

Лабораторная работа №15

Администрирование сетевых подсистем

Мишина А. А.

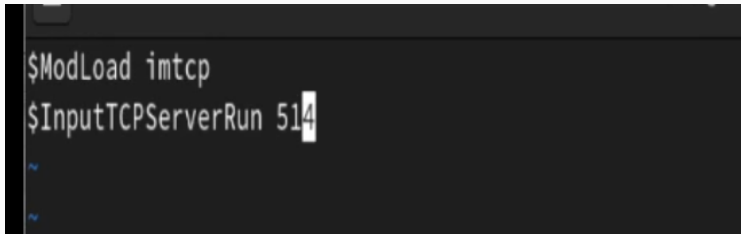
5 декабря 2024

Получение навыков по работе с журналами системных событий.

Выполнение лабораторной работы

На сервере создадим файл конфигурации сетевого хранения журналов:

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



```
$ModLoad imtcp  
$InputTCPServerRun 514
```

The image shows a terminal window with a dark background. The first line of text is '\$ModLoad imtcp' and the second line is '\$InputTCPServerRun 514'. A white cursor is positioned at the end of the second line. Below the second line, there are two blue tilde characters '~' on separate lines, indicating the prompt.

Рис. 1: Включение журналирования по TCP-порту 514

Настройка сервера сетевого журнала

```
rsyslogd 6677          root    4u    IPv4    42173    0t0    TCP *:shell (LISTEN)
rsyslogd 6677          root    5u    IPv6    42174    0t0    TCP *:shell (LISTEN)
rsyslogd 6677 6679 in:imjour  root    4u    IPv4    42173    0t0    TCP *:shell (LISTEN)
rsyslogd 6677 6679 in:imjour  root    5u    IPv6    42174    0t0    TCP *:shell (LISTEN)
rsyslogd 6677 6680 in:imtcp   root    4u    IPv4    42173    0t0    TCP *:shell (LISTEN)
rsyslogd 6677 6680 in:imtcp   root    5u    IPv6    42174    0t0    TCP *:shell (LISTEN)
rsyslogd 6677 6681 in:imtcp   root    4u    IPv4    42173    0t0    TCP *:shell (LISTEN)
rsyslogd 6677 6681 in:imtcp   root    5u    IPv6    42174    0t0    TCP *:shell (LISTEN)
rsyslogd 6677 6682 in:imtcp   root    4u    IPv4    42173    0t0    TCP *:shell (LISTEN)
rsyslogd 6677 6682 in:imtcp   root    5u    IPv6    42174    0t0    TCP *:shell (LISTEN)
rsyslogd 6677 6683 in:imtcp   root    4u    IPv4    42173    0t0    TCP *:shell (LISTEN)
rsyslogd 6677 6683 in:imtcp   root    5u    IPv6    42174    0t0    TCP *:shell (LISTEN)
rsyslogd 6677 6684 in:imtcp   root    4u    IPv4    42173    0t0    TCP *:shell (LISTEN)
rsyslogd 6677 6684 in:imtcp   root    5u    IPv6    42174    0t0    TCP *:shell (LISTEN)
rsyslogd 6677 6685 rs:main    root    4u    IPv4    42173    0t0    TCP *:shell (LISTEN)
rsyslogd 6677 6685 rs:main    root    5u    IPv6    42174    0t0    TCP *:shell (LISTEN)
[root@server.aamishina.net ~]#
```

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

```
[root@server.aamishina.net ~]# firewall-cmd --add-port=514/tcp  
success  
[root@server.aamishina.net ~]# firewall-cmd --add-port=514/tcp --permanent  
success  
[root@server.aamishina.net ~]# █
```

Рис. 3: Настройка межсетевого экрана для работы с TCP-портом 514

На клиенте создадим файл конфигурации сетевого хранения журналов:

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

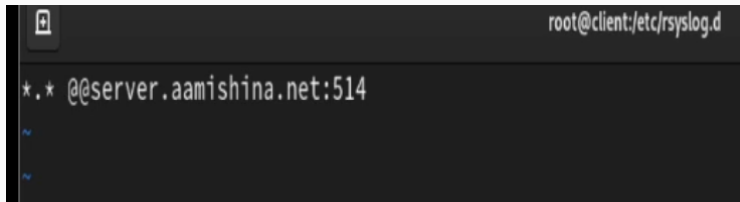
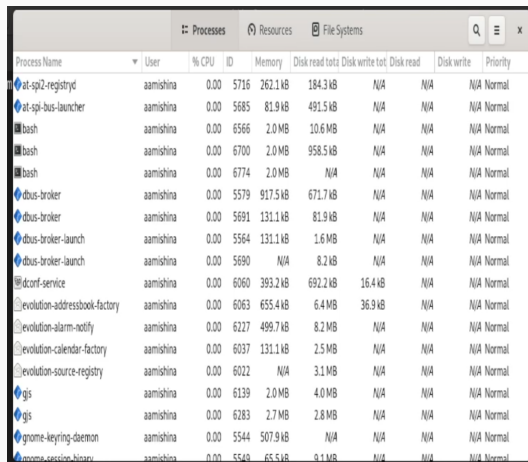



Рис. 4: Редактирование файла конфигурации сетевого хранения журналов на клиенте: включение перенаправления на 514 порт

```
systemctl restart rsyslog
```

```
[root@server.aamishina.net ~]# tail -f /var/log/messages
Oct 27 17:46:24 client rsyslogd[1210]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="1210"
" x-info="https://www.rsyslog.com"] exiting on signal 15.
Oct 27 17:46:24 client systemd[1]: rsyslog.service: Deactivated successfully.
Oct 27 17:46:24 client systemd[1]: Stopped System Logging Service.
Oct 27 17:46:24 client systemd[1]: Starting System Logging Service...
Oct 27 17:46:24 client systemd[1]: Started System Logging Service.
Oct 27 17:46:24 client rsyslogd[6817]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="6817"
" x-info="https://www.rsyslog.com"] start
Oct 27 17:46:24 client rsyslogd[6817]: imjournal: journal files changed, reloading... [v8.2310.0-4.el9 t
ry https://www.rsyslog.com/e/0 ]
Oct 27 17:46:35 server systemd[5482]: Created slice User Background Tasks Slice.
Oct 27 17:46:35 server systemd[5482]: Starting Cleanup of User's Temporary Files and Directories...
Oct 27 17:46:35 server systemd[5482]: Finished Cleanup of User's Temporary Files and Directories.
Oct 27 17:46:42 server systemd[1]: packagekit.service: Deactivated successfully.
Oct 27 17:46:42 server systemd[1]: packagekit.service: Consumed 1.738s CPU time.
```

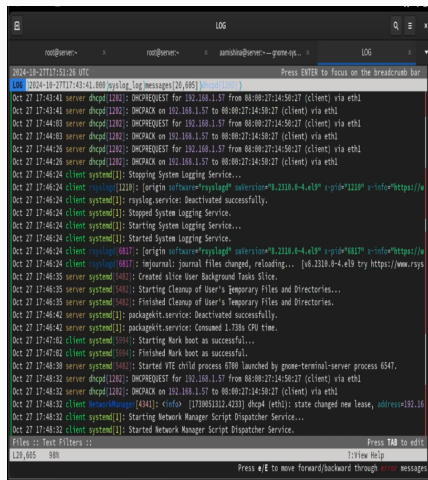
Рис. 5: Просмотр файла журнала на сервере



Processes									
Process Name	User	% CPU	ID	Memory	Disk read tot	Disk write tot	Disk read	Disk write	Priority
at-spi2-registryd	aamishina	0.00	5716	262.1 kB	184.3 kB	N/A	N/A	N/A	Normal
at-spi-bus-launcher	aamishina	0.00	5685	81.9 kB	491.5 kB	N/A	N/A	N/A	Normal
bash	aamishina	0.00	6566	2.0 MB	10.6 MB	N/A	N/A	N/A	Normal
bash	aamishina	0.00	6700	2.0 MB	958.5 kB	N/A	N/A	N/A	Normal
bash	aamishina	0.00	6774	2.0 MB	N/A	N/A	N/A	N/A	Normal
dbus-broker	aamishina	0.00	5579	917.5 kB	671.7 kB	N/A	N/A	N/A	Normal
dbus-broker	aamishina	0.00	5691	131.1 kB	81.9 kB	N/A	N/A	N/A	Normal
dbus-broker-launch	aamishina	0.00	5564	131.1 kB	1.6 MB	N/A	N/A	N/A	Normal
dbus-broker-launch	aamishina	0.00	5690	N/A	8.2 kB	N/A	N/A	N/A	Normal
dconf-service	aamishina	0.00	6060	393.2 kB	692.2 kB	16.4 kB	N/A	N/A	Normal
evolution-addressbook-factory	aamishina	0.00	6063	655.4 kB	6.4 MB	36.9 kB	N/A	N/A	Normal
evolution-alarm-notify	aamishina	0.00	6227	499.7 kB	8.2 MB	N/A	N/A	N/A	Normal
evolution-calendar-factory	aamishina	0.00	6037	131.1 kB	2.5 MB	N/A	N/A	N/A	Normal
evolution-source-registry	aamishina	0.00	6022	N/A	3.1 MB	N/A	N/A	N/A	Normal
gis	aamishina	0.00	6139	2.0 MB	4.0 MB	N/A	N/A	N/A	Normal
gis	aamishina	0.00	6283	2.7 MB	2.8 MB	N/A	N/A	N/A	Normal
gnome-keyring-daemon	aamishina	0.00	5544	507.9 kB	N/A	N/A	N/A	N/A	Normal
gnome-session-binary	aamishina	0.00	5549	65.5 kB	9.1 MB	N/A	N/A	N/A	Normal

Рис. 6: Запуск графической программы для просмотра журналов

```
dnf -y install lnav
```

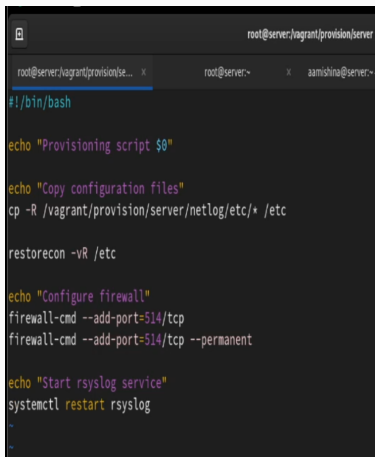


```
LOG
root@server:~ x root@server:~ x amishra@server:~ gnome-tp... x LOG x
2024-10-27T17:51:26 UTC Press ENTER to focus on the breadcrumb bar
LOG [2024-10-27T17:43:41.600 syslog_log[messages[20,605] %bpcd[100]]
Oct 27 17:43:41 server dhcpd[1202]: DHCPREQUEST for 192.168.1.57 from 08:00:27:14:50:27 (client) via eth1
Oct 27 17:43:41 server dhcpd[1202]: DHCPACK on 192.168.1.57 to 08:00:27:14:50:27 (client) via eth1
Oct 27 17:44:03 server dhcpd[1202]: DHCPREQUEST for 192.168.1.57 from 08:00:27:14:50:27 (client) via eth1
Oct 27 17:44:03 server dhcpd[1202]: DHCPACK on 192.168.1.57 to 08:00:27:14:50:27 (client) via eth1
Oct 27 17:44:26 server dhcpd[1202]: DHCPREQUEST for 192.168.1.57 from 08:00:27:14:50:27 (client) via eth1
Oct 27 17:44:26 server dhcpd[1202]: DHCPACK on 192.168.1.57 to 08:00:27:14:50:27 (client) via eth1
Oct 27 17:46:24 client systemd[1]: Stopping System Logging Service...
Oct 27 17:46:24 client rsyslogd[1210]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="1210" x-info="https://
Oct 27 17:46:24 client systemd[1]: rsyslog.service: Deactivated successfully.
Oct 27 17:46:24 client systemd[1]: Stopped System Logging Service.
Oct 27 17:46:24 client systemd[1]: Starting System Logging Service...
Oct 27 17:46:24 client systemd[1]: Started System Logging Service.
Oct 27 17:46:24 client rsyslogd[6817]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="6817" x-info="https://
Oct 27 17:46:24 client rsyslogd[6817]: imjournal: journal files changed, reloading... [v8.2310.0-4.el9 try https://www.rsys
Oct 27 17:46:35 server systemd[5402]: Created alice User Background Tasks Slice.
Oct 27 17:46:35 server systemd[5402]: Starting Cleanup of User's Temporary Files and Directories...
Oct 27 17:46:35 server systemd[5402]: Finished Cleanup of User's Temporary Files and Directories.
Oct 27 17:46:42 server systemd[1]: packagekit.service: Deactivated successfully.
Oct 27 17:46:42 server systemd[1]: packagekit.service: Consumed 1.738s CPU time.
Oct 27 17:47:02 client systemd[5094]: Starting Mark boot as successful...
Oct 27 17:47:02 client systemd[5094]: Finished Mark boot as successful.
Oct 27 17:48:30 server systemd[5402]: Started VTE child process 6700 launched by gnome-terminal-server process 6547.
Oct 27 17:48:32 server dhcpd[1202]: DHCPREQUEST for 192.168.1.57 from 08:00:27:14:50:27 (client) via eth1
Oct 27 17:48:32 server dhcpd[1202]: DHCPACK on 192.168.1.57 to 08:00:27:14:50:27 (client) via eth1
Oct 27 17:48:32 client NetworkManager[4341]: <info> [1730051312.4233] dhcp4 (eth1): state changed new Lease, address=192.16
Oct 27 17:48:32 client systemd[1]: Starting Network Manager Script Dispatcher Service...
Oct 27 17:48:32 client systemd[1]: Started Network Manager Script Dispatcher Service.
Files :: Text Filters :: Press TAB to edit:
L20,605 98n ::View Help
Press e/E to move forward/backward through error messages
```

Рис. 7: Использование `lnav` для просмотра логов

```
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/  
  
touch netlog.sh  
chmod +x netlog.sh
```

Внесение изменений в настройки внутреннего окружения виртуальной машины



```
root@server:/vagrant/provision/server

root@server:/vagrant/provision/se... x root@server:~ x aamishina@server:~

#!/bin/bash

echo "Provisioning script $0"

echo "Copy configuration files"
cp -R /vagrant/provision/server/netlog/etc/* /etc

restorecon -vR /etc

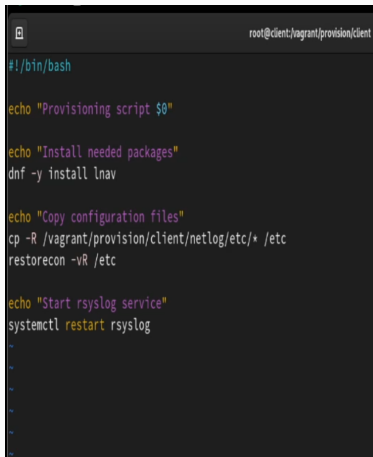
echo "Configure firewall"
firewall-cmd --add-port=514/tcp
firewall-cmd --add-port=514/tcp --permanent

echo "Start rsyslog service"
systemctl restart rsyslog
```

Рис. 8: Скрипт файла /vagrant/provision/server/netlog.sh


```
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/  
  
touch netlog.sh  
chmod +x netlog.sh
```

Внесение изменений в настройки внутреннего окружения виртуальной машины



```
root@client:/vagrant/provision/client

#!/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. 9: Скрипт файла /vagrant/provision/client/netlog.sh

```
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 данной работы были приобретены практические навыки по работе с журналами системных событий.