УДК 378.1

ЛАБОРАТОРНЫЕ ЗАНЯТИЯ ПО ОБЛАЧНЫМ ВЫЧИСЛЕНИЯМ С ИСПОЛЬЗОВАНИЕМ ОДНОЙ УЧЕТНОЙ ЗАПИСИ

МУХАМЕТОВ В.Н., МОСКАЛЕВ А.А.

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Республика Беларусь

Аннотация: Организация лабораторных занятий с использованием облачных сервисов. Использование одной учетной записи при проведении занятий. Сервис AWS IAM для обеспечения безопасного проведения занятий.

Ключевые слова: облачные вычисления, облачный провайдер, учетная запись, практическое занятие, AWS IAM.

LABORATORY CLASSES ON CLOUD COMPUTING USING A SINGLE ACCOUNT

MUKHAMETOV V.N., MOSKALEV A.A.

Belarusian State University of Informatics and Radioelectronics, Republic of Belarus

Abstract: Organization of laboratory classes using cloud services. Use of one account during classes. AWS IAM service to ensure the safe conduct of classes.

Keywords: CLOUD COMPUTING, CLOUD SERVICE PROVIDER, ACCOUNT, PRACTICE**,** AWS IAM.

В Институте информационных технологий БГУИР с 2010 года для специальности переподготовки 1-40 01 73 «Программное обеспечение информационных систем» читается дисциплина «Виртуализация и облачные вычисления». В рамках этой дисциплины проводятся лабораторные занятия с использованием облачных ресурсов крупнейших мировых провайдеров – Amazon Web Services (AWS) и Microsoft Azure (MS Azure) [1,2].

Для проведения лабораторных (практических) занятий в облаке слушатели должны выполнять работу в действующей учетной записи облачного провайдера. В определенной степени это является проблемой по нескольким причинам. Во-первых, создание такой учетной записи самостоятельно каждым слушателем (студентом), как показала практика, подчас вызывает у них трудности, что может сорвать выполнение заданий во время занятий. Во-вторых, начинающий пользователь сталкивается с большим количеством элементов управления и настроек, правильно управлять которыми он еще не умеет – это как начинающий водитель, впервые оказавшийся за рулем автомобиля в реальной дорожной обстановке. Неправильные действия могут, например, привести к списанию средств со счета пользователя, возможно немалых. Эти и другие трудности, связанные

с необходимостью выполнения заданий лабораторной работы во время занятия требуют поиска другого решения.

У ведущих облачных провайдеров, имеющих многочисленные сервисы (например, у AWS и Azure их насчитывается более двух сотен). Среди них есть и сервисы, обеспечивающие безопасную работу в облаке. Например, у AWS имеется группа сервисов *Security, Identity, & Compliance* (Безопасность, идентификация и соответствие требованиям), куда входят такие сервисы как *Identity and Access Management*, *IAM* (Управление идентификацией и доступом), *AWS Audit Manager* (Менеджер по аудиту AWS), *Resource Access Manager* (Менеджер доступа к ресурсам) и много других. Наибольший интерес в нашем случае представляет служба **IAM**.

С помощью *AWS Identity and Access Management (IAM)* можно указать, кто или что может получить доступ к сервисам и ресурсам AWS, централизованно управлять мелкими разрешениями и анализировать доступ для уточнения разрешений в AWS. Используя IAM, можно безопасно управлять доступом сотрудников (слушателей, студентов) к рабочим нагрузкам и масштабировать его. [3].

При создании учетной записи AWS вы начинаете с одного удостоверения для входа, которое имеет полный доступ ко всем сервисам и ресурсам AWS в учетной записи. Это удостоверение называется ***root user*** и доступ к нему осуществляется путем входа с адресом электронной почты и паролем, которые вы использовали для создания учетной записи. Мы настоятельно рекомендуем вам не использовать пользователя ***root*** для выполнения повседневных задач. Защитите свои учетные данные пользователя ***root*** и используйте их для выполнения задач, которые может выполнять только пользователь ***root***.

Когда вы используете свои учетные данные пользователя ***root***, у вас есть полный неограниченный доступ ко всем ресурсам в вашей учетной записи AWS, включая доступ к вашей платежной информации и возможность изменить свой пароль. Этот уровень доступа необходим при первой настройке учетной записи. Однако рекомендуется не использовать учетные данные пользователя ***root*** для повседневного доступа.

Вместо того, чтобы делиться своими учетными данными пользователя ***root*** с другими, можно создать отдельных ***IAM users*** (пользователей IAM) в своей учетной записи, которые соответствуют пользователям в вашей организации [4]. У каждого пользователя может быть свой пароль для доступа к Консоли управления AWS. Можно также создать индивидуальный ключ доступа для каждого пользователя, чтобы пользователь мог делать программные запросы для работы с ресурсами в корневой учетной записи. Этот ключ доступа потребуется при создании приложений, работающих с облачными ресурсами – необходимый элемент выполнения заданий лабораторной работы в облаке.

Управление доступом в AWS осуществляется путем создания политик и связывания их с удостоверениями IAM (пользователями, группами пользователей или ролями) или ресурсами AWS. Когда вы создаете пользователя IAM, он не может получить доступ ни к чему в вашей учетной записи, пока вы не дадите ему разрешение. Вы предоставляете разрешения пользователю, создавая политику на основе удостоверений, которая является политикой, прикрепленной к пользователю или группе, к которой принадлежит пользователь. Действия или ресурсы, которые явно не разрешены, по умолчанию запрещены.

Можно организовать пользователей IAM в группы IAM и прикрепить политику к группе. В этом случае отдельные пользователи по-прежнему имеют свои собственные учетные данные, но все пользователи в группе имеют разрешения, прикрепленные к группе. Используйте группы, чтобы упростить управление разрешениями и следовать рекомендациям по безопасности в IAM.

С помощью ***AWS Management Console*** (Консоли управления AWS) можно создать группу пользователей IAM с делегированными разрешениями. Затем создайте *IAM user* для другого пользователя и добавьте его в группу. Вы можете отредактировать свою **политику**, чтобы разрешить доступ только к тем службам, которые нужны вашим пользователям.

Политика – это объект в AWS, который при связывании с удостоверением или ресурсом определяет их разрешения. Можно использовать ***AWS Management Console*** (Консоль управления AWS), ***AWS CLI*** (интерфейс командной строки AWS) или ***AWS API*** для создания ***customer managed policies*** (политик, управляемых клиентом) в IAM. Политики, управляемые клиентом, — это автономные политики, которые вы администрируете в своей учетной записи AWS. Затем вы можете привязать политики к удостоверениям (пользователям, группам и ролям) в своей учетной записи AWS [5].

Начните с минимального набора разрешений и при необходимости предоставьте дополнительные разрешения. Это более безопасно, чем начинать со слишком мягких разрешений, а затем пытаться ужесточить их позже. Проверяйте свои политики. Вы можете выполнять проверку политик с помощью ***IAM Access Analyzer*** при создании и редактировании политик. ***IAM Access Analyzer*** обеспечивает более 100 проверок ваших политик. Он генерирует предупреждения безопасности, когда утверждение в вашей политике разрешает доступ, который считается чрезмерно разрешающим.

Мощным инструментом при настройках прав доступа *IAM users* является ***Policy Simulator*** (Симулятор политик). С помощью симулятора политик IAM можно тестировать и устранять неполадки. Симулятор оценивает выбранные политики и определяет действующие разрешения для каждого из указанных действий. Симулятор использует тот же механизм

оценки политик, который используется во время реальных запросов к сервисам AWS [6].

Использование сервиса IAM, создание учетных записей IAM users, управление ими, создание, редактирование и тестирование политик – все это требует достаточных знаний и опыта использования облачных сервисов вообще и сервисов AWS IAM в частности. Так, Руководство пользователя сервиса IAM на сегодня имеет объем 1165 страниц текста (на английском зыке) [7].

Полезными ограничениями, накладываемыми на действия пользователей (слушателей, студентов во время проведения лабораторных занятий), является, например, ограничение на тип (размер) экземпляра запускаемой в облаке виртуальной машины – действие *Launch Instance*. Дело в том, что размеры этих экземпляров (инстансов) варьируются в огромном диапазоне. Количество ядер процессора может задаваться от 1 до нескольких сотен, размер памяти инстанса – от 1 ГБ до единиц ТБ. Соответственно, стоимость работы такого инстанса изменяется от 1-2 центов до 70-80 долларов за час работы. Созданная группа *IAM users* имеет ограничение, заключающееся в том, что допустимый размер инстанса определен как *t2.micro* или *t3.micro* стоимостью не более 2 центов в час.

Учетные данные для доступа в ***AWS Management Console*** и использования ***AWS API*** в разработанных на лабораторном занятии приложениях преподаватель изменяет для каждого проводимого занятия. В консоли управления службой IAM после каждого занятия выполняется запрет на работу *IAM users* в *AWS Management Console* и блокируются или уничтожаются использованные ключи доступа.

В программе дисциплины переподготовки «Виртуализация и облачные вычисления», кроме лабораторных занятий, предусмотрена также самостоятельная работа (СР), задание по СР выдается слушателям в течение семестра (триместра). Все предшествующие годы первым пунктом задания было создание собственной учетной записи у одного из ведущих облачных провайдеров (провайдеры предоставляют пробный период на 12 месяцев). Все последующие пункты задания по СР выполнялись слушателем в собственной учетной записи. В текущем году создание новой учетной записи превратилось в трудновыполнимое или невыполнимое действие.

Использование учетных записей ведущих облачных провайдеров – Amazon Web Services (AWS), Microsoft Azure (MS Azure) и других встречает дополнительные трудности в текущем году. В сложившейся ситуации особенно актуально использование существующей учетной записи для проведения практических и лабораторных занятий по дисциплинам, связанным с изучением облачных вычислений.

Список литературы.

1. Мухаметов В.Н., Проведение занятий в облачных сервисах Amazon и Microsoft (опыт и сравнение) «Высшее техническое образование: проблемы

и пути развития»: материалы VI Междунар. науч.-метод. конф., Минск, ноябрь 2012, – Минск, БГУИР, 2012. – с.258-259

2. Мухаметов В. Н., Боброва Н. Л., Москалев А. А. Вопросы безопасности при проведении лабораторных занятий с использованием облачных сервисов // Дистанционное обучение – образовательная среда XXI века: материалы XI Международной научно-методической конференции, Минск, 12-13 декабря 2019 г. – Минск : БГУИР, 2019. – С. 208-209.

3. AWS IAM – Управление идентификацией и доступом AWS - Amazon Web Services [Электронный ресурс] – Режим доступа: https://aws.amazon.com/ru/iam/ Дата доступа: 2022-10-20

4. What is IAM – AWS Identity and Access Management – [Электронный ресурс] – Режим доступа: https://docs.aws.amazon.com/IAM/latest/UserGuide/ Дата доступа: 2022-10-20

5. Policies and permissions in IAM - AWS Identity and Access Management [Электронный ресурс] – Режим доступа: https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html Дата доступа: 2022-10-20

6. Testing IAM policies with the IAM policy simulator - AWS Identity and Access Management [Электронный ресурс] – Режим доступа: https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_testing-policies.html Дата доступа: 2022-10-20

7. AWS Identity and Access Management - User Guide (PDF document) [Электронный ресурс] – Режим доступа: https://docs.aws.amazon.com/IAM/latest/UserGuide/iam-ug.pdf Дата доступа: 2022-10-20