Como faço para migrar da quarentena de spam local no Cisco Email Security Appliance (ESA) para a quarentena de spam central no Security Management Appliance (SMA)?

Contents

Introduction

Este documento descreve como mover mensagens em quarentena da quarentena de spam local no ESA para a quarentena de spam central no SMA.

Como faço para migrar da quarentena de spam local no Cisco Email Security Appliance (ESA) para a quarentena de spam central no Security Management Appliance (SMA)?

Hipóteses

A solução a seguir supõe que o dispositivo SMA esteja configurado, de modo que os dispositivos ESA tenham sido adicionados e a quarentena centralizada tenha sido ativada.

Resumo da configuração

1. Habilitar quarentena centralizada no(s) dispositivo(s) ESA:**GUI > Serviços de segurança > Quarentena de spam >Marque Habilitar quarentena de spam externa**
2. Desative a(s) quarentena(s) local(is):**GUI > Monitor > Quarentena de spam> Desmarque Ativar quarentena de spam**
3. Enviar e confirmar alterações.
4. Opcionalmente, migre mensagens de quarentena de quarentena local para central através do processo abaixo.

Procedimento

No dispositivo ESA, você precisaria esvaziar a fila. Para esvaziar a fila de trabalho:

Suspenda todos os ouvintes usando o ouvinte suspensivo do comando CLI e escolha a opção "1. Tudo".

```
> suspendlistener

Choose the listener(s) you wish to suspend.
Separate multiple entries with commas.
1. All
2. Public
3. Test
[*]> 1
```

Aguarde algum tempo até que a maioria das mensagens entregues na fila de entrega seja entregue. (Você pode ver o número de "Destinatários ativos" na saída do **status** dos comandos e **tofosts**).

```
>status
...
Gauges:                                 Current
 Connections
   Current Inbound Conn.                      0
   Current Outbound Conn.                     0
 Queue
   Active Recipients                          1
   Messages In Work Queue                     0
   Kilobytes Used                            85
   Kilobytes Free                    71,303,083
   Messages In Quarantine
     Policy, Virus and Outbreak              10
   Kilobytes In Quarantine
     Policy, Virus and Outbreak              50

> tophosts

Sort results by:

1. Active Recipients
2. Connections Out
3. Delivered Recipients
4. Hard Bounced Recipients
5. Soft Bounced Events
[1]>1

Status as of:                  Mon Sep 29 13:09:53 2014 EDT
Hosts marked with '*' were down as of the last delivery attempt.

                               Active  Conn.     Deliv.       Soft       Hard
#   Recipient Host              Recip.    Out      Recip.    Bounced    Bounced

1   earthlink.net                    1      0          2          0          0
2   the.cpq.host                     0      0          1          0          0
3   the.encryption.queue             0      0         14          0          0
4   the.euq.queue                    0      0          2          0          0
5   the.euq.release.queue            0      0          0          0          0
```

Se após 1 a 2 horas ainda houver algumas mensagens na fila de entrega, você precisará devolver essas mensagens usando o comando **bouncerecipients** escolhendo a opção "3. Tudo" e aguarde até a fila ficar vazia.

```
> bouncerecipients

Please select how you would like to bounce messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 3
```

Remetentes de mensagens devolvidas receberão notificação de que a mensagem não pôde ser entregue)

Suspenda a entrega de mensagens usando o comando **suspenddel**.

```
> suspenddel

Enter the number of seconds to wait before abruptly closing connections.
[30]>
```

Faça um backup de sua configuração por meio do comando **saveconfig** ou **mailconfig**, pois ele exige a limpeza das rotas smtp e sua adição posterior:

```
> saveconfig

Do you want to mask the password? Files with masked passwords cannot be loaded using
loadconfig command. [Y]>
```

Através da GUI, vá para Network -> SMTP Routes e remova todas as rotas smtp. (anote as rotas antigas, pois você precisará adicioná-las novamente mais tarde). Ou, por meio da CLI, use **print** para exibir e, em seguida, **clear** to remove (limpar para remover).

```
> smtproutes


There are currently 4 routes configured.

Choose the operation you want to perform:
- NEW - Create a new route.
- EDIT - Edit destinations of an existing route.
- DELETE - Remove a route.
- PRINT - Display all routes.
- IMPORT - Import new routes from a file.
- EXPORT - Export all routes to a file.
- CLEAR - Remove all routes.
[]> print
..
[]> clear
```

Edite a rota smtp "Todos os outros domínios" e defina-a como o endereço IP do dispositivo SMA e a porta como **6025**.

```
>smtproutes
[]> edit

Enter the hostname you want to edit.
[]> ALL


Choose the operation you want to perform:
- ADD - Add new destination hosts.
- REPLACE - Specify a new destination or set of destinations
[]> REPLACE

Enter the destination hosts, separated by commas, which you want mail for ALL to be
delivered.
Enter USEDNS by itself to use normal DNS resolution for this route.
Enter /dev/null by itself if you wish to discard the mail.
Enclose in square brackets to force resolution via address (A)
records, ignoring any MX records.
[]> mysma.com:6025

Default route updated.
```

Verificar: confirme as alterações e libere 2-3 mensagens de spam da quarentena local como um teste.

```
> commit

Please enter some comments describing your changes:
[]> changed default smtp route to point to SMA
```

Se as mensagens liberadas chegarem corretamente à quarentena de spam centralizada, libere o restante das mensagens.

Depois que todas as mensagens tiverem sido transferidas para o dispositivo SMA, restaure as rotas SMTP antigas no dispositivo ESA.

Desative a quarentena de spam local e ative a quarentena centralizada.

Retomar a operação normal no ESA usando o comando **continuar.**

```
> resume
Mail delivery resumed.
```