AWS Assigning Permission via Groups

In Chapter 10, we discuss how IT resources are delineated using Cloud-Based Security Group. Although in AWS Security Groups acts as Firewall rules, the concept of allow access to resources are done through grouping objects that might have similar functions. In AWS, we create IAM *users*, put them into IAM *groups*, and then apply *permissions* to that group. The same can be done using IAM Roles, however IAM Roles are to assign permissions on Cloud Services for access to other Services (ie. An EC2 instance need to access S3 storage).

**Prerequisite**

If you didn’t keep an EC2 instance from previous lab, create either a Windows or Linux EC2 before you start. Either way, make sure the Instance is NOT running before you proceed.

**Create New Group**

1) Log into your AWS console using your ***Administrator*** account.

2) Go to **IAM** under **Services.**

3) Click on **User groups** on the navigation pane.

4) Click **Create group** button.

5) For the User group name, type **EC2Start-Stop-grp** then scroll to the bottom and click the **Create group** button. Your group will have permissions undefined.

**Create New Policy**

6) On the navigation pane, **Policies**

7) Click the **Create Policy** button

8) Click the **JSON** tab and then copy/paste the JSON code below into the window. Make sure there are no errors.

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Action": [

"ec2:DescribeInstances",

"ec2:DescribeInstanceStatus",

"ec2:DescribeTags"

],

"Resource": "\*"

},

{

"Effect": "Allow",

"Action": [

"ec2:StartInstances",

"ec2:StopInstances"

],

"Resource": "\*"

}

]

}

…..Last line. It should be blank in the AWS JSON window

9) After confirming no errors, click the **Next: Tags** button

10) No Tags are necessary, click **Next: Review**

11) Under Review policy, give it the name **EC2Start-Stop-grp-Policy**

12) Click **Create Policy**

**Create New User**

13) On the navigation pane, click **Users**

14) Add a user called ***TestUser1***.

15) Check the *Provide user access to the AWS Console* box

16) Select **I want to create an IAM user** in the *Are you providing console access to a person?* box.

17) Select **Custom password** and uncheck **User must create a new password at the next sign-in**.

18) Click **Next.**

19) Under *Permissions option* make sure *Add user to group* is selected*.*

20 ) Under User groups, check **EC2Start-Stop-grp**

21) Click **Next**

22) On the Review and create page, click **Create user** button

23) Download the .CSV file to your computer. Save it as *TestUser1.csv*

24) Click the **Return to user list** button

**Testing**

25) Open an *Incognito* Window in Chrome or *Private* Window in Firefox. These browser windows(tabs) do not store cookies so it’s not aware you’re already logged into the AWS console

26) Copy/paste your alias URL into the browser. If you use your account number URL, select IAM user (not Root User)

27) Log in using *TestUser1* and the password

28) Select the **N. Virginia** region.

29) Under **Services**, go to **Compute** then **EC2**.

30) Note you can’t get any information about Instances. All you see are API Errors. This is because TestUser1 has no permission set.

31) Click on **Launch Instance** button and **Launch Instance** from the drop down. If the try to create a new instance you should get an error stating you’re not authorized.

32) Go back to your AWS Console where you’re logged in as Administrator.

33) Click on (IAM) **User groups** on the left, then **EC2Start-Stop-grp**

34) Click **Permissions**

35) Under **Add permission** dropdown, select **Attach Policies**

36) Check the box next to **EC2Start-Stop-grp-Policy**

37) Scroll down and click **Add permissions**

38) Click on **User groups** in left pane. Your *EC2Start-Stop* group should now show a Defined permission.

39) Go back to your Incognito windows with TestUser1 still logged in.

40) Go to **Services** then **EC2** (EC2 Dashboard)

41) You should now be able to see an Instances (1) count and Instances Running count (0).

42) Click on **Instances** 1.

43) Check the box next to your server and click the **Instance State** dropdown.

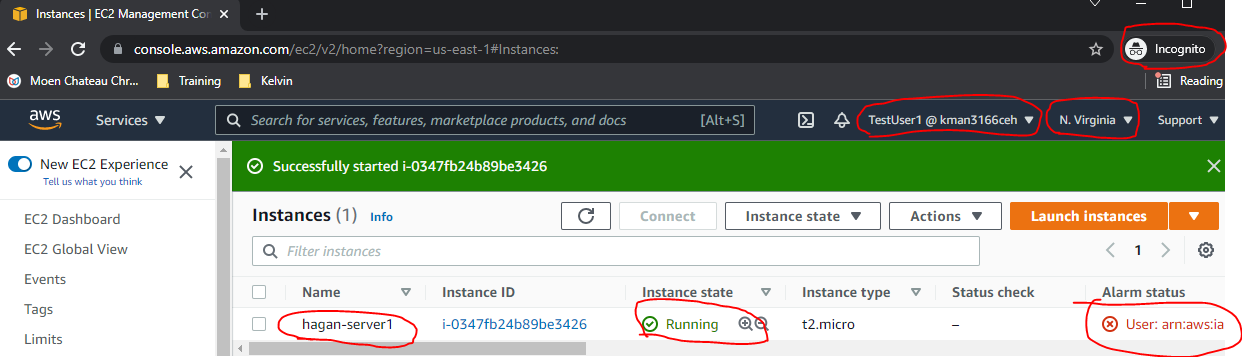
44) Click **Start** **instance**. You should be able to start instance at this point.

45) Wait until the instance status is running (you may have to refresh a few times).

46) Open a Word Doc and call it ***yourlastname*-AWSGroupPerms.docx**

47) Capture and paste the following screens. Make sure to include the things I have circled.

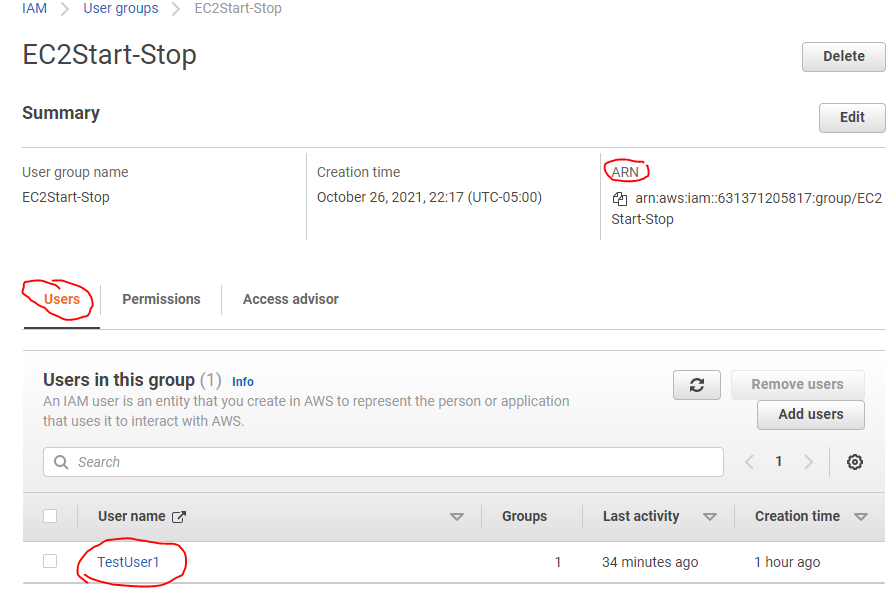
**Screenshot of instance started under TestUser1. Paste into Word doc under heading Screenshot 1.**



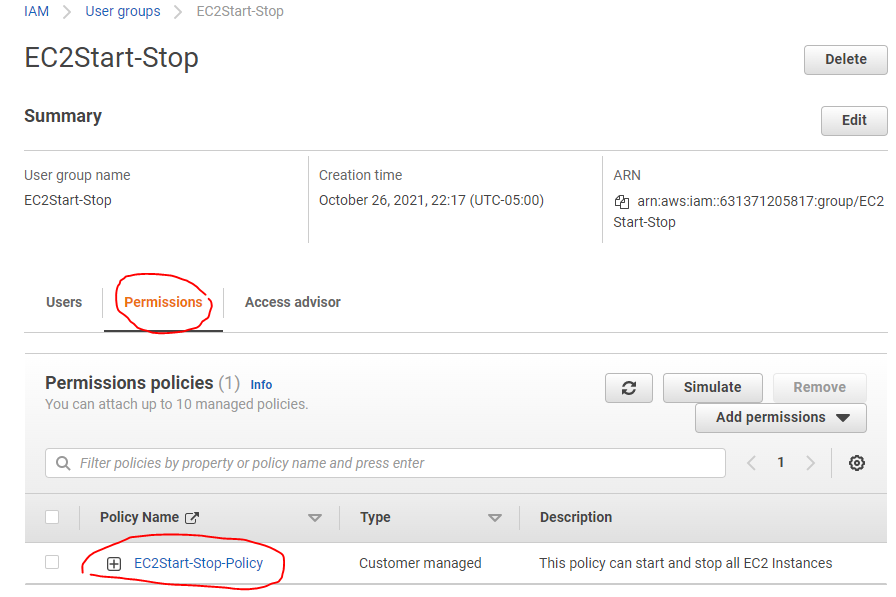
48) Go back to AWS Administrator console and select (IAM) **User groups**.

49) Click on your **EC2START-Stop-grp** group. Capture/paste the following into your Word doc:

**Screenshot of group’s Users. Paste into Word doc under heading Screenshot 2.**



**Screenshot of group’s Permissions. Paste into Word doc under heading Screenshot 3.**



50) Don’t forget to Stop/Terminate the Instance in the Administrator console and logout.

**Submission**

51) Save and upload Word doc to Bb for credit.