AWS Cloud Practitioner Notes 👩‍💻🚀

Simple Queue Service (SQS)

- [ ] Send, store, and retrieve messages between software components (distributed components distributed components of an application)
- [ ] microservices (decoupled)

Simple Notification Service (SNS)

- [ ] Send out notifications / messages to end users
    - [ ] natively supports Java, Go, Power shell, Node.js, AWS Lambda c#, Python, Ruby
- [ ] run code w/o managing servers (serverless)
    - [ ] provides a Runtime API which allows customers to use any additional programming language
- [ ] Lambda function
    - [ ] Run code under 15 mins
    - [ ] Automatically scalable

Containers

- [ ] Package application codes and dependencies into a single object
- [ ] Run on top of instances (i.e. host is an EC2 instance)
- [ ] Container Orchestration : help deploy, manage and scale containerized applications
- [ ] cluster: contains + EC2 instance

Elastic Container Service (ECS)

- [ ] highly scalable, high-performance Container management system that enables to run and scale containerized applications on AWS
    - [ ] Support Docker containers
    - [ ] API calls to launch /stop Docker-enabled apps
    - [ ] ECS has 2 modes: i. Fargate (serverless) ii.EC2 launch

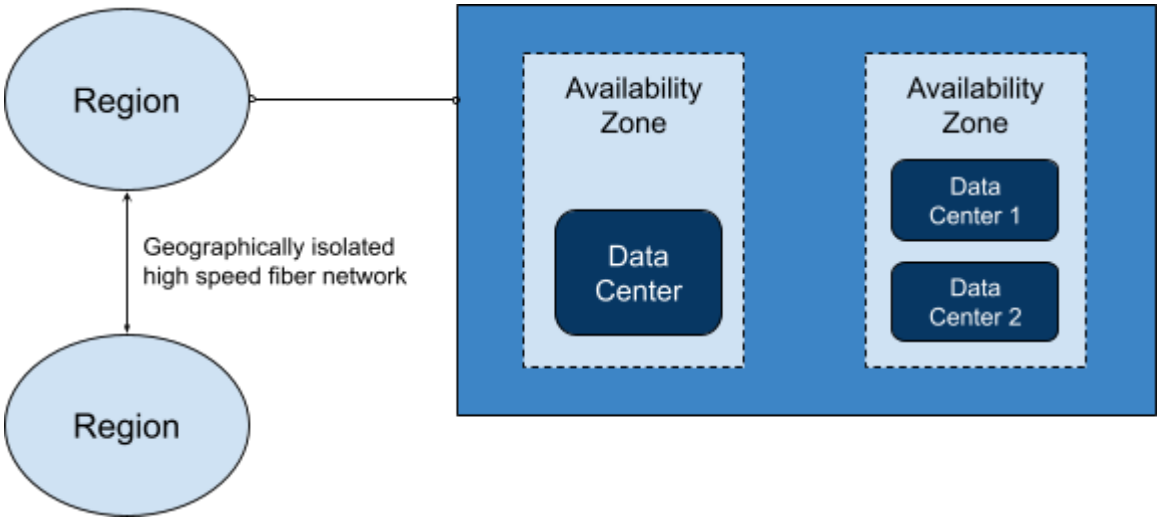
Elastic kubernetes Service (EKS)

- [ ] fully managed service that Kubernetes on AWS

AWS Fargate

- [ ] a serverless engine for containers
- [ ] works w/ both ECS and EKS

Global Infrastructure



Edge Locations

- ☐ a site that Amazon CloudFront uses to store cached copies of your content closer to your customers for faster delivery
  - ☐ retrieves the file from the cache in the edge location and delivers files (Content Delivery Networks, CDNS)
- ☐ edge locations are separated from regions
  - ☐ more availability zones than regions, more edge locations than availability zones
- ☐ Global Accelerator: improve performance for global Apps by routing end-user requests to the closest AWS region

Domain Name Service (DNS)

- ☐ help direct customers to the correct web locations w/ reliably low latency (aka. Route 53)

AWS Outposts

- ☐ fully operational mini Region inside customer's own data center
- ☐ customers can use Outpost can run AWS services locally

AWS Elastic Beanstalk

- ☐ i. Application container; ii. Deploy & scale web applications and services
- ☐ AWS environment management tool (provide code and configuration settings)
  - ☐ Adjust capacity
  - ☐ Load balancing
  - ☐ Automatic scaling
  - ☐ Application health monitoring

AWS Cloud Formation

- ☐ Environment tool which treats infrastructure as code
- ☐ cloudFormation template: define a variety of AWS resources in a declarative way using JSON or YAML text-based document

- [ ] Not limited to EC2-based solutions

Virtual Private Cloud (VPC)

- [ ] a network service that can be used to establish boundaries around your AWS resources
    - [ ] subnet: separate areas that are used to group together resources

Internet Gateway

- [ ] allow public traffic from the internet to access your VPC

Virtual Private Gateway

- [ ] allow to create a VPN connection between a private network
    - [ ] client VPN: users anywhere <~> AWS / on-premise network
    - [ ] site-to-site VPN: premises network <~> AWS
- [ ] encrypts/protects your internet traffic from all other requests

Direct Connect

- [ ] enable to establish a dedicated private connection between your data Center and a VPC

Network access Control Lists (ACLS)

- [ ] a virtual firewall traffic at the that controls inbound and outbound traffic at the subnet level
- [ ] an account's default network ACL allows ALL inbound and outbound traffic (allow & deny rule)
- [ ] Perform stateless packet filtering: remember NOTHING and check packets that cross subnet border each way

Security Groups

- [ ] a virtual firewall that controls inbound and outbound traffic for an EC2 instance
- [ ] By default, it does NOT allow any traffic into the instance (allow rule ONLY)
- [ ] Perform stateful packet filtering: remember previous decision made for incoming packets
    - [ ] ALL OUTBOUND traffic is allowed from a security group

Domain Name System (BNS) Resolution

- [ ] the process of translating a domain name to an IP address

Route 53

- [ ] route / connect user requests to infrastructure running in AWS
- [ ] manage the DNS records for domain names
    - [ ] register new domain names directly in Route 53

Elastic Block Store (EBS)

- [ ] provides block-level storage volumes that can be used with EC2 instances.
- [ ] EBS Volume persists between starts and stops of an EC2 instance

- ☐ virtual hard drive attached to EC2, which is separate from the local instance store volume → NOT directly tied to the host of the EC2 running on

Elastic Load Balancer (ELB)

- ☐ a service that distributes incoming traffic across multiple targets, such as EC2 instances
  - ☐ Application LB: HTTP / HTTPS
  - ☐ Netwrok LB: TCP, UDP
  - ☐ Gateway LB: 3rd-party virtual apps
  - ☐ Classic LB: apps within EC2
- ☐ monitor the health & performance of applications real-time

Auto Scaling

- ☐ a service that monitors applications and automatically adds / removes capacity from resource groups in response to changing demands

EBS Snapshot

- ☐ an incremental backup of EBS volumes → only backup the data that has been changed since the most recent snapshot was saved

Simple Storage Service (S3)

- ☐ a service provides object-level storage, which stores data as objects in buckets
- ☐ S3 storage classes: https://aws.amazon.com/s3/storage-classes/

EBS vs. S3

- ☐ S3 is web enabled every object has a URL that you can control access rights
- ☐ S3 is regionally distributed and serverless
- ☐ objects storage treats any files as a complete, discrete object → no delta updates → occasional change
- ☐ block storage breaks files down to small components → complex read, write, change functions

Elastic File System (EFS)

- ☐ a scalable file system used w/ AWS cloud services and on-premises resources
- ☐ allow multiple instances accessing the data in EFS at the same time

EBS vs. EFS

- ☐ EBS volume attaches to EC2 instances → an Availability Zone-level resource
- ☐ EFS stores data in and cross multiple availability zones → a regional service
  - ☐ EFS can have multiple instances reading and writing from it at the same time
  - ☐ on-premises servers can access Amazon EFS using Direct Connect

Amazon Relational Database Service (RDS)

- ☐ a service that enables you to run relational DB in the AWS Cloud (managed Service)

- [ ] RDS Read Replicas: provide enhanced performance and durability for DB

Amazon Aurora

- [ ] an enterprise - class relational DB replicates 6 copies of your data across 3 availability zones and continuously back up your data to S3

Amazon DynamoDB

- [ ] a key-value / non-relational (NoSQL) DB service
- [ ] Serverless: i. NOT need to patch or manage servers; ii. NOT need to install, maintain or operate software
- [ ] automatically scalable: suitable for use cases that require high performance while scaling
- [ ] stores data redundantly across availability zones

Amazon Redshift (single AZ)

- [ ] data warehouse: a system that pulls data from many different sources within an organization for reporting and analysis
- [ ] stores historical data, NOT store current info nor update in real-time
- [ ] Redshift Spectrum: a feature of Red shift that enables you to run SQL queries against exabytes of data in S3

Database Migration Service (DMS)

- [ ] Enable to migrate relational DB, non relational DB, and other types of data stores
    - [ ] Homogeneous migration: source and target DB are same type
    - [ ] Heterogeneous migration: Source and target DB are different
        - [ ] 2 steps: i. convert w/ Schema Conversion types Tool; ii. use DMS to migrate
- [ ] Source DB remains operational during the migration
- [ ] Development and test DB migration: use DMS to migrate a copy of your production DB to your dev / test environments
- [ ] DB Consolidations: combining several DBs into a central DB
- [ ] Continuous Replication: Sending ongoing copies of data to other target sources instead of doing one-time migration

Identity and Access Management (IAM)

- [ ] IAM enables you to manage access to AWS services and resources securely
- [ ] root user: has complete access to all AWS services and resources in the account (multi-factor authentication)

IAM Users

- [ ] an identity that you create in AWS
    - [ ] consists of name and credentials

Principle of least privilege

- [ ] a user is granted access only to what they need

IAM Policies

- ☐ a JSON document that allows or denies permissions to AWS services and resources
  - ☐ Principal (who needs accesses)
  - ☐ Action
  - ☐ Resource
  - ☐ Effect
  - ☐ Condition

IAM Groups (Group users)

- ☐ a collection of IAM users (an IAM policy an IAM policy is assigned to group, all users in the group are granted permissions specified by the policy)

IAM Roles

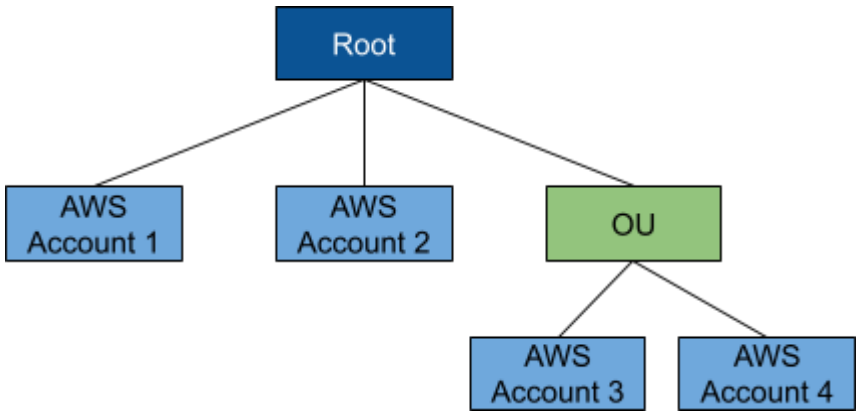
- ☐ an identity that you can assume to gain temporary access to permissions → Similar to user, but no username and password

AWS Organizations (Account Management & Consolidated Billing)

- ☐ Consolidate and manage multiple AWS accounts within a central location
- ☐ When an organization is created, AWS organizations automatically create root
- ☐ You can centrally control permissions for the accounts in your organization by using service control policies (SCPs) → SCPs place restrictions on the AWS services, resources, and individual API actions that users and roles in each account can access
  - ☐ SCP affects ALL IAM users, groups and roles (including the AWS account root users, IAM policies cannot be applied to AWS account root user)

Organizational Units (OUs) (Group accounts)

- ☐ Implement hierarchical groupings of your group accounts into OUs



AWS Artifact

- ☐ A Service that provides on-demand access to AWS Security and compliance reports and select online agreements.
  - ☐ AWS Artifact Agreements: review, accept and manage agreements of an individual account and all accounts in AWS organization regarding the use of certain types of info through AWS services

- [ ] Artifact Reports: provide compliance reports from 3rd-party auditors, which have tested and verified that AWS is compliant w/ a variety of global, regional and industry-specific security standards and regulations.

Customer Compliance Center

- [ ] resources to help learn more about AWS compliance

Denial-of-Service (DoS) Attack

- [ ] a deliberate attempt to make a website unavailable to users
- [ ] Distributed Denial-of-service (DDoS) attack: multiple sources are used to start an attack that aims to make a website or application unavailable

AWS Shield

- [ ] Shield Standard: automatically protects all AWS Customers from the most common types of DDoS attacks at no cost
- [ ] Shield Advanced: a paid service that provides detailed attack diagnostics and the ability to detect and mitigate complex DDoS attacks

AWS WAF

- [ ] a web application firewall that lets you monitor network requests that come into your web applications (monitor HTTP and HTTPS requests)
- [ ] AWS WAF to block or allow traffic by using a access control list (ACL) to protect AWS resources

Key Management Service (KMS)

- [ ] KMS enables you to perform encryption operations through the use of cryptographic keys

Cloud HSM

- [ ] a cloud-based hardware security module (HSM) that enables you to easily generate and use own encryption keys on the AWS cloud

Amazon Inspector

- [ ] to perform automated security assessments
- [ ] checks applications for security vulnerabilities and deviations from security best practices

AMazon GuardDuty

- [ ] provides intelligent threat detection for AWS infrastructure and resources
- [ ] identifies threats by continuously monitoring the network activity and account behavior within the AWS environment
- [ ] GuardDuty runs independently from your AWS services, so it won't affect performance / availability of the existing infrastructure and workload
- [ ] integrates w/ cloudWatch and Lambda to set up automated remediation actions

Amazon CloudWatch

- ☐ a web service that enables to monitor and manage various metrics and configure alarm actions based on data from those metrics
    - ☐ to automatically perform actions if the value of your metric has gone above / below an predefined threshold (integrated w/ SNS)
- ☐ Cloud watch Dashboard: access all the metrics of your resources from a single location → use this to optimize applications and operational resources

Amazon Cloud Trail

- ☐ a comprehensive API auditing tool that records API calls for your account → a complete history of user activity and API calls
- ☐ Cloud Trail Insights: optional features that allow Cloud Trail to automatically detect unusual API activities within AWS account

AWS Trusted Advisor

- ☐ an automated service that inspects your AWS environment and provides real-time recommendations
    - ☐ Cost Optimization (spend)
    - ☐ Performance
    - ☐ Security
    - ☐ Fault Tolerance (reliability)
    - ☐ Service Limits (max # of resources)

Pricing Concepts

- ☐ pay for what you need
- ☐ pay less when reserve
- ☐ pay less w/ volume-based discounts when use more

Aws Pricing Calculator

- ☐ create an estimate for the cost of your use cases on AWS → organize your AWS estimates by groups you defined
- ☐ estimated comparison of different EC2 instance types across AWS regions

Billing Dashboard

- ☐ Billing Cost Management Dashboard to pay bills, monitor usage, analyze and control costs
- ☐ **Consolidated Billing**: billing features of AWS Organization,which enabled to received a single bill for all AWS accounts in the organization
    - ☐ review itemized charges incurred each account
    - ☐ share bulk discount pricing

AWS Budgeting

- ☐ create budgets to plan your service usage, costs and instance reservations (update 3 times/day)
- ☐ set customize alerts when usage exceeds (or is forecasted to exceed) the budgeted amount

AWS Cost Explorer

- ☐ a console-based tool that enables you to visualize, understand and manage AWS costs and usage over time
  - ☐ default: top five cost-accruing services
  - ☐ apple customized filters and groups to analyze data

AWS Health Dashboard

- ☐ a single place to learn about the availability and operation of AWS services: NOT provide instance health checks
  - ☐ personalized view of service health
  - ☐ proactive notifications (important health event)
  - ☐ detailed troubleshooting guidance
  - ☐ Integration & Automation
  - ☐ Fine-grained access control by IAM
  - ☐ Aggregate health events across AWS organizations

AWS Support

- ☐ https://aws.amazon.com/premiumsupport/plans/

AWS Marketplace

- ☐ a curated digital catalog that includes software listings from independent 3rd party software vendors
  - ☐ to find, test and buy software that runs on AWS
  - ☐ click-and-go services

Deployment Models

- ☐ Cloud-Based Deployment
  - ☐ run all parts of application on Cloud
  - ☐ migrate existing applications to the cloud
  - ☐ design and build new applications in the cloud
- ☐ On-Premises Deployment: Private cloud
  - ☐ deploy resources by using virtualization and resource management tools
  - ☐ increase resource utilization by using application management and virtualization techs
- ☐ Hybrid Deployment
  - ☐ connect Cloud-based resources to on-premises infrastructure
  - ☐ integrate cloud-based resources w/ legacy IT applications

AWS Cloud Adoption Framework (AWS CAF)

- ☐ Business Perspective: ensures that IT aligns with business needs and that IT investments link to key business results

- ☐ People Perspective: supports development of an organization-wide change management strategy for successful cloud adoption
- ☐ Governance Perspective: focuses on the skills and processes to align IT strategy w/ business strategy →maximize business value and minimize risk
- ☐ Platform Perspective: principles and patterns for implementing new solutions on the cloud, and migrating on-premises workloads to the cloud
- ☐ Security perspective: ensures that the organization meets security objectives for visibility, auditability control and agility
- ☐ Operation Perspective: helps ensure, run, use, operate and recover IT workloads to the level agreed upon w/ your and business stakeholders

6 Strategies for Migration

- ☐ Rehosting: moving applications w/o changes (lift-and-shift)
- ☐ Replatforming: making a few cloud optimizations to realize a tangible benefits (lift, tinker, shift)
- ☐ Refactoring: re-imagining how an application is architected and developed by using cloud-native features
- ☐ Repurchasing: moving from a traditional license to a software-as-a-service model
- ☐ Retaining: keeping applications that're critical for the business in the source environment. applications that are
- ☐ Retiring: the process of removing no longer needed

AWS Snowcone

- ☐ a small, rugged, and secure edge computing and data transfer device
  - ☐ edge computing: i. EC2 instance; ii. IoT GreeGrass
- ☐ 2 CPUs, 4GB of memory, 8TB of usage storage

AWS Snowball (access the compute power of AWS locally**)**

- ☐ Snowball Edge Storage Optimized: devices are well-suited for large-scale data migrations and recurring transfer workflows
  - ☐ Storage: 80 TB hard disk drive, S3 compatible Storage, 1TB OF SATA solid state drive
  - ☐ Compute: 40 vCPUs, 80 GB memory to support EC2 instance
- ☐ Snowball Edge Compute Optimized: powerful computing resources for machine learning, analytics, etc.
  - ☐ Storage: 42TB HDD, S3 Compatible, 7.68 TB of usable NVMe SSD Capacity
  - ☐ Compute: 52 vCPUs, 208 GB memory, optional NVIDIA Tesla v100 GPU

AWS Snowmobile

- ☐ an exabyte-scale data transfer service used to move large amount of data to AWS → transfer up to 100 petabytes

Advantages of Cloud Computing

- ☐ Trade upfront expense for variable expense

- [ ] Benefits from massive economies of scale → AWS continuously lower costs as it grows
- [ ] Stop guessing capacity
- [ ] Increase speed and agility
- [ ] Stop spending money running and maintaining data centers
- [ ] Go global in minutes

==========

AWS Serverless Platform

1. No reservation when using serverless architecture
2. Compute resources are only used when code is being executed

- [ ] Compute Service: AWS Lambda, Lambda @Edge, AWS Fargate
- [ ] Storage: S3, EFS
- [ ] Data Stores: DynamoDB. Aurora Serverless, RDS proxy
- [ ] API Proxy: API Gateway
- [ ] Application Integration: SNS, SQS, AppSync, Event Bridge
- [ ] Orchestration: Step Functions
- [ ] Analytics : Kinesis, Athena

Amazon Services involved DDOS Mitigation

- [ ] AWS WAF
- [ ] Route 53
- [ ] CloudFront
- [ ] ELB
- [ ] VPCs & Security Groups

AWS Config

- [ ] access, audit and evaluate configurations of your resources

Horizontal Scaling

- [ ] increase capacity by adding more computers to the system

Vertical Scaling

- [ ] increase performance by adding more resources into one computer, like faster CPUs, memory, storage

AWS CodeDeploy

- [ ] fully managed deployment service that automates software deployments to a variety of compute services such as EC2, Fargate, Lambda, on-premises servers

Aws OpsWorks

- [ ] a configuration management service that provides managed instances of Chef and Puppet
    - [ ] Chef and Puppet: automation platforms that allow you to use code to automate the configurations of your servers

Total Cost of Ownership (TCO) Calculator

- [ ] to estimate the cost savings when using Aws and provide a detailed set of reports
- [ ] to reduce TCO by reducing the need to invest in large capital expenditures and providing a pay-as-you-go model
- [ ] Contributors of TCO → All costs of owning and operating a data center (physical hardware)
    - [ ] Storage Costs
    - [ ] Network Costs
    - [ ] IT Labor Costs
    - [ ] Server Costs
    - [ ] cooling and power consumption
    - [ ] data center space
    - [ ] data center real estate

EC2 Reserved Instances

- [ ] Standard RIs provide the most significant discount (up to 72% off On-demand) and best suited for Steady-state usage
- [ ] Convertible RIs: a discount (up to 54% off) and the capability to change the attribute of the RI as long as the exchange results in the creation of RI of equal / greater value
- [ ] Scheduled RIs: available to launch within the time windows you reserve Allows you to match your capacity reservation to a predictable recurring schedule that only requires a fraction of a day / week / month

ElastiCache

- [ ] a service that enables to set up, manage and scale a distributed in-memory or cache environment in the cloud → to provide ultrafast and inexpensive access to copies of data

AWS-managed Services

- [ ] AWS is responsible for performing all the operations needed to keep the service running (provide scalability and flexibility of cloud-based resource w/ less operational overhead)
    - [ ] Examples: Amazon RDS, DynamoDB, Redshift, Cloud front, etc.

Customer-managed Services

- [ ] services that are completely managed by the customers.
    - [ ] Examples: Elastic Compute Cloud (EC2), VPC, IAM
- [ ] AWS customers are allowed to perform Penetration testing on both AWS-managed and customer-managed services.

Cloud Computing Models

- [ ] Infrastructure as a Service (IaaS): typically provides access to networking services, computers and data storage space (EC2)
- [ ] Platform as a Service (PaaS): removes the need for your organization to manage the underlying infrastructure and allows you to focus on the deployment and management of applications

- Software as a Service (SaaS): provides you w/ a completed product that is run and managed by the service provider

AWS Concierge Team

- assist w/ the issues related to billing and account management

AWA Customer Service Team

- help customers understand what cloud computing is all about, and whether it can be used for their business.

Amazon Connect

- a cloud-based Contact Center Service that helps business to deliver customer service at a low cost

Share Responsibility Model

- Inherited Controls: controls which a customer fully inherits from AWS (AWS responsibility)
  - Physical and Environmental Controls
- Shared Controls: Controls which apply to both infrastructure layer and customer layer
  - Patch management
    - AWS: patching flaws within infrastructure
    - Customers: patching guest OS and apps
  - Configuration management
    - AWS: infrastructure devices
    - Customers: guest OS, databases, Apps
  - Awareness & Training
- Customer Specific: controls which are solely the customer responsibility based on applications they deploy within AWS
  - Service and Communications Protection / zone security

AWS X-Ray

- helps developers analyze and debug distributed applications in production or under development (like those built using micro service)

Amazon Machine Image (AMI)

- a supported and maintained image provided by AWS that provides the information required to launch an instance
- a template contains a software configuration (like OS, application Servers, apps) → save time, avoid errors

Multi-AZ Services

- DynamoDB
- S3
- EFS
- Aurora
- Redshift, EBS do NOT support multi-Az

- [ ] RDS does NOT automatically replicate data across multi-AZ

AWS Service Catalog

- [ ] allows organizations to create and manage catalogs of IT services that're approved for use on AWS → to centrally manage commonly deployed IT services and help achieve consistent governance and meet your compliance requirements

AWS Certificate Manager (ACM)

- [ ] provides server certificate → to enable HTTPS Connections to your website or application in AWS, an SSL/TLS server Certificate is needed
- [ ] use IAM as a certificate manager only when you must support HTTPS connections in a region that is not supported by ACM

AWS Software Development Kit (SDK)

- [ ] Simplifies using AWS services in your applications w/ an API tailored to your programming language or platform

AWS Elastic Disaster Recovery (next generation of CloudEndure)

- [ ] a disaster recovery solution that minimizes downtime and data loss by providing fast, reliable recovery of physical, virtual and cloud-based servers into AWS Cloud

AWS CloudEndure Disaster Recovery

- [ ] an agent-based solution that lets you recover your environment from unexpected infrastructure or application outages, data corruption, ransomware, or other malicious attacks

AWS Backup

- [ ] use to copy backups to a different AWS regions and recover from those backups in the new region in case of disaster
    - [ ] Backups & Restore strategy requires hours to be implemented

AWS Transit Gateway

- [ ] a network transit hub that simplifies how customers interconnect all their VPCs across thousands of AWS accounts and into their on-premises networks

Well-Architected Framework

- [ ] Operational Excellence: the ability to run workloads effectively to gain insight into their operations, and to continuously improve supporting processes and procedures
    - [ ] Perform operation as code
    - [ ] Make frequent, small, reversible changes
    - [ ] Refine operations procedures frequently
    - [ ] Anticipate failure
    - [ ] Learn from all operational failures
- [ ] Security: to protect data, systems and assets in a way that can improve your security posture
    - [ ] Implement a strong identity foundation
    - [ ] Enable traceability

- [ ] Apply security at all layers
- [ ] Automate security best practices
- [ ] Protect data in transit and at rest
- [ ] Keep people away from data
- [ ] Prepare for security events

- [ ] Reliability
  - [ ] Automatically recover from failures
  - [ ] Test recovery procedures
  - [ ] Scale horizontally to increase aggregate workload availability
  - [ ] Stop guessing capacity.
  - [ ] Manage change in automation
- [ ] Perform Efficiency: achieve and maintain efficient workloads
  - [ ] Democratize advanced technologies
  - [ ] Go global in minute
  - [ ] Use serverless architectures
  - [ ] Experiment more often
  - [ ] Consider mechanical sympathy
- [ ] Cost Optimization
  - [ ] Implement cloud financial management
  - [ ] Adopt a consumption model
  - [ ] measure overall efficiency
  - [ ] stop spending money on undifferentiated heavy Lifting
  - [ ] Analyze and attribute expenditure
- [ ] Sustanability
  - [ ] understand your impact and Establish sustainability goals
  - [ ] Minimize utilization
  - [ ] Anticipate and adopt new, more efficient hardware and software
  - [ ] se managed services
  - [ ] Reduce the downstream impact of cloud workloads

AWS Database

- [ ] RDS only supports Storage auto-scaling NOT instance auto-scaling If you want to scale Amazon RDS instances:
  1. Manual horizontal scaling (by adding read replicas)
  2. Manual vertical scaling (by upgrading / downgrading an existing instance)
- [ ] Aurora can scale instances automatically
- [ ] EBS is the primary storage service used by RDS
- [ ] Benefits of DynamoDB:

  1. Performance at scale: Consistent, single-cligit millisecond response time
  2. Serverless : automatically scales fables up and down to adjust for capacity and maintain performance
  3. Highly Available

- [ ] Database Snapshots: user-initiated backups of your RDS instance stored in Amazon S3 that are kept until you explicitly delete them
- [ ] In relation to Amazon RDS databases:
    - [ ] AWS is responsible for:
        1. managing the underlying infrastructure and foundation
        2. managing the operating system.
        3. Database setup
        4. Patching and backups
    - [ ] Customer is responsible for:
        1. Protecting the data stored in databases (through encryption and IAM access control)
        2. managing the database settings that are specific to the application
        3. Building the relational schema
        4. Network traffic protectionServices

- [ ] AWS customers have 2 options to host their DBs:
    - [ ] using a managing DB → AWS is responsible
    - [ ] Installing a DB software on EC2 → customer is responsible
    - [ ] It's the customer's responsibility to encrypt data either on the client side or the server side

AWS Pricing Models

- [ ] Saving Plans: low price on EC2, Lambda, Fargate usage in exchange for a commitment to a consistent amount of usage ($/hour) for a 1 or 3 years
    - [ ] beyond commitment will be charged on-demand rates
- [ ] Reserved Instance: a billing discount applied to the use of on-demand compute instances
- [ ] Dedicated Host: allow you to use your eligible software licenses from vendors →Bring Your Own License (BYOL) Model
- [ ] EC2 instance pricing varies depending on many variables:
    - [ ] Buying Option (On-demand, Saving Plans, Reserved, Spot, Dedicated)
    - [ ] Selected instance type
    - [ ] Selected region
    - [ ] Number of Instances
    - [ ] Loading balance: the # of hours the ELB runs and the amount of data it processes contribute to the EC2 monthly cost
    - [ ] Allocated Elastic IP addresses
    - [ ] Operating Systems and software packages
- [ ] AWS will charge users once a resource is allocated. Users should do the following once they are completing their work
    1. Delete all ELBs
    3. Delete the attached EBS volume
    2. Terminate all unused EC2 instances
    4. Release any unused ELBs

- [ ] Per-second Billing: EC2 Linux, Windows, Ubuntu provisioned storage for EBS volumes RDS, EMR, AWS Batch
- [ ] Use of reservations means that the customer will be charged the agreed upon Reserved Instance hourly rate irrespective of if the instance is running or not

AWS Management & Governance

- [ ] AWS Management Console lets users create new RDS instances through a web-based user interface
- [ ] AWS Cloud Formation lets users create new RDS instances using the CloudFormation template language
- [ ] AWS config records point-in-time configuration details for your AWS resources as Configuration Items (CIS) and allow you to automate the evaluation of recorded configurations of a specific resource against desired configurations → provides info about the changes made to a resource
- [ ] CloudTrail records user API activity on your account and allows you to access information about this activity → provides info about who made those changes

Storage

- [ ] S3: object storage built to store and retrieve any amount of data from anywhere on the internet
    - [ ] durable, highly available, infinitely scalable, low cost, limited I/O
        - [ ] S3 stores any number of objects, but each object w/ a size limitation
    - [ ] Common Use Case
        - [ ] media hosting (video, photo, music)
        - [ ] hosting static websites
        - [ ] backup and storage
        - [ ] deliver content globally: conjunction w/ cloudFront
        - [ ] hybrid cloud storage
- [ ] EBS: block Storage volumes for use w/ Amazon EC2 and RDS instances
    - [ ] quickly accessible, long-term persistence, single AZ
    - [ ] Common use Case
        - [ ] Storage for operating system, DBs or any applications that require fine granular updates
- [ ] EFS: simple, scalable, elastic file storage for use w/ AWS Cloud services and on-premises resources
    - [ ] elastically scale on demand, multiple AZ
    - [ ] massively parallel shared access
    - [ ] enable applications to achieve high level of aggregate throughput
- [ ] Storage Gateway: a hybrid storage system service that enables on-premises applications to seamlessly use AWS cloud storage
- [ ] S3 and EFS are automatically scaled. EBS provides persistent block level storage volumes only be used as a drive for EC2 or RDS
- [ ] S3 Provides a number of security features for the protection of data at rest:

- Permissions
- Versioning: to store a new version for every modified or deleted object from which you can restore compromised objects → protect data from accidental deletion
- Replication
- Encryption - Server side: AWS generates a unique encryption key for each object
- Encryption - Client side

- **AWS Macie**: a fully managed security service to help protect sensitive data in S3 ←use machine learning to automatically discover, classify and protect sensitive data in Amazon S3
- Storage Gateway supports 4 key hybrid cloud use cases:
  1. provides on-premises applications low latency access to data stored in AWS
  2. migrates on-premises data to AWS while maintaining fast local access to recently accessed data
  3. optimizes data transfer to Aws by sending only changed data and compressing data
  4. reduces on-premises storage w/ cloud-backed file shares
- S3 pricing is based on 4 factors:
  1. total amount of data (in GB) stored on S3
  2. Storage class
  3. Amount of data transferred out of Aws from S3
  4. Number of requests to S3 EBS
- EBS pricing is based on 2 factors:
  1. volume storage for all EBS volume type is charged by the amount of GB you provision per month until you release the storage
  2. Snapshot storage is based on the amount of space your data consumes in 53
- The factors that have the greatest impact on cost include:
  1. Compute
  2. Storage
  3. Data transfer out
- Reduce the costs of EBS:
  1. Delete unattached EBS volumes
  2. Resize / change the EBS volume type
  3. Delete stale EBS snapshots
- EFS is designed to provide massively parallel shared access to thousands of EC2 instances, enabling applications to achieve high levels of aggregate throughput and IOPS that scale as a file system grows, w/ low latencies
  - EBS or S3 cannot be attached to (multiple) compute resources
- CloudFront pricing is based on 3 factors:
  1. Traffic distribution: varies across geographic regions
  2. requests: number and type of requests (HTTPS or HTTP) made
  3. data transfer OUT
- AWS Lambda pricing is based on 2 factors:
  1. number of requests for your functions
  2. time it takes to execute the codes

AWS Support API

- [ ] provides programmatic access to AWS Support Center features to create, manage, and close support cases, and operationally manage Trusted Advisor Check and status
    - [ ] only available for AWS customers who have a Business or Enterprise support plan

Amazon Cloud Directory

- [ ] a cloud-native, highly scalable, high-performance directory that provides web-based directories to make it easy for you organize and manage all your apps resources (users, groups, locations, devices and policies)

AWS Directory Service

- [ ] service provides SSO to applications and services

Deploy Apps to EC2 instances: Elastic Beanstalk, cloud Formation, CodeDeploy, OpsWorks
Deploy Apps to on-premise servers: CodeDeploy, OpsWorks

AWS Security, Identity & Compliance

- [ ] Customers can work w/ AWS Identity and Access Management in any of the following ways:
  1. AWS Management Console: The console is a browser-based interface that can be used to manage IAM and AWS resources
  2. AWS Command Line Tools (CLI): to issue commands at your system's Command line to perform IAM and AWS tasks
  3. AWS SDKS: provides a convenient way to create programmatic access to IAM and AWS

- [ ] A Security Bulletins : publishes security bulletins about the latest security and privacy events w/ AWS services on the security bulletin pages
- [ ] Customers are responsible for protecting their data following ways:
  1. Data encryption
  2. Setting up access control
  B. Monitoring user activity
  4. Applying MFA
  5. Using advanced managed security services (like Macie)
- [ ] **AWS Detective**: a security service that makes it easy to analyze, investigate, and quickly identify the root cause of potential security issues or suspicious activities
- [ ] IAM roles w/ temporary Credentials are useful in the following situations:
  1. Applications running on EC2
  2. Federated user access
  3. Aws service access

IAM Policies → roles/users
SCPs → accounts

AWS Analytics & Compute

- [ ] Elastic Map Reduce (EMR): a web service that enables business, researchers, data analysts, and developers to easily and cost-effectively process vast amounts of data →a hosted Hadoop framework running on the web-scale infrastructure of EC2 and S3
- [ ] EMR is ideal for problems that necessitate the fast and efficient processing of large amounts of data

- [ ] 4 EMR compute Options:
  1. EC2
  2. EKS
  3. Outposts
  4. EMR Serveless

Lightsail

- [ ] is designed to be the easiest way to launch and manage a Web server using AWS (NOT severless)

Cloud Development Kit (CDK)

- [ ] an open-source software development framework for defining cloud infrastructure as code w/ modern programming languages and deploying it through CloudFormation

Miscellaneous

- [ ] A CloudFront, Aws shield, and AWS WAF work seamlessly together to create a flexible layered security perimeter against multiple types of attacks including network and application DDoS attacks
- [ ] AWS Organization has 5 main benefits:
  1. centrally manage access policies across
  2. Automate Aws account creation and management
  3. control access to Aws services multiple Aws accounts accounts
  4. consolidate billing across multiple AWS accounts
  5. configure Aws services across multiple
- [ ] Access keys (access key ID and secret access key) are long-term credentials for an IAM user or the account roof user → make API calls or use the AWS CLI
- [ ] Benefits of using On-Demand EC2 instances:
  1. no longer-term commitments or upfront payments are needed
  2. increase / decrease your compute capacity depending on the demands of your application and only pay what you use
  3. free you from the costs and complexities of planning purchasing and maintaining hardware → transfer commonly large fixed costs into much smaller variable costs
  4. remove the need to buy "safety net" capacity to handle periodic traffic spikes
- [ ] Cloud Computing better than traditional data center:
  1. High-availability
  2. Distributed infrastructure operates over 75 AZ within over 20 geographic Regions
  3. On-demand infrastructure for scaling applications / tasks
  4. Cost saving