فهم الفواصل الزمنية المفقودة لبيانات النطاق لمدة 3 دقائق واستكشاف أخطائها وإصلاحها على تعقب رسائل SMA

المحتويات

المقدمة

يوضح هذا المستند السبب وكيفية أستكشاف أخطاء بيانات تعقب الرسائل المفقودة وإصلاحها من خلال فواصل بيانات النطاق التي تبلغ 3 دقائق على SMA.

المتطلبات

معرفة هذه الموضوعات:

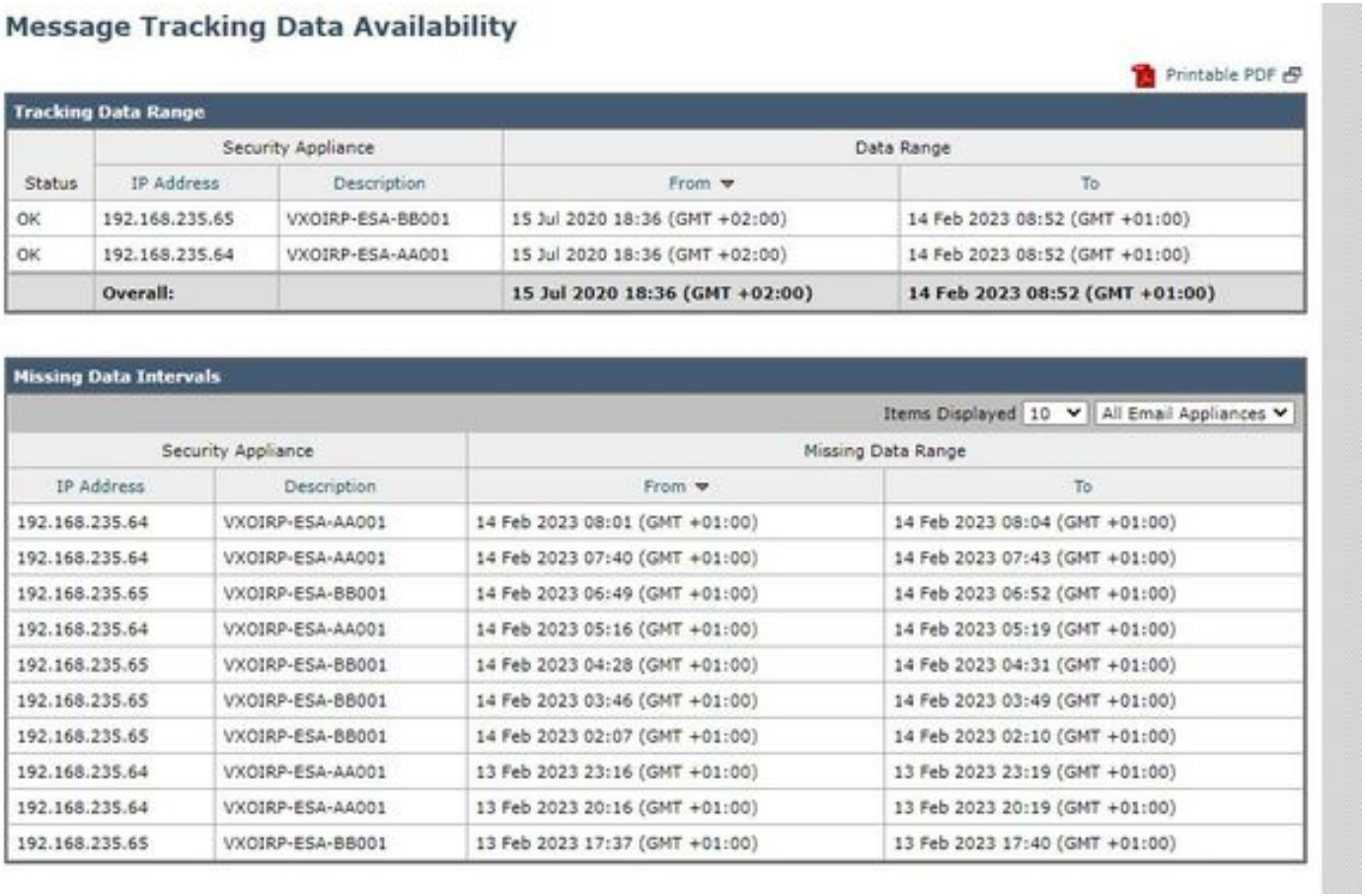
- أجهزة إدارة الأمان (SMA) من Cisco
- أجهزة أمان البريد الإلكتروني Cisco Email Security Appliance (ESA)
- تعقب الرسائل مركزيا

المكونات المستخدمة

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

المشكلة

تفتقد SMA فواصل بيانات كثيرة مدتها 3 دقائق من أجهزة 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)

الحل

سير عمل موجز لتتبع الرسائل المحلي والمركزي

يعمل التعقب في وضعين:
أولا - التتبع المحلي لكل قضاء الأوروبية.
1. يحلل Trackerd البيانات من تتبع ملفات السجلات الثنائية للمعلومات التي تمت معالجتها بواسطة QLOGD (التعقب.@*.s)

2. يقوم Trackerd بحفظه تحت /data/db/reporting/hestack.

ثانيا - التتبع المركزي لكل قضاء الأوروبية.
1. يقوم QLOGD بتتبع ملفات السجل الثنائية للمعلومات (التعقب@*.s.gz) في دليل /data/pub/export/tracking
2. تقوم SMA بفحص العملية وتسريحها ثم تقوم بحذف بيانات التعقب الأولية (التعقب@*.s.gz) من /data/pub/export/tracking directory الخاص بالإيسا.
3. يتم حفظ ملفات التتبع المسحوبة من ESAs على /data/log/tracking/<ESA_IP>/ دليل SMA.
4. يقوم Trackerd بنقل الملفات إلى دليل /data/tracking/incoming_queue/0/<ESA_IP>، ومعالجة الملفات.
5. تتم إزالة الملفات المعالجة المخزنة في قاعدة بيانات MT وملفات التعقب.

خطوات التحقيق

الخطوة 1. تحليل ESA Trackerd_LOG

بعد مراقبة Trackerd_log in /data/pub/trackerd_log/folder، تم تحديد أن Qlogd على ESA يكتب ملفات بيانات تعقب الفاصل الزمني بمقدار 3 دقائق.

في هذا المثال، تم تمثيل ملفات البيانات في المجلد /البيانات/pub/export/tracking/T* جزء من اسم الملف الوقت الذي تم إنشاؤه للملف. الفرق بين قيم T هو 3 دقائق.

```
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
```

الخطوة 2. تحليل SMA Trackerd_LOG

استنادا إلى المعلومات التي تم الحصول عليها في الخطوة 1، تحقق من **/data/pub/trackerd_log** في SMA لمعرفة ملفات البيانات التي تم فقدها وتأكيدها في قسم المشاكل.

يتم وصف نماذج السجل ذات الصلة بالنتائج في هذا الإطار. Trackerd_log الذي تمت تصفيته على SMA فقط ل ESA الأول (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
```

الخطوة 3. تحليل إجراءات المستخدم

تتمثل الخطوة التالية في التحقق من سلوك **SMA** SMAD على /data/pub/cli_log/ الخاص ب ESA.

كما ذكر، إذا عمليات فحص SMAD للملفات ESA في /data/pub/export/tracking (ls -af)، تنسخ الملف (scp -f /../tracking.*.s.gz) ثم تزيله (rm /../tracking.*.s.gz) بواسطة **smaduser** عبر وصول **SSH**.

في هذه الخطوة تم تحديد وجود SMA آخر (IP: 192.168.251.92) من اتصال SMA الرئيسي (IP: 172.24.81.94) ب ESA ويزيل الملف قبل SMA الرئيسي.

عندما يتحقق SMA الرئيسي من الملفات الموجودة في الدليل (ls -AF)، لا يمكنه رؤية الملف لأنه تمت إزالته بالفعل بواسطة 192.168.251.92 smaduser.
عينة السجل ذات الصلة هي كما يلي:

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

ملخص الحل

وقد ساعد تعقب عملية تعقب الرسائل نفسها في التغلب على المشكلة بنجاح.
من خلال CLI_LOG على ESA، تم تحديد SMA أخرى. تتصل ب ESA، وتسحب الملف ثم تقوم بإزالته قبل SMA الرئيسي.
يصبح الملف غير متاح ل SMA الرئيسي.

قم بإزالة خدمات ESA / تعطيل خدمات ESA على "أجهزة الأمان" SMA الزائدة وأ "SMA" الزائدة عن الحاجة الخاصة بتفكيك العمليات بالكامل من الإنتاج.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).