

Отчет по лабораторной работе 7

Генералов Даниил, НПИбд-01-21, 1032202280

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	13
5	Контрольные вопросы	14

Список иллюстраций

3.1	messages	7
3.2	secure	8
3.3	httpd	9
3.4	debug	9
3.5	journalctl	10
3.6	journalctl	11
3.7	journalctl	11
3.8	journalctl	12
5.1	rsyslog.conf	14
5.2	secure	15
5.3	logrotate.conf	15
5.4	rsyslog.conf	16
5.5	journalctl	16
5.6	journalctl	17

Список таблиц

1 Цель работы

В рамках этой лабораторной работы требуется выполнить операции по управлению сервисом ведения логов rsyslogd.

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 Выполнение лабораторной работы

Сначала я открыл для чтения файл `/var/log/messages`. Затем, сделав в другом терминале действия, я увидел, как сообщения об этих действиях были добавлены в конец этого файла.

```
Rocky Linux 9.0 (Blue Onyx)
Kernel 5.14.0-70.13.1.el9_0.x86_64 on an x86_64

dmgeneralov login: root
Password:
Last login: Sat Nov 26 16:16:58 on tty2
[root@dmgeneralov ~]# tail -f /var/log/messages
Nov 30 15:41:52 dmgeneralov systemd[1223]: Listening on D-Bus User Message Bus Socket.
Nov 30 15:41:52 dmgeneralov systemd[1223]: Finished Create User's Volatile Files and Directories.
Nov 30 15:41:52 dmgeneralov systemd[1223]: Reached target Sockets.
Nov 30 15:41:52 dmgeneralov systemd[1223]: Reached target Basic System.
Nov 30 15:41:52 dmgeneralov systemd[1223]: Reached target Main User Target.
Nov 30 15:41:52 dmgeneralov systemd[1223]: Startup finished in 281ms.
Nov 30 15:41:52 dmgeneralov systemd[1]: Started User Manager for UID 0.
Nov 30 15:41:52 dmgeneralov systemd[1]: Started Session 1 of User root.
Nov 30 15:41:52 dmgeneralov systemd[1]: Starting Hostname Service...
Nov 30 15:41:52 dmgeneralov systemd[1]: Started Hostname Service.
Nov 30 15:42:09 dmgeneralov systemd[1]: Started Getty on tty2.
Nov 30 15:42:13 dmgeneralov systemd[1]: Created slice User Slice of UID 1000.
Nov 30 15:42:13 dmgeneralov systemd[1]: Starting User Runtime Directory /run/user/1000...
Nov 30 15:42:13 dmgeneralov systemd-logind[713]: New session 3 of user dmgeneralov.
Nov 30 15:42:13 dmgeneralov systemd[1]: Finished User Runtime Directory /run/user/1000.
Nov 30 15:42:13 dmgeneralov systemd[1]: Starting User Manager for UID 1000...
Nov 30 15:42:13 dmgeneralov systemd[1258]: Queued start job for default target Main User Target.
Nov 30 15:42:13 dmgeneralov systemd[1258]: Created slice User Application Slice.
Nov 30 15:42:13 dmgeneralov systemd[1258]: Started Mark boot as successful after the user session has run 2 minutes.
Nov 30 15:42:13 dmgeneralov systemd[1258]: Started Daily Cleanup of User's Temporary Directories.
Nov 30 15:42:13 dmgeneralov systemd[1258]: Reached target Paths.
Nov 30 15:42:13 dmgeneralov systemd[1258]: Reached target Timers.
Nov 30 15:42:13 dmgeneralov systemd[1258]: Starting D-Bus User Message Bus Socket...
Nov 30 15:42:13 dmgeneralov systemd[1258]: Starting Create User's Volatile Files and Directories...
Nov 30 15:42:13 dmgeneralov systemd[1258]: Listening on D-Bus User Message Bus Socket.
Nov 30 15:42:13 dmgeneralov systemd[1258]: Reached target Sockets.
Nov 30 15:42:13 dmgeneralov systemd[1258]: Finished Create User's Volatile Files and Directories.
Nov 30 15:42:13 dmgeneralov systemd[1258]: Reached target Basic System.
Nov 30 15:42:13 dmgeneralov systemd[1258]: Reached target Main User Target.
Nov 30 15:42:13 dmgeneralov systemd[1258]: Startup finished in 153ms.
Nov 30 15:42:13 dmgeneralov systemd[1]: Started User Manager for UID 1000.
Nov 30 15:42:13 dmgeneralov systemd[1]: Started Session 3 of User dmgeneralov.
Nov 30 15:42:21 dmgeneralov su[1287]: FAILED SU (to root) dmgeneralov on tty2
Nov 30 15:42:30 dmgeneralov dmgeneralov[1290]: hello
Nov 30 15:42:43 dmgeneralov systemd[1]: systemd-hostnamed.service: Deactivated successfully.
```

Рис. 3.1: messages

Аналогично, в файле `/var/log/secure` хранятся сообщения о событиях, связан-

ных с безопасностью: например, о попытках входа в систему или использовании команды su.

```
[root@dmgeneralov ~]# tail -n 20 /var/log/secure
Nov 30 15:40:26 dmgeneralov sshd[773]: Server listening on 0.0.0.0 port 22.
Nov 30 15:40:26 dmgeneralov sshd[773]: Server listening on :: port 22.
Nov 30 15:41:51 dmgeneralov systemd[1223]: pam_unix(systemd-user:session): session opened for user root(uid=0) by (uid=0)
Nov 30 15:41:52 dmgeneralov login[778]: pam_unix(login:session): session opened for user root(uid=0) by (uid=0)
Nov 30 15:41:52 dmgeneralov login[778]: ROOT LOGIN ON tty1
Nov 30 15:42:12 dmgeneralov login[1254]: pam_unix(login:auth): user [dmgeneralov] has blank password: authenticated without it
Nov 30 15:42:13 dmgeneralov systemd[1258]: pam_unix(systemd-user:session): session opened for user dmgeneralov(uid=1000) by (uid=0)
Nov 30 15:42:13 dmgeneralov login[1254]: pam_unix(login:session): session opened for user dmgeneralov(uid=1000) by (uid=0)
Nov 30 15:42:13 dmgeneralov login[1254]: LOGIN ON tty2 BY dmgeneralov
Nov 30 15:42:19 dmgeneralov unix_chkpwd[1289]: password check failed for user (root)
Nov 30 15:42:19 dmgeneralov su[1287]: pam_unix(su:auth): authentication failure: logname=dmgeneralov uid=1000 euid=0 tty=/dev/tty2 ruser=dmgeneralov rhost= use
r=root
[root@dmgeneralov ~]# _
```

Рис. 3.2: secure

Можно настроить службы, чтобы они записывали свои события в системный лог. Например, веб-сервер httpd по умолчанию записывает свои события в файл /var/log/httpd/access_log и /var/log/httpd/error_log, но в настройках можно указать, чтобы он записывал их в системный лог. После этого нужно добавить в /etc/rsyslog.d файл, который бы описывал, что делать с записями в системный лог – в нашем случае, мы хотим сохранить их в файле /var/log/httpd-error.log


```

useradd warning: apache's uid 40 outside of the SYS_UID_MIN 201 and SYS_UID_MAX 999 range.

Installing      : httpd-fsfilesystem-2.4.53-7.el9.noarch                6/12
Installing      : rocky-logos-httpd-90.13-1.el9.noarch                7/12
Installing      : mailcap-2.1.49-5.el9.noarch                        8/12
Installing      : httpd-core-2.4.53-7.el9.x86_64                     9/12
Installing      : mod_lua-2.4.53-7.el9.x86_64                       10/12
Installing      : mod_http2-1.15.19-2.el9.x86_64                    11/12
Installing      : httpd-2.4.53-7.el9.x86_64                         12/12
Running scriptlet: httpd-2.4.53-7.el9.x86_64                        12/12
[ 492.196428] systemd-rc-local-generator[1383]: /etc/rc.d/rc.local is not marked executable, skipping.
Verifying       : mailcap-2.1.49-5.el9.noarch                        1/12
Verifying       : rocky-logos-httpd-90.13-1.el9.noarch            2/12
Verifying       : mod_lua-2.4.53-7.el9.x86_64                   3/12
Verifying       : httpd-tools-2.4.53-7.el9.x86_64               4/12
Verifying       : httpd-2.4.53-7.el9.x86_64                    5/12
Verifying       : httpd-fsfilesystem-2.4.53-7.el9.noarch        6/12
Verifying       : apr-util-openssl-1.6.1-20.el9.x86_64          7/12
Verifying       : apr-util-bdb-1.6.1-20.el9.x86_64              8/12
Verifying       : apr-util-1.6.1-20.el9.x86_64                 9/12
Verifying       : mod_http2-1.15.19-2.el9.x86_64              10/12
Verifying       : apr-1.7.0-11.el9.x86_64                     11/12
Verifying       : httpd-core-2.4.53-7.el9.x86_64              12/12

Installed:
apr-1.7.0-11.el9.x86_64      apr-util-1.6.1-20.el9.x86_64      apr-util-bdb-1.6.1-20.el9.x86_64      apr-util-openssl-1.6.1-20.el9.x86_64
httpd-2.4.53-7.el9.x86_64    httpd-core-2.4.53-7.el9.x86_64    httpd-fsfilesystem-2.4.53-7.el9.noarch  httpd-tools-2.4.53-7.el9.x86_64
mailcap-2.1.49-5.el9.noarch  mod_http2-1.15.19-2.el9.x86_64    mod_lua-2.4.53-7.el9.x86_64          rocky-logos-httpd-90.13-1.el9.noarch

Complete!
[root@dmgeneralov ~]# systemctl start httpd
[root@dmgeneralov ~]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[ 500.470443] systemd-rc-local-generator[1060]: /etc/rc.d/rc.local is not marked executable, skipping.
[root@dmgeneralov ~]# tail -f /var/log/httpd/error_log
[Wed Nov 30 15:48:34.674953 2022] [core:notice] [pid 1632:tid 1632] SELinux policy enabled: httpd running as context system_u:system_r:httpd_t:s0
[Wed Nov 30 15:48:34.677833 2022] [suexec:notice] [pid 1632:tid 1632] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this
message
[Wed Nov 30 15:48:34.714547 2022] [lbmethod:heartbeat:notice] [pid 1632:tid 1632] AH02282: No slotmem from mod_heartbeat
[Wed Nov 30 15:48:34.719833 2022] [mpm_event:notice] [pid 1632:tid 1632] AH00489: Apache/2.4.53 (Rocky Linux) configured -- resuming normal operations
[Wed Nov 30 15:48:34.719893 2022] [core:notice] [pid 1632:tid 1632] AH00694: Command line: '/usr/sbin/httpd -D FOREGROUND'
^C
[root@dmgeneralov ~]# echo 'ErrorLog syslog:local1' >> /etc/httpd/conf/httpd.conf
[root@dmgeneralov ~]# cat 'local1.*' > /var/log/httpd-error.log >> /etc/rsyslog.d/httpd.conf
cat: 'local1.*' > /var/log/httpd-error.log: No such file or directory
[root@dmgeneralov ~]# echo 'local1.*' > /var/log/httpd-error.log >> /etc/rsyslog.d/httpd.conf
[root@dmgeneralov ~]# systemctl restart rsyslog.service
[root@dmgeneralov ~]# systemctl restart httpd
[root@dmgeneralov ~]#

```

Рис. 3.3: httpd

Файлы конфигурации rsyslog описывают, какие сообщения следует записывать в какие файлы. Например, можно создать правило, которое будет сохранять все сообщения уровня debug в файл /var/log/messages-debug.

```

#Target="remote_host" Port="XXXX" Protocol="tcp")
[root@dmgeneralov ~]# echo "#debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf
[root@dmgeneralov ~]# systemctl restart rsyslogd.service
Failed to restart rsyslogd.service: Unit rsyslogd.service not found.
[root@dmgeneralov ~]# systemctl restart rsyslog.service
[root@dmgeneralov ~]# tail -f /var/log/messages-
messages-20221119 messages-20221120 messages-20221130 messages-debug
[root@dmgeneralov ~]# tail -f /var/log/messages-debug
Nov 30 15:55:16 dmgeneralov systemd[1]: Stopping System Logging Service...
Nov 30 15:55:16 dmgeneralov rsyslogd[1880]: [origin software="rsyslogd" swVersion="8.2102.0-101.el9_0.1" x-pid="1880" x-info="https://www.rsyslog.com"] exiting
on signal 15.
Nov 30 15:55:16 dmgeneralov systemd[1]: rsyslog.service: Deactivated successfully.
Nov 30 15:55:16 dmgeneralov systemd[1]: Stopped System Logging Service.
Nov 30 15:55:16 dmgeneralov systemd[1]: Starting System Logging Service...
Nov 30 15:55:16 dmgeneralov rsyslogd[2119]: [origin software="rsyslogd" swVersion="8.2102.0-101.el9_0.1" x-pid="2119" x-info="https://www.rsyslog.com"] start
Nov 30 15:55:16 dmgeneralov rsyslogd[2119]: imjournal: Journal files changed, reloading... [v8.2102.0-101.el9_0.1 try https://www.rsyslog.com/e/8 ]
Nov 30 15:55:41 dmgeneralov dmgeneralov[21251]: Daemon Debug Message

```

Рис. 3.4: debug

Программа journalctl позволяет просматривать журнал всех системных событий, а также фильтровать те события которые выводятся. Например, можно

следить в реальном времени за событиями, которые созданы процессом под пользователем root с важностью err.

```
[root@dmgeneralov ~]# journalctl -f
Nov 30 15:55:15 dmgeneralov systemd[1]: Finished Cleanup of Temporary Directories.
Nov 30 15:55:16 dmgeneralov systemd[1]: Stopping System Logging Service...
Nov 30 15:55:16 dmgeneralov rsyslogd[1888]: [origin software="rsyslogd" swVersion="8.2102.0-101.e19_0.1" x-pid="1888" x-info="https://www.rsyslog.com"] exiting
on signal 15.
Nov 30 15:55:16 dmgeneralov systemd[1]: rsyslog.service: Deactivated successfully.
Nov 30 15:55:16 dmgeneralov systemd[1]: Stopped System Logging Service.
Nov 30 15:55:16 dmgeneralov systemd[1]: Starting System Logging Service...
Nov 30 15:55:16 dmgeneralov rsyslogd[2119]: [origin software="rsyslogd" swVersion="8.2102.0-101.e19_0.1" x-pid="2119" x-info="https://www.rsyslog.com"] start
Nov 30 15:55:16 dmgeneralov systemd[1]: Started System Logging Service.
Nov 30 15:55:16 dmgeneralov rsyslogd[2119]: imjournal: journal files changed, reloading... [v0.2102.0-101.e19_0.1 try https://www.rsyslog.com/e/0 ]
Nov 30 15:55:41 dmgeneralov dmgeneralov[2125]: Daemon Debug Message
^C
[root@dmgeneralov ~]# journalctl _UID=0 -n 20
Nov 30 15:58:25 dmgeneralov systemd[1]: Stopping The Apache HTTP Server...
Nov 30 15:58:26 dmgeneralov systemd[1]: httpd.service: Deactivated successfully.
Nov 30 15:58:26 dmgeneralov systemd[1]: Stopped The Apache HTTP Server.
Nov 30 15:58:26 dmgeneralov systemd[1]: Starting The Apache HTTP Server...
Nov 30 15:58:26 dmgeneralov httpd[1889]: AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName'
Nov 30 15:58:26 dmgeneralov httpd[1889]: Server configured, listening on: port 80
Nov 30 15:58:26 dmgeneralov systemd[1]: Started The Apache HTTP Server.
Nov 30 15:55:15 dmgeneralov systemd[1]: Starting Cleanup of Temporary Directories...
Nov 30 15:55:15 dmgeneralov systemd-tmpfiles[2116]: Failed to remove "/tmp/test2", ignoring: Operation not permitted
Nov 30 15:55:15 dmgeneralov systemd-tmpfiles[2116]: Failed to remove "/tmp/test3", ignoring: Operation not permitted
Nov 30 15:55:15 dmgeneralov systemd[1]: systemd-tmpfiles-clean.service: Deactivated successfully.
Nov 30 15:55:15 dmgeneralov systemd[1]: Finished Cleanup of Temporary Directories.
Nov 30 15:55:16 dmgeneralov systemd[1]: Stopping System Logging Service...
Nov 30 15:55:16 dmgeneralov rsyslogd[1888]: [origin software="rsyslogd" swVersion="8.2102.0-101.e19_0.1" x-pid="1888" x-info="https://www.rsyslog.com"] exiting
Nov 30 15:55:16 dmgeneralov systemd[1]: rsyslog.service: Deactivated successfully.
Nov 30 15:55:16 dmgeneralov systemd[1]: Stopped System Logging Service.
Nov 30 15:55:16 dmgeneralov systemd[1]: Starting System Logging Service...
Nov 30 15:55:16 dmgeneralov rsyslogd[2119]: [origin software="rsyslogd" swVersion="8.2102.0-101.e19_0.1" x-pid="2119" x-info="https://www.rsyslog.com"] start
Nov 30 15:55:16 dmgeneralov systemd[1]: Started System Logging Service.
Nov 30 15:55:16 dmgeneralov rsyslogd[2119]: imjournal: journal files changed, reloading... [v0.2102.0-101.e19_0.1 try https://www.rsyslog.com/e/0 ]
[root@dmgeneralov ~]# journalctl -p err -n 10
-- No entries --
[root@dmgeneralov ~]#
```

Рис. 3.5: journalctl

Можно также выделить только те сообщения, которые были добавлены со вчерашнего дня (которые, в случае этой виртуальной машины, – это сообщения начиная с загрузки системы), которые имеют важность err. Можно также посмотреть каждое сообщение более подробно, используя опцию -o verbose.

```

[root@dmgeneralov ~]# journalctl --since yesterday -n 30
Nov 30 15:48:16 localhost kernel: Linux version 5.14.0-70.13.1.el9_0.x86_64 (mockbuild@dall-prod-builder001.bld.equ.rockylinux.org) (gcc (GCC) 11.2.1 20220127) #1 SMP Mon Nov 28 15:48:16 localhost kernel: The list of certified hardware and cloud instances for Red Hat Enterprise Linux 9 can be viewed at The Red Hat Ecosystem Catalog
Nov 30 15:48:16 localhost kernel: Command line: BOOT_IMAGE=qd0_mados1/vmlinuz-5.14.0-70.13.1.el9_0.x86_64 root=/dev/mapper/rh-root ro crashkernel=16-46:192M,efi
Nov 30 15:48:16 localhost kernel: x86/fpu: Supporting XSAVES feature 0x001: 'x87 floating point registers'
Nov 30 15:48:16 localhost kernel: x86/fpu: Supporting XSAVES feature 0x002: 'SSE registers'
Nov 30 15:48:16 localhost kernel: x86/fpu: Supporting XSAVES feature 0x004: 'AVX registers'
Nov 30 15:48:16 localhost kernel: x86/fpu: Supporting XSAVES feature 0x008: 'MPX bounds registers'
Nov 30 15:48:16 localhost kernel: x86/fpu: Supporting XSAVES feature 0x010: 'MPX CSR'
Nov 30 15:48:16 localhost kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
Nov 30 15:48:16 localhost kernel: x86/fpu: xstate_offset[3]: 832, xstate_sizes[3]: 64
Nov 30 15:48:16 localhost kernel: x86/fpu: xstate_offset[4]: 896, xstate_sizes[4]: 64
Nov 30 15:48:16 localhost kernel: x86/fpu: Enabled xstate features 0x1f, context size is 960 bytes, using 'compacted' format.
Nov 30 15:48:16 localhost kernel: signal: max sigframe size: 2032
Nov 30 15:48:16 localhost kernel: BIOS-provided physical RAM map:
Nov 30 15:48:16 localhost kernel: BIOS-e820: mem0 0x0000000000000000-0x0000000000000fff usable
Nov 30 15:48:16 localhost kernel: BIOS-e820: mem1 0x0000000000000fc00-0x0000000000000fff reserved
Nov 30 15:48:16 localhost kernel: BIOS-e820: mem2 0x0000000000000000-0x0000000000000fff reserved
Nov 30 15:48:16 localhost kernel: BIOS-e820: mem3 0x0000000000000000-0x0000000000000fff usable
Nov 30 15:48:16 localhost kernel: BIOS-e820: mem4 0x0000000000000000-0x0000000000000fff reserved
Nov 30 15:48:16 localhost kernel: BIOS-e820: mem5 0x0000000000000000-0x0000000000000fff reserved
Nov 30 15:48:16 localhost kernel: BIOS-e820: mem6 0x0000000000000000-0x0000000000000fff reserved
Nov 30 15:48:16 localhost kernel: BIOS-e820: mem7 0x0000000000000000-0x0000000000000fff reserved
Nov 30 15:48:16 localhost kernel: BIOS-e820: mem8 0x0000000000000000-0x0000000000000fff reserved
Nov 30 15:48:16 localhost kernel: BIOS-e820: mem9 0x0000000000000000-0x0000000000000fff reserved
Nov 30 15:48:16 localhost kernel: NX (Execute Disable) protection: active
Nov 30 15:48:16 localhost kernel: SMBIOS 2.8 present.
Nov 30 15:48:16 localhost kernel: DMI: QEMU Standard PC (Q35 + ICH9, 2009), BIOS Arch Linux 1.16.0-3-3 04/01/2014
Nov 30 15:48:16 localhost kernel: Hypervisor detected: KVM
Nov 30 15:48:16 localhost kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Nov 30 15:48:16 localhost kernel: kvm-clock: cpu 0, msr 25401001, primary cpu clock
Nov 30 15:48:16 localhost kernel: kvm-clock: using sched offset of 14540677493 cycles
[root@dmgeneralov ~]# journalctl --since yesterday -p err
-- No entries --
[root@dmgeneralov ~]# journalctl --since yesterday -n 1 -o verbose
Wed 2022-11-30 15:48:16.177694 MSK ts=707acc66451f4333b8de95a418c6cdec:i=1:b=1cd032d352414ccba242712d5b2f5b36:w=37b290:t=5eeaf6010e21e:x=5dda67fd609e6b3c]
_SOURCE MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
_PRIORITY=5
_SYSLOG_FACILITY=0
_SYSLOG_IDENTIFIER=kernel
MESSAGE=Linux version 5.14.0-70.13.1.el9_0.x86_64 (mockbuild@dall-prod-builder001.bld.equ.rockylinux.org) (gcc (GCC) 11.2.1 20220127 (Red Hat 11.2.1-9), GNU
_BOOT_ID=1cd032d352414ccba242712d5b2f5b36
_MACHINE_ID=cdffcd2cb9b4b4b7fec2021691b511
_HOSTNAME=localhost
[root@dmgeneralov ~]#

```

Рис. 3.6: journalctl

Наконец, можно выделить сообщения от какого-то конкретного сервиса, например, sshd или httpd.

```

[root@dmgeneralov ~]# journalctl _SYSTEMD_UNIT=sshd.service
Nov 30 15:48:26 dmgeneralov sshd[7731]: Server listening on 0.0.0.0 port 22.
Nov 30 15:48:26 dmgeneralov sshd[7731]: Server listening on :: port 22.
[root@dmgeneralov ~]# journalctl _SYSTEMD_UNIT=httpd.service
Nov 30 15:48:34 dmgeneralov httpd[16321]: AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName'
Nov 30 15:48:34 dmgeneralov httpd[16321]: Server configured, listening on: port 80
Nov 30 15:58:26 dmgeneralov httpd[18891]: AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName'
Nov 30 15:58:26 dmgeneralov httpd[18891]: Server configured, listening on: port 80
[root@dmgeneralov ~]#

```

Рис. 3.7: journalctl

По умолчанию журнал journald сохраняется в памяти, но можно настроить его сохранение на диск. Для этого нужно, чтобы существовала директория /var/log/journal, чтобы ей владел root:systemd-journal, и чтобы у нее были права на чтение и запись для группы systemd-journal. После этого там будут храниться журналы для каждой загрузки системы.

```
[root@dageneralov ~]# mkdir -p /var/log/journal
[root@dageneralov ~]# chown root:systemd-journal /var/log/journal
[root@dageneralov ~]# chmod 775 /var/log/journal
[root@dageneralov ~]# killall -USR1 systemd-journald
[ 1648.416288] systemd-journald[640]: Received SIGUSR1 signal from PID 2185, as request to flush runtime journal.
[root@dageneralov ~]# ls /var/log/journal/
eaffcc42cb9b4b04b7fec2821691b511
```

Рис. 3.8: journalctl

4 Выводы

Я получил опыт работы с rsyslogd и journald.

5 Контрольные вопросы

1. Какой файл используется для настройки rsyslogd?

/etc/rsyslog.conf, который подключает файлы из директории /etc/rsyslog.d/.

```
# rsyslog configuration file
# For more information see /usr/share/doc/rsyslog-*/rsyslog_conf.html
# or latest version online at http://www.rsyslog.com/doc/rsyslog_conf.html
# If you experience problems, see http://www.rsyslog.com/doc/troubleshoot.html

#### GLOBAL DIRECTIVES ####

# Where to place auxiliary files
global(workDirectory="/var/lib/rsyslog")

# Use default timestamp format
module(load="builtin:omfile" Template="RSYSLOG_TraditionalFileFormat")

# Include all config files in /etc/rsyslog.d
include(file="/etc/rsyslog.d/*.conf" mode="onetime")

#### MODULES ####

module(load="imsock" # provides support for local system logging (e.g. via logger command)
        SysSock.Use="off") # Turn off message reception via local log socket;
                           # local messages are retrieved through imjournal now.
module(load="imjournal" # provides access to the systemd journal
        StateFile="imjournal.state") # File to store the position in the journal
module(load="imklog") # reads kernel messages (the same are read from journald)
module(load="immark") # provides --MARK-- message capability

# Provides UDP syslog reception
# for parameters see http://www.rsyslog.com/doc/imudp.html
module(load="imudp") # needs to be done just once
input(type="imudp" port="514")

# Provides TCP syslog reception
# for parameters see http://www.rsyslog.com/doc/intcp.html
module(load="intcp") # needs to be done just once
input(type="intcp" port="514")

#### RULES ####

# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                          /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none      /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                     /var/log/secure

-- VISUAL LINE --
```

Рис. 5.1: rsyslog.conf

2. В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией?

/var/log/secure

```

[root@dmgeneralov ~]# cat /var/log/secure
Nov 30 15:48:26 dmgeneralov sshd(773): Server listening on 0.0.0.0 port 22.
Nov 30 15:48:26 dmgeneralov sshd(773): Server listening on :: port 22.
Nov 30 15:41:51 dmgeneralov systemd(1223): pam_unix(systemd-user:session): session opened for user root(uid=0) by (uid=0)
Nov 30 15:41:52 dmgeneralov login(778): pam_unix(login:session): session opened for user root(uid=0) by (uid=0)
Nov 30 15:41:52 dmgeneralov login(778): ROOT LOGIN ON tty1
Nov 30 15:42:12 dmgeneralov login(1254): pam_unix(login:auth): user [dmgeneralov] has blank password: authenticated without it
Nov 30 15:42:13 dmgeneralov systemd(1258): pam_unix(systemd-user:session): session opened for user dmgeneralov(uid=1000) by (uid=0)
Nov 30 15:42:13 dmgeneralov login(1254): pam_unix(login:session): session opened for user dmgeneralov(uid=1000) by (uid=0)
Nov 30 15:42:13 dmgeneralov login(1254): LOGIN ON tty2 BY dmgeneralov
Nov 30 15:42:19 dmgeneralov unix_chkpwd(12891): password check failed for user (root)
Nov 30 15:42:19 dmgeneralov su(12871): pam_unix(su:auth): authentication failure; logname=dmgeneralov uid=1000 euid=0 tty=/dev/tty2 ruser=dmgeneralov rhost= use
r=root
Nov 30 15:48:23 dmgeneralov groupadd(13411): group added to /etc/group: name=apache, GID=48
Nov 30 15:48:23 dmgeneralov groupadd(13411): group added to /etc/gshadow: name=apache
Nov 30 15:48:23 dmgeneralov groupadd(13411): new group: name=apache, GID=48
Nov 30 15:48:23 dmgeneralov useradd(13461): new user: name=apache, UID=48, GID=48, home=/usr/share/httpd, shell=/sbin/nologin, from=none
[root@dmgeneralov ~]# _

```

Рис. 5.2: secure

3. Если вы ничего не настроите, то сколько времени потребуется для ротации файлов журналов?

Одна неделя.

```

# see "man logrotate" for details
# global options do not affect preceding include directives
# rotate log files weekly
weekly
# keep 4 weeks worth of backlogs
rotate 4
# create new (empty) log files after rotating old ones
create
# use date as a suffix of the rotated file
dateext
# uncomment this if you want your log files compressed
#compress
# packages drop log rotation information into this directory
include /etc/logrotate.d
# system-specific logs may be also be configured here.

...
/etc/logrotate.conf" 23L, 496B
1.1 011

```

Рис. 5.3: logrotate.conf

4. Какую строку следует добавить в конфигурацию для записи всех сообщений с приоритетом info в файл /var/log/messages.info?

*.info /var/log/messages.info

```
[root@dmgeneralov ~]# echo "* info /var/log/messages.info" > /etc/rsyslog.d/info.conf
[root@dmgeneralov ~]# systemctl restart rsyslogd.service
Failed to restart rsyslogd.service: Unit rsyslogd.service not found.
[root@dmgeneralov ~]# systemctl restart rsyslog.service
[root@dmgeneralov ~]# cat /var/log/messages.info
Nov 30 16:14:53 dmgeneralov systemd[1]: Stopping System Logging Service...
Nov 30 16:14:53 dmgeneralov rsyslogd[2119]: forigin software="rsyslogd" swVersion="8.2102.0-101.e19_0.1" x-pid="2119" x-info="https://www.rsyslog.com" exiting
on signal 15.
Nov 30 16:14:54 dmgeneralov systemd[1]: rsyslog.service: Deactivated successfully.
Nov 30 16:14:54 dmgeneralov systemd[1]: Stopped System Logging Service.
Nov 30 16:14:54 dmgeneralov systemd[1]: Starting System Logging Service...
Nov 30 16:14:54 dmgeneralov rsyslogd[2228]: forigin software="rsyslogd" swVersion="8.2102.0-101.e19_0.1" x-pid="2228" x-info="https://www.rsyslog.com" start
Nov 30 16:14:54 dmgeneralov systemd[1]: Started System Logging Service.
Nov 30 16:14:54 dmgeneralov rsyslogd[2228]: imjournal: journal files changed, reloading... [v8.2102.0-101.e19_0.1 try https://www.rsyslog.com/e/8 ]
[root@dmgeneralov ~]#
```

Рис. 5.4: rsyslog.conf

5. Какая команда позволяет вам видеть сообщения журнала в режиме реального времени?

journalctl -f

```
[root@dmgeneralov ~]# date
Wed Nov 30 04:16:17 PM MSK 2022
[root@dmgeneralov ~]# sleep 20 && logger "Hello World!" &
[1] 2241
[root@dmgeneralov ~]# journalctl -f
Nov 30 16:07:41 dmgeneralov rsyslogd[2119]: imjournal: journal files changed, reloading... [v8.2102.0-101.e19_0.1 try https://www.rsyslog.com/e/8 ]
Nov 30 16:10:29 dmgeneralov NetworkManager[761]: (info) [1669013029.1955] dhcp4 (enp1s0): state changed new lease, address=192.168.122.107
Nov 30 16:14:53 dmgeneralov systemd[1]: Stopping System Logging Service...
Nov 30 16:14:53 dmgeneralov rsyslogd[2119]: forigin software="rsyslogd" swVersion="8.2102.0-101.e19_0.1" x-pid="2119" x-info="https://www.rsyslog.com" exiting
on signal 15.
Nov 30 16:14:54 dmgeneralov systemd[1]: rsyslog.service: Deactivated successfully.
Nov 30 16:14:54 dmgeneralov systemd[1]: Stopped System Logging Service.
Nov 30 16:14:54 dmgeneralov systemd[1]: Starting System Logging Service...
Nov 30 16:14:54 dmgeneralov rsyslogd[2228]: forigin software="rsyslogd" swVersion="8.2102.0-101.e19_0.1" x-pid="2228" x-info="https://www.rsyslog.com" start
Nov 30 16:14:54 dmgeneralov systemd[1]: Started System Logging Service.
Nov 30 16:14:54 dmgeneralov rsyslogd[2228]: imjournal: journal files changed, reloading... [v8.2102.0-101.e19_0.1 try https://www.rsyslog.com/e/8 ]
Nov 30 16:16:39 dmgeneralov root[2244]: Hello World!
-
```

Рис. 5.5: journalctl

6. Какая команда позволяет вам видеть все сообщения журнала, которые были написаны для PID 1 между 9:00 и 15:00?

journalctl _PID=1 --since "9:00" --until "15:00"

7. Какая команда позволяет вам видеть сообщения journald после последней перезагрузки системы?

journalctl -b

8. Какая процедура позволяет сделать журнал journald постоянным?

Создать директорию `/var/log/journal`, сделать ее владельцем `root:systemd-journal`, и дать права на чтение и запись для группы `systemd-journal`.

```
[root@dageneralov ~]# mkdir -p /var/log/journal
[root@dageneralov ~]# chown root:systemd-journal /var/log/journal
[root@dageneralov ~]# chmod 2755 /var/log/journal
[root@dageneralov ~]# killall -USR1 systemd-journald
[ 1648.416288] systemd-journald[648]: Received SIGUSR1 signal from PID 2185, as request to flush runtime journal.
[root@dageneralov ~]# ls /var/log/journal/
edffccd2cb9b4b04b7fec2821691b511
[root@dageneralov ~]#
```

Рис. 5.6: journalctl