Лабораторная работа №15

Настройка сетевого журналирования

Ромицына А. Р.

12 декабря 2025

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Ромицына Анастасия Романовна
- НПИбд-02-23 Студ. билет: 1132236132
- Российский университет дружбы народов
- 1132236132@pfur.ru

Вводная часть

Цель работы

- Целью данной работы является получение навыков по работе с журналами системных событий.

Основная часть

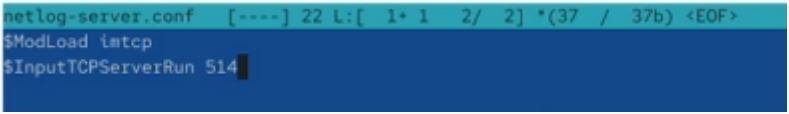
Настройка сервера сетевого журнала

- Создание на сервере файла конфигурации сетевого хранения журналов.

```
[arromichina@server.arromichina.net rsyslog.d]$ sudo -i
[sudo] password for arromichina:
[root@server.arromichina.net ~]# cd /etc/rsyslog.d
[root@server.arromichina.net rsyslog.d]# touch netlog-server.conf
[root@server.arromichina.net rsyslog.d]#
```

Настройка сервера сетевого журнала

- Включение в файле конфигурации /etc/rsyslog.d/netlog-server.conf приёма записей журнала по TCP-порту 514



Настройка сервера сетевого журнала

- Перезапуск службы rsyslog и просмотр прослушиваемых портов, связанных с rsyslog.

```
[root@server.arromichina.net rsyslog.d]# systemctl restart rsyslog
[root@server.arromichina.net rsyslog.d]# lsof | grep TCP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
      Output information may be incomplete.
lsof: WARNING: can't stat() fuse.portal file system /run/user/1001/doc
      Output information may be incomplete.
systemd      1                          root   42u     IPv4               5512       0t0        TCP *:sunrpc (LISTEN)
systemd      1                          root   44u     IPv6               5526       0t0        TCP *:sunrpc (LISTEN)
```

Настройка сервера сетевого журнала

- Настройка на сервере межсетевого экрана для приёма сообщений по TCP-порту 514

```
[root@server.arromichina.net rsyslog.d]# firewall-cmd --add-port=514/tcp
success
[root@server.arromichina.net rsyslog.d]# firewall-cmd --add-port=514/tcp --permanent
success
[root@server.arromichina.net rsyslog.d]#
```

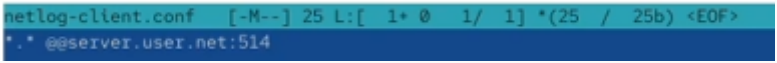
Настройка клиента сетевого журнала

- Создание на клиенте файла конфигурации сетевого хранения журналов.

```
[arromichina@client.arromichina.net ~]$ sudo -i
[sudo] password for arromichina:
[root@client.arromichina.net ~]# cd /etc/rsyslog.d
[root@client.arromichina.net rsyslog.d]# touch netlog-client.conf
[root@client.arromichina.net rsyslog.d]#
```

Настройка клиента сетевого журнала

- Включение в файле конфигурации /etc/rsyslog.d/netlog-client.conf перенаправления сообщений журнала на 514 TCP-порт сервера.



Настройка клиента сетевого журнала

- Перезапуск службы rsyslog.

```
[root@client.arromichina.net rsyslog.d]# systemctl restart rsyslog
[root@client.arromichina.net rsyslog.d]#
```

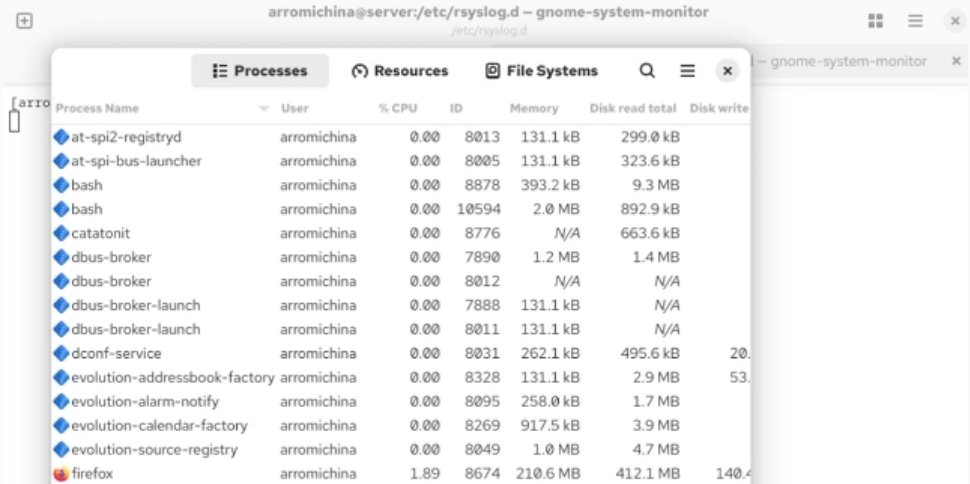
Просмотр журнала

- Просмотр на сервере одного из файлов журнала.

```
[root@server.arromichina.net rsyslog.d]# tail -f /var/log/messages
Dec 10 13:24:36 server named[1358]: timed out resolving 'ns4.dnsmadeeasy.com/A/IN': 127.0.0.1#53
Dec 10 13:24:36 server named[1358]: timed out resolving 'ns4.dnsmadeeasy.com/AAAA/IN': 127.0.0.1#53
Dec 10 13:24:36 server named[1358]: timed out resolving 'ns2.dnsmadeeasy.com/AAAA/IN': 127.0.0.1#53
Dec 10 13:24:36 server named[1358]: timed out resolving 'ns2.dnsmadeeasy.com/A/IN': 127.0.0.1#53
Dec 10 13:24:36 server named[1358]: timed out resolving 'ns0.dnsmadeeasy.com/A/IN': 127.0.0.1#53
Dec 10 13:24:36 server named[1358]: timed out resolving 'ns0.dnsmadeeasy.com/AAAA/IN': 127.0.0.1#53
Dec 10 13:24:37 server named[1358]: timed out resolving 'user.net/DS/IN': 127.0.0.1#53
Dec 10 13:24:37 server named[1358]: timed out resolving 'user.net/DS/IN': 127.0.0.1#53
Dec 10 13:24:42 server NetworkManager[4948]: <info>  [1765373082.1385] agent-manager: agent[bc4b1c00d5069170,:1.206/org.
gnome.Shell.NetworkAgent/1001]: agent registered
Dec 10 13:24:42 server gnome-shell[7970]: Gio.DBusError: GDBus.Error:org.freedesktop.DBus.Error.Failed: Set global engin
e failed: Operation was cancelled#012#012Stack trace:#012  _promisify/proto[asyncFunc]/</<@resource:///org/gnome/gjs/mod
ules/core/overrides/Gio.js:453:45#012  @resource:///org/gnome/shell/ui/init.js:21:20#012  ### Promise created here: ####
012  _setEngine@resource:///org/gnome/shell/misc/ibusManager.js:286:30#012  setEngine@resource:///org/gnome/shell/misc/i
busManager.js:299:24#012  activateInputSource@resource:///org/gnome/shell/ui/status/keyboard.js:523:27#012  _callHandler
s@resource:///org/gnome/gjs/modules/core/_signals.js:130:42#012  _emit@resource:///org/gnome/gjs/modules/core/_signals.j
s:119:10#012  activate@resource:///org/gnome/shell/ui/status/keyboard.js:66:14#012  _inputSourcesChanged@resource:///org
/gnome/shell/ui/status/keyboard.js:661:33#012  reload@resource:///org/gnome/shell/ui/status/keyboard.js:394:14#012  _ibu
sSetContentType@resource:///org/gnome/shell/ui/status/keyboard.js:736:14#012  _callHandlers@resource:///org/gnome/gjs/mo
dules/core/_signals.js:130:42#012  _emit@resource:///org/gnome/gjs/modules/core/_signals.js:119:10#012  _setContentType@
resource:///org/gnome/shell/misc/ibusManager.js:264:14#012  @resource:///org/gnome/shell/ui/init.js:21:20#012
```

Просмотр журнала

- Запуск на сервере под пользователем arromichina графической программы для просмотра журналов.



Просмотр журнала

- Установка на сервере просмотрщика журналов системных сообщений.

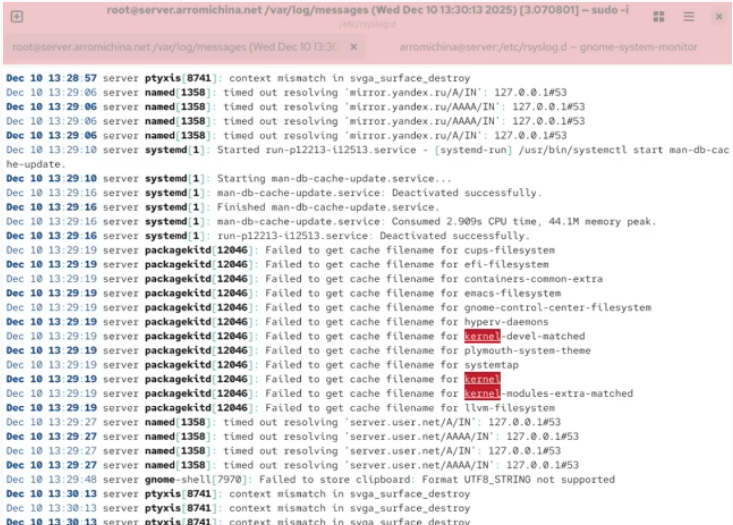
```
[root@server.arromichina.net rsyslog.d]# sudo dnf install -y multitail
Last metadata expiration check: 0:50:41 ago on Wed 10 Dec 2025 12:38:23 PM UTC.
Dependencies resolved.
================================================================================
 Package                Architecture            Version                 Repository
================================================================================
Installing:
 multitail              x86_64                  7.1.3-2.el10_0          epel

Transaction Summary
================================================================================
Install  1 Package

Total download size: 148 k
Installed size: 326 k
Downloading Packages:
multitail-7.1.3-2.el10_0.x86_64.rpm                          108 kB/s | 148 kB
--------------------------------------------------------------------------------
Total                                                         73 kB/s | 148 kB
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
```

Просмотр журнала

- Просмотр логов



Внесение изменений в настройки внутреннего окружения виртуальных машин

- Переход на виртуальной машине server в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создание в нём каталога netlog, в который помещаем в соответствующие подкаталоги конфигурационные файлы. Создание в каталоге /vagrant/provision/server исполняемого файла netlog.sh.

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

Настройка сервера NFSv4

- Открытие файла на редактирование и добавление в него скрипта.

```
netlog.sh          [-M--] 25 L:[  1+ 9  10/ 10] *(300 / 300b) <EOF>
#!/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
```

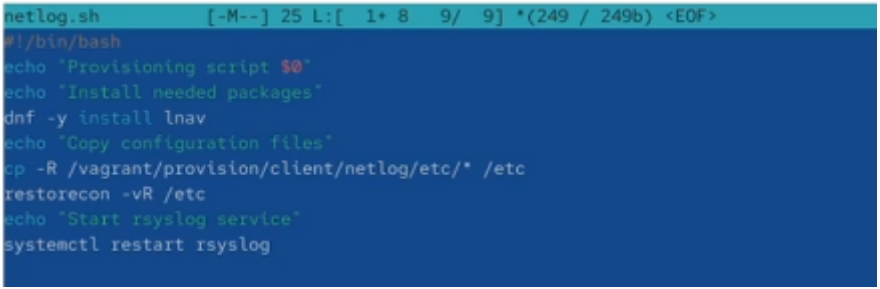
Монтирование NFS на клиенте

- Переход на виртуальной машине client в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/, создание в нём каталога nentlog, в который помещаем в соответствующие подкаталоги конфигурационные файлы. Создание в каталоге /vagrant/provision/client исполняемого файла netlog.sh.

```
[root@client.arromichina.net rsyslog.d]# cd /vagrant/provision/client
[root@client.arromichina.net client]# mkdir -p /vagrant/provision/client/netlog/etc/rsyslog.d
[root@client.arromichina.net client]# cp -R /etc/rsyslog.d/netlog-client.conf /vagrant/provision/client/netlog/etc/r
yslog.d/
[root@client.arromichina.net client]# cd /vagrant/provision/client
[root@client.arromichina.net client]# touch netlog.sh
[root@client.arromichina.net client]# chmod +x netlog.sh
[root@client.arromichina.net client]#
```

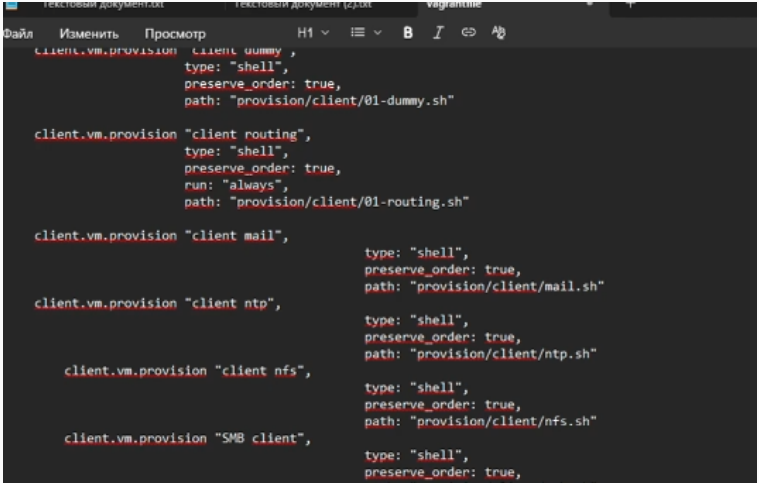
Монтирование NFS на клиенте

- Открытие файла на редактирование и добавление в него скрипта.



Монтирование NFS на клиенте

- Добавление конфигураций в конфигурационном файле Vagrantfile для сервера и клиента.



Вывод

Вывод

- В ходе выполнения лабораторной работы были получены навыки по работе с журналами системных событий.