



Подготовка машины ControlVM (на базе Альт Рабочая станция)

Задание:

1) Подготовка машины ControlVM

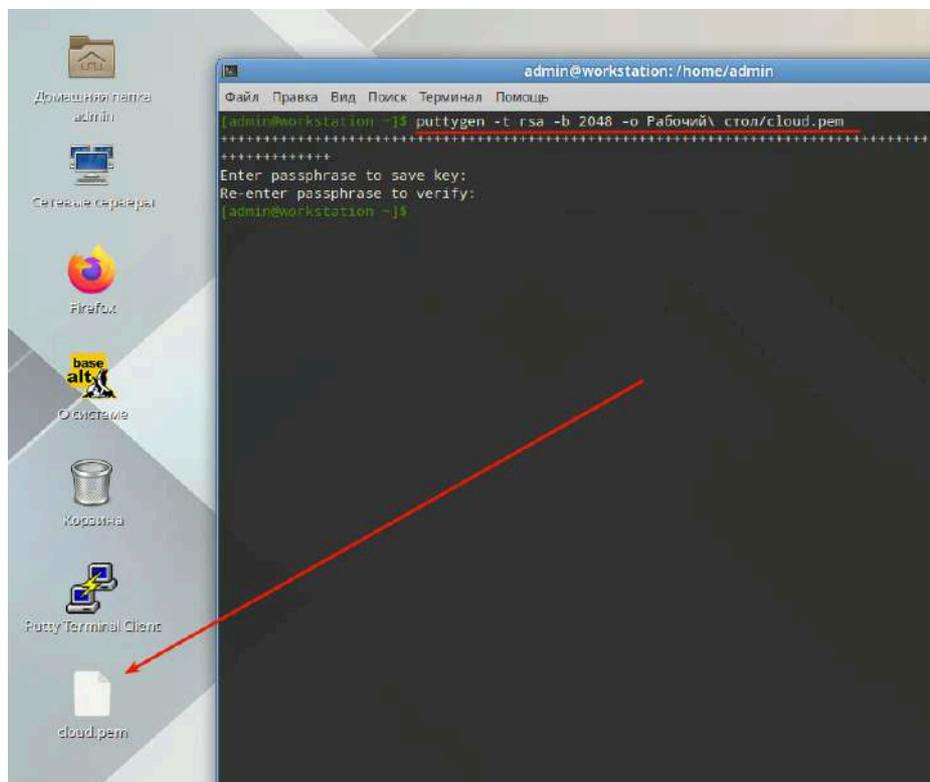
- а) Общие указания:
 - 1. Вся проверка выполнения задания будет осуществляться с машины ControlVM.
 - 2. НЕ удаляйте инстанс ControlVM после завершения задания.
- б) Создание и настройка инстанса ControlVM:
 - 1. Создайте виртуальный инстанс с именем ControlVM и подключите его к сети интернет.
 - 2. Установите следующие параметры для виртуальной машины:
 - i. Тип виртуальной машины: 2 vCPU, 4 ГБ RAM.
 - ii. Размер диска: 30 ГБ.
 - iii. Тип диска: SSD.
 - 3. ~~Отключите функции мониторинга и резервного копирования для данного инстанса.~~
 - 4. В качестве операционной системы выберите Альт Сервер 10.
 - 5. Настройте инстанс для разрешения внешних подключений по протоколу SSH.
 - 6. Сохраните ключевую пару для доступа на вашем локальном ПК на рабочем столе с расширением .pem.
- в) Настройка внешнего подключения к ControlVM:
 - 1. ~~Установите на локальный ПК клиент SSH PuTTY.~~
 - 2. Создайте в PuTTY профиль с именем cloud.
 - 3. Убедитесь в возможности установления соединения с инстансом ControlVM с локального ПК через PuTTY, без необходимости ввода дополнительных параметров.
 - 4. Для подключения используйте имя пользователя altlinux и ранее сохранённую ключевую пару.

Вариант реализации:

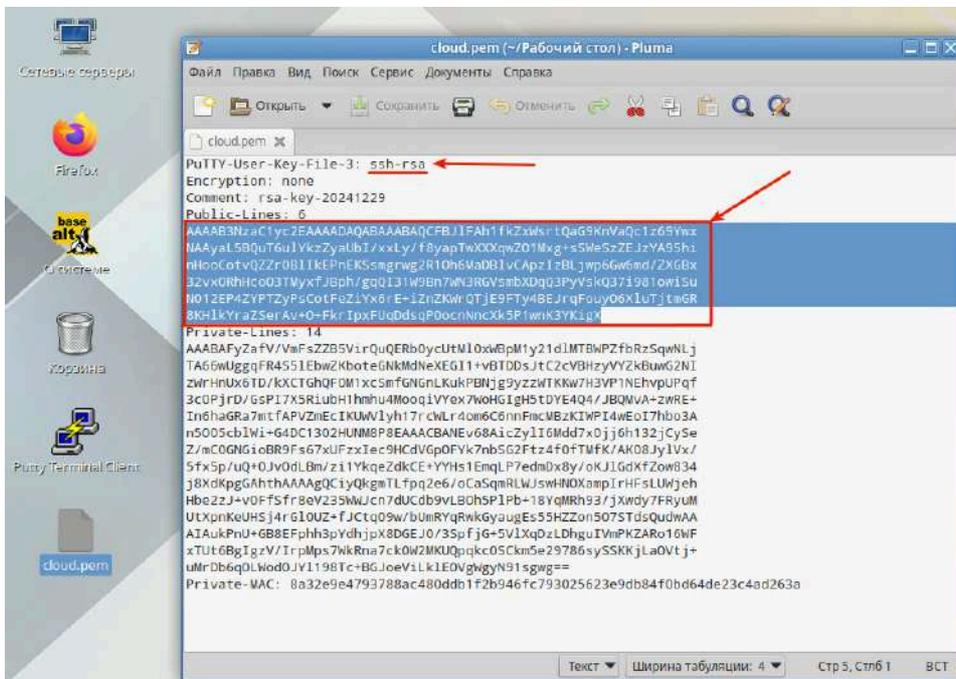
- Создаём ключевую пару для доступа к ControlVM на рабочем столе с расширением '.pem':

```
puttygen -t rsa -b 2048 -o Рабочий\ стол/cloud.pem
```

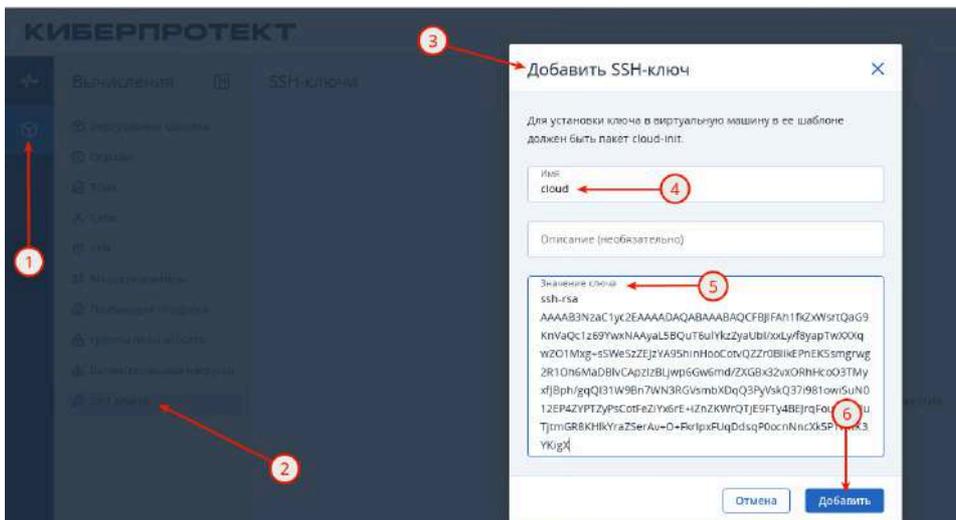
- Результат:



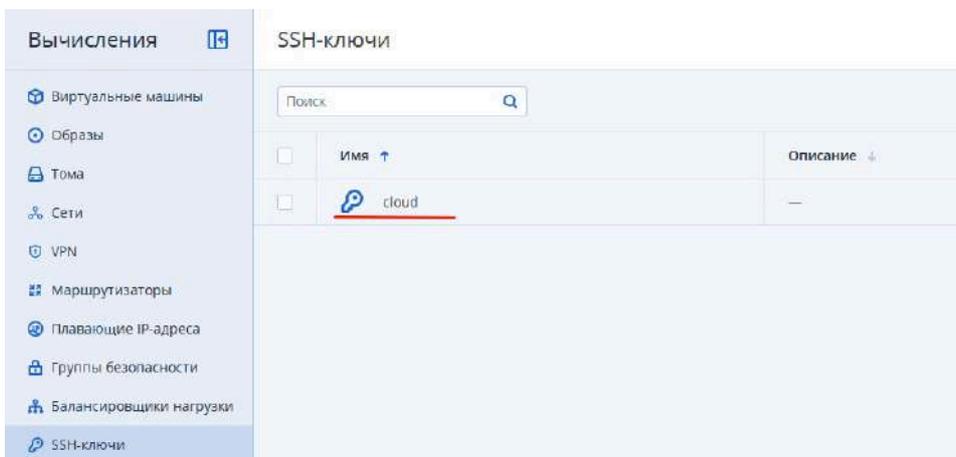
- Открываем в блокноте сгенерированный ключ и копируем заголовок **ssh-rsa** и публичную часть ключа:
 - Заголовок и публичную часть ключа необходимо будет поместить в Кибер Инфраструктура далее



- В веб-интерфейсе Кибер Инфраструктура создаём SSH-ключ:
 - В разделе **SSH-ключи** нажимаем **Добавить SSH-ключ** и даём понятное имя и ранее скопированное **Значение ключа** и нажимаем **Добавить**:

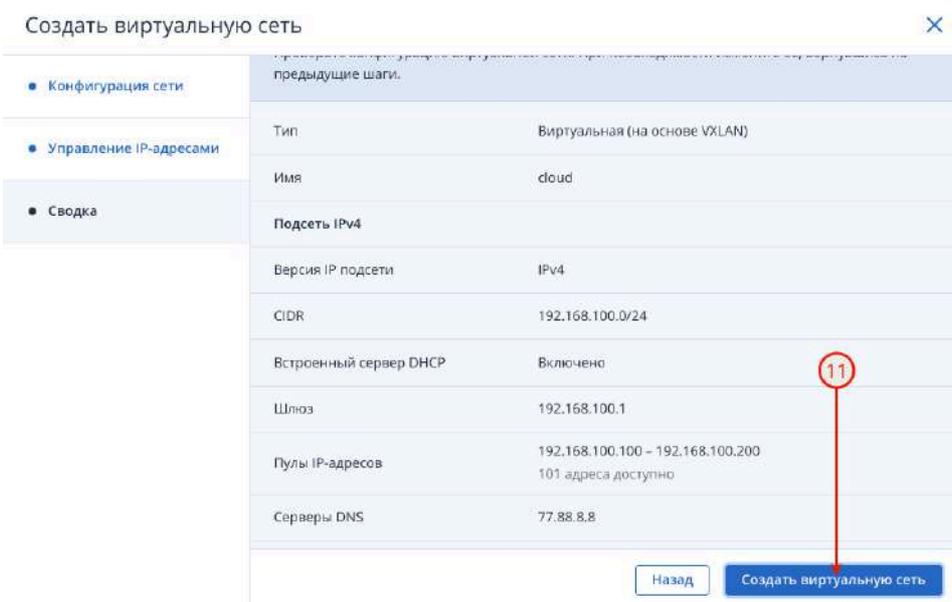
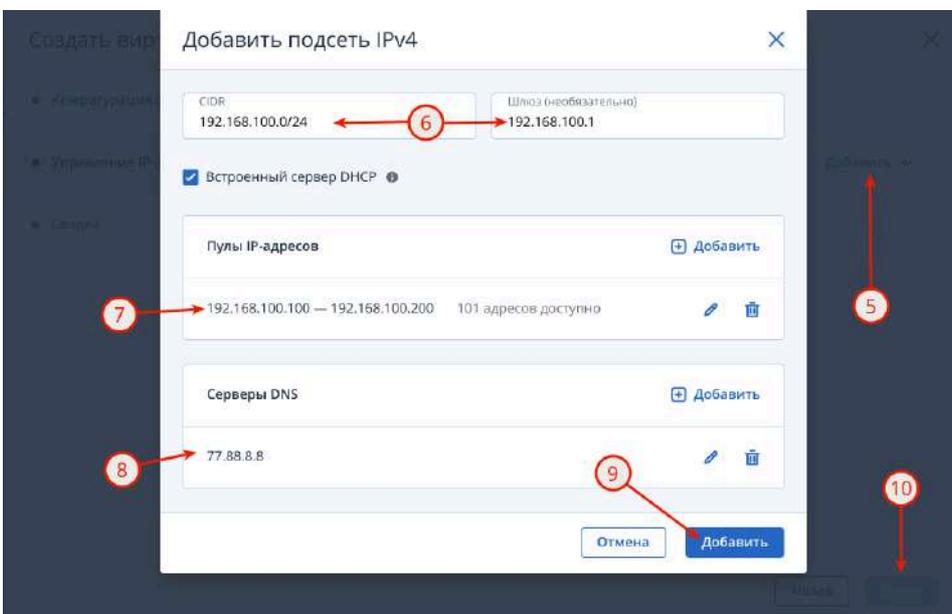
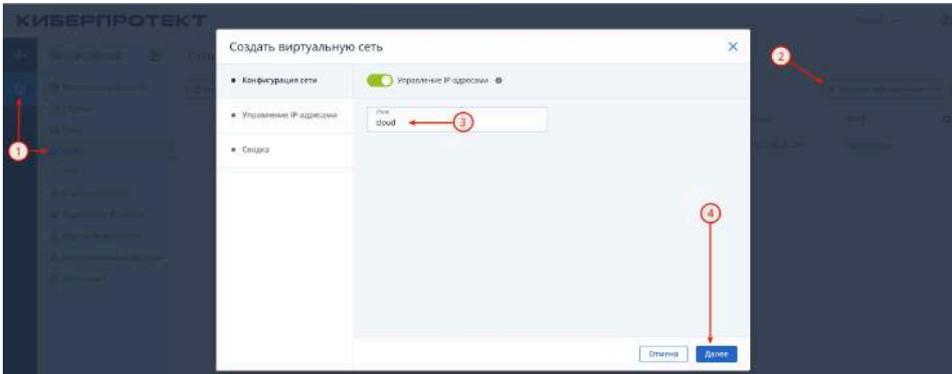


- Результат:
 - Созданный **SSH-ключ** с именем **cloud**:

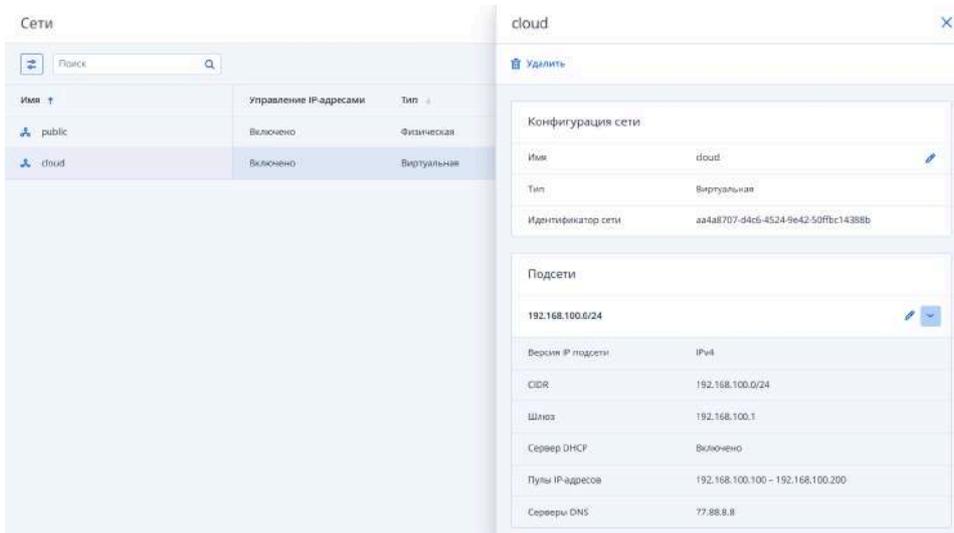


- Для создания **ControlVM** и подключения к ней с доступом в сеть Интернет, процесс создания зависит от настройки Кибер Инфраструктуры, а именно сети **'public'**, которая будет предоставлять Плавающие IP:
 - Если на сеть выданы права **Все права** - Предоставление полного доступа позволит виртуальным машинам в выбранных проектах обмениваться трафиком с данной сетью напрямую или через виртуальные маршрутизаторы.
 - Тогда для **ControlVM** достаточно просто подключить данную сеть и подключаться по полученному IP-адресу;
 - Если на сеть выданы права **Маршрутизируемый** - Предоставление маршрутизируемого доступа позволит виртуальным машинам в выбранных проектах обмениваться трафиком с данной сетью только через виртуальные маршрутизаторы.
 - Тогда для **ControlVM** потребуется предварительно создать:

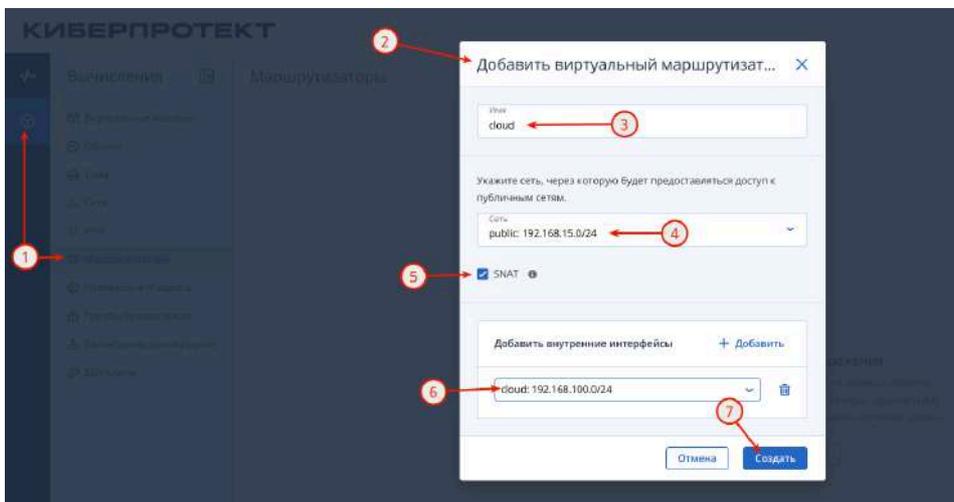
- Виртуальную подсеть;
 - Виртуальный маршрутизатор, который будет маршрутизировать в сеть Интернет (SNAT);
 - Плавающий IP ассоциируемый с данной виртуальной машиной;
- Рассмотрим процесс создания **ControlVM** когда для её работы необходимо создать ряд вспомогательных ресурсов описанных выше:
- Создадим виртуальную подсеть с именем **cloud**:
 - Имя может быть произвольным, но для наглядности все ресурсы необходимые для работы **ControlVM** будут именоваться **cloud**, чтобы в дальнейшем не удалять их случайно;



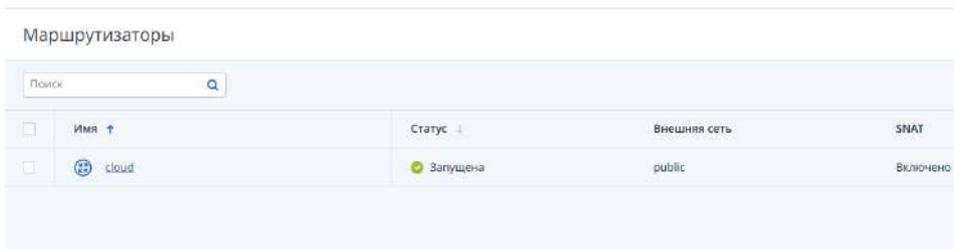
- Результат:
 - Созданная виртуальная сеть с именем **cloud** необходимая для работы **ControlVM** (не удалять в конце выполнения задания, ресурс необходим для работы ControlVM);



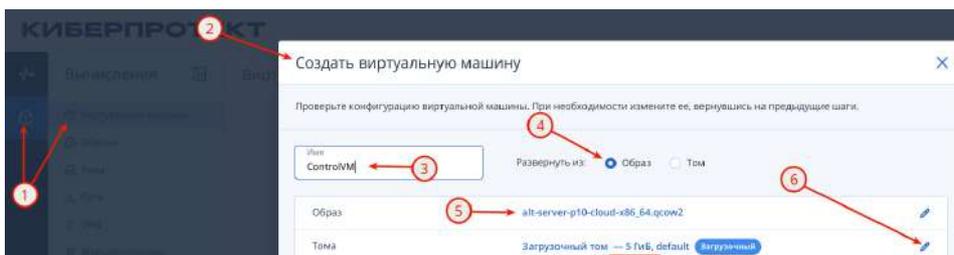
- Создадим Виртуальный маршрутизатор с именем **cloud**:
 - Имя может быть произвольным, но для наглядности все ресурсы необходимые для работы **ControlVM** будут именоваться **cloud**, чтобы в дальнейшем не удалить их случайно;

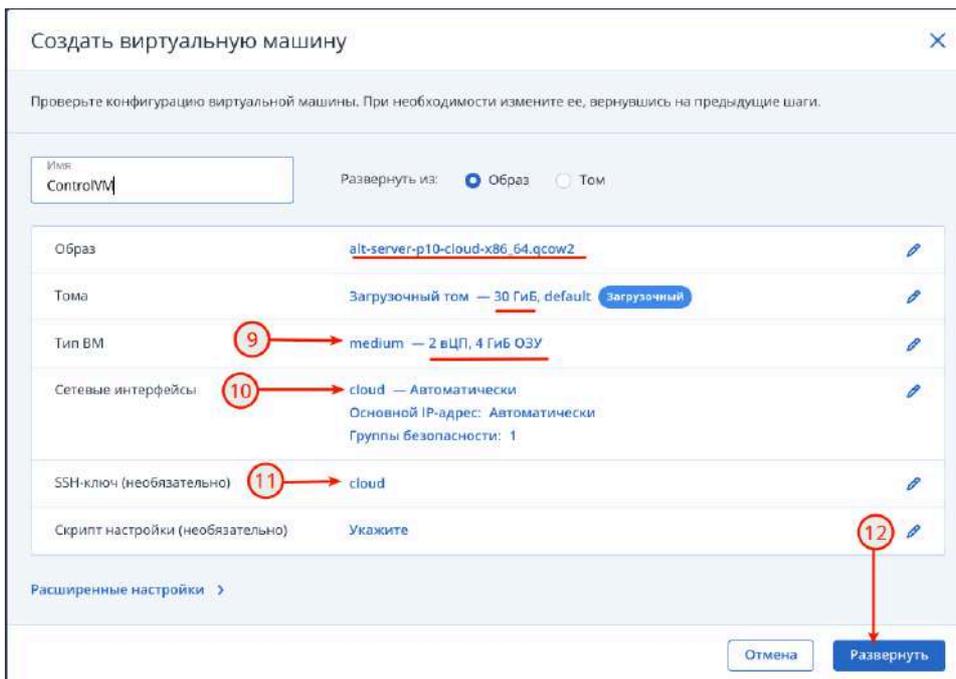
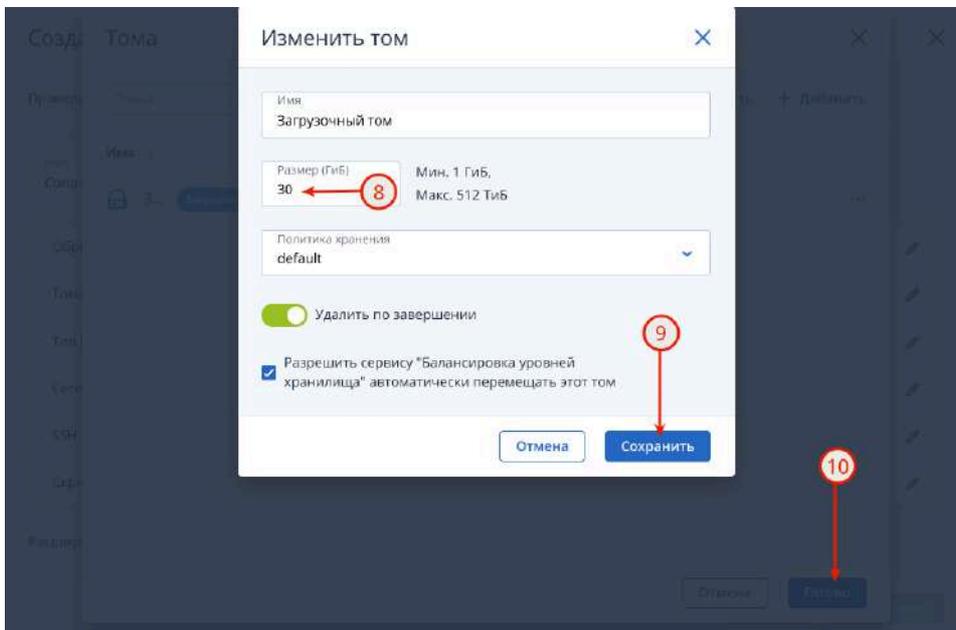
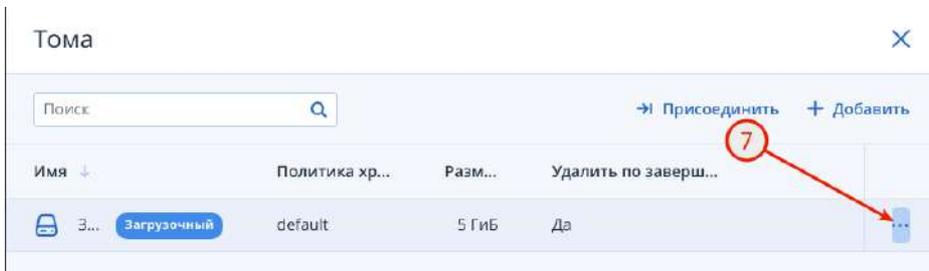


- Результат:
 - Созданный виртуальный маршрутизатор с именем **cloud** необходимая для работы **ControlVM** (не удалять в конце выполнения задания, ресурс необходим для работы ControlVM);

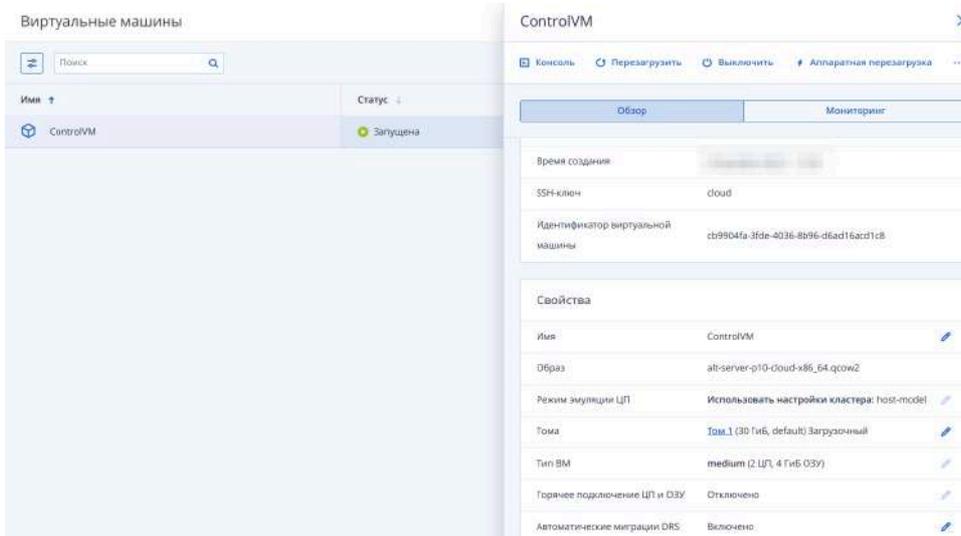


- Создаём инстанс (виртуальную машину) **ControlVM**:
 - Задаём имя в соответствие с заданием;
 - Выбираем образ **alt0server-p10-cloud**, т.к. по заданию ControlVM должен быть на Альт Сервер;
 - Размер диска следует поменять с 5 на 30, т.к. по заданию должно быть 30;
 - Выбираем **Тип VM** который соответствует требованиям задания **2vCPU** и **4RAM**;
 - **Сетевой интерфейс** подключаем к ранее созданной виртуальной сети **cloud**;
 - В качестве **SSH-ключа** указываем ранее созданный **cloud**;

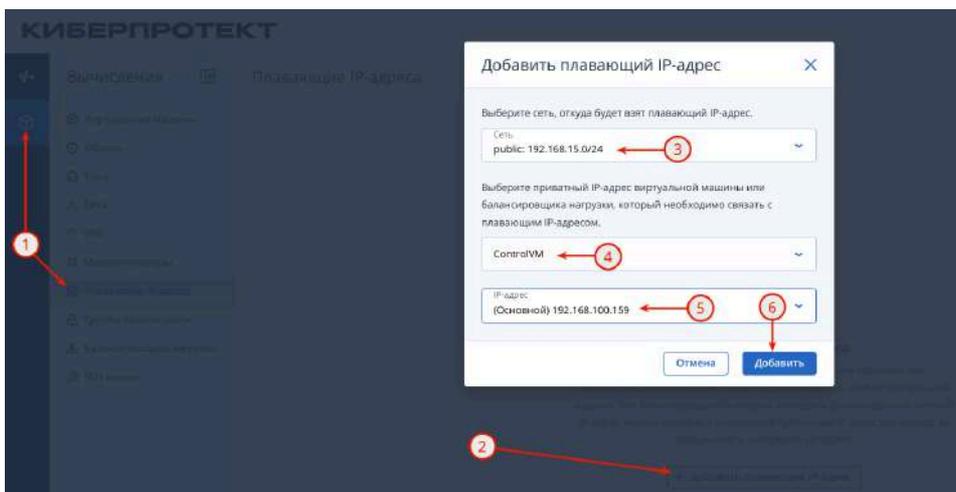




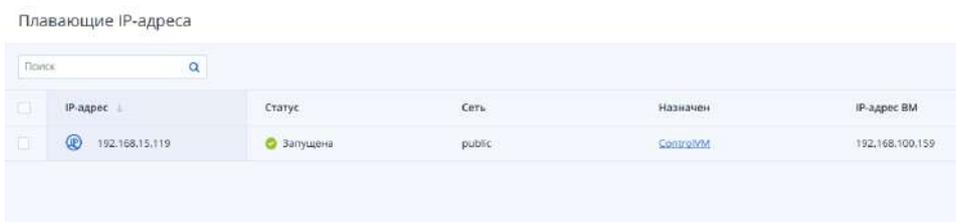
- Результат:
 - Созданная виртуальная машина **ControlVM** в соответствии с требованиями задания:



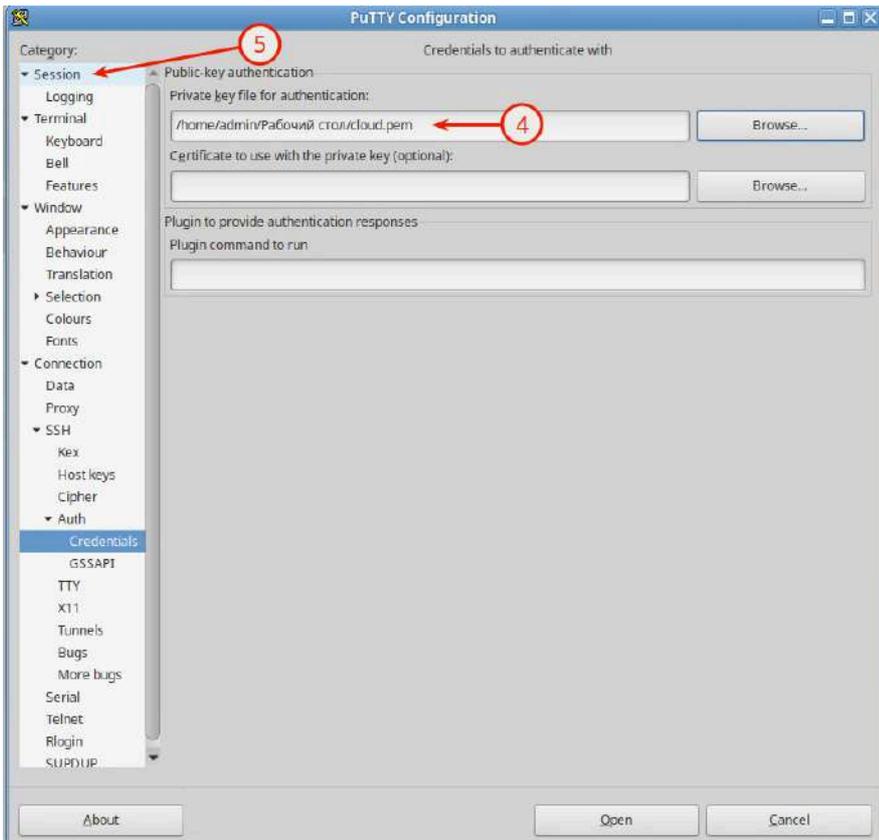
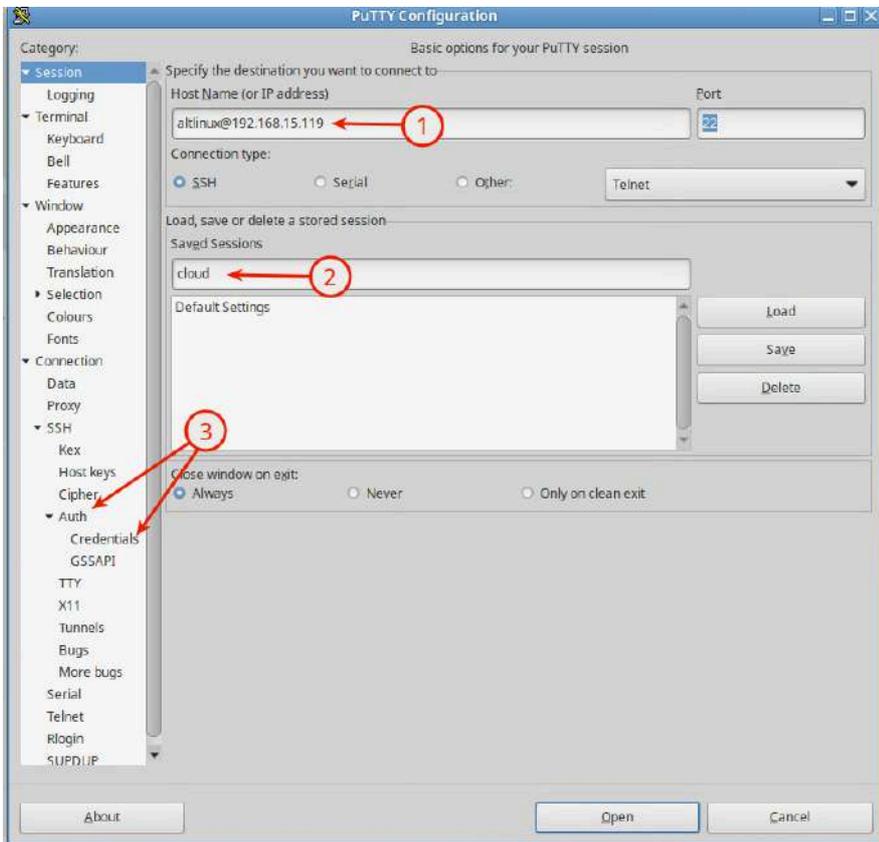
- Создаём **Плавающий IP** чтобы можно было подключиться к **ControlVM**:

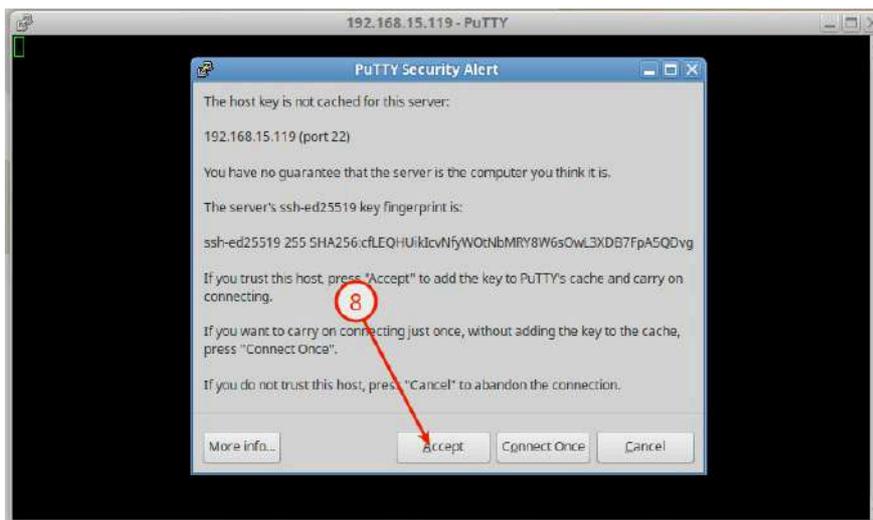
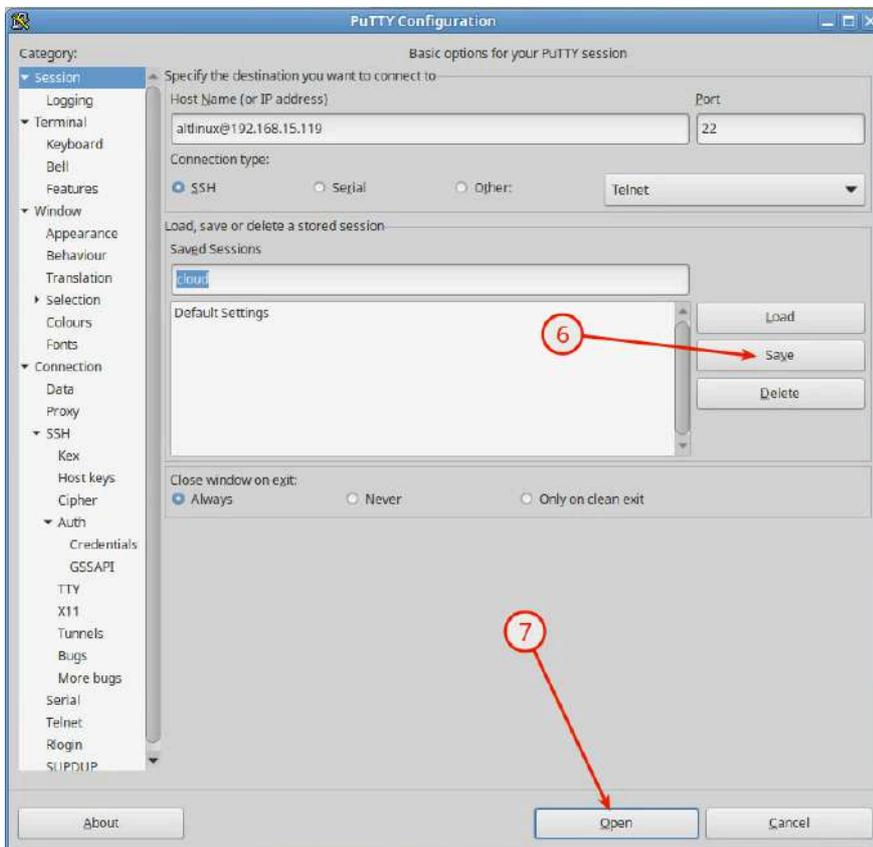


- Результат:
 - Созданный **Плавающий IP** адрес назначенный **ControlVM**:



- Для подключения к **ControlVM** создаём профиль в **putty**:
 - Используя для подключения **Плавающий IP** адрес и ранее сгенерированную ключевую пару на **Рабочем столе**:





- Результат:
 - Подключение к ControlVM под пользователем altlinux на основе ключевой пары используя putty:



- Проверяем сетевые параметры и доступ в сеть Интернет:

```
altlinux@controlvm: /home/altlinux
Using username "altlinux".
Authenticating with public key "rsa-key-20241229"
[altlinux@controlvm ~]$ ip -c -br -4 a
lo                UNKNOWN    127.0.0.1/8
eth0              UP        192.168.100.159/24 metric 100
[altlinux@controlvm ~]$ ip -c r
default via 192.168.100.1 dev eth0 proto dhcp src 192.168.100.159 metric 100
77.88.8.8 via 192.168.100.1 dev eth0 proto dhcp src 192.168.100.159 metric 100
169.254.169.254 via 192.168.100.1 dev eth0 proto dhcp src 192.168.100.159 metric 100
192.168.100.0/24 dev eth0 proto kernel scope link src 192.168.100.159 metric 100
192.168.100.1 dev eth0 proto dhcp scope link src 192.168.100.159 metric 100
192.168.100.100 dev eth0 proto dhcp scope link src 192.168.100.159 metric 100
[altlinux@controlvm ~]$ cat /etc/resolv.conf
# This is /run/systemd/resolve/resolv.conf managed by man:systemd-resolved(8).
# Do not edit.
#
# This file might be symlinked as /etc/resolv.conf. If you're looking at
# /etc/resolv.conf and seeing this text, you have followed the symlink.
#
# This is a dynamic resolv.conf file for connecting local clients directly to
# all known uplink DNS servers. This file lists all configured search domains.
#
# Third party programs should typically not access this file directly, but only
# through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a
# different way, replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 77.88.8.8
search .
[altlinux@controlvm ~]$ ping -c3 ya.ru
PING ya.ru (77.88.55.242) 56(84) bytes of data:
64 bytes from ya.ru (77.88.55.242): icmp_seq=1 ttl=246 time=26.7 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=2 ttl=246 time=27.0 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=3 ttl=246 time=26.4 ms

--- ya.ru ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 26.447/26.709/27.005/0.228 ms
[altlinux@controlvm ~]$
```

Последнее изменение: среда, 1 января 2025, 13:02

[Обратная связь](#)

[Подпишитесь](#)

[Вы используете гостевой доступ \(Вход\)](#)

[Сводка хранения данных](#)

Тема оформления сайта разработана

[conecti.me](#)