

Esempio di configurazione dei nomi file di log ESA degli allegati

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Configurazione](#)

Introduzione

In questo documento viene descritto come registrare i nomi file degli allegati che passano attraverso Cisco Email Security Appliance (ESA).

Prerequisiti

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ESA
- Tutte le versioni di AsyncOS

Configurazione

Nota: In AsyncOS versione 7.x e successive, gli allegati vengono registrati automaticamente se è installato almeno un filtro che controlla le informazioni del file (nome file, estensione, tipo di file, scansione del contenuto). Per ulteriori informazioni, consultare la guida per l'utente o la guida in linea di AsyncOS.

Questa soluzione può essere utilizzata per versioni AsyncOS precedenti.

1. Creare una nuova intestazione contenente i nomi file di tutti gli allegati.
2. Utilizzare **logconfig > logheaders** per registrare il valore dell'intestazione in **mail_log**.

Di seguito è riportato un filtro che registra i nomi file dei messaggi con allegati:

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

Il regex **"^.+\${}"** garantisce la presenza di un allegato con almeno un carattere nel nome file. Questo valore è false per i messaggi senza allegati, pertanto vengono registrati solo gli allegati.

Nota: La definizione di "Allegato" a un messaggio e-mail è discutibile. In genere, le prime parti di testo/testo normale e testo/HTML sono considerate il "corpo". Per ulteriori dettagli su ciò che viene considerato un allegato, consultare il manuale dell'utente.

Di seguito è riportato un esempio di ciò che appare 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
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).