Д. С. Симоненкова

О БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ ОБЛАЧНЫХ ТЕХНОЛОГИЙ

По данным исследования рынка облачных платформ (IaaS, или оборудование-как-услуга), которое проводилось ресурсом Gigaom, Amazon занимает лидирующую позицию на рынке облачных платформ. Amazon Web Services (AWS) включает около 450 000 серверов и, по подсчетам компании Accenture, приносит Amazon около 1 млрд долларов в год. Следом за Amazon располагаются такие сервисные провайдеры, как Rackspace — активный участник альянса OpenStack, Google — облачная платформа Google App Engine, IBM — облачная платформа SmartCloud [1].

Наиболее популярная облачная платформа AWS предоставляет пользователю широкий набор необходимых сервисов: вычислительные мощности, аренду виртуальных серверов, хранение данных как веб-сервис. Дата-центры AWS находятся в шести регионах мира, что позволяет подписчику выстроить инфраструктуру, устойчивую при стихийных бедствиях [2].

Ключевыми сервисами, предоставляемыми AWS, являются: Amazon Simple Storage (Amazon S3), Amazon CloudWatch и Amazon Elastic Compute Cloud (Amazon EC2), также Amazon Web Services предоставляет такие сервисы, как Amazon Relational Database Service (Amazon RDS), Amazon Simple Queue Service (Amazon SQS), Amazon Simple Notifications Service (Amazon SNS), Amazon Elastic MapReduce, Amazon Virtual Private Cloud (Amazon VPC), Amazon Route5, AWS Identity и Access Management (IAM) [3]. Взаимодействие сервисов Amazon Web Services представлено на рис. 1.

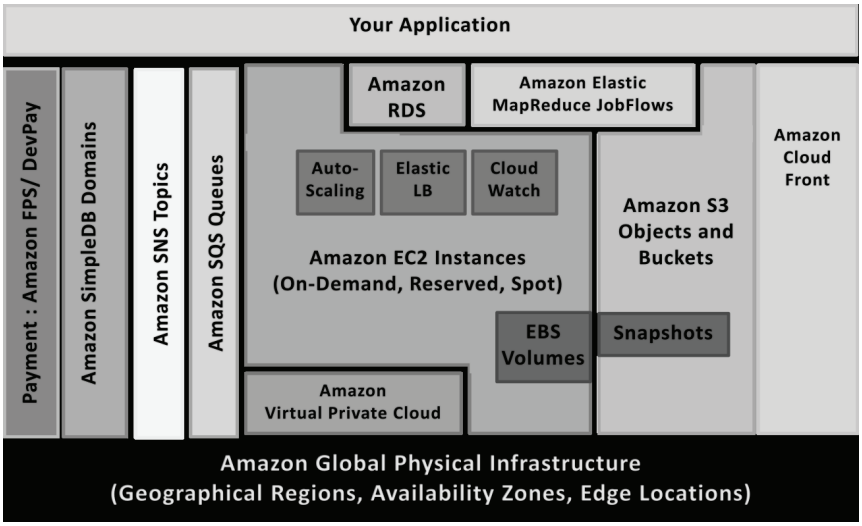

Рис. 1. Amazon Web Services

Amazon Relational Database Service (Amazon RDS)

Amazon RDS обеспечивает простой способ установки, эксплуатации и масштабирования реляционных баз данных в облаке. Имеется возможность запускать экземпляры БД, получать доступ к полнофункциональной БД MySQL и легко решать административные задачи, такие как резервное копирование, управление печатью и т. д. [4].

Amazon Simple Queue Service (Amazon SQS)

Amazon SQS является надежной, масштабируемой, распределенной очередью для хранения сообщений, передаваемых между компьютерами и отдельными приложениями [5].

Amazon Simple Notifications Service (Amazon SNS)

Amazon SNS предоставляет простой способ для уведомления приложений и подписчиков, работающих с облаком, путем создания заголовков и использования протоколов публикации-подписки [6].

Amazon Elastic MapReduce

Amazon Elastic MapReduce обеспечивает размещение в рамках Hadoop, находящихся в веб-пространстве Amazon Elastic Compute Cloud (Amazon EC2) и Amazon Simple Storage служб (Amazon S3) и позволяет создавать собственные JobFlows, представляющие собой последовательность шагов MapReduce [7].

Amazon Virtual Private Cloud (Amazon VPC)

Amazon VPC позволяет размещать корпоративную сеть подписчика в частном облаке, находящемся в AWS. Amazon VPC использует режим туннелирования IPSec, что позволяет создать защищенное соединение между шлюзом в центре обработки данных и шлюзом в AWS [8].

Amazon Route 53

Amazon Route 53 является масштабируемым DNS-сервисом, который позволяет управлять DNS-записями, создавая Hosted Zone для каждого домена, которым подписчик управляет.

AWS Identity and Access Management (IAM)

IAM позволяет создать несколько кабинетов подписчиков с уникальными учетными данными безопасности и управлять правами доступа для каждого из этих подписчиков в своем кабинете AWS. IAM изначально интегрированы в AWS Services. Ни одна из служб Application Programming Interface (API) интерфейса не была изменена для поддержки IAM, а значит, выход из приложения и комплект инструментов, надстроенный над AWS службой API, будет продолжать работать при использовании IAM [9].

Amazon Simple Storage (Amazon S3)

Amazon S3 является веб-службой, предоставляющей возможность для хранения и получения любого объема данных в любое время из любой точки сети.

Основными элементами, которыми оперирует Amazon S3, являются объекты. Объекты состоят из данных объекта и метаданных (набор пар «имя — значение», которые описывают объект). Хранятся объекты в контейнере и однозначно идентифицируются в контейнере по ключу и версии ID.

Политика контейнера обеспечивает централизованный контроль доступа в контейнер, основанный на различных условиях, в том числе операциях Amazon S3, запросах, ресурсах и аспектах запроса (например, IP-адрес). Правила, прикрепленные к контейнеру, применяются ко всем объектам в этом контейнере. Политики контейнера могут использовать как частные лица, так и организации.

Контроль доступа на уровне контейнеров и объектов обеспечивается Amazon S3 API-интерфейсом. По умолчанию авторизованный доступ к контейнеру/объекту предоставляется только владельцу. Информация о правах доступа к сервису хранится в Access Control List (ACL). При необходимости владелец может изменить права доступа к своим данным, сделав их, если потребуется, даже общедоступными, тем самым подписчик полностью осуществляет контроль доступа к своим данным.

Также Amazon S3 позволяет включить функцию ведения журнала доступа к контейнеру и объектам. В журнале доступа отображается подробная информация о каждом запросе доступа, в том числе тип запроса, запрашиваемый ресурс, IP пользователя, который совершал запрос, а также время и дата запроса [10].

Amazon CloudWatch

Amazon CloudWatch обеспечивает надежное, масштабируемое и гибкое решение для мониторинга ресурсов облака AWS и пользовательских приложений, запущенных на AWS, осуществляя контроль состояния сервисов AWS (мониторинг состояния серверов, доступность портов и т. д.).

Разработчики и системные администраторы могут использовать Amazon CloudWatch для сбора и отслеживания метрик — данных, собираемых с экземпляров и агрегируемых по различным критериям в группы. Не требуется создавать, управлять и масштабировать свои собственные системы и инфраструктуры мониторинга. Amazon CloudWatch позволяет предпринимать автоматизированные действия, основанные на состоянии облачной среды, для устранения возникающих неполадок [11].

Amazon Elastic Compute Cloud (Amazon EC2)

Amazon EC2 — веб-сервис, который обеспечивает изменение вычислительных мощностей в облаке, позволяя получать доступ и настраивать вычислительные мощности с минимальными затратами, и предоставляет подписчикам полный контроль над вычислительными ресурсами.

Amazon EC2 основывается на двух концепциях: Amazon Machine Image (AMI) и экземпляр (Instance). AMI представляет собой шаблон, содержащий настройки программного обеспечения (операционная система, сервер приложений). В AMI запускаются экземпляры, которые работают как копии AMI. Экземпляры продолжают работать до тех пор, пока подписчик не остановит их или пока не возникнет сбой в их работе.

Безопасность данных в Amazon EC2 может обеспечиваться на нескольких уровнях: хостовой ОС, ОС виртуального образа, или гостевой ОС, межсетевого экрана, вызова API Amazon. Целью защиты является построение структуры, работа которой обеспечит защиту данных в Amazon EC2 от доступа неавторизованного пользователя. Экземпляр Amazon EC2 должен быть защищен настолько, насколько это возможно без ущерба для гибкости конфигурации, необходимой пользователям [12].

Безопасность данных в Amazon EC2 на уровне хостовой ОС

Доступ к панели управления хостовой ОС имеют только администраторы, которые получают доступ к специально созданному административному хосту, используя схему многофакторной аутентификации. Все действия, производимые на специальном административном хосте, заносятся в журнал.

Безопасность данных в Amazon EC2 на уровне гостевой ОС

Виртуальные экземпляры полностью контролируются подписчиком. Администраторы Amazon CloudWatch не имеют доступа к гостевой ОС. Подписчики обладают полными правами доступа к административному управлению собственными аккаунтами, сервисами и приложениями. Также подписчикам обеспечивается набор привилегий в момент входа. Подписчики сами генерируют свои ключевые пары для обеспечения конфиденциальности и не передают их другим подписчикам или AWS.

Обеспечение безопасности на уровне МСЭ

Обязательной составляющей Amazon EC2 является МСЭ. При этом по умолчанию входящий трафик запрещен, и подписчики Amazon EC2 должны открывать необходимые порты для разрешения входящего трафика. Трафик может быть ограничен по протоколам, портам или IP-адресам источника.

Экземпляры могут быть объединены в различные классы, и каждому классу экземпляров могут быть заданы разные права доступа. Примером может служить стандартная трехуровневая модель, изображенная на рис. 2.

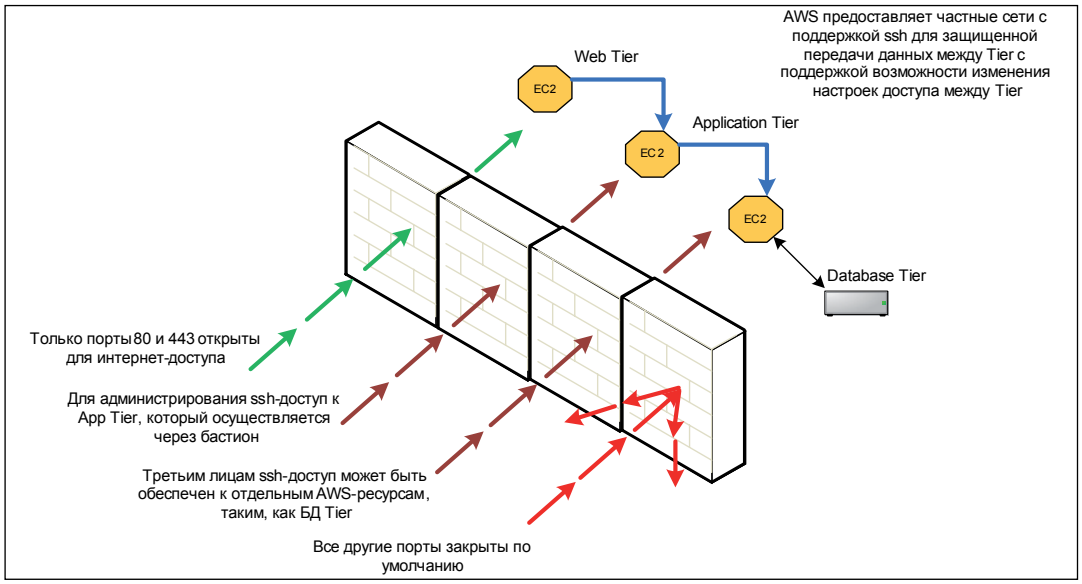

Рис. 2. Настройки безопасности МСЭ

Из рис. 2 видно, что для группы веб-серверов открыт порт 80 (HTTP) и/или порт 443 (HTTPS). Группа серверов приложений доступна только группе веб-серверов по порту 8000. Группа серверов баз данных доступна только группе серверов приложений по порту 3306 (MySQL). И ко всем этим группам открыт административный доступ по порту 22 (SSH).

Обеспечение безопасности на уровне API-вызовов

Доступ к экземплярам, изменению настроек МСЭ и т. д. производится посредством API-вызовов. При этом для осуществления всех изменений требуется авторизация при помощи цифрового сертификата X.509 и закрытого ключа, что обеспечивает дополнительный уровень обеспечения безопасности. Имеется поддержка шифрования API-вызовов с помощью SSL. Рекомендуется всегда использовать SSL-шифрование (по умолчанию SSL включен и обмен данными ведется через https).

Обеспечение сетевой защиты Amazon Web Services

Защита от атак класса «Распределенный отказ в обслуживании» (DDoS)

Для защиты от атак класса DDoS в Amazon введены ограничения на количество возможных одновременных соединений. AWS API пользователя располагается на обширной интернет-инфраструктуре мирового класса, инженерный опыт администрирования которой гарантирован крупнейшим в мире онлайн-ритейлером. К тому же сети AWS распределены между несколькими провайдерами, что обеспечивает дополнительную защиту.

Защита от атак класса «Человек посередине» (MITM)

Защита от атак класса MITM обеспечивается при помощи SSL. Все AWS API-интерфейсы доступны через SSL, обеспечивая тем самым защиту конечных пользователей и аутентификацию сервера. Amazon EC2 AMI автоматически генерирует новый SSL-сертификат хостовой системы. Подписчики могут использовать защищенные API-вызовы для доступа к хостовой системе.

Защита от атак класса IP Spoofing

Внутри Amazon EC2 экземпляры не могут генерировать трафик, так как это запрещается посредством использования МСЭ и AWS-контроллеров. Администрируемая AWS инфраструктура МСЭ предотвращает возможность передачи пакетов с IP- и MAC-адресами, отличными от собственных.

Port Scanning

Сканирование портов является нарушением политики использования AWS. Случаи сканирования отслеживаются и блокируются. Сканирование портов неэффективно ввиду того, что большинство портов в Amazon закрыты по умолчанию и открываются только по желанию подписчиков.

Защита от перехвата пакетов другими подписчиками

Экземпляр может получить только тот трафик, который адресован ему. Нельзя получить доступ к данным других экземпляров того же самого клиента, даже если эти экземпляры находятся физически на одной машине [13].

В заключение можно сказать, что, возможно, совсем скоро приложения перестанут привязываться к оборудованию. Будут доступны любые вычисления, хранение данных и интернет-ресурсы без необходимости работы с физическими серверами. Приложения будут адаптироваться к любым изменениям и получать доступ к ресурсам мгновенно и автоматически, что позволит достичь высочайших показателей мобильности использования. Способность изменяться, безопасность, доступность, отказоустойчивость, постоянная тестируемость и эластичность станут настраиваемыми свойствами архитектуры приложений и будут автоматически подстраиваться под архитектуру системы.

Сегодня лучшие практические реализации облачных вычислений продолжают модернизироваться и концентрируются не только на вопросах развития самого облака, но и на создании технологий и процессов, облегчающих разработчикам и архитекторам подключение приложений к облаку и обеспечивающих безопасность данных в облаке. Для обеспечения безопасности данных в облаке должны быть определены требования к системе защиты, а для этого должна быть построена детализированная модель угроз безопасности сред облачных вычислений. К сожалению, методика построения модели угроз информационных систем, основанных на технологиях облачных вычислений, на момент написания данной статьи авторам не известна.

СПИСОК ЛИТЕРАТУРЫ:

1. Топ 10 облачных платформ для бизнеса — 05.05.10. URL: http://www.livebusiness.ru/news/8937 (дата обращения: 10.11.2012).
2. About AWS. URL: http://aws.amazon.com/what-is-aws/ (дата обращения: 10.11.2012).
3. Amazon Web Services — Architecting for the Cloud: Best Practices — January 2010. URL: http://media.amazonwebservices.com/AWS_Cloud_Best_Practices.pdf (дата обращения: 10.11.2012).
4. Amazon Relational Database Service (Amazon RDS). URL: http://aws.amazon.com/rds (дата обращения: 10.11.2012).
5. Amazon Simple Queue Service (Amazon SQS). URL: http://aws.amazon.com/sqs and (дата обращения: 10.11.2012).
6. Amazon Simple Notifications Service (Amazon SNS). URL: http://aws.amazon.com/sns (дата обращения: 10.11.2012).
7. Amazon Elastic MapReduce. URL: http://aws.amazon.com/elasticmapreduce (дата обращения: 10.11.2012).
8. Amazon Virtual Private Cloud (Amazon VPC). URL: http://aws.amazon.com/vpc (дата обращения: 10.11.2012).
9. AWS Identity and Access Management (IAM). URL: http://aws.amazon.com/iam (дата обращения: 10.11.2012).
10. Amazon Simple Storage (Amazon S3). URL: http://aws.amazon.com/s3 (дата обращения: 10.11.2012).
11. Amazon CloudWatch. URL: http://aws.amazon.com/cloudwatch/ (дата обращения: 10.11.2012).
12. Amazon Elastic Compute Cloud (Amazon EC2). URL: http://aws.amazon.com/ec2 (дата обращения: 10.11.2012).
13. Amazon Web Services: Overview of Security Processes — May 2011. URL: aws.amazon.com/whitepapers/ (дата обращения: 10.11.2012).