Understand and Troubleshoot Missing 3-Minute Range Data Intervals on SMA Message Tracking

Contents

Introduction

This document describes the reason and how to troubleshoot missing Message Tracking Data with 3 minute range data intervals on SMA.

Requirements

Knowledge of these topics:

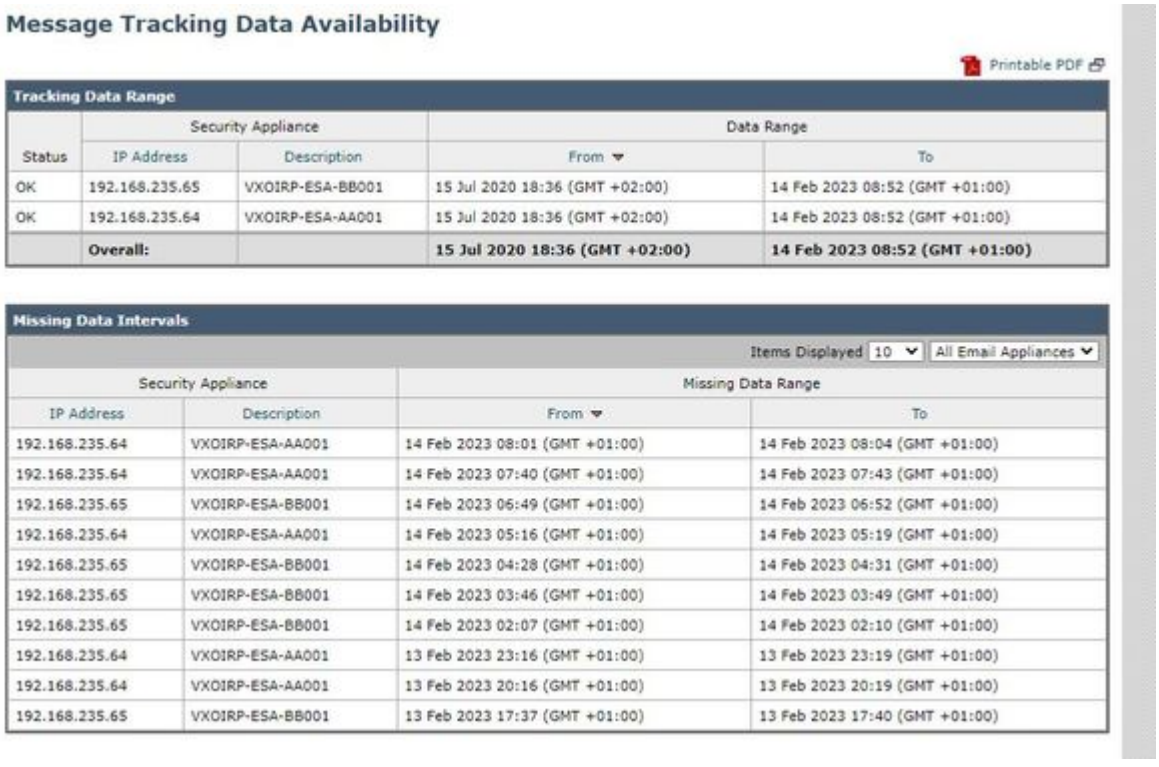
- Cisco Security Management Appliance (SMA)
- Cisco Email Security Appliance (ESA)
- Centralized Message Tracking

Components Used

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Problem

SMA encounters many 3 minutes missing data intervals from ESA appliances.



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)

Solution

Local and Centralized Message Tracking Brief Workflow

Tracking works in two modes:
I. ESA Local Tracking.
1. Trackerd parses data from tracking information binary log files processed by qlogd (tracking.@*.s)

2. Trackerd saves it under /data/db/reporting/haystack.

II. ESA Centralized Tracking.
1. qlogd writes out tracking information binary log files (tracking.@*.s.gz) into /data/pub/export/tracking directory
2. SMA smad process checks, pulls, and then deletes the tracking raw data (tracking.@*.s.gz) from /data/pub/export/tracking directory of ESA.
3. Pulled tracking files from ESAs are saved on /data/log/tracking/<ESA_IP>/ directory of SMA.
4. Trackerd moves files to /data/tracking/incoming_queue/0/<ESA_IP> directory, processes files.
5. Processed files stored in MT Database and tracking files are removed.

Investigation Steps

Step 1. ESA trackerd_logs Analysis

After observing trackerd_logs in **/data/pub/trackerd_logs/** folder, identified that generally **qlogd** on ESA writes out 3-minuntes interval tracking data files.

In this example, data files in folder **/data/pub/export/tracking/ T*** part of filename represents generated time of the file. Difference between T values are 3 minutes.

```
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.@20230308
Wed Mar  8 22:12:03 2023 Info: Tracking parser moved /data/log/tracking/172.16.200.12/tracking.@20230308
Wed Mar  8 22:14:28 2023 Info: Tracking parser moved /data/log/tracking/172.16.200.12/tracking.@20230308
Wed Mar  8 22:16:53 2023 Info: Tracking parser moved /data/log/tracking/172.16.200.12/tracking.@20230308
Wed Mar  8 22:19:19 2023 Info: Tracking parser moved /data/log/tracking/172.16.200.12/tracking.@20230308
Wed Mar  8 22:23:48 2023 Info: Tracking parser moved /data/log/tracking/172.16.200.12/tracking.@20230308
```

Step 2. SMA trackerd_logs Analysis

Based on information gained in step 1, check **/data/pub/trackerd_logs** on SMA in order to find out and confirm missed data files in **Problem** section.

Relevant log samples with results is described in this frame. Filtered trackerd_logs on SMA only for first ESA (192.168.235.64):

```
/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 add
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 add
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 to


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
```

Step 3. Analysis of smaduser Actions

Next step is checking of SMA **smad** behavior on /data/pub/cli_logs/ of ESA.

As mentioned smad checks for files of ESA in /data/pub/export/tracking (ls -AF), copies file (scp -f /../tracking.*.s.gz) and then removes it (rm /../tracking.*.s.gz) by **smaduser** via the **SSH** access.

In this step it has been identified that there is another SMA (IP: 192.168.251.92) than main SMA (IP: 172.24.81.94) connects to ESA downloads and removes the file before main SMA.

When main SMA checks for files in directory (ls -AF), it cannot see the file as it has been already removed by 192.168.251.92 smaduser.
Relevant log sample is as follows:

```
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 c
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 c
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/tra
Mon Feb 13 20:19:39 2023 Info: PID 51599: User smaduser logged out of Command Line Interface using SSH c


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 c
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/tra
Mon Feb 13 23:19:40 2023 Info: PID 19339: User smaduser logged out of Command Line Interface using SSH c


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

Solution Summary

Tracing of Message Tracking process itself helped to overcome the problem successfully.
Via cli_logs on ESA another SMA has been identified. It connects to ESA, pulls and then removes the file before main SMA. The file becomes unavailable for main SMA.

Remove ESAs / disable ESA Services on redundant SMA 'Security Appliances' or decommission redundant SMA completely from production.