# Como eu mantenho cópias das mensagens combinadas por meu filtro da mensagem?

## Índice



## Pergunta:

Como eu mantenho cópias das mensagens combinadas por meu filtro da mensagem?

## Resposta:

Há diversas maneiras de manter cópias das mensagens combinadas por um filtro da mensagem.

A ação do filtro da mensagem do arquivo arquivará uma cópia da mensagem a um arquivo de registro no ESA no formato do arquivo do mbox de UNIX (que é muito um formato de texto simples). Uma vez que criado, o arquivo de registro pode ser controlado com o comando CLI do `filters->logconfig`. Os arquivos de registro podem ser cortados em limites regulares, e regularmente ser empurrados fora para um fileserver do arquivo. Está aqui um exemplo de um filtro da mensagem para registrar todo o correio de entrada ao receptor alan@exchange.example.com:

```
Log-Alan-Todo-correio:
se (== "InboundMail" do RECV-ouvinte)
e (RCPT-ao == de "\ \ alan@exchange \ .example \ .com") {
  arquivo ("alan-todo-correio");
}
```

Na mensagem arquivada, adicional X-IronPort-RCPT-A: os encabeçamentos são adicionados para cada receptor do envelope (a que pôde diferir do índice: linha de cabeçalho.) Note por favor que esta lista de receptores do envelope não inclui necessariamente todos os receptores que o remetente designou. Se um remetente especifica um endereço do bcc, por exemplo, o MTA de emissão pôde escolher enviá-lo inteiramente como uma mensagem separada. São incluídos no log de arquivo os receptores do envelope da transação de SMTP que criou a mensagem.

Nota: A ação do filtro da mensagem do arquivo substitui a ação do log. Os filtros da mensagem que usam os nomes precedentes serão atualizados automaticamente quando o sistema é promovido.

Uma outra maneira de manter cópias de uma mensagem é gerar uma cópia com a ação do filtro do bcc. A ação do bcc faz uma cópia exata da mensagem e envia-a ao receptor designado, que

poderia ser uma caixa postal da coleção em um server do arquivo. Será uma cópia exata do conteúdo de mensagem, mas não inclui os receptores do envelope (a que pôde diferir do índice: linha de cabeçalho.)

```
Cópia-Alan-Todo-correio:
se (== "InboundMail" do RECV-ouvinte)
e (RCPT-ao == de "\ \ alan@exchange \ .example \ .com") {
  bcc ("sam@exchange.example.com ");
}
```

Em ambos os casos acima, a cópia da mensagem é criada pela ação do filtro e entregada sem processamento adicional, que inclui filtros adicionais dos filtros, do anti-Spam, os anti-vírus ou os satisfeitos da mensagem. Assim uma cópia da mensagem pôde conter um vírus.

Há uma ação do filtro nova chamada BCC-varredura.  Isto pode ser usado inseated do bcc para ter a cópia nova feita a varredura através do encanamento normal do email.  Isto deve ser feito para ajudar a reduzir as possibilidades dos vírus ou do Spam de incorporar sua rede.  Aqui está um exemplo:

```
Cópia-Alan-Todo-correio:
se (== "InboundMail" do RECV-ouvinte)
e (RCPT-ao == de "\ \ alan@exchange \ .example \ .com") {
  BCC-varredura ("sam@exchange.example.com ");
}
```

Note que nos filtros acima da mensagem, o argumento para RCPT-à regra é uma expressão regular, que exija operadores de escape do regex tais como ".".  Nas ações do arquivo ou do bcc, o argumento é simplesmente uma sequência de caracteres de texto.

Uma maneira muito a curto prazo de examinar as mensagens combinadas por um filtro envolve usar quarentena do sistema.

Para obter mais informações, consulte

Responda a ID 87: Como eu testo e debugo um filtro da mensagem ou um filtro satisfeito antes que eu o ponha na produção?

Para obter mais informações sobre das ações do filtro da mensagem, veja o AsyncOS para o manual de configuração avançada do email:

Cisco envia por correio eletrónico guias do utilizador final da ferramenta de segurança