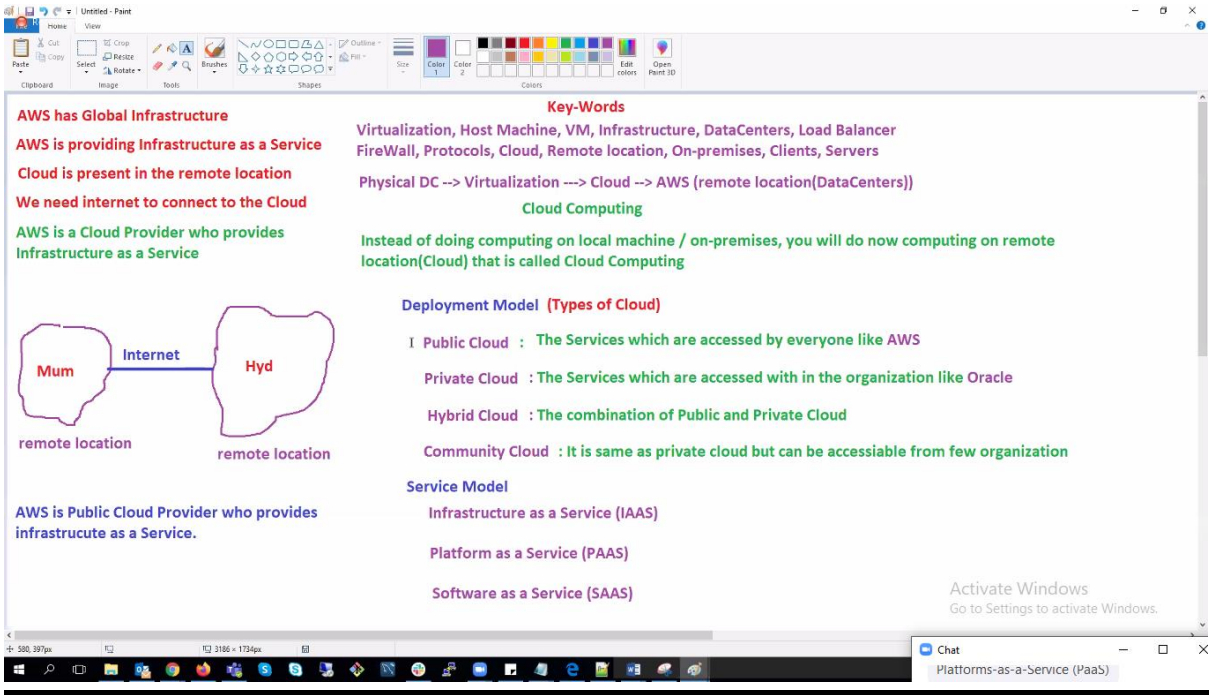
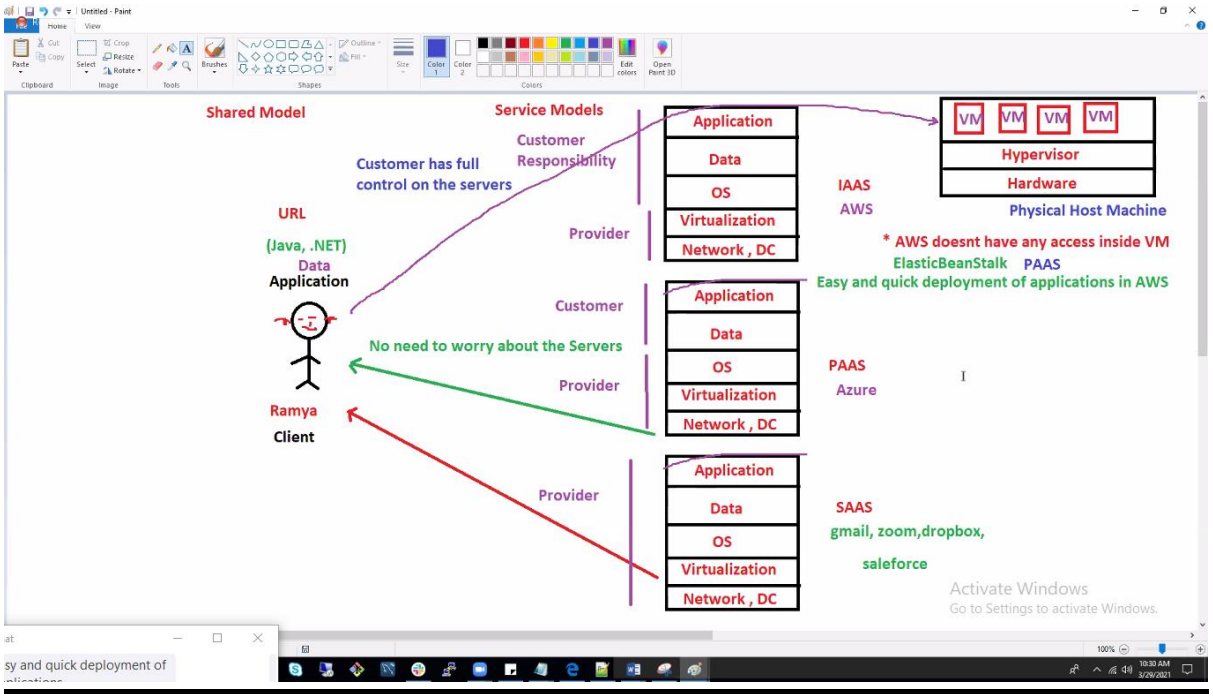
AWS


AWS has Global Infrastructure
AWS is providing Infrastructure as a Service
Cloud is present in the remote location
We need internet to connect to the Cloud
AWS is a Cloud Provider who provides Infrastructure as a Service
Key-Words
Virtualization, Host Machine, VM, Infrastructure, DataCenters, Load Balancer
FireWall, Protocols, Cloud, Remote location, On-premises, Clients, Servers
Physical DC --> Virtualization ---> Cloud --> AWS (remote location(DataCenters))
Cloud Computing
Instead of doing computing on local machine / on-premises, you will do now computing on remote location(Cloud) that is called Cloud Computing
Mum
Internet
Hyd
remote location
remote location
Deployment Model (Types of Cloud)
Public Cloud : The Services which are accessed by everyone like AWS
Private Cloud : The Services which are accessed with in the organization like Oracle
Hybrid Cloud : The combination of Public and Private Cloud
Community Cloud : It is same as private cloud but can be accessiable from few organization
Service Model
AWS is Public Cloud Provider who provides infrastrucute as a Service.
Infrastructure as a Service (IAAS)
Platform as a Service (PAAS)
Software as a Service (SAAS)
Activate Windows
Go to Settings to activate Windows.
Chat
Platforms-as-a-Service (PaaS)


Shared Model
Service Models
Customer Responsibility
Customer has full control on the servers
URL
(Java, .NET)
Data
Application
Ramya
Client
Provider
Customer
No need to worry about the Servers
Provider
Provider
Application
Data
OS
Virtualization
Network , DC
VM
VM
VM
VM
Hypervisor
Hardware
Physical Host Machine
IAAS
AWS
* AWS doesnt have any access inside VM
ElasticBeanStalk PAAS
Easy and quick deployment of applications in AWS
PAAS
Azure
SAAS
gmail, zoom,dropbox,
saleforce
Activate Windows
Go to Settings to activate Windows.
sy and quick deployment of

AWS has Global Infrastructure

A region has multiple DataCenters

A region has multiple AZ's

AZ's networks are interconnected

AZ's are in sync with each other(network) but not the DATA.

Best practise is to distribute the servers across multiple AZ's

Very less chance that 1AZ goes down

1 AZ = 1DC ✗

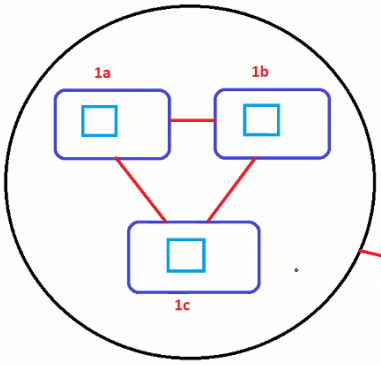
Server = Instance

AZ is a group of Datacenters

Regions and Availability Zones

Region: is a geographical area, Ex AWS-region = Mumbai

Availability Zone: Simply a DataCenter(AZ)



Every AWS region has a code

AWS Mumbai region = ap-south-1

AZ = ap-south-1a
ap-south-1b
ap-south-1c

Regions and AZ's are managed by AWS

AZ's can communicate with each other

Low Latency = good
High Latency = bad

google.com --> 1 sec
google.com --> 5 secs

network ✗ NO

AWS another region

1a	1b	1c
Andheri, juhu,vashi,	Kalyan,thane,chambur	pandra,parel,vasi

AWS Region = Mumbai

Regions dont communicate with each other by default, if required YES

LB can distribute the traffic to multiple instances across multiple AZ's

LB dosent have AZ. it is a serivce from AWS

Chat

IAM is FREE

IAM is Global

IAM - Deep Dive

IAM is used for Security Purpose

With IAM, you can control the entire AWS resources centrally

Dont Share your Email / Pwd to others

You can share AWS account by creating IAM Users

Root User --> Full Permissions

IAM User --> Limited Permissions

Permissions --> Policies

IAM users

- Babji --> EC2
- Lipsha --> S3
- Hari --> EFS
- Gouse --> BeanStalk
- Ansari --> Admin (Except Billing)

It is NOT AT ALL RECOMMENDED to use ROOT account for daily activities or work, instead use IAM user

MFA --> Multi Factor Authentication (Google Authenticator)

OPen AWS Page --> Login with Email/ PWD --> MFA Code --> Login to AWS Console

MFA is highly recommended for ROOT account and IAM user as well / Every IAM User should have MFA configured

We need to setup MFA for every individual IAM User

For IAM user, you can attach and detach the permissions / Policies

2 Ways to Access AWS

IAM Ashish EC2
- MFA Console(username/pwd)
- Programmatically(KEYS) NO MFA

Console Access
AWS Console webiste (GUI)
(email/pwd or username/pwd)
Root IAM

Programmatical Access
(CLI, SDK's, developer tools)

1 set { ACCESS KEY: SKDFBHSKFHSDKFH, SECRET KEY: SKJDFH7SDF67SDF8

Login with KEYS (Access Key and Secret Key)

It is not recommended to share the KEYS to anyone

KEYS are user specific, individual IAM users have their own keys

Create the KEYS based on the requirement, dont create it unnecessarily

KEYS also have same permissions like Console

Every IAM user can have max 2 set of KEYS

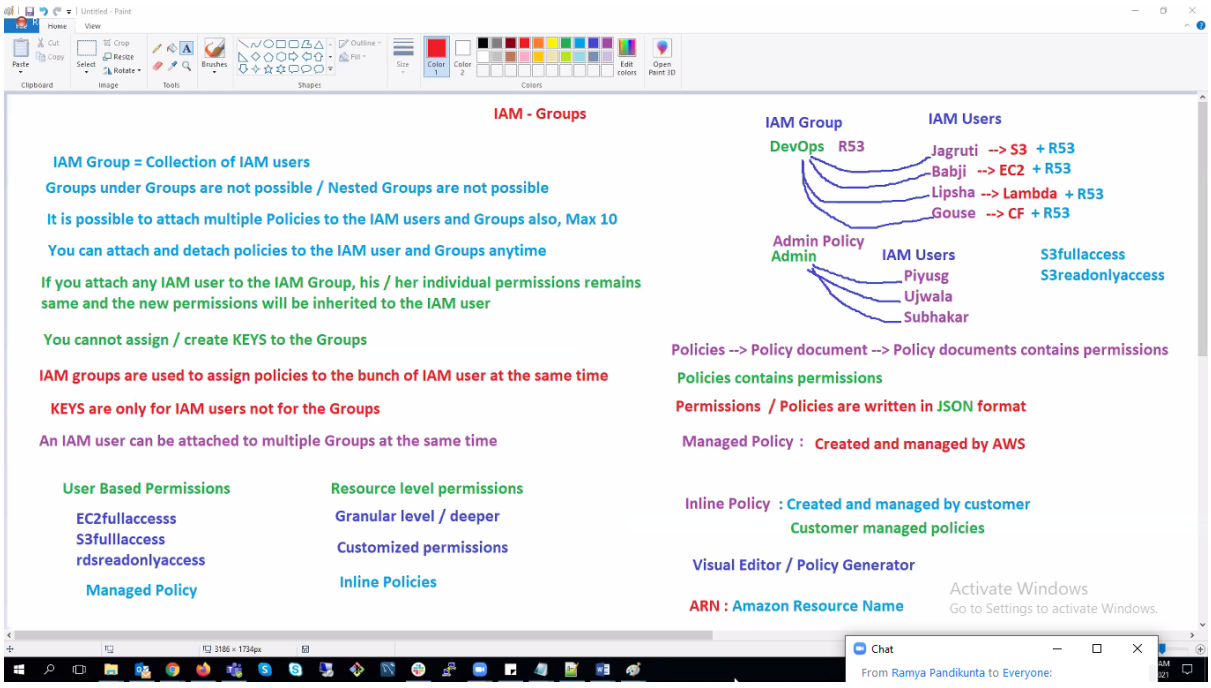
DONT Create KEYS for your ROOT account

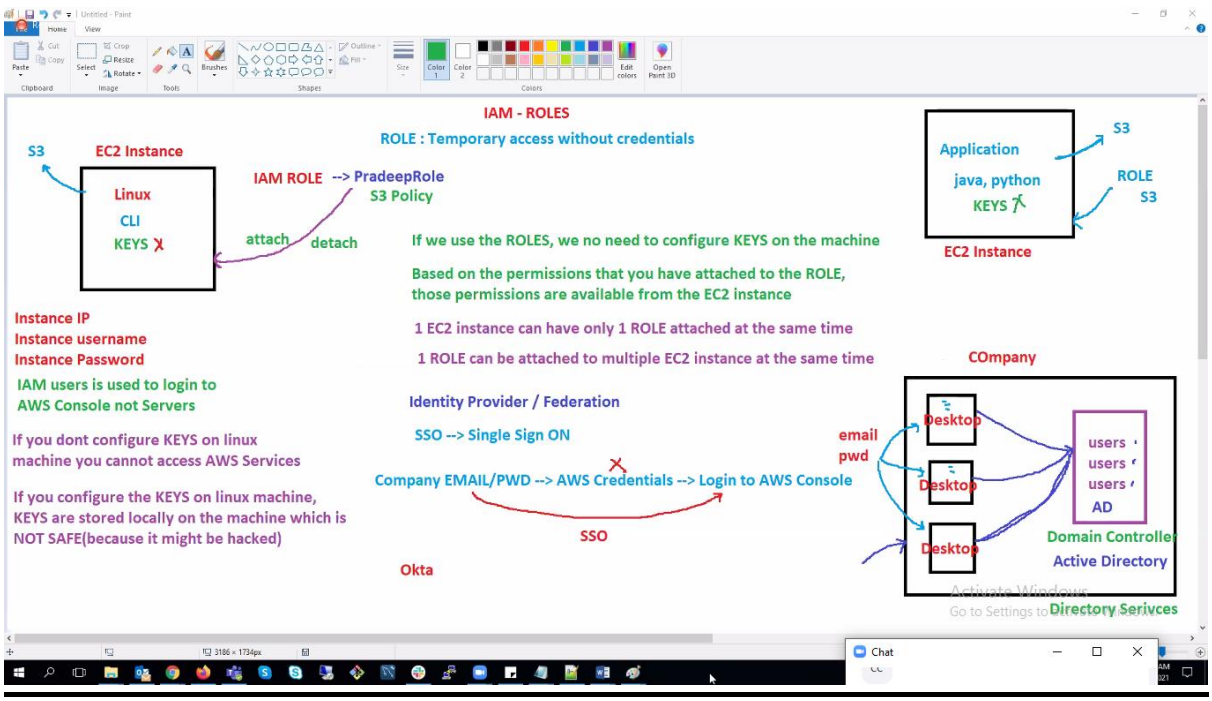
Once KEYS are lost it is lost, you cannot get the same KEYS back

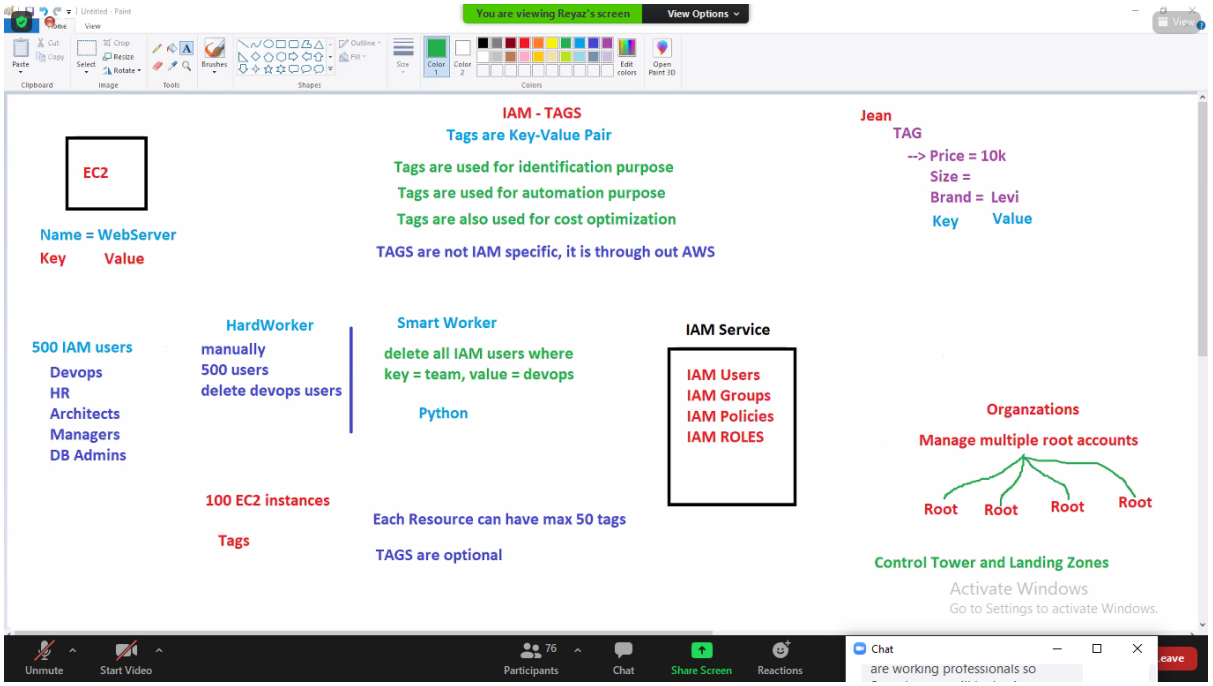
But, you can re-generatae it N number of times

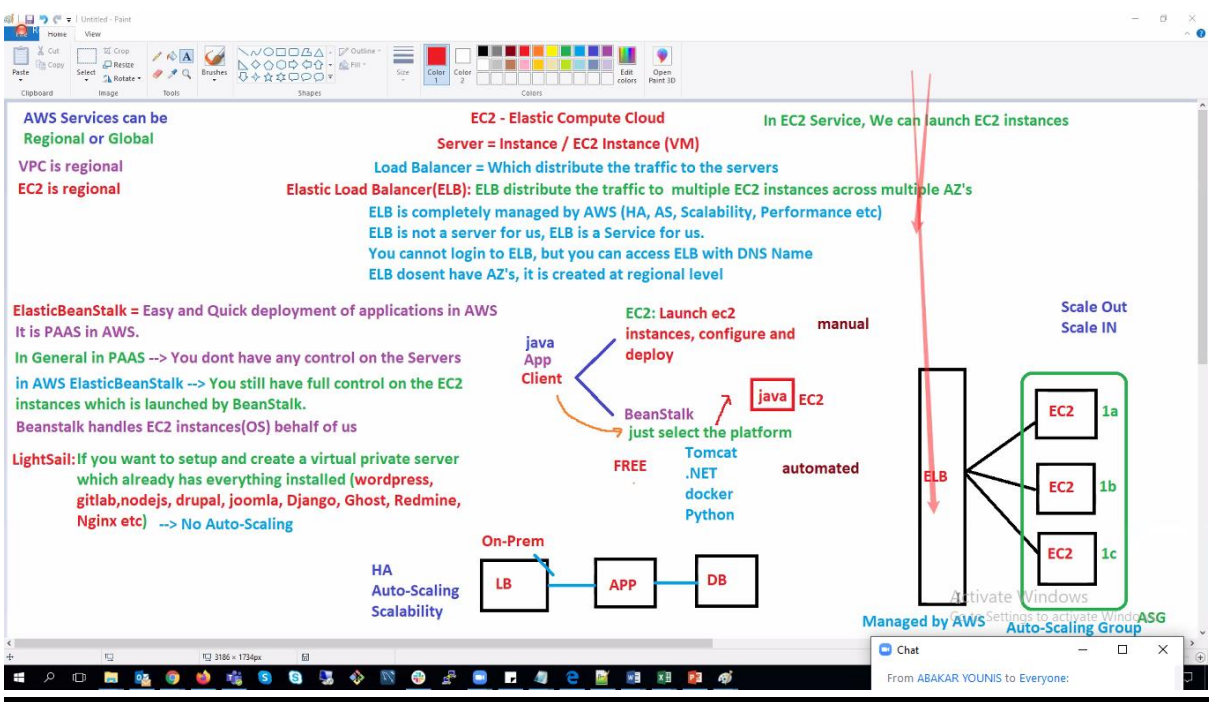
If you re-generate, you will get the new keys, you cannot get the Old keys back !!

Chat
From Ashish S to Everyone:


IAM - Groups
IAM Group = Collection of IAM users
Groups under Groups are not possible / Nested Groups are not possible
It is possible to attach multiple Policies to the IAM users and Groups also, Max 10
You can attach and detach policies to the IAM user and Groups anytime
If you attach any IAM user to the IAM Group, his / her individual permissions remains same and the new permissions will be inherited to the IAM user
You cannot assign / create KEYS to the Groups
IAM groups are used to assign policies to the bunch of IAM user at the same time
KEYS are only for IAM users not for the Groups
An IAM user can be attached to multiple Groups at the same time
User Based Permissions
EC2fullaccesss
S3fulllaccess
rdsreadonlyaccess
Managed Policy
Resource level permissions
Granular level / deeper
Customized permissions
Inline Policies
IAM Group
DevOps R53
IAM Users
Jagruti --> S3 + R53
Babji --> EC2 + R53
Lipsha --> Lambda + R53
Gouse --> CF + R53
Admin Policy
Admin
IAM Users
Piyusg
Ujwala
Subhakar
S3fullaccess
S3readonlyaccess
Policies --> Policy document --> Policy documents contains permissions
Policies contains permissions
Permissions / Policies are written in JSON format
Managed Policy : Created and managed by AWS
Inline Policy : Created and managed by customer
Customer managed policies
Visual Editor / Policy Generator
ARN : Amazon Resource Name
Activate Windows
Go to Settings to activate Windows.
Chat
From Ramya Pandikunta to Everyone:


IAM - ROLES
ROLE : Temporary access without credentials
S3
EC2 Instance
Linux
CLI
KEYS X
IAM ROLE --> PradeepRole
S3 Policy
attach
detach
If we use the ROLES, we no need to configure KEYS on the machine
Based on the permissions that you have attached to the ROLE, those permissions are available from the EC2 instance
1 EC2 instance can have only 1 ROLE attached at the same time
1 ROLE can be attached to multiple EC2 instance at the same time
Application
java, python
KEYS X
S3
ROLE
S3
EC2 Instance
Instance IP
Instance username
Instance Password
IAM users is used to login to AWS Console not Servers
If you dont configure KEYS on linux machine you cannot access AWS Services
If you configure the KEYS on linux machine, KEYS are stored locally on the machine which is NOT SAFE(because it might be hacked)
Identity Provider / Federation
SSO --> Single Sign ON
Company EMAIL/PWD --> AWS Credentials --> Login to AWS Console
SSO
Okta
COmpany
email
pwd
Desktop
Desktop
Desktop
users
users
users
AD
Domain Controller
Active Directory
Directory Serivces
Activate Windows
Go to Settings to
Chat


You are viewing Reyaz's screen
View Options
IAM - TAGS
Tags are Key-Value Pair
Tags are used for identification purpose
Tags are used for automation purpose
Tags are also used for cost optimization
TAGS are not IAM specific, it is through out AWS
EC2
Name = WebServer
Key Value
Jean
TAG
--> Price = 10k
Size =
Brand = Levi
Key Value
500 IAM users
Devops
HR
Architects
Managers
DB Admins
HardWorker
manually
500 users
delete devops users
Smart Worker
delete all IAM users where
key = team, value = devops
Python
IAM Service
IAM Users
IAM Groups
IAM Policies
IAM ROLES
Organzations
Manage multiple root accounts
Root
Root
Root
Root
100 EC2 instances
Tags
Each Resource can have max 50 tags
TAGS are optional
Control Tower and Landing Zones
Activate Windows
Go to Settings to activate Windows.
Unmute
Start Video
76
Participants
Chat
Share Screen
Reactions
Chat
are working professionals so


AWS Services can be
Regional or Global
VPC is regional
EC2 is regional
EC2 - Elastic Compute Cloud
Server = Instance / EC2 Instance (VM)
In EC2 Service, We can launch EC2 instances
Load Balancer = Which distribute the traffic to the servers
Elastic Load Balancer(ELB): ELB distribute the traffic to multiple EC2 instances across multiple AZ's
ELB is completely managed by AWS (HA, AS, Scalability, Performance etc)
ELB is not a server for us, ELB is a Service for us.
You cannot login to ELB, but you can access ELB with DNS Name
ELB dosent have AZ's, it is created at regional level
ElasticBeanStalk = Easy and Quick deployment of applications in AWS
It is PAAS in AWS.
In General in PAAS --> You dont have any control on the Servers
in AWS ElasticBeanStalk --> You still have full control on the EC2 instances which is launched by BeanStalk.
Beanstalk handles EC2 instances(OS) behalf of us
LightSail: If you want to setup and create a virtual private server which already has everything installed (wordpress, gitlab,nodejs, drupal, joomla, Django, Ghost, Redmine, Nginx etc) --> No Auto-Scaling
java
App
Client
EC2: Launch ec2 instances, configure and deploy
manual
BeanStalk
just select the platform
java
EC2
FREE
Tomcat
.NET
docker
Python
automated
On-Prem
HA
Auto-Scaling
Scalability
LB
APP
DB
Scale Out
Scale IN
ELB
EC2
1a
EC2
1b
EC2
1c
Managed by AWS
ASG
Auto-Scaling Group
Activate Windows
Chat
From ABAKAR YOUNIS to Everyone:

EC2 is regional

Servers = EC2 Instances

750 hours / month

for 1 year

EC2 - Elastic Compute Cloud

EC2 is a webservice from AWS that provides resizable compute services in the Cloud

Resizable = Scale up / Scale Down, Scale Out / Scale In

Scalability Elasticity (AS)

Price = Pay as you use

Pay every hour

5 mins --> terminated

5 mins --> terminated

2 hours

Launch

Stop --> No bill

Start

Reboot

Terminate --> No bill

Pricing Models in AWS

On-Demand Instances

Fixed Price (Hourly)

Pay for what you have used

No Commitment

No Upfront Payments

No Predictable usage

Spiky Applications

Reserved Instances

Long term commitment

1 or 3 years

Upfront payment (Full, Partial)

75% Discount on hourly price

Predictable usage

Standard RI : 75% Discount

Converitable RI: To change the capacity of the server anytime

Schedule RI: Reserve it for fraction of a day, a week or a month

Spot Instances

Bidding

Auctioning

Huge capacity for cheaper price

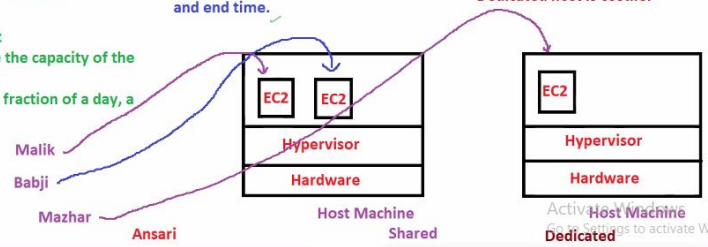
Application with start and end time.

Dedicated Host

If any customer need dedicated Physical machine

License based software

Dedicated host is costlier



EC2- Families

General Instances

Family member = Instance Type

t2.nano = 0.5GB RAM, 1 vCPU

t2.micro = 1 GB RAM, 1 vCPU

t2.small = 2 GB RAM, 2 vCPU

t2.medium = 4GB RAM

t2.large = 8GB RAM

t2.xlarge= 16 GB RAM

General Instances = For general Purpose

Family members --> Instance type

Memory Instances = If you need more memory for your applications

CPU Instances = More CPU

Storage Instances = More Storage

GPU Instances = Graphics, Heavy machines

All instance families	c5	d3en	inf1	m5n	r5	z1d
t1	c5a	f1	m1	m5zn	r5a	
t2	c5ad	g2	m2	m6g	r5ad	
t3	c5d	g3	m3	m6gd	r5d	
t3a	c5n	g3s	m4	mac1	r5dn	
t4g	c6g	g4dn	m5	p2	r5n	
a1	c6gd	h1	m5a	p3	r6g	
c1	cc2	i2	m5ad	p3dn	r6gd	
c3	d2	i3	m5d	r3	x1	
c4	d3	i3en	m5dn	r4	x1e	

Scalability = Increasing the capacity of the Instances

Scalability can be achieved by changing the instance type

Anytime Scale UP --> NO DATA LOST

Anytime Scale Down --> NO DATA LOST

EC2 2GB

t2.micro

t2.large

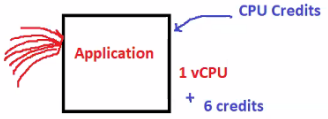
You should STOP the EC2 instance to change the instance type

If you change the instance type, data in the instance will NOT BE LOST

Burstable Performance instances

NOT FREE = BILL = Charged = Paid Service

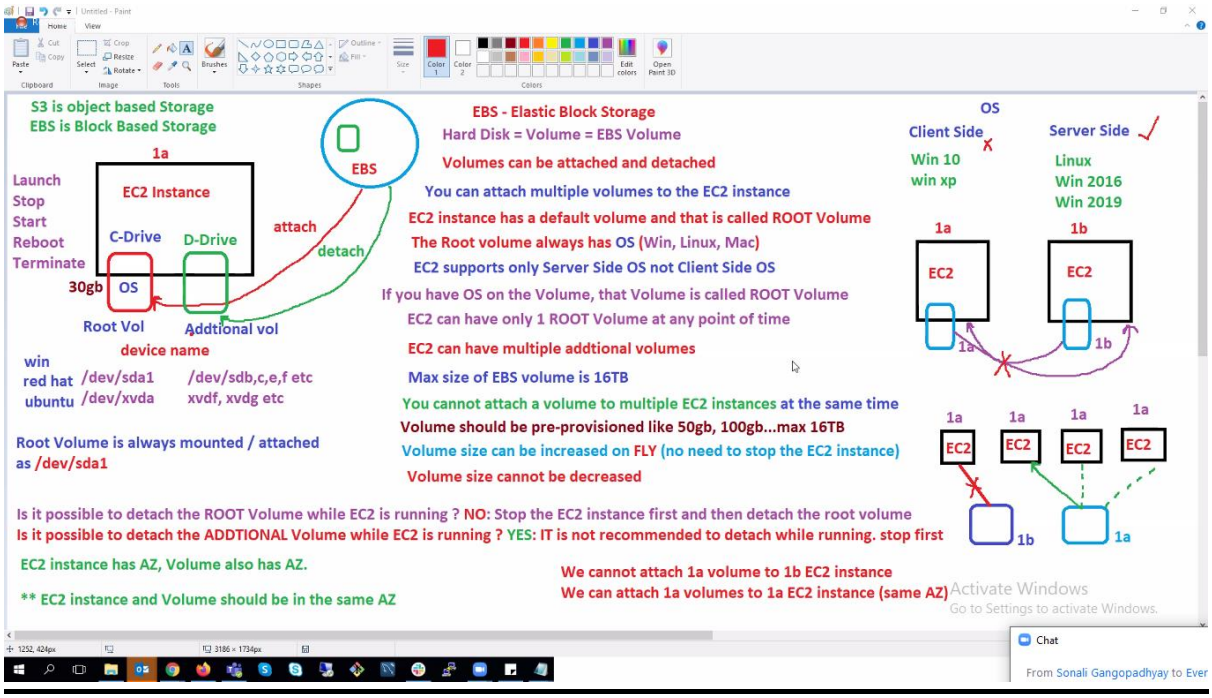
EC2 instance will enter into burstable mode and give high performance for limited period of time only

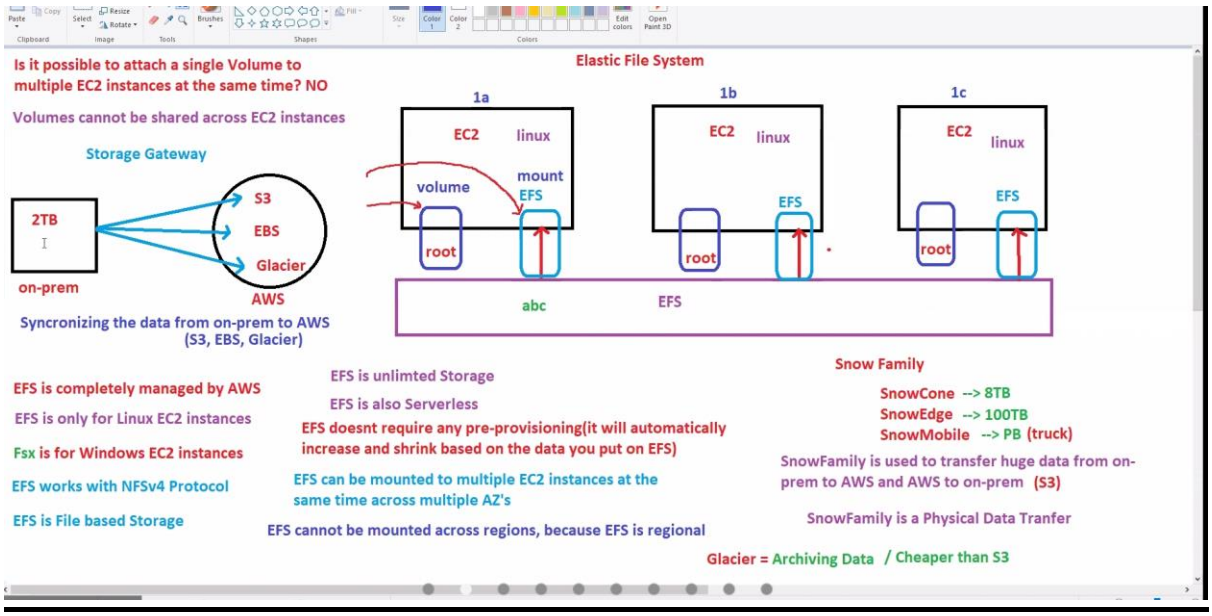


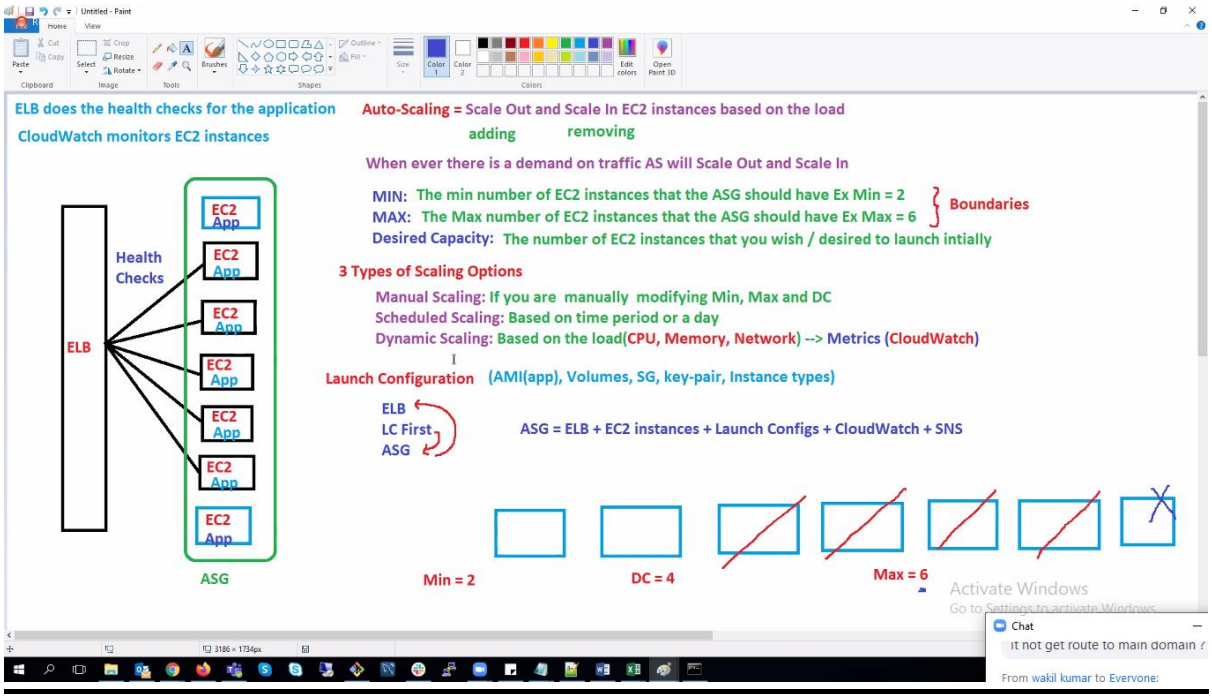
Only few instances supports burstable mode

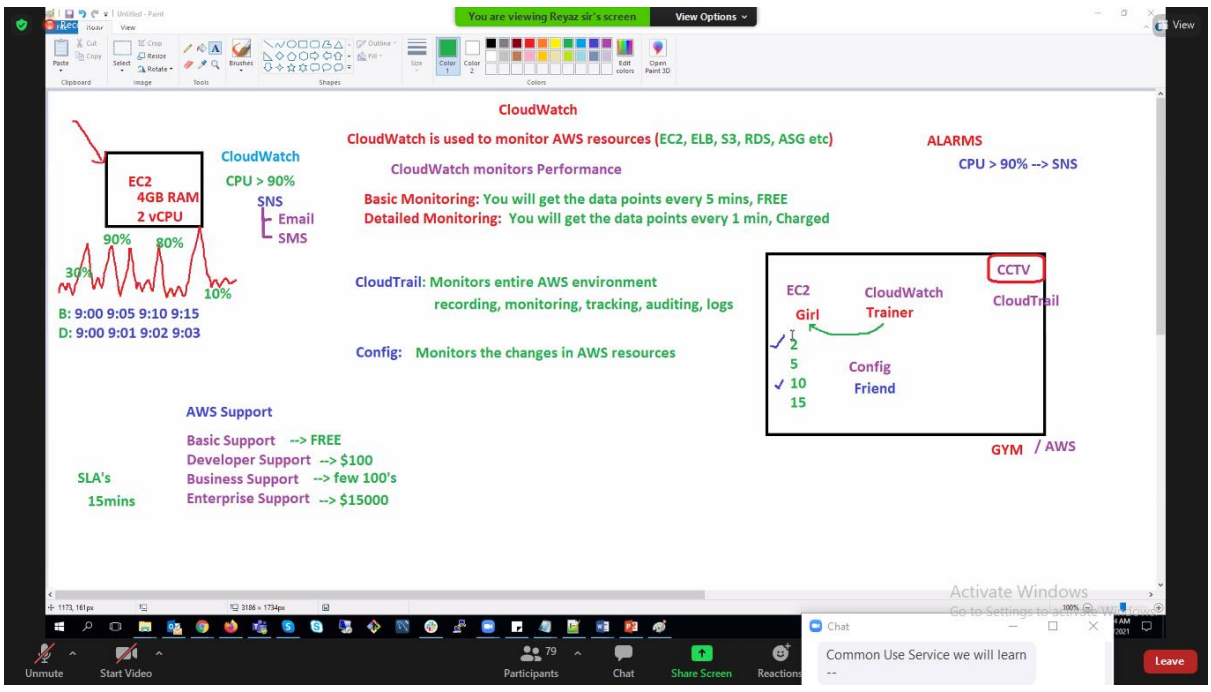
t2, t3

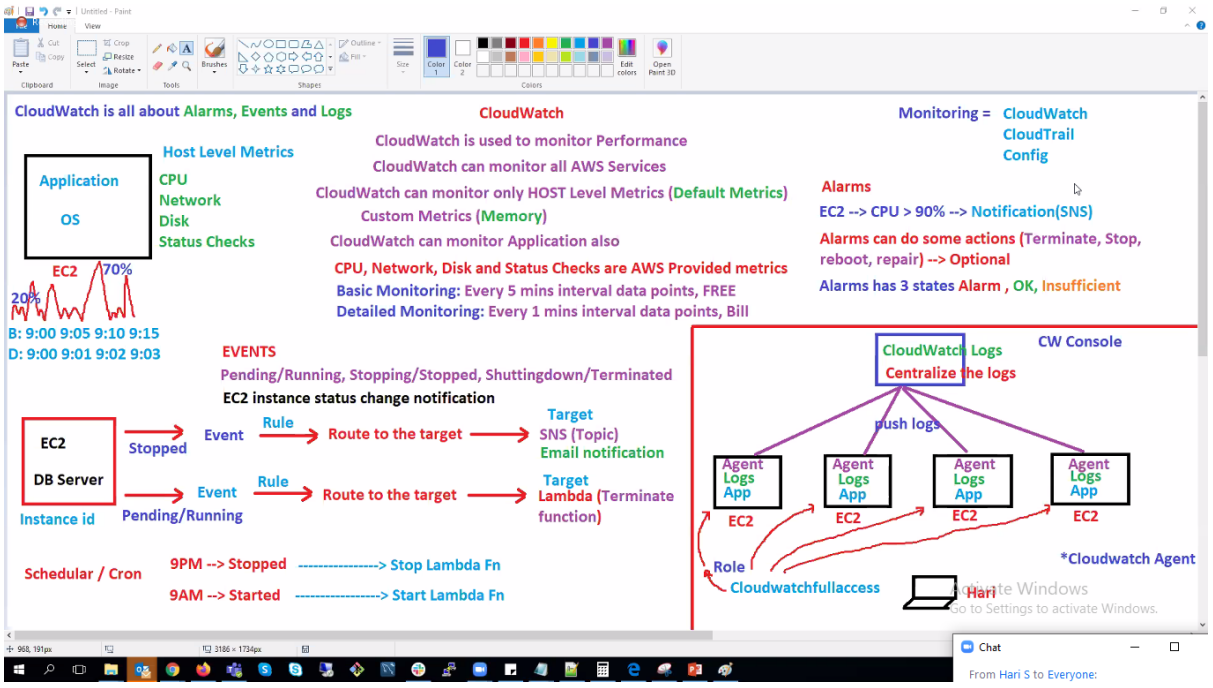
Credits depend upon instance type

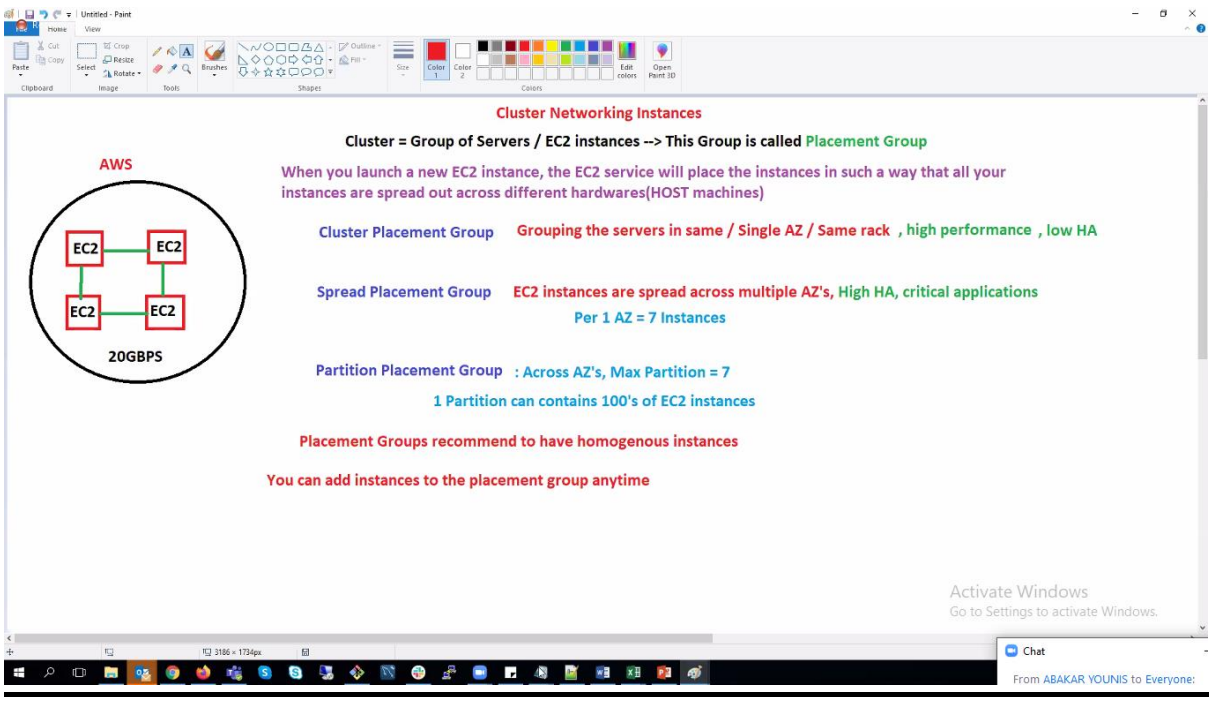

S3 is object based Storage
EBS is Block Based Storage
EBS - Elastic Block Storage
Hard Disk = Volume = EBS Volume
Volumes can be attached and detached
You can attach multiple volumes to the EC2 instance
EC2 instance has a default volume and that is called ROOT Volume
The Root volume always has OS (Win, Linux, Mac)
EC2 supports only Server Side OS not Client Side OS
If you have OS on the Volume, that Volume is called ROOT Volume
EC2 can have only 1 ROOT Volume at any point of time
EC2 can have multiple addtional volumes
Max size of EBS volume is 16TB
You cannot attach a volume to multiple EC2 instances at the same time
Volume should be pre-provisioned like 50gb, 100gb...max 16TB
Volume size can be increased on FLY (no need to stop the EC2 instance)
Volume size cannot be decreased
1a
EC2 Instance
Launch
Stop
Start
Reboot
Terminate
C-Drive
D-Drive
30gb
OS
EBS
attach
detach
Root Vol
Addtional vol
device name
win
red hat /dev/sda1 /dev/sdb,c,e,f etc
ubuntu /dev/xvda xvdf, xvdg etc
Root Volume is always mounted / attached as /dev/sda1
OS
Client Side
Server Side
Win 10
win xp
Linux
Win 2016
Win 2019
1a
1b
EC2
EC2
1a
1b
1a
1a
1a
1a
EC2
EC2
EC2
EC2
1b
1a
Is it possible to detach the ROOT Volume while EC2 is running ? NO: Stop the EC2 instance first and then detach the root volume
Is it possible to detach the ADDTIONAL Volume while EC2 is running ? YES: IT is not recommended to detach while running. stop first
EC2 instance has AZ, Volume also has AZ.
** EC2 instance and Volume should be in the same AZ
We cannot attach 1a volume to 1b EC2 instance
We can attach 1a volumes to 1a EC2 instance (same AZ)
Activate Windows
Go to Settings to activate Windows.
Chat
From Sonali Gangopadhyay to Ever

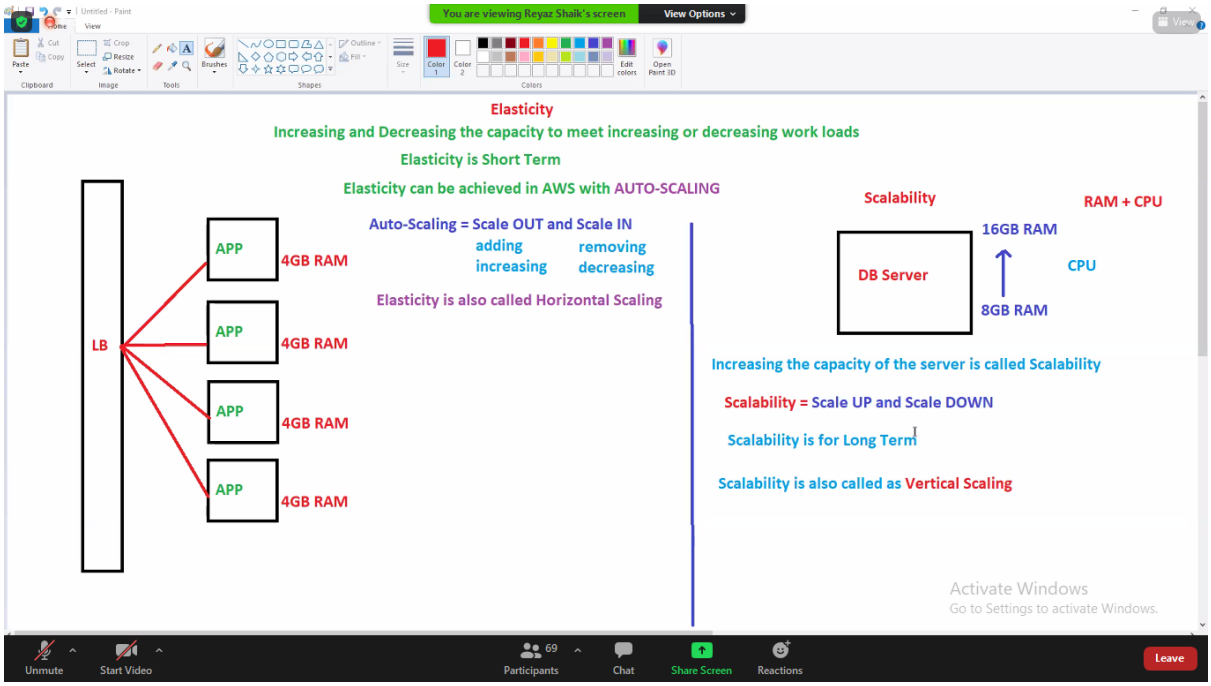

Is it possible to attach a single Volume to multiple EC2 instances at the same time? NO
Volumes cannot be shared across EC2 instances
Storage Gateway
2TB
on-prem
S3
EBS
Glacier
AWS
Syncronizing the data from on-prem to AWS (S3, EBS, Glacier)
Elastic File System
1a
1b
1c
EC2
linux
volume
mount
EFS
root
abc
EFS
EFS is completely managed by AWS
EFS is only for Linux EC2 instances
Fsx is for Windows EC2 instances
EFS works with NFSv4 Protocol
EFS is File based Storage
EFS is unlimted Storage
EFS is also Serverless
EFS doesnt require any pre-provisioning(it will automatically increase and shrink based on the data you put on EFS)
EFS can be mounted to multiple EC2 instances at the same time across multiple AZ's
EFS cannot be mounted across regions, because EFS is regional
Snow Family
SnowCone --> 8TB
SnowEdge --> 100TB
SnowMobile --> PB (truck)
SnowFamily is used to transfer huge data from on-prem to AWS and AWS to on-prem (S3)
SnowFamily is a Physical Data Tranfer
Glacier = Archiving Data / Cheaper than S3

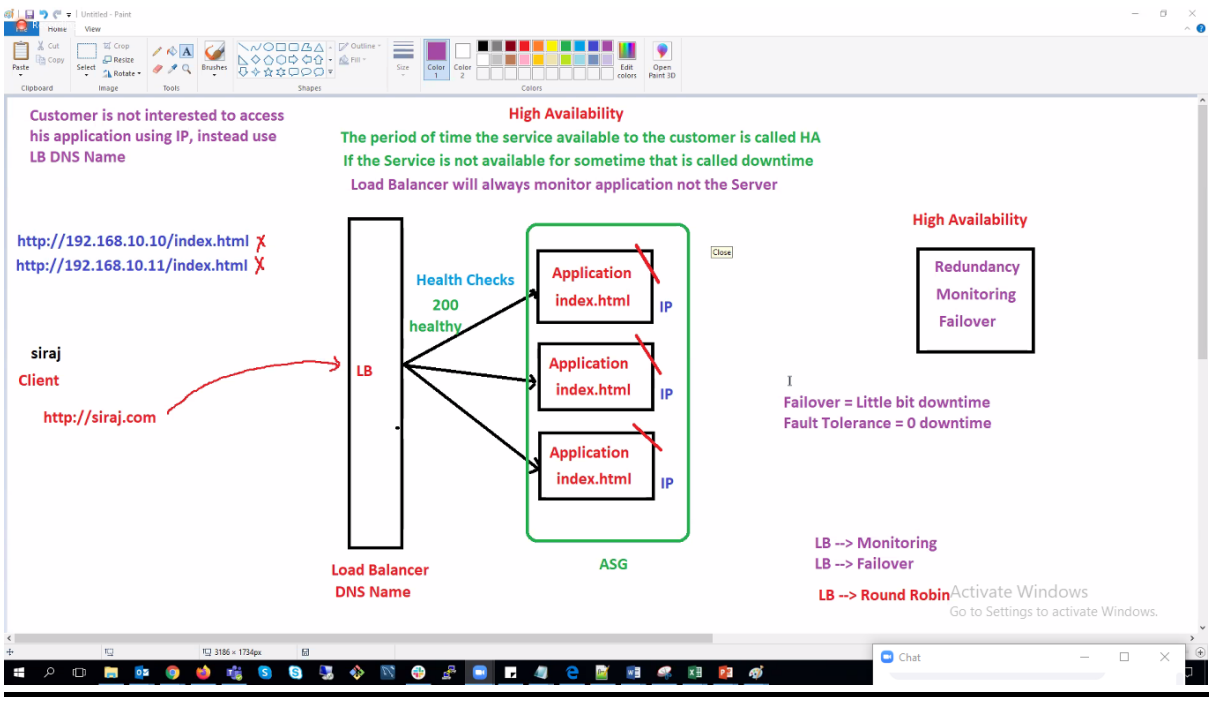

ELB does the health checks for the application
CloudWatch monitors EC2 instances
Auto-Scaling = Scale Out and Scale In EC2 instances based on the load
adding
removing
When ever there is a demand on traffic AS will Scale Out and Scale In
MIN: The min number of EC2 instances that the ASG should have Ex Min = 2
MAX: The Max number of EC2 instances that the ASG should have Ex Max = 6
Boundaries
Desired Capacity: The number of EC2 instances that you wish / desired to launch intially
3 Types of Scaling Options
Manual Scaling: If you are manually modifying Min, Max and DC
Scheduled Scaling: Based on time period or a day
Dynamic Scaling: Based on the load(CPU, Memory, Network) --> Metrics (CloudWatch)
Launch Configuration (AMI(app), Volumes, SG, key-pair, Instance types)
ELB
LC First
ASG
ASG = ELB + EC2 instances + Launch Configs + CloudWatch + SNS
ELB
Health Checks
EC2 App
EC2 App
EC2 App
EC2 App
EC2 App
EC2 App
ASG
Min = 2
DC = 4
Max = 6
Activate Windows
Chat
From wakil kumar to Everyone:

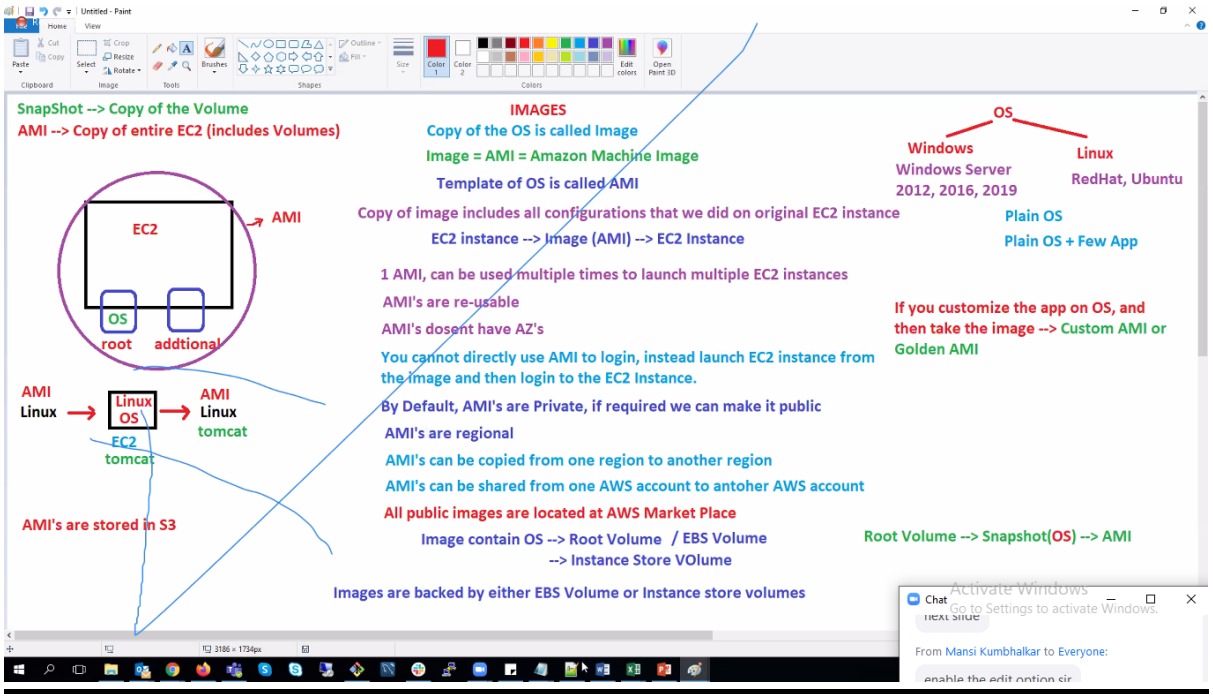

You are viewing Reyaz sir's screen
View Options
CloudWatch
CloudWatch is used to monitor AWS resources (EC2, ELB, S3, RDS, ASG etc)
CloudWatch monitors Performance
Basic Monitoring: You will get the data points every 5 mins, FREE
Detailed Monitoring: You will get the data points every 1 min, Charged
ALARMS
CPU > 90% --> SNS
EC2
4GB RAM
2 vCPU
CloudWatch
CPU > 90%
SNS
Email
SMS
90%
80%
30%
10%
B: 9:00 9:05 9:10 9:15
D: 9:00 9:01 9:02 9:03
CloudTrail: Monitors entire AWS environment
recording, monitoring, tracking, auditing, logs
Config: Monitors the changes in AWS resources
CCTV
EC2
Girl
CloudWatch
Trainer
CloudTrail
2
5
10
15
Config
Friend
GYM / AWS
AWS Support
Basic Support --> FREE
Developer Support --> $100
Business Support --> few 100's
Enterprise Support --> $15000
SLA's
15mins
Activate Windows
Chat
Common Use Service we will learn
Unmute
Start Video
Participants
Chat
Share Screen
Reactions
Leave

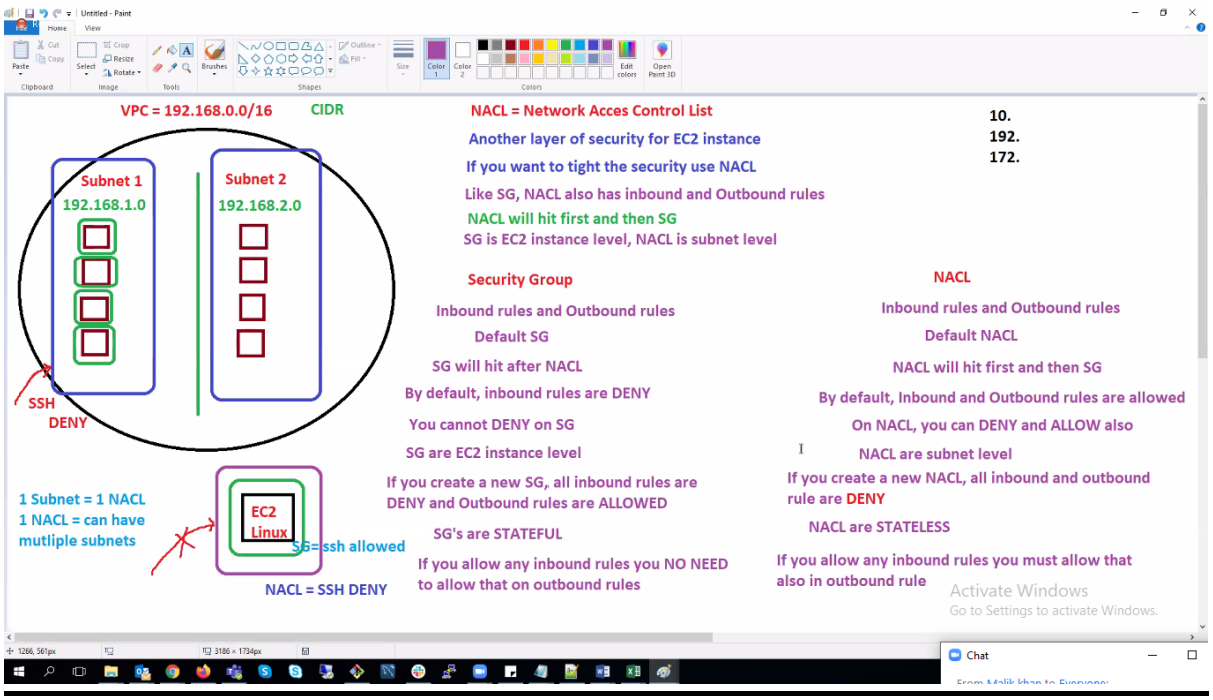

CloudWatch is all about Alarms, Events and Logs
CloudWatch
Monitoring = CloudWatch CloudTrail Config
Host Level Metrics
CPU
Network
Disk
Status Checks
Application
OS
EC2
70%
20%
B: 9:00 9:05 9:10 9:15
D: 9:00 9:01 9:02 9:03
CloudWatch is used to monitor Performance
CloudWatch can monitor all AWS Services
CloudWatch can monitor only HOST Level Metrics (Default Metrics)
Custom Metrics (Memory)
CloudWatch can monitor Application also
CPU, Network, Disk and Status Checks are AWS Provided metrics
Basic Monitoring: Every 5 mins interval data points, FREE
Detailed Monitoring: Every 1 mins interval data points, Bill
Alarms
EC2 --> CPU > 90% --> Notification(SNS)
Alarms can do some actions (Terminate, Stop, reboot, repair) --> Optional
Alarms has 3 states Alarm , OK, Insufficient
EVENTS
Pending/Running, Stopping/Stopped, Shuttingdown/Terminated
EC2 instance status change notification
EC2
DB Server
Instance id
Stopped
Event
Rule
Route to the target
Target
SNS (Topic)
Email notification
Pending/Running
Event
Rule
Route to the target
Target
Lambda (Terminate function)
Schedular / Cron
9PM --> Stopped ----------> Stop Lambda Fn
9AM --> Started ----------> Start Lambda Fn
CW Console
CloudWatch Logs
Centralize the logs
push logs
Agent Logs App
EC2
Role
Cloudwatchfullaccess
*Cloudwatch Agent
Hari
Activate Windows
Go to Settings to activate Windows.
Chat
From Hari S to Everyone:

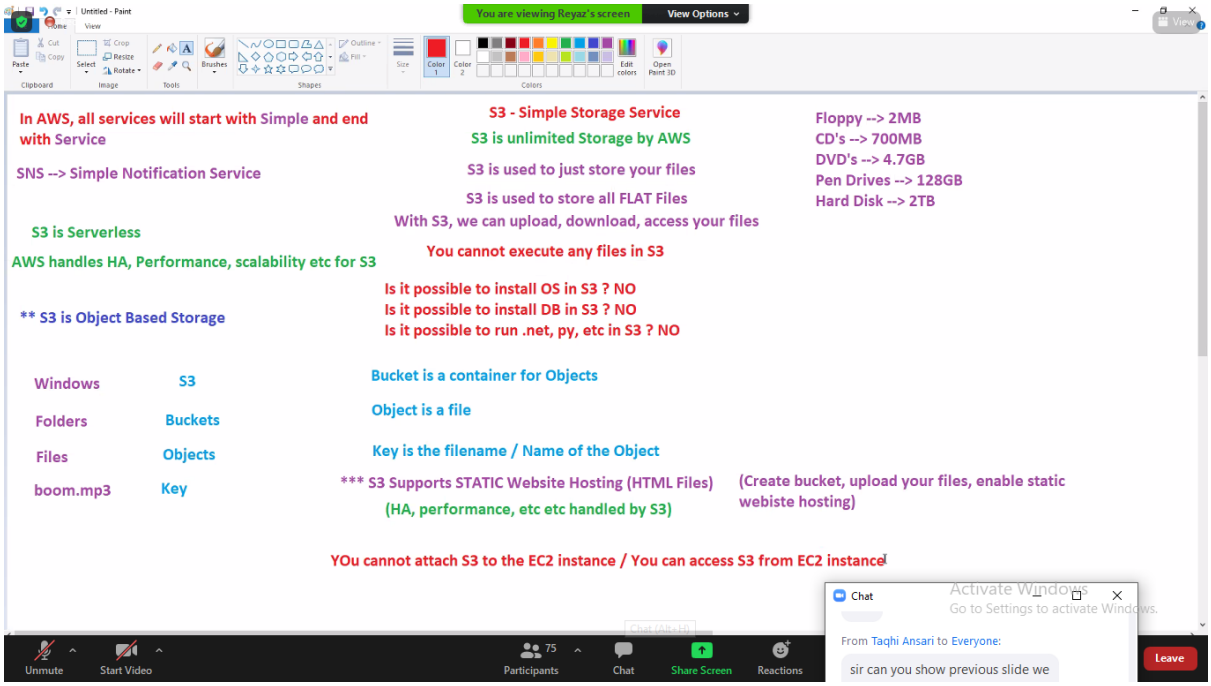

Cluster Networking Instances
Cluster = Group of Servers / EC2 instances --> This Group is called Placement Group
AWS
EC2
EC2
EC2
EC2
20GBPS
When you launch a new EC2 instance, the EC2 service will place the instances in such a way that all your instances are spread out across different hardwares(HOST machines)
Cluster Placement Group
Grouping the servers in same / Single AZ / Same rack , high performance , low HA
Spread Placement Group
EC2 instances are spread across multiple AZ's, High HA, critical applications
Per 1 AZ = 7 Instances
Partition Placement Group
: Across AZ's, Max Partition = 7
1 Partition can contains 100's of EC2 instances
Placement Groups recommend to have homogenous instances
You can add instances to the placement group anytime
Activate Windows
Go to Settings to activate Windows.
Chat
From ABAKAR YOUNIS to Everyone:

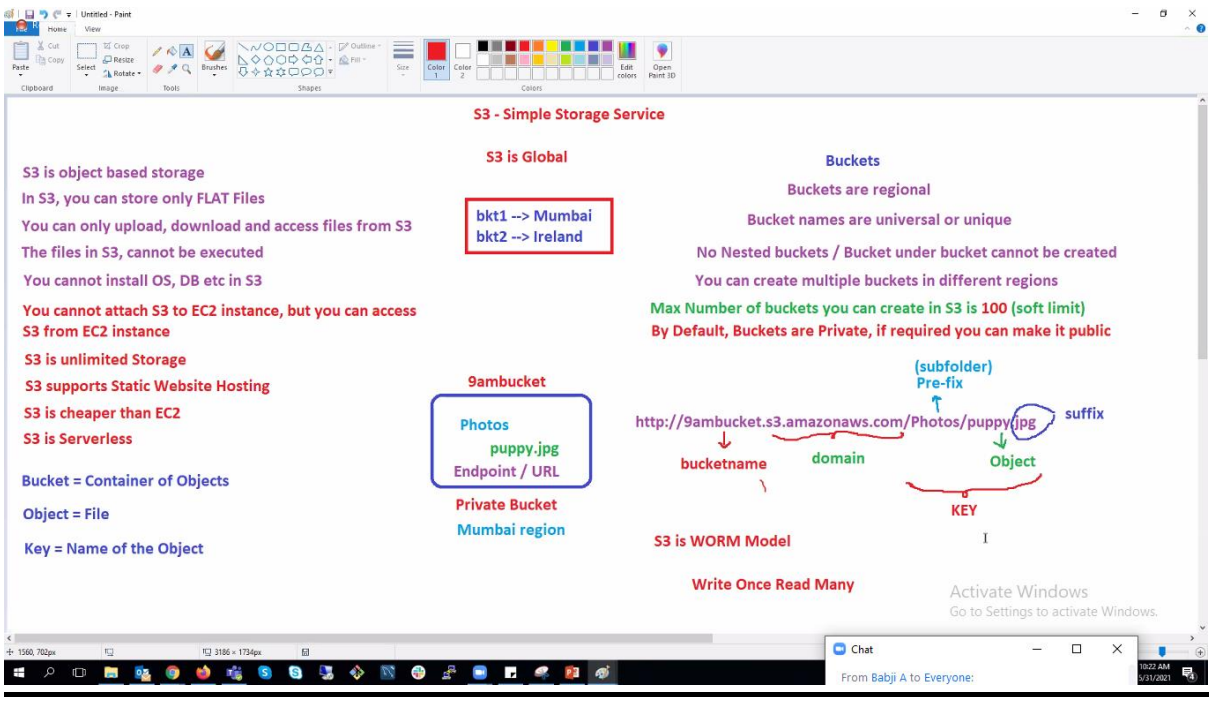

You are viewing Reyaz Shaik's screen
View Options
Elasticity
Increasing and Decreasing the capacity to meet increasing or decreasing work loads
Elasticity is Short Term
Elasticity can be achieved in AWS with AUTO-SCALING
LB
APP
4GB RAM
APP
4GB RAM
APP
4GB RAM
APP
4GB RAM
Auto-Scaling = Scale OUT and Scale IN
adding
increasing
removing
decreasing
Elasticity is also called Horizontal Scaling
Scalability
RAM + CPU
DB Server
16GB RAM
CPU
8GB RAM
Increasing the capacity of the server is called Scalability
Scalability = Scale UP and Scale DOWN
Scalability is for Long Term
Scalability is also called as Vertical Scaling
Activate Windows
Go to Settings to activate Windows.
Unmute
Start Video
69
Participants
Chat
Share Screen
Reactions
Leave


Customer is not interested to access his application using IP, instead use LB DNS Name
High Availability
The period of time the service available to the customer is called HA
If the Service is not available for sometime that is called downtime
Load Balancer will always monitor application not the Server
http://192.168.10.10/index.html
http://192.168.10.11/index.html
siraj
Client
http://siraj.com
LB
Health Checks
200
healthy
Application
index.html
IP
Application
index.html
IP
Application
index.html
IP
Load Balancer
DNS Name
ASG
High Availability
Redundancy
Monitoring
Failover
Failover = Little bit downtime
Fault Tolerance = 0 downtime
LB --> Monitoring
LB --> Failover
LB --> Round Robin
Activate Windows
Go to Settings to activate Windows.
Chat


SnapShot --> Copy of the Volume
AMI --> Copy of entire EC2 (includes Volumes)
IMAGES
Copy of the OS is called Image
Image = AMI = Amazon Machine Image
Template of OS is called AMI
Copy of image includes all configurations that we did on original EC2 instance
EC2 instance --> Image (AMI) --> EC2 Instance
OS
Windows
Windows Server 2012, 2016, 2019
Linux
RedHat, Ubuntu
Plain OS
Plain OS + Few App
EC2
AMI
OS
root
addtional
1 AMI, can be used multiple times to launch multiple EC2 instances
AMI's are re-usable
AMI's dosent have AZ's
If you customize the app on OS, and then take the image --> Custom AMI or Golden AMI
You cannot directly use AMI to login, instead launch EC2 instance from the image and then login to the EC2 Instance.
AMI Linux
Linux OS
AMI Linux tomcat
EC2 tomcat
By Default, AMI's are Private, if required we can make it public
AMI's are regional
AMI's can be copied from one region to another region
AMI's can be shared from one AWS account to antoher AWS account
All public images are located at AWS Market Place
AMI's are stored in S3
Image contain OS --> Root Volume / EBS Volume
--> Instance Store VOlume
Root Volume --> Snapshot(OS) --> AMI
Images are backed by either EBS Volume or Instance store volumes
Activate Windows
Go to Settings to activate Windows.
Chat
From Mansi Kumbhalkar to Everyone:


VPC = 192.168.0.0/16
CIDR
NACL = Network Acces Control List
Another layer of security for EC2 instance
If you want to tight the security use NACL
Like SG, NACL also has inbound and Outbound rules
NACL will hit first and then SG
SG is EC2 instance level, NACL is subnet level
10.
192.
172.
Subnet 1
192.168.1.0
Subnet 2
192.168.2.0
SSH
DENY
Security Group
Inbound rules and Outbound rules
Default SG
SG will hit after NACL
By default, inbound rules are DENY
You cannot DENY on SG
SG are EC2 instance level
If you create a new SG, all inbound rules are DENY and Outbound rules are ALLOWED
SG's are STATEFUL
If you allow any inbound rules you NO NEED to allow that on outbound rules
NACL
Inbound rules and Outbound rules
Default NACL
NACL will hit first and then SG
By default, Inbound and Outbound rules are allowed
On NACL, you can DENY and ALLOW also
NACL are subnet level
If you create a new NACL, all inbound and outbound rule are DENY
NACL are STATELESS
If you allow any inbound rules you must allow that also in outbound rule
1 Subnet = 1 NACL
1 NACL = can have mutliple subnets
EC2 Linux
SG=ssh allowed
NACL = SSH DENY
Activate Windows
Go to Settings to activate Windows.
Chat


You are viewing Reyaz's screen
View Options
In AWS, all services will start with Simple and end with Service
SNS --> Simple Notification Service
S3 is Serverless
AWS handles HA, Performance, scalability etc for S3
** S3 is Object Based Storage
S3 - Simple Storage Service
S3 is unlimited Storage by AWS
S3 is used to just store your files
S3 is used to store all FLAT Files
With S3, we can upload, download, access your files
You cannot execute any files in S3
Is it possible to install OS in S3 ? NO
Is it possible to install DB in S3 ? NO
Is it possible to run .net, py, etc in S3 ? NO
Floppy --> 2MB
CD's --> 700MB
DVD's --> 4.7GB
Pen Drives --> 128GB
Hard Disk --> 2TB
Windows S3
Folders Buckets
Files Objects
boom.mp3 Key
Bucket is a container for Objects
Object is a file
Key is the filename / Name of the Object
*** S3 Supports STATIC Website Hosting (HTML Files)
(HA, performance, etc etc handled by S3)
(Create bucket, upload your files, enable static webiste hosting)
YOu cannot attach S3 to the EC2 instance / You can access S3 from EC2 instance
Chat
From Taqhi Ansari to Everyone:
sir can you show previous slide we
Unmute
Start Video
Participants
Chat
Share Screen
Reactions
Leave


S3 - Simple Storage Service
S3 is object based storage
In S3, you can store only FLAT Files
You can only upload, download and access files from S3
The files in S3, cannot be executed
You cannot install OS, DB etc in S3
You cannot attach S3 to EC2 instance, but you can access S3 from EC2 instance
S3 is unlimited Storage
S3 supports Static Website Hosting
S3 is cheaper than EC2
S3 is Serverless
Bucket = Container of Objects
Object = File
Key = Name of the Object
S3 is Global
bkt1 --> Mumbai
bkt2 --> Ireland
9ambucket
Photos
puppy.jpg
Endpoint / URL
Private Bucket
Mumbai region
Buckets
Buckets are regional
Bucket names are universal or unique
No Nested buckets / Bucket under bucket cannot be created
You can create multiple buckets in different regions
Max Number of buckets you can create in S3 is 100 (soft limit)
By Default, Buckets are Private, if required you can make it public
(subfolder)
Pre-fix
http://9ambucket.s3.amazonaws.com/Photos/puppy.jpg
suffix
bucketname
domain
Object
KEY
S3 is WORM Model
Write Once Read Many
Chat
From Babji A to Everyone:

While uploading the objects into S3 selecting the storage class is mandatory

Storage Classes

Availability = Anytime

Durability = Long Time

Standard Frequently Access (FA)

This is used for frequently access data.

Default Storage Class

Regular purpose(websites, images, files, storage)

No Retrival Charges

Availability: 99.99%

Durability: 11 9's

Min Object Size = 0 bytes

Standard Infrequently Access (IA)

This is used for infrequently access data.

Cheaper than FA

Retrival Charges apply

Demand rapid access

Availability: 99.9%

Durability: 11 9's

Min Object Size = 128KB

Min Duration = 30 days

Reduced Redundancy Storage (RRS)

Frequently access but NOT CRITICAL

No Retrival charges

AWS does not recommend to use this storage class

Cheaper than others

Availability: 99.99%

Durability: 99.99%

One Zone IA

Infrequently access but NOT CRITICAL

Retirval Charges

Availability: 99.5 %

Durability: 11 9's

Min Object Size = 128KB

Min Duration = 30 days

Intelligent Tiering

Unknown access patterns

Availability: 99.9%

Durability: 11 9's

Min Duration = 30 days

Glacier

Infrequently access data

Archiving Purpose

Vault: Container of archives

Archives: Objects/Archives - 40TB

Unlimited number of archives

1000 Vaults

Retrival charges apply

Glacier has retrival options

Expedited: 1 to 5 mins

Standard: 3 to 5 hours

Bulk: 5 to 12 hours

Availability: 99.99%

Durability: 11 9's

Min Duration = 90 days

Deeper Glacier = 180 days

Life Cycle Management

It is possible to move the objects from one storage class to another storage class

Life Cycle Rules

Chat

From punam biswal to Everyone:

AWS has Global Infrastructure

A region has multiple DataCenters

A region has multiple AZ's

AZ's networks are interconnected

AZ's are in sync with each other(network) but not the DATA.

Best practise is to distribute the servers across multiple AZ's

Very less chance that 1AZ goes down

1 AZ = 1DC ✗

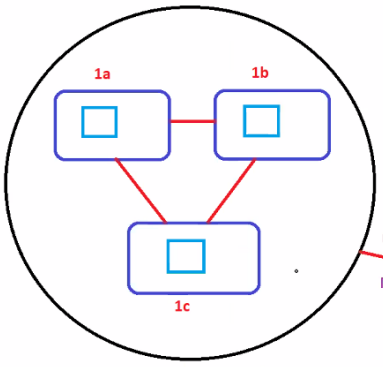
Server = Instance

AZ is a group of Datacenters

Regions and Availability Zones

Region: is a geographical area, Ex AWS-region = Mumbai

Availability Zone: Simply a DataCenter(AZ)



Every AWS region has a code

AWS Mumbai region = ap-south-1

AZ = ap-south-1a

ap-south-1b

ap-south-1c

Regions and AZ's are managed by AWS

AZ's can communicate with each other

Low Latency = good

High Latency = bad

google.com --> 1 sec

google.com --> 5 secs

network

NO

AWS another region

AWS Region = Mumbai

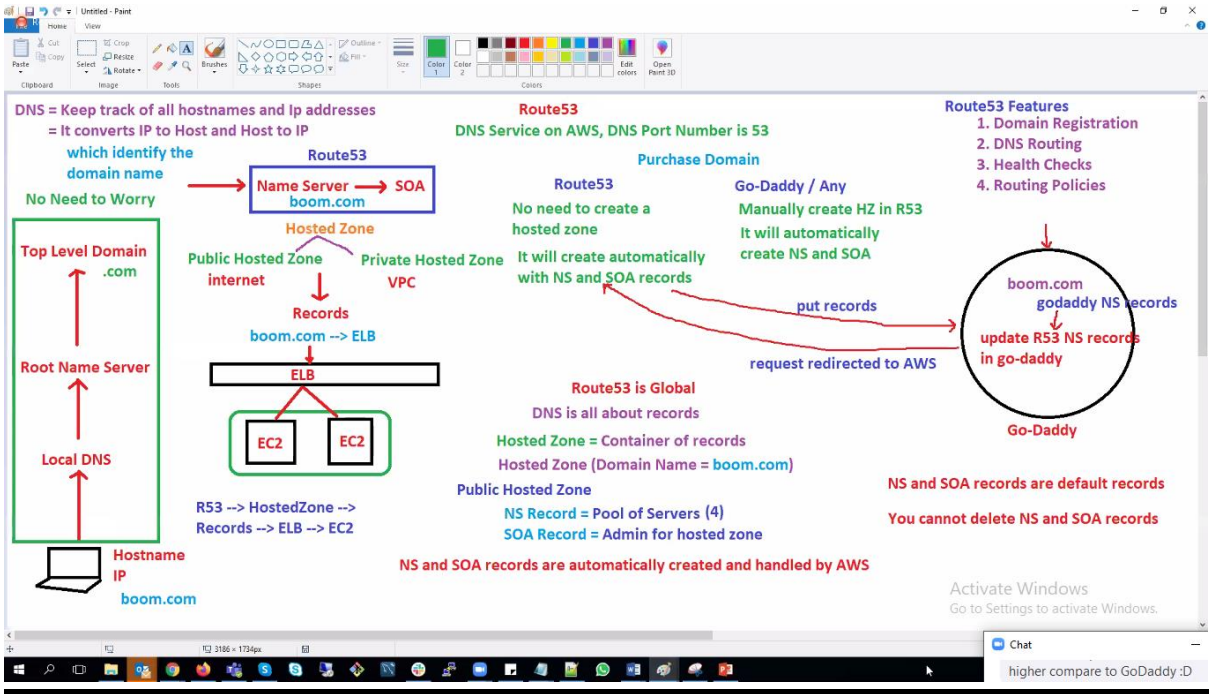
Regions dont communicate with each other by default, if required YES

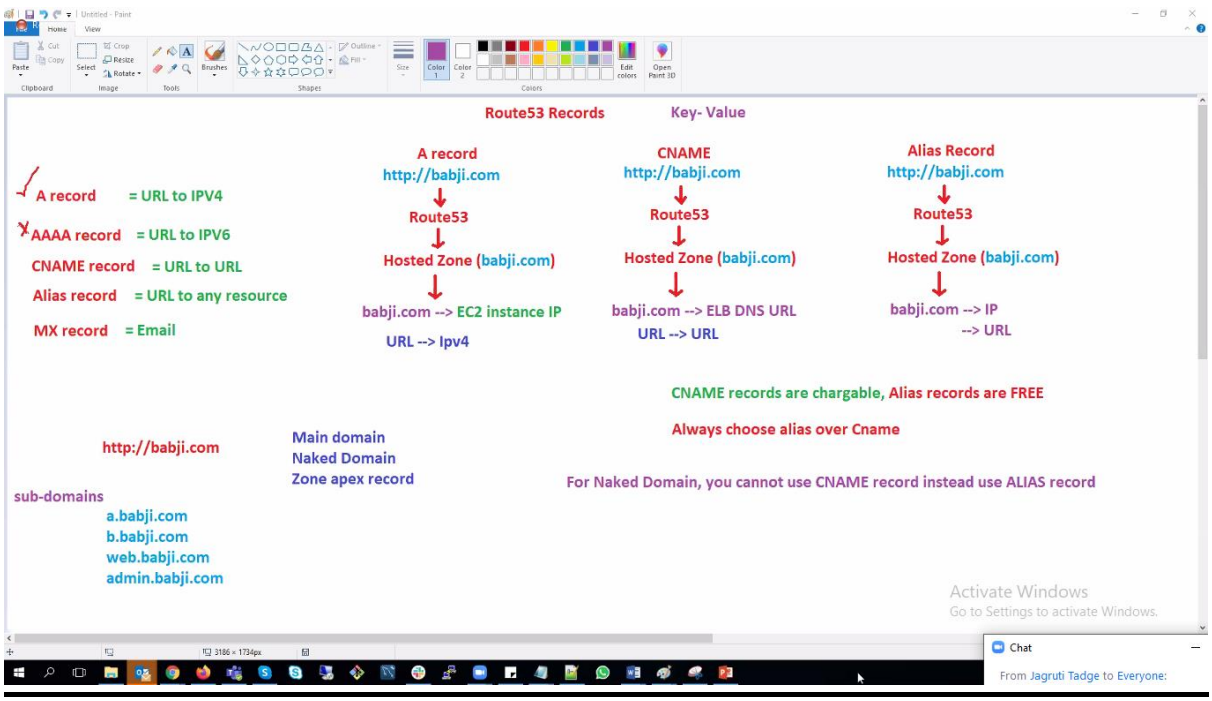
LB can distribute the traffic to multiple instances across multiple AZ's

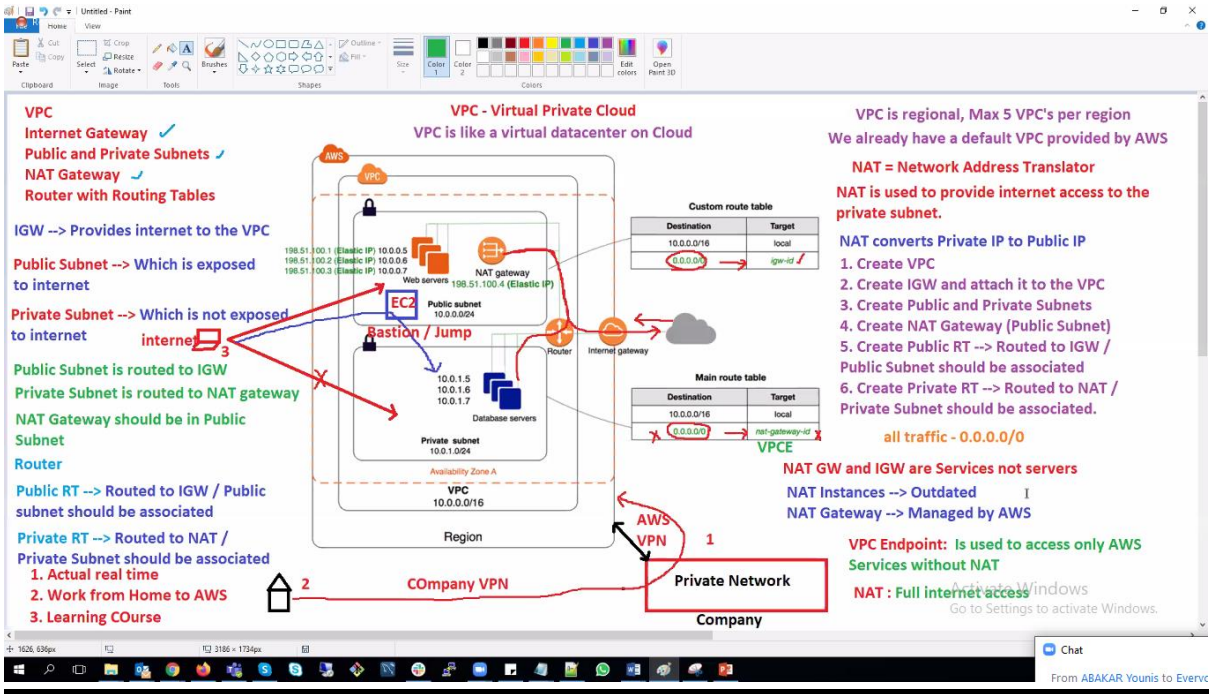
LB dosent have AZ. it is a serivce from AWS

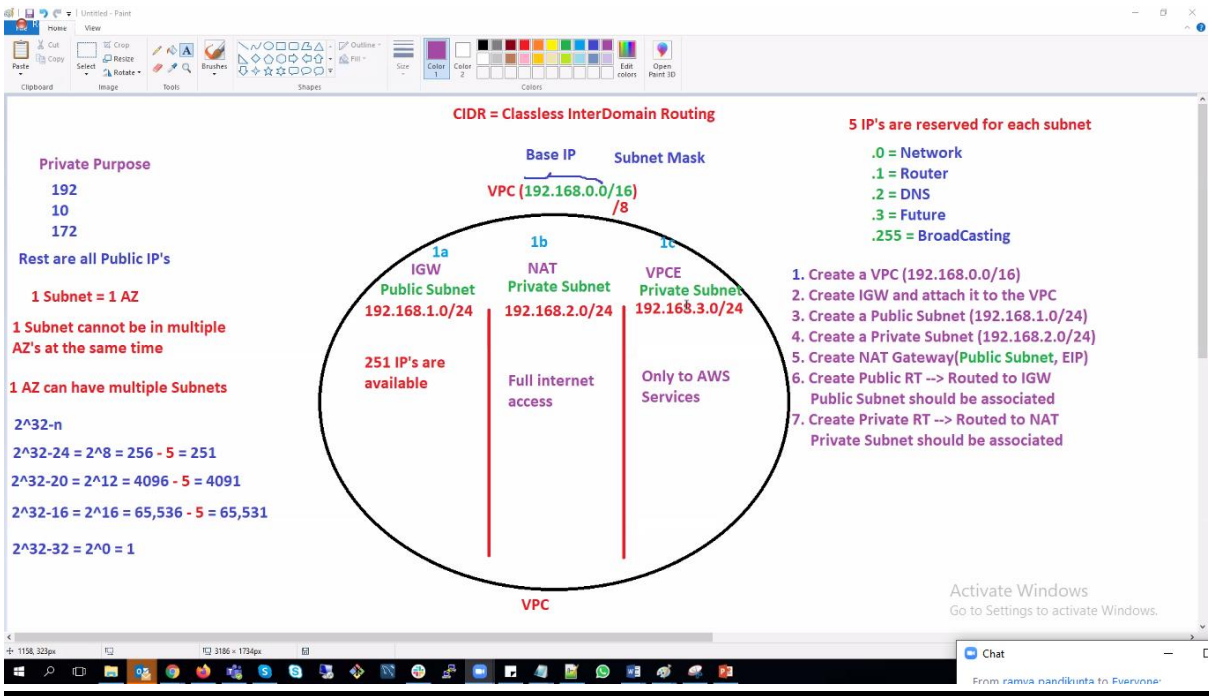
1a	1b	1c
Andheri, juhu,vashi,	Kalyan,thane,chambur	bandra,parel,vasi

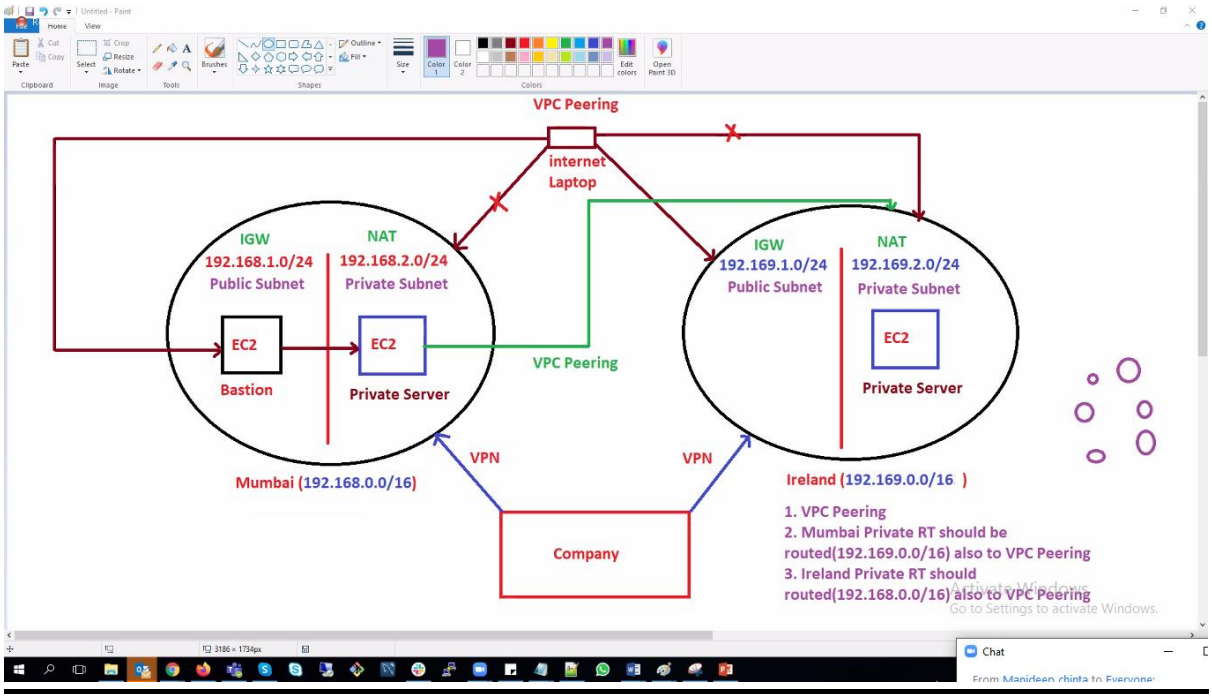
Chat

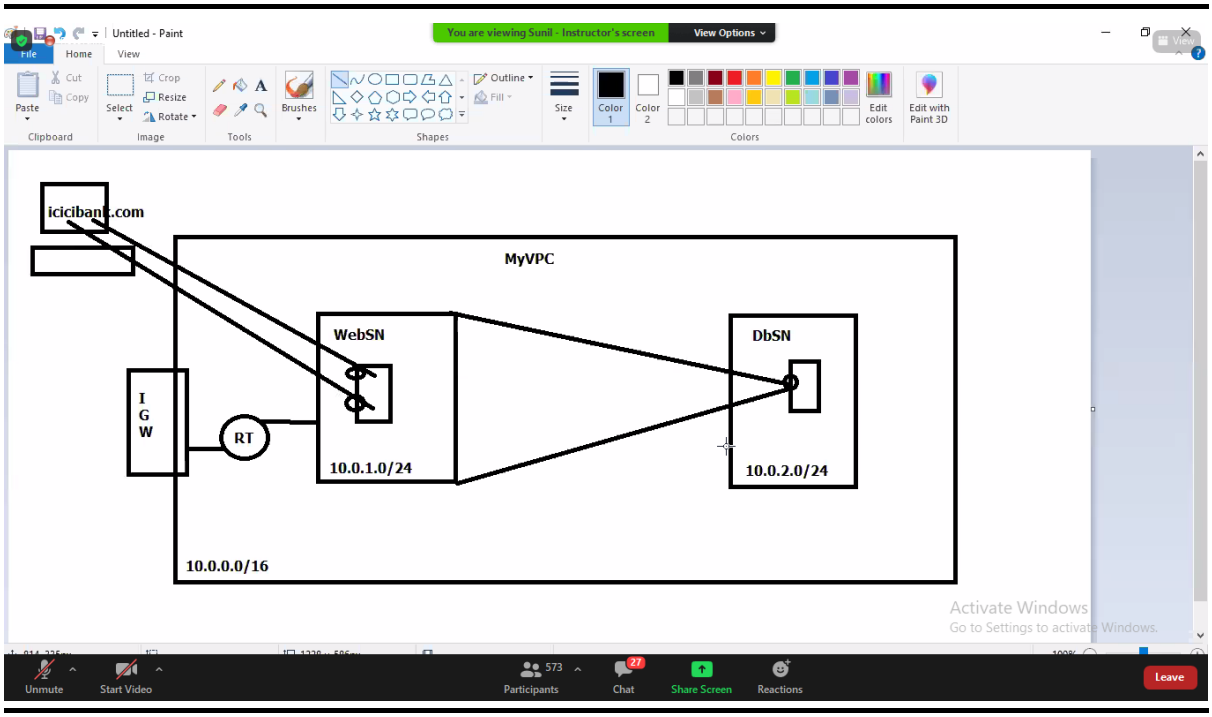

DNS = Keep track of all hostnames and Ip addresses
= It converts IP to Host and Host to IP
which identify the domain name
No Need to Worry
Route53
Name Server → SOA
boom.com
Top Level Domain .com
Root Name Server
Local DNS
Hostname
IP
boom.com
Hosted Zone
Public Hosted Zone
internet
Private Hosted Zone
VPC
Records
boom.com --> ELB
ELB
EC2
EC2
R53 --> HostedZone --> Records --> ELB --> EC2
Route53
DNS Service on AWS, DNS Port Number is 53
Purchase Domain
Route53
No need to create a hosted zone
It will create automatically with NS and SOA records
Go-Daddy / Any
Manually create HZ in R53
It will automatically create NS and SOA
put records
request redirected to AWS
boom.com
godaddy NS records
update R53 NS records in go-daddy
Go-Daddy
Route53 Features
1. Domain Registration
2. DNS Routing
3. Health Checks
4. Routing Policies
Route53 is Global
DNS is all about records
Hosted Zone = Container of records
Hosted Zone (Domain Name = boom.com)
Public Hosted Zone
NS Record = Pool of Servers (4)
SOA Record = Admin for hosted zone
NS and SOA records are automatically created and handled by AWS
NS and SOA records are default records
You cannot delete NS and SOA records
Activate Windows
Go to Settings to activate Windows.
Chat
higher compare to GoDaddy :D

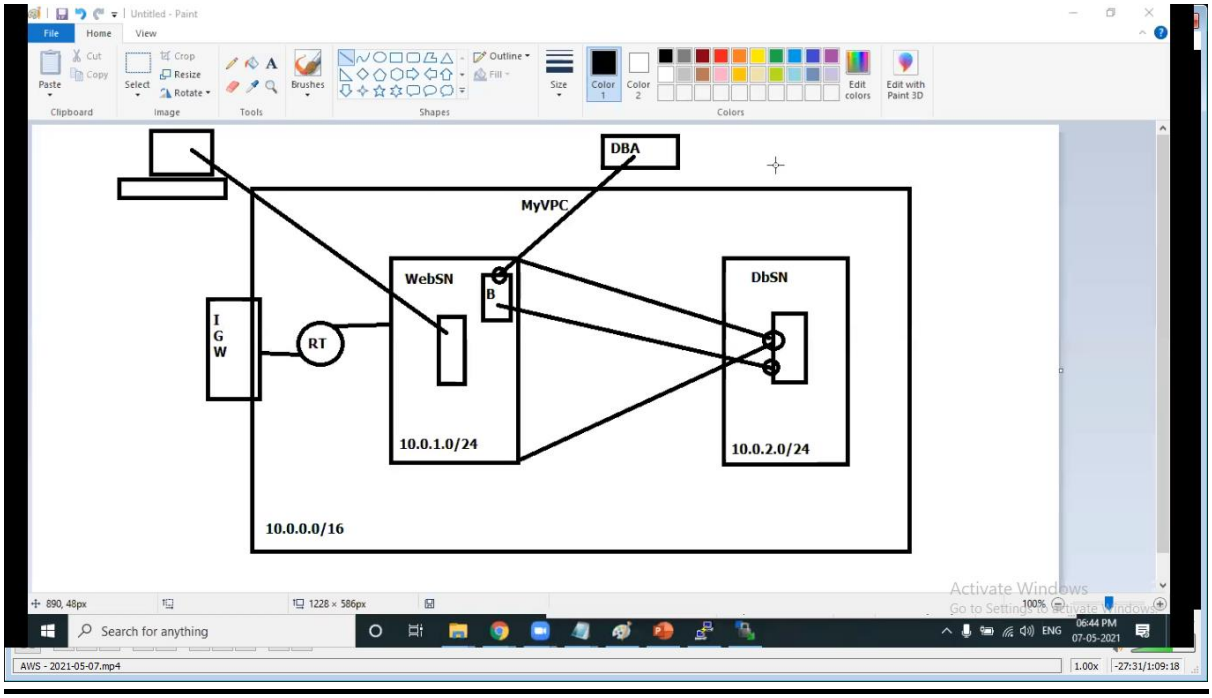

Route53 Records
Key- Value
A record = URL to IPV4
AAAA record = URL to IPV6
CNAME record = URL to URL
Alias record = URL to any resource
MX record = Email
A record
http://babji.com
Route53
Hosted Zone (babji.com)
babji.com --> EC2 instance IP
URL --> Ipv4
CNAME
http://babji.com
Route53
Hosted Zone (babji.com)
babji.com --> ELB DNS URL
URL --> URL
Alias Record
http://babji.com
Route53
Hosted Zone (babji.com)
babji.com --> IP
--> URL
CNAME records are chargable, Alias records are FREE
Always choose alias over Cname
For Naked Domain, you cannot use CNAME record instead use ALIAS record
http://babji.com
Main domain
Naked Domain
Zone apex record
sub-domains
a.babji.com
b.babji.com
web.babji.com
admin.babji.com
Activate Windows
Go to Settings to activate Windows.
Chat
From Jagruti Tadge to Everyone:


VPC
Internet Gateway
Public and Private Subnets
NAT Gateway
Router with Routing Tables
IGW --> Provides internet to the VPC
Public Subnet --> Which is exposed to internet
Private Subnet --> Which is not exposed to internet
Public Subnet is routed to IGW
Private Subnet is routed to NAT gateway
NAT Gateway should be in Public Subnet
Router
Public RT --> Routed to IGW / Public subnet should be associated
Private RT --> Routed to NAT / Private Subnet should be associated
1. Actual real time
2. Work from Home to AWS
3. Learning COurse
VPC - Virtual Private Cloud
VPC is like a virtual datacenter on Cloud
AWS
VPC
Custom route table
Destination
Target
10.0.0.0/16
local
0.0.0.0/0
igw-id
198.51.100.1 (Elastic IP) 10.0.0.5
198.51.100.2 (Elastic IP) 10.0.0.6
198.51.100.3 (Elastic IP) 10.0.0.7
Web servers
NAT gateway
198.51.100.4 (Elastic IP)
EC2
Public subnet
10.0.0.0/24
Bastion / Jump
internet
3
Router
Internet gateway
10.0.1.5
10.0.1.6
10.0.1.7
Database servers
Private subnet
10.0.1.0/24
Availability Zone A
Main route table
Destination
Target
10.0.0.0/16
local
0.0.0.0/0
nat-gateway-id
VPCE
VPC
10.0.0.0/16
Region
AWS VPN
1
2
COmpany VPN
Private Network
Company
VPC is regional, Max 5 VPC's per region
We already have a default VPC provided by AWS
NAT = Network Address Translator
NAT is used to provide internet access to the private subnet.
NAT converts Private IP to Public IP
1. Create VPC
2. Create IGW and attach it to the VPC
3. Create Public and Private Subnets
4. Create NAT Gateway (Public Subnet)
5. Create Public RT --> Routed to IGW / Public Subnet should be associated
6. Create Private RT --> Routed to NAT / Private Subnet should be associated.
all traffic - 0.0.0.0/0
NAT GW and IGW are Services not servers
NAT Instances --> Outdated
NAT Gateway --> Managed by AWS
VPC Endpoint: Is used to access only AWS Services without NAT
NAT : Full internet access
Activate Windows
Go to Settings to activate Windows.
Chat
From ABAKAR Younis to Everyo


CIDR = Classless InterDomain Routing
Base IP
Subnet Mask
VPC (192.168.0.0/16)
/8
Private Purpose
192
10
172
Rest are all Public IP's
1 Subnet = 1 AZ
1 Subnet cannot be in multiple AZ's at the same time
1 AZ can have multiple Subnets
2^32-n
2^32-24 = 2^8 = 256 - 5 = 251
2^32-20 = 2^12 = 4096 - 5 = 4091
2^32-16 = 2^16 = 65,536 - 5 = 65,531
2^32-32 = 2^0 = 1
1a
IGW
Public Subnet
192.168.1.0/24
251 IP's are available
1b
NAT
Private Subnet
192.168.2.0/24
Full internet access
1c
VPCE
Private Subnet
192.168.3.0/24
Only to AWS Services
VPC
5 IP's are reserved for each subnet
.0 = Network
.1 = Router
.2 = DNS
.3 = Future
.255 = BroadCasting
1. Create a VPC (192.168.0.0/16)
2. Create IGW and attach it to the VPC
3. Create a Public Subnet (192.168.1.0/24)
4. Create a Private Subnet (192.168.2.0/24)
5. Create NAT Gateway(Public Subnet, EIP)
6. Create Public RT --> Routed to IGW
Public Subnet should be associated
7. Create Private RT --> Routed to NAT
Private Subnet should be associated
Activate Windows
Go to Settings to activate Windows.
Chat


VPC Peering
internet
Laptop
IGW
192.168.1.0/24
Public Subnet
NAT
192.168.2.0/24
Private Subnet
EC2
Bastion
EC2
Private Server
VPC Peering
IGW
192.169.1.0/24
Public Subnet
NAT
192.169.2.0/24
Private Subnet
EC2
Private Server
VPN
VPN
Mumbai (192.168.0.0/16)
Ireland (192.169.0.0/16)
Company
1. VPC Peering
2. Mumbai Private RT should be routed(192.169.0.0/16) also to VPC Peering
3. Ireland Private RT should routed(192.168.0.0/16) also to VPC Peering
Activate Windows
Go to Settings to activate Windows.
Chat


Untitled - Paint
You are viewing Sunil - Instructor's screen
View Options
icicibank.com
MyVPC
WebSN
DbSN
I
G
W
RT
10.0.1.0/24
10.0.2.0/24
10.0.0.0/16
Activate Windows
Go to Settings to activate Windows.
Unmute
Start Video
Participants
Chat
Share Screen
Reactions
Leave


Untitled - Paint
File
Home
View
DBA
MyVPC
WebSN
B
DbSN
I
G
W
RT
10.0.1.0/24
10.0.2.0/24
10.0.0.0/16
Activate Windows
Search for anything
ENG
06:44 PM
07-05-2021
AWS - 2021-05-07.mp4
1.00x
-27:31/1:09:18