

用于分析终端的DHCP参数请求列表选项55配置示例

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[验证](#)

[故障排除](#)

[日志分析](#)

[相关信息](#)

简介

本文档介绍使用DHCP参数请求列表选项55作为配置使用身份服务引擎(ISE)的设备的替代方法。

先决条件

要求

Cisco 建议您：

- DHCP发现过程的基本知识
- 使用ISE配置自定义分析规则的经验

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ISE版本3.0
- Windows 10

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

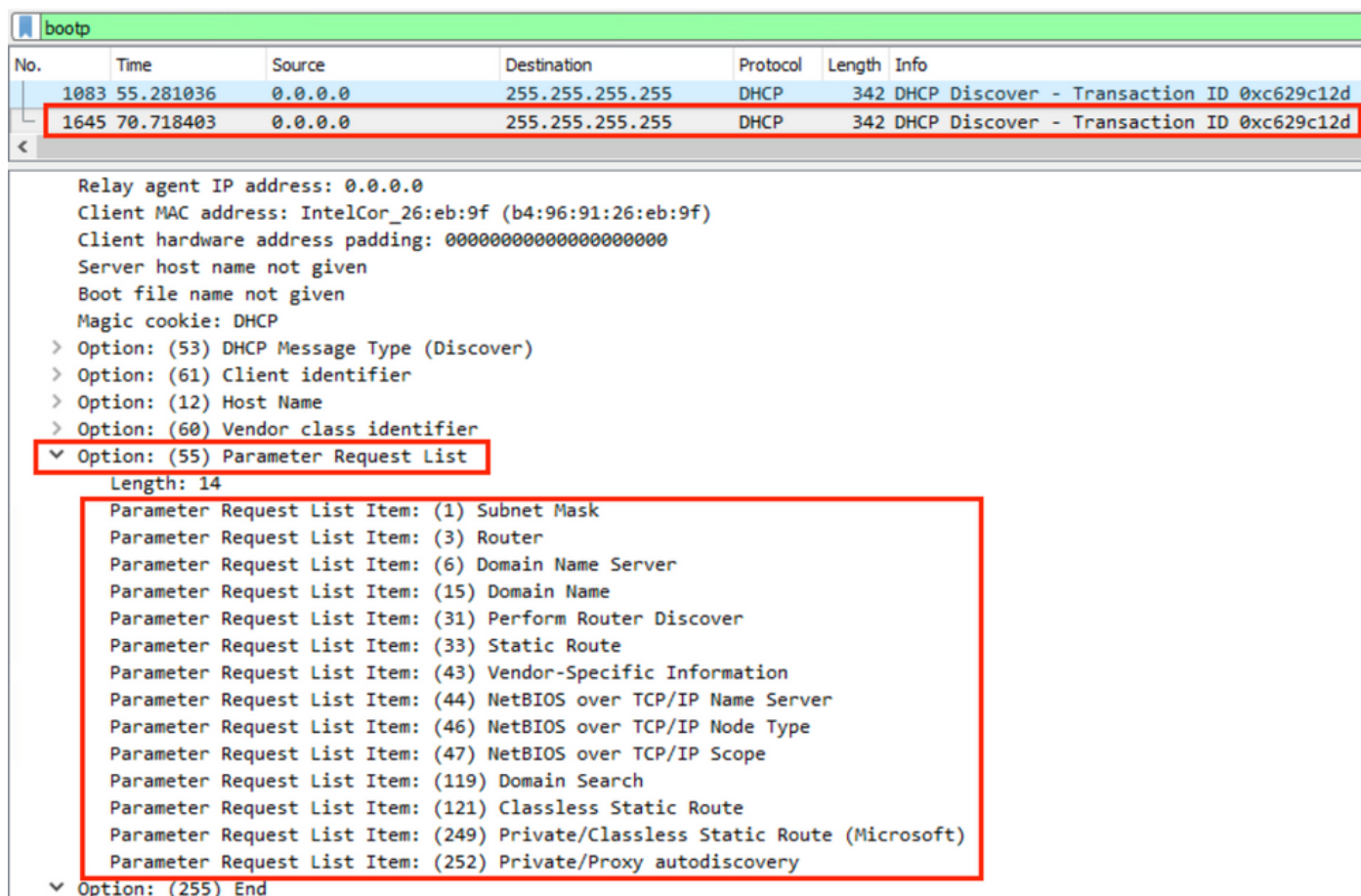
在生产ISE部署中，一些更常部署的分析探测功能包括RADIUS、HTTP和DHCP。由于URL重定向在ISE工作流的中心，HTTP探测功能被广泛使用，以从用户代理字符串捕获重要终端数据。但是，在某些生产使用案例中，不需要URL重定向，而且首选Dot1x，这使得更难准确分析终端。例如，连接到企业服务集标识符(SSID)的员工PC获得完全访问权，而其个人iDevice(iPhone、iPad、

iPod)仅获得互联网访问权。在这两种情况下，用户都会被分析并动态映射到一个更具体的身份组，以进行授权配置文件匹配，而不依赖用户打开Web浏览器。另一个常用的替代方法是主机名匹配。此解决方案不完美，因为用户可能将终端主机名更改为非标准值。

在这些情况下，DHCP探测功能和DHCP参数请求列表选项55可用作配置这些设备的替代方法。DHCP数据包中的“参数请求列表”字段可用于为终端操作系统(如入侵防御系统(IPS)使用签名来匹配数据包)指纹。当终端操作系统在线路上发送DHCP发现或请求数据包时，制造商会包括其打算从DHCP服务器(默认路由器、域名服务器(DNS)、TFTP服务器等)接收的DHCP选项的数字列表。DHCP客户端从服务器请求这些选项的顺序非常独特，可用于为特定源操作系统指纹。“参数请求列表”选项的使用不像HTTP用户代理字符串那样精确，但是，它比主机名和其他静态定义数据的使用受到的控制要多得多。

注意：DHCP参数请求列表选项不是完美的解决方案，因为它生成的数据取决于供应商，并且可以由多种设备类型复制。

在配置ISE分析规则之前，请在ISE上使用终端/交换端口分析器(SPAN)或传输控制协议(TCP)转储捕获的Wireshark捕获，以评估DHCP数据包中的参数请求列表选项(如果存在)。此示例捕获显示Windows 10的DHCP参数请求列表选项。



The image shows a Wireshark packet capture window titled "bootp". It displays two DHCP Discover packets. The second packet is selected and its details are expanded. The details pane 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 (highlighted with a red box)
 - 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

结果的“参数请求列表”字符串以逗号分隔格式写入：1、3、6、15、31、33、43、44、46、47、119、121、249、252。在ISE中配置自定义分析条件时使用此格式。

配置部分演示了使用自定义分析条件将Windows 10工作站与Windows 10工作站进行匹配。

配置

1. 登录ISE管理GUI并导航至Policy > Policy Elements > Conditions > Profiling。单击Add以添加新的自定义分析条件。在本示例中，我们使用Windows 10参数请求列表指纹。有关“参数请求列表”值的完整列表，请参阅Fingerbank.org。

注意：属性值文本框可能不显示所有数字选项，您可能需要用鼠标或键盘滚动才能查看完整列表。

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. 定义自定义条件后，导航到Policy > Profiling > Profiling Policies以修改当前分析策略或配置新策略。在本示例中，编辑默认的工作站、Microsoft-Workstation、Windows10-Workstation策略，以包括新的参数请求列表条件。向工作站、Microsoft-Workstation、Windows10-Workstation分析器策略规则添加新的复合条件，如下所示。根据需要修改“确定系数”，以获得所需的分析结果。

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

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

注意：使用[命令查找工具](#)（仅限注册用户）可获取有关本部分所使用命令的详细信息。

验证

步骤 1-

导航至ISE > Operations > Live Logs。第1个身份验证与未知授权策略匹配，并向ISE提供有限访问权限。分析设备后，ISE触发CoA，在ISE上收到另一个身份验证请求并匹配新配置文件——Windows10工作站。

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

步骤 2-

使用本部分可确认配置能否正常运行。

- 导航至 **Context Visibility > Endpoints**，搜索终端，单击编辑。
- 确认 **EndPointPolicy** 是 **Window10-Workstation**，并且 **dhcp-parameter-request-list** 值与之前配置的条件值匹配。

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

故障排除

本节提供可用于排除配置故障的信息。

- 验证DHCP数据包已到达执行分析功能的ISE策略节点（使用帮助地址或SPAN）。
- 使用 **Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump** 工具？从ISE管理GUI本地运行TCP转储捕获。
- 在ISE PSN节点上启用以下调试 — -nsf-nsf-session— 轻量会话目录-profiler-runtime-AAA
- Profiler.log、prrt-server.log和Isd.log显示相关信息。
- 有关“参数请求列表”选项的当前列表，请参阅Fingerbank.org DHCP指纹数据库。
- 确保在ISE分析条件中配置了正确的参数请求列表值。一些更常用的字符串包括：

注意：使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

日志分析

++在ISE PSN节点上启用以下调试 —

-nsf

-nsf-session

— 轻量会话目录

-profiler

-runtime-AAA

++初始身份验证

++prrt-server.log

++在ISE节点上收到的访问请求

Radius , 2020-12-29 06:35:19,377,DEBUG , 0x7f1cdbc700,cntx=0001348461,sesn=isee30-primary/397791910/625,CallingStationID=B4-96-91-26-EB-9F,**RADIUS数据包**
: **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-9F,**AuthorizationPolicyMatchedRule=Unknown_Profile**, EapTunnel=EAP-FAST , EapAuthentication=EAP-MSCHAPv2,UserType=User , CPMSID=0A6A270B00000018B44013AC , EndPointMACAddress=B4-96-91-26-EB-9F,

++ISE发送访问接受，限制访问

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数据包** : **Code=2(AccessAccept)Identifier=186 Length=331**

++ISE收到包含DHCP信息的记帐更新

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

[1]用户名 — 值 : [dot1xuser]

[87] NAS-Port-Id — 值 : [千兆以太网1/0/13]

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

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

++ISE发回记帐响应

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

++Profiler.log

++收到记帐更新后 , DHCP选项dhcp-parameter-request-list (DHCP选项) , ISE开始分析设备

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 2020-12-29 0 06:35:41 .467 +00:00 0000234376 3002通知Radius-Accounting:RADIUS记帐监视器更新,**
ConfigVersionId=99 , 设备IP地址=10.106.39.11 , 用户名=dot1xuser , 请求延迟=6 , 网络设备名称=软件 , 用户名=dot1xuser , NAS-IP — 地址=10.106.39.11, NAS-Port=50113,
Class=CACS:0A6A270B00000018B44013AC:isee30-primary/397791910/625, Called-Station-ID=A0-EC-F9-3C-82-0D , Calling-Station-ID=B4-96-91-26-EB-9F, NAS-Identifier=Switch , acct-Status-Type=Interim-Update , acct-Delay-Time=0, acct-Input-octets=174, acct-output-octets=0, act , act-act-act , act-act会话ID=0000000b , Acct-authentic=Remote , Acct-Input-Packets=1, Acct-Output-Packets=0, Event-Timestamp=1609341899, NAS-Port-Id=GigabitEthernet1/0/13, **cisco-av-pair=dhcp-option=parameter-request-list=lister=list1\、 3\、 6\、 15\、 31\、 33\、 43\、 44\、 46\、 47\、 119\、 121\、 249\、 252, cisco-av-pair=audit-session-id=0A6A270B00000018B44013AC , cisco-av-pair=method=dot1x ,**

2020-12-29 06:35:41,471 DEBUG [RADIUSParser-1-thread-2]]
cisco.profiler.probes.radius.RadiusParser -::: — **已解析IOS传感器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\, 44\, 46\, 47\, 119\, 121\, 249\, 252, audit-session-id=0A6A270B00000018B44013AC , 方法=dot1x

属性 : dhcp-parameter-request-list值 : 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:-所有者对于此Mac: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: — 终端的当前所有者B4:96:91:26:EB:9F是ise30-primary.anshsinh.local和消息代码为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:Profiler收集: — 是终端源真

++新属性

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:ProfilerCollection: — 终端已修改但已设置属性:

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:---parameter-request列表**,

++不同的规则与不同的确定性因素匹配

2020-12-29 06:35:41,484调试[RMQforwarder-4[]]
cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:分析: — **策略Intel-Device匹配B4:96:91:26:EB:9F (确定性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:分析: — **策略工作站匹配B4:96:91:26:EB:9F (确定性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:分析: — **策略Microsoft — 工作站B4:96:91:26:EB:9F (确定性10)**

2020-12-29 06:35:41,487调试[RMQforwarder-4[]]
cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:分析: — **策略Windows10工作站与B4:96:91:26:EB:9F匹配 (确定性20)**

++Windows10-Workstation根据配置具有最高的确定系数40, 因此它选择作为设备的终端配置文件

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:分析策略层次结构后: **终端: B4:96:91:26:EB:9F**
EndpointPolicy:Windows10-Workstation for:40 ExceptionRuleMatched:false

2020-12-29 06:35:41,487调试[RMQforwarder-4[]]
cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:分析: — **终端B4:96:91:26:ENDPOINTEB:9F匹配策略已更改。**

2020-12-29 06:35:41,489调试[RMQforwarder-4[]]

cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:分析 : — 终端B4:96:91:26:eb:9F IdentityGroup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: — 设置身份组IN终端B4:96:91:26:EB:9F - 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:- 调用终端缓存点B4:96:91:26:EB:9F , 策略Windows10-Workstation , 匹配策略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: — 将事件发送到永久端点b4:96:91:26:EB:9F和ep消息代码= 3002

2020-12-29 06:35:41,489调试[RMQforwarder-4][[]

cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:分析 : — 终端B4:96:91:26:eb:9F身份组/逻辑配置文件已更改。发出条件CoA

2020-12-29 06:35:41,489调试[RMQforwarder-4][[]

cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5 : 分析 : - ConditionCoAE包含终端详细信息的事件 : EndPoint[id=ff19ca00-499f-11eb-b713-1a99022ed3c5,name=<null>]

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

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

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

属性 : MAC地址值 : B4:96:91:26:EB:9F

++将数据发送到轻量会话目录

2020-12-29 06:35:41,489 DEBUG [RMQforwarder-4][[]

cisco.profiler.infrastructure.probemgr.LSDForwarderHelper -:::- Endpoint.B4:96:91:26:EB:9F与Windows10-Workstation匹配

2020-12-29 06:35:41,489 DEBUG [RMQforwarder-4][[]

cisco.profiler.infrastructure.probemgr.LSDForwarderHelper -::: — 发送事件以在转发器、defaultradius、defaultad B4:96:91:26:EB:9F添加LSD终端

++全局CoA被选为Reauth

2020-12-29 06:35:41,489调试[CoAHandler-52-thread-1][[]

cisco.profiler.infrastructure.profiling.CoAHandler -:B4:96:91:26:EB:9F:9fe38b30-43ea-11eb-b713-1a99022 ed3c5:ProfilerCoA: — 已配置全局CoA命令类型= Reauth

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

cisco.profiler.infrastructure.cache.AbstractEndpointCache -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5::- 更新终端 — EP来自传入 : B4:96:91:26:EB:9FepSource:RADIUS探测

SGA:falseSG:工作站

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

cisco.profiler.infrastructure.cache.AbstractEndpointCache -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:- 更新终端 — EP合并后 : B4:96:91:26:EB:9FepSource:RADIUS探测
SGA:falseSG:Windows10-Workstation

++ISE匹配策略以检查是否需要发送CoA。ISE仅在CoA具有与配置文件更改匹配的任何策略时才会触发

2020-12-29 06:35:41,701调试[CoAHandler-52-thread-1][

cisco.profiler.infrastructure.profiling.CoAHandler -:B4:96:91:26:EB:9F:9fe38b30-43ea-11eb-b713-1a99022Ed3c5:ProfilerCoA: — 处理本地异常策略集交换机中的所有可用策略
, policystatus=ENABLED

2020-12-29 06:35:41,701调试[CoAHandler-52-thread-1][

cisco.profiler.infrastructure.profiling.CoAHandler -:B4:96:91:26:EB:9F:9fe38b30-43ea-11eb-b713-1a99022 ed3c5:ProfilerCoA:-策略名称 : 交换机策略状态 : 启用

2020-12-29 06:35:41,702调试[CoAHandler-52-thread-1][

cisco.profiler.infrastructure.profiling.CoAHandler -:B4:96:91:26:EB:9F:9fe38b30-43ea-11eb-b713-1a99022 ed3c5:ProfilerCoA:- lhsvalue name 6d954800-8bff-11e6-996c-525400b48521 rhsID
42706690-8c00-11e6-996c-525400b48521 rhsvalue工作站 : Microsoft-Workstation:Windows10工
作站

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: — 授权策略中可用的
指定条件

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: — 授权策略
HAVING策略 : 42706690-8c00-11e6-996c-525400b48521

++授权策略匹配此条件 , 并触发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-11eb-b713-1a99022 ed3c5:ProfilerCoA:- applyCoa:根据终端RADIUS属性创建描述符 :

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

会话 ID:[0A6A270B00000018B44013AC]

AAA 服务器:[isee30-primary] IP:[10.106.32.119]

AAA接口 : [10.106.32.119]

NAD IP地址 : [10.106.39.11]

NAS端口ID:[千兆以太网1/0/13]

NAS端口类型 : [以太网]

服务类型 : [帧]

是无线 : [false]

是VPN:[false]

是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-b713-1a99022 ed3c5:ProfilerCoA: — 将要为和IP调用CoA:10.106.39.11 (适用于终端) : B4:96:91:26:EB:9F CoA命令 : 重新授权

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-b713-1a99022 ed3c5:ProfilerCoA: — 通过AAA服务器应用CoA-REAUTH:10.106.32.119 (通过接口) : 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_Passe_Asse_Ad_Ad_Authenticationse0000000656 2 1 Stada=2 1 Ste=2 Data=2=2=2(port=2=2=2(p)= 1700 \ , 类型= Cisco CoA), CoASourceComponent=Profiler , CoAReason=在授权策略中使用的终端身份组/策略/逻辑配置文件中的更改 , CoAType=Reauthentication — 最后 , 网络设备配置文件=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 80006INFO Profiler:分析器正在触发授权请求更改 , 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\,EndPointPolicyID=42706690-8c00-11e6-996c-525400b48521\,UseCase=\,NAS-Caseport-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]已接收传入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已发送 —

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数据包 : 代码=43(CoARequest)标识符=27长度=225

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

[31]呼叫站ID — 值 : [B4:96:91:26:EB:9F]

[87] NAS-Port-Id — 值 : [千兆以太网1/0/13]

[26] cisco-av-pair — 值 : [用户 : 命令=重新验证]

[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数据包 : 代码=44(CoAACK)标识符=27

++新访问请求

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数据包 : Code=1(AccessRequest)Identifier=187 Length=285

++ISE匹配与终端设备的终端策略匹配的新授权配置文件

AcsLogs , 2020-12-29 06:35:42,060,DEBUG , 0x7f1cdcad1700,cntx=0001348636,sesn=isee30-primary/397791910/628,CPMSessionID=0A6A270B00000018B44013AC , 用户=dot1xuser , CallingStationID=B4-96-91-26-EB-9FIdentityPolicyMatchedRule=Default , AuthorizationPolicyMatchedRule=Microsoft_workstation , EapTunnel=EAP-FAST , EapAuthentication=EAP-MSCHAPv2,UserType=User , CPPMSESSIONID=0A6A270B00000018B44013AC、EndPointMACAddress=B4-96-91-26-EB-9F、PostureAssessmentStatus=NotApplicable、EndPointMatchedProfile=Windows10-Workstation、

++接入已发送 —

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数据包 : Code=2(AccessAccept)Identifier=191 Length=340

相关信息

- [Fingerbank.org DHCP指纹数据库](#)
- [技术支持和文档 - Cisco Systems](#)