AWS 2 → Solution architect Associat | SAA-C02

Date / / No

AVaiability Zone → is data Center
↓ is a building fired with servers

Edge location → are end Points for AWS. that are used for Caching Content. this consists of Cloud front Amazon's CDN

IAM is Unversal : It doesn't apply to regions at this time
The Root Account: it is created when you first set up your AWS account and it has complete admin access.

S3 is object-Based-Storage
↳ Provide Secure, durable, highly Scalable object Storage
↳ allows you to store and retrieve any amount of data.
↳ Simple → is easy to use

* high availability and Durability
* Designed for frequent Access
* Suitable for Most Workloads

* all Version are Stored is S3

life cycle Managment : automates moving your objects between the different Storage tiers, thereby maximizing cost effectiveness

S3 object lock → You can use it to store objects using a write once read many (WORM) model. It can help prevents objects from deleting or modifing for a fixed amount of time
↳ use it to meet regulatory requirements that require WORM Storage, or add an extra layer of protection against object changes and deletion.

Date / / No

S3 object lock Modes

(1) Governance Mode : users can't overwrite or delete an object version or alert its lock setting unless they have Special Permissions.

* With governance mode, you protect objects against being deleted by most users, but you can still grant some users permission to alter the retention settings or delete the object if necessary

Retention Periods protects an object version for a fixed amount of time

Amazon S3 stores a timestamp in the object version's metadata to indicate when the retention period expires.

* After it expires, object version will be overwritten or deleted unless you placed legal hold on the object version.

Prevents an object version from being overwritten or deleted.

Can be placed and removed by any user who has S3:PutObjectLegalHold permission

Glacier Vault lock to easily deploy and enforce compliance controls for individual S3 Glacier Vaults with a Vault lock Policy

(2) Compliance Mode : a protected object version can't be overwritten or deleted by any user, including the root user in your AWS account

Date / / No

Types of Encryptom

1. Encryptom in Transit : SSL / TLS - HTTPS
2. ~ at Rest : Server-Side Encryptom
   - SSE-S3 : manged keys using AES 256-bit encryptom
   - SSE-KMS : AWS Key Management Service - manged keys
   - SSE-C : Customer - Provided keys.
3. Encryptom at Rest : Client-Side Encryptom
   You encrypt the files yourself before you upload them to S3

Enforcing Server-Side Encryptom → by
- Console
- Bucket Policy

S3 Replicatom

1. You can replicate objects from one bucket to another.
2. objects in an existing bucket are not replicated automatically.
3. delete markers are not replicated by default.

Remember when you use roles :
1. Preferred optm
2. Avoid Hard-Coding your credentials
3. Policies
4. Updates
5. Attaching and detaching

Security Groups

are virtual firewalls for your EC2 instance.. By default everything is blocked
to let everything in 0.0.0.0/0

Date ..../..../.... No ....

Bootstrap scripts :- script that runs when instance first runs

User data is simply bootstrap scripts
Meta data is about your EC2 instances.
You can use bootstrap scripts (user data) to access metadata

Networking With EC2

You can attach 3 different types of virtual networking cards to your EC2 instances.

ENI	EN	EFA
Elastic Network Interface	Enhanced Networking	Elastic Fabric Adapter
day to day networking	uses single root I/O Virtualization (SR-IOV) to provide high Performance	Accelerate high Performance computing (HPC) and machine learning apps

3 Types of placement group

* cluster placement groups
* Partition placement groups
  - Multiple EC2 instances HDFS, HBase and Cassandra
* Spread placement groups
  - individual critical EC2 instances

* You can't merge Placement group
  You can move an existing instance into a placement group

Date ..../..../.... No ....

Spot Fleets is a collection of spot instances and optionally on demand Instances.

↳ attempts to launch the number of spot instances and on-Demand instances to meet the target capacity you specified in the request.

EBS → Elastic Block Store
Storage volumes you can attach to your EC2 instance

① gp2: General Purpose SSD
Suitable for boot disks and general apps → up to 16000 IOPS per volume

② gp3: General Purpose SSD
for high Performance apps → to 3000 IOPS / 125 MiB/s of size

③ io1: Provisioned IOPS SSD.
for OLTP and latency-sensitive apps. → 50 IOPS / 6 GiB
up to 64000 IOPS per volume

④ io2: Provisioned IOPS SSD
for OLTP ——— , 500 IOPS / 6 GiB

Volumes are virtual hard disks.
You need a minimum of 1 volume per EC2 instance
↳ this is called the root device volume

SnapShots exist on S3
are point in time
are incremental

Date ..../..../.... No ....

Encrypted volumes

* Data at rest is encrypted inside the volume
* all data in flight moving between the instance and the volume is encrypted
* All Snapshots are encrypted
* All volumes created from the snapshot are encrypted

EC2 Hibernation

* When you hibernate an EC2 instance, the operating system is told to perform hibernation (suspend-to-disk)
* Hibernation saves the contents from the instance memory (RAM) to your Amazon EBS root volume.

FSx for windows

Provides a fully managed native Microsoft Windows file system so you can easily move your windows ~~file system~~ based applications that require file storage to AWS

EFS → a managed NAS for EC2 instances based on Network file system
one of the first Network file sharing protocols native to Unix an Linux.

FSx for Lustre

a fully managed file system → optimized for Compute intensive workloads → High Performance, Machine learning, Media Data

Date / / No

OLAP	OLTP
Online analytical Processing	online transaction Processing
Process complex queries to analyze historical data	Process data from transactions in real time
~~Customers orders, banking~~ analyzing net Profit figures from 3 years and sales forecasting	Customers order, banking transaction Payment, booking system
is all about data analysis using large amount of data, as well as Complex queries that take a long time to complete	is all about data Processing and Completing large numbers of small transactions

Read replica is a read-only copy of your Primary data base.
* great for read-heavy workloads and takes the load off your primary data base.
* Copy databases in the same AZ, cross A-Z or cross-region

Multi AZ
an exact copy of your Production database in another Availability zone, used for disaster recovery
* in the event of a failure, RDS will automatically fail over to the standby instance.

Aurora is MySQL and PostgreSQL-compatible relational database engine that combines the speed and availability of high-end commercial databases with the simplicity and cost effectiveness of open-source databases

* Scaling → Storage is also self-healing.

Dar Kareem

Aurora

Date ... / ... / ... No ...

* You Can Share Aurora SnapShots with other AWS accounts
* 3 types of replica

Aurora replicas : MySQL replicas : PostgreSQL replicas

DynamoDB

* is a fast and flexible NoSQL database service for all apps
* It is a fully managed database and supports both document and Key-Value data models.
* Stored on SSD storage, spread across 3 geographically distinct data centers

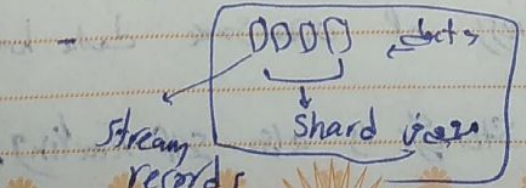
Eventually Consistent Reads

Eventually consistent reads
Consist across all copies of data is usually reached with a second.

Strongly consistent reads
returns a result that reflects all writes that recieved a successful response prior to the read

Point in time Recovery (PITR)
* restore to any point in last 35 days
* incremental backups
Protects against accidental writes or deletes
latest restorable: 5 minutes

Streams
* time ordered sequence of item-level changes in a table
Stored for 24 hours



Dar Kareem

Date / / No

VPC — Virtual data center in the Cloud

* isolated Part of AWS where you can define your own network
* Complete Control of virtual network, including your own IP address

We can do with VPC : 1- launch instances 2- internet gateway
3- custom IP Adress 4- Route tables
5- More Control 6- Access Control lists

NAT GateWays You can use a network address translation to enable instances in a private Subnet to connect to the internet or AWS services

* Security Groups are Virtual Firewalls for an EC2 instance
By default every thing is blocked

ACL
* Your VPC automatically comes with a default network ACL
* You can create Custom network Acls
* " " block IP addresses by Acl
* each Subnet in your VPC must be associated with ACL

End Points → are Virtual devices, they are horizontally Scaled redundant, and highly available VPC Components that allow Communication between instances in your VPC and Services without imposing availability risks or bandwidth constraints on your network traffic

Interface End Points
is an Elastic network interface with Private Ip address.

Gateway EndPoints
Similar to NAT Gateway
* is Virtual device you Provision

Date ..../..../.... No ....

AWS VPN Cloud Hub

if you have multiple sites, each with its own VPN Connection you can use AWS VPN CloudHub to connect those site together. It is Similar to VPC Peering in that it works on a hub-and-spoke model.

Direct-Connection is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS

Private Connectivity using AWS direct-Connect: you can establish private connectivity between AWS and your dat center or office

transit Gateway → connects VPCs and on premises networks through a central hub.

DNS → to Convert domain name into IP addresses

IPV4: 32-bit, only 4 billion address ← IPV6: Created to solve this, ~~64 b~~ 128 bits, have 340 undecillion رقم قدامه 38 صفر

address Record: is the fundamental type of DNS record.

* is used by computers to translate the name of the domain to an IP address

TTL → time to live → length that DNS record is cached on either the resolving server or the user's own local PC is equal to TTL in seconds

Dar Kareem

Date / / No

CNAME : Canonical name → can be used to resolve one domain name to another. Can't be used for naked domain name;

Alias Records : are used to map resource record sets in your hosted zone to load balancers or S3 buckets.
Can be used for naked name

Weighted Routing Policy : allows you to split your traffic based on different weights assigned.

Failover Routing Policy : are used when you want to create an active / Passive set up.

Elastic load Balancing → automatically distributes incoming app traffic across multiple targets such as Amazon EC2 instances, this can be done across multiple AZs

layer 7 | layer 4 | layer 4/7

Application load Balancer
intelligence
You can enable Sticky sessions

Network load Balancer
Performance

classic load Balancer
classic | Test
Dev

Sticky Sessions : allows you to bind a user's session to a specific EC2 instance

Date / / No

Deregistration Delay : allows load Balance to keep existing connection open if the EC2 instances are de-registered or become unhealthy.

* Cloud Watch is the main tool for anything alarm related.
* Not every thing should go through Cloud Watch. ~~We don't~~
* the Standered metric is delivered every 5 minutes, while detailed monitoring delivers data every 1 minute
* Cloud Watc logs is the Place for logs.

Templates	Configurations
More than auto Scaling	only for auto Scaling
Supports Versioning	Immutable
More granularity	Limited Configuration options
Aws recommended	don't use them

Scaling Types

Reactive Scaling — Scheduled Scaling — Predictive Scaling

Relational Database Scaling

* Read replicas
* Vertical Scaling
* Aurora Everything
* Careful with Storage
* Multi-AZ

Date ... / ... / ... No ...

SQS :- Simple Queue Service is a messaging queue that allows asynchronous processing of work. One resource will write a message to an SQS queue and then another resource will retrieve that message from SQS

SQS Setting :-

- delivery delay → up to 15 minutes
- message size → 256 KB
  - Encryption
  - message Retention : 4 days → can be set between 1 minute and 14 days
  - long Polling isn't the default
  - Queue Depth

DLQ : Dead Letter Queues are the best sideline
- Monitor
- It is not special → are just SQS queues to receive the reject messages
- Same Retention window up to 14 days
- Usable with SNS

Fifo Queue → the only option → to message ordering

SNS : is a Push-based messaging service. it deliver messages to the end Points subscribed to it.

Date ... / ... / ... No ...

The 3 V's of Big Data

Volume
ranges from terabytes of Peta bytes of data

Variety
includes data from a wide range of sources and formats

Velocity
Businesses require speed. Data needs to be collected, stored, processed and analyzed with a short period of time.

Redshift : is a fully managed, Petabyte-Scale data warehouse service in the cloud. It's a very large relational database traditionally used in big data ~~apps~~ apps

Elastic MapReduce

EMR → is a managed big data platform that allows you to process vast amounts of data using open-source tools such as Spark, Hive, HBase, ...

Kinesis → allows you to ingest, process and analyze real-time streaming data.

Data Streams
Real time streaming for ingesting data

Data Firehose
Data transfer tool to get information to S3, Redshift --

* You are responsible for creating the Consumer and Scaling the Stream

* Plug and Play with Aws Architecture

Date ..../..../.... No ....

Athena is an interactive Query Service that makes it easy to analyze data in S3 using SQL.

Glue: is a Serverless data integration service that makes it easy to discover, Prepare, and combine data. It allows you to Perform ETL workloads Without managing underlying servers

QuickSight:- is a fully managed business intelligence (BI) data visualization service. It allows you to easily create dash boards and share them within your company

Elastic Search:- is a fully manged Version of the open source app Elastic Search. allows you to quickly search over your stored data and analyze the data you get back

Fargate: a Serverless compute engine for containers
works with ECS and EKS.

Event bridge:- Serverless event bus. it allows you to pass events from a source to an end point
It is the glue that holds your serverless app together

DDoS Attack: Distributed Denial of service attack
→ attempts to make your website or app unavailable to your end users

layer 4 DDoS attack: referred to as a SYN Flood.
It works at the transport layer (TCP)

SYN floods uses the built in allocation of TCP stack to overwhelm a server by sending a large number of SYN packets and then ignoring the SYN-ACKs returned by the server.

Layer 7 Attack : occurs when a web server receives a flood of GET or POST requests usually ~~a flood~~ from a botnet or a large number of compromised computers.

CloudTrail → increase visibility into your user and resource activity by recording AWS Management console actions and API calls

Shield : free DDOS protection
WAF : web application firewall → lets you monitor HTTP and HTTPS request.

GuardDuty is threat detection service that uses machine learning to continously monitor for malicious behavior

PII : Personally Identifiable Information

* Personal data used to establish an individual's identity
* this data could be exploited by criminals, used in identity theft and financial fraud

* Macie uses machine learning and pattern matching to discover sensitive data stored in S3

Date / / No

Amazon Inspector :- is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS.

KMS :- Key Management Service → makes it easy for you to create and control the encryption keys used to encrypt your data.

CMK :- Customer master key
is a logical representation of a master key.
* CMK includes metadata, such as the key ID creation date, description, and key state

HSM : Hardware security module : is a physical computing device that safeguards and manages digital keys and performs encryption and decryption functions.

* All KMS CMKs have a key policy

Cloud HSM : is a cloud based HSM that enables you to easily generate and use your own encryption keys on the AWS Cloud.

Secret Manager :- is a service that securely store, encrypts and rotates your database credentials and other secrets.
* reduce risk of credentials being compromised.

Date ..../..../.... No ....

Parameter Store : is a capability of AWS systems Manager that provides secure, hierarchical storage for configuration data management and secrets management.

* All objects in S3 are Private by default.

(ARNs)
Amazon Resource Name

arn : Partition : Service : region : account-id : resource type /resource

Partition → aws | aws-cn
Service → S3, ec2, rds
region → us-est-1
account-id → 123495678

AWS certificate Manager allows you to create, manage, deploy Public and Private SSL certificates for use with other AWS services

DAX → to Dynamo DB, only when you store data in this service
Elasticache → gives you a bit more flexibility. It can front just about any data base.

Organizations : is a free governance tool → allows you to create and manage multiple AWS accounts.
* You control your accounts from a single location rather than Jumping from account to account

Date / / No

AWS RAM → Resource Access Manager.
is a free service that allows you to share AWS resources with other accounts

Cross-Account Role Access
as the number of AWS accounts increases, you will need to set up cross-account access
* gives you the ability to set up temporary access you can easily control

Directory Service → allows you to offload the painful parts of keeping AD online to AWS while still giving you the full control and flexibility AD provides

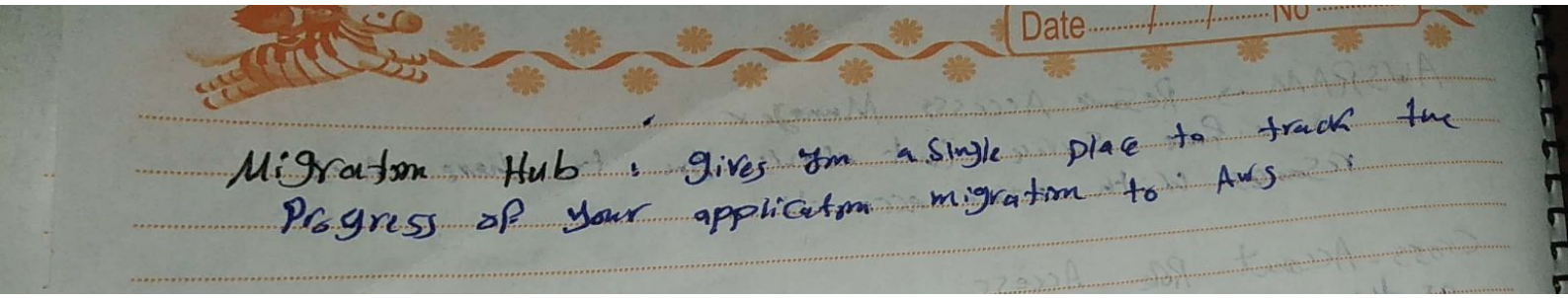
Budgets → allows organizations to easily plan and set expectations around cloud costs.

Snow-family: is a set of secure appliances that provide petabyte-scale data collection and processing solutions at the edge and migrate large-scale data into and out of AWS

Data-Sync, is an agent-based solution for migrating on premises storage to AWS. it allows you to easily move data between NFS and SMB
* is a Migration Service

Transfer family: allows you to easily move files in and out of S3 or EFS using secure file transfer protocol SFTP, FTPS, FTP

Dar Kareem



Migration Hub : gives you a single place to track the progress of your application migration to AWS.