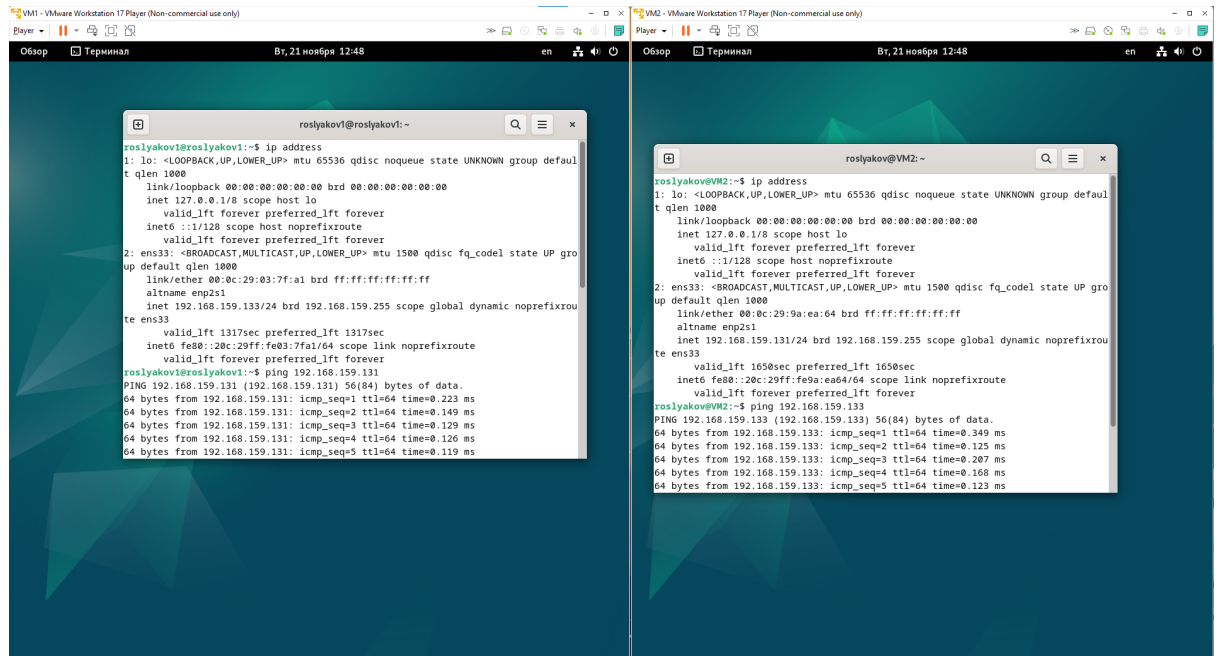
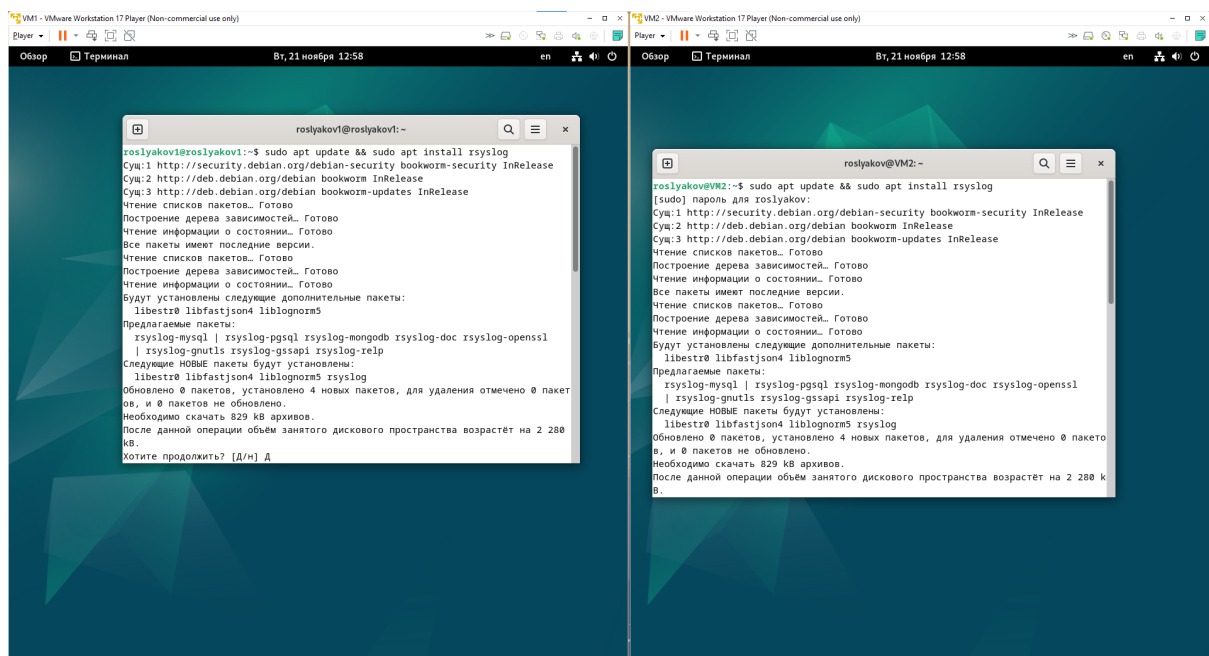


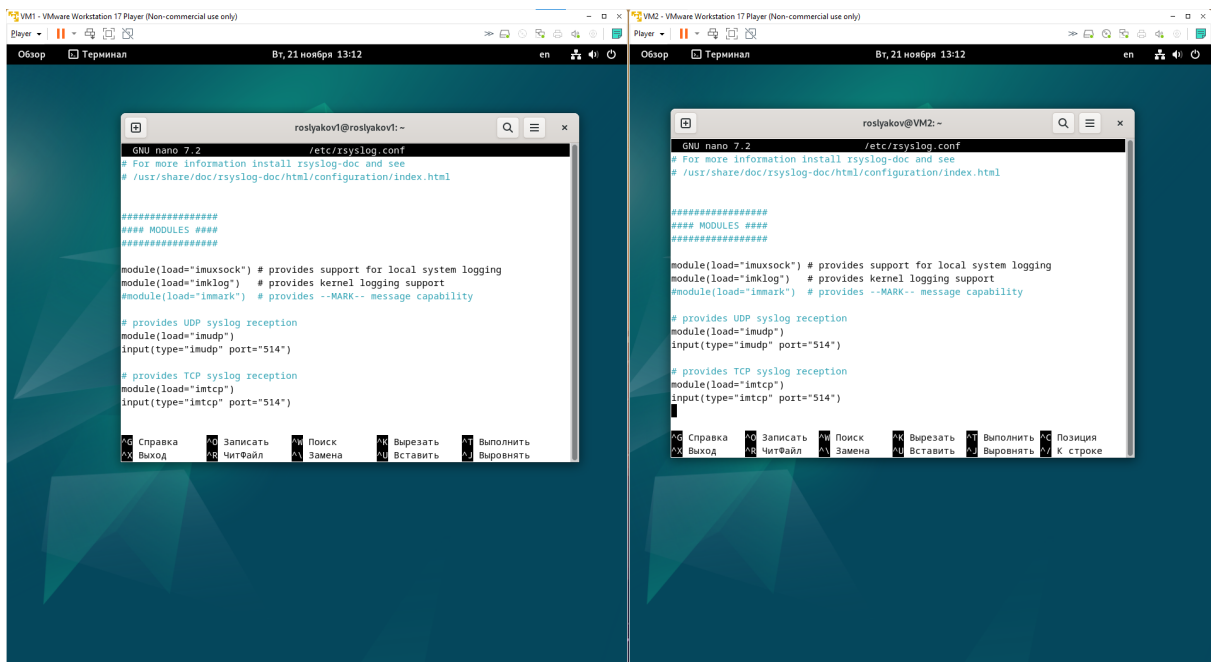
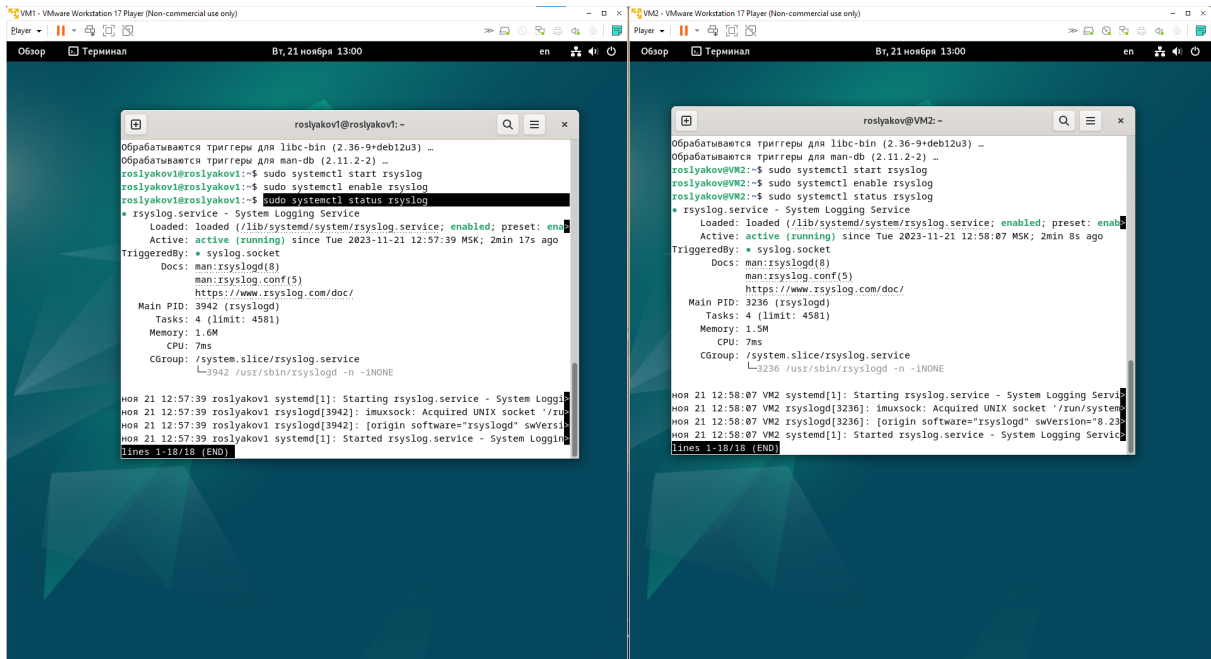
практическая работа ТОИБ

- 1) созданы 2 виртуальные машины на базе Debian 12
- 2) обеспечен сетевой обмен между ними

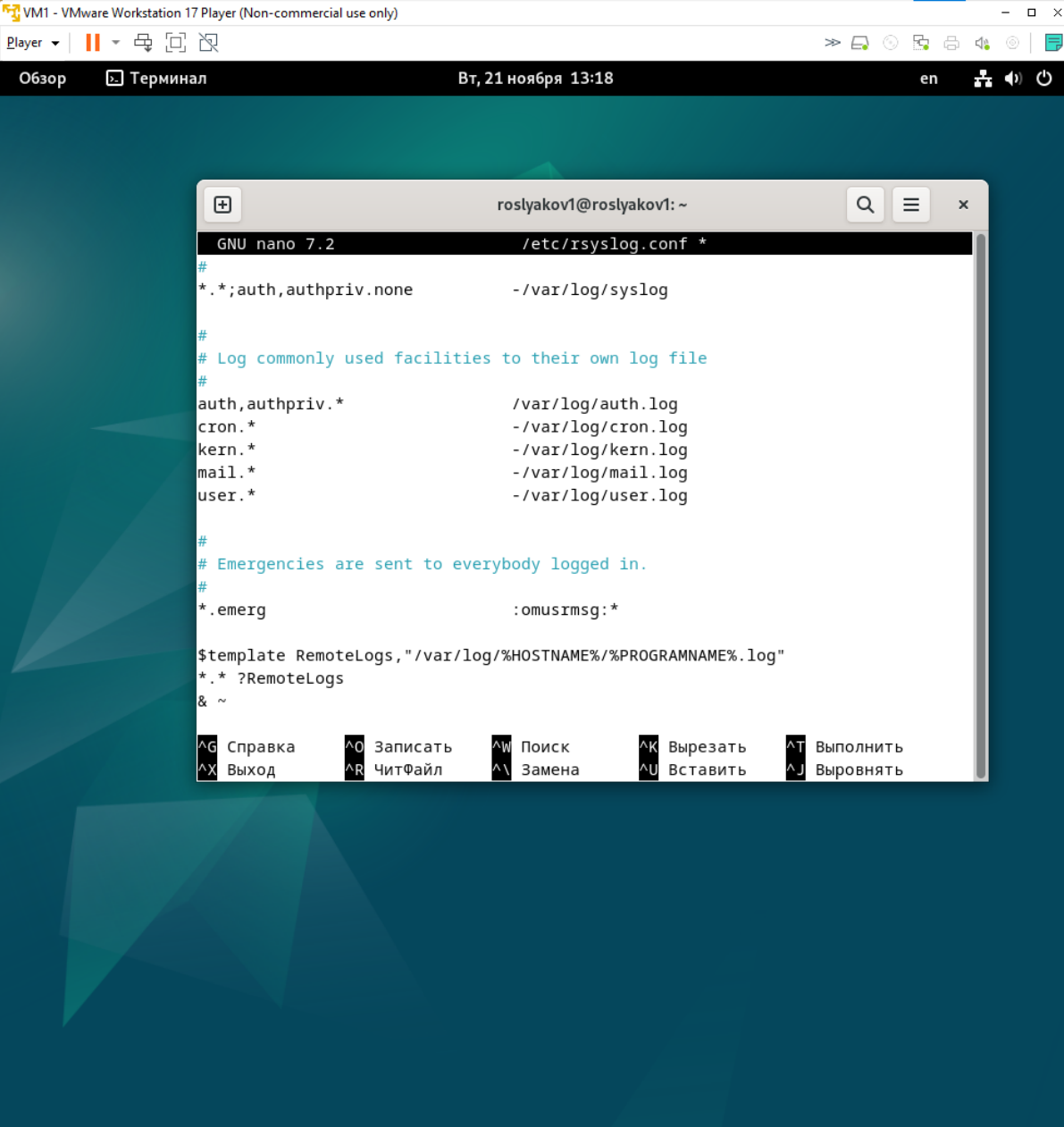


- 3) Включен на 1й из VM передачу логов по протоколу rsyslog на 2ю VM





4) Установка правил на сервер



The screenshot shows a VMware Workstation 17 Player window titled "VM1 - VMware Workstation 17 Player (Non-commercial use only)". The interface includes a top toolbar with icons for Player, a status bar showing "Вт, 21 ноября 13:18", and a language dropdown set to "en". The main display area shows a terminal window titled "roslyakov1@roslyakov1: ~" running the GNU nano 7.2 text editor. The editor is editing the file "/etc/rsyslog.conf". The content of the file is as follows:

```
GNU nano 7.2 /etc/rsyslog.conf *
#
*. *;auth,authpriv.none -/var/log/syslog
#
# Log commonly used facilities to their own log file
#
auth,authpriv.* /var/log/auth.log
cron.* -/var/log/cron.log
kern.* -/var/log/kern.log
mail.* -/var/log/mail.log
user.* -/var/log/user.log
#
# Emergencies are sent to everybody logged in.
#
*.emerg :omusrmsg:*

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

At the bottom of the nano editor window, there is a keyboard shortcuts menu:

^G Справка	^O Записать	^W Поиск	^K Вырезать	^T Выполнить
^X Выход	^R ЧитФайл	^I Замена	^U Вставить	^J Выровнять

5) установка правил на клиент



VM2 - VMware Workstation 17 Player (Non-commercial use only)

Player ▾ | [Icons] | [Icons] | [Icons] | [Icons] | [Icons] | [Icons]

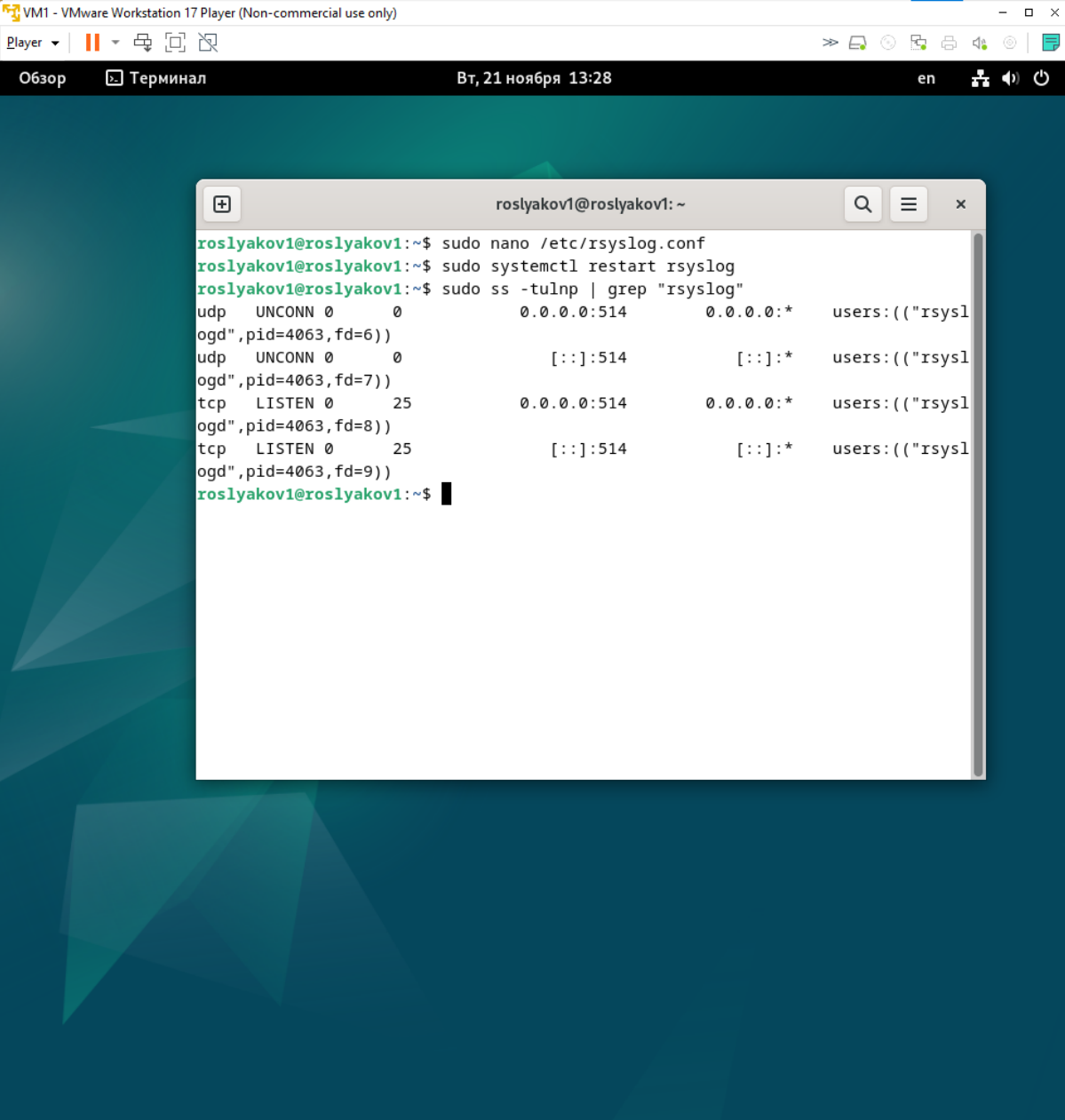
Обзор | Терминал | Вт, 21 ноября 13:26 | en | [Icons]

```
roslyakov@VM2: ~
GNU nano 7.2 /etc/rsyslog.conf *
# Log anything besides private authentication messages to a single log file
#
*. *;auth,authpriv.none -/var/log/syslog
#
# Log commonly used facilities to their own log file
#
auth,authpriv.* /var/log/auth.log
cron.* -/var/log/cron.log
kern.* -/var/log/kern.log
mail.* -/var/log/mail.log
user.* -/var/log/user.log
#
# Emergencies are sent to everybody logged in.
#
*.emerg :omusrmsg:*
*.* @@192.168.159.133:514

```

⌘ Справка ⌘ Записать ⌘ Поиск ⌘ Вырезать ⌘ Выполнить ⌘ Позиция
⌘ Выход ⌘ ЧитФайл ⌘ Замена ⌘ Вставить ⌘ Выровнять ⌘ К строке

6)Проверка

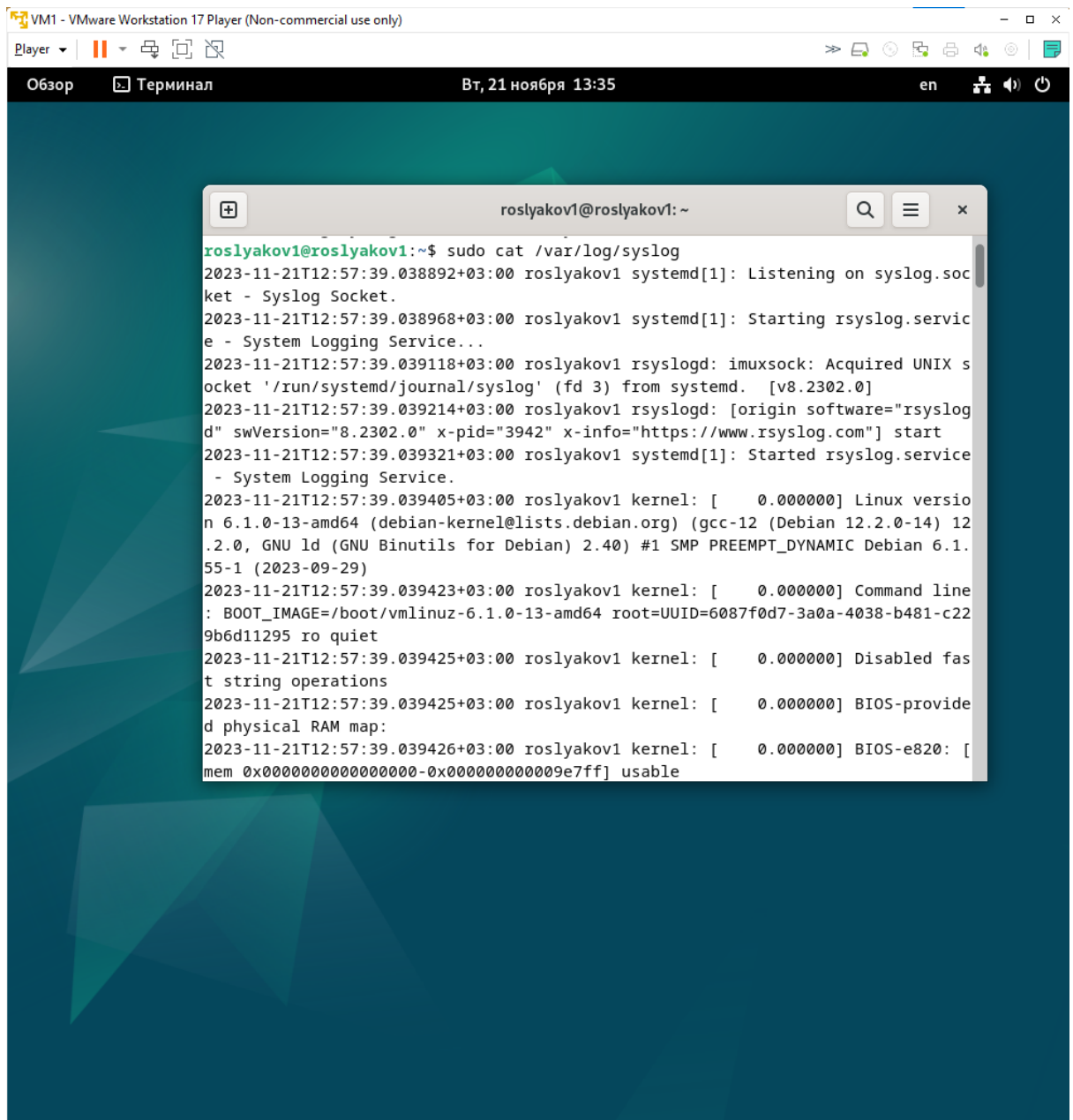


The screenshot shows a VMware Workstation 17 Player window titled "VM1 - VMware Workstation 17 Player (Non-commercial use only)". The interface includes a top toolbar with icons for Player, a status bar with "Обзор" (Overview) and "Терминал" (Terminal) tabs, and a system clock showing "Вт, 21 ноября 13:28". The language is set to "en".

The terminal window, titled "roslyakov1@roslyakov1: ~", displays the following commands and output:

```
roslyakov1@roslyakov1:~$ sudo nano /etc/rsyslog.conf
roslyakov1@roslyakov1:~$ sudo systemctl restart rsyslog
roslyakov1@roslyakov1:~$ sudo ss -tulnp | grep "rsyslog"
udp    UNCONN 0      0             0.0.0.0:514    0.0.0.0:*    users:(("rsysl
ogd",pid=4063,fd=6))
udp    UNCONN 0      0             [::]:514      [::]:*      users:(("rsysl
ogd",pid=4063,fd=7))
tcp    LISTEN 0      25           0.0.0.0:514    0.0.0.0:*    users:(("rsysl
ogd",pid=4063,fd=8))
tcp    LISTEN 0      25           [::]:514      [::]:*      users:(("rsysl
ogd",pid=4063,fd=9))
roslyakov1@roslyakov1:~$
```

7) Проверка получения логов на сервере



The screenshot shows a VMware Workstation 17 Player window titled "VM1 - VMware Workstation 17 Player (Non-commercial use only)". The interface includes a top toolbar with icons for Player, Power, Snapshot, and other functions. Below the toolbar, a status bar displays "Обзор" (Overview), "Терминал" (Terminal), the date and time "Вт, 21 ноября 13:35", and the language "en". The main area shows a terminal window titled "roslyakov1@roslyakov1: ~". The terminal output displays system logs for rsyslogd and the kernel, including timestamps, IP addresses, and system messages.

```
roslyakov1@roslyakov1:~$ sudo cat /var/log/syslog
2023-11-21T12:57:39.038892+03:00 roslyakov1 systemd[1]: Listening on syslog.socket - Syslog Socket.
2023-11-21T12:57:39.038968+03:00 roslyakov1 systemd[1]: Starting rsyslog.service - System Logging Service...
2023-11-21T12:57:39.039118+03:00 roslyakov1 rsyslogd: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd. [v8.2302.0]
2023-11-21T12:57:39.039214+03:00 roslyakov1 rsyslogd: [origin software="rsyslogd" swVersion="8.2302.0" x-pid="3942" x-info="https://www.rsyslog.com"] start
2023-11-21T12:57:39.039321+03:00 roslyakov1 systemd[1]: Started rsyslog.service - System Logging Service.
2023-11-21T12:57:39.039405+03:00 roslyakov1 kernel: [ 0.000000] Linux version 6.1.0-13-amd64 (debian-kernel@lists.debian.org) (gcc-12 (Debian 12.2.0-14) 12.2.0, GNU ld (GNU Binutils for Debian) 2.40) #1 SMP PREEMPT_DYNAMIC Debian 6.1.55-1 (2023-09-29)
2023-11-21T12:57:39.039423+03:00 roslyakov1 kernel: [ 0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-6.1.0-13-amd64 root=UUID=6087f0d7-3a0a-4038-b481-c229b6d11295 ro quiet
2023-11-21T12:57:39.039425+03:00 roslyakov1 kernel: [ 0.000000] Disabled fast string operations
2023-11-21T12:57:39.039425+03:00 roslyakov1 kernel: [ 0.000000] BIOS-provided physical RAM map:
2023-11-21T12:57:39.039426+03:00 roslyakov1 kernel: [ 0.000000] BIOS-e820: [ mem 0x0000000000000000-0x000000000009e7ff] usable
```

8)Запуск контейнеров Loki и Grafana

```
roslyakov1@roslyakov1:~$ sudo docker run -d --name=loki -p 3100:3100 grafana/loki
Unable to find image 'grafana/loki:latest' locally
latest: Pulling from grafana/loki
7264a8db6415: Pull complete
95959d24c6a5: Pull complete
24832b05718c: Pull complete
f2c1184e4d69: Pull complete
52aa554919fe: Pull complete
e7b72d49fcb6: Pull complete
Digest: sha256:6074e01dbe03cbf8f848c478f7e98df326f984d263162eff5bd47db3970f7ffb
Status: Downloaded newer image for grafana/loki:latest
be6043b25a74c0469a32f9a66f47521b44cefa94b4102b14f52a7a50584f0eb6
roslyakov1@roslyakov1:~$ sudo docker run -d --name=grafana -p 3000:3000 grafana/grafana
Unable to find image 'grafana/grafana:latest' locally
latest: Pulling from grafana/grafana
96526aa774ef: Pull complete
932a65841cb5: Pull complete
a486d8a79b5f: Pull complete
9f17a73c904a: Pull complete
c1ade82e0f62: Pull complete
882619e0a642: Pull complete
2f0808654570: Pull complete
df5835f957f7: Pull complete
b94284e881a5: Pull complete
3e944d3294a3: Pull complete
Digest: sha256:e3e9c2b5776fe3657f4954dfa91579224f98a0316f51d431989b15425e95530f
Status: Downloaded newer image for grafana/grafana:latest
16d2b28da0f55230bf7183020e06f6971cadcdcee4b6d003b0d67f78ddacb84
```

9)запуск promtail

```
roslyakov1@roslyakov1:~$ sudo docker run -d --name=promtail -v /var/log:/var/lo
g -v /home/roslyakov1/promtailconf:/etc/promtail/config.eml grafana/promtail
Unable to find image 'grafana/promtail:latest' locally
latest: Pulling from grafana/promtail
e67fdae35593: Pull complete
40fc0fd1b651: Pull complete
695575f8fc12: Pull complete
e733908d7d5f: Pull complete
8329f7ce5bd9: Pull complete
09f61dac9b77: Pull complete
Digest: sha256:3ec78a089e5cb5173f5348ee29de4d3cdab29493776ac5704db8727fa0cda60f
Status: Downloaded newer image for grafana/promtail:latest
3dc268f2c77d5a95398e175c90f4dca3c3b6860616920c9c3877dc26ce937207
roslyakov1@roslyakov1:~$
```

10)конфиг Promtail

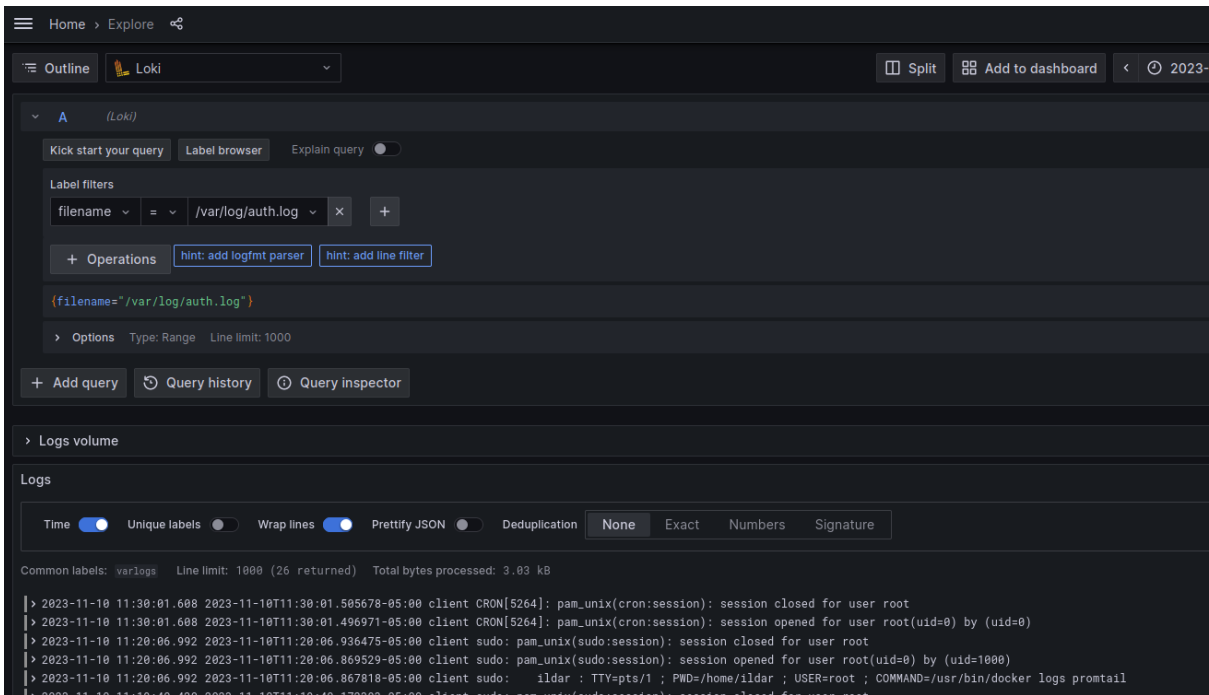
```
GNU nano 7.2
server:
  http_listen_port: 9080
  grpc_listen_port: 0

positions:
  filename: /tmp/positions.yaml

clients:
  - url: http://10.0.0.10:3100/loki/api/v1/push

scrape_configs:
- job_name: system
  static_configs:
  - targets:
    - localhost
    labels:
      job: varlogs
      __path__: /var/log/*log
```


11) проверка работы Grafana



12) проверка работы Signoz

