Comprendere Wifi Analytics per la classificazione degli endpoint su ISE 3.3

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Premesse
Configurazione
Configurazioni su WLC
Passaggio 1. Abilita globalmente la funzionalità di classificazione dei dispositivi
Passaggio 2. Abilita memorizzazione nella cache TLV e profilatura RADIUS
Configurazioni su ISE
Passaggio 1. Abilitare i servizi di profilatura nei PSN nella distribuzione
Passaggio 2. Abilita la sonda di profilatura RADIUS su ISE PSN
Passaggio 3. Imposta filtro attributi endpoint e tipo CoA
Passaggio 4. Configurare i criteri di autorizzazione con gli attributi dei dati di WiFi Analytics
<u>Verifica</u>
Risoluzione dei problemi
Passaggio 1. Pacchetti contabili raggiunti da ISE
Passaggio 2. ISE analizza il pacchetto di accounting con gli attributi dell'endpoint
Passaggio 3. Gli attributi dell'endpoint vengono aggiornati e l'endpoint viene classificato
Passaggio 4. CoA e riautenticazione
Informazioni correlate

Introduzione

In questo documento viene descritto il funzionamento di WiFi Analytics for Endpoint Classification. Viene inoltre descritto come configurarlo, verificarlo e risolverlo.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione dei Wireless LAN Controller (WLC) 9800
- Configurazione Identity Services Engine (ISE)
- Autenticazione RADIUS. Flusso e terminologia dei pacchetti AAA (Authorization and Accounting)

in questo documento si presume che vi siano già client di autenticazione WLAN funzionanti che utilizzano ISE come server RADIUS.

Affinché questa funzionalità funzioni, è necessario disporre almeno di:

- 9800 WLC Cisco IOS® XE Dublino 17.10.1
- Identificare Services Engine v3.3.
- Access point 802.11ac Wave2 o 802.11ax (Wi-Fi 6/6E)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- 9800 WLC Cisco IOS XE v17.12.x
- Identity Services Engine (ISE) v3.3
- Dispositivo Android 13

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Tramite WiFi Device Analytics, Cisco 9800 WLC può imparare gli attributi, come il numero di modello e la versione del sistema operativo, da un set di endpoint connessi a questo dispositivo e condividerlo con ISE. ISE può quindi utilizzare queste informazioni per la classificazione degli endpoint, nota anche come profilatura.

Attualmente, WiFi Analytics è supportato per questi fornitori:

- Apple
- Intel
- Samsung

Il WLC condivide le informazioni sugli attributi con il server ISE usando i pacchetti di accounting RADIUS.

Flusso di dati di



WiFi Analytics

È importante ricordare che i pacchetti di accounting RADIUS su un flusso AAA RADIUS vengono inviati solo dopo che il server RADIUS invia un pacchetto RADIUS Access-Accept come risposta al tentativo di autenticazione dell'endpoint. In poche parole, il WLC condivide le informazioni degli attributi dell'endpoint solo dopo che è stata stabilita una sessione RADIUS per l'endpoint tra il server RADIUS (ISE) e il dispositivo di accesso alla rete (WLC).

Questi sono tutti gli attributi che ISE può usare per la classificazione e l'autorizzazione degli endpoint:

- VERSIONE_FIRMWARE_INFO_DISPOSITIVO
- MODELLO_INFO_DISPOSITIVO
- DEVICE_INFO_MANUFACTURER_MODEL
- NOME_MODELLO_INFO_DISPOSITIVO
- NUM_MODELLO_INFO_DISPOSITIVO
- VERSIONE_INFO_DISPOSITIVO
- TIPO_FORNITORE_INFO_DISPOSITIVO



Nota: il WLC può inviare più attributi a seconda del tipo di endpoint che si connette, ma solo quelli elencati possono essere utilizzati per la creazione dei criteri di autorizzazione in ISE.

Una volta ricevuto il pacchetto di accounting, ISE può elaborare e utilizzare i dati di analisi in esso contenuti e riassegnare un profilo dell'endpoint/gruppo di identità.

Gli attributi di WiFi Endpoint Analytics sono elencati nel dizionario WiFi_Device_Analytics. Gli amministratori di rete possono includere questi attributi nei criteri e nelle condizioni di autorizzazione degli endpoint.

Select attribute for condition ×																
Q	ŋ	0	串	۲	P	Ţ	8				©	1	o	Ŀ	Ŷ	J
	Dictionary				Att	Attribute				ID		Info				
	w	fi_Devi	ce_An	ilytics'	×	Att	Attribute				ID					
Ŀ	WB	i_Devic	e_Ana	lytics		DEV	DEVICE_INFO_FIRMWARE						0			
Ŀ	Wit	i_Devic	ce_Ana	lytics		DEVICE_INFO_HW_MODEL						0				
£	Wif	i_Devic	e_Ana	lytics		DEVICE_INFO_MANUFACT			(0					
F	Wit	i_Devic	e_Ana	lytics		DEV	DEVICE_INFO_MODEL_NA					0	0			
Ŀ	Wifi_Device_Analytics					DEVICE_INFO_MODEL_NUM					0					
E	Wifi_Device_Analytics				DEVICE_INFO_OS_VERSION						0					
ъ	& Wifi_Device_Analytics					DEVICE_INFO_VENDOR_T				0						

Dizionario analisi dispositivo WiFi

Se vengono apportate modifiche ai valori degli attributi correnti archiviati da ISE per l'endpoint, ISE avvia un processo CoA (Change of Authorization), che consente di valutare l'endpoint tenendo conto degli attributi aggiornati.

Configurazione

Configurazioni su WLC

Passaggio 1. Abilita globalmente la funzionalità di classificazione dei dispositivi

Passare a Configurazione > Wireless > Globale wireless e selezionare la casella di controllo Classificazione dispositivo.

Configuration * > Wireless * > Wireless Global

Default Mobility Domain *	default
RF Group Name*	default
Maximum Login Sessions Per User*	0
Management Via Wireless	
Device Classification	
Device Classification AP LAG Mode	
Device Classification AP LAG Mode Dot15 Radio	

Configurazione classificazione dispositivi

Passaggio 2. Abilita memorizzazione nella cache TLV e profilatura RADIUS

Passare a Configurazione > Tag e profili > Criterio e selezionare il Profilo criterio utilizzato dalla WLAN a cui si connettono i client RADIUS.

Configuration * > Tags & Profiles * > Policy									
+ Add × Delete Clone									
	Admin Y Status	Associated 0 T Policy Tags	Policy Profile Name	Description					
	٢	•	ise-policy						
0	0		default-policy-profile	default policy profile					

Selezione criteri wireless

Fare clic su Criteri di accesso e selezionare le opzioni Profiling RADIUS, HTTP TLV Caching e DHCP TLV Caching. A causa dell'azione eseguita nel passaggio precedente, lo stato globale della classificazione del dispositivo ora è impostato su Attivato.

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.





Configurazione profilatura e memorizzazione nella cache RADIUS

Accedere alla CLI del WLC e abilitare l'accounting TLV dot11.

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

×



Nota: prima di utilizzare questo comando, è necessario disabilitare il profilo dei criteri wireless. Questo comando è disponibile solo nella versione 17.10.1 di Cisco IOS XE Dublino e successive.

Configurazioni su ISE

Passaggio 1. Abilitare i servizi di profilatura nei PSN nella distribuzione

Passare a Amministrazione > Distribuzione e fare clic sul nome del numero di serie del servizio.

Deployment Nodes

	0.0					Selected 0 lotal 1	*
Edit	B Register	5 Syncup	lo Deregister			All V	v
	Hostname	^	Personas	Role(s)	Services	Node Status	
	iselab		Administration, Monitoring, Policy Service	STANDALONE	SESSION, PROFILER		

ISE PSN Node Selection

Scorrere verso il basso fino alla sezione **Policy Service** e selezionare la casella di controllo **Enable Profiling Service** (Abilita servizio di profilatura). Fare clic sul pulsante **Salva**.

Policy S	arvice			
🗹 🗸 Enab	e Session Services			
Include	Node in Node Group None	~ 0		
🗹 Enable Profi	ing Service 🕡			
Enable Three	It Centric NAC Service 🕠			
□ > Enab	e SXP Service			
Enable Devi	ce Admin Service 🕕			
Enable Pass	ive Identity Service 🕡			
> pxGrid	O			
			Reset	Save
Configurazione ser	vizi profiler			

Passaggio 2. Abilita la sonda di profilatura RADIUS su ISE PSN

Scorrere la pagina verso l'alto e fare clic sulla scheda **Configurazione profilo**. In questo modo vengono visualizzate tutte le sonde di profilatura disponibili per l'uso con ISE. Attivate la **sonda RADIUS** e fate clic su **Salva** (**Save**).

Deployment Nodes List > iselab

Edit Node



Nota: il pacchetto CoA contiene sempre un campo Identity vuoto, ma l'ID endpoint è lo stesso del primo pacchetto di autenticazione.

Fare clic sull'icona disponibile nella colonna Dettagli del record Modifica di autorizzazione.



Accesso ai dettagli del pacchetto CoA

Le informazioni dettagliate sul CoA vengono visualizzate in una nuova scheda del browser. Scorrere verso il basso fino alla sezione Altri attributi.

Il componente di origine CoA viene visualizzato come profiler. Il motivo CoA viene visualizzato come Modifica nel profilo logico/gruppo di identità dell'endpoint utilizzato nei criteri di autorizzazione.

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 Clisco Location#All Locations Device Type#All Device Types IPSEC#Is IPSEC Device#No 172.16.5.169 A90510AC0000005BD7DDDAA7

Componente di attivazione CoA e motivo

Passare a Visibilità contesto > Endpoint > scheda Autenticazione. In questa scheda utilizzare i filtri per individuare l'endpoint di test.

Fare clic sull'indirizzo MAC dell'endpoint per accedere agli attributi dell'endpoint.

	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	Authentica	Authentication Polic	Authorization Policy
	0A:5A:F0:B3:B5:9C	*L.		bob	Victor-s-S22	Location	Android	-	Default	Wifi Endpoint Analy

Visibilità endpoint nel contesto

Questa azione consente di visualizzare tutte le informazioni memorizzate da ISE sull'endpoint. Fare clic su Attributi sezione, quindi selezionare Altri attributi.

MAC ADDRESS: 0A:5A:F0:03:05:9C 2 2 0 Username: bob Endpoint Profile: Android Current IP Address: -	MFC Endpoint Type: Phone ③ MFC Hardware Manufacturer: Samsung Electronics Co.,Ltd ③ MFC Hardware Model: Samsung Galaxy S22+ ①	0
Applications Authentication Threats Vulnerabilities	MFC Operating System: Android 13 ()	đanage 🗸
General Attributes Custom Attributes Other Attributes		

Selezione di altri attributi dell'endpoint in base alla visibilità del contesto

Scorrere verso il basso fino a individuare gli attributi del **dizionario WiFi_Device_Analytics**. L'individuazione di questi attributi in questa sezione indica che ISE li ha ricevuti correttamente tramite i pacchetti di accounting e che possono essere utilizzati per la classificazione degli endpoint.

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

Attributi di WiFi Analytics sulla visibilità del contesto

Di seguito sono riportati alcuni esempi di attributi di Windows 10 e iPhone da utilizzare come riferimento:

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

Esempio di

DEVICE_INFO_DEVICE_FORM 0 DEVICE_INFO_MODEL_NUM IPHONE 11 PRO DEVICE_INFO_OS_VERSION IOS 16.4 DEVICE_INFO_VENDOR_TYPE 1

attributi dell'endpoint Windows 10Esempio di attributi dell'endpoint iPhone

Passaggio 1. Pacchetti contabili raggiunti da ISE

Dalla CLI del WLC, verificare che l'accounting TLV DOT11, la cache TLV DHCP e la cache TLV HTTP siano abilitate nelle configurazioni del profilo dei criteri.

<#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

Raccogliere le **acquisizioni dei pacchetti** sulle estremità WLC o ISE durante la connessione a un endpoint. È possibile utilizzare qualsiasi strumento di analisi dei pacchetti noto, ad esempio Wireshark, per analizzare i file raccolti.

Filtra in base ai pacchetti di accounting RADIUS e all'ID della stazione chiamante (verifica dell'indirizzo MAC dell'endpoint). Ad esempio, questo filtro può essere utilizzato:

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

Una volta individuati, espandere i campi Cisco-AVPair per individuare i dati di analisi WiFi nel pacchetto di accounting.

No.	Time		Source	Destination	Protocol	Length	Info
τ*	104 2023-09-27 12:19:2	23.584661	172.16.5.169	172.16.5.112	RADIUS		976 Accounting-Request id=39
_							
	> AVP: t=Vendor-Specif	ic(26) l=28	vnd=ciscoSystems(9)				
	> AVP: t=Vendor-Specif	ic(26) l=36	vnd=ciscoSystems(9)				
	AVP: t=Vendor-Specif	ic(26) l=39	vnd=ciscoSystems(9)				
	AVP: t=Vendor-Specif	ic(26) l=36	vnd=ciscoSystems(9)				
	AVP: t=Vendor-Specif	ic(26) l=49	vnd=ciscoSystems(9)				
	Type: 26						
	Length: 49						
	Vendor ID: ciscoSy	/stems (9)					
	> VSA: t=Cisco-AVPai	ir(1) l=43 v	al=dot11-device-info=\0	000\000\000\023Samsung Galaxy	S22+		
	AVP: t=Vendor-Specif	ic(26) l=33	vnd=ciscoSystems(9)				
	Type: 26						
	Length: 33	(D)					
	VENDOF ID: CISCOSY	stems (9)	al-dat11_davice_info=)(000 001 000 002006			
	AVP: t=Vendor_Specif	$i_{1}(1) = 27$	vpd=ciscoSystems(0)	000/001/000/005Wh0			
	Type: 26	10(20) (-33	vila=ciscosystems(s)				
	Length: 33						
	Vendor ID: ciscoSy	stems (9)					
	> VSA: t=Cisco-AVPai	ir(1) l=27 v	al=dot11-device-info=\(000\002\000\003MX0			
	AVP: t=Vendor-Specif	ic(26) l=31	vnd=ciscoSystems(9)				
	Type: 26						
	Length: 31						
	Vendor ID: ciscoSy	/stems (9)					
	VSA: t=Cisco-AVPai	ir(1) l=25 va	al=dot11-device-info=\0	000\003\000\0011			
	AVP: t=Vendor-Specif	ic(26) l=40	vnd=ciscoSystems(9)				
	Type: 26						
	Length: 40						
	Vendor ID: ciscoSy	/stems (9)					
	> VSA: t=C1sco-AVPai	Lr(1) L=34 V	al=dot11-device-info=\0	000\004\000\nAndroid 13			
	AVP: t=Vendor-Specif	1C(26) L=37	vnd=clscoSystems(9)				
	Type: 26						
	Vender TD: ciccoSu	(ctome (D)					
	VSA: t=Cisco=AVPai	r(1) = 31 w	al=dot11_device_info=\(00) 005) 000) allokoown			
	AVP: t=Vendor=Specif	ic(26) 1=31	vnd=ciscoSystems(9)	000 (000 (000 (dolikilowi			
	Type: 26	10(20) (-31	The Clacoby a cema (a)				
	Length: 31						
_	Vendor ID: ciscoSy	/stems (9)					
	> VSA: t=Cisco-AVPai	ir(1) l=25 v	al=dot11-device-info=\0	000\n\000\0012			
	> AV/D: t-Eramod_TD_Add	ress(9) 1-6	val-172 16 5 76				

Attributi TLV endpoint all'interno di un pacchetto di accounting

Passaggio 2. ISE analizza il pacchetto di accounting con gli attributi dell'endpoint

All'estremità ISE, questi componenti possono essere impostati sul livello DEBUG per garantire che i pacchetti di accounting RADIUS inviati dal WLC raggiungano l'ISE e vengano elaborati correttamente.

È quindi possibile raccogliere il **pacchetto di supporto ISE** per raccogliere i file di log. Per ulteriori informazioni su come raccogliere il pacchetto di supporto, fare riferimento alla sezione **Informazioni correlate**.

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

Componenti di cui eseguire il debug per la risoluzione dei problemi



Nota: i componenti sono abilitati al livello DEBUG solo sul PSN che autentica gli endpoint.

Su iseLocalStore.log, il messaggio Accounting-Start viene registrato senza la necessità di abilitare alcun componente al livello DEBUG. Qui, ISE deve vedere il pacchetto di accounting in ingresso contenente gli attributi WiFi Analytics.

<#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,

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-in

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,

Su port-server.log, ISE analizza il messaggio syslog del pacchetto di accounting ricevuto, inclusi gli attributi di WiFi Analytics. Utilizzare i campi **CallingStationID** e **CPMSessionID** per garantire la registrazione della sessione e dell'endpoint corretti.

<#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 value 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

Passaggio 3. Gli attributi dell'endpoint vengono aggiornati e l'endpoint viene classificato

Questo messaggio syslog viene quindi condiviso con il componente profiler. Profiler.log riceve il messaggio syslog analizzato ed estrae gli attributi dell'endpoint.

<#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 000000297 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_(

```
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,
```

Le informazioni sugli attributi dell'endpoint vengono aggiornate.

<#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::::-
```

<#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

L'aggiornamento dell'attributo attiva un nuovo evento di profilatura dell'endpoint. I criteri di profilatura vengono valutati di nuovo e viene assegnato un nuovo profilo.

<#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 -:A90510AC0000005BD7DDDAA7::62cc7a10-5d62-DEBUG [pool-533-thread-35]

[[]] cisco.profiler.infrastructure.profiling.ProfilerManager -: A90510AC000005BD7DDDAA7::62cc7a10-5d62-Policy Android matched 0A:5A:F0:B3:B5:9C (certainty 30)

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

Passaggio 4. CoA e riautenticazione

ISE deve inviare un CoA per la sessione dell'endpoint quando è stata apportata una modifica agli attributi di WiFi Device Analytics.

<#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 changed

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:Destination

L'acquisizione dei pacchetti aiuta a garantire che ISE invii il CoA al WLC. Mostra anche che viene ricevuto un nuovo pacchetto Access-Request dopo l'elaborazione del CoA.

L	- 111 2023-09-27 12:19:24.357572 - 112 2023-09-27 12:19:24.361138	172.16.5.112 172.16.5.169	172.16.5.169 172.16.5.112	RADIUS RADIUS	244 CoA-Request id=13 111 CoA-ACK id=13
~ ~ ~ ~ ~	Frame 111: 244 bytes on wire (1952 Ethernet II, Src: VMware_b3:f0:73 (Internet Protocol Version 4, Src: 1 User Datagram Protocol, Src Port: 4 RADIUS Protocol	bits), 244 bytes captured (1 00:50:56:b3:f0:73), Dst: Cis 72.16.5.112, Dst: 172.16.5.1 1440, Dst Port: 1700	.952 bits) :co_5c:16:ff (00:1e:f6:5c:16 69 	:ff)	·
	Code: CoA-Request (43) Packet identifier: 0xd (13) Length: 202 Authenticator: d622a25b73d3b2b475 IThe response to this request is > AVP: t=NA5-IP-Address(4) l=6 vz > AVP: t=Calling-Station-Id(31) I Type: 31 Length: 19 Calling-Station-Id: 0A:5A:F0: > AVP: t=Event-Timestamp(55) l=6 > AVP: t=Event-Timestamp(55) l=6 > AVP: t=Event-Timestamp(55) l=6 > AVP: t=Event-Specific(26) l=43 Type: 26 Length: 43 Vendor ID: ciscoSystems (9) > VSA: t=Cisco-AVPair(1) l=37 v < AVP: t=Vendor-Specific(26) l=41 Type: 26 Length: 41 Vendor ID: ciscoSystems (9) > VSA: t=Cisco-AVPair(1) l=35 v < AVP: t=Vendor-Specific(26) l=42 Type: 26 Length: 49 Vendor ID: ciscoSystems (9) > VSA: t=Cisco-AVPair(1) l=35 v < AVP: t=Vendor-Specific(26) l=45 Type: 26 Length: 49 Vendor ID: ciscoSystems (9) > VSA: t=Cisco-AVPair(1) l=34 v 	cf5d4ad2b00b5c in frame 112] l=172.16.5.169 =19 val=0A:5A:F0:B3:B5:9C val=Sep 27, 2023 12:19:24.0() l=18 val=3edaf9ffdb25ceeet vnd=ciscoSystems(9) val=subscriber:reauthenticat vnd=ciscoSystems(9) val=subscriber:command=reaut vnd=ciscoSystems(9) val=subscriber:command=reaut vnd=ciscoSystems(9)	00000000 CST 5451e90a1cef21af e-type=last henticate C0000005BD7DDDAA7		

Pacchetto CoA Radius dopo profilatura endpoint

111 2023-09-27 12:19:24.357572	172.16.5.112	172.16.5.169	RADIUS	244 CoA-Request 1d=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

Radius CoA e nuova richiesta di accesso dopo la profilatura degli endpoint

Informazioni correlate

- <u>Guida dell'amministratore di Cisco Identity Services Engine, versione 3.3</u>
- Note sulla versione di Cisco Identity Services Engine, versione 3.3
- Raccogli pacchetto di supporto su Identity Services Engine

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).