aws Training Notes 2020 ACSAA

by Neal Davis

[H2] PREREQUISITES

[H3] The Exam Blueprint

The exam includes 65 questions to be answered within 130 mins.
To pass, score ≥ 720 out of 1000 points.
Question formats:

1. Multiple choice: one right answer from four options
2. Multiple responses: two or more correct answers from five or more options

Note that there can be multiple correct answers but you must select the answer that best fits the scenario, e.g. MOST secure, MOST cost-effective, LEAST complex, etc.

[H3] Domains & Objectives

Domain 1. Design resilient architectures (30%)
- Design a multi-tier architecture solution
- Design a highly available and/or fault-tolerant architecture. (Amazon Elastic Load Balancing, Amazon Route 53, Amazon RDS Read Replicas, Multi-AZ.)
- Design decoupling mechanisms (Amazon SQS, Amazon SWF)
- Choose appropriate resilient storage (Amazon EBS, Instance Store, Amazon EFS, Amazon S3, and Amazon FSx)

Domain 2. Design high-performing architecture (28%)
- Identify elastic and scalable compute solution (EC2 Auto Scaling)
- Select high-performing ~~storage~~ storage/database solution (storage solution like DDB, S3, etc. caching layer like Amazon ElasticCache, Amazon DynamoDB DAX, Amazon CloudFront)
- Select high-performing networking solution

Domain 3. Design secure applications and architectures (24%)
- Design secure access to AWS resources. (users, groups, and roles in AWS IAM, which services can use multi-factor authentication (MFA), AWS Directory Services)
- Design secure application tiers. (Amazon EC2 instance deploy options, ~~Attt~~ Amazon VPC configurations; DDoS mitigation with AWS Auto Scaling, Amazon CloudFront, Amazon Route 53; Monitor and logging with Amazon CloudWatch and AWS CloudTrail; Penetration testing with AWS cloud; compliance programs, etc.)
- Select appropriate data security options. (Amazon VPC, AWS KMS, AWS CloudHSM, AWS IAM, Amazon Cognito, and AWS Directory Services.)

Domain 4. Design cost-optimized architecture (18%)
- Identify cost-effective compute services. (EC2 spot/reserved/on-demand)
- Identify cost-effective storage and database solutions.
- Design cost-optimized network architectures (Amazon CloudFront)

H2 COMPUTE

H3 Amazon EC2

AWS are transitioning to a vCPU based, rather than instance based, limit.

Key pairs are used to secure connection to EC2 instances.

- A key pair contains a public key AWS stores, and a private key file that you store.
- For Windows AMIs, the private key file is to obtain the password used to log into your ~~root~~ instance. While for Linux AMIs, the private key file is for secure SSH.

Metadata and User data:

- Metadata is the data about your instance configuration
- User data is < 16 KB script you can provide to run when starting an instance.

Billing and Provisioning:

1. On-demand:
   - Pay for hours used without commitment
   - Ideal for auto-scaling groups and unpredictable workloads.
   - Good for dev / test
2. Reserved:
   - Purchase EC2 instances in advance for 31% ~ 60% discounts comparing with on-demand instances.
   - Need a commit of 1 or 3 years.
   - RIs are used for steady state workloads and predictable usage.
   - Can sell reserved instances on the AWS marketplaces.
3. Spot:
   - Spot instances let you take advantage of unused EC2 capacities in AWS cloud, with a 90% discount comparing with on-demand.
   - Can be terminated at any time with a 2-min interruption notice.
   - Good for stateless, fault-tolerant, or flexible applications.
   - New pricing model: price is determined by long term trend in supply and demand for EC2 spare capacity.

Amazon Machine Images (AMI) provides information required to launch an instance. An AMI includes:

- A template for the root volume of the instance. (e.g. OS, application server, and applications)
- Launch permissions on which AWS account can use the AMI.
- A block device mapping to specify the volumes to attach to EC2.
  - EBS (Elastic Block Store). EBS snapshots reside on S3.
  - Instance store. It is non-persistent that will be lost once the instance is shut down. Also uses S3 underlying.

IP Addresses for EC2:

- Elastic IP addresses are static public IP addresses that can be remapped (moved) between instances.
- By default, EC2 instance comes with a private IP assigned to the primary network interface (eth0)

ENI v.s. ENA v.s. EFA

1. ENI (Elastic Network Interface) is a basic logical networking component in a VPC that represents a virtual network card. It contains:
   - A primary private IPV4 address from your VPC IPv4 range;
   - One or more secondary IPv4 addresses.
   - One elastic IP address per private IPv4 address.
   - One public IPv4 address
   - One or more IPv6 addresses.
   - One or more security groups.
   - A MAC address
   - A source/destination check flag
   - A description

2. ENA (Elastic Network Adapter) is used for enhanced networking. ENA should be considered if your packet per-second rate appears to have reached its ceiling. AWS currently supports this by using SR-IOV.

3. EFA (Elastic Fabric Adapter) is an AWS Elastic Network Adapter (ENA) with added capabilities.
   - EFA supports an important access model commonly called OS bypass.
   - This model allows the application (most commonly through some user-space middleware) access the network interface without having to get the operating system involved with each message.
   - With EFA, High Performance Computing (HPC) applications using the Message Passing Interface (MPI, MPI is another mechanism/philosophy comparing with Apache Spark) and Machine Learning applications using NVIDIA Collective Communications Library (NCCL) can scale to thousands of CPUs or GPUs.

- ENI VS ENA VS EFA
  - When to use ENI: This is the basic adapter type can be used with all instance types.
  - When to use ENA: Good to use cases the require higher bandwidth and lower inter-instance latency. Support for limited instance types (HVM only).
  - When to use EFA: For high performance computing, MPI and ML use cases, tightly coupled applications, and can also be used with all instance types, like ENI.

EC2 migration

- VM Import/Export is a tool for migrating EC2 instances to VMware, Microsoft or XEN VMs. It can also migrate the other way around.
- AWS Server Migration Service (SMS) is an agent-class service which makes it easier and faster to migrate thousands of on-premises workloads to AWS.

High Availability approaches for compute

- Horizontally scalable architectures are preferred because risk can be spread across multiple smaller machines v.s. one large machine.
- Reserved instances are the only way to ensure the resources are always available ~~way~~ when you need it.
- Auto scaling + Elastic Load Balancing to provide automated recovery as well as maintaining minimum instances.
- Route 53 also provides "self-healing" by redicting traffics.

H3 Amazon EBS

EBS stands for Elastic Block Store, EBS volumes are network attached storage that can be attached to EC2 instances.

EBS volume data persist independently of the life of instance. But note that by default, termination protection is turned off and must be manually enabled to persist your data after terminating an EC2 instance.

EBS volumes do not need to be attached to an instance.

Instance store

- Instance Store provides temporary (non-persistent) block-level storage for your instance. You can specify instance store volumes for an instance only when you launch it.
- This is a good option when you need very high performance/latency but you don't need the data to persist when your instance terminates, or you can take advantage of fault-tolerant architectures.
- △ Exam tips: Look out for Qs that mention distributed or replicated databases that need high I/O. It is also cost-effective as instance store cost is included in the instance charges so cheaper than EBS.

EBS v.s. Instance Store

- EBS-backed means the root volume is an EBS volume and storage is persistent.
- Instance-store-backed means the root volume is an instance store volume and storage is not persistent.
- Instance store volumes cannot be detached/reattached.
- By default, both volumes will be deleted on termination unless you configured otherwise.

although save is incremental, EBS snapshot is designed in the way that with "deletion", you just need to persist the latest snapshot.

Snapshots

- Snapshots capture a point-in-time state of an instance.
- Use cases:
  1. as a back-up strategy. Note that if you set up recurring snapshots, the snapshots are incremental, meaning the later snapshots contain only incremental changes only.
  2. Share datasets with other users or accounts.
  3. Migrate a system to a new AZ or region.
  4. Convert an unencrypted volume to an encrypted one.
- Snapshots are stored in S3, and hence region specific instead of AZ specific (unlike EBS which is AZ specific)

Encryption of EBS

- Expect the same IOPS performances on encrypted and unencrypted volumes.
- Encryption key can be either the default KMS, or KMS CMK, which uses AES-256 encryption algorithm.
- There is ~~not~~ no direct way of changing the encryption state of a volume.
- You cannot change the CMK key that is used to encrypt a volume.

RAID: can be used to increase IOPS

- RAID 0 = 0 striping — increased performance, no redundancy
- RAID 1 = 1 mirroring — with redundancy, no increase for performance
- RAID 10 = 10 combined of 1 and 0, at the cost of distributed disks.
- EBS optimized EC2 is another way of increasing performance.

H3 Elastic Load Balancing

Elastic Load Balancing automatically ~~et~~ distributes incoming application traffic across multiple targets, such as EC2 instances, containers, and IP addresses.

Three types of ELB on AWS:

1. CLB, classic Load Balancer: the oldest, in the way to be deprecated, provides both layer 4 and layer 7 load balancing. HTTP/HTTPS/TCP/SSL
2. ALB, application Load Balancer: layer 7 at HTTP/HTTPS protocals.
3. NLB, network Load Balancer: layer 4 at TCP/TLS/UDP/TCP_UDP

Only 1 subnet ~~or~~ per AZ can be enabled for each ELB.
Route 53 can be used for region load balancing with ELB instances configured in each region.

ELBs can be internet facing (associate with public subnet) or internal ~~or~~ only (associate with private subnet).

ELB forwards traffic to eth0 (primary IP address)

ELB does not support client certificate authentication (API Gateway does support this).

ELB Security Groups.

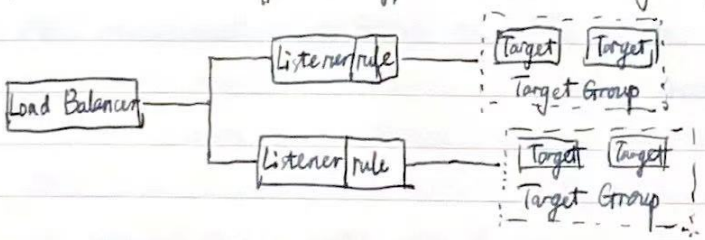
- Security groups ~~or~~ controls the ports and protocals that can reach the front-end listeners.
- You must assign a security group for the ports and protocals on the front-end listener.
- You need also allow the ports and protocals for the health check ports and back-end listeners.

Distributed Denial of Service (DDoS) protection with ELB:

- ELB automatically distributes incoming application traffics to multiple targets, such as EC2, containers, and IP addresses.
- ELB, like CloudFront, only supports valid TCP requests, so DDoS attacks such as UDP and SYN floods are not able to reach EC2 instances.
- ELB also offers a sigle points of management and serve as a line of defence between the internet and your backend.

Target groups.

- Target groups are a logical grouping of targets (EC2 instances or ECS ~~?~~ or IP addresses).
- Target groups are a regional construct.
- You cannot mix different types with in a target group.



H3 AWS Auto Scaling

AWS Auto Scaling monitors your applications and automatically adjusts capacity to maintain steady predictable performance at the lowest possible cost.

AWS Auto Scaling refers to a collection of Auto Scaling capacities across several AWS services, including:

- Amazon EC2 (known as Amazon EC2 Auto-scaling)
- Amazon ECS (including service auto-scaling and the new coming cluster auto-scaling by Capacity Provider)
- Amazon DynamoDB (WCU and RCU scaling)
- Amazon Aurora.

Auto-scaling provides horizontal scaling (~~scale~~ scale-out) for your instances. And it will try to distribute EC2 instances evenly across AZs.

Auto Scaling Groups (ASG) is a logical grouping of EC2 instances managed by an auto-scaling policy.

Four scaling options:

1. Maintain — keep a specific or minimum num of instances.
2. Manual — uses maximum, minimum, or a specific num.
3. Scheduled — if you have a predictive and fix pattern of traffic.
4. Dynamic — scale based on real-time metrics (e.g. CloudWatch metrics)

Scaling policy types:

1. Target Tracking Policy : track a specific metric and scale accordingly.
2. Simple Scaling Policy : wait until health check and cool down period expires before re-evaluating. AWS recommends others over this.
3. Step Scaling Policy : track several metrics/alarms. scaling by steps.

Scaling based on Amazon SQS: We can emit metrics from SQS (e.g. "ApproximateNumberOfMessages" for messages/traffic num) and use Target tracking policy or step scaling policy for auto-scaling.

If using an ELB it's best to enable ELB health checks otherwise EC2 status checks may conflict with ELB status hence avoid terminating instances unexpectly.

[H3] Amazon ECS

Amazon Elastic Container Service supports docker containers and allows you to easily run applications on a managed cluster of Amazon EC2 instances.

Amazon ECS eliminates the need for you to install, operate, and scale your own cluster management infra.

There is no additional charge for Amazon ECS.

It is possible to associate a service on Amazon ECS to an Application Load Balancer (ALB) for the Elastic Load Balancing (ELB) service.

ECS also has Blox, a collection of open source projects for container management and orchestration. Blox makes it easy to consume events from ECS, store the cluster state locally, and query the local data store through APIs.

ECS v.s. EKS

- EKS stands for Elastic Container Service for Kubernetes, which can be used to deploy, manage, and scale containerized apps using Kubernetes on AWS.
- ECS defines "tasks" while EKS defines "Pods".
- ECS leverages other AWS services like ELB, Route 53, and CloudWatch while EKS handles these internally.
- ECS is less extensible, while Kubernetes is highly scalable as has many 3P / community add-ons.

Launch Types: EC2 or Fargate.

- Amazon EC2 launch type gives you more controls over infrastructure.
- Amazon Fargate is a fully managed infrastructure for ECS that takes care of ALB, Route 53, and auto-scaling for you.
- Amazon Fargate only supports container images hosted on Elastic Container Registry (ECR) or Docker Hub.

EC2 Terms

- Cluster : Logical grouping of EC2 instances.
- Container Instances : EC2 instance running the ECS agent
- Task Definition : Blueprint that describes how a docker container should launch.
- Task : A running container using settings in a Task Definition.
- Service : Define long running tasks - can control task count with Auto Scaling and attach an ELB.
- Images : Contain the instructions for creating a Docker container. Images are stored in a registry. e.g. DockerHub, ECR.
- Container Agent : Allow container instances to connect to the cluster.

ECS Auto-Scaling

1. Service Auto Scaling : This is similar with EC2 Auto Scaling that you can use Target Tracking Scaling Policies, Step Scaling Policies to adjust EC2 or containers.
2. Cluster Auto Scaling : This is new feature released in Dec. 2019. It uses a ECS resource type called "Capacity Provider". A Capacity Provider is associated with ASG, and can scale your ASG automatically by using 2 new features of ECS :
   a) Managed Scaling, with an auto-created scaling policy ~~called~~ tracking a new auto-created metric called "Capacity Provider Reservation" and scales ASG automatically.
   b) Managed Instance termination protection, which provide container-aware termination of instances in the ASG when scale-in happens.

H3 AWS Lambda

AWS Lambda lets you run code as functions without provisioning or managing services. "Serverless applications" are composed of functions triggered by events.

AWS Lambda allocates CPU power proportional to the memory you specify using the same ratio as a general purpose EC2 instance type.

The components of AWS Lambda are :

- A Lambda function
- Event Sources. e.g. SNS, SQS, DynomoDB events, etc.
- Downstream Resources.
- Log streams.

Lambda functions provide access only to a single VPC. If multiple subnets are specified, they must be in the same VPC.

AWS SAM : AWS Serverless Application Model is a specification that prescribes the rules for expressing serverless applications on AWS.

Lambda @ Edge allows you to run codes globally without provisioning or managing the servers, responding to end users at the lowest network latency by executing functions in AWS locations close to users.

X-Ray is an AWS service that can be used to detect, analyze, and optimize performance issues with Lambda applications.

H3 AWS Elastic Beanstalk

AWS Elastic Beanstalk allows developers to upload applications and it handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring.

Considered a Platform as a Service (PaaS) solution.

Allows full control of the underlying resources, and there is no additional charge for Elastic Beanstalk.

H2 STORAGE

- for read after write: all clients immediately see the new after writing.
- for eventlogly: eventually all clients see the newer version.

H3 Amazon S3

- Files can be from 0 bytes to 5 TB.
- The largest object that can be uploaded in a single put is 5GB
- Object > 100 MB ? use multi-parts upload.
- ~~Upload~~ Updates to an object are atomic: when reading an updated object, you either get the new one or the old one but never a partial updated one.
  - Also: provide read after write consistency for NEW object PUT.
  - provide eventually consistency for overwite PUT/DELETE. (means take time to propagate).

For read intensive requests, use CloudFront edge locations to offload from S3. (tranfer acceleration)

Storage types:

1. Persistent data storage (S3, Glacier, EBS, EFS): Data is durable and sticks around after reboots, restarts, or power cycles.

2. Transient Data storage (SNS, SQS): Data is just temporarily stored and passed along to another process as end goal.

3. Ephemeral Data storage (EC2 instance store, Memcached): Data is lost when the system is stopped.

S3's buckets:

- Note that S3 does not provide a hierarchy of objects;
- But you can use an object key name to mimic folders.
- Why? Note that S3 is not a "file system", it is a storage for "objects".

S3 is a universal namespace so name of bucket must be unique globally.

S3 Storage Classes.

- S3 standard; S3 standard-IA; S3 standard One-zone IA; (→ still have redundancy, just that it is in the same AZ)
- S3 Intelligent Tiering
- S3 Glacier (≥90 days); S3 Glacier Deep Archive (>180 days) ⇒ hour-level retrieval

S3 supports wild-card.

S3 to use for static web hosting:

- cannot use dynamic content, e.g. PHP, .Net
- Do not support HTTPS/SSL.

Pre-signed URLs.

- can use it to provide temporary access. No need of AWS credentials.
- expiration date + time must be specified.
- can be either downloading or uploading.

Standard IA v.s. One-Zone IA S3: one-zone is cheaper with lower availability at 99.5%

△ S3 best practices.

1. Scale horizontally by issuing multiple concurrent requests instead of single request of a large file. (multiple part processing).
2. Use byte-range fetches
3. Retry request (with aggressive timeout) for latency-sensitive apps.
4. Combine S3 with EC2 in the same AWS region. (S3 global bucket does not mean the same latency from any location on the earth! You selected region when creating buckets).
5. Use Amazon S3 Transfer Accelaration (a.k.a. CloudFront edge location) to minimize latency caused by distance. (can be seen as a further improvement to item 4).

H3 Glacier

Glacier upload is synchronous, while download is asychronous.

Download process: ① Send request of retrieval; ② S3 copy data from Glacier to S3 One Zone-IA; ③ S3 sends SNS message when ready to be retrieved; ④ The data can be retrieved within 24 hours (available for the next)

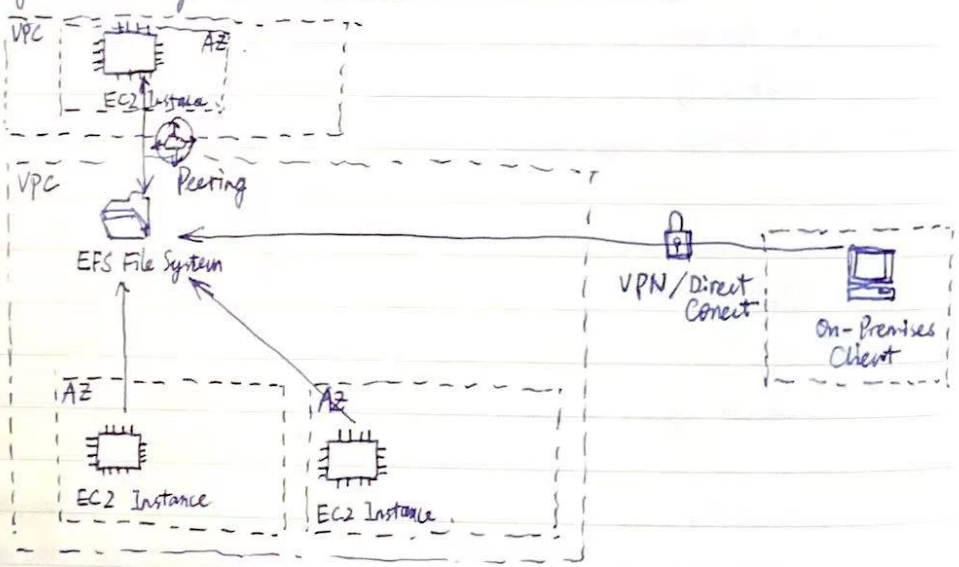
Archive retrival tier:

- Expedited: 1-5 min retrival (most expensive).
- Standard: 3.5 hours (10 GB free per month)
- Bulk Retrieval: 5-10 hours.

H3 Amazon EFS

EFS = Elastic File System => ~~the~~ the NFS (Network File System) on cloud. The implementation of NFS file share is accessed using the NFSv4.1 protocal.

EFS can be mounted either from EFS File Sync Agent or for on-premise systems through Direct Connect or a VPN connection.



* On-Premises Software V.S. SaaS and Cloud Solutions
本地端部署

	Amazon EFS	Amazon EBS(Provisoned IOPS)
Availability& Durability	Store data redundantly across multiple AZs	Store data redundantly in a single AZ
Access	Multiple EC2 Mount	Single EC2 Mount
Through Put	10+ GB/s	Up to 2GB/s
Use Cases	Big data, ML, FS/sharing	Boot Volume, NoSQL Database, etc.

EFS File Sync provides a fast and simple way to securely sync existing file systems to Amazon EFS. It's 5x faster than Linux default "scp," ~~Not~~ Note the other direction of data transferring cannot be done.

AWS service compatibility: CloudWatch, Cloud Trail, IAM, CF, Tagging

H3 AWS Storage Gateway

It enabled hybrid storage between on-premises environment and the AWS cloud, by providing low-latency caching frequently accessed data on premises and storing data securely and durably in Amazon cloud storage.

AWS Storage Gateway provides 3 types of storage interfaces:

1. File: Allow on-premises or EC2 to store objects in S3 via NFS or SMB.
2. Volume { Cached Volume Mode: Entired dataset on S3 and a cache on-site
   Stored Volume Mode: Entired dataset on-site and async backup to S3.
3. Tape: Virtual media changer and tape library for use with existing backup software.

[H3] Amazon FSx

Amazon FSx provides fully managed third-party (3P) file systems:

1. Amazon FSx for Windows File server for Windows-based applications.
2. Amazon FSx for Lustre for computing-intensive applications, including:
   - HPC: High-Performance Computing;
   - ML: Machine Learning; (High throughput: hundreds of GB/s; million IOPS)
   - EDA: Electronic Design Automation.

   - SMB protocal full support; (Server Message Block used by software-defined data center (SDDC))
   - Windows NTFS: NT File System
   - AD: Microsoft Active Directory integration.

△ Note IAM integration with AWS FS related service (e.g. EFS, FSx): IAM in these cases manage administers assignment, but the access control to files and directories in FS themselves are controled by FS's design, usually POSIX (user and group-level permissions; chmod command controls).

[H2] AWS DATABASE

[H3] Amazon RDS

Amazon Relational Data Service (RDS) is a managed service that makes it easy to set up, operate, and scale a relational database in cloud.

OLTP type of database. OLTP = Online Transaction processing comparing with OLAP: Online Analytic processing, e.g. Redshift.

RDS supports:

- Amazon Aurora
- MySQL
- Maria ~~DB~~ DB.
- Oracle
- SQL Server
- PostgreSQL

RDS do not grant you access to the underlying EC2.

You can only scale RDS up, you can not decrease the allocated storage for an RDS instance.

RDS uses EBS for storage, so you have 3 storage types selectable:
① General Purpose (SSD); ② Provisioned IOPS (SSD); ③ Magnetic.

Multi-AZ Deployment V.S.	Read Replicas
Synchronous replication - highly durable	Asynchronous replication - highly scalable
Only database on primary instance is active	All ~~the~~ replicas are accessible
Always span to 2 AZs within a single Region	Flexible across AZ / Region
Automatic fail over to standby if problem	Can be manually promoted to an instance.

RDS DB Snapshots : user initiated and enable you to back up your DB instances in a know state as frequently as you wish, and then restore to that specific state.

▲ Cannot be used for PITR.

AWS Database Migration Service (DMS) helps you migrate databases to AWS quickly and securely.

{ DMS is for a smaller, simpler conversions and supports DDB / MangoDB
SCT is used for larger, more complex dataset like data warehouse.
↳ schema conversion tool.

H2 Amazon Aurora

Amazon Aurora is a relational database service that combines the speed and availability of high-end commercial databases with the simplicity and cost-effectiveness of open source database. (to replace Oracle).

2 copies of data are kept in each AZ with a minimum of 3 AZs (6 copy)

Types of Aurora :

1. Aurora replicas. 2 types: Aurora replica and MySQL Read Replica.
2. Cross-region read replicas, allows you to :
   1) improve your disaster recovery posture ;
   2) scale read operations in regions closer to your user.
   3) easily migrate from one region to another.
3. Global database: a single Aurora database spans across multiple AWS regions.
4. Multi-master: scale out write performance across multiple AZs. with read after write consistency.
5. Aurora Serverless : on-demand auto-scaling configurations.

Aurora scaling : allows you to handle sudden increases in connectivity or workload.

Amazon Aurora allows PITR (note that RDS doesn't) It also has automated backups that you can enable.

Note that you can not restore from a DB snapshot into an existing DB instances.

H3 Amazon DynamoDB

Amazon DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability.

DynamoDB is schema-less.

Two read modes:

1. Eventually consistent reads (Default): mean the readed results may not reflect the result of a recent writes.
2. Strongly consistent reads: returns a result that reflect all writes that received a success response prior to the read.

A single record's maximum size is 400 KB.

Two kinds of secondary indexes:

1. Global Secondary Index: An index with a partition key and sort key that can be different with those on table.
2. Local Secondary Index: An index that has the same partition key but a different sort key.

Amazon DynamoDB Accelerator (DAX): in memory cache for DynamoDB.

- You can apply an IAM role to DAX nodes.
- You can apply Security Groups to the DAX nodes.
- DynamoDB DAX sits within your VPC.

DynamoDB is integrated with Apache Hive on EMR. You can:

- Query DynamoDB using HiveQL (a SQL like language).
- Copy data into HDFS and vice versa.
- Perform join operations on DynamoDB tables.

DynamoDB Global Tables: a fully managed solution for deploying a multi-region, multi-master, active-active database.

- A global table is a collection of one or more replica tables.
- A replica table is a single DynamoDB table that each replica stores the same set of data asynchronously. Not one region can only have at most 1 replica.

△ DynamoDB doesn't support strongly consistent read across regions.

△ HA options for databases
↓ DynamoDB over RDS
↓ Aurora over other RDS
↓ Multi-AZ RDS, for strong consistency, though only 1 master table
↓ Frequent snapshot for against data corruption, no impact to performance of Multi-AZ RDS.
↓ Regional Replication is also an option, though no strong consistency.
↓ If a database is running on a EC2, you need to design HA by yourself.

H3 Amazon ElasticCache

Amazon ElasticCache is a fully managed implementation of two popular in-memory data stores - Redis and Memcached.

Elasticcache EC2 nodes cannot be accessed from the Internet, nor can be accessed by EC2 instances in other VPCs.

Elasticcache is a good fit for storing session state.

Two types of ElasticCache engine:

- Memcached: simplest model, can run large nodes with multiple cores/threads, can be scaled in and out, can cache objects such as DBs.
- Redis: complex model, supports encryption, master/worker replication, cross AZ (HA), automatic failover and backup/restore.

Memcached	Redis
Not persistent	Data is persistent
Supports large node with multi-thread	Not multi-threaded.
Scales by adding/removing nodes.	Scales by adding shards, not nodes
Don't support multi-AZ failover	Multi-AZ is possible using read
Don't support replications	replicas in another AZ in the same region.

H2 Amazon Redshift

Amazon Redshift is a fully managed data warehouse that makes it simple and cost-effective to analyze all your data using SQL and BI tools.

Redshift is an Online ~~Ap~~ Analytics Processing (OLAP) tools. (comparing with OLTP tool)

Redshift is compatible with PostgreSQL with JDBC and ODBC drives, compatible with most BI tools out of the box.

Redshift use columnar data storage, which is ideal for data storage and analytics.

HA for Redshift:

- Redshift currently doesn't support multi-AZ deployments.
- The best HA option is to use multi-nodes cluster which supports data replication and node recovery.

H2 MIGRATION

H3 AWS Snowball

Petabyte scale data transport solution for transferring data into or out of AWS. Note that Snowball is physical transportation.

Snowball can import into S3 or export from S3. Also note that Snowball doesn't work with Glacier directly.

Each Snowball upper limit: 80TB.

- AWS Snowball Edge: Same with Snowball, but with onboard Lambda and clustering.
- AWS Snowmobile: A shipping container full of storage (up to 100 PB) and a truck to transport it.

△ AWS DMS v.s. SCT. v.s. DataSync.

1. AWS DMS: AWS Data Migration Service helps you migrate databases to AWS quickly and securely.
2. Schema Conversion Tool can copy database schemas for homogenous migrations (same database) and also for heterogeneous migrations (different database).
3. AWS DataSync makes it simple and fast to move large amount of data online between on-premises storage and Amazon S3 or EFS. It works with AWS Direct Connects. DataSync also supports VPCE (powered by AWS PrivateLink).

Biggest differences between them:

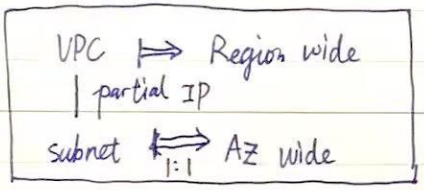
- DMS v.s. SCT: SCT is majorly on on-premises side as a tool for transform schema; DMS does the actual migration between on-premises and AWS cloud;
- DMS v.s. DataSync: DataSync is "online", requires Direct Link / VPCE. But DMS works with Snowball which enables you to physically migrate.

H2 NETWORKING AND CONTENT DELIVERY

H3 Amazon VPC

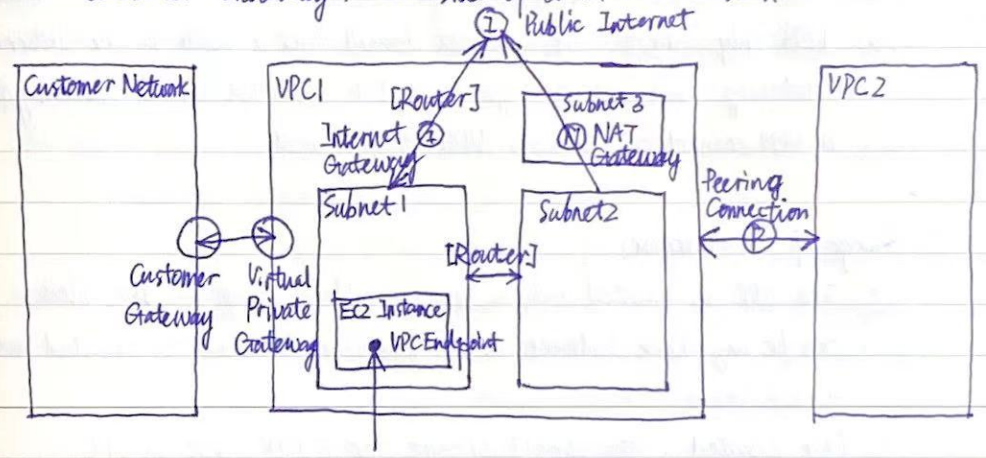
Amazon VPC lets you provision a logically isolated section of the AWS cloud where you can launch AWS resources in a virtual network you define.

VPCs are region wide, including selection of IP ranges, creation of subnets, and configuration of route tables and gateways.



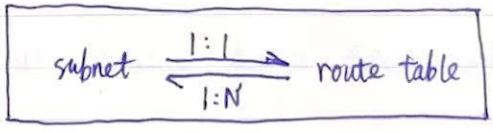
The default VPC has all-public subnets.
Public subnet is the subnet that has:
- "Auto assigned public IPv4 Address.
- The subnet route table has an attached Internet Gateway.

△ Components of VPC:
- A Virtual Private Cloud.
- Subnet: A segment of a VPC's IP address range where you can put resources.
- Internet Gateway: A highly available, managed Network Address Translation (NAT) service for your resources in a private ~~cloud~~ subnet to access the Internet.
- Hardware VPN connection: A hardware based VPN connection between your Amazon VPC and your data center, home network, or co-location facility.
- Virtual Private Gateway: The Amazon VPC side of a VPN connection.
- Customer Gateway: Your side of a VPN connection.



Routing:
- The VPC Router performs routing between subnets / AZs within a region.
- The VPC Router connets the VPC to the Internet Gateway.

- Route table:
  1. used to forward traffic within a VPC
  2. also has entries to external destinations. eg. Internet / VPN/VPC



Subnets and Subnet Sizing:

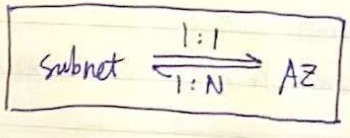
- Types of subnets:
  1. Public Subnet: traffic of the subnet is routed to an Internet Gateway.
  2. Private Subnet: traffic of the subnet doesn't have a route to Internet Gateway.
  3. VPN-only Subnet: If a subnet doesn't have a route to the Internet Gateway, but has its traffic routed to a Virtual Private Gateway for a VPN connection, then its VPN-only subnet.

- Range of IP Addresses
  - The VPC is created with a master address range (CIDR block, can be anywhere between 16-28 bits), and subnet is created using a sub-range address.
  - Once created, you cannot change the CIDR block in VPC.
  - CIDR: Classic Inter-Domain Routing, a method for allocating and representing IP. The # of address in a CIDR:

$$\#\text{ of addresses} = 2^{\text{add length} - \text{prefix length}}$$

in which, IPv4 = 32, IPv6 = 128

- The first 4 and last 1 IPaddresses ~~of~~ in a subnet are reserved by AWS.



- Each subnet must be in a AZ, cannot span across AZs.

Gateways: [At VPC level concept, for connection to/from outside VPC]

1. Internet Gateway (IGW): AWS VPC side of the connection to the public Internet.
2. Virtual Private Gateway (VPG): ~~VPC endpoint~~ VPN connection on the AWS side.
3. Customer Gateway (CGW): VPN connection on the customer side.

To enable access to or from Internet for instances in a VPC subnet, you'd:

1. Attach an Internet Gateway to your VPC.
2. Ensure your subnet's route table points to the Internet Gateway.
3. Ensure that instances in your subnet have a globally unique IPaddress (ie: public IPv4 address, Elastic IP Address, or IPv6 address).
4. Ensure that your Network Access Control List (NACL) and instances' security Group rules allow the relevant traffic to and from your instances!

VPC Wizard:

- NACL + Security Group can be used to provide strict control over inbound and outbound traffic to your instances.
  - NACL for configuring "blocking" IPs.
  - SG for adding "Allow rules".

- Private subnet instances can establish outbound connections to Internet via NAT Gateway / Instances.
  - NAT is configured directly to instances, not subnet level.
  - NAT can be Gateway / Instances (see later notes), they sits in a public subnet.

NAT Instances	NAT Gateways.
managed by you	managed by AWS
must be in a public subnet	the same, in public subnet
Not HA, can lead to bottlenecks	HA, multi-AZ redundancy
HA can be achieved by using ASG, multi-AZ, etc.	
Can be used as a bastion host	Cannot be used as a bastion host.

Security Groups.

- Security Group acts like a firewall at the instance level., specifically, the network interface level.
- Can only assign permit rules, cannot assign deny rules.
- Security Group is stateful, i.e. the response to a permitted request is also allowed.
- A custom Security Group allows all outbound traffic, but no inbound rule which implicitly denies all inbound traffic

NACL (Network ACL's).

- NACL function at subnet level instead of instance level.
- The VPC Router hosts the NACL function.
- You can have permit and deny rules at NACL. But NACL is preferred if you block
- NACL is stateless, so responses are subject to the rules for the direction of traffic.

A VPC comes along with a default NACL which allows all inbound/outbound
A custom NACL by default denies all in bound / outbound traffic.

- Comparing blocking rules with SG, SG cannot be used to block a specific range of IP address, so NACL is preferred for blocking traffics.

VPN Connectivity : several ways of connecting to a VPC.

1. AWS Managed VPN.
   - IPsec VPN connection, fully managed by AWS. requires a Virtual Private Gateway on AWS side and a customer Gateway on customer side.
   - Note that VPN cannot be used to access Elastic IPs on your VPC. The Elastic IP must be accessed from the Internet.

2. AWS Direct Connect
   - Dedicated private line connection from on-premises / office site to AWS backbone directly.
   - To establish Direct Connect, create Virtual Interfaces (VIFs) to connect to VPCs (private VIFs) or other AWS services like S3 / Glacier (public VIF)
   - AWS Direct Connect doesn't do traffic encryption in transit.

3. AWS Direct Connect ~~plus~~ plus VPN
   - IPSec VPN connection over private lines, which is more secure.

4. AWS VPN CloudHub
   - Hub-and-spoke manner for multi-branch offices at different locations.
   - Branches can talk to each other, hence providing redundancies.

5. Software VPN
   - This is recommended if you want to manage both end of VPN connection, "bring your own Virtual Private Gateway".

6. Transit VPC.
- A common strategy for connecting multiple, geographically disperse VPCs and remote networks in order to create a global network transit center.
- Used for data center / network ~~transit~~ center.
- To distinguish with Cloud Hub: Cloud Hub can also connecting several remote networks but is for building branch office networks.

7. VPC Peering
- AWS provided network connectivity between 2 VPCs.
- The VPCs can sit in different regions / accounts.
- It's neither a gateway or VPN, also doesn't have SPOF or bandwidth bottleneck.

8. AWS PrivateLink
- AWS-provided network connectivity between VPCs and / or AWS services using interface endpoints.

9. VPC Endpoints (VPCE)
- Use private Link and is an ENI (Elastic Network Interface) with a private IP address that serves as an entry point for traffics to a supported service/application.
- Types: Interface Endpoint and Gateway Endpoint
- Note that: Only DynamoDB and S3 uses Gateway Endpoints, all others are using Interface Endpoints.

10. Shared Services VPCs.
- Enables subnet to be shared with other AWS accounts within the same AWS Organization.
- With VPC sharing, your IT team can own and manage your VPCs. and your applications. Developer no longer needs to create / configure VPCs but they can use it ~~to~~ when they needed.

VPC Flow Logs.
- Captures info about IP traffic going to and from network interfaces in a VPC.
- Flow logs underlying uses CloudWatch Logs.
- Compare with CloudTrail:
  1. CloudTrail uses for auditing on actions to AWS resources.
  2. VPC Flow Logs have visibility into IP traffic's requests/response info, e.g. packet header. CloudTrail doesn't.
- Can be created at the following levels:
  - VPC
  - Subnet
  - Network Interface.
- After a flow log has been created, you can not change its configuration, have to delete and create a new one.

H3 AWS CloudFront

AWS CloudFront distribute ~~frequ~~ content with low latency and high data transfer speed. (CDN)

AWS CloudFront is a good fit for the distribution of frequently accessed static content that benefits from edge delivery.

- Ingress: to upload objects.
- Egress: to distribute content

CF supports wildcard CNAME.
CF supports wildcard SSL certificates, which means HTTPS is supported.

Origins: can either be S3 bucket, an EC2 instance, an ELB, or Route53, and even external (non-AWS). and Lambda@Edge

Types of distribution:
1. Web Distribution. For normal static files.
2. RTMP: Adobe's Real Time Messaging Protocol
   - For distributing and streaming media files, using Adobe Flash Media Server's RTMP.
   - Allows customer to start playing a media file before downloading finish.
   - Files origin must be S3 in this type of distribution.

CloudFront has a geo-restriction feature for you to restrict at country level.

AWS WAF is a web application firewall that lets you monitor HTTP and HTTPS requests that are forwarded to CloudFront and lets you control access to your content.
- You can use WAF's Web ACL to block access to content by:
  - Origin IP addresses / range.
  - Values in query string.

H3 Amazon Route 53

Amazon Route 53 is a HA and scalable Domain Names System (DNS) service.

Amazon Route 53 features:
- Domain Name resolution
- Domain Name registry
- Health checking of resources.

Hosted zones are collections of records for a specified domain.

Amazon Route53 supported DNS record types:
- All major record types, like A, AAAA, CNAME, CAA, MX, NS NAPTR, PTR, SOA, SPF, SRV, TXT.
- Alias type. This is an Amazon Route 53 specific DNS record type.
  - used to map ~~resource~~ domain record set to AWS resources, including: Amazon ELB, CloudFront, AWS Elastic Beanstalk Env, S3.

Amazon Route 53 Routing policy:

- Simple.
- Failover : If primary fails, routes to the secondary destination.
- Geolocation : Route to the closest region (not necessary the lowest latency)
- Geoproximity :
- Latency : lowest latency route to resources.
- Multivalue Answer : return several IP addresses.
- Weighted : Use relative weights asign to resources, e.g. 80% to ELB and 20% to on-premises.

H3 AWS Global Accelerator

A service to improve the availability and performance of applications for local or global users.

It provides a static IP address that acts as a fix entry point to application endpoint in a signle or multiple AWS Regions, such as ALB, NLB or EC2.

It uses the global network to optimize the path from users to applications, improving the performance of TCP and UDP traffic.

With the static IP, a benefit is you don't need to make any client facing changes or update DNS records when you modify or replace endpoints.

H3 Amazon API Gateway

Amazon API Gateway is a collection of resources ~~that~~ and methods that are integrated with back-end HTTP endpoints, Lambda functions, or other AWS services.

It can help handle all aspects of creating and operating robust APIs for application back-ends.

Amazon API Gateway + Lambda form the app-facing part of AWS serverless infrastructure.

Can enable CORS (Cross Origin Resource Sharing) for multiple domain use with Javascript / AJAX.

An API Endpoint type refers to the hostname of the API.
The API Endpoint type can be:

- Edge-optimized : best for geographically distributed clients.
- Regional : Intended for clients in the same region
- Private : can only be accessed from your Amazon VPC using an interface VPC endpoint.

H3 AWS Direct Connect

Mentioned before in AWS VPC connectivity, AWS Direct Connect connects on-premises sites to AWS cloud through private networks (not VPN/Internet)

For HA, you must have ≥ DX connections. It can be active-active or active-standby.

AWS Direct Connect Gateway:

- is a grouping of Virtual Private Gateway ~~(VPG)~~ (VGW) and Private Virtual Interfaces (VIFs) that belong to the same AWS account.

You can connect Direct Connect Gateway with either of:

- Virtual Private Gateway (normal VPC's VPN connection).
- Transit Gateway (the last type of connectivity in VPC, to creat a network transit center; transit VPC)

H2 MANAGEMENT TOOLS

H3 Amazon CloudWatch

A monitoring serice for AWS cloud resources and the application you run on AWS.

CloudWatch keeps logs indefinitely by default. Configurable, you may want 30 days retention.

CloudWatch keeps metric data as follows:

- a period of less than 60 sec: 3 hours
- 1 min: 15 days
- 5 min: 63 days
- 1 hour: 455 days (15 months)

H3 ~~Amazon~~ AWS CloudTrail

AWS CloudTrail is an AWS service recording activity made on your account. → user activity for audit purpose.

Two types of logged events:

1. Data events. Corresponding to data plane operations, of operations on or within a resource.
2. Management events (Control events). Corresponding to control plane operations, of management operations on AWS resources

H2 AWS OpsWorks

AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet two ~~of~~ very popular automation platforms. It transforms infrastructure into codes.

Three major features:

1. AWS OpsWorks for Chef Automate
2. AWS opsWorks for Puppet Enterprise
3. AWS opsWorks Stacks: An AWS creation, underlying runs Chef ~~recei~~ recipes.

H2 AWS CloudFormations

Infrastructure as code.

Comparing with Elastic Beanstalk:

1. Elastic Beanstalk is more on deploying applications to EC2 (PaaS)
2. CloudFormation can deploy Elastic Beanstalk-hosted applications but the reverse is not possible.

Concepts:

- Templates: The json or YAML files containing infra codes.
- Stacks: The entire env described by the template.
- Change sets: A summary of proposed changes to your stack.

Two ways of deploying CloudFormation changes:

1. Direct deployment. can cause outage if resources are not created as expected to.
2. Changeset: View change summary in change set and then deploy.

AWS CloudFormation supports Puppet and Chef.

H2 AWS Config

AWS Config is a fully managed serice that provides you with an AWS Resource Inventory, configuration history, and config change notifications to enable security and governance.

It enables compliance auditing, security analysis, resource change tracking, and troubleshooting.

AWS Config v.s. CloudTrail:

- AWS Config: "What did my AWS resources look like?"
- CloudTrail: "Who made an API call to modify my resources?"

Concept: Configuration ~~It~~ Item (CI) is the config of a resource at a given point-in-time.