ASA Troubleshooting Guide: Missing Logs at Syslog Destination(s)

Contents

Introduction

This document describes how to troubleshoot the problem with the capability of the Adaptive Security Appliance (ASA) to send syslogs to various destinations, and, more specifically, issues where symptoms such as these are observed:

- Slow real-time logging on Adaptive Security Device Manager (ASDM).
- Intermittent syslogs missing at one or more syslog destinations.

Before You Begin

Requirements

There are no specific requirements for this document.

Components Used

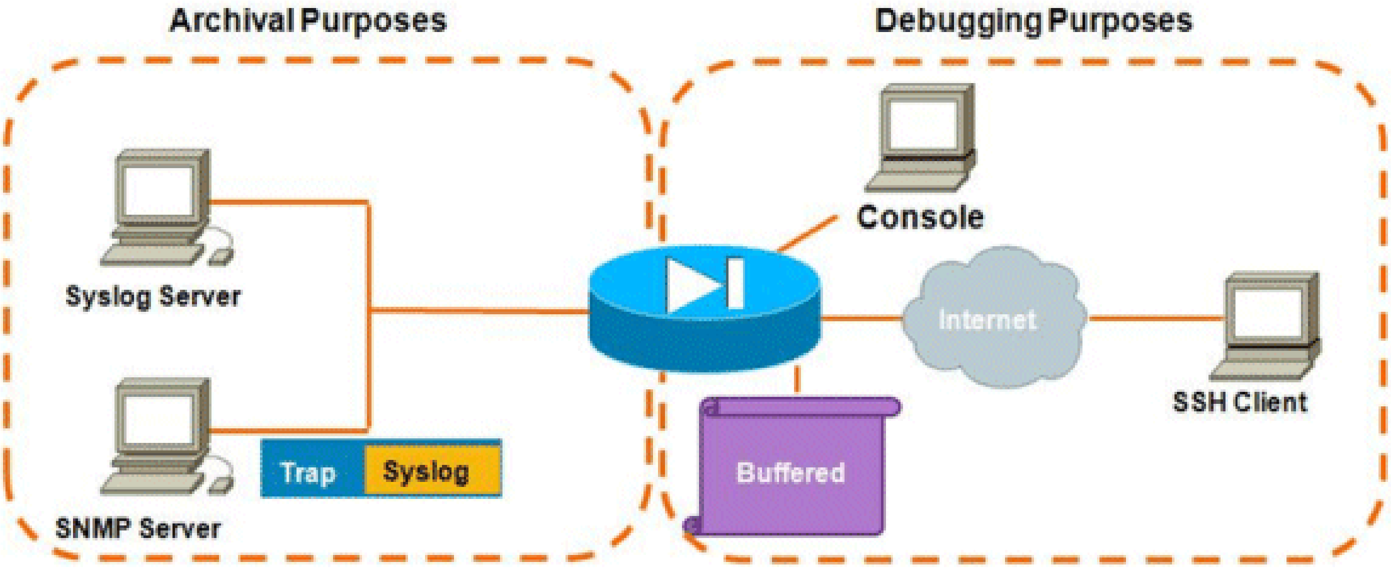
The information in this document is based on the Cisco ASA and it is not limited to a specific ASA software version.

Conventions

For more information on document conventions, refer to Cisco Technical Tips Conventions.

Feature Information

ASAs, as most other Cisco devices, are capable of sending syslogs to multiple syslog destinations. Some of the more commonly used destinations are illustrated here:



The number of destinations possible is a real advantage. If chosen carefully, and as illustrated here, they can be broadly classified into two main categories based on the purpose they serve:

- Archival
- Real-time Debugging/Troubleshooting

In most networks, it is sufficient to have just the archival destinations enabled unless one or more of the debugging destinations are necessary. At the same time, and quite often, problems result from enabling multiple syslog destinations simultaneously at high logging levels such as informational (Level 6) or above.

Troubleshooting Methodology

Whenever issues occur where there is a loss of syslog information at one or more destinations, there are two things that you should check:

- Review the syslogging configuration (output of **show run logging**).
- Look at the output of **show logging queue**.

Data Analysis

Review the Syslogging Configuration

Complete these steps:

1. Make sure that the syslog message you are looking for is not disabled by the **no logging message** <*ID*> command.
2. Once confirmed, look at the number of syslog destinations enabled and the level at which each log is sent to each. This is an example of such a configuration:`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
```

In this example, the ASA is sending syslogs to 4 different destinations at the informational level (Level 6).

Output of show logging queue

With a configuration such as the above, where multiple destinations are receiving large amounts of log messages, you can run into a situation where the ASA drops syslog messages due to an overflow of the logging queue. In such cases, the output will appear similar to this:

```
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
```

By default, the logging queue holds 512 messages.

Common Problems

When running into issues where syslog messages are not being recorded, consider these options:

- Disable console logging. Logging in to the console **should not** be enabled for normal operation. Console logging should be used only for real-time troubleshooting, with either low logging level or low traffic. Logging in to the console at a high rate will cause the logging process to severely rate-limit the messages. The console is only capable of logging messages at 9600 bps, and it does not take a of logs before it starts trying to dump more to the console than the console can output to the screen. In this situation, the logs will start to be buffered in the logging queue. Once the logging queue fills up, messages will be tail-dropped.
- Increase the size of the **logging queue** beyond 512. The maximum logging queue is 1024 on the ASA-5505, 2048 on the ASA-5510, and 8192 on all other platforms. Note: The logging queue is used for "bursts" of syslogs. If the sustained rate of syslogs is faster than the ASA can transmit them to the various destinations, no logging queue limit will be large enough.
- Disable individual syslog messages that you are not interested in archiving. Issue the **no logging message** *<syslog_id>* command in order to disable individual syslogs.
- Be careful of logging messages to the disk (flash) of the ASA. Writing to the flash is a very slow operation. Excessive logging to flash will cause the ASA to buffer the syslog files up in memory, eventually depleting all available memory (RAM). Additionally, logging large amounts of syslog messages to flash may elevate the CPU. It is recommended to only log Level 1 messages to flash (which cover critical system events).

Related Information

- **Technical Support & Documentation - Cisco Systems**