**AWS Architect Training – Important Notes**

**IAM:**

* IAM consists of Users, Groups, Roles and Policy Docs (JSON or key value pair).
* IAM is universal. It doesn’t apply to regions.
* Root account is created when the AWS account is setup. It has admin access.
* Users have no permission by default.
* Users are assigned with Access key and secret Access key. These can used to access AWS via the APIs and CLI.
* You can customize password rotation policy or custom password.
* Best practice to implement multifactor authentication.

**S3:**

* S3 is an object based storage.
* Files can be from 0 bytes to 5 TB.
* Unlimited storage.
* S3 bucket is a universal namespace – it must be unique globally.
* Read after write consistency for PUTs of new objects.
* Eventual consistency for overwrite PUTS and DELETES (can take some time to propagate).
* S3 – durable, immediately available, frequently accessed
* S3 –IA : durable, immediately available, infrequently accessed
* S3 – Reduced Redundancy storage (data that is easily reproducible such as thumb nails etc.)
* Glacier – good for archived data. 3-5 hours to access the data.
* It’s a key (name) value (data) store, version id, metadata, ACL.
* Not suitable to install an operating system on (EBS should be used)
* Pay for each version of the object.
* Once versioning is enabled, it cannot be disabled, only suspended.
* Versioning’s MFA Delete capability, which uses multi-factor authentication, can be used to provide an additional layer of security.
* Cross region replication – requires versioning enabled on the source bucket as well as the destination.
* Lifecycle management can be used in conjunction with versioning.
* Lifecycle can be applied to current and previous versions
* Lifecycle – Transition to the standard –IA 128kb and 30 days after the creation date
* Lifecycle – Archive to the Glacier 30 days after IA if relevant.
* Lifecycle – can permanently delete.
* Edge Location is the location where the content will be cached. This is separate to an AWS region/AZ
* Distribution – CDN which consists of a collection of Edge locations.
  + Web distribution – used for websites.
  + RTMP – for media streaming.
* Edge locations are not just READ only, you can write to them too.
* Cloudfront : Objects are cached for the life of the TTL (in seconds). By default to 24 hrs.
* You can clear cached objects but you will be charged.
* By default all newly created buckets are PRIVATE
* Setup access by using bucket policies or ACL.
* Two types of encryption –
  + in transit SSL/TLS,
  + at rest encryption:
    - Server side encryption – S3 managed keys SSE-S3,
    - AWS Key Management Service SSE KMS
    - Server side encryption with customer provided keys SSE-C
  + Client side encryption

**Storage gateway**

* Storage Gateway – to connect between on premise to cloud.
* Storage Gateway –
  + File Gateway (NFS) – for flat files.
  + Volumes Gateway (iSCSI) – virtual hard disk: Stored volumes, cached volumes
  + Tape Gateway (VTL) – Backup and archiving solution
* Volume gateway (virtual hard disk) is an interface between local disk to Amazon EBS. It can be backup asynchronously.
  + Stored volume – store locally and back asynchronously to AWS. 1 GB – 16 TB EBS size.
  + Cached volume – more recent data saved on prem and rest in cloud. 1 GB to 32 TB size.
  + iSCSI connection is used to connect these virtual volumes.

**Snowball:**

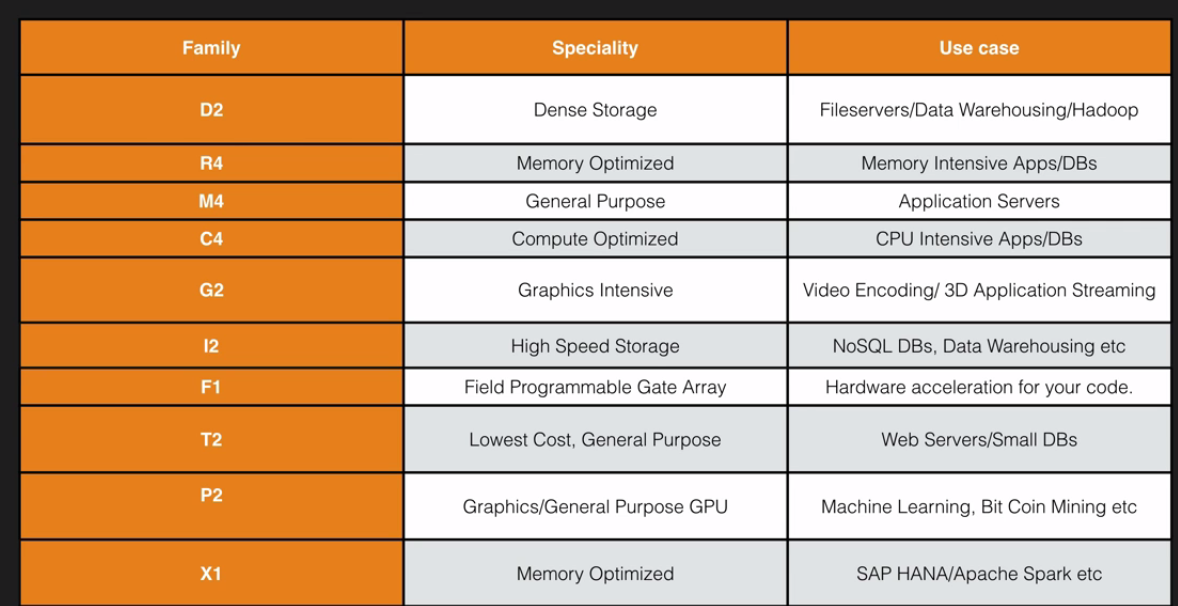
* Snowball can import to s3 and export from s3. It’s a petabyte-scale data transport solution. 80 TB snowball in all regions. 256 bit encryption and industry standard Trusted Platform Module (TPM) – it’s a onboard storage
* Snowball Edge contains 100 TB – storage with compute capabilities. It can allow lambda functions.
* Snowmobile – Exabyte-scale data transfer service. – 6 months to transfer the data. 45 foot long ruggedized shipping container pulled by a semi-trailer truck.
* S3 transfer acceleration: it utilized the cloudfront edge network to accelerate your uploads to S3. You will get a distinct url to upload the data.
* We can use S3 to host static websites (its server less). It can support STATIC pages only. Cannot host dynamic sites.
* HTTP 200 code for the successful write.
* You can load files to S3 much faster by enabling multipart upload.

**Security Group**

* All inbound traffic is blocked by default
* All outbound traffic is allowed
* Any rules applied to security group will be implemented immediately.
* Security group is the first line of defense.
* Inbound rules will allow outbound traffic be by default for security group.
* Can’t deny an IP or to an outside instance.
* You can associate multiple security groups to an instance.
* Security groups are STATEFUL instead use Network Access Control Lists.
* You can specify allow rules, but not deny rules.

**EC2:**

* Pricing differs for each type – On Demand, Spot, Reserved and dedicated Hosts.
* Spot instances – cost is low
* Reserved instances – Reserved for a fixed user count.
* On Demand – black Friday
* Dedicated hosts – legal and security requirements.



* EBS
  + SSD – General Purpose – GP2-Upto 10,000 IOPS)
  + SSD, Provisioned IOPS – IO1 – More than 10,000 IOPS.
  + HDD, Throughput Optimized – ST1 – Frequently accessed workloads.
  + HDD, Cold – SC1 – Less frequently accessed data.
  + ST1 and SC1 cannot be used for boot volume, however they can be used as additional volume.
  + You cannot mount 1 EBS volume to multiple EC2 instances, instead use EFS.
  + Root volume to be deleted when the instance is terminated.
  + Root volumes cannot be encrypted by default, you need third party tools such as bit locker.
  + Additional volumes can be encrypted.
  + Volumes exist on EBS – Virtual hard disk.
  + Snapshot of volume is stored on S3.
  + Snapshots are incremental. Only the blocks that have changed since your last snapshot are moved to S3.
  + Snapshots are encrypted automatically.
  + You can share snapshots but only if they are unencrypted.
  + Snapshots can be shared with other AWS accounts.
  + Amazon EBS volumes that serve as root devices, you should stop the instance before taking the snapshot.
  + Instance store volumes are sometimes called ephemeral storage.
  + Instance store volumes cannot be stopped. If the underlying host fails, you will lose your data.
  + EBS backed instances can be stopped. You will not lose the data on this instance if it is stopped.
  + Snapshot for RAID array can only be done once you freeze the file system, unmount the RAID array and shutting down the associated EC2 instance.
  + AMI are stored regional.
  + Standard Monitoring – 5 min. Detailed monitoring =1 min at additional charge
  + Cloudwatch is for performance monitoring
  + CloudTrail is for auditing.
  + Cloudwatch – dashboard, alarms, events, logs.
  + Roles are more secure than storing your access key and secret access key on individual EC2 instances.
  + Roles are easier to manage.
  + Roles are universal.
  + Instance meta data – info about an instance.
  + Curl : <http://169.254.169.254/latest/meta-data/>
  + EFS supports Network File System version 4 (NFSv4) protocol.
  + Lambda – runs code in serverless environment.

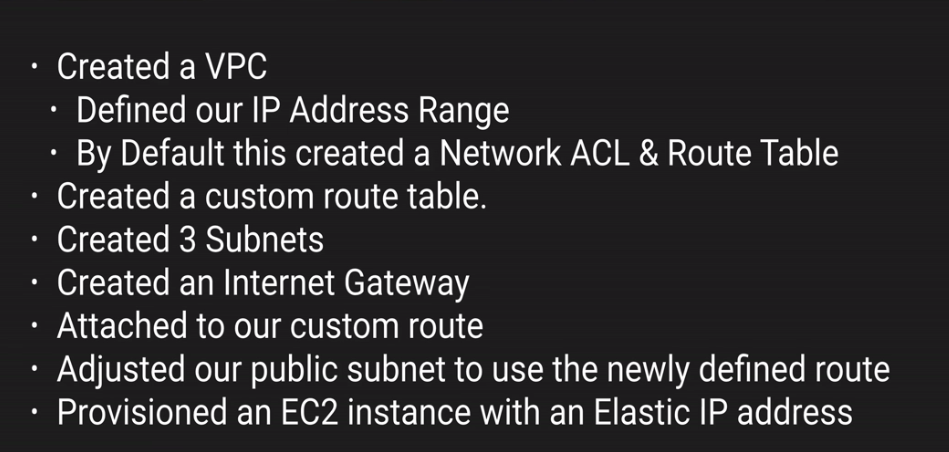
**Route53:**

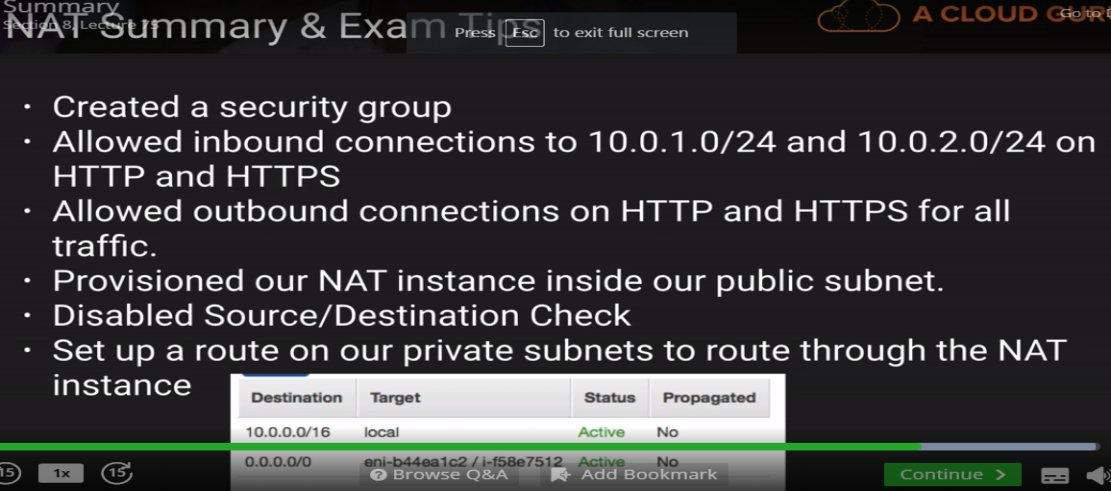
* Elastic load balance doesn’t have IP, it will resolve to DNS which amazon handles.
* Always choose an alias record over CNAME
* Routing polices
  + Simple
  + Weighted
  + Latency
  + Failover
  + Geolocation

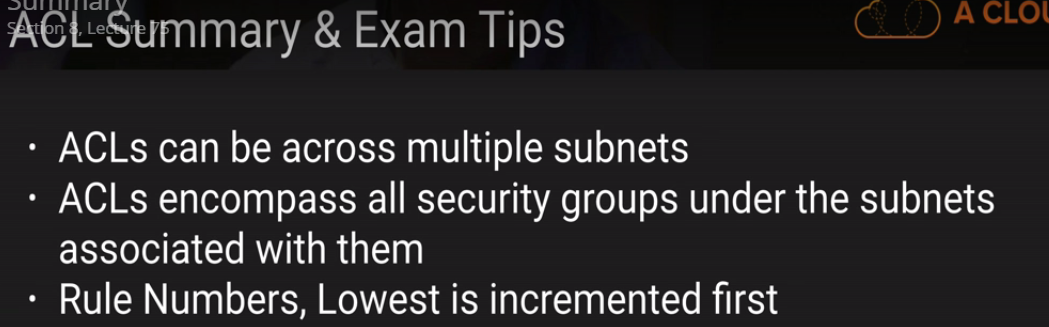
**RDS:**

* RDS – OLTP – sql, mysql, postgresql, oracle, aurora, mariadb.
* Dynamodb – no sql
* Redshift – OLAP
* Elastic cache – mem and redis
* 5 upto read replicas
* Aurora – 2 copies of your data is contained in each availability zone, with minimum of 3 availability zones. 6 copies of your data.
* Aurora is designed to transparently handle the loss of upto two copies of data without affecting database write availability and upto three copies without affecting the read availability.
* Aurora storage is also self healing. Data blocks and disks are continuously scanned for errors and repaired automatically.
* Auro – two types of replicas.
  + Aurora replicas (currently 15)
  + MYSQL red replicas (currently 5)
* DynamoDB offers “push button” scaling. No downtime is required.
* Stored on SSD, spread across 3 geographically distinct data centres. Eventual consistent reads by default, strongly consistent reads.
* Redshift – single node – 160GB. Multi-node – Leader and compute nodes. Upto 128 compute nodes.

**VPC:**







**Application Services:**

* SQS is pull based, messages are 256 KB in size. Messages can be kept in the queue form 1 min to 14 days. 4 days is default.
* Visibility time out maximum for 12 hours.
* SQS guarantees that you messages will be processed at least once.
* Queues can either be standard or FIFO.
* SWF retention period is upto 1 year for workflow executions
* SWF presents a task-oriented API, whereas SQL offers a message oriented API.
* SWF ensures that a task is assigned only once and is never duplicated.
* AWS Actors –
  + Workflow starters – an application that can initiate a workflow.
  + Deciders – control the flow of activity tasks in a workflow.
  + Actviity workers – carry out the activity tasks.
* SNS – http, https, email, email-json, sqs, application and lambda.
* Elastic transcoder converts the media files from the original source to different formats that will play on smartphones, tablets and PCs etc.
* Pay based on the minutes that you transcode and the resolution at which you transcode.

**Linux commands:**

|  |  |
| --- | --- |
| Bin bash is used to set the default folder for commands | #!/bin/bash |
| Install updates | yum update –y |
| install apache | yum install httpd –y |
| Apache web server to start | service httpd start |
| Aparche web server status | service httpd status |
| Update config to start the webserver at the boot | chkconfig httpd on |
| Web server folder – default | /var/www/html/ |
| Default editor | Nano |
|  |  |

Important points:

* Amazon's SLA guarantees a Monthly Uptime Percentage of at least 99.95% for Amazon EC2 and Amazon EBS within a Region.
* Amazon S3 objects that are stored using the Amazon Glacier option are only accessible through the Amazon S3 APIs or the Amazon S3 Management Console.
* Standard - IA is designed for larger objects and has a minimum object size of 128KB. Objects smaller than 128KB in size will incur storage charges as if the object were 128KB.
* Multipart Upload is recommended for files greater than 100 Mb, and is required for files 5 GB or larger. S3 Transfer Acceleration is especially useful in cases where your bucket resides in a Region other than the one in which the file transfer was originated.
* You can use just one bucket and enable CRR on just a subset of uploaded objects (such as JPGs and PDF's) by using specifying prefixes.
* The best solutions for instant access, but lowese cost would be S3 - Infrequently Accessed storage.
* Each Classic Load Balancer has an associated IPv4, IPv6, and dualstack (both IPv4 and IPv6) DNS name. However, IPv6 is not supported in VPC at this time.
* You can securely upload/download your data to/from Amazon S3 via SSL or HTTP endpoints using HTTPS.
* You can choose to encrypt data using SSE-S3, SSE-C, SSE-KMS, or a client library such as the Amazon S3 Encryption Client. All four enable you to store sensitive data encrypted at rest in Amazon S3.
* S3 - IA is 99.9% available. Do not confuse availability with durability.
* Only the owner of an Amazon S3 bucket can permanently delete a version.
* A Dedicated Host is required if you'd like to use your existing Windows Server licenses.
* By default, all accounts are limited to 5 Elastic IP addresses per region.
* Amazon EC2 cluster placement group functionality allows users to group Cluster Compute Instances in clusters – allowing applications to get the low-latency network performance necessary for tightly-coupled node-to-node communication typical of many HPC applications.
* By default, customers can provision up to 100 buckets per AWS account. However, you can increase your Amazon S3 bucket limit by visiting AWS Service Limits.
* S3 with Cross-Region Replication (CRR) automatically replicates data across AWS regions. With CRR, every object uploaded to an S3 bucket is automatically replicated to a destination bucket in a different AWS region that you choose.
* Amazon CloudWatch stores metrics for terminated Amazon EC2 instances or deleted Elastic Load Balancers for 2 weeks.
* The two different types of virtualization available are Hardware Virtual Machine (HVM) & Paravirtual Machine (PVM).
* SSE-S3 uses managed keys and one of the strongest block ciphers available, AES-256, to secure your data at rest.
* Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and your Amazon S3 bucket. Transfer Acceleration leverages Amazon CloudFront’s globally distributed AWS Edge Locations.
* CRR replicates every object-level upload that you directly make to your source bucket. The metadata and ACLs associated with the object are also part of the replication.
* Using IPv6 support for Amazon S3, applications can connect to Amazon S3 without needing any IPv6 to IPv4 translation software or systems.
* Amazon RDS retains backups of a DB Instance for a limited, user-specified period of time called the retention period, which by default is one day but can be set to up to thirty five days.

You can have:

* Five Amazon VPCs per AWS account per region
* Two hundred subnets per Amazon VPC
* Five Amazon VPC Elastic IP addresses per AWS account per region
* One Internet gateway per VPC
* Five virtual private gateways per AWS account per region
* Fifty customer gateways per AWS account per region
* Ten IPsec VPN Connections per virtual private gateway
* EBS: You can create up to 75 applications and 1,000 application versions. By default, you can run up to 200 environments across all of your applications