Configuration de la détection et de l'application des terminaux anormaux sur ISE 2.2

Contenu

Introduction

Ce document décrit la détection et l'application des points de terminaison anormaux. Il s'agit d'une nouvelle fonctionnalité de profilage introduite dans Cisco Identity Services Engine (ISE) pour une visibilité accrue du réseau.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration MAB (Wired MAC Authentication Bypass) sur le commutateur
- Configuration MAB sans fil sur le contrôleur LAN sans fil (WLC)
- Modification de la configuration d'autorisation (CoA) sur les deux périphériques

Components Used

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

1. 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 cartes filaires et sans fil

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

La fonction de détection des points de terminaison anormaux permet à ISE de surveiller les modifications apportées à des attributs et des profils spécifiques pour les points de terminaison connectés. Si une modification correspond à une ou plusieurs règles de comportement anormal préconfigurées, ISE marquera le point de terminaison comme Anomaleux. Une fois détecté, ISE peut prendre des mesures (avec CoA) et appliquer certaines stratégies pour restreindre l'accès au point de terminaison suspect. L'un des cas d'utilisation de cette fonctionnalité inclut la détection de l'usurpation d'adresse MAC.

- Note: Cette fonctionnalité ne traite pas tous les scénarios potentiels d'usurpation d'adresse MAC. Assurez-vous de lire les types d'anomalies couverts par cette fonctionnalité pour déterminer son applicabilité à vos cas d'utilisation.

Une fois la détection activée, ISE surveille toutes les nouvelles informations reçues pour les terminaux existants et vérifie si ces attributs ont changé :

1. **NAS-Port-Type** - Détermine si la méthode d'accès de ce point de terminaison a changé. Par exemple, si la même adresse MAC que celle connectée via Wired Dot1x est utilisée pour les connexions sans fil Dot1x et visa-versa.

2. **ID de classe DHCP** - Détermine si le type de client/fournisseur du point de terminaison a changé. Cela ne s'applique que lorsque l'attribut d'ID de classe DHCP est rempli avec une certaine valeur et est ensuite modifié en une autre valeur. Si un point de terminaison est configuré avec une adresse IP statique, l'attribut d'ID de classe DHCP ne sera pas renseigné sur ISE. Plus tard, si un autre périphérique usurpe l'adresse MAC et utilise DHCP, l'ID de classe passera d'une valeur vide à une chaîne spécifique. Cela ne déclenchera pas la détection des comportements des Anomouls.

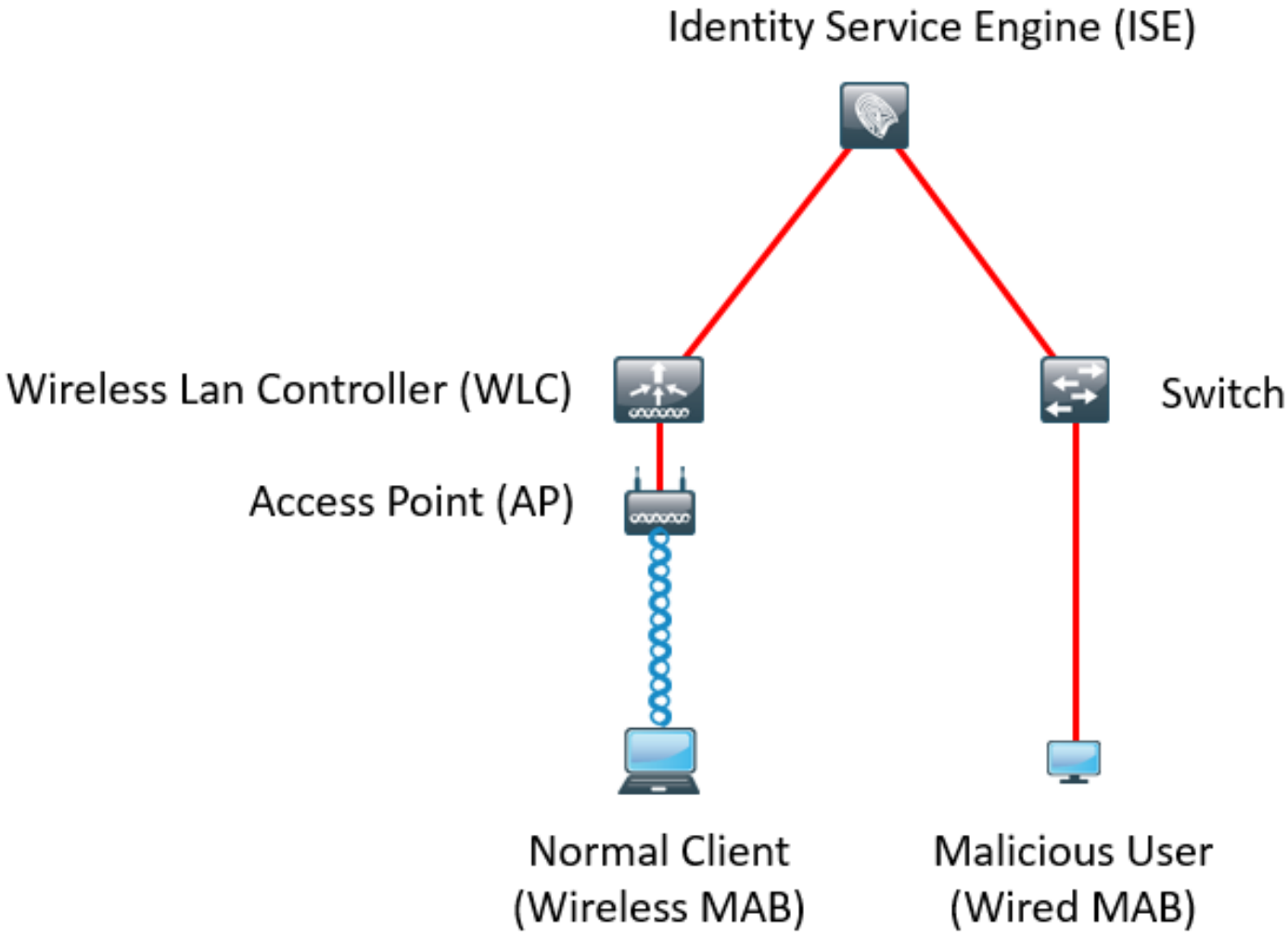
3. **Stratégie de point de terminaison -** Modification du profil de point de terminaison de l'**imprimante** ou du **téléphone IP** à **la station de travail**.

Une fois que ISE a détecté l'une des modifications mentionnées ci-dessus, l'attribut AnomalousBehavior est ajouté au point de terminaison et défini sur True. Cette condition peut être utilisée ultérieurement dans les stratégies d'autorisation pour restreindre l'accès au point de terminaison dans les authentifications futures.

Si l'application est configurée, ISE peut envoyer une CoA une fois que la modification est détectée pour une nouvelle authentification ou pour exécuter un renvoi de port pour le point de terminaison. En effet, il peut mettre en quarantaine le point de terminaison anormal en fonction des stratégies d'autorisation configurées.

Configuration

Diagramme du réseau

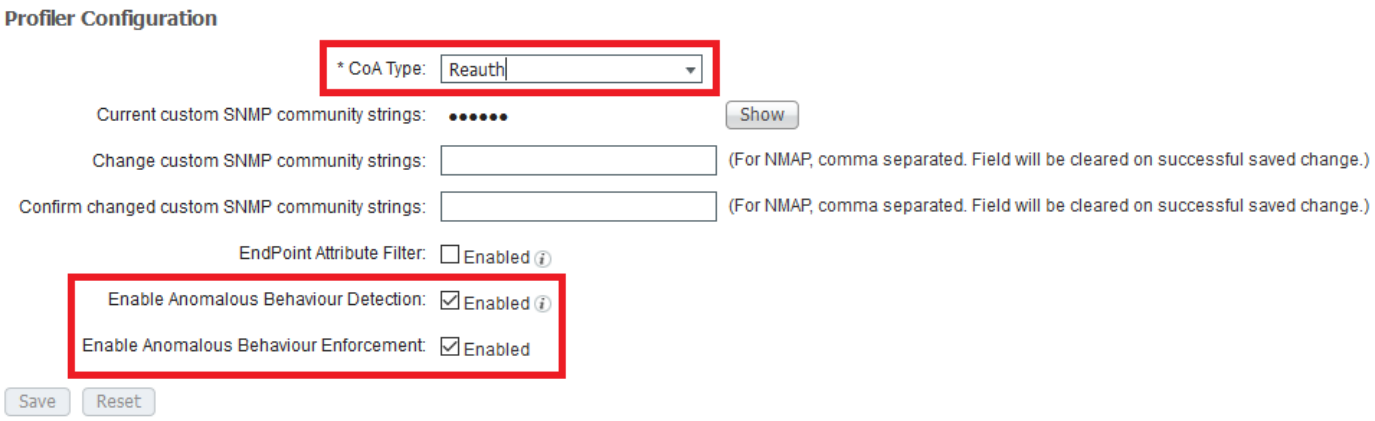


Configurations

Des configurations MAB et AAA simples sont effectuées sur le commutateur et le WLC. Pour utiliser cette fonction, procédez comme suit :

Étape 1. Activez la détection des anomalies.

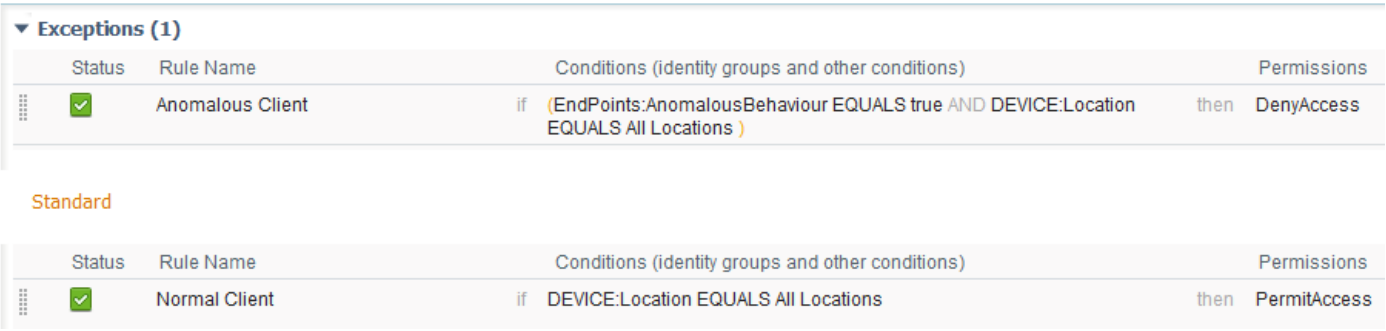
Accédez à **Administration > System > Settings > Profilage**.



La première option permet à ISE de détecter tout comportement anormal, mais aucune CoA n'est envoyée (mode Visibilité uniquement). La deuxième option permet à ISE d'envoyer CoA une fois que le comportement anormal est détecté (Mode Application).

Étape 2. Configurez la stratégie d'autorisation.

Configurez l'attribut comportement anormal comme condition dans la stratégie d'autorisation, comme illustré dans l'image :

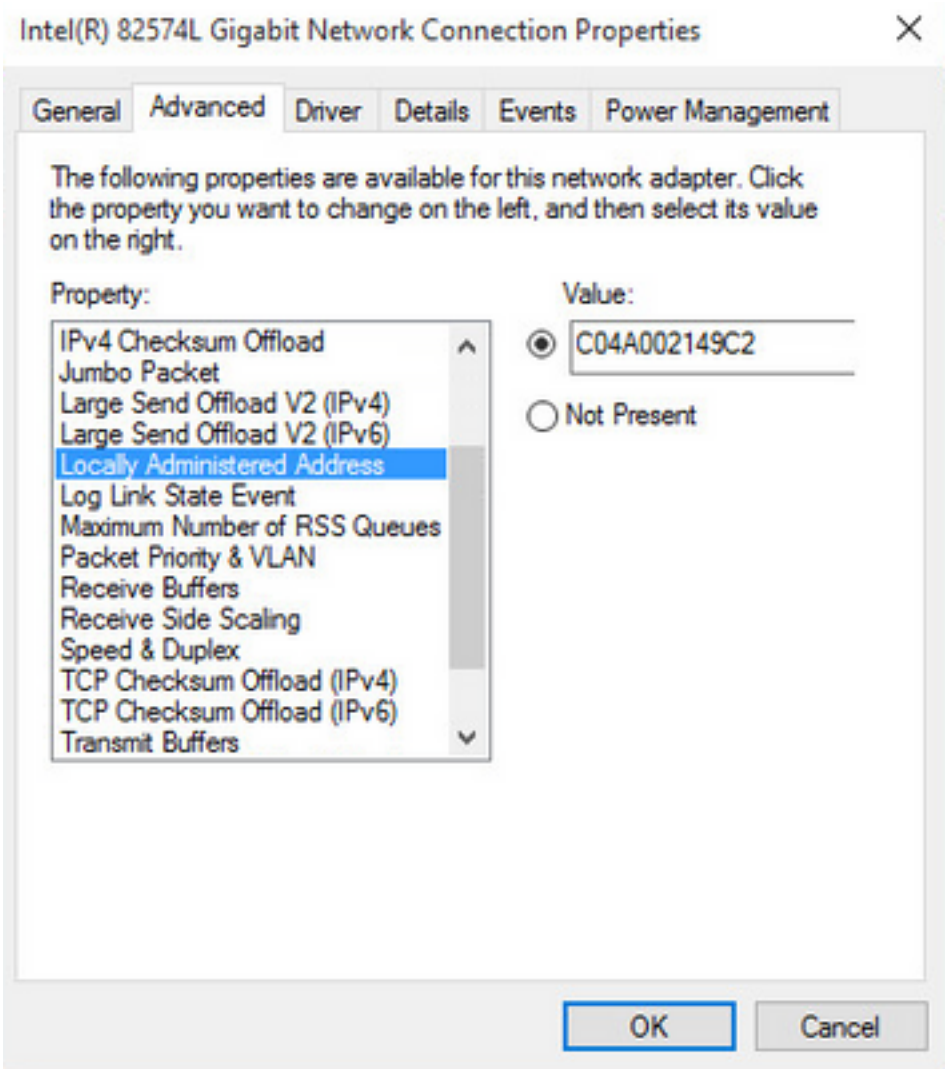


Vérification

Connectez-vous avec un adaptateur sans fil. Utilisez la commande **ipconfig /all** pour rechercher l'adresse MAC de la carte sans fil, comme illustré dans l'image :

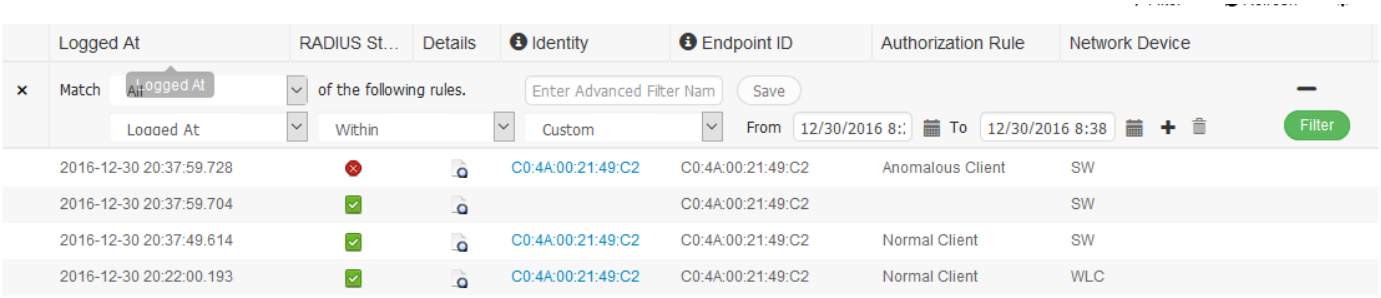
```
Wireless LAN adapter Wi-Fi:

   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 Tcpip. . . . . . . . : Enabled
```

Pour simuler un utilisateur malveillant, vous pouvez usurper l'adresse MAC de la carte Ethernet pour qu'elle corresponde à l'adresse MAC de l'utilisateur normal.



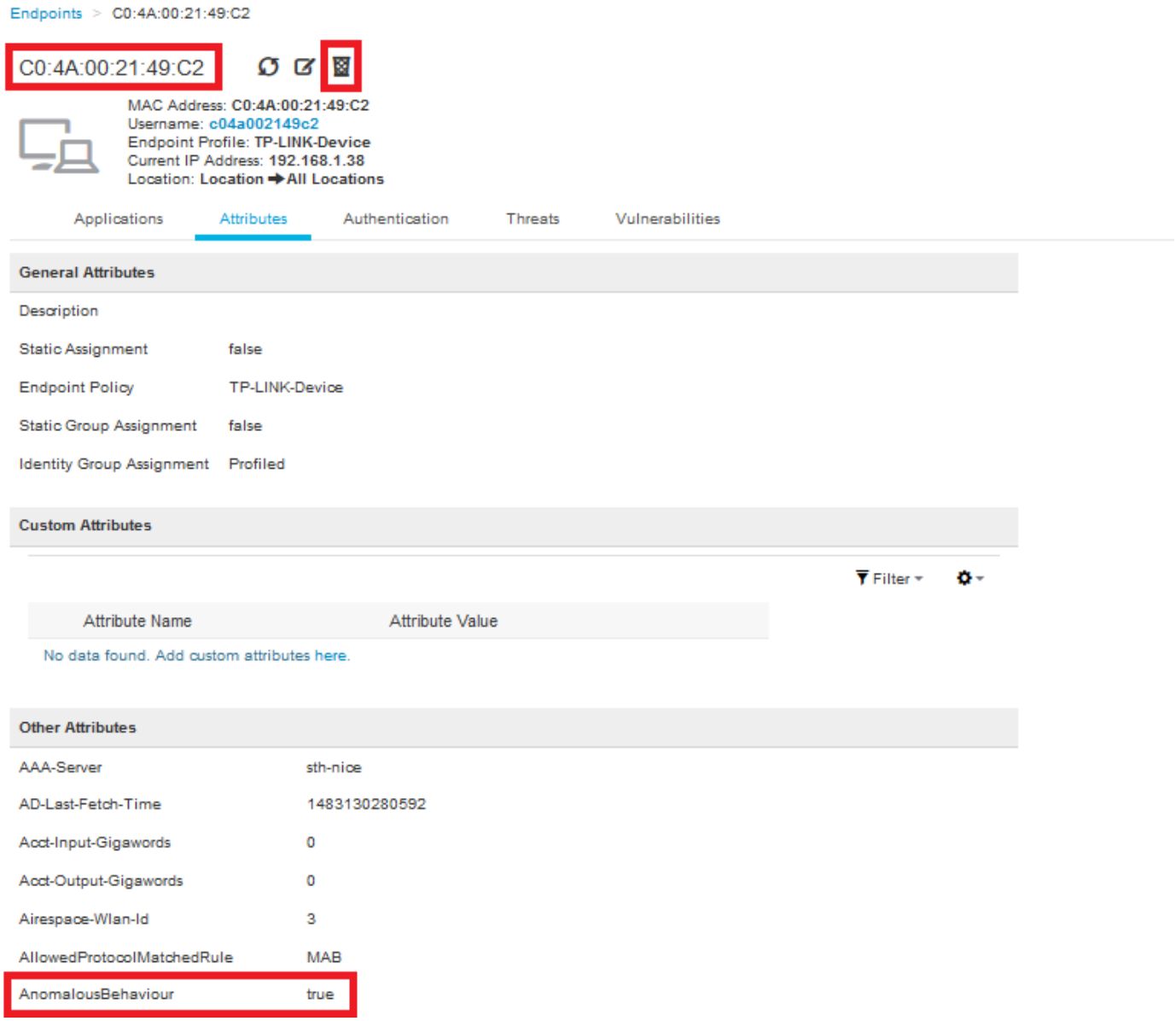
Une fois que l'utilisateur Normal se connecte, une entrée de point d'extrémité s'affiche dans la base de données. Ensuite, l'utilisateur malveillant se connecte à l'aide d'une adresse MAC usurpée.

Àpartir des rapports, vous pouvez voir la connexion initiale à partir du WLC. Par la suite, l'utilisateur malveillant se connecte et 10 secondes plus tard, une CoA est déclenchée en raison de la détection du client anormal. Puisque le type CoA global est défini sur **Réalité**, le point de terminaison tente de se reconnecter. ISE a déjà défini l'attribut AnomalousBehavior sur True pour qu'ISE corresponde à la première règle et refuse l'utilisateur.



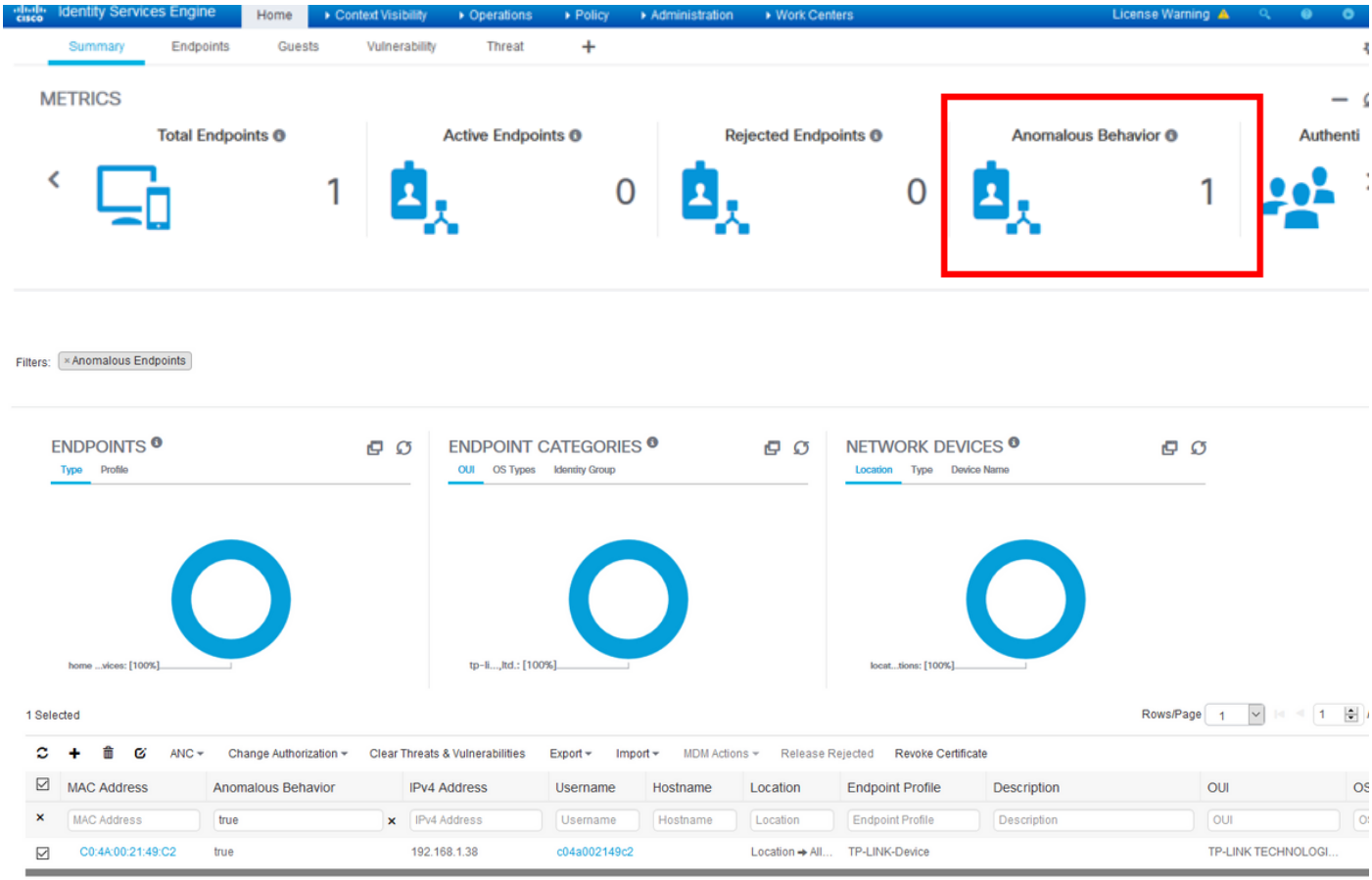
Logged At	RADIUS St...	Details	Identity	Endpoint ID	Authorization Rule	Network Device
2016-12-30 20:37:59.728	✗		C0:4A:00:21:49:C2	C0:4A:00:21:49:C2	Anomalous Client	SW
2016-12-30 20:37:59.704	✓			C0:4A:00:21:49:C2		SW
2016-12-30 20:37:49.614	✓		C0:4A:00:21:49:C2	C0:4A:00:21:49:C2	Normal Client	SW
2016-12-30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

Comme l'illustre l'image, vous pouvez voir les détails sous le point de terminaison dans l'onglet Visibilité contextuelle :



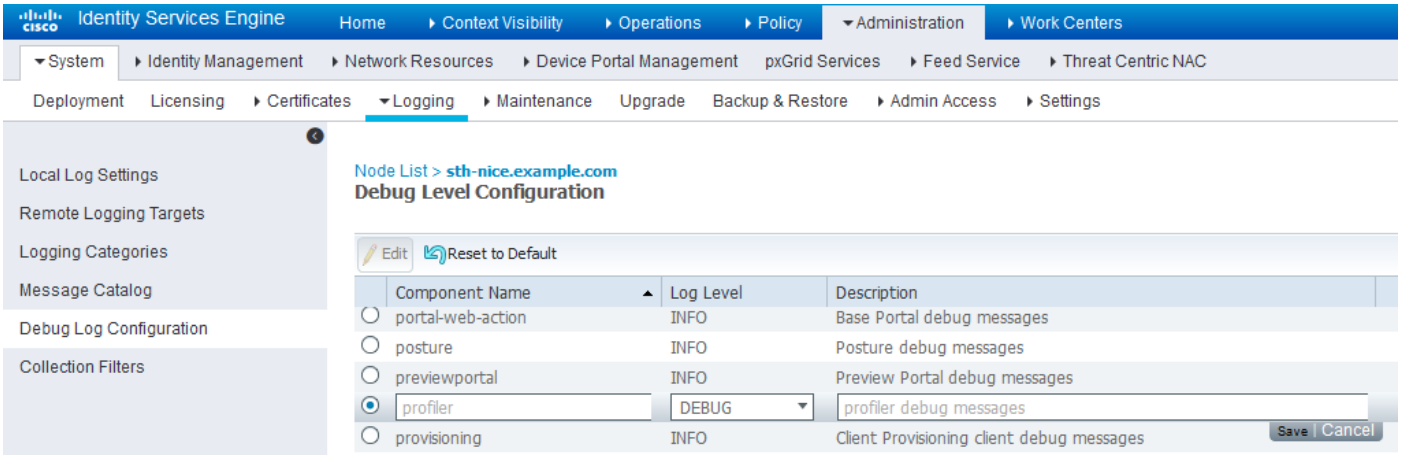
Comme vous pouvez le voir, le point de terminaison peut être supprimé de la base de données pour effacer cet attribut.

Comme l'illustre l'image, le tableau de bord comprend un nouvel onglet pour afficher le nombre de clients présentant ce comportement :

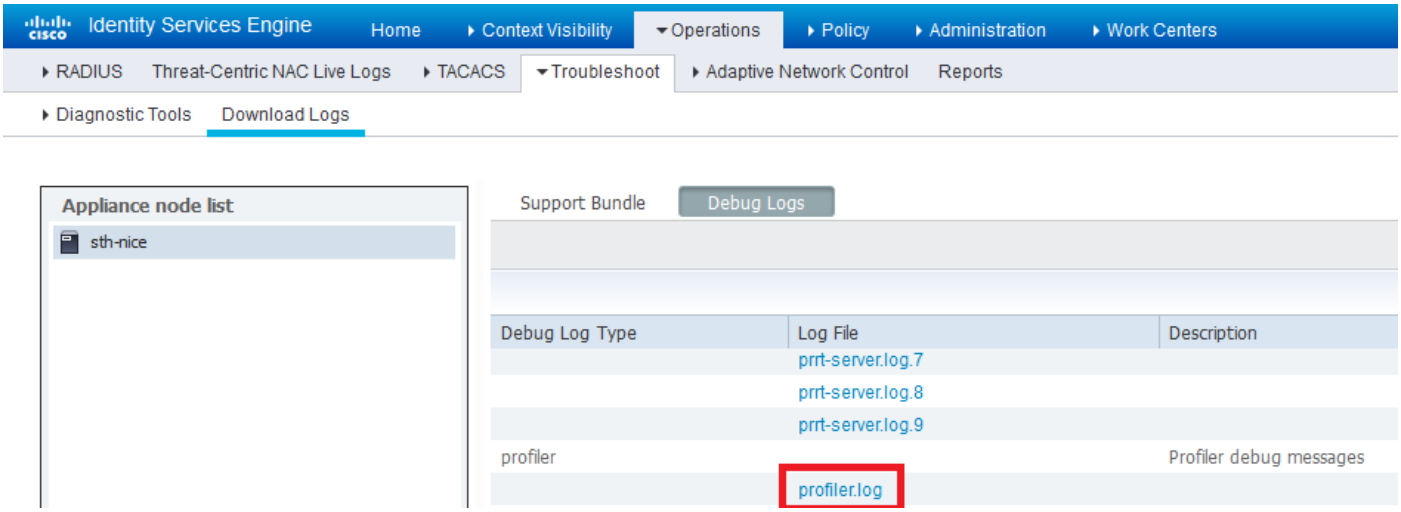


Dépannage

Afin de dépanner, activez le débogage du profileur, lorsque vous accédez à **Administration > System > Logging > Debug Log Configuration**.



Afin de trouver le fichier **Profiler.log** ISE, accédez à **Operations > Download Logs > Debug Logs**, comme indiqué dans l'image :



Ces journaux affichent des extraits du fichier **Profilage.log**. Comme vous pouvez le voir, ISE a pu détecter que le point de terminaison avec l'adresse MAC C0:4A:00:21:49:C2 a modifié la méthode d'accès en comparant les anciennes et les nouvelles valeurs des attributs NAS-Port-Type. Il s'agit d'un réseau sans fil, mais il est remplacé par Ethernet.

```
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  [MACSpoofingEventHandler-52-thread-1][]
profiler.infrastructure.probemgr.event.MACSpoofingEventHandler -:ProfilerCollection:- Received
AttrsModifiedEvent in MACSpoofingEventHandler MAC: C0:4A:00:21:49:C2
2016-12-30 20:37:49,618 DEBUG  [MACSpoofingEventHandler-52-thread-1][]
profiler.infrastructure.probemgr.event.MACSpoofingEventHandler -:ProfilerCollection:- Received
AttrsModifiedEvent in MACSpoofingEventHandler MAC: C0:4A:00:21:49:C2
2016-12-30 20:37:49,618 INFO   [MACSpoofingEventHandler-52-thread-1][]
com.cisco.profiler.api.MACSpoofingManager -: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  [MACSpoofingEventHandler-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  [MACSpoofingEventHandler-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  [MACSpoofingEventHandler-52-thread-1][]
profiler.infrastructure.probemgr.event.EndpointPersistEventHandler -:ProfilerCollection:- Adding
to queue endpoint persist event for mac: C0:4A:00:21:49:C2
```

Par conséquent, ISE prend des mesures puisque l'application est activée. L'action ici consiste à envoyer une CoA en fonction de la configuration globale dans les paramètres de profilage mentionnés ci-dessus. Dans notre exemple, le type CoA est défini sur Reauth, ce qui permet à ISE de réauthentifier le point de terminaison et de vérifier à nouveau les règles qui ont été configurées. Cette fois-ci, il correspond à la règle client Anomalie et par conséquent il est refusé.

```
2016-12-30 20:37:49,625 INFO   [MACSpoofingEventHandler-52-thread-1][]
profiler.infrastructure.probemgr.event.MACSpoofingEventHandler -:ProfilerCollection:- Taking mac
spoofing enforcement action for mac: C0:4A:00:21:49:C2
2016-12-30 20:37:49,625 INFO   [MACSpoofingEventHandler-52-thread-1][]
profiler.infrastructure.probemgr.event.MACSpoofingEventHandler -: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 d'ISE 2.2