Добрый день, уважаемые студенты! Я рад вас всех видеть на очередной сессии разбора лабораторной работы. Тема лабораторной работы – Amazon EC2. Для начала нам необходимо авторизоваться в AWS academy. Далее в нужном курсе Cloud Foundations перейти на вкладку Modules. Здесь необходимо в Module 6 – Compute найти третью лабораторную работу, которая называется Lab 3 – Introduction to Amazon EC2. Давайте нажмём на эту ссылку, чтобы перейти на лабораторную работу.

Мы находимся на основной странице лабораторной работы. Опционально, вы можете нажать на кнопку Start lab для того, чтобы инициировать создание временного AWS аккаунта для вашей сессии. Рекомендую также убрать флажок с окна Terminal и оставить её только для README для удобства работы.

Мы с вами начинаем разбор лабораторной работы. Тема лабораторной работы – Введение в сервис Amazon EC2. Я вам напоминаю, что Amazon EC2 – это тот сервис, который предоставляет нам виртуальные серверы. Более подробно мы с вами проговорили на лекционном занятии. Здесь мы получим практический опыт по работе с сервисом Amazon EC2. Всего на выполнение лабораторной работы рекомендуется потратить 35 минут. На самом деле выделяется намного больше времени для выполнения, более того если времени не хватает, вы помните, что вы нажав на кнопку Start lab, можете обнулить счётчик и при этом, сохраняя текущий прогресс, получить дополнительное время. Так как временный AWS аккаунт создаётся в рамках нашей сессии лабораторной работы, то у этого аккаунта есть определённое ограничение. Доступ выдан для всех тех сервисов и features этих сервисов, которые мы рассматриваем в рамках лабораторной работы. Для всего остального, других сервисов и другого функционала сервисов, вы будете видеть сообщение о том, что у вас нет прав и доступа. Это является спецификой этих временных AWS аккаунтов. Когда вы будете создавать и работать в своём собственном AWS аккаунте, вы как Root пользователь получите неограниченные права и у вас будет доступ к любому из существующих сервисов.

Мы двигаемся дальше. Нам необходимо нажать на кнопку Start lab, выйдет всплывающее окно. Нам необходимо дождаться, что там появится сообщение «Lab status: ready». Как только мы увидим это сообщение, мы можем закрыть всплывающее окно и далее нажать на кнопку AWS. После нажатия на эту кнопку нас перенаправит на страницу AWS Management Console.

Первое задание в рамках лабораторной работы – это запуск нового Amazon EC2 инстанса. Для того чтобы это сделать, нам необходимо перейти на сервис Amazon EC2. Как только мы переходим на сервис Amazon EC2, необходимо убедиться, что мы находимся в регионе North Virgina. Напоминаю, что это один из самых основных регионов и при прочих равных условиях, когда вы в будущем будете использовать AWS, рекомендуется использовать именно этот регион. Почему? Потому что все новые обновления выходят в первую очередь в этом регионе. Как только мы оказались на главной странице cервиса Amazon EC2, нам необходимо нажать на кнопку Launch instances. Откроется новая страница c необходимыми входными данными для создания нашего Amazon EC2 инстанса. Первым предлагается ввести название нашего инстанса, давайте введём туда Web Server. Я напоминаю, что это поле создаёт тег, где ключом является Name с заглавной буквы, а значением является то значение, которое вы введёте в это поле. Вторым шагом нам необходимо выбрать AMI. Это – Amazon Machine Image. Это snapshot инстанса, который определяет какая операционная система будет использоваться в нашем Amazon EC2 инстансе. Давайте оставим выбранное значение Amazon Linux. Далее ниже есть детализация, также необходимо оставить дефолтовые значения Amazon Linux 2 AMI (HVM). Если мы прокрутим чуть ниже, у нас будет отдельное поле для выбора типа инстанса, давайте также здесь оставим то значение, которое предлагается. Это – t2.mісro – это один из самых маленьких типов инстанса. Так как мы в рамках нашей лабораторной работы создадим простейший веб-сервер, то мощности этого типа инстанса для нас будет достаточно.

Следующим шагом необходимо выбрать SSH ключи. В рамках лабораторной работы для нас специально предварительно был создан SSH ключ, который называется vockey. Давайте из возможного списка ключей выберем это значение.

Двигаемся дальше, ниже есть секция по настройке деталей в сети, т.е. Network settings. Нам необходимо нажать на кнопку Edit, для того чтобы начать её редактировать. Как в VPC необходимо выбрать Lab VPC, это уже предварительно созданный для нас Lab VPC, у которой есть два public subnets в двух различных Availability Zones. Чуть ниже если прокрутить, есть cекция называется Firewall (Security groups), т.е. настройка Security groups. Нам необходимо выбрать опцию create security group, мы создадим новый security group, как название security group укажем Web Server security group, а как description укажем Security group for my web server. Здесь следует напомнить, что Security group выступает как некий виртуальный Firewall, который контролирует трафик нашим инстансом. Если мы прокрутим ниже, то в секции и Inbound Security group rules мы увидим все rules, т.е. правила, которые разрешают входящий доступ к инстансам, к которым привязана эта конкретная Security group. Нам необходимо удалить существующее правило. Таким образом, у нас в секции Inbound Security group не будет ни одного правила, это говорит о том, что извне к инстансам, у которых есть привязка к этой конкретной Security group, подключиться к ним извне будет невозможно. Мы чуть позже после создания нашего инстанса введём некоторые изменения в эту Security group.

Далее в следующей секции нам предлагается ввести настройки хранилища. Давайте оставим все значения по умолчанию, а именно здесь говорится о том, что мы по умолчанию будем использовать сервис Amazon EBS, для того чтобы создать жёсткий диск. На этом жёстком диске будет установлена операционная система и по умолчанию для этого жёсткого диска выделяется 8 гигабайтов дисковой памяти. Оставляем это значение как есть и двигаемся дальше.

Далее нам необходимо прокрутить в самый низ экрана и развернуть секцию, которая называется Аdvanced details. Мы будем вносить некоторые изменения в настройках внутри этой секции. Давайте прокрутим до поля, которое называется Termination protection и выберем значение Enable. Что такое Termination protection? Это та feature, которая позволяет нам защитить наши инстансы от удаления. Даже пользователи, у которых есть доступ к удалению этого конкретного инстанса, не смогут сразу её удалить. Для того чтобы её успешно удалить, сперва нужно снять защиту, после чего появляется возможность её удалить.

Далее нам необходимо прокрутить чуть ниже и добраться до поля, которое называется User datа. Что такое User datа? Это некий набор команд, который позволяет нам финализировать настройку нашего инстанса. В рамках этой лабораторной работы вам необходимо скопировать готовые команды и вставить в это поле. Что делают эти команды? Первая команда устанавливает, Apache web server. Вторая команда настраивает автозагрузку, чтобы при каждом запуске нашего инстанса запускался наш веб-сервер. Далее, после того как эти настройки будут произведены, на третьем шаге, третья команда стартует наш веб-сервер и на четвёртом шаге мы создаём новую простейшую html страницу, для того чтобы мы смогли к ней обратиться.

После того как мы вели все необходимые входные данные для создания нашего инстанса, необходимо в нижней части страницы с правой стороны нажать на кнопку Launch instance. Вы увидите сообщение, что команда по инициализации создания нашего инстанса успешно выполнена и инстанс начинает создаваться. Вас направят на следующую страницу: на этой странице вам также необходимо нажать на кнопку, на которой написано View all instances. Как только вы ее нажмете, вы перейдете на страницу со списком всех инстансов в вашем AWS аккаунте. Если вы не увидели список инстансов, также вы не видите свой новый созданный сервер, проверьте, что вы находитесь в правильном регионе. Как только вы отмечаете флажок возле названия вашего инстанса, то в нижней части экрана появляется дополнительная информация по этому инстансу. Она оформлена в виде нескольких tab-ов: сгруппированная информация по инстансу, отдельно по безопасности, отдельно по сетям и так далее. Здесь вы также в первой вкладке можете найти публичный IP-адрес нашего Amazon EC2 инстанса. В списке инстансов в самом начале в колонке State, вы будете видеть значение Pending. Это говорит о том, что команда по созданию нашего инстанса запущена и она ожидает своего выполнения. Далее pending перейдёт в состояние Initializing, т.е. она создаётся, поднимается для нас, как только все настройки будут выполнены и инстанс будет готов к бою, он перейдёт в состояние Running. При этом обратите внимание, нам также нужно дождаться, что в столбце Status checks у нас будет иконка с галочкой и написано два из двух все проверки пройдены. Для того чтобы обновлять информацию по нашим инстансам, вы можете нажимать на иконку обновления, либо обновлять всю страницу. Как только эти два значения появятся, это говорит о том, что ваш инстанс успешно создан. Веб-сервер на нем поднят и я вас с этим поздравляю. Мы с вами вместе создали новый Amazon EC2 Instance.

Теперь мы с вами переходим ко второй части – это мониторинг нашего инстанса. Мы посмотрим и научимся, как мы можем посмотреть в каком состоянии находится наш инстанс. Отлично. Нам необходимо сейчас выбрать из списка инстансов наш новый созданный инстанс, т.е. отметить флажком. После чего в нижней части странице отобразится несколько вкладок, где есть информация по конкретно этому инстансу. Нам необходимо выбрать вкладку Status checks. Это как раз таки те две проверки, которые ждали нас в верхней части нашей лабораторной работы. Они называются System reachability и Instance reachability. Простыми словами, происходит простейшая проверка, что мы можем обратиться и подключиться к этому инстансу. Если эти проверки пройдены, то значит, со стороны AWS никаких проблем нет и мы двигаемся дальше. Представим, что у нас есть какая-то проблема и мы, таким образом, исключая различные возможные места поломки, рассматриваем все возможные места, где что-то может сломаться. Таким образом находим проблемное место и устраняем.

Мы двигаемся дальше к следующей вкладке, которая называется Monitoring. В этой вкладке представлена информация по всем имеющимся метрикам из сервиса Amazon CloudWatch, непосредственно привязана к выбранному инстансу. На текущий момент будет отображаться не так много метрик, так как инстанс был создан относительно недавно. Вы видите несколько различных графиков. Каждый из этих графиков вы можете отдельно увеличить для того, чтобы ввести дополнительную информацию, например, увеличить период отображения метрик, вы можете изменить детализацию и так далее. Здесь следует отметить, также, что в Amazon CloudWatch передаются метрики по умолчанию Basic monitoring, т.е. каждые пять минут эта опция бесплатная. Есть платная опция, которая позволяет передавать наши метрики чаще, если это требует ваша бизнес задача. В этом случае называется Detailed monitoring и метрики передаются каждую минуту. В этой вкладке Monitoring, давайте нажмём на кнопку Actions, это выпадающее меню. В этом меню выберем секцию, кнопку Monitor and troubleshoot. Здесь также вы увидите выпадающее меню, и выберем опцию Get system log. Вы перейдёте на страницу, где будут отображаться системные логи. Это как раз таки вывод всех тех команд, которые были запущены на нашем инстансе. Посмотрев на эти логи, вы можете понять, все ли команды были успешно запущены. Таким образом вам нет необходимости напрямую подключаться по SSH к этому инстаyсу, чтобы это проверить. Обратите внимание, что в этих log-ах вы видите, что мы успешно установили пакет HTTP, т.е. установили Apache web server. Я вам напоминаю, что мы устанавливали Apache web server в рамках команд записанных в User datа.

Хорошо, мы посмотрели ещё один вариант как можно искать проблемы, если они возникают с нашими Amazon EC2 инстансами. Давайте нажмём на кнопку Cancel и посмотрим ещё одно место. Нам необходимо убедиться, что наш web server выбран. Далее в отобразившхся в нижней части экрана вкладках, выбираем вкладку Monitoring. Здесь выбираем кнопку Actions, появится выпадающее меню – это то же самое выпадающее меню, которое мы выбирали чуть выше. Нам необходимо также выбрать опцию Monitor and troubleshoot, но на этот раз выбрать опцию внутри Get instance screenshot. Что это такое? Здесь мы получим screenshot консоли с нашего Amazon EC2 инстанса. В случае, если мы не можем подключиться к этому инстансу напрямую в виду неких проблем, мы можем попытаться получить screenshot. По screenshot-у можем либо получить ответ, либо как минимум дополнительную информацию о том, что же происходит на этом инстансе. Хорошо, это было ещё одно место, которое помогает нам troubleshoot-ить, т.е. искать и решать проблемы связанные с Amazon EC2 инстансами. Нам необходимо нажать на кнопку Cancel. Таким образом мы успешно завершили второе наше задание и переходим к следующему.

Мы с вами переходим к третьему заданию и здесь мы будем редактировать Security group для того, чтобы предоставить доступ из интернета нашему веб-серверу. Что нам необходимо сейчас сделать? Давайте выберем наш веб-сервер из списка инстансjв, далее во вкладке Details найдём значение публичного IPv4 address, мы скопируем этот IP-адрес и откроем новую страницу в вашем браузере. Попробуйте открыть эту страницу. Смогли ли вы прогрузить любую страницу, что-то отображается или нет? Скорее всего, вы ничего не увидите и вы увидите сообщение, что либо не существует эта страница, либо какую-то другую ошибку. Почему она не отображается? Давайте с вами сделаем небольшую активность, остановите это видео и попробуйте угадать. Хорошо, я думаю каждый из вас смог правильно ответить. Ответ в том, что, если вы помните, в начале, когда мы создавали наш Amazon EC2 инстанс, мы создавали новую Security group-у. В рамках этой Security group мы удалили все rules, все Inbound rules у этой Security group. Это говорит о том, что мы никаким образом не можем извне подключиться к этому инстансу. Даже по SSH мы не можем подключиться, потому что для подключения по SSH необходимо предоставить доступ к TCP порт 22. Хорошо, что нам необходимо сделать? Нам необходимо сейчас попытаться сделать настройки таким образом, чтобы мы увидели созданную нами веб-страницу. Для этого в EC2 console нам необходимо в левом навигационном меню выбрать вкладку Security groups. В списке Security groups мы увидим созданную нами Security group. Она называется Web Server security group. Давайте на неё нажмём. Далее вы увидите Outbound и Inbound rules, привязанные к этой Security group. Нас на текущий момент интересует Inbound rules. Если мы откроем эту вкладку, то мы увидим, что никаких rule-ов нет, поэтому мы добавим новый rule. Для этого необходимо нажать на кнопку Edit Inbound rules. Вы перейдёте на страницу редактирования всех существующих rule-ов, здесь ничего не будет, будет только единственная кнопка Add rule, давайте на неё нажмём. Как только вы на неё нажмёте, появится новая строчка. В этой строчке вам необходимо выбрать как тип – HTTP, как Source выбрать – Anywhere-IPv4, это говорит о том, что мы предоставляем доступ по HTTP, это протокол TCP порт 80, который заполнится автоматически и говорит о том, что из интернета можно будеть подключаться. Нам необходимо нажать в нижней части экрана кнопку Save rules. Как только вы нажмёте на эту кнопку, вас перебросит на следующую страницу, но при этом все те изменения, которые вы внесли, станут работать сразу в этот момент. Теперь, если вы не закрыли ту страницу нашего веб-сервера, то перейдите на неё и попробуйте обновить страницу. Если вы закрыли эту страницу, ничего страшного, вы знаете, как найти публичный IPv4 адрес нашего инстанса. Давайте мы её найдём. Как только вы откроете эту страницу, то должна успешно отобразиться страница, в которой будет написано Hello From your Web Server! Отлично, я вас поздравляю! Вы сейчас настроили ваш Amazon EC2 инстанс, а также правильно настроили Security group для того, чтобы трафик из интернета доходил до вашего инстанса, а также этот инстанс благодаря установленному веб-серверу мог отвечать и показывать нам нашу простейшую веб-страницу. Мы с вами переходим к следующему заданию.

Мы добрались до четвёртого задания и здесь нам необходимо изменить тип инстанса, изменить размер нашего жёсткого диска. Представим, что наш инстанс либо слишком мощный на текущий момент, при текущей нашей нагрузки, либо наоборот слишком слабый и необходимо увеличить его Instance type. Это простейшая операция, которую мы можем выполнять с нашими инстансами. Это очень легко делается внутри AWS. Для того чтобы произвести эти операции, первым делом нам необходимо остановить наш инстанс. Для этого нам необходимо в списке EC2 инстансов выбрать наш веб-сервер. Далее, нажать на выпадающее меню Instance State и выбрать опцию Stop Instance. В окне появится дополнительное сообщение о том, действительно ли мы хотим остановить наш инстанс, нам необходимо подтвердить и нажать на кнопку stop. Как только мы на неё нажмём, начнётся процесс остановки нашего инстанса. Поэтому вы как cтатус у нашего инстанса будете видеть значение stopping, т.е. он в процессе остановки. Давайте подождём некоторое время. После того как мы обновим страницу, мы увидим, что состояние поменялось на stopped и отображается красной иконкой. После того как сервер остановлен, мы с лёгкостью можем менять тип инстанса, а также размер жёстких дисков. Давайте в первую очередь поменяем тип инстанса. Для этого нам необходимо также выбрать наш инстанс из списка. Далее нажать на выпадающее меню Actions, там выбрать опцию Instance settings, внутри выбрать Change instance type, т.е. поменять тип нашего инстанса. В новой открывшейся странице выберем следующий размер виртуальной машины, а именно t2.small. Этот размер в два раза больше, чем текущее наше значение t2.micro. Хорошо, нам необходимо в нижней части страницы нажать на кнопку Apply. Как только мы на неё нажали, все изменения уже вступят в силу и как только мы включим наш инстанс, то он уже будет запущен с новым типом инстанса, т.е. более мощная виртуальная машина. Но перед тем как мы включим, давайте также изменим размер нашего жёсткого диска. Для этого необходимо в списке инстансов выбрать наш инстанс. В отобразившихся в нижней части страницы вкладках необходимо выбрать вкладку Storage. Далее нам необходимо выбрать опцию Actions и нажать на кнопку Modify volume. Вы перейдёте на новую страницу, где будет отображена информация о текущем размере нашего жёсткого диска, а именно 8 гигабайтов, давайте, поменяем это значение на 10. Как только вы это сделали, давайте нажмём на кнопку Modify и далее выйдет всплывающее сообщение о том, что действительно ли мы хотим изменить размер нашего жёсткого диска. Да, мы подтверждаем, поэтому нажимаем на кнопку Modify. Как только мы произвели эти изменения, нам необходимо включить наш инстанс, для этого в списке наших инстансов нам необходимо выбрать наш инстанс. Далее в выпадающем меню Instance state стоит выбрать опцию Start instance. Как только инстанс полностью включится, вы увидите в списке инстансов, в соответствующем столбце, что поменялся тип с t2.micro на t2.small, а также увидите в дополнительной информации об этом инстансе, что значение жёсткого диска вместо 8 стало 10. Вы увидели как легко происходит изменение типа инстанса на более мощный, либо на более слабый, а также как мы можем увеличивать размеры наших жёстких дисков.

Мы двигаемся дальше – пятое задание. Здесь мы посмотрим как мы можем проверить, какие лимиты на текущий момент есть для сервиса Amazon EC2. Для этого в левом навигационном меню нам необходимо выбрать вкладку Limits. Как только вы перейдёте на эту страницу, вы можете видеть некоторые сообщения с ошибкой. Вы можете игнорировать эти сообщения, так как на реальном AWS аккаунте под Root пользователем этих ошибок у вас не будет. В выпадающем меню в All limits, давайте выберем значение Running instances. Таким образом, как пример, вы видите информацию по количеству и типу инстансов, которые могут быть запущены конкретно в этом AWS аккаунте в этом выбранном регионе. Если посмотрите значение Running On-demand Standard, мы увидим большую часть семейства типов инстансов в том числе и семейство T, общего назначения, что такое-то количество инстансов могут быть запущены в этом регионе. Следует помнить, что Limits бывают двух видов: это Soft limits и Hard limits. Hard limits – это те элементы, которые изменить не получится. Если вы доходите до Hard limits, рекомендуется создать другой AWS аккаунт и продолжать работать там. Если же вы добрались до Soft limits, то в этом случае вы можете всегда написать в техподдержку о том, чтобы этот Soft limit был увеличен. Здесь никаких проблем по большей части не возникает, обычно техподдержка проверяет, действительно ли вы добрались до этого soft limit, если это так, то soft limit увеличивается на то значение, которое вы указываете для себя.

Мы добрались до самого последнего задания в рамках нашей лабораторной работы и здесь мы протестируем работу Termination Protection. Для этого нам необходимо в левом навигационном меню выбрать вкладку Instances, так мы увидим список всех инстансов, которые есть в конкретном выбранном регионе. Нам необходимо выбрать наш инстанс веб-сервер. Далее нажать на кнопку Instance state и в выпадающем меню выбрать опцию Terminate instance. Выйдет всплывающее окно о том, что действительно ли вы хотите отключить этот инстанс. Да, мы хотим его отключить, поэтому мы нажимаем на кнопку Terminate. После того как вы нажмёте на эту кнопку, вы увидите сообщение, что вам не удалось запустить процесс отключения инстанса с таким-то ID, это ID нашего инстанса веб-сервер и выйдет информация, которая объясняет, почему так произошло. Мы знаем, что у него включена защита от удаления. Давайте теперь попробуем отключить эту защиту, для этого нам необходимо в выбранном состоянии нашего инстанса нажать на выпадающее меню Actions. Далее выбрать опцию Instance settings и внутри выбрать опцию Change termination protection. Откроется дополнительная страница, либо всплывающее окно и вы увидите, что в ячейке Enable, отмечен флажочек и для нас включён termination protection. Нам необходимо этот флажок убрать и нажать на кнопку Save. Мы с вами отключили termination protection для нашего инстанса. Давайте теперь попробуем повторить и отключить этот инстанс. Мы выбираем наш веб-сервер. Далее нажимаем на кнопку Instance state и выбираем опцию Terminate instance. После этого подтверждаем удаление, нажав на кнопку Terminate. Вы увидите, что ваш инстанс успешно был отключён, процесс отключения был запущен и через некоторое время, когда вы обновите страницу ещё раз, вы увидите наш веб-сервер уже в состоянии Terminated, либо наш инстанс из списка вовсе исчезнет, если вы это сделаете через некоторое время.

Отлично, мы с вами добрались до конца нашей лабораторной работы и я вас с этим поздравляю. Если вы параллельно проделывали все задания, то вам необходимо правильно завершить эту лабораторную работу. Для этого необходимо нажать на кнопку End Lab в всплывающем окне. Как только вы увидите сообщение «DELETE has been initiated… You may close this message box now», это говорит о том, что процесс удаления созданного временного AWS аккаунта был запущен, и вы можете закрывать это окно, а также выходить из AWS academy.

На этом мы заканчиваем сессию разбора лабораторной работы. Я надеюсь, что у вас не возникнет проблем при ее выполнении, и мы с вами увидимся на следующих наших активностях.