Comprendre et dépanner les intervalles de données manquants de 3 minutes sur le suivi des messages SMA

Table des matières

Introduction

Ce document décrit la raison et la façon de dépanner les données de suivi des messages manquantes avec des intervalles de données de plage de 3 minutes sur SMA.

Exigences

Connaissance de ces sujets :

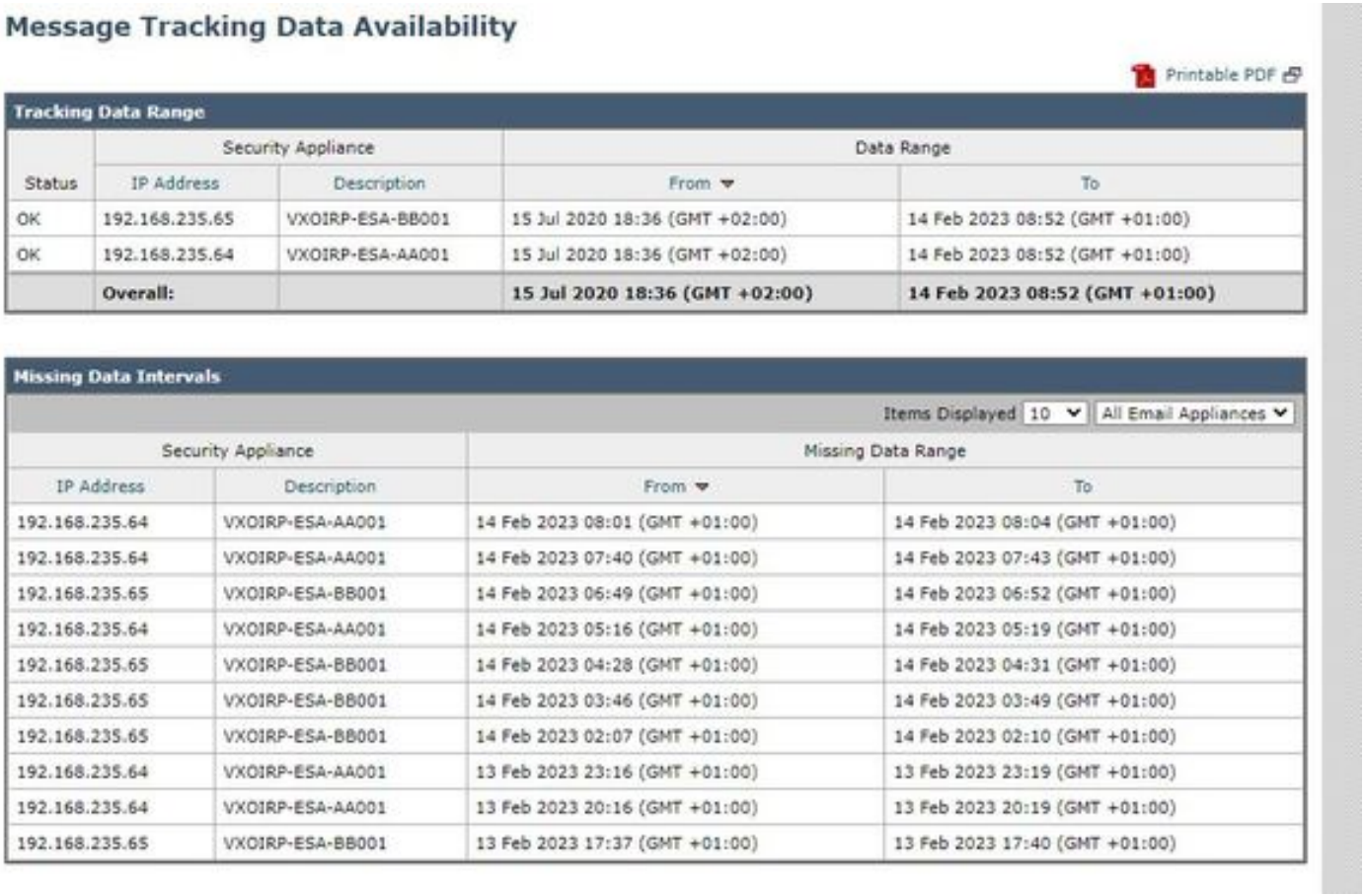
- Appliance de gestion de la sécurité Cisco (SMA)
- Appliance de sécurisation de la messagerie Cisco (ESA)
- Suivi centralisé des messages

Composants utilisés

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Problème

SMA détecte de nombreux intervalles de données manquants de 3 minutes dans les appliances 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)

Solution

Workflow de suivi des messages local et centralisé

Le suivi fonctionne selon deux modes :
I. Suivi local ESA.
1. Trackerd analyse les données des fichiers journaux binaires d'informations de suivi traités par qlogd (tracking.@*.s)

2. Trackerd l'enregistre dans /data/db/reporting/haystack.

II. Suivi centralisé ESA.
1. qlogd écrit les fichiers journaux binaires d'informations de suivi (tracking.@*.s.gz) dans le répertoire /data/pub/export/tracking
2. SMA smad process vérifie, extrait, puis supprime les données brutes de suivi (tracking.@*.s.gz) du répertoire /data/pub/export/tracking de ESA.
3. Les fichiers de suivi extraits des ESA sont enregistrés dans le répertoire /data/log/tracking/<ESA_IP>/ de SMA.
4. Trackerd déplace les fichiers vers le répertoire /data/tracking/incoming_queue/0/<ESA_IP>, traite les fichiers.
5. Les fichiers traités stockés dans la base de données MT et les fichiers de suivi sont supprimés.

Étapes d'investigation

Étape 1. Analyse ESA trackerd_logs

Après avoir observé trackerd_logs dans /data/pub/trackerd_logs/ dossier, identifié que généralement qlogd sur ESA écrit des fichiers de données de suivi d'intervalle de 3 minutes.

Dans cet exemple, les fichiers de données du dossier /data/pub/export/tracking/ T* partie du nom de fichier représente l'heure de génération du fichier. La différence entre les valeurs T est de 3 minutes.

```
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
```

Étape 2. Analyse de trackerd_logs SMA

En fonction des informations obtenues à l'étape 1, vérifiez **/data/pub/trackerd_logs** sur SMA afin de découvrir et de confirmer les fichiers de données manqués dans la section **Problem**.

Les échantillons de log pertinents avec les résultats sont décrits dans cette trame. Trackerd_logs filtrés sur SMA uniquement pour le premier 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
```

Étape 3. Analyse des actions des utilisateurs intelligents

L'étape suivante consiste à vérifier le comportement de SMA **smad** sur /data/pub/cli_logs/ de ESA.

Comme mentionné, smad recherche les fichiers de ESA dans /data/pub/export/tracking (ls -AF), copie le fichier (scp -f /../tracking.*.s.gz) puis le supprime (rm /../tracking.*.s.gz) par **smaduser** via l'accès **SSH**.

Dans cette étape, il a été identifié qu'il y a un autre SMA (IP : 192.168.251.92) que le SMA principal (IP : 172.24.81.94) se connecte aux téléchargements ESA et supprime le fichier avant le SMA principal.

Lorsque le SMA principal recherche des fichiers dans le répertoire (ls -AF), il ne peut pas voir le fichier car il a déjà été supprimé par 192.168.251.92 smaduser.
L'exemple de journal pertinent est le suivant :

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

Résumé de la solution

Le suivi du processus de suivi des messages lui-même a permis de résoudre le problème.
Via cli_logs sur ESA, un autre SMA a été identifié. Il se connecte à ESA, extrait puis supprime le fichier avant le SMA principal. Le fichier devient indisponible pour le SMA principal.

Supprimez les ESA / désactivez les services ESA sur les « appliances de sécurité » SMA redondants ou désactivez complètement les SMA redondants de la production.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.