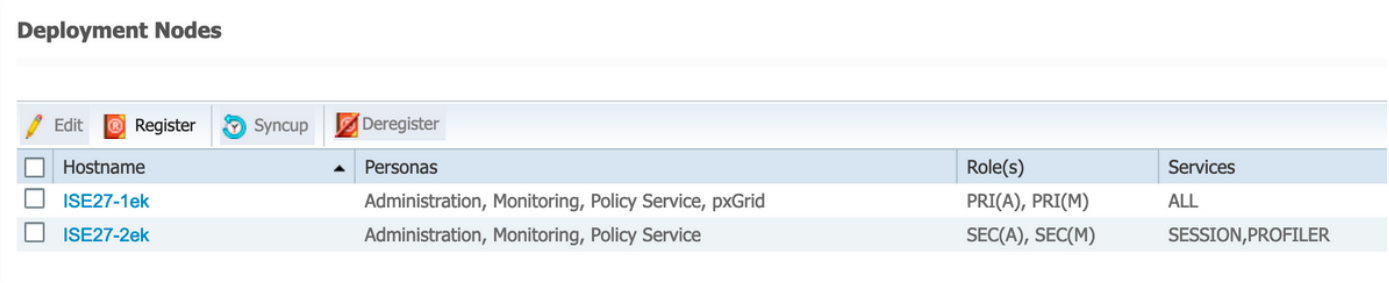
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configuration

Diagramme de flux de haut niveau



Ce déploiement ISE est utilisé dans la configuration.



ISE 2.7-1ek est le noeud d'administration principal (PAN) et le noeud pxGrid.

ISE 2.7-2ek est un noeud de service de stratégie (PSN) avec sonde pxGrid activée.

Voici les étapes qui correspondent au schéma mentionné précédemment.

1. CCV s'enregistre sur assetTopic sur ISE via pxGrid version 2. Journaux correspondants de CCV :

> **Note**: Afin de revoir les journaux pxGrid sur CCV, émettez la commande suivante **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. ISE PSN avec la sonde pxGrid activée effectue un téléchargement en masse des actifs pxGrid existants (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. Les terminaux sont ajoutés au PSN avec la sonde pxGrid activée et PSN envoie un événement persist au PAN pour enregistrer ces terminaux (profiler.log). Les points de terminaison créés sur ISE peuvent être affichés dans les détails des points de terminaison sous Visibilité contextuelle.

```
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. Après avoir placé un point de terminaison dans un groupe, CCV envoie un message STOMP via le port 8910 pour mettre à jour le point de terminaison avec les données de groupe dans les attributs personnalisés. Journaux correspondants de CCV :

```
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. Le noeud PxGrid reçoit la mise à jour STOMP et transmet ce message à tous les abonnés, il inclut les PSN avec la sonde pxGrid activée. **pxgrid-server.log** sur le noeud pxGrid.

```
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. PSN avec la sonde pxGrid activée en tant qu'abonné sur la rubrique des ressources reçoit le message du noeud pxGrid et met à jour le point de terminaison (**profiler.log**). Les terminaux mis à jour sur ISE peuvent être affichés dans les détails des terminaux sous Visibilité contextuelle.

```
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. PSN avec la sonde pxGrid activée reprofile le point de terminaison au fur et à mesure qu'une nouvelle stratégie est mise en correspondance (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 -:
```

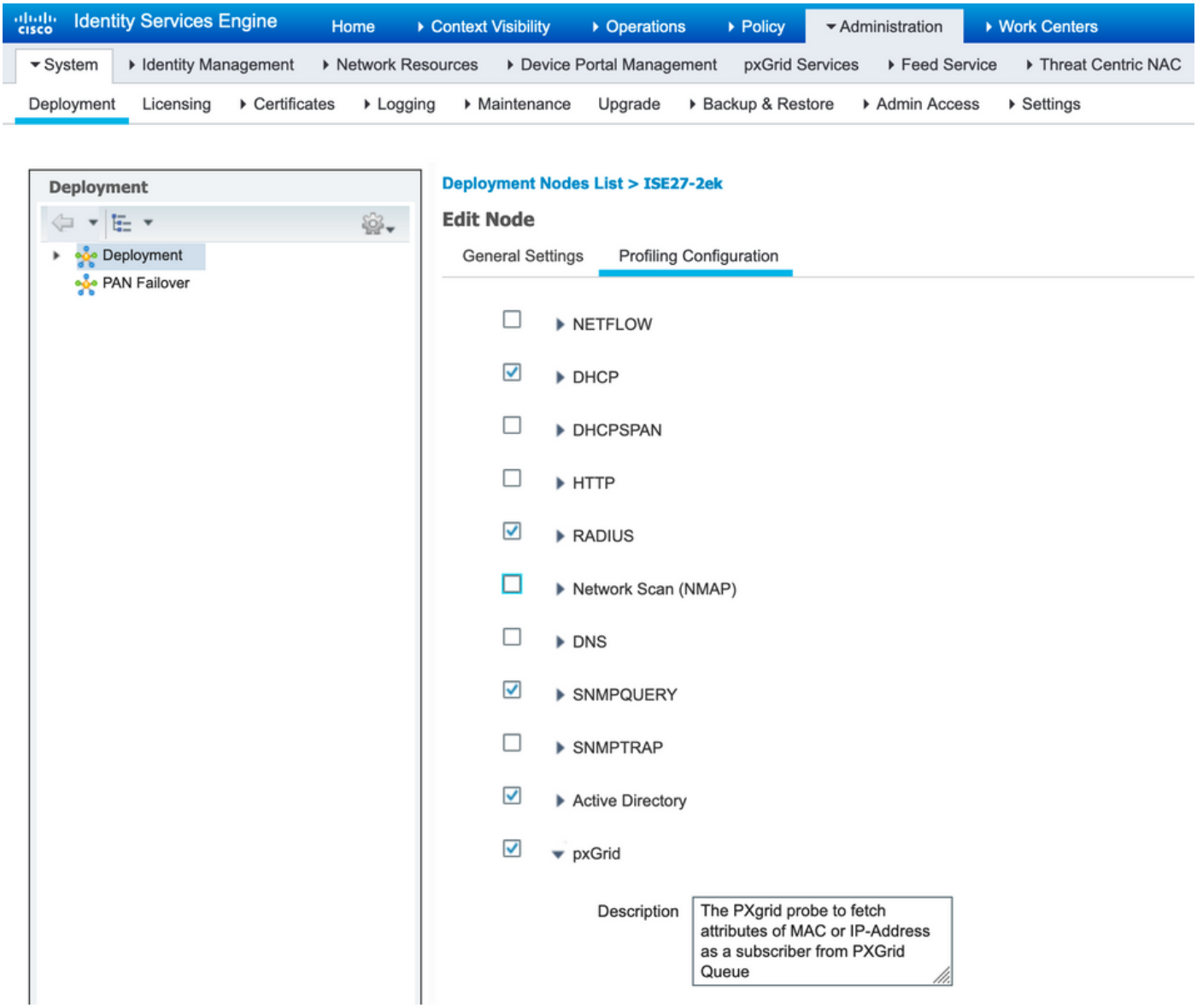
```
00:F2:8B:A0:3A:59:9d077480-b628-11ea-bdb7-82edacd9a457:Profiling:- After analyzing policy
hierarchy: Endpoint:
00:F2:8B:A0:3A:59 EndpointPolicy:ekorneyc_ASSET_Group1 for:20 ExceptionRuleMatched:false
2020-06-24 14:40:13,778 DEBUG [forwarder-9][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:
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
```

Configurations

> **Note**: Les étapes 1 à 4 sont obligatoires même si vous souhaitez avoir une visibilité de assetGroup et dans Visibilité contextuelle.

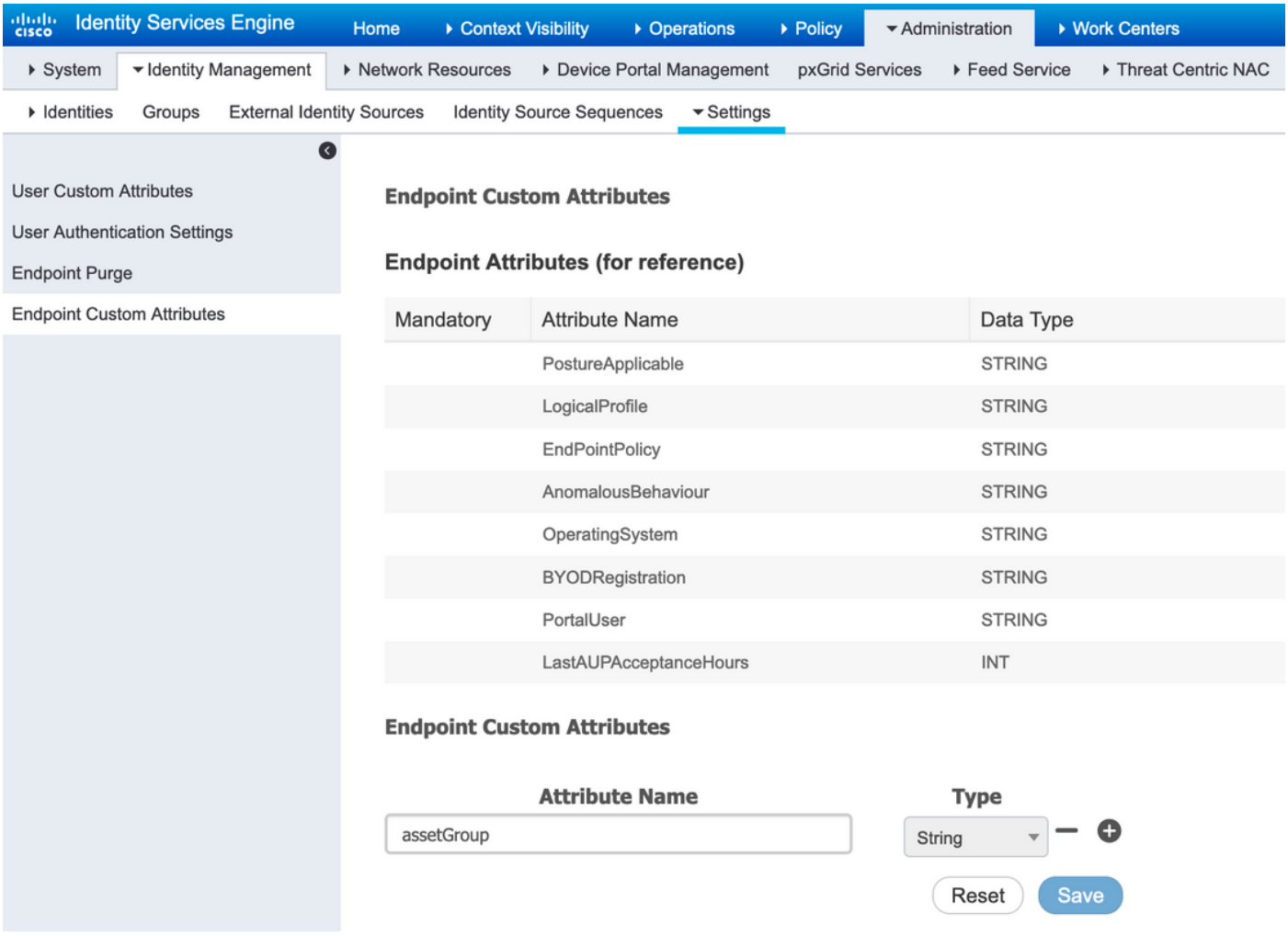
1. Activer la sonde pxGrid sur l'un des PSN

Accédez à **Administration > System > Deployment**, sélectionnez ISE node with PSN Persona. Basculez vers l'onglet **Configuration du profilage**. Vérifiez que la sonde **pxGrid** est activée.



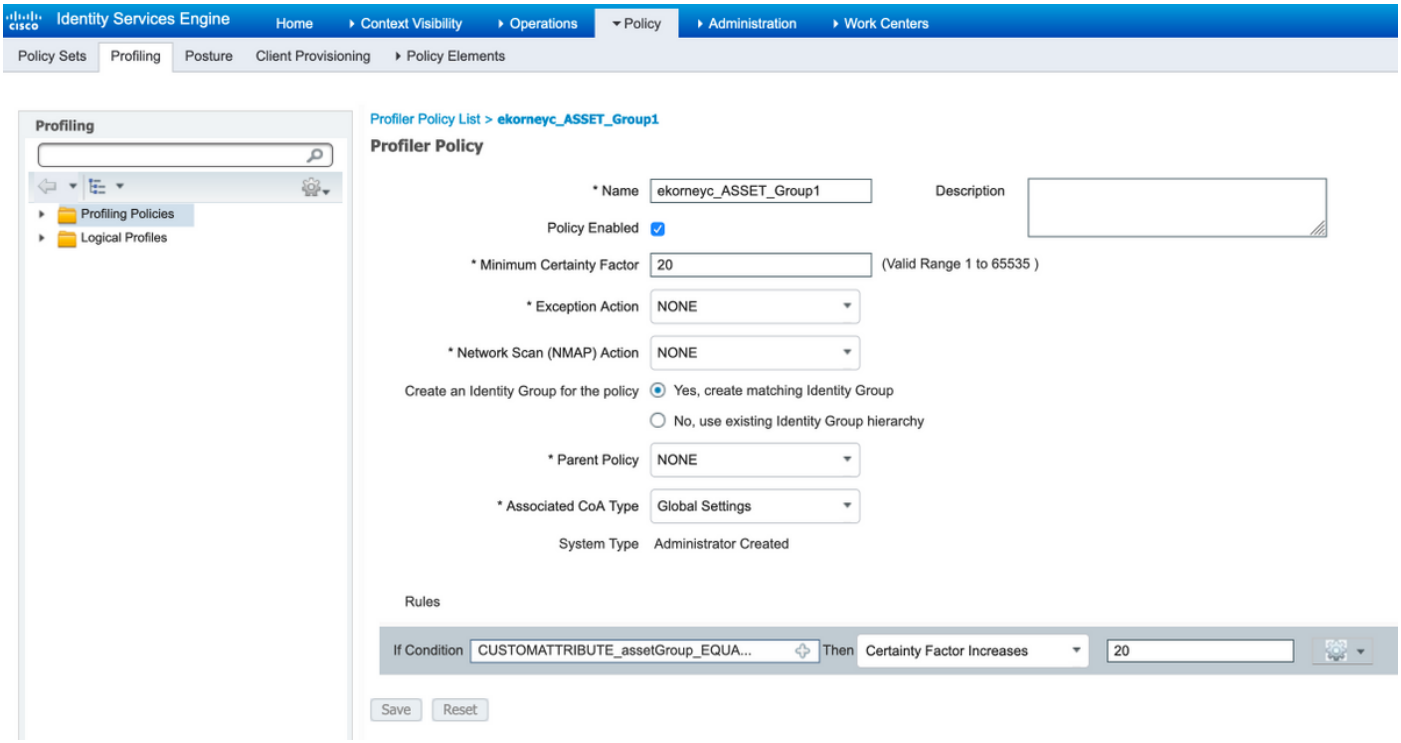
2. Configurer les attributs personnalisés des points de terminaison sur ISE

Accédez à **Administration > Identity Management > Settings > Endpoint Custom Attributes**. Configurez les attributs personnalisés (assetGroup) en fonction de cette image. CCV 3.1.0 prend uniquement en charge l'attribut **assetGroup** personnalisé.



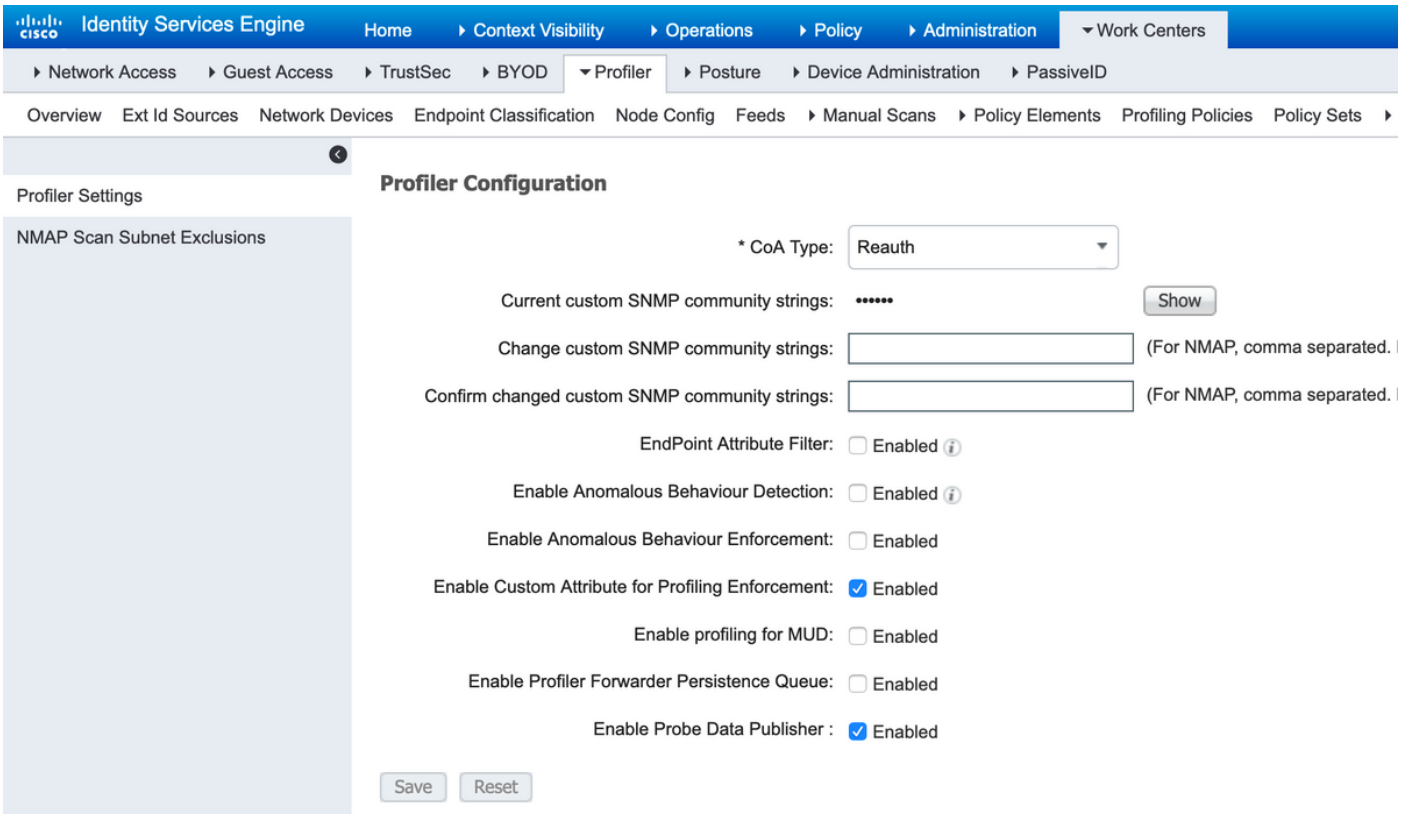
3. Configurer la stratégie de profileur à l'aide d'attributs personnalisés

Accédez à **Centres de travail > Profiler > Stratégies de profilage**. Cliquez sur **Ajouter**. Configurez la stratégie de profileur de la même manière que cette image. L'expression de condition utilisée dans cette stratégie est **CUSTOMATTRIBUTE : assetGroup EQUALS Group1.**



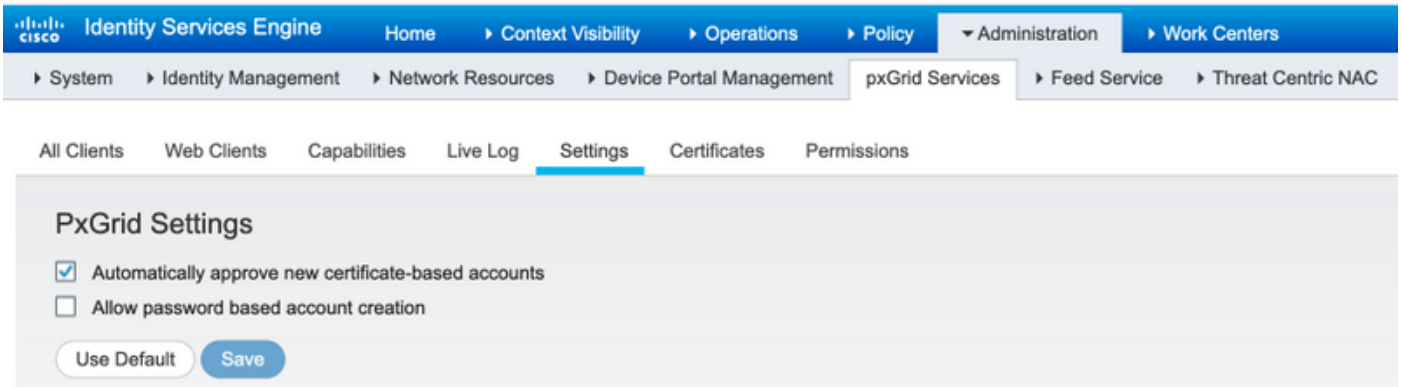
4. Activer les attributs personnalisés pour l'application du profilage

Accédez à **Centres de travail > Profiler > Stratégies de profilage**. Cliquez sur **Ajouter**. Configurez la stratégie de profileur de la même manière que cette image. Assurez-vous que l'option **Activer l'attribut personnalisé pour l'application de profilage** est activée.



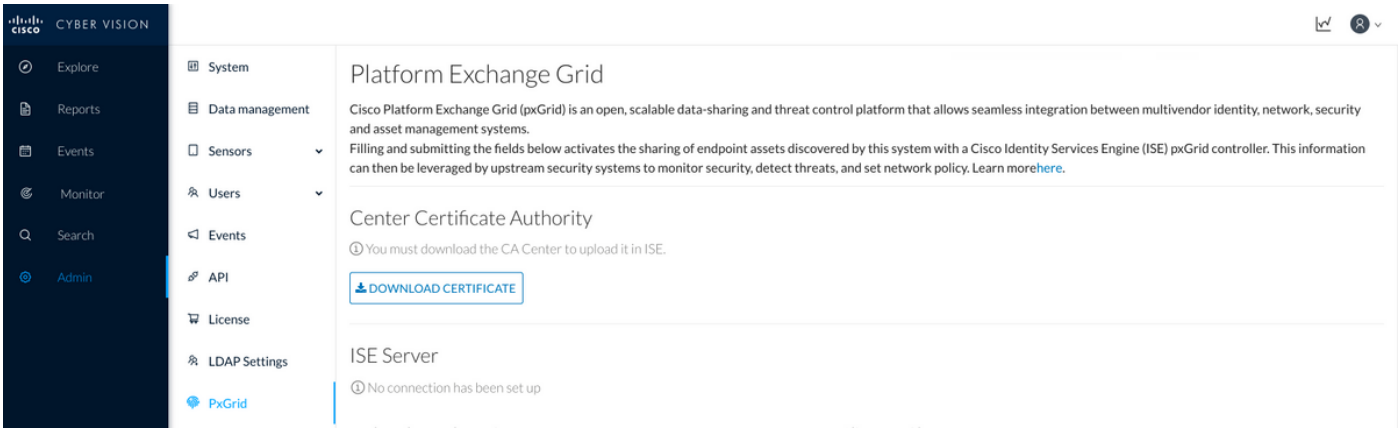
5. Configurer l'approbation automatique pour les clients pxGrid

Accédez à **Administration > pxGrid Services > Settings**. Sélectionnez **Approuver automatiquement les nouveaux comptes basés sur des certificats** et cliquez sur **Enregistrer**. Cette étape garantit que vous n'avez pas besoin d'approuver CCV une fois l'intégration terminée.



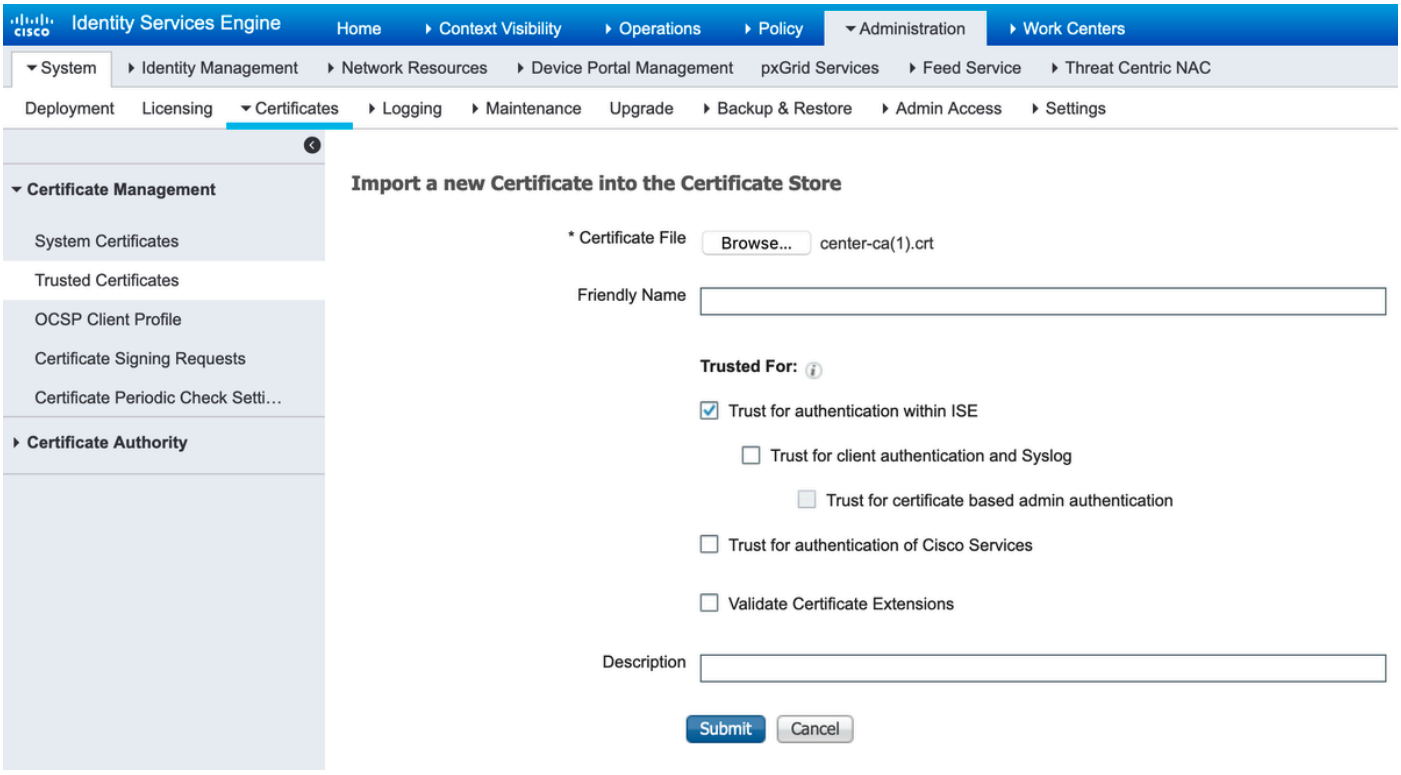
6. Exporter le certificat CCV

Accédez à **Admin > pxGrid**. Cliquez sur **TÉLÉCHARGER LE CERTIFICAT**. Ce certificat est utilisé lors de l'enregistrement pxGrid, de sorte que ISE doit lui faire confiance.



7. Télécharger le certificat d'identité CCV dans le magasin de confiance ISE

Accédez à **Administration > Certificats > Certificate Management > Trusted Certificates**. Cliquez sur **Importer**. Cliquez sur **Parcourir** et sélectionnez le certificat CCV à l'étape 5. Cliquez sur Submit.



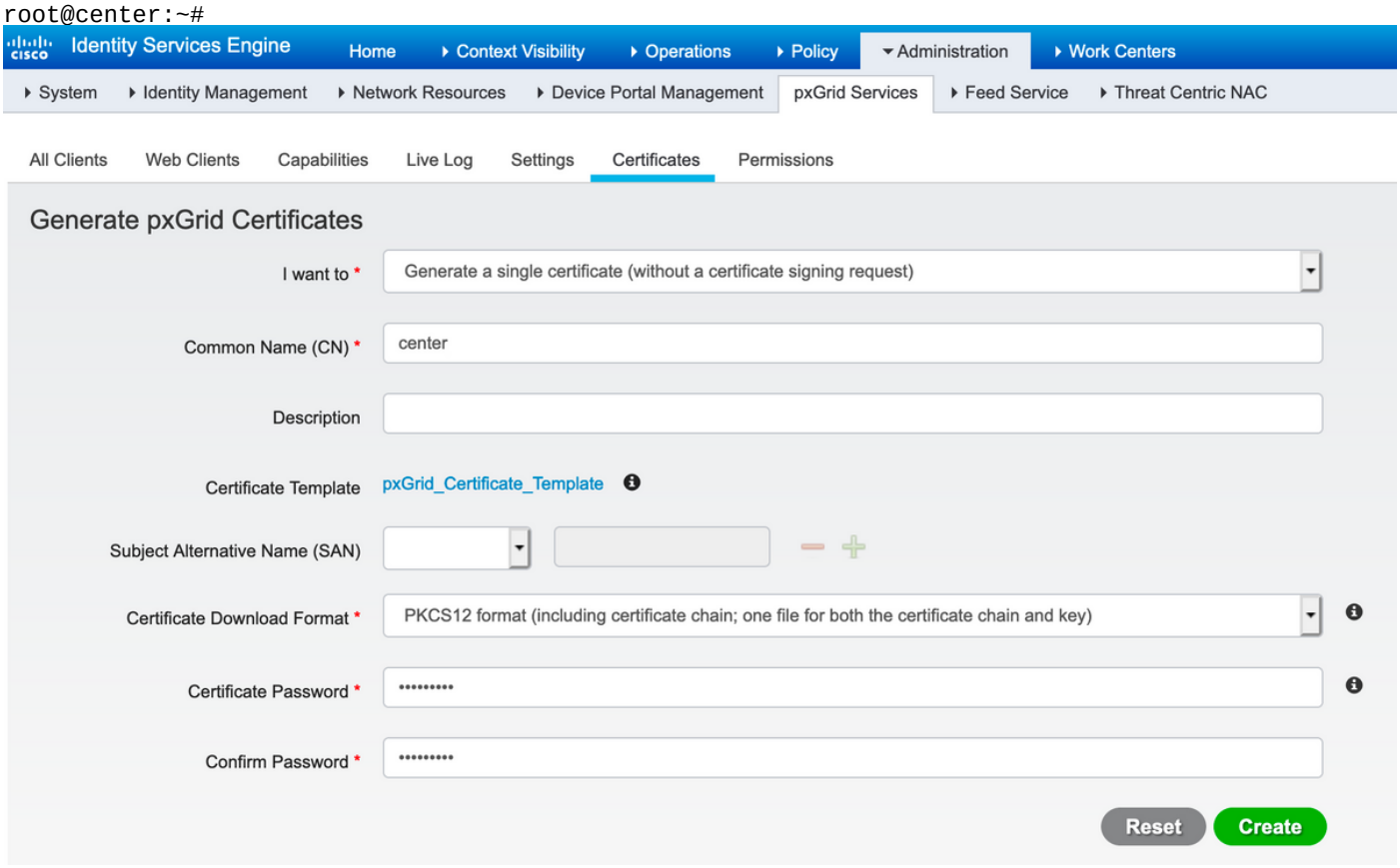
8. Générer un certificat pour CCV

Lors de l'intégration et des mises à jour de pxGrid, CCV a besoin du certificat client. Il doit être émis par l'autorité de certification interne ISE, à l'aide de **PxGrid_Certificate_Template**.

Accédez à **Administration > pxGrid Services > Certificates**. Remplir les champs en fonction de cette image. Le champ Nom commun (CN) est obligatoire car l'objectif de l'AC ISE est d'émettre un certificat d'identité. Vous devez entrer le nom d'hôte CCV, la valeur du champ CN est critique. Afin de vérifier le nom d'hôte de CCV, émettez la commande **hostname**. Sélectionnez PKCS12 comme **format de téléchargement de certificat.**

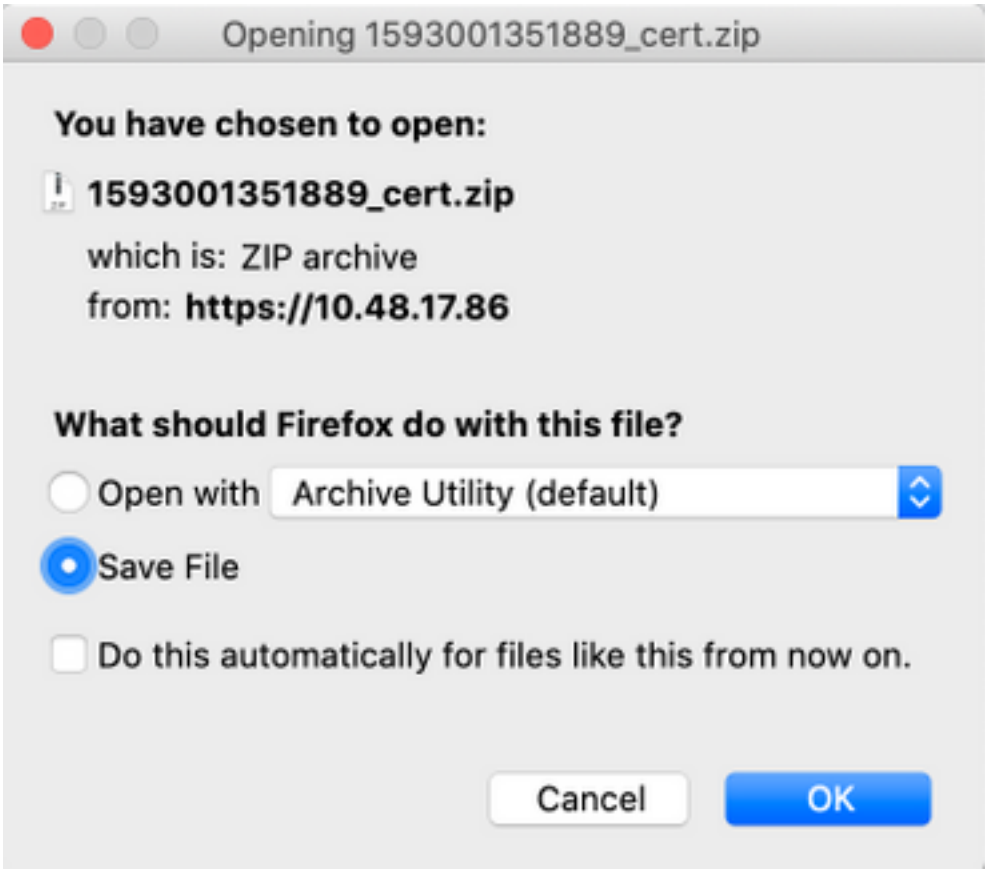
```
root@center:~# hostname
center
```

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



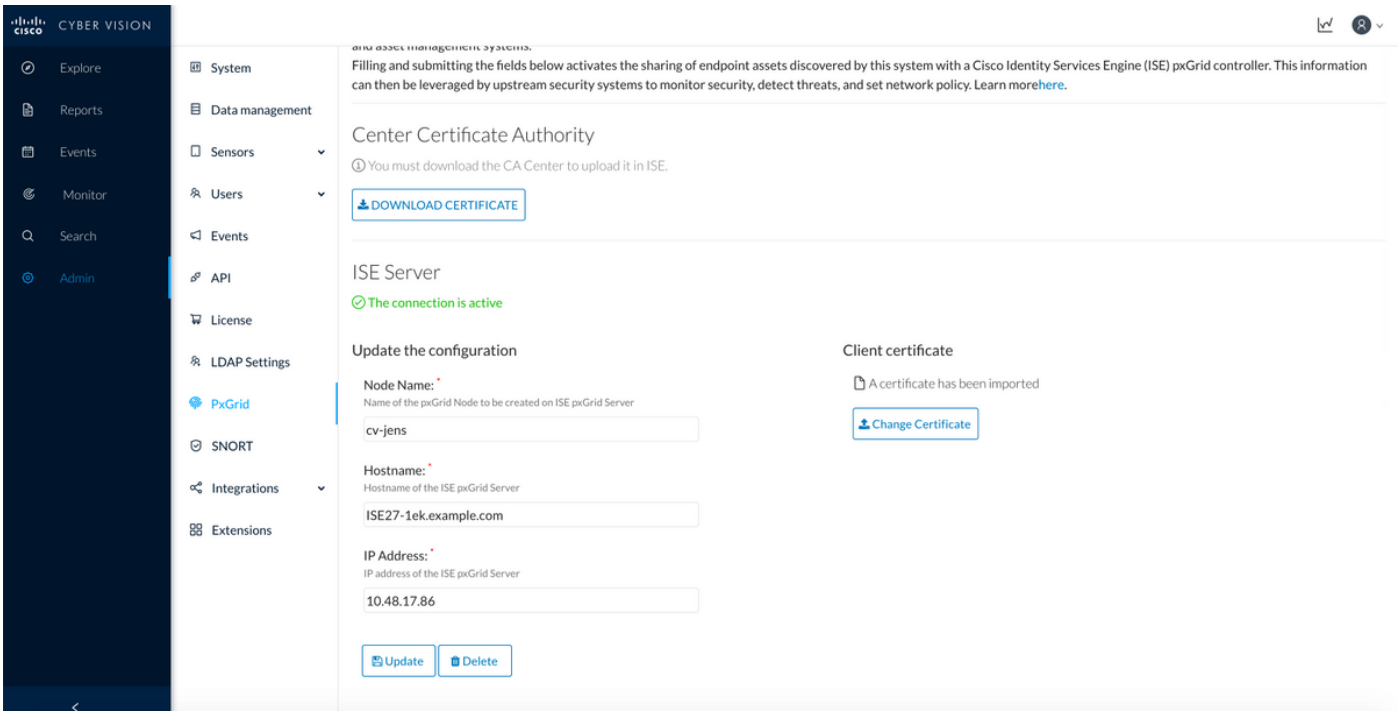
9. Télécharger la chaîne de certificats au format PKCS12

Lorsque vous installez le certificat au format PKCS12, ainsi que la chaîne d'autorité de certification interne ISE du certificat d'identité CCV est installée sur CCV pour vous assurer que CCV fait confiance à ISE lorsque la communication pxGrid est initiée à partir d'ISE, par exemple, des messages de test d'activité pxGrid.



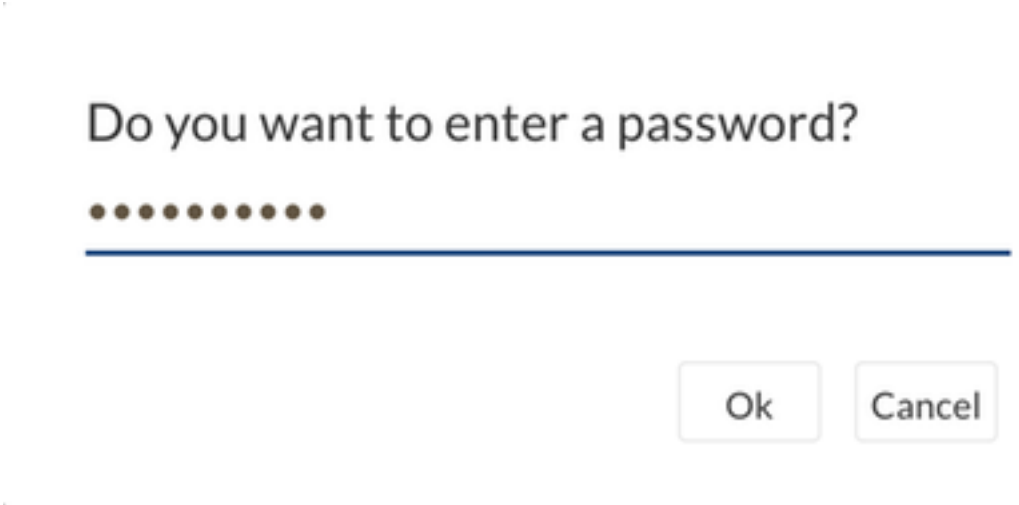
10. Configurer les détails de l'intégration ISE sur CCV

Accédez à **Admin > pxGrid**. Configurez le nom du noeud. Ce nom s'affichera sur ISE en tant que nom de client à **Administration > pxGrid Services > Web Clients.** Configurez **le nom d'hôte** et l'**adresse IP** du noeud ISE pxGrid. Assurez-vous que CCV peut résoudre le nom de domaine complet ISE.



11. Télécharger la chaîne de certificats sur CCV et lancer l'intégration

Accédez à **Admin > pxGrid**. Cliquez sur **Modifier le certificat**. Sélectionnez un certificat émis par l'autorité de certification ISE dans les étapes 8 à 9. Entrez le mot de passe à l'étape 8. puis cliquez sur **OK.**



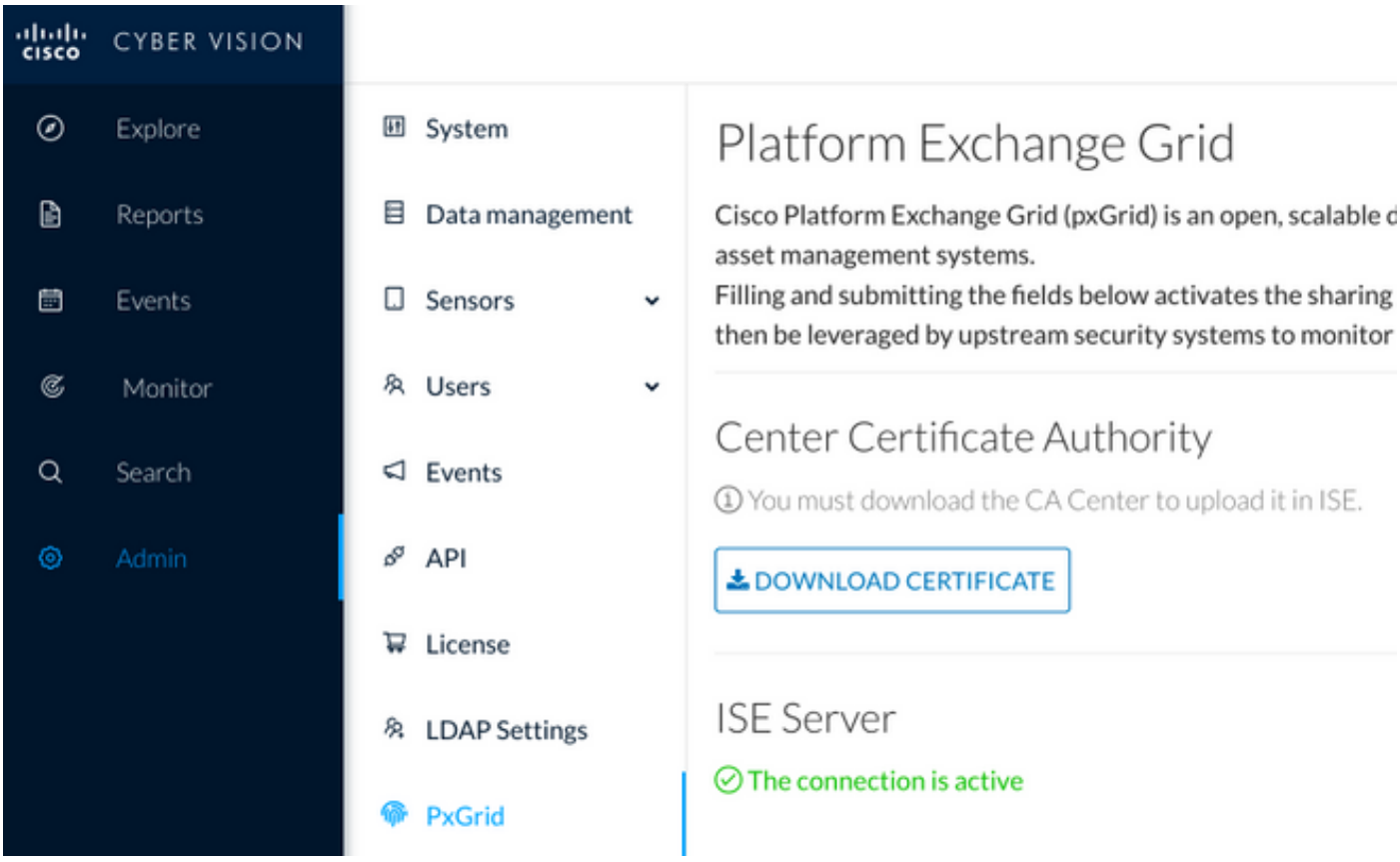
Cliquez sur **Update**, qui déclenche l'intégration CCV - ISE réelle.

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Vérification de l'intégration CCV

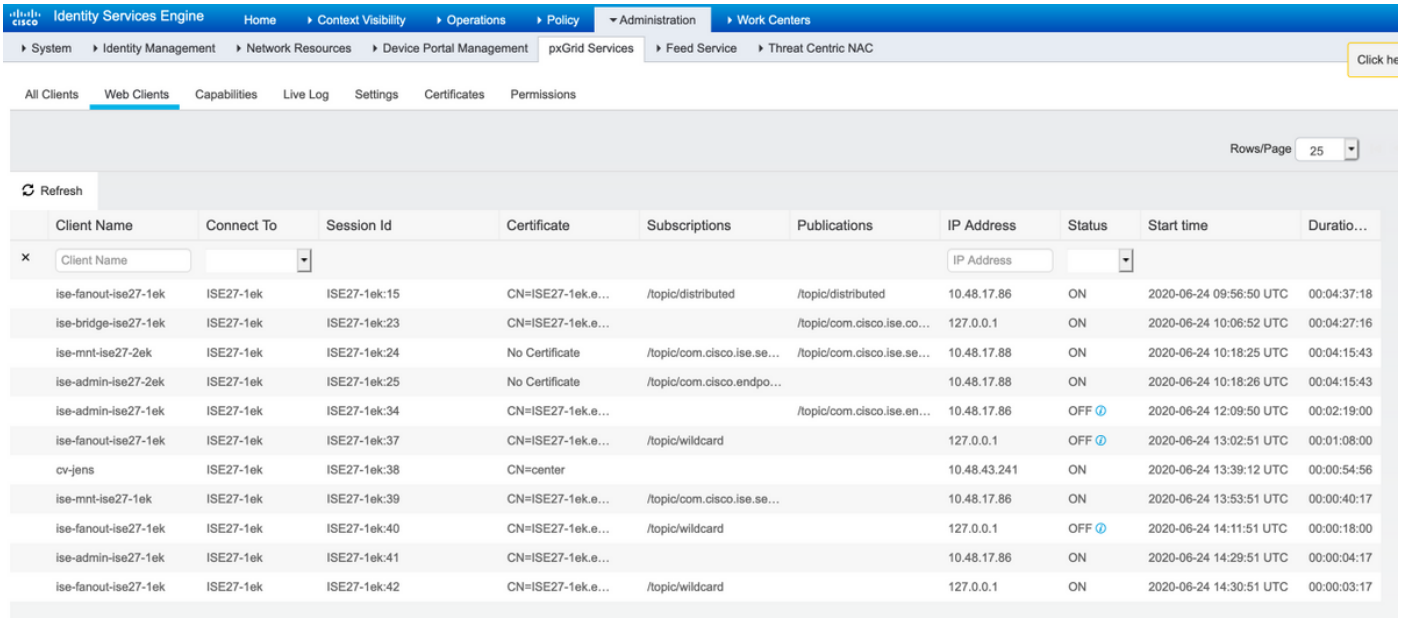
Une fois l'intégration terminée, vous pouvez confirmer qu'elle réussit en accédant à **Admin > pxGrid**. Vous devriez voir **le** message **Connexion active** sous Serveur ISE.



Vérification de l'intégration ISE

Accédez à **Administration > pxGrid Services > Web Clients**. Vérifiez que l'état du client CCV (cv-jens) est **ACTIVÉ.**

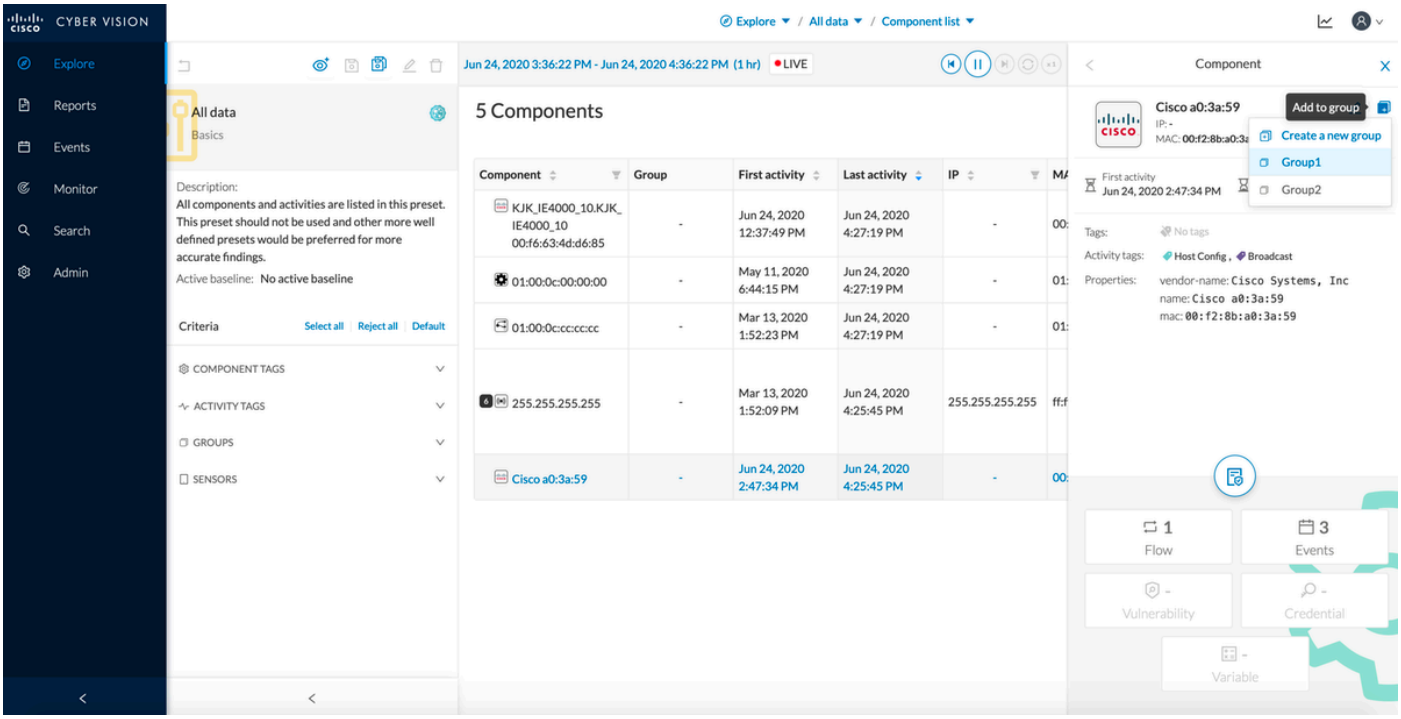
> **Note**: Il est prévu que le statut du client CCV pxGrid soit **hors connexion** dans le menu **Tous les clients**, car il affiche uniquement l'état de pxGrid v1.



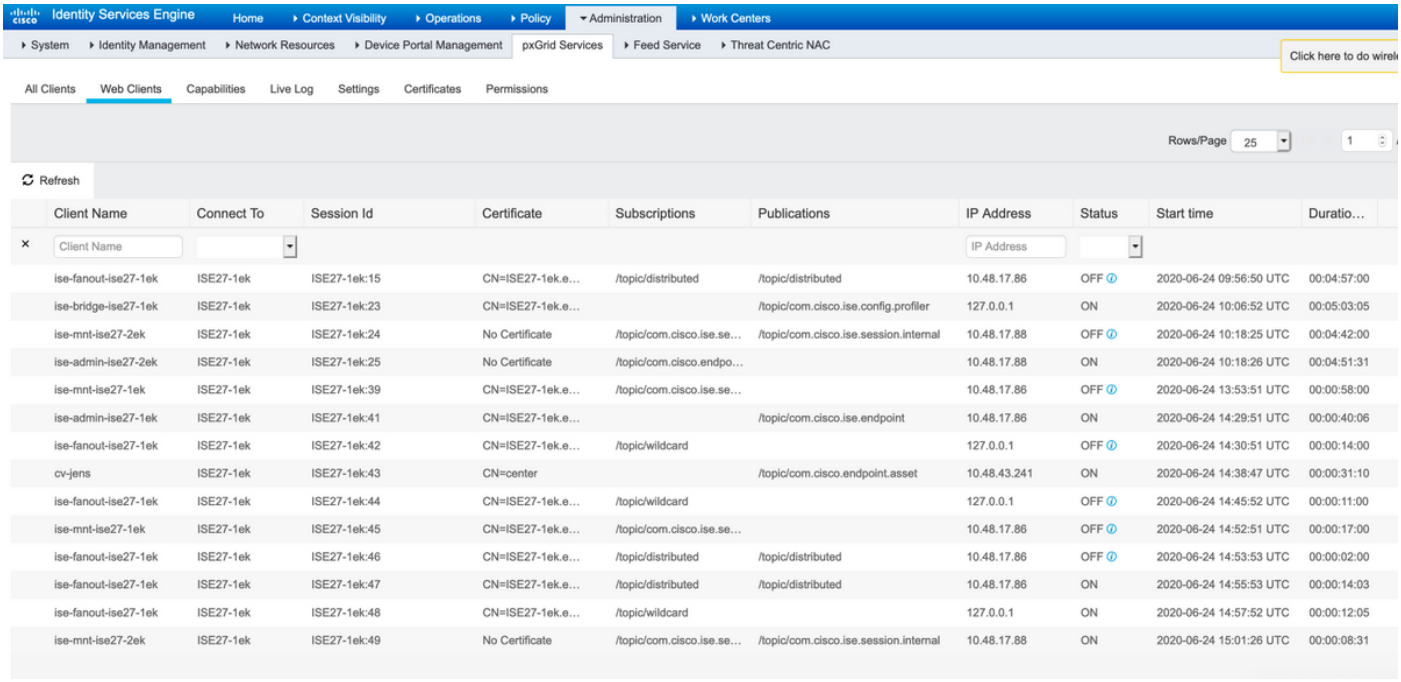
> **Note**: En raison de CSCvt78208 vous ne verrez pas immédiatement CCV ayant **/topic/com.cisco.ise.endpoint.asset**, il ne sera affiché que lors de la première publication.

Vérifier la modification du groupe CCV

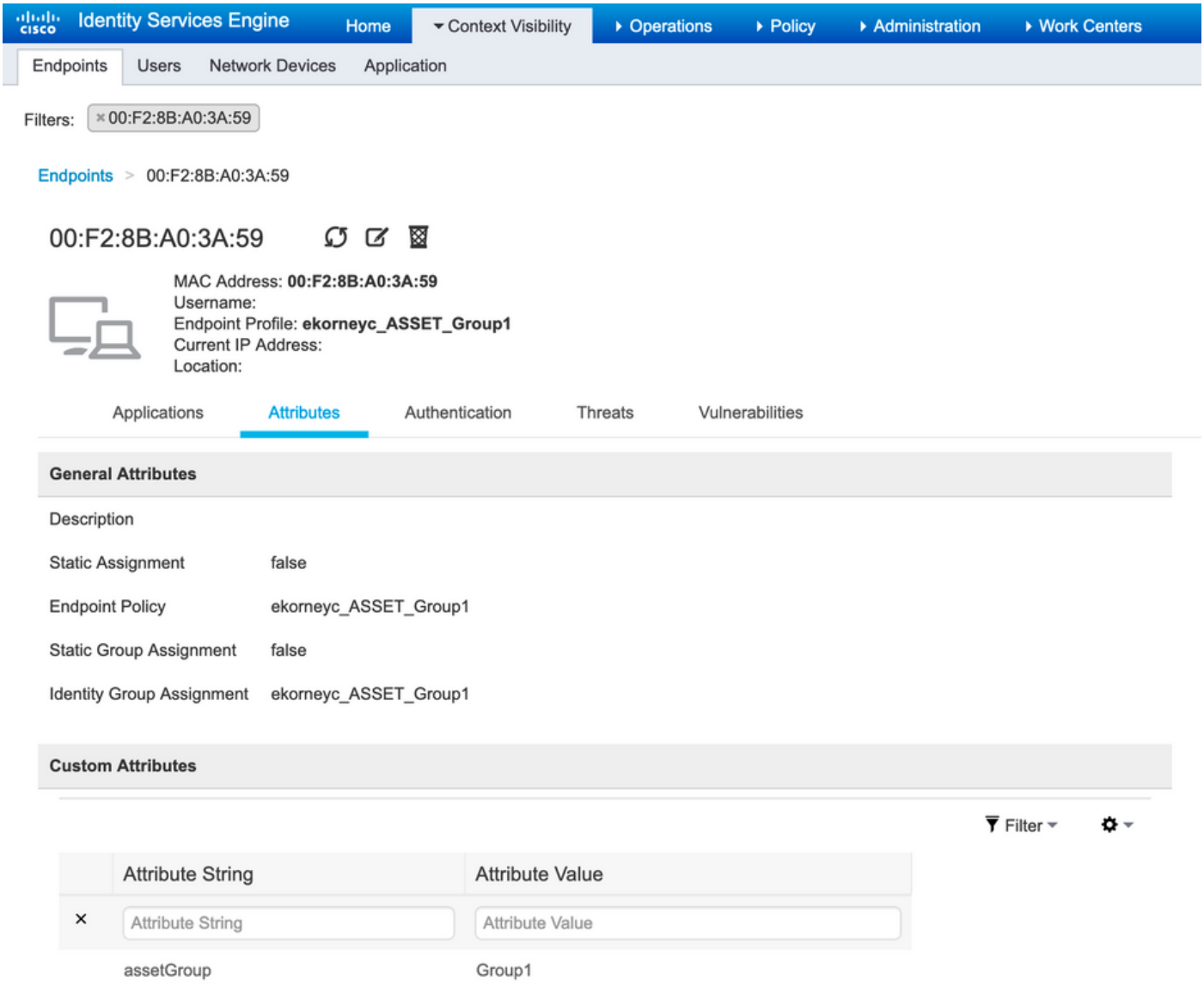
Accédez à **Explore > All data > Component list**. Cliquez sur l'un des composants et **ajoutez**-le au groupe.



Vérifiez que **/topic/com.cisco.ise.endpoint.asset** figure désormais dans la liste Publications de CCV.



Vérifiez que le groupe 1 attribué via CCV est reflété dans ISE et que la stratégie de profilage est entrée en vigueur en accédant à **Visibilité contextuelle > Terminaux**. Sélectionnez le point de terminaison mis à jour à l'étape précédente. Basculez vers l'onglet Attributs. La section des attributs personnalisés doit refléter le groupe nouvellement configuré.



La section Autres attributs répertorie tous les autres attributs d'actif reçus de CCV.

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

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Activer les débogages sur ISE

Afin d'activer les débogages sur ISE, accédez à **Administration > System > Logging > Debug Log Configuration**. Définissez les niveaux de journal sur les éléments suivants :

Persona	Nom du composant	Niveau du journal	Fichier à vérifier
PAN (facultatif)	profileur	DÉBOGUER	profiler.log
PSN avec sonde pxGrid activée	profileur	DÉBOGUER	profiler.log
PxGrid	pxgrid	TRAITER	pxgrid-server.log

Activer les débogages sur CCV

Afin d'activer les débogages sur CCV :

- Créer un fichier **/data/etc/sbs/pxgrid-agent.conf** avec la commande **touch /data/etc/sbs/pxgrid-agent.conf**
- Collez ce contenu dans le fichier **pxgrid-agent.conf** à l'aide de l'éditeur **vi** à l'aide de la commande **vi /data/etc/sbs/pxgrid-agent.conf**

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

- Redémarrez pxgrid-agent en exécutant la commande **systemctl restart pxgrid-agent**
- Afficher les journaux à l'aide de la commande **journalctl -u pxgrid-agent**

Échec du téléchargement en masse

CCV publie l'URL de téléchargement en masse vers ISE pendant l'intégration. ISE PSN avec la sonde pxGrid activée effectue le téléchargement en masse à l'aide de cette URL. Vérifiez les points suivants :

- Le nom d'hôte de l'URL peut être résolu correctement du point de vue de l'ISE
- La communication de PSN sur le port 8910 vers CCV est autorisée

profiler.log sur PSN avec sonde pxGrid activée :

```
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}]]
```

Le téléchargement en masse peut échouer en raison de CSCvt75422, vous devriez voir cette erreur dans **profiler.log** sur ISE pour la confirmer. Le défaut est corrigé dans CCV 3.1.0.

```
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)
```

Tous les terminaux ne sont pas créés sur ISE

Certains points de terminaison sur CCV peuvent avoir trop d'attributs attachés, de sorte que la base de données ISE ne pourra pas les gérer. Il peut être confirmé si vous voyez ces erreurs dans **profiler.log** sur ISE.

```
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 n'est pas disponible sur ISE

Si AssetGroup n'est pas disponible sur ISE, la stratégie de profilage n'est probablement pas configurée à l'aide d'attributs personnalisés (reportez-vous aux étapes 2 à 4. dans la partie Configurations du document). Même pour la visibilité contextuelle, l'affichage des attributs de groupe, des stratégies de profilage et d'autres paramètres des étapes 2 à 4 est obligatoire.

Les mises à jour de groupe de terminaux ne sont pas reflétées dans ISE

En raison de CSCvu80175, CCV ne publie pas de mises à jour de terminaux sur ISE avant le redémarrage de CCV juste après l'intégration. Vous pouvez redémarrer CCV une fois l'intégration effectuée comme solution de contournement.

La suppression d'un groupe de CCV ne le supprime pas de ISE

Ce problème est détecté en raison du défaut connu sur CCV CSCvu47880.La mise à jour pxGrid envoyée lors de la suppression du groupe de CCV ayant un format différent de celui attendu, le groupe n'est donc pas supprimé.

CCV quitte les clients Web

Ce problème est dû au défaut connu sur ISE CSCvu47880 où les clients passent à l'état OFF, suivi d'une suppression complète des clients Web. Le problème est résolu dans les correctifs 2.6 7 et 2.7 2 de l'ISE.

Vous pouvez le confirmer si vous voyez ces erreurs dans **pxgrid-server.log** sur ISE :

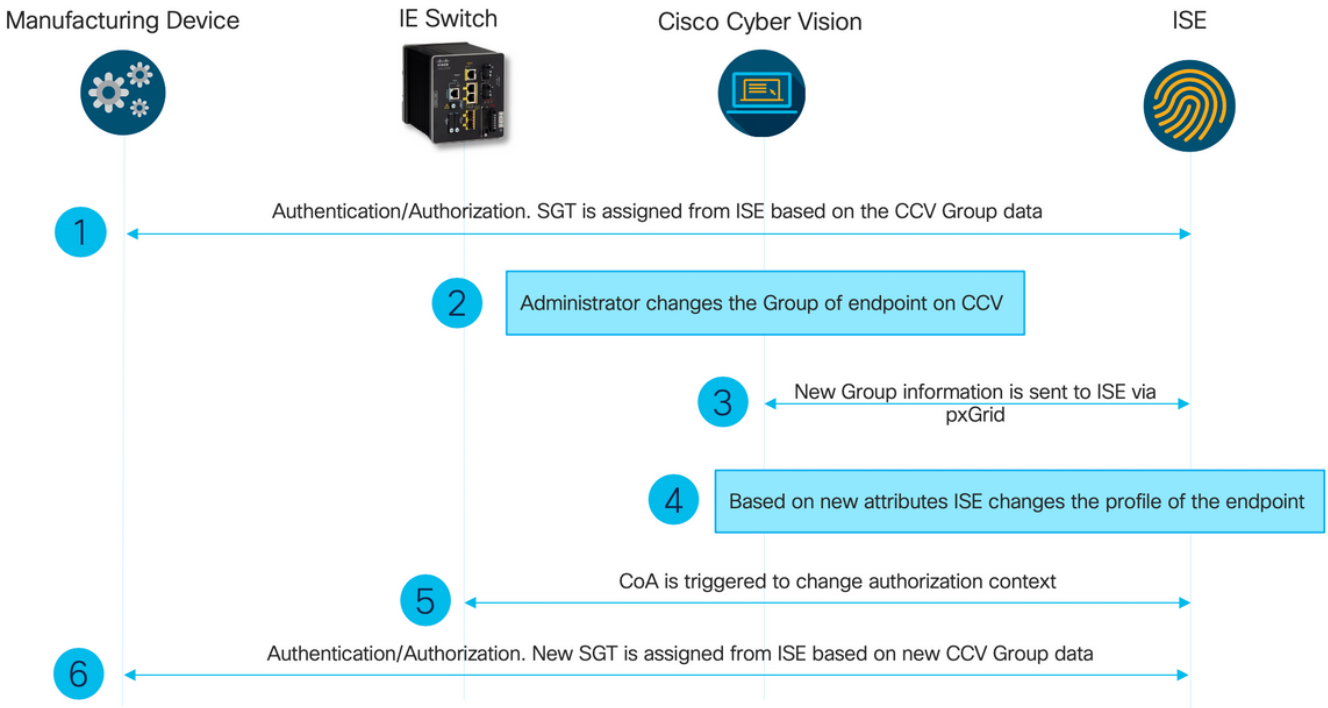
```
2020-06-26 09:42:28,772 DEBUG [Pxgrid-SessionManager-LookupAccountsTask][]
cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -::::::-
onClose: session=[14f,CLOSED], sessionInfo=WSSessionInfo [id=336, nodeName=cv-jens,
addr=10.48.43.241, sessionID=14f, status=OFF,
creationTime=2020-06-26 08:19:28.726,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

Intégration ISE avec Cas d'utilisation CCV TrustSec

Cette configuration montre comment l'intégration ISE avec CCV peut bénéficier de la sécurité de bout en bout lorsque TrustSec est en place. Ce n'est qu'un exemple de la façon dont l'intégration peut être utilisée, une fois l'intégration effectuée.

> **Note**: L'explication de configuration du commutateur TrustSec n'entre pas dans le champ de cet article, cependant, elle se trouve dans l'annexe.

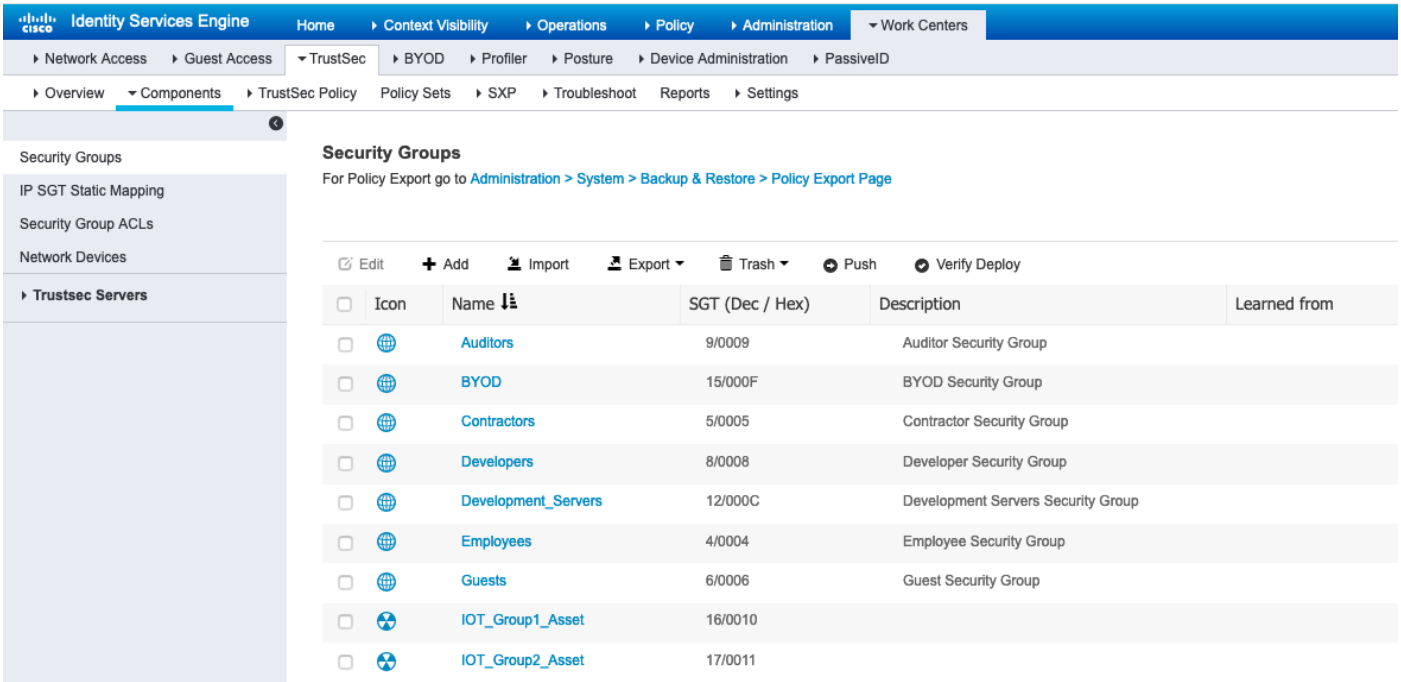
Topologie et flux



Configuration

1. Configurer des balises de groupe évolutif sur ISE

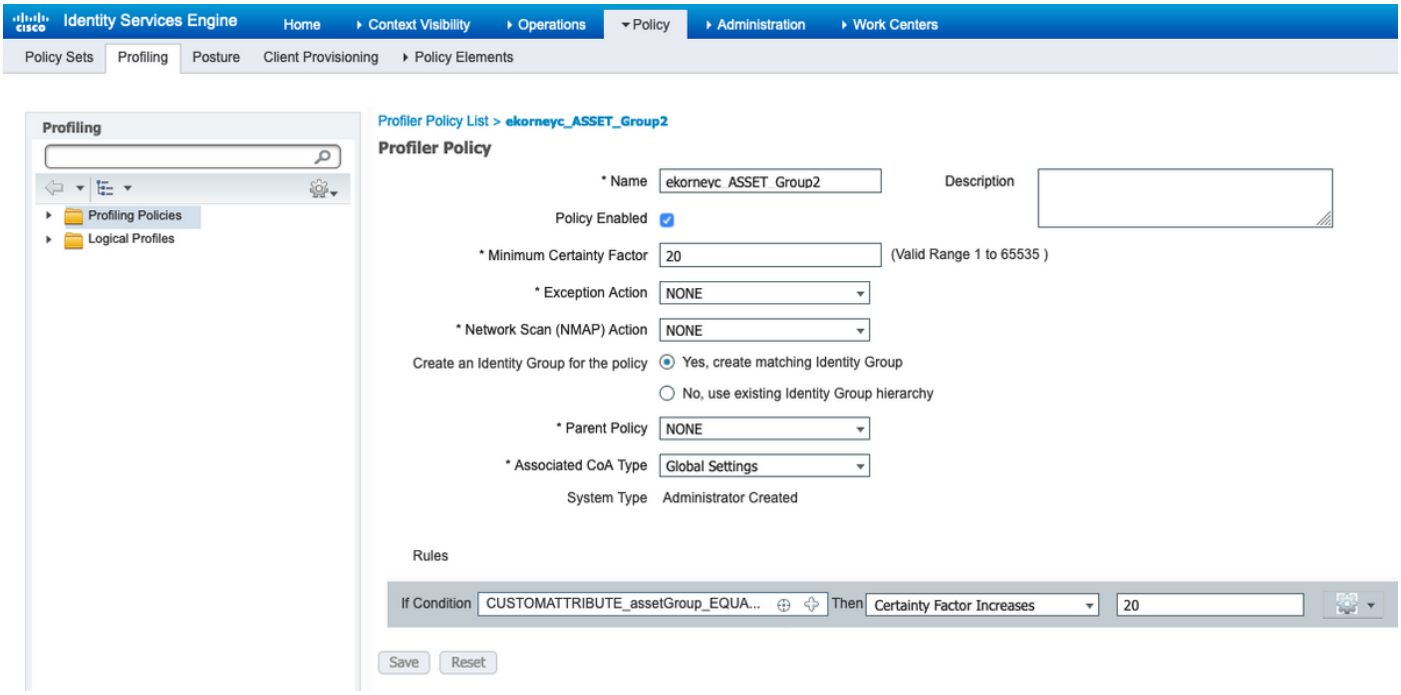
Afin d'atteindre le cas d'utilisation mentionné précédemment, les balises IOT_Group1_Asset et IOT_Group2_Asset de TrustSec sont configurées manuellement pour différencier les ressources CCV de Group1 de Group2. Accédez à **Centres de travail > TrustSec > Composants > Groupes de sécurité**. Cliquez sur **Ajouter.** Nommez les balises de groupe de sécurité (SGT) comme indiqué dans l'image.



2. Configurer la stratégie de profileur avec des attributs personnalisés pour le groupe 2

Note: La configuration du profilage pour le groupe 1 a été effectuée à l'étape 3. dans la première partie du document.

Accédez à **Centres de travail > Profiler > Stratégies de profilage**. Cliquez sur **Ajouter**. Configurez la stratégie de profileur de la même manière que cette image. L'expression de condition utilisée dans cette stratégie est **CUSTOMATTRIBUTE : assetGroup EQUALS Group2.**



3. Configurer les stratégies d'autorisation pour attribuer des balises de groupe de sécurité basées sur des groupes d'identité de point de terminaison sur ISE

Accédez à **Stratégie > Jeux de stratégies**. Sélectionnez **Jeu de stratégies** et configurez **les stratégies d'autorisation** comme indiqué dans cette image. Notez que par conséquent, les balises de groupe de sécurité sont configurées à l'étape 1. sont affectées.

Nom de la règle	Conditions	Profils	Groupes de sécurité
Politique du groupe 1 CCV	IdentityGroup · Name EQUALS Endpoint Identity Groups:Profilé:ekorneyc_ASSET_Group1	AutoriserAccès	Groupe_IOT1_Actif
Politique du groupe 2 CCV	IdentityGroup · Name EQUALS Endpoint Identity Groups:Profilé:ekorneyc_ASSET_Group2	AutoriserAccès	Groupe_IOT2_Actif

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

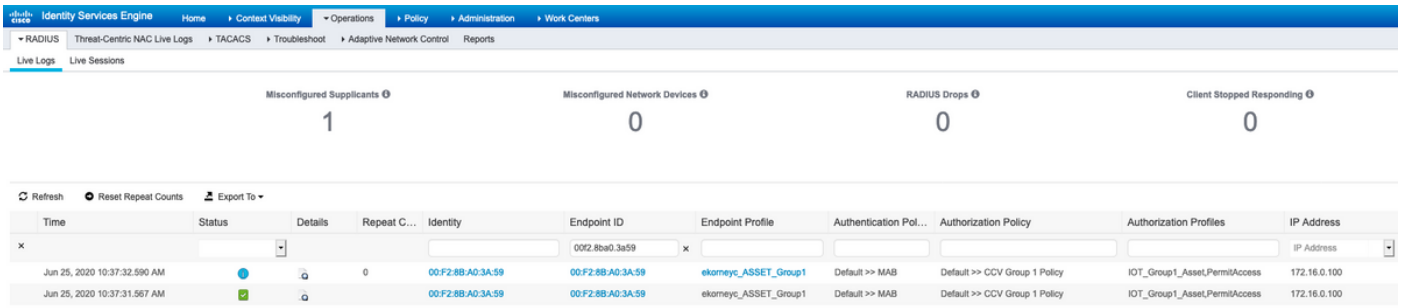
1. Authentification des terminaux sur la base du groupe CCV 1

Sur le commutateur, vous pouvez voir que les données d'environnement incluent à la fois **16-54:IOT_Group1_Asset** et **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#
```

Les terminaux s'authentifient et, par conséquent, la **stratégie de groupe 1 CCV** est mise en correspondance, SGT **IOT_Group1_Asset** est affectée.



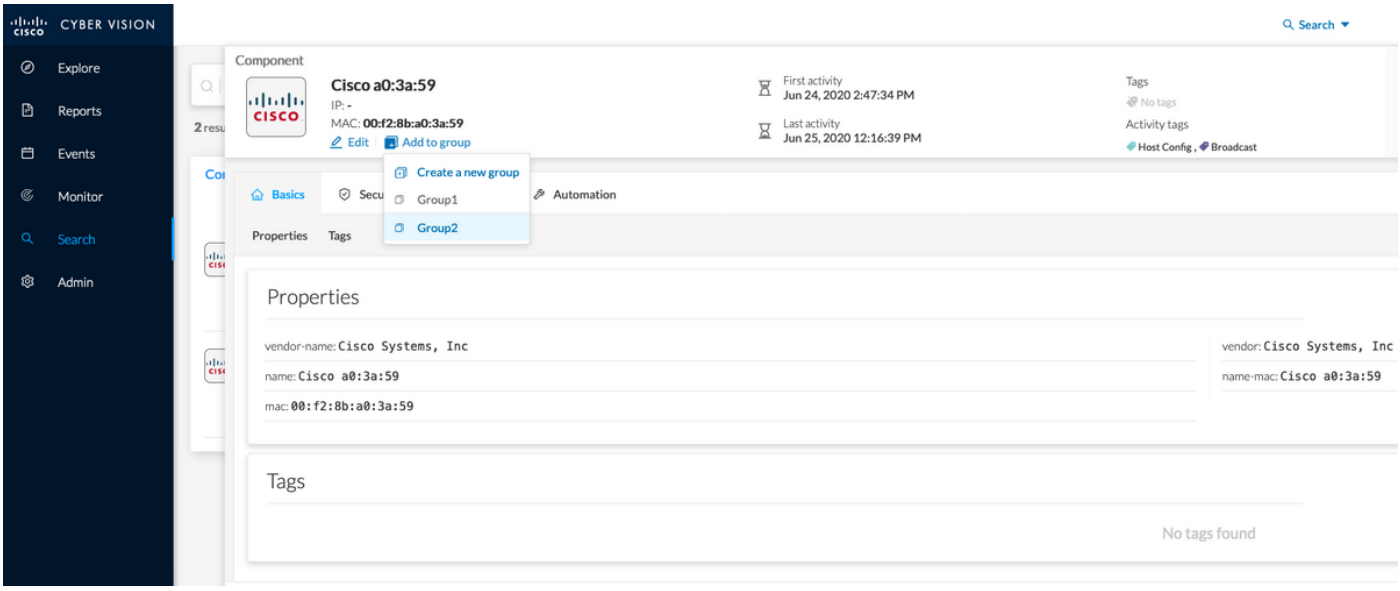
Le commutateur **show authentication sessions interface fa1/7 detail** confirme que les données Access-Accept ont été appliquées avec succès.

```
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. L'administrateur modifie le groupe

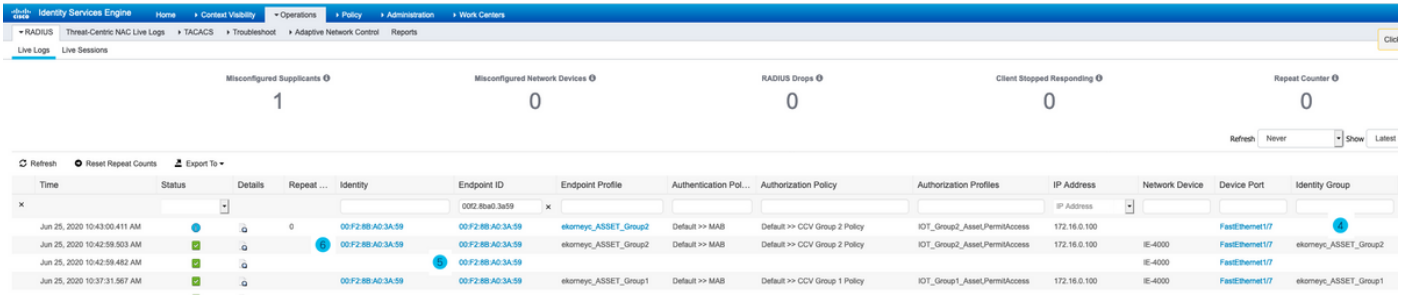
Accédez à **Rechercher**. Collez l'adresse Mac du point de terminaison, cliquez dessus et **ajoutez-**la au groupe 2.

> **Note**: Sur CCV, vous ne pouvez pas changer le groupe de 1 à 2 en une fois. Par conséquent, vous devez d'abord supprimer le point de terminaison du groupe et affecter ensuite le groupe 2.



3-6 . Effet du changement de groupe de terminaux sur CCV

Étapes 4, 5. et 6. sont reflétées dans cette image. Grâce au profilage, le point de terminaison a changé Identity Group en ekorneyc_ASSET_Group2 vu à l'étape 4., ce qui a provoqué l'envoi de CoA au commutateur (étape 5) et la réauthentification des points de terminaison (étape 6).



Le commutateur **show authentication sessions interface fa1/7 detail** confirme que la nouvelle SGT est attribuée.

```
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#
```

Annexe

Configuration associée TrustSec du commutateur

> **Note**: Les informations d'identification Cts ne font pas partie de running-config et doivent être configurées avec la commande **cts identification <id> password <password>** en mode d'exécution privilégié.

```
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#
```