Добрый день, уважаемые студенты! Рад вас видеть на очередной сессии разбора лабораторной работы. Эта лабораторная работа посвящена более подробному знакомству с сервисом AWS IAM. Давайте начнем. Для начала надо открыть основную страницу лабораторной работы. Для этого необходимо воспользоваться платформой AWS Academy, авторизоваться в этой платформе, далее выбрать необходимый курс, открыть четвертый модуль, и в активностях четвертого модуля будет ссылка Lab 1: Introduction to AWS IAM. Как только вы нажмете на эту ссылку, вы перейдете на указанную страницу, которая является основной страницей лабораторной работы. Здесь необходимо нажать на кнопку в меню “Start Lab” для того, чтобы активировать песочницу, и создался специальный AWS-аккаунт для вашей сессии. После успешного старта лабораторной работы, вам необходимо нажать на кнопку AWS для того, чтобы перейти в AWS Management Console.

Как только вы перейдете по ссылке, вы окажетесь на основной странице AWS Management Console. Обратите внимание, вверху справа вы авторизованы под сгенерированным пользователем, а также для вас был специально создан уникальный AWS Account ID.

Далее вам необходимо в верхней строке поиска сервисов AWS начать писать IAM. В выдаче этот сервис будет первым в списке. Давайте перейдем на него. Как только вы попадаете на основную страницу сервиса AWS IAM, необходимо в левом навигационном меню нажать на вкладку “Users” для того, чтобы отобразился список существующих пользователей в этом AWS аккаунте. В рамках лабораторной работы были предварительно созданы три пользователя – User-1, User-2 и User-3. Откроем User-1, чтобы посмотреть некоторые детали по этому пользователю. Если открыть вкладку Permissions, видно, что у этого пользователя нет привязанных к нему Policy. Если нужно это сделать, вы можете воспользоваться кнопкой Add Permissions. Следующая вкладка – это Groups. В этой вкладке отображаются все группы, к которым относится этот пользователь. Мы видим, что данный пользователь в данный момент не относится ни к одной из групп. Следующая вкладка, которую я хотел бы просмотреть – это Security Credentials. На этой странице вы можете найти все Credentials этого пользователя. На этой вкладке необходимо обратить внимание, что Console Password находится в режиме Enabled. Это говорит о том, что у этого пользователя (IAM-User), есть возможность авторизоваться в AWS Management Console.

Мы подробно рассмотрели, какие пользователи были для нас созданы. Также можно открыть подробную информацию о двух других пользователях и убедиться, что она совпадает. Далее необходимо в левом навигационном меню нажать на вкладку User Groups для того, чтобы открылся список существующих групп в этом AWS аккаунте. В этом AWS аккаунте в рамках лабораторной работы было создано три группы: EC2-Admin, EC2-Support и S3-Support. Откроем группу EC2-Support, чтобы посмотреть его детали. На открывшейся странице перейдем на вкладку Permissions и мы видим, что у этой группы одна привязанная Policy, которая называется AmazonEC2ReadOnlyAccess. Здесь я хотел бы обратить внимание, что эта Policy по типу AWS Managed, т.е созданием, обновлением, а также сопровождением этого Policy занимается сам AWS. Нажмем на иконку plus возле этого Policy, чтобы посмотреть, на что нам дается доступ. Мы видим, что в основном выдается доступ на action-ы, операции типа describe и list, т.е. у этого Policy нет возможности изменять ресурсы в рамках AWS, можно только просматривать в режиме чтения. Если мы говорим о сервисах, то это EC2, Elastic Load Balancing, CloudWatch, а также Autoscaling. Далее у нас идет следующая группа. Нажмите в левом навигационном меню вкладку “User Groups” и в открывшемся списке групп перейдите на S3-Support. Здесь открываем вкладку Permissions и мы видим, что у этой группы есть привязанная Policy AmazonS3ReadOnlyAccess. Она также является AWS Managed Policy. Если мы нажмем на кнопку plus, то мы увидим тело этого Policy. Оно нам дает доступ на get, list операции в рамках сервиса S3, т.е. этот Policy также является read only. Сделав это еще раз, мы откроем список существующих групп через вкладку User Groups в левом навигационном меню и переходим к третьей группе EC2-Admin. В этой группе, открыв вкладку Permissions, мы видим, что есть одна привязанная Policy – EC2-Admin-Policy. По типу можно видеть, что это Customer Inline, это говорит о том, что эта Policy была создана индивидуально в рамках этой конкретной группы. Нажав на кнопку plus, мы увидим тело этого Policy. Мы видим, что выдается доступ на все операции, action-ы, начинающиеся с describe для сервиса EC2, а также дополнительно выдается доступ на action-ы start instance и stop instance. Таким образом, мы подробно ознакомились с созданными специально для нас в рамках лабораторной работы IAM группами. Теперь необходимо наших IAM пользователей добавить в соответствующие группы согласно заданию лабораторной работы. Для этого перейдем в левом навигационном меню на вкладку “User Groups” и откроем группу S3-Support.

На странице группы S3-Support переходим на вкладку “Users” и нажимаем на кнопку “Add Users”. Откроется страница с существующими пользователями на этом AWS аккаунте, затем выбираем для группы S3-Support “User-1” и нажимаем на кнопку “Add Users”. Мы будем перенаправлены на основную страницу группы S3-Support. В верхней части появится уведомление зеленого цвета о том, что пользователи были успешно добавлены в эту группу. Если посмотреть на вкладку “Users”, то также увидим только что добавленного пользователя “User-1” в списке пользователей, относящихся к группе S3-Support. Те же действия проделываем со следующими группами, поэтому необходимо еще раз нажать в левом навигационном меню вкладку “User Groups” и перейти в группу EC2-Support. Далее во вкладке “Users” нажимаем на кнопку “Add Users”, выбираем следующего пользователя “User-2”и нажимаем “Add Users”. После чего переходим на страницу EC2-Support и видим аналогичное сообщение о том, что пользователь был добавлен.

Идем дальше. Остается третья группа. В левом навигационном меню нажимаем на вкладку “User Groups”, чтобы отобразился список существующих групп. Затем нажимаем третью группу EC2-Admin и здесь также через вкладку Users нажимаем на кнопку “Add Users”. В списке пользователей мы выбираем третьего пользователя User-3 и нажимаем на кнопку “Add Users”. Мы перейдем на основную страницу группы EC2-Admin и увидим соответствующее сообщение об успешном выполнении этой операции, а во вкладке Users увидим нашего пользователя User-3. Если мы нажмем еще раз на вкладку User Groups в левом навигационном меню, откроется список групп и в этом списке есть специальная колонка Users, которая отображает количество пользователей в соответствующих IAM группах. Мы видим, что в каждой группе сейчас по одному пользователю. Если вы проделали все те действия, которые проделали мы, в конце у вас должна получиться такая картина.

Мы завершили нашу задачу с привязкой пользователей к группам. Перейдем к следующей части, а именно в левом навигационном меню нажмем на вкладку Dashboard. На отобразившейся странице в правой части вы увидите ссылку “Sign in URL for IAM users”, ее надо скопировать и эту ссылку вы можете раздавать вашим сотрудникам и они, используя эту ссылку, могут авторизоваться в вашем AWS аккаунте под IAM пользователями. Авторизуемся под созданными для нас пользователями в этом AWS аккаунте и посмотрим, на какие сервисы у них есть или нет доступа.

Рекомендую вам открыть эту ссылку в Инкогнито режиме. Как только вы откроете эту страницу, появится окно для введения аккаунта ID. Он уже будет введен, так как сидит в этой ссылке. Достаточно ввести логин пользователя и пароль. Логин пользователя это user-1. Пароль вы можете посмотреть на странице с заданием лабораторной работы в AWS Academy. После авторизации в правой верхней части можно увидеть, что мы сидим под тем же AWS account ID, но под пользователем user-1. Давайте перейдем на сервис S3, чтобы посмотреть, отработали ли выданные права для этого пользователя. Как мы видим, здесь успешно отобразился список существующих бакетов на этом AWS аккаунте. Если мы нажмем на единственный бакет, мы провалимся внутрь этого бакета и у нас будет возможность посмотреть, какие же объекты сохранены, загружены в этот бакет. Так как в рамках этой лабораторной работы не было загружено никаких объектов в этот бакет, мы ничего здесь не увидим.

Теперь выполним следующее: откроем сервис EC2, зная, что для user-1 мы не выдавали доступа на сервис EC2. Как только мы перейдем на сервис EC2, в левом навигационном меню нажмем на вкладку instances, чтобы отобразились все существующие инстансы в этом регионе и в этом AWS аккаунте. Вы увидите сообщение “You are not authorized to perform this operation”, это означает, что у нас нет достаточных прав для отображения списка инстансев. Здесь надо отметить, что даже отображение списка ресурсов требует отдельного доступа. Таким образом, можно максимально тонко и детально настраивать доступы внутри нашего облака AWS.

Мы закончили с пользователем user-1, нажмите в верхней правой части на аккаунт ID и в выпадающем меню нажмите на кнопку “sign out”, для того, чтобы разлогиниться и рассмотреть этот AWS аккаунт под другим пользователем. Теперь авторизуемся в нашем AWS аккаунте под пользователем user-2. Для этого воспользуемся той же ссылкой, которую мы скопировали ранее. Необходимо в user name ввести user-2, а также пароль со страницы с заданием лабораторной работы в AWS Academy. После авторизации обязательно обратите внимание в верхней правой части, что вы авторизованы под пользователем user-2. Если все правильно, то мы переходим на сервис EC2. Напомню, что для пользователя user-2 мы выдали права для работы в сервисе EC2 в режиме чтения. Таким образом, у нас есть права отображать список существующих инстансев в рамках региона North Virginia. Чтобы это проверить, перейдем на вкладку в левом навигационном меню, который называется Instances. Он должен отобразить список имеющихся инстансев в этом регионе. Если список инстансов ничего не показывает, он пуст, то обязательно проверьте, что в верхней правой части как регион выбран North Virginia. Если у вас выбран другой регион, нажмите на его название, отобразится список регионов, и внутри необходимо выбрать регион North Virginia или системное название us-east-1. Как только вы это сделаете, вы отобразите список существующих инстансов уже в регионе North Virginia и увидите следующие два инстанса. Мы помним, что для пользователя User-2 выдано право только в режиме чтения. Тем не менее, давайте попробуем остановить наш инстанс LabHost. Выбираем из списка наш инстанс LabHost, вверху справа необходимо нажать на кнопку Instance State и в выпадающем списке нажать на действие Stop Instance. Появится сообщение с запросом подтверждения, действительно ли мы хотим остановить этот инстанс. Указывается Instance ID, в скобках имя этого инстанса, нажимаем на кнопку Stop для подтверждения отключения\остановки этого инстанса. Как только вы это нажмете, появится сообщение красного цвета о том, что у этого пользователя нет прав для остановки инстанса с таким-то ID. Закроем это уведомление.

Теперь перейдем на сервис S3. Мы знаем, что для пользователя User-2 не давалось прав на сервис S3. Таким образом, если мы перейдем в левом навигационном меню на вкладку Buckets, отобразится список бакетов, но этот список будет пустым. Это говорит о том, что сработал Implicit Deny, т.е. по умолчанию, не явно, мы запрещаем доступ на ресурсы AWS. На этом мы заканчиваем с пользователем User-2. В верхней правой части выбираем Account ID и в выпадающем меню нажмем на кнопку Sign Out, чтобы разлогиниться.

Остается последнее задание — посмотреть, что мы можем сделать внутри нашего AWS аккаунта под пользователем User-3. Как мы помним, пользователь User-3 отличается от других пользователей тем, что помимо read only доступа этому пользователю выданы права на остановку и старт instance EC2. Авторизуемся под этим пользователем. Логин User-3, пароль вы можете найти на странице AWS Academy с заданием для лабораторной работы.

После успешной авторизации обязательно проверьте сверху справа, что мы сидим под пользователем User-3. Далее нам необходимо перейти на сервис EC2, поэтому вводим EC2 в верхней строке поиска сервисов AWS. Как только мы перешли на сервис EC2, в левом навигационном меню нажмем на вкладку Instances. Убедитесь, что вы находитесь в регионе North Virginia. Если это так, вам должны отобразиться следующие два инстанса. Попробуем выбрать инстанс LabHost и остановить этот инстанс. Для этого нажимаем на кнопку instance state и в выпадающем списке действий выбираем stop instance. Отобразится окно подтверждения, что действительно мы хотим остановить instance ID такой-то с названием LabHost. Да, мы хотим это сделать и нажимаем на кнопку stop. На следующей странице вы видите, что выходит сообщение зеленого цвета о том, что мы успешно запустили, выполнили действия по остановке этого инстанса. В списке инстансев видно, что instance state, т.е. состояние этого инстанса, находится в режиме “stopping”, т.е. в процессе остановки. Подождав некоторое время и нажав кнопку refresh, то есть обновить список инстансев, мы увидим, что его статус поменялся на stopped, т.е. он полностью остановлен.

Таким образом, мы завершили это задание в рамках лабораторной работы. Можем закрыть это окно, которое было открыто в Инкогнито режиме. Далее у нас есть страница с условным root пользователем, когда мы со страницы с заданием по лабораторной работе, нажав на кнопку AWS, перешли на страницу AWS Management Console. Это именно та страница. Давайте успешно и правильно разлогинимся. Для этого необходимо в верхней правой части нажать на account ID и в выпадающем списке действий в самом внизу нажать на кнопку “sign out” для того, чтобы разлогиниться. Вы увидите следующее сообщение. Значит все отлично, мы можем закрыть эту страницу.

Также не забываем правильно завершить лабораторную работу, чтобы не было в будущем проблем с открытием следующих лабораторных работ. Для этого необходимо на странице AWS Academy и конкретно на странице лабораторной работы в основном меню верхней правой части нажать на кнопку “end lab”. При этом выйдет всплывающее окно с подтверждением, действительно ли мы хотим остановить лабораторную работу. Да, мы хотим остановить, поэтому нажимаем на кнопку “Yes”. После этого отображается другое всплывающее окно, в нем будет сообщение “you may close this message box now”. Это говорит о том, что процесс удаления всех ресурсов и созданного специально для вашей сессии AWS-аккаунта запустился. Теперь она будет работать в фоновом режиме, и вы можете безопасно закрыть это окно. Также вы можете безопасно закрыть страницу AWS Academy и на этом закончить лабораторную работу. Поздравляю вас, мы вместе с вами закончили лабораторную работу, посвященную сервису AWS IAM. На этом с вами прощаюсь, до встречи на следующих наших активностях!