**Applied Cloud Computing - DIY Project 1**

You are advised to complete the following tasks related to Identity and Access Management of any cloud services (e.g. AWS). Perform the following procedures as listed below:

1. Login as root user and create IAM group called Administrators. Attach the managed policy <policy name>, to the administrator group.
2. Customize a sign-in link, and write down the new link name in full.
3. Create a password policy for your account.
4. While logged in as the root user, create a new IAM user called Administrator.
5. Add the new user created above to the Administrators group.
6. On the details page for the administrator user, create a password.
7. Log out as the root user.
8. Use the customized sign-in link to sign in as Administrator.
9. While signed in as Administrator, create an Amazon EC2-type role named TestClient.
10. Attach the managed policy, <ReadOnlyAccess> to the TestClient.
11. Launch an Amazon Linux EC2 instance with the new role attached.
12. SSH into the new instance, and use the CLI to list the contents of an Amazon S3 bucket.
13. Now, add a policy to your IAM Administrator user with a conflicting permission. Use the policy generator to create a new policy. Create the policy with effect: Deny;AWS Service:Amazon S3;Actions:\*; and ARN:\*.
14. Attach the new policy to the Administrators group.
15. Use the CLI to attempt to list the contents of an Amazon S3 bucket. The policy that allows access and the policy that denies access should resolve to deny access.

Perform each steps using your cloud account login and take screen shots for each steps. Your answer document should comprise of steps, explanations/commands/codes and screen shots.