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](#)
[トラブルシュート](#)
[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。

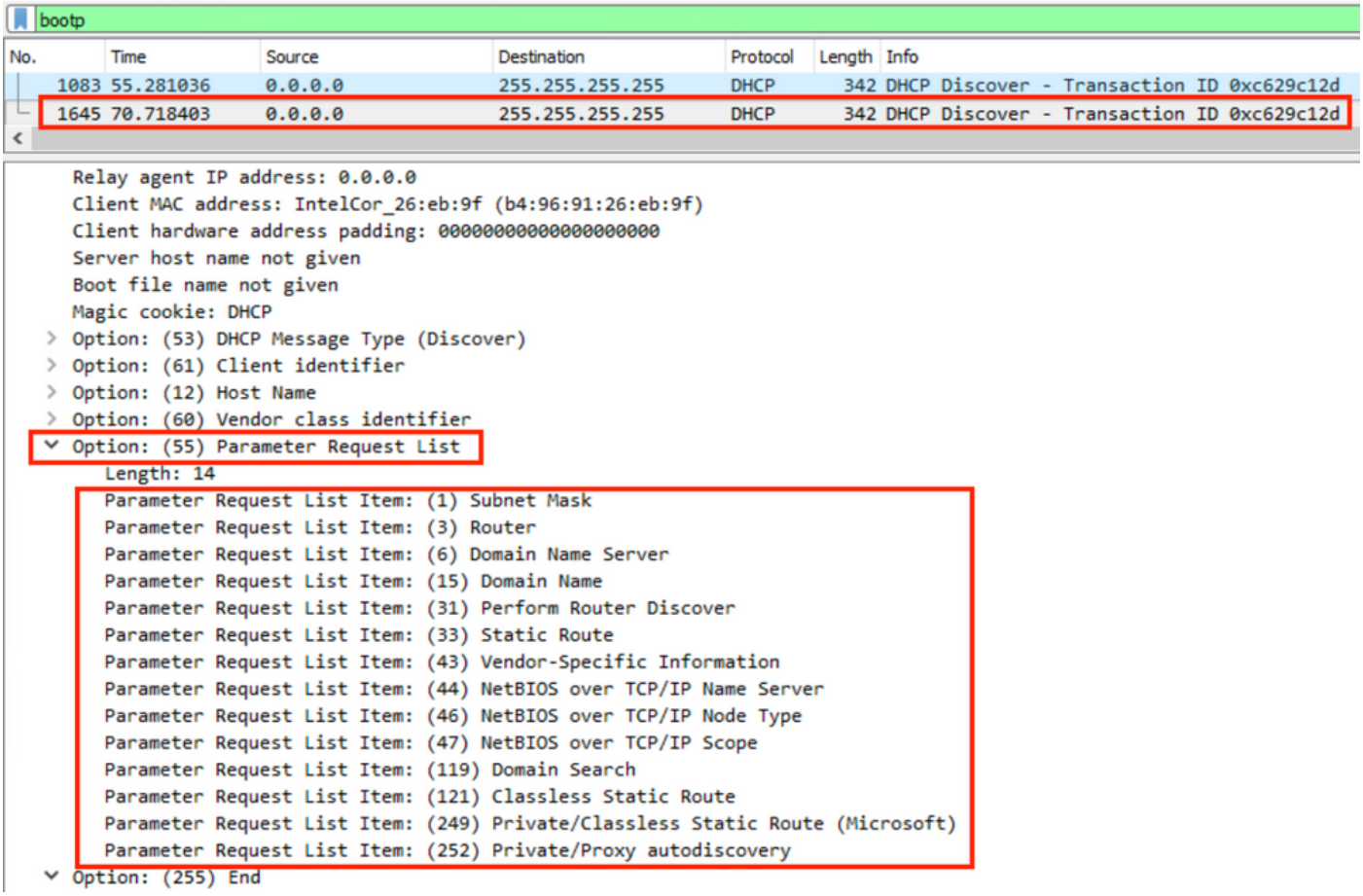
背景説明

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 プローブには、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 プローブ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的な 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 プローブおよび「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ほとんど同様に、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。

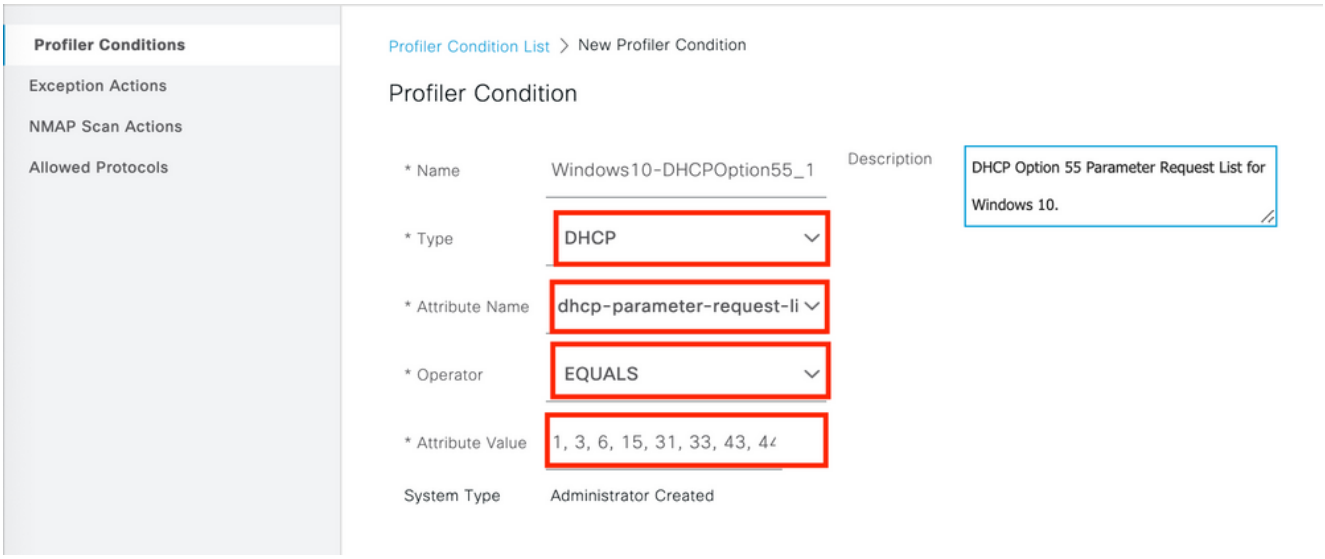


結果の「パラメータ要求リスト」の文字列は、1、3、6、15、31、33、43、43、44、46、47、119、121、249、252。ISEでカスタム・プロファイリング条件を構成する場合は、この形式を使用します。

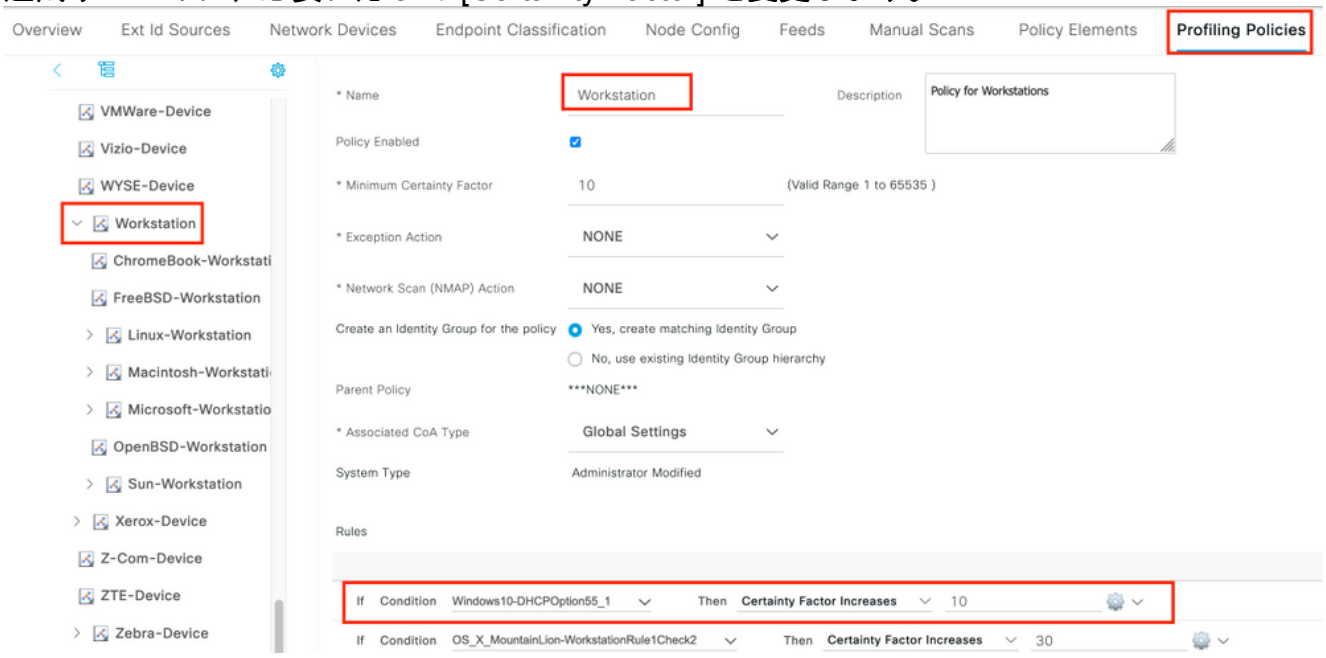
設定セクションでは、Windows 10ワークステーションをWindows 10-Workstationに一致させるためのカスタムプロファイリング条件の使用について説明します。

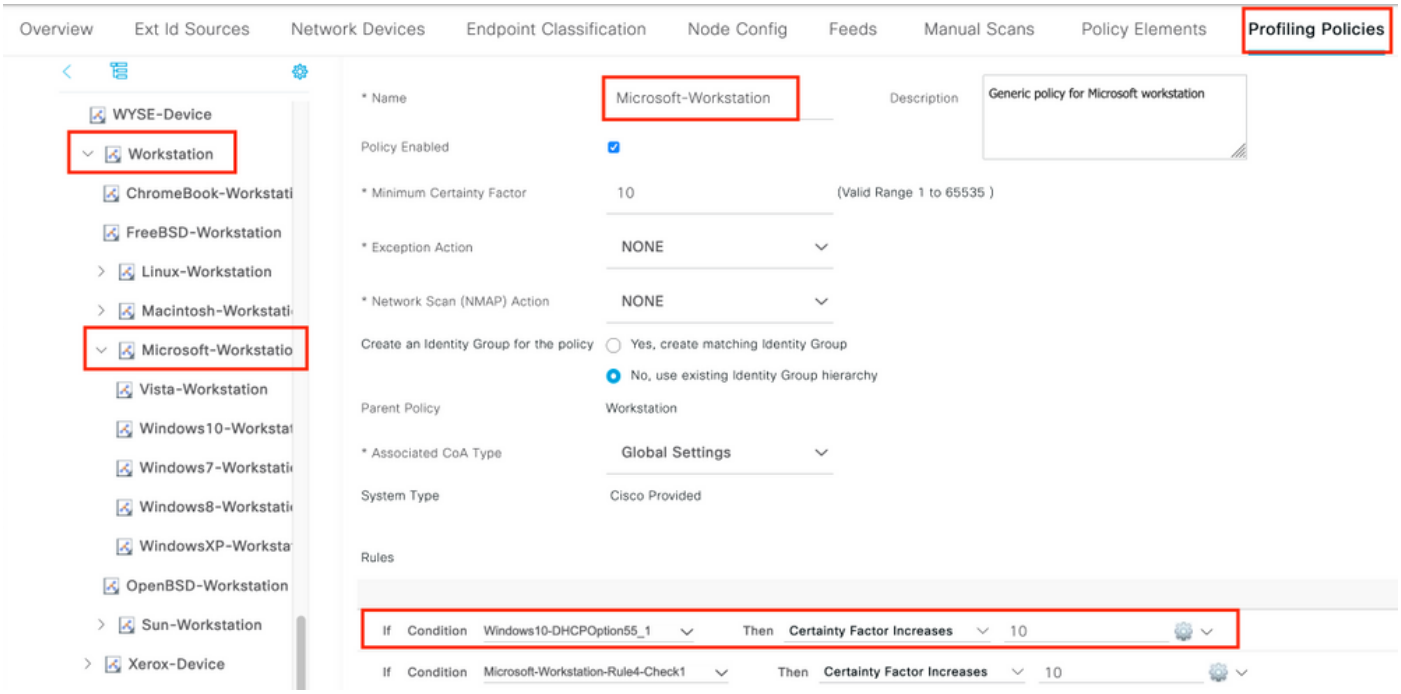
設定

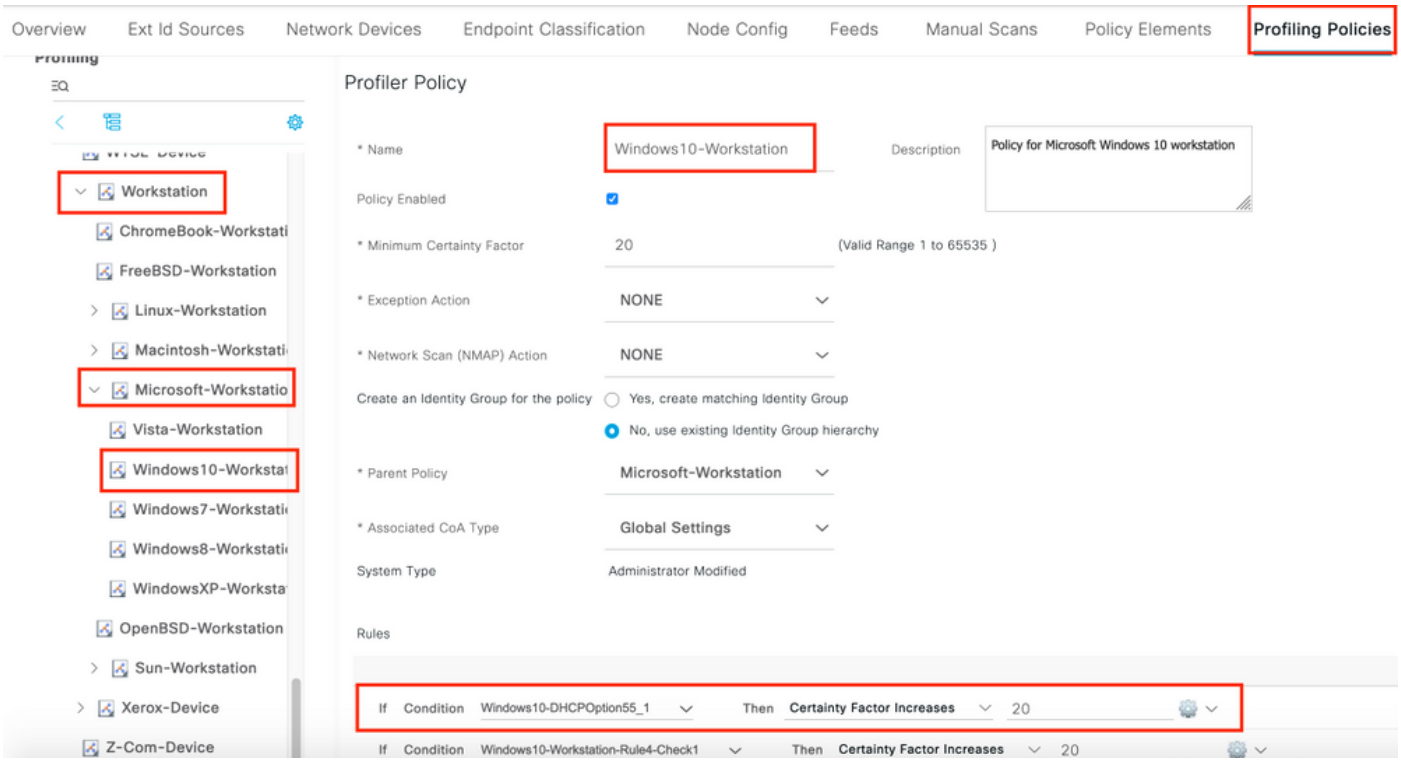
1. ISE の管理 GUI にログインし、[Policy] > [Policy Elements] > [Conditions] > [Profiling] に移動します。[Add] をクリックして、新規のカスタム プロファイリング条件を追加します。この例では、Windows 10のパラメータ要求リスト(NRLIST)フィンガープリントを使用しています。「パラメータ要求リスト」の値の全体のリストについては、「Fingerbank.org 」を参照してください。
   注：[Attribute Value] テキスト ボックスに数字のオプションの一部が表示されない場合があり、その場合はリストす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。



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。**





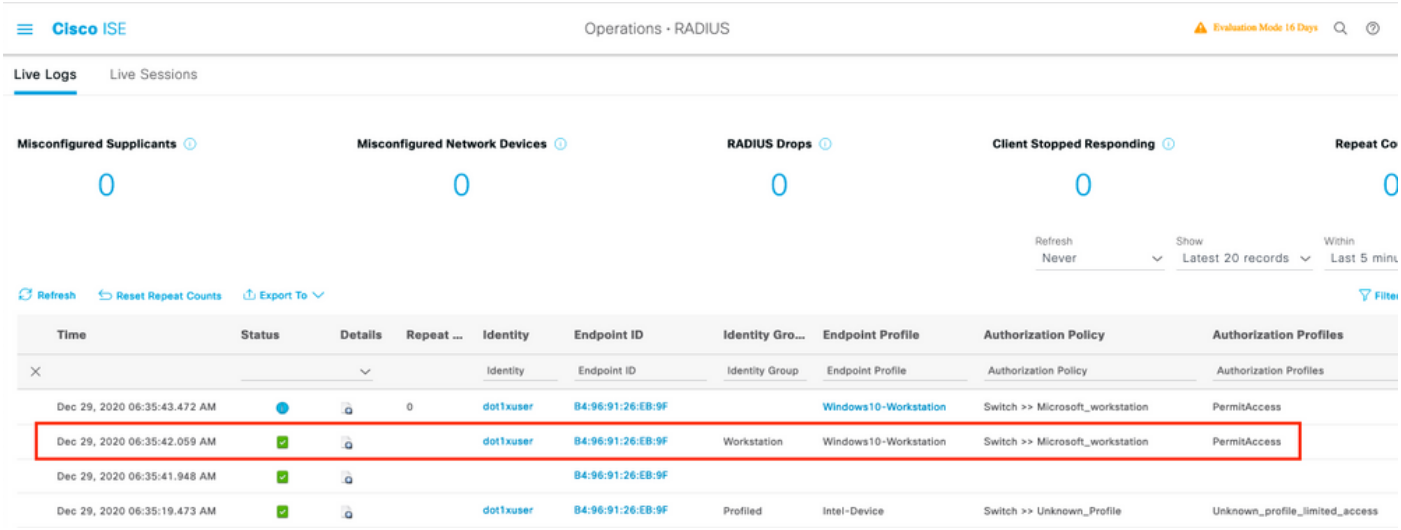


注：このセクションで使用されるコマンドの詳細については、Command Lookup Tool（登録ユーザ専用）を使用してください。

確認

ステップ 1-

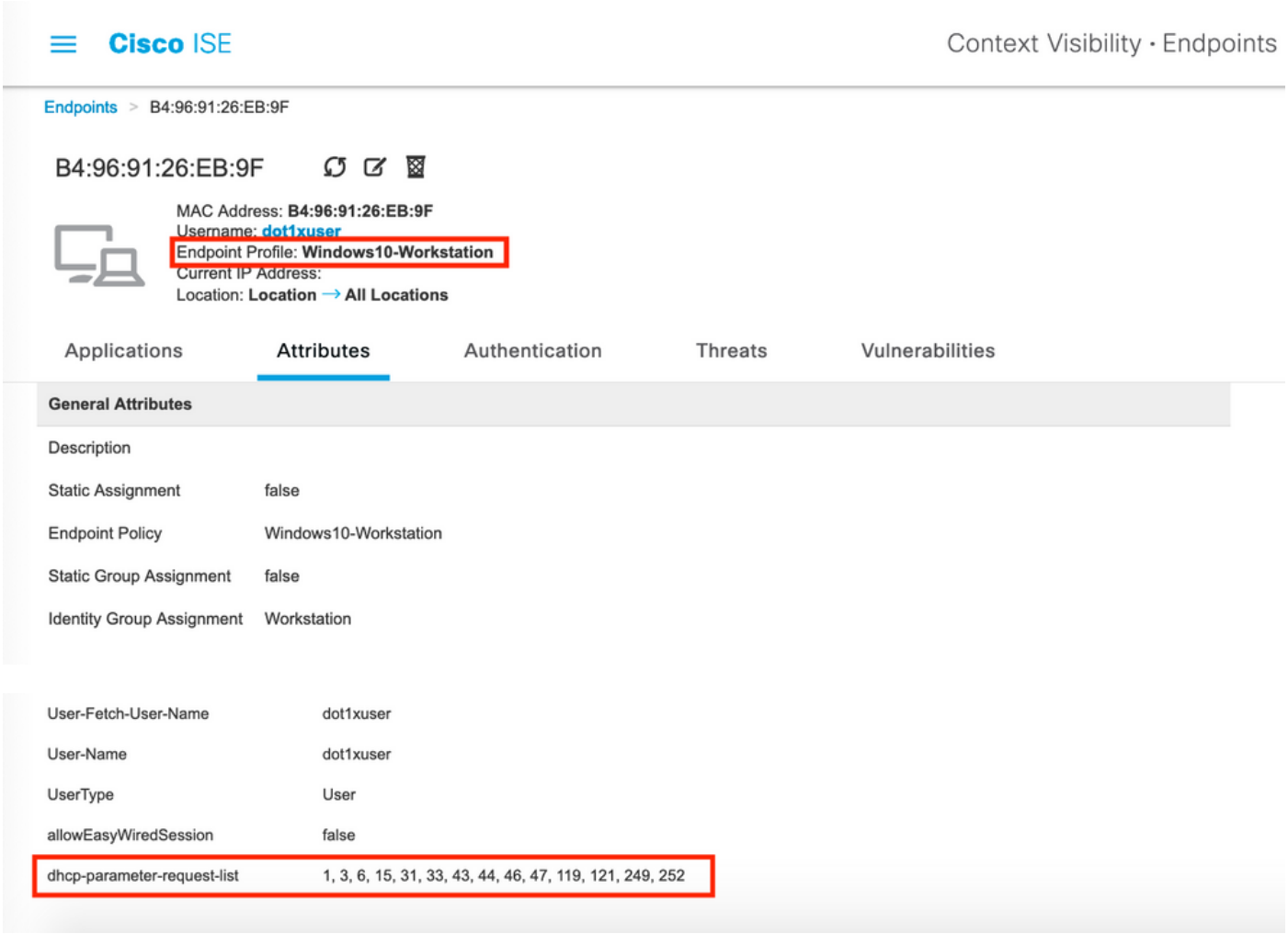
[ISE] > [Operations] > [Live Logs]に移動します。最初の認証はUnknown Authorization Policyに一致し、制限付きアクセスがISEに付与されます（ISEはISEに対してアクセスを許可します）。デバイスのプロファイルが作成された後、ISEはCoAをトリガーし、ISEで別の認証要求を受信し、新しいプロファイル(Windows10 Workstation)と一致します。



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。**



トラブルシュート

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 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,0x7f1cdcbd2700,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MACAddress=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ティング更新を受信

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がアカウンティング応答を返信

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でアカウンティング更新を受信すると、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.SyslogDefragmentter -:::- **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アカウンティング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:プロファイラが認可変更の要求、**ConfigVersionId=99、**EndpointCoA=Reauth、**EndpointMacAddress=B4:96:91:26:EB:9F、EndpointNADAddress=10.106.39.11、**EndpointPolicy=Windows10-Workstation、**Endpoint **Property=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：[サブスクライバ：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, cpmsESSION 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