

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ №15

дисциплина: администрирование локальных подсистем

Студент: Саинт-Амур Измаэль

Группа: НПИбд-02-20

МОСКВА

2023 г.

Постановка задачи

Получение навыков по работе с журналами системных событий.

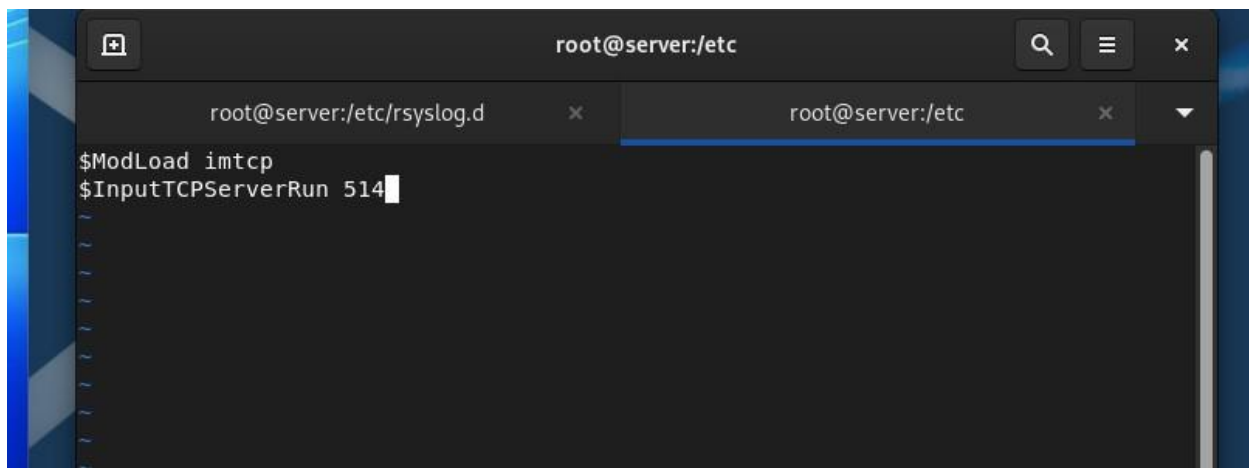
Выполнение работы

15.4.1. Настройка сервера сетевого журнала

1. На сервере создал файл конфигурации сетевого хранения журналов:

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

2. В файле конфигурации /etc/rsyslog.d/netlog-server.conf включил приём записей журнала по TCP-порту 514:



3. Перезапустил службу rsyslog и посмотрел, какие порты, связанные с rsyslog, прослушиваются:

```
[root@server.saismael.net rsyslog.d]# systemctl restart rsyslog
[root@server.saismael.net rsyslog.d]#
[root@server.saismael.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.
```

Process	PID	Protocol	Address	State	User	FD	IP	Port
systemd	1	TCP	*:sunrpc	(LISTEN)	root	42u	IPv4	16950
systemd	1	TCP	*:sunrpc	(LISTEN)	root	44u	IPv6	16966
rpcbind	515	TCP	*:sunrpc	(LISTEN)	rpc	4u	IPv4	16950
rpcbind	515	TCP	*:sunrpc	(LISTEN)	rpc	6u	IPv6	16966
cupsd	789	TCP	localhost:ipp	(LISTEN)	root	6u	IPv6	20977
cupsd	789	TCP	localhost:ipp	(LISTEN)	root	7u	IPv4	20978
sshd	799	TCP	*:ssh	(LISTEN)	root	3u	IPv4	21001
sshd	799	TCP	*:ssh	(LISTEN)	root	4u	IPv6	21010

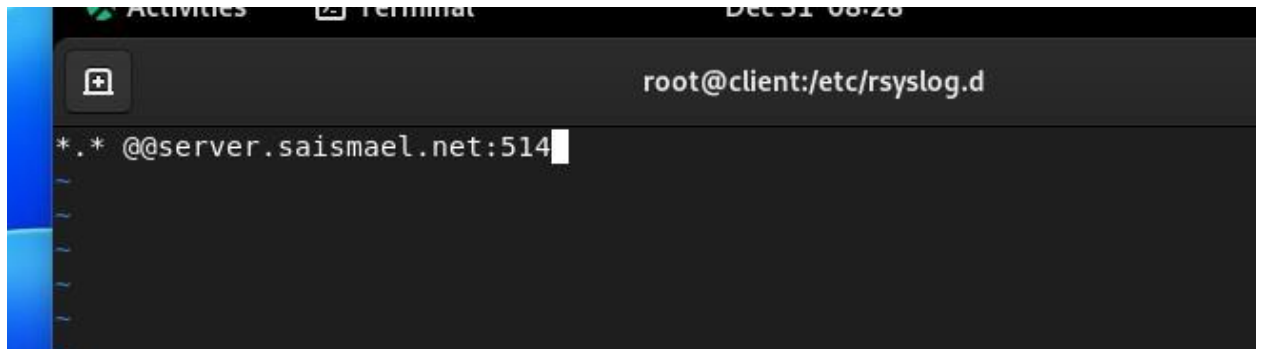
4. На сервере настроил межсетевой экран для приёма сообщений по TCP-порту 514:

```
[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]#
```

15.4.2. Настройка клиента сетевого журнала

1. На клиенте создал файл конфигурации сетевого хранения журналов:

2. На клиенте в файле конфигурации `/etc/rsyslog.d/netlog-client.conf` включил перенаправление сообщений журнала на 514 TCP-порт



3. Перезапустил службу rsyslog:

```
[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]#
```

15.4.3. Просмотр журнала

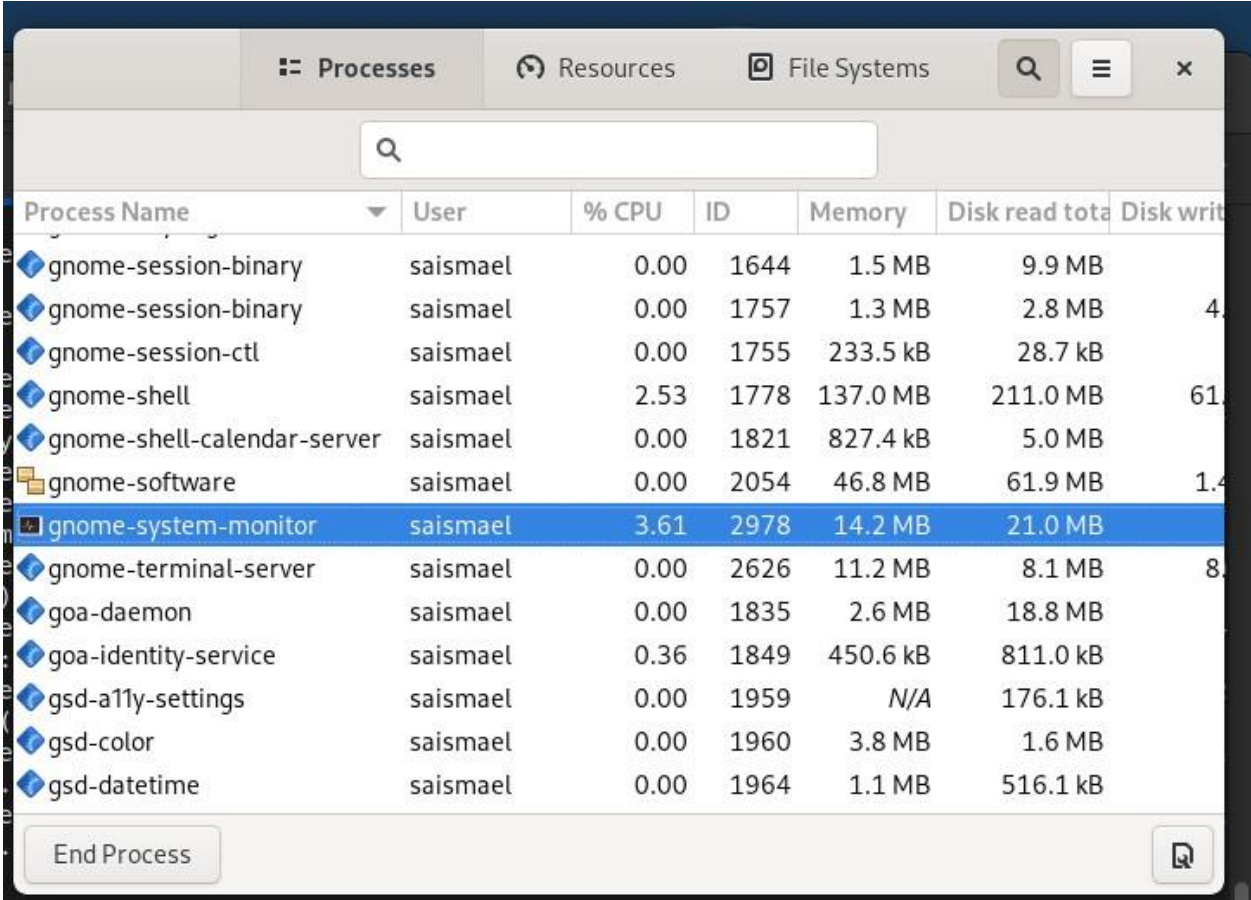
1. На сервере просмотрел один из файлов журнала

```

[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, reloadi
ng... [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

```

2. На сервере под пользователем saismael запустил графическую программу для просмотра журналов:



Process Name	User	% CPU	ID	Memory	Disk read total	Disk write
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	

3. На сервере установил просмотрщик журналов системных сообщений lnav:

```

[root@server.saismael.net rsyslog.d]#
[root@server.saismael.net rsyslog.d]# dnf -y install lnav
Last metadata expiration check: 0:03:57 ago on Sat 31 Dec 2022 08:48:58 AM UTC.
No match for argument: lnav
Error: Unable to find a match: lnav
[root@server.saismael.net rsyslog.d]# lnav
bash: lnav: command not found...
[root@server.saismael.net rsyslog.d]# cd
[root@server.saismael.net ~]# dnf -y install lnav
Last metadata expiration check: 0:04:44 ago on Sat 31 Dec 2022 08:48:58 AM UTC.
No match for argument: lnav
Error: Unable to find a match: lnav
[root@server.saismael.net ~]# lnav
bash: lnav: command not found...
[root@server.saismael.net ~]# dnf install lnav
Last metadata expiration check: 0:05:22 ago on Sat 31 Dec 2022 08:48:58 AM UTC.
No match for argument: lnav
Error: Unable to find a match: lnav

```

4. Просмотрел логи с помощью lnav:

15.4.4. Внесение изменений в настройки внутреннего окружения

виртуальных машин

1. На виртуальной машине server перейдите в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создайте в нём каталог netlog, в который поместите в соответствующие подкаталоги конфигурационные файлы:

2. В каталоге /vagrant/provision/server создайте исполняемый файл netlog.sh:

```

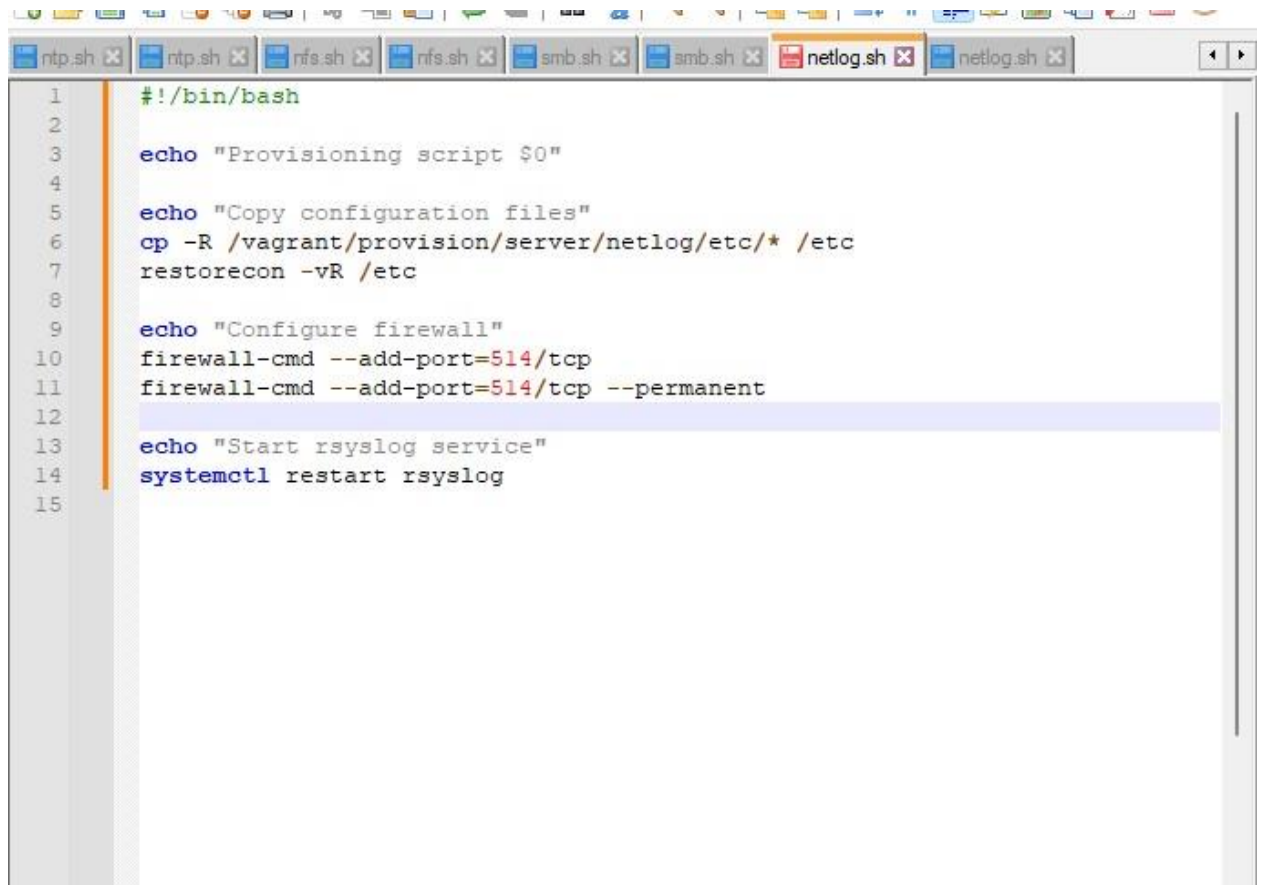
bash: lnav: command not found...
[root@server.saismael.net ~]# cd /vagrant/provision/server
[root@server.saismael.net server]# mkdir -p /vagrant/provision/server/netlog/etc
/rsyslog.d

```

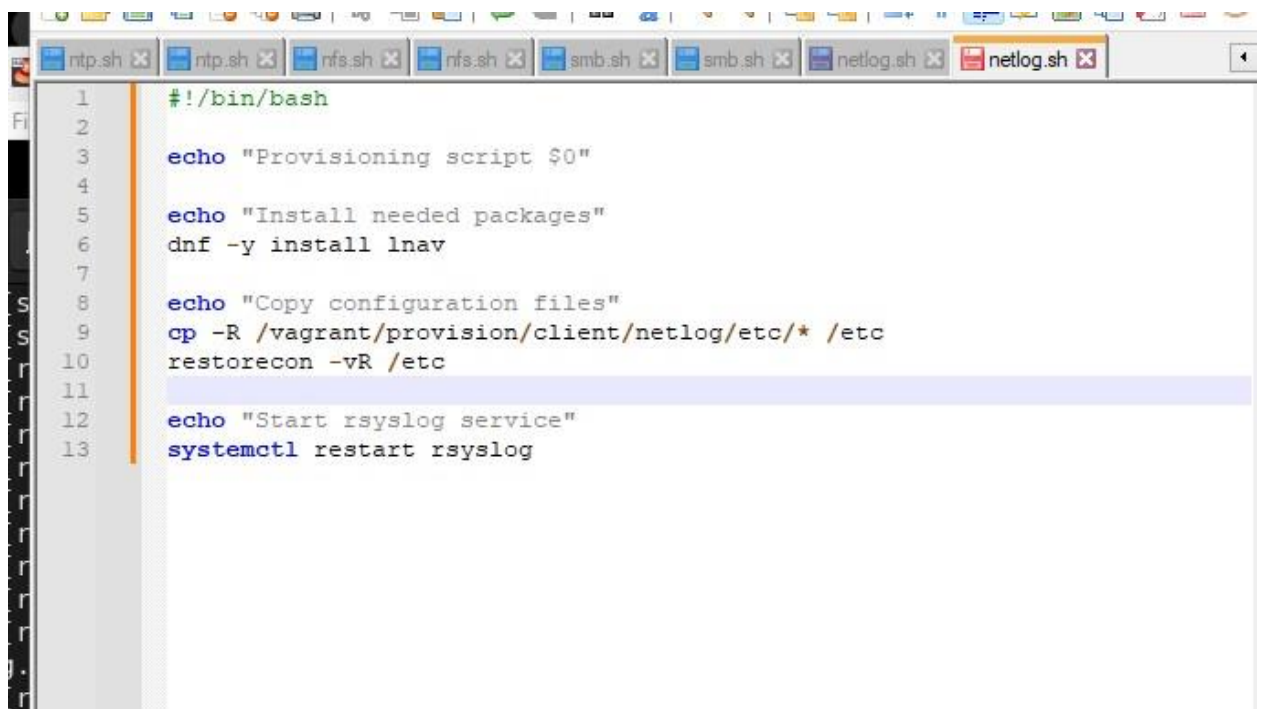
```

[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]#

```

```
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
```



```
1  #!/bin/bash
2
3  echo "Provisioning script $0"
4
5  echo "Install needed packages"
6  dnf -y install lnav
7
8  echo "Copy configuration files"
9  cp -R /vagrant/provision/client/netlog/etc/* /etc
10 restorecon -vR /etc
11
12 echo "Start rsyslog service"
13 systemctl restart rsyslog
```

```
Vagrantfile x 01-routing.sh x dhcp.sh x mysql.sh x firewall.sh x mail.sh x mail.sh x ntp.sh x
75     server.vm.provision "server nfs",
76         type: "shell",
77         preserve_order: true,
78         path: "provision/server/nfs.sh"
79
80     server.vm.provision "SMB server",
81         type: "shell",
82         preserve_order: true,
83         path: "provision/server/smb.sh"
84
85
86     server.vm.provision "server netlog",
87         type: "shell",
88         preserve_order: true,
89         path: "provision/server/netlog.sh"
90
```

```
"C:\Users\ismae\OneDrive\Attachments\Desktop\AC\packer\vagrant\Vagrantfile - Notepad++
le Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ? +
Vagrantfile x 01-routing.sh x dhcp.sh x mysql.sh x firewall.sh x mail.sh x mail.sh x ntp.sh x
35         type: "shell",
36         preserve_order: true,
37         path: "provision/client/mail.sh"
38
39     client.vm.provision "client ntp",
40         type: "shell",
41         preserve_order: true,
42         path: "provision/client/ntp.sh"
43
44     client.vm.provision "client nfs",
45         type: "shell",
46         preserve_order: true,
47         path: "provision/client/nfs.sh"
48
49     client.vm.provision "SMB client",
50         type: "shell",
51         preserve_order: true,
52         path: "provision/client/smb.sh"
53
54     client.vm.provision "client netlog",
55         type: "shell",
56         preserve_order: true,
57         path: "provision/client/netlog.sh"
58
59     client.vm.provider :virtualbox do |v|
60         v.linked_clone = true
61         v.customize ["modifyvm", :id, "--natdnshostresolver1", "on"]
62         # Customize the amount of memory on the VM
63         v.memory = 1024
64         v.cpus = 1
65         v.name = "client"
66         # Display the VirtualBox GUI when booting the machine
```

Вывод

Получил навыки по работе с журналами системных событий.