Introduction

This document describes how to configure Device Sensor, so that it can be used for profiling purposes on ISE. Device sensor is a feature of access devices. It allows to collect information about connected endpoints. Mostly, information collected by Device Sensor can come from the following protocols:

- Cisco Discovery Protocol (CDP)
- Link Layer Discovery Protocol (LLDP)
- Dynamic Host Configuration Protocol (DHCP)

On some platforms it is possible to use also H323, SIP (Session Initiation Protocol), MDNS (Multicast Domain Resolution) or HTTP protocols. Configuration possibilities for device sensor capabilities can vary from protocol to protocol. As an example above is available on Cisco Catalyst 3850 with software 03.07.02.E.

Once the information is collected, it can be encapsulated in radius accounting and send to a profiling server. In this article Identity Service Engine (ISE) is used as a profiling server.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Radius protocol
- CDP, LLDP and DHCP protocols
- Cisco Identity Service Engine
- Cisco Catalyst Switch 2960

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Identity Service Engine version 1.3 patch 3
- Cisco Catalyst Switch 2960s version 15.2(2a)E1
- Cisco IP Phone 8941 version SCCP 9-3-4-17

Configure

Step 1. Standard AAA configuration

In order to configure Authentication, Authorization and Accounting (AAA), follow the steps below:

1. Enable AAA using `aaa new-model` command and enable 802.1X globally on the switch
2. Configure Radius server and enable dynamic authorization (Change of Authorization - CoA)
3. Enable CDP and LLDP protocols
4. Add switchport authentication configuration

   In newer software version command `radius-server vsa send accounting` is enabled by default. If you cannot see attributes send in accounting, verify if the command in enabled.

Step 2. Configure Device Sensor

1. Determine which attributes from CDP/LLDP are needed to profile the device. In case of Cisco IP Phone 8941 you can use the following:

   - LLDP SystemDescription attribute
   - CDP CachePlatform attribute
For our purpose it would be enough to obtain just one of those since both of them provide Certainty Factory increase of 70 and Minimum Certainty Factory required to be profiled as Cisco-IP-Phone-8941 is 70:

![Cisco Identity Services Engine Profiling](image)

In order to be profiled as specific Cisco IP Phone, you need to satisfy minimum conditions for all parent profiles. This means profiler needs to match Cisco-Device (min. Certainty Factor 10) and Cisco-IP-Phone (min. Certainty Factor 20). Even though profiler matches those two profiles, it should still be profiled as specific Cisco IP Phone since each IP Phone model has min. Certainty Factor of 70. Device is assigned to the profile for which it has highest Certainty Factor.

2. Configure two filter lists - one for CDP and another one for LLDP. Those indicate which attributes should be included in Radius accounting messages. This step is optional.

3. Create two filter-specs for CDP and LLDP. In filter spec you can either indicate that list of attributes should be included or excluded from accounting messages. In the example following attributes are included:

- `device-name` from CDP
- `system-description` from LLDP

You can configure additional attributes to be transmitted via Radius to ISE if needed. This step is also optional.

4. Add command `device-sensor notify all-changes`. It triggers updates whenever TLVs are added, modified or removed for current session.

5. In order to actually send the information gathered via Device Sensor functionality, you need to explicitly tell the switch to do so with command `device-sensor accounting`.
Step 3. Configure profiling on ISE

1. Add switch as a network device in "Administration>Network Resources>Network Devices". Use the radius server key from the switch as shared secret in Authentication Settings:

2. Enable Radius probe on the profiling node in "Administration>System>Deployment>ISE node>Profiling Configuration". If all PSN nodes should be used for profiling, enable the probe on all of them:
3. Configure ISE Authentication Rules. In the example the default authentication rules preconfigured on ISE are used:

![ISE Authentication Page]

**Authentication Policy**

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

**Policy Export** go to Administration > System > Backup & Restore > Policy Export Page

Policy Type: Simple (Rule-based)

![Authentication Rule Examples]

- MAB: If Wired_MAB OR Wireless_MAB
  - Default: use Internal Endpoints
  - Allow Protocols: Default Network Access

- Dot1X: If Wired_802.1X OR Wireless_802.1X
  - Default: use All_User_ID_Stores
  - Allow Protocols: Default Network Access

Default Rule (if no match): Allow Protocols: Default Network Access and use: All_User_ID_Stores

4. Configure ISE Authorization Rules. 'Profiled Cisco IP Phones' rule is used, which is preconfigured on ISE:

![ISE Authorization Page]

**Authorization Policy**

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

**Policy Export** go to Administration > System > Backup & Restore > Policy Export Page

First Matched Rule Applies

![Authorization Rule Examples]

- Standard:
  - Wireless Black List Default
  - Profiled Cisco IP Phones

**Verify**

In order to verify if profiling is working correctly, please refer to "Operations>Authentications" on ISE:

![ISE Operations Page]
First the device was authenticated using MAB (18:49:00). Ten seconds later (18:49:10) it was reprofiled as Cisco-Device and finally after 42 seconds since first authentications (18:49:42) it received Cisco-IP-Phone-8941 profile. As a result ISE returns Authorization Profile specific for IP Phones (Cisco_IP_Phone) and Downloadable ACL that permits all traffic (permit ip any any). Please note that in this scenario the unknown device has basic access to the network. It can be achieved by adding mac address to ISE internal endpoint database or allowing very basic network access for previously unknown devices.

Initial profiling took around 40 seconds in this example. On the next authentication ISE already knows the profile and correct attributes (permission to join voice domain and DACL) are applied instantly, unless ISE receives new/updated attributes and it needs to reprofile the device again.

In "Administration>Identity Management>Identities>Endpoints>tested endpoint" you can see what kind of attributes were collected by Radius probe and what their values are:
As you can observe the total Certainty Factor computed is 210 in this scenario. It comes from the fact that endpoint matched also Cisco-Device profile (with total certainty factor of 30) and Cisco-IP-Phone profile (with total certainty factor of 40). Since profiler matched both conditions in profile Cisco-IP-Phone-8941, certainty factor for this profile is 140 (70 for each attribute according to profiling policy). To sum up: 30+40+70+70=210.

**Troubleshoot**

**Step 1. Verify information collected by CDP/LLDP**

If you cannot see any data collected verify the following:

- Check the state of authentication session on the switch (it should be successful):
- Check if CDP and LLDP protocols are enabled. Check if there are any non-default commands regarding CDP/LLDP/etc. and how those can affect attribute retrieval from the endpoint
- Verify in configuration guide for your endpoint if it supports CDP/LLDP/etc

**Step 2. Check Device Sensor cache**

If you do not see any data in this field or information is not complete verify ‘device-sensor’ commands, in particular filter-lists and filter-specs.

**Step 3. Check if attributes are present in Radius Accounting**

You can verify that using ‘debug radius’ command on the switch or performing packet capture between switch and ISE.

Radius debug:

```
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: Vendor, Cisco [26] 23
Mar 30 05:34:58.721: RADIUS: Vendor, Cisco [26] 59
Mar 30 05:34:58.721: RADIUS: Vendor, Cisco [26] 19
Mar 30 05:34:58.721: RADIUS: Vendor, Cisco [26] 49
Mar 30 05:34:58.721: RADIUS: Vendor, Cisco [26] 19
Mar 30 05:34:58.721: RADIUS: Vendor, Cisco [26] 18
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-Port-Id [87] 23 "GigabitEthernet1/0/13"
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]
```
Step 4. Verify profiler debugs on ISE

If the attributes were sent from the switch, it is possible to check if they were received on ISE. In order to check this, please enable profiler debugs for correct PSN node (Administration>System>Logging>Debug Log Configuration>PSN>profiler>debug) and perform authentication of the endpoint one more time.

Look for following information:

- Debug indicating that radius probe received attributes:

cisco.profiler.probes.radius.RadiusParser -::--
MSG_CODE=[3002], VA=[true], PRRT_TIMESTAMP=[2015-11-25 19:29:53.637 +00:00],
ATRTRS=[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=0000016, Acct-Input-Packets=1138, Acct-Output-Packets=513476,
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=0AE51820000002040099C216, cisco-av-pair=vr-id=101,
cisco-av-pair=method=mab, AcsSessionID=ise13/235487054/2511, SelectedAccessService=Default
Network Access,
Step=11004, Step=11017, Step=15049, Step=15008, Step=11004, Step=11005,
NetworkDeviceGroups=Location#All Locations,
NetworkDeviceGroups=Device Type#All Device Types, Service-Type=Call Check,
CPMSessionID=0AE51820000002040099C216,
AllowedProtocolMatchedRule=MAB, Location=Location#All Locations, Device Type=Device Type#All
Device Types,

- **Debug indicating that attributes were successfully parsed:**
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=132529, Acct-Output-Octets=2871426,
Acct-Input-Octets=132529, Acct-Output-Packets=1138, Acct-Input-Packets=2722,
Event-Timestamp=1301458555, NAS-Port-Type=Ethernet, NAS-Port-Id=10/0/11,
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=0AE51820000002040099C216, cisco-av-pair=vr-id=101,
cisco-av-pair=method=mab, AcsSessionID=ise13/235487054/2511, SelectedAccessService=Default
Network Access,
Step=11004, Step=11017, Step=15049, Step=15008, Step=11005,
NetworkDeviceGroups=Location#All Locations,
NetworkDeviceGroups=Device Type#All Device Types, Service-Type=Call Check,
CPMSessionID=0AE51820000002040099C216,
AllowedProtocolMatchedRule=MAB, Location=Location#All Locations, Device Type=Device Type#All
Device Types,

- **Debug indicating that attributes are processed by forwarder:**
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

A forwarder stores endpoints into the Cisco ISE database along with their attributes data, and then notifies the analyzer of new endpoints detected on your network. The analyzer classifies endpoints to the endpoint identity groups and stores endpoints with the matched profiles in the database.

Step 5. Typically after new attributes are added to the existing collection for specific device, this device/endpoint is added to profiling queue in order to check if it has to be assigned different profile based on new attributes:

2015-11-25 19:29:53,646 DEBUG [EndpointHandlerWorker-6-31-thread-1][]
Classify hierarchy 20:BB:C0:DE:06:AE
2015-11-25 19:29:53,656 DEBUG [EndpointHandlerWorker-6-31-thread-1][]
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][]
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][]
Policy Cisco-IP-Phone-8941 matched 20:BB:C0:DE:06:AE (certainty 140)

for:210 ExceptionRuleMatched:false

Related Information
