

了解并排除SMA消息跟踪中缺少3分钟范围数据间隔的问题

目录

简介

本文档介绍原因以及如何排除SMA上缺少3分钟范围数据间隔的消息跟踪数据的故障。

要求

了解以下主题：

- 思科安全管理设备(SMA)
- 思科邮件安全设备(ESA)
- 集中邮件跟踪

使用的组件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

问题

SMA从ESA设备遇到多达三分之一的缺少数据间隔。

Message Tracking Data Availability

Printable PDF 

Tracking Data Range				
Status	Security Appliance		Data Range	
	IP Address	Description	From ▼	To
OK	192.168.235.65	VXOIRP-ESA-BB001	15 Jul 2020 18:36 (GMT +02:00)	14 Feb 2023 08:52 (GMT +01:00)
OK	192.168.235.64	VXOIRP-ESA-AA001	15 Jul 2020 18:36 (GMT +02:00)	14 Feb 2023 08:52 (GMT +01:00)
Overall:			15 Jul 2020 18:36 (GMT +02:00)	14 Feb 2023 08:52 (GMT +01:00)

Missing Data Intervals				
Items Displayed 10 ▼ All Email Appliances ▼				
Security Appliance		Missing Data Range		
IP Address	Description	From ▼	To	
192.168.235.64	VXOIRP-ESA-AA001	14 Feb 2023 08:01 (GMT +01:00)	14 Feb 2023 08:04 (GMT +01:00)	
192.168.235.64	VXOIRP-ESA-AA001	14 Feb 2023 07:40 (GMT +01:00)	14 Feb 2023 07:43 (GMT +01:00)	
192.168.235.65	VXOIRP-ESA-BB001	14 Feb 2023 06:49 (GMT +01:00)	14 Feb 2023 06:52 (GMT +01:00)	
192.168.235.64	VXOIRP-ESA-AA001	14 Feb 2023 05:16 (GMT +01:00)	14 Feb 2023 05:19 (GMT +01:00)	
192.168.235.65	VXOIRP-ESA-BB001	14 Feb 2023 04:28 (GMT +01:00)	14 Feb 2023 04:31 (GMT +01:00)	
192.168.235.65	VXOIRP-ESA-BB001	14 Feb 2023 03:46 (GMT +01:00)	14 Feb 2023 03:49 (GMT +01:00)	
192.168.235.65	VXOIRP-ESA-BB001	14 Feb 2023 02:07 (GMT +01:00)	14 Feb 2023 02:10 (GMT +01:00)	
192.168.235.64	VXOIRP-ESA-AA001	13 Feb 2023 23:16 (GMT +01:00)	13 Feb 2023 23:19 (GMT +01:00)	
192.168.235.64	VXOIRP-ESA-AA001	13 Feb 2023 20:16 (GMT +01:00)	13 Feb 2023 20:19 (GMT +01:00)	
192.168.235.65	VXOIRP-ESA-BB001	13 Feb 2023 17:37 (GMT +01:00)	13 Feb 2023 17:40 (GMT +01:00)	

解决方案

本地和集中邮件跟踪简要工作流程

跟踪工作有两种模式：

I. 欧空局本地跟踪。

1. Trackerd解析由qlogd(tracking.@*.s)处理的跟踪信息二进制日志文件中的数据
2. Trackerd将其保存在/data/db/reporting/haystack下。

二。欧空局集中跟踪。

1. qlogd将跟踪信息二进制日志文件(tracking.@*.s.gz)写入/data/pub/export/tracking目录
2. SMA smad进程检查、拉动，然后从ESA的/data/pub/export/tracking目录中删除跟踪原始数据(tracking.@*.s.gz)。
3. 从ESA提取的跟踪文件保存在SMA的/data/log/tracking/<ESA_IP>/目录中。
4. Trackerd将文件移动到/data/tracking/incoming_queue/0/<ESA_IP>目录，并处理文件。
5. 删除存储在MT数据库和跟踪文件中的已处理文件。

调查步骤

步骤1:ESA trackerd_logs分析

在/data/pub/trackerd_logs/folder中观察trackerd_logs后，发现ESA上的qlogd一般会写入3分钟间隔

的跟踪数据文件。

在本示例中，文件夹/data/pub/export/tracking/T*部分文件名中的数据文件表示文件的生成时间。T值之间的差值为3分钟。

```
grep "172.16.200.12" trackerd.current | tail
Wed Mar  8 22:07:36 2023 Info: Tracking parser moved /data/log/tracking/172.16.200.12/tracking.@2023030
Wed Mar  8 22:12:03 2023 Info: Tracking parser moved /data/log/tracking/172.16.200.12/tracking.@2023030
Wed Mar  8 22:14:28 2023 Info: Tracking parser moved /data/log/tracking/172.16.200.12/tracking.@2023030
Wed Mar  8 22:16:53 2023 Info: Tracking parser moved /data/log/tracking/172.16.200.12/tracking.@2023030
Wed Mar  8 22:19:19 2023 Info: Tracking parser moved /data/log/tracking/172.16.200.12/tracking.@2023030
Wed Mar  8 22:23:48 2023 Info: Tracking parser moved /data/log/tracking/172.16.200.12/tracking.@2023030
```

第二步：SMA trackerd_logs分析

根据步骤1中获取的信息，检查SMA上的/data/pub/trackerd_logs，以便在问题部分中查找和确认丢失的数据文件。

此帧中介绍了相关日志示例及其结果。仅对第一个ESA(192.168.235.64)在SMA上过滤的trackerd_logs:

```
/data/pub/trackerd_log on SMA - filtered only for ESA 192.168.235.64
```

```
Mon Feb 13 20:11:06 2023 Info: Tracking parser moved /data/log/tracking/192.168.235.64/tracking.@202302
Mon Feb 13 20:15:18 2023 Info: Tracking parser moved /data/log/tracking/192.168.235.64/tracking.@202302
Mon Feb 13 20:17:26 2023 Info: Tracking parser moved /data/log/tracking/192.168.235.64/tracking.@202302
tracking.@20230213T191631Z_20230213T191931Z.s.gz - the file is missing -- this line is manually ad
Mon Feb 13 20:23:40 2023 Info: Tracking parser moved /data/log/tracking/192.168.235.64/tracking.@202302
Mon Feb 13 20:25:51 2023 Info: Tracking parser moved /data/log/tracking/192.168.235.64/tracking.@202302
```

```
Mon Feb 13 23:15:20 2023 Info: Tracking parser moved /data/log/tracking/192.168.235.64/tracking.@202302
Mon Feb 13 23:17:27 2023 Info: Tracking parser moved /data/log/tracking/192.168.235.64/tracking.@202302
tracking.@20230213T221632Z_20230213T221932Z.s.gz - the file is missing -- this line is manually ad
Mon Feb 13 23:23:42 2023 Info: Tracking parser moved /data/log/tracking/192.168.235.64/tracking.@202302
Mon Feb 13 23:25:52 2023 Info: Tracking parser moved /data/log/tracking/192.168.235.64/tracking.@202302
Mon Feb 13 23:30:04 2023 Info: Tracking parser moved /data/log/tracking/192.168.235.64/tracking.@202302
```

..... Log examples for two missed files can be considered satisfactory. Omitted logs for other files t

In Summary, Missing file examples on SMA from ESA 192.168.235.64:

```
tracking.@20230213T191631Z_20230213T191931Z.s.gz
tracking.@20230213T221632Z_20230213T221932Z.s.gz
tracking.@20230214T041633Z_20230214T041933Z.s.gz
tracking.@20230214T064034Z_20230214T064334Z.s.gz
tracking.@20230214T070134Z_20230214T070434Z.s.gz
```

第三步：smaduser操作分析

下一步是检查ESA的/data/pub/cli_logs/上的SMA smad行为。

如前所述，smad在/data/pub/export/tracking(ls -AF)中检查ESA的文件，复制文件(scp -f ./tracking.*.s.gz)，然后由smaduser通过SSH访问删除该文件(rm ./tracking.*.s.gz)。

在此步骤中，发现主SMA(IP: 172.24.81.94)在主SMA下载和删除文件之前还有另一个SMA(IP: 192.168.251.92)。

当主SMA检查目录(ls -AF)中的文件时，它无法看到该文件，因为192.168.251.92 smaduser已将其删除。

相关日志示例如下：

```
for file tracking.@20230213T191631Z_20230213T191931Z.s.gz
```

```
grep -i "tracking.@20230213T191631Z_20230213T191931Z.s.gz" cli.current (missing file on SMA)
Mon Feb 13 20:19:29 2023 Info: PID 51423: User smaduser login from 172.24.81.94 on 192.168.235.64
Mon Feb 13 20:19:29 2023 Info: PID 51423: User smaduser executed batch command: 'ls -AF /export/tracking
Mon Feb 13 20:19:29 2023 Info: PID 51423: User smaduser logged out of Command Line Interface using SSH
Mon Feb 13 20:19:32 2023 Info: PID 51485: User smaduser login from 192.168.251.92 on 192.168.235.64
Mon Feb 13 20:19:32 2023 Info: PID 51485: User smaduser executed batch command: 'ls -AF /export/tracking
Mon Feb 13 20:19:32 2023 Info: PID 51485: User smaduser logged out of Command Line Interface using SSH
Mon Feb 13 20:19:35 2023 Info: PID 51541: User smaduser login from 192.168.251.92 on 192.168.235.64
Mon Feb 13 20:19:35 2023 Info: PID 51541: User smaduser executed batch command: 'scp -f /export/tracking
Mon Feb 13 20:19:38 2023 Info: PID 51599: User smaduser login from 192.168.251.92 on 192.168.235.64
Mon Feb 13 20:19:38 2023 Info: PID 51599: User smaduser executed batch command: 'rm /export/tracking/tr
Mon Feb 13 20:19:39 2023 Info: PID 51599: User smaduser logged out of Command Line Interface using SSH
```

```
for file tracking.@20230213T221632Z_20230213T221932Z.s.gz
```

```
grep -i "tracking.@20230213T221632Z_20230213T221932Z.s.gz" cli.current
Mon Feb 13 23:19:33 2023 Info: PID 19143: User smaduser login from 192.168.251.92 on 192.168.235.64
Mon Feb 13 23:19:33 2023 Info: PID 19143: User smaduser executed batch command: 'ls -AF /export/tracking
Mon Feb 13 23:19:33 2023 Info: PID 19143: User smaduser logged out of Command Line Interface using SSH
Mon Feb 13 23:19:37 2023 Info: PID 19231: User smaduser login from 192.168.251.92 on 192.168.235.64
Mon Feb 13 23:19:37 2023 Info: PID 19231: User smaduser executed batch command: 'scp -f /export/tracking
Mon Feb 13 23:19:40 2023 Info: PID 19339: User smaduser login from 192.168.251.92 on 192.168.235.64
Mon Feb 13 23:19:40 2023 Info: PID 19339: User smaduser executed batch command: 'rm /export/tracking/tr
Mon Feb 13 23:19:40 2023 Info: PID 19339: User smaduser logged out of Command Line Interface using SSH
```

..... Log examples for two missed files can be considered satisfactory. Omitted logs for other files t

解决方案摘要

跟踪邮件跟踪过程本身有助于成功解决此问题。

在ESA上通过cli_logs确定了另一个SMA。它会连接到ESA，拉取并删除文件，然后删除主SMA。该文件对于主SMA不可用。

在冗余SMA“安全设备”上删除ESA/禁用ESA服务，或完全停用生产中的冗余SMA。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。