

# Лабораторная работа №15

## Настройка сетевого журналирования

Газизянов Владислав Альбертович

2025-12-13

# Содержание I

## 1. Цели и задачи

**Цель:** Получение навыков работы с журналами системных событий и настройки централизованного журналирования

**Задачи:** - Настройка сервера сетевого журналирования - Конфигурация клиентов для передачи логов - Использование инструментов анализа журналов - Автоматизация развертывания системы

## 2. Настройка сервера журналирования

**Конфигурация rsyslog:** - Создание конфигурационных файлов - Активация TCP-приёмника на порту 514 - Перезапуск службы rsyslog - Проверка работы сервера

```
GNU nano 8.1                               /etc/rsyslog.d/netlog-server.conf
$ModLoad imtcp
$InputTCPServerRun 514
```

Рисунок 1: Конфигурация TCP-приёмника rsyslog

### 3. Сетевая безопасность

**Настройка firewall:** - Открытие TCP-порта 514 - Добавление постоянных правил - Проверка доступности сервера - Обеспечение защищённого обмена

```
*:shell (LISTEN)
[root@server.vagazizianov.net rsyslog.d]# firewall-cmd --add-port=514/tcp
success
[root@server.vagazizianov.net rsyslog.d]# firewall-cmd --add-port=514/tcp --permanent
success
```

Рисунок 2: Настройка firewall для сетевого журналирования

## 4. Клиентская конфигурация

**Перенаправление логов:** - Создание клиентских конфигураций - Настройка отправки сообщений на сервер - Перезапуск клиентских служб - Проверка соединения с сервером

```
GNU nano 8.1          /etc/rsyslog.d/netlog-client.conf
*.* @@server.vagazizia.net:514
```

Рисунок 3: Настройка перенаправления логов на сервер

## 5. Мониторинг журналов в реальном времени

**Отслеживание событий:** - Использование команды tail -f - Анализ сообщений от разных хостов - Выявление системных проблем - Мониторинг работы служб

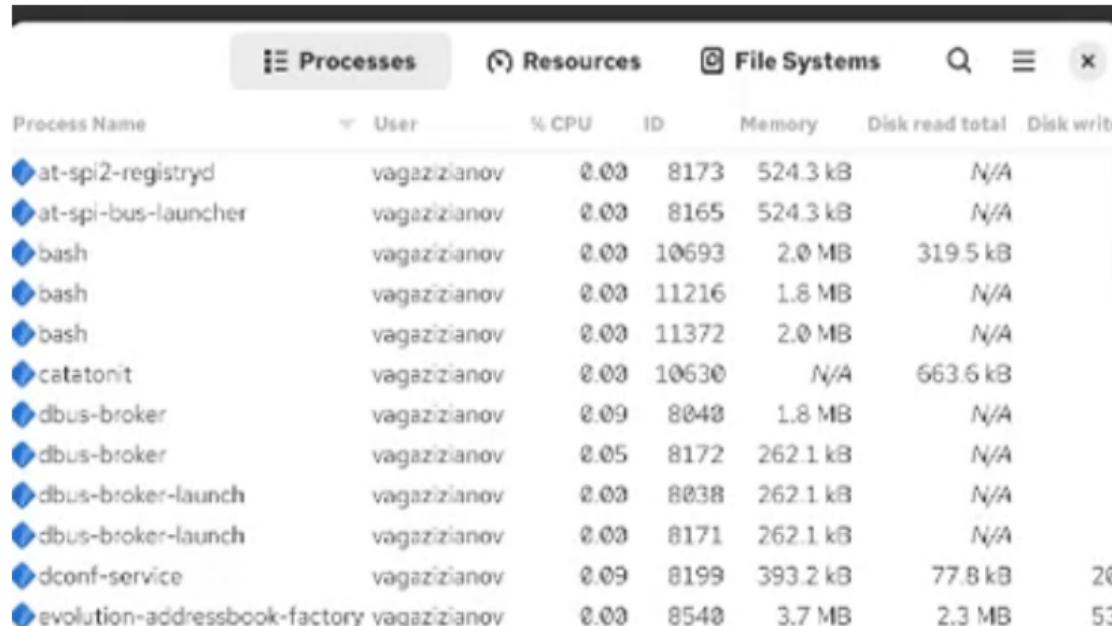
```
[sudo] password for vagazizianov.
[root@server.vagazizianov.net ~]# tail -f /var/log/messages
Dec 13 07:47:31 server systemd[1]: Started systemd-hostnamed.service - Hostname Service.
Dec 13 07:47:31 client ptyxism[10742]: context mismatch in svga_surface_destroy
Dec 13 07:47:31 client ptyxism[10742]: context mismatch in svga_surface_destroy
Dec 13 07:47:31 client ptyxism[10742]: context mismatch in svga_surface_destroy
Dec 13 07:47:31 client ptyxism[10742]: context mismatch in svga_surface_destroy
Dec 13 07:47:31 server systemd-coredump[11275]: Process 11265 (VBoxClient) of user 1001 dumped core.
#012#012Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64#012Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64#012Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64#012Module libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#012Stack trace of thread 11268:#012#0 0x000000000041db4b n/a (n/a + 0x0)#012#1 0x00000000000041dac4 n/a (n/a + 0x0)#012#2 0x0000000000450a8c n/a (n/a + 0x0)#012#3 0x0000000000435890 n/a (n/a + 0x0)#012#4 0x00007ff4ff231b68 start_thread (libc.so.6 + 0x94b68)#012#5 0x00007ff4ff2a26bc __clone3 (libc.so.6 + 0x1056bc)#012#012Stack trace of thread 11265:#012#0 0x00007ff4ff2a04bd syscall (libc.so.6 + 0x1034bd)#012#1 0x00000000004347a2 n/a (n/a + 0x0)#012#2 0x00000000004506d6 n/a (n/a + 0x0)#012#3 0x0000000000405123 n/a (n/a + 0x0)#012#4 0x00007ff4ff1c730e __libc_start_main (libc.so.6 + 0x2a30e)#012#5 0x00007ff4ff1c73c9 __libc_start_main@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Dec 13 07:47:31 server systemd[1]: systemd-coredump@150-11271-0.service: Deactivated successfully.
Dec 13 07:47:32 client kernel: traps: VBoxClient[11139] trap int3 ip:41db4b sp:7f32458b6cd0 error:0 in VBoxClient[1db4b,400000+bb000]
Dec 13 07:47:32 client systemd-coredump[11140]: Process 11136 (VBoxClient) of user 1001 terminated abnormally with signal 5/Trap, processing...
```

Рисунок 4: Мониторинг журнала сообщений в реальном времени



## 6. Графические инструменты анализа

**Использование системного монитора:** - Запуск gnome-system-monitor -  
 Просмотр различных категорий событий - Анализ сообщений от клиентов -  
 Визуализация системной информации



The screenshot shows a window titled "gnome-system-monitor" with a tab bar at the top containing "Processes", "Resources", "File Systems", a search icon, and a close button. The "Processes" tab is selected. Below the tabs is a table with the following columns: Process Name, User, % CPU, ID, Memory, Disk read total, and Disk write.

Process Name	User	% CPU	ID	Memory	Disk read total	Disk write
at-spi2-registryd	vagazizianov	0.03	8173	524.3 kB	N/A	
at-spi-bus-launcher	vagazizianov	0.03	8165	524.3 kB	N/A	
bash	vagazizianov	0.03	10693	2.0 MB	319.5 kB	
bash	vagazizianov	0.03	11216	1.8 MB	N/A	
bash	vagazizianov	0.03	11372	2.0 MB	N/A	
catatonit	vagazizianov	0.03	10630	N/A	663.6 kB	
dbus-broker	vagazizianov	0.09	8048	1.8 MB	N/A	
dbus-broker	vagazizianov	0.05	8172	262.1 kB	N/A	
dbus-broker-launch	vagazizianov	0.03	8038	262.1 kB	N/A	
dbus-broker-launch	vagazizianov	0.03	8171	262.1 kB	N/A	
dconf-service	vagazizianov	0.09	8199	393.2 kB	77.8 kB	20
evolution-addressbook-factory	vagazizianov	0.03	8548	3.7 MB	2.3 MB	53

## 7. Установка специализированных инструментов

**Расширенные возможности анализа:** - Установка просмотрщика lnav - Настройка цветового выделения - Использование фильтров и поиска - Анализ структурированных логов

```
success
[root@server.vagazizianov.net rsyslog.d]# dnf -y install lnav
Extra Packages for Enterprise Linux 7.3 [    ==   ] --- B/s | 0 B --:-- ETA
```

Рисунок 6: Установка просмотрщика журналов lnav

## 8. Продвинутый анализ журналов

## **Работа с I nav: - Просмотр и фильтрация сообщений - Анализ временных меток - Поиск ошибок и предупреждений - Мониторинг сетевой активности**

```
[root@samevag:~]# tail -f /var/log/messages
root@samevag:~]# tail -f /var/log/messages
root@server ~]# sudo -i
vagelislaran@server ~]# gnome-system-monitor
vagelislaran@server ~]#
ture: AMD x86_64
Dec 13 09:00:40 client systemd[1]: systemd-coredump@976-21354-0.service: Deactivated successfully
Dec 13 09:00:43 server systemd-coredump[143075]: Process 143063 (VBoxClient) of user 1001 dumped core
.#012#012Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012Module libxcb.so.1 from rpm libXau-1.17-0.3.el10.x86_64#012Module libX11.so.6 from rpm libX11-1.8-10-1.el10.x86_64#012Stack trace of thread 143066:#012#0 0x000000000041db4b n/a (n/a + 0x0)#012#1 0x000000000041dc4c n/a (n/a + 0x0)#012#2 0x0000000000453890 n/a (n/a + 0x0)#012#3 0x0000000000453890 n/a (n/a + 0x0)#012#4 0x000000fffe31b68 pthread_cancel@GLIBC_2.2.5 (libc.so.6 + 0x9b68)@012#0 0x012#1 0x012#2 Stack trace of thread 143063:#012#0 0x00007ff4ff2a04bd preadv64v2 (libc.so.6 + 0x1024bd)@012#0 0x012#1 0x012#2 Stack trace of thread 143065:#012#0 0x7fff4ff2a04bd preadv64v2 (libc.so.6 + 0x1024bd)@012#0 0x012#1 0x012#2 Stack trace of thread 143064:#012#0 0x0000fffa2a04bd preadv64v2 (libc.so.6 + 0x1024bd)@012ELF object binary architecture: AMD x86_64
Dec 13 09:00:43 server systemd[1]: systemd-coredump@834-143067-0.service: Deactivated successfully
Dec 13 09:00:45 client systemd: traps: VBoxClient[21364] trap int3 ip:41db4b sp:7f32458b6cd0 error in VBoxClient[1db4b, 400000+b000]
Dec 13 09:00:45 client systemd-coredump[21365]: Process 21361 (VBoxClient) of user 1001 terminated normally with signal 5/TRAP, processing...
Dec 13 09:00:45 client systemd[1]: Started systemd-coredump@977-21365-0.service - Process Core Dump PID 21365(UID 0).
Dec 13 09:00:45 client systemd-coredump[21366]: Process 21361 (VBoxClient) of user 1001 dumped core
.#012#012Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012Module libxcb.so.1 from rpm libXau-1.17-0.3.el10.x86_64#012Module libX11.so.6 from rpm libX11-1.8-10-1.el10.x86_64#012Module libffbfi.so.1 from rpm libffbfi-3.4-4.9-el10.x86_64#012Module libwayland-client.so.0 from rpm wayland-1.23-0.2.el10.x86_64#012Stack trace of thread 21366:#012#0 0x000000000041db4b n/a (n/a + 0x0)#012#1 0x000000000041dc4c n/a (n/a + 0x0)#012#2 0x0000000000453890 n/a (n/a + 0x0)#012#3 0x0000000000453890 n/a (n/a + 0x0)#012#4 0x0000007f3253f5fb68 start_thread (libc.so.6 + 0x9b68)@012#5 0x0000007f3253fd06bc __clone (libc.so.6 + 0x1056bc)@012#0 0x0000007f3253fc4eb4 syscall (libc.so.6 + 0x1034bd)@012#1 0x00000000004340f n/a (n/a + 0x0)#012#2 0x000000000045126b n/a (n/a + 0x0)#012#3 0x000000000043592n/a (n/a + 0x0)#012#4 0x0000000000450a8c n/a (n/a + 0x0)#012#5 0x000000435890 n/a (n/a + 0x0)#012#6 0x0000007f3253f5fb68 start_thread (libc.so.6 + 0x9b68)@012#7 0x00000053fd06bc __clone3 (libc.so.6 + 0x1056bc)@012#0 0x0000007f3253fd06bc __clone3 (libc.so.6 + 0x1034bd)@012#1 0x000000000043472 n/a (n/a + 0x0)#012#2 0x0000000000450a8c n/a (n/a + 0x0)#012#3 0x0000000000416449 n/a (n/a + 0x0)#012#4 0x00000000004181ca n/a (n/a + 0x0)
```

## 9. Автоматизация развертывания

**Скрипты provisioning:** - Разработка скриптов для сервера и клиентов -  
Автоматическая настройка конфигураций - Интеграция с системой виртуализации -  
Тестирование работы автоматизации

```
GNU nano 8.1                                     netlog.sh
#!/bin/bash
echo "Provisioning script $0"
echo "Copy configuration files"
cp -R /vagrant/provision/server/netlog/etc/* /etc
restorecon -vR /etc
echo "Configure firewall"
firewall-cmd --add-port=514/tcp
firewall-cmd --add-port=514/tcp --permanent
echo "Start rsyslog service"
systemctl restart rsyslog
```

Рисунок 8: Скрипт настройки сервера журналирования

## 10. Выводы

**Результаты работы:** - Освоена настройка сервера сетевого журналирования -  
Приобретён опыт конфигурации клиентских устройств - Изучены инструменты  
анализа системных логов - Разработана система автоматизации развертывания -  
Освоены методы диагностики на основе журналов - Получены навыки обеспечения  
безопасности журналирования