根据ISE 3.1上的授权结果配置警报

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[背景信息](#)
[配置](#)
[验证](#)
[故障排除](#)

简介

本文档介绍根据身份服务引擎(ISE)上RADIUS身份验证请求的授权结果配置警报所需的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- RADIUS协议
- ISE管理员访问

使用的组件

本文档中的信息基于身份服务引擎(ISE)3.1。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

在本示例中，将为定义了阈值限制的特定授权配置文件配置自定义警报，如果ISE达到配置的授权策略上的阈值限制，将触发警报。

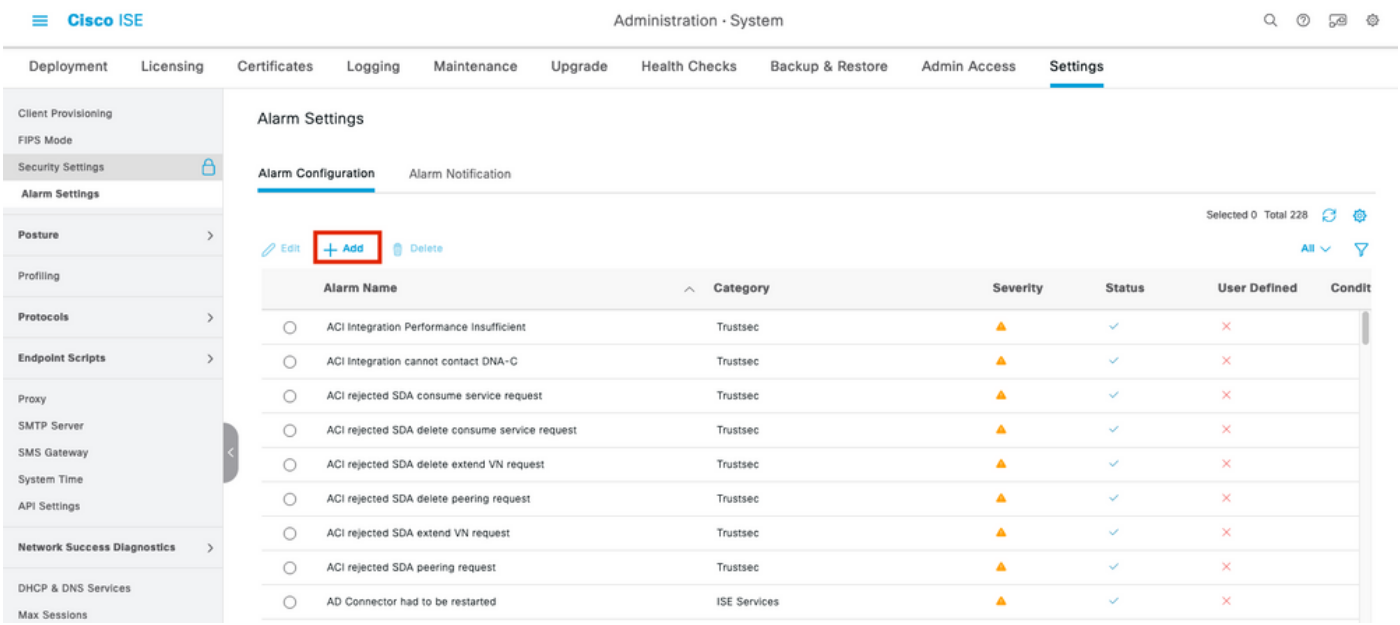
配置

在本示例中，我们将为当Active Directory(AD)用户登录时推送的授权配置文件(“ad_user”)创建警报，并根据配置的阈值触发警报。

> **注意：**对于生产服务器，阈值必须是较高的值，以避免出现大量警报。

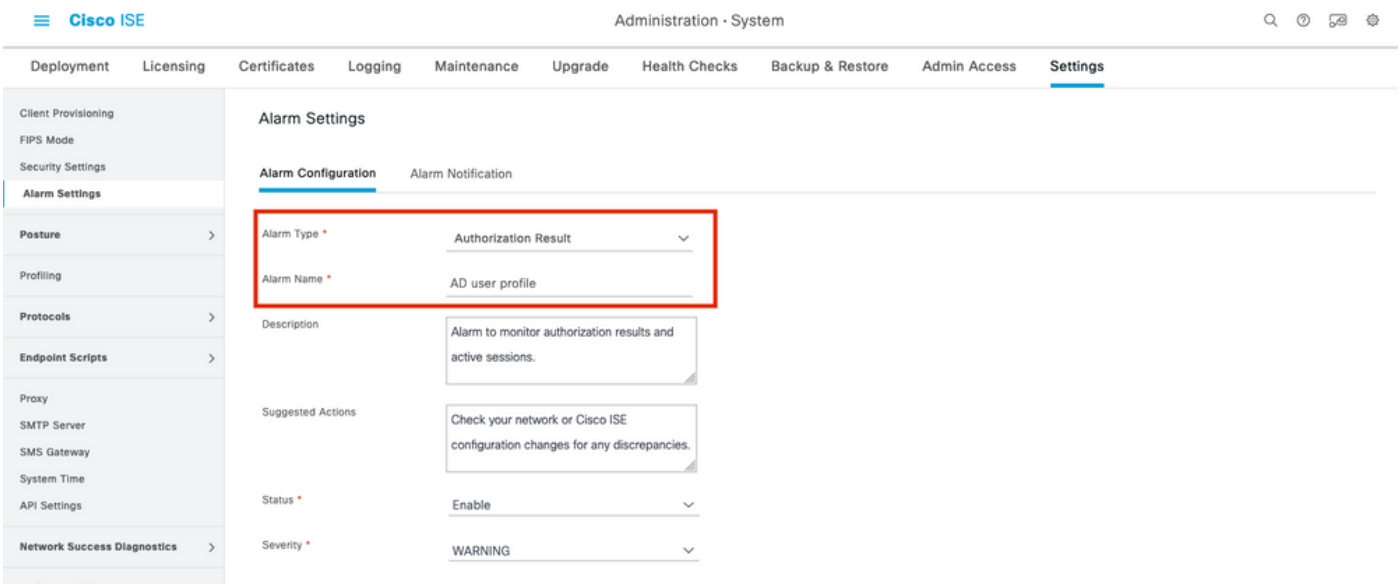
步骤1.导航至**Administration > System > Alarm Settings**。

步骤2.在Alarm Configuration下，单击**Add**创建警报，如图所示。



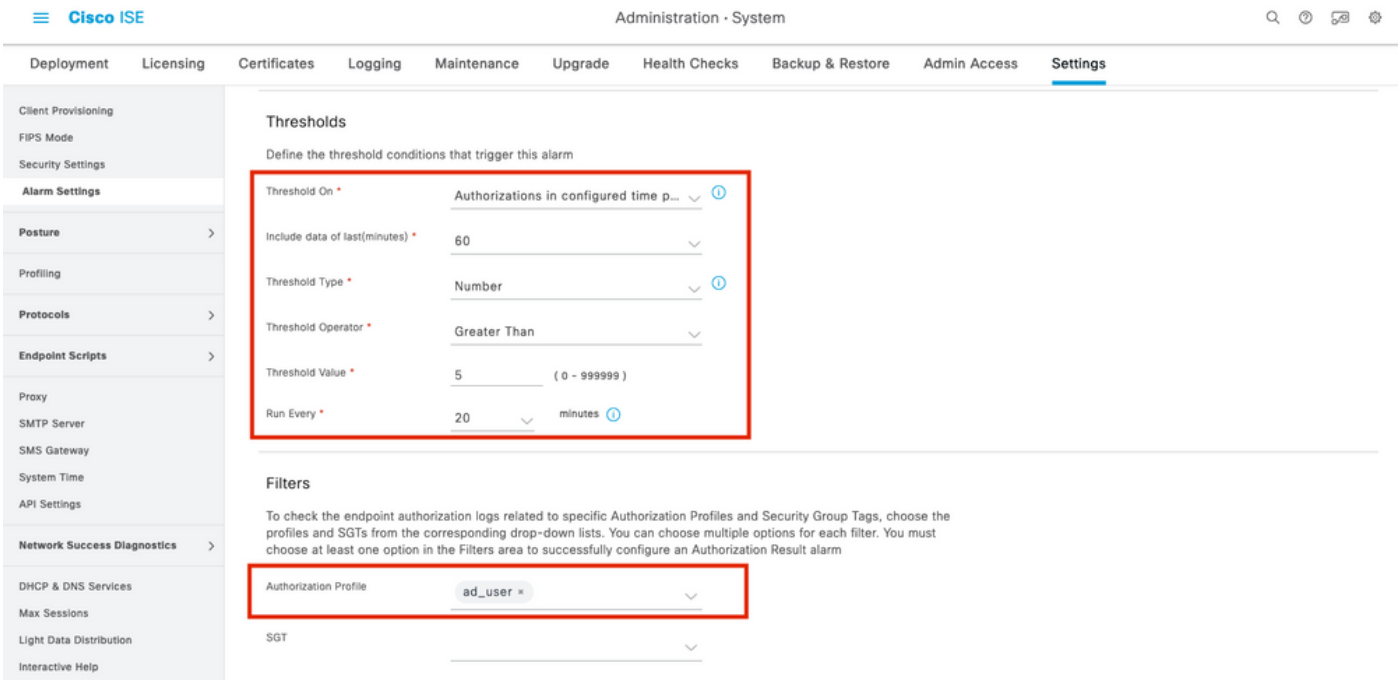
基于授权结果的ISE 3.1警报 — 警报设置

步骤3.选择警报类型作为授**权结**果并输入警报名称，如图所示。



基于授权结果的ISE 3.1警报 — 配置警报

步骤4.在“阈值”**部分**，在“阈值开”下**拉菜单中**选择“配置的时间段内授权”，并为“阈值”和必填字段输入适当的值。在过滤器部分，调用必须触发警报的授权配置文件，如图所示。



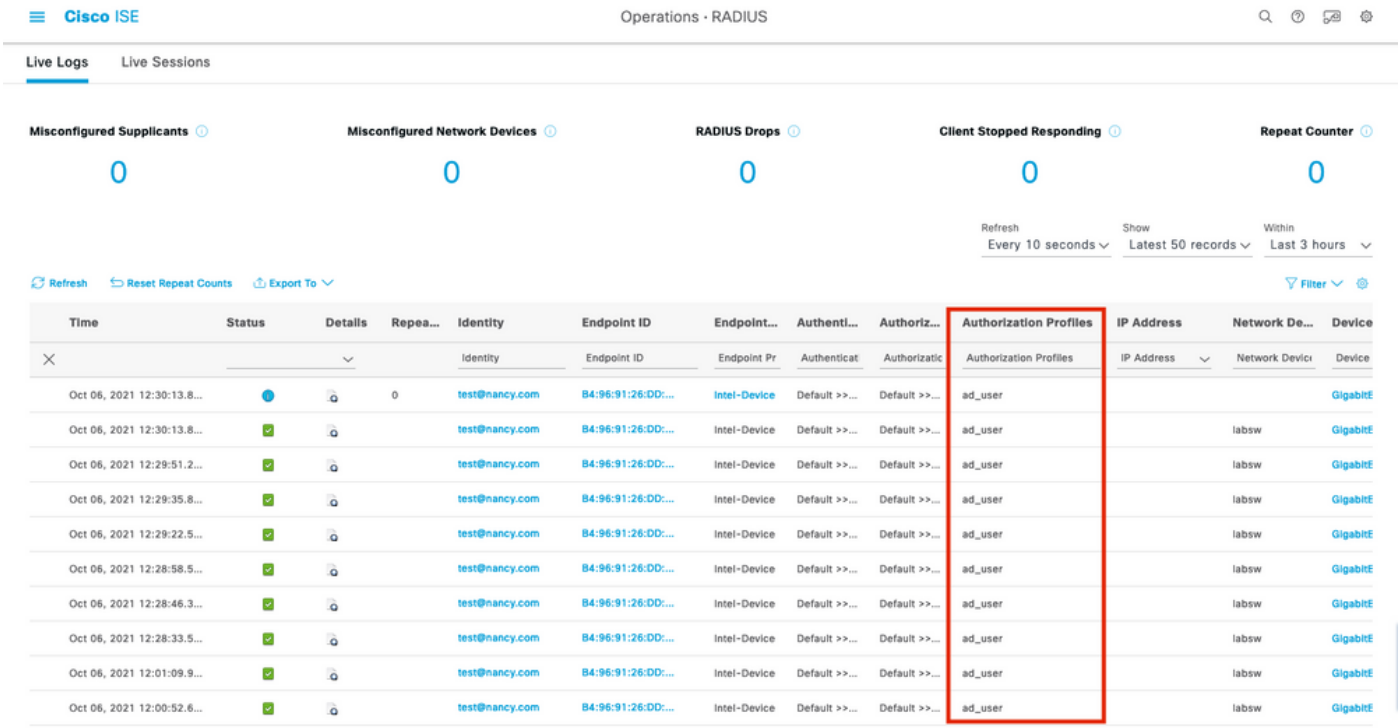
基于授权结果的ISE 3.1警报 — 配置警报阈值

> **注意**：确保在Policy > Policy Elements > Results > Authorization > Authorization Profiles下定义用于警报的授**权配置文件。**

验证

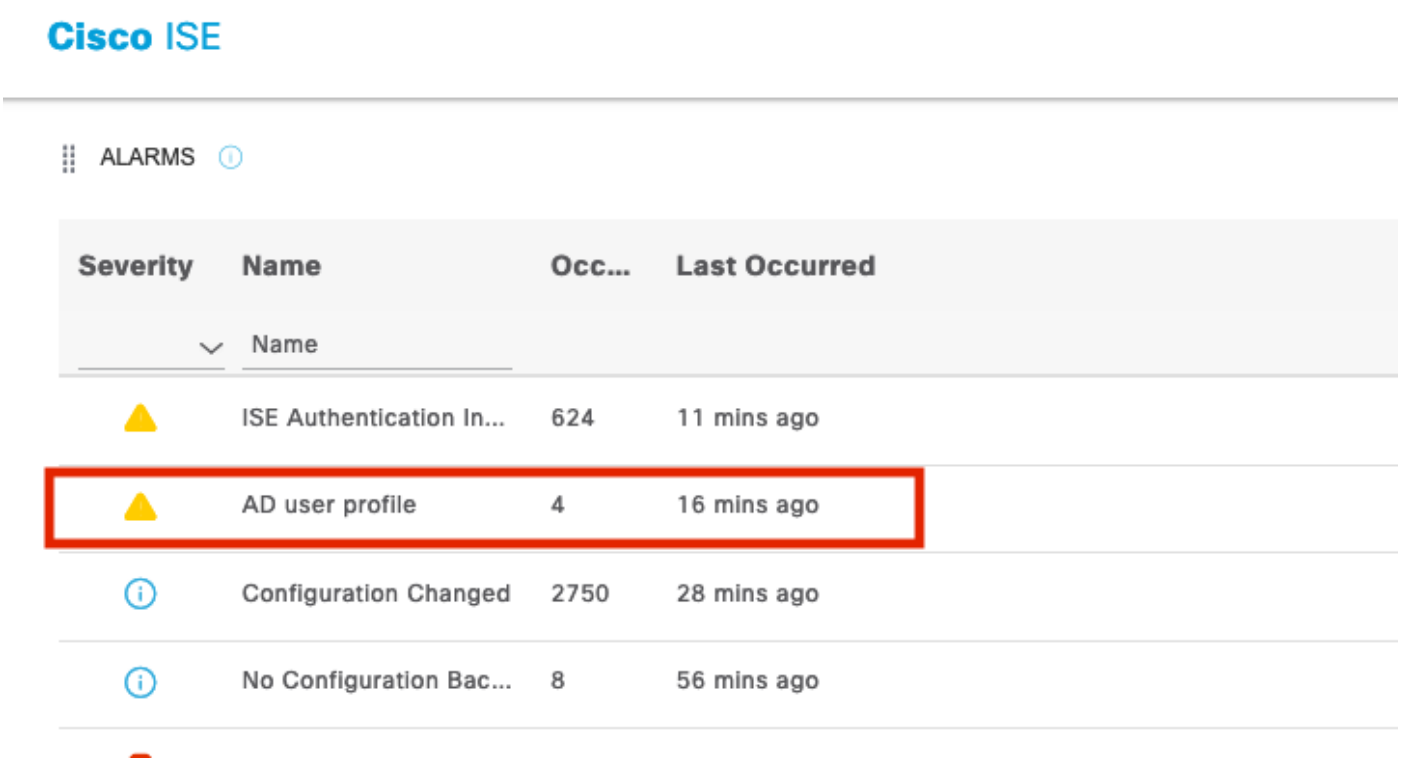
使用本部分可确认配置能否正常运行。

当ISE推送RADIUS身份验证请求警报中调用的授权配置文件并满足轮询间隔内的阈值条件时，它将触发ISE控制面板中显示的警报，如图所示。警报ad_user配置文件的触发器是配置文件在过去20分钟（轮询间隔）内被推送了5次以上（阈值）。



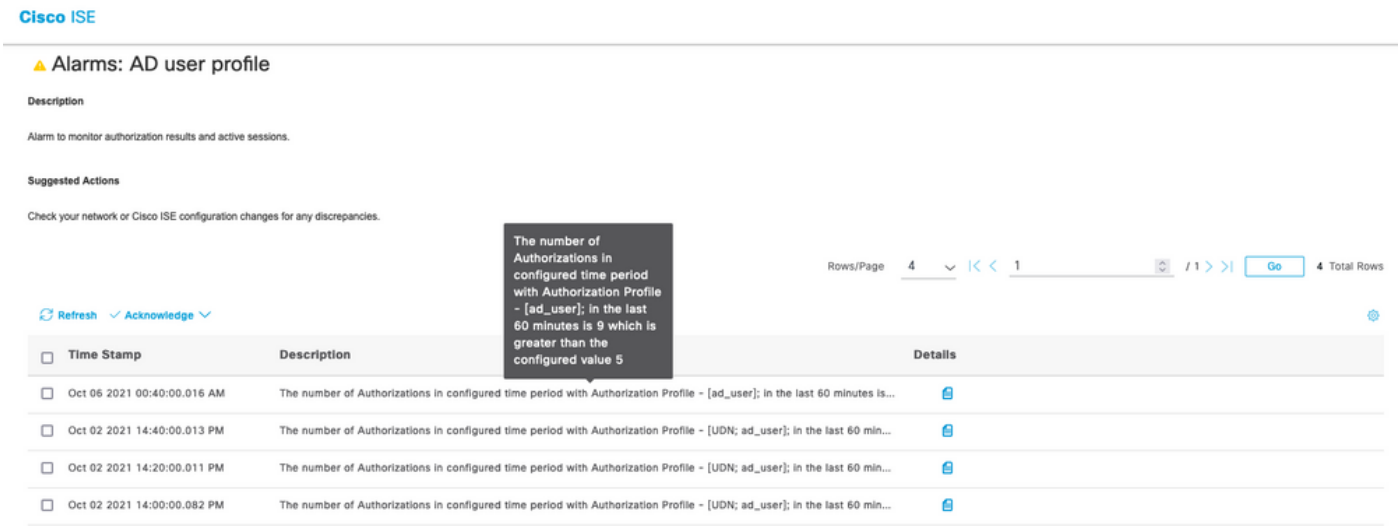
基于授权结果的ISE 3.1警报 — ISE实时日志

步骤1.要检查警报，请导航至ISE控制面板并点击**ALARMS窗口**。新网页将打开，如下所示：



基于授权结果的ISE 3.1警报 — 警报通知

步骤2.要获取警报的更多详细信息，请选择警报，它将提供有关警报触发和时间戳的更多详细信息。

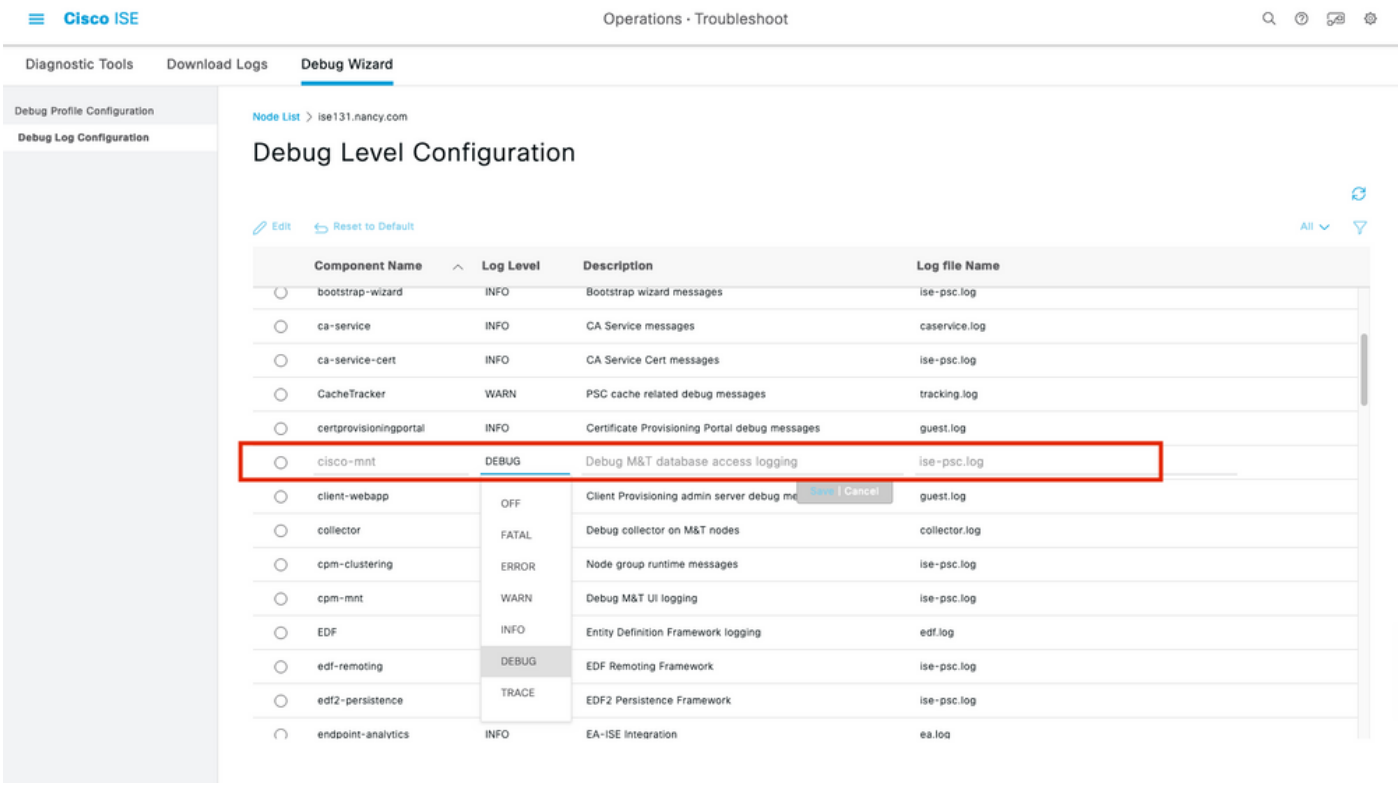


基于授权结果的ISE 3.1警报 — 警报详细信息

故障排除

本部分提供了可用于对配置进行故障排除的信息。

要排除与警报相关的问题，必须在MnT节点上发生警报评估时启用监控节点(MnT)上的cisco-mnt组件。导航至**操作>故障排除>调试向导>调试日志配置**。选择正在运行监控服务的节点，并将Log Level（日志级别）更改为Debug for Component Name cisco-mnt，如下所示：



基于授权结果的ISE 3.1警报 — ISE调试配置

触发警报时记录片段。

```
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={65,108,97,114,109,32,116,111,32,1
09,111,110,105,116,111,114,32,97,117,116,104,111,114,105,122,97,116,105,111,110,32,114,101,115,1
17,108,116,115,32,97,110,100,32,97,99,116,105,118,101,32,115,101,115,115,105,111,110,115,46},

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]
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,filterCondi
tionOperator=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,filterConditio
```

```
nOperator=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={65,108,97,114,109,32,116,111,32,1
09,111,110,105,116,111,114,32,97,117,116,104,111,114,105,122,97,116,105,111,110,32,114,101,115,1
17,108,116,115,32,97,110,100,32,97,99,116,105,118,101,32,115,101,115,115,105,111,110,115,46},

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:如果警报在推送授权配置文件后仍未触发，请检查以下情况：包括警报中配置的最后（分钟）、阈值运算符、阈值和轮询间隔的数据。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。