Лабораторная работа

Номер 15

Мошаров Д.М.

01 января 1970

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Мошаров Денис Максимович
- Студент
- Российский университет дружбы народов

Цель работы

Получение навыков по работе с журналами системных событий

Создание файла конфигурации на сервере

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

Рис. 1: Создание файла конфигурации на сервере

Редактирование конфигурации rsyslog на сервере

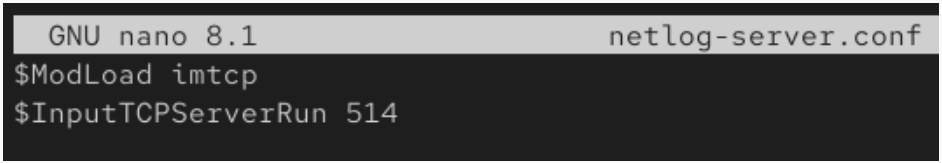

Рис. 2: Редактирование конфигурации rsyslog на сервере

Перезапуск службы и начало проверки портов

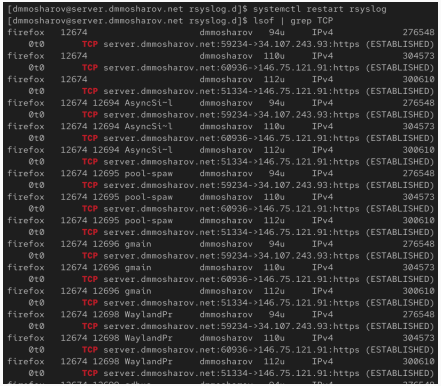

Рис. 3: Перезапуск службы и начало проверки портов

Подтверждение прослушивания порта 514

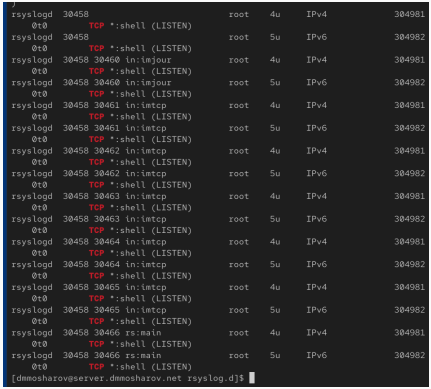

Рис. 4: Подтверждение прослушивания порта 514

Настройка firewall на сервере

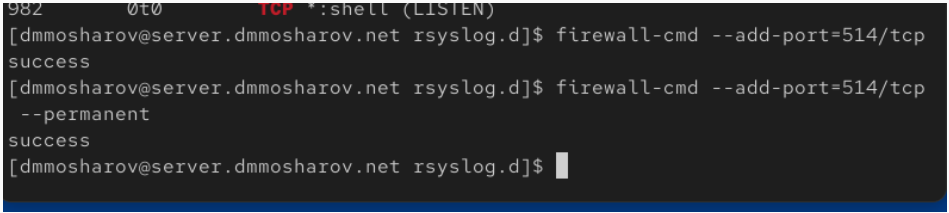

Рис. 5: Настройка firewall на сервере

Создание файла конфигурации на клиенте

```
[dmmosharov@client.dmmosharov.net ~]$ cd /etc/rsyslog.d
[dmmosharov@client.dmmosharov.net rsyslog.d]$ touch netlog-client.conf
touch: cannot touch 'netlog-client.conf': Permission denied
[dmmosharov@client.dmmosharov.net rsyslog.d]$ sudo touch netlog-client.conf
[sudo] password for dmmosharov:
[dmmosharov@client.dmmosharov.net rsyslog.d]$ sudo nano netlog-client.conf
[dmmosharov@client.dmmosharov.net rsyslog.d]$
```

Рис. 6: Создание файла конфигурации на клиенте

Редактирование конфигурации rsyslog на клиенте

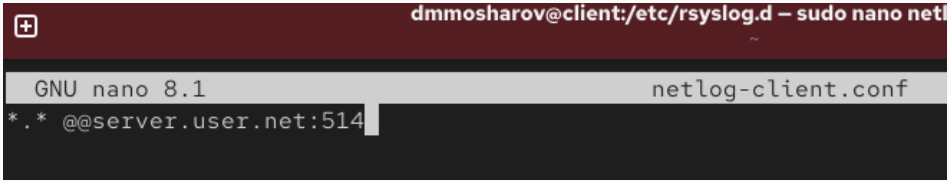

Рис. 7: Редактирование конфигурации rsyslog на клиенте

Просмотр логов на сервере через tail

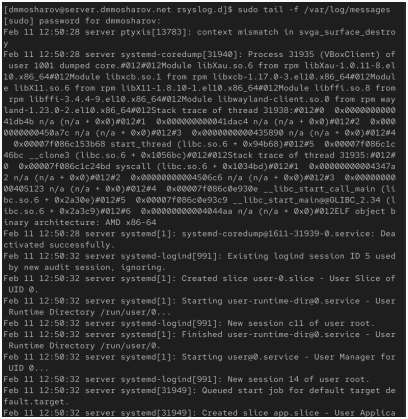

Рис. 8: Просмотр логов на сервере через tail

Интерфейс Gnome System Monitor

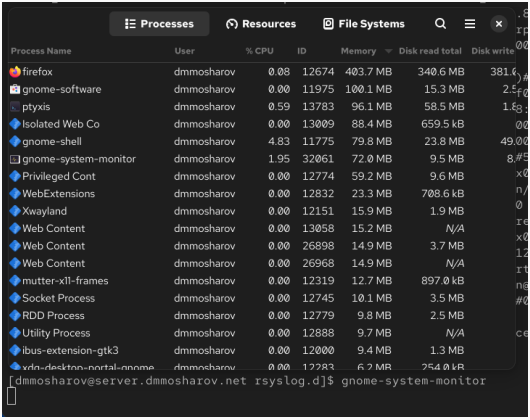

Рис. 9: Интерфейс Gnome System Monitor

Ручная установка lnav на сервере

```
[dmmosharov@server.dmmosharov.net rsyslog.d]$ cd ~/Downloads/
[dmmosharov@server.dmmosharov.net Downloads]$ sudo cp lnav /usr/bin
cp: cannot stat 'lnav': No such file or directory
[dmmosharov@server.dmmosharov.net Downloads]$ sudo cp lnav /usr/bin
[dmmosharov@server.dmmosharov.net Downloads]$ lnav
✗ error: default syslog file is not readable -- /var/log/messages
[dmmosharov@server.dmmosharov.net Downloads]$ sudo lnav
[dmmosharov@server.dmmosharov.net Downloads]$
```

Рис. 10: Ручная установка lnav на сервере

Просмотр логов через lnav на сервере

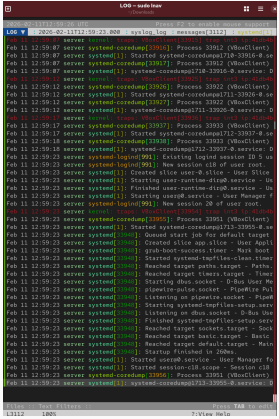

Рис. 11: Просмотр логов через lnav на сервере

Подготовка файлов для автоматизации сервера

```
[dmmosharov@server.dmmosharov.net Downloads]$ cd /vagrant/provision/server
[dmmosharov@server.dmmosharov.net server]$ mkdir -p /vagrant/provision/server
/netlog/etc/rsyslog.d
[dmmosharov@server.dmmosharov.net server]$ cp -R /etc/rsyslog.d/netlog-server
.conf /vagrant/provision/server/netlog/etc/rsyslog.d
[dmmosharov@server.dmmosharov.net server]$ cd /vagrant/provision/server
[dmmosharov@server.dmmosharov.net server]$ touch netlog.sh
[dmmosharov@server.dmmosharov.net server]$ chmod +x netlog.sh
[dmmosharov@server.dmmosharov.net server]$ nano netlog.sh
[dmmosharov@server.dmmosharov.net server]$
```

Рис. 14: Подготовка файлов для автоматизации сервера

Скрипт provisioning для сервера

```
  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
```

Рис. 15: Скрипт provisioning для сервера

Подготовка файлов для автоматизации клиента

```
[dmmosharov@client.dmmosharov.net rsyslog.d]$ cd /vagrant/provision/cli
ent
[dmmosharov@client.dmmosharov.net client]$ mkdir -p /vagrant/provision/
client/netlog/etc/rsyslog.d
[dmmosharov@client.dmmosharov.net client]$ cp -R /etc/rsyslog.d/netlog-
client.conf /vagrant/provision/client/netlog/etc/rsyslog.d/
[dmmosharov@client.dmmosharov.net client]$ cd /vagrant/provision/client
[dmmosharov@client.dmmosharov.net client]$ touch netlog.sh
[dmmosharov@client.dmmosharov.net client]$ chmod +x netlog.sh
[dmmosharov@client.dmmosharov.net client]$ nano netlog.sh
```

Рис. 16: Подготовка файлов для автоматизации клиента

Скрипт provisioning для клиента

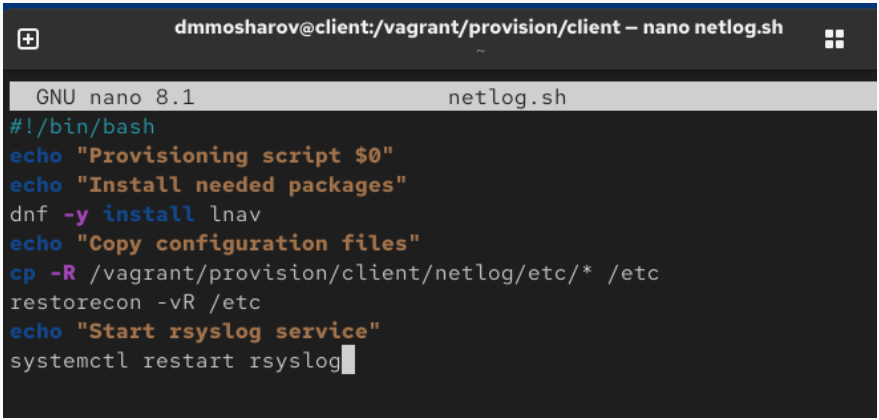

Рис. 17: Скрипт provisioning для клиента

Настройка Vagrantfile

Рис. 18: Настройка Vagrantfile

Выводы

В результате выполнения лабораторной работы были получены навыки использования журналов системных событий