瞭解並解決SMA消息跟蹤中缺少的3分鐘範圍資料間隔問題

目錄

簡介

本文檔介紹在SMA上使用3分鐘範圍資料間隔缺失消息跟蹤資料的原因以及如何對其進行故障排除。

需求

瞭解以下主題：

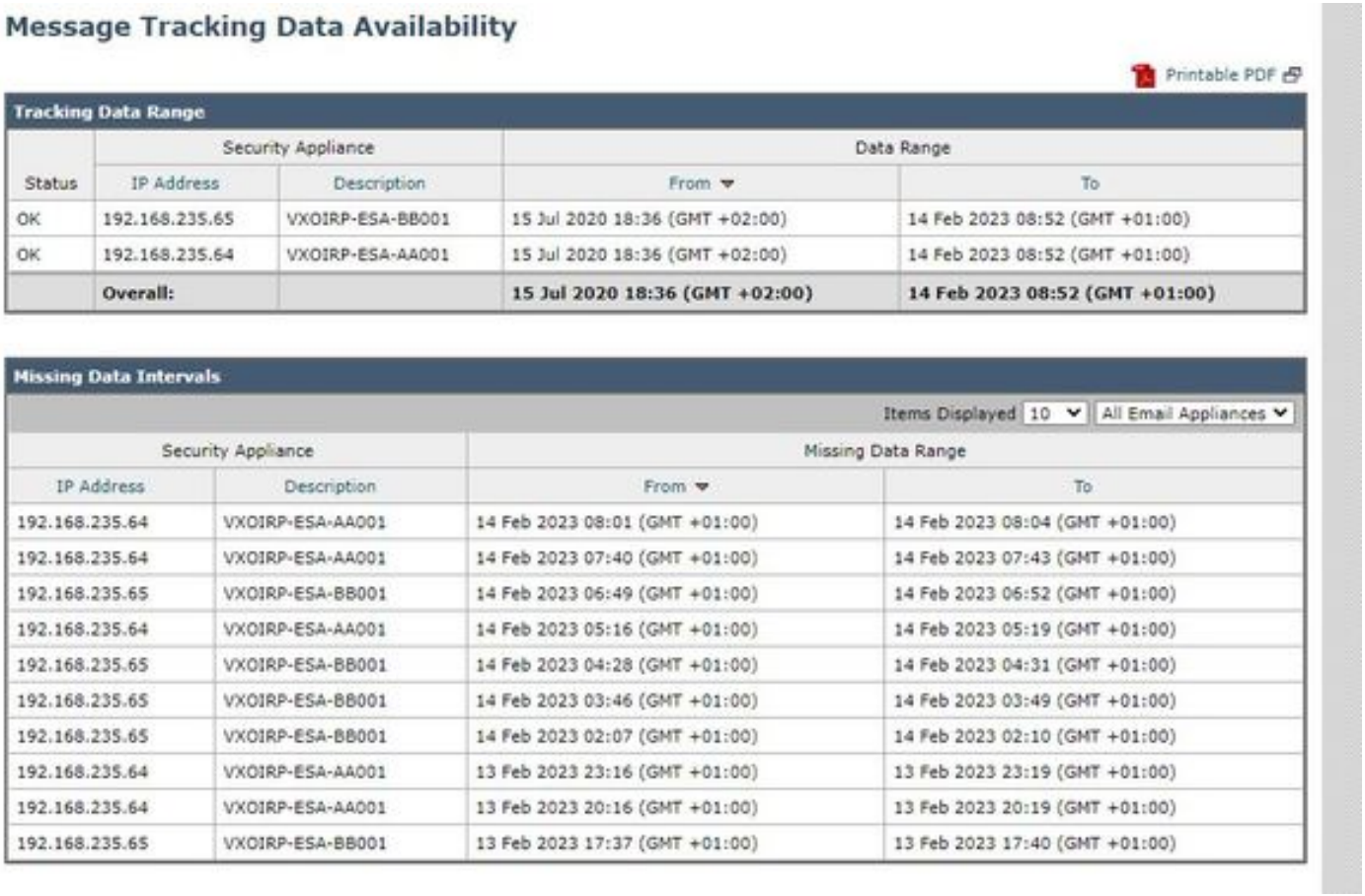
- 思科安全管理裝置(SMA)
- 思科電子郵件安全裝置(ESA)
- 集中郵件跟蹤

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在ESA裝置上遇到許多3分鐘的資料間隔缺失。



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

追蹤工作有兩種模式：
I.歐洲太空總署本地跟蹤。
1. Trackerd解析由qlogd（跟蹤。@*.s）處理的跟蹤資訊二進位制日誌檔案中的資料

2. 跟蹤者將其儲存在佔有頻寬下。

二。歐洲太空總署集中跟蹤。
1. qlogd將跟蹤資訊二進位制日誌檔案(tracking.@*.s.gz)寫到/data/pub/export/tracking目錄中
2. SMA smad進程檢查、提取，然後從ESA的/data/pub/export/tracking目錄中刪除跟蹤原始資料(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會將檔案移至/data/tracking/incoming_queue/0/<ESA_IP>目錄，並處理檔案。
5. 處理MT資料庫儲存檔案和跟蹤檔案被刪除。

調查步驟

步驟 1.ESA trackerd_logs分析

在/data/pub/trackerd_logs/資料夾中觀察trackerd_logs後，發現ESA上通常使用qlogd命令會寫出

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*中的資料檔案是檔名的一部分，代表檔案的生成時間。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 trackerd_logs分析

根據在步驟1中獲取的資訊，在SMA上檢查**/data/pub/trackerd_logs**，以便在問題部分中查詢並確認丟失的資料檔案。

本架構將介紹相關日誌示例和結果。僅針對第一個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: Tra
```

步驟 3.smaduser動作分析

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**透過**SSH**訪問將其刪除(rm /../tracking.*.s.gz)。

在此步驟中，發現另一個SMA (IP： 192.168.251.92)比主SMA (IP： 172.24.81.94)連線到ESA下載並在主SMA之前刪除檔案。

主SMA檢查目錄(ls -AF)中的檔案時，無法看到檔案，因為192.168.251.92 smaduser已將其刪除。
相關日誌樣本如下：

```
for file tracking.@20230213T191631Z_20230213T191931Z.s.gz grep -i "tracking.@20230213T191631Z_20230213T
```

解決方案摘要

追蹤訊息追蹤程式本身可協助成功克服問題。
透過ESA上的cli_logs，確定了另一個SMA。它連線到ESA，在主SMA之前提取並刪除檔案。該檔案對主SMA不可用。

刪除ESA/停用冗餘SMA「安全裝置」上的ESA服務，或完全停用生產中的冗餘SMA。

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）。