Amazon Web Services

Путь к сертификату архитектора

Привет!

Сергей Василенко.
Работал саппортом, админом, CTO, Тимлидом.
Получил AWS SAA этой весной и еще не успел забыть.

linkedin.com/in/svasylenko

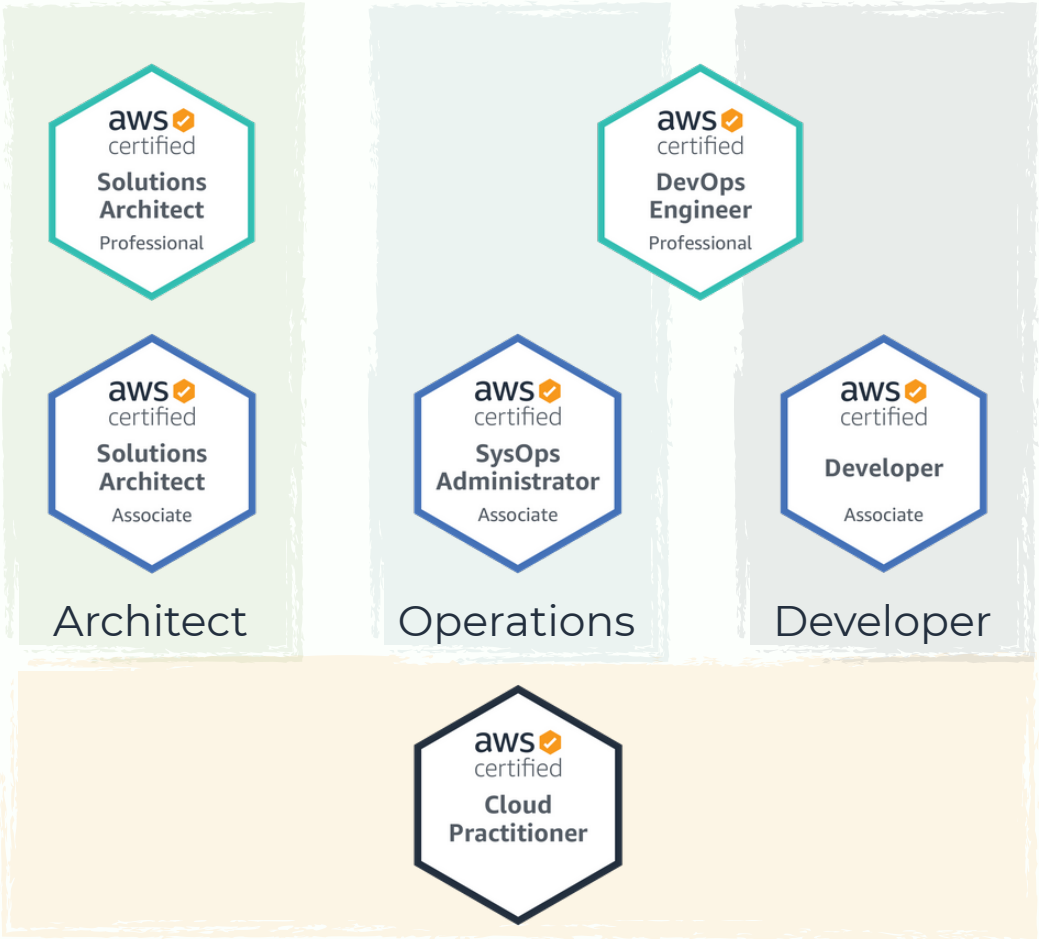
- Во-первых, это огромная и очень интересная платформа с 200+ сервисами
- Во-вторых, это лидер (по прежнему) рынка облачных вычислений == часто используется в проектах
- 😉 А еще сертификация AWS SAA входит в топ-3 списка Top-Paying IT Certifications 2020

Про сертификаты

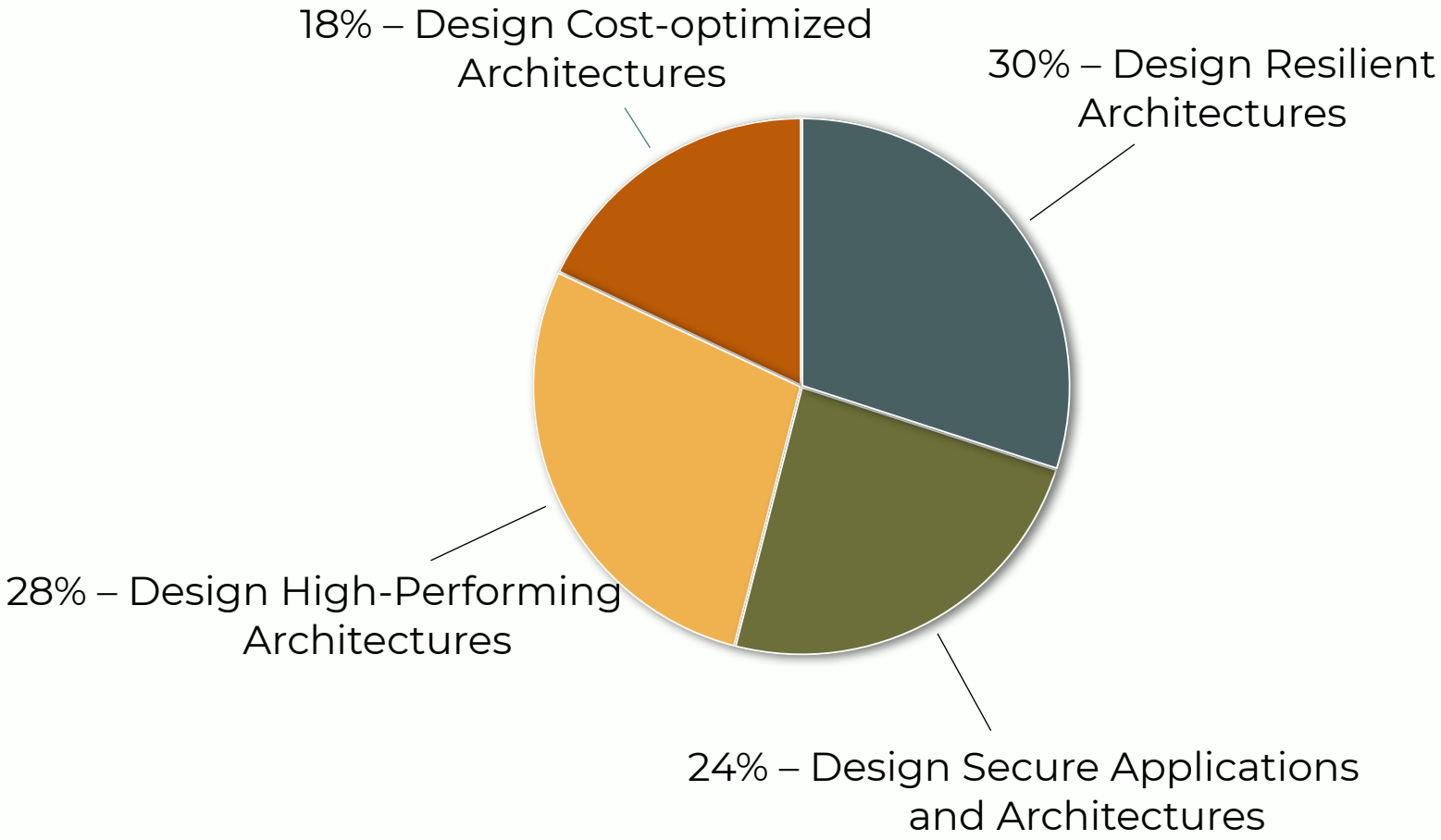
2 года комплексного опыта создания, управления, отладки решений

1 год опыта внедрения решений

6 месяцев опыта с основными сервисами



Состав экзамена



Сервисы AWS, представленные в экзамене


IAM


Kinesis

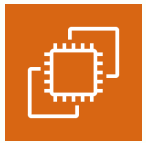

DynamoDB


Beanstalk


EBS


Macie


API Gateway


EC2


Auto Scaling


ELB


Aurora


EFS


SNS


VPC


CloudFront


Redshift


CloudWatch


RDS


SQS


ECS


Lambda


Elasticache


WAF

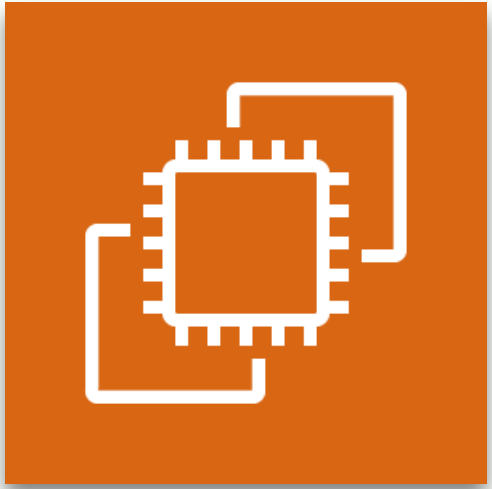

CloudFormation


S3


Cognito


KMS

Route53



Elastic Compute Cloud

Классификация и ценообразование

General Purpose: A.x, T.x, M.x

Compute Optimized: C.x

Memory Optimized: R.x, X.x

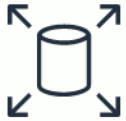
Accelerated Computing: P.x, G.x, F.x

Storage Optimized: I.x, D.x, H.x

On Demand

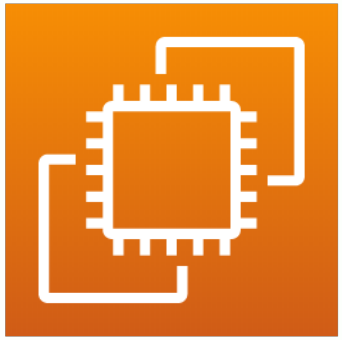
Spot instances

Savings Plans & Reserved Instances



Elastic Block Store

EBS Snapshot



EC2 Instance

Amazon Machine Image

Security Groups

Key Pairs

User Data

🤔

A company's application is running on Amazon EC2 instances in a single Region. In the event of a disaster, a solutions architect needs to ensure that the resources can also be deployed to a second Region.
Which combination of actions should the solutions architect take to accomplish this? [Select two]

A) Detach a volume on an EC2 instance, create snapshot and store it to Amazon S3.

B) Copy an AMI of an EC2 instance and specify a different Region for the destination.

C) Launch a new EC2 instance in a new Region and copy a volume from Amazon S3 to the new instance.

D) Launch a new EC2 instance from an AMI in a new Region.

E) Copy an EBS volume from Amazon S3 and launch an EC2 instance in the destination Region using that EBS volume.

🤔

A company's application is running on Amazon EC2 instances in a single Region. In the event of a disaster, a solutions architect needs to ensure that the resources can also be deployed to a second Region.
Which combination of actions should the solutions architect take to accomplish this? [Select two]

Технически реализуемо (почти), но не подходит

❌ A) Detach a volume on an EC2 instance, create snapshot and store it to Amazon S3.

✅ B) Copy an AMI of an EC2 instance and specify a different Region for the destination.

❌ C) Launch a new EC2 instance in a new Region, copy a snapshot from Amazon S3, and create EBS for the the new instance.

Вы не можете работать с snapshot в S3 напрямую

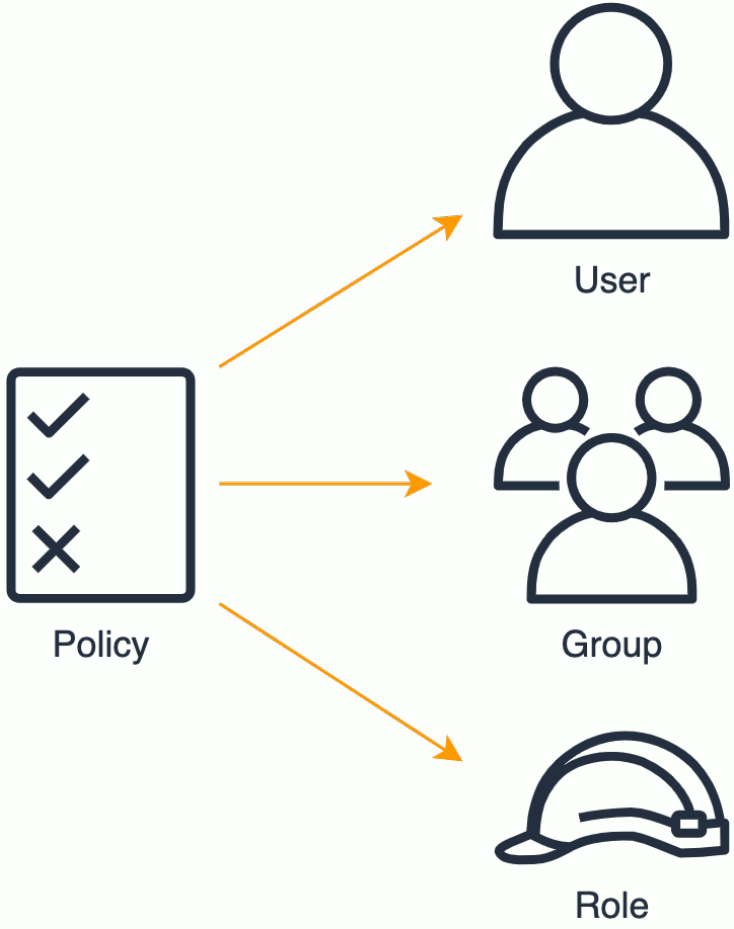
✅ D) Launch a new EC2 instance from an AMI in a new Region.

❌ E) Copy an EBS volume from Amazon S3 and launch an EC2 instance in the destination Region using that EBS volume.

В S3 хранятся snapshots,
вы не можете их явно копировать оттуда + AMI где?

Identity and Access Management

Основные компоненты



Идентичность и учетные данные, которые использует человек или приложение для взаимодействия с AWS.

Набор правил, определяющих разрешение или запрет на взаимодействие с ресурсами AWS.

Набор / коллекция из нескольких user. Все пользователи наследуют policy своей группы.

Сущность, определяющая набор привилегий, которую могут использовать user или другой AWS service

Особенности

Разрешение на доступ выдается явно
Запрещающее правило имеет приоритет над разрешающим

Permissions boundaries – политики, которые ограничивают IAM-сущность в правах, даже если ей назначена policy, которая превышает ограничение

Resource Access Manager – предоставление доступа другим AWS-аккаунтам к ограниченному набору ресурсов в своём аккаунте.

You are working in the media industry, and you have created a web application, hosted on EC2, where users will be able to upload photos they create to your website. This web application must be able to call the S3 API in order to be able to function. Where should you store your API credentials whilst maintaining the maximum level of security.

A) Get the API credentials using EC2 instances User Data.

B) Save the API credentials locally to each EC2 instance.

C) Save your API credentials as encrypted entry in Secrets Manager.

D) Don’t save your API credentials. Create IAM Role instead and assign to EC instance.

🤔

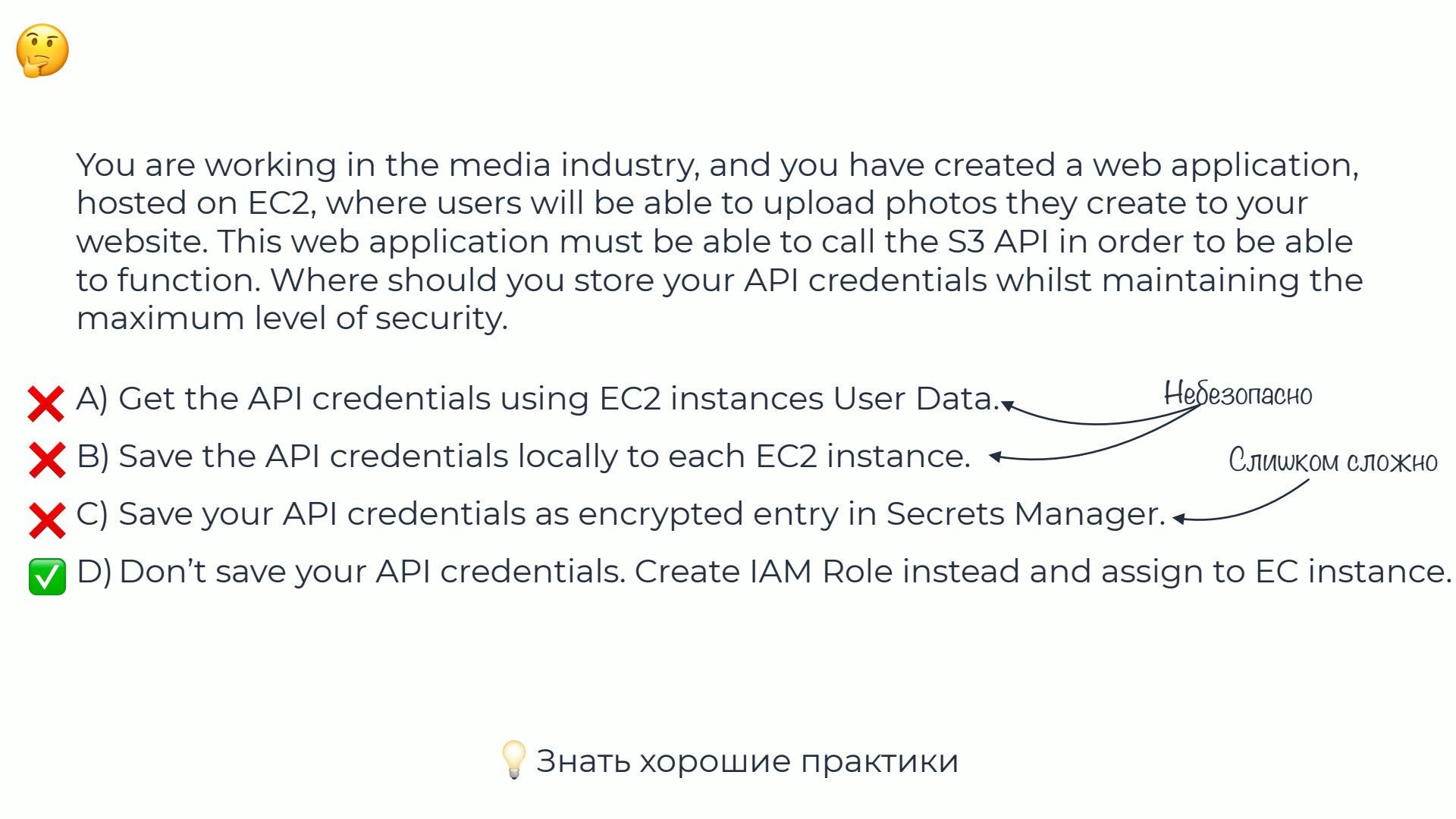
You are working in the media industry, and you have created a web application, hosted on EC2, where users will be able to upload photos they create to your website. This web application must be able to call the S3 API in order to be able to function. Where should you store your API credentials whilst maintaining the maximum level of security.

❌ A) Get the API credentials using EC2 instances User Data.

❌ B) Save the API credentials locally to each EC2 instance.

❌ C) Save your API credentials as encrypted entry in Secrets Manager.

✅ D) Don’t save your API credentials. Create IAM Role instead and assign to EC instance.



💡 Знать хорошие практики

Simple Storage Service

Основные компоненты

Bucket

Хранилище для объектов.
Любое количество и общий размер хранимых объектов
Версионирование и репликация
Политики и журналирование доступа, аналитика и метрики
Шифрование и запрет на изменение объектов
Автоматизация жизненного цикла объектов

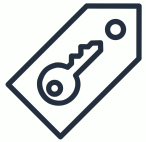
Основные компоненты

Bucket

Хранилище для объектов.
Любое количество и общий размер хранимых объектов
Версионирование и репликация
Политики и журналирование доступа, аналитика и метрики
Автоматизация жизненного цикла объектов

Object

Файл и набор метаданных, которые связаны с ним
Доступ через web интерфейс
Несколько режимов хранения (storage class)
Настройка доступа на уровне объекта
Multipart uploads для upload & byte-rage fetch для download



Key

Имя объекта – уникальный идентификатор внутри bucket

Databases

Базы данных

RDS

Microsoft SQL
MySQL
PostgreSQL
Oracle
MariaDB

Multi-AZ – disaster recovery
Read Replica – performance

Automated backups
Database snapshots
(из обоих можно создать новый RDS)

Aurora

MySQL
PostgreSQL

Может быть Serverless

Шифрование передачи и хранения данных

Базы данных

Elasticache

Memcached
Redis

In-memory cache: производительность для веб-приложений и баз данных

DynamoDB

NoSQL

- Serverless
- Распределена по 3 AZ
- Мультирегиональные таблицы (global tables)
- Контроль доступа через IAM
- Ускорение доступа через DAX
- Шифрование передачи и хранения данных

Базы данных

Redshift

PostgreSQL-based

Data Warehouse
- OLAP (аналитика bigdata)
- Petabytes-scaled
- Clusters (parallel processing)
- Шифрование передачи и хранения данных

Neptune

Graph database

Работа со связанными данными:
- сервисы рекомендаций
- системы выявления мошенничества
- обеспечение сетевой безопасности

🤔

Your company has a busy online store that consists of a two-tier architecture. The webservers are behind an Auto Scaling Group and the database is on a Large RDS MySQL instance. The performance for the last sale was very low during the peak load. You determined that the database was struggling to keep up with the number of reads that the store was generating. How can you successfully scale this environment out so as to increase the speed of the site? [Select 2]

A) Migrate the database to a MySQL Multi-AZ database.

B) Migrate the database to Aurora for better performance.

C) Create a read replica of the MySQL database.

D) Place the RDS instance behind Elasticache.

🤔

Your company has a busy online store that consists of a two-tier architecture. The webservers are behind an Auto Scaling Group and the database is on a Large RDS MySQL instance. The performance for the last sale was very low during the peak load. You determined that the database was struggling to keep up with the number of reads that the store was generating. How can you successfully scale this environment out so as to increase the speed of the site? [Select 2]

❌ A) Migrate the database to a MySQL Multi-AZ database.

Это не для performance

✅ B) Migrate the database to Aurora for better performance.

❌ C) Create a read replica of the MySQL database.

✅ D) Place the RDS instance behind Elasticache.

А тут надо код менять значительно

💡 Знать, как комбинировать сервисы

Route53

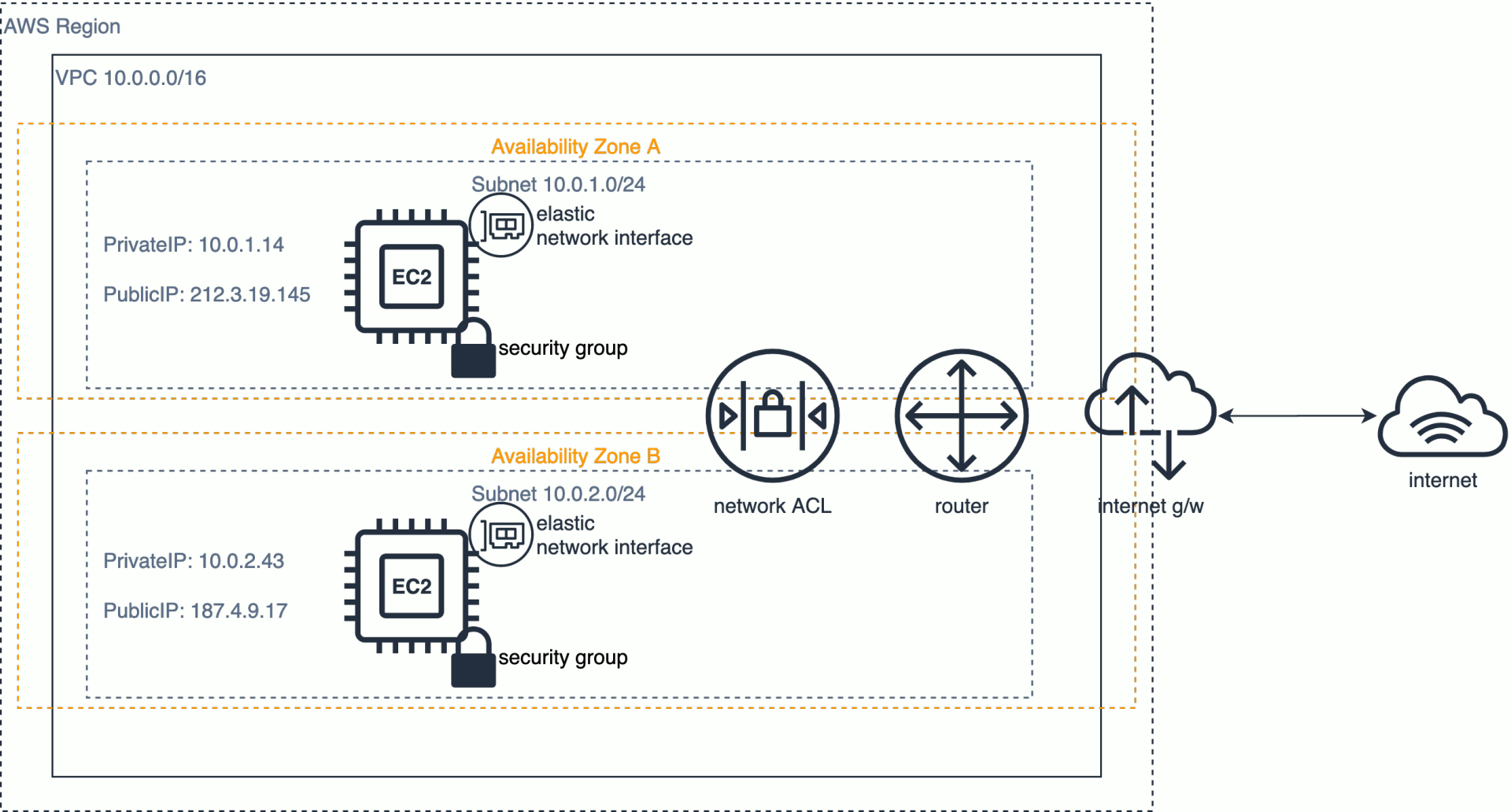
DNS

Alias vs CNAME records

Политики маршрутизации (routing policies):

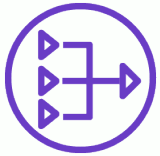
- Simple
- Weighted
- Latency-based
- Failover
- Geolocation & Geoproximity
- Multivalue answer with health check

VPC


AWS Region
VPC 10.0.0.0/16
Availability Zone A
Subnet 10.0.1.0/24
PrivateIP: 10.0.1.14
PublicIP: 212.3.19.145
EC2
elastic
network interface
security group
Availability Zone B
Subnet 10.0.2.0/24
PrivateIP: 10.0.2.43
PublicIP: 187.4.9.17
EC2
elastic
network interface
security group
network ACL
router
internet g/w
internet

Дополнительные сервисы

Flow Logs

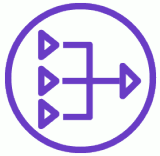


NAT Gateway

VPC Peering

Дополнительные сервисы

Flow Logs



NAT Gateway

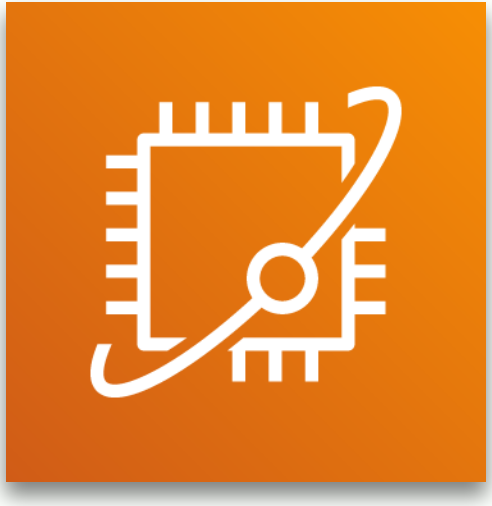
VPC Peering

Direct Connect

Global Accelerator

PrivateLink

Transit Gateway



HA Architecture

🤔

A customer relationship management (CRM) application runs on Amazon EC2 instances in multiple Availability Zones behind an Application Load Balancer. If one of these instances fails, what occurs?
[Select 1]

A) The load balancer will terminate the failed instance.

B) The load balancer will stop sending requests to the failed instance.

C) The load balancer will automatically replace the failed instance.

D) The load balancer will return 504 Gateway Timeout errors until the instance is replaced.

🤔

A customer relationship management (CRM) application runs on Amazon EC2 instances in multiple Availability Zones behind an Application Load Balancer. If one of these instances fails, what occurs?
[Select 1]

Это делает ASG

❌ A) The load balancer will terminate the failed instance.

✅ B) The load balancer will stop sending requests to the failed instance.

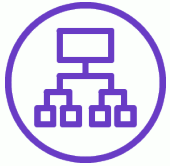
❌ C) The load balancer will automatically replace the failed instance.

❌ D) The load balancer will return 504 Gateway Timeout errors until the instance is replaced.

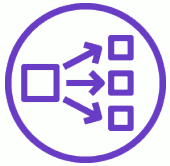
У вас много instances и коды ошибок могут быть разными

💡 Знать, как работают сервисы

Load Balancing



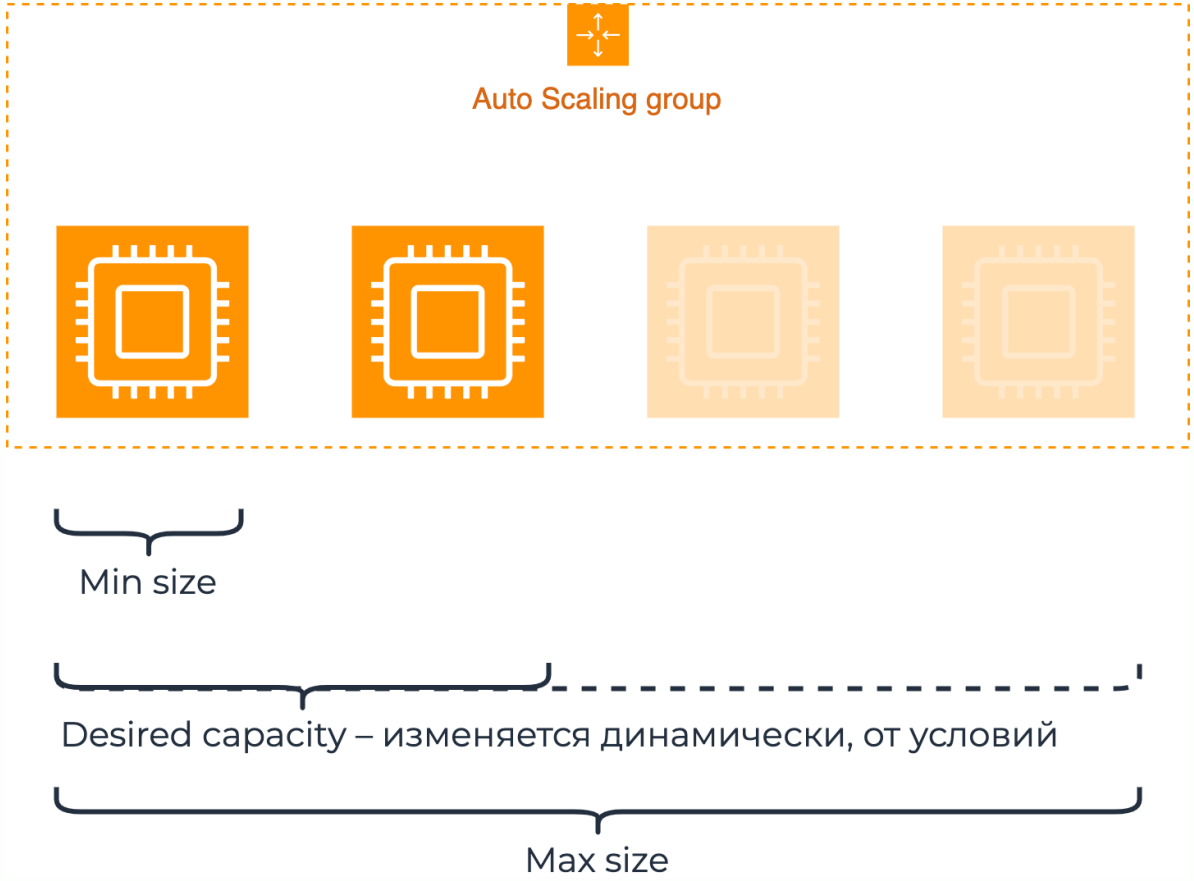
Application Load Balancer: маршрутизация запросов HTTP/HTTPS



Network Load Balancer: маршрутизация трафика TCP/UDP

Classic Load Balancer: HTTP, HTTPS, and TCP (старый, но дешевый)

Auto Scaling



Auto Scaling

Auto scaling group (ASG) – группа инстансов, объединённых для масштабирования и управления.

Launch template & Launch configuration – шаблоны конфигураций для EC2 инстансов, которые используются для их запуска в ASG. Определяет различные параметры, включая AMI, instance type, SG, Keypair и EBS’s.

Scaling policies – набор условий для масштабирования, например изменение потребления ресурсов или по расписанию.

Работа с приложениями

You work for a games development company that are re-architecting their production environment. They have decided to make all web servers stateless. Which of the following AWS services will help them achieve this goal? [Select 3]

A) RDS

B) EMR

C) DynamoDB

D) ElastiCache

E) Lambda

🤔

You work for a games development company that are re-architecting their production environment. They have decided to make all web servers stateless. Which of the following the AWS services will help them achieve this goal? [Select 3]

✅ A) RDS

❌ B) EMR ← Это не про webservers, это про big data processing

✅ C) DynamoDB

✅ D) ElastiCache

❌ E) Lambda ← Это server**less**, а у нас в вопросе web**servers**

💡 Знать, для чего нужны / что умеют сервисы

Simple Queue Service

Позволяет разделять (decouple) и распределять инфраструктуру (и приложение) на микросервисы

Pull-based – приложение должно обращаться к менеджеру очереди самостоятельно

Standard Queue:
- гарантия доставки сообщения в очередь хотя бы 1 раз (но может быть и больше одного раза)
- "почти неограниченное" количество транзакций в секунду

FIFO Queue:
- гарантия доставки сообщения ровно 1 раз
- ограничения на количество транзакций в секунду
- поддержка групп сообщений

Simple Notification Service

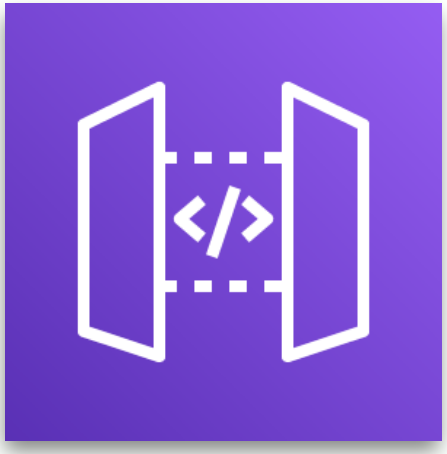
Позволяет разделять (decouple) и распределять инфраструктуру (и приложение) на микросервисы

Push-based – приложение/сервис ожидает сообщение от менеджера очереди

Получатели:
- сервисы AWS
- Mobile & web push
- SMS / Email
- HTTP endpoint

Позволяет логически группировать получателей по подпискам (topics)

Сервис для создания и управления API



API Gateway

- Автоматическое масштабирование
- Взаимодействие с другими сервисами AWS
- Балансировка между разными backends
- Правила доступа и throttling запросов
- Поддержка легирования и WAF
- Поддержка кеширования ответов backends

Сервис сбора, обработки и анализа потоков данных

Kinesis

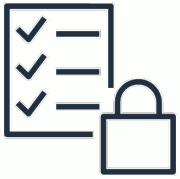
- Поддержка видео потоков
- Real-time прием данных от тысяч источников
- Real-time трансформация и сохранение данных
- Real-time анализ входящих данных
- Интеграция с EC2, Lambda, S3, Redshift, Elasticsearch, т.д.

Безопасность

Key Management Service

Web Application Firewall

Cloud Hardware Security Module



Security Groups

Parameter Store & Secrets Manager

Network ACL

Serverless

Сервис для выполнения кода

Lambda

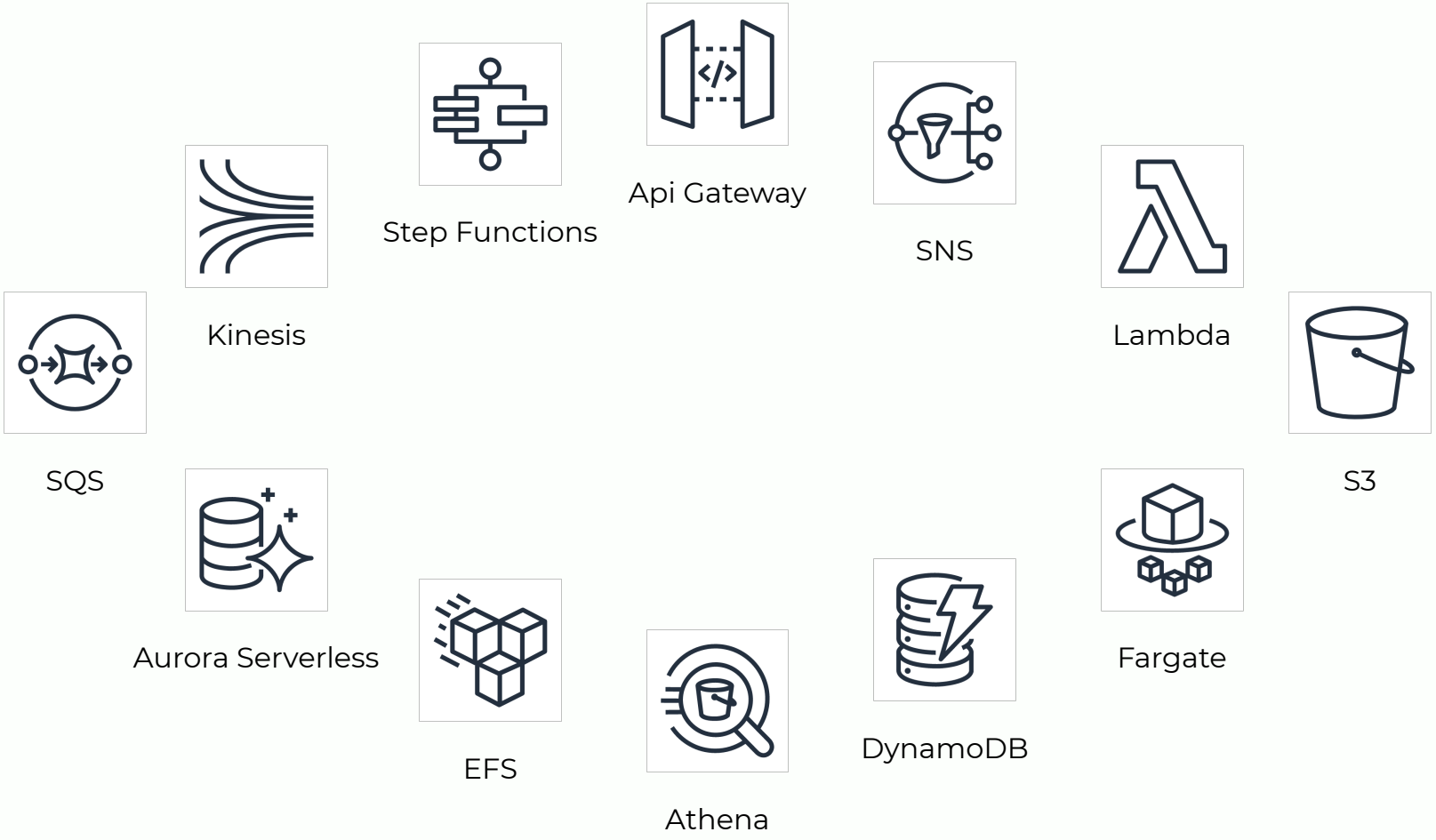
- Java, Go, PowerShell, Node.js, C#, Python, Ruby
- Ограниченное время работы
- Логирование и метрики
- Связь с другими сервисами AWS
- Поддержка триггеров
- Высокая масштабируемость/параллелизм

Оркестратор Docker контейнеров

Elastic
Container Service

- Поддержка кластеров
- EC2-based и Fargate (serverless)
- Различные настройки deployment
- Управление ресурсами
- Автоматическое масштабирование
- Бесплатный (но вы платите за ресурсы)

Что еще в AWS – serverless?



Подготовка

Как зарегистрироваться на экзамен

www.aws.training/Certification

Вам нужен аккаунт Amazon для авторизации.

Заполните ваш профиль. Имя/фамилия – как в загран.паспорте.
Не ошибайтесь в буквах! Исправление ошибки – несколько дней.

"Pearson VUE" – центр сертификации, который проводит экзамен on-line.

Цена – USD 150 (USD 20 – пробный).

Как проходит экзамен

⚠️ Offline в аккредитованных центрах – может быть недоступно (COVID)

Online с вашего устройства + webcam (за вами будут наблюдать)

65 вопросов, 130 минут

Выбор из нескольких вариантов: один или несколько правильных

aws.amazon.com/certification/faqs

home.pearsonvue.com/aws/onvue

Пример техники ответов

Вопросы

Фаза 1

В начале отвечайте эти

Фаза 2

Отвечайте эти

И

Определите эти

Фаза 3

Отвечайте эти

~~или угадывайте~~

Легкий Средний Сложный

Как готовиться

Курс от CloudGuru – 23.5 часа
acloud.guru/learn/aws-certified-solutions-architect-associate
Тот же курс на Udemy: udemy.com/course/aws-certified-solutions-architect-associate

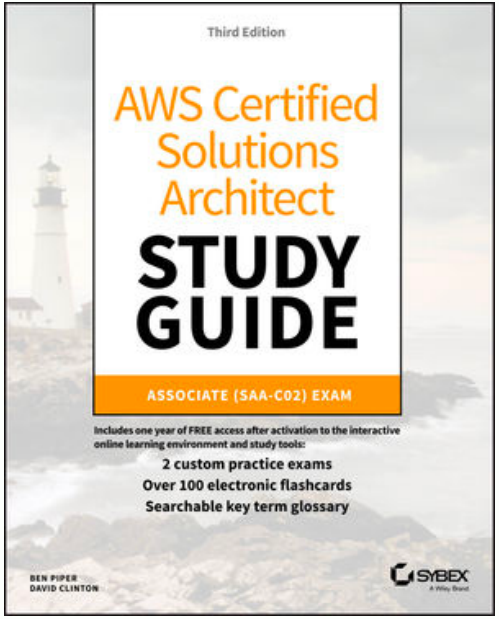
- ➕ Есть симулятор экзамена
- ➖ Практика в вашем собственном аккаунте AWS

Курс от LinuxAcademy – 57 часов (включая лабораторки)
linuxacademy.com/course/aws-certified-solutions-architect-associate-level

- ➕ Дают доступ в AWS для практики
- ➖ Нет симулятора экзамена


Советую конспектировать – лучше запомните

Как готовиться



AWS Certified Solutions Architect Study Guide: Associate SAA-C02 Exam, 3rd Edition
ISBN: 978-1-119-71308-1

Как готовиться

AWS Ramp-Up Guide: Architect

For AWS Cloud Architects, Solutions Architects and Engineers

aws training and certification

Updated July 2020

AWS Training and Certification has created this and other AWS Ramp-Up Guides to help build your knowledge of the AWS Cloud. Each expertly curated guide features free digital training, classroom courses, videos, whitepapers, certifications, and other information you're looking for. To enroll in training and certification exams, and track your progress, visit **aws.training** and set up a free account.

Learn the fundamentals of AWS Cloud

LEARNING RESOURCE	DURATION	TYPE
What is Cloud Computing?	10 minutes	Webpage »
Overview of AWS	2 hours	Whitepaper »
AWS Cloud Practitioner Essentials (Second Edition)	6+ hours	Digital Training »
Cloud Computing with AWS	10 minutes	Webpage »
AWS Glossary	30 minutes	Whitepaper »
Job Roles in the Cloud	30 minutes	Digital Training »

Step 1: Learn cloud architect fundamentals

LEARNING RESOURCE	DURATION	TYPE
Introduction to the AWS Well-Architected Framework	2 hours	Whitepaper »
AWS Well-Architected Framework - Information and resources	10 minutes	Webpage »
How AWS Pricing Works	45 minutes	Whitepaper »
AWS Technical Essentials	1 day	Classroom Training »
AWS Shared Responsibility Model	5 minutes	Digital Training »
AWS Well-Architected Training	1.5 hours	Digital Training »

1 ***Added to this guide June 2020. Duration times are estimated.**

AWS Ramp-Up Guide: Architect

For AWS Cloud Architects, Solutions Architects and Engineers

aws training and certification

Updated July 2020

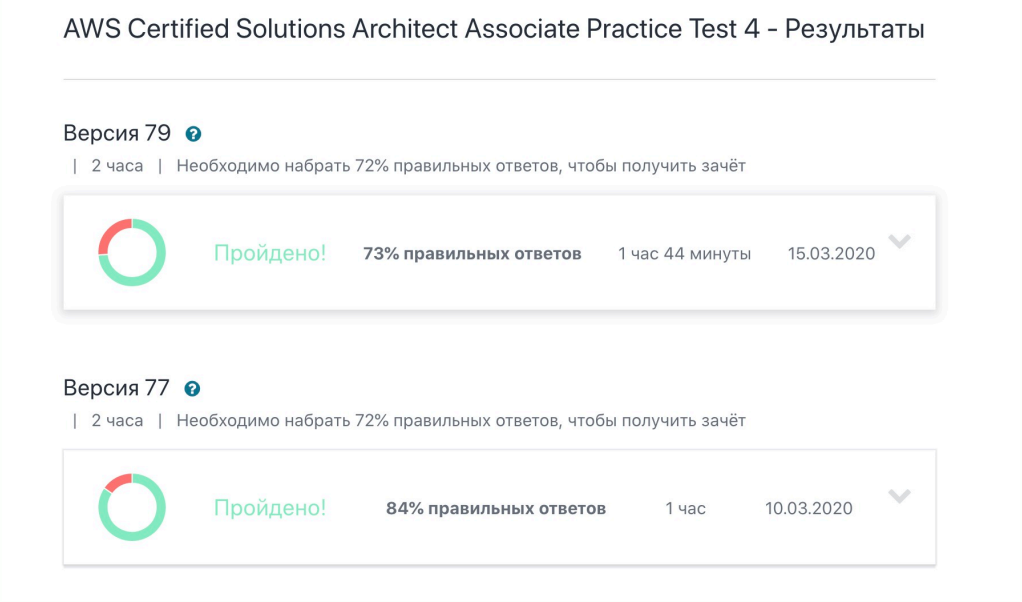
Step 2: Learn AWS Cloud Architecting concepts and best practices

LEARNING RESOURCE	DURATION	TYPE
Architecting on AWS	3 days	Classroom Training »
Advanced Architecting on AWS	3 days	Classroom Training »
OPTIONAL *Architecting on AWS - Accelerator*	5 days	Classroom Training »
Exam Readiness Intensive Workshop: AWS Certified Solutions Architect – Associate	5 days	Classroom Training »
AWS Architecture Center*	15 minutes	Webpage »

AWS Ramp-Up Guide: Architect

ссылка

Как готовиться



Симуляторы экзаменов, например:
udemy.com/course/aws-certified-solutions-architect-associate-amazon-practice-exams-saa-c02

portal.tutorialsdojo.com/courses/free-aws-certified-solutions-architect-associate-practice-exams-sampler

Как готовиться

⚠️ Must read: aws.amazon.com/faqs

Бесплатные лекции от AWS: www.aws.training/LearningLibrary

Exam Readiness: www.aws.training/Details/Curriculum?id=20685

Well-Architected Framework: aws.amazon.com/architecture/well-architected

Спасибо за внимание!