AWS Developer – Cheat Sheet

API Gateway

- HTTP, WebSockets, REST API
- HTTP : Easy to create. Typically Lambda backend
- WebSockets to used when connection oriented tasks/apps like Chat or continuous update of Dashboards
- REST : You want complete control over all aspects. Want to integrate services directly like S3, SQS, SNS, DynamoDB etc.
- Deployment : Manual and Automatic
- Deployment : Deployment in Stages. You can pass parameters called stage parameters
- Security :
    - Lambda authorization
    - JWT authorization (can be integrated with Cognito)
- General: If not using SDK, the REST HTTP must have a SigV4 signature
- AppSync service: For GraphQL queries.

Lambda

- Serverless service
- Synchronous and Asynchronous
- API Gateway – Lambda is synchronous. API Gateway waits for the return value
- S3, SQS, SNS – Asynchronous
- Lambda can also be invoked as a schedule
- Versions in Lambda. The latest version is called $LATEST
- Alias – Connects a particular version as an Alias
- Deployment – Alias is used for Canary deployment
- Deployment – Lambda can be deployed behind an Application Load Balancer
- Layers – Layers are like common functions which you can load and point to. This helps keeping your code smaller.
- Limitations:
    - 15 mins is the max run time
    - 10 GB is the max memory
    - Max size of deployment : 200 or 250 MB
- Lambda in S3 : Object Lambda Endpoint. Lambda is executed when you try to access an object
- Security : Role is necessary to give permission to Lambda to access certain services

S3 Storage

- Object storage
- REST APIs (built on HTTP)
- Buckets / Objects / Object Keys
- Buckets can be used to host a static website
- S3 Events : Events can be handled directly (S3 to Lambda, S3 to SQS, S3 to SNS)
- S3 Events : EventBridge can be used to handle S3 events
- Difference: Direct event handling has only a single target. Eventbridge has upto 5 targets

- Security :
    - CORS (Cross Origin Resource Sharing)
    - Policies to ensure only specified people can access the bucket
    - We can our bucket either private or public (default is private)
    - Pre-signed URL to access private content

SQS

- Simple Queue Service
- Standard and FIFO queues
- FIFO : Limitation is 300 transactions per second
- Dead Letter Queue for messages that have some problem
- Short and Long Polling
- Visibility time (upto 12 hrs. 30 secs the default)
- Concept of delay queues
- Integrations: Lambda triggers (Lambda reads from the queue and also deletes the message after processing the message. We have to give the processing logic.)
- Security : Based on policies which allow or disallow certain users

Kinesis Streams

- Kinesis : Kinesis Streams, Kinesis Firehose, Kinesis Analytics, Kinesis Video Streams
- Kinesis Firehose : It takes data from the Kinesis stream and stores in some destination like S3, EMR etc. This is done without us having to write any code.
- Kinesis Analytics : Lets you query the stream in real time using SQL
- Kinesis Stream is made up of shards
- Each shard has different read and write capacity
- Each shard supports upto 2 MB read/sec
- Each shard supports upto 1 MB write/sec
- Read capacity is shared by all application reading from the same stream. If fan out is chosen, each application gets 2MB/sec read capacity
- Partition key is used to select which shard the data is written to. The no:of partition keys should be at least equal to the number of shards or greater.
- Security : Based on policies
- Integration : Lambda function. Lambda will read the messages.
- KCL : Kinesis Client Library to be used for ease of programming

DynamoDB & NoSQL

- Four types of NoSQL
    - Key Value : DynamoDB, ElasticCache (Redis/Memcached)
    - Document : DocumentDB (MongoDB compatible)
    - Graph DB : Neptune
    - Columnar DB : Redshift
- DynamoDB managed NoSQL DB and has no storage limits
- Key Value database
- Primary Key
    - Simple Key : Partition Key
    - Composite : Partition Key and Sort Key
- Two types of reads:

    - Eventually Consistent
    - Strongly consistent read
- Read and Write throughputs
    - Read throughput : 1 unit to read of one item (upto 4 KB) strongly consistent or 2 items of eventual consistent read (upto 4 KB per item)
    - Write throughput: 1 unit of write of one item (upto 1 Kb)
- Secondary Index
    - Global Secondary Index (GSI)
    - Local Secondary Index (LSI)
- DAX : DynamoDB accelerator – In memory cache for sub million read responses
- DynamoDB Streams : Integrate with Lambda
- DynamoDB changes can also be put into Kinesis stream

Security

- Roles
- For storing secrets
    - Secrets Manager
        - Automatic rotation of keys possible
    - System Manager Parameter Store
- Encryption
    - KMS
        - Master Key
        - Data Key
        - Envelope encryption
    - Rotate Keys in KMS
- IAM for Application
    - Cognito
    - User Pools
        - Authentication
        - Also for 3rd party authentication like Google, Facebook etc
        - Uses OAuth protocol (or OpenID)
    - Identity Pools
        - Authorization
        - Can provide temporary credentials
- AWS Cloudwatch Logs
    - You can send logs to cloudwatch
    - Get metrics from the logs
- X-Ray
    - For API Gateway and Lambda functions

Microservices Deployment

- EKS (Elastic Kubernetes Service) – Managed Kubernetes service
- ECS (Elastic Container Service) –
    - Container Def
    - Task Def
    - Service
    - Cluster

- ECS works in two modes
    - EC2 Cluster
    - Fargate
- Integrated with both Load Balancer and Autoscaling of AWS

Web Application Deployment

- Elastic Beanstalk (PaaS)
- Automatic deployment
- Multiple kinds of deployment
    - Rolling Updates
    - Rolling with Additional Batch
    - Immutable
    - All at once
- Blue / Green deployment
- .ebextensions to customize the environment
- Swap URL for Blue Green Deployment

Other services

- Code Build for automated serverless code build
- Code Deploy to deploy on EC2 Instances / Elastic Beanstalk / ECS
- Code Pipeline for CICD