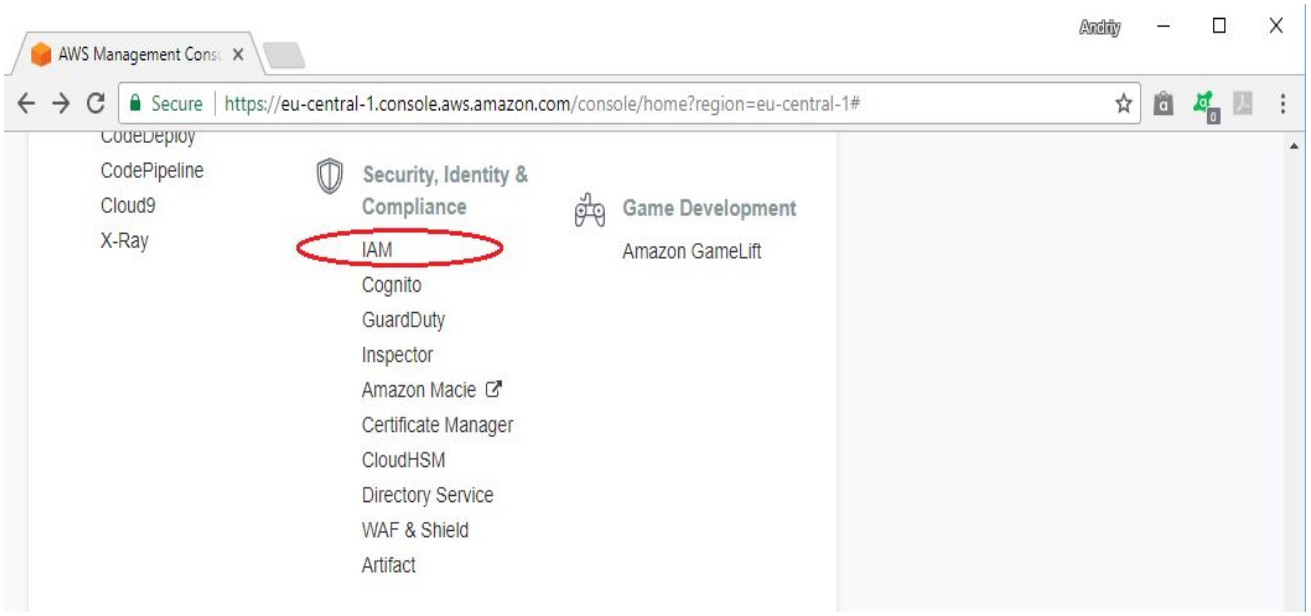
MODULE 5 – LAB EXERCISES

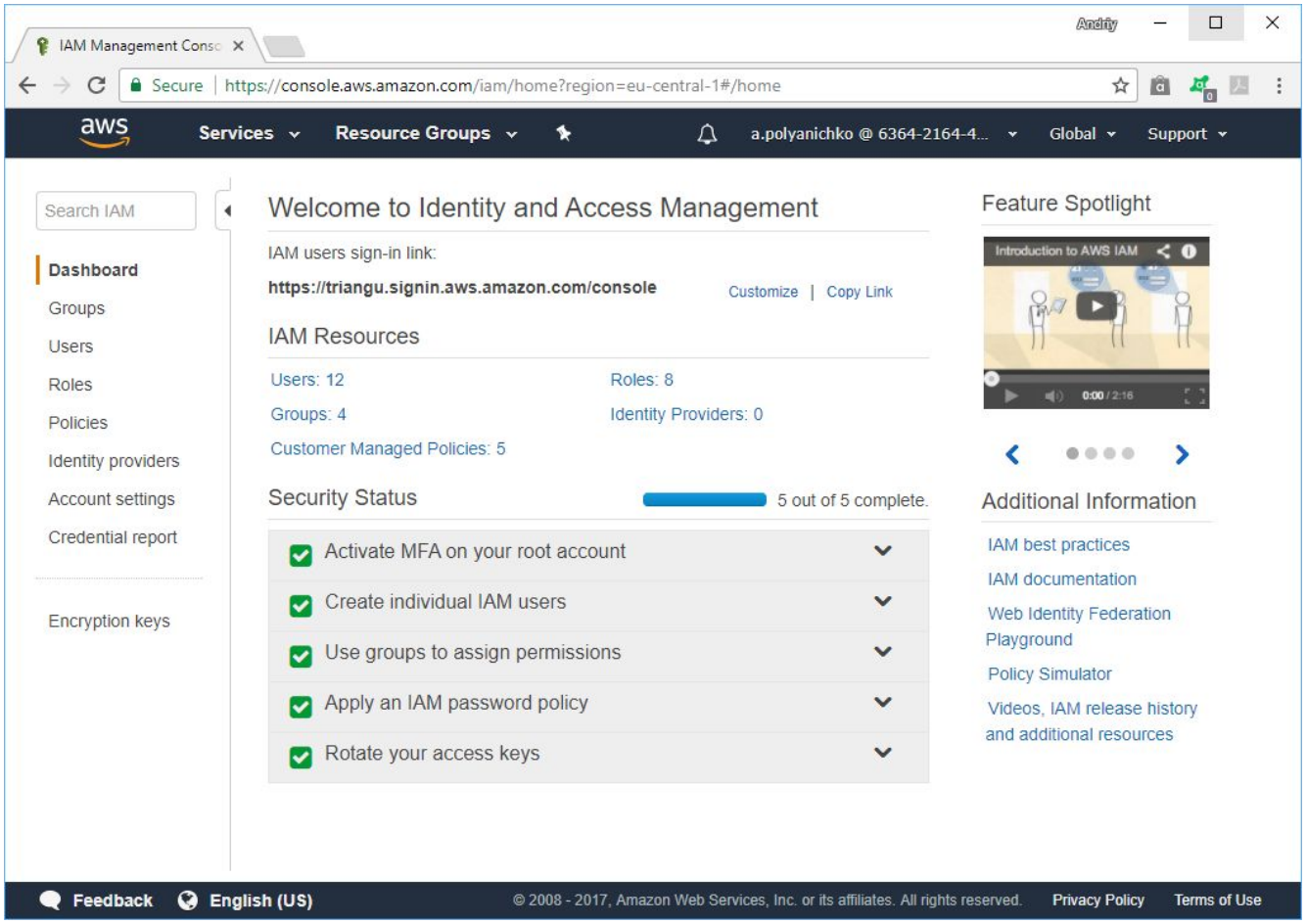
During the hands-on exercises you will get acquainted with the main points related to the management and configuration of Identity and Access Management (IAM) functionality.

1. IAM Operation Getting Started

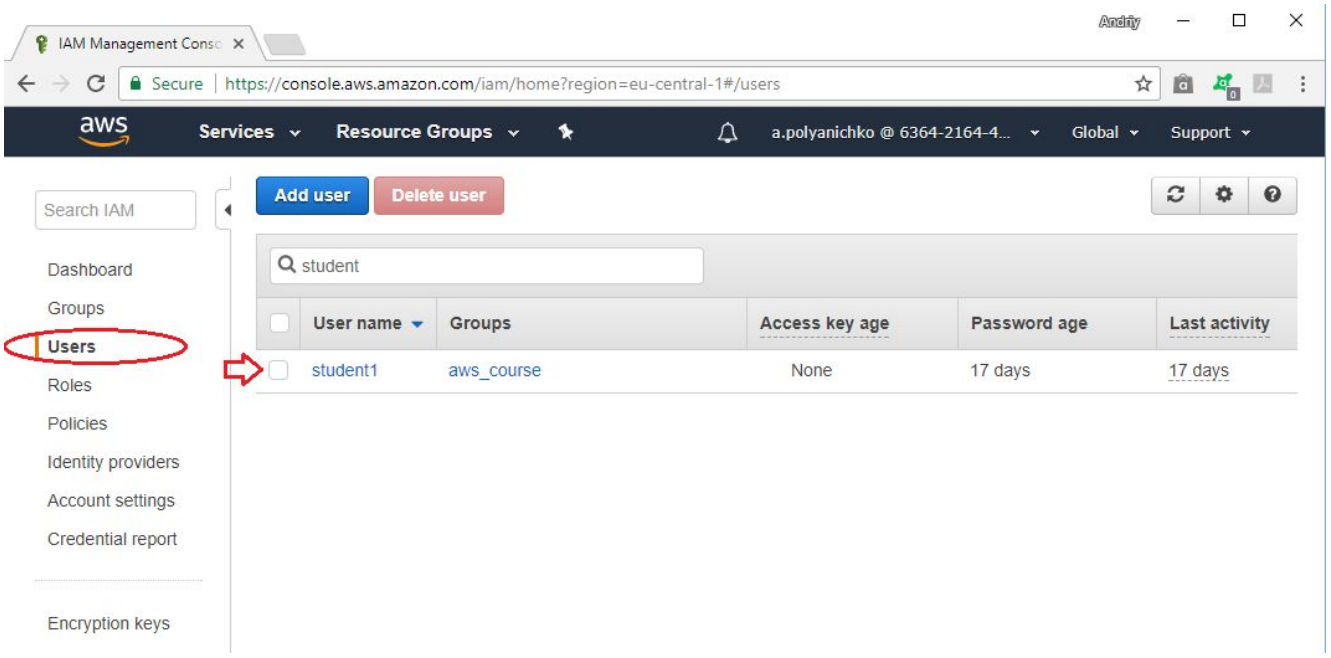
Open AWS Management Console as usual and then find and click on IAM link:



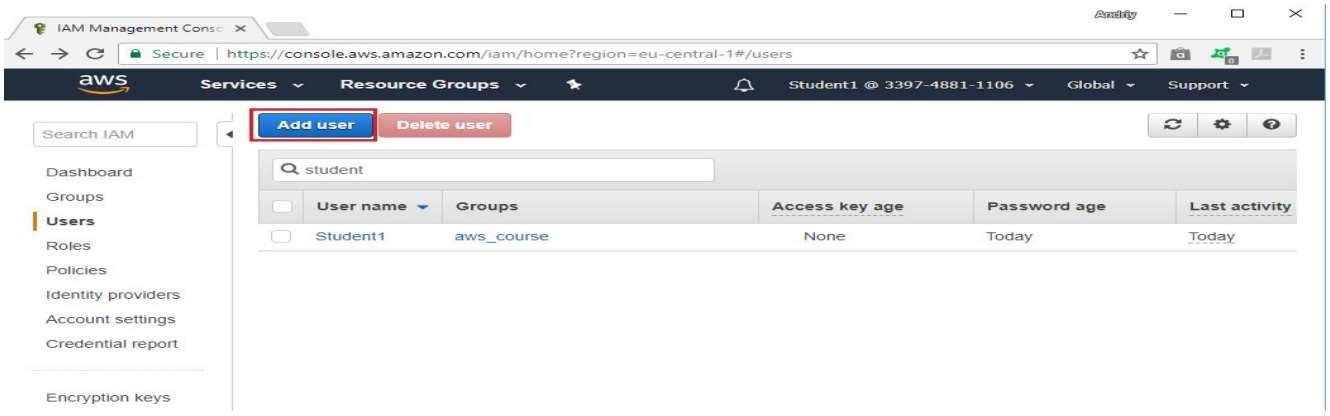
IAM Dashboard main page will be opened:



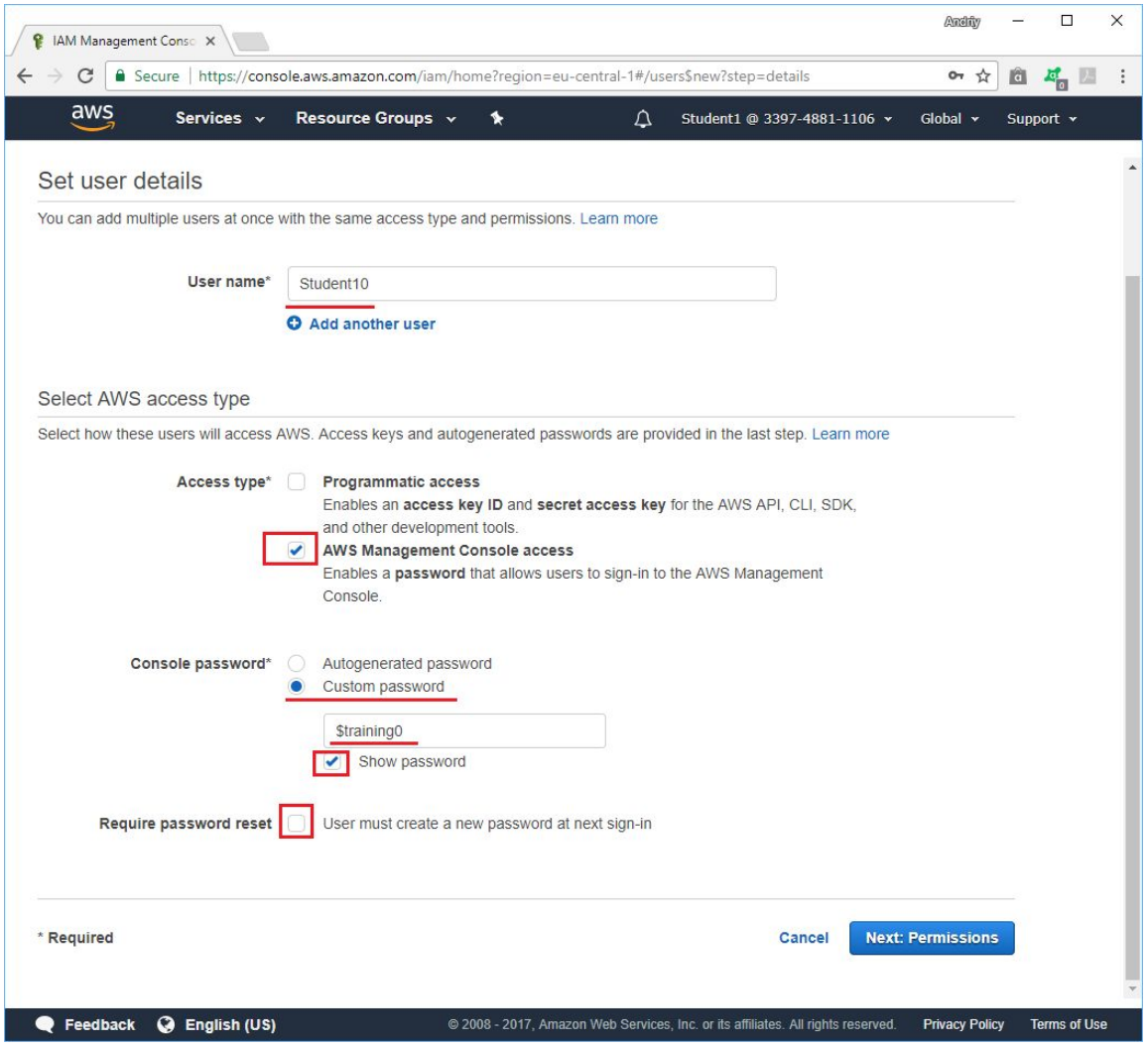
Click on “Users” link at left-side menu ribbon and find yourself in the list:



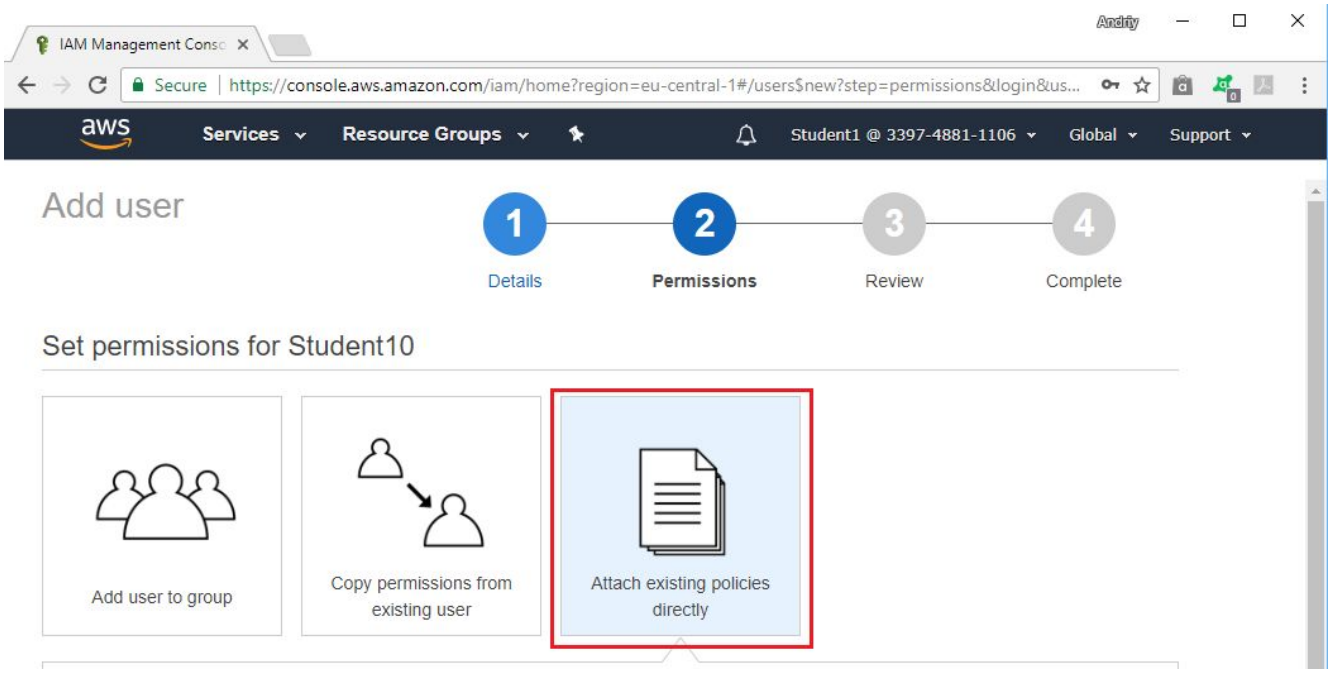
Click on “Add User” button to start creation of new user:



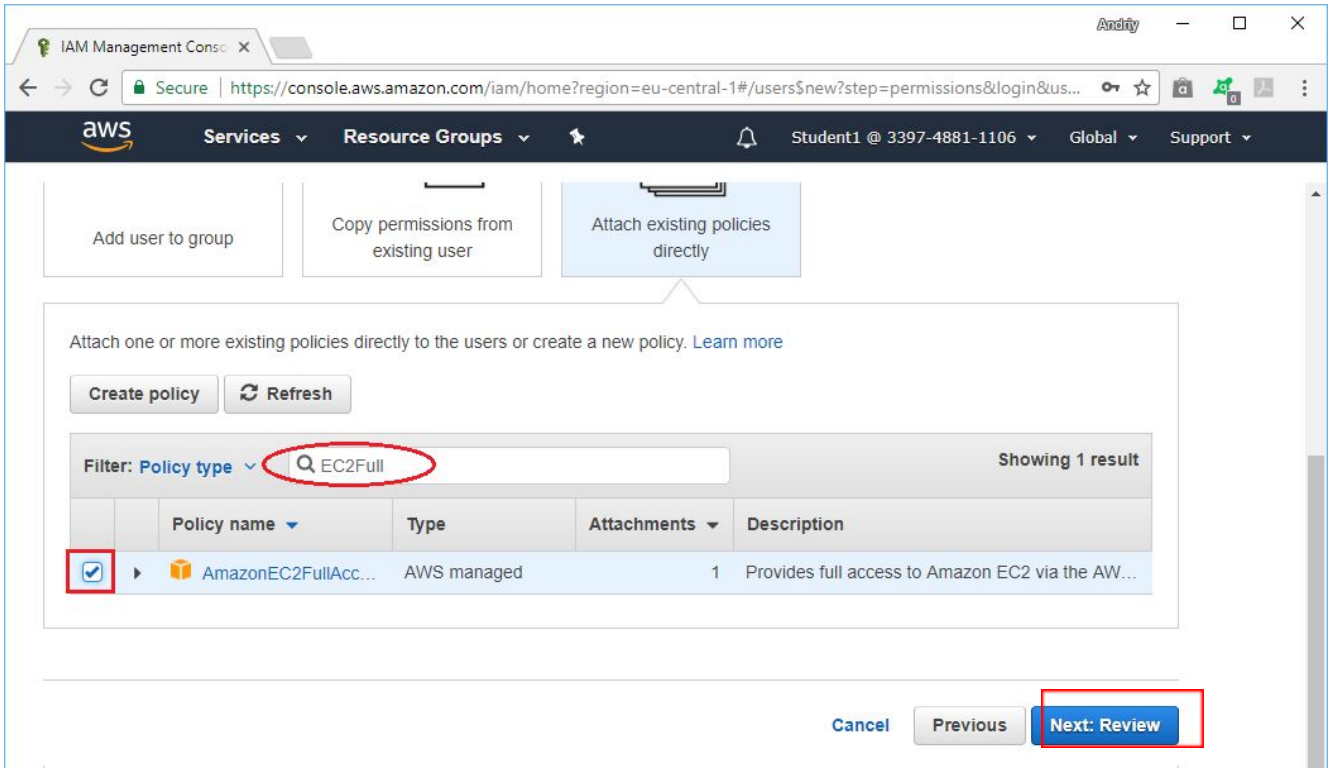
On the next page specify user details as shown below:



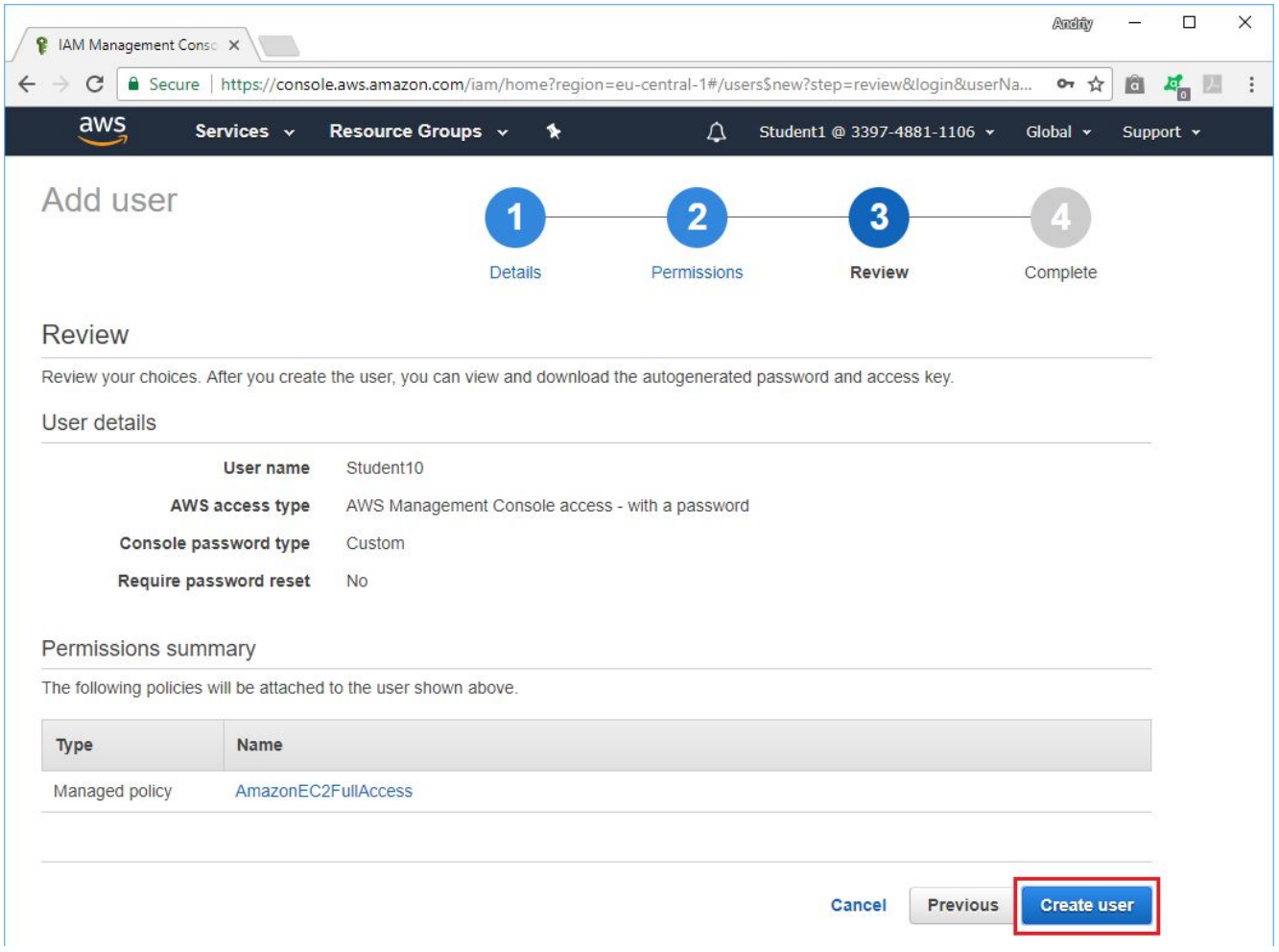
On the next page select “Add existing policies directly” option:



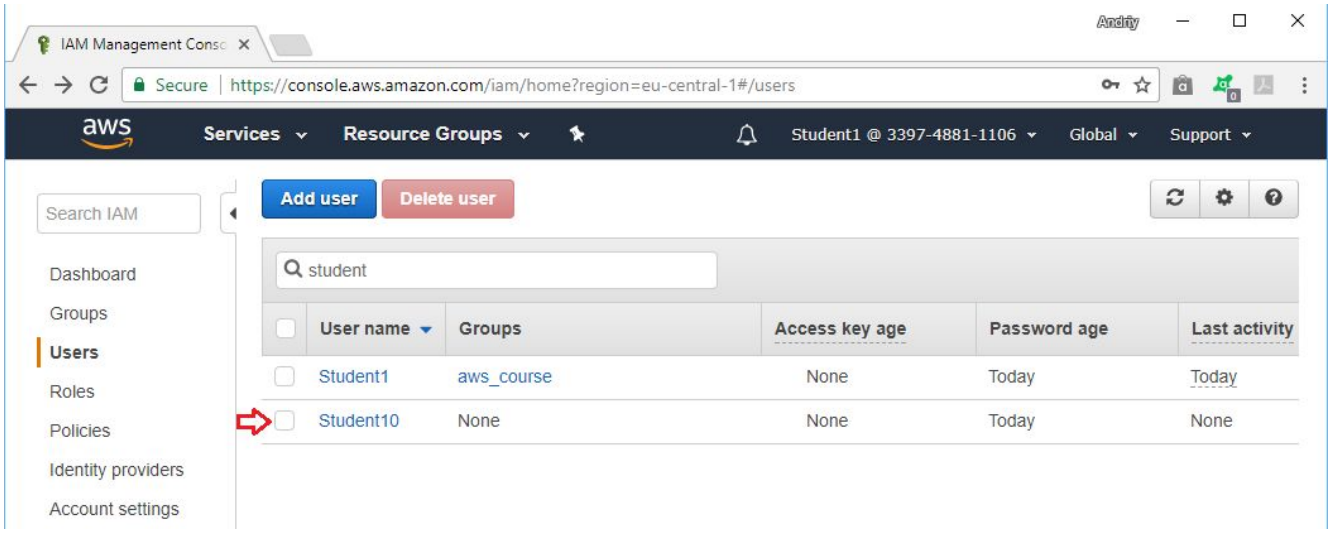
and then find and select "AmazonEC2FullAccess" policy name using filter field by type of policy as shown below, then click on "Next: Review: button:



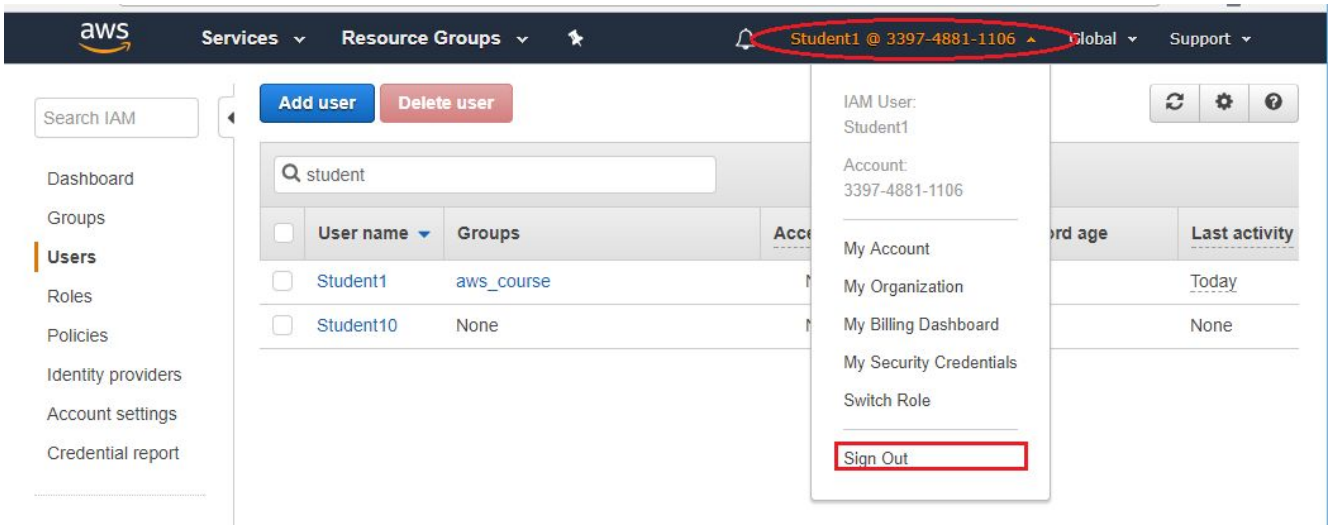
Click on “Create User” button:



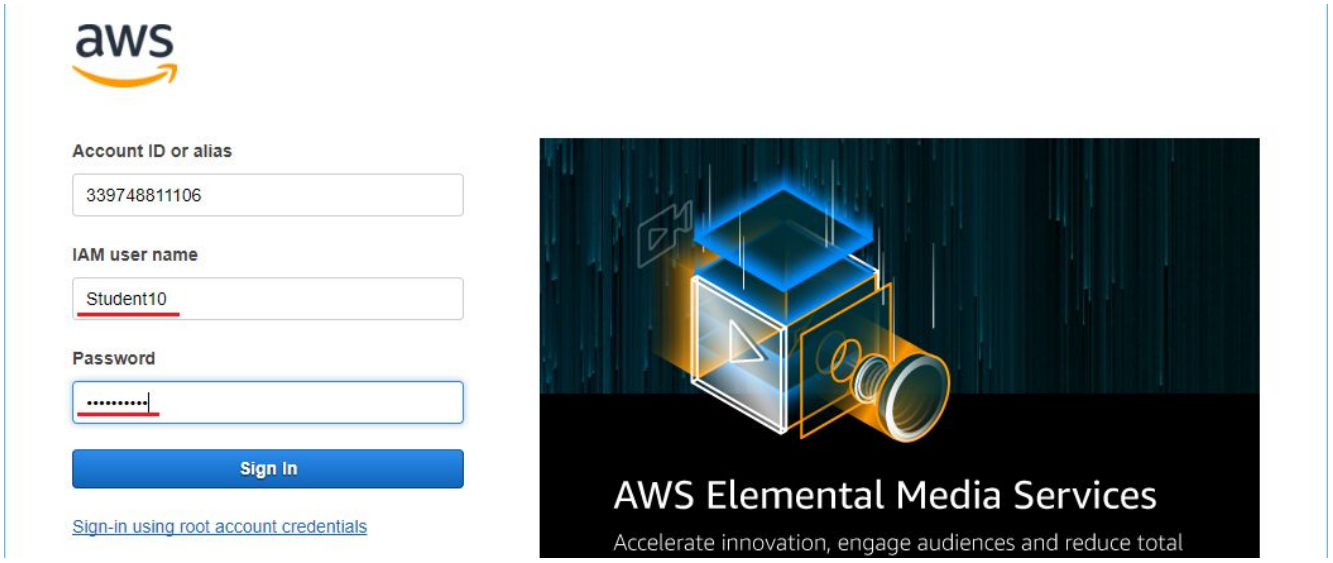
then confirm the creation of new user and finally find it in the list of available users:



Sign-out from your current account using top menu:



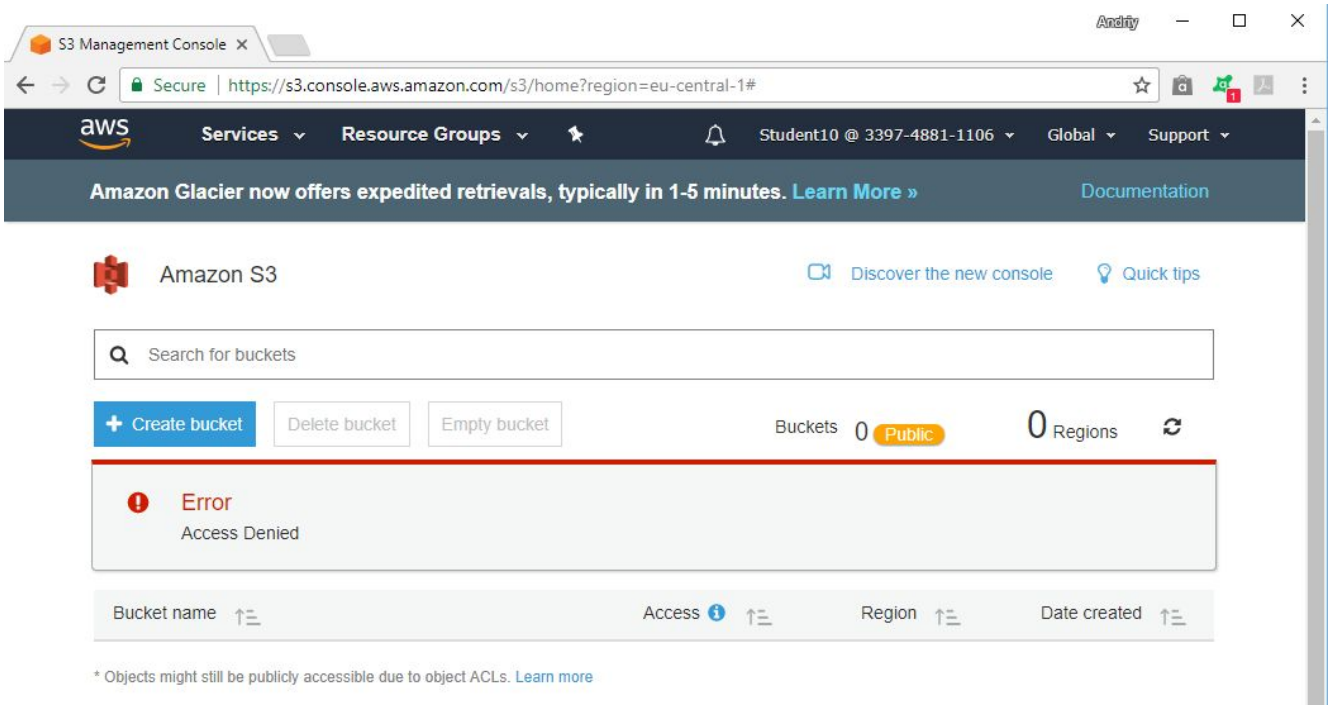
and log in again using Username and password of user you've created before:



You will enter AWS Management Console as usual.

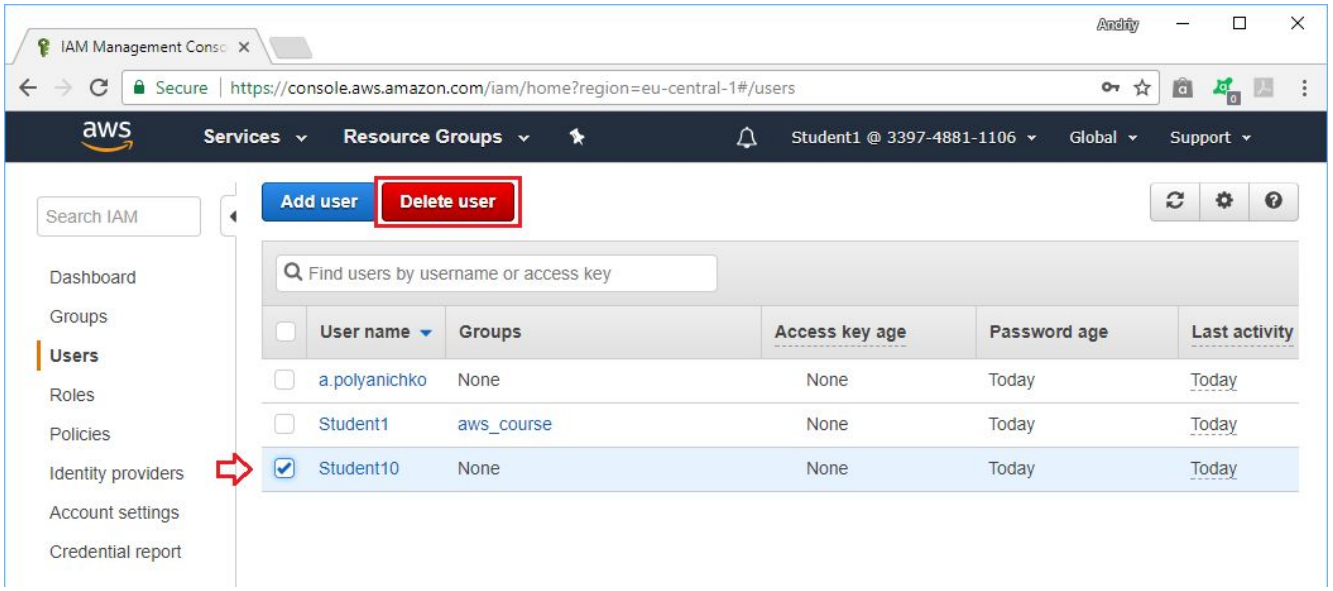
Now, if you will try to access EC2 services, you may consider that Student10 has complete access to all EC2 service functionalities (please check the availability of links which we had used in previous modules, hopefully everything is working).

If we are trying access S3 service, the message will appear:

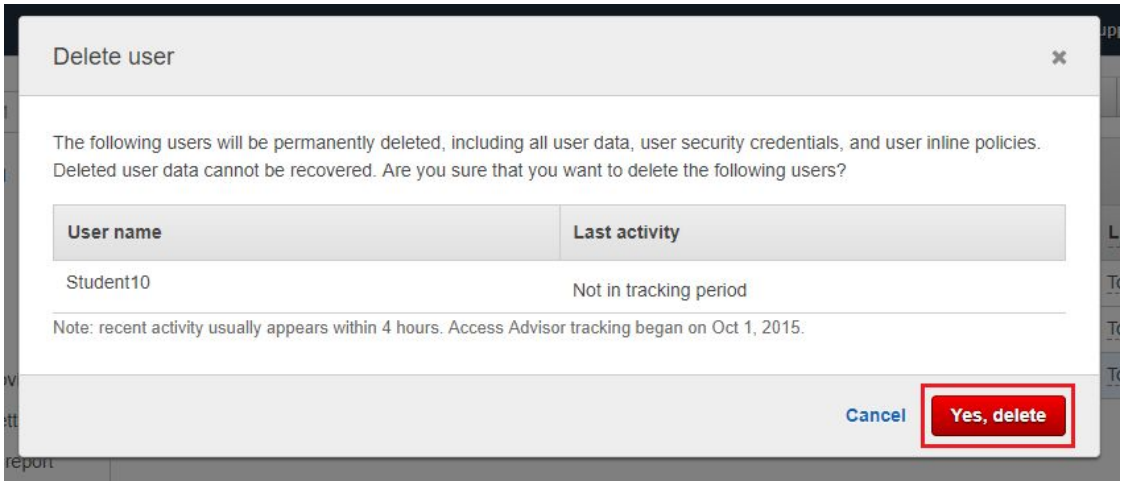


So Student 10 is restricted to access S3 due to corresponding privilege is not allowed explicitly in the attached managed policy.

Please sign out from Student10 user and then sign in again under your original user name. Open IAM Dashboard, click on “Users” item in left-side menu ribbon and delete temporary user which were named Student 10 in our examples:



Please confirm the deletion of user:

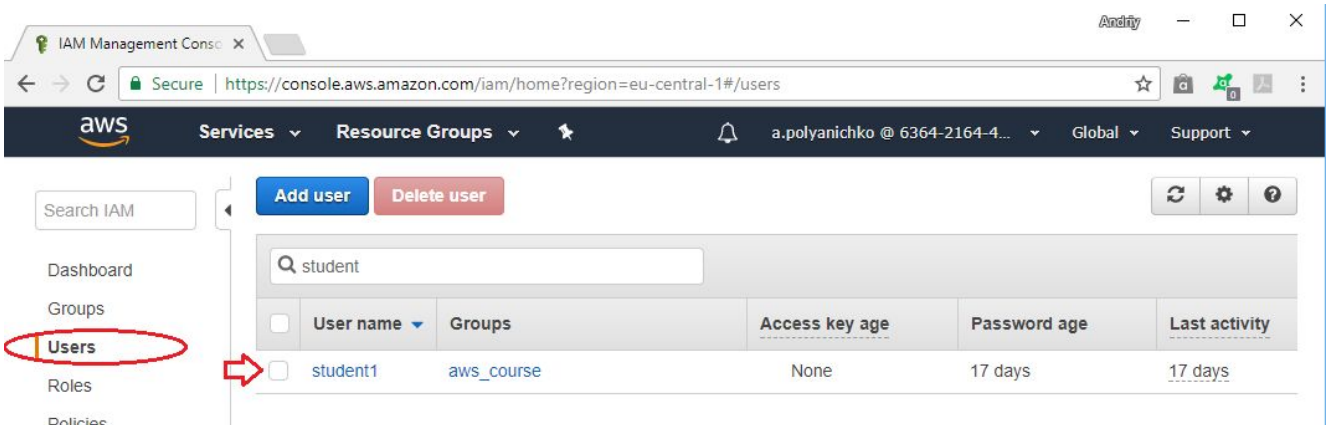


and finally check the list of available users in IAM.

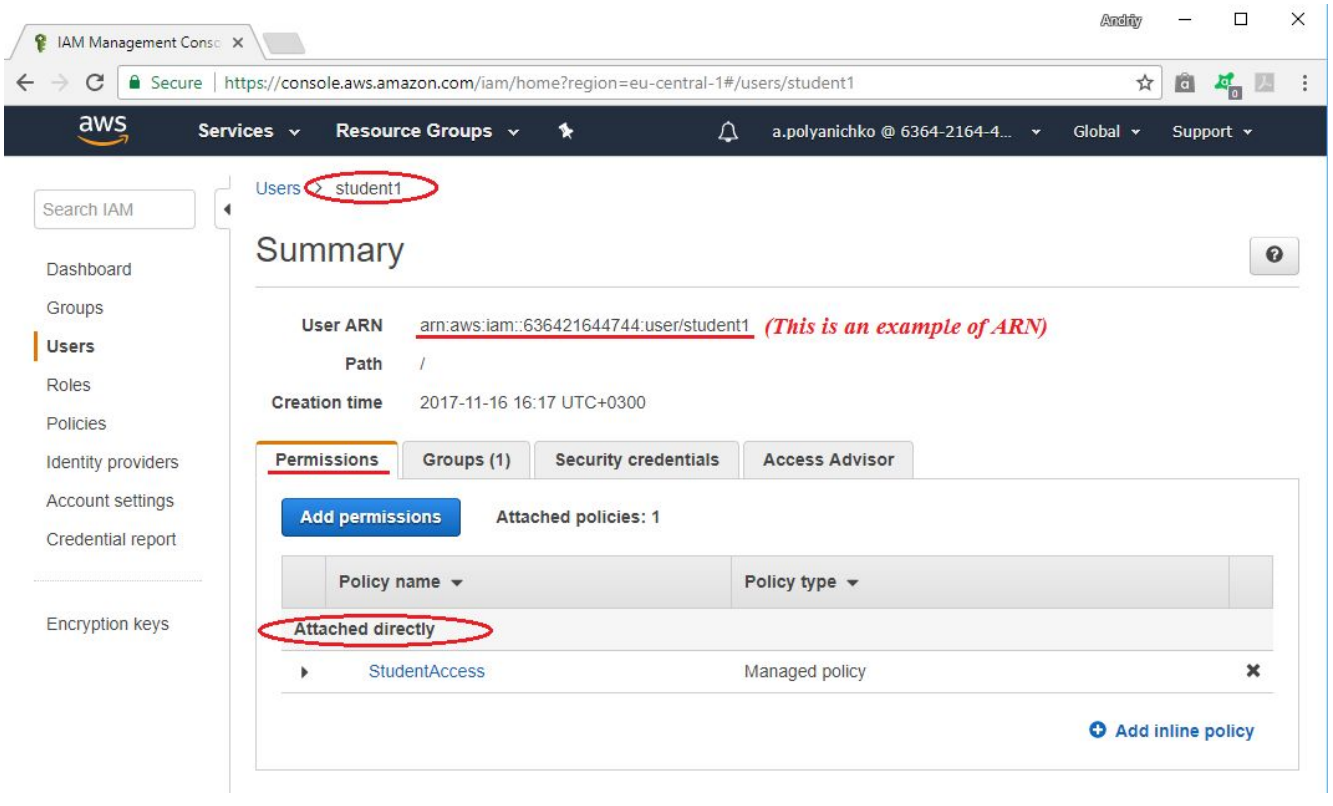
2. IAM and User Profile in details

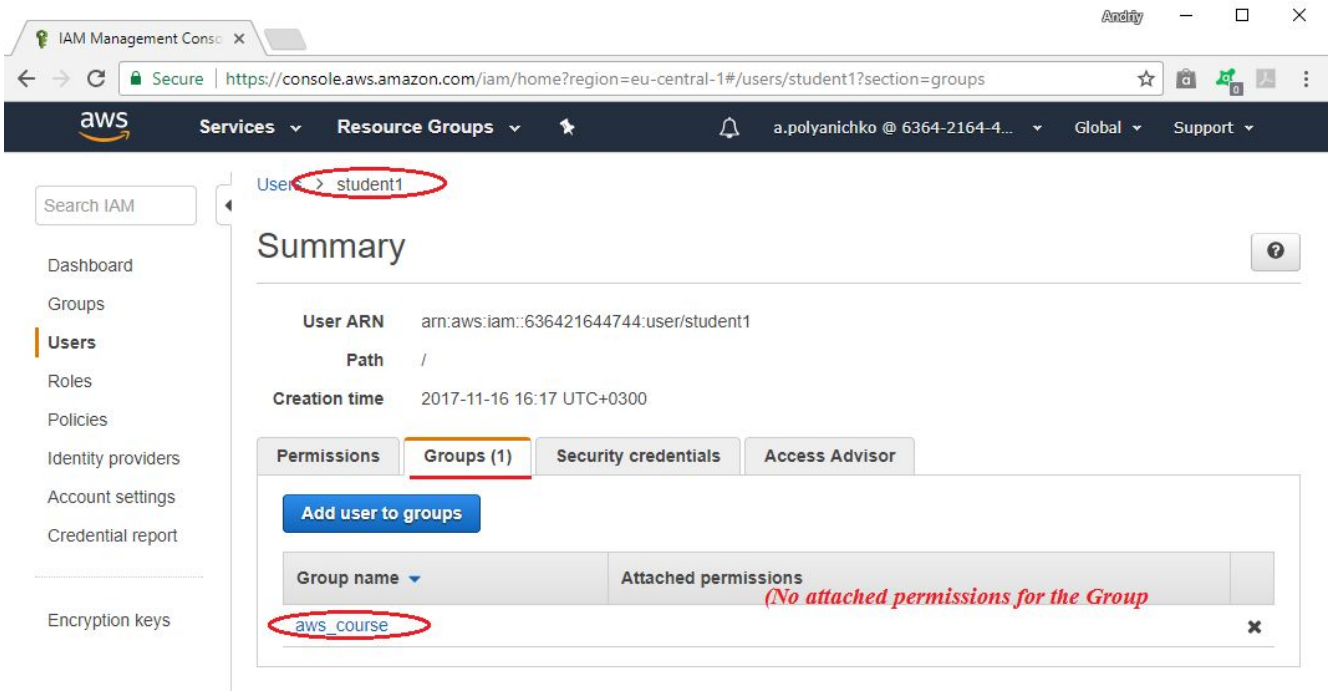
	Please be noted that you may be restricted more or less in some configuration operations because you are not root user in this training account and therefore you will be limited in some access rights and privileges.

Please open IAM Dashboard → "Users" page and find your username as it was shown in previous exercise:

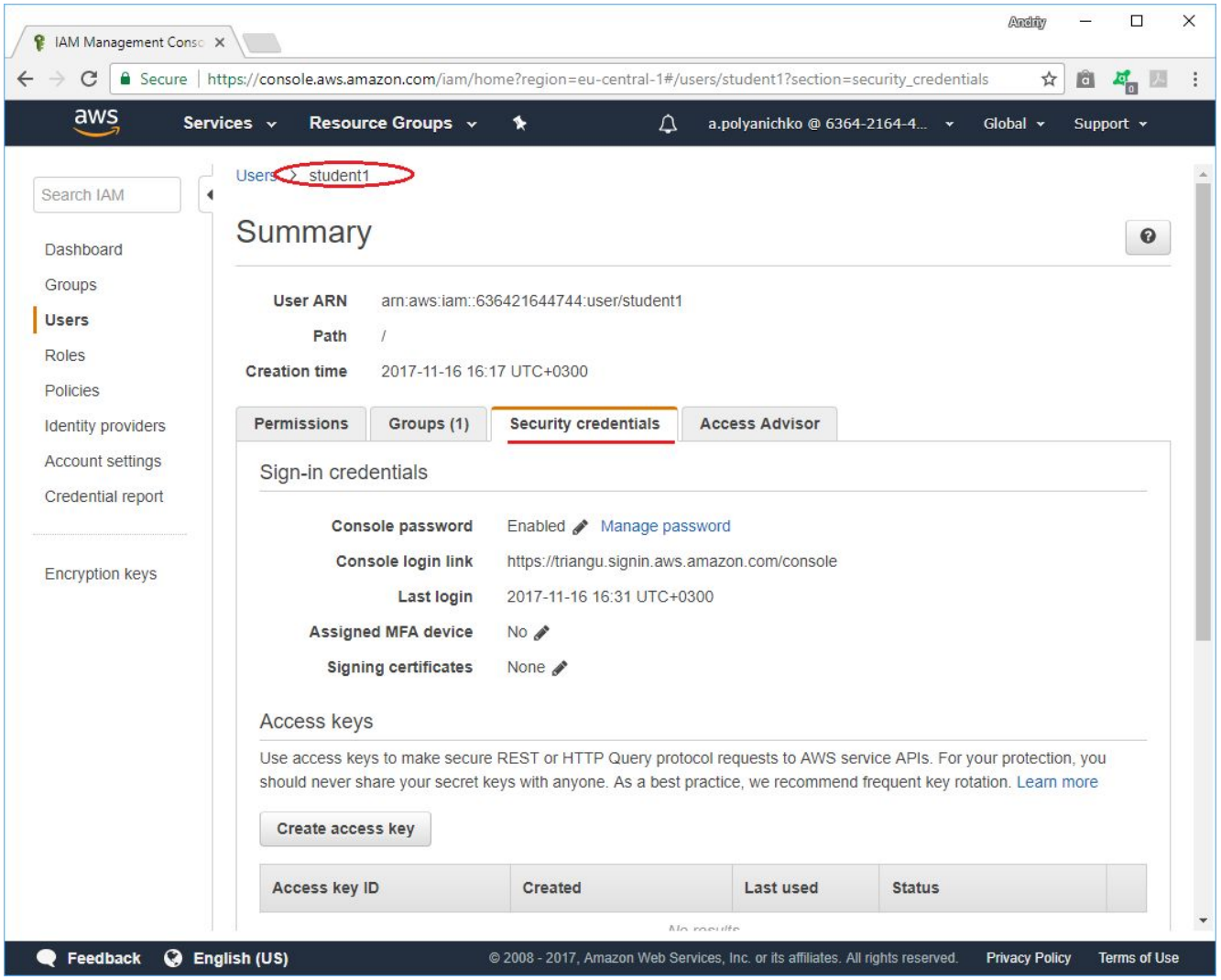


Click on your User name link and then explore details of your training account on "Permissions" and "Groups" tabs:



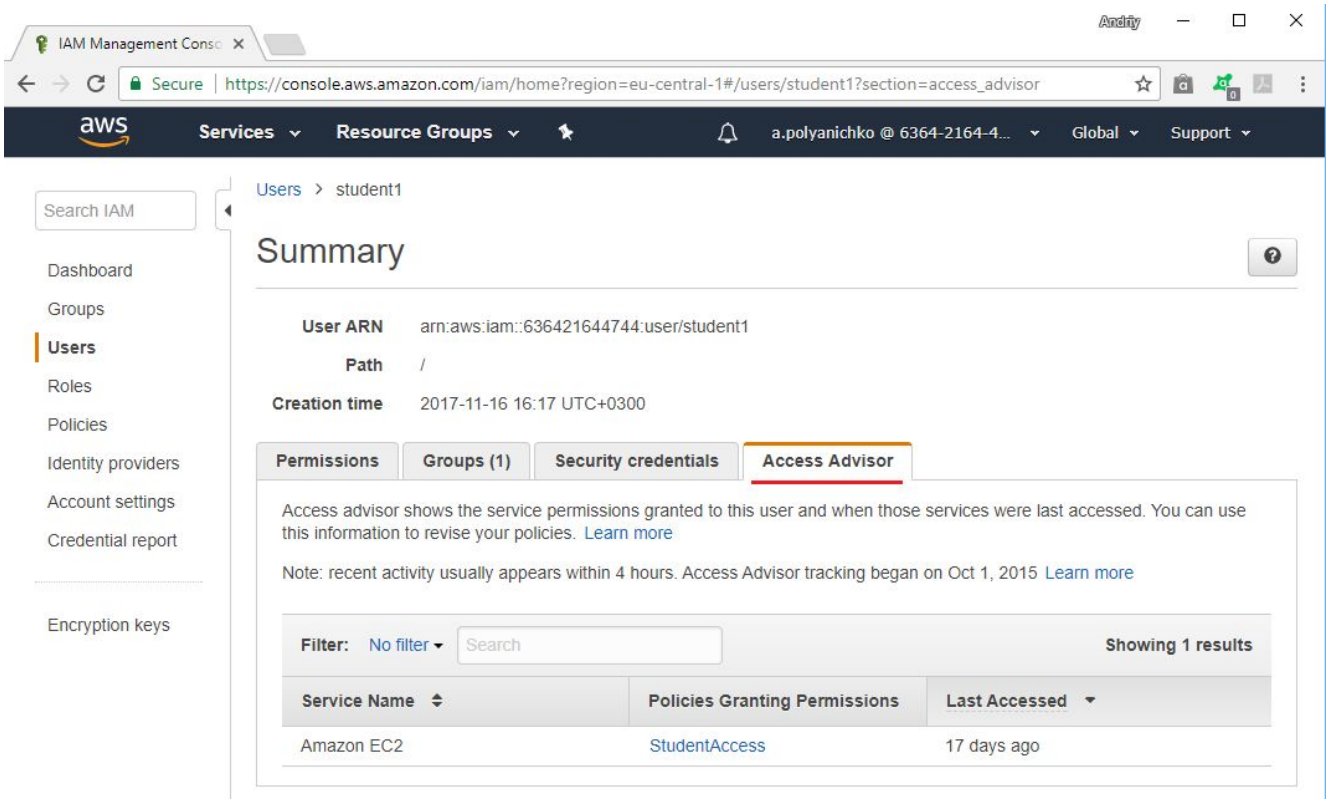


Switch on “Security Credentials” tab and check what we can do for Sign-in credentials, Access keys, SSH keys and HTTPS Git credentials for AWS Code Commit:

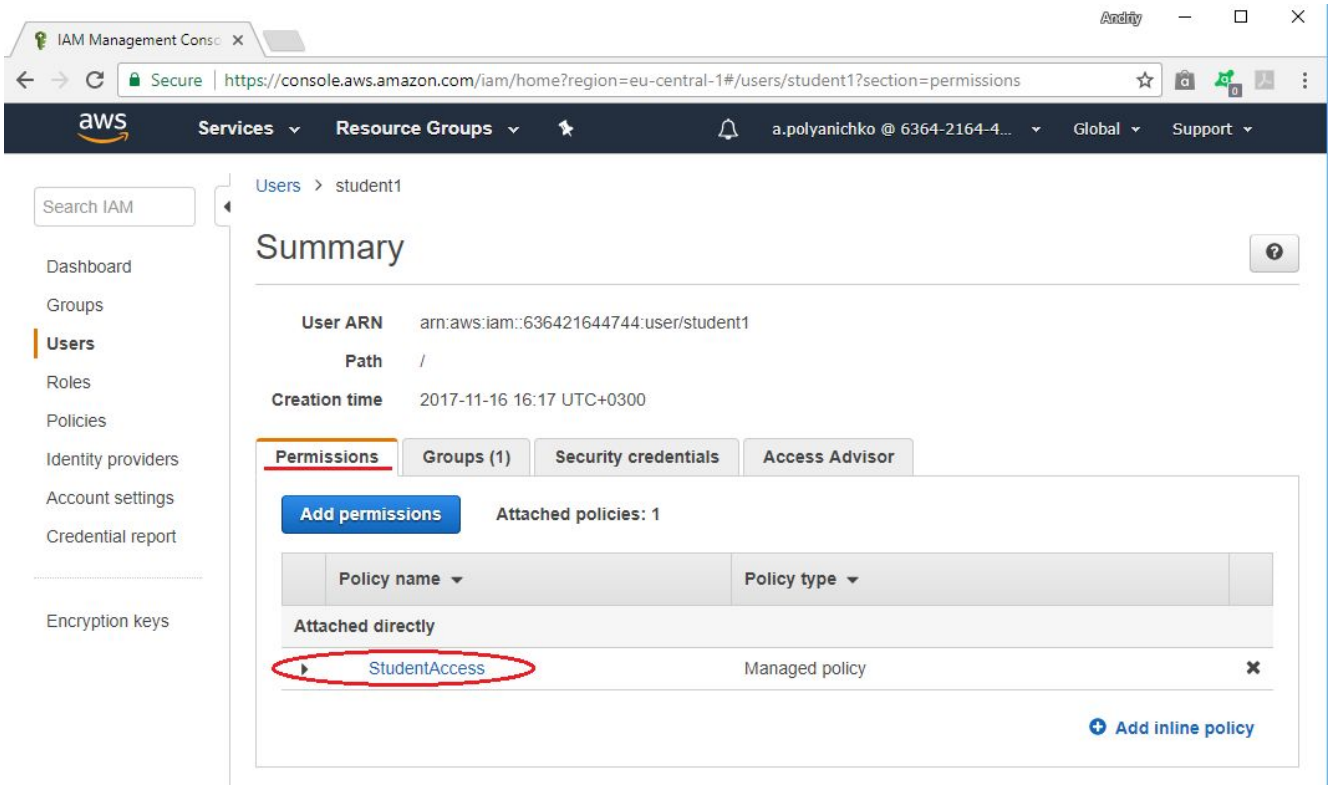


	We recommend you to avoid changing current settings of your training account. Surely all of your actions are safe in the training environment but occasionally your actions with account may block your access to system and the repair will take a time. On the other hand, practice is a criterion of truth, so you are free to choose.

Click on “Access Advisor” tab and revise the permissions granted to you and last access time for each of them:

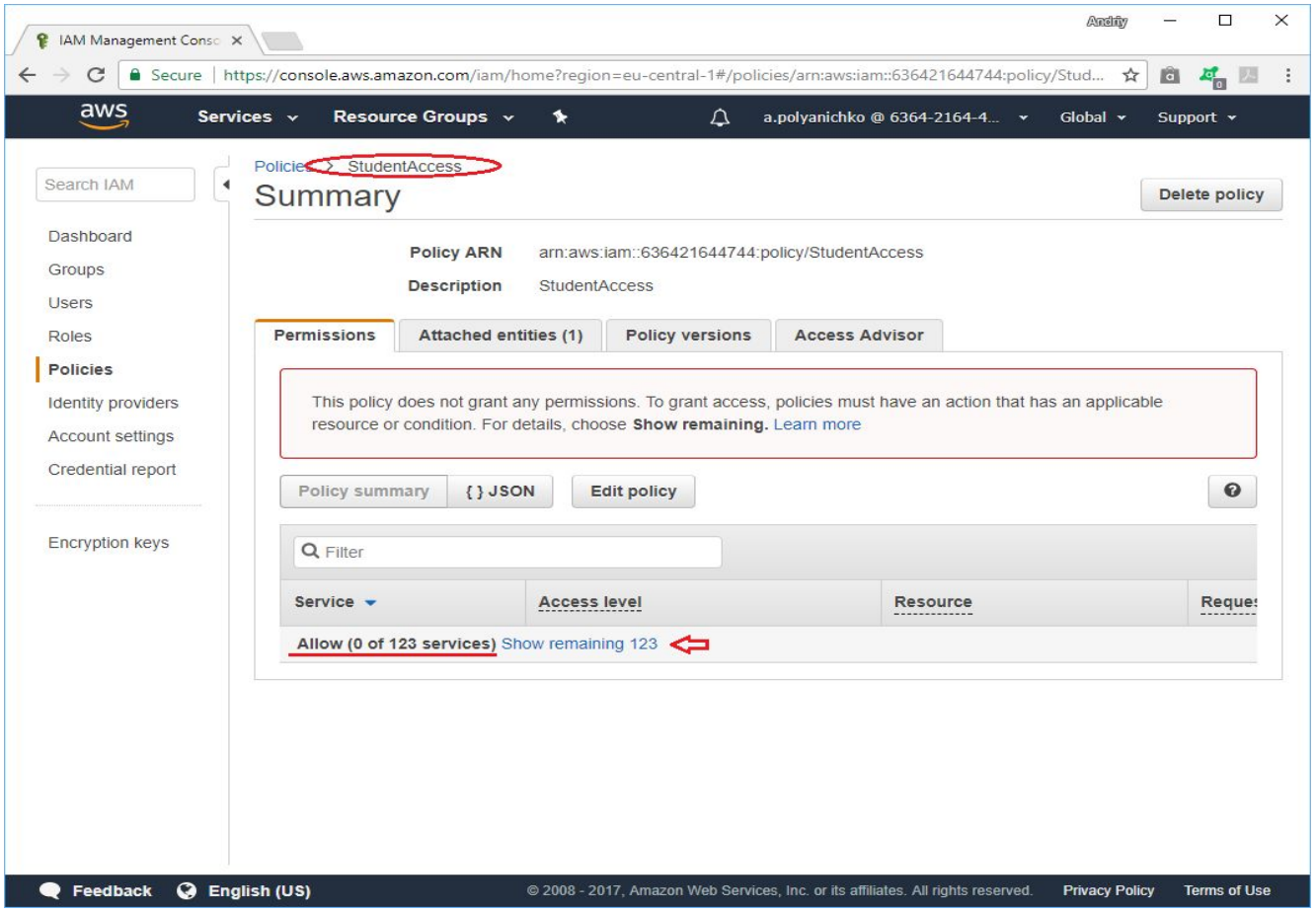


Let's revert back to "Permissions" tab and then click on the name of directly attached policy to check your permissions in training infrastructure:



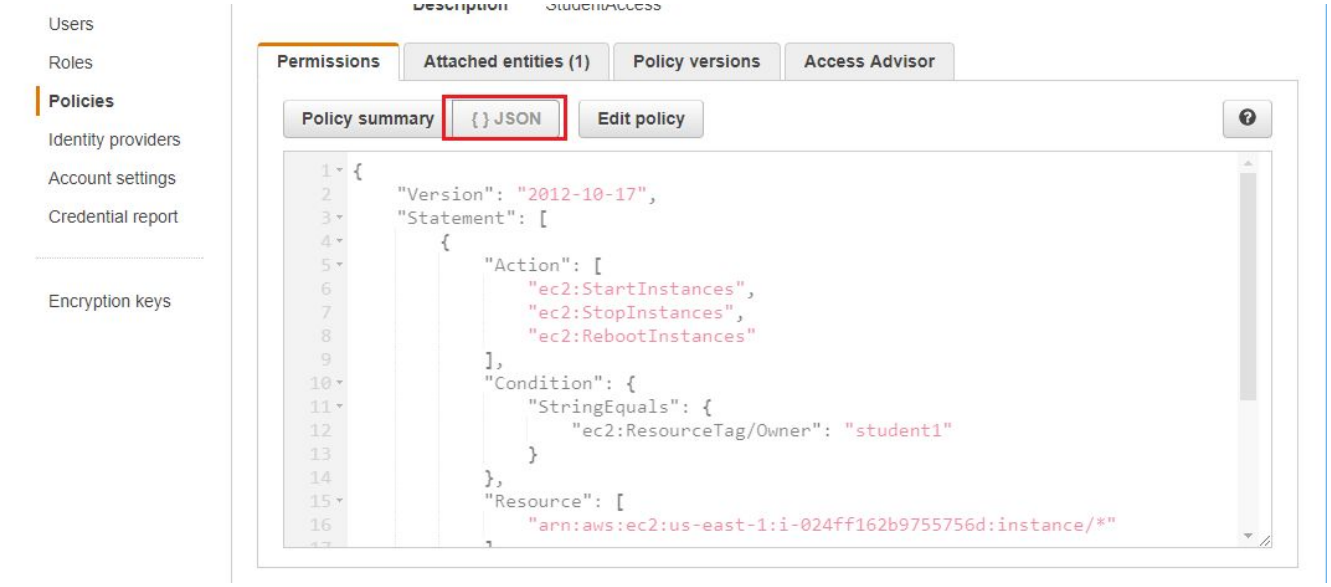
The next page will navigate you to "Policies" item on left-side menu ribbon and will show the

summary of your policy:

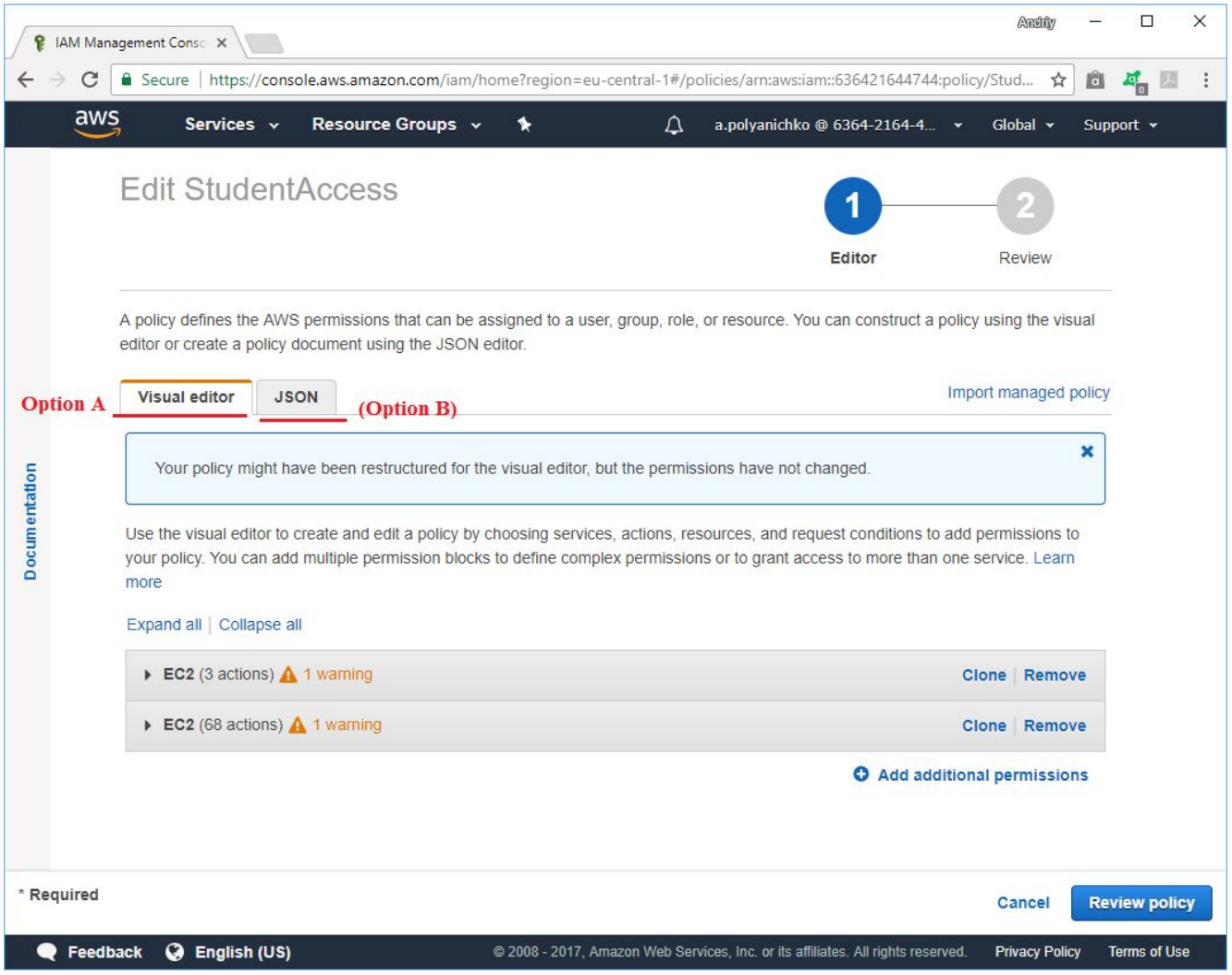


Here you may see directly all permissions with “Allow” value in Effect field (in the example above no Allow permissions are present for the given user, suppose you will be more fortunate) and also you may open full permission list by clicking on “Show remaining N” link.

If you want you may see the policy as JSON document by clicking on corresponding button:



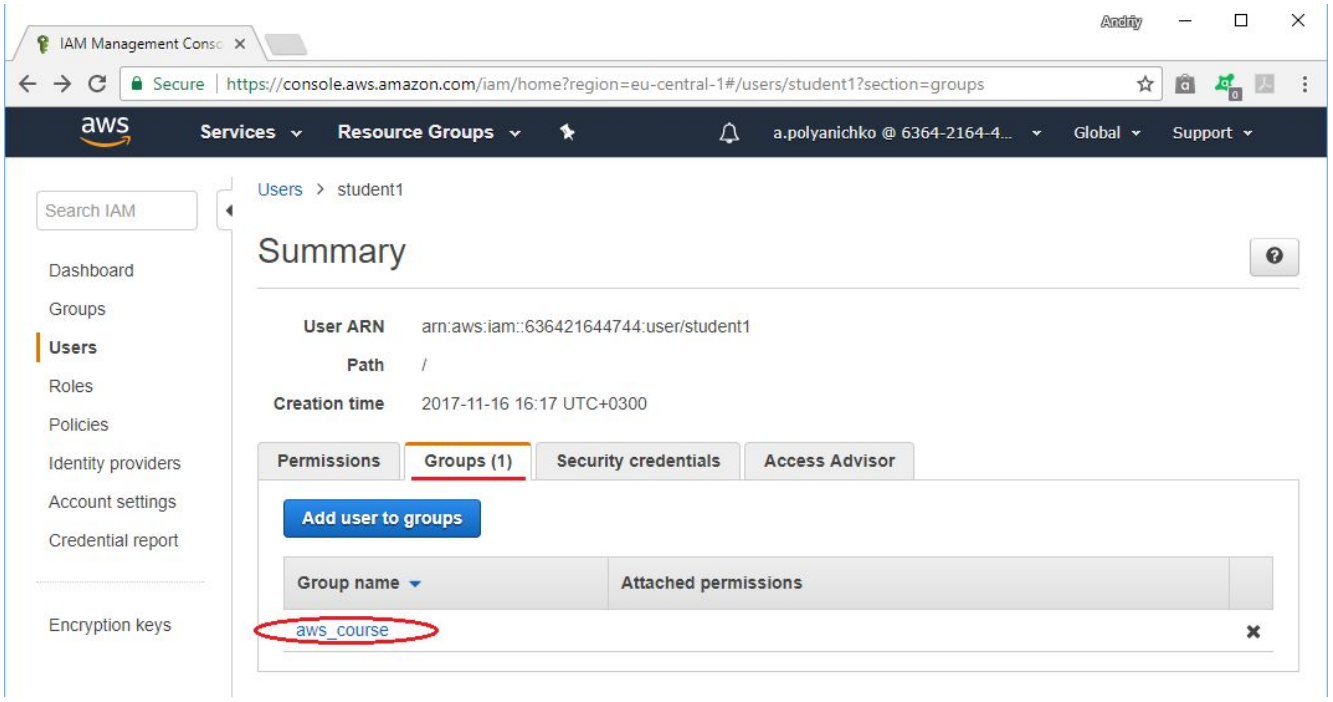
Click on “Edit policy” button and have a look how you can edit your policy if necessary:



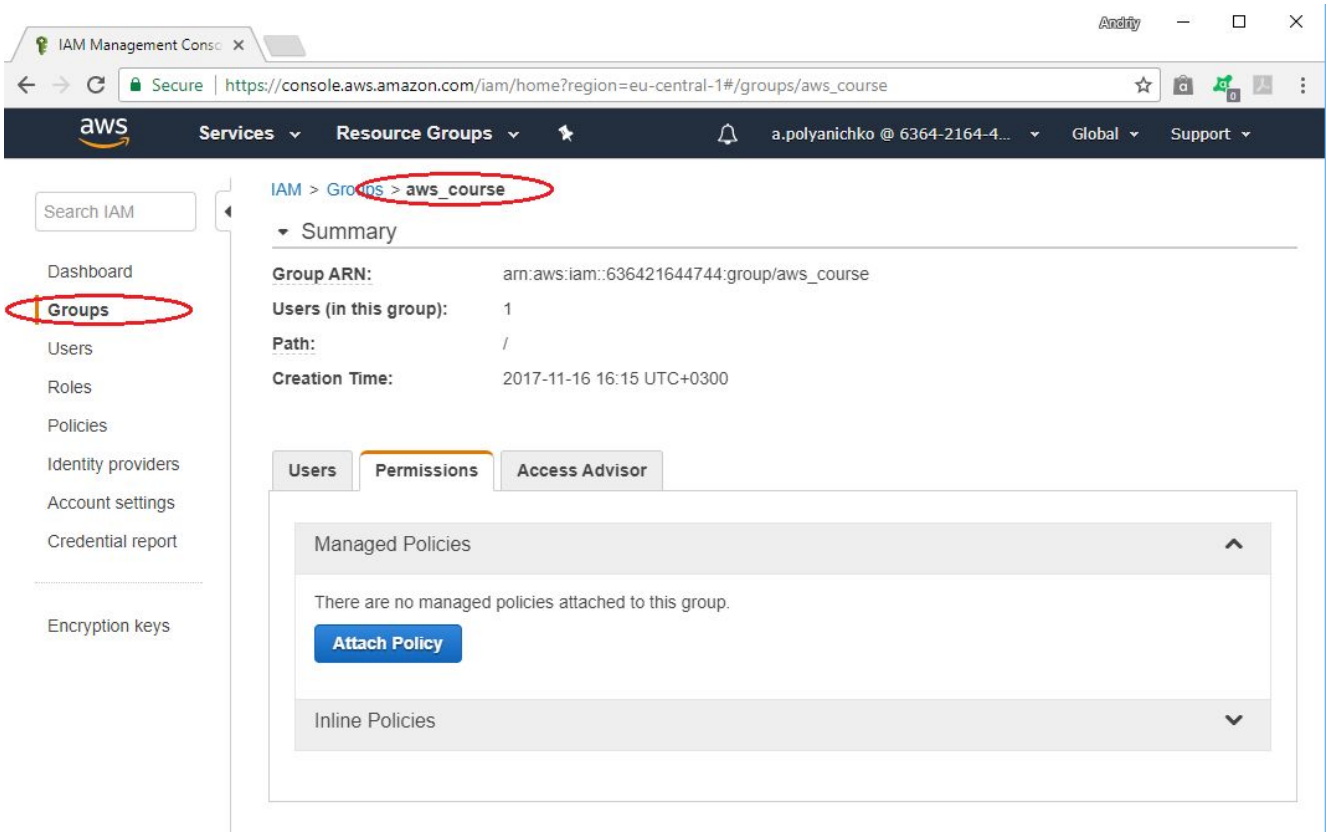
	On this page you may select Visual editor or JSON editor depending on what is preferable edit option for you. Finally the result will be the same for any edit options. Also we will have the point to review and check the policy before it will be saved.

	Perhaps, depending on what are your privileges in training account, you will not be able to save your changing in the policy.

Let's revert back to "Groups" tab on User summary and then click on the name of group where your user is assigned:

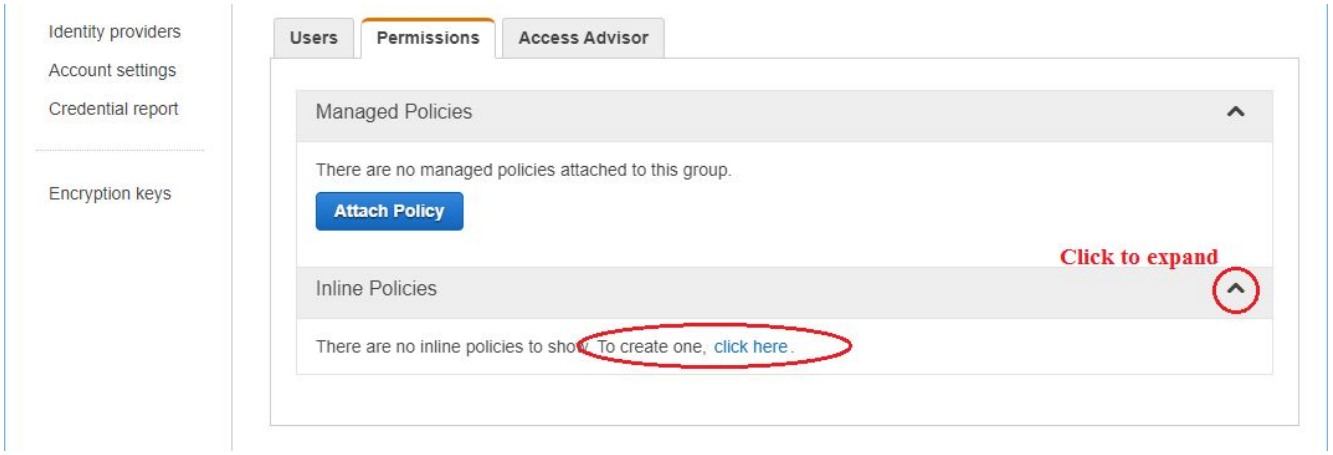


On the next page you will be navigated to “Groups” item on left-side menu ribbon and “permission” tab for the group will be opened:

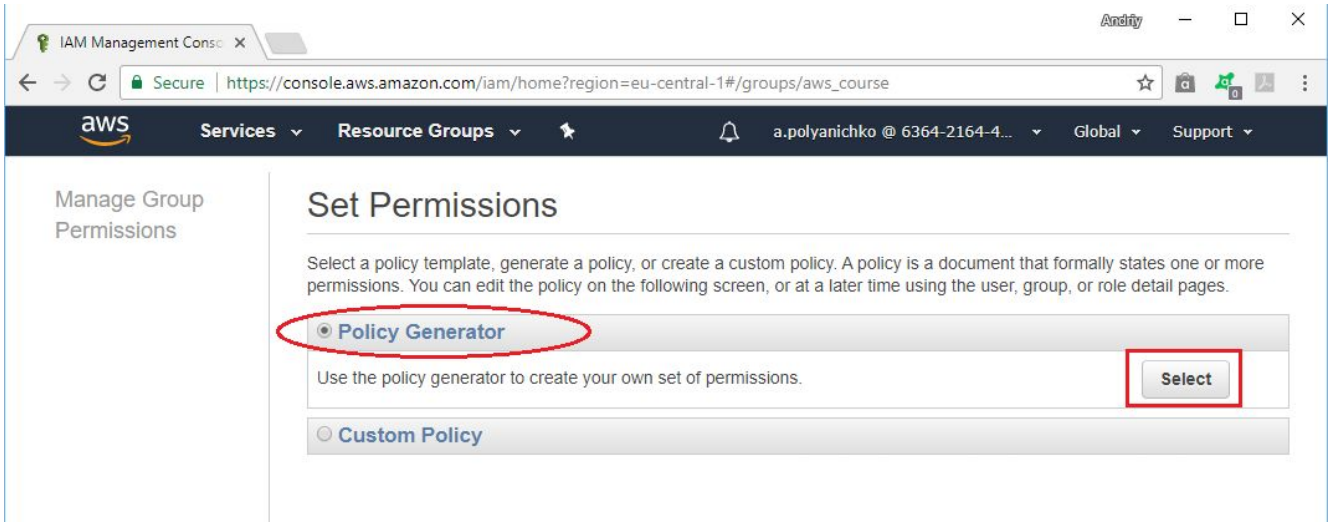


Starting from here let’s try to create Inline Policy for the group.

First of all we need to expand “Inline Policies” group by clicking on appropriate arrow to the right and then find and click on appeared link to create new inline policy:

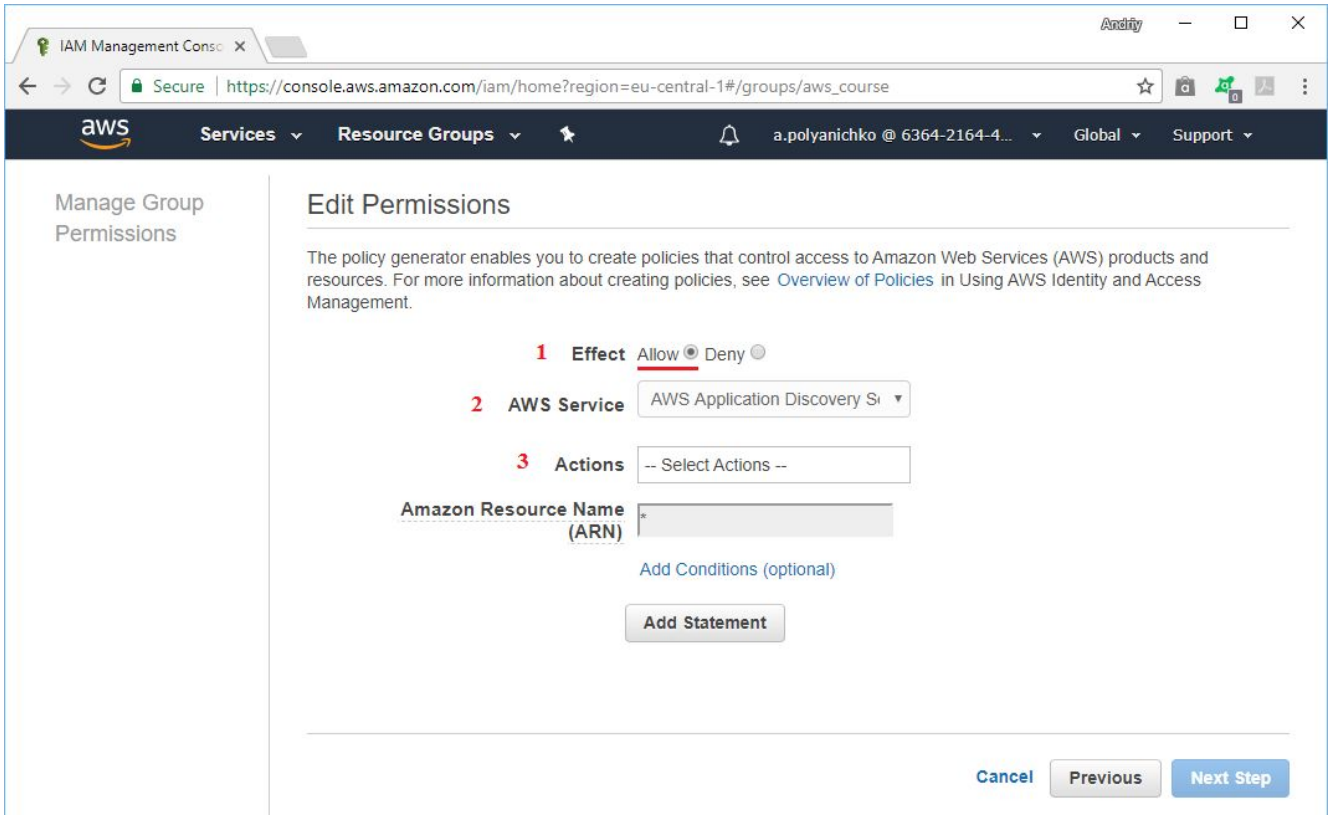


Please select Policy Generator option to set permissions in our exercise:

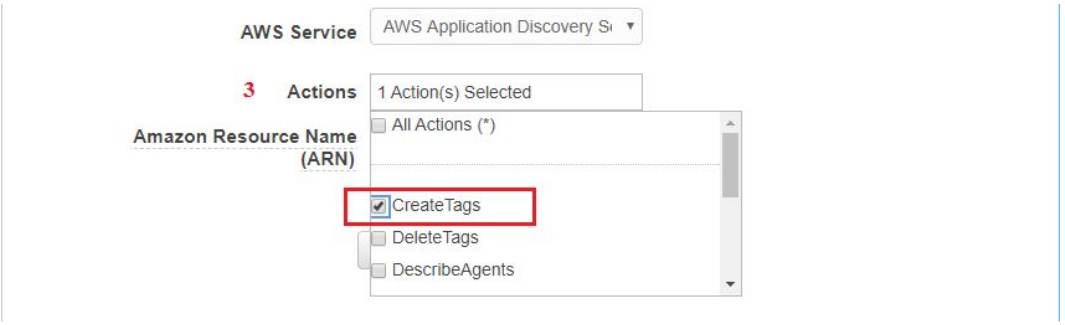


	The second option, Custom Policy, will point you to JSON document editor and you will be prompted to start policy creation from zero.

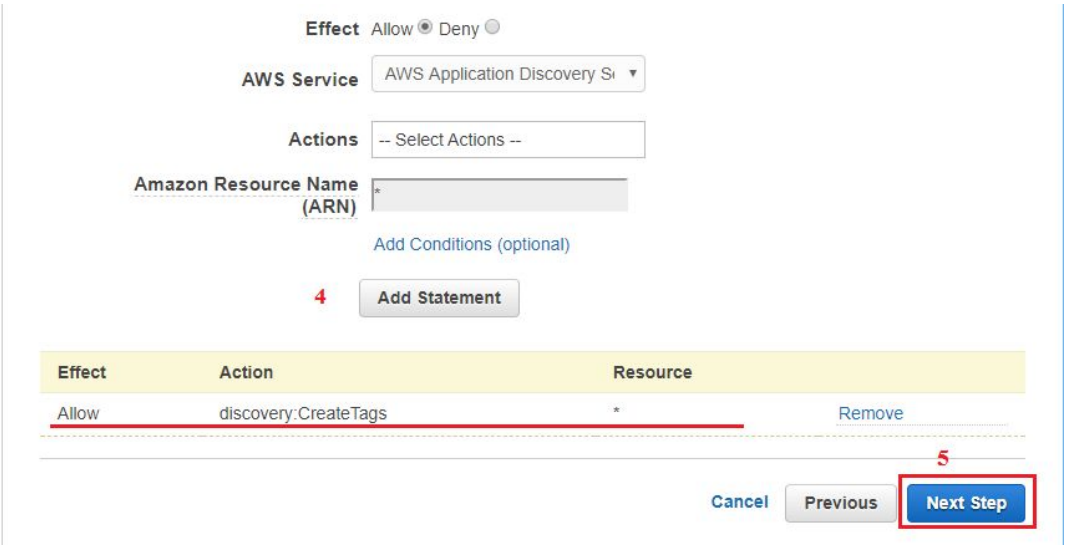
On the next page you will see Edit Permission screen; let’s describe the following process step by step:



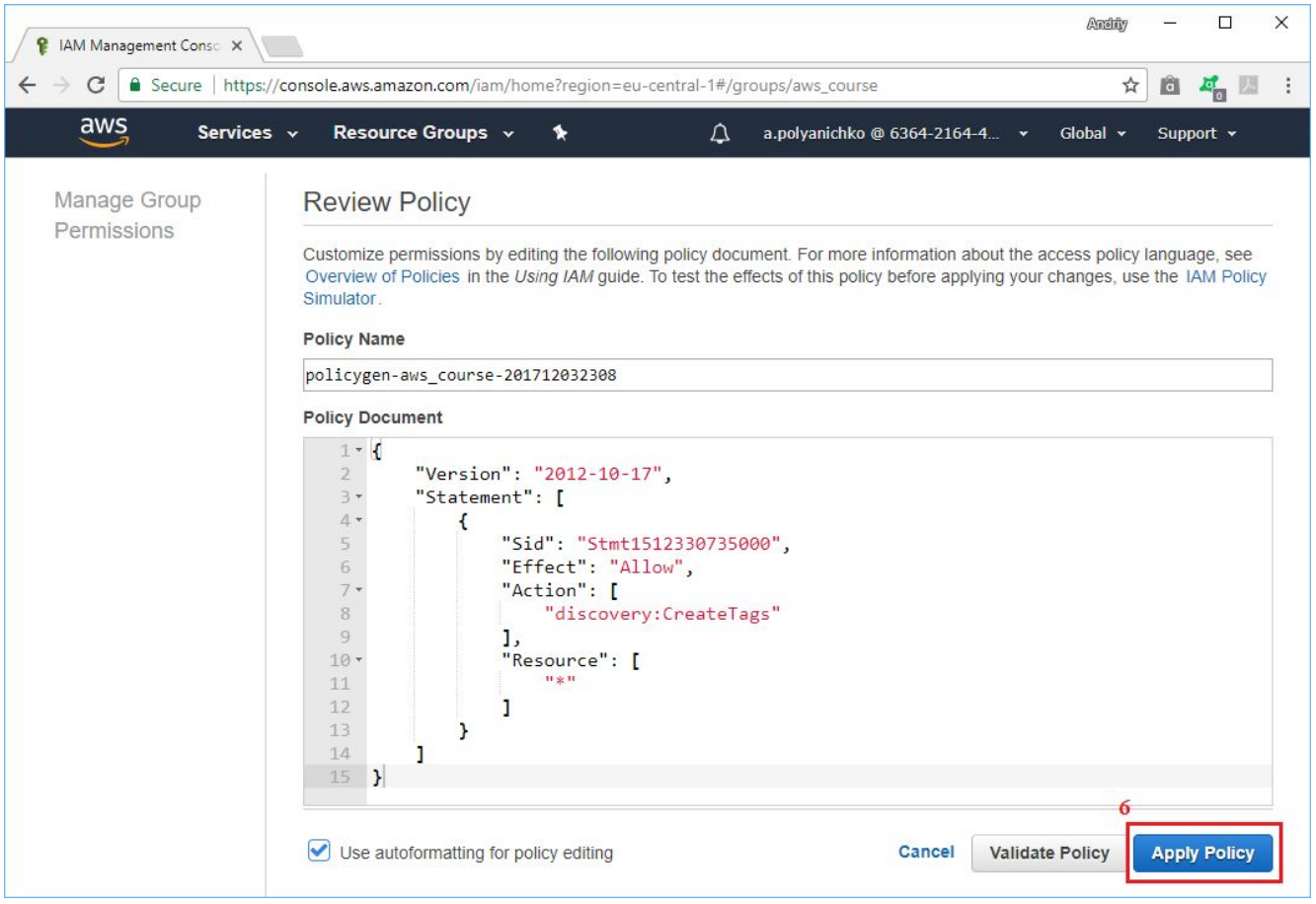
1) Select **Effect** – "Allow";
2) Select **AWS Service** – leave the default value;
3) Select **Actions**:



4) Click on "Add Statement" button and revise the statement which you are planning to add:



5) Click on “Next Step button”:



6) Click on “Apply Policy” to save editing.

Now you may see your policy assigned to the group as inline one and also you may perform some actions with the policy (show, edit, remove or stimulate):