Содержание

Управление логами с помощью rsyslog

rsyslog — сервис управления системными журналами. Работает как демон, предоставляет средства сбора сообщений и их вывода в место хранения.

Функции rsyslog:

- Принимать сообщения
- Фильтровать и сортировать сообщения — определять их уровень важности и тип
- Сохранять сообщения — записывать их в определенный файл либо отправлять на удаленный сервер

Система гибко конфигурируется: можно настроить сохранение любых типов сообщений в любые файлы.
rsyslog может принимать и передавать логи по протоколу **syslog** по сети, используя как TCP, так и UDP, через стандартный порт 514.

Скрипты для интеграции логов СКАТ с syslog и systemd-юниты для их запуска:

- `parser.bash` — мониторинг логов СКАТ и конвертация в формат rsyslog с помощью модуля logger.
- `bng_logmon.service` — юниты systemd для запуска скриптов.
- `bng.conf` — пример конфигурации для отправки на удаленный сервер, можно использовать как есть или модифицировать для более гибкой настройки.

Требования

- работающий процесс fastdpi — он формирует записи в журналы, это нужно для работы скриптов отправки сообщений, формируемых СКАТ
- работающий демон rsyslog

Установка

1. Установить `bnglogmon`:

   ```
   yum install bnglogmon
   ```

2. Отредактировать файл `/etc/rsyslog.d/bng.conf` — указать адрес сервера и IP-адрес отправителя (при необходимости указать конкретный IP-адрес).
3. Включить автоматический запуск `bnglogmon` при старте системы:

   ```
   systemctl enable bnglogmon.service
   ```

Запуск

1. Запустить bnglogmon:

   ```
   systemctl start bnglogmon.service
   ```

2. Перезапустить rsyslog:

   ```
   systemctl restart rsyslog.service
   ```

Конфигурация

Конфигурация демона rsyslog выполняется согласно настройкам, описанным в его официальной документации.