

Configurez la détection et l'application anormales de point final sur ISE 2.2

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations](#)

[Étape 1. Détection anormale d'enable.](#)

[Étape 2. Configurez la stratégie d'autorisation.](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

Introduction

Ce document décrit la détection et l'application anormales de point final. C'est une nouvelle fonctionnalité introduite de profilage dans le Logiciel Cisco Identity Services Engine (ISE) pour la visibilité améliorée de réseau.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de câble de dérivation d'authentification MAC (MAB) sur le commutateur
- Configuration Sans fil de MAB sur le contrôleur LAN Sans fil (WLC)
- Modification de configuration de l'autorisation (CoA) sur les deux périphériques

[Composants utilisés](#)

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

1. Cisco Identity Services Engine 2.2

2. Contrôleur LAN Sans fil 8.0.100.0
3. Commutateur Cisco Catalyst 3750 15.2(3)E2
4. Windows 10 avec les adaptateurs de câble et Sans fil

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

ISE peut détecter les points finaux qui sont impliqués dans la mystification d'adresse MAC. Une fois qu'il est détecté, ISE peut agir (avec le CoA) et imposer certaines stratégies pour limiter l'accès du point final méfiant.

Une fois que la détection est activée, ISE surveille n'importe quelles nouvelles informations reçues pour des points finaux existants et vérifie si ces attributs ont changé :

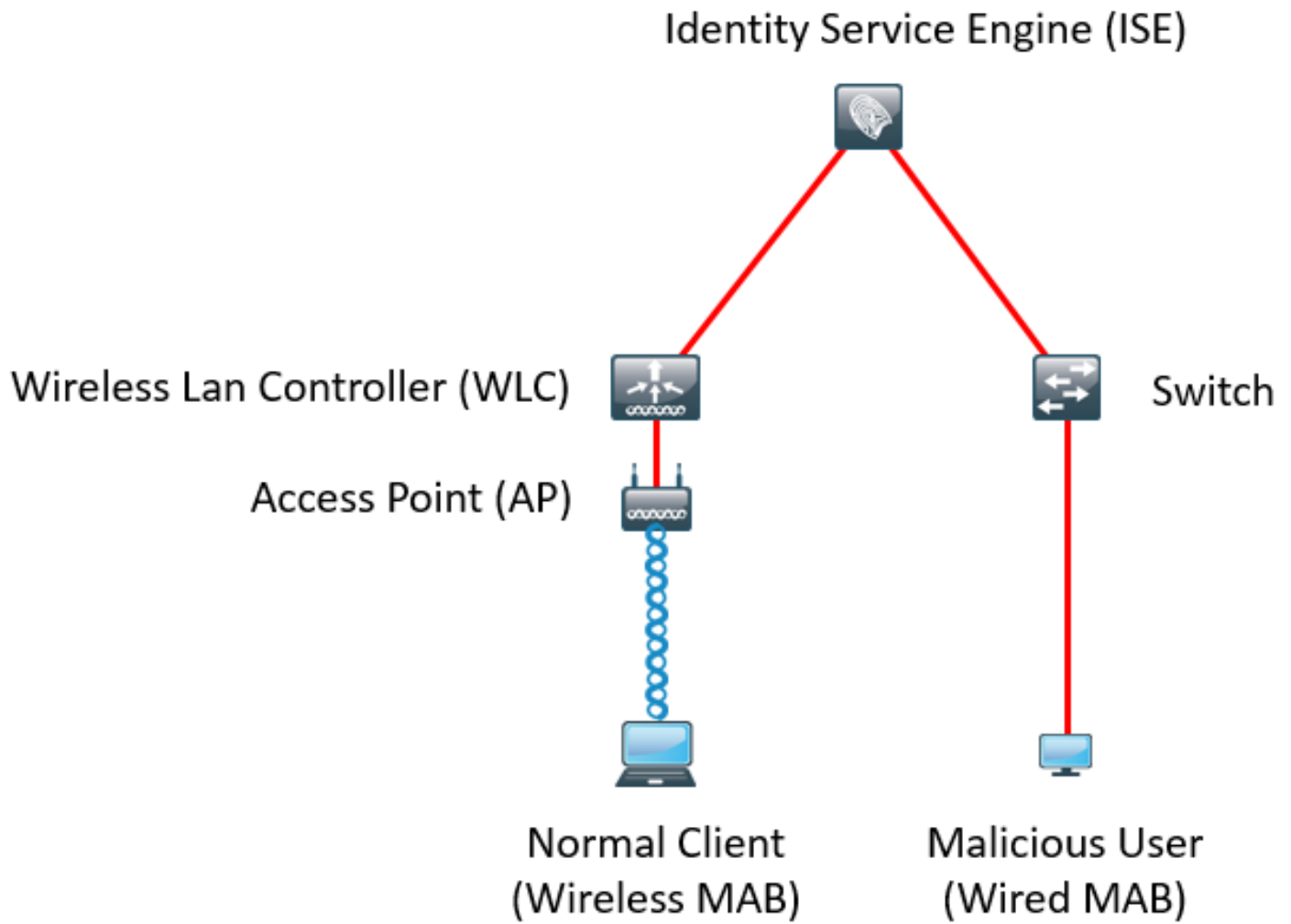
1. **Nas-Port-type** - Détermine si la méthode d'accès de ce point final a changé. Par exemple, si la même adresse MAC qui s'est connectée par l'intermédiaire du dot1x de câble est utilisée pour le dot1x Sans fil et le visa-versa.
2. **ID de classe DHCP** - Détermine si le type du client/de constructeur de point final a changé. Ceci s'applique seulement quand l'attribut d'ID de classe DHCP est rempli avec une certaine valeur et est puis changé à une autre valeur. Si un point final est configuré avec un IP statique, l'attribut d'ID de classe DHCP ne sera pas rempli sur ISE. Plus tard, si un autre périphérique charrie l'adresse MAC et utilise le DHCP, l'ID de classe changera d'une valeur vide en une chaîne spécifique. Ceci ne déclenchera pas la détection de comportement d'Anomalous.
3. **Stratégie de point final** - Modifications cruciales de profil. Par exemple, une modification de **téléphone** ou d'**imprimante au poste de travail**.

Une fois qu'ISE détecte une des modifications mentionnées ci-dessus, l'attribut d'AnomalousBehaviour est ajouté au point final et au positionnement pour rectifier. Ceci peut être utilisé plus tard comme une condition dans des stratégies d'autorisation pour limiter l'accès pour le point final dans de futures authentifications.

Si l'application est configurée, ISE peut envoyer un CoA une fois que la modification est détectée pour authentifier à nouveau ou exécuter un rebond de port pour le point final. Si en effet, il peut mettre en quarantaine le point final anormal selon les stratégies d'autorisation qui ont été configurées.

Configurez

Diagramme du réseau



Configurations

Des configurations simples de MAB et d'AAA sont exécutées sur le commutateur et le WLC. Pour utiliser cette caractéristique, suivez ces étapes :

Étape 1. Détection anormale d'enable.

Naviguez vers la **gestion > le système > les configurations > en profilant**.

Profiler Configuration

* CoA Type:

Current custom SNMP community strings: ●●●●●●

Change custom SNMP community strings: (For NMAP, comma separated. Field will be cleared on successful saved change.)

Confirm changed custom SNMP community strings: (For NMAP, comma separated. Field will be cleared on successful saved change.)

EndPoint Attribute Filter: Enabled ⓘ

Enable Anomalous Behaviour Detection: Enabled ⓘ

Enable Anomalous Behaviour Enforcement: Enabled

Le premier choix permet à ISE pour détecter n'importe quel comportement anormal mais aucun CoA n'est envoyé (mode réservé à la visibilité). La deuxième option permet à ISE pour envoyer le CoA une fois que le comportement anormal est détecté (mode d'application).

Étape 2. Configurez la stratégie d'autorisation.

Configurez l'attribut d'Anomalousbehaviour comme condition dans la stratégie d'autorisation, suivant les indications de l'image :

▼ Exceptions (1)			
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Anomalous Client	if (EndPoints:AnomalousBehaviour EQUALS true AND DEVICE:Location EQUALS All Locations)	then DenyAccess

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Normal Client	if DEVICE:Location EQUALS All Locations	then PermitAccess

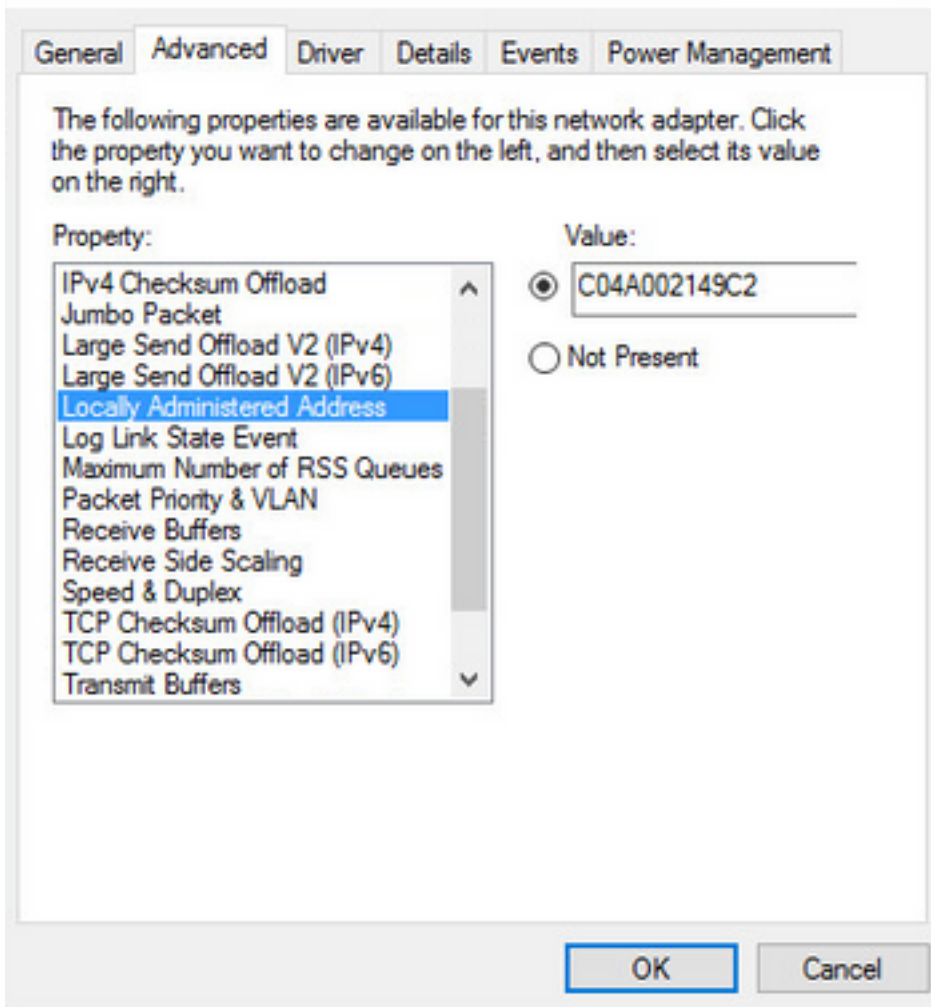
Vérifiez

Connectez à un adaptateur Sans fil. Employez la commande ipconfig /all pour trouver l'adresse MAC de l'adaptateur Sans fil, suivant les indications de l'image :

```
Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : 
Description . . . . . : 802.11n USB Wireless LAN Card
Physical Address. . . . . : C0-4A-00-21-49-C2
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::1c54:884a:33c0:bcf1%4(Preferred)
IPv4 Address. . . . . : 192.168.1.38(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Friday, December 30, 2016 5:17:12 AM
Lease Expires . . . . . : Friday, December 30, 2016 6:17:12 AM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 46156288
DHCPv6 Client DUID. . . . . : 00-01-00-01-1F-F3-74-5F-C0-4A-00-21-49-C2
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                       fec0:0:0:ffff::2%1
                       fec0:0:0:ffff::3%1
NetBIOS over Tcpi. . . . . : Enabled
```

Pour simuler un utilisateur malveillant, vous pouvez charrier l'adresse MAC de l'adaptateur Ethernet pour appairer l'adresse MAC de l'utilisateur normal.



Une fois que l'utilisateur normal se connecte, vous pouvez voir une entrée de point final dans la base de données. Après, l'utilisateur malveillant se connecte utilisant une adresse MAC charriée.

Des états vous pouvez voir la connexion initiale du WLC. Après, l'utilisateur malveillant se connecte et 10 secondes plus tard, un CoA est dû déclenché à la détection du client anormal. Puisque le type global CoA est placé à **Reauth**, les essais de point final à connecter de nouveau. ISE a déjà placé l'attribut d'AnomalousBehaviour pour rectifier ainsi ISE apparie la première règle et refuse l'utilisateur.

Logged At	RADIUS St...	Details	Identity	Endpoint ID	Authorization Rule	Network Device
2016-12-30 20:37:59.728	✘	of the following rules.	C0:4A:00:21:49:C2	C0:4A:00:21:49:C2	Anomalous Client	SW
2016-12-30 20:37:59.704	✔		C0:4A:00:21:49:C2	C0:4A:00:21:49:C2	Normal Client	SW
2016-12-30 20:37:49.614	✔		C0:4A:00:21:49:C2	C0:4A:00:21:49:C2	Normal Client	SW
2016-12-30 20:22:00.193	✔		C0:4A:00:21:49:C2	C0:4A:00:21:49:C2	Normal Client	WLC

Suivant les indications de l'image, vous pouvez voir les détails sous le point final dans l'onglet de visibilité de contexte :

C0:4A:00:21:49:C2   

MAC Address: C0:4A:00:21:49:C2
Username: c04a002149c2
Endpoint Profile: TP-LINK-Device
Current IP Address: 192.168.1.38
Location: Location → All Locations


Applications **Attributes** Authentication Threats Vulnerabilities

General Attributes

Description

Static Assignment	false
Endpoint Policy	TP-LINK-Device
Static Group Assignment	false
Identity Group Assignment	Profiled

Custom Attributes

Filter 

Attribute Name	Attribute Value
----------------	-----------------

No data found. [Add custom attributes here.](#)

Other Attributes

AAA-Server	sth-nice
AD-Last-Fetch-Time	1483130280592
Acct-Input-Gigawords	0
Acct-Output-Gigawords	0
Airespace-Wlan-Id	3
AllowedProtocolMatchedRule	MAB
AnomalousBehaviour	true










Comme vous pouvez voir, le point final peut être supprimé de la base de données pour effacer cet attribut.

Suivant les indications de l'image, le tableau de bord inclut un nouvel onglet pour afficher le nombre de clients montrant ce comportement :

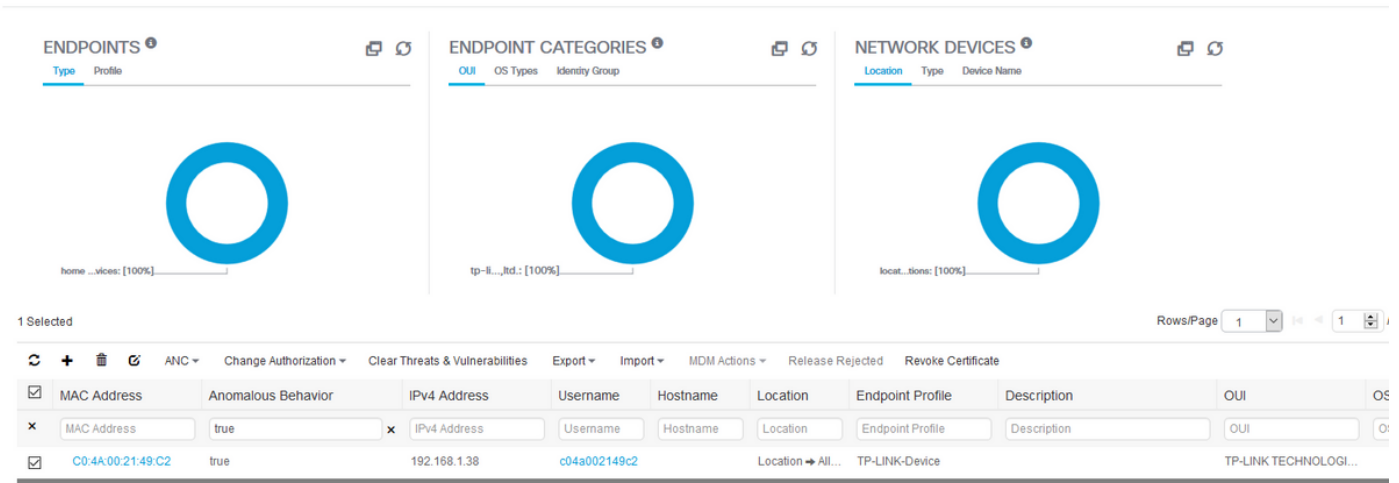
Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

Summary Endpoints Guests Vulnerability Threat +

METRICS

Total Endpoints 	Active Endpoints 	Rejected Endpoints 	Anomalous Behavior 	Authenti
 1	 0	 0	 1	

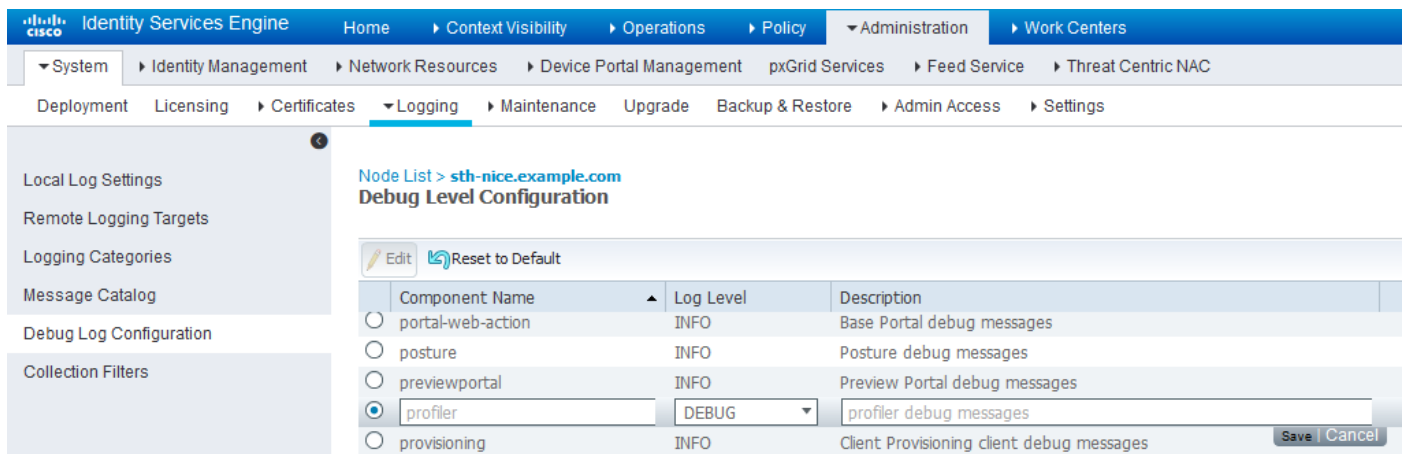
Filters: Anomalous Endpoints



MAC Address	Anomalous Behavior	IPv4 Address	Username	Hostname	Location	Endpoint Profile	Description	OUI	OS
C0:4A:00:21:49:C2	true	192.168.1.38	c04a002149c2		Location -> All...	TP-LINK-Device			TP-LINK TECHNOLOGI...

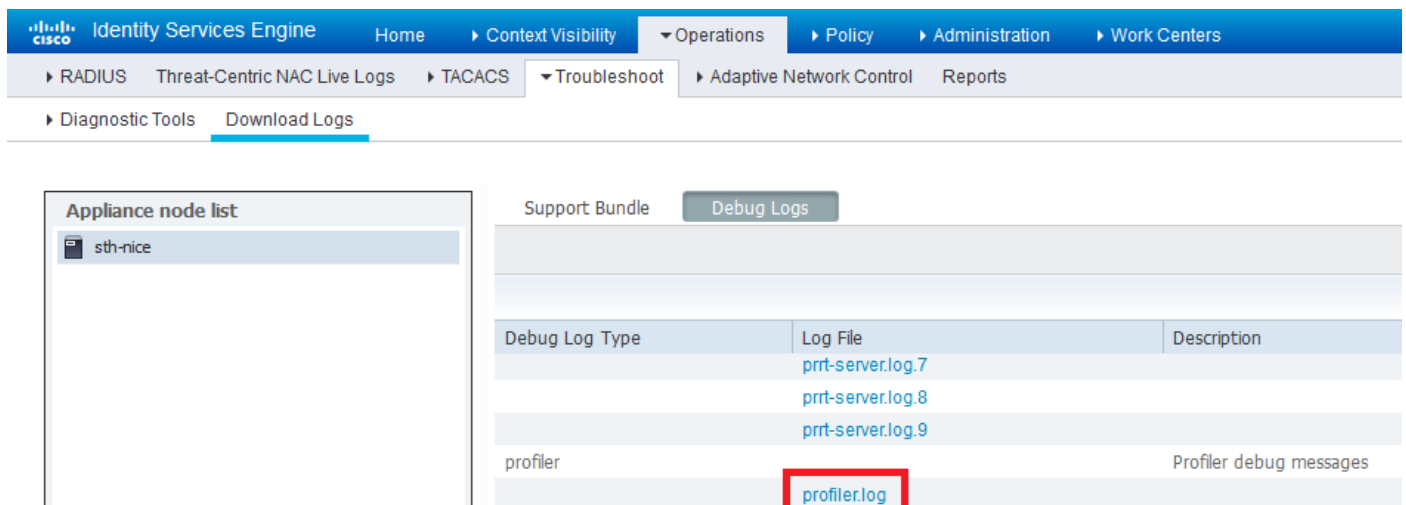
Dépannez

Afin de dépanner, le profileur d'enable mettent au point, car vous naviguez vers la **gestion > le système > se connectant > configuration de log de debug.**



Component Name	Log Level	Description
<input type="radio"/> portal-web-action	INFO	Base Portal debug messages
<input type="radio"/> posture	INFO	Posture debug messages
<input type="radio"/> previewportal	INFO	Preview Portal debug messages
<input checked="" type="radio"/> profiler	DEBUG	profiler debug messages
<input type="radio"/> provisioning	INFO	Client Provisioning client debug messages

Afin de trouver le fichier ISE **Profiler.log**, naviguez vers des **exécutions > des logs de téléchargement > des logs de debug**, suivant les indications de l'image :



Debug Log Type	Log File	Description
	prrt-server.log.7	
	prrt-server.log.8	
	prrt-server.log.9	
profiler	profiler.log	Profiler debug messages

Ces logs affichent quelques extraits à partir du fichier de **Profiling.log**. Comme vous pouvez voir, ISE pouvait détecter que le point final avec l'adresse MAC de C0:4A:00:21:49:C2 a changé la

méthode d'accès en comparant les vieilles et nouvelles valeurs des attributs de Nas-Port-type. Il est Sans fil mais est changé aux Ethernets.

```
2016-12-30 20:37:43,874 DEBUG [EndpointHandlerWorker-2-34-thread-1][[]
cisco.profiler.infrastructure.profiling.ProfilerManager -:Profiling:- Classify hierarchy
C0:4A:00:21:49:C2
2016-12-30 20:37:43,874 DEBUG [MACSpooferingEventHandler-52-thread-1][[]
profiler.infrastructure.problemgr.event.MACSpooferingEventHandler -:ProfilerCollection:- Received
AttrsModifiedEvent in MACSpooferingEventHandler MAC: C0:4A:00:21:49:C2
2016-12-30 20:37:49,618 DEBUG [MACSpooferingEventHandler-52-thread-1][[]
profiler.infrastructure.problemgr.event.MACSpooferingEventHandler -:ProfilerCollection:- Received
AttrsModifiedEvent in MACSpooferingEventHandler MAC: C0:4A:00:21:49:C2
2016-12-30 20:37:49,618 INFO [MACSpooferingEventHandler-52-thread-1][[]
com.cisco.profiler.api.MACSpooferingManager -:ProfilerCollection:- Anomalous Behaviour Detected:
C0:4A:00:21:49:C2 AttrName: NAS-Port-Type Old Value: Wireless - IEEE 802.11 New Value: Ethernet
2016-12-30 20:37:49,620 DEBUG [MACSpooferingEventHandler-52-thread-1][[]
cisco.profiler.infrastructure.cache.EndPointCache -:ProfilerCollection:- Updating end point: mac
- C0:4A:00:21:49:C2
2016-12-30 20:37:49,621 DEBUG [MACSpooferingEventHandler-52-thread-1][[]
cisco.profiler.infrastructure.cache.EndPointCache -:ProfilerCollection:- Reading significant
attribute from DB for end point with mac C0:4A:00:21:49:C2
2016-12-30 20:37:49,625 DEBUG [MACSpooferingEventHandler-52-thread-1][[]
profiler.infrastructure.problemgr.event.EndpointPersistEventHandler -:ProfilerCollection:- Adding
to queue endpoint persist event for mac: C0:4A:00:21:49:C2
```

Par conséquent, ISE agit puisque l'application est activée. L'action ici est d'envoyer un CoA selon la configuration globale dans les configurations de profilage mentionnées ci-dessus. Dans notre exemple, le type CoA est placé à Reauth qui permet à ISE pour authentifier à nouveau le point final et pour vérifier les règles qui ont été configurées. Cette fois, il apparie la règle anormale de client et donc on lui refuse.

```
2016-12-30 20:37:49,625 INFO [MACSpooferingEventHandler-52-thread-1][[]
profiler.infrastructure.problemgr.event.MACSpooferingEventHandler -:ProfilerCollection:- Taking mac
spoofering enforcement action for mac: C0:4A:00:21:49:C2
2016-12-30 20:37:49,625 INFO [MACSpooferingEventHandler-52-thread-1][[]
profiler.infrastructure.problemgr.event.MACSpooferingEventHandler -:ProfilerCollection:- Triggering
Delayed COA event. Should be triggered in 10 seconds
2016-12-30 20:37:49,625 DEBUG [CoAHandler-40-thread-1][[]
cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:- Received CoAEvent
notification for endpoint: C0:4A:00:21:49:C2
2016-12-30 20:37:49,625 DEBUG [CoAHandler-40-thread-1][[]
cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:- Configured Global CoA command
type = Reauth
2016-12-30 20:37:49,626 DEBUG [CoAHandler-40-thread-1][[]
cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:- Received
FirstTimeProfileCoAEvent for endpoint: C0:4A:00:21:49:C2
2016-12-30 20:37:49,626 DEBUG [CoAHandler-40-thread-1][[]
cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:- Wait for endpoint:
C0:4A:00:21:49:C2 to update - TTL: 1
2016-12-30 20:37:49,626 DEBUG [CoAHandler-40-thread-1][[]
cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:- Setting timer for endpoint:
C0:4A:00:21:49:C2 to: 10 [sec]
2016-12-30 20:37:49,626 DEBUG [CoAHandler-40-thread-1][[]
cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:- Rescheduled event for
endpoint: C0:4A:00:21:49:C2 to retry - next TTL: 0
2016-12-30 20:37:59,644 DEBUG [CoAHandler-40-thread-1][[]
cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:- About to call CoA for nad IP:
10.62.148.106 for endpoint: C0:4A:00:21:49:C2 CoA Command: Reauth
2016-12-30 20:37:59,645 DEBUG [CoAHandler-40-thread-1][[]
cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:- Applying CoA-REAUTH by AAA
```


Server: 10.48.26.89 via Interface: 10.48.26.89 to NAD: 10.62.148.106

[Informations connexes](#)

- [Guide d'administration ISE 2.2](#)