

瞭解並排除SMA消息跟蹤中缺少3分鐘範圍資料間隔的問題

目錄

簡介

本文檔介紹原因以及如何排除SMA上缺少3分鐘範圍資料間隔的消息跟蹤資料的故障。

需求

瞭解以下主題：

- 思科安全管理裝置(SMA)
- 思科電子郵件安全裝置(ESA)
- 集中郵件跟蹤

採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

問題

SMA從ESA裝置發現丟失資料間隔多達三分鐘。

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)	

解決方案

本地和集中郵件跟蹤簡要工作流程

跟蹤工作有兩種模式：

I. 歐空局當地跟蹤。

1. Trackerd分析由qlogd (跟蹤。@*.s) 處理的跟蹤資訊二進位制日誌檔案中的資料
2. Trackerd將其儲存在/data/db/reporting/haystack下。

二。歐空局的集中跟蹤。

1. qlogd將跟蹤資訊二進位制日誌檔案(tracking.@*.s.gz)寫入/data/pub/export/tracking目錄
2. SMA smad進程檢查、拉入，然後從ESA的/data/pub/export/tracking目錄刪除跟蹤原始資料(tracking.@*.s.gz)。
3. 從ESA提取的跟蹤檔案儲存在SMA的/data/log/tracking/<ESA_IP>/目錄中。
4. Trackerd將檔案移動到/data/tracking/incoming_queue/0/<ESA_IP>目錄，處理檔案。
5. 已處理儲存在MT資料庫中的檔案和跟蹤檔案將被刪除。

調查步驟

步驟1。ESA trackerd_logs分析

在/data/pub/trackerd_logs/folder中觀察trackerd_logs後，發現ESA上通常qlogd會寫出3分鐘間隔的

跟蹤資料檔案。

在本示例中，資料夾/data/pub/export/tracking/ T*部分檔名中的資料檔案表示檔案的生成時間。T值之間的差值為3分鐘。

```
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
```

步驟2。SMA跟蹤日誌分析

根據在步驟1中獲取的資訊，檢查SMA上的/data/pub/trackerd_logs，以在「問題」部分中查詢和確認丟失的資料檔案。

此幀中介紹了相關日誌樣本及其結果。僅對第一個ESA(192.168.235.64)在SMA上過濾的 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
```

步驟3。smaduser操作分析

下一步是檢查ESA的/data/pub/cli_logs/上的SMA smad行為。

如前所述，smad檢查/data/pub/export/tracking(ls -AF)中的ESA檔案，複製檔案(scp -f ./tracking.*.s.gz)，然後由smaduser通過SSH訪問將其刪除(rm ./tracking.*.s.gz)。

在此步驟中，發現與主SMA(IP: 172.24.81.94)相比，有另一個SMA(IP: 192.168.251.92)連線到ESA下載並刪除檔案，然後才進行主SMA。

主SMA檢查目錄(ls -AF)中的檔案時，它無法看到該檔案，因為192.168.251.92 smaduser已將其刪除。

相關日誌示例如下：

```
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

解決方案摘要

跟蹤郵件跟蹤過程本身有助於成功解決此問題。

在ESA上通過cli_logs確定了另一個SMA。它會連線到ESA，拉出並移除主SMA之前的檔案。該檔案對於主SMA不可用。

在冗餘SMA「安全裝置」上刪除ESA/禁用ESA服務，或將冗餘SMA完全退出生產。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。