**AWS IAM**

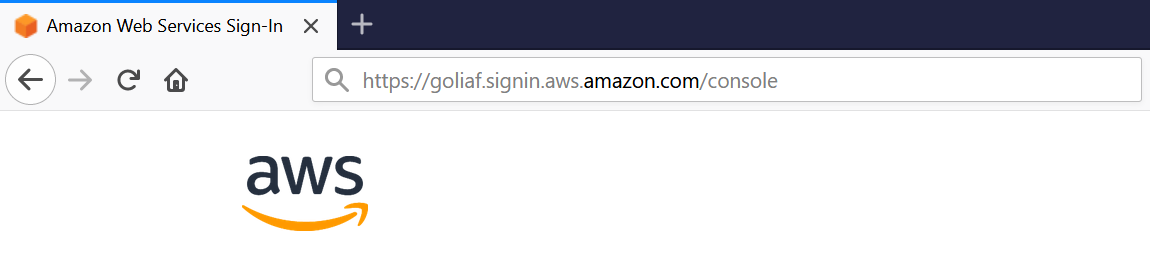
During the hands-on exercises you will get acquainted with the main points related to the management and configuration of Identity and Access Management (IAM) functionality.

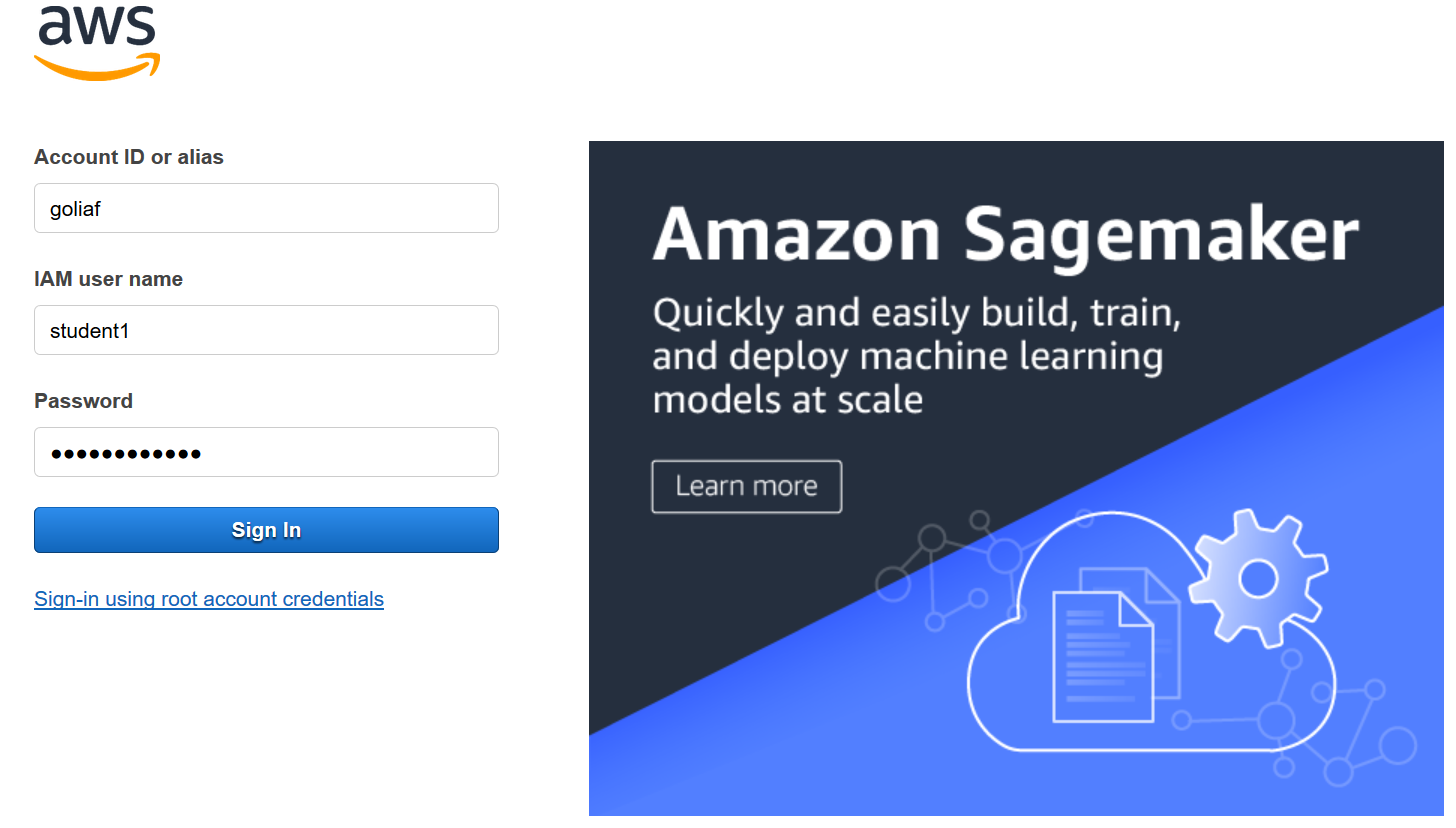
1. **Signing-in AWS Management Console**

We are using URL

<https://goliaf.signin.aws.amazon.com/console>

to sign-in AWS Management Console for training purpose.

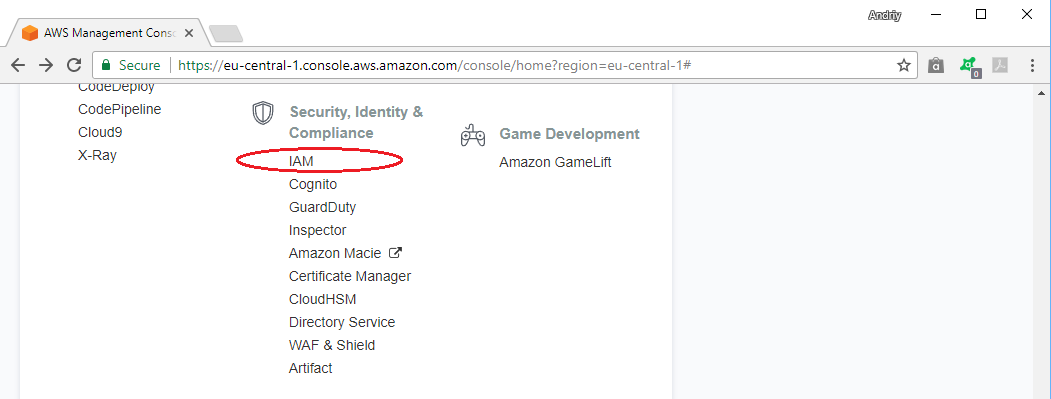


After that we will be redirected to AWS Login page: 

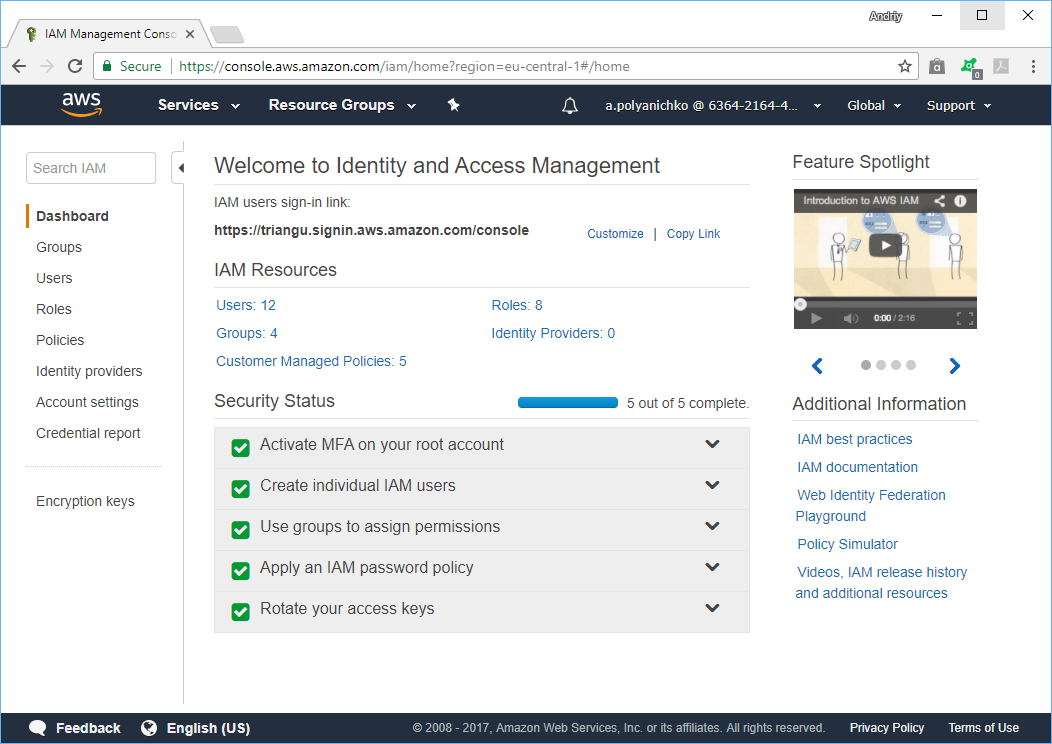
Enter IAM User name and Password here and then click “Sign In” button. AWS Console Home page will be opened:

1. **IAM Operation Getting Started**

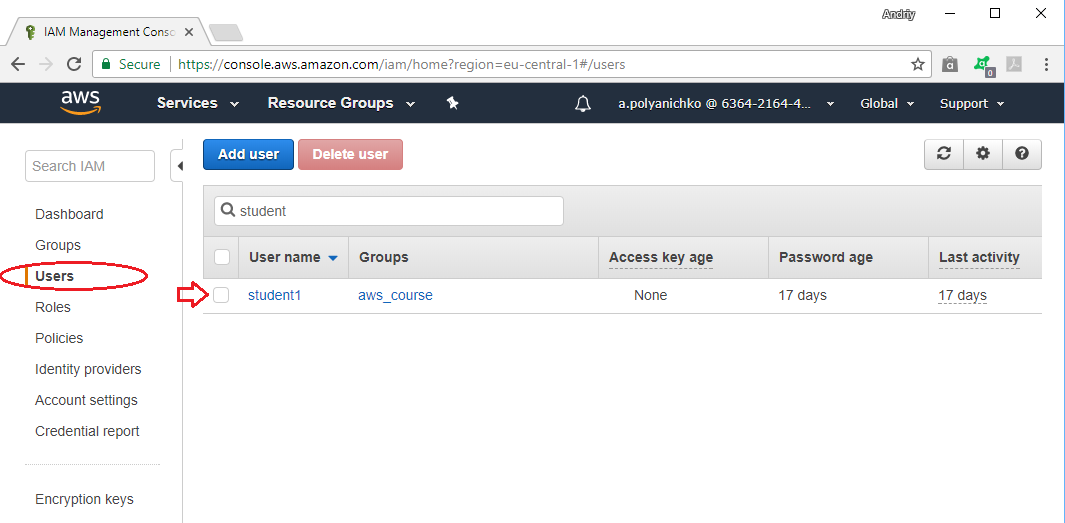
Open AWS Management Console as usual and then find and click on IAM link:



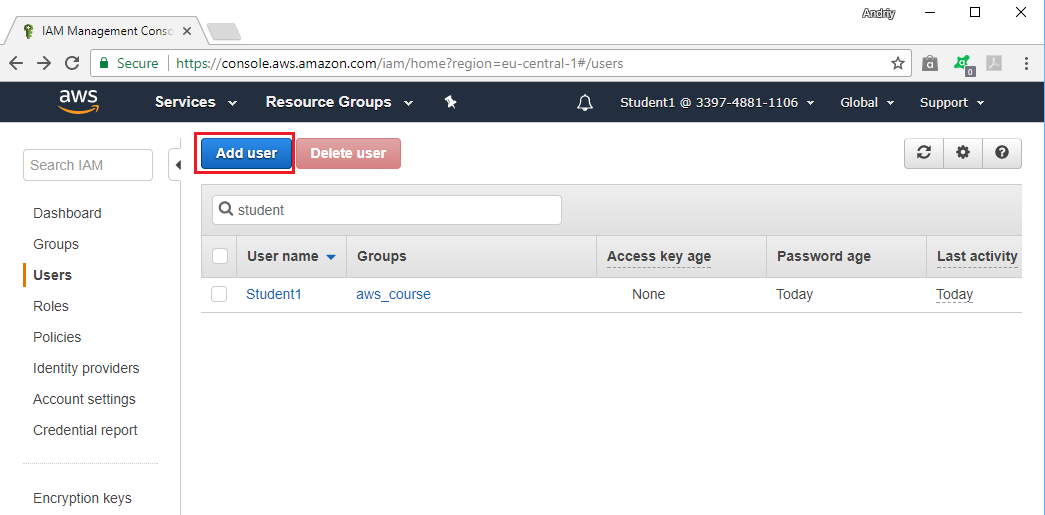
IAM Dashboard main page will be opened:



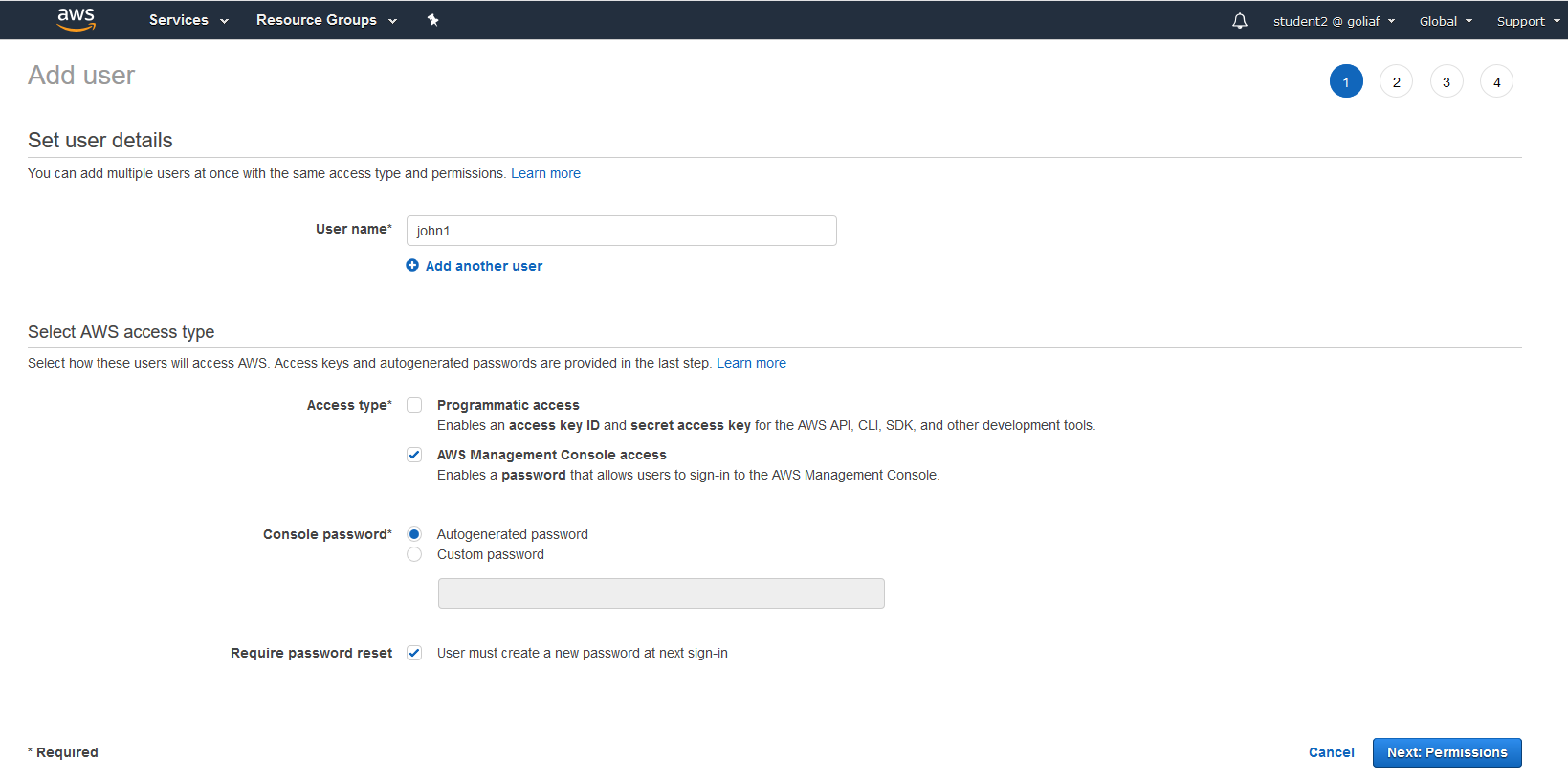
Click on “Users” link at left-side menu ribbon and find yourself in the list:



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



On the next page specify user details as shown below:

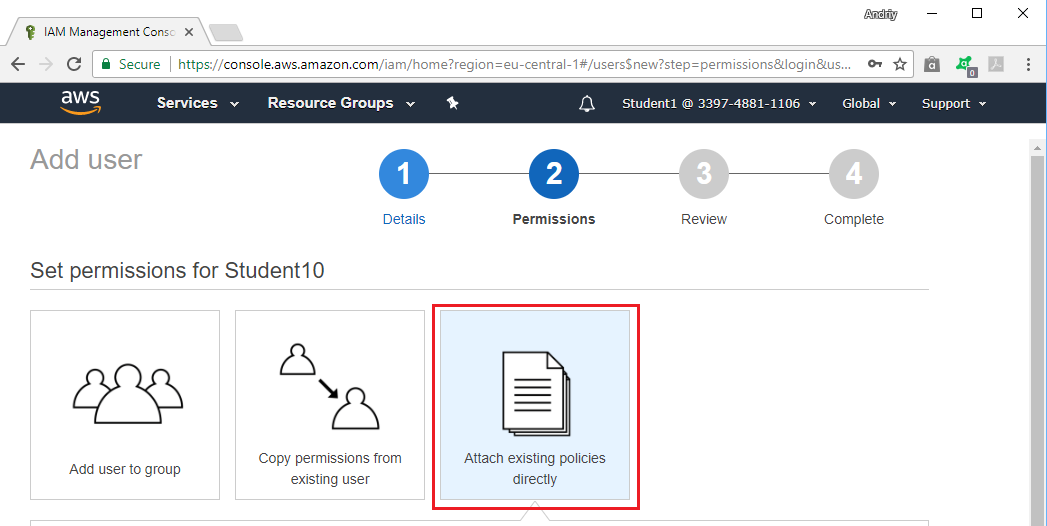


**User Name:** starting with **john1** up to **john99**

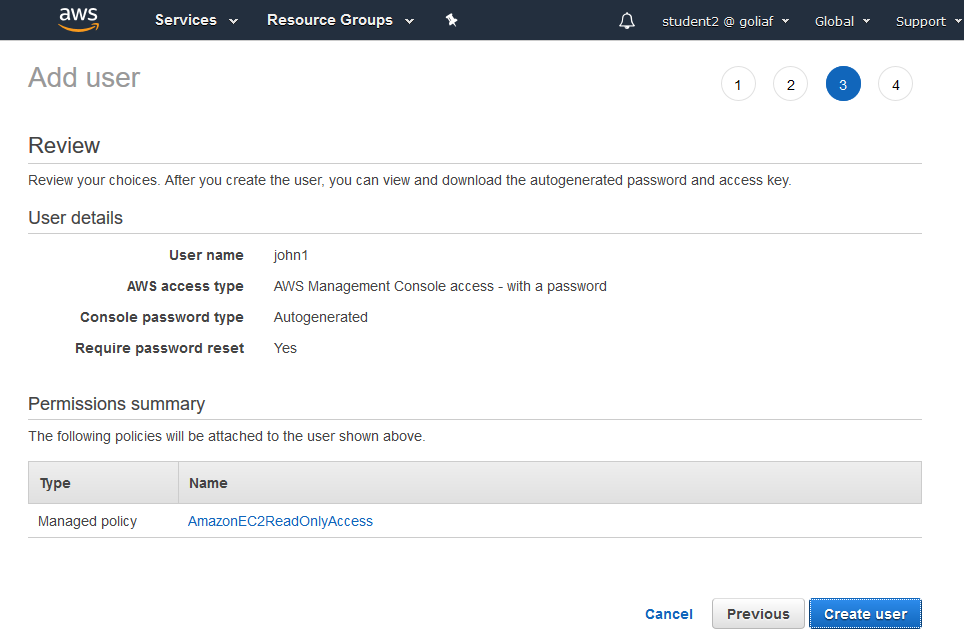
Check AWS Management Console Access

Choose Autogenerated password

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

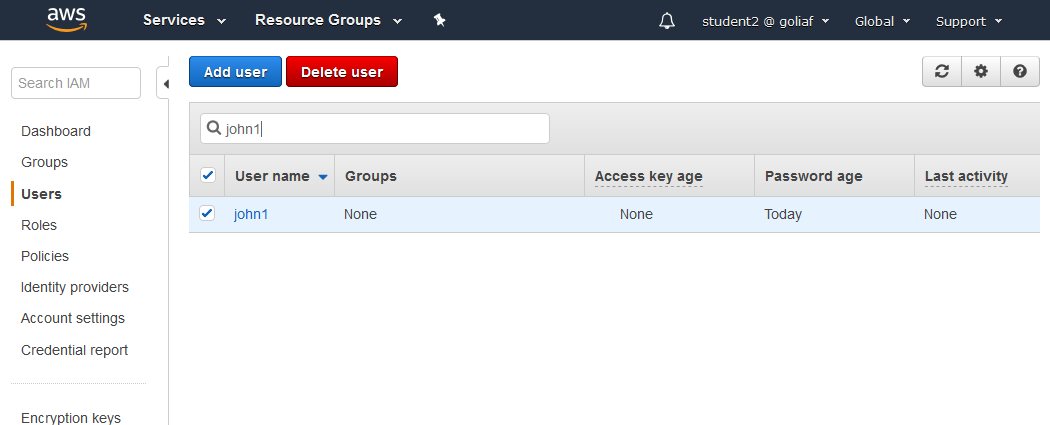


and then find and select “AmazonEC2ReadOnlyAccess” policy name using filter field by type of policy as shown below, then click on “Next: Review: button:

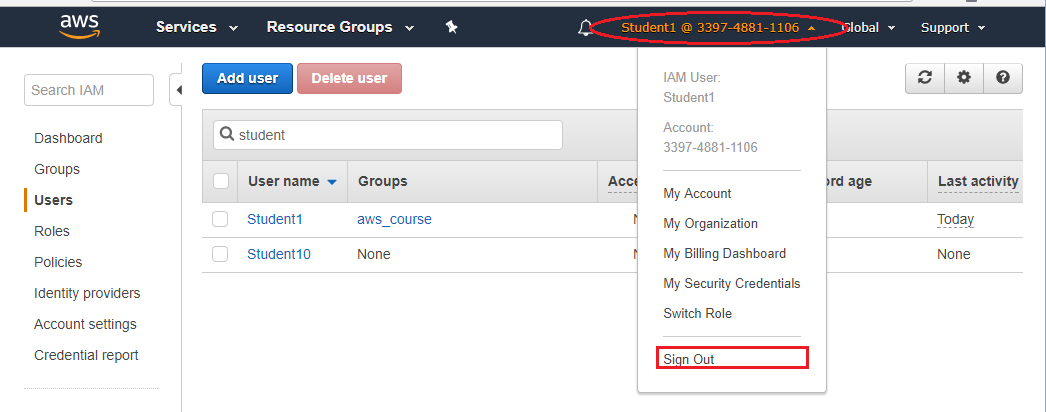


Click on “Create User” button.

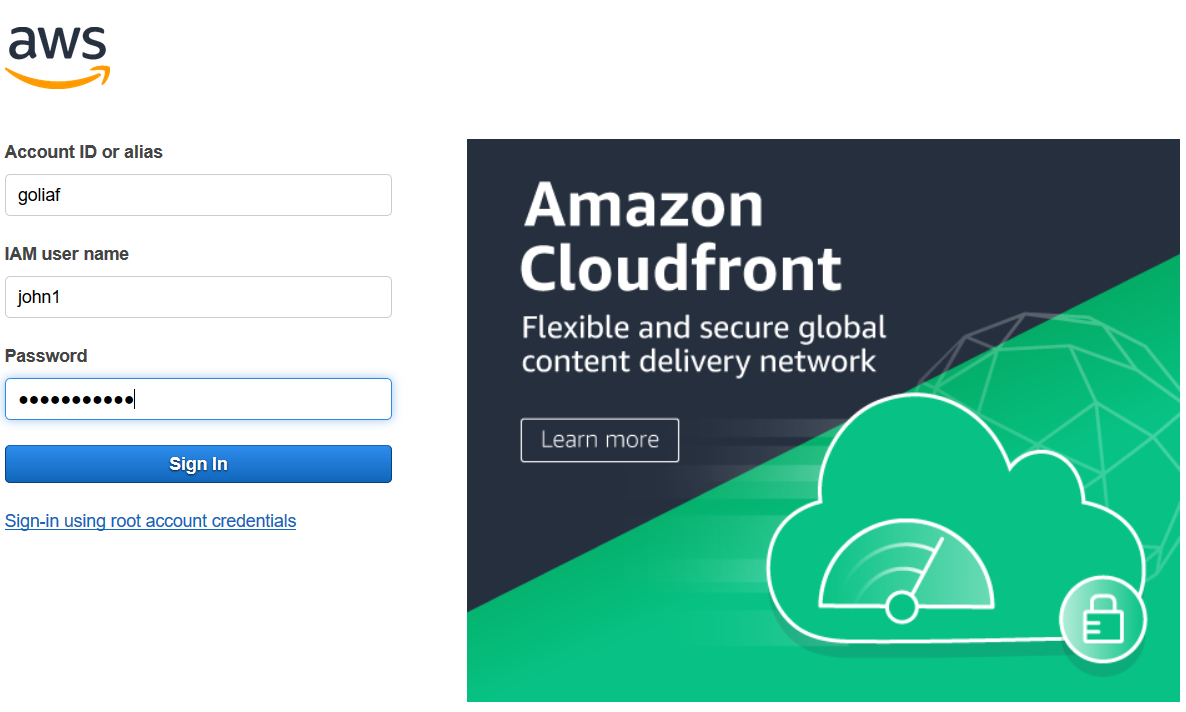
Confirm the creation of new user and finally find it in the list of available users:



1. Sign-out from your current account using top menu:



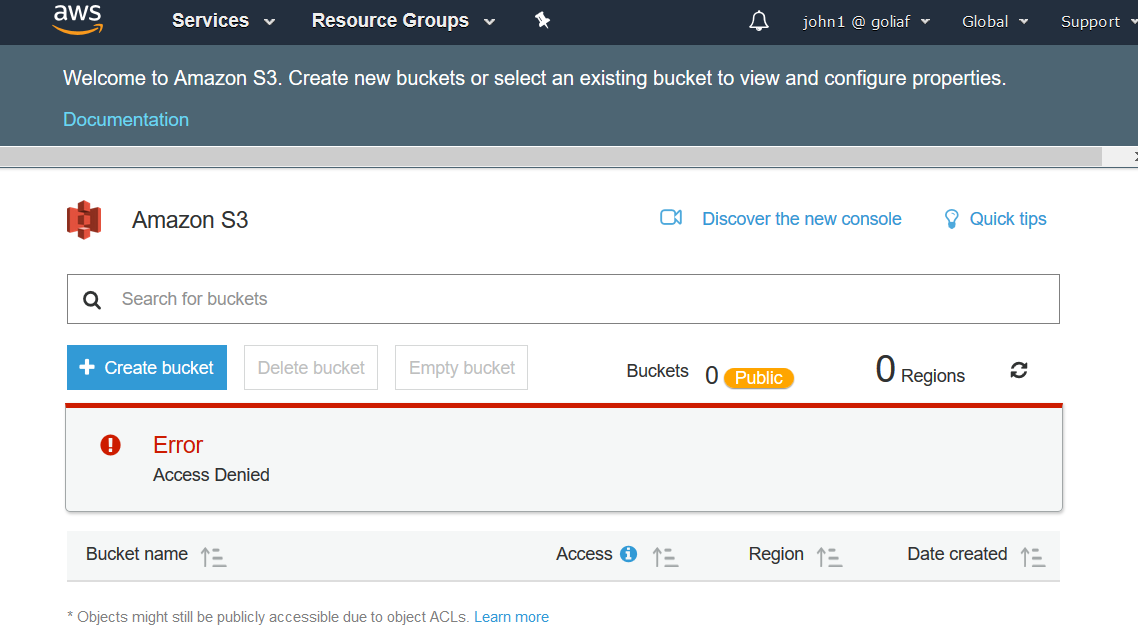
and log in again using Username and password of user you’ve created before:



You will enter AWS Management Console as usual.

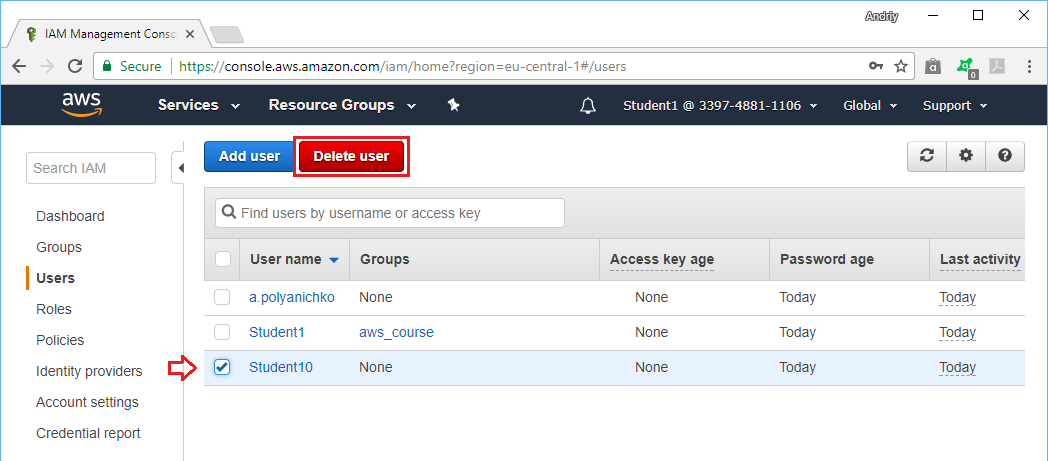
Now, if you will try to access EC2 services, you may consider that **john1** has complete access to all EC2 service functionalities (please check the availability of links which we had used in previous modules, hopefully everything is working).

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

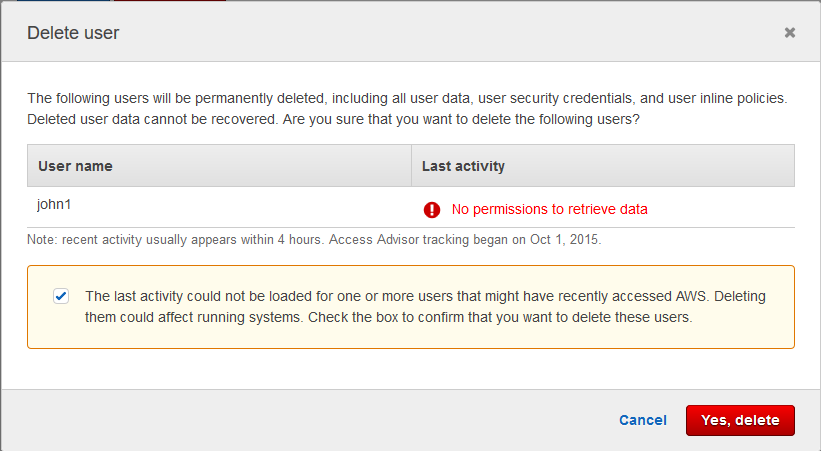


So **john1** is restricted to access S3 due to corresponding privilege is not allowed explicitly in the attached managed policy.

Please sign out from **john1** 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.

