AWS Certified Cloud Practitioner Exam Content Outline

Cloud Concepts (28%)

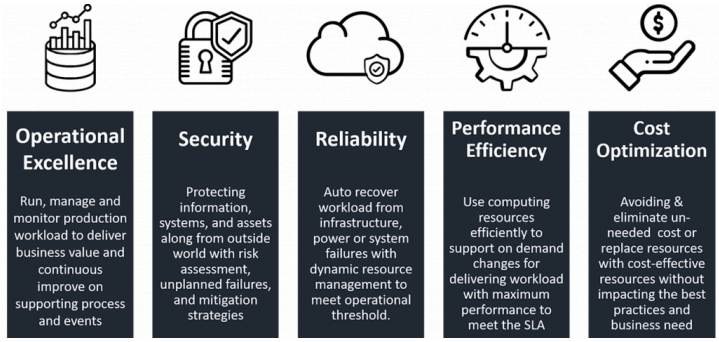
- Value Proposition: Trade Capital Expense for Variable Expense
- AWS offers lower upfront and lower variables compared to a traditional data centre and virtualized cloud computing

Identify aspects of AWS Cloud economics

- Reduce/stop spending money on running and maintaining data centers
- Leverage elasticity to match supply with fluctuating demand
- Only pay when consume computing resources, and only pay for how much you consume
- Continual refinement and improvement of system (optimize over time – can measure, monitor, and improve architecture from data you've collected on AWS platform).

Pillars of well-Architected Framework

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



Security (24%)

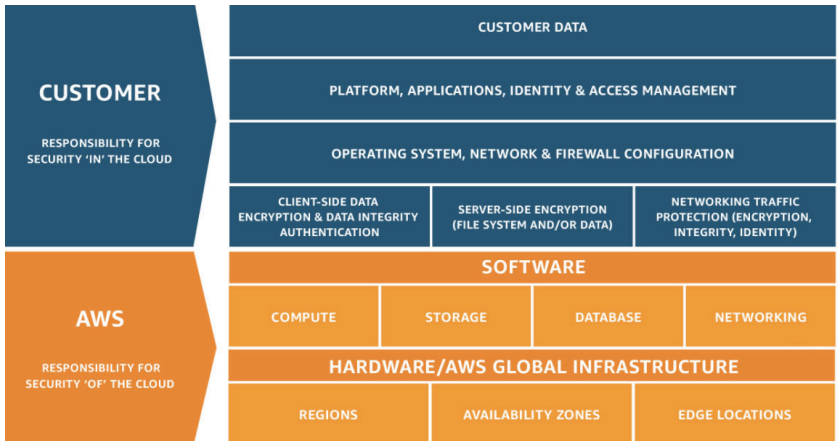
Define the AWS Shared Responsibility model

AWS responsible for SECURITY "OF" THE CLOUD

- Software (AWS Foundation Services): Compute, Storage, Database, Networking
- Hardware/AWS Global Infrastructure: Regions, Availability Zones (Data centers), Edge Locations

Customer Responsible for SECURITY "IN" THE CLOUD

- Customer Data
- Platforms, Applications, Identity and Access Management
- Operating System, Network & Firewall Configuration
    - (i) Client-Side Data Encryption and Data Integrity Authentication, (ii) Server-Side Encryption (File System and/or Data), (iii) Networking Traffic Protection (Encryption, Integrity, Identity)



Define AWS Cloud security and compliance concepts

- No public tours of Data Centers
- Encryption at rest and/or in transit
- AWS CloudTrail captures actions made directly by the user or on behalf of the user by an AWS service (Use cases: compliance, security analysis, data exfiltration detection)
- **Application Load Balancer** supports direct integration with the Web Application Firewall (WAF); Supported Protocols; Cloudwatch Metrics; Acess Logs; Health Check.

Security Group	Network ACL
Operates at the instance level (first layer of defense)	Operates at the subnet level (second layer of defense)
Supports allow rules only	Supports allow rules and deny rules
Is stateful: Return traffic is automatically allowed, regardless of any rules	Is stateless: Return traffic must be explicitly allowed by rules
We evaluate all rules before deciding whether to allow traffic	We process rules in number order when deciding whether to allow traffic
Applies to an instance only if someone specifies the security group when launching the instance, or associates the security group with the instance later on	Automatically applies to all instances in the subnets it's associated with (backup layer of defense, so you don't have to rely on someone specifying the security group)

Identify AWS access management capabilities

- Security Groups and NACLs (Network Access Control Lists)
    - By default with Security Groups, no inbound traffic allowed, all outbound traffic allowed (firewall at instance)
    - NACL rules are applied to all EC2 instances in the associated subnet; security groups are applied on a per-instance basis
- IAM: AWS Identity and Access management, authentication, and authorization service (IAM roles a secure way to grant permissions to entities that you trust to access AWS resources)
    - 5 areas of IAM: manage user password, manage access keys, manage signing certificates, delete user, add user to groups
- Identity and Access Management (IAM) Policies:

  - To manage access in AWS: (i) create a policy defining permissions, (ii) associate policy with an identity or resource
  - AWS supports six types of policies: identity-based policies, resource-based policies, permissions boundaries, Organizations SCPs, ACLs, and session policies
- To enable clients to sign-up and sign-in to your mobile and web app, use Amazon Cognito
- NAT Gateways: You can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances.

Identify resources for security support

- AWS Inspector – perform security assessment on instances to check for exposure, vulnerabilities and deviations
- AWS Multi-Factor Authentication (MFA) – simple best practice adds an extra layer of protection of login security to a user's AWS Management Console
- AWS Config – a service that enables you to assess, audit, and evaluate the configurations of your AWS resources

Technology (36%)

Define the AWS global infrastructure

- **Regions**: geographic areas that host two or more A-Zs
- **Availability Zones**: collection of **data centers** in a specific Region
- **Edge Locations**: enable quicker content delivery (host a CDN called AWS CloudFront)

Identify the core AWS services

—Compute—

- **EC2** – Elastic Cloud Compute
  - server-based t2 instance type (free tier) good for running Linux but not enough memory to run Windows OS with these
- ECS – EC2 Container Service, highly scalable, supports Docker containers
- **AWS Lambda** – serverless; pay only for the compute time
- Elastic Beanstalk – provides container for different platforms and helps **deploying and scaling web applications** within minutes.

		File Amazon EFS	Object Amazon S3	Block Amazon EBS
Performance	Per-operation latency	Low, consistent	Low, for mixed request types, and integration with CloudFront	Lowest, consistent
	Throughput scale	Multiple GBs per second	Multiple GBs per second	Single GB per second
Characteristics	Data Availability/Durability	Stored redundantly across multiple AZs	Stored redundantly across multiple AZs	Stored redundantly in a single AZ
	Access	One to thousands of EC2 instances or on-premises servers, from multiple AZs, concurrently	One to millions of connections over the web	Single EC2 instance in a single AZ
	Use Cases	Web serving and content management, enterprise applications, media and entertainment, home directories, database backups, developer tools, container storage, big data analytics	Web serving and content management, media and entertainment, backups, big data analytics, data lake	Boot volumes, transactional and NoSQL databases, data warehousing & ETL

—Storage—

- **S3**-Simple Storage Service
  - Supports versioning and MFA for object recover, object lifecycle management, secure, durable storage
  - Can define following actions on objects: Archive Only, Permanently Delete Only, Archive and then Permanently Delete
  - Billed for storage, requests, data transfer
- Amazon **S3 Storage Classes**:
  - **Standard**: general-purpose storage of frequently accessed data, 99.999999%Durability and 99.99% Availa
  - **Reduced Redundancy Storage(RRS)**: store noncritical, reproducible data at lower level of redundancy, provide 99.99% durability and availability
  - **Infrequent Access (IA)**: for long-lived but less frequently accessed data, lowest availability rate 99.90%
  - **Glacier**: long-term archive and digital preservation, archive files in case of compliance
  - Intelligent-Tiering: unknown or changing access
- **EBS**-Elastic Block Store
  - detachable/movable data – can reattach to another EC2 instance

    - network-linked persistent storage volume that you can attach to EC2 instances
    - unformatted because don't know format until attach it, encrypted using KMS
- AWS storage services: S3;EBS;EFS(Elastic File Storage);Glacier;Storage Gateway(On-premise)

—Database—

- **Relational Database Service (RDS)** – set up, operate, and scale a relational database, including Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle and Microsoft SQL Server, **ideal for data with frequent overwrites or updated and deletion**
- **DynamoDB** – fast and flexible **NoSQL** database service for any scale, at single-digit millisecond latency; **key-value and document** database; handle item size upto 400KB; Automatic scaling of throughput capacity
- **Aurora** – MySQL and PostgreSQL-compatible **relational database built for the cloud**
- Redshift – fast, simple, cost-effective data warehouse that can extend queries to your data lake
- ElastiCahe— a web service for **in-memory data store or cache**, offload the **read** traffic, improves web performance

—Networking & Content—

- **VPC**-Virtual Private Cloud
    - An isolated virtual network on AWS cloud
    - **By default, ports are off Internet Gateway(IGW)& Virtual Private Gateway(VGW)== VPN on AWS**
    - Subnets within Availability Zone (AZ).
    - VPC peering: a **networking connection between two VPC**s, enables route traffic
- **Route 53** – a global, highly available and scalable cloud Domain Name System (DNS) web service; hosted zones
- CloudFront – fast, secure and programmable content delivery network (CDN),built-in DDoS mitigation, caching services utilizes in Edge locations
- Direct Connect – create *virtual interfaces* directly to public AWS services via Ethernet cable, hybrid connection, dedicated high bandwidth, throughput and low latency

—Management & Governance—

- AWS Organizations –centrally apply policy-based controls across multiple accounts, volume pricing qualification
- Security Groups: one of the highest priorities; act as **built-in firewalls**; control accessibility
- CloudFormation – model and provision all of your cloud infrastructure resources, create a template describes all the AWS resources (Infrastructure as code)
- **CloudWatch** – complete visibility (monitoring and management) of your cloud resources and applications, monitor operational health and performance
- CloudTrail – continuously monitor and track user activity and API usage
- Auto Scaling – configure a set of instructions to optimize utilization of AWS resources
- AWS OpsWorks – a configuration management service using Chef, an automation platform that treats server configuration as code. Allows interaction with **On-premises servers**

—Security, Identity, & Compliance—

- AWS Key Management Service (KMS) – easily create and manage keys and control the use of encryption across a wide range of AWS services and in your applications.
- AWS Shield – A managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. Shield Advanced: DDoS Response Team (DRT 24/7)
- AWS Artifact – provides on-demand access to AWS' security and compliance reports and select online agreements

—Others—

- Simple Notification Service (SNS) – fully managed sub/pub messaging for microservices, distributed systems, and serverless applications (HTTP/ Email-JSON/ SQS/ SMS/Lambda)
- Simple Queue Services (SQS) – asynchronous message queue service, fully managed message queues for microservices, distributed systems, and serverless applications; build loosely coupled
- Server Migration Service (SMS) – automates the migration of your on-premises, replicates your server VMs as cloud-hosted Amazon Machine Images (AMIs) ready for deployment on EC2
- Snowball – **petabyte-scale** data transport solution (**less than** 10PB or in **multiple locations**)
- Snowmobile – **extrabyte-scale** data transfer service (10PB + in a **single location, i.e. video file**)

AWS Certified Cloud Practitioner Exam Content Outline

—Analytics—

- Athena – interactive query service that makes it easy to analyze data directly in S3 using standard SQL
- Kinesis – easily collect, process, and analyze video and data streams in real time, at high frequency

Billing and Pricing (12%)

Compare and contrast the various pricing models for AWS

- EC2s via on-demand instances, reserved instances, spot (bid) instances: cheapest with interrupt (Spot Block: launch Spot Instances with a specified duration without interruption)
- Dedicated Instance: run on hardware dedicated to a single customer
- **Dedicated Hosts**: physical servers to provision AWS EC2 resources, fully dedicated to your use

Recognize the various account structures in relation to AWS billing and pricing

- Object Storage Class Levels: Min storage duration 30 days (except Glacier – for long-term storage/archiving – which is 90 days) – pay for entire minimum duration even if change mind after first day.
- AWS Cost Explorer –

Identify types of AWS support

- **Technical Account Manager (TAM)**: Proactive Guidance
- **AWS Trusted Advisor**: Cost Optimization; Performance; Security; Fault Tolerance—Access to the 7 core Trusted Advisor checks and guidance to **provision your resources following best practices** to increase performance and improve security
- **AWS Support Concierge**: Account Assistance, Billing
- Four support plans:

  Basic; Developer; Business; Enterprise

- AWS Total Cost of Ownership (TCO) Calculators

  – **compare the cost** of your applications in an on-prer or traditional hosting environment to AWS

  – provides directional guidance on **possible savings** when deploying AWS

Features	Basic Current plan	Developer	Business	Enterprise
Customer service and communities	24x7 access to customer service, documentation, whitepapers, and support forums	24x7 access to customer service, documentation, whitepapers, and support forums	24x7 access to customer service, documentation, whitepapers, and support forums	24x7 access to customer service, documentation, whitepapers, and support forums
Best practices	Access to 7 core Trusted Advisor checks	Access to 7 core Trusted Advisor checks	Access to all Trusted Advisor checks	Access to all Trusted Advisor checks
Health status and Notifications	Access to Personal Health Dashboard	Access to Personal Health Dashboard	Access to Personal Health Dashboard & Health APIs	Access to Personal Health Dashboard & Health APIs
Technical support		Business hours** access to Cloud Support Associates via email	24x7 access to Cloud Support Engineers via email, chat, and phone	24x7 access to Cloud Support Engineers via email, chat, and phone
Who can open cases		One primary contact/ Unlimited cases	Unlimited contacts/ Unlimited cases (IAM supported)	Unlimited contacts/ Unlimited cases (IAM supported)
Case severity/Response times*		General guidance: < 24 hours System impaired: < 12 hours	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour Business-critical system down: < 15 minutes
Architecture support		General guidance	Contextual guidance based on your use-case	Consultative review and guidance based on your applications and solutions
Launch support			Infrastructure Event Management (Available for additional fee)	Infrastructure Event Management (Included)
Programmatic case management			AWS Support API	AWS Support API
Third-party software support			Interoperability and configuration guidance and troubleshooting	Interoperability and configuration guidance and troubleshooting
Architecture review				Access to a Well-Architected Review delivered by AWS Solution Architects
Operations support				Operational reviews, recommendations, and reporting
Training				Access to online self-paced labs
Account assistance				Assigned Support Concierge
Proactive guidance				Designated Technical Account Manager
Pricing	Included	Starting at $29 per month See pricing detail and sample	Starting at $100 per month See pricing detail and sample	Starting at $15,000 per month See pricing detail and sample

Additional Notes

- Access AWS through Management Console, CLI, SDKs
- AWS X-Ray – helps developers analyze and debug production, distributed applications
- AWS CodePipeline – a fully managed continuous delivery service that helps you automate your release pipelines for fast and reliable application and infrastructure updates
- Amazon Machine Image – provides the information required to launch an instance, launch multiple instances with same configuration; pre-baked pre-configured image
- **Instance store volumes** for your EC2 instance delete root volume configuration when you terminate the instance.
- Disaster Recovery Option from cheapest to most expensive