Настройка сетевого журналирования

Лабораторная работа №15

Элсаиед Адел

7 января 2026

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Цель лабораторной работы

Получение практических навыков настройки и использования журналов системных событий, а также организации централизованного сетевого журналирования на базе rsyslog.

Выполнение работы

Конфигурация rsyslog

- Создан отдельный конфигурационный файл для сетевого журналирования
- Включён приём сообщений по TCP
- Использован стандартный порт 514

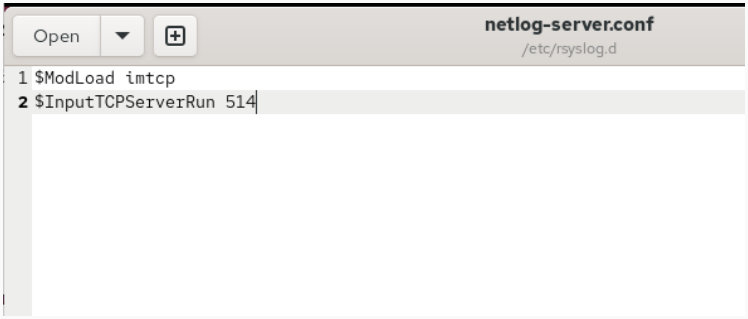


Рис. 1: Настройка приёма журналов по TCP

Настройка межсетевого экрана

- Разрешён входящий трафик на TCP-порт 514
- Правила добавлены во временную и постоянную конфигурацию
- Обеспечена доступность сервера после перезагрузки

```
smbd[192. 18952                    elsaiedadel   33u     IPv4            120104       0t0       TCP www.elsaiedadel.
net:microsoft-ds->client.elsaiedadel.net:47188 (ESTABLISHED)
rsyslogd  20540                          root    4u     IPv4            146032       0t0       TCP *:shell (LISTEN)
rsyslogd  20540                          root    5u     IPv6            146033       0t0       TCP *:shell (LISTEN)
rsyslogd  20540 20543 in:imjour          root    4u     IPv4            146032       0t0       TCP *:shell (LISTEN)
rsyslogd  20540 20543 in:imjour          root    5u     IPv6            146033       0t0       TCP *:shell (LISTEN)
rsyslogd  20540 20544 in:imtcp           root    4u     IPv4            146032       0t0       TCP *:shell (LISTEN)
rsyslogd  20540 20544 in:imtcp           root    5u     IPv6            146033       0t0       TCP *:shell (LISTEN)
rsyslogd  20540 20545 w0/imtcp           root    4u     IPv4            146032       0t0       TCP *:shell (LISTEN)
rsyslogd  20540 20545 w0/imtcp           root    5u     IPv6            146033       0t0       TCP *:shell (LISTEN)
rsyslogd  20540 20546 w1/imtcp           root    4u     IPv4            146032       0t0       TCP *:shell (LISTEN)
rsyslogd  20540 20546 w1/imtcp           root    5u     IPv6            146033       0t0       TCP *:shell (LISTEN)
rsyslogd  20540 20547 rs:main            root    4u     IPv4            146032       0t0       TCP *:shell (LISTEN)
rsyslogd  20540 20547 rs:main            root    5u     IPv6            146033       0t0       TCP *:shell (LISTEN)
[root@server.elsaiedadel.net rsyslog.d]# firewall-cmd --add-port=514/tcp
success
[root@server.elsaiedadel.net rsyslog.d]# firewall-cmd --add-port=514/tcp --permanent
success
[root@server.elsaiedadel.net rsyslog.d]#
```

Рис. 2: Настройка firewall

Конфигурация клиента

- Создан файл конфигурации rsyslog клиента
- Настроена пересылка всех сообщений на сервер
- Использован TCP-протокол для надёжной доставки

Рис. 3: Настройка клиента rsyslog

Анализ логов на сервере

- Выполнен просмотр системных журналов
- Зафиксированы сообщения от сервера и клиента
- Подтверждена корректная идентификация хостов

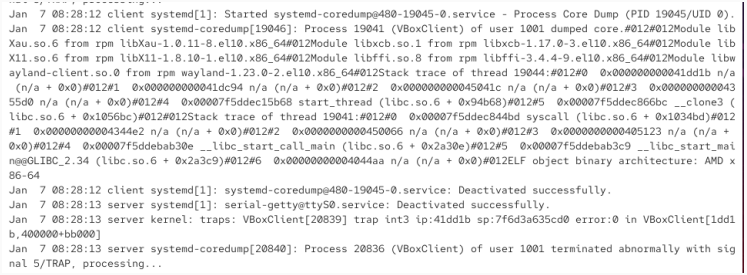
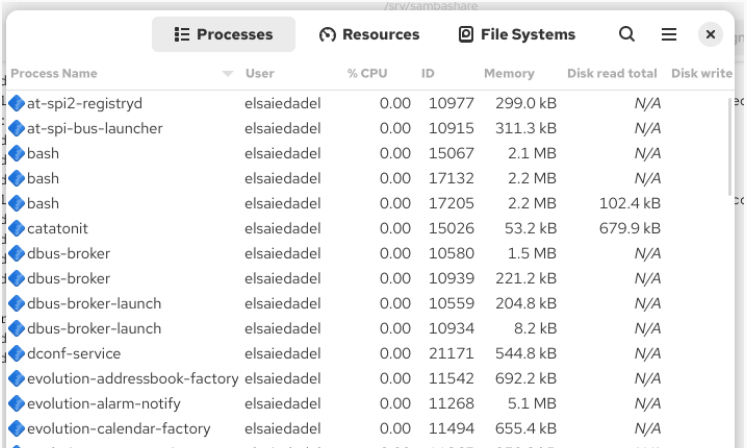


Рис. 4: Просмотр журналов

Мониторинг состояния системы

- Использован графический монитор ресурсов
- Проанализированы процессы и нагрузка CPU
- Оценено использование памяти и файловых систем



Подготовка server provisioning

```
[root@server.elsaiedadel.net rsyslog.d]#
[root@server.elsaiedadel.net rsyslog.d]# cd /vagrant/provision/server/
[root@server.elsaiedadel.net server]# mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server.elsaiedadel.net server]# cp -R /etc/rsyslog.d/netlog-server.conf /vagrant/provision/server/netlog/etc/rsy
slog.d
[root@server.elsaiedadel.net server]# touch netlog.sh
[root@server.elsaiedadel.net server]# chmod +x netlog.sh
[root@server.elsaiedadel.net server]#
```

Рис. 6: Provision server

Provisioning-скрипт сервера

Vagrantfile | smb.sh | smb.sh | 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
```

Рис. 7: netlog.sh server

Provisioning клиента

Vagrantfile | smb.sh | smb.sh | netlog.sh | netlog.sh

```
1  #!/bin/bash
2  echo "Provisioning script $0"
3  echo "Install needed packages"
4  dnf -y install lnav
5  echo "Copy configuration files"
6  cp -R /vagrant/provision/client/netlog/etc/* /etc
7  restorecon -vR /etc
8  echo "Start rsyslog service"
9  systemctl restart rsyslog
10
```

Рис. 8: netlog.sh client

Выводы

Итоги работы

- Настроено централизованное сетевое журналирование
- Реализована клиент-серверная модель rsyslog
- Выполнена автоматизация конфигурации с помощью Vagrant
- Обеспечена воспроизводимость и масштабируемость решения