Ontbrekende 3-minuten bereik data-intervallen op SMA Message Tracking begrijpen en problemen oplossen

Inhoud

Inleiding

Dit document beschrijft de reden en de manier om problemen op te lossen met ontbrekende Message Tracking Data met 3 minuten bereik data intervallen op SMA.

Vereisten

Kennis van deze onderwerpen:

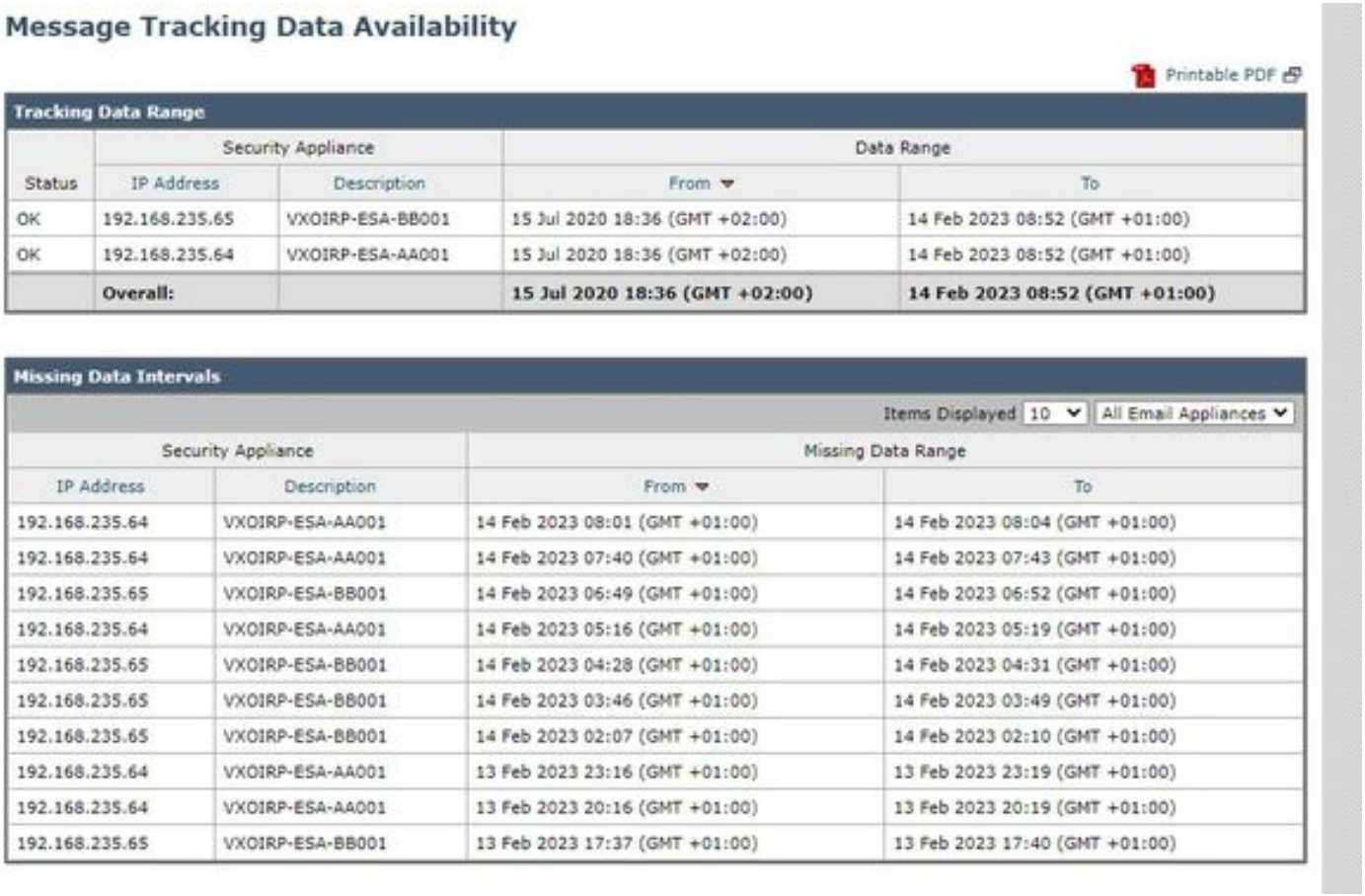
- Cisco Security Management-applicatie (SMA)
- Cisco e-mail security applicatie (ESA)
- Gecentraliseerde tracering van berichten

Gebruikte componenten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Probleem

SMA komt veel 3 minuten ontbrekende data-intervallen van ESA-apparaten tegen.



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)

Oplossing

Lokale en gecentraliseerde korte werkstroom voor het volgen van berichten

Het volgen werkt in twee modi:
I. lokale tracering van het ESA.
1. Trackerd parseert gegevens van het bijhouden van informatie binaire logbestanden die zijn verwerkt door qlogd (tracking.@*.s)

2. Trackerd slaat het op onder hooiberg.

II. Gecentraliseerde tracering van het ESA.
1. qlogd schrijft trackinginformatie binaire logbestanden (tracking.@*.s.gz) in de directory /data/pub/export/tracking
2. SMA verstuurde procescontroles, pulls, en verwijdert dan de tracking ruwe gegevens (tracking.@*.s.gz) uit de /data/pub/export/tracking directory van ESA.
3. Gepulseerde tracking-bestanden van ESA's worden opgeslagen op /data/log/tracking/<ESA_IP>/ directory van SMA.
4. Trackerd verplaatst bestanden naar /data/tracking/inkomende_wachtrij/0/<ESA_IP> directory, verwerkt bestanden.
5. Verwerkte bestanden die zijn opgeslagen in MT-database en tracking-bestanden worden verwijderd.

Onderzoeksstappen

Stap 1. ESA trackerd_logs Analyse

Na het waarnemen van trackerd_logs in /data/pub/trackerd_logs/folder, identificeerde dat over het algemeen qlogd op ESA 3-minuten interval tracking data bestanden.

In dit voorbeeld representeren gegevensbestanden in map/data/pub/export/tracking/ T* deel van filename de gegenereerde tijd van het bestand. Het verschil tussen de T-waarden bedraagt 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
```

Stap 2. SMA trackerd_logs Analyse

Op basis van informatie die is verkregen in stap 1, check /data/pub/trackerd_logs op SMA om gemiste gegevensbestanden te vinden en te bevestigen in de sectie Probleem.

Relevante logmonsters met resultaten worden in dit kader beschreven. Gefilterde trackerd_logs op SMA alleen voor eerste 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 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
```

Stap 3. Analyse van smaduser Acties

De volgende stap is het controleren van SMA smad gedrag op /data/pub/cli_logs/ van ESA.

Zoals vermeld smad controleert bestanden van ESA in /data/pub/export/tracking (ls -AF), kopieert bestand (scp -f /../tracking.*.s.gz) en verwijdert het vervolgens (rm /.../tracking.*.s.gz) door smaduser via de SSH toegang.

In deze stap is vastgesteld dat er een andere SMA (IP: 192.168.251.92) dan de hoofdSMA (IP: 172.24.81.94) verbinding maakt met ESA downloads en het bestand verwijdert voor de hoofdSMA.

Wanneer de SMA bestanden in map (ls -AF) controleert, kan het bestand niet zien zoals het al is verwijderd door 192.168.251.92 smaduser.
Relevante logmonsters zijn als volgt:

```
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
```

Samenvatting van oplossing

Het overtrekken van het proces van het Traceren van het Bericht zelf hielp om het probleem met succes te overwinnen.
Via cli_logs op ESA is een andere SMA geïdentificeerd. Het verbindt met ESA, trekt en verwijdert dan het bestand voor de hoofdSMA. Het bestand is niet beschikbaar voor de SMA.

ESA’s verwijderen / ESA-services uitschakelen op redundante SMA 'Security applicaties' of redundante SMA volledig uit productie nemen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.