Упражнение 1: Настройка сервера Rsyslog на RedOS 7.

Задача 1: Настройка сервера Rsyslog.

1. Установите Rsyslog (**`rsyslog`**) на машине **srv**.

> *ПРИМЕЧАНИЕ:*
> *Rsyslog (**`rsyslog`**) уже установлен в RedOS 7 и поэтому может быть только обновлен.*

2. При помощи конфигурационного файла **`/etc/rsyslog.conf`** настройте прием сообщений syslog по протоколам TCP и UDP.
3. Перезапустите службу rsyslog.
4. Убедитесь, что служба запущена и настроена на автоматический запуск.
5. Разрешите входящий траффик на порту 514 для UDP и TCP в FirewallD.

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

6. Запустите интерактивный вывод сообщений из файла журнала **`/var/log/messages`** при помощи команды **`tail`**.

Задача 2: Настройка клиента Rsyslog.

1. Установите Rsyslog (**`rsyslog`**) на машине **cli**.

> *ПРИМЕЧАНИЕ:*
> *Rsyslog (**`rsyslog`**) уже установлен в RedOS 7 и поэтому может быть только обновлен.*

2. При помощи конфигурационного файла **`/etc/rsyslog.conf`** настройте правило отправки всех сообщений syslog на сервер **srv**.
3. Перезапустите службу rsyslog.
4. Убудеитесь, что служба запущена и настроена на автоматический запуск.
5. Убедитесь, что сообщения syslog начали поступать в файл **`/var/log/messages`** на систему **srv**.

> *ПРИМЕЧАНИЕ:*
> *Для отправки тестового сообщения в журнал можно воспользоваться командой **`logger`**:*
> ***`# logger -t test "Test Log Message"`***

Задача 3: Настройка фильтрации журналов Rsyslog.

1. При помощи конфигурационного файла **`/etc/rsyslog.conf`** настройте правило записи всех сообщений syslog от хоста **srv** в файл **`/var/log/srv`**, а сообщений syslog от хоста cli в файл **`/var/log/cli`**.
2. Перезапустите службу **`rsyslog`**.
3. Убедитесь, что служба **`rsyslog`** запущена.
4. Убедитесь, что файлы журнала **`/var/log/srv`** и **`/var/log/cli`** создались и содержат сообщения syslog.

Ответы к упражнению 1: Настройка сервера Rsyslog на RedOS 7.

Задача 1: Настройка сервера Rsyslog.

1. Установите Rsyslog (**rsyslog**) на машине **srv**.

```
# yum install rsyslog
```

ПРИМЕЧАНИЕ:
*Rsyslog (**rsyslog**) уже установлен в RedOS 7 и поэтому может быть только обновлен.*

2. При помощи конфигурационного файла **/etc/rsyslog.conf** настройте прием сообщений syslog по протоколам TCP и UDP.

```
# vi /etc/rsyslog.conf
# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514

# Provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514
```

3. Перезапустите службу **rsyslog**.

```
# systemctl restart rsyslog.service
```

4. Убедитесь, что служба **rsyslog** запущена и настроена на автоматический запуск.

```
# systemctl status rsyslog.service
# systemctl is-enabled  rsyslog.service
```

5. Разрешите входящий траффик на порту 514 для UDP и TCP в FirewallD.

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

6. Запустите интерактивный вывод сообщений из файла журнала **/var/log/messages** при помощи команды **tail**.

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

Задача 2: Настройка клиента Rsyslog.

1. Установите Rsyslog (**rsyslog**) на машине **cli**.

```
# yum install rsyslog
```

ПРИМЕЧАНИЕ:
*Rsyslog (**rsyslog**) уже установлен в RedOS 7 и поэтому может быть только обновлен.*

2. При помощи конфигурационного файла **/etc/rsyslog.conf** настройте правило отправки всех сообщений syslog на сервер **srv**.

```
# vi /etc/rsyslog.conf
#### RULES ####

*.* @srv:514
```

3. Перезапустите службу **rsyslog**.

```
# systemctl restart rsyslog.service
```

4. Убедитесь, что служба **rsyslog** запущена и настроена на автоматический запуск.

```
# systemctl status rsyslog.service
# systemctl is-enabled  rsyslog.service
```

5. Убедитесь, что сообщения syslog начали поступать в файл **/var/log/messages** на систему **srv**.

```
# tail -f /var/log/messages
…
Sep 27 05:22:05 cli test: Test Log Message
```

ПРИМЕЧАНИЕ:
*Для отправки тестового сообщения в журнал можно воспользоваться командой **logger**:*
 # logger -t test "Test Log Message"

Задача 3: Настройка фильтрации журналов Rsyslog.

1. При помощи конфигурационного файла **/etc/rsyslog.conf** настройте правило записи всех сообщений syslog от хоста **srv** в файл **/var/log/srv**, а сообщений syslog от хоста cli в файл **/var/log/cli**.

```
# vi /etc/rsyslog.conf
#### RULES ####

:hostname, isequal, "srv" /var/log/srv
:hostname, isequal, "cli" /var/log/cli
```

2. Перезапустите службу **rsyslog**.

```
# systemctl restart rsyslog.service
```

3. Убедитесь, что служба **rsyslog** запущена.

```
# systemctl status rsyslog.service
```

4. Убедитесь, что файлы журнала **/var/log/srv** и **/var/log/cli** создались и содержат сообщения syslog.

```
# ls /var/log/c7-server0?
# tail -n 1 /var/log/srv
# tail -n 1 /var/log/cli
```