﻿ Добрый день, уважаемые студенты, на сессии разбора лабораторной работы. Тема лабораторной работы – это Amazon VPC и её компоненты. Так как эта сессия является разбором, то я буду фактически выполнять эту лабораторную работу, и по ходу выполнения буду давать от себя дополнительные комментарии, для того чтобы пояснить, что мы делаем.

Итак, давайте начнём. Эту сессию мы начнём с основной страницы лабораторной работы. Для того чтобы добраться до этой страницы, вам необходимо авторизоваться в AWS Academy, и перейти на соответствующий курс Cloud Practitioner. Далее необходимо в пятом модуле найти активность Lab 2: Build your VPC and Launch a Web Server. Как только вы перейдете по ссылке, вы попадете на эту страницу. Также ожидается, что вы инициировали создание временного AWS аккаунта для вашей сессии, нажав на кнопку Start Lab в верхнем правом меню. Как только это все будет готово, мы можем начинать. Нам необходимо нажать на кнопку AWS. Мы будем направлены на главную страницу AWS Management Console.

В AWS Management Console сверху справа видим, что мы авторизовались под временным пользователем для того чтобы выполнить нашу лабораторную работу. Хорошо, нам необходимо перейти на главную страницу сервиса Amazon VPC. Для этого в строке поиска сервисов начнём вводить VPC и в поисковой выдаче мы увидим самую первую необходимую нам ссылку. Давайте на нее нажмем, чтобы перейти на сервис Amazon VPC. На основной странице Amazon VPC нам необходимо в левом навигационном меню вверху убедиться, что переключатель включен, и мы сидим в новом интерфейсе сервиса Amazon VPC. Далее там же в левом навигационном меню необходимо нажать на вкладку VPC Dashboard, и на открывшейся странице нажать на кнопку Create VPC для того чтобы создать новую VPC. На открывшейся странице мы сейчас будем вводить необходимые для нас значения, для того чтобы создать кастомную VPC с необходимыми нам настройками. В VPC Settings давайте выберем VPC and more, для того чтобы создать еще и дополнительные компоненты внутри этой VPC. Как название нашей VPC введем Lab и поставим галочку на Auto-generate, эта галочка сгенерирует Tag Name со значением, которое мы ввели в поле, а именно Lab. Далее, если мы прокрутим чуть ниже, мы можем ввести наш IPv4 CIDR block для нашей VPC. Давайте введём 10.0.0.0/16, далее чуть ниже есть настройки количества Availability Zones, которые будут в VPC, нам необходимо выбрать одну Availability Zone. Чуть ниже необходимо указать, что у нас будет один Public Subnet, а также один Private Subnet. Если развернуть секцию Customize Subnets CIDR Blocks, то мы можем для всех наших Subnets конкретно указать CIDR Blocks. Для Public Subnets укажем 10.0.0.0/24. Для Private Subnets укажем 10.0.1.0/24. Далее, в настройках NAT Gateway укажем, что у нас один NAT Gateway в одной Availability Zone, а также мы не будем использовать VPC Endpoints. Самая последняя секция DNS Options, поставим флажки для обеих опций, т.е. Enable DNS hostnames, а также Enable DNS resolution. На основной странице с правой стороны вы видите preview, как будет выглядеть VPC, из каких компонентов она будет состоять. У нас будет создана VPC, которая называется lab-vpc. В этой VPC будет два Subnets, один Private, другой Public, с соответствующими названиями внутри Availability Zones us-east-1a. Далее у нас создаются два Route tables, один для Public Subnet, второй для Private Subnet. Из дополнительных компонентов это Network Connections, а именно Internet Gateway и NАT Gateway, которую мы создаем в одной Availability Zone.

Давайте вернёмся обратно к левой части страницы и нажмём на кнопку Create VPC для того чтобы запустить создание VPC и всех необходимых компонентов. Мы будем направлены на страницу, где будут указаны все компоненты, которые будут созданы вместе с нашей VPC. Создание NAT Gateway может занять некоторое время, от одной до трех минут, поэтому нам необходимо дождаться создания всех ресурсов. Как только все ресурсы будут созданы, вы увидите полный список, а также для некоторых ресурсов у вас будут доступны прямые ссылки. В самом низу страницы, также появится кнопка View VPC, для того чтобы перейти на главную страницу новой созданной VPC. Давайте на нее нажмем. Здесь вы видите все детали касательно нашей VPC. Давайте теперь создадим дополнительные Subnets в другой Availability Zone внутри нашей VPC. Для этого необходимо в левом навигационном меню нажать на вкладку Subnets. Мы перейдём на страницу со всеми Subnets в этом AWS аккаунте. Нам необходимо нажать на кнопку Create subnet в верхней правой части экрана. Мы окажемся на странице с настройками, с входными данными для создания нового Subnet. Как VPC ID нам необходимо выбрать наш новый VPC, который называется Lab-vpc из выпадающего списка. Далее необходимо указать имя Subnet – это Lab-subnet-public2. Если прокрутить чуть ниже, у нас есть возможность выбрать Availability Zone. Нам необходимо выбрать отличную другую Availability Zone. Как мы с вами помним для VPC мы для Subnet внутри VPC мы с вами выбирали Availability Zone us-east-1a, для нового нашего Subnet мы выберем другую Availability Zone, а именно us-east-1b. Также мы можем указать CIDR block, давайте напишем 10.0.2.0/24, для того чтобы она не пересекалась с существующими Subnet-ами, после чего внизу экрана нажмём на кнопку Create subnet.

Мы будем направлены на страницу со всеми Subnets, увидим сообщение зеленого цвета о том, что Subnet был успешно создан, а также отобразится список с одним только новым созданным нашим Subnet, так как при переходе на страницу автоматически был создан фильтр на этот Subnet. Теперь нам необходимо создать второй Private Subnet. Для этого необходимо нажать также на кнопку Create subnet. В открывшемся меню настроек нового Subnet нам необходимо также выбрать VPC, которая называется Lab-vpc. Далее как название Subnet укажем lab-subnet-private2. Как Availability Zone выберем вторую Availability Zone, а именно us-east-1b, и как CIDR block укажем следующий, не пересекающийся block – это 10.0.3.0/24. После чего нажмем на кнопку Create subnet.

Мы также увидим сообщение об успешном создании Subnet и отфильтрованный список с нашим новым Subnet. Далее нам необходимо наши новые созданные Subnets привязать к Route tables. Для этого в левом навигационном меню нажмем на вкладку Route tables. Откроется список всех Route tables в этом AWS аккаунте. Давайте начнём с Route table, который был создан для Private subnets. Выберем его из списка и перейдем на вкладку Route tables внизу экрана. Мы видим, что у нас есть два Route, второй – это Default, который позволяет всем Subnet-ам внутри VPC обмениваться информацией между собой. Первый – это тот Route, который был создан вместе с созданием нашей VPC, а именно мы указываем, что через NAT Gateway как Target мы выходим в интернет, который указан как Destination.

Давайте перейдём на следующую вкладку Subnet associations, для того чтобы посмотреть какие Subnets привязаны к этому Route table. Мы с вами увидим, что есть один явно привязанный Subnet, который также был создан вместе с созданием VPC и является Private subnet. Нам необходимо далее нажать на кнопку Edit subnet associations и привязать уже второй Private subnet к этому Route table. В отобразившемся списке мы увидим, что первый Private subnet уже был выбран, для того чтобы добавить второй Private subnet, мы тоже его отметим и в нижней правой части экрана нажмём на кнопку Save associations.

Хорошо, мы успешно создали Associations. Теперь к Private route table привязаны оба наши Private subnets. Далее нам необходимо сделать все тоже самое для Public route table. Перед тем как мы это сделаем, давайте выберем этот Route table и посмотрим какие у нас Routes есть. Мы также здесь видим два Routes, второй Route – это Default route, который позволяет всем Subnets внутри VPC обмениваться данными между собой. Первый Route – это тот Route, который был создан вместе с созданием VPC и другими компонентами и который как Target указывает Internet gateway, т.е. через Internet gateway мы идём в Destination, как Destination указан интернет. Таким образом, мы через Internet gateway выходим в интернет. Давайте перейдём на следующую вкладку Subnet associations. Здесь мы увидим, что к этому Route table привязан первый Public subnet. Нам необходимо нажать на кнопку Edit subnet associations и на открывшейся новой странице необходимо дополнительно к первому Public subnet также выбрать второй Public subnet. После чего нажмем на кнопку Save associations. Далее нам необходимо создать кастомную Security groups, для этого в левом навигационном меню нажмем на вкладку Security groups. На открывшейся странице нажимаем на кнопку Create security group. Мы перейдём в настройки создания новой Security group. Давайте, как название новой Security group введем Web Security Group. Далее, как Description напишем Enable HTTP access и как VPC в выпадающем списке выберем наш новый созданный VPC – Lab-vpc. Для этой Security group в рамках лабораторной работы мы создадим один Inbound rule. Для этого необходимо в этой секции нажать на кнопку Add rule, для того чтобы добавилась новая строчка, и в этой строчке как Type выбрать HTTP, как Source выберем Anywhere from IPv4, и вы увидите, что появится квадратик со всеми нулями обозначающий весь интернет. Далее, в самой последней колонке Description введем Permit web requests. Это все, что необходимо сделать в этой Security group. Давайте прокрутим вниз и нажмём на кнопку Create security group. После нажатия на эту кнопку, мы переходим на основную страницу новой созданной Security group, а также вверху экрана увидим сообщение о том, что наша Security group была успешно создана на зеленом уведомлении.

Следующим шагом нам необходимо поднять веб-сервер, для этого перейдём на сервисы Amazon EC2. В верхней строке поиска сервисов начнём вводить EC2 и самая первая ссылка будет нужная для нас ссылка. Давайте на неё перейдём. Как только мы оказались на главной странице сервиса Amazon EC2, нам необходимо в левом навигационном меню вверху убедиться, что переключатель New EC2 Experience был включён, для того чтобы отобразился новый интерфейс AWS Management console для этого сервиса. Далее там же в левом навигационном меню выберем вкладку EC2 Dashboard. На открывшейся странице в нижней части необходимо нажать на кнопку Launch instance. Откроется страница со всеми необходимыми входными данными для того чтобы создать новый Instance. Давайте, в поле Name введем Web Server 1, далее AMI, т.е. Amazon Machine Image выберем то, что нам предлагается – это Amazon Linux, а конкретнее – это Amazon Linux 2 AMI (HVM). Я вам напоминаю, что AMI – это образ для EC2 Instance, в котором указывается какая операционная система будет там установлена. Если мы прокрутим чуть ниже, мы можем выбрать Instance type, т.е. это мощный сервер, либо какой-то слабый, в нашем случае, давайте оставим по умолчанию значение t2.micro. Чуть ниже выбирается Key pair, для того чтобы подключаться по SSH. В рамках нашей лабораторной работы был сгенерирован Key pair Vockey, давайте его и выберем.

Двигаемся дальше. В настройках Network Settings мы видим, что нам необходимо изменить эти настройки, поэтому нажмем на кнопку Edit. Теперь мы можем изменять значения, как VPC выберем наш Lab-vpc. Далее, как Subnet выберем второй наш созданный Public subnet, который называется Lab-subnet-public-2. Чуть ниже там, где Auto-assign public IP выберем опцию Enable, для того чтобы для созданного EC2 Instance был автоматически сгенерирован временно публичный IP адрес. Этот IP адрес мы будем использовать для того чтобы подключиться к этому веб-серверу. Обо всем по порядку. Дальше нам необходимо выбрать Security group, для этого в секции Firewall (security groups) нам необходимо выбрать опцию Select existing security group и в появившимся поле выпадающем меню нам необходимо выбрать новую созданную нами Security group. Эта Security group называется Web security group. Чуть ниже есть настройки хранилища, т.е. это тот жёсткий диск, на котором будет установлена операционная система, другими словами Root volume. Как Root volume предлагается использовать gp2, это General Purpose (SSD) жёсткий диск и выделяется 8 гигабайтов. Давайте оставим эти значения по умолчанию, так как в рамках лабораторной работы нам этого достаточно.

Самая последняя секция – это Advanced details, т.е. дополнительные настройки. Давайте ее раскроем и спозиционируемся на поле User data. User data – это специальное поле, куда вы можете ввести набор команд, которые будут выполнены в момент первого запуска вашего EC2 Instance. Если вы перезагружаете ваш сервер, то User data повторно не запускается. Повторюсь, User data запускает эти команды только при первом запуске EC2 Instance. Давайте скопируем те команды, которые даны в лабораторной работе на этой странице и вставим сюда. Этот код копирует Zip архив, в котором есть код для PHP веб-сервера. Мы при помощи команд устанавливаем этот веб-сервер и его запускаем. Это последние настройки, которые необходимо было сделать. Мы можем сейчас нажать в правой части страницы на кнопку Launch instance для того чтобы создать наш EC2 Instance. На следующей странице мы увидим зелёное сообщение о том, что мы успешно инициировали создание этого Instance. Давайте в нижней правой части страницы нажмем на кнопку View all instances, и мы перейдём на страницу со всеми Instances в этом AWS аккаунте и конкретном регионе. Если этот список не отображается, то обязательно в верхней правой части посмотрите, что как регион был выбран North Virginia или системное название us-east-1. В отобразившемся списке Instances мы видим только что созданный нами Instance Web Server 1. Вы можете заметить, что на столбце Status check стоит пометка Initializing, т.е. не пройдены системные проверки для этого Instance и он ещё не готов к использованию. Мы можем использовать иконку обновления, для того чтобы периодически обновлять всю эту таблицу, и как только значение станет зелёным, будет написано, что две проверки из двух были успешно пройдены, тогда мы можем выбрать наш Instance. В появившемся меню снизу необходимо выбрать вкладку Details. В этой вкладке вы видите основную информацию по этому Instance, также есть другие вкладки по соответствующей теме Security, Networking, Storage, Status checks, Monitoring и Tags. Нас интересует во вкладке Details поле Public IPv4-address. Нам необходимо этот IP адрес скопировать и открыть в браузере на новой странице. Как только вы это сделаете, у вас откроется похожая страница с логотипом AWS, а также с мета данными нового созданного EC2 Instance. Если вы открыли подобную страницу, я вас поздравляю, вы все сделали верно, и на этом основную часть лабораторной работы завершили.

Теперь вы можете закрыть эту страницу, и осталось лишь правильно выйти со всех систем. Нам необходимо в AWS Management Console сверху справа нажать на нашего пользователя, для того чтобы в выпадающем меню нажать на кнопку Sign out. Как только вы на нее нажмете, вы перейдете на страницу логина AWS Management Console. Как только вы видите похожую страницу, это будет говорит о том, что вы успешно вышли из системы, вы можете закрыть эту страницу. Также нам необходимо правильно завершить лабораторную работу, чтобы не было проблем с открытием следующих лабораторных работ. Для этого в меню лабораторной работы необходимо нажать на кнопку End Lab. Выйдет сообщение, что действительно ли мы хотим завершить лабораторную работу. Нажимаем на кнопку Yes, после чего отобразится всплывающее окно и как только вы увидите сообщение You may close this message box now, это говорит о том, что ваша команда по завершению лабораторной работы была передана в систему, и сейчас инициирован процесс удаления всех ресурсов и временно созданного для вас AWS аккаунта. Мы можем не дожидаться завершения этого процесса и закрывать это окно, а также можем выходить из AWS Academy.

На этом мы успешно завершили лабораторную работу, разобрали её. Я вас с этим поздравляю. Ну, а теперь мы переходим к следующим нашим активностям, где мы с вами и увидимся. До встречи!