

Лабораторная работа № 15.

Настройка сетевого журналирования

Сущенко Алина
НПИбд-01-23

Российский университет дружбы народов имени Патриса Лумумбы

2025

Цель работы

- ▶ Получение навыков по работе с журналами системных событий.

Настройка сервера сетевого журнала

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

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

Настройка сервера сетевого журнала

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

~

~

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

Настройка сервера сетевого журнала

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.: Проверка прослушиваемых rsyslog портов.

Настройка сервера сетевого журнала

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

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

Настройка клиента сетевого журнала

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

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

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

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

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

Рис.: Перезапуск службы rsyslog.

Просмотр журнала

```
[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.: Просмотр файла журнала на сервере.

Просмотр журнала

```
Installed:  
lnav-0.11.1-1.el9.x86_64  
  
Complete!
```

Рис.: Установка просмотрщика журналов системных сообщений на сервер.

Просмотр журнала

```
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/AAA/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/AAA/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/AAA/IN': 80.250.174.240#53
Dec 1 08:49:21 server named[907]: REFUSED unexpected RCODE resolving 'codecs.fedoraproject.org/A/IN': 10.128.0.240#53
Dec 1 08:49:22 server named[907]: REFUSED unexpected RCODE resolving 'codecs.fedoraproject.org/AAA/IN': 80.250.174.240#53
Dec 1 08:49:22 server named[907]: REFUSED unexpected RCODE resolving 'codecs.fedoraproject.org/A/IN': 10.128.0.240#53
Dec 1 08:49:23 server named[907]: REFUSED unexpected RCODE resolving 'liv.ns.cloudflare.com/A/IN': 80.250.174.240#53
Dec 1 08:49:23 server named[907]: REFUSED unexpected RCODE resolving 'liv.ns.cloudflare.com/AAA/IN': 80.250.174.240#53
Dec 1 08:49:23 server named[907]: REFUSED unexpected RCODE resolving 'morgan.ns.cloudflare.com/A/IN': 80.250.174.240#53
Dec 1 08:49:23 server named[907]: REFUSED unexpected RCODE resolving 'morgan.ns.cloudflare.com/AAA/IN': 80.250.174.240#53
Dec 1 08:49:23 server named[907]: REFUSED unexpected RCODE resolving 'mirrors.rockylinux.org/A/IN': 80.250.174.240#53
Dec 1 08:49:23 server named[907]: REFUSED unexpected RCODE resolving 'mirrors.rockylinux.org/AAA/IN': 80.250.174.240#53
Dec 1 08:49:24 server named[907]: timed out resolving 'liv.ns.cloudflare.com/A/IN': 10.128.0.240#53
Dec 1 08:49:24 server named[907]: timed out resolving 'liv.ns.cloudflare.com/AAA/IN': 10.128.0.240#53
Dec 1 08:49:24 server named[907]: timed out resolving 'morgan.ns.cloudflare.com/A/IN': 10.128.0.240#53
Dec 1 08:49:24 server named[907]: timed out resolving 'morgan.ns.cloudflare.com/AAA/IN': 10.128.0.240#53
Dec 1 08:49:24 server named[907]: timed out resolving 'mirrors.rockylinux.org/A/IN': 10.128.0.240#53
Dec 1 08:49:24 server named[907]: timed out resolving 'mirrors.rockylinux.org/AAA/IN': 10.128.0.240#53
Dec 1 08:49:29 server named[907]: REFUSED unexpected RCODE resolving 'dualstack.dl.map.rockylinux.org/AAA/IN': 80.250.174.240#53
Dec 1 08:49:29 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/AAA/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/AAA/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/AAA/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 08:49:43 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/AAA/IN': 80.250.174.240#53
Dec 1 08:49:44 server named[907]: REFUSED unexpected RCODE resolving 'ns2.fastly.net/AAA/IN': 80.250.174.240#53
Dec 1 08:49:44 server named[907]: REFUSED unexpected RCODE resolving 'ns4.fastly.net/AAA/IN': 80.250.174.240#53
Dec 1 08:49:44 server named[907]: REFUSED unexpected RCODE resolving 'ns3.fastly.net/AAA/IN': 80.250.174.240#53
Dec 1 08:49:45 server named[907]: timed out resolving 'ns1.fastly.net/AAA/IN': 10.128.0.240#53
Dec 1 08:49:45 server named[907]: timed out resolving 'ns2.fastly.net/AAA/IN': 10.128.0.240#53
Dec 1 08:49:45 server named[907]: timed out resolving 'ns4.fastly.net/AAA/IN': 10.128.0.240#53
Dec 1 08:49:45 server named[907]: timed out resolving 'ns3.fastly.net/AAA/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.: Просмотр общих логов на сервере.

Просмотр журнала

```
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_6
podata/repo-md.xml (IP: 5.83.232.126)
18:39:04 client dnf[2973]: Error: Failed to download metadata for repo 'appstream': Cannot download repom
Status code: 403 for http://mir01.syntis.net/rockylinux/9.5/AppStream/x86_64/os/repo-md.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.: Логи на клиенте.

Контрольный вопрос 1

Вопрос: Какой модуль rsyslog вы должны использовать для приёма сообщений от journald?

Ответ: Для приёма сообщений от journald в rsyslog следует использовать модуль `imjournal`.

Контрольный вопрос 2

Вопрос: Как называется устаревший модуль, который можно использовать для включения приёма сообщений журнала в rsyslog?

Ответ: Устаревший модуль, который можно использовать для этой цели, называется `imuxsock`.

Контрольный вопрос 3

Вопрос: Чтобы убедиться, что устаревший метод приёма сообщений из `journald` в `rsyslog` не используется, какой дополнительный параметр следует использовать?

Ответ: Чтобы отключить устаревший метод, в конфигурации модуля `imjournal` следует использовать параметр `omit_synchronization`.

Контрольный вопрос 4

Вопрос: В каком конфигурационном файле содержатся настройки, которые позволяют вам настраивать работу журнала?

Ответ: Основные настройки работы системного журнала содержатся в файле `/etc/systemd/journald.conf`.

Контрольный вопрос 5

Вопрос: Каким параметром управляется пересылка сообщений из journald в rsyslog?

Ответ: Пересылка сообщений из journald в rsyslog управляется параметром `ForwardToSyslog` в файле `/etc/systemd/journald.conf`.

Контрольный вопрос 6

Вопрос: Какой модуль rsyslog вы можете использовать для включения сообщений из файла журнала, не созданного rsyslog?

Ответ: Для чтения сообщений из произвольного файла журнала используется модуль `imfile`.

Контрольный вопрос 7

Вопрос: Какой модуль rsyslog вам нужно использовать для пересылки сообщений в базу данных MariaDB?

Ответ: Для пересылки сообщений в базу данных MariaDB используется модуль вывода ommysql.

Контрольный вопрос 8

Вопрос: Какие две строки вам нужно включить в rsyslog.conf, чтобы позволить текущему журнальному серверу получать сообщения через TCP?

Ответ: Для приёма сообщений через TCP необходимо добавить в rsyslog.conf следующие строки:

```
module(load="imtcp")
input(type="imtcp"port="514")
```

Контрольный вопрос 9

Вопрос: Как настроить локальный брандмауэр, чтобы разрешить приём сообщений журнала через порт TCP 514?

Ответ: Для настройки firewalld можно использовать команды:

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

Выводы

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