ESA消息处理确定

目录

简介

本文描述如何确定一个消息的处理与从多种on命令检索的邮件日志的Cisco电子邮件安全工具(ESA)。

先决条件

本文档中的信息基于：

- ESA
- AsyncOS所有版本

消息跟踪

如果运行电子邮件版本6.0或以上的AsyncOS，多数有效方式确定什么发生在特定消息将使用从监视器选项卡的消息跟踪页。这允许您搜索与在一个易用Web接口的各种各样的选项。

如果运行早版本或需要采集所有为了实现故障排除目的记录行，请使用**grep**或**findevent**命令详情参见以下部分。

Findevent命令

如果有电子邮件版本5.1.2或以上的AsyncOS， CLI **findevent**命令简化搜索特定留言。**Findevent**让您由信封从，信封收件人或者消息主题搜索。这可以执行不管案件。一旦查找您的消息，您能归还每条记录行与该消息有关。如果运行**findevent**没有参数，启动向导为了通过进程指导您。一如既往，您能使用**help命令**为了学习简易格式：

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

第一个形式进行一个特定信封从，主题或者信封的一搜索对在已命名log_name内并且列出消息ID (MID)该匹配。- i标志位能用于非案例敏感的搜索。

第二表显示所有给的MID的记录行。

如果有一早版本， **grep命令的**CLI可以用于为了完成同一件事。然而，使用**grep命令**如何要求更多详细的知识ESAs日志消息事件。

grep命令

第一挑战，当您搜索邮件日志时是查找您的消息。如果搜索发送方，收件人，或者主题，您能执行此。一旦找到您的消息，知道是重要的邮件日志如何被组织。内容安全邮件日志事件给缩略语。最重要的事件是ICID、MID、RID和DCID。

射入连接ID (ICID) ：当远程主机建立对设备时的连接，该连接分配ICID。一个ICID能产生许多MID。

> **Note**:**ICID 0**定义了从本身被注入的消息。实际上，数字0，在ICID或DCID是指会话开放到/从设备的本地环路地址后。

MID ：一旦连接被建立，每成功的简单邮件传输协议(SMTP)**邮件从：**命令创建新的MID。单个MID能产生许多RID。

收件人ID (RID) ：每收件人(对：抄送：或者BCC获得RID。RID只产生多个DCIDs，如果有一次软的跳动(连接错误)，并且交付是重新尝试。

交付连接ID (DCID) ：去同一个目的地域的每收件人接收同样DCID至接收系统的限额。因此，如果收件人消息全部去同一个域，然后有所有的一个DCID RID。如果，每个RID去一个分开的域，则有一对一相关性。

> **Note**:**DCID 0**定义了未曾传送的信息。实际上，数字0，在ICID或DCID是指会话开放到/从设备的本地环路地址后。

通常，当您查找您的消息时，您查找其MID。然后您MID的grep和确定ICID和RID。使用ICID，您能确定SenderBase名誉斯克尔(SBRS)在发送方上。使用RID然后DCID，您能确定发生什么，当ESA尝试了交付。

> **Note**:一旦有MID、ICID和DCID，您能获取所有该消息的行在一**grep**，如果消息的始发地比您的最旧的邮件日志不旧。

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

示例

1. 消息主题的搜索：

```
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'
```

这生成包含在主题的**测验的**几匹配。信息传送了在近似3:42pm，因此您能使用该MID下搜索。

这是注释的一些impotant点关于问题：

是否希望此搜索是不区分的案件？[Y] **>**
如果回答**是**对此问题，不管案件，查找条目。

是否要盯梢日志？[N] **>**
如果回答**是**对此问题，只查找新的条目，当他们生成。它不搜索所有日志文件。选择**没有**为了搜索所有日志。

是否要上页数输出？[N] **>**
如果回答**是**对此问题，每次显示条目一个页。如果需要执行一一般搜索和期望获取许多条目，这是有用的。这从移动显示终止条目。

2. MID的搜索：

```
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
```

注意MID条目提供关于的更多信息消息如何处理。MID条目也参考ICID和DCID。如果要知道更多流入连接， ICID的**grep**。如果要知道更多发生什么，当ESA尝试了交付， DCID的**grep**。

3. 为了确定消息哪里传送，请搜索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
```

注意消息从**192.168.0.199**接口传送到有IP地址10.1.1.112的主机在端口25。

如果交付未尝试，但是消息**为交付排队**，表明系统也许有在其通信的困难用目标服务器。您能使用从CLI的**hoststatus**为了发现接收主机的状况是否下降和验证指定IP匹配您的目的地域的SMTP路由或公共MX记录，如可适用。