NAME : Vytla Harsha Vardhan   cloud computing - CS360

ROLL : 18bcs118   END SEM - 10/05/2021

(7) → when you terminate EC2 instance the instance will be shutdown and virtual machine that was provisioned for you will be permanently taken away and you will no longer be charged for instance usage.

→ Any data that was stored locally on that instance will be lost

→ It is not possible to recover the terminated instance or any volumes that are deleted as part of termination process

(5) → AWS is a cloud computing platform from Amazon. It's always beneficial to know how many ways we can connect to AWS

→ There are mainly 3ways

(i) AWS Console

→ In all the ways of connecting prior you should create AWS account.

→ Console is the easiest way to manage resources on AWS. you can login with credentials

(ii) AWS CLI

→ AWS Command Line Interface (CLI) is a unified tool to manage your AWS services

→ with just one tool to download and configure you can control multiple AWS services from command line

→ Installing AWS CLI in our system is also a semple process

(iii) AWS SDK : (Software development kit)

→ AWS has tools for developing and managing applications on it.

→ AWS supports these languges C++, GO, java, javascript, .NET, Node.js, PHP, python & Ruby.

(3)

a) cloud watch , ~~[illegible] tole~~ Name Spaces

b) ~~Alarm~~ Simple Notification Service (SNS) / cloud watch Alarms

(8) → Very often we may ferget our crendential to login to an instance

→ To recover the credentials/to login to instance.

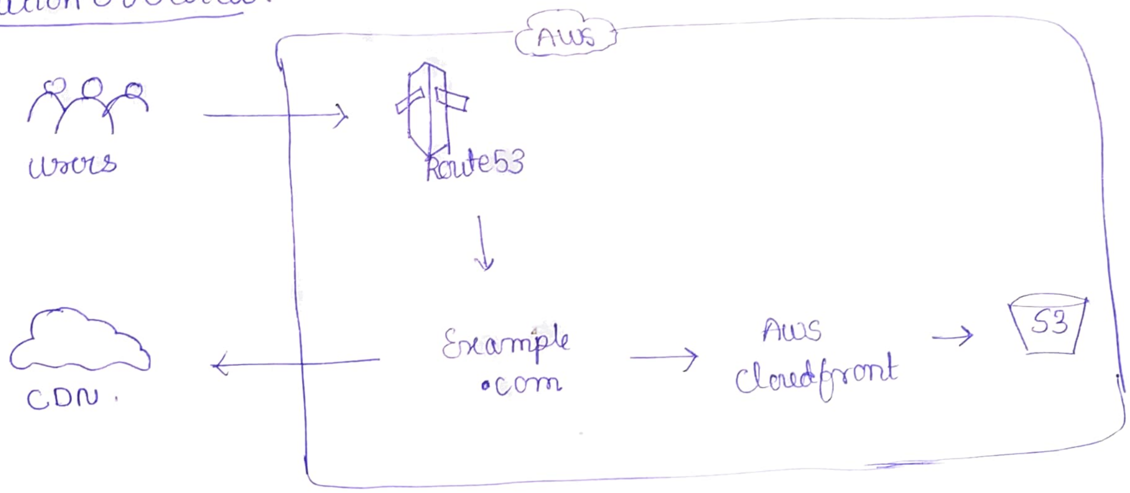
- Gather config details fr Original Instance
- Power off the original Instance of EC2 which you wanna login
- Launch a new recovery Instance and generate a new keypair
- Login via SSH to new recovery instance
- Detach the primary EBS volume from original (target) instance (taking note fr its current attachment)
- Attach the previously detached volume to new Instance
- Copy Authorized keys from recovery instance ~~and~~ to mounted volume. ~~reattach back to original instance~~. ~~using noted configs~~
- Start the original target Instance and now login with new key pair by unmounting target volume from recovery instance and reattach back to original
- Delete temporary (recovery) instance created

(6) → To protect your web application against DDoS attacks, you can use AWS shield, a DDoS protection service that AWS provides Automatically to all AWS customers at no additional charge

→ You can use AWS shield in conjunction with DDoS resilient web services such as Amazon cloud front and Route 53 to improve ability to defend DDoS attacks.

→ You can also use Route 53 with an externally hosted CDN (content delivery network)

Solution overview:



→ In this solutions AWS services Route 53, S3, cloudfront are used

Deployment of solⁿ:

S1 : create an S3 bucket with HTTP redirection

S2 : create and configure a cloud front web distribution

S3: configure an alias reservices record set in hosted zone

S4: validate that the redirect is working

Hosting a static website requires a bucket to follow the DNS restrictions

AWS S3 bucket follows the DNS rules so that we can use the same website endpoints.

Ex: Let consider we are making a bucket named "Mybuc" in EU(paris): eu-west-3 and US East (N. virginia): us-east-1

Step 1: Create a Bucket first with name "Mybuc"

Step 2: Enable website hosting as it was not enabled by default by going to properties tab

Step 3: Index document is the webpage appears when user requests the home URL.

Step 4: Configure Errors
→ you can configure error page at the time of enabling static website hosting & for custom error pages you can set the redirection rules

Step 5: website access permissions add to allow public access bucket

Step 6: Traffic logging.

②

S1: open functions page on Lambda console

S2: choose a function

S3: under functional overview, choose "Add trigger"

S4: now select API Gateway

S5: for API, choose create an API

S6: for security choose open

S7: choose Add.

THE END