

Häufig gestellte Fragen zur ESA: Wie analysieren Sie zeitweilige E-Mail-Zustellungsprobleme auf der ESA?

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Wie analysieren Sie zeitweilige E-Mail-Zustellungsprobleme auf der ESA?](#)

Einführung

In diesem Dokument wird beschrieben, wie Probleme bei der gelegentlichen E-Mail-Zustellung auf der Cisco E-Mail Security Appliance (ESA) analysiert werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco ESA
- AsyncOS

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf allen Versionen von AsyncOS.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Wie analysieren Sie zeitweilige E-Mail-Zustellungsprobleme auf der ESA?

Sie können die Injection Debug Logs verwenden, um die gesamte SMTP-Konversation (Simple Mail Transfer Protocol) zwischen der ESA und der eingehenden Serververbindung nachzuverfolgen. Jede Zeile in den Injection Debug Logs (Debugprotokolle) beschreibt die Daten, die während der SMTP-Konversation gesendet und empfangen werden.

Gehen Sie wie folgt vor, um die Injection Debug-Protokolle über die Benutzeroberfläche zu aktivieren:

1. Navigieren Sie in der GUI zu **Systemverwaltung > Protokollabonnements**.
2. Wählen Sie **Protokollabonnement hinzufügen aus....**
3. Wählen Sie im Feld Protokolltyp die Option **Injection Debug Logs (Injection Debug-Protokolle) aus**, und geben Sie die entsprechenden Daten ein.

Hier sind einige wichtige Überlegungen, wenn Sie die Daten und den Doppelpunkt Injection Debug Logs eingeben.

- Die CIDR-Adressen wie **10.1.1.0/24** sind zulässig.
- Die IP-Adressbereiche wie **10.1.1.10-20** sind zulässig.
- Die IP-Subnetze wie **10.2.3** sind zulässig.
- Hostnamen und Platzhalter wie **crm.example.com** sind zulässig (aber nicht **example.com**).
- Wildcards sollten als **.example.com** (ohne Sternchen) ausgedrückt werden.
- Wenn Sie eine eingehende E-Mail nachverfolgen, sollte der Hostname dem Absenderhost entsprechen.
- Wenn Sie eine ausgehende E-Mail-Nachricht verfolgen, muss der Hostname mit dem bzw. den internen Hostnamen übereinstimmen.
- Die Anzahl der SMTP-Sitzungen muss zwischen einer und 25 liegen.

Gehen Sie wie folgt vor, um die Injection Debug-Protokolle mit der CLI zu aktivieren:

1. Geben Sie den Befehl **logconfig > new** in die CLI ein.
2. Wählen Sie **Injection Debug Logs aus**.
3. Geben Sie einen Namen für das Protokoll ein, z. B. **debugging_example**.
4. Geben Sie den Hostnamen, die IP-Adresse oder den IP-Adressblock ein, für den Sie die

Informationen zum Debuggen der Injektion aufzeichnen möchten, z. B. **mail1.example.com**.

5. Geben Sie die Anzahl der SMTP-Sitzungen ein, die Sie für diese Domäne aufzeichnen möchten. Stellen Sie sicher, dass der Wert zwischen 1 und 25 liegt.
6. Geben Sie die Methode ein, die Sie zum Abrufen der Protokolle verwenden möchten, z. B. **FTP-Umfrage**.
7. Geben Sie den Dateinamen ein. Sie können den Standarddateinamen verwenden, wenn Sie möchten.
8. Wählen Sie die verbleibenden Standardeinstellungen aus.

Dieses Beispiel zeigt die Injection Debug-Protokolle, wenn die ESA E-Mails von einem Server akzeptiert.

Hinweis: Die Injection Debug Logs und die Domain Debug Logs ähneln den mail_logs, sodass Sie die Befehle **grep** und **tail** verwenden können.

```
Sent to '10.251.21.203': '220 ironportappliance ESMTP\r\n'
Rcvd from '10.251.21.203': 'EHLO outgoing.example.com\r\n'
Sent to '10.251.21.203': '250-nibbles.run\r\n250-8BITMIME\r\n250
SIZE 104857600\r\n'
Rcvd from '10.251.21.203': 'MAIL FROM:<jsmith@example.com>\r\n'
Sent to '10.251.21.203': '250 sender <jsmith@example.com> ok\r\n'
Rcvd from '10.251.21.203': 'RCPT TO:<test@example.org>\r\n'
Sent to '10.251.21.203': '250 recipient <test@example.org>ok\r\n'
Rcvd from '10.251.21.203': 'DATA\r\n'
Sent to '10.251.21.203': '354 go ahead\r\n'
Rcvd from '10.251.21.203': 'To: "test@example.org" <test@example.org>
\r\nSubject: 12:14pm - test\r\nFrom: Hotel_Users <jsmith@example.com>
\r\nContent-Type: text/plain; format=flowed; delp=yes;
charset=iso-8859-15\r\nMIME-Version: 1.0\r\nContent-Transfer-Encoding:
7bit\r\nDate: Tue, 09 Jan 2007 12:14:35 -0800\r\nMessage-ID:
<op.tlwk6lvgwomlp4@outgoing.example.com>\r\nUser-Agent: Opera Mail/9.10
(Win32)\r\n\r\ntest\r\n'
Rcvd from '10.251.21.203': '\r\n.\r\n'
Sent to '10.251.21.203': '250 ok: Message 270 accepted\r\n'
Rcvd from '10.251.21.203': 'QUIT\r\n'
Sent to '10.251.21.203': '221 nibbles.run\r\n'
```