Bestimmung der ESA-Nachrichtenverteilung

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Einstufung einer Nachricht mit den E-Mail-Protokollen ermittelt wird, die von verschiedenen Befehlen der Cisco E-Mail Security Appliance (ESA) abgerufen wurden.

Voraussetzungen

Die Informationen in diesem Dokument basieren auf:

- ESA
- Alle Versionen von AsyncOS

Nachrichtenverfolgung

Wenn Sie AsyncOS für E-Mail Version 6.0 oder höher ausführen, können Sie am effektivsten feststellen, was mit einer bestimmten Nachricht passiert ist, indem Sie die Seite Nachrichtenverfolgung auf der Registerkarte Monitor verwenden. So können Sie in einer benutzerfreundlichen Webschnittstelle mit einer Vielzahl von Optionen suchen.

Wenn Sie eine ältere Version ausführen oder alle Protokollzeilen zu Fehlerbehebungszwecken sammeln müssen, verwenden Sie die Befehle **grep** oder **findevent** wie in den nächsten Abschnitten beschrieben.

Findevent-Befehl

Wenn Sie AsyncOS für E-Mail Version 5.1.2 oder höher haben, wird die Suche nach einer bestimmten Nachricht mithilfe des Befehls CLI **Findevent** vereinfacht. **Findevent** ermöglicht die Suche nach dem Umschlag, dem Umschlagempfänger oder der Betreffzeile. Dies kann auch unabhängig vom Einzelfall erfolgen. Sobald Sie Ihre Nachricht gefunden haben, können Sie jede für diese Nachricht relevante Protokollzeile zurückgeben. Wenn Sie **Findevent** ohne Argumente

ausführen, wird ein Assistent gestartet, der Sie durch den Prozess führt. Wie immer können Sie den Befehl **help** verwenden, um die Kurzform zu lernen:

```
> help findevent
findevent [-i] [-f from | -s subject | -t to] log_name
findevent -m mid log_name
```

Das erste Formular führt eine Suche nach einem bestimmten Umschlag von, Betreff oder Umschlag innerhalb des benannten log_name durch und listet die übereinstimmenden Nachrichten-IDs (MIDs) auf. Das -i-Flag kann für die Suche ohne Groß- und Kleinschreibung verwendet werden.

Im zweiten Formular werden alle Protokollzeilen für die angegebene MID angezeigt.

Wenn Sie eine ältere Version haben, kann der Befehl CLI **grep** verwendet werden, um dasselbe zu erreichen. Die Verwendung des Befehls **grep** erfordert jedoch genauere Informationen darüber, wie ESAs Meldungen protokollieren.

Grep-Befehl

Die erste Herausforderung bei der Suche nach E-Mail-Protokollen besteht darin, Ihre Nachricht zu finden. Sie können dies tun, wenn Sie nach dem Absender, dem Empfänger oder dem Betreff suchen. Sobald Sie Ihre Nachricht gefunden haben, ist es wichtig zu verstehen, wie die Mail-Protokolle organisiert sind. Content Security-E-Mail-Protokollereignisse werden mit Akronymen versehen. Die wichtigsten Ereignisse sind ICID, MID, RID und DCID.

Injection Connection ID (ICID): Wenn ein Remotehost eine Verbindung zur Appliance herstellt, wird dieser Verbindung eine ICID zugewiesen. Eine ICID kann viele MIDs hervorrufen.

> **Hinweis**: **ICID 0** definiert eine Nachricht, die von sich selbst eingebracht wurde. Tatsächlich bezieht sich die Zahl 0 nach einer ICID oder DCID auf Sitzungen, die der lokalen Schleifenadresse des Geräts oder von dieser aus offen stehen.

MID: Sobald eine Verbindung hergestellt wurde, erhalten Sie jede erfolgreiche SMTP-**E-Mail von:** erstellt eine neue MID. Eine einzige MID kann viele RIDs hervorrufen.

Empfänger-ID (RID): Jeder Empfänger (An: CC: oder Bcc erhält eine RID. RIDs geben nur dann mehrere DCIDs aus, wenn ein Soft Bounce (Verbindungsfehler) vorliegt und die Zustellung erneut versucht wird.

Delivery Connection ID (DCID): Jeder Empfänger, der an dieselbe Zieldomäne weitergeleitet wird, erhält bis zu den Grenzen des empfangenden Systems die gleiche DCID. Wenn also die Empfänger einer Nachricht alle an dieselbe Domäne gehen, gibt es eine DCID für alle RIDs. Wenn stattdessen jede RID zu einer separaten Domäne wechselt, gibt es eine 1:1-Korrelation.

> **Hinweis**: **DCID 0** definiert eine Nachricht, die nie gesendet wurde. Tatsächlich bezieht sich die Zahl 0 nach einer ICID oder DCID auf Sitzungen, die der lokalen Schleifenadresse des Geräts oder von dieser aus offen stehen.

Wenn Sie Ihre Nachricht finden, finden Sie im Allgemeinen die zugehörige MID. Anschließend

werden die MID und die ICID und die RID eingezeichnet. Mit der ICID können Sie die SenderBase-Reputationsbewertung (SBRS) für den Absender festlegen. Mit der RID und dann der DCID können Sie bestimmen, was passiert ist, als die ESA versuchte, die Lieferung durchzuführen.

> **Hinweis**: Sobald Sie die MID, die ICID und die DCID haben, können Sie alle Zeilen für diese Nachricht in einem **grep** abrufen, wenn der Ursprung der Nachricht nicht älter als das älteste E-Mail-Protokoll ist.

```
example.com> grep -e " MID 11123" -e " ICID 11092" -e " DCID 23349" mail_logs
```

Beispiel

1. Suchen Sie nach dem Betreff der Nachricht:

```
example.com> grep
Currently configured logs:
16. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
Enter the number of the log you wish to grep.
[]> 16
Enter the regular expression to grep.
[]> test
Do you want this search to be case insensitive? [Y]>
Do you want to tail the logs? [N]>
Do you want to paginate the output? [N]>
Mon Jan 23 10:25:03 2006 Info: SMTP listener testpairlist starting
Tue Jan 24 12:10:15 2006 Info: Message aborted MID 8 Dropped by filter
'testdrop'
Tue Jan 31 23:55:38 2006 Info: MID 32 Subject 'testmsgquarantine'
Wed Feb 1 00:23:59 2006 Info: MID 62 Subject 'testmsgquarantine'
Wed Feb 1 00:27:48 2006 Info: MID 64 Subject 'testmsg2'
Wed Feb 1 22:30:37 2006 Info: MID 80 Subject 'test zip'
Wed Feb 1 22:37:51 2006 Info: MID 83 Subject 'FW: test zip'
Wed Feb 1 22:41:50 2006 Info: MID 84 Subject 'FW: test zip'
Fri Feb 3 15:17:47 2006 Info: MID 94 Subject 'test'
Fri Feb 3 15:42:06 2006 Info: MID 96 Subject 'test'
```

Dadurch wurden mehrere Übereinstimmungen generiert, die **Test** im Betreff enthielten. Die Nachricht wurde um ca. 15:42 Uhr gesendet, sodass Sie diese MID für die nächste Suche verwenden können.

Im Folgenden sind einige wichtige Punkte zu den Fragen aufgeführt:

Soll diese Suche ohne Berücksichtigung der Groß- und Kleinschreibung durchgeführt werden? [J]>
Wenn Sie diese Frage mit **Ja** beantworten, werden Einträge unabhängig vom Fall gefunden.

Möchten Sie die Protokolle abschalten? [N]>
Wenn Sie **Ja** zu dieser Frage beantworten, werden nur neue Einträge gefunden, wie sie generiert werden. Es werden nicht alle Protokolldateien durchsucht. Wählen Sie **Nein**, um

alle Protokolle zu durchsuchen.

Möchten Sie die Ausgabe paginieren? [N]>
Wenn Sie **Ja** zu dieser Frage beantworten, werden die Einträge nacheinander angezeigt. Dies ist nützlich, wenn Sie eine allgemeine Suche durchführen und viele Einträge abrufen müssen. Dadurch wird verhindert, dass die Einträge von der Anzeige wegscrollen.

2. Suchen Sie nach der MID:

```
mail.example.com> grep
Currently configured logs:
16. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
Enter the number of the log you wish to grep.
[]> 16
Enter the regular expression to grep.
[]> MID 96
Do you want this search to be case insensitive? [Y]>
Do you want to tail the logs? [N]>
Do you want to paginate the output? [N]>
Fri Feb 3 15:41:43 2006 Info: Start MID 96 ICID 10394
Fri Feb 3 15:41:43 2006 Info: MID 96 ICID 10394 From: <bob@example.net>
Fri Feb 3 15:41:58 2006 Info: MID 96 ICID 10394 RID 0 To:
<nasir@example.com>
Fri Feb 3 15:42:06 2006 Info: MID 96 Message-ID
<4o8836$30@mail.example.com>
Fri Feb 3 15:42:06 2006 Info: MID 96 Subject 'test'
Fri Feb 3 15:42:06 2006 Info: MID 96 ready 23 bytes from
<bob@example.net>
Fri Feb 3 15:42:06 2006 Info: MID 96 matched all recipients for
per-recipient policy DEFAULT in the outbound table
Fri Feb 3 15:42:06 2006 Info: MID 96 antivirus negative
Fri Feb 3 15:42:06 2006 Info: MID 96 queued for delivery
Fri Feb 3 15:42:06 2006 Info: Delivery start DCID 14 MID 96 to RID [0]
Fri Feb 3 15:42:06 2006 Info: Message done DCID 14 MID 96 to RID [0]
Fri Feb 3 15:42:06 2006 Info: MID 96 RID [0] Response '2.6.0
<4o8836$30@mail.example.com> Queued mail for delivery'
Fri Feb 3 15:42:06 2006 Info: Message finished MID 96 done
```

Beachten Sie, dass die MID-Einträge weitere Informationen über die Verarbeitung der Nachricht enthalten. Die MID-Einträge beziehen sich auch auf die ICID und die DCID. Wenn Sie mehr über die eingehende Verbindung wissen möchten, **grep** für die ICID. Wenn Sie mehr darüber erfahren möchten, was passiert ist, als die ESA eine Lieferung versuchte, **grep** für die DCID.

3. Um zu bestimmen, wo die Nachricht zugestellt wurde, suchen Sie nach der DCID.

```
mail.example.com> grep
Currently configured logs:
16. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
Enter the number of the log you wish to grep.
[]> 16
Enter the regular expression to grep.
[]> DCID 14
Do you want this search to be case insensitive? [Y]>
```

```
Do you want to tail the logs? [N]>
Do you want to paginate the output? [N]>
Fri Feb 3 15:42:06 2006 Info: New SMTP DCID 14 interface 192.168.0.199
address 10.1.1.112 port 25
Fri Feb 3 15:42:06 2006 Info: Delivery start DCID 14 MID 96 to RID [0]
Fri Feb 3 15:42:06 2006 Info: Message done DCID 14 MID 96 to RID [0]
Fri Feb 3 15:42:11 2006 Info: DCID 14 close
```

Beachten Sie, dass die Nachricht von der Schnittstelle **192.168.0.199** mit der IP-Adresse **10.1.112** über Port 25 an den Host übermittelt wurde.

Wenn die Zustellung nicht versucht wurde, die Nachricht aber **zur Zustellung in die Warteschlange gestellt** wurde, weist dies darauf hin, dass das System Schwierigkeiten bei der Kommunikation mit dem Zielserver haben könnte. Sie können den **Hoststatus** in der CLI verwenden, um zu überprüfen, ob der Status des Empfängerhosts **Down** ist und um zu überprüfen, ob die bestellten IPs entweder Ihren SMTP-Routen für die Zieldomäne oder den öffentlichen MX-Datensätzen entsprechen.