Отчёт по лабораторной работе №15

Дисциплина: Администрирование сетевых подсистем

Ибрахим Мохсейн Алькамаль

Содержание

# 1. Цель работы

Получение навыков по работе с журналами системных событий.

# 2. Выполнение лабораторной работы

## 2.1 Настройка сервера сетевого журнала

В каталоге /etc/rsyslog.d на сервере создан файл конфигурации netlog-server.conf для настройки сетевого хранения журналов ([рис. 1](#fig-1)). Команды cd /etc/rsyslog.d и touch netlog-server.conf обеспечивают размещение и создание нового конфигурационного файла.

|  |
| --- |
| Рисунок 1: Создание файла конфигурации rsyslog netlog-server.conf |

В файле /etc/rsyslog.d/netlog-server.conf включён приём журналов по TCP-порту 514 посредством загрузки модуля imtcp и активации сервера ввода ($ModLoad imtcp, $InputTCPServerRun 514) ([рис. 2](#fig-2)). Данные директивы активируют обработку входящих TCP-соединений службой rsyslog.

|  |
| --- |
| Рисунок 2: Настройка приёма журналов по TCP 514 в rsyslog |

После перезапуска службы rsyslog выполнена проверка прослушиваемых TCP-портов с использованием lsof | grep TCP ([рис. 3](#fig-3)). В выводе отображается процесс rsyslog, находящийся в состоянии LISTEN, что подтверждает активацию TCP-приёма.

|  |
| --- |
| Рисунок 3: Проверка прослушиваемых TCP-портов службой rsyslog |

На сервере настроен межсетевой экран для разрешения входящих соединений по TCP-порту 514 с помощью команд firewall-cmd --add-port=514/tcp и firewall-cmd --add-port=514/tcp --permanent ([рис. 4](#fig-4)). Это обеспечивает как временное, так и постоянное открытие порта для приёма сетевых сообщений журнала.

|  |
| --- |
| Рисунок 4: Настройка firewalld для открытия TCP-порта 514 |

## 2.2 Настройка клиента сетевого журнала

В каталоге /etc/rsyslog.d на клиенте создан файл конфигурации netlog-client.conf для настройки сетевой отправки журналов ([рис. 5](#fig-5)). Команды cd /etc/rsyslog.d и touch netlog-client.conf обеспечивают размещение и создание конфигурационного файла клиента.

|  |
| --- |
| Рисунок 5: Создание файла конфигурации netlog-client.conf на клиенте |

В файле /etc/rsyslog.d/netlog-client.conf настроено перенаправление всех сообщений журнала на TCP-порт 514 сервера с использованием строки \*.\* @@server.alkamal.net:514 ([рис. 6](#fig-6)). Символы @@ указывают на передачу сообщений по протоколу TCP.

|  |
| --- |
| Рисунок 6: Настройка перенаправления журналов на сервер по TCP 514 |

После внесения изменений выполнен перезапуск службы rsyslog командой systemctl restart rsyslog, что применяет новую конфигурацию клиента.

## 2.3 Просмотр журнала

На сервере выполнен просмотр файла системного журнала /var/log/messages с использованием команды tail -f ([рис. 7](#fig-7)). В выводе отображаются сообщения служб rsyslog, systemd, а также указаны имена хостов client и server, что подтверждает поступление удалённых записей журнала.

|  |
| --- |
| Рисунок 7: Просмотр журнала /var/log/messages на сервере |

Под пользователем alkamal на сервере запущена графическая программа мониторинга системы gnome-system-monitor ([рис. 8](#fig-8)). Интерфейс отображает активные процессы, их идентификаторы, использование CPU и памяти.

|  |
| --- |
| Рисунок 8: Запуск gnome-system-monitor на сервере |

На сервере установлен просмотрщик системных журналов lnav с помощью пакетного менеджера dnf ([рис. 9](#fig-9)). В выводе подтверждена успешная установка пакета версии 0.11.1-1.el9 из репозитория epel.

|  |
| --- |
| Рисунок 9: Установка lnav на сервере |

Просмотр журналов на сервере выполнен с использованием lnav ([рис. 10](#fig-10)). В интерфейсе отображаются записи как локального сервера, так и клиента, включая сообщения служб systemd, rsyslog, cupsd и других.

|  |
| --- |
| Рисунок 10: Просмотр журналов сервера в lnav |

На клиенте выполнена установка пакета lnav командой dnf -y install lnav ([рис. 11](#fig-11)). Вывод подтверждает загрузку и подготовку к установке пакета.

|  |
| --- |
| Рисунок 11: Установка lnav на клиенте |

На клиенте выполнен просмотр системных журналов с помощью lnav ([рис. 12](#fig-12)). В журнале отображаются записи служб клиента (systemd, rsyslog, packagekit), что подтверждает корректную работу локального логирования и передачу сообщений на сервер.

|  |
| --- |
| Рисунок 12: Просмотр журналов клиента в lnav |

## 2.4 Внесение изменений в настройки внутреннего

На виртуальной машине server выполнен переход в каталог /vagrant/provision/server, создан каталог netlog/etc/rsyslog.d и скопирован файл конфигурации netlog-server.conf для последующего автоматического развёртывания ([рис. 13](#fig-13)). Команды mkdir -p и cp -R обеспечивают формирование структуры каталогов и размещение конфигурационного файла в директории provisioning.

|  |
| --- |
| Рисунок 13: Создание каталога netlog и копирование конфигурации rsyslog |

В каталоге /vagrant/provision/server создан исполняемый скрипт netlog.sh, которому назначены права выполнения, и в него добавлен сценарий автоматической настройки ([рис. 14](#fig-14)). Скрипт выполняет копирование конфигурационных файлов в /etc, восстановление контекстов SELinux (restorecon -vR /etc), открытие TCP-порта 514 в firewalld и перезапуск службы rsyslog, что обеспечивает автоматизацию настройки сетевого журнала.

|  |
| --- |
| Рисунок 14: Содержимое скрипта netlog.sh для автоматической настройки |

На виртуальной машине client выполнен переход в каталог /vagrant/provision/client, создан каталог netlog/etc/rsyslog.d и скопирован файл конфигурации netlog-client.conf для последующего автоматического развёртывания ([рис. 15](#fig-15)). Команды mkdir -p и cp -R обеспечивают формирование структуры каталогов и размещение конфигурационного файла клиента.

|  |
| --- |
| Рисунок 15: Создание каталога netlog и копирование конфигурации клиента |

В каталоге /vagrant/provision/client создан исполняемый файл netlog.sh, которому назначены права выполнения, и в него добавлен сценарий автоматической настройки клиента ([рис. 16](#fig-16)). Скрипт выполняет установку пакета lnav, копирование конфигурационных файлов в /etc, восстановление контекстов SELinux и перезапуск службы rsyslog.

|  |
| --- |
| Рисунок 16: Содержимое скрипта netlog.sh на клиенте |

В конфигурационном файле Vagrantfile в разделе сервера добавлен блок автоматического выполнения скрипта provision/server/netlog.sh при загрузке виртуальной машины ([рис. 17](#fig-17)). Параметр preserve\_order: true обеспечивает сохранение последовательности выполнения provisioning-скриптов.

|  |
| --- |
| Рисунок 17: Добавление provisioning для сервера в Vagrantfile |

Аналогичный блок добавлен в разделе клиента для автоматического запуска скрипта provision/client/netlog.sh при старте виртуальной машины ([рис. 18](#fig-18)). Это обеспечивает применение настроек сетевого журналирования на обеих машинах при их инициализации.

|  |
| --- |
| Рисунок 18: Добавление provisioning для клиента в Vagrantfile |

# 3. Выводы

В ходе работы выполнена настройка централизованного сетевого журналирования на базе rsyslog с использованием TCP-порта 514. На сервере организован приём журналов по протоколу TCP и настроено разрешение соответствующего порта в межсетевом экране. На клиенте реализовано перенаправление всех сообщений журнала на сервер.

Корректность конфигурации подтверждена просмотром файла /var/log/messages, где зафиксированы записи как локального сервера, так и удалённого клиента. Использование утилиты lnav позволило проанализировать системные сообщения в удобном интерактивном режиме.

Дополнительно реализована автоматизация развёртывания конфигурации посредством provisioning-скриптов netlog.sh и интеграции их в Vagrantfile, что обеспечивает воспроизводимость и автоматическое применение настроек при запуске виртуальных машин.

Таким образом, создана функционирующая система централизованного сбора и анализа системных журналов.

# 4. Ответы на контрольные вопросы

1. Какой модуль rsyslog вы должны использовать для приёма сообщений от journald?

Для приёма сообщений от journald следует использовать модуль imjournal.

1. Как называется устаревший модуль, который можно использовать для включения приёма сообщений журнала в rsyslog?

imklog

1. Чтобы убедиться, что устаревший метод приёма сообщений из journald в rsyslog не используется, какой дополнительный параметр следует использовать?

Cледует использовать параметр “SystemCallFilter[include:omusrmsg.conf?]” в конфигурационном файле rsyslog.conf.

1. В каком конфигурационном файле содержатся настройки, которые позволяют вам настраивать работу журнала?

Настройки, позволяющие настраивать работу журнала, содержатся в конфигурационном файле rsyslog.conf.

1. Каким параметром управляется пересылка сообщений из journald в rsyslog?

Пересылка сообщений из journald в rsyslog управляется параметром “ForwardToSyslog” в файле конфигурации journald.conf.

1. Какой модуль rsyslog вы можете использовать для включения сообщений из файла журнала, не созданного rsyslog?

Модуль rsyslog, который можно использовать для включения сообщений из файла журнала, не созданного rsyslog, называется imfile.

1. Какой модуль rsyslog вам нужно использовать для пересылки сообщений в базу данных MariaDB?

Для пересылки сообщений в базу данных MariaDB следует использовать модуль ommysql.

1. Какие две строки вам нужно включить в rsyslog.conf, чтобы позволить текущему журнальному серверу получать сообщения через TCP?

Для позволения текущему журнальному серверу получать сообщения через TCP нужно включить две строки в rsyslog.conf:

$ModLoad imtcp   
$InputTCPServerRun 514

1. Как настроить локальный брандмауэр, чтобы разрешить приём сообщений журнала через порт TCP 514?

firewall-cmd --add-port=514/tcp  
firewall-cmd --add-port=514/tcp --permanent