AWS

IAM (Security, Identity & Compliance)

root Acc → email Add used for sign in @ Amaze

Global (Region) → (Question can come)

MFA → Multifactor Authentication

→ Virtual →

download → Google Authenticator

675945 → code1

579849 → code2

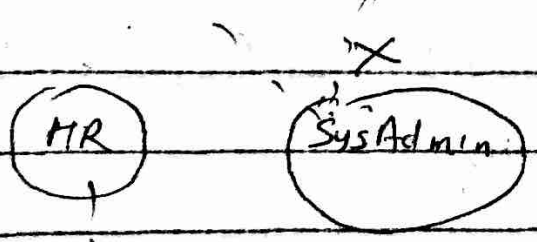
Create grp → System_admin → type admin

→ System Admin → Admen-Access

Create User →

New Grp → HR → Amazon S3 Read Only Access

ryan john



John

→ Attach (add policy)

↓

glacier (Add permissn)

redshift

Pagerduty

Create Billing Alarm (Question can come)

EC2

Pricing Model — FAQ read.

- On demand → Pay by hour, fixed rate
- Reserved → 1 to 3 yrs (Predictable use)
- Spot → flexibility (bid Price) ex: Stock Mkt.
  - ↳ change based on region → or Availability zone
  - → Urgency need
  - → Pharmaceutical comp. used
- Dedicated host → hourly rate
  - ↳ Multitenant virtualization

→ F1 went F1.50 Terminated EC2 instance.

Instance Type — (not charged for partial hour. If user terminates after 1.5 hrs. user will pay for 2 hrs while if company does it will take 1 hr.)

- D2 → Dense Storage
- R4 → memory Optimized — DR MC GIFT PX
- M4 → General purpose
- C4 → Comp. Optimized
- G2 → Graphs. Intensive
- I2 → high speed storage
- F1 → Field Prog Gate Array (H/w Acceleration, underline)
- T2 → low cost (webserver & DB)
- P2 → Graphic/General purpose
- X1 → Memory optimize (Apache spark, need extream memory)

EC2 — Elastic Compute Cloud.

EBS → Disk (Block based)

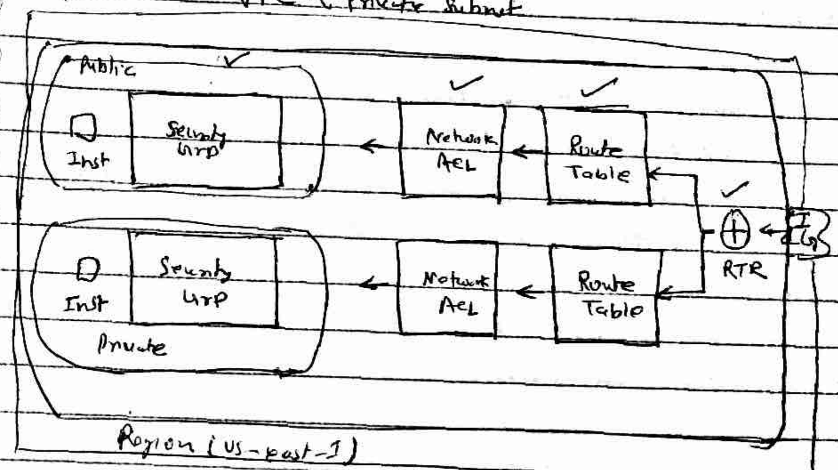
EBS three Types

1. SSD — GP2 (General purpose) 40 to 10,000
   SSD — IOPS-IO1 (3IOPS = 1 GB) More than 10,000 to 20,000 — Provisional IOPS SSD
2. Magnetic: HDD — ST1 — written in seq. (Big Data etc.) — Cannot Boot
   Magnetic: HDD — SC1 (cold hdd)
3. HDD Magnetic Standard → bootable.

* 1 Sub-net → 1 Availability zone.

* 10.0.0.0 → Private Internet
  172.16.0.0 — 172.31.0.0
  192.168.0.0 → home network

* VPC & Private Subnet



* No Transitive peering — (I)R cannot possible
* 1 IG for subnet — * Default 251 IP available)
* .1, .2, .3 reserved.
* Multiple IG cannot used for perform —

Creating Web-Server

→ Chmod 400 <keypair>
→ ssh ec2-user@public_IP -i <key>
→ y → sudo su
→ yum update -y
→ yum install httpd
→ cd var/www/html
→ nano index.html
→ service httpd start
→ hit Browser with public IP

Elastic Compute cloud.

→ All inbound traffic blocked by default
→ " Outbound " allowed " "
→ Changes to Security Group take effect immediately.
→ You can have any no. of EC2 instance within a Security group
→ multiple sec grp attached to EC2.
→ Sec Group are stateful.

Upgrade EBS

/dev/xvda
/dev/sdb
lsblk
mkfs -t ext4 /dev/xvdb (create file system)
mkdir /acloudguru
mount /dev/xvdb /acloudguru
lsblk (Check for mount)

Cd /acloudguru
ls
nano test.html
ctrl x, ys.

umount /dev/xvdb
ls
mount /dev/xvdb /acloudguru.

file -s /dev/xvdf

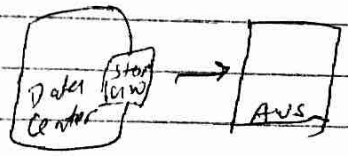
#
✓ Raid 0 - Striped, No Redundancy, Good performance
" 1 - Mirrored, Redundancy
" 5 - 3 or more (Amazon don't prefer Raid 5)
✓ " 10 - Raid 0 + Raid 1

Security Group
RDP - 3389 - My IP
2012-R2

Encryption

In Transit → SSL/TLS
At Rest → SSE - S3
- KMS
- C

Storage GW:



→ NFS (file)
→ iSCSI (volume)
→ Stored
→ Cached
→ Tape GW (VTL)

Snowball (Data from AWS)

80TB

→ Snowball

→ Snowball Edge. — 100TB

→ Snowmobile — Peta byte / Exa byte level data

(Before Snowball) legacy was import / export disk

Snowball can → import from S3, also export

⇒ S3 Transfer Acceleration

⇒ S3 → Obj based

⇒ files can be 0 byte to 5TB

→ files can be stored in bucket

→ S3 - region . amazon . —

Security Access key

Secret " "

Token

Expire

Secure Token Service (STS)

Databases

RDS → 1. MS SQL

2. Oracle

3. MySQL

4. PostgreSQL

5. Aurora

6. MariaDB

DynamoDB

Non Relational → Db

- Collection — Table
- Doc — Row
- Key value pair

Data warehouse →

OLTP → Transaction

OLAP → Analytical

DMS → for migration

/dev/sda

/sda1 — 524 MB

free space — 41 MB

/sda2 134 "

/sda3 7B6 "

/sda4 255 MB

/sda5 232 "

/sda6 472 MB

free space 10 GB (install Mx)

Window installer (ub 16.04)

Sudo apt install unetbootin

Run → sudo unetbootin

Multi AZ → no (Initial set-up)

VPC security grp

DynamoDB

Stored in SSD

3 Geographic distinct
↓
faulty

Write throughput $0.0065 for 10 Units

read " " 50 "

1 million — write capacity.

$\frac{.0065}{10} \times 12 \times 24$

Good for read. (If proj. need more read)

We can add column etc. on requirement.

RedShift — Warehouse soln.

10 time faster

SSL

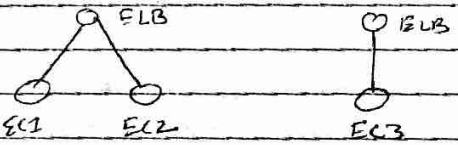
Not for multi AZ (only one availability zone)

Elasticache

Route 53

→ Set-up one domain (Pandhari)

→



Routing policies

→ Simple → (Record set) Assign ELB to Pandhari domain.

Weighted →

Latency →

Failover

Geolocation

Vyavahar

10,000 view - part 1

→ Region (Geo location)
→ Availability zone (Data Center, 2 or more)
→ Edge location (CDN end point for CloudFront)

Currently 66 Edge location. ↓ Bunch of Edge location

VPC more virtual data Center

Route 53 is DNS Service
↓
DNS port

Direct Connect → connecting physical Data Center to cloud using phone line.

EC2 → Virtual machine

EC2 Container Service → highly Scalable, Support docker etc. (hi perform.)
or ECS

Elastic Beanstalk → Upload at beastalk, provisioning to code.

Lambda → Serverless

Storage S3 (555) → Store Obj.

Glacier → 7 years ok. (Data Archival low cost)
Takes 3 to 4 hour.

Snapshots.

EFS → Elastic File system (file based can be shared, multiple virtual machine we can share)

555 →

Storage GW → Virtual machine at premise.

Databases RDS (MySQL, MariaDB, Sql, oracle, aurora)

Dynamo DB (Non-Relational)

Redshift Datawarehouse Elasticache

Migration

Snowball

DMS (Database Migration)

Kinesis → Real time data running (Big data)

Analytics Tera byte.

Data pipeline → moving data

Cloud search

EMR

Elastic search

IAM

WAF (firewall, App protection)

Mgmt tools

Cloud watch (performance, disk, RAM e

Cloud Formation → Infra. pt doc. describe Arch
Env., doc. Infrastructure to code.

Cloud Trail → Auditing

Opsworks → Chefs

Config Mgt → Many env. related

Service Catalog →

App Services SWF

API GW

Elastic Transcoder → Converting Video

SQS → Queue Service

② IAM

→ Users → Roles　　IAM is global
→ Groups → Policies
https://no.sign.aws.amazon.com/console

Imp { root Acc → email address for sign in aws
Imp { Policy doc written in JSON language.

Imp { Access Key id
{ Secret Access Key] Programatical only used

User & Pass → Mgmt console.

③

S3 → obj. based. 0 byte to 5TB
→ S3-Region.amazonaws.com/acloudguru
→ http200 (successful)
→ Read after write Consistency for PUTS of new obj.
→ Eventual Consistency for overwrite PUTS & DELETES
update or delete
Can take some time
→ 99.99 availability
→ 99.9 S2A
→ 99.999 999 999 Durability
→ S3-IA lower fee than S3, Charged for retrival.
→ Glaciar - Very cheap. Takes 3-5 hours for retrival.

S3	S3-IA	Glaciar
99.99	99.9	99.9...
99.99	99.9	99
99.9	99	NA
NA	30	90 days
	infrequent access	

{ Key → Name of obj
Value → Data
VersionID
Metadata

→ Unique bucket name, ...
→ Private (bucket first time Creation)
by default it is Private

https://S3-Region.amazonaws.com/bucket name/file
→ Change permission after Creation.

Versioning
→ It only disable, (cannot remove versioning after Creation only disable possible)
→ Don't update large file constantly, it will hit size. (oldversion size + new version size ...)
→ V Great back-up tool
→ Additional Security using MFA

Cross Region Replication
→ Regions must be Unique (Not Same)
→ versioning must be enabled on both the source and dest buckets
→ You cannot replicate to multiple buckets or daisy chain it
→ Delete mark replicated

Life Cycle
Action on Current version
0 days → (30 days) S3-IA → +30 (60 days) Glaciar → Exp 425 or 61 or etc.

Action on Previous Version
150 days (minimum for delete) [60+90 → 150]

→ Can be Used Conjuction with versioning.

Cloud Front

CDN

Edge location
Objects are cached for the life of the TTL
Distribution → CDN which consists of a collection of Edge locations.

Origin → S3, EC2 instance, Elastic load bal or route 53

Whitelist → list of Countries where you want cloudfront
Blacklist → " " " " " don't want "

Edge location both read and write.

Securing your buckets
→ by default, all newly created bucket are private
→ Bucket Policies
→ Access Control lists.
→ Server side
SSE - S3
" - KMS
" - C

Storage GW:- → It is on-premise virtual appliance that can be used to cache S3 locally at a customer site.
→ File GW (NFS) → Flat files on S3 only
Block based (OS etc) → Volume GW (iSCSI)
→ Stored Volume (GB)
→ Cached " (32TB)
→ Tap GW (VTL)
(back-up app like NetBackup)

Snow ball → Previous Import/Export (Before Snowball)
→ 80 TB Snowball in all regions.
→ Peta byte Scale
→ Box
(Standard, Snowball Edge (u can run lambda func.), Snow mobile)

S3 Transfer Acceleration (speed up transfer)

Static web site Using S3
→ Serverless
→ http://mys3website.s3-website-eu-west-2.amazonaws.com
→ http 200
→ multipart upload fast

EC2:- Elastic Compute Cloud
On demand → low cost flexibility, without commitment
Reserved → Steady state
Spot → Flexible start & End
Dedicated hosts

D2 → Dense
R4 → memory (RAM)
M4 → main choice u purpose app
C4 → compute
G2 → Graphics
I2 → IOPS
F1 → Create Array
T2 → low cost (think pics)
P2 → Graphics / high performance / mem optimize
X1 → Extreme Memory (RAM)

DR MC GIFT PX

Security Group (Virtual Firewall)
→ Any no. EC2 inst. in SG.
→ 1 instance have multiple Security Group.
→ Statefull (In then automatically op)
→ Immediately change reflect
→ No deny rule
→ All inbound Traffic block by default
→ All o/p allow by default
→ You can't block IP using Security Grp.

EBS Disk attach to
→ SSD (GP2) - upto 10,000 IOPS
→ SSD (IO1) - More than 10,000 IOPS
→ HDD (ST1) - frequently access workload
→ HDD (SC1) - less " "
→ Magnetic - Cheap, infrequent access
→ 1 EBS cannot mount to Multiple EC2 instances, instead use EFS.

→ 1 instance can have multiple security groups.

→ Stateful, If u add inbound rule by default outbound rule be there.

→ All inbound Traffic is Blocked by default
→ " Outbound " is Allowed
→ Changes to security Groups take effect immediatly
→ You can have any no. of EC2 instance within a security Group
→ Security Group is Stateful
→ You cannot block specific IP address using security Groups, instead Use Network Access Control Lists.

EBS Upgrade :-

→ EBS Volume can be changed on the fly (Except for magnetic standard).
→ Best practice to stop EC2 instance and then changed the volume.
→ After changin on fly wait for 6 hours before making change.
→ Volumes must be on same AZ as EC2 inst.

RAID (Redundant Array of Independent Disk)

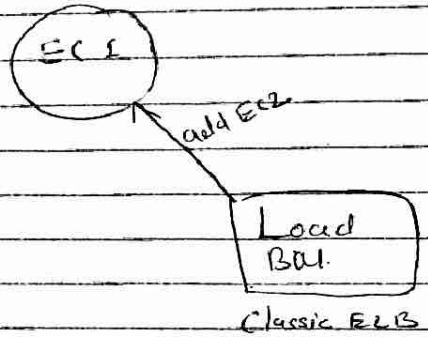
Raid 0 — Striped, No Redundancy, Good performance
1 → mirrored, Redundancy
5 → Good for read, bad for write (AWS not recommd)
10 → Striped, mirrored, redund., good perfor

AMI

Amazon machine Image

Instance store volume cannot be stopped.
(Ephemeral storage)

Elastic Load Balancers



→ ELB created as Internet or Outofservice
→ ELB has own DNS name.
→

Cloud Watch

- CPU related
- Disk "
- Networ "
- Status Chek "

Events :- Automatically invoke an AWS Lambda function to update DNS
standard monitory 5 min
Dashboard
Alarm & Event
logs - CloudWatch Logs help to aggregate, monitor and store logs
↓ for logging (Monitoring)
(Cloud Trail ↓ Auditing)

AWS Command Line

> aws s3 ls
> aws configure
Access key & id
> aws s3 ls

Commands -
cp, ls, mv etc.

IAM Roles Lab

IAM → Roles
S3FullAccess (S3-Admin-Access)

S3 CLI

Bash Scripting

S3 bucket → Place file there
Role (IAM) → MyS3Admin
EC2 create (Instance)
Advance detail (Put Bash Script)
#!/bin/bash
yum update -y

EC2 Metadata

Curl http://169.254.169.254/latest/meta-data/
Curl // // // public-IPV4
// // // // IPV6

Launch Configuration & Auto Scaling Group.

Auto Scaling Group
↓
Select AMI

EC2 Placement Group

Hadoop cluster

→ Placement can't span multiple AZ.
→ HPC, MPI, Storage optimize

EFS Concept & lab

→ EFS is block based

Lambda

Node.JS ✓
Java ✓
C# ✓
Python ✓

→ no of request
→ First 1 million are free, .20 per 1 million thereafter.
→ No servers.
→ 1 event = 1 function
→ Scales out
→ 1 event = x functions

Route53

IPv4 → 32 bit
IPv6 → 128 bit

Domain creation

Routing Policies

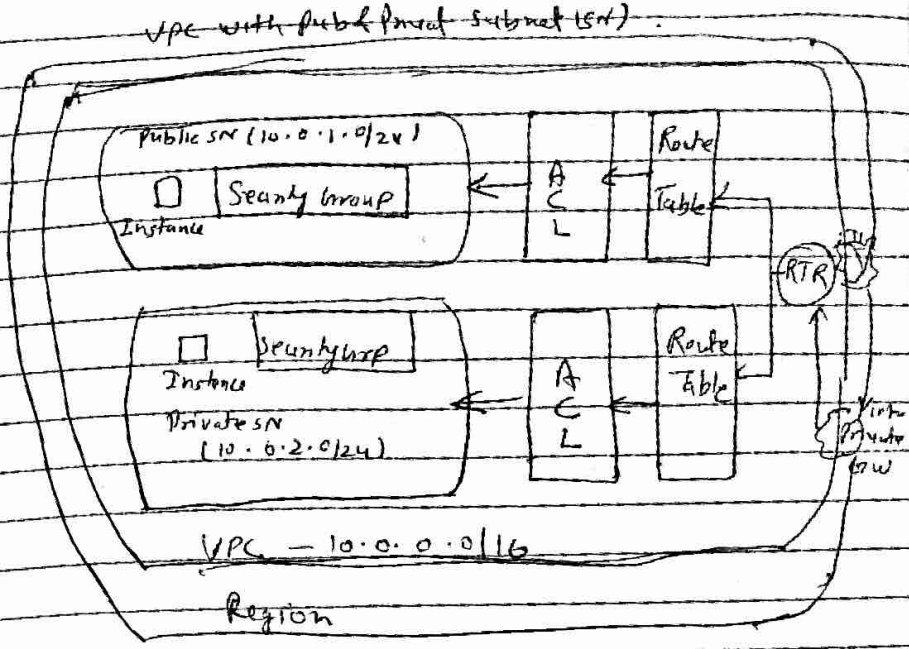
- Simple → User → Route53 → Region
- Weighted → To ESD etc.
- Latency
- Failover
- Geolocation

Route53 → Create Record Set

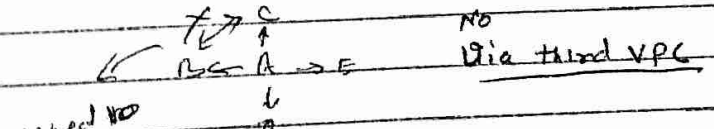
Databases

Imp.
- RDS → SQL, Oracle, MySQL, Postgresql, Aurora, mariaDB
- DynamoDB → Non Relational

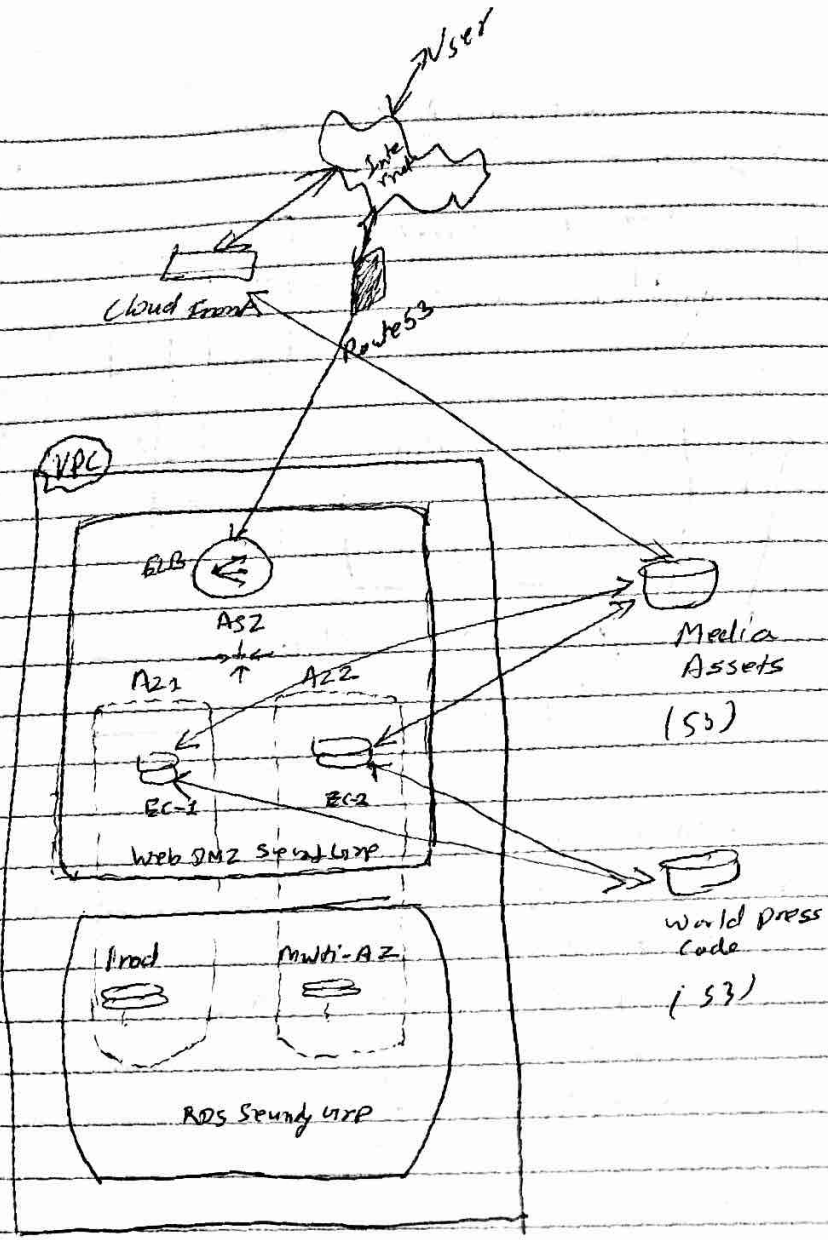
Elastic Cache
Redshift
DMS



→ 1 Subnet = 1 availability zone (AZ)
→ Security Grp & ACL, Route Table can span multiple AZ.
→ IGW → One IGW per VPC
→ Security Grp → (stateful) while ACL (stateless)
→ Default VPC during Acc. creation.
→ Don't delete default VPC, otherwise need help from Aws.
→ No Transitive Peering.



We need to create VPC
You cannot talk via other VPC



DynamoDB 101

↓

No SQL, fully managed.

→ Stored on SSD

→ 3 Geo distinct or 3 location

Write : to 3

→ Eventual consistency Reads (within 1 sec)

→ Strongly Consistent Reads

→ 35 level of nesting.

→ $0.0065 Per hr for 10 units. (Write)

→ " Per hr " 50 " (Read)

→ First 25GB free

$0.25 GB Per month.

→ Table, Item, attributes

Ex:- 1 million read
1 " write } Per day.

Write

$\frac{1000000}{24 \times 10} \times .0065 + 1 \Rightarrow ?$

$\frac{100000}{24 \times 60 \times 60} \rightarrow \frac{10000}{864} \Rightarrow 11.6$ Per second

$\frac{.0065}{10} \times 24 \times 12 \Rightarrow .1872$ Per/day

Read

~~1000000 / 1000~~ 0.0374 Per/day

$30 \times (.1872 + .0374) \times (.25 \times 3)$

$\Rightarrow \$7.488$

Primary key

→ Unique ID (Partition key) or hash key
(No nested)

One attribute.

→ Composite key (More than one code)
(Partition key & sort key)

Hash | Range

Indexes

Local
→ Can't be removed

Global →
diff partition key & diff sort key.

→ Stream stored for 24 Hrs → lambda func.

Query

To reverse the order, set the ScanIndexForward parameter to false.

Scan

Whole table, Every single Item in table.

Eventual → 2 reads/sec
Strong Consitency → 1 " / "

Ex:-

Item → row

$$\frac{\text{Size of Read rounded nearest 4KB chunk}}{4} \times \text{no of Item} = \text{read throughput}$$

① $\frac{4}{4} \times 10 \Rightarrow 10$

Eventual $\Rightarrow \frac{10}{2} \Rightarrow$ 5 Units read throughput

② $\frac{8}{4} \times 10 \Rightarrow 20$

Eventual $\Rightarrow \frac{20}{2} = 10$

③ $\frac{12}{4} \times 5 \Rightarrow 15$

Eventual $\Rightarrow 7.5 \Rightarrow 8$ Units.

④ $\frac{12}{4} \times 5 \Rightarrow 15$

Strong Consitency $\Rightarrow 15$

Write throughput

① 5 x 10 ⇒ 50 write Units.

② 12 x 100 ⇒ 1200 write Units.

⇒ 4xx Http Status code – Provision throughput Exceeded Exception

Web Identity Providers → ① User Authenticate with ID provider
② Pass Token by ID
③ Your code calls AssumeRoleWithIdentity

Id → Token → web Identity.

Conditional Update ✓

Atomic Counters ✓ Prefer Conditional based on critical.
If some margin of error use Atomic Counter.
If no error margin then use Conditional update.

DynamoDB FAQ → Important

Ques:-

$\frac{8^2}{4} \times \frac{600}{60} \Rightarrow \frac{1800}{2} \Rightarrow \frac{600}{60}$

$10 \times \frac{8^2}{4} \Rightarrow \frac{20}{2} \Rightarrow 10$

$\frac{10}{4} \times 8^2 \Rightarrow 20$

$\frac{16}{4} \times 25 \Rightarrow \frac{100}{2} \Rightarrow 50$

$\frac{10}{4} \times 25 \Rightarrow 10$

2 items of 15 KB per 50

$10 \times \frac{8^2}{4}$

Terraform

Variables

us-west2 (Region) etc.

```
resource "aws instance" "web" {
    ami = "ami no"
    Instance typ = "ms.small"
}

resource "aws-elb" {
    # other attributes
}
```

main.tf

↓

teraform.

Terraform init +

Terraform plan ~

Terraform Apply ~ update

-/+ destroy & re-create

↓ ordering

transient error

Variables

Outputs

Interpolation Functions

Modules

Remote State

$ var. core.id

Cloud Formation

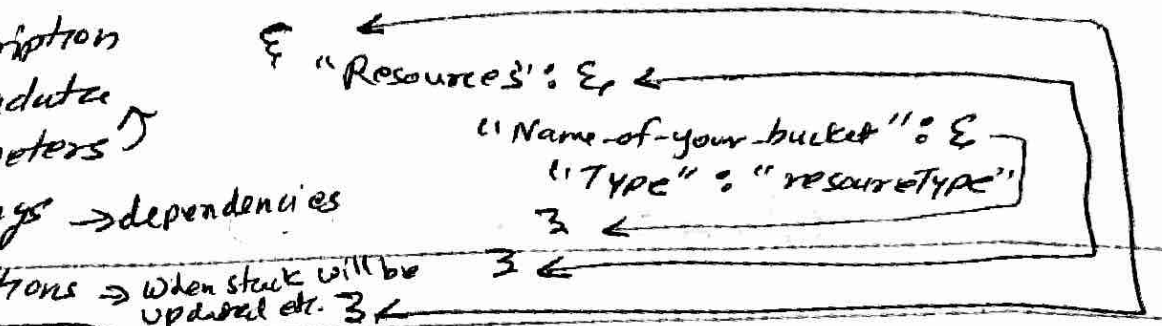
```
{
  "Resources" : {
    "HelloBucket" : {
      "Type" : "AWS::S3::Bucket"
    }
  }
}
```

```
"IIBSecurityGroup" : {
  "Type" : "AWS::EC2::SecurityGroup"
  "Properties" : {

    "Type" : "CustomTcpRule"
      "Protocol" : "TCP"
      PortRange :

"InstanceSecurityGroup" : {
  "Type" : "AWS::EC2::SecurityGroup",
  "Properties" : {
    "GroupDescription" : "Enable SSH"
    "SecurityGroupIngress" : [ {
      "IpProtocol" : "tcp"
      "FromPort" : "20",
      "CidrIP" : "  "
    } ]
```

✓ Description
✓ Metadata
✓ Parameters
Mappings → dependencies
Conditions → When stack will be updated etc.
Resources → All the AWS resources.



{
"Resources": {
"ABC123"
"Type": AWS::S3::Bucket"
"properties":
}
}

Environment Provisioning

1. Terraform
2. cloud Formation
3. Heat

Install MK

1. Packer
2. chef
3. Puppet

Creating & starting VM

1. chef

Delete Resource

Terraform Destroy.

DevOps

→ Continuous Delivery & Automation 55%
→ Monitoring, Metrics, and Logging 20%
→ Security, Governance, and Validation 10%
→ HA & Elasticity 15%

Monitoring, Metrics and Logging

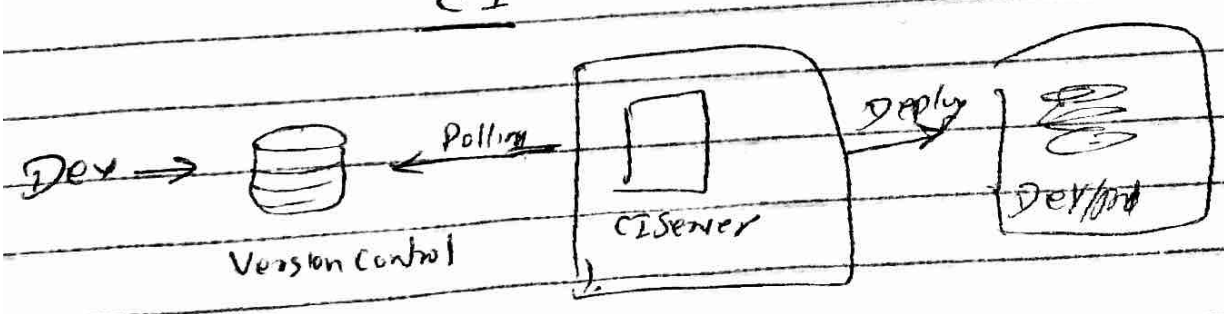
→ Cloud watch
→ Custom Cloud Watch
→ Creating Cloudwatch Alarms
→ Monitoring API Calls with CloudTrail

Cloud watch

→ Monitor AWS Resource → Monitor custom metrics
→ Monitor & store logs → Set Alarm
→ View Graph & Statics → Monitor & react to change.

Continuous Delivery & Automation

CI



Cont. Delivery

Source →(Auto) Build →(Auto) Staging →(Manual) Prod

Cont. Deployment

Source →(Auto.) Build →(Auto) Stag →(Auto) Prod

https://git-scm.com/download/win

git-hub id → psd12

mikepfeiffer

Create New Role → CDInstanceRole → EC2 → Codedeploy
(AmazonEC2RoleforAWSCon...) →

CDServiceRole → CodeDeploy

EC2 → Amazon Linux (2 Instance) → CDInstanceRole → gist (mike...) gistfile1

Add Rule (http).

Code Deploy → App Name → Value (Dev) → One at a time
→ ARN → Create App

Dev Tool → Code Pipeline → GitHub → Connect
→ mike/aws-cod-... → build provider → No

Build → AWS code deployment → Code Role

Terraform (02/11/18)

Terraform Installation

→ Download from terraform.io
→ sudo mkdir -p /opt/terraform
→ sudo unzip <path> -d /opt/terraform
→ update .bashrc
nano .bashrc
→ /opt/terraform
→ export PATH="opt/terraform:$PATH"
→ source ~/.bashrc
→ terraform --version

AWS Config for Terraform
→ AWS Acc → Create User
→ Store Access Key & Secret Access Key } CLI
→ sudo apt install awscli
→ aws configure
[Enter keys & Region]

HCL → Hashi Confi Language

EC2 Provisioning
→ Create file with values
provider "aws" { access, secret, re...
resource "aws_ins..."
{ ami, ... }
nano for creating file
→ terraform init
→ terraform plan
→ terrafor apply

Docker (02/10/18)

Install docker

→ from website or directly on ubuntu

Configure

Configure dockerfile with project binary

Create Image

docker build

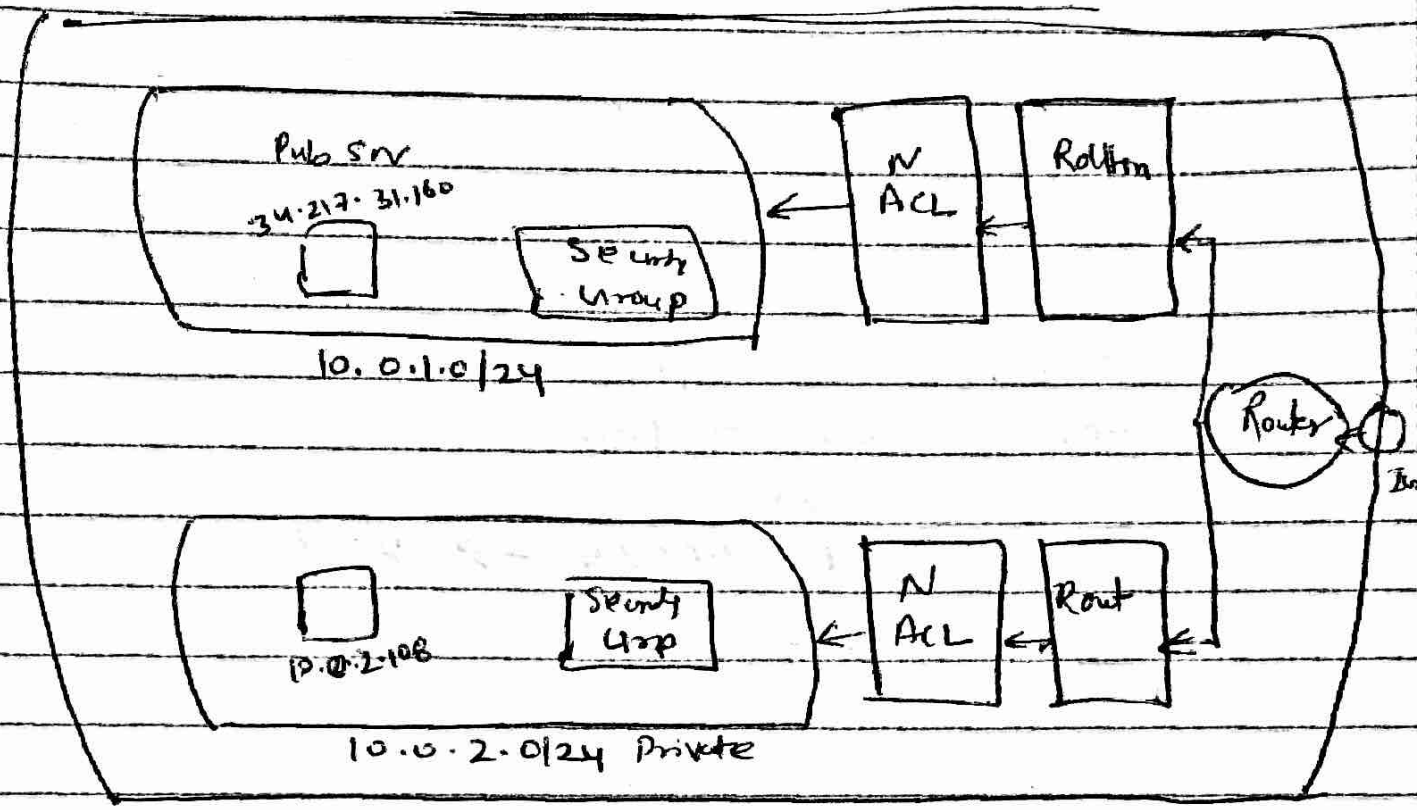
docker image

02/10/18

→ VPC creation Practice

→ VPN " "

VPC



10.0.128.0/20 10.0.144.0/20

10.0.0.0/19 10.0.32.0/19

10.00.0/16

SQS

→ default 30 sec (Visibility Time out)

→ Max 12 hrs (" ")

→ De couple

→ SQS Long polling (Untill message comes out or long Poll timeout)

→ " Short " (returns immediatly)

no message also return.

even Que empty.

→ Inexpensive 9m40s
Return ASAP one message
If no message no return
or Max long poll time = 20 sec

It asks is there message, If not not poll. If message it retrive.

Max → 20 Se.

If message arrives no need to wait for 20 se.

SQS Fanning out with SNS.

→ FIFO @ Oregon, Ohio, N Verginia & Ireland

→ Que are regon specfi

→ sec at Que.

SNS

(1) ARN

(2) TTL (After that message deleted)

(3) Protocol → HTTP(S), Email, Email-JSON, SQS, SMS

(4) SSN → Aple
→ google
→ Bedo
→ win

(5) 3 da Exp subscription. (6) TOPIC

(7) Type, Mosed, TOPIC, Sub, mess, Tm.

Sig, Sig version, Unsubscribe

Azure CI/CD

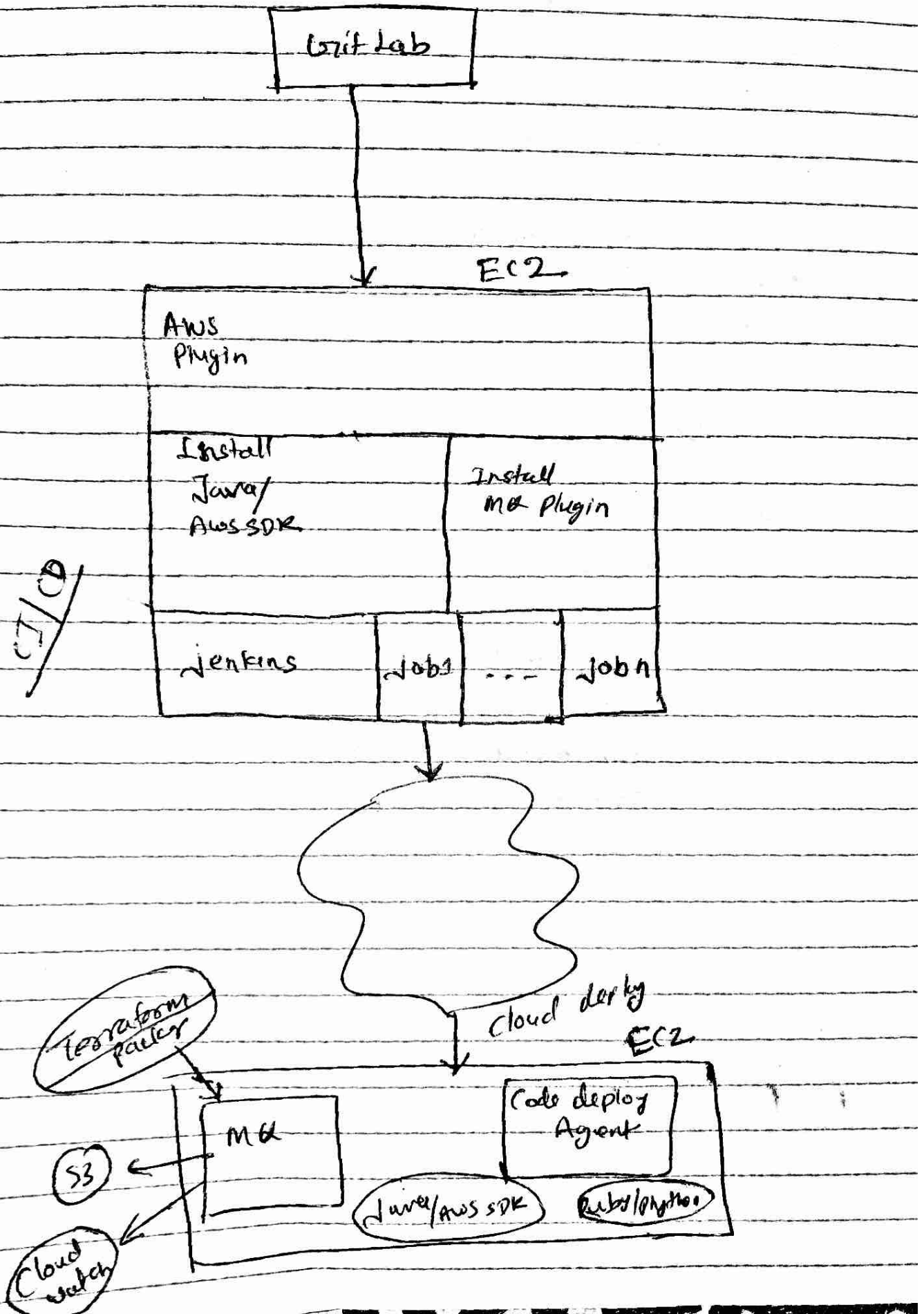
1. Service Principle
2. Git lab
3. VSTS
4. Visual Studio code

Dev Master Branch
QA
Prod

Dev — Master Branch Sync

Build
- ↳ MVN
- ↳ Java
- → Any Tool

Deploy → Configuration
Release ssh etc.


Git Lab
EC2
AWS Plugin
Install Java/ Aws SDK
Install M2 Plugin
CI/CD
Jenkins
Job1
...
Jobn
Cloud deploy
EC2
Terraform packer
M2
S3
Cloud watch
Code deploy Agent
Java/AWS SDK
Ruby/Python