

Отчет по лабораторной работе № 15. Настройка сетевого журналирования

Сущенко Алина
НПИбд-01-23

2025

Содержание

1	Цель работы	3
2	Выполнение работы	4
2.1	Настройка сервера сетевого журнала	4
2.2	Настройка клиента сетевого журнала	5
2.3	Просмотр журнала	6
2.4	Внесение изменений в настройки внутреннего окружения виртуальных машин	8
3	Выводы	9

1 Цель работы

Получение навыков по работе с журналами системных событий.

2 Выполнение работы

2.1 Настройка сервера сетевого журнала

1. На сервере создали файл конфигурации сетевого хранения журналов (Рис. 1):

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

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

Рис. 1: Создание файла конфигурации для сетевого хранения журналов на сервере.

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

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

```
$ModLoad imtcp  
$InputTCPServerRun 514|  
#  
#
```

Рис. 2: Включение приема записей журнала по TCP-порту 514.

3. Перезапустили службу rsyslog и посмотрели, какие порты, связанные с rsyslog, прослушиваются (Рис. 3):

```
systemctl restart rsyslog  
lsof | grep TCP
```

TCP	server.ansusenko.net:ssh->_gateway:57289	(ESTABLISHED)				
rsyslogd	8721	root	4u	IPv4	41953	0t0
	TCP *:shell (LISTEN)					
rsyslogd	8721	root	5u	IPv6	41954	0t0
	TCP *:shell (LISTEN)					
rsyslogd	8721 8723 in:imjour	root	4u	IPv4	41953	0t0
	TCP *:shell (LISTEN)					
rsyslogd	8721 8723 in:imjour	root	5u	IPv6	41954	0t0
	TCP *:shell (LISTEN)					
rsyslogd	8721 8724 in:imtcp	root	4u	IPv4	41953	0t0
	TCP *:shell (LISTEN)					
rsyslogd	8721 8724 in:imtcp	root	5u	IPv6	41954	0t0
	TCP *:shell (LISTEN)					
rsyslogd	8721 8725 in:imtcp	root	4u	IPv4	41953	0t0
	TCP *:shell (LISTEN)					
rsyslogd	8721 8725 in:imtcp	root	5u	IPv6	41954	0t0
	TCP *:shell (LISTEN)					
rsyslogd	8721 8726 in:imtcp	root	4u	IPv4	41953	0t0
	TCP *:shell (LISTEN)					
rsyslogd	8721 8726 in:imtcp	root	5u	IPv6	41954	0t0
	TCP *:shell (LISTEN)					
rsyslogd	8721 8727 in:imtcp	root	4u	IPv4	41953	0t0
	TCP *:shell (LISTEN)					
rsyslogd	8721 8727 in:imtcp	root	5u	IPv6	41954	0t0
	TCP *:shell (LISTEN)					
rsyslogd	8721 8728 in:imtcp	root	4u	IPv4	41953	0t0

Рис. 3: Проверка прослушиваемых rsyslog портов.

- На сервере настроили межсетевой экран для приёма сообщений по TCP-порту 514 (Рис. 4):

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

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

Рис. 4: Настройка межсетевого экрана для приема сообщений по TCP-порту 514.

2.2 Настройка клиента сетевого журнала

- На клиенте создали файл конфигурации сетевого хранения журналов (Рис. 5):

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

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

Рис. 5: Создание файла конфигурации сетевого хранения журналов на клиенте.

2. На клиенте в файле конфигурации `/etc/rsyslog.d/netlog-client.conf` включили перенаправление сообщений журнала на 514 TCP-порт сервера (Рис. 6):

```
*.* @@server.ansusenko.net:514
```

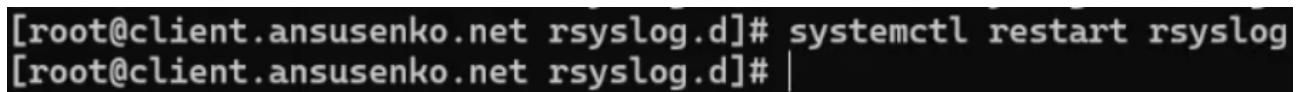


```
*.* @@server.ansusenko.net:514
```

Рис. 6: Включение перенаправления сообщений журнала на сервер через TCP-порт 514.

3. Перезапустили службу `rsyslog` (Рис. 7):

```
systemctl restart rsyslog
```



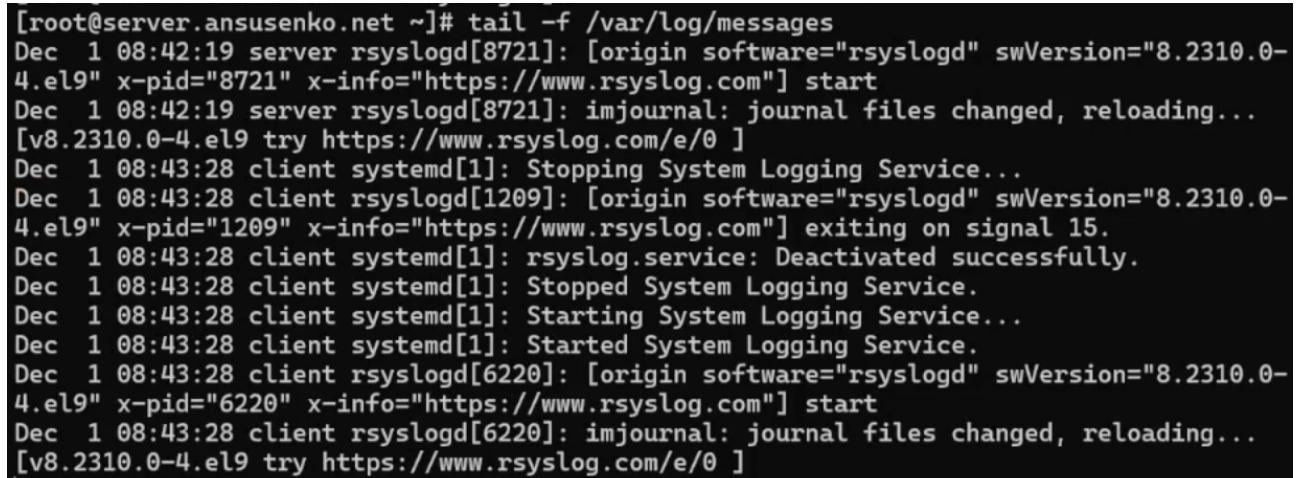
```
[root@client.ansusenko.net rsyslog.d]# systemctl restart rsyslog
[root@client.ansusenko.net rsyslog.d]# |
```

Рис. 7: Перезапуск службы `rsyslog`.

2.3 Просмотр журнала

1. На сервере просмотрели один из файлов журнала (Рис. 8)

```
tail -f /var/log/messages
```



```
[root@server.ansusenko.net ~]# tail -f /var/log/messages
Dec 1 08:42:19 server rsyslogd[8721]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="8721" x-info="https://www.rsyslog.com"] start
Dec 1 08:42:19 server rsyslogd[8721]: imjournal: journal files changed, reloading...
[v8.2310.0-4.el9 try https://www.rsyslog.com/e/0 ]
Dec 1 08:43:28 client systemd[1]: Stopping System Logging Service...
Dec 1 08:43:28 client rsyslogd[1209]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="1209" x-info="https://www.rsyslog.com"] exiting on signal 15.
Dec 1 08:43:28 client systemd[1]: rsyslog.service: Deactivated successfully.
Dec 1 08:43:28 client systemd[1]: Stopped System Logging Service.
Dec 1 08:43:28 client systemd[1]: Starting System Logging Service...
Dec 1 08:43:28 client systemd[1]: Started System Logging Service.
Dec 1 08:43:28 client rsyslogd[6220]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="6220" x-info="https://www.rsyslog.com"] start
Dec 1 08:43:28 client rsyslogd[6220]: imjournal: journal files changed, reloading...
[v8.2310.0-4.el9 try https://www.rsyslog.com/e/0 ]
```

Рис. 8: Просмотр файла журнала на сервере.

Обратите внимание на имя хоста и другие сообщения о работе сервисов. При наличии сообщений о некорректной работе сервисов исправьте ошибки в настройках соответствующих служб.

2. На сервере установили просмотрщик журналов системных сообщений `lnav` или его аналог (Рис. 9):

```
dnf -y install lnav
```

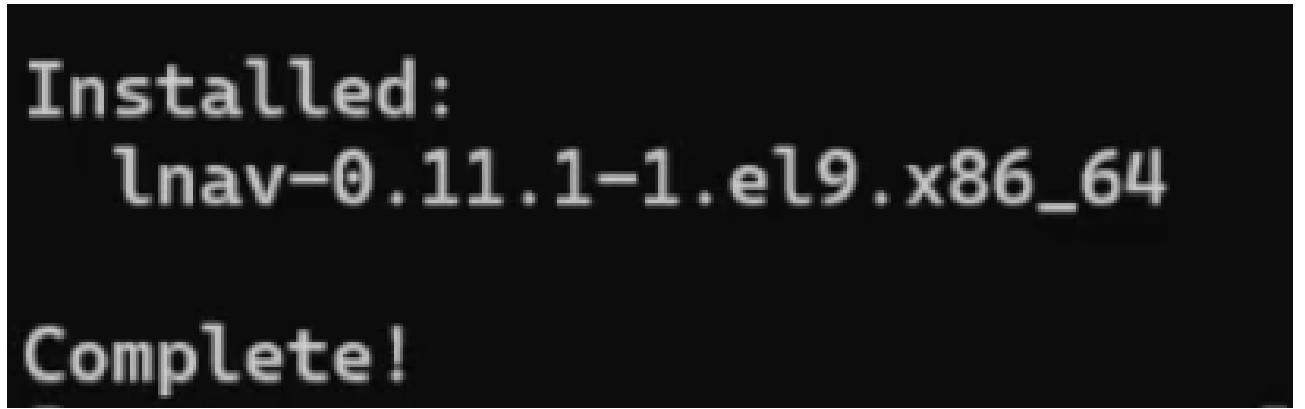


Рис. 9: Установка просмотрица журналов системных сообщений на сервер.

3. Просмотрели логи с помощью lnav (Рис. 10 , 11):

```
lnav
```

```
Dec 1 08:49:18 server named[907]: timed out resolving 'fedora-mirror02.rbc.ru/AAAA/IN': 10.128.0.240#53
Dec 1 08:49:19 server named[907]: REFUSED unexpected RCODE resolving 'mrr01.extra.rbc.ru/A/IN': 80.250.174.240#53
Dec 1 08:49:19 server named[907]: REFUSED unexpected RCODE resolving 'mrr01.extra.rbc.ru/AAAA/IN': 80.250.174.240#53
Dec 1 08:49:20 server named[907]: timed out resolving 'mrr01.extra.rbc.ru/A/IN': 10.128.0.240#53
Dec 1 08:49:20 server named[907]: timed out resolving 'mrr01.extra.rbc.ru/AAAA/IN': 10.128.0.240#53
Dec 1 08:49:20 server named[907]: REFUSED unexpected RCODE resolving 'codecs.fedoraproject.org/A/IN': 80.250.174.240#53
Dec 1 08:49:21 server named[907]: REFUSED unexpected RCODE resolving 'codecs.fedoraproject.org/AAAA/IN': 80.250.174.240#53
Dec 1 08:49:32 server named[907]: timed out resolving 'codecs.fedoraproject.org/A/IN': 10.128.0.240#53
Dec 1 08:49:32 server named[907]: timed out resolving 'codecs.fedoraproject.org/AAAA/IN': 10.128.0.240#53
Dec 1 08:49:33 server named[907]: REFUSED unexpected RCODE resolving 'liv.ns.cloudflare.com/A/IN': 80.250.174.240#53
Dec 1 08:49:33 server named[907]: REFUSED unexpected RCODE resolving 'liv.ns.cloudflare.com/AAAA/IN': 80.250.174.240#53
Dec 1 08:49:33 server named[907]: REFUSED unexpected RCODE resolving 'morgan.ns.cloudflare.com/A/IN': 80.250.174.240#53
Dec 1 08:49:33 server named[907]: REFUSED unexpected RCODE resolving 'morgan.ns.cloudflare.com/AAAA/IN': 80.250.174.240#53
Dec 1 08:49:33 server named[907]: REFUSED unexpected RCODE resolving 'mirrors.rockylinux.org/A/IN': 80.250.174.240#53
Dec 1 08:49:33 server named[907]: REFUSED unexpected RCODE resolving 'mirrors.rockylinux.org/AAAA/IN': 80.250.174.240#53
Dec 1 08:49:33 server named[907]: REFUSED unexpected RCODE resolving 'liv.ns.cloudflare.com/A/IN': 10.128.0.240#53
Dec 1 08:49:34 server named[907]: timed out resolving 'liv.ns.cloudflare.com/AAAA/IN': 10.128.0.240#53
Dec 1 08:49:34 server named[907]: timed out resolving 'morgan.ns.cloudflare.com/A/IN': 10.128.0.240#53
Dec 1 08:49:34 server named[907]: timed out resolving 'morgan.ns.cloudflare.com/AAAA/IN': 10.128.0.240#53
Dec 1 08:49:34 server named[907]: timed out resolving 'mirrors.rockylinux.org/A/IN': 10.128.0.240#53
Dec 1 08:49:34 server named[907]: REFUSED unexpected RCODE resolving 'dualstack.dl.map.rockylinux.org/AAAA/IN': 80.250.174.240#53
Dec 1 08:49:39 server named[907]: REFUSED unexpected RCODE resolving 'dualstack.dl.map.rockylinux.org/A/IN': 80.250.174.240#53
Dec 1 08:49:40 server named[907]: timed out resolving 'dualstack.dl.map.rockylinux.org/AAAA/IN': 10.128.0.240#53
Dec 1 08:49:40 server named[907]: timed out resolving 'dualstack.dl.map.rockylinux.org/A/IN': 10.128.0.240#53
Dec 1 08:49:41 server named[907]: REFUSED unexpected RCODE resolving 'rockylinux.map.fastly.net/AAAA/IN': 80.250.174.240#53
Dec 1 08:49:41 server named[907]: REFUSED unexpected RCODE resolving 'rockylinux.map.fastly.net/A/IN': 80.250.174.240#53
Dec 1 08:49:42 server named[907]: timed out resolving 'rockylinux.map.fastly.net/AAAA/IN': 10.128.0.240#53
Dec 1 08:49:42 server named[907]: timed out resolving 'rockylinux.map.fastly.net/A/IN': 10.128.0.240#53
Dec 1 08:49:43 server named[907]: REFUSED unexpected RCODE resolving '_.map.fastly.net/A/IN': 80.250.174.240#53
Dec 1 08:49:44 server named[907]: timed out resolving '_.map.fastly.net/A/IN': 10.128.0.240#53
Dec 1 08:49:44 server named[907]: REFUSED unexpected RCODE resolving 'ns1.fastly.net/AAAA/IN': 80.250.174.240#53
Dec 1 08:49:44 server named[907]: REFUSED unexpected RCODE resolving 'ns2.fastly.net/AAAA/IN': 80.250.174.240#53
Dec 1 08:49:44 server named[907]: REFUSED unexpected RCODE resolving 'ns4.fastly.net/AAAA/IN': 80.250.174.240#53
Dec 1 08:49:44 server named[907]: REFUSED unexpected RCODE resolving 'ns3.fastly.net/AAAA/IN': 80.250.174.240#53
Dec 1 08:49:45 server named[907]: timed out resolving 'ns1.fastly.net/AAAA/IN': 10.128.0.240#53
Dec 1 08:49:45 server named[907]: timed out resolving 'ns2.fastly.net/AAAA/IN': 10.128.0.240#53
Dec 1 08:49:45 server named[907]: timed out resolving 'ns4.fastly.net/AAAA/IN': 10.128.0.240#53
Dec 1 08:49:45 server named[907]: timed out resolving 'ns3.fastly.net/AAAA/IN': 10.128.0.240#53
Dec 1 08:50:06 server systemd[1]: Started /usr/bin/systemctl start man-db-cache-update.
Dec 1 08:50:06 server systemd[1]: Starting man-db-cache-update.service...
Dec 1 08:50:08 server systemd[1]: man-db-cache-update.service: Deactivated successfully.
Dec 1 08:50:08 server systemd[1]: Finished man-db-cache-update.service.
Dec 1 08:50:08 server systemd[1]: run-r29fe3f5e4abd4c9eaaf0a86a55c5004c.service: Deactivated successfully.
```

Рис. 10: Просмотр общих логов на сервере.

```

18:39:01 client dnf[2973]: Rocky Linux 9 - BaseOS          3.7 kB/s | 4.1 kB   00:01
18:39:02 client dnf[2973]: Rocky Linux 9 - AppStream      6.7 kB/s | 4.5 kB   00:00
18:39:03 client dnf[2973]: Rocky Linux 9 - AppStream      288 B/s | 199 B    00:00
18:39:03 client dnf[2973]: Errors during downloading metadata for repository 'appstream':
18:39:03 client dnf[2973]: - Status code: 403 for http://mir01.syntis.net/rockylinux/9.5/AppStream/x86_64/repo/repodata/repomd.xml (IP: 5.83.232.126)
18:39:04 client dnf[2973]: Error: Failed to download metadata for repo 'appstream': Cannot download repomd.xml
Status code: 403 for http://mir01.syntis.net/rockylinux/9.5/AppStream/x86_64/os/repo/repodata/repomd.xml (IP: 2.126)
18:39:04 client systemd[1]: dnf-makecache.service: Main process exited, code=exited, status=1/FAILURE
18:39:04 client systemd[1]: dnf-makecache.service: Failed with result 'exit-code'.
18:39:04 client systemd[1]: Failed to start dnf makecache.
18:39:04 client systemd[1]: dnf-makecache.service: Consumed 17.306s CPU time.

```

Рис. 11: Логи на клиенте.

Можно заметить, что все логи, имеющиеся на клиенте, также присутствуют и на сервере соответствующей отметкой о принадлежности.

2.4 Внесение изменений в настройки внутреннего окружения виртуальных машин

- На виртуальной машине `server` перешли в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создали в нём каталог `netlog`, в который поместили в соответствующие подкаталоги конфигурационные файлы:

```

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

```

- В каталоге `/vagrant/provision/server` создали исполняемый файл:

```

cd /vagrant/provision/server
touch netlog.sh
chmod +x netlog.sh

```

Открыли его на редактирование, прописали в нём следующий скрипт:

```

#!/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

```

- На виртуальной машине `client` перешли в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/client/`, создали в нём каталог `netlog`, в который поместили в соответствующие подкаталоги конфигурационные файлы:

```
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/
```

4. В каталоге `/vagrant/provision/client` создали исполняемый файл `netlog.sh`:

```
cd /vagrant/provision/client  
touch netlog.sh  
chmod +x netlog.sh
```

Открыв его на редактирование, прописали в нём следующий скрипт:

```
#!/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  
systemctl restart rsyslog
```

5. Для отработки созданных скриптов во время загрузки виртуальных машин `server` и `client` в конфигурационном файле `Vagrantfile` добавили в соответствующих разделах конфигураций для сервера и клиента:

```
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"
```

3 Выводы

В результате выполнений лабораторной работы получили навыки настройки сетевого хранения журналов системных событий.