لماذا توجد أخطاء في الشبكة عند اتصال ESA بخادم syslog؟

المحتويات

المقدمة

يوضح هذا المستند سبب عدم قدرة جهاز أمان البريد الإلكتروني (ESA) على إرسال البيانات إلى خادم syslog.

لماذا توجد أخطاء في الشبكة عند اتصال ESA بخادم syslog؟

تم تكوين ESA لدفع اشتراكات السجل إلى خادم syslog. **قد يتم دفع الملفات بنجاح إلى خادم syslog وقد لا يتم ذلك.** على أي حال، يمكن أن تكون هناك أخطاء في الشبكة في ملف سجل البريد مشابهة لهذا:

```
Log Error: Subscription Mail_Log: Network error while sending log data
to syslog server
```

يظهر التقاط حزمة بين ESA وخادم syslog عمليات إسقاط اتصال تم بدؤها بواسطة خادم syslog، وهو في هذا المثال 10.44.167.30.

o.	Time	Source	Destination	Protocol	Info
278	2015-06-25 08:50:04.111689	10.229.24.230	10.44.167.30	TCP	26040 > shell [SYN] Seq=0 Win=16384 Len=0 MSS=1460 WS=8 SACK_P
279	2015-06-25 08:50:04.114360	10.44.167.30	10.229.24.230	TCP	shell > 26040 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1350
280	2015-06-25 08:50:04.114375	10.229.24.230	10.44.167.30	TCP	26040 > shell [ACK] Seq=1 Ack=1 Win=17550 Len=0
281	2015-06-25 08:50:04.114518	10.229.24.230	10.44.167.30	RSH	Client -> Server data
282	2015-06-25 08:50:04.114877	10.44.167.30	10.229.24.230	TCP	shell > 26040 [ACK] Seq=1 Ack=48 Win=32073 Len=0
283	2015-06-25 08:50:04.114883	10.229.24.230	10.44.167.30	RSH	Client -> Server data
284	2015-06-25 08:50:04.115362	10.44.167.30	10.229.24.230	TCP	shell > 26040 [ACK] Seq=1 Ack=413 Win=31755 Len=0
285	2015-06-25 08:50:04.116192	10.44.167.30	10.229.24.230	TCP	shell > 26040 [RST, ACK] Seq=1 Ack=413 Win=32120 Len=0

إذا اتبعت تدفق TCP في التقاط الحزمة فسترى ما يلي:

```
Jun 25 08:50:03 example.com: Info: Begin Logfile<22>
Jun 25 08:50:03 example.com: Info: Version: 8.0.1-023 SN: A4BADB4712A9-511AA1E<22>
Jun 25 08:50:03 example.com: Info: Time offset from UTC: 7200 seconds<22>
Jun 25 08:50:03 example.com: Info: A System/Critical alert was sent to<22>
:alerts@ironport.com with subject "Critical <System> mail.example.com: Log Error
."...Subscription Mail_Log: Network error while sending l
```

تشير الأخطاء إلى وجود جدار حماية أو نظام منع التسلل (IPS) يمنع الوصول إلى خادم syslog على عنوان IP. إذا كان قد تم فحص جميع الأجهزة التي تقع بين السطور وتأكيدها للسماح بحركة المرور، فقد يعني ذلك أيضا أن خادم syslog مشغول جدا ويرفض الاتصالات. عندما ال ESA يكون شكلت أن يرسل سجل مبرد إلى syslog نادل، بعد ذلك افتراضيا هو يستعمل ال udp syslog ميناء 514 ما لم يشكل أن يستعمل TCP. بمجرد تكوين الجهاز، فإن الشيء الوحيد الذي يتسبب في إدراج الاتصال كمرفوض هو إذا كان يستلم حزم تغلق الاتصال عند فتحه.

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).