Презентация по лабораторной работе №15

Администрирование сетевых подсистем

true

2025-12-02

Вводная часть

Цель работы

Целью данной работы получить навыки по работе с журналами системных событий.

Задание

1. Настроить сервер сетевого журналирования событий
2. Настроить клиент для передачи системных сообщений в сетевой журнал на сервере
3. Просмотреть журналы системных событий с помощью нескольких программ. При наличии сообщений о некорректной работе сервисов исправить ошибки в настройках соответствующих служб
4. Написать скрипты для Vagrant, фиксирующие действия по установке и настройке сетевого сервера журналирования

Выполнение лабораторной работы

Настройка сервера сетевого журнала

Загрузили нашу операционную систему и перешли в рабочий каталог с проектом: cd /var/tmp/tbmanturov/vagrant

Настройка сервера сетевого журнала

Запустили виртуальную машину server: make server-up

Настройка сервера сетевого журнала

Далее на виртуальной машине server вошли под созданным нами пользователем и открыли терминал. Перешли в режим суперпользователя: sudo -i

Настройка сервера сетевого журнала

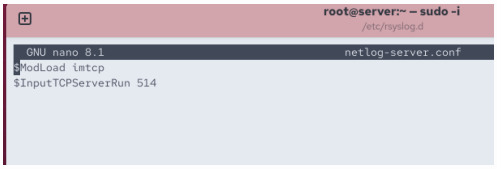
На сервере создали файл конфигурации сетевого хранения журналов ([рис. @fig-004]):

```
[tbmanturov@server.tbmanturov.net ~]$ cd /etc/rsyslog.d
[tbmanturov@server.tbmanturov.net rsyslog.d]$ touch netlog-server.conf
touch: cannot touch 'netlog-server.conf': Permission denied
[tbmanturov@server.tbmanturov.net rsyslog.d]$ sudo -i
[sudo] password for tbmanturov:
[root@server.tbmanturov.net ~]# touch netlog-server.conf
```

Создание файла /etc/rsyslog.d/netlog-server.conf на server

Настройка сервера сетевого журнала

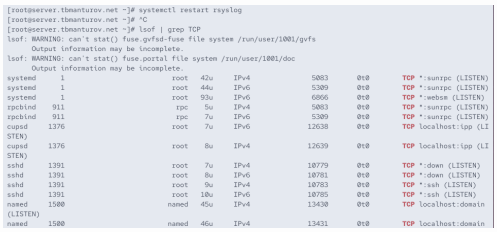
В файле конфигурации */etc/rsyslog.d/netlog-server.conf* включили приём записей журнала по TCP-порту 514 ([рис. @fig-005]):



Редактирование файла /etc/rsyslog.d/netlog-server.conf на server

Настройка сервера сетевого журнала

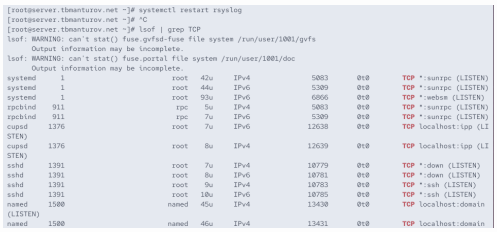
Перезапустили службу rsyslog на сервере: systemctl restart rsyslog ([рис. @fig-006])



Перезапуск службы rsyslog на server

Настройка сервера сетевого журнала

Посмотрели, какие порты, связанные с rsyslog, прослушиваются: lsof | grep TCP ([рис. @fig-007])



Просмотр прослушиваемых портов связанных с rsyslog

Настройка сервера сетевого журнала

На сервере настройте межсетевой экран для приёма сообщений по TCP-порту 514 ([рис. @fig-008]):

```
[root@server.tbmanturov.net ~]# firewall-cmd --add-port=514/tcp
Warning: ALREADY_ENABLED: '514:tcp' already in 'public'
success
[root@server.tbmanturov.net ~]# firewall-cmd --add-port=514/tcp --permanent
Warning: ALREADY_ENABLED: 514:tcp
success
[root@server.tbmanturov.net ~]#
```

Настройка межсетевого экрана для приёма сообщений по TCP-порту 514

Настройка клиента сетевого журнала

Запустили виртуальную машину client: make client-up ([рис. @fig-009])

Настройка клиента сетевого журнала

Далее на виртуальной машине client вошли под созданным нами пользователем и открыли терминал. Перешли в режим суперпользователя: sudo -i ([рис. @fig-010])

Настройка клиента сетевого журнала

На клиенте создали файл конфигурации сетевого хранения журналов ([рис. @fig-011]):

```
[root@client.tbmanturov.net ~]# cd /etc/rsyslog.d
[root@client.tbmanturov.net rsyslog.d]# touch netlog-client.conf
[root@client.tbmanturov.net rsyslog.d]#
```

Создание файла /etc/rsyslog.d/netlog-client.conf на client

Настройка клиента сетевого журнала

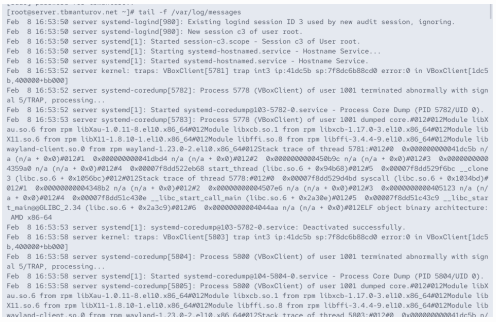
На клиенте в файле конфигурации */etc/rsyslog.d/netlog-client.conf* включили перенаправление сообщений журнала на 514 TCP-порт сервера: *.* @@server.tbmanturov.net:514 ([рис. @fig-012])

```
 GNU nano 8.1                                  netlog-client.conf
*.* @@server.tbmanturov.net:514
```

Редактирование файла /etc/rsyslog.d/netlog-client.conf на client

Просмотр журнала

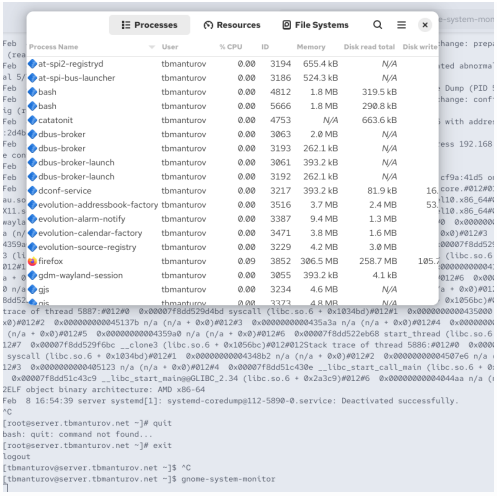
На сервере посмотрели один из файлов журнала: tail -f /var/log/messages ([рис. @fig-014])



Просмотр одного из файлов журнала на server

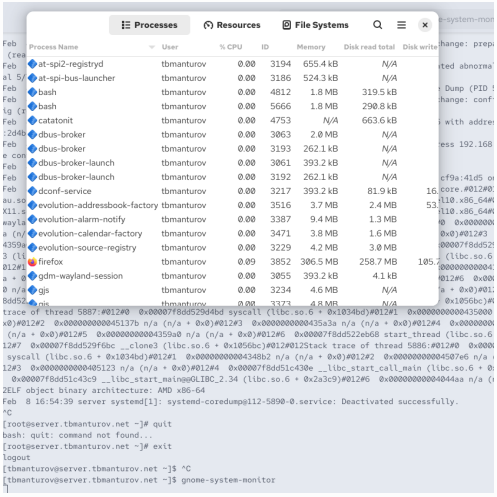
Просмотр журнала

На сервере под пользователем tbmanturov запустили графическую программу для просмотра журналов: gnome-system-monitor ([рис. @fig-015]), ([рис. @fig-016])



Запуск графической программы для просмотра журналов

Просмотр журнала



Просмотра журналов в графической программе gnome-system-monitor

Просмотр журнала

На сервере установили просмотрщик журналов системных сообщений lnav.

```
[root@server.tbmanturov.net ~]# dnf -y install lnav
```

Установка lnav на server (1)

Просмотр журнала

Далее посмотрели логи с помощью lnav: lnav ([рис. @fig-022])

Запуск lnav на server

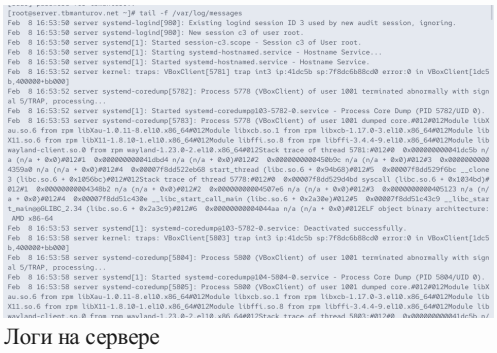
Просмотр журнала

Просмотр общих логов на сервере

Просмотр общих логов на сервере

Просмотр журнала

Посмотрели логи на клиенте: tail -f /var/log/messages. Все логи, имеющиеся на клиенте, также отображаются на сервере ([рис. @fig-014])



Логи на сервере

Внесение изменений в настройки внутреннего окружения виртуальной машины

На виртуальной машине server перешли в каталог для внесения изменений в настройки внутреннего окружения */vagrant/provision/server/* и создали в нём каталог *netlog*, в который поместили в соответствующие подкаталоги конфигурационные файлы ([рис. @fig-025]):

Копирование конфигурационных файлов в каталог netlog на сервере

Внесение изменений в настройки внутреннего окружения виртуальной машины

В каталоге */vagrant/provision/server* создали исполняемый файл netlog.sh ([рис. @fig-026]):

```
[root@server.tbmanturov.net server]# touch netlog.sh
[root@server.tbmanturov.net server]# chmod +x netlog.sh
[root@server.tbmanturov.net server]# nano netlog.sh
[root@server.tbmanturov.net server]#
```

Создание исполняемого файла netlog.sh на сервере

Внесение изменений в настройки внутреннего окружения виртуальной машины

Открыв его на редактирование, прописали в нём следующий скрипт ([рис. @fig-027]):

```
 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
```

Редактирование файла netlog.sh на сервере

Внесение изменений в настройки внутреннего окружения виртуальной машины

На виртуальной машине client перешли в каталог для внесения изменений в настройки внутреннего окружения */vagrant/provision/client/* и создали в нём каталог *netlog*, в который поместили в соответствующие подкаталоги конфигурационные файлы ([рис. @fig-028]):

```
[root@client.tbmanturov.net ~]# cd /vagrant/provision/client
[root@client.tbmanturov.net client]# mkdir -p /vagrant/provision/client/netlog/etc/rsyslog.d
[root@client.tbmanturov.net client]# cp -R /etc/rsyslog.d/netlog-client.conf /vagrant/provision/client/netlog/etc/rsy
slog.d/
[root@client.tbmanturov.net client]#
```

Копирование конфигурационных файлов в каталог netlog на клиенте

Внесение изменений в настройки внутреннего окружения виртуальной машины

В каталоге */vagrant/provision/client/* создали исполняемый файл netlog.sh ([рис. @fig-029]):

```
[root@client.tbmanturov.net client]# touch netlog.sh
[root@client.tbmanturov.net client]# chmod +x netlog.sh
[root@client.tbmanturov.net client]#
```

Создание исполняемого файла netlog.sh на клиенте

Внесение изменений в настройки внутреннего окружения виртуальной машины

Открыв его на редактирование, прописали в нём следующий скрипт ([рис. @fig-030]):

```
 GNU nano 8.1                                                netlog.sh
#!/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
```

Редактирование файла netlog.sh на клиенте

Внесение изменений в настройки внутреннего окружения виртуальной машины

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 ([рис. @fig-031]), ([рис. @fig-032]):

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

Редактирование файла Vagrantfile (1)

Внесение изменений в настройки внутреннего окружения виртуальной машины

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

Редактирование файла Vagrantfile (2)

Внесение изменений в настройки внутреннего окружения виртуальной машины

После этого можно выключать виртуальные машины server и client: make server-halt и make client-halt ([рис. @fig-033])

Подведение итогов

Выводы

В ходе выполнения лабораторной работы №15 мы получили навыки по работе с журналами системных событий.

Список литературы

1. Лабораторая работа №15