Amazon Web Services

Автор: Барабанщикова Н.И.

Облачные вычисления

- В последние годы облачные вычисления приобретают все большую популярность.
- Одним из лидеров этого рынка является компания Amazon.

Web-сервисы Amazon

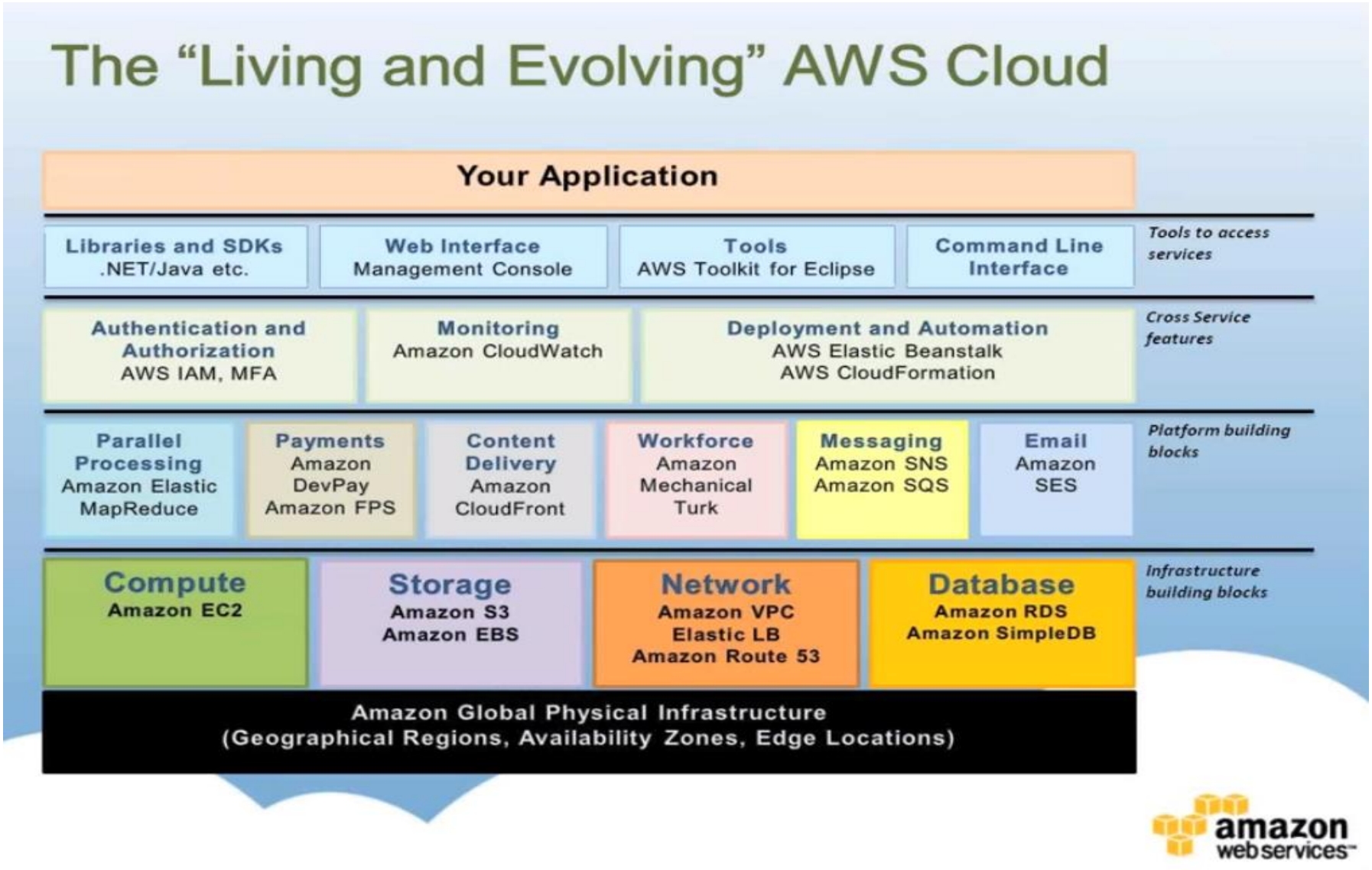
- AWS используются для развертывания и сопровождения Web-приложений в облаке.
- Для облачных вычислений Amazon использует подход «Инфраструктура как сервис» (IaaS).

Иерархия AWS

Иерархия Web-сервисов Amazon содержит несколько уровней:

1. Глобальная физическая инфраструктура.
2. Блоки построения инфраструктуры.
3. Блоки построения платформы.
4. Кросс-сервисные возможности.
5. Инструментальные средства доступа к сервисам.

Иерархия AWS

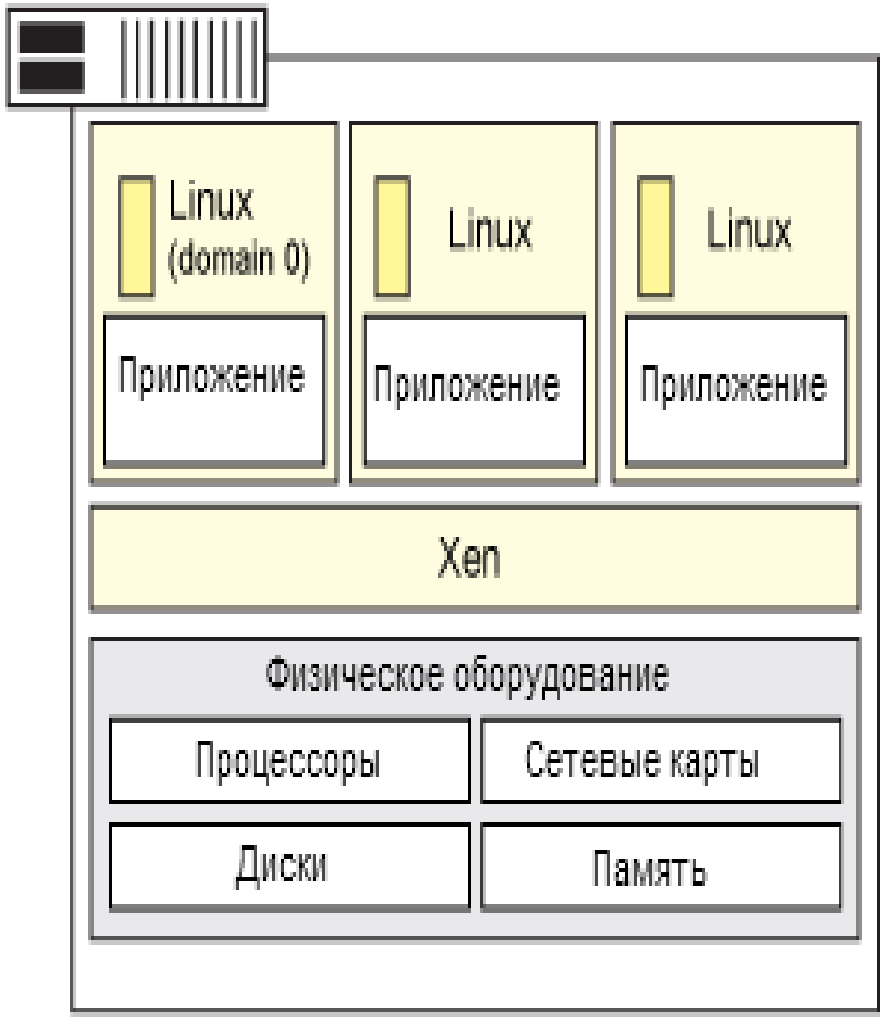


Физическая инфраструктура AWS

- Основой AWS является аппаратная виртуализация.
- Благодаря виртуализации один физический сервер можно разделить на много виртуальных серверов (ВС).
- На каждом ВС работает своя ОС.
- Каждому ВС выделяются такие ресурсы, как память, процессоры и диски.

Виртуализация

- Amazon использует виртуализацию на основе ПО Xen.
- Xen – это гипервизор, на котором может работать несколько гостевых ОС.
- Гипервизор создает уровень аппаратных абстракций, позволяя гостевым ОС совместно использовать ресурсы физического сервера, не имея к ним прямого доступа.

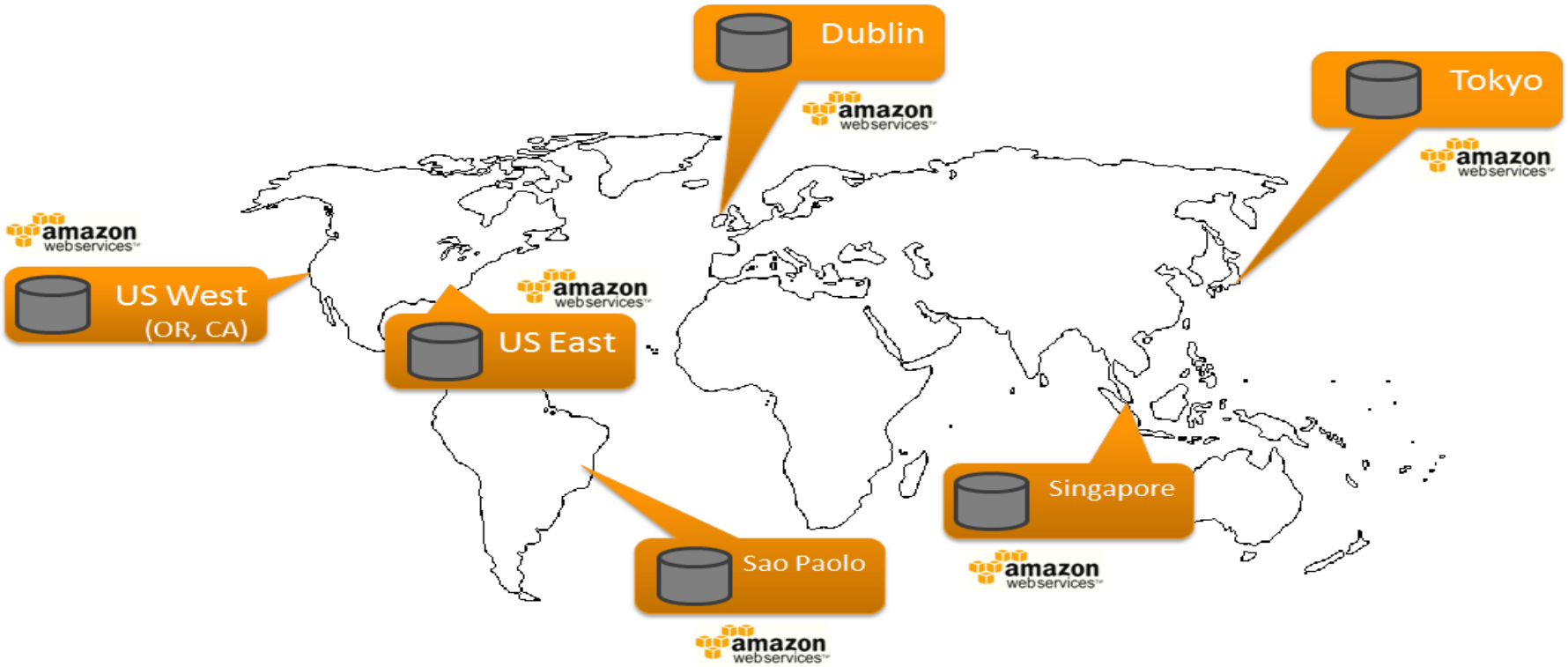


Центры обработки данных

Сервера и сетевое оборудование сосредоточены в центрах обработки данных (ЦОД) Amazon.

География ЦОДов Amazon

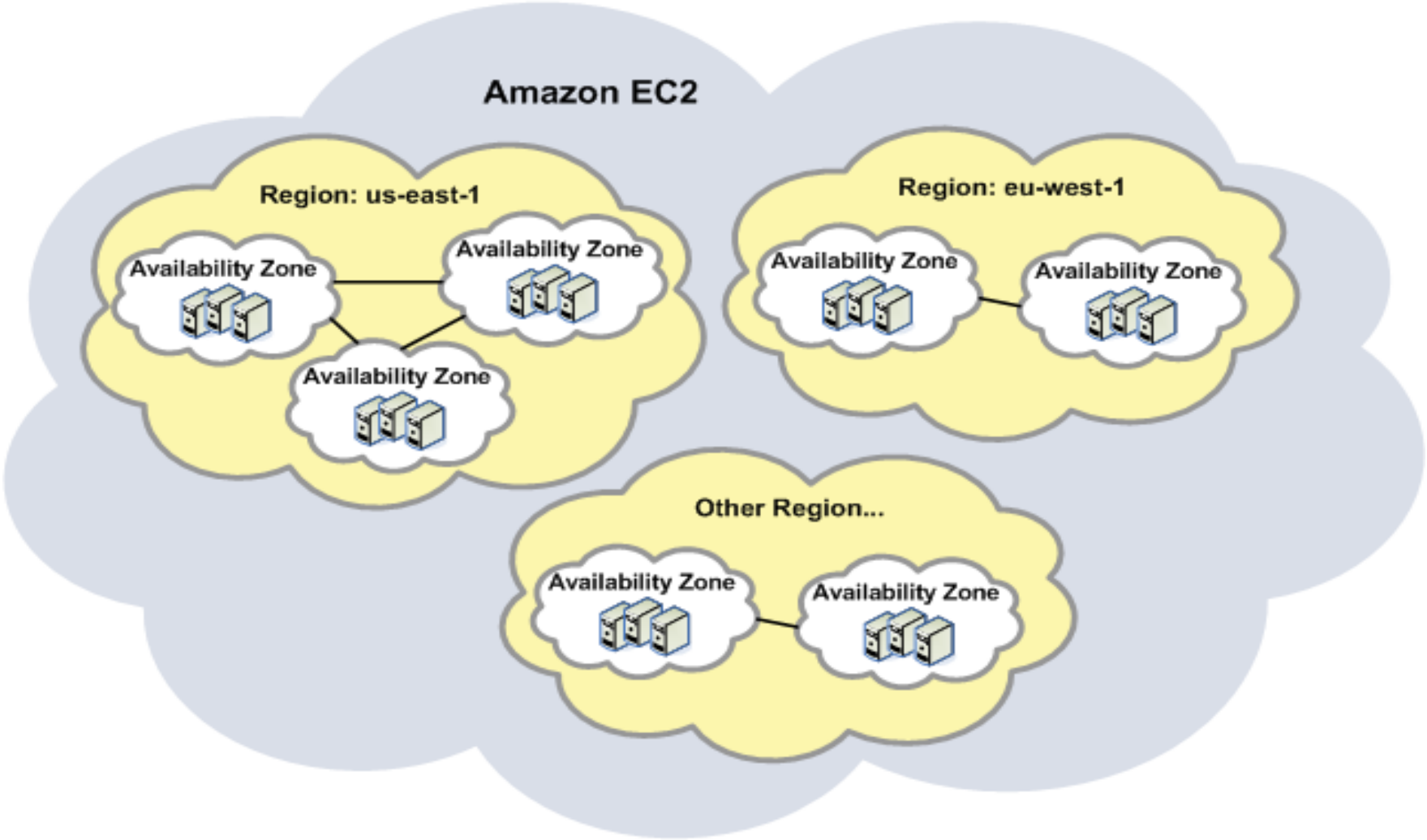
В настоящее время серверы Amazon Web Services развернуты во многих странах по всему миру.



Терминология физической инфраструктуры

- **Регион** (Region) – это региональное местоположение дата-центров, в которых работают виртуальные машины.
- Регионы делятся на **зоны доступности** (Availability Zone).
- Сервисы AWS доступны в дата-центрах расположенных в США, Ирландии, Сингапуре и Японии.
- Для пользователей из России, логичным будет использование региона в Ирландии (EU West Ireland).

Концепция регионов и зон доступности



Уровень построения инфраструктуры

Содержит Web-сервисы для работы с:

- **Виртуальными серверами** (Compute) – Amazon EC2
- **Системами хранения** (Storage) – Amazon S3, Amazon EBS.
- **Сетью** (Network) – Amazon VPC Elastic LB, Amazon Route.
- **Базами данных** (Database) – Amazon RDS, Amazon Simple DB

Amazon EC2

Amazon Elastic Compute Cloud (EC2) — это облачный сервис, предоставляющий:

- виртуальные сервера
- 2 вида хранилищ данных:
  - краткосрочное (исчезает вместе с ВМ)
  - блочное (остается при удалении ВМ).
- балансировщик нагрузки.

Функциональность Amazon EC2

- **Позволяет запускать сконфигурированные сервера** с предустановленными ОС (Linux, Windows).
- **Создавать свои образы** (Amazon Machine Image).
- **Балансировка нагрузки и автомасштабирование**. Можно создать правила при которых станет возможно автоматически увеличить количество серверов, если один или несколько серверов не справляются с нагрузкой.
- **Настроить защиту доступа к серверам**.

Запуск инстанса EC2

- **Через AWS Management Console**:

  - Зайти в консоль

    https://console.aws.amazon.com/ec2/

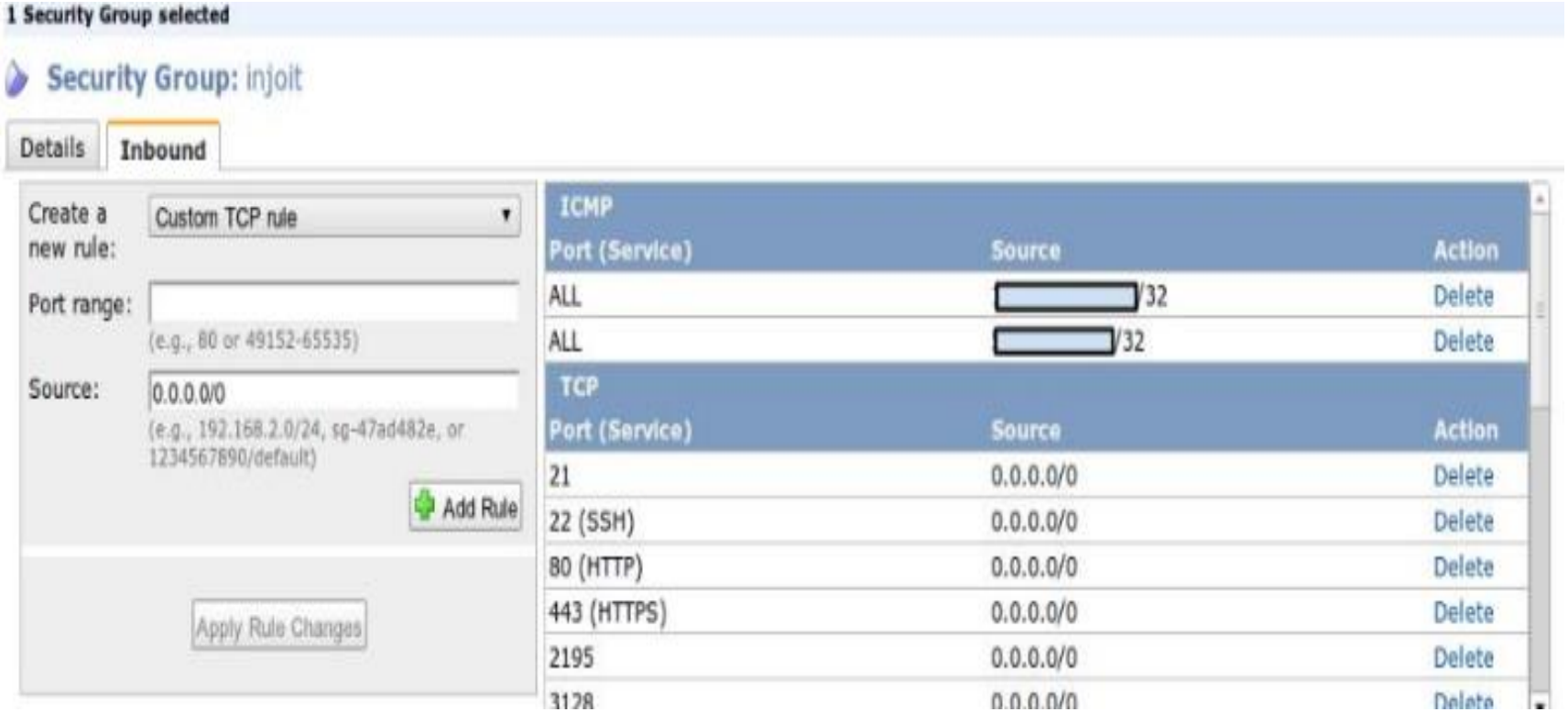
  - В панели консоли выбрать **Launch Instance**

- **Через командную строку**:

$ ec2-run-instances ami_id --availability-zone zone

Настройка групп безопасности

EC2 инстансы объединяются в группы безопасности (Security Group) с возможностью ограничения доступа по портам с IP или подсетей.



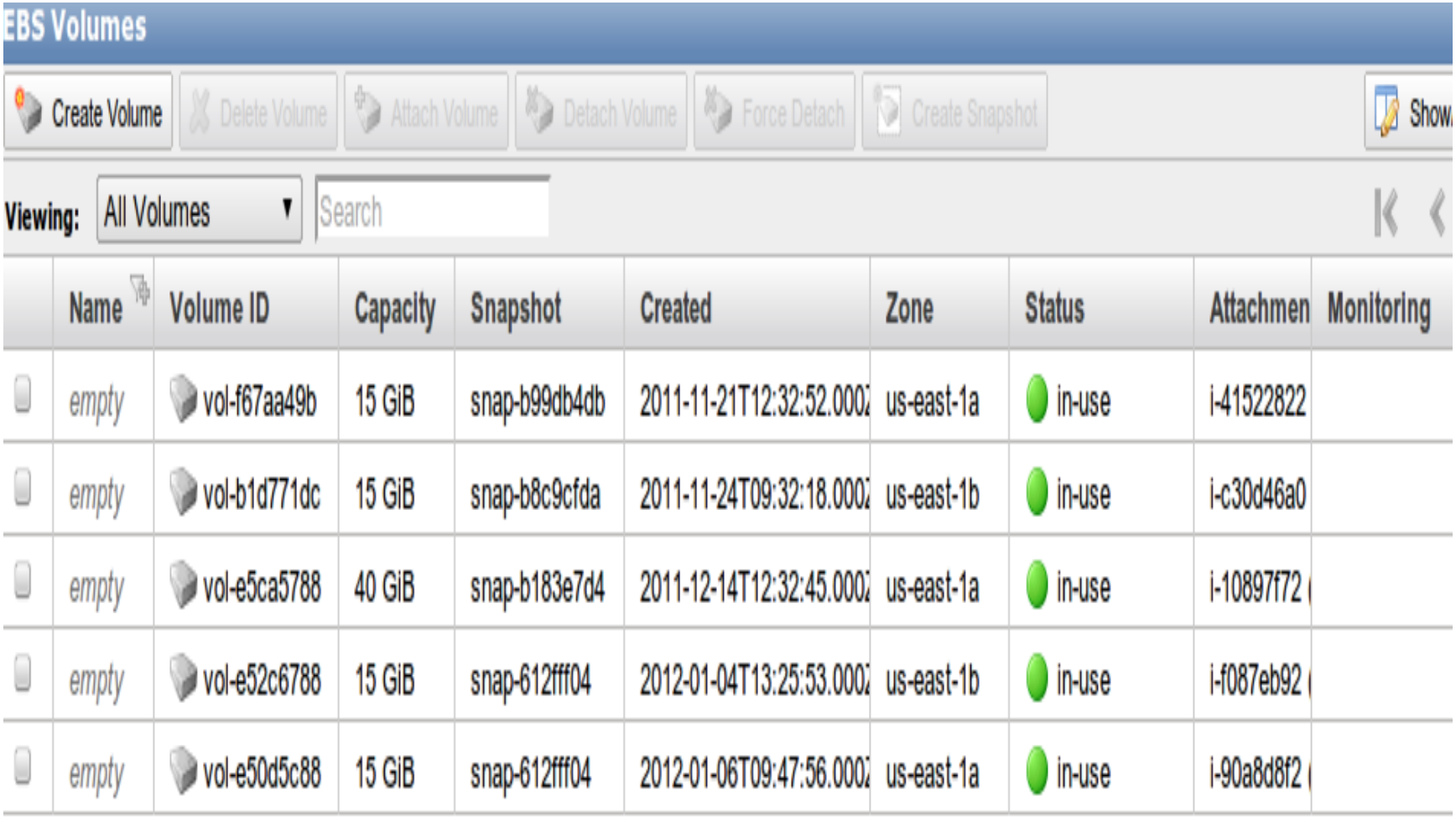
Серверы EC2

Название	Платформа	ОЗУ	EC2 compute units *	Заметки
Micro Instances				
Micro	32 и 64 битная	613 Мб	2 (краткосрочно)	При нагрузке более 3-4 секунд становится не производительнее мобильного телефона. Бесплатный. Только EBS.
Standard Instances				
Small	32 битная	1.7 Гб	1	Используется по умолчанию.
Large	64 битная	7.5 Гб	4	
Extra Large	64 битная	15 Гб	8	
High-Memory Instances				
High-Memory Extra Large Instance	64 битная	17.1 Гб	6.5 (2 по 3.25)	
High-Memory Double Extra Large Instance	64 битная	34.2 Гб	13 (4 по 3.25)	
High-Memory Quadruple Extra Large Instance	64 битная	64.4 Гб	26 (8 по 3.25)	
High-CPU Instances				
High-CPU Medium Instance	32 битная	1.7 Гб	5 (2 по 2.5)	
High-CPU Extra Large Instance	64 битная	7 Гб	20 (8 по 2.5)	
Cluster Compute Instances				
Cluster Compute Quadruple Extra Large	64 битная	23 Гб	35.5	
Cluster Compute Eight Extra Large	64 битная	60.6 Гб	88	
Cluster GPU Instances				
Cluster GPU Quadruple Extra Large	64 битная	22 Гб	33.5	2 x NVIDIA Tesla “Fermi” M2050 для обработки графики

Amazon EBS

- EBS (Elastic Block Storage) — это один из типов хранилища в EC2.
- Диски, создаваемые по этой технологии не зависимы от VPS-ноды и расположены на специальных Storage серверах, в отличии от Instance хранилищ, которые расположены непосредственно на серверах виртуализации.
- Используя EBS, к запущенным серверам можно “наживую” добавлять диски любого размера.

Управление дисками EBS



Amazon S3

- **Amazon S3** это сервис для хранения данных в файлах.
- Предоставляется безразмерное пространство для хранения файлов размером от 1 байта до 5 Терабайт.
- **Файлы хранятся в отдельных бакетах (bucket)**, в которых можно создавать директории и поддиректории.
- **Бакеты хранятся в разных регионах** (Region).
- Доступны следующие регионы: US Standard, US West (Oregon), US West (Northern California), EU (Ireland), Asia Pacific (Singapore), Asia Pacific (Tokyo), South America (Sao Paulo), и GovCloud (US).

Amazon S3

- **К бакетам можно применять разного рода политики безопасности**: делать их приватными, публичными, а так же разделять права между пользователями.
- **S3 может логгировать запросы и складывать отчёты в отдельный бакет**. Это удобно при расследовании, когда много пользователей или приложений имеют доступ к сервису.
- **Загрузка, удаление и другие операции доступны по REST или SOAP**, так же возможно шифрование канала передачи данных с S3.

Amazon S3

- **Можно встроить BitTorrent протокол** заменой http, как основного протокола скачивания файлов.
- **Предоставляется 99.999999999% гарантия целостности** и 99.99% гарантия доступности файлов в год.
- **S3 так же предполагает версионность файлов**. Всегда можно восстановить файл предыдущей версии, т.е. откатиться до нужного состояния.
- **Пространство имен бакетов одно на всех пользователей**, поэтому названия бакетов должны быть уникальными.

Использование Amazon S3

- Создание корзины (bucket), где будут храниться файлы:

s3cmd mb s3://*BUCKET*

- Заполнение корзины файлами:

s3cmd put *LOCAL_FILE* s3://*BUCKET/S3FILE*

- Извлечение файла из облака:

s3cmd get s3://*BUCKET/S3FILE* *LOCAL_FILE*

Amazon Relational Database Service

RDS — это сервис баз данных, который выносится на отдельную машину.

Проще говоря, это отдельные VPS серверы, оптимизированные для работы с базами данных.

Amazon Relational Database Service

В Amazon RDS доступны следующие СУБД:

- MySQL community edition
- Oracle Database Standard Edition One
- Oracle Database Standard Edition
- Oracle Database Enterprise Edition

Выбор СУБД в Amazon RDS

mysql
MySQL Community Edition

Select

ORACLE

oracle-se1
Oracle Database Standard Edition One

Select

ORACLE

oracle-se
Oracle Database Standard Edition

Select

ORACLE

oracle-ee
Oracle Database Enterprise Edition

Select

Amazon RDS

- Дисковое пространство RDS инстанса заказывается клиентом.
- Минимальный размер стораджа — 5 Гб.
- **Можно гибко настроить доступ к серверу БД с помощью групп безопасности**. Доступ возможно дать отдельным адресам/подсетям или же группам безопасности EC2 и всем серверам, которые в неё входят.
- **Можно настроить репликацию между серверами БД** через консоль или утилиты командной строки.

Amazon RDS

- **RDS поддерживает мгновенные слепки (Snapshot) и автобекап**, давая возможность быстро и качественно восстановить данные.
- Если случаются проблемы с аппаратным обеспечением, **RDS автоматически перенесёт ваш хост на здоровую ноду.**
- При выходе обновлений, **СУБД могут быть автоматически пропатчены и перезагружены**. Клиенты уведомляются заблаговременно.
- **root доступа к СУБД нет**. Возможности хранения встроенных процедур и тонкие настройки осуществляются через API и утилиты командной строки.
- **Все RDS инстансы работают на 64 битной платформе.**

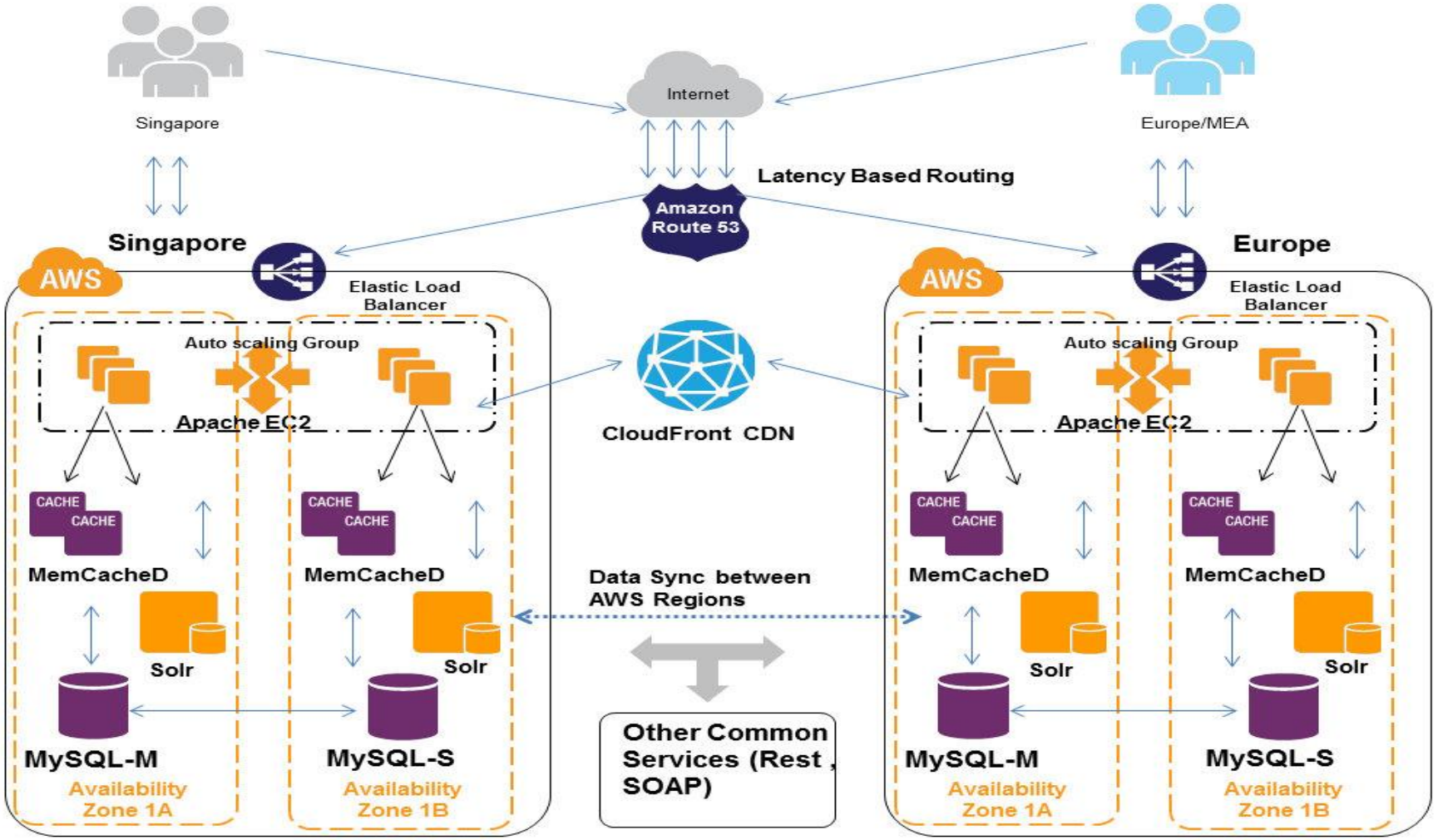
Типы RDS инстансов

Тип	ОЗУ	ECU	IO capacity
Small	1.7 Гб	1	Средняя
Large	7.5 Гб	2x2	Высокая
Extra Large	15 Гб	4x2	Высокая
High-Memory Extra Large	17.1 Гб	2x3.25	Высокая
High Memory Double Extra Large	34 Гб	4x3.25	Высокая
Hitgh Memory Quadraple Extra Large	68 Гб	8x3.25	Высокая

Amazon Route 53

- **Route53** — это облачный DNS сервис от Amazon.
- Помогает улучшить производительность приложений в глобальном масштабе.
- Amazon постоянно собирают анонимную информацию о задержках до конечных пользователей и проводят сравнительные анализы этих самых задержек.
- Amazon Route 53 автоматически определит ближайший к клиенту датацентр и отдаст IP вашего приложения в нем.

Amazon Route 53



Уровень построения платформы

Содержит Web-сервисы для работы с:

- **Параллельной обработкой** – Amazon Elastic MapReduce.
- **Платежными системами** – Amazon DevPay, Amazon FPS.
- **Доставкой контента** – Amazon CloudFront.
- **Workforce** – Amazon Mechanical Turk.
- **Обработкой сообщений** – Amazon SNS, Amazon SQS
- **Электронной почтой** – Amazon SES.

Amazon DevPay

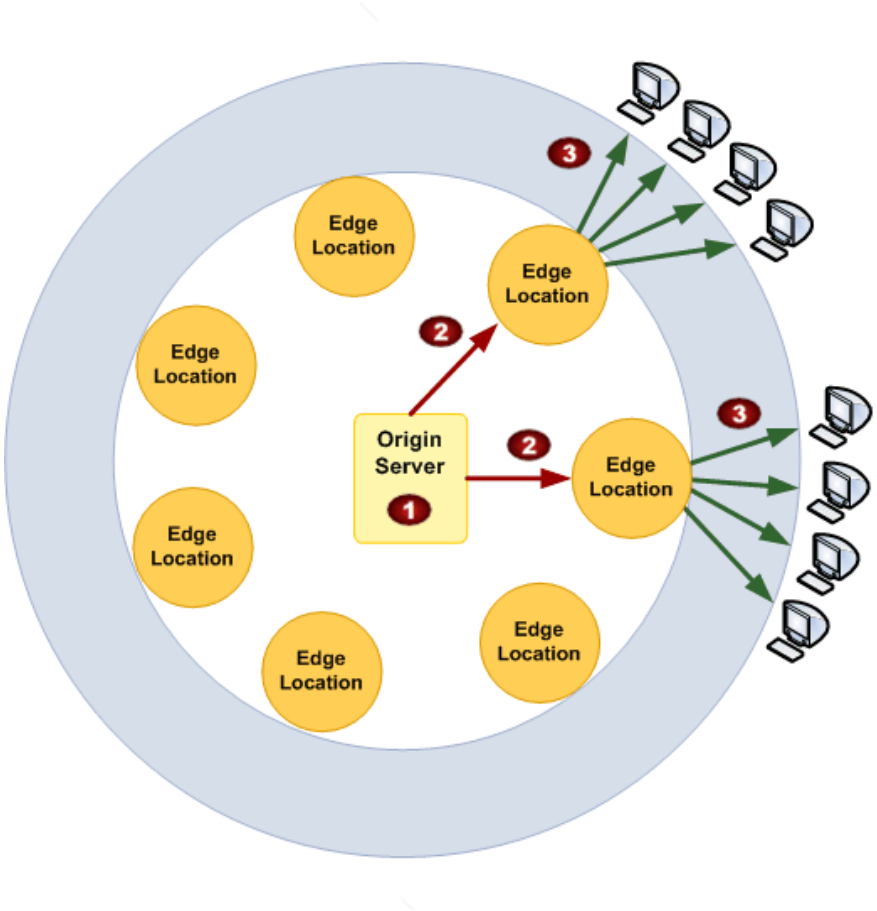
- **Amazon DevPay** – это облачный сервис, который позволяет вам управлять расчетными счетами и собирать оплату за ваши AWS-приложения.

Amazon CloudFront

- **Amazon CloudFront** — сервис для доставки контента.
- Этот сервис позволяет распространять ваше информационное наполнение по периферии сети с учетом того, что информация будет доставлена из точки, близкой к местоположению запросившего ее пользователя.
- Цель сервиса — дать разработчикам и предприятиям простой способ распространять контент для конечных пользователей с минимальными задержками и высокой скоростью передачи данных.

Amazon CloudFront

1. Размещение файлов в месте их обычного хранения (**Origin Server**).
2. Копирование файлов на географически близкий для пользо-вателя Web-сайт (**Edge Location**).
3. Доставка файлов пользователю.



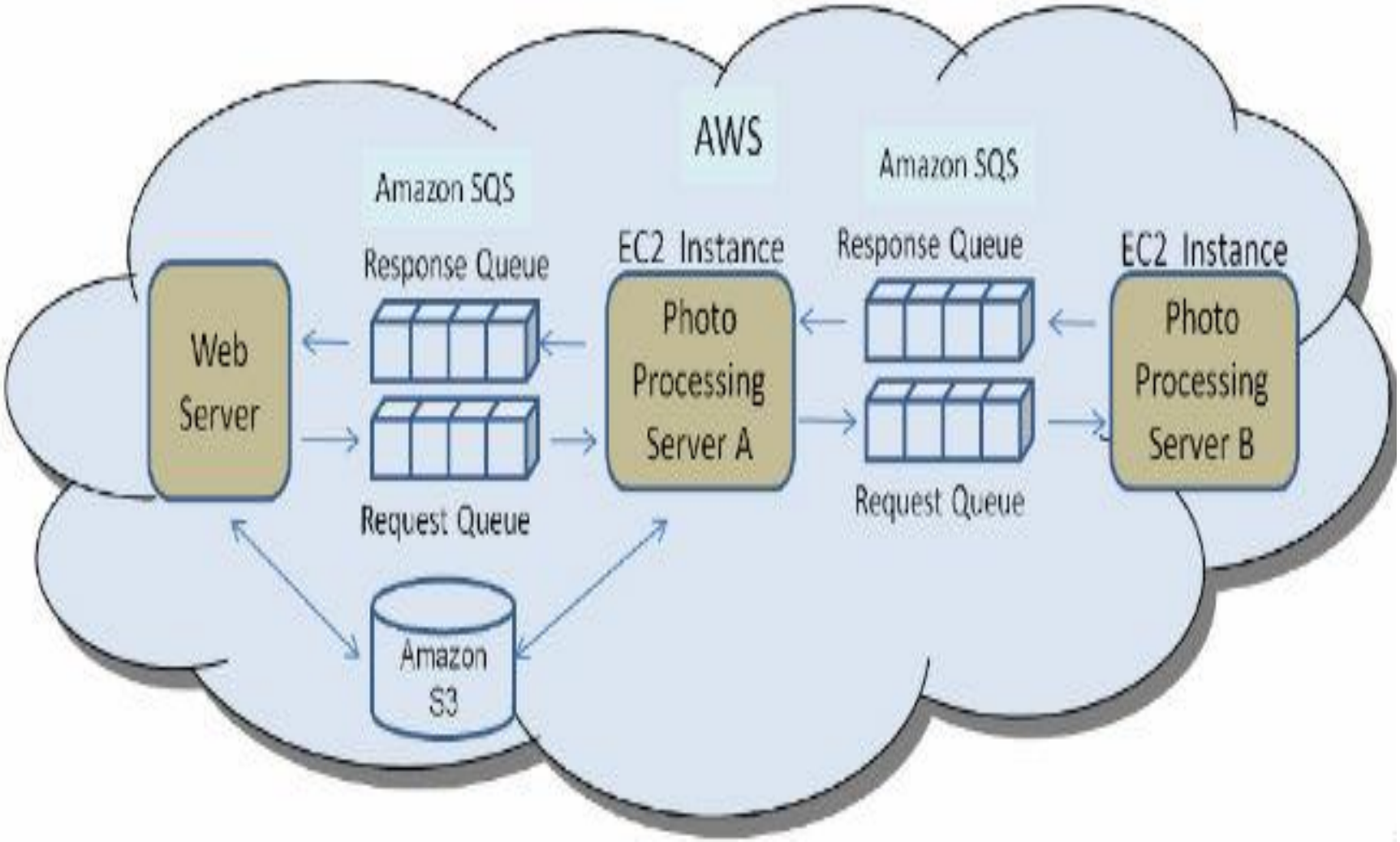
Amazon Simple Queue Service (SQS)

SQS — сервис для построения очередей событий.

Amazon SQS принимает сообщения и передает их серверам, подписанным на очередь сообщений.

Система обмена сообщениями позволяет многим компьютерам обмениваться информацией, не имея никаких сведений друг о друге.

Пример использования SQS

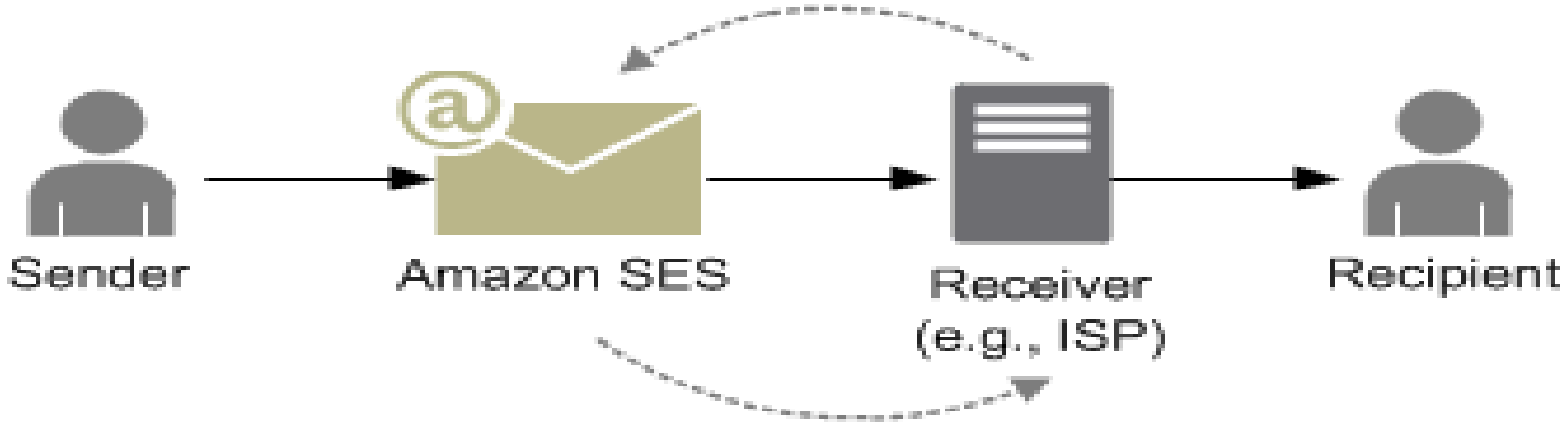


Amazon Simple Email Service (SES)

SES используется для отправки почты, а точнее рассылок. Высокая репутация IP адресов, высокая производительность серверов, позволяющая слать десятки-сотни тысяч писем в день даёт возможность осуществлять рассылку сообщений от малого до большого корпоративного размера предприятия.

Функционал Amazon SES

- SES позволяет слать письма через API — прямо из приложения.
- Существуют десятки библиотек, плагинов дающих возможность слать письма обходя SMTP методы.
- Для приложений, которые не могут быть интегрированы с SES через API — существует опция включения SMTP сервера с авторизацией по связке логин-пароль.



Уровень кросс-сервисных возможностей

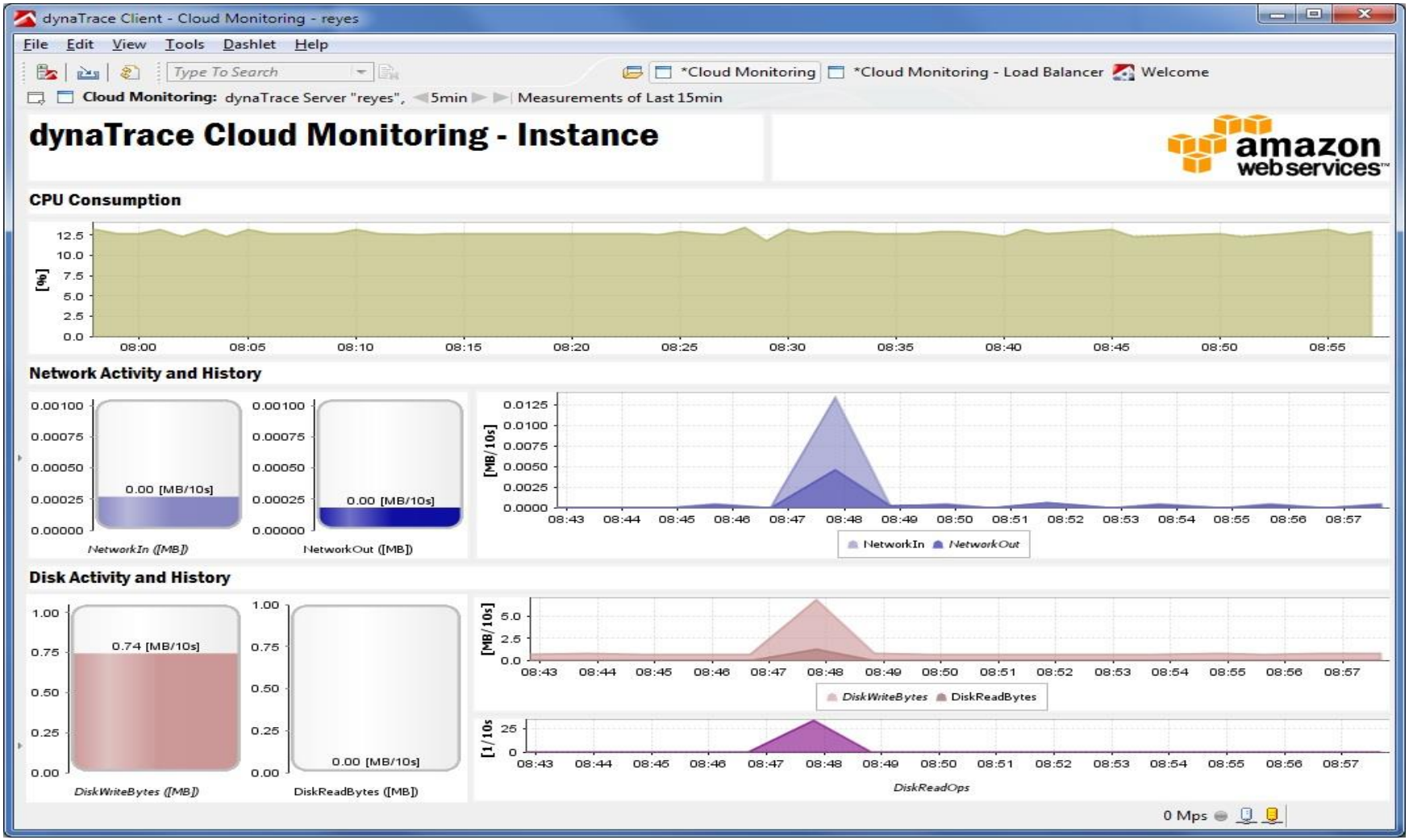
Содержит Web-сервисы для работы с:

- **Аутентификацией и авторизацией** – AWS IAM, MFA.
- **Мониторингом** – Amazon CloudWatch.
- **Развертыванием и автоматизацией** – AWS Elastic Beanstalk, AWS Cloud Formation.

Amazon Cloud Watch

Cloud Watch используется для мониторинга здоровья и состояния всех сервисов AWS, включая стандартный мониторинг здоровья серверов, доступность тех или иных портов, систем хранения, работу СУБД, место на S3 и очень много всяких других проверок.

Amazon Cloud Watch



Amazon Cloud Watch

Cloud Watch существует 3 типа состояний:

- **OK** (нормальное состояние)
- **ALARM** (ошибка или тревога)
- **UNSUFFICIENT DATA** (неизвестное состояние)

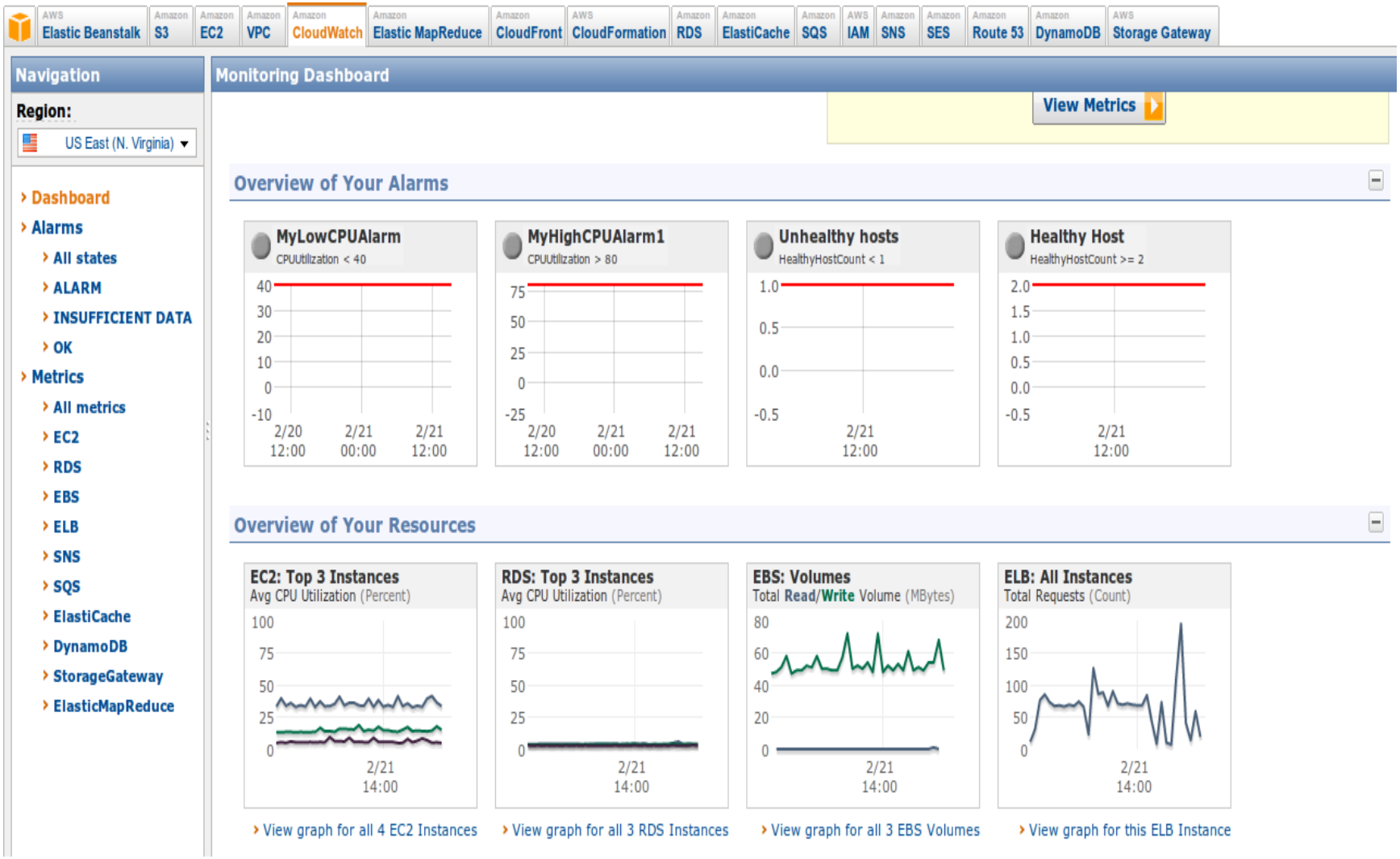
На все состояния можно настроить триггеры, которые будут срабатывать во время изменения счётчика в это состояние.

Amazon Cloud Watch

- Автомасштабирование построено на показателях счётчиков CloudWatch.

- По политикам CloudWatch могут сработать триггеры, которые запускают новые копии серверов для увеличения мощности приложения, и так же при снижении нагрузки потушить ненужные серверы.

Консоль управления CloudWatch

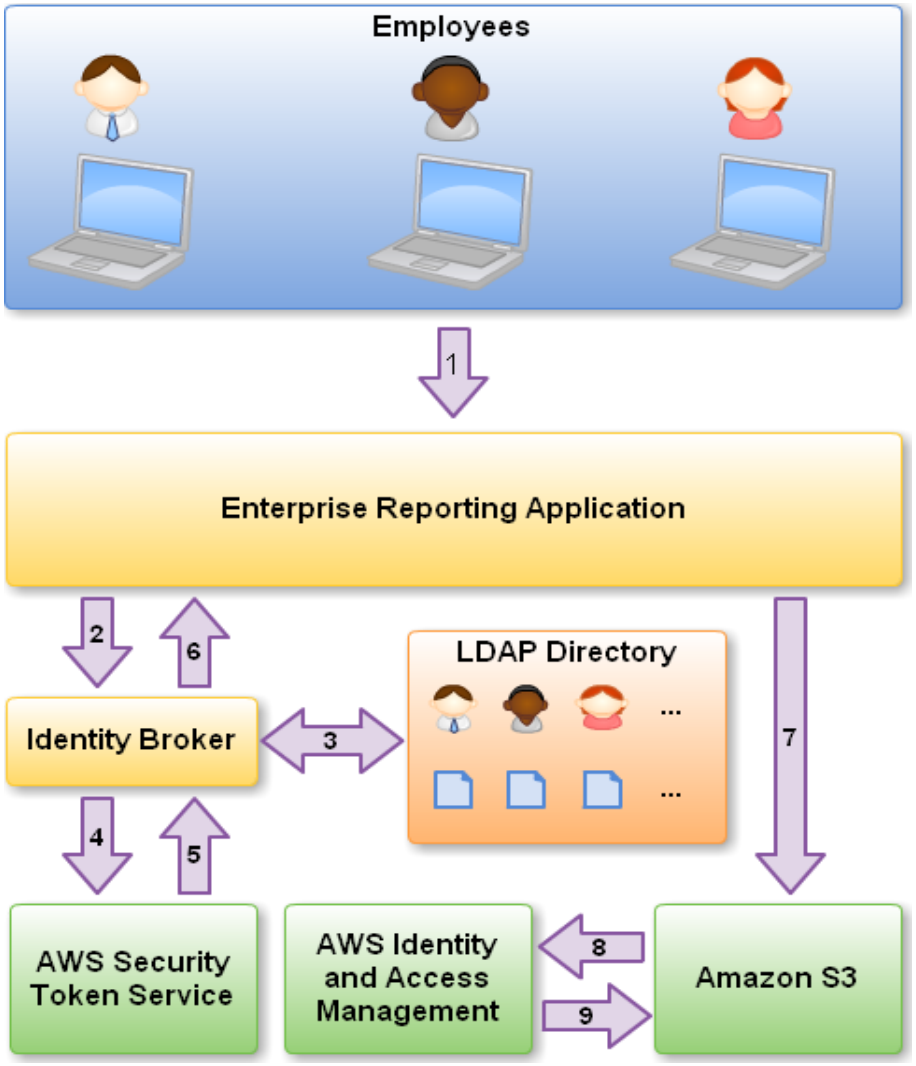


AWS Identity and Access Management

- Сервис IAM позволяет контролировать права доступа ко всем остальным сервисам AWS.
- Каждому IAM пользователю можно присвоить:
  - пару ключей
  - логин и пароль
  - пару сертификатов

AWS IAM

- С ключами и сертификатами пользователи могут иметь доступ к API и утилитам командной строки.
- С логином и паролем — в консоль, которая доступна лишь членам организации.



AWS IAM

IAM так же легко использовать для передачи прав на короткое время третьим лицам, например фрилансерам для настройки сервисов.

Ключи, сертификаты и пароли легко быстро отозвать, тем самым прекратив доступ к AWS.

Уровень средств доступа к сервисам

Доступ к Web-сервисам Amazon можно осуществлять с помощью:

- **Интерфейса командной строки**.
- **Консоли управления с Web-интерфейсом.**
- **Интегрированной среды разработки Eclipse** (AWS Toolkit for Eclipse)
- **Интерфейса прикладного программирования** (библиотеки для Java и .NET).

Управление AWS

Управление AWS осуществляется с помощью:

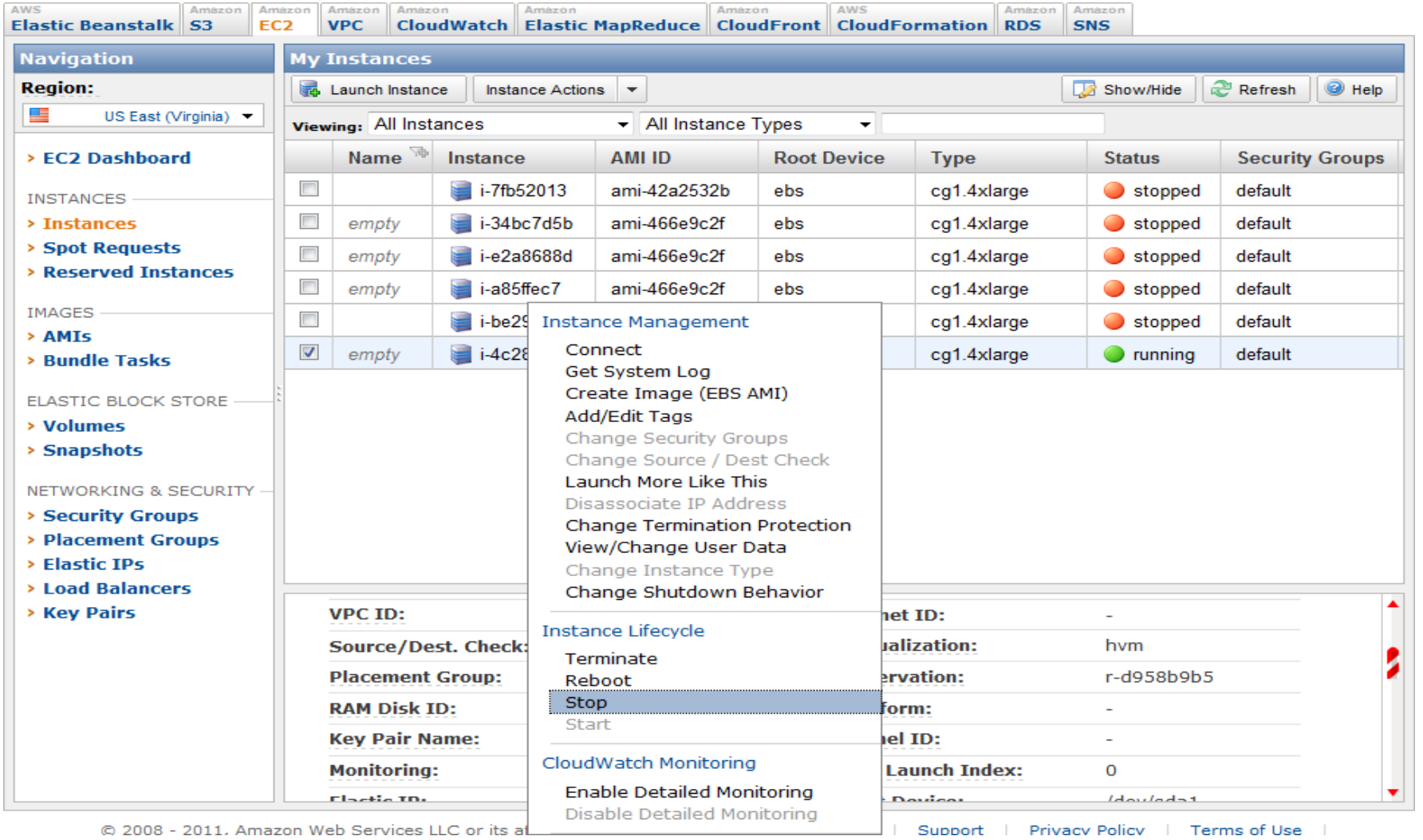
- **веб интерфейса (AWS console)**
- **Command Line Tools**.

В консоли собраны все сервисы AWS, но функциональность настройки несколько обрезана.

В командной строке можно более гибко настроить тот или иной сервис, так же доступны закрытые в консоли функции.

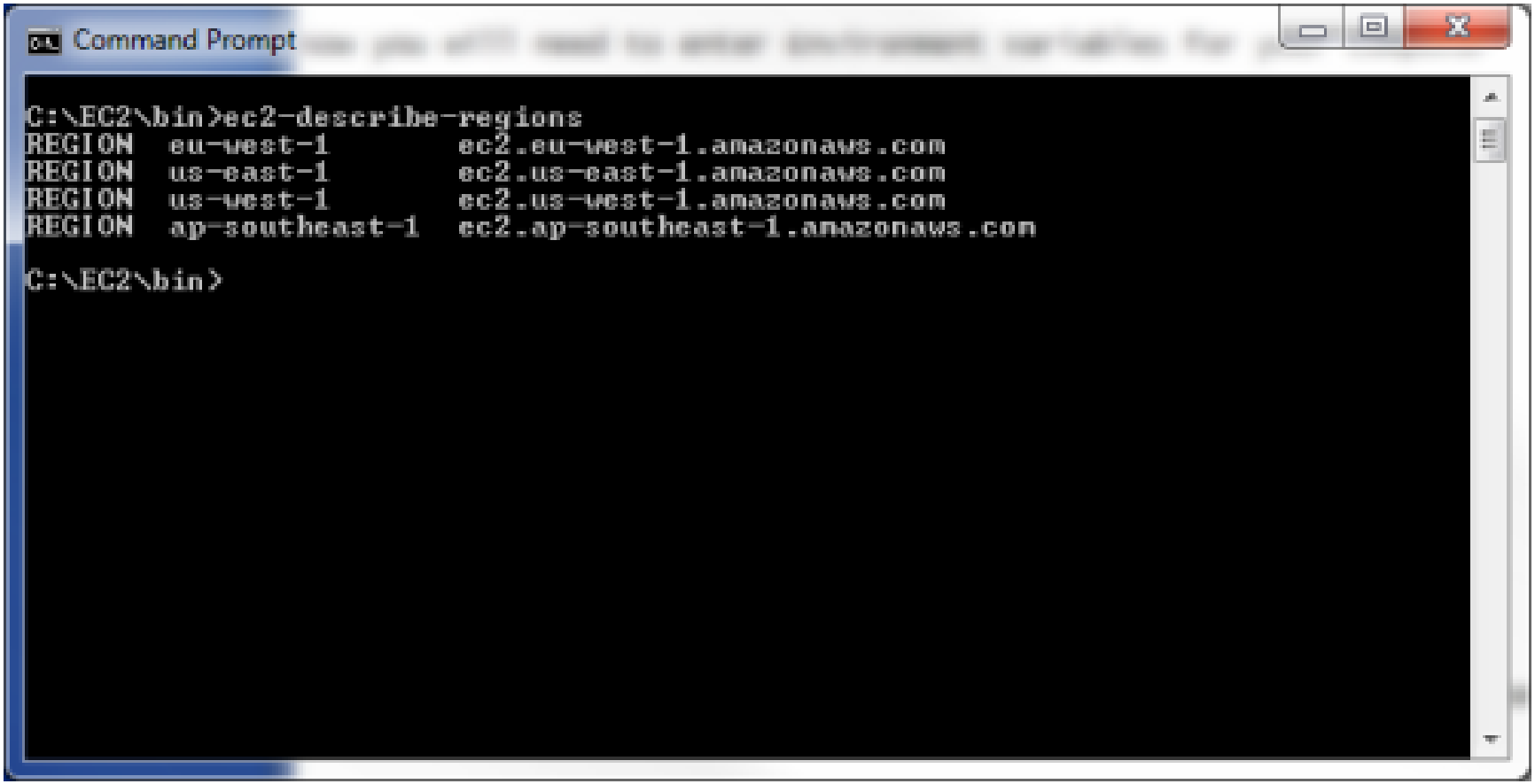
Управление AWS с помощью консоли

URL Web-консоли: **http://console.aws.amazon.com**



Управление AWS из командной строки

Надо скачать **AWS Command Line Tools** с сайта http://aws.amazon.com и инсталлировать их на свой компьютер.



Оплата за использование AWS

Оплата EC2 ведётся почасово, некоторые подсервисы, такие как EBS имеют помесячный биллинг.

Для каждого подсервиса есть свой отдельный биллинг по заведомо утверждённой цене в час или в месяц.

Цены на сервис Amazon EC2

	vCPU	ECU	Memory (GiB)	Instance Storage (GB)	Linux/UNIX Usage
General Purpose - Current Generation					
m3.xlarge	4	13	15	2 x 40 SSD	$0.495 per Hour
m3.2xlarge	8	26	30	2 x 80 SSD	$0.990 per Hour
General Purpose - Previous Generation					
m1.small	1	1	1.7	1 x 160	$0.065 per Hour
m1.medium	1	2	3.75	1 x 410	$0.130 per Hour
m1.large	2	4	7.5	2 x 420	$0.260 per Hour
m1.xlarge	4	8	15	4 x 420	$0.520 per Hour

Цены на сервис Amazon S3

Объем	Цена за Гб/Месяц
Первый 1Тб	$0.125
Последующие 49Тб	$0.110
Последующие 450Тб	$0.095
Последующие 500Тб	$0.090
Последующие 4000Тб	$0.080
Свыше 5000Тб	$0.055

Как сэкономить на оплате?

Так же у EC2 инстансов существует так называемая **резервация (Reservation)** — оплачивается сразу 3-4 месяца работы сервера, после чего, час работы сервера стоит в ~1,5 раза дешевле.

Резервации удобно использовать, если EC2 используется на постоянной основе.

Бесплатное использование AWS

- Компания Amazon предоставляет первый год пользования сервисом бесплатно, при условии, что вы не превысите лимитов сервиса.
- Это дает возможность бесплатно изучить AWS и протестировать свое приложение.

Бесплатный пакет AWS Free Usage Tier

EC2 (инстансы — виртуальные машины ОС)

- 750 часов использования виртуальной машины с Linux или Windows Server (613 Мб ОЗУ, 32- битная или 64-битная платформа)
- 750 часов Elastic Load Balancer плюс 15 Гб обработки трафика
- 30 Гб Amazon Elastic Block Storage, плюс 2 миллиона операций ввода/вывода и 1 Гб для хранения снэпшотов.
- 15 Гб трафика

Бесплатный пакет AWS Free Usage Tier (продолжение)

S3 (файловое хранилище)

- 5 Гб Amazon S3 стандартного хранилища, 20000 Get запросов и 2000 Put запросов

Relational Database Service (служба реляционных баз данных, RDS)

- 750 часов сервиса для запуска MySQL, Oracle BYOL или SQL Server
- 20 Гб хранилище базы данных
- 10 миллионов операций ввода/вывода
- 20 Гб хранилище для бекапов для автоматического резервного копирования вашей базы данных и возможностью создать снэпшот базы данных

Итоги

- AWS предоставляет все необходимое для развертывания и сопровождения Web-приложений в облаке.
- AWS представляет собой конструктор, из которого можно собрать сколь угодно сложную, распределенную сетевую инфраструктуру.