DNS 101.

* DNS is used to convert human friendly domain names like http://acloud.guru to an IP address.
* IP address are used by computers to identify each other on the network. IPv4 and IPv6.

IPv4 – 4 billion different address
IPv6 – To solve depletion issue. 340 undecillion Address.

Route 53 supports IPv6. VPC also IPv6 compatible.

* NS records → Name Server Records. Amazon is also a domain registrars like Godaddy. Used by Top Level domain Servers to direct traffic to the Content DNS Server.

A records → translate name of domain to IP address.

TTL → Time to live of DNS record cache in local PC.
Ex: 300 Seconds or 5minutes.

CName (Canonical names) → Alias kind of.
i.e m.acloud.guru → mobile.acloud.guru

** → Similar to CName. But used with AWS resources. i.e ELB's.
Alias records, used to map resource record in your hosted zone to ELB, CloudFront distributions or S3 buckets.

* main website i.e http://acloud.guru cannot be a CName it should be a "A Record".

Exam:
* ELB's dont have a pre-defined IPv4 address, resolved using DNS
* Diff b/w Alias vs CName. CName is charged by Route 53. Alias records are not charged.

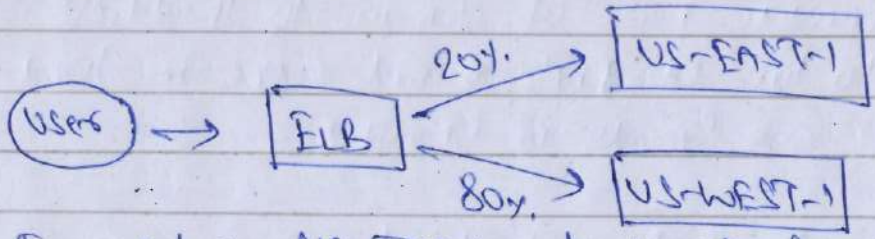
Domain Name : NS records and SOA - Start of Authority will be there → (Server details like admin of the Zone, name of the server etc.)

Route 53 Routing Policy :- (Global Service like IAM)

① Simple - This is the default routing Policy when you create a new record set. Ex: one webServer serving content for a website and NS round robin.

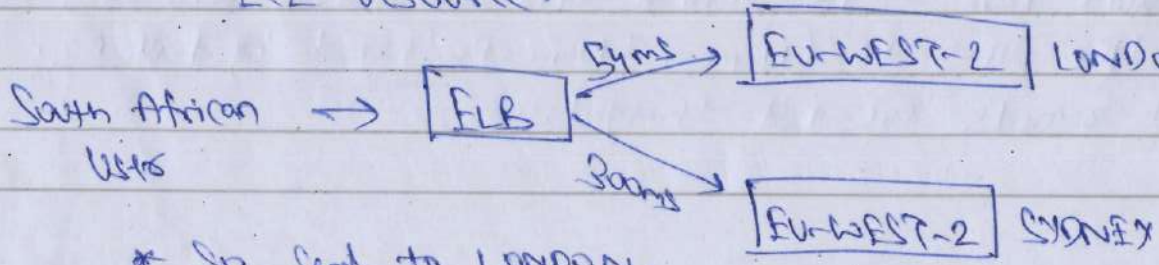
Create Record Set in Route 53.
Alias domain name : helloCloudGurus.com i.e no www.

② Weighted Routing Policy :- Split traffic based on different weights.



Ex: used in A/B Testing kind of services.
To route 80% traffic to Prod and 20% to new design.

③ Latency Routing Policy :-
→ Allows you to route traffic based on the lowest network latency for your end user.
* Create a latency resource record for the Amazon EC2 resource.



* So send to LONDON.

④ Fail over Routing Policy :-

→ Used when you want to create active/passive set URLs.
Ex: Primary Site in London & Secondary in Sydney.

→ Route 53 monitors a health check, if Primary fails then all traffic to Passive i.e SYDNEY here.

Route 53 → Create a health check.
i.e End Point of an ELB i.e DNS name.

⑤ Geo Location Routing Policy :-

→ Routing traffic based on Geographic location.
ie All queries for european customers to be routed to EC2 instance in europe so that all prices displayed in euros.

DNS Summary.

* ELB's dont have an IP address, it's only DNS name. Hence Amazon has provided with Alias records
* Diff b/w Alias and CName.
- Alias can resolve ELB's and other AWS resource unlike CName.
* Always Prefer Alias over CName as Alias is free.

* AWS Shared Responsibility model.

① Managed by AWS.
- AWS Endpoints
- Regions, Availability Zones, Edge locations.
- Compute, Storage, DB's, Networking.

② Managed by AWS Customers.
- Encryption : Client & Server Side
- Network Traffic ie HTTP vs HTTPS.
- OS, Network & Firewall Configuration.
- Platform & application Mgmt.
- Customer Data.

* Shared Responsibility for Container Services :-
like Amazon RDS and Amazon Elastic Map Reduce.

① Managed by AWS :
- underlying infrastructure & foundation services.
- Operating System
- Application Platform.

Example: Disaster Recovery, Business Continuity

② Managed by Customers
- Data, firewall rules for access to Container Service.

* Shared Responsibility for Abstracted Services : Also applicable for Lambda.
- for Amazon S3 and Dynamo DB.

① Managed by Customers
- Client Side data encryption &
Data Integrity Authentications.

Ex: For S3, You can use Platform-Provided encryption of data.
- For Customer Data.

Shared responsibility for Infrastructure.
Ex: AWS EC2 as Infra as a Service. Amazon responsible till Hypervisor level.

EC2 Continued...

* Amazon EBS are Placed in Specific Availability Zone, where they are automatically replicated to Protect you from Single Point of failure.

EBS Volume Types:

1. GP2 SSD - around 3000 IOPS
2. Provisioned IOPS SSD - Application > 10,000 IOPS
3. Magnetic Disk
   - i) Throughput Optimized HDD - for Data written in Sequence.
     - Big Data
     - Data warehouse
     - log Processing

     ★ Cannot be a boot volume.
   - ii) Cold HDD (SC1)
     - lowest cost storage for infrequently accessed data
     - File servers
     - Cannot be a boot volume.
   - iii) Magnetic Standard.
     - lowest cost Per GB
     - EBS volume that is bootable.

From.

* You cannot mount 1 EBS volume to multiple EC2 instances, instead use EFS.

Ami - Amazon machine Image.

Exam.

* "Delete on Termination" → Delete an EBS volume associated to EC2 instance when it is terminated. Automatically.
* EC2 Root volume is not encrypted, only additional volumes can be encrypted.
* Tags : key - value pair.

Security Group :

- A virtual fire wall.

→ - One instance can have multiple security groups.

Summary :

* On EBS backed instances, the default action is for the root EBS volume to be deleted when the instance is terminated.
* Root volumes cannot be encrypted by default, you need a third party tool (like bit locker) to encrypt root volume.
* Additional volumes can be encrypted.

Security Group Continued :

* First line of defense for Security Purpose.
* Any rule applied to a security group, takes effect immediately ie if you remove HTTP from inbound rule - Security group.
* Security group is "stateful" → Inbound rule is enough, no need of a seperate outbound rule.
* Rules only to allow traffic, you can't deny traffic. Or deny a specific IP address. instead use N/w ACL's.

Volumes & Snapshots.

* EBS volumes available to EC2 instances if they are in the same Availability Zone.
* Snapshots are point in time photographic copy of the original virtual volumes. → Just the delta is stored in S3.
* We could create a new volume using an existing snapshots.

→ Volumes exist on EBS
  • Virtual Hard Disk.
→ Snapshot exist on S3
→ Snapshot is a point in time copy of a volume
→ Snapshots are incremental. (only Deltas will be stored after the initial Snapshot creation).

AWS CLI:

* Roles are more secure than storing your access key and secret access key on individual EC2 instances.
* Roles are easier to manage

Use AWS EC2 DESCRIBE-INSTANCES → To see running instances
AWS EC2 DESCRIBE-IMAGES → To describe AMI we own images
AWS EC2 RUN-INSTANCES → To create a EC2.
AWS EC2 TERMINATE-INSTANCES.

AWS Lambda

(2006)
Data Centers → IAAS (EC2) → PAAS (Platform as a Service)
(Infrastructure as a Service)
Elastic Bean Stalk:
i.e includes OS and other stuff.
↓
Container Service (Docker) → Deploy to Server.

(Everything is taken care of
Just Upload your code) "Server Less" ← (Lambda)

* Lambda → Just Submit your pure code and AWS manages everything else. ie
- Data Centers
- Hardware
- Assembly Code / Protocols
- Operating Systems
- Application Layer.

AWS Lambda is a Compute Service where you can Upload your code and create a lambda function. Lambda takes care of Provisioning and managing the Servers that run your code.

Lambda can be used in 2 ways:

1. Event-driven Compute Service — ie run code in response to events. like changes in S3 bucket or DynamoDB table
2. As a Compute Service in response to HTTP requests using Amazon API Gateway.

Languages Supported.

i) Node.JS
ii) Java 8
iii) Python
iv) C#
v) Go

lambda (001 11.

* NO SERVERS
* Continous Scaling
* Super Cheap.

Elastic Load Balancer :- (Priced feature, Not free)

(Layer 7)
① Application load Balancer - Routing decesions at app layer (HTTP/HTTPS)
② Classic load Balancer - Routing at Transport layer (Layer 4) ie (TCP / SSL) or app layer.

ELB can also have Tags ie key-value.

⇒ ELB always don't have a Public IP address, Amazon wants you to use the DNS name. Because Public IP changes for ELB.

⇒ App load Balancer not in the exam.

* Instances monitored by ELB are reported as InService or Out of Service
* Health Check → instance health by talking to it
* ELB have Own DNS name and not Public IP.

EC2 Summary.

* On Demand - Pay by the hour · Black Friday Sale
  Spot - Huge Big data Processing.
  Reserved - Normal Site
  Dedicated Hosts - Not have multitenant Compute

* Termination Protection is turned off by default, You must turn it on.
* Snapshot of encrypted volumes are encrypted automatically.
* Volumes restored from encrypted snapshots are encrypted automatically.
* You can share snapshots, if they are not encrypted.
* Snapshots can be shared with other AWS account or with Public.

AMI's are regional — launch an AMI from the region where it is stored. However copy AMI's to other regions using Console, command line or Amazon EC2 API.

* Cloud watch is for Performance monitoring.
  Cloud Trail is for Auditing. ⟷ Ex: History of all EC2 API calls made.

Cloud watch ?

→ Create awesome dashboards to see what is happening with your AWS env.
→ Alarms — notify particular threshold.
→ Events — For State Change of an AWS resource.
→ logs — Aggregate & Share logs.

* http://169.254.169.254/latest/meta-data
  No such thing as user-data for an instance.

EC2 FAQ's.

* EBS → data persistent independently from lifetime of instance.
  Ex: like a Laptop.
* Local instance store → persists during life of the instance

1) Can i get history of all EC2 API calls made on my account?
   → Yes. Cloud Trail in AWS for EC2 API calls including VPC & EBS.

2) If i transfer data between Availability Zones using Public IP addresses will i be charged twice for regional data transfer?
   No. Regional Data Transfer rates apply if,
   i) Other instance in a different AZ, regardless of address
   ii) Public or Elastic IP addresses are used, regardless of which AZ the other instance is in.

3) How many Spot instances can i request?
   You are limited to requesting Spot instances per your dynamic Spot limit for each region. Note that not all instances types are available on Spot.

4) Can i specify a different AMI (Amazon machine Image) for each instance type that i want to use?
   Yes.

5) Can i use Spot fleet with Elastic load Balancing, Auto Scaling or Elastic Map Reduce?
   Spot fleet → with Auto Scaling
   ELB or EMR not possible to trigger.

6) How can i tell if an application needs more CPU resources?
   "Cloud watch" metric for CPU utilization will be 100% utilization.

EBS Exam Tips.

* EBS volumes can be changed on the fly (except for magnetic standard → Stop EC2 . Create a SnapShot . Then Create volume from that SnapShot).
* Best Practice to Stop the EC2 instance & then change the volume.
* You can change volume types by taking a new SnapShot & then using the SnapShot to create a new volume.
* Change volume on the fly → wait 6 hours before making another change.
* Scale EBS volumes up only. Can't convert 500GB EBS volume to 256 GB.
* Volumes must be in the same AZ as the EC2 instances.

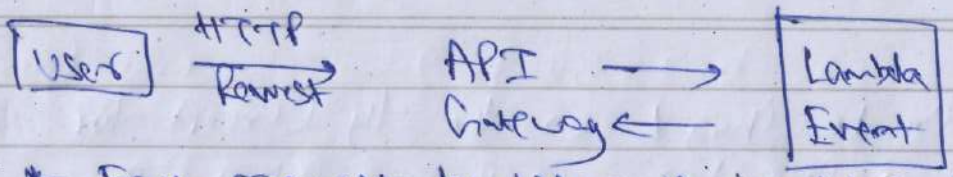
* To view instance metadata

curl http://169.254.169.254/latest/meta-data/Public-ipv4
/local-hostname

Lambda Continued:

* lambda can communicate with other AWS services likes SQS, S3 etc.
* One instance of lambda running per HTTP (user) request.
* lambda Trigger - AWS IOT, Dynamo DB, Code Commit, Alexa Skills, Cloud Front, Cloud watch API Gateway, Kinesis, SNS, S3

** Exam Tolic



* Each request by user is invoking a lambda function.
  i.e 200 users simultaneously requesting → 200 calls made to lambda event.

Pricing:

→ Based on Number of requests
  - 1 million requests are free. $0.20 Per 1 million requests thereafter.

→ Duration based. (function can't execute above 5 mins)
  Time to execute your code. (charged Per every 1ms of resource used Per Second.

* lambda → ① Provides Continous Scaling. Not like Auto ② Scaling triggers Conditions. This happens instantly. ③ Super Chief.

Exam Tips:

→ lambda scales out (not up) automatically.
→ 1 event = 1 function.
→ lambda is Serverless.
→ lambda can trigger other lambda functions.
  1 event = x functions
→ Aws X-ray allows to debug.
→ lambda can do things globally. i.e one S3 bucket can be copied to other S3 bucket.

CKAPS0986H3

Security Token Service (STS)

* Grants users limited and temporary access to AWS resources. Users can come from below 3 sources:
  1. Federation (typically Active Directory)
     - User Store - Does not need to be an IAM user.
  2. Federation with mobile Apps.
     - FB, Google Providers for login
  3. Cross Account Access
     - Users from one AWS account to access resources in another.
* Federation :- Combining or Joining a list of users in one domain (such as IAM) with list of users in another domain (such as FB)
* Identity Broker :- Service that allows you to take an identity from point A and join it to point B.
  - ** This service needs to be developed in-house.
* Identity Store :- Service like FB, Google, LinkedIn etc
* Identity - A user of a service like FB.

Exam:

1. Develop an Identity Broker to communicate with LDAP & AWS STS.
2. Identity Broker always authenticates with LDAP first, THEN with AWS STS.
3. Application then gets temporary access to AWS resource.

VPC Continued.

VPC Flow logs :-

* Capture info about IP traffic going to & from network interfaces in your VPC.
* Flow log data ⟶ Stored using Amazon Cloud watch logs.

Can be created at 3 levels:
1. VPC — capture all traffic
2. Subnet
3. N/W interface level.

* VPC ⟶ Actions ⟶ Create Flow log ⟶ Set a Accept or Reject Filter.
  * Cloud watch ⟶ Create New log group.

Exam Tips :

* You cannot enable flow logs for VPC that are Peered with your VPC unless the Peer VPC is in your account.
* You cannot tag a Flow log.
* After a flow log has been created, you can't change it's configuration. Ex: Diff IAM role with flow log.
* Not All IP Traffic is monitored.
  Ex: i) Windows instance for Amazon windows license activation related
  ii) Amazon DNS Server related traffic
  iii) Traffic to & from 169.254.169.254 (instance metadata)
  iv) DHCP Traffic
  v) Reserved IP address for Default VPC router.

VPC End Point :-

* Allows you to securely connect your VPC to another service.
  Ex: Allowing S3 access to EC2 instances.
* Interface - Singe ENI (Elastic Network interface)
  Gateway - Highly available endPoint. (like how NAT Gateway is highly available)
* With endPoints, the source IP address from instances in the same region will be Private IP address, not Public.

Exam Tips :-

* NAT instance should be in a Public Subnet
* NAT instance ⟶ Disable Source / Destination Check on the instance.
* There must be a route out of the Private Subnet to the NAT instance. i.e Check Route Table & add a route 0.0.0.0/0 to the NAT. Also associate Public Subnet here.

* NAT Gateway is more Secure than NAT instances. (02 Amazon takes care for you.

Exam Questions:

* Dynamo DB uses "Conditional writes" to data items, i.e. for PutItem, DeleteItem & UpdateItem operations.
* Dynamo DB requests are eventually consistent reads unless specified using Consistent Read Parameter.
* Cloud Formation templates do not have any limit.
  Stacks have 200 default limit)
* Max Retention Period for SQS is 14 days.
* Dynamo DB Tables per account 256 } Both can be increased
  S3 buckets per account 100 } by contacting AWS.

* Dynamo DB "UpdateTable" does not consume Capacity units. All other does.
* ProvisionedThroughputExceededException → Can also come if the Table's Partition Capacity exceeds.
* S3 buckets: (Naming Conventions)
  → Bucket name 3 to 63 chars long.
  → Contain only lower case chars.
  → Start name is lower case or numbers.
  → Can't name ←, end with dash or Period.
  → Can't be a IP address.
* Cloud Formation → invalid Syntax in JSON template then won't even continue with Stack deployment.
* S3 - 403 Error - Access denied - Invalid Access key ID
  → Missing Security Header → NO 404 Error code.
  404 Error - NoSuchBucket.
  409 Conflict - BucketNotEmpty

AWS Template format version (optional)
Resources (Required field)

* Cloud formation template → Optional conditions - Spin instances type based on Environment.
* S3 - Multipart Upload
  * Allows to stop & resume uploads.
    Uploads in Parallel.
  → For objects larger than 100 MB → Consider Multi-part
  → Can upload objects as & when creation. Scalability.
* SQS Queue → want to make sure message does not become visible again?
  API → DeleteMessage.
* SQS Queue :
  API : ReceiveMessage - retrieve the message
  ChangeMessageVisibility - increase visibility timeout.
* SQS visibility TimeOut - 30 seconds -
  0 means - message immediately available.
* SWF - Decider, Activity worker - Polls tasks for work & making decisions.
  Workflow starter → First task of workflow.
* Recommendations to ensure load-testing requests are evenly distributed :
  ① DNS should be re-resolved - Otherwise tests might continue to hit single IP address when ELB has allocated multiple IP addresses.
  ② Use multiple / 3rd party test clients to simulate increased load.

* Dynamo DB max number of Tables Per account can be increased.

* Dynamo DB Provisioned Throughput can be increased by Contacting AWS Team.
  Ex: US (N. Virginia Region)
  Per Table – 40,000 read Capacity & write Capacity
  Per Account – 80,000 read & write Capacity.

* EBS volume – Secure data at rest
  ✱ Using an Encrypted File on top of the volume
  i.e. Using Encryption at OS level.

* S3 – Introduce Randomness to key.
  ⇒ Add Hash String as Prefix to key name. Ex: Compute a MD5 hash of the Char Seqvence. From this hash, Pick Specific number of Chars and add as Prefix to keyname.
  HH-DD-MM-YYYY-log-instance-ID
  This is random.

* Dynamo DB – When using a large Scan operation, use a Reduced Page Size to minimize the impact of a Scan.

⇒ Scan operation Provides a Limit Parameter that can be Used to Set Page Size for your request.

* AWS Elasticache is a distributed in-memory key-value Environment.

* SQS – How to handle unsuccessfully Processed messages?
  ⇒ Configure "Dead letter queues".

* SQS Supports TLS 1.0, TLS 1.1 & TLS 1.2 Protocols.

* SNS – max number of Topics allowed – 100,000.

SNS – MessageId – A universally unique identifier, unique for each notification published.

* Does CloudFormation support EC2 tagging?
  Yes. AWS also automatically tags EBS volumes and EC2 instances.
* CloudFormation parameters & outputs limit?
  parameters – 60
  outputs – 60
* What type of data can be stored in S3?
  Virtually any type of data format.

* DynamoDB → Can't support complex relational queries or complex transactions.

* Customer needs to contact AWS permision for all penetration tests.

* AWS Flow Framework enables you to develop SWF based applications.

* SWF – Max – Activity Tasks – 1000.

* How to ensure max preserve versions protection in S3?
  ⇒ Using versioning's MFA Delete capability.

* AWS ELB Protocols ⟹ HTTP & HTTPS, TCP & SSL only.
* ELB Connection draining - max connection time - 300 seconds.

* VPC - 200 Subnets Per VPC

* Multi Part Upload (S3) - 3 step Process.
  ① Initiate the Upload
  ② Upload the Object Parts
  ③ Complete MP Upload

* Cloud Formation Template
  - valid Sections : Parameters, Outputs, Resources

* Auto Scaling Pricing - Enabled by Cloud watch & EC2 - Free

* Dynamo DB - Partition key ⟷ Hash key
  Sort key ⟷ Range Attribute. - Physically Stored Closer.

* S3 - Header to request Server-Side encryption.
  ⟹ x-amz-Server-Side-encryption.

* RDS → Can be deployed within a VPC
  Supports automated backups.
  DB's Supported - MySQL, MariaDB, PostgreSQL, Oracle, MS SQL Server.
  * Each DB engine has its own supported features.

** Fail over Process for multi-Availability Zone RDS
  ⟹ The DNS record for the RDS endPoint is changed from Primary to Standby.

* S3

* When there is an error, header info contains:
  Content-Type: application/xml
  An appropriate 3xx, 4xx or 5xx HTTP status code.

EC2 → When you pass the logical ID of an AWS::EC2::Instance object to intrinsic Ref function, the object's InstanceId is returned.

⇒ EC2, VM role can be added only from console, not using AWS console.

SQS: In addition to XML, JSON and unformatted text, an SQS message may contain certain Unicode characters.

DynamoDB: Max item size range 1 byte upto 400KB.

Cloud Formation → list all resources that belong to a CloudFormation stack..
  ⇒ List Stack Resources.

* Provides a set of python helper scripts to install S/W & start services on EC2 instances
* Can be used with:
  i) Chef
  ii) Puppet } helps to manage infrastructure.
* Data can be saved when a stack is deleted.
  i.e via deletion Policies → Snapshots be created to EBS volume or RDS or S3.

* Dynamo DB : NO limit on the number of attributes an item can have. However, the total size of an item, including attribute names and values cannot exceed 400 KB.

* SNS topic → Time for a user available for confirmation. 3 days.

* SWF → max 10,000 workflow.
  * 100 SWF domains, 1000 Activity Tasks.
  * Humans can perform an activity task, but not a decision task.
* DynamoDB → Smallest amount of reserved capacity units (reads or writes) is 100.

* S3 ⟹ Supports SNS notification events
  * New object created event - S3 : Object Created : Put
  * An object removed event - i.e notification when an object is deleted or version object permanent deletion. S3 : Object Removed : *
    S3 : Object Removed : Delete Marker Created.
  * An RRS object lost event

* S3 Object range 0 bytes to 5 TB.
  Singe PUT → max is 5GB.

* All S3 resources i.e. buckets, objects & related sub resources are private ; Only the resource owner, an AWS account that created it can access the resource.
* There is no Read Object in S3. The API call to get an object is Get Object.

* ELB → Use Fn::GetAtt to get the DNSName of the ELB.
  Ex: "Fn::Join" : ["", ["HTTP://", {"Fn::GetAtt" : ["ElasticLoadBalancer", "DNSName"]}]]

* SNS Subscription :
  * UnSubscribe URL
  * AWS Console → Delete the subscription.

* S3 website Hosting : Make sure to change the Permissions on the index.html file, so that everyone has access.

* IAM : Best Practice is to create roles which has specific access to an AWS Service & then give the User Permission to the AWS Service via the role.

* Which API call occurs in the final process of creating an AMI?
  Register Image. → Final step before you can launch an instance from the AMI.

* All Operations on Elastic IP addresses can be performed Programatically through the API, or manually from the AWS Console.

* SNS message body has :
  - Message Id
  - Topic ARN
  - Subject
  - Message
  - Time Stamp
  - Signature
  - Signing Cert URL
  - UnSubscribe URL

* SNS : SNS notification to mobile endPoints ?
  (1) Register the app with AWS.
      i.e Enter name for app, Select Platform Supported, Credentials
  (2) Create an endPoint for the app & mobile device
  (3) EndPoint is now ready to be used by SNS.

* SQS : Need to send more than 256 KB data ?
  ⇒ Use the SQS Extended Client library for Java. This will enable you to send data as large as 2GB.

** Receive Message Wait Time Seconds ⇒ To enable long Polling Set this to greater than 0 & less than or equal to 20 second

** Can Create unlimited message queues.

** Does SQS Support Anonymous Access ?
  Yes. Configure an Access Policy that allows Anonymous users to access a message queue.

* SQS is DS certified. (Level)

* AWS officially Supported AWS SDK.
  Java .Net Node.js
  PHP Phyton Ruby
  Go C++ AWS mobile.

* Amazon Bundle an instance store - windows instance.
  Bundle Instance.
* Diff b/w Amazon EBS & instance-store
  * for EBS → instance type & kernal can easily be changed while instance is stopped.

* SWF use cases:
  - Media Processing
  - Business Process Automation
  - Data Analytics
  - Migration to the Cloud & Batch Processing.

* Ways to Access SWF.
  - Aws SDK for Java, Ruby, .Net & PHP.
  - Aws Flow Framework for Java
  - Aws SWF Web Service APIs
  - Aws Management Console.

* Cloud formation.

* Fn::FindInMap - Get keys from a two-level map declared in mappings section.
* Fn::Select - Returns a single object from a list of objects by index.

* Info on the stacks based on a specific filter i.e StackStatusFilter.
  ListStacks.

* Default Timeout of Temporary Security Credentials : 1 hour — min is issued by AWS 15 minutes.

* BatchGet Item api can retrieve upto 1MB of data, which contain as many as 100 items.
  * Can retrieve items from multiple tables.

* DynamoDB supports document and key-value data models.

* limit Access to S3 → Bucket Policies
  Access Control lists.

* S3 bucket uses HTTPS protocol in its URL
  S3 Hosted website uses HTTP protocol.

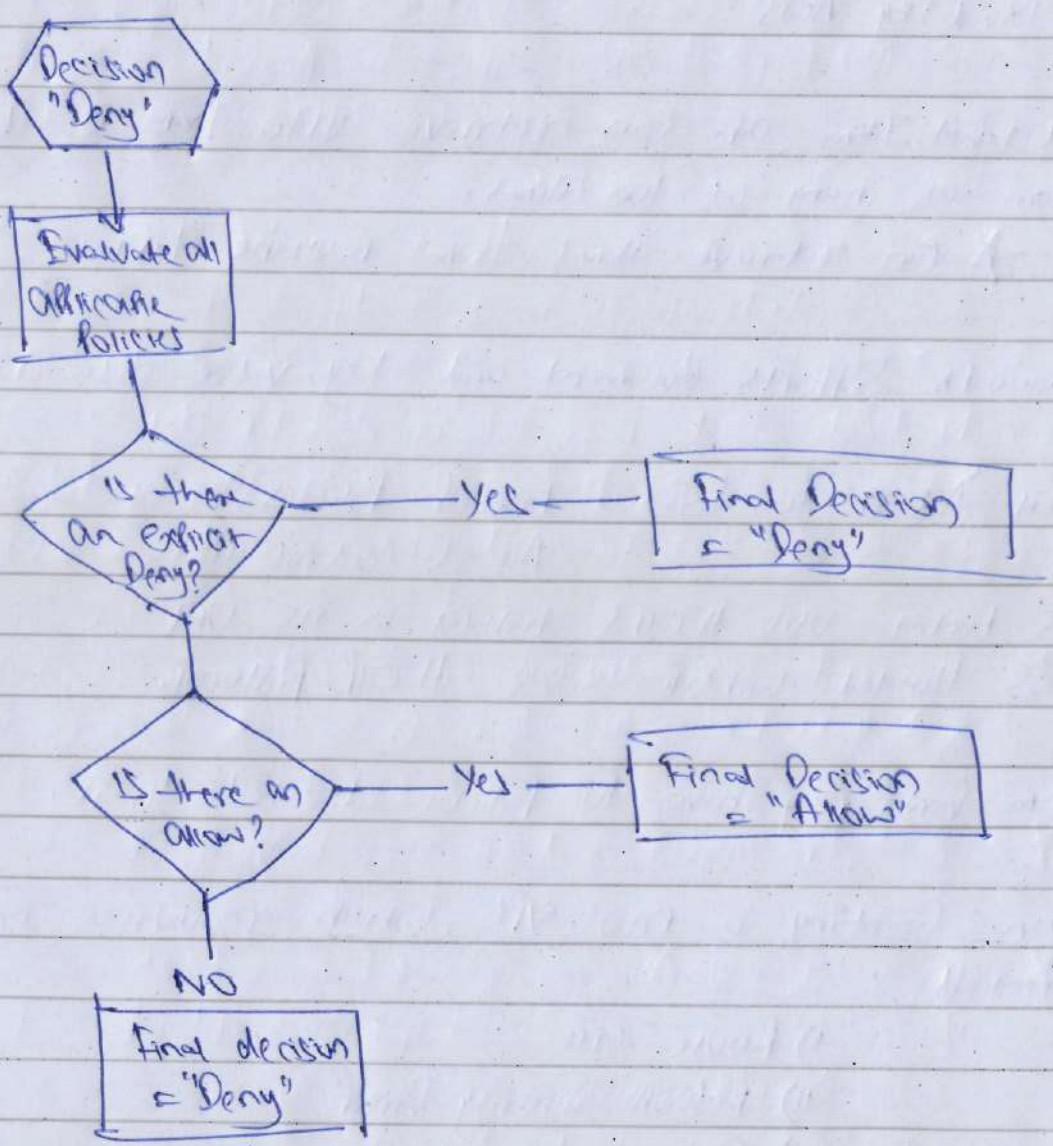
* IAM group may have 10 policies attached to it.

* When creating a new VPC, which resources are automatically created :
  i) Route Table
  ii) Default Security Group.
  iii) Default Network ACL's

* A Subnet can be associated with only one Access Control list.

* VPC's allowed in a Single region by Default → Five.

* Evaluation logic of IAM Policies.



* SNS owner operations :-
  - Create Topic
  - Delete Topic
  - Add Permission
  - Remove Permission