

# エンドポイントのプロファイリングに使用される DHCP パラメータ要求リスト オプション 55 の設定例

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[ログ分析](#)

[関連情報](#)

## 概要

このドキュメントでは、Identity Services Engine (ISE) を使用するデバイスをプロファイリングするための代替の方法として、DHCP パラメータ要求リスト オプション 55 を使用する方法について説明します。

## 前提条件

### 要件

Cisco では次の前提を満たす推奨しています。

- DHCP ディスカバリ プロセスに関する基本知識があること
- ISE を使用したカスタム プロファイリング ルールの設定に関する経験があること

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ISE バージョン 3.0
- Windows 10

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

## 背景説明

ISE の実稼働導入で、より一般的に導入されるプロファイリング プロープには、RADIUS、HTTP、DHCP などがあります。User-Agent 文字列から重要なエンドポイント データをキャプチャするために、ISE ワークフローの中央で URL リダイレクションを使用した、HTTP プロープが広く使用されています。ただし、一部の実稼働のユースケースでは、URLリダイレクトが望ましくなく、Dot1xが優先されるため、エンドポイントを正確にプロファイルすることが困難になります。たとえば、企業のService Set Identifier(SSID)に接続する従業員のPCはフルアクセスを取得し、個人のiDevice(iPhone、iPad、iPod)はインターネットアクセスのみを取得します。両方のシナリオで、ユーザはプロファイリングされ、Web ブラウザを開くのにユーザに依存しない、認可プロファイル照合用のより特定の ID グループに動的にマッピングされます。よく使用される別の代替方法は、ホスト名の照合です。この解決策は、ユーザがエンドポイントのホスト名を非標準の値に変更する可能性があるため不完全です。

このような難しいケースでは、DHCP プロープおよび「DHCP のパラメータ要求リスト」のオプション 55 を、これらのデバイスのプロファイリングのための代替方法として使用できます。DHCP パケット内の「パラメータ要求リスト」フィールドは、侵入防御システム (IPS) がパケットを照合するために署名を使用するのと同様に、エンドポイントのオペレーティングシステムのフィンガープリントを照合するために使用できます。エンドポイントのオペレーティングシステムが DHCP ディスカバーまたは DHCP 要求のパケットを回線に送信する場合、製造業者は DHCP サーバ ( デフォルト ルータ、ドメイン ネーム サーバ ( DNS )、TFTP サーバなど ) から受信予定の DHCP オプションの数字のリストを組み込みます。DHCP クライアントがサーバからこれらのオプションを要求する順序はかなり独自のもので、特定の送信元のオペレーティングシステムのフィンガープリントを照合するために使用できます。「パラメータ要求リスト」オプションの使用は、HTTP の User-Agent 文字列ほど厳密ではありませんが、ホスト名や他の静的に定義されたデータよりもはるかに制御されたものです。

**注：**「DHCP のパラメータ要求リスト」のオプションは完全な解決策ではありません。この理由は、このオプションで生成されるデータがベンダーに依存し、複数のデバイス タイプで重複する可能性があるためです。

ISE のプロファイリング ルールを設定する前に、DHCP パケット内に「パラメータ要求リスト」のオプションを評価するために ( 存在する場合 )、エンドポイントまたは Switched Port Analyzer ( SPAN; スイッチド ポート アナライザ ) からの Wireshark キャプチャ、または ISE の Transmission Control Protocol ( TCP ) ダンプのキャプチャを使用します。次のキャプチャ例は、Windows 10のDHCPパラメータ要求リスト(NRLIST)オプションを示しています。

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
< 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

```

結果の「パラメータ要求リスト」の文字列は、1、3、6、15、31、33、43、43、44、46、47、119、121、249、252。ISEでカスタム・プロファイリング条件を構成する場合は、この形式を使用します。

設定セクションでは、Windows 10ワークステーションをWindows 10-Workstationに一致させるためのカスタムプロファイリング条件の使用について説明します。

## 設定

1. ISE の管理 GUI にログインし、[Policy] > [Policy Elements] > [Conditions] > [Profiling] に移動します。[Add] をクリックして、新規のカスタム プロファイリング条件を追加します。この例では、Windows 10のパラメータ要求リスト(NRLIST)フィンガープリントを使用しています。「パラメータ要求リスト」の値の全体のリストについては、「[Fingerbank.org](http://Fingerbank.org)」を参照してください。

注：[Attribute Value] テキスト ボックスに数字のオプションの一部が表示されない場合があります、その場合はリストすべてを表示するために、マウスまたはキーボードでスクロールすることが必要になります。

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. カスタム条件を定義した状態で、[Policy] > [Profiling] > [Profiling Policies]に移動して、現在のプロファイリングポリシーを変更するか、新しいプロファイリングポリシーを設定します。この例では、新しいパラメータ要求リストの条件を含むため、デフォルトの Workstation、Microsoft-Workstation、Windows10-Workstationポリシーが編集されます。次に示すように、新しい複合条件をWorkstation、Microsoft-Workstation、Windows10-Workstationのプロファイラポリシールールに追加します。目的のプロファイリング結果を達成するために、必要に応じて [Certainty Factor] を変更します。

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

VMWare-Device  
Vizio-Device  
WYSE-Device  
**Workstation**  
ChromeBook-Workstati  
FreeBSD-Workstation  
Linux-Workstation  
Macintosh-Workstati  
Microsoft-Workstatio  
OpenBSD-Workstation  
Sun-Workstation  
Xerox-Device  
Z-Com-Device  
ZTE-Device  
Zebra-Device

* 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

注：このセクションで使用されるコマンドの詳細については、[Command Lookup Tool \(登録ユーザ専用\)](#) を使用してください。

## 確認

### ステップ 1-

[ISE] > [Operations] > [Live Logs] に移動します。最初の認証はUnknown Authorization Policyに一致し、制限付きアクセスがISEに付与されます (ISEはISEに対してアクセスを許可します)。デバイスのプロファイルが作成された後、ISEはCoAをトリガーし、ISEで別の認証要求を受信し、新しいプロファイル(Windows10 Workstation)と一致します。

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	<span style="color: blue;">●</span>		0	dot1xuser	B4:96:91:26:EB:9F		Windows10-Workstation	Switch >> Microsoft_workstation	PermitAccess
Dec 29, 2020 06:35:42.059 AM	<span style="color: green;">●</span>			dot1xuser	B4:96:91:26:EB:9F	Workstation	Windows10-Workstation	Switch >> Microsoft_workstation	PermitAccess
Dec 29, 2020 06:35:41.948 AM	<span style="color: green;">●</span>				B4:96:91:26:EB:9F				
Dec 29, 2020 06:35:19.473 AM	<span style="color: green;">●</span>			dot1xuser	B4:96:91:26:EB:9F	Profiled	Intel-Device	Switch >> Unknown_Profile	Unknown_profile_limited_access

## ステップ2-

ここでは、設定が正常に機能しているかどうかを確認します。

- [コンテキストの表示] > [エンドポイント]に移動し、エンドポイントを検索して[編集]をクリックします。
- EndPointPolicyがWindow10-Workstationであり、dhcp-parameter-request-listの値が以前に設定した条件値と一致していることを確認します。

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

## トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

- DHCP パケットが ( helper-address または SPAN を使用して ) プロファイリング機能を実行する ISE ポリシー ノードに到達したことを検証します。
- [Operations] > [Troubleshoot] > [Diagnostic Tools] > [General Tools] > [TCP Dump] ツールを使用します。ISE 管理 GUI から TCP ダンプ キャプチャ をネイティブで実行します。
- ISE PSN ノードで次のデバッグを有効にします。-nsf-nsf-session-lightweight セッションディレクトリ-プロファイラ-runtime-AAA
- Profiler.log、prrt-server.log、および lsd.log に関連情報が表示されます。
- 「パラメータ要求リスト」のオプションの現時点のリストについては、[Fingerbank.org](http://Fingerbank.org) の [DHCP フィンガープリントのデータベースを参照してください。](#)
- 正しい「パラメータ要求リスト」の値を ISE のプロファイリング条件に必ず設定するようにしてください。一般的によく使用されるいくつかの文字列には、次のものがあります。

注 : debug コマンドを使用する前に、[「デバッグ コマンドの重要な情報」を参照してください。](#)

## ログ分析

++ISE PSN ノードで次のデバッグを有効にします。

-nsf

-nsf-session

-lightweight セッションディレクトリ

-プロファイラ

-runtime-AAA

++初期認証

++prrt-server.log

++ISE ノードでアクセス要求を受信

```
Radius,2020-12-29 06:35:19,377,DEBUG,0x7f1cdc7bd2700,cntx=0001348461,sesn=isee30-  
primary/397791910/625,CallingStationID=B4-96-91-26-EB-9F,RADIUS  
PACKET::Code=1(AccessRequest) Identifier=182 Length=285
```

++ISE が Unknown\_profile に一致する

```
AcsLogs, 2020-12-29 06:35:19,473,DEBUG,0x7f1cdc7ce700,cntx=0001348476,sesn=isee30-  
primary/397791910/625,CPMSessionID=0A6A270B00000018B4401 3AC、user=dot1xuser、  
CallingStationID=B4-96-91-26-EB-9F、AuthorizationPolicyMatchedRule=Unknown_Profile、  
EapTunnel=EAP-FAST、EapAuthentication=EAP-MSCHAPv2、UserType=User、  
CPMSessionID=0A6A270B00000018B44013AC、エンドポイント MAC Address=B4-96-91-26-EB-  
9F、
```

++ISE が制限付きアクセスで Access Accept を送信

Radius,2020-12-29 06:35:19,474,DEBUG,0x7f1ce7ce700,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がDHCP情報を含むアカウント更新を受信

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,RADIUS PACKET::**Code=4(AccountingRequest)** Identifier=45 Length=381

[1]ユーザー名 – 値 : [dot1xuser]

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

[26] cisco-av-pair – 値 : [dhcp-option=

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

++ISEがアカウント回答を返信

Radius,2020-12-29 06:35:41,472,DEBUG,0x7f1cc5cc700,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

++DHCPオプションdhcp-parameter-request-listでアカウント更新を受信すると、ISEはデバイスのプロファイリングを開始します

2020-12-29 06:35:41,470 DEBUG [SyslogListenerThread[]]  
cisco.profiler.probes.radius.SyslogDefragmenter -::: - **parseHeader inBuffer=<181>Dec 29**  
06:35:41 isee30-primary EXICE\_RADIUS\_Accounting 0000000655 2 2020-12-29.4 67 +00:00  
0000234376 3002**注意Radius-Accounting:RADIUSアカウントウォッチドッグアップデート**  
、ConfigVersionId=99、デバイスIPアドレス=10.106.39.11、UserName=dot1xuser、  
RequestLatency=6、NetworkDeviceName=Sw、User-Name=dot1xuser、NAS-IP-  
Address=10.106.39.11、NAS-Port=50 113、Class=CACS:0A6A270B00000018B44013AC:ise30-  
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、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 \, 33\, 43\, 44\, 46\, 47\, 119\, 121\, 249\, 252, cisco-av-pair=audit-**  
**session-id=0A6A270B00000018B4013AC, cisco-av-pair=method=dot1x,**

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

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

属性 : 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:Profilerコレクション : :このMacの所有者 : 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: – エンドポイントB4:96:91:26:EB:9Fis  
isee30-primary.anshsinh.localの現在の所有者とメッセージコードは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: – エンドポイントソースradius true

++新しい属性

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: – 新しい属性 : 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:Profilerコレクション : – エンドポイント変更された属性セット :

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

++異なるルールが異なる確信度に一致

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 : プロファイル – ポリシーIntel-Device matched B4:96:91:26:EB:9F ( 確実性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 : プロファイル – ポリシーワークステーションがB4:96:91:26:EB:9Fに一致 ( 確実性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 : プロファイル – ポリシーMicrosoft-WorkstationがB4:96:91:26:EB:9Fと一致しました ( 確実性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 : プロファイル : ポリシー : Windows10-Workstationが  
B4:96:91:26:EB:9Fと一致しました ( 確実性20 )

++Windows10-Workstationは、設定に基づいて確信度が40の最も高いため、デバイスのエンドポイントプロファイルとして選択されます

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 : プロファイリング – ポリシー階層の分析 : エンドポイント  
:B4:96:91:26:EB:9F EndpointPolicy:Windows10-Workstation for: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 : プロファイルエンドポイント : B4:96:91:26:EB:9F Matched Policy  
Changed.

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 : プロファイルエンドポイント : B4:96:91:26:EB:9F IdentityGroupが変更されました。

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:設定エンドポイントB4:96:91:26:EB:9F - 3b76f840-8c00-11e6-996c-525400b48521のアイデンティティグループID

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 : プロファイル – プロファイルされたエンドポイントB4:96:91:26:EB:9F、  
ポリシーWindows10-Workstation、一致したポリシーWindows10-Workstationを持つエンドポイント  
トキャッシュ

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:送信エンドポイントB4:96:91:26:EB:9F、およびepメッセージコードを保持  
するイベント= 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 : プロファイルエンドポイント : B4:96:91:26:EB:9F IdentityGroup /論理  
プロファイルが変更されました。条件付きCoAの発行

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:- Profiling: エンドポイントの詳細を含む  
CoAEvent:EndPoint[id=ff19ca00-499f-11eb-b713-1a99022ed3c5,name=<null>]

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

属性 : Calling-Station-ID値 : B4-96-91-26-EB-9F

属性 : EndPointMACAddress値 : B4-96-91-26-EB-9F

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

++Lightweightセッションディレクトリへのデータの送信

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

2020-12-29 06:35:41,489 DEBUG [RMQforwarder-4[]]  
cisco.profiler.infrastructure.probemgr.LSDForwarderHelper -:::- forwarder,defaultus,defaultad  
B4:96:91:26:EB:9F用にLSDを追加しているときにイベントを送信する

++グローバルCoAが再認証として選択されている

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-  
1a 99022ed3c5:ProfilerCoA: - 設定済みグローバルCoAコマンドタイプ= 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::- エンドポイントの更新 - 着信からの  
EP:B4:96:91:26:EB:9FepSource:RADIUS ProbeSGA:falseSG:ワークステーション

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::- エンドポイントの更新 - マージ後の  
EP:B4:96:91:26:EB:9FepSource:RADIUS ProbeSGA:falseSG:Windows10-Workstation

++ISEはポリシーに一致し、CoAを送信する必要があるかどうかを確認します ( CoAが必要かどうか ) 。 ISEがCoAをトリガーするのは、プロファイルの変更に一致するポリシーがある場合だけです

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-  
1a 9 9022ed3c5:ProfilerCoA:- Local Exception PolicySet Switch , 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-  
1a 99022ed3c5:ProfilerCoA: - ポリシー名 : スイッチポリシーステータス : 有効

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-  
1a 99022ed3c5:ProfilerCoA:- lhsvalue name 6d954800-8bff-11e6-996c-525400b48521 rhs  
operandID 42706690-8c000 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-b713-1a9902 2ed3c5:ProfilerCoA: - 指定された条件が  
承認ポリシーで使用可能

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-b713-1a9902 2ed3c5:ProfilerCoA:- Authorization Policy  
HAVING Policy :42706690-8c00-11e6-996c-525400b48521

++認可ポリシーがこの条件に一致し、CoAがトリガーされます

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-b713-1a 99022ed3c5:ProfilerCoA:- applyCoa:エンドポイントRADIUS属性に基づいて記述子を作成 :

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

Session ID:[0A6A270B00000018B44013AC]

AAA サーバ : [isee30-primary] IP:[10.106.32.119]

AAAインターフェイス : [10.106.32.119]

NAD IPアドレス : [10.106.39.11]

NASポートID:[GigabitEthernet1/0/13]

NAS Port Type:[イーサネット]

Service-Type:[フレーム]

ワイヤレス : [false]

VPN:[false]

MAB:[false]

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-b713-1a 99022ed3c5:ProfilerCoA:- and IPのCoAをコールしようとしています : エンドポイント用の 10.106.39.11:B4:96:91:26:EB:9F CoAコマンド : 再認証

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-b713-1a 99022ed3c5:ProfilerCoA:- AAAサーバによるCoA-REAUTHの適用 : 10.106.32.119 via Interface:10.106.32.119からNAD:10.106.39.11

2020-12-29 06:35:41,949 DEBUG [SyslogListenerThread][]

cisco.profiler.probes.radius.SyslogDefragmentter -::- parseHeader inBuffer=<181>Dec 29 06:35:41 isee30-primary EXCISE\_Passed\_Authentications 0000000656 2 1 StepData=2= = 1700 \, type = Cisco CoA ), CoASourceComponent=Profiler, CoAReason=認証ポリシーで使用されるエンドポイントアイデンティティグループ/ポリシー/論理プロファイルの変更 , CoAType=Reauthentication – 最後のネットワークデバイスプロファイル=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:プロファイルが認可変更の要求、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={User-Name=dot1xuser};

DynamicAuthorizationFlow,2020-12-29

06:35:41,939,DEBUG,0x7f1cdc3ca700,cntx=0001348614,[DynamicAuthorizationFlow::onLocalHttpEvent] Received incoming CoA command:

```
<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>
```

```
</再認証>
```

++CoA送信済み -

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パケット : Code=43(CoARequest) Identifier=27 Length=225

[4] NAS-IP-Address – 値 : [10.106.39.11]

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

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

[26] cisco-av-pair – 値 : [サブスクリイバ : コマンド=再認証]

[26] cisco-av-pair – 値 : [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パケット : Code=44 (CoAACK) Identifier=27

++新しいアクセス要求

Radius,2020-12-29 06:35:41,970,DEBUG,0x7f16cd700,cntx=0001348621,sesn=isee30-primary/397791910/628,CallingStationID=B4-96-91-26-EB-9F,RADIUS CDC:Code=1(AccessRequest) Identifier=187 Length=285

++ISEは、エンドポイントデバイスのエンドポイントポリシーに一致する新しい認可プロファイルと一致します

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, cpmsSESSION ID=0A6A270B00000018B44013AC、EndPointMACAddress=B4-96-91-26-EB-9F、PostureAssessmentStatus=NotApplicable、EndPointMatchedProfile=Windows10-Workstation、

++Access Acceptが送信されます。

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 PACKET::Code=2(AccessAccept) Identifier=191 Length=340

## 関連情報

- [Fingerbank.org の DHCP フィンガープリントのデータベース](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)