ISE 2.7 pxGrid CCV 3.1.0統合の設定

内容

概要 前提条件 要件 使用するコンポーネント 設定 概要フロー図 設定 1. PSNの1つでpxGridプローブを有効にする 2. ISEでのエンドポイントカスタム属性の設定 3.カスタム属性を使用したプロファイラポリシーの構成 4.プロファイル適用のカスタム属性の有効化 5. pxGridクライアントの自動承認の設定 6. CCV証明書のエクスポート 7. CCV ID証明書のISE信頼ストアへのアップロード 8. CCVの証明書の生成 9. PKCS12形式での証明書チェーンのダウンロード 10. CCVでのISE統合の詳細の設定 11. CCVへの証明書チェーンのアップロードと統合の開始 確認 CCV統合の検証 ISE統合の検証 CCVグループの変更の確認 トラブルシュート ISEでのデバッグの有効化 CCVでのデバッグの有効化 一括ダウンロードの失敗 すべてのエンドポイントがISEで作成されるわけではありません AssetGroupがISEで使用できない エンドポイントグループの更新がISEに反映されない CCVからグループを削除してもISEからグループを削除できない WebクライアントからのCCVドロップ CCV TrustSecによるISE統合の使用例 トポロジとフロー 設定 1. ISEでのスケーラブルグループタグの設定 2.グループ2のカスタム属性を使用したプロファイラポリシーの設定 3. ISE上のエンドポイントIDグループに基づいてSGTを割り当てる認可ポリシーの設定 確認 1. CCVグループ1に基づいてエンドポイントを認証

2.管理者によるグループの変更

<u>3-6.エンドポイントグループ変更のCCVへの影響 付録 スイッチTrustSec関連の設定</u>

概要

このドキュメントでは、Platform Exchange Grid v2(pxGrid)上でCisco Cyber Vision(CCV)3.1.0と Identity Services Engine(ISE)2.7の統合を設定およびトラブルシューティングする方法について説 明します。CCVはpxGrid v2にパブリッシャとして登録され、エンドポイント属性に関する情報を IOTASSETディクショナリ用にISEに公開します。

前提条件

要件

次の項目に関する基本的な知識が推奨されます。

- ISE
- Cisco Cyber Vision

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco ISEバージョン2.7パッチ1
- Cisco Cyber Visionバージョン3.1.0
- Industrial EthernetスイッチIE-4000-4TC4G-E(s/w 15.2(6)E)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

設定

概要フロー図



このISE導入は、セットアップで使用されます。

Deployment Nodes									
📝 Edit 🔯 Register 🦁 Syncup	2 Deregister								
Hostname	Personas	Role(s)	Services						
ISE27-1ek	Administration, Monitoring, Policy Service, pxGrid	PRI(A), PRI(M)	ALL						
ISE27-2ek	Administration, Monitoring, Policy Service	SEC(A), SEC(M)	SESSION, PROFILER						

ISE 2.7-1ekはプライマリ管理ノード(PAN)ノードおよびpxGridノードです。

ISE 2.7-2ekは、pxGridプローブが有効なポリシーサービスノード(PSN)です。

上記の図に対応する手順を次に示します。

1. pxGridバージョン2経由でISEのassetTopicにCCVが登録されます。CCVからの対応するログ:

注: CCVのpxGridログを確認するには、次のコマンドjournalctl -u pxgrid-agentを発行します。

```
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. pxGridプローブを有効にしたISE PSNは、既存のpxGridアセット(**profiler.log**)を一括ダウンロー ドします。

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", "assetVendor":"XEROX

3.エンドポイントがpxGridプローブを有効にしてPSNに追加され、PSNはpersistイベントを PANに送信して、これらのエンドポイント(**profiler.log**)を保存します。 ISEで作成されたエンドポ イントは、[Context Visibility]の下のエンドポイントの詳細で表示できます。

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.エンドポイントをグループに配置した後、CCVはポート8910経由でSTOPメッセージを送信し 、カスタム属性のグループデータを使用してエンドポイントを更新します。CCVからの対応する

ログ:

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ノードはSTOP更新を受信し、このメッセージをすべての加入者に転送します。これに はpxGridプローブが有効なPSNが含まれます。pxGridノード上の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][]

Distributing stomp frame from=[2b,cv-jens,OPEN], topic=/topic/wildcard,to=[2a,ise-fanout-ise27-lek,OPEN]

6. pxGridプローブが有効なPSNがアセットトピックのサブスクライバである場合、pxGridノード からメッセージを受信し、エンドポイント(**profiler.log**)を更新します。 ISE上の更新されたエンド ポイントは、[Context Visibility]の下のエンドポイントの詳細で表示できます。

2020-06-24 14:40:13,767 DEBUG [Grizzly(2)][] cisco.profiler.infrastructure.probemgr.INDSubscriber -::::-Parsing push notification response: {"opType":"UPDATE","asset":{"assetId":"ce0lade2-eb6f-53c8a646-9661b10c976e", "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: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. pxGridプローブを有効にしたPSNは、新しいポリシーが一致したときにエンドポイントを再プ
ロファイルします(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

```
設定
```

注:assetGroupとContext Visibilityだけを表示したい場合でも、ステップ1 ~ 4が必要です。

1. PSNの1つでpxGridプローブを有効にする

[**Administration**] > [**System] > [Deployment]に移動**し、[ISE node with PSN Persona]を選択します 。[プロファイルの設**定]タブに切**り替えます。pxGridプローブが有効に**なってい**ることを確認しま す。

dent	ity Services Engine	e Home	▶ Context Visibility	 Operations 	Policy	- Administration	▶ Work Centers
▼ System	Identity Managem	ent Network	Resources Device	Portal Management	pxGrid S	Services Feed Se	rvice
Deployment	Licensing • Ce	ertificates + Log	gging I Maintenance	Upgrade Ba	ackup & Res	store Admin Acce	ss > Settings

Deployment	Deployment Nodes List > ISE27-2ek
↓	Edit Node
See	General Settings Profiling Configuration
NAN Failover	□ ► NETFLOW ✓ ► DHCP
	DHCPSPAN
	□ ▶ HTTP
	RADIUS
	▶ Network Scan (NMAP)
	DNS
	SNMPQUERY
	SNMPTRAP
	Active Directory
	V v pxGrid
	Description The PXgrid probe to fetch attributes of MAC or IP-Address as a subscriber from PXGrid Queue

2. ISEでのエンドポイントカスタム属性の設定

[Administration] > [Identity Management] > [Settings] > [Endpoint Custom Attributes]に移動します 。このイメージに従ってカスタム属性(assetGroup)を設定します。CCV 3.1.0はカスタム assetGroupアトリビュートのみ**をサポート**しま**す**。

cisco Ident	ity Services Engine	Home Context	Visibility	▶ Policy	- Administration	Work Centers		
 System 	 Identity Management 	 Network Resources 	Device Portal Management	pxGrid S	ervices Feed Ser	vice		
Identities	Groups External Ider	ntity Sources Identity S	Source Sequences	3				
	6	•						
User Custom	Attributes	Endpoint Cust	tom Attributes					
User Authentication Settings								
Endpoint Purg	le	Endpoint Attr	ibutes (for reference)					
Endpoint Cust	om Attributes	Mandatory	Attribute Name		Data T	уре		
			PostureApplicable		STRING	3		
			LogicalProfile		STRING	3		
			EndPointPolicy		STRING	3		
			AnomalousBehaviour		STRING	3		
			OperatingSystem		STRING			
			BYODRegistration		STRING	3		
			PortalUser		STRING	3		
			LastAUPAcceptanceHours		INT			
		Endpoint Cus	tom Attributes					
			Attribute Name		Туре			
					String	- •		
					Reset	Save		

3.カスタム属性を使用したプロファイラポリシーの構成

[Work Centers] > [Profiler] > [Profiling Policies] に移動します。[Add] をクリックします。次の図に 似たプロファイラポリシーを設定します。このポリシーで使用される条件**式は** CUSTOMATTRIBUTE:assetGroup EQUALS Group1です。

cisco	Identity Service	s Engine	Home	 Context Visibility 	 Operations 	▼ Policy	Administration	▶ Wo	ork Centers			
Polic	y Sets Profiling	Posture	Client Provision	ning	ents							
Pr	ofiling		٩	Profiler Policy List Profiler Policy	> ekorneyc_ASSET	_Group1						
4	• E •		₩ .		•	Name eko	rneyc_ASSET_Group1		Description			7
;	Profiling Policie Logical Profiles	S			Policy En	abled 🔽						 li.
				-,	Minimum Certainty F	actor 20			(Valid Range 1 to 65535)		
					* Exception /	Action	NE	•				
				* Netv	vork Scan (NMAP)	Action NO	NE	*				
				Create an Ide	entity Group for the	policy 💿 ١	es, create matching Ide	entity G	Group			
						0	lo, use existing Identity	Group	hierarchy			
					* Parent I	Policy NO	NE	•				
					* Associated CoA	Type Glo	bal Settings	*				
					System	Type Adm	ninistrator Created					
				Rules								
				If Condition	CUSTOMATTRIBUT	E_assetGro	up_EQUA 💠	Then	Certainty Factor Increases	•	20	- (i)
				Save Reset]							

4.プロファイル適用のカスタム属性の有効化

[Work Centers] > [Profiler] > [Profiling Policies] に移動します。[Add] をクリックします。次の図に 似たプロファイラポリシーを設定します。プロファイル**適用のカスタム属性の有効化が有効にな** っていることを確認します。

cisco	lden	tity Ser	vices E	ngine	Home	e	ibility 🕨 🕨	Operatio	ons	Polic	cy ⊧Ac	dministrat	tion	→ Wor	rk Centers			
► Ne	twork	Access	▶ Gu	est Access	▶ Tru:	stSec + BYOD	▼ Profiler	▶ Pos	sture	Device	e Administr	ation	Passiv	veID				
Overv	view	Ext Id So	ources	Network De	vices	Endpoint Classifica	tion Node	Config	Feeds	▶ Ma	nual Scans	Polic	y Eleme	nts F	Profiling Policie	es P	olicy Se	ts 🕨
				G	Pro	ofiler Configura	tion											
Profile	r Settir	ngs				5												
NMAP	Scan	Subnet E	xclusio	ns					* CoA ⁻	Туре:	Reauth			•				
						Current	custom SNN	/IP comm	nunity str	rings:	•••••				Show			
						Change	custom SNN	/IP comm	nunity str	rings:					(For NMAP,	comn	na sepa	rated.
						Confirm changed	custom SNN	/IP comm	nunity str	rings:					(For NMAP,	comn	na sepa	rated.
							En	dPoint A	ttribute F	Filter:	Enabled	(i)						
						Enable	Anomalous	Behavio	our Dete	ction:	Enabled	(i)						
						Enable Ar	nomalous Be	haviour	Enforcer	ment:	Enabled							
						Enable Custom	Attribute for I	Profiling	Enforcer	ment:	🗸 Enabled							
							Ena	able profi	iling for M	NUD:	Enabled							
						Enable Profi	ler Forwarde	er Persis	tence Qı	ueue:	Enabled							
							Enable F	Probe Da	ta Publis	sher :	Enabled							
					Sa	Reset												

5. pxGridクライアントの自動承認の設定

[Administration] > [pxGrid Services] > [Settings]に移動します。[Automatically approve new certificate-based accounts]を選択し、[Save]をクリックします。この手順により、統合が完了したらCCVを承認する必要がなくなります。

altalta cisco	Identi	ty Services Engi	ine Home	e → Conte	xt Visibility	Operation	s	Policy	▼ Adm	ninistration	→ Wo	ork Centers
▶ Sy	stem	 Identity Manage 	ment Netw	ork Resources	Devic	e Portal Manage	ment	pxGrid S	ervices	Feed Ser	vice	Threat Centric NAC
All C	Clients	Web Clients	Capabilities	Live Log	Settings	Certificates	Perm	nissions				
Р	xGric	l Settings										
	Autor	natically approve ne	ew certificate-ba	sed accounts								
	Allow	password based a	ccount creation									
	Use De	fault Save										

6. CCV証明書のエクスポート

[**Admin**] > [pxGrid]**に移動します**。[Download certificate] をクリックします。この証明書は pxGridの登録時に使用されるため、ISEはこれを信頼する必要があります。



7. CCV ID証明書のISE信頼ストアへのアップロード

[Administration] > [Certificates] > [Certificate Management] > [Trusted Certificates]に移動します。 [インポート]をク**リックします**。[Browse]をクリックし、ステップ5からCCV証明書を選択します 。[Submit]をクリック**します**。

uludu 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						
Deployment Licensing - Certificate	es Logging Maintenance Upgrade Backup & Restore Admin Access Settings						
0							
✓ Certificate Management	Import a new Certificate into the Certificate Store						
System Certificates	* Certificate File Browse center-ca(1).crt						
Trusted Certificates	Friendly Name						
OCSP Client Profile							
Certificate Signing Requests	Trusted For: 👔						
Certificate Periodic Check Setti	✓ Trust for authentication within ISE						
Certificate Authority	Trust for client authentication and Syslog						
	Trust for certificate based admin authentication						
	Trust for authentication of Cisco Services						
	□ Validate Certificate Extensions						
	Description						
	Submit Cancel						

8. CCVの証明書の生成

pxGridの統合とアップデートの際、CCVにはクライアント証明書が必要です。 PxGrid_Certificate_Templateを使用して、ISE内部CAから発行する必要があります。

[Administration] > [pxGrid Services] > [Certificates]に移動します。この図に従ってフィールドに入 力します。ISE CAの目的はID証明書を発行することであるため、[Common Name (CN)]フィール ドは必須です。CCVのホスト名を入力する必要があります。CNフィールドの値は重要です。 CCVのホスト名を確認するには、hostnameコマンドを発行します。[Certificate Download Format]として[PKCS12]を選択します。

root@center:~#						
Identity Services Engine Hor	ne Context Visibility	 Operations 	► Policy - Adm	ninistration	Work Centers	
System Identity Management Net	work Resources	e Portal Management	pxGrid Services	Feed Service	e Fhreat Centric NAC	
All Clients Web Clients Capabilities	Live Log Settings	Certificates Pern	nissions			
Generate pxGrid Certificates						
I want to *	Generate a single certific	cate (without a certificat	e signing request)			•
Common Name (CN) *	center					
Description						
Certificate Template	pxGrid_Certificate_Templat	e 6				
Subject Alternative Name (SAN)	•		- +			
Certificate Download Format *	PKCS12 format (includin	g certificate chain; one	file for both the certi	ificate chain and l	key)	- 0
Certificate Password *	••••••					0
Confirm Password *	•••••					
					Reset Crea	te

9. PKCS12形式での証明書チェーンのダウンロード

PKCS12形式で証明書をインストールすると、CCV ID証明書ISE内部CAチェーンとともにCCVに インストールされ、pxGrid通信がISEから開始されたときにCCVがISEを信頼します(pxGridキー プアライブメッセージなど)。



10. CCVでのISE統合の詳細の設定

[Admin] > [pxGrid]**に移動します**。ノード名を設定します。この名前は、[Administration] > [pxGrid Services] > [Web Clients]で[Client Name]としてISEに表示されま**す。**ISE pxGridノードの**ホスト** 名とIPアドレスを設定します。CCVがISE FQDNを解決できることを確認します。

uluulu cisco	CYBER VISION			<u>₩</u> ® ~				
۲		🖽 System	Filling and submitting the fields below activates the sharing of can then be leveraged by upstream security systems to monitor	Illing and submitting the fields below activates the sharing of endpoint assets discovered by this system with a Cisco Identity Services Engine (ISE) pxGrid controller. This information an then be leveraged by upstream security systems to monitor security, detect threats, and set network policy. Learn morehere.				
Ð		E Data management						
Ē		🛛 Sensors 🗸 👻	© You must download the CA Center to upload it in ISE.	Center Certificate Authority) You must download the CA Center to upload it in ISE.				
C		冬 Users 🗸 🗸	DOWNLOAD CERTIFICATE					
Q		⊲ Events						
۲		o ^g API	ISE Server					
		₩ License	⊘ The connection is active					
		冬 LDAP Settings	Update the configuration	Client certificate				
		PxGrid	Node Name: Name of the pxGrid Node to be created on ISE pxGrid Server cv-iens	A certificate has been imported				
		☑ SNORT						
		🗠 Integrations 👻	Hostname: Hostname of the ISE pxGrid Server					
		88 Extensions	ISE27-1ek.example.com					
			IP Address: IP address of the ISE pxGrid Server					
			10.48.17.86					
			Delete					

11. CCVへの証明書チェーンのアップロードと統合の開始

[**Admin**] > [pxGrid]**に移動します**。[Change Certificate]をクリ**ックします**。ステップ8 ~ 9からISE CAによって発行された証明書を選択します。ステップ8のパスワードを入力し、[**OK**]をクリック します。

Do you want to enter a password?					
•••••					
	Ok	Cancel			

[Update]をクリックします。これにより、実際のCCV - ISE統合がトリガーされます。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

CCV統合の検証

統合が完了したら、[Admin] > [pxGrid]の順に選択して、統合が正常に完了したことを確認**できま** す。ISEサーバの下に「The connection is active」というメッセージが表示されます。

cisco	CYBER VISION		
۲	Explore	I System	Platform Exchange Grid
ß	Reports	Data management	Cisco Platform Exchange Grid (pxGrid) is an open, scalable d asset management systems.
	Events	□ Sensors ✓	Filling and submitting the fields below activates the sharing then be leveraged by upstream security systems to monitor
C	Monitor	糸 Users 🗸	
۵	Search	⊲ Events	 You must download the CA Center to upload it in ISE.
	Admin	o [⊄] API	LOWNLOAD CERTIFICATE
		₩ License	
		条 LDAP Settings	ISE Server
		PxGrid	⊘ The connection is active

ISE統合の検証

[Administration] > [pxGrid Services] > [Web Clients]に移動します。CCVクライアント(cv-jens)の ステータスがONであることを確認します。

注: CCV pxGridクライアントのステータスは、[すべてのクライアント(All Clients)]メニュー で[オフライン(Offline)]と表示されます。これは、pxGrid v1のステータスだけが表示される ためです。

cisco	Identi	ty Services Engin	ie Home	F Con	text Visibility	 Operations 	Policy	- Administration	Work Cer	nters				
▶ Sy	stem	 Identity Manager 	nent I Netwo	ork Resourc	es Device	e Portal Manageme	ent pxGrid Ser	vices Feed Se	rvice + Thr	eat Centric NAC				Click
All C	Clients	Web Clients	Capabilities	Live Log	Settings	Certificates P	Permissions						2	
C F	Refresh												Rows/Page	25
	Client	t Name	Connect To	S	ession Id	С	ertificate	Subscripti	ons	Publications	IP Address	Status	Start time	Duratio
×	Clien	t Name		•							IP Address	•	·	
	ise-far	nout-ise27-1ek	ISE27-1ek	IS	E27-1ek:15	C	N=ISE27-1ek.e	. /topic/distrib	uted	/topic/distributed	10.48.17.86	ON	2020-06-24 09:56:50 UTC	00:04:37:18
	ise-bri	dge-ise27-1ek	ISE27-1ek	IS	E27-1ek:23	C	N=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-mr	nt-ise27-2ek	ISE27-1ek	IS	E27-1ek:24	N	o Certificate	/topic/com.c	isco.ise.se	/topic/com.cisco.ise.se	10.48.17.88	ON	2020-06-24 10:18:25 UTC	00:04:15:43
	ise-ad	min-ise27-2ek	ISE27-1ek	IS	E27-1ek:25	N	o Certificate	/topic/com.c	sisco.endpo		10.48.17.88	ON	2020-06-24 10:18:26 UTC	00:04:15:43
	ise-ad	min-ise27-1ek	ISE27-1ek	IS	E27-1ek:34	С	N=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-far	nout-ise27-1ek	ISE27-1ek	IS	E27-1ek:37	C	N=ISE27-1ek.e	. /topic/wildca	ard		127.0.0.1	OFF 🕖	2020-06-24 13:02:51 UTC	00:01:08:00
	cv-jen	s	ISE27-1ek	IS	E27-1ek:38	C	N=center				10.48.43.241	ON	2020-06-24 13:39:12 UTC	00:00:54:56
	ise-mr	nt-ise27-1ek	ISE27-1ek	IS	E27-1ek:39	C	N=ISE27-1ek.e	. /topic/com.o	isco.ise.se		10.48.17.86	ON	2020-06-24 13:53:51 UTC	00:00:40:17
	ise-far	nout-ise27-1ek	ISE27-1ek	IS	E27-1ek:40	C	N=ISE27-1ek.e	. /topic/wildca	ard		127.0.0.1	OFF 🕖	2020-06-24 14:11:51 UTC	00:00:18:00
	ise-ad	min-ise27-1ek	ISE27-1ek	IS	E27-1ek:41	C	N=ISE27-1ek.e				10.48.17.86	ON	2020-06-24 14:29:51 UTC	00:00:04:17
	ise-far	nout-ise27-1ek	ISE27-1ek	IS	E27-1ek:42	C	N=ISE27-1ek.e	. /topic/wildca	ard		127.0.0.1	ON	2020-06-24 14:30:51 UTC	00:00:03:17

注: <u>CSCvt78208</u>により、/topic/com.cisco.ise.endpoint.assetを持つCCVがすぐに表示され ないため、最初の公開時にのみ表示されます。

CCVグループの変更の確認

[探索] > [すべての**データ] > [コンポーネントリスト]に移動します**。いずれかのコンポーネントを クリック**し**、グループに追加します。

uluilu cisco	CYBER VISION				⊭ 8.√							
Ø		⊐ © ₿ ₫ ∠ †	Jun 24, 2020 3:36:22 PM - Jun 2	24, 2020 4:36:22 Pl	d (1 hr) •LIVE				< Component			
Ē	Reports Events	All data 🛞	5 Components						Cisco a0:3a:59 IP:- MAC: 00:f2:8b:a0:3	Add to group		
¢	Monitor	Description:	Component 💠 🛛 🐨	Group	First activity $\ \ \diamondsuit$	Last activity 🝦	IP ‡	M/	First activity	Group1		
Q	Search	All components and activities are listed in this preset. This preset should not be used and other more well defined presets would be preferred for more	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:	Tags: Rotags			
ø	Admin	accurate indings. Active baseline: No active baseline	01:00:0c:00:00:00		May 11, 2020 6:44:15 PM	Jun 24, 2020 4:27:19 PM		01:	Properties: vendor-name: Cisco a0	Broadcast sco Systems, Inc :3a:59		
		Criteria Select all Reject all Default	🖾 01:00:0c:cc:cc:cc		Mar 13, 2020 1:52:23 PM	Jun 24, 2020 4:27:19 PM		01:	mac:00:f2:8b:	a0:3a:59		
		© COMPONENT TAGS ~ ~ ACTIVITY TAGS ~ □ GROUPS ~	a a 255.255.255.255		Mar 13, 2020 1:52:09 PM	Jun 24, 2020 4:25:45 PM	255.255.255.255	ff:f				
		□ SENSORS V	Cisco a0:3a:59		Jun 24, 2020 2:47:34 PM	Jun 24, 2020 4:25:45 PM	•	00:				
									C 1 Flow	i 3 Events O - Credential		
	<	<										

/topic/com.cisco.ise.endpoint.assetがCCVに対するパブリケーションとしてリストされていること を確認します。

cisco	Identit	ty Services Eng	jine Hom	e Context Visibility Operations Policy Administration Work Centers										
► Sy	/stem	Identity Manag	ement	vork Reso	urces	ce Portal Manager	ment pxGrid Se	Feed Se	ervice + Thr	eat Centric NAC				Click here to do wire
All	Clients	Web Clients	Capabilities	Live Lo	g Settings	Certificates	Permissions							
													Rows/Page 25	• 1 0
CI	Refresh													
	Client	t Namo	Connect T		Section Id		Cortificato	Subscripti	long	Publications	ID Address	Statue	Start time	Duratio
	Cilent	LINAIIIE	Connect is		3635101110		Certificate	Subscript	10115	Fublications	IF Address	Status	Start time	Duratio
×	Client	t Name		•							IP Address	-		
	ise-far	nout-ise27-1ek	ISE27-1ek		ISE27-1ek:15		CN=ISE27-1ek.e.	/topic/distrit	buted	/topic/distributed	10.48.17.86	OFF 🕖	2020-06-24 09:56:50 UT	C 00:04:57:00
	ise-bri	idge-ise27-1ek	ISE27-1ek		ISE27-1ek:23		CN=ISE27-1ek.e.			/topic/com.cisco.ise.config.profiler	127.0.0.1	ON	2020-06-24 10:06:52 UT	C 00:05:03:05
	ise-mr	nt-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 UT	C 00:04:42:00
	ise-ad	lmin-ise27-2ek	ISE27-1ek		ISE27-1ek:25		No Certificate	/topic/com.	cisco.endpo		10.48.17.88	ON	2020-06-24 10:18:26 UT	C 00:04:51:31
	ise-mr	nt-ise27-1ek	ISE27-1ek		ISE27-1ek:39		CN=ISE27-1ek.e.	/topic/com.	cisco.ise.se		10.48.17.86	OFF 🕖	2020-06-24 13:53:51 UT	C 00:00:58:00
	ise-ad	lmin-ise27-1ek	ISE27-1ek		ISE27-1ek:41		CN=ISE27-1ek.e.			/topic/com.cisco.ise.endpoint	10.48.17.86	ON	2020-06-24 14:29:51 UT	C 00:00:40:06
	ise-far	nout-ise27-1ek	ISE27-1ek		ISE27-1ek:42		CN=ISE27-1ek.e.	/topic/wildc	ard		127.0.0.1	OFF 🕖	2020-06-24 14:30:51 UT	C 00:00:14:00
	cv-jen:	s	ISE27-1ek		ISE27-1ek:43		CN=center			/topic/com.cisco.endpoint.asset	10.48.43.241	ON	2020-06-24 14:38:47 UT	C 00:00:31:10
	ise-far	nout-ise27-1ek	ISE27-1ek		ISE27-1ek:44		CN=ISE27-1ek.e.	/topic/wildc	ard		127.0.0.1	OFF 🕖	2020-06-24 14:45:52 UT	C 00:00:11:00
	ise-mr	nt-ise27-1ek	ISE27-1ek		ISE27-1ek:45		CN=ISE27-1ek.e.	/topic/com.	cisco.ise.se		10.48.17.86	OFF 🕖	2020-06-24 14:52:51 UT	C 00:00:17:00
	ise-far	nout-ise27-1ek	ISE27-1ek		ISE27-1ek:46		CN=ISE27-1ek.e.	/topic/distrit	buted	/topic/distributed	10.48.17.86	OFF 🕖	2020-06-24 14:53:53 UT	C 00:00:02:00
	ise-far	nout-ise27-1ek	ISE27-1ek		ISE27-1ek:47		CN=ISE27-1ek.e.	/topic/distrit	buted	/topic/distributed	10.48.17.86	ON	2020-06-24 14:55:53 UT	C 00:00:14:03
	ise-far	nout-ise27-1ek	ISE27-1ek		ISE27-1ek:48		CN=ISE27-1ek.e.	/topic/wildc	ard		127.0.0.1	ON	2020-06-24 14:57:52 UT	C 00:00:12:05
	ise-mr	nt-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 UT	C 00:00:08:31

CCVを介して割り当てられたGroup1がISEに反映され、[Context Visibility] > [Endpoints]に移動し てプロファイリングポリシーが有効になったこ**とを確認します**。前の手順で更新したエンドポイ ントを選択します。[Attributes]タブに切り替えます。カスタム属性セクションには、新しく設定 されたグループが反映されている必要があります。

dentity Services Engine Home						- Context Visibility	 Operation 	ons Policy	Administration	► Work 0	Centers
Endp	oints	Users	Network	Contraction Contractico Con	Applic	ation					
Filters:	: ×00										
Endp	points										
00):F2:										
Ç	 	MA Use Enc Cui Loc									
	A	pplication	s	Attributes	,	Authentication	Threats	Vulnerabilities			
Ge	neral /	Attributes									
De	scriptic	'n									
Sta	atic Ass	ignment		false							
End	dpoint	Policy		ekorneyc	ASSET_	_Group1					
Sta	atic Gro	oup Assign	nment	false							
Ide	entity G	roup Assig	gnment	ekorneyc_	ASSET_	_Group1					
Cu	stom /	Attributes	i								
									T	Filter -	\$ -
		Attribute	String			Attribute V	alue				
	×	Attribute	String			Attribute Va	lue				
		assetGrou	up			Group1					

その他のアトリビュート(Attributes)セクションには、CCVから受信した他のすべてのアセットア トリビュートがリストされます。

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

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

ISEでのデバッグの有効化

ISEでデバッグを有効にするには、[Administration] > [System] > [Logging] > [Debug Log Configuration]**に移動します**。ログレベルを次のように設定します。

ペルソナ PAN(オプション)	コンポーネント名 プロファイラ	ログ レベル デバッグ	チェックするファイ. profiler.log
pxGridプローブが有効な PSN	プロファイラ	デバッグ	profiler.log
pxGrid	pxgrid	トレース	pxgrid-server.log

CCVでのデバッグの有効化

CCVでデバッグを有効にするには、次の手順を実行します。

- touch /data/etc/sbs/pxgrid-agent.confコマンドを使用して、ファイル/data/etc/sbs/pxgridagent.confを作成します
- この内容をpxgrid-agent.confファイルに貼り付けるには、vi /data/etc/sbs/pxgrid-agent.confコ マンドでviエディタを使用します

/data/etc/sbs/pxgrid-agent.conf
base:

loglevel: debug

- systemctl restart pxgrid-agentコマンドを実行して、pxgrid-agentを再起動します
- journalctl -u pxgrid-agentコマンドを使用してログを表示する

ー括ダウンロードの失敗

CCVは、統合時に一括ダウンロードURLをISEに公開します。pxGridプローブが有効なISE PSNは、このURLを使用して一括ダウンロードを実行します。次の点を確認します。

- URLのホスト名は、ISEの観点から正しく解決できます
- ・ポート8910のPSNからCCVへの通信が許可される

pxGridプローブが有効になっているPSNの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}]] <u>CSCvt75422</u>が原因で一括ダウンロードが失敗する場合があり、ISEのprofiler.logにこのエラーが 表示され、確認できます。この不具合はCCV 3.1.0で修正されています。

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)

すべてのエンドポイントがISEで作成されるわけではありません

CCV上の一部のエンドポイントにアタッチされている属性が多すぎるため、ISEデータベースで は処理できません。ISEのprofiler.logに次のエラーが表示される**場合に確認**できます。

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がISEで使用できない

AssetGroupがISEで使用できない場合、ほとんどの場合、プロファイルポリシーはカスタム属性 を使用して設定されていません(ドキュメントの「設定」の部分のステップ2 ~ 4を参照)。 コ ンテキストの可視性の場合でも、グループ属性、プロファイリングポリシー、およびその他の設 定をステップ2 ~ 4で表示する必要があります。

エンドポイントグループの更新がISEに反映されない

CSCvu80175<u>が原因で</u>は、統合の直後にCCVがリブートするまで、CCVはエンドポイントのアッ プデートをISEに公開しません。統合が完了したら、CCVをリブートできます。

CCVからグループを削除してもISEからグループを削除できない

この問題は、CCV <u>CSCvu47880</u>の既知の不具合が原因で発生します。予期された形式と異なる CCVからのグループの削除時にpxGridアップデートが送信されるため、グループは削除されませ ん。

WebクライアントからのCCVドロップ

この問題は、ISE <u>CSCvu47880</u>の既知の不具合で、クライアントがOFF状態に移行した後、 Webクライアントから完全に削除された場合に発生します。この問題は、ISEの2.6パッチ7およ び2.7パッチ2で解決されています。

ISEのpxgrid-server.logに次のエラーが表示された場合は、このエラーを確認できます。

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]]

CCV TrustSecによるISE統合の使用例

この設定は、TrustSecが導入されている場合に、ISEとCCVの統合がエンドツーエンドのセキュ リティにどのように役立つかを示します。これは、統合が完了した後の統合方法の例の1つにすぎ ません。

注:TrustSecスイッチの設定の説明は、この記事の範囲外ですが、付録で確認できます。

トポロジとフロー

Manufacturing Device	IE Switch	Cisco Cyb	per Vision	ISE
** *				
	Authentication/Authorization	on. SGT is assigned from ISE	based on the CCV Group dat	a
	2	Administrator changes the	Group of endpoint on CCV	
		3	New Group information is pxGrid	sent to ISE via
		4 Bas	ed on new attributes ISE char	iges the profile of the endpoint
	5 -	CoA is triggered	to change authorization cont	ext
6	Authentication/Authorization	n. New SGT is assigned from	n ISE based on new CCV Gro	up data

設定

1. ISEでのスケーラブルグループタグの設定

前述の使用例を達成するために、TrustSecタグのIOT_Group1_AssetおよびIOT_Group2_Assetは 、それぞれGroup1 CCVアセットをGroup2と区別するように手動で設定されています。[ワークセ ン**ター] > [TrustSec] > [コンポーネント] > [セキュリティグループ]に移動します**。[Add] をクリッ クします。図に示すように、SGTに名前を付けます。

dentity Services Engine	Home	y ► Operations ► Polic	cy Administration	Nork Centers	
Network Access Guest Access	TrustSec → BYOD →	Profiler + Posture + Devic	e Administration Passivel)	
♦ Overview	Sec Policy Policy Sets	SXP Troubleshoot Rep	oorts		
0					
Security Groups	Security Groups	Iministration > System > Backur	& Restore > Policy Export Pag		
IP SGT Static Mapping	For Folicy Export go to A	aministration > System > Dackup	a Residie - Folicy Export Fag	e	
Security Group ACLs					
Network Devices	🖸 Edit 🕂 Add	🛎 Import 🛛 💆 Export 🗸	Trash 🔹 🕒 Push	Verify Deploy	
Trustsec Servers	Icon Nam	e 🗜	SGT (Dec / Hex)	Description	Learned from
	Auc	litors	9/0009	Auditor Security Group	
	D 🌐 BY	DC	15/000F	BYOD Security Group	
	Cor	ntractors	5/0005	Contractor Security Group	
		velopers	8/0008	Developer Security Group	
		velopment_Servers	12/000C	Development Servers Security Group	
	🗆 🌐 Em	ployees	4/0004	Employee Security Group	
	Gue Gue	ests	6/0006	Guest Security Group	
	тоі 😌 🗆	_Group1_Asset	16/0010		
	го 😌 пот	_Group2_Asset	17/0011		

2.グループ2のカスタム属性を使用したプロファイラポリシーの設定

注:グループ1のプロファイル設定は、ドキュメントの最初の部分のステップ3で行いまし

[Work Centers] > [Profiler] > [Profiling Policies] に移動します。[Add] をクリックします。次の図に 似たプロファイラポリシーを設定します。このポリシーで使用される条件**式は** CUSTOMATTRIBUTE:assetGroup EQUALS Group2です。

dentity Services Engine	Home • C	Context Visibility	Operations	➡ Policy	Administration	Work Centers			
Policy Sets Profiling Posture	Client Provisioning	Policy Element	nts						
Profiling ↓ III ↓ Profiling Policies ↓ Profiling Policies ↓ Digical Profiles	(م ∰∙	Profiler Policy List > Profiler Policy * M * Netwo Create an Ider	• ekorneyc_ASSET_(• Ni Policy Enai inimum Certainty Fa • Exception Ac ork Scan (NMAP) Ac ork Scan (NMAP) Ac ortity Group for the po • Parent Po • Parent Po • Associated CoA T System T	Group2 ame ekor bled 2 actor 20 Ction NON Ction NON Olicy Y NN NON VON Type Glob	Theyc ASSET Group2	Description (Valid Range 1 to 6553) (Valid Range 1 to 6553) r r r r r r r r r r r r r r r r r r r	5)		11.
		Rules							
		If Condition CL	USTOMATTRIBUTE	assetGrou	ıp_EQUA ⊕ ↔	Then Certainty Factor Increases	~	20	
		Save Reset							

3. ISE上のエンドポイントIDグループに基づいてSGTを割り当てる認可ポリシーの設定

[Policy] > [Policy Sets]に移動します。ポリシーセットを選択し、このイメージに従って認可ポリ シーを設定します。その結果、ステップ1.で設定したSGTが割り当てられることに注意してくだ さい。

ルール名	条件	プロファイル	セキュリティグルー
CCVグループ1ポリシー	IdentityGroup・Name EQUALSエンドポイント IDグループ:プロファイル :ekorneyc_ASSET_Grou p1	PermitAccess	IOT_Group1_Asset
CCVグループ2ポリシー	IdentityGroup・Name EQUALSエンドポイント IDグループ:プロファイル :ekorneyc_ASSET_Grou p2	PermitAccess	IOT_Group2_Asset

este Ide	ntity Servi	ces Engine Home	 Context 	Visibility + Operations •	Policy Administration	Work Centers													ા લ	0 0 0	
Policy Sel	ts Profile	g Posture Client Provisi	ioning +	Policy Elements														lick here to do wire	less setup Do r	ot show this again.	
Policy S	iets → D	efault												Reset Policyset Hitcounts Reset Sa							
	Status	Policy Set Name		Description	Conditions												Allow	ed Protocols / Se	erver Sequen	e Hits	
Search																					
	ø	Default		Default policy set													Defi	suit Network Access	×* •	P 10	
> Authe	intication I	Policy (3)																			
> Autho	vrization P	alicy - Local Exceptions																			
> Autho	vization P	olicy - Global Exceptions																			
M Autho	vization P	alicy.(18)																			
														Results							
٠	Status	Rule Name		Conditions										Profiles			Security Groups		Hits	Actions	
Search																					
	ø	CCV Group 1 Policy		4 identityGroup-Name EQ	UALS Endpoint Identity Groups	s:Profiled:ekorneyc_ASS	SET_Group1							× PermitAcc	ess	+	IOT_Group1_Asset	x = +		٥	
	Ø	CCV Group 2 Policy		a identityGroup-Name EQ	UALS Endpoint Identity Groups	s:Profiled:ekorneyc_ASSi	SET_Group2							× PermitAcc	ess	+	IOT_Group2_Asset	×* +	1	٥	



ここでは、設定が正常に機能しているかどうかを確認します。

1. CCVグループ1に基づいてエンドポイントを認証

スイッチでは、環境データにSGTの16-54:IOT_Group1_Assetと17-54:IOT_Group2_Assetの両方 が含まれていることがわかります。

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# エンドポイントが認証され、その結果、CCV Group 1 Policyが一致し、SGT IOT_Group1_Assetが割り当てられます。

cisco Iden	ntity Services Engine H	ome	sibility • Operation	ons Policy	Administration	Work Centers								
	Threat-Centric NAC Live Log	s + TACACS + Tr	roubleshoot + Ada	aptive Network C	ontrol Reports									
Live Logs	Live Sessions													
		Mis	sconfigured Supplic	ants O		Misconfigured Network De	vices O	RADI	US Drops	Client Stopped Respo	Client Stopped Responding ()			
			1			0			0	0				
C Refrest	h O Reset Repeat Counts	Export To 👻												
Tim	e	Status	Details	Repeat C	Identity	Endpoint ID	Endpoint Profile	Authentication Pol	Authorization Policy	Authorization Profiles	IP Address			
×			•			00f2.8ba0.3a59	×				IP Address	٠		
Jun	Jun 25, 2020 10:37:32.590 AM 😑 🙍 0 00:F2:8B:A0:3A:59		00:F2:8B:A0:3A:59	00:F2:8B:A0:3A:59 ekomeyc_ASSET		Group1 Default >> MAB Default >> CCV Group 1 Policy		IOT_Group1_Asset,PermitAccess	172.16.0.100					
hun	Jun 25, 2020 10:37:31 567 AM			00-52-88-40-24-59	00-52-98-40-24-59	ekomeus ASSET Genunt	T Group1 Default to MAR Default to CPU Group 1 Policy IOT Group1 Asset Permitheoase			172 16 0 100				

スイッチ**のshow authentication sessions interface fa1/7 detailは、**Access-Acceptデータが正常に 適用されたことを確認します。

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: 0x0000010 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.管理者によるグループの変更

[検索]にナビゲー**トします**。エンドポイントのMACアドレスを貼り付け、クリックし**てグ**ループ 2に追加します。

注:CCVでは、グループを1回で1から2に変更することはできません。したがって、まずグ ループからエンドポイントを削除し、次にグループ2を割り当てる必要があります。

uluulu cisco	CYBER VISION				Q Search 🔻		
0	Explore Reports Events	Q 2 resu	Component	Cisco a0:3a:59 First activity Tags IP Jun 24, 2020 2:47:34 PM ₩ No tags MAC: 00:12:8b:a0:3a:59 Last activity Activity tags	Broadcast		
C	Monitor	Сог		Image: Create a new group Image: Create a new group			
۹		ata	Properties	Tags Croup2			
\$	Admin	CISK	Prope	rties			
		ates	vendor-na	vendor: Cisco Systems, Inc			
		CIS	name: Cis	name-mac: Cisco a0:3a:59			
			mac: 00: f				
			Tags				
			No tags	No tags found			

3-6.エンドポイントグループ変更のCCVへの影響

手順4.、5.、および6.はこのイメージに反映されます。プロファイリングにより、エンドポイント は手順4で確認したアイデンティティグループをekorneyc_ASSET_Group2に変更しました。これ により、ISEはスイッチにCoAを送信し(手順5)、最後にエンドポイントの再認証を行いました (手順6)。

alata Istant	b. Contone England																	
cisco identi	ky Services Engine	Home Con	text Visibility	Operations	Policy Administr	ston	 Work Centers 											
*1040105	Inneat-Centric NAC Live L	Logs FIAUAUS	+ Iroubleshoo	K Mospove N	versionik Control Preports													Clic
Live Logs	Live Sessions																	
		Misconfigured Supplicants O						Misconfigured Network Devices O			RADIUS Drops ()	Client Stopped Responding ()				Repeat Counter (9		
	1				0			0			0				0			
	1				0				0		0							
															c Chan Latert			
																	Hereford 11010	. Daren conse
S Refresh 🗢 Reserva Counts 🕹 Expon To -																		
Time		Status	Details	Repeat	Identity		Endpoint ID		Endpoint Profile	Authentication Pol	Authorization Policy		Authorization Profiles	IP Address		Network Device	Device Port	Identity Group
×			•				00f2.8ba0.3a59	×						IP Address	*			
Jun 2	5, 2020 10:43:00.411 AM	0	0	0	00:F2:88:A0:3A:59		00:F2:88:A0:3A:59		ekomeyc_ASSET_Group2	Default >> MAB	Default >> CCV Group 2 Policy		IOT_Group2_Asset,PermitAccess	172.16.0.100			FastEthernet1/7	4
Jun 2	5, 2020 10:42:59.503 AM	2	0	6	00:F2:88:A0:3A:59		00:F2:88:A0:3A:59		ekorneyc_ASSET_Group2	Default >> MAB	Default >> CCV Group 2 Policy		IOT_Group2_Asset,PermitAccess	172.16.0.100		IE-4000	FastEthernet1/7	ekomeyc_ASSET_Group2
Jun 2	5, 2020 10:42:59.482 AM	1	à			5	00.F2:88:A0:3A:59									IE-4000	FastEthernet1/7	
Jun 2	5, 2020 10:37:31.567 AM	2			00:F2:88:A0:3A:59		00:F2:88:A0:3A:59		ekomeyc_ASSET_Group1	Default >> MAB	Default >> CCV Group 1 Policy		IOT_Group1_Asset,PermitAccess	172.16.0.100		IE-4000	FastEthernet1/7	ekomeyc_ASSET_Group1

スイッチ**のshow authentication sessions interface fa1/7 detailは、新しいSGTが割り当て**られてい ることを確認します。

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: 0x0000010 Handle: 0x58000003 Current Policy: POLICY_Fa1/7

Security Policy: Should Secure Security Status: Link Unsecure

Server Policies: SGT Value: 17

Method status list: Method State

mab Authc Success

KJK_IE4000_10#



スイッチTrustSec関連の設定

注: Ctsクレデンシャルはrunning-configの一部ではなく、特権EXECモードでcts credentials id <id> password <password>コマンドを使用して設定する必要があります。

```
aaa new-model
aaa group server radius ISE
server name ISE-1
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
1
dot1x system-auth-control
!
aaa server radius dynamic-author
client 10.48.17.86
server-key cisco
aaa session-id common
1
cts authorization list ISE
cts role-based enforcement
1
interface FastEthernet1/7
description --- ekorneyc TEST machine ---
switchport access vlan 10
switchport mode access
authentication port-control auto
mab
1
radius server ISE-1
address ipv4 10.48.17.86 auth-port 1645 acct-port 1646
pac key cisco
1
end
KJK_IE4000_10#
```