

Отчет по лабораторной работе 7

Управление журналами событий в системе

Власов Артем Сергеевич

Содержание

1. Цель работы.....	1
2. Задание.....	1
3. Выполнение лабораторной работы 7.....	1
4. Выводы.....	7
Список литературы.....	7

1. Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

2. Задание

Продemonстрировать навыки умения работать с журналом мониторинга событий, созданием файла конфигурации мониторинга, `journald` и `journalctl`.

3. Выполнение лабораторной работы 7.

Запускаем 3 терминала, открываем во втором журнал мониторинга, на третьем пробуем получить права администратора с неверным паролем.

```
root@asvlasov:~  
[root@asvlasov ~]# tail -f /var/log/messages  
tail: невозможно открыть '/var/log/messages' для чтения: Нет такого файла или каталога  
tail: больше нет файлов  
[root@asvlasov ~]# tail -f /var/log/messages  
Oct 18 19:52:49 asvlasov systemd[2919]: Started VTE child process 4083 launched by gnome-terminal-server process 3923.  
Oct 18 19:53:02 asvlasov systemd[1]: Starting Fingerprint Authentication Daemon  
n...  
Oct 18 19:53:02 asvlasov systemd[1]: Started Fingerprint Authentication Daemon  
.  
Oct 18 19:53:04 asvlasov su[4109]: (to root) asvlasov on pts/2  
Oct 18 19:53:04 asvlasov systemd[1]: Starting Hostname Service...  
Oct 18 19:53:04 asvlasov systemd[1]: Started Hostname Service.  
Oct 18 19:53:08 asvlasov su[4149]: (to root) asvlasov on pts/0  
Oct 18 19:53:14 asvlasov su[4183]: (to root) asvlasov on pts/1  
Oct 18 19:53:33 asvlasov systemd[1]: fprintd.service: Deactivated successfully  
.  
Oct 18 19:53:44 asvlasov systemd[1]: systemd-hostnamed.service: Deactivated successfully.  
Oct 18 19:56:07 asvlasov systemd[1]: Starting Fingerprint Authentication Daemon  
n...  
Oct 18 19:56:07 asvlasov systemd[1]: Started Fingerprint Authentication Daemon  
.  
Oct 18 19:56:11 asvlasov su[4231]: FAILED SU (to root) asvlasov on pts/1  
[
```

Неверный пароль администратора

Выводим в журнал сообщение hello.

```
root@asvlasov:~  
[root@asvlasov ~]# tail -f /var/log/messages  
tail: невозможно открыть '/var/log/messages' для чтения: Нет такого файла или каталога  
tail: больше нет файлов  
[root@asvlasov ~]# tail -f /var/log/messages  
Oct 18 19:52:49 asvlasov systemd[2919]: Started VTE child process 4083 launched by gnome-terminal-server process 3923.  
Oct 18 19:53:02 asvlasov systemd[1]: Starting Fingerprint Authentication Daemon  
n...  
Oct 18 19:53:02 asvlasov systemd[1]: Started Fingerprint Authentication Daemon  
.  
Oct 18 19:53:04 asvlasov su[4109]: (to root) asvlasov on pts/2  
Oct 18 19:53:04 asvlasov systemd[1]: Starting Hostname Service...  
Oct 18 19:53:04 asvlasov systemd[1]: Started Hostname Service.  
Oct 18 19:53:08 asvlasov su[4149]: (to root) asvlasov on pts/0  
Oct 18 19:53:14 asvlasov su[4183]: (to root) asvlasov on pts/1  
Oct 18 19:53:33 asvlasov systemd[1]: fprintd.service: Deactivated successfully  
.  
Oct 18 19:53:44 asvlasov systemd[1]: systemd-hostnamed.service: Deactivated successfully.  
Oct 18 19:56:07 asvlasov systemd[1]: Starting Fingerprint Authentication Daemon  
n...  
Oct 18 19:56:07 asvlasov systemd[1]: Started Fingerprint Authentication Daemon  
.  
Oct 18 19:56:11 asvlasov su[4231]: FAILED SU (to root) asvlasov on pts/1  
Oct 18 19:56:38 asvlasov systemd[1]: fprintd.service: Deactivated successfully  
.  
Oct 18 19:56:39 asvlasov asvlasov[4246]: hello  
[
```

Сообщение

Открываем 20 последних строчек журнала.

```
[root@asvlasov ~]# tail -n 20 /var/log/secure
Oct 18 19:18:35 asvlasov useradd[1905]: failed adding user 'vboxadd', exit code: 9
Oct 18 19:18:35 asvlasov useradd[1906]: failed adding user 'vboxadd', exit code: 9
Oct 18 19:18:44 asvlasov systemd[2459]: pam_unix(systemd-user:session): session opened for user gdm(uid=42) by gdm(uid=0)
Oct 18 19:18:45 asvlasov gdm-launch-environment[2454]: pam_unix(gdm-launch-environment:session): session opened for user gdm(uid=42) by (uid=0)
Oct 18 19:18:49 asvlasov polkitd[798]: Registered Authentication Agent for unix-session:c1 (system bus name :1.25 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale ru_RU.UTF-8)
Oct 18 19:19:24 asvlasov gdm-password[2898]: gkr-pam: unable to locate daemon control file
Oct 18 19:19:24 asvlasov gdm-password[2898]: gkr-pam: stashed password to try later in open session
Oct 18 19:19:24 asvlasov systemd[2919]: pam_unix(systemd-user:session): session opened for user asvlasov(uid=1000) by asvlasov(uid=0)
Oct 18 19:19:24 asvlasov gdm-password[2898]: pam_unix(gdm-password:session): session opened for user asvlasov(uid=1000) by asvlasov(uid=0)
Oct 18 19:19:24 asvlasov gdm-password[2898]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Oct 18 19:19:28 asvlasov polkitd[798]: Registered Authentication Agent for unix-session:? (system bus name :1.71 [/usr/bin/gnome-shell], object path /org/fr
```

20 строчек

Устанавливаем и запускаем httpd.

```
root@asvlasov:~
[root@asvlasov ~]# systemctl start httpd
[root@asvlasov ~]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[root@asvlasov ~]#
```

httpd

Смотрим логи ошибок httpd.

```
[root@asvlasov ~]# tail -f /var/log/httpd/error_log
[Sat Oct 18 20:18:18.880510 2025] [core:notice] [pid 17160:tid 17160] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Sat Oct 18 20:18:18.884071 2025] [suexec:notice] [pid 17160:tid 17160] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Sat Oct 18 20:18:18.953597 2025] [lbmethod_heartbeat:notice] [pid 17160:tid 17160] AH02282: No slotmem from mod_heartbeat
[Sat Oct 18 20:18:18.966719 2025] [mpm_event:notice] [pid 17160:tid 17160] AH00489: Apache/2.4.62 (Rocky Linux) configured -- resuming normal operations
[Sat Oct 18 20:18:18.966841 2025] [core:notice] [pid 17160:tid 17160] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
```

Логи ошибок

Заходим в файл конфигурации и дописываем строчку.

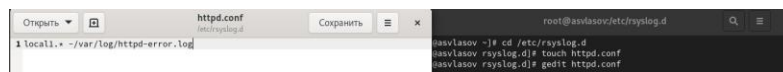


```
323 <IfModule mime_magic_module>
324     #
325     # The mod_mime_magic module allows the server to use various hints f
326     # contents of the file itself to determine its type. The MIMEMagicF
327     # directive tells the module where the hint definitions are located.
328     #
329     MIMEMagicFile conf/magic
330 </IfModule>
331
332 #
333 # Customizable error responses come in three flavors:
334 # 1) plain text 2) local redirects 3) external redirects
335 #
336 # Some examples:
337 #ErrorDocument 500 "The server made a boo boo."
338 #ErrorDocument 404 /missing.html
339 #ErrorDocument 404 "/cgi-bin/missing_handler.pl"
340 #ErrorDocument 402 http://www.example.com/subscription_info.html
341 #
342
343 #
344 # EnableMMAP and EnableSendfile: On systems that support it,
345 # memory-mapping or the sendfile syscall may be used to deliver
346 # files. This usually improves server performance, but must
347 # be turned off when serving from networked-mounted
348 # filesystems or if support for these functions is otherwise
349 # broken on your system.
350 # Defaults if commented: EnableMMAP On, EnableSendfile Off
351 #
352 #EnableMMAP off
353 EnableSendfile on
354
355 # Supplemental configuration
356 #
357 # Load config files in the "/etc/httpd/conf.d" directory, if any.
358 IncludeOptional conf.d/*.conf
359
360 ErrorLog syslog:local
```

Текст ▾ Ширина табуляции: 8

Изменение файла конфигурации

Создаем новый файл конфигурации и заполняем его.



```
root@asvlasov:~# touch httpd.conf
root@asvlasov:~# gedit httpd.conf
```

Новый файл конфигурации

Перезапускаем сервисы и дописываем строчку в файл конфигурации debug.conf.



```
root@asvlasov:~# systemctl restart rsyslog.service
root@asvlasov:~# systemctl restart httpd
root@asvlasov:~# echo "> /etc/rsyslog.d/debug.conf"
```

debug

Затем отправляем сообщение в другой журнал мониторинга.

```
root@asvlasov:~# tail -f /var/log/messages-debug
Oct 18 20:27:04 asvlasov systemd[1]: Stopping System Logging Service...
Oct 18 20:27:04 asvlasov rsyslogd[44373]: [origin software="rsyslogd" swVersion="8.2412.0-1.el9" x-pid="44373" x-info="https://www.rsyslog.com"] exiting on signal 15
Oct 18 20:27:04 asvlasov systemd[1]: rsyslog.service: Deactivated successfully.
Oct 18 20:27:04 asvlasov systemd[1]: Stopped System Logging Service.
Oct 18 20:27:04 asvlasov systemd[1]: Starting System Logging Service...
Oct 18 20:27:05 asvlasov rsyslogd[44397]: [origin software="rsyslogd" swVersion="8.2412.0-1.el9" x-pid="44397" x-info="https://www.rsyslog.com"] start
Oct 18 20:27:05 asvlasov rsyslogd[44397]: imjournal: journal files changed, reloading... [v8.2412.0-1.el9 try https://www.rsyslog.com/e/0 ]
Oct 18 20:28:21 asvlasov root[44406]: Daemon Debug Message
```

Сообщение в журнале

Начинаем работу с journalctl. Смотрим журнал в реальном времени.

```
[root@asvlasov ~]# journalctl -f
bash: journalctl: команда не найдена...
[root@asvlasov ~]# journalctl -f
окт 18 20:27:04 asvlasov.localdomain systemd[1]: Stopped System Logging Service.
окт 18 20:27:04 asvlasov.localdomain systemd[1]: Starting System Logging Service.
окт 18 20:27:05 asvlasov.localdomain systemd[1]: Started System Logging Service.
окт 18 20:27:05 asvlasov.localdomain rsyslogd[44397]: [origin software="rsyslogd" swVersion="8.2412.0-1.el9" x-pid="44397" x-info="https://www.rsyslog.com"] start
окт 18 20:27:05 asvlasov.localdomain rsyslogd[44397]: imjournal: journal files changed, reloading... [v8.2412.0-1.el9 try https://www.rsyslog.com/e/0 ]
окт 18 20:28:21 asvlasov.localdomain root[44406]: Daemon Debug Message
окт 18 20:29:25 asvlasov.localdomain systemd[1]: Starting PackageKit Daemon.
окт 18 20:29:25 asvlasov.localdomain PackageKit[44417]: daemon start
окт 18 20:29:25 asvlasov.localdomain systemd[1]: Started PackageKit Daemon.
окт 18 20:29:26 asvlasov.localdomain PackageKit[44417]: search-file transaction /1089_eabbeccc from uid 0 finished with success after 501ms
```

Журнал в реальном времени

Затем смотрим строки связанные с UID 0.

```
[root@asvlasov ~]# journalctl _UID=0
окт 18 19:17:58 asvlasov.localdomain systemd-journald[244]: Journal started
окт 18 19:17:58 asvlasov.localdomain systemd-journald[244]: Runtime Journal (>
окт 18 19:17:58 asvlasov.localdomain systemd-sysusers[246]: Creating group 'n>
окт 18 19:17:58 asvlasov.localdomain systemd-sysusers[246]: Creating group 'u>
окт 18 19:17:58 asvlasov.localdomain systemd-sysusers[246]: Creating group 'd>
окт 18 19:17:58 asvlasov.localdomain systemd-sysusers[246]: Creating user 'db>
окт 18 19:17:58 asvlasov.localdomain systemd[1]: Starting Create Volatile Fil>
окт 18 19:17:58 asvlasov.localdomain systemd-modules-load[245]: Inserted modu>
окт 18 19:17:58 asvlasov.localdomain systemd-modules-load[245]: Module 'msr' >
окт 18 19:17:58 asvlasov.localdomain systemd[1]: Finished Load Kernel Modules>
окт 18 19:17:58 asvlasov.localdomain systemd[1]: Starting Apply Kernel Variab>
окт 18 19:17:58 asvlasov.localdomain systemd[1]: Finished Apply Kernel Variab>
окт 18 19:17:58 asvlasov.localdomain systemd[1]: Finished Create Static Devi>
окт 18 19:17:58 asvlasov.localdomain systemd[1]: Finished Create Volatile Fil>
окт 18 19:17:59 asvlasov.localdomain systemd[1]: Finished Setup Virtual Conso>
окт 18 19:17:59 asvlasov.localdomain systemd[1]: dracut ask for additional cm>
окт 18 19:17:59 asvlasov.localdomain systemd[1]: Starting dracut cmdline hook>
окт 18 19:17:59 asvlasov.localdomain dracut-cmdline[262]: dracut-9.6 (Blue On>
```

Журнал

Смотрим последние 20 строк журнала и строки с ошибками.

```

[root@asvlasov ~]# journalctl -n 20
ОКТ 18 20:23:55 asvlasov.localdomain systemd[1]: httpd.service: Consumed 2.93>
ОКТ 18 20:23:55 asvlasov.localdomain systemd[1]: Starting The Apache HTTP Ser>
ОКТ 18 20:23:55 asvlasov.localdomain httpd[44382]: AH00526: Syntax error on l>
ОКТ 18 20:23:55 asvlasov.localdomain httpd[44382]: Invalid command 'ErrorLog',>
ОКТ 18 20:23:55 asvlasov.localdomain systemd[1]: httpd.service: Main process>
ОКТ 18 20:23:55 asvlasov.localdomain systemd[1]: httpd.service: Failed with r>
ОКТ 18 20:23:55 asvlasov.localdomain systemd[1]: Failed to start The Apache H>
ОКТ 18 20:27:04 asvlasov.localdomain systemd[1]: Stopping System Logging Servi>
ОКТ 18 20:27:04 asvlasov.localdomain rsyslogd[44373]: [origin software="rsysl>
ОКТ 18 20:27:04 asvlasov.localdomain systemd[1]: rsyslog.service: Deactivated>
ОКТ 18 20:27:04 asvlasov.localdomain systemd[1]: Stopped System Logging Servi>
ОКТ 18 20:27:04 asvlasov.localdomain systemd[1]: Starting System Logging Servi>
ОКТ 18 20:27:05 asvlasov.localdomain systemd[1]: Started System Logging Servi>
ОКТ 18 20:27:05 asvlasov.localdomain rsyslogd[44397]: [origin software="rsysl>
ОКТ 18 20:27:05 asvlasov.localdomain rsyslogd[44397]: imjournal: journal file>
ОКТ 18 20:28:21 asvlasov.localdomain root[44406]: Daemon Debug Message
ОКТ 18 20:29:25 asvlasov.localdomain systemd[1]: Starting PackageKit Daemon...
ОКТ 18 20:29:25 asvlasov.localdomain PackageKit[44417]: daemon start
ОКТ 18 20:29:25 asvlasov.localdomain systemd[1]: Started PackageKit Daemon.
ОКТ 18 20:29:26 asvlasov.localdomain PackageKit[44417]: search-file transact>

[root@asvlasov ~]# journalctl -p err
ОКТ 18 19:17:58 asvlasov.localdomain kernel: Warning: Deprecated Hardware is>
ОКТ 18 19:17:58 asvlasov.localdomain systemd[1]: Invalid DMI field header.>
ОКТ 18 19:17:59 asvlasov.localdomain kernel: Warning: Unmaintained driver is>
ОКТ 18 19:18:00 asvlasov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERRO>
ОКТ 18 19:18:00 asvlasov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERRO>
ОКТ 18 19:18:00 asvlasov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERRO>
ОКТ 18 19:18:06 asvlasov.localdomain systemd[1]: Invalid DMI field header.>
ОКТ 18 19:18:09 asvlasov.localdomain alsactl[828]: alsa-lib main.c:1554:(snd>
ОКТ 18 19:18:11 asvlasov.localdomain kernel: Warning: Unmaintained driver is>
ОКТ 18 19:18:44 asvlasov.localdomain systemd[1]: Failed to start vboxadd.serv>
ОКТ 18 19:18:44 asvlasov.localdomain systemd[1]: Failed to start vboxadd-serv>
ОКТ 18 19:19:24 asvlasov.localdomain gdm-password[2898]: gkr-pam: unable to>
ОКТ 18 19:19:26 asvlasov.localdomain systemd[2919]: Failed to start Applicati>
ОКТ 18 19:19:29 asvlasov.localdomain systemd[2919]: Failed to start Applicati>
ОКТ 18 19:19:32 asvlasov.localdomain gdm-wayland-session[2476]: GLib: Source>
ОКТ 18 19:19:32 asvlasov.localdomain gdm-launch-environment[2454]: GLib-60bj>
ОКТ 18 20:23:55 asvlasov.localdomain systemd[1]: Failed to start The Apache H>

```

20 строк и ошибки

Смотрим все ошибки со вчерашнего дня.

```

[root@asvlasov ~]# journalctl --since yesterday -p err
ОКТ 18 19:17:58 asvlasov.localdomain kernel: Warning: Deprecated Hardware is>
ОКТ 18 19:17:58 asvlasov.localdomain systemd[1]: Invalid DMI field header.>
ОКТ 18 19:17:59 asvlasov.localdomain kernel: Warning: Unmaintained driver is>
ОКТ 18 19:18:00 asvlasov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERRO>
ОКТ 18 19:18:00 asvlasov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERRO>
ОКТ 18 19:18:00 asvlasov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERRO>
ОКТ 18 19:18:06 asvlasov.localdomain systemd[1]: Invalid DMI field header.>
ОКТ 18 19:18:09 asvlasov.localdomain alsactl[828]: alsa-lib main.c:1554:(snd>
ОКТ 18 19:18:11 asvlasov.localdomain kernel: Warning: Unmaintained driver is>
ОКТ 18 19:18:44 asvlasov.localdomain systemd[1]: Failed to start vboxadd.serv>
ОКТ 18 19:18:44 asvlasov.localdomain systemd[1]: Failed to start vboxadd-serv>
ОКТ 18 19:19:24 asvlasov.localdomain gdm-password[2898]: gkr-pam: unable to>
ОКТ 18 19:19:26 asvlasov.localdomain systemd[2919]: Failed to start Applicati>
ОКТ 18 19:19:29 asvlasov.localdomain systemd[2919]: Failed to start Applicati>
ОКТ 18 19:19:32 asvlasov.localdomain gdm-wayland-session[2476]: GLib: Source>
ОКТ 18 19:19:32 asvlasov.localdomain gdm-launch-environment[2454]: GLib-60bj>
ОКТ 18 20:23:55 asvlasov.localdomain systemd[1]: Failed to start The Apache H>

```

Ошибки с определенной даты

Просмотр детальной информации

```
[root@asvlasov ~]# journalctl -o verbose
Sat 2025-10-18 19:17:58.677082 MSK [s=8cb80feba247454eb5b61aff96174f65;i=1;b=>
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
PRIORITY=5
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
MESSAGE=Linux version 5.14.0-570.37.1.el9_6.x86_64 (mockbuild@iad1-prod-b>
_BOOT_ID=63c468765c994298a15e6a96f1a71395
_MACHINE_ID=632ddcdda5794c52ad928429cbc91d0b
_HOSTNAME=asvlasov.localdomain
_RUNTIME_SCOPE=initrd
Sat 2025-10-18 19:17:58.677102 MSK [s=8cb80feba247454eb5b61aff96174f65;i=2;b=>
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
PRIORITY=5
```

Детальная информация

Просмотр дополнительной информации о модуле sshd.

```
[root@asvlasov ~]# journalctl _SYSTEM_UNIT=sshd.service
-- No entries --
```

sshd

Создаем каталог для хранения записей журнала, задаем ему права, принимаем изменения командой. Теперь журнал постоянный.

```
[root@asvlasov ~]# mkdir -p /var/log/journal
[root@asvlasov ~]# chown root:systemd-journal /var/log
local/ lock/ log/
[root@asvlasov ~]# chown root:systemd-journal /var/log/journal
[root@asvlasov ~]# chmod 755 /var/log/journal
[root@asvlasov ~]# killall -USR1 systemd-journal
[root@asvlasov ~]# journalctl -b
out 18 19:17:58 asvlasov.localdomain kernel: Linux version 5.14.0-570.37.1.el9_6.x86_64 (mockbuild@iad1-prod-build001.bld.eur.rockylinux.org) (gcc (GCC) 11.5
out 18 19:17:58 asvlasov.localdomain kernel: The list of certified hardware and cloud instances for Enterprise Linux 9 can be viewed at the Red Hat Ecosystem
out 18 19:17:58 asvlasov.localdomain kernel: Command line: BOOT_IMAGE=(hd0,mdo5)/vmlinuz-5.14.0-570.37.1.el9_6.x86_64 root=/dev/mapper/rh_Linux-root ro res
out 18 19:17:58 asvlasov.localdomain kernel: [Firmware Bug]: TSC doesn't count with PG frequency!
out 18 19:17:58 asvlasov.localdomain kernel: BIOS-provided physical RAM map:
out 18 19:17:58 asvlasov.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000000fff] usable
out 18 19:17:58 asvlasov.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000ffff] reserved
out 18 19:17:58 asvlasov.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000ffff] reserved
out 18 19:17:58 asvlasov.localdomain kernel: BIOS-e820: [mem 0x0000000001000000-0x00000000000ffff] usable
out 18 19:17:58 asvlasov.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000ffff] ACPI data
out 18 19:17:58 asvlasov.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000ffff] reserved
out 18 19:17:58 asvlasov.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000ffff] reserved
out 18 19:17:58 asvlasov.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000ffff] reserved
out 18 19:17:58 asvlasov.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000ffff] reserved
out 18 19:17:58 asvlasov.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000ffff] reserved
out 18 19:17:58 asvlasov.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000ffff] reserved
out 18 19:17:58 asvlasov.localdomain kernel: APIC: Static calls initialized
out 18 19:17:58 asvlasov.localdomain kernel: SMIOIS 2.5 present.
out 18 19:17:58 asvlasov.localdomain kernel: DM: smntek Golem VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
out 18 19:17:58 asvlasov.localdomain kernel: Hypervisor detected: KVM
out 18 19:17:58 asvlasov.localdomain kernel: kvm-clock: Using msrc 4b564d01 and 4b564d00
out 18 19:17:58 asvlasov.localdomain kernel: kvm-clock: using tscd offset of 816643668 cycles
```

Создание постоянного журнала

4. Выводы

Мы научились работать с журналами мониторинга событий в системе.

Список литературы