

用於配置檔案端點的DHCP引數請求清單選項55配置示例

目錄

- [簡介](#)
- [必要條件](#)
- [需求](#)
- [採用元件](#)
- [背景資訊](#)
- [設定](#)
- [驗證](#)
- [疑難排解](#)
- [日誌分析](#)
- [相關資訊](#)

簡介

本文檔介紹使用DHCP引數請求清單選項55作為配置使用身份服務引擎(ISE)的裝置的可選方法。

必要條件

需求

思科建議您：

- DHCP發現過程的基本知識
- 使用ISE配置自定義分析規則的經驗

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- ISE版本3.0
- Windows 10

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

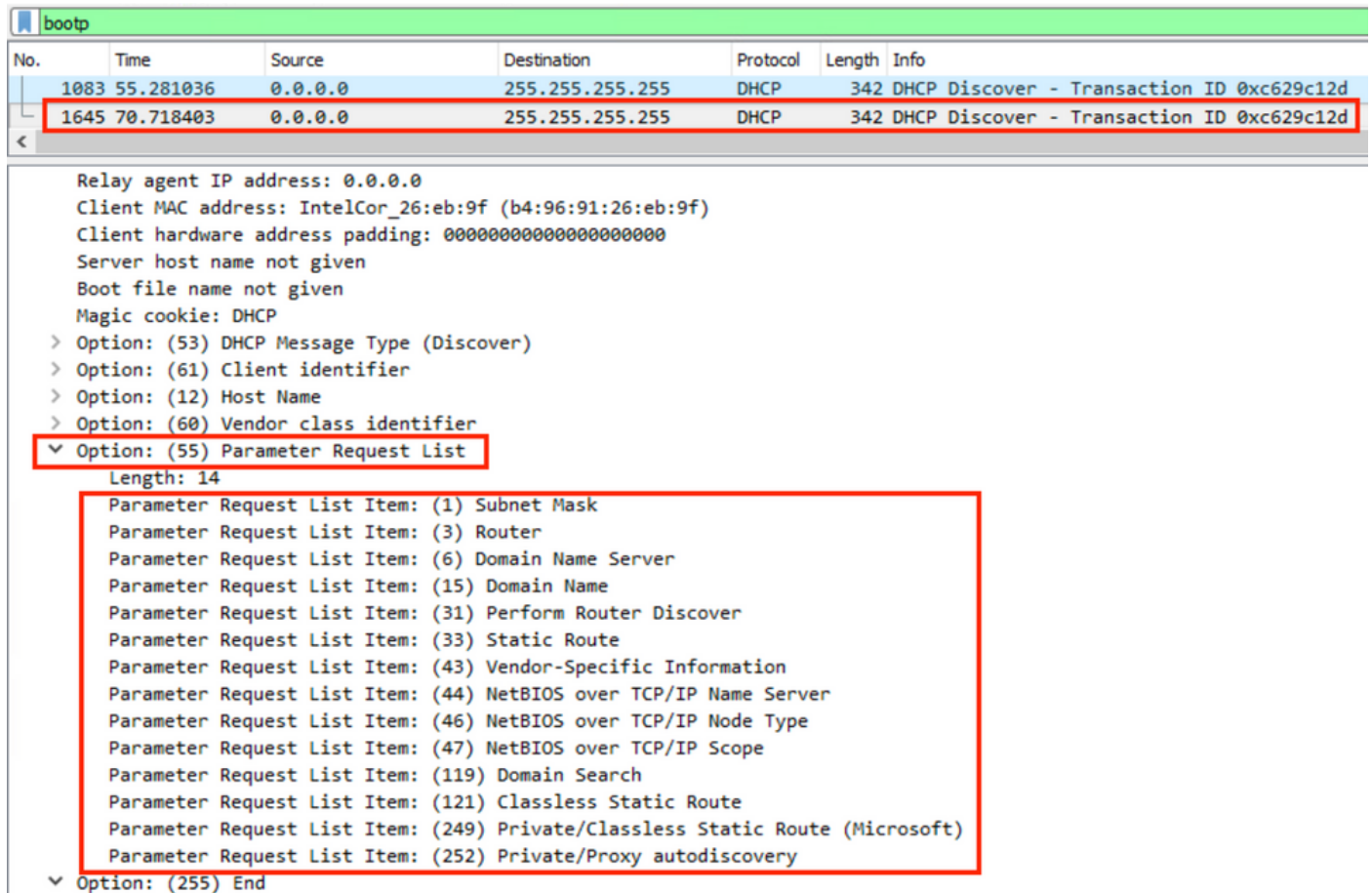
在生產ISE部署中，一些更常用的分析探測包括RADIUS、HTTP和DHCP。由於URL重定向位於ISE工作流的中心，HTTP探測被廣泛使用，以便從使用者代理字串捕獲重要的終端資料。但是，在某些生產使用情形中，不需要URL重定向，並且首選Dot1x，這使得更難準確地分析端點。例如，連線到企業服務集識別符號(SSID)的員工PC獲得完全訪問許可權，而其個人iDevice(iPhone、

iPad、iPod)僅獲得Internet訪問許可權。在這兩種情況下，使用者都被分析並動態對映到更具體的身份組以進行授權配置檔案匹配，而不依賴使用者開啟Web瀏覽器。另一個常用的替代方法是主機名匹配。此解決方案並不完美，因為使用者可能會將終端主機名更改為非標準值。

在諸如此類的拐角情況下，DHCP探測功能和DHCP引數請求清單選項55可用作對這些裝置進行概要分析的替代方法。DHCP資料包中的Parameter Request List欄位可用於對終端作業系統進行指紋，與入侵防禦系統(IPS)使用簽名來匹配資料包類似。當終端作業系統線上路上傳送DHCP發現或請求資料包時，製造商會提供它打算從DHCP伺服器(預設路由器、域名伺服器(DNS)、TFTP伺服器等)接收的DHCP選項數字清單。DHCP客戶端向伺服器請求這些選項的順序相當唯一，可用於對特定源作業系統進行指紋。Parameter Request List選項的使用並不像HTTP User-Agent字串那樣精確，但是，它遠比使用主機名和其他靜態定義的資料來控制。

附註： DHCP Parameter Request List選項並不是完美的解決方案，因為它生成的資料取決於供應商，並且可由多種裝置型別複製。

在配置ISE分析規則之前，請使用Wireshark捕獲，從ISE上的終端/交換埠分析器(SPAN)或傳輸控制協定(TCP)轉儲捕獲，以評估DHCP資料包中的引數請求清單選項（如果存在）。此示例捕獲顯示Windows 10的DHCP引數請求清單選項。



The image shows a Wireshark packet capture of a DHCP Discover message. The packet list pane shows two packets: packet 1083 (Time: 55.281036) and packet 1645 (Time: 70.718403), both from source 0.0.0.0 to destination 255.255.255.255, protocol DHCP, length 342. Packet 1645 is highlighted with a red box. The packet details pane for packet 1645 shows the following information:

```
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
< 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
< Option: (255) End
```

結果以以下逗號分隔格式寫入的引數請求清單字串：1、3、6、15、31、33、43、44、46、47、119、121、249、252。在ISE中配置自定義分析條件時使用此格式。

配置部分演示了使用自定義分析條件將Windows 10工作站匹配到Windows10-Workstation。

設定

1. 登入到ISE管理員GUI並導航到**Policy > Policy Elements > Conditions > Profiling**。按一下**Add**以新增新的自定義分析條件。在本示例中，我們使用Windows 10引數請求清單指紋。有關引數請求清單值的完整清單，請參閱Fingerbank.org。

附註： **Attribute Value** 文本框可能未顯示所有數字選項，您可能需要使用滑鼠或鍵盤滾動才能檢視完整清單。

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. 定義自定義條件後，導航到**Policy > Profiling > Profiling Policies**以修改當前分析策略或配置新的分析策略。在本示例中，編輯預設**Workstation**、**Microsoft-Workstation**和**Windows10-Workstation**策略，以便包含新的「引數請求清單」條件。將新的複合條件新增到**Workstation**、**Microsoft-Workstation**、**Windows10-Workstation**分析器策略規則，如下所示。根據需要修改**Constability Factor**，以便獲得所需的效能分析結果。

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

< 管理

* Name	Workstation	Description	Policy for Workstations
Policy Enabled	<input checked="" type="checkbox"/>		
* Minimum Certainty Factor	10	(Valid Range 1 to 65535)	
* Exception Action	NONE		
* Network Scan (NMAP) Action	NONE		
Create an Identity Group for the policy	<input checked="" type="radio"/> Yes, create matching Identity Group		
	<input type="radio"/> 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

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
 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

附註：使用[命令查詢工具](#)(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

驗證

第1步 —

導航到ISE >操作>即時日誌。第1個身份驗證與未知授權策略匹配，並向ISE授予有限的訪問許可權。在裝置分析後，ISE觸發CoA並在ISE上收到另一個身份驗證請求並匹配新的配置檔案 — 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

第2步 —

使用本節內容，確認您的組態是否正常運作。

- 導航到 **Context Visibility > Endpoints**，搜索端點，然後點選edit。
- 確認 **EndPointPolicy** 是 **Window10-Workstation**，並且 **dhcp-parameter-request-list** 值與之前配置的條件值匹配。

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

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

- 驗證DHCP資料包是否到達執行分析功能的ISE策略節點 (使用幫助程式地址或SPAN)。
- 使用 **Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump tool?** 以便從 ISE 管理員 GUI 本地運行 TCP 轉儲捕獲。
- 在 ISE PSN 節點上啟用以下調試 — -nsf-nsf-session-lightwight 會話目錄-profiler-runtime-AAA
- Profiler.log 、 prrt-server.log 和 Isd.log 顯示相關資訊。
- 請參閱 Fingerbank.org DHCP 指紋資料庫，獲取引數請求清單選項的當前清單。
- 確保在 ISE 分析條件中配置正確的引數請求清單值。一些比較常用的字串包括：

附註：使用 `debug` 指令之前，請先參閱 [有關 Debug 指令的重要資訊。](#)

日誌分析

++在 ISE PSN 節點上啟用以下調試 —

-nsf

-nsf-session

-lightwight 會話目錄

-profiler

-runtime-AAA

++初始驗證

++prrt-server.log

++在 ISE 節點上接收的訪問請求

Radius , 2020-12-29 06:35:19,377,DEBUG , 0x7f1cdc7ce700,cntx=0001348461,sesn=isee30-primary/397791910/625,CallingStationID=B4-96-91-26-EB-9F , **RADIUS資料包**
: **Code=1(AccessRequest)Identifier=182 Length=285**

++ISE 匹配 Unknown_profile

AcsLogs , 2020-12-29 06:35:19,473,DEBUG , 0x7f1cdc7ce700,cntx=0001348476,sesn=isee30-primary/397791910/625,CPMSessionID=0A6A270B00000018B44013AC , user=dot1xuser , CallingStationID=B4-96-91-26-EB-EB F , **AuthorizationPolicyMatchedRule=Unknown_Profile**, EapTunnel=EAP-FAST , EapAuthentication=EAP-MSCHAPv2, UserType=User , CPMSessionID=0A6A270B00000018B44013AC , EndPointMACAdress=B4-96-91-26-EB-9F ,

++ISE 傳送具有有限訪問許可權的訪問接受

Radius , 2020-12-29 06:35:19,474,DEBUG , 0x7f1cdc7ce700,cntx=0001348476,sesn=isee30-primary/397791910/625,CPMSessionID=0A6A270B00000018B44013AC , user=dot1xuser , CallingStationID=B4-96-91-26-EB-9F , **RADIUS PACKET:Code=2(AccessAccept)Identifier=186 Length=331**

++ISE 收到包含 DHCP 資訊的記帳更新

Radius , 2020-12-29 06:35:41,464,DEBUG , 0x7f1cdcad1700,cntx=0001348601,sesn=isee30-primary/397791910/627,CPMSessionID=0A6A270B00000018B44013AC , CallingStationID=B4-96-91-26-EB-9F , RADIUSPACKET:Code=4(AccountingRequest)Identifier=45 Length=381

[1]使用者名稱 — 值 : [dot1xuser]

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

[26] cisco-av-pair — 值 : [dhcp-option=

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

++ISE傳送回記帳響應

Radius , 2020-12-29 06:35:41,472 , 調試 , 0x7f1cdc5cc700,cntx=0001348601,sesn=isee30-primary/397791910/627,CPMSessionID=0A6A270B00000018B44013AC , user=dot1xuser , CallingStationID=B4-96-91-26-EB-9F , RADIUS PACKET:Code=5(AccountingResponse)Identifier=45 Length=20,RADIUSHandler.cpp:2216

++Profiler.log

++收到DHCP選項dhcp-parameter-request-list的記帳更新後 , ISE開始分析裝置

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 0000000655 2 0 2020-16:35:41 67 +00:00 0000234376 3002 NOTICE Radius-Accounting:RADIUS記帳監視程式更新

, ConfigVersionId=99 , 裝置IP地址=10.106.39.11 , 使用者名稱=dot1xuser , 請求延遲=6 , 網路裝置名稱=Sw , 使用者名稱=dot1xuser , NAS-IP-Address=10.106.39.11,NAS-Port=50113 , 類=CACS:0A6A270B00000018B44013 AC: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=Interim-Update , Acct-Delay-Time=0 , Acct-Input-Octets=174 , Acct-Output-Octets=0 , Acct-Session-Id=0000000b , Acct-Authentic=Remote , 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-parameter-request-list=1\, 3\, 6\, 15\, 31\, 44\, 46\, 47\, 1 9\, 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 -::: — 已解析的IOS感測器1:dhcp-parameter-request-list=[1, 3, 6, 15, 31, 33, 43, 44, 46, 47, 119, 121, 249, 252]

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

屬性 : dhcp-parameter-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 [RMQforwarder-4[]]

cisco.profiler.infrastructure.cache.AbstractEndpointCache -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:ProfilerCollection: — 此Mac的所有者 : B4:96:91:26:EB:9F is 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: — 端點B4:96:26:EB:Prob當前所有者fis isee30-primary.anshsinh.local , 消息代碼為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:- **is endpoint source radius true**

++新屬性

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:- **New attribute: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: — 已修改端點屬性但已設定 :

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:**Profiler集合 : - dhcp-parameter-request-list ,**

++不同的規則與不同的確定性因子匹配

2020-12-29 06:35:41,484 DEBUG [RMQforwarder-4]
cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:**Profiling: — 策略英特爾裝置匹配B4:96:91:EB:F (確定性5)**

2020-12-29 06:35:41,485 DEBUG [RMQforwarder-4]
cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:**Profiling: — 策略工作站與B4:96:26:EB:9F匹配0)**

2020-12-29 06:35:41,486 DEBUG [RMQforwarder-4] cisco.profiler.infrastructure.profilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:**Profiling: — 與B4:96:91:EB:9F匹配的策略Microsoft-Profiler (確定性10)**

2020-12-29 06:35:41,487 DEBUG [RMQforwarder-4] cisco.profiler.infrastructure.profilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:**Profiling:-Windows10-Workstation匹配策略B4:96:91:26:EB :9F (確定性20)**

++Windows10-Workstation基於配置的最高確定係數為40 , 因此選擇此作為裝置的終端配置檔案

2020-12-29 06:35:41,487 DEBUG [RMQforwarder-4]
cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:Profiling: — 分析策略層次結構後 : 終端 : **B4:96:91:26:EB:9F端點策略 : Windows10-Workstation for:40 ExceptionRuleMatched:false**

2020-12-29 06:35:41,487 DEBUG [RMQforwarder-4] cisco.profiler.infrastructure.profilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:**Profiling:-Endpoint B4:96:91:26:EB:9F匹配策略是。**

2020-12-29 06:35:41,489 DEBUG [RMQforwarder-4] cisco.profiler.infrastructure.profilerManager

-:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:Profiling:-Endpoint
B4:96:91:26:EB:9F身份組已更改。

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: — 設定終端B4:96:26:EB:Profiling上的身份組ID f - 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:-Calling end point cache with profiled end point B4:96:91 F , 策略
Windows10-Workstation , 匹配的策略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:-Sending event to persist end point B4:96:91:21:26:26:EB:EB:F
ep消息代碼= 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:-Endpoint B4:96:91:26:EB:9F身份組/邏輯配置檔案已更改。簽發有
條件的CoA

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:-ConditionalCoAEvent with Endpoint詳細資訊
: EndPoint[id=ff19ca00-499f-11eb-b713-1a99022ed3c5,name=<null>]

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

屬性 : Calling-Station-ID值 : B4-96-91-26-EB-9F

屬性 : EndPointMACAddress值 : B4-96-91-26-EB-9F

屬性 : MAC地址值 : B4:96:91:26:EB:9F

++將資料傳送到Lightweight Session Directory

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

2020-12-29 06:35:41,489 DEBUG [RMQforwarder-4][]
cisco.profiler.infrastructure.probemgr.LSDForwarderHelper -::: — 傳送事件到持久端點 , 同時為轉
發器新增LSD , defaultradius , defaultad B4:96:91:26:EB:9F

++選擇全域CoA作為Reauth

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-11ea-b713-
1a99022ed3c5:ProfilerCoA:- Configured Co全域性配置A命令型別= 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:: — 更新終點 — 來自傳入的EP:B4:96:91:26:EB:9Fep來源 : RADIUS探測SGA:falseSG:工作站

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:: — 合併後更新終點 — EP:B4:96:91:26:EB:9Fep來源 : RADIUS探測SGA:falseSG:Windows10-Workstation

++ISE匹配策略以檢查是否需要傳送CoA。ISE僅在具有符合配置檔案更改的任何策略時觸發CoA

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-11ea99022ed3c5:ProfilerCoA: — 處理所有可用策略本地異常策略集交換機, 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-11ea-b713-1a99022ed3c5:ProfilerCoA: — 策略名稱 : 交換機策略狀態 : 已啟用

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-11ea-b713-1a99022ed3c5:ProfilerCoA:- hsname 6d 954800-8bff-11e6-996c-525400b48521 rhs運算元ID 42706690-8c00-11e6-996c-525400b48521 rsvaluenameworkstation : 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: — 授權策略中可用的指定條件

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: — 具有策略的授權策略 : 42706690-8c00-11e6-996c-525400b48521

++授權策略與此條件匹配 , 並且觸發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-11ea-b713-1a99022ed3c5:ProfilerCoA:- applyCoa:基於終端RADIUS屬性建立的描述符 :

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

會話ID:[0A6A270B00000018B44013AC]

AAA伺服器 : [isee30-primary] IP:[10.106.32.119]

AAA介面 : [10.106.32.119]

NAD IP地址 : [10.106.39.11]

NAS埠Id:[GigabitEthernet1/0/13]

NAS埠型別 : [乙太網]

Service-Type:[已框架處理]

是否無線 : [假]

是VPN:[假]

是MAB:[假]

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-11ea-b713-1a99022ed3c5:ProfilerCoA: — 即將呼叫A for nad IP:10.106.39.11用於終端 : B4:96:91:26:EB:9F
CoA命令 : Reauth

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-11ea-b713-1a99022ed3c5:ProfilerCoA:-Applying CoCoCoCoCoCoCoCoCoCoCoCoA:-
CoCoCoCoCoCoCoCoCoCoCoCoCoCoCoCoCoA-REAUTH by AAA Server:10.106.32.119 via
Interface:10.106.32.119到NAD: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_Authentications 0000000656 2 1 StepData=2 (埠= 1700\ , 型別=
Cisco CoCoCoCoA) , CoASourceComponent=Profiler , CoAReason=用於授權策略的終端身份
組/策略/邏輯配置檔案的更改 , CoAType=Reauthentication - last , Network Device
Profile=Cisco ,

++prrt-server.log

AcsLogs , 2020-12-29
06:35:41,938,DEBUG , 0x7f1c6ffcb700,cntx=0001348611,Log_Message=[2020-12-29
06:35:41.938 +00:00 0000234379 80006 INFO Profiler:Profiler正在觸發授權請求更改 ,
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\,End
PointPolicyID=42706690-8c00-11e6-996c-525400b48521\,UseCase=\,NAS-Port-
Id=GigabitEthernet1/0/13\,NAS-Port-Type=Ethernet\,Response={User-Name=dot1xuser\;

DynamicAuthorizationFlow,2020-12-29
06:35:41,939,DEBUG , 0x7f1cdc3ca700,cntx=0001348614,[DynamicAuthorizationFlow::onLocalH
ttpEvent]收到傳入CoA命令 :

<Reauthenticate 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">GigabitEthernet1/0/13</identifierAttribute>

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

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

</session>

</Reauthenticate>

++CoA已傳送 —

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資料包
: **Code=43(CoARequest)**Identifier=27 Length=225

[4] NAS-IP-Address — 值 : [10.106.39.11]

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

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

[26] cisco-av-pair — 值 : [subscriber:command=reauthenticate]

[26] cisco-av-pair — 值 : [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資料包
: **Code=44(CoAAck)**Identifier=27

++新訪問請求

Radius , 2020-12-29 06:35:41,970,DEBUG , 0x7f1cdc6cd700,cntx=0001348621,sesn=isee30-primary/397791910/628,CallingStationID=B4-96-91-26-EB-9F , RADIUS
PACKET:**Code=1(AccessRequest)**Identifier=187 Length=285

++ISE匹配與終端裝置的終端策略匹配的新授權配置檔案

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_workstation , EapTunnel=EAP-FAST ,
EapAuthentication=EAP-MSCHAPv2, UserType=User ,
CPMSessionID=0A6A270B00000018B44013AC , EndPointMACAdress=B4-96-91-26-EB-9F
posture , F AssessmentStatus=NotApplicable , **EndPointMatchedProfile=Windows10-Workstation** ,

++訪問接受已傳送 —

Radius , 2020-12-29 06:35:42,061,DEBUG , 0x7f1cdcad1700,cntx=0001348636,sesn=isee30-primary/397791910/628,CPMSessionID=0A6A270B00000018B44013AC , user=dot1xuser , CallingStationID=B4-96-91-26-EB-9F radius封包 : **Code=2(AccessAccept)**Identifier=191 Length=340

相關資訊

- [Fingerbank.org DHCP指紋資料庫](#)
- [技術支援與文件 - Cisco Systems](#)