Instructions

Examination paper released: **04:12.2023 10:00**

Examination deadline: 11.12.2023 **10:00 AM**

Exam format: Individual written home examination

Final report format: Recommended LaTeX or Word format and font 12 with 1.0 spacing. List of the bibliography, appendix can come in addition to this.

Grading scale: The Norwegian grading system uses the graded scale A - F, where A is the best grade, E is the lowest pass grade, and F is fail.

Weighting: 100% of the overall grade

Support materials: All supported materials are allowed.

Plagiarism control: We expect your independent work. Please, use citations and quotations if there is a material you want to include in the report. **You cannot copy from a friend or schoolmate. You are not allowed to request someone to do the exams for you.**

Oppgave 1- 70% of the exams

Case Description

Medicoms has recently decided to move to the cloud. Their major concern is security so they have decided to hire a consultant to design a secure solution for them. The solution should satisfy the following security requirements:

1. The solution should ensure segregation of duty between platform and infrastructure administrators as well as secure infrastructure, and platform access.
2. The solution should enforce least privilege for all resources, S3 buckets, users etc.
3. The solution should support both account and network isolation.
4. The solution should implement network security including defense in-depth.
5. The solution should ensure application security.

In response to Medicoms' request, the consultant developed a terraform script that will automatically create a cloud solution for Medicoms. The script creates one VPC and two subnets in one account and a directory **/home/ubuntu/logs** for application logs. It also creates an S3 bucket with name sensitive-bucket-xxxx to share data among the developers.

1. According to the consultant, the terraform script should be run using the access key ID and secret access key of AWS account root user to ensure easy deployment.
2. The private key of the SSH key pairs should be stored on the public instance to enable easy SSH access to the private instance.
3. Three tier architecture is not necessary because both the internal and private tiers are not accessible from the internet, therefore the script only implements 2-tier architecture with public and private subnets in one account.
4. Instance metadata service should be set to optional.

Your Tasks

1. You have been asked by Medicoms to run the terraform script and analyze every aspect of the deployment to determine if the consultant meets all the **FIVE** security requirements of Medicoms**.**

   How to answer this question:

   - **You are expected to explain each of the requirements.**

- **Run the script and analyze the solution to determine if the implementation has any security risk.**
- **Show how to mitigate the risk if you identify any and which cloud service(s) is/are required to do so [30 points].**

This task does not require any configuration from you just deploy the script and analyze the results to determine if they meet Medicoms' security requirements.

2. You are required to analyze the consultants' suggestions to determine if they are sound security advice. If not suggest improvements that are consistent with cloud security best practices **[20 points].**
3. List 5 critical security issues you can mitigate to improve the security of the overall solution. Configure your own secure alternative solution to addresses these 5 critical issues [20 points]. **This task requires actual configuration, show screenshots and explanations. Make sure you write a clear and easy to read report**.

Where to find the script and configuration

The script and instructions to run it is attached to the exams**.**

What Give marks

- **Correct explanation of requirements.**
- **Correct identification and explanation of security risk if any.**
- **Show how to mitigate the risk if any and which cloud service(s) is/are required to do so.**
- **Correct analysis and discussion of the consultant's suggestions.**
- **Suggestion and implementation of alternative solutions and services required if any.**

Oppgave 2- 30% of the Exams

1. What is the meaning of the following statement "Customer is responsible for security **IN** the cloud and provider is responsible for security **OF** the cloud" [**2 Points**].
2. The table below is the outbound network access control (NACL) configuration of a public EC2 instance. Explain the function of NACLs, rule priorities and whether the Google's DNS server, 8.8.8.8 can be reached by an administrator of the EC2 instance [**5 Points**].

Type	Port	Source	Allow/Deny
100	ALL	0.0.0.0/0	DENY
101	ALL	8.8.8.8	ALLOW

3. Write a short note explaining inbound and outbound traffic and whether they can be restricted to specific IP ranges [**3 Points**].
4. Explain the principles behind effective policies and write down the effective policy when the following policies are combined [**5 Points**]:

Rule	Policy	Policy type
1	IAM Policy	S3 FullAccess

2	SCP	Full Access all resources
3	Permission boundary	EC2 Full Access

5. A private AWS instance is unable to receive updates from the internet if the security groups are configured correctly, what might be the possible cause of the issue. Explain why [**5 Points**].
6. Discuss the continuous monitoring concept and explain the function of three AWS continuous monitoring services [**4 Points**].
7. Database of an organization was compromised due to SQL injection flaws. What can the organization do to quickly fix the SQL injection vulnerability [**3 points**].
8. Identify the kind of log below and explain each of the field [**3 Points**].
   2 123456789010 eni-1235b8ca123456789 172.31.16.139 172.31.16.21 20641 22 6 20 4249 1418530010 1418530070 REJECT OK

Before You Run the Script

1. Generate access key ID and secret access key for a user with the necessary privilege (such as administrator access or root access whichever is more secure).
2. Configure your access key ID and secret access key on your laptop with the **aws configure** command.
3. Specify a region of your choice.

How to Run the Script

1. Download the consultant's script from the exam's portal.
2. Unzip the consultant file.
3. Change directory to the consultant folder where the script is.
4. Install terraform on your laptop.
5. Run the command **terraform init** in the consultant folder.
6. Run **terraform validate** to check if everything is fine.
7. Run **terraform plan** and then **terraform apply** to execute the script.
8. Type yes if asked. Wait for some few minutes.
9. The script will automatically generate an SSH key called examkey.pem in the script's folder.
10. Use this key to access the instances.
11. Go to your account, choose the region you configured your access credentials.
12. Check if the VPC, the subnets, EC2 instances, routes, gateways, and buckets are created.
13. You can now analyze the deployment to answer the exams questions.
14. Run **terraform destroy** to delete everything from your account whenever you want to take a long break. Type yes if asked.
15. You can always recreate the environment with the **terraform apply** command.