Esempio di configurazione dell'opzione 55 dell'elenco di richieste dei parametri DHCP usata per profilare gli endpoint

Sommario

Introduzione

In questo documento viene descritto come usare l'opzione 55 dell'elenco di richieste dei parametri DHCP come metodo alternativo per profilare i dispositivi che usano Identity Services Engine (ISE).

Prerequisiti

Requisiti

Cisco raccomanda:

- Conoscenze base del processo di rilevamento DHCP
- Esperienza nell'uso di ISE per configurare regole di profiling personalizzate

Componenti usati

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

- ISE versione 3.0
- Windows 10

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.

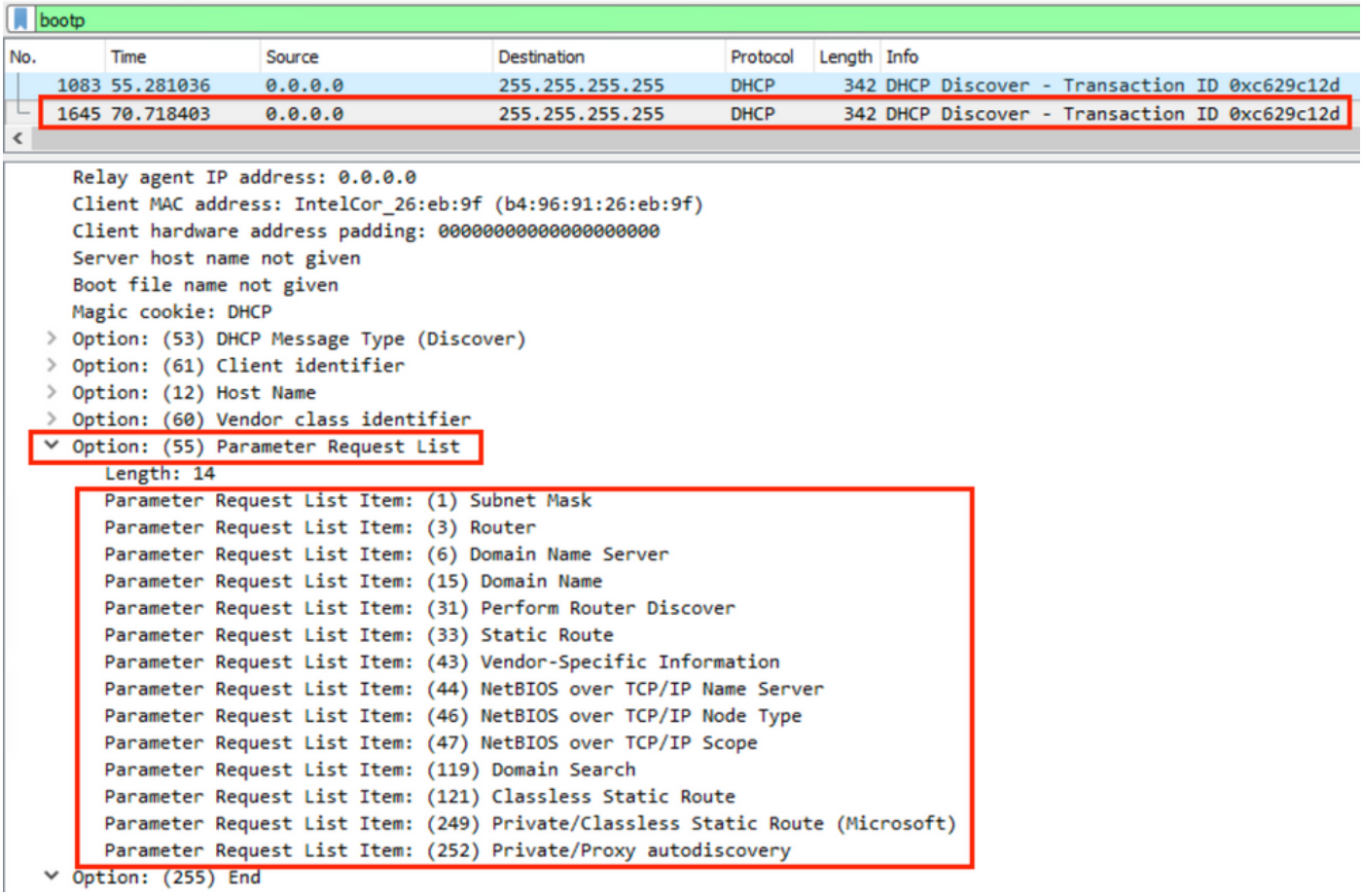
Premesse

Nelle distribuzioni ISE di produzione, alcune delle sonde di profilatura più comuni includono RADIUS, HTTP e DHCP. Con il reindirizzamento degli URL al centro del flusso di lavoro ISE, la sonda HTTP viene ampiamente utilizzata per acquisire dati importanti sull'endpoint dalla stringa User-Agent. Tuttavia, in alcuni scenari di produzione, non è desiderato il reindirizzamento dell'URL e si preferisce il dot1x, il che rende più difficile la profilatura accurata di un endpoint. Ad esempio, un PC dipendente che si connette a un SSID (Service Set Identifier) aziendale ottiene l'accesso completo, mentre il relativo iDevice personale (iPhone, iPad, iPod) ottiene solo l'accesso a Internet. In entrambi gli scenari, gli utenti vengono profilati e mappati dinamicamente a un gruppo di identità più specifico per la corrispondenza del profilo di autorizzazione che non si basa sull'utente per aprire un browser Web. Un'altra alternativa comunemente utilizzata è la corrispondenza dei nomi host. Questa soluzione non è perfetta perché gli utenti potrebbero modificare il nome host dell'endpoint in un valore non standard.

In questi casi, l'opzione 55 dell'elenco di richieste dei parametri DHCP e della sonda DHCP può essere usata come metodo alternativo per profilare questi dispositivi. Il campo Parameter Request List (Elenco richieste parametri) nel pacchetto DHCP può essere usato per rilevare le impronte digitali di un sistema operativo di endpoint, in modo simile a quando un sistema di prevenzione delle intrusioni (IPS) usa una firma per identificare un pacchetto. Quando il sistema operativo dell'endpoint invia un pacchetto di rilevamento o di richiesta DHCP in transito, il produttore include un elenco numerico di opzioni DHCP che intende ricevere dal server DHCP (router predefinito, DNS (Domain Name Server), server TFTP, ecc.). L'ordine in base al quale il client DHCP richiede queste opzioni al server è abbastanza univoco e può essere utilizzato per l'impronta digitale di un particolare sistema operativo di origine. L'utilizzo dell'opzione Parameter Request List non è così preciso come la stringa HTTP User-Agent, tuttavia è molto più controllato rispetto all'utilizzo dei nomi host e di altri dati definiti staticamente.

> **Nota:** L'opzione DHCP Parameter Request List non è una soluzione perfetta perché i dati prodotti dipendono dal fornitore e possono essere duplicati da più tipi di dispositivi.

Prima di configurare le regole di profiling ISE, usare Wireshark capture da un endpoint/SPAN (Switched Port Analyzer) o TCP (Transmission Control Protocol) Dump capture su ISE per valutare le opzioni dell'elenco di richieste di parametri nel pacchetto DHCP (se presente). In questa acquisizione di esempio vengono visualizzate le opzioni dell'elenco di richieste di parametri DHCP per Windows 10.

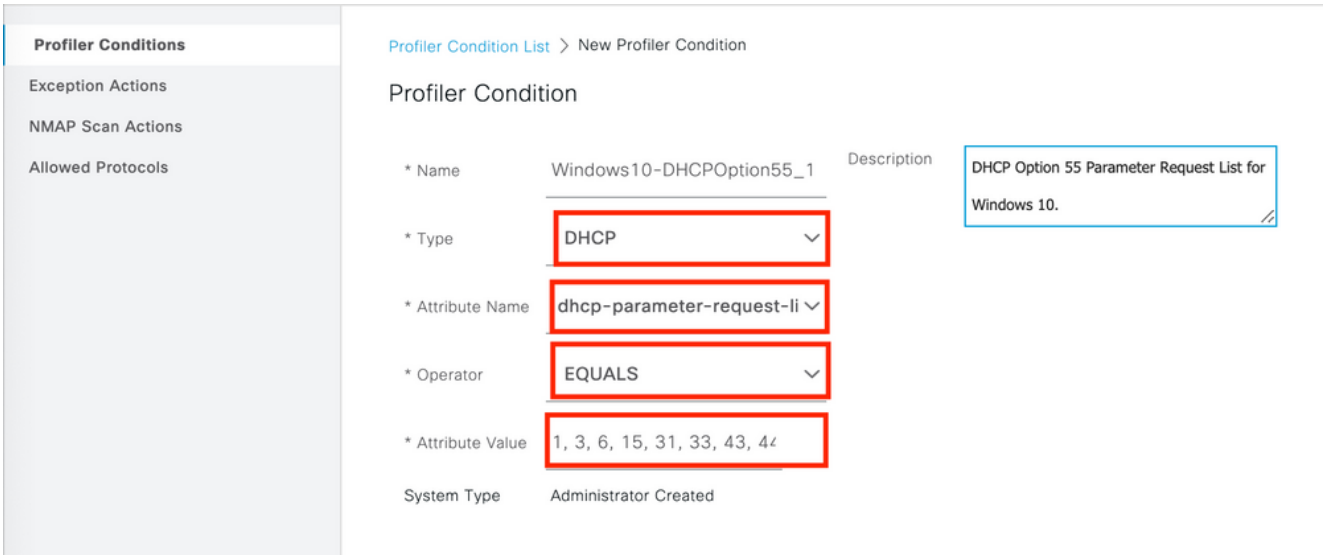


La stringa Parameter Request List risultante viene scritta nel seguente formato separato da virgole: 1, 3, 6, 15, 31, 33, 43, 44, 46, 47, 119, 121, 249, 252. Usa questo formato quando configuri le condizioni di profilatura personalizzate in ISE.

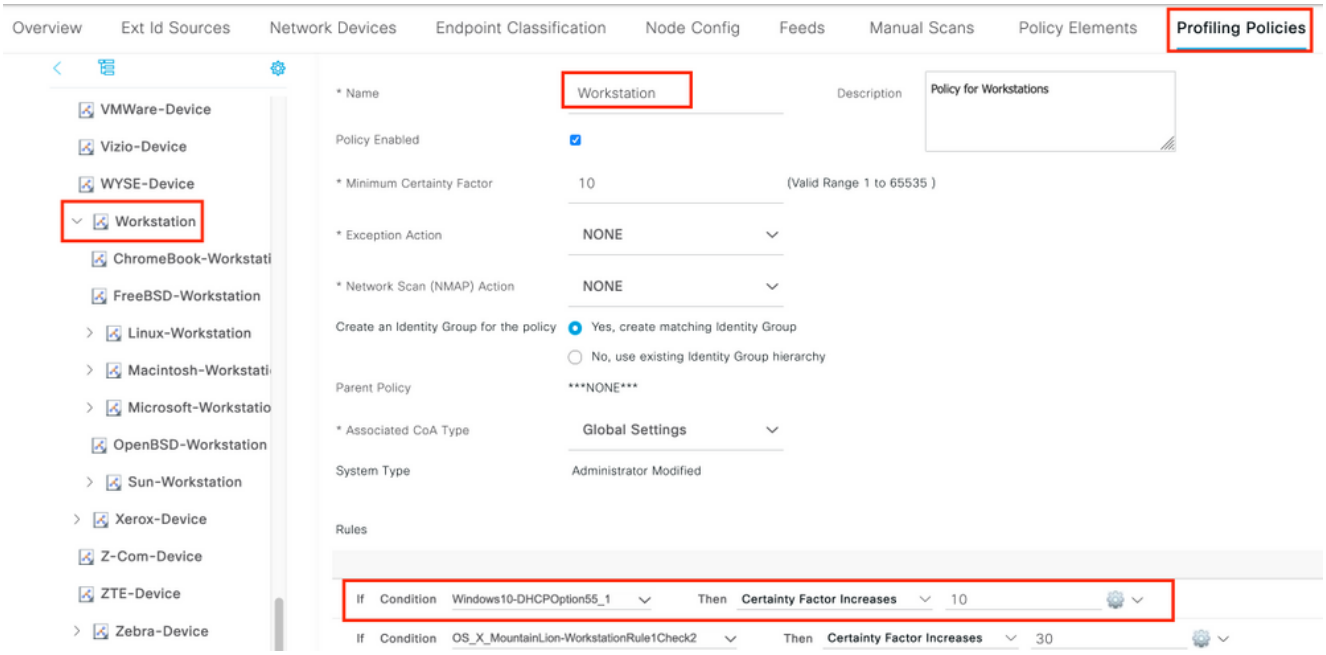
Nella sezione Configurazione viene illustrato l'utilizzo di condizioni di profiling personalizzate per adattare una workstation Windows 10 a una **workstation Windows10**.

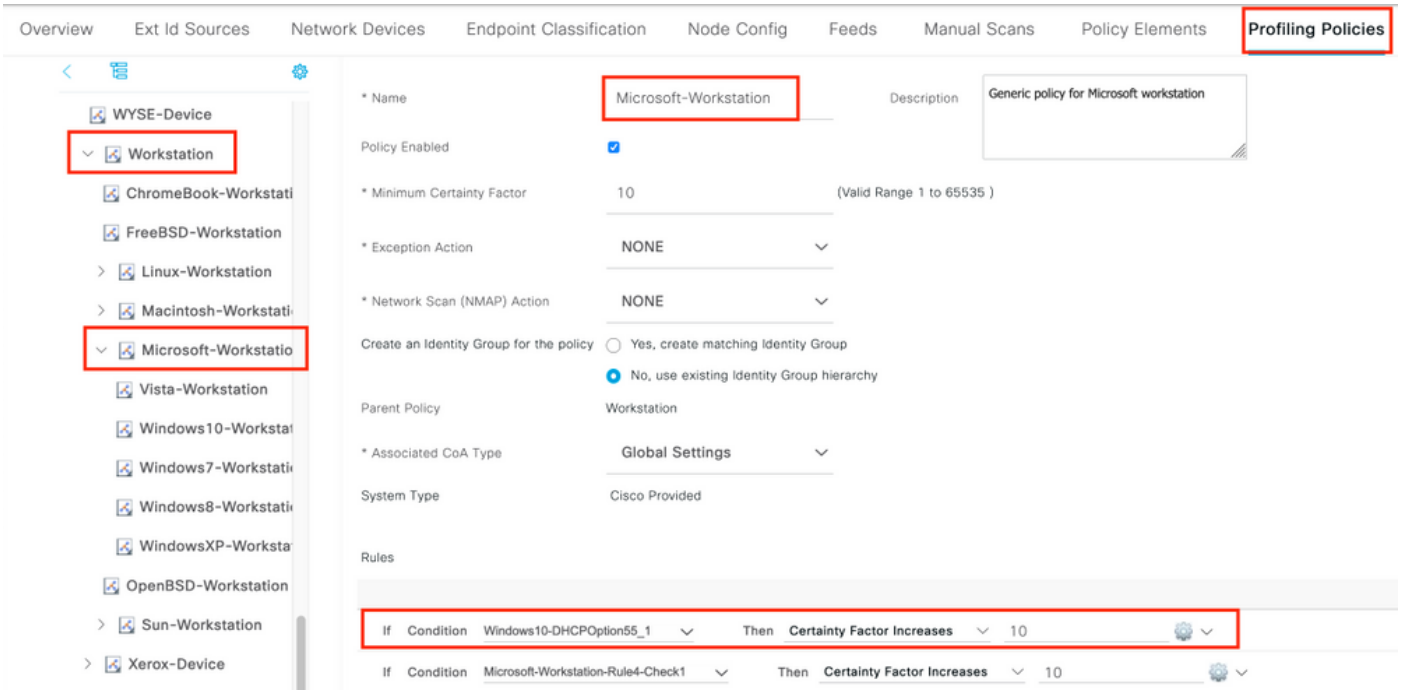
Configurazione

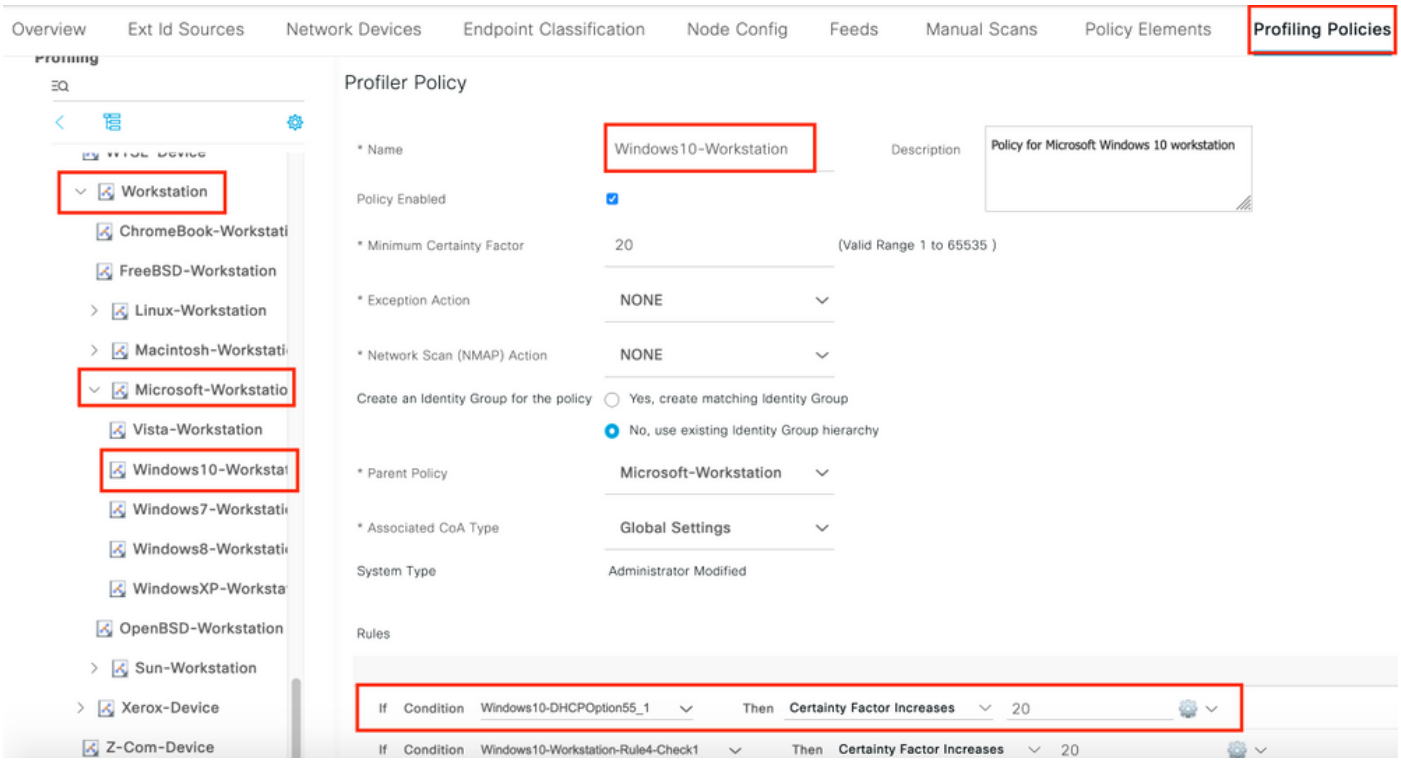
1. Accedere alla GUI di amministrazione di ISE e selezionare **Policy > Policy Elements > Conditions > Profiling** (Policy > Elementi della policy > Condizioni > Profiling). Per aggiungere una nuova condizione di profilatura personalizzata, fare clic su **Add** (Aggiungi). In questo esempio vengono utilizzate le impronte digitali dell'elenco di richieste di parametri di Windows 10. Fare riferimento a Fingerbank.org per un elenco completo dei valori dell'elenco di richieste di parametri.
   Nota: È possibile che nella casella di testo **Valore attributo** non vengano visualizzate tutte le opzioni numeriche e che sia necessario scorrere il riquadro con il mouse o la tastiera per visualizzare l'elenco completo.



2. Con le condizioni personalizzate definite, passare a **Criterio > Profilatura > Criteri di profilatura** per modificare un criterio di profilatura corrente o per configurarne uno nuovo. In questo esempio vengono modificati i criteri predefiniti **Workstation, Microsoft-Workstation e Windows10-Workstation** per includere le nuove condizioni dell'elenco di richieste di parametri. Aggiungere una nuova condizione composta alla regola dei criteri del profiler **Workstation, Microsoft-Workstation, Windows10-Workstation** come mostrato di seguito. Modificare il **fattore di certezza** in base alle esigenze per ottenere il risultato di profilatura desiderato.





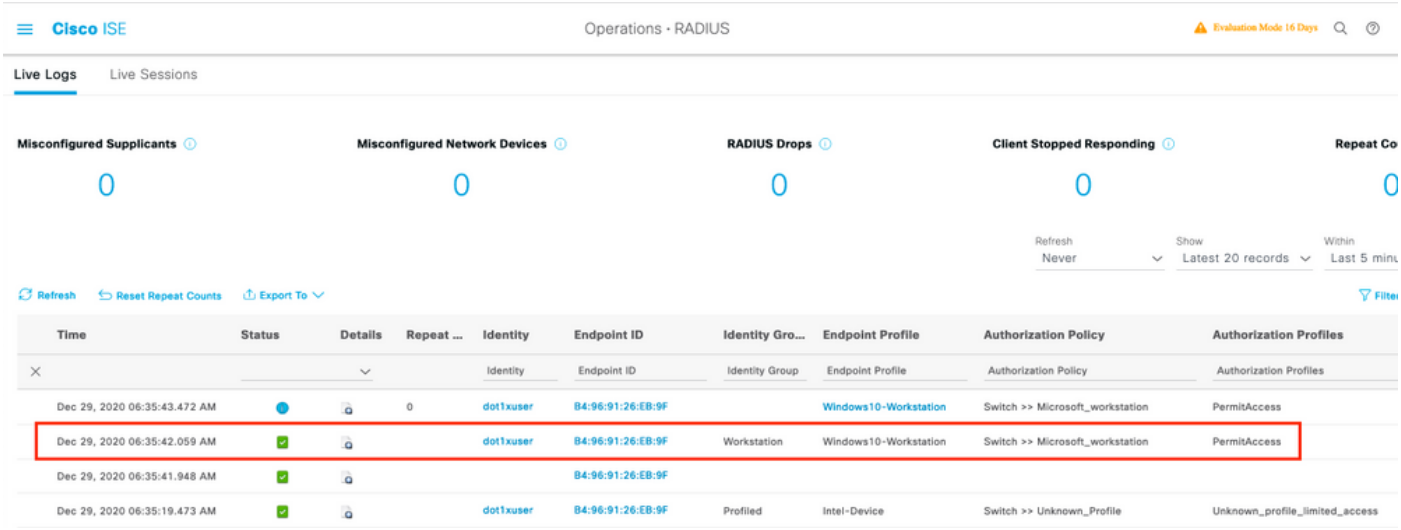


Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo [strumento di ricerca dei comandi (solo utenti registrati).]

Verifica

Passaggio 1-

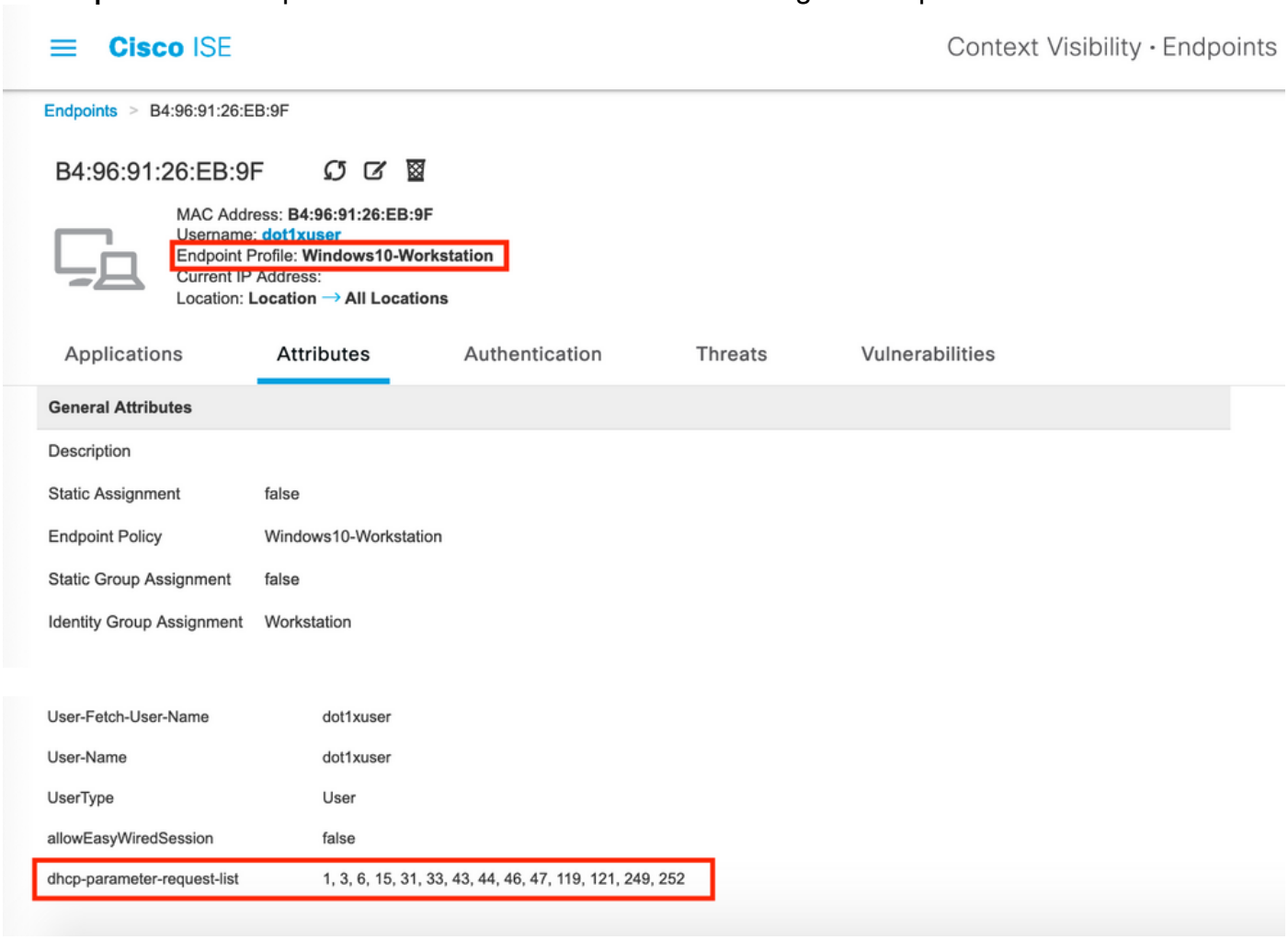
Selezionare ISE > Operations > Live Logs. La prima autenticazione corrisponde ai criteri di autorizzazione sconosciuti e l'accesso limitato è concesso ad ISE. Dopo aver profilato il dispositivo, ISE attiva la CoA e riceve un'altra richiesta di autenticazione che corrisponde al nuovo profilo, Windows10 Workstation.



Passaggio 2-

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

- Passare a **Visibilità contesto > Endpoint,** cercare l'endpoint, fare clic su Modifica.
- Confermare che **EndPointPolicy** sia Window10-Workstation e che i valori **dhcp-parameter-request-list** corrispondano ai valori della condizione configurata in precedenza.



Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla

configurazione.

- Verificare che i pacchetti DHCP abbiano raggiunto i nodi dei criteri ISE che eseguono la funzione di profiling (con indirizzo dell'helper o SPAN).
- Utilizzare **Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump** Tool? (Operazioni > Risoluzione dei problemi > Strumenti di diagnostica > Strumenti generali > TCP Dump Tool). per eseguire in modo nativo le clip TCP Dump dalla GUI di amministrazione di ISE.
- Abilita i seguenti debug sul nodo PSN ISE - -nsf-nsf-session-lighttwight Session Directory-profiler-runtime-AAA
- Profiler.log , prrt-server.log e lsd.log mostrano informazioni rilevanti.
- Per un elenco aggiornato delle opzioni dell'elenco di richieste di parametri, consultare il database delle impronte digitali DHCP Fingerbank.org.
- Verificare che nelle condizioni di profilatura ISE siano configurati i valori corretti dell'elenco di richieste di parametri. Di seguito sono elencate alcune delle stringhe più utilizzate.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug.**

Analisi log

++Attiva sotto i debug sul nodo PSN ISE -

-nsf

-nsf-session

-lighttwight Session Directory

-profiler

-runtime-AAA

++Autenticazione iniziale

++server-porta.log

++Richiesta di accesso ricevuta sul nodo ISE

Radius,2020-12-29 06:35:19,377,DEBUG,0x7f1cdcbd2700,cntx=0001348461,ssen=isee30-primary/39791910/625,CallingStationID=B4-96-91-26-EB-9F **PACCHETTO RADIUS: Code=1(AccessRequest)** Identifier=182 Length=285

++ISE corrisponde a Unknown_profile

AcsLogs,2020-12-29 06:35:19,473,DEBUG,0x7f1cdc7ce700,cntx=0001348476,ssen=isee30-primary/397791910/625,CPMSessionID=0A6A270B00000
0018B44013AC,user=dot1xuser,CallingStationID=B4-96-91-26-EB-9F,**AuthorizationPolicyMatchedRule=Unknown_Profile**, EapTunnel=EAP-FAST, EapAuthentication=EAP-MSCHAPv2, UserType=User, CPMSessionID=0A6A270B0000018B44013AC, EndPointMACAddress=B4-96-91-26-EB-9F,

++ISE invia l'autorizzazione di accesso con accesso limitato

Radius,2020-12-29 06:35:19,474,DEBUG,0x7f1cdc7ce700,cntx=0001348476,ssen=isee30-primary/39791910/625,CPMSessionID=0A6A270B000000 8B44013AC,user=dot1xuser,CallingStationID=B4-96-91-26-EB-9F,PACCHETTO RADIUS: **Code=2(AccessAccept)** Identifier=186 Length=331

++ISE ha ricevuto un aggiornamento contabile con le informazioni DHCP

Radius,2020-12-29 06:35:41,464,DEBUG,0x7f1cdcad1700,cntx=0001348601,ssen=isee30-primary/39791910/627,CPMSessionID=0A6A270B00000 18B44013AC,CallingStationID=B4-96-91-26-EB-9F,PACCHETTO RADIUS: **Code=4(AccountingRequest)** Identifier=45 Length=381

[1] Nome utente - valore: [dot1xuser]

[87] NAS-Port-Id - valore: [Gigabit Ethernet 1/0/13]

[26] **cisco-av-pair - valore: [dhcp-option= opzione dhcp**

[26] cisco-av-pair - valore: [audit-session-id=**0A6A270B0000018B44013AC**]

++ISE invia risposta di accounting

Radius,2020-12-29 06:35:41,472,DEBUG,0x7f1cdc5cc700,cntx=0001348601,ssen=isee30-primary/39791910/627,CPMSessionID=0A6A270B00000 18B44013AC,user=dot1xuser,CallingStationID=B4-96-91-26-EB-9F,PACCHETTO RADIUS: **Code=5(AccountingResponse)** Identifier=45 Length=20,RADIUSHandler.cpp:2216

++Profiler.log

++Una volta ricevuto l'aggiornamento dell'accounting con l'opzione DHCP dhcp-parameter-request-list , ISE avvia la profilatura del dispositivo

2020-12-29:06:35:41,470 DEBUG [SyslogListenerThread][] cisco.profiler.probes.radius.SyslogDefragmenter -::::- **parseHeader inBuffer**=<181>Dec 29:06:35:41 isee30-primary CISE_RADIUS_Accounting 00000652 2020-12-29 06:35:41.467 +00:00 000234376 3002 AVVISO **Radius-Accounting: Aggiornamento watchdog accounting RADIUS**, ConfigVersionId=99, Device IP Address=10.106.39.11, UserName=dot1xuser, RequestLatency=6, NetworkDeviceName=Sw, User-Name=dot1xuser, NAS-IP-Address=10.106.39.11, NAS-Port=50113, Class=CACS:0A6A270B000000 8B44013AC:isee30-primary/39791910/625, Called-Station-ID=A0-EC-F9-3C-82-0D, Calling-Station-ID=B4-96-91-26-EB-9F, NAS-Identifier=Switch, Acct-Status-Type=Interim-Update, Acct-Delay-Time=0, Acct-Input-Octets=174, Acct-Output-Time ets=0, Acct-Session-Id=000000b, Acct-Authentic=Remote, Acct-Input-Packets=1, Acct-Output-Packets=0, Event-Timestamp=1609341899, NAS-Port-Type=Ethernet, NAS-Port-Id=Gigabit Ethernet1/0/13, **cisco-av-pair=dhcp-option=dhcp-parameter-request-list=1\, 3\, 6\, 15\, 3\, 33\, 43\, 44\, 46\, 47\, 119\, 121\, 249\, 252, cisco-av-pair=audit-session-id=0A6A270B0000018B44013AC,** cisco-av-pair=method=dot1x,

2020-12-29:35:41,471 DEBUG [RADIUSParser-1-thread-2][] cisco.profiler.probes.radius.RadiusParser -::::- **Sensore IOS analizzato 1: dhcp-parameter-request-list=[1, 3, 6, 15, 31, 33, 43, 44, 46, 47, 119, 121, 249, 252]**

Attributo:cisco-av-pair valore:dhcp-option=dhcp-parameter-request-list=1\, 3\, 6\, 15\, 31\, 33\, 43\,

44\, 46\, 47\, 119\, 121\, 249\, 252, audit-session-id=0A6A270B0000018B44013AC, metodo=dot x

Attributo:dhcp-parameter-request-list valore:1, 3, 6, 15, 31, 33, 43, 44, 46, 47, 119, 121, 249, 252

2020-12-29-06:35:41,479 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.cache.AbstractEndpointCache -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:ProfilerCollection: - **Proprietario per questo Mac: B4:96:91:26:EB:9F è isee30-primary.anshsinh.local**

2020-12-29-06:35:41,479 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.probemgr.Forwarder -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:ProfilerCollection: **- proprietario corrente per l'endpoint B4:96:91:26:EB:9Fis isee30-primary.anshsinh.local e il codice messaggio è 3002**

2020-12-29-06:35:41,479 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.probemgr.Forwarder -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:ProfilerCollection: **- è true il raggio di origine dell'endpoint**

++Nuovo attributo

2020-12-29-06:35:41,480 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.probemgr.Forwarder -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:ProfilerCollection: **- Nuovo attributo: dhcp-parameter-request-list**

2020-12-29-06:35:41,482 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.probemgr.Forwarder -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:ProfilerCollection:- set di attributi modificato del punto:

2020-12-29-06:35:41,482 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.probemgr.Forwarder -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:**ProfilerCollection: dhcp-parameter-request-list**

++Regole diverse corrispondono a un fattore di certezza diverso

2020-12-29-06:35:41,484 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:**Profiling: Intel-Device corrispondente a B4:96:91:26:EB:9F (certezza 5)**

2020-12-29-06:35:41,485 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:**Profiling: La workstation corrisponde a B4:96:91:26:EB:9F (certezza 10)**

2020-12-29-06:35:41,486 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:**Profiling: Microsoft-Workstation corrispondente a B4:96:91:26:EB:9F (certezza 10)**

2020-12-29-06:35:41,487 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:**Policy: Windows10-Workstation corrispondente a B4:96:91:26:EB:9F (certezza 20)**

++Windows10-Workstation ha il fattore di certezza più alto di 40 in base alla configurazione e

quindi sceglie questo come profilo dell'endpoint per il dispositivo

2020-12-29-06:35:41,487 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:Profiling:- analisi della gerarchia dei criteri: **Endpoint: B4:96:91:26:EB:9F EndpointPolicy:Windows10-Workstation per:40 ExceptionRuleMatched:false**

2020-12-29-06:35:41,487 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:**Profiling: Dpoint B4:96:91:26:EB:9F Criterio Corrispondente Modificato.**

2020-12-29-06:35:41,489 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:**Profiling: Punto B4:96:91:26:EB:9F IdentityGroup Modificato.**

2020-12-29-06:35:41,489 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:**Profiling: ID gruppo di identità sull'endpoint B4:96:91:26:EB:9F - 3b76f840-8c00-11e6-996c-525400b48521**

2020-12-29-06:35:41,489 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:Profiling:- Caricamento della cache degli endpoint con endpoint profilato B4:96:91:26:EB:9F, criteri Windows10-Workstation, criteri corrispondenti Windows10-Workstation

2020-12-29-06:35:41,489 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:**Profiling: evento finale per mantenere il punto finale B4:96:91:26:EB:9F e codice messaggio ep = 3002**

2020-12-29-06:35:41,489 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:**Profiling: Punto B4:96:91:26:EB:9F IdentityGroup / Profilo logico modificato. Rilascio di un CoA condizionale**

2020-12-29-06:35:41,489 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:Profiling:- Dettagli ionalCoAEvent con endpoint: **EndPoint[id=ff19ca00-499f-11eb-b713-1a99022ed3c5,name=<null>]**

MAC: B4:96:91:26:EB:9F

Attributo:Calling-Station-ID, valore:B4-96-91-26-EB-9F

Attributo:EndPointMACAddress, valore:B4-96-91-26-EB-9F

Attributo:MACAddress, valore:B4:96:91:26:EB:9F

++Invio dei dati alla directory di sessione Lightweight

2020-12-29:35:41,489 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.probemgr.**LSDForwarderHelper** -:::- Endpoint.B4:96:91:26:EB:9F **corrispondente a Windows10-Workstation**

2020-12-29 06:35:41,489 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.probemgr.**LSDForwarderHelper -::::- Invio evento per rendere permanente l'endpoint durante l'aggiunta per LSD per il server d'inoltro,defaultradius,defaultad B4:96:91:26:EB:9F**

++CoA globale è selezionato come Riautenticazione

2020-12-29-06:35:41,489 DEBUG [CoAHandler-52-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -:B4:96:91:26:EB:9F:9fe38b30-43ea-11eb-b713-1a99022ed3c5:**Profiler CoA:- Configured Global CoA command type = Reauth**

2020-12-29-06:35:41,490 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.cache.AbstractEndpointCache -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:- endpoint - EP da in ingresso: **B4:96:91:26:EB:9FepFonte: ProbeSGA RADIUS: falseSG: Workstation**

2020-12-29-06:35:41,490 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.cache.AbstractEndpointCache -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:- punto finale - EP dopo l'unione: **B4:96:91:26:EB:9FepFonte: ProbeSGA RADIUS: falseSG:Windows10-Workstation**

++ISE corrisponde alla Policy per verificare se è necessario inviare il CoA. ISE attiverà CoA solo se dispone di criteri corrispondenti alla modifica del profilo

2020-12-29-06:35:41,701 DEBUG [CoAHandler-52-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -:B4:96:91:26:EB:9F:9fe38b30-43ea-11eb-b713-1a99022ed3c5:**Profiler** R:- Elabora tutti i criteri disponibili in Parametro set di criteri eccezione locale, policystatus=ENABLED

2020-12-29-06:35:41,701 DEBUG [CoAHandler-52-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -:B4:96:91:26:EB:9F:9fe38b30-43ea-11eb-b713-1a99022ed3c5:**Profiler CoA:- Nome criterio : Cambia stato criteri: ATTIVATO**

2020-12-29-06:35:41,702 DEBUG [CoAHandler-52-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -:B4:96:91:26:EB:9F:9fe38b30-43ea-11eb-b713-1a99022ed3c5:**Profiler CoA:- lhsvalue name 6d954800-8bff-11e6-996c-525400b48521 rhs operandID 42706690-8c00-11e6-996c-525400b48521 rhsvaluename Workstation:Microsoft-Workstation:Windows10-Workstation**

2020-12-29-06:35:41,933 DEBUG [CoAHandler-52-thread-1][] com.cisco.profiler.api.Util -:B4:96:91:26:EB:9F:9fe38b30-43ea-11eb-b713-1a99022ed3c5:**ProfilerCoA: - Condizione specificata DISPONIBILE nei criteri di autorizzazione**

2020-12-29-06:35:41,933 DEBUG [CoAHandler-52-thread-1][] com.cisco.profiler.api.Util -:B4:96:91:26:EB:9F:9fe38b30-43ea-11eb-b713-1a99022ed3c5:**ProfilerCoA: - Criterio di autorizzazione HAVING: 42706690-8c00-11e6-996c-525400b48521**

++Il criterio di autorizzazione soddisfa questa condizione e viene attivata la funzione CoA

2020-12-29-06:35:41,935 DEBUG [CoAHandler-52-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -:B4:96:91:26:EB:9F:9fe38b30-43ea-11eb-b713-1a99022ed3c5:**Profiler CoA:- applyCoa: Descrittore creato in base agli attributi RADIUS dell'endpoint:**

MAC: [B4:96:91:26:EB:9F]

ID sessione: [0A6A270B00000018B44013AC]

Server AAA: IP [isee30-primary]: [10.106.32.119]

Interfaccia AAA: [10.106.32.119]

Indirizzo IP AND: [10.106.39.11]

ID porta NAS: [Gigabit Ethernet 1/0/13]

Tipo di porta NAS: Ethernet

Service-Type: [Con frame]

Wireless: [falso]

VPN: [falso]

MAB: [falso]

2020-12-29-06:35:41,938 DEBUG [CoAHandler-52-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -:B4:96:91:26:EB:9F:9fe38b30-43ea-11eb-b713-1a99022ed3c5:**Profiler CoA:- Sta per chiamare CoA per e IP: 10.106.39.11 per l'endpoint: B4:96:91:26:EB:9F Comando CoA: Riautenticazione**

2020-12-29-06:35:41,938 DEBUG [CoAHandler-52-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -:B4:96:91:26:EB:9F:9fe38b30-43ea-11eb-b713-1a99022ed3c5:**Profiler CoA:- Applicazione di CoA-REAUTH da parte del server AAA: 10.106.32.119 tramite interfaccia: 10.106.32.119 alla AND: 10.106.39.11**

2020-12-29:06:35:41,949 DEBUG [SyslogListenerThread][] cisco.profiler.probes.radius.SyslogDefragmenter -:::- parseHeader inBuffer=<181>Dec 29:06:35:41 isee30-primary CISE_Passed_Authentication 00000656 2 Passaggio 1=2=(porta = 1700 \, tipo = Cisco CoA), **CoASourceComponent=Profiler, CoAReason=Modifica nell'endpoint identità, gruppo/criteri/profilo logico utilizzati nei criteri di autorizzazione, CoAType=Reauthentication** - last, Network Device Profile=Cisco,

++server-porta.log

AcsLogs,2020-12-29 06:35:41,938,DEBUG,0x7f1c6ffcb700,cntx=0001348611,Log_Message=[2020-12-29 06:35:41.938 +00:00 0023437 9 80006 **INFO Profiler: Il profiler sta attivando la modifica della richiesta di autorizzazione,** ConfigVersionId=99, **EndpointCoA=Reauth,** EndpointMacAddress=B4:96:91:26:EB:9F, EndpointNADAddress=10.106.39.11, **EndpointPolicy=Windows10-Workstation,** EndpointProperty=Service-Type=Framed\,MessageCode=3002\,EndPointPolicyID=42706690-8c00-11e6-996c-525400b48521\,UseCase=\,NAS-Port-Id=Gigabit Ethernet1/0/13\,NAS-Port-Type=Ethernet\,Response=\{Nome-Utente=dot1xuser\;

DynamicAuthorizationFlow,2020-12-29 06:35:41,939,DEBUG,0x7f1cdc3ca700,cntx=0001348614,[DynamicAuthorizationFlow::onLocalHtt

pEvent] Ricevuto comando CoA in ingresso:

<Reauthentication id="39c74088-52fd-430f-95d9-a8fe78eaa1f1" type="last">

<session serverAddress="10.106.39.11">

<identifierAttribute name="UseInterface">10.106.32.119</identifierAttribute>

<identifierAttribute name="Calling-Station-ID">B4:96:91:26:EB:9F</identifierAttribute>

<identifierAttribute name="NAS-Port-Id">Gigabit Ethernet 1/0/13</identifierAttribute>

<identifierAttribute name="cisco-av-pair">audit-session-id=0A6A270B0000018B44013AC</identifierAttribute>

<identifierAttribute name="ACS-Instance">COA-IP-TARGET:10.106.32.119</identifierAttribute>

</session>

</Riautentica>

++CoA inviato -

RadiusClient,2020-12-29 06:35:41,943,DEBUG,0x7f1ccb3f3700,cntx=0001348614,ssen=39c74088-52fd-430f-95d9-a8fe78eaa1f1,CallingStationID=B4:96 1:26:EB:9F, PACCHETTO RADIUS: Code=43 (CoARequest) Identifier=27 Length=225

[4] Indirizzo-IP-NAS - valore: [10.106.39.11]

[31] Calling-Station-ID - valore: [B4:96:91:26:EB:9F]

[87] NAS-Port-Id - valore: [Gigabit Ethernet 1/0/13]

[26] cisco-av-pair - valore: [sottoscrittore:comando=riautentica]

[26] cisco-av-pair - valore: [audit-session-id=0A6A270B0000018B44013AC]

RadiusClient,2020-12-29 06:35:41,947,DEBUG,0x7f1cdcad1700,cntx=0001348614,ssen=39c74088-52fd-430f-95d9-a8fe78eaa1f1,CallingStationID=B4:96 1:26:EB:9F, PACCHETTO RADIUS: Code=44 (CoAACK) Identifier=27

++Nuova richiesta di accesso

Radius,2020-12-29 06:35:41,970,DEBUG,0x7f1cdc6cd700,cntx=0001348621,ssen=isee30-primary/39791910/628,CallingStationID=B4-96-91-26-EB-9F,RADIUS ET: Code=1(AccessRequest) Identifier=187 Length=285

++ISE corrisponde al nuovo profilo di autorizzazione corrispondente ai criteri endpoint del dispositivo endpoint

AcsLogs,2020-12-29 06:35:42,060,DEBUG,0x7f1cdcad1700,cntx=0001348636,ssen=isee30-

primary/397791910/628,CPMSessionID=0A6A270B0000
0018B44013AC,user=dot1xuser,CallingStationID=B4-96-91-26-EB-
9FIdentityPolicyMatchedRule=Default, **AuthorizationPolicyMatchedRule=Microsoft_workstation,**
EapTunnel=EAP-FAST, EapAuthentication=EAP-MSCHAPv2, UserType=User,
CPMSessionID=0A6A270B000001 8B44013AC, EndPointMACAddress=B4-96-91-26-EB-9F,
PostureAssessmentStatus=NotApplicable, **EndPointMatchedProfile=Windows10-Workstation,**

++Viene inviata l'autorizzazione di accesso -

Radius,2020-12-29 06:35:42,061,DEBUG,0x7f1cdcad1700,cntx=0001348636,ssen=isee30-
primary/39791910/628,CPMSessionID=0A6A270B00000
18B44013AC,user=dot1xuser,CallingStationID=B4-96-91-26-EB-9F,PACCHETTO RADIUS:
Code=2(AccessAccept) Identifier=191 Length=340

Informazioni correlate

- Fingerbank.org DHCP Impronte digitali
- Documentazione e supporto tecnico – Cisco Systems