Содержание

Log Management with rsyslog

rsyslog is a service for managing system logs. It works as a daemon, providing tools to collect messages and send them to a storage location.

Functions of rsyslog:

- Receive messages
- Filter and sort messages — determine their priority and type
- Store messages — write them to specific files or forward them to a remote server

The system is highly configurable: you can set it to save any type of message to any file.
rsyslog can receive and transmit logs over the **syslog** protocol across a network, using both TCP and UDP through the standard port 514.

Scripts for integrating SCAT logs with syslog and systemd units for their execution:

- `parser.bash` — monitors SCAT logs and converts them to rsyslog format using the logger module.
- `bng_logmon.service` — systemd units to launch the scripts.
- `bng.conf` — an example configuration for sending logs to a remote server, which can be used as is or modified for more flexible settings.

Requirements

- A running fastdpi process — it generates log entries, required for the SSG message-sending scripts.
- A running rsyslog daemon.

Installation

1. Install `bnglogmon`:

   ```
   yum install bnglogmon
   ```

2. Edit the file `/etc/rsyslog.d/bng.conf` — specify the server address and the sender's IP address (if necessary, provide a specific IP).
3. Enable automatic startup of `bnglogmon` at system boot:

   ```
   systemctl enable bnglogmon.service
   ```

Execution

1. Start bnglogmon:

```
systemctl start bnglogmon.service
```

2. Restart rsyslog:

```
systemctl restart rsyslog.service
```

Configuration

The rsyslog daemon is configured according to the settings described in its official documentation.