DHCP-parameter-toepassingsoptie 55 gebruikt voor configuratievoorbeeld van profiel voor endpoints

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Configureren Verifiëren Problemen oplossen Log analyse Gerelateerde informatie

Inleiding

In dit document wordt het gebruik van optie 55 van de DHCP-parameterlijst beschreven als een alternatieve methode voor profielapparaten die de Identity Services Engine (ISE) gebruiken.

Voorwaarden

Vereisten

Cisco raadt u aan:

- Basiskennis van het DHCP-detectieproces
- Ervaring met het gebruik van ISE om aangepaste profileringsregels te configureren

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ISE versie 3.0
- Windows 10

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Bij productie ISE-implementaties omvatten een aantal van de meest gebruikte profielen RADIUS, HTTP en DHCP. Met URL redirectie in het centrum van de ISE-werkstroom wordt de HTTP-sonde breed gebruikt om belangrijke eindpuntgegevens van de User-Agent-string op te nemen. In sommige gevallen van productiegebruik is een URL-omleiding echter niet gewenst en heeft Dot1x de voorkeur, wat het moeilijker maakt om nauwkeurig een eindpunt te bepalen. Zo krijgt een PC van de werknemer die aan een Identifier (SSID) van het Bedrijf Service Set verbindt volledige toegang terwijl zijn persoonlijk (iPhone, iPad, iPod) slechts de toegang van Internet krijgt. In beide scenario's worden de gebruikers geprofileerd en dynamisch in kaart gebracht aan een meer specifieke identiteitsgroep voor het afstemmen van autorisatieprofielen die niet van de gebruiker afhankelijk is om een webbrowser te openen. Een ander veelgebruikt alternatief is hostname matching. Deze oplossing is niet perfect omdat gebruikers de eindpunthostname in een nietstandaard waarde kunnen veranderen.

In hoek gevallen zoals deze, kunnen de DHCP-toets en DHCP-parameterlijst optie 55 worden gebruikt als alternatieve methode om deze apparaten te profileren. Het veld Parameter Application List in het DHCP-pakket kan worden gebruikt om vingerafdrukken en endpointbesturingssystemen te selecteren, net zoals een IPS (Inbraakpreventiesysteem), gebruikt een handtekening om een pakket aan te passen. Wanneer het end-of-endpointbesturingssysteem een DHCP-pakket op de bedrading verstuurt of aanvraagt, bevat de fabrikant een numerieke lijst met DHCP-opties die u van de DHCP-server wilt ontvangen (standaardrouter, Domain Name Server (DNS), TFTP-server, enzovoort). De volgorde waarin de DHCP-client deze opties van de server opvraagt is vrij uniek en kan worden gebruikt om een bepaald bronbesturingssysteem af te drukken. Het gebruik van de optie Lijst van het Parameter Verzoek is niet zo nauwkeurig als de HTTP User-Agent string, maar het is veel meer gecontroleerd dan het gebruik van hostnamen en andere statistisch gedefinieerde gegevens.

Opmerking: De optie DHCP-parameterlijst is geen perfecte oplossing omdat de gegevens die het produceert, van een verkoper afhankelijk zijn en door meerdere apparaten kunnen worden gedupliceerd.

Voordat u de ISE profileringsregels configureren, gebruikt u Wireless-shark opnamen van een endpoints/Switched Port Analyzer (SPAN) of TCP-pompopnamen (Transmission Control Protocol) op ISE om de opties van de Lijst met parameteraanvragen in het DHCP-pakket (indien aanwezig) te evalueren. Deze voorbeeldopname geeft de opties van de DHCP-parameterlijst voor een Windows 10 weer.

bo	оф								
No.	Time	Source	Destination	Protocol	Length	Info			
1	083 55.281036	0.0.0.0	255.255.255.255	DHCP	342	DHCP	Discover -	Transaction	ID 0xc629c12d
- 1	1645 70.718403	0.0.0.0	255.255.255.255	DHCP	342	DHCP	Discover -	Transaction	ID 0xc629c12d
<									
	Relay agent IP ad	dress: 0.0.0.0							
	Client MAC addres	s: IntelCor_26:eb:	9f (b4:96:91:26:eb:9f)						
	Client hardware a	ddress padding: 00	000000000000000000000000000000000000000						
	Server host name	not given							
	Boot file name no	ot given							
	Magic cookie: DHC	P							
>	Option: (53) DHCP	P Message Type (Dis	cover)						
>	Option: (61) Clie	ent identifier							
>	Option: (12) Host	Name							
>	Option: (60) Vend	lor class identifie	r						
~	Option: (55) Para	meter Request List							
	Length: 14						_		
	Parameter Requ	est List Item: (1)	Subnet Mask						
	Parameter Requ	est List Item: (3)	Router						
	Parameter Requ	est List Item: (6)	Domain Name Server						
	Parameter Requ	est List Item: (15) Domain Name						
	Parameter Requ	lest List Item: (31) Perform Router Discov	er					
	Parameter Requ	est List Item: (33) Static Route						
	Parameter Requ	est List Item: (45) Vendor-Specific Infor	mation					
	Parameter Requ	est List Item: (44) NetBIOS over TCP/IP N	ame Serve	:r				
	Parameter Requ	est List Item: (40) NetBIOS over TCP/IP N	ode Type					
	Parameter Requ	est List Item: (4/	A) Domain Search	cope					
	Parameter Requ	est List Item: (11	1) Classless Static Pour	ta					
	Parameter Requ	est list Item: (24	a) Private/Classless Static Rou	atic Rout	e (Mic	rosof	+)		
	Parameter Requ	est List Item: (25	 Private/Proxy autodi 	scovery	(nite	. 0301	-/		
~	Option: (255) End		-,						

De string van de Parameter Application List die de resultaten bevat wordt geschreven in het volgende komma-gescheiden formaat: 1, 3, 6, 15, 31, 33, 43, 44, 46, 47, 119, 121, 249, 252. Gebruik deze indeling bij het configureren van aangepaste profielen in ISE.

De configuratie sectie demonstreert het gebruik van aangepaste profileringsvoorwaarden om Windows 10-werkstation aan te passen aan een **Windows 10-werkstation**.

Configureren

 Log in op de ISE admin GUI en navigeer naar Beleidselementen > Voorwaarden > Profileren. Klik op Toevoegen om een nieuwe voorwaarde voor aangepaste profilering toe te voegen. In dit voorbeeld gebruiken we vingerafdrukken van Windows 10 Parameter Application List. Raadpleeg <u>Fingerbank.org</u> voor een compleet overzicht van de waarden in de Lijst met parameteraanvragen.

Opmerking: Het tekstvak **Waarde van** kenmerk geeft mogelijk niet alle numerieke opties weer en u moet met de muis of het toetsenbord bladeren om de volledige lijst te kunnen bekijken.

Profiler Conditions	Profiler Condition List > New Profiler Condition								
Exception Actions	Profiler Condition								
NMAP Scan Actions									
Allowed Protocols	* Name	Windows10-DHCPOption55_1	Description	DHCP Option 55 Parameter Request List for					
	* Type	DHCP 🗸		Windows 10.					
	* Attribute Name	dhcp-parameter-request-li \sim							
	* Operator	EQUALS ~							
	* Attribute Value	1, 3, 6, 15, 31, 33, 43, 44							
	System Type	Administrator Created							

2. Als de aangepaste omstandigheden worden gedefinieerd, navigeer dan naar Beleidsbeleid > Profileren > Beleid om een huidig profiel aan te passen of om een nieuw beleid te vormen. In dit voorbeeld wordt het standaard werkstation, Microsoft-Workstation en Windows10-Workstation beleid bewerkt om de nieuwe voorwaarden van de Lijst met parameteraanvragen op te nemen. Voeg een nieuwe samengestelde conditie toe aan het werkstation, Microsoft-Workstation, Windows10-Workstation Profiler-beleidsregel zoals hieronder weergegeven. Wijzig de zekerheidsfactor zoals vereist om het gewenste profileringsresultaat te bereiken.

view Ext Id Sources N	etwork Devices Endpoint Class	sification Node Confi	g Feeds Manual Scans Policy Elements Profiling Polic
< 🔁 🙀	* Name	Workstation	Description Policy for Workstations
🔀 Vizio-Device	Policy Enabled	•	li.
WYSE-Device	* Minimum Certainty Factor	10	(Valid Range 1 to 65535)
V 🔀 Workstation	* Exception Action	NONE	~
GromeBook-Workstati	* Network Scan (NMAP) Action	NONE	~
> 🔀 Linux-Workstation	Create an Identity Group for the poli	icy 🧿 Yes, create matching Ide	ntity Group
> 🔀 Macintosh-Workstati	Parent Policy	No, use existing Identity ***NONE***	Group hierarchy
 Microsoft-Workstatio OpenBSD-Workstation 	* Associated CoA Type	Global Settings	~
> Sun-Workstation	System Type	Administrator Modified	
> 🔀 Xerox-Device	Rules		
Z-Com-Device			
ZTE-Device	If Condition Windows10-DHC	POption55_1 🗸 Then	Certainty Factor Increases \vee 10
> 🔀 Zebra-Device	If Condition OS_X_MountainL	ion-WorkstationRule1Check2	Then Certainty Factor Increases V 30

Overview Ext Id Sources	Network Devices Endpoint Classi	ification Node Config	Feeds Man	ual Scans Policy Elements	Profiling Policies
	* Name	Microsoft-Workstation	Description	Generic policy for Microsoft workstation	
WYSE-Device	Policy Enabled	0			li.
ChromeBook-Workstati	* Minimum Certainty Factor	10	(Valid Range 1 to 65	535)	106
FreeBSD-Workstation					
> 🔀 Linux-Workstation	* Exception Action	NONE	~		
> 🔀 Macintosh-Workstati	* Network Scan (NMAP) Action	NONE	~		
V K Microsoft-Workstatio	Create an Identity Group for the polic	y O Yes, create matching Identit	ty Group		
🔀 Vista-Workstation	Parent Policy	 No, use existing identity Gro Workstation 	oup hierarchy		
K Windows10-Workstat	* Associated CoA Type	Global Settings	~		
🔀 Windows7-Workstatie	System Type	Cisco Provided			
🔀 Windows8-Workstati	oyaan yya	0.000 1 1011000			
WindowsXP-Worksta	Rules				
CopenBSD-Workstation					-
Veren Device	If Condition Windows10-DHCP	Option55_1 V Then C	ertainty Factor Increases	<u>~ 10</u>	
	If Condition Microsoft-Workstat	ion-Rule4-Check1 V The	Certainty Factor Increa	ases ~ 10	
ΞQ < 12 4	Profiler Policy		-		
M WIGE DEVICE	* Name	Windows10-Workstation	Description	Policy for Microsoft Windows 10 worksta	ition
V K Workstation	Policy Enabled	•			lle.
🔀 ChromeBook-Workstati	* Minimum Certainty Factor	20	(Valid Range 1 to 65	535)	
FreeBSD-Workstation	* Exception Action	NONE	~		
> K Linux-Workstation					
Microsoft-Workstatio	* Network Scan (NMAP) Action	NONE	~		
Vista-Workstation	Create an Identity Group for the policy	 Yes, create matching Identit No, use existing Identity Group 	ty Group oup hierarchy		
Windows10-Workstat	* Parent Policy	Microsoft-Workstation	~		
K Windows7-Workstati					
🔀 Windows8-Workstatio	* Associated CoA Type	Global Settings	~		
🔀 WindowsXP-Worksta	System Type	Administrator Modified			
GpenBSD-Workstation	Rules				
> 🔀 Sun-Workstation					
> 🔀 Xerox-Device	If Condition Windows10-DHCP0	Option55_1 V Then C	ertainty Factor Increases	<u>~ 20</u>	/
Z-Com-Device	If Condition Windows10-Workst	tation-Rule4-Check1 🗸 T	Then Certainty Factor Inc	reases V 20	40

Opmerking: Gebruik de <u>Command Lookup Tool (alleen voor geregistreerde gebruikers) voor</u> meer informatie over de opdrachten die in deze sectie worden gebruikt.

Verifiëren

Stap 1 -

Navigatie in naar ISE > Operations > Live Logs. 1ste echtheidscontrole komt overeen met het Onbekend machtigingsbeleid en de beperkte toegang wordt aan ISE verleend. Nadat het apparaat is geprofileerd, brengt ISE CoA in werking en een ander authentificatieverzoek wordt ontvangen op ISE en past het nieuwe profiel - Windows10 Workstation aan.

≡ Cisco ISE		Operations · RADIUS	Operations - RADIUS			
Live Logs Live Sessions						
Misconfigured Supplicants 🕕	Misconfigured Network Device	es 🕕 RADIUS D	rops 🕕	Client Stopped Responding ①		Repeat Co
0	0	O		0		О
				Refresh	Show	Within
				Never ~	Latest 20 records 🗸	Last 5 minu
ジ Refresh				Never 🗸	Latest 20 records 🗸	Last 5 minu
Ø Refresh ≤ Reset Repeat Counts ① Export To ∨ Time Status	Details Repeat Identity	Endpoint ID Identity G	ro Endpoint Profile	Never ~	Latest 20 records ~ Authorization Prof	Last 5 minu 7 Filter Ies
G Refresh Seeset Repeat Counts ① Export To ∨ Time Status ×	Details Repeat Identity	Endpoint ID Identity Gr Endpoint ID Identity Gro	ro Endpoint Profile	Never	Latest 20 records ~ Authorization Prof Authorization Profiles	Last 5 minu Filter les
Image: Second secon	Details Repeat Identity identity identity identity	Endpoint ID Identity Gr Endpoint ID Identity Gro 04:96:91:26:E8:9F	vo Endpoint Profile up Endpoint Profile Windows10-Workstation	Never ✓ Authorization Policy ✓ Authorization Policy ✓ Switch >> Microsoft_workstation ✓	Latest 20 records V Authorization Profiles PermitAccess	Last 5 minu V Filter les
C Refresh Seset Repeat Counts ① Export To ∨ Time Status ×	Details Repeat Identity ···· ···· Identity ···· 0 dot1xuser ···· ···· dot1xuser	Endpoint ID Identity Gro Endpoint ID Identity Gro B4:96:91:26:E8:9F Workstation B4:96:91:26:E8:9F Workstation	ro Endpoint Profile up Endpoint Profile Windows10-Workstation Windows10-Workstation	Never ~ Authorization Policy	Latest 20 records Authorization Profiles PermitAccess PermitAccess	Last 5 minu Filte
S Refresh S Reset Repeat Counts ① Export To ∨ Time Status ×	Details Repeat Identity · Identity · 0 dot1xuser · · dot1xuser · · ·	Endpoint ID Identity Gr Endpoint ID Identity Gro B4:96:91:26:E8:9F Workstation B4:96:91:26:E8:9F Workstation	ro Endpoint Profile up Endpoint Profile Windows10-Workstation Windows10-Workstation	Never Authorization Policy Authorization Policy Switch >> Microsoft_workstation Switch >> Microsoft_workstation	Latest 20 records Authorization Profiles PermitAccess PermitAccess	Last 5 minu Filter

Stap 2 -

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

- Navigeer naar Context Visibility > Endpoints, zoek het eindpunt, klik op Bewerken.
- Bevestig dat het EndPointPolicy Window10-Workstation is en dat de dhcp-parameter-requestlist-waarden overeenkomen met de eerder ingestelde conditioningswaarden.

≡ Cisco ISE				Context Visib	ility • Endpoints
Endpoints > B4:96:91:26:E	B:9F				
B4:96:91:26:EB:9	F Ø Ø 🛛				
MAC Addr Username Endpoint P Current IP Location: I	ess: B4:96:91:26:EB:9F : dot1xuser ?rofile: Windows10-Work Address: Location → All Location	station			
Applications	Attributes	Authentication	Threats	Vulnerabilities	
General Attributes					
Description					
Static Assignment	false				
Endpoint Policy	Windows10-Workstation	1			
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	3, 43, 44, 46, 47, 119, 121, 249, 2	252		

Problemen oplossen

Deze sectie verschaft de informatie die u kunt gebruiken om problemen met uw configuratie op te

lossen.

- Controleer dat de DHCP-pakketten de ISE-beleidsknooppunten bereikten die de profileringsfunctie (met Help-adres of SPAN) uitvoeren.
- Gebruik de **Operations > Troubleshooter > Diagnostische tools > Algemene tools > TCP**stomp? om TCP dump van de ISE admin GUI in werking te stellen.
- Onder uiteinden inschakelen op ISE PSN-knooppunt -nsfnsf-sessieSessiemap voor lichtprofieluit uitvoering genomen door AAA
- Profiler.log , prrt-server.log en lsd.log tonen relevante informatie.
- Raadpleeg de DHCP-gegevensbank <u>Fingerbank.org</u> voor een huidige lijst met opties op de lijst met parameteraanvragen.
- Zorg ervoor dat de juiste waarden van de Parameter Application List in de ISE profilering worden ingesteld. Enkele van de meest gebruikte strings zijn:

Opmerking: Raadpleeg <u>Important Information on Debug Commands (Belangrijke informatie over opdrachten met debug) voordat u opdrachten met debug opgeeft.</u>

Log analyse

++Onder-uitgangen op ISE PSN-knooppunt inschakelen -

-nsf

nsf-sessie

Sessiemap voor licht

profiel

uit uitvoering genomen door AAA

++Initiële verificatie

++prt-server.log

++Toegangsaanvraag ontvangen op ISE-knooppunt

Radius, 2020-12-29 06:35:19,377,DEBUG,0x7f1cdcbd2700,cntx=0001348461,sens=isee30primaire/3 97791910/625,CallingID=B4-96-91-26-EB-9F,**RADIUS-PAKKET: Code=1** (AccessApplication Identifier=182 Lengte=285

++ISE komt overeen met Onbekend_profiel

AcsLogs,2020-12-29 06:35:19,473,DEBUG,0x7f1cdc7ce700,cntx=0001348476,sens=isee30primaire/3 97791910/625,CPMSession=0A6A270B0000018B4013AC, gebruiker=dot1xuser,CallingID=B4-96-91-26-96 EB-9F, **AuthorizationPolicyMatchedRule=Onbekend_Profile**, EapTunnel=EAP-FAST, EapAuthentication=EAP-MSCHAPv2, UserType=User, CPMSessionID=0A6A270B000018B4401 3AC, EndPointMACA-adres=B4-96-91-26-EB-9F,

++ISE Zendt access point met beperkte toegang

Radius, 2020-12-29 06:35:19,474,DEBUG,0x7f1cdc7ce700,cntx=0001348476,ssen=isee30primaire/39 791910/625,CPMSession=0A6A270B0000018B44013AC, gebruiker=dot1xuser,CallingID=B4-96-91-26-EB-9B F, RADIUS-PAKKET: **Code=2(AccessAccept)** Identifier=186 Lengte=331

++ISE ontvangen accounting update met DHCP-informatie

Radius, 2020-12-29 06:35:41,464,DEBUG,0x7f1cdcad1700,cntx=0001348601,sens=isee30primaire/39 791910/627,CPMSession=0A6A270B0000018B4013AC,CallingID=B4-96-91-26-EB-9F,US PACKET:: **Code=4(AccountingApplication)** Identifier=45 Lengte=381

[1] Gebruikersnaam - waarde: [dot1xuser]

[87] NAS-Port-ID - waarde: [Gigabit Ethernet1/0/13]

[26] cisco-av-paarwaarde: [dhcp-optie="

[26] cisco-av-paar - waarde: [audit-sessie-id=0A6A270B0000018B44013AC]

++ISE-respons voor back-upaccounting

Radius, 2020-12-29 06:35:41,472,DEBUG,0x7f1cdc5cdc700,cntx=0001348601,sens=isee30primaire/39 7791910/627,CPMSession=0A6A270B0000018B4013AC, gebruiker=dot1xuser,CallingID=B4-96-91-26-EB 9F, RADIUS-PAKKET: **Code=5(AccountingResponse)** Identifier=45 Lengte=20,RADIUSandler.cpp:2216

++Profiler.log

++once Accounting Update wordt ontvangen met de DHCP-optie dhcp-parameter-request-list, ISE begint met het profileren van het apparaat

2020-12-29 06:35:41.470 DEBUG [SyslogconformThread][]

cisco.profiler.probes.Straal.SyslogDefragmenter -::- **verlader in Buffer**=<181>29 dec. 29 06:35:41 is 30-primaire CISE_RADIUS_Accounting 000000655 2 0 2020-12-29 06:35:41.467 +00:000 0234376 3002 OPMERKING **Radius-accounting: RADIUS-**beheerprogramma voor **accounting**, configuratieID=99, apparaatadres=10.106.39.11, UserName=dot1xuser, requestLatency=6, NetworkDevicesName=Sw, User-Name=dot1xuser, NAS-IP-Address=10.106.3 9.11, NASpoorts=50113, klasse=CACS:0A6A270B0000018B44013AC:ISE30-primaire/39791910/625, CD-ROM-D=A0-EC-F9-3C-82D, Calling-ID=B4-96-91-26-EB-9F, NAS-Identifier=Switch, Acct-Statustype=Interim-Update, Acct-Delay-Time=0, Acct-Input-Octets=174, Acct-O Octets=0, accountingsessie-id=000000b, Toets-authentiek=Remote, Acct-Input-Packets=1, Acct-O-Packets=0, Event-Time-stamp=1609341899, NAS-poorts-type=Ethernet, NAS-Port-Port-poort=1 **3**\, **6**\, **15**\, **33**\, **43**\, **44**\, **46**\, **47**\, **119**\, **121**\, **24**\ **9**\, **252**, **cisco-av-pair=audit-sessieid=0A6A270B0000018B44013AC**, cisco-av-pair=methode=dot1x,

2020-12-29 06:35:41,471 DEBUG[RADIUSParser-1-thread-2][] cisco.profiler.probes.Straal.RadiusParser -:- Geparseerde IOS-sensor 1: dhcp-parameter-requestlist=[1, 3, 6, 15, 31, 33, 43, 44, 46, 47, 119, 121, 249, 252]

Toestand:cisco-av-paarwaarde:dhcp-optie=dhcp-parameter-request-list=1\, 3\, 6\, 15\, 31\, 33\, 43\, 44\, 46\, 47\, 119\, 121\, 249\, 252 audit-sessie-id=0A6A270B0000018B44013AC, methode=dot1x

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

2020-12-29 06:35:41.479 DEBUG [RMQexpediteur-4][] cisco.profiler.cache.AbstractEndpointCache -:B4:96:91:26:EB:9F:124 13370-49a0-11eb-b713-1a99022ed3c5:ProfilerCollector:- **Eigenaar voor deze Mac: B4:96:91:26:EB:9F is isee30primaire.anshsinh.plaatselijk**

2020-12-29 06:35:41.479 DEBUG [RMQexpediteur-4][] cisco.profiler.infrastructure.sondmgr.Forwarder - B4:96:91:26:EB:9F:1241 - huidige eigenaar voor het eindpunt B4:96:91:26:EB:9Fis isee30-primaire.anshsinh.lokale en berichtcode is 330 002

2020-12-29 06:35:41.479 DEBUG [RMQexpediteur-4][] cisco.profiler.infrastructure.sondmgr.Forwarder - B4:96:91:26:EB:9F:1241 370-49a0-11eb-b713-1a99022ed3c5:ProfilerCollector:- is de boogstraal voor de eindpuntbron waarboven het is

++Nieuw kenmerk

2020-12-29 06:35:41.480 DEBUG [RMQexpediteur-4][] cisco.profiler.infrastructure.sondmgr.Forwarder - B4:96:91:26:EB:9F:1241 370-49a0-11eb-b713-1a99022ed3c5:ProfilerCollector:- **Nieuwe eigenschap: dhcp-parameter-request-list**

2020-12-29 06:35:41.482 DEBUG [RMQexpediteur-4][] cisco.profiler.infrastructure.sondmgr.Forwarder - B4:96:91:26:EB:9F:1241 370-49a0-11eb-b713-1a99022ed3c5:ProfilerCollector:- Aangepaste eindpuntset:

2020-12-29 06:35:41.482 DEBUG [RMQexpediteur-4][] cisco.profiler.infrastructure.sondmgr.Forwarder - B4:96:91:26:EB:9F:1241 370-49a0-11eb-b713-1a99022ed3c5:**ProfilerCollector:- dhcp-parameter-request-list,**

++Verschillende regels zijn voorzien van verschillende zekerheidsfactoren

2020-12-29 06:35:41.484 DEBUG [RMQexpediteur-4][] cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:124 3370-49a0-11ebb713-1a99022ed3c5:**Profilering:- Op beleidsIntel-Devices is een model B4:96:91:26:EB:9F** (zekerheid 5)

2020-12-29 06:35:41.485 DEBUG [RMQexpediteur-4][] cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:124 3370-49a0-11ebb713-1a99022ed3c5:**Profilering:- Beleidswerkstation afgesloten B4:96:91:26:EB:9F (zekerheid 10)**

2020-12-29 06:35:41.486 DEBUG [RMQexpediteur-4][] cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:124 3370-49a0-11ebb713-1a99022ed3c5:**Profilering:- Op het beleid van Microsoft-Workstation werd een afgesloten B4:96:91:26:EB:9F (zekerheid 10)**

2020-12-29 06:35:41.487 DEBUG [RMQexpediteur-4][] cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:124 3370-49a0-11ebb713-1a99022ed3c5:**Profileren:- Op Windows10-werkstation is een afgesloten B4:96:91:26:EB:9F** (zekerheid 20)

++Windows10-Workstation heeft de hoogste veiligheidsfactor van 40 op basis van de configuratie en dus kiest dit als het Endpoint Profile voor het apparaat 2020-12-29 06:35:41.487 DEBUG [RMQexpediteur-4][]

cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:124 3370-49a0-11ebb713-1a99022ed3c5:Profileren:- Na analyse van de beleidhiërarchie: Eindpunt: B4:96:91:26:EB:9F EndpointPolicy:Windows10-Workstation voor:40 ExceptionRuleMatched:vals

2020-12-29 06:35:41.487 DEBUG [RMQexpediteur-4][] cisco.profiler.infrastructure.profiler.ProfilerManager -: B4:96:91:26:EB:9F:124 3370-49a0-11ebb713-1a9022ed3c5:**Profilering:- Eindpunt B4:96:91:26:EB:9F aangepast beleid gewijzigd.**

2020-12-29 06:35:41.489 DEBUG [RMQexpediteur-4][] cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:124 3370-49a0-11ebb713-1a9022ed3c5:**Profileren:- Eindpunt B4:96:91:26:EB:9F IdentityGroup gewijzigd.**

2020-12-29 06:35:41.489 DEBUG [RMQexpediteur-4][] cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:124 3370-49a0-11ebb713-1a99022ed3c5:**Profilering:- ID van de groep-identiteit instellen op eindpunt B4:96:91:26:EB:9F - 3b76f840-8c00-1 1e6-996c-525400b48521**

2020-12-29 06:35:41.489 DEBUG [RMQexpediteur-4][] cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:124 3370-49a0-11ebb713-1a99022ed3c5:Profileren:- **Calling end-end-point cache met gedeponeerd eindpunt B4:96:91:26:EB:9F, beleid Windows10-Workstation, aangepast beleid Windows10 werkstation**

2020-12-29 06:35:41.489 DEBUG [RMQexpediteur-4][] cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:124 3370-49a0-11ebb713-1a99022ed3c5:**Profileren:- Verzendende gebeurtenis blijft eindpunt B4:96:91:26:EB:9F, en ep-berichtcode = 3002**

2020-12-29 06:35:41.489 DEBUG [RMQexpediteur-4][] cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:124 3370-49a0-11ebb713-1a99022ed3c5:**Profileren:- Eindpunt B4:96:91:26:EB:9F IdentityGroup / Logical Profile** gewijzigd. Uitgifte van een voorwaardelijke CoA

2020-12-29 06:35:41.489 DEBUG [RMQexpediteur-4][] cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:124 3370-49a0-11ebb713-1a9022ed3c5:Profileren:- VoorwaardelijkCoAEvent met endpointdetails: EndPoint[id=ff19ca00-499f-11eb-b713-1a99022ed3c5, naam=<nul>]

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

Kenmerk:Calling-ID waarde:B4-96-91-26-EB-9F

Kenmerk:EndPointMACAdingewaarde:B4-96-91-26-EB-9F

Toekenning:MACA-adreswaarde:B4:96:91:26:EB:9F

++Verzenden van de gegevens naar lichtgewicht sessiemap

2020-12-29 06:35:41.489 DEBUG [RMQexpediteur-4][] cisco.profiler.infrastructure.probemgr.LSDForwarderHelper: 6:B:9F afgesloten voor Windows10-werkstation

2020-12-29 06:35:41.489 DEBUG[RMQexpediteur-4][]

cisco.profiler.infrastructure.sondmgr.LSDForwarderHelper -:- Verzendingsevenement om het eindpunt te handhaven en voor expediteur toe te voegen standaard B4:96:91:26:EB:9F

++Global CoA is geselecteerd als Reauth

2020-12-29 06:35:41.489 DEBUG [CoAHandler-52-thread-1][] cisco.profiler.infrastructure.profiler.CoAHandler - B4:96:91:26:EB:9F 9fe38b30-43ea-11eb-b713-1a99022ed3c5:**ProfilerCoA:- Geconfigureren Global CoA-opdrachttype = Reauth**

2020-12-29 06:35:41,490 DEBUG [RMQexpediteur-4][] cisco.profiler.cache.AbstractEndpointCache -:B4:96:91:26:EB:9F:124 13370-49a0-11eb-b713-1a99022ed3c5:- **Bijgewerkt eindpunt - EP van binnenkomende: B4:96:91:26:EB:9FepSource: RADIUS-testSGA: valseSG: werkstation**

2020-12-29 06:35:41,490 DEBUG [RMQexpediteur-4][] cisco.profiler.cache.AbstractEndpointCache -:B4:96:91:26:EB:9F:124 13370-49a0-11eb-b713-1a99022ed3c5:- **Updaterend eindpunt - EP na fusie: B4:96:91:26:EB:9FepSource: RADIUStestSGA: valse SG:Windows10-werkstation**

++ISE komt overeen met het te controleren beleid als u CoA moet verzenden. ISE zal CoA alleen activeren als er een beleid is dat overeenstemt met de wijziging in het profiel

2020-12-29 06:35:41,701 DEBUG [CoAHandler-52-thread-1][] cisco.profiler.infrastructure.profiler.CoAHandler -:B4:96:91:26:EB:9F 38b30-43ea-11eb-b713-1a99022ed3c5:**ProfilerCoA:- Alle beschikbare beleidslijnen verwerken in Local Exception PolicySet-switch, beleidsstatus=ENABLED**

2020-12-29 06:35:41,701 DEBUG [CoAHandler-52-thread-1][] cisco.profiler.infrastructure.profiler.CoAHandler - B4:96:91:26:EB:9F 9fe38b30-43ea-11eb-b713-1a99022ed3c5:**ProfilerCoA:- Beleidsnaam: Beleidsstatus overschakelen : INGESCHAKELD**

2020-12-29 06:35:41,702 DEBUG [CoAHandler-52-thread-1][] cisco.profiler.infrastructure.profiler.CoAHandler - B4:96:91:26:EB:9F 9fe38b30-43ea-11eb-b713-1a99022ed3c5:**ProfilerCoA:- Lhswaarde naam 6d954800-8bff-11e6-996c-52 B5400b48521 rhs**bediening, ID 42706690-8c00-11e6-996c-525400b48521 nl, nl. werkstation:Microsoft-

Workstation:Windows10 werkstation

2020-12-29 06:35:41,933 DEBUG [CoAHandler-52-thread-1][] com.cisco.profiler.api.Util -:B4:96:91:26:EB:9F:93 88b30-43ea-11eb-b713-1a99022ed3c5:**ProfilerCoA:- Gespecificeerde** voorwaarde beschikbaar in het autorisatiebeleid

2020-12-29 06:35:41,933 DEBUG [CoAHandler-52-thread-1][] com.cisco.profiler.api.Util -:B4:96:91:26:EB:9F:93 **ProfilerCoA:- autorisatiebeleid: 42706690-8c00-11e6-996c-525400b48521**

++Authorized Policy voldoet aan deze voorwaarde en CoA wordt geactiveerd

2020-12-29 06:35:41,935 DEBUG [CoAHandler-52-thread-1][] cisco.profiler.infrastructure.profiler.CoAHandler - B4:96:91:26:EB:9F 9fe38b30-43ea-11eb-b713-1a99022ed3c5:**ProfilerCoA:- passenCacaoa toe: Er is een beschrijving gemaakt op basis van RADIUS-kenmerken van endpoints:**

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

Session-id: [0A6A270B0000018B44013AC]

AAA-server: [isee30-primaire] IP: [10.106.32.119]

AAA-interface: [10.106.32.119]

NAD IP-adres: [10.106.39.11]

NAS poort-id: [Gigabit Ethernet1/0/13]

NAS-poorttype: [Ethernet]

Servicetype: [Framed]

Is draadloos: [onjuist]

Is VPN: [onjuist]

Is MAB: [onjuist]

2020-12-29 06:35:41,938 DEBUG [CoAHandler-52-thread-1][] cisco.profiler.infrastructure.profiler.CoAHandler - B4:96:91:26:EB:9F 9fe38b30-43ea-11eb-b713-1a99022ed3c5:**ProfilerCoA:- staat op het punt om CoA voor en IP te bellen: 10.106.39.11 voor eindpunt: B4:96:91:26:EB:9F CoA-opdracht: Reauth**

2020-12-29 06:35:41,938 DEBUG [CoAHandler-52-thread-1][] cisco.profiler.infrastructure.profiler.CoAHandler - B4:96:91:26:EB:9F 9fe38b30-43ea-11eb-b713-1a99022ed3c5:**ProfilerCoA:- CoA-REAUTH toepassen door AAA-server: 10.106.32.119 via Interface: 10.106.32.119 bij NAD: 10.106.39.11**

2020-12-29 06:35:41.949 DEBUG [SyslogconformThread][]

cisco.profiler.probes.Straal.SyslogDefragmenter -::- verladerHeader in Buffer=<181>dec 29 6:35:41 isee30-primaire CISE_Passed_Authentications 000000656 2 1 StapData=2=(poort = 1700 \, type = Cisco CoA), CoASSourceComponent=Profiler, CoARason=Verandering in eindpuntgroep/beleids-/logisch profiel dat wordt gebruikt in het vergunningsbeleid, CoAType=herauthenticatie - last, Network Devices Profile=Cisco;

++prt-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 000234379 80006 INFO-profiler: Profiler brengt verandering van autorisatieaanvraag in, ConfigVersieID=99, EndpointCoA=Reauth, EndpointMacAddress=B4:96:91:26:EB:9F, EndpointNADAAddress=10.106.39.11, pointPolicy=Windows10-Workstation, EndpointEigenschap=Service-type=framed\,MessageCode=3002\,EndPointPolicyID=42706690-8c00-11e6-996c-52540b48 521\,UseCase=\,NAS-poorts-ID=GigabitEthernet1/0/13\,NAS-poortstype=Ethernet\,Response=\ {User-Name=dot1xuser\;

DynamicAuthorizationFlow, 2020-12-29

06:35:41,939,DEBUG,0x7f1cdc3ca700,cntx=0001348614,[DynamicAuthorizationFlow::opLocalTht tpEvent] Ontvangen inkomende CoA opdracht:

<Reecht id="39c7408-52fd-430f-95d9-a8fe78eaa1f1" type="last">

<SessieserverAddress="10.106.39.11">

<identifierNaam="UseInterface">10.106.32.119</identifierkenmerk>

<identifierNaam="Calling-Station-ID">B4:96:91:26:EB:9F</identifierKenmerken>

<identifierNaam="NAS-poorts-ID">Gigabit Ethernet1/10/13</identifierKenmerk>

<identifierNaam="cisco-av-paar">audit-sessieid=0A6A270B0000018B4013AC</identifierkenmerk>

<identifierNaam="ACS-instantie">COA-IP-TARGET:10.106.32.119</identifierkenmerk>

</sessie>

</opnieuw authentiseren>

++CoA verzonden -

Radius-client, 2020-12-29 06:35:41,943,DEBUG,0x7f1cb3f3700,cntx=0001348614,sens=39c744 888-52fd-430f-95d9-a8fe78eaa1f1,CallingID=B4:96:91:26:EB:9F, RADIUS-PACKET: **Code=43** (CoARequest) Identifier=27 Lengte=225

[4] NAS-IP-Address - value: [10.106.39.11]

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

[87] NAS-Port-ID - waarde: [Gigabit Ethernet1/0/13]

[26] cisco-av-paar - waarde: [abonnee:opdracht=reecht]

[26] cisco-av-paar - waarde: [audit-sessie-id=0A6A270B0000018B44013AC]

Radius-client, 2020-12-29 06:35:41.947,DEBUG,0x7f1cdcad1700,cntx=0001348614,sens=39c740 88-52fd-430f-95d9-a8fe78eaa1f1,CallingID=B4:96:91:26:EB:9F, RADIUS-PACKET: **Code=44** (CoAACK) Identifier=27

++Nieuw toegangsverzoek

Radius, 2020-12-29 06:35:41,970,DEBUG,0x7f1cdc6cd700,cntx=0001348621,sens=isee30primaire/39 791910/628,CallingID=B4-96-91-26-EB-9F,RADIUS-PAKKET: **Code=1** (AccessApplication Identifier=187 Lengte=285

++ISE komt overeen met het nieuwe autorisatieprofiel dat overeenkomt met het endpointbeleid van het endpointapparaat

AcsLogs,2020-12-29 06:35:42,060,DEBUG,0x7f1cdcad1700,cntx=0001348636,ssen=isee30primaire/beide 397791910/628,CPMSession=0A6A270B0000018B4013AC, gebruiker=dot1xuser,CallingID=B4-96-91-26 -EB-9FIdentityPolicyMatchedRule=Default, **AuthorizationPolicyMatchedRule=Microsoft_workstation,** EapTunnel=EAP-FAST, EapAuthentication=EAP-MSCHAPv2, UserType=User, CPMSessionID=0A6A270B0000 18B44013AC, EndPointMACAdjurk=B4-96-91-26-EB-9F, PostureAssessmentStatus=NotApplication, **EndPointMatchedProfile=Windows10-Workstation**, ++Access Accept wordt verzonden -

Radius, 2020-12-29 06:35:42,061,DEBUG,0x7f1cdcad1700,cntx=0001348636,sens=isee30primaire/39 7791910/628,CPMSession=0A6A270B0000018B4013AC, gebruiker=dot1xuser,CallingID=B4-96-91-26-EB 9F, RADIUS-PAKKET: **Code=2(AccessAccept)** Identifier=191 Lengte=340

Gerelateerde informatie

- Fingerbank.org DHCP-Fingerprint database
- Technische ondersteuning en documentatie Cisco Systems