

Konfigurationsbeispiel für ESA-Protokolldateinamen von Anhängen

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Konfigurieren](#)

Einleitung

In diesem Dokument wird beschrieben, wie die Dateinamen von Anhängen protokolliert werden, die die Cisco E-Mail Security Appliance (ESA) passieren.

Voraussetzungen

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- ESA
- Alle Versionen von AsyncOS

Konfigurieren

Anmerkung: In AsyncOS Version 7.x und höher werden Anlagen automatisch protokolliert, wenn mindestens ein Filter installiert ist, der nach Dateiinformatoren sucht (Dateiname, Erweiterung, Dateityp, Inhaltssuche). Weitere Informationen finden Sie im Benutzerhandbuch oder in der Online-Hilfe zu AsyncOS.

Diese Lösung kann für frühere AsyncOS-Versionen verwendet werden.

1. Erstellen Sie einen neuen Header, der die Dateinamen aller Anhänge enthält.
2. Verwenden Sie `logconfig > logheaders`, um den Wert dieses Headers in `mail_log` aufzuzeichnen.

Hier ist ein Filter, der die Dateinamen von Nachrichten mit Anhängen aufzeichnet:

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

Der reguläre Ausdruck `"^.+ $"` stellt sicher, dass ein Anhang mit mindestens einem Zeichen im Dateinamen vorhanden ist. Bei Nachrichten ohne Anhänge ist dies falsch, daher werden nur Anhänge protokolliert.

Anmerkung: Die Definition von "Anhang" zu einer E-Mail-Nachricht ist umstritten.

Normalerweise werden die ersten Text-/Klartext- und Text-/HTML-Teile als "Text" betrachtet. Im Benutzerhandbuch finden Sie weitere Informationen dazu, was als Anhang betrachtet wird.

Hier ist ein Beispiel, was es in der in 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
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.