Configuración de Alarmas Basada en los Resultados de Autorización en ISE 3.1

Contenido

Introducción

Este documento describe los pasos necesarios para configurar las alarmas en función del resultado de la autorización para una solicitud de autenticación RADIUS en Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- protocolo RADIUS
- acceso de administrador ISE

Componentes Utilizados

La información de este documento se basa en 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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

En este ejemplo, se configuraría una alarma personalizada para un perfil de autorización específico con un límite de umbral definido y si ISE alcanza el límite de umbral en la política de autorización configurada, se activaría la alarma.

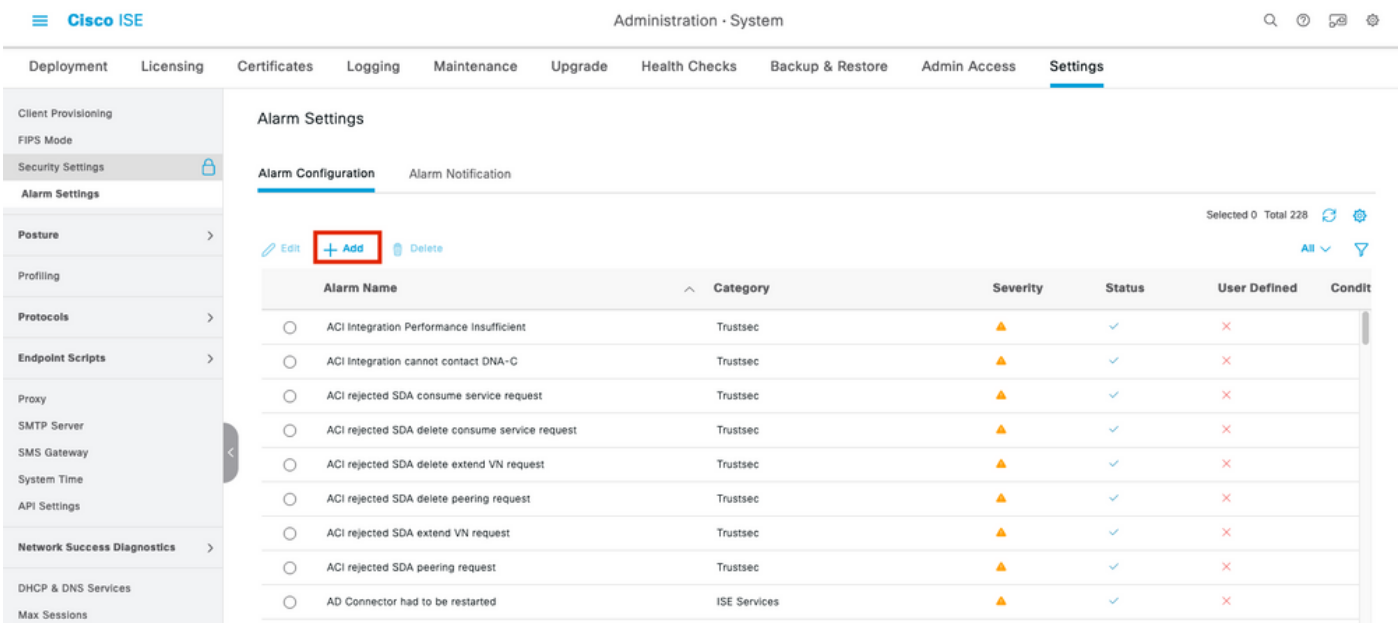
Configurar

En este ejemplo, crearemos una alarma para el perfil de autorización ("ad_user") que se envía cuando un usuario de Active Directory (AD) inicia sesión y la alarma se activa en función del umbral configurado.

> **Nota:** Para un servidor de producción, el umbral debe ser un valor más alto para evitar grandes ocurrencias de la alarma.

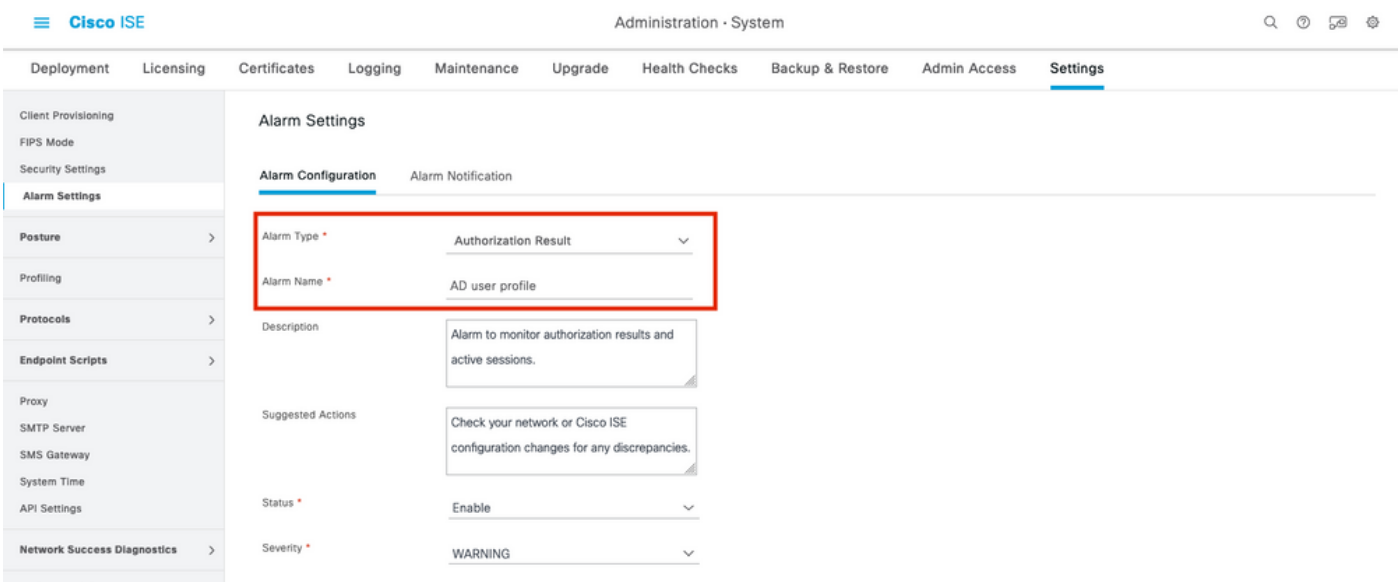
Paso 1. Vaya a **Administration > System > Alarm Settings**.

Paso 2. En Configuración de alarma, haga clic en **Agregar** para crear una alarma como se muestra en la imagen.



Alarmas ISE 3.1 basadas en los resultados de la autorización - Configuración de alarmas

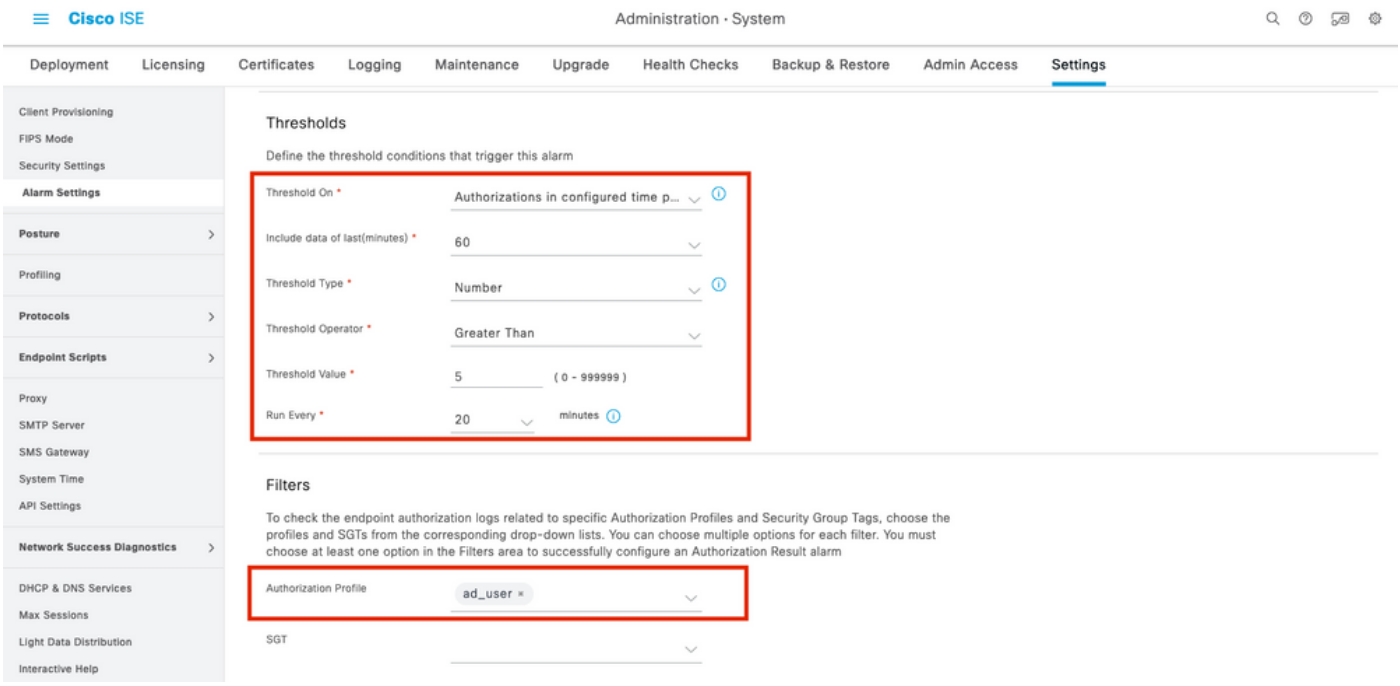
Paso 3. Seleccione el tipo de alarma como **resultado de autorización** e introduzca el nombre de alarma como se muestra en la imagen.



Alarmas ISE 3.1 basadas en los resultados de la autorización - Configurar alarma

Paso 4. En la sección **Umbral**, seleccione **Autorización en un período de tiempo configurado** en la

lista desplegable Umbral en e introduzca los valores adecuados para Umbral y los campos obligatorios. En la sección de filtros, llame al perfil de autorización para el que se debe activar la alarma como se muestra en la imagen.



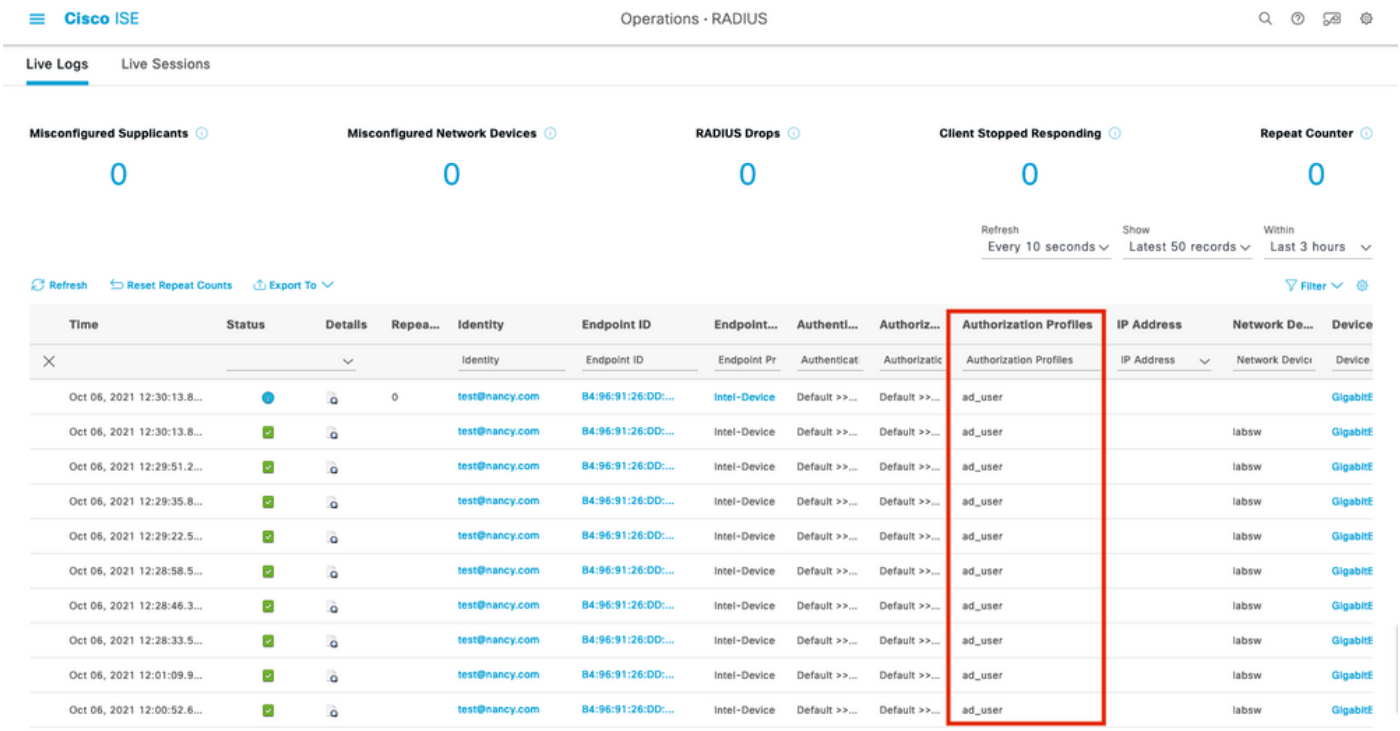
Alarmas ISE 3.1 basadas en los resultados de la autorización - Configuración del umbral de alarma

> **Nota:** Asegúrese de que el perfil de autorización utilizado para la alarma esté definido en **Política > Elementos de política > Resultados > Autorización > Perfiles de autorización**.

Verificación

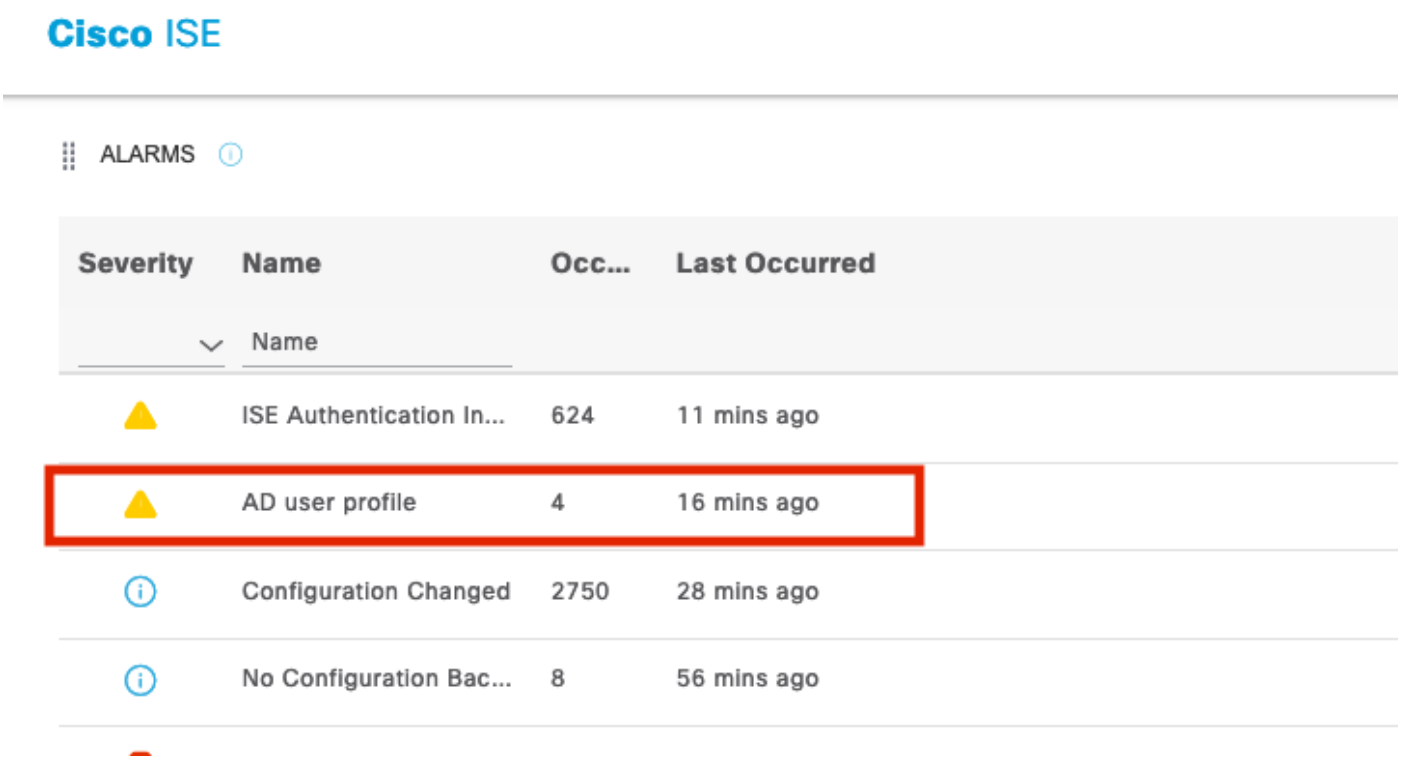
Utilize esta sección para confirmar que su configuración funcione correctamente.

Cuando ISE envía el perfil de autorización llamado en la alarma para la solicitud de autenticación RADIUS y cumple la condición de umbral dentro del intervalo de sondeo, activaría la alarma vista en el panel ISE como se muestra en la imagen. El disparador para el perfil ad_user de alarma es que el perfil se ha pulsado más de 5 veces (valor de umbral) en los últimos 20 minutos (intervalo de sondeo).



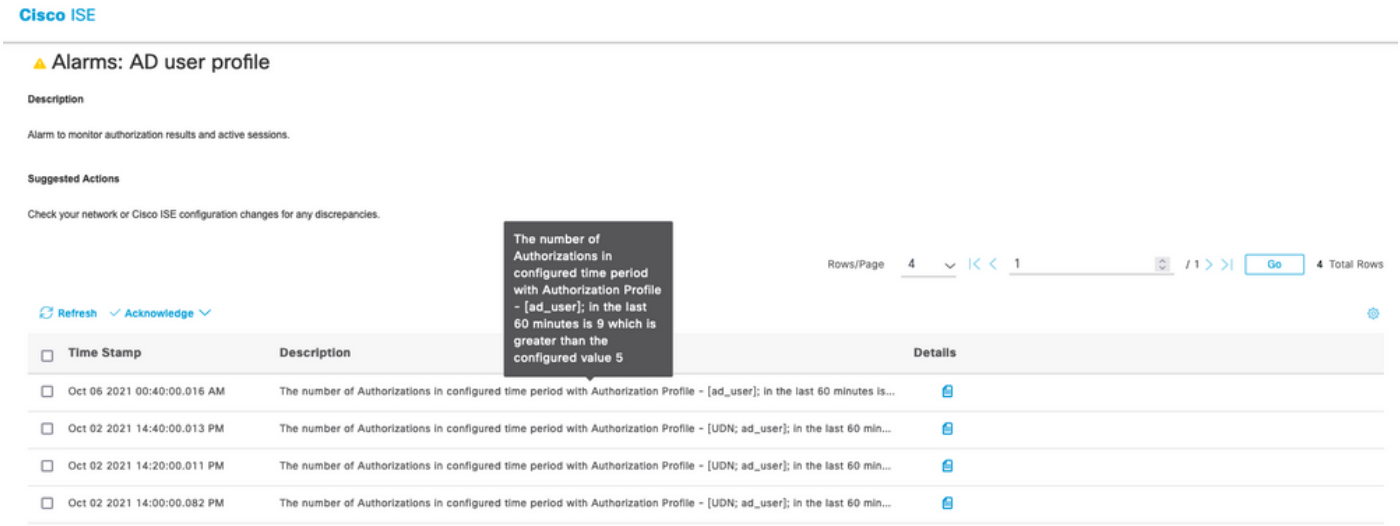
Alarmas ISE 3.1 basadas en los resultados de la autorización: registros en directo de ISE

Paso 1. Para comprobar la alarma, navegue hasta el panel ISE y haga clic en la ventana **ALARMS**. Se abrirá una nueva página web como se muestra a continuación:



Alarmas ISE 3.1 basadas en los resultados de la autorización - Notificación de alarma

Paso 2. Para obtener más detalles de la alarma, seleccione la alarma y dará más detalles sobre el disparador y la marca de tiempo de la alarma.

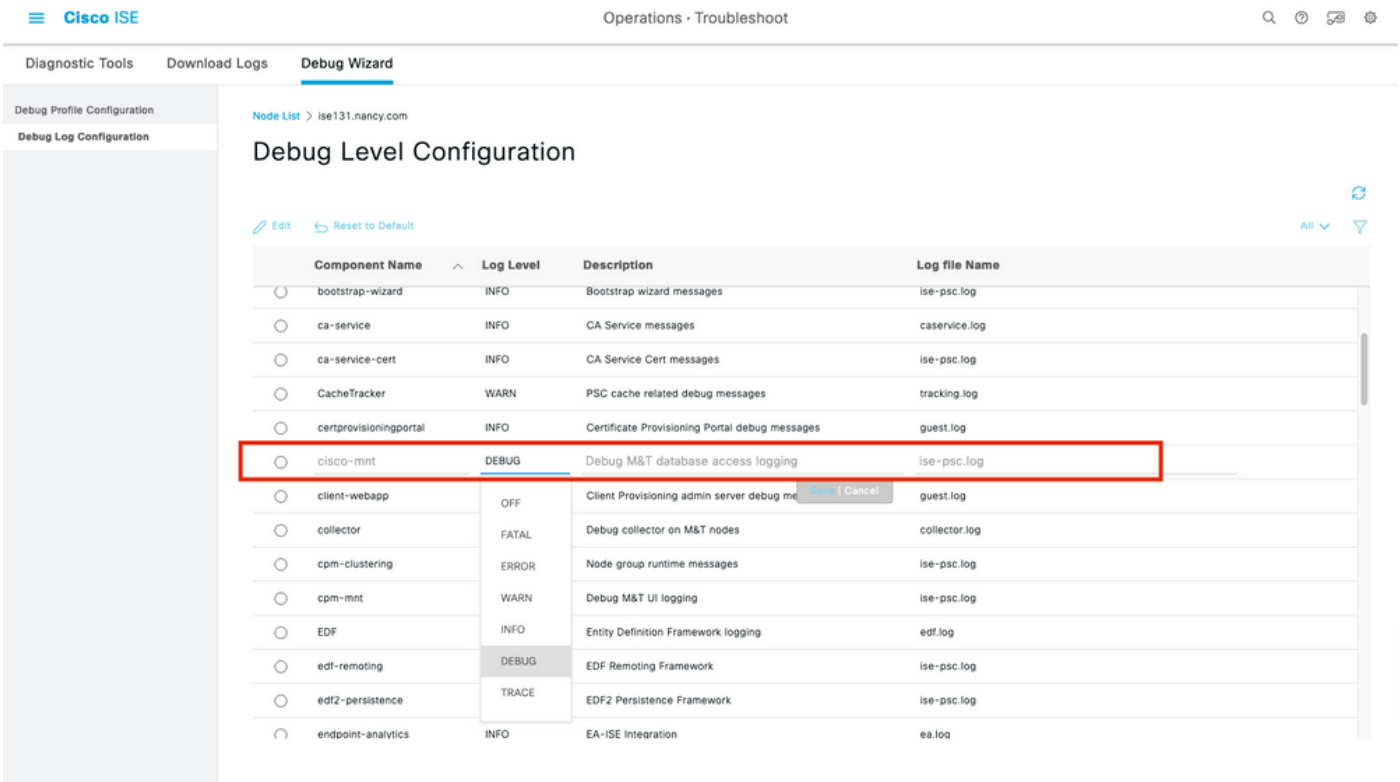


Alarmas ISE 3.1 basadas en los resultados de la autorización - Detalles de la alarma

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Para solucionar problemas relacionados con la alarma, el componente cisco-mnt del nodo de supervisión (MnT) debe habilitarse cuando la evaluación de la alarma se produzca en el nodo MnT. Vaya a **Operaciones > Solucionar problemas > Asistente de depuración > Configuración de registro de depuración**. Seleccione el nodo en el que se ejecutan los servicios de supervisión y cambie el nivel de registro a Depurar para nombre de componente cisco-mnt como se muestra a continuación:



Alarmas ISE 3.1 basadas en los resultados de la autorización: configuración de depuración de ISE

Registra fragmentos cuando se activa la alarma.

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
,37,50,48,111,114,37,50,48,67,105,115,99,111,37,50,48,73,83,69,37,50,48,99,111,110,102,105,103,1
17,114,97,116,105,111,110,37,50,48,99,104,97,110,103,101,115,37,50,48,102,111,114,37,50,48,97,11
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 la alarma no se activa incluso después de que se presione el perfil de autorización, verifique condiciones como: Incluya los datos de los últimos (minutos), el operador de umbral, el valor de umbral y el intervalo de sondeo configurados en la alarma.