Contenu

Introduction

Ce document décrit comment configurer le capteur de périphérique, de sorte qu'il puisse être utilisé pour profiler des buts sur ISE. Le capteur de périphérique est une caractéristique des périphériques d'accès. Il laisse collecter des informations sur des points finaux connectés. En grande partie, les informations collectées par le capteur de périphérique peuvent provenir les protocoles suivants :

- Cisco Discovery Protocol (CDP)
- Protocole LLDP (Link Layer Discovery Protocol)
- Protocole DHCP (DHCP)

Sur quelques Plateformes il est possible d'utiliser également le h323, le SIP (protocole SIP), les MDN (résolution de domaine de Multidiffusion) ou les protocoles HTTP. Les possibilités de configuration pour des capacités de capteur de périphérique peuvent varier du protocole au protocole. Comme exemple au-dessus de est disponible sur Cisco Catalyst 3850 avec le logiciel 03.07.02.E.

Une fois que les informations sont collectées, elles peuvent être encapsulées en comptabilité de rayon et envoyer à un serveur de profilage. Dans cette engine de gestion d'identité d'article (ISE) est utilisé en tant que serveur de profilage.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Protocole RADIUS
- Protocoles de CDP, de LLDP et DHCP
- Engine de gestion d'identité de Cisco
- Commutateur Cisco Catalyst 2960

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Correctif 3 de version 1.3 d'engine de gestion d'identité de Cisco
- Version 15.2(2a)E1 du commutateur Cisco Catalyst 2960s
- SCCP 9-3-4-17 de version du téléphone IP 8941 de Cisco

Configurez

Étape 1. Configuration standard d'AAA

Afin de configurer l'authentification, l'autorisation et la comptabilité (AAA), suivent les étapes ci-dessous :

1. Activez l'AAA utilisant la commande d'**`aaa new-model`** et activez le 802.1X globalement sur le commutateur

2. Configurez le serveur de rayon et activez l'autorisation dynamique (modification de l'autorisation - le CoA)

3. Protocoles de CDP et de LLDP d'enable

4. Ajoutez la configuration d'authentification de switchport

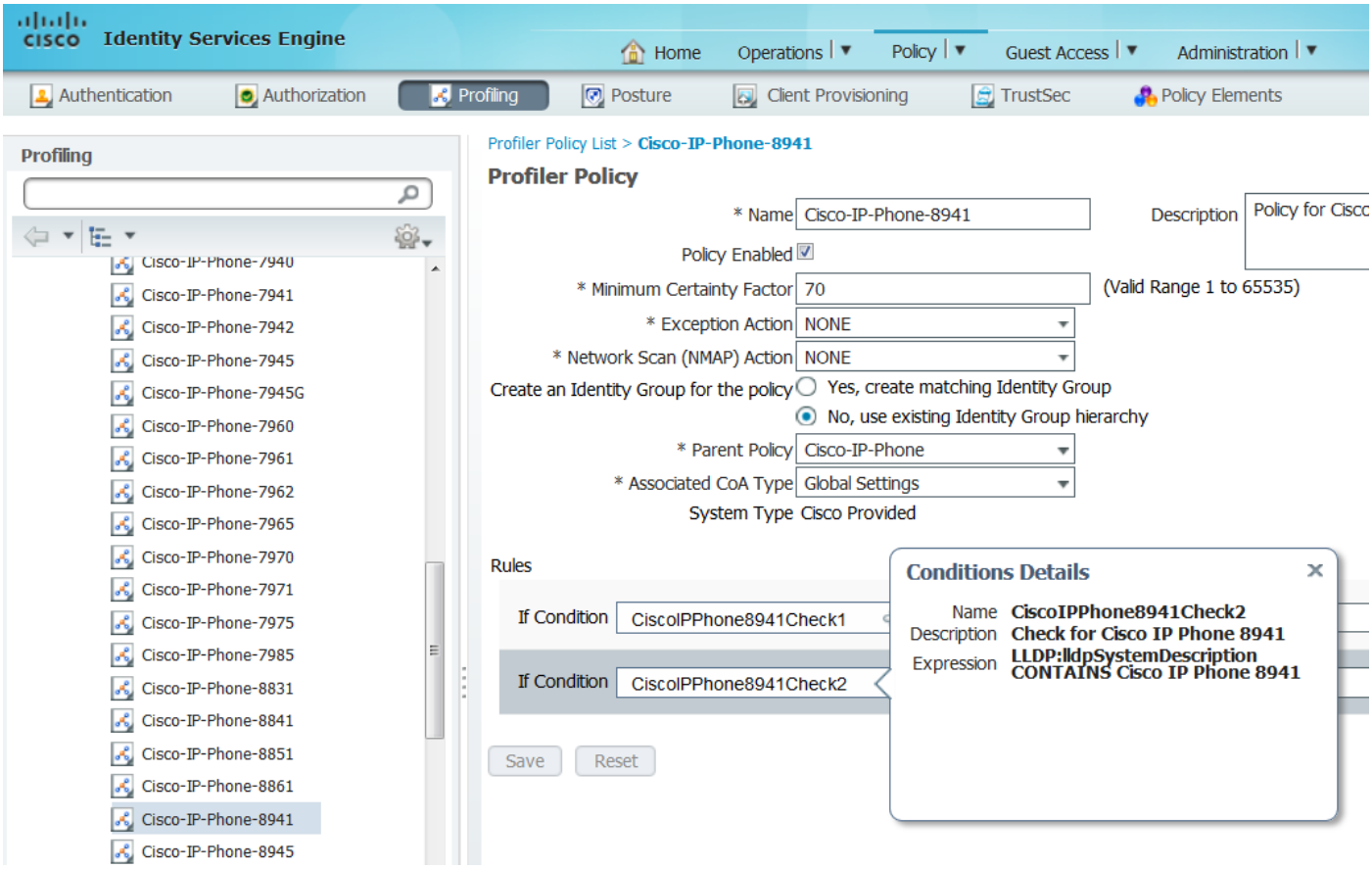
```
!
aaa new-model!aaa authentication dot1x default group radiusaaa authorization network default
group radiusaaa accounting update newinfoaaa accounting dot1x default start-stop group radius!
aaa server radius dynamic-author
 client 1.1.1.1 server-key xyz
!
dot1x system-auth-control
!lldp run
cdp run!interface 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 portfastend!radius-server host 1.1.1.1 auth-port 1812 acct-port 1813 key xyz
!
```

> **Dans un plus nouveau `radius-server vsa send de` commande de version de logiciel la `comptabilité` est activée par défaut. Si vous ne pouvez pas voir des attributs introduire la comptabilité, vérifiez si la commande dans activé.**

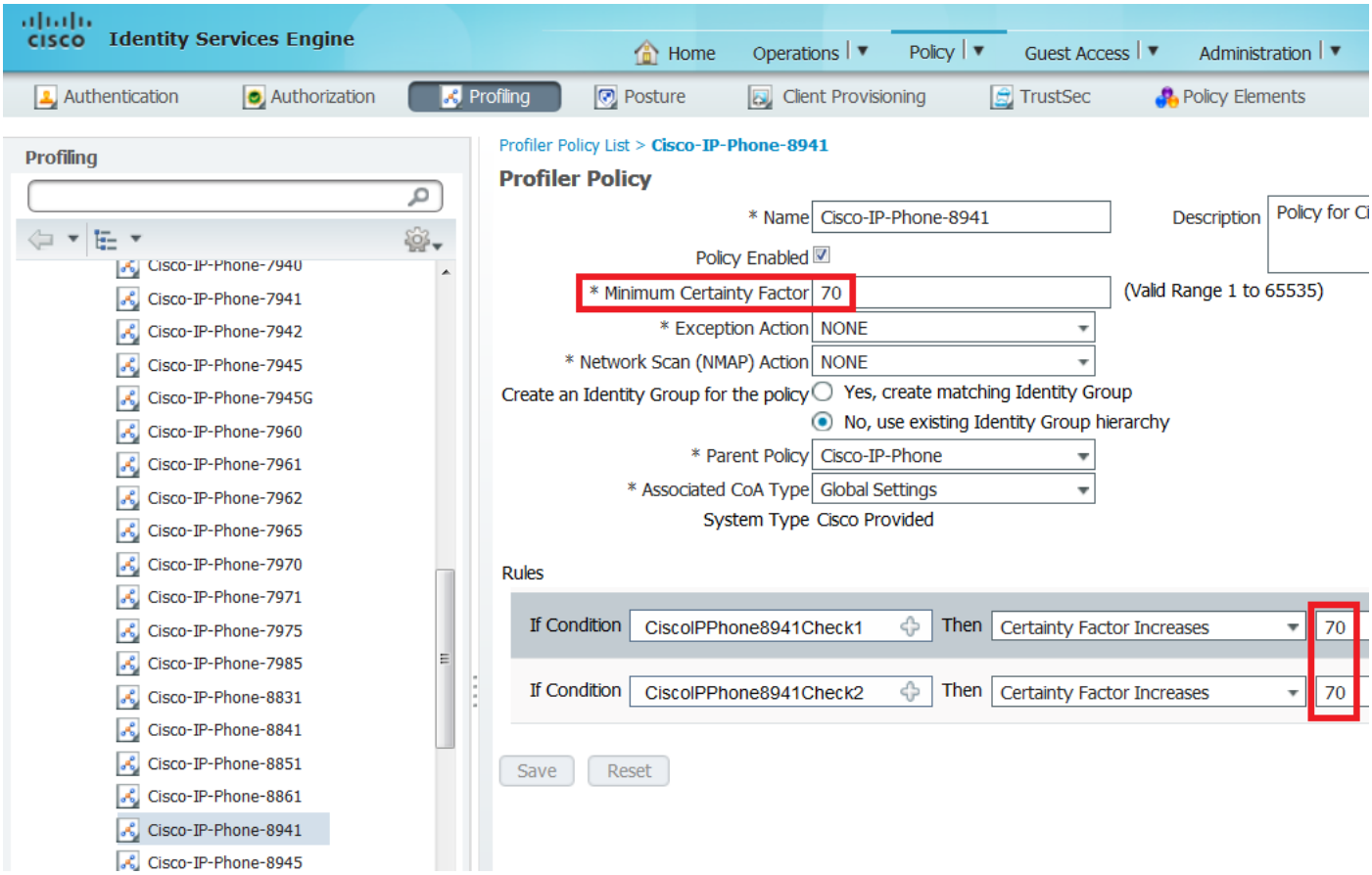
Étape 2. Configurez le capteur de périphérique

1. Déterminez quels attributs de CDP/LLDP sont nécessaires pour profiler le périphérique. En cas de téléphone IP 8941 de Cisco vous pouvez utiliser ce qui suit :

- Attribut de SystemDescription de LLDP
- Attribut de CachePlatform de CDP



Pour notre but il serait assez pour obtenir juste un de ceux puisque chacun d'eux fournissent l'augmentation d'usine de certitude de 70 et l'usine minimum de certitude exigée pour être profilé comme Cisco-IP-Phone-8941 est 70 :



Afin d'être profilé en tant que téléphone IP spécifique de Cisco, youneed pour remplir des conditions minimum pour tous les profils de parent. Ceci signifie que le profileur doit apparier le Cisco-périphérique (facteur minimal de certitude 10) et le Cisco-IP-téléphone (facteur minimal 20 de certitude). Quoique le profileur apparie ces deux profils, il devrait encore être profilé en tant que téléphone IP spécifique de Cisco puisque chaque modèle de téléphone IP a le facteur minimal de certitude de 70. Le périphérique est assigné au profil pour lequel il a le facteur de certitude le plus élevé.

2. Configurez deux listes de filtre - une pour le CDP et un autre pour le LLDP. Ceux indiquent que ce qui attribue devrait être inclus dans des messages de comptabilité de rayon. Cette étape est facultative

3. Créez deux filtre-spécifications pour le CDP et le LLDP. Dans la spécification de fiter vous pouvez l'un ou l'autre indiquer que la liste d'attributs devrait être incluse ou exclue des messages de comptabilité. Dans l'exemple les attributs suivants sont inclus :

- nom du périphérique de CDP
- système-description de LLDP

Vous pouvez configurer des attributs supplémentaires à transmited par l'intermédiaire du rayon à ISE si nécessaire. Cette étape est également facultative.

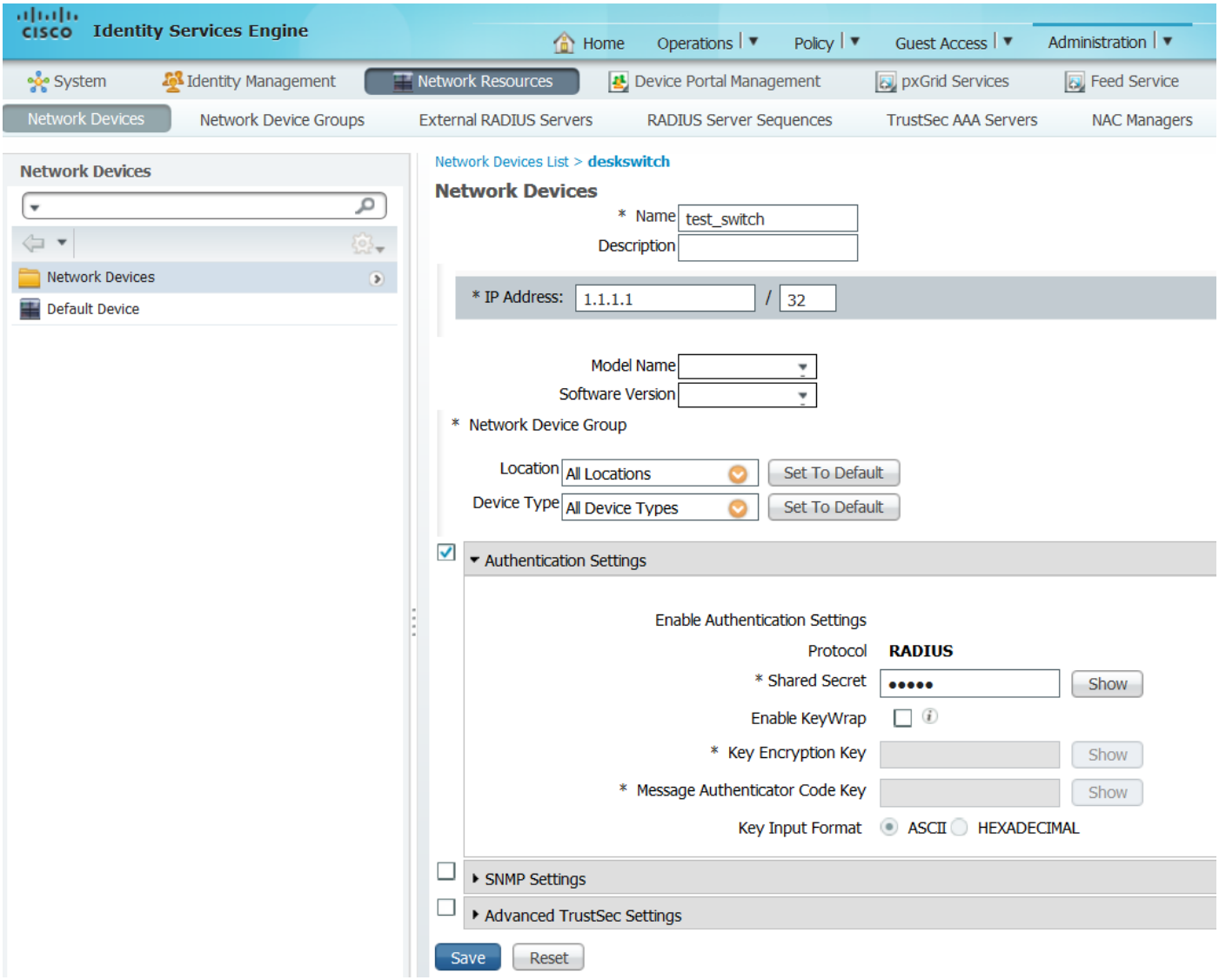
4. Ajoutez le périphérique-**`capteur de`** commande **`informent des tout-modifications`**. Il déclenche des mises à jour toutes les fois que TLVs sont ajoutés, modifiés ou retirés pour la session en cours

5. Afin d'envoyer réellement les informations a recueilli par l'intermédiaire de la fonctionnalité de capteur de périphérique, vous doit dire explicitement le commutateur de faire ainsi avec la **`comptabilité de périphérique-capteur de`** commande

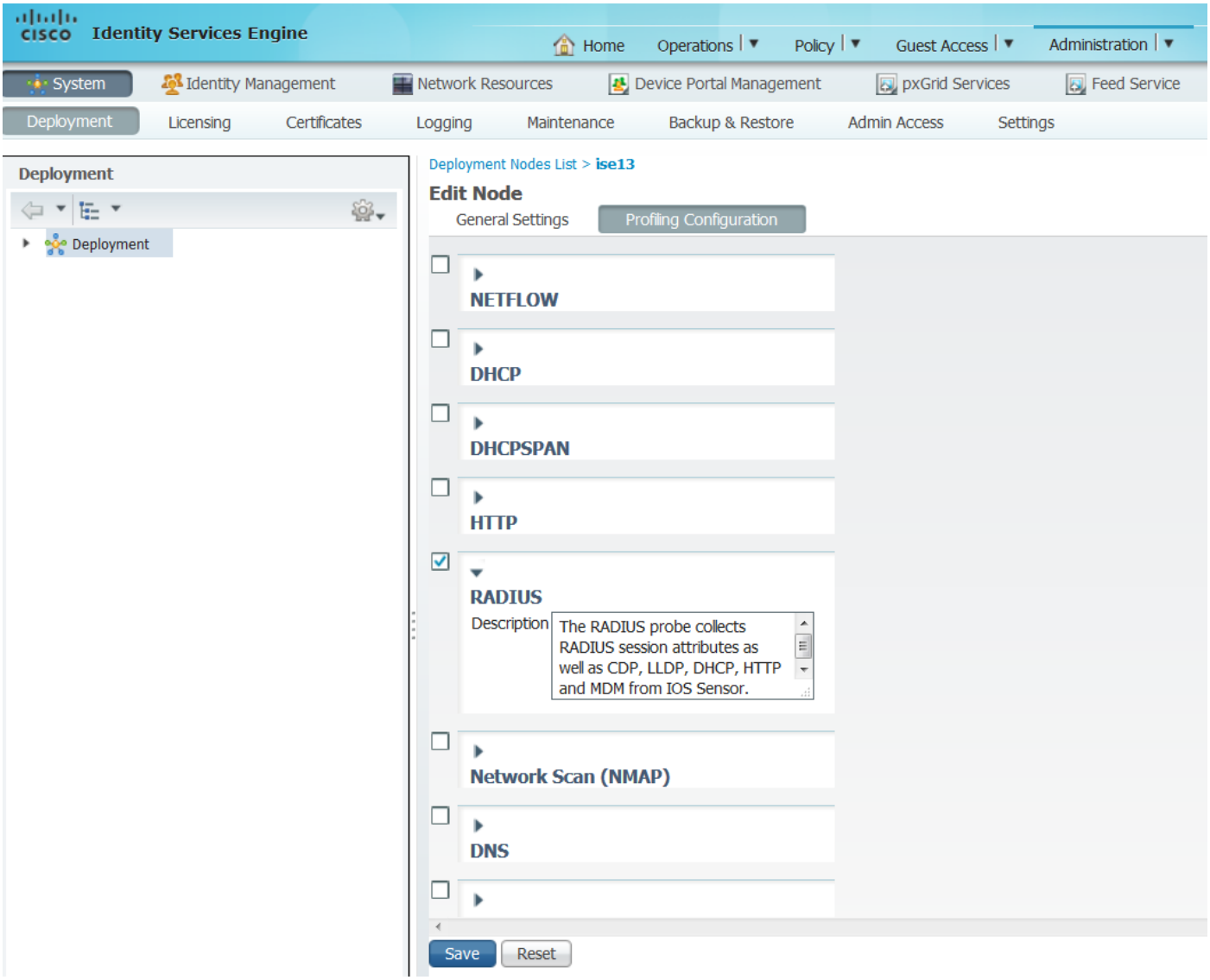
```
!device-sensor filter-list cdp list cdp-list tlv name device-name
 tlv name platform-type!device-sensor filter-list lldp list lldp-list tlv name system-
description!device-sensor filter-spec lldp include list lldp-listdevice-sensor filter-spec cdp
include list cdp-list!device-sensor accountingdevice-sensor notify all-changes!
```

Étape 3. Configure profilant sur ISE

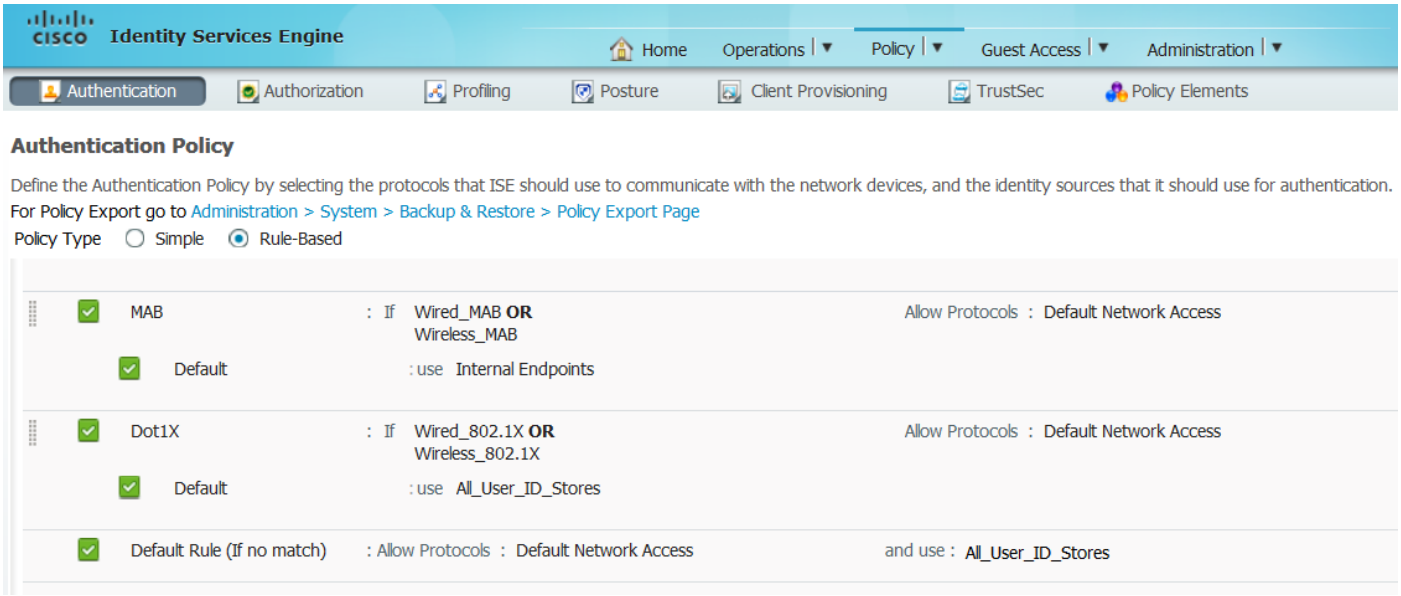
1. Ajoutez le commutateur comme périphérique de réseau dans des « périphériques d'Administration>Network Resources>Network ». Utilisez la clé de serveur de rayon du commutateur en tant que secret partagé dans des configurations d'authentification :



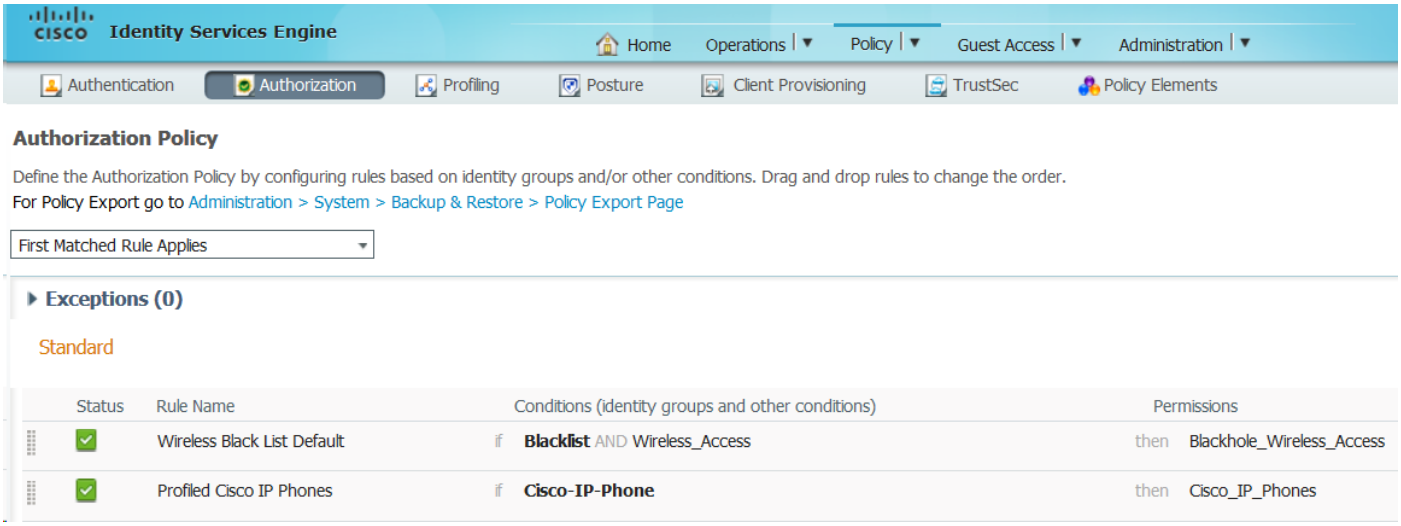
2. Sonde de rayon d'enable sur le noeud de profilage dans « la configuration node>Profiling d'Administration>System>Deployment>ISE ». Si tous les Noeuds RPC sont utilisés pour le profilage, activez la sonde sur tous :



3. Configurez les règles d'authentification ISE. Dans l'exemple les règles d'authentification par défaut préconfigurées sur ISE sont utilisées :

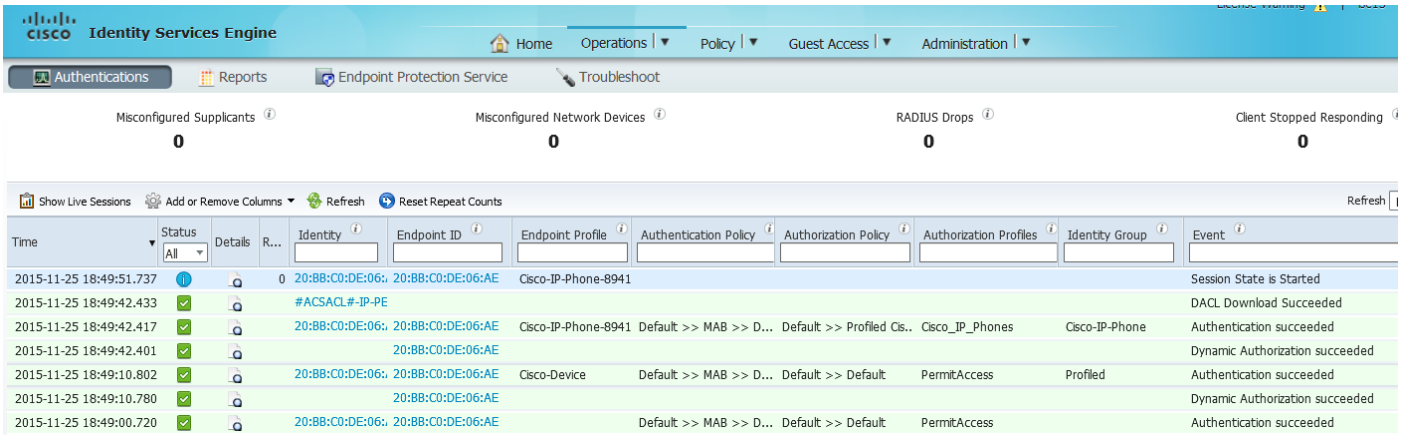


4. Configurez les règles d'autorisation ISE. « La règle des téléphones IP profilés de Cisco est utilisée, qui est préconfigurée sur ISE :



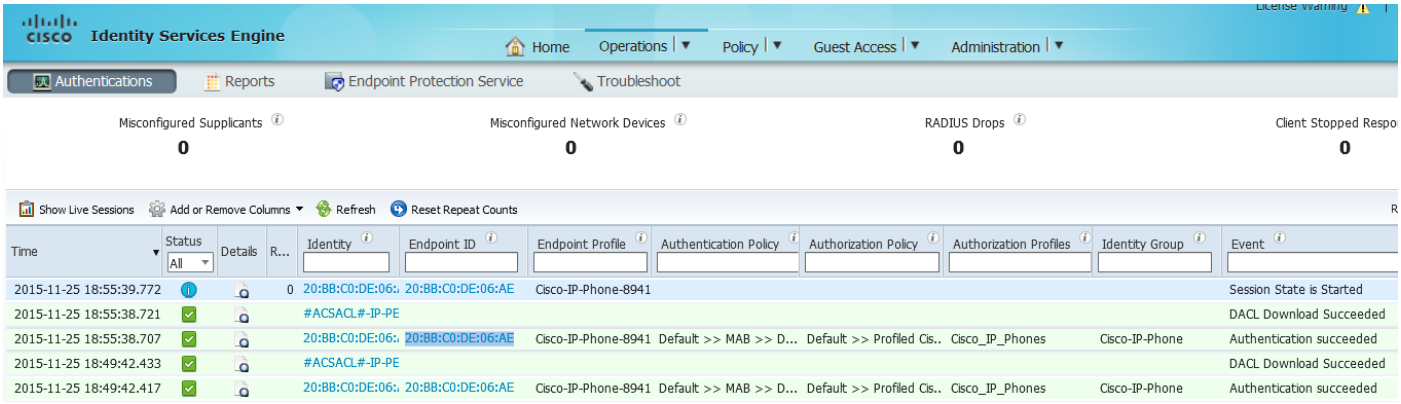
Vérifiez

Afin de vérifier si le profilage fonctionne correctement, référez-vous s'il vous plaît à « Operations>Authentications » sur ISE :

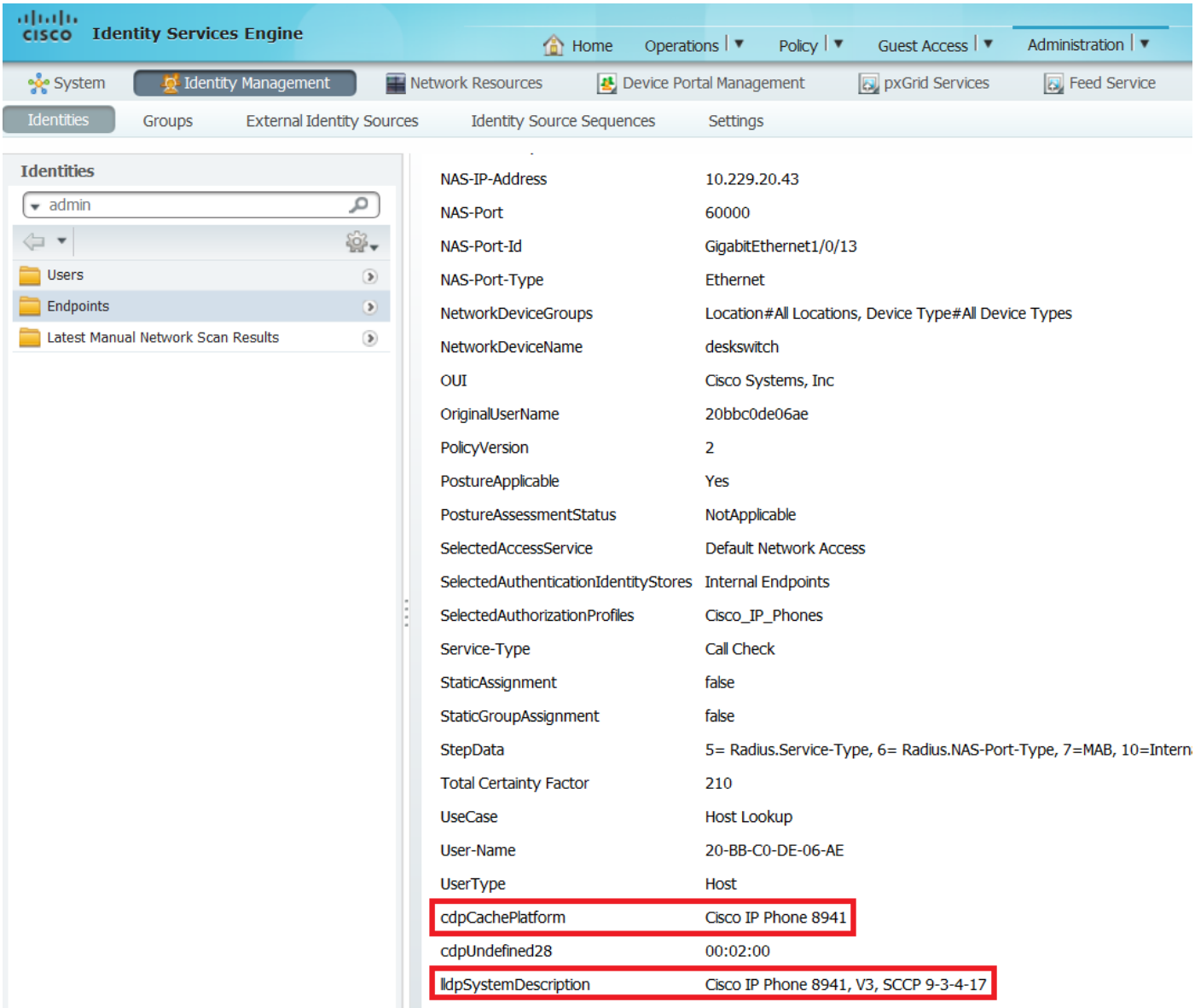


D'abord le périphérique a été authentifié utilisant le MAB (18:49:00). Dix secondes plus tard (18:49:10) il reprofiled comme Cisco-périphérique et finalement après 42 secondes puisque les premières authentifications (18:49:42) il ont reçu le profil Cisco-IP-Phone-8941. En conséquence ISE renvoie la particularité de profil d'autorisation pour des Téléphones IP (Cisco_IP_Phones) et l'ACL téléchargeable qui permet tout le trafic (IP d'autorisation tout). Veuillez noter que dans ce scénario le périphérique inconnu a accès de base au réseau. Il peut être réalisé en ajoutant le MAC address à la base de données interne de point final ISE ou en permettant l'accès au réseau très de base pour les périphériques précédemment inconnus.

> **Le profilage initial a pris environ 40 secondes dans cet exemple. Sur la prochaine authentification ISE déjà connaît le profil et corrige des attributs (autorisation de joindre le domaine de Voix et le DACL) est appliqué immédiatement, à moins qu'ISE reçoive nouveaux/mis à jour attributs et il a besoin reprofile du périphérique de nouveau.**



Dans le « point final d'Administration>Identity Management>Identities>Endpoints>tested » vous pouvez voir que ce qui attribue un peu ont été collectés par la sonde de rayon et ce que sont leurs valeurs :



Comme vous pouvez observer tout le facteur de certitude calculé est 210 dans ce scénario. Il est livré le fromt le fait que le point final a apparié également le profil de Cisco-périphérique (avec le facteur total de certitude de 30) et le profil de Cisco-IP-téléphone (avec le facteur total de certitude de 40). Puisque le profileur a apparié les deux conditions dans le profil Cisco-IP-Phone-8941, le facteur de certitude pour ce profil est 140 (70 pour chaque attribut selon profiler la stratégie). Pour résumer : 30+40+70+70=210.

Dépannez

Étape 1. Vérifiez les informations collectées par CDP/LLDP

```
switch#sh cdp neighbors g1/0/13 detail-------------------------Device ID: SEP20BBC0DE06AEEntry
address(es):Platform: Cisco IP Phone 8941 ,  Capabilities: Host Phone Two-port Mac
RelayInterface: GigabitEthernet1/0/13,  Port ID (outgoing port): Port 1Holdtime : 178 secSecond
Port Status: DownVersion :SCCP 9-3-4-17advertisement version: 2Duplex: fullPower drawn: 3.840
WattsPower request id: 57010, Power management id: 3Power request levels are:3840 0 0 0 0Total
cdp entries displayed : 1

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
```

Si vous ne pouvez voir aucune données collectées pour vérifier ce qui suit :

- Vérifiez l'état de session d'authentification sur le commutateur (il devrait être réussi) :
  ```
  piborowi#show authentication sessions int g1/0/13 details            Interface:
  GigabitEthernet1/0/13          MAC Address:  20bb.c0de.06ae         IPv6 Address:  Unknown
  IPv4 Address:  Unknown            User-Name:  20-BB-C0-DE-06-AE               Status:
  Authorized               Domain:  VOICE       Oper host mode:  multi-domain     Oper control
  dir:  both      Session timeout:  N/A    Common Session ID:  0AE518200000020400 99C216
  Acct Session ID:  0x00000016               Handle:  0xAC0001F6       Current Policy:
  POLICY_Gi1/0/13Local Policies:        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
  (priority 150)Server Policies:Method status list:       Method           State       dot1x
  Stopped       mab              Authc Success
  ```
- Vérifiez si des protocoles de CDP et de LLDP sont activés. Vérifiez s'il y a des commandes de non-par défaut concernant CDP/LLDP/etc. et comment ceux peuvent affecter la récupération d'attribut du point final
  ```
  switch#sh running-config all | in cdp runcdp runswitch#sh running-config all | in lldp
  runlldp run
  ```
- Vérifiez dans le guide de configuration pour votre point final s'il prend en charge CDP/LLDP/etc

Étape 2. Cache de capteur de périphérique de contrôle

```
switch#show device-sensor cache interface g1/0/13Device: 20bb.c0de.06ae on port
GigabitEthernet1/0/13-------------------------------------------------Proto Type:Name
Len ValueLLDP     6:system-description          40 0C 26 43 69 73 63 6F 20 49 50 20 50 68 6F 6E
65                                        20 38 39 34 31 2C 20 56 33 2C 20 53 43 43 50 20
39 2D 33 2D 34 2D 31 37CDP      6:platform-type               24 00 06 00 18 43 69 73 63 6F 20
49 50 20 50 68 6F                                        6E 65 20 38 39 34 31 20CDP
28:secondport-status-type       7 00 1C 00 07 00 02 00
```

Si vous ne voyez pas aucune donnée dans ce domaine ou les informations n'est complète vérifie des commandes de « périphérique-capteur », en particulier des filters-list et des filtre-spécifications.

Étape 3. Vérifiez si les attributs sont présents en comptabilité de rayon

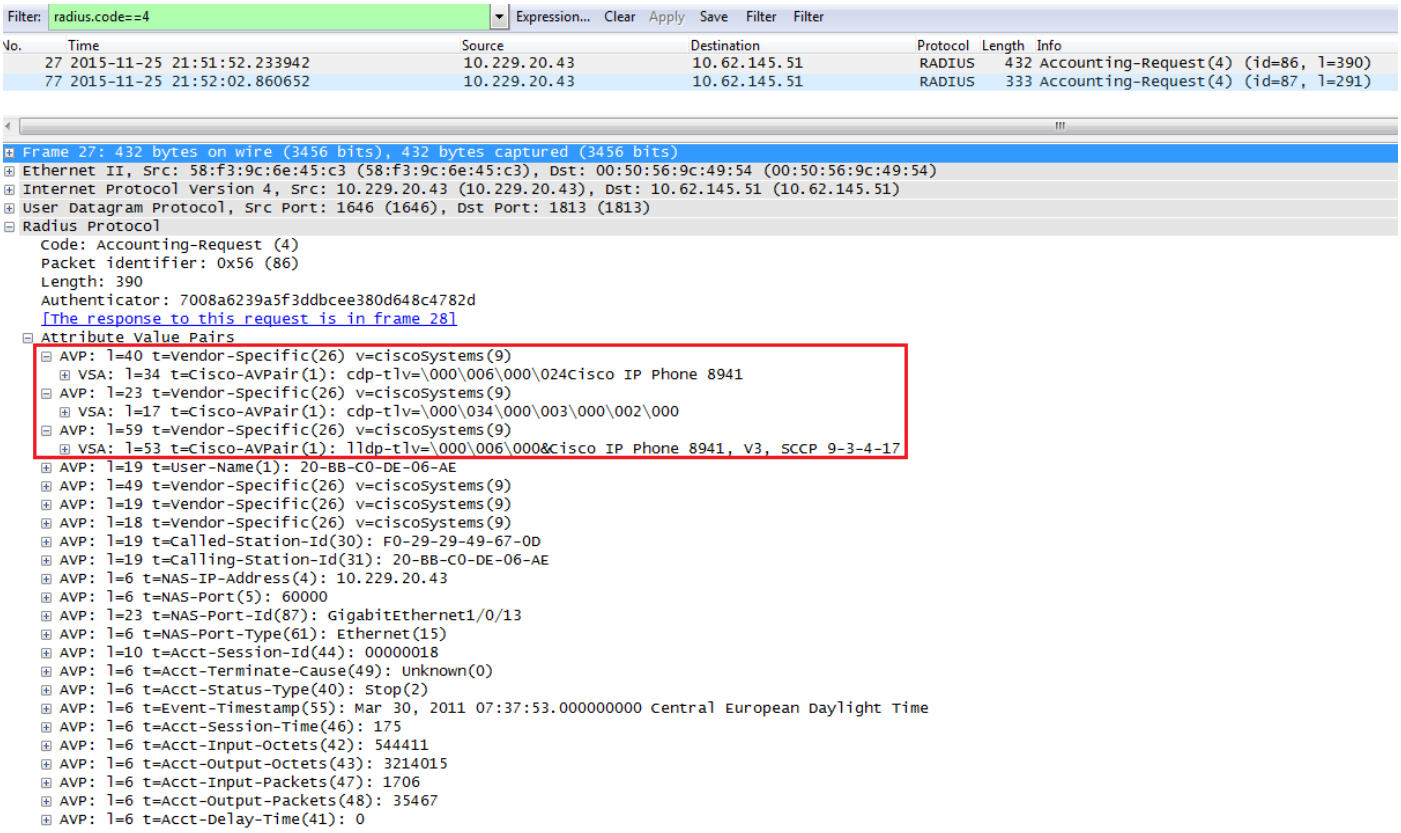
Vous pouvez vérifier cela utilisant la « commande des debugs radius sur le commutateur ou exécuter la capture de paquet entre le commutateur et l'ISE.

Le rayon mettent au point :

```
Mar 30 05:34:58.716: RADIUS(00000000): Send Accounting-Request to 1.1.1.1:1813 id 1646/85, len
378Mar 30 05:34:58.716: RADIUS:  authenticator 17 DA 12 8B 17 96 E2 0F - 5D 3D EC 79 3C ED 69
20Mar 30 05:34:58.716: RADIUS:  Vendor, Cisco       [26]  40Mar 30 05:34:58.716: RADIUS:   Cisco
AVpair       [1]   34  "cdp-tlv= "Mar 30 05:34:58.716: RADIUS: Vendor, Cisco [26] 23Mar 30
05:34:58.716: RADIUS: Cisco AVpair [1] 17 "cdp-tlv= "Mar 30 05:34:58.721: RADIUS: Vendor, Cisco
[26] 59Mar 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: Vendor, Cisco [26] 49Mar 30
05:34:58.721: RADIUS: Cisco AVpair [1] 43 "audit-session-id=0AE518200000022800E2481C"Mar 30
05:34:58.721: RADIUS: Vendor, Cisco [26] 19Mar 30 05:34:58.721: RADIUS: Cisco AVpair [1] 13
"vlan-id=101"Mar 30 05:34:58.721: RADIUS: Vendor, Cisco [26] 18Mar 30 05:34:58.721: RADIUS:
Cisco AVpair [1] 12 "method=mab"Mar 30 05:34:58.721: RADIUS: Called-Station-Id [30] 19 "F0-29-
29-49-67-0D"Mar 30 05:34:58.721: RADIUS: Calling-Station-Id [31] 19 "20-BB-C0-DE-06-AE"Mar 30
05:34:58.721: RADIUS: NAS-IP-Address [4] 6 10.229.20.43Mar 30 05:34:58.721: RADIUS: NAS-Port [5]
6 60000Mar 30 05:34:58.721: RADIUS: NAS-Port-Id [87] 23 "GigabitEthernet1/0/13"Mar 30
05:34:58.721: RADIUS: NAS-Port-Type [61] 6 Ethernet [15]Mar 30 05:34:58.721: RADIUS: Acct-
Session-Id [44] 10 "00000018"Mar 30 05:34:58.721: RADIUS: Acct-Status-Type [40] 6 Watchdog
[3]Mar 30 05:34:58.721: RADIUS: Event-Timestamp [55] 6 1301463298Mar 30 05:34:58.721: RADIUS:
Acct-Input-Octets [42] 6 538044Mar 30 05:34:58.721: RADIUS: Acct-Output-Octets [43] 6 3201914Mar
30 05:34:58.721: RADIUS: Acct-Input-Packets [47] 6 1686Mar 30 05:34:58.721: RADIUS: Acct-Output-
Packets [48] 6 35354Mar 30 05:34:58.721: RADIUS: Acct-Delay-Time [41] 6 0Mar 30 05:34:58.721:
```

```
RADIUS(00000000): Sending a IPv4 Radius PacketMar 30 05:34:58.721: RADIUS(00000000): Started 5
sec timeoutMar 30 05:34:58.737: RADIUS: Received from id 1646/85 10.62.145.51:1813, Accounting-
response, len 20
```

Capture de paquet :



Étape 4. Vérifiez le profileur met au point sur ISE

Si les attributs étaient envoyés du commutateur, il est possible de vérifier s'ils étaient reçus sur ISE. Afin de vérifier ceci, activez s'il vous plaît le profileur met au point pour le noeud correct RPC (log Configuration>PSN>profiler>debug d'Administration>System>Logging>Debug) et exécute l'authentification du point final une fois de plus.

Look for après les informations :

- Debug indiquant que la sonde de rayon reçue attribue :

```
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=0AE518200000020400 99C216, cisco-av-pair=vlan-id=101,
cisco-av-pair=method=mab, AcsSessionID=ise13/235487054/2511, SelectedAccessService=Default
Network Access,
Step=11004, Step=11017, Step=15049, Step=15008, Step=15004, Step=11005,
NetworkDeviceGroups=Location#All Locations,
```

```
NetworkDeviceGroups=Device Type#All Device Types, Service-Type=Call Check,
CPMSessionID=0AE518200000020400 99C216,
AllowedProtocolMatchedRule=MAB, Location=Location#All Locations, Device Type=Device Type#All
Device Types, ]
```

- Debug indiquant que des attributs ont été avec succès analysés :

```
2015-11-25 19:29:53,642 DEBUG  [RADIUSParser-1-thread-1][]
cisco.profiler.probes.radius.RadiusParser -:::- Parsed IOS Sensor 1: cdpCachePlatform=[Cisco
IP Phone 8941]2015-11-25 19:29:53,642 DEBUG  [RADIUSParser-1-thread-1][]
cisco.profiler.probes.radius.RadiusParser -:::- Parsed IOS Sensor 2:
cdpUndefined28=[00:02:00]2015-11-25 19:29:53,642 DEBUG  [RADIUSParser-1-thread-1][]
cisco.profiler.probes.radius.RadiusParser -:::- Parsed IOS Sensor 3:
lldpSystemDescription=[Cisco IP Phone 8941, V3, SCCP
```

- Débuggez indiquer que des attributs sont traités par l'expéditeur :

```
2015-11-25 19:29:53,643 DEBUG  [forwarder-6][]
cisco.profiler.infrastructure.probemgr.Forwarder -:20:BB:C0:DE:06:AE:ProfilerCollection:-
Endpoint Attributes:ID:nullName:nullMAC: 20:BB:C0:DE:06:AE        Attribute:AAA-Server
value:ise13        (... more attributes ...)        Attribute:User-Name      value:20-BB-C0-
DE-06-AE        Attribute:cdpCachePlatform value:Cisco IP Phone 8941
Attribute:cdpUndefined28 value:00:02:00 Attribute:lldpSystemDescription value:Cisco IP Phone
8941, V3, SCCP 9-3-4-17 Attribute:SkipProfiling value:false
```

Un expéditeur enregistre des points finaux dans la base de données de Cisco ISE avec leurs données d'attributs, et puis informe l'analyseur de nouveaux points finaux détectés sur votre réseau. L'analyseur classifie des points finaux à l'identité de point final groupe et enregistre des points finaux avec les profils appariés dans la base de données.

Étape 5. Typiquement après que de nouveaux attributs soient ajoutés à la collection existante pour l'appareil spécifique, ces périphérique/point final est ajouté à profiler la file d'attente afin de vérifier si elle doit être assignée le profil différent basé sur de nouveaux attributs :

```
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 ExceptionRuleMatched:false
```

Informations connexes

1. http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/howto_30_ise_profiling.pdf

2. http://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_prof_pol.html