# 了解ISE 3.3上用于终端分类的Wifi分析

目录 简介 先决条件 要求 使用的组件 <u>背景信息</u> 配置 <u>WLC上的配置</u> 步骤1:全局启用设备分类功能 第二步: 启用TLV缓存和RADIUS分析 ISE上的配置 步骤1:在部署的PSN中启用分析服务 <u>第二步:在ISE PSN上启用RADIUS分析探测</u> <u>第三步:设置CoA类型和终端属性过滤器</u> <u>第四步:使用WiFi分析数据属性配置授权策略</u> <u>验证</u> 故障排除 步骤1:计费数据包到达ISE <u>第二步:ISE使用终端属性解析记账数据包</u> <u>第三步:终端属性已更新且终端已分类</u> <u>第四步:CoA和重新身份验证</u> 相关信息

# 简介

本文档介绍用于终端分类的WiFi分析的工作原理。还介绍了如何对其进行配置、验证和故障排除。

# 先决条件

# 要求

Cisco 建议您了解以下主题:

- 9800无线LAN控制器(WLC)配置
- 身份服务引擎(ISE)配置
- RADIUS 身份验证.授权和记帐(AAA)数据包流和术语

本文档假设已有一个正在运行的WLAN对使用ISE作为RADIUS服务器的客户端进行身份验证。 要使用此功能,必须至少具备以下条件:

- 9800 WLC Cisco IOS® XE都柏林17.10.1
- 识别服务引擎v3.3。
- 802.11ac Wave 2或802.11ax (Wi-Fi 6/6E) 接入点

# 使用的组件

本文档中的信息基于以下软件和硬件版本:

- 9800 WLC 思科IOSXE v17.12.x
- 身份服务引擎(ISE) v3.3
- Android 13设备

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

# 背景信息

通过WiFi设备分析,Cisco 9800 WLC可以从连接到此设备的一组终端获取属性(例如型号和操作系 统版本),并与ISE共享这些属性。然后,ISE可以将此信息用于终端分类(也称为分析)。

目前,以下供应商支持WiFi分析:

- 苹果
- 英特尔
- 三星

WLC使用RADIUS记账数据包与ISE服务器共享属性信息。



WiFi分析数据流

请务必记住,RADIUS AAA流上的RADIUS记账数据包仅在RADIUS服务器发送RADIUS Access-Accept数据包作为对终端身份验证尝试的应答后发送。按照顺序排列,WLC仅在RADIUS服务器 (ISE)和网络接入设备(WLC)之间为该终端建立RADIUS会话之后才共享终端属性信息。

以下是ISE可用于终端分类和授权的所有属性:

- DEVICE\_INFO\_FIRMWARE\_VERSION
- DEVICE\_INFO\_HW\_MODEL
- DEVICE\_INFO\_MANUALER\_MODEL
- DEVICE\_INFO\_MODEL\_NAME
- DEVICE\_INFO\_MODEL\_NUM
- DEVICE\_INFO\_OS\_VERSION
- DEVICE\_INFO\_VENDOR\_TYPE



注意:WLC可根据连接的终端类型发送更多属性,但只有列出的属性可用于在ISE中创建授 权策略。

ISE收到记账数据包后,即可处理和使用其中的此分析数据,并使用它重新分配终端配置文件/身份 组。 WiFi终端分析属性列在WiFi\_Device\_Analytics词典下。网络管理员可以在终端授权策略和条件中包含这些属性。

Select attribute for condition ×															
9	□ · · · · · · · · · · · · · · · · · · ·							O	F	Ŷ	)				
	Dictionary				Att	Attribute			ID		Info				
	W	Wifi_Device_Analytics ~ ×				Att	Attribute ID								
Ŀ	Wit	i_Devic	e_Ana	lytics		DEV	DEVICE_INFO_FIRMWARE				0				
Ŀ	Wifi_Device_Analytics				DEV	DEVICE_INFO_HW_MODEL					0				
E	Wifi_Device_Analytics				DEV	DEVICE_INFO_MANUFACT				0					
ъ	Wifi_Device_Analytics				DEV	DEVICE_INFO_MODEL_NA				0					
Ŀ	Wifi_Device_Analytics				DEV	DEVICE_INFO_MODEL_NUM				0					
ь	Wifi_Device_Analytics				DEV	DEVICE_INFO_OS_VERSION				0					
ъ	Wif	i_Devic	e_Ana	lytics		DEV	DEVICE_INFO_VENDOR_T					0			

WiFi设备分析词典

如果ISE为终端存储的当前属性值发生任何更改,则ISE会启动授权更改(CoA),允许对终端进行评估以计入更新的属性。

# 配置

WLC上的配置

步骤1:全局启用设备分类功能

导航到Configuration > Wireless > Wireless Global,然后选中Device Classification复选框。

# Configuration \* > Wireless \* > Wireless Global

Default Mobility Domain *	default
RF Group Name*	default
Maximum Login Sessions Per User*	0
Management Via Wireless	0
Device Classification	
AP LAG Mode	0
Dot15 Radio	0
Wireless Password Policy	None v (i

设备分类配置

# 第二步:启用TLV缓存和RADIUS分析

# 导航到配置>标签和配置文件>策略,选择RADIUS客户端所连接的WLAN所使用的策略配置文件。

Conf	Configuration * > Tags & Profiles * > Policy									
+	+ Add × Delete									
	Admin <b>Y</b> Status	Associated <b>() Y</b> Policy Tags	Policy Profile Name	Description						
	0	•	ise-policy							
	0		default-policy-profile	default policy profile						

无线策略选择

单击Access Policies,然后选中RADIUS Profiling、HTTP TLV Caching和DHCP TLV Caching选项。由于上一步中执行的操作,设备分类的全局状态现在显示为Enabled状态。

# **Edit Policy Profile**

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





RADIUS分析和缓存配置

登录到WLC CLI并启用dot11 TLV Accounting。

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

×



注意:使用此命令之前,必须禁用无线策略配置文件。此命令仅在Cisco IOS XE Dublin 17.10.1版本及更高版本上可用。

ISE上的配置

步骤1:在部署的PSN中启用分析服务

导航到管理>部署,点击PSN的名称。

# **Deployment Nodes**

							Selected 0 Total 1 🤮	Ø
0	Edit	Register	Syncup	🔂 Deregister			All $\sim$	$\nabla$
(	Hostname A Personas		Role(s)	Node Status				
		iselab		Administration, Monitoring, Policy Service	STANDALONE	SESSION, PROFILER		

ISE PSN节点选择

# 向下滚动到Policy Service部分并标记Enable Profiling Service复选框。点击保存按钮。

✓ Policy Service			
Enable Session Services			
Include Node in Node Group None ~	0		
Enable Profiling Service 🕢			
Enable Threat Centric NAC Service 🕢			
> Enable SXP Service			
Enable Device Admin Service ()			
Enable Passive Identity Service 🕡			
> pxGrid ()			
		Reset	Save

分析器服务配置

## 第二步:在ISE PSN上启用RADIUS分析探测

向上滚动到页面顶部,然后单击Profiling Configuration选项卡。此命令将显示可在ISE上使用的所有分析探测。启用RADIUS Probe并单击Save。

Deployment Nodes List > iselab

# Edit Node



**注意**:CoA数据包的标识字段始终为空,但终端ID与第一个身份验证数据包中的相同。



CoA详细信息显示在新的浏览器选项卡中。向下滚动到Other Attributes部分。

CoA源组件显示为分析器。CoA Reason显示为授权策略中使用的终端身份组/策略/逻辑配置文件的更改。

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/logical profile which are used in authorization policies
CoAReason Network Device Profile	Change in endpoint identity group/policy/logical profile which are used in authorization policies Cisco
CoAReason Network Device Profile Location	Change in endpoint identity group/policy/logical profile which are used in authorization policies Cisco Location#All Locations
CoAReason Network Device Profile Location Device Type	Change in endpoint identity group/policy/logical profile which are used in authorization policies Cisco Location#All Locations Device Type#All Device Types
CoAReason Network Device Profile Location Device Type IPSEC	Change in endpoint identity group/policy/logical profile which are used in authorization policies Cisco Location#All Locations Device Type#All Device Types IPSEC#Is IPSEC Device#No
CoAReason Network Device Profile Location Device Type IPSEC Device IP Address	Change in endpoint identity group/policy/logical profile which are used in authorization policies Cisco Location#All Locations Device Type#All Device Types IPSEC#Is IPSEC Device#No 172.16.5.169
CoAReason Network Device Profile Location Device Type IPSEC Device IP Address CPMSessionID	Change in endpoint identity group/policy/logical profile which are used in authorization policies Cisco Location#All Locations Device Type#All Device Types IPSEC#Is IPSEC Device#No 172.16.5.169 A90510AC0000005BD7DDDAA7

CoA触发组件和原因

导航到情景可视性(Context Visibility) >终端(Endpoints) >身份验证(Authentication)选项卡。在此选项卡上,使用过滤器查找测试终端

o

## 点击终端MAC地址以访问终端属性。

	MAC Address	Status	IP Address	Username	Hostname	Location	Endpoint Profile	Authen	Authentication	Authorization P
$\times$	0A:5A:F0:B3:B5:9C ×	Status ~	IP Address	Username	Hostname	Location	Endpoint Profile	Authentica	Authentication Polic	Authorization Policy
	0A:5A:F0:B3:B5:9C	۰.		bob	Victor-s-S22	Location	Android	-	Default	Wifi Endpoint Analy

情景可视性上的终端

### 此操作显示ISE存储的有关此终端的所有信息。点击属性部分,然后选择其他属性。

	AC ADDRESS: 0A:SA:F0:83:85:9C 2 2 2 0 Username: bob Endpoint Profile: Android Current IP Address: - Location: Location → All Locations	MFC Endpoint Type: Phone () MFC Hardware Manufacture: Samsung Electronics CoLtd () MFC Hardware Model: Samsung Galaxy S22+ () MFC Operating System: Android 13 ()	٥			
Applications Attributes Authentication Threats Vulnerabilities						
	Beneral Attributes Custom Attributes					

基于情景可视性的终端其他属性选择

向下滚动,直到找到WiFi\_Device\_Analytics词典属性。在此部分找到这些属性意味着ISE通过记帐数据包成功接收这些属性,并且可 用于终端分类。

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	мхо
DEVICE_INFO_VENDOR_TYPE	SAMSUNG

有关情景可视性的WiFi分析属性

以下是Windows 10和iPhone属性的示例,供您参考:

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

Windows 10终端

DEVICE_INFO_DEV	/ICE_FORM 0	
DEVICE_INFO_MO 11 PRO	DEL_NUM IPHON	NE
DEVICE_INFO_OS_	VERSION IOS 16	5.4
	DOR_TYPE 1	
iPhone终端属性示例		

## 在WLC CLI上,确保在策略配置文件配置中启用DOT11 TLV记账、DHCP TLV缓存和HTTP TLV缓存。

### <#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

连接终端时,收集WLC或ISE终端上的数据包捕获。您可以使用任何已知的数据包分析工具(如Wireshark)来分析收集的文件。

按RADIUS记账数据包和呼叫站ID (测试终端MAC地址)过滤。例如,可以使用以下过滤器:

radius.code == 4 && radius.Calling\_Station\_Id == "xx-xx-xx-xx-xx"

找到后,展开Cisco-AVPair字段以查找会计数据包中的WiFi Analytics Data。

NO.	Time		Source	Destination	Protocol	Length	Info
	104 2023-09-27 12	:19:23.584661	172.16.5.169	172.16.5.112	RADIUS	9	76 Accounting-Request id=39
_							
	> AVP: t=Vendor-Sp	pecific(26) l=28 v	nd=ciscoSystems(9)				
	> AVP: t=Vendor-Sp	pecific(26) l=36 v	nd=ciscoSystems(9)				
	> AVP: t=Vendor-Sp	pecific(26) l=39 v	nd=ciscoSystems(9)				
	> AVP: t=Vendor-Sp	pecific(26) l=36 v	<pre>/nd=ciscoSystems(9)</pre>				
	AVP: t=Vendor-Sp	pecific(26) l=49 v	<pre>nd=ciscoSystems(9)</pre>				
	Type: 26						
	Length: 49						
	Vendor ID: ci	scoSystems (9)					
	> VSA: t=Cisco-/	AVPair(1) l=43 va	l=dot11-device-info=\	000\000\000\023Samsung Galaxy S22+			
	AVP: t=Vendor-Sp	pecific(26) l=33 v	<pre>/nd=ciscoSystems(9)</pre>				
	Type: 26						
	Length: 33						
	Vendor ID: ci	scoSystems (9)					
	> VSA: t=C1sco-/	AVPair(1) L=2/ va	l=dot11-device-into=\	000/001/000/003WH6			
	AVP: t=vendor-Sp	pecific(26) l=33 \	nd=ciscoSystems(9)				
	Type: 20						
	Vender TD: ci	ccoSuctome (0)					
	VSA: t=Cisco-	AVPair(1) = 1-27 val	-dot11-device-info-	0001 0021 0001 003020			
	AVP: t=Vendor=Sr	ecific(26) = 1-31	und-ciscoSystems(0)	000 (002 (000 (003000			
	Type: 26		nu=c13c03y3ceiii3(37				
	Length: 31						
	Vendor ID: ci	scoSvstems (9)					
	> VSA: t=Cisco-/	AVPair(1) l=25 va	l=dot11-device-info=\	000\003\000\0011			
	AVP: t=Vendor-St	pecific(26) l=40 v	<pre>nd=ciscoSystems(9)</pre>				
	Type: 26						
	Length: 40						
	Vendor ID: ci	scoSystems (9)					
	> VSA: t=Cisco-/	AVPair(1) l=34 va	l=dot11-device-info=\	000\004\000\nAndroid 13			
	AVP: t=Vendor-Sp	pecific(26) l=37 v	<pre>vnd=ciscoSystems(9)</pre>				
	Type: 26						
	Length: 37						
	Vendor ID: ci	scoSystems (9)					
	> VSA: t=Cisco-/	AVPair(1) l=31 va	l=dot11-device-info=\	000\005\000\aUnknown			
	AVP: t=Vendor-Sp	pecific(26) l=31 v	nd=ciscoSystems(9)				
	Type: 26						
	Length: 31						
	Vendor ID: c1	SCOSYSTEMS (9)	-datil davida info				
	AVP: t=C1SCO-/	$\frac{AVPair(1)}{P} = \frac{1}{25} \frac{Va}{Va}$	(=dot11=dev1ce=1nto=\	000/0/00012		_	

记账数据包中的终端TLV属性

### 第二步:ISE使用终端属性解析记账数据包

在ISE端,可以将这些组件设置为调试级别,以确保然后WLC发送的RADIUS记账数据包到达ISE并正确处理。

## 然后,您可以收集ISE**支持捆**绑包以收集日志文件。有关如何收集支持捆绑的详细信息,请参阅相关信息部分。

	Component Name	Log Level	Description	Log file Name
×	Component Name	DEBUG V X	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

要调试以进行故障排除的组件



**注意**:仅在验证终端的PSN上启用组件以调试级别。

在iseLocalStore.log上,记帐-开始消息无需启用任何组件到调试级别。在这里,ISE必须看到包含WiFi分析属性的传入记帐数据包。

# <#root>

 $2023\text{-}09\text{-}27\ 18\text{:}19\text{:}23.600 + 00\text{:}00\ 0000035538\ 3000$ 

NOTICE Radius-Accounting: RADIUS Accounting start request,

ConfigVersionId=1493, Device IP Address=172.16.5.169,

UserName=bob

, NetworkDeviceName=lab-wlc, User-Name=bob, NAS-IP-Address=172.16.5.169, NAS-Port=260613, Framed-IP-Address=172.16.5.76, Class=CACS:A90510AC0000005BD7DDDAA7:iselab/484624451/303, Called-Station

#### Calling-Station-ID=0a-5a-f0-b3-b5-9c

, NAS-Identifier=vimontes-wlc, Acct-Status-Type=Start, Acct-Delay-Time=0, Acct-Session-Id=00000018, Acct-Authentic=Remote, Event-Timestamp=1695838756, NAS-Port-Type=Wireless - IEEE 802.11, cisco-av-pair=cisco-av-pair=dc-device-name=Victor-s-S22, cisco-av-pair=dc-device-class-tag=Samsung Galaxy S22+, cisco cisco-av-pair=64:63:2d:6f:70:61:71:75:65:3d:01:00:00:00:00:00:00:00:00:00:00:00, cisco-av-pair=dc-protocisco-av-pair=dhcp-option=dhcp-class-identifier=android-dhcp-13, cisco-av-pair=dhcp-option=dhcp-parameter

cisco-av-pair=dot11-device-info=DEVICE\_INFO\_MODEL\_NUM=Samsung Galaxy S22+, cisco-av-pair=dot11-device-ir

cisco-av-pair=dot11-device-info=DEVICE\_INFO\_SALES\_CODE=MXO, cisco-av-pair=dot11-device-info=DEVICE\_INFO\_

cisco-av-pair=dot11-device-info=DEVICE\_INFO\_OS\_VERSION=Android 13, cisco-av-pair=dot11-device-info=DEVICE

#### cisco-av-pair=dot11-device-info=DEVICE\_INFO\_VENDOR\_TYPE=2,

cisco-av-pair=audit-session-id=A90510AC0000005BD7DDDAA7, cisco-av-pair=vlan-id=2606, cisco-av-pair=met cisco-av-pair=cisco-wlan-ssid=VIcSSID, cisco-av-pair=wlan-profile-name=ISE-AAA, Airespace-Wlan-Id=1, Ac RequestLatency=15, Step=11004, Step=11017, Step=15049, Step=15008, Step=22083, Step=11005, NetworkDevice NetworkDeviceGroups=Device Type#All Device Types,

#### CPMSessionID=A90510AC000005BD7DDDAA7

, TotalAuthenLatency=15, ClientLatency=0, Network Device Profile=Cisco, Location=Location#All Locations Device Type=Device Type#All Device Types, IPSEC=IPSEC#Is IPSEC Device#No,

在prrt-server.log上,ISE解析收到的计费数据包系统日志消息,包括WiFi分析属性。请使用**CallingStationID**和**CPMSessionID**字段确保 跟踪正确的会话和终端。

### <#root>

Radius,2023-09-27 18:19:23,586,

DEBUG,0x7f50a2b67700,

cntx=0000192474, sesn=iselab/484624451/304,

CPMSessionID=A90510AC000005BD7DDDAA7

```
CallingStationID=0a-5a-f0-b3-b5-9c
```

,FramedIPAddress=172.16.5.76,

```
RADIUS PACKET::
```

Code=4(AccountingRequest)

```
Identifier=39 Length=934
```

[1] User-Name - value: [bob]

[4] NAS-IP-Address - value: [172.16.5.169] [5] NAS-Port - value: [260613] [8] Framed-IP-Address - valu 26] cisco-av-pair - value: [dot11-device-info=<00><00><13>Samsung Galaxy S22+] [26] cisco-av-pair -[26] cisco-av-pair - value: [audit-session-id=A90510AC0000005BD7DDDAA7] [26] cisco-av-pair - value: [v

#### 第三步:终端属性已更新且终端已分类

然后,将与Profiler组件共享此系统日志消息。Profiler.log接收解析的系统日志消息并提取终端属性。

#### <#root>

2023-09-27 1

8:19:23,601 DEBUG [SyslogListenerThread]

[[]] cisco.profiler.probes.radius.SyslogMonitor -::::-

#### Radius Packet Received 1266

2023-09-27

18:19:23,601 DEBUG [SyslogListenerThread]

[[]] cisco.profiler.probes.radius.SyslogDefragmenter -::::- parseHeader inBuffer=<181>Sep 27 18:19:23

CISE\_RADIUS\_Accounting 000000297

3 0 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,

#### UserName=bob

, NetworkDeviceName=lab-wlc, User-Name=bob, NAS-IP-Address=172.16.5.169, NAS-Port=260613, Framed-IP-Add Called-Station-ID=00-1e-f6-5c-16-ff,

#### Calling-Station-ID=0a-5a-f0-b3-b5-9c

, NAS-Identifier=vimontes-wlc, Acct-Status-Type=Start, Acct-Delay-Time=0, Acct-Session-Id=00000018, Acc Event-Timestamp=1695838756, NAS-Port-Type=Wireless - IEEE 802.11, cisco-av-pair=dc-profile-name=Samsung cisco-av-pair=dc-device-class-tag=Samsung Galaxy S22+, cisco-av-pair=dc-certainty-metric=40, cisco-av-pair=64:63:2d:6f:70:61:71:75:65:3d:01:00:00:00:00:00:00:00:00:00:00:00; cisco-av-pair=dc-proto

### 18:19:23,601 DEBUG

[SyslogListenerThread][[]] cisco.profiler.probes.radius.SyslogMonitor -:::::-

#### Radius Packet Received 1267

2023-09-27

#### 18:19:23,601 DEBUG

[SyslogListenerThread][[]] cisco.profiler.probes.radius.SyslogDefragmenter -::::- parseHeader inBuffe

# CISE\_RADIUS\_Accounting 0000000297 3 1

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,

#### 终端属性信息已更新。

```
<#root>
2023-09-27 18:19:23,602
DEBUG [RADIUSParser-1-thread-2][[]]
cisco.profiler.probes.radius.RadiusParser -: A90510AC0000005BD7DDDAA7::::-
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 -: A90510AC0000005BD7DDDAA7::::-
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 -: A90510AC0000005BD7DDDAA7::::-
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 -: A90510AC0000005BD7DDDAA7::::-
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 -: A90510AC0000005BD7DDDAA7::::-
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 -: A90510AC0000005BD7DDDAA7::::-
```

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 -:A90510AC0000005BD7DDDAA7::::- 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

属性更新会触发新的终端分析事件。分析策略会再次评估,并分配新的配置文件。

#### <#root>

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

DEBUG [pool-533-thread-35]

[[]] cisco.profiler.infrastructure.profiling.ProfilerManager -:A90510AC0000005BD7DDDAA7::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 -: A90510AC000005BD7DDDAA7::62cc7a10-5d62-DEBUG [pool-533-thread-35]

[[]] cisco.profiler.infrastructure.profiling.ProfilerManager -: A90510AC0000005BD7DDDAA7::62cc7a10-5d62--Policy Android matched 0A:5A:F0:B3:B5:9C (certainty 30)

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

第四步:CoA和重新身份验证

当WiFi设备分析属性发生更改时,ISE必须为终端会话发送CoA。

#### <#root>

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

DEBUG [pool-533-thread-35]

[[]] cisco.profiler.infrastructure.profiling.ProfilerManager -: A90510AC0000005BD7DDDAA7::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.profiling.ProfilerManager -:A90510AC000005BD7DDDAA7::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

数据包捕获有助于确保ISE向WLC发送CoA。它还显示处理CoA后收到新的访问请求数据包。

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				
<ul> <li>Frame 111: 244 bytes on wire (1952 bits), 244 bytes captured (1952 bits)</li> <li>Ethernet II, Src: VMware_b3:f0:73 (00:50:56:b3:f0:73), Dst: Cisco_5c:16:ff (00:1e:f6:5c:16:ff)</li> <li>Internet Protocol Version 4, Src: 172.16.5.112, Dst: 172.16.5.169</li> <li>User Datagram Protocol, Src Port: 41440, Dst Port: 1700</li> <li>PADIUS Protocol</li> </ul>								
Code: CoA-Request (43) Packet identifier: 0xd (13) Length: 202 Authenticator: d622a25b73d3b2b475cf5d [The response to this request is in f	4ad2b00b5c rame 112]							
<ul> <li>Attribute Value Pairs</li> </ul>								
> 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:E	5:9C							
<pre>&gt; AVP: t=Event-Timestamp(55) l=6 val=</pre>	Sep 27, 2023 12:19:24.00	0000000 CST						
> AVP: t=Message-Authenticator(80) l=	18 val=3edaf9ffdb25ceee	5451e90a1ce†21a†						
<ul> <li>AVP: t=vendor-Specific(26) l=43 vnd</li> <li>Tuno: 26</li> </ul>	=ciscoSystems(9)							
Type: 26								
Vendor ID: ciscoSystems (9)								
<pre>&gt; VSA: t=Cisco-AVPair(1) l=37 val=s</pre>	ubscriber:reauthenticat	e-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=s	ubscriber:command=reaut	henticate						
~ AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)								
Type: 26								
Length: 49								
Vendor ID: CISCOSystems (9)	udit_coscion_id=A00510A							
VSA: (-CISCO-AVPair(1) (=45 Val=a	uurr-36221011-10-A90210A	C000003507000AK7						

终端分析后的Radius CoA数据包

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

终端分析后的Radius CoA和新访问请求

- <u>思科身份服务引擎管理员指南,版本3.3</u>
- <u>思科身份服务引擎版本说明,版本3.3</u>
- <u>收集身份服务引擎上的支持捆绑包</u>

# 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。