

Les notifications d'alarme par e-mail ISE ne fonctionnent pas après la mise à niveau logicielle

Table des matières

Problème

Les notifications d'alarme par e-mail de Cisco Identity Services Engine (ISE) ne sont pas envoyées aux destinataires configurés. La fonction de test SMTP dans ISE réussit, mais les événements d'alarme réels ne déclenchent pas l'envoi de notifications par e-mail. Ce problème a commencé après la mise à niveau de la version 3.2 d'ISE vers la version 3.4 du patch 3, et a persisté même après l'application du patch 5 de la version 3.4. Les e-mails d'alarme ont fonctionné brièvement immédiatement après l'application du patch 5, mais ont cessé de fonctionner à nouveau lorsque les notifications par e-mail ont été réactivées après avoir été temporairement désactivées en raison d'un volume élevé.

Environnement

- Cisco Identity Services Engine (ISE) version 3.4, correctif 5
- Déploiement ISE avec 6 noeuds de service de stratégie (PSN), 2 noeuds de surveillance et de dépannage (MnT) et 2 noeuds d'administration de stratégie (PAN)
- Noeud MnT principal : COR089ISE-MnT02 (IP : 172.29.134.2)
- Serveur SMTP : smtp1.us.parker.corp
- Configuration de travail précédente sur ISE version 3.2
- Problème commencé après la mise à niveau de la version 3.2 vers la version 3.4 du patch 3 en octobre

Résolution

Pour résoudre les problèmes de notification d'alarme par e-mail ISE, suivez les étapes de diagnostic et de résolution décrites dans les sections suivantes.

Étape 1: Vérification de la configuration SMTP et du fonctionnement des tests

Vérifiez que le test SMTP dans ISE a réussi et vérifiez la configuration du serveur de messagerie :

1. Accédez à Administration > System > Settings > SMTP Server dans l'interface utilisateur graphique ISE.
2. Vérifiez tous les paramètres SMTP, y compris l'adresse du serveur, le port, la configuration TLS/STARTTLS et les paramètres d'authentification.
 - Assurez-vous que l'adresse IP ou le nom de domaine complet du serveur SMTP (passerelle de messagerie) est correct.
 - Vérifiez le port SMTP : La valeur par défaut est le port 25. Si la transmission sécurisée (TLS/STARTTLS) est activée, elle doit correspondre explicitement au port ouvert sur le serveur de messagerie (tel que le port 587).
3. Testez la connexion SMTP à l'aide de la fonction de test intégrée.
4. Coordonnez-vous avec les administrateurs du serveur de messagerie pour confirmer si des e-mails de test sont reçus au niveau du serveur.

Étape 2: Activer la journalisation de débogage sur le noeud MnT principal

Utilisez l'accès racine pour déterminer si le problème provient d'un déclenchement interne réussi ou d'une erreur de connexion externe avec le serveur :

```
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
```

Si un dépannage supplémentaire est nécessaire ou si vous ne pouvez pas effectuer de

surveillance via la racine, activez la journalisation détaillée pour capturer la génération d'alarmes et les tentatives de remise d'e-mails.

Activez ces composants de débogage sur le noeud MnT principal :

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

Étape 3: Capturer le trafic réseau pendant les événements d'alarme

Effectuez une capture de paquets pour vérifier si ISE tente d'établir des connexions SMTP pour les événements d'alarme :

1. Accédez à Operations > Troubleshoot > Diagnostic Tools > TCP Dump sur le noeud MnT principal.
2. Sélectionnez l'interface réseau utilisée pour communiquer avec le serveur SMTP.
3. Démarrez la capture des paquets.
4. Lors de la capture, effectuez les deux opérations suivantes :
 - Exécutez le test SMTP à partir d'ISE (pour capturer une session SMTP dont le fonctionnement a été vérifié).
 - Générer ou attendre qu'un événement d'alarme se produise.
5. Arrêtez la capture et téléchargez le fichier PCAP pour analyse.

Étape 4: Surveiller les journaux des applications pendant la génération des alarmes

Surveillez les journaux d'application ISE pour identifier les tentatives d'envoi d'e-mails.

Exécutez cette commande sur l'interface de ligne de commande du noeud principal MnT pendant

la génération d'une alarme :

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

Capturez le résultat et notez l'horodatage des événements d'alarme qui doivent déclencher des notifications par e-mail.

Étape 5: Coordination avec l'administration du serveur de messagerie

Collaborer avec les administrateurs du serveur de messagerie pour vérifier le traitement côté serveur.

Pendant le test des alarmes, demandez à l'équipe de messagerie de vérifier les journaux du serveur SMTP pour :

- Connexions SMTP à partir de l'adresse IP du noeud MnT principal
- Statut d'acceptation, de rejet ou de report des messages
- Codes d'erreur ou motifs de rejet si les messages ne sont pas acceptés

Étape 6: Analyser les données capturées et implémenter la résolution

Passez en revue les captures de paquets, les journaux et les informations côté serveur collectées afin de déterminer :

- Indique si ISE tente d'envoyer des e-mails d'alarme (visibles dans la capture de paquets).
- Codes de réponse du serveur et motifs de rejet éventuels.
- Différences entre les sessions de test SMTP réussies et les sessions déclenchées par alarme.

Sur la base de l'analyse, implémentez les correctifs appropriés tels que :

- Réglage de la configuration du serveur SMTP ou des stratégies de sécurité.

- Modification des paramètres de notification par e-mail ISE.
- Mise à jour des paramètres d'adresse ou d'authentification.

Étape 7: Désactiver la consignation du débogage

Une fois le dépannage terminé, désactivez les composants de journalisation du débogage pour empêcher la croissance du fichier journal.

Désactivez les composants de débogage sur le noeud principal MnT :

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

Motif

Le problème peut provenir de différences dans la façon dont le noeud MnT (Primary Monitoring & Troubleshooting) gère les sessions SMTP pour les événements d'alarme par rapport aux fonctions de test SMTP. Bien que le test SMTP réussisse, les tentatives d'envoi d'e-mails déclenchées par une alarme peuvent échouer en raison d'incompatibilités de configuration, du filtrage côté serveur ou de modifications apportées au processus d'envoi d'e-mails introduit dans la nouvelle version d'ISE.

Autres informations utiles

- [Guide d'administration de Cisco ISE 3.4 - Dépannage](#)
- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.