24 regions, 77 Availability Zones, 150 Edge Locations.

Compute

EC2:

- **Max 20 EC2 instances** per region per account.
- User data commands called/executed **only at first time**
- Uses Xen Linux & Nitro Hypervisor for VM provisioning

EC2 Launch Modes:

- On-demand instance costs 10cents/hour
- Reserved instance costs 75% less than on-demand
- Reserved instance **must be reserved for 1 to 3 years**
- Convertible reserved instance costs 54% less of on-demand
- Spot instance costs 90% less compared to on-demand
- 2 mins grace period before retrenching spot instances
- Spot block instance lifetime 1 to 6 hrs. max

EC2 Instance Types:

- R => RAM intensive workload
- C => CPU intensive workload
- M => Medium workload
- I => IO intensive workload
- G => GPU intensive workload
- T2/T3 => Burstable type of instances

Security Group:

- Region Specific
- By default, allow all outbound
- Acts like a filter
- EC2 not aware?
- Connection refused error then ec2 issues
- Timeout issues => Security Group issues
- Permission issues on the SSH key => run "chmod 0400"
- Security groups can refer other security groups instead of IP address ranges

Private IP vs Public IP vs Elastic IP:

- IPv6 is mainly used for IoT
- IPv4 allows **3.7 billion** different addresses
- Private IP networked machines connect to WWW using a NAT + Internet Gateway (i.e., Proxy)
- In EC2, when we stop/start an instance, its public IP can change. To avoid and have a fixed public IP for your instance, you need an Elastic IP
- Elastic IP is a public IPv4 IP you own as long as you don't delete it. You can attach **one instance at a time**
- With an Elastic IP address, you can mask failure of an instance or software by rapidly remapping the address to another instance in your account
- **5 Elastic IP per account** (you can ask AWS to increase this limit)
- **Try avoid using elastic IP**. This shows poor architectural decisions. Instead, use a random public IP and register a DNS name to it.
- Best architectural pattern is, using load balancer and don't use a public IP

AMI (Amazon Machine Images):

- You can create AMIs to pre-install software on your EC2 to have faster boot time
- AMI by default region scoped not global
- AMI can be copied across regions and accounts

EC2 Placement Group:

- Cluster => All **EC2 can be closed together in a single-AZ,** when needed very high-performance computing. Same Rack & Same AZ
  - Low-latency, 10 Gbps network
  - **Not applicable for T2 type of instances**
- Spread => When you want EC2 instances to be spread around multiple availability zones (**Maximum 7 instances per group per AZ**). Good fit for critical applications.
  - Span across multiple AZ, reduced risk of simultaneous failure
- Partition => Spread instances across many different partitions (different set of racks) within an AZ. Scales to 100s of EC2 instances per group. Good fit for Hadoop/Cassandra/Kafka
  - **Up to 7 partition per AZ**

Elastic Network Interfaces (ENI):

- Logical component in a VPC that represents a virtual network card
- Bound **to a specific AZ**
- Attributes:
  - Primary private IPv4, one or more secondary IPv4
  - One Elastic IP (IPv4) per private IPv4
  - One Public IPv4
  - One or more security groups
  - A MAC addresses

EC2 Hibernate:

- The in-memory state is preserved. RAM state is
- to a file in root EBS volume hence root EBS volume must be encrypted. Root volume shouldn't be instance store and it must be large enough.
- Best fit for: long-running processing, saving the RAM state, services that take time to initialize
- Doesn't support all EC2 instance types. Only applicable for: C3, C4, C5, M3, M4, M5, R3, R4 & R5
- Instance RAM size must be < 150GB. Instance size not supported for bare metal instances
- Available only for on-demand and reserved instances
- Instance cannot be hibernated for more than 60 days

Scalability vs High Availability:

- Vertical Scaling: Increase instance size (= scale up/down)
- Horizontal Scaling: Increase number of instances (= scale out/in)
  - Auto Scaling Group
  - Load Balancer
- High Availability: Run instances for the same application across multi-AZ
  - Auto Scaling Group multi-AZ
  - Load Balancer multi-AZ

ELB (EC2 Load Balancer):

- Managed Load Balancer (AWS guarantee)
- Costs less when compared to setting up your own load balancer
- Integrated with many AWS offerings/services
- Types:
  - CLB (Classic Load Balancer) v1 old generation – year 2009
    - Supports: HTTP & HTTPS (Layer 7), TCP (Layer 4)
    - Comes with static host name
    - Stickiness configuration done at load balancer level
    - Cross-zone load balancing disabled by default. When enabled, no charge to pay by user
    - Supports **only one SSL certificate**
    - Must use multiple CLB for multiple hostnames with multiple SSL certificates
  - ALB (Application Load Balancer) v2 new generation – year 2016
    - Supports: HTTP, HTTPS, WebSockets
    - Load balancing to multiple HTTP applications across machines (target groups)
    - Load balancing to multiple applications on the same machine (containers)
    - Support for HTTP/2 & WebSocket
    - Support redirects (HTTP to HTTPS)
    - Routing tables to different target groups (EC2 instances/ECS/Lambda/Private IP Addresses)
      - Path in URL
      - Hostname in URL
      - QueryString & Request Headers
    - **Health check is done at target group level**
    - Best fit for micro services & container-based applications
    - To get client IP address/port number/protocol scheme, refer **X-Forwarded-For, X-Forwarded-Port, X-Forwarded-Proto** respectively
    - Comes with static host name
    - Stickiness configuration done at **target group level**
    - Cross-zone load balancing **enabled by default.** No charge to pay by user
    - Supports multiple listeners with multiple SSL certificates. SNI make it to work
  - NLB (Network Load Balancer) v2 new generation – year 2017
    - Supports: TCP, TLS (secure TCP) & UDP
    - Handle millions of requests / second
    - Less latency **~100ms (vs 400ms for ALB)**
    - **Comes with one static IP / EZ and supports assigning Elastic IP (vs CLB or ALB where it is having static host name)**
    - Cross-zone load balancing **disabled by default.** When enabled, **user have to pay charge**
    - Supports multiple listeners with multiple SSL certificates. SNI make it to work
- Setup:
  - Internal (Private within your network)
  - External (Public)
- Troubleshooting
  - 4xx errors → client induced errors
  - 5xx errors → application induced errors
  - Load Balancer error 503 → At capacity or no registered target
  - If LB can’t connect to your application, check your security group
- Monitoring
  - ELB access logs will log all access requests
  - Cloud watch metrics will give you aggregate statistics

- SNI (Server Name Indication)
  - SNI solves the problem of loading multiple SSL certificates onto one web server (to serve multiple websites)
  - Only works **for ALB & NLB, CloudFront**
  - Not supported by CLB
- Connection Draining
  - In CLB it is called Connection Draining
  - In Target Groups (ALB & NLB) it is called Deregistration Delay
  - Default 300 seconds we can configure it between 1 to 3600 seconds (i.e., 1 hr)

Auto Scaling Group:

- Launch template (newer version) allows you to use on-demand and/or spot instances (mixed) whereas Launch configuration allows you to select only one instance type
- A launch configuration or launch templates
  - AMI + Instance Type
  - EC2 User Data
  - EBS Volumes
  - Security Groups
  - SSH Key Pair
- Min / Max / Initial (or) Desired capacity
- Network + Subnet's information
- Load Balancer Information
- Scaling (Out/In) Policies
  - Target tracking scaling
  - Simple / Step scaling
  - Scheduled Actions
  - Rules:
    - Target Avg CPU usage
    - Number of requests on the ELB per instance
    - Avg Network In or Out
- Auto Scaling Alarms
  - It is possible to scale an ASG based on Cloudwatch alarm
  - An alarm monitors a metric (ex: Avg CPU). Metrics computed for overall ASG instances
  - Auto Scaling based on custom metric (ex: number of connected users)
    - EC2 need to send the custom metric data to CloudWatch
  - Auto Scaling based on a schedule (ex: visitor patterns for your website)
- IAM roles assigned to an ASG will get assigned to EC2 instances
- ASG are free. You pay only for the resources launched by ASG
- Cooldown - in ASG, within short time 2 alarms triggered, CPU>70%, space<40%. Actions shouldn't overlap. So, after every action, it waits for cooling time.
- Life cycle hooks: EC2-Pending, In-service, Terminating, Terminated.

Storage

EBS Volumes: (AZ specific & Attached to one instance at a time)

- GP2 (General Purpose SSD) - **Cheap**
  - Recommended for most workloads. System boot volumes. Virtual desktops
  - Low-latency interactive applications. Development and test environment
  - Size: 1 GB to 16 TB. Small GP2 volumes can burst IOPS to 3000. Min IOPS is 100 (even if the size is 1 GB, we'll get 100 IOPS) because max ratio is 3:1 (i.e., 3 IOPS per GB) means 5,334 GB (i.e., 5TB) from 5 TB to 16 TB, we'll get Max IOPS is 16000
- IO1 (Provisioned IOPS SSD) - **Expensive**
  - Critical business applications require sustained IOPS performance or more than 16,000 IOPS (GP2 limit)
  - Best fit for large database workloads (MySQL, Oracle, PostgreSQL, Cassandra, SQL Server, MongoDB)
  - Size: 4 GB to 16 TB. IOPS is Provisioned (PIOPS). Min 100 to max 64000 (for Nitro instances) or otherwise 32000 (other instances)
  - Max ratio for PIOPS per size is 50:1 (i.e., for each GB we'll get 50 IOPS but min is 100 PIOPS)
- ST1 (Throughput Optimized SSD)
  - Streaming workloads requires consistent, fast throughput at a low price
  - Best fit for Big Data, Data Warehouse, Log Processing, Apache Kafka.
  - Cannot be a boot volume
  - Size: 500 GB to 16 TB. Max IOPS 500. Max throughput 500MB/s (baseline: 40MBps per TB)
- SC1 (Cold HDD)
  - Throughput oriented storage for large volume of data that is infrequently accessed
  - Best fit for workloads that requires lowest storage cost is important. Cannot be boot volume
  - Size: 500 GB to 16 TB. Max IOPS 250. Max throughput: 250MB/s (baseline: 12MBps per TB)

EBS Snapshots

- Snapshot is taken only for the blocks that are used.
- Stored in S3 but cannot see them directly
- Best practices: Detach volume from an instance and take snapshot (but other way around is possible)
- Max 1,00,000 snapshots per account
- Can copy across AZ or region. Can make AMI from snapshot.
- Snapshots can be automated using Amazon Data Lifecycle Manager

EBS Instance Store:

- Some instances do not come with Root EBS volumes; instead, they have "instance store" = ephemeral storage
- Instance store is physically attached to the machines (EBS is a network drive)
- **Pros:** Better I/O performance, Good for buffer/cache/scratch data/temporary content, Data survives reboots
- **Cons:** On stop or termination, the instance store is lost, you cannot resize instance store, Backup must be taken care by user

EBS RAID Configurations:

- RAID 0 (a.k.a., Performance):
  - Two or more EBS volumes forms a logical group. Combined will have high IOPS & throughput. At a time, a block of data gets written into one of the actual volumes
  - If one of the volumes fails, the whole logical volume will become unavailable
- RAID 1 (a.k.a., Fault Tolerance)
  - Two or more EBS volumes forms a logical group. Combined will have high IOPS & throughput. At a time, a block of data gets written into all the volumes (fault tolerant)
  - If one of the volumes fails, the logical volume will still be accessible
- RAID 5 (Not recommended)
- RAID 6 (Not recommended)
- RAID 10

EFS:

- Only for Linux instances (POSIX file system)
- Can be accessed by 100s of instances all across AZ
- Encrypt using KMS. Can attach EFS only after EC2 launched. So, use User data to attach EFS.
- 3 times more expensive than EBS. Use EFS-IA to save costs. Use lifecycle policy to move files from EFS to EFS-IA. 7 to 90 days old files
- EFS – We pay for what we use whereas for EBS we pay for the provisioned capacity

S3 (Simple Storage Service)

- Region specific but accessed globally. Max 100 buckets/account. Min size of file 0bytes. Max 3500 PUTS,5500 GETS/s per prefix for a bucket.5TB max size/file.
- No SG, only bucket policy, bucket ACL, object ACL. To access a bucket, user needs an IAM policy for him. HTTP403 - no public access for bucket.
- Object version ID null for objects created before enabling versions. Delete object-adds delete marker. Delete version-permanent delete.
- Security
  - SSE-S3 - AES-256 at rest. Set header x-amz-server-side-encryption.
  - SSE-KMS - AWS manage encryption but have full control over key rotation policy. User level control and audit trail. Customer Master Key (managed by User)
  - SSE-C - Encryption key passed from outside of AWS. Key not stored in AWS. only supported in CLI.
  - Client Side - Encrypt before upload. Decrypt after download. Encryption in console set to none.
- S3 encryption happens at version level of objects. So, few can be turned on/off. Can add bucket policy to deny upload of objects if not encrypted say KMS, or S3.
- S3 Access logs in AuditTrail, API call logs in CloudTrail. CORS Headers needed for apps to access S3 from Cross Origin.
- S3 – Access logs can be stored in another bucket. Analyzed by Athena (data analytics). takes some time to display logs, not immediate.
- S3 - Read after write consistency. Eventual consistency for PUTS and DELETE. No way to make strong consistency.
- S3 -MFA Deletes. Delete a version, turn-off version. can be disabled only by bucket owner, enable MFA only by root. Same from console-Deletes the file, but can’t delete version Gives error.
- Exponential Backoff - limit rate of calls to API. to avoid DDOS.
- S3-Replication-CRR, SRR. CRR-Low latency, HA. SRR-Log Aggregation, live replication, prod to test sync. Both replications are async.
- S3-Replica-After enabling replication, affects only new ones not existing objects. Deletes are not replicated.

- S3-Presigned URL - Used for CLI&SDK. TTL -3600. URLs inherit same role and permission as account generated from.
- S3-StorageClass-Std (Avai-99.99%) S3-IA (Avai-99.9%), S3-1Z-IA (Avai-99.5%) - Durability - 99.119s.
- S3-Glacier-Retrieval-Expedited (1-5mins), Std (3-5hrs), Bulk (5-12hrs). DeepArchive Glacier-STD (12hrs), bulk (48hrs)
- S3-ByteRangeGets-BreakFile into byte-range. Like Get 1st 100lines. S3-Select/GlacierSelect-Filter files, rows, columns on server side.
- S3-EventNotification-trigger event for every action. Event can trigger SQS, SNS, λ. Not Versioned Obj with 2 parallel events might get only 1 event triggered.
- S3-Object-Lock/Vault-Lock-WORK-WriteOnceReadMany. Cant change files once written. Cant delete even by admin.
- Snowball-physical transport few tb to pb. Snowball Edge-physical box with computation capability. Supports cpu, gpu, λ, AMI. Used for precomputation. SnowMobile - 1000-10000PB. Truck can enable encryption. Can't move to glacier, need lifecycle rule to move to Glacier.
- Athena-Data Analytics. Charged/query. Can connect to DB to put results. work on csv, parquet, Avro, json. ELB Logs, VPC AccessLog, CloudTrails all logs processed.

Storage Gateway:

- On-prem to cloud. Caching possible.
- **File:** Mount S3 as NFS on on-prem.
- **Volume** (For EBS) iSCSI protocol.
- **Tape** (for tapes from glacier).
- Install software on on-prem for all 3 to use.

Databases

RDS:

- It is a managed service
  - Automated provisioning & OS patching
  - Continuous backup (automatic) and restore to specific timestamp (Point in Time restore)
    - Daily full backup of the database (during the maintenance window you define)
    - Transaction logs are backed up by RDS every 5 mins (i.e., ability to restore to any point in time (from oldest backup to 5 mins ago)
    - 7 days retention (can be increased to 35 days)
    - DB snapshots are backups that are manually triggered by the user. Retention of such backups as long as you want
  - Monitoring dashboards
  - Read replicas for improved read performance
  - Multi AZ setup for DR
  - Maintenance windows for upgrades
  - Scaling capability (Vertical and Horizontal)
  - Storage backed by EBS (gp2 or io1)
- Cannot do SSH into it underlying instances
- Database Identifier must be unique across the region
- Deploy RDS only in private subnet
- Ports: FTP -21, SSH & SFTP - 22, HTTP - 80, HTTPS - 443, MSSQL - 1433, Oracle - 1521, MySQL & Maria - 3306, Postgres - 5432

RDS Read Replicas vs Multi AZ

- **Read Replicas** (**ASYNC** replication) **- SCALABILITY**
  - Up to **5 read replicas** (within AZ, cross AZ or cross region)
    - Within same AZ, there is no network cost incurred
    - Whereas for cross AZ, there is network cost you need to pay
  - Replication is ASYNC so reads are eventually consistent
  - Replicas can be promoted to their own DB
  - Applications must update the connection string to leverage read replicas
- **Multi AZ** (**SYNC** replication) **– DISASTER RECOVERY**
  - One DNS name will be used by application to connect to DB. Thanks to this DNS, when primary DB goes down, automatic failover takes place to the standby DB
  - Not used for Scaling
- We can very well make use of Read Replicas be setup as Multi AZ for disaster recovery

RDS Encryption

- At rest encryption
  - Possibility to encrypt the master & read replicas with AWS KMS – AES256 encryption
  - Encryption has to be defined at launch time
  - If the master is not encrypted, then read replicas cannot be encrypted
  - Transparent Data Encryption (TDE) available for Oracle & SQL Server
- In-flight encryption
  - SSL certificates to encrypt data to RDS in-flight
  - Provide SSL option with trust certificate when connecting to database
- Encrypting RDS backups
  - Snapshots of un-encrypted RDS databases are un-encrypted

    - Snapshots of encrypted RDS databases are encrypted
    - Can copy a snapshot into an encrypted one
    - When DB is created from encrypted snapshot, DB will be encrypted as well
- Encrypt an un-encrypted RDS database
    - Create a snapshot of the un-encrypted database
    - Copy the snapshot and enable encryption for the snapshot
    - Restore the database from the encrypted snapshot
    - Migrate applications to the new database, delete old database

<u>RDS Network & Security</u>

- IAM Credentials can be used only for MySQL, Postgres.
- IAM Auth token lifetime 15 mins

<u>Aurora</u>

- Can have 15 read replicas. Scales from 10GB up to 64TB. By default, you get 6 instances across 3AZ (including read and write. like 5 read, 1 write. so on).
- Failover in 30 seconds.
- Serverless Aurora - Pay-per-second. Gives 2 endpoints, 1 read endpoint, 1 write endpoint.
- Global Aurora - Cross region read replicas. 1 primary, 5 reads. up to 16 read-replicas. Failover - 1min.

<u>Memcached & Redis</u>

- Memcached vs Redis - MultiNode shard/Cluster, lighter/heavy, cant persist once restart data gone/persist. No backup and restore/redis has.
- Redis Cache can use password login, token for login. SASL auth available only for MemCached.

Virtual Private Cloud (VPC): - Virtual data centers in the Cloud

- Launch instances into a subnet of your choosing
- Assign custom IP address ranges in each subnet
- Configure route tables between subnets (Route tables allows which subnet can speak to which subnets)
- Create internet gateway and attach it to our VPC (**Only one internet gateway allowed per VPC**)
- Much better security control over your AWS resources
- Instance security groups (**Security groups can span AZ**). Security groups can span multiple subnets as well.
- Subnet network access control lists (NACLs)
- Default VPC vs Custom VPC
  - Default VPC is user friendly. Allowing you to deploy instances.
  - All subnets in default VPC have a route out to the internet. You cannot have private subnets in default VPC
  - Each EC2 instance has both a public and private IP Addresses **(When in case of custom VPC and if you have a private subnet, you won't get public IP Addresses)**
- You can have maximum (soft limit) of 5 VPCs in a region (However you can write to AWS in case if you need more than 5 VPCs)
- VPC Peering
  - Allows you to connect one VPC with another via a direct network route using private IP Addresses
  - Instances behave as if they were on the same private network
  - You can peer VPC's with other AWS accounts as well as with other VPCs in the same account
  - Peering is in a star configuration: i.e., 1 central VPC peers with 4 others (**NO TRANSITIVE PEERING**)

Exam Tips:

- Think of a VPC as a logical datacenter in AWS
- Consists of IGWs (or Virtual Private Gateways), Route Tables, Network Access Control Lists, Subnets and Security Groups
- 1 Subnet = 1 Availability Zone
- Security Groups are stateful whereas Network Access Control Lists are stateless
  - It means, when you open Port 80 under Security Group, both in-bound and out-bound are allowed by default
  - Whereas in NACLs, you need to explicitly open in-bound and out-bound rule lists
- No Transitive Peering
- When you create a new VPC, the following will be created automatically by AWS
  - Route Tables
  - NACLs
  - Security Group **(Security Groups don't span different VPCs)**
  - No subnet will be created. No internet gateway will be created
- When you create custom subnet for your custom VPC, not all requested IP addresses available for you. 5 IP addresses are taken by AWS
  - x.x.x.0 → Network Address
  - x.x.x.1 → Reserved by AWS for the VPC router
  - x.x.x.2 → Reserved by AWS

    - x.x.x.3 → Reserved by AWS for future use
    - x.x.x.255 → Network broadcast address. AWS doesn't support broadcast in a VPC.
- When you're going to create your own Internet Gateway, by default, its not attached to any of your VPC. You can't have more than one Internet Gateway.
- **Security Groups don't span VPC**
- When you create your own subnet by default it will be associated to main route table.
- When you create your own subnet, the CIDR range must be between (x.x.x.x/16 to x.x.x.x/28)
- How to give internet access to a subnet?
    - Create internet gateway
    - Attach it to a VPC
    - Create a route table
        - After creating the route table, go to "Routes" tab, add 0.0.0.0/0 (IPv4), ::/0 (IPv6) and specify Target as the internet gateway you've created
    - By default, all subnets associated with this route tables/VPC are given internet access. And those subnets will become public subnets
- NAT Instances:
    - NAT Instances can get from Community AMIs.
    - Each EC2 instance performs source/destination checks by default. It means, that the instance must be the source or destination of any traffic it sends or receives. However, a NAT instance must be able to send and receive traffic when the source or destination is not itself. **Therefore, you must disable source/destination checks on the NAT instance**.
    - NAT instance must be in a public subnet
    - There must be a route out of the private subnet to the NAT instance, in order for this to work
    - The amount of traffic that NAT instances can support depends on the instance size. If you are bottlenecking, increase the instance size. For production environment, better go for higher bandwidth. T2Micro may not be a right choice.
    - You can create high availability using Autoscaling Groups, multiple subnets in different AZs, and a script to automate failover.
    - NAT instances must be kept behind a Security Group.
- NAT Gateways (IPv4)/Egress Only Internet Gateways (IPv6)
    - Preferred by enterprises
    - Scale automatically up to 10 Gbps
    - No need to patch
    - Not associated with security groups
    - Automatically assigned a public ip address. Remember AWS take 10/15 minutes to create.
    - Remember to update route tables. Having 1 NAT Gateway in 1 AZ is not good enough.
    - No need to disable Source/Destination checks
    - More secure than a NAT instance.

- NACLs vs Security Groups
    - Subnets can be associated with **only one** NACLs.
    - Your VPC automatically comes with a default NACL, and by default it allows all inbound and outbound traffic.
    - You can create custom NACL. By default, inbound and outbound traffic is denied until you add rules.
    - Each subnet in your VPC must be associated with a NACL. If you don't explicitly associate a subnet with a NACL, the subnet is automatically associated with a default NACL.

    - You can associate a NACL with multiple subnets; however, a subnet can be associated with only one NACL at a time. When you associate a NACL with a subnet, the previous association for that subnet is removed.
    - NACL can span multiple AZ whereas subnets cannot.
    - NACLs contain a numbered list of rules that is evaluated in order, starting with lowest numbered rule
    - NACLs have separate inbound and outbound rules, and each rule can either allow or deny traffic
    - NACLs are stateless; responses to allowed inbound rules are subject to the rules for outbound traffic (and vice versa)
    - You can block IP addresses using NACLs **but cannot be done using Security Groups**
- Elastic Load Balancers & VPC
    - You can create ELB under custom VPC. **But you must specify 2 public facing subnets from two different availability zone in order to setup your ELB.**
- VPC Flow Log
    - VPC flow logs is a feature that enables you to capture information about IP traffic going to and from network interfaces in your VPC.
    - Flow log data is stored using Amazon CloudWatch logs.
    - After you've created a flow log, you can view and retrieve its data in Amazon CloudWatch logs
    - Flow logs can be created at 3 levels
        - VPC
        - Subnet
        - Network interface level
    - You cannot enable flow logs for VPCs that are peered with your VPC unless the peer VPC is in your account
    - You cannot tag a flow log
    - After you've created a flow log, you cannot change its configuration; for example, you can't associate a different IAM role with the flow log
    - Not all IP traffic is monitored; The following scenarios are not monitored
        - Traffic generated by instances when they contact the Amazon DNS Server. If you use your own DNS server, then all traffic to that DNS server is logged
        - Traffic generated by a Windows instance for Amazon Windows license activation
        - Traffic to and from 169.254.169.254 for instance metadata
        - DHCP traffic
        - Traffic to the reserved IP address for the default VPC router
- NAT vs Baston Service
    - A NAT instance is used to provide internet traffic to EC2 instances in private subnets
    - A Bastion instance is used to securely administer EC2 instances (using SSH or RDP) in private subnets. In Australia we call them jump boxes.
- VPC End Points
    - 2 kinds of VPC endpoints
        - Interface Endpoint is an Elastic Network Interfaces (ENI) that serves as an entry point for traffic destined to the service
        - Gateway Endpoint serves as a target for a route in your route table for traffic destined for the service

CIDR (Classless Inter-Domain Routing)

- You cannot specify an IPv4 CIDR block larger than /16.
- You can optionally associate an Amazon provided IPv6 CIDR block with the VPC

- Example CIDR address: 10.0.0.0/16

Other Services

- Route53 - Max - 50 DNS Names allowed for an account. For more contact AWS.
- Route53 - Route Types - A-IPv4, AAAA-IPv6, CNAME-only Subdomain not root. Hostname to hostname. Alias-AWSResource same or other account. Both root and sub domain but only AWS.
- Route53 - Costs 0.5$/month. Buy Domain - 12$/year. TTL - 60s - 34hr. Default 300s.
- AWS EC2 Metadata: http://169.254.169.254/latest.meta-data
- AWS SDK - Default region us-east-1. But can specify region. Needed SDK for λ or DynamoDB.
- SDK Auth - Credential provider chain. AWS configure. IAM roles for EC2. AWS_ACCESS_KEY_ID, AWS_SECRET_ACCESS_KEY (env var, not recommended).
- FSx for windows - No EFS for windows so use this. Support AD,NFS for windows. Access from On-prem (need hardware).
- FSx for Luster - Linux+Cluster. Support ML, HighPerfComputing. Write to S3. Increase IOPs within Cluster. Video processing. Can connect to on-prem (need Hardware).
- Cloudfront-CDN. Lies in edge location. Protects from DDoS. Integrates with Shield, WAF, Macie (ML). Can process HTTPS for external world, but HTTP for internal backends.
- OAI-OriginAccessIdentifier-IAM Role attached to S3, EC2, ALB then that service accessible only via Cloudfront, not directly. Enhanced Security.
- GeoRestiction-White/blacklist country. Country found by 3rdparty GeoIP DB. CloudFront can cache dynamic content-update with underlying copy. Has TTL.
- CloudFront SignedURL/SignedCookies-Generate using SDK. Can get content from anywhere S3, etc. URL-1 URL/file. Cookies-1 URL/multiple files.
- CloudFront SignedURL vs S3Signed. All AWS/only S3. Account wide URL, managed by root/only permission of account generated from. Can use cache/can't. Filter by IP, Path, Date, Expiration/Exp set.
- GlobalAccelerator-GlobalPaidSvc not under CloudFront separate service. App deployed in 1region, make available whole world. Low latency. Route via AWS network from US CloudFront to INDIA.
- GlobalAccelerator -Unicast/Anycast IP: 1 Server 1 IP/Multiple server same IP. Picked server by low latency. Support EC2, ALB, NLB, Elastic IP, Public, Private IP. HealthChecks.
- GlobalAccelerator vs CloudFront: Both use EdgeLocation, Integrate with Shield, WAF, DDoS protection. Improve performance by caching both dynamic & static content/just proxy. Good for HTTP/for UDP, IoT.
- SQS-Decoupling. Retention after consumed-min/max/default: 1min/14days/4days. Max256kb. No ordering maintained. Atleast (not max) 1 delivery. Once consumed, delete message by consumer. Aauto-scale.
- SQS-Encryption inflight. Can use client side encrypt. At rest KMS. SQS Access policy like bucket Policy. ACL based on IAM. Message Visibility Time-Once consumed after this time, if not deleted, msg shows in queue. Min/Max/Default: 1s/12D/30s
- DeadLetter Queue-Failed processing msg, can move here after failure threshold. Delay Queue: Delay msg showing up in Queue, so consumers don't see it yet. Min/Default: 0s/15m.
- Long/Short Polling: Short returns empty for consumer if Queue empty. Long waits for msg to show up in Queue even empty.
- SQS-FIFO: Ordering guarantee. Exactly consume once. Limited throughput-300rec/s. Batch mode 3000rec/s. Queue Name should end with .fifo. like kafka consumerGrp,msg GroupID. But no partition, create 100 grpID and have 100consumers.
- SNS-Topic, pub/sub. Subs can add filter pattern to choose msg.100k SNS/Account. Subs can be SQS (called fanout), λ, SNS, HTTP. Producer can be CloudWatch, ASG, S3, Cloudformation.
- Kinesis-Alternative for Kafka (shards~partition). Data automatically replicated in 3 AZ. Support ETL, Spark, Bigdata, NiFi. Low Latency Streaming. Add shard to scaleup.

- KinesisStream-retention-1 to 7days. Same shard can have multiple consumer. Ability to replay. Can’t delete explicitly unlike SQS. 1000msg/s. ProvisionedThroughputExceeded.
- KCL-Kiniesis Client Lib-Java/Python. Uses DynamoDB to track offsets.
- KinesisFirehose: Load stream into S3, Redshift, ELK, Splunk. KinesisAnalytics: Run Analytics on KinesisStream, Firehose.
- AmazonMQ: MQTT. Runs on dedicated machine. Both Queue and Topic supported. Provides separate endpoint for ports: MQTT, STOMP,AMQP,WSS.
- API Gateway - Create rest API on top of λs.
- λ - Memory 128mb-3GB. Max exec time -15min. Environment variables size - 4kb. Disk capacity - 512MB. Concurrent Execution-1000. Code archive size (Jar/war) - 50mb. Uncompressed-250mb.
- λ@Edge: Run λ in CloudFront. Can choose request to process by λ. Can return flat responses from λ. Can tap req/responses and modify them.
- DynamoDB: NoSQL, Serverless, 3 AZ replication, Millions of req/sec. 100sTB of storage. Has primary key can query only on PK. IAM Integration. Max size of row 400KB (Key+val). Has List, Map datasets.
- DynamoDB: 1RCU 4kb/s ($0.00013). 1WCU 1kb/s ($0.00065/WCU). Add any num of WCU/RCU per need. ProvisionedThrougputExceededException->ASG->Add WCU/RCU. Can use burst credits.
- DAX: Caching. Speeds up Reads. write-through Cache->writes go through DAX. HotKeyProb solved (too many reads on 1 val). TTL-5min. latency ms. Cross Region Replication available, but Streams must be enabled as ChangeLogs are used for replication.
- DynamoStream: Like trail. Every operation gets logged to stream. Can add λ to process logs. Feed to ELK. Logging speed: 2 to 10 rows or 4MB of data/sec. VPC Endpoint for on-prem. IAM, KMS. SSL. Backup/Restore available. Has MigrationTool from other NoSql, SQL, S3.
- APIGateway-Create REST endpoints. Use with λ. Can cache responses. Expose ALB. Create websockets. APIVersioning, Req throttling, Security (authentication &authorization), SwaggerAPI, Test/validate req/resp. Expose any AWS Service.
- APIGateway Endpoints: 1. EdgeOptimized-Global clients, but API Gateway deployed in 1 Region only. 2.Regional-Works 1 region. Can work with CloudFrong. 3.Private-for VPC Endpoints.
- API Gateway: Sigv4 Headers with IAM Credential Signatures. λ authorizer-run λ to validate sign/token using SAML/OATH/IAM Policy.
- API Gateway with Cognito, but only authenticate not authorize. Implement backend for authorize. Can use Google, FB login. Authenticate and issue token. Attach Token to req header and hit λ. Consecutive hits, checks validity of token at API GW.
- Cognito: 1. User Pools-Create simple Login/Multi Factor Authentication. JSON Web Token - generate & validate token. Use Google/FB login. 2. Identity pools-Federated Integrity pool. Can use token from user pools. AWS credentials authentication. Provide temp access to S3 using FB login. 3.Cognito Sync: Sync data from device to Cognito. Deprecated. works Offline. Uses FIP. Replaced by AppSync.
- SAM: Serverless App Model. Framework for developing Serverless app. Only YML config. Can config λ, DynamoDB, API Gateway, Cognito User Pools. Can use CodeDeploy to deploy λ functions.
- DB: RDS, Aurora-great for joins. Nosql-Elastic Search, DynamoDB, Neptune. DataWarehousing - SQLAnalytics, BI. RedShift, Athena. Neptune-Graphs. Display Relationship between data. Social Networking, Wikipedia.
- OLAP: Redshift. OLTP: ANY RDS.
- RDS: Must provide an EC2, EBS Volume (including Aurora). For 1AZ instance, taking snapshot, I/O may be suspended for few Seconds also elevated latency. For any error during API Call, check ERROR Node in response.

- RDS: Doesn't auto-scale (instead Go for aurora serverless). Scaling Read replicas, need manual intervention and code change. Provisioned IOPS with MSSQL has 16TB capacity. Changes to Backup window, take effect immediately.
- ElastiCache: Redis/Memcached. In memory datastore. SubMillisecond Latency. Redis Support cluster. KMS, Security Group, IAM policy (not authentication), RedisAuth. Monitor in Cloudwatch. Backup, restore. Can store user session data.
- Athena: Serverless, Interactive query service and data analytics on S3 only, logs, can output back to S3. IAM+S3 security. Uses Presto engine.
- RedShift: Not serverless. Underneath PostgreSQL. But OLAP enhanced. DataWarehousing-SQLAnalytics, BI tools - AWS QuickSight, tableau. Redshift Spectrum (Serverless)- run against S3.
- RedShift Backup every 8 hours. or every 5GB. Supports cluster. Manual retention-snapshot retained until manual delete.
- Redshift Spectrum vs Athena: Both does data warehousing, serverless. but cluster not possible in Athena. So can manage performance.
- Cloudwatch: Global, Serverless, Free (standard).10 Dimension (i.e., Metric). Memory Metric not captured by default, do custom metric. EC2 gets /5 mins. Detailed Monitoring(Paid)-/1min.
- Cloudwatch: Standard metric (metric -/5min. alarm-/1min), HighResolution Custom metric (metric-/1sec. alarm-/10sec). 3 dashboard, 50Metric free. After that $3/month/dashboard. Collect log from VPC, λ ,API Gateway, Route53, EC2, Beanstalk, Cloudtrail. Custom Metric for RAM, Swap space, Processes, Netstat.
- Cloudwatch Logs: By default LOGS (not metrics) are not sent from EC2. Add Cloudwatch Unified Agent in EC2, add CloudWatchLogsFullAccess permission. On-prem also agent can be installed.
- Cloudwatch Alarms: State: OK, Insufficient_Data, Alarm. HighResolutionCustomMetric-trigger alarm within 10-30sec, capture metric every second. Using alarm, if there is system failure on EC2, we can initiate/run system recovery steps.
- Cloudwatch Event: Event target can be λ, Cron, SQS, SNS, Pipeline (every push/commit), Stepfunctions etc.
- Cloudtrail: provide governance, compliance, audit of AWS account. Enabled by default. capture events, API calls made. Resource is deleted, check cloudtrail first. No matter originated from SDK, CLI, console.
- AWS Config: Record config changes over time. Can push to S3/Athena. Do S3 buckets have public access?, is SSH unrestricted from EC2? How ALB Config changed over time. - provides answers to such questions.
- AWS Config (Paid): Receive alerts from config changes. alerts can be pushed to SNS.75 ready-to-use config rules available. Custom rule-create λ. Reactive not preventive. $2/rule/month.
- IAM: STS TTL 15min-1hr. Cross account = STS. AssumeRole: AssumeRoleWithSAML(SAML)-Integrate with AD, AssumeRoleWithWebIdentity (fb login) get temp AWS credentials with IAM Role, GetSessionToken (MFA), AssumeRoleAPI (SDK), SSO (Non-SAML login once in AWS Console, get token, use token to access all AWS Resource),
- AWS Directory Service: AWS Managed MS AD. Can work with on-premise AD by AD Connecter.
- AWS Organization: Global service. Main account is Master. Others are member account. Member can be in 1 Org only. Consolidate billing across account - single payment. Pricing benefits from aggregation usage. Use tagging for billing purposes.
- AWS Organization: Master account -> multiple OU (Finance, Sales) -> Accounts (SalesAcc1, SalesAcc2) -> Members. OU can have multiple OU under it. Move Account across OU. remove member from OU, send invite to new OU, accept invite from new OU.
- ServiceControlPolicy (SCP) works only with Orgs-applied at OU level can't apply to master. SCP Doesn't allow anything by default. Restrict access to certain service using SCP-λ, EMR. Permission inherited from parent. Even though explicitly deny in child won't affect, if parent allowed. Root acc will have FullAWSAccess SCP Policy attached.

- AWS Conditions: Whitelist IPs for API Calls and create IAM policy. Whitelist region. Restrict access based on tags. If specific tag missing, don't allow stop/start EC2.Or Force MFA for stop/start.
- IAM For S3: Provide access to bucket 2 ways. Create role attach policy for that role to access S3. Create bucket policy and allow access to that account. Bucket policy is better, since assume role access will be only as per role. but bucket policy is additional role.
- IAM Permission Boundaries: Only for roles, users. Not groups. Set permission boundary as access S3. even though user is admin can't access anything other than S3.
- Evaluation: Policy (IAM/S3), SCP, Permission Boundary, Session Policy (STS), Identity Based Policy are intersection. If allowed (or not denied in other 4) in all 5, then can only access.
- AWS RAM: Resource Access Manger - share AWS resources with other account, within or outside Org. Help to avoid resource duplication.
- Cognito: Allow users to their own space under S3. Cognito helps in that.
- KMS: Provided by AWS and free. Symmetric (AES-256) single encryption. Asymmetric (RSA & ECC Pair) Public key/private key combo. can create and import keys/per region from outside- $1/month+3cents per 10k API calls. Only Symmetric supported. encrypt 4kb per call.>4kb use envelope encryption.
- SSM Param Store: Secure storage for config and secret. optional, Serverless sdk. GetParameters, GetParameterByPath API Call from SDK. Standard-10k params free. 1 param 4kb max. ADV-100k, 8kb per param. Can use TTL to delete params. Param can be string, stringlist, SecureString (Password)
- AWS Secret Manger: Only for storing secret. Rotation policy can be defined. Integrate with RDS. Encrypted by KMS.
- CloudHSM- Alternate for KMS. Paid. Can manage, support multi-AZ, both symmetric/asymmetric. can use with SSE-C.
- AWS Shield-DDoS protection. Standard-free, Enabled by default for all. Protect from layer 3,4(TCP) attack. ADV-$3000/Month/Organization. If req spike because of attack, fee waived. 24h support.
- WAF: Layer 7 (HTTP) protection. Protect SQLInjection, XSS.Define web ACL-IPAddress, URI, HTTPHeader check, GEO Match restriction. Rate based rule. eg:1 IP can make 5 req/sec.

Cognito User Pools vs Identity Pools:

- A user pool is a directory in Amazon Cognito. With a user pool, users can sign-in to your web or mobile app through Amazon Cognito or federate through a third-party identity provider. Whether your users sign-in directly or through a third party, all members of the user pool have a directory profile that you can access through a SDK
- With identity pool, users can obtain temporary AWS credentials to access AWS services, such as Amazon S3 or DynamoDB.

AWS Global Accelerator:

- It is a networking service that helps to improve the availability and performance of the applications that you offer to your global users.
- It provides a Static IP addresses that provide a fixed entry point to your applications to eliminate the complexity of managing specific IP addresses for different AWS regions and AZ
- Routes user traffic to optimal endpoint based on performance, user's location
- Good fit for non-HTTP use cases such as gaming (UDP), IoT (MQTT) or VOIP