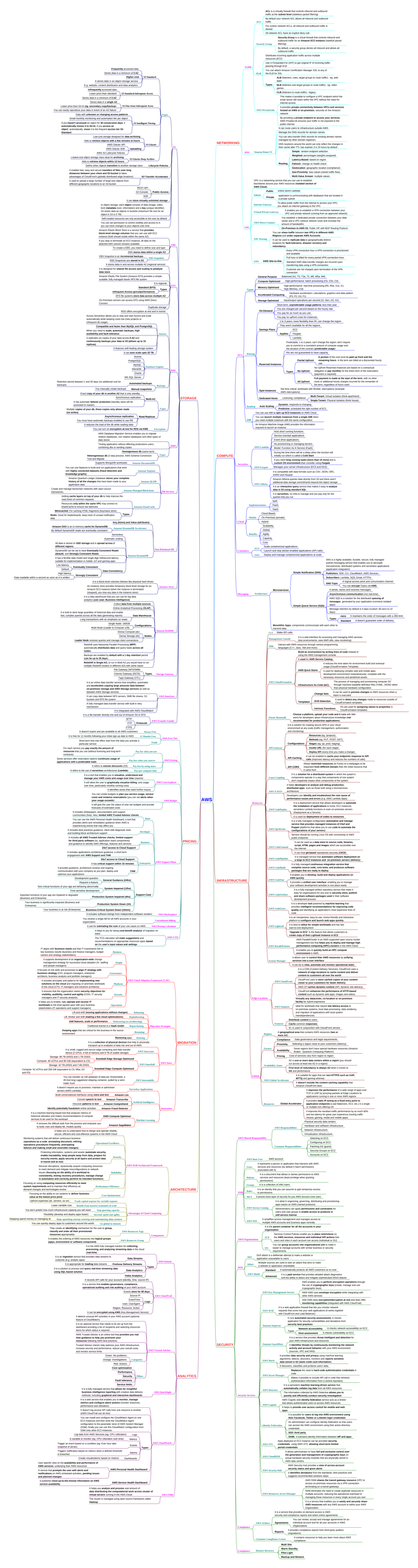
AWS
NETWORKING
VPC
ACL is a virtually firewall that controls inbound and outbound traffic at the subnet level (stateless packet filtering)
By default your network ACL allows all inbound and outbound traffic
For custom network ACLs, all inbound and outbound traffic is blocked
All network ACL have an explicit deny rule
ACL
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
Traffic
Distributes incoming application traffic across multiple targets (EC2)
ELB
Use X-Forwarded-For (XFF) to get original IP of incoming traffic passing through ELB
You can attach Amazon Certification Manager SSL to any of the ELB for SSL
Types
ALB (layers, rules, target groups to route traffic) - eg: web apps
NLB (listeners and target groups to route traffic) - eg: video games
CLB (listeners to route traffic) - legacy
This makes it possible to configure a VPC endpoint which the overall service will make within the VPC without the need for internet access
AWS PrivateLink
Enables connectivity between VPCs and services hosted on AWS or on-premises, security 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
It can route users to infrastructure outside AWS
Manage the DNS records for domain names
You can also transfer DNS records for existing domain names to Amazon Route 53 without downtime
DNS
DNS resolvers around the world can only reflect the changes in their cache after TTL has expired, it is 24 hours by default
Amazon Route 53
Simple - random endpoint selection
Weighted - percentages (weights assigned)
Latency-Based - based on region
Routing
Failover - change on health check
Geolocation - geographic location (compliance)
Geo-Proximity - bias values (needs traffic flow)
Multi-Value Answer - multiple values
VPC is a networking service that you can use to establish boundaries around your AWS resources **isolated section of AWS Cloud**
Public
online store's website
Subnet
Private
application is communicating with databases that are located in a private subnet
To allow public traffic from the internet to access your VPC, you attach an internet gateway to the VPC
Internet Gateway
It enables you to establish a VPN connection between your VPC and private network (coming from an approved network)
Virtual Private Gateway
Provides a dedicated network connection between your network and a VPC (reduce network costs and increase the amount of bandwidth)
Direct Connect
VPC
On-Premises to AWS SS Public VIP with BGP Routing Protocol
You can **share traffic** between **two VPCs in different AWS accounts** and **within separate AWS Accounts**
VPC Peering
It can be used to **replicate data** to geographically distinct regions for **high-bandwidth, disaster recovery and redundancy**
Every VPN connection-hour a VPN connection is provisioned and available
VPN
Full hour is billed for every partial VPN connection-hour
VPN
AWS Site-to-Site
Standard AWS data transfer charges are incurred upon transferring data using a VPN connection
Customer are not charged upon termination of the VPN connection
STORAGE
S3
Relational (A1, T3, T3a, T2, M5, M5a, M4)
Compute Optimized
High-performance batch processing (C5, C5n, C4)
Types
Memory Optimized
High-performance real-time processing (R5b, X1e, X1, High Memory, z1d)
Accelerated Computing
Hardware accelerators: calculations, graphics and data pattern (P3, P2, G3, F1)
Storage Optimized
Input/output operations per second (D3, D2e, I3, I2)
EC2
Pricing
On-Demand
You pay for as much as you use
You pay no upfront costs for instances
Pay-as-you-go, more flexibility than RI, can change the region
Savings Plans
EC2
Applies
Fargate
Lambda
Predictable: 1 to 3 years, can change the region; don't require a specific type of instance; can change the instance size; the duration of the contract **profoundly** saves
Reserved Instances
RIs are not guaranteed to have capacity
Term
A portion of the cost must be **paid up front and the remaining hours** in the term are billed at a discounted hourly rate
Partial Upfront
Types
No Upfront
No Upfront Reserved Instances are based on a contracted monthly billing for the duration for the entire term of the reservation (payment is deferred)
Full payment is made at the start of the term, with no other costs or additional hourly charges incurred for the remainder of the term, regardless of hours used
Spot Instances
Not time critical; workloads with flexible; interruptions (example batch interruptions)
Multi-Tenant Virtual Isolation (think apartment)
Single-Tenant: Physical isolation (think house)
Scaling
Auto Scaling
Dynamic: responds to changing
Predictive: scheduled the right number of EC2
You can use AWS to **spin up EC2 instances** on AWS Cloud
AMI
You can **launch multiple instances from a single AMI** when you need multiple instances with the same configuration
An Amazon Machine Image (AMI) provides the information required to launch an instance
COMPUTE
Hosted
Hosted shared web functions
Service-oriented applications
Event driven applications
AWS Lambda
No provisioning or managing servers
Model: Function As A Service (FaaS)
During the time there will be a delay when the function will initially be invoked (**cold start**)
Serverless
If you need long running **scaling (more than 15 mins)** and a **custom OS environment** then consider using **Fargate**
AWS Fargate
Manages your server infrastructure (EC2 and ECS)
It is compatible with data formats such as CSV, JSON, ORC, Avro and Parquet
AWS Athena
Amazon Athena queries data directly from S3 and there aren't additional data storage commitments beyond the storage charge
It is an **interactive query service** that makes it easy to **analyze data in Amazon S3 using standard SQL**
Athena is a serverless service to manage and you pay only for the queries that you run
Cloud
Implementation
PaaS
SaaS
Cloud-Based
Model
On-Premises (private)
Hybrid
Scalability
Global
Agility
Capacity
Elasticity
Lightsail
Scale containerized applications
Containers
EKS
Deploy and manage containerized applications at scale
ECS
Launch and stop docker enabled applications (API calls)
Microservices
Architecture
Simple Notification (SNS)
SNS is a highly available, durable, secure, fully managed pubsub messaging service that enables you to decouple microservices, distributed systems and serverless applications (application integration)
Publishers: SDK, CLI, CloudWatch, AWS Services
Subscribers: Lambda, SQS, Email, HTTPs
SNS Topic
A logical access point and communication channel
Simple Queue Service (SQS)
You can **encrypt** Topics via **KMS**
It sends, stores and receives messages
Asynchronous communication (not real time)
AWS SQS is a solution for the distributed **queuing of messages** generated by your application (consumer) hosted on EC2
Message retention by default is 4 days (custom: 60 secs to 14 days)
Types
FIFO
It maintains the order of messages with a 300 tmit
Standard
It doesn't guarantee order of delivery
Monolithic App: components communicate with each other to operate data.
CLI
Make API calls
Management Console
It is a web interface for accessing and managing AWS services (test environments, view AWS bills, view monitoring)
Programmatic Tools
Interact with AWS resources through various programming languages (C++, Java, PHP, Python, Ruby, .Net)
AWS Cloudformation
It automatically provisions and configures resources on **on-premises storage and AWS Storage services** as well as between AWS Storage services
It can copy data between NFS servers, SMB file shares, S3 buckets and EFS file system
A fully managed data transfer service with built-in retry mechanism
It is integrated with AWS CloudWatch
It is a file transfer directly into and out of Amazon S3 or EFS
Elastic Beanstalk
Storage Gateway
Types
File Gateway (NFS)
Volume Gateway (iSCSI)
Tape Gateway (VTL)
Storage Gateway
Protocols
SFTP
FTP
FTPS
Amazon Snowball
It is a solution for a **distributed system** in which the data components operate in a way that components of one system dont depend impact other components of the system
It helps **developers to analyze and debug production, distributed apps** such as those built using a microservices architecture
Resources
Developers can **identify and troubleshoot the root cause of performance issues** using AWS Lambda logs
It is a deployment service that allows developers to **automate software deployments** to a variety of compute or AWS services: serverless Lambda functions or even on-premises servers (Deployment as a Service)
It can be **deployed of codes to resources**
It is a fully managed configuration **automation and manage service that provides managed instances of Chef and Puppet** (platforms that allow you to use **code to automate the configurations of your servers**)
Servers should be running one of the supported Windows or AWS public endpoints
It can be used as a **data store to source code, binaries, scripts, HTML pages and images** which are accessible over the internet
It can have **pre-based** repositories security (IDE/IDE)
It is a fully managed **continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy**
It enables you to **develop, build and deploy applications on AWS quickly**
It provides a **fully qualified user interface**, enabling you to manage your software development activities in one easy-to-use place
It is a fully managed artifact repository service that makes it easy for organizations for any size to **securely store, publish and share software packages used** in their software development process
It is a developer **tool powered by machine learning** that provides automated code reviews and recommendations **for code quality** and identifying an applications most expensive lines of code
It is an inexpensive, easy-to-use, resource-friendly and interactive **source control service** that hosts **git repositories**
It can be used **to collaborate with multiple workmates** and has fast and scalable
Upgrade to EC2: is the feature that allows customers to **create copy of Cloud Instance in EC2**
AWS Cloudformation
AWS Elastic Beanstalk
AWS Codecommit
AWS Codebuild
AWS Codedeploy
AWS Codepipeline
AWS Codestar
AWS Codeartifact
AWS Codeguru
AWS Cloudwatch
AWS Cloudtrail
AWS Opsworks
AWS Cloudfront
AWS Cloudsearch
AWS Lightsail
AWS Cloud9
AWS Sqs
AWS Sns
AWS Ses
AWS Mq
AWS Kinesis
AWS Cloudfront
AWS Cloudwatch
AWS Security Hub
AWS Resources Access Manager
AWS Sso
AWS Cognito
AWS Kms
AWS Cloudhsm
AWS Cloudtrail
AWS Inspector
AWS Macie
AWS Guardduty
AWS Shield
AWS Waf
AWS Firewall Manager
AWS Cloud Adoption Framework (CAF)
Business
People
Governance
Platform
Security
Operation
Rehosting
Replatforming
Refactoring (re-architecting)
Migration Strategies
Retaining
Retiring
Migration
Cost Optimization
Operational Excellence
Security
Reliability
Performance Efficiency
AWS Well-Architected Framework
Pillars
Security Pillar
Fault tolerance
Service limits
AWS Quicksight
AWS Cloudtrail
Logs
Metrics
Events
Types
Alarms
Dashboards
AWS Cloudtrail
AWS Trusted Advisor
AWS Personal Health Dashboard
AWS Health Dashboard
AWS EMR
ANALYTICS
INFRASTRUCTURE
PRICING
SECURITY
Amazon Inspector
Amazon Macie
Amazon Guardduty
Amazon Cognito
Amazon Kms
Amazon Cloudhsm
Amazon Cloudtrail
Amazon Cloudwatch
Amazon Security Hub
Amazon Resources Access Manager
Amazon Sso
Amazon Cognito
Amazon Kms
Amazon Cloudhsm
Amazon Cloudtrail
Amazon Cloudwatch
Amazon Security Hub
Amazon Resources Access Manager
Amazon Sso
Security Services
Compliance
AWS Artifact
Agreements
Reports
Compliance Center
Compliance
Disaster Recovery
Multi Site
Warm Standby
Pilot Light
Backup and Restore