

Entender e solucionar problemas de intervalos de dados de 3 minutos ausentes no rastreamento de mensagens do SMA

Contents

Introdução

Este documento descreve o motivo e como solucionar problemas de dados de rastreamento de mensagem ausentes com intervalos de dados de intervalo de 3 minutos no SMA.

Requisitos

Conhecimento destes tópicos:

- Cisco Security Management Appliance (SMA)
- Dispositivo de segurança de e-mail (ESA) da Cisco
- Rastreamento de mensagem centralizado

Componentes Utilizados

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Problema

O SMA encontra intervalos de dados ausentes de 3 minutos nos 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)	

Solução

Fluxo de trabalho do resumo de rastreamento de mensagem local e centralizado

O rastreamento funciona em dois modos:

I. Rastreio local da ESA.

1. Trackerd analisa dados de informações de rastreamento arquivos de log binários processados por qlogd (tracking.@*.s)
2. Trackerd salva-o sob o palheiro.

II. Rastreamento centralizado ESA.

1. qlogd grava as informações de rastreamento nos arquivos de log binários (tracking.@*.s.gz) no diretório /data/pub/export/tracking
2. O processo smad do SMA verifica, obtém e exclui os dados brutos de rastreamento (tracking.@*.s.gz) do diretório /data/pub/export/tracking do ESA.
3. Os arquivos de rastreamento extraídos dos ESAs são salvos no diretório /data/log/tracking/<ESA_IP>/ do SMA.
4. Trackerd move arquivos para o diretório /data/tracking/incoming_queue/0/<ESA_IP>, processa arquivos.
5. Arquivos processados armazenados no banco de dados MT e arquivos de rastreamento são removidos.

Etapas da investigação

Etapa 1. Análise de registros rastreados ESA

Depois de observar a pasta `trackerd_logs` in `/data/pub/trackerd_logs/`, identificou que geralmente `qlogd` no ESA grava arquivos de dados de rastreamento de intervalo de 3 minutos.

Neste exemplo, os arquivos de dados na pasta `/data/pub/export/tracking/ T*` parte do nome do arquivo representa o tempo gerado pelo arquivo. A diferença entre os valores `T` é 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
```

Etapa 2. Análise de `trackerd_logs` do SMA

Com base nas informações obtidas na etapa 1, verifique `/data/pub/trackerd_logs` no SMA para descobrir e confirmar arquivos de dados perdidos na seção **Problema**.

As amostras de log relevantes com resultados são descritas neste quadro. Logs rastreados filtrados no SMA somente para o primeiro 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: Tra
```

Etapa 3. Análise de ações `smaduser`

A próxima etapa é verificar o comportamento do `smad` do SMA em `/data/pub/cli_logs/` do ESA.

Como mencionado, o `smad` verifica os arquivos do ESA em `/data/pub/export/tracking` (`ls -AF`), copia o arquivo (`scp -f ../tracking.*.s.gz`) e depois o remove (`rm ../tracking.*.s.gz`) pelo `smaduser` através do acesso **SSH**.

Nesta etapa, foi identificado que há outro SMA (IP: 192.168.251.92) que o SMA principal (IP: 172.24.81.94) se conecta aos downloads do ESA e remove o arquivo antes do SMA principal.

Quando o SMA principal verifica se há arquivos no diretório (`ls -AF`), ele não pode ver o arquivo, pois ele já foi removido por 192.168.251.92 `smaduser`.

A amostra de registro relevante é a seguinte:

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

Resumo da solução

O rastreamento do próprio processo de Rastreamento de Mensagens ajudou a superar o problema com êxito.

Por meio de cli_logs no ESA, outro SMA foi identificado. Ele se conecta ao ESA, obtém e remove o arquivo antes do SMA principal. O arquivo fica indisponível para o SMA principal.

Remova ESAs/desative os serviços ESA em "dispositivos de segurança" SMA redundantes ou desative o SMA redundante completamente da produção.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.