ASA故障排除指南：系统日志目标处缺少日志

目录

简介

本文档介绍如何解决自适应安全设备(ASA)向各种目标发送系统日志的功能问题，更具体地说，如何发现这些症状：

- 自适应安全设备管理器(ASDM)上的慢实时日志记录。
- 一个或多个系统日志目标上缺少间歇性系统日志。

开始使用前

要求

本文档没有任何特定的要求。

使用的组件

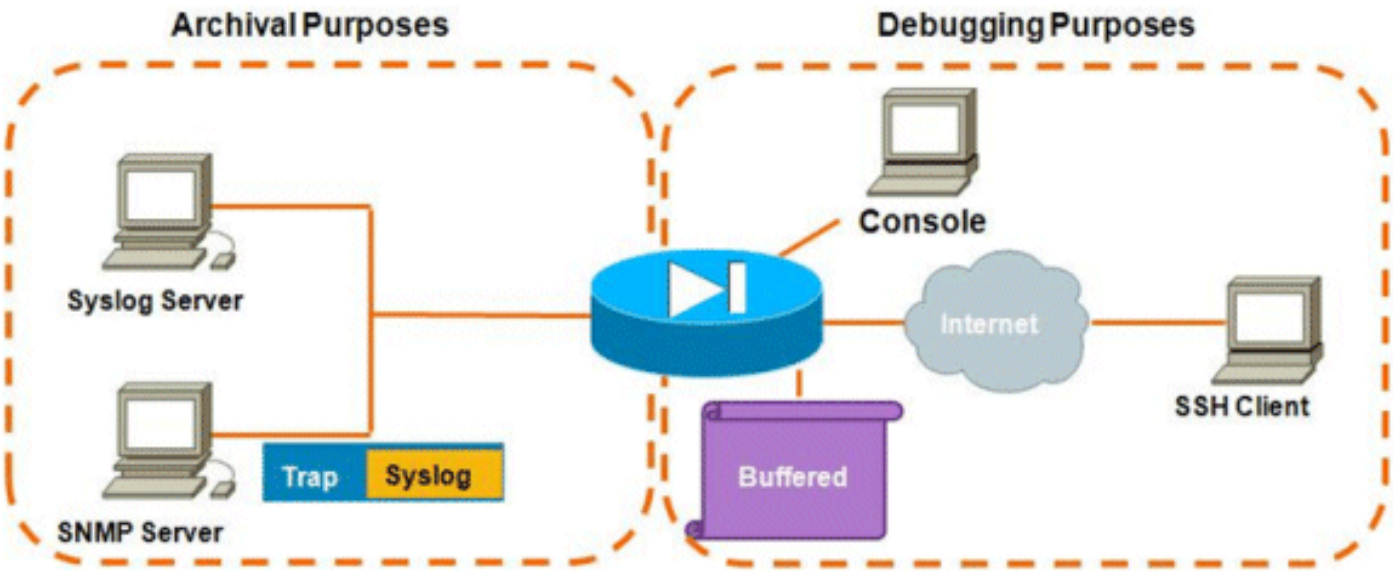
本文档中的信息基于Cisco ASA，并且不限于特定ASA软件版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

功能信息

ASA与大多数其他思科设备一样，能够将系统日志发送到多个系统日志目标。以下是一些更常用的目的地：



可能的目的地数量是一个真正的优势。如果选择得当，并且如下所示，根据其服务目的，它们大致可分为两大类：

- 存档
- 实时调试/故障排除

在大多数网络中，只启用存档目标就足够了，除非需要一个或多个调试目标。同时，在信息（第6级）或更高级别上同时启用多个系统日志目标会导致问题。

故障排除方法

当在一个或多个目的地丢失系统日志信息时，应检查以下两项：

- 查看syslogging配置(show run logging**的输出**)。
- 查看show logging queue**的输出**。

数据分析

查看Syslogging配置

请完成以下步骤：

1. 确保您正在查找的系统日志消息未被no logging message**<ID>命令禁**用。
2. 确认后，查看启用的系统日志目标数量以及将每个日志发送到每个日志的级别。以下是此类配置的示例：

```
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
```

在本示例中，ASA在信息级别（6级）将系统日志发送到4个不同的目标。

show logging queue的输出

在上述配置中，多个目标正在接收大量日志消息，您可能会遇到ASA由于日志队列溢出而丢弃系统日志消息的情况。在这种情况下，输出将如下所示：

```
ciscoasa# show logging queue

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

默认情况下，日志记录队列包含512条消息。

常见问题

当遇到系统日志消息未被记录的问题时，请考虑以下选项：

- 禁用控制台日志记录。不应为正常操**作启**用登录控制台。控制台日志记录应仅用于实时故障排除，具有低日志记录级别或低流量。以高速率登录控制台将导致日志记录过程严重限制消息速率。控制台仅能以9600 bps的速率记录消息，并且它在开始尝试将更多的日志转储到控制台之前，不需要花费太多的日志，而控制台可以输出到屏幕。在这种情况下，日志将开始在日志记录队列中缓冲。一旦日志记录队列满，消息将被尾部丢弃。
- 将日志记录队列的大小增加到512以上。在ASA-5505上，最大日志记录队列为1024，在ASA-5510上，最大日志记录队列为2048，在所有其他平台上，最大日志记录队列为8192。注意：日志记录队列用于系统日志的“突发”。如果系统日志的持续速率比ASA可以将其传输到不同目的地的速度快，则日志记录队列限制将不会足够大。
- 禁用您对存档不感兴趣的单个系统日志消息。发出no logging message *<syslog_id>*命令以禁用单个系统日志。
- 请注意将消息记录到ASA的磁盘（闪存）。写入闪存操作非常慢。过多的闪存日志记录将导致ASA将系统日志文件缓冲到内存中，最终耗尽所有可用内存(RAM)。 此外，将大量系统日志消息记录到闪存中可能会提高CPU。建议仅将第1级消息记录到闪存（涵盖关键系统事件）。

相关信息

- 技术支持和文档 - Cisco Systems