Добрый день, уважаемые студенты! Я рад всех вас видеть! Добро пожаловать на очередную Демо-сессию! Сегодня мы с вами подробно поговорим о сервисе AWS Identity and Access Management (IAM). Чаще вы можете встретить этот сервис как AWS IAM. Итак, начнем.

После авторизации в AWS Management Console, мы попадаем на основную страницу. С этого места мы начинаем наше Демо. Нам необходимо попасть на основную страницу сервиса AWS IAM. Для этого в специальной строке поиска сервисов AWS начнем вводить IAM. Вы увидите, что в выдаче первым выдается необходимая нам ссылка. Давайте на нее нажмем, для того чтобы перейти на основную страницу сервиса. Мы перешли на необходимую нам страницу. Вы видите с левой стороны, что мы находимся во вкладке IAM Dashboard. Давайте подробнее посмотрим, что же мы можем увидеть на этой странице.

Самый первый блок – это Security recommendations. Это список пунктов, которые необходимо выполнить, для того чтобы обезопасить ваш AWS аккаунт. Список может отличаться в зависимости от того, вы авторизованы как Root пользователь или как IAM User. В этом списке наглядно отмечены те пункты, которые выполнены, зеленой галочкой, а также будут отображены красным крестиком, те пункты, которые крайне рекомендуется выполнить.

Следующий блок – IAM Resources. В этом блоке вы можете видеть какое количество определенного вида ресурса у вас есть. Например, на текущем аккаунте есть 1 User group, 1 User, 17 Roles, 5 Policies и 1 Identity provider.

Следующий блок, который я бы вам хотел показать – это AWS account. Давайте, посмотрим, что же в этом блоке есть. Самое первое, что вы можете увидеть – Account ID. Это уникальный идентификатор вашего аккаунта, который вам выдается во время его создания. Есть специальная кнопка, которая позволяет быстро его скопировать. Второе ­– вы можете увидеть настройки Account Alias. Для каждого аккаунта вы можете настроить Alias, для того чтобы проще идентифицировать ваш аккаунт и прямо здесь вы можете его задать. Как только вы задаете Alias, ваш Sign-in URL, т.е. URL, который вы передаете вашим сотрудникам для авторизации как IАM пользователь, он поменяется и вместо Account ID подставится ваш Account Alias. Мы рассмотрели самые основные блоки, которые отображаются на основной странице сервиса AWS IAM.

Давайте теперь подробнее рассмотрим, какие виды ресурсов AWS IAM бывают. Начнем с User groups. Для того чтобы отобразить список существующих групп на этом аккаунте, нам необходимо перейти на вкладку User groups. В этом аккаунте вы можете видеть, что есть одна единственная группа, которая называется admins. Давайте воспользуемся кнопкой в верхней правой части экрана, для того чтобы создать новую группу. На этой странице вам необходимо будет ввести название новой группы, а также вы можете добавить существующих пользователей к этой новой группе. Если вы прокрутите страницу чуть ниже, то вы увидите, что вы также можете добавить к этой группе один или несколько существующих Policies. Мы не будем заполнять опциональные (Optional) поля, поэтому прокрутим до самого конца страницы и нажмем на кнопку Create group. Как только вы нажмете на кнопку Create group, вас перенаправят на страницу с существующими группами. Также на этой странице отобразится уведомление зеленого цвета в самом верху, которое говорит о том, что группа была успешно создана. На основной странице вы видите, что наша новая созданная группа Students, появилась в списке вместе с другими группами.

Мы с вами переходим к следующему виду ресурсов сервиса AWS IAM – это IAM Users. Для того чтобы перейти к списку существующих IAM пользователей, вам необходимо перейти на вкладку Users. Мы видим, что на этом AWS аккаунте есть один пользователь Admin. Давайте создадим нового IAM пользователя. Для этого нам необходимо нажать на кнопку Add user в правой части экрана. При создании IAM пользователя нам необходимо пройти по пяти различным страницам с настройками нового пользователя. Не все страницы являются обязательными. Давайте пройдемся по каждому из них. На самой первой странице вам необходимо будет ввести имя пользователя. На этой же странице ниже вы можете выбрать, какой доступ выдать пользователю. Самый первый блок – это Access key - Programmatic access. Вы отмечаете этот пункт в том случае, если пользователь будет использовать AWS CLI либо AWS SDK, т.е. ему необходим программный доступ. Далее, если вашему пользователю нужен доступ в AWS Management Console, то в этом случае вам необходимо поставить соответствующую галочку. Также вы можете указать настройки пароля либо это будет генерируемый пароль, либо какой-то пароль, который задаете вы сами. Если пользователю необходимо сменить пароль после первой авторизации, то вам необходимо поставить галочку в самом последнем пункте.

На второй странице настроек создания нового пользователя нам необходимо определиться, какие права мы выдаем этому пользователю. Существует 3 варианта. Первый вариант – это добавить этого пользователя к одной из существующих групп. Второй вариант – это скопировать права и доступы одного из существующих пользователей. Третий вар0иант – это напрямую добавить существующие Policies к этому пользователю. Мы выбираем первый вариант, добавить пользователя к одной из существующих групп. Как только вы нажмете на эту опцию, отобразится список существующих групп в нижней части экрана. Давайте добавим нашего пользователя к недавно созданной группе Students. После чего нажмем на кнопку next, для перехода на следующую страницу настроек.

На третьей странице настроек нам предлагается ввести тэги для нового пользователя. Как мы помним, пользователь также является ресурсом AWS. Эта страница является опциональной, поэтому мы не будем ее заполнять и нажмем на кнопку next для перехода к следующей странице настроек.

На четвертой странице вы можете увидеть все введенные вами настройки для нашего пользователя. Если все правильно, мы нажимаем на кнопку create user, для того чтобы создать этого пользователя.

На пятой странице настроек создания пользователя, пользователь уже создается, и вы видите соответствующее сообщение. В центральной части экрана вы видите сгенерированные credentials для нового пользователя. Давайте пройдемся по каждому из них. Первый – это логин пользователя. Второй и третий – это Access key ID и Secret access key, которые нужны для программного доступа к программе AWS. Программный доступ – это использование AWS CLI или AWS SDK. Четвертый – это пароль. Пароль нужен для того, чтобы авторизоваться в AWS Management Consolе. Обратите внимание, что эта информация предоставляется только на этой странице. Поэтому, если это ваш пользователь, то рекомендуется сохранить в надежном месте ваш Secret access key, Access key ID, а также логин и пароль. В случае, если вы создаете пользователя для вашего сотрудника, то рекомендуется воспользоваться функционалом send email для того, чтобы эти credentials отправить на почту вашему сотруднику. Как только вся необходимая информация сохранена, мы можем нажать на кнопку close в нижней части экрана и перейти на следующую страницу. Как только мы нажимаем на кнопку Close, мы завершаем процесс создания нового пользователя и переходим обратно на страницу с существующими пользователями. Вы можете видеть в верхней части экрана сообщение, выделенное зеленым цветом о том, что пользователь успешно создан. В центральной части экрана, где список пользователей, вы также можете увидеть нового созданного нами пользователя.

Давайте проведем небольшую активность. Для этого нам необходимо перейти в сервис Amazon S3. Чтобы перейти в Amazon S3 давайте воспользуемся строкой поиска. Как только мы переходим к сервису Amazon S3, мы открываем вкладку Buckets. Вы можете это видеть в левой части меню. В центральной части экрана вы видите список существующих бакетов (Buckets). В нашем случае у нас есть один созданный Bucket. Давайте теперь авторизуемся в AWS Management Consolе под нашим новым пользователем yelzhan. Так как мы авторизуемся самый первый раз, то нам предлагается заменить пароль и создать новый, который будем знать только мы. Как только мы переходим на основную страницу AWS Management Consolе, в верхней правой части экрана мы видим, что мы авторизовались под пользователем yelzhan. Теперь перейдем в сервис Amazon S3. Для этого воспользуемся строкой поиска. После того, как мы переходим к сервису Amazon S3, открывается вкладка Buckets и мы видим список созданных на этом аккаунте Amazon S3 Buckets. В нашем случае Buckets не отображаются, более того кнопка create bucket не активна. Вопрос. Почему такое произошло? Вы можете сейчас остановить видео и попробовать ответить на этот вопрос. Хорошо. Я думаю, многие из вас ответили правильно. Правильный ответ это то, что, да, мы создали пользователя, да, мы добавили пользователя в группу Students, но ни у группы, ни у пользователя нет соответствующих прав. Для того чтобы пользователь мог что-то делать в AWS аккаунте, в том числе видеть существующие Buckets, либо создавать новый Bucket, ему необходимо выдать соответствующие права.

За выдачу прав в облаке AWS отвечает следующий ресурс сервиса AWS IAM – это IAM Policies. Для того чтобы выдать пользователю Yelzhan соответствующие права, давайте авторизуемся обратно под пользователем admin, перейдем в сервис AWS IAM и откроем вкладку Policies в левой части меню. Вы можете видеть, что в нашем AWS аккаунте есть 975 различных созданных Policy. Давайте сделаем еще одну активность. Остановите это видео и попробуйте ответить. Почему у нас такое большое количество Policу? Хорошо. Правильный ответ это то, что большинство этих Policies не были созданы вручную. Это – managed policy. Как мы с вами помним из лекции, managed policy – ­­это policy, который управляется AWS, дополняются, обновляются, формируются им. Мы можем, для того чтобы ускорить процесс создания чего-либо в облаке, использовать эти policy. По необходимости вы можете создать свое custom policy. Для этого вы можете воспользоваться в верхней правой части экрана кнопкой create policy. В рамках нашей Демо-сессии мы не будем создавать custom policy, а воспользуемся policy, который нам предоставляет AWS. Давайте отфильтруем список этих policy и оставим только те policy, которые связанны с сервисом Amazon S3. В отобразившемся списке в учебных целях выберем policy AmazonS3FullAccess. Здесь хотелось бы еще раз отметить, что когда мы выдаем в облаке доступы к любому из Identity, будь то Role, пользователь или группа, мы всегда должны придерживаться least privilege access, т.е. выдаем только те права, которые необходимы. Далее в верхней правой части выберем Actions и в выпадающем меню выбираем Attach. Как только мы нажмем на эту кнопку, мы попадем на страницу со списком всех существующих identity. Давайте отфильтруем этот список и оставим только User groups. В отфильтрованном списке выберем группу students, которую мы недавно создали. Далее нажимаем кнопку attach policy в нижней правой части экрана. Нас перекинет обратно на вкладку Policies. В верхней части экрана вы можете увидеть зеленое уведомление о том, что мы успешно привязали к одному entity наш AmazonS3FullAccess policy. Давайте теперь посмотрим со стороны группы students, какие изменения там произошли. Для этого нам необходимо в левой части меню перейти во вкладку User groups и открыть группу students. На странице группы students мы можем посмотреть список пользователей, которые находятся в этой группе, а также во вкладке Permissions мы можем увидеть Policies, которые добавлены в эту группу. В нашем случае мы видим AmazonS3FullAccess. Теперь давайте авторизуемся обратно под пользователем yelzhan. Вы можете увидеть, что мы уже сделали это в верхней правой части экрана. Далее, открываем сервис Amazon S3, вкладка Buckets и мы видим, что под этим пользователем отображаются все Buckets в этом AWS аккаунте. Более того, у нас стала активна кнопка create backet. Таким образом, мы видим, что мы выдали им необходимые права, и они сразу применились к нашим сущностям. В нашем случае к пользователю yelzhan через группу Students.

Самая последняя часть нашей сегодняшней Демо-сессии посвящена последнему виду ресурса внутри сервиса AWS IAM ­– это IAM Roles. Для того чтобы посмотреть список существующих Roles (ролей), вам необходимо в левой части меню нажать на вкладку Roles. Давайте с вами попробуем создать новую Role. Для этого необходимо нажать на кнопку Create role в верхней правой части экрана. При создании Role нам необходимо пройтись по трем страницам настройки, которые вы видите с левой стороны экрана. На первой странице нам необходимо определиться с trusted entity, т.е. для чего, либо для кого создается эта Role. Самые популярные два варианта, это: AWS сервис, т.е. мы создаем Role для AWS сервиса, чтобы она могла использовать другие AWS сервисы. Второе – это когда мы создаем Role для другого AWS аккаунта. Это нужно для того, чтобы пользователи из другого AWS аккаунта могли использовать Role на этом аккаунте и получать доступ к ресурсам, сервисам на текущем AWS аккаунте. В рамках нашего Демо мы создадим Role для AWS сервиса. Как только вы выбираете этот пункт, внизу отображается список сервисов, которые вы можете выбрать. Самыми популярными вариантами являются: Amazon EC2 и AWS Lambda. Давайте выберем AWS Lambda и нажмем на кнопку next, для того чтобы перейти на следующую страницу. На второй странице настройки создания Role нам необходимо отметить те policy, которые мы добавляем к этой Role. В рамках нашего Демо мы привяжем к нашей Role следующую policy, называется AWSLambdaBasicExecutionRole. Для того чтобы его быстро найти, нам необходимо в строке для фильтра ввести Lambda и Basic. После того как мы выбрали эту policy, нажимаем на кнопку next в нижней правой части экрана, для того чтобы перейти к следующей настройке. На третьей странице настройки нам предлагается в обязательном порядке заполнить название будущей Role. Далее, при необходимости вы также можете заполнить описание. Если мы прокрутим страницу ниже, то мы можем увидеть сгенерированный JSON, который описывает trusted entity. Этот trusted entity мы вводили на первом шаге. Далее отображается то, что мы выбрали на втором этапе, т.е. все permissions, которые привязаны к этой Role. Если мы прокрутим эту страницу немного ниже, то мы увидим, что мы опционально можем добавить тэги к этой Role. В рамках Демо мы не будем останавливаться на этом подробно. Продолжим и нажмем на кнопку Create role. После того как вы нажмете на кнопку Create role, нас перенаправит на страницу со списком существующих Roles на этом AWS аккаунте. Если вы начнете вводить название вашей Role, то он быстро отсортирует и отобразит нам созданный Role. Также в верхней части экрана вы видите зеленое уведомление о том, что новая Role была успешно создана.

На этом мы завершаем нашу Демо сессию. Мы сегодня более подробно рассмотрели сервис AWS IAM и ее компоненты. Надеюсь, это видео для вас было полезным и мы с вами увидимся на следующих занятиях.