This document is for reviewing for the AWS Cloud Practitioner Exam (up to 4/2023)

Table of Contents

Foundations of Cloud Computing

Cloud Concepts

- Compute
- Networking
- Storage
- Analytics
- Development
- Security
- Databases

6 Advantages

- High availability, elasticity, agility, durability.
- CapEx vs OpEx.

3 Models

- IaaS (Infrastructure): underlying building blocks, web hosting.
- SaaS (Software): complete product.
- PaaS (Platform): used by developers, develop software without installation.
- DaaS (Desktop) *: Amazon WorkSpaces; cloud based virtual desktop.

Deployment Methods

- On-premises: private, high security, internal.
- Cloud: AWS public cloud.
- Hybrid: connected via **Direct Connect.**

Global Infrastructure

- Regions: Physical locations and fully isolated.
- Availability Zones (AZs): multiple within a region, high availability.
- Edge Locations: Used for cache **CloudFront.**

Technology

Management Console: Visibility of services on web

CLI (Command Line Interface): Same but through terminal

- Programmatic Access: CLI, SDK, Application Codes

Computing Services

EC2 (Elastic Cloud Compute): Rent and manage servers in the cloud.

- Virtual servers on physical servers.
- Use **AMI** to launch instances.
- Deploy applications directly to EC2.

- Deploy databases, web applications.
- Access via Management Console, SSH (Local Laptop), EIC, Systems Manager.

Pricing Plan

- On-demand: pay as you go, no contract.
- Spot: Unused EC2 capacity, only when available, save up to 90%
- Reserved: 1 or 3 years, requires capacity reservation, save up to 75% (54% for Reserved Convertible aka more flexibility)
- Dedicated hosts: physical server for you that is not share, own software license, save up to 70%.
- Savings Plan: compute usage, up to 72% discount, AWS Cost Explorer Saving Plan recommendations.

ELB (Elastic Load Balancing): Distribute traffic across multiple EC2 Instances

- **Classic:** Basic load balancing across multiple EC2 instances (request and connection level).
- **Application:** HTTP and HTTPS traffic.
- **Gateway:** Third-party virtual appliances.
- **Network:** Load of TCP, UDP, TLS; layer 4; routes traffic to targets within Amazon VPC.

Auto Scaling: add/replace EC2 instances across AZs based on needs, horizontal scaling.

AWS Lambda

- Let's you write code without managing server
- Scales automatically
- Serverless
- Real-time file processing
- Email notifications
- Backend business logic
- Supports popular programming languages.
- 15-minute time out (maximum)
- Pricing: duration, request counts, always free up to 1000000 calls monthly

Containers

- **AWS Fargate:** Serverless compute engine for containers, scales automatically
- **AWS LightSail:** Quickly launch all resources, small projects.
- **AWS Outpost:** On-premise needs, hybrid, access to cloud servers and APIs.
- **AWS Batch:** Process large workloads in small batches.

Storage Services

S3 (Simple Storage Service)

- Objects are stored in buckets.
- Access is granted through ACLs (access control list), bucket policies, or access point policies. S3 Access Logs to track access.

- Versioning: storing multiple variants in same bucket.
- Regional service but name is globally unique.
  - Cross-region replication set by users.
- Durability and Availability (objects are never lost, 11 9s; 99.99% availability)
- **S3 Standard**: general purpose, multiple AZs, low latency, frequently accessed data
- **S3 Intelligent Tiering:** Moves to most cost-effective storage class, data with unknown or changing access patterns.
- **S3 Standard In-frequent Access:** Accessed less frequently but require rapid access (milliseconds), long-lived data.
- **S3 One-Zone Infrequent Access:** Similar but only in 1 AZ, cheaper but less durability. Re-creatable data.
- **S3 Glacier:** Long-term backup data storage at very low cost. Takes longer data retrieval.
- **S3 Glacier Deep Archive:** Cheapest. 12/48hrs retrieval. Only access once or twice a year. Retaining data for compliance requirements.
- **S3 Outposts:** Data that needs to be kept local, demanding application performance needs. Provides object storage on-premises. Store data across multiple devices and servers.
- **S3 can be used for:** static websites (CloudFront for global deployment); data archive; analytics system (use with services like Redshift-data warehousing-and Athena-SQL); mobile applications.

EC2 Storage

- Host computer is divided into individual instances.
- Instances must have a root drive: EBS volume or instance store volumes.
- **EBS** are persistent, can stop/terminate or attach to a different instance.
- **Elastic Block Store (EBS):** storage system to attach volume to EC2 instances.
  - Data will persist even when EC2 instance is not running.
  - Can only be attached to one instance in the same AZ.
  - Tied to one AZ.
  - Quickly accessible, long-term data storage.
- **EC2 Instance Store:** Physically attached to EC2 host and cannot be removed.
  - Storage is temporary, lost when not running.
  - Faster with higher I/O speed (does not have to travel over network)
  - Temporary storage needs, data replicated across multiple instances.
- **Elastic File System (EFS):** Serverless network system for sharing files.
  - Only on Linux file system.
  - Accessible across different AZ in the same Region
  - More expensive than EBS.
  - Business-critical apps need shared directories, Lift-and-Shift on existing enterprise apps.
- **Storage Gateway:** Hybrid storage service.
  - Connect on-premises and cloud data.
  - Moving backups to the cloud, reducing costs, low latency access to data.
- **AWS Backup**: helps manage backup data with EC2, EBS, EFS, and more.
  - Backup plan that includes frequency and retention.

Content Delivery Network (CDN): deliver content efficiently based on geographic location.

- **Amazon CloudFront:** Global distribution with low latency.
    - Can restrict based on location.
    - CloudFront Origins: S3, ELB, domain name.
    - Speeds up delivery of static and dynamic web content.
    - Uses edge location to cache content.
    - If not cached, content is retrieved from origin request (S3, EC2 Instance, ELB)
    - **S3 Static Websites, Prevent Attacks (DDoS), IP Address Blocking.**
- **Amazon Global Accelerator:** Sends users through AWS Global Network.
    - Improves latency and availability of single-region applications, sends traffic through AWS Global Network infrastructure, 60% performance boosts.
    - Reroutes traffic to available regional endpoints.
- **S3 Transfer Acceleration:** Improves content uploads to and from S3 buckets.
    - Improves content uploads and downloads to and from S3 buckets.
    - Uses CF's globally distributed edge locations.
    - Fast transfer over long distances.
    - Global customers can upload to a central bucket.

Networking connects computers together in a secure manner using routers, firewalls, network management services.

- **Virtual Private Cloud (VPC):** allows you to create a secure private network in the cloud to launch your resources.
    - Private Virtual Network: subnets, security groups.
    - Launch EC2 instances inside VPC.
    - Isolate and protect resources.
    - Spans across AZs in a region.
    - **ACLs (Network Access Control List):** Ensures proper traffic into the subnet.
    - **Router and Route Table:** Define where network traffic is routed.
    - **Internet Gateway:** Allows public traffic to the internet from the VPC.
    - **VPC Peering:** Connect 2 VPCs to facilitate transfer of data in a secure manner through a peering connection.

Additional Networking

- **DNS (Domain Name Service)**
    - **Route53**: DNS, Health checks, routes users to applications, hybrid architecture.
- **Direct Connect**
    - On-premises to AWS, super-fast, large volume of data.
- **AWS Site-to-Site VPN**
    - Direct connect but over public internet
    - **Virtual Private Gateway** (AWS -> On-premises)
    - **Customer Gateway** (On-premises -> AWS)
- **API Gateway** – Manage and build APIs
    - **API:** share data between systems

        - Integrated with servers like Lambda

Databases

- **RDS, Aurora** (Relational)
    - **Aurora: MySQL, PostgreSQL**
- **DynamoDB** (Non-relational, serverless, scales).
- **Neptune** (graph-based) – good for social media connections.
- **DocumentDB** is document-based linked to MongoDB, non-relational.
- **ElastiCache** is memory based and can be lost but good for high usage.

DMS (Database Migration Service) and **SMS** (Server Migration Service)

- **DMS** (different types of databases to the cloud)
- **SMS** (customers moving from on-premises to cloud)
    - **Snow Family** (Physical data transfer service)
        - **Snowcone** – 3 terabytes
        - **Snowball** – petabyte, cheaper
            - **Snowball Edge** supports EC2 and Lambda and is used when disconnected or in a remote environment.
        - **Snowmobile** – multi-peta, loaded to S3.
- **DataSync**
    - Transfer data online from on-premises to **S3** or **EFS (Elastic File System)**
    - Uses **Direct Connect** or internet.
    - Replicate data across region and account.

Analytics Services

- **Data Warehouse**, used for querying, analytics, and business intelligence tools.
    - **RedShift,** high speed and efficient, exabyte-scale (massive)
        - Data consolidation
- **Athena** is an SQL service for **S3.**
    - Pay-per-query, considered serverless.
- **Glue** is an ETL service to prepare and load data.
- **Kinesis** allows real time analysis of data, videos, and logs.
- **Elastic MapReduce** is for large amounts of data to process big data.
    - Analyse data using Hadoop.
    - Works with big data frameworks.
- **Data Pipeline** helps move data between compute and storage services running either on AWS or On-premises.
    - Move data based on intervals or conditions, sends notifications on success of failure.
- **QuickSight** is an interactive dashboard to visualize data.

Machine Learning

- **Rekognition:** recognizes image and video features.
- **Comprehension:** recognizes insights within texts for analytical purposes.

- **Polly:** Turn text into speech.
- **SageMaker:** build, train, and test machine learning models; deep learning AMIs.
- **Translate:** translate between languages.
- **Lex:** Used by Alexa; conversational interface.

Development

- **Cloud9:** IDE (Integrated Development Environment); web browser for development.
- **CodeCommit:** Private repository; similar to GitHub.
- **CodeBuild:** Used to prototype and test code. **CI/CD** (Continuous integration and delivery).
- **CodeDeploy:** Compute in cloud or on premises; deployment of code; maintain application uptime.
- **CodePipeline:** Integrates with CodeCommit/Build/Deploy to automate software release.
- **CodeStar:** For collaboration; comes with issue tracking dashboard.
- **Xray:** Debug and analyse production application; map app components; view E2E releases.
- **CodeWhisperer*:** ChatGpt for programming.

Deployment and Infrastructure Management

- **CloudFormation:** repeatable, allows you to provision AWS resources using **IaC (Infrastructure as Code)**
- **Elastic Beanstalk:** deploy applications to the AWS Cloud, handles capacity
- **OpsWorks:** deploy applications on-premises (and EC2 instances on AWS cloud); automate using Chef or Puppet.

Messaging and Integration Services

- **SQS (Simple Queue Service)**
  - Component to component queueing for loose coupling.
  - FIFO (First In First Out) order.
- **SNS (Simple Notification Service)**
  - Send email/text; works with CloudWatch for alarms.
- **SES (Simple Email Service)**
  - Send emails in HTML format from applications; good for marketing or adverts!

Auditing, Logging, Monitoring

- **CloudWatch:** monitors EC2 instances to notify when certain events occur; collects metrics, detects anomalies, set alarms.
- **CloudTrail:** logs user activity accessed through management console and programmatic access (SDK and CLI); detect unusual activity.
  - Username, event time and name, IP address, region, access key, and error code.

Security and Compliance

Shared Responsibility Model

- AWS is responsible for security OF the cloud.
  - Global infrastructure, networking components, building security, software.
  - Patching the HOST OS.
- Customers are responsible for security IN the cloud.
  - Application data, security configuration, patching, IAM, network traffic, installed software.
  - Patching the GUEST OS.

6 Pillars of a Well-Architected Framework

- Operational Excellence, Security, Reliability, Cost Optimization, Performance Efficiency, Sustainability

IAM (Identity Access Management)

- Who can access (authentication) and what they can access (authorization).
  - **Least Privilege Principle**
- Identity: who? Root, individual, group, roles. Applications can also be users.
- Access: controlled through policies in JSON format.
- Enable MFA (Multi-factor Authentication).
- Provides downloadable credential report.
- Role vs Group: Role is an identity you can assume for temporary access; Group is a collection of IAM users that a policy can be assigned to.

Application Security Service

- **Software Based Security Tools**
  - **WAF (Web Application Firewall)** is used to protect again SQL injection and cross-site scripting, to block again common attack patterns.
  - **Shield** is used to protect against **DDoS (Distributed Denail of Service)** attacks.
    - **Standard:** Free protection.
    - **Advanced:** Enhanced protection. 24/7 access to AWS expert.
  - **Macie** uses machine learning to uncover personally identifiable information (PII) stored on S3 (such as credit card numbers, social security, etc.)
- **Additional Services**
  - **Config**: detect changes in preferred software configurations.
  - **GuardDuty**: uses ML to detect unauthorized behaviours.
    - Build in detection for EC2, S3, IAM.
    - Automated remediation via CloudWatch events and AWS Lambda.
  - **Inspector**: built in EC2 to inspect vulnerabilities.
  - **Artifact:** repository for security and compliance report (non-specific to accounts).

Secrets Management Service

- **KMS (Key Management Service)** generates keys managed by AWS.
- **CloudHSM (Hardware Security Module)** generates key managed by customers.

    - i.e. used to meet compliance requirements.
- **Secrets Manager** manages and retrieves secrets and encrypts secrets at rest.
    - Integrated with RedShift, documentDB, RDS.

Pricing, Billing, Governance

Pricing Services

- **TCO (Total Cost of Ownership)** is the financial estimate for cost.
    - **Pricing Calculator** to estimate.
    - Reduced via 3 following ways:
        - Minimize CapEx, Utilise Reserved Instances, Right Size Resources.
    - **Application Discovery Service** is used to plan migration with AWS Cloud.
- **EC2 Pricing**
    - On-demand
    - Savings Plan (1/3 years)
    - Reserved Instances
    - Spot Instances
    - Dedicated Hosts
- **Lambda Pricing**
    - Per use (free up to 1000000/month)
    - Code execution time
- **S3 Pricing**
    - Storage type (i.e. standard, glacier)
    - Object size and numbers
    - Outbound data transferred.
    - Requests and data retrieval.
- **RDS Pricing**
    - Running clock hours.
    - Type of database
    - Storage.
    - Purchase type (on-demand/reserved).
    - Database count.
    - API requests and calls.
    - Deployment type (single vs multiple AZs)
    - Outbound data transfer.

Billing Services

- **Budgets** alerts users when cost exceeds a defined threshold via email or SNS.
- **Cost and Usage** is a comprehensive report on cost and usage; download via S3.
- **CostExplorer** is used to visualize the cost of AWS service for past and future forecasts.
- **Cost Allocation Tags** are useful to track spending.

Governance Services

- **Organizations** centrally manage multiple AWS accounts under one.
  - **SCP (Service Control Policies)** is used as permission for everyone to follow.
  - **Three benefits:**
    - **Consolidated Billing.**
    - **Cost Savings** via shared usage.
    - **Account Governance** (create and manage AWS accounts)
- **Control Tower** ensures account conforms to company made policies.
  - Integrated with Organizations; contains dashboard.
- **SystemsManager**
  - Visibility and control over AWS resources
  - Patch and run commands on EC2 and RDS instances automatically.
- **TrustedAdviser** checks account and recommends better practices.
- **LicenseManager** manages software license for on-premises and AWS.
- **CertificateManager** provision SSL/TLS certificates (free certs.)

Management Services

- **Managed Service** is used to manage infrastructure, reduce operational risks, and augment your stuff.
- **Professional Service** helps with the migration to cloud for enterprise level.
  - Propose, Architect, Implement Solutions
- **AWS Partner Network (APN)** is a global network for consulting containing approved vendors.
- **Marketplace** is a digital catalogue for 3rd party solutions
- **Personal Health Dashboard** is used to alert events and trouble shoot

Support Plans

- **Basic**
  - 24/7 email
- **Developer**
  - 1 primary contact, business hours email <24hrs
- **Business**
  - All ticket types, unlimited contacts, 24/7 email, phone, chat.
- **Enterprise**
  - Technical Accent Manager, extremely fast response time.
- **Ticket Types**
  - Account and billing, service limits, technical support (business and enterprise)

LINKS

https://pluralsight.visme.co/view/mxz10wwn-s01-l00-table-of-contents