Comprender y solucionar problemas de intervalos de datos de 3 minutos que faltan en el rastreo de mensajes SMA

Contenido

Introducción

Este documento describe el motivo y cómo resolver problemas de datos de rastreo de mensajes perdidos con intervalos de datos de rango de 3 minutos en SMA.

Requirements

Conocimiento de estos temas:

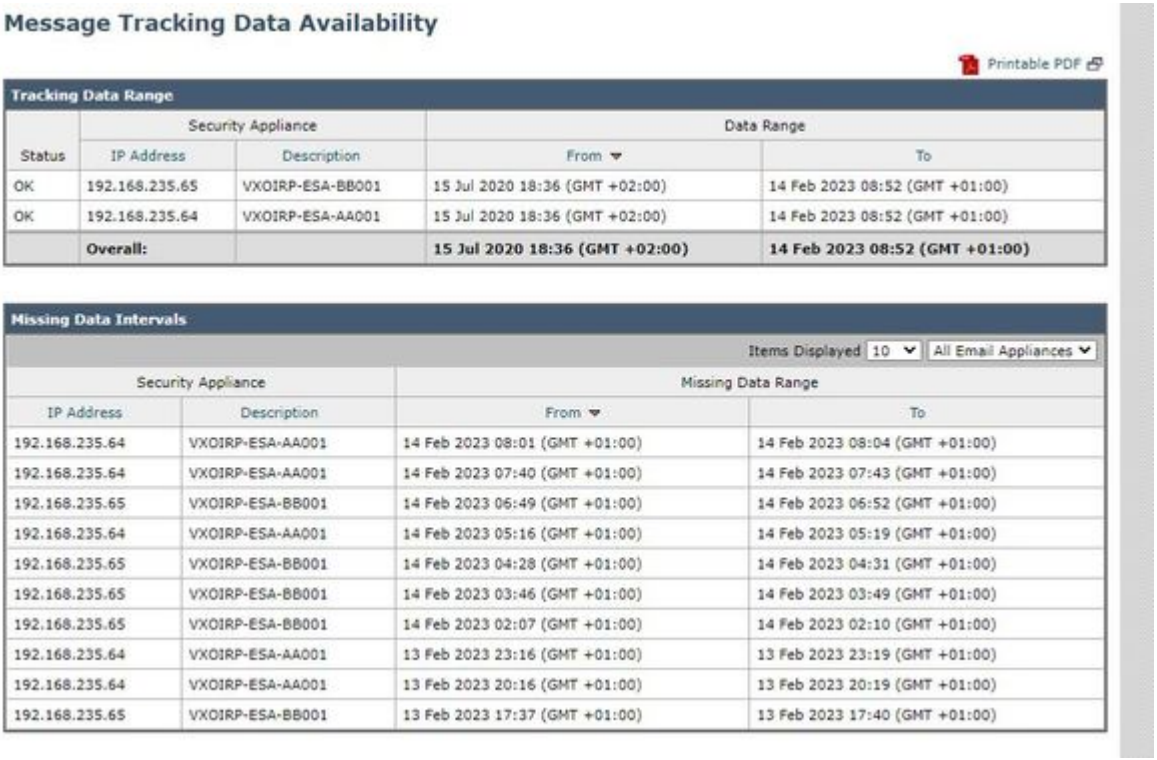
- Dispositivo de administración de seguridad de Cisco (SMA)
- Dispositivo de seguridad Cisco Email Security Appliance (ESA)
- Rastreo de mensajes centralizado

Componentes Utilizados

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Problema

El SMA detecta muchos intervalos de datos de 3 minutos que faltan en los dispositivos ESA.



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)

Solución

Flujo de trabajo breve de rastreo de mensajes local y centralizado

El seguimiento funciona de dos modos:
I. Seguimiento local ESA.
1. Trackerd analiza los datos de seguimiento de la información de seguimiento de los archivos de registro binarios procesados por qlogd (tracking.@*.s)

2. Trackerd lo guarda bajo /data/db/reporting/haystack.

II. Seguimiento centralizado de la ESA.
1. qlogd escribe información de rastreo archivos de registro binarios (tracking.@*.s.gz) en el directorio /data/pub/export/tracking
2. El proceso SMA smad comprueba, extrae y elimina los datos sin procesar de seguimiento (tracking.@*.s.gz) del directorio /data/pub/export/tracking de ESA.
3. Los archivos de seguimiento extraídos de los ESA se guardan en el directorio /data/log/tracking/<ESA_IP>/ del SMA.
4. Trackerd mueve archivos al directorio /data/tracking/incoming_queue/0/<ESA_IP>, procesa archivos.
5. Los archivos procesados almacenados en la base de datos MT y los archivos de seguimiento se eliminan.

Pasos de investigación

Paso 1. Análisis de ESA trackerd_logs

Después de observar trackerd_logs en **/data/pub/trackerd_logs/** carpeta, identificó que generalmente **qlogd** en ESA escribe archivos de datos de seguimiento de intervalos de 3 minutos.

En este ejemplo, los archivos de datos de la parte folder **/data/pub/export/tracking/ T*** de nombre de archivo representan la hora de generación del archivo. La diferencia entre los valores T es de 3 minutos.

```
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
```

Paso 2. Análisis de SMA trackerd_logs

Basándose en la información obtenida en el paso 1, verifique **/data/pub/trackerd_logs** en SMA para encontrar y confirmar los archivos de datos perdidos en la sección **Problema**.

En este marco se describen las muestras de registro relevantes con resultados. Registros rastreados filtrados en SMA solo para el primer 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
```

Paso 3. Análisis de acciones de smaduser

El siguiente paso es verificar el comportamiento de SMA **smad** en /data/pub/cli_logs/ de ESA.

Como se mencionó smad verifica los archivos de ESA en /data/pub/export/tracking (ls -AF), copia el archivo (scp -f /../tracking.*.s.gz) y luego lo elimina (rm /../tracking.*.s.gz) por **smaduser** a través del acceso **SSH**.

En este paso se ha identificado que hay otro SMA (IP: 192.168.251.92) que el SMA principal (IP:

172.24.81.94) se conecta a las descargas ESA y elimina el archivo antes del SMA principal.

Cuando el SMA principal verifica los archivos en el directorio (ls -AF), no puede ver el archivo porque ya ha sido eliminado por 192.168.251.92 smaduser.
El ejemplo de registro pertinente es el siguiente:

```
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
```

Resumen de soluciones

El seguimiento del propio proceso de Rastreo de mensajes ayudó a superar el problema con éxito.
A través de cli_logs en ESA se ha identificado otro SMA. Se conecta al ESA, extrae y luego elimina el archivo antes del SMA principal. El archivo deja de estar disponible para el SMA principal.

Elimine los ESA/desactive los servicios ESA en los 'dispositivos de seguridad' SMA redundantes o retire completamente de la producción el SMA redundante.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).