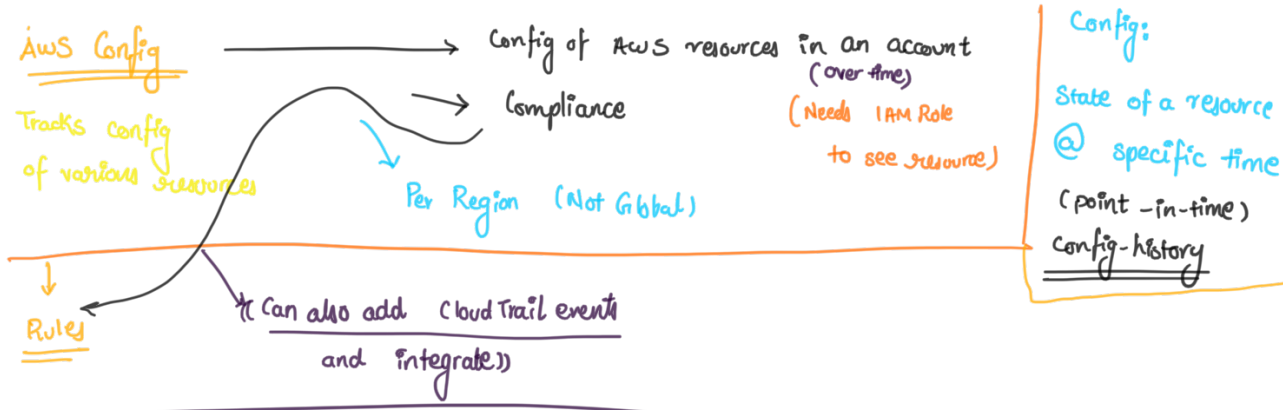
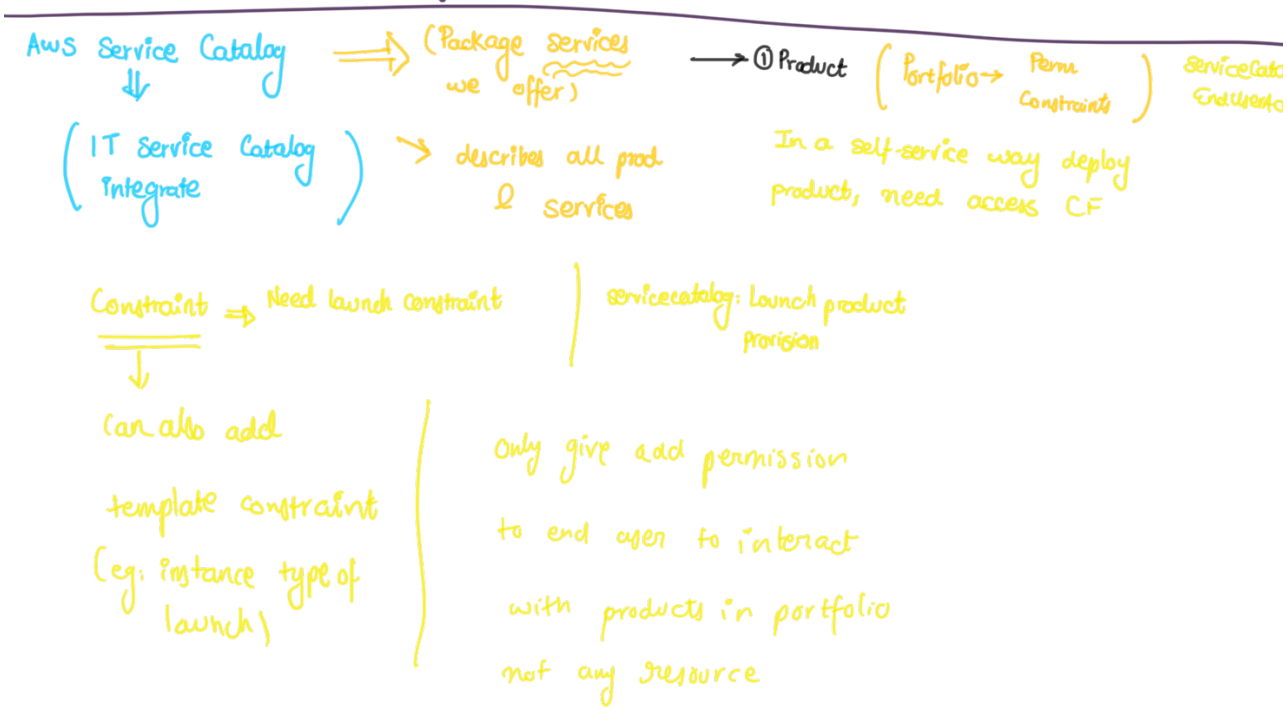
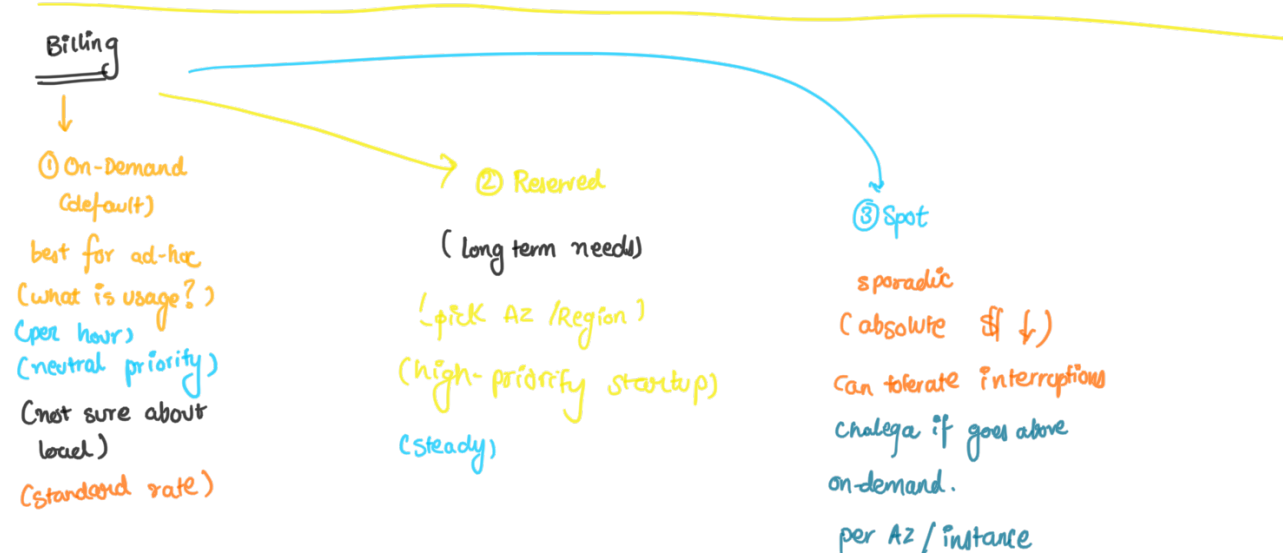
SAA-PRO


AWS Config
Tracks config of various resources
Config of AWS resources in an account (over time)
(Needs IAM Role to see resource)
Compliance
Per Region (Not Global)
Rules
(Can also add CloudTrail events and integrate))
Config:
State of a resource @ specific time
(point-in-time)
Config-history


AWS Service Catalog
(Package services we offer)
① Product
(Portfolio → Perm Constraints)
(IT Service Catalog Integrate)
describes all prod & services
In a self-service way deploy product, need access CF
Constraint
Need launch constraint
servicecatalog: launch product provision
Can also add template constraint (eg: instance type of launch)
Only give add permission to end user to interact with products in portfolio not any resource


Billing
① On-Demand (default)
best for ad-hoc (what is usage?)
(per hour)
(neutral priority)
(not sure about level)
(standard rate)
② Reserved
(long term needs)
(pick AZ / Region)
(high-priority startup)
(steady)
③ Spot
sporadic
(absolute $$ ↓)
Can tolerate interruptions
Charges if goes above on-demand.
per AZ / instance

Identity Federation ⇒ (Bridge security domains)

↓

STS & IAM Role

(AssumeRoleWithWebIdentity

STS swaps for temp. security credentials)

then interact (which is Controlled by the Role)

① Get ID Token

Send to STS

(Temp. Sec. Cred)

we can revoke role for breach

Use of APPonly

② SAML

SAML IDFS

Assertion → Send to SSO Endpoint → STS → (Console URL generated) ⇒ Access Console

(AssumeRoleSAML ✓✓

↓

STS)

49

IAM Boundaries (think of SCP)

Applied to Users, Roles, Organizations

Permission delegation:

(don't need permission to change their own right)

Policy eval:

D → A → D

① Org. Policies

(Blw SCP's then permission)

② User/Role Boundaries

③ Role Policies → Trust / Perm. Policy

(AssumeRole with STS)

④ Permissio

① VPC & Networking

((S3, DynamoDB, CW Logs))

(Public) Endpoint)

Private VPC, Public Services, Public Internet

Tenancy: → Def (Shared HW)

↓ Dedicated

(Single) HOST or DEDICATED

RAM: (Sharing VPC resources blw accounts) ✓ organizations (All features) in org

AZ-ID is diff. for diff. accounts

OWNER / Participant ⇒ we have resource share

AZ - Zone name will be diff. (id consistent)

Subnets ⇒ only custom VPC's

(only same org. accounts) ⇒ can't use SG by other

(Stop share ↓ can only modify) owner can't delete if person has resource

(VPC & VPC Level resources)

↓

((Owner))

(Participant ⇒ inside VPC Can't modify)

But can reference SG's

VPC Routing

① Router (per VPC)

(NACL's only IP no logical)

explicitly DENY

SG: Network interfaces, instances

No order to evaluate

Private / Public

Bastion ← public inet

Bastion → private subnets

IGW does static translation

Bastion does not have private IP // public

((IGW handles))

NAT GW ← ↙

↓ all same public IP

req. Elastic IP

((NAT GW not highly available))

100's of private → 1 IP

Egress:

IPv6 is publically routable

we cannot use NAT bcoz of this

(talk out but not talk-in)

VPC, Subnet, EC2) all alloca IPv6

IGW → Publically (IPv4, IPv6)

DNS in a VPC:

where you are doing from

(public IPv4) can't connect

within, yes ✓

DNS does not pick-up internal

Route 53 allows internal hosted zones

Resolver:

↓↑ inbound endpoint

(VPN, DC)

VPC Flow Logs

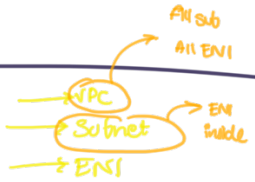
↓

NW Traffic

Traffic metadata

↓

DHCP, DNS, metadata, License Activation Requests



((CW Logs)) OR ↔ S3

IAM Role: Needs permission

GW endpoints

⇩

object not in subnet → apply policy

(prefix list, route table)

IIF endpoints

No routing

physical in a subset

SG

private IP

by using (priv DN,

of endpoint

(unique DNS endpoints)

Peering: connect VPC

① Create Peer
② Logical Route
③ SG-referencing only same region

account @ sg-

(Cross-region only IP)

Tunnel endpoint

VPN's – VPN

Hardware-based
(use public i/net)
(fully encrypted)

2 Tunnels in AWS from 1 CRouter (diff AZ) (BGP dynamic)

(2 C/G/w and 2 Tunnels)

① Customer G/w ⇩ H/Bl router

IPSec VPN conn
Stat/dynamic

simple
what's next' core available?
IP range

dyna
over 8
(BGP ASN
((BGP ro
or privat

② VPG/w ⇩

VPC router will route to this
attach to a VPC

Local > DC, Highest static (prop → NO)

Dynamic BGP
VPN (lowest)

- quick setup
- cheap. /hour (sporadic, lower)
- CPU perf. encryption

Direct Connect: private connection

→ ① speed?
② public VIF:

change (all regions) only access public zone resources (region)

private VIF: one VPG/w same region

DConnected ⇒ (Not encrypted)

DC: G/w: ⇩ VP G/w in any region

(VPG/w) ⇒ public zone

one
VLAN ⇔ VPN

Layer VPN over (public VIF)

Data out + $; in → no $

(All BGP) > (BGP VPN)

Transit G/w: (Hub-spoke) ⇩ G/w object ↘ diff. accounts ↓ replace VPG/w

VPC's & VPN's

((envelope encoding))

ACM: ✓ Data @ Rest

(Level-2) FIPS 140-2; KMS

X.509: SSL/TLS

(API)

Directory Services:

① Simple AD → Samba 4 (cut-down → not all enterprise)

AD Connector → SSO, EC2 & WorkSpaces

Microsoft AD → Bridge On-premise & AWS

Cognito → Trust with existing → scalable, authentic Microsoft AD

Cloud Directory → Web Scale: identity fed (not console but apps) (User Identity Pools)

Graph based (AWS managed graph based) → object info, relationships and schema management

Anti

all deployed in VPCs

WAF & Shield

WAF ⇓

control traffic (ACL) ↓

(IP, string, SQL) → Cross-site, Geo location

(CloudFront, ELB, API GW) → Size Constraints

Condition ⇒ Something AND something rules ⇒ rule1 rule2 WebAcl

DDOS attack → shield advanced (SYN Floods UDP/TCP)

GuardDuty → Access data sources from AWS accounts

→ Cloud Watch Events

→ Console

→ Trusted IP List

master

only 1 GuardDuty member

VPC Flowlogs, DNS Logs, CloudTrail,

need Service Role

Containers

isolated env:

applications with libraries

Portability

Virtualization

App

OS OS OS

VM VM VM

hypervisor

H/W isolation

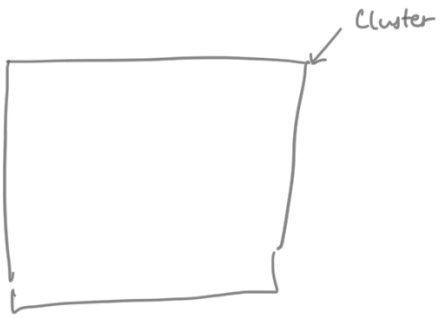
((Mapped to external ports))

Container → Host

↓ tcp/80

Remote Service Access

ECS:



Task → EC2 → ECS agent (management)
Task → Fargate (managed)
↳ Task (instantiate)
Container