Q-1. Explain RTO and RPO.

1. RTO is the recovery time objective and RPO is the recovery point objective. Therefore, RTO indicates the maximum time for which data can be offline after a security incident and RPO indicates the maximum time, indicated by service level agreements, for which the data might be lost according to the security incident (Hamadah, 2019).

Q-2. What are the major benefits of using Terraform?

2. The major benefits of using Terraform are as follows:
    a. Providing consistency across various cloud platforms through the provided service of infrastructure as code (IaC)
    b. Terraform provides an automated workflow ecosystem by managing cloud resource lifecycles
    c. Risk is significantly reduced since the IaC ecosystem of Terraform provides validation before execution
    d. Terraform supports the tenet of being modular and promotes reusability across various projects.

Q-3. What is “in Transit” and “at rest” encryption?

3. To understand the answer to this, first consider each physical data position with respect to time:
    a. Encryption in transit implies that data is moved from a given source to a destination is relatively safe from malicious actors. This can be accomplished by various protocols such as secure hypertext transfer protocol (HTTPS), transport layer security (TLS), or secure sockets layer (SSL) using an RSA keypair consisting of public and private counterparts. (*Data Protection: : Data In transit vs. Data At Rest*, 2019)
    b. Therefore, encryption at rest implies that the data is at some stable location, such as a company hard drive, or a database, and is encrypted for secure storage. Commonly, cryptographic algorithms such as SHA256 or AES, are used to provide such security. Then, only the actor with the proper key can unlock and decipher the data. (*Data Protection: : Data In transit vs. Data At Rest*, 2019)

Q-4. What is S3 replication? Can I select only a set of files to replicate?

4. S3 replication is the aspect of a data recovery strategy concerned with establishing data redundancy across S3 buckets and availability zones. This feature increases the overall fault tolerance of the system and promotes adherence to previously established service level agreements. Therefore, replication can affect either the entire bucket or files added to that bucket after redundancy has been enabled.

Q-5. What is “Tag” in AWS?

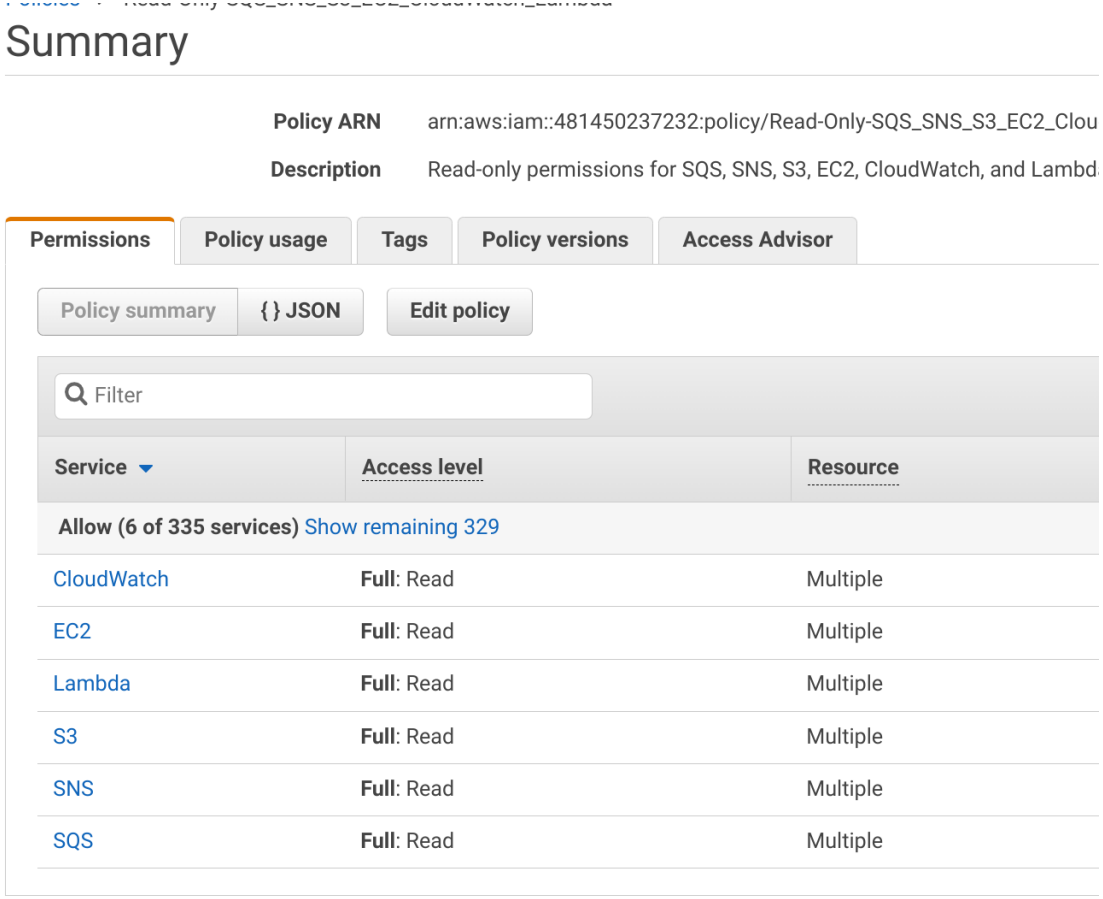
5. Tags in AWS serve to promote organizational structure within the organizational resource ecosystem. Most effectively, they are business-relevant and include subsets from technical tags and automation-related tags. In this way, technical tags imply indicators such as name, environment, application ID, or cluster. Thus, automation tags imply indicators such as data, security, or if a resource should be included in an automated activity via opt-out/opt-in.

Q-6. What is CICD?

6. CICD implies continuous integration and continuous deployment and is a software development lifecycle model. CI/CD is typically supported by a microservice architecture where modules use application programming interfaces (API) for interaction (Paul, 2020).

Q-7. Create user “sethm” and assign read-only permission for Ec2, S3, SQS, SNS, Lambda and CloudWatch. Send details in the doc file for username, password, and login details.

7. Answer:
    a. User creation:
        i.
```
[cloudshell-user@ip-10-1-176-97 ~]$ aws iam create-user --user-name sethm
{
    "User": {
        "Path": "/",
        "UserName": "sethm",
        "UserId": "AIDAXAGFLTUYNRT6YKXC4",
        "Arn": "arn:aws:iam::481450237232:user/sethm",
        "CreateDate": "2022-10-07T22:56:31+00:00"
    }
}
[cloudshell-user@ip-10-1-176-97 ~]$
```
        ii. Console Signin Link:
            1. https://481450237232.signin.aws.amazon.com/console
        iii. Password:
            1. TemproaryPassword001
    b. Make policy:

i. 

(forgot how to do it via CLI)

c. Read-only permissions:

i.
```
[cloudshell-user@ip-10-1-176-97 ~]$ aws iam attach-user-policy --user-name sethm --policy-arn arn:aws:iam::48145
0237232:policy/Read-Only-SQS_SNS_S3_EC2_CloudWatch_Lambda
[cloudshell-user@ip-10-1-176-97 ~]$
```

Q-8. Create an S3 bucket with versioning on, and set up an event so that whenever anyone deletes an object, you will get a notification. You have to use either CLI/CloudFormation/Terraform to provision resources. Once you test, delete/destroy all resources and send code/templates.

8. Please see included file *main.tf*

Q-9. Create Role for Lambda service to get/access all s3 buckets and Ec2 instances operation using terraform.

9. Please see the included file *main1.tf*

Q-10. Create bucket using CLI with object lock enabled. Upload 2 files via CLI. Take screenshots of S3 buckets and send along with the CLI command.

10.
```
[cloudshell-user@ip-10-1-176-97 ~]$ aws s3api create-bucket --bucket recovery-bucket20221007 --object-lock-enabled-for-bucket
{
    "Location": "/recovery-bucket20221007"
}
```

References:

Data Protection: Data In transit vs. Data At Rest. (2019, July 15). Retrieved from

https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest.

Hamadah, S. (2019). ICIC Express Letters ICIC International © 2019 ISSN. *ICIC Express Letters*, *13*, 593–599.

https://doi.org/10.24507/icicel.13.07.593

Paul, H. (2020, April 29). Build An Automated Testing Pipeline With GitLab CI/CD & Selenium Grid. Retrieved from

https://www.lambdatest.com/blog/automated-testing-pipeline-with-gitlab-ci-cd-and-selenium/