

As notificações de alarme por e-mail do ISE não funcionam após a atualização do software

Contents

Problema

As notificações de alarme por e-mail do Cisco Identity Services Engine (ISE) não estão sendo entregues aos destinatários configurados. A função de teste SMTP no ISE é bem-sucedida, mas os eventos de alarme reais não disparam notificações por e-mail para serem enviadas. Esse problema começou a ocorrer após a atualização do ISE versão 3.2 para 3.4 Patch 3 e persistiu até mesmo após a aplicação do 3.4 Patch 5. Os emails de alarme funcionaram rapidamente imediatamente após a aplicação do Patch 5, mas pararam de funcionar novamente quando as notificações de email foram reativadas depois de serem temporariamente desativadas devido ao alto volume.

Ambiente

- Cisco Identity Services Engine (ISE) versão 3.4 Patch 5
- Implantação do ISE com 6 nós de serviço de política (PSNs), 2 nós de monitoramento e solução de problemas (MnT) e 2 nós de administração de política (PANs)
- Nó MnT primário: COR089ISE-MnT02 (IP: 172.29.134.2)
- Servidor SMTP: smtp1.us.parker.corp
- Configuração anterior em funcionamento no ISE versão 3.2
- Problema iniciado após a atualização da versão 3.2 para a 3.4 Patch 3 em outubro

Resolução

Para solucionar problemas de notificação de alarme por e-mail do ISE, siga as etapas de diagnóstico e resolução descritas nas próximas seções.

Passo 1: Verificar a configuração SMTP e a funcionalidade do teste

Confirme se o teste de SMTP no ISE foi bem-sucedido e verifique a configuração do servidor de e-mail:

1. Navegue até Administration > System > Settings > SMTP Server na GUI do ISE.
2. Verifique todas as configurações de SMTP, incluindo endereço do servidor, porta, configuração de TLS/STARTTLS e configurações de autenticação.
 - Verifique se o endereço IP ou o FQDN do servidor SMTP (Mail Gateway) está correto.
 - Verifique a porta SMTP: O padrão é a porta 25. Se a transmissão segura (TLS/STARTTLS) estiver habilitada, ela deverá corresponder explicitamente à porta aberta no servidor de e-mail (como a porta 587).
3. Teste a conexão SMTP usando a função de teste interna.
4. Coordene com os administradores do servidor de e-mail para confirmar se os e-mails de teste estão sendo recebidos no nível do servidor.

Passo 2: Ativar log de depuração no nó MnT primário

Use o acesso raiz para isolar se o problema é um êxito de disparador interno ou um erro de conexão externa com o 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
2026-06-02 14:51:54,853 ERROR [MnT-AlarmWorkerMail-Threadpool-0][[]] cisco.mnt.common.alarms.AlarmWorke
```

Se for necessária uma solução de problemas adicional ou se você não puder monitorar via raiz, ative o registro detalhado para capturar a geração de alarme e as tentativas de envio de e-mail.

Ative estes componentes de depuração no nó MnT primário:

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

Passo 3: Capturar o tráfego de rede durante eventos de alarme

Execute a captura de pacotes para verificar se o ISE tenta estabelecer conexões SMTP para eventos de alarme:

1. Navegue até Operations > Troubleshoot > Diagnostic Tools > TCP Dump no nó MnT primário.
2. Selecione a interface de rede usada para se comunicar com o servidor SMTP.
3. Inicie a captura de pacotes.
4. Durante a captura, execute:
 - Execute o teste de SMTP do ISE (para capturar uma sessão SMTP em boas condições).
 - Gerar ou aguardar um evento de alarme real.
5. Pare a captura e faça download do arquivo PCAP para análise.

Passo 4: Monitorar Logs de Aplicativos Durante a Geração de Alarmes

Monitore os registros de aplicativos do ISE para identificar tentativas de envio de e-mail.

Execute este comando na CLI do nó MnT primário enquanto um alarme está sendo gerado:

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

Capture a saída e anote o carimbo de data e hora de todos os eventos de alarme que precisam disparar notificações por e-mail.

Passo 5: Coordenar com a administração do servidor de e-mail

Trabalhar com administradores de servidor de email para verificar o processamento no servidor.

Durante o teste de alarme, peça que a equipe de e-mail verifique os registros do servidor SMTP para:

- Conexões SMTP do endereço IP do nó MnT primário
- Status de aceitação, rejeição ou adiamento de mensagem
- Quaisquer códigos de erro ou motivos de rejeição se as mensagens não forem aceitas

Passo 6: Analise os dados capturados e implemente a resolução

Revise as capturas de pacote coletadas, os registros e as informações do servidor para determinar:

- Se o ISE está tentando enviar emails de alarme (visíveis na captura de pacotes).
- Códigos de resposta do servidor e quaisquer motivos de rejeição.
- Diferenças entre sessões de teste SMTP bem-sucedidas e sessões acionadas por alarme.

Com base na análise, implemente correções apropriadas como:

- Ajuste da configuração do servidor SMTP ou das políticas de segurança.
- Modificando configurações de notificação de e-mail do ISE.
- Atualizando endereço do remetente ou parâmetros de autenticação.

Passo 7: Desabilitar Log de Depuração

Após concluir a solução de problemas, desative os componentes de log de depuração para impedir o crescimento do arquivo de log.

Desative os componentes de depuração no nó MnT primário:

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

Causa

O problema pode ser originado de diferenças em como o nó MnT (Primary Monitoring & Troubleshooting, Monitoramento principal e solução de problemas) trata as sessões SMTP para eventos de alarme versus funções de teste SMTP. Embora o teste de SMTP seja bem-sucedido, as tentativas reais de e-mail acionadas por alarme podem falhar devido a incompatibilidades de configuração, filtragem no servidor ou alterações no processo de envio de e-mail introduzidas na versão mais recente do ISE.

Conteúdo relacionado

- [Guia de administração do Cisco ISE 3.4 - Solução de problemas](#)
- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.