Лабораторная работа № 15

Настройка сетевого журналирования

Митрофанов Тимур Александрович

2025-12-13

Содержание I

1. Информация

2. Вводная часть

3. Выполнение заданий

4. Выводы

Раздел 1

1. Информация

1.1 Докладчик

- Митрофанов Тимур Александрович

1.1 Докладчик

- Митрофанов Тимур Александрович
- Российский университет дружбы народов им. П. Лумумбы

Раздел 2

2. Вводная часть

2.1 Цели и задачи

Цель - получение навыков по работе с журналами системных событий.

1. Настройте сервер сетевого журналирования событий.

2.1 Цели и задачи

Цель - получение навыков по работе с журналами системных событий.

1. Настройте сервер сетевого журналирования событий.
2. Настройте клиент для передачи системных сообщений в сетевой журнал на сервере.

2.1 Цели и задачи

Цель - получение навыков по работе с журналами системных событий.

1. Настройте сервер сетевого журналирования событий.
2. Настройте клиент для передачи системных сообщений в сетевой журнал на сервере.
3. Просмотрите журналы системных событий с помощью нескольких программ. При наличии сообщений о некорректной работе сервисов исправьте ошибки в настройках соответствующих служб.

2.1 Цели и задачи

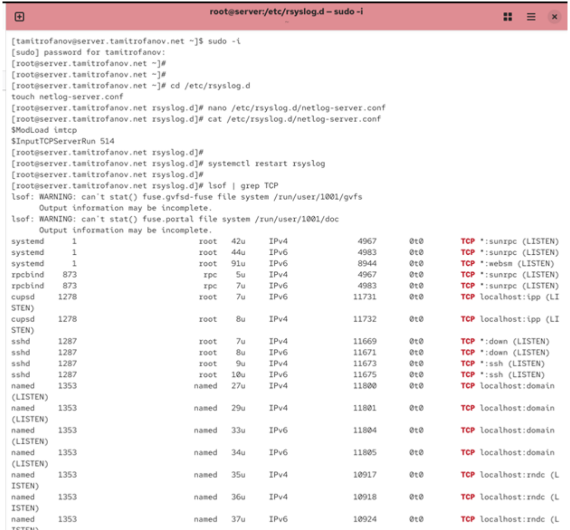
Цель - получение навыков по работе с журналами системных событий.

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

Раздел 3

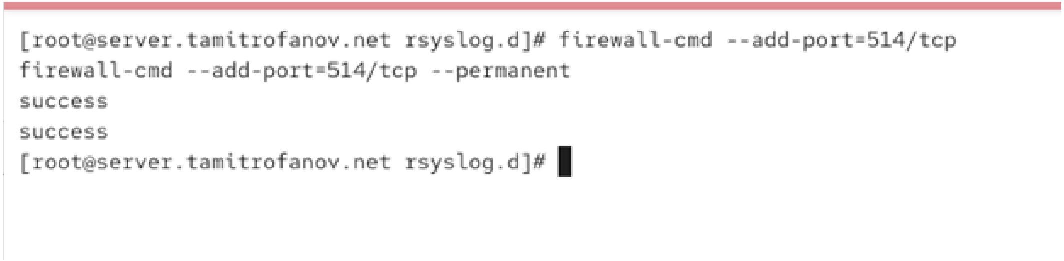
3. Выполнение заданий

3.1 Настройка сервера сетевого журнала



```
[tamitrofanov@server.tamitrofanov.net ~]$ sudo -i
[sudo] password for tamitrofanov:
[root@server.tamitrofanov.net ~]#
[root@server.tamitrofanov.net ~]#
[root@server.tamitrofanov.net ~]# cd /etc/rsyslog.d
touch netlog-server.conf
[root@server.tamitrofanov.net rsyslog.d]# nano /etc/rsyslog.d/netlog-server.conf
[root@server.tamitrofanov.net rsyslog.d]# cat /etc/rsyslog.d/netlog-server.conf
$ModLoad imtcp
$InputTCPServerRun 514
[root@server.tamitrofanov.net rsyslog.d]#
[root@server.tamitrofanov.net rsyslog.d]# systemctl restart rsyslog
[root@server.tamitrofanov.net rsyslog.d]#
[root@server.tamitrofanov.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            4967      0t0        TCP *:sunrpc (LISTEN)
systemd       1                        root   44u     IPv6            4983      0t0        TCP *:sunrpc (LISTEN)
systemd       1                        root   91u     IPv6            8944      0t0        TCP *:websm (LISTEN)
rpcbind     873                         rpc    5u     IPv4            4967      0t0        TCP *:sunrpc (LISTEN)
rpcbind     873                         rpc    7u     IPv6            4983      0t0        TCP *:sunrpc (LISTEN)
cupsd      1278                        root    7u     IPv6           11731      0t0        TCP localhost:ipp (LI
STEN)
cupsd      1278                        root    8u     IPv4           11732      0t0        TCP localhost:ipp (LI
STEN)
sshd       1287                        root    7u     IPv4           11669      0t0        TCP *:down (LISTEN)
sshd       1287                        root    8u     IPv6           11671      0t0        TCP *:down (LISTEN)
sshd       1287                        root    9u     IPv4           11673      0t0        TCP *:ssh (LISTEN)
sshd       1287                        root   10u     IPv6           11675      0t0        TCP *:ssh (LISTEN)
named      1353                       named   27u     IPv4           11800      0t0        TCP localhost:domain
(LISTEN)
named      1353                       named   29u     IPv4           11801      0t0        TCP localhost:domain
(LISTEN)
named      1353                       named   33u     IPv6           11804      0t0        TCP localhost:domain
(LISTEN)
named      1353                       named   34u     IPv6           11805      0t0        TCP localhost:domain
(LISTEN)
named      1353                       named   35u     IPv4           10917      0t0        TCP localhost:rndc (L
ISTEN)
named      1353                       named   36u     IPv4           10918      0t0        TCP localhost:rndc (L
ISTEN)
named      1353                       named   37u     IPv6           10924      0t0        TCP localhost:rndc (L
```

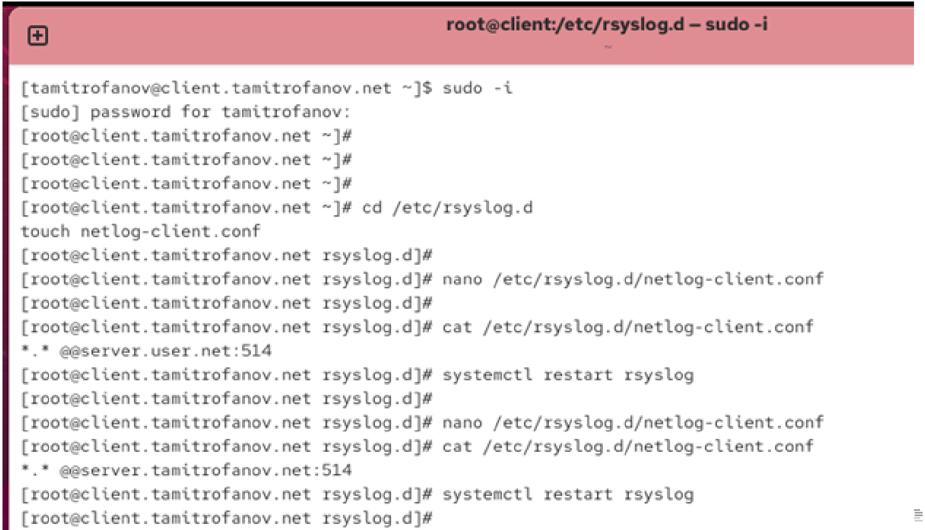
3.2 Настройка межсетевого экрана



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

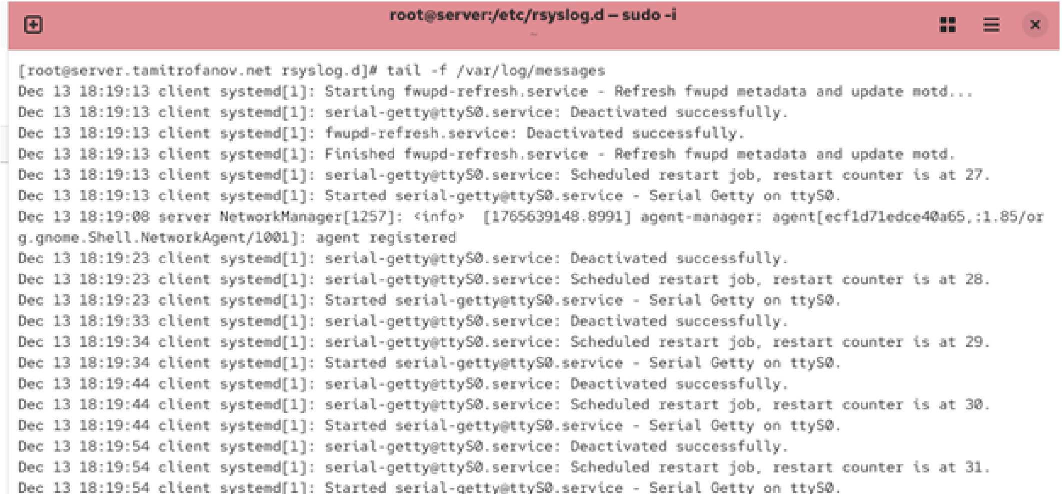
Рисунок 2: Настройка межсетевого экрана

3.3 настройка клиента



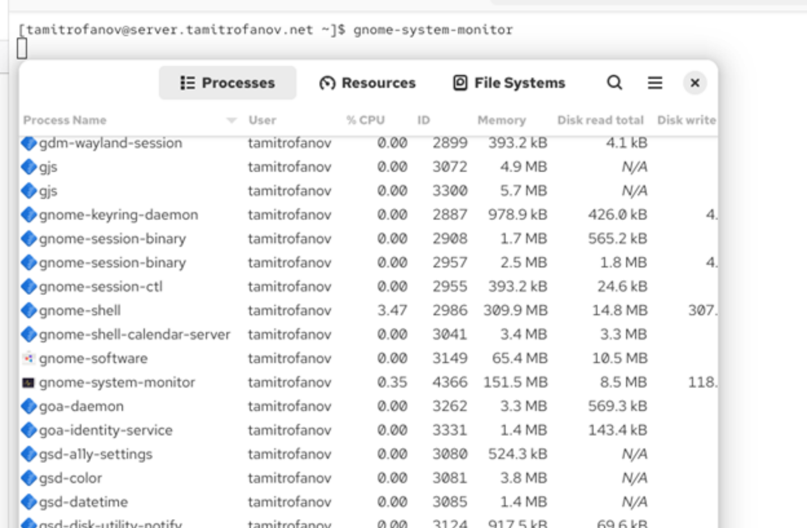
```
[tamitrofanov@client.tamitrofanov.net ~]$ sudo -i
[sudo] password for tamitrofanov:
[root@client.tamitrofanov.net ~]#
[root@client.tamitrofanov.net ~]#
[root@client.tamitrofanov.net ~]#
[root@client.tamitrofanov.net ~]# cd /etc/rsyslog.d
touch netlog-client.conf
[root@client.tamitrofanov.net rsyslog.d]#
[root@client.tamitrofanov.net rsyslog.d]# nano /etc/rsyslog.d/netlog-client.conf
[root@client.tamitrofanov.net rsyslog.d]#
[root@client.tamitrofanov.net rsyslog.d]# cat /etc/rsyslog.d/netlog-client.conf
*.* @@server.user.net:514
[root@client.tamitrofanov.net rsyslog.d]# systemctl restart rsyslog
[root@client.tamitrofanov.net rsyslog.d]#
[root@client.tamitrofanov.net rsyslog.d]# nano /etc/rsyslog.d/netlog-client.conf
[root@client.tamitrofanov.net rsyslog.d]# cat /etc/rsyslog.d/netlog-client.conf
*.* @@server.tamitrofanov.net:514
[root@client.tamitrofanov.net rsyslog.d]# systemctl restart rsyslog
[root@client.tamitrofanov.net rsyslog.d]#
```

3.4 Просмотр журнала



```
[root@server.tamitrofanov.net rsyslog.d]# tail -f /var/log/messages
Dec 13 18:19:13 client systemd[1]: Starting fwupd-refresh.service - Refresh fwupd metadata and update motd...
Dec 13 18:19:13 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 18:19:13 client systemd[1]: fwupd-refresh.service: Deactivated successfully.
Dec 13 18:19:13 client systemd[1]: Finished fwupd-refresh.service - Refresh fwupd metadata and update motd.
Dec 13 18:19:13 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 27.
Dec 13 18:19:13 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 13 18:19:08 server NetworkManager[1257]: <info>  [1765639148.8991] agent-manager: agent[ecf1d71edce40a65,:1.85/or
g.gnome.Shell.NetworkAgent/1001]: agent registered
Dec 13 18:19:23 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 18:19:23 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 28.
Dec 13 18:19:23 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 13 18:19:33 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 18:19:34 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 29.
Dec 13 18:19:34 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 13 18:19:44 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 18:19:44 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 30.
Dec 13 18:19:44 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 13 18:19:54 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 18:19:54 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 31.
Dec 13 18:19:54 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
```

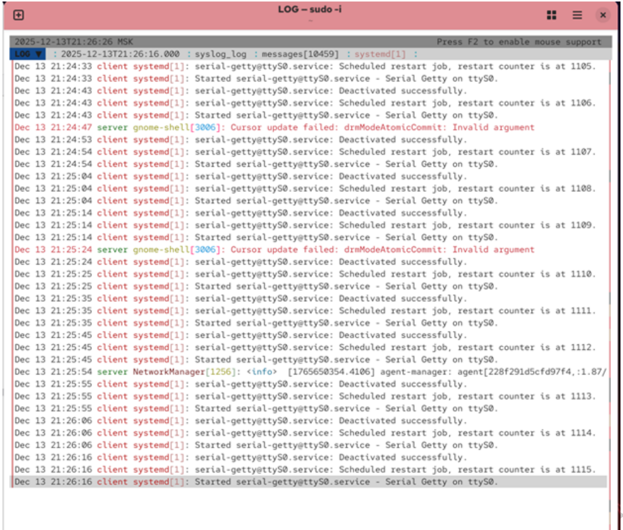
3.5 Графическое окружение



```
[tamitrofanov@server.tamitrofanov.net ~]$ gnome-system-monitor
```

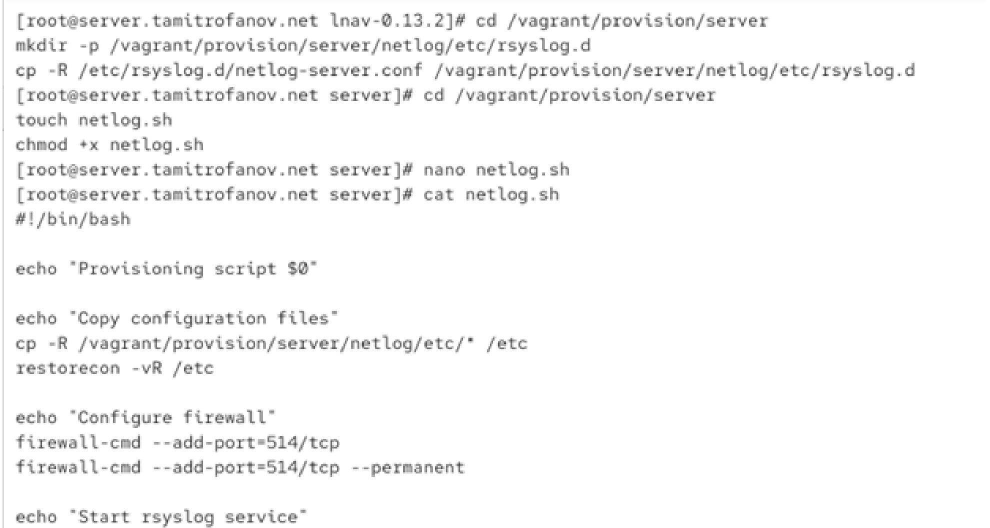
Process Name	User	% CPU	ID	Memory	Disk read total	Disk write
gdm-wayland-session	tamitrofanov	0.00	2899	393.2 kB	4.1 kB	
gjs	tamitrofanov	0.00	3072	4.9 MB	N/A	
gjs	tamitrofanov	0.00	3300	5.7 MB	N/A	
gnome-keyring-daemon	tamitrofanov	0.00	2887	978.9 kB	426.0 kB	4.
gnome-session-binary	tamitrofanov	0.00	2908	1.7 MB	565.2 kB	
gnome-session-binary	tamitrofanov	0.00	2957	2.5 MB	1.8 MB	4.
gnome-session-ctl	tamitrofanov	0.00	2955	393.2 kB	24.6 kB	
gnome-shell	tamitrofanov	3.47	2986	309.9 MB	14.8 MB	307.
gnome-shell-calendar-server	tamitrofanov	0.00	3041	3.4 MB	3.3 MB	
gnome-software	tamitrofanov	0.00	3149	65.4 MB	10.5 MB	
gnome-system-monitor	tamitrofanov	0.35	4366	151.5 MB	8.5 MB	118.
goa-daemon	tamitrofanov	0.00	3262	3.3 MB	569.3 kB	
goa-identity-service	tamitrofanov	0.00	3331	1.4 MB	143.4 kB	
gsd-a11y-settings	tamitrofanov	0.00	3080	524.3 kB	N/A	
gsd-color	tamitrofanov	0.00	3081	3.8 MB	N/A	
gsd-datetime	tamitrofanov	0.00	3085	1.4 MB	N/A	
gsd-disk-utility-notify	tamitrofanov	0.00	3124	917.5 kB	69.6 kB	

3.6 lnav



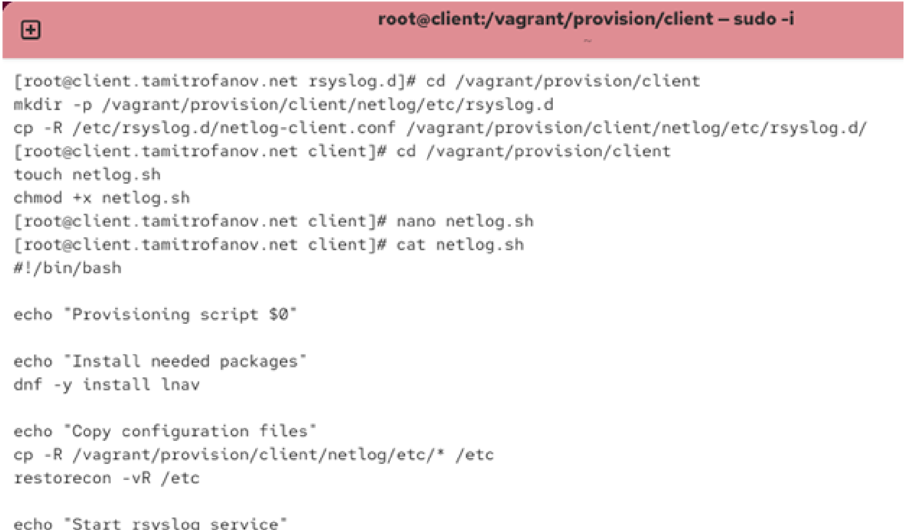
```
2025-12-13T21:26:26 MSK                                                     Press F2 to enable mouse support
LOG ▼  : 2025-12-13T21:26:16.000 : syslog_log : messages[10459] : systemd[1] :
Dec 13 21:24:33 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 1105.
Dec 13 21:24:33 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 13 21:24:43 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 21:24:43 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 1106.
Dec 13 21:24:43 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 13 21:24:47 server gnome-shell[3006]: Cursor update failed: drmModeAtomicCommit: Invalid argument
Dec 13 21:24:53 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 21:24:54 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 1107.
Dec 13 21:24:54 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 13 21:25:04 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 21:25:04 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 1108.
Dec 13 21:25:04 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 13 21:25:14 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 21:25:14 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 1109.
Dec 13 21:25:14 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 13 21:25:24 server gnome-shell[3006]: Cursor update failed: drmModeAtomicCommit: Invalid argument
Dec 13 21:25:24 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 21:25:25 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 1110.
Dec 13 21:25:25 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 13 21:25:35 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 21:25:35 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 1111.
Dec 13 21:25:35 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 13 21:25:45 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 21:25:45 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 1112.
Dec 13 21:25:45 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 13 21:25:54 server NetworkManager[1256]: <info>  [1765650354.4106] agent-manager: agent[228f291d5cfd97f4,:1.87/
Dec 13 21:25:55 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 21:25:55 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 1113.
Dec 13 21:25:55 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 13 21:26:06 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 21:26:06 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 1114.
Dec 13 21:26:06 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 13 21:26:16 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 21:26:16 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 1115.
Dec 13 21:26:16 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
```

3.7 Настройка запуска службы на сервере



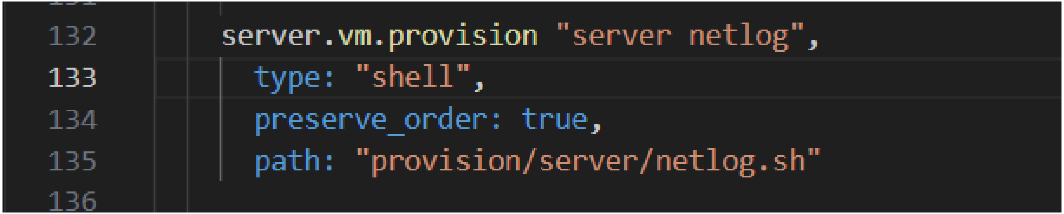
```
[root@server.tamitrofanov.net lnav-0.13.2]# cd /vagrant/provision/server
mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d
cp -R /etc/rsyslog.d/netlog-server.conf /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server.tamitrofanov.net server]# cd /vagrant/provision/server
touch netlog.sh
chmod +x netlog.sh
[root@server.tamitrofanov.net server]# nano netlog.sh
[root@server.tamitrofanov.net server]# cat 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"
```

3.8 Настройка запуска службы на клиенте



```
[root@client.tamitrofanov.net rsyslog.d]# 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/
[root@client.tamitrofanov.net client]# cd /vagrant/provision/client
touch netlog.sh
chmod +x netlog.sh
[root@client.tamitrofanov.net client]# nano netlog.sh
[root@client.tamitrofanov.net client]# cat 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"
```

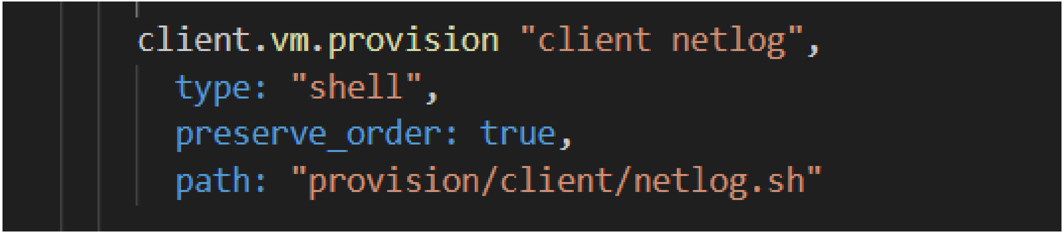
3.9 Вагрант для сервера



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

Рисунок 9: Вагрант для сервера

3.10 Вагрант для клиента



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

Рисунок 10: Вагрант для клиента

Раздел 4

4. Выводы

4.1 слайд 1

Сегодня я получил навыки по работе с журналами системных событий.