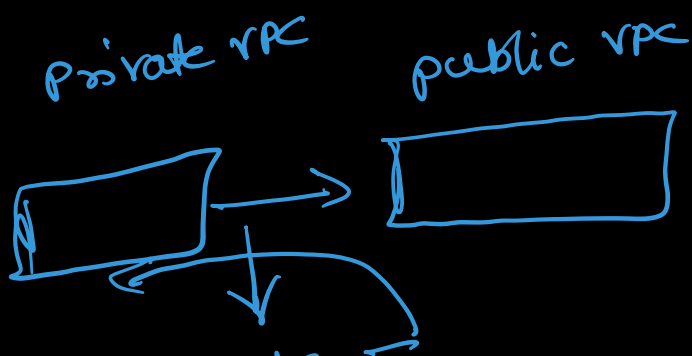
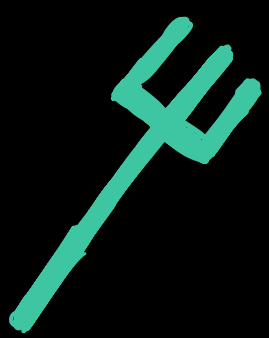
VPC will get Internet using NAT Gateways

- Route table for NAT Gateways has to be created.



Route table for NAT Gateway & Route



- EBS volumes

→ Can only be attached in the same Availability zones.

- EBS volumes dettach when EC2 instance restarts. (if we want to detach)
- If you wanna change the AZ take snapshot and create a new volume from it.
- New EBS volumes doesn't require prewarming However, Volumes which are newly created using snapshot does requires pre-warming.

- Termination protection is turned off by default
- upto 5,000 EBS volumes by default
- Upto 10,000 snapshots by default.
- Using AWS Multi-attach you can attach single provisioned IOPS volume to multiple AWS instances.

- EBS Fast Snapshot Allows You to create a volume which is fully initialized.
- once encrypted it cannot be disabled on the volume.

Amazone Lustre -
fast parallel processing open-source fs.

S3 storage

- After you create bucket, you cannot change the name.
- By default you can create upto 100 Buckets.
- You cant change its region after creation.
- Transfer Acceleration cannot be disabled, and can only be suspended.
- Bucket policies are limited to 20kB
-

ACL

- ACL can only grant permissions
- There is no explicit deny.

- Resource Based policies
  - Access control list
  - Bucket policies.

- User policies
  - AWS IAM
    - IAM user Access keys
    - Temporary Security credentials.

- Versioning
  - only owner can delete the versions.
  - once enabled cannot be disabled.

- logging in S3

- AWS CloudWatch
- AWS CloudTrail Monitoring -
  - monitor cloudtrail log files in real time by sending them to cloudwatch logs.

- for Notifications in S3
  - SNS - Simple Notification Service.
  - SQS - Simple Queue Service
  - Lambda

- Cross Region Replication

—

- Requirements for cross Region Replication (CRR)
  - Must have versioning enabled
  - Must have to be in different region
  - Must have permissions to replicate

- Only following is replicated
  - objects you add after the replication configuration.

-

This cannot be replicated
- ① objects which were added befor the versioning
  ② objects created using server-side encryption using customer provided keys. (SSE-C)
  ③ objects in bucket where the owner doesn't have the permission
  ④ object in source bucket that are replicas created by another

cross-region replication.

- You can replicate objects from source bucket to only one destination bucket.

- AWS Transfer family.

- can transfer files in or out of AWS storage.
- protocols supported - SFTP, FTPS, FTP.
- Managed file transfer Workflows (MFTW) is fully managed, serverless file transfer Workflow service to set up.
-

- Amazone S3 Event Notifications you can subscribe to the Event Notifications
  — Subscribers

Amazon S3 Access points

-

- To manage acess at a lenge scale services

access point is used as an endpoint for connection.

- Access point can also be restricated to particular VPC.

AWS AppSync - streamlines the dev of modern web and mobile Appln.

- GraphQL API -
- Appsync Pub/Sub -

- Amazon API Gateway!
  - Enable developers to maintain, monitor, and secure APIs at any scale.

- Remember this - whenever there is auto scaling involved there will be slight delay as it takes time to initialize the EC2 instances.
-

cloud HSM

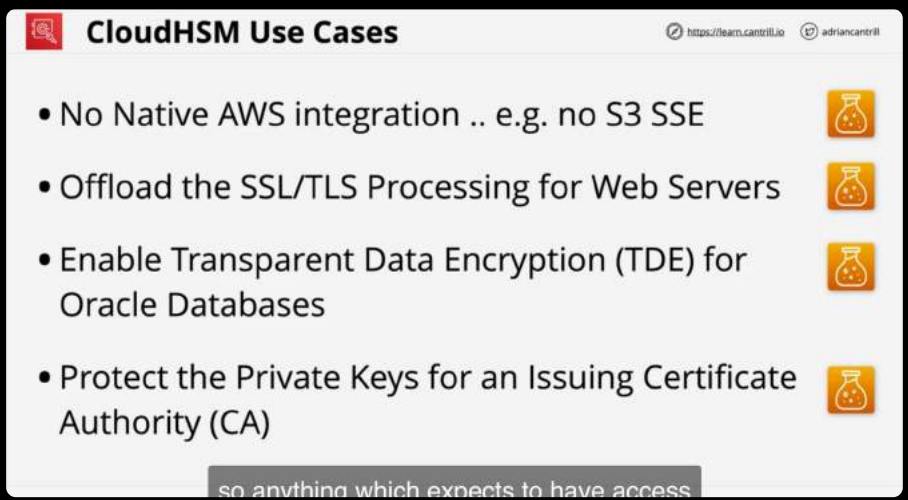
– Hardware security Module

— performance cryptographic operations and provides secure storage for cryptographic keys.

– Generate keys, manages keys other services interact with it.

- It's a single tenant Hardware security Module
- It can be cloud HSM or on-premise HSM.
- FIPS 140-2 Level 3 compliant
- KMS is 140-2 level 2 compliant.
-

- cloud HSM client has to be installed on EC2 Instances to use them.
- There is no native integration of cloud HSM with other services for ex. can't use s3 with conjuction with HSM.
- It is not accessed by Any AWS API's
- HSM can also be used to do cryptographic processing of SSL/TLS certificates and It is more economical and cost effective.
- for industry standard API or which does not include AWS the answer might be HSM.



* AWS local zone *

- So with the help of local zone's you can get even lower latency
- That is achieved by taking advantage of Az closer to your Business.
- use when you need Highest performance.

throttling limit and results caching in API

- lambda scales faster than the regular auto scaling group.

- S3 object lock can do write once read many (WORM) model.
- S3 object lock can only be created at the time of creation.
- Once enabled cannot be disabled on

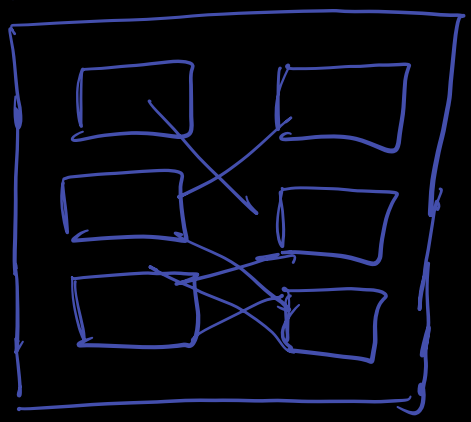
that bucket.

Acess points

- Acess points can be used to create endpoint with the S3 bucket and we can limit on who can access the bucket.

- By default Lambda encrypts the sensitive information by using the AWS key-managed services. But it is still visible to other users.
- Creating your own key gives you more flexibility including ability to create, rotate, disable and define access controls.
- To encrypt your sensetive information correctly use KMS with the encryption helpers. (Lambda)
- VPC endpoints are used to privately connect VPC to AWS services.
- cloudHub - private communication bet'n sites.
- Direct connect is for on premise to AWS Service.
- Transit Gateway - on-premise & VPC connection through central hub.
- DynamoDB - flexible schema.

placement group



Cluster

Recommended
- All instances has to be started at once
- with the same configuration.

10GB

performance, Low Latency.

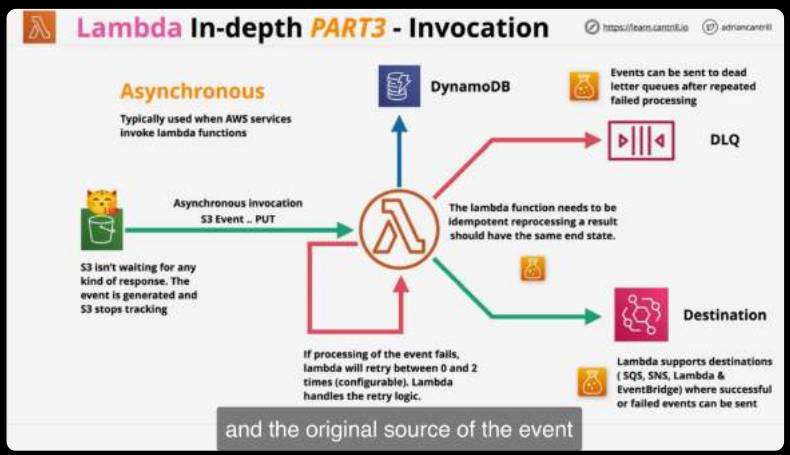
2. a Spread placemen group
   - 7 AZ limit
   - infrastructure isolation
     its own network & power.

3. Partition placement group
   Same structure like spread placement group
   with as much as you can instances per
   need. no 7 instance per AZ limit.

- Lambda
  - function As a service
- Billed for amount of time function run only.
- Lambda function is stateless means everytime lambda function runs it runs a brand new enviornment.
- You can directly control the amount of memory allocated to lambda function.
- 15m - 900sec running time.
- step function to run large function.
- Lambda function does not have acess to VPC bosed services unless public IPs are provided
- In case Lamba function running inside a VPC We can use gateway endpoint to give acess on the public internet.
- Treat lambda f? as any other VPC bosed resource to understand the functioning.
- logs → cloudwatch, cloudwatch logs & x-ray.
- x-ray → for distributed tracing.

  Lambda function can be invoked in three ways
  - —— synchronous
  - —— Asynchronous - mostly used for AWS services
  - —— Event source mapping - batch processing
- If Lambda function run first time it will take some time to initialize (cold start) but after that for executions which are done frequently don't need execution time.

- provisioned concurrency to keep code warm.
  ↓ can be used



VPC flow log

- Captures metadata (not content)
- Attached to a VPC - All ENI's in that VPC
- Subnet - all subnet in that subnet
- flow logs are not realtime

Egress-only Internet Gateway

-

State Machines

- different states such as start — states — end
- Max duration 1 year
- It is kind of alternative to Lambda to run functions which takes more than 15 min

They are same like Workflows also works for 1 years

Step Functions vs. SWF for AWS workloads

AREA	STEP FUNCTIONS	SIMPLE WORKFLOW SERVICE (SWF)
Infrastructure management and integrations	100% managed, 100% serverless. Tasks in Step Functions were originally just Lambda functions, but support has increased to include integrations with services such as AWS Batch, DynamoDB, Elastic Container Service, Fargate, Simple Notification Service, Simple Queue Service, Glue and SageMaker. Tasks also can integrate with any HTTPS endpoint, not only native services.	Workflow applications can run on EC2 instances, on-premises servers or other cloud providers' infrastructure. Users are responsible for infrastructure management; SWF only takes care of state management.
Tasks and conditions executions	Flow logic is defined in the Step Functions service. Tasks can be executed by integrated services, such as AWS Lambda functions.	Task execution (activity workers) and flow conditions (decider workers) are defined in the application code, not in SWF.
Graphic interface	Workflows can be defined with a GUI to simplify user experience.	Workflows can only be defined in the application code.
Infrastructure as code	Workflows can be defined with CloudFormation and AWS Serverless Application Model.	Only EC2 infrastructure can be defined in CloudFormation.
Portability	Any process with an HTTPS endpoint can be integrated into Step Functions, as long as it has inputs and outputs that can be fed into the workflow definition.	Application code has to be written to follow strict SWF requirements, typically with the Flow Framework.
Learning curve	Low. A user typically gets started with a few AWS resource launches—such as Lambda functions—and uses intuitive workflow concepts.	High. A user needs to understand multiple SWF concepts, and many application components need to be in place, such as Java interfaces, implementation classes, workflow starters, annotations and IDE setup.
Support for long-running tasks	Technically, users could run a task that takes up to a year to execute. If using Lambda functions, they'll be limited by Lambda's maximum timeout of 15 minutes.	Up to one year.
Throughput limits	▪ Maximum open executions: 1 million. ▪ Max workflow execution time: 1 year. ▪ Limited by AWS resource integrations such as Lambda concurrent executions and DynamoDB provisioned throughput. ▪ Max workflow retention: 90 days. ▪ Max history size: 25,000 events. ▪ Max pollers per task list: 1,000 per state machine. ▪ Execution rate limits can be increased by request.	▪ 100,000 open workflows per domain (100 domains max): 10 million open workflows. ▪ Max workflow execution time: 1 year. ▪ Max workflow retention: 90 days. ▪ Max history size: 25,000 events. ▪ Max pollers per task list: 1,000 per task list. ▪ Execution rate limits can also be increased by request.
Cost (U.S.-East-1, excluding free tier, compute costs, AWS integrations and data transfer)	Cost is defined by state transitions. $25 per 1 million state transitions. Example: Three-step workflow, 1 million executions: $100 (4 million state transitions).	$100 per 1 million workflow executions. $25 per 1 million tasks. Example: Three-step workflow, 1 million executions: $100 (workflow executions) + $75 (3 million tasks) = $175.

Try to use step functions for all of your new work

VPC peering.

→ VPC peering – lets you create a private network link **betn two VPC's** only *
max two VPC's only
same/cross region or same/cross Acc

- Connection **betn VPC peering is not transitive** → means if there is Connection betn A → B & B → C that doesn't mean there is connection betn A → C
- VPC IP's have to be unique to each other.

- Secret manager
  - password manager, API
  - Rotating secret
  ex. RDS

- parameter stores
  - Config.

AWS Config

- Record configuration changes over time on resources
  - To detect mis-configurations
  - for governance over your resource
  - If it detects an issue with your config it will flag that.
- Used for auditing changes, compliance with standards
  - Auditing & compliance.
  - Security analysis.
- Users can be notified when there is a change in configuration using SNS Notifications & near-real time event using EventBridge & Lambda.
- With AWS config rules we can check the services if it is compliant or not

—x—

- Amazon Macie

- Data security and Data privacy service
- Discover, Monitor and protect Data
- Automated discovery of Data i.e PII, PHI, finance.
- Regex Based.
- Macie has two types of findings policy finding's and sensetive data findings.

Amazon Inspector

- Vulnerabilities
- Security reports = Amz Inspector
- Reports of findings with priority
- scans EC2 instance and Instance OS.
- Network & Host assesment agent
- for network assesment no agent required
- same for network reachability.
- There is CVE - common vulnerabilities and exposure package.
- Center for Internet security Benchmarks
- Security Best practices for Amazon Inspector.

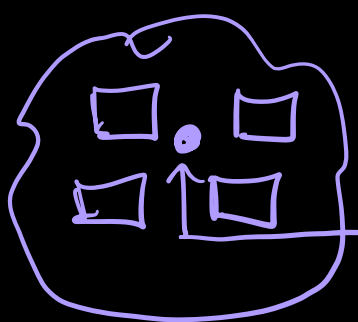
Amazon Guarduty

- Continuous Security monitoring Service.
- to detect any unexpected or unauthorized access to the service. and we can send the alert to Event bridge or Lambda function to perform remedies on the same.

Amazon Sagemaker

- fully managed Machine Learning (ML) service.
- fetch, clean, prepare, Train, Evaluate, Deploy
- Sagemaker studio - Build, train, debug & monitor
- Sagemaker Domain - partition of project
- Containers - Docker containers
- Sagemaker has no costing → only the services does

Aurora
- built-in Reader Endpoints



Cluster of DB instances connected together and intermediate handler is where is connection occurs.

- That's why load balancing is done automatically
-

[Oracle Real Application Cluster (RAC)
- Way of accessing database from multiple database servers.

Resource Manager (RAM) ↑ Acess
- Helps you to share resources among multiple AWS accounts.
- centrally govern access to resources.
- Least privilege on shared resources.

- Expidite retrival is used to retrieve data faster
  available within 15 min

- provisioned capacity ensures that when you need retrival capacity it is reserved for you.

— Amazon Redshift Spectrum

— Allows you to directly run SQL queries against exabytes of unstructured data in Amazon S3.

x-ray — Helps developers analyze and debug production, distributed Applications.

* can directly move data to Glacier or Glacier Deep Archive.

Amazon Datasync — It's for files and objects used with NFS & SMB file systems.
DMS is for database.

- migrate your on-premises data to Amazon S3 Amazon EFS and amazon fsx.
- Amazon storage gateway is more suitable if you still want to retain acess to the migrated data
- EBS does not support object lock.
- Amazon Datasync can directly move data from on-premises to S3 Deep archieve.

on-premise ⟶ Glacier / Deep Archieve

— Datasync agent is required for Data Sync.

* Amazon Redshift

- fast scalable data warehouse that makes it simple and cost effective to analyze all your data across your data warehouse and data lake.

- performance super-fast analytics on massive data set in near real time.

- To ensure the previous state of file is preserved and there is no changes to be done on that we allow "object versioning".

* Gateway endpoint

- Type of VPC endpoint that provides reliable connectivity to Amazon S3 & DynamoDB without requiring an internet gateway.

- It would take a lot of time to config Bucket policy for each S3 bucket

- Therefore you should use an endpoint policy to control the traffic to the

trusted Amazon S3 buckets.

Transit Gateway - is primarily used to connect VPC & on-premises networks through central hub.

* Guard duty

- checks for unauthorized access even on S
- security token service (STS) to temporarily provide login access.

- RDS proxy

- Helps you manage a large number of connections from lambda to an RDS database by establishing a warm connection pool to the database.

• EBS

— EBS volumes supports live configuration changes while in production which means that you can modify the volume type, volume size, and IOPS capacity without service interruptions.

— storage gateway is aka tape Gateway.

Decoupled Architecture can be created using Amazon Simple Queue Service and Amazon simple workflow service. (SWF)

* Whenever it says decoupled Architecture think of sqs

Nat Gateway for connection of VPC with public internet but preventing any inbound connection.

NAT Gateway is commonly used to provide internet access to EC2 instances in private subnets while preventing external services from initiating connections to the instances. This component is not necessary for the application to work. Take note that you cannot directly integrate the AWS Network Firewall with the Application Load Balancer. There is a straightforward way of integrating an AWS WAF with an ALB but not an AWS Network Firewall with an ALB.

- We cannot connect Network firewall directly with Application Load Balancer.
  Web Application Firewall WAF ♥ Application Load Balancer.

- Manage and update deployments * Accelerate Application Deployment.

AWS Proton allows you to deploy any serverless or container-based application with increased efficiency, consistency, and control. You can define infrastructure standards and effective continuous delivery pipelines for your organization. Proton breaks down the infrastructure into environment and service ("infrastructure as code" templates).

As a developer, you select a standardized service template that AWS Proton uses to create a service that deploys and manages your application in a service instance. An AWS Proton service is an instantiation of a service template, which normally includes several service instances and a pipeline.

- once instance is started, It is not possible to start the hibernation.

- origin access identity (OAI) - can be used to restrict access in the origin.
  Its used in cloudfront to restrict access of s3 only for cloudfront so anyone cannot directly access the Bucket.

- Reserved Instances has to be terminated or else put on marketplace for sell. once it's no longer need.

- If messages in the Appl'n is not being deleted then only they will be sent again to SQS queue.

Visibility time — the amount for which the msg will be visible for consumer to process it. If msg is sent twice, that means visibility timeout is too short and consumer is unable to process the msg and delete it afterwards.

* - you cannot set priority to individual messages in SQS queues.
  - Has to be two diff SQS for free & premium?

Yes.

You need two different queues for this purpose. Consume premium first then consume messages from free.

Guardrails - AWS organization.

- used for multi-account governance
  1. Mandatory
  2. strongly recommended
  3. Elective
- Account factory - allows automation of Accounts.
- Accounts can be closed or repurposed.

Bucket policy

* Resource policy vs identity policy.

They are inverse to what their name says

Resource policy - Who can acess the bucket
= identity
→ control over identity

identity policy - What can be access
= Resources
- control over resources.

To differentiate policies
- If policy has principal in it its a resource policy.

because in identity policy we already know the identity which is you.

— Bucket can have only one policy at a time. but that policy can have multiple statements.

* for anonymous users only identity policy apply or resource policy only apply on identity.

— At legacy S3 used to use ACL

- When it comes to allowing or denying lots of different resources on aws identity policy is used.
- When giving access to services when one user or Account involved used resource policy.

Never Use ACL or try to avoid using it if you are not certain.

- Elastic fabric Adapter (EFA's) are used for HPC (High p computing)
- Redshif is not Highly available it does need backups stored in other places.
- Cloudwatch alarms can trigger EC2 instance restart.
- Server Acess Logging provides logs of all users, Roles and services. It is more granular than cloudwatch.
  It also provides object-level logs.

- Security group denies inbound traffic and allows outbound traffic.
- NACL allows both incoming and outgoing traffic. to start deny default configuration must be edited.

- To use file Gateway this must be fullfilled
  - Configure Microsoft AD
  - Configure private networking VPN or AWS direct.

- parameter store is cheaper option than secret manager.
- Aurora is serverless
- AWS site-to-site VPN should have
  1.- Transit Gateway
  2.- Virtual private Gateway
  - Amazon DynamoDB Global Tables

  * — Transit Gateway for VPC & site-to-site VPN
  - Active Directory users acess to AWS without IAM users are
    - SAML 2.0
    - OPen ID connect
  - AWS X-ray (Analyze debug Application, Generate detailed Service Map. Audit your data securely.) for granular checking of API.
  - If we are using EC2 instance and encrypted EBS volume. In that case all the data in-transit betn EC2 & EBS volume is also encrypted along with data at rest.

- VPC endpoints are specific to one region only
They do not provide inter-domain conn

AWS Site-to-Site VPN this type of connection traverses the public Internet. Moreover, it doesn't provide a high bandwidth throughput and a more consistent network experience than Internet-based solutions.

Amazon Workspaces -
virtual desktops for everyone

Trusted Advisor - when it comes to providing guidance on provisioning resources

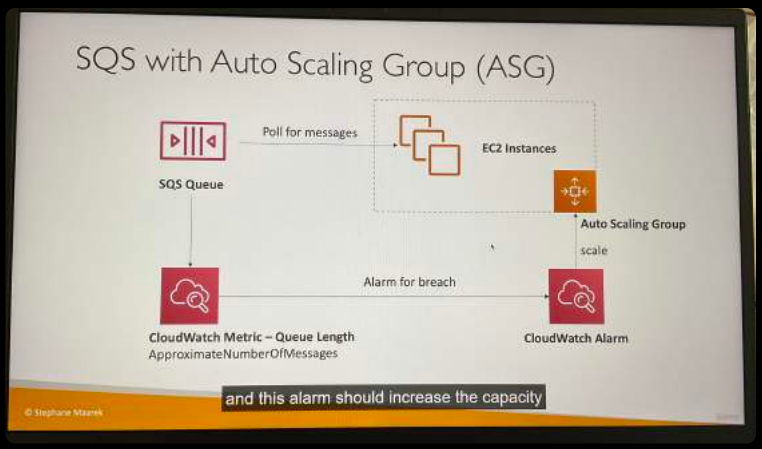
- cost optimization
- Performance
- Security
- fault tolerance
- service quotas

It inspects your AWS resources and makes recommendations on saving Money improving system performance and reliability or closing security gaps.

SQS

- default retention is 4days, max 14 days
- has to be small 256 kb per message
- can have duplicate message
- also out-of order messagin
- To improve the throughput of processing We can do Horizontal scaling

* To add sqs in auto scaling group we need some kind of Metric to monitor so that we can add auto scaling we use cloudwatch matric



- Visibility timeout - When a message is being consumed by one consumer that message will Not be visible to other consumers when they make request in that timeframe but if that message is not processed in that timeframe it will be visible again.
- If a message is not processed within the visibility timeout, it will be processed again and again until it's proceed or added to dead letter queue.
- Consumer can call ChangeMessageVisibility API to get more time

Long Polling in SQS

- Will decrease the no. of API calls made to SQS = Money Saving.
- If consumer requests (poll) and there is no message in the queue consumer can wait to reduce the no. of API calls.

Ways to optimize API calls?.

→ Long Polling

can be enabled at the queue level using

→ WaitTimeSeconds

Lambda

- By default its launched inside AWS VPC
- To launch Lambda inside a VPC it needs security group, VPCID and the subnets.
- Lambda will create ENI (Elastic Network Interface) to connect to VPC.

- Lambda with RDS proxy
- Lambda → (direct conn) → To RDS

may cause
- To many open connections under high load.

Benefits of using RDS proxy
1. Improve Scalability
2. Improve Availability
3. Improve security.

DynamoDB

- NOSQL Database
- Scale to massive Workload

Two modes
1. provisioned
   - you select read and write
   - possible to add auto scaling

② on demand —
- more expensive
- auto scale up/down with your workloads
- Great for unpredictable, steep sudden spikes

features of DynamoDB DAX

① DAX – DynamoDB Accelerator (DAX)
— In-memory cache for increasing read congestion.
— Microsecond latency for cached data.

DynamoDB streams
— 24 Hr retention period
— Limited # of consumers

Both are real-time

kinesis data streams
— 1year retention
— High # of consumers

DynamoDB Global Table
— To make it accessible at multiple region at low Latency.

Redshift

- Mostly used for data Warehousing
  It is based on PostgreSQL but not used for OLTP.
- Redshift has No-Multi AZ mode.
- Redshift can be configured to copy snapshots to another AWS Region.

• Transit Gateway

- Better soln than VPC peering - Which allows single one connection to be used to connecting multiple VPC's together. reduces network complexity.
- Also connects VPC connection & customer Gateway
- ★ IP Multicast is only supported by Transit Gateway No other service.
- To increase Bandwidth Transit Gateways are helpful.

- Traffic mirroring

- allows you to capture and inspect network traffic in your VPC.

- Egress only Internet Gateway

- used for IPV6 only
- only outbound connection from IPV6
- Must update the route table.

- If we are using different engines to transfer data then we can use SCT - schema conversion tool.

RDS MySQL to Aurora MySQL

① Taking snapshot But there is downtime

② create aurora Read Replicas & once both in sync then Secondary promote to main.

for external

- xtraBackup or Percona Utility

* DMS if both database are up and Running

NACL = Explicitly Deny

Security Group = Explicitly allow

not good when we want to allow

traffic from multiple resources.

- Datasync needs Datasync agent to transfer the data. or move the data.
  - ENA - Enhanced Networking Adapter for higher Bandwidth, Higher PPS.

  - Elastic fabric Adapter -
    - Improved ENA for HPC, only works for Linux
    - Best for tightly coupled workloads.

fastest iops

EBS = scales upto 256k

instant store scales upto millions of IOPS

file system dedicated for HPC = fsx for Lustre

- AWS Parallel cluster
  - Open Source cluster management tool to deploy HPC on AWS.

- AWS GRAFANA - Visualization of time-series data such as system metrics (CPU load, disk storage, memory utilization, temperature, etc)

- AWS OpenSearch – interactive log analysis, real-time application monitoring, website search and more.
  Search and analytics tool.
  It also includes kibana.

  use cases
  - analyze the data

- IAM database authentication
  With this you don't need to use pass. you authenticate using Auth token.
  With Auth tokens-
  - Network traffic is encrypted using SSL
  - You can use IAM to centrally manage access to your database resources.
  - for EC2 you can use profile rather than credentials

- AWS Aurora replication provides replication latency of Below 1 second. Which is in some ms.

Cluster placement group

- Make sure to launch all of them at once.
- With same configuration (same instance type)

- If you try to add more EC2 instances type in the placement group.
- OR if you try to add more instances to the placement group later.

- AWS comprehend is for NLU that uses machine learning to find the insights and relationship in text.
- AWS lex enable you to build App'n using speech and text. chatbots can be build using lex.

- cloudformation – Resource Section is only required section in cloudformation.

* • Trusted Advisor – provides real-time guidence on provisioning your resources. only provides alerts where you are not using best practice and tells you ways to improve it.

NAT Gateway :– Allows your internal (VPC) EC2 instances to connect to internet but at the same time doesn't allow any outside connection.

- Egress-only internet Gateway – used for VPC that uses IPV6
- NAT Instances – Allows private subnet to connect to internet & prevent conn" from internet same like NAT Gateway.

* path conditions are used to define rules that forward requests to different target groups based on the URL in the request.

* When it says cost-efficient storage always check the minimum storage duration.
if its below 30 days use S3 standard

- EBS vs EFS Learn again

- Allow multiple concurrent connections from EC2 think of EFS.

- EBS - Block storage can only have one connection to EC2 instance at a time in some cases but you can multi-attach EBS to EC2 instances using cluster but there are limitations.
- EBS can be attached/detached from EC2 instances in the same AZ

* learn Redis from teatodojo

Security groups - Explicit allow and upto 5 Sec groups can be attached to one instance.

* DynamoDB When you want single digit ms response time.

* Redshift - Sub-sequent response time.

* kinesis firehouse destination → S3, Redshift Elastic Search 4HTTP endpoint.

* To check anything for ex. check the ACM(AWS certificate Manager) for expiry. Eventbridge can be run daily

* Efs

- Mostly used to mount and it uses (NFS) Network file system.
- Multiple connection at a time.
- Efs can only be mounted on linux.

cloudwatch -

- By default cloudwatch monitor events every 5 min.
-

Amazon Lustre

- When you need High-speed, High-capacity distributed storage.

RDS

- SQL Server
- Oracle
- Postgres
- MySQL
- Aurora
- MariaDB

— Elastic Cache two engines
  ① — memcached
  ② — Redis

Two serverless database in AWS
— ① Aurora
② DynamoDB.

- ELB doesn't have predefined IPV4 addresses, you resolve them using DNS Name.

cloudHub

- If you are given a scenario when multiple sites are connecting using VPN, consider cloudHub.

Practice - 4

cloudfront

To restrict the access of files we can use **signed cookies & signed URL**

1. **signed URL** – When access is restricted to individual file
   - When users are using client that doesn't support cookies.
2. Signed Cookies – Provide access to multiple restricted files
   - You don't want to change your current URL.

Use kinesis data stream rather than SQS when
① Data should not go missing
② No duplicates are produced

- **enhanced Monitoring metrics at RDS** gives information on following
  ① RDS child **processes**
  ② OS **process**

- Glacier used for data archieving only not for processing it

- Whenever you see RabitMQ think of Amazon MQ.

Neptune – ?

x-ray → ?

* Whenever you see a policy it can be distinguished using directory id.

* If we cannot use SAML 2.0 look for alternative STS or SSO ← But it has to explicitly mention SSO.

* Service controll policy is used to control Multiple AWS Accs.

* To get DNS hostname & DNS resolutions on newly created VPC you need to enable DNS.

* To process data at geoproximity to user at real-time use cloudfront with Lambda@Edge & process it using kinesis

* To check something for example access keys and delete it after 90 days use AWS config along with Lambda to deactivate and delete it.

* for better performance of the website we use
  - Cloudfront
  - Elasticache

* DynamoDB Stream - Easy to do automation & trigger the lambda function.

* flow logs are only used in VPC

* cloudwatch alarms can to stop, terminate, reboot or recover

* Personal Health Dashboard - Will show the status of your own services & Health Dashboard shows public events

* If you have SQS But you are getting an error where same message is appearing twice to completely avoid that use
  - ① SQS FIFO Queue
    OR
    ② Replace SQS Queues with Amazon Simple Work Flows

* only kms shows audit trail that shows when your CMK was used.

* Application Migration Service (MGN) is the primary migration service recommended for lift and shift migrations to AWS.

* Application Discovery service — Used to track the Migration status of your on-premises applications from migration Hub Console.

DataSync –

① Transfer To & from AWS
② Built in validation

Set 1

① Route table should always be configured inside an private subnets

② To scale out API → We need to Configure throttling limit

③ — cloudwatch metrics available and not available list

Types of endpoints in Aurora
- — cluster endpoints
- — Reader endpoints
- — Custom endpoints
- — Instance endpoint

① - cluster endpoint – (only one with write)
Connects your Application to current primary DB.
Only one that can perform write operations.

② Reader endpoint – (Used for Reading operations)
- provides support for load-balancing for read-only connections to the DB cluster.
- Used for read operation.

③ Custom endpoint (used to segregate traffic.) - Represents set of instance that you choose.
- It chooses one of the instance in the group to handle the connection.
- You define which instances this endpoint refers to, and you decide what purpose the endpoint serves.

④ — Instance endpoint – connects to Specific DB
- provides direct control over connections to the DB cluster.

AWS Transfer family

- AWS Transfer family allows
  - SFTP
  - FTPS
  - FTP

  } — either to EFS or S3

- Non Server Aurora DB is called as provisioned DB.
- Normal Aurora aka provisioned aurora works well when load is predictable as we have to manually provision the DB.

— check the Error codes again

- Data Lake - Centralized, curated and secured repository that stores all your data.

• • go through S3 encryption once from AC

- SSE-KMS to use when you got regulations under key control → because we can add policy to deny access to files using SSE-KMS.
- Everytime we create a EBS volume from scratch it creates new DEK (Data encryption key)
- EBS once encrypted there is no way to change that.
- AMI's are regional — so as KMS keys

- • Amazon ECS doesn't support resource based policy. also you cannot encrypt database infor using ACM.
- File gateway supports SMB protocol, NFS.
- tape gateway is cost effective way to store on-premise data to cloud but it takes time to retrieve information. also it does not maintain local cache like file gateway.
- Aurora Global database — provides RPO of 1 sec & RTO of 1 min
- To improve database performance of DynamoDB
  - → Use partition keys with high-cardinality attributes, which has large no. of distinct values for each item.
  - → Add more partition keys into DynamoDB to improve performance.

- RDS read replicas provide Asynchronous replication.
- With convertible Reserved instances you can exchange for

another convertible reserved instance of a different family.

- Unused standard reserved instances can be sold at the reserved instance Marketplace.

\# — 3 types of files storage
- EFS — Scalable, elastic
- fx for windows — for Windows

\# → - fx for Lustre — High performance can be integrated with S3
Machine learning ↑ High performance

- AWS Directory AD connectors — easy integration with identity federation and role based access control.

Amazon cloudwatch (CDN)
- CPU Utilization
- Disk performance / Disk reads & write
- Network

cloudwatch agent
- Memory util:
- Disk swap util:
- Disk space util:
- Page file util:
- log collection

- Amazon Neptune = graph database for superior scalability and availability

• Aurora can grow upto 64 TB
Handles OLTP complex queries and highly transactional.

Two VPC comm without using public net
① setup a peering connection
② Re-configure the route table's target and destination of the instance's subnet.

- VPC endpoints are region specific only and do not support inter-region communication.

Datasync	Storage gateway
• Migrate & move	• move data
• Better for move or migrate your data	• Replicating data
• On-premise data will not be used anymore	• create a cache copy on-premise for low latency.
	• on-premise data still can be used.

Two types of cloudtrail events
— ① Management
② Data

① management provides visibility into management operations that can also include non-API events
② Data events provides visibility into the resource oper^{n} performed on or within a resources.

SimpleDB vs DynamoDB
— SimpleDB has a limit on scalability.

Aurora in-case of failure
— ① Aurora replica →
— flip the CNAME record to point to healthy replica.

② Aurora Serverless
— Automatically recreate the DB instance in different AZ.

③ Aurora single instance —
— Will attempt to create a new DB instance in the same AZ as original instance.

— S3 by default provides
— 3500 request to add data/S
— 5500 request to retrieve data/S

— VPC endpoints to estiblish connection bet^{n} VPC & AWS services Without using internet gateway.

Two types of endpoints
① Gateway endpoint.
- no access from on-premise
- no access from another AWS region
Not Billed

② Interface endpoints
— Uses private IP from your VPC to access S3.
— Allow access from on-premise
— allow access from VPC in another region using VPC peering or AWS Transit Gateway.
— Billed.

- Each Load Balancer does a health check to ensure the target is healthy. After target is register it must pass the health check to be considered healthy.

- Transit Gateway - Connects your VPC and on-premises networks through a central hub.
  Simplify the Connection
  → (Acts as a highly scalable cloud router)

* System Manager run Command -
  lets you manage the configuration of your managed instances

* Load Balancer Ip changes everytime — so we should be using alias such as (A) record rather than IP.

* By default cloudtrail log file is encrypted

ENA	EFA
• Higher bandwidth, low latency, Higher packet per second performance, • for windows look for ENA	Same • provides os-bypass feature • os-bypass only supported to linux not windows

* parallel cluster - Tool to deploy and manage HPC cluster on AWS.

* Application Load Balancer have access logs which can be enabled.

object lock
- ① Legal hold - can be put & removed by user
  ② retention period - cannot be removed

* Database that can scale globally and handle frequent schema changes. aka NOSQL
  ↳ DynamoDB

RDS

- Data warehousing
  OLAP
- Well defined schema

DynamoDB

- Web-scale applin:
  social media, gaming,
  IOT
- schema-less
- More flexible

- EFS Lifecycle doesn't delete

* Amazon fraud detector doesn't check for any S3 data containing (PII) unlike amazon Macie.

* learn Eventbridge.

RDS

* Multi-AZ deployments

- - Synchronous replication
  - Highly durable
- Automated Backups are taken
- Always spans two az within single region.
- Automatic failover to standby when a problem is detected.

* Read Replicas

- asynchronous replication
  - highly scalable
- No autobackup config.
- can be within an AZ, cross AZ, cross-region.
- can be manually promoted to standalone db

* learn more on DynamoDB stream
ex. follow feature on social media done by DB stream.
- It has to be enabled first

- Redshift Spectrum
  - query and analyze all of your data in Amazon S3 using the open data formats you already use.

- AWS artifact
  - provides compliance report from AWS and ISV's
  - Download Report

- Inspector - Automated vulnerability management service. that continually scans AWS Workloads for software vulnerabilities.

- parameter store doesn't rotate the password.
  - secret manager rotates the passwords.

- SWf - Simple workflow Architecture can be used to create decoupled architecture along with SQS.
  - makes it easy to cordinate work across distributed appl^n components.

- step fun^n - also used for decoupled distribution of Appl^n

Step function	vs	SWF Simple workflow
- Newer and better • both used for decoupled Architecture • JSON		• If you need external signals deciders to intervene use SWf. • Decider programs.

- Gateway endpoint

  for traffic bet^n VPC and DynamoDB within AWS service use Gateway endpoints.

*you cannot directly integrate Network firewall with ALB.

privatelink - To privately connect your supported AWS services to VPC.
- can also be used when VPC connection is in peering bet^n other VPC.
  - makes it possible for customers to privately connect to a service even if that service's endpoint resides in different Amazon VPC.

AWS Glue is - Serverless crawler, data preperation, data transformation and data ingestion.

storage gateway

- Migration, storage tiering, Disaster Recovery
  - ↳ Replacement of Backup systems.
- ↳ Assist with disaster recovery.
  - ↳ great for full disk Backup.

File storage gateway

- mount points - NFS or SMB
- Map directly on S3 Bucket
- Allows lifecycle.
- primary data is held in S3.

Macie

- Monitor, Discover and protect data in S3.

automated discovery

- Inspector

EC2 — instance OS & containers.

- Common Vulnerabilities and exposure (CVE)
- center of internet security Benchmarks
- Security best practices for Amazon Inspector.