AWS Certifications

Quick documentation links:
AWS Whitepapers
AWS Documentation
How AWS Pricing Works
Overview of Amazon Web Services AWS Whitepaper

AWS Cloud Practitioner Essentials

Module 1: INTRODUCTION

Definitions

- **Cloud computing**="…on-demand delivery of IT resources over the internet with pay-as-you-go pricing."

Module 2: COMPUTE IN THE CLOUD

- Amazon **EC2 instance types** (5):
  - General purpose
  - Compute optimized
  - Memory optimized
  - Accelerated computing
  - Storage optimized
- Amazon **EC2 pricing**
  - On-Demand - …for short-term, irregular workloads that cannot be interrupted…
  - Savings Plan - …commitment to a consistent amount of usage (measured in $/hour) for a 1 or 3 year term….
  - Reserved Instances - …assigned to a specific Availability Zone, they provide a capacity reservation… either 1 year or 3 years…
  - Spot instances - …spare Amazon EC2 computing capacity; AWS can re-claim any time; 2 minute warning…
  - Dedicated Hosts

Note: …primary difference between the two programs is that Reserved Instances offer a discount against On-Demand pricing depending on committed utilization, whereas Savings Plans offer a discount depending on committed spend…. link

- Amazon EC2 **Auto Scaling** (2)
  - *dynamic* scaling - responds to changing demand
  - *predictive* scaling - automatically schedules…based on predicted demand
- Elastic Load Balancing (**ELB**) - *Regional* level
- **Messaging and queuing**
  - Note: **loosely coupled** - …an architecture where if one component fails, it is isolated and therefore won't cause cascading failures throughout the whole system…
  - Simple Queue Service (**SQS**) - a message queuing service; *…fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless application…*; data in message='payload'

  - Simple Notification Service (**SNS**) - a publish/subscribe service; *...messaging service for both application-to-application (A2A) and application-to-person (A2P) communication...*

- AWS **Lambda** - serverless compute service; run time <15min
- Amazon Elastic Container Service (Amazon **ECS**) - *...a container management system...*
- Amazon Elastic Kubernetes Service (Amazon **EKS**) - *... a fully managed service that you can use to run Kubernetes on AWS...*
- Amazon **Fargate** - *...serverless compute engine for containers. It works with both Amazon ECS and Amazon EKS...*
- Overview **Compute Services** link
  - Instances (Virtual machines)
  - Containers
  - Serverless
  - Edge and Hybrid

Module 3: GLOBAL INFRASTRUCTURE AND RELIABILITY

- **Region** - separate geographic area; consists of *two or more* Availability Zones (AZ)
- Sselection criteria for choosing a region (four business factors):
  - **Compliance** with data governance and legal requirements
  - **Proximity** to your customers
  - **Feature availability** - Available services within a Region
  - **Pricing** - each region has different price sheet
- **Availability zone** (**AZ**)
  - availability zone = one or many datacenters
  - ...as a best practice with AWS, we always recommend you run across at least two Availability Zones in a Region.....
  - many services are on a regional level already (e.g. ELB); regionally scoped service = meaning they run synchronously across multiple AZs
- **Edge locations**
  - CDN = Content Delivery Network
  - Amazon's CDN = Amazon **Cloudfront**
  - Cloudfront uses 'Edge locations'
  - Also run 'Amazon Route 53' - highly available and scalable cloud Domain Name System (DNS) web service
- **AWS Outposts** - where AWS will basically install a fully operational mini Region, right inside your own data center.
- Ways to interact with AWS services (3):
  - AWS Mangement Console
  - AWS Command line interface (CLI)
  - SDKs

- AWS **Elastic Beanstalk** - …service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python… link
- AWS **CloudFormation** - …infrastructure as code tool…

Module 4: NETWORKING

- Amazon Virtual Private Cloud (**VPC**) - logically isolated (network) section; essentially your own private network in AWS
  - **Internet gateway** - to allow public traffic from the internet to access your VPC
  - **Virtual private gateway** - enables you to establish a virtual private network (VPN) connection between your VPC and a private network
  - **AWS Direct Connect** - a service that enables establishing a dedicated private connection between your DC and a VPC; need to work with a Direct Connect partner *Note:* …a VPC can have multiple types of gateways attached …
- …only technical reason to use subnets in a VPC is to control access to the gateways.…public subnets have access to the internet gateway; the private subnets do not
- Network access control lists (**ACL**s) - virtual firewall that controls inbound and outbound traffic at the *subnet level.*
  - …Each AWS account includes a default network ACL…which allows all inbound and outbound traffic
  - *Note:* Network ACL = **stateless**
- **Security groups** - virtual firewall that controls inbound and outbound traffic for an Amazon EC2 instance = *EC 2 instance level*
  - *Note:* Security group = **stateful**
- Amazon Route 53 (DNS) routing policies:
  - latency-based routing
  - geolocation DNS
  - geoproximity
  - weighted round robin.

Module 5: STORAGE AND DATABASES

- EC2 instance - local storage called *instance store volumes*; volumes are physically attached to the (EC2-)host. **ephemeral!** (temporary)
- Amazon Elastic Block Store (Amazon **EBS**); virtual harddrives = EBS volumes
- EBS snapshot - incremental backup.
- Amazon Simple Storage Service (Amazon *S3*)
  - bject-level storage
  - 11 9s of durability
  - max. file size 5TB
  - supports cross-region replication
- S3 storage classes; two factors: (1) how often retrieve data; (2) how available data needs to be; min 3 AZs (*regional* service)
  - S3 Standard - data stored in at least 3 AZs
  - S3 Standard-Infrequent Access (S3 Standard-IA)
  - S3 One Zone-Infrequent Access (S3 One Zone-IA)

  - S3 Intelligent-Tiering
  - S3 Glacier
  - S3 Glacier Deep Archive

- Amazon Elastic File System (Amazon **EFS**) - fully managed elastic NFS file system; scalable.
  - regional service storing data within and across multiple Availability Zones (AZs)
  - Note: for **EFS** on-premises servers can access Amazon EFS using AWS Direct Connect.

Amazon EBS	Amazon EFS
Volumes EC2 instance attached	Multiple instances can read/write
AZ level resource; need be same AZ as EC2 instance	Regional resource
Volumes to not automatically scale	Automatically scales

- Amazon Relational Database Service (Amazon **RDS**) - managed service that enables you to run relational databases in the AWS Cloud.
  - **RDS** services includes: automated patching, backups, redundancy, failover, disaster recovery
  - supports cross-Region read replicas
  - Amazon **RDS** is available on *six database engines*
    - MySQL
    - PostgreSQL
    - MariaDB
    - Oracle
    - Microsoft SQL Server
    - Amazon **Aurora** - MySQL and PostgreSQL-compatible relational database built for the cloud (replicates six copies to three AZs; continuously backs up data to S3)
- Amazon **DynamoDB** - non-relational, NoSQL database; key-value and document database service; serverless.
- Amazon **Redshift** - data warehousing service (e.g. for big data analytics; BI solutions).
- AWS Database Migration Service (AWS **DMS**)
  - "…The source and target databases can be of the *same* type *or different* types…."
  - "…supports homogeneous migrations such as Oracle to Oracle, as well as heterogeneous migrations between different database platforms…"
- Additional database services
  - Amazon **DocumentDB** - document database service; MongoDB compatible.
  - Amazon **Neptune** - graph database service.
  - Amazon **Quantum Ledger Database** (Amazon *QLDB*) - ledger database service; immutable system of record
  - Amazon **Managed Blockchain**
  - Amazon **ElastiCache** - service adding caching layers on top db; supports two types of data stores: *Redis* and *Memcached*.
  - Amazon **DynamoDB Accelerator** - in-memory cache for DynamoDB; improving read-times.

Module 6: SECURITY

- **Shared responsibility model** - *AWS* controls security **of** the cloud and *customers* control security **in** the cloud
  - Customers: Security in the cloud
  - AWS: Security of the cloud
- AWS Identity and Access Management (**IAM**)
  - authentication and authorization as a service
  - identity federation
  - **root account user** = owner of the AWS account.
- **IAM users** - by default IAM user has zero permissions.
- **IAM policy** - a document that allows or denies permissions to AWS services and resources; JSON format; can apply to IAM users, groups, or roles.
  - `Action`: can list any AWS API call
  - `Resource`: list what AWS resource that specific API call is for.
- **IAM group** - is a collection of IAM users
- **IAM roles** - an identity that you can assume to gain temporary access to permissions.
  - Note: *When someone assumes an IAM role, they abandon all previous permissions that they had under a previous role and assume the permissions of the new role.*
- **AWS Organizations** - group accounts into organizational units (OUs) to make it easier to manage accounts
  - Centralized management
  - Consolidated billing - combine the usage across all accounts in the organization to share pricing discounts
  - Hierarchical groupings of accounts
  - AWS service and API actions access control
  - Service control policies (**SCP**s) - can be applied to an organization *root*, an *individual member account*, or an *OU*.
- **AWS Artifact** - a service that provides on-demand access to AWS security and compliance reports
  - Access AWS compliance reports on-demand.
  - Review, accept, and manage agreements with AWS.
- Customer Compliance Center link
- AWS will not automatically replicate data across regtions
- **DDos** attack - a deliberate attempt to make a website or application unavailable to users
  - *distributed* DDoS attack - multiple sources are used to start an attack
- **AWS Shield** - a service that protects applications against DDoS attacks
  - *Standard* - automatically protects all AWS customers at no cost.
  - *Advanced* - paid service; detailed attack diagnostics; detect and mitigate sophisticated DDoS attacks; integrates with CloudFront, Route 53, ELB, and AWS WAF.

- Additional security services:
  - AWS **Key Management Service** (AWS **KMS**)
  - AWS **WAF** - web application firewall.
  - Amazon **Inspector** - automated security assessment service for exposure, vulnerabilities, and deviations from best practices. EC2 agent available.
  - Amazon **GuardDuty** - intelligent threat detection for infrastructure and resources; analyzes continuous streams of metadata from your account, and network activity from CloudTrail events, VPC Flow Logs, and DNS logs.

Module 7: MONITORING AND ANALYTICS

- **Monitoring** - Oberving systems, collecting metrics, and then using data to make decision.

- Amazon **CloudWatch** - monitoring and observability service (for applications); CloudWatch alarms; integrated with SNS.

AWS CloudTrail

- AWS **CloudTrail** records API calls for account; recorded information includes:
  - identity of the API caller
  - time of the API call
  - source IP address of the API caller
  - etc
- Events are typically updated in CloudTrail within 15 minutes after an API call; can filter events.
- AWS **CloudTrail *Insights*** - optional feature; automatically detect unusual API activities

AWS Trusted Advisor

- AWS **Trusted Advisor** - online tool providing real time guidance following AWS best practices
- Some checks are free (7 core Trusted Advisor checks), others available depending on the level support plan. AWS Business Support and AWS Enterprise Support customers get access to all Trusted Advisor checks.
- Checks fall under five categories:
  - Cost optimization - e.g. eliminating unused and idle resources or by making commitments to reserved capacity.
  - Performance - e.g. checking service limits, ensuring taking advantage of provisioned throughput, and monitoring for overutilized instances.
  - Security - e.g. closing gaps, enabling various AWS security features, and examining your permissions.
  - Fault tolerance - e.g. increase availability + redundancy of AWS application by taking advantage of auto scaling, health checks, multi AZ, and backup capabilities.
  - Service limit - checks for service usage that is more than 80% of the service limit.
- AWS Basic Support and AWS Developer Support customers
- AWS Trusted Advisor states:
  - green - no problems.
  - orange - recommended investigations.
  - red - recommended actions.

Module 9: PRICING AND SUPPORT

- AWS **Free Tier**:
  - Always Free
  - 12 Months Free
  - Trials
- Pricing:
  - Pay for what you use.
  - Pay less when you reserve.
  - Pay less with volume-based discounts when you use more.
- **Consolidated billing**
- **AWS Budgets** - create budgets (monthly/quarterly/yearly) to plan your service usage, service costs, and instance reservations.
- **AWS Cost Explorer**
- **AWS Support plans**
  - Basic support - any customer
  - Developer tier - in addition: Email customer support (24h response)
  - Business tier - *all* Trusted Advisor functionality, direct phone support access
  - Enterprise support -
    - 15-minute SLA
    - Technical Account Manager (TAM)
    - AWS Infrastructure Event Management (IEM) e.g. support during the preparation and execution of planned events
- **AWS Marketplace** - digital catalog that includes thousands of software listings from independent software vendors.

Module 9: MIGRATION AND INNOVATION

- AWS Cloud Adoption Framework (AWS **CAF**) - organizes guidance into six areas of focus, called *Perspectives*:
- *Business perspectives*:
  - Business Perspective (1) - ensures that IT aligns with business needs and that IT investments link to key business results.
  - People Perspective (2) - development of an organization-wide change management strategy for successful cloud adoption.
  - Governance Perspectiv (3) - skills and processes to align IT strategy with business strategy.
- *Technical Perspectives*:
  - Platform Perspective (4) - principles and patterns for implementing new solutions on the cloud, and migrating on-premises workloads to the cloud.
  - Security Perspective (5) - ensures meeting security objectives for visibility, auditability, control, and agility.
  - Operations Perspective (6) - focuses on operating and recovering IT workloads to meet the requirements of your business stakeholders.
- **Migration strategies** - six of the most common migration strategies (six **R**s)
  - (1) Rehosting - lift-and-shift

  - (2) Replatforming - lift, tinker, and shift; Optimization is achieved without changing the core architecture of the application.
  - (3) Refactoring / re-architecting - …Refactoring is driven by a strong business need to add features, scale, or performance…
  - (4) Repurchasing - e.g. move from a traditional license to a software-as-a-service model.
  - (5) Retaining - keep applications that are critical for the business in the source environment.
  - (6) Retiring - removing applications that are no longer needed.
- AWS **Snow Family** - collection of physical devices that help to physically transport data in and out of AWS.
  - Example: dedicated 1Gbps network moved 1 PB of data in ~ 100 days.
- AWS Snow Family is composed of:
  - AWS Snowcone - holds up to 8TB of data.
  - AWS Snowball - either Edge Storage Optimized (80 TB) or Edge Compute Optimized (42 TB)
  - AWS Snowmobile - 100 Petabytes
- Innovation with AWS
  - VMWare Cloud on AWS
  - Amazon **SageMaker** - machine learning (ML)
  - Amazon Augmented AI (**A2I**) - provides built-in human review workflows for common machine learning use cases, such as content moderation and text extraction from documents.
  - Amazon Lex - core of Alexa
  - Amazon **Textract** - extract text
  - AWS **Deep Racer**
  - Internet of Things
  - AWS Ground Statsion - satelite time
  - etc

Module 10: THE CLOUD JOURNEY

- AWS **Well-Architected Framework**. Five Pillars:
  - **Operational Excellence** - gain insight; run and monitor systems to deliver business value and to continually improve supporting processes and procedures.
  - **Security** - protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies.
  - **Reliability** - recover from infrastructure or service disruptions; dynamically acquire resources to meet demand; mitigate disruptions.
  - **Performance Efficiency** - use computing resources efficiently to meet system requirements; informed decision.
  - **Cost Optimization** - run systems to deliver business value at the lowest price point.
- **Well-Architected Tool**
- Benefits of the AWS Cloud (6)
  - Trade upfront expense for variable expense. (1)
  - Benefit from massive economies of scale. (2)
  - Stop guessing capacity. (3)
  - Increase speed and agility. (4)
  - Stop spending money running and maintaining data centers. (5)
  - Go global in minutes. (6)

Module 11: AWS CERTIFIED CLOUD PRACTITIONER BASICS

- **Exam strategies**
  - Read the full question.
  - Predict the answer before reviewing the response options.
  - Eliminate incorrect response options.

Final Assessment

- Which Perspective of the AWS Cloud Adoption Framework focuses on recovering IT workloads to meet the requirements of your business stakeholders? *Operations Persepctive* (answered: Governance b/c of DR)

- Which statement best describes an Availability Zone? *A fully isolated portion of the AWS global infrastructure.*; "A separate geographical location with multiple locations that are isolated from each other" - This response option describes a Region.

- Which pillar of the AWS Well-Architected Framework focuses on using computing resources in ways that meet system requirements? *Performance Efficiency*

  - Performance Efficiency pillar focuses on using computing resources efficiently to meet system requirements, and to maintain that efficiency as demand changes and technologies evolve.
  - Operational Excellence pillar includes the ability to run workloads effectively, gain insights into their operations, and continuously improve supporting processes to deliver business value.
  - Security pillar focuses on protecting data, systems, and assets. It also focuses on using cloud technologies to improve the security of your workloads.
  - Reliability pillar focuses on the ability of a workload to consistently and correctly perform its intended functions.

- Which compute option reduces costs when you commit to a consistent amount of compute usage for a 1-year or 3-year term? Not: Reserved instances; Correct: Savings Plan

  - Amazon EC2 Savings Plans enable you to reduce your compute costs by committing to a consistent amount of compute usage for a 1-year or 3-year term.
  - Reserved Instances are a billing discount that is applied to the use of On-Demand Instances in your account. You can purchase Standard Reserved and Convertible Reserved Instances for a one-year or three-year term, and Scheduled Reserved Instances for a one-year term. *Unlike Savings Plans, Reserved Instances do not require you to commit to a consistent amount of compute usage over the duration of the contract.*

- Which AWS Trusted Advisor category includes checks for your service limits and overutilized instances? *Performance*

  - Performance - improve the performance of your services by providing recommendations for how to take advantage of provisioned throughput.
  - Security category includes checks that help you to review your permissions and identify which AWS security features to enable.
  - Cost Optimization category includes checks for unused or idle resources that could be eliminated and provide cost savings.
  - Fault Tolerance category includes checks to help you improve your applications' availability and redundancy.

- Which service enables you to build the workflows that are required for human review of machine learning predictions? Correct: Amazon A2I
- **Misc**
  - A network access control list (ACL) is a virtual firewall that controls inbound and outbound traffic at the subnet level.
  - A security group is a virtual firewall that controls inbound and outbound traffic for an Amazon EC2 instance.
  - S3 One Zone-IA is ideal for infrequently accessed data that does not require high availability.
  - A service that helps protect your applications against distributed denial-of-service (DDoS) attacks - *AWS Shield.*
  - AWS Direct Connect is a service that enables you to establish a dedicated private connection between your data center and VPC.
  - A virtual private gateway enables you to establish a VPN connection between your VPC and a private network, such as an on-prem DC.

AWS Certified Solutions Architect

Documentation to read

- AWS Documentation
- AWS FAQs
- AWS Whitepapers
  - Architecting for the Cloud: AWS Best Practices (Archived) (Archived)
    - *Successor:* AWS Well Architected Framework
  - AWS Security Best Practices
  - Overview of Amazon Web Services
  - AWS Storage Services Overview
  - AWS Well Architected Framework
  - Overview of Security Processes
- AWS Architecture Center
- AWS Answers

Read Whitepapers initially (top 3), study thoroughly when preparing for exam. Additional ones: bottom three; at a later stage but also fundamental.

Videos

- AWS Event Videos
- Suggested video: Another Day, Another Billion Packets