

根據ISE 3.1上的授權結果配置警報

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[驗證](#)

[疑難排解](#)

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。

The screenshot shows the Cisco ISE Administration interface for Alarm Settings. The left sidebar contains navigation options like Client Provisioning, Security Settings, and Alarm Settings. The main content area shows the Alarm Configuration tab with a table of existing alarms. A red box highlights the '+ Add' button at the top of the table.

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。

The screenshot shows the configuration form for a new alarm. The 'Alarm Type' is set to 'Authorization Result' and the 'Alarm Name' is 'AD user profile'. A red box highlights these two fields.

Alarm Type: Authorization Result
Alarm Name: 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.
Status: Enable
Severity: WARNING

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。

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）。

Operations · RADIUS

Live Logs Live Sessions

Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 0 Client Stopped Responding 0 Repeat Counter 0

Refresh Every 10 seconds Show Latest 50 records Within Last 3 hours

Refresh Reset Repeat Counts Export To Filter

Time	Status	Details	Repe...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authorization Profiles	IP Address	Network De...	Device
Oct 06, 2021 12:30:13.8...	●	<input type="button" value="ⓘ"/>	0	test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user			GigabitE
Oct 06, 2021 12:30:13.8...	✓	<input type="button" value="ⓘ"/>		test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:29:51.2...	✓	<input type="button" value="ⓘ"/>		test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:29:35.8...	✓	<input type="button" value="ⓘ"/>		test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:29:22.5...	✓	<input type="button" value="ⓘ"/>		test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:28:58.5...	✓	<input type="button" value="ⓘ"/>		test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:28:46.3...	✓	<input type="button" value="ⓘ"/>		test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:28:33.5...	✓	<input type="button" value="ⓘ"/>		test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:01:09.9...	✓	<input type="button" value="ⓘ"/>		test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:00:52.6...	✓	<input type="button" value="ⓘ"/>		test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE

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：

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。

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.

Refresh Acknowledge

Rows/Page 4 | 1 | Go 4 Total Rows

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...	
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...	
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...	
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...	

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

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：

Node List > ise131.nancy.com

Debug Level Configuration

[Edit](#) [Reset to Default](#) All

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 me	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={65,108,97,114,109,32,116,111,32,109,111,110,105,116,111,114,32,97,117,116,104,111,114,105,122,97,116,105,111,110,32,114,101,115,117,108,116,115,32,97,110,100,32,97,99,116,105,118,101,32,115,101,115,115,105,111,110,115,46},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,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。