Отчёт по лабораторной работе №7

Артём Дмитриевич Петлин

Содержание

# 1. Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

# 2. Задание

1. Продемонстрируйте навыки работы с журналом мониторинга событий в реальном времени (см. раздел 7.4.1).
2. Продемонстрируйте навыки создания и настройки отдельного файла конфигурации мониторинга отслеживания событий веб-службы (см. раздел 7.4.2).
3. Продемонстрируйте навыки работы с journalctl (см. раздел 7.4.3).
4. Продемонстрируйте навыки работы с journald (см. раздел 7.4.4).

# 3. Теоретическое введение

В системах на базе Unix/Linux важное место при администрировании занимает отслежи- вание системных событий (и в частности возникновение возможных ошибок в процессе настройки каких-то служб) через ведение log-файлов процессов системы. Журнали- рование системных событий заключается в фиксировании с помощью сокета syslog в лог-файлах сообщений об ошибках и сообщений о состоянии работы практически всех процессов системы.

# 4. Выполнение лабораторной работы

|  |
| --- |
| Рисунок 1: su - |

Запускаем три вкладки терминала и в каждой из них получаем полномочия администратора.

|  |
| --- |
| Рисунок 2: tail |

На второй вкладке терминала запускаем мониторинг системных событий в реальном времени, отслеживая общий файл журнала.

|  |
| --- |
| Рисунок 3: ctrl + d |

В третьей вкладке терминала возвращаемся к учётной записи своего пользователя и пытаемся получить полномочия администратора, вводя неправильный пароль. Наблюдаем появление соответствующей записи во второй вкладке с мониторингом.

|  |
| --- |
| Рисунок 4: logger |

Из оболочки пользователя отправляем тестовое сообщение в системный журнал. Убеждаемся, что сообщение появляется в режиме реального времени в мониторинге.

|  |
| --- |
| Рисунок 5: tail |

Останавливаем трассировку общего файла журнала и просматриваем последние записи в файле журнала безопасности, где находим сообщения о неудачной попытке авторизации.

|  |
| --- |
| Рисунок 6: httpd |

Устанавливаем веб-сервер Apache, если он не был установлен ранее. Запускаем веб-службу и добавляем её в автозагрузку.

|  |
| --- |
| Рисунок 7: tail |

Просматриваем стандартный журнал ошибок веб-службы в режиме реального времени.

|  |
| --- |
| Рисунок 8: httpd.conf |

В конфигурационном файле веб-сервера изменяем параметр логирования, чтобы перенаправить сообщения об ошибках в системный журнал, используя специальный локальный объект.

|  |
| --- |
| Рисунок 9 |

В каталоге конфигурации системного журналирования создаём отдельный файл конфигурации для веб-службы. В этом файле указываем правило, которое все сообщения для выбранного локального объекта записывает в отдельный файл.

|  |
| --- |
| Рисунок 10: restart |

Перезапускаем службу системного журналирования и веб-сервер, чтобы применить новые настройки.

|  |
| --- |
| Рисунок 11: debug.conf |

Создаём ещё один файл конфигурации для системного журналирования, в котором настраиваем запись всех отладочных сообщений в отдельный файл.

|  |
| --- |
| Рисунок 12: echo | restart |

Снова перезапускаем службу системного журналирования.

|  |
| --- |
| Рисунок 13: tail |

Запускаем мониторинг нового файла с отладочными сообщениями.

|  |
| --- |
| Рисунок 14: logger |

|  |
| --- |
| Рисунок 15: tail |

Отправляем тестовое отладочное сообщение и проверяем его появление в мониторинге.

|  |
| --- |
| Рисунок 16: journalctl |

Просматриваем всё содержимое журнала systemd с момента последней загрузки системы, используя постраничный просмотр.

|  |
| --- |
| Рисунок 17: journalctl |

Выводим содержимое журнала без использования пейджера.

|  |
| --- |
| Рисунок 18: journalctl |

Запускаем режим просмотра журнала в реальном времени.

|  |
| --- |
| Рисунок 19: journalctl |

Изучаем доступные параметры фильтрации для утилиты journalctl.

|  |
| --- |
| Рисунок 20: journalctl |

Просматриваем события, связанные с определённым идентификатором пользователя(UID).

|  |
| --- |
| Рисунок 21: journalctl |

Ограничиваем вывод журнала, показывая только последние записи.

|  |
| --- |
| Рисунок 22: journalctl |

Фильтруем сообщения журнала, отображая только сообщения с уровнем ошибки.

|  |
| --- |
| Рисунок 23: journalctl |

Используем временные интервалы для фильтрации записей журнала, например, просматриваем все сообщения за вчерашний день.

|  |
| --- |
| Рисунок 24: journalctl |

Комбинируем фильтры, просматривая сообщения об ошибках за определённый период.

|  |
| --- |
| Рисунок 25: journalctl |

Включаем подробный формат вывода для просмотра детальной информации о записях журнала.

|  |
| --- |
| Рисунок 26: journalctl |

Для просмотра дополнительной информации о модуле sshd вводим.

|  |
| --- |
| Рисунок 27: journald |

Получаем полномочия администратора. Создаём каталог для постоянного хранения журналов systemd. Настраиваем права доступа для созданного каталога, чтобы служба systemd-journald могла в него записывать. Перезапускаем службу системного журналирования с помощью специального сигнала, чтобы активировать постоянное хранение журналов без перезагрузки системы. Убеждаемся, что журнал стал постоянным, и просматриваем сообщения с момента последней загрузки системы.

# 5. Выводы

Мы получили навыки работы с журналами мониторинга различных событий в системе.

# Список литературы

1. Поттеринг Л. Systemd для администраторов: цикл статей. — 2010. — URL: http: //wiki.opennet.ru/Systemd.
2. Емельянов А. Управление логгированием в systemd. — 2015. — URL: https://blog. selectel.ru/upravlenie-loggirovaniem-v-systemd/.
3. Neil N. J. Learning CentOS: A Beginners Guide to Learning Linux. — CreateSpace Inde- pendent Publishing Platform, 2016.
4. Goyal S. K. Precise Guide to Centos 7: Beginners guide and quick reference. — Indepen- dently published, 2017.
5. Unix и Linux: руководство системного администратора / Э. Немет, Г. Снайдер, Т. Хейн, Б. Уэйли, Д. Макни. — 5-е изд. — СПб. : ООО «Диалектика», 2020.