ISE 3.1の許可結果に基づくアラームの設定

内容

概要

このドキュメントでは、Identity Services Engine(ISE)でのRADIUS認証要求の許可結果に基づいてアラームを設定するために必要な手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- RADIUS プロトコル
- ISE管理アクセス

使用するコンポーネント

このドキュメントの情報は、Identity Services Engine(ISE)3.1に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

この例では、しきい値の制限が定義された特定の認可プロファイルに対してカスタムアラームを設定し、設定された認可ポリシーのしきい値にISEが到達すると、アラームがトリガーされます。

設定

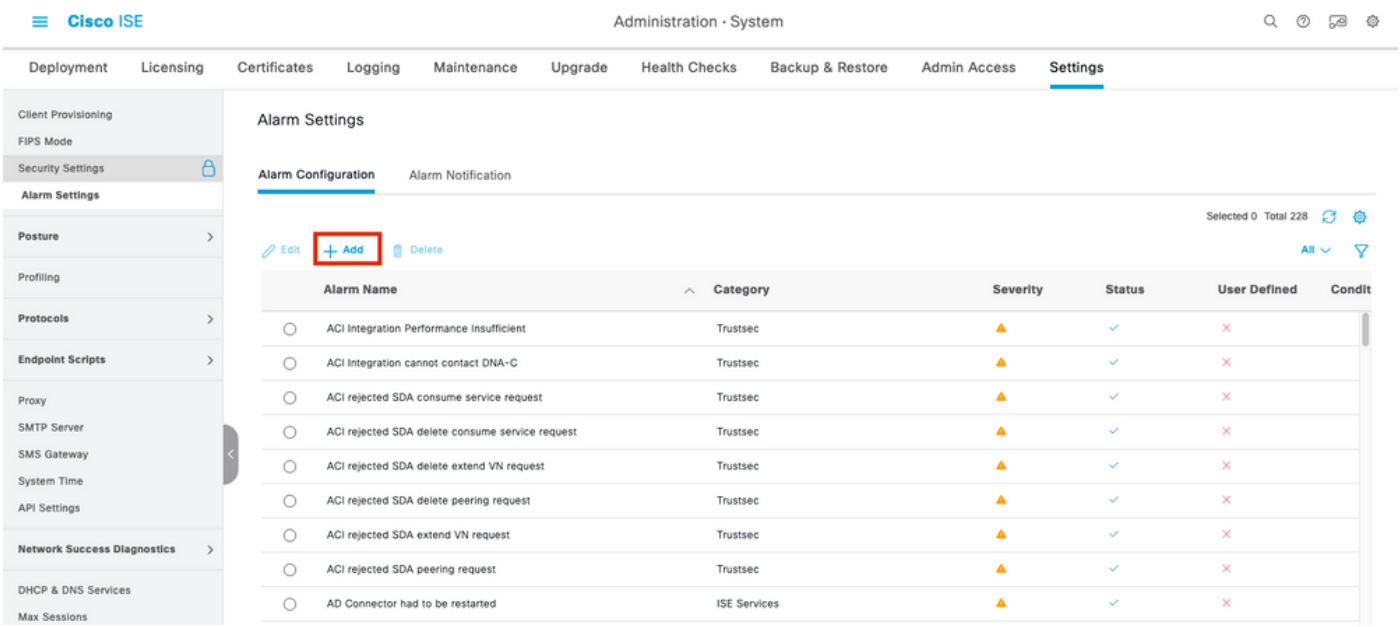
この例では、Active Directory(AD)ユーザがログインしたときにプッシュされる認可プロファイル

(「ad_user」)のアラームを作成し、設定されたしきい値に基づいてアラームをトリガーします。

> **注**：実稼働サーバでは、アラームが大きく発生するのを防ぐために、しきい値を高い値にする必要があります。

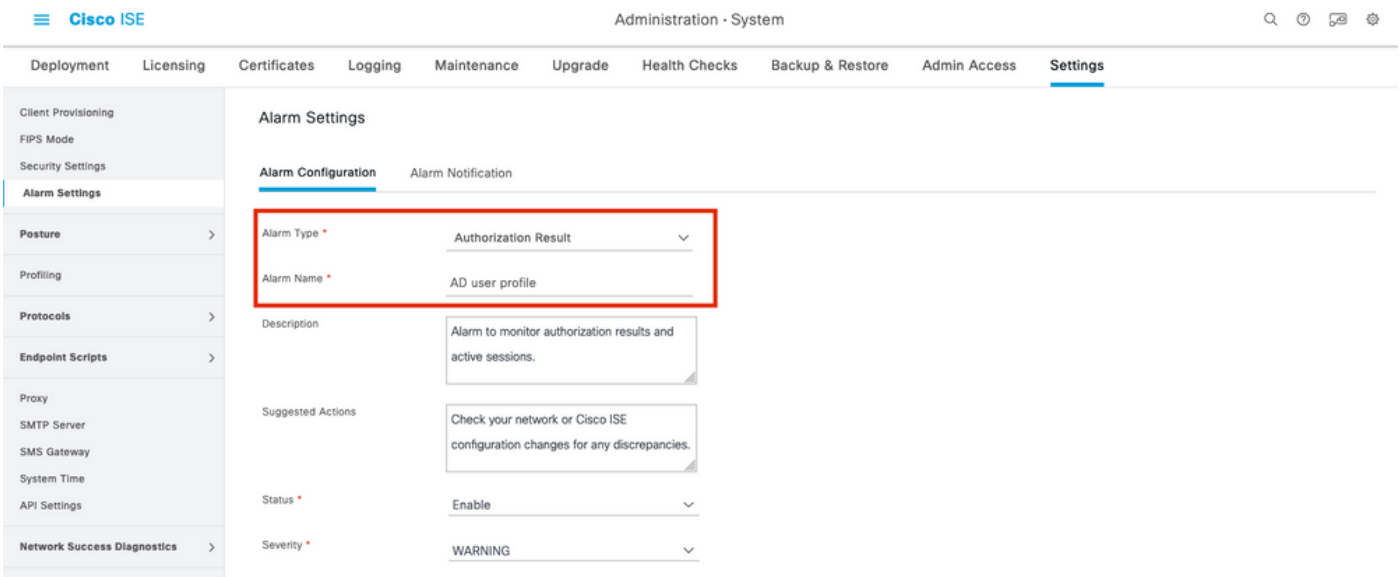
ステップ1:[**Administration**] > [**System**] > [**Alarm Settings**]**に移動します**。

ステップ2:[Alarm Configuration]で、[**Add**]をクリックして、図に示すようにアラームを作成します。



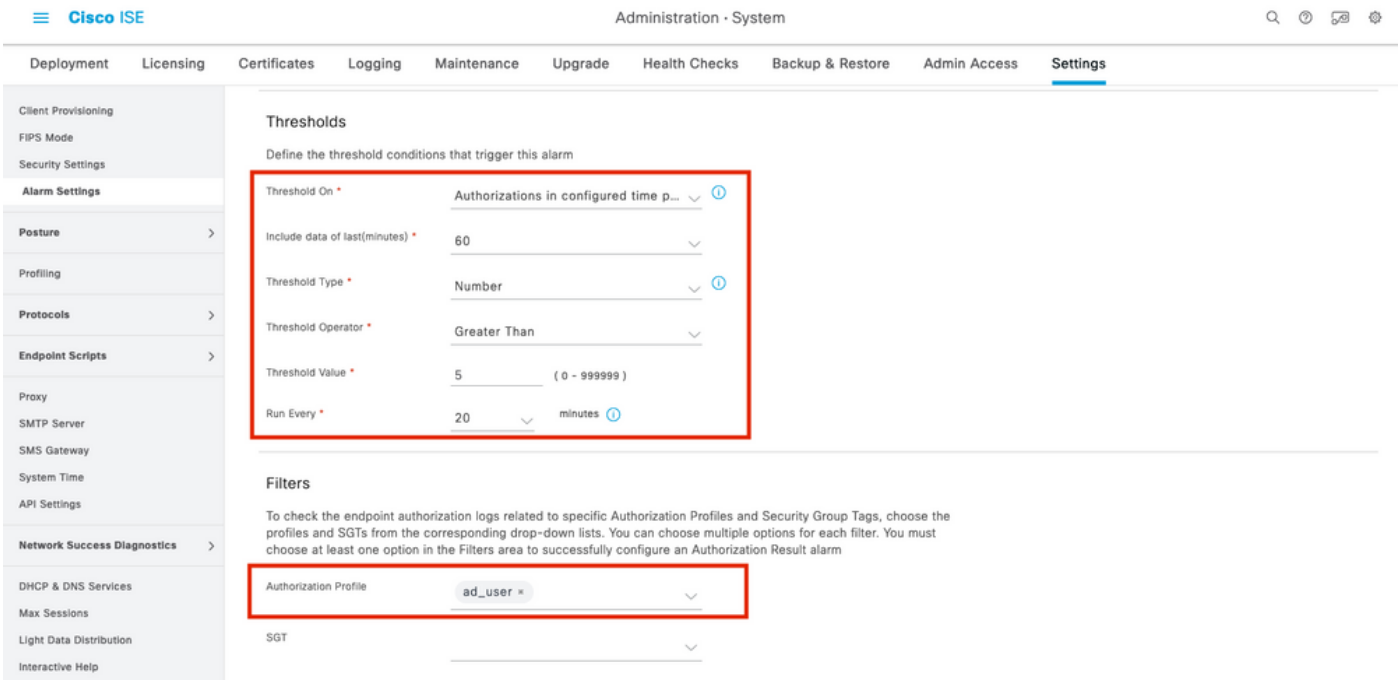
許可結果に基づくISE 3.1アラーム：アラーム設定

ステップ3:[Alarm Type]で[**Authorization Result**]を選択し、図に示すようにアラーム名を入力します。



許可結果に基づくISE 3.1アラーム：アラームの設定

ステップ4:[Threshold]セクションで、[Threshold On]ドロップダウンで**設定した期間の認可を選択**し、[Threshold]フィールドと必須フィールドに適切な値を入力します。フィルタセクションで、図に示すように、アラームをトリガーする必要がある認可プロファイルを呼び出します。



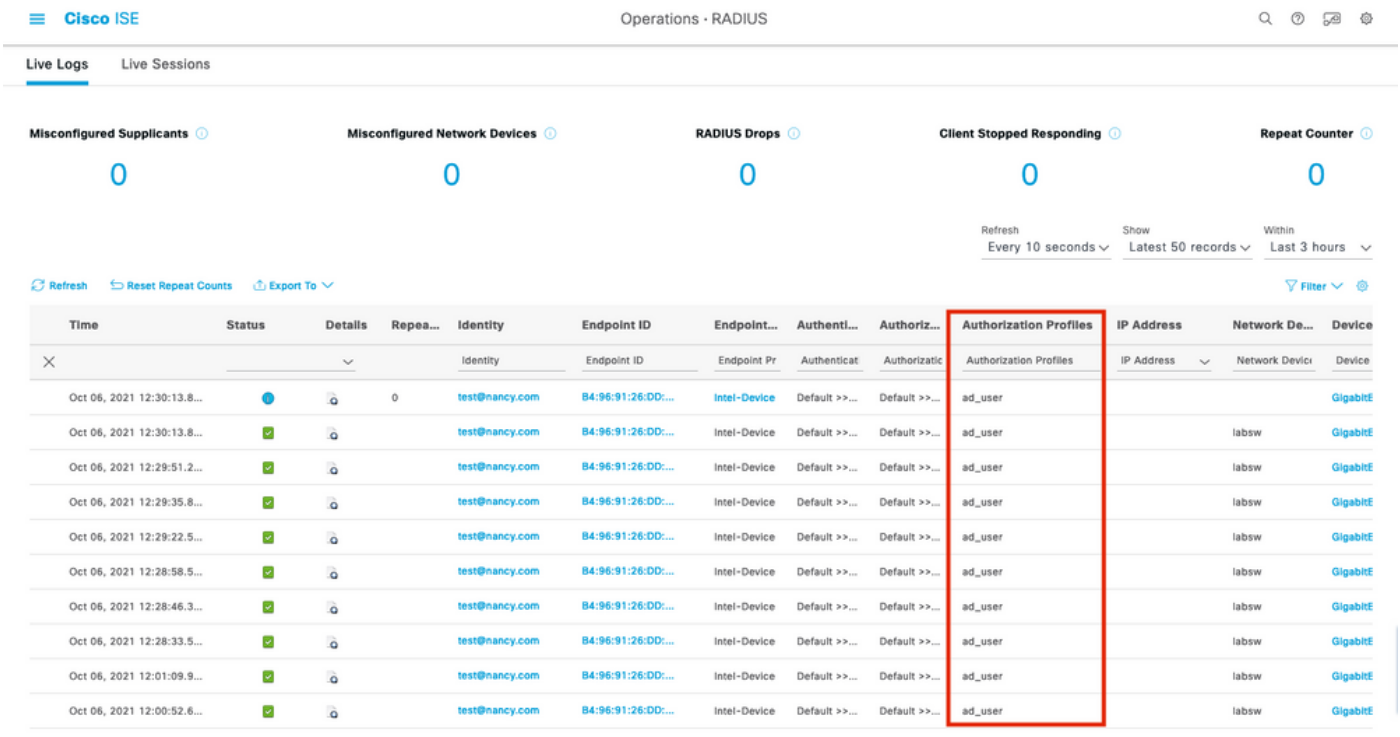
許可結果に基づくISE 3.1アラーム：アラームしきい値の設定

> **注：アラームに使用する認可プロファイルが[Policy] > [Policy Elements] > [Results] > [Authorization] > [Authorization Profiles]で定義されていることを確認します。**

確認

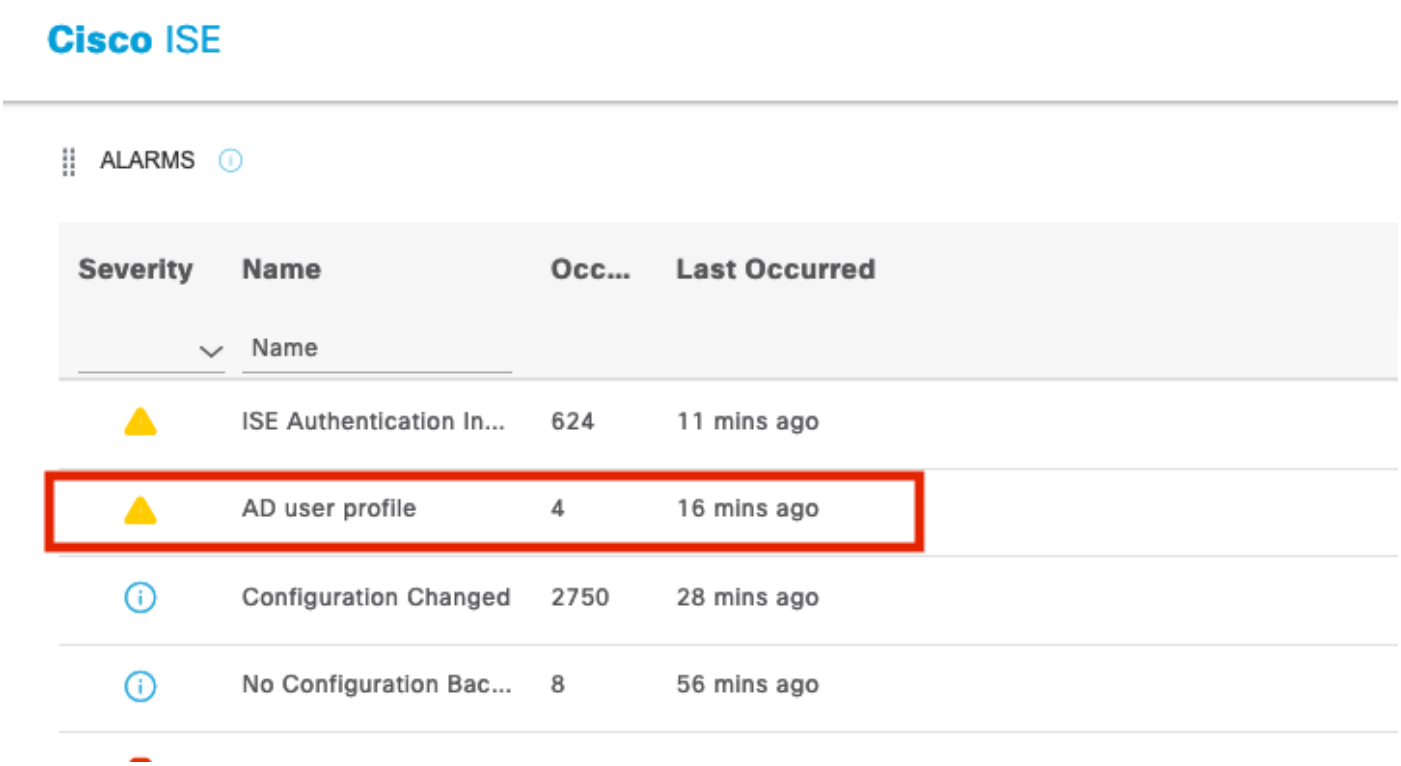
ここでは、設定が正常に機能しているかどうかを確認します。

ISEがRADIUS認証要求のアラームで呼び出された認可プロファイルをプッシュし、ポーリング間隔内のしきい値条件を満たすと、図に示すように、ISEダッシュボードに表示されるアラームがトリガーされます。アラームad_userプロファイルのトリガーは、過去20分間（ポーリング間隔）にプロファイルが5倍以上（しきい値）プッシュされることです。



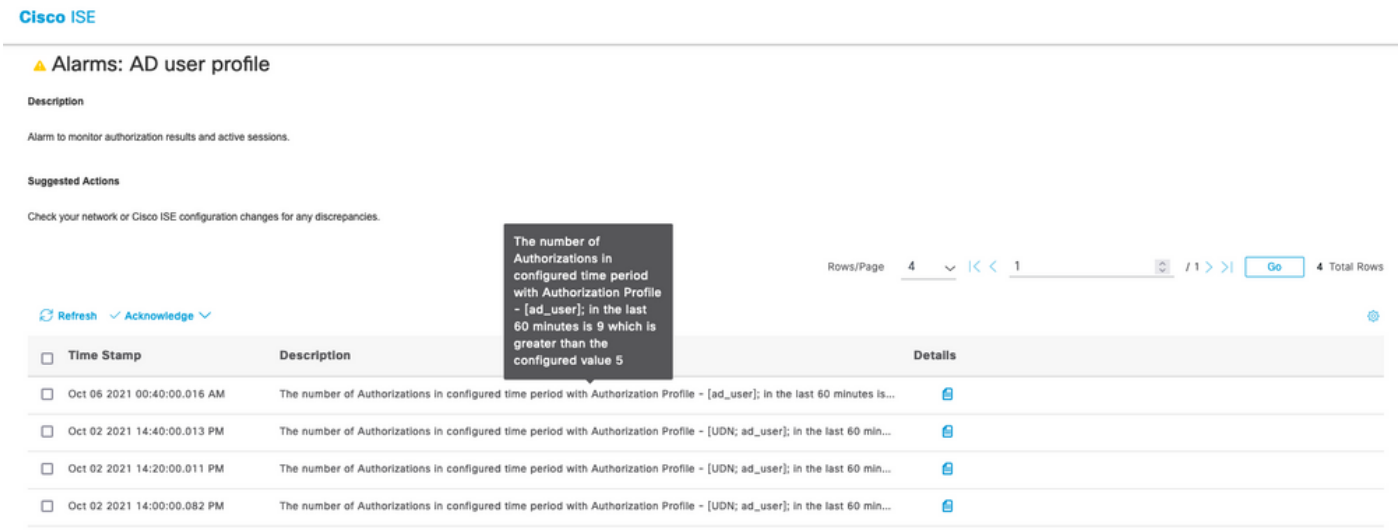
許可結果に基づくISE 3.1アラーム：ISEライブログ

ステップ1：アラームを確認するには、[ISE Dashboard]に移動し、[ALARMS]ウィンドウをクリックします。新しいWebページが次のように開きます。



許可結果に基づくISE 3.1アラーム：アラーム通知

ステップ2：アラームの詳細を取得するには、アラームを選択します。アラームのトリガーとタイムスタンプの詳細が表示されます。



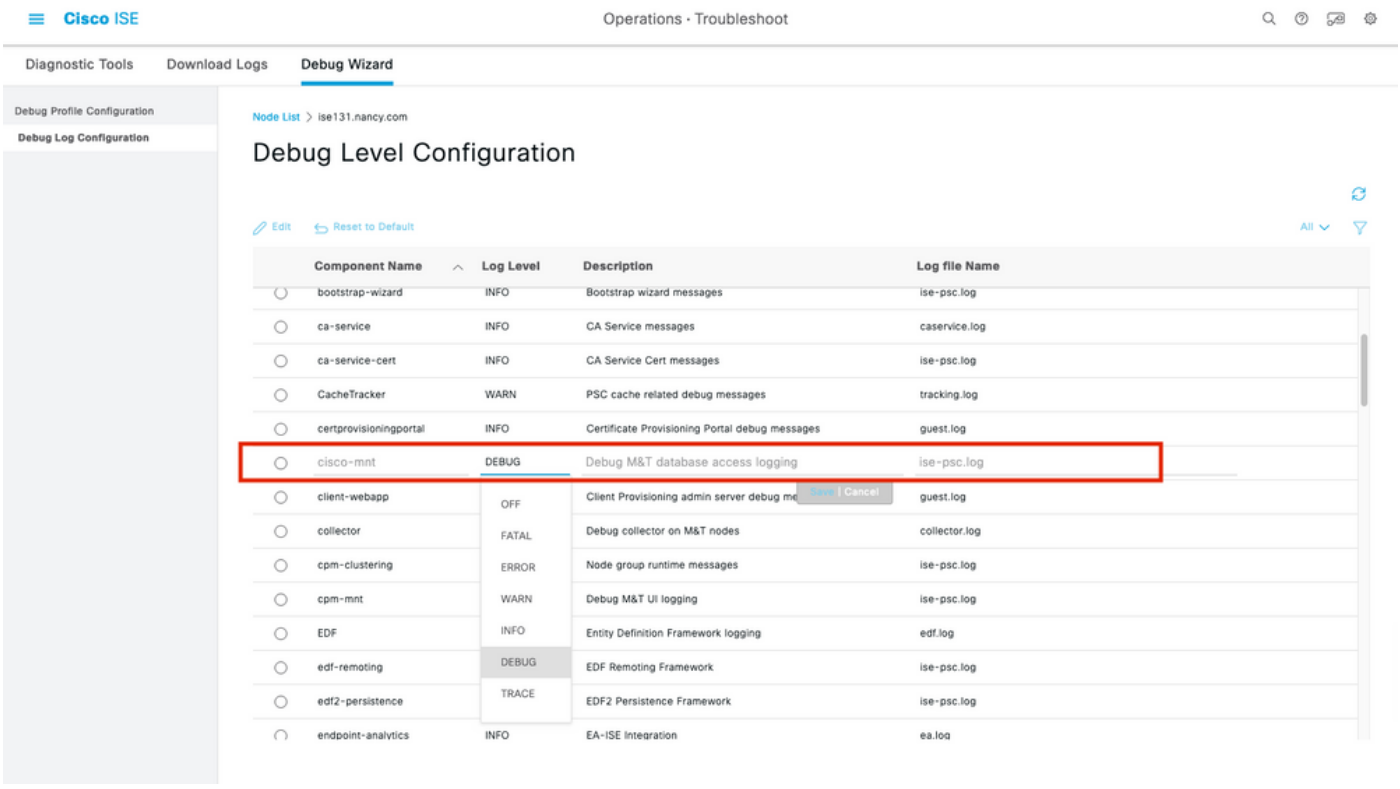
許可結果に基づくISE 3.1アラーム：アラームの詳細

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

アラームに関連する問題をトラブルシューティングするには、MnTノードでアラーム評価が行われるため、モニタリングノード(MnT)のcisco-mntコンポーネントを有効にする必要があります。

[Operations] > [Troubleshoot] > [Debug Wizard] > [Debug Log Configuration]に移動します。次に示すように、モニタリングサービスが実行されているノードを選択し、[Log Level]を[Debug for Component Name]に[cisco-mnt]に変更します。



許可結果に基づくISE 3.1アラーム：ISEデバッグ設定

アラームがトリガーされたときにスニペットをログに記録します。

```
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
```

注：認可プロファイルがプッシュされた後でもアラームがトリガーされない場合は、次のような条件を確認します。アラームで設定された最後（分）、しきい値演算子、しきい値、ポーリング間隔のデータを含めます。