**CLOUD WATCH**

1. **How to create alarm notification for terminating instance**

Step 1:- Create instance 🡪 copy instance id

Step 2:- In cloud watch🡪 Alarm 🡪 all alarm 🡪 create alarm 🡪 metric 🡪 select metric 🡪 EC2 🡪 per –instance metric 🡪 past and enter instance id 🡪

🡪select CPU utilization 🡪 select metric

Step 3:- Specify metric condition 🡪 condition 🡪 threshold type (static)🡪 cpu utilization (greater)🡪50🡪additional configuration 🡪 data point to alarm 1 out of 1 🡪next

Step 4 :- Configuration 🡪 alarm state tigger 🡪in alarm 🡪 send notification to the following sns topic🡪 create new topic 🡪 name to topic🡪 email endpoint that will receive the notification 🡪email id🡪create topic (conform mail)

Step 5:- EC2 action 🡪in alarm state trigger 🡪 in alarm🡪take the following action 🡪terminate the instance🡪next

Step 6:- alarm name 🡪 terminate instance 🡪 alarm description 🡪next 🡪create alarm

(after 5 min alarm state is ok the take ssh)

Step 7:- on mobaextream :- sudo –i

Amazon-linux-extras install epel –y

Yum install stress –y

Stress –help

Stress –cpu 80 – io4

Increase cpu utilization 🡪 in alarm state🡪 terminate instance automatically

1. **Stream ec2 logs in cloud watch monitoring**

Step 1:- Create IAM policy 🡪 in json from

{

“version”:”2012-10-17”,

“statement”: [

{

“Effect” : “allow”,

“Action”: [

“logs:createloggroup”,

“log:Createlogstream”,

“logs:Putlogevent”,

“logs:describelogstreams”

],

“Resource”: [

“arn :aws : logs :\*:\*:\*”

]

}

]

}

Next tag 🡪 next :review🡪 review policy🡪 name (cloudwatch-logs-policy)🡪description🡪(cloud watch logs-policy-region-us-east-1)🡪create policy

Step 2:- Roles 🡪aws service 🡪 ec2🡪next🡪search your create policy🡪next 🡪role details 🡪role name (ec2 cloudwatchlog-role)🡪 create role

Step 3:- ec2🡪 launch instance 🡪 iam role 🡪http🡪 launch instance 🡪cloud watch 🡪logs 🡪log group (no logs)

Step 4:- Mobaxtrem

Sudo –i

Yum install http –h

Service http start

Sudo su

Cd /var/log/httpd/

ls 🡪 access\_log error\_log

cat access\_log

cat error\_log

sudo yum install awslogs –y

sudo vim /etc/awslogs/awscli.conf 🡪 (edit aws file)

[plugins]

cwlogs = cwlogs

[default]

Region = ap-south-1 🡪 esc 🡪 :wq

Pwd 🡪 ls

Sudo vim /etc/awslogs /awslogs.conf

[Edit the path for application logs]

[general]

state\_file = /var /lib/awslogs/agent-state

[application\_logs]

region = ap-south-1

datetime\_format =%b %d %H:%M:%S

file = /var/log/httpd/access\_log

buffer\_duration = 5000

log\_stream\_name = {instance\_id}

initial\_position = start\_of\_file

log\_group\_name = access\_logs 🡪 :wq

cat /etc/awslogs/awslogs.conf

service awslogs start

Step5:- Cloud watch🡪 logs 🡪 logs groups 🡪then we see our create logs access\_logs 🡪 access\_log🡪showing instance id

1. **How to create rule in event bridge OR Instance state change notification**

Step1 :- Cloud watch 🡪 event 🡪 rule 🡪 go to Amazon event bridge 🡪 create rule 🡪 name 🡪 instance state change 🡪 description (this rule will change my instance) 🡪 event bus (default) 🡪next

Step2 :-Bulid event pattern🡪event source🡪 aws event Or eventbridge 🡪sample event 🡪aws event

Step3:- Event pattern 🡪event source 🡪aws service 🡪(ec2)🡪 event type 🡪 ec2 instance state change notification 🡪any state🡪 any instance🡪 Next

Step 4:- Select Target 🡪aws service🡪select target🡪SNS topic🡪topic (select created topic)🡪next 🡪create rule

Step5:- SNS (simple notification service)🡪 subscription🡪create subscription🡪 Topic ARN 🡪 protocol🡪Email (ur email address)🡪create subscription.

Step6:- confirm subscription through email

Step7:- ec2🡪launch instance 🡪 show all instance stage

**EC2 (Elastic compute cloud)**

**NFS**

Step1:- Launch instance server-01 and clinet-02 with security group of nfs and new key pair

Step2:- EFS🡪 then create file system🡪 NFS (none)🡪click NFS🡪 Network🡪 Manage🡪select security group with AZ🡪 attach

Step3:- Start mobaexterm with instance public ip of the server and client instance

Server:- sudio -i

mkdir /jack (create a directory)

cd /jack (change dir)

touch file{1..10} (create files)

ls /jack (list files)

yum install amazon-efs-utils -y (install efs)

mount -t efs port id:/ /jack (mount files)

ls /jack

df-hT

same steps for client

**VPC (virtual private cloud)**

**Creating Vpc, Subnet, Routtable, Internet gateway, Nat gateway**

Step1:-Create vpc🡪vpc-name {my-vpc-01}🡪IPV4 CIDR🡪{192.168.0.17}🡪 click🡪{no-ipv6} Tenancy🡪Default🡪create VPC

Step2:-Subnet🡪create subnet-1🡪VPC id select🡪subnet-name{my-public-subnet}🡪AZs🡪{east-1a}🡪ipv4 CIDR-block 🡪192.168.0.0/19🡪add-subnet-2🡪my-private-subnet-2🡪AZs{east-2b}🡪ipv4-cidr-block🡪{192.168.0.33/19}🡪(create-subnet)

Step3:-instance🡪launch-instance🡪name {vpc-instance}🡪network-setting🡪 vpc🡪 select vpc🡪 auto assign public IP🡪Enable🡪select subnet🡪Launch Instance

Step4:-Create-Internet Gateway 🡪name🡪create select🡪action🡪attach to VPC

Step 5:-Route🡪 route table🡪0.0.0.0/0 select igw🡪create

Step6:- Go to mobaexterm 🡪 copy public ip and take ssh

private ip access🡪 sudo ssh-i /home/ec2-user/key-pair-name ec2-user@private-ip

Step7:-Attached NAT Gateway🡪create nat gateway🡪name {my-first-nat-gateway }🡪select-subnet🡪public-subnet🡪select Elastic IP allocation id🡪create

Step 8:-Create Route Table🡪name{sub-RT}🡪vpc select🡪create select created RT🡪go to subnet association🡪select private-subnet🡪save association

Step9:-Route table🡪sub-RT{click}🡪add route🡪0.0.0.0/0🡪select NAT gateway🡪save changes

Step10:- Go to mobaxterm 🡪 copy public ip and take ssh🡪ping [www.google.com](http://www.google.com) 🡪private ip access🡪sudo ssh-i /home/ec2-user/key-pair-name ec2-user@private ip🡪ping [www.google.com](http://www.google.com)

{NAT gateway it is used to access internet for private ip}

# Amazon Route 53 the DNS service for an existing domain

Step-1 : Create a instance using script

Step-2 : Go to freenom.com for free domain name then create domain name

Step-3 : Go to route 53 click hosted zone 🡪 then create hosted name 🡪 domain name (which is already created in freenom) 🡪 Description 🡪 Public hosted zone 🡪 Create hosted name

Step-4 : Copy value traffic from record name to freenom 🡪 Domain 🡪 Manage domain 🡪 Management Tools 🡪 Nameservers & paste in it 🡪 Change Name servers

Step-5: Route 53 🡪 Create Record 🡪 Put IP of Instance 🡪 Record Type A 🡪 Create Record

Step-6 : Copy Domain name & host in new tab