22CS2223 CLOUD INFRASTRUCTURE AND SERVICES

IMPORTANT KEYWORDS

CO1- Cloud Concepts

AWS Cloud Structure

----

cloud-> OnDemand resource sharing over internet or LAN.

Region->500mi,disaster recovery(natural disasters).

Availability zones->maintenance, high speed connectivity,99,one or more dc(data centre).

Edge Location->CDN, closest point, caching.

AWS Pillars

----

1. Operational Excellence->Development, run workloads efficiently, anticipate failure, small changes.

2. Security->IAM, Traceability, layers.

3. Reliability->failure recovery, Auto Scaling(elasticity).

4. Performance Efficiency->Advanced technology.

5. Cost Optimisation->stop heavy spending.

6. Sustainability->long term goals/carbon free environment

Agility->Improvise, fast.

Interacting with AWS

AWS Console

CMD or Terminal -> AWS Configure, Access key and Secrete key, IAM User Permission

Backing UP Data

Backup -> Automated, Replace same instances.

Snapshot -> point in time recovery, in new instance, manual, AMI (amazon machine image), AMI- EBS image.

Data Transferring

Snowball :- petabyte data transfer

Snowmobile:- exabyte data transfer.

Storage Gateway

Storage gateway :- like google photos with file storage gateway

volume Storage Gateway->Copies block by block.

Tape storage gateway->recording in cloud.

AWS Direct Connect -> on premises to AWS 100+ locations, dedicated connection, fast and secure transfer

AWS Glue -> serverless data integration service, discover, prepare, move and integrate data, provide data for analytics, ML, App development

CO2- Cloud Technology and Services

Compute Services

EC2 -> Virtual Machine, Server based, billing cycle start to stop.

Lambda -> serverless, microservices, function, billing only for listening, Lambda Layers, Lambda Environment Variables, event sources like S3, DynamoDB, SNS, HTTP endpoints.

Elastic Beanstalk :-EC2 with PAAS, internal load balancing, autoscaling, RDS, AWS takes care of provisioning, monitoring, and scaling infrastructure

AWS Batch-> running a job or in a batch of instances.

Light sail-> WordPress, templates, quick websites.

Workspace-> virtual desktop/laptop.

AWS Outposts - low latency on hybrid

Local zones - low-latency access, extension of an AWS region and may be used as an additional availability zone for redundancy.

wavelength - AWS compute and storage services to the edge of the 5G networks, ultra-low latency and high-performance application development for mobile and connected devices

AWS APP RUNNER - build, deploy, and scale containerized web applications quickly

AWS SIMSPACE WEAVER - create expansive simulation worlds at increased levels of complexity and scale.

AWS SERVERLESS APPLICATION REPOSITORY - developers to discover, deploy, and share serverless applications and application components, pre-built templates and components that can be easily deployed.

AWS Fargate - seamlessly with Amazon ECS and Amazon EKS (Elastic Kubernetes Service), which are container orchestration services

EC2 IMAGE BUILDER - creation, management, and deployment of AMIs

Networking

VPC -> Like a Nerwork, Virtual Private Cloud

Internet Gateway -> Attached to VPC

Subnet -> Public and Private Subnet

Subnet and Availability Zone -> Overlapping.

Public Subnet -> Internet traffic can access

Private Subnet -> Only VPC traffic and Internet traffic through NAT Gateway

NAT Gateway -> Network Address Translation, placed in public gateway, between private subnet and internet g/w

Routing Tables -> mapping IP (10.0.1.2) to subnet and making subnet as public or private

CIDR - Class Less Interdomain Routing (10.0.1.2/24)

ACL -> Access Control List, Stateless (setting both inbound and outbound traffic), precedence number based, top rule satisfied then bottom rule not checked, by default deny all traffic, you can set allow or deny

Security Groups -> at service level security check, stateful (configuring only inbound rules), any one rule should permit.

Cloud Formation-> Infrastructure as a code, JSON (or) .yml(yamal) templates, users stack(queue is not used) for creation and deletion.

SNS -> simple notification service, topic and subscribers, end point can be email, SMS etc.

SQS -> simple queuing service, Aws says do not build monolithic architecture, stores request and delivers to aws service, Supports loosely Coupled architecture.

Storage Services

S3 -> Used for flat storage, like a pen drive without installation support, cheapest storage in AWS, Static web hosting, uses cloud front for caching, having life cycle and storage classes

EBS -> Elastic Block Storage, supports installation, like a hard disk, can hold os, TFS(Typical to share), KMS Encryption

EFS -> Elastic File Sharing, efficient for sharing EFS to multiple ec2, hierarchal Structure(file Structure), provided all support like EBS, costly

Simple Storage Service S3

----

1. Standard :- Simply putting and accessing files.
2. Intelligence-Tiering:- Predicting Pattern
3. Standard Infrequent access :- When access is infrequent we use this
4. One zone in frequent Access :- only one zone, no backup, reduces cost.
5. S3 Glacier :- very cheap, more retrieve time ,very infrequent access in terms of months
6. S3 Glacier Deep Archive: -not accessing for years.

Aws Athena -> Query and analyse locks from S3, Cloud trial, Cloud Watch.

Caching Mechanism

Cloud Front -> edge location, CDN, used with s3, caching

DAX -> DynamoDB Accelerator, caching

Elastic Caching -> can be separate DB, attached in front of RDS, Redis and Memcached, costly and most efficient caching

Lambda@Edge -> cloud front for lambda service, only available to create in US-East-1 (N. Virginia) region

Routing Traffic

Route53 -> Routes traffic to AWS resources (under various policies->weighted routing, latency based routing, geographical routing, failure routing)

ELB -> elastic load balancer, also routes traffic to different ec2 instances.

AWS Global Accelerator -> routes traffic to the closest edge location

API Gateway -> It is URL based, Used to trigger lambda and other services.

Database

RDS-> Serverless, Charge For Listening/start to stop, Amazon Aurora(MYSQL,PostgreSql), MYSQL, PostGreSQL, mariaDB, Oracle, SQL Server.

Dynamo DB-> Serverless, No charge for listening, Query Execution Time Charged, Faster Than RDS, No SQL DB, Session Handling, Dax-Catch(Frequent Query).

Document DB-> Serverless, No SQL DB. Similar to MongoDB.

Elastic Catch -> Session Handling, Fastest DB, Costliest DB.

RedShift->Data Warehouse.

Other database

Amazon KeySpaces -> wide column

Amazon Neptune -> Graph

Amazon Timestream -> Time line based

Amazon QLDB -> Ledger

CICD(Continuous integration and Continuous deployment)

1.AWS Code Commit->Like github repository, has master branch for deployment, possible to create other branches for employee, unit testing will be in sub branches or(other branches), Integration testing will be in min branch.

2.Aws Code Built->Testing tool, alternate to Jenkins (testing tool),Build environment for testing, all successful built, it creates a artifact or jar file, push the jar to S3.

3.AWS Code deploy-> deployment service, picks artifact from S3 and deploys EC2/Lambda. On premises system/aws fargate, In place deployment(In existing system, downtime), blue-green deployment(0 down time, deploy in new instance).

4. AWS Code Pipleine-> Automate the trigger of code built and code deploy when master branch updated.

5.AWS Code Star-> Set ups complete pipeline with the pre defined applications which include code commit, deploy, build, only available in few regions.

6. AWS Fargate-> Serverless Computing instance to deploy containers.

7. AWS SAM-> Serverless Application Model, works with lambda, Synchronize local system code to Lambda on every save.

Containers

Docker image -lightweight, read-only template that contains everything needed to run a piece of software, including code, runtime (O.S Packages), system tools, libraries, and application dependencies.

Container - contains docker image, can be mount over kernel, can be deployed in any OS, Runnable or Deployable Product of Docker Image

ECR(elastic container registry)->stores the container and provides for ECS and EKS.

ECS(Elastic Container Service)->manages simple to moderate applications, free according to aws.

EKS(Elastic Kubernetes Service)->manages complex to large applications, high level scaling, expertise required, aws dashboard will charge, auto scaling.

CO3-Security and Compliance

Shared Responsibility

Customers Responsibility- Network level security (NACLs, security groups), operating system patches and updates, IAM user access management, and client and server-side data encryption.

AWS Responsibility- for protecting the infrastructure that runs all the services (compute, storage, database, networking, regions, availability zones)

Monitoring

AWS Cloud Watch -> Service level, installing cloud watch agent, custom metric for typical one, metric filter, maintain metrics and logs, dashboard view and graph, trigger alarm

AWS Cloud Trail -> User logs for last 90 days, Service creation, deletion

AWS X-Ray -> Monitoring inside code, instrumenting code manually, installing demon.

AWS Config -> record and normalize changes, check compliance, deploy rules and remediation across account, security monitoring.

personal health dashboard ->Monitors health of aws service, health of integrated services(EC2 with EBS), troubleshooting, quick(quicker troubleshoot).

Storing Password

Secrets Manager -> maintains password and more secure than system manager.

system manager -> password can be stored in parameter store as a secure string and referred as a parameter variable where required.

lambda environment variable -> stores password and uses with lambda, lambda will not go for other service to store password.

Encryption and Key Management

HSM -> Hardware security model, generate and use encryption keys, most secured, costly.

KMS -> Key management system, generate and manage keys, rotation of key possible, key for key possible

Security

Security -> Both aws and customer are responsible.

IAM Access Analyzer -> Who is having which access, recommend.

IAM Group, IAM User -> Access Permission for Employees

MFA -> Most Secured IAM, Mobile OTP

GaurdDuty -> Thread detection, monitor malicious activity, security findings (block), integrate with s3 and lambda for update the findings (list of troubling IP's).

Inspector -> automated Vulnerabilities, network exposure in ec2 and workloads

HSM -> Hardware security model, generate and use encryption keys, most secured, costly.

Cognito->provides application login (millions of users),user pool, password based, social media based, identity pool (between aws and end user),MFA possible(multi factor authentication).

AWS Shield -> protects against DOS and DDOS attacks over the server(DOS->Denial of service, DDOS->Distributed denial of service attacks).

AWS WAF -> web application firewall, protects against bots and exploits, have list of ip address to block

AWS Artifact -> on-demand access to security and compliance report

AWS License Manager -> maintains s/w license across aws services and on premises resources.

AWS Certificate Manager -> ACM provision, manage and deploy SSL/TLS (for https) certificate with AWS and internal connected services.

Amazon Detective -> simplifies investigation process, determine nature and extent of security issues

Occasional Services

Amazon AppStream 2.0 - secure access to desktop applications

Amazon Elastic Transcoder - CONVERT TO FORMAT Play on multiple devices

Amazon Comprehend - sentiment analysis

Amazon Rekognition - machine learning capability

AWS Compliance Program - regional regulatory requirements

Amazon QuickSight - visual reports (like graphs)

AWS Service Quotas - service limit

Amazon Polly - text to speech

CO-4 Billing, Pricing, and Support

Aws support Plan

1.basic-free tier, only general Questions (documentation, whitepapers, and support forums)

2.Developer plan: -suitable for testing and experiment, possible with technical questions. (email support during business hours, with a response time of up to 12 hours)

3.Enterprise on ramp-suitable for production and critical work loads.

4.Business plan: -suitable for production workload (email support during business hours, with a response time of up to 12 hours)

5.Enterprise: -suitable for machine critical workload (dedicated Technical Account Manager (TAM)

AWS Management Service and Professional service

Management Service:- response within 24hrs, maintenance, trouble shooting, networking, security.

Professional service: - Immediate response, dedicated aws person, consultancy, migration, deployment, advanced trouble shooting(supports us in developed aspects).

EC2 Purchasing

- On-Demand Instances – Pay, by the second, default one
- Savings Plans –consistent amount of usage, in USD per hour, for a term of 1 or 3 years.

- Reserved Instances –Commitment to a consistent instance configuration, including instance type and Region, for a term of 1 or 3 years.
- Spot Instances – Request unused EC2 instances, which can reduce your Amazon EC2 costs significantly. 90% discount and frequent interruption may happen.
- Dedicated host:- Separated hardware (per-socket, per-core, or per-VM software licenses)

Management and Billing

AWS Organization: centrally manage policies across multiple AWS accounts, automate account creation, and consolidate billing.

AWS pricing Calculator :- Cost Estimation, input architecture(like EC2,Lambda),output estimated cost.

AWS budget:- used to set budget limits and predict future by observing current usage alerts through SNS when alarm triggers

AWS cost explorer :- Maintains report upto two years, visualize in graphical format, breakdown the reports by account ,subaccounts, teams, producers one report for 24hrs.

AWS cost and usage Management:- Device report by hours, day and month and also by tags, produce 3 reports per day, sends reports to S3,create,retrieve delete reports are possible.

Total Cost of Ownership (TCO)- overall expenses associated with owning and operating IT infrastructure.

AWS marketplace: -place to search software as a service, third party service

Amazon Kinesis -> live data gathering (like twitter, facebook),real time, uses shades as queue(Buffer memory).

Trusted Advisor- Real-time assistance in cost optimization, performance, security, fault tolerance, service limits.