Problem Statement:

You work for XYZ Corporation, and the company is using AWS for its infrastructure. For administrative purposes, it needs to provide certain employees with access to certain tasks.

You are asked to:

1. a) Create a user account that can login to the console

b) Create a group, and make sure that the group can only launch or stop EC2 instances using the previously created account

2. a) Provide the permission to let the users of the previously created account create VPCs, subnets, NACL, and security groups

b) Further, add the permission for the users to be able to crea te an RDS instance

c) Explore security options to protect the AWS resources and secure the permissions provided to the group

d) Create an IAM Access Analyzer, and find any role that might indicate a potential risk

Procedure: -

To address the tasks and implement the required permissions and security measures:

1. User and Group Setup:

a) Create a User Account:

- Create an IAM user with console access.
- Assign appropriate permissions to the user based on the tasks they need to perform.

b) Create a Group for EC2 Instance Management:

- Create an IAM group (e.g., EC2InstanceManagers).
- Attach a policy to the group that grants permissions to launch or stop EC2 instances.

2. Permissions for VPC, Subnets, NACLs, Security Groups, and RDS Instances:

a) Provide Permissions for VPC, Subnets, NACLs, and Security Groups:

- Create an IAM policy granting permissions to create VPCs, subnets, NACLs, and security groups.
- Attach the policy to the user group.

b) Add Permissions for RDS Instance Creation:

- Create an IAM policy granting permissions to create RDS instances.
- Attach the policy to the user group.

3. Security Options for Resource Protection and Permission Management:

a) Secure Permissions:

- Follow the principle of least privilege, granting only the permissions necessary for each user or group.

- Regularly review and audit IAM policies to ensure they align with security requirements.

b) Use Resource Tagging:

- Tag AWS resources with appropriate metadata to track ownership, usage, and compliance requirements.

- Leverage resource tags in IAM policies for fine-grained access control.

c) Enable AWS CloudTrail:

- Enable AWS CloudTrail to log all API activity across AWS services.

- Monitor CloudTrail logs for unauthorized actions and security incidents.

d) Implement IAM Access Analyzer:

- Create an IAM Access Analyzer to continuously analyze permissions granted to IAM roles and identify any potential risks or unintended access.

- Review access analyzer findings regularly and remediate any identified risks.

Conclusion:

By following these steps and best practices, XYZ Corporation can effectively manage user access, secure AWS resources, and ensure compliance with security policies and regulations. Regular monitoring, auditing, and enforcement of security measures will help maintain a secure and compliant AWS environment.