

55 مقر DHCP تاملعم تابلط ئامئاق رايخ طاقن نيوكت لاثم فيرعت فلم مدخلت سمل اهنا

تاي وتحمل

قىدمىلا

قىس اس الاتابلى تاملى

تابلى تاملى

قىدمىلا تانوكىملا

قىس اس اتامولعم

نيوكتلا

قىصلانم قىچتلا

اھالص او عاطخ الافاش كتسا

لچسلا لىلحت

قلص تاذ تامولعم

قىدمىلا

ةلىد ب قىيرطك 55 DHCP تاملعم تابلط ئامئاق رايخ مادختسى دنتسمل اذه فصىي ئي وهلا تامدوكىم مدخلت سىت يىتل ازه جالا فىي صوت (ISE).

قىس اس الاتابلى تاملى

تابلى تاملى

كىدىل نوكىي نأب Cisco يىصوت:

- DHCP فاشتكا قىلمع ب قىس اس اتامولعم
- ئاصىخمل افىرعتلا تافلم دعاوچ نيوكتلا ISE رايعد مادختسى ئىبرجت

قىدمىلا تانوكىملا

ةيلاتلا ئي داملا تانوكىمل او جماربلا تارادصى إل دنتسمل اذه يىف ئىراولى تامولعملا دنتسست:

- ISE 3.0 رادصى إل
- Windows 10 ليغشتلا ماظن

ةصالخ ئىلمع م ئىپ يىف ئىدوچوملا ازه جالا نم دنتسمل اذه يىف ئىراولى تامولعملا ئاشن امىت تناك اذا. (يىضارت فا) حوسىم نيوكتلا دنتسمل اذه يىف ئامىل ئامولعملا ئاشن امىت تأدب رمأ يىأ لىمتحمل ارى ثأتللى كەمەف نم دكأت ف، ئوشابم كتكمىش.

قىس اس اتامولعم

اهشن مت يتل اتافلمل اصحف تايىلمع ضعب نممضتت، جاتنالل ISE ۆزيم رشن تايىلمع يف زكرم يف URL ناونع هيجوت ۆداعا عم DHCP و HTTP و RADIUS نم الک اعويش رثکا لکشب ۆطقن تانايىب طاقتلارجا نم عس اولكشب HTTP قييقحت مادختسا متى، ISE لمع ريس، جاتنالا مادختسا تالاح ضعب يف، كلذ عم و مدخلتسملارلىك و ۆلسلس نم ۆممەل ۆياهنلا ۆطقن فيصوت ۆبعص نم ديزى امم، Dot1x، لضفيو بوغرم رىغ URL ناونع هيجوت ۆداعا نوكىي تامدخ ۆعومجم فرعمب لصتى فظوم رتوبيمك يألك نكمى، لاثملارلىك بسىل ۆوصول (SSID) ۆكرشلا ىلع iPod و iPhone ىصخشلا ھزاهج لوصح نىچىلىا لماكىلا ۆوصول (SSID) ۆكرشلا مهه طييطةختو نيمدختسملار ضرع متى، نىھويرانىسلا الک يف. طقف تنرتنالا ىلى ۆوصول دمتعت ال يتلار، ليوختلار فىيرعت فلم ۆقباطمل ادىدحت رثکا ۆي و ۆعومجم ىلى ايكمانيد مسا ۆقباطم مادختسالا ۆعئاشلا ىرخالا لئادبلا نمو. بى و ضرعتسم حتفل مدخلتسملارلى ۆطقن فيضم مسا رىيغتب نوموقى دق نيمدختسملارنى لماك رىغ لحل اذه. فيضم ملا ۆياسىق رىغ ۆميق ىلى ۆياهنلا.

مقر DHCP و DHCP تامىل ع تابلط ۆمىاقي رايىخ مادختسا نكمى، هذه لىم ۆيىچنالا تالاحلا يف يف "تامىل ع تابلط ۆمىاقي" لىچ مادختسا نكمى. ۆزهجانلا هذه فيصوتل ۆلىد ۆقيرطك 55 يذلا (IPS) لىلسلا عنم ماظن لىم ۆياهنلا ۆطقن ليغشت ماظن عباسا تامىصل ۆمنزح فاشتكا ۆمنزح ۆياهنلا ۆطقن ليغشت ماظن لىرسري امدنۇع. ۆمنزح ۆقباطمل اعىقوقت مدخلتسىخ يتلارا تارايىخ ب ئيمقر ۆمىاقي ۆعنىصملارلى ۆكرشلا نممضتت، كلسلا ىلع اھبلط وأ دامى، TFTP مداخو، (DNS) لاجملار مسا مداخو، يضارتفالا ھجوملا) DHCP مداخ نم اھىقلت يف بغرت نكمىوام دح ىلى ديرف مداخلا نم تارايىخلا هذه DHCP ليمع ھب بلىطي يذلا بىترتلا. (كلذ ىلى تابلط ۆمىاقي رايىخ مادختسا دعىي ال. نىيعم ردصم ليغشت ماظن عباسا تامىصل ھمادختسما مادختسا نم امكىح رثکا یەف، كلذ عم و HTTP مدخلتسملارلىك و ۆلسلس ك اقىقد تامىل ع تابلط ۆمىاقي تباڭ لکشب ۆددەملا تانايىبلا نم اھرىغ و فيضم ملا عامسا.

اهجتننت يتلار تانايىبلا نألى ايلاثم الـ DHCP تامىل ع تابلط ۆمىاقي رايىخ دعىي ال: **ۆظحالىم** ۆددەتم ۆزهجانلا اهاراركت نكمىو دروملا ىلع ۆدمىع.

ذفنم لىحەم/ۆياهن ۆطقن نم Wireshark تاقاصل مدخلتسا، ISE فيصوت دعاوچ نېوكت لباق مييقتل ISE ىلع (TCP) لاسرا لا يف مكحتلا لوكوتورب غيرفت طاقتلارجا (SPAN) لوحەم تارايىخ ۆنيعلار طاقتلارلا اذه ضرعى. (تىدوچو نا) DHCP ۆمنزح يف تامىل ع تابلط ۆمىاقي تارايىخ ليغشتلا ماظنلار DHCP تامىل ع تابلط ۆمىاقي Windows 10.

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: 000000000000000000000000
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

لوصفمل ايلاتل اقيسنلتلاب جئاتنلا ئېباتك متي يېتللا تامالعملات ابلط ۋەمئاقد ئەلسلىس اذه مىختسأ. 252 و 249 و 121 و 119 و 47 و 46 و 44 و 33 و 31 و 15 و 6 و 3 و 1: قەلصاپسى يىف ئەصصىخىملە فىرعتللا تافلم طورش نىوكت دىنۇ قىسنلتللا.

ةطحىم ۋەقباطىم ئەصصىخىملە فىرعتللا تافلم عاشنى طورش مادختسى نىوكتللا مىسىقى حمىرى لە ئەم ئەچىتلىك Windows 10 ئەلەن.

نىوكتللا

لقتىن او ISE ئەرادىب ئەصصىخىملە (الاى) ئەيموسىرلا مىختىسىملى ۋە جاولى لىجىسىتىب مۇق 1. **فىيضاي ئەقطقىط لېلەتلىك > طورشلى > ئاسايىسلە رەزانىع > ئاسايىسلە ئىلە** ۋەمئاقد ئەباصل ئامىصىپ مىختىسىن، لاثمەن اذه يىف. طورشلى كىشتى سىچەن دىدج تەۋەضأ مىيقەب ئەلماك ئەمئاقد ئىلە لوضىچىللى FingerBank.org ئىلە عجرا Windows 10.

ئەلەن ئاجاتحت دىقۇ، ئەيمقىرىللا تارايىخىلا عېمەج ئەمسىللا ئەمېقىتىنلا بىرمتىرىنى ئەل دىق: ةطحىم ئەلەن مەكلى ئەمئاقلە ضرۇل حىتەفمەلە ۋەحول وە سۆامىلە مادختىساب رېرمەتلى.

Profiler Conditions

- Exception Actions
- NMAP Scan Actions
- Allowed Protocols

Profiler Condition List > New Profiler Condition

Profiler Condition

* Name	Windows10-DHCPOption55_1	Description
* Type	DHCP	
* Attribute Name	dhcp-parameter-request-li	
* Operator	EQUALS	
* Attribute Value	1, 3, 6, 15, 31, 33, 43, 44	
System Type	Administrator Created	

تاس اي اس > تافل ملا دي دح **<** جهن يلى لقتنا ، وددملا ظورشلا مادختساب .
 ةدي دج ءاس اي اس نيوكتل وأ ئيلاحلا فيرعتلا فلم ءاس اي اس لي دعتعل تافل ملا دي دح .
Microsoft-Workstation و ئي ضارت فالا **لمعلا** ئطحوم تاس اي اس ريرحت متى ، لاثملما اذه يف
 اطرش فضأ . ةدي دجل ا تاملعملما تابلط ئمياق طورش نيمضتل **Windows10-Workstation** ئطحوم ررحمو ،
Microsoft-Workstation ئطحوم جهن ئدعاق يلى ادي دج ابكرم
 و هامك نيقيلما لمعاع لي دعتب مق . هان دأ حضوم و هامك **Windows10-Workstation** **لمعلا** .
بولطملا فينصنستلا ئجيتن قيقحت لجا نم بولطم

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

Workstation

* Name	Workstation	Description
Policy Enabled	<input checked="" type="checkbox"/>	Policy for Workstations
* 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**

Name: 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

Profiler Policy

Name: Windows10-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

نم ديزم ىلע لوصح ل (طقف نيلجس ملا عالمع ل) رم اولا ثحب ئادا مدخلت سأ: ئاظحال مسقلما اذه يف ئامدختسم ملا رم اولا لوح تامولعملما.

حصلا نم ققحتلا

1- ۋەطخىلا

س ايىس ىلولما ئاداصىملا قباقات . ئاشابملا تالجىسلا > تايىلمۇلا > ISE ىلى لقتنىا ISE موقىي، زاهىلغا ئاشندا دىجىلە دودجم لوصحىنەم مەتىي و ئافورىملا رىيغلىي و خىتلە ئاداصىم بىلەت يېقلىت مەتىي و CoA لىيغىش تېرىپتىنەم - دىدەجىلە فېيىصوتلىق بىلەت يېقلىت مەتىي و CoA لىيغىش تېرىپتىنەم Windows10 .

Live Logs Live Sessions

Misconfigured Suplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Co...
0	0	0	0	0
Refresh	Reset Repeat Counts	Export To	Show	Within
Never	Latest 20 records	Last 5 min		
			Filter	

2- وظخلا

حيحصل لكشب نيوكتل المع ديكلأ مسقل اذه مدخلتسا.

- قف رقناو، ةياهنلا ةطقن يف ثحب او، ةياهنلا طاقن > قايسلأ ةيفر ةيناكم ايل لقتنا ريرحت.
- نأ نم دكأت **EndPointPolicy** و **Window10-Workstation** ميق **dhcp-parameter-request-list** اقبسم اهننيوكت مت يتلما طورشلا ميق قباطت.

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

اهم اوصاف اطخالا فاشكتسا

اـحـالـصـ اوـ نـيـوـكـتـلـاـ عـاطـخـاـ فـاشـكـتـسـ اـلـ اـهـمـادـخـتـسـ اـلـ كـنـكـمـيـ يـتـلـاـ تـامـوـلـعـمـلـاـ مـسـقـلـاـ اـذـهـ رـفـوـيـ.

تـافـلـمـلـاـ عـاشـنـاـ ةـفـيـظـوـ يـدـوـتـ يـتـلـاـ ISEـاـسـ دـقـعـ ىـلـاـ تـلـصـ وـ DHCـPـ مـزـحـ نـأـ نـمـ قـقـحـتـ •
نـيـتـمـاعـدـ نـيـبـ ـقـحـسـفـلـاـ وـأـ دـعـاـسـمـلـاـ نـاـونـعـ مـادـخـتـسـابـ).

ةـادـأـ > ةـمـاعـ تـاوـدـاـ > صـيـخـشـتـلـاـ تـاوـدـاـ > اـهـالـصـ اوـ عـاطـخـاـلـاـ فـاشـكـتـسـاـ > تـايـلـمـعـلـاـ مـدـخـتـسـاـ •
ةـهـجـاـوـنـمـ يـعـيـبـ طـلـكـشـبـ TCPـ غـيـرـفـتـ طـاقـتـلـاـ لـيـغـشـتـلـ؟ـ Lـوـكـوـتـوـرـبـ غـيـرـفـتـ
ISEـ ةـرـادـإـبـ ةـصـاخـلـاـ (GUIـ)ـ ةـيـمـوـسـرـلـاـ مـدـخـتـسـمـلـاـ.

ةـسـلـجـ لـيـلـدـةـسـلـجـ ISEـ PSNـ -~NSF~NSFـ حـيـحـصـتـ نـيـكـمـتـ •
لـيـغـشـتـلـاـ تـقـوـفـيـرـعـتـلـاـ تـافـلـمـ ئـشـنـمـ ةـعـاصـإـلـاـ

• Profiler.logـ prrt-server.logـ lsd.logـ وـ لـلـصـلـاـ تـاذـ تـامـوـلـعـمـلـاـ رـهـظـتـ وـ دـعـاـقـ عـجـارـ •
ةـيـلـاحـ ةـمـئـاـقـ ىـلـعـ لـوـصـحـلـلـ DHCPـ عـبـاـصـأـ تـامـصـبـ تـانـاـيـبـ ةـمـئـاـقـ تـارـاـيـخـ بـ

فـيـرـعـتـ فـلـمـ عـاشـنـاـ طـورـشـ يـفـ ةـحـيـحـصـلـاـ "ـتـامـلـعـمـلـاـ تـابـلـطـ ةـمـئـاـقـ"ـ مـيـقـ نـيـوـكـتـ نـمـ دـكـأـتـ •
يـلـيـ اـمـ اـمـادـخـتـسـاـ رـثـكـأـلـاـ لـسـالـسـلـاـ ضـعـبـ نـمـضـتـتـ ISEـ:

رـمـاـوـاـ مـادـخـتـسـاـ لـبـقـ حـيـحـصـتـلـاـ رـمـاـوـاـلـوـحـ قـمـمـ تـامـوـلـعـمـ ىـلـاـ عـجـراـ:ـظـحـاـلـمـ debugـ.

لـجـسـلـاـ لـيـلـحـتـ

ISEـ PSNـ -~NSF~NSFـ ةـدـقـعـ ىـلـعـ عـاطـخـاـلـاـ حـيـحـصـتـ نـمـ يـلـيـ اـمـ نـيـكـمـتـ++

-NSF

ةـسـلـجـ

ةـعـاصـإـلـاـ ةـسـلـجـ لـيـلـدـ

فـيـرـعـتـلـاـ تـافـلـمـ ئـشـنـمـ-

-لـيـغـشـتـلـاـ تـقـوـ

ةـيـلـوـأـلـاـ ةـقـدـاـصـمـلـاـ++

++prrt-server.log

ISEـ ةـدـقـعـ ىـلـعـ لـوـصـوـلـاـ بـلـطـ يـقـلـتـ مـتـ++

RADIUS,2020-12-29 06:35:19.377,DEBUG,0x7f1cdcbd2700,cntx=0001348461,sesn=isee30-primary/397910/625,CallStationID=B4-96-91-26-EB-9F,RADIUS packet=code: 1 (AccessRequest)
فـرـعـمـلـاـ=285ـلـوـطـلـاـ

++ISEـ لـاـ قـبـاـطـيـ unknown_profile

AcsLog,2020-12-29 06:35:19.473,DEBUG,0x7f1cdc7ce700,cntx=0001348476,sesn=isee30-primary/39791910/625,CPMSessionID=0A6A270B0000018B44444
013ac,user=dot1xuser,CallStationID=B4-96-91-26-EB-9F,AuthorizationPolicyMatchRule=Unknown_Profile,EapTunnel=EAP-FAST,
EapAuthentication=EAP-MSCHAPv2,UserType=User,CPMSessionID=0A6A270B0000018B4413AC,EndPointMACAddress=B4-96-91-26-EB-9F,

دوـحـمـ لـوـصـوـعـمـ لـوـصـوـلـاـ لـوـبـقـ لـسـرـيـ++ISEـ

radius.2020-12-29 06:35:19.474.DEBUG.0x7f1cdc7ce700.ctx=001348476,sesn=isee30-primary/39791910/625.CPMSessionID=0A6A270B000018B44018B4441
3AC.user=dot1xuser,CallStationID=B4-96-91-26-EB-9F, RADIUS: زمرة=2(AccessAccept)
فروعملاء=331

تم وصول مادختساب ةبساحملاثيـدحت ++ISE

radius.2020-12-29 06:35:41.464.debug.0x7f1cdcad1700.ctx=0001348601.sesn=isee30-primary/39791910/627.CPMSessionID=0A6A270B0000018B4444 13ac, CallStationID=B4-96-91-26-EB-9F, RADIUS: زمرة=4(AccountingRequest)
فروعملاء=381

[1] [dot1xuser]: مدخلـتـسـمـلـا مـسـا مـقـلـا - مـمـيـقـلـا

[87] [GigabitEthernet1/0/13]: مـمـيـقـلـا NAS-Port-ID -

[26] [DHCP-option=]: مـمـيـقـلـا Cisco-av - جـوـز

[26] [audit-session-id=0a6A270B000018B44013AC]: Cisco-av - جـوـز مـمـيـقـلـا

ةبساحملاء بـاجـتـسـا لـسـرـي ++ISE

radius.2020-12-29 06:35:41.472.debug.0x7f1cdc5cc700.ctx=001348601.sesn=isee30-primary/39791910/627.CPMSessionID=0A6A270B000018B4401
3AC.user=dot1xuser,CallStationID=B4-96-91-26-EB-9F, RADIUS: زمرة=5(AccountingResponse)
فروعملاء=45

++Profiler.log

أدبـي ++ISE DHCP رـايـخـعـم يـبـسـاحـمـلـا ثـيـدـحـتـلـا يـقـلـتـ مـتـيـ نـاـ اـمـ زـاهـجـلـلـ فـيـرـعـتـ فـلـمـ عـاشـنـاـ يـفـ

2020-12-29 06:35:41.470 [SyslogListenerThread]
Cisco.profiler.probes.radius.SyslogDefragmenter -:::- ParseHeader inBuffer=<181>Dec
2906:35:41 isee30-primary CISE_RADIUS_Accounting0000652020-10522-10 2-29 06:35:41.467
+00:0000234376 3002 رـاعـشـا Radius-Accounting: ثـيـدـحـتـ RADIUS Accounting Watchdog.
ConfigVersionId=99, IP زـاهـجـلـلـ=10.106.39.11, UserName=dot1xuser, RequestLatency=6,
NetworkDeviceName=SW, User-Name=dot1xuser, NAS-IP=10.106.39.11, NAS-
Port=50113, class=CACS:0a6a270b0000018b44013ac:isee30-primary/397910/625, call-station-
id=a0-EC-F9-3c-82-0d, call-station-id=a 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=00000b, acct-authentic=remote, acct-input-packet=1, acct-output-packet=0, event-
timestamp=160 341899, NAS-Port-Type=Ethernet, NAS-Port-ID=GigabitEthernet1/0/13. Cisco-av-
pair=dhcp-option=dhcp-parameter-request-list=1\, 3\, 6\, 15\, 33\, 43\, 44\, 46\, 47\, 119\, 121\,
249\, 252, cisco-v-pair=audit-id=0a6a7 0b0000018b44013ac, Cisco-av-pair=method=dot1x.

2020-12-29 06:35:41.471 [RadioUSParser-1-thread-2]
cisco.profiler.probes.radius.RadiusParser -:::-

هـلـيـلـحـتـ مـتـ يـذـلـا IOS رـعـشـتـسـمـ 1: dhcp-
parameter-request-list=[1, 3, 6, 15, 31, 33, 43, 44, 46, 47, 119, 121, 249, 252]

ةـمـسـلـا Cisco-av-pair value=dhcp-option=dhcp-parameter-request-list=1\, 3\, 6\, 15\, 33\, 43\, 44\,
46\, 47\, 119\, 121\, 249\, 252, audit-session-id=0A6A270B000018B44013ac, Cisco-av-pair=dot1x

ةـمـسـلـا 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 [RMQforwarder-4] []
cisco.profiler.infrastructure.cache.AbstractEndpointCache -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:ProfilerCollection:- كلام Mac اذى: b4:96:91:26:eb:9f و isee30-primary.anhsinh.local

2020-12-29 06:35:41.479 [RMQforwarder-4] []
cisco.profiler.infrastructure.probemgr.forwarder -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:ProfilerCollection:- 196:91:26:EB:9fis isee30-primary.anhsinh.local 3002 و لاسرلا زمر و 3002

2020-12-29 06:35:41.479 [RMQforwarder-4] []
cisco.profiler.infrastructure.probemgr.forwarder -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:ProfilerCollection:- يقيق حلا ردم ملا رطق فصن و

++ ديدج مس

2020-12-29 06:35:41.480 [RMQforwarder-4] []
cisco.profiler.infrastructure.probemgr.forwarder -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:ProfilerCollection:- بـلـطـلـا ـمـئـاـقـ دـيـدـجـ

2020-12-29 06:35:41.482 [RMQforwarder-4] []
cisco.profiler.infrastructure.probemgr.forwarder -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:ProfilerCollection:- دـعـمـلـا ـيـاهـنـلـا طـاقـنـا ـعـوـمـجـ

2020-12-29 06:35:41.482 [RMQforwarder-4] []
cisco.profiler.infrastructure.probemgr.forwarder -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:Profilercollection:- dhcp-parameter-request-list.

فلتخم نيقى لماع عم فلتخمل دع او قب اطت ++

2020-12-29 06:35:41.484 [RMQforwarder-4] []
cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:Profilercollection:- Intel:b4 96:91:26:EB:9F (5) زاحق س ايسل ا تافل ملا عاشن|

2020-12-29 06:35:41.485 [RMQforwarder-4] []
cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:Profilercollection:- فـيـرـعـتـلـا تـافـلـمـا عـاشـنـا (10) نـيـقـيـلـا

2020-12-29 06:35:41.486 [RMQforwarder-4] []
cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:Profile:- Microsoft-Workstation:b4 96:91:26:EB:9F (10) نـيـقـيـلـا

2020-12-29 06:35:41.487 [RMQforwarder-4] []
cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:Profile:- Windows10-B b4:96:91:26:EB:9F (20) نـيـقـيـلـا

مـثـ نـمـ وـكـتـلـاـ لـلـاـ اـداـنـتـسـاـ 40ـ رـادـقـمـبـ نـيـقـيـ لـمـاعـ ىـلـعـ اـهـيـ دـلـ زـاـهـجـلـلـ ئـيـاهـنـلـاـ ئـطـقـنـ فـيـرـعـتـ فـلـمـكـ تـارـايـتـخـالـاـ هـذـهـفـ

2020-12-29 06:35:41.487 [RMQforwarder-4] []
cisco.profiler.infrastructure.profile.profilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:Profile:- س ايسل يل كيهلا لسلستلا ليتح دعب:

B4::96:91:26:EB:9F EndpointPolicy:Windows10-Workstation J:40 ExceptionRuleMatch:false

2020-12-29 06:35:41.487 [اطفال حيحصت RMQforwarder-4] []
cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-
b713-1a9022ed3c5:-:ياهنلا ةطقن -:تافلملا عاشن|:96:b4:96:9 ئباقطم ئسأيس رئيغت مت
٪1:26:EB:9F.

2020-12-29 06:35:41.489 [اطفال حيحصت RMQforwarder-4] []
cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-
b713-1a9022ed3c5:-:ياهنلا ةطقن -:تافلملا عاشن|:96:b4:96:9 فيرعت ئعومجم رئيغت مت
٪1:26:EB:9F.

2020-12-29 06:35:41.489 [اطفال حيحصت RMQforwarder-4] []
cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-
b713-1a9022ed3c5:Profile:-:ياهنلا ةطقن ئل ع 4:96:91:26:eb:9f -
3b76f840-8c00-11e6-996c-525400b48521

2020-12-29 06:35:41.489 [اطفال حيحصت RMQforwarder-4] []
cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-
b713-1a9022ed3c5:Profile:-:ياهنلا ةطقن ئل ع 4:96:91:26:eb:9f -
4:96:91:26:EB:9F ئسأيس قبات Windows10-Workstation

2020-12-29 06:35:41.489 [اطفال حيحصت RMQforwarder-4] []
cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-
b713-1a99022ed3c5:Profile:-:ياهنلا ةطقن ئل ا ثدحلا لاسرا EP =
3002

2020-12-29 06:35:41.489 [اطفال حيحصت RMQforwarder-4] []
cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-
b713-1a9022ed3c5:-:ياهنلا ةطقن -:تافلملا عاشن|:
يطرش CoA رادصإ 9F/1:26:EB. فيرعت ئعومجم / يقطنملا

2020-12-29 06:35:41.489 [اطفال حيحصت RMQforwarder-4] []
cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-
b713-1a9022ed3c5:Profile:-:CoCoConditional AE عم ليصافت ئاهنلا ةطقن -:
EndPoint[id=ff19ca00-499f-11eb-b713-1a99022ed3c5, name=<null>]

كام b4:96:91:26:EB:9F

مسلا Call-station-id: B4-96-91-26-EB-9F

مسلا EndPointMACAddress: B4-96-91-26-EB-9F

مسلا MacaDdress: B4:96:91:26:EB:9F

Lightweigth لسلج ليلد ئل ا تانايبل لاسرا ++

2020-12-29 06:35:41.489 [اطفال حيحصت RMQforwarder-4] []
cisco.profiler.infrastructure.probemgr.LSDForwarderHelper -::: بـ B4:96:91:26:EB:9F
قبايطم Windows10-Workstation

2020-12-29 06:35:41.489 [اطفال حيحصت RMQforwarder-4] []
cisco.profiler.infrastructure.probemgr.LSDForwarderHelper -::: بـ B4:96:91:26:EB:9F
ئاهنلا ةطقن ئل ا ثدحلا لاسرا

DefaultTable.B4:96:91:26:EB:9F ءانثأةتباث LSD ىلإ ةفاصلا عاجو مل جو

++CoA ك ةددحم ةيـمومـعـلـا Reauth

2020-12-29 06:35:41.489 [CoAHandler-52-thread-1][] حـيـحـصـتـ أـطـاخـأـلـاـ [cisco.profiler.infrastructure.profiling.CoAHandler -:B4:96:91:26:EB:9F:9fe38b30-43ea-11b-713-1a99022ed3c5:ProfilerCoA: رـمـأـ عـونـ مـاعـلـاـ] = Reauth

2020-12-29 06:35:41.490 [RMQforwarder-4][] حـيـحـصـتـ أـطـاخـأـلـاـ [cisco.profiler.infrastructure.cache.AbstractEndpointCache -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a9022ed3c5:- درـأـواـلـاـ دـيـرـبـلـاـ نـمـ ةـيـاهـنـ ةـطـقـنـ ثـيـدـحـتـ] - RADIUS ProbeSGA: falseSG: لمـعـلـاـ ةـطـحـمـ

2020-12-29 06:35:41.490 [RMQforRouder-4][] حـيـحـصـتـ أـطـاخـأـلـاـ [cisco.profiler.infrastructure.cache.AbstractEndpointCache -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a9022ed3c5:- جـمـدـلـاـ دـعـبـ ةـيـاهـنـ ةـطـقـنـ ثـيـدـحـتـ] - EP: b4: 96:91:26:EB:9FEPsource: RADIUS ProbeSGA: falseSG: Windows10-Workstation

طقـفـ CoA ليـغـشـتـبـ ISEـ مـوقـيـسـ .ـ CoAـ لـاسـراـ مـزـلـيـ نـاكـ اـذـاـ اـمـ قـقـحـتـلـلـ جـهـنـلـاـ قـبـاطـيـ فـيـرـعـتـلـاـ فـلـمـ رـيـيـغـتـ قـبـاطـتـ ةـسـاـيـسـ يـأـ هـيـدـلـ نـاكـ اـذـاـ

2020-12-29 06:35:41.701 [CoAHandler-52-thread-1][] حـيـحـصـتـ أـطـاخـأـلـاـ [cisco.profiler.infrastructure.profiling.CoAHandler -:B4:96:91:26:EB:9F:9fe38b30-43ea-11b-713-1a99022ed3c5:ProfilerCoA: اـهـلـكـ ةـيـلـمـعـلـاـ جـهـنـلـاـ] لـوحـمـ يـفـ رـفـوتـمـلـاـ PolicySet ءانـثـسـاـلـلـ اـلـحـمـلـاـ،ـ PolicyStatus=Enabled

2020-12-29 06:35:41.701 [CoAHandler-52-thread-1][] حـيـحـصـتـ أـطـاخـأـلـاـ [cisco.profiler.infrastructure.profiling.CoAHandler -:B4:96:91:26:EB:9F:9fe38b30-43ea-11b-713-1a99022ed3c5:ProfilerCoA: Name: Switch policyStatus: نـكـمـمـ] ةـسـاـيـسـ

2020-12-29 06:35:41.702 [CoAHandler-52-thread-1][] حـيـحـصـتـ أـطـاخـأـلـاـ [cisco.profiler.infrastructure.profiling.CoAHandler -:B4:96:91:26:EB:9F:9fe38b30-43ea-11b-713-1a99022ed3c5:ProfilerCoA: lha: svalue name 6d954800-8bff-11e6-996c-525400b48521 rhs operandID 4270690-8c00-11e6-996c-525400b48521 rhsvaluename Microsoft-workstation:Windows10-workstation]

2020-12-29 06:35:41.933 [CoAHandler-52-thread-1][] com.cisco.profiler.api.util - ةـلـاحـ يـفـ دـدـحـمـ طـرـشـ ةـسـاـيـسـ ضـيـوـفـتـ ProfilerCoA- ليـوـخـتـلـاـ جـهـنـ ةـحـاتـمـ

2020-12-29 06:35:41.933 [CoAHandler-52-thread-1][] com.cisco.profiler.api.util - ةـسـاـيـسـ ضـيـوـفـتـ ProfilerCoA: 42706690-8c00-11e6-996c-525400b48521 ةـسـاـيـسـلـاـ

++CoA ليـغـشـتـ مـتـيـوـ طـرـشـلـاـ اـذـهـلـ قـبـاطـمـ ليـوـخـتـلـاـ جـهـنـنـ

2020-12-29 06:35:41.935 [CoAHandler-52-thread-1][] حـيـحـصـتـ أـطـاخـأـلـاـ [cisco.profiler.infrastructure.profiling.CoAHandler -:B4:96:91:26:EB:9F:9fe38b30-43ea-11b-713-1a99022ed3c5:ProfilerCoA: COA: قـبـطيـ اـفـصـاـلـاـ مـتـ يـذـلـاـ هـفـاـشـنـ] تـامـسـ ىـلـ اـدـانـتـسـاـ RADIUS ةـيـاهـنـ ةـطـقـنـلـاـ

[B4:96:91:26:EB:9F] كـامـ

فرع م سل ج ل مع جا: [0a6a270b0000018b44013ac]

داخ م AAA: [isee30-primary] IP: [10.106.32.119]

و ج اه AAA: [10.106.32.119]

ن اون ع IP صاخ لا NAD: [10.106.39.11]

فرع م ذف نم NAS: [GigabitEthernet1/0/13]

عن و ن ذف نم NAS: [Ethernet]

ع و ن ذف نم دخل ا: [framed]

لاصتا ل اصل س ال ك ل ي: [false]

أ ط خ [] VPN:

أ ط خ [] و MAB:

2020-12-29 06:35:41.938 [CoAHandler-52-thread-1] []
cisco.profiler.infrastructure.profiling.CoAHandler -:B4:96:91:26:EB:9F:9fe38b30-43ea-11b-713-
1a99022ed3c5:ProfilerCoA: لوح CoA IP: 10.106.39.11 و ل اعدت س ال: م داخ ة طق ن ل
B4:96:91:26:EB:9F رمأ coA: reauth

2020-12-29 06:35:41.938 [CoAHandler-52-thread-1] []
cisco.profiler.infrastructure.profiling.CoAHandler -:B4:96:91:26:EB:9F:9fe38b30-43ea-11b-713-
1a99022ed3c5:ProfilerCoA: CoA-Reauth AAA: 10.106.32.119 و ل اول ربع م داخ ة طس او ب
10.106.32.119 | NAD: 10.106.39.11

2020-12-29 06:35:41.949 [SyslogListenerThread] []
Cisco.profiler.probes.radius.SyslogDefragmenter -:::- parseHeader inBuffer=<181>Dec
2906:35:41 isee30-primary CISE_Pass_Authentication 000006562 1 StepData=2==71() 00 \.
ةي و ه ع و مجم ي ف CoASourceComponent=Profiler, CoAReason=Change ع و ن ل
تاس اي س ي ف ه م ادخت س ا مت ي ي ذ ل ا ي ق ط ن م ل ا ف ل م /ة س اي س ل /ة ي اه ن ل ا ة طق ن
ة ك ب ش ل ا زاه ج ف ي رع ت ف ل م ، ا ر ي خ او - ل ي و خ ت ل ا CoAType=Reauthentication Cisco.

++prrt-server.log

acsLog.2020-12-29 06:35:41.938.DEBUG.0x7f1c6ffcb700.ctx=0001348611.log_message=[2020-
12-29 06:35:41.938 +00:000023437980006 :ف ي رع ت ل ا ت ا ف ل م ئ ش ن م ت ا م و ل ع م
، ض ي و ف ت ل ا ب ل ط ي ف ر ي ي غ ت ث ا د ح ا ب ف ي رع ت ل ا ت ا ف ل م
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, EndPoint
PolicyID=4270690-8c00-11e6-996c-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.ctx=001348614,[DynamicAuthorizationFlow::onLocalHttp
Event] رمأ CoA در او:

<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=call-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=0A6A270B000018B44013AC</identifierAttribute>  
    <identifierAttribute name="acs-instance">coa-ip-target:10.106.32.119</identifierAttribute>  
</رودل/>
```

ة قداص ملا ةداعا/

++ لاسن را CoA -

RadiusClient.2020-12-29

06:35:41.943.DEBUG.0x7f1ccb3f3700.ctx=0001348614.sesn=39c74088-52fd-430f-95d-
a8fe78eaa1f1.CallStationID=B4:96:91:26:EB:9f، RADIUS: زمرة =43 (CoArEquest)
فرعمل =27 لوطلا

[4] ناونع [10.106.39.11]: ميقل ناونع

[31] فرع م - طح لاصتا [B4:96:91:26:EB:9F]: ميقل

[87] GigabitEthernet1/0/13: NAS-Port-ID - ميقل

[26] [subscriber:Command=reauthenticate]: Cisco-AV - ميقل

[26] [audit-session-id=0a6A270B000018B44013AC]: Cisco-av - ميقل

RadiusClient.2020-12-29

06:35:41.947.DEBUG.0x7f1cdcad1700.ctx=0001348614.sesn=39c74088-52fd-430f-95d9-
a8fe78eaa1f1.CallStationID=b4:96:91:26:EB:9f، RADIUS: زمرة =44 (CoACK) فرعمل =27

ديج لوص و بلط ++

RADIUS.2020-12-29 06:35:41.970.DEBUG.0x7f1cdc6cd700.ctx=001348621.sesn=isee30-primary/397910/628.CallStationID=B4-96-91-26-EB-9F.RADIUS packet:: زمرة =18 (بلط لوصولا) فرعمل =285 لوطلا =187

طقن زاهجل ةياهنلا ةطقن ةس اي س قباطي يذلا ديجل ا ليوختلا فيرعت فلم ++ISE قباطي ةياهنلا

acsLog.2020-12-29 06:35:42.060.DEBUG.0x7f1cdcad1700.ctx=0001348636.sesn=isee30-primary/39791910/628.CPMSessionID=0A6A270B0000018B444 4013AC.user=dot1xuser.CallStationID=B4-96-91-26-EB-9F.IdentityPolicyMatchRule=Default, AuthorizationPolicyMatchingRule=Microsoft_Workstation, EapTunnel=EAP-FAST, EapAuthentication=EAP-MSCHAPv2, UserType=User, CPMSessionID=0A6A270B0000000000000000 018B44013ac, EndPointMACress=B4-96-91-26-EB-

9F, PostureAssessmentStatus=NotApplication, EndPointMatchProfile=Windows10-Workstation.

- لوصول ا لوبق لاسرا مت++

RADIUS,2020-12-29 06:35:42.061,DEBUG,0x7f1cdcad1700,cntx=0001348636,sesn=isee30-primary/39791910/628,CPMSessionID=0A6A270B0000018B440
13AC,user=dot1xuser,CallStationID=B4-96-91-26-EB-9F, RADIUS: زمرة =2(AccessAccept)
فرعلم=340 لوطلا 191

ةلص تاذ تامولع م

- [ع باص ألا تامصب تاناي ب ةدعاق DHCP Fingerbank.org](#)
- [- تادنت سمل او ينقتلا مع دلا Cisco Systems](#)

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).