

Notificaciones de alarma de correo electrónico de ISE que no funcionan después de la actualización de software

Contenido

Problema

Las notificaciones de alarmas por correo electrónico de Cisco Identity Services Engine (ISE) no se envían a los destinatarios configurados. La función de prueba SMTP de ISE se realiza correctamente, pero los eventos de alarma reales no activan el envío de notificaciones de correo electrónico. Este problema comenzó a producirse después de actualizar de ISE versión 3.2 a 3.4 parche 3, y persistió incluso después de aplicar el parche 5 de la versión 3.4. Los correos electrónicos de alarma funcionaron brevemente inmediatamente después de aplicar el parche 5, pero dejaron de funcionar de nuevo cuando se volvieron a habilitar las notificaciones de correo electrónico después de desactivarse temporalmente debido al gran volumen.

Entorno

- Parche 5 de Cisco Identity Services Engine (ISE) versión 3.4
- Implementación de ISE con 6 nodos de servicios de políticas (PSN), 2 nodos de supervisión y solución de problemas (MnT) y 2 nodos de administración de políticas (PAN)
- Nodo MnT principal: COR089ISE-MnT02 (IP: 172.29.134.2)
- Servidor SMTP: smtp1.us.parker.corp
- Configuración operativa anterior en ISE versión 3.2
- El problema comenzó después de la actualización de la versión 3.2 a la 3.4 del parche 3 en octubre

Resolución

Para solucionar problemas de notificación de alarmas de correo electrónico de ISE, siga los pasos de diagnóstico y resolución que se describen en las siguientes secciones.

Paso 1: Verificar configuración SMTP y funcionalidad de prueba

Confirme que la prueba SMTP de ISE se ha realizado correctamente y verifique la configuración del servidor de correo electrónico:

1. Navegue hasta Administración > Sistema > Configuración > Servidor SMTP en la GUI de ISE.
2. Compruebe todos los parámetros de SMTP, incluidos la dirección del servidor, el puerto, la configuración de TLS/STARTTLS y los parámetros de autenticación.
 - Asegúrese de que la dirección IP o FQDN del servidor SMTP (puerta de enlace de correo) es correcta.
 - Verifique el puerto SMTP: El valor predeterminado es el puerto 25. Si se habilita la transmisión segura (TLS/STARTTLS), debe coincidir explícitamente con el puerto abierto del servidor de correo electrónico (como el puerto 587).
3. Pruebe la conexión SMTP utilizando la función de prueba incorporada.
4. Coordine con los administradores del servidor de correo electrónico para confirmar si se están recibiendo correos electrónicos de prueba en el nivel del servidor.

Paso 2: Habilitar el registro de depuración en el nodo MnT principal

Utilice el acceso raíz para aislar si el problema es un éxito del disparador interno o un error de conexión externa con el servidor:

```
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
```

Si se requiere una resolución de problemas adicional o no puede supervisar a través de root, habilite el registro detallado para capturar la generación de alarmas y los intentos de entrega de correo electrónico.

Habilite estos componentes de depuración en el nodo MnT primario:

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

Paso 3: Capturar tráfico de red durante eventos de alarma

Realice la captura de paquetes para verificar si ISE intenta establecer conexiones SMTP para eventos de alarma:

1. Navegue hasta Operaciones > Solución de problemas > Herramientas de diagnóstico > Volcado TCP en el nodo MnT primario.
2. Seleccione la interfaz de red utilizada para comunicarse con el servidor SMTP.
3. Inicie la captura de paquetes.
4. Durante la captura, realice ambos:
 - Ejecute la prueba SMTP desde ISE (para capturar una sesión SMTP de funcionalidad comprobada).
 - Generar o esperar a que se produzca un evento de alarma real.
5. Detenga la captura y descargue el archivo PCAP para su análisis.

Paso 4: Supervisar registros de aplicaciones durante la generación de alarmas

Supervise los registros de la aplicación ISE para identificar los intentos de envío de correo electrónico.

Ejecute este comando en la CLI del nodo MnT primario mientras se genera una alarma:

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

Capture la salida y anote la marca de tiempo de cualquier evento de alarma que necesite activar notificaciones de correo electrónico.

Paso 5: Coordinación con la administración del servidor de correo electrónico

Trabaje con los administradores del servidor de correo electrónico para verificar el procesamiento en el servidor.

Durante las pruebas de alarma, pida al equipo de correo electrónico que compruebe los registros del servidor SMTP para:

- Conexiones SMTP desde la dirección IP del nodo MnT principal
- Estado de aceptación, rechazo o aplazamiento del mensaje
- Cualquier código de error o motivo de rechazo si no se aceptan mensajes

Paso 6: Analizar los datos capturados e implementar la resolución

Revise las capturas de paquetes, los registros y la información del servidor recopilados para determinar:

- Si ISE está intentando enviar correos electrónicos de alarma (visible en la captura de paquetes).
- Códigos de respuesta del servidor y cualquier motivo de rechazo.
- Diferencias entre sesiones de prueba SMTP satisfactorias y sesiones activadas por alarma.

En función del análisis, implemente correcciones adecuadas como:

- Ajustando la configuración del servidor SMTP o las directivas de seguridad.
- Modificación de la configuración de notificación de correo electrónico de ISE.
- Actualizando la dirección del remitente o los parámetros de autenticación.

Paso 7: Deshabilitar registro de depuración

Después de completar la resolución de problemas, inhabilite los componentes de registro de depuración para evitar el crecimiento del archivo de registro.

Inhabilite los componentes de depuración en el nodo MnT primario:

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

Causa

El problema puede deberse a diferencias en la forma en que el nodo de Supervisión y solución de problemas primarios (MnT) gestiona las sesiones SMTP para eventos de alarma frente a las funciones de prueba SMTP. Si bien la prueba de SMTP se realiza correctamente, los intentos reales de envío de correo electrónico activados por alarmas pueden fallar debido a incompatibilidades de configuración, filtrado en el servidor o cambios en el proceso de envío de correo electrónico introducido en la versión más reciente de ISE.

Contenido relacionado

- [Guía de administración de Cisco ISE 3.4: resolución de problemas](#)
- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).