

軟體升級後不工作的ISE電子郵件警報通知

目錄

問題

思科身份服務引擎(ISE)電子郵件警報通知不會傳送給已配置的收件人。ISE中的SMTP測試功能成功，但實際警報事件不會觸發要傳送的電子郵件通知。從ISE 3.2版升級到3.4版Patch 3後開始出現此問題，甚至在應用3.4版Patch 5後仍然存在。警報電子郵件在應用Patch 5後立即短暫工作，但當電子郵件通知由於高容量而暫時禁用後重新啟用時停止工作。

環境

- 思科身分識別服務引擎(ISE)版本3.4補丁5
- ISE部署包含6個策略服務節點(PSN)、2個監控和故障排除(MnT)節點和2個策略管理節點(PAN)
- 主MnT節點：COR089ISE-MnT02(IP:172.29.134.2)
- SMTP伺服器：smtp1.us.parker.corp
- ISE版本3.2上以前工作配置
- 從3.2版升級到3.4版Patch 3後於10月出現問題

解析

要排除ISE電子郵件警報通知問題，請按照下一節中描述的診斷和解決步驟操作。

步驟 1:驗證SMTP配置和測試功能

確認ISE內的SMTP測試成功並驗證電子郵件伺服器配置：

- 1.在ISE GUI中導航到管理>系統>設定>SMTP伺服器。
- 2.驗證所有SMTP設定，包括伺服器地址、埠、TLS/STARTTLS配置和身份驗證設定。
 - 確保SMTP伺服器（郵件網關）的IP地址或FQDN正確。
 - 檢查SMTP埠:預設值為埠25。如果啟用了安全傳輸(TLS/STARTTLS)，則必須顯式匹配電子郵件伺服器上的開放埠（如埠587）。
- 3.使用內建測試功能測試SMTP連線。
- 4.與電子郵件伺服器管理員協調，確認是否在伺服器級別接收測試電子郵件。

步驟 2:在主MnT節點上啟用調試日誌記錄

使用root訪問來隔離問題是內部觸發成功還是與伺服器的外部連線錯誤：

```
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
```

如果需要進一步的故障排除，或者無法通過root使用者進行監控，請啟用詳細日誌記錄以捕獲警報生成和電子郵件傳送嘗試。

在主MnT節點上啟用以下調試元件：

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

步驟 3:在警報事件期間捕獲網路流量

執行資料包捕獲以驗證ISE是否嘗試為警報事件建立SMTP連線：

1.在主MnT節點上導航到操作>故障排除>診斷工具> TCP轉儲。

2.選擇用於與SMTP伺服器通訊的網路介面。

3.開始資料包捕獲。

4.捕獲時，請同時執行兩項：

- 從ISE運行SMTP測試（以捕獲已知良好的SMTP會話）。
- 生成或等待實際的警報事件發生。

5.停止捕獲並下載PCAP檔案進行分析。

步驟 4:在生成警報期間監視應用程式日誌

監控ISE應用程式日誌以識別電子郵件傳送嘗試。

生成警報時，在主MnT節點CLI上運行此命令：

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

捕獲輸出並記下需要觸發電子郵件通知的所有警報事件的時間戳。

步驟 5:與電子郵件伺服器管理協調

與電子郵件伺服器管理員一起驗證伺服器端處理。

在警報測試期間，讓電子郵件團隊檢查SMTP伺服器日誌，瞭解：

- 來自主MnT節點IP地址的SMTP連線

- 報文接受、拒絕或延期狀態
- 任何錯誤代碼或拒絕原因（如果消息未被接受）

步驟 6:分析捕獲的資料並實施解決方案

檢視收集的資料包捕獲、日誌和伺服器端資訊以確定：

- ISE是否嘗試傳送警報電子郵件（在資料包捕獲中可見）。
- 伺服器響應代碼和任何拒絕原因。
- 成功的SMTP測試會話和警報觸發的會話之間的差異。

根據分析，實施適當的修復，例如：

- 調整SMTP伺服器配置或安全策略。
- 修改ISE電子郵件通知設定。
- 正在更新發件人地址或身份驗證引數。

步驟 7:禁用調試日誌記錄

完成故障排除後，請禁用調試日誌記錄元件以防止日誌檔案增長。

在主MnT節點上禁用調試元件：

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

原因

此問題可能是由於Primary Monitoring & Troubleshooting(MnT)節點處理警報事件的SMTP會話的方

式與SMTP測試功能的不同。當SMTP測試成功時，由於配置不相容、伺服器端過濾或在較新ISE版本中引入的電子郵件傳送進程更改，實際的警報觸發電子郵件嘗試可能失敗。

相關內容

- [思科ISE 3.4管理指南 — 故障排除](#)
- [思科技術支援與下載](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。