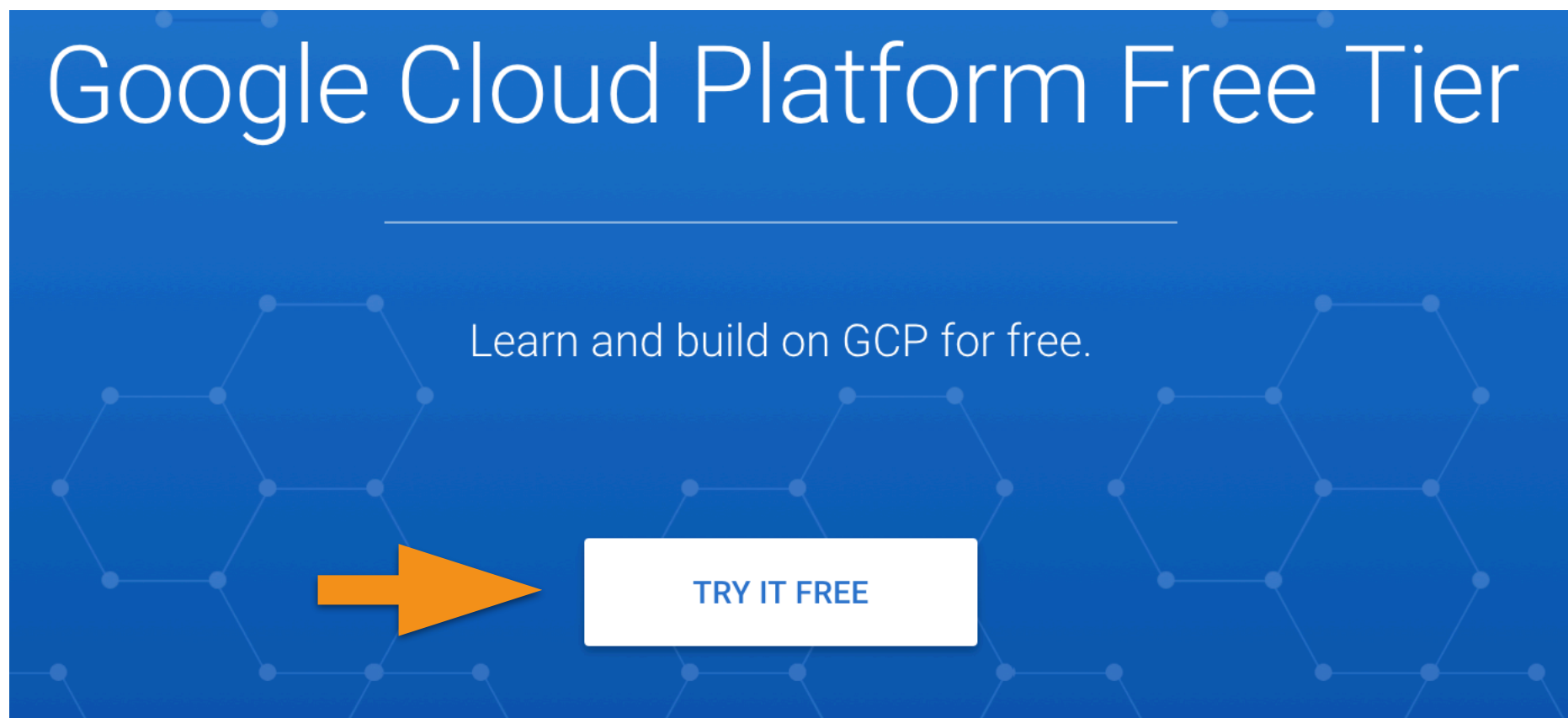


# Знакомство с облачной инфраструктурой Google Cloud Platform



# Создание учетной записи в Google Cloud Platform

Необходимо зарегистрироваться по ссылке  
<https://cloud.google.com/free/>



Для регистрации рекомендуется использовать новую и отдельную учетную запись Google

# Создание учетной записи в Google Cloud Platform



Попробуйте Cloud Platform бесплатно

Google

Страна

Россия

Условия использования

Я хочу получать информацию о новых функциях, советы по повышению производительности, приглашения поделиться отзывом или поучаствовать в опросе, а также специальные предложения.

☐ Да ☒ Нет

Я принимаю [Условия использования](#) и соглашаюсь с тем, что ими регулируется любое использование [сервисов и связанных с ними API](#). Я принимаю [Условия бесплатного пробного периода Google Cloud Platform](#).  
Это обязательное поле.

☒ Да ☐ Нет

Принять и продолжить


# Создание учетной записи в Google Cloud Platform

Во время регистрации Google может запросить ввести данные платежной карты, это единственное платежное требование.

После окончания trial периода Google не будет автоматически снимать средства с карты, можно не волноваться. На предлог использовать карту после окончания trial периода, рекомендуется отказываться от подобных предложений.


# Создание учетной записи в Google Cloud Platform


Заполняем требуемые для регистрации поля

 Google Cloud Platform

Попробуйте Cloud Platform бесплатно [Google](#)

**Сведения о клиенте**

 Тип аккаунта ⓘ  
юридического лица

 Наименование и адрес ⓘ

Название компании  
otus

Имя  
otus otus

Первая строка адреса  
Uchenicheskaya 12/3

Вторая строка адреса

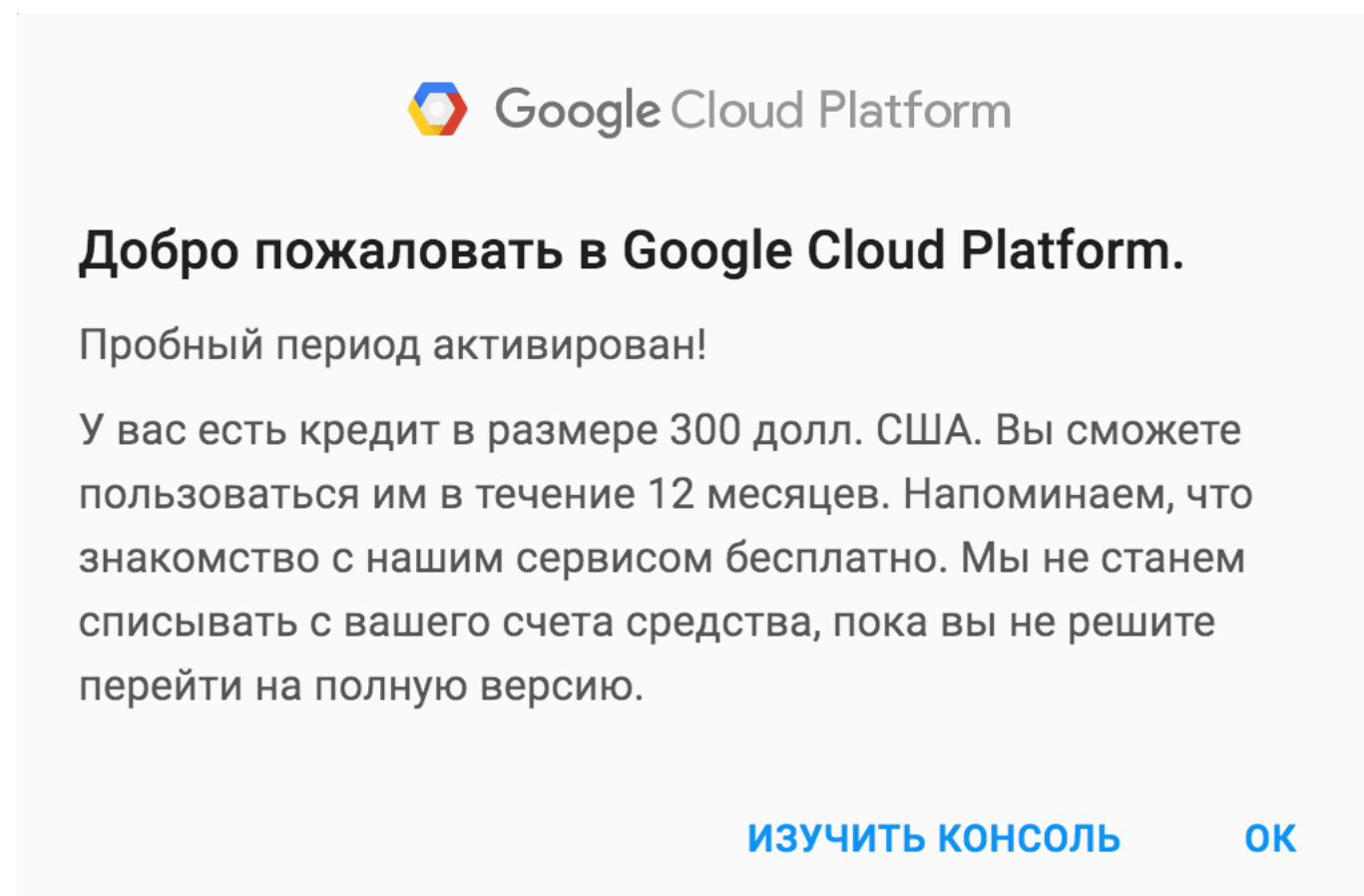
Город  
Moscow

Область  
Москва

Индекс  
119000 ⓘ

# Создание учетной записи в Google Cloud Platform

В конце успешной регистрации должно отобразиться окно приветствия



# Основные элементы управления

The screenshot shows the Google Cloud Platform console interface. The top navigation bar is blue and contains the Google Cloud Platform logo, a project selection dropdown menu labeled "Выберите проект", a search bar, and a set of utility icons including a mail icon, an exclamation mark, a question mark, a bell, and a user profile icon. Below the navigation bar, the main content area features three prominent cards: "Запустите сервис Compute Engine" (highlighted with a blue background), "Попробуйте Cloud Storage", and "Изучите интерактивные руководства". Each card includes a brief description and a "Начать" (Get started) button. Orange arrows and text annotations are overlaid on the image to identify key UI elements.

Google Cloud Platform Выберите проект

Начало работы

Выбор проекта с облачными сервисами

Основное меню облачных сервисов

Запустите сервис Compute Engine

Создайте виртуальную машину Google Compute Engine и запустите в ней приложение "Список задач" на базе Node.js и MongoDB.

Попробовать Compute Engine

Попробуйте Cloud Storage

Cloud Storage – это мощный и удобный сервис хранения. Изучив наше руководство, вы узнаете, как создавать сегмент хранилища, загружать в него файлы и предоставлять доступ к ним по ссылке.

Попробовать Cloud Storage

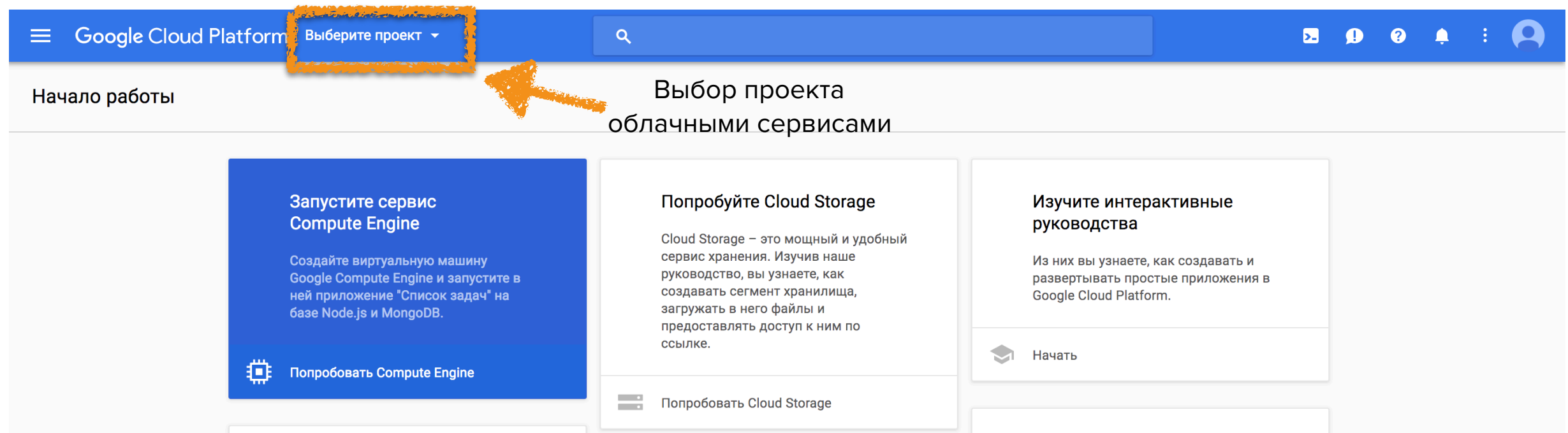
Изучите интерактивные руководства

Из них вы узнаете, как создавать и разворачивать простые приложения в Google Cloud Platform.

Начать

Cloud shell, справочная информация и уведомления по учетной записи

# Создаем новый проект



The screenshot shows the Google Cloud Platform console interface. At the top, there is a blue header bar with the Google Cloud Platform logo, a search bar, and several utility icons. Below the header, the main content area is titled "Начало работы" (Getting started). A prominent orange box highlights the "Выберите проект" (Select project) dropdown menu in the top navigation bar, with an orange arrow pointing to it. Below this, the main content area is titled "Выбор проекта облачными сервисами" (Select project with cloud services). It features three main cards: "Запустите сервис Compute Engine" (Launch Compute Engine service), "Попробуйте Cloud Storage" (Try Cloud Storage), and "Изучите интерактивные руководства" (Learn interactive guides). Each card contains a brief description and a "Начать" (Get started) button.

Google Cloud Platform Выберите проект

Начало работы

Выбор проекта облачными сервисами

**Запустите сервис Compute Engine**

Создайте виртуальную машину Google Compute Engine и запустите в ней приложение "Список задач" на базе Node.js и MongoDB.

Попробовать Compute Engine

**Попробуйте Cloud Storage**

Cloud Storage – это мощный и удобный сервис хранения. Изучив наше руководство, вы узнаете, как создавать сегмент хранилища, загружать в него файлы и предоставлять доступ к ним по ссылке.

Попробовать Cloud Storage

**Изучите интерактивные руководства**



Из них вы узнаете, как создавать и разворачивать простые приложения в Google Cloud Platform.


Начать




# Создаем новый проект

## Выбор области действия



Недавние Все

Название	Идентификатор
 Без организации	0

ОТМЕНА ОТКРЫТЬ

# Создаем новый проект

## Создание проекта

i Остаток проектов в рамках квоты 12. [Подробнее...](#)

Название проекта ?

Идентификатор проекта: week-3-178304. ? [Изменить](#)

Ожидаем до минуты, в окне уведомления должна появиться нотификация, выбираем созданный проект

# Работа с Google Compute Engine

В следующих заданиях мы будем работать с IaaS слоями Google Compute Platform

- VPC сети (Virtual Private Network)
- GCE Metadata (для управления ключами доступа к серверам)
- GCE VM (для создания и управления инстансами виртуальных машин)

Создадим пару ключей и привяжем ее к метаданным GCE (Google Compute Engine) для последующего получения доступа на виртуальные машины

# Работа с Google Compute Engine

Из основного меню переходим в Compute Engine (GCE), ожидаем активации

Compute Engine

Экземпляры VM

Экземпляры VM

Группы экземпляров

Шаблоны экземпляров

Диски

Снимки

Образы

Скидки за обязательства ...

Метаданные

Проверки состояния

Зоны

Операции

Квоты

Настройки

Идет активация Compute Engine. Это может занять несколько минут. [Документация по Compute Engine](#)

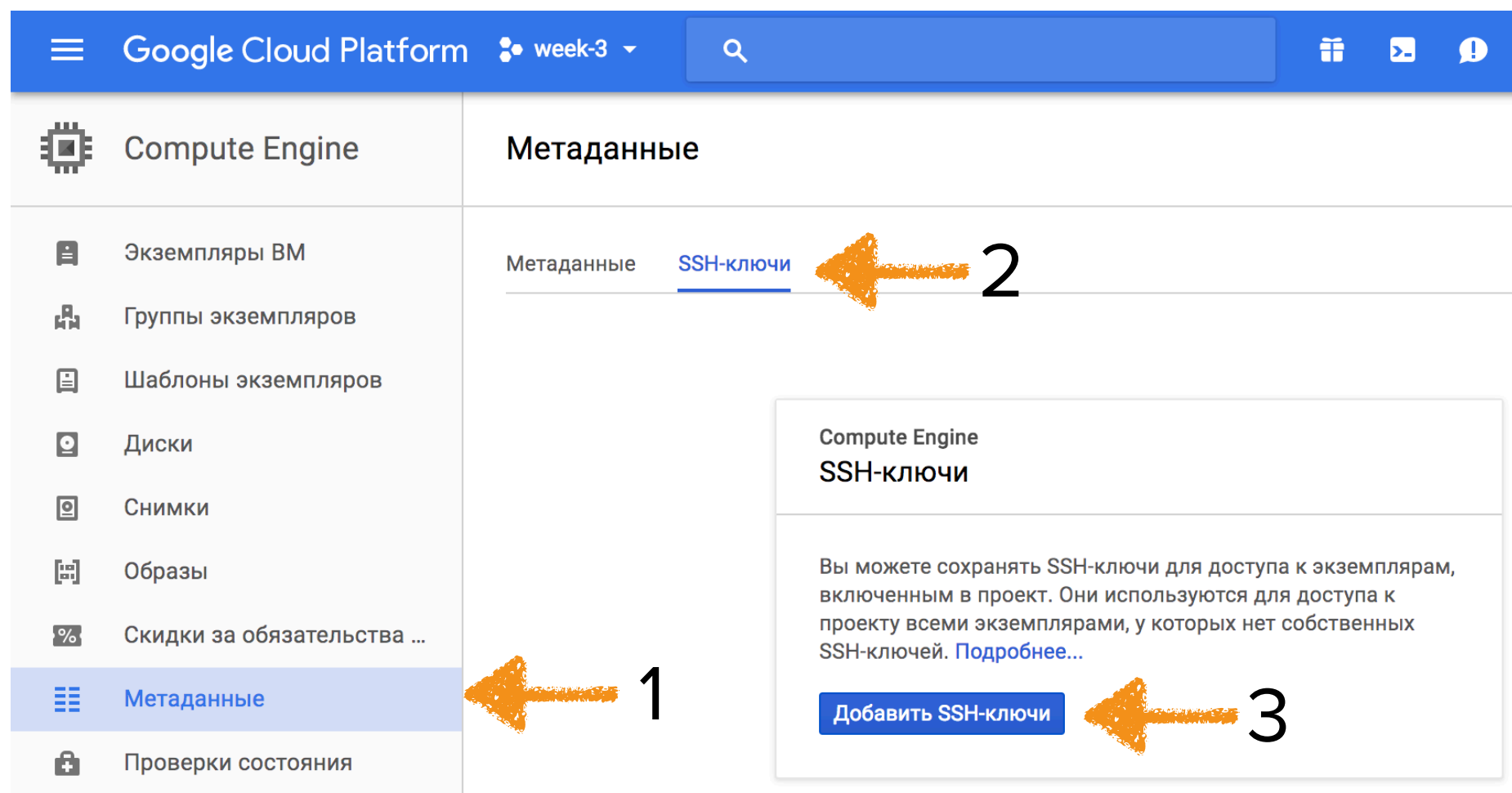
Compute Engine  
Экземпляры VM

Сервис Compute Engine позволяет вам запускать свои собственные VM в инфраструктуре Google – от микромашин до более крупных систем, на которые можно устанавливать Debian, Windows и другие стандартные образы. Создайте экземпляр VM и импортируйте его через CloudEndure или запустите быструю настройку, чтобы развернуть типовое приложение.

Создать или Перенести или Запустить мастер

# Работа с Google Compute Engine (метаданные)

Для начала перейдем в раздел меню Метадата, выберем вкладку SSH ключи и нажмем добавить ssh-ключи



The screenshot shows the Google Cloud Platform interface. The top navigation bar includes the Google Cloud Platform logo, a dropdown menu for 'week-3', a search bar, and icons for settings, help, and notifications. The left sidebar contains a list of services: Compute Engine, VM instances, VM instance groups, VM instance templates, Disks, Snapshots, Images, and Discounts for commitments. The 'Metadata' service is selected, indicated by an orange arrow and the number 1. The main content area displays the 'Metadata' section for Compute Engine. The 'SSH-keys' tab is selected, indicated by an orange arrow and the number 2. A modal window titled 'Compute Engine SSH-ключи' is open, showing instructions on how to use SSH keys for access to VM instances. The 'Add SSH-keys' button is highlighted with an orange arrow and the number 3.

# Генерация пары ключей

На вашей пользовательской Linux/Unix системе необходимо сгенерировать пару ключей можно при помощи утилиты `ssh-keygen` (часть `ssh-agent`)

Пример:

```
ssh-keygen -f ~/.ssh/week3
```

```
$ ssh-keygen -f ~/.ssh/week3
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /Users/serj/.ssh/week3.
Your public key has been saved in /Users/serj/.ssh/week3.pub.
The key fingerprint is:
SHA256:pgfTRnJe4CFMJ+2Vp/N1R0cJCH0iS7ejcsvxRzLWHpI serj@mbps.local
The key's randomart image is:
+---[RSA 2048]---+
|  o+.+++.o....o|
|  .=00*.. .o|
|  .++o.o  ..|
|  .*+..+  .o|
|  o.Sooo .  ..|
|  *.E.+  .|
|  ..+o *  .|
|  ++  o|
|  o  ..|
+-----[SHA256]-----+
```

# Генерация пары ключей

В результате действий предыдущего слайда, мы получаем пару из приватного и публичного ключей в домашнем каталоге текущего пользователя системы

## **Приватный ключ**

`~/ .ssh/week3`

## **Публичный ключ**

`~/ .ssh/week3.pub`

# Вносим в форму публичный ключ

Содержимое ~/.ssh/week3.pub вносим в форму ввода ключа и нажимаем сохранить

Метаданные SSH-ключи

serj

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQD975+kRV1gX2pk0XA0grtSmJgxkHtdjlRv
oYQvFCnNR015agodPKeU3YlGLIPbmShIeiM0ebk+V7l/WP0HjSH3Ao8izI+TQ1PcBTQEUSi
dBeI9LFmigTrDi6052PENQKqC+Q8e6bvOzFL79o9Le8P7RuG2tTVn1B+N18HIdbVFwD0MNuo
17o9u0tm1Mn0J7+aLiVZLN2D2dquGPftUw5adhmxYVt3ujqXR3VEtP+BjgLjFQtH2LjzNDaU
OkN/MBkCAPmicELinHGZQfS+4+Dhpjr6fau8pAz+kj8hTPfV36VRRjFaY++jBApR+hnMEiJ3
50wiQSAhzN6s/hmyWaoZ serj@mbps.local
```



+ Добавить

Сохранить

Отмена



# ssh-ключи в Метадате проекта GCP

- Действуют на все виртуальные машины в проекте
- Могут быть переопределены при создании виртуальной машины
- Могут быть заблокированы при создании виртуальной машины - чтобы ни один из описанных в метадате проекта ключей не использовался

# Создаем Экземпляр VM (инстанс)

The screenshot shows the Google Cloud Platform console interface. The top navigation bar includes the Google Cloud Platform logo, a dropdown menu for 'week-3', a search bar, and icons for help and notifications. The left sidebar contains a list of navigation items: Compute Engine, Экземпляры VM (highlighted), Группы экземпляров, Шаблоны экземпляров, Диски, Снимки, Образы, Скидки за обязательства ..., Метаданные, Проверки состояния, Зоны, and Операции. The main content area is titled 'Экземпляры VM'. A modal window is displayed in the center-right, titled 'Compute Engine Экземпляры VM'. It contains a paragraph of text explaining the service and three buttons: 'Создать' (Create), 'Перенести' (Move), and 'Запустить мастер' (Run wizard). An orange arrow points to the 'Создать' button.

Google Cloud Platform week-3

Compute Engine

Экземпляры VM

Экземпляры VM

Группы экземпляров

Шаблоны экземпляров

Диски

Снимки

Образы

Скидки за обязательства ...

Метаданные

Проверки состояния

Зоны

Операции

Compute Engine  
Экземпляры VM

Сервис Compute Engine позволяет вам запускать свои собственные VM в инфраструктуре Google – от микромашин до более крупных систем, на которые можно устанавливать Debian, Windows и другие стандартные образы. Создайте экземпляр VM и импортируйте его через CloudEndure или запустите быструю настройку, чтобы развернуть типовое приложение.

Создать или Перенести или Запустить мастер

# Создаем Экземпляр VM (инстанс)

The screenshot shows the Google Cloud Platform console interface. The top navigation bar includes the Google Cloud Platform logo, a dropdown menu for 'week-3', a search bar, and icons for help and notifications. The left sidebar contains a list of navigation items: Compute Engine, Экземпляры VM (highlighted), Группы экземпляров, Шаблоны экземпляров, Диски, Снимки, Образы, Скидки за обязательства ..., Метаданные, Проверки состояния, Зоны, and Операции. The main content area is titled 'Экземпляры VM'. A modal window is displayed in the center-right, titled 'Compute Engine Экземпляры VM'. It contains a paragraph of text explaining the service and three buttons: 'Создать' (Create), 'Перенести' (Move), and 'Запустить мастер' (Run wizard). An orange arrow points to the 'Создать' button.

Google Cloud Platform week-3

Compute Engine

Экземпляры VM

Экземпляры VM

Группы экземпляров

Шаблоны экземпляров

Диски

Снимки

Образы

Скидки за обязательства ...

Метаданные

Проверки состояния

Зоны

Операции

Compute Engine  
Экземпляры VM

Сервис Compute Engine позволяет вам запускать свои собственные VM в инфраструктуре Google – от микромашин до более крупных систем, на которые можно устанавливать Debian, Windows и другие стандартные образы. Создайте экземпляр VM и импортируйте его через CloudEndure или запустите быструю настройку, чтобы развернуть типовое приложение.

Создать или Перенести или Запустить мастер

# Создаем Экземпляр VM (инстанс)

Вбиваем имя хоста: **bastion** ← Создать экземпляр

Зона: **europe\***

Тип машины:

**микромашина**

Загрузочный диск: **Ubuntu 16.04**

Название ?

bastion

Зона ?

europe-west1-d

Тип машины

микромашина...

0,6 ГБ памяти

[Настроить](#)

Если вы [перейдете на платный аккаунт](#), то сможете создавать экземпляры с количеством ядер до 64.

Загрузочный диск ?



Новый стандартный постоянный диск объемом 10 ГБ

Образ

Ubuntu 16.04 LTS

[Изменить](#)

# Создаем Экземпляр VM (инстанс)

Настройка параметров сети -> Сеть -> Сетевой интерфейс

Оставляем сеть **default**  
Внешний IP: **Создать адрес**  
Название адреса: **bastion**

default сеть может отличаться от той что на скриншоте, это нормально

Сетевые интерфейсы ?

Сетевой интерфейс

Сеть ?

default

Подсеть ?

default (10.132.0.0/20)

Основной внутренний IP-адрес ?

Назначается автоматически

Показать псевдонимы диапазонов IP-адресов

Внешний IP-адрес ?

bastion (146.148.26.242)

IP-перееадресация ?

Выкл.

Готово

Отмена

# Создаем Экземпляр VM (инстанс)

# Нажимаем **Создать** инстанс и дожидаемся готовности VM на панели Compute Engine

Экземпляры ВМ

Группы экземпляров

Шаблоны экземпляров

Диски

Снимки

Введите фильтр

<input type="checkbox"/> <div>Название ^</div>	Зона	Рекомендация	Внутренний IP-адрес	Внешний IP-адрес	Подключиться
<input type="checkbox"/> <div>✓ bastion</div>	us-central1-c		10.128.0.2	Внешний IP	SSH <div></div>

# Проверяем подключение по полученному внешнему адресу

Проверяем из локальной консоли подключение к созданной VM

```
> ssh -i ~/.ssh/week3 ubuntu@<внешний IP VM>
```

```
$ ssh -i ~/.ssh/week3 ubuntu@<внешний ip VM>
The authenticity of host '146.148.80.202 (146.148.80.202)' can't be established.
ECDSA key fingerprint is SHA256:TdC2ZuIT+T0B3Q0KtqKCLu5sgWmttoNMqZHQLvm10kM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '146.148.80.202' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.10.0-32-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud

0 packages can be updated.
0 updates are security updates.

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@bastion:~$ cat /etc/issue
Ubuntu 16.04.3 LTS \n \l
```



Часть IaaS состоит из сетевого слоя, это не значит что управление им обязательно должно отдельно выполняться через раздел VPC

В нашем случае, при создании проектов автоматом создавалось по одной приватной сети на каждый регион и шлюз для выхода в интернет

При создании VM мы также указали, что хотим завести статический внешний IP bastion, который также будет виден в VPC разделе



# VPC: приватные сети

Из главного меню, откройте раздел VPC

Сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Сети VPC

Внешние IP-адреса









Правила брандмауэра




Маршруты

Точки обмена данными V...

Общая сеть

# VPC: Публичные адреса

 Сеть VPC	Внешние IP-адреса    <a href="#">ПОКАЗАТЬ ИНФОРМАЦИЮ</a>					
 Сети VPC						
 Внешние IP-адреса						
 Правила брандмауэра						
 Маршруты						

<input type="checkbox"/>	Название	Внешний адрес	Регион	Тип 	Версия	Используется
						
<input type="checkbox"/>	bastion	146.148.80.202	us-central1	Статический 	IPv4	Экземпляр bastion Зона с

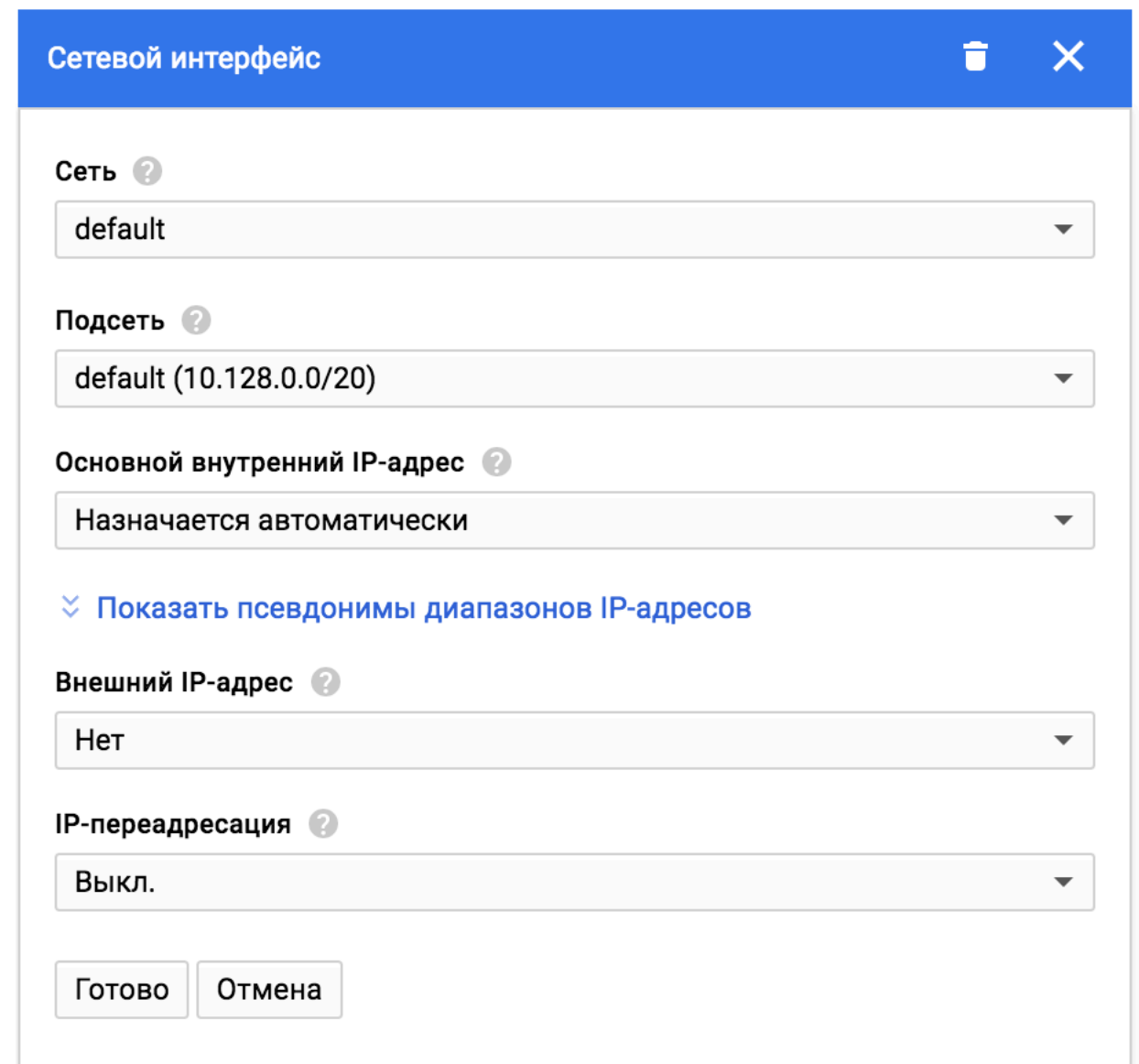


Примеры управления сетями и разделение топологий будут описаны в будущих лекциях, с использованием инструментов, работающих через API интерфейс

# Создаем вторую VM без внешней сети

По аналогии с предыдущими шагами по созданию VM, инициировать создание второй машины с именем **someinternalhost**

Среди отличий в создании, в разделе управления сетями, убрать создание публичного адреса (см скриншот)



Сетевой интерфейс

Сеть ?  
default

Подсеть ?  
default (10.128.0.0/20)

Основной внутренний IP-адрес ?  
Назначается автоматически

✕ Показать псевдонимы диапазонов IP-адресов

Внешний IP-адрес ?  
Нет

IP-переадресация ?  
Выкл.

Готово Отмена

# Проверяем результат

Compute Engine

Экземпляры VM

Группы экземпляров

Шаблоны экземпляров

Диски

Снимки

Образы

+

↓

↺

▶

■

↻

🗑

ПОКАЗАТЬ ИНФОРМАЦИОННУЮ ПАНЕЛЬ

Введите фильтр

?

Столбцы ▼

<input type="checkbox"/> <b>Название</b> ^	Зона	Рекомендация	Внутренний IP-адрес	Внешний IP-адрес	Подключиться	
<input type="checkbox"/> bastion	us-central1-c		10.128.0.2	<Внешний адрес VM>	SSH ▼	⋮
<input type="checkbox"/> someinternalhost	europa-west1-d		10.132.0.2	Не задан	SSH ▼	⋮

# Рассмотрим текущее состояние хостов

Для верности эксперимента, пробуем зайти по ssh на **bastionhost**, а с него по внутреннему адресу на **internalhost** (используйте ваши адреса)

```
$ ssh -i ~/.ssh/week3 ubuntu@146.148.80.202
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.10.0-32-generic x86_64)
 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
  Get cloud support with Ubuntu Advantage Cloud Guest:
    http://www.ubuntu.com/business/services/cloud
0 packages can be updated.
0 updates are security updates.
Last login: Tue Aug 29 06:32:23 2017 from 79.164.31.28
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
ubuntu@bastion:~$ ssh 10.132.0.2
Permission denied (publickey).
ubuntu@bastion:~$
```

Результат неудовлетворителен

# Используем Bastion host для прямого подключения к инстансам в внутренней сети

Настроим SSH Forwarding на вашей локальной машине

```
$ ssh-add -L  
The agent has no identities.
```

Добавим приватный ключ в ssh агент авторизации

```
$ ssh-add ~/.ssh/week3  
Identity added: /Users/otus/.ssh/week3 (/Users/otus/.ssh/week3)
```

# Используем Bastion host для сквозного подключения

Попробуем подключаться вновь, добавив в параметры подключения ключик -A для явного указания намерения использовать Agent Forwarding

```
$ ssh -i ~/.ssh/week3 -A ubuntu@146.148.80.202
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.10.0-32-generic x86_64)
ubuntu@bastion:~$ ssh 10.132.0.2
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.10.0-32-generic x86_64)
 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud
0 packages can be updated.
0 updates are security updates.
Last login: Tue Aug 29 06:32:27 2017 from 10.128.0.2
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
ubuntu@someinternalhost:~$ hostname
someinternalhost
ubuntu@someinternalhost:~$ ip a show ens4
2: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1460 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 42:01:0a:84:00:02 brd ff:ff:ff:ff:ff:ff
    inet 10.132.0.2/32 brd 10.132.0.2 scope global ens4
        valid_lft forever preferred_lft forever
    inet6 fe80::4001:aff:fe84:2/64 scope link
        valid_lft forever preferred_lft forever
```



# Успех, но не очень удобно

Проверим отсутствие каких-либо приватных ключей на bastion машине

```
ubuntu@bastion:~$ ls -la ~/.ssh/  
total 16  
drwx----- 2 ubuntu ubuntu 4096 Aug 29 06:07 .  
drwxr-xr-x 4 ubuntu ubuntu 4096 Aug 29 06:07 ..  
-rw----- 1 ubuntu ubuntu 397 Aug 29 05:50 authorized_keys  
-rw-r--r-- 1 ubuntu ubuntu 222 Aug 29 06:03 known_hosts
```

# Самостоятельное задание

Исследовать способ подключения к **internalhost** в одну команду из вашего рабочего устройства, проверить работоспособность найденного решения и отписать вариант решения преподавателю

**Бонусная часть:** Предложить вариант решения для подключения из консоли при помощи команды вида `ssh internalhost` из локальной консоли рабочего устройства, чтобы подключение выполнялось по алиасу `internalhost`

# Создаем VPN сервер для серверов GCP

Не удаляя предыдущие серверы, создадим схему с VPN сервером, после сгенерируем конфигурацию VPN клиента и подключимся к VPN сети с последующим доступом в частную сеть облака

# Создаем VPN сервер для серверов GCP

Перед установкой перейдем в настройки bastion VM через панель управления и проставим в Фаерволла отметки разрешения http/https трафика

## Брандмауэры

- ☒ Разрешить трафик HTTP
- ☒ Разрешить трафик HTTPS

# Создаем VPN сервер для серверов GCP

На хосте **bastion** выполняем команды

```
$ cat <<EOF> setupvpn.sh
#!/bin/bash
echo "deb http://repo.mongodb.org/apt/ubuntu xenial/mongodb-org/3.4 multiverse" > /etc/
apt/sources.list.d/mongodb-org-3.4.list
echo "deb http://repo.pritunl.com/stable/apt xenial main" > /etc/apt/sources.list.d/
pritunl.list
apt-key adv --keyserver hkp://keyserver.ubuntu.com --recv
0C49F3730359A14518585931BC711F9BA15703C6
apt-key adv --keyserver hkp://keyserver.ubuntu.com --recv
7568D9BB55FF9E5287D586017AE645C0CF8E292A
apt-get --assume-yes update
apt-get --assume-yes upgrade
apt-get --assume-yes install pritunl mongodb-org
systemctl start pritunl mongod
systemctl enable pritunl mongod
EOF
```

Затем

```
$ sudo bash setupvpn.sh
```

# Создаем VPN сервер для серверов GCP

На хосте **bastion** выполняем команды

```
$ cat <<EOF> setupvpn.sh
> #!/bin/bash
> echo "deb http://repo.mongodb.org/apt/ubuntu xenial/mongodb-org/3.4 multiverse" > /etc/
apt/sources.list.d/mongodb-org-3.4.list
> echo "deb http://repo.pritunl.com/stable/apt xenial main" > /etc/apt/sources.list.d/
pritunl.list
> apt-key adv --keyserver hkp://keyserver.ubuntu.com --recv
0C49F3730359A14518585931BC711F9BA15703C6
> apt-key adv --keyserver hkp://keyserver.ubuntu.com --recv
7568D9BB55FF9E5287D586017AE645C0CF8E292A
> apt-get --assume-yes update
> apt-get --assume-yes upgrade
> apt-get --assume-yes install pritunl mongodb-org
> systemctl start pritunl mongod
> systemctl enable pritunl mongod
> EOF
```

Затем

```
$ sudo bash setupvpn.sh
```

# Создаем VPN сервер для серверов GCP

Открываем в браузере ссылку  
`http://<адрес bastion VM>/setup`

Ошибку SSL пропускаем и доверяем этому сайту, следуем инструкциям на экране (запрашиваемые команды запускать через **sudo**)

# Создаем VPN сервер для серверов GCP

В конце установки авторизуемся используя  
следующие данные

Имя пользователя: **pritunl**

Пароль: **pritunl**



# Создаем VPN сервер для серверов GCP

В конце установки авторизуемся используя  
следующие данные

Имя пользователя: **pritunl**

Пароль: **pritunl**