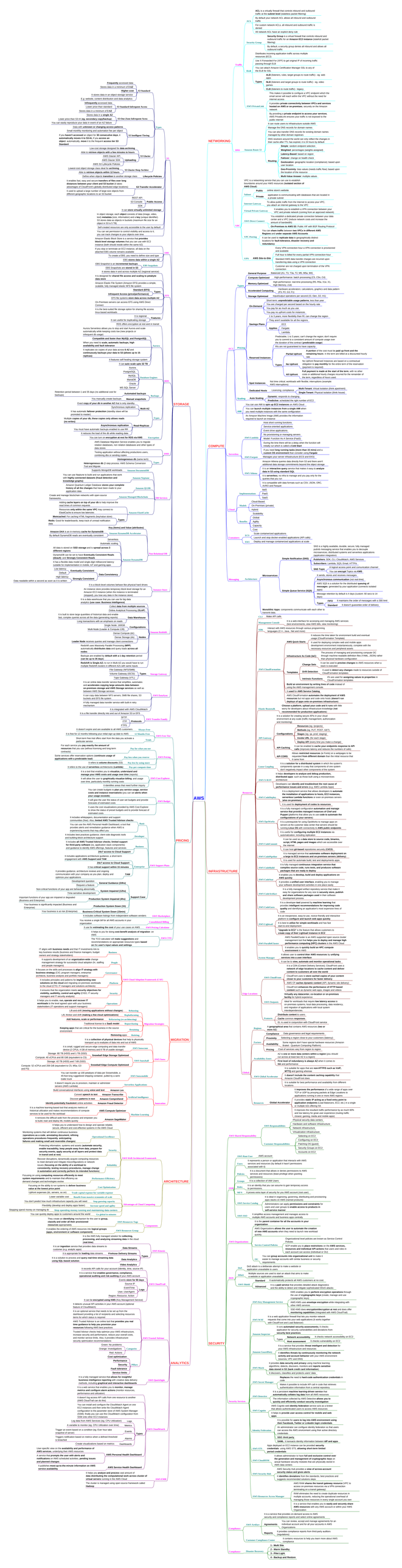
AWS
NETWORKING
ACL
ACL is a virtually firewall that controls inbound and outbound traffic at the subnet level (stateless packet filtering)
By default your network ACL allows all inbound and outbound traffic
For custom network ACL is all inbound and outbound traffic is denied
All network ACL have an explicit deny rule
Security Group
Security Group is a virtual firewall that controls inbound and outbound traffic for an Amazon EC2 instance (stateful packet filtering)
By default, a security group denies all inbound and allows all outbound traffic
Distributes incoming application traffic across multiple instances (EC2)
Use it Forwarded For (XFF) to get original IP of incoming traffic (client IP address)
You can attach Amazon Certification Manager SSL to any of the ELB: SSL
ALB (listeners, rules, target groups to route traffic) - eg. web apps
Types
NLB (listeners and target groups to route traffic) - eg. video streaming
CLB (listeners to route traffic) - legacy
This makes it possible to configure a VPC endpoint which the virtual server will reach within the VPC without the need for internet access
VPC Peering
It provides private connectivity between VPCs and services hosted in AWS or on-premises, securely on the Amazon network
By providing a private endpoint to access your services, AWS PrivateLink ensures your traffic is not exposed to the public internet
Allows users to infrastructure outside AWS
Manage the DNS records for domain names
You can also transfer DNS records for existing domain names registered in other domain registrars
DNS resolvers around the world can only reflect the changes in their cache after TTL has expired, it is 24 hours by default
Simple: sender endpoint selection
Weighted: percentages (weights assigned)
Latency-Based: based on region
Failover: change on health checks
Routing
Geolocation: geographic location (compliance); based upon the location of the resource
Multi-Value Answer: multiple values
VPC is a networking service that you can use to establish private cloud within AWS resources (isolated section of AWS Cloud)
Subnet
Public
online store's website
application is communicating with databases that are located in a private subnet
Internet Gateway
To allow public traffic from the Internet to access your VPC, you attach an Internet gateway to the VPC
Virtual Private Gateway
Establishes a secure VPN connection between your VPC and private network (coming from an approved network)
VPN Direct Connect
You establish a dedicated private connection between your data center and a VPC (reduce network costs and increase bandwidth throughput)
On-Premises to AWS S3: Public VIF with BGP Routing Protocol
You can share traffic between two VPCs in different AWS accounts using VPC Peering connections
VPC Peering
It can be used to replicate data to geographically distant locations for fault-tolerance, disaster recovery and redundancy
VPN
Every VPN connection-hour a VPN connection is provisioned and available
Full hour is billed for every partial VPN connection-hour
Standard VPN data transfer charges are incurred upon transferring data using a VPN connection
Customer are not charged upon termination of the VPN connection
STORAGE
S3
General Purpose
Frequently accessed data
Store data in a minimum of 3 AZ
Higher cost
S3 Standard
It stores data in an object storage service
E.g. website, content distribution and data analytics
Infrequently accessed data
Lower price than standard
Store data in a minimum of 3 AZ
Lower cost than standard
S3 Standard-Infrequent Access
One-Zone Infrequent Access
Lower price than S3 or the one accessing unpredictable
S3 Intelligent-Tiering
You can easily repurpose your data in event of an AZ failure
Glacier
Data archiving
Small monthly monitoring and automation fee per object
If you haven't accessed an object for 30 days, it automatically moves it to S3-IA, if you access an object 2 consecutive times it is the next access to S3 Standard
S3 Glacier Deep Archive
Low-cost storage designed for data archiving
Able to retrieve objects within a few minutes to hours
S3 Glacier
AWS Glacier API
Uploading
AWS S3 Lifecycle Policies
Lowest-cost object storage class ideal for archiving
Able to retrieve objects within 12 hours
S3 Glacier Deep Archive
Define when objects transition to another storage class
Lifecycle Policies
It enables fast, easy and secure transfers of files over long distances between your client and an S3 bucket
Transfer Acceleration
advantages of Cloudfront's globally distributed edge locations
S3 Transfer Acceleration
It used to upload a large number of large files over different geographic locations in an S3 bucket
EBS
RESTAPI
EBS Snapshot
Public Access
SDK
Private Access
It can store virtually unlimited storage
In object storage, each object consists of data (image, video, text document), a key (unique identifier for the object), and metadata (S3 stores data as objects in buckets (maximum file size for an object is 5 to 5 TB)
Read-created resources are only accessible to the user by default
You can set permissions to control visibility and access to it, using S3 bucket policies and S3 access lists
Amazon Elastic Block Store (EBS)
Types
SSD
HDD
Provisioned IOPS
General Purpose
Magnetic
block-level storage volumes that you can use with EC2 instance (both should reside within the same AZ)
If you stop or terminate an EC2 instance, all data on the attached EBS volume remains unaffected
To create a EBS volume, you must specify its size, volume type and region
EBS Snapshots
It can be used to create new EBS volumes or store data within a single AZ
EBS Snapshots
EBS Snapshots are stored in S3
It stores data in and across multiple AZ (regional service)
Amazon Elastic File System (Amazon EFS)
Types
Standard (EFS)
Infrequent Access (EFS IA)
It is designed for shared file access and scaling to petabyte data store
Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system
Amazon Elastic File System (Amazon EFS) provides multi-AZ resilience and high throughput
Amazon Elastic File System (Amazon EFS) provides multi-AZ resilience and high throughput
Amazon Elastic File System (Amazon EFS) provides multi-AZ resilience and high throughput
Amazon Elastic File System (Amazon EFS) provides multi-AZ resilience and high throughput
Amazon Elastic File System (Amazon EFS) provides multi-AZ resilience and high throughput
EFS file system access from multiple AZ
EFS file system access from multiple AZ
EFS file system access from multiple AZ