Проверка rsyslog

- **/etc/rsyslog.conf** на машине L-SRV
    1. Раскомментировали данные строки

```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")
```

    2. В разделе **RULES** создали два новых правила:

```
#
# L-SRV and L-FW logs
#
auth.*                          /opt/logs/L-SRV/auth.log
if $hostname contains "L-FW" or $fromhost-ip contains "172.16.20.1"
then {
*.err                           /opt/logs/L-FW/error.log
}
```

- **/etc/rsyslog.conf** на машине L-FW
    1. В конце файла указали тип логов и адрес для отправки

```
#
# Remote logs
#
*.err                           @172.16.20.10
```

Файлы логов

```
root@L-SRV:~# ls -al /opt/logs/L-SRV/
total 16
drwxr-xr-x 2 root root 4096 Oct 21 21:37 .
drwxr-xr-x 4 root root 4096 Oct 21 20:59 ..
-rw-r----- 1 root adm  1519 Oct 22 22:35 auth.log
-rw-r----- 1 root adm   149 Oct 21 20:56 auth.log.1.gz

root@L-SRV:~# ls -al /opt/logs/L-FW/
total 16
drwxr-xr-x 2 root root 4096 Oct 21 22:16 .
drwxr-xr-x 4 root root 4096 Oct 21 20:59 ..
-rw-r----- 1 root adm    32 Oct 21 22:16 error.log
-rw-r----- 1 root adm    64 Oct 21 21:01 error.log.1.gz
```

```
root@L-SRV:~#
```

- auth.log

```
Oct 22 21:48:22 L-SRV systemd-logind[466]: New seat seat0.
Oct 22 21:48:22 L-SRV systemd-logind[466]: Watching system buttons on /dev/input/event4 (Power Button)
Oct 22 21:48:22 L-SRV systemd-logind[466]: Watching system buttons on /dev/input/event0 (AT Translated Set 2 keyboard)
Oct 22 21:49:03 L-SRV sshd[515]: Server listening on 0.0.0.0 port 22.
Oct 22 21:49:03 L-SRV sshd[515]: Server listening on :: port 22.
Oct 22 21:52:59 L-SRV systemd-logind[466]: New session 1 of user root.
Oct 22 22:35:38 L-SRV sshd[813]: Accepted password for root from 192.168.229.1 port 50669 ssh2
Oct 22 22:35:38 L-SRV systemd-logind[466]: New session 4 of user root.

```

- error.log

```
Oct 21 22:16:24 l-fw root: test
```