|  |
| --- |
| Close-up image showing the leaf-sides of two oversized books side-by-side on a bookshelf, with additional books in soft focus background |
| AWS Certified Cloud Practitioner  Revision Notes |
| |  |  |  | | --- | --- | --- | |  | 2/16/22 | AWS Fundamentals | |

**AWS Cloud Practitioner**

[AWS Power Hour: Cloud Practitioner (awscloud.com)](https://pages.awscloud.com/Global_traincert_AWS_Power_Hour_Cloud_Practitioner_FY21.html)

**Cloud computing** in on-demand delivery of IT resources via the internet with Pay-As-You-Go pricing model

**Cloud Deployment Model**

* On-Premise / Private Cloud (if virtualization deployed)
* Cloud Deployment
* Hybrid Deployment

**Benefits of moving to AWS**

* trade upfront expense for variable expense
* stop spending money to run maintain datacenters
* stop guessing capacity
* benefit from massive economies of scale
* increased speed and agility
* go global in minutes

**Ways to Interact with AWS**

* AWS Management Consoles
* AWS CLI - make API calls using terminal on your machine
* AWS SDKs - though various programming languages

**EC2** - **E**lastic **C**ompute **C**loud / VMs

* General Purpose - T series
* Compute Optimized - C series
* Memory Optimized - R series
* Accelerated computing - P series
* Storage optimized - I series

**AWS Lambda** - managed compute / Serverless < 15 Mins

**ECS** - EC2 Container service (Docker)

**EKS** - EC2 Kubernetes service

**AWS Fargate** - Serverless for ECS or EKS

**Billing**

* on-demand
* Spot instance
* Reserves instanced
* saving plans

**Amazon Auto Scaling**

**ELB** - Elastic Load Balancing

**Messaging Service**

**Amazon SQS** - Simple Queue Service

**Amazon SNS** - Simple Notification Service (publish/subscribe)

**AWS datacenter**:- https://aws.amazon.com/compliance/data-center/data-centers/

**Global Infrastructure:-** https://aws.amazon.com/about-aws/global-infrastructure/

* Redundant Power and Internet
* AZ / Availability zone consist of multiple datacenter
* Group of AZs called Region
* AZs connected by high speed links
* For Resiliency - keep VMs/EC2 in at least 2 AZs
* Regions are connected by AWS backbone

**AWS Region Key business factors**

* Regulation / compliance
* proximity
* feature availability
* pricing

**Availability Zone** –

* single data center or a group of data centers within a Region
* run across at least 2 AZs in a region
* ELB/SNS/SQS AWS Regional service are already highly available

**Edge Location**

* Amazon Cloud Front is CDN
* different from AWS Regions
* edge location can run Route 53

**AWS Outpost**

* Extend AWS infrastructure and services to your on-premises data center
* https://aws.amazon.com/outposts/

**For online diagram**

* https://app.diagrams.net/

**AWS Elastic Beanstalk** –

* you provide code and configuration settings, and it deploys the resources necessary to perform

**AWS CloudFormation** –

* infra as code

**Networking**

* VPC - Virtual Private Cloud. Is regional resource and hence it can span over AZs
* Subnet:- Public Subnet, Private Subnet
  + subnet are assigned within Availability zone
* CIDR - Classless Inter-domain Routing
* Public Network -->Internet Gateway(managed service) --> VPC/Pub.Subnet-->EC2 ---> NAT Gateway(managed service)
* CorpDC --> Cust.Agteway-->Virtual Private Gateway --> SecurityGroup / ELB-->Private Subnet
* CorpDC -->AWS Direct Connect
* Cust.FW-->Cust.Router-->AWSDirectConnectEndPoint
* Network SecurityGroup(stateful) at EC2 instance level
* Network ACL(stateless) at boundary of subnet level

**Storage:**

* **Instance Storage** 
  + is temp storage
* **Elastic Block Store** –
  + EBS Volume
  + SSD - low latency, high i/o.
  + HDD - high latency
  + Replicated with AZ
  + Can be encrypted
  + Can be scaled
  + AZ level resource. need to be attached to EC2 in same AZ
  + EBS allows incremental back/snapshot backup
  + size up to 16TB
  + SSD by default. HDD options
  + does not expand automatically
* **EFS**
* use when we need to share between multiple EC2 instance
* For Linux workload
* this is called FSx for Windows workload
* Both EBS & EFS/FSx are meant for EC2 instance

**S3 Amazon simple storage service**

* S3 is object level storage. When a file in object storage is modified, the entire object is updated.
* objects are identified by keys
* EBS is identified by address
* s3 is web enabled. regionally distributed
* Unlimited storage
* write once/ready many
* 99.999999999% durability
* The maximum object size for an object in Amazon S3 is 5 TB
* Can set permission and versioning on objects
* typically accessed over internet HTTPs
* secure by default. no access by deals
* access policies need to be configured
* can enable versioning
* life cycle policy (S3 frequently accessed(STD)/infrequently accessed - IA) i.e. STD and IA

**S3 Standard**

* Frequently accessed data
* stored in minimum 3 AZs

**S3 Standard IA Infrequent Access**

* in-frequently accessed data
* stored in 3 AZs

**S3 one-zone-IA**

* only in one AZ
* saves cost. store data which can be reproduced easily

**S3 Intelligent-Tiering**

* Ideal for data with unknown or changing access patterns
* Requires a small monthly monitoring and automation fee per object

**S3 Glacier**

* Low-cost storage designed for data archiving
* Able to retrieve objects from 3 minutes to 12 hours

**S3 Glacier Deep Archive**

* Lowest-cost object storage class ideal for archiving
* Able to retrieve objects within 12 hours

**Storage Gateway**:-

* a hardware or VM which you will run in on-prem and upload files to S3

**Amazon EFS - Amazon Elastic File System**

* regional resource
* multiple instance can read/write simultaneously
* Linux file system

**Managed & Un-Managed Database service**

**Amazon RDS database engines (managed service)**

* Amazon Aurora
* PostgreSQL
* MySQL
* MariaDB
* Oracle Database
* Microsoft SQL Server
* customer own network, data and schema

**Amazon Aurora**

* enterprise-class relational database
* compatible with MySQL and PostgreSQL
* up to five times faster than standard MySQL and up to three times faster than standard PostgreSQL
* Consider Amazon Aurora if your workloads require high availability
* replicates six copies of your data across three Availability Zones and continuously backs up your data to Amazon S3

**Amazon DynamoDB**

* no-SQL DB
* key-value database service. It delivers single-digit millisecond performance at any scale
* Serverless and auto scale

**Athena**

* to run SQL queries on S3. for analytics purpose

**Amazon EMR**

* Big data processing

**Amazon Kinesis**

* Real-time analytics

**Amazon Elastic MapReduce**

* to work on ApcheSparrk

**Amazon Redshiftt**

* data warehousing as service
* use for big data analytics

**DataLake**

* to bring data in once place

**Amazon DMS (data migration service)**

* for homogeneous db migration
* target can be EC2 or RDS
* for heterogeneous migration
* convert schema
* db migration
* development and test db migration
* db consolidation

**Amazon DocumentDB**

* (with MongoDB compatibility) - document database service

**Amazon Neptune**

* graph database service.
* to build and run applications that work with highly connected datasets, such as recommendation engines, fraud detection, and knowledge graphs.

**Amazon Quantum Ledger Database (Amazon QLDB)**

* ledger database service
* to review a complete history of all the changes that have been made to your application data

**Amazon Managed Blockchain**

* to create and manage blockchain networks with open-source frameworks.
* a distributed ledger system that lets multiple parties run transactions and share data without a central authority

**Amazon ElastiCache**

* a service that adds caching layers on top of your databases to help improve the read times of common requests
* 1)Redis and 2) Memcached

**Amazon DynamoDB Accelerator**

* an in-memory cache for DynamoDB
* helps improve response times from single-digit milliseconds to microseconds
* continuous DB replication

**Shared Responsibility Model**

* Security of the cloud. AWS Foundation Service - by AWS
* Security in the cloud. Customer data - customer

**AWS IAM**

* **Users** - root user has all permission. when creating new account, access can be given only to CLI(Key & secret) or Console. Controlled by identity and access management policy. policies can be applied to group as well
* **Group**
* **Roles** - not tied to user or group.
* Access Policies
* Identity federation / use RBAC
* MFA. must for root user and optional for normal users

**AWS Organization**

* central management of all AWS account using root account on parent container for all accounts
* consolidated billing
* Organizational Unit(OUs)hierarchical group of account
* IDAM policies can be applied at OU level
* AWS services and API action access control
* SCP service control policies

**Compliance**

* GDPR
* HIPAA
* AWS artifacts
  + a service that provides on-demand access to AWS security and compliance reports and select online agreements
  + consists of two main sections: AWS Artifact Agreements and AWS Artifact Reports
* AWS compliance

**Customer Compliance Center**

* contains resources to help you learn more about AWS compliance.
* an read customer compliance stories to discover how companies in regulated industries have solved various compliance, governance, and audit challenges

**Denial-of-service attack(DDoS)**

* is a deliberate attempt to make a website or application unavailable to users
* UDP Flood (low level attack) - solution:-security group. operates at AWS network level and not at EC2 level
* HTTP level attacks - ELB
* Slowloris attack

**AWS Shield**

* **Standard** - automatically protects all AWS customers at no cost.
* **Advanced** - a paid service that provides detailed attack diagnostics and the ability to detect and mitigate sophisticated DDoS attacks
* integrates with other services such as Amazon CloudFront, Amazon Route 53, and Elastic Load Balancing
* an integrate AWS Shield with AWS WAF by writing custom rules to mitigate complex DDoS attacks.

**Additional security service**

* **Encryption at rest**
* **Encryption at transit**
* **AWS Key Management** Service (AWS KMS) - enables you to perform encryption operations through the use of cryptographic keys.
* **AWS WAF** -
  + a web application firewall that lets you monitor network requests that come into your web applications
  + works together with Amazon CloudFront and an Application Load Balancer
* **Amazon Inspector**
  + helps to improve the security and compliance of applications by running automated security assessments
  + After Amazon Inspector has performed an assessment, it provides you with a list of security findings
  + Network config reachability piece
  + Amazon agent
* **security assessment service**

**Amazon GaurdDuty**

* is a service that provides intelligent threat detection for your AWS infrastructure and resources.
* It identifies threats by continuously monitoring the network activity and account behavior within your AWS environment

**Amazon CloudWatch**

* a web service that enables you to monitor and manage various metrics and configure alarm actions based on data from those metrics
* can create alarms that automatically perform actions if the value of your metric has gone above or below a predefined threshold
* CloudWatch dashboard feature enables you to access all the metrics for your resources from a single location

**AWS AuditTrial**

* records API calls for your account
* The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, and more

**CloudTrail Insights**

* This optional feature allows CloudTrail to automatically detect unusual API activities in your AWS account

**AWS Config** –

* keeps track of changes in AWS configuration

**Security Hub**

* give comprehensive view of security alerts across aws accounts. central view for alerts.

**Aws Macie**

* looks for PII in S3 through ML

**AWS Trusted Advisor**

* is a web service that inspects your AWS environment and provides real-time recommendations in accordance with AWS best practices
* compares its findings to AWS best practices in five categories: cost optimization, performance, security, fault tolerance, and service limits
* The green check indicates the number of items for which it detected no problems.
* The orange triangle represents the number of recommended investigations.
* The red circle represents the number of recommended actions.

**AWS Free Tier**

* Always free (Amazon lambda below 1 mn invocation/month)
* AWS Lambda allows 1 million free requests and up to 3.2 million seconds of compute time per month.
* Amazon DynamoDB allows 25 GB of free storage per month
* 12 months free (Amazon S3 up to 5GB std storage)
* specific amounts of Amazon S3 Standard Storage,
* thresholds for monthly hours of Amazon EC2 compute time
* amounts of Amazon CloudFront data transfer out.
* Trials (AWS Lightsail - 1 month
* trial upto 750hrs usage)
* Amazon Inspector offers a 90-day free trial.
* Amazon Lightsail (a service that enables you to run virtual private servers) offers 750 free hours of usage over a 30-day period

**Pay for what you use. -** pay for exactly the amount of resources that you actually use, without requiring long-term contracts or complex licensing

**Pay less when you reserve -** Some services offer reservation options that provide a significant discount compared to On-Demand Instance pricing

**Pay less** with volume-based discounts when you use more.

Some services offer tiered pricing, so the per-unit cost is incrementally lower with increased usage.

**AWS Pricing Calculator**

* lets you explore AWS services and create an estimate for the cost of your use cases on AWS.
* You can organize your AWS estimates by groups that you define. A group can reflect how your company is organized, such as providing estimates by cost center

**AWS Billing & Cost Management dashboard**

* to pay your AWS bill, monitor your usage, and analyze and control your costs.
* Compare your current month-to-date balance with the previous month, and get a forecast of the next month based on current usage.
* View month-to-date spend by service.
* View Free Tier usage by service.
* Access Cost Explorer and create budgets.
* Purchase and manage Savings Plans.
* Publish AWS Cost and Usage Reports.

**Consolidated billing**

* enables you to receive a single bill for all AWS accounts in your organization.
* By consolidating, you can easily track the combined costs of all the linked accounts in your organization.
* The default maximum number of accounts allowed for an organization is 4, but you can contact AWS Support to increase your quota, if needed
* benefit of consolidated billing is the ability to share bulk discount pricing, Savings Plans, and Reserved Instances across the accounts in your organization

**AWS Budgets**

* can create budgets to plan your service usage, service costs, and instance reservations.
* The information in AWS Budgets updates three times a day. This helps you to accurately determine how close your usage is to your budgeted amounts or to the AWS Free Tier limits
* can also set custom alerts when your usage exceeds (or is forecasted to exceed) the budgeted amount

**AWS Cost Explorer**

* is a tool that enables you to visualize, understand, and manage your AWS costs and usage over time.
* includes a default report of the costs and usage for your top five cost-accruing AWS services
* can apply custom filters and groups to analyze your data

**AWS Support plans**

* **Basic**
  + Limited selection of AWS Trusted Advisor checks.
  + can use the AWS Personal Health Dashboard, a tool that provides alerts and remediation guidance when AWS is experiencing events that may affect you
* **Developer**
  + Best practice guidance
  + Client-side diagnostic tools
  + Building-block architecture support, which consists of guidance for how to use AWS offerings, features, and services together
* **Business**
  + Use-case guidance to identify AWS offerings, features, and services that can best support your specific needs
  + All AWS Trusted Advisor checks
  + Limited support for third-party software, such as common operating systems and application stack components
* **Enterprise**
  + Application architecture guidance, which is a consultative relationship to support your company’s specific use cases and applications
  + Infrastructure event management: A short-term engagement with AWS Support that helps your company gain a better understanding of your use cases. This also provides your company with architectural and scaling guidance.
  + A Technical Account Manager

**AWS Marketplace:-** is a digital catalog that includes thousands of software listings from independent software vendors

**AWS CAF (Cloud Adoption Framework)**

**Business capabilities**

* **Business** - create a strong business case for cloud adoption and prioritize cloud adoption initiatives
* **People** - to evaluate organizational structures and roles, new skill and process requirements, and identify gaps. This helps prioritize training, staffing, and organizational changes.
* **Governance** - to understand how to update the staff skills and processes necessary to ensure business governance in the cloud. Manage and measure cloud investments to evaluate business outcomes

**Technical capabilities**

* **Platform** - includes principles and patterns for implementing new solutions on the cloud, and migrating on-premises workloads to the cloud
* **Security** - ensures that the organization meets security objectives for visibility, auditability, control, and agility
* **operations** - helps you to enable, run, use, operate, and recover IT workloads to the level agreed upon with your business stakeholders

**Migration strategies**

* 6Rs strategies for migration. based on time, cost and criticality
* Rehosting / Lift & Shift as-is. up to 30% saving. optimize later
* Replat forming - Lift-Tinker-Shift. like SQL to RDS
* Refactoring/re-architecting - Write new code
* Repurchasing - abandon legacy software and get new app
* Retain -
* Retiring - apps no longer-in-use and replacement app already running

**AWS Snow Cone**

* is a small, rugged, and secure edge computing and data transfer device.
* It features 2 CPUs, 4 GB of memory, and 8 TB of usable storage.

**AWS Snowball Edge Storage Optimized**

* **Storage**: 80 TB of hard disk drive (HDD) capacity for block volumes and Amazon S3 compatible object storage, and 1 TB of SATA solid state drive (SSD) for block volumes.
* **Compute**: 40 vCPUs, and 80 GiB of memory to support Amazon EC2 sbe1 instances (equivalent to C5).

**Snowball Edge Compute Optimized**

* Storage: 42-TB usable HDD capacity for Amazon S3 compatible object storage or Amazon EBS compatible block volumes and 7.68 TB of usable NVMe SSD capacity for Amazon EBS compatible block volumes.
* Compute: 52 vCPUs, 208 GiB of memory, and an optional NVIDIA Tesla V100 GPU. Devices run Amazon EC2 sbe-c and sbe-g instances, which are equivalent to C5, M5a, G3, and P3 instances.

**AWS SnowMobile**

* is an exabyte-scale data transfer service used to move large amounts of data to AWS.
* can transfer up to 100 petabytes of data per Snowmobile, a 45-foot long ruggedized shipping container, pulled by a semi-trailer truck.

**Other Amazon Services**

* **Amazon SageMaker** - enables you to quickly build, train, and deploy machine learning models
* **Amazon Textract** - is a machine learning service that automatically extracts text and data from scanned document
* **Amazon Lex** - is a service that enables you to build conversational interfaces using voice and text
* **AWS DeepRacer** - is an autonomous 1/18 scale race car that you can use to test reinforcement learning models.

**AWS Well-Architected Framework**

* helps you understand how to design and operate reliable, secure, efficient, and cost-effective systems in the AWS Cloud
* Operational Excellence - is the ability to run and monitor systems to deliver business value and to continually improve supporting processes and procedures
* Security - is the ability to protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies
* Reliability - is the ability of a system to do Recover from infrastructure or service disruptions, Dynamically acquire computing resources to meet demand, Mitigate disruptions such as misconfigurations or transient network issues
* Performance Efficiency - is the ability to use computing resources efficiently to meet system requirements and to maintain that efficiency as demand changes and technologies evolve.
* Cost Optimization - is the ability to run systems to deliver business value at the lowest price point.

**Benefits of the AWS Cloud**

* AWS Service
* AWS terminology
* 6 main benefits
* on-prem data center costs
* save money with aws by recommendation from trusted advisor
* lower variable cost
* stop guessing capacity
* Increase speed and agility.
* Stop spending money running and maintaining data centers.
* Go global in minutes

Prepared by: Saravanan Subbaiah