SMA 메시지 추적에 대한 3분 범위 데이터 간격 누락 이해 및 트러블슈팅

목차

소개

이 문서에서는 SMA에서 3분 범위의 데이터 간격으로 누락된 메시지 추적 데이터를 트러블슈팅하는 방법과 그 이유에 대해 설명합니다.

요구 사항

다음 항목에 대한 지식:

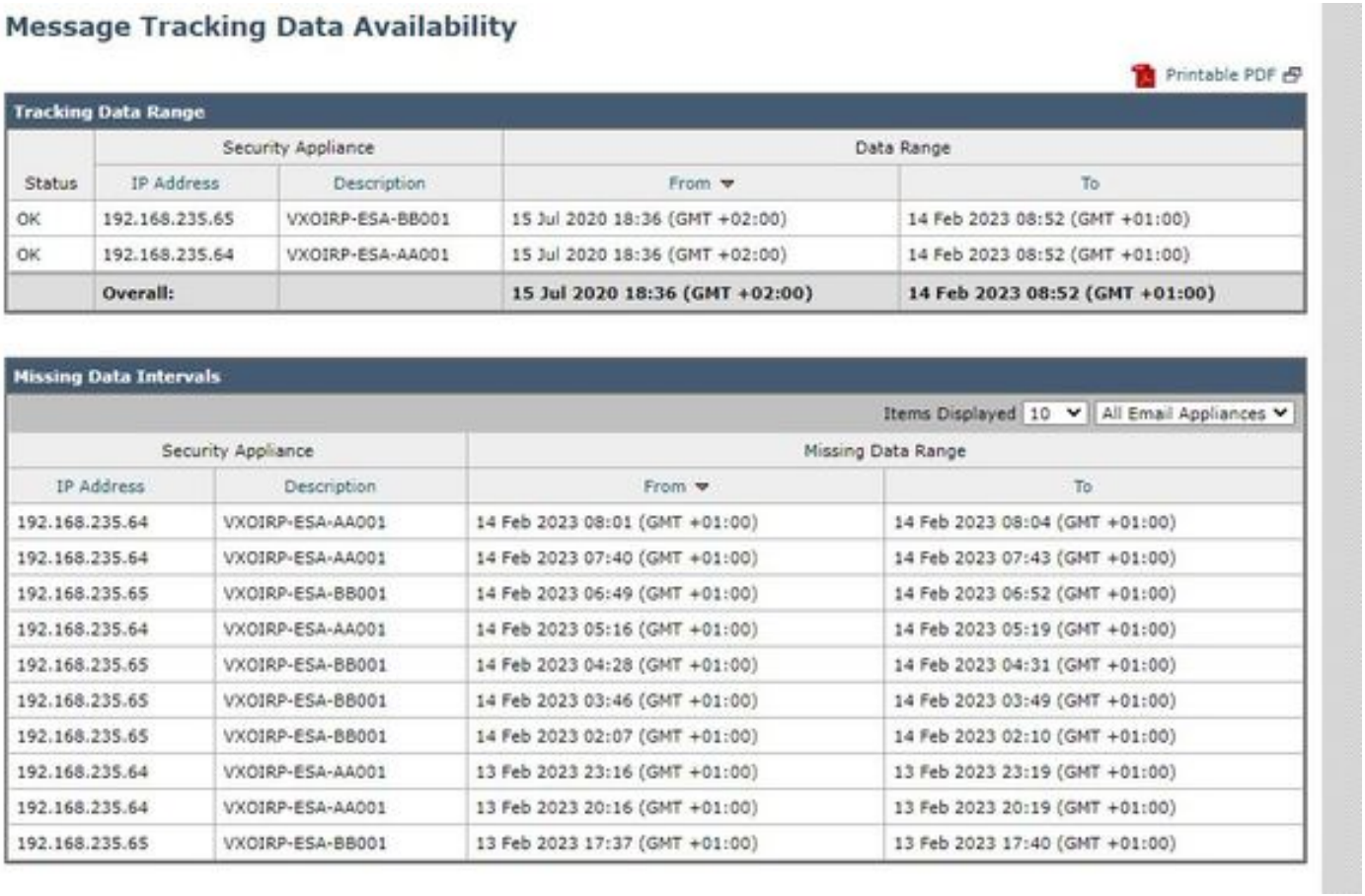
- Cisco SMA(Security Management Appliance)
- Cisco ESA(Email Security Appliance)
- 중앙 메시지 추적

사용되는 구성 요소

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

문제

SMA에서는 ESA 어플라이언스에서 3분 동안 데이터 간격이 누락되는 경우가 많습니다.



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)

솔루션

로컬 및 중앙 메시지 추적 요약 워크플로

추적은 두 가지 모드로 작동합니다.
I. ESA 로컬 추적
  1. Trackerd는 qlogd에서 처리된 추적 정보 이진 로그 파일에서 데이터를 구문 분석합니다 (tracking.@*.s).

  2. Trackerd는 /data/db/reporting/haystack에 저장합니다.

II. ESA 중앙 추적
  1. qlogd는 추적 정보 이진 로그 파일(tracking.@*.s.gz)을 /data/pub/export/tracking 디렉토리에 씁니다.
  2. SMA smad 프로세스는 ESA의 /data/pub/export/tracking 디렉토리에서 추적 원시 데이터 (tracking.@*.s.gz)를 확인, 풀링한 다음 삭제합니다.
  3. ESA에서 가져온 추적 파일은 SMA의 /data/log/tracking/<ESA_IP>/ 디렉토리에 저장됩니다.
  4. 추적된 파일은 /data/tracking/incoming_queue/0/<ESA_IP> 디렉토리로 이동하고 파일을 처리합니다.
  5. MT 데이터베이스에 저장된 가공 파일 및 추적 파일이 제거됩니다.

조사 단계

1단계. ESA trackerd_logs 분석

trackerd_logs in /data/pub/trackerd_logs/folder를 관찰한 후, 일반적으로 ESA에서 qlogd가 3분 간격 추적 데이터 파일을 기록하는 것을 확인했습니다.

이 예에서 파일 이름의 폴더/data/pub/export/tracking/T* 부분의 데이터 파일은 파일의 생성 시간을 나타냅니다. T 값의 차이는 3분입니다.

```
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
```

2단계. SMA trackerd_logs 분석

1단계에서 얻은 정보를 기반으로 SMA의 /data/pub/trackerd_logs를 확인하여 Problem 섹션에서 누락된 데이터 파일을 찾아 확인합니다.

결과가 포함된 관련 로그 샘플은 이 프레임에 설명되어 있습니다. 첫 번째 ESA에 대해서만 SMA에서 필터링된 trackerd_logs(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 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
```

3단계. smaduser 작업 분석

다음 단계는 ESA의 /data/pub/cli_logs/에서 SMA smad 동작을 확인하는 것입니다.

앞서 언급한 대로 smad는 /data/pub/export/tracking(ls -AF)에서 ESA의 파일을 확인하고 파일(scp -f /.../tracking.*.s.gz)을 복사한 다음 SSH 액세스를 통해 smaduser가 이 파일(rm /../tracking.*.s.gz)을 제거합니다.

이 단계에서는 주 SMA(IP: 172.24.81.94)가 ESA에 연결하여 주 SMA 이전에 파일을 다운로드하고 제거하는 것보다 다른 SMA(IP: 192.168.251.92)가 있는 것으로 확인되었습니다.

기본 SMA가 디렉토리(ls -AF)에서 파일을 확인할 때 192.168.251.92 smaduser에 의해 이미 제거된 파일을 볼 수 없습니다.
관련 로그 샘플은 다음과 같습니다.

```
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/trackin
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/trackin
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/trackin
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/trackin
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/trackin
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
```

솔루션 요약

메시지 추적 프로세스 추적 자체가 문제를 성공적으로 해결하는 데 도움이 되었습니다.
ESA의 cli_logs를 통해 다른 SMA가 식별되었습니다. ESA에 연결하여 주 SMA 전에 파일을 가져온 다음 제거합니다. 주 SMA에서 파일을 사용할 수 없게 됩니다.

중복 SMA 'Security Appliances'에서 ESA를 제거하거나 ESA 서비스를 비활성화하거나 프로덕션 환경에서 중복 SMA를 완전히 해제합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.