DHCP Parameter Request List Option 55 Used to Profile Endpoints Configuration 예

목차

소개

이 문서에서는 ISE(Identity Services Engine)를 사용하는 디바이스를 프로파일링하는 대체 방법으로 DHCP Parameter Request List 옵션 55를 사용하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco는 다음과 같은 기능을 권장합니다.

- DHCP 검색 프로세스에 대한 기본 지식
- ISE를 사용하여 사용자 지정 프로파일링 규칙을 구성하는 경험

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ISE 버전 3.0
- Windows 10

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

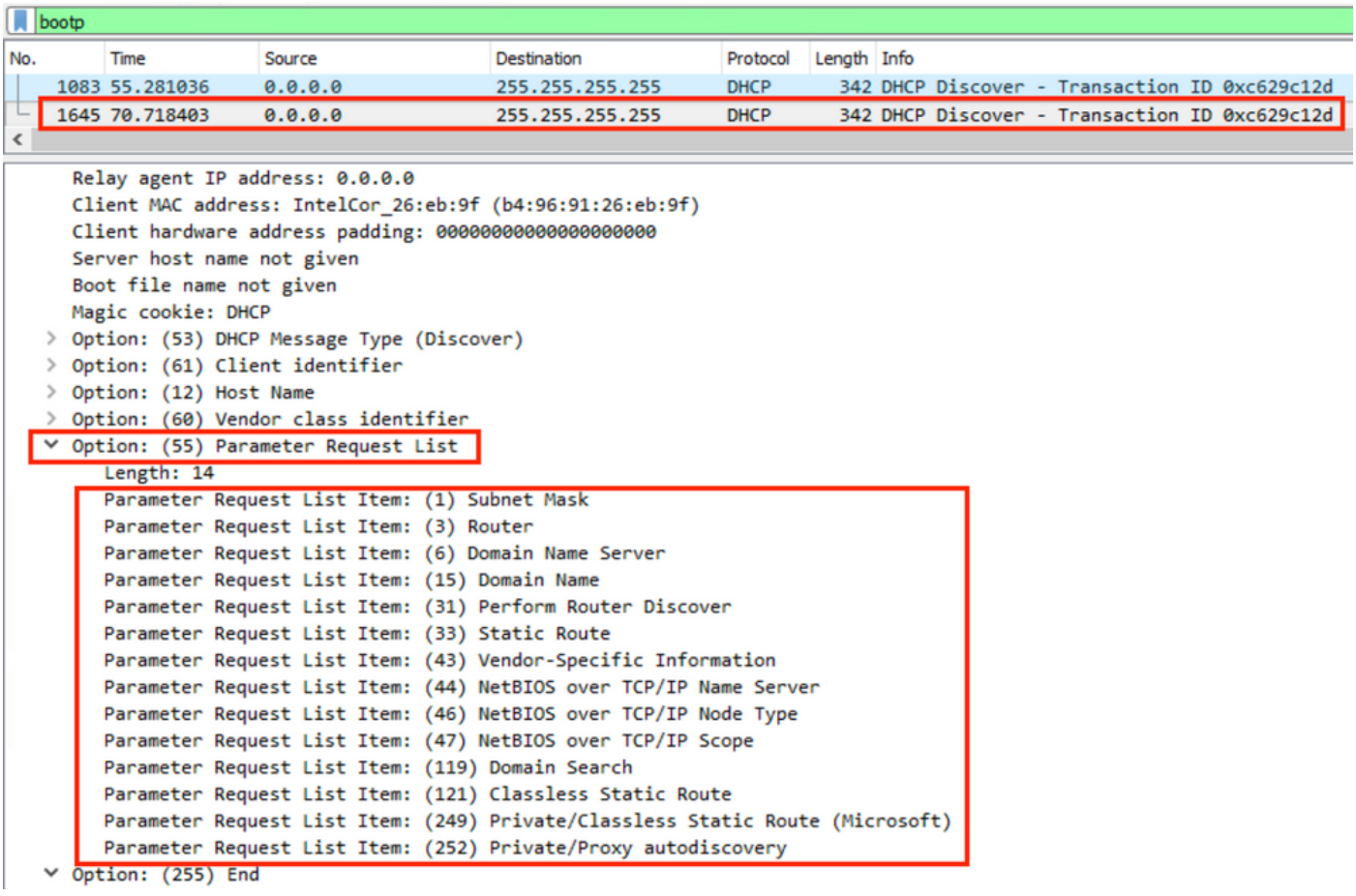
프로덕션 ISE 구축에서, 더 많이 구축되는 프로파일링 프로브 중 일부는 RADIUS, HTTP 및 DHCP를 포함합니다.ISE 워크플로의 중심에 URL 리디렉션이 있는 경우 HTTP 프로브는 User-

Agent 문자열에서 중요한 엔드포인트 데이터를 캡처하기 위해 널리 사용됩니다.그러나 일부 프로덕션 활용 사례에서는 URL 리디렉션을 원하지 않으며 Dot1x를 선호하므로 엔드포인트를 정확하게 프로파일링하기가 더 어렵습니다.예를 들어, 회사 SSID(Service Set Identifier)에 연결하는 직원 PC는 개인 iDevice(iPhone, iPad, iPod)가 인터넷 액세스만 받는 동안 전체 액세스 권한을 갖습니다.두 시나리오에서 모두 사용자가 웹 브라우저를 열 때 사용자에게 의존하지 않는 권한 부여 프로파일 일치를 위해 더 구체적인 ID 그룹에 동적으로 매핑되고 프로파일링됩니다.일반적으로 사용되는 또 다른 대안은 호스트 이름 일치입니다.사용자가 엔드포인트 호스트 이름을 비표준 값으로 변경할 수 있으므로 이 솔루션은 불완전합니다.

이러한 경우 DHCP 프로브 및 DHCP Parameter Request List 옵션 55를 이러한 디바이스를 프로파일링하는 대체 방법으로 사용할 수 있습니다.IPS(Intrusion Prevention System)에서 시그니처를 사용하여 패킷을 확인하는 것과 같이 DHCP 패킷의 Parameter Request List 필드를 사용하여 엔드포인트 운영 체제를 핑거프린트 처리할 수 있습니다.엔드포인트 운영 체제가 DHCP 검색 또는 요청 패킷을 와이어에 전송할 때 제조업체는 DHCP 서버(기본 라우터, DNS(Domain Name Server), TFTP 서버 등)에서 수신할 DHCP 옵션의 숫자 목록을 포함합니다. DHCP 클라이언트가 서버에서 이러한 옵션을 요청하는 순서는 매우 고유하며 특정 소스 운영 체제의 핑거프린트 처리를 위해 사용할 수 있습니다.Parameter Request List(매개변수 요청 목록) 옵션의 사용은 HTTP User-Agent 문자열만큼 정확하지는 않지만, 호스트 이름 및 기타 정적으로 정의된 데이터의 사용보다 훨씬 더 제어됩니다.

> **참고:**DHCP Parameter Request List(DHCP 매개변수 요청 목록) 옵션은 공급업체에 종속적이며 여러 디바이스 유형에 의해 중복될 수 있으므로 완벽한 솔루션이 아닙니다.

ISE 프로파일링 규칙을 구성하기 전에 DHCP 패킷의 Parameter Request List 옵션을 평가하기 위해 ISE에서 엔드포인트/SPAN(Switched Port Analyzer) 또는 TCP(Transmission Control Protocol) 덤프 캡처의 Wireshark 캡처를 사용합니다(있는 경우). 이 샘플 캡처는 Windows 10에 대한 DHCP 매개 변수 요청 목록 옵션을 표시합니다.

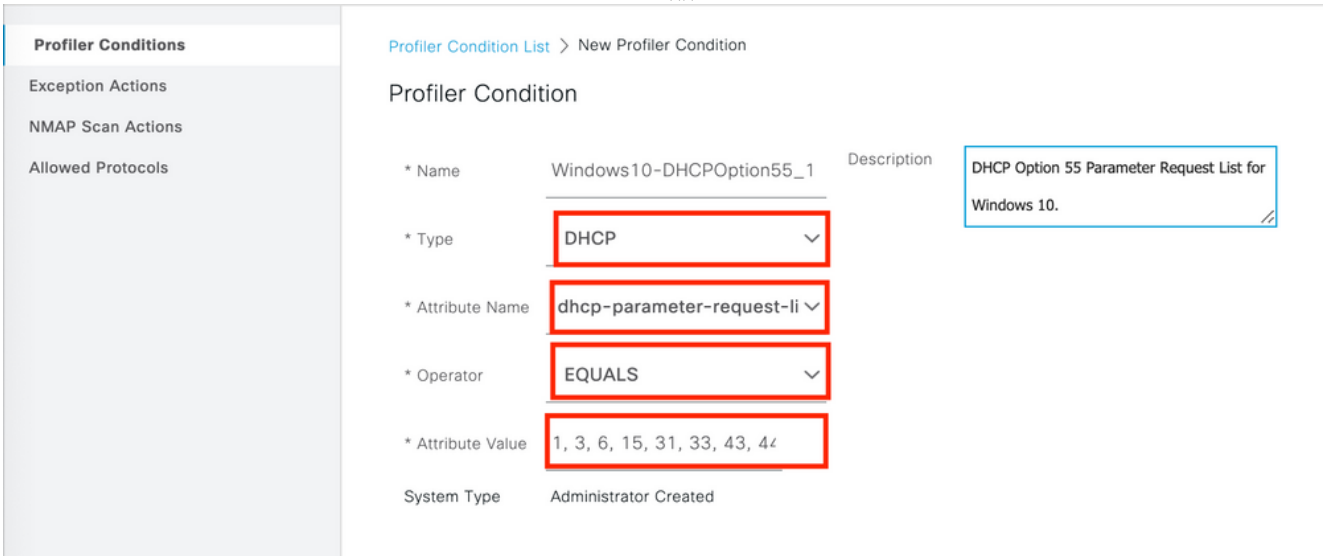


결과를 나타내는 매개변수 요청 목록 문자열은 쉼표로 구분된 다음 형식으로 작성됩니다.1, 3, 6, 15, 31, 33, 43, 44, 46, 47, 119, 121, 249, 252. ISE에서 사용자 정의 프로파일링 조건을 구성할 때 이 형식을 사용합니다.

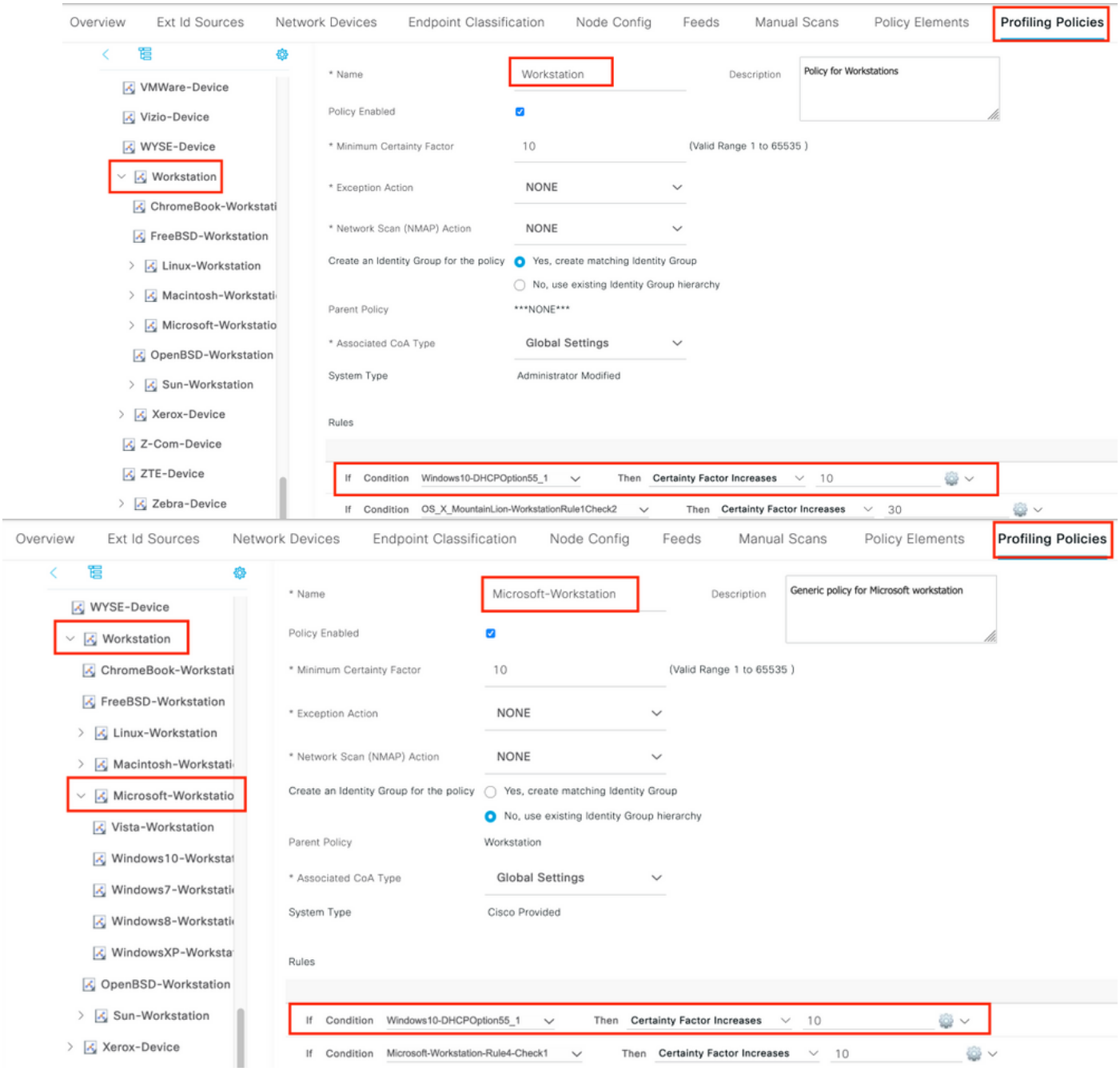
구성 섹션에서는 Windows 10 워크스테이션을 **Windows10-Workstation**에 일치시키기 위해 사용자 지정 프로파일링 조건을 사용하는 방법을 **보여 줍니다**.

구성

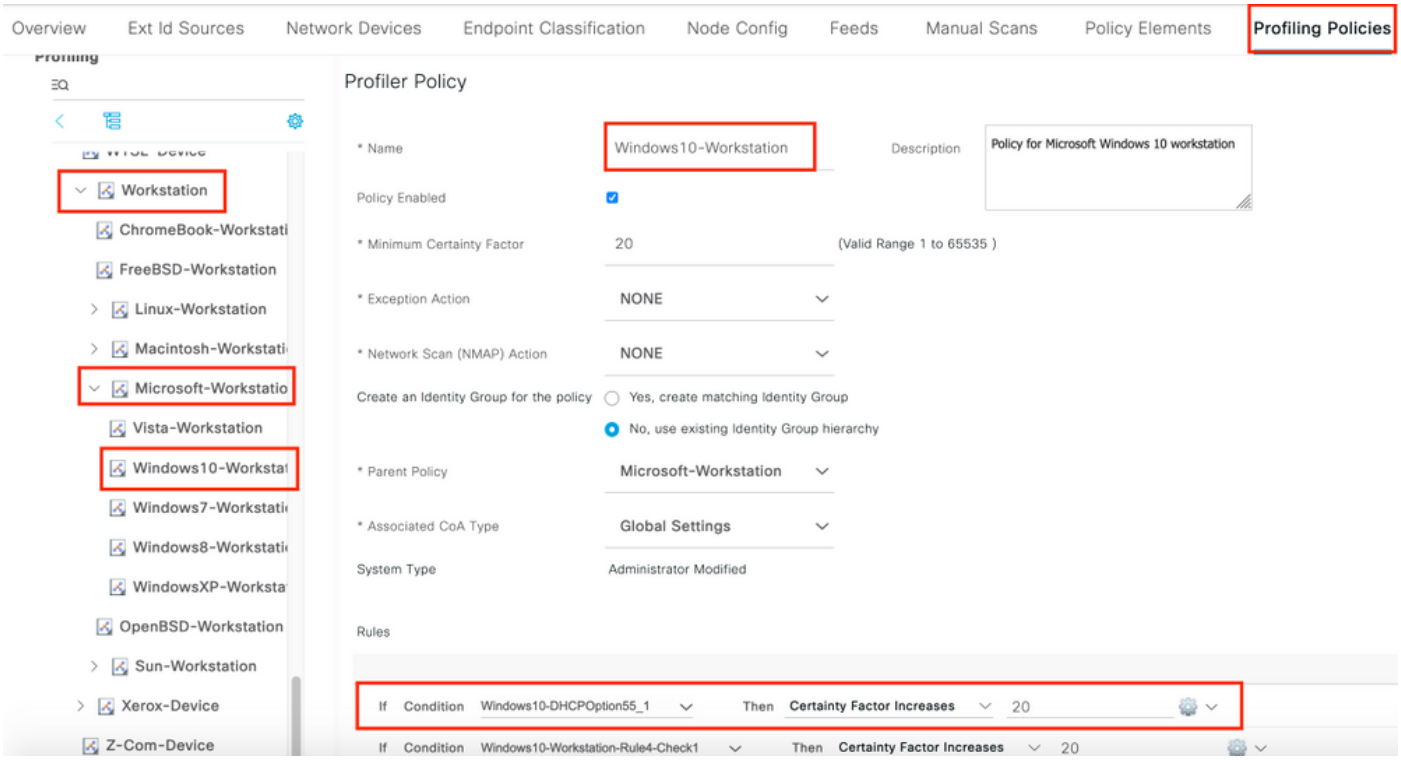
1. ISE 관리 GUI에 로그온하고 Policy(정책) **> Policy Elements(정책 요소) > Conditions(조건) > Profiling(프로파일링)으로 이동합니다**.새 사용자 지정 프로파일링 조건을 추가하려면 **Add**를 클릭합니다.이 예에서는 Windows 10 매개 변수 요청 목록 핑거프린트를 사용합니다.매개변수 **요청 목록** 값의 전체 목록은 Fingbank.org를 참조하십시오.
   참고:속성 **값** 텍스트 상자에 일부 숫자 옵션이 표시되지 않을 수 있으며 전체 목록을 보려면 마우스나 키보드를 사용하여 스크롤해야 할 수도 있습니다.



2. 사용자 지정 조건이 정의되면 현재 프로파일링 정책을 수정하거나 새 정책을 구성하기 위해 **Policy(정책) > Profiling(프로파일링) > Profiling Policies(프로파일링 정책)**로 이동합니다.이 예에서는 기본 **워크스테이션, Microsoft-Workstation, Windows10-Workstation** 정책이 새 매개변수 요청 목록 조건을 포함하도록 편집됩니다.아래와 같이 Workstation, **Microsoft-Workstation, Windows10-Workstation** 프로파일러 정책 규칙에 새 복합 조건을 추가합니다.원하는 **프로파일링** 결과를 얻으려면 필요한 만큼 확실성 요소를 수정합니다.


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
* 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-Workstat
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

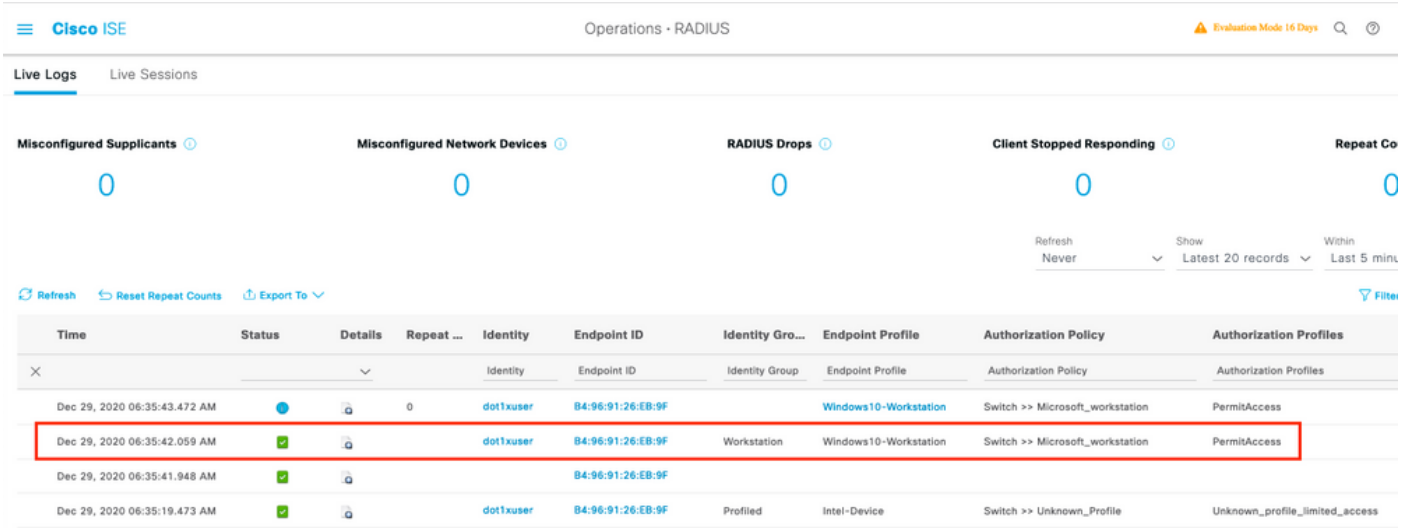


참고:이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

다음을 확인합니다.

1단계 -

ISE > Operations > Live Logs로 이동합니다.첫 번째 인증은 알 수 없는 권한 부여 정책과 일치하며 제한된 액세스는 ISE에 부여됩니다.디바이스가 프로파일링된 후 ISE는 CoA를 트리거하고 ISE에서 다른 인증 요청을 수신하고 새 프로파일(Windows10 Workstation)과 일치시킵니다.



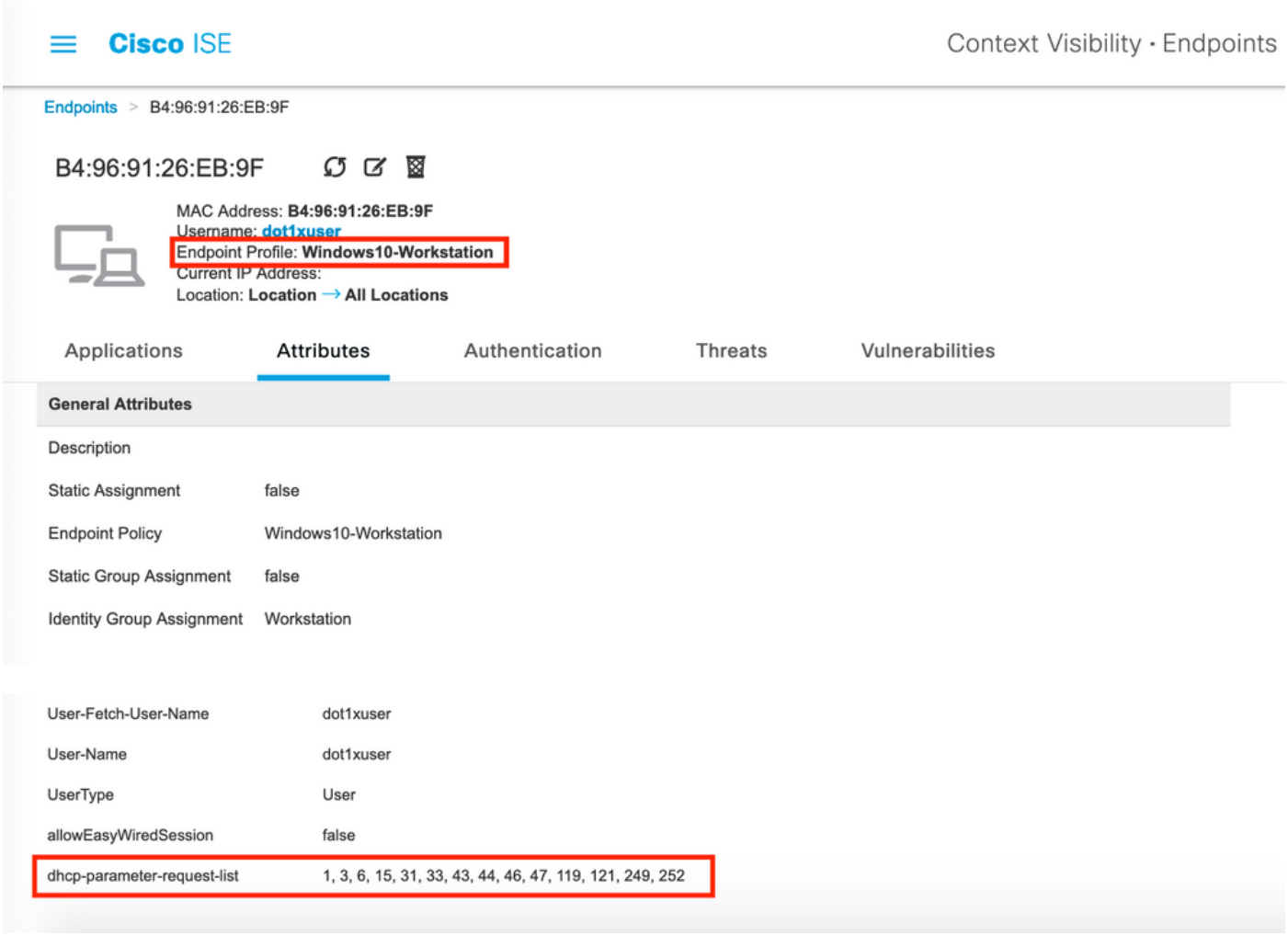
2단계 -

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

- Context Visibility(**상황 가시성) > Endpoints(엔드포인트)로 이동하여 엔드포인트를** 검색하고

Edit(수정)를 클릭합니다.

- EndPointPolicy가 **Window**10-Workstation이고 dhcp-parameter-**request-list** 값이 이전에 구성한 조건 값과 일치하는지 확인합니다.



문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

- DHCP 패킷이 프로파일링 기능(헬퍼 주소 또는 SPAN 사용)을 수행하는 ISE 정책 노드에 도달했는지 확인합니다.
- Operations(**운영) > Troubleshoot(문제 해결) > Diagnostic Tools(진단 도구) > General Tools(일반 툴) > TCP Dump(TCP 덤프** 툴)?ISE 관리 GUI에서 TCP 덤프 캡처를 기본적으로 실행하려면
- ISE PSN 노드에서 아래 디버깅 활성화 - -nsf-nsf 세션-light 세션 디렉터리-프로 파 일러-런타임 -AAA
- Profiler.log, prrt-server.log 및 lsd.log는 관련 정보를 표시합니다.
- 매개변수 요청 목록 옵션의 현재 목록은 Fingerbank.org DHCP 지문 데이터베이스를 참조하십시오.
- ISE 프로파일링 조건에서 올바른 매개변수 요청 목록 값이 구성되었는지 확인합니다.일반적으로 사용되는 문자열 중 일부는 다음과 같습니다.

참고:debug 명령을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

로그 분석

++ISE PSN 노드의 하위 디버깅 사용 -

-nsf

-nsf 세션

-light 세션 디렉터리

-프로 파 일러

-런타임-AAA

++초기 인증

++prrt-server.log

++ISE 노드에서 수신된 액세스 요청

RADIUS,2020-12-29 06:35:19,377,DEBUG,0x7f1cdcbd2700,cntx=001348461,sesn=isee30-primary/39791910/625,전화 id=B4-96-91-26-EB-9F,**RADIUS 패킷:코드=1(AccessRequest)** 식별자=182 길이=285

++ISE는 Unknown_profile과 일치

AcsLogs,2020-12-29 06:35:19,473,DEBUG,0x7f1cdc7ce700,cntx=001348476,sesn=isee30-primary/39779110/625,CPMS ID=0A6A270B0000018B44013AC,사용자=dot1xuser,CallingStationID=B4-96-91-26-EB-9F,AuthorizationPolicyMatchedRule=Unknown_Profile, EAP-Tunnel=EAP-EAP fast, EapAuthentication=EAP-MSCHAPv2, UserType=사용자, CPMSessionID=0A6A270B0000018B44013AC, EndPointMACAddress=B4-96-91-26-EB-26-EB-EB-EB ,

++ISE는 액세스 허용을 전송 액세스 제한

RADIUS,2020-12-29 06:35:19,474,DEBUG,0x7f1cdc7ce700,cntx=001348476,sesn=isee30-primary/397791910/625,CPMS5 0A6A270B0000018B44013AC,user=dot1xuser,CallingStationID=B4-96-91-26-EB-9F,RADIUS 패킷:**코드=2(AccessAccept)** 식별자=186 길이=331

++ISE가 DHCP 정보로 계정 업데이트를 받았습니다.

RADIUS,2020-12-29 06:35:41,464,DEBUG,0x7f1cdcad1700,cntx=001348601,sesn=isee30-primary/39791910/627,CPID=0A6A270B0000018B44013AC,CallingStationID=B4-96-91-26-EB-9F,RADIUS 패킷:**코드=4(AccountingRequest)** 식별자=45 길이=381

[1] 사용자 이름 - 값:[dot1xuser]

[87] NAS 포트 ID - 값:[기가비트 이더넷1/0/13]

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

[26] cisco av 쌍 - 값:[audit-session-id=**0A6A270B00000018B44013AC**]

++ISE는 어카운팅 응답을 다시 보냅니다.

RADIUS,2020-12-29 06:35:41,472,DEBUG,0x7f1cdc5cc700,cntx=001348601,sesn=isee30-primary/397791910/627,CPDM=ID 0A6A270B0000018B44013AC,user=dot1xuser,CallingStationID=B4-96-91-26-EB-9F,RADIUS 패킷:**코드=5(AccountingResponse)** 식별자=45 길이=20,RADIUSHandler.cpp:2216

++프로파일러.log

++Once Accounting Update is received with the DHCP option dhcp-parameter-request-list , ISE 디바이스 프로파일링 시작

2020-12-29 06:35:41,470 DEBUG [SyslogListenerThread][] cisco.profiler.radius.SyslogDefragmenter -:::::- **parseHeader inBuffer**=<18181>Dec06:35:41 isee330-primary CISE RADIUS_Accounting 000000655 2 0 2020-12-29 06:35:41.467 +00:00000234376 3002 알림 **Radius-계정:RADIUS 계정 관리 감시 업데이트**, ConfigVersionId=99, 장치 IP 주소=10.106.39.11, UserName=dot1xuser, RequestLatency=6, NetworkDeviceName=sw, User-Name=dot1xuser, NAS-IP-Address=10.106.39.11, NAS-Port=50113, Class=ACS:0A6A 0B00000018B44013AC:isee30-primary/39791910/625, Called-Station-ID=A0-EC-F9-3C-82-0D, Calling-Station-ID=B4-96-96 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=0000000000b, Acct-Authenticate-Input, Input=Acct-Remote, Acct-Input, Acct-Input, Input-Acct-Input, Acct-Input-Input, Acct-Acct-Acct-Input, Input-Input-Acct-Input, Acct-Acct-Input-Acct-Acct-Input, Acct-Input, Acct-Acct-Acct-Access-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\, 3\, 31\, 33\, 34\, 43\, 43\ \, 46\, 47\, 119\, 121\, 249\, 252, cisco-av-pair=audit-session-id=0A6A270B0000018B44013AC, cisco-av-pair=dot1x,

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

특성: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=0A6A70B000000000\ 118B44013AC, 메서드 =dot1x

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

2020-12-29 06:35:41,479 디버그 [RMQforwarder-4][] cisco.profiler.infrastructure.cache.AbstractEndpointCache -:B4:96:91:26:26:EB:9F:12413370-4-49a-17a-11eb 13-1a99022ed3c5:ProfilerCollection:- **이 Mac의 소유자:B4:96:91:26:EB:9F는 isee30-primary.anshsinh.local입니다.**

2020-12-29 06:35:41,479 디버그 [RMQforwarder-4][] cisco.profiler.infrastructure.probemgr.Forwarder -:B4:96:91:26:26:EB:9F:12413370-49-1-b1-31eb -1a99022ed3c5:ProfilerCollection:- **엔드포인트 B4:96:91:26:EB:9Fis30-primary.anshsinh.local 및 메시지 코드는 3002입니다.**

2020-12-29 06:35:41,479 디버그 [RMQforwarder-4][] cisco.profiler.infrastructure.probemgr.Forwarder -:B4:96:91:26:26:EB:9F:12413370-49-1-b1-31eb -

1a99022ed3c5:ProfilerCollection:- **엔드포인트 소스 radius true입니다.**

++새 특성

2020-12-29 06:35:41,480 디버그 [RMQforwarder-4][]
cisco.profiler.infrastructure.probemgr.Forwarder -:B4:96:91:26:26:EB:9F:12413370-49-1-b1eb-
1a99022ed3c5:ProfilerCollection:- **새 특성:dhcp-parameter-request-list**

2020-12-29 06:35:41,482 디버그 [RMQforwarder-4][]
cisco.profiler.infrastructure.probemgr.Forwarder -:B4:96:91:26:26:EB:9F:12413370-49-1-b1eb-
1a99022ed3c5:ProfilerCollection:- 엔드포인트가 속성 집합을 수정했습니다.

2020-12-29 06:35:41,482 디버그 [RMQforwarder-4][]
cisco.profiler.infrastructure.probemgr.Forwarder -:B4:96:91:26:26:EB:9F:12413370-49-1-b1eb -
1a99022ed3c5:**ProfilerCollection:- dhcp-parameter-request-list,**

++서로 다른 규칙이 서로 다른 확실성 요소와 일치함

2020-12-29 06:35:41,484 디버그 [RMQforwarder-4][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:26:EB:9F:12413370-49-11eb 3-
1a99022ed3c5:**프로파일링:- 정책 Intel-Device 매칭 B4:96:91:26:EB:9F(확실성 5)**

2020-12-29 06:35:41,485 디버그 [RMQforwarder-4][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:26:EB:9F:12413370-49-11eb 3-
1a99022ed3c5:**프로파일링:- 정책 워크스테이션이 B4:96:91:26:EB:9F(확실성 10)와 일치함**

2020-12-29 06:35:41,486 디버그 [RMQforwarder-4][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:26:EB:9F:12413370-49-11eb 3-
1a99022ed3c5:**프로파일링:- 정책 Microsoft-Workstation 매칭 B4:96:91:26:EB:9F(확실성 10)**

2020-12-29 06:35:41,487 디버그 [RMQforwarder-4][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:26:EB:9F:12413370-49-11eb 3-
1a99022ed3c5:**프로파일링:- 정책 Windows10-워크스테이션이 B4:96:91:26:EB:9F(확실성 20)**

++Windows10-Workstation은 구성에 따라 40의 확실성 수준이 가장 높으므로 디바이스의 엔드포인트 프로필로 선택합니다.

2020-12-29 06:35:41,487 디버그 [RMQforwarder-4][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:26:EB:9F:12413370-49-11eb 3-
1a99022ed3c5:프로파일링:- **정책 계층 구조 분석 후:엔드포인트:B4:96:91:26:EB:9F 엔드포인트 정책:Windows10-Workstation for:40 ExceptionRuleMatched:false**

2020-12-29 06:35:41,487 디버그 [RMQforwarder-4][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:26:EB:9F:12413370-49-11eb 3-
1a99022ed3c5:**프로파일링:- 엔드포인트 B4:96:91:26:EB:9F 일치하는 정책이 변경되었습니다.**

2020-12-29 06:35:41,489 디버그 [RMQforwarder-4][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:26:EB:9F:12413370-49-11eb 3-
1a99022ed3c5:**프로파일링:- 엔드포인트 B4:96:91:26:EB:9F IdentityGroup 변경됨**

2020-12-29 06:35:41,489 디버그 [RMQforwarder-4][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:26:EB:9F:12413370-49-11eb 3-
1a99022ed3c5:**프로파일링:- 엔드포인트 B4:96:91:26:EB:9F - 3b76f840-8c00-11e6-996c-**

525400b485211

2020-12-29 06:35:41,489 디버그 [RMQforwarder-4][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:26:EB:9F:12413370-49-11eb 3-1a99022ed3c5:프로파일링:- **프로파일링된 엔드포인트 B4:96:91:26:EB:9F, 정책 Windows10-Workstation, 일치하는 정책 Windows10-Workstation을 사용하여 엔드포인트 캐시를 호출하는 중입니다.**

2020-12-29 06:35:41,489 디버그 [RMQforwarder-4][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:26:EB:9F:12413370-49-11eb 3-1a99022ed3c5:**프로파일링:- 엔드포인트 B4:96:91:26:EB:9F 및 ep 메시지 코드 = 3002로 지속하는 이벤트를 보냅니다.**

2020-12-29 06:35:41,489 디버그 [RMQforwarder-4][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:26:EB:9F:12413370-49-11eb 3-1a99022ed3c5:**프로파일링:- 엔드포인트 B4:96:91:26:EB:9F IdentityGroup/논리적 프로파일이 변경되었습니다.조건부 CoA 발급**

2020-12-29 06:35:41,489 디버그 [RMQforwarder-4][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:26:EB:9F:12413370-49-11eb 3-1a99022ed3c5:프로파일링:- **엔드포인트 세부사항이 포함된 ConditionalCoAEvent:EndPoint[id=ff19ca00-499f-11eb-b713-1a99022ed3c5,name=<null>]**

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

속성:Calling-Station-ID 값:B4-96-91-26-EB-9F

특성:EndPointMACAddress 값:B4-96-91-26-EB-9F

속성:MACAddress 값:B4:96:91:26:EB:9F

++Lightweight Session Directory로 데이터 전송

2020-12-29 06:35:41,489 DEBUG [RMQforwarder-4][]
cisco.profiler.infrastructure.probemgr.**LSDForwarderHelper** -:::::::::- 엔드포인트 .B4:96:91:26:EB:EB:9F **Windows0-Workstation**

2020-12-29 06:35:41,489 DEBUG [RMQforwarder-4][]
cisco.profiler.infrastructure.probemgr.LSDForwarderHelper -:::::::- LSDfor defaultruus,defaultus,B4:96:96:21:26:222:EB 9F

++글로벌 CoA가 재인증으로 선택됨

2020-12-29 06:35:41,489 디버그 [CoAhandler-52-thread-1][]
cisco.profiler.infrastructure.profiling.CoAhandler -:B4:96:91:26:26:EB:9F:9fe38b-30-43eb-13eb -b713-1a99022ed3c5:**ProfilerCoA:- 구성된 전역 CoA 명령 유형 = Reauth**

2020-12-29 06:35:41,490 디버그 [RMQforwarder-4][]
cisco.profiler.infrastructure.cache.AbstractEndpointCache -:B4:96:91:26:26:EB:9F:12413370-49-a-17a-11eb 13-1a99022ed3c5::- **수신 엔드포인트 업데이트 중 - EP:B4:96:91:26:EB:9FepSource:RADIUS 프로브 SGA:falseSG:워크스테이션**

2020-12-29 06:35:41,490 디버그 [RMQforwarder-4][]

cisco.profiler.infrastructure.cache.AbstractEndpointCache -:B4:96:91:26:26:EB:9F:12413370-49-a-17a-11eb 13-1a99022ed3c5::- **병합 후 엔드포인트 업데이트 - EP:B4:96:91:26:EB:9FepSource:RADIUS 프로브 SGA:falseSG:Windows10-Workstation**

++ISE는 정책을 매칭하여 CoA를 전송해야 하는지 확인합니다.ISE는 프로필 변경과 일치하는 정책이 있는 경우에만 CoA를 트리거합니다.

2020-12-29 06:35:41,701 디버그 [CoAhandler-52-thread-1][] cisco.profiler.infrastructure.profiling.CoAhandler -:B4:96:91:26:26:EB:9F:9fe330-43b-ea-11eb 713-1a99022ed3c5:**ProfilerCoA:- 로컬 예외 정책세트 스위치에서 사용 가능한 모든 정책을 처리합니다. policystatus=ENABLED**

2020-12-29 06:35:41,701 디버그 [CoAhandler-52-thread-1][] cisco.profiler.infrastructure.profiling.CoAhandler -:B4:96:91:26:26:EB:9F:9fe38b-30-43eb-13eb - b713-1a99022ed3c5:**ProfilerCoA:- 정책 이름:스위치 정책 상태:사용**

2020-12-29 06:35:41,702 디버그 [CoAhandler-52-thread-1][] cisco.profiler.infrastructure.profiling.CoAhandler -:B4:96:91:26:26:EB:9F:9fe38b-30-43eb-13eb - b713-1a99022ed3c5:**ProfilerCoA:- lhsvalue name 6d954800-8bff-11e6-996c-525400b48521 rhs operandID 427060690-c0-8c-11e6-996c-525400b48521 rhvaluename 워크스테이션:Microsoft-Workstation:Windows10-Workstation**

2020-12-29 06:35:41,933 디버그 [CoAhandler-52-thread-1][] com.cisco.profiler.api.util - :B4:96:91:26:EB:9F:9fe38b38b-43ea-11eb 3-1a99022ed3c5:**ProfilerCoA: - 권한 부여 정책에서 사용 가능한 지정된 조건**

2020-12-29 06:35:41,933 디버그 [CoAhandler-52-thread-1][] com.cisco.profiler.api.util - :B4:96:91:26:EB:9F:9fe38b38b-43ea-11eb 3-1a99022ed3c5:**ProfilerCoA:- 권한 부여 정책 HAVING 정책:4270690-8c00-11e6-996c-525400b48521**

++권한 부여 정책이 이 조건과 일치하고 CoA가 트리거됩니다.

2020-12-29 06:35:41,935 디버그 [CoAhandler-52-thread-1][] cisco.profiler.infrastructure.profiling.CoAhandler -:B4:96:91:26:26:EB:9F:9fe38b-30-43eb-13eb - b713-1a99022ed3c5:**ProfilerCoA:- applyCoa:엔드포인트 RADIUS 특성을 기반으로 만든 설명자:**

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

세션 ID:[0A6A270B00000018B44013AC]

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

AAA 인터페이스:[10.106.32.119]

NAD IP 주소:[10.106.39.11]

NAS 포트 ID:[기가비트 이더넷1/0/13]

NAS 포트 유형:[이더넷]

서비스 유형:[프레임]

무선:[거짓]

VPN 여부:[거짓]

MAB 여부:[거짓]

2020-12-29 06:35:41,938 디버그 [CoAhandler-52-thread-1][]
cisco.profiler.infrastructure.profiling.CoAhandler -:B4:96:91:26:26:EB:9F:9fe38b-30-43eb-13eb-b713-1a99022ed3c5:**ProfilerCoA:- CoA에 대한 및 IP를 호출하려고 합니다.엔드포인트 10.106.39.11:B4:96:91:26:EB:9F CoA 명령:재인증**

2020-12-29 06:35:41,938 디버그 [CoAhandler-52-thread-1][]
cisco.profiler.infrastructure.profiling.CoAhandler -:B4:96:91:26:26:EB:9F:9fe38b-30-43eb-13eb-b713-1a99022ed3c5:**ProfilerCoA:- AAA 서버에서 CoA-REAUTH 적용:10.106.32.119을 통한 인터페이스:10.106.32.119 - 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_Authered_Authentications 00000656 2 1 StepData=2=(포트 = 1700 \, type = Cisco CoA), CoASourceComponent**=Profiler, CoAReason=권한 부여 정책에서 사용되는 엔드포인트 ID 그룹/정책/논리 프로필 변경, CoAType=Reauthentication** - 마지막, 네트워크 장치 프로파일=Cisco

++prrt-server.log

AcsLogs,2020-12-29 06:35:41,938,DEBUG,0x7f1c6ffcb700,cntx=001348611,Log_Message=[2020-12-29 06:35:41.900:00 0000234379 80006 **정보 프로파일러:프로파일러가 권한 부여 요청 변경 사항**을 트리거하고 있습니다. ConfigVersionId=99, EndpointCoA=**Reauth,** EndpointMacAddress=B4:96:91:26:EB:9F, EndpointADAddress=10.106.39.11, EndpointPolicy=Windows10-Workstation, EndpointProperty=Framed-Service,MessageCode=3002\,EndPointPolicyID=42706690-8c00-11e6-996c-525400b48521\,UseCase=\,NAS-Port-Id=GigabitEthernet1/0/13\-Type=이더넷\,응답=\{사용자 이름=dot1xuser\;

DynamicAuthorizationFlow,2020-12-29 06:35:41,939,DEBUG,0x7f1cdc3ca700,cntx=001348614,[DynamicAuthorizationFlow::onLocalHttpEvent] 수신 CoA 명령:

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

<세션 서버 주소="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=0A6A270B0000018B44013AC</identifierAttribute>**

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

</session>

</reauthenticate>

++CoA 전송 -

RadiusClient,2020-12-29 06:35:41,943,DEBUG,0x7f1ccb3f3700,cntx=001348614,sesn=39c7408-52fd-430f-95fe9-8d9-95d9 8eaa1f1,CallingStationID=B4:96:91:26:EB:9F, RADIUS 패킷:**코드=43(CoARequest)** 식별자=27 길이=225

[4] NAS-IP-주소 - 값:[10.106.39.11]

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

[87] NAS 포트 ID - 값:[기가비트 이더넷1/0/13]

[26] cisco av 쌍 - 값:[가입자:명령=재인증]

[26] cisco av 쌍 - 값:[audit-session-id=0A6A270B00000018B44013AC]

RadiusClient,2020-12-29 06:35:41,947,DEBUG,0x7f1cdcad1700,cntx=001348614,sesn=39c7408-52fd-430f-95fe9-a8fe9 8eaa1f1,CallingStationID=B4:96:91:26:EB:9F, RADIUS 패킷:**코드=44(CoACK)** 식별자=27

++새 액세스 요청

Radius,2020-12-29 06:35:41,970,DEBUG,0x7f1cdc6cd700,cntx=001348621,sesn=isee30-primary/39791910/628,CallingStationID b4-96-91-26-EB-9F,RADIUS 패킷:**코드=1(AccessRequest)** 식별자=187 길이=285

++ISE는 엔드포인트 디바이스의 엔드포인트 정책과 일치하는 새 권한 부여 프로파일을 매칭합니다 .

AcsLogs,2020-12-29 06:35:42,060,DEBUG,0x7f1cdcad1700,cntx=001348636,sesn=isee30-primary/3977919110/628 SessionID=0A6A270B0000018B44013AC,user=dot1xuser,CallingStationID=B4-96-91-26-EB-9FI-9ENTITYPolicyMatCHEDDefault, **AuthorIZATIONPolicyRule=MatCHEDRule MICROSOFT_WORKSTATION,** EapTunNEL=EAP-FAST, EapAuthentication=EAP-MSCHAPv2, UserType=사용자, CPMSessionID=0A6A270B000018B440013AC, EndPointMACA4-Dddress=B9-91-26-EB-9F, PostureAssessmentStatus=NotApplicable, **EndPointMatchedProfile=Windows10-Workstation,**

++액세스 수락이 전송됨 -

RADIUS,2020-12-29 06:35:42,061,DEBUG,0x7f1cdcad1700,cntx=001348636,sesn=isee30-primary/39791910/628,CPID=0A6A270B0000018B44013AC,user=dot1xuser,CallingStationID=B4-96-91-26-EB-9F,RADIUS 패킷:**코드=2(AccessAccept)** 식별자=191 길이=340

관련 정보

- Fingbank.org DHCP 지문 데이터베이스
- 기술 지원 및 문서 – Cisco Systems