根據ISE 3.1上的授權結果配置警報

目錄

簡介

本文檔介紹根據身份服務引擎(ISE)上的RADIUS身份驗證請求的授權結果配置警報所需的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- RADIUS通訊協定
- ISE管理員訪問許可權

採用元件

本檔案中的資訊是根據身分識別服務引擎(ISE)3.1。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

在此示例中，為特定授權配置檔案配置自定義警報，並定義閾值限制，如果ISE達到配置的授權策略閾值限制，將觸發警報。

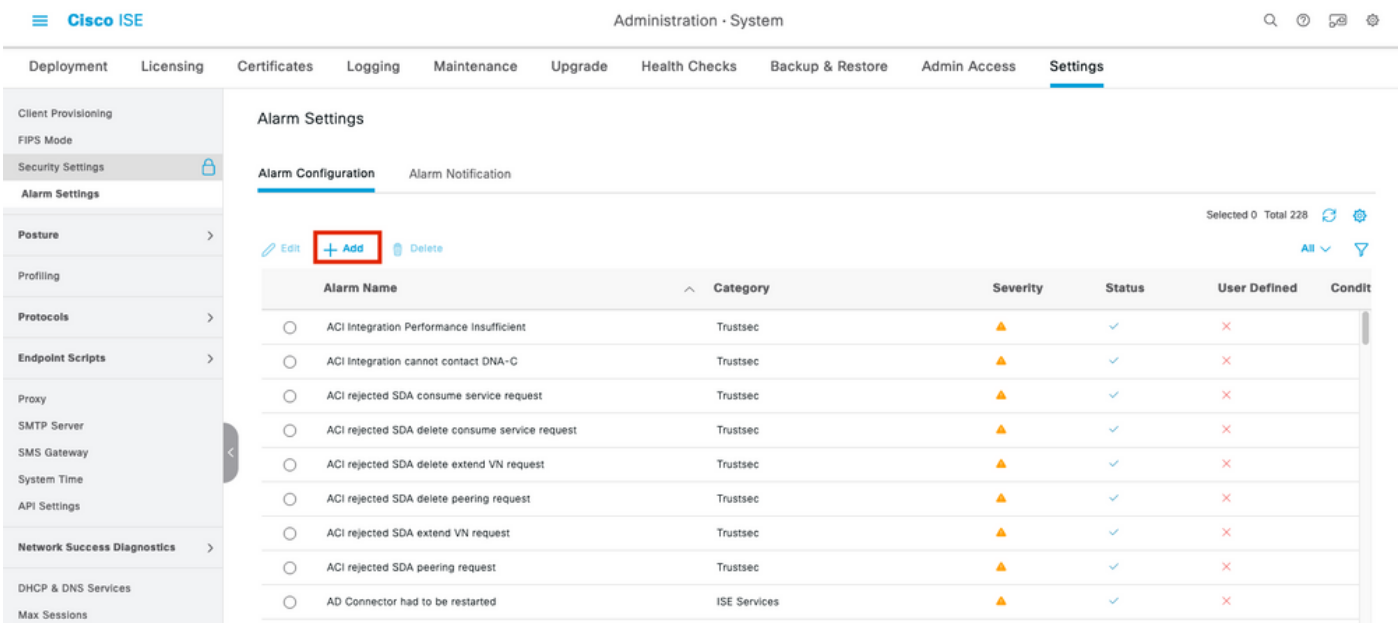
設定

在本示例中，我們將為Active Directory(AD)使用者登入時推送的授權配置檔案(「ad_user」)建立警報，並根據配置的閾值觸發警報。

> **附註**：對於生產伺服器，閾值必須是更高的值，以避免出現大量警報。

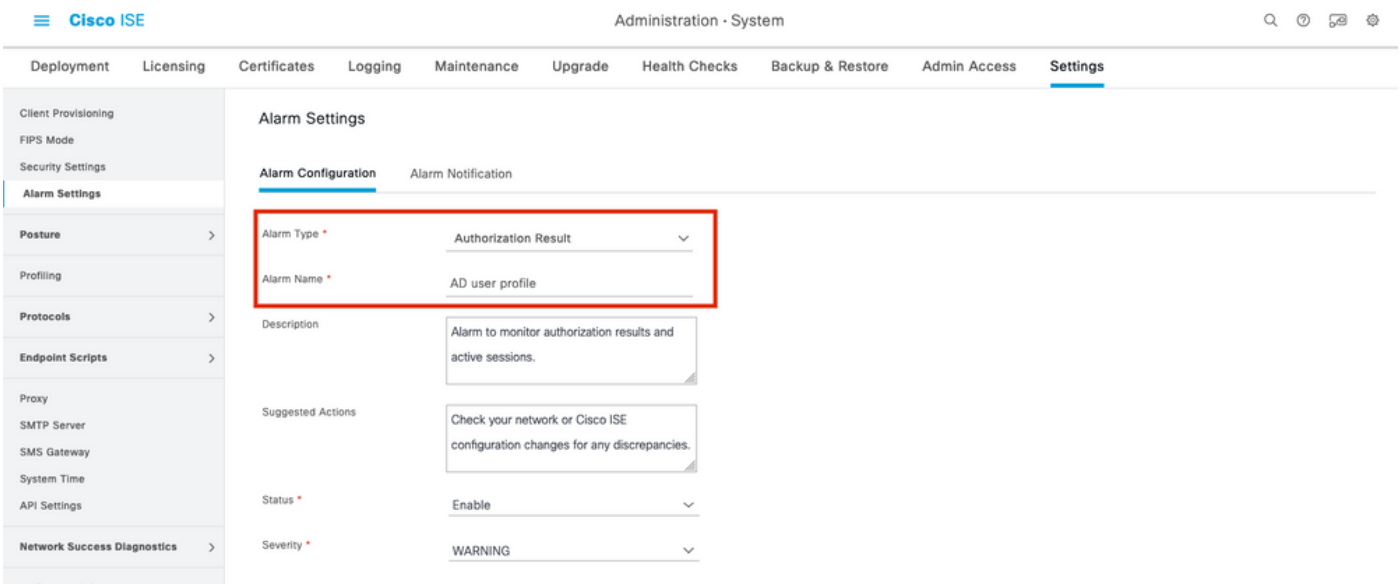
步驟1.導覽至**Administration > System > Alarm Settings**。

步驟2.在「Alarm Configuration」下，按一下**Add**以建立一個警報，如下圖所示。



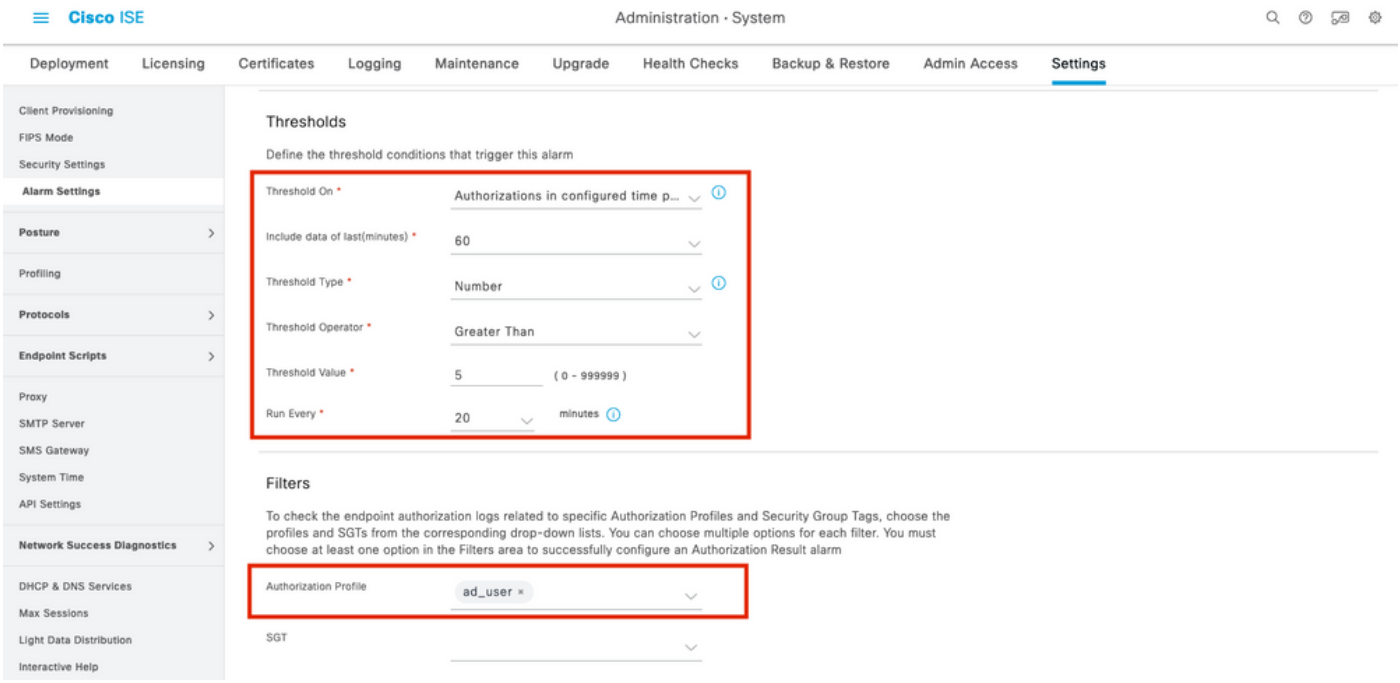
基於授權結果的ISE 3.1警報 — 警報設定

步驟3.選擇警報型別作為**Authorization Result**，然後輸入警報名稱，如下圖所示。



基於授權結果的ISE 3.1警報 — 配置警報

步驟4.在**Threshold**部分，在Threshold On下拉選單中選擇**Authorization in configured time period**，然後為Threshold和必填欄位輸入適當的值。在過濾部分，呼叫必須觸發警報的授權配置檔案，如下圖所示。



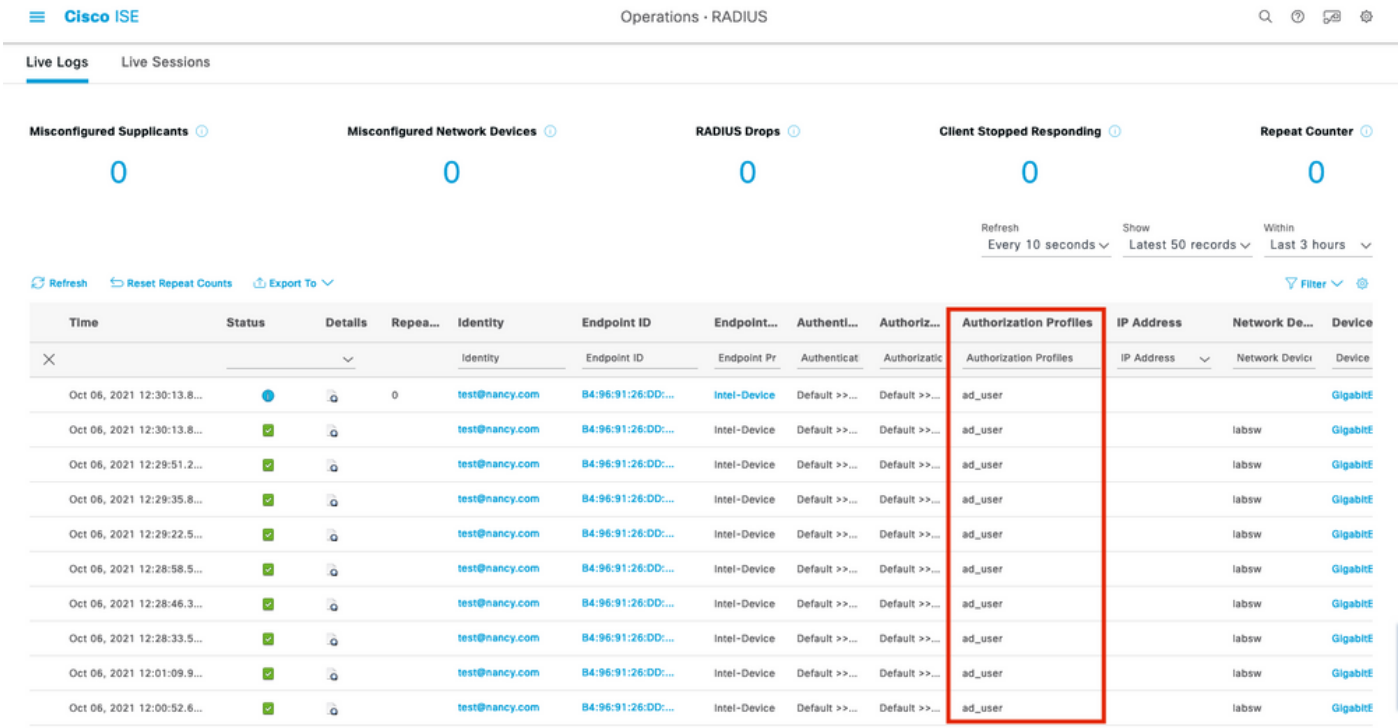
基於授權結果的ISE 3.1警報 — 配置警報閾值

> **附註**：確保在**Policy > Policy Elements > Results > Authorization > Authorization Profiles**下定義用於警報的授權配置檔案。

驗證

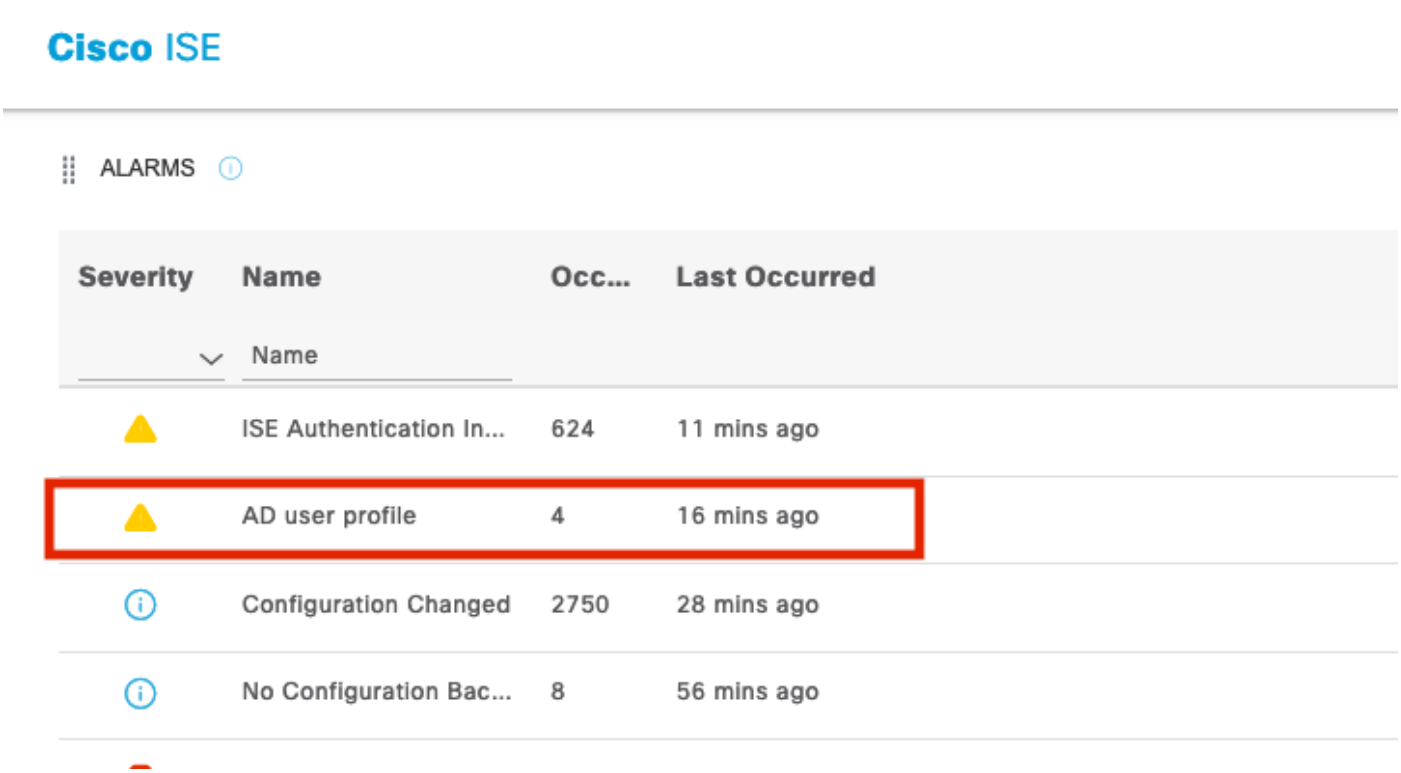
使用本節內容，確認您的組態是否正常運作。

當ISE推送警報中為RADIUS身份驗證請求呼叫的授權配置檔案並在輪詢間隔內滿足閾值條件時，它將觸發ISE控制面板中顯示的警報，如圖所示。alarm ad_user配置檔案的觸發機制是在最近20分鐘（輪詢間隔）內推送配置檔案超過5次（閾值）。



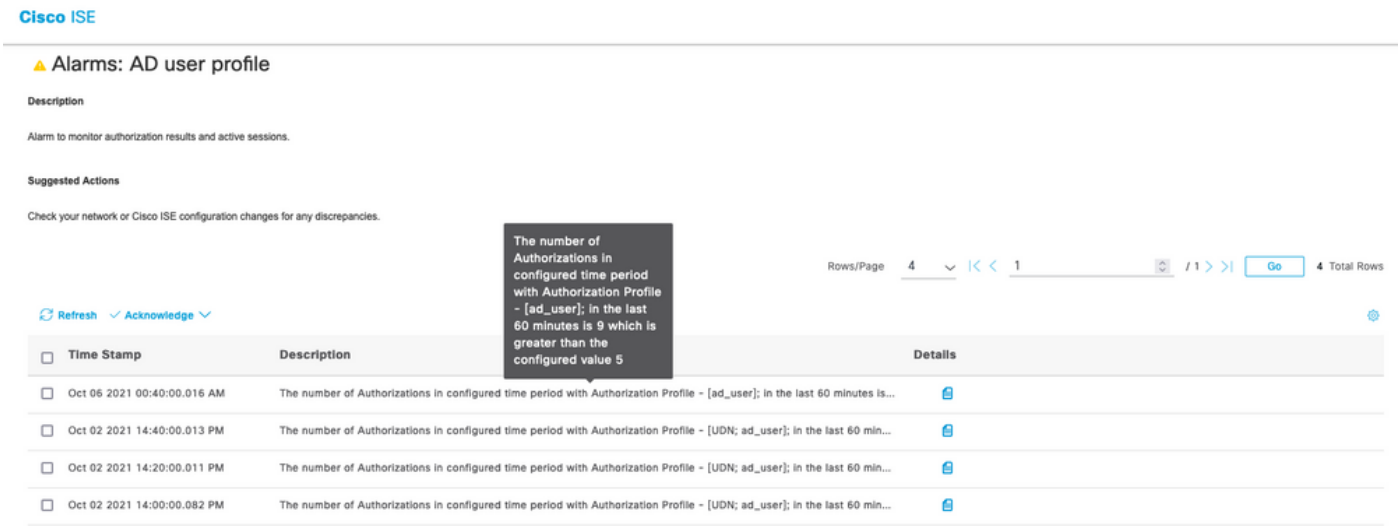
基於授權結果的ISE 3.1警報 — ISE即時日誌

步驟1。要檢查警報，請導航到ISE儀表板並按一下**ALARMS**視窗。將開啟一個新網頁，如下所示：



基於授權結果的ISE 3.1警報 — 警報通知

步驟2.要獲取警報的更多詳細資訊，請選擇警報，它將提供有關警報觸發和時間戳的更多詳細資訊。

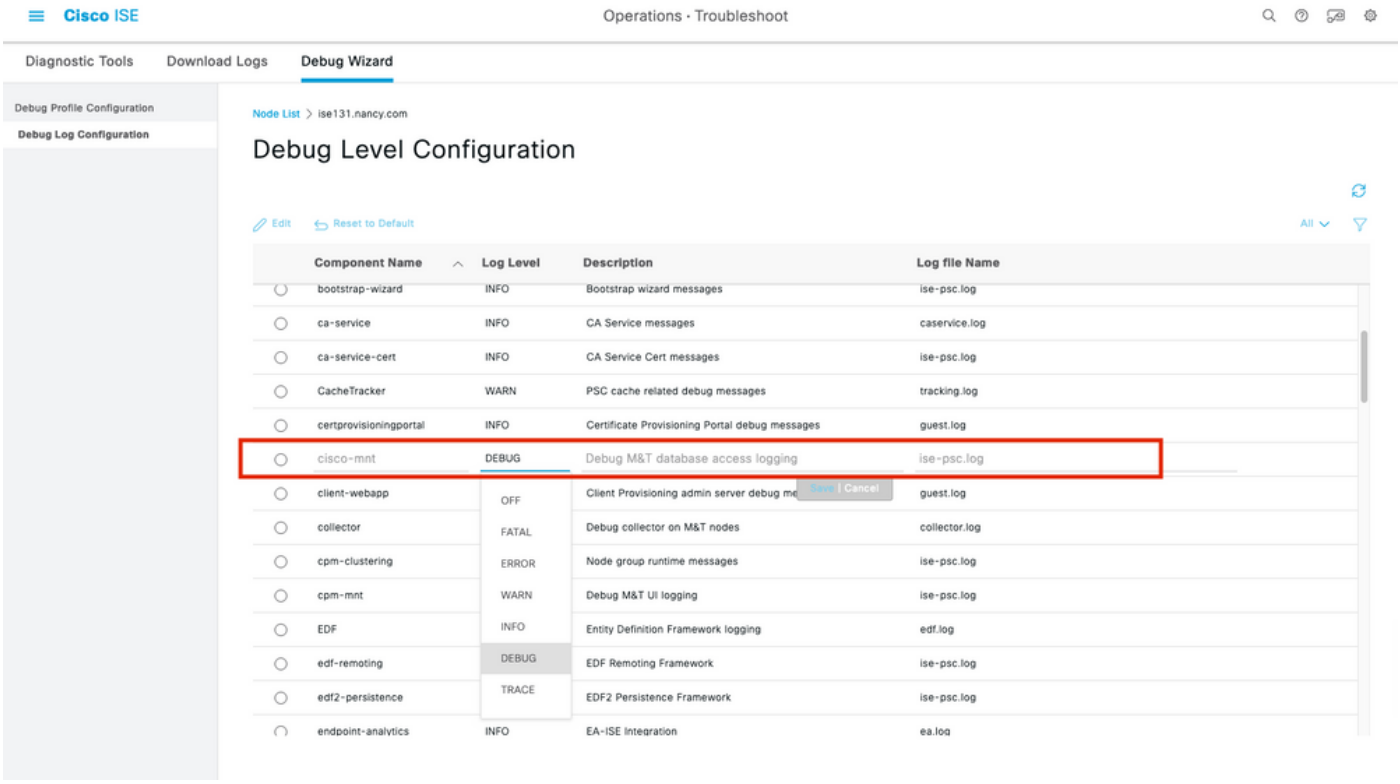


基於授權結果的ISE 3.1警報 — 警報詳細資訊

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

若要排解與警報相關的問題，必須啟用監控節點(MnT)上的cisco-mnt元件，因為MnT節點上會發生警報評估。導航到**操作>故障排除>調試嚮導>調試日誌配置**。選擇正在運行監控服務的節點，並將元件名稱cisco-mnt的日誌級別更改為調試，如下所示：



基於授權結果的ISE 3.1警報 — ISE調試配置

觸發警報時記錄片段。

```
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
```

附註：如果在推送授權配置檔案後仍未觸發警報，請檢查以下條件：包括警報中配置的過去（分鐘）、閾值操作員、閾值和輪詢間隔的資料。