

Configurazione degli allarmi in base ai risultati dell'autorizzazione su ISE 3.1

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare gli allarmi in base al risultato dell'autorizzazione per una richiesta di autenticazione RADIUS su Identity Services Engine (ISE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- protocollo RADIUS
- Accesso come amministratore ISE

Componenti usati

Il riferimento delle informazioni contenute in questo documento è Identity Services Engine (ISE) 3.1.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

In questo esempio, un allarme personalizzato viene configurato per un profilo di autorizzazione specifico con un limite di soglia definito e, se ISE raggiunge il limite di soglia nella policy di autorizzazione configurata, l'allarme viene attivato.

Configurazione

In questo esempio verrà creato un avviso per il profilo di autorizzazione ("ad_user") inviato quando un utente di Active Directory (AD) esegue l'accesso e l'avviso verrà attivato in base alla soglia configurata.

Nota: Per un server di produzione, la soglia deve essere un valore superiore per evitare il verificarsi di un allarme di grandi dimensioni.

Passaggio 1. Passare a **Amministrazione > Sistema > Impostazioni allarme**.

Passaggio 2. In Configurazione allarme, fare clic su **Add** (Aggiungi) per creare un allarme come mostrato nell'immagine.

The screenshot shows the Cisco ISE Administration interface. The left sidebar contains navigation options 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'. A '+ Add' button is highlighted with a red box. Below it 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	▲	✓	✗	

Allarmi ISE 3.1 basati sui risultati dell'autorizzazione - Impostazioni allarme

Passaggio 3. Selezionare il tipo di allarme **Risultato autorizzazione** e immettere il nome dell'allarme come mostrato nell'immagine.

The screenshot shows the 'Add Alarm' configuration form in the Cisco ISE Administration interface. The 'Alarm Type' dropdown is set to 'Authorization Result' and the 'Alarm Name' field contains 'AD user profile'. Both are highlighted with a red box. Other fields include Description, Suggested Actions, Status (set to 'Enable'), and Severity (set to 'WARNING').

Allarmi ISE 3.1 basati sui risultati dell'autorizzazione - Configurazione dell'allarme

Passo 4: nella sezione **Soglia**, selezionare **Autorizzazione nel periodo di tempo configurato** nell'elenco a discesa Soglia il e inserire i valori appropriati per Soglia e i campi obbligatori. Nella sezione filtro, chiamare il Profilo di autorizzazione per il quale deve essere attivato l'allarme, come mostrato nell'immagine.

The screenshot displays the Cisco ISE Administration console interface. The top navigation bar includes 'Cisco ISE' and 'Administration - System'. The main menu on the left lists various settings categories, with 'Alarm Settings' selected. The 'Thresholds' configuration page is shown, with a red box highlighting the 'Thresholds' section. This section includes the following fields:

- 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

Below the 'Thresholds' section is the 'Filters' section, which includes a red box around the 'Authorization Profile' dropdown menu, currently set to 'ad_user'.

Allarmi ISE 3.1 basati sui risultati dell'autorizzazione - Configurazione della soglia di allarme

Nota: Verificare che il profilo di autorizzazione utilizzato per l'allarme sia definito in **Criteri > Elementi della policy > Risultati > Autorizzazione > Profili di autorizzazione**.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Quando ISE attiva il profilo di autorizzazione chiamato nell'allarme per la richiesta di autenticazione RADIUS e soddisfa la condizione di soglia entro l'intervallo di polling, viene attivato l'allarme visualizzato nel dashboard ISE, come mostrato nell'immagine. L'innesco dell'allarme `ad_user_profile` è che il profilo è stato premuto più di 5 volte (valore soglia) negli ultimi 20 minuti (intervallo di polling).

Live Logs Live Sessions

Misconfigured Suppliants 0

Misconfigured Network Devices 0

RADIUS Drops 0

Client Stopped Responding 0

Repeat Counter 0

0

0

0

0

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
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

Allarmi ISE 3.1 basati sui risultati dell'autorizzazione - Live Log ISE

Passaggio 1. Per controllare l'allarme, passare a ISE Dashboard e fare clic sulla finestra **ALARMS**. Verrà aperta una nuova pagina Web come illustrato di seguito:

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

Allarmi ISE 3.1 basati sui risultati dell'autorizzazione - Notifica di allarme

Passaggio 2. Per ottenere ulteriori dettagli sull'allarme, selezionare l'allarme e fornire ulteriori dettagli sull'innescò e l'indicatore orario dell'allarme.

▲ 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

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

<input type="checkbox"/>	Time Stamp	Description	Details
<input type="checkbox"/>	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...	Details
<input type="checkbox"/>	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...	Details
<input type="checkbox"/>	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...	Details
<input type="checkbox"/>	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...	Details

Allarmi ISE 3.1 basati sui risultati dell'autorizzazione - Dettagli allarme

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Per risolvere i problemi relativi agli allarmi, è necessario abilitare il componente cisco-mnt sul nodo di monitoraggio (MnT) quando la valutazione dell'allarme avviene sul nodo MnT. Passare a **Operazioni > Risoluzione dei problemi > Debug guidato > Configurazione log di debug**. Selezionare il nodo su cui sono in esecuzione i servizi di monitoraggio e modificare il livello di log in Debug per nome componente cisco-mnt, come mostrato:

Cisco ISE Operations · Troubleshoot

Diagnostic Tools Download Logs **Debug Wizard**

Debug Profile Configuration
Debug Log Configuration

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

Allarmi ISE 3.1 basati sui risultati dell'autorizzazione - Configurazione debug ISE

Registra frammenti quando l'allarme viene attivato.

```
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={67,104,101,99,107,37,50,48,121,111,117,114,37,50,48,110,101,116,119,111,114,107,37,50,48,111,114,37,50,48,67,105,115,99,111,37,50,48,73,83,69,37,50,48,99,111,110,102,105,103,117,114,97,116,105,111,110,37,50,48,99,104,97,110,103,101,115,37,50,48,102,111,114,37,50,48,97,110,121,37,50,48,100,105,115,99,114,101,112,97,110,99,105,101,115,46},detailsLink=#pageId=page_reports_details&pullOutId=authorizationResultAlarmDetails&definition=/Diagnostics/Authorization-Result-Alarm-Details.xml,
```

17,114,97,116,105,111,110,37,50,48,99,104,97,110,103,101,115,37,50,48,102,111,114,37,50,48,97,110,121,37,50,48,100,105,115,99,114,101,112,97,110,99,105,101,115,46},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] : 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

NOTA: Se l'allarme non viene attivato anche dopo che è stato premuto il profilo di autorizzazione, verificare le seguenti condizioni: Includere i dati degli ultimi (minuti), Operatore soglia, Valore soglia e intervallo di polling configurati nell'allarme.