

# AWS Certified Solution Architect Practice Tests

classmate

Date \_\_\_\_\_

Page \_\_\_\_\_

- ① VPC has no inbound rules and all traffic is denied by default.  
Outbound rules allow traffic to all IP addresses.
- ② ELB feature called "Connection Draining" is used to ensure that connections close cleanly.  
"Deletion Protocol" is used to protect the ELB from draining.
- ③ TCP → Layer 4  
HTTP & HTTPS → Layer 7
- ④ EventBridge uses event-based architecture. You can set rules to configure other services to be triggered when an event reaches.

## ⑤ Hasil Block Storage

- Network drive. So expect some latency.

- Snapshot Possible  
↳ A-Z

### General Purpose SSD

- Cost Effective
- Low Latency

### Provisioned IOPS (PIOPS) SSD

- Critical business applications with sustained IOPS
- Great for database workloads  
(sensitive to storage perf and consistency)

## Hard Disk Drives

- Cannot be boot volume

### Throughput optimized HDD

### Throughput optimized HDD

## ⑥ IAM role vs User

IAM user is an entity that you create in AWS to represent the person or service that uses to interact with AWS.

IAM role is an AWS identity with permission policies that determine what identity can vs cannot do.

AWS Lake Formation has a feature to manage permissions using tags and grant cross-account permissions

EC2 instance metadata contains information including

- IAM role assigned
- Instance ID

RAID: Redundant Array of Inexpensive Independent Disks

- Does not improve performance
- Improves redundancy.

Amazon Auto Scaling policy for Dynamo DB is to provision capacity, in response to actual traffic patterns.

Dynamo DAX is used to improve read performance. It is expensive.

⑪ Internet gateway allows both inbound and outbound access to instances. GW allows instances with public IP address. NAT gateway only allows for outgoing access. Allows instances with no internet access.

⑫ IAM credentials report is tool for IAM security.

⑬ EC2 uses data  
→ Script that runs when EC2 is created.  
→ Runs as root user

⑭ Types of EC2 instances  
→ On Demand  
→ Reserved  
→ Convertible Reserved  
→ Savings  
→ Spot  
→ Dedicated Host  
→ Capacity Reservations  
→ Spot Fleets

⑮ NACL vs Security Groups

### (15) Network Access Control List (NACL) vs Security Groups (SG)

- Both allow controlling inbound & outbound traffic
- NACL ~~controls~~ access at VPC level subnet
- SG controls access at EC2 level.
- You can modify EC2 instance security group any time vs you need to disconnect NACL from subnet to do same
- SG → stateful (only allows rules)  
NACL → ~~not~~ stateless (allow & deny rules)
- SG: Control Ports / NACL: List IP address control

(16) EC2 instances Reserve can be done for 1 or 3 years.  
NOT in between

(17) EBS → single EC2 instance (except io1/iop2)  
EFS → multiple EC2 instances within a region

(18) VPC Flow Logs can track traffic going in/out of VPC / ELB  
You have to create network interface for your load balancers

Cloud Trail cannot be used as it only tracks audits API actions & does not support packet capturing.

19

## NACL VS WAF

↓  
Network Access

Control List

Web Application

Firewall

- Layer 4
- Stateless
- Block specific IP addresses
- Tied to VPC Subnets
- Layer 7
- Stateful
- Controls via HTTP headers & payloads
- Associated to specific AWS service

20

To encrypt data in transit for an RDS instance you can download AWS provided root certificates. Use the certificate when connecting to RDS DB instance.

21

When migrating from on-premises DB to RDS if

- changing the DB engine => use Schema Conversion Tool
- Not using => Don't do anything. Just migrate to use DMS.

21

You can use CloudFront with custom origin to point to on-premis.

(22)

## IAM Policy & Priorities

- o Explicit Deny
- o Explicit Allow
- o Default Deny (or Implicit Deny)

(23)

## Object storage refers to

- Data you want to store
- Expandable amount of data
- Unique identifiers for the data to retrieve

(24)

## Encryption can be done in 3 ways for server side

- S3 Managed Keys / SSE - S3 (server side encryption)
  - Amazon manages encryption and decryption for you automatically
  - You concede control to AWS
  - Ease of use
  - Unlike KMS, each object is encrypted using unique key
- AWS Key Management Service (AWS KMS)
  - Amazon and you both manage
- Server side encryption by customer provided keys.

(25) Once versioning is enabled, it cannot be disabled. Only suspended.

Cross Region Replication only works if versioning is enabled.

Deletes are not replicated.

(26) S3 Transfer Acceleration leverages Cloudfront CDNs.

called edge locations

You send data to custom CDN URL.

and that transfers to AWS S3

(27) S3 Event Notifications on

- SQS
- Lambda
- SNS

Must be indexed as well.

Search can be done via Elasticsearch

SQL like queries cannot be done via Elasticsearch

(28) S3 downloads can be parallelized

using byte-range-fetches

(29) S3 Select works on JSON, CSV, Parquet

JSON is not compatible with "Byte Range

Fetch" parameter which limits the

amount of data retrieved from S3

object

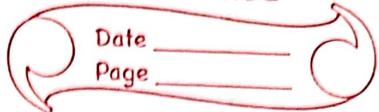
(30)

(31)

(32)

(33)

Storage gateway is block based storage  
and hence cannot be used  
over long distances



↑  
Not same as

- (30) Storage Gateway → Fx for windows gateway  
→ File Gateway: Operates via NFS or SMB  
used to store files in S3 over network  
filesystem to mount point in supplied  
Virtual Machine



→ Volume Gateway: Operates via  
iSCSI and used to store copies of  
hard disk or virtual drives.  
useful for block storage

→ Tape Gateway: Virtual Tape Library

Volume Gateway

- Stored Volumes → S3 used as backup  
→ Cached Volumes → S3 used as primary,  
On-prem caching layer

- (31) EC2 Termination protection is done using  
CloudFormation.

- (32) NLB are preferred over ALB because  
• Very low latency  
• Handle millions of requests per second  
• Block at Layer 4

③② DynamoDB vs SQL DBs (RedShift, RDS, ...)

③③ DynamoDB vs. SQS (RedShift, RDS, Aurora)

Choose DynamoDB because

- You are not sure of schema or it will change frequently
- Want Fast Reads. Normalized DB is slower because of joins
- SQL DBs have ACID compliance checks, making them slower.
- Dynamo leverages parallel processing to get data from SSD

③④ Dynamo Streams

• Control Flow of Info

Stream writes to

- Batch change DynamoDB writes to stream
- Lambda can be configured

Dynamo DB Global Tables

- Multi Region, Multi Masters Replication
- Requires enabling Dynamo Streams

### 35) Network Access Control List (NACL)

### Security Groups (SG)

- Control inbound & outbound for subnets
- Stateless (You have to allow) (Allowing inbound & outbound)
- Both sides must have allows outbound

- Default everything is denied / allowed
- Default everything is allowed.

- Has rule based priority
- NACL can be associated with multiple subnets
- Possible to block IP
- Similarities
  - Both control network access
  - Both are integral part of VPC

Security groups do not have a blacklist. They can only implicitly deny by excluding in allow list except through default.

(36) IAM Groups can only contain users  
not other groups

(37) IAM Security Tools

- IAM Credential Report
- List all account users and status of credentials
- IAM Access Advisor
  - Shows service permissions granted to a user and when those were last accessed

(38) EC2 Placement Groups

- Clusters: High communication b/w everything under same rack
- Spread: Spans across availability zones
- Partition: 100s of EC2 instances across many A-Z regions

(39) These are 4 types of services which improve networking capability in AWS

- Elastic IP Address
- Elastic Network Interface (ENI)
- Elastic Fabric Adapter (EFA)
- Elastic Network Adapters (ENA)

## Elastic IP address

- Creates static IPv4 address
- Can be associated with any instance in your VPC
- Avoid downtime by quickly remapping address

## Elastic Network Interface

- Beneficial to create sophisticated networking scenarios
- Design network topology within AWS cloud

## Elastic Fabric Adapter (EFA)

- Help accelerate High Performance Computing (HPC) and machine learning applications
- Helps bypass TCP/IP stack to provide low latency + high throughput in inter node communication
- (222) small memory

## Elastic Network Adapter (ENA)

- High Throughput + Low Latency for EC2
- Designed for modern DBs, distributed memory cache
- Supports 10GbPS of network bandwidth.

- ④ EBS Snapshots
- Not necessary to detach volume, but recommended
  - Snapshotting while in use can lead to possibility of capturing inconsistent data
  - I/O Performance
  - Avoid app/EC2 performance degrading
  - Speed of Snapshot

### • Features

- EBS Snapshot Archive
- Recycle bin for EBS Snapshots
  - Setup rules to recover deleted snapshots
- Fast Snapshot Restore

### ⑤ EBS Volume Types

#### • General Purpose (SSD)

• Burst IOPS 3000 (Small)

• Burst IOPS 16000 (Large)

IOPS  $\Rightarrow$  Input Output Per Second.

classmate

Date \_\_\_\_\_

Page \_\_\_\_\_

(41)

## EBS Volume Types

- Only gp2/gp3 and io2/io3 can be used as boot volumes.

Boot volume is where OS stores system files.

### General Purpose SSD

- Size 1GB - 16TB
- gp2
  - Small: IOPS: 3000
  - Storage & IOPS are linked
  - Max IOPS: 16000
  - You get 3IOPS per GB  $\Rightarrow$  Max out at 5334 GB

### Provisioned IOPS SSD

- Great for DB workloads
- Useful when IOPS  $> 16K$
- io1/io2
  - Storage 4GB - 16TB
  - Storage & IOPS
  - Nitro EC2 instance: 64000
  - Other EC2 instances: 32000
  - io2 have more durability
- io2 Block Express
  - Storage, 4GB - 64TB
  - Sub millisecond latency
  - Max PIOPS: 256,000

IOPS/GB : 1000:1

Supports  
Multi EBS  
Attach

## • Hard Disk Drives (HDD)

- Storage: 125GB to 16TB
- Throughput Optimized HDD (ST1)
- Max Throughput 500 MB/s
- Max IOPS: 500

## ④ EFS (Elastic File System)

- Uses NFSv4.1 protocol
- No capacity planning
- Mount 100s of instances
- More expensive than EBS
- Performance Mode
  - General Purpose
  - Max I/O 500 MB/s
- Throughput Mode
  - Bursting
  - Provisioned
  - Elastic: Auto-scale based on needs

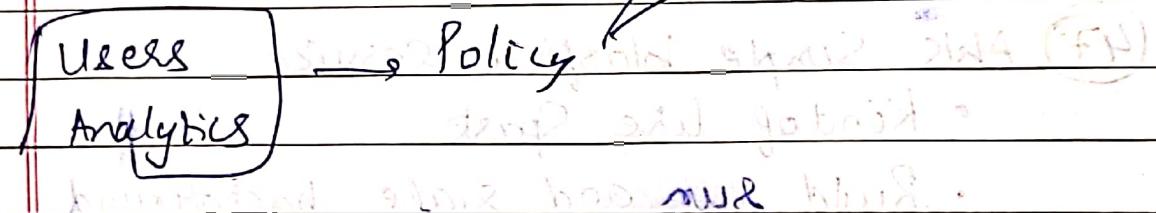
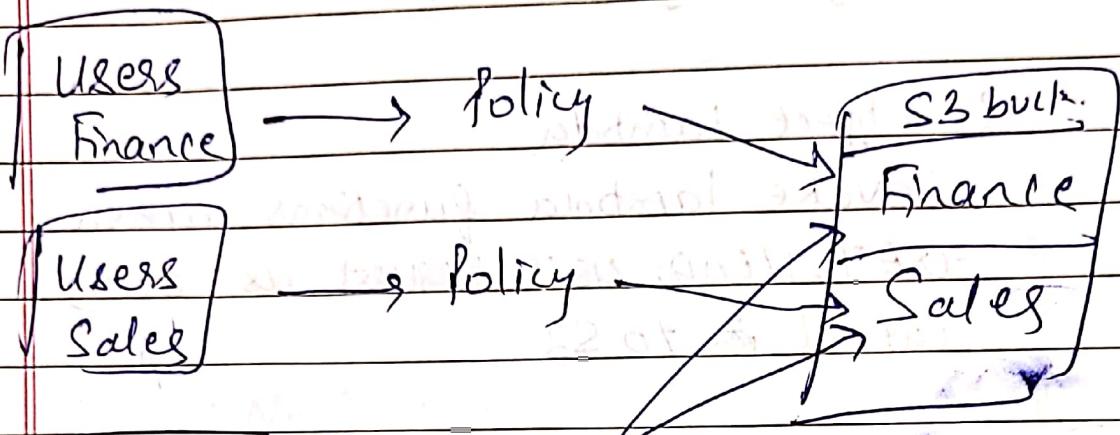
## Storage Tiers

- Standard
- Infrequent Access

43

S3 Access Points are useful when

- You have large numbers of users requesting access to specific S3 bucket data
- S3 bucket contain lot of data



44

RAID 0 vs RAID 12 vs RAID 5

→ Redundancy & Performance

→ Striping with personal S3 → Mirroring

Focuses on performance

Focuses on resiliency

If one drive fails → Data on 1 drive  
all the data is lost → means it  
lost

can still be recovered

45

S3 Object Lock prevents deletion during a customer-defined retention period.

S3 PutObject Legal Hold: Avoids deletion of objects until legal hold is removed.

- (46) S3 Event Notifications
- Receive notification when certain events happen in S3 bucket
  - Supports with SQS, SNS, Lambda
  - Fully Managed

### S3 Object Lambda

- Invoke lambda functions when GET, HEAD, LIST request us being called to S3

(47) AWS Simple Workflow Service

- Kind of like Spark
- Build run and scale background jobs at scale
- Suitable for process automation

(48) To monitor EC2 memory/disk space, you must use CloudWatch agent which collects the desired metrics

(49) AWS Storage Gateway is useful when you want on-premise system to access S3/EBS/EFS data seamlessly

- Provide storage

AWS DataSync is useful when you want to migrate large amounts of data and use AWS as a backup

- Provide fast and managed data sync

- transfer in block level (Amazon EBS)

(50) AWS Sagemaker is for building, training and deploying ML Models at scale using notebooks, debuggers, profilers, pipelines etc.

(51) AWS License Manager is useful to manage software license for vendors centrally across AWS and on premise environments.

(52) To improve recovery time of an EC2 instance

RAID0 → No Resiliency

RAID 1 → Resiliency present  $\rightarrow$  Fastest

Cloudwatch triggers  $\rightarrow$  Slow & More Resilient to removes EC2

(53) Snowcone → Edge Computing + Data Migration  
 $\rightarrow$  8TB HDD or 14TB SSD

Snowball → Edge Computing + Data Migration

Edge  $\rightarrow$  80TB

Snowmobile  $\rightarrow$   $> 10PB$

$\rightarrow$  Via Truck

(54) Start/Stop DB instance vs Snapshot Restore



- Charge for start/stop
- Charge for snapshots
- Charge for automated backups
- Charge for provisioned



- Charge for start
- Charge for snapshot

More costly

(55) You cannot use Auto Scaling groups with RDS instance

(56) KMS is used for creating & managing encryption keys. You cannot store credentials in KMS

(57) Elastic Search cannot query on S3. It cannot run SQL like statements or perform joins.

### Amazon Athena

- can do complex joins on S3 data
- supports SQL like format

(58) CloudFront Functions

- lightweight functions in Javascript for high scale latency sensitive CDN customizations
- cheap
- useful for URL rewrites
- Headers manipulation

### Lambda@Edge

- specialized functions is possible
- higher latency
- higher costs

(59) AWS Direct Connect takes several weeks to implement as on-premise to closest edge location line has to be setup

## (60) S3 PUT headers

x-amz-server-side-encryption : Controls server side encryption of the object at rest

x-amz-acl : Controls who can access the object. "private" ensures only object owner has access

Secure Transport: True → Makes HTTPS mandatory

(61) AWS Global Accelerator uses static IP address as fixed entry points for your application

You can migrate 2 /24 IPv4 address ranges for Global Accelerator to point to.

## (62) AWS Dynamo

- Proprietary to AWS
- DAX for very high reads
- Fully Managed
- Highly Available

Provisioned vs Auto Scaling

VS On-Demand

Global Table Feature: Active Active Setup

Has T7L feature

Dynamo DB Streams

## AWS DocumentDB

- Built on top with MongoDB. Fully compatible

- Fully Management
- Highly Available

63 Amazon Po

## 63 AWS ML Services

- Polly (Text to Speech)
  - Converts text to speech to build speech enabled products
  - Use SSML to customize
- Transcribe (Speech to text)
  - Automate speech to text quickly
  - Automatically remove PII data
- SageMaker
  - Fully managed platform to train, deploy ML models

## 64 AWS ML Services

- Textract (Extract text and data)

Read documents to extract text,  
handwriting etc.,

## 65 AWS ML Services

- Kendra (Find Accurate Info Faster)

Search info in different content  
repositories and documents

## 66 AWS ML Services

- Personalize

Build Real time personalized  
recommendations

## 67 AWS ML Services

- Forecast

Delivers highly managed forecasts

- Rekognition (Image and Video Analysis)
  - Identify objects, people, text, scenes, activities
  - Detect inappropriate content

- Lex (Conversational AI) + Connect
  - Chatbots
    - Receive calls, contact flows

- Comprehend (NLP)
  - Find insights and relationships in text
  - Fully managed

### • Translate (NLP Translation)

54 AWS ~~Rheosie~~

• Data Streams

• Data Analytics

• Data Firehouse

• Video Streams

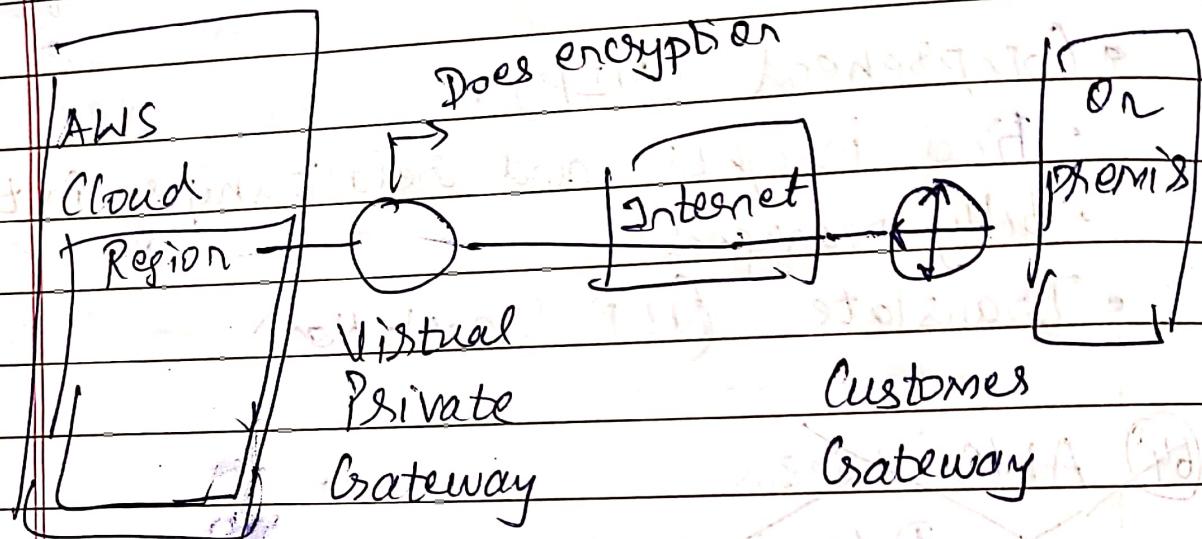
64 Important AWS Services General Info

• AWS ~~Pivot~~ Connect

## (63) Network to Amazon VPC Options

### (64) Amazon VPC Connectivity Options

- (a) AWS Site-to-Site VPN (Virtual Private Network)
  - IPSec VPN b/w remote network and Amazon VPC over Internet



- Automated Resiliency and failovers built in

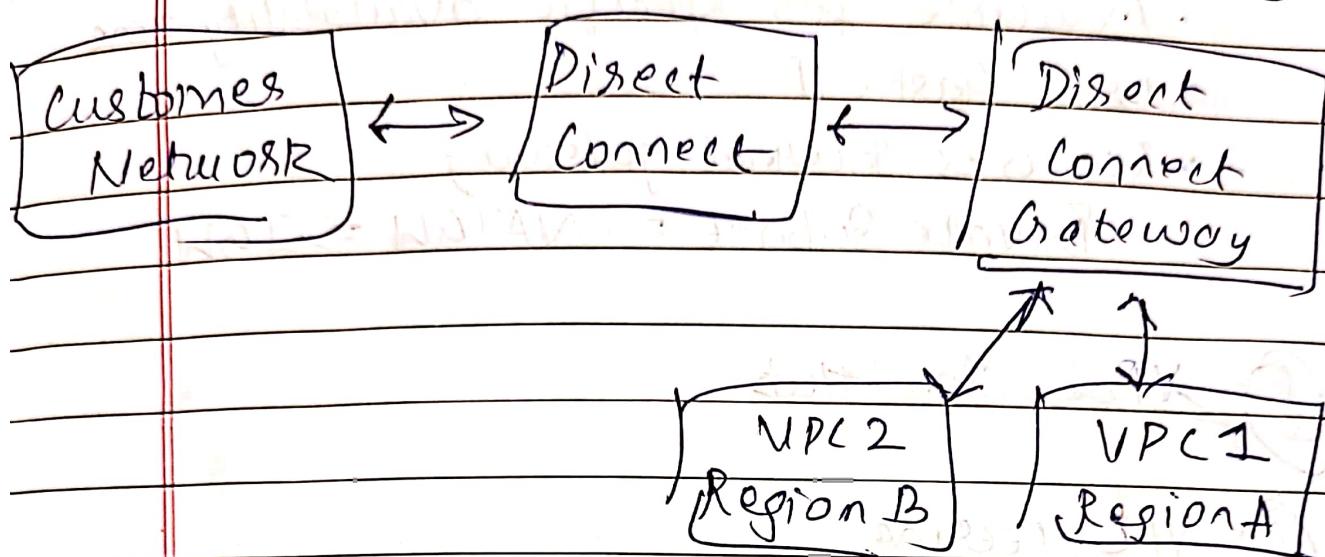
Using multiple customer gateway leads to resiliency and failovers on your side of VPN.

### (b) Direct Connect

- Establish direct private connection with on-premise network
- Physical setup is required which takes 1 or more month
- Data in transit is not encrypted but private

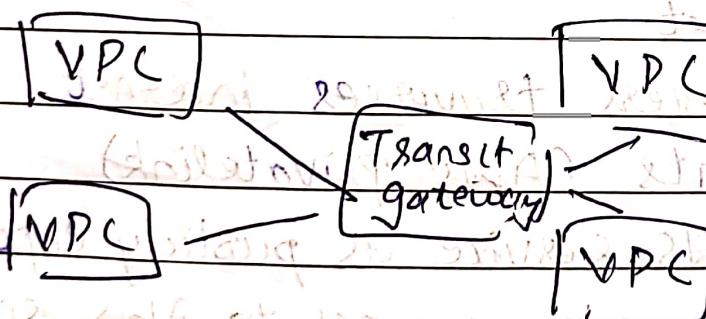
Solves that

If you want to setup direct connect to one or more VPC in different regions, use Direct Connect Gateway



### c) Transit Gateway

- Peering between thousands of VPC
- Uses hub-and-spoke model.



- You can make it cross region
- Route tables can limit VPC interaction.

### d) Internet Gateway (IGW)

- Allows communication b/w VPC and Internet
- Route table must also be edited
- Allows both inbound and outbound access to Internet

Capable to handle way  
more traffic compared  
to NAT instance

classmate

Date \_\_\_\_\_  
Page \_\_\_\_\_

### ⑤ NAT Gateway

- only allows for outbound access
- Allows instances with no public internet
- Available for specific availability zone
- Uses elastic IP
- Requires Internet gateway  
Private Subnet  $\Rightarrow$  NATGW  $\Rightarrow$  IGW

### ⑥ VPC CloudHubs

### ⑦ VPC Peering

- Privately connect two VPCs
- NOT transitive in nature
- CIDR should not overlap
- Supports inter-region peering
- Must update route table in each VPC subnet
- Traffic never traverses internet

### ⑧ VPC Endpoints (AWS PrivateLink)

- Every AWS service is publicly exposed
- Allows you to connect to AWS service using private network (otherwise via internet)
- Redundancy and horizontally scalable

#### Interface Endpoints

Provisions ENI as entry point

• \$per hour + \$per GB

• Must attach security groups

#### Gateway Endpoints

- Used as a target in route table
- Supports S3 & DynamoDB
- Free provision

## (h) Cloud WAN

- Provides configuration management for operating large networks
- Allows you to centrally manage and visualize cloud WAN core network and Transit Gateway

## (i) VPC Flow Logs

- Track packets (and corresponding metadata) going in and out
- Monitoring packets ~~for data misuse~~  
Packet Sniffer ~~monitoring~~
- Data can store in S3, CloudWatch & Kinesis Data Firehose

(65)

## API Gateway (lives in a region)

- Supports web sockets
- Handles versioning, authentication, validation, caching, Request throttling
- Integrations
- Lambda Function
- HTTP via signatures

## Edge Endpoint Types

- Edge Optimized

Requests are routed through Cloudfront

- Regional

- Private

Access from your VPC only

Use resource policy to define access

## User Authentication

- IAM roles
- Cognito
- Custom Authorizes (your own logic)
- Perform canary release deployment

Integration with AWS Certificate Manager

### 66 Amazon Cognito

Give users identity for web/mobile apps.

#### • Cognito User Pools (CUP)

- Serverless database to manage users,
- Provides password reset, email & phone verification, MFA.
- Integrates with API gateway & ALB

#### • Cognito Identity Pools (Federated)

Federated Identity: Users who can't sign in using well known (External Identity Providers) such as Facebook, Google etc.

You receive authentication token, and temp credentials in return.

The credentials are mapped to IAM role with permissions.

Default IAM roles for authenticated and unauthenticated users.

## (67) AWS Step Functions

- Serverless visual workflows
- Features: Error Handling, Sequence, Parallel, conditions
- Integrates with EC2, ECS, On-premise

## (68) Disaster Recovery & Migrations

### Types of Disaster Recovery

• On-premise  $\Rightarrow$  On-premise

• On-premise  $\Rightarrow$  AWS Cloud

• AWS Cloud  $\Rightarrow$  AWS Cloud

Region A

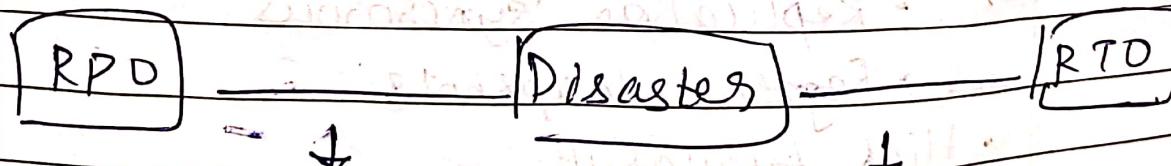
Region B

### Recovery Time Objective

• Time between disaster and last backup  
i.e. the data loss容忍時間

### Recovery Time Objective

• Time between disaster and recovery



= 1

Disaster

= 1

Downtime

## Recovery Strategies

- Backup & Restore (High RPO, High RTO)
- Pilot Light (High RPO, Medium RTO)
  - Small version containing critical capabilities always running (High RPO, Medium RTO)
- Warm Standby (Medium RPO, Medium RTO)
  - Full system running at minimum size
  - Replication ongoing
- Multi-Site / Hot-Site Approach (Medium/Low RPO, Low RPO)
- All AWS Multi Region

## How to perform good disaster recovery

- Backups
  - Replication Synchronous
  - Regular Snapshots
- High Availability
  - Automatic Route 53 Failover
  - Direct Connect for site to AWS Recovery
- Replication
- Automation
  - Lambda Functions
  - CloudFormation / Elastic Beanstalk
  - Recover via CloudWatch Alarm

## Database Migration Service (DMS)

- On-premise to AWS Database migration
- Continuous Data Replication (CDC)
- Must create EC2 instance for replication
  - prefers compute intensive
- Use Schema Conversion Tool (SCT) when DB engine is changing

Multi-AZ enabled by DMS maintains a stand-by replica

- Provides data redundancy
- Eliminates I/O freezes
- Minimizes latency spikes

## RDS & Aurora MySQL Migrations

- RDS MySQL to Aurora MySQL

Option 1) DB Snapshot from RDS

Restore to Aurora

Option 2) Create Aurora read replica

Set replication lag to 0

Promote as its own DB cluster

- External MySQL to Aurora MySQL

Option 1) Percona Xtra Backup to S3

Create Aurora DB from backup

Option 2) Create Aurora DB

Use mysqldump utility to migrate / sync

## RDS & Aurora PostgreSQL Migrations

- RDS PostgreSQL to Aurora PostgreSQL

- option 1) • Take snapshot of DB

- Restore to Aurora

- option 2) • Create Aurora Read Replica

Set Replication lag to 0

Promote as your own cluster

- External PostgreSQL to Aurora PostgreSQL

- Create backup and put to S3

- Import using aur-s3 Aurora extension

## On Premises Strategy with AWS

- Ability to download Amazon Linux 2 AMI

- VM Import/Export

- Migrate to EC2

- AWS Application Discovery Service

- AWS Database Migration Service

- AWS Server Migration Service

## AWS Backup

- Fully Managed Service

- Supports Cross Region Backups

- Supports Cross Account Backups

- Supported Services

EC2 / EBS • RDS / Aurora / Dynamo DB

S3 • DocumentDB / Neptune

FSX / EFS • Storage / Volume Gateway

- Supports Point in Time Recovery  
→ similar to time travel in Snowflake
- On Demand vs Schedule Backups
- Tag Based Backups
- Backup Plans based on
  - Frequency
  - Window
  - Transition to cold storage
  - Retention Period

### Backup Vault Lock

- Similar to S3 Object Lock
- Even root user cannot delete backups

### AWS Application Discovery Service

- Plan migration projects by gathering information about on-premises data centers
- Server utilization data and dependency mapping is important

### Agentless Discovery (Agentless Discovery)

- VM Inventory, Performance history like
- Configuration of CPU, Memory, Disk Usage

### Agent Based Discovery (AWS Application)

- System Configuration
- System Performance
- Running processes
- Details of network connection b/w systems

## Application Migration Service

- Lift & shift solution
- Converts servers to run natively on AWS
- Minimal downtime
- Reduced costs

## 69) AWS Monitoring, Audit & Performance

### Cloudwatch

- Provides metric for all AWS services
- Can create dashboards out of metrics
- Can create custom metrics
- Stream them to Kinesis Data Firehouse

or 3rd party tools like New Relic, Splunk

- Can filter metrics

Log groups: Name representing application/service

Log stream: Instances with application

Can define log expiration policy

Can send logs to

- S3

• Kinesis Data Streams

• Kinesis Data Firehouse

• AWS Lambda

• OpenSearch

- Can triggers Cloudwatch alarms
- Cloudwatch logs can take up 12 hours to be available for export.
- Cloudwatch Log Subscribers can make it near-real-time
- Kinesis can take logs from multiple accounts / regions
- You can safely send Cloudwatch logs
  - Run Cloudwatch agent on EC2
  - Make sure IAM policies are correct
    - Cloudwatch log agent can be setup on-premises
- To send Cloudwatch logs

### Cloudwatch unified agent metrics

- CPU
- ORAM
- Disk Metrics
- Netstat (No. of TCP, UDP connections, net packets, bytes)
- Processes
- Swap Space

### Cloudwatch Alarms

- Used to notify on event
- Triggers AutoScaling via SNS notification
- Composite alarms to avoid "alarm noise" by using AND/OR conditions
- EC2 instance recovery is possible via Cloudwatch alarm

Event Bus: Acts as broker to manage which event services receive

classmate

Date \_\_\_\_\_

Page \_\_\_\_\_

## Amazon Eventbridge (a.k.a Cloudwatch Events)

- Schedule : cron jobs
- event pattern : Rules based to trigger SNS/Lambda/SQS



works with variety of services Origin

- EC2
- Codebuild
- CloudTrail
- S3
- Trusted Advisor

Advisors

works with variety of destinations

- Compute : Lambda, AWS Batch, ECS Task
- Integration: SQS, SNS, Kinesis Data Stream
- Orchestration: Step Functions, CodePipeline, Code Build

Maintainence : SSM , EC2 Actions

- Archiving events is possible
- Replay events is possible

Event bridge supports schema inference

Schema Registry allows you to generate code for application, that knows in advance structure of event bus

## Cloud Watch Container Insights

- Collect & analyze logs from containers
- Supported on ECS, EKS, Kubernetes platforms on EC2, Fargate

## Cloudwatch Lambda Insights

- Monitoring for serverless apps on Lambda
- Also collects info on cold start and lambda workers shutdown

## Cloudwatch Contributors Insights

- See top N contributors
- Total unique contributors
- Useful for identifying bad hosts
- Identifying heaviest network users

## Cloudwatch App Insights

- Automated Dashboards
- Powered by Sagemaker
- Enhanced visibility to reduce time it takes to troubleshoot and repair apps.
- Alerts sent to Event Bridge & SSM Ops Center

## Cloudwatch Insights and Operational Visibility

- Container Insights

CloudTrail integrates with EventBridge to intercept API call

classmate

Date \_\_\_\_\_

Page \_\_\_\_\_

## AWS CloudTrail

- Provides governance, compliance and audit
- Enabled by default
- Can export to CloudWatch or S3
- A trail can be applied to all regions (default) or single region
- If resource is deleted, investigate cloudtrail first
- Retention for 90 days

### CloudTrail Events

#### → Management Events

- Operations performed on resources in your account

Can be

separated

- Read Events: List S3 buckets
- List EC2 instances
- Write Events: Terminate EC2 resource

#### → Data Events

- Not logged by default (as they are high volume)
  - e.g. Lambda execution time

### CloudTrail Insights

- Detect unusual activity
  - inaccurate resource provisioning
  - hitting service limits
  - Burst of API IAM actions

## AWS Config

- Helps with auditing and compliance
- Helps record configurations over time
- You receive alerts for changes
- AWS Config cannot prevent actions from happening
- AWS Config uses per region service
- AWS Managed Rules or set your own rules using AWS Lambda

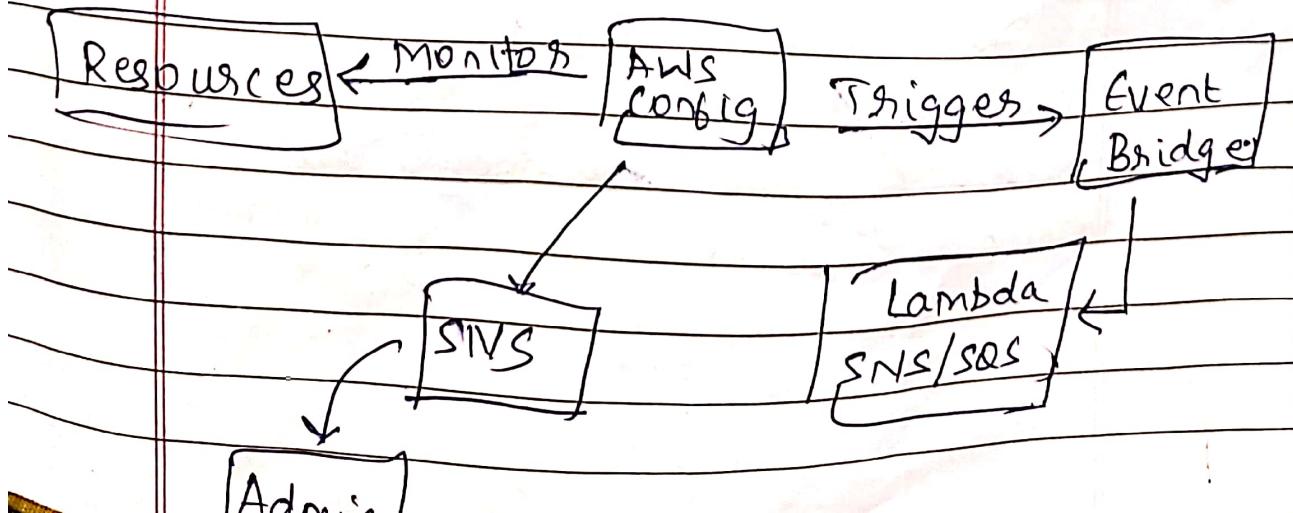
## Resource

- View compliance over time
- View configuration over time
- View CloudTrail over time

## Remediations

- Automatic Remediations via SSM Automation Documents
- Can set Remediation Retries

## Notifications



(70)

## CloudWatch vs CloudTrail vs Config

### Cloudwatch

- Performance monitoring
- Dashboards
- Events & Alerts
- Log Aggregation and Analysis

### CloudTrail

- Record API call
- Can define trail for specific resources
- Global Service

### Config

- Record configuration changes
- Evaluate resources against compliance rules
- Give timeline of changes and compliance

## (7) AWS Security and Encryption

- Encryption in flight (SSL)
  - Encrypted before sending
  - Decrypted after receiving
  - Avoids Man in the Middle Attack (MITM)
- Server side encryption at rest
  - Encrypted after received by server
  - Decrypted before being sent
- Client side encryption
  - Encrypted by client, never decrypted by server
  - Decryption also handled by client

## AWS Key Managed Service

- AWS manages the keys
- Integrated with IAM
- Audit key usage with CloudTrail

## Key Types

- Symmetric (AES-256 keys)
  - Single key for encryption and decryption
  - AWS services integrated with KMS
- User symmetric CMKs
  - You never get access to KMS unencrypted (must use KMS API)

- Asymmetric (RSA & ECC key pairs)
- Public & private keys
  - Public: Encryption
  - Private: Decryption
- Useful when you want to encrypt outside of AWS

### Types of KMS Keys

- AWS Owned: SSE-S3, SSE-SQS, ...
- AWS Managed: aws/rds

### Automatic Key Rotation

- Automatic Rotation of 1 year
- Customer managed KMS key : 1 year
- Imported Keys: Perform manual rotation

### You can create custom KMS policies

- define users, roles, that can access KMS key
- define who can administer the key
- Useful for cross account access to your key

Access controls are very similar to S3 bucket policies.

## KMS Multi Region Keys

- Same key can be replicated to multiple regions.
- Allows encryption in one region and decryption in another
- No need of cross region API calls
- Each Multi-region key is managed independently

KMS Multi Region Key is useful for multi-region / global databases like

Dynamo DB - Global Tables

Amazon Aurora - Global db.

Each replica will decrypt from their own region KMS.

## S3 Replication - Encryption Considerations

- Unencrypted objects, objects encrypted with SSE-S3 ~~and SSE-KMS~~ are replicated
- Encryption using SSE-KMS one should enable ~~the~~ KMS Keys, Target Bucket
  - Attach IAM Key Policy to target
- Note: Although you can use AWS KMS keys, they are treated as independent keys by Amazon S3, (object will be decrypted and then encrypted again)

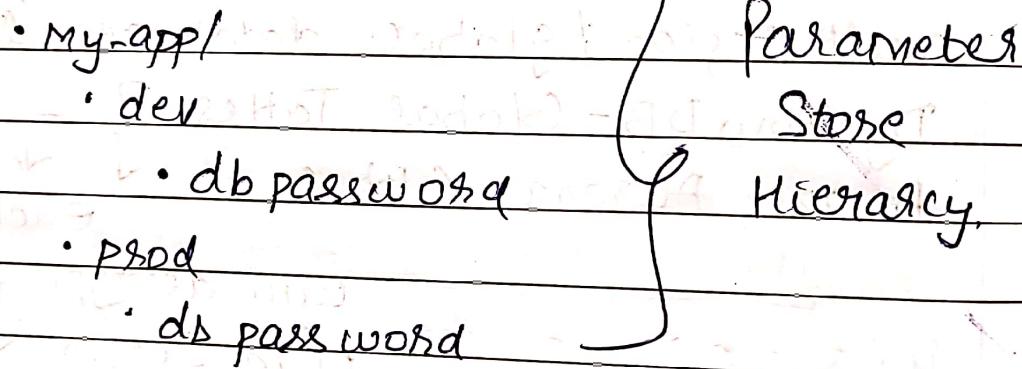
## AWS erasing policies

AWS erasing process encryptable via KMS

## SSM Parameter Store

- Secure place to store secrets and config
- You can encrypt using KMS
- Version tracking of configuration/secrets
- Integrated with IAM, Eventbridge, Cloudformation

/mydepartment



Parameters types: ① Standard ② Advanced

### (Advanced) parameter policies

- Allow TTL to parameters
- Can assign multiple policies at a time

AWS Config can check for certificate expiry.

CLASSMATE

Date \_\_\_\_\_

Page \_\_\_\_\_

## AWS Secrets Manager

- Newer service, meant for storing secrets
- Additional features (compared to Parameters Store)

### • Feature rotation of secrets

- Automate generation of secrets & via Lambda
- Integrate with RDS
- Secrets are encrypted using KMS
- Multi Region Secrets
  - Automatic sync with replicas
  - Ability to promote replica as master
  - Useful in multi-region setup
  - Disaster Recovery Strategy

## AWS Certificate Manager

- Deploy and manage TLS certificates
- TLS certificates are used for in-flight encryption. That is what HTTPS means.
- Supports public & private TLS
- Automatic TLS certificate renewal
- Integrates with ELB, CloudFront, API Gateway. NOT with EC2

Requesting certificate can include wildcards

- List domain names to be included

Select Validation : DNS or Email.

• DNS is automated.

• DNS will leverage CNAME to DNS config

• Takes a few hours to complete

## API Gateway Endpoint Types

- Edge Optimized
- Private
- Regional

## ACM Integration with API gateway

- Create custom domain names
- Edge Optimized (default)
  - Routed via CloudFront
  - API gateway still lives in one region
  - TLS cert. must be in same region as CloudFront
- Regional

## AWS Web Application Firewall (WAF)

Protects from common web exploits

- Only Layer 7 (HTTPS)
- Avoid Cross-site Scripting (XSS)
- Size constraints enforcement
- Geo-Match
- Avoid SQL injection
- Rate-based rules (count occurrences of events) to avoid DDoS

## Web ACL

Web ACL (Access Control List) is region and WAF integrates with AWS services:-

- Application Load Balancer
- API gateway
- CloudFront
- AppSync GraphQL API
- Cognito User Pool

Separate WAF for each.

## AWS Shield : Protect from DDoS attack

- Standard
  - Protect against more sophisticated attacks.
- Advanced
  - Protect against more sophisticated attacks.
  - 24/7 access to response team

## AWS Firewall Manager

- Manage rules across all accounts
- Security policies
- WAF rules which includes XNACL
  - AWS Shield Advanced
- Security groups for EC2
- Network Firewall
- Route 53

Rules are applied automatically when a new service is created.

## WAF vs Shield vs Firewall Manager

- They combined provided comprehensive solution
- WAF: More granular protection
- Shield provides more features on top of AWS WAF
- Shield Advanced specializes in DDoS attacks.

Guard duty, Macie and Inspector cannot be configured using AWS Firewall

classmate

Date \_\_\_\_\_  
Page \_\_\_\_\_

### Amazon Guard Duty

- Identify threats using ML algos
  - Cloud Trail Logs
  - Unusual API calls
  - Unauthorized deployments

#### Sources



#### VPC Flow Logs

- Unusual internal traffic

#### DNS Logs

- Compromised EC2 instances sending encoded data within DNS queries

#### Kubernetes Audit Logs

- Potential EKS cluster compromises

Can setup event bridge rules

### Amazon Inspector

- Automated security assessments
  - on EC2, Lambda, Container Images
  - Identify vulnerabilities
  - Code vulnerabilities
  - Network Reachability

AWS Macie

- Identify and protect your sensitive data in AWS using ML algos
- Can send notification to EventBridge

(72) When looking for a cost effective solution and usage is unknown

- Glacier → Expensive as reads cost \$
- S3 Intelligent → This has additional fee
- S3 Standard → ✓

(73) In order to setup CloudFront for S3, you also need to point CloudFront to S3 Images

(74) EBS Volume Types

- gp2/gp3 (SSD) : General Purpose
- io2/io3 (SSD) : Low Latency + High Throughput
- st1 (HDD) : Access Frequent data
- oot2 (HDD) : Very low cost  
Access Infrequent data

(75) Spot Instances are not ideal for development environment as they can be shut down randomly.  
Using on-demand capacity reservations makes more sense

(76) Quantum Ledger Database

Use when  
you read "immutable"

classmate

Date \_\_\_\_\_

Page \_\_\_\_\_

### 76) Amazon Quantum Ledger Database

- Book recording financial transactions
- Fully managed, high availability, replication across 3AZ
- Used to review all changes made to application data over time
- Central database

↳ Unlike Amazon Managed Blockchain

### 77) Amazon Aurora has read replicas by default. You do not need to enforce it.

### 78) Amazon FSx

- Provides fully managed third party file systems
- Provides 4 options
  - Windows File Server for Windows based application
  - Lustre for compute-intensive workloads
  - Netapp ONTAP
  - OpenZFS

#### a) Windows File Server

- Provides shared storage for windows
- Uses SSD storage, supports running Microsoft applications, supports SMB protocol

- You can also connect Linux based systems by installing cifs-utils

### Lustre (only with Linux)

- High performance computing
- Extremely high IOPS
- Can be accessed from on-premises systems

79) To make sure all traffic coming in to Cloudfront is inspected by AWS WAF



this is retrieving data from S3

- Attach WAF to Cloudfront
- Since distribution uses S3 as origin, we need to ensure request cannot hit S3 directly. This can be done by configuring an origin access identity (OAI). This is a special type of Cloudfront user. Only this user should have access to S3.

80) You cannot create a multi-region Aurora DB clusters. You should use Aurora global which provides RTO & RPO < 1 minute

Multi-master DB only work within a region and not cross region

(81) AWS Global Accelerators and Route 53 geoproximity based routing, both do reduce latency.

However Global Accelerator does it much better.

Global Accelerator directs traffic to closest edge location

↳ You can provide up to 2 IP addresses to link point to

(82) All AWS networking / VPC based solutions are highly redundant and hence they do not have single point of failure.

When AWS connects with on-premise over VPC, the only single point is customer gateway device.

(83) Fast Failovers and high availability are two different things.

(84) AWS KMS integrates with AWS EKS to make sure the configurations stored in ConfigMaps is encrypted.

Secret Manager can store db credentials but not encrypt EKS config.

## 85) Redis vs Memcached

	Redis	Memcached
Sub Millisecond	✓	✓
Latency	✓	✓
Developer ease of use	✓	✓
Data Partitioning	✓	✓
Support for multiple languages	✓	✓
Multi-threaded architecture	✗	✓
Advanced data structures	✗	✗
Snapshots	✓	✗
Replication	✓	✗
Transactions	✓	✗
Pub/Sub	✓	✗
Lua Scripting	✓	✗
Geospatial support	✓	✗

86) AWS registers upto 2 IPs. This allows for automatic failovers (similar to routes).

## 87) Section 30, Other Services

CloudFront  
Amazon Route 53  
Amazon S3  
Amazon Lambda  
Amazon VPC  
Amazon Kinesis

(87)

## Section 30: Other Services

### Cloudformation

- Declarative way to outline your AWS services

- Cloudformation creates services in right order and exact configuration

- Benefits

- Infrastructure as Code

- Infra changes through code review

- Cost

- Each resource gets a tag.

- Set savings strategy like deletion of services

- Productivity

- Ability to create/destroy infra on fly

- Automated generation of diagrams

for your template

- Useful when running multiple envs

- Infra as code

Repeat architecture in different region  
environment / account

- IAM role that allow cloudformation to create/modify/delete resources

- If you do not provide IAM role it uses your permissions.

## Simple Email Service (SES)

- Allows inbound / outbound emails
- Fully managed.
- Supports Domain Keys Identified Mail (DKIM) Sender Policy Framework (SPF)

## Amazon Pinpoint

- Marketing communication service
- Supports sending emails / SMS / in-app message
- Possibility to receive replies

Customer

SMS

Amazon  
Pinpoint

Kinesis SNS

CloudWatch  
Logs

## Versus SNS vs SES

- SNS / SES you manage audience content and delivery schedule

## ~~SSM Session Manager~~

- Start secure shell on EC2 / on-premise
- No SSH access, bastion hosts
- No port 22 needed

(88)

SSD backed volumes are useful when large transactions with small I/O size happens.

(89)

HDD volumes are useful when limited transactions with high MB/s requirement.

(90)

### AWS Glue

- Fully managed & serverless
- Focus on ETL and not worry about configuration and management of compute resources.
- Can automatically generate code to retrieve and store data from variety of AWS services
- Run on-demand or define or schedule trigger AWS Data Pipeline
- Provides high flexibility in terms of execution environment
- Launches compute resources in EC2 or EMR clusters.

## AWS EMR

- Cost Effective.
- You have to manage everything
- Utilizes hosted Hadoop framework

(91) Any database upgrade in RDS database instance with Multi-AZ deployment causes both primary and secondary databases to be upgraded at the same time.

A downtime is expected.

OS upgrade does not lead to downtime in Multi-AZ.

(92) If you have application in multiple AZ in private subnet, and want to create highly available NAT gateway.  
Create 1 NAT gateway for each availability zone

## Amazon RDS

• Multi AZ deployments ①

• Multi-Region deployments ②

• Read Replicas ③

①

②

③

• High availability, Disaster recovery, Scalability

• Recovery time objective

• Synchronous, Non-Asynchronous, Asynchronous  
Replication, bidirectional replication

94 You can use Route 53 to create privately hosted zones in your VPC  
 You must change VPC settings to true for enableDNSSupport and enableDNSHostnames

### 95 AWS Kinesis

- Data streams
- Data firehouse
- Data analytics in analytics category
- Video streams

Stands in

### 96 Data Streams

- Data Ingestion
- Provides temporary storage
- Multiple consumers consume at their own pace.
- Possible to rollback to specific time
- Useful when data is handled incorrectly from some other service

### 97 Data Analytics

- Analyze and transform data.
- Time window analysis joins.
- Wait till data comes fully also
- This does provide real-time analytics but does not provide long term storage

96

97

98

## Data Firehouse

- Data Ingestion
- Native integration with destinations like S3, Redshift
- Can have only one delivery destination
- Simple transformations is possible

## Data streams VS SQS

- Data streams does not work when sudden spikes come up. SQS can handle it.
- SQS does not have rollback option.

⑨6 Both S3 Managed Keys (SSE-S3) and KMS Keys (SSE-KMS)

can be used for S3 server side encryption.

However KMS would cost while S3 managed keys is free of use.

⑨7 Spot Instances : Can be shut down with 2 min notice

Spot Block Request EC2 spot instance for 1 to 6 hours, without interruption

Spot Fleet : Try to use spot if possible, else used on-demand.

⑨8 When performing data replication via EC2 instances, if ~~separate~~ the data has to transfer  $\rightarrow$  more costly.

(99) Elastic Load Balancing has a feature called "Access Logs". It allows you to capture info about requests sent to your load balancers. Contains time the request was received, client IP address, latencies, request path & server responses.

You can use to analyze traffic patterns.

### (100) AWS Batch

- Fully managed batch processing at scale. No need to manage instances
- Dynamically scale EC2
- Defined as docker images
- Compatible with many frameworks for Batch vs Lambda
- Time limit of 15 min in Lambda
- Batch is not serverless

### Amazon AppFlow

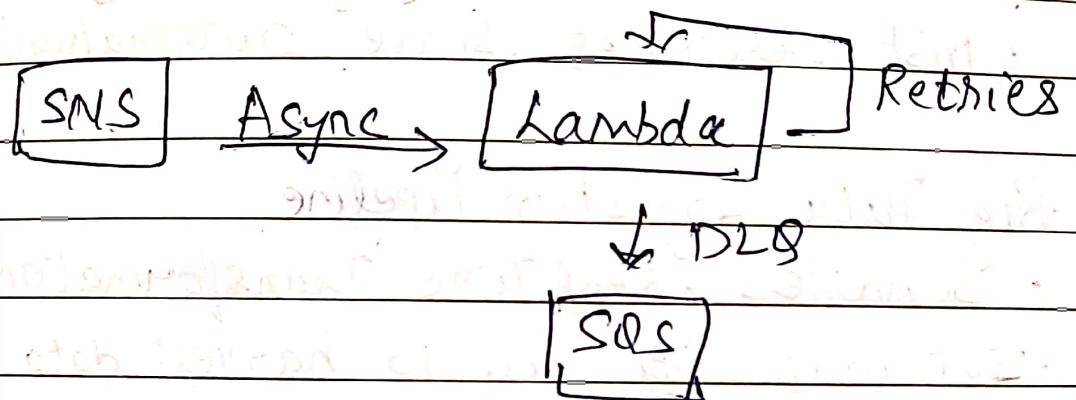
- Fully managed integration service, enables you to securely transfer data between SaaS and AWS.
- Destinations can be non-AWS services

- AWS Amplify: Web and mobile applications  
• Set of tools and services that help you deploy scalable full stack web and mobile applications

- Can be considered elastic beanstalk to mobile and web applications
- Choose this instead of cloudfront for cost-effectiveness

(101)

We can use this architecture



(102)

## AWS Lake Formation

- Data Lake is a central place to have all data for analytical purposes
  - Automate manual steps like cleaning, transformation
  - Out of box blueprints: S3, RDS
  - Fine grained access control (row and column)
- Built on top of glue
- Services that can use datalake: Athena, Redshift, EMR, Spark

## (103) Managing Streaming for Apache Kafka

- Alternative to Kinesis
- Fully managed Apache Kafka on AWS
  - Deploy in VPC
  - Multi-AZ support
  - Data is stored in EBS
- MSK Serverless
  - Run without managing capacity
  - MSK resources scale automatically

## (104) Big Data Ingestion Pipeline

- Serverless, Real Time Transformation
- IoT cores allow you to harvest data from IoT devices

(105) You can transition objects to S3 Standard IA or S3 One Zone IA after it has been for atleast 30 days.

## (106) RDS Proxy uses

- Share database connections to improve ability to scale
- More resilient by automatically connecting to standby instance

(107)

(108)

(109)

(110)

(111)

(107)

AWS Global Accelerator helps managing traffic hosted across multiple AWS regions

S3 Transfer Acceleration helps speed up long distance object transfers between S3 buckets. No caching is done. Only network path is optimised.

CloudFront is content delivery which helps in caching data at edge.

(108)

AWS EC2 Instance Store provides block storage for your application

(109)

To make sure developers do not attach administrative policy, ~~create~~ set IAM permissions boundary on developer IAM role that explicitly denies attaching the admin policy.

(110)

Redshift

- Columnar DB

- Inbuilt Caching (No need to implement)  
you can do it yourself or use elastic cache

(111)

You cannot delete root user account.  
You can only make it more secure.

## (112) File vs Block vs Object Storage

(113)

### Object Storage

- No hierarchy
- Stores data in small chunks
- Must use API to access and manage objects
- ~~Cannot lock files~~
- Slower performance than other storage types

### File Storage

- All data is saved together in a single file.
- File may also be stored in NAS
- Uses hierarchical structures
- Easy to access on small scale
- File sharing / lock can be done at file level

### Block Storage

- Divide data in fixed blocks of data
- You can store on Storage Area Networks (SAN)
- Very fast, but expensive
- AWS Instance store is block storage

113

Bastion Hosts are hosted in public subnet

### Ephemeral Ports

- Client connects to defined port
- Client expects response on an ephemeral port
- They allow multiple client applications to establish simultaneous connections to a server without interfering.

Virtual Private Gateway (Virtual) is created and attached to the VPC from which you want to create Site-to-Site VPN. You need to enable Route Propagation.

### VPN Cloud Hub

- Provides secure connections when you have multiple VPN connections
- Low cost hub and spoke model
- Virtual Private Gateway connects to multiple customer gateways

High Resiliency via Direct connect is achieved by multiple DX across regions

Max Resiliency us multiple connections in each region

Cheaper option us to use Site-to-Site VPN as alternate/backup.

VPC Transit gateway is the only service that supports IP multicast.

ECMP: Equal Cost Multi Path Routing.

- Routing strategy to allow forwarding a packet over multiple best path.
- Creates multiple site-to-site VPN connections to increase bandwidth of your connection to AWS.

(IP4)

VPC Traffic Mirroring

- Capture and inspect network traffic
- Captures from network interface
- Different from VPC Flow Logs which capture to/from your VPC

Egress Only Internet Gateway  
Like NAT gateway, but for IPv6

No. of IP allowed by a CIDR block is as follow

e.g. 10.0.4.0/28

$$\Rightarrow (32-28) = 4$$

$$\Rightarrow 2^4 = 16$$

Know that AWS reserves 5 IP addresses

IPv4 & IPv6 cannot be disabled for any VPC. You can add one CIDR if IPv4

## AWS Network Firewall

- Protect entire VPC
- Protects from Layer 3 to 7
- Supports 1000s of rules

(14)

## AWS Services

### AWS Wavelength

- Delivers ultra low latency apps for 5G ~~services~~ devices
- Edge Computing for 5G

### AWS Private 5G

- Deploy & operate your own mobile network
- All hardware & software provided by AWS

### AWS AppSync

- Sits as an interface between apps and AWS

- Supports GraphQL access points

- Flexible API to combine data from diff AWS App Flow sources.

AWS App Flow  
Transfers data b/w SaaS applications & AWS Services.

## AWS Well Architected Framework

### Well Architect Tool

- Stop guessing your capacity needs
- Test at prod scale
- Automation & Fast Iteration of Architecture

### 6 Pillars

- operational Excellence
- Security                      • Performance Efficiency
- Reliability                    • Cost Optimization
- Sustainability

### AWS Trusted Advisor

- High Level Account Advisor
- Analyze your AWS Accounts and provide recommendation on 6 categories
  - Cost Optimization
  - Performance                      • Fault Tolerance
  - Security                          • Service Limits
  - Operational Excellence

### AWS Outposts

- Bring AWS services to any location on-premises
- Order your configuration of EC2/EBS/...
- You provide internet + power and connect to AWS via VPN/PX
- Like running AWS locally on-premises!

## AWS openSearch

- Derived from Elasticsearch
- Supports Fuzzy search

(115) AWS EFS cannot transition data to S3 via ~~life~~ lifecycle policies

## S3 Event Notifications

- Triggers when changes in S3 to enable automated workflows

## S3 Object Lambda

- Transform object as it is retrieved from S3

To transform data on demand, use object lambda

## AWS Cost Management

### AWS Budgets

- Set alerts on budgets
- Create scheduled reports
- Projected spend amount
- Budget actions to respond to thresholds

→ AWS Cost Explorer

- Visualize your costs over time
- Set cost allocation tags
- Retrieve via API if possible

→ AWS Cost and Usage Report

- Comprehensive cost and usage report

→ AWS Compute Optimizer

- Get recommendations to optimize your use of AWS resources
- Helps avoiding over-provisioning and under-provisioning of EC2, EBS, ECS & Lambda

→ AWS Savings Plan

- Save money via upfront cost

- No upfront cost + Pay-as-you-go

- Partial upfront cost

- All upfront cost

• Types of savings

- Compute Savings Plan

- EC2 Savings Plan

- SageMaker Savings Plan

→ AWS Cost Anomaly Detection

- Automated cost anomaly detection and root cause analysis

(118) AWS API Gateway has support for Canary release deployment.

↳ Allows you to split traffic between already deployed version and new version, rolling out to a subset of users before rolling it out fully.

## Deployment Strategies

- In-place

- Blue/Green addition of units

- Canary gradual increase of traffic

- Linear

- All-at-once

(119) AWS Route 53 can perform automatic failovers. However health checks must be enabled.

(120) Default security group rules:

- No inbound rules and all traffic is implicitly denied

- Outbound rule that allows all traffic to all IP addresses.

(121)

(121)

## AWS Network Firewall

(123)

Protection can be done via

- NACL
- VPC Security groups
- WAF
- Shield & Shield Advanced
- Firewall Manager

How to protect entire VPC in sophisticated way:

→ AWS Network Firewall

→ Layer 3 to 7

→ Any direction you can protect

(124)

Fine grained controls

- IP Filtering
- Domain Filtering
- Protocol Filtering
- General pattern match
- Alert on rules
- Active rule matching to send to S3, ~~SNS~~, CloudWatch, Kinesis

(125)

(122)

## SCP vs Permission Boundary vs Inline Policy

Org or  
Account  
Level

User Groups  
and IAM users  
Level

Directly  
attachable  
to IAM users

(123) Launch configuration vs Launch Template in Auto Scaling groups

Launch configuration is immutable  
Launch Template can have multiple versions

AWS recommends Launch Template

Launch Template exclusively supports having both spot and on-demand instances or specific types of instances

(124) If you intend to reuse code in more than one AWS Lambda function, you should consider creating AWS Lambda layers for re-usable code

You can create CloudWatch alarm to notify when Lambda has scaled too much

(125) Request throttling can be done by

- API gateway
- SNS (CloudWatch Metrics)
- Kinesis data streams
- Lambda with error handling

Cannot be done by

- AWS Lambda
- Elastic Load Balancers

126

## Network Load Balancer



EC2 instances in  
public subnet

- Traffic above is sorted through private IP address
- Sorts traffic based on the top slot

130

127

Type of Access Control for S3

Account Level

User Level

IAM Policies

ACL

Bucket Policies

131

128

Up to 7 instances can be put in a single AZ via spread placement group

132

129

In GBS encryption

- Data is encrypted at rest

- Data is encrypted in transit between volume and instance

- Snapshots created are encrypted.

(130) RDS by default does not allow you to access most OS of database. For this, you need RDS custom. This setup is a shared responsibility between customers and AWS.

(131) NAT instance provide more control than NAT gateway. However you have to manage the maintenance.

NAT instance can (gateway cannot)

- Support Port Forwarding
- Used as bastion servers
- Attach security groups

(132) AWS DataSync simplifies, automates and accelerates transfer of large amounts of data

You can migrate data to S3, EFS, FSX, via public virtual interface

- Private virtual interface

via transit virtual interface

Direct + Private + Data Sync  
Connect via VIP + Sync OR  
VPN.

(133) S3 Transfers Acceleration cannot be used for copying objects across S3 buckets

(134) Supported S3 Lifecycle Transitions

S3 Standard / Reduced Redundancy

→ S3 Standard IA

→ S3 Intelligent-Tiering

→ S3 One-Zone IA

→ S3 Colacres

→ S3 Colacres Deep Archive

(135) DMS allows you to migrate from existing application to stream from S3 to Kinesis Data Streams ~~Standard / Enhanced~~

(136) You can distribute traffic using AWS Global Accelerator as well as AWS Route 53 weighted routing. Using ~~static~~ latter cannot bypass DNS Caching.

(137)

(138)

(139)

(140)

(141)

(137)

SQS FIFO queues are supposed to have .fifo as suffix

FIFO SQS supports

- 3K messages per second with batching
- 300 messages per second without batching

(138)

Resource Access Manager has VPC sharing. This allows you to create apps/services in a shared and centrally managed VPC.

The owner cannot share the VPC itself, but rather one or more subnets of VPC.

(139)

If you use AWS Shield Advanced without consolidated billing, you will end up being charged a lot more.

(140)

If you define Aurora failovers as

- Tier 1 16TB → ② 7
- Tier 1 32TB → ① Orders Up
- Tier 10 32TB → ③ Priority.

(141)

When you take snapshot of instance and create AMI, and then copy AMI to another region ⇒ You have copied snapshot also. This is because AMI are based on underlying snapshots.

- 142 S3 can scale to
- 3500 TPS for PUT/COPY/UPDATE/DELETE
  - 5500 TPS for GET/HEAD

If you want to scale further, you can create more prefix.

- 143 S2 Data Transfer pricing is free

- Data transfer within region

- Data transfer from internet

- Data transfer to Cloudfront

For S3 transfer acceleration, you only pay if upload speed improves.

- 143 ~~AZ~~

- 143 RDS Multi-AZ  $\Rightarrow$  Synchronous Replication

At least 2 AZs.

Read Replicas  $\Rightarrow$  Asynchronous  
can be cross region.

- 144 AWS Systems Manager provides visibility and control of infra in AWS.

- Automate operational tasks across AWS resources

~~Patch Manager: Can apply patches to EC2 instances and not designed for Command.~~

~~Patch Manager is not designed for Command.~~

~~Run Command.~~

~~and forward requests directly to EC2 instances.~~

145) AWS organization, different accounts can share Reserved Instances.

146) If you have

- DB using EC2 instance in VPC A
- App using EC2 instance in VPC B

The way to connect will be to

- setup Peering connection
- Create inbound rules in A that allows traffic from private IP addresses of EC2 instances in B.

### (147) SQS delay queues

Helps delay delivery of new messages to a queue for a number of seconds. Range 0 - 15 mins.

### SQS Temporary Queues

- Helps save dev time and costs
- Provides high throughput request-response pattern

### (148) You can attach security groups to

EFS, EBS, RDS

This can avoid the problems associated with ~~unauthorized~~ unauthorized access.

Be careful in security groups vs IAM side.

### (149) If a VPC needs private access to S3 & DynamoDB you need to

- Create separate gateway endpoint for S3 & DynamoDB
- Add update route table of VPC to include target entries

(150)

## Bastion Hosts

- Always available in public subnet
- Provides SSH access to EC2 instances without exposing to internet
- Happens on Layer 4 protocol
- Use NLB (not ALB) + Autoscaling for high availability

(151)

## Dedicated Hosts

### Dedicated Hosts - Dedicated Instances

- Billing
- Visibility of cores, host ID
- Host and instance affinity + Instance placement + Automatic recovery

(152) Presigned URL allows you to get temp

access to files stored in your buckets

It contains security tokens valid for limited amount of time

Signed URLs have parameters that are hashed + secret. Primary creates to make sure URL has not been tampered.

(153)

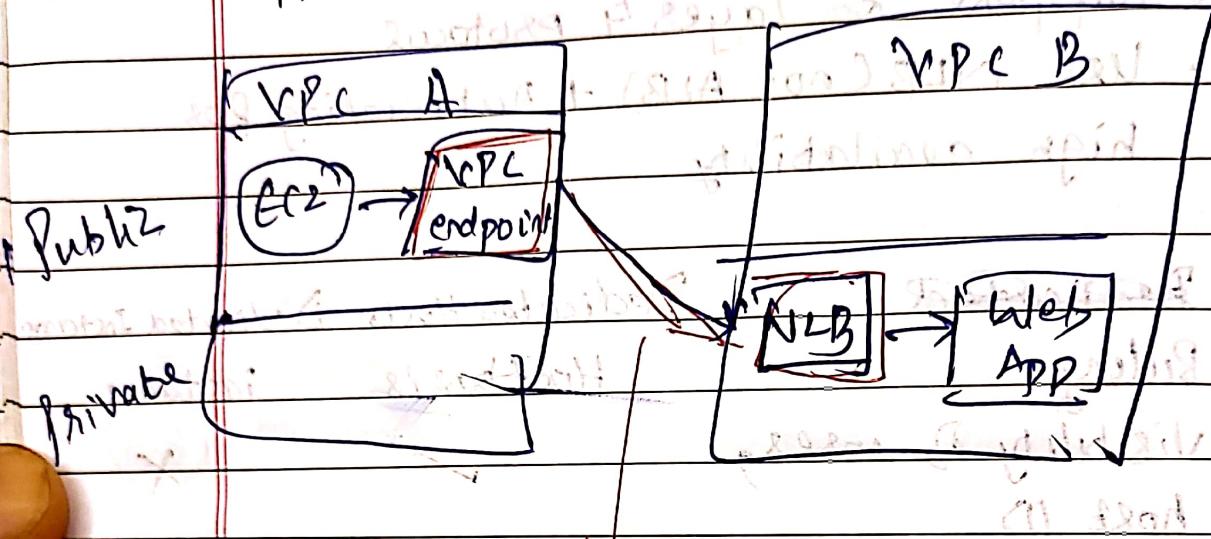
To improve resiliency of direct connect

- Have 2 direct connects
- Have 2 customer gateway on different devices

(154)

If you have VPC A, and another app in VPC B.

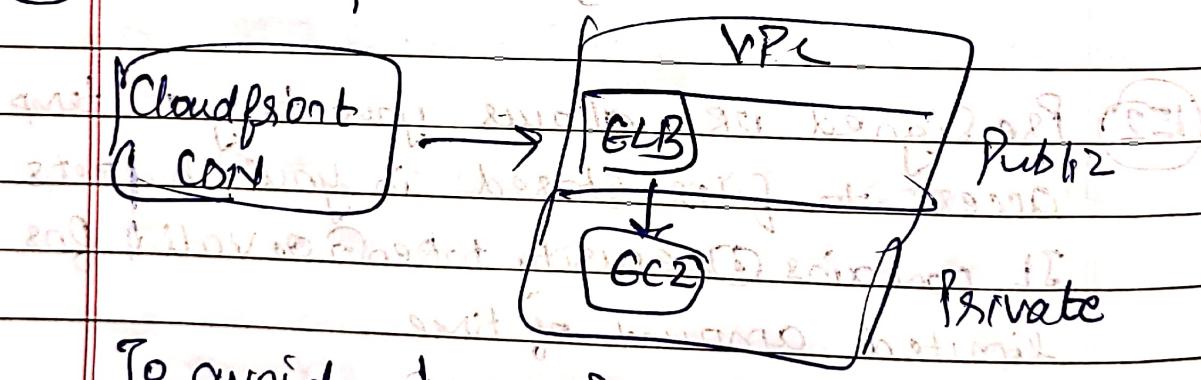
If apps in VPC A need to connect to app in VPC B



This is required.

(155)

For a setup like this



To avoid bypassing ELB, you can create security group for ELB to only allow Cloudfront to access private IP addresses.

Since addresses change from time to time, Lambda service needs to update SNS as well.

(156) Multi Masters DBs only work within a region of AWS.

AWS Organizations

• Helps you centrally manage your accounts

• Can create accounts programmatically

• Can setup SSO logins

• Can apply Service Control Policies (SCP)

• Available in two feature sets

• Consolidated Billing

• All features

AWS Organization: Collection of AWS accounts that you organize into a hierarchy.

AWS Account: Contains most AWS resources

Management Account: Account you use to create your organization

Member Account: AWS Account, other than Management account, that is part of org.

Administrative Root: Starting point for organizing your accounts

Organization Unit: Group containing accounts

- Migrating accounts b/w orgs
- Must have root/IAM access to both members and management accounts
  - Before migration download any billing or reporting history

### Service Control Policies (SCP)

- Available in organization with all features enabled
- Tasks and entities are not restricted by SCP

### Resource Groups

- Organize AWS resources
- Automate and manage large number of ~~to~~ resources at one time
- Resource group is a collection of AWS resources that are in the same region, and match criteria provided in a query

Tag-Based Queries: include list of resources and tags. Keys that help identify and sort your resources

(158) AWS API gateway can directly hit dynamo DB