

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。

The screenshot shows the Cisco ISE Administration - System interface. On the left, there's a sidebar with various settings like Client Provisioning, Security Settings, and Alarm Settings. The main area is titled 'Alarm Settings' and has two tabs: 'Alarm Configuration' (selected) and 'Alarm Notification'. Below these tabs is a toolbar with 'Edit', '+ Add' (highlighted with a red box), and 'Delete' buttons. A table lists several alarms, each with columns for 'Alarm Name', 'Category', 'Severity', 'Status', 'User Defined', and 'Condit'. The first few rows show ACI-related errors.

| Alarm Name | Category | Severity | Status | User Defined | Condit |
|---|--------------|----------|--------|--------------|--------|
| ACI Integration Performance Insufficient | Trustsec | ⚠️ | ✓ | ✗ | |
| ACI Integration cannot contact DNA-C | Trustsec | ⚠️ | ✓ | ✗ | |
| ACI rejected SDA consume service request | Trustsec | ⚠️ | ✓ | ✗ | |
| ACI rejected SDA delete consume service request | Trustsec | ⚠️ | ✓ | ✗ | |
| ACI rejected SDA delete extend VN request | Trustsec | ⚠️ | ✓ | ✗ | |
| ACI rejected SDA delete peering request | Trustsec | ⚠️ | ✓ | ✗ | |
| ACI rejected SDA extend VN request | Trustsec | ⚠️ | ✓ | ✗ | |
| ACI rejected SDA peering request | Trustsec | ⚠️ | ✓ | ✗ | |
| AD Connector had to be restarted | ISE Services | ⚠️ | ✓ | ✗ | |

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。

The screenshot shows the Cisco ISE Administration - System interface. The 'Alarm Configuration' tab is selected. A red box highlights the 'Alarm Type *' dropdown set to 'Authorization Result' and the 'Alarm Name *' input field containing 'AD user profile'. Below these fields are 'Description' and 'Suggested Actions' sections, both containing placeholder text. Further down are 'Status *' (set to 'Enable') and 'Severity *' (set to 'WARNING').

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。

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access **Settings**

Client Provisioning

FIPS Mode

Security Settings

Alarm Settings

Posture >

Profiling

Protocols >

Endpoint Scripts >

Proxy

SMTP Server

SMS Gateway

System Time

API Settings

Network Success Diagnostics >

DHCP & DNS Services

Max Sessions

Light Data Distribution

Interactive Help

Thresholds

Define the threshold conditions that trigger this alarm

Threshold On * Authorizations in configured time p... ⓘ

Include data of last(minutes) * 60

Threshold Type * Number ⓘ

Threshold Operator * Greater Than ⓘ

Threshold Value * 5 (0 - 999999)

Run Every * 20 minutes ⓘ

Filters

To check the endpoint authorization logs related to specific Authorization Profiles and Security Group Tags, choose the profiles and SGTs from the corresponding drop-down lists. You can choose multiple options for each filter. You must choose at least one option in the Filters area to successfully configure an Authorization Result alarm

Authorization Profile ad_user ⓘ

SGT

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）。

Cisco ISE Operations · RADIUS

Live Logs Live Sessions

Misconfigured Suplicants ⓘ Misconfigured Network Devices ⓘ RADIUS Drops ⓘ Client Stopped Responding ⓘ Repeat Counter ⓘ

| Time | Status | Details | Repea... ts | Identity | Endpoint ID | Endpoint Pr | Authenticat | Authoriz... | Authorization Profiles | IP Address | Network De... | Device |
|----------------------------|--------|---------|----------------|----------------|--------------------|--------------|---------------|---------------|------------------------|------------|---------------|----------|
| Oct 06, 2021 12:30:13.8... | | | 0 | test@nancy.com | B4:96:91:26:DD:... | Intel-Device | Default >>... | Default >>... | ad_user | IP Address | Network Devic | GigabitE |
| Oct 06, 2021 12:30:13.8... | | | 0 | test@nancy.com | B4:96:91:26:DD:... | Intel-Device | Default >>... | Default >>... | ad_user | IP Address | Network Devic | GigabitE |
| Oct 06, 2021 12:29:51.2... | | | 0 | test@nancy.com | B4:96:91:26:DD:... | Intel-Device | Default >>... | Default >>... | ad_user | IP Address | Network Devic | GigabitE |
| Oct 06, 2021 12:29:35.8... | | | 0 | test@nancy.com | B4:96:91:26:DD:... | Intel-Device | Default >>... | Default >>... | ad_user | IP Address | Network Devic | GigabitE |
| Oct 06, 2021 12:29:22.5... | | | 0 | test@nancy.com | B4:96:91:26:DD:... | Intel-Device | Default >>... | Default >>... | ad_user | IP Address | Network Devic | GigabitE |
| Oct 06, 2021 12:28:58.5... | | | 0 | test@nancy.com | B4:96:91:26:DD:... | Intel-Device | Default >>... | Default >>... | ad_user | IP Address | Network Devic | GigabitE |
| Oct 06, 2021 12:28:46.3... | | | 0 | test@nancy.com | B4:96:91:26:DD:... | Intel-Device | Default >>... | Default >>... | ad_user | IP Address | Network Devic | GigabitE |
| Oct 06, 2021 12:28:33.5... | | | 0 | test@nancy.com | B4:96:91:26:DD:... | Intel-Device | Default >>... | Default >>... | ad_user | IP Address | Network Devic | GigabitE |
| Oct 06, 2021 12:01:09.9... | | | 0 | test@nancy.com | B4:96:91:26:DD:... | Intel-Device | Default >>... | Default >>... | ad_user | IP Address | Network Devic | GigabitE |
| Oct 06, 2021 12:00:52.6... | | | 0 | test@nancy.com | B4:96:91:26:DD:... | Intel-Device | Default >>... | Default >>... | ad_user | IP Address | Network Devic | GigabitE |

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：

Cisco ISE

ALARMS

| Severity | Name | Occ... | Last Occurred |
|----------|--------------------------|--------|---------------|
| ⚠ | ISE Authentication In... | 624 | 11 mins ago |
| ⚠ | AD user profile | 4 | 16 mins ago |
| ⓘ | Configuration Changed | 2750 | 28 mins ago |
| ⓘ | No Configuration Bac... | 8 | 56 mins ago |

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。

Cisco ISE

⚠ Alarms: AD user profile

Description

Alarm to monitor authorization results and active sessions.

Suggested Actions

Check your network or Cisco ISE configuration changes for any discrepancies.

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

| Time Stamp | Description | Details |
|-----------------------------|---|----------------------|
| Oct 06 2021 00:40:00.016 AM | The number of Authorizations in configured time period with Authorization Profile - [ad_user]; in the last 60 minutes is... | View |
| Oct 02 2021 14:40:00.013 PM | The number of Authorizations in configured time period with Authorization Profile - [UDN; ad_user]; in the last 60 min... | View |
| Oct 02 2021 14:20:00.011 PM | The number of Authorizations in configured time period with Authorization Profile - [UDN; ad_user]; in the last 60 min... | View |
| Oct 02 2021 14:00:00.082 PM | The number of Authorizations in configured time period with Authorization Profile - [UDN; ad_user]; in the last 60 min... | View |

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：

Diagnostic Tools Download Logs **Debug Wizard**

Debug Profile Configuration Node List > ise131.nancy.com Debug Log Configuration

Debug Level Configuration

| | | Component Name | Log Level | Description | Log file Name |
|-----------------------|--|------------------------|-----------|--|---------------|
| <input type="radio"/> | | bootstrap-wizard | INFO | Bootstrap wizard messages | ise-psc.log |
| <input type="radio"/> | | ca-service | INFO | CA Service messages | caservice.log |
| <input type="radio"/> | | ca-service-cert | INFO | CA Service Cert messages | ise-psc.log |
| <input type="radio"/> | | CacheTracker | WARN | PSC cache related debug messages | tracking.log |
| <input type="radio"/> | | certprovisioningportal | INFO | Certificate Provisioning Portal debug messages | guest.log |
| <input type="radio"/> | | cisco-mnt | DEBUG | Debug M&T database access logging | ise-psc.log |
| <input type="radio"/> | | client-webapp | OFF | Client Provisioning admin server debug message | guest.log |
| <input type="radio"/> | | collector | FATAL | Debug collector on M&T nodes | collector.log |
| <input type="radio"/> | | cpm-clustering | ERROR | Node group runtime messages | ise-psc.log |
| <input type="radio"/> | | cpm-mnt | WARN | Debug M&T UI logging | ise-psc.log |
| <input type="radio"/> | | EDF | INFO | Entity Definition Framework logging | edf.log |
| <input type="radio"/> | | edf-remoting | DEBUG | EDF Remoting Framework | ise-psc.log |
| <input type="radio"/> | | edf2-persistence | TRACE | EDF2 Persistence Framework | ise-psc.log |
| <input type="radio"/> | | endpoint-analytics | INFO | EA-ISE Integration | ea.log |

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={65,108,97,114,109,32,116,111,32,109,111,110,105,116,111,114,32,97,117,116,104,111,114,105,122,97,116,105,111,110,32,114,101,115,117,108,116,115,32,97,110,100,32,97,99,116,105,118,101,32,115,101,115,115,105,111,110,115,46}, 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=[ ], customEmailExt={}, 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, filterConditionValue=]
```

```

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_re
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。