Enterprise Cloud Migration &

Internal Infrastructure Rebuild for QTech

Submission Requirements:

Your submission for this assignment must include the following:

1. **Individual Written Report**
   An individual written report that follows the guidelines provided in this document and includes all sections required in the QTech assignment brief, covering:
   - Design and implementation of the public Auto-Scaling Web Environment on AWS.
   - Configuration and hardening of the internal secure Linux server.
   - Implementation of the automated daily S3 backup mechanism.
   - Reflections on challenges faced and how they were resolved.

2. **Configuration and Script Files**
   All relevant configuration and script files used in your solution must be submitted as **plain text (TXT) files** (compressed), including but not limited to:
   - User Data scripts.
   - Bash backup scripts.
   - Any additional shell or configuration files you created.

3. **Evidence of Implementation**
   Provide appropriate technical evidence of your work, which may include:
   - Screenshots from the AWS Management Console showing:
     - S3 bucket configuration.
     - IAM roles and policies.
     - Launch Template, Auto Scaling Group, and Application Load Balancer.
     - SNS topics and CloudWatch alarms.
   - Screenshots from the internal Linux server demonstrating:
     - Directory structure under /company.
     - User and group creation.
     - Permission settings and access control.
     - Backup logs and verification of S3 uploads.

Any instance of plagiarism will result in penalties in accordance with HTU policies and regulations. An oral discussion (viva) will be scheduled by your instructor after the assignment deadline.

Report Guidelines

Your written report must meet the following standards:

- The report must be submitted as a **Word document**.
- It must be written in a **formal business style**, using:
  - Font size: **12**
  - Line spacing: **Single**
- Each answer or section must clearly indicate the **task number and sub-task number** as defined in the assignment brief (for example: 1.1, 3.2, 7.1, etc.).
- You must provide a **step-by-step explanation** for every action you perform, including:
  - The exact commands used on the Linux server.
  - The configuration steps performed in AWS.
  - A detailed explanation of what each command or configuration does and why it was used.
- Screenshots included in the report must be:
  - Clear and readable.

Use of AI Tools

Using AI tools is allowed in a limited and responsible manner to assist you in writing code, preparing configuration files, or structuring the report. However, you must:

- Fully understand all content generated with the help of AI tools.
- Carefully review, edit, and adapt any AI-assisted content to ensure it is correct and suitable for your specific solution.
- Clearly state in your report that AI tools were used and explain:
    - Which parts they were used for (e.g., draft Bash script, refine explanation, etc.).
    - How you verified and adapted the generated content.

Part 2 – Oral Exam (Viva)

An in-class oral examination will be conducted after the submission deadline.

During the viva:

- Your answers must be clear, detailed, and technically accurate.
- You may be asked to:
    - Explain the design of your AWS infrastructure (S3, IAM, EC2, Auto Scaling, ALB, SNS, CloudWatch).
    - Demonstrate or describe the deployment of the web application on the Auto-Scaling environment.
    - Explain the directory structure, user/group configuration, and permission model on the internal Linux server.
    - Walk through the logic of your backup script and how it uploads archives to S3.
    - Explain the functionality of specific Linux or AWS commands you used.
    - Compare and contrast related commands or services (for example: chmod vs chown, or scaling policies types).
    - Troubleshoot and propose solutions for realistic server or cloud-related issues derived from the scenario.

Attendance at the oral discussion and/or any in-class exam is **mandatory** at the date and time set by your instructor. The final viva schedule will be announced after the submission period ends.

Following a recent major service disruption and the departure of multiple Cloud Administrators, QTech's cloud environment was left without proper documentation, monitoring, or operational standards. As a result, the company's public-facing web services suffered severe performance issues, and internal departments lost access to their working environment.

To avoid similar incidents, QTech has requested a complete rebuild of its cloud infrastructure, including:

- A **highly available public web application** capable of auto-scaling under fluctuating workloads.
- A **secure internal Linux server** with isolated environments for HR, Dev, and Ops.
- A **fully automated daily backup system** storing departmental data in Amazon S3.

You are assigned as the new Cloud & Systems Engineer responsible for rebuilding QTech's environment from the ground up.

---

1. Public Auto-Scaling Web Environment (AWS)

You must redesign QTech's external web platform using scalable AWS services. The application must remain available under heavy load and automatically scale when CPU usage increases.

1.1 S3 Static Content

Prepare the application's static content:

- Create an **S3 bucket**.
- Upload a static index.html file.
- Keep the bucket private.
- EC2 instances must download this file using IAM Role permissions.

---

2. IAM Configuration

To ensure secure and controlled access, you must configure an IAM Role that grants EC2 instances read-only access to S3.

Your IAM Role must:

- Allow GetObject from the specific S3 bucket.
- Be attached to EC2 instances via the Launch Template created in later steps.

---

3. Launch Template Creation

Create a Launch Template that will serve as the blueprint for all web instances in the Auto Scaling Group.

3.1 Operating System

- Amazon RHEL

3.2 User Data Script

Your User Data must:

1. Install Apache Web Server
2. Install AWS CLI
3. Download index.html from S3
4. Move it to /var/www/html/
5. Start and enable Apache

3.3 Additional Requirements

- Attach the previously created IAM Role
- Use an SSH Key Pair for admin access

---

4. Security Group Configuration

Create a Security Group to protect the EC2 instances.

Inbound Rules

- **Port 80 (HTTP):**
  - Accept traffic *only from the Load Balancer's Security Group*
- **Port 22 (SSH):**

Outbound Rules

- Allow all traffic (required for S3 access)

---

5. Auto Scaling Group (ASG)

Rebuild the public computing layer using Auto Scaling to maintain availability and resource efficiency.

5.1 ASG Configuration

- Attach the Launch Template
- Deploy EC2 instances in **All Availability Zones**
- Configure Capacity:
    - Desired: **2**
    - Minimum: **1**
    - Maximum: **4**
- Enable Metrics Collection

5.2 Load Balancer Integration

Your ASG must be connected to:

- An **Application Load Balancer**
- A dedicated **Target Group**

---

6. Application Load Balancer (ALB)

Design and configure the ALB as the public entry point of QTech's web application.

6.1 Requirements

- Internet-facing ALB
- Listener on port **80**
- Attached to the same public subnets used by the ASG

6.2 Target Group

- Protocol: HTTP
- Port: 80
- Health Check Path: /

---

7. Scaling Policy

To ensure automatic resource adjustment, configure a Target Tracking Scaling Policy:

- **Metric:** ASGAverageCPUUtilization
- **Target Value: 50%**

The ASG must automatically add or remove EC2 instances depending on total CPU load.

---

8. Monitoring & Notifications

To maintain operational visibility and prevent unnoticed failures, configure SNS and CloudWatch alerts.

8.1 SNS Topic for ASG Events

Create an SNS Topic:

- Subscribe using an email address
- Enable notifications for:
  - EC2_INSTANCE_LAUNCH
  - EC2_INSTANCE_TERMINATE

8.2 CloudWatch Alarm

Create an alarm to notify when the ASG reaches its maximum capacity:

- **Metric:** GroupDesiredCapacity
- **Threshold:** equal to **4** (MaxSize)
- **Action:** send notification to asg-capacity-alerts SNS topic

Example email subject:
Auto Scaling Group has reached maximum capacity!

---

9. Internal Secure Linux Server (HR, Dev, Ops)

QTech’s internal departments require an isolated Linux environment hosted on AWS. This server must provide:

- Isolated directories for HR, Dev, and Ops
- Dedicated department groups
- Strong access restrictions
- Automated daily S3 backups

---

10. EC2 Deployment for Internal Server

Deploy a separate EC2 instance:

10.1 Operating System

- Red Hat Enterprise Linux (RHEL)

10.2 Security Group

- Allow SSH (22)

10.3 Access

Connect via SSH using your key pair.

---

11. Departmental Directory Structure

QTech operates several departments, each requiring its own dedicated workspace for storing and managing internal files. To set this up, you must use the command-line interface to create the required directory structure and organize it according to departmental needs. Once the directories are in place, you must establish comprehensive access-control rules using advanced permission management, ensuring that members of each department can collaborate securely while preventing unauthorized access or modification.

To begin implementing this structure, create the following departmental directories:

/company/hr

/company/dev

/company/ops

/company/management

/company/it

11.1 Access Requirements

- Full isolation between departments must be enforced.
- Users in the same department must be able to collaborate in their respective departmental directory.
- Newly created files must inherit group ownership automatically using the appropriate permission mechanisms.
- Users must be prevented from deleting files they do not own, even if those files reside within their department's directory.

---

12. User Groups and Assignments

QTech's departments depend on clearly defined user accounts and group memberships to control access to internal resources. To restore proper identity and permission management, you must create and manage the required users and assign each one to the appropriate department group using the command-line interface. As part of establishing comprehensive access control, each account must follow the organization's password requirements and be placed under the correct departmental or administrative policy.

To establish proper departmental access control, you must create the following groups representing each QTech department:

hr

dev

ops

management

it

12.1 User Accounts

All required user accounts must be created and assigned to the appropriate department group.

Use the password below for all accounts:

Htu@123

User, Group, and Privilege Mapping:

Username	Department	Primary Group	Administrative Privileges	Password
sara	**HR**	**hr**	**No**	**Htu@123**
huda	**HR**	**hr**	**No**	**Htu@123**
ahmed	**Dev**	**dev**	**No**	**Htu@123**
rami	**Dev**	**dev**	**No**	**Htu@123**
omar	**Ops**	**ops**	**No**	**Htu@123**
ali	**Ops**	**ops**	**No**	**Htu@123**
manager	**Management**	**management**	**No**	**Htu@123**
admin1	**IT**	**it**	**Yes**	**Htu@123**
admin2	**IT**	**it**	**Yes**	**Htu@123**

12.2 Home Directory Requirements

All users must be created following these rules:

Each user must have a home directory created automatically during the account creation process.

Each user must belong only to their department's group without any additional group memberships, except where administrative privileges are required.

Only the IT users (admin1 and admin2) must receive administrative privileges by being added to the appropriate administrative group.

---

13. Backup Mechanism Implementation

QTech requires a dependable backup routine that runs automatically without manual intervention. To accomplish this, you must first create an advanced Bash script that performs the required backup operations. After preparing the script, you will automate the backup task implemented in your Bash script by scheduling it to run at the appropriate time using cron.

To begin implementing the automated backup process, create a script that performs the following actions:

13.1 Backup Script

Create a Bash script that:

- Archives all departmental directories located under /company on a daily basis
- Compresses each directory into an individual .tar.gz file
  - Examples:
    - hr_YYYY-MM-DD.tar.gz
    - dev_YYYY-MM-DD.tar.gz
    - ops_YYYY-MM-DD.tar.gz
    - management_YYYY-MM-DD.tar.gz
    - it_YYYY-MM-DD.tar.gz
- Uploads all generated archive files to the designated Amazon S3 backup bucket
- Writes detailed operational logs to /var/log/s3backup.log
- Ensures the entire process runs in a fully automated and fault-tolerant manner

> Note:
> The backup script must be implemented using robust coding practices, ensuring it can properly handle potential errors, validate prerequisites before execution, and maintain consistent and clear logging throughout its entire runtime. All uploads to S3 must be confirmed to ensure backup integrity.

13.2 Automation

Configure a cron job to run the backup script automatically at **2:00 AM every day**.

This scheduled task must:

- Trigger the execution of the backup script at the designated time
- Ensure daily S3 backup uploads are completed successfully
- Guarantee that each operation is logged and any anomalies are recorded for review

Important Note

You are required to follow the scenario and implement all tasks requested by the company. The implementation steps provided in this document serve as guidance to support you during the assignment; they are **not meant to restrict your technical approach**. You may modify, improve, or extend any part of the implementation if your changes are clearly explained and technically justified within your report.

Your report must clearly state:

- What modifications you made
- Why you made these changes

BEST WISHES