

А. Г. УЙМИН

ПРАКТИКУМ.  
ДЕМОНСТРАЦИОННЫЙ  
ЭКЗАМЕН  
БАЗОВОГО УРОВНЯ.  
СЕТЕВОЕ И СИСТЕМНОЕ  
АДМИНИСТРИРОВАНИЕ

УЧЕБНОЕ ПОСОБИЕ



САНКТ-ПЕТЕРБУРГ•МОСКВА•КРАСНОДАР  
2023

УДК 004  
ББК 32.81я723

**У 36 Уймин А. Г.** Практикум. Демонстрационный экзамен базового уровня. Сетевое и системное администрирование : учебное пособие для СПО / А. Г. Уймин. — Санкт-Петербург : Лань, 2023. — 116 с. : ил. — Текст : непосредственный.

**ISBN 978-5-507-46869-0**

Учебное пособие предназначено для преподавателей и студентов, осваивающих основные профессиональные образовательные программы СПО укрупненных групп «Информатика и вычислительная техника» и «Информационная безопасность» в целях повышения уровня умений и знаний в области профессиональной деятельности; обеспечивает подготовку к сдаче Демонстрационного экзамена в рамках проектов, реализуемых ФГБОУ ДПО «Институт развития профессионального образования» (код и наименование профессии (специальности) среднего профессионального образования 09.02.06 — «Сетевое и системное администрирование», наименование квалификации — «Сетевой и системный администратор»).

Соответствует современным требованиям Федерального государственного образовательного стандарта среднего профессионального образования и профессиональным квалификационным требованиям.

УДК 004  
ББК 32.81я723

**Автор:**

А. Г. Уймин — старший преподаватель кафедры безопасности информационных технологий факультета комплексной безопасности ТЭК РГУ нефти и газа (НИУ) им. И. М. Губкина, сертифицированный эксперт Союза «Молодые профессионалы (Worldskills Russia)» по компетенции «Сетевое и системное администрирование».

**Рецензент:**

*A. B. БЕЛОУСОВ* — кандидат технических наук, доцент, доцент кафедры разведочной геофизики и компьютерных систем, зав. кафедрой безопасности информационных технологий Российского государственного университета нефти и газа (НИУ) им. И. М. Губкина.

**Обложка**  
*П. И. ПОЛЯКОВА*

© Издательство «Лань», 2023  
© А. Г. Уймин, 2023  
© Издательство «Лань», художественное оформление, 2023

## **ПРЕДИСЛОВИЕ**

Учебное пособие актуально и соответствует требованиям и содержанию:

– Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;

– приказа Министерства образования и науки Российской Федерации от 1 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам» (зарегистрирован в Министерстве юстиции Российской Федерации 20 августа 2013 г., регистрационный № 29444);

– приказа Министерства образования и науки Российской Федерации от 23 августа 2017 г. № 816 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ» (зарегистрирован в Министерстве юстиции Российской Федерации 18 сентября 2017 г., регистрационный № 48226);

– приказа Министерства науки и высшего образования Российской Федерации и Министерства просвещения Российской Федерации от 5 августа 2020 г. № 882/391 «Об организации и осуществлении образовательной деятельности при сетевой форме реализации образовательных программ» (зарегистрирован в Министерстве юстиции Российской Федерации 10 сентября 2020 г. № 59764);

– приказа Министерства науки и высшего образования Российской Федерации и Министерства просвещения Российской Федерации от 5 августа 2020 г. № 885/390 «О практической подготовке обучающихся» (зарегистрирован в Министерстве юстиции Российской Федерации 11 сентября 2020 г., регистрационный № 59778).

Учебное пособие может быть использовано преподавателями и студентами, осваивающими основные профессиональные образовательные программы СПО укрупненных групп 09.00.00 «Информатика и вычислительная техника»; 10.00.00 «Информационная безопасность». Также учебное пособие может быть использовано при освоении дополнительных образовательных программ повышения квалификации педагогических работников образовательных организаций, реализующих программы среднего профессионального образования, из числа преподавателей и мастеров производственного обучения.

Учебное пособие разработано в целях повышения уровня умений и знаний в области сетевого и системного администрирования, профессиональной деятельности в соответствии с профессиональным стандартом 06.026 «Системный администратор информационно-коммуникационных систем».

Структурно учебное пособие представляет собой комплект практических работ, включающий описание задания; необходимое оборудование, приборы, материалы и программное обеспечение для выполнения задания; методику выполнения задания; сетевые диаграммы; схему оценивания выполненного задания, являющуюся одним из вариантов заданий, выполняемых в процессе прохождения промежуточной аттестации, включая квалификационные экзамены по профессиональным модулям.

Для каждого задания имеются пошаговые инструкции выполнения элементов заданий, пояснения выполняемых действий и объяснения последствий неправильных действий и приемов; скриншоты экрана; ссылки на электронные ресурсы для получения необходимой информации и инструкций для выполнения заданий.

В результате выполнения заданий по практическим работам обучающиеся смогут систематизировать и закрепить знания и умения, а преподаватели — оценить уровень подготовки обучающихся к самостоятельной работе и уровень практических навыков для участия в сдаче не только промежуточной аттестации, но и итоговой государственной аттестации.

Руководитель профильного ресурсного Центра  
информационных технологий и робототехники, почетный работник СПО,  
эксперт, имеющий право участия в оценке демонстрационного экзамена по стандартам

Worldskills по компетенции «Сетевое и системное администрирование»,  
мастер-эксперт по компетенции «Корпоративная защита от внутренних угроз  
информационной безопасности»  
О. А. Терентьева

## **ВВЕДЕНИЕ**

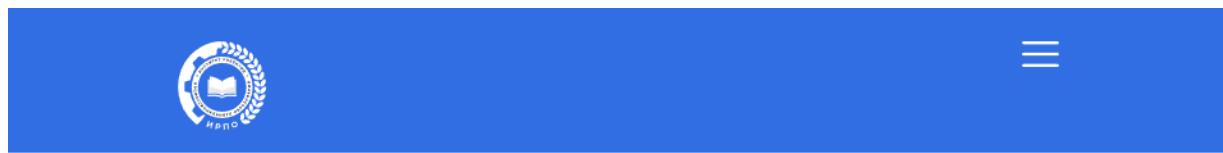
В 2023 г. ГИА проводится в форме, установленной федеральными государственными образовательными стандартами среднего профессионального образования (далее — ФГОС СПО), в соответствии с которыми обучающиеся завершают освоение образовательной программы. Оценочные материалы для проведения ГИА в форме демонстрационного экзамена базового и профильного уровня в 2023 г. размещены на следующих информационных ресурсах:

2023 г. и после — <https://om.firpo.ru/competencies>;

до 2023 г. — <https://om.firpo.ru/archive>.

Оценочные материалы для проведения ГИА в форме демонстрационного экзамена профильного уровня в рамках федерального проекта «Профессионализм» в 2023 г. размещены на следующем информационном ресурсе: <https://firpo.ru/activities/register-of-evaluation-materials>.

Комплект оценочной документации — паспорт КОД 1.1- 2022-2024 — размещен по ссылке <https://om.firpo.ru/competencies/b6cee2a9-6cff-4dc1-aca4-333ed0982842/categories/97e6cfe2-face-48b3-84df-a74f3bd428fe>.



[« Назад](#)

[Главная](#) > [Разделы](#) > [Раздел](#)



### **09.02.06**

#### **Сетевое и системное администрирование**



**09.02.06 Сетевое и системное администрирование 2023**

Настоящий КОД предназначен для организации и проведения аттестации обучающихся по программам среднего профессионального образования в форме демонстрационного экзамена базового уровня.

В данном разделе указаны основные характеристики КОД, и они должны использоваться при планировании, проведении и оценке результатов демонстрационного экзамена образовательными организациями, ЦПДЭ.

Согласно оценочным материалам демонстрационного экзамена базового уровня комплект с оценочной документацией предназначен для:

Код и наименование профессии (специальности) среднего профессионального образования	09.02.06 Сетевое и системное администрирование
Наименование квалификации	Сетевой и системный администратор
Федеральный государственный образовательный стандарт среднего профессионального образования по профессии (специальности) среднего профессионального образования (ФГОС СПО):	ФГОС СПО по специальности 09.02.06 «Сетевое и системное администрирование», утвержденный приказом Министерства образования и науки РФ от 09.12.2016 № 1548
Код комплекта оценочной документации	КОД 09.02.06-2023

# ВИРТУАЛЬНЫЕ МАШИНЫ И КОММУТАЦИЯ

Таблица 1

## Характеристики и адресация ВМ

Имя ВМ	ОС	ОЗУ	Кол-во ядер	IP-адреса	Дополнительно
RTR-L	Debian 11	2 Гб	2	4.4.100/24 192.168.200.254/ 24	
	Cisco CSR		4		
RTR-L	Debian 11	2 Гб	2	5.5.5/100/24 172.16.100.254/ 4	
	Cisco CSR		4		
SRV	Windows Server 2019	4 Гб	4	192.168.200.200/24	Дополнительные диски: 2 шт. по 2 Гб
WEB-L	Debian 11	2 Гб	2	192.168.200.100/24	
WEB-R	Debian 11	2 Гб	2	172.16.100.100/24	
ISP	Debian 11	2 Гб	2	4.4.4.1/24 5.5.5.1/24 3.3.3.1/24	
CLI	Windows 10	4	4	3.3.3.10/24	

Cisco CSR не используется в связи с уходом компании Cisco из РФ.

Таблица 2

## DNS-записи зон

Зона	Тип записи	Ключ	Значение
demo.wsr	A	ISP	3.3.3.1
	A	www	4.4.4.100
	A	www	5.5.5.100
	CNAME	internet	ISP
int.demo.wsr	A	WEB-L	192.168.200.100
	A	WEB-R	172.16.100.100
	A	SRV	192.168.200.200
	A	rtr-l	192.168.200.254
	A	rtr-r	172.16.100.254
	CNAME	webapp	web-l
	CNAME	webapp	WEB-R
	CNAME	ntp	SRV
	CNAME	dns	SRV

# ПОРЯДОК ВЫПОЛНЕНИЯ

Рекомендуемый порядок выполнения задания представлен следующим образом:

## Образец задания



**Рис. 1**  
Топология

# **ВЫПОЛНЕНИЕ ПРОЕКТИРОВАНИЯ КАБЕЛЬНОЙ СТРУКТУРЫ КОМПЬЮТЕРНОЙ СЕТИ**

## **1. Виртуальные машины и коммутация**

Необходимо выполнить работу по созданию виртуальных машин и их базовой конфигурации.

На основе предоставленных ВМ или шаблонов ВМ создайте отсутствующие виртуальные машины в соответствии со схемой.

Характеристики ВМ установите в соответствии со схемой сети.

Коммутацию (если таковая выполнена) выполните в соответствии со схемой сети.

Имена хостов в созданных ВМ должны быть установлены в соответствии со схемой.

Адресация должна быть выполнена в соответствии с таблицей 1.

## **2. Сетевая связанность**

В рамках данного модуля требуется обеспечить сетевую связанность между регионами работы приложения, а также обеспечить выход ВМ в имитируемую сеть Интернет:

– сети, подключенные к ISP, считаются внешними: запрещено прямое попадание трафика из внутренних сетей во внешние и наоборот.

Настройте статический маршрут по умолчанию на маршрутизаторах RTR-L и RTR-R.

Настройте динамическую трансляцию портов (PAT):

– на маршрутизаторе RTR-L настройте динамическую трансляцию портов (PAT) для сети 192.168.200.0/24 в соответствующие адреса исходящего интерфейса;

– на маршрутизаторе RTR-R настройте динамическую трансляцию портов (PAT) для сети 172.16.100.0/24 в соответствующие адреса исходящего интерфейса.

## **3. Конфигурация виртуальных частных сетей**

Между платформами RTR-L и RTR-R должен быть установлен туннель, позволяющий осуществлять связь между регионами с применением внутренних адресов со следующими параметрами:

а) используйте в качестве VTI интерфейс Tunnell;

б) между платформами должен быть установлен туннель, позволяющий осуществлять связь между регионами с применением внутренних адресов.

## **4. Настройка списков контроля доступа**

Платформа управления трафиком RTR-R выполняет контроль входящего трафика согласно следующим правилам:

а) разрешаются подключения к портам HTTP и HTTPS для всех клиентов;

б) разрешаются подключения к портам HTTP и HTTPS для всех клиентов:

– порты необходимы для работы настраиваемых служб;

с) разрешается работа выбранного протокола организации защищенной связи:

– разрешение портов должно быть выполнено по принципу «необходимо и достаточно»;

д) разрешается работа протоколов ICMP;

е) разрешается работа протокола SSH;

ф) прочие подключения запрещены;

г) для обращений к платформам со стороны хостов, находящихся внутри регионов, ограничений быть не должно.

Обеспечьте настройку служб SSH регионов Left:

а) подключения со стороны внешних сетей по протоколу к платформе управления трафиком RTR-L на порт 2244 должны быть перенаправлены на ВМ WEB-L;

б) подключения со стороны внешних сетей по протоколу к платформе управления трафиком RTR-L на порт 2222 должны быть перенаправлены на ВМ WEB-R.

## **5. Инфраструктурные службы**

В рамках данного модуля необходимо настроить основные инфраструктурные службы и настроить представленные ВМ на применение этих служб для всех основных функций.

Выполните настройку первого уровня DNS-системы стенда:

а) используется BM ISP;

б) обслуживается зона demo.wsr:

– наполнение зоны должно быть реализовано в соответствии с таблицей 2;

с) сервер делегирует зону int.demo.wsr на SRV:

– поскольку SRV находится во внутренней сети Западного региона, делегирование происходит на внешний адрес маршрутизатора данного региона;

– маршрутизатор региона должен транслировать соответствующие порты DNS-службы в порты сервера SRV;

д) внешний клиент CLI должен использовать DNS-службу, развернутую на ISP по умолчанию.

5.2. Выполните настройку второго уровня DNS-системы стенда:

а) используется BM SRV;

б) обслуживается зона int.demo.wsr;

с) обслуживаются обратные зоны для внутренних адресов регионов;

д) сервер принимает рекурсивные запросы, исходящие от адресов внутренних регионов;

е) внутренние хосты регионов (равно как и платформы управления трафиком) должны использовать данную DNS-службу для разрешения всех запросов имен.

Выполните настройку первого уровня синхронизации времени:

а) используется сервер ISP;

б) сервер считает собственный источник времени верным, stratum = 3;

с) сервер допускает подключение только через внешний адрес соответствующей платформы управления трафиком:

– подразумевается обращение SRV для синхронизации времени;

д) клиент CLI должен использовать службу времени ISP.

Выполните конфигурацию службы второго уровня времени на SRV:

а) сервер синхронизирует время с хостом ISP:

– синхронизация с другими источниками запрещена;

б) сервер должен допускать обращения внутренних хостов регионов, в том числе и платформы управления трафиком, для синхронизации времени;

с) все внутренние хосты (в том числе и платформы управления трафиком) должны синхронизировать свое время с SRV.

Реализуйте файловый SMB-сервер на базе SRV:

а) сервер должен предоставлять доступ для обмена файлами серверами WEB-L и WEB-R;

б) сервер, в зависимости от ОС, использует следующие каталоги для хранения файлов:

– /mnt/storage для систем на базе Linux;

– диск R:\ для систем на базе Windows;

с) хранение файлов осуществляется на диске (смонтированном по указанным выше адресам), реализованном по технологии RAID типа «Зеркало».

Сервера WEB-L и WEB-R должны использовать службу, настроенную на SRV, для обмена файлами между собой:

а) служба файлового обмена должна позволять монтирование в виде стандартного каталога Linux:

– разделяемый каталог должен быть смонтирован по адресу /opt/share;

б) каталог должен позволять удалять и создавать файлы в нем для всех пользователей.

5.7. Выполните настройку центра сертификации на базе SRV:

а) в случае применения решения на базе Linux используется центр сертификации типа OpenSSL и располагается по адресу /var/ca;

б) выдаваемые сертификаты должны иметь срок действия не менее 300 дней;

с) параметры выдаваемых сертификатов:

– страна RU;

- организация (DEMO, WSR);
- прочие поля (за исключением CN) должны быть пусты.

## **6. Инфраструктура веб-приложения**

Данный блок подразумевает установку и настройку доступа к веб-приложению, выполненному в формате контейнера Docker.

Образ Docker (содержащий веб-приложение) расположен на ISO-образе дополнительных материалов:

- а) выполните установку приложения AppDocker0.

Пакеты для установки Docker расположены на дополнительном ISO-образе.

Инструкция по работе с приложением расположена на дополнительном ISO-образе.

Необходимо реализовать следующую инфраструктуру приложения:

- а) клиентом приложения является CLI (браузер Edge);

- b) хостинг приложения осуществляется на ВМ WEB-L и WEB-R;

- c) доступ к приложению осуществляется на DNS-имени www.demo.wsr:

– имя должно разрешаться во «внешние» адреса ВМ управления трафиком в обоих регионах;

- d) доступ к приложению должен быть защищен с применением технологии TLS:

– необходимо обеспечить корректное доверие сертификату сайта, без применения «исключений» и подобных механизмов;

е) незащищенное соединение должно переводиться на защищенный канал автоматически.

Необходимо обеспечить отказоустойчивость приложения:

а) сайт должен продолжать обслуживание (с задержкой не более 25 с) в следующих сценариях:

- отказ одной из ВМ WEB;

- отказ одной из ВМ управления трафиком.

При необходимости для доступа к приложению допускается реализовать реверс-прокси или трансляцию портов.

# ЗАДАНИЯ

**Задание 1.** Имена хостов в созданных ВМ должны быть установлены в соответствии со схемой (рис. 2).

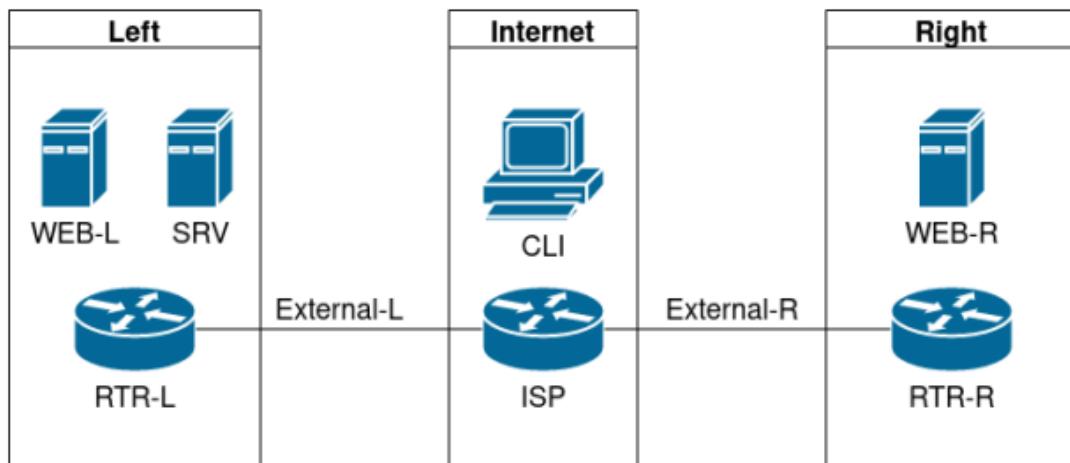


Рис. 2  
Публичная схема экзаменационного задания

## Как делать

Изначально имя машины стандартное — localhost.

```
localhost login: root
Password:
Last login: Thu Apr  2 08:08:14 EDT 2020 on tty1
Linux localhost 4.19.0-5-amd64 #1 SMP Debian 4.19.37-5 (2019-04-10)
The programs included with the Debian GNU/Linux system are free
software; the exact distribution terms for each program are described in
individual files in /usr/share/doc/*/*copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@localhost:~# _
```

Учетная запись для работы с операционной системой настраивается самостоятельно (по умолчанию логин root с паролем toor).

Для установки имени виртуальной машины необходимо воспользоваться утилитой HOSTNAMECTL

hostnamectl set-hostname <hostname>; exec bash.

```
ISP (DEB)

root@debian:~# hostnamectl set-hostname ISP; exec bash
root@ISP:~#
```

Описание применяемых команд:

hostnamectl — программа для управления именем машины;  
set-hostname — аргумент, позволяющий выполнить изменение хостнейма;  
<hostname> — целевое имя машины;  
exec bash — перезапуск оболочки bash для отображения нового хостнейма.

### Как проверить

Перезагрузите компьютер с помощью команды reboot. После загрузки компьютера изменилось приглашение системы к вводу команд.

```
ISP login: root
Password:
Linux ISP 5.10.0-10-amd64 #1 SMP Debian 5.10.84-1 (2021-12-08) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Jan 15 21:38:36 MSK 2022 on ttu1
root@ISP:~# hostname
ISP
root@ISP:~# _
```

Команда hostname выведет текущее название машины.

```
Last login: Sat Jan 15 21:38:36 MSK 2022 on
root@ISP:~# hostname
ISP
root@ISP:~#
```

**Дополнительная информация:** hostname — это имя, которое присваивается компьютеру, подключенному к сети, которое однозначно идентифицирует его в сети и вашей инфраструктуре.

### Краткая справка

- присваивание имени компьютеру (Hostname) (Debian) (<https://www.debian.org/doc/manuals/debian-handbook/sect.hostname-name-service.ru.html>; <https://www.redhat.com/sysadmin/set-hostname-linux>);
- присваивание имени компьютеру (Hostname) (Windows Server) (<https://www.snel.com/support/hostname-change-on-windows-server-2019>).

**Задание 2.** Адресация должна быть выполнена в соответствии с таблицей 1.

### Как делать

Настройка IP-адресов в системе Debian происходит в конфигурационном файле /etc/network/interfaces, но сначала нужно узнать всю необходимую информацию.

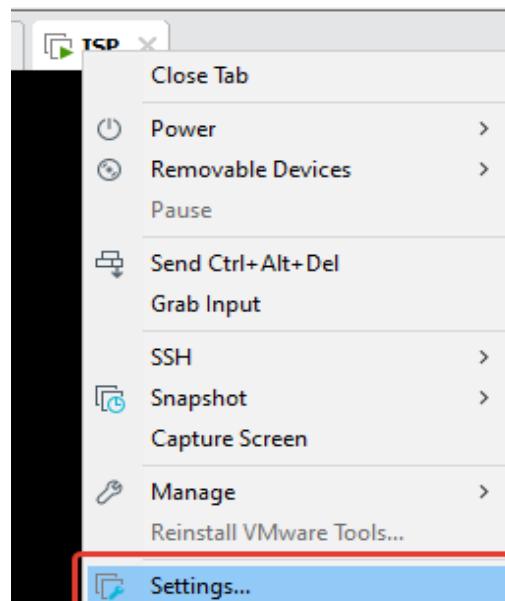
Просмотр существующих интерфейсов выполняется командой

ip a

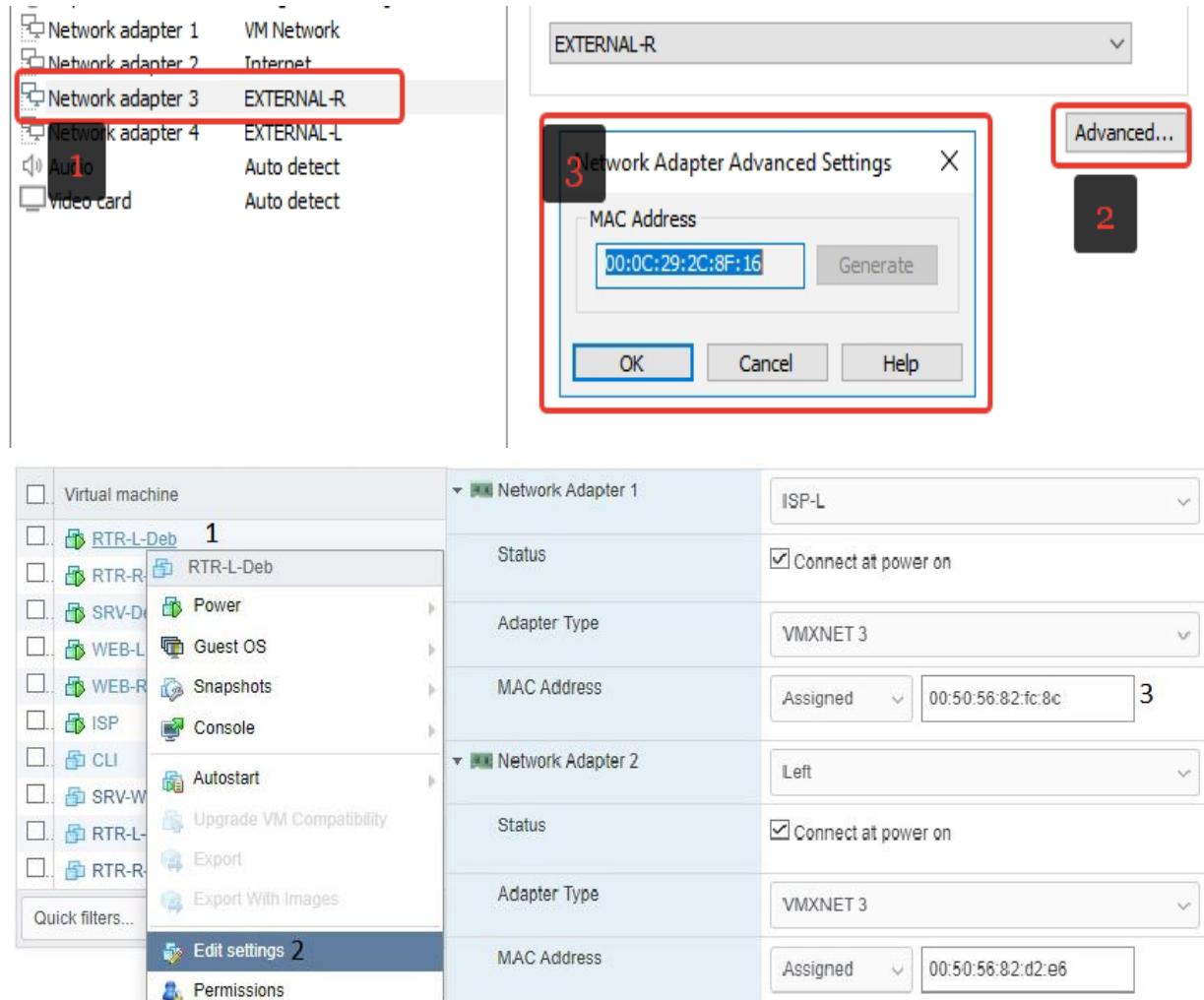
а=вывести IP-адресацию.

```
root@ISP:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens32: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
00
    link/ether 00:0c:29:2c:8f:0c brd ff:ff:ff:ff:ff:ff
    altname enp2s0
    inet 3.3.3.1/24 brd 3.3.3.255 scope global ens32
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe2c:8f0c/64 scope link
        valid_lft forever preferred_lft forever
3: ens35: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 q
00
    link/ether 00:0c:29:2c:8f:16 brd ff:ff:ff:ff:ff:ff
    altname enp2s3
    inet 5.5.5.1/24 brd 5.5.5.255 scope global ens35
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe2c:8f16/64 scope link
        valid_lft forever preferred_lft forever
```

Красным цветом показано название интерфейса (в примере оно может отличаться!), оранжевым цветом — его MAC-адрес (в примере MAC-адрес может отличаться!). Для того чтобы понять, какой интерфейс куда настроен, необходимо ориентироваться по их MAC-адресам. В настройках виртуальной машины, в настройках сетевых интерфейсов можно увидеть MAC-адрес (кнопка Advanced) и сеть, к которой подключен сетевой интерфейс. Нажатием правой кнопки мыши на имя виртуальной машины откроется выпадающее меню, необходимо открыть ее настройки.



Перейдя на вкладку **Settings**, можно увидеть список всех настроенных параметров виртуальной машины. Параметры сетевых интерфейсов просматриваются во вкладке **Advanced** относительно каждого сетевого адаптера.



### Настройка на ESXi.

Например, возьмем интерфейс под номером 3 с названием EXTERNAL-R, что по названию указывает на его принадлежность к внешней подсети провайдера в сторону RIGHT. MAC-адрес оканчивается на 8F:16.

Чтобы сравнить MAC-адреса, используется команда ip a.

```
3: ens35: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
00
    link/ether 00:0c:29:2c:8f:16 brd ff:ff:ff:ff:ff:ff
    altname enp2s3
    inet 5.5.5.1/24 brd 5.5.5.255 scope global ens35
        valid_lft forever preferred_lft forever
```

Интерфейс имеет имя `ens35`, соответственно, именно его предстоит настроить как внешний интерфейс до `RTR-R` — с адресом `5.5.5.1/24`. Соответствующие действия необходимо проделать с каждым интерфейсом ISP и других ВМ.

После того, как были определены подключения всех интерфейсов, можно переходить к настройке.

Сетевые параметры интерфейсов в Debian 11 располагаются в файле /etc/network/interfaces. Он открывается с помощью любого текстового редактора, в рамках примера используется редактор vim

```
vim /etc/network/interfaces
```

Для установки vim необходимо подключить DVD-1 образ в настройках машины и произвести установку с DVD (apt-cdrom add, затем apt update. Если apt отклонит источник обновления как ненадежный (здесь и далее), следует добавить параметр [trusted=yes] через пробелы между deb и cdrom в /etc/apt/sources.list, если проверка безопасности не одобрит обновления)).

Далее опишем параметры, обязательные к указанию в данном файле.

### Правила настройки

auto <interface\_name><sup>1</sup> — автоматическое включение интерфейса;

iface <interface\_name><sup>2</sup> inet static — перевод интерфейса в режим статического IP.

Также, в случае, если необходимо настроить получение адреса динамически, через протокол DHCP, то следует указать запись:

iface <interface\_name><sup>2</sup> inet dhcp;

address <IP>/<MASK><sup>3</sup> — установка IP-адреса и маски подсети;

gateway <gateway><sup>4</sup> — шлюз по умолчанию;

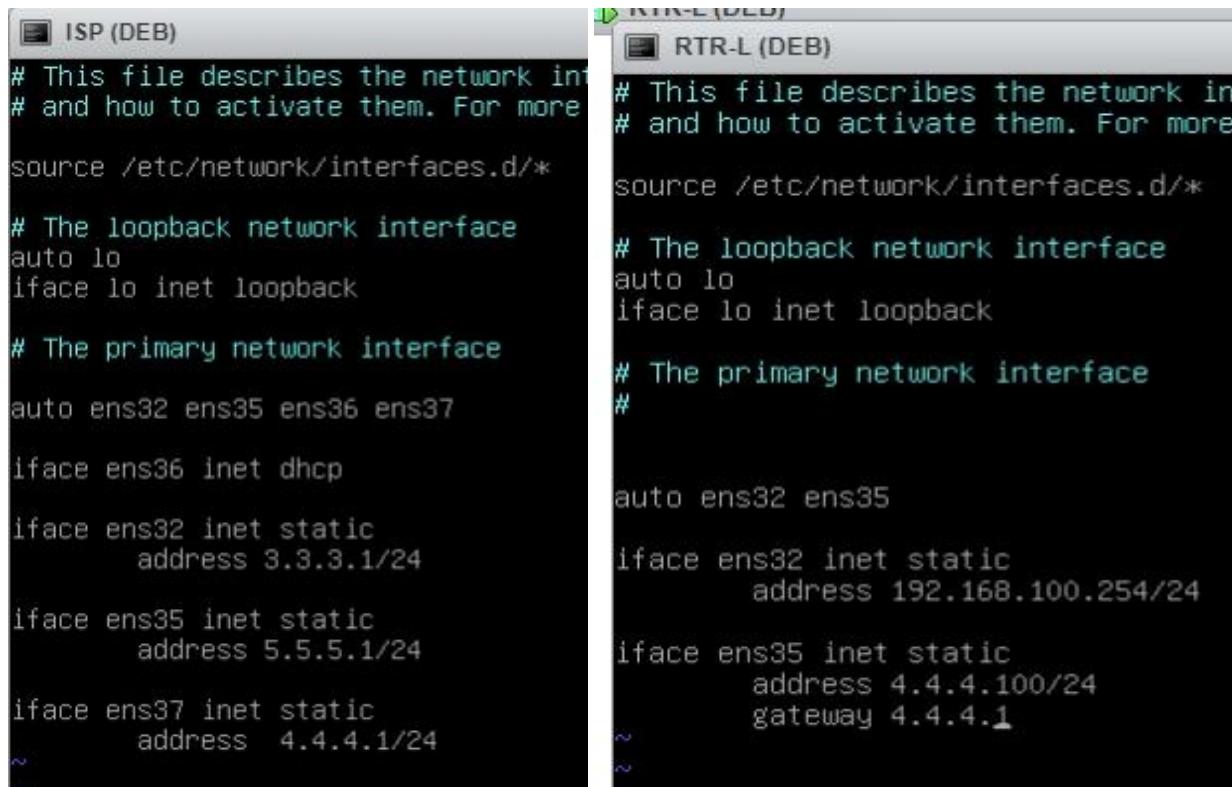
<sup>1</sup><interface\_name> — имя сетевого интерфейса;

<sup>2</sup><IP> — IP-адрес в соответствии с топологией;

<sup>3</sup><MASK> — маска подсети в соответствии с топологией;

<sup>4</sup><gateway> — IP-адрес шлюза по умолчанию. Для оконечных устройств шлюзом будет являться вышестоящий маршрутизатор или сетевой экран.

### Примеры описания настроек на виртуальных машинах экзаменационного стенда



```
ISP (DEB)
# This file describes the network interfaces
# and how to activate them. For more
source /etc/network/interfaces.d/*
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto ens32 ens35 ens36 ens37

iface ens36 inet dhcp

iface ens32 inet static
    address 3.3.3.1/24

iface ens35 inet static
    address 5.5.5.1/24

iface ens37 inet static
    address 4.4.4.1/24
~
```

```
RTR-L (DEB)
# This file describes the network interfaces
# and how to activate them. For more
source /etc/network/interfaces.d/*
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
#
# auto ens32 ens35

iface ens32 inet static
    address 192.168.100.254/24

iface ens35 inet static
    address 4.4.4.100/24
    gateway 4.4.4.1
~
```

## RTR-R

```
# This file describes the network interfaces on your system. For more information  
# about interfaces and how to activate them, For more information  
source /etc/network/interfaces.d/*  
  
# The loopback network interface  
auto lo  
iface lo inet loopback  
  
# The primary network interface  
  
auto ens32 ens35  
  
iface ens32 inet static  
    address 172.16.100.254/24  
  
iface ens35 inet static  
    address 5.5.5.100/24  
    gateway 5.5.5.1  
~  
~  
~
```

## WEB-L

```
# This file describes the network interfaces on your system. For more information  
# about interfaces and how to activate them, For more information  
source /etc/network/interfaces.d/*  
  
# The loopback network interface  
auto lo  
iface lo inet loopback  
  
# The primary network interface  
auto ens32  
iface ens32 inet static  
    address 192.168.100.100/24  
    gateway 192.168.100.254  
~  
~  
~
```

## WEB-R

```
# This file describes the network interfaces on your system. For more information  
# about interfaces and how to activate them, For more information  
source /etc/network/interfaces.d/*  
  
# The loopback network interface  
auto lo  
iface lo inet loopback  
  
auto ens32  
iface ens32 inet static  
    address 172.16.100.100/24  
    gateway 172.16.100.254  
~  
~
```

## SRV

```
source /etc/network/interfaces.d/*  
  
# The loopback network interface  
auto lo  
iface lo inet loopback  
  
auto ens32  
iface ens32 inet static  
    address 192.168.100.200/24  
    gateway 192.168.100.254  
~  
~
```

После настройки конфигурационного файла /etc/network/interfaces необходимо перезапустить службу networking (на всех виртуальных машинах, где производилась настройка): systemctl restart networking.

### Как проверить

Проверка осуществляется командой: ip a.

```
2: ens32: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc  
00  
    link/ether 00:0c:29:2c:8f:0c brd ff:ff:ff:ff:ff:ff  
    altname enp2s0  
   inet 3.3.3.1/24 brd 3.3.3.255 scope global ens32  
        valid_lft forever preferred_lft forever  
    inet6 fe80::20c:29ff:fe2c:8f0c/64 scope link  
        valid_lft forever preferred_lft forever
```

### Дополнительная информация

На Debian можно установить ПО nmtui и производить настройку в графическом режиме, с помощью данной команды выполняется его установка

```
apt install network-manager
```

Но стоит обратить внимание, что если изначальная настройка была произведена с помощью конфигурационного файла `/etc/network/interfaces`, то не рекомендуется настраивать сетевую адресацию через `nmtui`. Разные сетевые менеджеры вызовут в системе конфликт настроек, в итоге не применив ни одну из конфигураций.

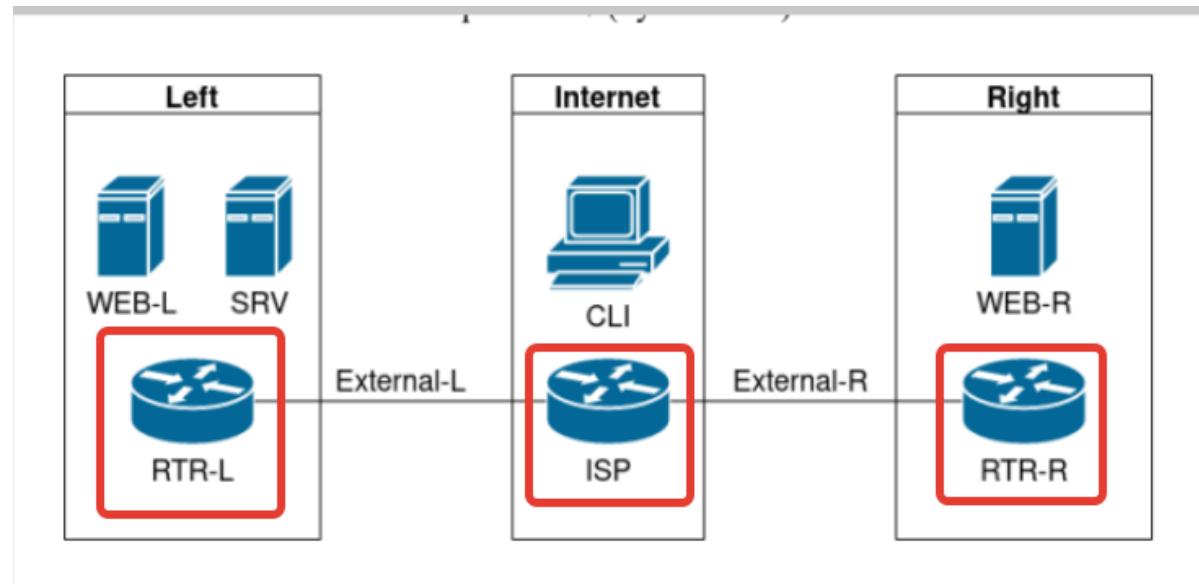
#### Краткая справка

– сетевая настройка на Debian (Debian) (<https://wiki.debian.org/NetworkConfiguration> <https://manpages.debian.org/buster/network-manager/nmtui.1>).

**Задание 3.** На всех сетевых устройствах необходимо включить `ip forwarding` для включения маршрутизации на оборудовании.

Данного пункта задания нет в документе, но он обязателен для успешного выполнения.

#### Как делать



На данных устройствах необходимо провести настройку.

На RTR-R, RTR-L и ISP выполняется следующая команда

```
echo "net.ipv4.ip_forward=1" > /etc/sysctl.conf; sysctl -p
```

Если все выполнено верно — отобразится введенный выше параметр:

```
root@RTR-R:~# echo "net.ipv4.ip_forward=1" > /etc/sysctl.conf; sysctl -p
net.ipv4.ip_forward = 1
root@RTR-R:~#
```

`echo` — утилита, которая возвращает текст, переданный ей в качестве аргумента. По умолчанию возврат происходит в `stdout` (в текущую сессию терминала), но можно перенаправить вывод в файл при помощи указателя «`>`»;

`net.ipv4.ip_forward=1` — параметр ядра, разрешающий пересылку пакетов между интерфейсами;

`/etc/sysctl.conf` — файл, в котором хранятся опции ядра;

`sysctl -p` — команда, которая читает файл `/etc/sysctl.conf` и применяет перечисленные в нем параметры.

#### Дополнительная информация

Пересылка пакетов включается для реализации в дальнейшем маршрутизации пакетов в сети.

#### Краткая справка

– подробнее про `sysctl` (<https://manpages.debian.org/stretch/procps/sysctl.8.en.html>);

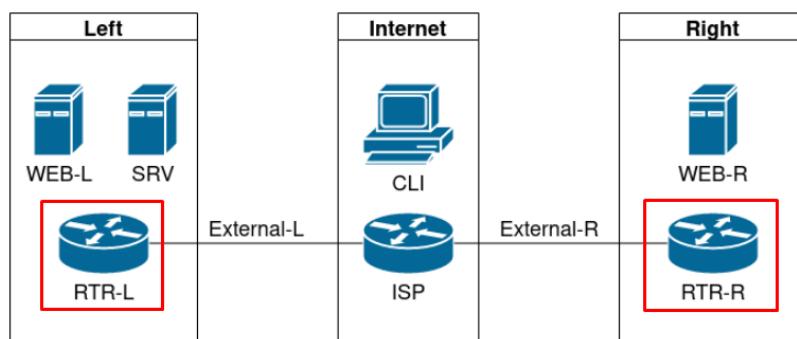
– подробнее про настройку сетевой инфраструктуры на Debian (Debian) (<https://www.debian.org/doc/manuals/debian-handbook/network-infrastructure.ru.html>).

# ОСУЩЕСТВЛЕНИЕ ВЫБОРА ТЕХНОЛОГИИ, ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ И СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ ПРИ ОРГАНИЗАЦИИ ПРОЦЕССА РАЗРАБОТКИ И ИССЛЕДОВАНИЯ ОБЪЕКТОВ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

**Задание 1.** Настройте статический маршрут по умолчанию на маршрутизаторах RTR-L и RTR-R. Настройте динамическую трансляцию портов (PAT):

- на маршрутизаторе RTR-L настройте динамическую трансляцию портов (PAT) для сети 192.168.200.0/24 в соответствующие адреса исходящего интерфейса;
- на маршрутизаторе RTR-R настройте динамическую трансляцию портов (PAT) для сети 172.16.100.0/24 в соответствующие адреса исходящего интерфейса.

**Как делать**



Одной из проблем в развитии сетей является ограниченное количество существующих IPv4-адресов — их около 4,3 млрд. С повсеместным распространением Интернета и ростом количества пользователей стало очевидно, что этого недостаточно. Возникла потребность в инструменте, способном решить эту проблему (по крайней мере до момента, когда будут внедрены IPv6) — и одним из таких инструментов стала технология NAT (Network Address Translation).

Трансляция сетевых адресов (Network Address Translation, NAT) — это подмена какого-либо адреса или порта в пакете. Она, как правило, требуется на границе между сетью компании и провайдером Интернет. Однако это далеко не единственная задача.

Настроить NAT можно с использованием разных пакетов. В качестве примера можно использовать nftables. В Debian 11 пакет установлен по умолчанию, что позволяет сразу перейти к его настройке. Настройка производится при помощи описания конфигурации в файле /etc/nftables.conf.

```
root@RTR-L:~# vim /etc/nftables
```

```
#!/usr/sbin/nft -f
flush ruleset
table inet filter {
    chain input {
        type filter hook input priority 0;
    }
    chain forward {
        type filter hook forward priority 0;
    }
    chain output {
        type filter hook output priority 0;
    }
}
table ip nat {
    chain postROUTING {
        type nat hook postROUTING priority 0;
        ip saddr 192.168.100.0/24 oifname ens35 counter masquerade;
    }
}
```

## Конфигурация RTR-L

```
#!/usr/sbin/nft -f

flush ruleset

table inet filter {
    chain input {
        type filter hook input priority 0;
    }
    chain forward {
        type filter hook forward priority 0;
    }
    chain output {
        type filter hook output priority 0;
    }
}

table ip nat {
    chain postrouting {
        type nat hook postrouting priority 0;
        ip saddr 172.16.100.0/24 oifname ens35 counter masquerade
    }
}
```

## Конфигурация RTR-R

Пояснение касательно настроек в конфигурационных файлах:

`#!/usr/sbin/nft -f` — системная конструкция указывает, что чтение данного файла нужно произвести при помощи команды `/usr/sbin/nft -f`;

`flush ruleset` — очистить все существующие правила перед записью новых;

`table ip nat { }` — создание таблицы с названием nat. Использование протокола IPv4;

`chain postrouting { }` — создание цепочки с названием postrouting;

`type nat` — тип цепочки=nat;

`hook postrouting` — только трафик, прошедший процесс маршрутизации, попадает в эту цепочку;

`priority 0` — цепочка выполняется самой первой для трафика;

`ip saddr` — указывает подсеть, трафик из которой должен попасть в nat;

`oifname` — имя интерфейса, на который был смаршрутизирован трафик;

`counter` — ключевое слово для подсчета пакетов, попавших в данное правило;

`masquerade` — действие, производимое с трафиком (трансляция в адрес исходящего интерфейса).

```
table ip nat {
    chain postrouting {
        type nat hook postrouting priority 0;
        ip saddr 172.16.100.0/24 oifname ens35 counter masquerade
    }
}
```

Данное правило можно прочитать как «В таблице nat, которая работает только с IPv4-трафиком, на этапе, когда трафик прошел процесс маршрутизации, необходимо выбрать пакеты только из подсети 172.16.100.0 с 24 маской, идущие на интерфейс ens35, посчитать их и произвести трансляцию в адрес исходящего интерфейса».

### Как проверить

Для проверки корректности написания правил и немедленного применения можно выполнить команду `nft -f /etc/nftables.conf`

```
root@RTR-R:~# nft -f /etc/nftables.conf
root@RTR-R:~#
```

На данном этапе, в случае ошибок в правописании команд, программа nftables отправит отчет, где подчеркнет опечатку.

После того, как правила были успешно применены, можно посмотреть список правил и счетчики при помощи команды nft list ruleset.

```
root@RTR-R:~# nft list ruleset
table inet filter {
    chain input {
        type filter hook input priority filter; policy accept;
    }

    chain forward {
        type filter hook forward priority filter; policy accept;
    }

    chain output {
        type filter hook output priority filter; policy accept;
    }
}
table ip nat {
    chain postrouting {
        type nat hook postrouting priority filter; policy accept;
        ip saddr 172.16.100.0/24 oifname "ens35" counter packets 4 bytes 298 masquerade
    }
}
root@RTR-R:~#
```

Для того чтобы активировать правила после перезагрузки, в поставке nftables присутствует сервис nftables, по умолчанию он выключен. Необходимо добавить его в автозагрузку и активировать при помощи команды systemctl enable --now nftables.

```
root@RTR-R:~# systemctl enable --now nftables
Created symlink /etc/systemd/system/sysinit.target.wants/nftables.service → /lib/systemd/system/nfta
bles.service.
root@RTR-R:~# _
```

После этого можно на практике проверить работоспособность конфигурации. Для этого достаточно выполнить с WEB-L, WEB-R или SRV трассировку до сервера ISP при помощи команды traceroute -n 5.5.5.1.

```
root@WEB-L:~# traceroute -n 5.5.5.1
traceroute to 5.5.5.1 (5.5.5.1), 30 hops max, 60 byte packets
 1  192.168.100.254  0.443 ms  0.615 ms  0.531 ms
 2  5.5.5.1  1.453 ms  1.514 ms  1.933 ms
root@WEB-L:~# _
```

### Краткая справка

- подробнее про firewalld ([https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/7/html/security\\_guide/sec-viewing\\_current\\_status\\_and\\_settings\\_of\\_firewalld](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sec-viewing_current_status_and_settings_of_firewalld));
- подробнее про iptables (<https://wiki.debian.org/iptables>).

**Задание 2.** Сети, подключенные к ISP, считаются внешними:

– запрещено прямое попадание трафика из внутренних сетей во внешние и наоборот.

Так как внутренние сети теперь расположены за NAT-трафик из внешних сетей не сможет попасть к ним напрямую. Данный пункт выполнен в связи с настройками NAT.

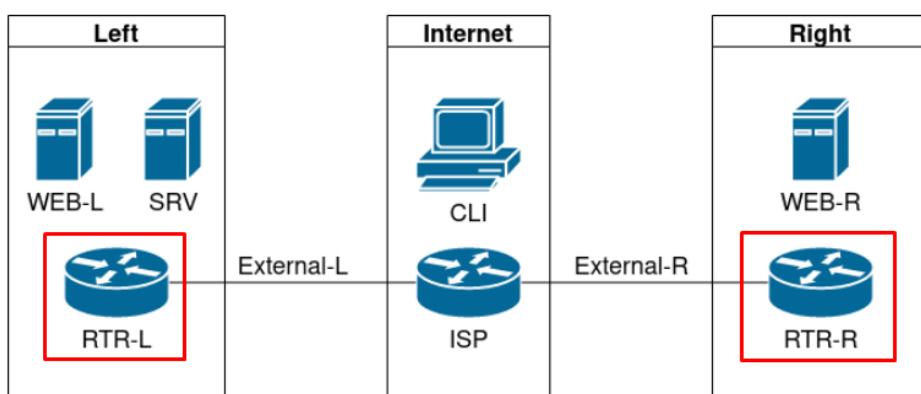
```
root@ISP:~# ping 172.16.100.100
ping: connect: Network is unreachable
```

# КОНФИГУРАЦИЯ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ

**Задание 1.** Между платформами RTR-L и RTR-R должен быть установлен защищенный туннель, позволяющий осуществлять связь между регионами с применением внутренних адресов:

- трафик, проходящий по данному туннелю, должен быть защищен;
- платформа ISP не должна иметь возможности просматривать содержимое пакетов, идущих из одной внутренней сети в другую;
- туннель должен позволять защищенное взаимодействие между платформами управления трафиком по их внутренним адресам;
- взаимодействие по внешним адресам должно происходить без применения туннеля и шифрования;
- трафик, идущий по туннелю между регионами по внутренним адресам, не должен транслироваться.

## Как делать



Для формирования защищенного канала связи между регионами есть множество решений, например, IPSec-туннели, SSL VPN и прочее. Как пример, можно настроить — GRE over IPSec.

GRE — это протокол, не предоставляющий шифрование, из чего следует, что соединение окажется небезопасным. В дальнейшем будет настроена технология IPSec, которая обеспечит приватность соединения.

Сначала необходимо создать GRE-туннель для обеспечения незащищенного соединения между регионами. Для его настройки на каждой машине создается скрипт конфигурирования туннеля по пути — /etc/gre.up.

### RTR-L

```
#!/bin/bash
ip tunnel add tun0 mode gre local 4.4.4.100 remote 5.5.5.100
ip addr add 10.5.5.1/30 dev tun0
ip link set up tun0
ip route add 172.16.100.0/24 via 10.5.5.2
~
```

### RTR-R

```
#!/bin/bash
ip tunnel add tun0 mode gre local 5.5.5.100 remote 4.4.4.100
ip addr add 10.5.5.2/30 dev tun0
ip link set up tun0
ip route add 192.168.100.0/24 via 10.5.5.1
~
```

## Описание применимых команд

ip tunnel add <имя\_интерфейса> — команда для создания туннеля;

mode gre — указываем режим инкапсуляции gre;

local — адрес источника, откуда будет происходить подключение;

remote — адрес назначения, куда будет происходить подключение;

ip addr add <адрес/маска\_подсети> dev <имя\_интерфейса> — команда для добавления IP-адреса на интерфейс;

ip link set up <имя\_интерфейса> — команда, включающая интерфейс;

ip route add <адрес\_сети\_региона/маска\_подсети> via <туннельный\_адрес\_роутера\_напротив> — команда для добавления маршрута в сеть другого региона, таким образом мы сразу же добавим в автонастройку подключение сетей двух регионов.

После того, как скрипты были написаны, необходимо дать им права на выполнение при помощи команды

```
chmod +x /etc/gre.up
```

Проверить корректность работы скриптов можно их выполнением при помощи команды /etc/gre.up — такой командой передается скрипт на выполнение операционной системой.

```
root@RTR-R:~# ./etc/gre.up
root@RTR-R:~#
```

В случае опечаток в написании скрипта на данном этапе система укажет на допущенные ошибки.

После этого необходимо добавить скрипт в автозагрузку. Для этого на RTR-R и RTR-L редактируется файл /etc/crontab и в конце добавляется строка @reboot root /etc/gre.up

```
GNU nano 5.4                               /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .---- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .-- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# | | | |
# * * * * * user-name command to be executed
17 *    * * *   root      cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root      test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root      test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root      test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
@reboot root /etc/gre.up
```

## Как проверить

После выполнения команды должен появиться туннельный интерфейс.

```
root@RTR-R:~# ip --br a
lo          UNKNOWN      127.0.0.1/8 ::1/128
ens32        UP          172.16.100.254/24 fe80::250:56ff:fe95:365/64
ens35        UP          5.5.5.100/24 fe80::20c:29ff:fee6:37e0/64
gre0@NONE   DOWN
gretap0@NONE DOWN
enspan0@NONE DOWN
tun0@NONE   UNKNOWN      10.5.5.2/30 fe80::200:5efe:505:564/64
root@RTR-R:~#
```

Также проверяется соединение в рамках туннеля с помощью утилиты ping.

```
root@RTR-R:~# ping 10.5.5.1
PING 10.5.5.1 (10.5.5.1) 56(84) bytes of data.
64 bytes from 10.5.5.1: icmp_seq=1 ttl=64 time=0.981 ms
64 bytes from 10.5.5.1: icmp_seq=2 ttl=64 time=0.687 ms
64 bytes from 10.5.5.1: icmp_seq=3 ttl=64 time=2.49 ms
64 bytes from 10.5.5.1: icmp_seq=4 ttl=64 time=1.38 ms
^C
--- 10.5.5.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.687/1.383/2.488/0.683 ms
root@RTR-R:~#
```

Для проверки пути трафика можно запустить сквозную трассировку от хоста WEB-L до WEB-R.

```
root@WEB-L:~# traceroute -n 172.16.100.100
traceroute to 172.16.100.100 (172.16.100.100), 30 hops max, 60 byte packets
 1  192.168.100.254  1.717 ms  1.679 ms  1.519 ms
 2  * * *
 3  172.16.100.100  6.593 ms  6.903 ms  6.922 ms
root@WEB-L:~# _
```

Незащищенное соединение между регионами настроено, осталось его защитить. Защита соединения производится при помощи стандарта IPSec. Стандарт IPSec в Debian 11 реализуется пакетом strongswan. В первую очередь необходимо установить данный пакет на RTR-R и RTR-L при помощи команды

```
apt install strongswan
```

Предварительно необходимо подключить DVD-3-образ в настройках машины и проповести установку с DVD (apt-cdrom add, потом apt update).

```
root@RTR-L:~# apt install strongswan
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libcharon-extauth-plugins libstrongswan libstrongswan-standard-plugins strongswan-charon
    strongswan-libcharon strongswan-starter
Suggested packages:
  libstrongswan-extra-plugins libcharon-extra-plugins
The following NEW packages will be installed:
  libcharon-extauth-plugins libstrongswan libstrongswan-standard-plugins strongswan
    strongswan-charon strongswan-libcharon strongswan-starter
0 upgraded, 7 newly installed, 0 to remove and 14 not upgraded.
Need to get 1,439 kB of archives.
After this operation, 4,084 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

После успешной установки пакета необходимо добавить конфигурацию в два основных конфигурационных файла: /etc/ipsec.conf и /etc/ipsec.secrets.

В файле /etc/ipsec.conf содержится основная информация о параметрах соединения, ниже представлены примеры на RTR-L и RTR-R:

```
config setup
    # strictcrlpolicy=yes
    # uniqueids = no

# Add connections here.

# Sample VPN connections

conn vpn
    auto=start
    type=tunnel
    authby=secret
    left=5.5.5.100
    right=4.4.4.100
    leftsubnet=0.0.0.0/0
    rightsubnet=0.0.0.0/0
    leftprotoport=gre
    rightprotoport=gre
    ike=aes128-sha256-modp3072
    esp=aes128-sha256
```

RTR-R

```
config setup
    # strictcrlpolicy=yes
    # uniqueids = no

# Add connections here.

# Sample VPN connections

conn vpn
    auto=start
    type=tunnel
    authby=secret
    left=4.4.4.100
    right=5.5.5.100
    leftsubnet=0.0.0.0/0
    rightsubnet=0.0.0.0/0
    leftprotoport=gre
    rightprotoport=gre
    ike=aes128-sha256-modp3072
    esp=aes128-sha256
```

RTR-L

conn vpn — создание соединения с именем vpn;

auto=start — запускать соединение автоматически при старте демона IPSec;

type=tunnel — указывает IPSec работать в туннельном режиме. Туннельный режим работы шифрует изначальный IP-пакет полностью и добавляет новый заголовок IP. Транспортный режим работы шифрует все, что выше уровня IP, а заголовок IP оставляет без изменений.

Грубо говоря, туннельный режим используется для того, чтобы связать две приватные сети через публичную, обеспечив при этом шифрование (что-то вроде безопасного GRE). Транспортный же актуален тогда, когда IP-связность уже достигнута, но трафик между узлами нужно шифровать;

authby=secret — указывает IPSec на аутентификацию по ключу из файла /etc/ipsec.secrets;

left — указывает локальный адрес (откуда подключаемся);

right — указывает удаленный адрес (куда подключаемся);

leftsubnet — локальные подсети, трафик из которых необходимо шифровать;

rightsubnet — удаленные подсети, трафик к которым необходимо шифровать;

leftprotoport — локальный транспортный протокол для шифрования;

rightprotoport — удаленный транспортный протокол для шифрования;

ike — параметры первой фазы IPSec;

esp — параметры второй фазы IPSec.

Файл /etc/ipsec.secrets на обоих хостах одинаковый.

```
# This file holds shared secrets or RSA private keys for authentication.

# RSA private key for this host, authenticating it to any other host
# which knows the public part.

4.4.4.100 5.5.5.100 : PSK "P@ssw0rd"
~  
~  
~
```

## **Комментарии к настройке**

Указываются два публичных IP-адреса, которые используются для создания туннеля.

Порядок их записи не важен. Далее разделитель в виде двоеточия.

PSK — Pre-Shared Key — в криптографии предварительный общий ключ — это общий секретный ключ, который принят между двумя сторонами, использующими некоторый защищенный канал, прежде чем его нужно зашифровать.

Далее указывается секретный пароль, он должен быть одинаковым для обеих сторон.

После того, как конфигурация написана, необходимо добавить в автозагрузку и запустить IPSec при помощи команды

```
systemctl enable --now ipsec
```

## **Как проверить**

Проверить работоспособность защищенного соединения можно при помощи команды **IPSec Status**. Если не показывает соединения, то запускаем IPSec Update, затем IPSec Restart — программа выдаст сообщение об ошибке синтаксиса в конфигах (строчку):

```
root@RTR-R:~# ipsec status
Security Associations (1 up, 0 connecting):
    vpn[17]: ESTABLISHED 45 minutes ago, 5.5.5.100[5.5.5.100]...4.4.4.100[4.4.4.100]
    vpn{65}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c5802c38_i c6e9b133_o
    vpn{65}:  0.0.0.0/0[gre] == 0.0.0.0/0[gre]
root@RTR-R:~# _
```

## **Краткая справка**

Справка IPSec (<https://wiki.debian.org/IPsec>).

Подробнее про IPSec (<https://linkmeup.gitbook.io/sdsm/7.-vpn/2.-ipsec>).

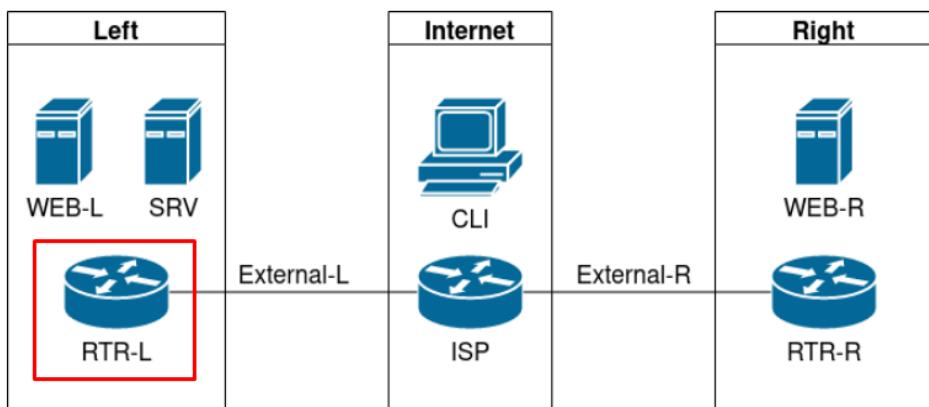
Документация разработчиков пакета StrongSwan (<https://wiki.strongswan.org/projects/strongswan/wiki/UserDocumentation>).

# НАСТРОЙКА СПИСКОВ КОНТРОЛЯ ДОСТУПА

**Задание 1.** Платформа управления трафиком RTR-L выполняет контроль входящего трафика согласно следующим правилам:

- разрешаются подключения к портам DNS, HTTP и HTTPS для всех К[к]лиентов;
- порты необходимы для работы настраиваемых служб;
- разрешается работа выбранного протокола организации защищенной связи;
- разрешение портов должно быть выполнено по принципу «необходимо и достаточно»;
- разрешается работа протокола ICMP;
- разрешается работа протокола SSH;
- прочие подключения запрещены;
- для обращений к платформам со стороны хостов, находящихся внутри регионов, ограничений быть не должно.

**Как делать**



Для настройки межсетевого экрана используется знакомый nftables. Внутри файла /etc/nftables.conf необходимо добавить новую таблицу записей table inet filter.

```
#!/usr/sbin/nft -f
flush ruleset

table inet filter {
    chain input {
        type filter hook input priority 0;
        udp dport 53 accept; #1
        tcp dport 80 accept; #2
        tcp dport 443 accept; #3
        ct state {established, related} accept; #4
        ip protocol gre accept; #5
        ip protocol icmp accept; #6
        udp dport 500 accept; #7
        ip saddr 192.168.100.0/24 accept; #8
        ip saddr 172.16.100.0/24 accept; #9
        ip version 4 drop; #10_
    }
    chain forward {
        type filter hook forward priority 0;
    }
    chain output {
        type filter hook output priority 0;
    }
}
table ip nat {
    chain postrouting {
        type nat hook postrouting priority 0;
        ip saddr 192.168.100.0/24 oifname ens35 counter masquerade;
    }
}
```

Стоит обратить внимание на то, что на скриншоте правил nftables присутствует нумерация правил, ссылки на них можно прочитать ниже:

- разрешает работу DNS (порт 53, зарегистрированный IANA);
- разрешает работу HTTP (порт 80, зарегистрированный IANA);
- разрешает работу HTTPS (порт 443, зарегистрированный IANA);
- отслеживание состояния соединений;
- разрешает работу GRE;
- разрешает работу ICMP;
- разрешает работу IPSec (порт 500, зарегистрированный IANA);
- разрешает обращение клиентов из офиса Left;
- разрешает обращение клиентов из офиса Right;
- запрещает весь прочий трафик по протоколу IPv4.

### Как проверить

После написания конфигурации необходимо применить правила при помощи команды `nft -f /etc/nftables.conf`.

Также можно использовать команду `nft list ruleset`, чтобы отобразить список всех текущих настроек.

```
root@RTR-L:~# nft list ruleset
table inet filter {
    chain input {
        type filter hook input priority filter; policy accept;
        udp dport 53 accept
        tcp dport 80 accept
        tcp dport 443 accept
        ct state { established, related } accept
        ip protocol gre accept
        ip protocol icmp accept
        udp dport 500 accept
        ip saddr 192.168.100.0/24 accept
        ip saddr 172.16.100.0/24 accept
        ip version 4 drop
    }

    chain forward {
        type filter hook forward priority filter; policy accept;
    }

    chain output {
        type filter hook output priority filter; policy accept;
    }
}
```

### Краткая справка

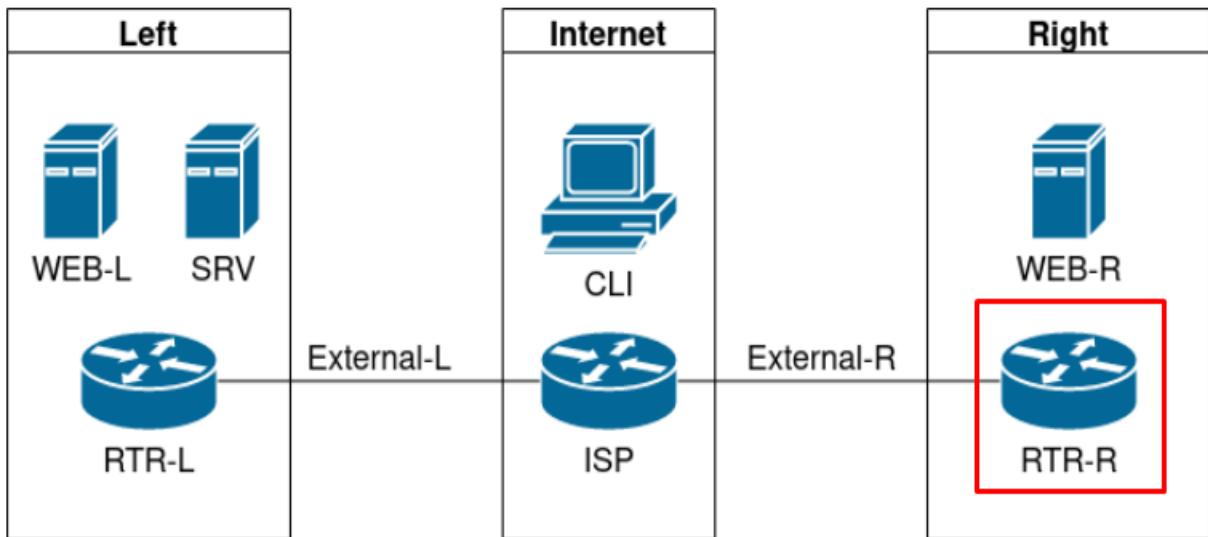
- справочник (<https://wiki.debian.org/nftables>);
- краткий справочник по NFTABLES (<https://habr.com/ru/company/ruvds/blog/580648>);
- официальная документация NFTABLES ([https://wiki.nftables.org/wiki-nftables/index.php/Main\\_Page](https://wiki.nftables.org/wiki-nftables/index.php/Main_Page)).

**Задание 2.** Платформа управления трафиком RTR-R выполняет контроль входящего трафика согласно следующим правилам:

- разрешаются подключения к портам HTTP и HTTPS для всех клиентов;
- порты необходимы для работы настраиваемых служб;
- разрешается работа выбранного протокола организации защищенной связи;
- разрешение портов должно быть выполнено по принципу «необходимо и достаточно»;
- разрешается работа протоколов ICMP;

- разрешается работа протокола SSH;
- прочие подключения запрещены;
- для обращений к платформам со стороны хостов, находящихся внутри регионов, ограничений быть не должно.

### Как делать



Для настройки межсетевого экрана используется nftables. В файле /etc/nftables.conf необходимо добавить новую таблицу записей table inet filter.

```
#!/usr/sbin/nft -f

flush ruleset

table inet filter {
    chain input {
        type filter hook input priority 0;
        tcp dport 80 accept; #1
        tcp dport 443 accept; #2
        ct state {established, related} accept; #3
        ip protocol gre accept; #4
        ip protocol icmp accept; #5
        udp dport 500 accept; #6
        ip saddr 192.168.100.0/24 accept; #7
        ip saddr 172.16.100.0/24 accept; #8
        ip version 4 drop; #9
    }
    chain forward {
        type filter hook forward priority 0;
    }
    chain output {
        type filter hook output priority 0;
    }
}
table ip nat {
    chain postrouting {
        type nat hook postrouting priority 0;
        ip saddr 192.168.100.0/24 oifname ens35 counter masquerade;
    }
}
```

Стоит обратить внимание, что на скриншоте правил nftables присутствует нумерация правил, ссылки на них можно прочитать ниже:

- разрешает работу HTTP (порт 80, зарегистрированный IANA);
- разрешает работу HTTPS (порт 443, зарегистрированный IANA);
- отслеживание состояния соединения;
- разрешает работу GRE;
- разрешает работу ICMP;
- разрешает работу IPSec (порт 500, зарегистрированный IANA);
- разрешает обращение клиентов из офиса Left;
- разрешает обращение клиентов из офиса Right;
- запрещает весь прочий трафик по протоколу IPv4.

После написания конфигурации необходимо применить правила при помощи команды `nft -f /etc/nftables.conf`

### Как проверить

Ввести команду — `nft list ruleset`.

```
root@centos-7: ~# nft list ruleset | more
table inet filter {
    chain input {
        type filter hook input priority filter; policy accept;
        tcp dport 80 accept
        tcp dport 443 accept
        ct state { established, related } accept
        ip protocol gre accept
        ip protocol icmp accept
        udp dport 500 accept
        ip saddr 192.168.100.0/24 accept
        ip saddr 172.16.100.0/24 accept
        ip version 4 drop
    }

    chain forward {
        type filter hook forward priority filter; policy accept;
    }

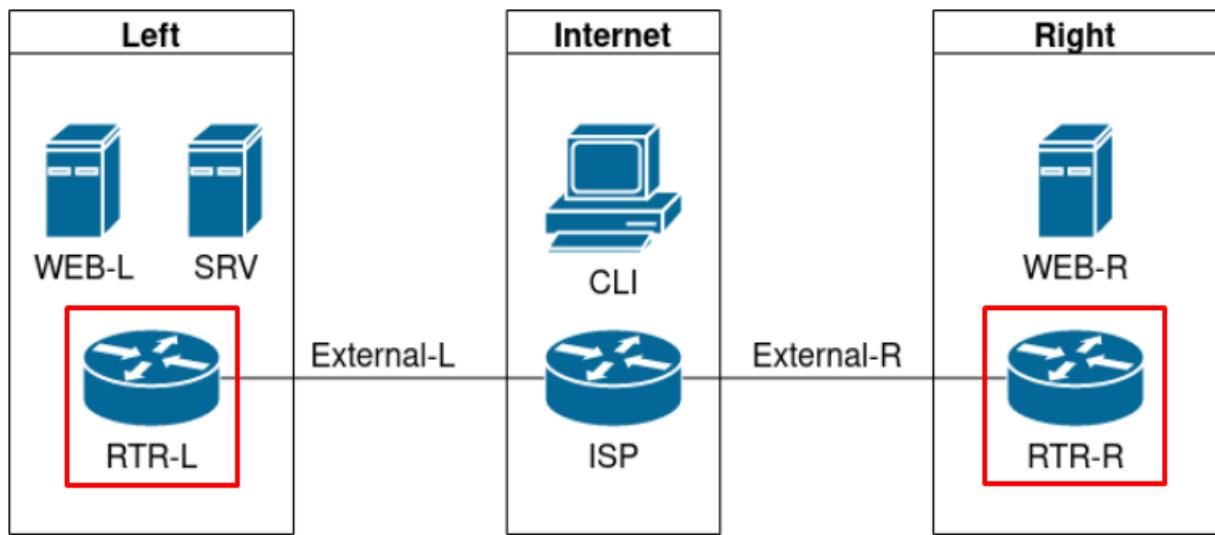
    chain output {
        type filter hook output priority filter; policy accept;
    }
}
```

# АДМИНИСТРИРОВАНИЕ ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ И ПРИНЯТИЕ МЕР ПО УСТРАНЕНИЮ ВОЗМОЖНЫХ СБОЕВ

**Задание 1.** Обеспечьте настройку службы SSH региона Left:

- подключения со стороны внешних сетей по протоколу к платформе управления трафиком RTR-L на порт 2222 должны быть перенаправлены на BM WEB-L;
- подключения со стороны внешних сетей по протоколу к платформе управления трафиком RTR-R на порт 2244 должны быть перенаправлены на BM WEB-R.

**Как делать**



Для настройки достаточно добавить правила в таблицы prerouting в nftables на машинах RTR-L и RTR-R. Необходимо открыть файл /etc/nftables.conf и настроить его согласно скриншоту.

```
ip saddr 192.168.100.624 accept
ip saddr 172.16.100.0/24 accept
tcp dport 2222 counter packets 0 bytes 0 #1
ip version 4 drop
}

chain forward {
    type filter hook forward priority filter; policy accept;
}

chain output {
    type filter hook output priority filter; policy accept;
}
}
table ip nat {
    chain postROUTING {
        type nat hook postROUTING priority filter; policy accept;
        ip saddr 192.168.100.0/24 oifname "ens224" counter packets 1948 bytes 140247 masquerade
    }
    chain prerouting #2
        type nat hook prerouting priority filter; policy accept;
        tcp dport 2222 dnat to 192.168.100.100:22 #2
}
}
```

RTR-L Описание введенных правил:

- открыть порт 2222;
- перенаправление трафика с порта 2222 на адрес 192.168.100.100 порт 22.

```

        ip saddr 172.16.100.0/24 accept
        tcp dport 2244 accept #1
        ip version 4 drop
    }

    chain forward {
        type filter hook forward priority filter; policy accept;
    }

    chain output {
        type filter hook output priority filter; policy accept;
    }

table ip nat {
    chain postROUTING {
        type nat hook postROUTING priority filter; policy accept;
        ip saddr 172.16.100.0/24 oifname "ens224" counter packets 1401 bytes 103142 masquerade
    }
}

chain prerouting {
    type nat hook prerouting priority filter; policy accept;
    tcp dport 2244 dnat to 172.16.100.100:22 #2
}

```

## RTR-R

Описание введенных правил:

- открыть порт 2244;
- перенаправление трафика с порта 2244 на адрес 172.16.100.100 порт 22.

### Как проверить

После написания конфигурации необходимо применить правила при помощи команды nft -f /etc/nftables.conf.

Для проверки выполняется подключение по SSH на данные порты. Предварительно на WEB-L и WEB-R необходимо выполнить команды

su - user

passwd

Затем необходимо ввести пароль (на свое усмотрение, в примере — resu) и повторить его ввод.

Подключение необходимо выполнять с внешнего клиента, пароль для user задан был выше.

```

root@ISP:~# ssh user@4.4.4.100 -p 2222
The authenticity of host '[4.4.4.100]:2222 ([4.4.4.100]:2222)' can't be established.
ECDSA key fingerprint is SHA256:K7INq9eRdgpbsUUKKxmJXHSfU6rVueVo+pzJYzg6FF4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[4.4.4.100]:2222' (ECDSA) to the list of known hosts.
user@4.4.4.100's password:
Linux WEB-L 5.10.0-9-amd64 #1 SMP Debian 5.10.70-1 (2021-09-30) x86_64

```

```

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

```

```

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
user@WEB-L:~$
```

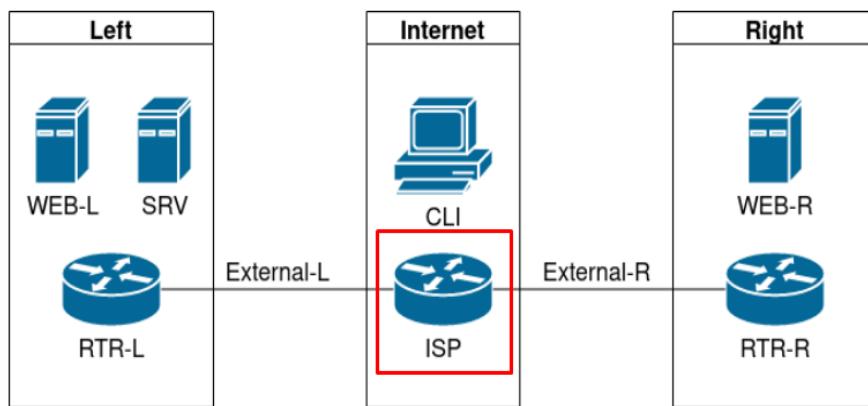
Для WEB-R команда изменится на ssh root@5.5.5.100-p2244.

# АДМИНИСТРИРОВАНИЕ СЕТЕВЫХ РЕСУРСОВ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

**Задание.** Выполните настройку первого уровня DNS-системы стенда:

- используется BM ISP;
- обслуживается зона demo.wsr;
- наполнение зоны должно быть реализовано в соответствии с таблицей 2;
- сервер делегирует зону int.demo.wsr на SRV;
- поскольку SRV находится во внутренней сети западного региона, делегирование происходит на внешний адрес маршрутизатора данного региона;
- маршрутизатор региона должен транслировать соответствующие порты DNS-службы в порты сервера SRV;
- внешний клиент CLI должен использовать DNS-службу, развернутую на ISP, по умолчанию.

## Как делать



В качестве DNS-сервера используем BIND. Необходимо установить его на ISP при помощи команды

```
apt install bind9
```

Предварительно необходимо подключить DVD-2 образ в настройках машины и произвести установку с DVD (apt-cdrom add, потом apt update).

После успешной установки необходимо отредактировать конфигурационные файлы.

Выполняется конфигурация файла `/etc/bind/named.conf.options` согласно скриншоту

```
options {  
    directory "/var/cache/bind";  
  
    // If there is a firewall between you and nameservers you want  
    // to talk to, you may need to fix the firewall to allow multiple  
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113  
  
    // If your ISP provided one or more IP addresses for stable  
    // nameservers, you probably want to use them as forwarders.  
    // Uncomment the following block, and insert the addresses replacing  
    // the all-0's placeholder.  
  
    forwarders {  
        8.8.8.8; #1  
    };  
  
    //================================================================= //  
    // If BIND logs error messages about the root key being expired,  
    // you will need to update your keys. See https://www.isc.org/bind-keys  
    //=================================================================  
    dnssec-validation no; #2  
    allow-query {any;}; #3  
    recursion yes; #4  
    listen-on { any; }; #5  
};
```

## Описание измененных параметров в конфигурационном файле

- пересылка запросов на внешние DNS-сервера для доступа к локальным репозиториям или репозиториям в Интернете. Стоит обратить внимание на то, что конструкция forwarders по умолчанию вся закомментирована, необходимо убрать // перед конфигурированием этого параметра;
- отключить DNSSec;
- разрешить запросы от всех клиентов;
- разрешить рекурсивные запросы;
- слушать на всех интерфейсах.

Выполняется конфигурация файла `/etc/bind/named.conf.default-zones` согласно скриншоту

```
// prime the server with knowledge of the root servers
zone "." {
    type hint;
    file "/usr/share/dns/root.hints";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
    type master;
    file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
    type master;
    file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
    type master;
    file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
    type master;
    file "/etc/bind/db.255";
};

zone "demo.wsr" {
    type master;
    file "/etc/bind/demo.wsr";
    forwarders {};
};

~  
~  
"/etc/bind/named.conf.default-zones" 34L, 576B
```

## Разбор конфигурации

zone “demo.wsr” { — описание зоны, которая контролируется нашим сервером;  
type master; — указание типа зоны. Master — указывает на то, что наш сервер — основной владелец зоны и имеет право редактировать ее;  
file “/etc/bind/demo.wsr”; — файл зоны, где хранятся все записи зоны demo.wsr;  
forwarders {} ; — отключение пересылки для зоны необходимо для нормальной работы делегирования  
};

Для создания шаблона зоны demo.wsr необходимо перейти в каталог /etc/bind и скопировать файл db.local в /etc/bind с названием demo.wsr. Сделать это можно при помощи команды

```
cd /etc/bind; cp db.local demo.wsr
```

```
root@ISP:~# cd /etc/bind; cp db.local demo.wsr;
root@ISP:/etc/bind# ls
bind.keys  db.255      demo.wsr          named.conf.local    zones.rfc1918
db.0        db.empty   named.conf        named.conf.options
db.127      db.local   named.conf.default-zones rndc.key
root@ISP:/etc/bind# _
```

Далее необходимо открыть файл с помощью любого текстового редактора demo.wsr и сформировать таблицу DNS-имен.

```
;
; BIND data file for demo.wsr_interface
;
$TTL     86400
$ORIGIN demo.wsr.
@       IN      SOA    demo.wsr. root.demo.wsr. (
                        1           ; Serial
                        604800      ; Refresh
                        86400       ; Retry
                        2419200    ; Expire
                        86400 )     ; Negative Cache TTL
;
@       IN      NS     demo.wsr.
@       IN      A      3.3.3.1
isp     IN      A      3.3.3.1
www     IN      A      4.4.4.100
www     IN      A      5.5.5.100
internet      IN      CNAME   isp

$ORIGIN int.demo.wsr.
@       IN      NS     int.demo.wsr.
@       IN      A      4.4.4.100
```

После того, как файл зоны сформирован, необходимо выполнить проверку конфигурации, проверку файла зоны и перезапустить bind9.

### Как проверить

Проверки выполняются при помощи команд named-checkconf и named-checkconf-z соответственно.

В случае, если в выводе команд named-checkconf отображается результат, похожий на то, что можно увидеть в скриншотах ниже, значит, синтаксических ошибок в конфигурации зон нет.

```
root@ISP:/etc/bind# named-checkconf
root@ISP:/etc/bind# named-checkconf -z
zone localhost/IN: loaded serial 2
zone 127.in-addr.arpa/IN: loaded serial 1
zone 0.in-addr.arpa/IN: loaded serial 1
zone 255.in-addr.arpa/IN: loaded serial 1
zone demo.wsr/IN: loaded serial 2
root@ISP:/etc/bind#
```

После этого выполняется перезагрузка сервера DNS, для загрузки сервиса — **systemctl restart bind9**.

```
root@ISP:/etc/bind# systemctl restart bind9
root@ISP:/etc/bind# _
```

Выполнить практическую проверку можно при помощи утилиты host, поставляемой в пакете dnsutils

```
host <запрашиваемый_ресурс> <ip_адрес_сервера_для_опроса>
root@WEB-L:~# host demo.wsr 3.3.3.1
Using domain server:
Name: 3.3.3.1
Address: 3.3.3.1#53
Aliases:

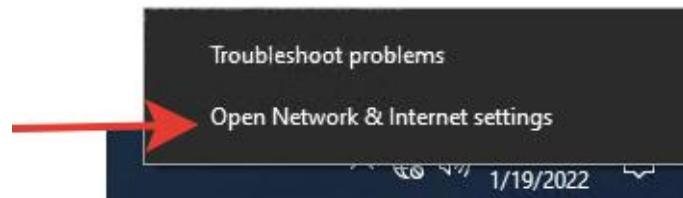
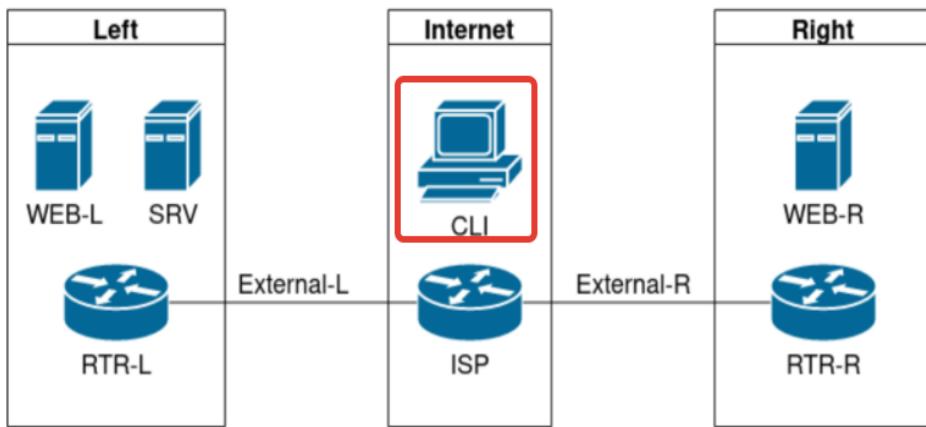
demo.wsr has address 3.3.3.1
root@WEB-L:~# host isp.demo.wsr 3.3.3.1
Using domain server:
Name: 3.3.3.1
Address: 3.3.3.1#53
Aliases:

isp.demo.wsr has address 3.3.3.1
root@WEB-L:~# host www.demo.wsr 3.3.3.1
Using domain server:
Name: 3.3.3.1
Address: 3.3.3.1#53
Aliases:

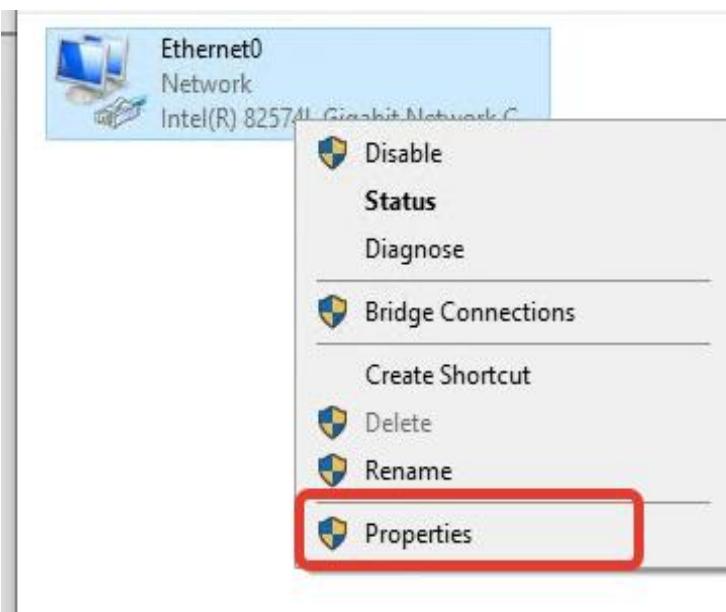
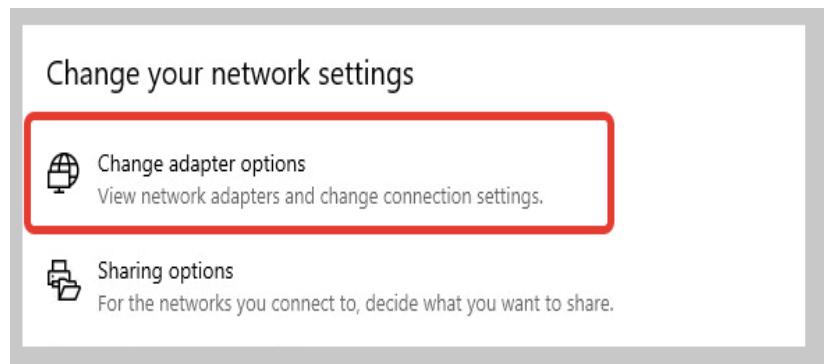
www.demo.wsr has address 4.4.4.100
www.demo.wsr has address 5.5.5.100
root@WEB-L:~# host internet.demo.wsr 3.3.3.1
Using domain server:
Name: 3.3.3.1
Address: 3.3.3.1#53
Aliases:

internet.demo.wsr is an alias for isp.demo.wsr.
isp.demo.wsr has address 3.3.3.1
root@WEB-L:~# _
```

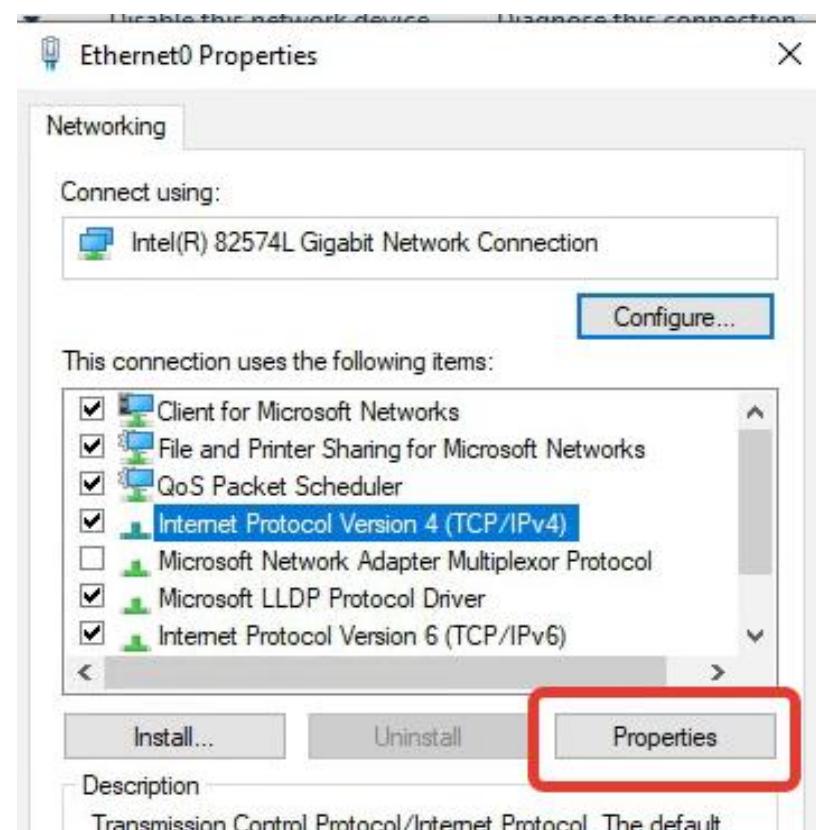
Если проверки прошли успешно — на внешнем клиенте необходимо настроить адрес DNS сервера ISP. Удаленная машина CLI имеет операционную систему Windows 10. Дальнейшая конфигурация производится на компьютере CLI.



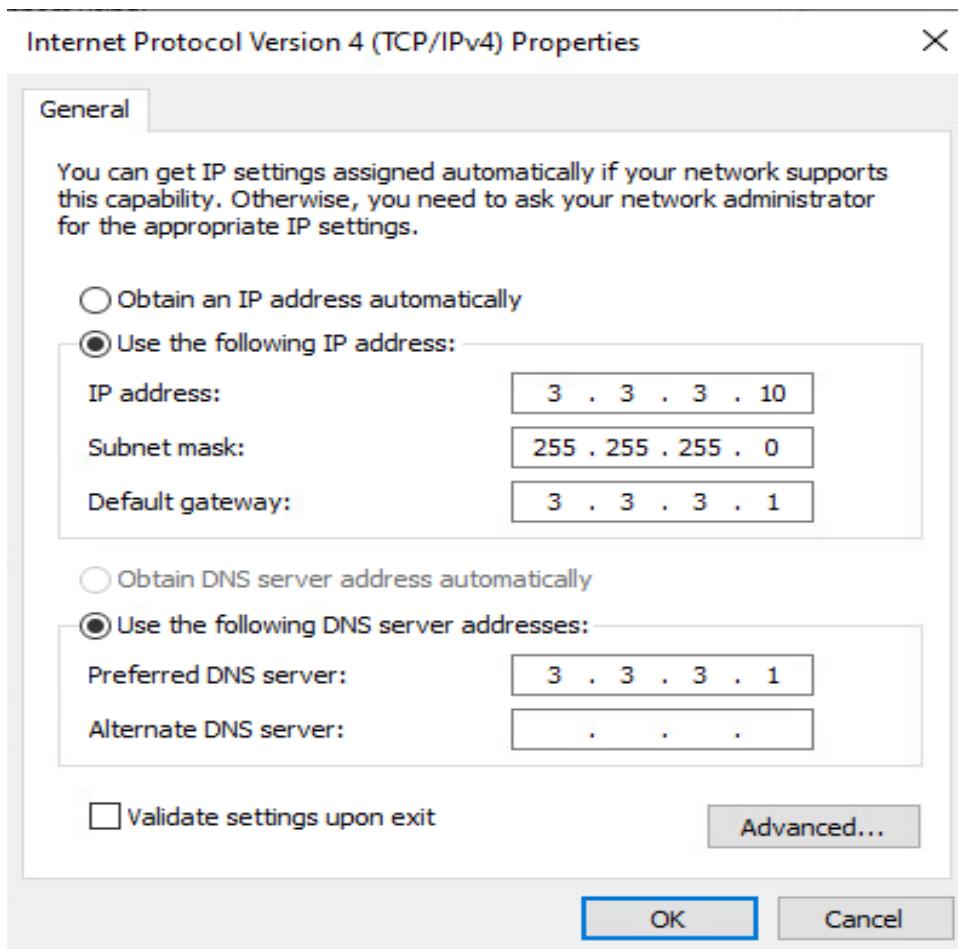
Правой кнопкой мыши необходимо открыть настройки сети. Далее в меню нужно открыть параметр Change Adapter Options.

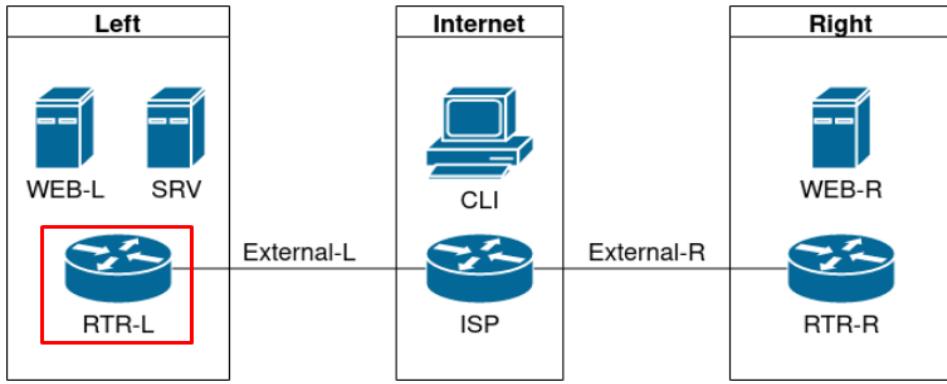


Правой кнопкой мыши необходимо открыть свойства сетевого адаптера, далее — Internet Protocol Version 4 и его свойства.



Необходимо настроить сетевые реквизиты машины CLI в соответствии со схемой сети.





Также необходимо добавить правило для трансляции портов на RTR-L. В данный момент работоспособность зоны int.demo.wsr не проверяется, так как данная зона не сконфигурирована. Внутри файла /etc/nftables.conf необходимо произвести настройку согласно скриншоту ниже.

```
table ip nat {
    chain postrouting {
        type nat hook postrouting priority 0;
        ip saddr 192.168.100.0/24 oifname ens192 counter masquerade;
    }
    chain prerouting {
        type nat hook prerouting priority filter; policy accept;
        tcp dport 2222 dnat to 192.168.100.100:22;
        udp dport 53 dnat to 192.168.100.200:53; #new
    }
}
```

#new — строчка указывает на переброс всех запросов на 53-й порт внешнего адреса RTR-L на сервер 192.168.100.200:53.

#### Дополнительная информация

Прямые зоны служат для преобразования имен узлов в IP-адреса. Наиболее часто используются для этого записи: A, CNAME, SRV.

Для определения имени узла по его IP-адресу служат обратные зоны, основной тип записи в обратных зонах — PTR. Для решения данной задачи создан специальный домен с именем in-addr.arpa. Для каждой IP-сети в таком домене создаются соответствующие поддомены, образованные из идентификатора сети, записанного в обратном порядке. Например, для сети 192.168.0.0/24 необходимо создать зону с именем 0.168.192.in-addr.arpa. Для узла с адресом 192.168.0.10 и именем example.ru в данной зоне должна быть создана запись 10 PTR example.ru.

В задании использовались обратные зоны 16.172.in-addr.arpa и 16.192.in-addr.arpa (для сетей 172.16.0.0/16 и 192.168.0.0/16 соответственно). Но возникает вопрос — ведь таких сетей в задании нет. Все очень просто. Для того чтобы не создавать зоны для каждой подсети, а их 5 шт., просто используют «вышестоящую сеть», так как сеть 172.16.x.0/24 является подсетью 172.16.0.0/16, и, соответственно, сеть 192.168.x.0/24 является подсетью 192.168.0.0/16.

#### Краткая справка

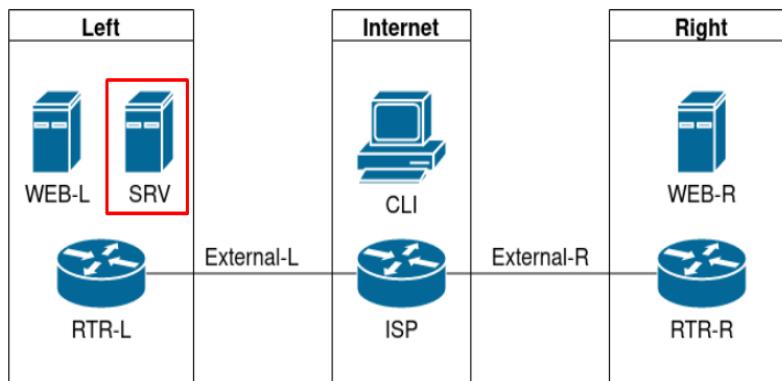
- подробнее про BIND (<https://wiki.debian.org/Bind9>);
- обширная документация по BIND от разработчиков (<https://downloads.isc.org/isc/bind9/9.17.1/doc/arm/Bv9ARM.pdf>).

#### Задание 2. Выполните настройку второго уровня DNS-системы стенда:

- используется BM SRV;
- обслуживается зона int.demo.wsr;
- наполнение зоны должно быть реализовано в соответствии с таблицей 2;
- обслуживаются обратные зоны для внутренних адресов регионов;
- имена для разрешения обратных записей следует брать из таблицы 2;
- сервер принимает рекурсивные запросы, исходящие от адресов внутренних регионов;

- обслуживание клиентов (внешних и внутренних), обращающихся к зоне int.demo.wsr, должно производиться без каких-либо ограничений по адресу источника;
- внутренние хосты регионов (равно как и платформы управления трафиком) должны использовать данную DNS-службу для разрешения всех запросов имен.

### Как делать



В качестве DNS-сервера необходимо использовать ПО bind9. Для начала необходимо установить bind9 на SRV с использованием команды

```
apt install bind9
```

Установка пакетов происходит по аналогии с установкой на ISP.

После установки необходимо отредактировать конфигурационные файлы.

Сначала необходимо открыть файл /etc/bind/named.conf.options.

```
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        3.3.3.1; #1
    };

    //========================================================================
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.isc.org/bind-keys
    //================================================================
    dnssec-validation no; #2
    listen-on { any; }; #3
    recursion yes; #4
    allow-query {any;}; #5
    allow-recursion { 172.16.100.0/24; 192.168.100.0/24; }; #6
};
```

Стоит обратить внимание на цифровые указания на скриншоте, их описание представлено ниже:

- пересылка всех неизвестных запросов на ISP;
- отключение DNSSEC;
- слушать на всех интерфейсах;
- принимать рекурсивные запросы;
- принимать запросы от всех;
- рекурсивные запросы принимаются только из внутренних сетей регионов.

После этого необходимо открыть файл /etc/bind/named.conf.default-zones и создать там три зоны, пример на скриншоте:

```
zone "int.demo.wsr" {
    type master;
    file "/etc/bind/int.demo.wsr";
};

zone "100.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/left.reverse";
};

zone "100.16.172.in-addr.arpa" {
    type master;
    file "/etc/bind/right.reverse";
};
```

Пояснения по поводу правил описания зон указаны выше. Проясним, что конкретно создается в данном пункте задания:

int.demo.wsr — внутренняя зона для прямого обслуживания;

100.168.192.in-addr.arpa — обратная зона для региона Left;

100.16.172.in-addr.arpa — обратная зона для региона Right.

Далее необходимо перейти в директорию /etc/bind/ и создать шаблоны для трех зон, необходимо именовать их так же, как описание зон в конфигурационных файлах /etc/bind/named.conf.default-zones.

```
root@SRV:~# cd /etc/bind
root@SRV:/etc/bind# cp db.local int.demo.wsr
root@SRV:/etc/bind# cp db.local left.reverse
root@SRV:/etc/bind# cp db.local right.reverse
root@SRV:/etc/bind# ls
bind.keys  db.255  int.demo.wsr  named.conf.default-zones  right.reverse
db.0        db.empty  left.reverse  named.conf.local      rndc.key
db.127      db.local   named.conf   named.conf.options    zones.rfc1918
root@SRV:/etc/bind#
```

Сначала нужно заполнить прямую зону — int.demo.wsr.

```
; BIND data file for int.demo.wsr interface
;
$TTL    604800
@       IN      SOA     int.demo.wsr. root.int.demo.wsr. (
                        2           ; Serial
                        604800      ; Refresh
                        86400       ; Retry
                        2419200     ; Expire
                        604800 )     ; Negative Cache TTL
;
@       IN      NS      int.demo.wsr.
@       IN      A       192.168.100.200
web-1   IN      A       192.168.100.100
web-r   IN      A       172.16.100.100
srv     IN      A       192.168.100.200
rtr-1   IN      A       192.168.100.254
rtr-r   IN      A       172.16.100.254
ntp     IN      CNAME   srv
dns    IN      CNAME   srv
webapp IN      CNAME   web-1

root@SRV:~# vim /etc/bind/int.demo.wsr
```

После этого нужно заполнить обратную зону для подсети LEFT — 100.168.192.in-addr.arpa.

```
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     100.168.192.in-addr.arpa. root.100.168.192.in-addr.arpa. (
                      2           ; Serial
                      604800      ; Refresh
                      86400       ; Retry
                     2419200     ; Expire
                     604800 )    ; Negative Cache TTL
;
@       IN      NS      int.demo.wsr.
@       IN      A       192.168.100.200
100    PTR     web-1.int.demo.wsr.
200    PTR     srv.int.demo.wsr.
254    PTR     rtr-1.int.demo.wsr.
~
```

А также обратную зону для подсети RIGHT — 100.16.172.in-addr.arpa.

```
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     100.16.172.in-addr.arpa. root.100.16.172.in-addr.arpa. (
                      2           ; Serial
                      604800      ; Refresh
                      86400       ; Retry
                     2419200     ; Expire
                     604800 )    ; Negative Cache TTL
;
@       IN      NS      int.demo.wsr.
@       IN      A       192.168.100.200
100    PTR     web-r.int.demo.wsr.
254    PTR     rtr-r.int.demo.wsr.
~
```

После того, как заполнение файлов зон закончено, можно проверить конфигурационные файлы и перезапустить bind9:

named-checkconf — проверка конфигурационных файлов;  
namec-checkconf -z — проверка файлов зон.

```
root@SRV:/etc/bind# named-checkconf
root@SRV:/etc/bind# named-checkconf -z
zone localhost/IN: loaded serial 2
zone 127.in-addr.arpa/IN: loaded serial 1
zone 0.in-addr.arpa/IN: loaded serial 1
zone 255.in-addr.arpa/IN: loaded serial 1
zone int.demo.wsr/IN: loaded serial 2
zone 100.168.192.in-addr.arpa/IN: loaded serial 2
zone 100.16.172.in-addr.arpa/IN: loaded serial 2
root@SRV:/etc/bind# systemctl restart bind9
root@SRV:/etc/bind# _
```

Проверку можно произвести при помощи утилиты host:  
host <запрашиваемый\_ресурс> <ip\_адрес\_сервера\_для\_опроса>

```

root@SRV:/etc/bind# host int.demo.wsr 192.168.100.200
Using domain server:
Name: 192.168.100.200
Address: 192.168.100.200#53
Aliases:

int.demo.wsr has address 192.168.100.200
root@SRV:/etc/bind# host web-1.int.demo.wsr 192.168.100.200
Using domain server:
Name: 192.168.100.200
Address: 192.168.100.200#53
Aliases:

web-1.int.demo.wsr has address 192.168.100.100
root@SRV:/etc/bind# host web-r.int.demo.wsr 192.168.100.200
Using domain server:
Name: 192.168.100.200
Address: 192.168.100.200#53
Aliases:

web-r.int.demo.wsr has address 172.16.100.100
root@SRV:/etc/bind# host srv.int.demo.wsr 192.168.100.200
Using domain server:
Name: 192.168.100.200
Address: 192.168.100.200#53
Aliases:

srv.int.demo.wsr has address 192.168.100.200
root@SRV:/etc/bind# host ntp.int.demo.wsr 192.168.100.200
Using domain server:
Name: 192.168.100.200
Address: 192.168.100.200#53
Aliases:

ntp.int.demo.wsr is an alias for srv.int.demo.wsr.
srv.int.demo.wsr has address 192.168.100.200
root@SRV:/etc/bind# _

```

Так же заполняем и обратные зоны:

`host <запрашиваемый_рекурс> <ip_адрес_сервера_для_опроса>`

```

root@SRV:/etc/bind# host 192.168.100.200 192.168.100.200
Using domain server:
Name: 192.168.100.200
Address: 192.168.100.200#53
Aliases:

200.100.168.192.in-addr.arpa domain name pointer srv.int.demo.wsr.
root@SRV:/etc/bind# host 192.168.100.100 192.168.100.200
Using domain server:
Name: 192.168.100.200
Address: 192.168.100.200#53
Aliases:

100.100.168.192.in-addr.arpa domain name pointer web-1.int.demo.wsr.
root@SRV:/etc/bind# host 172.16.100.100 192.168.100.200
Using domain server:
Name: 192.168.100.200
Address: 192.168.100.200#53
Aliases:

100.100.16.172.in-addr.arpa domain name pointer web-r.int.demo.wsr.
root@SRV:/etc/bind# _

```

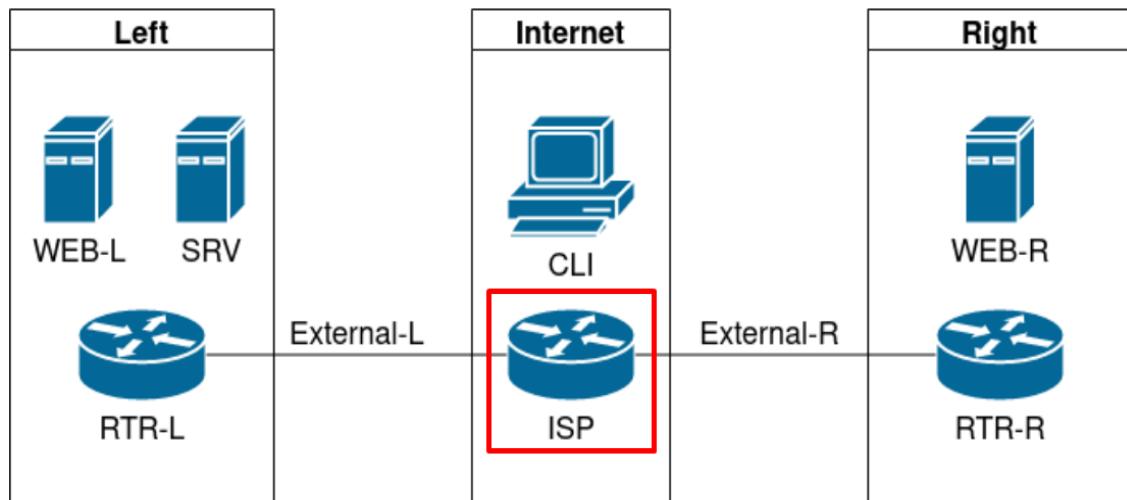
Также можно выполнить проверку с внешнего клиента:  
nslookup <запрашиваемый\_ресурс> <ip\_адрес\_сервера\_для\_опроса>

```
Command Prompt  
Microsoft Windows [Version 10.0.19044.1645]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\User>nslookup web-1.int.demo.wsr 3.3.3.1  
Server: UnKnown  
Address: 3.3.3.1  
  
Non-authoritative answer:  
Name: web-1.int.demo.wsr  
Address: 192.168.100.100  
  
C:\Users\User>
```

**Задание 3.** Выполните настройку первого уровня системы синхронизации времени:

- используется сервер ISP;
- сервер считает собственный источник времени верным, stratum = 4;
- сервер допускает подключение только через внешний адрес;
- соответствующей платформы управления трафиком;
- подразумевается обращение SRV для синхронизации времени;
- клиент CLI должен использовать службу времени ISP.

**Как делать**



NTP — сетевой протокол для синхронизации внутренних часов компьютера с использованием серверов времени. Для реализации NTP-сервера используется ПО chrony. Chrony необходимо установить при помощи команды

```
apt install chrony
```

Предварительно необходимо подключить DVD-2-образ в настройках машины и произвести установку с DVD (apt-cdrom add, потом apt update).

После установки необходимо открыть конфигурационный файл /etc/chrony/chrony.conf и добавить в него следующую конфигурацию.

```
server 127.127.1.0 #1
allow 5.5.5.0/24 #2
allow 4.4.4.0/24 #3
allow 3.3.3.0/24 #4
local stratum 4 #5
```

1 — в качестве источника времени использовать localhost;  
2–4 — указать, устройства с каких подсетей имеют возможность синхронизироваться с сервером;

5 — указать стратум (*англ. stratum*), т.е. слой. NTP использует иерархическую сеть, где каждый уровень имеет свой номер, называемый слоем. Слой 1 — первичные серверы, непосредственно синхронизирующиеся с национальными службами времени через спутник, радио или телефонный modem. Слой 2 — вторичные серверы, синхронизирующиеся с первичными серверами, и т. д. Как правило, клиенты и серверы NTP с относительно небольшим числом клиентов не синхронизируются с первичными серверами.

После изменения конфигурации необходимо перезапустить chrony при помощи команды

```
systemctl restart chronyd
```

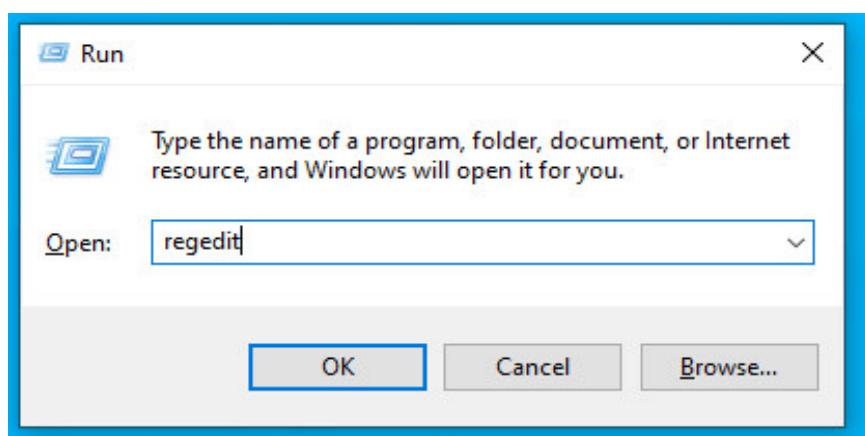
#### Как проверить

На ISP используется команда Chronyc Sources — она укажет на сервера, к которым подключился сконфигурированный сервер времени ISP.

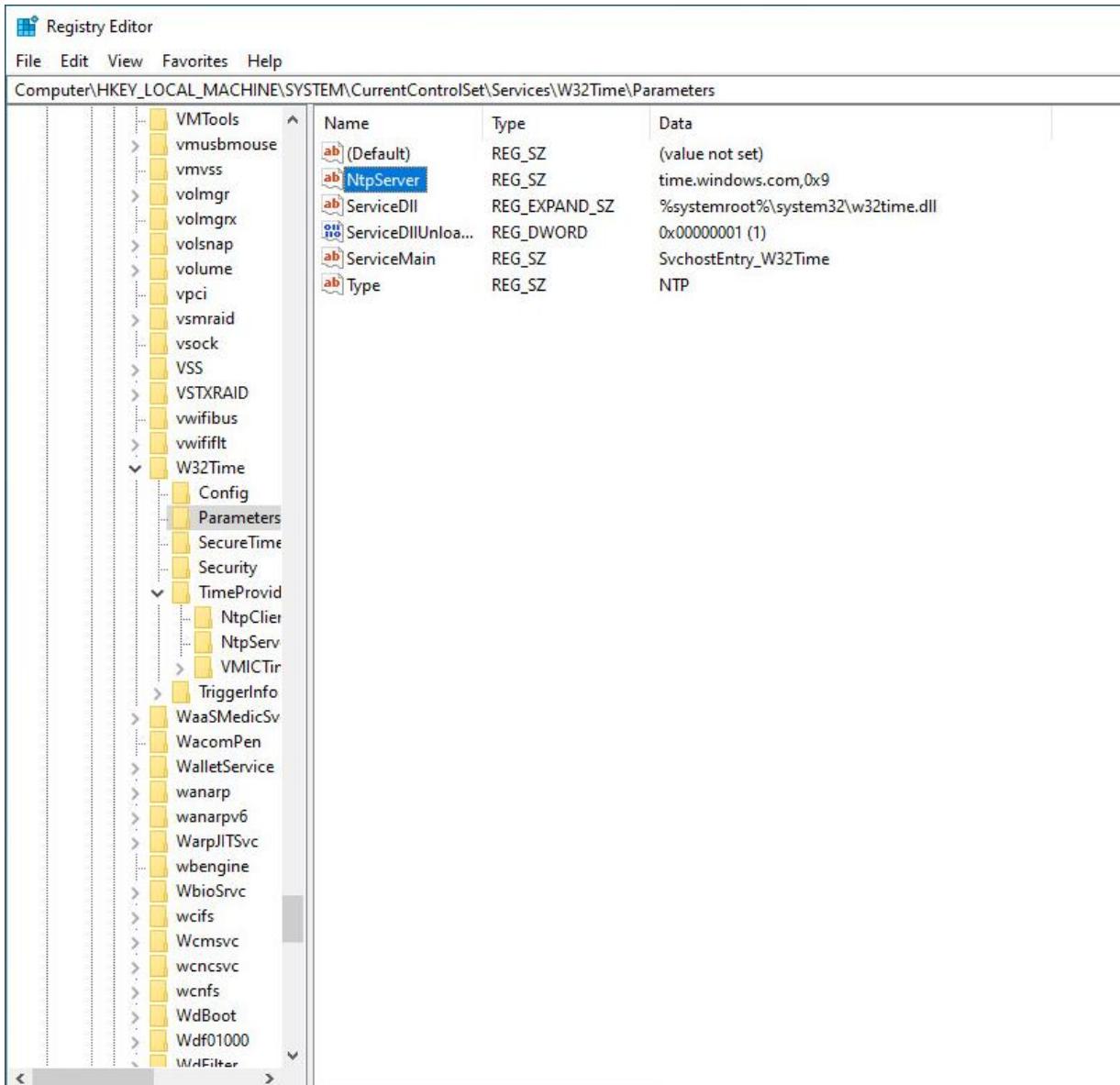
```
root@ISP:/# chronyc sources
MS Name/IP address          Stratum Poll Reach LastRx Last sample
=====
^? 127.127.1.0              0    6    0    -    +0ns[  +0ns] +/-    0ns
root@ISP:/#
```

После завершения настройки NTP-сервера необходимо подключить NTP клиентов. В качестве клиента выступает машина CLI.

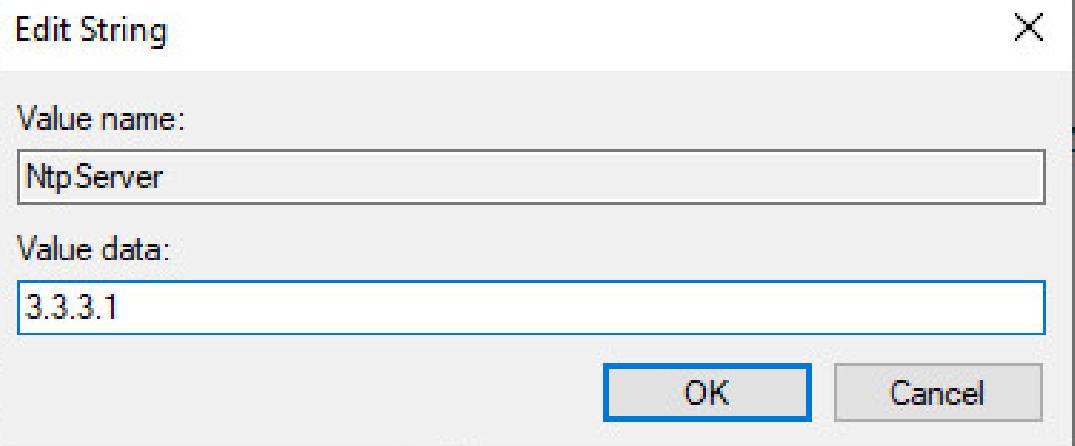
В первую очередь необходимо выполнить команду regedit при помощи утилиты Run, вызвать её можно нажатием клавиш (Win + R).



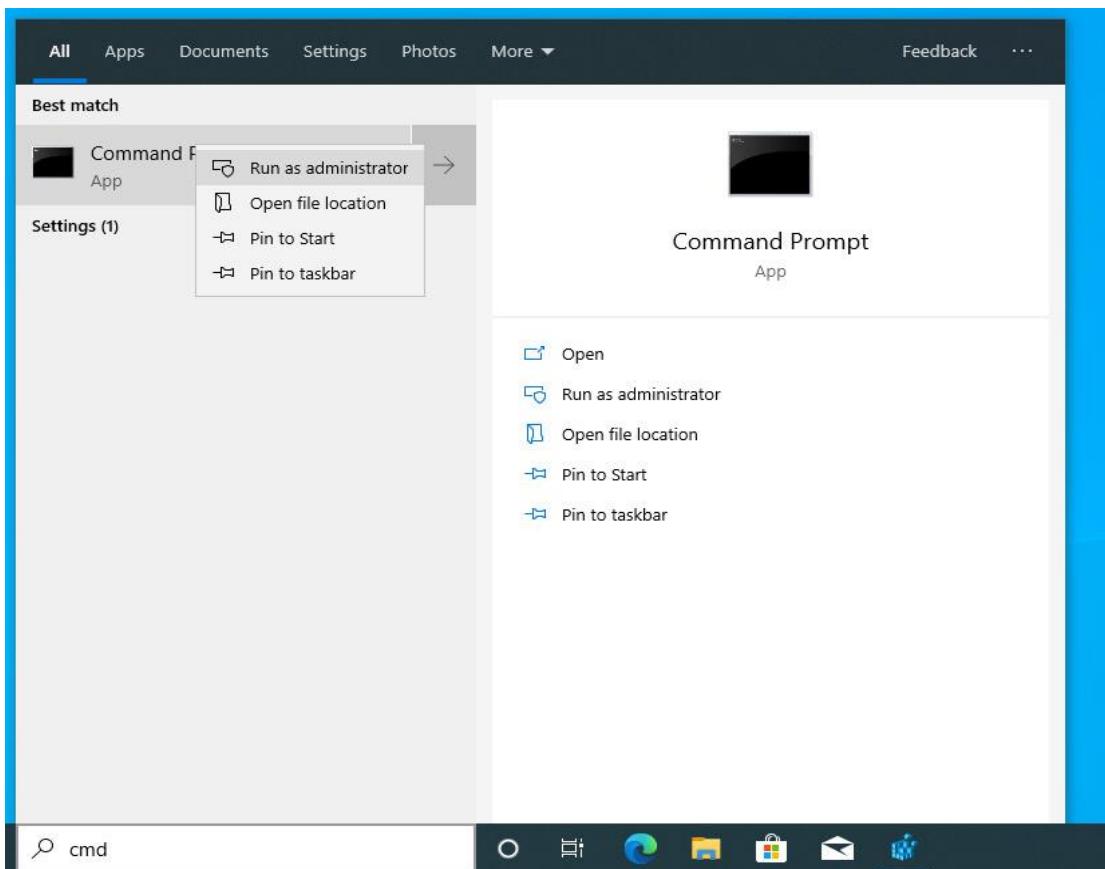
В открывшемся окне редактора реестра необходимо перейти по пути HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters и найти ключ NtpServer.



Необходимо изменить поле NtpServer, указав в качестве значения адрес сервера ISP.



После внесения изменения в реестр необходимо перезапустить сервис w32time. Сделать это можно из командной строки, запустив ее от имени администратора.



В командной строке введем команды по перезагрузке сервиса времени w32time:  
net stop w32time — отключаем сервис w32time;  
net start w32time — включаем сервис w32time.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.18363.418]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net stop w32time
The Windows Time service is stopping.
The Windows Time service was stopped successfully.

C:\Windows\system32>net start w32time
The Windows Time service is starting.
The Windows Time service was started successfully.

C:\Windows\system32>
```

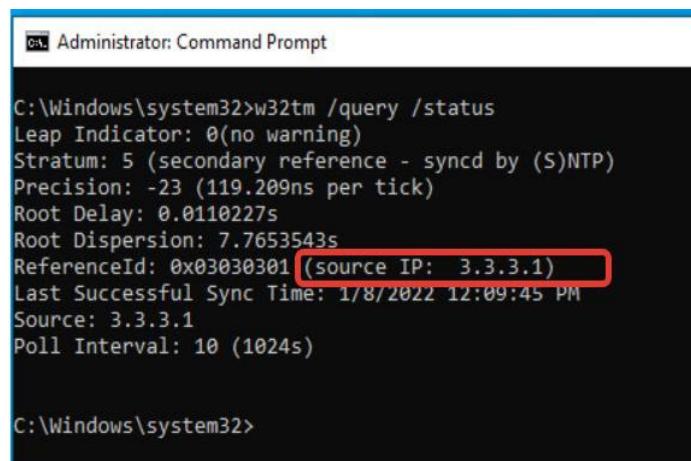
После перезапуска сервера необходимо выполнить команду `w32tm /resync /rediscover` для синхронизации с новым NTP-сервером.

```
Administrator: Command Prompt

C:\Windows\system32>w32tm /resync /rediscover
Sending resync command to local computer
The command completed successfully.

C:\Windows\system32>
```

Далее можно выполнить проверку состояния синхронизации при помощи команды w32tm /query /status

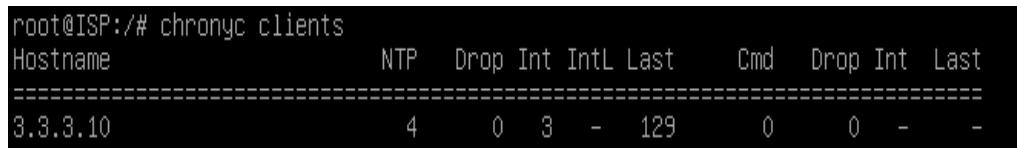


```
C:\Windows\system32>w32tm /query /status
Leap Indicator: 0(no warning)
Stratum: 5 (secondary reference - syncd by (S)NTP)
Precision: -23 (119.209ns per tick)
Root Delay: 0.0110227s
Root Dispersion: 7.7653543s
ReferenceId: 0x03030301 (source IP: 3.3.3.1)
Last Successful Sync Time: 1/8/2022 12:09:45 PM
Source: 3.3.3.1
Poll Interval: 10 (1024s)

C:\Windows\system32>
```

Обратите внимание, что в поле SOURCE IP указан адрес того сервера времени, к которому подключилась машина CLI.

На сервере времени ISP можно ввести команду **chronyc clients**:



Hostname	NTP	Drop	Int	IntL	Last	Cmd	Drop	Int	Last
3.3.3.10	4	0	3	-	129	0	0	-	-

Сервер укажет всех клиентов, среди них виден CLI с адресом 3.3.3.100.

#### Краткая справка

– установка NTP ([https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/6/html/deployment\\_guide/sect-date\\_and\\_time\\_configuration-command\\_line\\_configuration-network\\_time\\_protocol](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/deployment_guide/sect-date_and_time_configuration-command_line_configuration-network_time_protocol));

- крупнейший сайт-агрегатор серверов времени в России (<https://www.ntp-servers.net>);
- сайт протокола NTP (<http://www.ntp.org>).

#### Задание 4. Реализуйте файловый SMB-сервер на базе SRV.

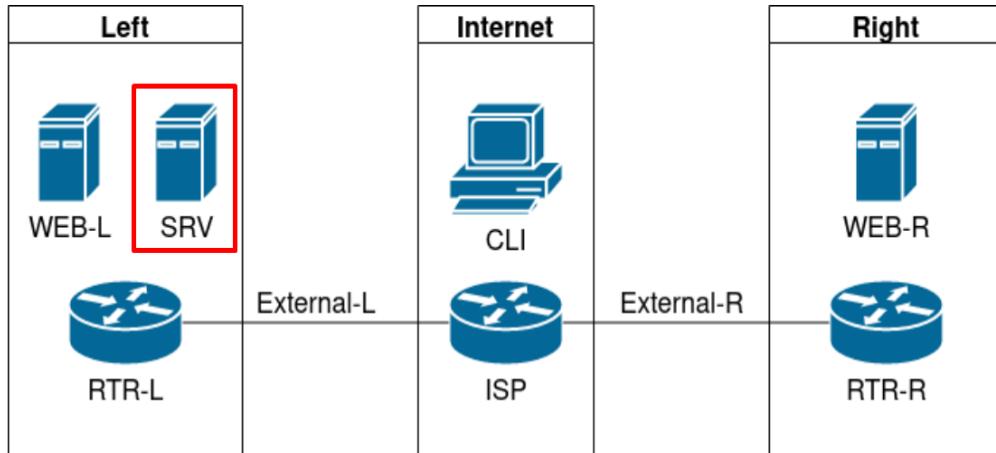
Сервер должен предоставлять доступ для обмена файлами серверам WEB-L и WEB-R.

Сервер, в зависимости от ОС, использует следующие каталоги для хранения файлов:

- /mnt/storage для системы на базе Linux;
- Диск R:\ для систем на базе Windows.

Хранение файлов осуществляется на диске (смонтированном по указанным выше адресам), реализованном по технологии RAID типа «Зеркало».

#### Как делать

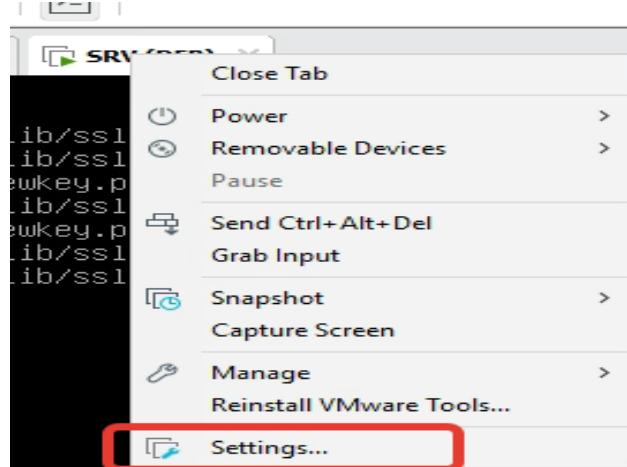


RAID — технология виртуализации данных для объединения нескольких физических дисковых устройств в логический модуль для повышения отказоустойчивости и (или) производительности. Существует множество реализаций RAID, как правило, выделяется 7 (от 0 до 6) основных базовых уровней RAID, остальные реализации считаются комбинированными. В рамках выполнения задания нам необходимо настроить RAID «Зеркало» или RAID1. Это делается при помощи утилиты mdadm, которую необходимо установить при помощи команды

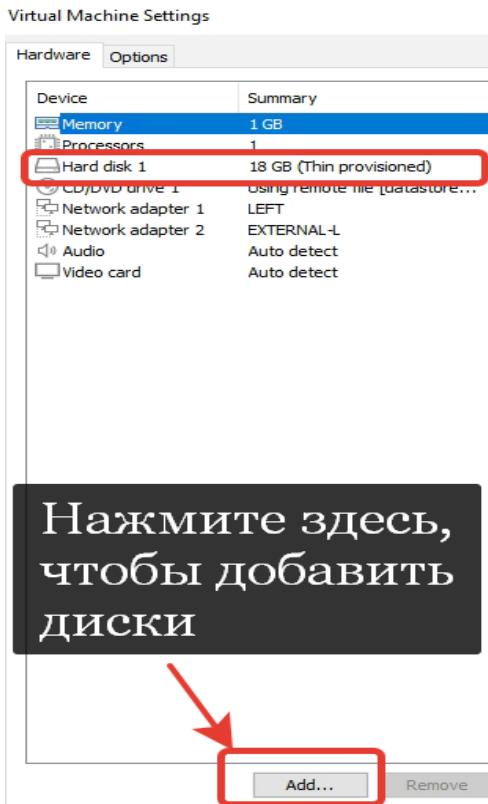
```
apt install mdadm
```

Предварительно необходимо подключить DVD-1 образ в настройках машины и пропозиции установку с DVD (apt-cdrom add, потом apt update).

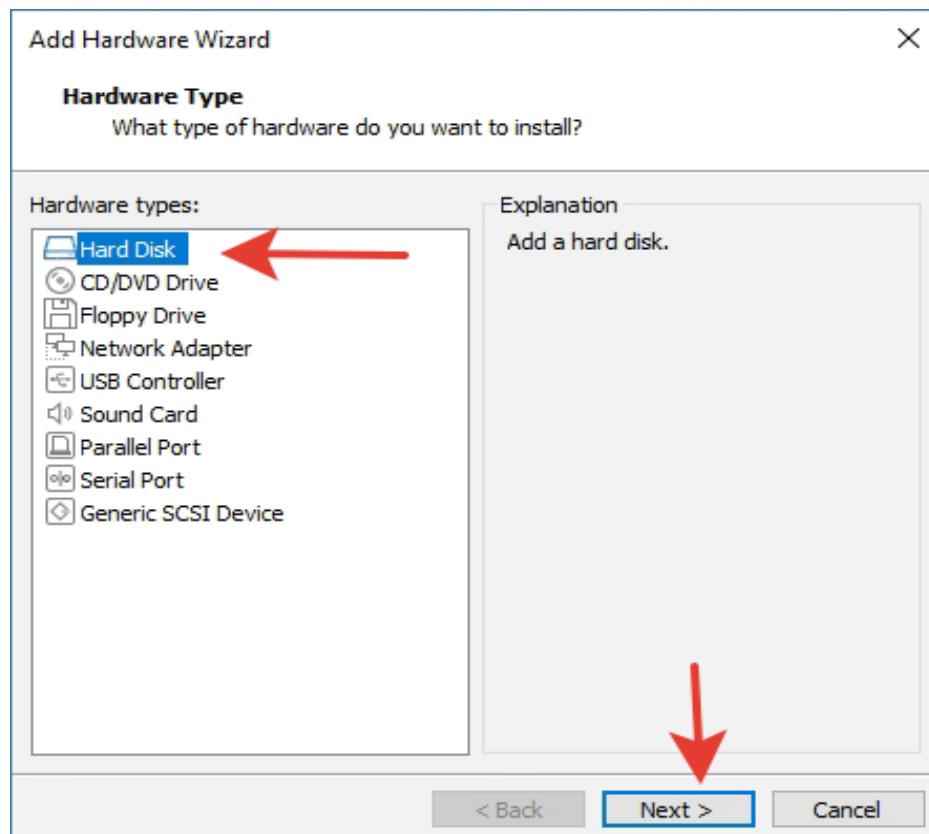
Далее необходимо проверить, присутствуют ли в настройках виртуальной машины SRV подключенные жесткие диски. Нужно открыть настройки виртуального компьютера SRV.



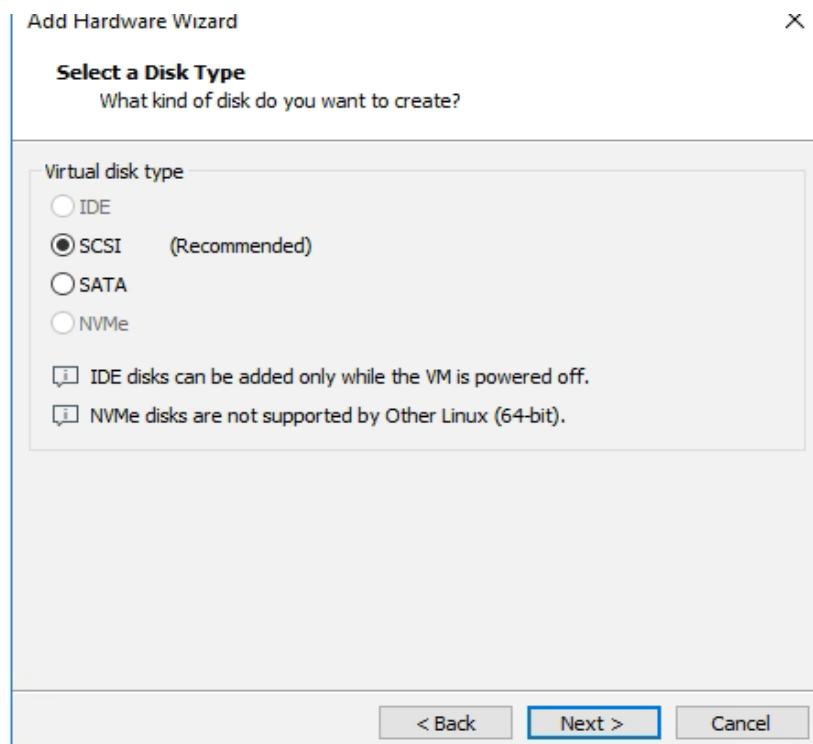
Как можно заметить, в настройках виртуальной машины SRV существует только диск на 18GB, на котором установлена операционная система. Необходимо добавить диск нажатием на Add...



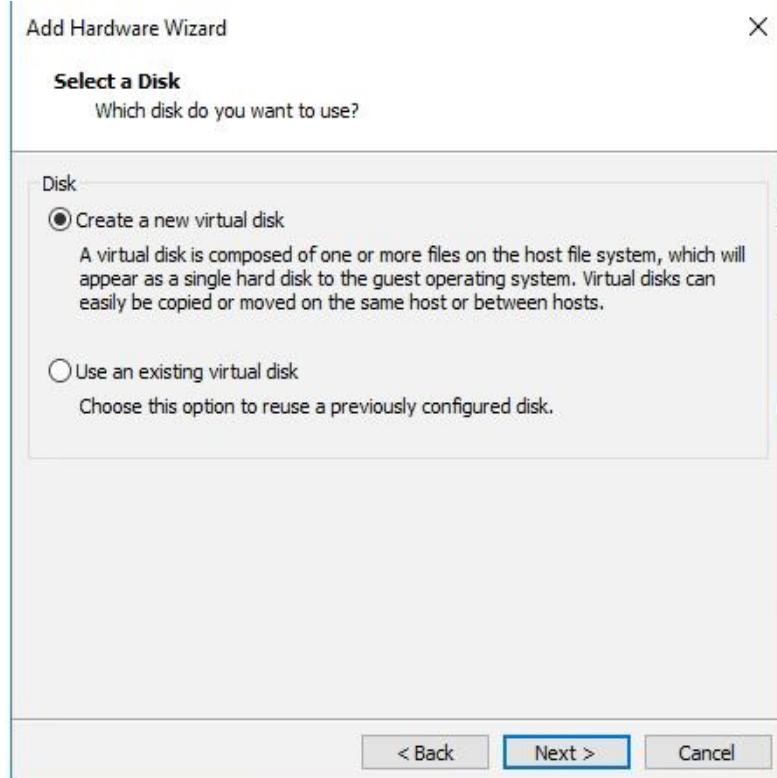
Далее система уточнит, какое устройство добавляется в ВМ, нужно выбрать Hard Disk.



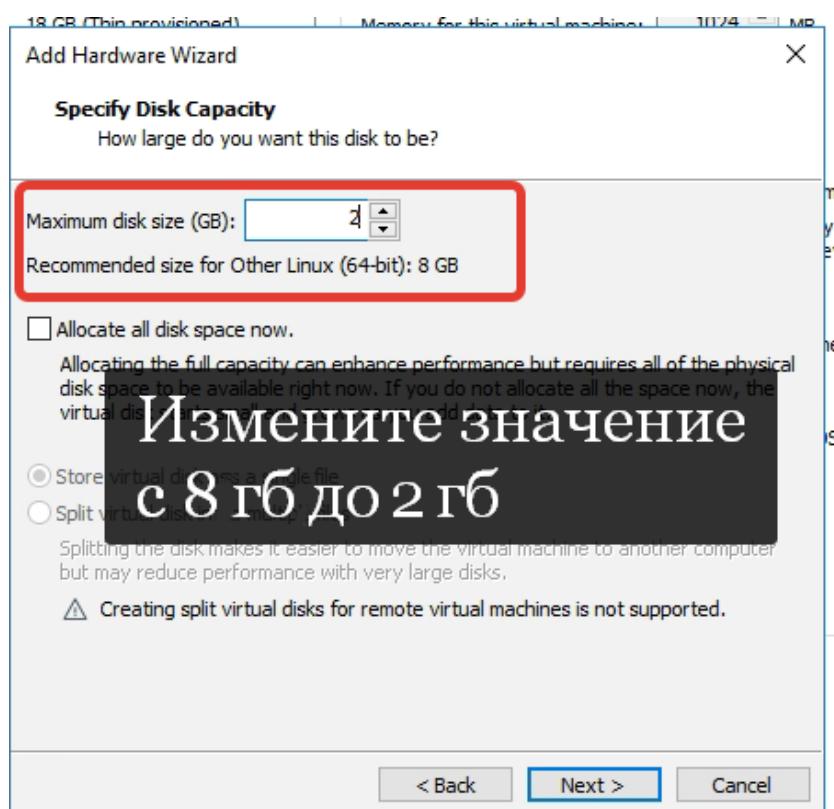
Далее система запрашивает указать тип подключения диска к ВМ, Vmware рекомендует SCSI, необходимо оставить данную настройку по умолчанию.



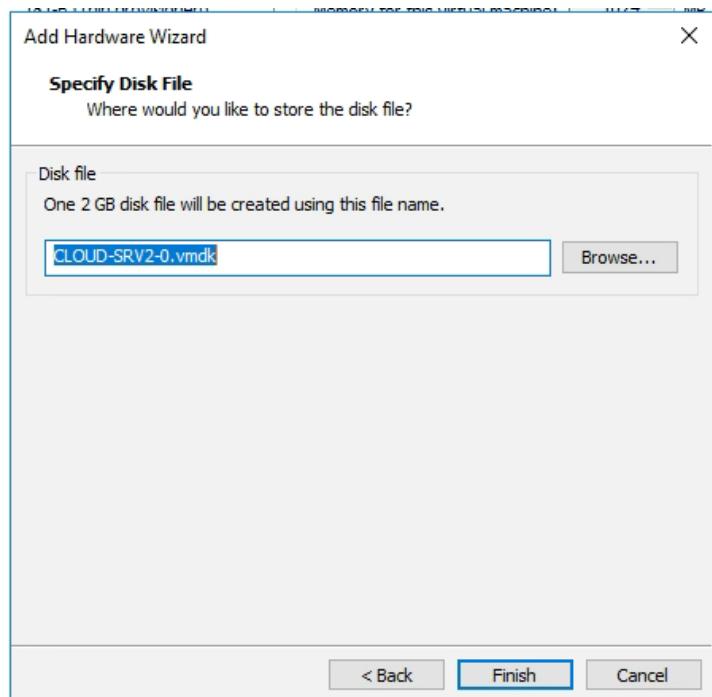
Далее система уточнит, создать ли новый диск или добавить уже существующий. Необходимо создать новый диск, это вариант по умолчанию.



В новом окне нужно указать объем диска, подключаемого к ВМ. Стоит обратить внимание, что для виртуальных дисков используется доступное физическое дисковое пространство сервера.



Далее указывается имя добавляемого диска, рекомендуется изменить имя на любое удобное. Смена имени со значения по умолчанию позволит избежать в будущем возможные проблемы с конфликтом имен.



После этого завершается добавление устройства нажатием на кнопку Finish. Необходимо повторить процедуру еще раз, создав второй жесткий диск объемом в 2 Гб.

После завершения настроек следует перезагрузить виртуальную машину, а после загрузки ввести команду lsblk.

```
root@SRV:~# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda      8:0    0   2G  0 disk
        8:16    0   18G  0 disk
          └─sdb1  8:17    0   17G  0 part /
          └─sdb2  8:18    0   1K   0 part
          └─sdb5  8:21    0  975M 0 part [SWAP]
sdc      8:32    0   2G  0 disk
sr0     11:0    1  3.7G  0 rom
root@SRV:~#
```

Стоит обратить внимание на два диска объемом по 2 Гб — sda и sdc, они без разметки диска, поэтому не имеют цифрового идентификатора, в отличие от диска sdb, который имеет подразделы:

- sdb1;
- sdb2;
- sdb5.

Все разделы, перечисленные выше, — системные, в столбце MOUNTPOINT указано, в какую директорию смонтированы данные разделы диска.

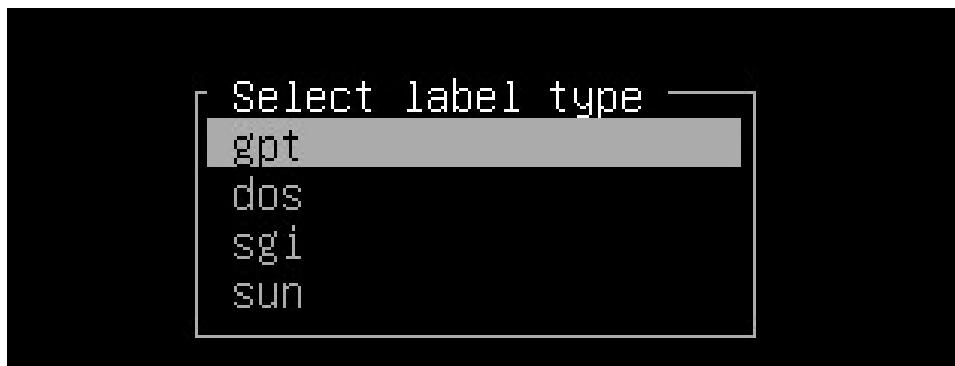
На новых неразмеченных дисках необходимо создать разделы при помощи утилиты cfdisk

cfdisk /dev/sdX , где X — буква того диска, который вы желаете форматировать.

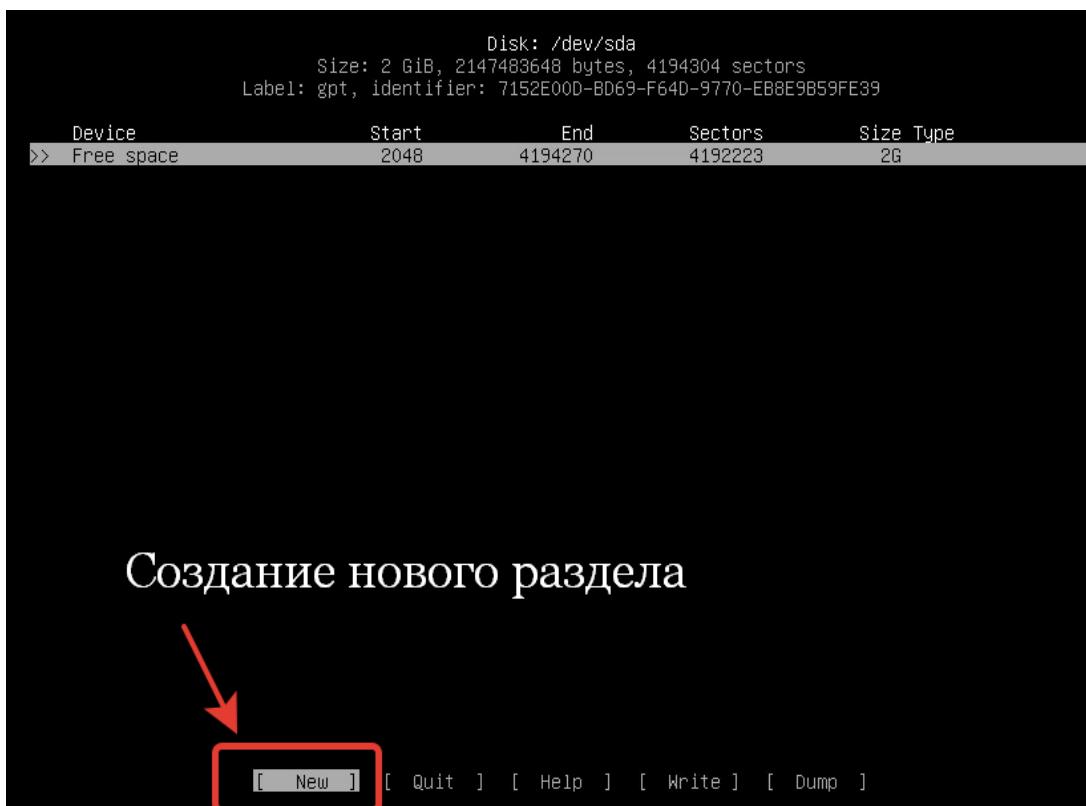
Например, разметка диска /dev/sda будет выглядеть вот так:

cfdisk /dev/sda — введите данную команду в терминал.

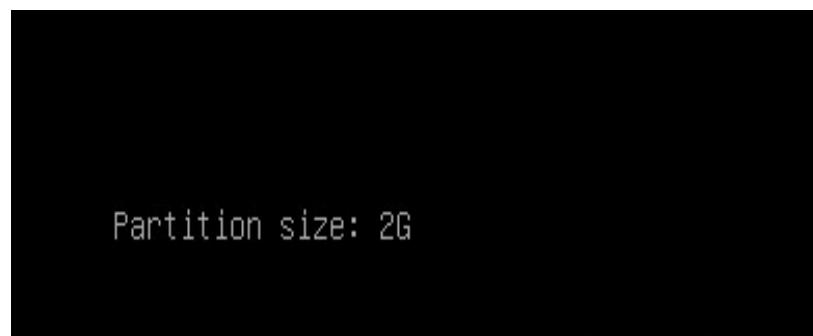
Откроется псевдографическая утилита, на данном этапе необходимо указать метку раздела — значение по умолчанию, GPT.



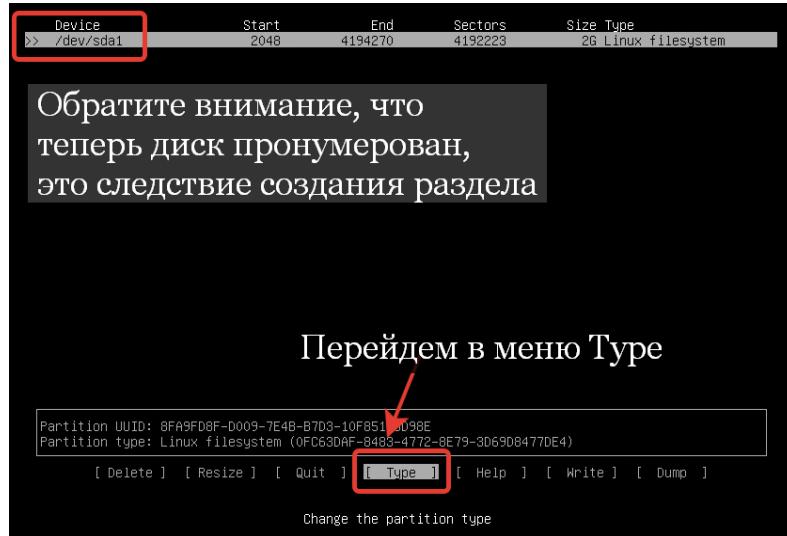
Далее необходимо выбрать New для создания нового раздела.



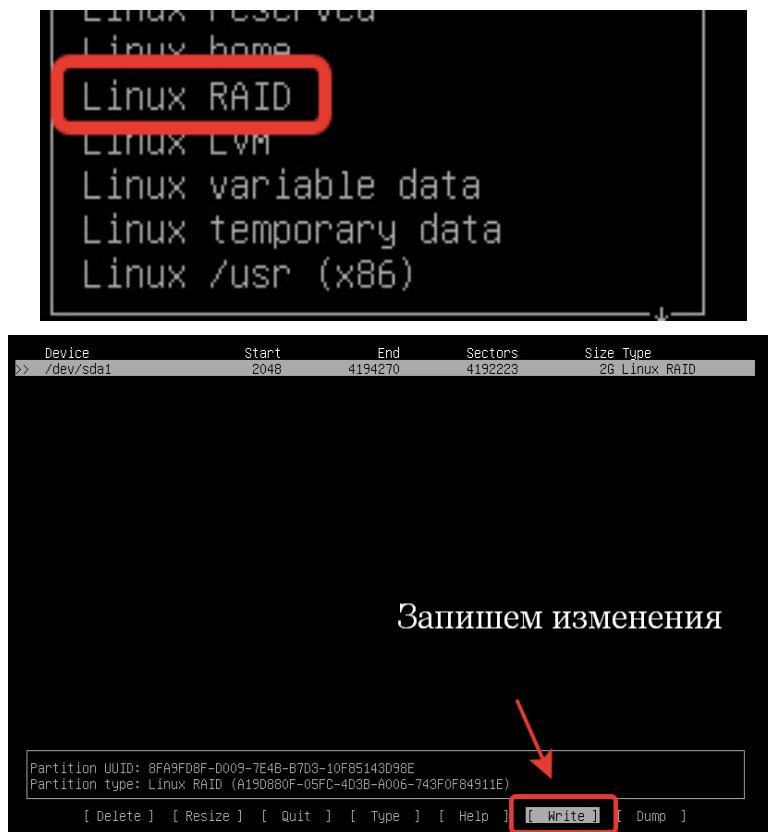
Далее указывается размер создаваемого раздела, по умолчанию указывается все свободное пространство целевого диска. Нажатием Enter происходит соглашение с размером раздела.



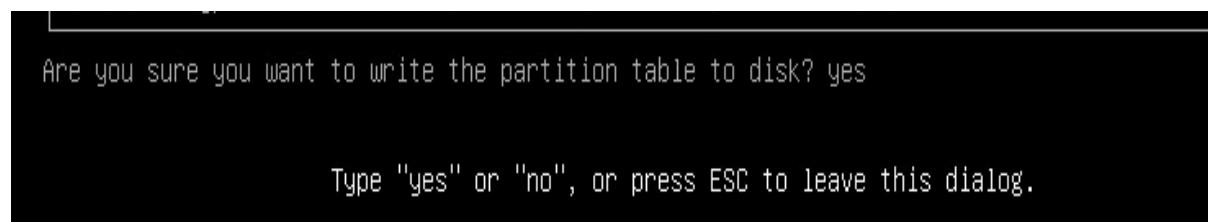
После чего необходимо перейти в опцию меню Type, чтобы указать, какой формат разметки выбрать. По умолчанию выбирается Linux Filesystem, но для создания RAID-массива потребуется отформатировать диск в Linux RAID.



В указанном списке выбирается Linux RAID.



Вручную пишется слово yes, чтобы принять изменения и отформатировать диск.



После внесенных правок необходимо покинуть утилиту cfdisk, выбрав параметр Quit.

```
Partition UUID: 8FA9FD8F-D009-7E4B-B7D3-10F85143D98E  
Partition type: Linux RAID (A19D880F-05FC-4D3B-A006-743F0F84911E)
```

```
[ Delete ] [ Resize ] [ Quit ] [ Type ] [ Help ] [ Write ] [ Dump ]
```

Необходимо повторить данную процедуру также и со вторым добавленным диском.

### Как проверить

Созданные разделы можно увидеть в выводе команды lsblk.

```
root@SRV:~# lsblk  
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT  
└─sda    8:0    0   2G  0 disk  
  └─sda1  8:1    0   2G  0 part  
└─sdb    8:16   0 18G  0 disk  
  └─sdb1  8:17   0 17G  0 part /  
  └─sdb2  8:18   0   1K  0 part  
  └─sdb5  8:21   0 975M 0 part [SWAP]  
└─sdc    8:32   0   2G  0 disk  
  └─sdc1  8:33   0   2G  0 part  
sr0     11:0    1 3.7G  0 rom  
root@SRV:~#
```

### Краткая справка

- управление RAID ([https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/9/html/managing\\_storage\\_devices/managing-raid\\_managing-storage-devices](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/managing_storage_devices/managing-raid_managing-storage-devices));
- кратко о RAID-массивах ([https://ru.bmstu.wiki/RAID\\_\(Redundant\\_Array\\_of\\_Independent\\_Disks\)](https://ru.bmstu.wiki/RAID_(Redundant_Array_of_Independent_Disks)));
- дополнительная информация о RAID ([https://ru.wikipedia.org/wiki/RAID#RAID\\_1E](https://ru.wikipedia.org/wiki/RAID#RAID_1E)).

Далее необходимо собрать RAID1-массив. Для этого необходимо воспользоваться командой

```
mdadm --create /dev/md0 --level=1 --raid-devices=2 /dev/sda1 /dev/sdc1
```

```
root@SRV:~# mdadm --create /dev/md0 --level=1 --raid-devices=2 /dev/sda1 /dev/sdc1  
mdadm: Note: this array has metadata at the start and  
      may not be suitable as a boot device. If you plan to  
      store '/boot' on this device please ensure that  
      your boot-loader understands md/v1.x metadata, or use  
      --metadata=0.90  
Continue creating array?  
Continue creating array? (y/n) y  
mdadm: Defaulting to version 1.2 metadata  
mdadm: array /dev/md0 started.  
root@SRV:~#
```

### Комментарии к введенной команде

- mdadm — обращение к утилите mdadm;
- --create — создать новый массив;
- /dev/md0 — указывается, как будет называться логический том RAID-массива, /dev/mdX, где X — порядковый номер RAID-массива, а mdX — зарезервированное имя устройства для RAID в Linux;

- --level=1 — указывается уровень RAID-массива. 1 — указывает на RAID1 («Зеркало»);
  - --raid-devices=2 — указывается количество устройств, добавленных в RAID-массив;
  - /dev/sda1 /dev/sdc1 — перечисляются диски, которые добавим в RAID-массив.
- После этого утилита mdadm начнет создание RAID-массива.  
Процесс сборки RAID-массива можно наблюдать в выводе файла /proc/mdstat  
cat /proc/mdstat:

```
root@SRV:~# cat /proc/mdstat
Personalities : [linear] [multipath] [raid0] [raid1] [raid6] [raid5] [raid4] [raid10]
md0 : active raid1 sdc1[1] sda1[0]
      2094080 blocks super 1.2 [2/2] [UU]
unused devices: <none>
root@SRV:~# _
```

Обозначение букв UU (use;use) указывает на то, что оба диска прошли инициализацию и сборку в RAID-массив и готовы к работе.

После того, как массив собран, его необходимо сохранить при помощи команды mdadm --detail --scan --verbose | tee -a /etc/mdadm/mdadm.conf

```
root@SRV:~# mdadm --detail --scan --verbose | tee -a /etc/mdadm/mdadm.conf
ARRAY /dev/md0 level=raid1 num-devices=2 metadata=1.2 name=SRV:0 UUID=6a3718c6:6ec730b6:03d1b030:f48
15b0a
  devices=/dev/sda1,/dev/sdc1
root@SRV:~#
```

#### **Комментарии к введенной команде**

- mdadm — обращение к утилите mdadm;
- --detail — вывести информацию о активных RAID-массивах;
- --scan — просканировать все RAID-массивы с целью получения актуализированной информации;
- --verbose — вывести расширенную информацию по выводу команды --detail. Данный ключ работает только в связке с опциями --detail --scan или --examine --scan;
- | — указатель, что вывод предыдущей команды необходимо перенаправить в другой файл;
- tee — считывает данные из стандартного устройства ввода и записывает их на стандартное устройство вывода или в файл;
- -a — добавить данные к указанным файлам, без перезаписи;
- /etc/mdadm/mdadm.conf — указать файл, к которому добавляется вывод mdadm.

Далее необходимо пересоздать initramfs с поддержкой данного массива при помощи команды update-initramfs -u — данная команда обновит информацию о монтируемых при загрузке разделах RAID.

```
root@SRV:~# update-initramfs -u
update-initramfs: Generating /boot/initrd.img-5.10.0-9-amd64
root@SRV:~#
```

Готовый массив также отобразится в выводе утилиты lsblk.

```
root@SRV:~# lsblk
  NAME   MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINT
  sda      8:0    0   2G  0 disk
  └─sda1   8:1    0   2G  0 part
    └─md0    9:0    0   2G  0 raid1
  sdb      8:16   0  18G  0 disk
  └─sdb1   8:17   0  17G  0 part  /
  └─sdb2   8:18   0   1K  0 part
  └─sdb5   8:21   0 975M 0 part  [SWAP]
  sdc      8:32   0   2G  0 disk
  └─sdc1   8:33   0   2G  0 part
    └─md0    9:0    0   2G  0 raid1
  sr0     1:0    1  3.7G 0 rom
root@SRV:~# _
```

После того, как массив собран, необходимо форматировать его в файловую систему ext4 и настроить автоматическое монтирование при загрузке.

Форматирование можно произвести при помощи команды  
mkfs.ext4 /dev/md0

Данная команда отформатирует файловый раздел в файловую систему ext4.

```
root@SRV:~# mkfs.ext4 /dev/md0
mke2fs 1.46.2 (28-Feb-2021)
Creating filesystem with 523520 4k blocks and 131072 inodes
Filesystem UUID: 4033baf0-8fbe-4f5a-8295-c0819b82e7a2
Superblock backups stored on blocks:
            32768, 98304, 163840, 229376, 294912

Allocating group tables: done
Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done

root@SRV:~# _
```

Далее необходимо создать точку монтирования данного массива, сделать это можно при помощи команды

mkdir /mnt/storage

```
root@SRV:~# mkdir /mnt/storage
root@SRV:~# _
```

После этого необходимо добавить запись в файл /etc/fstab.

```

# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
#  <mount point> <type> <options> <dump> <pass>
# / was on /dev/sda1 during installation
UUID=329bcda3-aeee-47ae-b729-00e77cc0ae01 / ext4 errors=remount-ro 0 1
# swap was on /dev/sda5 during installation
UUID=6ad82a17-09b1-4da1-9e19-2d878a0fb12b none swap sw 0 0
/dev/sr0 /media/cdrom0 udf,iso9660 user,noauto 0 0

/dev/md0 /mnt/storage ext4 defaults 0 0_

```

### Комментарии к введенной строке

- /dev/md0 — указывается устройство, планируемое к монтированию в операционную систему;
- /mnt/storage — указывается точка монтиrovания — созданная ранее директория;
- ext4 — указывается файловая система целевого устройства;
- defaults — указывает, что параметры монтирования файловой системы будут выполнены по умолчанию;
- первый ноль — указывает параметр, который должен использоваться, если в системе установлены утилиты резервного копирования. Если установлен 0, значит, резервное копирование выключено;
- второй ноль — если установлен 0, то данный раздел не проверяется на ошибки разделов утилитой fsck, иные значения указывают на проверку раздела.

### Как проверить

Протестировать автоматическое монтирование без перезагрузки машины можно при помощи команды mount -av.

```

root@SRV:~# mount -av
/ : ignored
none : ignored
/media/cdrom0 : ignored
/mnt/storage : successfully mounted
root@SRV:~#

```

После этого можно протестировать автоматическое монтирование перезагрузкой машины.

Необходимо перезагрузить машину с помощью команды reboot.

После успешной перезагрузки вводится команда lsblk.

```

Debian GNU/Linux 11 SRV tty1
SRV login: root
Password:
Linux SRV 5.10.0-9-amd64 #1 SMP Debian 5.10.70-1 (2021-09-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Jan  8 04:51:04 EST 2022 on tty1
root@SRV:~# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda    8:0    0   2G  0 disk
└─sda1 8:1    0   2G  0 part
  └─md0 9:0    0   2G  0 raid1 /mnt/storage
sdb    8:16   0 400G  0 disk
└─sdb1 8:17   0 17G  0 part /
└─sdb2 8:18   0 1K   0 part
└─sdb5 8:21   0 975M 0 part [SWAP]
sdc    8:32   0   2G  0 disk
└─sdc1 8:33   0   2G  0 part
  └─md0 9:0    0   2G  0 raid1 /mnt/storage
sr0   11:0    1  5.7G 0 rom
root@SRV:~#

```

## Дополнительная информация

- автоматическое монтирование системных файлов с помощью fstab ([https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/4/html/introduction\\_to\\_system\\_administration/s2-storage-mount-fstab](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/4/html/introduction_to_system_administration/s2-storage-mount-fstab));
- подробнее про fstab (<https://linode.com/understanding-each-entry-of-linux-fstab-etcfstab-file>);
- подробнее про mdadm (<http://xgu.ru/wiki/mdadm>);
- далее необходимо реализовать файловый сервер по протоколу SMB. Для этого необходимо установить пакет SAMBA при помощи команды  
`apt install samba`  
После установки пакета необходимо открыть его конфигурационный файл /etc/samba/smb.conf.  
Не меняя остальных параметров, в конце файла необходимо описать новый общий ресурс.

```
[share] #1
path = /mnt/storage #2
browseable = yes #3
read only = no #4
guest ok = yes #5_
```

Если в задании указано, что файлы, создаваемые средствами сетевого обмена, принадлежат специально созданному пользователю smbuser вне зависимости от того, кто их создал, либо все созданные файлы в рамках обмена должны принадлежать одному специальному пользователю, выполняем следующие шаги.

Необходимо создать пользователя командой useradd smbuser и внести следующие изменения в /etc/samba/smb.conf:

```
# This option controls how unsuccessful authentication attempts are mapped
# to anonymous connections
map to guest = bad user
guest account = smbuser
```

```
[share]
path = /mnt/storage
browseable = yes
read only = no
guest ok = yes
force user = smbuser
```

Подробне: <https://www.thegeekdiary.com/how-to-force-user-group-ownership-of-files-on-a-samba-share>.

Стоит обратить внимание, что каждая строчка пронумерована, комментарии к каждой из строчек:

- 1 — название общего ресурса;
- 2 — физический путь к общей папке;

- 3 — разрешить обнаружение папки;
- 4 — включить режим чтения и записи;
- 5 — разрешить анонимный доступ.

После внесения конфигурации необходимо перезапустить сервисы SMBD и NMBD при помощи команд

```
systemctl restart smbd
systemctl restart nmbd
```

Далее необходимо установить максимальные права на каталог для обеспечения полнофункционального анонимного доступа при помощи команды chmod 777 /mnt/storage.

```
root@SRV:~# systemctl restart smbd nmbd
root@SRV:~# _
```

В целях тестирования создается пустой файл в директории /mnt/storage с помощью команды

```
touch /mnt/storage/test
```

#### **Дополнительная информация**

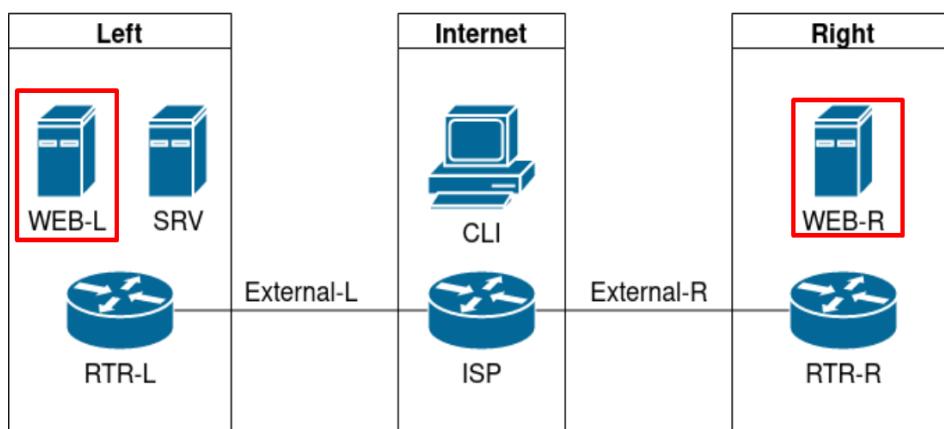
- использование SAMBA как сервера ([https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/8/html/deploying\\_different\\_types\\_of\\_servers/assembly\\_using-samba-as-a-server\\_deploying-different-types-of-servers](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/deploying_different_types_of_servers/assembly_using-samba-as-a-server_deploying-different-types-of-servers));
- документация протокола SAMBA (<https://www.samba.org/samba/docs>);
- информация о пакете NMBD (<https://www.opennet.ru/man.shtml?topic=nmbd&category=8&ussian=0>).

На данном этапе выполнить функциональную проверку не получится, поэтому необходимо перейти к следующему заданию, по формулировке которого становится очевидно, что созданный на машине SRV сетевой ресурс по SAMBA используется для серверов WEB-L и WEB-R.

**Задание 5.** Сервера WEB-L и WEB-R должны использовать службу, настроенную на SRV, для обмена файлами между собой:

- служба файлового обмена должна позволять монтирование в виде стандартного каталога Linux;
- разделяемый каталог должен быть смонтирован по адресу /opt/share;
- каталог должен позволять удалять и создавать файлы в нем для всех пользователей.

#### **Как делать**



Для монтирования разделяемого ресурса на сервера WEB-L и WEB-R необходимо установить пакеты samba-client и cifs-utils при помощи команды

```
apt install samba-client cifs-utils
```

После установки пакетов необходимо использовать команду mount для монтирования каталога.

```
root@WEB-L:~# mkdir /opt/share
root@WEB-L:~# mount //192.168.100.200/share /opt/share/ -o guest
root@WEB-L:~# ls /opt/share
lost+found test
root@WEB-L:~#
```

#### Комментарии к ряду введенных команд

- mkdir /opt/share — создать каталог /opt/share;
- mount //192.168.100.200/share /opt/share -o guest — монтируем сетевой папку по протоколу SMB в папку /opt/share, -o указывает на логин пользователя для монтирования;
- ls /opt/share — указывается содержимое папки /opt/share.

Смонтированный ресурс отображается в выводе команды df -h.

```
root@WEB-L:~# df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            473M    0  473M   0% /dev
tmpfs           98M  620K  98M   1% /run
/dev/sda1        17G  1.2G  15G   8% /
tmpfs           489M    0  489M   0% /dev/shm
tmpfs           5.0M    0  5.0M   0% /run/lock
tmpfs           98M    0  98M   0% /run/user/0
//192.168.100.200/share  2.0G  119M  1.9G   6% /opt/share
root@WEB-L:~#
```

Для автоматического монтирования необходимо добавить запись в /etc/fstab.

```
root@WEB-L:~# cat /etc/fstab
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# systemd generates mount units based on this file, see systemd.mount(5).
# Please run 'systemctl daemon-reload' after making changes here.
#
# <file system> <mount point> <type> <options> <dump> <pass>
# / was on /dev/sda1 during installation
UUID=0bf811ab-47b8-435c-aa07-d9132e65832b /          ext4    errors=remount-ro 0      1
# swap was on /dev/sda5 during installation
UUID=d0941241-95d4-4c9d-9ef1-287d4272d2f1 none       swap      sw      0      0
/dev/sr0        /media/cdrom0 udf,iso9660 user,noauto     0      0
//192.168.100.200/share /opt/share cifs defaults,guest,rw      0      0
root@WEB-L:~#
```

Параметры монтирования уже обсуждались ранее, добавленная запись guest указывает на то, что при монтировании указывается логин guest, а строка rw — указывает права на монтируемый ресурс для чтения и записи.

## Как проверить

Проверить возможность монтирования без перезагрузки можно при помощи команды `mount -av`

```
root@WEB-L:~# mount -av
/
none          : ignored
/media/cdrom0 : ignored
mount.cifs kernel mount options: ip=192.168.100.200,unc=\192.168.100.200\share,user=,pass=
/opt/share    : successfully mounted
root@WEB-L:~# touch /opt/share/123123testtest123
root@WEB-L:~# ls /opt/share/
123123testtest123  lost+found  test
root@WEB-L:~# _
```

Командой **touch** можно создать любой файл в смонтированной директории `/opt/share`.

## Дополнительная информация

- монтирование SAMBA-папок в Linux ([https://wiki.samba.org/index.php/Mounting\\_samba\\_shares\\_from\\_a\\_unix\\_client](https://wiki.samba.org/index.php/Mounting_samba_shares_from_a_unix_client));
- создание SAMBA-папок (<http://linuxsql.ru/content/nastroika-failovogo-servera-samba-na-debian-chast-tretya>).

**Задание 6.** Выполните настройку центра сертификации на базе SRV.

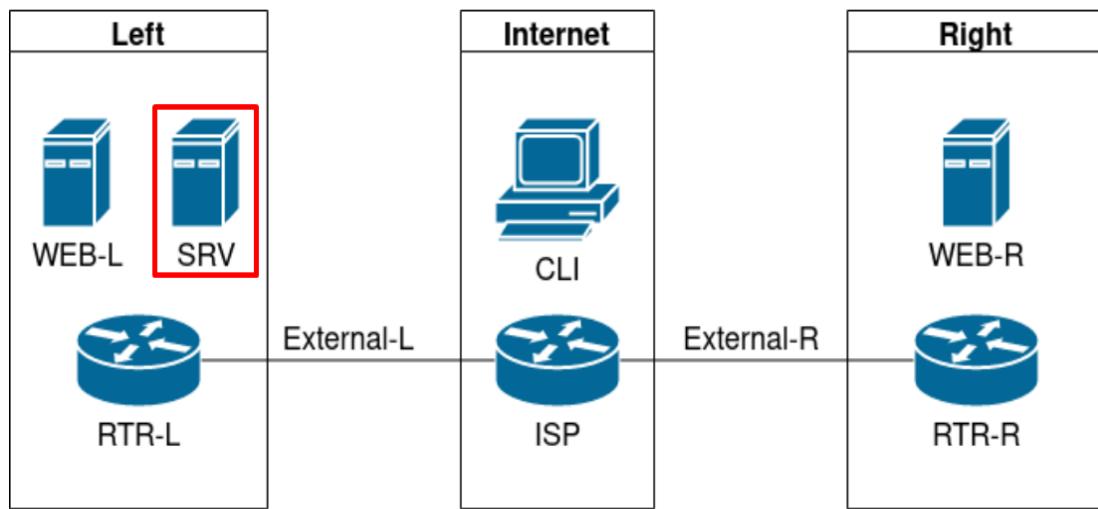
В случае применения решения на базе Linux используется центр сертификации типа OpenSSL и располагается по адресу `/var/ca`.

Выдаваемые сертификаты должны иметь срок жизни не менее 300 дней.

Параметры выдаваемых сертификатов:

- страна RU;
- организация DEMO.WSR;
- прочие поля (за исключением CN) должны быть пусты.

## Как делать



Для настройки центра сертификации используется утилита CA.pl. Данная утилита присутствует в Debian 11 по умолчанию, но стоит указать, что в случае недоступности данную утилиту можно установить с помощью команды

```
apt install libcrypt-openssl-* -y
```

Во-первых, необходимо изменить конфигурационный файл `/usr/lib/ssl/openssl.cnf`. На строке 48 следует изменить значение dir на `/var/ca`. Также нужно указать директорию хранения конфигурации центра сертификации, согласно условиям задания.

```

40
41 ##### [ ca ]
42 [ ca ]           = CA_default          # The default ca section
43
44 ##### [ CA_default ]
45 [ CA_default ]
46
47
48 dir      = /var/ca                # Where everything is kept
49 certs   = $dir/certs             # Where the issued certs are kept
50 crl_dir = $dir/crl               # Where the issued crl are kept
51 database = $dir/index.txt       # database index file.
52 #unique_subject = no            # Set to 'no' to allow creation of
53                      # several certs with same subject.
54 new_certs_dir = $dir/newcerts    # default place for new certs.
55
56 certificate = $dir/cacert.pem    # The CA certificate
57 serial     = $dir/serial           # The current serial number
58 crlnumber  = $dir/crlnumber       # the current crl number
59                      # must be commented out to leave a V1 CRL
-- VISUAL LINE --

```

1 48,14-25 7%

В строке 78 изменить default\_days на 1024 (или любое значение больше 300), так как по условиям задания сказано, что срок действия сертификата должен быть больше 300 дней.

```

72
73 # Extensions to add to a CRL. Note: Netscape communicator chokes on V2 CRL
74 # so this is commented out by default to leave a V1 CRL.
75 # crlnumber must also be commented out to leave a V1 CRL.
76 # crl_extensions = crl_ext
77
78 default_days = 1024                # how long to certify for
79 default_crl_days= 30                 # how long before next CRL
80 default_md   = default              # use public key default MD
81 preserve     = no                   # keep passed DN ordering
82
83 # A few difference way of specifying how similar the request should look
84 # For type CA, the listed attributes must be the same, and the optional
85 # and supplied fields are just that :-
86 policy       = policy_match
87
88 # For the CA policy
89 [ policy_match ]
90 countryName      = match
91 stateOrProvinceName = match
92 organizationName = match
93 organizationalUnitName = optional
94 commonName       = supplied
95 emailAddress     = optional
-- VISUAL LINE --

```

1

В строке 134 изменить значение страны на RU, согласно условиям задания.

```

129
130 # req_extensions = v3_req # The extensions
131
132 [ req_distinguished_name ]
133 countryName           = Country Name
134 countryName_default  = RU
135 countryName_min       = 2
136 countryName_max       = 2
137

```

В строке 139 поставить точку вместо значения, в строке 144 прописать DEMO.WSR, согласно условиям задания. На этом пункте указывается название организации, которая занимается поддержкой данного центра сертификации.

```

137
138 stateOrProvinceName      = State or Province Name (full name)
139 stateOrProvinceName_default = .
140
141 localityName            = Locality Name (eg, city)
142
143 organizationName        = Organization Name (eg, company)
144 organizationName_default = DEMO.WSR
145

```

Необходимо убрать комментарий из строки 151 и также поставить точку, в данном пункте можно указать имя подразделения или отдела в указанной выше компании, который занимается поддержкой данного центра сертификации.

```

148 #1.organizationName_default = World Wide Web Pty Ltd
149
150 organizationalUnitName    = Organizational Unit Name (eg, section)
151 organizationalUnitName_default = .
152

```

После этого необходимо сохранить и закрыть файл, затем перейти в директорию /usr/lib/ssl/misc и открыть для редактирования скрипт CA.pl. Этот скрипт используется для удобного и автоматизированного управления центром сертификации с помощью пакета openssl.

В строке 28 изменить значение days на 1024 (или любое значение больше 500).

```

26
27 my $OPENSSL_CONFIG = $ENV{"OPENSSL_CONFIG"} || "";
28 my $DAYS = "-days 1024";
29 my $CADAYS = "-days 1095";      # 3 years
30 my $REQ = "$openssl req $OPENSSL_CONFIG";
31 my $CA = "$openssl ca $OPENSSL_CONFIG";
32 my $VERIFY = "$openssl verify";
33 my $X509 = "$openssl x509";
34 my $PKCS12 = "$openssl pkcs12";
35

```

В строке 37 изменить значение на /var/ca.

```

35
36 # default openssl.cnf file has setup as per the following
37 my $CATOP = "/var/ca";
38 my $CAKEY = "cakey.pem";
39 my $CAREQ = "careq.pem";
40 my $CACERT = "cacert.pem";
41 my $CACRL = "crl.pem";
42 my $DIRMODE = 0777;
43

```

После того, как конфигурация центра сертификации отредактирована, можно приступить к его развертыванию. Для этого необходимо из каталога /usr/lib/ssl/misc выполнить команду-вызов скрипта

`./CA.pl -newca`

Данная команда выполнит скрипт и передаст ему ключ -newca, необходимый для инициализации центра сертификации и конфигурирования его корневого сертификата.

Система потребует ввести пароль, необходимо повторить его дважды.

```
ca.pl      tsget      tsget.pl
root@...:/usr/lib/ssl/misc# ./CA.pl -newca
CA certificate filename (or enter to create)

Making CA certificate - P@ssword
=====
openssl req -new -keyout .../private/cakey.pem -out .../careq.pem
Generating a RSA private key
..+++++
.....!!!!!
writing new private key to ' .../private/cakey.pem'
Enter PEM pass phrase:_

```

```
root@SRV:/usr/lib/ssl/misc# ./CA.pl -newca
CA certificate filename (or enter to create)

Making CA certificate ...
=====
На данном этапе скрипту
===== требует указать страну ЦС
===== Значение в [] указывает на значение
===== Enter PEM pass phrase:
===== Enter
===== You are about to be asked to enter information that will be incorporated
===== into your certificate request.
===== What you are about to enter is what is called a Distinguished Name or a DN.
===== There are quite a few fields but you can leave some blank
===== For some fields there will be a default value,
===== If you enter '.', the field will be left blank.
===== Country Name (2 letter code) [RU]:_

```

```
===== If you enter '.', the field will be left blank.
===== Country Name (2 letter code) [RU]:_
===== State or Province Name (full name) [.]:#1
===== Locality Name (eg, city) []:#2
===== Organization Name (eg, company) [DEMO.WSR]:#3
===== Organizational Unit Name (eg, section) [.]:#4
===== Common Name (e.g. server FQDN or YOUR name) []:WSR CA#5
===== Email Address []:#6

===== Please enter the following 'extra' attributes
===== to be sent with your certificate request
===== A challenge password []:#7
===== An optional company name []:#8
===== ==> 0
===== =====
===== =====
```

## **Комментарии к каждой строчке в процессе создания сертификата**

- запрашивается область или штат центра сертификации. Если нажать Enter без ввода параметров, поле будет заполнено тем содержимым, что видно в квадратных скобках, в нашем случае это символ точки;
- запрашивается город. Если нажать Enter без ввода параметров, поле будет заполнено содержимым в квадратных скобках;
- указывается имя организации. Если нажать Enter без ввода параметров, поле будет заполнено содержимым в квадратных скобках, в данном случае это слово DEMO.WSR;
- запрашивается имя отдела-поддержки центра сертификации, данный пункт пропускается;
- запрашивается имя центра сертификации, необходимо вручную указать — WSR CA;
- запрашивается электронная почта администратора данного центра сертификации, необходимо оставить поле пустым;
- запрашивается пароль для сертификата, необходимо оставить поле пустым;
- запрашивается альтернативное название компании, необходимо оставить поле пустым.

После ввода этих параметров система начнет процесс создания корневого сертификата.

```
openssl ca -create_serial -out /var/ca/cacert.pem -days 1095 -batch -keyfile /var/ca/private/cakey.pem -selfsign -extensions v3_ca -infiles /var/ca/careq.pem
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for /var/ca/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
Subject: countryName = RU
stateOrProvinceName =
organizationName = DEMO.WSR
commonName = WSR CA
X509v3 extensions:
    X509v3 Subject Key Identifier:
        A7:4B:03:55:02:20:34:EE:19:98:CF:52:1A:5B:79:38:58:E2:A7:D2
    X509v3 Authority Key Identifier:
        KeyId:A7:4B:03:55:02:20:34:EE:19:98:CF:52:1A:5B:79:38:58:E2:A7:D2
    X509v3 Basic Constraints: critical
        CA:TRUE
Certificate is to be certified until Jan 7 12:38:37 2025 GMT (1095 days)

Write out database with 1 new entries
Data Base Updated
==> 0
=====
CA certificate is in /var/ca/cacert.pem
```

Центр сертификации развернут, осталось добавить корневой сертификат в доверенные.

Файл с корневым сертификатом можно найти по пути

/var/ca/cacert.pem

Для Linux-машин необходимо скопировать данный файл в директорию /usr/local/share/ca-certificates с расширением .crt

```
cp /var/ca/cacert.pem /usr/local/share/ca-certificates/cacert.crt
```

и выполнить команду

```
update-ca-certificates — для обновления хранилища сертификатов.
```

```
root@SRV:~# cp /var/ca/cacert.pem /usr/local/share/ca-certificates/cacert.crt
root@SRV:~# update-ca-certificates
Updating certificates in /etc/ssl/certs...
 1 added, 0 removed; done.
 Running hooks in /etc/ca-certificates/update.d...
done.
root@SRV:~# _
```

## Как проверить

Проверить работоспособность доверия можно при помощи команды  
openssl verify /usr/local/share/ca-certificates/cacert.crt  
Если команда вернет OK — все сделано правильно.

```
root@SRV:~# openssl verify /usr/local/share/ca-certificates/cacert.crt
/usr/local/share/ca-certificates/cacert.crt: OK
root@SRV:~# _
```

Для Windows-машин установка сертификата выполняется при помощи установщика сертификатов.

Во-первых, необходимо отправить сертификат с расширением .crt на Windows-машину. Сделать это можно при помощи SCP, например:

SCP — утилита для копирования файлов между хостами через SSH. Для начала необходимо настроить SSH-сервер на машине SRV и WEB-L, для входа под именем пользователя root

/etc/ssh/sshd\_config — необходимо открыть с помощью текстового редактора данный документ.

Отредактировать 34-ю строчку в данном документе, такая настройка позволит пользователю root подключаться к машине по протоколу SSH с использованием логина и пароля, по умолчанию такая функция запрещена из соображений безопасности.

```
33 #!loginGraceTime 2m
34 PermitRootLogin yes
35 #StrictModes yes
```

После изменения настроек необходимо перезагрузить сервис sshd  
systemctl restart sshd

Так как машина CLI находится в Интернете, прямого доступа к машине SRV у нее нет. Для передачи сертификата следует воспользоваться машиной WEB-L, так как машина RTR-L транслирует 2222-й порт из внешнего Интернета на 22-й порт именно WEB-L.

Для начала необходимо передать сертификат с SRV в директорию /root/ на машине WEB-L.

Команда выглядит следующим образом

```
scp root@192.168.100.200:/var/ca/cacert.pem ./cacert.crt
```

```
root@WEB-L:~# scp root@192.168.100.200:/var/ca/cacert.pem ./cacert.crt
The authenticity of host '192.168.100.200' (192.168.100.200) can't be established.
ECDSA key fingerprint is SHA256:K7INq9eRdgpbshUKKxmJXHsfU6rVueVo+pzJYzg6FF4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.100.200' (ECDSA) to the list of known hosts.
root@192.168.100.200's password: введите пароль от root
cacert.pem                                         100% 4288      3.1MB/s   00:00
root@WEB-L:~# _
```

## Комментарии к введенной команде

- SCP — обращение к утилите SCP, дословно ее можно перевести как ssh-copy;
- root@192.168.100.200 — указывается логин пользователя и адрес, к которому происходит подключение;
- /var/ca/cacert.pem — указывается файл на стороне удаленной машины, который необходимо перенести;

— ./cacert.crt — с помощью специального символа ./ указывается, что планируется сохранить файл в текущей директории с именем cacert.crt.

При вводе Enter система потребует подтвердить подключение — необходимо написать слово yes. После этого вводится пароль от пользователя root и ожидается загрузка файла.

Убедиться в том, что файл точно появился в текущей директории на сервере WEB-L, можно с помощью команды ls.

```
root@WEB-L:~# ls
app.tar cacert.crt
root@WEB-L:~#
```

Также необходимо отредактировать /etc/ssh/sshd\_config.

После на машине CLI вводим следующее:

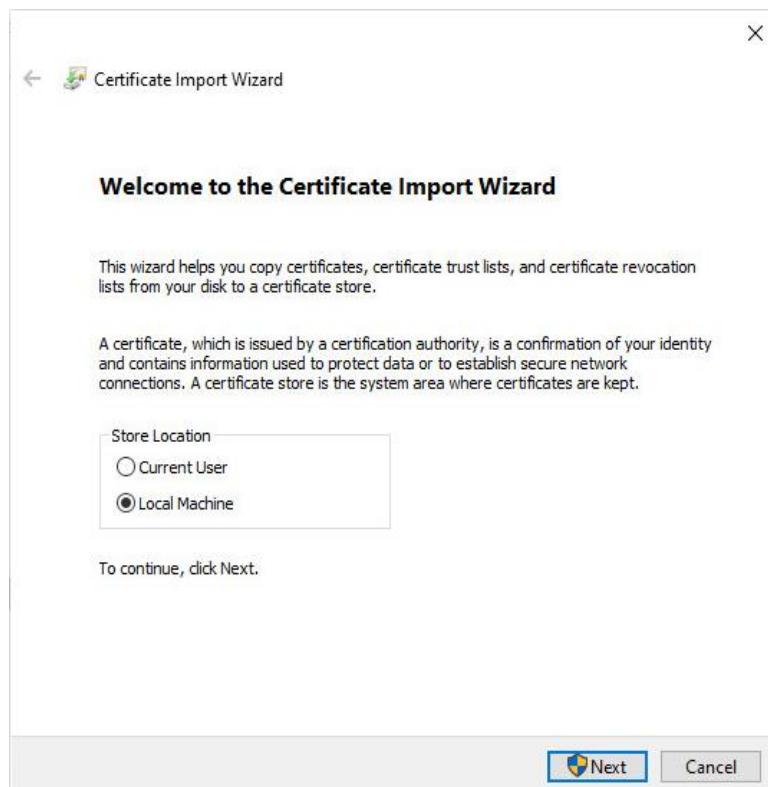
```
^C
C:\Users\user1>scp -P 2222 root@4.4.4.100:/root/ca* ./
root@4.4.4.100's password:
cacert.crt
```

Файл cacert.crt был успешно перемещен и сохранен по пути — C:\Users\user1, необходимо перейти по этому пути.

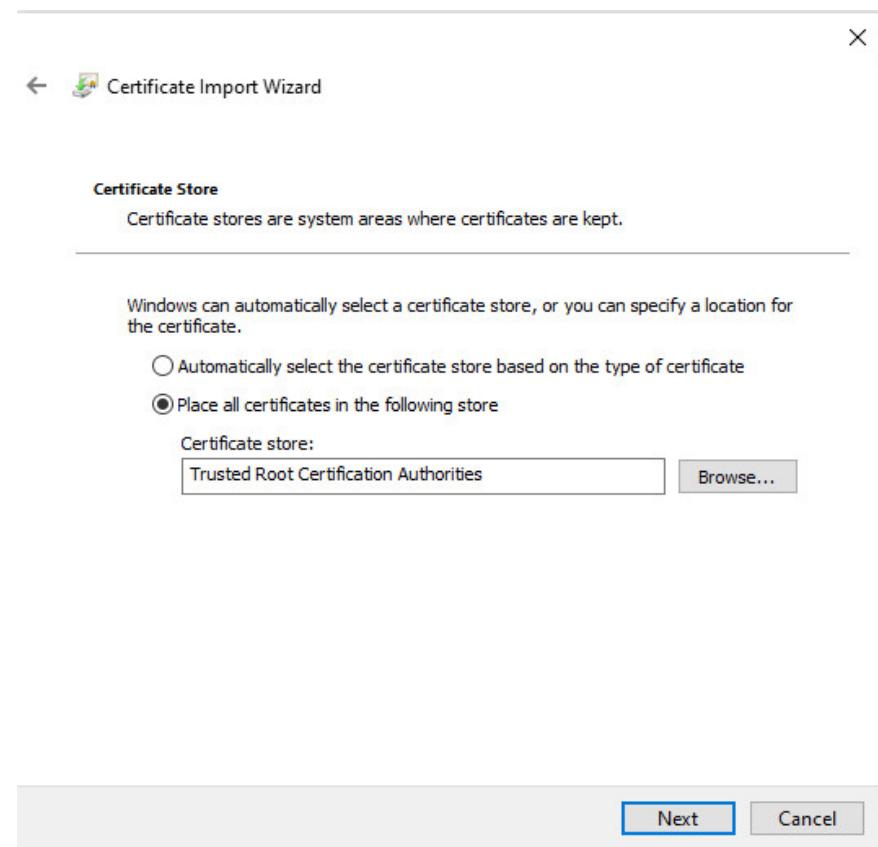
После этого необходимо нажать на файл ПКМ и выбрать install certificate.



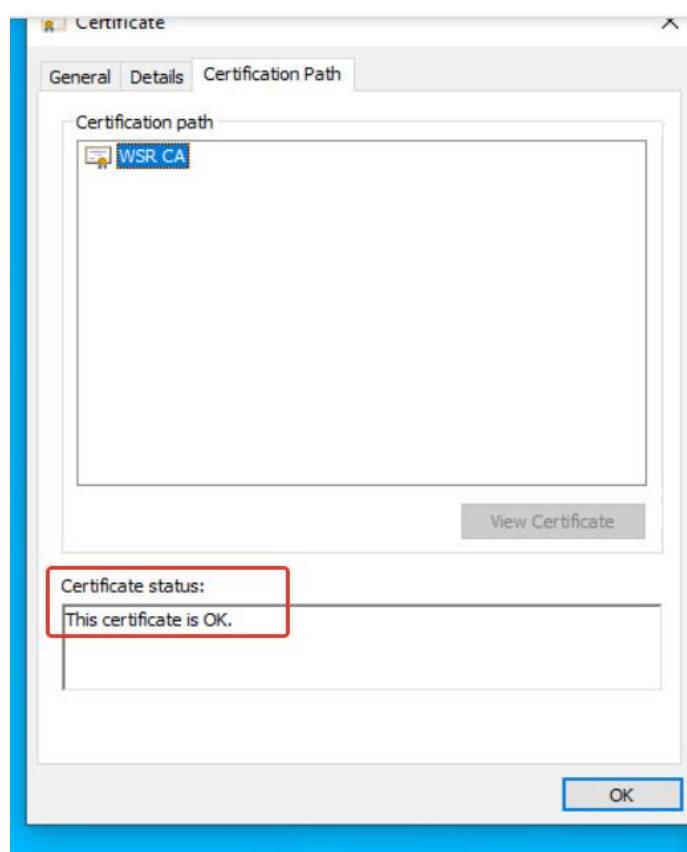
В качестве места хранилища необходимо выбрать Local Machine.



В качестве хранилища — Trusted Root Certification Authorities.



Проверить, доверяет ли клиент сертификату, можно просто открыв файл с сертификатом и перейдя во вкладку Certification Path.



### **Дополнительная информация**

- использование OpenSSL ([https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/7/html/security\\_guide/sec-using.openssl](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sec-using.openssl));
- что такое Центры сертификации? (<https://www.globalsign.com/ru-ru/ssl-information-center/what-are-certification-authorities-trust-hierarchies>);
- официальная документация на пакет OpenSSL (<https://www.openssl.org/docs>).

# ВЗАИМОДЕЙСТВИЕ СО СПЕЦИАЛИСТАМИ СМЕЖНОГО ПРОФИЛЯ ПРИ РАЗРАБОТКЕ МЕТОДОВ, СРЕДСТВ И ТЕХНОЛОГИЙ ПРИМЕНЕНИЯ ОБЪЕКТОВ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

**Задание 1.** Выполните установку приложения AppDocker0.

Образ Docker (содержащий веб-приложение) расположен на ISO-образе дополнительных материалов.

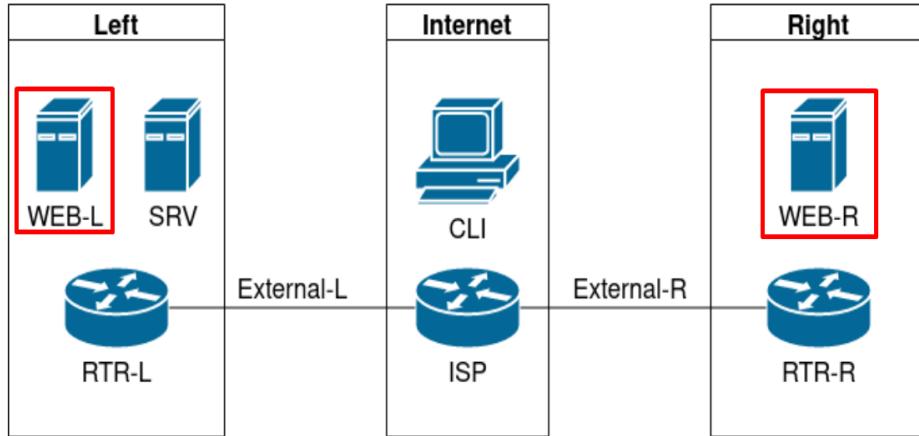
Пакеты для установки Docker расположены на дополнительном ISO-образе.

Инструкция по работе с приложением расположена на дополнительном ISO-образе.

Необходимо реализовать следующую инфраструктуру приложения:

- клиентом приложения является CLI (браузер Edge);
- хостинг приложения осуществляется на ВМ WEB-L и WEB-R;
- доступ к приложению осуществляется по DNS-имени www.demo.wsr;
- имя должно разрешаться во «внешние» адреса ВМ управления трафиком в обоих регионах;
- при необходимости для доступа к приложению допускается реализовать реверс-прокси или трансляцию портов;
- доступ к приложению должен быть защищен с применением технологии TLS;
- необходимо обеспечить корректное доверие сертификату сайта, без применения «исключений» и подобных механизмов;
- незащищенное соединение должно переводиться на защищенный канал автоматически;
- необходимо обеспечить отказоустойчивость приложения;
- сайт должен продолжать обслуживание (с задержкой не более 25 с) в следующих сценариях:
  - а) отказ одной из ВМ Web;
  - б) отказ одной из ВМ управления трафиком.

**Как делать**



На ВМ WEB-L и WEB-R необходимо выполнить установку Docker. Это можно сделать при помощи команды

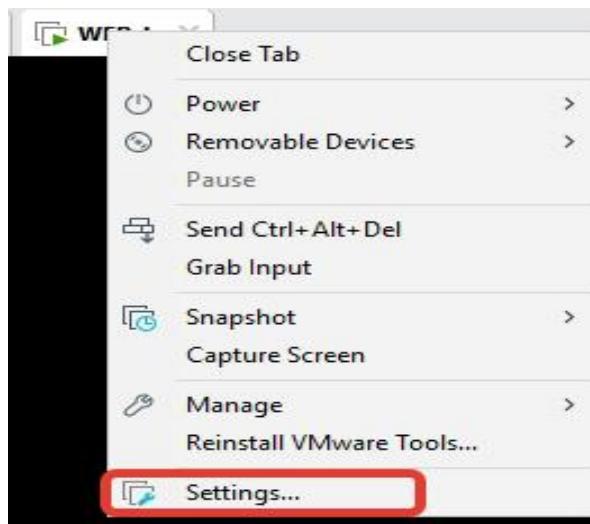
```
apt install docker docker.io
```

Если работа идет без интернета, то требуется наличие диска с ОС DVD 1, загруженного с сайта производителя ОС.

После того, как установка была выполнена, необходимо смонтировать к ВМ образ с дополнительными материалами и скопировать образ приложения.

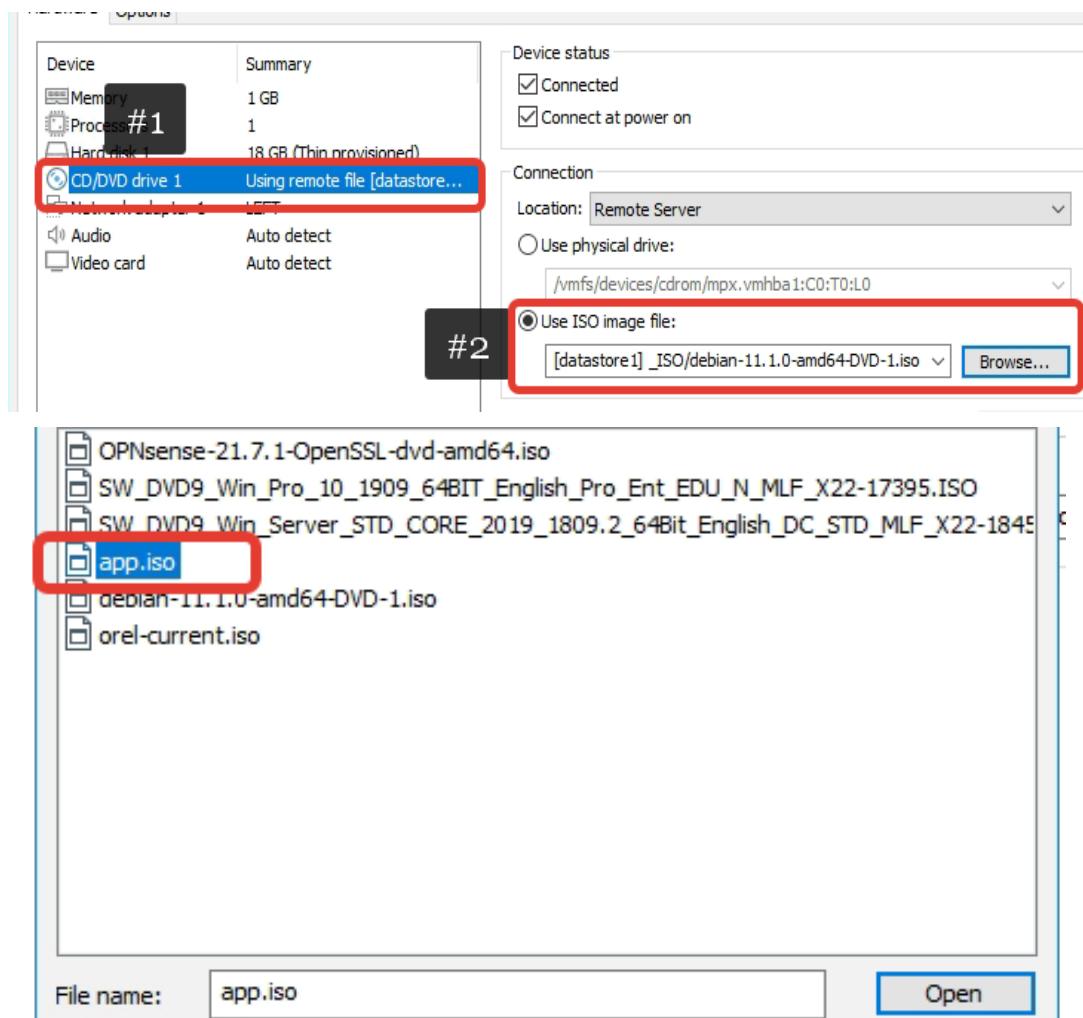
Для подключения диска ISO-формата к виртуальной машине необходимо выполнить следующие действия:

- правой кнопкой мыши нажать на имя машины, далее открыть настройки.

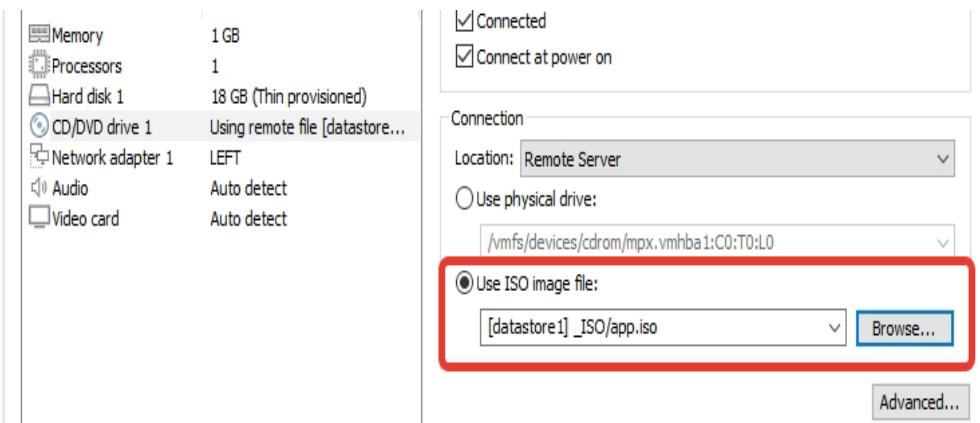


Следует выбрать устройство CD/DVD привод:

- указывается, что планируется смонтировать ISO-образ;
- с помощью Browse... (обзор) выбирается необходимый диск app.iso (важное уточнение: название образа с приложением Docker может отличаться, в данном примере он называется app.iso).



Стоит обратить внимание на то, что в окне программы Vmware Workstation изменился смонтированный ISO-файл.



После настройки виртуальной машины необходимо ввести команду `mount /dev/cdrom /media/cdrom`.

Данная команда монтирует устройство DVD-привод (`/dev/cdrom`) в директорию `(/media/cdrom)`.

Далее нужно скопировать архив `app.tar` с образа в домашнюю директорию `/root`  
`cp /media/cdrom/app.tar /root` (или, как в примере ниже, поставить символ «точка», при условии, что работа производится в папке `/root`).

```
root@WEB-L:~# mount /dev/cdrom /media/cdrom
mount: /media/cdrom0: WARNING: source write-protected, mounted read-only.
root@WEB-L:~# cp /media/cdrom/app.tar .
root@WEB-L:~# ls
app.tar
root@WEB-L:~#
```

После того, как приложение скопировано, образ необходимо импортировать в Docker.  
Для этого используется команда

`docker load < app.tar`

```
root@WEB-L:~# docker load < app.tar
8d3ac3489996: Loading layer 5.866MB/5.866MB
5302fd37b896: Loading layer 48.28MB/48.28MB
326c3133e665: Loading layer 14.23MB/14.23MB
f4626d9be0d5: Loading layer 14.61MB/14.61MB
65e59ee8da4c: Loading layer 5.041MB/5.041MB
fa7799618eb3: Loading layer 3.072KB/3.072KB
5f70bf18a086: Loading layer 1.024KB/1.024KB
9b029af87d1e: Loading layer 2.56KB/2.56KB
45dcf3341df4: Loading layer 3.072KB/3.072KB
Loaded image: app:latest
root@WEB-L:~#
```

Проверить, что образ импортировался корректно, можно при помощи команды `docker images`

```
root@WEB-L:~# docker images
REPOSITORY TAG IMAGE ID CREATED SIZE
app latest 735843fae2c4 23 minutes ago 83.4MB
root@WEB-L:~#
```

Далее приложение необходимо запустить. В данном примере приложение работает на 5000-м порту, поэтому необходимо запустить с прямой трансляцией 5000-го порта. Сделать это можно при помощи команды docker run -d -p 5000:5000 --name app app.

```
root@WEB-L:~# docker run -d -p 5000:5000 --name app app
b18a926176f8daafdb247427a8e7e6ce76361ab72f6f96fa6489c766ca1fe8c3
root@WEB-L:~#
```

### Комментарии к введенной команде

– docker — обращение к утилите docker;  
– run — опция, указывающая на запуск контейнера;  
– -d — включать контейнер в режиме daemon. Данный ключ необходим, так как Docker по умолчанию запускает контейнер в текущем stdout, и все логи отправляются в терминал пользователя;

– -p 5000:5000 — ключ, указывающий, как выполнять трансляцию обращений от адреса на хостовой машине к контейнеру. Первым числом указывается порт хоста, вторым числом порт контейнера. В инструкции к приложению может быть сказано, что оно работает на порту 1337, но необходимо обеспечить его работоспособность на порту 80 (стандартном для HTTP), в таком случае описать конфигурацию нужно будет так: docker run -d -p 80:1337;

– --name — указать имя контейнера Docker вручную. Если этого не сделать, Docker сформирует имя самостоятельно случайным образом, что может быть неудобно для дальнейшего администрирования;

- app — указывается имя контейнера;
- app — указывается имя образа, которое называется так же, как и сам контейнер.

Для внесения ясности следует запомнить, что в Docker существуют образы и контейнеры. Образ Docker — упаковывает приложение и среду, необходимые приложению для запуска, во что-то, похожее на архив (как, например, zip), что позволяет передавать данный образ на другие устройства, а **контейнер** является запущенным экземпляром образа на конкретной хостовой машине.

### Как проверить

Проверить, запущено ли приложение, можно при помощи команды docker ps.

```
root@WEB-L:~# docker ps
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS
NAMES
b18a926176f8 app "/bin/sh -c 'flask r..." 18 seconds ago Up 17 seconds 0.0.0.0:5000->500
0/tcp app
root@WEB-L:~# _
```

Посмотреть логи приложения можно при помощи команды docker logs app.

```
root@WEB-L:~# docker logs app
* Environment: production
  WARNING: This is a development server. Do not use it in a production deployment.
  Use a production WSGI server instead.
* Debug mode: off
* Running on all addresses.
  WARNING: This is a development server. Do not use it in a production deployment.
* Running on http://172.17.0.2:5000/ (Press CTRL+C to quit)
root@WEB-L:~#
```

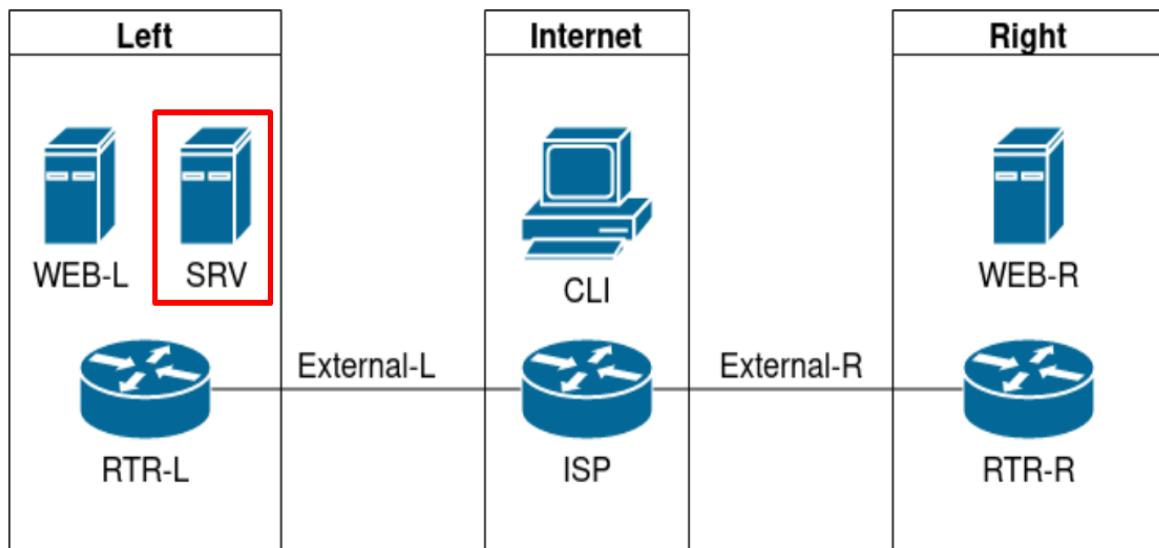
Протестировать работоспособность приложения можно при помощи curl, отправив запрос на 127.0.0.1:5000  
curl 127.0.0.1:5000

```
root@WEB-L:~# curl 127.0.0.1:5000
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>AppDocker0</title>
</head>
<body>
<p>
    Hello, fellow user, this is AppDemo0!
</p>
</body>
</html>root@WEB-L:~#
```

В ответ приходит HTML-код, который расположен в данном контейнере.  
Необходимо выполнить такую же операцию на машине WEB-R.

**Задание 2.** Настроить reverse-прокси на платформах управления трафиком.

В качестве reverse-прокси используем HAProxy. Так как необходимо обеспечить защищенное соединение через SSL (сертификаты, выписанные центром сертификации на машине SRV), перед конфигурированием HAProxy необходимо выпустить сертификаты.



Сделать это нужно на SRV. Сначала нужно сформировать файл запроса при помощи команды

```
./CA.pl -newreq-nodes
```

```
Country Name (2 letter code) [RU]: #1
State or Province Name (full name) [ . ]: #2
Locality Name (eg, city) [ ]: #3
Organization Name (eg, company) [DEMO.WSR]: #4
Organizational Unit Name (eg, section) [ . ] #5
Common Name (e.g. server FQDN or YOUR name) [ ]: www.demo.wsr #6
Email Address [ ]: #7
```

## **Комментарии к каждой строчке в данном конфигурационном файле**

- запрашивается код страны, оставляя значение по умолчанию, применяется значение из квадратных скобок, в данном случае — RU;
- запрашивается штат или область;
- запрашивается город;
- запрашивается имя организации, которая выпустила сертификат;
- запрашивается подразделение, которое выпускает сертификат;
- запрашивается имя, на которое будет выпущен сертификат, в данный момент необходимо указать имя — www.demo.wsr — доменное имя будущего сайта;
- почтовый адрес администратора.

Дальнейшие запросы скрипта можно опустить, нажав Enter:

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
==> 0
=====
Request is in newreq.pem, private key is in newkey.pem
root@SRV:/usr/lib/ssl/misc#
```

После того, как запрос был сформирован, его необходимо подписать. Сделать это можно при помощи команды

```
./CA.pl -sign
```

```
root@SRV:/usr/lib/ssl/misc# ./CA.pl -sign
=====
openssl ca -policy policy_anything -out newcert.pem -infiles newreq.pem
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for /var/ca/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
    Serial Number:
        4b:c5:d0:b2:6b:d5:b6:96:20:ea:15:8f:64:0e:cf:82:30:7b:b5:f8
    Validity
        Not Before: Jan  9 06:02:08 2022 GMT
        Not After : Oct 29 06:02:08 2024 GMT
    Subject:
        countryName      = RU
        stateOrProvinceName = .
        organizationName   = DEMO.WSR
        commonName         = www.demo.wsr
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        Netscape Comment:
            OpenSSL Generated Certificate
    X509v3 Subject Key Identifier:
        03:0C:48:81:4B:44:63:FB:5B:99:3C:F3:AE:8C:53:EF:5F:9B:D2:40
    X509v3 Authority Key Identifier:
        keyid:A7:4B:03:55:02:20:34:EE:19:98:CF:52:1A:5B:79:38:58:E2:A7:D2
```

Certificate is to be certified until Oct 29 06:02:08 2024 GMT (1024 days)
Sign the certificate? [y/n]:

Вводом Y можно согласиться с подпиской сертификата

```
Certificate is to be certified until Oct 29 06:02:08 2024 GMT (1024 days)
Sign the certificate? [y/n]:y
```

```
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
==> 0
```

```
-----  
Signed certificate is in newcert.pem  
root@SRV:/usr/lib/ssl/misc#
```

newcert.pem

Далее необходимо переместить сертификат и его приватный ключ в какую-нибудь отдельную директорию на сервере для удобства. В данном примере будет использована директория /root/www.

Используется команда ls, чтобы обнаружить новый сертификат newcert.pem в директории со скриптом CA.pl.

Создается папка /root/www - mkdir /root/www.

```
root@SRV:/usr/lib/ssl/misc# ls
CA.pl  newcert.pem  newkey.pem  newreq.pem  tsget  tsget.pl
root@SRV:/usr/lib/ssl/misc# _
```

Переносятся файлы в новую директорию с помощью команды mv.

```
root@SRV:~/www# mv /usr/lib/ssl/misc/newcert.pem /root/www/
root@SRV:~/www#
root@SRV:~/www# mv /usr/lib/ssl/misc/newkey.pem /root/www/
root@SRV:~/www# _
```

После этого данные сертификаты, а также корневой сертификат центра сертификации необходимо передать на платформы управления трафиком. Сделать это можно при помощи SCP.

Предварительно для RTR-L и RTR-R тоже необходимо отредактировать /etc/ssh/sshd\_config по аналогии с предыдущим заданием.

```
root@WEB-L:~# ls
app.tar  cacert.crt
root@WEB-L:~# _
```

Команда по отправке ключей и сертификата на RTR-L  
scp new\* root@192.168.100.254:/root/

```
root@SRV:~# scp new* root@192.168.100.254:/root/
```

```
-
```

Для RTR-R

```
scp new* root@172.16.100.254:/root/
```

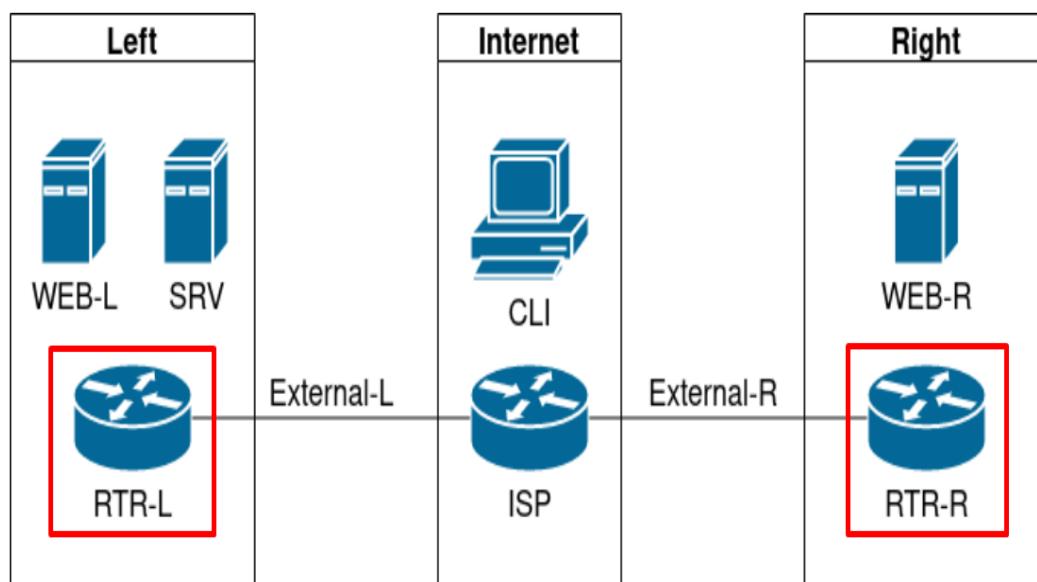
```
root@SRV:~# scp new* root@172.16.100.254:/root/
The authenticity of host '172.16.100.254 (172.16.100.254)' can't be established.
ECDSA key fingerprint is SHA256:K7INq9eRdgpbshUKKxmJXHSfU6rVueVo+pzJYzg6FF4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.16.100.254' (ECDSA) to the list of known hosts.
root@172.16.100.254's password:
newcert.pem                               100%   0
newkey.pem                                100%   0
```

Вслед за сертификатом и ключом сайта необходимо отправить и корневой сертификат:  
scp /var/ca/cacert.pem root@192.168.100.254:/root/

```
root@SRV:~# scp /var/ca/cacert.pem root@192.168.100.254:/root/
```

```
scp /var/ca/cacert.pem root@172.16.100.254:/root/
```

```
root@SRV:~# scp /var/ca/cacert.pem root@172.16.100.254:/root/
root@172.16.100.254's password:
cacert.pem
root@SRV:~# _
```



После этого на RTR-R и RTR-L необходимо установить HAProxy. Сделать это можно при помощи команды  
apt install haproxy

(пакет расположен на DVD-3).

Перед конфигурацией HAProxy следует создать папку /root/www для удобного хранения сертификатов. Перенести все скопированные сертификаты в данную папку

```
mkdir /root/www/  
cd /root/www/  
cp /root/newcert.pem /root/www/  
cp /root/newkey.pem /root/www/
```

Необходимо переименовать файл newkey.pem в newcert.pem.key с помощью команды  
mv newkey.pem newcert.pem.key

Следует убедиться с помощью команды ls в том, что сертификаты расположены в директории /root/www.

```
root@RTR-L:~/www# ls  
newcert.pem newcert.pem.key  
root@RTR-L:~/www# pwd  
/root/www  
root@RTR-L:~/www#
```

Следует убедиться, что на машине RTR-R данные файлы расположены по тому же пути — /root/www.

Данную команду необходимо повторить на устройстве RTR-L и убедиться, что данные файлы расположены там же.

Корневой сертификат следует скопировать в хранилище локальных сертификатов  
cp /root/cacert.pem /usr/local/share/ca-certificates/cacert.crt

Необходимо повторить данную команду на машине RTR-R соответственно.

После установки HAProxy и передачи сертификатов необходимо отредактировать основной конфигурационный файл HAProxy

```
/etc/haproxy/haproxy.cfg
```

В конец необходимо добавить секции backend и frontend.

RTR-R:

```
frontend www.demo.wsr  
    bind 5.5.5.100:80 #1  
    bind 5.5.5.100:443 ssl crt /root/www/newcert.pem #2  
    http-request redirect scheme https unless { ssl_fc } #3  
    default_backend web #4  
  
backend web  
    balance roundrobin #5  
    option httpchk #6  
    server web-r 172.16.100.100:5000 check #7  
    server web-l_4.4.4.100:443 check ssl ca-file /usr/local/share/ca-certificates/cacert.crt #8  
~  
"/etc/haproxy/haproxy.cfg" 47L, 1653B
```

47,14-21 Bot

#### Комментарии к строчкам, введенным в данном файле

– указывается, на каком адресе и порту HAProxy принимает запросы (80 — стандартный порт протокола HTTP);

– указывается, на каком адресе и порту HAProxy принимает запросы (443 — стандартный порт протокола HTTPS), а также указываются ключевые слова ssl crt /root/www/newcert.pem — указывается путь до сертификата в директории /root/www;

- данная опция включается для поддержки редиректа с HTTP на HTTPS с сохранением URL-запроса;
- указывается, к каким серверам ссылается frontend HAProxy;
- указывается, каким образом происходит балансировка нагрузки между контейнерами, в данном случае ROUNDROBIN — запросы идут по принципу 1 к 1, часть запросов на сервер WEB-R, а часть на WEB-L;
- указывается опция проверки, в данном случае HTTPCHK — это означает, что HAProxy периодически отправляет HTTP-запрос, а в случае отсутствия ответа HAProxy посчитает данный сервер нерабочим и перестанет отправлять клиентов на данную машину. В целом HAProxy имеет множество опций проверки доступности разных ресурсов;
- указывается первый сервер для балансировки, дописанная в конце опция check указывает на проверку данного сервера по указанному выше параметру;
- указывается второй сервер для балансировки, опция check указывает на проверку данного сервера, по указанному выше параметру **ssl ca-file** необходим.

На машине RTR-L необходимо выполнить аналогичную настройку, за исключением разных IP-адресов в параметре frontend

RTR-L:

```
frontend www.demo.wsr
    bind 4.4.4.100:80
    bind 4.4.4.100:443 ssl crt /root/www/newcert.pem
    http-request redirect scheme https unless { ssl_fc }
    default_backend web

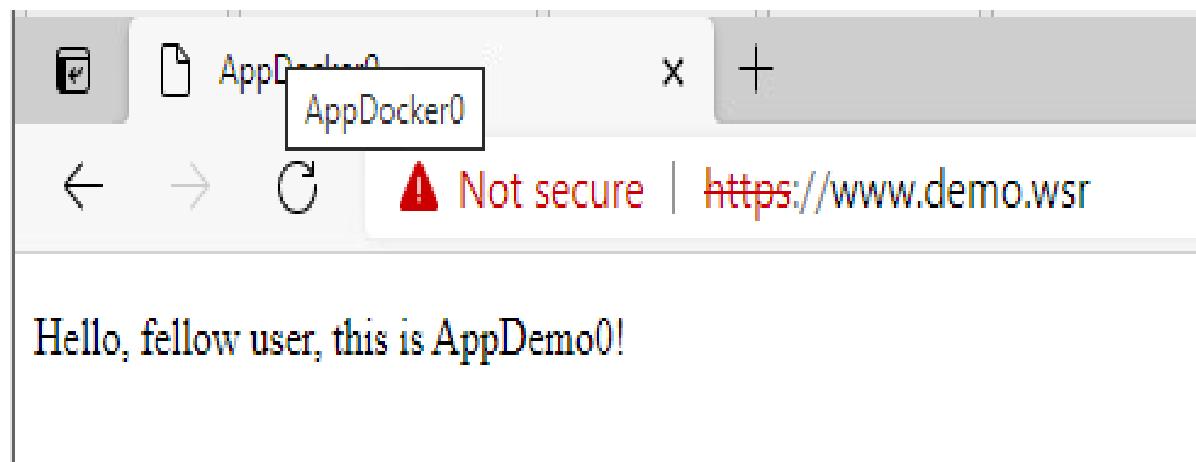
backend web
    balance roundrobin
    option httpchk
    server web-r 192.168.100.100:5000 check
    server web-l 5.5.5.100:443 check ssl ca-file /usr/local/share/ca-certificates/cacert.crt
```

### Как проверить

После того, как конфигурация изменена, необходимо перезапустить HAProxy с помощью команды

`systemctl restart haproxy`

и можно проверить с CLI доступность данного ресурса по имени `www.demo.wsr`:



### Дополнительная информация

- установка и настройка HAProxy ([https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/7/html/load\\_balancer\\_administration/install\\_haproxy\\_example1](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/load_balancer_administration/install_haproxy_example1));
- документация на HAProxy (<https://www.haproxy.com/documentation/hapee/latest/onelpage>);
- методы проксирования на основе HAProxy (<https://habr.com/ru/post/244027>);
- введение в HAProxy (<https://russianblogs.com/article/2064998131>).

# ПРИЛОЖЕНИЯ

## Приложение 1

### Разбор случая вариативности и загрузки OVA-шаблонов на ESXi-сервер

Во втором варианте задания рассматривается топология, при которой один из роутеров — это Cisco CSR (в данном примере машина RTR-L), а во втором случае — Debian Linux 11 (в данном примере это машина RTR-R).

Для выполнения данного курса необходимо скачать Cisco CSR.

Скачать Cisco CSR можно бесплатно, по учетной записи Cisco-академии — <https://software.cisco.com/download/home/284364978/type/282046477/release/Fuji-16.9.5>.

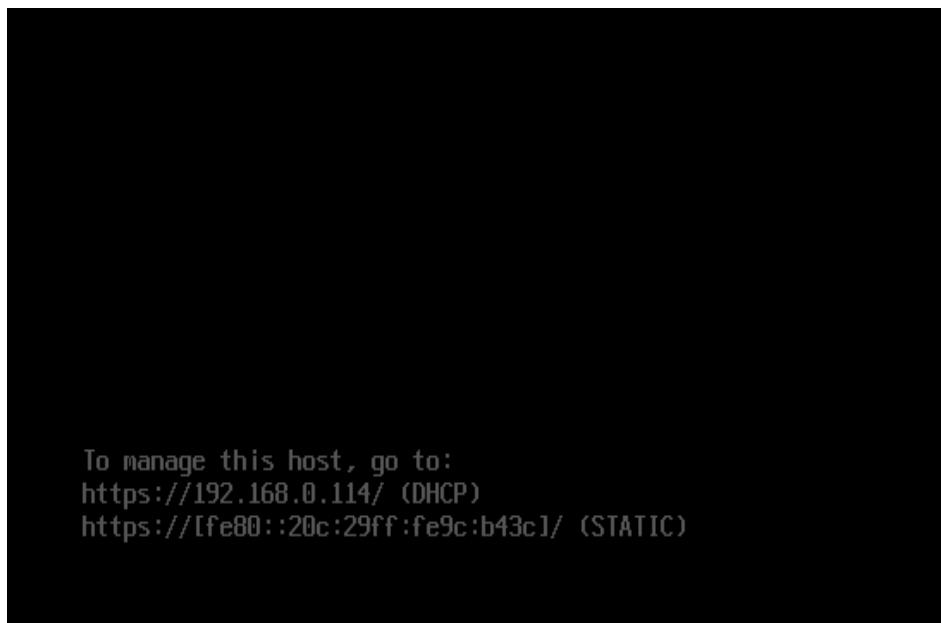
Скачать готовый OVA-шаблон стенда для демоэкзамена в 2022 г. можно по ссылке: <http://39.s300v4.ru:8088/demo/index.html>.

Необходимо выбрать необходимый формат. В случае, если работа происходит на базе платформы Vmware ESXi, требуется формат OVA.

Далее необходимо импортировать скачанный OVA-образ.

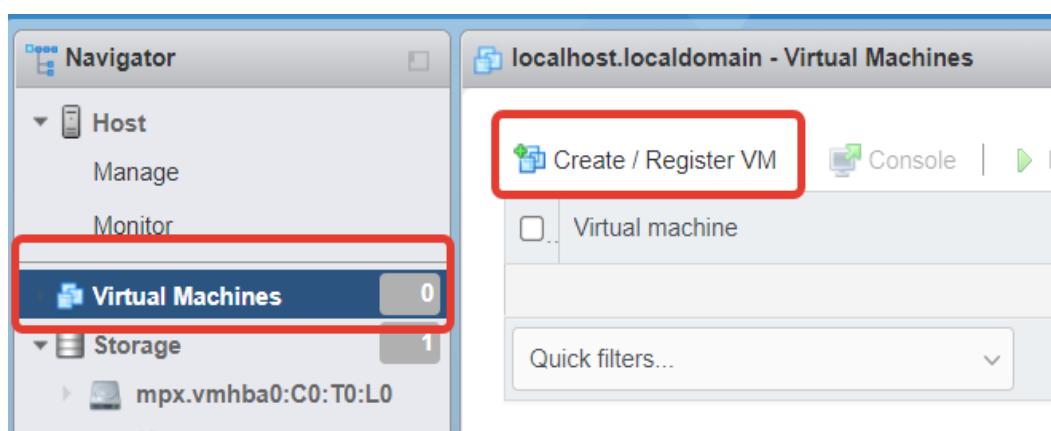
Если установлен Vmware ESXi 7.0 версии, то необходимо:

перейти по адресу ESXi-сервера, в данном примере это — 192.168.0.114.

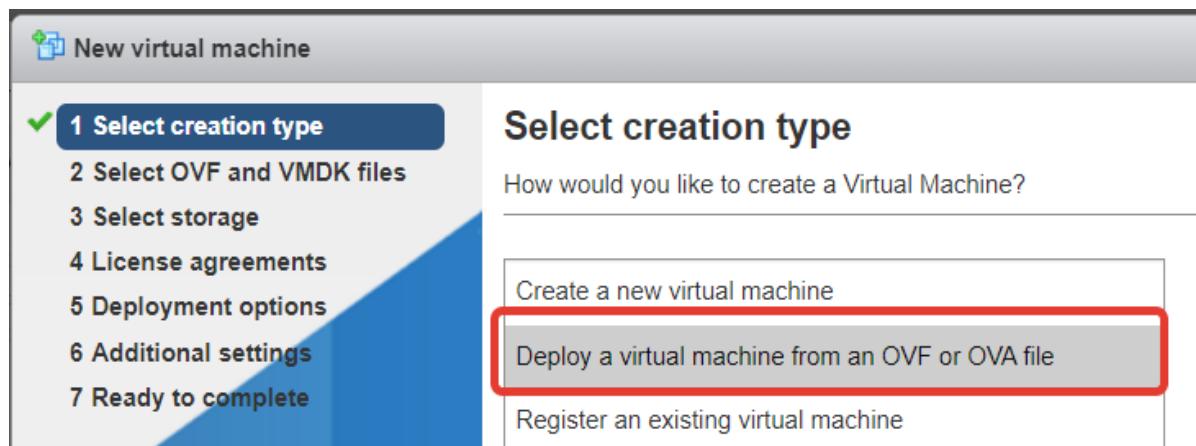


Главный экран блокировки Vmware ESXi

Открыть вкладку Virtual Machines, а затем Create/Register VM.

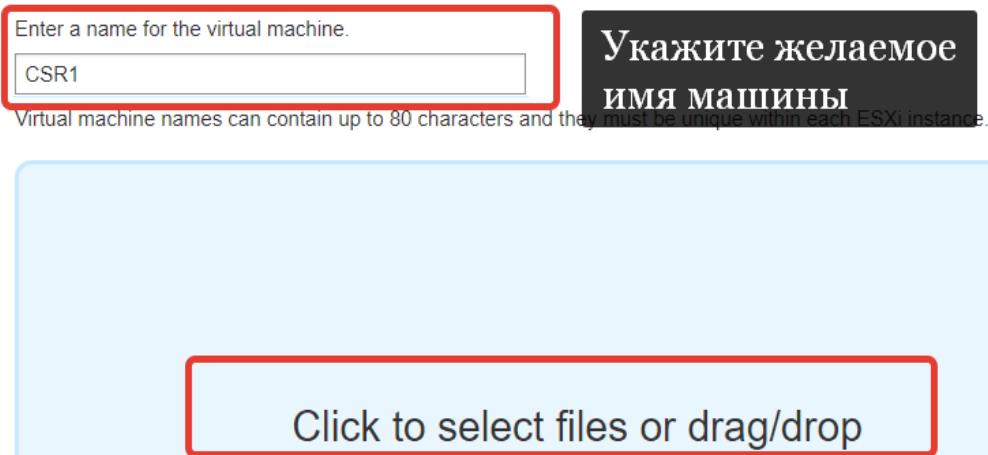


Выбрать параметр Deploy a virtual machine from an OVF or OVA file, то есть развертывание образа из OVA- или OVF-шаблона.



Далее система потребует задать имя виртуальной машины, которая будет установлена с помощью загрузки шаблона.

Затем необходимо выбрать параметр Click to select files or drag\drop для того, чтобы открыть файловый проводник и передать на сервер OVA-шаблон.



В открывшемся проводнике выбрать OVA-образ, который необходимо загрузить.

7.0U3c	2/5/2022 12:36	File folder	
17763.737.190906-2324.rs5_release_svc_r...	12/16/2021 16:58	UltraISO File	5,172,572 ...
App.iso	1/31/2022 9:20	UltraISO File	86,058 KB
appdockerdemo.tar.gz	2/5/2022 11:11	Архив WinRAR	120,847 KB
clonezilla-live-2.8.1-12-amd64.iso	2/4/2022 15:00	UltraISO File	331,776 KB
csr1000v-universalk9.16.11.01a.ova	1/8/2022 14:02	Open Virtualizatio...	439,490 KB
debian-11.2.0-amd64-DVD-1.iso	1/8/2022 14:02	UltraISO File	3,806,288 ...
orel-current.iso	9/10/2021 18:13	UltraISO File	4,225,264 ...
Untitled Diagram-Page-3.drawio.png	2/4/2022 16:58	PNG File	62 KB
WIN_CLI_ENT.iso	1/9/2022 12:12	UltraISO File	4,780,686 ...

Стоит отметить, что загрузка OVA-образа — не только Cisco CSR, но и любого другого — происходит так же.

Далее система потребует выбрать место хранения виртуальной машины, в данном случае — это пространство памяти с именем DATASTORE.

New virtual machine - CSR

1 Select creation type  
2 Select OVF and VMDK files  
**3 Select storage**  
4 Deployment options  
5 Ready to complete

### Select storage

Select the storage type and datastore

Standard Persistent Memory

Select a datastore for the virtual machine's configuration files and all of its' virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
DATASTORE	39.75 GB	38.34 GB	VMFS6	Supported	Single

1 items

### Deployment options

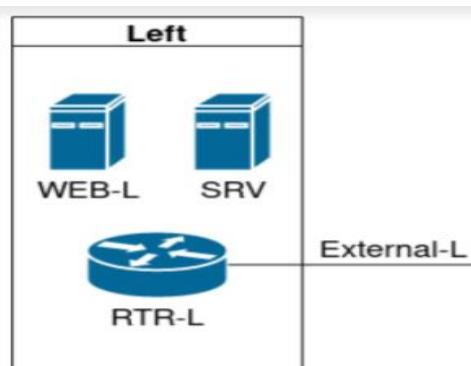
Select deployment options

Network mappings	GigabitEthernet1 GigabitEthernet2 GigabitEthernet3	VM Network VM Network VM Network
Deployment type	#2	Medium Medium hardware profile - 2 vCPUs, 4 GB RAM
Disk provisioning	<input checked="" type="radio"/> Thin <input type="radio"/> Thick	
Power on automatically	<input checked="" type="checkbox"/>	

Далее система укажет параметры, необходимые для развертывания образа Cisco CSR.

Под цифрой 1 указаны интерфейсы, которые по умолчанию создаются роутером Cisco CSR. Их может быть больше трех, но по умолчанию используются лишь они.

Назначьте их в соответствии с конкурсной документацией.



В данном случае конфигурация получается следующей:

Network mappings	GigabitEthernet1 GigabitEthernet2 GigabitEthernet3	External LEFT VM Network
------------------	--	--------------------------------

Интерфейс GigabitEthernet3 можно удалить в дальнейшем, так как он не используется. Под цифрой 2 указан тип развертывания, Cisco CSR представлен в разных версиях сборки, в зависимости от задач:

Small — версия на 1 процессор и 4 Гб ОЗУ;

Medium — версия на 2 процессора и 4 Гб ОЗУ;

Large — версия на 4 процессора и 4 Гб ОЗУ;

Large + DRAM Upgrade — версия на 4 процессора и 8 Гб ОЗУ. Также данная версия позволяет дополнительно увеличивать вычислительные мощности роутера, но для этого потребуется закупить лицензию и обновить образ Cisco CSR.

Для комфортной работы на стенде в рамках задания рекомендуется установить версию Medium.

Product	Cisco CSR 1000V Cloud Services Router
VM Name	CSR
Files	csr1000v_harddisk.vmdk csr1000v-universalk9.16.11.01a-vga.iso
Datastore	DATASTORE
Provisioning type	Thin
Network mappings	GigabitEthernet1: VM Network, GigabitEthernet2: VM Network, GigabitEthernet3: VM Network
Guest OS Name	Cisco IOS-XE Software
Profile	Minimal hardware profile - 1 vCPU, 4 GB RAM

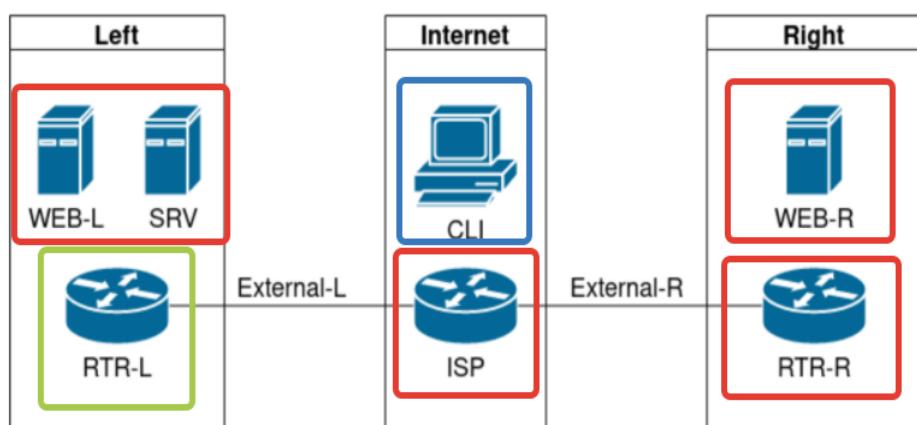


Do not refresh your browser while this VM is being deployed.



После этого необходимо нажать Next и затем завершить развертывание виртуальной машины Cisco CSR нажатием клавиши Finish.

Дождаться ее развертывания. Используя полученные навыки, реализовать стенд по следующему плану:



- красным цветом — Debian 11;
- зеленым — Cisco CSR;
- синим — Windows 10.

## Приложение 2

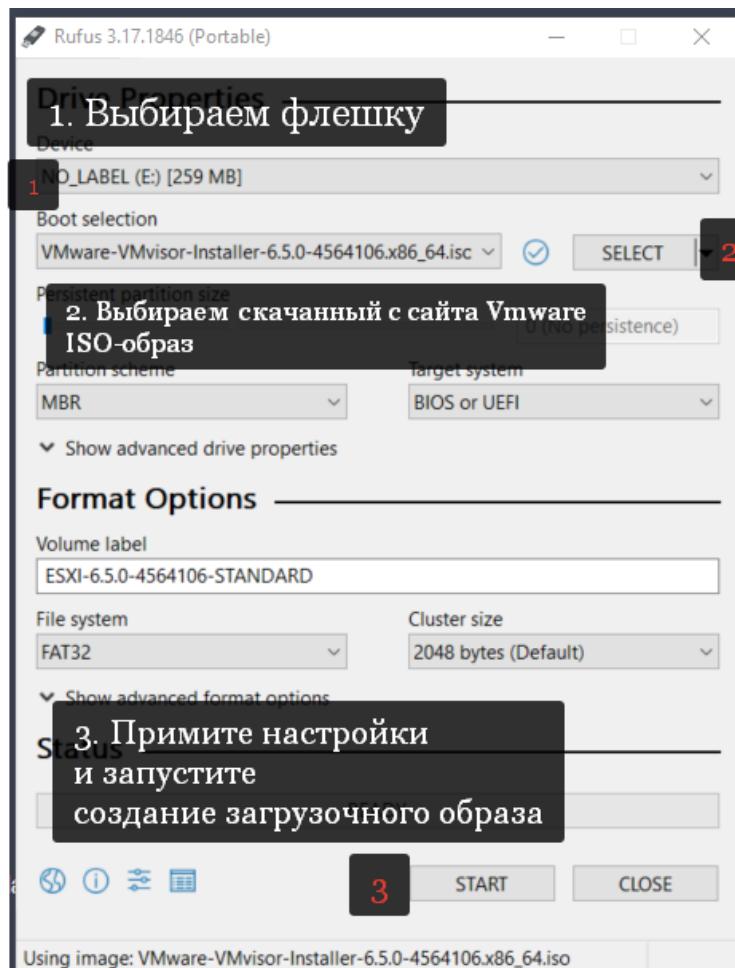
### Как создать самостоятельно рабочее место для подготовки студентов?

Для работы необходим сервер с характеристиками, соответствующими инфраструктурному листу. В качестве сервера рекомендуется использовать полноценные серверные решения. Расчет аппаратной мощности необходимо проводить следующим образом: расчет ресурсов для каждой ВМ, в зависимости от рекомендуемых системных требований ОС, и 10–15% ресурсов в качестве резервных.

На данном сервере необходимо развернуть сервер виртуализации ESXi. Дистрибутив VMware vSphere Hypervisor (ESXi) можно бесплатно скачать с сайта производителя. Пробная версия: 60 дней. Ее функционала достаточно, чтобы выдавать обучающемуся полный доступ к гипервизору ESXi с подготовленными виртуальными машинами, подключенными образами. Доступ с рабочих мест рекомендуется осуществлять через VMware Workstation 16 PRO (пробная версия: 30 дней):

– скачать ESXi актуальной версии с официального сайта компании Vmware ([https://customerconnect.vmware.com/en/downloads/info/slug/datacenter\\_cloud\\_infrastructure/vmware\\_vsphere/7\\_0](https://customerconnect.vmware.com/en/downloads/info/slug/datacenter_cloud_infrastructure/vmware_vsphere/7_0)) (для скачивания не требуется регистрация);

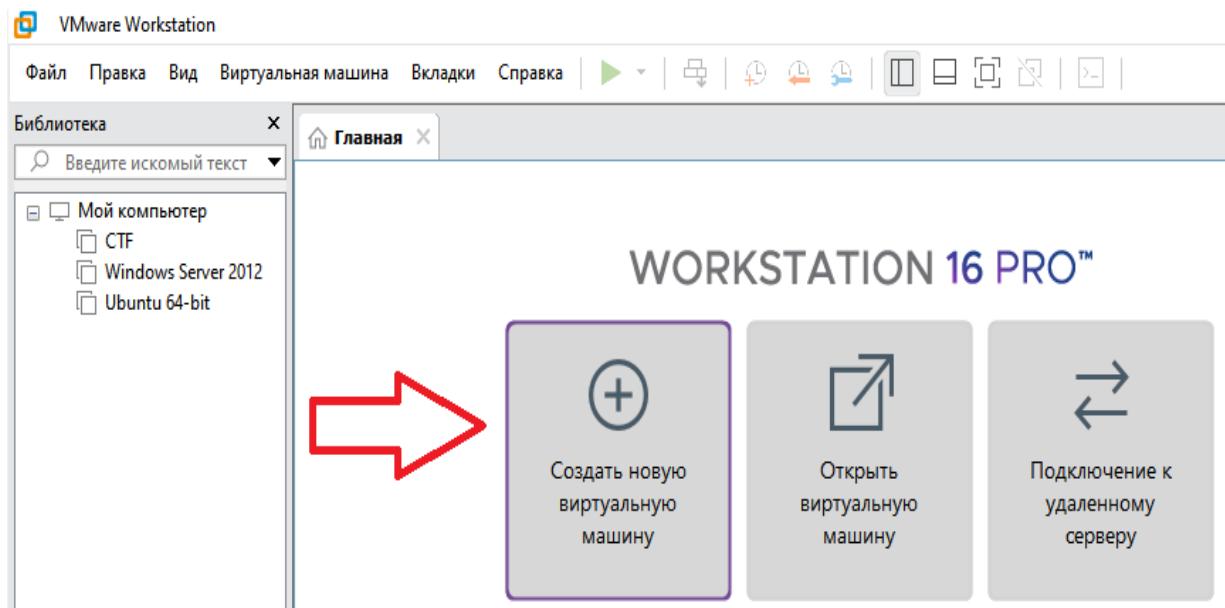
– используя Rufus (<https://rufus.ie/>), необходимо создать загрузочную флешку с ESXi, согласно скриншоту, указанному ниже:



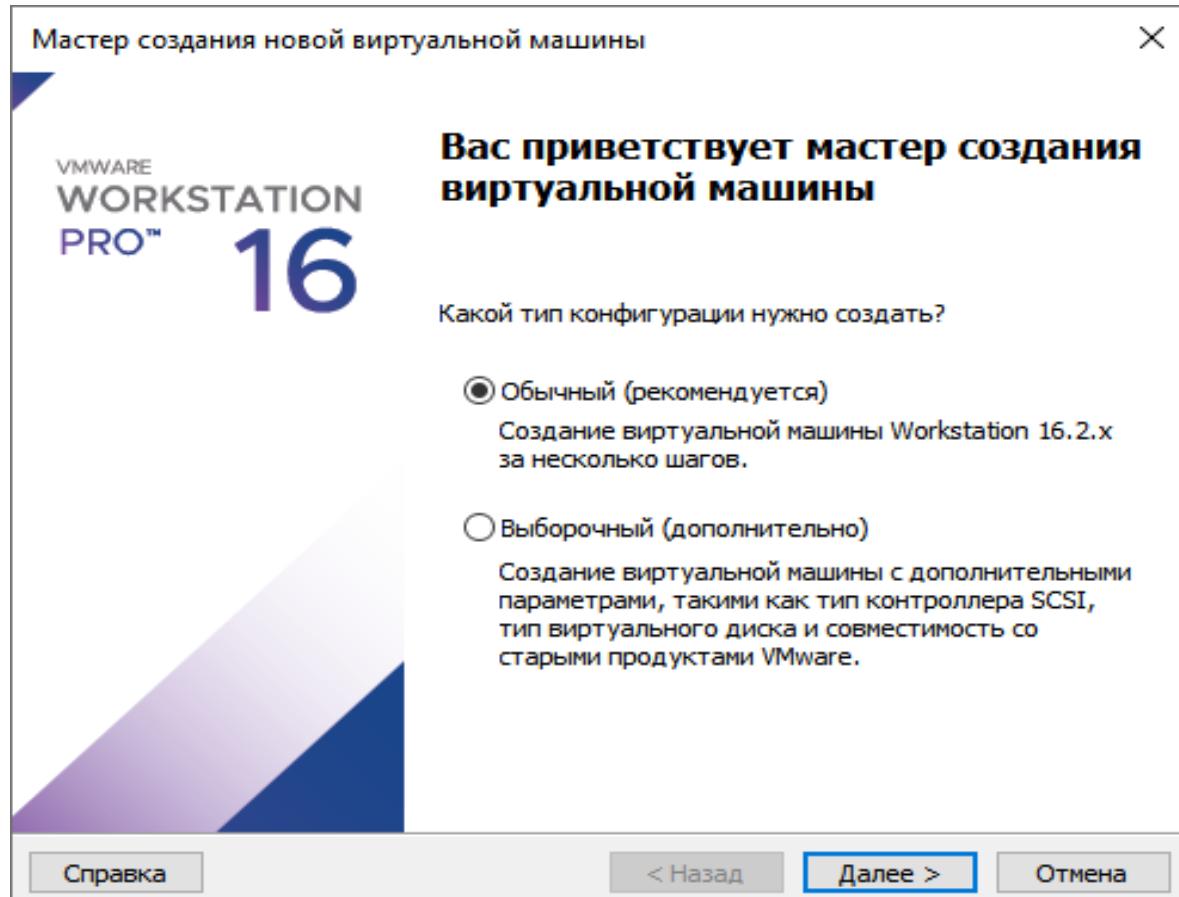
После чего подключить FLASH-накопитель к целевому серверу и в настройках BIOS сервера указать загрузку с данного устройства, а также включить поддержку виртуализации. (ссылка на то, как это может выглядеть, — <https://remontka.pro/zagruzka-s-fleshki/> <https://remontka.pro/enable-virtualization>). Затем можно будет наблюдать работу установщика Vmware ESXi. На скриншотах ниже можно увидеть версию установки ESXi версии 6.0.0, стоит обрат-

тить внимание — установка ESXi более старших версий (7.0.0, 7.0.0u2 и т. д.) не отличается от нее.

Демонстрация установки на VMware Workstation:



Необходимо выбрать пункт создания новой виртуальной машины.



Далее требуется выбрать тип конфигурации. В данном случае следует выбрать обычный.

## Мастер создания новой виртуальной машины

X

### Установка гостевой операционной системы

Виртуальная машина, это как физический компьютер для которой также необходима ОС. Как нужно установить гостевую ОС?

Установить из:

Установочный диск:

Нет доступных дисков

Файл образа установки (iso):

D:\VMware-VMvisor-Installer-7.0U1-16850804.x86\_64

Обзор...

VMware ESXi 7 and later обнаружен.

Я установлю операционную систему позже.

Виртуальная машина будет создана с пустого жесткого диска.

Справка

< Назад

Далее >

Отмена

Указывается путь до образа ESXi, скачанного с официального сайта.

## Мастер создания новой виртуальной машины

X

### Имя виртуальной машины

Какое имя использовать для этой виртуальной машины?

Имя виртуальной машины:

VMware ESXi 7 and later

Расположение:

D:\ESXi

Обзор...

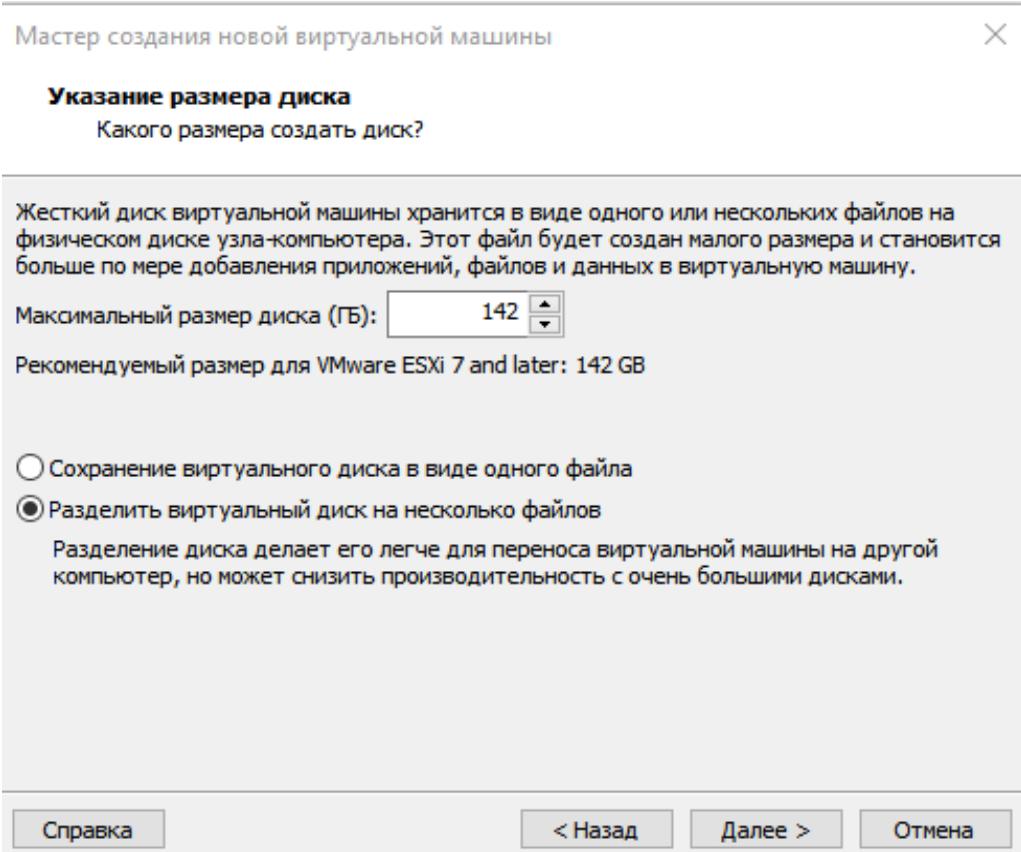
Расположение по умолчанию может быть изменено в меню Правка > Настройки.

< Назад

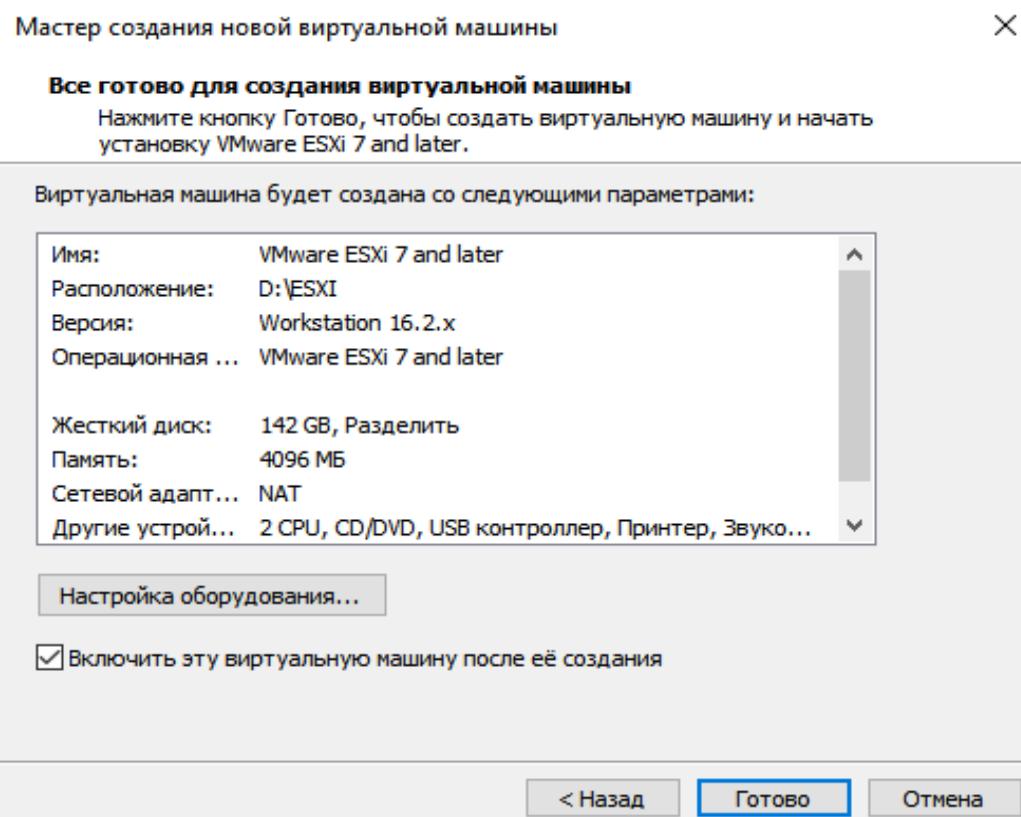
Далее >

Отмена

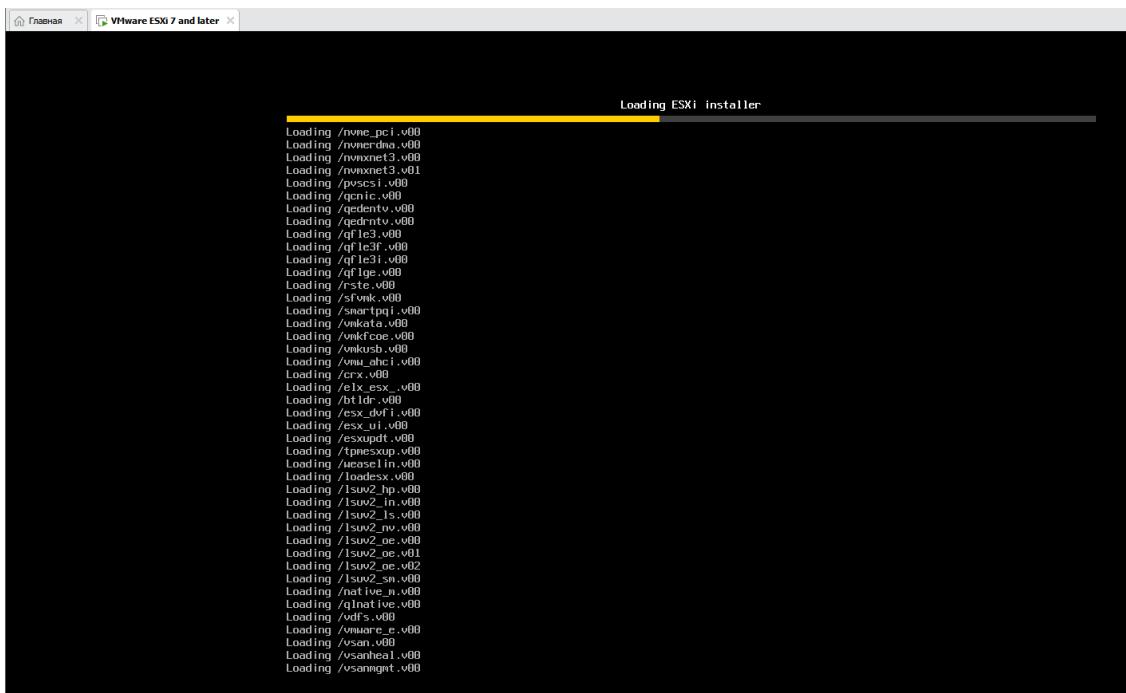
Указывается имя и расположение виртуальной машины.



Следует указать максимальный размер диска и выбрать пункт «Разделить виртуальный диск на несколько файлов».



Готово!



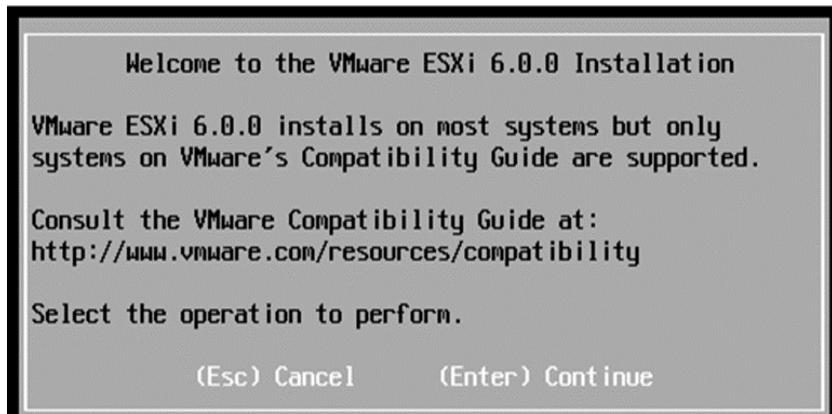
Ожидаем установки ESXi.



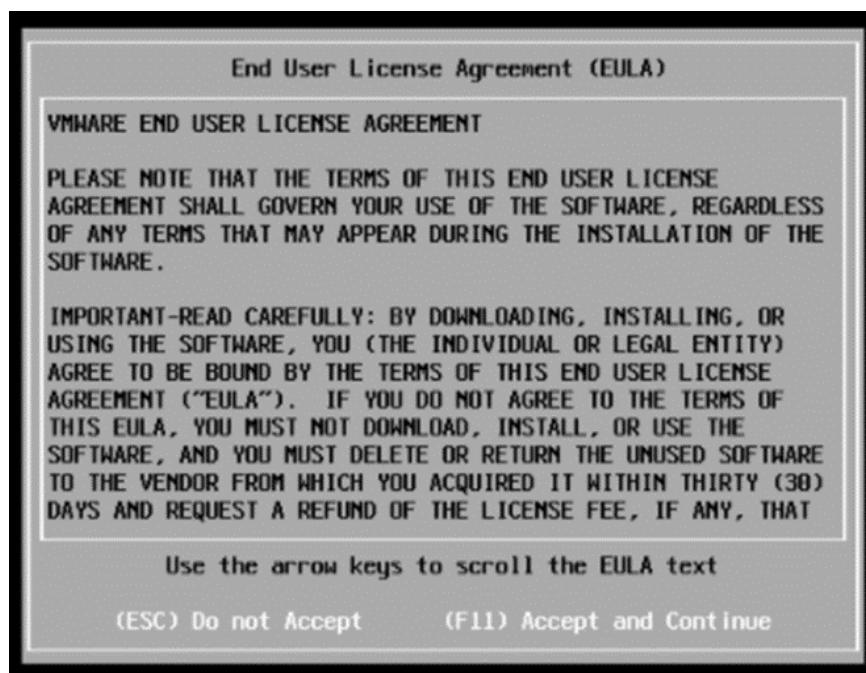
На данном скриншоте представлено приветственное окно установщика ESXi. Необходимо выбрать первый вариант в данном меню.



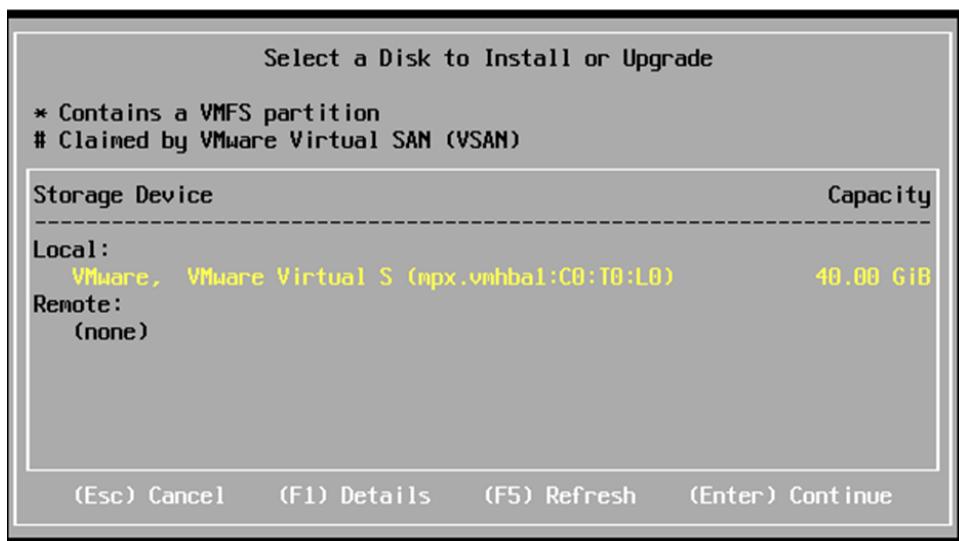
Ожидаем загрузки ESXi-установщика.



После открывается окно помощника по установке гипервизора, необходимо нажать Enter и перейти к следующему этапу установки.



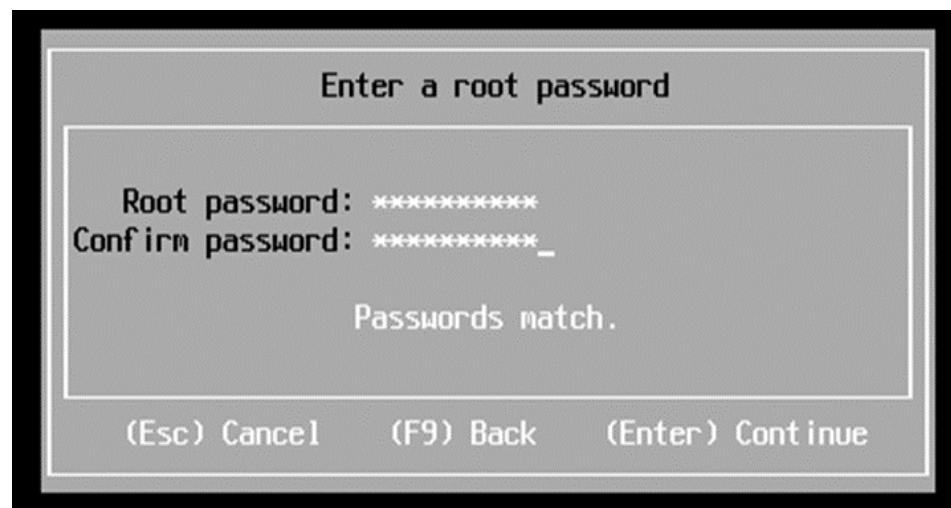
Следует нажать F11 и принять лицензионное соглашение.



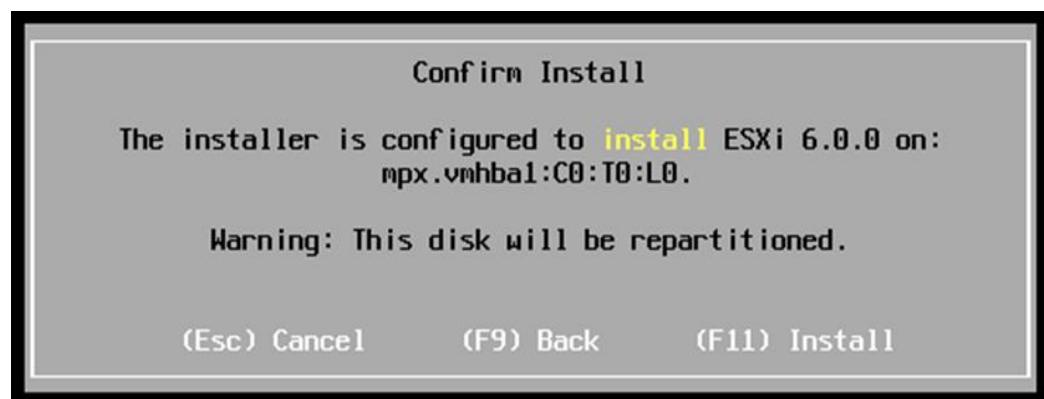
Далее необходимо выбрать постоянный диск, на котором расположится операционная система гипервизора.



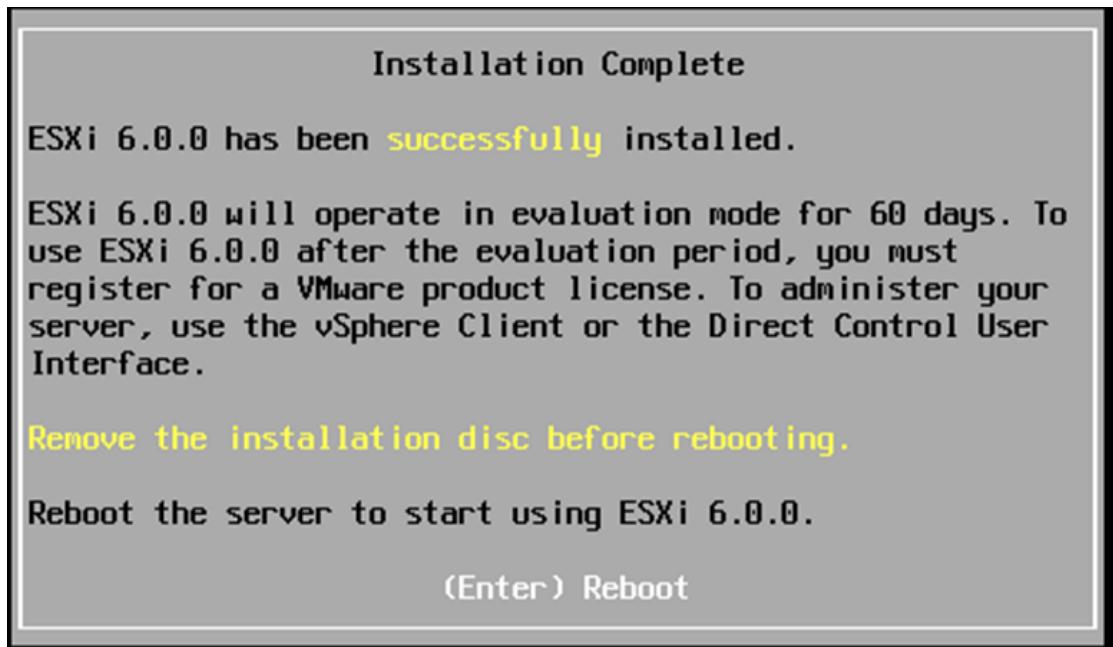
Затем выбирается язык системы. Рекомендуется US Default.



Необходимо установить пароль для пользователя root. Это основной пользователь в системе, которому доступен полный контроль над сервером. Следует запомнить введенный пароль.



После этого нужно подтвердить запуск установки с помощью кнопки F11. Происходит установка ОС, следует подождать некоторое время.



После необходимо нажать Enter. Сервер автоматически перезагрузится и запустится уже в гипервизор.

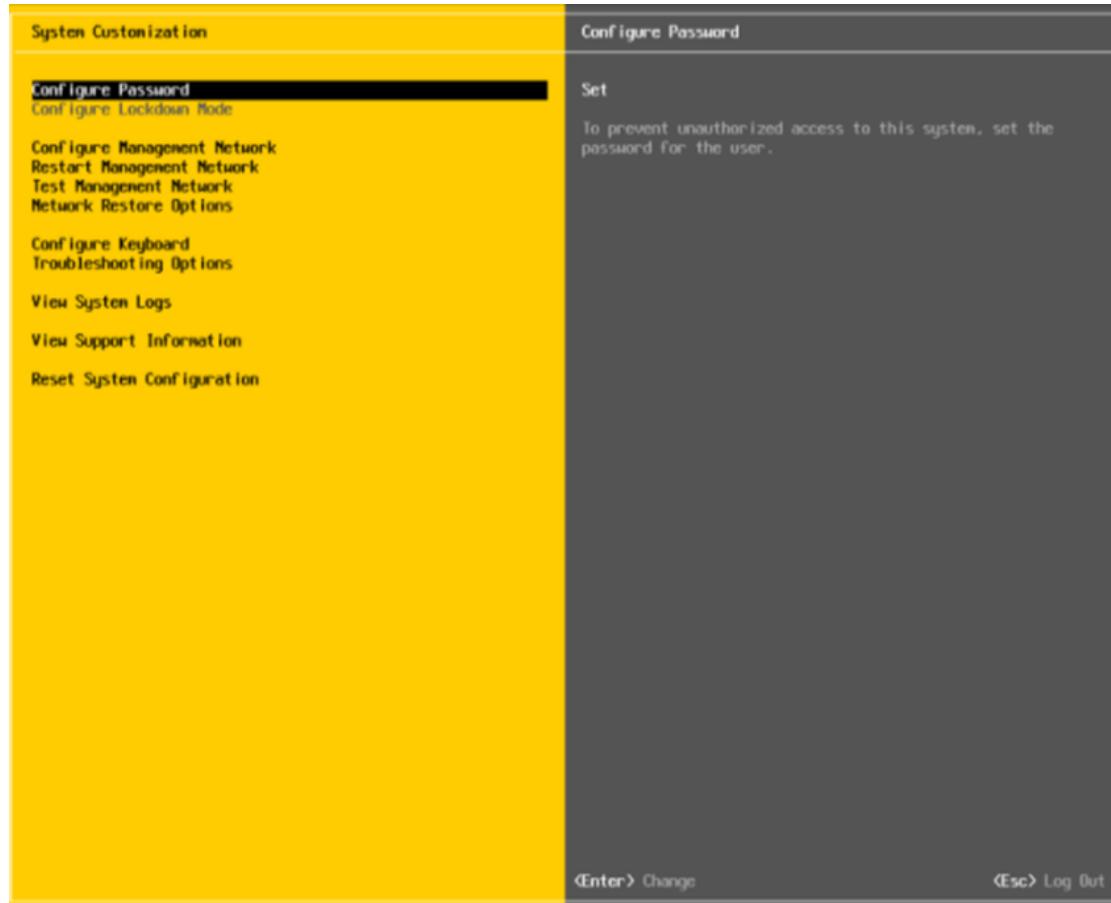


Установка сервера ESXi завершена, далее нужно его настроить.

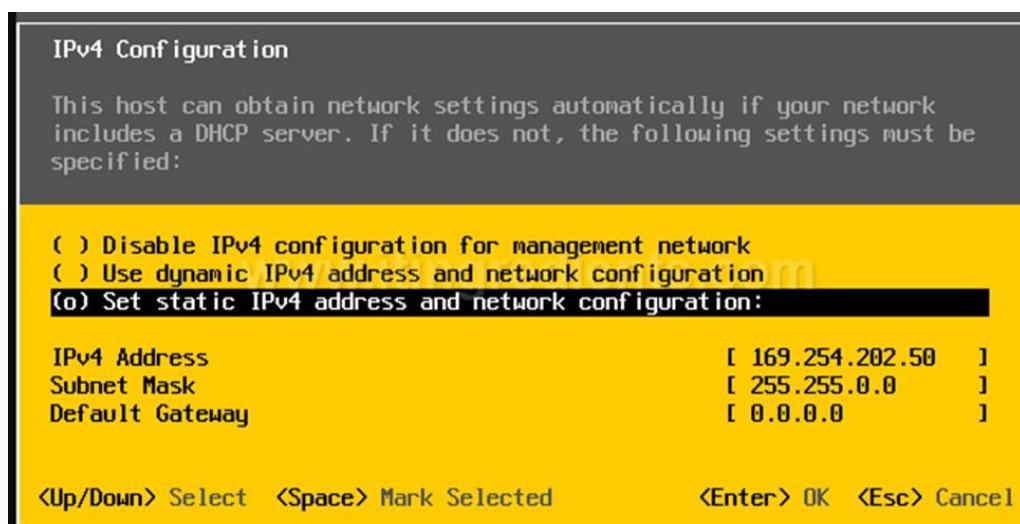
Если в сети присутствует DHCP-сервер, то можно будет наблюдать IP-адрес, который получил сервер автоматически. Стоит обратить внимание на этот адрес, он понадобится в дальнейшем.

Необходимо нажать клавишу F2 для перехода в меню конфигурации системы. ESXi на этом этапе потребует ввод пароля от root, необходимо использовать тот, что ранее был указан при установке ОС.

После чего откроется меню конфигурации системы.



Необходимо открыть вкладку Configure Management Network и настроить IP-адресацию.



Установить адрес, доступный в подсети. Стоит обратить внимание на то, что в сети не может быть два одинаковых IP-адреса. Необходимо указать тот, который не принадлежит в сети какому-либо устройству.

Установив какой-либо адрес, нужно открыть любой браузер (Microsoft Edge v. 79 и выше; Mozilla Firefox v. 60 и выше; Google Chrome v. 75 и выше) и перейти по настроенному адресу по протоколу HTTPS.

Откроется web-страница с ошибкой — указанием на незащищенное соединение, так как отсутствует сертификат. Чтобы все равно попасть на web-страницу, необходимо нажать кнопку Advanced и в открывшемся снизу тексте нажать Proceed to..., чтобы перейти даже при незащищенном соединении.



Your connection is not private

Attackers might be trying to steal your information from **10.11.8.209** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR\_CERT\_AUTHORITY\_INVALID

Help improve Chrome security by sending [logs of some pages you visit](#), limited system information, and [some page content](#) to Google. [Privacy policy](#)

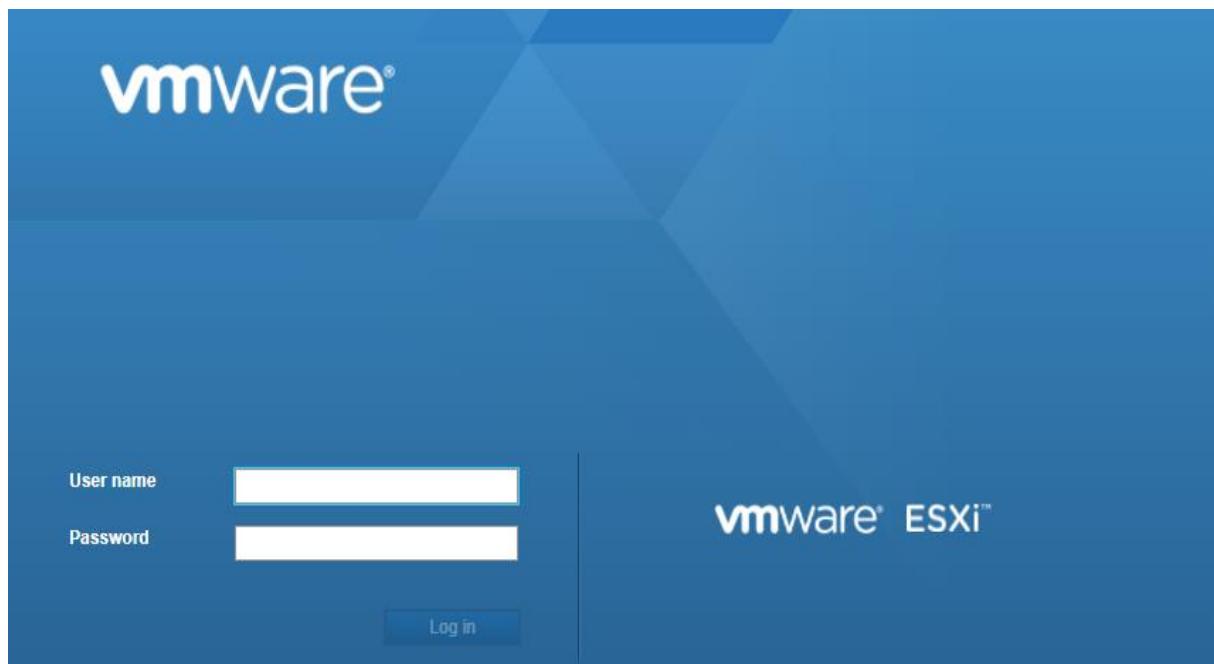
[Hide advanced](#)

[Back to safety](#)

This server could not prove that it is **10.11.8.209**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

[Proceed to 10.11.8.209 \(unsafe\)](#)

Далее откроется окно авторизации на веб-сайте, необходимо указать логин root и пароль, заявленный ранее при установке ESXi.



После ввода данных откроется панель управления сервером.

Откроется окно основных параметров вашего сервера.

localhost.au.team

Get vCenter Server | Create/Register VM | Shut down | Reboot | Refresh | Actions

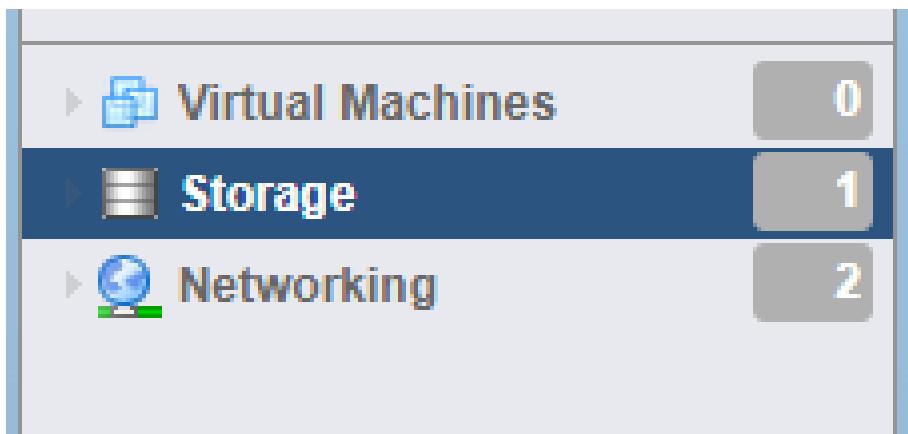
**localhost.au.team**

Version: 6.5.0 (Build 4564106)  
State: Normal (not connected to any vCenter Server)  
Uptime: 4 days

**Hardware**

Manufacturer	VMware, Inc.
Model	VMware7,1
CPU	14 CPUs x Intel(R) Xeon(R) Silver 4108 CPU @ 1.80GHz

Нужно перейти на вкладку Storage, там можно найти созданный по умолчанию Datastore-массив. На данном массиве будут храниться виртуальные машины, а также ISO-образы и прочие файлы, которые необходимо использовать для выполнения задания.



Во вкладке Datastore Browser можно посмотреть содержимое хранилища.

New datastore | Increase capacity | Register a VM | **Datastore browser** | Refresh | Actions

Name	Drive Type	Capacity
datastore1	Non-SSD	171.75 GB

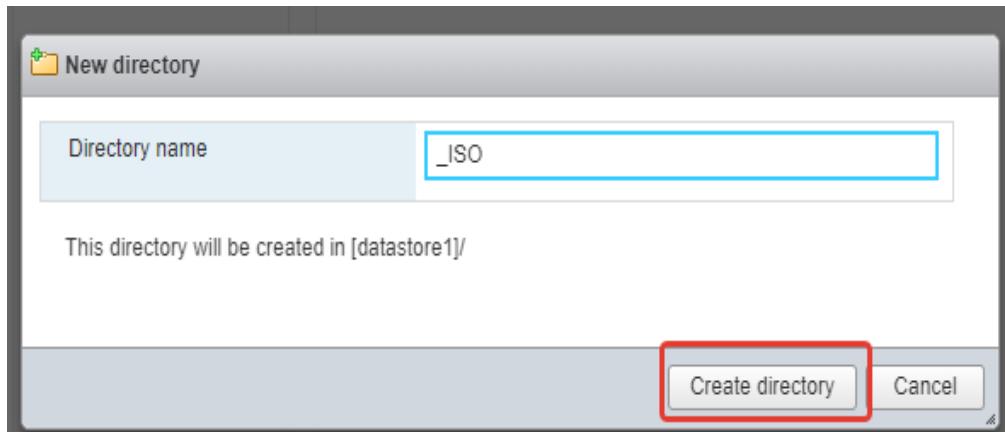
Необходимо создать директорию, в которой будут храниться все установочные ISO-образы.

**Datastore browser**

Upload Download Delete Move Copy **Create directory** Refresh

**datastore1** .sdd.sf

Можно использовать имя \_ISO, но сразу стоит упомянуть, что имя данной папки не является обязательным требованием, можно использовать любое название. Рекомендуется создавать папки только с использованием латиницы.



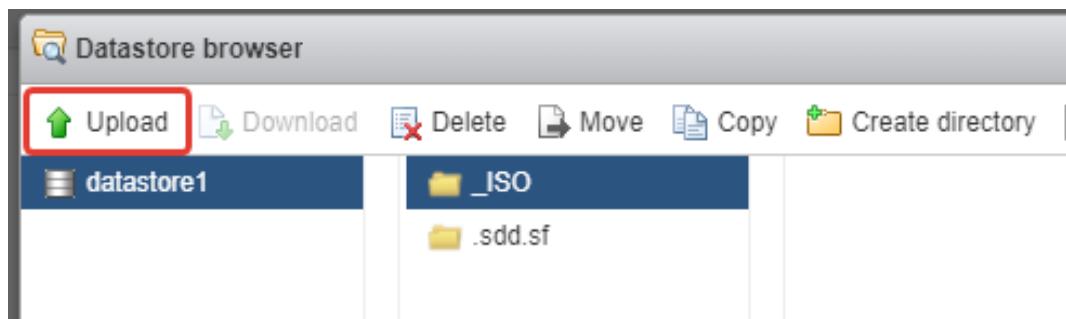
В созданную папку необходимо загрузить все ISO-образы, необходимые для сборки стенда. Для этого следует внимательно изучить вариант задания, которое используется.

В КОД 1.1 в таблице 1 уже указаны виртуальные машины, необходимые для работы, их название, системные требования и установленная операционная система. Снизу представлен пример.

Имя ВМ	ОС	ОЗУ	Кол-во ядер
RTR-L	Debian 11	2 Гб	2
	Cisco CSR		4
RTR-R	Debian 11	2 Гб	2
	Cisco CSR		4
SRV	Debian 11	2 Гб	2
	Windows Server 2019	4 Гб	4

Следует загрузить на стенд образ Debian 11, так как, в отличие от Cisco CSR, он не требует покупки лицензии и не требует столько ресурсов, как Windows Server 2019.

В качестве места хранения следует выбрать папку \_ISO, далее Upload.



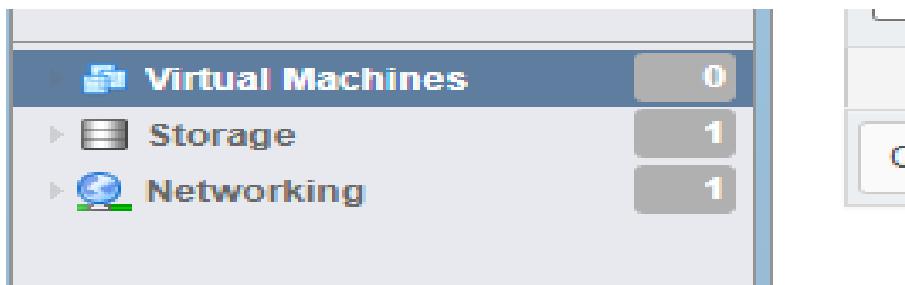
Выбирается для загрузки необходимый ISO-образ (необходимо скачать заранее с официального источника образов, в данном случае — <http://debian.mirror.iweb.com/debian-cd/current/amd64/iso-dvd/> DVD-1 для установки непосредственно системы, DVD-2 и DVD-3 для установки дополнительных пакетов, которые будут использоваться далее).

[Image]	12/4/2020 20:52	Лист Microsoft Ex...	13 KB
[Image] debian-11.1.0-amd64-DVD-1.iso	11/15/2021 14:10	UltraISO File	3,883,008 KB
[Image]	2/11/2021 9:34	Text Document	1 KB

В правом углу появилась полоса загрузки образа.

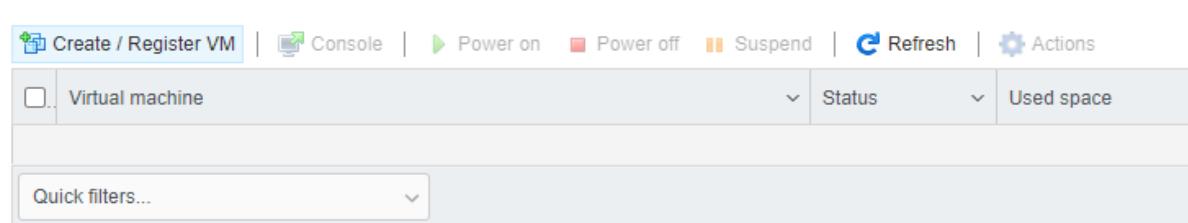


После загрузки ISO-образа необходимо перейти на вкладку Virtual Machines.

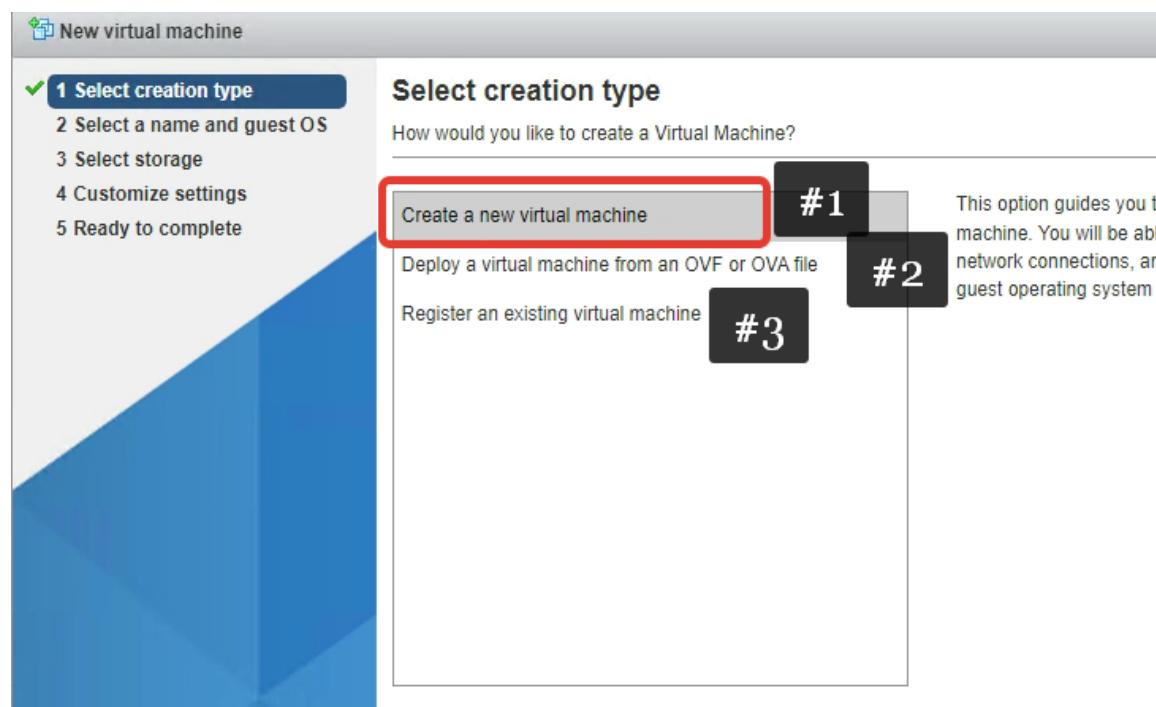


На данной вкладке в дальнейшем можно найти все уже имеющиеся виртуальные машины (ВМ), а также создать новые.

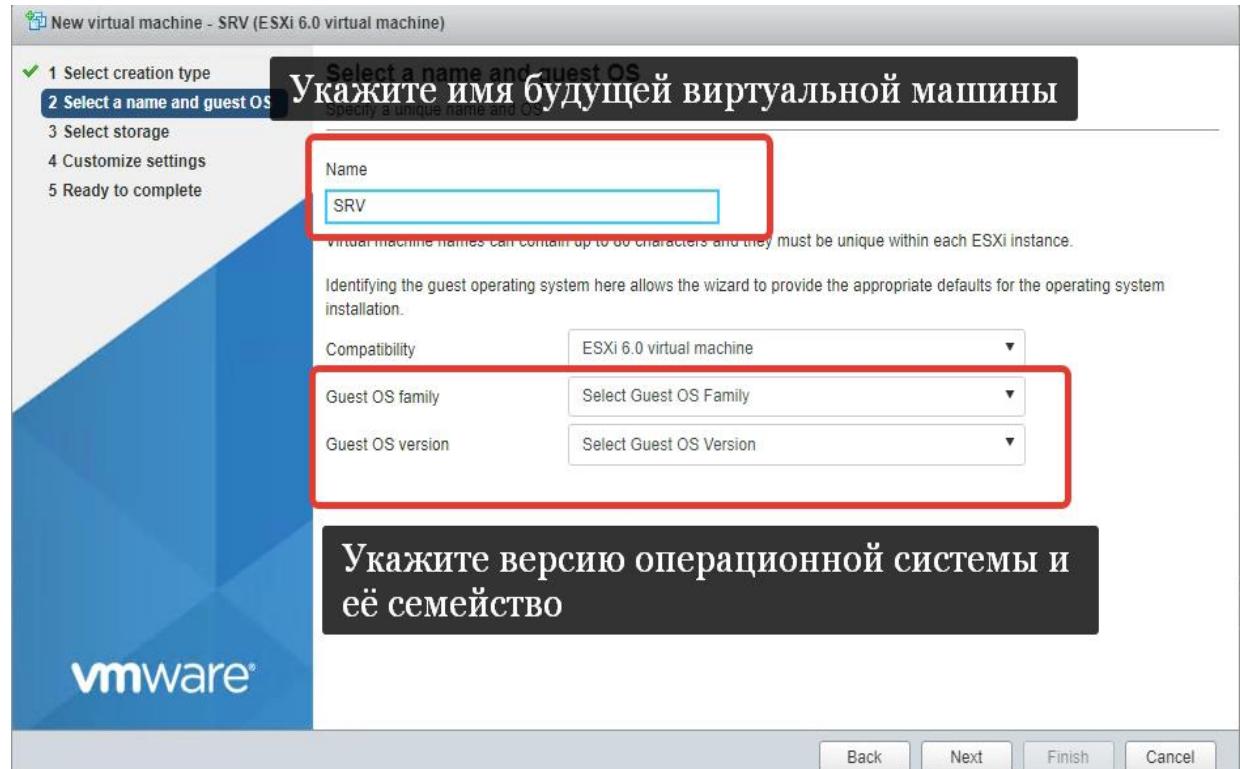
Теперь необходимо создать ВМ.



Create/Register VM — данный параметр используется, чтобы создать виртуальную машину:



- первый параметр, который выбирается сейчас для работы, указывает на создание новой виртуальной машины;
- второй параметр указывает на развертывание виртуальной машины из OVA-шаблона. Такой параметр будет необходим, если стоит задача развернуть скачанный шаблон;
- зарегистрировать уже существующую на сервере ESXi виртуальную машину.

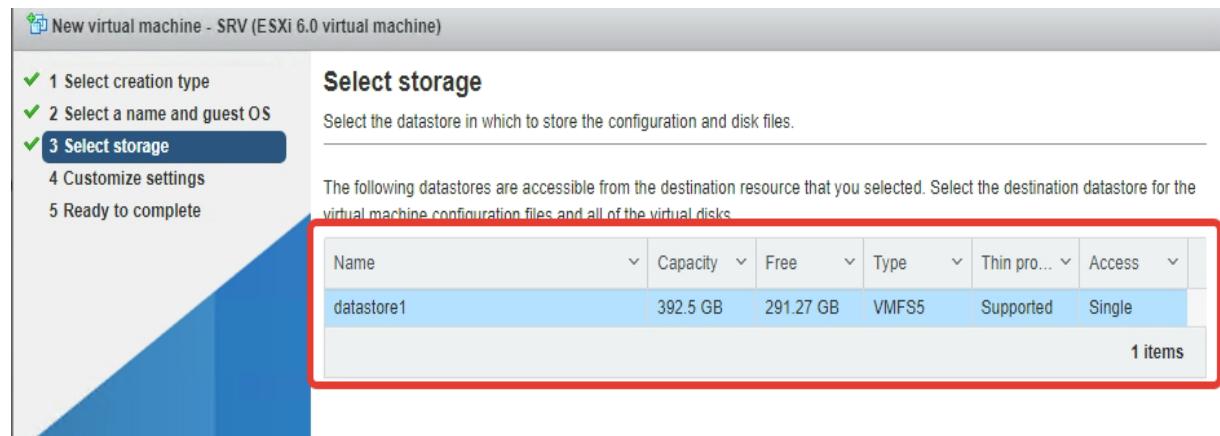


В данном примере машина SRV — Debian 11, поэтому следует выбрать параметры данного меню следующим образом:

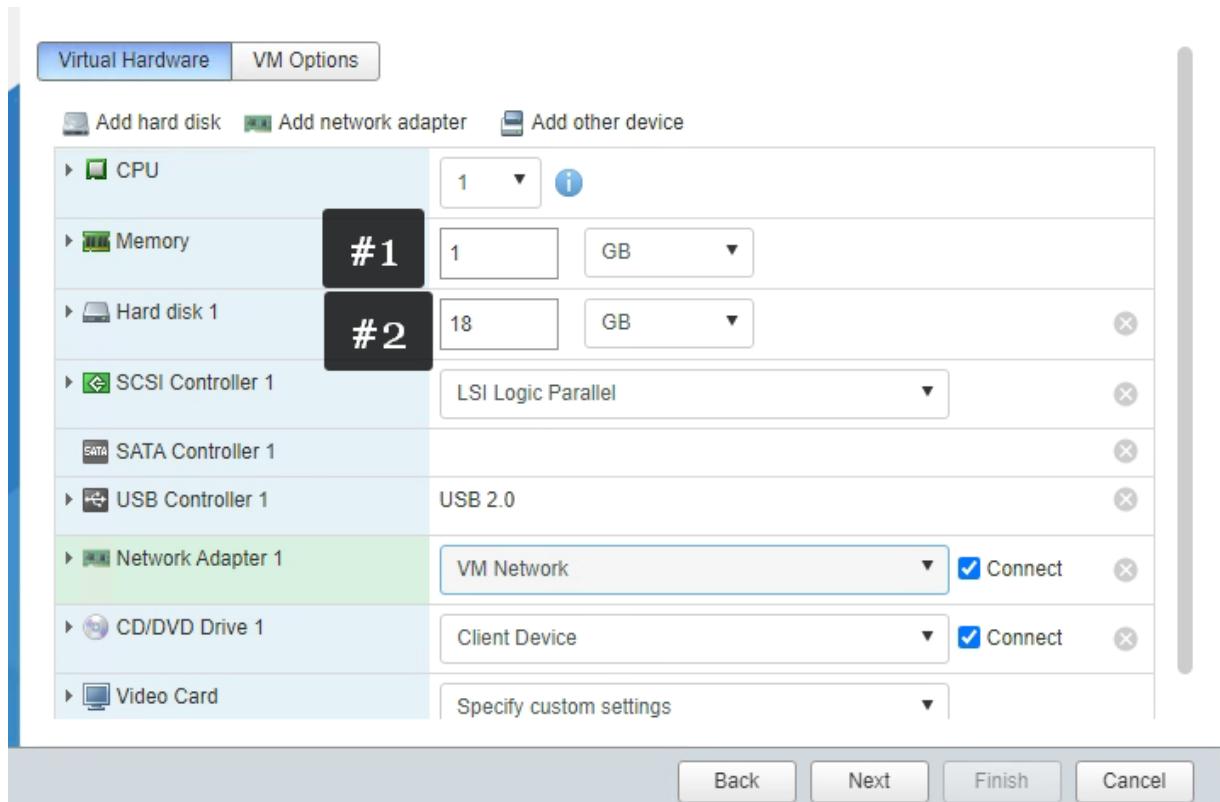
Guest OS family	Linux
Guest OS version	Other Linux (64-bit)

Other Linux, так как Debian 11 неизвестен серверу ESXi.

Далее необходимо выбрать место хранения виртуальной машины.



После чего откроется окно настроек виртуальной машины, следует настроить ее также, как указано на скриншоте:



– изменение выделяемого объема оперативной памяти с 384 Мб на 1 Гб;

– изменение выделяемого объема постоянной памяти с 8 Гб на 18 Гб.

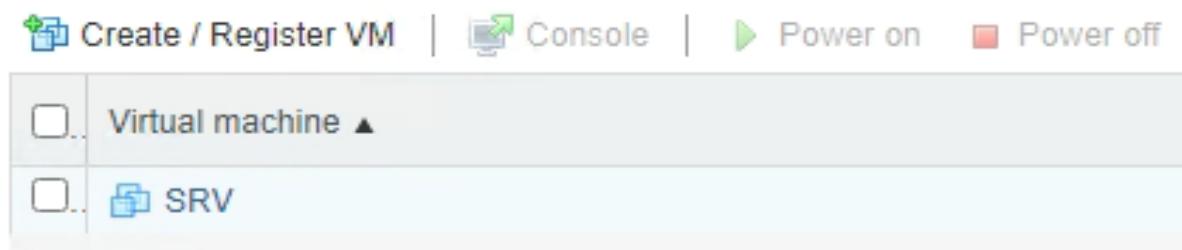
Далее внимательно следует изучить итоговый отчет о параметрах ВМ, которая сейчас появится на сервере.

Provisioning type	new
Name	SRV
Datastore	datastore1
Guest OS name	Other Linux (64-bit)
Compatibility	ESXi 6.0 virtual machine
vCPUs	1
Memory	1 GB
Network adapters	1
Network adapter 1 network	VM Network
Network adapter 1 type	E1000
SCSI Controller 1	LSI Logic Parallel
SATA Controller 1	New SATA controller
Hard disk 1	
Capacity	18GB
Datastore	datastore1

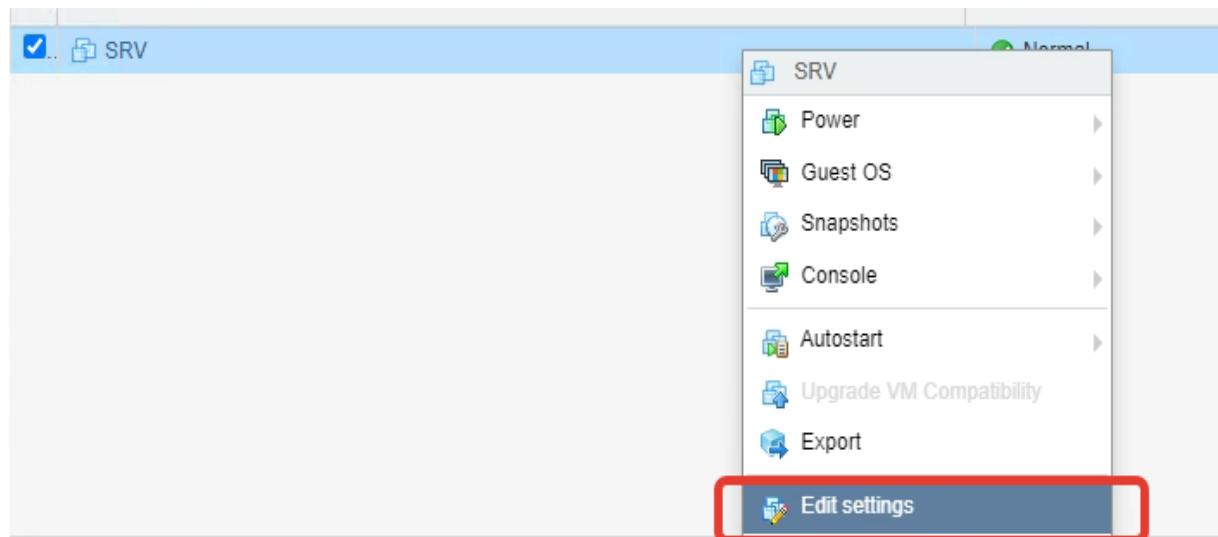
At the bottom are buttons for Back, Next, **Finish** (highlighted with a red box), and Cancel.

Виртуальная машина появилась в списке. На этапе настройки виртуальной машины умышленно не было упомянуто подключение ISO-образа для установки операционной системы на данную ВМ. Необходимо выполнить данную операцию сейчас; таким образом, до-

полнительно можно изучить, как изменять настройки виртуальных машин уже после развертывания.



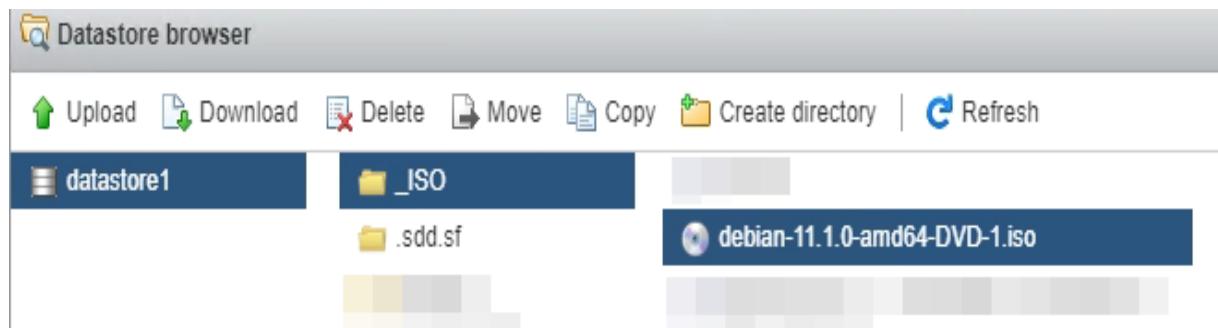
Правой кнопкой мыши необходимо нажать на виртуальную машину и выбрать Edit settings...



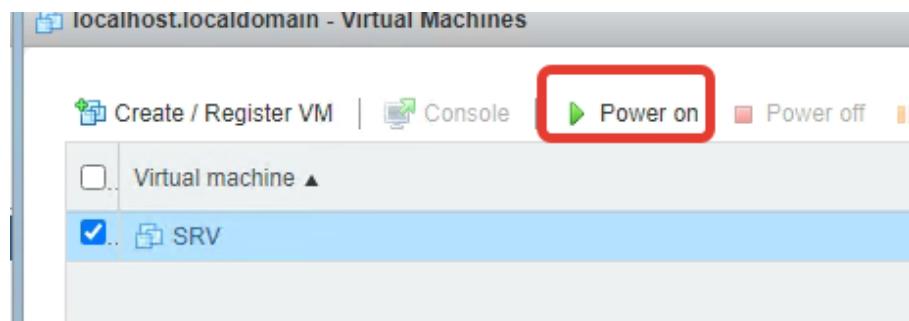
Необходимо найти в списке устройств CD/DVD Drive 1, открыть раскрывающийся список и выбрать параметр Datastore ISO File.



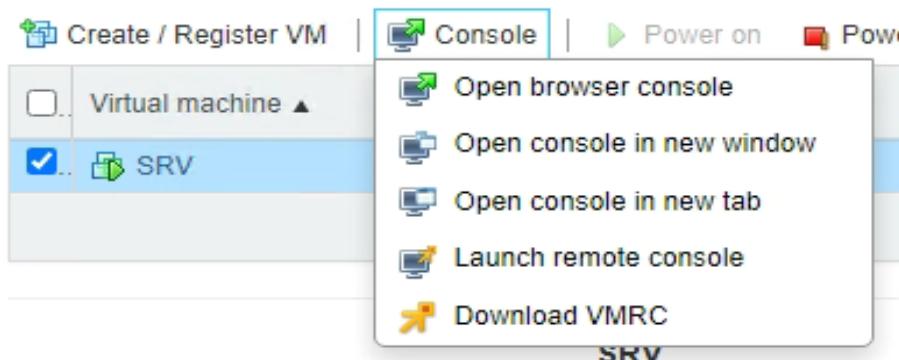
Откроется проводник Datastore, следует выбрать созданную ранее папку \_ISO и выбрать загруженный ISO-образ.



После этого нажать Save и запустить виртуальную машину.



Для того, чтобы подключиться к виртуальной машине, используется параметр Console, в появившемся списке отображены все способы подключения к виртуальной машине:



– open browser console — откроет браузерную консоль в текущей вкладке браузера;  
– open console in new windows — откроет браузерную консоль в новом окне браузера;  
– open console in new tab — откроет браузерную консоль в новой вкладке браузера;  
– launch remote console — запустит проприетарный протокол VMRC для подключения к виртуальной машине, данный способ работы самый предпочтительный, для его работы необходимо иметь на компьютере установленную программу Vmware Workstation или Vmware Remote Console;

– Download VMRC — в случае, если отсутствует программа Vmware Remote Console, нажатие на данный параметр откроет официальный сайт Vmware для загрузки данного ПО. Оно полностью бесплатно.

Рекомендуется пользоваться Remote Console — выбирая данный вариант, браузер автоматически предупредит об открытии стороннего приложения Vmware. В примере ниже браузер открывает Workstation, установленный на ПК.

Открыть приложение "Vmware Workstation"?

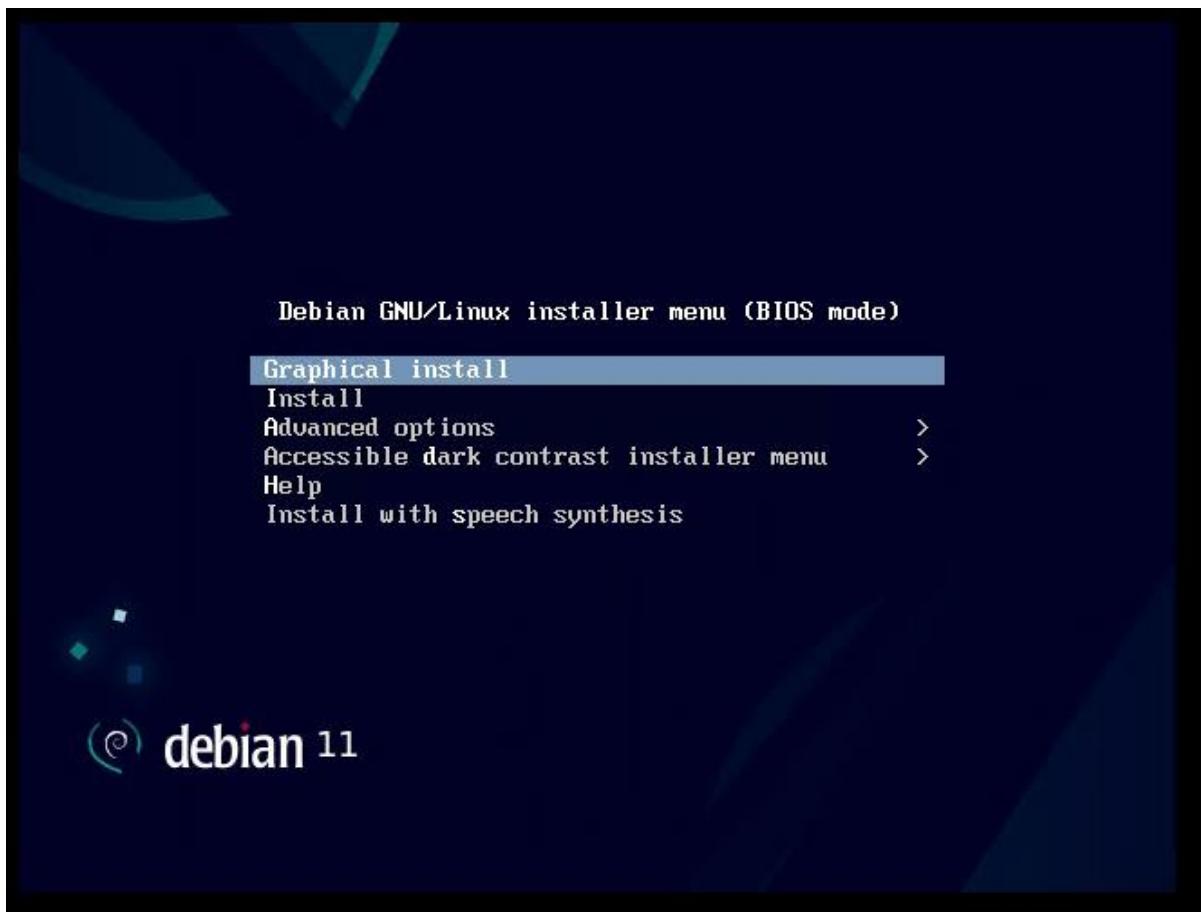
Сайт <https://> собирается открыть это приложение.

Всегда разрешать сайту <https://> открывать ссылки этого типа в связанном приложении

[Открыть приложение "Vmware Workstation"](#)

[Отмена](#)

Открывается установщик операционной системы Debian 11, установку необходимо выполнить самостоятельно (руководство по установке — <https://www.debian.org/releases/bullseye/installmanual>).



Теперь можно перейти к настройке машины на Windows 10 или Windows Server, не забывая при этом загрузить на сервер ESXi ISO-образ Windows Server 2019.

Далее указываются только отличающиеся от установки SRV параметры.

## Select a name and guest OS

Specify a unique name and OS

Name

DC

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance

Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

Compatibility

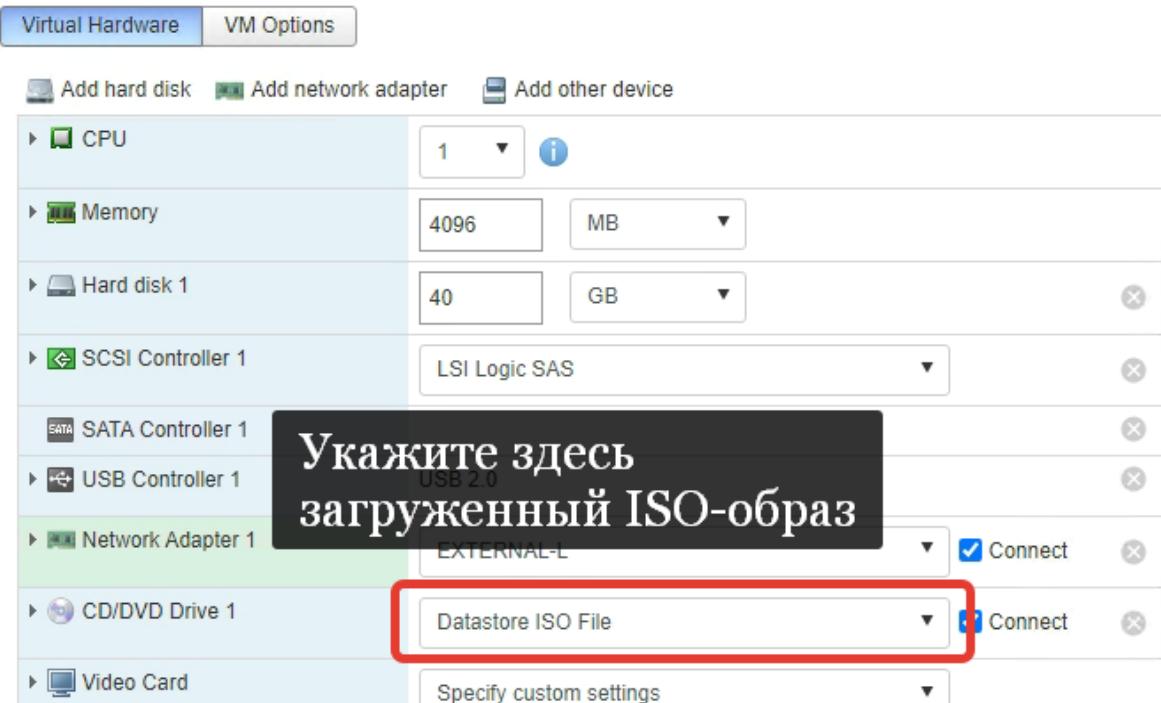
ESXi 6.0 virtual machine

Guest OS family

Windows

Guest OS version

Microsoft Windows Server 2016 (64-bit)



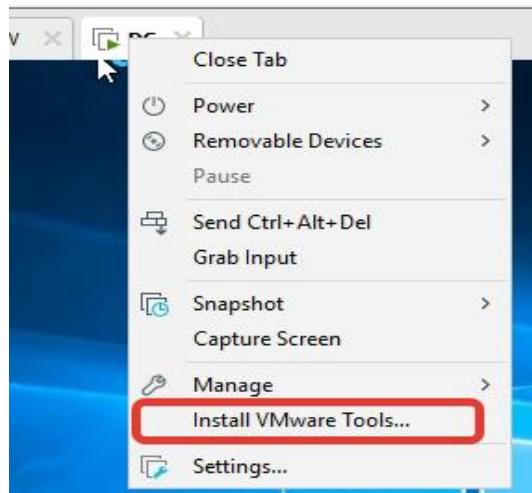
После этого необходимо подключиться к машине DC с помощью Remote Console.



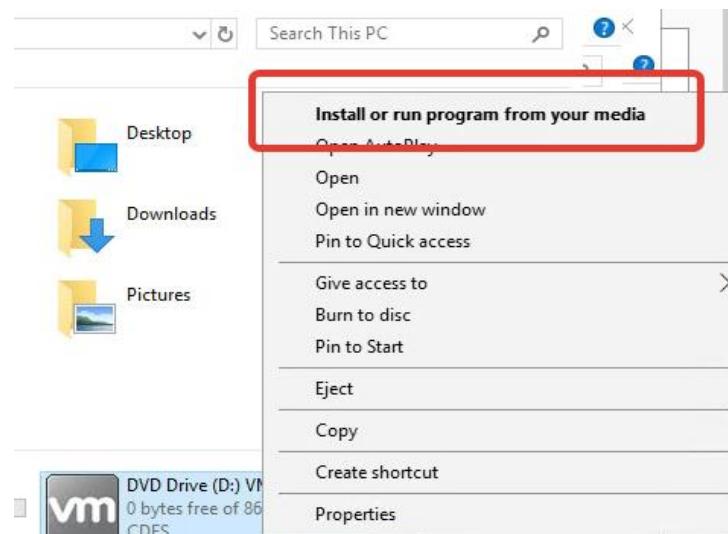
Следует выполнить стандартную установку Windows Server 2019.

После установки операционной системы стоит обратить внимание на то, что Windows работает медленно, работать с помощью мыши неудобно и так далее. Чтобы исправить это, необходимо установить Vmware Tools.

Правой кнопкой мыши необходимо нажать на имя виртуальной машины и выбрать параметр Install Vmware Tools.



Затем открыть Windows-проводник — там можно обнаружить подключенный диск D. Необходимо нажать на него правой кнопкой мыши и выбрать параметр Install or run program from your media.

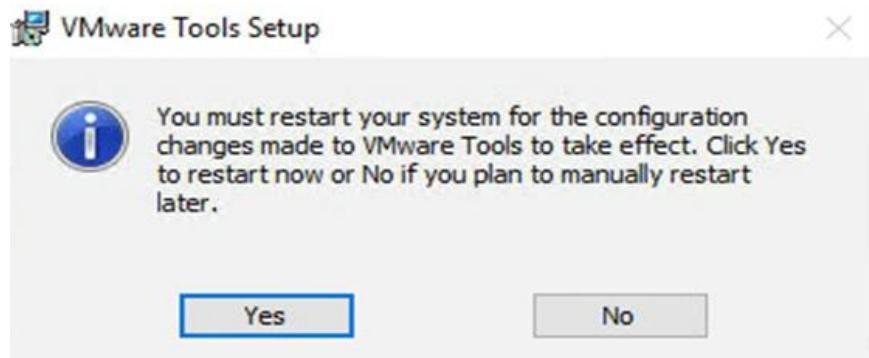


Откроется установщик Vmware Tools.



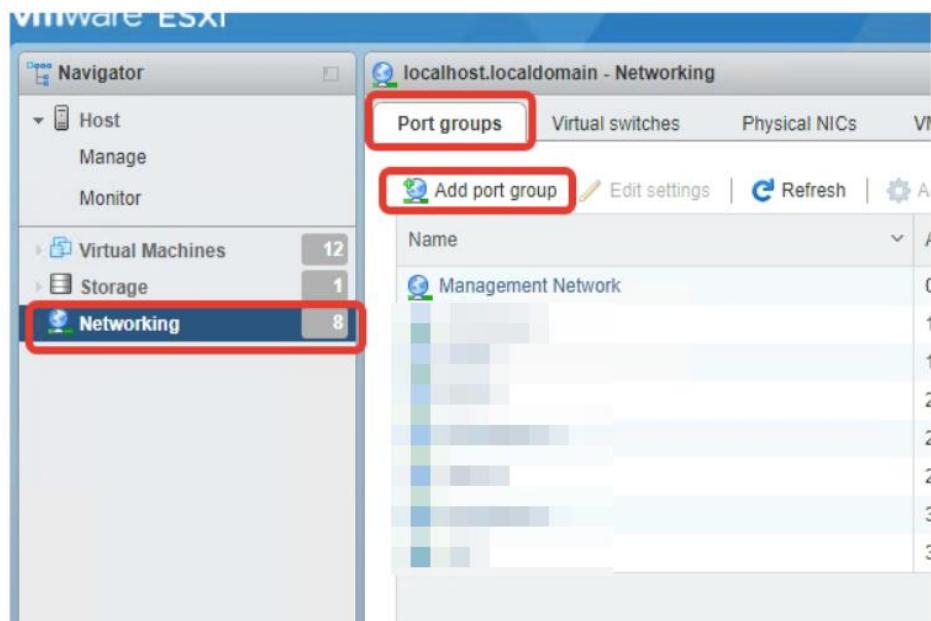
Необходимо выполнить установку данного инструмента. Менять параметры, предлагаемые помощником, не нужно.

После установки Vmware Tools нужно выбрать Yes для того, чтобы перезагрузить компьютер и применить обновление.

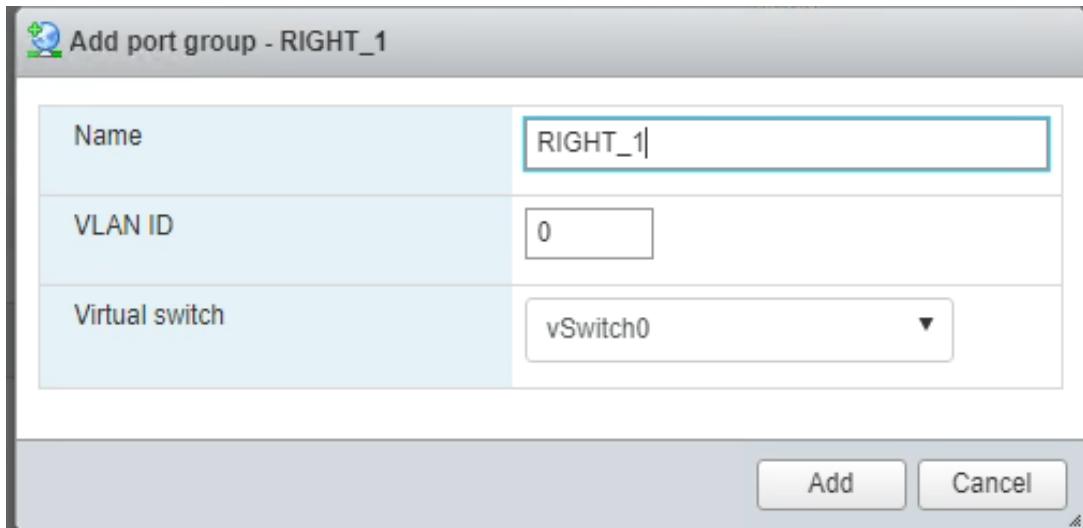


После перезагрузки Windows будет работать намного лучше.

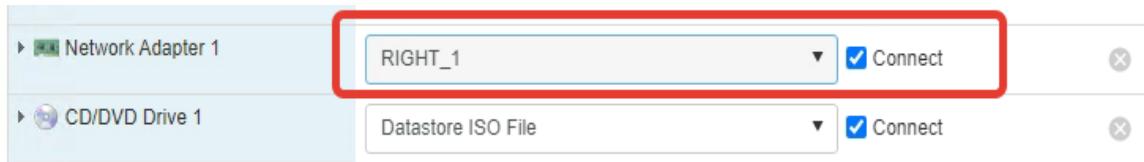
Для создания сетей в ESXi необходимо перейти в Networking → Port Groups → Add port group.



Теперь нужно создать сеть, в данном примере — с названием RIGHT\_1.

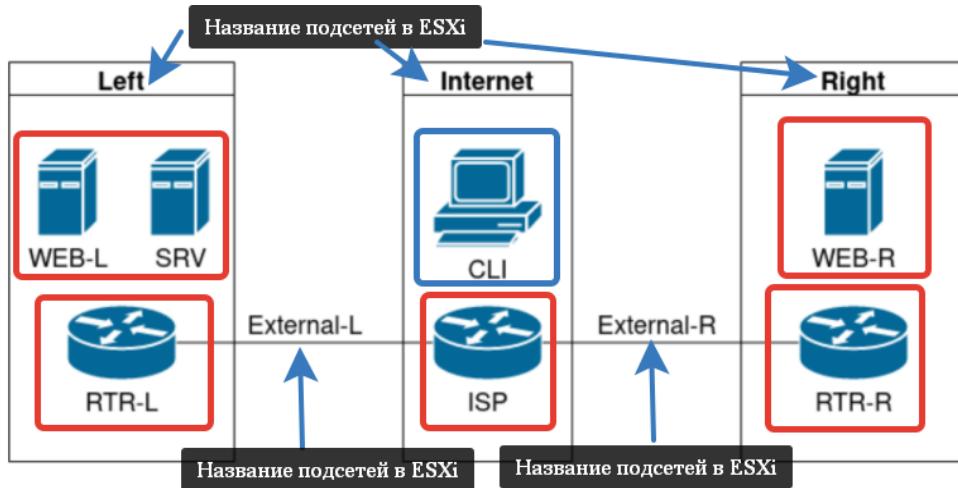


Далее необходимо изменить значение в Network Adapter на RIGHT\_1 на машине SRV и DC соответственно.



Теперь виртуальные машины находятся в одной подсети, словно если бы их соединили одним общим кабелем «витая пара».

Используя полученные знания, необходимо собрать стенд по указанной топологии:



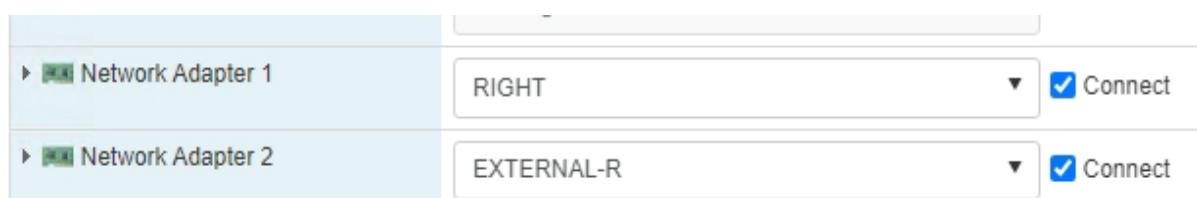
- красным выделены машины, которые будут настроены на базе Debian 11;
- синим — Windows 10.

Ярлык «название подсетей в ESXi» указывает на то, какие Port Groups нужно создать и каким образом подключить к виртуальным машинам.

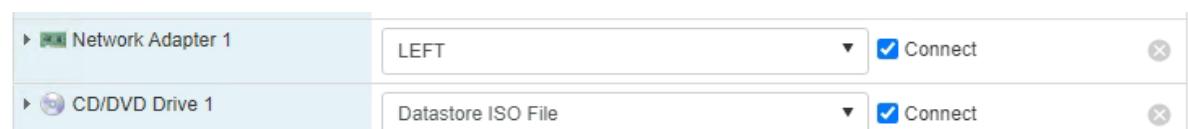
Для дополнительной помощи представлены скриншоты некоторых итоговых машин. Например, RTR-L,



RTR-R,



SRV



и WEB-L.



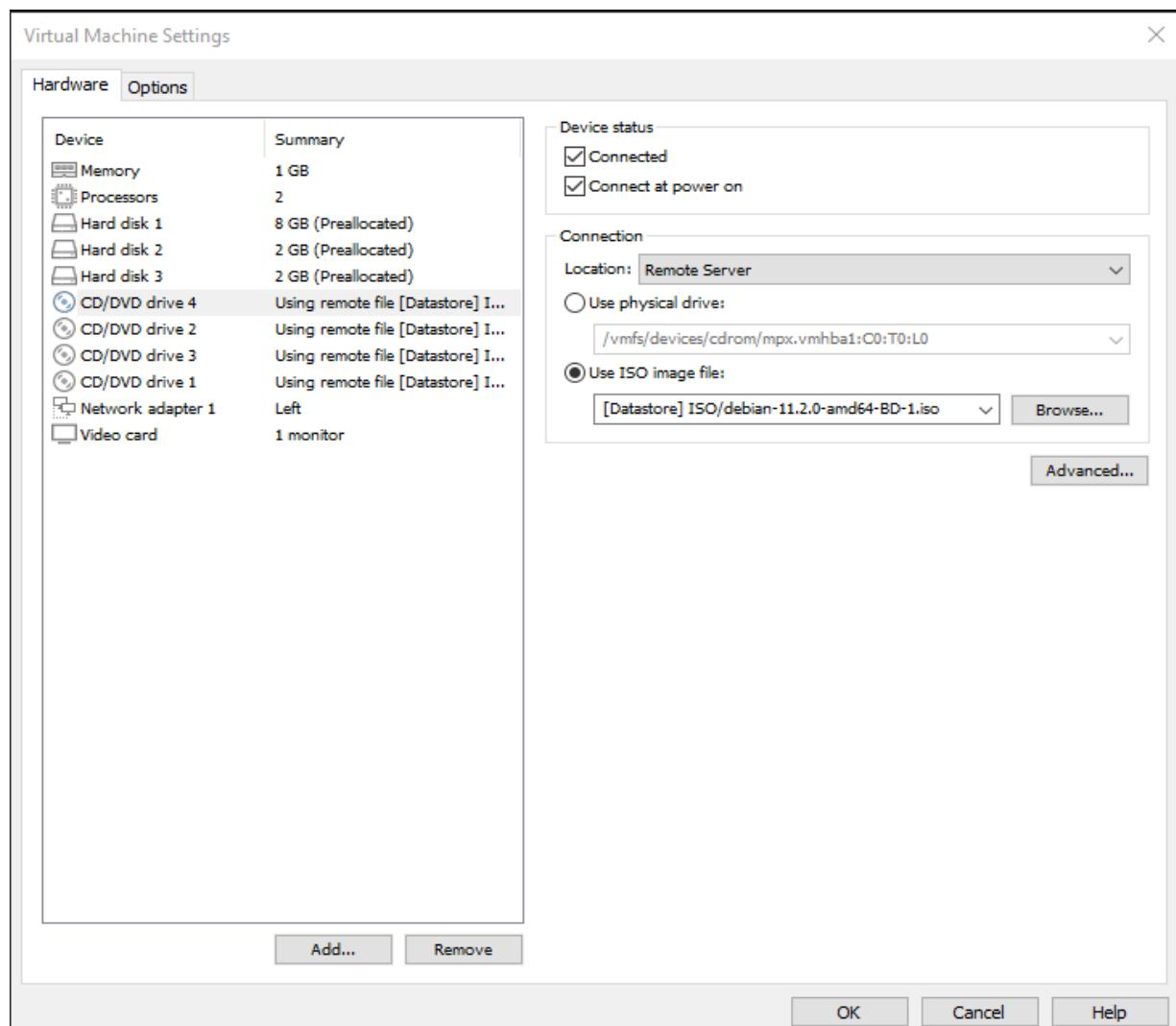
Стоит обратить внимание, что в данном методическом материале выполнение задания идет не в том порядке, как в экзаменационной документации. Порядок в методике обусловлен взаимосвязью различных сервисов друг с другом и стратегией рационального выполнения. В первом разделе данного методического документа будет рассмотрено задание, в котором все машины находятся под управлением ОС Debian 11. За исключением CLI, в рамках задания любых вариантов они всегда под управлением ОС Windows 10.

Вместо RAID-массива задача может быть следующего вида:

- реализуйте iSCSI Target на базе SRV;
- сервер должен предоставлять доступ для подключения диска по протоколу iSCSI только и исключительно для WEB-L;
- используется диск на базе подключенного дополнительного диска, согласно таблице 1;
- на WEB-L iSCSI-раздел должен быть смонтирован по адресу /mnt/iscsi и быть отформатирован в ext4.

#### Порядок выполнения

- необходимо подключить к виртуальной машине SRV 4 BluRay-диска, что находится на Datastore сервера;



- перейти в консоль сервера SRV и ввести команду  
`apt install tgt -y`
- после установки пакета tgt (программы для настройки iSCSI-инициатора) необходимо настроить файл конфигурации согласно скриншоту  
`/etc/tgt/targets.conf`

```
<target iqn.2023-02.wsr.demo.int:srv>
  backing-store /dev/sdd
  initiator-address 192.168.100.100
</target>
```

### Комментарии к заполненным параметрам

В начале секции target указывается IQN — полностью определенное имя цели, которое имеет следующий формат

`iqn.<год-месяц>.<реверс_имени_домена>:<имя_таргета>`

Далее указываются параметры — `backing-store`, он ссылается на диск `/dev/sdd` — необходимо добавить новый диск на SRV, а с помощью команды `lsblk` убедиться, какое у него название.

```
root@SRV:~# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINT
sda     8:0    0   8G  0 disk
└─sda1  8:1    0   7G  0 part   /
└─sda2  8:2    0   1K  0 part
└─sda5  8:5    0  975M 0 part   [SWAP]
sdb     8:16   0   2G  0 disk
└─sdb1  8:17   0   2G  0 part
  └─md0   9:0    0   2G  0 raid1 /mnt/storage
sdc     8:32   0   2G  0 disk
└─sdc1  8:33   0   2G  0 part
  └─md0   9:0    0   2G  0 raid1 /mnt/storage
sdd     8:48   0   1G  0 disk
```

В параметре `initiator-address` указываются адреса машин, которым можно подключаться к iSCSI-target.

После внесения всех настроек следует перезапустить службу с помощью команды  
`systemctl restart tgt`

Перезапуск службы `targetcli` должен выполниться успешно. Чтобы точно убедиться в том, что все настройки заданы верно, следует использовать команду

`tgtadm --mode target --op show`

```
Backing store flags:
LUN: 1
  Type: disk
  SCSI ID: IET      00010001
  SCSI SN: beaf11
  Size: 1074 MB, Block size: 512
  Online: Yes
  Removable media: No
  Prevent removal: No
  Readonly: No
  SWP: No
  Thin-provisioning: No
  Backing store type: rdwr
  Backing store path: /dev/sdd
  Backing store flags:
    Account information:
    ACL information:
    192.168.100.100
```

В выводе команды необходимо внимательно найти строки, которые относятся к iSCSI-LUN.

## **Настройка клиентов.**

Монтировать ресурс по iSCSI необходимо на машине WEB-L.

На клиентах нужно подключить первый BD-диск и установить пакет — open-iscsi  
apt install open-iscsi

После установки данного пакета нужно настроить конфигурационный файл — /etc/iscsi/iscsid.conf

```
# To request that the iscsi initd scripts startup a session set to "automatic".
node.startup = automatic
#
# To manually startup the session set to "manual". The default is manual.
#node.startup = manual
```

Необходимо убрать комментарии со строки node.startup=automatic. Это нужно для того, чтобы iSCSI монтировался в систему автоматически при включении ОС.

Необходимо убрать комментарии со строки node.startup=manual.

Затем ввести команду поиску опубликованных на сервере целей для подключения iscsadm -m discovery -t sendtargets -p 192.168.100.200:3260

```
root@WEB-R:~# iscsadm -m discovery -t sendtargets -p 192.168.100.200:3260
192.168.100.200:3260,1 iqn.2023-02.wsr.demo.int:srv
root@WEB-R:~#
```

В ответ команда вернет iqn-адрес. Именно к нему и нужно выполнить подключение с помощью команды:

iscsadm -m node --targetname “iqn.2023-02.wsr.demo.int:srv” --portal “192.168.100.200:3260” --login

```
root@WEB-R:~# iscsadm -m node --targetname 'iqn.2023-02.wsr.demo.int:srv' --portal "192.168.100.200
:3260" --login
Logging in to [iface: default, target: iqn.2023-02.wsr.demo.int:srv, portal: 192.168.100.200,3260]

Login to [iface: default, target: iqn.2023-02.wsr.demo.int:srv, portal: 192.168.100.200,3260] succe
ssful.
root@WEB-R:~#
```

По итогу ввода команды отобразится уведомление, где сообщается об успешном входе в систему.

Необходимо использовать команду lsblk, чтобы вывести все доступные блочные устройства. Как можно заметить, теперь в системе появился диск — /dev/sdb, который можно использовать как напрямую подключенный к ПК диск.

Необходимо создать на новом диске файловую систему ext4, как того требует задание, с помощью команды

mkfs.ext4 /dev/sdb

```
root@WEB-R:~# mkfs.ext4 /dev/sdb
mke2fs 1.46.2 (28-Feb-2021)
Creating filesystem with 262144 4k blocks and 65536 inodes
Filesystem UUID: 0c8ad714-a2b4-4c20-957b-db2c5ad09b0c
Superblock backups stored on blocks:
            32768, 98304, 163840, 229376

Allocating group tables: done
Writing inode tables: done
Creating journal (8192 blocks):

done
Writing superblocks and filesystem accounting information: done

root@WEB-R:~#
```

Все параметры следует оставить по умолчанию. А затем смонтировать диск в директорию /mnt/iscsi —

```
mkdir /mnt/iscsi  
mount /dev/sdb /mnt/iscsi
```

Настраивать механизм автомонтируания не требуется.

Также в рамках модуля создания веб-сайтов может присутствовать следующее задание.

Выполните конфигурацию дополнительного веб-сайта;

- используется BM SRV;
- доступ к приложению осуществляется по DNS-имени backup.int.demo.wsr;
- в качестве заглушки используется простой текст “TODO”;
- доступ разрешен только с WEB-L и WEB-R;
- прочий доступ следует запретить.

#### Порядок выполнения задания

Установка с DVD-1 пакета nginx: apt install nginx.

В директории /var/www/html/ создается файл index.html следующего содержания:

```
<html>  
    <head>  
        <title>TODO</title>  
    </head>  
    <body>  
        <h1>TODO</h1>  
    </body>  
</html>
```

Запускаем службу nginx: systemctl start nginx.

Создается файл /etc/nginx/sites-available/backup.int.demo.wsr следующего содержания:

```
server {  
    listen 80;  
    server_name backup.int.demo.wsr;  
    root /var/www/html;  
    index index.html;  
  
    location / {  
        allow 192.168.100.100;  
        allow 172.16.100.100;  
        deny all;  
    }  
}
```

Создается ссылка на файл

```
ln -s /etc/nginx/sites-available/backup.int.demo.wsr /etc/nginx/sites-enabled
```

Проверяется правильность синтаксиса командой nginx -t.

Добавляется домен в /etc/bind/int.demo.wsr.

```
backup IN A 192.168.100.200
```

Перезапускается служба bind9: systemctl restart bind9.

Проверяется доступ к заглушки командой

```
curl http://backup.int.demo.wsr, ожидается получить ошибку доступа (403).
```

Чтобы WEB-L и WEB-R получили доступ к домену, необходимо отредактировать на обоих машинах файл конфигурации /etc/resolv.conf:

```
nameserver 192.168.100.200  
search backup.int.demo.wsr
```

После чего перезапустить службу командой  
systemctl restart systemd-resolved

После этого с помощью команды curl http://backup.int.demo.wsr ожидается увидеть заглушку.

Примечание: если пакет curl отсутствует, его необходимо установить с DVD-1.

## **БЛАГОДАРНОСТИ**

Хочется выразить благодарность всем специалистам, которые помогали в написании и последующей проверке данного учебного пособия для изучения информационных систем:

- Грекову Владимиру Сергеевичу, специалисту ИТ РГУ нефти и газа (НИУ) имени И. М. Губкина;
- Машкову Ивану Романовичу, специалисту ИТ РГУ нефти и газа (НИУ) имени И. М. Губкина;
- Мокшанцеву Михаилу Александровичу, эксперту отдела аналитики и разработки АО КОНСИСТ-ОС, отдела аналитики и разработки ГЕОП;
- Морозову Илье Михайловичу, учебному мастеру РГУ нефти и газа (НИУ) имени И. М. Губкина;
- Токареву Георгию Ивановичу, учебному мастеру РГУ нефти и газа (НИУ) имени И. М. Губкина.

## **СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ**

1. Уймин, А. Г. Сетевое и системное администрирование. Демонстрационный экзамен КОД 1.1 : учебно-методическое пособие для СПО / А. Г. Уймин. — 3-е изд., стер. — СПб. : Лань, 2022. — 480 с. — ISBN 978-5-8114-9255-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/189420> (дата обращения: 15.03.2023). — Режим доступа: для авториз. пользователей.
2. Уймин, А. Г. Технические средства информатизации : практикум для СПО / А. Г. Уймин. — Саратов, М. : Профобразование, Ай Пи Ар Медиа, 2023. — 434 с. — ISBN 978-5-4488-1589-8, 978-5-4497-2023-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/128552.html> (дата обращения: 03.03.2023). — Режим доступа: для авториз. пользователей. — DOI: <https://doi.org/10.23682/128552>.
3. Федеральный закон «Об образовании в Российской Федерации» № 273-ФЗ от 29 декабря 2012 г. (с изм. от 06.03.2019 № 17-ФЗ).
4. Федеральный государственный образовательный стандарт среднего профессионального образования по профессии 09.01.02 «Наладчик компьютерных сетей», утвержденный приказом от 2 августа 2013 г. № 853 Министерства образования и науки Российской Федерации.
5. Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 09.02.02 «Компьютерные сети», утвержденный приказом от 28 июля 2014 г. № 803 Министерства образования и науки Российской Федерации.
6. Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 09.02.06 «Сетевое и системное администрирование», утвержденный приказом от 9 декабря 2016 г. № 1548 Министерства образования и науки Российской Федерации.
7. Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 09.02.07 «Информационные системы и программирование», утвержденный приказом от 9 декабря 2016 г. № 1547 Министерства образования и науки Российской Федерации.
8. Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 10.02.02 «Информационная безопасность телекоммуникационных систем», утвержденный приказом от 13 августа 2014 г. № 1000 Министерства образования и науки Российской Федерации.
9. Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 10.02.03 «Информационная безопасность автоматизированных систем», утвержденный приказом от 28 июля 2014 г. № 806 Министерства образования и науки Российской Федерации.
10. Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем», утвержденный приказом от 9 декабря 2016 г. № 1551 Министерства образования и науки Российской Федерации.
11. Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», утвержденный приказом от 9 декабря 2016 г. № 1553 Министерства образования и науки Российской Федерации.
12. Приказ Министерства образования и науки Российской Федерации от 16 августа 2013 г. № 968 «Об утверждении порядка проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования» от 17.11.2017 г. № 1138 «О внесении изменений в порядок проведения государственной итоговой аттестации

по образовательным программам среднего профессионального образования», утвержденный приказом Министерства образования и науки Российской Федерации от 16.08.2013 г. № 968.

13. Комплект оценочной документации 09.02.06-2023 демонстрационного экзамена базового уровня по коду «09.02.06» и наименованию профессии «Сетевое и системное администрирование».

# ОГЛАВЛЕНИЕ

Предисловие .....	3
Введение .....	5
Виртуальные машины и коммутация.....	6
Порядок выполнения .....	7
Выполнение проектирования кабельной структуры компьютерной сети .....	8
Задания .....	11
Осуществление выбора технологий, инструментальных средств и средств вычислительной техники при организации процесса разработки и исследования объектов профессиональной деятельности.....	18
Конфигурация виртуальных частных сетей .....	22
Настройка списков контроля доступа.....	27
Администрирование локальных вычислительных сетей и принятие мер по устранению возможных сбоев.....	31
Администрирование сетевых ресурсов в информационных системах.....	33
Взаимодействие со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности.....	71
Приложения .....	81
Приложение 1 .....	81
Приложение 2 .....	85
Благодарности .....	112
Список используемых источников.....	113

**Антон Григорьевич УЙМИН**  
**ПРАКТИКУМ.**  
**ДЕМОНСТРАЦИОННЫЙ ЭКЗАМЕН БАЗОВОГО УРОВНЯ.**  
**СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ**  
**УЧЕБНОЕ ПОСОБИЕ**

Зав. редакцией литературы  
по информационным технологиям и системам связи *О. Е. Гайнутдинова*  
Ответственный редактор *Е. А. Дмитриева*  
Подготовка макета *Д. А. Вакурова*  
Корректор *М. А. Ланда*  
Выпускающий *В. А. Иутин*

ЛР № 065466 от 21.10.97  
Гигиенический сертификат 78.01.10.953.П.1028  
от 14.04.2016 г., выдан ЦГСЭН в СПб  
**Издательство «ЛАНЬ»**  
lan@lanbook.ru; www.lanbook.com  
196105, Санкт-Петербург, пр. Ю. Гагарина, д. 1, лит. А.  
Тел./факс: (812) 336-25-09, 412-92-72.  
Бесплатный звонок по России: 8-800-700-40-71

**ГДЕ КУПИТЬ**

**ДЛЯ ОРГАНИЗАЦИЙ:**

*Для того, чтобы заказать необходимые Вам книги,  
достаточно обратиться в любую из торговых компаний Издательского Дома «ЛАНЬ»:*

**по России и зарубежью**  
«ЛАНЬ-ТРЕЙД». 196105, Санкт-Петербург, пр. Ю. Гагарина, д. 1, лит. А.  
тел.: (812) 412-85-78, 412-14-45, 412-85-82; тел./факс: (812) 412-54-93  
e-mail: trade@lanbook.ru; ICQ: 446-869-967

**www.lanbook.com**  
пункт меню «Где купить»  
раздел «Прайс-листы, каталоги»  
**в Москве и в Московской области**  
«ЛАНЬ-ПРЕСС». 109387, Москва, ул. Летняя, д. 6  
тел.: (499) 722-72-30, (495) 647-40-77; e-mail: lanpress@lanbook.ru

**в Краснодаре и в Краснодарском крае**  
«ЛАНЬ-ЮГ». 350901, Краснодар, ул. Жлобы, д. 1/1  
тел.: (861) 274-10-35; e-mail: lankrd98@mail.ru

**ДЛЯ РОЗНИЧНЫХ ПОКУПАТЕЛЕЙ:**  
интернет-магазин  
**Издательство «Лань»: <http://www.lanbook.com>**

магазин электронных книг  
**Global F5: <http://globalf5.com/>**

Подписано в печать 25.07.23.  
Бумага офсетная. Гарнитура Школьная. Формат 60×90 1/8.  
Печать офсетная/цифровая. Усл. п. л. 14,50. Тираж 30 экз.

Заказ № 965-23.

Отпечатано в полном соответствии  
с качеством предоставленного оригинал-макета в АО «Т8 Издательские Технологии».  
109316, г. Москва, Волгоградский пр., д. 42, к. 5.