

Лабораторная работа № 15. Настройка сетевого журналирования

15.1. Цель работы

Получение навыков по работе с журналами системных событий.

15.2. Предварительные сведения

15.2.1. Журналирование системных событий

В системах на базе Unix/Linux важное место при администрировании занимает отслеживание системных событий (и в частности возникновение возможных ошибок в процессе настройки каких-то служб) через ведение log-файлов процессов системы. Журналирование системных событий заключается в фиксации с помощью сокета syslog в лог-файлах сообщений об ошибках и сообщений о состоянии работы практически всех процессов системы. Обычно лог-файлы располагаются в каталоге `/var/log`.

Для управления логированием событий обычно используется служба `syslog` или её модификация `rsyslog`. С их помощью можно настроить уровень подробности логирования для каждого процесса. Все настройки `rsyslog` находятся в файле `/etc/rsyslog.conf`. В этот же файл подключаются дополнительные файлы настройки из каталога `/etc/rsyslog.d/`.

15.2.2. Зачем нужен сервер сетевого журнала

Сохранение всех событий системы приводит к быстрому заполнению дискового пространства. Кроме того, если требуется администрировать несколько узлов сети, то удобнее это делать с одного узла:

- проще обеспечить безопасность и целостность лог-сообщений, которые в этом случае не будут доступны злоумышленнику, если не нарушена безопасность самого сервера;
- проще и удобнее управлять дисковым пространством и политиками по времени хранения информации в журналах, в том числе настроить `logrotate` для сохранения сообщений в течение более длительного периода, чем период по умолчанию;
- проверять файлы журналов на одном сервере проще, чем подключиться к нескольким серверам для анализа информации, которая была зарегистрирована.

15.3. Задание

1. Настройте сервер сетевого журналирования событий (см. раздел 15.4.1).
2. Настройте клиент для передачи системных сообщений в сетевой журнал на сервере (см. раздел 15.4.2).
3. Просмотрите журналы системных событий с помощью нескольких программ (см. раздел 15.4.3).
4. Напишите скрипты для Vagrant, фиксирующие действия по установке и настройке сетевого сервера журналирования (см. раздел 15.4.4).

15.4. Последовательность выполнения работы

15.4.1. Настройка сервера сетевого журнала

1. На сервере создайте файл конфигурации сетевого хранения журналов:

- ```
cd /etc/rsyslog.d
touch netlog-server.conf
```
- В файле конфигурации `/etc/rsyslog.d/netlog-server.conf` включите приём записей журнала по TCP-порту 514:

```
$ModLoad imtcp
$InputTCPServerRun 514
```
  - Перезапустите службу `rsyslog` и посмотрите, какие порты, связанные с `rsyslog`, прослушиваются:

```
systemctl restart rsyslog
lsof | grep TCP
```
  - На сервере настройте межсетевой экран для приёма сообщений по TCP-порту 514:

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

### 15.4.2. Настройка клиента сетевого журнала

- На клиенте создайте файл конфигурации сетевого хранения журналов:

```
cd /etc/rsyslog.d
touch netlog-client.conf
```
- На клиенте в файле конфигурации `/etc/rsyslog.d/netlog-client.conf` включите перенаправление сообщения журнала на 514 TCP-порт сервера (вместо `user` укажите свой логин):

```
. @server.user.net:514
```
- Перезапустите службу `rsyslog`:

```
systemctl restart rsyslog
```

### 15.4.3. Просмотр журнала

- На сервере просмотрите один из файлов журнала

```
tail -f /var/log/messages
```

Обратите внимание на имя хоста.
- На сервере запустите графическую программу для просмотра журналов:

```
gnome-system-log
```
- На сервере установите просмотрщик журналов системных сообщений `lnav`:

```
dnf -y install lnav
```
- Просмотрите логи с помощью `lnav`:

```
lnav
```

Просмотрите записи с сервера и клиента.

### 15.4.4. Внесение изменений в настройки внутреннего окружения виртуальных машин

- На виртуальной машине `server` перейдите в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создайте в нём каталог `netlog`, в который поместите в соответствующие подкаталоги конфигурационные файлы:

```
cd /vagrant/provision/server
mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d
cp -R /etc/netlog-server.conf
↵ /vagrant/provision/server/netlog/etc/rsyslog.d
```
- В каталоге `/vagrant/provision/server` создайте исполняемый файл `netlog.sh`:

```
cd /vagrant/provision/server
touch netlog.sh
chmod +x netlog.sh
```

Открыв его на редактирование, пропишите в нём следующий скрипт:

```
#!/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
```

3. На виртуальной машине `client` перейдите в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/client/`, создайте в нём каталог `netlog`, в который поместите в соответствующие подкаталоги конфигурационные файлы:

```
cd /vagrant/provision/client
mkdir -p /vagrant/provision/client/netlog/etc/rsyslog.d
cp -R /etc/rsyslog.d/netlog-client.conf
↪ /vagrant/provision/client/netlog/etc/rsyslog.d/
```

4. В каталоге `/vagrant/provision/client` создайте исполняемый файл `netlog.sh`:

```
cd /vagrant/provision/client
touch netlog.sh
chmod +x netlog.sh
```

Открыв его на редактирование, пропишите в нём следующий скрипт:

```
#!/bin/bash

echo "Provisioning script $0"

echo "Install needed packages"
dnf -y install lnav

echo "Copy configuration files"
cp -R /vagrant/provision/client/netlog/etc/* /etc
restorecon -vR /etc

echo "Start rsyslog service"
systemctl restart rsyslog
```

5. Для отработки созданных скриптов во время загрузки виртуальных машин `server` и `client` в конфигурационном файле `Vagrantfile` необходимо добавить в соответствующих разделах конфигураций для сервера и клиента:

```
server.vm.provision "server netlog",
 type: "shell",
 preserve_order: true,
 path: "provision/server/netlog.sh"
```

```
client.vm.provision "client netlog",
 type: "shell",
 preserve_order: true,
 path: "provision/client/netlog.sh"
```

## 15.5. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
  - скриншоты (снимки экрана), фиксирующие выполнение работы;
  - подробное описание настроек служб в соответствии с заданием;
  - полные тексты конфигурационных файлов настраиваемых в работе служб;
  - результаты проверки корректности настроек служб в соответствии с заданием (подтверждённые скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

## 15.6. Контрольные вопросы

1. Какой модуль `rsyslog` вы должны использовать для приёма сообщений от `journald`?
2. Как называется устаревший модуль, который можно использовать для включения приёма сообщений журнала в `rsyslog`?
3. Чтобы убедиться, что устаревший метод приёма сообщений из `journald` в `rsyslog` не используется, какой дополнительный параметр следует использовать?
4. В каком конфигурационном файле содержатся настройки, которые позволяют вам настраивать работу журнала?
5. Каким параметром управляется пересылка сообщений из `journald` в `rsyslog`?
6. Какой модуль `rsyslog` вы можете использовать для включения сообщений из файла журнала, не созданного `rsyslog`?
7. Какой модуль `rsyslog` вам нужно использовать для пересылки сообщений в базу данных `MariaDB`?
8. Какие две строки вам нужно включить в `rsyslog.conf`, чтобы позволить текущему журнальному серверу получать сообщения через TCP?
9. Как настроить локальный брандмауэр, чтобы разрешить приём сообщений журнала через порт TCP 514?