Como posso identificar e reagir a um caso de loop de correio no ESA?

Índice

Introdução
Informações de Apoio
Solução
Como evitar que loops de correio ocorram?

Introdução

Este documento descreve como identificar um loop de correio no Email Security Appliance (ESA).

Informações de Apoio

Os loops de correio podem ser identificados por mensagens que apresentam a mesma ID de mensagem mais de 3 vezes. Esses loops geram sintomas como alta utilização da CPU, entrega lenta e outros problemas de desempenho. Normalmente, IDs de mensagem inseridas mais de uma vez já indicariam loop, mas há casos em que as IDs aparecem mais de uma vez devido a problemas ou por descuido de um remetente de spam que envia mensagens com a mesma ID.

O mais comum é que um loop de correio seja gerado por um problema na infraestrutura de e-mail que envia a mesma mensagem ou conjunto de mensagens na rede, de servidor de e-mail a servidor de e-mail, ininterruptamente. Mesmo sendo possível que as mensagens mantenham-se entretidas nessa função por um bom tempo, esse problema não é positivo para a largura de banda da rede nem para o custo de processamento dispendido pelo ESA.

Solução

Em geral, não é difícil identificar um loop de correio, mas é preciso estar atento aos indícios. Acesse a interface de linha de comando (CLI) do sistema e insira um dos seguintes comandos (ou ambos, se julgar necessário):

```
grep "Subject" mail_logs
grep "Message-ID" mail_logs
```

Especificamente em pesquisas por IDs de mensagem, um mail loop pode ser identificado se forem localizadas instâncias recorrentes da mesma ID. Às vezes, contudo, isso não é suficiente, pois, ao reagrupar a mesma mensagem, um dos servidores de e-mail pode estar tentando ajudar alterando ou removendo o cabeçalho da ID de mensagem. Portanto, se não houver indícios substanciais com a verificação das IDs de mensagem, tente a verificação de Assunto.

Se você conseguiu localizar a mensagem em loop pela ID da mensagem, é necessário coletar outras informações sobre a mensagem e sua conexão de entrada (ICID). Com a ID de mensagem e um MID na mesma linha de log, é possível executar:

```
grep -e "MessageID_I_found" -e "MID 123456" mail_logs
```

Com o resultado de saída obtido, é possível identificar o ICID e o DCID relevantes e executar:

```
grep -e "MessageID_I_found" -e "MID 123456" -e "ICID 1234567" -e "DCID 2345767" mail_logs
```

Agora, você dispõe da transação completa entre conexão e mensagem e pode identificar de onde a mensagem veio e onde foi entregue (se isso já ocorreu). Uma vez identificada a mensagem em loop, a próxima etapa é verificar a mensagem para corrigir o problema. Se a causa do loop não for corrigida, é provável que essa e outras mensagens continuem em loop ou que o problema volte a ocorrer em breve.

Crie um filtro de mensagem semelhante a este:

```
loganddrop_looper:
if(header("Message-ID") == "MessageID_I_found") {
  archive("looper");
  drop();
```

Agora, confirme a alteração e digite o comando a seguir para verificar a mensagem:

```
tail looper
```

Com as informações obtidas sobre o sistema remoto ao verificar os logs de correio, juntamente com as outras informações obtidas ao verificar a mensagem, é possível determinar onde está o problema.

Como evitar que loops de correio ocorram?

Em ambientes complexos isto pode ser difícil. É essencial compreender como funciona o fluxo de correio em seu ambiente e como uma nova alteração à rede afetará o tráfego, seja no ESA ou em outro dispositivo. Uma das causas comuns de loops de correio não identificados é a remoção do cabeçalho de recebimento. O ESA detectará e impedirá automaticamente um loop de correio ao identificar 100 cabeçalhos de recebimento em uma mensagem, mas o ESA permite a remoção desse encabeçamento, o que frequentemente gera um loop de correio grave. A menos que haja um bom motivo, não desative ou provoque a remoção do cabeçalho de recebimento.

Abaixo, segue um exemplo de filtro que pode ajudar a prevenir ou corrigir um loop de correio: