

Лабораторная работа №7.

Управление журналами событий в системе

Жукова А.А

19 октября 2024

Российский университет дружбы народов, Москва, Россия

Информация

- Жукова Арина Александровна
- Студент бакалавриата, 2 курс
- группа: НПИбд-03-23
- Российский университет дружбы народов
- 1132239120@rudn.ru



Вводная часть

Цель работы

Лабораторная работа направлена на получение навыков работы с журналами мониторинга различных событий в системе.

Задание

1. Продемонстрируйте навыки работы с журналом мониторинга событий в реальном времени.
2. Продемонстрируйте навыки создания и настройки отдельного файла конфигурации мониторинга отслеживания событий веб-службы.
3. Продемонстрируйте навыки работы с journalctl.
4. Продемонстрируйте навыки работы с journald.

Результаты и анализ лабораторной работы

Основные файлы журналов

- `/var/log/messages` – общий файл журнала, в который записывается большинство сообщений системы (наиболее часто используемый файл журнала);
- `/var/log/dmesg` – журнал сообщений ядра системы;
- `/var/log/secure` – журнал сообщений, связанных с аутентификацией в системе;
- `/var/log/boot.log` – журнал сообщений, связанных с запуском системы;
- `/var/log/audit/audit.log` – журнал сообщений аудита (например, в него записываются сообщения SELinux);
- `/var/log/maillog` – журналы сообщений, связанных с почтовой службой;
- `/var/log/samba` – журналы сообщений службы samba (samba по умолчанию не управляет через `rsyslogd`);
- `/var/log/sssd` – журналы сообщений службы `sssd`;
- `/var/log/cups` – журналы службы печати `cups`;
- `/var/log/httpd/` – каталог с журналами веб-службы Apache (Apache записывает сообщения в эти файлы напрямую, а не через `rsyslog`).

Мониторинг журнала системных событий в реальном времени

- Команда tail -f: Мониторинг файла /var/log/messages в реальном времени, пример: tail -f /var/log/messages

```
[root@aazhukoval ~]# tail -f /var/log/messages
Oct 18 19:14:57 aazhukoval PackageKit[1897]: uid 1000 obtained auth for org.freedesktop.packagekit.system-sources-refresh
Oct 18 19:15:01 aazhukoval systemd[1]: fprintd.service: Deactivated successfully.
Oct 18 19:15:03 aazhukoval systemd[2258]: Started VTE child process 3298 launched by gnome-terminal-server process 3071.
Oct 18 19:15:11 aazhukoval systemd[1]: Starting Fingerprint Authentication Daemon...
Oct 18 19:15:11 aazhukoval systemd[1]: Started Fingerprint Authentication Daemon.
Oct 18 19:15:14 aazhukoval su[3328]: (to root) aazhukoval on pts/2
Oct 18 19:15:41 aazhukoval systemd[1]: fprintd.service: Deactivated successfully.
Oct 18 19:15:44 aazhukoval systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Oct 18 19:16:07 aazhukoval systemd[2258]: Starting Mark boot as successful
```

Мониторинг журнала системных событий в реальном времени

- tail -n 20 /var/log/secure: Вывод последних 20 строк из файла /var/log/secure

```
ser gum  
Oct 18 19:13:57 aazhukoval polkitd[740]: Unregistered Authentication Agent for unix-session:c1 (system bus name :1.26, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale ru_RU.UTF-8) (disconnected from bus)  
Oct 18 19:14:34 aazhukoval su[3133]: pam_unix(su-l:session): session opened for user root(uid=0) by aazhukoval(uid=1000)  
Oct 18 19:14:57 aazhukoval su[3203]: pam_unix(su-l:session): session opened for user root(uid=0) by aazhukoval(uid=1000)  
Oct 18 19:15:14 aazhukoval su[3328]: pam_unix(su-l:session): session opened for user root(uid=0) by aazhukoval(uid=1000)  
Oct 18 19:17:24 aazhukoval su[3133]: pam_unix(su-l:session): session closed for user root  
Oct 18 19:17:35 aazhukoval unix_chkpwd[3403]: password check failed for user (root)  
Oct 18 19:17:35 aazhukoval su[3396]: pam_unix(su-l:auth): authentication failure: logname=aazhukoval uid=1000 euid=0 tty
```

Мониторинг журнала системных событий в реальном времени

- logger hello: Запись сообщения “hello” в системный журнал

```
Oct 18 19:18:01 aazhukoval systemd[1]: fprintd.service: Deactivated successfully.  
Oct 18 19:18:02 aazhukoval aazhukoval[3412]: hello
```

Изменение правил rsyslog.conf:

- ErrorLog syslog:local1: Добавление строки в конфигурационный файл Apache, чтобы сообщения об ошибках записывались в системный журнал.

```
httpd.conf [-M--] 22 L:[341+18 359/359] *(12027/12027b) <EOF>
```

```
#  
  
#  
# EnableMMAP and EnableSendfile: On systems that support it,.  
# memory-mapping or the sendfile syscall may be used to deliver  
# files. This usually improves server performance, but must  
# be turned off when serving from networked mounted
```

Изменение правил rsyslog.conf:

- echo “*.debug /var/log/messages-debug” > /etc/rsyslog.d/debug.conf: Запись правила в файл debug.conf для отправки отладочной информации в файл /var/log/messages-debug

ошиб. синтаксическая ошибка рядом с неожиданным маркером «плюс плюс»

```
[root@aazhukoval rsyslog.d]# echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf  
[root@aazhukoval rsyslog.d]# mc
```

Использование journalctl

- journalctl: Просмотр журнала системных событий

```
[root@aazhukoval ~]# journalctl
окт 18 19:12:13 aazhukoval.localdomain kernel: Linux versio>
окт 18 19:12:13 aazhukoval.localdomain kernel: The list of >
окт 18 19:12:13 aazhukoval.localdomain kernel: Command line>
окт 18 19:12:13 aazhukoval.localdomain kernel: x86/fpu: Sup>
окт 18 19:12:13 aazhukoval.localdomain kernel: x86/fpu: xst>
окт 18 19:12:13 aazhukoval.localdomain kernel: x86/fpu: Ena>
окт 18 19:12:13 aazhukoval.localdomain kernel: signal: max >
окт 18 19:12:13 aazhukoval.localdomain kernel: BIOS-provide>
окт 18 19:12:13 aazhukoval.localdomain kernel: BIOS-e820: [>
окт 18 19:12:13 aazhukoval.localdomain kernel: NX (Execute >
```

Использование journalctl

- journalctl –since “2023-10-26”: Просмотр журнала с определенной даты

```
[root@aazhukoval ~]# journalctl --since yesterday
окт 18 19:12:13 aazhukoval.localdomain kernel: Linux versi>
окт 18 19:12:13 aazhukoval.localdomain kernel: The list of>
окт 18 19:12:13 aazhukoval.localdomain kernel: Command lin>
окт 18 19:12:13 aazhukoval.localdomain kernel: x86/fpu: Su>
окт 18 19:12:13 aazhukoval.localdomain kernel: x86/fpu: xs>
окт 18 19:12:13 aazhukoval.localdomain kernel: x86/fpu: En>
окт 18 19:12:13 aazhukoval.localdomain kernel: signal: max>
окт 18 19:12:13 aazhukoval.localdomain kernel: BIOS-provid>
окт 18 19:12:13 aazhukoval.localdomain kernel: BIOS-e820: >
```

Использование journalctl

- journalctl -p err: Фильтрация журнала по имени службы и уровню важности

```
[root@aazhukoval ~]# journalctl -p err
окт 18 19:12:13 aazhukoval.localdomain systemd[1]: Invalid DMI field header.
окт 18 19:12:13 aazhukoval.localdomain kernel: Warning: Unmaintained driver is detected: e1000
окт 18 19:12:13 aazhukoval.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on an unsupported hardware
окт 18 19:12:13 aazhukoval.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely to cause problems
окт 18 19:12:13 aazhukoval.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported hardware
окт 18 19:12:16 aazhukoval.localdomain systemd[1]: Invalid DMI field header.
окт 18 19:12:17 aazhukoval.localdomain systemd-udevd[622]: vboxguest: /etc/udev/rules.d/60-vboxadd.rules:1 Only one uev
окт 18 19:12:17 aazhukoval.localdomain systemd-udevd[651]: vboxuser: /etc/udev/rules.d/60-vboxadd.rules:2 Only one uev
окт 18 19:12:18 aazhukoval.localdomain alsactl[778]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to open file
окт 18 19:12:19 aazhukoval.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
окт 18 19:13:36 aazhukoval.localdomain gdm-password][2208]: gkr-pam: unable to locate daemon control file
окт 18 19:13:50 aazhukoval.localdomain gdm-password][2246]: gkr-pam: unable to locate daemon control file
окт 18 19:13:57 aazhukoval.localdomain gdm-wayland-session[1250]: GLib: Source ID 2 was not found when attempting to cancel source
окт 18 19:13:57 aazhukoval.localdomain gdm-launch-environment][1108]: GLib-GObject: g_object_unref: assertion failed: (object != NULL)
```

Постоянный журнал journald

По умолчанию журнал journald хранит сообщения в оперативной памяти системы и записи доступны в каталоге /run/log/journal только до перезагрузки системы. Для того чтобы сделать журнал journald постоянным необходимо создать каталог для хранения записей журнала, скорректируйте права доступа для каталога /var/log/journal, чтобы journald смог записывать в него информацию, перезагрузить систему.

```
[root@aazhukoval ~]# mkdir -p /var/log/journal  
[root@aazhukoval ~]# chown root:systemd-journal /var/log/journal  
[root@aazhukoval ~]# chmod 2755 /var/log/journal  
[root@aazhukoval ~]# killall -USR1 systemd-journald
```

Выводы

Выводы

В ходе выполнения лабораторной работы были получены навыки работы с журналами мониторинга различных событий в системе.