

ISE プロファイリング用のデバイス センサーの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ステップ 1: 標準AAA設定](#)

[ステップ 2: デバイスセンサーの設定](#)

[ステップ 3: ISEでのプロファイリングの設定](#)

[確認](#)

[トラブルシューティング](#)

[ステップ 1: CDP/LLDPによって収集された情報の確認](#)

[ステップ 2: デバイスセンサーキャッシュの確認](#)

[ステップ 3: RADIUS アカウンティングに属性があるかどうかの確認](#)

[ステップ 4: ISEでのプロファイラデバッグの確認](#)

[ステップ 5: 新しい属性とデバイス割り当てのプロファイリング](#)

[関連情報](#)

はじめに

このドキュメントでは、ISEでプロファイリング目的で使用できるようにデバイスセンサーを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- RADIUS プロトコル
- Cisco Discovery Protocol(CDP)、Link Layer Discovery Protocol(LLDP)、およびDynamic Host Configuration Protocol(DHCP)
- Cisco Identity Service Engine(ISE)

- Cisco Catalyst スイッチ 2960

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いています。

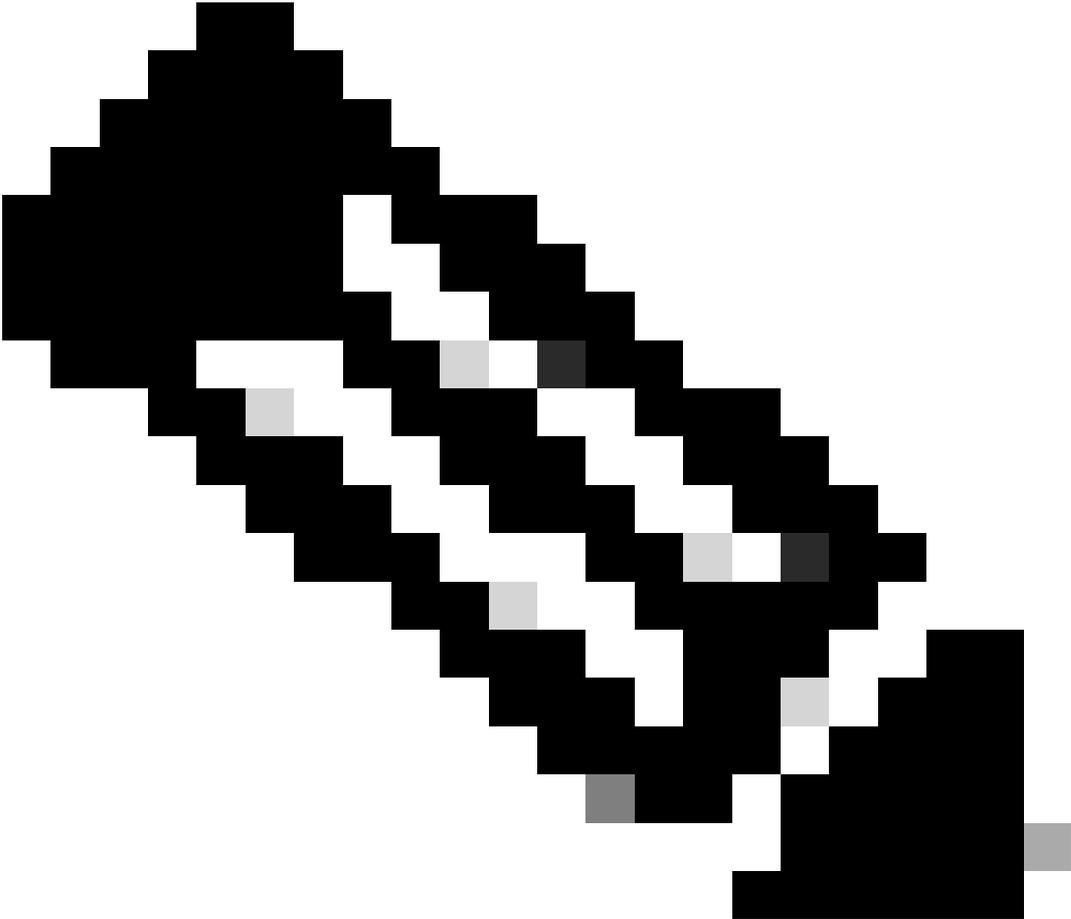
- Cisco ISEバージョン1.3パッチ3
- Cisco Catalyst スイッチ 2960 バージョン 15.2(2a)E1
- Cisco IP Phone 8941 バージョン SCCP 9-3-4-17

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、クリアな（デフォルト）設定で作業を開始しています。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。

背景説明

デバイスセンサーは、アクセスデバイスの機能です。これにより、接続エンドポイントに関する情報を収集できます。ほとんどの場合、デバイスセンサーによって収集される情報は、次のプロトコルから取得されます。

- CDP
- LLDP
- DHCP



注：一部のプラットフォームでは、H323、Session Initiation Protocol(SIP)、マルチキャストドメイン解決(MDNS)、またはHTTPプロトコルも使用できます。デバイスセンサー機能を設定できるかどうかは、プロトコルによって異なります。この例は、ソフトウェア03.07.02.Eが稼働するCisco Catalyst 3850で使用できます。

収集された情報は、RADIUSアカウントングにカプセル化してプロファイリングサーバに送信できます。この記事では、ISEをプロファイリングサーバとして使用します。

設定

ステップ 1：標準AAA設定

認証、認可、アカウントング(AAA)を設定するには、次の手順を参照してください。

1. aaa new-modelコマンドを使用してAAAを有効にし、スイッチで802.1Xをグローバルに有効にします。
2. RADIUSサーバを設定し、動的許可(Change of Authorization - CoA)を有効にします。

3. CDPおよびLLDPプロトコルを有効にします。

4. switchport認証設定を追加します。

```
!  
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：新しいソフトウェアバージョンでは、コマンドradius-server vsa send accountingはデフォルトで有効になっています。アカウントングで属性の送信が確認できない場合は、コマンドが有効になっているかどうかを確認します。

ステップ 2：デバイスセンサーの設定

1. デバイスをプロファイリングするために必要なCDP/LLDPの属性を決定します。Cisco IP Phone 8941の場合は、次のコマンドを使用できます。

- LLDP SystemDescription 属性

- CDP CachePlatform 属性

The screenshot displays the Cisco Identity Services Engine (ISE) Profiling configuration interface. The main panel shows the configuration for the 'Cisco-IP-Phone-8941' profiler policy. Key settings include:

- Name:** Cisco-IP-Phone-8941
- Description:** Policy for Cisco
- 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

The 'Rules' section contains two conditions:

- If Condition:** CiscoIPPhone8941Check1
- If Condition:** CiscoIPPhone8941Check2

A 'Conditions Details' pop-up window is open for 'CiscoIPPhone8941Check2', showing the following details:

- Name:** CiscoIPPhone8941Check2
- Description:** Check for Cisco IP Phone 8941
- Expression:** LLDP:lldpSystemDescription CONTAINS Cisco IP Phone 8941

どちらの場合も確信度のファクトリ値が70増加し、Cisco-IP-Phone-8941としてプロファイリングする必要がある最小確信度のファクトリ値が70であるため、いずれか1つのみを取得するだけで十分です。

- 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 C

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



注：特定のCisco IP Phoneとしてプロファイリングするには、すべての親プロファイルの最小条件を満たす必要があります。つまり、プロファイラはCisco-Device（最小確信度10）とCisco-IP-Phone（最小確信度20）に一致する必要があります。プロファイラがこの2つのプロファイルに一致しても、各IPフォンモデルの最小確信度は70であるため、特定のCisco IP Phoneとしてプロファイリングする必要があります。デバイスは、確信度が最も高いプロファイルに割り当てられます。

2. 2つのフィルタリストを設定します。1つはCDP用で、もう1つはLLDP用です。これらは、RADIUSアカウントメッセージに含める必要がある属性を示します。この手順は任意です。

3. CDPとLLDPの2つのフィルタ仕様を作成します。filter-specでは、アカウントメッセージに含める属性と除外する属性のリストを指定できます。この例では、次の属性が含まれています。

- device-name (CDP)
- system-description (LLDP)

必要に応じて、Radius経由でISEに送信される追加の属性を設定できます。この手順もオプションです。

4. コマンドdevice-sensor notify all-changesを追加します。現在のセッションに対してTLVが追加、変更、または削除されるたびに、更新がトリガーされます。

5. デバイスセンサー機能を使用して収集した情報を実際に送信するには、device-sensor accountingコマンドを使用してスイッチに対しこの操作を実行するように明示的に指示する必要があります。

```
! 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
```

ステップ 3 : ISEでのプロファイリングの設定

1. スイッチをネットワークデバイスとしてAdministration > Network Resources > Network Devicesに追加する。次のように、Authentication SettingsでスイッチからのRADIUSサーバキーを共有秘密鍵として使用します。

CISCO Identity Services Engine Home Operations | Policy | Guest Access | Administration |

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service

Network Devices Network Device Groups External RADIUS Servers RADIUS Server Sequences TrustSec AAA Servers NAC Managers

Network Devices List > deskswitch

Network Devices

* Name: test_switch
Description: []

* IP Address: 1.1.1.1 / 32

Model Name: []
Software Version: []

* Network Device Group

Location: All Locations [Set To Default]
Device Type: All Device Types [Set To Default]

Authentication Settings

Enable Authentication Settings

Protocol: **RADIUS**

* Shared Secret: [] [Show]

Enable KeyWrap: [i]

* Key Encryption Key: [] [Show]

* Message Authenticator Code Key: [] [Show]

Key Input Format: ASCII HEXADECIMAL

SNMP Settings
 Advanced TrustSec Settings

[Save] [Reset]

2. Administration > System > Deployment > ISE node > Profiling ConfigurationのプロファイルノードでRADIUSプローブを有効にします。すべてのPSNノードをプロファイルに使用する必要がある場合は、これらすべてのノードでプローブを有効にします。

Deployment Nodes List > ise13

Edit Node

General Settings | Profiling Configuration

- NETFLOW
- DHCP
- DHCPSPAN
- HTTP
- RADIUS

Description: The RADIUS probe collects RADIUS session attributes as well as CDP, LLDP, DHCP, HTTP and MDM from IOS Sensor.
- Network Scan (NMAP)
- DNS
-

Save | Reset

3. ISE認証ルールの設定この例では、ISEで事前に設定されたデフォルトの認証ルールが使用されます。

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. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Policy Type Simple Rule-Based

<input checked="" type="checkbox"/>	MAB	: If Wired_MAB OR Wireless_MAB	Allow Protocols : Default Network Access
<input checked="" type="checkbox"/>	Default	: use Internal Endpoints	
<input checked="" type="checkbox"/>	Dot1X	: If Wired_802.1X OR Wireless_802.1X	Allow Protocols : Default Network Access
<input checked="" type="checkbox"/>	Default	: use All_User_ID_Stores	
<input checked="" type="checkbox"/>	Default Rule (If no match)	: Allow Protocols : Default Network Access and use : All_User_ID_Stores	

4. ISE認可ルールの設定ISE で事前に設定された「Profiled Cisco IP Phone」ルールを使用します。

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.
 For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

First Matched Rule Applies

▶ Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones

確認

プロファイリングが正しく機能しているかどうかを確認するには、「ISEでのOperations > Authentications:

Cisco Identity Services Engine

Home | Operations | Policy | Guest Access | Administration

Authentications | Reports | Endpoint Protection Service | Troubleshoot

Misconfigured Supplicants: 0 | Misconfigured Network Devices: 0 | RADIUS Drops: 0 | Client Stopped Responding: 0

Time	Status	Details	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Identity Group	Event
2015-11-25 18:49:51.737	!		0	20:BB:C0:DE:06; 20:BB:C0:DE:06:AE	Cisco-IP-Phone-8941					Session State is Started
2015-11-25 18:49:42.433	✓		#ACSACL#-IP-PE							ACL Download Succeeded
2015-11-25 18:49:42.417	✓		20:BB:C0:DE:06; 20:BB:C0:DE:06:AE	20:BB:C0:DE:06:AE	Cisco-IP-Phone-8941	Default >> MAB >> D...	Default >> Profiled Cis..	Cisco_IP_Phones	Cisco-IP-Phone	Authentication succeeded
2015-11-25 18:49:42.401	✓			20:BB:C0:DE:06:AE						Dynamic Authorization succeeded
2015-11-25 18:49:10.802	✓		20:BB:C0:DE:06; 20:BB:C0:DE:06:AE	20:BB:C0:DE:06:AE	Cisco-Device	Default >> MAB >> D...	Default >> Default	PermitAccess	Profiled	Authentication succeeded
2015-11-25 18:49:10.780	✓			20:BB:C0:DE:06:AE						Dynamic Authorization succeeded
2015-11-25 18:49:00.720	✓		20:BB:C0:DE:06; 20:BB:C0:DE:06:AE			Default >> MAB >> D...	Default >> Default	PermitAccess		Authentication succeeded

まず、デバイスはMAB(18:49:00)を使用して認証されました。10秒後(18:49:10)にCisco-Deviceとして再プロファイルされ、最後に最初の認証(18:49:42)から42秒後にCisco-IP-Phone-8941プロファイルを受信しました。その結果、ISEはIPフォン (Cisco_IP_Phones)固有の認証プロファイルと、すべてのトラフィックを許可するダウンロード可能ACL(permit ip any)を返します。このシナリオでは、不明なデバイスがネットワークへの基本的なアクセス権を持っていることに注意してください。これは、ISE内部エンドポイントデータベースにMACアドレスを追加するか、または未知のデバイスに対して非常に基本的なネットワークアクセスを許可することで実現できます。



注：この例では、初回プロファイリングに約40秒かかりました。次の認証では、ISEはすでにプロファイルを認識しており、正しい属性（音声ドメインとDACLに参加する権限）が即座に適用されます。ただし、ISEが新しい属性や更新された属性を受け取り、デバイスの再プロファイルを実行する必要がある場合は除きます。

Administration > Identity Management > Identities > Endpoints > tested endpoint

Time	Status	Details	R...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Identity Group	Event
2015-11-25 18:55:39.772				0	20:BB:C0:DE:06: 20:BB:C0:DE:06:AE	Cisco-IP-Phone-8941					Session State is Started
2015-11-25 18:55:38.721				#ACSAcl#-IP-PE							DAcl Download Succeeded
2015-11-25 18:55:38.707				20:BB:C0:DE:06: 20:BB:C0:DE:06:AE	Cisco-IP-Phone-8941	Default >> MAB >> D...	Default >> Profiled Cs..	Cisco_IP_Phones	Cisco-IP-Phone		Authentication succeeded
2015-11-25 18:49:42.433				#ACSAcl#-IP-PE							DAcl Download Succeeded
2015-11-25 18:49:42.417				20:BB:C0:DE:06: 20:BB:C0:DE:06:AE	Cisco-IP-Phone-8941	Default >> MAB >> D...	Default >> Profiled Cs..	Cisco_IP_Phones	Cisco-IP-Phone		Authentication succeeded

では、Radiusプロンプトによって収集された属性の種類と、その値を確認できます。

Identities	
NAS-IP-Address	10.229.20.43
NAS-Port	60000
NAS-Port-Id	GigabitEthernet1/0/13
NAS-Port-Type	Ethernet
NetworkDeviceGroups	Location#All Locations, Device Type#All Device Types
NetworkDeviceName	deskswitch
OUI	Cisco Systems, Inc
OriginalUserName	20bbc0de06ae
PolicyVersion	2
PostureApplicable	Yes
PostureAssessmentStatus	NotApplicable
SelectedAccessService	Default Network Access
SelectedAuthenticationIdentityStores	Internal Endpoints
SelectedAuthorizationProfiles	Cisco_IP_Phones
Service-Type	Call Check
StaticAssignment	false
StaticGroupAssignment	false
StepData	5= Radius.Service-Type, 6= Radius.NAS-Port-Type, 7=MAB, 10=Intern
Total Certainty Factor	210
UseCase	Host Lookup
User-Name	20-BB-C0-DE-06-AE
UserType	Host
cdpCachePlatform	Cisco IP Phone 8941
cdpUndefined28	00:02:00
ldpSystemDescription	Cisco IP Phone 8941, V3, SCCP 9-3-4-17

ご覧のように、このシナリオで計算される確信度の合計は210です。これは、エンドポイントがCisco-Deviceプロファイル（確信度の合計が30）およびCisco-IP-Phoneプロファイル（確信度の合計が40）にも一致したためです。プロファイルはプロファイル Cisco-IP-Phone-8941の両方の条件に一致したため、このプロファイルの確信度は140です（プロファイリングポリシーに従って、属性ごとに70）。合計すると、30+40+70+70=210になります。

トラブルシューティング

ステップ 1 : CDP/LLDPによって収集された情報の確認

```
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
```

収集されたデータが表示されない場合は、次の点を確認してください。

- スイッチの認証セッションの状態を確認します (成功するはずです)。

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

- CDP プロトコルと LLDP プロトコルが有効になっているかどうかを確認します。CDP/LLDPなどに関するデフォルト以外のコマンドがあるかどうか、それらがエンドポイントからの属性取得にどのように影響するかを確認します

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

- エンドポイントがCDP/LLDPなどをサポートしているかどうかを、エンドポイントのコンフィギュレーションガイドで確認します。

ステップ 2 : デバイスセンサーキャッシュの確認

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

このフィールドにデータが表示されない場合、または情報が不完全な場合は、「device-sensor」コマンド、特にfilter-listsとfilter-specsを確認します。

ステップ 3 : RADIUS アカウンティングに属性があるかどうかの確認

スイッチでdebug radiusコマンドを使用するか、スイッチとISE間でパケットキャプチャを実行していることを確認できます。

RADIUS デバッグ :

```
<#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

パケットキャプチャ :

Filter: radius.code==4

No.	Time	Source	Destination	Protocol	Length	Info
27	2015-11-25 21:51:52.233942	10.229.20.43	10.62.145.51	RADIUS	432	Accounting-Request(4) (id=86, l=390)
77	2015-11-25 21:52:02.860652	10.229.20.43	10.62.145.51	RADIUS	333	Accounting-Request(4) (id=87, l=291)

Frame 27: 432 bytes on wire (3456 bits), 432 bytes captured (3456 bits)

- Ethernet II, Src: 58:f3:9c:6e:45:c3 (58:f3:9c:6e:45:c3), Dst: 00:50:56:9c:49:54 (00:50:56:9c:49:54)
- Internet Protocol Version 4, Src: 10.229.20.43 (10.229.20.43), Dst: 10.62.145.51 (10.62.145.51)
- User Datagram Protocol, Src Port: 1646 (1646), Dst Port: 1813 (1813)
- Radius Protocol
 - Code: Accounting-Request (4)
 - Packet identifier: 0x56 (86)
 - Length: 390
 - Authenticator: 7008a6239a5f3ddbcee380d648c4782d
 - The response to this request is in frame 28!
 - Attribute Value Pairs
 - AVP: l=40 t=Vendor-Specific(26) v=ciscoSystems(9)
 - VSA: l=34 t=Cisco-AVPair(1): cdp-tlv=\000\006\000\024Cisco IP Phone 8941
 - AVP: l=23 t=Vendor-Specific(26) v=ciscoSystems(9)
 - VSA: l=17 t=Cisco-AVPair(1): cdp-tlv=\000\034\000\003\000\002\000
 - AVP: l=59 t=Vendor-Specific(26) v=ciscoSystems(9)
 - VSA: l=53 t=Cisco-AVPair(1): lldp-tlv=\000\006\000&Cisco IP Phone 8941, V3, SCCP 9-3-4-17
 - AVP: l=19 t=User-Name(1): 20-BB-C0-DE-06-AE
 - AVP: l=49 t=Vendor-Specific(26) v=ciscoSystems(9)
 - AVP: l=19 t=Vendor-Specific(26) v=ciscoSystems(9)
 - AVP: l=18 t=Vendor-Specific(26) v=ciscoSystems(9)
 - AVP: l=19 t=Called-Station-Id(30): F0-29-29-49-67-0D
 - AVP: l=19 t=Calling-Station-Id(31): 20-BB-C0-DE-06-AE
 - AVP: l=6 t=NAS-IP-Address(4): 10.229.20.43
 - AVP: l=6 t=NAS-Port(5): 60000
 - AVP: l=23 t=NAS-Port-Id(87): GigabitEthernet1/0/13
 - AVP: l=6 t=NAS-Port-Type(61): Ethernet(15)
 - AVP: l=10 t=Acct-Session-Id(44): 00000018
 - AVP: l=6 t=Acct-Terminate-Cause(49): Unknown(0)
 - AVP: l=6 t=Acct-Status-Type(40): Stop(2)
 - AVP: l=6 t=Event-Timestamp(55): Mar 30, 2011 07:37:53.000000000 Central European Daylight Time
 - AVP: l=6 t=Acct-Session-Time(46): 175
 - AVP: l=6 t=Acct-Input-Octets(42): 544411
 - AVP: l=6 t=Acct-Output-Octets(43): 3214015
 - AVP: l=6 t=Acct-Input-Packets(47): 1706
 - AVP: l=6 t=Acct-Output-Packets(48): 35467
 - AVP: l=6 t=Acct-Delay-Time(41): 0

ステップ 4 : ISEでのプロファイラデバッグの確認

スイッチから属性が送信された場合は、ISEで属性が受信されたかどうかを確認できます。これを確認するには、正しいPSNノード(Administration > System > Logging > Debug Log Configuration > PSN > profiler > debug)のプロファイラデバッグを有効にし、エンドポイントの認証をもう一度実行します。

次の情報を探します。

- RADIUS プロローブが属性を受信したことを示すデバッグ :

<#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=0AE51820000002040099C216, 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#All
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**

- 属性が正常に解析されたことを示すデバッグ :

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

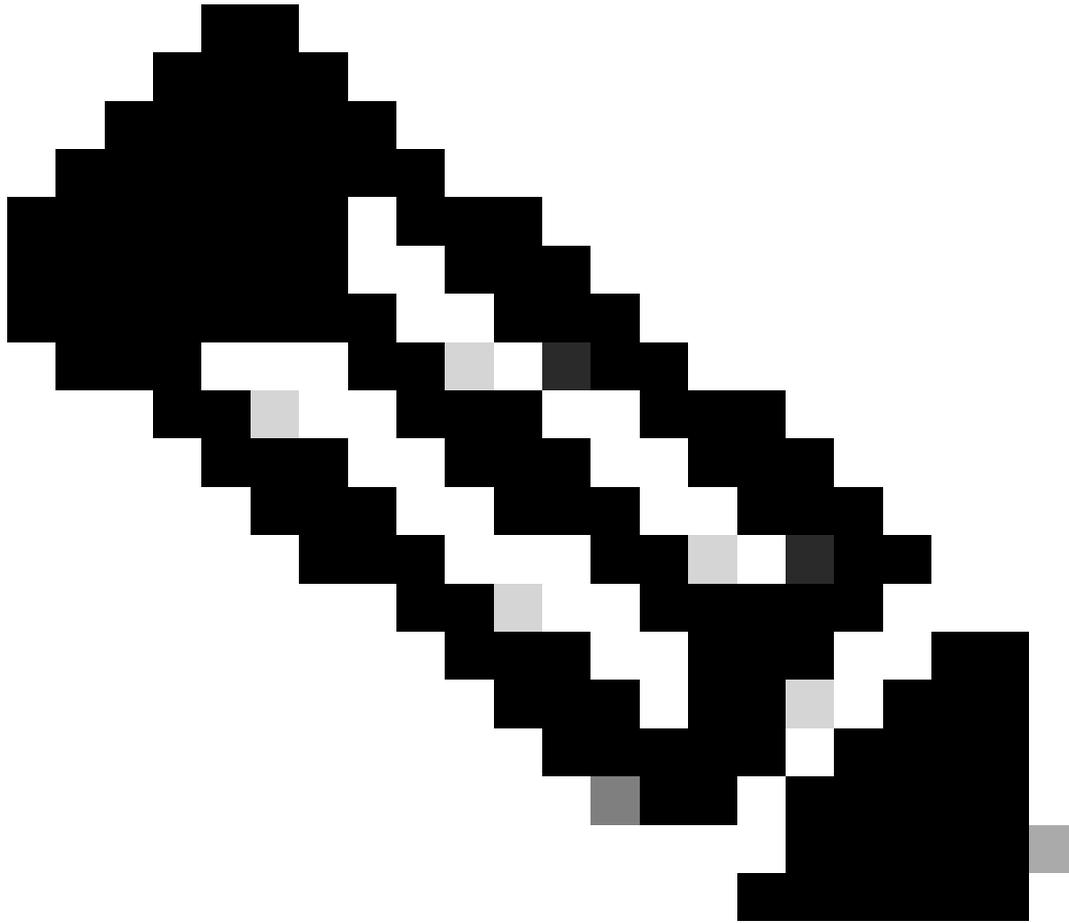
- 属性がフォワーダによって処理されることを示すデバッグ :

<#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:1

Attribute:SkipProfiling value:false



注：フォワーダは、エンドポイントをその属性データとともにCisco ISEデータベースに保存し、ネットワークで検出された新しいエンドポイントをアナライザに通知します。アナライザは、エンドポイントを終端ポイント ID グループに分類し、一致プロファイルとともにエンドポイントをデータベースに保存します。

ステップ 5：新しい属性とデバイス割り当てのプロファイル

通常、特定のデバイスの既存のコレクションに新しい属性が追加されると、このデバイス/エンドポイントがプロファイルキューに追加され、新しい属性に基づいて別のプロファイルを割り当てる必要があるかどうかを確認します。

<#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

関連情報

- <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
- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。