

Ejemplo de Configuración de la Opción 55 de la Lista de Solicitud de Parámetro DHCP Utilizada para Perfilar Terminales

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Verificación](#)

[Troubleshoot](#)

[Análisis de registro](#)

[Información Relacionada](#)

Introducción

Este documento describe el uso de la opción 55 de la lista de solicitudes de parámetros DHCP como método alternativo para los dispositivos de perfil que utilizan Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recomienda que tenga:

- Conocimiento básico del proceso de detección de DHCP
- Experiencia con el uso de ISE para configurar reglas de definición de perfiles personalizadas

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ISE versión 3.0
- Windows 10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

En las implementaciones de ISE de producción, algunas de las sondas de definición de perfiles implementadas con más frecuencia incluyen RADIUS, HTTP y DHCP. Con la redirección de URL en el centro del flujo de trabajo de ISE, la sonda HTTP se utiliza ampliamente para capturar datos importantes del terminal de la cadena User-Agent. Sin embargo, en algunos casos prácticos de producción, no se desea una redirección de URL y se prefiere Dot1x, lo que dificulta el establecimiento de perfiles precisos de un terminal. Por ejemplo, un PC de empleado que se conecta a un identificador de conjunto de servicios (SSID) corporativo obtiene acceso completo mientras que su iDevice personal (iPhone, iPad, iPod) solo obtiene acceso a Internet. En ambos escenarios, los usuarios tienen un perfil y una asignación dinámica a un grupo de identidad más específico para la coincidencia de perfiles de autorización que no depende del usuario para abrir un navegador web. Otra alternativa utilizada comúnmente es la coincidencia de nombres de host. Esta solución es imperfecta porque los usuarios pueden cambiar el nombre de host del terminal a un valor no estándar.

En casos de esquina como estos, la sonda DHCP y la opción 55 de la Lista de Solicitud de Parámetro DHCP se pueden utilizar como método alternativo para perfilar estos dispositivos. El campo de lista de solicitudes de parámetros del paquete DHCP se puede utilizar para identificar un sistema operativo de terminal de la misma manera que un sistema de prevención de intrusiones (IPS) utiliza una firma para hacer coincidir un paquete. Cuando el sistema operativo del terminal envía un paquete de detección o solicitud DHCP en el cable, el fabricante incluye una lista numérica de opciones DHCP que pretende recibir del servidor DHCP (router predeterminado, servidor de nombres de dominio (DNS), servidor TFTP, etc.). El orden por el cual el cliente DHCP solicita estas opciones del servidor es bastante único y se puede utilizar para identificar un sistema operativo de origen determinado. El uso de la opción Parameter Request List no es tan exacto como la cadena HTTP User-Agent; sin embargo, está mucho más controlado que el uso de hostnames y otros datos definidos estáticamente.

Nota: La opción DHCP Parameter Request List (Lista de solicitudes de parámetros DHCP) no es una solución perfecta porque los datos que genera dependen del proveedor y pueden duplicarse con varios tipos de dispositivos.

Antes de configurar las reglas de definición de perfiles de ISE, utilice las capturas de Wireshark de capturas de volcado de protocolo de control de transmisión (TCP) o punto final de un analizador de puerto conmutado (SPAN) en ISE para evaluar las opciones de lista de solicitudes de parámetros en el paquete DHCP (si las hay). Esta captura de ejemplo muestra las opciones de la Lista de solicitudes de parámetros DHCP para Windows 10.

No.	Time	Source	Destination	Protocol	Length	Info
1083	55.281036	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xc629c12d
1645	70.718403	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xc629c12d


```

Relay agent IP address: 0.0.0.0
Client MAC address: IntelCor_26:eb:9f (b4:96:91:26:eb:9f)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
> Option: (53) DHCP Message Type (Discover)
> Option: (61) Client identifier
> Option: (12) Host Name
> Option: (60) Vendor class identifier
v Option: (55) Parameter Request List
  Length: 14
  Parameter Request List Item: (1) Subnet Mask
  Parameter Request List Item: (3) Router
  Parameter Request List Item: (6) Domain Name Server
  Parameter Request List Item: (15) Domain Name
  Parameter Request List Item: (31) Perform Router Discover
  Parameter Request List Item: (33) Static Route
  Parameter Request List Item: (43) Vendor-Specific Information
  Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
  Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
  Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
  Parameter Request List Item: (119) Domain Search
  Parameter Request List Item: (121) Classless Static Route
  Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
  Parameter Request List Item: (252) Private/Proxy autodiscovery
v Option: (255) End

```

La cadena de lista de solicitudes de parámetros que da lugar se escribe en el siguiente formato separado por comas: 1, 3, 6, 15, 31, 33, 43, 44, 46, 47, 119, 121, 249, 252. Utilice este formato al configurar las condiciones de definición de perfiles personalizadas en ISE.

La sección de configuración muestra el uso de condiciones de definición de perfiles personalizadas para hacer coincidir la estación de trabajo de Windows 10 con una **estación de trabajo de Windows10**.

Configurar

1. Inicie sesión en la GUI de administración de ISE y navegue hasta **Política > Elementos de políticas > Condiciones > Definición de perfiles**. Haga clic en **Agregar** para agregar una nueva condición de definición de perfiles personalizada. En este ejemplo, utilizamos las huellas dactilares de la Lista de Solicitud de Parámetro de Windows 10. Refiérase a Fingerbank.org para obtener una lista completa de valores de la Lista de Solicitud de Parámetro.

Nota: Es posible que el cuadro de texto **Valor de atributo** no muestre todas las opciones numéricas y que deba desplazarse con el ratón o el teclado para ver la lista completa.

Profiler Conditions

Exception Actions

NMAP Scan Actions

Allowed Protocols

Profiler Condition List > New Profiler Condition

Profiler Condition

* Name	Windows10-DHCPOption55_1	Description	DHCP Option 55 Parameter Request List for Windows 10.
* Type	DHCP		
* Attribute Name	dhcp-parameter-request-li		
* Operator	EQUALS		
* Attribute Value	1, 3, 6, 15, 31, 33, 43, 44		
System Type	Administrator Created		

2. Con las condiciones personalizadas definidas, navegue hasta **Política > Perfiles > Políticas de perfiles** para modificar una política de perfiles actual o para configurar una nueva. En este ejemplo, se editan las políticas predeterminadas **Workstation**, **Microsoft-Workstation**, **Windows10-Workstation** para incluir las nuevas condiciones de la Lista de Solicitud de Parámetro. Agregue una nueva condición compuesta a la regla de política del generador de perfiles de estación de trabajo, **Microsoft-Workstation** y **Windows10-Workstation** como se muestra a continuación. Modifique el **factor de certeza** según sea necesario para lograr el resultado deseado de la definición de perfiles.

Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements **Profiling Policies**

Workstation

Policy for Workstations

Policy Enabled

* Minimum Certainty Factor 10 (Valid Range 1 to 65535)

* Exception Action NONE

* Network Scan (NMAP) Action NONE

Create an Identity Group for the policy Yes, create matching Identity Group
 No, use existing Identity Group hierarchy

Parent Policy ***NONE***

* Associated CoA Type Global Settings

System Type Administrator Modified

Rules

If	Condition	Windows10-DHCPOption55_1	Then	Certainty Factor Increases	10
If	Condition	OS_X_MountainLion-WorkstationRule1Check2	Then	Certainty Factor Increases	30

Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements **Profiling Policies**

WYSE-Device
 Workstation
 ChromeBook-Workstati
 FreeBSD-Workstation
 Linux-Workstation
 Macintosh-Workstati
 Microsoft-Workstatio
 Vista-Workstation
 Windows10-Workstati
 Windows7-Workstati
 Windows8-Workstati
 WindowsXP-Worksta
 OpenBSD-Workstation
 Sun-Workstation
 Xerox-Device

* Name: Microsoft-Workstation Description: Generic policy for Microsoft workstation

Policy Enabled:

* Minimum Certainty Factor: 10 (Valid Range 1 to 65535)

* Exception Action: NONE

* Network Scan (NMAP) Action: NONE

Create an Identity Group for the policy: Yes, create matching Identity Group No, use existing Identity Group hierarchy

Parent Policy: Workstation

* Associated CoA Type: Global Settings

System Type: Cisco Provided

Rules

If Condition: Windows10-DHCPOption55_1 Then Certainty Factor Increases 10

If Condition: Microsoft-Workstation-Rule4-Check1 Then Certainty Factor Increases 10

Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements **Profiling Policies**

Profiling

Workstation
 ChromeBook-Workstati
 FreeBSD-Workstation
 Linux-Workstation
 Macintosh-Workstati
 Microsoft-Workstatio
 Vista-Workstation
 Windows10-Workstati
 Windows7-Workstati
 Windows8-Workstati
 WindowsXP-Worksta
 OpenBSD-Workstation
 Sun-Workstation
 Xerox-Device
 Z-Com-Device

Profiler Policy

* Name: Windows10-Workstation Description: Policy for Microsoft Windows 10 workstation

Policy Enabled:

* Minimum Certainty Factor: 20 (Valid Range 1 to 65535)

* Exception Action: NONE

* Network Scan (NMAP) Action: NONE

Create an Identity Group for the policy: Yes, create matching Identity Group No, use existing Identity Group hierarchy

* Parent Policy: Microsoft-Workstation

* Associated CoA Type: Global Settings

System Type: Administrator Modified

Rules

If Condition: Windows10-DHCPOption55_1 Then Certainty Factor Increases 20

If Condition: Windows10-Workstation-Rule4-Check1 Then Certainty Factor Increases 20

Nota: Use la [Command Lookup Tool \(clientes registrados solamente\)](#) para obtener más información sobre los comandos usados en esta sección.

Verificación

Paso 1-

Vaya a ISE > Operations > Live Logs . La primera autenticación coincide con la Política de autorización desconocida y el acceso limitado se da a ISE . Una vez que se ha definido el perfil del dispositivo , ISE activa la CoA y se recibe otra solicitud de autenticación en ISE y coincide con el nuevo perfil: Windows10 Workstation .

Cisco ISE Operations - RADIUS Evaluation Mode 16 Days

Live Logs Live Sessions

Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 0 Client Stopped Responding 0 Repeat Co 0

Refresh Never Show Latest 20 records Within Last 5 min

Refresh Reset Repeat Counts Export To Filter

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Identity Gro...	Endpoint Profile	Authorization Policy	Authorization Profiles
Dec 29, 2020 06:35:43.472 AM	●	🔒	0	dot1xuser	B4:96:91:26:EB:9F		Windows10-Workstation	Switch >> Microsoft_workstation	PermitAccess
Dec 29, 2020 06:35:42.059 AM	●	🔒		dot1xuser	B4:96:91:26:EB:9F	Workstation	Windows10-Workstation	Switch >> Microsoft_workstation	PermitAccess
Dec 29, 2020 06:35:41.948 AM	●	🔒			B4:96:91:26:EB:9F				
Dec 29, 2020 06:35:19.473 AM	●	🔒		dot1xuser	B4:96:91:26:EB:9F	Profiled	Intel-Device	Switch >> Unknown_Profile	Unknown_profile_limited_access

Paso 2-

Utilice esta sección para confirmar que su configuración funcione correctamente.

- Navegue hasta **Visibilidad de contexto > Terminales**, busque el terminal y haga clic en editar.
- Confirme que **EndPointPolicy** sea **Window10-Workstation** y que los valores **dhcp-parámetro-request-list** coincidan con los valores de condición previamente configurados.

Cisco ISE Context Visibility · Endpoints

Endpoints > B4:96:91:26:EB:9F

B4:96:91:26:EB:9F 🔄 ✎ 🗑️

MAC Address: B4:96:91:26:EB:9F
 Username: dot1xuser
Endpoint Profile: Windows10-Workstation
 Current IP Address:
 Location: Location → All Locations

Applications Attributes Authentication Threats Vulnerabilities

General Attributes

Description

Static Assignment	false
Endpoint Policy	Windows10-Workstation
Static Group Assignment	false
Identity Group Assignment	Workstation

User-Fetch-User-Name	dot1xuser
User-Name	dot1xuser
UserType	User
allowEasyWiredSession	false
dhcp-parameter-request-list	1, 3, 6, 15, 31, 33, 43, 44, 46, 47, 119, 121, 249, 252

Troubleshoot

Esta sección proporciona la información que puede utilizar para resolver problemas de su

configuración.

- Verifique que los paquetes DHCP alcanzaron los nodos de política ISE que realizan la función de definición de perfiles (con dirección de ayudante o SPAN).
- ¿Utilizar la herramienta **Operaciones > Solución de problemas > Herramientas de diagnóstico > Herramientas generales > Volcado TCP?** para ejecutar de forma nativa las capturas de volcado TCP desde la GUI de administración de ISE.
- Habilitar a continuación las depuraciones en el nodo PSN de ISE - -nsf-nsf-session-directorio de sesión ligero-profiler-Runtime-AAA
- Profiler.log , prrt-server.log y lsd.log muestran información relevante.
- Refiérase a la base de datos de huellas dactilares DHCP Fingerbank.org para ver una lista actual de opciones de la Lista de Solicitudes de Parámetro.
- Asegúrese de que los valores correctos de la Lista de Solicitud de Parámetro estén configurados en las condiciones de definición de perfiles de ISE. Algunas de las cadenas más utilizadas son:

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un comando debug.

Análisis de registro

++Activar a continuación depuraciones en el nodo PSN de ISE -

-nsf

-nsf-session

-directorio de sesión ligero

-profiler

-Runtime-AAA

++Autenticación inicial

++prrt-server.log

++Solicitud de acceso recibida en el nodo ISE

Radius,2020-12-29 06:35:19,377,DEBUG,0x7f1cdc7d2700,cntx=0001348461,sesn=isee30-primary/33 97791910/625,CallingStationID=B4-96-91-26-EB-9F, **PAQUETE RADIUS: Code=1(AccessRequest) Identificador=182 Longitud=285**

++ISE coincide con Unknown_profile

AcsLogs,2020-12-29 06:35:19,473,DEBUG,0x7f1cdc7ce700,cntx=0001348476,sesn=isee30-primary/3 97791910/625,CPMSessionID=0A6A270B00000018B44013AC,user=dot1xuser,CallingStationID=B4-96-91-26-EAC B-9F, **AuthorizationPolicyMatchedRule=Unknown_Profile**, EapTunnel=EAP-FAST, EapAuthentication=EAP-MSCHAPv2, UserType=User, CPMSessionID=0A6A270B00000018B4013AC EndPointMACAddress=B4-96-91-26-EB-9F,

++ISE envía Access Accept con acceso limitado

Radius,2020-12-29 06:35:19,474,DEBUG,0x7f1cdc7ce700,cntx=0001348476,sesn=isee30-primary/3977
791910/625,CPMSessionID=0A6A270B00000018B44013AC,user=dot1xuser,CallingStationID=B4-96-91-26-EB-9F PAQUETE RADIUS: **Código=2(AccessAccept)** Identificador=186 Longitud=331

++ISE recibió actualización de contabilidad con la información DHCP

Radius,2020-12-29 06:35:41,464,DEBUG,0x7f1cdcad1700,cntx=001348601,sesn=isee30-primary/397 791910/627,CPMSessionID=0A6A270B00000018B44013AC,CallingStationID=B4-96-91-26-EB-9F,RADIUS ET: **Código=4(AccountingRequest)** Identificador=45 Longitud=381

[1] Nombre de usuario: valor: [dot1xuser]

[87] NAS-Port-Id - valor: [GigabitEthernet1/0/13]

[26] Cisco-av-pair - valor: [dhcp-option=

[26] cisco-av-pair - valor: [audit-session-id=0A6A270B00000018B44013AC]

++ISE devuelve respuesta de contabilidad

Radius,2020-12-29 06:35:41,472,DEBUG,0x7f1cdc5cc700,cntx=0001348601,sesn=isee30-primary/3977
791910/627,CPMSessionID=0A6A270B00000018B44013AC,user=dot1xuser,CallingStationID=B4-96-91-26-EB-9F PAQUETE RADIUS: **Código=5(AccountingResponse)** Identificador=45 Longitud=20,RADIUSHandler.cpp:2216

++Profiler.log

++Una vez que se recibe la actualización de la contabilidad con la opción DHCP dhcp-parámetro-request-list , ISE comienza a crear perfiles del dispositivo

2020-12-29 06:35:41,470 DEBUG [SyslogListenerThread][]
cisco.profiler.probes.radius.SyslogDefragmenter -:::- **parseHeader en búfer =<181>22 9 06:35:41**
isee30-primary CISE_RADIUS_Accounting 000000655 2 0 2020-12-29 06:35:41.467 +00:00
000233 4376 3002 AVISO **Radius-Accounting: Actualización de RADIUS Accounting Watchdog**,
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, Clase=CACS:0A6A270B00000018B44013AC:isee30-primary/397791910/625,
Called-Station-ID A0-EC-F9-3C-82-0D, Calling-Station-ID=B4-96-91-26-EB-9F, NAS-
Identifier=Switch, Acct-Status-Type=Provisional-Update, Acct-Delay-Time=0, Acct-Input-
Octets=174, Acct-Output-Octets=0 Acct-Session-Id=000000b, Acct-Authentication=Remoto, Acct-
Input-Packets=1, Acct-Output-Packets=0, Event-Timestamp=1609341899, NAS-Port-
Type=Ethernet, NAS-Port-Id=GigabitEthernet1/0/13 , **cisco-av-pair=dhcp-option=dhcp-parámetro-
request-list=1\, 3\, 6\, 15\, 31\, 33\, 43\, 44\, 46\, 47\, 119\, 121\, 249\, 252, cisco av pair=audit-
session-id=0A6A270B00000018B44013AC, cisco-av-pair=method=dot1x,**

2020-12-29 06:35:41,471 DEBUG [RADIUSParser-1-thread-2][]
cisco.profiler.probes.radius.RadiusParser -:::- **Sensor 1 de IOS analizado: dhcp-parámetro-
request-list=[1, 3, 6, 15, 31, 33, 43, 44, 46, 47, 119, 121, 249, 252]**

Atributo:cisco-av-pair value:dhcp-option=dhcp-parámetro-request-list=1\, 3\, 6\, 15\, 31\, 33\, 43\, 44\, 46\, 47\, 119\, 121\, 249\, 252, audit-session-id=0A6A270B00000018B44013AC, method=dot1x

Atributo:dhcp-parámetro-request-list value:1, 3, 6, 15, 31, 33, 43, 44, 46, 47, 119, 121, 249, 252

2020-12-29 06:35:41,479 DEBUG [RMQforwarding-4][]
cisco.profiler.infrastructure.cache.AbstractEndpointCache -:B4:96:91:26:EB:9F:1241 3370-49a0-11eb-b713-1a99022ed3c5:ProfilerCollection:- **Propietario de este Mac: B4:96:91:26:EB:9F es isee30-primary.anshsinh.local**

2020-12-29 06:35:41,479 DEBUG [RMQforwarding-4][]
cisco.profiler.infrastructure.probemgr.Forwarder -:B4:96:91:26:EB:9F:124133 70-49a0-11eb-b713-1a99022ed3c5:ProfilerCollection:- **propietario actual del terminal B4:96:91:26:EB:9F es isee30-primary.anshsinh.local y el código de mensaje es 300000 2**

2020-12-29 06:35:41,479 DEBUG [RMQforwarding-4][]
cisco.profiler.infrastructure.probemgr.Forwarder -:B4:96:91:26:EB:9F:124133 70-49a0-11eb-b713-1a99022ed3c5:ProfilerCollection:- **es true en el radio de origen del terminal**

++Nuevo atributo

2020-12-29 06:35:41,480 DEBUG [RMQforwarding-4][]
cisco.profiler.infrastructure.probemgr.Forwarder -:B4:96:91:26:EB:9F:124133 70-49a0-11eb-b713-1a99022ed3c5:ProfilerCollection:- **Nuevo atributo: dhcp-parámetro-request-list**

2020-12-29 06:35:41,482 DEBUG [RMQforwarding-4][]
cisco.profiler.infrastructure.probemgr.Forwarder -:B4:96:91:26:EB:9F:124133 70-49a0-11eb-b713-1a99022ed3c5:ProfilerCollection:- **Terminal modificado atributo establecido:**

2020-12-29 06:35:41,482 DEBUG [RMQforwarding-4][]
cisco.profiler.infrastructure.probemgr.Forwarder -:B4:96:91:26:EB:9F:124133 70-49a0-11eb-b713-1a99022ed3c5:ProfilerCollection:- **dhcp-parámetro-request-list,**

++Las diferentes reglas coinciden con diferentes factores de seguridad

2020-12-29 06:35:41,484 DEBUG [RMQforwarding-4][]
cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:12413 370-49a0-11eb-b713-1a99022ed3c5:Definición de perfiles:- **Política que el dispositivo Intel coincide B4:96:91:26:EB:9F (certeza 5)**

2020-12-29 06:35:41,485 DEBUG [RMQforwarding-4][]
cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:12413 370-49a0-11eb-b713-1a99022ed3c5:Definición de perfiles:- **Estación de trabajo de políticas coincidentes B4:96:91:26:EB:9F (certeza 10)**

2020-12-29 06:35:41,486 DEBUG [RMQforwarding-4][]
cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:12413 370-49a0-11eb-b713-1a99022ed3c5:Definición de perfiles:- **Política de Microsoft-Workstation coincidente B4:96:91:26:EB:9F (certeza 10)**

2020-12-29 06:35:41,487 DEBUG [RMQforwarding-4][]
cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:12413 370-49a0-11eb-

b713-1a99022ed3c5:Definición de perfiles:- Política de Windows10-Estación de trabajo coincidente B4:96:91:26:EB:9F (certeza 20)

++Windows10-Workstation tiene el factor de seguridad más alto de 40 basado en la configuración y, por lo tanto, se elige como el perfil de terminal para el dispositivo

2020-12-29 06:35:41,487 DEBUG [RMQforwarding-4][
cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:12413 370-49a0-11eb-
b713-1a99022ed3c5:Definición de perfiles:- Después de analizar la jerarquía de políticas:
Terminal: B4:96:91:26:EB:9F EndpointPolicy:Windows10-Workstation para:40
ExceptionRuleMatched:false

2020-12-29 06:35:41,487 DEBUG [RMQforwarding-4][
cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:12413 370-49a0-11eb-
b713-1a99022ed3c5:Definición de perfiles:- Extremo B4:96:91:26:EB:9F Política coincidente
modificada.

2020-12-29 06:35:41,489 DEBUG [RMQforwarding-4][
cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:12413 370-49a0-11eb-
b713-1a99022ed3c5:Definición de perfiles:- Extremo B4:96:91:26:EB:9F IdentityGroup Cambiado.

2020-12-29 06:35:41,489 DEBUG [RMQforwarding-4][
cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:12413 370-49a0-11eb-
b713-1a99022ed3c5:Definición de perfiles:- Configuración de ID de grupo de identidad en el
terminal B4:96:91:26:EB:9F - 3b76f840-8c0000011e6-996c-525400b48521

2020-12-29 06:35:41,489 DEBUG [RMQforwarding-4][
cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:12413 370-49a0-11eb-
b713-1a99022ed3c5:Definición de perfiles:- Llamada a la memoria caché del punto final con el
punto final B4:96:91:26:EB:9F, política Windows10-Estación de trabajo de políticas coincidentes
Windows10-

2020-12-29 06:35:41,489 DEBUG [RMQforwarding-4][
cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:12413 370-49a0-11eb-
b713-1a99022ed3c5:Definición de perfiles:- Envío del evento para conservar el punto final
B4:96:91:26:EB:9F, y código de mensaje ep = 3002

2020-12-29 06:35:41,489 DEBUG [RMQforwarding-4][
cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:12413 370-49a0-11eb-
b713-1a99022ed3c5:Definición de perfiles:- Extremo B4:96:91:26:EB:9F IdentityGroup / Perfil
lógico cambiado. Emisión de un CoA condicional

2020-12-29 06:35:41,489 DEBUG [RMQforwarding-4][
cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:12413 370-49a0-11eb-
b713-1a99022ed3c5:Definición de perfiles:- ConditionalCoAEvent con detalles del terminal :
EndPoint[id=ff19ca00-499f-11eb-b713-1a99022ed3c5,name=<null>]

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

Atributo:valor de estación de llamada:B4-96-91-26-EB-9F

Atributo:EndPointMACAddress valor:B4-96-91-26-EB-9F

Atributo:MACAddress value:B4:96:91:26:EB:9F

++Envío de los datos al directorio de sesión ligero

2020-12-29 06:35:41,489 DEBUG [RMQforwarding-4][
cisco.profiler.infrastructure.probemgr.LSDForwarderHelper -:::- Terminal.B4:96:91:26:EB:9F
coincidente con Windows10-Workstation

2020-12-29 06:35:41,489 DEBUG [RMQforwarding-4][
cisco.profiler.infrastructure.probemgr.LSDForwarderHelper -::::- **Enviando evento para conservar
el punto final mientras se agrega LSD para reenviador, tradius,defaultad B4:96:91:26:EB:9F**

++La CoA global se selecciona como Reauth

2020-12-29 06:35:41,489 DEBUG [CoAHandler-52-thread-1][
cisco.profiler.infrastructure.profiles.CoAHandler -:B4:96:91:26:EB:9F:9fe 38b30-43ea-11eb-b713-
1a99022ed3c5:**ProfilerCoA:- Tipo de comando CoA global configurado = Reauth**

2020-12-29 06:35:41,490 DEBUG [RMQforwarding-4][
cisco.profiler.infrastructure.cache.AbstractEndpointCache -:B4:96:91:26:EB:9F:1241 3370-49a0-
11eb-b713-1a99022ed3c5::- **Actualización del punto final - EP desde el entrante:
B4:96:91:26:EB:9FepFuente: RADIUS ProbeSGA: falseSG: Estación de trabajo**

2020-12-29 06:35:41,490 DEBUG [RMQforwarding-4][
cisco.profiler.infrastructure.cache.AbstractEndpointCache -:B4:96:91:26:EB:9F:1241 3370-49a0-
11eb-b713-1a99022ed3c5::- **Actualización del punto final - EP después de la fusión:
B4:96:91:26:EB:9FepFuente: RADIUS ProbeSGA: falseSG:Estación de trabajo Windows10**

++ISE coincide con la política para comprobar si es necesario enviar CoA . ISE activará la CoA sólo si tiene alguna política que coincida con el cambio de perfil

2020-12-29 06:35:41,701 DEBUG [CoAHandler-52-thread-1][
cisco.profiler.infrastructure.profiles.CoAHandler -:B4:96:91:26:EB:9F:9fe3 8b30-43ea-11eb-b713-
1a99022ed3c5:**ProfilerCoA:- Procesar todas las políticas disponibles en el switch de conjunto de
políticas de excepciones locales ,policy status=ACTIVADO**

2020-12-29 06:35:41,701 DEBUG [CoAHandler-52-thread-1][
cisco.profiler.infrastructure.profiles.CoAHandler -:B4:96:91:26:EB:9F:9fe 38b30-43ea-11eb-b713-
1a99022ed3c5:**ProfilerCoA:- Nombre de la política : Estado de la política del switch: HABILITADO**

2020-12-29 06:35:41,702 DEBUG [CoAHandler-52-thread-1][
cisco.profiler.infrastructure.profiles.CoAHandler -:B4:96:91:26:EB:9F:9fe 38b30-43ea-11eb-b713-
1a9022ed3c5:**ProfilerCoA:- lhsvalue name 6d954800-8bff-11e6-996c-5254 00b48521 rhs
operandID 42706690-8c00-11e6-996c-525400b48521 rhsvalue 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:9fe38b 30-43ea-11eb-b713-1a99022ed3c5:**ProfilerCoA:- Condición
especificada DISPONIBLE en la política de autorización**

2020-12-29 06:35:41,933 DEBUG [CoAHandler-52-thread-1][com.cisco.profiler.api.Util -
:B4:96:91:26:EB:9F:9fe38b 30-43ea-11eb-b713-1a99022ed3c5:**ProfilerCoA:- Política de
autorización TENIENDO política : 42706690-8c00-11e6-996c-525400b48521**

++La política de autorización coincide con esta condición y se activa la CoA

2020-12-29 06:35:41,935 DEBUG [CoAHandler-52-thread-1][
cisco.profiler.infrastructure.profiles.CoAHandler -:B4:96:91:26:EB:9F:9fe 38b30-43ea-11eb-b713-
1a99022ed3c5:ProfilerCoA:- applyCoa: **Descriptor creado basado en atributos RADIUS del terminal:**

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

ID de Sesión: [0A6A270B00000018B44013AC]

Servidor AAA: IP de [isee30-primary]: [10.106.32.119]

Interfaz AAA: [10.106.32.119]

Dirección IP de NAD: [10.106.39.11]

ID de puerto NAS: [GigabitEthernet1/0/13]

Tipo de puerto NAS: [Ethernet]

Tipo de servicio: [Enmarcado]

Es inalámbrico: [falso]

¿Es VPN? [falso]

Es MAB: [falso]

2020-12-29 06:35:41,938 DEBUG [CoAHandler-52-thread-1][
cisco.profiler.infrastructure.profiles.CoAHandler -:B4:96:91:26:EB:9F:9fe 38b30-43ea-11eb-b713-
1a99022ed3c5:ProfilerCoA:- **A punto de llamar a CoA para e IP: 10.106.39.11 para el terminal:**
Comando B4:96:91:26:EB:9F CoA: Reauth

2020-12-29 06:35:41,938 DEBUG [CoAHandler-52-thread-1][
cisco.profiler.infrastructure.profiles.CoAHandler -:B4:96:91:26:EB:9F:9fe 38b30-43ea-11eb-b713-
1a99022ed3c5:ProfilerCoA:- **Aplicación de CoA-REAUTH por servidor AAA: 10.106.32.119 a través de la interfaz: 10.106.32.119 a NAD: 10.106.39.11**

2020-12-29 06:35:41,949 DEBUG [SyslogListenerThread][
cisco.profiler.probes.radius.SyslogDefragmenter -:::- parseHeader inBuffer=<181>2906:35:41
isee30-primary CISE_Passed_Authentications 000000656 2 1 StepData=2=(port = 1700 \, type =
Cisco CoA), **CoASourceComponent=Profiler, CoAReason=Cambiar en el grupo/política de identidad de terminal perfil lógico/lógico que se utiliza en las políticas de autorización, CoAType=Reauthentication** - last, Network Device Profile=Cisco,

++prrt-server.log

AcsLogs,2020-12-29
06:35:41,938,DEBUG,0x7f1c6ffcb700,cntx=0001348611,Log_Message=[2020-0 12-29
06:35:41.938 +00:00 0000234379 80006 **Perfilador INFO: El generador de perfiles está activando la solicitud de cambio de autorización, 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=GigabitEthernet1/0/13,NAS-Port-Type=Ethernet,Response={UserName=dot1xuser};

DynamicAuthorizationFlow,2020-12-29

06:35:41,939,DEBUG,0x7f1cdc3ca700,cntx=001348614,[DynamicAuthorizationFlow:LocalHttpEvent] Se recibió el comando CoA entrante:

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

<session serverAddress="10.106.39.11">

<identificadorAtributo name="UseInterface">10.106.32.119</identificadorAttribute>

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

<identificadorAtributo name="NAS-Port-Id">GigabitEthernet1/0/13</identificadorAttribute>

<identificadorAtributo name="cisco-av-pair">audit-session-id=0A6A270B00000018B44013AC</identificadorAttribute>

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

</session>

</Reauthenticate>

++CoA enviado -

RadiusClient,2020-12-29 06:35:41,943,DEBUG,0x7f1ccb3f3700,cntx=0001348614,sesn=39c74088-52fd-430f-95d9-a8fe78eaa1f1,CallingStationID=B4:96:91:26:EB:9F, RADIUS PACKET: Código=43 (CoARequest) Identificador=27 Longitud=225

[4] NAS-IP-Address: valor: [10.106.39.11]

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

[87] NAS-Port-Id - valor: [GigabitEthernet1/0/13]

[26] cisco-av-pair - valor: [subscriber:command=reautenticar]

[26] cisco-av-pair - valor: [audit-session-id=0A6A270B00000018B44013AC]

RadiusClient,2020-12-29

06:35:41,947,DEBUG,0x7f1cdcad1700,cntx=0001348614,sesn=39c74088-52fd-430f-95d9-a8fe78eaa1f1,CallingStationID=B4:96:91:26:EB:9F, RADIUS PACKET: Código=44 (CoAACK) Identificador=27

++Nueva solicitud de acceso

Radius,2020-12-29 06:35:41,970,DEBUG,0x7f1cdc6cd700,cntx=0001348621,sesn=isee30-

primary/3977 791910/628,CallingStationID=B4-96-91-26-EB-9F,PAQUETE RADIUS:
Code=1(AccessRequest) Identificador=187 Longitud=285

++ISE coincide con el nuevo perfil de autorización que coincide con la política de terminal del dispositivo terminal

AcsLogs,2020-12-29 06:35:42,060,DEBUG,0x7f1cdcad1700,cntx=0001348636,sesn=isee30-
primary
397791910/628,CPMSessionID=0A6A270B00000018B44013AC,user=dot1xuser,CallingStationID
=B4-96-91-26 EB-9FIdentityPolicyMatchedRule=Default,
AuthorizationPolicyMatchedRule=Microsoft_estación de trabajo, EapTunnel=EAP-FAST,
EapAuthentication=EAP-MSCHAPv2, UserType=User, CPMSessionID=0A6A270B00000018B
44013AC, EndPointMACAddress=B4-96-91-26-EB-9F, PostureAssessmentStatus=NoAplicable,
EndPointMatchedProfile=Windows10-Workstation,

++Access Accept se envía -

Radius,2020-12-29 06:35:42,061,DEBUG,0x7f1cdcad1700,cntx=001348636,sesn=isee30-
primary/397
791910/628,CPMSessionID=0A6A270B00000018B44013AC,user=dot1xuser,CallingStationID=B4
-96-91-26-EB-9F,PAQUETE RADIUS: **Código=2(AccessAccept)** Identificador=191 Longitud=340

Información Relacionada

- [Base de datos de huellas dactilares DHCP de Fingerbank.org](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)