Amazon CloudFront
- Edge Locations (CDN)
- Route 53 (DNS)

AWS Outpost (on premises)

Regions (geologically seperated)
Availability Zone (close together)
Edge Locations (CDN)
- cached copy

# How To Provision AWS

AWS Management Console

AWS Command Line Interface (CLI)

AWS SDKs

AWS Elastic Beanstalk
- adjust capacity
- Local Balancing
- Automatic scaling
- Health monitoring

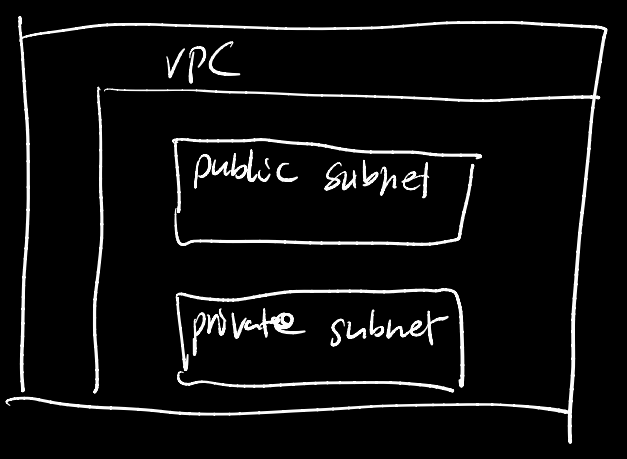
AWS Cloud formation
- json, yaml
- cloudformation template
- calls AWS API for me.

infra as code

# AWS Virtual Private Cloud (VPC)

public subnet
private subnet

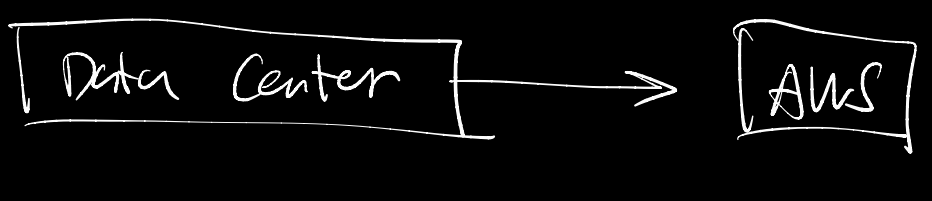
AWS

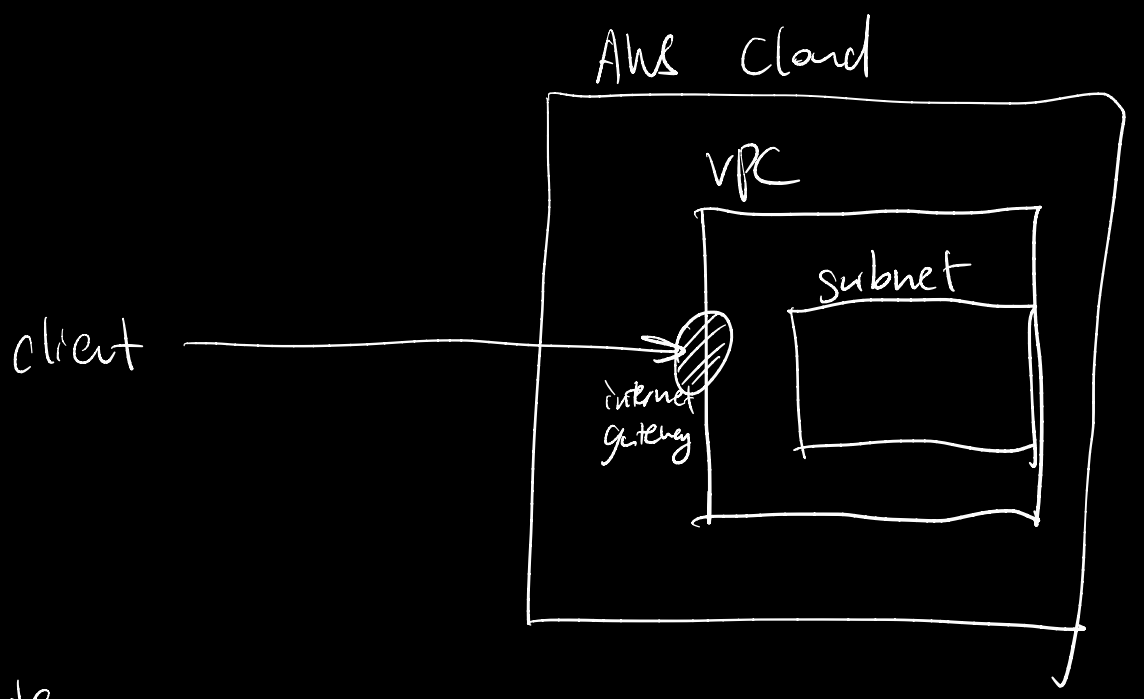



## Subnet

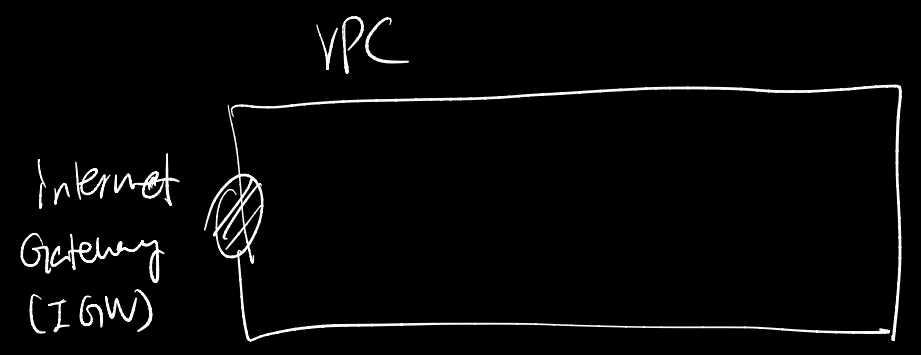
public gateway
virtual private gateway

AWS Direct Connect → physical line

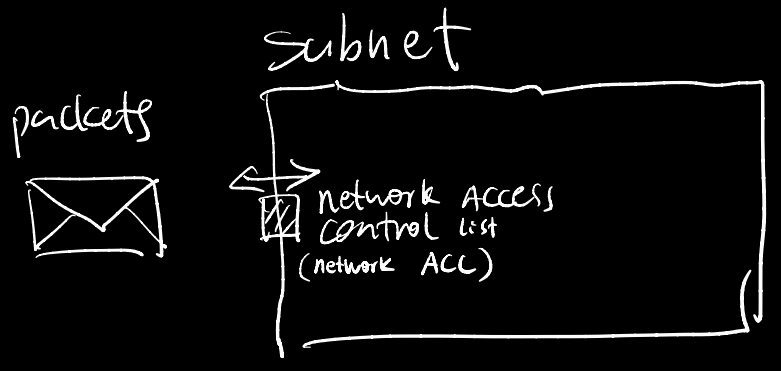


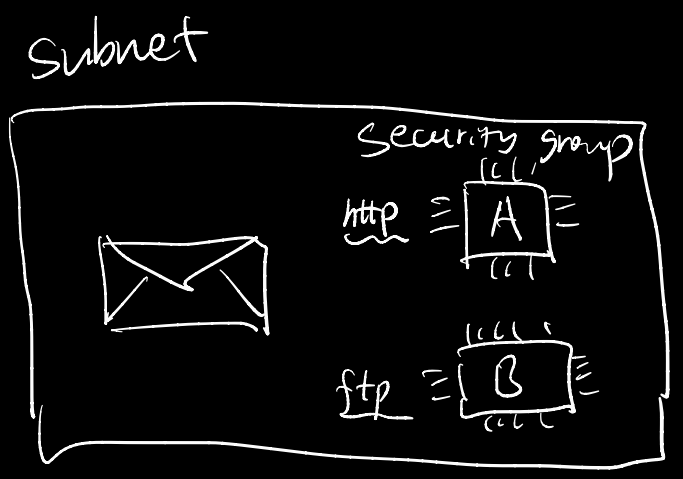



# Subnet & Access Control List




# Network Hardening




## Network Access Control List (ACL)

stateless

default: allow all

## Security Group

(for specific EC2 instances)

stateful

↑ by default, if a packet is allowed in, it can leave

default: deny all inbound
allow all outbound.

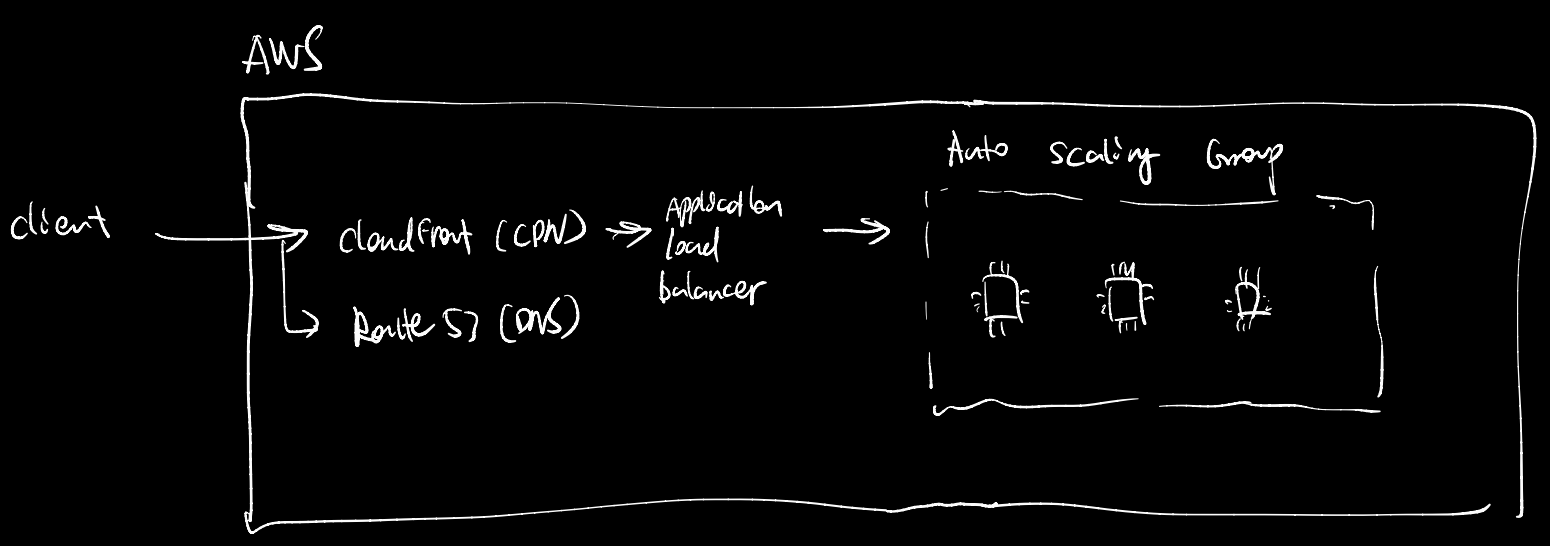
E.X.

Global Network

Route 53 → DNS

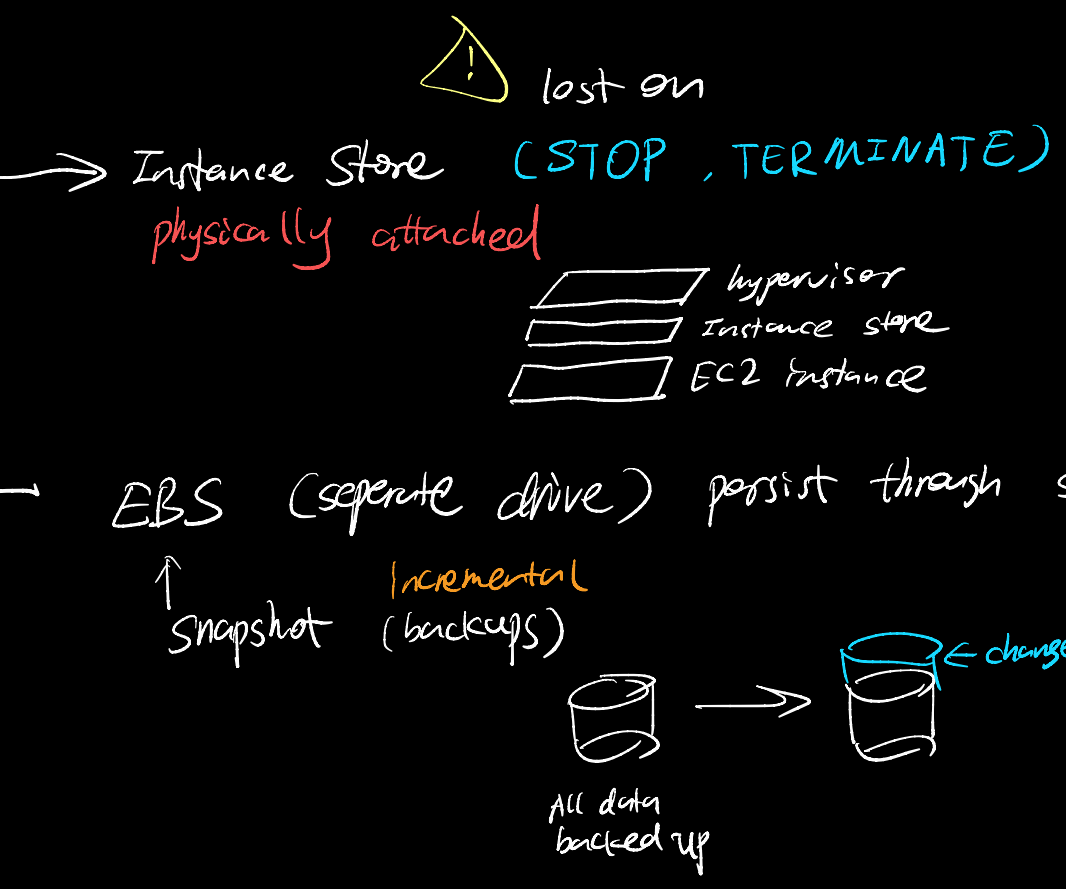
- → latency-based routing
- → geolocation DNS
- → Geoproximity routing
- → Weighted round robin

Amazon Cloud Front (CDN)



# Database & Storages

- Instance Store
- Amazon Elastic Block Store (EBS)




# S3 (Simple Storage Service)

1. up to 5TB
2. as object
3. buckets
4. versioning
5. multiple buckets - permission

## Standards / Storage Class

| | | | |
|---|---|---|---|
| 1. S3 standard | 11 9th | intact 1 year | |

↳ concurrent loss at 2 facilities

2. S3 Standard-Infrequent Access (S3 Standard-IA)

minimum 3 zone (same as S3 standard)

lower storage cost

higher retrieval price

S3 One Zone-Infrequent Access (S3 One Zone-IA)

S3 Intelligent-Tiering S3 Standard <— No access in 30 days? —> S3 Standard-IA

3. S3 Glacier (min — hours retrieval)

Lpolicy (Write Once / Read Many WORM) ← once set, cannot change

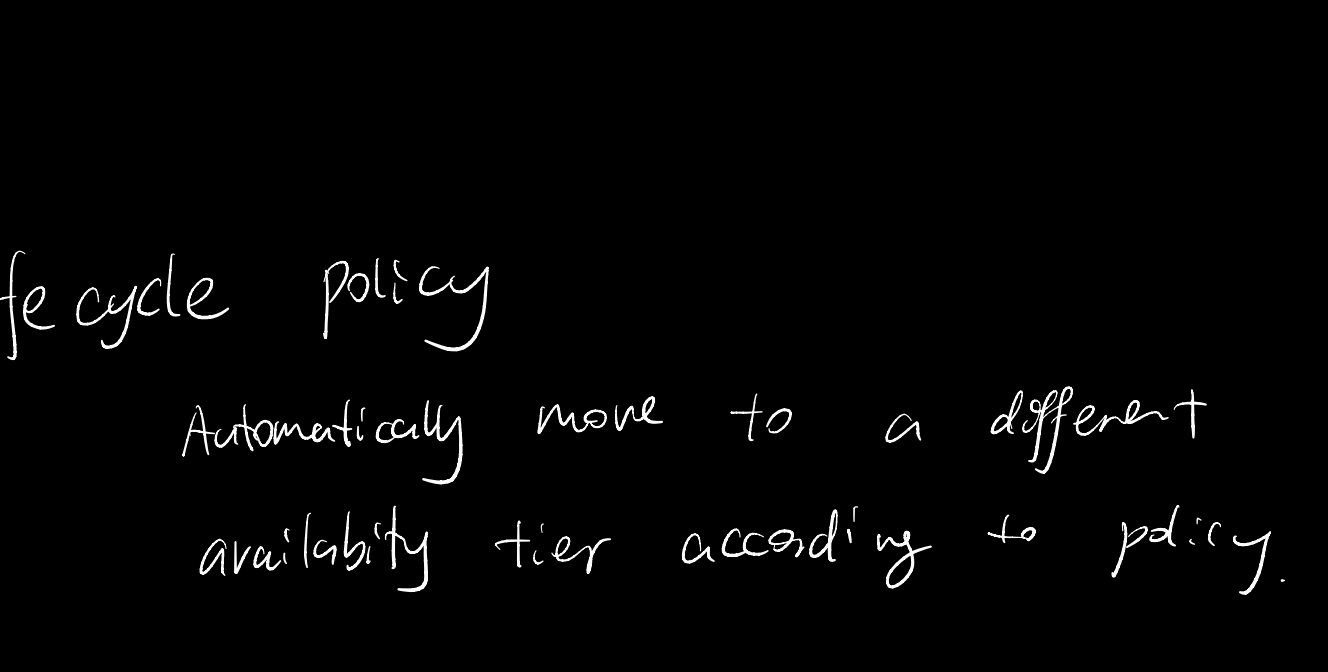
compliance

S3 Glacier Deep Archive (< 12h access)

lifecycle policy

Automatically move to a different availability tier according to policy.

# Object Storage



# EBS

16TB
survive terminations of EC2
SSD by default
HDD Options

has to be at the same availability zone as EC2

# S3

unlimited storage
5TB / single file
write once / read many
99.999999999 %

web enabled
regionally distributed
serverless

# Amazon Elastic File System (EFS)

multiple EC2 r/w same time

Regional Resource

On premises servers access through AWS Direct Connect

# AWS Relational Database Service (RDS)

MySQL
PostSQL  lift-and-shift

RDS — managed
  └ automatic patching
  backups
  redundancy
  failover
  disaster recovery

Encryption
  . encryption at rest
  in transit

1. Amazon Aurora
2. PostSQL
3. MySQL
4. MariaDB
5. Oracle Database
6. Microsoft SQL Server

Amazon Aurora - enterprise-class relational database

MySQL - x5
PostSQL - x3  faster

1. 1/10 commercial DB $
2. 6 replications across 3 availability zones
3. upto 15 READ replicas
4. continuous backup to S3
5. point-in-time recovery

# Amazon DynamoDB (NoSQL)

item → attributes

1. NoSQL
2. purpose built
3. msec response time
4. fully managed
5. highly scalable

serverless

# Amazon Redshift DATA WAREHOUSE

big data analytics

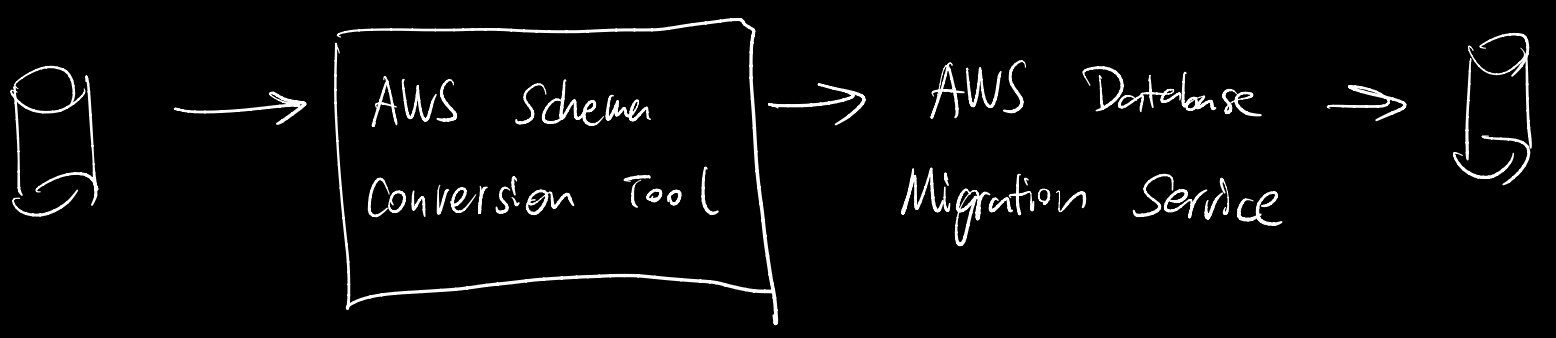
pull data from many sources

# AWS Database Migration Service (AWS DMS)

1. No down time, source DB remain operational during migration
2. Source, destination don't have to be the same DB type

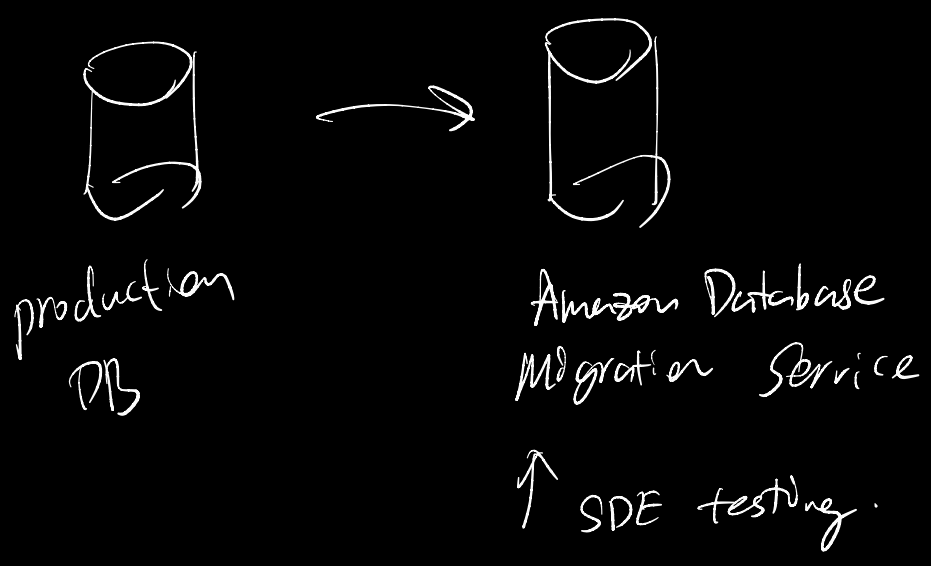
## Homogenous DB


## Heterogeneous DB




## Other Use Cases

1. Development and Test DB Migrations




2. Database Consolidation
3. Continuous Replication

# Additional Database Services

Amazon DocumentDB (compatible w/ Mongo DB)

↳ CMS, catalogues

Amazon Neptune ← graph DB

social network
fraud detection
recommendation engines
knowledge graphs

Amazon Quantum Ledger Database (QLDB)

immutable database, compliance

Amazon ElastiCache

① MemcacheD
② Redis

Amazon DynamoDB Accelerator (DAX)

improve read time for NoSQL

ms → μs

# Security

## Shared Responsibility Model

AWS : of the cloud

customer : in the cloud

## User permissions and Access

root

MFA (multi-factor authentications)

### AWS Identity and Access Management (AWS IAM)

default : no permissions

principle of least privilege

IAM Policy → IAM User

IAM Policy → IAM Groups

json

allow / deny

action : API calls

resource :

### AWS Roles

1. associated permissions
2. allow / deny
3. assumed for temporary amounts of time.
4. no username / password
5. access to temporary permissions

be granted permission to switch to a role

↓

assume role

→ AWS resources
- Users
- External Identities
- Applications
- Other AWS Services

when assume a role, abandon all previous permissions they had under a previous role

# AWS Organizations

① Individual member account
② organizational unit (OU)

1. manage multiple AWS accounts
2. consolidated billings
3. hierachical grouping of accounts
4. AWS service and API action access control

# SCP Service Control Policies (SCP)

maximum permissions

## Organizational Units (OU)

---

## Compliance

### AWS Artifact

compliance report & agreement

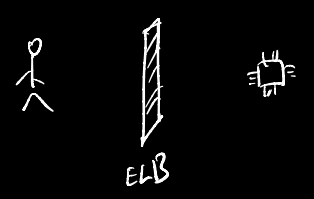
- AWS Artifact Agreement
- AWS Artifact Reports

### Customer Compliance Center

white papers
AWS answer to key compliance questions
overview of AWS risk and compliance
an Auditing security checklist

# DDOS

1. UDP Flood ⟶ security groups
2. HTTP level attack
3. slowloris attack ⟶ elastic load balancer




4. AWS Shield with AWS WAF
   web application firewall
   machine learning

## AWS Shield

- standard (no cost)
- advanced
  - + AWS WAF custom rules
    web application firewall
    machine learning

# Additional Security Service

**Encryption**
1. at rest
2. in transit

AWS DynoDB
- Encryted at rest
  - AWS Key Management Service (KMS)
    - ↳ cryptographic keys

# Amazon Inspector

* network configuration reachability
* amazon agent → EC2
* security assessment service

# Amazon GuardDuty

* intelligent threat detection
* continuous monitoring the network & account activity
  - VPC flow logs
  - DNS logs

# Amazon WAF Web Application Firewall

web access control list (ACL)

↑ different from network ACL with subnet

# Amazon CloudWatch (near realtime)

metrics

cloudwatch alarm → SNS

① Access all metrics from a central location
② gain visibility into APP/Infra/services
③ reduce | MTTR (Mean Time To Resolution) | and | TCO (Total Cost of Ownership)

④ drive insight to optimize applications & operational resources

# AWS CloudTrail (15 min delay)

auditing engine

record API calls for your account

- identity of caller
- ip
- time

## CloudTrail Insight (optional)

- detect unusual API activities

# AWS Trusted Advisor

1. cost optimization
2. performance
3. security
4. fault tolerance
5. service limits

real-time recommendations in accordance with AWS best practices.

# Cost

## Free Tier

- always free
- 12 month free
- trials

| | | |
|---|---|---|
| Lambda | < 1 million | Invocation/month 3.2m sec/month |
| S3 | 12 month | 5G |
| LightSail (VPS) | 1 month | upto 750h of usage |
| SageMaker | | |
| Comprehend Medical | | |
| DynamoDB | 25GB/month | |
| SNS | | |
| Cognito | | |
| Inspector | 90 day | |

# Consolidated Billing

1. Free
2. sharing saving across accounts
3. simplify billing process

default 4 accounts, can request more.

# AWS Budgets

- alert

# AWS Cost Explorer

- 12 month historical data

# AWS Support Plans

## Basic

① 24/7 customer service
② Documentation
③ white papers
④ support forum
⑤ AWS Trusted Advisor
⑥ AWS Pesonal Health Dashboard

## Developer

① Email customer service
* Best practice guidance
* client-side diagnostic tools
* Building-block architecture support

## Business

① AWS Trusteed Advisor
full sets of best practice
② Direct phone access to cloud support engineers 4h SLA Impaired
1h SLA down
③ Infra event managements

Enterprise is min SLA business critical workloads

TAM technical account manager

↳ architecture review

① Operational Excellence

② Security

③ Reliability

④ Performance Efficiency

⑤ Cost Optimization

AWS Marketplace for 3rd party software vendors

1-click deployment

pay-as-you go options

custom terms and pricing

a private marketplace

integration into your procurement systems

cost management tools

# Migration

## AWS Cloud Adoption Framework (CAF)

| | | |
|---|---|---|
| | ① Business | ← Billing, finance, budget |
| | ② People | ← HR |
| | ③ Governance | ← CIO / PM / Enterprise Architect / Business Analyst / Portfolio Managers |
| Technical | ④ Platform | ← CTO / IT manager / Solution Architect |
| | ⑤ Security | ← CISO / Security Manager / Analyst |
| | ⑥ Operation | ← IT Operation Manager / IT Support Manager |

↓

## AWS CAF Action Plan

# Migration Strategies

## The 6 Rs

① Rehosting — "lift & shift"

② Replatforming — "lift, tinker & shift" MySQL → RDS MySQL / Amazon Aurora

③ Retire

④ Retain

⑤ Repurchasing (ex. CRM) traditional license → SAAS

⑥ Refactoring

# AWS Snow Family

Snowcone 8TB 2CPU 4G

Snowball

Storage: 80TB 40vCPU 80G

Compute 42TB 52vCPU 208G

Snowmobile 100PB

# Innovation with AWS

VMWare

Augmented AI

Amazon Lex — chat bot like Alexa

Textract

Deepracer ∈ 1/18 race car to test reinforcement learning models

Ground Station

Transcribe speech → text

Comprehend discover patterns in text

Amazon SageMaker ← ML model

# AWS Well-Architected Framework

① Operational Excellence — annotating documentations, anticipating failure
frequently making small, reversible changes
② Security — encryption
③ Reliability — recovery
④ Performance Efficiency — right EC2 type
⑤ Cost Optimization

# AWS Well-Architected Tool

# AWS Takeways

service
termination

# AWS Benefits

- Upfront cost v.s. variable expense
- economy of scale
- stop guessing capacity
- increase speed and agility
- stop spending $ running & maintaining data centers
- Go global in minutes