

ISE-Mail-Warnmeldungen funktionieren nach Software-Upgrade nicht

Inhalt

Problem

E-Mail-Warnmeldungen der Cisco Identity Services Engine (ISE) werden nicht an konfigurierte Empfänger zugestellt. Die SMTP-Testfunktion in der ISE ist erfolgreich, aber tatsächliche Alarmereignisse lösen keine E-Mail-Benachrichtigungen aus, die gesendet werden sollen. Dieses Problem trat nach dem Upgrade von ISE Version 3.2 auf 3.4 Patch 3 auf und bestand auch nach dem Anwenden von 3.4 Patch 5 fort. Die Alarm-E-Mails funktionierten unmittelbar nach dem Anwenden von Patch 5 kurz, funktionierten aber wieder nicht, als die E-Mail-Benachrichtigungen nach der vorübergehenden Deaktivierung aufgrund eines hohen Volumens wieder aktiviert wurden.

Umwelt

- Cisco Identity Services Engine (ISE) Version 3.4 Patch 5
- ISE-Bereitstellung mit 6 Policy Service Nodes (PSNs), 2 Monitoring & Troubleshooting (MnT)-Knoten und 2 Policy Administration Nodes (PANs)
- Primärer MnT-Knoten: COR089ISE-MnT02 (IP: 172.29.134.2)
- SMTP-Server: smtp1.us.parker.corp
- Ältere Konfiguration auf der ISE Version 3.2
- Problem begann nach dem Upgrade von Version 3.2 auf 3.4 Patch 3 im Oktober

Auflösung

Um ISE-Warnmeldungsprobleme bei E-Mail-Warnmeldungen zu beheben, befolgen Sie die Diagnose- und Lösungsschritte, die in den nächsten Abschnitten beschrieben werden.

Schritt 1: Überprüfen der SMTP-Konfiguration und der SMTP-Testfunktionen

Bestätigen Sie, dass der SMTP-Test in der ISE erfolgreich war, und überprüfen Sie die Konfiguration des E-Mail-Servers:

1. Navigieren Sie in der ISE-GUI zu Administration > System > Settings > SMTP Server.
2. Überprüfen Sie alle SMTP-Einstellungen, einschließlich Serveradresse, Port, TLS/STARTTLS-Konfiguration und Authentifizierungseinstellungen.
 - Stellen Sie sicher, dass die IP-Adresse oder der FQDN des SMTP-Servers (Mail-Gateway) richtig ist.
 - Überprüfen Sie den SMTP-Port: Der Standardwert ist Port 25. Wenn die sichere Übertragung (TLS/STARTTLS) aktiviert ist, muss sie explizit mit dem offenen Port auf dem E-Mail-Server übereinstimmen (z. B. Port 587).
3. Testen Sie die SMTP-Verbindung mit der integrierten Testfunktion.
4. Koordinieren Sie sich mit den Administratoren des E-Mail-Servers, um zu überprüfen, ob Test-E-Mails auf Serverebene empfangen werden.

Phase 2: Debug-Protokollierung auf primärem MnT-Knoten aktivieren

Verwenden Sie den Root-Zugriff, um festzustellen, ob es sich um einen internen Auslöser oder einen externen Verbindungsfehler mit dem Server handelt:

```
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
```

Wenn eine weitere Fehlerbehebung erforderlich ist oder Sie nicht in der Lage sind, den

Datenverkehr über das Root-Netzwerk zu überwachen, aktivieren Sie die detaillierte Protokollierung, um Erinnerungen zu generieren und Übermittlungsversuche per E-Mail zu erfassen.

Aktivieren Sie diese Debugkomponenten auf dem primären MnT-Knoten:

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

Schritt 3: Erfassung von Netzwerkverkehr bei Alarmereignissen

Führen Sie eine Paketerfassung durch, um zu überprüfen, ob die ISE versucht, SMTP-Verbindungen für Alarmereignisse herzustellen:

1. Navigieren Sie zu Operations > Troubleshoot > Diagnostic Tools > TCP Dump auf dem primären MnT-Knoten.
2. Wählen Sie die Netzwerkschnittstelle für die Kommunikation mit dem SMTP-Server.
3. Starten der Paketerfassung
4. Führen Sie bei der Erfassung beide folgenden Schritte aus:
 - Führen Sie den SMTP-Test von der ISE aus (um eine zweifelsfrei funktionierende SMTP-Sitzung zu erfassen).
 - Generieren oder Warten, bis ein tatsächliches Alarmereignis eintritt
5. Beenden Sie die Erfassung und laden Sie die PCAP-Datei zur Analyse herunter.

Schritt 4: Überwachung von Anwendungsprotokollen während der Alarmgenerierung

Überwachen von ISE-Anwendungsprotokollen, um E-Mail-Sendeversuche zu identifizieren

Führen Sie diesen Befehl in der CLI des primären MnT-Knotens aus, während ein Alarm generiert wird:

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

Notieren Sie sich die Ausgabe und den Zeitstempel aller Alarmereignisse, die E-Mail-Benachrichtigungen auslösen müssen.

Schritt 5: Mit E-Mail-Serveradministration abstimmen

Zusammenarbeit mit E-Mail-Serveradministratoren zur Überprüfung der serverseitigen Verarbeitung

Lassen Sie das E-Mail-Team während des Alarmtests die SMTP-Serverprotokolle auf Folgendes überprüfen:

- SMTP-Verbindungen von der IP-Adresse des primären MnT-Knotens
- Status der Annahme, Ablehnung oder des Aufschubs von Nachrichten
- Fehlercodes oder Ablehnungsgründe, wenn Nachrichten nicht akzeptiert werden

Schritt 6: Analysieren der erfassten Daten und Implementieren der Lösung

Überprüfen Sie die erfassten Paketerfassungen, Protokolle und serverseitigen Informationen, um Folgendes zu ermitteln:

- Ob die ISE versucht, Alarm-E-Mails zu senden (sichtbar bei der Paketerfassung).
- Serverantwortcodes und Gründe für die Ablehnung.
- Unterschiede zwischen erfolgreichen SMTP-Testsitzungen und alarmausgelösten Sitzungen.

Implementieren Sie auf der Grundlage der Analyse geeignete Korrekturen, z. B.:

- Anpassen der SMTP-Serverkonfiguration oder der Sicherheitsrichtlinien.

- ISE-Mail-Benachrichtigungseinstellungen werden geändert.
- Absenderadresse oder Authentifizierungsparameter werden aktualisiert.

Schritt 7: Debug-Protokollierung deaktivieren

Deaktivieren Sie nach Abschluss der Fehlerbehebung die Debugprotokollierungskomponenten, um das Wachstum der Protokolldatei zu verhindern.

Deaktivieren Sie die Debugkomponenten auf dem primären MnT-Knoten:

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

Ursache

Das Problem kann darauf zurückzuführen sein, dass der Knoten für primäre Überwachung und Fehlerbehebung (Primary Monitoring & Troubleshooting, MnT) SMTP-Sitzungen für Alarmereignisse anders behandelt als SMTP-Testfunktionen. Während der SMTP-Test erfolgreich war, können die tatsächlichen, durch einen Alarm ausgelösten E-Mail-Versuche fehlschlagen, weil die Konfiguration inkompatibel ist, der E-Mail-Sendevorgang serverseitig gefiltert wurde oder Änderungen vorgenommen wurden, die in der neueren ISE-Version vorgenommen wurden.

Verwandte Inhalte

- [Cisco ISE 3.4 Administrationsleitfaden - Fehlerbehebung](#)
- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.