Отчет о лабораторной работе

Лабораторная работа №7

Казначеев Сергей Ильич

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

2 Выполнение лабораторной работы

Для начала откроем три вклдки терминала и в каждом из них получим полномочия администратора рис. 2.1).

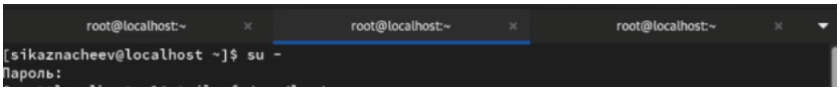

Рис. 2.1: 1

Теперь во второй вкладке пропишем команду tail -f /var/log/messages чтобы вывести события в реальном времени.После чего перейдем в 3 терминал и попробуем зайти в супер пользователя введя неправильный пароль и у нас во 2 терминале появится сообщение «FAILED SU (to root) username ...». (рис. 2.2).

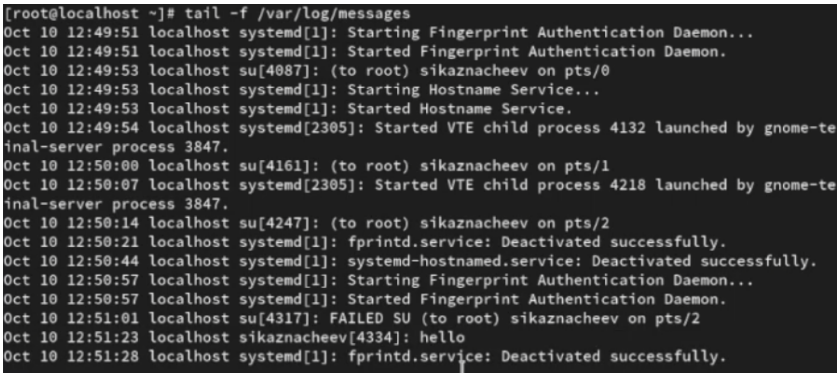

Рис. 2.2: 2

После в 3 терминале введем из оболочки пользователя logger hello (рис.2.3).

Рис. 2.3: 3

Далее открываем второй терминал и проверям то что hello записалось (рис. 2.4).

Рис. 2.4: 4

Затем введем команду tail -n 20 /var/log/secure чтобы увидить сообщения, которые ранее были зафиксированы во время ошибки (рис. 2.5).

Рис. 2.5: 5

В первой вкладке установим httpd (рис. 2.6).

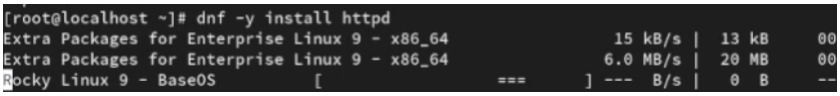

Рис. 2.6: 6

После окончания процесса установки запустим веб-службу (рис. 2.7).

Рис. 2.7: 7

После во второй вкладке терминала посмотрим журнал сообщений об ошибках веб-служб командой tail -f /var/log/httpd/error_log (рис. 2.8).

Рис. 2.8: 8

Далее в 3 терминале запишем в файл конфигурации /etc/httpd/conf/httpd.conf в конце добавим ErrorLog syslog:local1 (рис. 2.9).

Рис. 2.9: 9

После чего переходим в каталог /etc/rsyslog.d и создаем файл мониторинга событий веб-службы (рис. 2.10).

Рис. 2.10: 10

Далее открыв его на редактировании запишем local1.* -/var/log/httpd-error.log

(рис. 2.11).

Рис. 2.11: 11

После чего переходим в первую вкладку терминала и перезагружаем концигурацию rsyslogd и веб-службу (рис. 2.12).

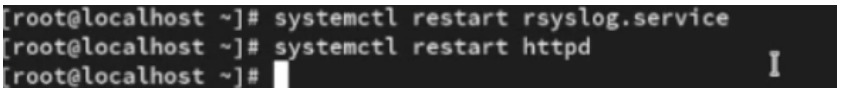

Рис. 2.12: 12

После в третьей вкладке терминала создайем отдельный файл концигурации для мониторинга отладочной информации и в том же терминале вводим echo “*.debug /var/log/messages-debug” > /etc/rsyslog.d/debug.conf

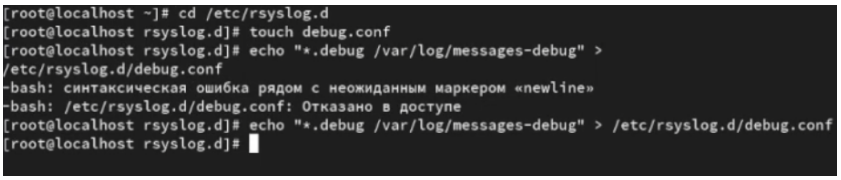

Рис. 2.13: 13

Затем в первой вкладке терминала снова перезапускаем rsyslogd (рис. 2.14).

Рис. 2.14: 14

Далее переходим во вторую вкладку терминала запускаем мониторинг отладочной информации tail -f /var/log/messages-debug (рис. 2.15).

Рис. 2.15: 15

Далее в третьей вкладке терминала введем logger -p daemon.debug “Daemon Debug Message”

Рис. 2.16: 16

Проверим это (рис. 2.17).

Рис. 2.17: 17

Во второй вкладке терминала посмотрим содержимое журнала с событиями с момента последнего запуска системы (рис. 2.18).

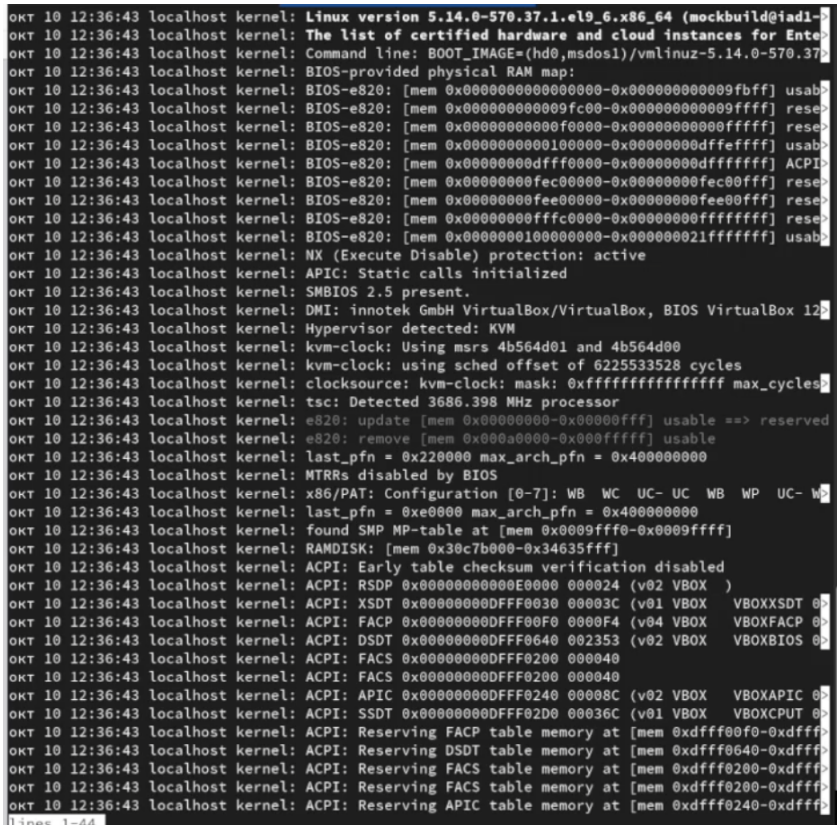

Рис. 2.18: 18

Затем просмотрим содержимое журнала без использования пейджера командой journalctl –no-pager и просмотрим журнал в реальном времени journalctl -f

(рис. 2.19).

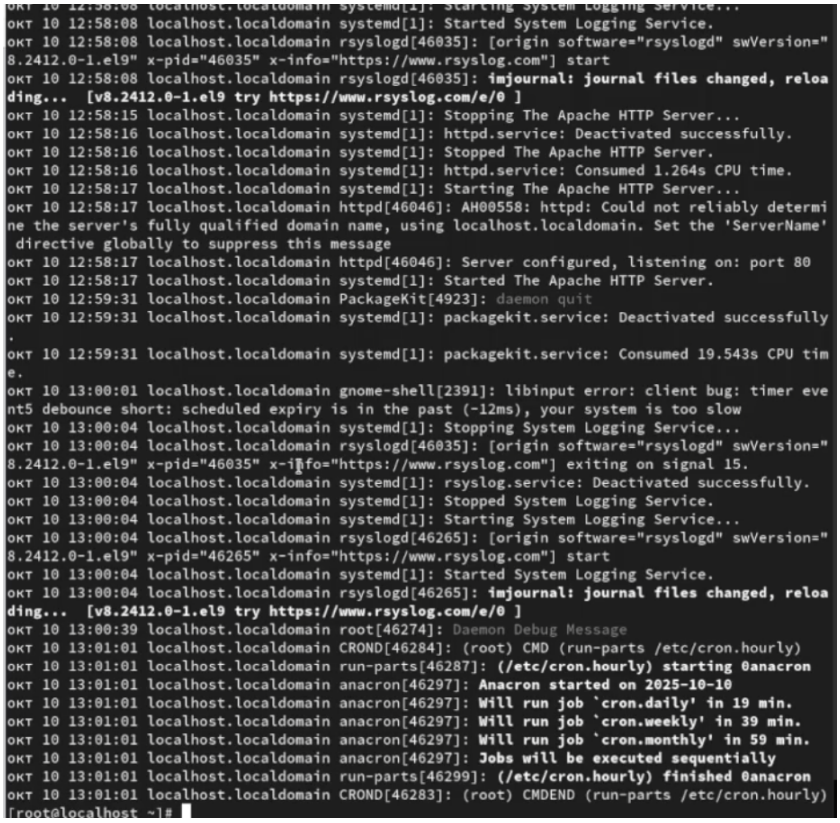

Рис. 2.19: 19

После чего используем фильтрацию просмотра конкретных параметров журнала введя команду journalctl и дважды нажав на tab

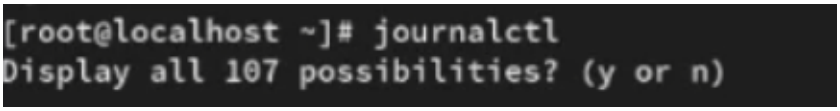

Рис. 2.20: 20

Пробуем просмотреть события для uid0

Рис. 2.21: 21

После чего запустим journalctl -n 20 для просмотра только сообщений об ошибке используем комаду journalctl -p err

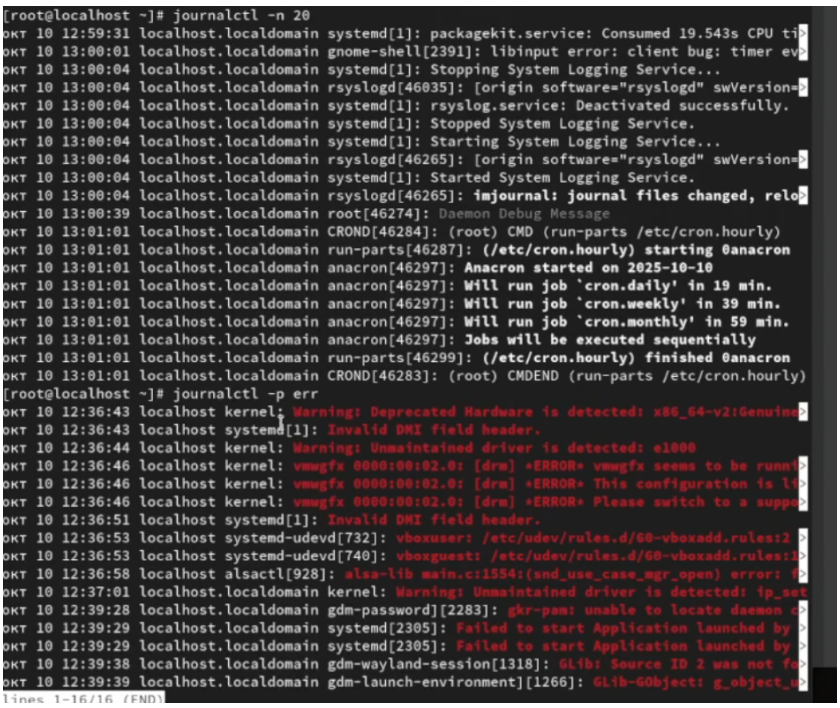

Рис. 2.22: 22

Теперь просмотрим сообщейния вчерашнего дня введя команду journalctl –since yesterday

Рис. 2.23: 23

Затем выведем все сообщения с ошибкой приоритета которые были зафиксированы со вчерашнего дня

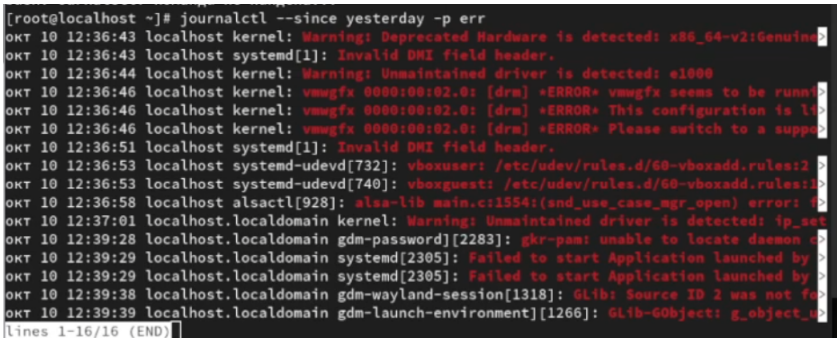

Рис. 2.24: 24

Затем выведем детальную информацию с помощью команды journalctl -o verbose

Рис. 2.25: 25

Далее просмотрим дополнительную информацию о модуле sshd введя команду journalctl _SYSTEMD_UNIT=sshd.service

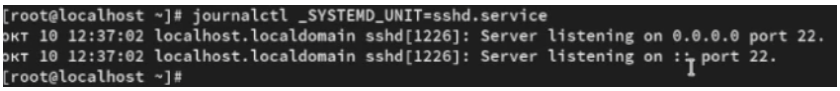

Рис. 2.26: 26

После чего откроем новый терминла и создадим новый каталог и скорректируем его права доступа для каталога /var/log/journal, чтобы journald смог записывать в него информацию и для принятия изменений необходимо перезагрузить систему или использовать команду killall SR1 systemd-journald

Рис. 2.27: 27

Теперь журнал systemd теперь постоянный и можем проверить это командой journalctl -b


Linux version 5.14.0-570.37.1.el9_6.x86_64 (mockbuild@iad1-prod-build001.bld.equ.ro
The list of certified hardware and cloud instances for Enterprise Linux 9 can be vi
Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-570.37.1.el9_6.x86_64 root=/de
BIOS-provided physical RAM map:
BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
BIOS-e820: [mem 0x0000000000100000-0x00000000dffeffff] usable
BIOS-e820: [mem 0x00000000dfff0000-0x00000000dfffffff] ACPI data
BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
BIOS-e820: [mem 0x0000000100000000-0x000000021fffffff] usable
NX (Execute Disable) protection: active
APIC: Static calls initialized
SMBIOS 2.5 present.
DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Hypervisor detected: KVM
kvm-clock: Using msrs 4b564d01 and 4b564d00
kvm-clock: using sched offset of 6225533528 cycles
clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_idl
tsc: Detected 3686.398 MHz processor
e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
e820: remove [mem 0x000a0000-0x000fffff] usable
last_pfn = 0x220000 max_arch_pfn = 0x400000000
MTRRs disabled by BIOS
x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT
last_pfn = 0xe0000 max_arch_pfn = 0x400000000
found SMP MP-table at [mem 0x0009fff0-0x0009ffff]
RAMDISK: [mem 0x30c7b000-0x34635fff]
ACPI: Early table checksum verification disabled
ACPI: RSDP 0x00000000000E0000 000024 (v02 VBOX)
ACPI: XSDT 0x00000000DFFF0030 00003C (v01 VBOX VBOXXSDT 00000001 ASL 00000061)
ACPI: FACP 0x00000000DFFF00F0 0000F4 (v04 VBOX VBOXFACP 00000001 ASL 00000061)
ACPI: DSDT 0x00000000DFFF0640 002353 (v02 VBOX VBOXBIOS 00000002 INTL 20100528)
ACPI: FACS 0x00000000DFFF0200 000040
ACPI: FACS 0x00000000DFFF0200 000040
ACPI: APIC 0x00000000DFFF0240 00008C (v02 VBOX VBOXAPIC 00000001 ASL 00000061)
ACPI: SSDT 0x00000000DFFF02D0 00036C (v01 VBOX VBOXCPUT 00000002 INTL 20100528)
ACPI: Reserving FACP table memory at [mem 0xdfff00f0-0xdfff01e3]
ACPI: Reserving DSDT table memory at [mem 0xdfff0640-0xdfff2992]
ACPI: Reserving FACS table memory at [mem 0xdfff0200-0xdfff023f]
ACPI: Reserving FACS table memory at [mem 0xdfff0200-0xdfff023f]
ACPI: Reserving APIC table memory at [mem 0xdfff0240-0xdfff02cb]
ACPI: Reserving SSDT table memory at [mem 0xdfff02d0-0xdfff063b]
No NUMA configuration found
Faking a node at [mem 0x0000000000000000-0x000000021fffffff]
NODE_DATA(0) allocated [mem 0x21ffd1000-0x21fffbfff]
crashkernel reserved: 0x00000000cf000000 - 0x00000000df000000 (256 MB)
Zone ranges:
DMA [mem 0x0000000000001000-0x0000000000ffffff]
DMA32 [mem 0x0000000001000000-0x00000000ffffffff]
Normal [mem 0x0000000100000000-0x000000021fffffff]
Device empty
Movable zone start for each node

Рис. 2.28: 27

3 Контрольные вопросы

1. Какой файл используется для настройки rsyslogd?

Ответ - файл /etc/rsyslog.conf

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

Ответ - файл журнала айнтефекации /var/log/auth.log

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

Ответ - период ротации журналов по умолчанию раз в неделю

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

Ответ - строку /var/log/message.info

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

Ответ - команда tail -f /var/log/syslog

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

Ответ - команада journalctl _PID=1 –since “9:00” –until “15:00”

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

Ответ - команда journalctl -b

8. Какая процедура позволяет сделать журнал journald постоянным?

Ответ - команда создать каталог и перезапустить службу mkdir -p /var/log/journal systemctl restart systemd-journald

4 Выводы

В результате выполнения лабораторной работы я получил навыки работы с журналами мониторинга различных событий в системе