Configurar alarmes com base nos resultados da autorização no ISE 3.1

Contents

Introduction

Este documento descreve as etapas necessárias para configurar alarmes com base no resultado da autorização para uma solicitação de autenticação RADIUS no Identity Services Engine (ISE).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- protocolo RADIUS
- Acesso de administrador do ISE

Componentes Utilizados

As informações neste documento são baseadas no 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Neste exemplo, um alarme personalizado seria configurado para um perfil de autorização específico com um limite de limite definido e se o ISE atingisse o limite na política de autorização configurada, o alarme seria disparado.

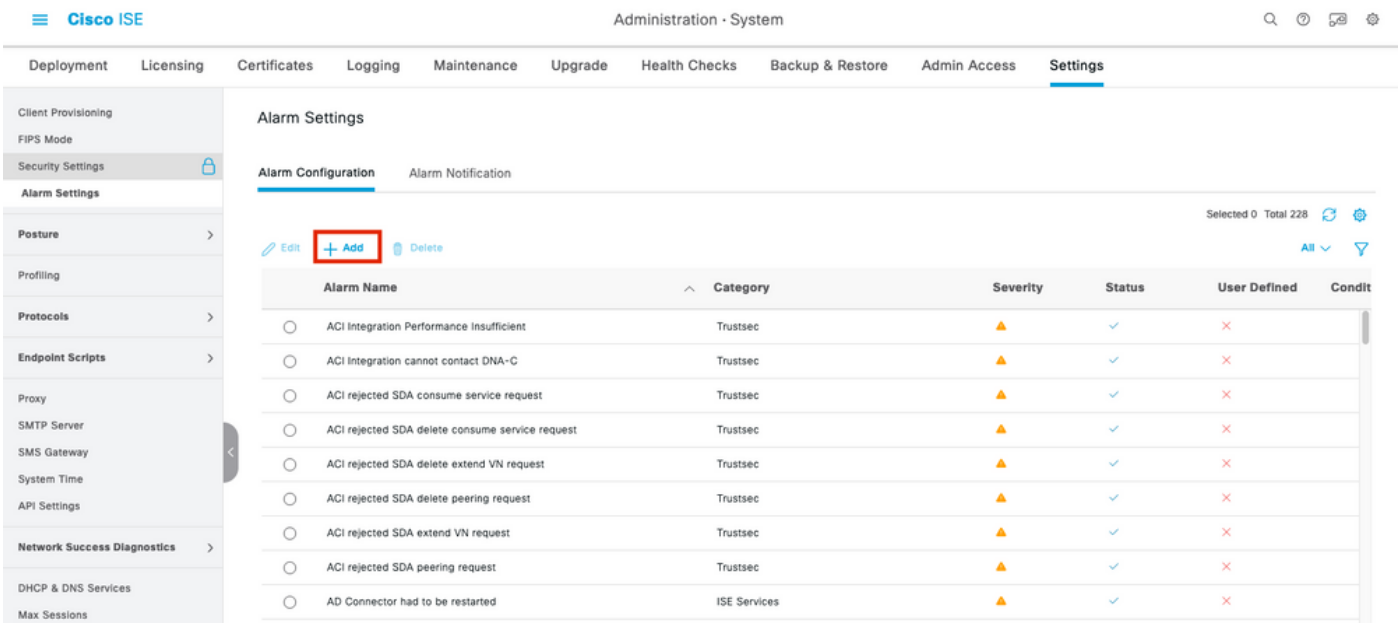
Configurar

Neste exemplo, criaremos um alarme para o perfil de autorização ("ad_user") enviado quando um usuário do Ative Diretory (AD) fizer login e o alarme for disparado com base no limite configurado.

> **Note**: Para um servidor de produção, o limite deve ser um valor maior para evitar ocorrências grandes do alarme.

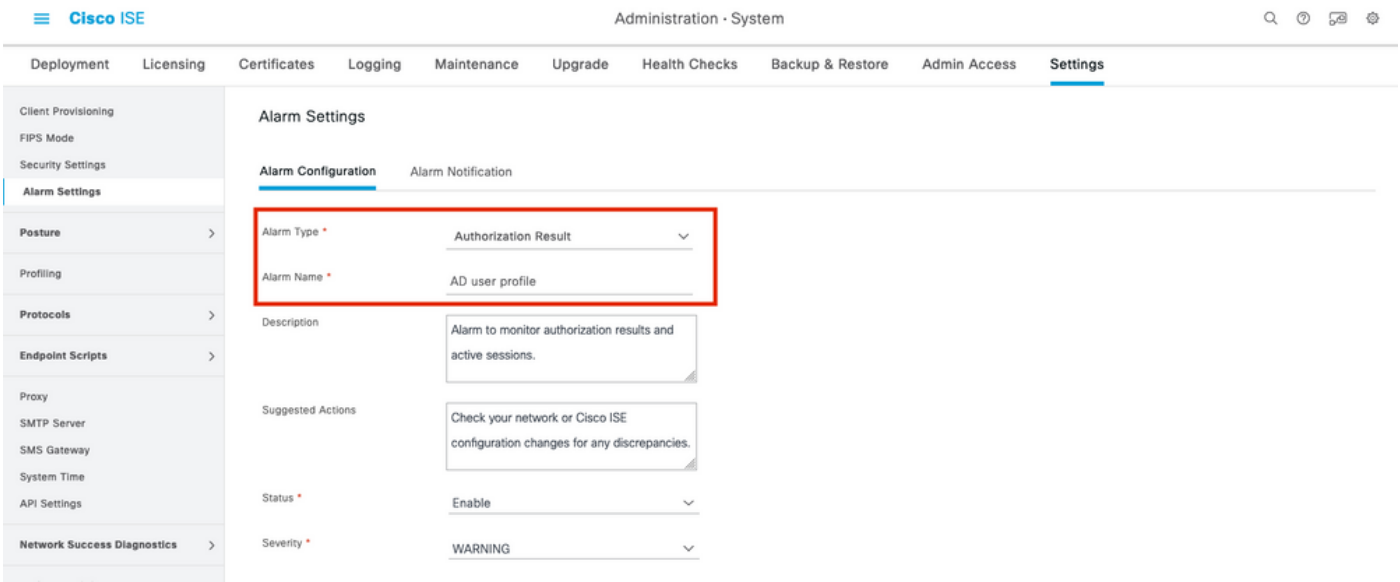
Etapa 1. Navegue até **Administration > System > Alarm Settings**.

Etapa 2. Em Alarm Configuration (Configuração de alarme), clique em **Add** para criar um Alarm, como mostrado na imagem.



Alarmes do ISE 3.1 com base nos resultados da autorização - Configurações de alarme

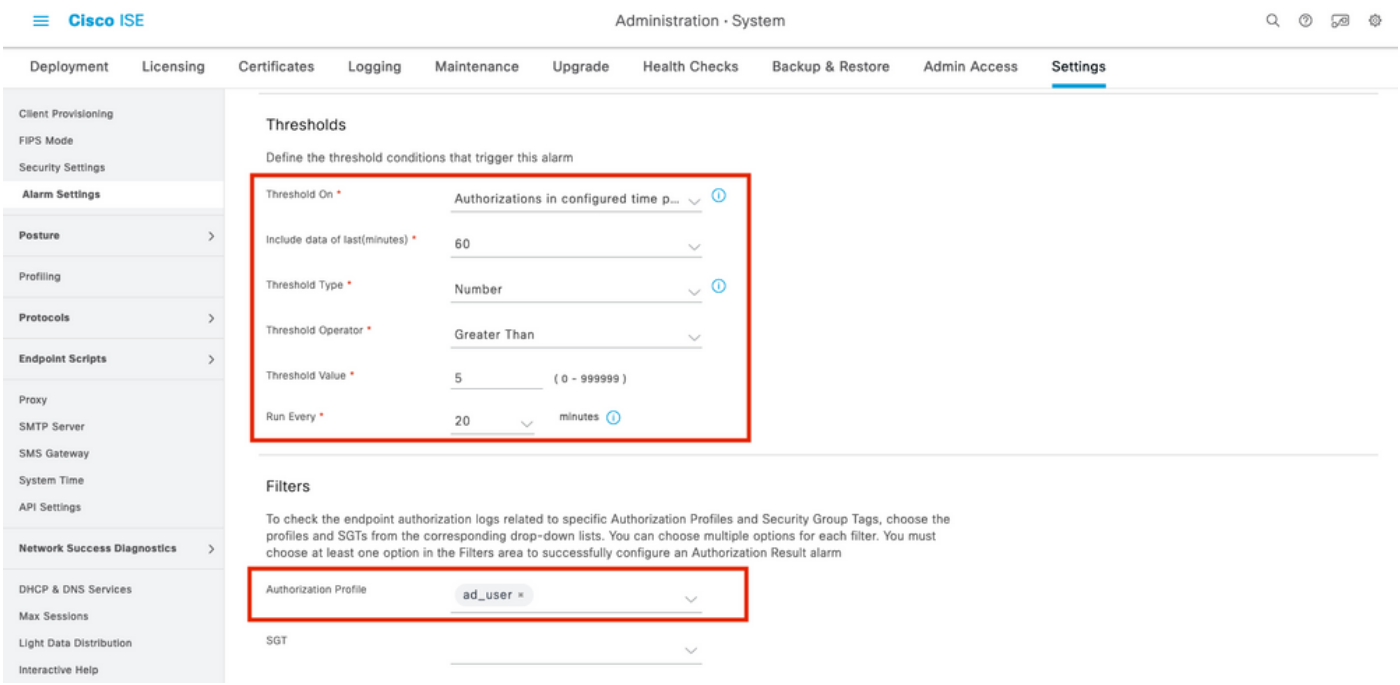
Etapa 3. Selecione o tipo de alarme como **resultado da autorização** e insira o nome do alarme como mostrado na imagem.



Alarmes do ISE 3.1 com base nos resultados da autorização - Configurar o alarme

Etapa 4. Na seção **Limite**, selecione **Autorização no período de tempo configurado** na lista suspensa Limite ativado e insira os valores apropriados para o Limite e os campos obrigatórios.

Na seção de filtro, chame o Perfil de autorização para o qual o alarme deve ser disparado conforme mostrado na imagem.



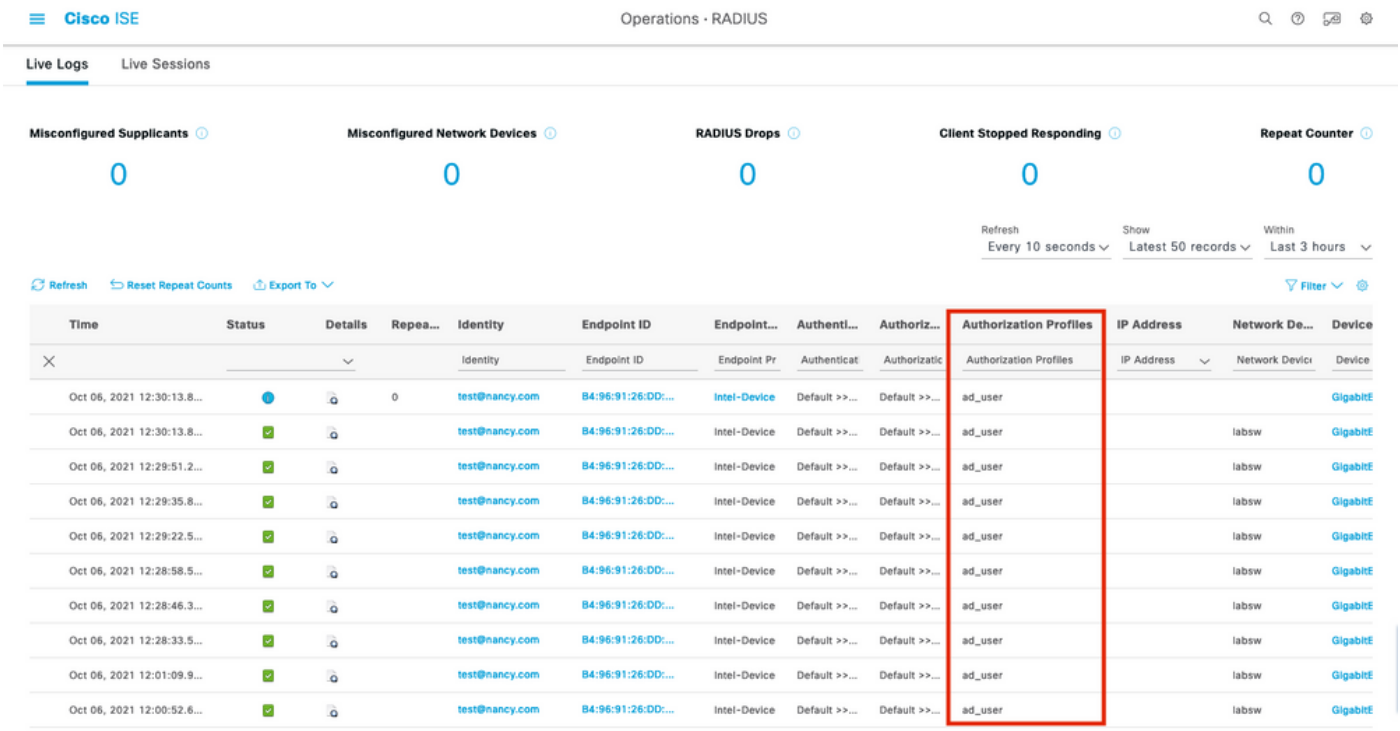
Alarmes do ISE 3.1 com base nos resultados da autorização - Configurar o limite de alarme

> **Note**: Verifique se o perfil de autorização usado para alarme está definido em **Política > Elementos de política > Resultados > Autorização > Perfis de autorização**.

Verificar

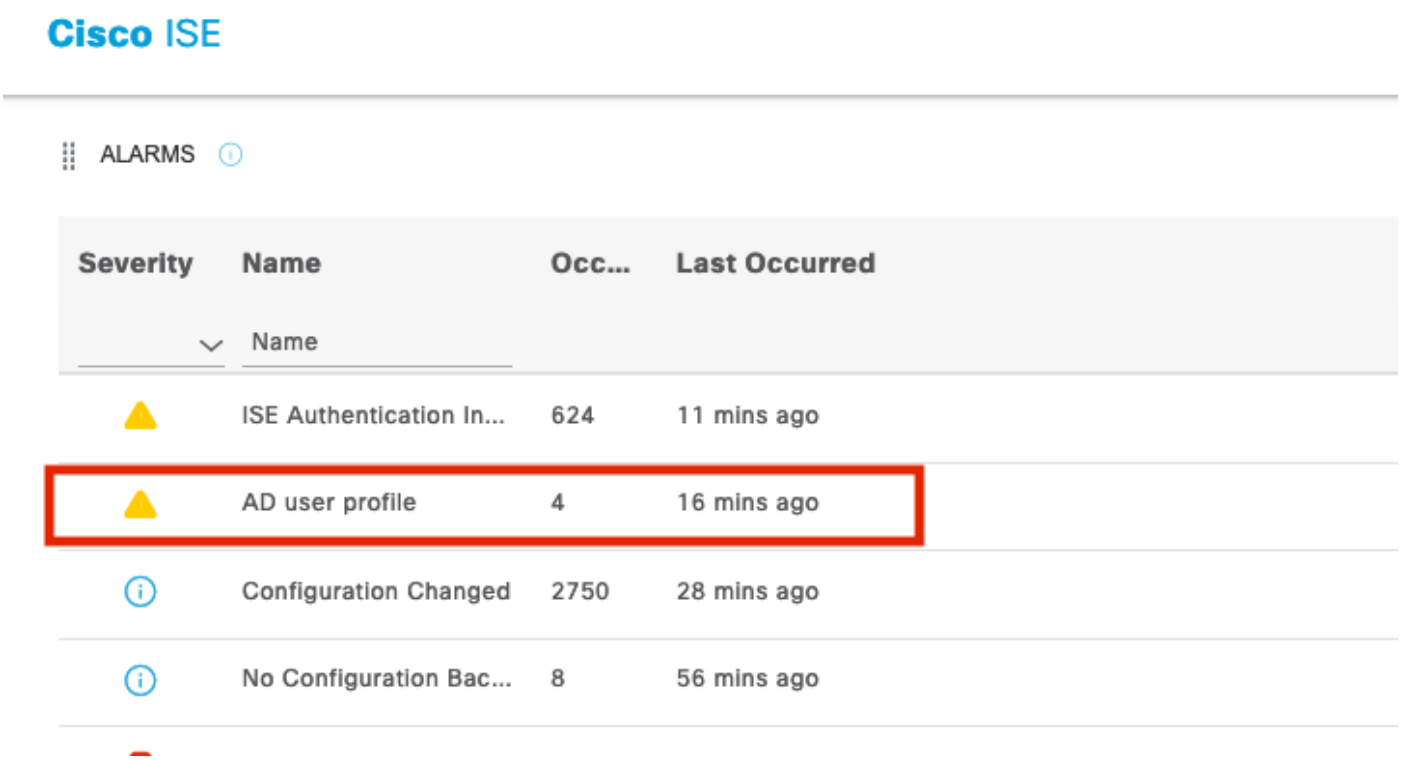
Use esta seção para confirmar se a sua configuração funciona corretamente.

Quando o ISE envia o perfil de autorização chamado no alarme para solicitação de autenticação RADIUS e atende à condição de limite dentro do intervalo de pesquisa, ele aciona o alarme visto no painel do ISE, como mostrado na imagem. O disparador para o perfil de alarme ad_user é que o perfil é empurrado mais de 5 vezes (valor limite) nos últimos 20 minutos (intervalo de sondagem).



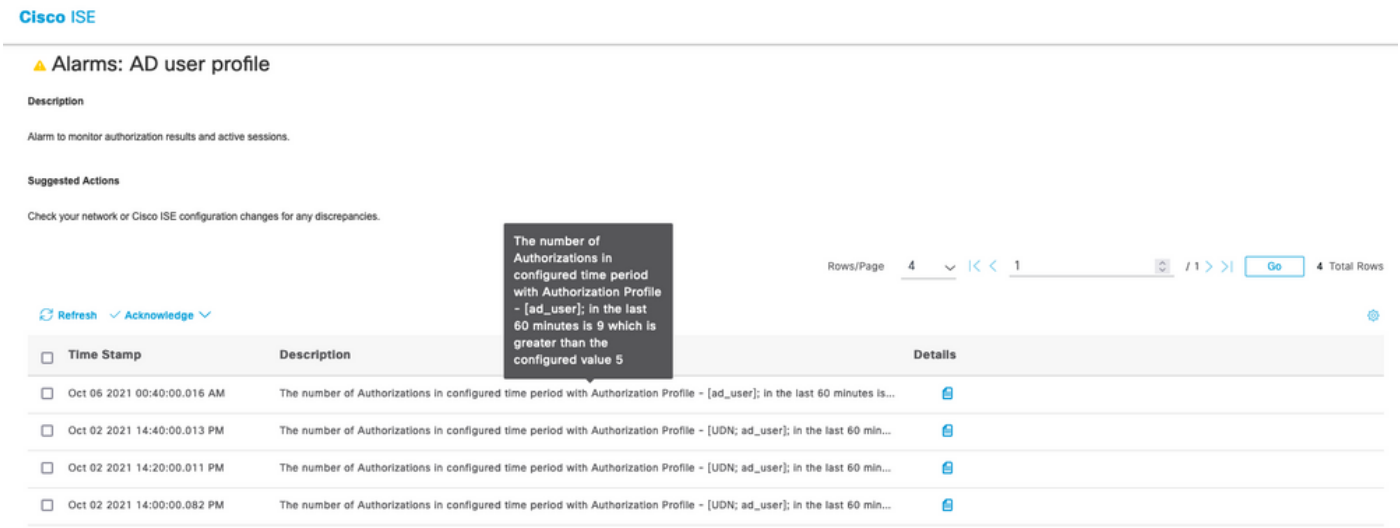
Alarmes do ISE 3.1 com base nos resultados da autorização - registros ao vivo do ISE

Etapa 1. Para verificar o alarme, navegue até ISE Dashboard e clique na janela **ALARMS**. Uma nova página da Web será aberta conforme mostrado:



Alarmes do ISE 3.1 com base nos resultados da autorização - notificação de alarme

Etapa 2. Para obter mais detalhes sobre o alarme, selecione-o e ele fornecerá mais detalhes sobre o disparador e o timestamp do alarme.

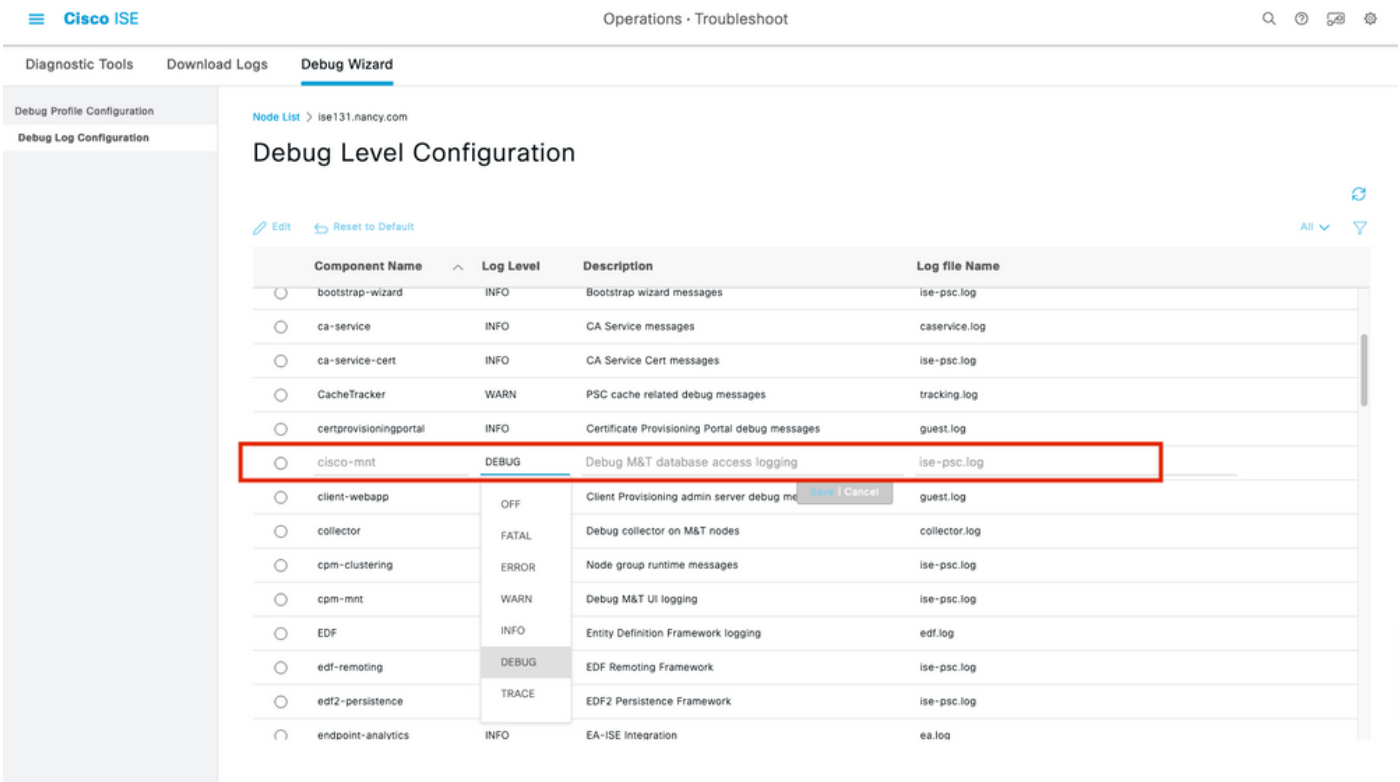


Alarmes do ISE 3.1 com base nos resultados da autorização - Detalhes do alarme

Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Para solucionar problemas relacionados ao alarme, o componente cisco-mnt no nó de monitoramento (MnT) deve estar ativado à medida que a avaliação de alarme acontece no nó MnT. Navegue até **Operations > Troubleshoot > Debug Wizard > Debug Log Configuration**. Selecione o nó no qual os serviços de monitoramento estão sendo executados e altere o Nível de log para Depurar para Nome do componente cisco-mnt, conforme mostrado:



Alarmes do ISE 3.1 com base nos resultados da autorização - configuração de depuração do ISE

Registre os trechos quando o alarme é disparado.

```
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: Se o alarme não for disparado mesmo depois que o perfil de autorização for pressionado, verifique as condições como: Inclua dados do último (minutos), Operador de Limite, Valor de Limite e intervalo de polling configurados no alarme.