ВОПРОСЫ БЕЗОПАСНОСТИ ПРИ ПРОВЕДЕНИИ ЛАБОРАТОРНЫХ ЗАНЯТИЙ С ИСПОЛЬЗОВАНИЕМ ОБЛАЧНЫХ СЕРВИСОВ

Мухаметов В.Н., Боброва Н.Л., Москалев А.А.

Институт информационных технологий БГУИР, г. Минск, Беларусь,
valery@bsuir.by, natasha.bobrowa@gmail.com, alamos-edu@mail.ru

Abstract. Organization of laboratory classes using cloud services (IaaS). Security is provided by services such as IAM from AWS. Shared Security Responsibility Model, Security of the Cloud, Security in the Cloud.

Проведение лабораторных занятий по ИТ дисциплинам в вузе требует наличия разнообразных программных инструментов и сред, подчас в различных операционных системах.

Использование облачных сервисов для проведения дистанционных лабораторных занятий имеет преимущества перед другими технологиями [1].

Сегодня существует эффективная форма проведения дистанционных лабораторных занятий, позволяющая обеспечить каждого слушателя качественным, унифицированным и в то же время уникальным для каждой лабораторной работы рабочим местом (виртуальной машиной, ВМ). Такую форму проведения занятий обеспечивает использование сервиса IaaS (Infrastructure as a Service, Инфраструктура как сервис) с арендой ресурсов в Public Cloud (публичном облаке). Авторы имеют опыт проведения лабораторных работ дистанционно с использованием облачных сервисов [2].

Существует немало известных крупных облачных провайдеров, предоставляющих услуги IaaS: Amazon Web Services, Microsoft Azure, Google Cloud Platform и другие. Они обеспечивают возможность быстрого развертывания из одного образа (Image) нужного количества одинаковых экземпляров (Instances) виртуальных машин требуемого типа, с предустановленным программным обеспечением. Возможна предварительная подготовка собственного образа на базе предоставленного базового. Следует отметить, что использование экземпляров ВМ в облаке не требует дополнительных расходов на лицензирование используемого ПО.

Если говорить о практической стороне дела, то подготовка необходимого образа ВМ заключается в установке и настройке требуемого программного обеспечения. Таким образом, можно создать уникальный образ ВМ для каждой лабораторной работы. Если создание образа перед каждым циклом лабораторных занятий слишком затратно по времени, однажды созданный образ можно сохранить. Авторы имеют опыт как создания образа непосредственно перед проведением занятия с последующим удалением, так и хранения образов для их повторного использования.

Использование экземпляров ВМ в облаке является формой аренды вычислительных ресурсов ЦОД провайдера и тарифицируется с учетом времени аренды и типа (по сути, «мощности») ВМ. Многие провайдеры имеют разнообразные варианты ценообразования (особенно этим отличается AWS). Так, тип ВМ, называемый у AWS «micro» (1 ядро CPU, 1 Гбайт RAM) стоит от 0,4 до 2 центов в час (в зависимости от установленной ОС, от региона и от варианта оплаты. Более мощные ВМ с двумя ядрами CPU – «medium» (4GB RAM) и «large» (8GB RAM) – стоят 3-7 и 6-12 центов в час, соответственно. Если использовать облачные ресурсы регулярно, можно встретить цены ниже на 20-40%, а при определенных условиях – ниже на 50-75% [3].

Время использования экземпляра ВМ на занятии не превышает 3 часов (астрономических). Таким образом, проведение одной лабораторной работы с аудиторией 15 человек (типовая численность подгруппы) может обойтись в $1-6 (при постоянно работающей ВМ).

Аренда оплачиваемых ресурсов предполагает решение важного аспекта безопасного использования ресурсов – исключение или уменьшение вероятности значительного увеличения стоимости на каком-либо рабочем месте. В первые годы существования сервисов IaaS провайдеры не могли предоставить инструмента для решения этой проблемы. Однако, в дальнейшем, ситуация изменилась. На сегодня лидером в этом направлении является Amazon Web Services (AWS), предлагающий сервис Identity and Access Management (IAM) – Управление идентификацией и доступом [4].

Облачный провайдер AWS определяет модель обеспечения безопасности, как Модель совместной ответственности (Shared Security Responsibility Model). Такая модель помогает снизить операционную нагрузку на клиента, поскольку AWS берет на себя вопросы эксплуатации, контроля и управления компонентами от уровня виртуализации до уровня физической безопасности объектов, где работает сервис.

Различают следующие понятия:

– меры безопасности, реализуемые и поддерживаемые поставщиком облачных сервисов (AWS), – «безопасность облака» (Security of the Cloud);

– меры безопасности, реализуемые и поддерживаемые клиентом и относящиеся к безопасности клиентского контента и приложений, использующих сервисы AWS, – «безопасность в облаке» (Security in the Cloud).

Безопасностью облака управляет AWS, безопасность в облаке входит в ответственность клиента [5, 6].

Концепция безопасности AWS предполагает создание дочерних учетных записей пользователей IAM (*IAM users*), распространения на них действия различных политик безопасности, присвоения им определенных ролей, что обеспечивает наличие только необходимых для выполнения заданий прав по отношению к ресурсам AWS.

Сервис AWS IAM позволяет создавать пользователей и группы пользователей AWS, а затем управлять ими, обеспечивает точный контроль доступа к ресурсам AWS. AWS Identity and Access Management – это веб-служба, которая помогает безопасно контролировать доступ к ресурсам AWS. IAM используется для управления тем, кто аутентифицирован (вошел в систему) и авторизован (имеет разрешения) на использование ресурсов. Когда вы впервые создаете учетную запись AWS, вы начинаете с идентификатора единого входа, который имеет полный доступ ко всем службам и ресурсам AWS в учетной записи. Это удостоверение называется корневым пользователем (root user) учетной записи AWS, и к нему можно получить доступ, указав адрес электронной почты и пароль, которые вы использовали для создания учетной записи. «Настоятельно рекомендуется не использовать пользователя root для выполнения повседневных задач, даже административных. Вместо этого придерживайтесь наилучшей практики использования пользователя root только для создания своего первого пользователя IAM [7].

Управление пользователями IAM можно выполнять в IAM различными способами:

– создание пользователей IAM и управление ими;
– создание групп IAM и управление ими;
– управление данными для доступа пользователей;
– создание политик доступа и управление ими.

Для назначения разрешений можно создать и назначить политики с помощью Консоли управления AWS, API IAM или интерфейса командной строки AWS.

Управляемые политики – это ресурсы IAM, устанавливающие разрешения с помощью языка политик IAM. Они могут создаваться, редактироваться и управляться отдельно от пользователей, групп и ролей IAM, с которыми они связаны. Управляемую политику можно связать с несколькими пользователями, группами или ролями IAM. Управляемые политики могут быть назначены только пользователям, группам или ролям IAM. Их нельзя использовать как политики на основе ресурсов [8].

AWS IAM имеет очень удобный встроенный симулятор политики. Симулятор политики IAM – это инструмент, позволяющий понять, проверить и оценить эффективность политик управления доступом. Симулятор политик можно использовать несколькими способами. Можно проверять изменения политик перед тем, как передать их в работу, чтобы убедиться, что они работают так, как нужно. Можно проводить оценку существующих политик, назначенных пользователям, группам и ролям, чтобы проверить разрешения и решить связанные с ними проблемы. Можно также использовать симулятор политик для того, чтобы разобраться, как политики IAM и политики на основании ресурсов работают совместно и предоставляют или отклоняют доступ к ресурсам AWS [7].

AWS IAM предоставляет возможность создавать временные данные для доступа. Временные данные для доступа включают идентификатор ключа доступа AWS, секретный ключ доступа и токен безопасности. Временные данные, подтверждающие права доступа, действуют в течение определенного периода времени и для определенного набора разрешений. Временные данные, подтверждающие права доступа, иногда просто называются токенами.

Следование концепции безопасности в облаке предусматривает выдачу студентам (слушателям) реквизитов безопасности (логин, пароль, ключи доступа), использование которых исключает нежелательные инциденты при проведении лабораторной работы. Так, например, имеется возможность ограничить тип и количество запускаемых экземпляров ВМ под этими учетными записями (если такое право предоставлять некоторым учетным записям). Конечно же, возможность блокировки и разблокировки учетных записей IAM и/или соответствующих ключей доступа делает весьма безопасным такое использование облачных ресурсов.

IAM – это возможность аккаунта AWS, которая предоставляется без дополнительной оплаты.

Авторы имеют опыт многократного проведения лабораторных занятий в облачных сервисах AWS с использованием службы IAM.

Литература

1. Мухаметов, В. Н. Проведение дистанционных лабораторных работ с использованием облачных сервисов / В. Н. Мухаметов, Н. Л. Боброва, А. А. Москалев // Дистанционное обучение – образовательная среда XXI века : материалы X международной научно-методической конференции (Минск, 7–8 декабря 2017 года). – Минск : БГУИР, 2017. – С. 279–280

2. 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.

3. Цены на Amazon EC2 – AWS [Электронный ресурс]. – Режим доступа: https://aws.amazon.com/ru/ec2/pricing.

4. Identity and Access Management (IAM) – Amazon Web Services (AWS) [Электронный ресурс]. – Режим доступа: https://aws.amazon.com/ru/iam.

5. Безопасность облака – Amazon Web Services (AWS) [Электронный ресурс]. – Режим доступа: https://aws.amazon.com/ru/security.

6. Модель общей ответственности – Amazon Web Services (AWS) [Электронный ресурс]. – Режим доступа: https://aws.amazon.com/ru/compliance/shared-responsibility-model.

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

8. Вопросы и ответы по IAM – Amazon Web Services (AWS) [Электронный ресурс]. – Режим доступа: https://aws.amazon.com/ru/iam/faqs.