Сервер

Задаём правильный часовой пояс

```
[lazzur@localhost ~]$ \cp /usr/share/zoneinfo/Europe/Kaliningrad /etc/localtime
cp: невозможно создать обычный файл '/etc/localtime': Отказано в доступе
[lazzur@localhost ~]$ sudo !!
sudo \cp /usr/share/zoneinfo/Europe/Kaliningrad /etc/localtime
[lazzur@localhost ~]$
```

Устанавливаем chrony

```
[lazzur@localhost ~]$ sudo yum install chrony
Последняя проверка окончания срока действия метаданных: 0:31:31 назад, Пн 14 фев
 2022 21:14:13.
Пакет chrony-4.1-1.el8.x86_64 уже установлен.
Зависимости разрешены.
Отсутствуют действия для выполнения
Выполнено!
```

Запускаем его

```
[lazzur@localhost ~]$ sudo systemctl enable chronyd
[lazzur@localhost ~]$ sudo systemctl start chronyd
```

Открываем порт 514 для TCP/UDP

```
[lazzur@localhost ~]$ sudo firewall-cmd --permanent --add-port=514/{tcp,udp}
Warning: ALREADY_ENABLED: 514:tcp
Warning: ALREADY_ENABLED: 514:udp
success
```

Проверяем SELinux и выключаем

```
[lazzur@localhost ~]$ getenforce
Enforcing
[lazzur@localhost ~]$ setenforce 0
setenforce:  setenforce() failed
[lazzur@localhost ~]$ sudo !!
sudo setenforce 0
[sudo] пароль для lazzur:
[lazzur@localhost ~]$ getenforce
Permissive
```

Устанавливаем rsyslog

```
[lazzur@localhost ~]$ yum install rsyslog
Ошибка: Эту команду нужно запускать с привилегиями су
стве систем - под именем пользователя root).
[lazzur@localhost ~]$ sudo !!
sudo yum install rsyslog
Последняя проверка окончания срока действия метаданны
 2022 21:14:13.
Пакет rsyslog-8.2102.0-7.el8.x86_64 уже установлен.
Зависимости разрешены.
Отсутствуют действия для выполнения
Выполнено!
[lazzur@localhost ~]$
```

Запускаем

```
Выполнено!
[lazzur@localhost ~]$ sudo systemctl enable rsyslog
[lazzur@localhost ~]$ sudo systemctl start rsyslog
```

В файле /etc/rsyslog.conf включаем TCP

```
# Provides TCP syslog reception
# for parameters see http://www.rsyslog.com/doc/imtcp.html
module(load="imtcp") # needs to be done just once
input(type="imtcp" port="514")
```

И задаем правило логгирования

```
$template RemoteLogs,"/var/log/rsyslog/%HOSTNAME%/%PROGRAMNAME%.log"
*.* ?RemoteLogs
& stop
```

Рестарт и статус

```
[lazzur@localhost ~]$ systemctl restart rsyslog
[lazzur@localhost ~]$ sudo systemctl start rsyslog
[lazzur@localhost ~]$ sudo systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor pre>
   Active: active (running) since Mon 2022-02-14 22:09:45 EET; 15s ago
     Docs: man:rsyslogd(8)
           https://www.rsyslog.com/doc/
 Main PID: 4041 (rsyslogd)
    Tasks: 8 (limit: 4772)
   Memory: 1.6M
   CGroup: /system.slice/rsyslog.service
           └─4041 /usr/sbin/rsyslogd -n

фев 14 22:09:45 localhost.localdomain systemd[1]: Stopped System Logging Servic>
фев 14 22:09:45 localhost.localdomain systemd[1]: Starting System Logging Servi>
фев 14 22:09:45 localhost.localdomain rsyslogd[4041]: [origin software="rsyslog>
фев 14 22:09:45 localhost.localdomain systemd[1]: Started System Logging Servic>
фев 14 22:09:45 localhost.localdomain rsyslogd[4041]: imjournal: journal files >
lines 1-16/16 (END)
```

Клиент

Устанавливаем rsyslog

```
[blinzy@localhost ~]$ sudo yum install rsyslog
CentOS Stream 8 - AppStream                     202 kB/s |  20 MB     01:38
CentOS Stream 8 - BaseOS                        527 kB/s |  19 MB     00:37
CentOS Stream 8 - Extras                         22 kB/s |  18 kB     00:00
Пакет rsyslog-8.2102.0-7.el8.x86_64 уже установлен.
Зависимости разрешены.
Отсутствуют действия для выполнения
Выполнено!
```

Запускаем

```
Выполнено!
[blinzy@localhost ~]$ systemctl enable rsyslog
[blinzy@localhost ~]$ sudo systemctl start rsyslog
```

Создаём файл конфигурации, куда клиенту отправлять логи

```
  GNU nano 2.9.8                  /etc/rsyslog.d/all.conf

*.* @@10.0.0.2:514
```

Перезапускаем

(blinzy@localhost сменилось на client1 дабы избежать наслоения папок логов rsyslog для каждой из машин, сервера и клиента)

```
[blinzy@client1 ~]$ sudo nano /etc/rsyslog.d/all.conf
[blinzy@client1 ~]$ sudo systemctl restart rsyslog
```

```
[blinzy@client1 ~]$ sudo systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor pre>
   Active: active (running) since Mon 2022-02-14 23:22:37 MSK; 3min 22s ago
     Docs: man:rsyslogd(8)
           https://www.rsyslog.com/doc/
 Main PID: 1232 (rsyslogd)
    Tasks: 3 (limit: 4772)
   Memory: 1.6M
   CGroup: /system.slice/rsyslog.service
           └─1232 /usr/sbin/rsyslogd -n
```

Видим на сервере логи с client1

```
[lazzur@localhost ~]$ sudo ls /var/log/rsyslog/
client1  localhost
```