

Создание новой виртуальной машины в проекте.

Создание виртуальной машины в новом проекте

Подготовка к созданию

1. Подключение к облачной инфраструктуре

Перейти по [ссылке](#). Для подключения использовать домен AD, а также учётную запись пользователя, используемую для подключения к WiFi СПбГУТ



Войти

Домен

AD

Имя пользователя

Пароль

Вход

2. Открыть: `проект` -> `сеть` -> `сети`, и убедиться, что там есть сеть `external-direct-net` или `external-net`

← → ↻ cloud.resds.ru/horizon/project/networks/

openstack AD • имя_вашего_проекта ▾

Проект ▾ Проект / Сеть / Сети

Доступ к API

Вычислительные ресурсы > **Сети**

Диски >

Сеть ▾

Сетевая топология Отображено 3 значения

Сети

Маршрутизаторы

<input type="checkbox"/>	Name	Subnets Associated
<input type="checkbox"/>	external-direct-net	external-direct-subnet 172.17.5.0/24

“ external-direct-net - сеть маршрутизируема в сети бонча

3. Генерация ключевой пары.

При первом входе сгенерировать ключевую пару, для доступа к Linux виртуальным машинам.

“ Ключевая пара - это взаимосвязанная пара, состоящая из открытого и закрытого асимметричного ключа. Используется для подключения к виртуальной машине, без использования пароля

Открыть: Проект -> ключевая пара -> создать ключевую пару

Проект ▾ Проект / Вычислительные ресурсы / Ключевые пары

Доступ к API

Вычислительные ресурсы ▾ **Ключевые пары**

Обзор

Инстансы

Образы

Ключевые пары

Группы серверов

Диски >

Сеть >

Администратор >

Идентификация >

Нажмите здесь, для фильтрации или полнотекстового поиска x

+ Создать ключевую пару

Импортировать открытый ключ

Удалить ключевые пары

Отображено 2 значения

<input type="checkbox"/>	Название	Тип	
<input type="checkbox"/>	> shared-temasky-ad-keypair	ssh	Удалить ключевую пару
<input type="checkbox"/>	> test-key-pair	ssh	Удалить ключевую пару

Отображено 2 значения

В открывшемся окне ввести имя ключевой пары и тип ключа(ssh-key)

Создать ключевую пару

Имя ключевой пары *

my-keypair

Key Type*

SSH Key

Отмена

Создать ключевую пару

Имя ключевой пары может быть любым

Ключ будет сохранен на ваш компьютер, он понадобится в дальнейшем.

Создание виртуальной машины

4. Создать виртуальную машину.

Открыть меню Проект > вычислительные ресурсы > инстансы > запустить инстанс

cloud.resds.ru/horizon/project/instances/

openstack. AD • имя_вашего_проекта

Проект

Доступ к API

Вычислительные ресурсы

Обзор

Инстансы

Образы

Ключевые пары

Группы серверов

Диски

Проект / Вычислительные ресурсы / Инстансы

Инстансы

Отображено 7 значений

Отображено 7 значений

ID инстанса

Фильтр

Запустить инстанс

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task
---------------	------------	------------	--------	----------	--------	-------------------	------

В открывшемся окне, во вкладке подробности ввести имя инстанса и нажать Следующая > внизу страницы.

Запустить инстанс

Подробности

Источник *

Тип инстанса *

Сети *

Сетевые порты

Группы безопасности

Ключевая пара

Конфигурация

Группы серверов

Подсказки планировщика

Метаданные

Укажите начальное имя хоста для экземпляра, зону доступности для его развёртывания и количество разворачиваемых экземпляров. Увеличьте количество для развёртывания нескольких одинаковых экземпляров.

Имя инстанса *

my-instance

Описание

Зона доступности

Любая зона доступности

Количество *

1

Всего инстансов (100 Max)

21%

20

Использовано на текущий момент

1

Добавлено

79

Свободно

Отмена

Назад

Следующая >

Запустить инстанс

“ Имя инстанса может быть любым

В следующем меню (Источник) выбрать источник – `образ` , указать размер тома данных, выбрать `удаление диска при удалении инстанса` , выбрать `необходимый вам образ из доступных` (например `Ubuntu-server-20.04:docker`), и нажать справа от него стрелку вверх

Подобности

Источник

Тип инстанса *

Сети *

Сетевые порты

Группы безопасности

Ключевая пара

Конфигурация

Группы серверов

Подсказки планировщика

Метаданные

Источник инстанса - шаблон, используемый при создании инстанса. Можно использовать образ, снимок инстанса (снимок образа), диск или снимок диска (если доступно). Также можно выбрать постоянный тип хранения, создав новый диск.

Выберите источник загрузки

Образ

Создать новый диск

Да Нет

Размер диска (ГБ) *

1

Удалить диск при удалении инстанса

Да Нет

Выделенный

Отображено 0 значений

Название	Обновлено	Размер	Тип	Видимость
Выберите элемент из доступных элементов ниже				
Отображено 0 значений				

Доступно 35

Выберите одно

Нажмите здесь, для фильтрации или полнотекстового поиска

Отображено 35 значений

Название	Обновлено	Размер	Тип	Видимость
Ubuntu-server-20.04:docker	10/27/21 11:52 AM	5.00 ГБ	RAW	Публичный

Отображено 35 значений

Отмена

Назад

Следующая >

Запустить инстанс

В следующем меню (тип инстанса) определить объем выделяемых виртуальной машине вычислительных ресурсов. Для этого нужно выбрать один из predetermined типов инстансов (например `small`), и нажать справа от него стрелку вверх.



Подробности

Источник

Тип инстанса *

Сети

Сетевые порты

Группы безопасности

Ключевая пара

Конфигурация

Группы серверов

Подсказки планировщика

Метаданные

Типы инстансов отвечают за количество выделяемой памяти, дисков и процессорной мощности для создаваемых инстансов.

Выделенный

Название	VCPU	ОЗУ	Объем диска	Основной диск	Временный диск	Публичный
Выберите элемент из доступных элементов ниже						

▼ Доступно 15

Выберите одно

Q	Нажмите здесь, для фильтрации или полнотекстового поиска						✕
Название	VCPU	ОЗУ	Объем диска	Основной диск	Временный диск	Публичный	
> small	1	2 ГБ	8 ГБ	8 ГБ	0 ГБ	Да	↑

✕ Отмена

< Назад

Следующая >

Запустить инстанс

В меню сети выбрать нужную вам сеть, к которой будет подключена виртуальная машина (наличие сети было проверено в п.1). Если в инфраструктуре доступна только одна сеть, она будет выбрана автоматически, и выбирать ничего не нужно.



Подробности

Источник

Тип инстанса

Сети *

Сетевые порты

Группы безопасности

Ключевая пара

Конфигурация

Группы серверов

Подсказки планировщика

Метаданные

Сеть предоставляет канал связи между инстансами в облаке.

▼ Выделенный

Выберите сети из списка.

Сеть	Связанные подсети	Общая	Административное состояние	Статус
Выберите элемент из доступных элементов ниже				

▼ Доступно 2

Выберите как минимум одну сеть.

Q	Нажмите здесь, для фильтрации или полнотекстового поиска				✕
Сеть	Связанные подсети	Общая	Административное состояние	Статус	
> external-direct-net	external-direct-subnet	Да	Включен	Активный	↑

✕ Отмена

< Назад

Следующая >

Запустить инстанс

Затем перейти к меню Ключевая пара, выбрать созданную ключевую пару, и нажать справа от неё стрелку вверх.

Запустить инстанс

Подробности

Источник

Тип инстанса

Сети

Сетевые порты

Группы безопасности

Ключевая пара

Конфигурация

Группы серверов

Подсказки планировщика

Метаданные

Ключевая пара позволяет войти в новый экземпляр по SSH. Можно выбрать существующую пару ключей, импортировать пару ключей или сгенерировать её.

+ Создать ключевую пару

Импортировать ключевую пару

Выделенный

Отображено 0 значений

Название	Тип
Выберите одну из доступных пар ключей.	

Отображено 0 значений

▼ Доступно 3

Выберите одну

Нажмите здесь, для фильтрации или полнотекстового поиска

Отображено 3 значения

Название	Тип	
> my-keypair	ssh	↑
> shared-temasky-ad-keypair	ssh	↑
> test-key-pair	ssh	↑

После выполнения всех действий - нажать справа снизу кнопку **запустить инстанс** для создания и запуска виртуальной машины.

5. Настройка правил безопасности.

Для работы с инстансом необходимо разрешить ему сетевое взаимодействие (например 80/TCP - HTTP, 22/TCP - SSH, 51820/UDP - other): Для этого нужно открыть **Проект** > **Сеть** > **Группы безопасности** > выбрать группу безопасности **default** и нажать - **управление правилами**

Проект

Доступ к API

Неиспользуемые ресурсы

Удалить

Сеть

Сетевые порталы

Сети

Интерфейсы

Группы безопасности

Проект / Сеть / Группы безопасности

Группы безопасности

Отображено 3 значения

Имя	ID группы безопасности	Описание	Действие
default	5474b112-5c3b-4282-60d9-4732aedc5c99	Default security group	Управление правилами
interconnect	96311152-32d3-4122-9d36-dac5287ec0d9	Allow all traffic	Управление правилами

В открывшемся меню добавить правило для входящего трафика

Проект

Доступ к API

Вычислительные ресурсы

Диски

Сеть

Сетевая топология

Сети

Маршрутизаторы

Группы безопасности

Плавающие IP

Проект / Сеть / Группы безопасности / Управление правилами гру...

Управление правилами группы безопасности: default

Отображено 2 значения

Direction

Ether Type

IP Protocol

Port Range

Remote IP Prefix

Remote Security Group

Description

Actions

Исходящий трафик

IPv4

Любой

Любой

0.0.0.0/0

-

-

Удалить правило

Входящий трафик

IPv4

Любой

Любой

0.0.0.0/0

-

-

Удалить правило

Отображено 2 значения

+ Добавить правило

Удалить правила

В открывшемся меню добавления правил, добавить правило для порта 80(tcp)

Для этого выбрать:

Правило: «Настраиваемое правило TCP»

Направление: Входящий трафик

Порт: 80

Формат записи подключаемого диапазона адресов: CIDR

Сам подключаемый диапазон адресов: 0.0.0.0/0

Последняя запись означает разрешение подключения с любого адреса.

После заполнения всех полей нажать кнопку

Добавить

 в правом нижнем углу.

Добавить правило



Правило *

Настраиваемое правило TCP

Описание ?

Направление

Входящий трафик

Открыть порт *

Порт

Порт * ?

80

Удаленный адрес * ?

CIDR

CIDR * ?

0.0.0.0/0

Тип сети

IPv4

Описание:

Правила определяют, какой трафик разрешен экземплярам, которым назначена группа безопасности. Правило группы безопасности состоит из трех основных частей:

Правило: Вы можете задать желаемый шаблон правила или использовать настраиваемые правила через опции Настраиваемое TCP Правило, Настраиваемое UDP Правило или Настраиваемое ICMP Правило.

Открываемый Порт/Диапазон портов: Для TCP и UDP правил вы можете открыть отдельный порт или диапазон портов. Выбор опции "Диапазон Портов" предоставит вам форму для ввода начального и конечного портов диапазона. Для ICMP правил вам необходимо будет указать ICMP тип и код в предоставленной форме.

Удаленная сторона: Вы должны указать источник трафика который будет разрешен этим правилом. Вы можете указать блок IP адресов (CIDR) или группу безопасности. Выбор группы безопасности предоставит доступ любым экземплярам из указанной группы к любым экземплярам к которым применится это правило.


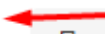
Отмена

Добавить



То же самое необходимо сделать для всех остальных портов.

6. Узнать адрес виртуальной машины



Для этого вернуться во вкладку экземпляры и в поле IP адрес будет IP адрес вашего виртуального экземпляра. Этот адрес понадобится в дальнейшем, для подключения к нему и его настройки.

Проект   Проект / Вычислительные ресурсы / Инстансы

Доступ к API


Вычислительные ресурсы   **Инстансы**


Обзор


Инстансы  ID инстанса 


Образы Отображено 7 значений

Ключевые пары ☐

<input type="checkbox"/>	Instance Name	Image Name	IP Address	Flavor	
	my-instance	Ubuntu-server-20.04:docker	xxx.xxx.xxx.xxx	small	-

Группы серверов 

Диски  Отображено 7 значений



Подключение к VM

7. Putty

Сделать это можно, например, с помощью `putty`. Для этого необходимо перейти на [страницу загрузки](#), выбрать `msi` установщик, так как понадобятся дополнительные компоненты. Открыть `puttygen`, нажать кнопку `load` и выбрать скачанный в п.2 ключ с расширением `.pem`. Puttygen автоматически подставит все поля из ключа. Далее необходимо нажать кнопку `save private key`, и выбрать место, куда ключ будет сохранен.

PuTTY Key Generator

File Key Conversions Help

Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDBFzEj6HZ/oT2812yr1KhDhayQ7CqPLyL
B7VY5PxbkNNsKbMJcn8Mr4feR0dZhFmKDu1XlugFDJVhUUYGjXC3kYmd1i1mJtdsR
UAeKcoY9q
+ZcabJQcRAgcHe1Sj7WpJcOCwpGZj1eVYiOCLC4JLTSUU2zGUFYD08uzZAWsNlu
```

Key fingerprint: ssh-rsa 2048 49:2a:a6:47:ca:6a:a0:61:5e:e1:04:4e:ea:f6:21:1a

Key comment: imported-openssh-key

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair 1 Generate

Load an existing private key file Load

Save the generated key Save public key Save private key

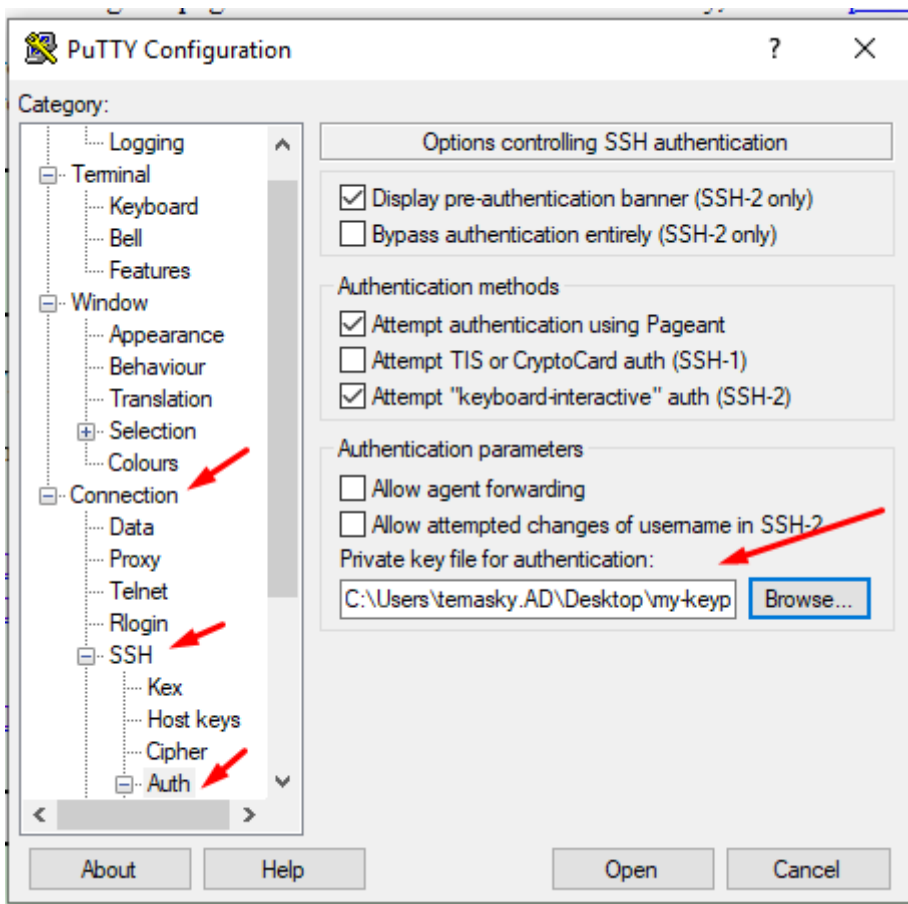
Parameters

Type of key to generate:

☒ RSA ☐ DSA ☐ ECDSA ☐ Ed25519 2 ☐ SSH-1 (RSA)

Number of bits in a generated key: 2048

Открыть расположение сохраненного ключа, и два раза нажать на него, для запуска помощника авторизации `agent` (`agent` откроется в трее рабочего стола, пользователь не увидит запуск никаких приложений на рабочем столе) Запустить `putty` Открыть меню `connection -> SSH -> Auth` и в открывшемся меню в поле `private key for authentication` выбрать путь к сгенерированному ключу



Открыть заново вкладку `session`, ввести адрес нашей VM и нажать `Open`. В открывшемся окне терминала ввести имя пользователя `cloudadmin`. Это позволит получить удалённый доступ к вашей виртуальной машине.

8. Linux

Для подключения в большинстве дистрибутивов уже установлены SSH-агенты и для подключения используя ключ достаточно добавить его в агент.

Для этого нужно выполнить команду, где `pemkey.pem`, это файл полученный вами на 3 пункте данной инструкции

```
ssh-add pemkey.pem
```

Для подключения в данном случае в терминале достаточно ввести команду:

```
ssh cloudadmin@172.17.5.1
```

“ адрес `172.17.5.1` необходимо заменить на ваш адрес полученный из пункта 6 инструкции

9. Windows 10 OpenSSH

В Windows 10 с версии 1809 включен пакет OpenSSH, проверить это можно с помощью команды (выполняется с правами администратора):

“ Дальнейшие действия выполняются в PowerShell

```
Get-WindowsCapability -Online | ? Name -like 'OpenSSH.Client*'
```

```
PS C:\Users\tarab> Get-WindowsCapability -Online | ? Name -like 'OpenSSH.Client*'

Name : OpenSSH.Client~~~~0.0.1.0
State : Installed
```

Если SSH клиент отсутствует (State: Not Present), его можно установить:

```
Add-WindowsCapability -Online -Name OpenSSH.Client*
```

Далее необходимо включить SSH-агент:

```
Start-Service ssh-agent
```

Добавить ключ можно с помощью команды:

```
ssh-add "C:\Users\username\.ssh\id_rsa"
```

Теперь вы можете подключиться используя команду:

```
ssh cloudadmin@172.17.5.1
```

“ адрес 172.17.5.1 необходимо заменить на ваш адрес полученный из пункта 6 инструкции

Версия #13

Тарабанов Илья Федорович создал 12 мая 2022 16:09:55

Тарабанов Илья Федорович обновил 27 апреля 2023 18:25:33