Руководство по поиску и устранению проблем ASA: пропавшие без вести журналов в назначении (назначениях) системного журнала

Содержание

Введение

Этот документ описывает, как устранять проблему с возможностью Устройства адаптивной защиты (ASA) передать системные журналы различным назначениям, и, более в частности, проблемы, где наблюдаются признаки, такие как они:

- Замедлите вход в реальном времени Менеджера устройств адаптивной безопасности (ASDM) (ASDM).
- Неустойчивые системные журналы, отсутствующие в одном или более назначениях системного журнала.

Перед началом работы

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на Cisco ASA, и это не ограничено определенной

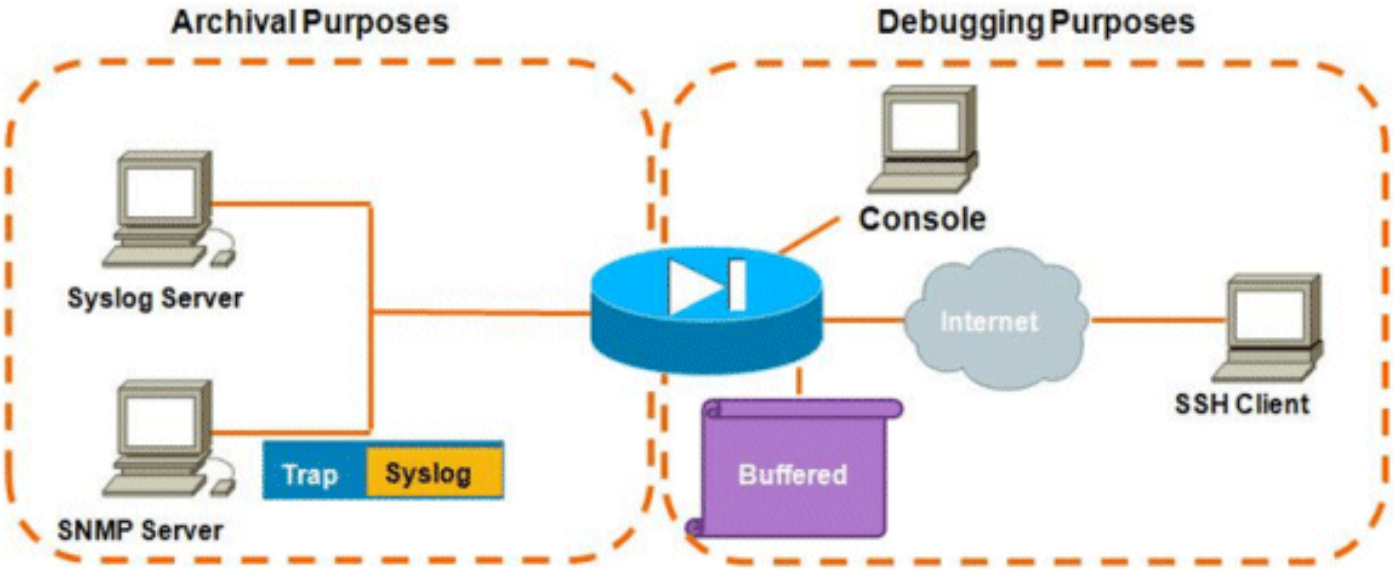
версией программного обеспечения ASA.

Условные обозначения

Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips Conventions.

Информация о функциональной возможности

ASA, как большинство других устройств Cisco, способны к передаче системных журналов ко множественным назначениям системного журнала. Некоторые более обычно используемые назначения проиллюстрированы здесь:



Количество возможных назначений является реальным преимуществом. Если выбрано тщательно, и, как проиллюстрировано здесь, они могут быть широко классифицированы в две основных категории на основе цели, которой они служат:

- Архивация
- Отладка в реальном времени / Устранение проблем

В большинстве сетей достаточно иметь просто архивные назначения, включенные, пока один или больше назначений отладки не необходимы. В то же время, и довольно часто, результат задач включения множественных назначений системного журнала одновременно в высоких уровнях регистрации такой как информационный (Уровень 6) или выше.

Методика устранения проблем

Каждый раз, когда проблемы происходят, где существует потеря сведений системного журнала в одном или более назначениях, существует две вещи, которые необходимо проверить:

- Рассмотрите конфигурацию записи в системный журнал (выходные данные **показа, выполненного, регистрировав**).
- Посмотрите на выходные данные **очереди show logging**.

Анализ данных

Рассмотрите конфигурацию записи в системный журнал

Выполните следующие действия:

1. Удостоверьтесь, что сообщение системного журнала, которое вы ищете, не отключено **никакой** командой *<ID>* **сообщения регистрации**.
2. После того, как подтвержденный, посмотрите на количество включенных назначений системного журнала и уровень, на котором каждый журнал передается каждому. Это - пример такой конфигурации:
```
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
```

В данном примере ASA передает системные журналы 4 другим назначениям в информационном уровне (Уровень 6).

Выходные данные очереди show logging

С конфигурацией такой как вышеупомянутое, где сложные адресаты информации получают большие количества сообщений журнала, можно столкнуться с ситуацией, где ASA отбрасывает сообщения системного журнала из-за переполнения logging queue. В таких случаях выходные данные будут казаться подобными этому:

```
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
```

По умолчанию logging queue держит 512 сообщений.

Типичные неполадки

При столкновении с проблемами, где сообщения системного журнала не регистрируются, рассмотрите эти опции:

- Отключите вход через консоль. Регистрация к консоли **не должна** быть включена для нормальной работы. Вход через консоль должен использоваться только для устранения проблем в реальном времени, или с низким уровнем регистрации или с низким трафиком. Регистрация к консоли в высокой скорости вызовет процесс регистрации к сильно rate-limit сообщения. Консоль только способна к сообщениям регистрации в 9600 битах в секунду, и она не берет журналов, прежде чем она начнет пытаться формировать дамп больше к консоли, чем консоль может вывести на экран. В этой ситуации журналы начнут буферизоваться в logging queue. Как только logging queue заполняется, сообщения будут отброшены хвостом.
- Увеличьте размер logging queue вне 512. Максимальный logging queue 1024 на ASA 5505, 2048 на ASA 5510, и 8192 на всех других платформах. Примечание: Logging queue

используется для "пакетов" системных журналов. Если устойчивая скорость системных журналов будет быстрее, чем ASA может передать их различным назначениям, то никакой предельный размер очереди регистрации не будет достаточно большим.
- Отключите отдельные сообщения системного журнала, что вы не интересуетесь архивацией. Не выполните сообщение регистрации команда *<syslog_id>* для отключения отдельных системных журналов.
- Будьте осторожны в сообщениях регистрации к диску (флэш-память) ASA. Запись во флэш-память является очень медленной операцией. Чрезмерная регистрация для мигания заставит ASA буферизовать файлы системного журнала в памяти, в конечном счете истощая всю доступную память (ОЗУ). Кроме того, регистрация больших количеств сообщений системного журнала для мигания может поднять ЦП. Рекомендуется только регистрировать сообщения Уровня 1 для мигания (которые покрывают события Критической системы).

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация