Если вы видите что-то необычное, просто сообщите мне.

Анализ логов.

Классификация логов

- доступа (access_log) — записывают IP-адрес, время запроса, другую информацию о пользователях;
- ошибок (error_log) — показывают файлы, в которых выявлены ошибки и классифицируют сбои;
- загрузки системы — с его помощью выполняется отладка при появлении проблем, в файл записываются основные системные события, включая сбои;
- основной — содержит информацию о действиях с файерволом, DNS-сервером, ядром системы, FTP-сервисом;
- баз данных — хранит подробности о запросах, сбоях, ошибки в логах сервера отображаются наравне с другой важной информацией;
- веб-сервера — содержит информацию о возникавших ошибках, обращениях;

Для чего необходим анализ логов.

- Анализ работы приложения
- Анализ работы инфраструктуры.

Journalctl - инструмент работы системы

Systemd

- systemd — менеджер системы и сервисов
- systemctl — утилита для просмотра и управление статусом сервисов
- systemd-analyze — предоставляет статистику по процессу загрузки системы, проверяет корректность unit-файлов и так же имеет возможности отладки systemd

Место где можно найти конфигурации сервисов, демонов `/etc/systemd/system/`

- Journald - системный демон журналов systemd. Systemd спроектирован так, чтобы централизованно управлять системными логами от процессов, приложений и т.д. Все такие события обрабатываются демоном journald, он собирает логи со всей системы и сохраняет их в бинарных файлах.

Команды:

Отображение всех логов системы

```
journalctl
```

`-e` - отматает в самый конец `-f` - следить за логами в реальном времени.

Фильтрация по важности

```
journalctl -p 0
```

Уровни важности:

- 0: emergency (неработоспособность системы)
- 1: alerts (предупреждения, требующие немедленного вмешательства)
- 2: critical (критическое состояние)
- 3: errors (ошибки)
- 4: warning (предупреждения)
- 5: notice (уведомления)
- 6: info (информационные сообщения)
- 7: debug (отладочные сообщения)

Фильтрация по старту системы

```
journalctl -b 0
```

- 0 - текущая загрузка
- -1 - прошлая загрузка

Фильтрация сообщений ядра

```
journalctl -k
```

Фильтрация сообщений определенного сервиса

```
journalctl -u NetworkManager.service
```

Revision #4

Created 2021-09-22 11:59:22 UTC by gasick

Updated 2023-11-08 16:10:47 UTC by gasick