Date
10-05-2021.

Mid-Sem-Examination.

CS360- Cloud Computing.

P. Bhanu prakash.

Reg no:- 18BEC035.

Branch:- ECE.

7. When an EC2 instance is stopped using the stop-instances Command the following is registered at the OS level:-

* The API requests sends a button press event to the guest.
* various System service are stopped as a result of the button press event. Graceful shutdown is triggered by the ACPI shutdown button press event from the hypervisor.
* ACPI shutdown is initiated.
* The instance shuts down when the graceful shutdown process exits.
* If the instance OS does not shut down cleanly within a few minutes, a hard shutdown is performed.

When we stop the EC2 instance will be shutdown and the virtual machine that was provisioned for you will be permanently taken away and you will no longer be charged for instance usage. When you start a stopped instance the EBS volume is simply attached to the newly provisioned instance.

Once you stop an EC2 instance, the instance is shutdown and the vm that was provisioned for you will be taken away indefinitely. You will not be charged for instance usage once this has happened.

8.

LOST the credentials to AWS EC2 instance login:-

In the Below steps are required to covered in this post to recovery access to your EC2 instance after losing your credentials.

→ Gather Configure details of the original target instance.

→ power off the original target EC2 instance of which you want to regain access.

→ launch new (recovery) instance and generate new key-pair.

→ login via ssh to the new recovery instance.

→ Detach the primary EBS volume from original instance

→ Attach / mount the previously detached volume to the new instance.

→ Copy authorized keys from recovery instances to the mounted volume.

→ unmount target volume from recovery instance and reattach back to original instance using configs noted earlier.

→ start the original instance and login with new pair

→ Delete temporary (recovery) instance.

→ once logged in successfully, return to the EC2 management console, Select the original instance you will like to replace the lost instance key and Select "Stop"

→ once the instance state changes to "Stopped' select the instance again, and the 'instance properties pane, click on the root device and then click on the volume id.

4th. Static website hosting on Amazon S3 is one of the very Popular use cases of Amazon S3. It allows you to host an entire static website and on a very low cost. Amazon S3 is a highly available & scalable hosting solution.

Amazon S3 is designed to deliver 99.9% durability and scale for trillions of objects world wide. It. It's very easy to host a static website on Amazon S3 with very minimal steps.

Amazon has other service to store dynamic websides on AWS you may like to start with "Amazon EC2 - Elastic Compute Cloud" for instance.

⇒ Static websites only contain static resources like. HTML, Images, Javascript, CSS and fonts, etc,.... Static web hosting doesn't contain server-side processing or scripting. In Constrast. a dynamic website relies on server side Processing, including server-side scripts such as JSP, PHP or ASP.NET etc,...

A static website deliveries exactly the same content on each request because pare are stored in file storage. with no dynamic manipulation on content at runtime. which makes the static website much faster on. Comparision to the dynamic websites. Most of the static website hosting platform allows to cache data large extent.

Hosting static website on Amazon S3.

* Create bucket.
* Enable website hosting.
* Index documents & folders.
* Configuring Errors
* Website Access Permission.
* Traffic loging.

6. DDOS (Distributed denail of service) attacks are sometimes used by malicious ties in an attempt to flood a network, System or application with more traffic connections or requests.

that can handle this DDOS attack could be classified as the federal criminal offense under Computer fraud and Abuse act. this attack is very bad because of no. of machines or network that receive and respond to these. Packets is very large, victim's Computer will be flooded with traffic. This overloads victim Computer will be founded with traffic. This overloads victim Computer and can even makes it unusable during such attack

→ ECB [Elastic load Balancing] helps to achieve greater fault tolearnce by automatically routing inbound traffic across multiple Amazon EC2 instances. It also, allows to reduce your attact outo by receiving. requests on Behalf on your ~~stattle~~ to automatically. scaling to handle it.

2. You can create a web API with an HTTP endpoint for your lambda function by using Amazon API gateway. API gateway provides tools for creating and documenting web API's that route HTTP requests to lambda functions. You can secure access to your API with authentication controls. your API's can serve traffic over the internet or can be accessible only within your VPC.

→ Open the function page on the lambda console
→ choose a function.
→ under functional overview, choose add trigger.
→ select API gateway.
→ for API choose create an API
→ for security, choose open.
→ choose add.

API gateways are comprised of stages, sources, methods and integration.

* API path format.

Choosing an API type:-

* HTTP API → A lightweight, low-tenancy Restful API.
* REST API → A customizable, feature rich Restful API.
* web socket API → A web API that maintains persistent connections with clients for full-duplex communication.

5th. AWS (Resource Access Manager)(RAM) is a service that enables you to easily and securily share AWS resources with any AWS account or within your AWS organization. you can share AWS Transit gateways, subnets, AWS license management configurations, and Amazon Route 53 resolver rules resources with RAM.

Many organizations use multiple accounts to create administrative or billing isolation, and to limit the impact of errors, RAM eliminates the need to create duplicate resources in multiple accounts, reducing the operational overhead of managing those resources in every single account you own. you can create resources in every single account you own. you can create resources centraly in a multi-account environment and use RAM to share those resources across in the three simple steps: create a Resource share, specify resource share, specify resources and specify accounts RAM is available to you at no additional charge

Benefits:-

* Reduce operational overhead:-
These eliminates the need to provision duplicate resources in every account in multi-account environment.

* Improve Security and visibility.

* optimize costs.

Sharing resources such as AWS license Manager configurations across accounts allows you to leverage license in multiple parts of your company to increase utilization and optimize costs.

3.

a.

Amazon cloud watch service allows users to create logs which will display metrics as per user monitering needs.

b. It also creates SNS (simple Notification Service). and take actions based on the thresholds Notifications for the same can be triggered which can send mails to the user mailbox.

* a. cloud watch, logs.

* b. SNS.