Добрый день, уважаемые студенты! Рад вас видеть на очередной сессии разбора лабораторной работы. Тема лабораторной работы – введение в сервис Amazon EC2. Итак, давайте начнем.

Сессия начинается с главной страницы лабораторной работы. Необходимо убедиться, что вы находитесь на правильной странице внутри AWS Academy, а также запустить предварительно лабораторную работу путем нажатия на кнопку «Start Lab». Как только все будет готово, нажимаем на кнопку «AWS» для перехода на главную страницу AWS Management Console.

После перехода на AWS Management Console, вверху справа можно видеть, что специально для нас был создан временный аккаунт, и мы сидим здесь под специальным пользователем Test Student. В первом задании необходимо создать новый EC2 инстанс. Для этого перейдите на сервис EC2. Как мы помним, достаточно в строке поиска сервисов AWS начать вводить часть сервиса, в нашем случае это EC2, и в выдаче первой выйдет нужная нам ссылка. Нажмем на нее, чтобы перейти на основную страницу сервиса Amazon EC2. Вверху справа убедитесь, что вы находитесь в регионе North Virginia. В левом навигационном меню сверху также надо убедиться, что включена опция New EC2 Experience, затем на основной странице чуть ниже нажимаем на кнопку «Launch Instance» и мы попадаем в помощник создания нового EC2 инстанса. В названии нашего EC2 инстанса введем Web Server. Прокрутим чуть ниже и остановимся на секции Application and OS Images (Amazon Machine Images). Здесь мы выбираем образ нашего инстанс, оставляем все значения по умолчанию, т.е. Amazon Linux, а внутри Amazon Linux именно AMI, который называется Amazon Linux Tool AMI (HVM).

Двигаемся дальше. Чуть ниже есть секция, где мы указываем тип нашего инстанса. По умолчанию будет значение t2.micro. В этом типе инстанса для нас будет доступно одно ядро процессора и один гигабайт оперативной памяти. Смотрим чуть ниже, и там есть секция для выбора SSH ключей. Для нас в рамках нашей лабораторной работы был создан SSH ключ под именем «vockey». Приватный ключ вы можете скачать на основной странице лабораторной работы, а здесь в качестве SSH ключ (public key) мы используем vockey. Этот публичный ключ Amazon передаст EC2 инстансу и в момент, когда мы с приватным SSH ключом будем подключаться к этому инстансу, он будет сверяться с публичным ключом. Как только произойдет совпадение, мы сможем авторизоваться в нашем инстансе. Немного ниже вы видите большую секцию по настройке сетей. Здесь необходимо в правой части секции нажать на кнопку Edit для того, чтобы поля стали доступными. После этого нам сразу необходимо поменять VPC. Как VPC мы выбираем не дефолтовый, а специально созданный для нас VPC, Lab VPC. Ниже, в подсекции Firewall (security groups), выбираем опцию Create Security Group, т.е. мы создаем новую Security Group. Как название группы вписываем Web Server Security Group, далее, как description прописываем Security Group for my web server. Прокрутив еще ниже, для этой Security мы можем настроить inbound rules. Здесь уже есть дефолтовый рул, это доступ по 22 порту через интернет, т.е. есть через интернет можно таким образом подключаться к нашему инстансу. Нажмем на кнопку Remove, чтобы удалить этот рул. Таким образом, у нас не будет ни одного inbound rules. Security groups мы будем редактировать чуть позже.

Следующая секция это настройка хранилища, т.е. жестких дисков. Нам рекомендуется создать один жесткий диск как root volume, на котором будет установлена операционная система. Всего предлагается сделать размер 8 ГБ и тип EBS volume выбрать gp2. Не обращайте внимания, почему именно этот тип, более подробно типы EBS volume мы разберем на следующих наших лекциях. Далее прокручиваем ниже до самого конца и открываем секцию Advanced details. В этой секции нам необходимо будет внести некоторые правки. Найдем поле под названием termination protection и установим значение enable, т.е. мы termination protection включаем для этого инстанса. Еще ниже, в самом внизу, мы увидим поле user data. Что это такое, мы уже проговаривали с вами несколько раз. А сейчас необходимо скопировать команды, которые даны нам на странице лабораторной работы и вставить в это поле. После чего нажать на кнопку launch instance для запуска процесса создания нашего инстанса. Как только вы это сделаете, появится уведомление зеленого цвета, где сообщается, что процесс успешно инициирован и вашему инстансу присвоен следующий ID. Внизу вы увидите кнопку «view all instances», нажмем на нее для перехода на страницу со всеми инстансами. После этого нас перенаправит на страницу со списком всех инстансов в этом регионе, в этом AWS аккаунте. Вы можете видеть, что появился новый инстанс под названием Web Server, а также, что через какое-то время «instance state» становится «running», но при этом какое-то время должно пройти, чтобы в колонке «status check» значение «initializing» поменялось и стало «2/2 checks passed». Для обновления страницы можно нажимать не только «F5», вы можете сделать частичное обновление, а именно список инстансов путем нажатия на иконку «обновить» в верхней части страницы. После завершения всех проверок вы видите соответствующий текст, теперь выбираем этот инстанс и в нижней части отобразится вся необходимая информация касательно этого инстанса в нескольких различных вкладках. Первая вкладка «details», здесь находится самая основная информация, в том числе публичный IP-адрес нашего инстанса. У вас может возникнуть вопрос, что это за две проверки, которые отображаются в списке в колонке «status check». Это самые основные проверки «system status check» и «instance status check». Так проверяется, что наш инстанс был успешно поднят и он доступен для подключения по сети. Как только проверки пройдены, это говорит о том, что сервер готов. Теперь давайте посмотрим, какими инструментами и features мы можем воспользоваться для проверки состояния нашего инстанса. Перейдем на вкладку «monitoring». Здесь находятся различные графики. Сейчас графики не нарисованы, так как сервер был относительно недавно запущен, но давайте выберем самый первый график, это нагрузка процессора, нажмем на три кнопки и нажмем на кнопку «enlarge» для увеличения этого графика. Отобразится всплывающее окно, где мы можем лучше посмотреть все метрики. Каждая метрика отображается как точка и если у нас всего несколько метрик, они соединяются между собой линиями и мы увидим график. На текущий момент у нас одна единственная метрика, которая говорит о том, что нагрузка на процессор было 14,5%. Также на этой странице мы можем настраивать различные периоды – от одного часа до целого года, группировать наши метрики по пяти минутам и выше. Более того, во время группировки мы можем применить некую операцию – это может быть среднее значение, максимальное, минимальное, и так далее.

Давайте закроем эту страницу и посмотрим, какие еще у нас есть варианты проверки состояния нашего инстанса внутри AWS Management Console. Что необходимо для этого сделать? Из списка инстансов выбираем наш веб-сервер. Далее, вверху справа нажимаем на выпадающий список «actions», выбираем опцию «Monitor and Troubleshoot» и в следующем выпадающем списке выбрать опцию «Get System Lock». Вас перенаправит на страницу с логами всех команд, которые были запущены на этом инстансе. Это информация, которая доступна для вас для любого инстанса. В случае, если у вас некие проблемы с этим инстансом, либо по тем или иным причинам вы не можете подключиться к нему, можно всегда открыть эту страницу и посмотреть, как отработали команды, запущенные на этом инстансе. Также путем нажатия на иконку обновления в режиме реального времени можно видеть все новые логи, которые появляются здесь, можно скопировать эти логи, либо загрузить в виде файла.

Теперь нажмем на кнопку Cancel и посмотрим еще одну доступную для нас опцию. Выбираем наш веб-сервер, в выпадающем меню «Actions», затем опцию «Monitor and Troubleshoot» и вторую опцию, которая называется «Get Instance Screenshot». Как только вы ее нажмете, в консоли EC2 инстанса в командной строке сделается ее скриншот, отправится и отобразится здесь. Вы увидите этот скриншот и, если у вас проблемы с подключением к вашему инстансу, так вы можете увидеть текущее состояние консоли и предпринять какие-либо меры. Даже если эта информация не даст вам однозначного ответа, в целом это может быть ценным и данные, которые помогут вам найти проблемное место.

Теперь нажмем на Cancel, закроем это окно и посмотрим, что у нас есть еще, что мы можем сделать в рамках сервиса Amazon EC2. Мы с вами запустили веб-сервер на нашем EC2 инстансе, создали простейшую веб-страницу, которая должна быть для нас доступна. Для этого в левом навигационном меню откроем вкладку «Instances» и из списка выберем наш инстанс под названием Web Server. Внизу в отобразившихся вкладках выберем вкладку Details и вы увидите, как отображается public IPv4-адрес нашего веб-сервера. Давайте скопируем и откроем ее на отдельной странице. Вы видите, что мы не можем подключиться к этому инстансу, почему это так, мы разобрали в сессии разбора лабораторной работы. Проблема была в том, что мы убрали все inbound rules в Security Group, которая была привязана к нашему инстансу и таким образом, к этому инстансу никак нельзя подключиться извне. Теперь давайте модифицируем нашу Security Group, чтобы мы могли обращаться к нашему веб-серверу через интернет. Для этого в левом навигационном меню выбираем вкладку Security Groups, здесь отобразится список Security Group, созданные в этом AWS аккаунте. Выбираем Security Group, которая называется Web Server Security Group. Как только вы ее выберете, в нижней части экрана отобразится несколько вкладок. Нам необходимо перейти на вкладку «Inbound Rules». Разумеется, что на текущий момент у нас нет inbound rules. Это нормально, это ожидаемо, теперь их необходимо создать. Для этого нажимаем в правой части на кнопку «Edit inbound rules» и вас направит на страницу редактирования существующих inbound rules. Сейчас у нас нет rules, жмем на кнопку «Add Rule» и появится новая строчка. В этой строчке в столбце «Type» выбираем HTTP, при этом столбцы «Protocol» и «Port Range» заполнятся автоматически с соответствующими значениями Protocol TCP и Port 80. В столбце «Source» выбираем Anywhere IPv4 и справа в соседнем столбце вставится CIDR-блок со всеми нулями. Это и есть CIDR-блок всего нашего интернета. На этом настройка inbound rules заканчивается, в нижней части страницы нажимаем кнопку «Save Rules» и все изменения сразу же вступят в силу. После этого на следующей странице появится соответствующее уведомление зеленого цвета о том, что Security Group успешно обновлена. Открыв либо обновив эту страницу, если вы ее не закрывали, мы увидим сообщение Hello From Your Web Server. Отлично, я поздравляю вас! Мы настроили Security Group правильным образом, чтобы мы могли c интернета добираться до нашего веб-сервера и получать от него ответ.

Давайте теперь представим ситуацию, когда вы работаете облачным инженером и вас попросили увеличить либо уменьшить размер EC2 инстанса, а также необходимо увеличить размер жестких дисков, чтобы оставить больше места для данных. В AWS это делается очень легко, буквально пару кликов внутри AWS Management Console. Давайте попробуем это сделать. Необходимо в левом навигационном меню нажать на вкладку Instances. Там отобразится список всех существующих инстансов, выбираем наш инстанс под названием Web Server. Затем вверху справа нажимаем на выпадающий список Instance type и остановить этот инстанс. Почему мы его останавливаем? Тип инстанса и размер жестких дисков могут быть изменены только тогда, когда инстанс остановлен. В отобразившемся окошке необходимо подтвердить, что мы останавливаем наш инстанс и нажать «Stop». Запускается процесс остановки и «Instance state» отображается как stopping, т. е. в процессе. Через некоторое время, если обновить список инстансов, мы увидим, что состояние поменялось со stopping на stopped, т. е. окончательно остановлен. Теперь можно переходить к изменению типа инстанса. Для этого выбираем наш инстанс, далее в выпадающем меню «Actions» выбираем Instance settings. Здесь отобразится несколько опций, из них выбираем Change instance type. Нажав на нее, вы будете перенаправлены на другую страницу. Здесь вы видите текущее значение типа инстанса, и можете ввести новое значение. Давайте выберем t2.small. Это следующий размер инстанса, он в два раза больше, т.е. у нас в два раза больше количество ядер, и в два раза больше оперативной памяти. На этом мы закончили все необходимые настройки на этой странице, нажимаем внизу страницы на Apply.

Отлично. Теперь необходимо изменить размер жестких дисков. Для этого выбираем опять наш веб-сервер и переходим на вкладку Storage. Прокрутив чуть ниже, мы увидим единственный жесткий диск, это основной жесткий диск, на котором установлена операционная система. Если мы нажмем на ссылку, то есть ID жесткого диска, мы перейдем на соответствующую страницу со всеми жесткими дисками, при этом нужный жесткий диск уже будет отфильтрован. Выберем ее, вверху справа выберем Actions и нажмем на опцию Modify volume. Нас снова перенаправят на новую страницу, здесь нам необходимо увеличить размер с 8 до 10 ГБ. Отлично. Нажимаем на «Modify» и в всплывающем окне подтверждаем, что мы изменяем размер жесткого диска. Мы проделали все необходимые изменения, теперь можно включать наш веб-сервер. В левом навигационном меню выбираем вкладку «Instances», здесь отобразится список всех существующих инстансов. Нам необходимо выбрать наш EC2 инстанс с именем Web server и далее в выпадающем меню Instance state выбрать опцию «Start instance». Сейчас я рекомендую вам остановить видео и самостоятельно убедиться, что наши изменения типа инстанса, а также размера жесткого диска вступили в силу, сервер остался доступен и наша веб-страница также работает. Отлично, я думаю, у вас не возникло проблем с проверкой. Мы двигаемся дальше.

Следующее задание состоит из проверки, какие лимиты у нас есть в рамках сервиса Amazon EC2. Выбираем в левом навигационном меню вкладку «Limits». Как только вы перейдете на эту страницу, вы увидите много красных уведомлений с ошибкой. Не обращайте на них внимания, можете эти сообщения сейчас закрыть. Когда вы будете работать в своем личном AWS аккаунте либо корпоративном и будете сидеть под root-пользователем, то подобные сообщения отображаться не будут. Закроем все эти ошибки и попробуем отфильтровать наши лимиты и отобразим Running Instances. Вы видите, какое количество инстансов доступно для нас в рамках определенных семейств типов инстанса. Если мы посмотрим на значение Running On Demand All Standard, куда в том числе входит семейство T, мы увидим, что для нас доступно 32 ядра процессора для запуска в этом регионе.

Мы добрались до последнего задания в рамках нашей лабораторной работы, а именно проверить, как работает Termination Protection для EC2 инстанса. Для этого в левом навигационном меню переходим на вкладку Instances. В списке инстансов необходимо выбрать наш, который называется Web Server. Затем нажимаем на выпадающий список «Instance State» и пробуем нажать на опцию «Terminate Instance». В зависимости от версии вашей консоли у вас эта кнопка будет доступна, но по нажатию вы увидите ошибку, либо в моей версии, вы увидите, что кнопка недоступна и при наведении мышкой на опцию «Terminate Instance», выходит всплывающая подсказка о том, что Terminated Protection у нас включен. Отлично, давайте попробуем этот Termination Protection отключить. Для этого необходимо в выбранном состоянии EC2 инстанса нажать на Actions, далее опцию Instance Settings, затем еще одну опцию Change Termination Protection. Отобразится всплывающее окно, здесь видно, что Termination Protection в состоянии enable и поставлена галочка. Нам необходимо эту галочку убрать и сохранить изменения. Как только мы нажмем на «Save», мы увидим, что для инстанса с таким-то ID Termination Protection был отключен. Уведомление зеленого цвета. Отлично, теперь мы можем попробовать этот инстанс отключить. Выбираем этот инстанс, далее нажимаем на выпадающий список Instance State и видим, что Termination Instance опция уже доступна. Давайте на нее нажмем, утвердительно ответим на всплывающее окно и на кнопку «Terminate». После этого мы увидим соответствующее сообщение, что инстанс с таким-то ID был отключен, но при этом он еще не отключен, а запущен процесс его отключения. Поэтому в столбце Instance State мы видим значение Shutting Down, т. е. в процессе отключения. Подождем какое-то время и обновив список инстансов, вы увидите наш и инстанс Web Server в состоянии «Instance State Terminated», т.е. он отключен. Обновив еще через какое-то время, мы увидим, что этот инстанс полностью пропал из общего списка.

Поздравляю вас, мы закончили нашу лабораторную работу! Осталось правильно отключиться и корректно выйти из всех систем. Для этого вверху справа нажмите AWS Management Console и в выпадающем списке выберите «Sign Out» в самом внизу. Это делается для того, чтобы разлогиниться с AWS Management Console. Далее, необходимо правильно отключить систему внутри AWS Academy. На основной странице лабораторной работы нажимаем «End Lab». Выйдет сообщение, действительно ли вы хотите остановить лабораторную работу. Мы все закончили, мы говорим «Yes». Отображается всплывающее окно, и вы видите сообщение «You may close this message box now, lab resources are terminating…». Это говорит о том, что мы инициировали процесс удаления созданного для нас AWS аккаунта и мы можем закрыть это окно, и выйти с AWS Academy.

На этом мы заканчиваем разбор лабораторной работы. Я думаю, вы научились чему-то новому, и получили ответы на ваши вопросы и более подробно ознакомились с сервисом Amazon EC2. Спасибо! Увидимся на следующих наших активностях!