دليل أستكشاف أخطاء ASA وإصلاحها: السجلات المفقودة في وجهة (وجهات) Syslog

المحتويات

المقدمة

يوضح هذا المستند كيفية أستكشاف المشكلة وحلها مع قدرة جهاز الأمان القابل للتكيف (ASA) على إرسال syslog إلى وجهات مختلفة، وبشكل أكثر تحديدا، المشكلات التي يتم فيها ملاحظة الأعراض مثل هذه:

- برنامج ASDM (Adaptive Security Device Manager) لتسجيل الدخول في الوقت الفعلي البطيء.
- Syslog المتقطعة مفقودة في واحد أو أكثر من وجهات syslog.

قبل البدء

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

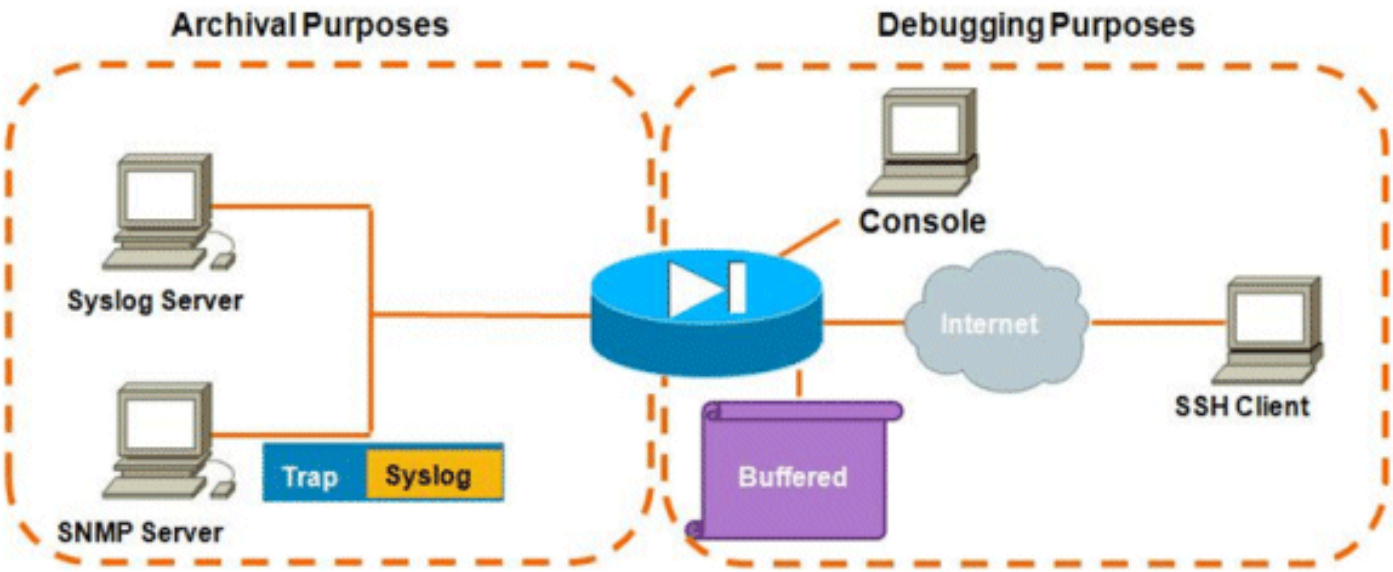
تستند المعلومات الواردة في هذا المستند إلى Cisco ASA ولا يقتصر على إصدار برنامج ASA محدد.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

معلومات الميزة

يكون ASAs، مثل معظم أجهزة Cisco الأخرى، قادر على إرسال syslog إلى وجهات syslog متعددة. ويتم توضيح بعض الوجهات الأكثر إستخداما هنا:



عدد الوجهات الممكنة هو ميزة حقيقية. وإذا أختيرت بعناية، وكما هو موضح هنا، يمكن تصنيفها عموما في فئتين رئيسيتين على أساس الغرض الذي تخدمه:

- أرشيفال
- تصحيح الأخطاء/أستكشاف الأخطاء وإصلاحها في الوقت الفعلي

في معظم الشبكات، يكفي أن يتم تمكين وجهات الأرشفة فقط إلا إذا كان واحد أو أكثر من وجهات تصحيح الأخطاء ضروريا. وفي الوقت نفسه، وفي كثير من الأحيان، تنشأ المشاكل من تمكين وجهات syslog المتعددة في آن واحد على مستويات تسجيل عالية مثل المعلومات (المستوى 6) أو أعلى.

منهجية أستكشاف الأخطاء وإصلاحها

كلما حدثت مشاكل حيث هناك فقد لمعلومات syslog في واحد أو أكثر من الوجهات، هناك أمران يجب عليك فحصهما:

- راجع تكوين syslogging (إخراج تسجيل تشغيل العرض).
- راجع إخراج قائمة انتظار التسجيل show.

تحليل البيانات

راجعت ال syslogging تشكيل

أكمل الخطوات التالية:

1. تأكد من أن رسالة syslog التي تبحث عنها غير معطلة بواسطة الأمر **no logging message *<id>***.
2. وبمجرد تأكيدها، راجع عدد وجهات syslog الممكنة والمستوى الذي يتم فيه إرسال كل سجل إلى كل منها. هذا مثال من هذا تشكيل:

```
logging enable
logging timestamp
logging standby
logging console informational
logging buffered informational
logging trap informational
logging asdm informational
```

```
logging device-id hostname
logging host inside 172.16.110.32
```

في هذا مثال، ال ASA يرسل syslogs إلى 4 غاية مختلف على المستوى المعلوماتي (مستوى 6).

إخراج قائمة انتظار show logging

باستخدام تكوين مثل المذكور أعلاه، حيث تتلقى وجهات متعددة كميات كبيرة من رسائل السجل، يمكنك مواجهة حالة يقوم فيها ASA بإسقاط رسائل syslog بسبب تجاوز قائمة انتظار التسجيل. في مثل هذه الحالات، سيظهر الإنتاج مماثل ل:

```
ciscoasa# show logging queue

(Logging Queue length limit : 512 msg(s
msg(s) discarded due to queue overflow 2352325
msg(s) discarded due to memory allocation failure 0
Current 512 msg on queue, 512 msgs most on queue
```

بشكل افتراضي، تحمل قائمة انتظار التسجيل 512 رسالة.

مشاكل مشتركة

عند الدخول في مشاكل لا يتم فيها تسجيل رسائل syslog، ضع في الاعتبار الخيارات التالية:

- تعطيل تسجيل وحدة التحكم. **يجب عدم** تمكين تسجيل الدخول إلى وحدة التحكم للتشغيل العادي. يجب إستخدام تسجيل وحدة التحكم فقط لاستكشاف الأخطاء وإصلاحها في الوقت الفعلي، مع مستوى تسجيل منخفض أو حركة مرور منخفضة. سيؤدي تسجيل الدخول إلى وحدة التحكم بمعدل مرتفع إلى جعل عملية التسجيل تؤدي إلى تحديد معدل الرسائل بشكل كبير. وحدة التحكم قادرة فقط على تسجيل الرسائل بسرعة 9600 بت في الثانية، ولا تأخذ مجموعة من السجلات قبل أن تبدأ في محاولة تفريغ المزيد إلى وحدة التحكم مما يمكن لوحدة التحكم إخراجه إلى الشاشة. في هذه الحالة، سيبدأ تخزين السجلات مؤقتا في قائمة انتظار التسجيل. بمجرد تعبئة قائمة انتظار التسجيل، سيتم إسقاط الرسائل من الخلف.
- قم بزيادة حجم قائمة انتظار التسجيل إلى ما بعد 512. الحد الأقصى لقائمة انتظار التسجيل هو 1024 على ASA-5505، و 2048 على ASA-5510، و 8192 على جميع الأنظمة الأساسية الأخرى. ملاحظة: يتم إستخدام قائمة انتظار التسجيل ل "دفعات" من syslog. إذا كان المعدل المستمر لسلاسل syslog أسرع من معدل ASA الذي يمكنه إرسالها إلى الوجهات المختلفة، فلن يكون أي حد لقائمة انتظار التسجيل كبيرا بشكل كاف.
- قم بتعطيل رسائل syslog الفردية التي لا ترغب في أرشفتها. قم بإصدار الأمر no logging message *<<syslog_id* لتعطيل syslog الفردية.
- احذر من تسجيل الرسائل إلى قرص (flash) من ال ASA. الكتابة إلى البرق عملية بطيئة جدا. سيتسبب التسجيل الزائد إلى ذاكرة Flash (الذاكرة المؤقتة) في قيام ASA بتخزين ملفات syslog مؤقتا في الذاكرة، وبالتالي إستنزاف جميع الذاكرة المتاحة (RAM). وبالإضافة إلى ذلك، قد يؤدي تسجيل كميات كبيرة من رسائل syslog إلى ذاكرة Flash (الذاكرة المؤقتة) إلى رفع وحدة المعالجة المركزية. يوصى بتسجيل رسائل المستوى 1 فقط إلى ذاكرة Flash (التي تغطي أحداث النظام الهامة).

معلومات ذات صلة

- الدعم التقني والمستندات - Cisco Systems

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).