Scenario for Project 2

Instructions: This project is a part of your assessment.

Scenario:

Heaven Classics successfully creates an EC2 Server Instance for Windows 2012 Server. After launching the instance on the server, the next step was to monitor the operations.

Monitoring is important to keep an eye on the performance of an EC2 instance. It helps gather data from all parts, and is useful for debugging failure.

The monitoring team at Heaven Classics started monitoring activities using the CloudWatch Service in the AWS Management Console. The Heaven Classics support team were required to meet the following objectives:

1. Check the CPU Utilization.

2. Create an Alarm.

3. Create an IAM User.

4. Create the IAM Administrator Group, and add the user to the Administrator Group.

5. Create a Role

PREFACE

This mini project of course aws technical essensials of master course of cloud architect has been done under the guidance of ***Simplilearn Solutions*** self pace learning by ***PRAKHAR SRIVASTAVA*** .

SCREENSHOT DESCRIPTION STEP BY STEP SOLUTION OF PROJECT

1. First of login to aws console from lms portal with username and password.

2. Going services option ***click*** -> services->***launch*** instances then ***select***->windows server 2012 R2base.
3. Then.click freetier eligible option on the list which has ***general purpose*** type of ***t2.micro*** & memory of ***1 gib*** , then review and then ***launch***.
4. During launching of instance, a key pair will be generated ,downloaded and used for public–**key** cryptography to encrypt and decrypt login information.
5. After going to EC2 instances option ,you can that machine is ready.
6. You can come in bottom in the monitoring option,you can look to the cpu utilization.
7. There in the top right side in monitoring section ,you can create alarm for cpu utilization using sns services according to requirement.
8. Now come on the IAM service of option in service section.as I Prakhar Srivvastava is already a IAM user so, if you have to create on users ->username->access type->click>then create.
9. Click on groups for creating administrative group then name it,then attach policy like I have administrator then I have opted policy adminstartor then review it and create group.
10. From 9 point you can create user,go to set permission ,click on add user in group,click next,and added in group.
11. To create a role ,click->iam->role,then another aws account and next by giving account id and click on multiple factor authentication ,then either create on policy or take from below in my administrator policy is give so I just clicked.finally I given the role name and description.and created role.
12. To check user in group.simply iam->groups->users .