Exemple de configuration de l'option 55 de liste de requêtes de paramètres DHCP utilisée pour profiler les points d'extrémité

Contenu

Introduction

Ce document décrit l'utilisation de l'option 55 de la liste de requêtes de paramètres DHCP comme méthode alternative aux périphériques de profil qui utilisent ISE (Identity Services Engine).

Conditions préalables

Conditions requises

Cisco recommande que vous ayez :

- Connaissance de base du processus de découverte DHCP
- Expérience de l'utilisation d'ISE pour configurer des règles de profilage personnalisées

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ISE version 3.0
- Windows 10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

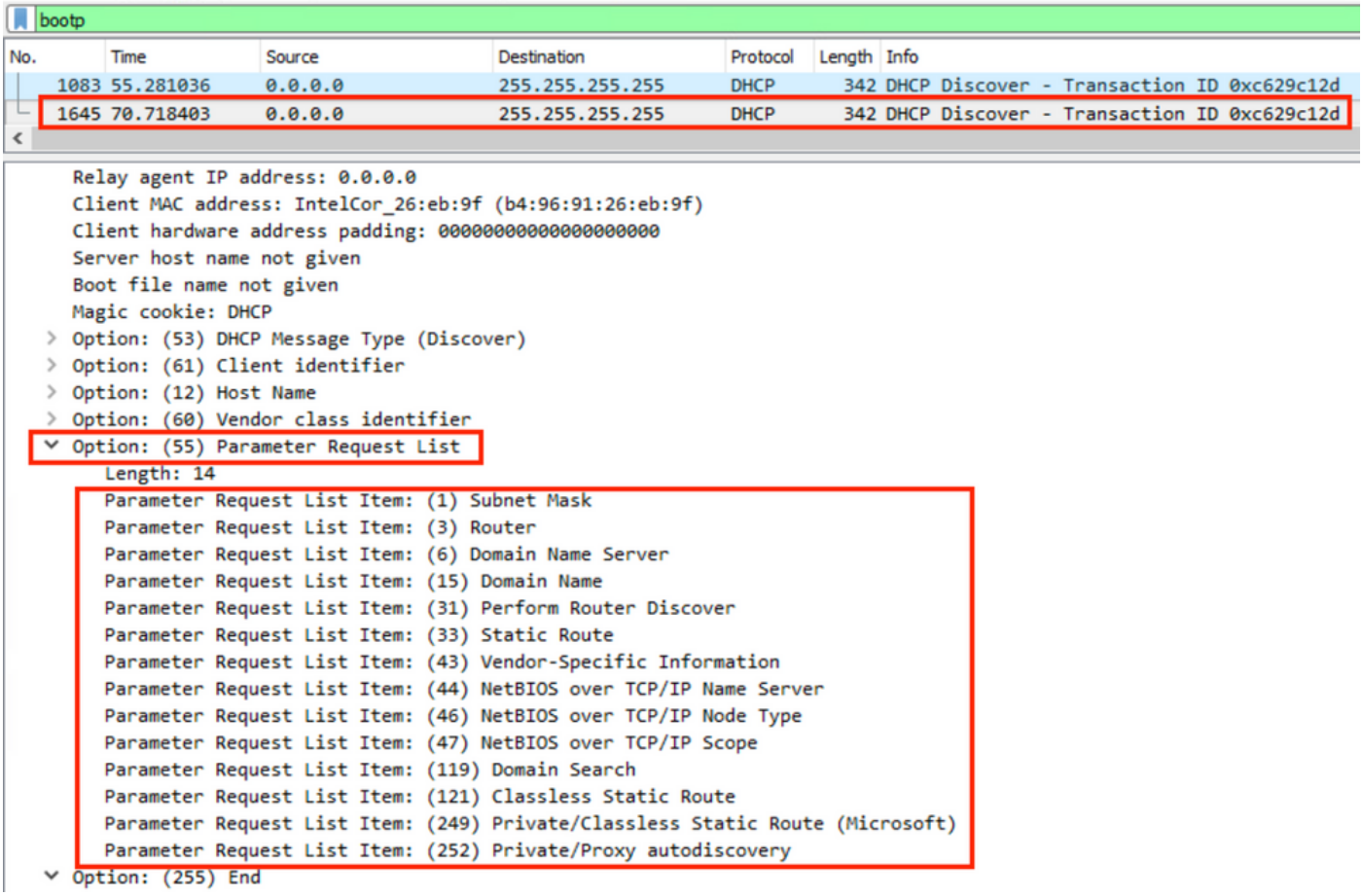
Informations générales

Dans les déploiements ISE de production, certaines des sondes de profilage les plus couramment déployées incluent RADIUS, HTTP et DHCP. Avec la redirection d'URL au centre du flux de travail ISE, la sonde HTTP est largement utilisée afin de capturer des données importantes de point de terminaison à partir de la chaîne User-Agent. Cependant, dans certains cas d'utilisation de production, une redirection d'URL n'est pas souhaitée et Dot1x est préféré, ce qui rend plus difficile le profilage précis d'un point de terminaison. Par exemple, un PC employé qui se connecte à un SSID (Service Set Identifier) d'entreprise obtient un accès complet alors que son iDevice personnel (iPhone, iPad, iPod) n'a accès qu'à Internet. Dans les deux scénarios, les utilisateurs sont profilés et mappés dynamiquement à un groupe d'identité plus spécifique pour la correspondance des profils d'autorisation qui ne dépend pas de l'utilisateur pour ouvrir un navigateur Web. Une autre alternative couramment utilisée est la correspondance de nom d'hôte. Cette solution est imparfaite car les utilisateurs peuvent remplacer le nom d'hôte du point d'extrémité par une valeur non standard.

Dans des cas d'angle tels que ceux-ci, l'option 55 de la sonde DHCP et de la liste de requêtes de paramètres DHCP peut être utilisée comme méthode alternative pour profiler ces périphériques. Le champ Parameter Request List du paquet DHCP peut être utilisé afin d'empreintes digitales d'un système d'exploitation de point d'extrémité, tout comme un système de prévention des intrusions (IPS) utilise une signature afin de correspondre à un paquet. Lorsque le système d'exploitation du point d'extrémité envoie un paquet de détection ou de requête DHCP sur le câble, le fabricant inclut une liste numérique des options DHCP qu'il entend recevoir du serveur DHCP (routeur par défaut, serveur de noms de domaine (DNS), serveur TFTP, etc.). L'ordre dans lequel le client DHCP demande ces options au serveur est assez unique et peut être utilisé pour l'empreinte d'un système d'exploitation source particulier. L'utilisation de l'option Parameter Request List n'est pas aussi exacte que la chaîne HTTP User-Agent, cependant, elle est beaucoup plus contrôlée que l'utilisation de noms d'hôte et d'autres données définies de manière statique.

> **Note**: L'option DHCP Parameter Request List n'est pas une solution parfaite, car les données qu'elle produit dépendent du fournisseur et peuvent être dupliquées par plusieurs types de périphériques.

Avant de configurer les règles de profilage ISE, utilisez des captures Wireshark à partir d'un SPAN (Point de terminaison/Switched Port Analyzer) ou des captures de vidage TCP (Transmission Control Protocol) sur ISE afin d'évaluer les options de liste de requêtes de paramètres dans le paquet DHCP (le cas échéant). Cet exemple de capture affiche les options DHCP Parameter Request List pour Windows 10.

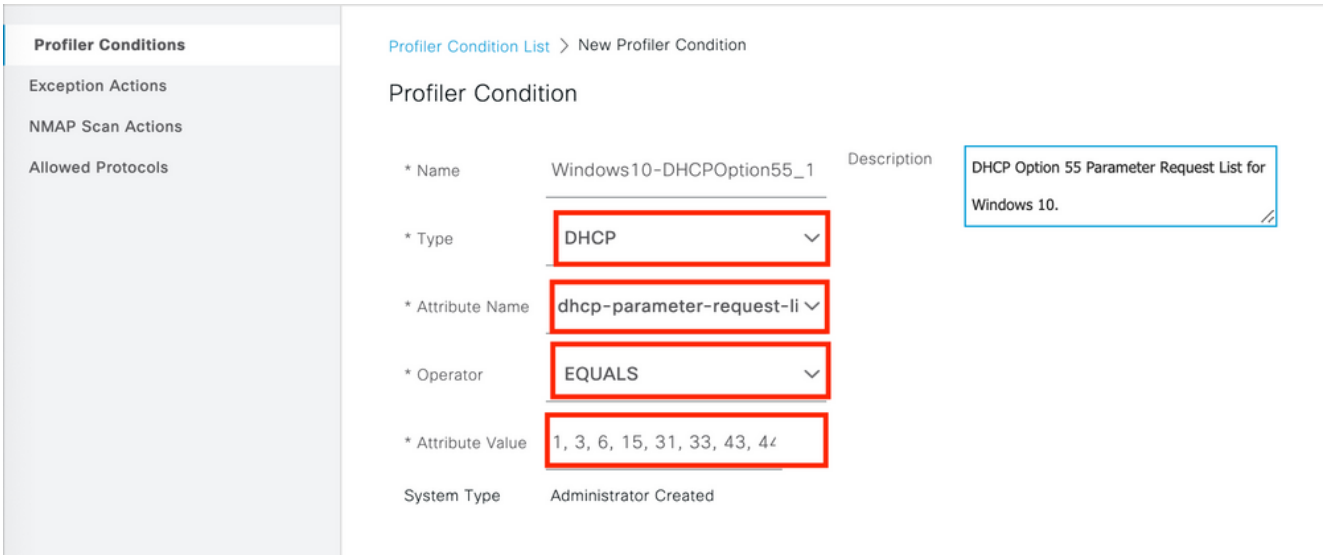


La chaîne de liste de requêtes de paramètres qui en résulte est écrite au format suivant, séparé par des virgules : 1, 3, 6, 15, 31, 33, 43, 44, 46, 47, 119, 121, 249, 252. Utilisez ce format lors de la configuration des conditions de profilage personnalisées dans ISE.

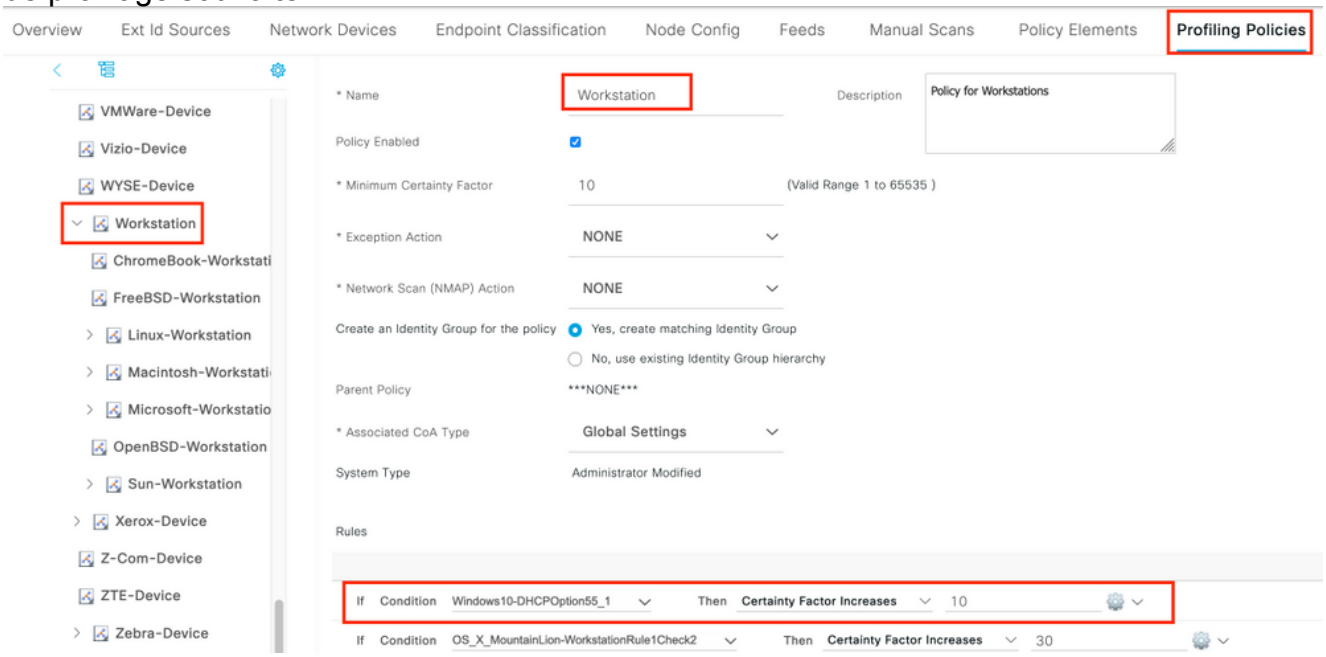
La section Configuration illustre l'utilisation de conditions de profilage personnalisées pour faire correspondre une station de travail Windows 10 à une **station de travail Windows10**.

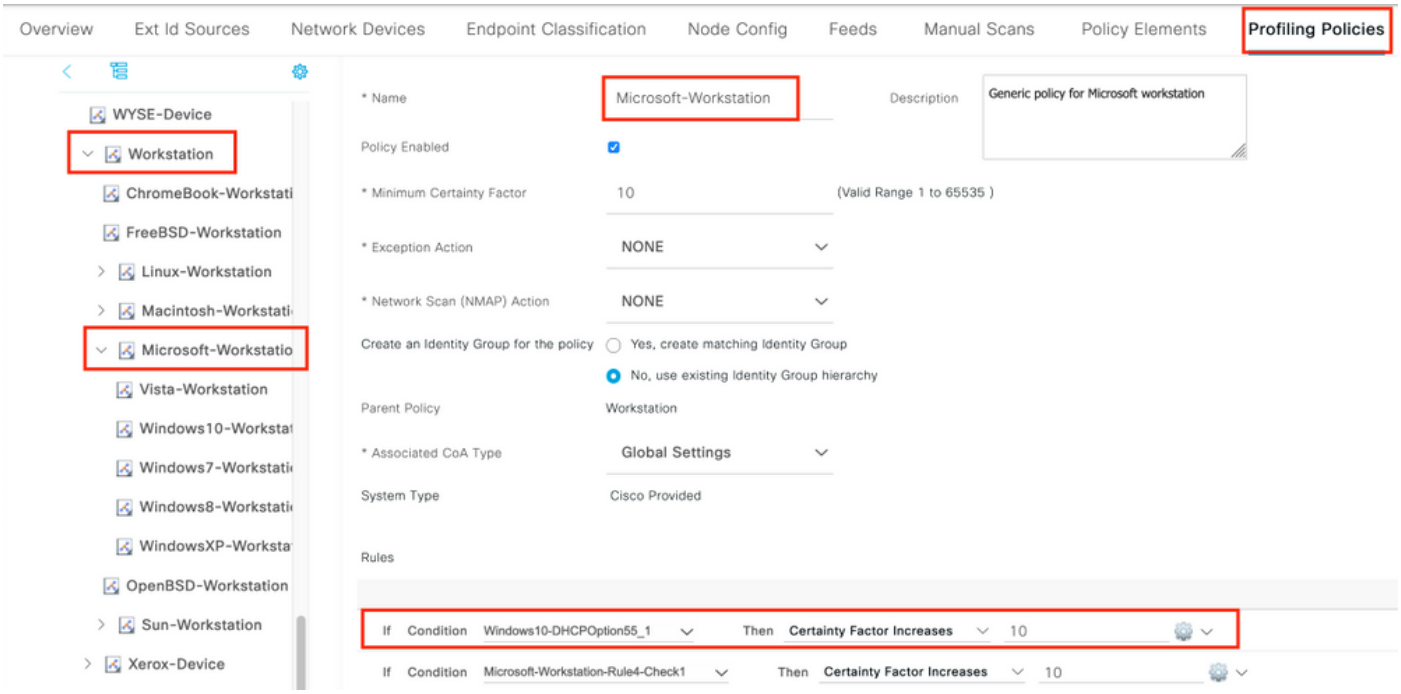
Configuration

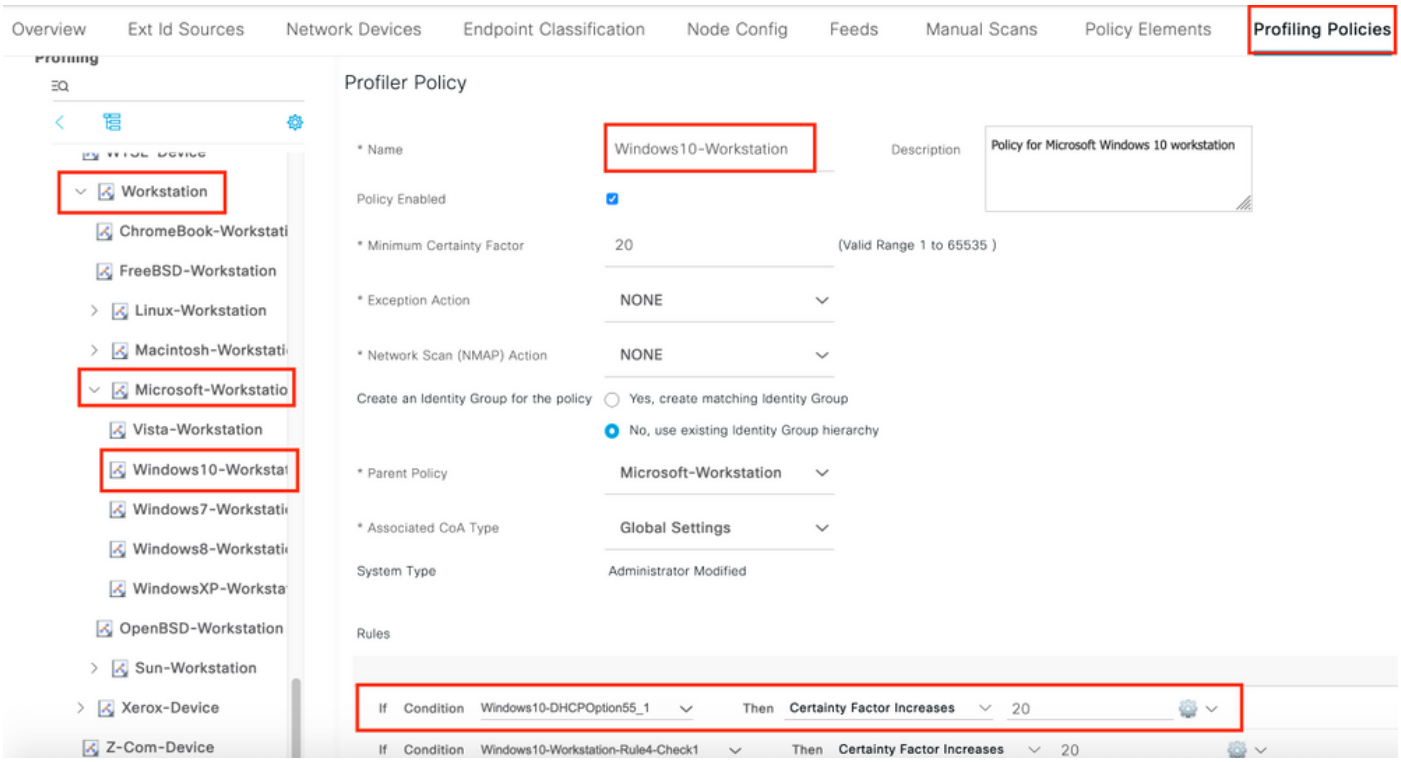
1. Connectez-vous à l'interface utilisateur de l'administrateur ISE et accédez à **Policy > Policy Elements > Conditions > Profilage**. Cliquez sur **Ajouter** afin d'ajouter une nouvelle condition de profilage personnalisée. Dans cet exemple, nous utilisons les empreintes digitales de la liste de requêtes de paramètres Windows 10. Reportez-vous à Fingerbank.org pour obtenir une liste complète des valeurs de la liste de requêtes de paramètres.
   Note: La zone de texte **Valeur d'attribut** n'affiche peut-être pas toutes les options numériques et vous devrez peut-être faire défiler la liste à l'aide de la souris ou du clavier.



2. Lorsque les conditions personnalisées sont définies, accédez à **Stratégie > Profilage > Stratégies de profilage** afin de modifier une stratégie de profilage actuelle ou d'en configurer une nouvelle. Dans cet exemple, les stratégies par défaut **Workstation, Microsoft-Workstation, Windows10-Workstation** sont modifiées afin d'inclure les nouvelles conditions de liste de demandes de paramètres. Ajoutez une nouvelle condition composée à la règle de stratégie du profileur de **station de travail, Microsoft-Workstation et Windows10-Workstation** comme indiqué ci-dessous. Modifiez le **facteur de certitude** au besoin afin d'obtenir le résultat de profilage souhaité.





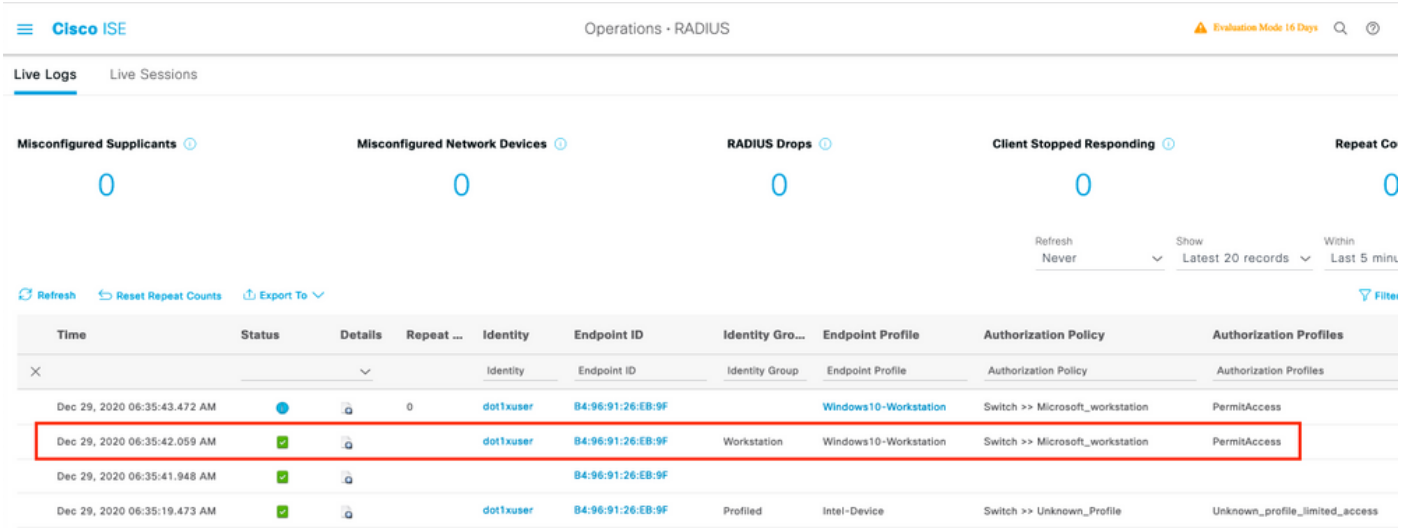


Note: Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Vérification

Étape 1-

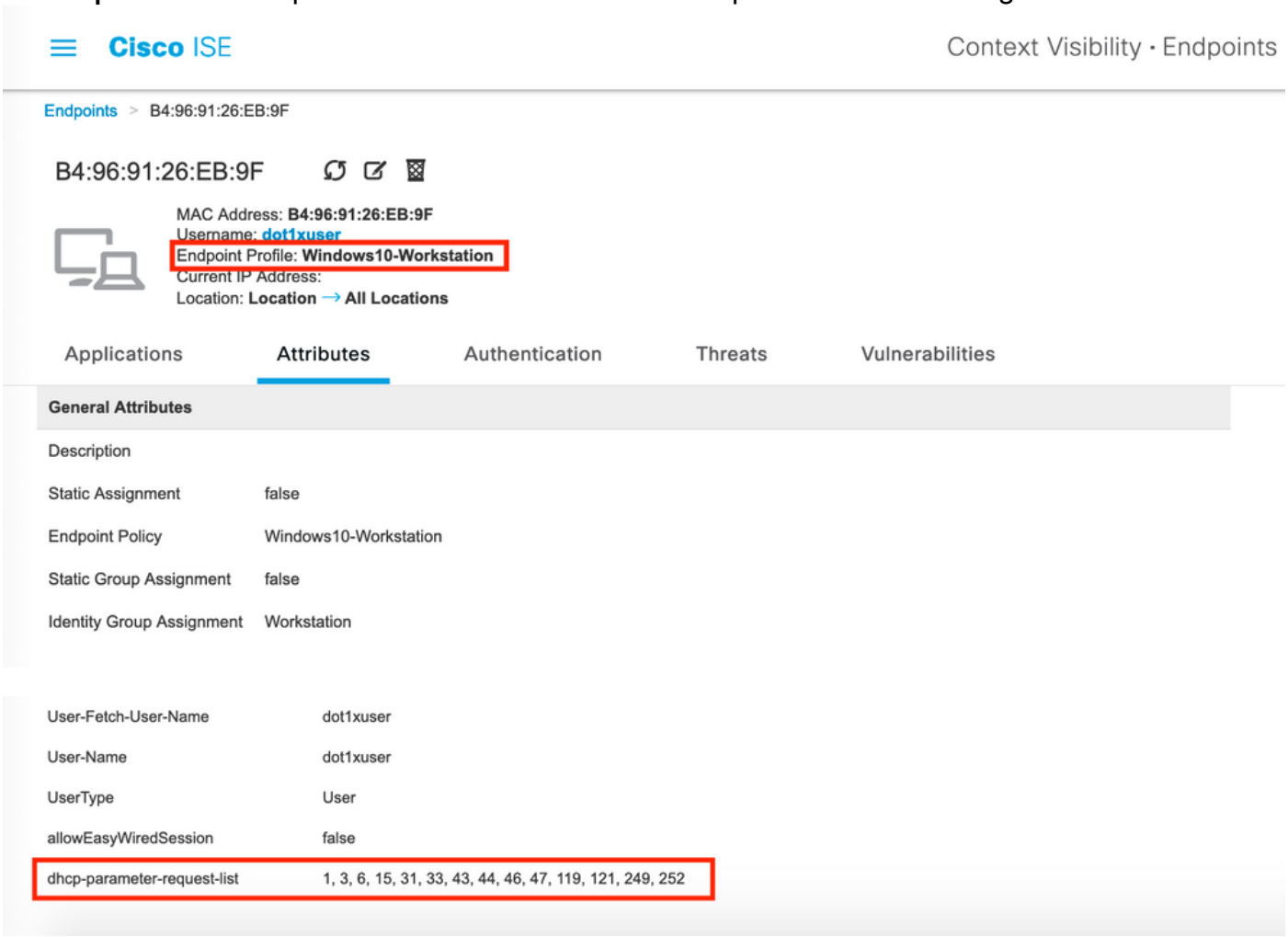
Accédez à ISE > Operations > Live Logs . La première authentification correspond à la politique d'autorisation inconnue et un accès limité est accordé à ISE . Une fois le périphérique profilé , ISE déclenche la CoA et une autre demande d'authentification est reçue sur ISE et correspond au nouveau profil - Station de travail Windows10 .



Étape 2-

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

- Accédez à **Visibilité contextuelle > Terminaux,** recherchez le terminal, cliquez sur Modifier.
- Vérifiez que **EndPointPolicy** est Window10-Workstation et que les valeurs **dhcp-paramètre-request-list** correspondent aux valeurs de condition précédemment configurées.



Dépannage

Cette section fournit les informations que vous pouvez utiliser pour dépanner votre configuration.

- Vérifiez que les paquets DHCP ont atteint les noeuds de stratégie ISE qui exécutent la fonction de profilage (avec adresse d'assistance ou SPAN).
- Utilisez l'outil **Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump** ? afin d'exécuter nativement les captures TCP Dump à partir de l'interface utilisateur de l'administrateur ISE.
- Activer les débogages ci-dessous sur le noeud PSN ISE - -nsf-nsf-session- Répertoire de session allégé-profiler-runtime-AAA
- Profiler.log, prrt-server.log et lsd.log montrent les informations pertinentes.
- Reportez-vous à la base de données d'empreintes DHCP Fingerbank.org pour obtenir la liste actuelle des options de liste de requêtes de paramètres.
- Assurez-vous que les valeurs correctes de la liste de requêtes de paramètres sont configurées dans les conditions de profilage ISE. Parmi les chaînes les plus utilisées, citons :

Note: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de débogage.

Analyse des journaux

++Activer les débogages ci-dessous sur le noeud PSN ISE -

-nsf

-nsf-session

- Répertoire de session allégé

-profiler

-runtime-AAA

++Authentification initiale

++prrt-server.log

++Requête d'accès reçue sur le noeud ISE

Radius,2020-12-29 06:35:19,377,DEBUG,0x7f1cdcbd2700,cntx=0001348461,ses=isee30-primary/3 97791910/625, CallingStationID=B4-96-91-26-EB-9F, **PAQUET RADIUS : Code=1(AccessRequest)** Identificateur=182 Longueur=285

++ISE correspond au profil inconnu

AcsLogs,2020-12-29 06:35:19,473, DEBUG,0x7f1cdc7ce700, cntx=0001348476, ssen=isee30-primary/3 97791910/625, CPMSessionID=0A6A270B00000018B44013AC, user=dot1xuser, CallingStationID=B4-96-91-26 EB-9F, **AuthorizationPolicyMatchedRule=Unknown_Profile**, EapTunnel=EAP-FAST, EapAuthentication=EAP-MSCHAPv2, UserType=User, CPMSessionID=0A6A270B00000018B440 13AC, EndPointMACAddress=B4-96-91-26-EB-9F,

++ISE envoie l'accès Accepter avec un accès limité

Radius,2020-12-29 06:35:19,474,DEBUG,0x7f1cdc7ce700,cntx=0001348476,ssen=isee30-

primary/3977 791910/625, CPMSessionID=0A6A270B0000018B44013AC, user=dot1xuser, CallingStationID=B4-96-91-26-EB-9F, PAQUET RADIUS : **Code=2(AccessAccept)** Identificateur=186 Longueur=331

++ISE a reçu la mise à jour de comptabilité avec les informations DHCP

Radius,2020-12-29 06:35:41,464,DEBUG,0x7f1cdcad1700,cntx=0001348601,ssen=isee30-primary/397 791910/627, CPMSessionID=0A6A270B0000018B44013AC, CallingStationID=B4-96-91-26-EB-9F, PAQUET RADIUS : **Code=4(AccountingRequest)** Identificateur=45 Longueur=381

[1] Nom d'utilisateur - valeur : [dot1xuser]

[87] NAS-Port-Id - valeur : [GigabitEthernet1/0/13]

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

[26] cisco-av-pair - valeur : [audit-session-id=**0A6A270B00000018B44013AC**]

++ISE renvoie la réponse de comptabilité

Radius,2020-12-29 06:35:41,472,DEBUG,0x7f1cdc5cc700,cntx=0001348601,ssen=isee30-primary/397 791910/627, CPMSessionID=0A6A270B0000018B44013AC, user=dot1xuser, CallingStationID=B4-96-91-26-EB-9F, PAQUET RADIUS : **Code=5(AccountingResponse)** Identifier=45 Longueur=20, RADIUSHandler.cpp:2216

++Profiler.log

++Une fois la mise à jour de comptabilité reçue avec l'option DHCP dhcp-paramètre-request-list , ISE commence à profiler le périphérique

2020-12-29 06:35:41,470 DEBUG [SyslogListenerThread][] cisco.profiler.probes.radius.SyslogDefragmenter -:::- **parseHeader inBuffer**=<181>Dec9 06:35:41 isee30-primary CISE_RADIUS_Accounting 000000655 2 0 2020-12-29 06:35:41.467 +00:00 000234 376 3002 AVIS **Radius-Accounting : Mise à jour du chien de garde de la comptabilité RADIUS**, ConfigVersionId=99, Device IP Address=10.106.39.11, UserName=dot1xuser, RequestLatency=6, NetworkDeviceName=Sw, User-Name=dot1xuser, NAS-IP-Address=10.16.39 11, NAS-Port=50113, Class=CACS:0A6A270B00000018B44013AC:isee30-primary/39791910/625, station appelée ID=A0-EC-F9-3C-82-0D, Calling-Station-ID=B4-96-91-26-EB-9F, NAS-Identifier=Commutateur, Acct-Status-Type=Progress-Update, Acct-Delay-Time=0, Acct-Input-Octets=174, Acct-Output-Octets=0, Acct-Session-Id=000000b, Acct-Authentic=Remote, Acct-Input-Packets=1, Acct-Output-Packets=0, Event-Timestamp=1609341899, NAS-Port-Type=Ethernet, NAS-Port-Id=GigabitEthernet1/0/13 **cisco-av-pair=dhcp-option=dhcp-paramètre-request-list=1\, 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 -::- **Parsed IOS Sensor 1 : dhcp-paramètre-request-list=[1, 3, 6, 15, 31, 33, 43, 44, 46, 47, 119, 121, 249, 252]**

Attribut : cisco-av-pair value : dhcp-option=dhcp-paramètre-request-list=1\, 3\, 6\, 15\, 31\, 33\, 43\, 44\, 46\, 47\, 119\, 121\, 249\, 252,-session-id=0A6A270B00000018B44013AC, méthode=dot1x

Attribut : dhcp-paramètre-request-list value : 1, 3, 6, 15, 31, 33, 43, 44, 46, 47, 119, 121, 249, 252

2020-12-29 06:35:41,479 DEBUG [RMQforwarder-4][]
cisco.profiler.infrastructure.cache.AbstractEndpointCache -:B4:96:91:26:EB:9F:12413 370-49a0-11eb-b713-1a99022ed3c5:ProfilerCollection:- **Propriétaire de ce Mac : B4:96:91:26:EB:9F est 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:1241370-49a0-11eb-b713-1a99022ed3c5:ProfilerCollection:- **propriétaire actuel du point de terminaison B4:96:91:26:EB:9Fis isee30-primary.anshsinh.local et code de message 30000000000000000000 2**

2020-12-29 06:35:41,479 DEBUG [RMQforwarder-4][]
cisco.profiler.infrastructure.probemgr.Forwarder -:B4:96:91:26:EB:9F:124137 0-49a0-11eb-b713-1a99022ed3c5:ProfilerCollection:- **est la source de terminal radius true**

++Nouveau attribut

2020-12-29 06:35:41,480 DEBUG [RMQforwarder-4][]
cisco.profiler.infrastructure.probemgr.Forwarder -:B4:96:91:26:EB:9F:1241370-49a0-11eb-b713-1a99022ed3c5:ProfilerCollection:- **Nouvel attribut : dhcp-paramètre-request-list**

2020-12-29 06:35:41,482 DEBUG [RMQforwarder-4][]
cisco.profiler.infrastructure.probemgr.Forwarder -:B4:96:91:26:EB:9F:124137 0-49a0-11eb-b713-1a99022ed3c5:ProfilerCollection:- Jeu d'attributs modifié de point de terminaison :

2020-12-29 06:35:41,482 DEBUG [RMQforwarder-4][]
cisco.profiler.infrastructure.probemgr.Forwarder -:B4:96:91:26:EB:9F:1241370-49a0-11eb-b713-1a99022ed3c5 : **ProfilerCollection :- dhcp-paramètre-request-list,**

++Différentes règles sont associées à un facteur de certitude différent

2020-12-29 06:35:41,484 DEBUG [RMQforwarder-4][]
cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:124133 70-49a0-11eb-b713-1a99022ed3c5 : **Profilage : - Politique Appareils Intel B4:96:91:26:EB:9F (certitude 5)**

2020-12-29 06:35:41,485 DEBUG [RMQforwarder-4][]
cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:124133 70-49a0-11eb-b713-1a99022ed3c5 : **Profilage : - Station de travail de stratégie appariée B4:96:91:26:EB:9F (certitude 10)**

2020-12-29 06:35:41,486 DEBUG [RMQforwarder-4][]
cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:124133 70-49a0-11eb-b713-1a99022ed3c5 : **Profilage : - Politique Microsoft-Workstation appariée B4:96:91:26:EB:9F (certitude 10)**

2020-12-29 06:35:41,487 DEBUG [RMQforwarder-4][]
cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:124133 70-49a0-11eb-b713-1a99022ed3c5**:Profilage : - Stratégie Windows10-Workstation appariée B4:96:91:26:EB:9F (certitude 20)**

++Windows10-Workstation a le facteur de certitude le plus élevé de 40 en fonction de la configuration et donc cela fait office de profil de point de terminaison pour le périphérique

2020-12-29 06:35:41,487 DEBUG [RMQforwarder-4][]

cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:124133 70-49a0-11eb-b713-1a99022ed3c5 :Profilage : - **Après analyse de la hiérarchie des politiques : Point de terminaison : B4:96:91:26:EB:9F EndpointPolicy:Windows10-Workstation for:40 ExceptionRuleMatched:false**

2020-12-29 06:35:41,487 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:124133 70-49a0-11eb-b713-1a99022ed3c5 : **Profilage : - Point de terminaison B4:96:91:26:EB:9F Politique correspondante modifiée.**

2020-12-29 06:35:41,489 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:124133 70-49a0-11eb-b713-1a99022ed3c5 : **Profilage : - Point de terminaison B4:96:91:26:EB:9F IdentityGroup modifié.**

2020-12-29 06:35:41,489 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:124133 70-49a0-11eb-b713-1a99022ed3c5 : **Profilage : - Définition de l'ID de groupe d'identité sur le point de terminaison B4:96:91:26:EB:9F - 3b76f840-8c00-11e6 996c-525400b48521**

2020-12-29 06:35:41,489 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:124133 70-49a0-11eb-b713-1a99022ed3c5:Profilage:- **Appel du cache de point d'extrémité avec le point d'extrémité profilé B4:96:91:26:EB:9F, stratégie Windows10-Workstation, stratégie correspondante Windows10-Station de travail**

2020-12-29 06:35:41,489 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:124133 70-49a0-11eb-b713-1a99022ed3c5 : **Profilage : - Envoi d'événement pour persister point d'extrémité B4:96:91:26:EB:9F, et code de message ep = 3002**

2020-12-29 06:35:41,489 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:124133 70-49a0-11eb-b713-1a99022ed3c5 : **Profilage : - Point de terminaison B4:96:91:26:EB:9F IdentityGroup / Profil logique modifié. Émission d'une CoA conditionnelle**

2020-12-29 06:35:41,489 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiler.ProfilerManager -:B4:96:91:26:EB:9F:124133 70-49a0-11eb-b713-1a99022ed3c5 :Profilage :- **ConditionalCoAEvent avec détails du point de terminaison : EndPoint[id=ff19ca00-499f-11eb-b713-1a99022ed3c5, name=<null>]**

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

Attribut:Valeur Calling-Station-ID:B4-96-91-26-EB-9F

Attribut : Valeur EndPointMACAddress : B4-96-91-26-EB-9F

Attribut : valeur MACAddress : B4:96:91:26:EB:9F

++Envoi des données au répertoire de la session la plus claire

20-12-29 06:35:41,489 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.probemgr.**LSDForwarderHelper** -:::- Endpoint.B4:96:91:26 BE:9F **correspondant à Windows10-Workstation**

2020-12-29 06:35:41,489 DEBUG [RMQforwarder-4][]
cisco.profiler.infrastructure.probemgr.**LSDForwarderHelper -:::- Envoi d'un événement à un point de terminaison persist tout en ajoutant pour LSD pour forwarder,default us, par défaut B4:96:91:26:EB:9F**

++La CoA globale est sélectionnée en tant que Réalité

2020-12-29 06:35:41,489 DEBUG [CoAHandler-52-thread-1][]
cisco.profiler.infrastructure.profiler.CoAHandler -:B4:96:91:26:EB:9F:9fe 38b30-43ea-11eb-b713-1a99022ed3c5 : **ProfilerCoA :- Type de commande CoA globale configuré = Réalité**

2020-12-29 06:35:41,490 DEBUG [RMQforwarder-4][]
cisco.profiler.infrastructure.cache.AbstractEndpointCache -:B4:96:91:26:EB:9F:12413 370-49a0-11eb-b713-1a99022ed3c5 ::- **Mise à jour du point d'extrémité - EP à partir de l'entrée : B4:96:91:26:EB:9FepSource : SGA de sonde RADIUS : falseSG : Station de travail**

2020-12-29 06:35:41,490 DEBUG [RMQforwarder-4][]
cisco.profiler.infrastructure.cache.AbstractEndpointCache -:B4:96:91:26:EB:9F:12413 370-49a0-11eb-b713-1a99022ed3c5 ::- **Mise à jour du point d'extrémité - EP après fusion : B4:96:91:26:EB:9FepSource : SGA de sonde RADIUS : falseSG:Windows10-Workstation**

++ISE correspond à la stratégie pour vérifier si doit envoyer CoA . ISE ne déclenchera CoA que s'il a une politique correspondant à la modification du profil

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 :- Traiter toute stratégie disponible dans Commutateur de jeu de stratégies d'exception local, policy status=ENABLED**

2020-12-29 06:35:41,701 DEBUG [CoAHandler-52-thread-1][]
cisco.profiler.infrastructure.profiler.CoAHandler -:B4:96:91:26:EB:9F:9fe 38b30-43ea-11eb-b713-1a99022ed3c5 : **ProfilerCoA : - Nom de la politique : État de la stratégie de commutateur : ACTIVÉE**

2020-12-29 06:35:41,702 DEBUG [CoAHandler-52-thread-1][]
cisco.profiler.infrastructure.profiler.CoAHandler -:B4:96:91:26:EB:9F:9fe 38b30-43ea-11eb-b713-1a99022ed3c5 : **ProfilerCoA :- lhsvalue name 6d954800-8bff-11e6-996c-5254 00b48521 rhs operandID 42706690-8c00-11e6-996c-525400b48521 rhsvaluename Workstation:Microsoft-Workstation:Windows10-Workstation**

2020-12-29 06:35:41,933 DEBUG [CoAHandler-52-thread-1][] com.cisco.profiler.api.Util -:B4:96:91:26:EB:9F:9fe38b 30-43ea-11eb-b713-1a99022ed3c5 : **ProfilerCoA :- Condition spécifiée DISPONIBLE dans la politique d'autorisation**

2020-12-29 06:35:41,933 DEBUG [CoAHandler-52-thread-1][] com.cisco.profiler.api.Util -:B4:96:91:26:EB:9F:9fe38b 30-43ea-11eb-b713-1a99022ed3c5 : **ProfilerCoA : - Politique d'autorisation HAVING Politique : 42706690-8c00-11e6-996c-525400b48521**

++La stratégie d'autorisation correspond à cette condition et la CoA est déclenchée

2020-12-29 06:35:41,935 DEBUG [CoAHandler-52-thread-1][]
cisco.profiler.infrastructure.profiler.CoAHandler -:B4:96:91:26:EB:9F:9fe 38b30-43ea-11eb-b713-1a99022ed3c5 : **ProfilerCoA : - ApplyCoa : Descripteur créé en fonction des attributs RADIUS du**

point de terminaison :

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

ID de session : [0A6A270B00000018B44013AC]

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

Interface AAA : [10.106.32.119]

Adresse IP NAD : [10.106.39.11]

ID de port NAS : [GigabitEthernet1/0/13]

Type de port NAS : [Ethernet]

Type de service : [Cadre]

Est sans fil : [faux]

Est VPN : [faux]

Est MAB : [faux]

2020-12-29 06:35:41,938 DEBUG [CoAHandler-52-thread-1][]
cisco.profiler.infrastructure.profiler.CoAHandler -:B4:96:91:26:EB:9F:9fe 38b30-43ea-11eb-b713-1a99022ed3c5 : **ProfilerCoA : - Sur le point d'appeler CoA pour et IP : 10.106.39.11 pour le point de terminaison : B4:96:91:26:EB:9F Commande CoA : Réalité**

2020-12-29 06:35:41,938 DEBUG [CoAHandler-52-thread-1][]
cisco.profiler.infrastructure.profiler.CoAHandler -:B4:96:91:26:EB:9F:9fe 38b30-43ea-11eb-b713-1a99022ed3c5 : **ProfilerCoA :- Application de CoA-REAUTH par serveur AAA : 10.106.32.119 via l'interface : 10.106.32.119 à NAD : 10.106.39.11**

2020-12-29 06:35:41,949 DEBUG [SyslogListenerThread][]
cisco.profiler.probes.radius.SyslogDefragmenter -:::- parseHeader inBuffer=<181>Dec 2906:3 5:41 isee30-primary CISE_Passed_Authentications 0000000656 2 1 StepData=2=(port = 1700 \, type = Cisco CoA), **CoASourceComponent=Profiler, CoAReason=Modification du groupe d'identités/stratégie/logique du point de terminaison profil utilisé dans les stratégies d'autorisation, CoAType=Réauthentification** - last, Network Device Profile=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 000234379 80006 **INFO Profileur : Le profileur déclenche une demande de modification d'autorisation,** ConfigVersionId=99, **EndpointCoA=Réauth,** EndpointMacAddress=B4:96:91:26:EB:9F, EndpointNADAddress=10.106.39.11, **dpointPolicy=Windows10-Workstation,** EndpointProperty=Service-Type=Framed\, MessageCode=3002\, EndPointPolicyID=42706690-8c00-11e6-996c-525400b 8521\, UseCase=\, NAS-Port-Id=GigabitEthernet1/0/13\, NAS-Port-Type=Ethernet\, Response=\{User-Name=dot1xuser\;

DynamicAuthorizationFlow,2020-12-29
06:35:41,939,DEBUG,0x7f1cdc3ca700,cntx=0001348614,[DynamicAuthorizationFlow :
:onLocalHttpEvent] Commande CoA entrante reçue :

<Réauthentifier 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>

</Réauthentifier>

++CoA envoyé -

RadiusClient,2020-12-29 06:35:41,943,DEBUG,0x7f1ccb3f3700,cntx=0001348614,ssen=39c740
88-52fd-430f-95d9-a8fe78eaa1f1, CallingStationID=B4:96:91:26:EB:9F, PAQUET RADIUS :
Code=43 (CoARequest) Identificateur=27 Longueur=225

[4] Adresse IP NAS - valeur : [10.106.39.11]

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

[87] NAS-Port-Id - valeur : [GigabitEthernet1/0/13]

[26] cisco-av-pair - valeur : [abonné : commande=réauthentifier]

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

RadiusClient,2020-12-29
06:35:41,947,DEBUG,0x7f1cdcad1700,cntx=0001348614,ssen=39c7408 8-52fd-430f-95d9-
a8fe78eaa1f1, CallingStationID=B4:96:91:26:EB:9F, PAQUET RADIUS : Code=44 (CoAACK)
Identificateur=27

++Nouvelle demande d'accès

Radius,2020-12-29 06:35:41,970,DEBUG,0x7f1cdc6cd700,cntx=0001348621,seses=isee30-
primary/397 791910/628, CallingStationID=B4-96-91-26-EB-9F, PAQUET RADIUS :
Code=1(AccessRequest) Identificateur=187 Longueur=285

++ISE correspond au nouveau profil d'autorisation correspondant à la stratégie de point de terminaison du périphérique de point de terminaison

AcsLogs,2020-12-29 06:35:42,060, DEBUG,0x7f1cdcad1700, cntx=0001348636, sens=isee30-primary 397791910/628, CPMSessionID=0A6A270B00000018B44013AC, user=dot1xuser, CallingStationID=B4-96-91-26 -EB-9FIdentityPolicyMatchedRule=Par défaut, **AuthorizationPolicyMatchedRule=Microsoft_workstation,** EapTunnel=EAP-FAST, EapAuthentication=EAP-MSCHAPv2, UserType=Utilisateur, CPMSessionID=0A6A270B00000 018B44013AC, EndPointMACAddress=B4-96-91-26-EB-9F, PostureAssessmentStatus=Sans objet, **EndPointMatchedProfile=Station de travail Windows10,**

++Accept d'accès envoyé -

Radius,2020-12-29 06:35:42,061,DEBUG,0x7f1cdcad1700,cntx=0001348636,ssen=isee30-primary/397 791910/628, CPMSessionID=0A6A270B00000018B44013AC, user=dot1xuser, CallingStationID=B4-96-91-26-EB-9F , PAQUET RADIUS : **Code=2(AccessAccept)** Identificateur=191 Longueur=340

Informations connexes

- Base de données d'empreintes digitales DHCP Fingerbank.org
- Support et documentation techniques - Cisco Systems