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 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) Event Bridge is based on event based architecture. You can set rules to configure other services to be triggered when an event reaches.

⑤ Elastic Block Storage
- Network drive. So expect some latency.
- Snapshot Possible
- Locked to 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 Users

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 ~~if~~ 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 DynamoDB 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 internet. IGW allows instances with public IP address. NAT gateway only allows for outbound access. Allows instances with no internet access

(12) IAM credentials report is tool for IAM security.

(13) EC2 user 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 Securit

(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 anytime vs you need to disconnect NACL from subnet to do same
- SG → stateful (only allow rules)
  NACL → 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/io2)
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 balancer

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

(19) NACL vs WAF

NACL	WAF
Network Access Control List	Web Application Firewall
→ Layer 4	→ Layer 7
→ Stateless	→ Stateful
→ Block specific IP addresses	→ Controls via HTTP headers & payloads
→ Tied to VPC subnets	→ 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 use DMS.

(21) You can use CloudFront with custom origin to point to on-premis

(22) IAM Policy with Priorities
- Explicit Deny
- Explicit Allow
- 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 retri

(24) Encryption can be done in 3 ways for servers side

- S3 Managed Keys / SSE-S3 (Servers side encryption)
→ Amazon manages encryption and decryption for you automatically
→ You concede control to AWS
→ Ease of use
- AWS Key Management Service (AWS KMS)
→ Unlike KMS, each object is encrypted using uniquekey
→ 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

Search can be done via Elastic Search must be indexed as well.

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 It is not compatible with "Byte Range Fetch" parameter which limits the amount of data retrieved from S3 object

(30)

(31)

(32)

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

(30) Storage Gateway → Not same as FSx 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: iSCSI 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
- Work at Layer 4

(32) ~~DynamoDB vs SQL DBs (RedShift,~~

(33) DynamoDB vs SQL (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 leverage parallel processing to get data from SSD

(34) Dynamo Streams
- Control Flow of Info
- ~~Stream writes to~~
- With change DynamoDB writes to stream Lambda can be configured

DynamoDB Global Tables
- Multi Region, Multi Master Replication
- Requires enabling Dynamo Streams

(35)

Network Access Control List (NACL)	Security Group (SG)
• Control inbound & outbound for subnets	• Control inbound & outbound for instances
• Stateless (You have to allow both sides)	• Stateful (Allowing inbound allows outbound)
• Default, everything is ~~denied~~ /allowed	• Default everything is allowed.
• Has rule based priority	• No rule based priority
• NACL can be associated with multiple subnets	• Can be associated with multiple instances
• Possible to block IP	• Blocking IP is not possible

Similarities

- Both control network access
- Both are integral part of VPC

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

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

(37) IAM Securities 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
- Cluster: High Communication b/w EC2. Low availability as everything under same rack
- Spread: Spans across availability zones
- Partition: 100s of EC2 instances across many A-Z. Big Data like HDFS, HBase, Cassandra

NOT suitable for large workloads

(39) There are 4 types of services which improve networking capability in AWS
- Elastic IP Address
- Elastic Network Interface (ENI)
- Elastic Fabric Adapter (EFA)
- Elastic Network Adapter (ENA)

Page

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 sophesticated 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

Elastic Network Adapter (ENA)
- High Throughput + Low Latency for EC2
- Designed for modern DBs, distributed memory cache
- Supports 100GBps of network bandwidth.

(40) EBS Snapshots ~~Feature~~

- Not necessary to detach volume, but recomended
  - → Snapshoting 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

(41) EBS Volume Types

- General Purpose (SSD)
  - gp2
    - Burst IOPS 3000 (Small)
    - Burst IOPS 16000 (Large)

IOPS ⇒ Input Output Per Second.

(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 ⇒ Max out at 5334 GB

  You cannot increase one without another

- Provisioned IOPS SSD
  - Great for DB workloads
  - Useful when IOPS > 16K
  - io1/io2
    - Storage 4GB - 16TB
    - Storage & IOPS
    - Nitro EC2 instance : 64000
    - Other EC2 instance : 32000
    - io2 have more durability
  - io2 Block Express
    - Storage : 4GB - 64TB
    - Sub millisecond latency
    - Max PIOPS : 256,000
      IOPS/GB : 1000:1

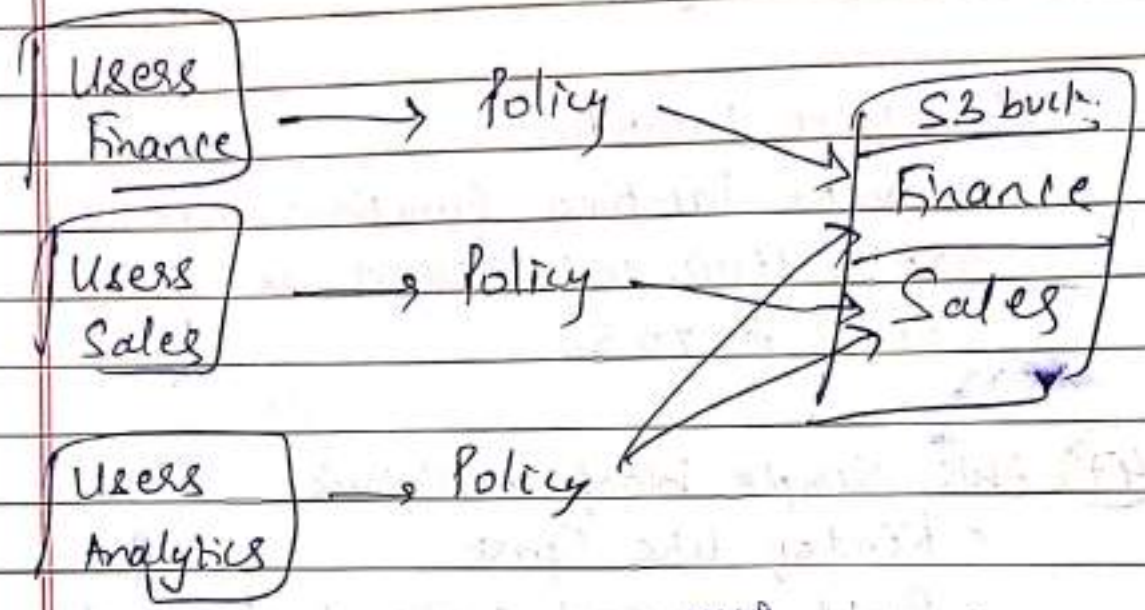
  • Supports Multi EBS Attach

- Hard Disk Drives (HDD)
- Storage: 125GB to 16TB
- Throughput Optimized HDD (st1)
  - Max Throughput 500 MB/s
  - Max IOPS: 500

(42) 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
- Throughput Mode
  - Bursting
  - Provisioned
  - Elastic: Auto scale based on needs

Storage Tiers
- Standard
- Infrequent Access

(43) S3 Access Points is useful when
- You have large numbers of users requiring access to specific S3 bucket data
- S3 bucket contain lot of data



(44) RAID 0 vs RAID 1

Striping	Mirrors
Focuses on performance	Focuses on resiliency
If one drive fails all the data is lost	Data in 1 drive is lost means it can still be recovered

(45) S3 Object lock prevents deletion during a customer-defined retention period.
S3:PutObjectLegalHold : 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 is 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 transfer

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

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

(52) To improve recovery time of an EC2 instance

RAID 0 → No Resiliency
RAID 1 → Resiliency present ⇒ Fastest
Cloudwatch triggers → Slow & more
to reroves EC2 Resilient

(53) Snowcone → Edge Computing + Data Migration
→ 8TB HDD or 14TBSSD
Snowball → Edge Computing + Data Migration
Edge → 80TB
Snowmobile → >10PB
→ 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 Autoscaling 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) Cloud front Functions
- Lightweight functions in Javascript for high scale latency sensitive CDN customizations
- Cheap . Useful for → URL re-writes
→ Header 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
SecureTransport: 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 accelerators to point to.

(62)

AWS Dynamo DB	AWS DocumenDB
• Proprietry to AWS	• Built on top with MongoDB. Fully compatible
• DAX for very high reads	
• Fully Managed	• Fully management
• Highly Available	• Highly Available

- Provisioned vs Autoscaling vs On-Demand
- Global Table Feature: Active Active Setup
- Has TTL feature
- Dynamo DB Streams

~~62 Amazon~~ Po

63 AWS ML Services

- Polly (Text to Speech)
  - Converts text to speech to build speech enabled products
  - Use SS ML to customize
- Transcribe (Speech to text)
  - Automate speech to text quickly
  - Automatically remove PII data
- Sagemaker
  - Fully managed platform to train, deploy ML models
- Textract (Extract text and data)
  Read documents to extract text, handwriting etc.,
- Kendra (Find Accurate Info Faster)
  - Search info in different content repositories and documents
- Personalize
  Build Real time personalized recommendations
- Forecast
  Delivers highly managed forecasts

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

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

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

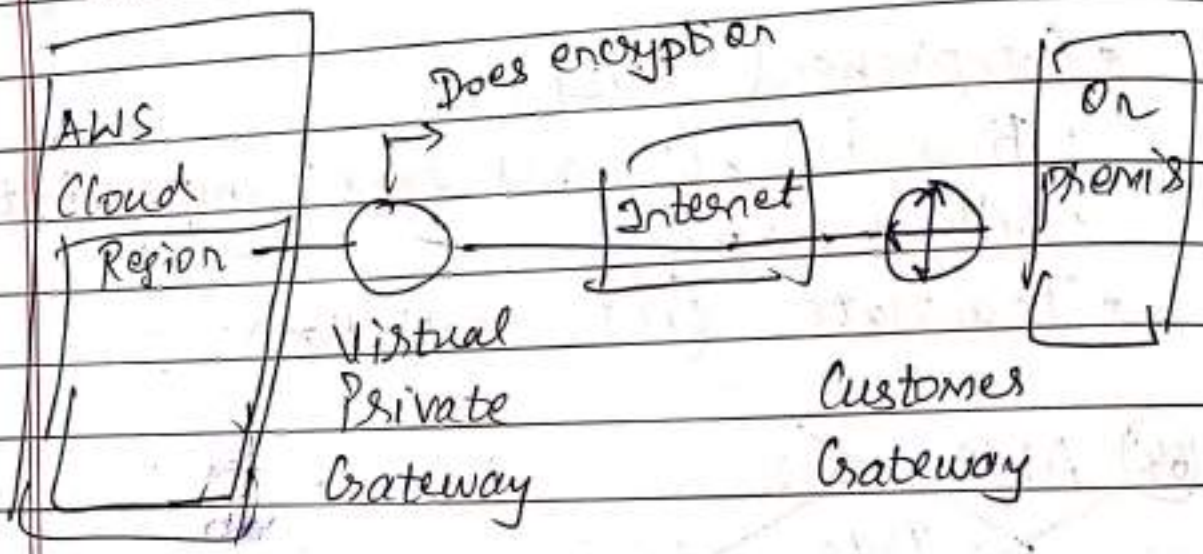
64) AWS ~~Kinesis~~
- Data Streams
- Data Analytics
- Data Firehouse
- Video Streams

64) ~~Important~~ AWS ~~Services~~ General Info
- AWS ~~Direct~~ 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

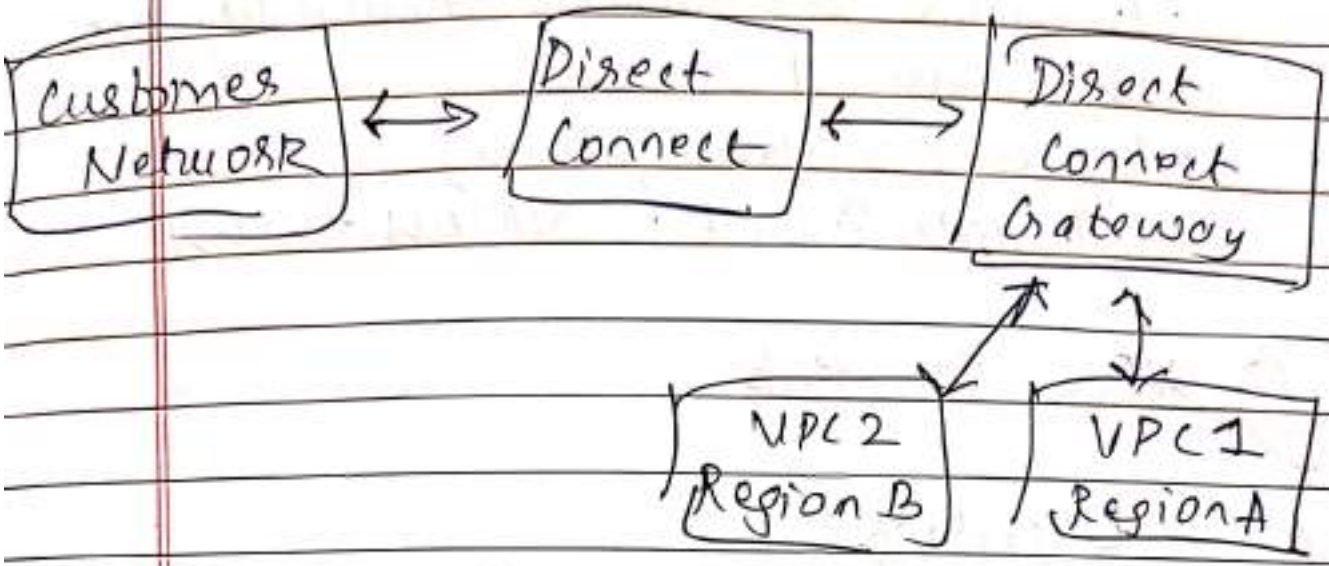


- Automated Resiliency and Failover built in

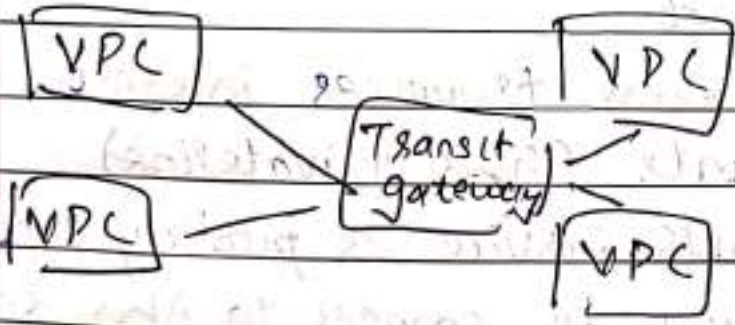
Using multiple customer gateway leads to resiliency and failover on your side of VPN.

(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, Direct Connect + VPN 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.



- Make sure no overlapping CIDR.
- 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

e) 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 => NATGW => IGW

f) ~~VPN CloudHub~~

g) VPC peering
- Privately connect two VPCs
- NOT transitive in nature
- Supports Inter Region peering
- Must update route table in each VPC subnet
- Traffic never traverses internet

- CIDR should not overlap

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

Interface Endpoints	Gateway Endpoints
Provisions ENI as entry point	• Used as a target in route table
• $per hour + $per GB	• Supports S3 & Dynamo DB
• Must attach security groups	• Free

(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 ~~data~~ data request packet sniffer
- Data can store in S3, CloudWatch & Kinesis Data Firehouse

(65) API Gateway (lives in a region)
- Support for web sockets
- Handles versioning, authentication, validation caching, etc. Request throttling
- Integrations
  - Lambda Function
  - AWS Service
  - HTTP
- ~~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 Authorizers (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 sign in using well known (External Identity Provides) such as facebook, google etc.
You recieve authentication token, and temp ~~sec~~ credentials in return.

The credentials are mapped to IAM role with permissions

Default IAM roles for authenticated and

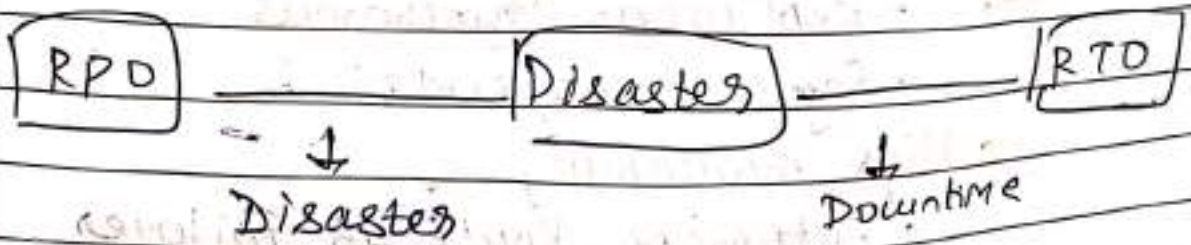
(67) AWS Step Functions
- Serverless visual workflows
- Features: Error Handling, Sequence, Parallel, conditions
- Integrates with EC2, ECS, Onpremise

(68) Disaster Recovery & Migrations

Types of Disaster Recovery
- Onpremise ⇒ On-premise
- On-premise ⇒ AWS Cloud
- AWS Cloud ⇒ AWS Cloud
  Region A Region B

Recovery Time Objective
- Time between disaster and last backup i.e the data loss

Recovery Time Objective
- Time between disaster and recovery



Recovery Strategies

- Backup & Restore (High RPO, High RTO)
- Pilot Light (High RPO, Modium 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
  - Cloud Formation / Elastic Beanstalk
  - Recover via CloudWatch Alarm

Database Migration Service (DMS)

- On premise to AWS Database migration
- Continious Data Replication (CDC)
- Must create EC2 instance for replication
  - prefer compute intensive

- Use Schema Conversion Tool (SCT) when DB engine is changing

Multi A-Z 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 aws_s3 Aurora extension

On Premise 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 / DynamoDB
  • 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 : Transition to cold storage
  - Window : 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-premis data centers
- Server utilisation data and dependency mapping is important

Agentless Discovery (Agentless Discovery Connector)
- VM Inventory, Performance history like
- Configuration CPU, Memory, Disk Usage

Agent Based Discovery (AWS Application Discovery Agent)
- 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 trigger 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 setup~~
- To send cloudwatch logs
  - Run cloudwatch agent on EC2
  - Make sure IAM policies are correct
  - cloudwatch log agent can be setup on-premise

Cloudwatch unified agent metrics

- CPU
- RAM
- Disk Metrics
- Netstat [No. of TCP, UDP connections, net packets, bytes]
- Processes
- Swap Space

Cloudwatch Alarms

- Used to notify on event
- Trigger 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 recieve

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
- S3
- Codebuild
- Trusted Advisor
- Cloud Trail

works with variety of destinations
- Compute : Lambda, AWS Batch, ECS Task
- Integration: SQS, SNS, Kinesis Data Stream
- Orchestration: Step Functions, Code Pipeline, Code Build
- Maintainence : SSM, EC2 Actions

- Archieving events is possible
- Replay events is possible

- Eventbridge supports schema inference
- Schema Registry allows you to generate code for application, that knows in advance structure of event bus

Cloud Watch Containes Insights
- Collect & analyze logs from containes
- 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 workes shutdown

Cloudwatch Contributor Insights
- See top N contributors
- Total unique contributors
- Useful for - identifying bad hosts
  - identifying heaviest network users

Cloud watch 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
- Containes Insights

CloudTrail integrates with EventBridge to intercept API call

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 90days.

CloudTrail Events

→ Management Events
- Operations performed on resources in your account

Can be seperated
- 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 recieve alerts for changes
  - AWS Config cannot prevent actions from happening
- AWS Config is per region service
- AWS Managed Rules or set your own rules using AWS Lambda

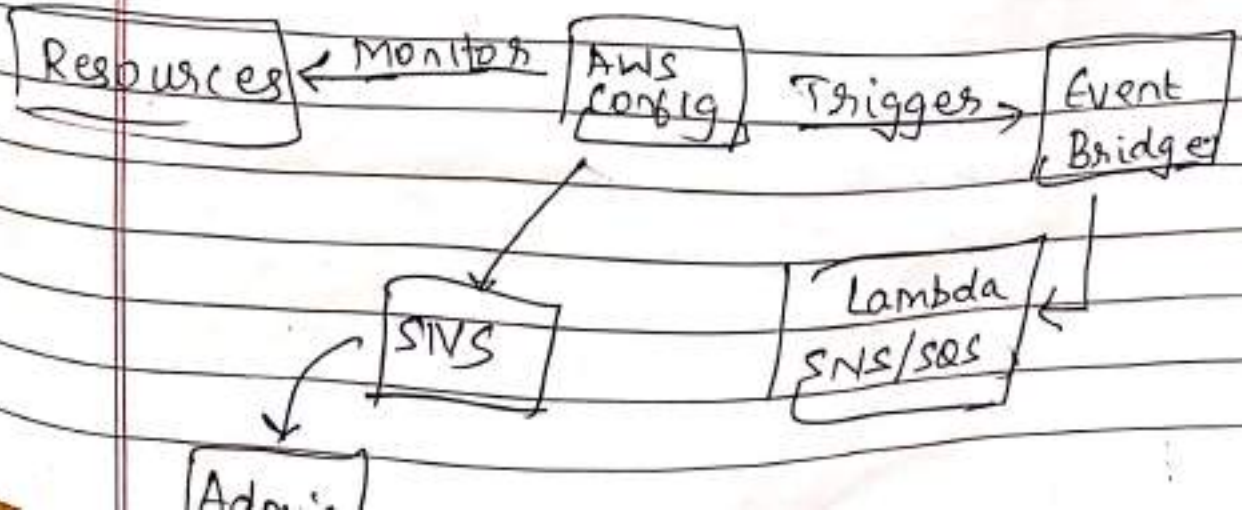
Resource

- 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

(71) 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 recieved 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 use symmetric CMKs
  - You never get access to KMS unencrypted (must use KMS API)

- Asymmetric (RSA & ECC key pairs)
- Public & private pair
  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 DynamoDB - Global Tables, Amazon Aurora - Global

Each replica will decrypt from their own region KMS.

S3 Replication - Encryption Considerations

- Unencrypted objects, objects encrypted with SSE-S3 are replicated
- Encryption using SSE-KMS one should enable • KMS Keys, Target Bucket
  • Attach IAM Key Policy to with 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)

~~API sharing policies~~
API sharing process encrypted 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
- my-app/
  - dev
    - db password
  - prod
    - db password

Parameter Store Hierarchy

Parameter tiers: 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.

AWS Secrets Manager

- Newer service, meant for storing secrets
- Additional features (compared to Parameter Store)
  - Force 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 certificate 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 vs Email.
  - DNS is automated.
    - DNS will leverage CNAME to DNS config
  - Takes a few hours

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~~ is
Web ACL (Access Control List) is region and WAF integrates with AWS services:-
- Application Load Balancer
- API gateway
- CloudFront
- AppSync Graph QL API
- Cognito User Pool

} Seperate WAF for each.

AWS Shield : Protect from DDOS attack

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

AWS Firewall Manager

- Manages rules across all accounts
- Security policies
  - WAF rules
  - AWS Shield Advanced
  - Security groups for EC2
  - Network Firewall
  - Route 53

NACL

Rules are applied automatically when a new service is created.

WAF vs Shield vs Firewall Manager

- They combined provide 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

Amazon Guard Duty

- Identify threats using ML algos
- Cloud Trail Logs
  - Unusual API calls
  - Unauthorized deployments
- VPC Flow Logs
  - Unusual internal traffic
  - Unusual IP addresses
- DNS Logs
  - Compromised EC2 instances sending encoded data within DNS queries
- Kubernetes Audit Logs
  - Potential EKS cluster compromises

Sources

Can setup event bridge rules

Amazon Inspector

- Automated security assesments on EC2, Lambda, Containes Images
- Identify vulnerabilities } existing DB
- Code vulnerabilities } containing CVE scores
- Network Reachability
- Can send notification to Event Bridge

AWS Macie

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

(72) When looking for a cost effective solution and usage is unkown
- 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
  Cost Effective
- st2 (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"

(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 with 4 options
  - Windows File Server for Windows based application
  - Lustre for compute-intensive workloads
  - Netapp ONTAP
  - OpenZS

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 dat 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 be~~ done by configuring an origin access identity (OAI). This is special type of cloudfront uses. Only this user should have access to S3

(80) You cannot create multi-region Aurora DB clustes. ~~You~~ 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 upto 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 Partioning	✓	✓
• Support for multiple languages	✓	✓
• Multi-threaded architecture	✗	✓
• Advanced data structures	✓	✗
• Snapshots	✓	✗
• Replication	✓	✗
• Transactions	✓	✗
• Pub/Sub	✓	✗
• Lua Scripting	✓	✗
• Geospatial support	✓	✗

Differences

(86) AWS registers upto 2 IPs. This allows for automatic failover (similar to Routes)

(87) Section 30: Other Services

(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
  - Infra as code

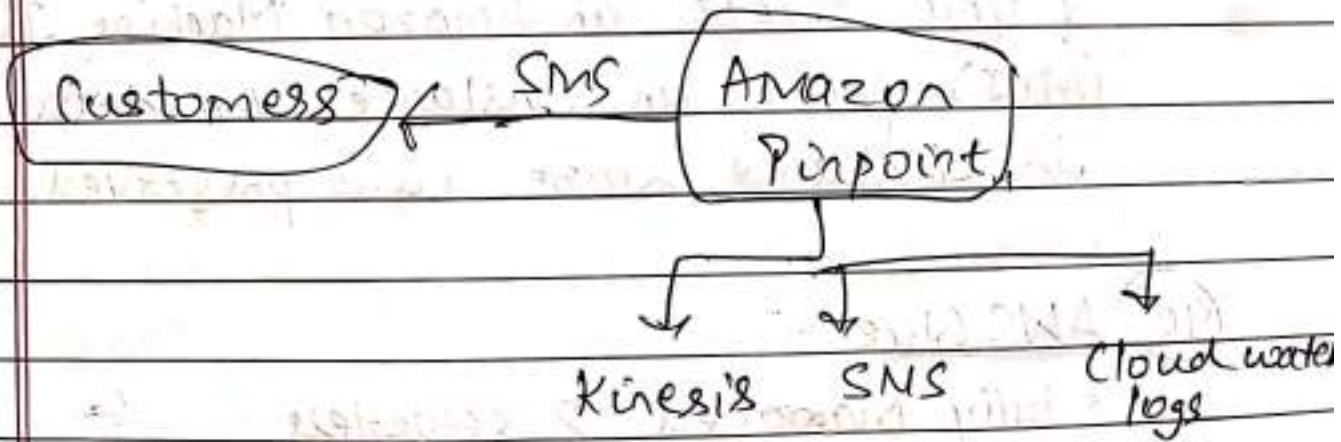
  Repeat architecture in different region/ environment/account
- IAM role that allow cloudformation to create/modify/delete resources
- If you do not ~~pro~~provide IAM role it uses your permissions.

Simple Email Service (SES)

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

Amazon Pinpoint

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



Versus SNS or 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

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

(89) When you stop, hibernate or terminate an instance every block of storage in the instance store is reset.

If you create an Amazon Machine Image (AMI) from an instance, the data in instance store isn't preserved.

(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 cluster.

Date
Page

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

(91) Any database upgrade in RDS database instance with multi A-Z 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

(93) Amazon RDS
- Multi AZ deployments (1)
- Multi-Region deployments (2)
- Read Replicas (3)

(1)	(2)	(3)
High availability	Disaster Recovery	Scalability
Synchronous Replication	Asynchronous replication	Asynchronous replication

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

(95) AWS Kinesis
- Data streams
- Data Firehouse
- Data analytics
- Video Streams

} Stands in analytics category of AWS.

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 services

(96)

(97)

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

(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
. 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 ~~source~~ the data has to → More costly.

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

You can use to analyze traffic patterns (101)

(100) AWS Batch

- Fully managed batch processing at scale. No need to manage instances
- Dynamically scale EC2
- Defined as docker image
- Compatible with many frameworks for multi-node comms, Tensorflow etc.. (102)

Batch vs Lambda

- Time limit of 15 mins in Lambda
- Batch is not serverless

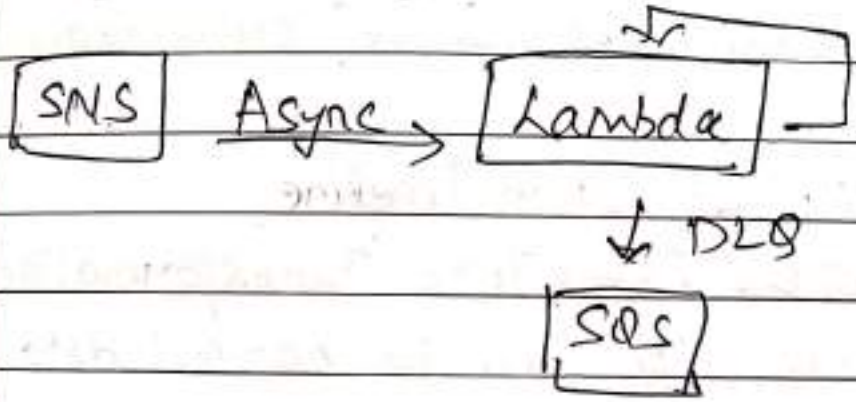
Amazon AppFlow

- 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)

(111)

(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 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

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 structure
- 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 Network 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 ephemal port.
- They allow multiple client applications to establish simultaneous connections to a server without interfering.

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

VPN CloudHub
- Provide secure connections when you have multiple VPN connections
- Low cost hub and spoke model
- Virtual Private Gateway connects to multiple customer gateway.

- High Resiliency via Direct connect is achieved by multiple DX across regions
- Max Resiliency is multiple connections in each region

Cheaper option is to use SitetoSite 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

(114)

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
=> (32-28) = 4
=> 2^4 = 16
Know that AWS reserves 5 IP addresses

IPV4 & IPV6 cannot be disabled for any VPC. You can add CIDR if IPV4 range is out.

AWS Network Firewall
- Protect entire VPC
- Protects from Layers 3 to 7
- Supports 1000s of rules

(114) 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 sources.

AWS AppFlow
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
- Reliability
- Sustainability
- Performance Efficiency
- Cost Optimisation

AWS Trusted Advisor

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

AWS Outposts

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

AWS openSearch
- Derived from Elastic Search
- Supports Fuzzy search

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

(116) 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

(117) 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 is 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
  - Partial upfront cost
  - All upfront cost
- Types of savings
  - Compute Savings Plan
  - EC2 Savings Plan
  - Sagemaker Savings Plan

→ AWS Cost Anamoly Detection
Automated cost anamdy 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
- Canary
- Linear
- All-at-once

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

(120) Default security group
- No inbound rules and all traffic is implicitly denied
- Outbound rule that allow all traffic to all IP addresses.

(121)

(121) AWS Network Firewall

Protection can be done via
- NACL
- VPC Security groups
- WAF
- Shield & Shield Advanced
- Firewall Manager

How to protect entire VPC in sophesticated way?
→ AWS Network Firewall
→ Layer 3 to 7
→ Any direction you can protect

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

(122) SCP vs Permission Boundary vs Inline Policy

Org or Account Level	User Groups and IAM user level	Directly attachable to IAM users

(123)

(124)

(125)

(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 layer 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
- SQS
- Kinesis data streams

Cannot be done by
- AWS Lambda
- Elastic Load Balancer

(126) Network Load Balancer

↓

EC2 instances in public subnet

(130)

Traffic above is routed through private IP address

(131)

(127)

Type of Access Control for S3	Account Level	User Level
IAM Policies	X	✓
ACL	✓	X
Bucket Policies	✓	✓

(132)

(128) Upto 7 instances can be put in a single A-Z via Spread placement group

(129) In EBS encryption

- Data is encrypted at rest
- Data is encrypted in transit b/w volume and instance
- Snapshot created is encrypted.

(130) RDS by default does not allow you to access host OS of database.
For this, you need RDS Custom.
This setup us a shared responsibility between customes and AWS.

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

NAT instance can (gateway cannot)
- Support Port Forwarding
- Used as bastian server
- Attach security groups

(132) AWS Datasync simplifies, automates and accelerate transfer of large amounts of data

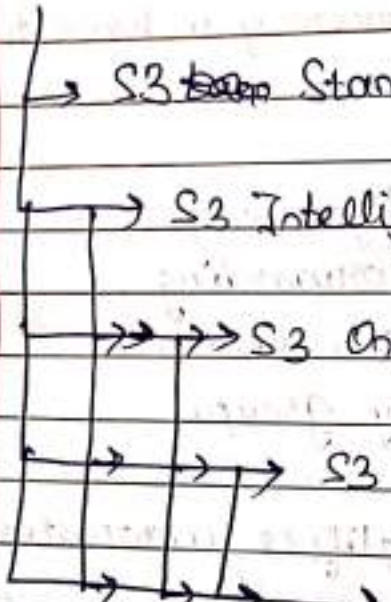
You can migrate data to S3, EFS, FSX, via
- public virtual interface
- private virtual interface
- transit virtual interface

Direct Connect + Private VIF + Data Sync ⇒ Secure
OR
VPN.

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

(134) Supported S3 Lifecycle Transitions

S3 Standard / Reduced Redundancy



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

(136) You can distribute traffic using AWS Global Accelerator as well as AWS Route 53 weighted routing. Using 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)
- Tier 1 32TB → (1)
- Tier 10 32TB → (2)

} order of 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) S3 Data Transfer pricing is free for
- Data transfer within region
- Data transfer from internet
- Data Transfer to Cloudfront

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

(143) RDS Multi AZ ⇒ Synchronous Replication
Atleast 2 AZs.
Read Replicas ⇒ 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
Patch Manager
Run Command.

(145) AWS organisation, different accounts can share Reserved Instances.

(146) If you have
- DB us EC2 instance in VPC A
- App us EC2 instance in VPC B

The way to connect will be to
- setup peering connection
- Create inbound rule 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
Rang 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 access,

Be careful in security groups vs IAM side.

(149) If a VPC needs private access to S3 & Dynamo DB you need to
- create seperate gateway endpoint for S3 & Dynamo DB
- 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)

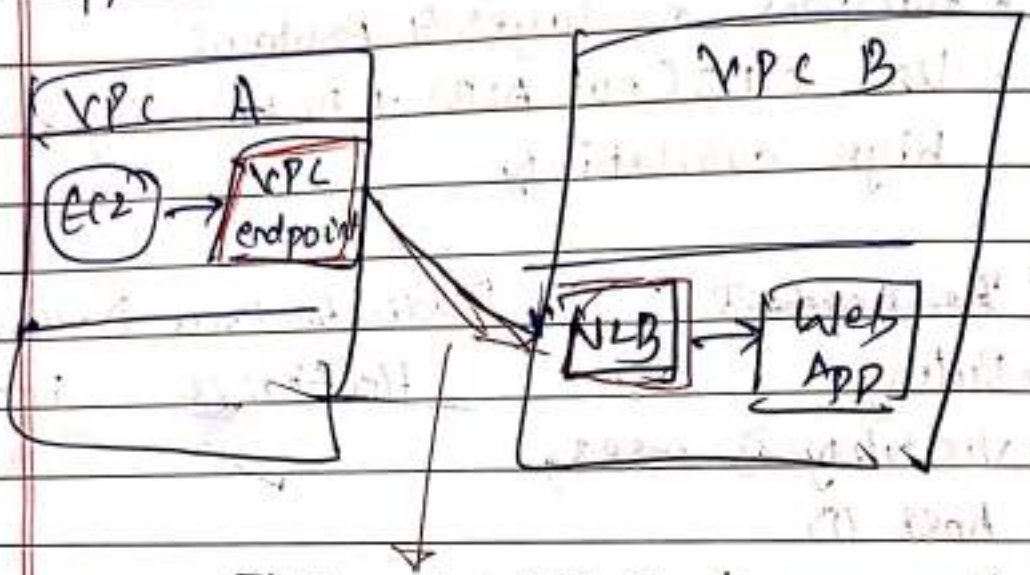
	Dedicated Hosts	Dedicated Instance
Billing	Hostbasis	instance
Visibility of cores, host ID	✓	✗
Host and instance affinity + Instance placement + Automatic recovery	✓	✗

(152) Pre Signed URL allows you to get temp access to files stored in your buckets
It contains ① Security token ② valid for limited amount of time

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

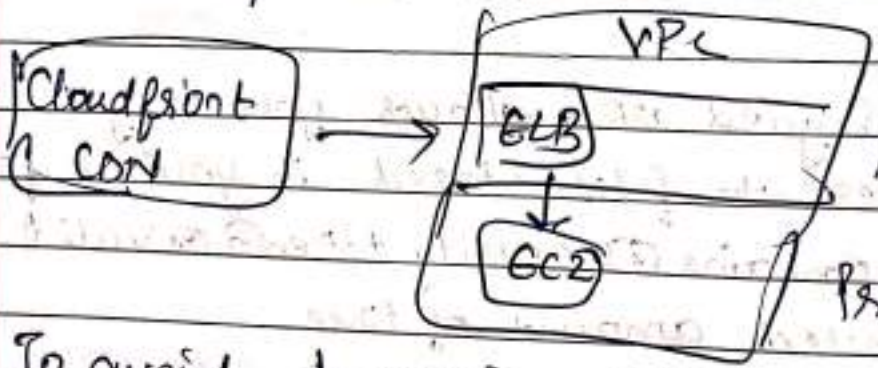
(153) To improve resiliency of direct connect
- Have 2 direct connects
- Have 2 customer gateway on different devices

(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 ~~CDN IPs~~ Private IP addresses.

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

156 Multi Master DBs only work within a region of AWS.

157 AWS Organizations
- Helps you centrally manage your accounts
- Can create accounts programatically
- 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: Containes for 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 member 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 ~~tags~~ 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 dynamoDB