AWS Exam - 4 Hours

**Instructions:**

* This exam consists of two sections: **Multiple Choice & Hands-on Questions (UI-Based)**.
* No AWS CLI is required; answer all questions based on AWS UI interactions and provide screenshots on completion.
* You may only use Google and not AI tools.
  + Terms that you are unfamiliar with, require you to google and answer.
* Time to complete: **3 Hours - 4 hours**

**Section 1: Multiple Choice Questions (MCQs)**

**1. AWS Core Services**

1. Which AWS service is used to store objects such as images, videos, and backups?  
     
   * A) EC2
   * B) RDS
   * C) S3
   * D) Lambda
2. What is the purpose of an AWS Availability Zone?  
     
   * A) It ensures high availability by distributing resources across multiple locations.
   * B) It acts as a data center located in different countries.
   * C) It is only used for networking and VPCs.
   * D) It is a security feature of AWS.
3. What is the default storage class for an S3 bucket when you create it?  
     
   * A) S3 Intelligent-Tiering
   * B) S3 Glacier
   * C) S3 Standard
   * D) S3 Infrequent Access (IA)

**2. IAM & Security**

1. What is the purpose of an IAM role?  
     
   * A) It is used to assign permissions to AWS services and users.
   * B) It is a dedicated user with full AWS access.
   * C) It replaces IAM users completely.
   * D) It is used only for temporary access.
2. In AWS IAM, what is the best practice for securing your root account?  
     
   * A) Keep it logged in at all times for easy access.
   * B) Use it only for creating IAM users and enable Multi-Factor Authentication (MFA).
   * C) Assign full administrator access to all IAM users.
   * D) Share credentials with your team for convenience.

**3. Networking and Connectivity**

1. What is the purpose of an Internet Gateway in AWS?  
     
   * A) To allow communication between instances within a VPC.
   * B) To provide internet access to resources in a private subnet.
   * C) To restrict public access to EC2 instances.
   * D) To encrypt data stored in S3.
2. What is the main difference between a Security Group and a Network ACL?  
     
   * A) Security Groups operate at the instance level, while NACLs operate at the subnet level.
   * B) NACLs provide fine-grained access control for IAM users.
   * C) Security Groups apply only to databases.
   * D) NACLs are only used for VPN connections.

**4. Storage & Databases**

1. Which AWS service provides a managed relational database service?  
     
   * A) DynamoDB
   * B) RDS
   * C) Redshift
   * D) S3
2. What happens if you delete an S3 bucket with objects inside it?  
     
   * A) The bucket is deleted, but the objects remain in AWS storage.
   * B) The bucket is deleted, and all objects inside it are permanently removed.
   * C) The bucket cannot be deleted unless it is empty.
   * D) The bucket is archived, and you can restore it later.

**5. AWS Billing & Pricing**

1. Which AWS pricing model allows you to pay only for the computing resources you use?

* A) Reserved Instances
* B) Spot Instances
* C) Pay-as-you-go
* D) Fixed-rate pricing

1. What tool in AWS helps users monitor their spending and set budget alerts?

* A) AWS Cost Explorer
* B) AWS Config
* C) AWS CloudTrail
* D) AWS Security Hub

**6. Research-based AWS Questions - using google only**

1. What are AWS Landing Zones, and how do they help with multi-account governance?  
    **A**: Landing Zones are multi-accounts AWS environments that provide a starting point from which you can deploy workloads and apps. AWS Landing Zones helps with multi-account governance by providing a standardized framework for account management, security, compliance, and operational efficiency, a landing zone addresses the complexities and risks associated with multi-account environments.
2. Explain how AWS WAF protects web applications from common attacks.  
   **A**: AWS WAF is a cloud-native web application firewall that helps protect web applications from common threats and vulnerabilities.  
   It works by filtering, monitoring, and blocking malicious HTTP and HTTPS traffic before it reaches your application. AWS WAF allows you to define custom security rules to block or allow requests based on various factors like IP addresses, HTTP headers, URI paths, etc.  
   Unlike traditional firewalls that focus on network traffic, AWS WAF is tailored for web application security. It’s especially designed to protect against threats like SQL injection, cross-site scripting (XSS), and other vulnerabilities.  
   Some of the key features of AWS WAF are:  
   **IP Set Control** – create IP sets to manage the traffic by whitelisting or blacklisting IP addresses.  
   **Geo-Blocking** – manage the traffic from specific countries or regions.  
   **Rate Limiting** - mitigate the DDos attacks by limiting the rate of requests from a particular IP address  
   **SQL Injection and XSS protection** - AWS WAF is equipped with pre-configured rules that automatically detect and block SQL injection attempts and Cross-Site Scripting (XSS) attacks.   
   **Logging and Metrics** - By analyzing these logs, you can uncover attack patterns and adjust your rules accordingly.
3. What is AWS Snowball, and when should it be used?  
   **A**: AWS Snowball accelerates transferring large amounts of data into and out of AWS using physical storage devices, bypassing the Internet.  
   The use case of AWS Snowball is to export and import data from and S3
4. What are the key differences between AWS Backup and manual snapshot backups?  
   **A**: An AWS snapshot is just a point-in-time copy of an Amazon EBS volume for an EC2 instance with limited storage and recovery options. An AWS EC2 backup is a more comprehensive and flexible copy of the cloud workloads, offering reliable protection and ensuring fast and consistent recovery.
5. How does AWS Shield help mitigate DDoS attacks?  
   **A**:  When AWS Shield detects a DDoS attack, it automatically deploys inline mitigations to filter out malicious traffic and allow legitimate traffic to reach customer resources.
6. Explain the differences between AWS Transit Gateway and VPC Peering.  
   **A**: VPC Peering and Transit Gateway are used to connect multiple VPCs. VPC Peering provides Full-mesh architecture while Transit Gateway provides hub-and-spoke architecture. Transit Gateway gives VPC connectivity at scale and simplifies VPC-to-VPC communication management over VPC Peering with a large number of VPCs.  
   **VPC Peering advantages**:  
   Low costs since the payment is only for the data transfer  
   No bandwidth limit  
   **VPC Peering disadvantages**:  
   Complex at scale, each new VPC add complexity to the network and it is harder to maintain rout tables compared to TGW  
   **TGW advantages**:  
   Each VPC is connected to a central hub  
   Supports more VPCs compared to peering  
   More fine graded routing.  
   **TGW disadvantages**:  
   Additional hop causing more latency  
   Extra cost of hourly charge per attachment in addition to data fees.
7. What is AWS Step Functions, and how does it help with workflow automation?  
   **A**: AWS Step Functions is a serverless orchestration service that lets developers create and manage multi-step application workflows in the cloud.   
   By using the service's drag-and-drop visual editor, teams can easily assemble individual microservices into unified workflows.
8. How does AWS Control Tower assist organizations in managing multiple AWS accounts?  
   **A**: AWS Control Tower allows to group accounts into organizational units (OUs) based on the organization’s structure or requirements. OUs work as a container for AWS accounts that allows for applying different policies and guardrails to specific groups of accounts. It is possible to create, delete and register OUs in the organization panel of the AWS control tower.  
   By deploying AWS Control Tower into an existing organization, it allows to register existing organizational units and the accounts they hold
9. What is the significance of AWS Outposts in hybrid cloud solutions?  
   **A**: AWS Outposts allows for a Hybrid service that is ideal for low-latency and local data processing or data residency.  
   AWS Outposts allows to deploy fully managed, rack-mountable servers at locations with space constraints and run applications using the same AWS infrastructure, services, APIs, and tools for a truly consistent hybrid experience.
10. Explain the key use cases for AWS Elastic File System (EFS) compared to S3 and EBS.  
    **A**: AWS EFS, S3 and EBS are 3 deferent storage solutions for 3 deferent use cases.  
    **S3** is a secure, durable, and highly scalable object storage that can store different types of files.  It’s a static storage service useful for static website hosting, media distribution, version management, big data analytics, and archiving.  
    **EBS** is a high-performance block storage service designed for use with Amazon EC2s machines for both throughput and transaction-intensive workloads at any scale.  
    **EFS** is a file system is excellent as a managed network file system that can be shared across different Amazon EC2 instances. Amazon EFS works like NAS devices and performs well for big data analytics, media processing workflows, and content management.

**Section 2: Hands-on UI-Based Questions**

**1. S3 Bucket Configuration**

* Navigate to the AWS Management Console and create a new S3 bucket.
* Enable versioning and explain the steps you took.
* Set a policy to allow only your IAM user to upload objects.
* **Provide a screenshot on completion**

**2. Launch an EC2 Instance**

* Using the AWS UI, create a **t2.micro** EC2 instance.
* Attach a Security Group that allows inbound SSH (port 22) and HTTP (port 80) traffic.
* **Provide a screenshot on completion**

**3. Configure an IAM User with S3 Access**

* Create a new IAM user with permissions to access only a specific S3 bucket.
* **Provide a screenshot on completion**
* How would you verify that the user has the correct permissions?

**4. Set Up a CloudWatch Alarm**

* Navigate to AWS CloudWatch and create an alarm to monitor CPU usage on an EC2 instance.
* Set the alarm to trigger if CPU utilization exceeds **70%** for **5 minutes**.
* Describe how you configured notifications for the alarm.
* **Provide a screenshot on completion**

**5. Identify AWS Billing Costs**

* Navigate to AWS Cost Explorer and check the billing details for the past month.
* Explain the steps to analyze usage and forecast costs.
* **Provide a screenshot on completion**

**Section 3: Hands-on advanced**

**Instructions:**

* **Perform the following tasks using the AWS UI.**
* **Provide screenshots as proof of completion.**
* **No AWS CLI is required; all actions must be performed using the AWS Management Console.**

**1. Deploy an Auto Scaling Group with a Single EC2 Instance**

* Create an Auto Scaling Group with a t2.micro Amazon Linux 2 instance.
* Configure the Launch Template to include the following:
  + Amazon Linux 2 AMI.
  + Security Group that allows inbound SSH (port 22) and HTTP (port 80).
* Set the desired capacity to 1 instance.
* Attach a Load Balancer to the Auto Scaling Group.
* Provide a screenshot of the Auto Scaling Group settings.

**2. Connect to the EC2 Instance and Install Nginx**

* Connect to the running EC2 instance via SSH.

**Install Nginx and create a simple HTML welcome page - see commands to run below:**

|  |
| --- |
| **sudo yum update -y sudo yum install -y nginx echo "<h1>Welcome to AWS Auto Scaling</h1>" | sudo tee /usr/share/nginx/html/index.html sudo systemctl start nginx sudo systemctl enable nginx**  **# Validate that it works by running:**  **curl** [**http://localhost:80**](http://localhost:80) |

* **Provide a screenshot of the running Nginx service on the instance and the output of the curl command**

**3. Access the Web Page via the Load Balancer**

* Retrieve the Load Balancer DNS name.
* Open a web browser and access the Load Balancer URL.
* Take a screenshot showing the browser with the Load Balancer DNS and the welcome page.

**4. IAM User Setup for S3 Access**

* Create a new IAM user with permissions limited to accessing a specific S3 bucket.
* Provide a screenshot of the IAM policy attached to the user.
* Log in as the IAM user and verify access to the S3 bucket.
* Provide a screenshot showing the IAM user accessing the S3 bucket in the AWS Console.

**5. Create a CloudWatch Alarm for CPU Usage**

* Navigate to AWS CloudWatch and create an alarm for the EC2 instance.
* Set the alarm to trigger when CPU utilization exceeds 70% for 5 minutes.
* Configure notifications via email (SNS).
* Provide a screenshot of the CloudWatch alarm configuration.

**End of Exam**

**Send your answers and screenshots via email to your instructor.**