

ISE 3.1の許可結果に基づくアラームの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

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、アラームが大きくなり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。

The screenshot shows the Cisco ISE Administration console. The left sidebar contains navigation options like Client Provisioning, Security Settings, Posture, etc. The main area is titled 'Alarm Settings' and has two tabs: 'Alarm Configuration' (selected) and 'Alarm Notification'. Below the tabs, there are 'Edit', '+ Add', and 'Delete' buttons. The '+ Add' button is highlighted with a red box. Below the buttons is a table of existing alarms.

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	▲	✓	×	

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。

The screenshot shows the 'Add Alarm' form in the Cisco ISE Administration console. The 'Alarm Type' dropdown menu is set to 'Authorization Result'. The 'Alarm Name' field contains the text 'AD user profile'. The 'Description' field contains the text 'Alarm to monitor authorization results and active sessions.' The 'Suggested Actions' field contains the text 'Check your network or Cisco ISE configuration changes for any discrepancies.' The 'Status' dropdown is set to 'Enable' and the 'Severity' dropdown is set to 'WARNING'.

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。

Cisco ISE Administration - System

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

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。

Cisco ISE 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	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authorization Profiles	IP Address	Network De...	Device
				Identity	Endpoint ID	Endpoint Pr	Authenticat	Authorizati	Authorization Profiles	IP Address	Network Devi	Device
Oct 06, 2021 12:30:13.8...	●	🔍	0	test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user			GigabitE
Oct 06, 2021 12:30:13.8...	✓	🔍		test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:29:51.2...	✓	🔍		test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:29:35.8...	✓	🔍		test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:29:22.5...	✓	🔍		test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:28:58.5...	✓	🔍		test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:28:46.3...	✓	🔍		test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:28:33.5...	✓	🔍		test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:01:09.9...	✓	🔍		test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:00:52.6...	✓	🔍		test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE

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。

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

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。

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

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

Rows/Page 4 / 1 >> Go 4 Total Rows

許可結果に基づくISE 3.1アラーム : アラームの詳細

トラブルシューティング

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。

The screenshot shows the Cisco ISE interface for Debug Wizard. The 'Debug Log Configuration' section is active, displaying a table of components and their log levels. The 'cisco-mnt' component is highlighted with a red box, and its log level is set to 'DEBUG'. Other components include bootstrap-wizard, ca-service, ca-service-cert, CacheTracker, certprovisioningportal, client-webapp, collector, cpm-clustering, cpm-mnt, EDF, edf-remoting, edf2-persistence, and endpoint-analytics.

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

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。