

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

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configuration](#)

[Vérification](#)

[Dépannage](#)

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.

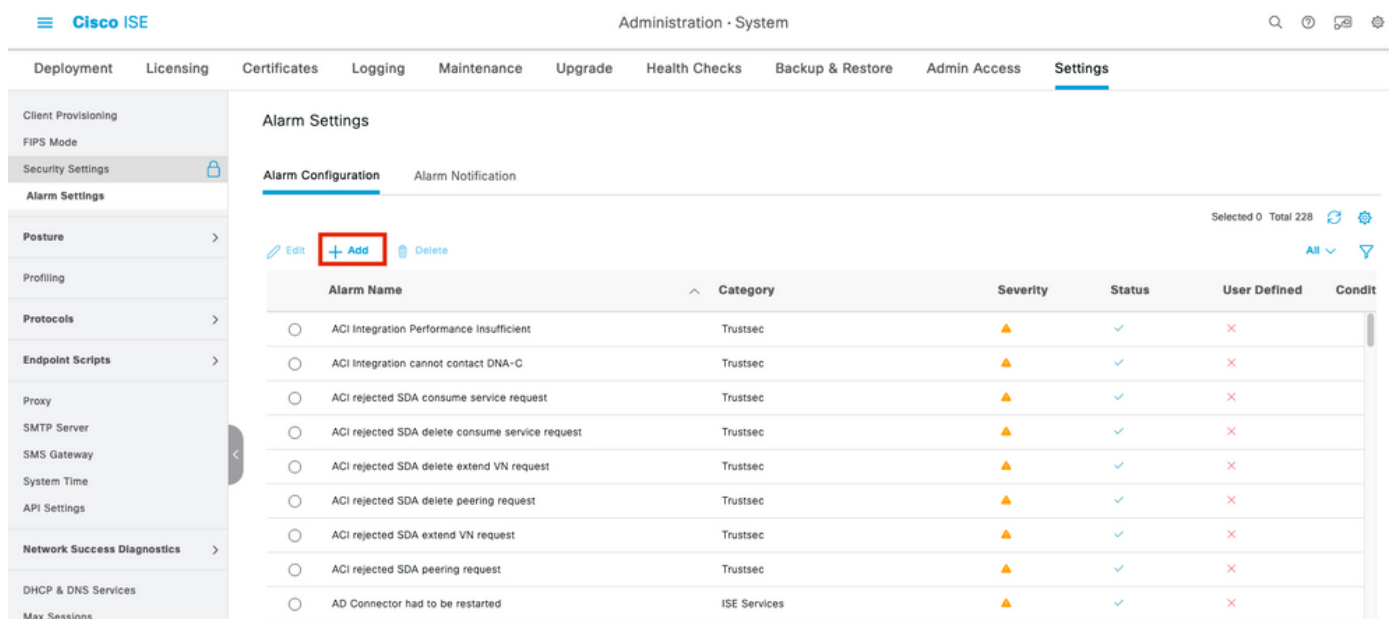
Configuration

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.

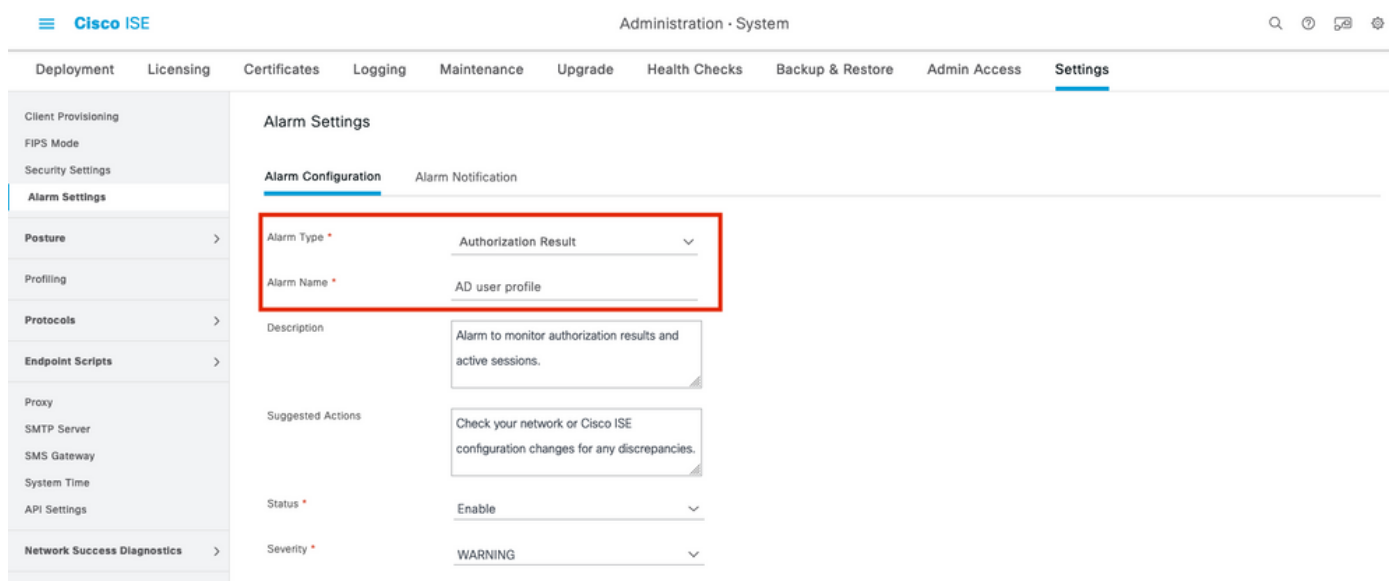


The screenshot shows the Cisco ISE Administration interface for Alarm Settings. The left sidebar contains navigation options like Client Provisioning, Security Settings, and Alarm Settings. The main content area is titled 'Alarm Settings' and has two tabs: 'Alarm Configuration' (active) and 'Alarm Notification'. Below the tabs, there are buttons for 'Edit', '+ Add' (highlighted with a red box), and 'Delete'. A table lists existing alarm configurations with columns for Alarm Name, Category, Severity, Status, User Defined, and Conditions.

Alarm Name	Category	Severity	Status	User Defined	Condit
ACI Integration Performance Insufficient	Trustsec	▲	✓	✗	
ACI Integration cannot contact DNA-C	Trustsec	▲	✓	✗	
ACI rejected SDA consume service request	Trustsec	▲	✓	✗	
ACI rejected SDA delete consume service request	Trustsec	▲	✓	✗	
ACI rejected SDA delete extend VN request	Trustsec	▲	✓	✗	
ACI rejected SDA delete peering request	Trustsec	▲	✓	✗	
ACI rejected SDA extend VN request	Trustsec	▲	✓	✗	
ACI rejected SDA peering request	Trustsec	▲	✓	✗	
AD Connector had to be restarted	ISE Services	▲	✓	✗	

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.



The screenshot shows the 'Add' alarm configuration form in Cisco ISE. The 'Alarm Type' dropdown is set to 'Authorization Result' and the 'Alarm Name' text field contains 'AD user profile'. Both are highlighted with a red box. Other fields include 'Description' (Alarm to monitor authorization results and active sessions), 'Suggested Actions' (Check your network or Cisco ISE configuration changes for any discrepancies), 'Status' (Enable), and 'Severity' (WARNING).

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.

The screenshot shows the Cisco ISE Administration System interface. The top navigation bar includes 'Administration · System' and a search icon. The main menu on the left lists various settings categories, with 'Alarm Settings' highlighted. The main content area is titled 'Thresholds' and contains the following configuration fields:

- Threshold On: Authorizations in configured time p... (dropdown)
- Include data of last(minutes): 60 (dropdown)
- Threshold Type: Number (dropdown)
- Threshold Operator: Greater Than (dropdown)
- Threshold Value: 5 (input field, range 0 - 999999)
- Run Every: 20 (input field) minutes (dropdown)

Below the thresholds section is the 'Filters' section, which includes the following configuration:

- Authorization Profile: ad_user (dropdown)
- SGT: (dropdown)

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).

Live Logs Live Sessions

Misconfigured Supplicants 0

Misconfigured Network Devices 0

RADIUS Drops 0

Client Stopped Responding 0

Repeat Counter 0

Refresh Every 10 seconds Show Latest 50 records Within Last 3 hours

Refresh Reset Repeat Counts Export To

Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authorization Profiles	IP Address	Network De...	Device
Oct 06, 2021 12:30:13.8...	🟡	🔍	0	test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user			GigabitE
Oct 06, 2021 12:30:13.8...	🟢	🔍		test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:29:51.2...	🟢	🔍		test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:29:35.8...	🟢	🔍		test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:29:22.5...	🟢	🔍		test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:28:58.5...	🟢	🔍		test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:28:46.3...	🟢	🔍		test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:28:33.5...	🟢	🔍		test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:01:09.9...	🟢	🔍		test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:00:52.6...	🟢	🔍		test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE

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 :

Cisco ISE

ALARMS ⓘ

Severity	Name	Occ...	Last Occurred
🟡	ISE Authentication In...	624	11 mins ago
🟡	AD user profile	4	16 mins ago
📘	Configuration Changed	2750	28 mins ago
📘	No Configuration Bac...	8	56 mins ago

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.

▲ Alarms: AD user profile

Description

Alarm to monitor authorization results and active sessions.

Suggested Actions

Check your network or Cisco ISE configuration changes for any discrepancies.

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

Rows/Page 4 | < < 1 | > > | Go 4 Total Rows

<input type="checkbox"/>	Time Stamp	Description	Details
<input type="checkbox"/>	Oct 06 2021 00:40:00.016 AM	The number of Authorizations in configured time period with Authorization Profile - [ad_user]; in the last 60 minutes is...	Details
<input type="checkbox"/>	Oct 02 2021 14:40:00.013 PM	The number of Authorizations in configured time period with Authorization Profile - [UDN; ad_user]; in the last 60 min...	Details
<input type="checkbox"/>	Oct 02 2021 14:20:00.011 PM	The number of Authorizations in configured time period with Authorization Profile - [UDN; ad_user]; in the last 60 min...	Details
<input type="checkbox"/>	Oct 02 2021 14:00:00.082 PM	The number of Authorizations in configured time period with Authorization Profile - [UDN; ad_user]; in the last 60 min...	Details

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 :

Operations · Troubleshoot

Diagnostic Tools Download Logs **Debug Wizard**

Debug Profile Configuration
Debug Log Configuration

Node List > ise131.nancy.com

Debug Level Configuration

[Edit](#) [Reset to Default](#) All

Component Name	Log Level	Description	Log file Name
<input type="radio"/> bootstrap-wizard	INFO	Bootstrap wizard messages	ise-psc.log
<input type="radio"/> ca-service	INFO	CA Service messages	caservice.log
<input type="radio"/> ca-service-cert	INFO	CA Service Cert messages	ise-psc.log
<input type="radio"/> CacheTracker	WARN	PSC cache related debug messages	tracking.log
<input type="radio"/> certprovisioningportal	INFO	Certificate Provisioning Portal debug messages	guest.log
<input type="radio"/> cisco-mnt	DEBUG	Debug M&T database access logging	ise-psc.log
<input type="radio"/> client-webapp	OFF	Client Provisioning admin server debug me	guest.log
<input type="radio"/> collector	FATAL	Debug collector on M&T nodes	collector.log
<input type="radio"/> cpm-clustering	ERROR	Node group runtime messages	ise-psc.log
<input type="radio"/> cpm-mnt	WARN	Debug M&T UI logging	ise-psc.log
<input type="radio"/> EDF	INFO	Entity Definition Framework logging	edf.log
<input type="radio"/> edf-remoting	DEBUG	EDF Remoting Framework	ise-psc.log
<input type="radio"/> edf2-persistence	TRACE	EDF2 Persistence Framework	ise-psc.log
<input type="radio"/> endpoint-analytics	INFO	EA-ISE Integration	ea.log

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={67,104,101,99,107,37,50,48,121,111,117,114,37,50,48,110,101,116,119,111,114,107,37,50,48,111,114,37,50,48,67,105,115,99,111,37,50,48,73,83,69,37,50,48,99,111,110,102,105,103,117,114,97,116,105,111,110,37,50,48,99,104,97,110,103,101,115,37,50,48,102,111,114,37,50,48,97,110,121,37,50,48,100,105,115,99,114,101,112,97,110,99,105,101,115,46},
```

0,121,37,50,48,100,105,115,99,114,101,112,97,110,99,105,101,115,46},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} : 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.