

Notifiche di allarme via e-mail ISE non funzionanti dopo l'aggiornamento del software

Sommario

Problema

Le notifiche di allarme e-mail di Cisco Identity Services Engine (ISE) non vengono recapitate ai destinatari configurati. La funzione di test SMTP all'interno di ISE ha esito positivo, ma gli eventi di allarme effettivi non attivano l'invio di notifiche e-mail. Questo problema ha iniziato a verificarsi dopo l'aggiornamento da ISE versione 3.2 a 3.4 Patch 3 e persiste anche dopo l'applicazione della patch 3.4 Patch 5. Le e-mail di allarme hanno funzionato brevemente subito dopo l'applicazione della patch 5, ma hanno smesso di funzionare di nuovo quando le notifiche e-mail sono state riattivate dopo essere state temporaneamente disabilitate a causa di un volume elevato.

Ambiente

- Patch 5 di Cisco Identity Services Engine (ISE) versione 3.4
- Implementazione ISE con 6 PSN (Policy Service Nodes), 2 nodi di monitoraggio e risoluzione dei problemi (MnT) e 2 PAN (Policy Administration Nodes)
- Nodo MnT primario: COR089ISE-MnT02 (IP: 172.29.134.2)
- Server SMTP: smtp1.us.parker.corp
- Configurazione di lavoro precedente su ISE versione 3.2
- Problema iniziato dopo l'aggiornamento dalla versione 3.2 alla 3.4 Patch 3 in ottobre

Risoluzione

Per risolvere i problemi relativi alle notifiche degli allarmi via e-mail, seguire le procedure di

diagnostica e risoluzione descritte nelle sezioni seguenti.

Passaggio 1: Verifica della configurazione SMTP e della funzionalità di test

Confermare che il test SMTP all'interno di ISE sia riuscito e verificare la configurazione del server e-mail:

1. Selezionare Amministrazione > Sistema > Impostazioni > Server SMTP nell'interfaccia utente di ISE.
2. Verificare tutte le impostazioni SMTP, inclusi l'indirizzo del server, la porta, la configurazione TLS/STARTTLS e le impostazioni di autenticazione.
 - Verificare che l'indirizzo IP o il nome di dominio completo (FQDN) del server SMTP (gateway di posta) sia corretto.
 - Controllare la porta SMTP: Il valore predefinito è la porta 25. Se è abilitata la trasmissione protetta (TLS/STARTTLS), deve corrispondere esplicitamente alla porta aperta sul server e-mail (ad esempio, la porta 587).
3. Verificare la connessione SMTP utilizzando la funzione di test incorporata.
4. Coordinarsi con gli amministratori del server e-mail per verificare se i messaggi di prova vengono ricevuti a livello del server.

Passaggio 2: Abilita registrazione debug sul nodo MnT primario

Utilizzare l'accesso root per stabilire se il problema è dovuto a un trigger interno riuscito o a un errore di connessione esterno con il server:

```
tail -F /opt/CSC0cpm/logs/ise-psc.log
2026-06-02 14:51:54,851 WARN [MnT-AlarmWorkerMail-Threadpool-0][[]] cisco.mnt.common.alarms.AlarmWorke
2026-06-02 14:51:54,851 INFO [MnT-AlarmWorkerMail-Threadpool-0][[]] cisco.mnt.common.alarms.AlarmWorke
2026-06-02 14:51:54,853 ERROR [MnT-AlarmWorkerMail-Threadpool-0][[]] cisco.mnt.common.alarms.AlarmWorke
```

Se è necessaria un'ulteriore risoluzione dei problemi o non si è in grado di eseguire il monitoraggio

tramite root, abilitare la registrazione dettagliata per acquisire la generazione di allarmi e i tentativi di recapito tramite e-mail.

Abilitare questi componenti di debug nel nodo MnT primario:

```
cisco-mnt  
cpm-mnt
```

Passaggio 3: Acquisire il traffico di rete durante gli eventi di allarme

Eseguire packet capture per verificare se ISE tenta di stabilire connessioni SMTP per eventi di allarme:

1. Passare a Operazioni > Risoluzione dei problemi > Strumenti diagnostici > Dump TCP sul nodo MnT principale.
2. Selezionare l'interfaccia di rete utilizzata per comunicare con il server SMTP.
3. Avviare l'acquisizione dei pacchetti.
4. Durante l'acquisizione, eseguire entrambe le operazioni:
 - Eseguire il test SMTP da ISE (per acquisire la sessione SMTP funzionante).
 - Generare o attendere che si verifichi un evento di allarme effettivo.
5. Interrompere l'acquisizione e scaricare il file PCAP per l'analisi.

Passaggio 4: Monitoraggio dei log delle applicazioni durante la generazione di allarmi

Monitorare i log delle applicazioni ISE per identificare i tentativi di invio di e-mail.

Eseguire questo comando sulla CLI del nodo MnT primario durante la generazione di un allarme:

```
show logging application ise-psc.log tail
```

Acquisire l'uscita e annotare l'indicatore orario di tutti gli eventi di allarme che devono attivare le notifiche e-mail.

Passaggio 5: Coordinamento con l'amministrazione del server e-mail

Collaborare con gli amministratori del server e-mail per verificare l'elaborazione lato server.

Durante il test degli allarmi, chiedere al team responsabile della posta elettronica di controllare i registri del server SMTP per:

- Connessioni SMTP dall'indirizzo IP del nodo MnT primario
- Stato di accettazione, rifiuto o rinvio del messaggio
- Codici di errore o motivi di rifiuto se i messaggi non vengono accettati

Passaggio 6: Analisi dei dati acquisiti e implementazione della risoluzione

Esaminare le acquisizioni dei pacchetti, i log e le informazioni sul lato server raccolti per determinare:

- Se ISE sta tentando di inviare e-mail di allarme (visibile nell'acquisizione dei pacchetti).
- Codici di risposta del server ed eventuali motivi di rifiuto.
- Differenze tra le sessioni di test SMTP riuscite e le sessioni attivate da allarmi.

In base all'analisi, implementare le correzioni appropriate, ad esempio:

- Regolazione della configurazione del server SMTP o dei criteri di protezione.
- Modifica delle impostazioni delle notifiche e-mail ISE.
- Aggiornamento dell'indirizzo del mittente o dei parametri di autenticazione.

Passaggio 7: Disabilita registrazione debug

Dopo aver completato la risoluzione dei problemi, disabilitare i componenti per la registrazione del debug per impedire l'aumento del file di log.

Disabilitare i componenti di debug nel nodo MnT primario:

```
cisco-mnt (disable)
cpm-mnt (disable)
```

Causa

Il problema può derivare da differenze nel modo in cui il nodo MnT (Primary Monitoring & Troubleshooting) gestisce le sessioni SMTP per gli eventi di allarme rispetto alle funzioni di test SMTP. Se il test SMTP ha esito positivo, i tentativi effettivi di e-mail con attivazione di allarme possono non riuscire a causa di incompatibilità di configurazione, filtro sul lato server o modifiche nel processo di invio dei messaggi e-mail introdotte nella nuova versione di ISE.

Contenuto correlato

- [Guida all'amministrazione di Cisco ISE 3.4 - Risoluzione dei problemi](#)
- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).