ISE 3.1의 권한 부여 결과를 기반으로 경보 구성

목차

소개

이 문서에서는 ISE(Identity Services Engine)에서 RADIUS 인증 요청에 대한 권한 부여 결과를 기반으로 경보를 구성하는 데 필요한 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- RADIUS 프로토콜
- ISE 관리자 액세스

사용되는 구성 요소

이 문서의 정보는 ISE(Identity Services Engine) 3.1을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

이 예에서는 임계값 제한이 정의된 특정 권한 부여 프로파일에 대해 사용자 지정 알람이 구성되고 ISE가 구성된 권한 부여 정책의 임계값 제한에 도달하면 경보가 트리거됩니다.

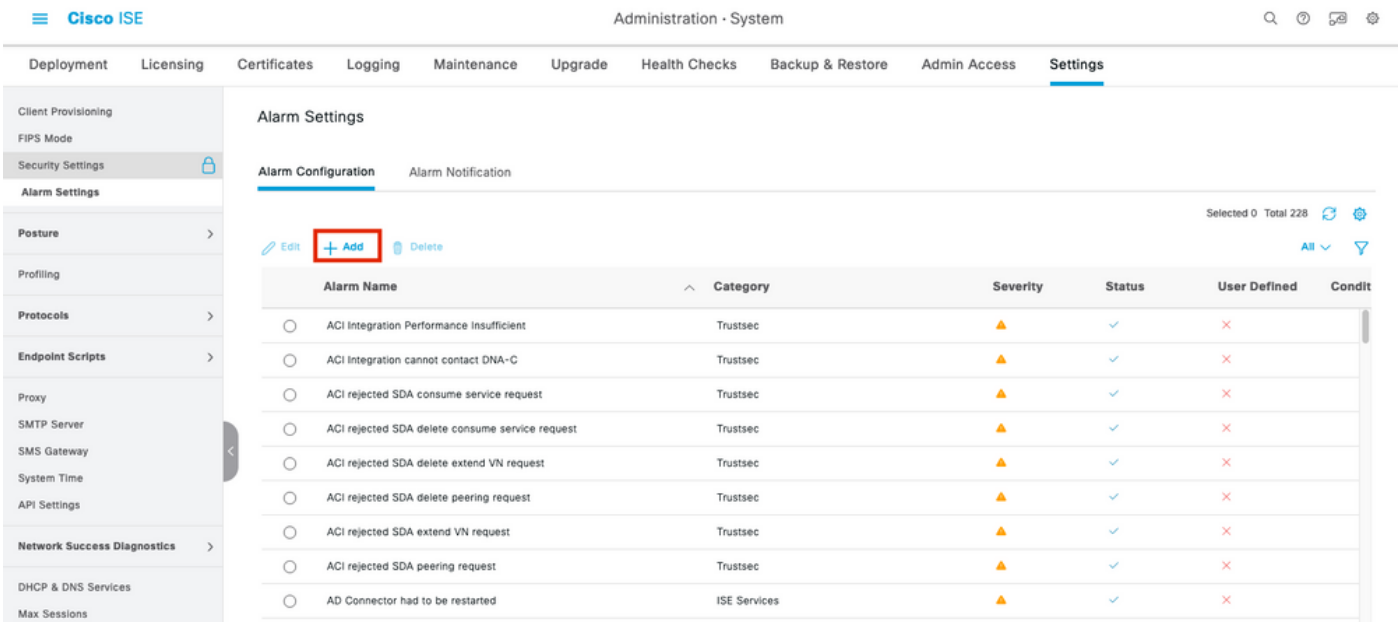
구성

이 예에서는 AD(Active Directory) 사용자가 로그인할 때 푸시되는 권한 부여 프로파일("ad_user")에 대한 경보를 생성하고, 구성된 임계값을 기준으로 경보가 트리거됩니다.

참고: 프로덕션 서버의 경우 경보가 크게 발생하지 않도록 하려면 임계값이 더 높아야 합니다.

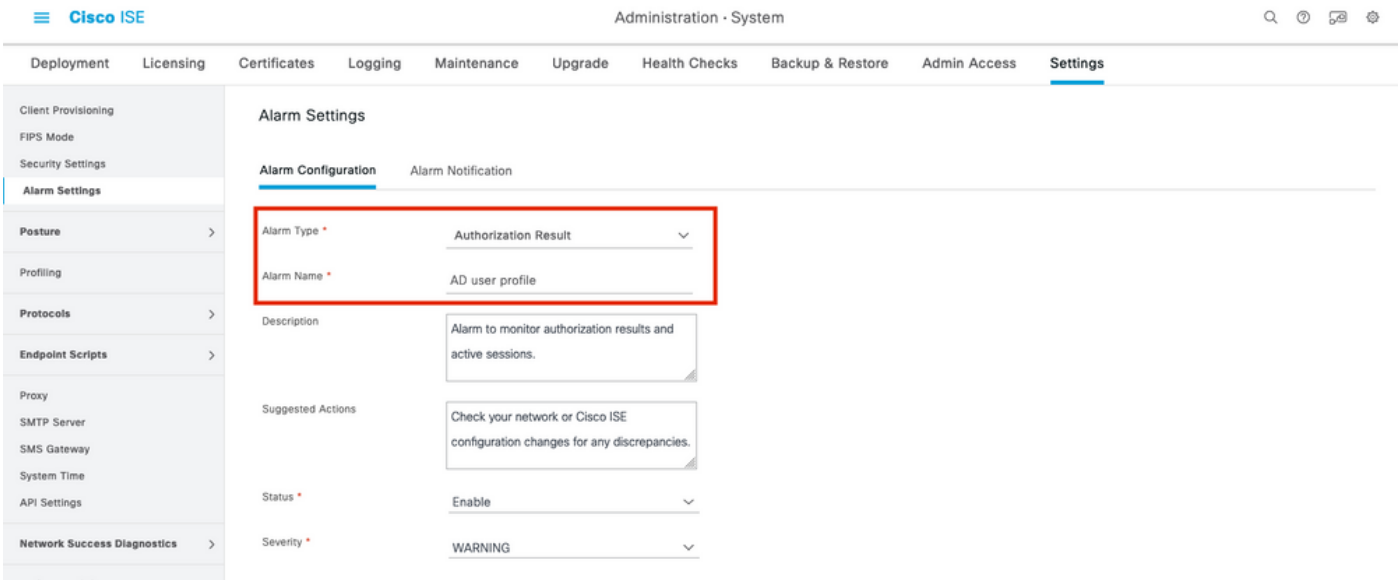
1단계. Administration(관리) **> System(시스템) > Alarm Settings(경보 설정)로 이동합니다**.

2단계. Alarm Configuration(경보 컨피그레이션)에서 **Add(추가)**를 클릭하여 이미지에 표시된 대로 경보를 생성합니다.



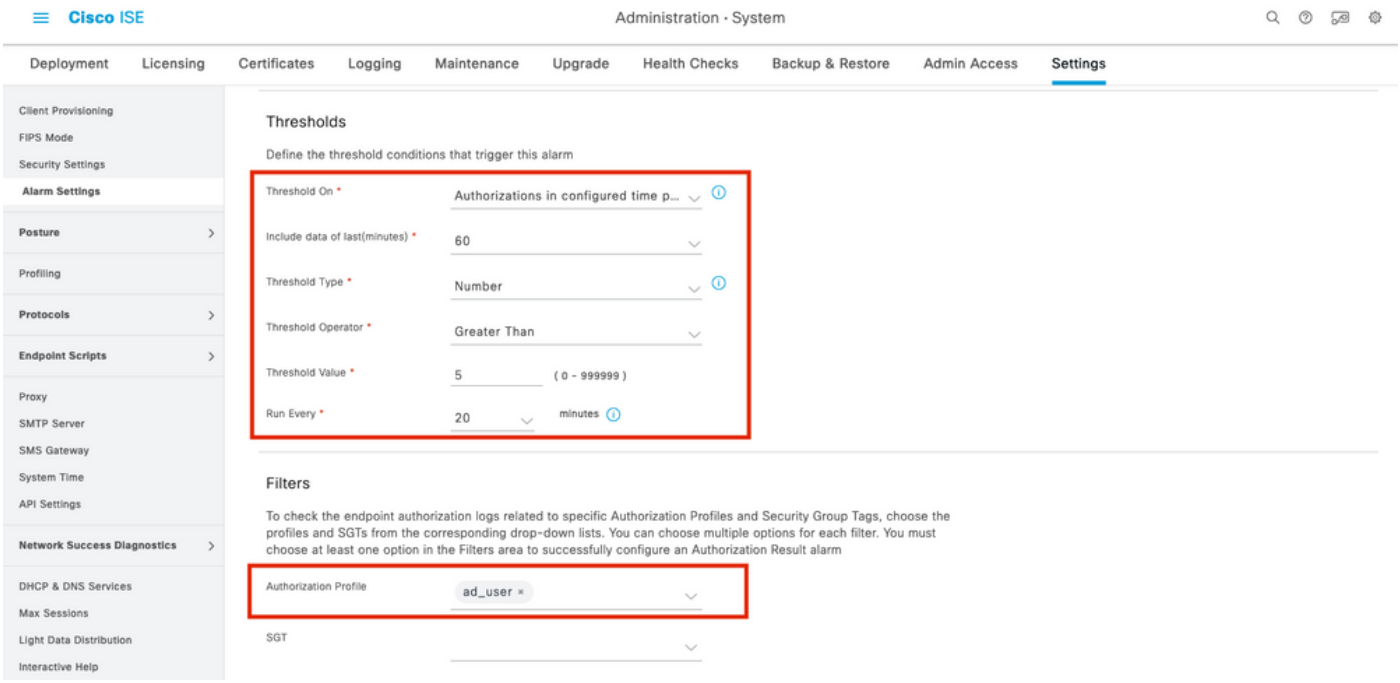
권한 부여 결과에 따른 ISE 3.1 경보 - 경보 설정

3단계. Alarm Type as Authorization **Result(권한 부여 결과**로 경보 유형)를 선택하고 이미지에 표시된 대로 경보 이름을 입력합니다.



권한 부여 결과에 따른 ISE 3.1 경보 - 경보 구성

4단계. Threshold(**임계값**) 섹션의 Threshold On(임계값 시간) 드롭다운**에서 Authorization in configured time period in configured time period(구성된 기간**의 권한 부여)를 선택하고 Threshold(임계값)와 필수 필드에 적절한 값을 입력합니다. 필터 섹션에서 이미지에 표시된 대로 경보를 트리거해야 하는 권한 부여 프로파일을 호출합니다.



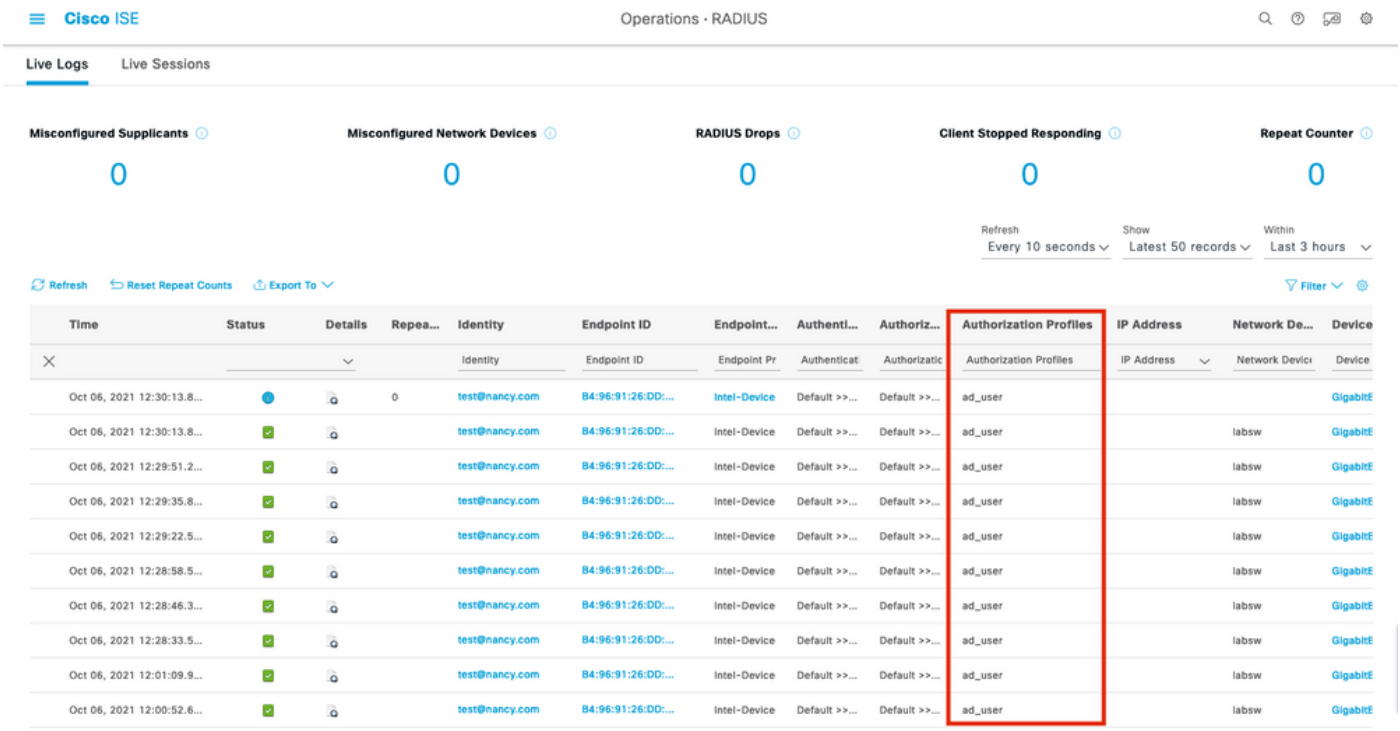
권한 부여 결과를 기반으로 하는 ISE 3.1 경보 - 경보 임계값 구성

참고: 경보에 사용되는 권한 부여 프로파일이 Policy(정책) **> Policy Elements(정책 요소) > Results(결과) > Authorization(권한 부여) > Authorization Profiles(권한 부여 프로파일)에 정의되어 있는지 확인합니다**.

다음을 확인합니다.

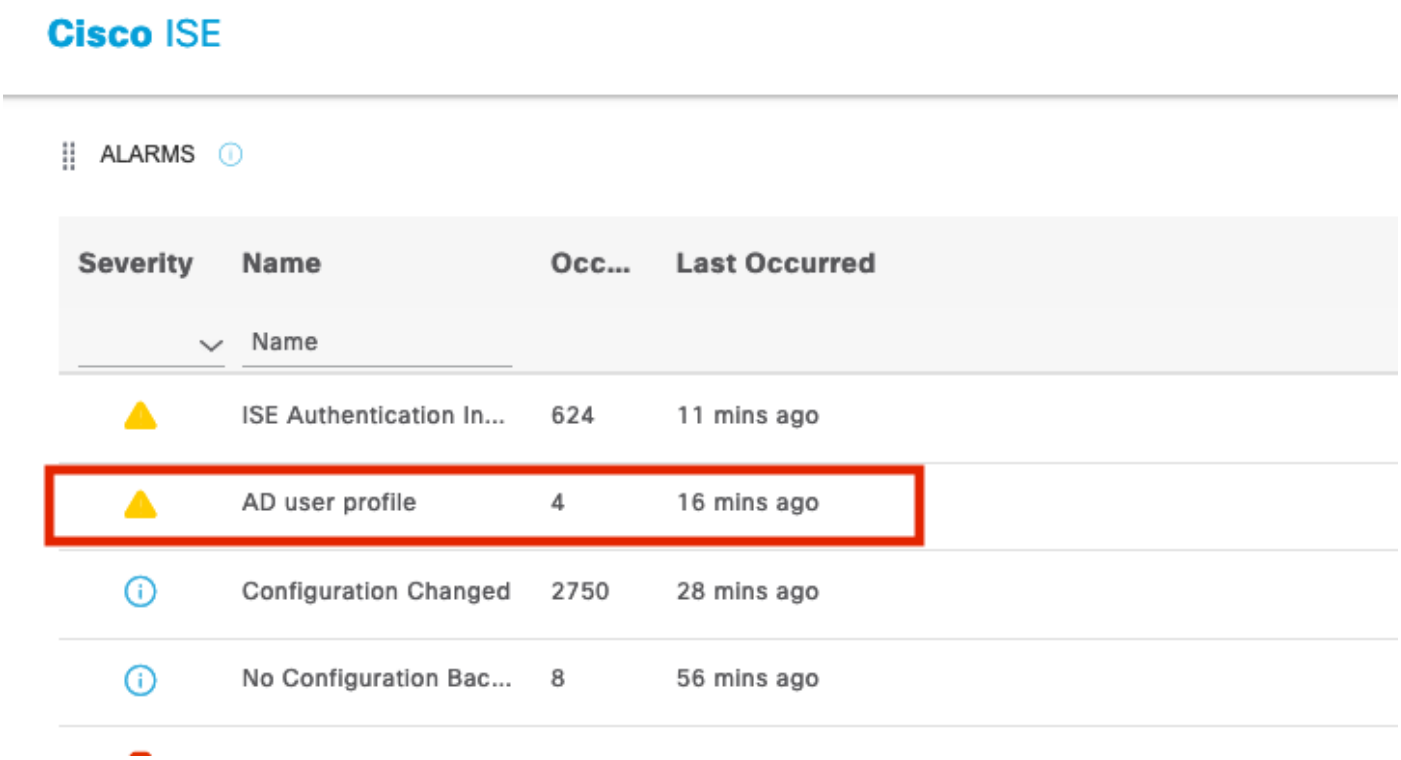
이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

ISE가 RADIUS 인증 요청에 대해 경보에 호출된 권한 부여 프로파일을 푸시하고 폴링 간격 내에 임계값 조건을 충족하면 이미지에 표시된 대로 ISE 대시보드에 경보가 트리거됩니다. alarm ad_user 프로필에 대한 트리거는 지난 20분(폴링 간격) 동안 프로파일이 5회 이상(임계값) 푸시된다는 것입니다.



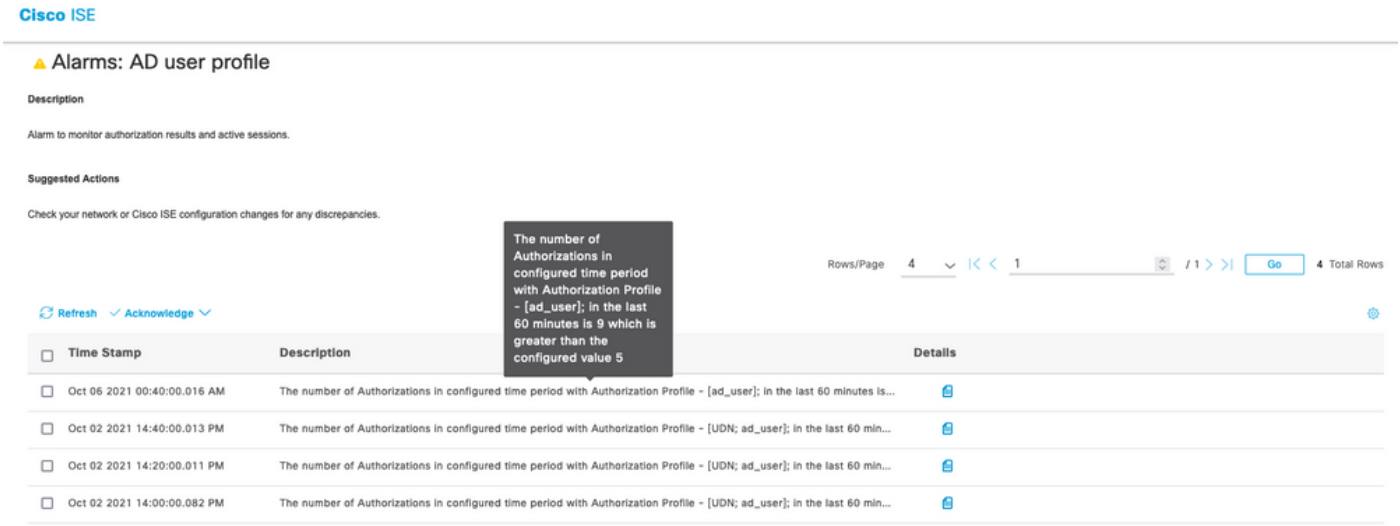
권한 부여 결과를 기반으로 하는 ISE 3.1 경보 - ISE 라이브 로그

1단계. 경보를 확인하려면 ISE Dashboard(ISE 대시보드)로 이동하고 ALARMS 창을 클릭합니다. 다음과 같이 새 웹 페이지가 열립니다.



권한 부여 결과를 기반으로 하는 ISE 3.1 경보 - 경보 알림

2단계. 경보에 대한 자세한 내용을 보려면 경보를 선택하면 경보의 트리거 및 타임스탬프에 대한 자세한 정보가 표시됩니다.

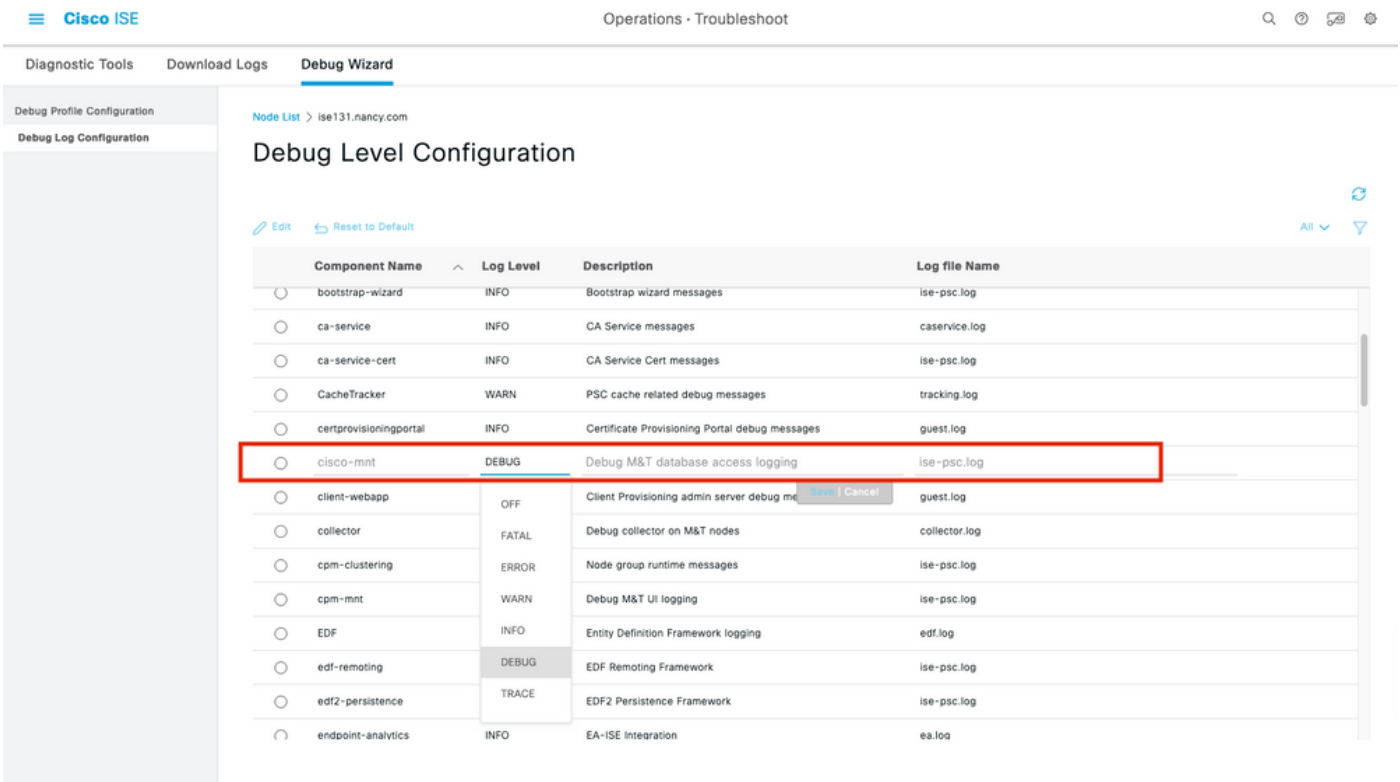


권한 부여 결과에 따른 ISE 3.1 경보 - 경보 세부 정보

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

경보 관련 문제를 해결하려면 MnT 노드에서 경보 평가가 수행되므로 모니터링 노드(MnT)의 cisco-mnt 구성 요소를 활성화해야 합니다. Operations(작업) **> Troubleshoot(문제 해결) > Debug Wizard(디버그 마법사) > Debug Log Configuration(디버그 로그 컨피그레이션)으로 이동합니다**. 다음과 같이 모니터링 서비스가 실행 중인 노드를 선택하고 구성 요소 이름 cisco-mnt에 대한 로그 레벨을 디버그로 변경합니다.



권한 부여 결과를 기반으로 하는 ISE 3.1 경보 - ISE 디버그 컨피그레이션

경보가 트리거될 때 코드 조각을 기록합니다.

```
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={67,104,101,99,107,37,50,48,121,111,117,114,37,50,48,110,101,116,119,111,114,107,37,50,48,111,114,37,50,48,67,105,115,99,111,37,50,48,73,83,69,37,50,48,99,111,110,102,105,103,117,114,97,116,105,111,110,37,50,48,99,104,97,110,103,101,115,37,50,48,102,111,114,37,50,48,97,11

0,121,37,50,48,100,105,115,99,114,101,112,97,110,99,105,101,115,46},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] : 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

참고: 권한 부여 프로파일이 푸시된 후에도 경보가 트리거되지 않으면 다음과 같은 조건을 확인합니다. 경보에 구성된 마지막(분), 임계값 연산자, 임계값 및 폴링 간격의 데이터를 포함합니다.