

Ejemplo de Configuración de Nombres de Archivo Log ESA de Archivos Adjuntos

Contenido

[Introducción](#)

[Prerequisites](#)

[Configurar](#)

Introducción

Este documento describe cómo registrar los nombres de archivo de los archivos adjuntos que pasan a través del dispositivo de seguridad Cisco Email Security Appliance (ESA).

Prerequisites

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ESA
- Todas las versiones de AsyncOS

Configurar

Nota: En AsyncOS versión 7.x y posteriores, los archivos adjuntos se registran automáticamente si tiene al menos un filtro instalado que comprueba la información del archivo (nombre de archivo, extensión, tipo de archivo y análisis de contenido). Consulte la guía del usuario o la ayuda en línea de AsyncOS para obtener más información.

Esta solución se puede utilizar para versiones anteriores de AsyncOS.

1. Cree un nuevo encabezado que contenga los nombres de todos los archivos adjuntos.
2. Utilice **logconfig > logheaders** para registrar el valor de ese encabezado en el **mail_log**.

Este es un filtro que registra los nombres de archivo de los mensajes que tienen archivos adjuntos:

```
add_filenames_header:
if (attachment-filename == "^.+${}") {
insert-header ("X-fn", "${filenames}");
```

El regex **"^.+\${}"** asegura que hay un adjunto con al menos un carácter en el nombre de archivo. Esto es falso para los mensajes sin archivos adjuntos, por lo que sólo se registran los archivos adjuntos.

Nota: La definición de "adjunto" a un mensaje de correo electrónico es discutible.

Normalmente, las primeras partes de texto/sin formato y texto/HTML se consideran el "cuerpo". Consulte la guía del usuario para obtener más información sobre lo que se considera un archivo adjunto.

A continuación se muestra un ejemplo de lo que aparece en el en mail_logs:

```
Fri Sep 15 13:49:39 2006 Info: Start MID 98 ICID 146
Fri Sep 15 13:49:39 2006 Info: MID 98 ICID 146 From: <joe@example.com>
Fri Sep 15 13:49:39 2006 Info: MID 98 ICID 146 RID 0 To: <carl@example.com>
Fri Sep 15 13:49:39 2006 Info: MID 98 Message-ID '<9151349.VSREACRQ@example.com>'
Fri Sep 15 13:49:39 2006 Info: MID 98 Subject '1:49 pm'
Fri Sep 15 13:49:39 2006 Info: MID 98 ready 20670 bytes from <joe@example.com>
Fri Sep 15 13:49:39 2006 Info: MID 98 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Fri Sep 15 13:49:39 2006 Info: MID 98 antivirus negative
Fri Sep 15 13:49:39 2006 Info: MID 98 queued for delivery
Fri Sep 15 13:49:39 2006 Info: Delivery start DCID 64 MID 98 to RID [0]
Fri Sep 15 13:49:41 2006 Info: Message done DCID 64 MID 98 to RID [0] [('X-fn',
'Encoding.txt')]
Fri Sep 15 13:49:41 2006 Info: MID 98 RID [0] Response '2.0.0 OK 1158353381
r66si9145992pye'
Fri Sep 15 13:49:41 2006 Info: Message finished MID 98 done
```

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).