Configuration des alarmes en fonction des résultats d'autorisation sur ISE 3.1

Contenu

Introduction

Ce document décrit les étapes requises pour configurer les alarmes en fonction du résultat d'autorisation d'une demande d'authentification RADIUS sur Identity Services Engine (ISE).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- protocole RADIUS
- Accès administrateur ISE

Components Used

Les informations de ce document sont basées sur Identity Services Engine (ISE) 3.1.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Dans cet exemple, une alarme personnalisée serait configurée pour un profil d'autorisation spécifique avec une limite de seuil définie et si ISE atteint la limite de seuil de la stratégie d'autorisation configurée, l'alarme serait déclenchée.

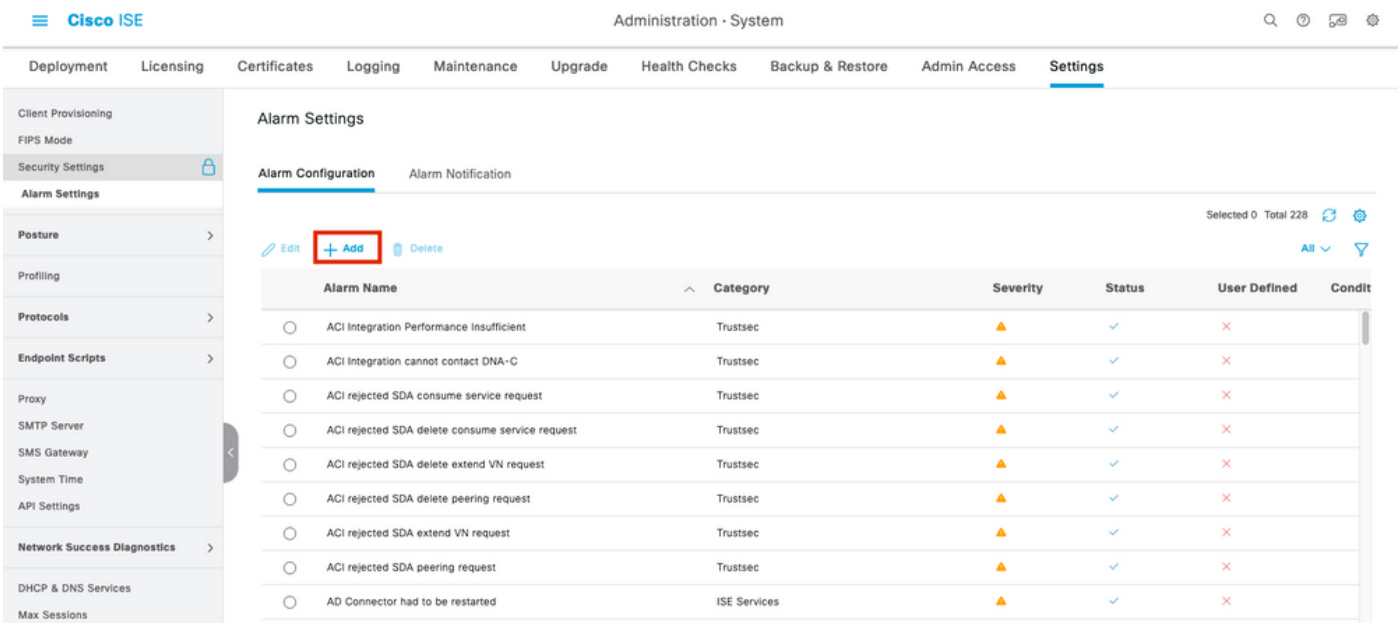
Configuration

Dans cet exemple, nous allons créer une alarme pour le profil d'autorisation (« ad_user ») poussé lorsqu'un utilisateur Active Directory (AD) se connecte et que l'alarme est déclenchée en fonction du seuil configuré.

> **Note**: Pour un serveur de production, le seuil doit être une valeur supérieure pour éviter de grandes occurrences de l'alarme.

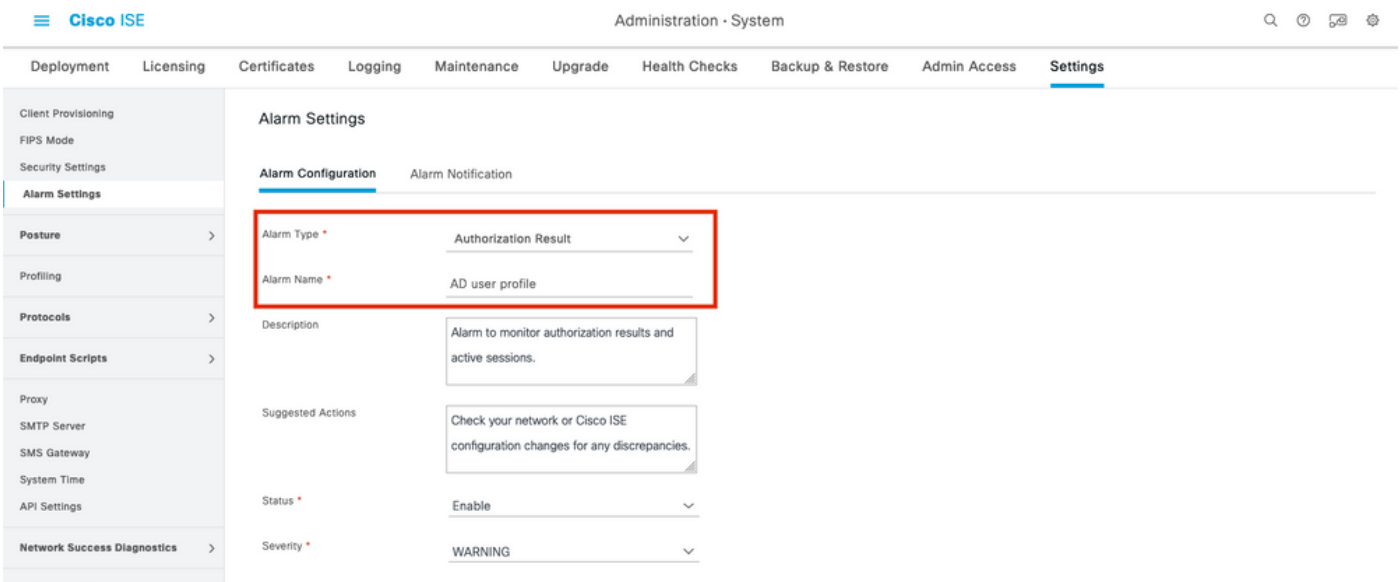
Étape 1. Accédez à **Administration > System > Alarm Settings**.

Étape 2. Sous Configuration des alarmes, cliquez sur **Ajouter** pour créer une alarme comme l'illustre l'image.



Alarmes ISE 3.1 basées sur les résultats d'autorisation - Paramètres d'alarme

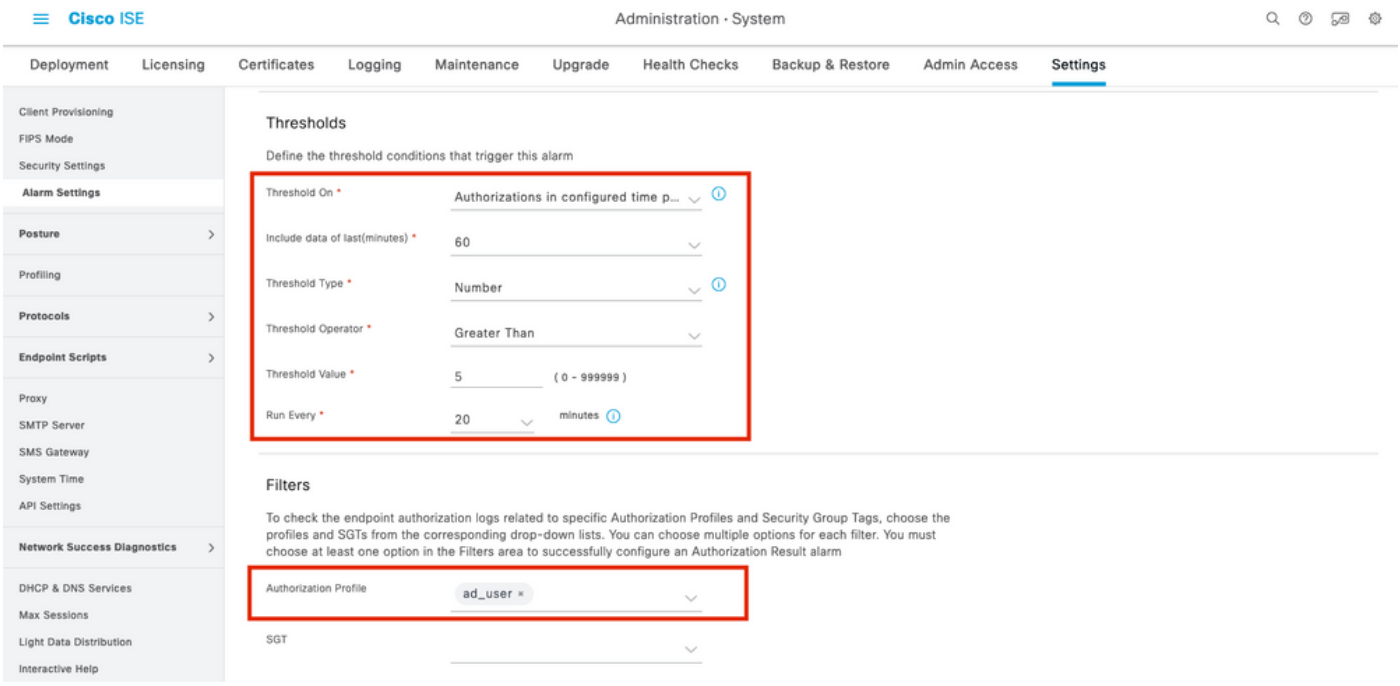
Étape 3. Sélectionnez le type d'alarme en tant que **résultat d'autorisation** et entrez le nom de l'alarme comme indiqué dans l'image.



Alarmes ISE 3.1 basées sur les résultats d'autorisation - Configurer l'alarme

Étape 4. Dans la section **Seuil**, sélectionnez **Autorisation dans la période de temps configurée**

dans la liste déroulante Seuil sur et saisissez les valeurs appropriées pour le seuil et les champs obligatoires. Dans la section Filter, appelez le profil d'autorisation pour lequel l'alarme doit être déclenchée, comme indiqué dans l'image.



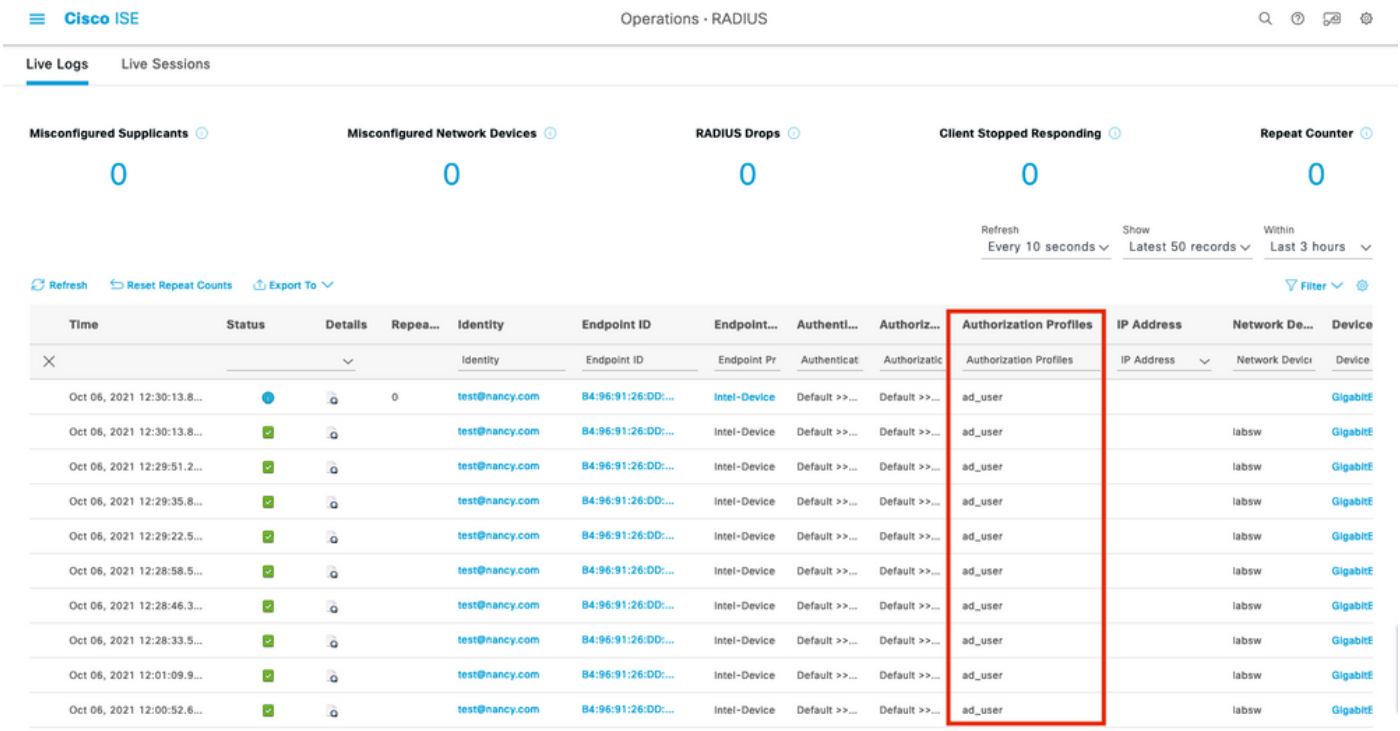
Alarmes ISE 3.1 basées sur les résultats d'autorisation - Configurer le seuil d'alarme

> **Note**: Assurez-vous que le profil d'autorisation utilisé pour l'alarme est défini sous **Stratégie > Éléments de stratégie > Résultats > Autorisation > Profils d'autorisation**.

Vérification

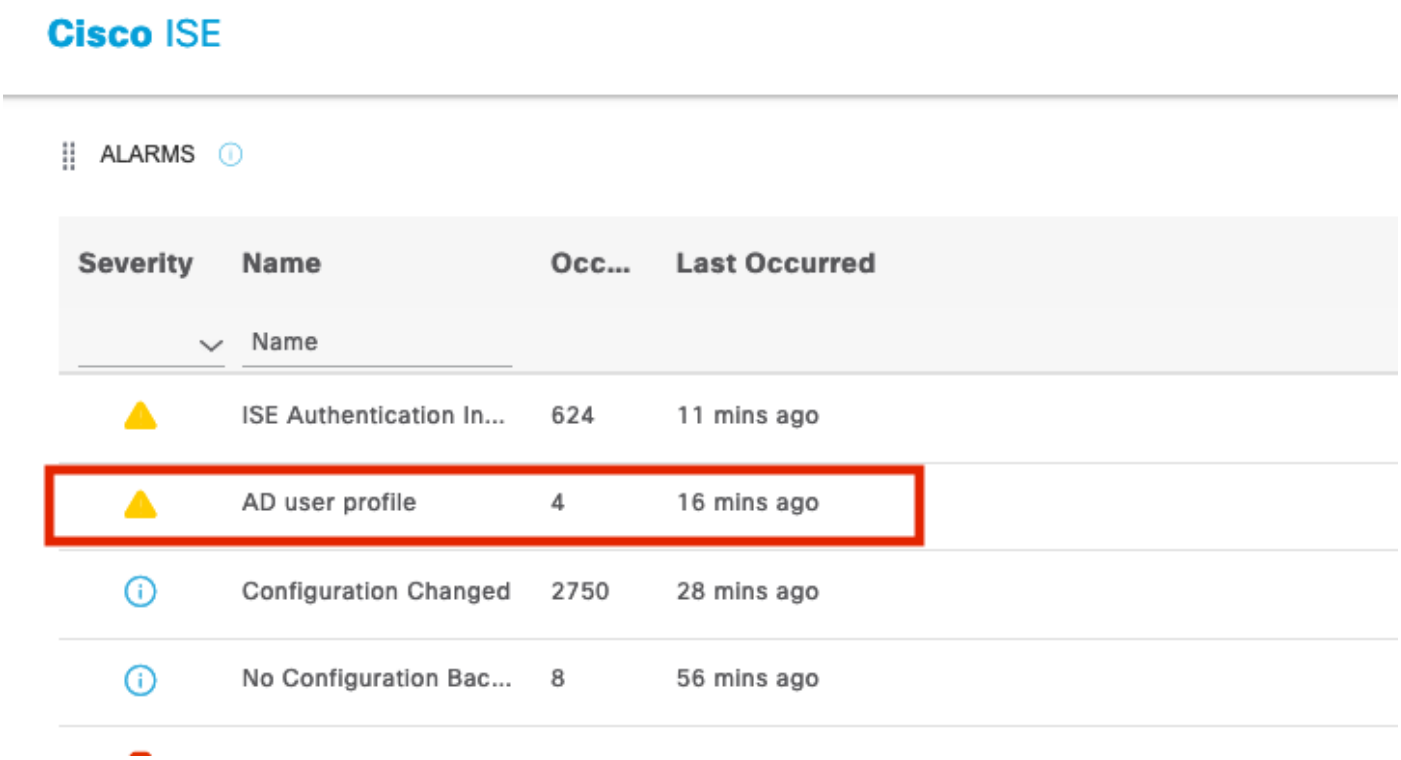
Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Lorsque ISE pousse le profil d'autorisation appelé dans l'alarme pour la demande d'authentification RADIUS et remplit la condition de seuil dans l'intervalle d'interrogation, il déclenche l'alarme vue dans le tableau de bord ISE comme illustré dans l'image. Le déclencheur de l'alarme et du profil utilisateur est que le profil est poussé plus de 5 fois (valeur seuil) au cours des 20 dernières minutes (intervalle d'interrogation).



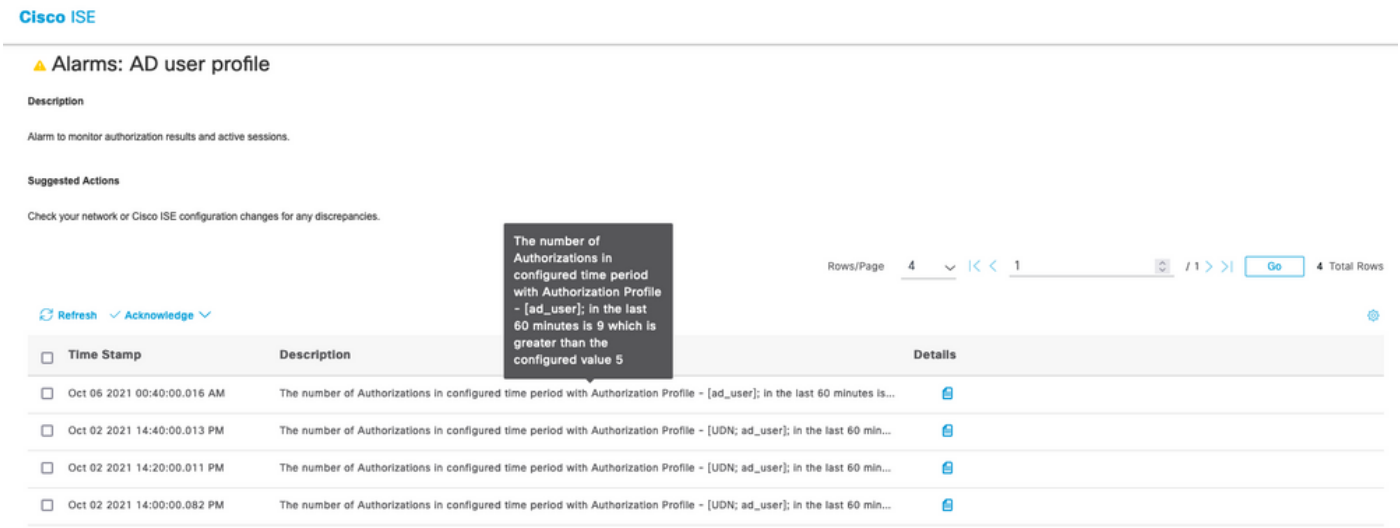
Alarmes ISE 3.1 basées sur les résultats d'autorisation - Journaux en direct ISE

Étape 1. Pour vérifier l'alarme, accédez au tableau de bord ISE et cliquez sur la fenêtre **ALARMS**. Une nouvelle page Web s'ouvre comme indiqué :



Alarmes ISE 3.1 basées sur les résultats d'autorisation - Notification des alarmes

Étape 2. Pour obtenir plus de détails sur l'alarme, sélectionnez l'alarme et elle donnera plus de détails sur le déclencheur et l'horodatage de l'alarme.

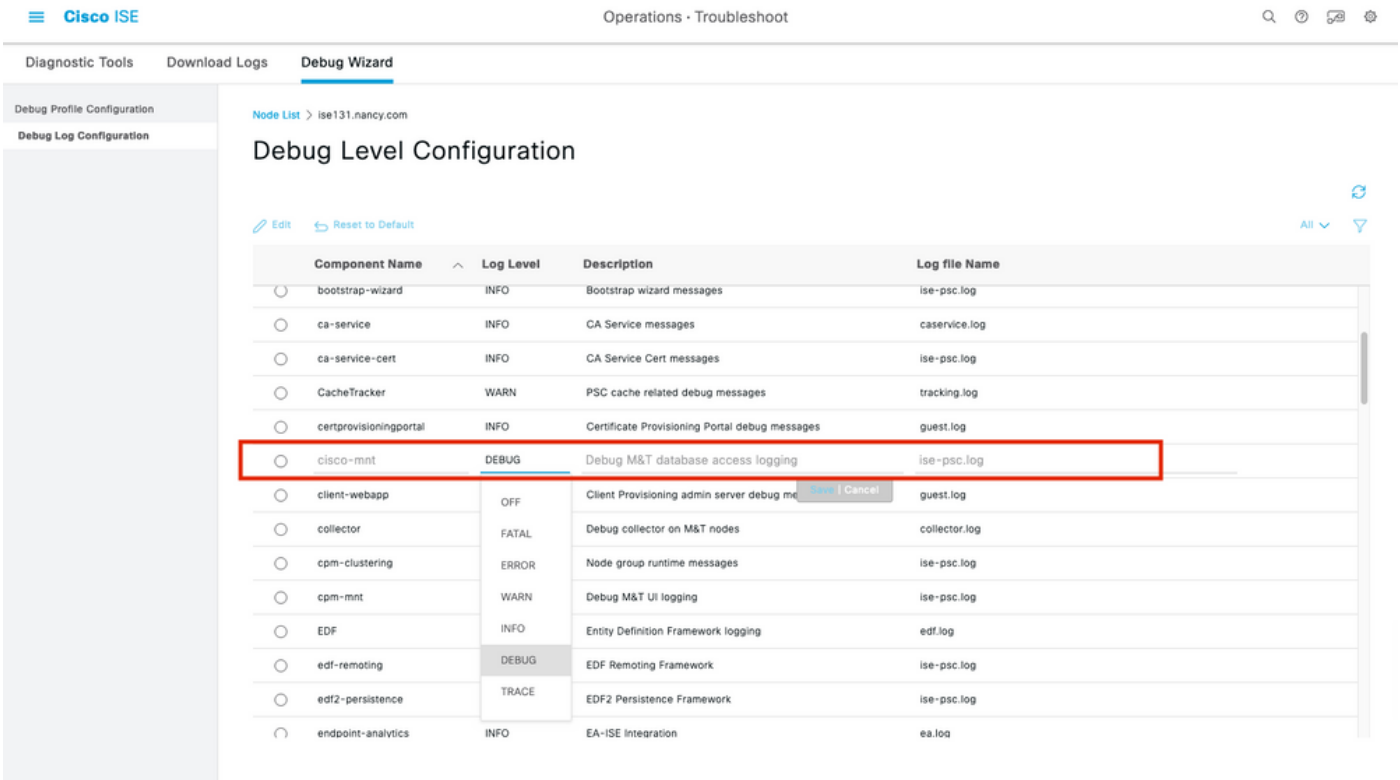


Alarmes ISE 3.1 basées sur les résultats d'autorisation - Informations détaillées sur les alarmes

Dépannage

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

Pour résoudre les problèmes liés à l'alarme, le composant cisco-mnt sur le noeud de surveillance (MnT) doit être activé lorsque l'évaluation de l'alarme se produit sur le noeud MnT. Accédez à **Operations > Troubleshoot > Debug Wizard > Debug Log Configuration**. Sélectionnez le noeud sur lequel les services de surveillance s'exécutent et modifiez le niveau de journal en Debug pour le nom de composant cisco-mnt comme indiqué :



Alarmes ISE 3.1 basées sur les résultats d'autorisation - Configuration du débogage ISE

Consigner les extraits lorsque l'alarme est déclenchée.

```
2021-10-06 00:40:00,001 DEBUG  [MnT-TimerAlarms-Threadpool-4][]
```

mnt.common.alarms.schedule.AlarmTaskRunner -::::- **Running task for rule: AlarmRule[id=df861461-89d5-485b-b3e4-68e61d1d82fc,name=AD user profile**,severity=2,isMandatory=false,enabled=true,description={65,108,97,114,109,32,116,111,32,109,111,110,105,116,111,114,32,97,117,116,104,111,114,105,122,97,116,105,111,110,32,114,101,115,117,108,116,115,32,97,110,100,32,97,99,116,105,118,101,32,115,101,115,115,105,111,110,115,46},

suggestedAction={67,104,101,99,107,37,50,48,121,111,117,114,37,50,48,110,101,116,119,111,114,107,37,50,48,111,114,37,50,48,67,105,115,99,111,37,50,48,73,83,69,37,50,48,99,111,110,102,105,103,117,114,97,116,105,111,110,37,50,48,99,104,97,110,103,101,115,37,50,48,102,111,114,37,50,48,97,110,121,37,50,48,100,105,115,99,114,101,112,97,110,99,105,101,115,46},detailsLink=#pageId=page_reports_details&pullOutId=authorizationResultAlarmDetails&definition=/Diagnostics/Authorization-Result-Alarm-Details.xml,

alarmTypeId=1065,isUserDefined=true,categoryId=1,enabledSyslog=true,emailAddress=[],customEmailText={},idConnectorNode=false]
2021-10-06 00:40:00,001 DEBUG [MnT-TimerAlarms-Threadpool-4][]
common.alarms.schedule.tasks.ScopedAlarmTask -::::- **Running custom alarm task for rule: AD user profile**
2021-10-06 00:40:00,010 INFO   [MnT-TimerAlarms-Threadpool-4][]
common.alarms.schedule.tasks.ScopedAlarmTask -::::- Getting scoped alarm conditions
2021-10-06 00:40:00,011 INFO   [MnT-TimerAlarms-Threadpool-4][]
common.alarms.schedule.tasks.ScopedAlarmTask -::::- Building attribute definitions based on Alarm Conditions
2021-10-06 00:40:00,011 DEBUG [MnT-TimerAlarms-Threadpool-4][]
common.alarms.schedule.tasks.ScopedAlarmTask -::::- Alarm Condition is:
AlarmCondition[id=bb811233-0688-42a6-a756-2f3903440feb,filterConditionType=STRING(2),filterConditionName=selected_azn_profiles,filterConditionOperator=LIKE(5),filterConditionValue=,filterConditionValues=[ad_user],filterId=]
2021-10-06 00:40:00,011 DEBUG [MnT-TimerAlarms-Threadpool-4][]
common.alarms.schedule.tasks.ScopedAlarmTask -::::- Alarm Condition is:
AlarmCondition[id=eff11b02-ae7d-4289-bae5-13936f3cdb21,filterConditionType=INTEGER(1),filterConditionName=ACSVIEW_TIMESTAMP,filterConditionOperator=GREATER_THAN(2),filterConditionValue=60,filterConditionValues=[],filterId=]
2021-10-06 00:40:00,011 INFO   [MnT-TimerAlarms-Threadpool-4][]
common.alarms.schedule.tasks.ScopedAlarmTask -::::- Attribute definition modified and already added to list
2021-10-06 00:40:00,011 DEBUG [MnT-TimerAlarms-Threadpool-4][]
common.alarms.schedule.tasks.ScopedAlarmTask -::::- Query to be run is SELECT COUNT(*) AS COUNT FROM RADIUS_AUTH_48_LIVE where (selected_azn_profiles like '%,ad_user,%' OR selected_azn_profiles like 'ad_user' OR selected_azn_profiles like '%,ad_user' OR selected_azn_profiles like 'ad_user,%') AND (ACSVIEW_TIMESTAMP > SYSDATE - NUMTODSINTERVAL(60, 'MINUTE')) AND (ACSVIEW_TIMESTAMP < SYSDATE)
2021-10-06 00:40:00,011 DEBUG [MnT-TimerAlarms-Threadpool-4][]
cisco.mnt.dbms.timesten.DbConnection -::::- in DbConnection - getConnectionWithEncryPassword call
2021-10-06 00:40:00,015 DEBUG [MnT-TimerAlarms-Threadpool-4][]
common.alarms.schedule.tasks.ScopedAlarmTask -::::- Threshold Operator is: Greater Than
2021-10-06 00:40:00,015 DEBUG [MnT-TimerAlarms-Threadpool-4][]
common.alarms.schedule.tasks.ScopedAlarmTask -::::- **Alarm Condition met: true**
2021-10-06 00:40:00,015 DEBUG [MnT-TimerAlarms-Threadpool-4][]
cisco.mnt.common.alarms.AlarmWorker -::::- df861461-89d5-485b-b3e4-68e61d1d82fc -> Enabled : true
2021-10-06 00:40:00,015 DEBUG [MnT-TimerAlarms-Threadpool-4][]
cisco.mnt.common.alarms.AlarmWorker -::::- Active MNT -> true : false
2021-10-06 00:40:00,015 DEBUG [MnT-TimerAlarms-Threadpool-4][]
cisco.mnt.common.alarms.AlarmWorker -::::- trip() : AlarmRule[id=df861461-89d5-485b-b3e4-68e61d1d82fc,**name=AD user profile**,severity=2,isMandatory=false,enabled=true,description={65,108,97,114,109,32,116,111,32,109,111,110,105,116,111,114,32,97,117,116,104,111,114,105,122,97,116,105,111,110,32,114,101,115,117,108,116,115,32,97,110,100,32,97,99,116,105,118,101,32,115,101,115,115,105,111,110,115,46},

suggestedAction={67,104,101,99,107,37,50,48,121,111,117,114,37,50,48,110,101,116,119,111,114,107,37,50,48,111,114,37,50,48,67,105,115,99,111,37,50,48,73,83,69,37,50,48,99,111,110,102,105,103,117,114,97,116,105,111,110,37,50,48,99,104,97,110,103,101,115,37,50,48,102,111,114,37,50,48,97,110

```
0,121,37,50,48,100,105,115,99,114,101,112,97,110,99,105,101,115,46},detailsLink=#pageId=page_rep
orts_details&pullOutId=authorizationResultAlarmDetails&definition=/Diagnostics/Authorization-
Result-Alarm-Details.xml,

alarmTypeId=1065,isUserDefined=true,categoryId=1,enabledSyslog=true,emailAddress=[],customEmailT
ext={},idConnectorNode=false] : 2 : The number of Authorizations in configured time period with
Authorization Profile - [ad_user]; in the last 60 minutes is 9 which is greater than the
configured value 5
```

NOTE: Si l'alarme n'est pas déclenchée même après l'activation du profil d'autorisation, vérifiez les conditions suivantes : Inclure les données des dernières (minutes), de l'opérateur de seuil, de la valeur de seuil et de l'intervalle d'interrogation configurés dans l'alarme.