

Презентация по лабораторной работе №15

Настройка сетевого журналирования

Галацан Николай

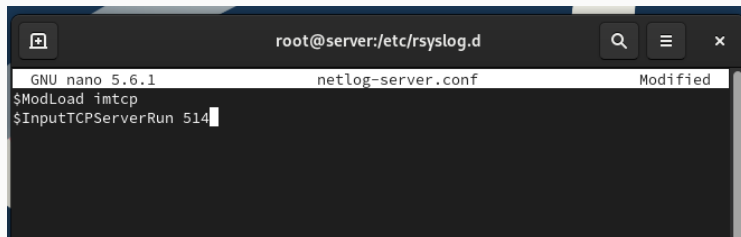
Российский университет дружбы народов, Москва, Россия

- Галацан Николай
- 1032225763
- уч. группа: НПИбд-01-22
- Факультет физико-математических и естественных наук
- Российский университет дружбы народов

Получение навыков по работе с журналами системных событий.

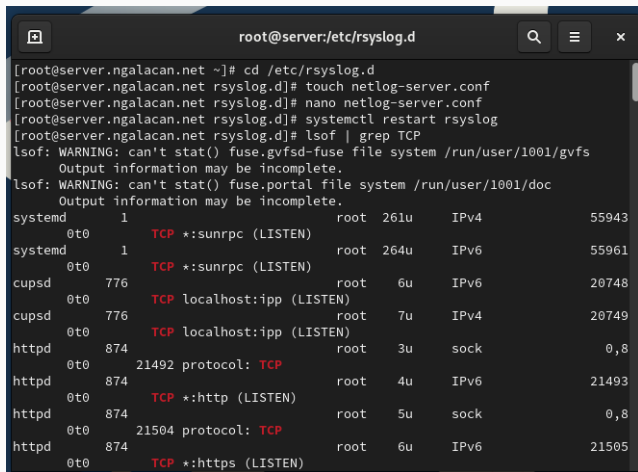
Настройка сервера сетевого журнала

```
cd /etc/rsyslog.d  
touch netlog-server.conf
```



```
root@server:/etc/rsyslog.d
GNU nano 5.6.1 netlog-server.conf Modified
$ModLoad imtcp
$InputTCPServerRun 514
```

Рис. 1: Редактирование файла конфигурации сетевого хранения журналов
`/etc/rsyslog.d/netlog-server.conf`



```
root@server:/etc/rsyslog.d

[root@server.ngalacan.net ~]# cd /etc/rsyslog.d
[root@server.ngalacan.net rsyslog.d]# touch netlog-server.conf
[root@server.ngalacan.net rsyslog.d]# nano netlog-server.conf
[root@server.ngalacan.net rsyslog.d]# systemctl restart rsyslog
[root@server.ngalacan.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    261u      IPv4      55943
   0t0      TCP *:sunrpc (LISTEN)
systemd      1      root    264u      IPv6      55961
   0t0      TCP *:sunrpc (LISTEN)
cupsd        776    root      6u      IPv6      20748
   0t0      TCP localhost:ipp (LISTEN)
cupsd        776    root      7u      IPv4      20749
   0t0      TCP localhost:ipp (LISTEN)
httpd        874    root      3u      sock      0,8
   0t0      21492 protocol: TCP
httpd        874    root      4u      IPv6      21493
   0t0      TCP *:http (LISTEN)
httpd        874    root      5u      sock      0,8
   0t0      21504 protocol: TCP
httpd        874    root      6u      IPv6      21505
   0t0      TCP *:https (LISTEN)
```

Рис. 2: Перезапуск `rsyslog` и просмотр прослушиваемых портов

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


Настройка клиента сетевого журнала

```
cd /etc/rsyslog.d  
touch netlog-client.conf
```

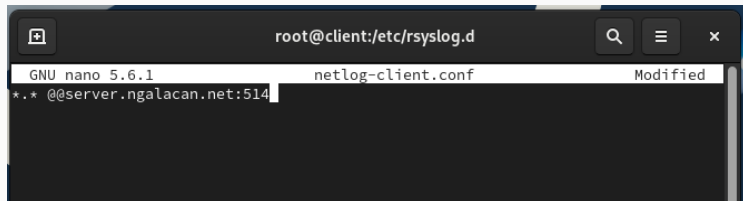
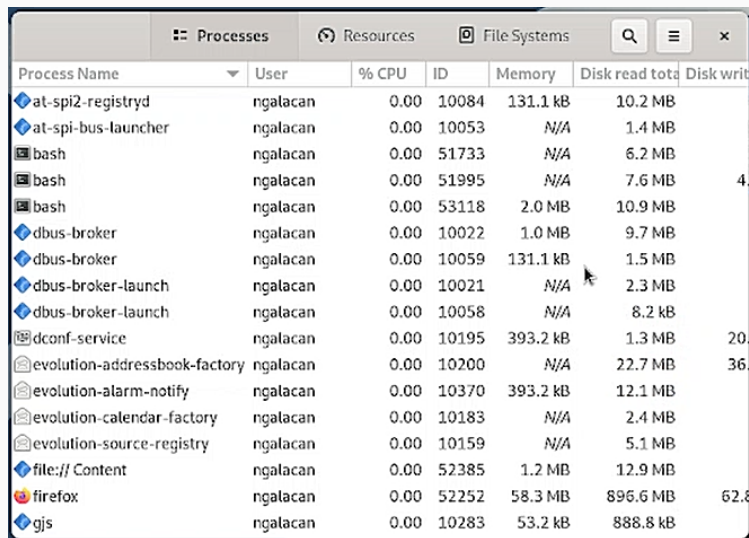


Рис. 3: Редактирование файла конфигурации сетевого хранения журналов на клиенте: включение перенаправления на 514 порт

Просмотр журнала

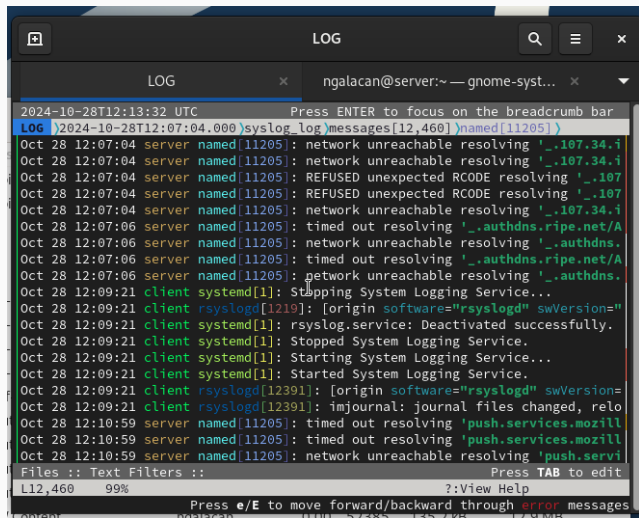
```
[root@server.ngalacan.net rsyslog.d]# tail -f /var/log/messages
Oct 28 12:07:06 server named[11205]: timed out resolving '_authdns.ripe.net/A/IN': 127.0.0.1#53
Oct 28 12:07:06 server named[11205]: network unreachable resolving '_authdns.ripe.net/A/IN': 2001:500:14:6100:ad::1#53
Oct 28 12:09:21 client systemd[1]: Stopping System Logging Service...
Oct 28 12:09:21 client rsyslogd[1219]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="1219" x-info="https://www.rsyslog.com"] exiting on signal 15.
Oct 28 12:09:21 client systemd[1]: rsyslog.service: Deactivated successfully.
Oct 28 12:09:21 client systemd[1]: Stopped System Logging Service.
Oct 28 12:09:21 client systemd[1]: Starting System Logging Service...
Oct 28 12:09:21 client systemd[1]: Started System Logging Service.
Oct 28 12:09:21 client rsyslogd[12391]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="12391" x-info="https://www.rsyslog.com"] start
Oct 28 12:09:21 client rsyslogd[12391]: imjournal: journal files changed, reloading... [v8.2310.0-4.el9 try https://www.rsyslog.com/e/0 ]
```

Рис. 4: Просмотр файла журнала на сервере



Process Name	User	% CPU	ID	Memory	Disk read total	Disk write total
at-spi2-registryd	ngalacan	0.00	10084	131.1 kB	10.2 MB	
at-spi-bus-launcher	ngalacan	0.00	10053	N/A	1.4 MB	
bash	ngalacan	0.00	51733	N/A	6.2 MB	
bash	ngalacan	0.00	51995	N/A	7.6 MB	4.0 MB
bash	ngalacan	0.00	53118	2.0 MB	10.9 MB	
dbus-broker	ngalacan	0.00	10022	1.0 MB	9.7 MB	
dbus-broker	ngalacan	0.00	10059	131.1 kB	1.5 MB	
dbus-broker-launch	ngalacan	0.00	10021	N/A	2.3 MB	
dbus-broker-launch	ngalacan	0.00	10058	N/A	8.2 kB	
dconf-service	ngalacan	0.00	10195	393.2 kB	1.3 MB	20.0 MB
evolution-addressbook-factory	ngalacan	0.00	10200	N/A	22.7 MB	36.0 MB
evolution-alarm-notify	ngalacan	0.00	10370	393.2 kB	12.1 MB	
evolution-calendar-factory	ngalacan	0.00	10183	N/A	2.4 MB	
evolution-source-registry	ngalacan	0.00	10159	N/A	5.1 MB	
file:/// Content	ngalacan	0.00	52385	1.2 MB	12.9 MB	
firefox	ngalacan	0.00	52252	58.3 MB	896.6 MB	62.8 MB
gjs	ngalacan	0.00	10283	53.2 kB	888.8 kB	

Рис. 5: Запуск графической программы для просмотра журналов



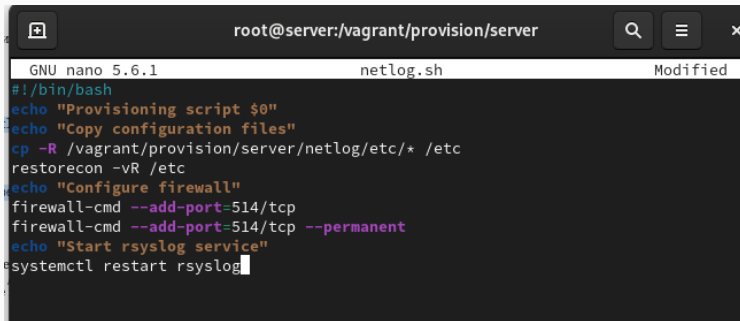
The screenshot shows a terminal window titled "LOG" with a search icon, a menu icon, and a close icon. The window displays a list of system logs. The first line is "2024-10-28T12:13:32 UTC Press ENTER to focus on the breadcrumb bar". The second line is "LOG >2024-10-28T12:07:04.000>syslog_log>messages[12,460]>named[11205]>". The logs are color-coded: "server" is orange, "client" is green, and "named[11205]" is blue. The logs show network unreachable errors, DNS resolution timeouts, and system service status changes. The bottom of the window shows a breadcrumb bar with "Files :: Text Filters ::" and "Press TAB to edit". The status bar at the bottom shows "Press e/E to move forward/backward through error messages".

```
2024-10-28T12:13:32 UTC Press ENTER to focus on the breadcrumb bar
LOG >2024-10-28T12:07:04.000>syslog_log>messages[12,460]>named[11205]>
Oct 28 12:07:04 server named[11205]: network unreachable resolving '._.107.34.i
Oct 28 12:07:04 server named[11205]: network unreachable resolving '._.107.34.i
Oct 28 12:07:04 server named[11205]: REFUSED unexpected RCODE resolving '._.107
Oct 28 12:07:04 server named[11205]: REFUSED unexpected RCODE resolving '._.107
Oct 28 12:07:04 server named[11205]: network unreachable resolving '._.107.34.i
Oct 28 12:07:06 server named[11205]: timed out resolving '._.authdns.ripe.net/A
Oct 28 12:07:06 server named[11205]: network unreachable resolving '._.authdns.
Oct 28 12:07:06 server named[11205]: timed out resolving '._.authdns.ripe.net/A
Oct 28 12:07:06 server named[11205]: network unreachable resolving '._.authdns.
Oct 28 12:09:21 client systemd[1]: Stopping System Logging Service...
Oct 28 12:09:21 client rsyslogd[1219]: [origin software="rsyslogd" swVersion="
Oct 28 12:09:21 client systemd[1]: rsyslog.service: Deactivated successfully.
Oct 28 12:09:21 client systemd[1]: Stopped System Logging Service.
Oct 28 12:09:21 client systemd[1]: Starting System Logging Service...
Oct 28 12:09:21 client systemd[1]: Started System Logging Service.
Oct 28 12:09:21 client rsyslogd[12391]: [origin software="rsyslogd" swVersion=
Oct 28 12:09:21 client rsyslogd[12391]: imjournal: journal files changed, relo
Oct 28 12:10:59 server named[11205]: timed out resolving 'push.services.mozill
Oct 28 12:10:59 server named[11205]: timed out resolving 'push.services.mozill
Oct 28 12:10:59 server named[11205]: network unreachable resolving 'push.servi
Files :: Text Filters :: Press TAB to edit
L12,460 99% ?::View Help
Press e/E to move forward/backward through error messages
```

Рис. 6: Использование lnav для просмотра логов

Внесение изменений в настройки
внутреннего окружения
виртуальной машины

```
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
```

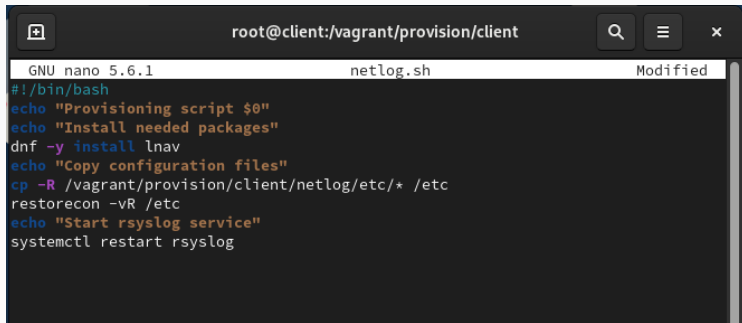


The screenshot shows a terminal window with the title bar 'root@server:/vagrant/provision/server'. The window contains the GNU nano 5.6.1 editor editing the file 'netlog.sh'. The editor's status bar at the top indicates 'GNU nano 5.6.1', 'netlog.sh', and 'Modified'. The code being edited is as follows:

```
#!/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. 7: Редактирование netlog.sh на сервере

```
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:/vagrant/provision/client

GNU nano 5.6.1 netlog.sh Modified
#!/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
```

Рис. 8: Редактирование netlog.sh на клиенте

```
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"
```

В результате выполнения работы были приобретены навыки по работе с журналами системных событий.