

软件升级后ISE电邮警报通知不工作

目录

问题

思科身份服务引擎(ISE)电邮警报通知不会发送给已配置的收件人。ISE中的SMTP测试功能成功，但实际警报事件不会触发要发送的邮件通知。此问题从ISE版本3.2升级到3.4补丁3后开始出现，甚至在应用3.4补丁5后仍然存在。警报邮件在应用补丁5后立即短暂工作，但在邮件通知因大量流量而暂时禁用后重新启用时停止运行。

环境

- 思科身份服务引擎(ISE)版本3.4补丁5
- 具有6个策略服务节点(PSN)、2个监控和故障排除(MnT)节点和2个策略管理节点(PAN)的ISE部署
- 主MnT节点：COR089ISE-MnT02(IP:172.29.134.2)
- SMTP服务器：smtp1.us.parker.corp
- ISE版本3.2上以前的运行配置
- 10月份从版本3.2升级到版本3.4补丁3后开始出现问题

分辨率

要排除ISE电邮警报通知问题，请按照下一节中描述的诊断和解决步骤进行操作。

步骤 1：验证SMTP配置和测试功能

确认ISE内的SMTP测试成功并验证电子邮件服务器配置：

- 1.在ISE GUI中导航到Administration > System > Settings > SMTP Server。
- 2.验证所有SMTP设置，包括服务器地址、端口、TLS/STARTTLS配置和身份验证设置。
 - 确保SMTP服务器（邮件网关）的IP地址或FQDN正确。
 - 检查SMTP端口:默认值为端口25。如果启用了安全传输(TLS/STARTTLS)，则必须明确匹配电子邮件服务器上的开放端口（例如端口587）。
- 3.使用内置的测试功能测试SMTP连接。
- 4.与电子邮件服务器管理员协调，确认是否在服务器级别接收测试电子邮件。

步骤 2：在主MnT节点上启用调试日志记录

使用root访问来隔离问题是内部触发成功还是与服务器的外部连接错误：

```
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
```

如果需要进一步的故障排除或您无法通过root进行监控，请启用详细日志记录以捕获警报生成和邮件传送尝试。

在主MnT节点上启用以下调试组件：

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

步骤 3：在警报事件期间捕获网络流量

执行数据包捕获，验证ISE是否尝试为警报事件建立SMTP连接：

1.在主MnT节点上导航到操作>故障排除>诊断工具> TCP转储。

2.选择用于与SMTP服务器通信的网络接口。

3.开始数据包捕获。

4.捕获时，请同时执行两项：

- 从ISE运行SMTP测试（以捕获已知良好的SMTP会话）。
- 生成或等待实际的警报事件发生。

5.停止捕获并下载PCAP文件进行分析。

步骤 4：在警报生成期间监控应用日志

监控ISE应用日志以确定邮件发送尝试。

生成警报时，在主MnT节点CLI上运行此命令：

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

捕获输出并记下需要触发邮件通知的所有警报事件的时间戳。

步骤 5：与电子邮件服务器管理协调

与电子邮件服务器管理员一起验证服务器端处理。

在警报测试期间，让电子邮件团队检查SMTP服务器日志，了解以下信息：

- 来自主MnT节点IP地址的SMTP连接

- 报文接受、拒绝或延期状态
- 任何错误代码或拒绝原因（如果消息未被接受）

步骤 6：分析捕获的数据并实施解决方案

查看收集的数据包捕获、日志和服务器端信息，以确定：

- ISE是否尝试发送警报邮件（在数据包捕获中可见）。
- 服务器响应代码和任何拒绝原因。
- 成功的SMTP测试会话和警报触发会话之间的差异。

根据分析，实施适当的修复，例如：

- 调整SMTP服务器配置或安全策略。
- 修改ISE邮件通知设置。
- 正在更新发件人地址或身份验证参数。

步骤 7：禁用调试日志记录

完成故障排除后，请禁用调试日志记录组件以防止日志文件增长。

禁用主MnT节点上的调试组件：

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

原因

此问题可能源于主监控和故障排除(MnT)节点处理警报事件的SMTP会话的方式与SMTP测试功能的

不同。当SMTP测试成功时，由于配置不兼容、服务器端过滤或较新ISE版本中引入的邮件发送过程更改，实际的警报触发邮件尝试可能失败。

相关内容

- [Cisco ISE 3.4管理指南 — 故障排除](#)
- [思科技术支持和下载](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。