配置裝置感測器以進行ISE分析

目錄

簡介

本文檔介紹如何配置裝置感測器，以便在ISE上用於分析目的。

必要條件

需求

思科建議您瞭解以下主題：

- Radius通訊協定
- 思科發現協定(CDP)、鏈路層發現協定(LLDP)和動態主機配置協定(DHCP)
- 思科身分辨識服務引擎(ISE)
- Cisco Catalyst交換器2960

採用元件

本文中的資訊係根據以下軟體和硬體版本：

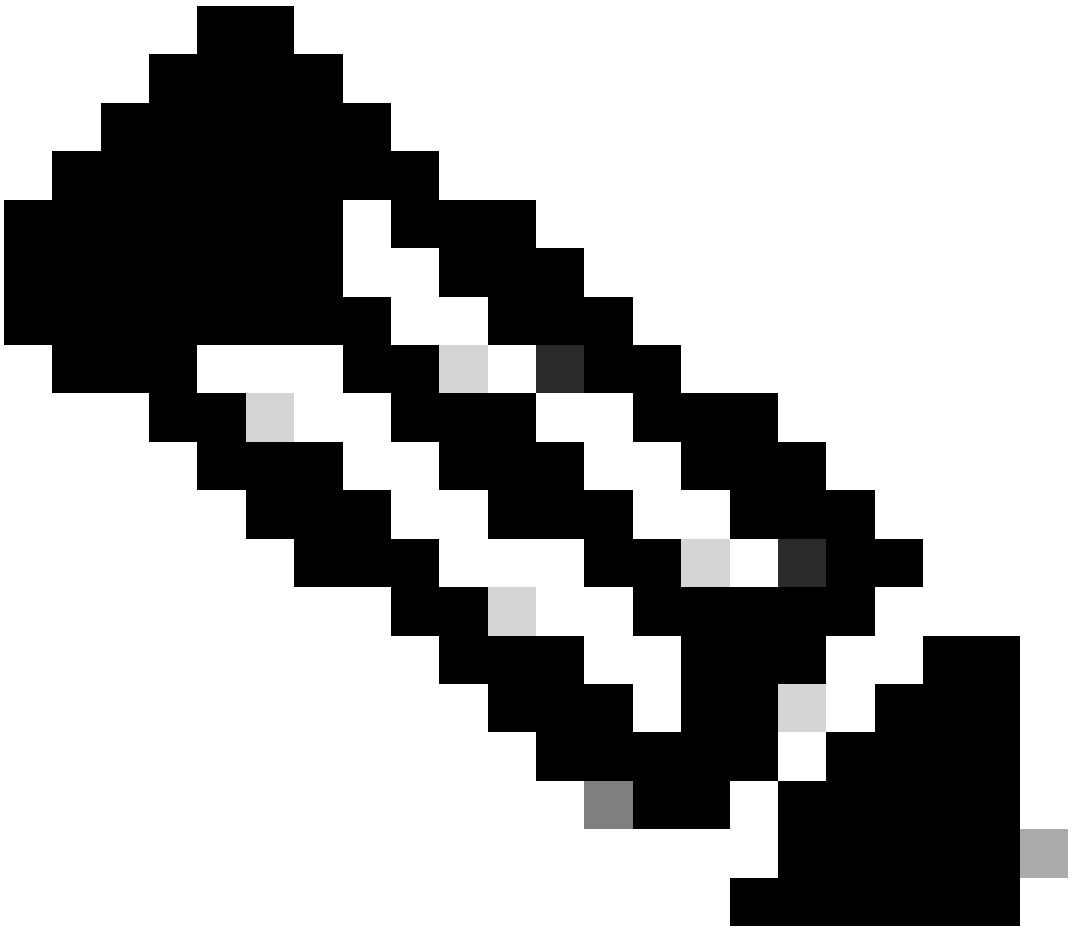
- Cisco ISE版本1.3修補3
- Cisco Catalyst交換器2960s版本15.2(2a)E1
- Cisco IP電話8941版本SCCP 9-3-4-17

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

裝置感測器是訪問裝置的一項功能。它允許收集有關已連線終端的資訊。大多數情況下，裝置感測器收集的資訊可能來自以下協定：

- CDP
- LLDP
- DHCP



注意：在某些平台上，還可以使用H323、會話初始協定(SIP)、組播域解析(MDNS)或HTTP協定。裝置感測器功能的配置可能因協定而異。示例在裝有03.07.02.E軟體的Cisco Catalyst 3850上提供。

收集資訊後，即可將其封裝在radius計量中並傳送到效能分析伺服器。在本文中，ISE用作分析伺服器。

設定

步驟 1.標準AAA配置

要配置身份驗證、授權和記帳(AAA)，請參閱以下步驟：

1. 使用aaa new-model命令啟用AAA，並在交換機上全局啟用802.1X。

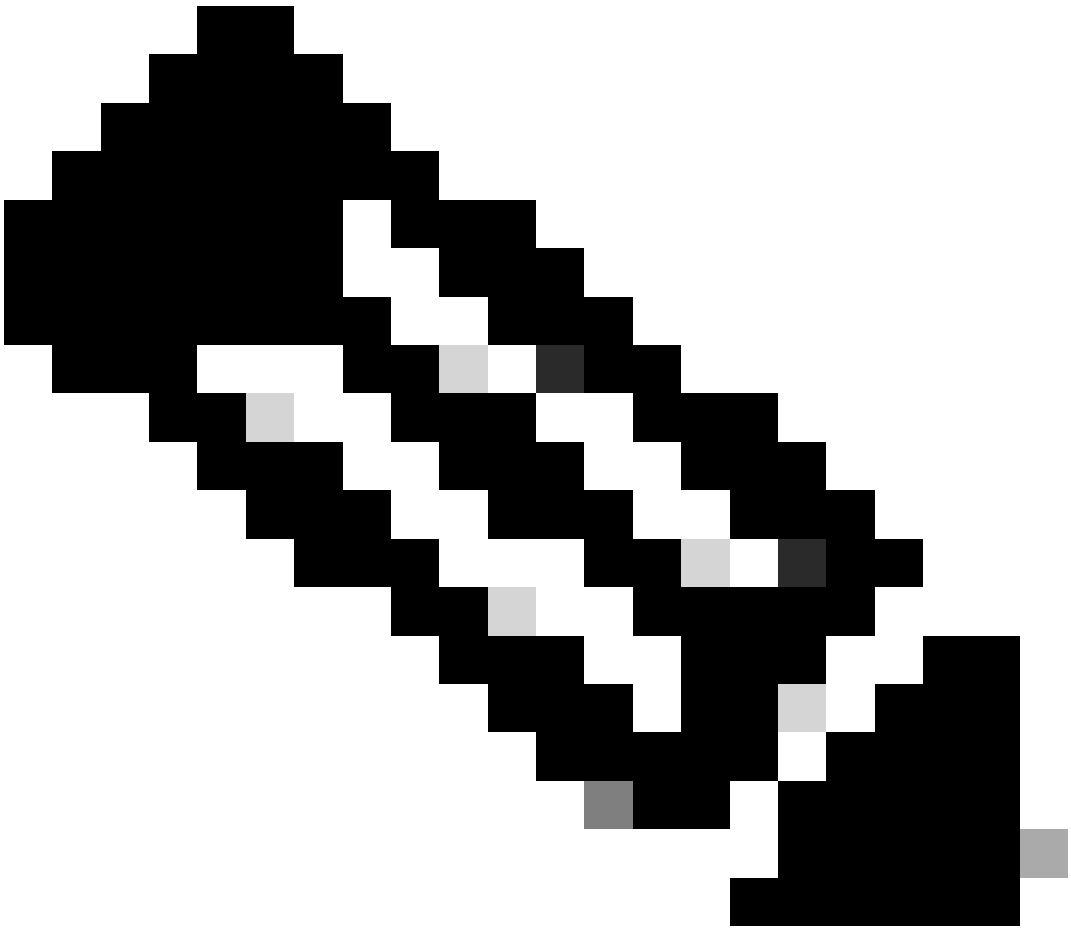
2. 配置Radius伺服器並啟用動態授權（授權更改- CoA）。

3. 啟用CDP和LLDP協定。

4. 增加交換機埠身份驗證配置

```
!
aaa new-model
!
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting update newinfo
aaa accounting dot1x default start-stop group radius
!
aaa server radius dynamic-author
 client 1.1.1.1 server-key xyz
!
dot1x system-auth-control
!
lldp run
cdp run
!
interface GigabitEthernet1/0/13
 description IP_Phone_8941_connected
 switchport mode access
 switchport voice vlan 101
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 2
 spanning-tree portfast
```

```
end
!
radius-server host 1.1.1.1 auth-port 1812 acct-port 1813 key xyz
!
```



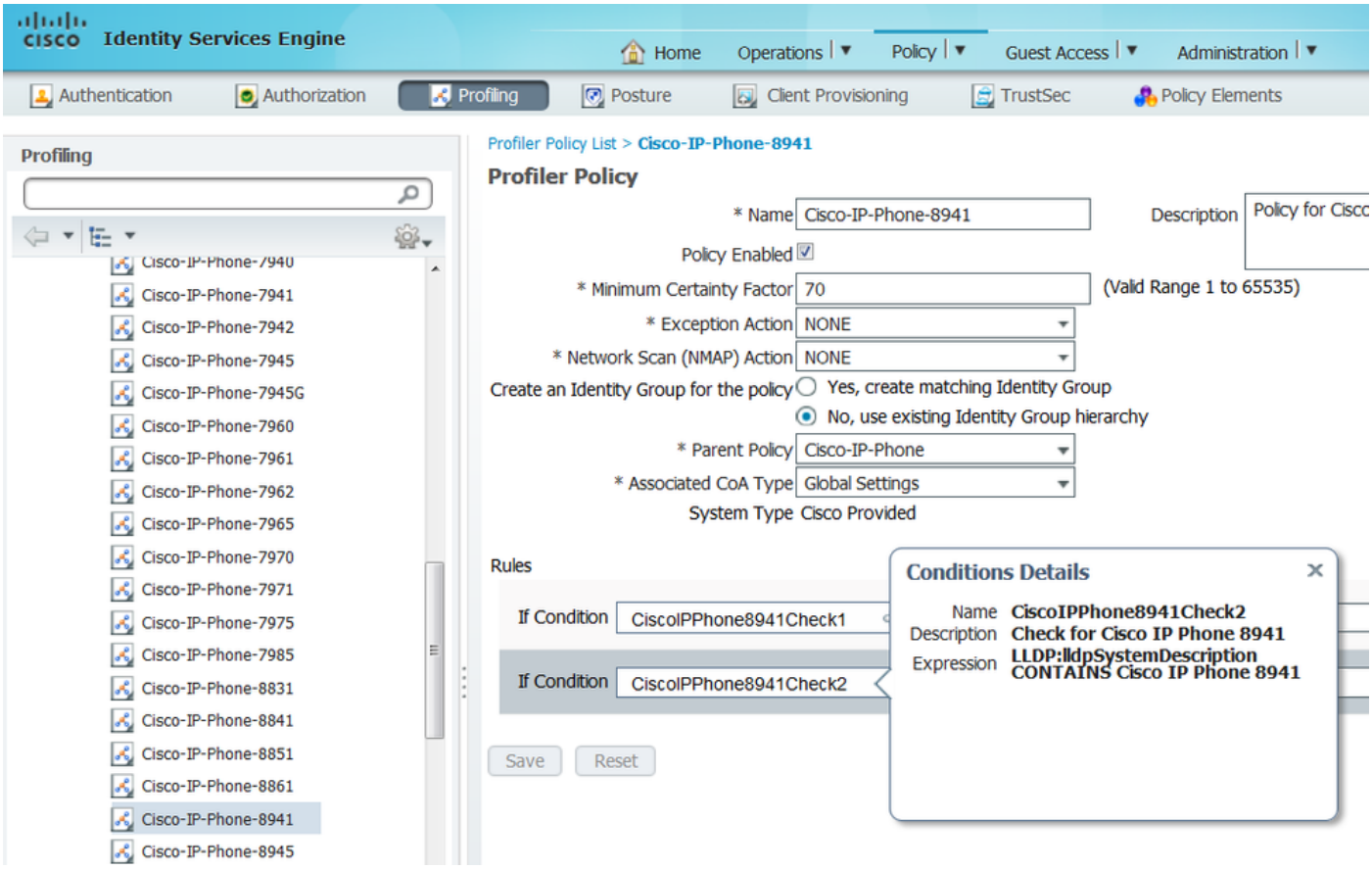
注意：在較新的軟體版本中，預設情況下啟用命令radius-server vsa send accounting。如果您看不到以記賬方式傳送的屬性，請確認指令是否已啟用。

步驟 2.配置裝置感測器

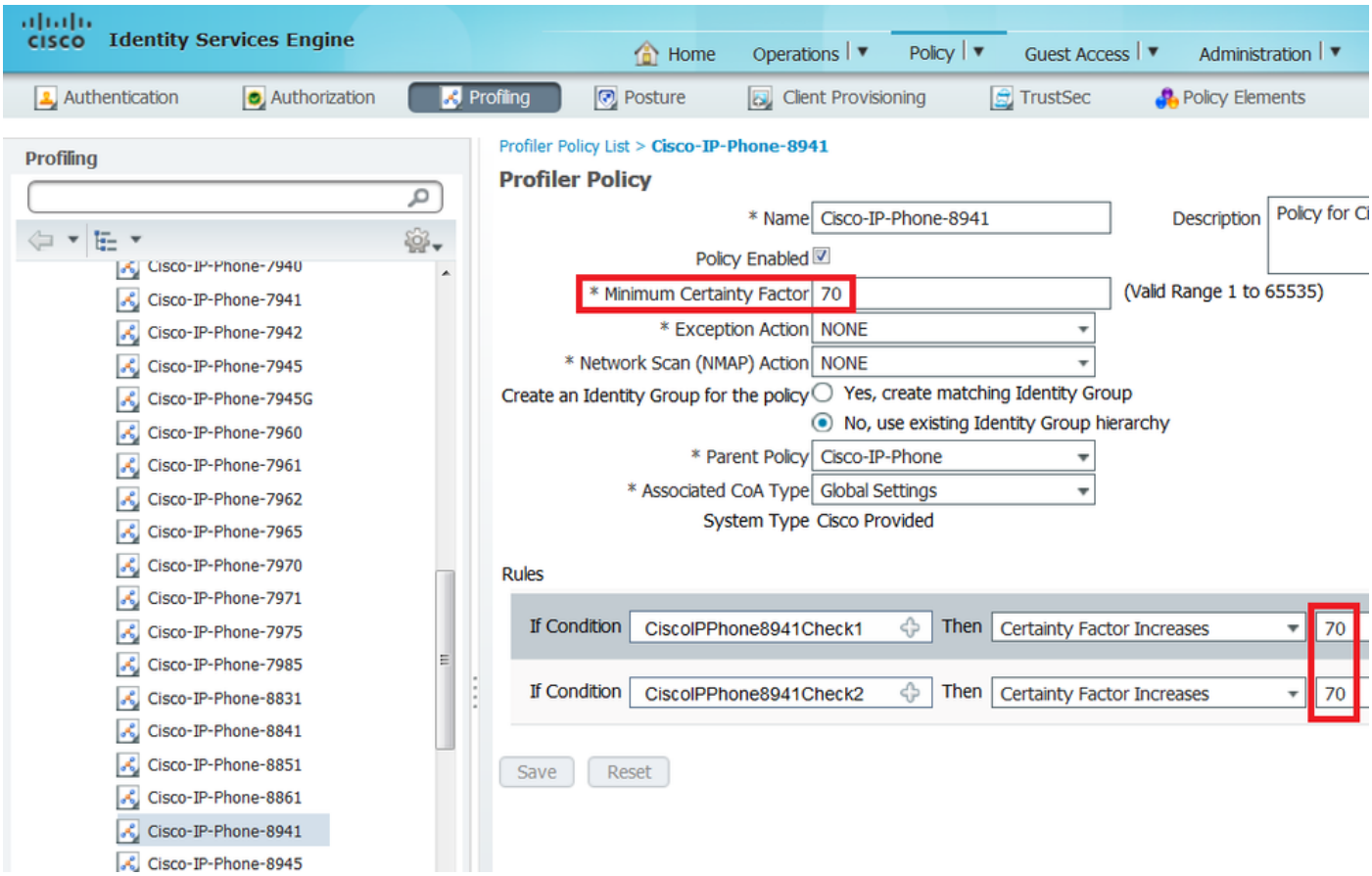
1.

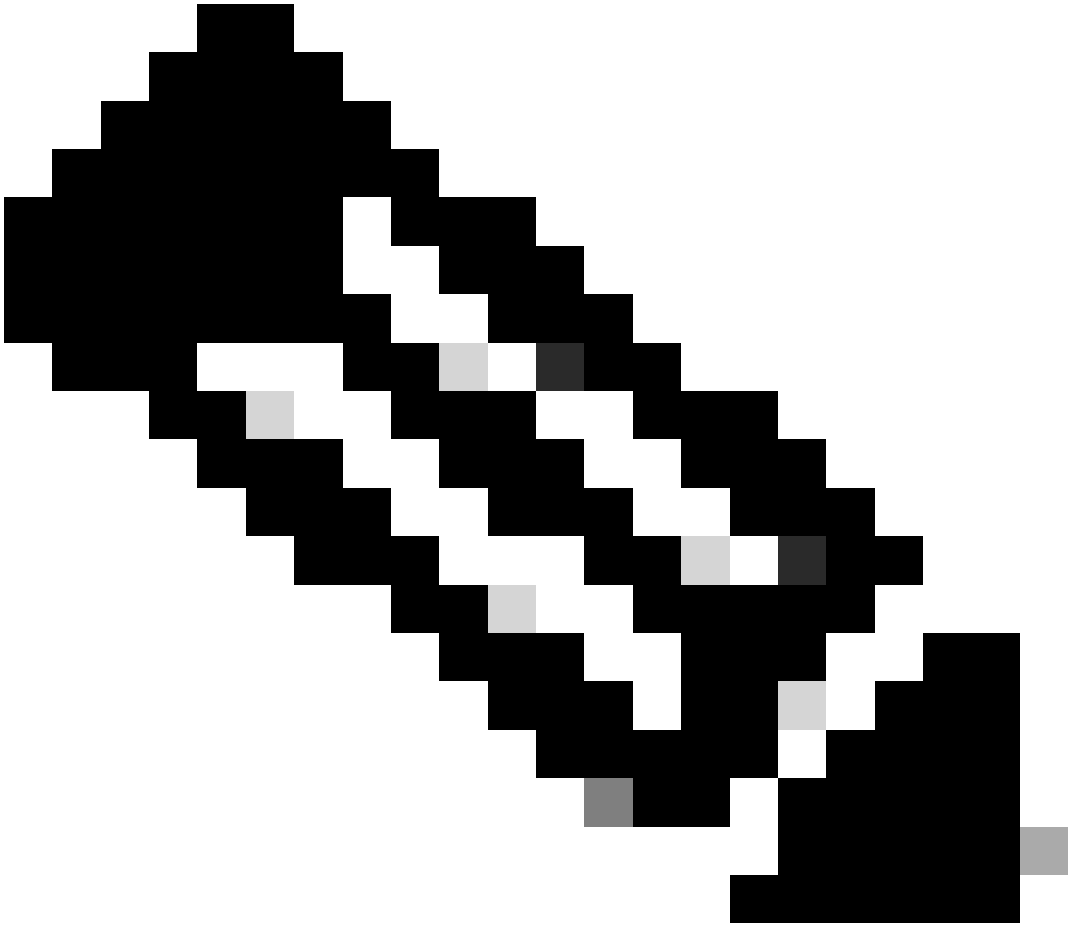
確定需要使用CDP/LLDP中的哪些屬性來分析裝置。對於Cisco IP電話8941，您可以使用以下命令：

- LLDP SystemDescription屬性
- CDP CachePlatform屬性



出於我們的目的，只需獲得其中一項就足夠了，因為這兩者均提供了增加70的確定性工廠，並且要求分析為Cisco-IP-Phone-8941的最低確定性工廠為70：


Identity Services Engine
Home
Operations
Policy
Guest Access
Administration
Authentication
Authorization
Profiling
Posture
Client Provisioning
TrustSec
Policy Elements
Profiling
Cisco-IP-Phone-7940
Cisco-IP-Phone-7941
Cisco-IP-Phone-7942
Cisco-IP-Phone-7945
Cisco-IP-Phone-7945G
Cisco-IP-Phone-7960
Cisco-IP-Phone-7961
Cisco-IP-Phone-7962
Cisco-IP-Phone-7965
Cisco-IP-Phone-7970
Cisco-IP-Phone-7971
Cisco-IP-Phone-7975
Cisco-IP-Phone-7985
Cisco-IP-Phone-8831
Cisco-IP-Phone-8841
Cisco-IP-Phone-8851
Cisco-IP-Phone-8861
Cisco-IP-Phone-8941
Cisco-IP-Phone-8945
Profiler Policy List > Cisco-IP-Phone-8941
Profiler Policy
* Name Cisco-IP-Phone-8941
Description Policy for Ci
Policy Enabled
* Minimum Certainty Factor 70
(Valid Range 1 to 65535)
* Exception Action NONE
* Network Scan (NMAP) Action NONE
Create an Identity Group for the policy
Yes, create matching Identity Group
No, use existing Identity Group hierarchy
* Parent Policy Cisco-IP-Phone
* Associated CoA Type Global Settings
System Type Cisco Provided
Rules
If Condition CiscoIPPhone8941Check1 Then Certainty Factor Increases 70
If Condition CiscoIPPhone8941Check2 Then Certainty Factor Increases 70
Save
Reset



註：要分析為特定Cisco IP電話，您必須滿足所有父配置檔案的最低條件。這意味著分析器必須匹配思科裝置（最低確定係數10）和思科IP電話（最低確定係數20）。即使效能評測器符合這兩個設定檔，它仍必須被評測為特定的Cisco IP電話，因為每個IP電話型號的最小確定性因子為70。裝置會指定給具有最高確定因數的設定檔。

2. 配置兩個過濾器清單-一個用於CDP，另一個用於LLDP。這些選項指示哪些屬性必須包含在Radius記帳消息中。此步驟是可選的。

3. 為CDP和LLDP建立兩個過濾器規格。在filter-spec中，您可以指示必須包括在記帳消息中或從中排除的屬性清單。在本範例中，包括下列屬性：

- CDP中的裝置名稱
-

來自LLDP的系統說明

如果需要，可以配置透過RADIUS傳輸到ISE的其他屬性。此步驟也是可選的。

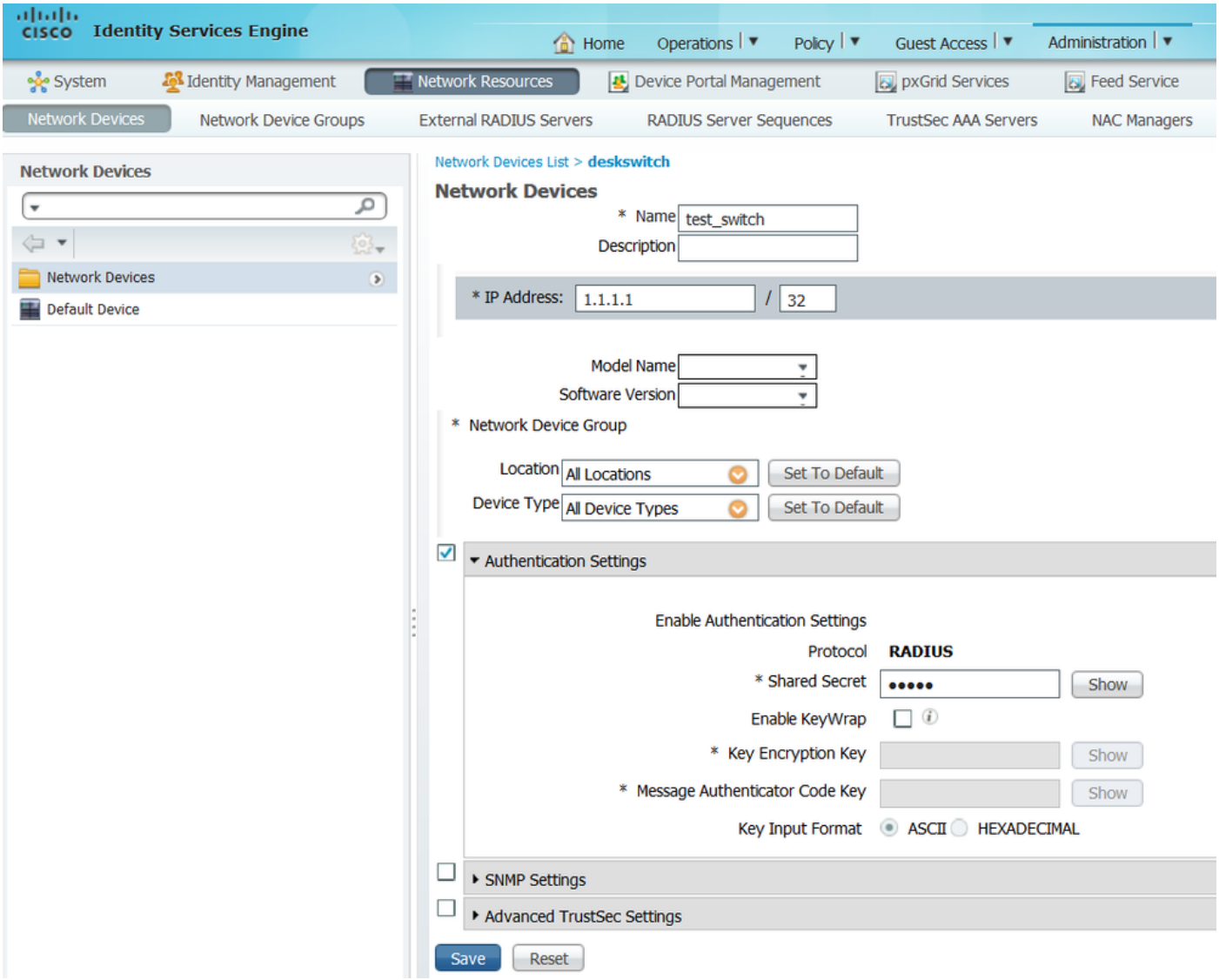
4. 增加命令device-sensor notify all-changes。每當為當前會話增加、修改或刪除TLV時，它都會觸發更新。

5. 要實際傳送透過裝置感測器功能收集的資訊，您必須使用device-sensor accounting命令明確告知交換機完成此步驟。

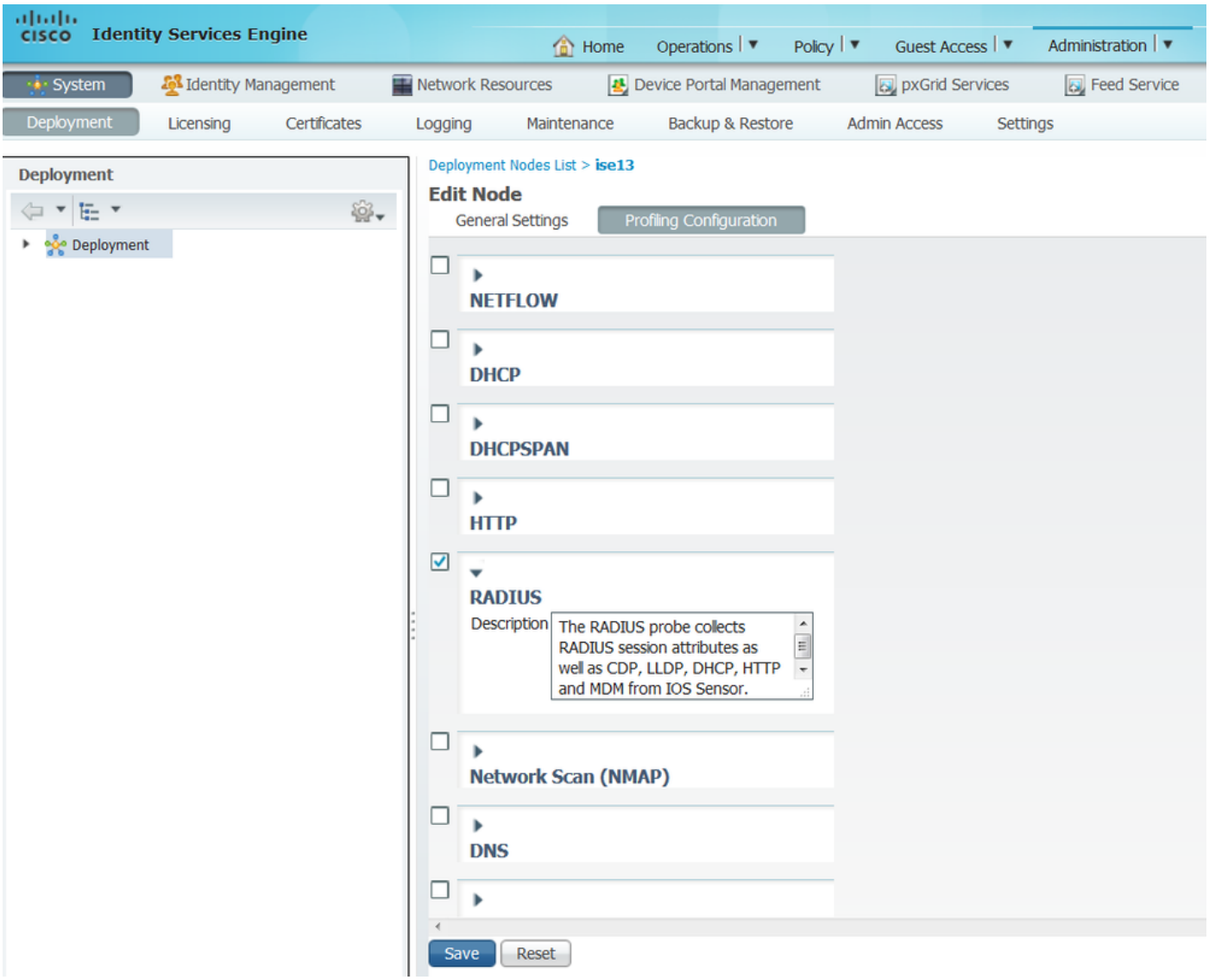
! device-sensor filter-list cdp list cdp-list tlv name device-name
tlv name platform-type ! device-sensor filter-list lldp list lldp-list tlv name system-description ! device-sensor filter-spec lldp include list lldp-list device-se

步驟 3.在ISE上配置分析

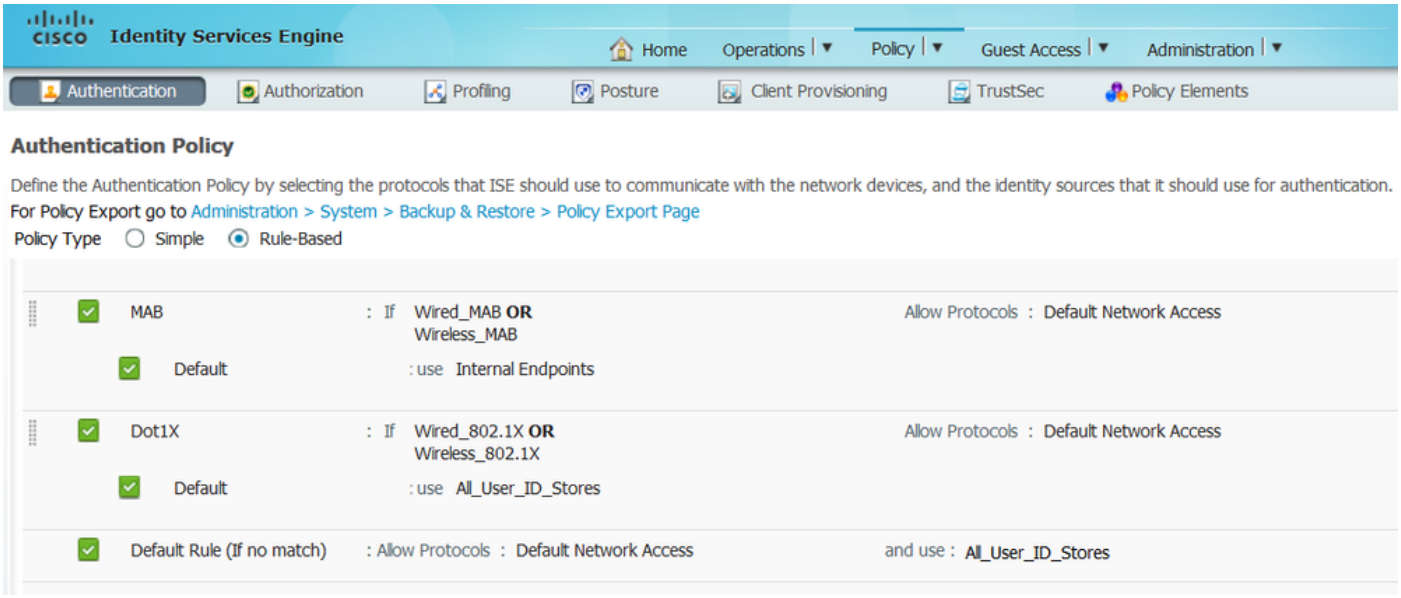
1. 在Administration > Network Resources > Network Devices中增加交換機作為網路裝置。在Authentication Settings：



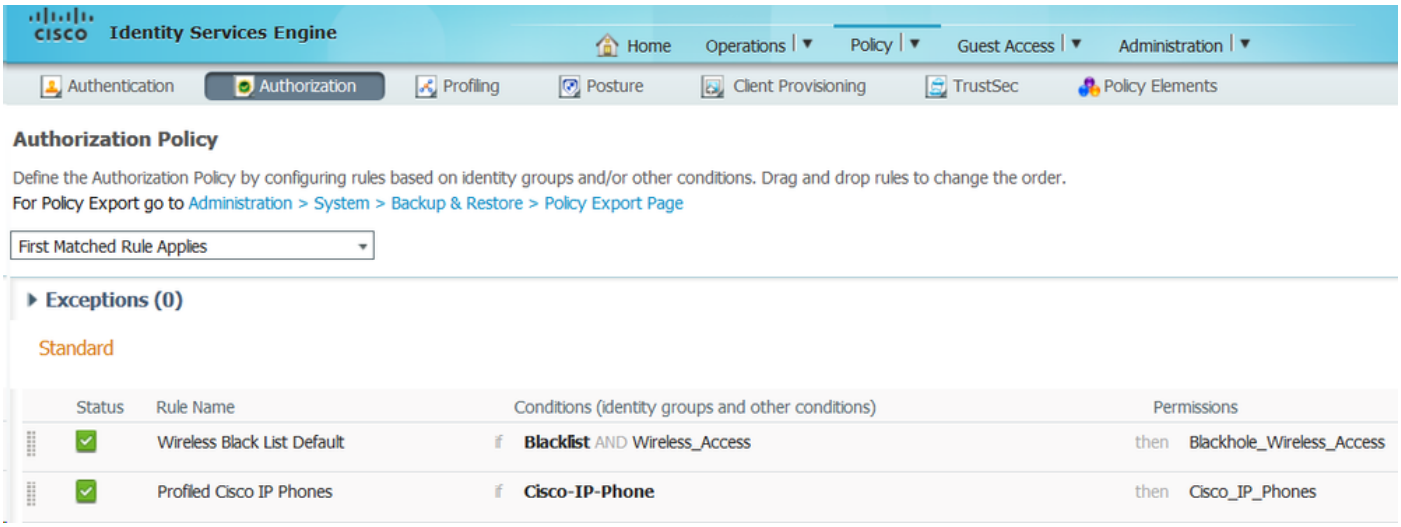
2. 在Administration > System > Deployment > ISE node > Profiling Configuration中的效能分析節點上啟用Radius探測。如果所有PSN節點都必須用於效能分析，請在所有PSN節點上啟用探測：



3. 配置ISE身份驗證規則。在示例中，使用ISE上預配置的預設身份驗證規則：

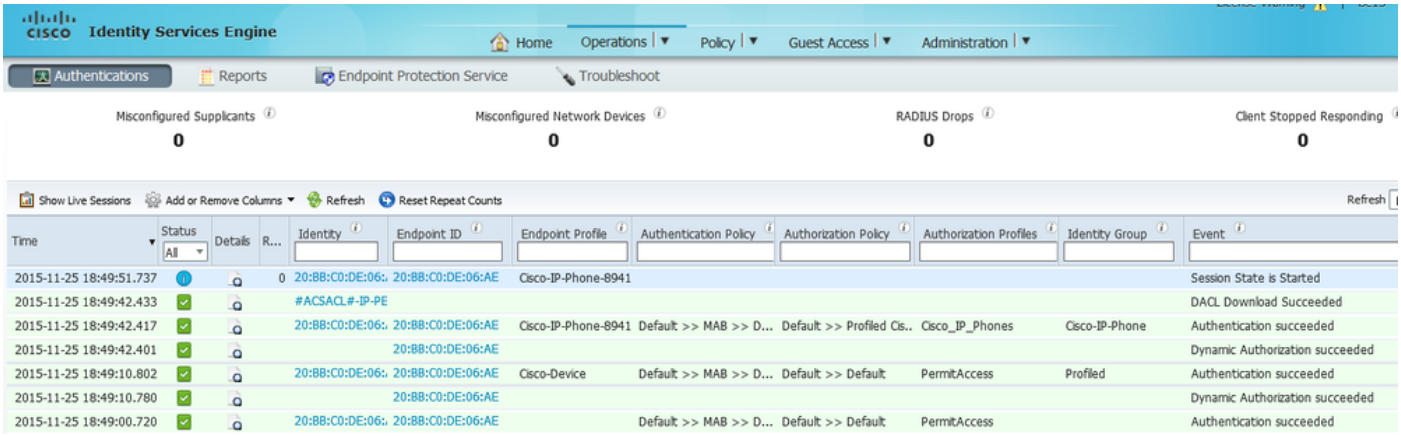


4. 配置ISE授權規則。使用「已分析的思科IP電話」規則，該規則在ISE上已預配置：

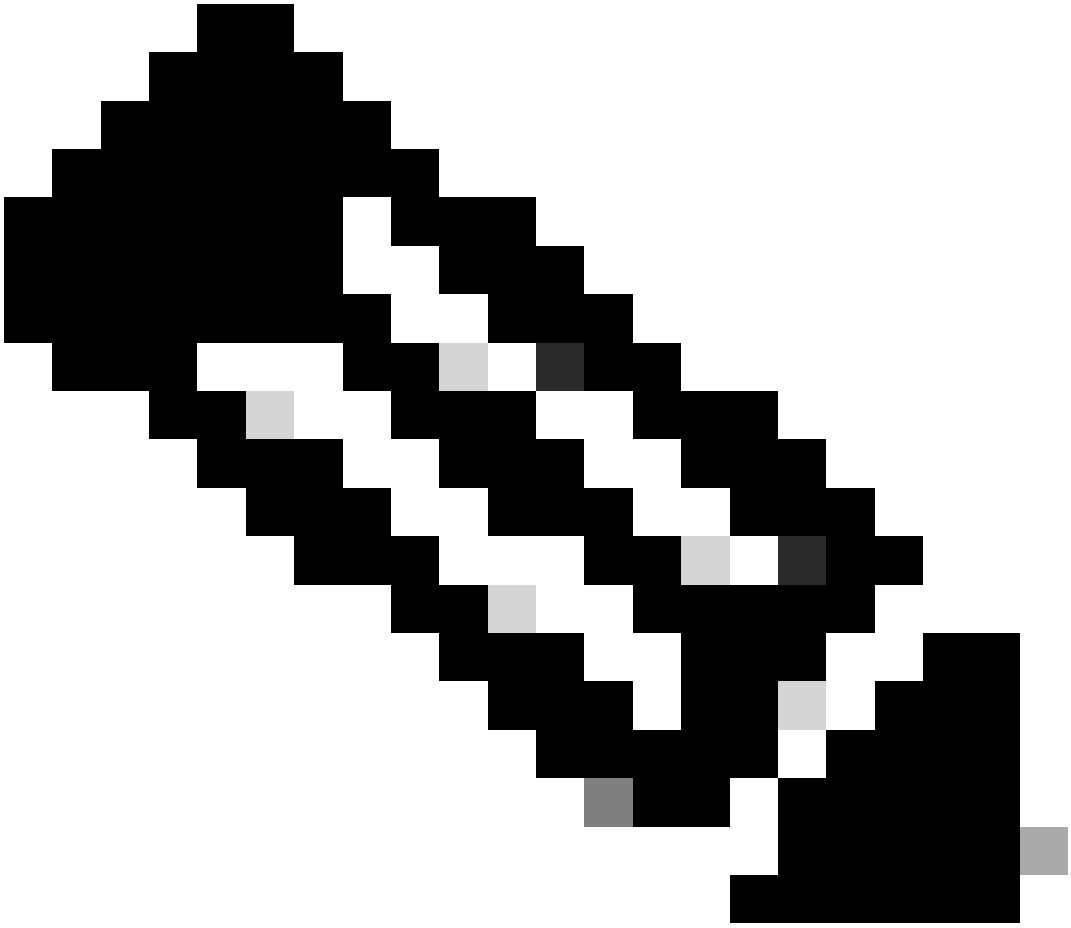


驗證

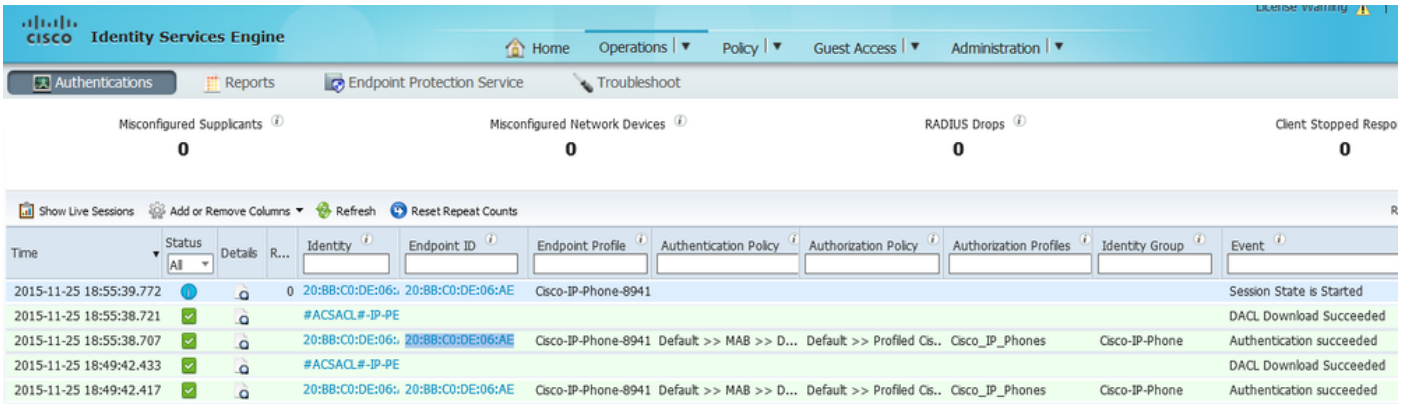
要驗證分析是否工作正常，請參閱在ISE上使用Operations > Authentications：



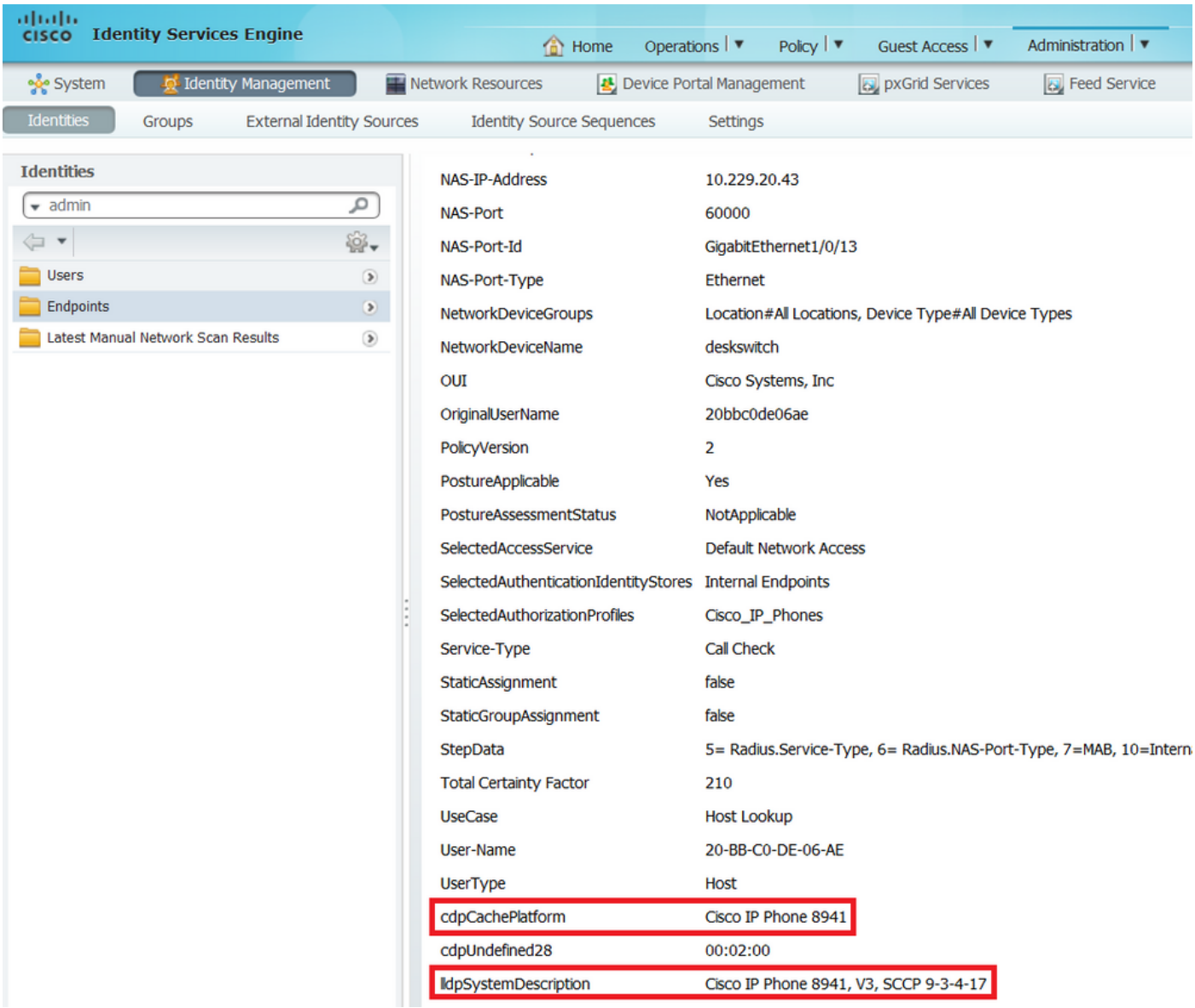
首先，使用MAB (18:49:00)對裝置進行身份驗證。10秒後(18:49:10)，它被重新存檔為Cisco-Device，最後在第一次身份驗證後的42秒後(18:49:42)，它接收了Cisco-IP-Phone-8941配置檔案。因此，ISE會返回特定於IP電話(Cisco_IP_Phones)的授權配置檔案和可下載ACL，允許所有流量(permit ip any)。請注意，在此場景中，未知裝置具有基本的網路訪問許可權。這可以透過將Mac地址增加到ISE內部終端資料庫或允許對以前未知的裝置進行非常基本的網路訪問來實現。



注意：在此示例中，初始分析大約需要40秒。在下次身份驗證時，ISE已經知道配置檔案，並且會立即應用正確的屬性（加入語音域和DACL的許可權），除非ISE收到新的/更新的屬性，並且必須重新對裝置進行配置檔案。



在Administration > Identity Management > Identities > Endpoints > tested endpoint中，您可以看到Radius探測器收集了哪些型別的屬性及其值：



如您所觀察，在此場景中計算出的總確定性因子為210。它來自一個事實，即終端還匹配思科裝置配置檔案（總確定性因子為30）和思科IP電話配置檔案（總確定性因子為40）。由於分析工具與配置檔案Cisco-IP-Phone-8941中的兩個條件匹配，因此此配置檔案的確定性因子為140（根據分析策略，每個屬性為70）。總和：30+40+70+70=210。

疑難排解

步驟 1.驗證CDP/LLDP收集的資訊

switch#sh cdp neighbors g1/0/13 detail ---------- Device ID: SEP20BBC0DE06AE Entry address(es): Platform: Cisco IP Phone 8941 , Capabil

switch#
switch#sh lldp neighbors g1/0/13 detail

Chassis id: 0.0.0.0
Port id: 20BBC0DE06AE:P1
Port Description: SW Port
System Name: SEP20BBC0DE06AE.

System Description:
Cisco IP Phone 8941, V3, SCCP 9-3-4-17

Time remaining: 164 seconds
System Capabilities: B,T
Enabled Capabilities: B,T
Management Addresses - not advertised
Auto Negotiation - supported, enabled
Physical media capabilities:
  1000baseT(FD)
  100base-TX(FD)
  100base-TX(HD)
  10base-T(FD)
  10base-T(HD)
Media Attachment Unit type: 16
Vlan ID: - not advertised

MED Information:

  MED Codes:
    (NP) Network Policy, (LI) Location Identification
    (PS) Power Source Entity, (PD) Power Device
    (IN) Inventory

  H/W revision: 3
  F/W revision: 0.0.1.0
  S/W revision: SCCP 9-3-4-17
  Serial number: PUC17140FBO
  Manufacturer: Cisco Systems , Inc.
  Model: CP-8941
  Capabilities: NP, PD, IN
  Device type: Endpoint Class III
  Network Policy(Voice): VLAN 101, tagged, Layer-2 priority: 0, DSCP: 0
  Network Policy(Voice Signal): VLAN 101, tagged, Layer-2 priority: 3, DSCP: 24
  PD device, Power source: Unknown, Power Priority: Unknown, Wattage: 3.8
  Location - not advertised

Total entries displayed: 1

如果您看不到收集的任何資料，請確認此情況：

- 檢查交換器上驗證作業階段的狀態（必須成功）：

piborowi#show authentication sessions int g1/0/13 details Interface: GigabitEthernet1/0/13 MAC Address: 20bb.c0de.06ae IPv6 Address: Unknown IPv4 A

- 檢查CDP和LLDP協定是否已啟用。檢查是否有任何與CDP/LLDP/等相關的非預設命令，以及這些命令如何影響從終端檢索屬性

```
switch#sh running-config all | in cdp run
cdp run
switch#sh running-config all | in lldp run
lldp run
```

- 驗證您的終端是否支援CDP/LLDP/等，請在配置指南中進行驗證。

步驟 2.檢查裝置感測器快取

switch#show device-sensor cache interface g1/0/13 Device: 20bb.c0de.06ae on port GigabitEthernet1/0/13 ---------- Proto

如果在此欄位中看不到任何資料或資訊不完整，請驗證「device-sensor」命令，特別是filter-lists和filter-specs。

步驟 3.檢查Radius記賬中是否存在屬性

可以在交換機上使用debug radius驗證或在交換機與ISE之間執行資料包捕獲。

Radius調試：

<#root>

Mar 30 05:34:58.716: RADIUS(00000000): Send Accounting-Request to 1.1.1.1:1813 id 1646/85, len 378 Mar 30 05:34:58.716: RADIUS: authenticator 1

cdp-tlv

= " Mar 30 05:34:58.716: RADIUS: Vendor, Cisco [26] 23 Mar 30 05:34:58.716: RADIUS: Cisco AVpair [1] 17

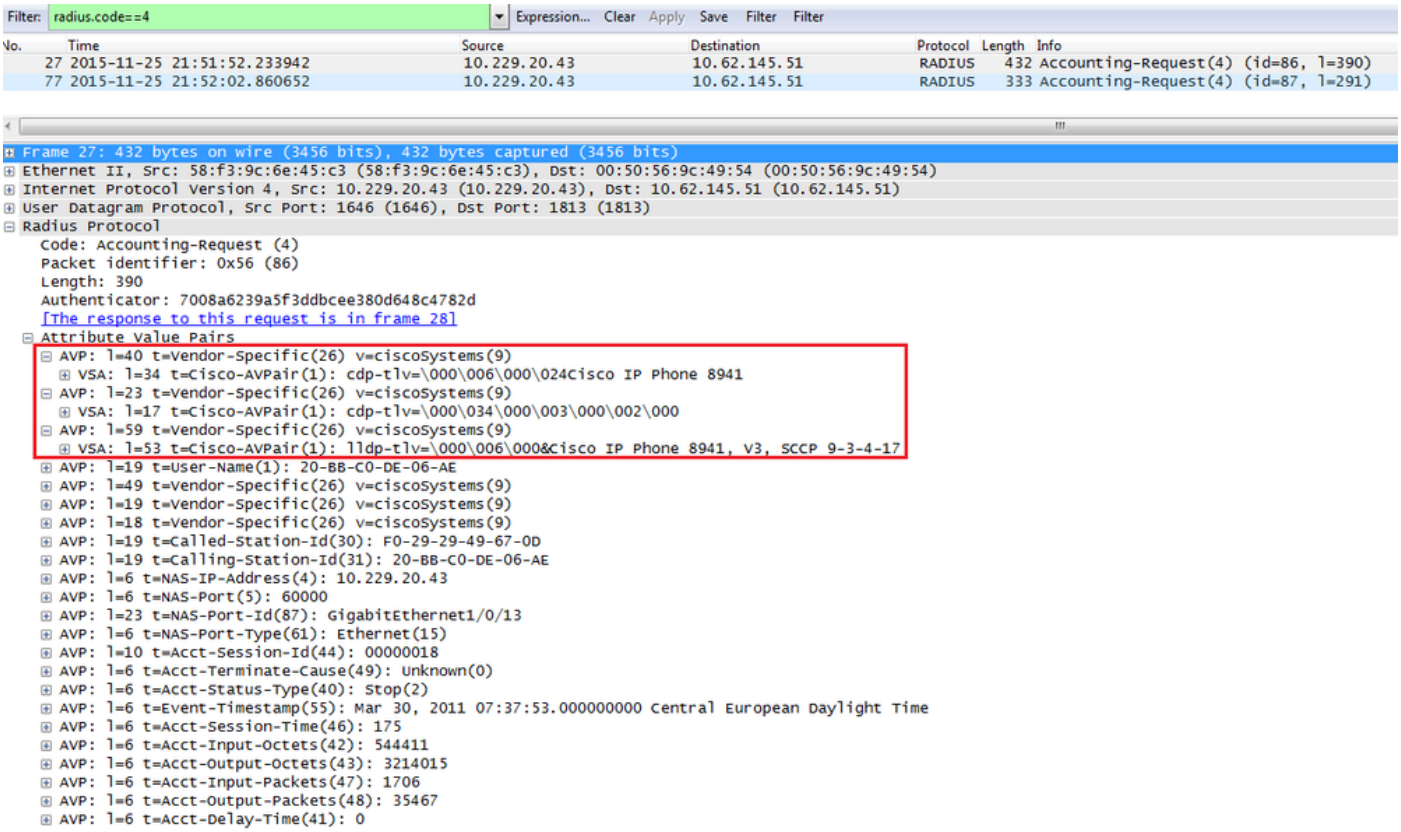
cdp-tlv

= " Mar 30 05:34:58.721: RADIUS: Vendor, Cisco [26] 59 Mar 30 05:34:58.721: RADIUS: Cisco AVpair [1] 53

lldp-tlv

= " Mar 30 05:34:58.721: RADIUS: User-Name [1] 19 "20-BB-C0-DE-06-AE" Mar 30 05:34:58.721: RADIUS: Vend

資料包捕獲：



步驟 4.驗證ISE上的分析器調試

如果屬性是從交換機傳送的，可以檢查它們是否在ISE上接收。要檢查此配置，請為正確的PSN節點(Administration > System > Logging > Debug Log Configuration > PSN > profiler > debug)啟用分析器調試，並再次執行終端身份驗證。

請查詢以下資訊：

- 調試指示radius探測功能已接收屬性：

<#root>

2015-11-25 19:29:53,641 DEBUG [RADIUSParser-1-thread-1][]
cisco.profiler.probes.radius.RadiusParser -:::-
MSG_CODE=[3002], VALID=[true], PRRT_TIMESTAMP=[2015-11-25 19:29:53.637 +00:00],
ATTRS=[Device IP Address=10.229.20.43, RequestLatency=7,
NetworkDeviceName=deskswitch, User-Name=20-BB-C0-DE-06-AE,
NAS-IP-Address=10.229.20.43, NAS-Port=60000, Called-Station-ID=F0-29-29-49-67-0D,
Calling-Station-ID=20-BB-C0-DE-06-AE, Acct-Status-Type=Interim-Update,
Acct-Delay-Time=0, Acct-Input-Octets=362529, Acct-Output-Octets=2871426,
Acct-Session-Id=00000016, Acct-Input-Packets=1138, Acct-Output-Packets=32272,
Event-Timestamp=1301458555, NAS-Port-Type=Ethernet, NAS-Port-Id=GigabitEthernet1/0/13,

cisco-av-pair=cdp-tlv=cdpCachePlatform=Cisco IP Phone 8941

,
cisco-av-pair=cdp-tlv=cdpUndefined28=00:02:00,

cisco-av-pair=lldp-tlv=lldpSystemDescription=Cisco IP Phone 8941\, V3\, SCCP 9-3-4-17,

cisco-av-pair=audit-session-id=0AE5182000000020400 99C216, cisco-av-pair=vlan-id=101,
cisco-av-pair=method=mab, AcsSessionID=ise13/235487054/2511, SelectedAccessService=Default Network Acce
Step=11004, Step=11017, Step=15049, Step=15008, Step=15004, Step=11005, NetworkDeviceGroups=Location#Al
NetworkDeviceGroups=Device Type#All Device Types, Service-Type=Call Check, CPMSessionID=0AE518200000020
AllowedProtocolMatchedRule=MAB, Location=Location#All Locations, Device Type=Device Type#All Device Typ

- 偵錯，指出已成功剖析屬性：

2015-11-25 19:29:53,642 DEBUG [RADIUSParser-1-thread-1][] cisco.profiler.probes.radius.RadiusParser -:::- Parsed IOS Sensor 1: cdpCachePlatform=[

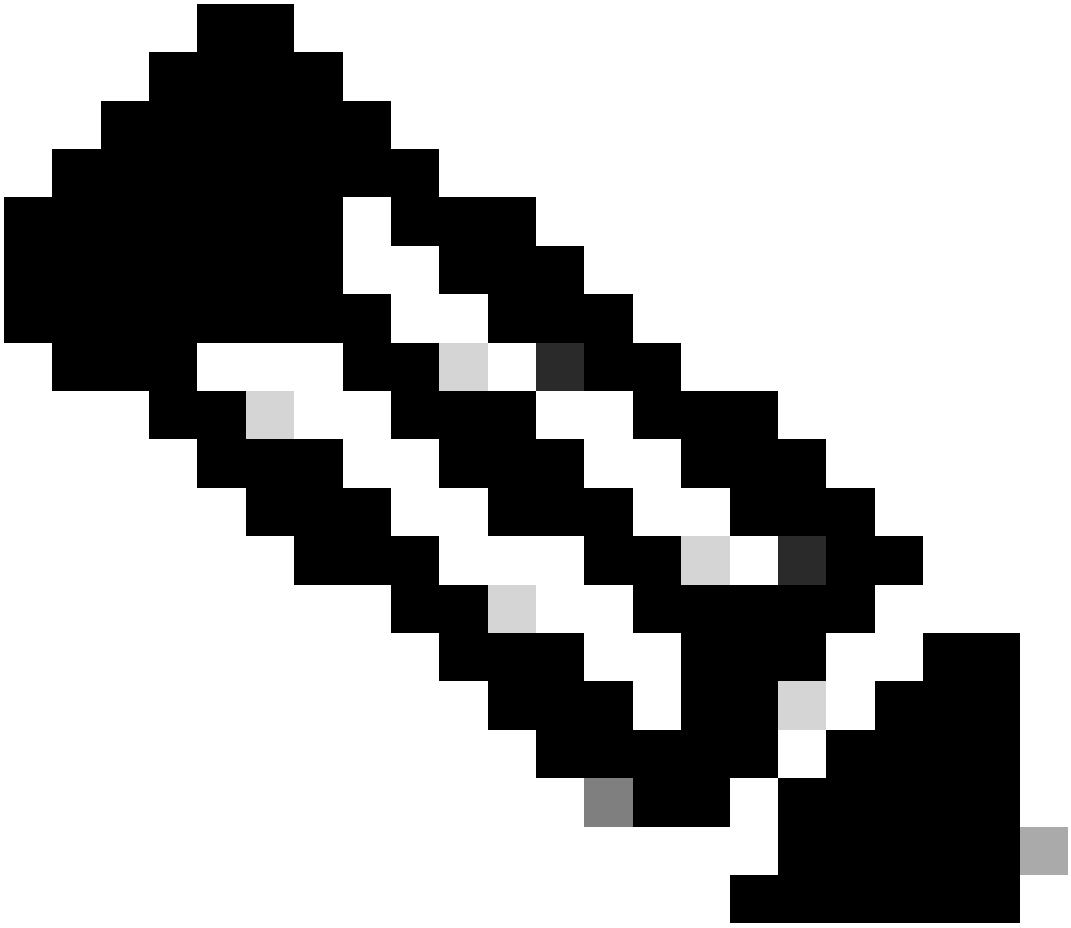
- 偵錯，指出屬性是由轉寄站處理：

<#root>

2015-11-25 19:29:53,643 DEBUG [forwarder-6][] cisco.profiler.infrastructure.probemgr.Forwarder -:20:BB:C0:DE:06:AE:ProfilerCollection:- Endpoint A

Attribute:cdpCachePlatform value:Cisco IP Phone 8941 Attribute:cdpUndefined28 value:00:02:00 Attribute:l

Attribute:SkipProfiling value:false



注意：轉發器將終端及其屬性資料儲存在思科ISE資料庫中，然後通知分析器您的網路中檢測到的新終端。分析器將終端分類到終端身份組，並將具有匹配配置檔案的終端儲存在資料庫中。

步驟 5. 分析新屬性和裝置分配

通常，將新屬性增加到特定裝置的現有集合後，此裝置/終端會被增加到分析隊列，以檢查是否需要根據新屬性為其分配不同的配置檔案：

<#root>

2015-11-25 19:29:53,646 DEBUG [EndpointHandlerWorker-6-31-thread-1][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:20:BB:C0:DE:06:AE:Profiling:-

Classify hierarchy 20:BB:C0:DE:06:AE

2015-11-25 19:29:53,656 DEBUG [EndpointHandlerWorker-6-31-thread-1][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:20:BB:C0:DE:06:AE:Profiling:-

Policy Cisco-Device matched 20:BB:C0:DE:06:AE (certainty 30)

2015-11-25 19:29:53,659 DEBUG [EndpointHandlerWorker-6-31-thread-1][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:20:BB:C0:DE:06:AE:Profiling:-

Policy Cisco-IP-Phone matched 20:BB:C0:DE:06:AE (certainty 40)

2015-11-25 19:29:53,663 DEBUG [EndpointHandlerWorker-6-31-thread-1][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:20:BB:C0:DE:06:AE:Profiling:-

Policy Cisco-IP-Phone-8941 matched 20:BB:C0:DE:06:AE (certainty 140)

2015-11-25 19:29:53,663 DEBUG [EndpointHandlerWorker-6-31-thread-1][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:20:BB:C0:DE:06:AE:Profiling:-

After analyzing policy hierarchy: Endpoint: 20:BB:C0:DE:06:AE EndpointPolicy:Cisco-IP-Phone-8941 for:210

相關資訊

- https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/index.html
- https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_prof_pol.html
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。