Configurar o sensor do dispositivo para o perfilamento ISE

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Configurar
Etapa 1. Configuração de AAA padrão
Etapa 2. Configurar o sensor do dispositivo
Etapa 3. Configure que perfila no ISE
Verificar
Troubleshooting
Etapa 1. Verifique a informações recolhidas por CDP/LLDP
Etapa 2. Verifique o esconderijo do sensor do dispositivo
Etapa 3. Verifique se os atributos estam presente na contabilidade do raio
Etapa 4. Verifique que o perfilador debuga no ISE
Informações Relacionadas
Cisco relacionado apoia discussões da comunidade

Introdução

Este documento descreve como configurar o sensor do dispositivo, de modo que possa ser usado perfilando finalidades no ISE. O sensor do dispositivo é uma característica dos dispositivos de acesso. Reserva recolher a informação sobre valores-limite conectados. Na maior parte, a informações recolhidas pelo sensor do dispositivo pode vir dos seguintes protocolos:

- Cisco Discovery Protocol (CDP)
- Protocolo de descoberta da camada de enlace (LLDP)
- Protocolo de Configuração de Host Dinâmico (DHCP)

Em algumas Plataformas é possível usar igualmente H323, o SORVO (protocolo de iniciação de sessão), o MDNS (definição do domínio do Multicast) ou os protocolos HTTP. As possibilidades de configuração para capacidades do sensor do dispositivo podem variar do protocolo ao protocolo. Como um exemplo acima de está disponível no Cisco catalyst 3850 com software 03.07.02.E.

Uma vez que a informação é recolhida, pode ser encapsulada na contabilidade do raio e enviar a um server de perfilamento. Nesta identidade do artigo preste serviços de manutenção ao motor (ISE) é usado como um server de perfilamento.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Protocolo de raio
- CDP, LLDP e protocolos DHCP
- Motor do serviço da identidade de Cisco
- Interruptor 2960 do Cisco catalyst

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Correção de programa 3 da versão 1.3 do motor do serviço da identidade de Cisco
- Versão 15.2(2a)E1 do interruptor 2960s do Cisco catalyst
- Versão SCCP 9-3-4-17 do Cisco IP Phone 8941

Configurar

Etapa 1. Configuração de AAA padrão

A fim configurar a autenticação, a autorização e a contabilidade (AAA), seguem as etapas abaixo:

1. Permita o AAA usando o **comando aaa new-model** e permita o 802.1X globalmente no interruptor

2. Configurar o servidor Radius e permita a autorização dinâmica (mudança da autorização - o CoA)

3. Permita protocolos CDP e LLDP

4. Adicionar a configuração de autenticação do switchport

```
!
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
!
```

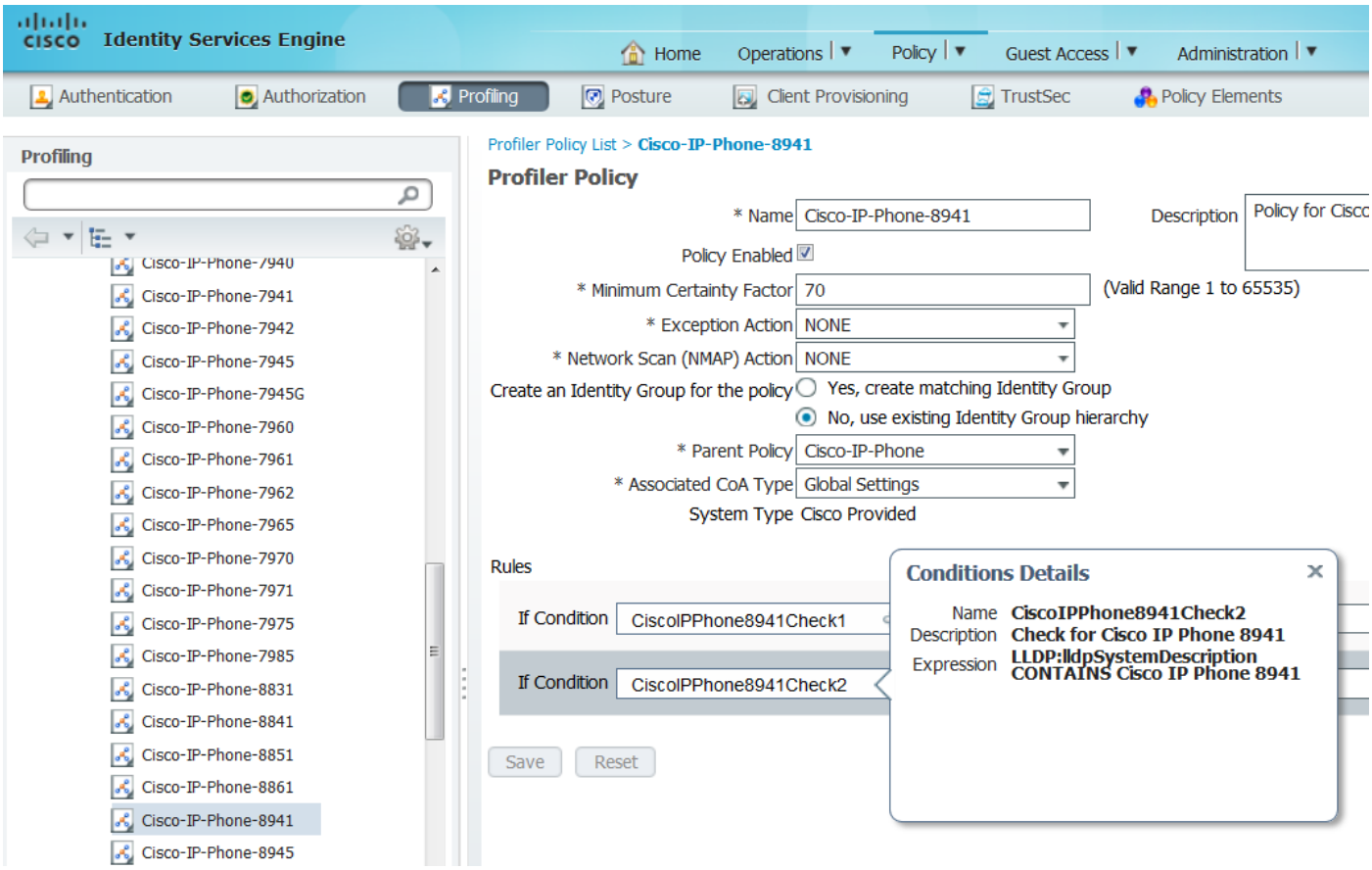
> **Em um comando radius-server vsa send mais novo da versão de software a contabilidade é permitida à revelia. Se você não pode ver atributos enviar na**

contabilidade, verifique se o comando no permitido.

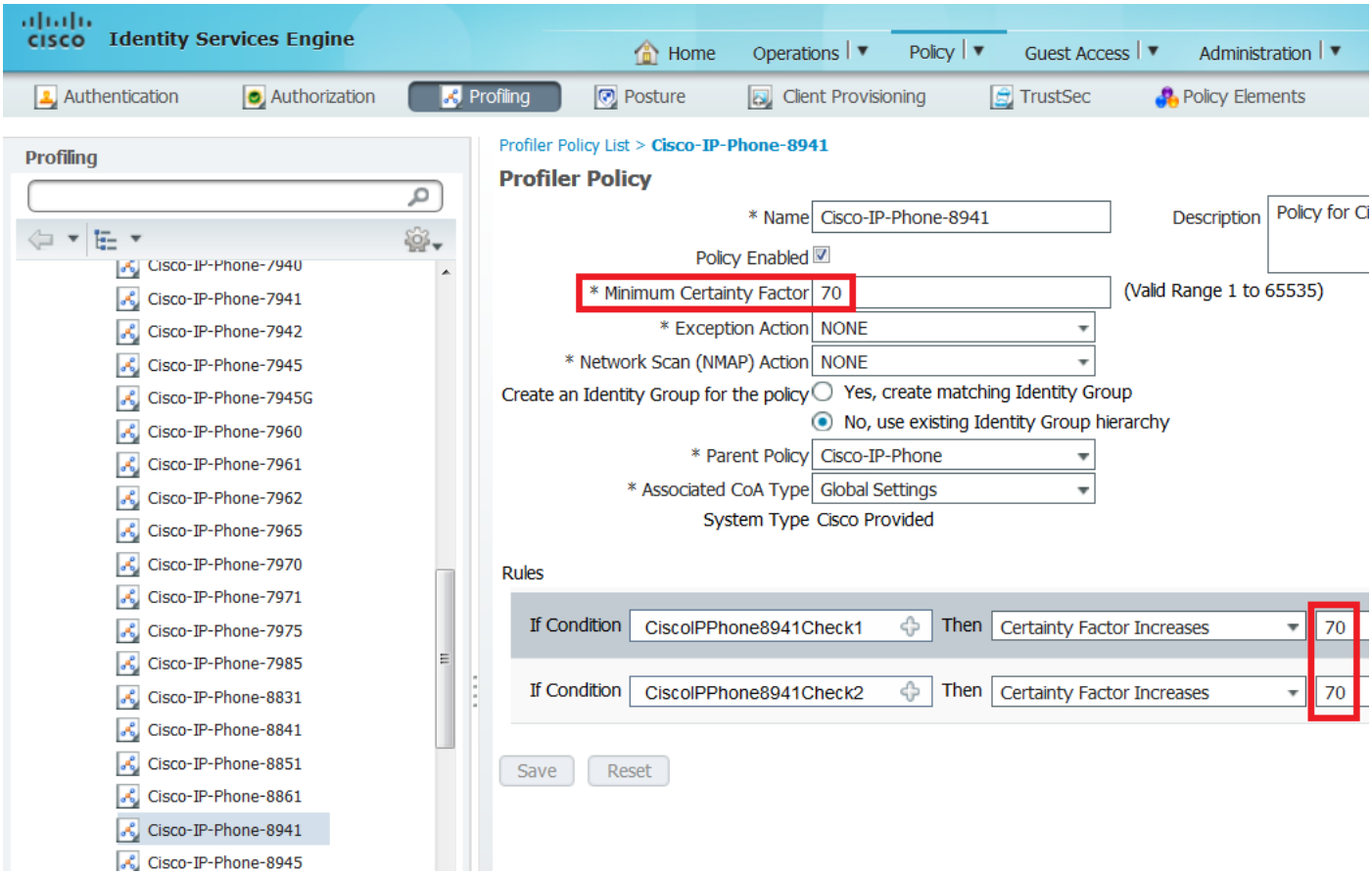
Etapa 2. Configurar o sensor do dispositivo

1. Determine que atributos de CDP/LLDP são precisados de perfilar o dispositivo. Em caso do Cisco IP Phone 8941 você pode usar o seguinte:

- Atributo LLDP SystemDescription
- Atributo CDP CachePlatform



Para nossa finalidade seria bastante para obter apenas um daqueles desde que ambos eles fornecem um aumento da fábrica da certeza de 70 e a fábrica mínima da certeza exigida para ser perfilado como Cisco-IP-Phone-8941 é 70:



A fim para ser perfilado como o Cisco IP Phone específico, youneed para satisfazer condições mínimas para todos os perfis do pai. Isto significa que o perfilador precisa de combinar o dispositivo Cisco (fator mínimo 10 da certeza) e o Cisco IP Phone (fator mínimo 20 da certeza). Mesmo que o perfilador combine aqueles dois perfis, deve ainda ser perfilado como o Cisco IP Phone específico desde que cada modelo do telefone IP tem um fator mínimo da certeza de 70. O dispositivo é atribuído ao perfil para que tem o fator o mais alto da certeza.

2. Configurar duas listas de filtro - uma para o CDP e outra para LLDP. Aqueles indicam que qual atribui deve ser incluído em mensagens da contabilidade do raio. Esta etapa é opcional

3. Crie dois filtro-SPEC para o CDP e o LLDP. Em especs. do fiter você pode qualquer um indicar que a lista de atributos deve ser incluída ou excluída das mensagens da contabilidade. No exemplo os atributos de seguimento são incluídos:

- nome de dispositivo do CDP
- descrição do sistema de LLDP

Você pode configurar os atributos adicionais a ser transmited através do raio ao ISE se necessário. Esta etapa é igualmente opcional.

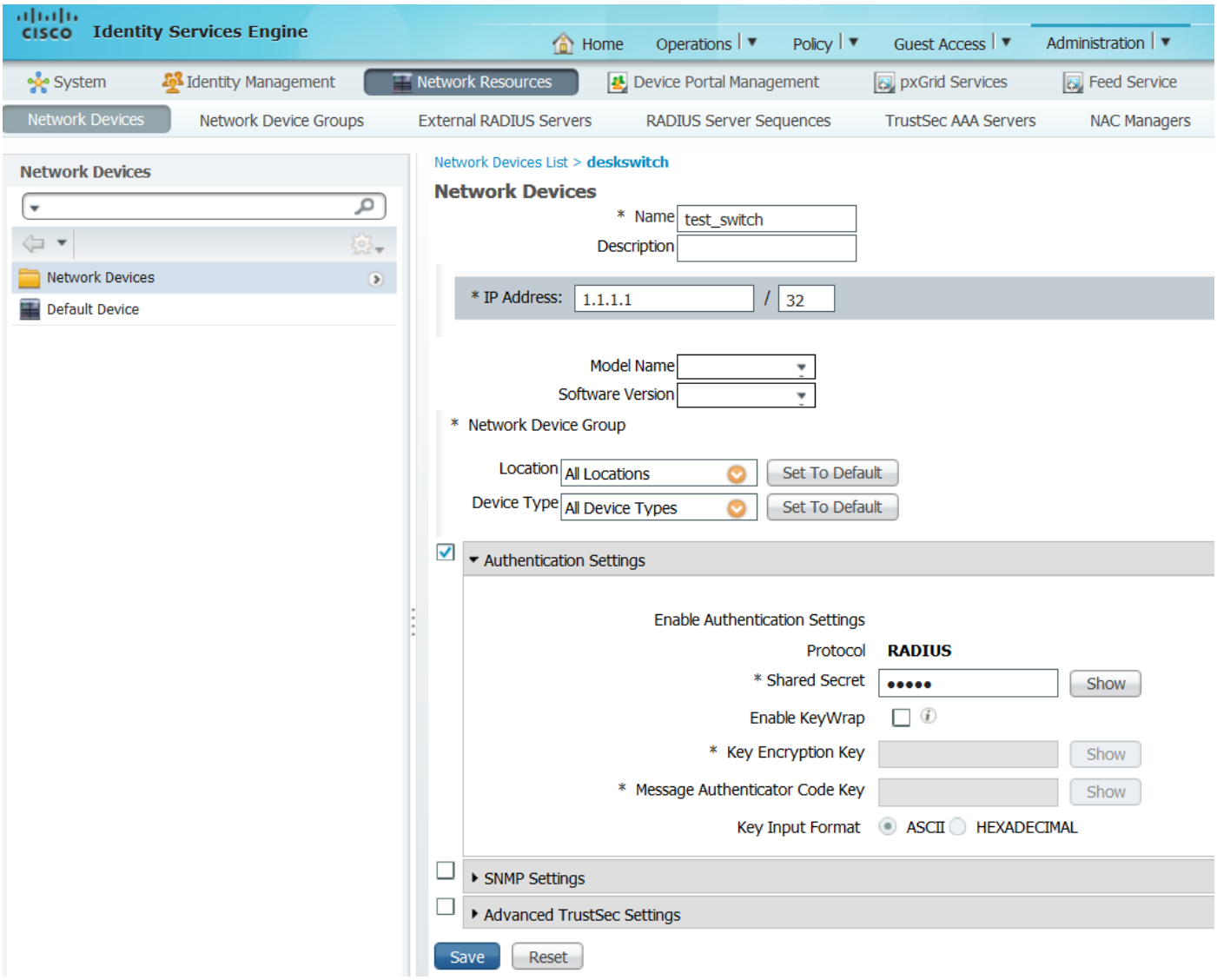
4. **`O dispositivo-sensor do`** comando Add **`notifica todo-mudanças`**. Provoca atualizações sempre que os TLV são adicionados, alterados ou removidos para a sessão atual

5. A fim enviar realmente a informação recolhida através da funcionalidade de sensor do dispositivo, você precisa de dizer explicitamente o interruptor para fazer assim com **`contabilidade do dispositivo-sensor do`** comando

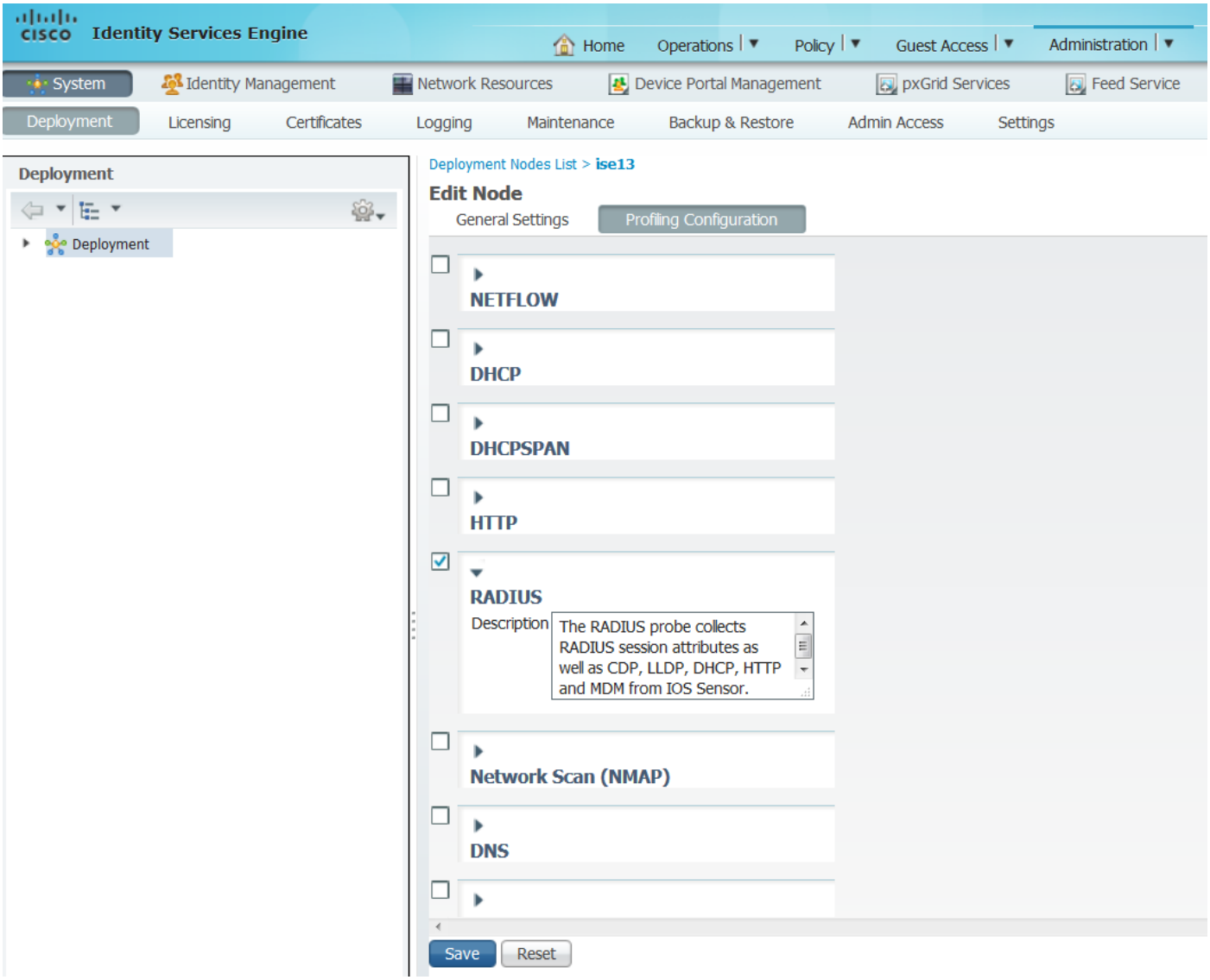
```
!
device-sensor filter-list cdp list cdp-list
 tlv name device-name
 tlv name platform-type ! device-sensor filter-list lldp list lldp-list tlv name system-
description ! device-sensor filter-spec lldp include list lldp-list device-sensor filter-spec
cdp include list cdp-list ! device-sensor accounting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

Etapa 3. Configure que perfila no ISE

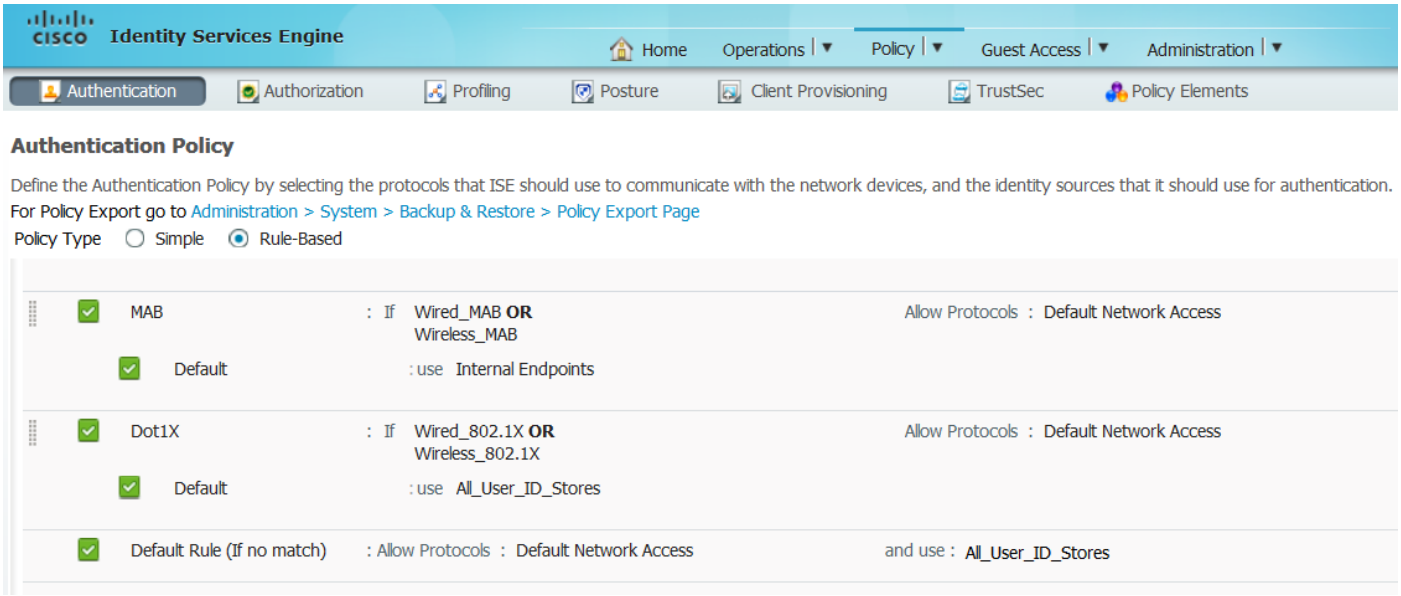
1. Adicionar o interruptor como um dispositivo de rede de “em dispositivos Administration>Network Resources>Network”. Use a chave do servidor Radius do interruptor como o segredo compartilhado em ajustes da autenticação:



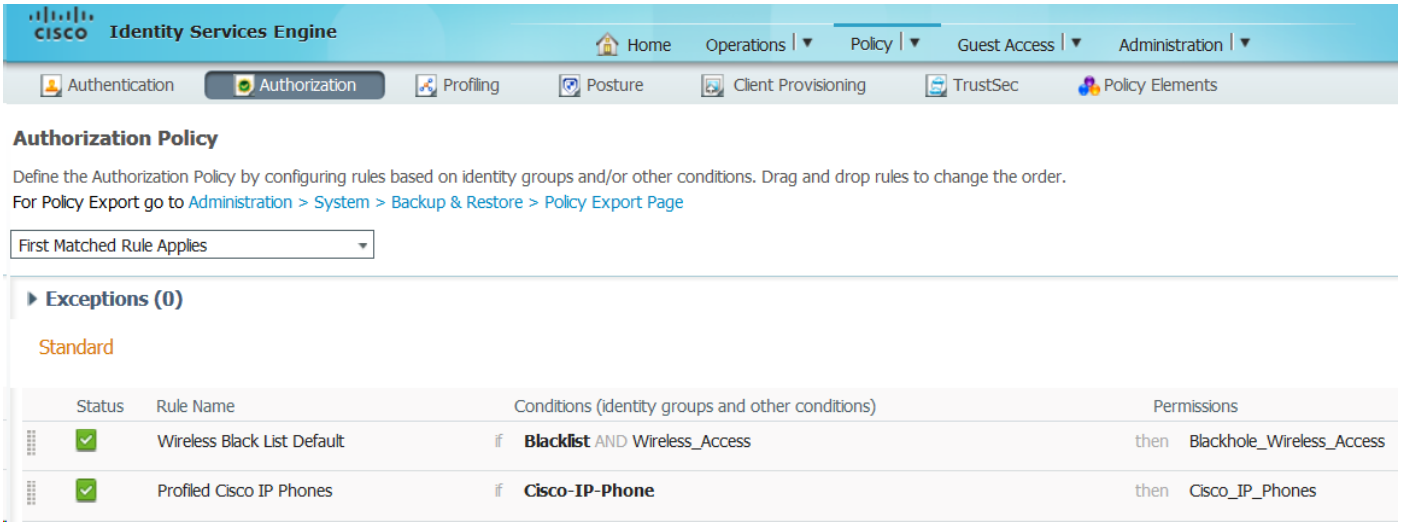
2. Permita a ponta de prova do raio no nó de perfilamento de “na configuração node>Profiling Administration>System>Deployment>ISE”. Se todos os Nós PSN forem usados perfilando, permita a ponta de prova em todo:



3. Configurar regras da autenticação ISE. No exemplo as regras da autenticação padrão preconfigured no ISE são usadas:

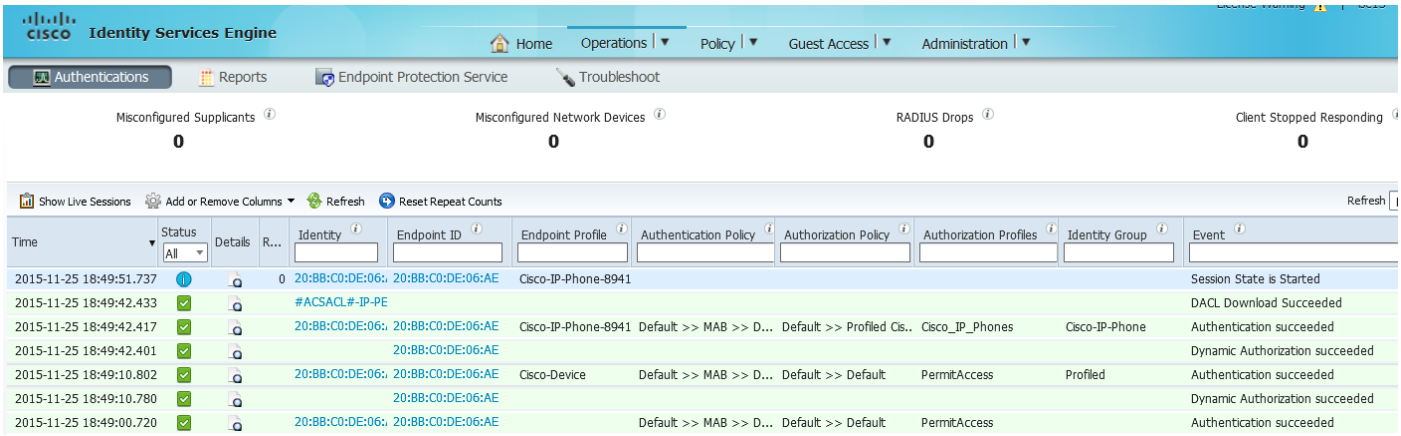


4. Configurar regras da autorização ISE. “A regra dos telefones IP perfilados de Cisco é usada, que preconfigured no ISE:



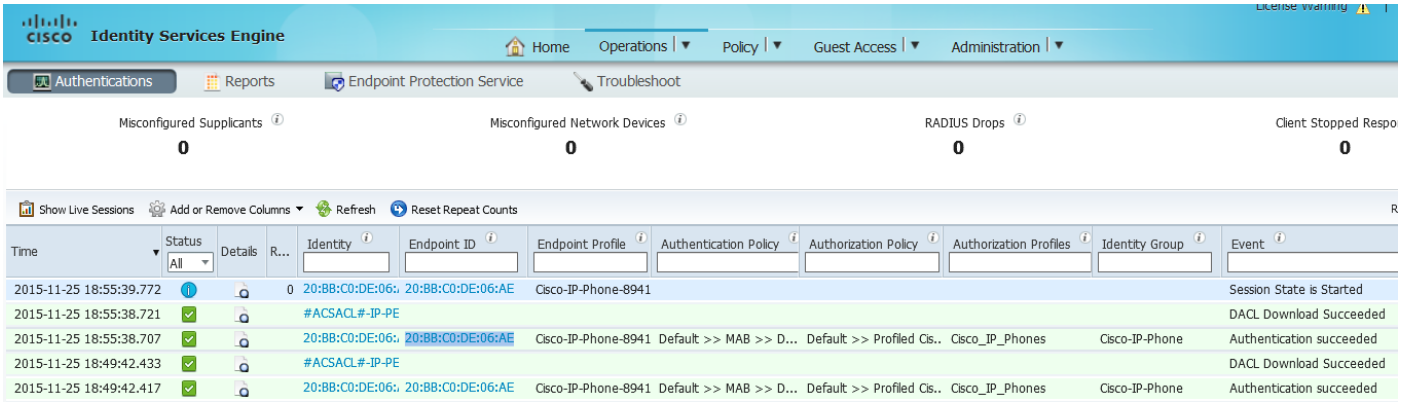
Verificar

A fim verificar se perfilar está trabalhando corretamente, refira por favor “Operations>Authentications” no ISE:

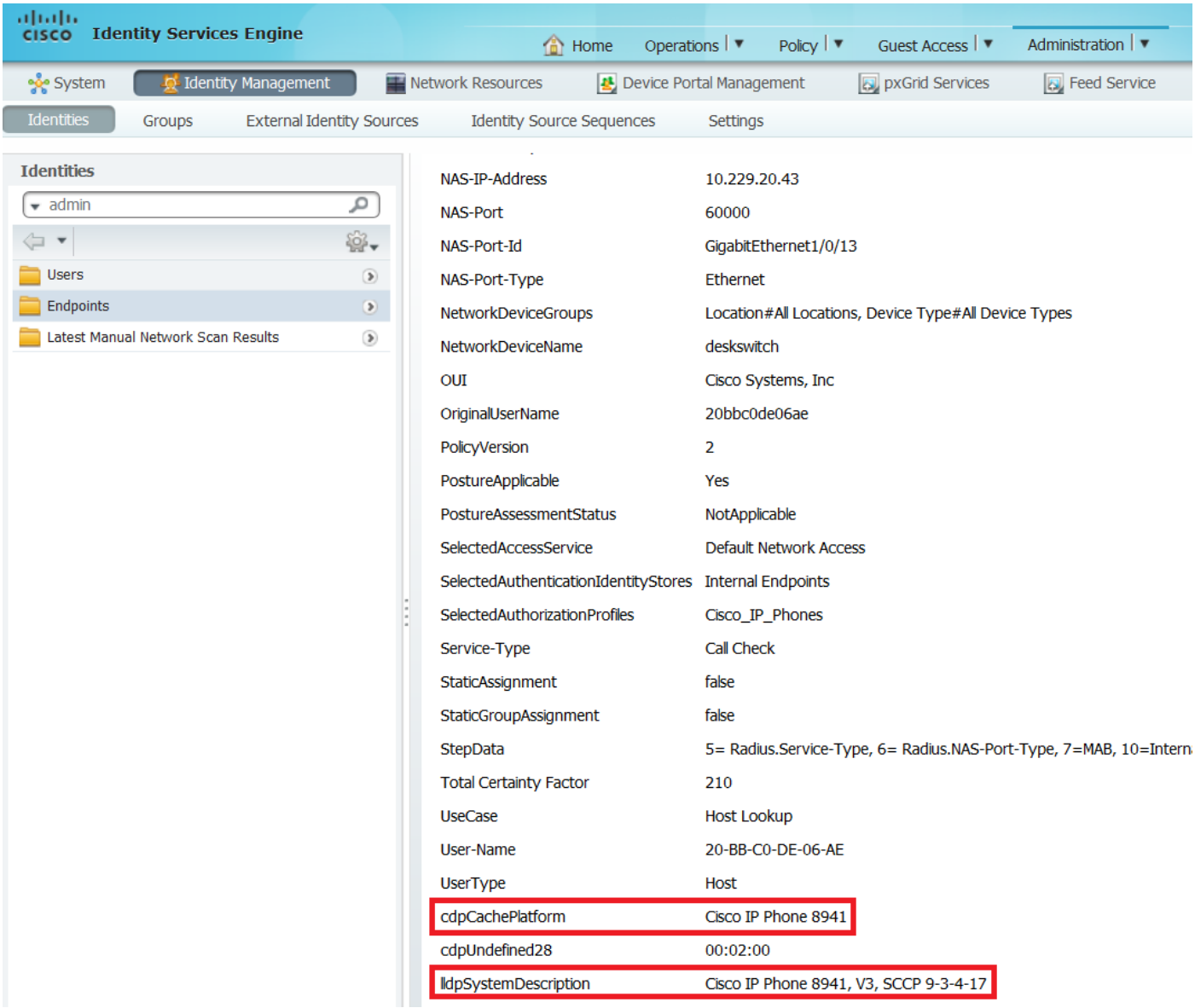


O dispositivo foi autenticado primeiramente usando MAB (18:49:00). Dez segundos depois (18:49:10) reprofiled como o dispositivo Cisco e finalmente após 42 segundos desde que as primeiras autenticações (18:49:42) ele receberam o perfil Cisco-IP-Phone-8941. Em consequência o ISE retornam o específico do perfil da autorização para Telefones IP (Cisco_IP_Phones) e ACL baixável que permite todo o tráfego (licença IP alguma). Note por favor que nesta encenação o dispositivo desconhecido tem o acesso básico à rede. Pode ser conseguido adicionando o MAC address ao base de dados interno do valor-limite ISE ou permitindo muito o acesso de rede básica para previamente dispositivos desconhecidos.

> **O perfilamento inicial tomou ao redor 40 segundos neste exemplo. Na autenticação seguinte ISE já conhece o perfil e corrigem atributos (permissão se juntar ao domínio da Voz e ao DACL) estão aplicados imediatamente, a menos que o ISE receber atributos novos/actualizados e precisar reprofile o dispositivo outra vez.**



De “no valor-limite Administration>Identity Management>Identities>Endpoints>tested” você pode ver que tipo dos atributos foi recolhido pela ponta de prova do raio e quais seus valores são:



Como você pode observar o fator total da certeza computado é 210 nesta encenação. Vem fromt o fato de que o valor-limite combinou igualmente o perfil do dispositivo Cisco (com fator total da certeza de 30) e o perfil do Cisco IP Phone (com fator total da certeza de 40). Desde que o perfilador combinou ambas as condições no perfil Cisco-IP-Phone-8941, o fator da certeza para este perfil é 140 (70 para cada atributo de acordo com o perfilamento da política). Para resumir: 30+40+70+70=210.

Troubleshooting

Etapa 1. Verifique a informações recolhidas por CDP/LLDP

```
switch#sh cdp neighbors g1/0/13 detail
------------------------
Device ID: SEP20BBC0DE06AE
Entry address(es):
Platform: Cisco IP Phone 8941 ,  Capabilities: Host Phone Two-port Mac Relay
Interface: GigabitEthernet1/0/13,  Port ID (outgoing port): Port 1
Holdtime : 178 sec
Second Port Status: Down

Version :
SCCP 9-3-4-17

advertisement version: 2
Duplex: full
Power drawn: 3.840 Watts
Power request id: 57010, Power management id: 3
Power request levels are:3840 0 0 0 0


Total 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
```

Se você não pode ver nenhuns dados recolhidos para verificar o seguinte:

- Verifique o estado de sessão da autenticação no interruptor (deve ser bem sucedido):

```
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_Gi1/0/13

Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:

Method status list:
       Method           State
       dot1x            Stopped

       mab              Authc Success
```

- Verifique se os protocolos CDP e LLDP são permitidos. Verifique se há algum comando não-padrão em relação a CDP/LLDP/etc. e como aqueles podem afetar a recuperação do atributo do valor-limite

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

- Verifique no manual de configuração para seu valor-limite se apoia CDP/LLDP/etc

Etapa 2. Verifique o esconderijo do sensor do dispositivo

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

```
Proto Type:Name                       Len Value
LLDP     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 37
CDP      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 20
CDP     28:secondport-status-type       7 00 1C 00 07 00 02 00
```

Se você não vê nenhuns dados nesta campo ou informação não estão completos verificam comandos do “dispositivo-sensor”, em particular listas de filtros e filtro-SPEC.

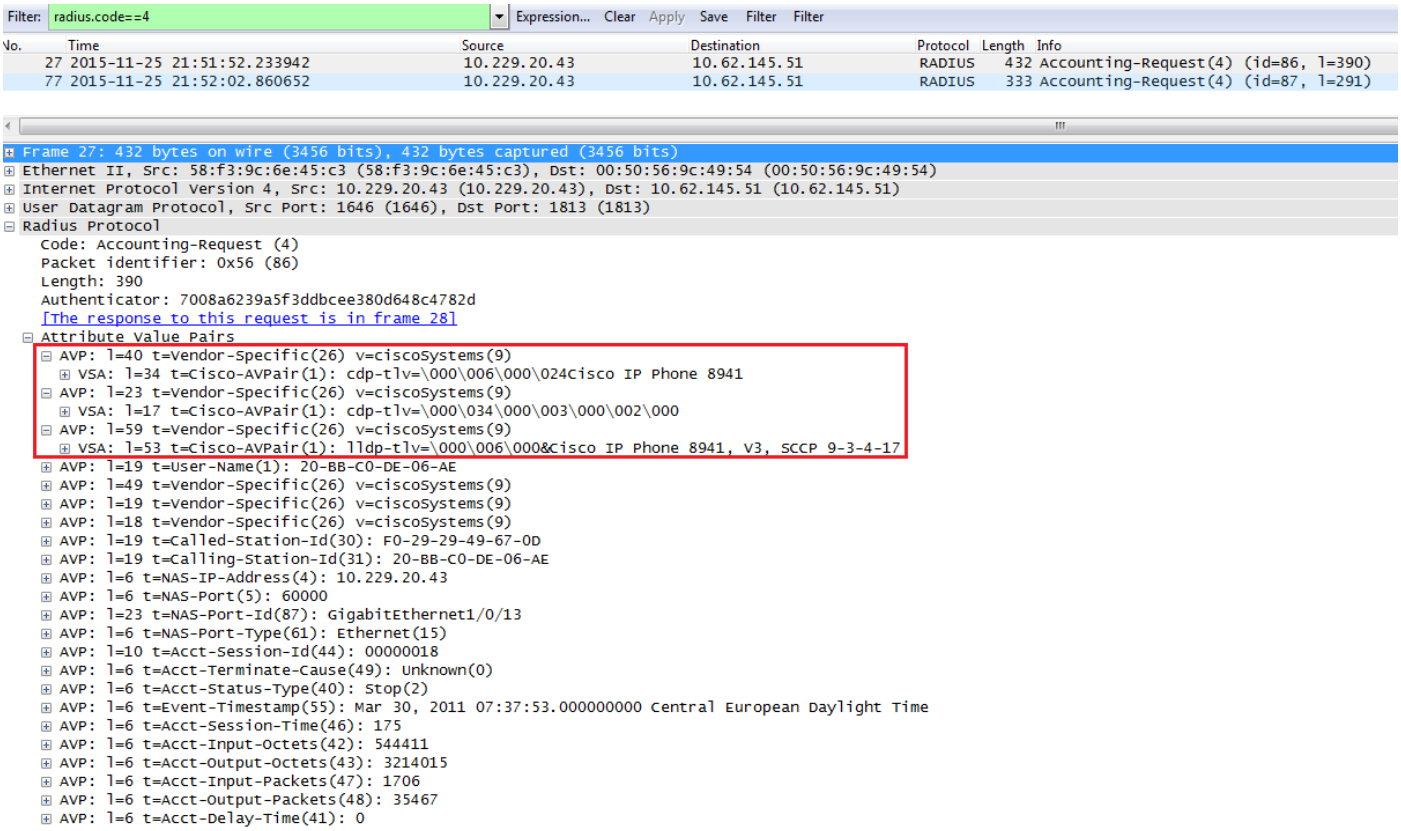
Etapa 3. Verifique se os atributos estam presente na contabilidade do raio

Você pode verificar que usando “debugar o comando do raio” no interruptor ou captura de pacote de informação da execução entre o interruptor e o ISE.

O raio debuga:

```
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 17 DA 12 8B 17 96 E2 0F - 5D 3D EC 79 3C ED 69 20
Mar 30 05:34:58.716: RADIUS:  Vendor, Cisco       [26]  40
Mar 30 05:34:58.716: RADIUS:   Cisco AVpair       [1]   34  "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:  Vendor, Cisco       [26]  49
Mar 30 05:34:58.721: RADIUS:   Cisco AVpair       [1]   43  "audit-session-
id=0AE518200000022800E2481C"
Mar 30 05:34:58.721: RADIUS:  Vendor, Cisco       [26]  19
Mar 30 05:34:58.721: RADIUS:   Cisco AVpair       [1]   13  "vlan-id=101"
Mar 30 05:34:58.721: RADIUS:  Vendor, Cisco       [26]  18
Mar 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   10.229.20.43
Mar 30 05:34:58.721: RADIUS:  NAS-Port            [5]   6   60000
Mar 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   1301463298
Mar 30 05:34:58.721: RADIUS:  Acct-Input-Octets   [42]  6   538044
Mar 30 05:34:58.721: RADIUS:  Acct-Output-Octets  [43]  6   3201914
Mar 30 05:34:58.721: RADIUS:  Acct-Input-Packets  [47]  6   1686
Mar 30 05:34:58.721: RADIUS:  Acct-Output-Packets [48]  6   35354
Mar 30 05:34:58.721: RADIUS:  Acct-Delay-Time     [41]  6   0
Mar 30 05:34:58.721: RADIUS(00000000): Sending a IPv4 Radius Packet
Mar 30 05:34:58.721: RADIUS(00000000): Started 5 sec timeout
Mar 30 05:34:58.737: RADIUS: Received from id 1646/85 10.62.145.51:1813, Accounting-response,
len 20
```

Captura de pacote de informação:



Etapa 4. Verifique que o perfilador debuga no ISE

Se os atributos foram enviados do interruptor, é possível verificar se foram recebidos no ISE. A fim verificar isto, permita por favor o perfilador debuga para o nó correto PSN (log Configuration>PSN>profiler>debug de Administration>System>Logging>Debug) e executam a autenticação do valor-limite mais uma vez.

Procure a informação seguinte:

- Debug que indica que a ponta de prova do raio recebida atribui:

```
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=0AE5182000000 2040099C216,
AllowedProtocolMatchedRule=MAB, Location=Location#All Locations, Device Type=Device Type#All
Device Types, ]
```

- Debug que indica que os atributos estiveram analisados gramaticalmente com sucesso:

```
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 que indica que os atributos estão processados pelo remetente:

```
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:null
Name:null
MAC: 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
```

Um remetente armazena valores-limite no base de dados de Cisco ISE junto com seus dados dos atributos, e notifica então o analisador dos valores-limite novos detectados em sua rede. O analisador classifica valores-limite à identidade do valor-limite agrupa e armazena valores-limite com os perfis combinados no base de dados.

Etapa 5. Tipicamente depois que os atributos novos são adicionados à coleção existente para o dispositivo específico, estes dispositivo/valor-limite está adicionado a perfilar a fila a fim verificar se ele tem que ser atribuído o perfil diferente baseado em atributos novos:

```
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

Informações Relacionadas

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