Monday, October 28, 2019

Basic AWS Services

- Region
- Availablity Zone
- Edge location

AWS Services

- Light Sail (Word press, virtual private server)
- Elastic bean stalk (upload code and rest taken care)
- Batch (batch computing)
- Elastic cache(manage and scale a distributed in memory cache in the cloud. cache commonly querying values in database)
- SnowBall - petabyte snowmobile - exabyte
- Migration
    - AWS migration hub
    - application discovery service
    - data migration service
    - server migration service

- Developer Tools Code Star, Cloud IDE, Code Commit, Code Build, Code Deploy, Code Pipeline
- X - Ray - analyze the behaviour of distributed applications by request tracing, exception collection and profiling
- Cloud Trial- records all API calls to AWS and delivers the log files to S3. Auditing,
- Config - provides inventory of your AWS resource. history of changes to these resources, rules for evaluating against compliance
- Ops works - chef and puppet way of automate your environment
- Service catalog - allows organization to manage approved catalog of IT resources and make them available for employees
- system manager - central place to view and manage your aws resources (patch update)
- trusted advisor - security issues open, cost savings money, scan your aws environment, improve security and reduce cost
- Managed services - IT operation management for AWS(change , incident, provision, patch, access,security, continiuty, reporting, ITSM management)
- Media services
    - Elastic transcoder - one format to another format (ipad to iphone)
    - media live - video input to live output (thanthi tv)
    - media store - store video assets
    - media tailor - advertise in video
    - media package - prepare,protect, distribute streaming video content to broad range of devices
- Machine Learning
    - Sage Maker - build, train and deploy machine learning models
    - comprehend - analyze unstructured text, NLP and text analytics, good and bad about product
    - Deep lens - deep learning enabled video camera , who is coming in and out
    - lex - chat bot, voice and text

    - machine learning - building ML models and generate prediction
    - Polly - turn text to our life like speech
    - Rekognition - search and analyze images
    - Translate - translate text in realtime

- Analytics
    - Athena - query data in s3. run query like excel
    - cloud search - search service for aws.
    - elastics search service - setup and operate and scale an elastic search cluster.
    - Quick sight - business intelligence tool
    - data pipeline - move, integrate and process data across AWS compute and storage resources as well as on premise resources.
    - Glue - ETL migrate large amount of data.
- IAM
    - Cognito - offers user pools and identity pools. User pools are user directories that provide sign up and sign in options for your app users. Identity pools provide AWS credentials to grant your users access to other services.
    - Guard duty - monitor aws for malicious activities
    - Inspector - analyze application security. generate report based on severity,install on ec2.
    - macie - sensitive data scan in s3
    - certificate manager - provide, manage and deploy SSL/TLS certificate.
    - directry service - host and manage directory service. (integrate microsoft AD)
    - WAF and shield - protect against DDOS and malicious traffic
    - artifact - aws compliance report, PCI reports
- MObile services
    - mobile hub - build, test and monitor mobile apps
    - device farm - testing your iphone , android app in real time

- Others
    - Amazon MQ - message broker for apache ActiveMQ
    - Amazon Connect - call center.
    - Alexa for business - meeting room
    - chime - VC hangout
    - work docs - docs
    - work email - email
    - work spaces - vdi
    - app stream - citrix

IAM

- Users, Group, Role, Policy(Permissions)
- Policy - Inline Policy, Managed policy
- Identity Federation - external identities are granted secure access to resource in your AWS account without having to create IAM users. External identies can be corporate identity provider(AD) or web identity provider(Amazon, Google). To enable this create Identity Provider(IDP) to enable trusted relationship between your account and identity provider.
- You can setup own password policy
- IAM Global
- Default User - No access

- Policies

  Effect - "Allow"
  Action - "List Bucket"
  Resource - "arn:aws::testcloudbucket"

- Access Advisor - who access what
- SSH Key - Code Commit Repo, External users - x509 certificate to use EC2 command line interface.
- One IAM role can be tied to instance
- Temporarily credentials associated with IAM role are automatically rotated multiple times a day. New credentials are available no later than 5 mins before the existing is going to over.
- Temporary credentials
  - Aws access key, secret key and security token.
  - Request token for their own use by calling STS Get session token API. default expiration is 12 hours
  - Temporarily security credentials can be revoked before expiration
  - Temporariy crentials can be obtained by GetFederatedtoken, Assume Role, Assumerole with SAML, Assume role with web identity STS API's

- Assume Role - AWS

  Primary user(not root user) -> STS Service Assume role and resource is other account
  new role s3 policy to list bucket add trusted entity as account user(1)

* KMS can't be deleted for 7 to 30 days
* Cross account role

  accessing other account bucket

* Credential report - Stored for 4 hours

Encryption

1) Encryption Types
   a) Data at Rest
      i) SSE encryption - AES 256 (AWS Provided master keys) aws/s3, auto key rotation
      ii) KMS encryption - Customer provided master key , manual key rotation, additional benefit of cloud trial logs who used when? , suspend keys any time.
      iii) Client side encryption and uploaded to S3

For KMS keys will be there in aws managed or customer managed keys.
aws/s3, aws/ebs aws/lambda etc.....

b) Data at Transit
1) SSL encryption

2) Hardware Security Module
KMS is shared hardware tenancy module. keys are in their own partition of the encryption module shared with other customers.
AWS Key data store - Keys are isolated in separate isolated module for compliance purpose
KMS only symmetric keys(same key for encryption and decryption)
HSM use both symmetric keys and asymmetric keys(public and private keys) public for encryption and private for decryption.
For HSM you need to create your cluster and have custom data store in KMS.

S3

1. Object storage and DNS compliant
2. 100 buckets per account
3. Global account
4. Region specific files can be present
5. S3 Object has key, value, metadata, ACl , version
6. Unique is key, value, versionId
7. Multipart upload - batch mode -initiate, upload, complete the process >5GB
8. Data consistency
    1. new object - read after write
    2. old object - eventual consistency

9. Security scenarios
    1) IAM Policies
    2) Bucket Policies
        Effect Allow
        Principal: account user
        Action: s3
        Resource: buckets

    3) Access control list
        with ACL's customer can grant specific permission (read,write, full control) to specific users for an individual object or bucket.

        ACL is sub resource attached to every S3 object and bucket. when you create a bucket or object S3 creates a default ACL that grants a resource owner full control over the resource.
        ACL your account, log delivery group, other account, everyone

    4) Query string authentication
        limited time validaity, presigned urls

Features	S3 Standard	S3 RRS	S3 Standard Infrequent	S3 One Zone IA	Glacier
Durability	99.999999999%	99.99%	99.999999999%	99.999999999%	NA
Availability	99.99%	99.99%	99.99%	99.95%	NA
Storage	Multi devices and multiple AZ	Multiple devices and multiple AZ but does not replicate.	Multi devices and AZ storage	One AZ Zone	Archival data
Fee	Higher	Lower than S3	Lower than S3	Lower than S3 IA	Lower fee compare to all
First byte latency	Milli seconds	Milli seconds	Milli seconds	Milli seconds	Expedited - quick Standard - 3-5 hours Bulk - 5-12 hours (archival retrieval JOB)
Minimum storage period	NA	NA	30 days	30 days	90 days
Accessiblity	Frequent	Frequent	Less Frequent	Less Frequent	Rare
Usage	Hosting, cloud apps	Temp image storage, netflix, reproducible,	Backup data	Backup data	Very old archival data
Retrieval Fee	NA	NA	Per GB retrieved	Per GB retrieved	Per GB retrieved

10) Intelligent Tiering - optimizes frequently and infrequently accessed objects.
11) Glacier - direct upload is possible. submit job request for retrieval. retrieval creates a temporary copy of data in s3 RRS and S3 IA. event notification is possible. Glacier has multiple vault each vault has archives. vault is container
12) Cross region replication- version need to be enabled in both buckets at two regions.
13) Versioning - once enable you can only suspend
14) Transfer accerleration
15) Events - lambda
16) life cycle management
17) Server access loggin - detailed records of requests made to the bucket. (log delivery group access), in same region bucket
18) Object level loggin - action taken by users will report in cloud trial.cloud trail in json yy mm forat etc.

19) Requester pays - charge for request and data download
20) delete and cancel is free
21) checksum data corruption
22) Query in place (select) - select where commands in data, no download of data, in csv, json and parquet.
23) Inventory - full inventory of s3 bucket or object in csv, orc, parquet files. weekly emial rpeort
24) S3 batch - update tag etc. update access controllist

Cloud Front

1. Web and RTMP (movies)
2. Check if data is there in edge location if not go and pull from server. (first is slow)
3. TTL
4. Both read and write.
5. If you clear manually before TTL charge is there.
6. Restrict Viewer Access - signed url or cookies.
7. Geo location - white list or black list. which location you can use.
8. S3 bucket is public and not KMS encrypted.
9. Usage S3 bucket -> static websites EC2 -> Dynamic websites
10. custom origin server also.
11. Lambda edge -> run edge locations without compromising or managing servers, responding to end users quickly at the low latency.
12. Cloud front events
    Viewer Request, Viewer Response, Origin request, origin response
13. Global not region specific
14. Security of cloudfront - shield and WAF

Storage Gateway

1. on prem to cloud connection for storage.
2. Storage gateway software appliances available for download as Virtual machine(VM) image that you can host in your data center. Do the activation to aws account.
3. Low latency performance and cache frequently accessed data on premises.
    a) file gateway (NFS) - video,picture and flat file, store and access objects in S3 from the file based applications with local caching. Objects in S3, Looks like File Share folder.
    Single filegateway with multiple nfs clients good for read operation and not for write operation.
    multiple file gateway - you can use read and write operation in same s3.

    b) Volume gateway(ISCSI)
        virtual hardisk (block based) os, sql server
        cached mode - low latency s3 data and frequently accessed in local.
        stored mode - both copies in s3 and local. async backed up to AWS
    c) tape gateway(ISCSI)
        archived glacier in glacier.

Snowball

1. SnowBall - 80TB petabyte - Device
2. SnowBall Edge - 100TB - datacenter in box
3. SnowBall mobile - >100TB - exabyte - Truck

SnowBall Client - identify, compress, encrypt and transfer data from local directory.
create SnowBall Job

EC2

1. AMI - template that contains software configuration(OS, application server) eg. windows image, linux image, DB image etc.
    1. AWS regular
    2. AWS market place (commercial vendors like wordpress)
    3. AWS community AMI (Ubuntu)

1. Solid State Drive Backed General Purpose - Boot Volumes, Dev Testing machines
2. Solid State Drive Backed Provisioned IOPS - Used for I/O intense database applications
3. Hard Disk Drive Backed Throughput Optimized - Big data analysis, data warehouse , log processing.
4. Hard Disk Backed Cold - requires few scans per day.
5. Magnetic Volume - backup data.

2. Instance Type - virtual servers - different CPU, memory, storage and networking capacity.
3. Instance type can be
    compute(c), memory(r), storage(i) and GPU based instances(g)
4. Root Volume - attached to EC2. instances data will persits only reboots else it will out
5. EBS volumes - block level storage /dev/xvda
6. Network, Subnet, Role, Enable Monitoring
7. Tenancy
8. User data, tags and storage.
9. Security Groups(virtual firewall on EC2) - protocol and port level. only incoming rule and no deny rule. In Bound is blocked by default and outbound is allowed.
10. Key Pair - Public key + private key
11. Each Instance has Private IP, PUblic IP or Elastic IP.
12. On Demand, Reserved,Schedule Reservation, Spot Instances, Dedicated instances, Dedicated host.
13. Instance metadata and user data 169.254.169.254
14. Shared instance (multiple customers), dedicated instances(hardware for one customer restart hardware change), dedicated host(device is for you).
15. Placement groups - logical group of instances in single AZ.
    a) cluster - cluster instances into a low latency group in single AZ.
    b) Spread - same hardware in same AZ or different AZ.(7 instances)

16. Network interfaces - instance can have many. should be same AZ. IP address will be attached to instance through Network interface.
17. Image - You can create image from instance.

18. Template - you can create an template from instance. has configuration information. you dont need to specificy for every instance creation.
19. Snapshot - create snapshot
20 Billing alarms stops - rebots, stops
21. Hibernation cost is there. - instance memory is root EBS.
22. Multiple volumes to one instance can be attached anot not one volume to multiple instances.
23. Cloud watch metrics 1 minute.

EBS

1. Block level storage
2. Two Types
    1. SSD (random, costly)
    2. HDD(sequential, less cost)

3. Different Storage Types

1. Solid State Drive Backed General Purpose - Boot Volumes, Dev Testing machines
2. Solid State Drive Backed Provisioned IOPS - Used for I/O intense database applications
3. Hard Disk Drive Backed Throughput Optimized - Big data analysis, data warehouse , log processing.
4. Hard Disk Backed Cold - requires few scans per day.
5. Magnetic Volume - backup data.

Volume Size	1 GiB - 16 TiB	4 GiB - 16 TiB	500 GiB - 16 TiB	500 GiB - 16 TiB
Max. IOPS**/Volume	16,000***	64,000****	500	250
Max. Throughput/Volume	250 MiB/s***	1,000 MiB/s†	500 MiB/s	250 MiB/s

4. IOPS - time to store any data in drive, throughput how fast data is transfer
5. cloudwatch metrics to measure IOPS and throughput
6. With EBS
    1. create new snapshot
    2. create new volume

7. EBS tied to attach or detach or modify to instance
.

Snapshots

1. snapshots are backup
2. snapshots are saved in s3.
3. incremental copies saved in s3.
4.

5. snapshot
    1. create volume
    2. create image

6. root volume - instance need to stop for snapshot creation others no need.
7. volume encrypted -> snapshot encrypted automatically
8. volume and instance should be in same AZ.
9. volume in another region -> create snapshot of existing volume. move the snapshot to another region and create volume
10. instance in another region -> create snapshot of existing instance and move it. and create image or volume in another region and create instance.
11. Each snapshot has unique identifier.
12. Regular s3 you cant access snapshot backups

EFS

1) NFS protocol - EFS connects to instance using mount target. each mount target has IP Address. Each AZ has mount target
2) Choose Performance mode (General purpose or Max I/O)
3) Choose throughput mode (bursting and provisioned) bursting - normal applications and provisioned for high throughput
4) SecurityGroups - can be configured for the mount target who can do the mounting
5) Read after write consistency
6) Block based storage
7) Load data from EC2 or on prem servers
    outside vpc - classic link
    on prem - direct connect
8) Storage classification

Amazon EFS is a file storage service for use with Amazon EC2. Amazon EFS provides a file system interface, file system access semantics (such as strong consistency and file locking), and concurrently-accessible storage for up to thousands of Amazon EC2 instances.

Amazon EBS is a block level storage service for use with Amazon EC2. Amazon EBS can deliver performance for workloads that require the lowest-latency access to data from a single EC2 instance.

Amazon S3 is an object storage service. Amazon S3 makes data available through an Internet API that can be accessed anywhere.

9) Data loading

AWS DataSync provides a fast and simple way to securely sync existing file systems with Amazon EFS. DataSync works over any network connection,

10) storage class

Amazon EFS offers a Standard and an Infrequent Access storage class.

11) has own life cycle management
12) backup files - AWS Backup

Lambda

1. handler, event, context(time to run) , logging, exception
2. one lambda function can trigger another function.
3. source code will be in s3, versioning by default.
4. AWS Lambda functions being invoked synchronously will return a throttling error (429 error code)
5. Lambda edge - cloud front request will come to lambda edge run at those locations. All edge location you need to have your code. each location can have different version of code. viewer request, viewer response, origin request, origin response.
6. lambda should in VPC
7. Step functions - invoke multiple lambda functions. in parallel way.

Route 53

Ping google.com -> .com(top level server) -> google.com(name server record) ->(SOA record) A record(101.1..1..)
DNS Resolver has TTL how long the cached query need to be there

Route 53 do the health checks

1) Register the domain or Transfer the Domain
2) Create a Hosted Zone (Public or Private)
3) Each hosted zone has NS record and SOA record
4) For private hosted zone (enableDNS Host names need to be enabled at VPC)
5) Record Set Types
    i. A Record -> your server IP Address
    ii. Alias Record -> S3 buckets or ay AWS services
    iii. Cname Record -> google.com www.google.com https://google.com reference the existing A record
    iv. MX Record -> mail server domain
    v. NS record -> Authoritatitve server for sub domain
6) Routing Policy
    i. Simple Routing Policy - 10.0.1.01
    ii. Multi Value Routing Policy - 10.901.1.1, 10.1.1.1, 10.2.2.2
    iii. Failover Routing Policy - Primary and Secondary (health check is must)
    iv. Weighted Routing Policy - (configure three individual A records, 10%, 20%,70%
    v. Latency Based Routing Policy - (configure region for each A record)
    vi. Geo Location Based routing -(configure North America , Europe
Geo Proximity Routing (you can configure the routing based on teh coordinates)

Cloud Watch

1. Monitoring services
2. You can get logs, show metrics like CPU usage,
3. Respond to events based on the log or metric data. event
4. Network usage and CPU usage is default metrics in cloud watch.
5. Install agents on EC2 instances to send monitoring data about the instance to cloud watch.
6. Query -> Insights - You can run a query like splunk and search and visualize the data. (Filtering logic)
    1. Eg: Route 53 queries number of requests, number of exceptions, cloud trial queries, vpc flow log queries, lambda queries , app sync queries like http status code.

7. Monitoring
    1. Basic Monitoring - Free, polls every 5 minutes, 10 metrics, 10GB data ingestion and storage
    2. Detailed monitoring - chargeable, charge per instance per month, every minute per second.

8. Metrics
Allows you to record metrics for EBS,EC2, ELB ,S3, Dyanamo Db, Billing (real time charge as soon as you change the value type of this you can see results)

9. Events - lambda
10. Alarms - warning CPU utlization is high

11. Cloud Trial - who is doing what with the API calls, recording api calls actions, source IP Address etc. (CCTV Survlience)
12. Cloud watch - performance monitoring, alarms, billling report and dashboard. (Gym trainer)
13. Cloud watch - monitor the applications & performance 5 minutes default and detailed monitoring for 1 minute.

ECS

1. In ECR - Create new repository and push your docker images that you created locally with the docker file.

2. Create Task Defintion (EC2 or Fargate)
    TD is nothing but which containers are included in task.
    Elastic Task Role - which AWS services that container can use it.
    Task Execution Role - pull images from ECR and publish container logs in Cloud Watch
    Task Memory
    Task CPU
    Volumes
    Add containers (any number of images you can add)
        Image Name
        Port Configuration
        Health Check, Environmental variables , Log Cloud Watch for container

3. Create Cluster(EC2 or Fargate)

Logical group of Amazon EC2 instances that you can place containers onto, can use different instance type in a same VPC. Can manage the state of containers on a single EC2 instances. ECS agent communicates with the docker daemon on the EC2 instance.

4. Create Service(Fargate or EC2)
Chose the task defintion
number of task.
Deployment Type(Blue green, Rolling update)
VPC, Subnet, security group, ALB, Auto scaling
Each service has the tab "Task" which is running.

If you choose instance based then "ECS Instances will have values instance running"
You can look at metrics
You can see the log at task wise.

Logical group of Amazon EC2 instances that you can place containers onto, can use different instance type in a same VPC. Can manage the state of containers on a single EC2 instances. ECS agent communicates with the docker daemon on the EC2 instance.

EMR

1. Elastic Map Reduce tool for large scale parallel processing of big data and other data workloads.
2. Log Analysis, machine learning, financial analysis, simulation.
3. upload, create, monitor
4. Cluster - Spark, hadoop, HBase, Presto
5. AWS Glue Catalog for metadata

Master node - Cluster (HDFS, Spark etc) No spot instances. Master fails then all other fails. It manages HDFS. Distrubute work loads, monitor health. Login to master node via ssh.
Core Node - They run tasks and manage data for hdfs. If they fail can cause cluster instablity
Task Nodes - Optional, run tasks. Spot instances

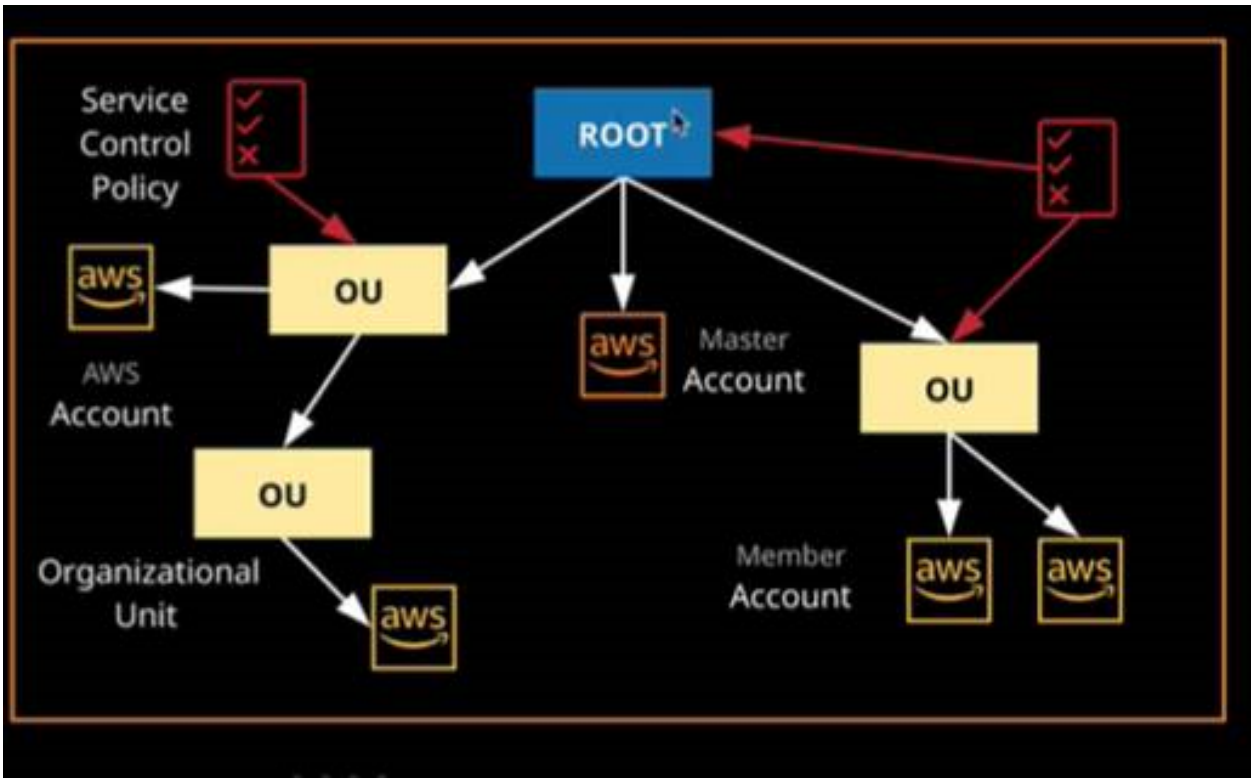
S3 location - input and output location. For data.

AWS Organization

1. AWS organization is managing multiple accounts in single business.
2. COnsolidated bills and discounts.

3. Limit account usage using service control policies.

Eg:
1) create organization. very master account by email.
2) you can add new accounts. member accounts. or can be organization accounts



Service Control Policies
Service Control Policies what individual account can do. It will define service control policy to only allow an account to access S3. SCP applies for root account, other organization unit or member accounts.

Role Switching
For each member account "IAM account" gets created. Role switching is method of accessing one account from another using only one set of credentials. It is used both within AWS organizations and between two unconnected accounts. For switch role you need the Role Name and Account Id

Trusted Advistor

1. scans your infrastructure and compares it with best practices in five categories.
    a) cost optimization (DB not connected for 7 days)
    b) performance (large EC2 apply)

c) security(s3 bucket permission)
d) fault tolerance(RDS multi AZ)
e) service limit(subnet usage limit)

Auto Scaling

1. Have your AMI (DB Server AMI, App Server AMI, Web Server AMI)
2. Create Launch Configuration group(Choose AMI, memory, instance type ,security group etc)
3. Create Auto Scaling group (Choose VPC, Subnet)
    a. Group Size - Number of instance at any time. (choose 2 AZ or more for easy span out

b. Scaling Policies ->
    i. You can keep this at initial level(group size specified)
    ii. Use scaling policies to adjust the capacity of this group -
        1. **Simple Scaling Policy** Scale between 1 to 2 instances
            Eg -> if average cpu utilization is 70 then do scale up one more server.
            Simple scaling policies must wait for the cooldown period to expire after a scaling activity or health check replacement before they can respond to alarms that are breached.

        2. **Step Scaling Policy** Scale between 1 to 10 instances
            Increase -> Eg -> When Average CPU utilization is >70 for some period then scale up more server
            For increase you need warm up period -> 60 seconds to warm up after each step (eg: based on userdata scripts you need that need to executed)
            Decrease -> Eg -> When Average CPU utlization is <50 for some period then scale down server.

            You can remove/add or set to 10 instances or two instances for increase and decrease or you can set in %
            Scaling policies with steps continuously evaluate alarms as they are breached, even while a scaling activity or health check replacement is in progress.

Health Check Grace Period -300seconds The length of time that Auto Scaling waits before checking an instance's health status. The grace period begins when an instance comes into service.(default is 300 seconds)
Default cool down period is 300 seconds

You can tie up Load balancer with Auto Scaling group
Auto scaling is free.

For the alarm policy you can send notification as well.

Metrics Values

Average CPU Utilization
Network In
Network Out
Application Load Balancer Target In

Disk Read/Write Operations (only for step up scaling policy)

Load Balancer

1. Application, Classic, Network Balancer
2. LB can be internet facing/intranet facing
2. What is the Listner Type HTTP 80
2. AZ (Two AZ)
2. Choose Security Groups
2. Configure Target Groups (Instance, IP, Lambda , route url, port)

Your load balancer routes requests to the targets in this target group using the protocol and port that you specify, and performs health checks on the targets using these health check settings. Note that each target group can be associated with only one load balancer.

2. Map the autoscaling to the target groups

3. load balancer is a device that acts as reverse proxy and distribute network or application traffic across number of servers.
4. Load balancers are used to increase capacity(concurrent users) and relablity of applications
5. Classic LB -> distribute traffic equally
6. Application LB -> image 1 lb, image2 lb, distrubute load

Sticky Session - Bind user session to particular Ec2 instances
Cross zone load balancing - load balance multiple availablity zones
Load balancer has its own "DNS Names"

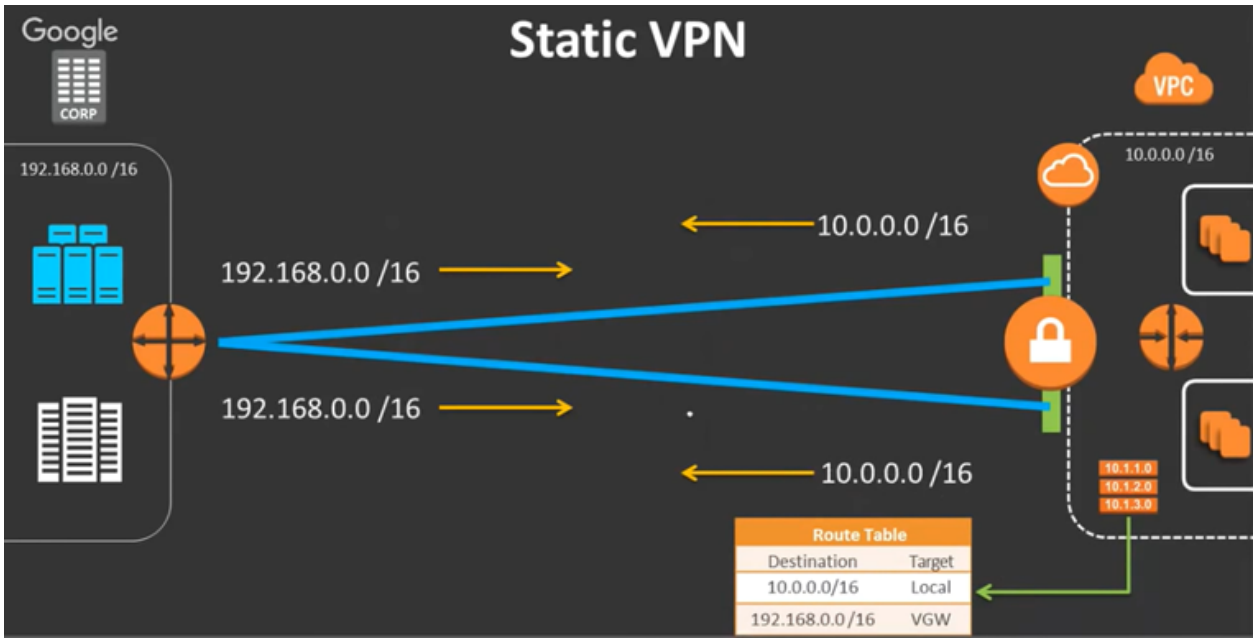
VPC

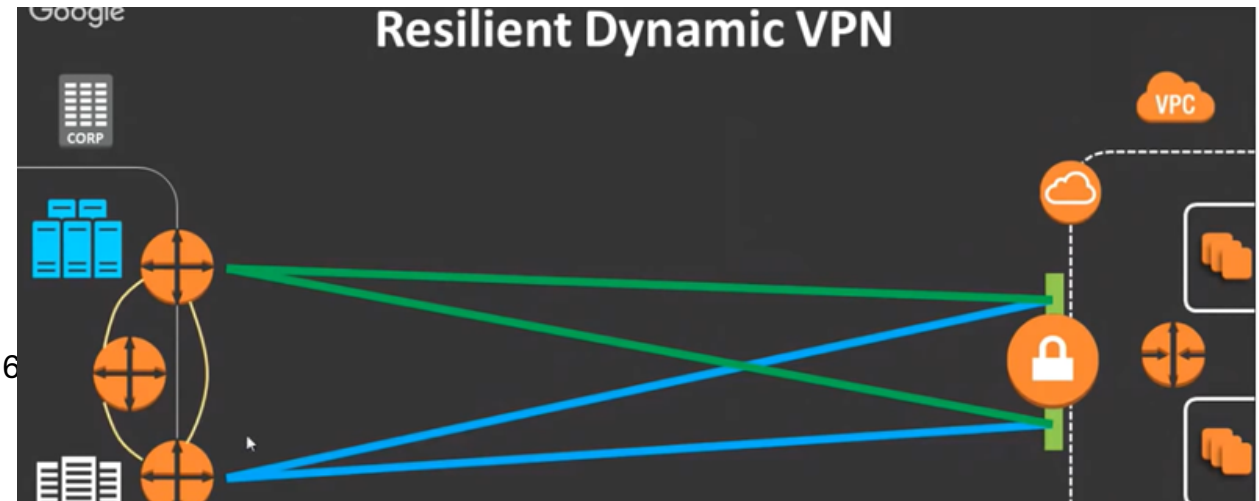
1. Life before VPC - router and ISP, connectivity
2. VPC - Isolated, In single region Single machine or multiple machines has IP Ranges - 10.0.0.0/16
3. Subnet - (private or public subnet in single AZ) 10.0.0.0/24 and 10.0.1.0/24
4. EC2 Instances 10.0.0.1 or 10.0.0.2 (private IP's)
5. Route Table - decides the subnet private or public. look at info in route table and route it accordingly
    1. Source Destination
    2. 10.0.0.0/16 Local
    3. 0.0.0.0/0 IGW
6. ENI - Virtual Network card tied to instance.
7. Internet Gateway - public subnet talks to internet through this IG.
8. VPN connection is established through your home router, customer gateway and Virtual Private Gateway. This establishes IPSEC connection.
9. VPC Peering - connecting two VPC. Peering connection who is acceptor and requester. have two private instances in two vpc and they want to connect. Do the route table configuration, should in same region, may be different account. no overlapping ip, no transitive peering, no edge routing. No IGW routing , no cross referencing of security group.
10. VPC Endpoint - private talk from EC2 to S3. EC2 to Dynamo DB

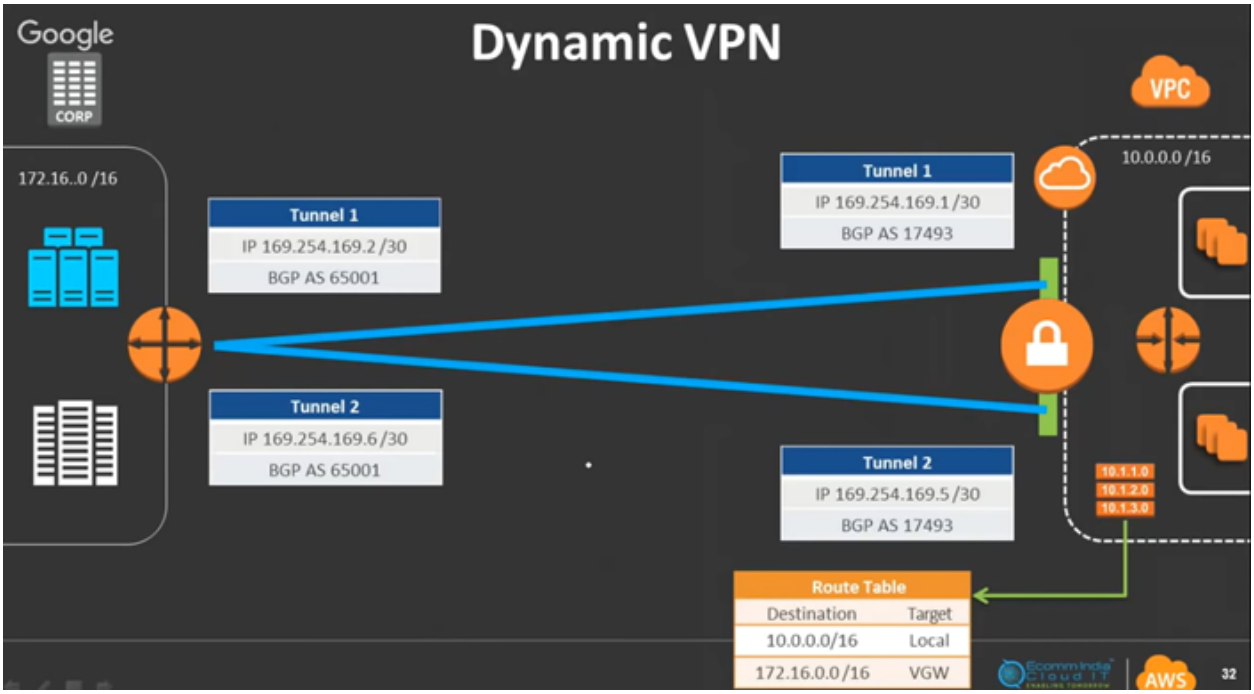
11. NAT Gateway - instances in private subnet talks to internet using NAT gateway. Outside user <- IGW <- public subnet <- NAT Gateway <- private subnet .
12. IP Address 0,1,2,3 and last is used by reserved IP Address.
    1. 10.0.0.0- 10.0.255.255
    2. 192.168.0.0/24 => 192.168.0.0 - 192.168.0.255

13. VPC Interface Endpoint - All other internet request routing
14. Security group is stateful and Network ACL is stateless
15. Security Group Inbound rules enter at port level and outbound is allow all. You can another security group in as well.
16. Network ACL - subnet level. rules are evaulated at incremental level(100,122)
17. VPC Logs (VPC or subnet level, or network interface) - cloud watch level. Flow logs are not realtime. and dont capture actual traffic. only metadata on the traffic.
18. Bastion Hosts - Any instances in private subnet can be connected using bastion host in public subnet. From bastion host talk to private subnets etc.
19. NAT instance - in public subnet. talks to IGW connects to internet. privat einstance go to NAT instance - IGW - internet

VPC - External Connectivity







Manually added static routes for a Site-to-Site VPN connection

20. Hardware VPN Connectivity
    1. Static VPN
        1. private connectivity over the internet
        2. secure IP Connection
        3. static BGP
        4. 2 IPSec per VPN Connection
        5. 2 tunnels between Customer Gateway and Virtual Gateway
        6. Static Routing means you need to share the routes in the router config with the AWS routers. If you need to add a new route with the AWS VPC you'll need to do it manually in the router config, If you had BGP configured it would take care of that for you.
        7. Manually added static routes for a Site-to-Site VPN connection
    2. Dynamic VPN
        1. BGP source and destination has BGP
        2. Each has ASN Number
        3. BGP propogated routes from site to site VPN connection.
    3. Resilient VPN
            1. multiple customer routes
            2. internal iBGP between all your routers.

19. Direct Connection

a) Regular Direct Connect
    1. Dedicated network connection(no internet)
    2. High speed
b) Dx Connect
    1) aws router are there in Dx location
    2) your router is there in Dx location
    3) Your router corpor -> dx location customer colo router – aws direct connect router (dx location) -> VPC

c) Dx partner
    If your customer don't have router to place in Dx location. Then go with partner network(sify or Verizon or Airtel or Tata telecom)
They have their router in the DX location

To avoid redundancy have multiple direct connection location multiple partners

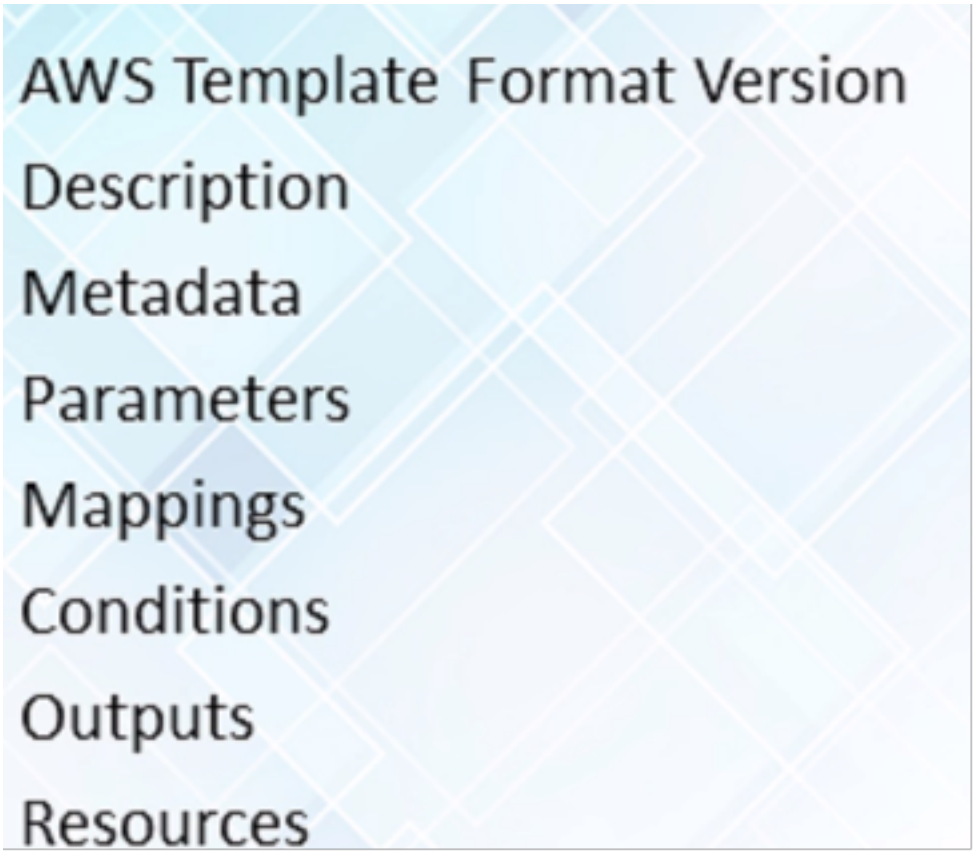
Cloud Trial

1. Any actions taken by user, role, aws services are recorded
2. store in S3 for 90 days

API Gateway

1. caching, throtiling, low cost, cloud watch logs all requests, scalablity

Cloud Formation Templates



1.resource management and infra creation.

Elastic Bean Stalk

1. upload the code
2. web app or worker nodes code.
3. Different stages

Elastic Cache

1. improve latency and throughput for read heavy application.
2. Fullly managed cache
3. Extreme performance
4. easily scalable.
5. Cache should pair with VPC,Subnet, security group etc.
6. You can use cache for database cache, session handling, object caching.
7. REDIS
    1. key value store, master/slave replication, **Multi AZ**

8. MEM Cached
    1. memory object cached. key value store, fully managed, **Scale Horizontally**

9. DAX
    1. In memory cache for dynamo DB.
    2. If item is there in DAX then cache hit if not cache miss go to Dynamo DB and get it.
    3. Item Cache - results from GetItem 5 minute TTL
    4. Query Cache - store results of query and scan operations based on parameters.

SQS

1. Pull Based
2. Each message has global identifier
3. Short Polling - messages retrieve asap. more empty messages, Long polling - wait for messages for waitTimeSeconds more efficient, less empty messages
4. Max format 256KB
5. Default visitblity time out - length of time the message recieved from a queue will be invisible to others.
6. Message retention period - max time period to retain the message.
7. Delivery Delay - the amount of time to delay the first delivery of all messages added to this queue.
8. SSE Encryption

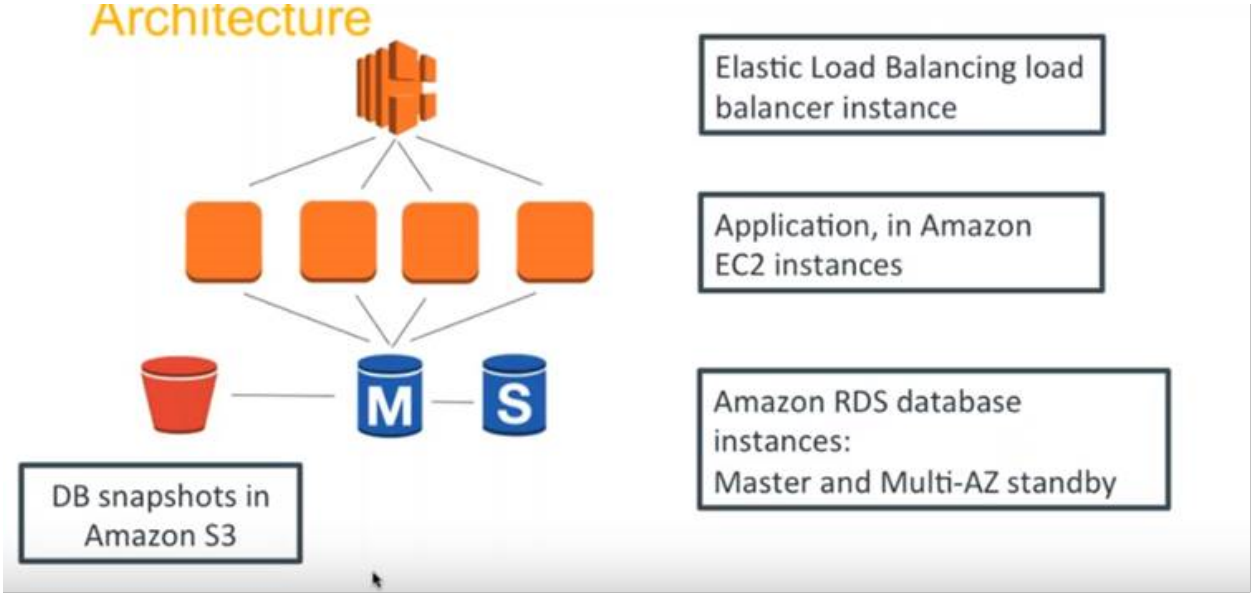
SNS

1. push based
2. 256Kb to topic
3. subscriber (https, json, email, sqs, mobile push notification, lambda, sms)
4. publisher (application, s3 events, cloud watch)

Databases - RDS

1. RDS supports - SQL, mySQL, Oracle, Aurora, PostGres, Maria
2. Storage - Auto scaling can be enabled
3. Auto back up - default is 7 days from 0 to 35 days
4. Backup window for maintenance
5. Subscribe to event for snapshots, instances, db clusters, export tasks.
6. DB Subnet group - private subnet

7. DB parameter group - configurable values timezone
8. DB optional group - manage your database, db reboot
9. Multi AZ- sync copy in another AZ in same Region, fail over automatic in case of master failure, planned mainteance happen in standby first.
10. Read Replica - async copy, 5 read replica. can have in anotehr AZ or region. automatic backup need to turn on for read replica.
11. migration of database outside VPC is not supported.
12. AWS config can be used to record changes in DB.



Databases - Aurora

13. 6 Copies of data in 3 AZ
14. Self healing of database.
15. 64TB Size
16. comptablile with PostGres and Mysql
17. each instance has reader and writer end point. so 3 reader and 3 writer

parallel Queries - you can run queires in all nodes
1) one writer multiple reader
2)one writer multiple reader - prallel query

3) multipe writer
4) serverless

Databases - Dynamo DB

18. Key value pair
19. spread across 3 AZ
20. stored in SSD Stroage
21. eventual consistency -> >1 second read best response (default)
22. strongly consistency read <1 second read for best response
23. Tables Items, Attributes are important . Table is collection, items is rows, attributes in key value pair
24. No fixed schema
25. Region specific at table level.
26. You need role to access dynamo db table
27. ecah table in 3 AZ. it is reslient in a region
28. Each item is unique value ie partition key or partiion and sort key. partition key is hash key and sort key is range key.
29. keys and values should be of 400KB in an item.
30. Querying using partition key and sort key
    1. GetItem
    2. Put Item
    3. scan - scan full table and filter by filter condition not effeicient
    4. query - efficient , look up by parition and sort key.

Global Table - > Table need to empty, enable streams, add region, create replica table in another region and called as master. you can do read and write her.e

Serverless **- no service only clusters.**

One leader node and two task nodes.

RCU ->

1 RCU for 2 * 4Kb for eventual consistency in a table per second.
1 RCU for 4KB for strongly consistency in a table per second.

WCU ->
1 WCU for 1Kb of data

Dynamo DB Streams and Triggers

Stream s a rolling 24 hour window of changes. Streams are enabled per table. Contains all data.

KEYS_ONLY
NEW_IMAGE
OLD_IMAGE
NEW_AND_OLD_IMAGES

Get the changes form table and put in another table.

Trigger -> Streams can be integrated with lambda. Invoking a function when item changes in dynamo DB(DB Trigger)

Indexes

Local secondary index - must be creating when table creation. Same partition key and alternate sort key. They share the same same WCU and RCU of main tbale

5 LSI

Global secondary index - can create at any time. Different partition key and sort key, own WCU and RCU of main table.

20 GSI

Databases - RedShift

Columnar DB
Peta byte scaling

Kinesis

1. Scalable, resilient, streaming service from AWS.
2. Eg Amazon orders, twitter data.
3. Producers - IOT Sensors, mobile devices
4. Consumers - Lambda
5. **Kinesis streams** - streams collect process and analyze data. All incoming message stores for 24 hours and can be increased to 7 days.
6. Kinesis shards - 1MiB ingesion and 2MiB consumption. shards are added to streams based on number of shards read and write varies.
7. For multiple inputs go for kinesis than sqs.
8. Multiple consumers - read put in s3,postgres etc.
9. **Kinessis firehouse** - autoamted to put file in S3 and goes to Dynamo DB
10. **Kinesis Analytics** - Run sql queries of the data

Athena

1. Analyze data in s3 using sql queries.
2. Serverless
3. To start with
    1. define your schema.
    2. start querying

Identity Federation and SSO.

1. Identity of external providers are recognized.
2. Types of Identity Providers
    1. Cross account roles - remote account is allowed to assume a role and access your account resources
    2. SAML - An on premise or AWS hosted directory service instance is configured to allow Active directory users to login to the console
    3. Web identity federation - google, amazon and facebook are allowed to assume roles and access resource in your account.

3. Cognito and Security Token Service(STS) are used as IDF
4. A federated identity is verified using an external IDP and by proving the identity using a token and allowed to swap that ID for temporary AWS credentials by assuming a role.

High Availablity vs Fault Tolerance

High Availablity vs Fault Tolerance

High Availablity
    1) Eg; Car if fault you need time to repair and stepanie is backup
    2) Active - Passive mode
    3) Less cost
Fault Tolerant
    1) Eg: Plane - if one engine fails go with second one
    2) Active - Active mode
    3) More cost

OAI

Origin acces identity is a virtual idenitty that can be associated with a distribution. An S3 bucket can be distributed to only allows this OAI to access it. All others identities can be idenied

Restriction bucket policy access only by OAI

Works only on S3 not on corporate server, ec2