

SMAメッセージトラッキングで3分間のデータインターバルが表示されない場合の説明とトラブルシューティング

内容

はじめに

このドキュメントでは、SMAの3分間の範囲データ間隔でメッセージトラッキングデータ(MDT)が欠落している場合のトラブルシューティングの理由と方法について説明します。

要件

次の項目に関する知識

- Cisco セキュリティ管理アプライアンス (SMA)
- Cisco Email Security Appliance (ESA)
- 一元化されたメッセージトラッキング

使用するコンポーネント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

問題

SMAは、ESAアプライアンスから3分のデータ欠落インターバルを多数検出します。

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)	

解決方法

ローカルおよび集中型のメッセージトラッキングの簡単なワークフロー

トラッキングは、次の2つのモードで動作します。

I. ESAローカルトラッキング

1. trackerdは、qlogdによって処理されたトラッキング情報バイナリログファイルからデータを解析します(tracking.@*.s)
2. trackerdは/data/db/reporting/haystackの下に保存します。

II. ESA中央集中型トラッキング

1. qlogdはトラッキング情報バイナリログファイル(tracking.@*.s.gz)を/data/pub/export/trackingディレクトリに書き出します
2. SMA smadプロセスは、ESAの/data/pub/export/trackingディレクトリから追跡未加工データ(tracking.@*.s.gz)をチェック、プル、削除します。
3. ESAからプルされたトラッキングファイルは、SMAの/data/log/tracking/<ESA_IP>/ディレクトリに保存されます。
4. trackerdは/data/tracking/incoming_queue/0/<ESA_IP>ディレクトリにファイルを移動し、ファイル进行处理します。
5. MTデータベースに保存されている処理済みファイルとトラッキングファイルは削除されます

。

調査手順

ステップ 1 : ESA trackerd_logsの分析

/data/pub/trackerd_logs/フォルダのtrackerd_logsを観察した後、ESAのqlodgが通常3分の間隔追跡データファイルを書き込むことを特定しました。

この例では、filenameのフォルダ/data/pub/export/tracking/ T*部分のデータファイルが、ファイルの生成時刻を表しています。T値の差は3分です。

```
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
```

ステップ 2 : SMA trackerd_logs分析

ステップ1で取得した情報に基づいて、SMAの/data/pub/trackerd_logsを確認し、「問題」セクションで欠落したデータファイルを見つけて確認します。

このフレームでは、結果を含む関連するログサンプルについて説明します。最初のESA(192.168.235.64)に対してのみSMAでtrackerd_logsをフィルタ処理：

```
/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
```

ステップ 3 : smaduserアクションの分析

次のステップは、ESAの/data/pub/cli_logs/でのSMA smadの動作を確認することです。

前述のように、smadは/data/pub/export/tracking (ls -AF)内のESAのファイルをチェックし、ファイル(scp -f ../tracking.*.s.gz)をコピーしてから、smaduserによってSSHアクセスを介して削除します。

この手順では、メインSMA(IP:172.24.81.94)以外の別のSMA(IP:192.168.251.92)がESAのダウンロードに接続し、メインSMAの前にファイルを削除することが確認されています。

メインSMAがディレクトリ(ls -AF)内のファイルをチェックする際に、192.168.251.92 smaduserによってすでに削除されているため、ファイルが表示されません。関連するログの例を次に示します。

```
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
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
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/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/tracking
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/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/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 to

ソリューションの概要

メッセージ追跡プロセス自体のトレースは、問題を正常に解決するのに役立ちました。
ESAのcli_logsを使用して、別のSMAが特定されました。ESAに接続し、メインSMAの前にファイルをプルして削除します。メインSMAでファイルが使用できなくなります。

冗長SMA「セキュリティアプライアンス」でESAを削除またはESAサービスを無効にするか、冗長SMAを完全に運用状態から切り離します。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。