

ISE 3.3でのエンドポイント分類のWiFi分析について

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](#)

[WLCでの設定](#)

[ステップ 1: デバイス分類機能をグローバルに有効にする](#)

[ステップ 2: TLVキャッシングとRADIUSプロファイルリングの有効化](#)

[ISEでの設定](#)

[ステップ 1: 展開内のPSNでプロファイルサービスを有効にする](#)

[ステップ 2: ISE PSNでのRADIUSプロファイルプローブの有効化](#)

[ステップ 3: CoAタイプとエンドポイント属性フィルタの設定](#)

[ステップ 4: WiFi分析データ属性を使用した認証ポリシーの設定](#)

[確認](#)

[トラブルシューティング](#)

[ステップ 1: アカウンティングパケットがISEに到達](#)

[ステップ 2: ISEがエンドポイント属性でアカウンティングパケットを解析](#)

[ステップ 3: エンドポイント属性が更新され、エンドポイントが分類される](#)

[ステップ 4: CoAと再認証](#)

[関連情報](#)

はじめに

このドキュメントでは、エンドポイント分類のWiFi分析の仕組みについて説明します。また、設定方法、確認方法、およびトラブルシューティング方法についても説明します。

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。

- 9800ワイヤレスLANコントローラ(WLC)の設定
- Identity Services Engine (ISE) の設定
- RADIUS 認証.許可とアカウンティング(AAA)パケットフローと用語

このドキュメントでは、RADIUSサーバとしてISEを使用しているクライアントを認証する

WLANがすでに動作していることを前提としています。

この機能が動作するには、少なくとも次のものがが必要です。

- 9800 WLC Cisco IOS® XEダブリン17.10.1
- Services Engine v3.3を確認する。
- 802.11ac Wave2または802.11ax(Wi-Fi 6/6E)アクセスポイント

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。

- 9800 WLC Cisco IOSXE v17.12.x
- Identity Services Engine(ISE)v3.3
- Android 13デバイス

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

WiFi Device Analyticsを通じて、Cisco 9800 WLCは、このデバイスに接続された一連のエンドポイントからモデル番号やOSバージョンなどの属性を学習し、それをISEと共有できます。ISEは、この情報をエンドポイント分類（プロファイリングとも呼ばれる）に使用できます。

現在、WiFi分析は次のベンダーでサポートされています。

- Apple
- Intel
- サムスン

WLCは、RADIUSアカウントリングパケットを使用して、ISEサーバと属性情報を共有します。



WiFi分析のデータフロー

RADIUS AAAフロー上のRADIUSアカウントングパケットは、RADIUSサーバがエンドポイント認証の試行に対する応答としてRADIUS Access-Acceptパケットを送信した後にのみ送信されることに注意してください。つまり、WLCは、RADIUSサーバ(ISE)とネットワークアクセスデバイス(WLC)の間でエンドポイントのRADIUSセッションが確立された後にのみ、エンドポイント属性情報を共有します。

ISEがエンドポイントの分類と許可に使用できるすべての属性を次に示します。

- デバイス情報ファームウェアのバージョン
- デバイス情報ハードウェアのモデル
- DEVICE_INFO_MANUFACTURER_モデル
- デバイス情報モデル名
- デバイス情報モデル番号
- デバイス情報OSバージョン
- デバイス情報ベンダータイプ



注:WLCは接続しているエンドポイントのタイプに応じて追加の属性を送信できますが、ISEでの認可ポリシーの作成に使用できるのはリストされている属性だけです。

ISEは、アカウントリングパケットを受信すると、その内部でこの分析データを処理して使用し、それを使用してエンドポイントプロファイル/アイデンティティグループを再割り当てできます。

WiFi Endpoint Analytics属性は、WiFi_Device_Analyticsディクショナリの下に一覧表示されます。ネットワーク管理者は、エンドポイント許可ポリシーおよび条件にこれらの属性を含めることができます。

Select attribute for condition



	Dictionary	Attribute	ID	Info
	Wifi_Device_Analytics	Attribute	ID	
	Wifi_Device_Analytics	DEVICE_INFO_FIRMWARE_...		ⓘ
	Wifi_Device_Analytics	DEVICE_INFO_HW_MODEL		ⓘ
	Wifi_Device_Analytics	DEVICE_INFO_MANUFACT...		ⓘ
	Wifi_Device_Analytics	DEVICE_INFO_MODEL_NA...		ⓘ
	Wifi_Device_Analytics	DEVICE_INFO_MODEL_NUM		ⓘ
	Wifi_Device_Analytics	DEVICE_INFO_OS_VERSION		ⓘ
	Wifi_Device_Analytics	DEVICE_INFO_VENDOR_T...		ⓘ

WiFi Device Analyticsディクショナリ

ISEがエンドポイント用に保存する現在の属性値が変更されると、ISEは認可変更(CoA)を開始し、更新された属性を考慮に入れてエンドポイントを評価できるようにします。

設定

WLCでの設定

ステップ 1：デバイス分類機能をグローバルに有効にする

Configuration > Wireless > Wireless Globalの順に移動し、Device Classificationチェックボックスをオンにします。

Default Mobility Domain *	<input type="text" value="default"/>
RF Group Name*	<input type="text" value="default"/>
Maximum Login Sessions Per User*	<input type="text" value="0"/>
Management Via Wireless	<input type="checkbox"/>
Device Classification	<input checked="" type="checkbox"/>
AP LAG Mode	<input type="checkbox"/>
Dot15 Radio	<input type="checkbox"/>
Wireless Password Policy	<input type="text" value="None"/> ⓘ

デバイス分類設定

ステップ 2 : TLVキャッシングとRADIUSプロファイリングの有効化

Configuration > Tags and Profiles > Policyの順に移動し、RADIUSクライアントが接続しているWLANによって使用されるPolicy Profileを選択します。

Configuration > Tags & Profiles > Policy

[+ Add](#) [x Delete](#) [Clone](#)

	Admin Status	Associated Policy Tags	Policy Profile Name	Description
<input checked="" type="checkbox"/>	✔	🔗	ise-policy	
<input type="checkbox"/>	⊘		default-policy-profile	default policy profile

ワイヤレスポリシーの選択

Access Policiesをクリックし、RADIUS Profiling、HTTP TLV Caching、DHCP TLV Cachingの各オプションを確認します。前のステップで行ったアクションにより、デバイス分類のグローバル状態がEnabledステータスとして表示されるようになりました。

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General **Access Policies** QOS and AVC Mobility Advanced

RADIUS Profiling
HTTP TLV Caching
DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification **Enabled** ⓘ

Local Subscriber Policy Name ⓘ

VLAN

VLAN/VLAN Group ⓘ

Multicast VLAN

WLAN ACL

IPv4 ACL ⓘ

IPv6 ACL ⓘ

URL Filters ⓘ

Pre Auth ⓘ

Post Auth ⓘ

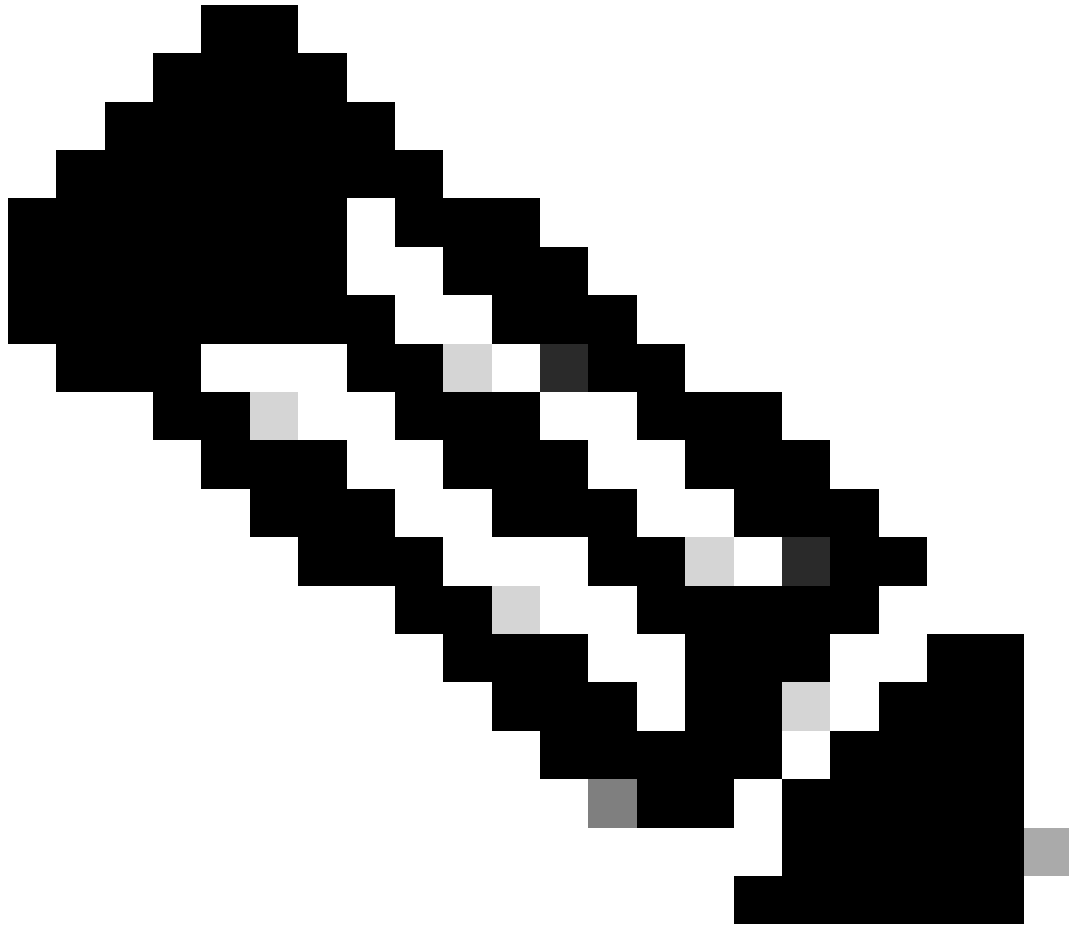
↶ Cancel

📄 Update & Apply to Device

RADIUSのプロファイリングとキャッシング設定

WLC CLIにログインして、dot11 TLVアカウントングを有効にします。

```
vimontes-wlc#configure terminal
vimontes-wlc(config)#wireless profile policy policy-profile-name
vimontes-wlc(config-wireless-policy)#dot11-tlv-accounting
```





注：このコマンドを使用する前に、ワイヤレスポリシープロファイルを無効にする必要があります。このコマンドは、Cisco IOS XE Dublin 17.10.1以降のバージョンでのみ使用できます。







ISEでの設定


ステップ 1：展開内のPSNでプロファイルサービスを有効にする

Administration > Deploymentに移動し、PSNの名前をクリックします。

Deployment Nodes

Selected 0 Total 1  

 Edit  Register  Syncup  Deregister All  


<input type="checkbox"/>	Hostname	Personas	Role(s)	Services	Node Status
<input type="checkbox"/>	ise1ab	Administration, Monitoring, Policy Service	STANDALONE	SESSION,PROFILER	


ISE PSNノードの選択


Policy Serviceセクションまでスクロールダウンして、**Enable Profiling Service**チェックボックスにチェックマークを付けます。
[Save] ボタンをクリックします。

Policy Service


Enable Session Services


Include Node in Node Group 


Enable Profiling Service 

Enable Threat Centric NAC Service 

> Enable SXP Service

Enable Device Admin Service 

Enable Passive Identity Service 

> pxGrid 

[Reset](#)

プロファイラサービスの構成

ステップ 2 : ISE PSNでのRADIUSプロファイルプローブの有効化

ページの最上部までスクロールして、**Profiling Configuration**タブをクリックします。ISEで使用できるすべてのプロファイルプローブが表示されます。**RADIUS Probe**を有効にし、**Save**をクリックします。

Edit Node

General Settings

Profiling Configuration

> NETFLOW

> DHCP

> DHCPSPAN

> HTTP

注:CoAパケットには常に空のIDフィールドがありますが、エンドポイントIDは最初の認証パケットと同じです。

認可変更(Change of Authorization)レコードの詳細(Details)列にあるアイコンをクリックします。

Sep 27, 2023 06:19:24.36...



0A:5A:F0:B3:B5:9C

CoAパケットの詳細へのアクセス

CoAの詳細情報が新しいブラウザタブに表示されます。**Other Attributes**セクションまでスクロールダウンします。

CoAソースコンポーネントはプロファイルとして表示されます。認証ポリシーで使用されるエンドポイントIDグループ、ポリシー、論理プロファイルの変更として、CoA理由が表示されます。

Other Attributes

ConfigVersionId	1493
Event-Timestamp	1695838764
Device CoA type	Cisco CoA
Device CoA port	1700
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	89f67978-be8f-4145-8801-45e2fffa1fe8
TotalAuthenLatency	3621649740
ClientLatency	3621649732
CoASourceComponent	Profiler
CoAReason	Change in endpoint identity group/policy/profile which are used in authorization policies
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
Device IP Address	172.16.5.169
CPMSessionID	A90510AC00000058D7D0DAA7
CiscoAVPair	subscriber:reauthenticate-type=last, subscriber:command=reauthenticate, audit-session-id=A90510AC00000058D7D0DAA7

CoAのトリガーとなるコンポーネントと理由

Context Visibility > Endpoints > Authentication タブに移動します。このタブで、フィルタを使用してテスト用エンドポイントを見つけます。

エンドポイントのMACアドレスをクリックして、エンドポイント属性にアクセスします。

<input type="checkbox"/>	MAC Address	Status	IP Address	Username	Hostname	Location	Endpoint Profile	Authen...	Authentication ...	Authorization P...
×	0A:5A:F0:B3:B5:9C	Status	IP Address	Username	Hostname	Location	Endpoint Profile	Authenticr	Authentication Polic	Authorization Policy
<input type="checkbox"/>	0A:5A:F0:B3:B5:9C			bob	Victor-s-S22	Location...	Android	-	Default	Wifi Endpoint Analy...

コンテキスト可視性のエンドポイント

このアクションは、このエンドポイントに関してISEが保存しているすべての情報を表示します。Attributesセクションをクリックして、Other Attributesを選択する。

MAC ADDRESS: 0A:5A:F0:B3:B5:9C

Username: bob
Endpoint Profile: Android
Current IP Address: -
Location: Location → All Locations

MFC Endpoint Type: Phone
MFC Hardware Manufacturer: Samsung Electronics Co.,Ltd
MFC Hardware Model: Samsung Galaxy S22+
MFC Operating System: Android 13

Applications | **Attributes** | Authentication | Threats | Vulnerabilities

General Attributes | Custom Attributes | **Other Attributes**

コンテキスト可視性でのその他の属性選択のエンドポイント

WiFi_Device_Analyticsディクショナリ属性が見つかるまで下にスクロールします。このセクションでこれらの属性を見つけることは、ISEがアカウントングパケットを通じてそれらを正常に受信し、エンドポイント分類に使用できることを意味します。

DEVICE_INFO_COUNTRY_CODE	Unknown
DEVICE_INFO_DEVICE_FORM	PHONE
DEVICE_INFO_FIRMWARE_VERSION	WH6
DEVICE_INFO_MODEL_NUM	Samsung Galaxy S22+
DEVICE_INFO_OS_VERSION	Android 13
DEVICE_INFO_SALES_CODE	MXO
DEVICE_INFO_VENDOR_TYPE	SAMSUNG

コンテキストの可視性に関するWiFi分析属性

参考として、Windows 10とiPhoneの属性の例を次に示します。

DEVICE_INFO_DEVICE_FORM	0
DEVICE_INFO_FIRMWARE_VERSION	22.180.02.01
DEVICE_INFO_HW_MODEL	AX201/AX1650
160MHZ	
DEVICE_INFO_MANUFACTURER_NAME	LENOVO
DEVICE_INFO_MODEL_NAME	20RAS0C000
DEVICE_INFO_MODEL_NUM	LENOVO
20RAS0C000	
DEVICE_INFO_OS_VERSION	WINDOWS 10
DEVICE_INFO_POWER_TYPE	AC POWERED
DEVICE_INFO_VENDOR_TYPE	3

Windows 10エンドポイント

DEVICE_INFO_DEVICE_FORM	0
DEVICE_INFO_MODEL_NUM	IPHONE
11 PRO	
DEVICE_INFO_OS_VERSION	IOS 16.4
DEVICE_INFO_VENDOR_TYPE	1

属性の例iPhoneエンドポイント属性の例

トラブルシューティング

ステップ 1 : アカウンティングパケットがISEに到達

WLC CLIで、**DOT11 TLV**アカウンティング、**DHCP TLV**キャッシングおよび**HTTP TLV**キャッシングがポリシープロファイル設定で有効になっていることを確認します。

<#root>

```
vimontes-wlc#show running-config | section wireless profile policy policy-profile-name
wireless profile policy policy-profile-name
aaa-override
accounting-list AAA-LIST
```

dhcp-tlv-caching

dot11-tlv-accounting

http-tlv-caching

radius-profiling

no shutdown

エンドポイントの接続中にWLCまたはISEのいずれかの端でパケットキャプチャを収集します。収集したファイルを分析するには、Wiresharkなどの既知のパケット分析ツールを使用できます。

RADIUSアカウンティングパケットおよび発呼端末ID (テストエンドポイントのMACアドレス) でフィルタリングします。たとえば、次のフィルタを使用できます。

```
radius.code == 4 && radius.Calling_Station_Id == "xx-xx-xx-xx-xx-xx"
```

これらが見つかったら、**Cisco-AVPair**フィールドを展開し、Accountingパケット内の**WiFi Analytics Data**を見つけます。

```

No. | Time | Source | Destination | Protocol | Length | Info
---|---|---|---|---|---|---
104 2023-09-27 12:19:23.584661 172.16.5.169 172.16.5.112 RADIUS 976 Accounting-Request id=39

> AVP: t=Vendor-Specific(26) l=28 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=36 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=39 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=36 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
  Type: 26
  Length: 49
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=43 val=dot11-device-info=\000\000\000\023Samsung Galaxy S22+
> AVP: t=Vendor-Specific(26) l=33 vnd=ciscoSystems(9)
  Type: 26
  Length: 33
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=27 val=dot11-device-info=\000\001\000\003WH6
> AVP: t=Vendor-Specific(26) l=33 vnd=ciscoSystems(9)
  Type: 26
  Length: 33
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=27 val=dot11-device-info=\000\002\000\003MX0
> AVP: t=Vendor-Specific(26) l=31 vnd=ciscoSystems(9)
  Type: 26
  Length: 31
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=25 val=dot11-device-info=\000\003\000\0011
> AVP: t=Vendor-Specific(26) l=40 vnd=ciscoSystems(9)
  Type: 26
  Length: 40
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=34 val=dot11-device-info=\000\004\000\0aAndroid 13
> AVP: t=Vendor-Specific(26) l=37 vnd=ciscoSystems(9)
  Type: 26
  Length: 37
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=31 val=dot11-device-info=\000\005\000\0aUnknown
> AVP: t=Vendor-Specific(26) l=31 vnd=ciscoSystems(9)
  Type: 26
  Length: 31
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=25 val=dot11-device-info=\000\n\000\0012
> AVP: t=Framed-IP-Address(8) l=6 val=172.16.5.76

```

アカウントングパケット内のエンドポイントTLV属性

ステップ 2 : ISEがエンドポイント属性でアカウントングパケットを解析

ISE側で、これらのコンポーネントをDEBUGレベルに設定して、WLCから送信されたRADIUSアカウントングパケットがISEに到達し、正しく処理されるようにすることができます。

その後、ISEサポートバンドルを収集してログファイルを収集できます。サポートバンドルの収集方法の詳細については、「関連情報」のセクションを参照してください。

Component Name	Log Level	Description	Log file Name
× Component Name	DEBUG	× Description	Log file Name
nsf	DEB... ▾	NSF related messages	ise-psc.log
nsf-session	DEB... ▾	Session cache messages	ise-psc.log
profiler	DEB... ▾	profiler debug messages	profiler.log
runtime-AAA	DEB... ▾	AAA runtime messages (prrt)	prrt-server.log

トラブルシューティングのためにデバッグするコンポーネント

注：コンポーネントは、エンドポイントを認証するPSNでのみデバッグレベルに有効化されます。

iseLocalStore.logでは、Accounting-Startメッセージがログに記録されるため、コンポーネントをDEBUGレベルに有効にする必要はありません。ここで、ISEはWiFi分析属性を含む着信アカウントリングパケットを確認する必要があります。

<#root>

2023-09-27 18:19:23.600 +00:00 0000035538 3000

NOTICE Radius-Accounting: RADIUS Accounting start request,

ConfigVersionId=1493,
Device IP Address=172.16.5.169,

cisco-av-pair=dhcp-option=host-name=Victor-s-S22, cisco-av-pair=dhcp-option=dhcp-class-identifier=andro
cisco-av-pair=dot11-device-info=DEVICE_INFO_MODEL_NUM=Samsung Galaxy S22+, cisco-av-pair=dot11-device-in

cisco-av-pair=dot11-device-info=DEVICE_INFO_DEVICE_FORM=1, cisco-av-pair=dot11-device-info=DEVICE_INFO_C

cisco-av-pair=dot11-device-info=DEVICE_INFO_VENDOR_TYPE=2, cisco-av-pair=audit-session-id=A90510AC000000
, cisco-av-pair=vlan-id=2606, cisco-av-pair=method=dot1x, cisco-av-pair=cisco-wlan-ssid=VICSSID,
cisco-av-pair=wlan-profile-name=ISE-AAA, Airespace-Wlan-Id=1, AcsSessionID=iselab/484624451/304,

エンドポイントの属性情報が更新されます。

<#root>

2023-09-27 18:19:23,602

DEBUG [RADIUSParser-1-thread-2][[]]

cisco.profiler.probes.radius.RadiusParser -:A90510AC0000005BD7DDDA7::::-

Device Analytics data 1: DEVICE_INFO_FIRMWARE_VERSION=[WH6]

2023-09-27 18:19:23,602

DEBUG [RADIUSParser-1-thread-2][[]]

cisco.profiler.probes.radius.RadiusParser -:A90510AC0000005BD7DDDA7::::-

Device Analytics data 1: DEVICE_INFO_SALES_CODE=[MXO]

2023-09-27 18:19:23,602

DEBUG [RADIUSParser-1-thread-2][[]]

cisco.profiler.probes.radius.RadiusParser -:A90510AC0000005BD7DDDA7::::-

Device Analytics data 1: DEVICE_INFO_DEVICE_FORM=[1]

2023-09-27 18:19:23,602

DEBUG [RADIUSParser-1-thread-2][[]]

cisco.profiler.probes.radius.RadiusParser -:A90510AC0000005BD7DDDA7::::-

Device Analytics data 1: DEVICE_INFO_OS_VERSION=[Android 13]

2023-09-27 18:19:23,602

DEBUG [RADIUSParser-1-thread-2][[]]

cisco.profiler.probes.radius.RadiusParser -:A90510AC0000005BD7DDDA7::::-

Device Analytics data 1: DEVICE_INFO_COUNTRY_CODE=[Unknown]

2023-09-27 18:19:23,602

DEBUG [RADIUSParser-1-thread-2][[]]

cisco.profiler.probes.radius.RadiusParser -:A90510AC0000005BD7DDDA7::::-

Device Analytics data 1: DEVICE_INFO_VENDOR_TYPE=[2]

<#root>

2023-09-27 18:19:23,602

DEBUG [RADIUSParser-1-thread-2][[]]

cisco.profiler.probes.radius.RadiusParser -:A90510AC0000005BD7DDDA7:::- Endpoint: EndPoint[id=,name=

MAC: 0A:5A:F0:B3:B5:9C

Attribute:AAA-Server value:iselab Attribute:Acct-Authentic value:Remote Attribute:Acct-Delay-Time valu

Attribute:DEVICE_INFO_COUNTRY_CODE value:Unknown Attribute:DEVICE_INFO_DEVICE_FORM value:PHONE Attribute

Attribute:Device IP Address value:172.16.5.169 Attribute:Device Type value:Device Type#All Device Type

属性の更新により、新しいエンドポイントプロファイルイベントがトリガーされます。プロファイルポリシーが再度評価され、新しいプロファイルが割り当てられます。

<#root>

2023-09-27 18:19:24,098

DEBUG [pool-533-thread-35]

[[]] cisco.profiler.infrastructure.profiling.ProfilerManager -:A90510AC0000005BD7DDDA7:::62cc7a10-5d62-

Policy Android matched 0A:5A:F0:B3:B5:9C (certainty 30)

2023-09-27 18:19:24,098

DEBUG [pool-533-thread-35]

[[]] cisco.profiler.infrastructure.profiling.ProfilerManager -:A90510AC0000005BD7DDDA7:::62cc7a10-5d62-

DEBUG [pool-533-thread-35]

[[]] cisco.profiler.infrastructure.profiling.ProfilerManager -:A90510AC0000005BD7DDDA7:::62cc7a10-5d62-

Policy Android matched 0A:5A:F0:B3:B5:9C (certainty 30)

com.cisco.profiler.infrastructure.profiling.ProfilerManager\$MatchingPolicyInternal@14ec7800

ステップ 4 : CoAと再認証

WiFi Device Analytics属性の変更が発生したため、ISEはエンドポイントセッションのCoAを送信する必要があります。

<#root>

2023-09-27 18:19:24,103

DEBUG [pool-533-thread-35]

```
[[]] cisco.profiler.infrastructure.profilng.ProfilerManager -:A90510AC000005BD7DDDA7::62cc7a10-5d62-
Endpoint 0A:5A:F0:B3:B5:9C IdentityGroup / Logical Profile Changed/ WiFi device analytics attribute char
2023-09-27 18:19:24,103
```

```
DEBUG [pool-533-thread-35]
```

```
[[]] cisco.profiler.infrastructure.profilng.ProfilerManager -:A90510AC000005BD7DDDA7::62cc7a10-5d62-
ConditionalCoAEvent with Endpoint Details : EndPoint[id=62caa550-5d62-11ee-bf1f-b6bb1580ab0d,name=] MAC:
Attribute:AAA-Server value:iselab Attribute:Airespace-Wlan-Id value:1 Attribute:AllowedProtocolMatched
Attribute:DEVICE_INFO_COUNTRY_CODE value:Unknown Attribute:DEVICE_INFO_DEVICE_FORM value:PHONE Attribute
Attribute:DTLSSupport value:Unknown Attribute:DestinationIPAddress value:172.16.5.112 Attribute:Destin
```

パケットキャプチャは、ISEがCoAをWLCに送信するのに役立ちます。また、CoAの処理後に新しいAccess-Requestパケットが受信されることも示しています。

111	2023-09-27 12:19:24.357572	172.16.5.112	172.16.5.169	RADIUS	244 CoA-Request id=13
112	2023-09-27 12:19:24.361138	172.16.5.169	172.16.5.112	RADIUS	111 CoA-ACK id=13

```

> Frame 111: 244 bytes on wire (1952 bits), 244 bytes captured (1952 bits)
> Ethernet II, Src: VMware_b3:f0:73 (00:50:56:b3:f0:73), Dst: Cisco_5c:16:ff (00:1e:f6:5c:16:ff)
> Internet Protocol Version 4, Src: 172.16.5.112, Dst: 172.16.5.169
> User Datagram Protocol, Src Port: 41440, Dst Port: 1700
< RADIUS Protocol
  Code: CoA-Request (43)
  Packet identifier: 0xd (13)
  Length: 202
  Authenticator: d622a25b73d3b2b475cf5d4ad2b00b5c
  [The response to this request is in frame 112]
  Attribute Value Pairs
  > AVP: t=NAS-IP-Address(4) l=6 val=172.16.5.169
  > AVP: t=Calling-Station-Id(31) l=19 val=0A:5A:F0:B3:B5:9C
    Type: 31
    Length: 19
    Calling-Station-Id: 0A:5A:F0:B3:B5:9C
  > AVP: t=Event-Timestamp(55) l=6 val=Sep 27, 2023 12:19:24.000000000 CST
  > AVP: t=Message-Authenticator(80) l=18 val=3edaf9ffdb25ceee5451e90a1cef21af
  < AVP: t=Vendor-Specific(26) l=43 vnd=ciscoSystems(9)
    Type: 26
    Length: 43
    Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=37 val=subscriber:reauthenticate-type=last
  < AVP: t=Vendor-Specific(26) l=41 vnd=ciscoSystems(9)
    Type: 26
    Length: 41
    Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=35 val=subscriber:command=reauthenticate
  < AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
    Type: 26
    Length: 49
    Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=43 val=audit-session-id=A90510AC000005BD7DDDA7

```

エンドポイントプロファイリング後のRADIUS CoAパケット

111	2023-09-27 12:19:24.357572	172.16.5.112	172.16.5.169	RADIUS	244 CoA-Request id=13
112	2023-09-27 12:19:24.361138	172.16.5.169	172.16.5.112	RADIUS	111 CoA-ACK id=13
113	2023-09-27 12:19:24.373874	172.16.5.169	172.16.5.112	RADIUS	480 Access-Request id=55
114	2023-09-27 12:19:24.386280	172.16.5.112	172.16.5.169	RADIUS	167 Access-Challenge id=55
115	2023-09-27 12:19:24.397609	172.16.5.169	172.16.5.112	RADIUS	557 Access-Request id=63
116	2023-09-27 12:19:24.400463	172.16.5.112	172.16.5.169	RADIUS	167 Access-Challenge id=63
117	2023-09-27 12:19:24.413943	172.16.5.169	172.16.5.112	RADIUS	720 Access-Request id=71
118	2023-09-27 12:19:24.456036	172.16.5.112	172.16.5.169	RADIUS	1179 Access-Challenge id=71
119	2023-09-27 12:19:24.477140	172.16.5.169	172.16.5.112	RADIUS	557 Access-Request id=79
120	2023-09-27 12:19:24.481172	172.16.5.112	172.16.5.169	RADIUS	1175 Access-Challenge id=79
121	2023-09-27 12:19:24.496743	172.16.5.169	172.16.5.112	RADIUS	557 Access-Request id=87
122	2023-09-27 12:19:24.499901	172.16.5.112	172.16.5.169	RADIUS	289 Access-Challenge id=87
123	2023-09-27 12:19:24.546538	172.16.5.169	172.16.5.112	RADIUS	715 Access-Request id=95
124	2023-09-27 12:19:24.553619	172.16.5.112	172.16.5.169	RADIUS	218 Access-Challenge id=95
125	2023-09-27 12:19:24.568069	172.16.5.169	172.16.5.112	RADIUS	557 Access-Request id=103
126	2023-09-27 12:19:24.571945	172.16.5.112	172.16.5.169	RADIUS	201 Access-Challenge id=103
127	2023-09-27 12:19:24.584229	172.16.5.169	172.16.5.112	RADIUS	594 Access-Request id=111
128	2023-09-27 12:19:24.588165	172.16.5.112	172.16.5.169	RADIUS	232 Access-Challenge id=111
129	2023-09-27 12:19:24.599493	172.16.5.169	172.16.5.112	RADIUS	648 Access-Request id=119
130	2023-09-27 12:19:24.624360	172.16.5.112	172.16.5.169	RADIUS	247 Access-Challenge id=119
131	2023-09-27 12:19:24.638515	172.16.5.169	172.16.5.112	RADIUS	592 Access-Request id=127
132	2023-09-27 12:19:24.642039	172.16.5.112	172.16.5.169	RADIUS	200 Access-Challenge id=127
133	2023-09-27 12:19:24.654578	172.16.5.169	172.16.5.112	RADIUS	557 Access-Request id=135
134	2023-09-27 12:19:24.677792	172.16.5.112	172.16.5.169	RADIUS	330 Access-Accept id=135

エンドポイントプロファイリング後のRADIUS CoAと新しいアクセス要求

関連情報

- [Cisco Identity Services Engine 管理者ガイド リリース 3.3](#)
- [Cisco Identity Services Engine, Release 3.3 のリリース ノート](#)
- [Identity Services Engineのサポートバンドルの収集](#)

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。