Analyse und Fehlerbehebung bei Datenintervallen im 3-Minuten-Bereich bei der SMA-Nachrichtenverfolgung

Inhalt

Einleitung

In diesem Dokument werden der Grund und die Fehlerbehebung für fehlende Nachrichtenverfolgungsdaten mit Datenintervallen von 3 Minuten auf SMA beschrieben.

Anforderungen

Kenntnisse dieser Themen:

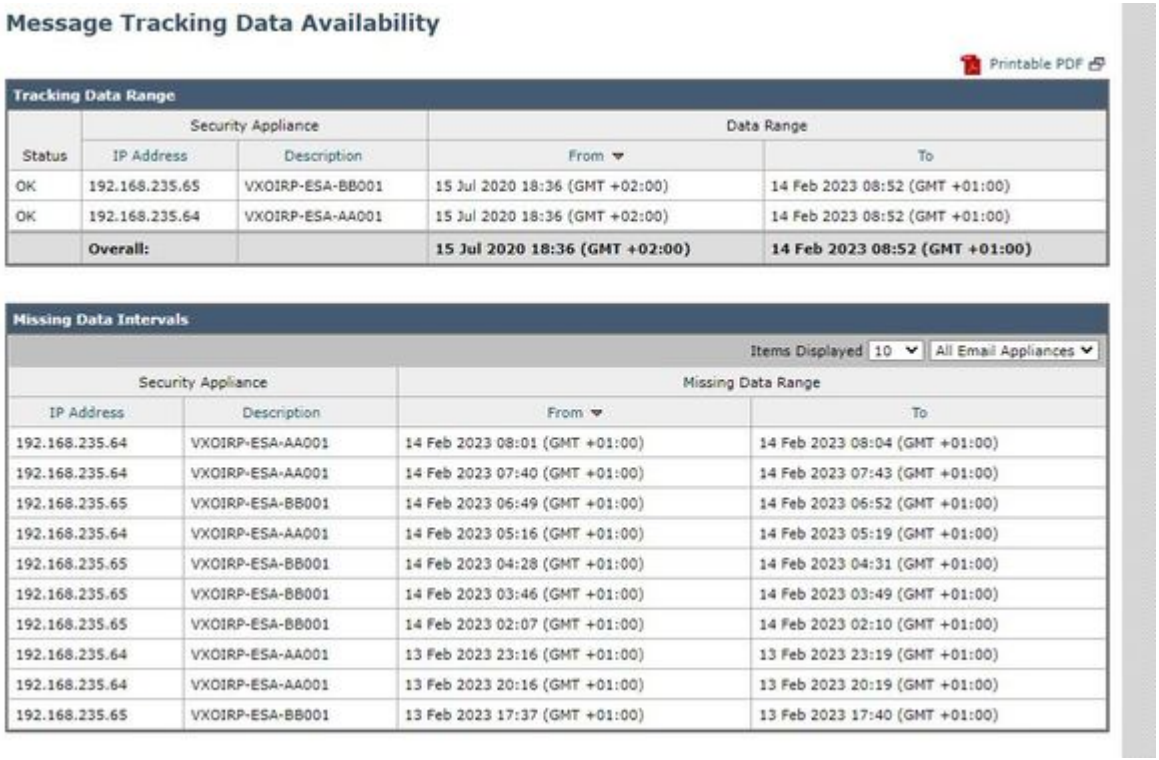
- Cisco Security Management Appliance (SMA)
- Cisco E-Mail Security Appliance (ESA)
- Zentrale Nachrichtenverfolgung

Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Problem

Bei SMA treten viele fehlende 3-Minuten-Datenintervalle bei ESA-Einheiten auf.



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)

Lösung

Lokaler und zentralisierter Workflow für die Nachrichtenverfolgung

Die Nachverfolgung funktioniert in zwei Modi:
I. Lokales ESA-Tracking.
1. Trackerd parst Daten von Nachverfolgungsinformationen binäre Protokolldateien, die von qlogd (tracking.@*.s) verarbeitet werden

2. Trackerd speichert es unter /data/db/reporting/haystack.

II. Zentrales ESVG-Tracking
1. qlogd schreibt binäre Protokolldateien (tracking.@*.s.gz) in das Verzeichnis /data/pub/export/tracking
2. SMA smad Prozess überprüft, zieht und löscht dann die Tracking-Rohdaten (tracking.@*.s.gz) aus dem Verzeichnis /data/pub/export/tracking der ESA.
3. Abgerufene Tracking-Dateien von ESAs werden im Verzeichnis /data/log/tracking/<ESA_IP>/ von SMA gespeichert.
4. Trackerd verschiebt Dateien in das Verzeichnis /data/tracking/incoming_queue/0/<ESA_IP> und verarbeitet Dateien.
5. Verarbeitete Dateien in MT-Datenbank gespeichert und Tracking-Dateien werden entfernt.

Ermittlungsschritte

Schritt 1: ESA-Trackerd_logs-Analyse

Nach der Beobachtung trackerd_logs in **/data/pub/trackerd_logs/**Ordner, identifiziert, dass im Allgemeinen **qlogd** auf ESA schreibt 3-minuntes Intervall-Tracking-Datendateien.

In diesem Beispiel stellt der Teil von Dateiname Datendateien im Ordner **/data/pub/export/tracking/T*** die generierte Zeit der Datei dar. Die Differenz zwischen den T-Werten beträgt 3 Minuten.

```
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
```

Schritt 2: Analyse von SMA-Protokollen

Basierend auf den in Schritt 1 gewonnenen Informationen überprüfen Sie /**data/pub/trackerd_logs** auf SMA, um verpasste Datendateien im Abschnitt **Problem** zu finden und zu bestätigen.

Relevante Protokollbeispiele mit Ergebnissen werden in diesem Frame beschrieben. Gefilterte trackerd_logs auf SMA nur für erste 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
```

Schritt 3: Analyse von Schlägeraktionen

Der nächste Schritt ist die Überprüfung des SMA-**SMAD**-Verhaltens auf /data/pub/cli_logs/ der ESA.

Wie erwähnt, überprüft smad Dateien der ESA in /data/pub/export/tracking (ls -AF), kopiert die Datei (scp -f /../tracking.*.s.gz) und entfernt sie dann (rm /../tracking.*.s.gz) durch **smaduser** über den **SSH**-Zugang.

In diesem Schritt wurde festgestellt, dass es eine andere SMA (IP: 192.168.251.92) als Haupt-SMA (IP: 172.24.81.94) verbindet sich mit ESA-Downloads und entfernt die Datei vor Haupt-SMA.

Wenn die Haupt-SMA nach Dateien im Verzeichnis (ls -AF) sucht, kann sie die Datei nicht sehen, da sie bereits von 192.168.251.92 smaduser entfernt wurde.
Relevante Protokollstichprobe:

```
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
```

Lösungsübersicht

Die Nachverfolgung der Nachrichtenverfolgung hat dazu beigetragen, das Problem erfolgreich zu beheben. Über cli_logs auf der ESA wurde eine weitere SMA identifiziert. Es stellt eine Verbindung zur ESA her, zieht und entfernt die Datei vor der Haupt-SMA. Die Datei ist für die Haupt-SMA nicht mehr verfügbar.

Entfernen Sie ESAs/deaktivieren Sie ESA Services auf redundanten SMA 'Security Appliances' oder setzen Sie redundante SMA vollständig aus der Produktion aus.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.