

Защита лабораторной работы № 15

Настройка сетевого журналирования

Администрирование сетевых подсистем

Работу Выполнил:
Саинт-Амур Измаэль
Группа: НПИбд-02-20

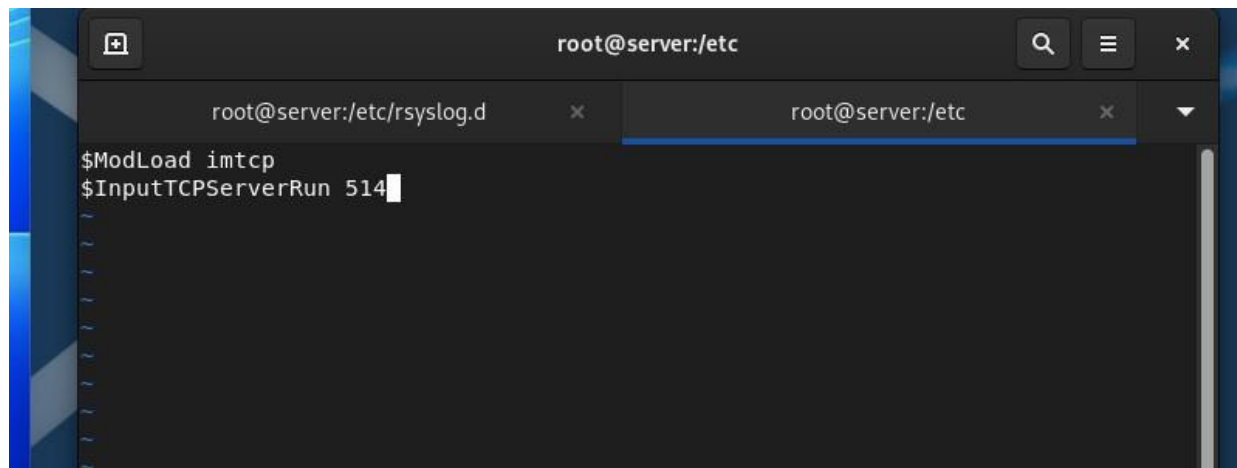


Цель работы

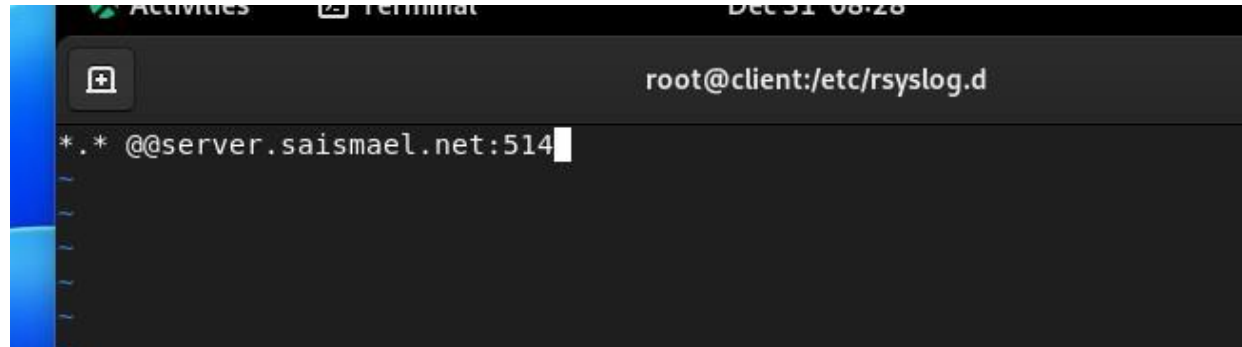
Получение навыков по работе с журналами системных событий.

```
[root@server.saismael.net ~]# cd /etc/rsyslog.d
[root@server.saismael.net rsyslog.d]# touch netlog-server.conf
[root@server.saismael.net rsyslog.d]#
```

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



Настройка клиента сетевого журнала



A terminal window titled "root@client:/etc/rsyslog.d" with a window icon on the left. The terminal shows the command `*.* @@server.saismael.net:514` being entered at the prompt.

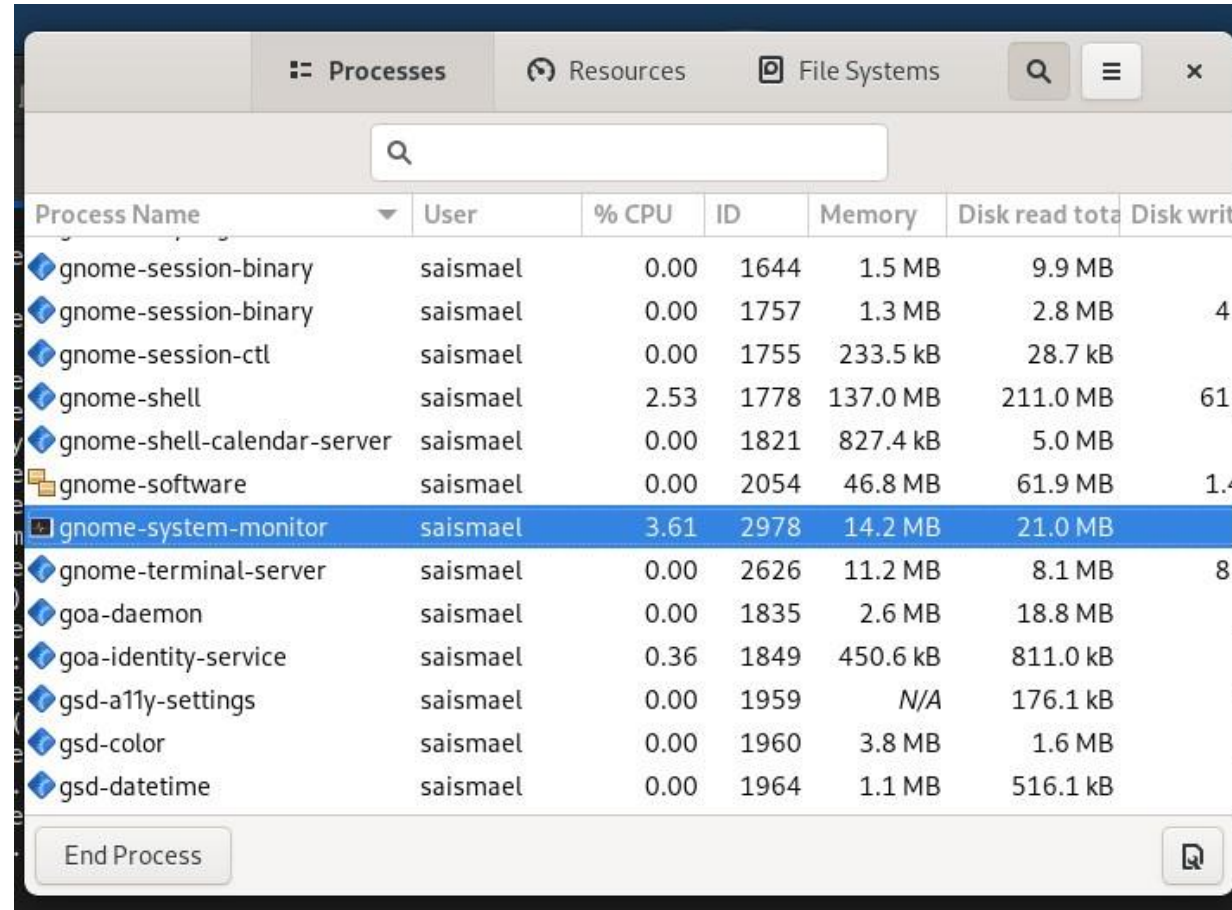
```
root@client:/etc/rsyslog.d
*.* @@server.saismael.net:514
```

```
[root@client.saismael.net ~]# cd /etc/rsyslog.d
[root@client.saismael.net rsyslog.d]# touch netlog-client.conf
[root@client.saismael.net rsyslog.d]#
[root@client.saismael.net rsyslog.d]# vi /etc/rsyslog.d/netlog-client.conf
[root@client.saismael.net rsyslog.d]#
[root@client.saismael.net rsyslog.d]# systemctl restart rsyslog
[root@client.saismael.net rsyslog.d]#
[root@client.saismael.net rsyslog.d]#
```

Просмотр журнала

```
[root@server.saismael.net rsyslog.d]#  
[root@server.saismael.net rsyslog.d]# tail -f /var/log/messages  
Dec 31 08:30:22 client systemd[1]: Starting System Logging Service...  
Dec 31 08:30:23 client systemd[1]: Started System Logging Service.  
Dec 31 08:30:23 client rsyslogd[2270]: [origin software="rsyslogd" swVersion="8.2102.0-101.el9_0.1" x-pid="2270" x-info="https://www.rsyslog.com"] start  
Dec 31 08:30:23 client rsyslogd[2270]: imjournal: journal files changed, reloading... [v8.2102.0-101.el9_0.1 try https://www.rsyslog.com/e/0 ]  
Dec 31 08:30:26 client dnf[2269]: Extra Packages for Enterprise Linux 9 - x86_64  
26 kB/s | 25 kB 00:00  
Dec 31 08:30:36 client dnf[2269]: Extra Packages for Enterprise Linux 9 - x86_64  
1.2 MB/s | 12 MB 00:10  
Dec 31 08:30:56 server named[837]: network unreachable resolving 'ns3.fastly.net /AAAA/IN': 2001:502:7094::30#53  
Dec 31 08:30:56 server named[837]: network unreachable resolving 'ns3.fastly.net /AAAA/IN': 2001:503:a83e::2:30#53  
Dec 31 08:30:57 client dnf[2269]: Rocky Linux 9 - BaseOS  
2.2 kB/s | 3.6 kB 00:01  
Dec 31 08:30:58 client dnf[2269]: Rocky Linux 9 - AppStream  
3.8 kB/s | 4.1 kB 00:01  
Dec 31 08:31:00 client dnf[2269]: Rocky Linux 9 - Extras  
2.5 kB/s | 2.9 kB 00:01
```


Просмотр журнала



Process Name	User	% CPU	ID	Memory	Disk read total	Disk write total
gnome-session-binary	saismael	0.00	1644	1.5 MB	9.9 MB	
gnome-session-binary	saismael	0.00	1757	1.3 MB	2.8 MB	4.0 MB
gnome-session-ctl	saismael	0.00	1755	233.5 kB	28.7 kB	
gnome-shell	saismael	2.53	1778	137.0 MB	211.0 MB	61.0 MB
gnome-shell-calendar-server	saismael	0.00	1821	827.4 kB	5.0 MB	
gnome-software	saismael	0.00	2054	46.8 MB	61.9 MB	1.4 MB
gnome-system-monitor	saismael	3.61	2978	14.2 MB	21.0 MB	
gnome-terminal-server	saismael	0.00	2626	11.2 MB	8.1 MB	8.0 MB
goa-daemon	saismael	0.00	1835	2.6 MB	18.8 MB	
goa-identity-service	saismael	0.36	1849	450.6 kB	811.0 kB	
gsd-a11y-settings	saismael	0.00	1959	N/A	176.1 kB	
gsd-color	saismael	0.00	1960	3.8 MB	1.6 MB	
gsd-datetime	saismael	0.00	1964	1.1 MB	516.1 kB	

End Process

Внесение изменений в настройки внутреннего окружения виртуальной машины

```
ntp.sh x ntp.sh x nfs.sh x nfs.sh x smb.sh x smb.sh x netlog.sh x netlog.sh x
1  #!/bin/bash
2
3  echo "Provisioning script $0"
4
5  echo "Copy configuration files"
6  cp -R /vagrant/provision/server/netlog/etc/* /etc
7  restorecon -vR /etc
8
9  echo "Configure firewall"
10 firewall-cmd --add-port=514/tcp
11 firewall-cmd --add-port=514/tcp --permanent
12
13 echo "Start rsyslog service"
14 systemctl restart rsyslog
15
```

```
[root@server.saismael.net server]# cp -R /etc/rsyslog.d/netlog-server.conf /vagr
ant/provision/server/netlog/etc/rsyslog.d/
[root@server.saismael.net server]# cd /vagrant/provision/server
[root@server.saismael.net server]# touch netlog.sh
[root@server.saismael.net server]# chmod +x netlog.sh
[root@server.saismael.net server]#
```

Получил навыки по работе с журналами
системных событий.