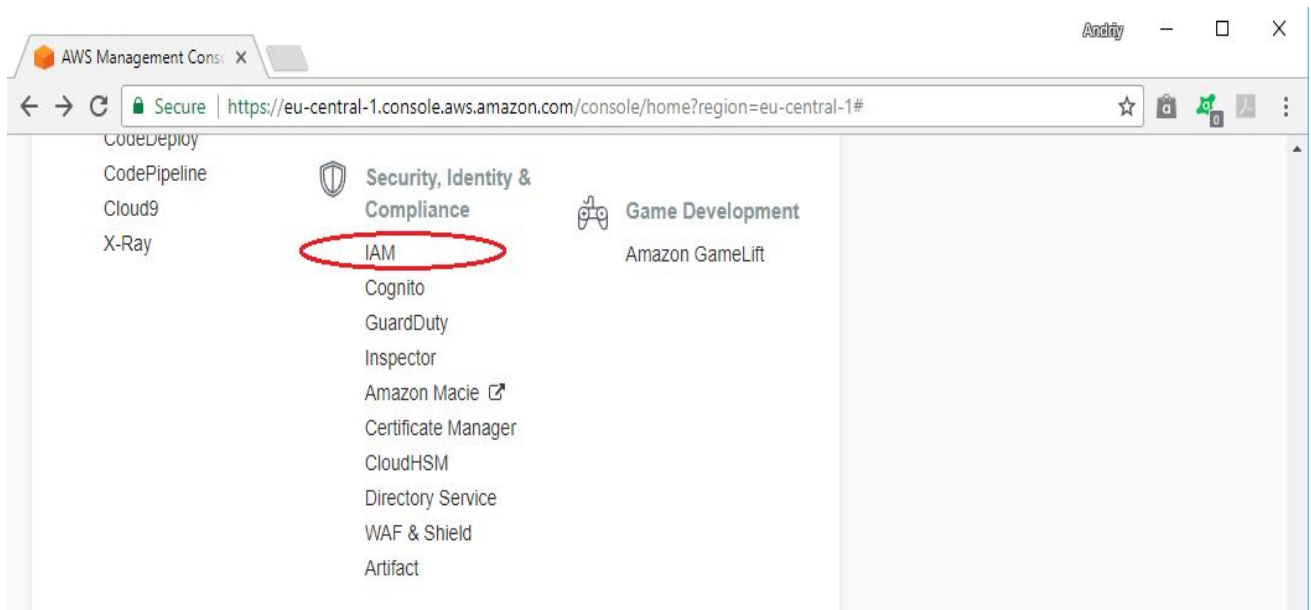


MODULE 5 – LAB EXERCISES

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:

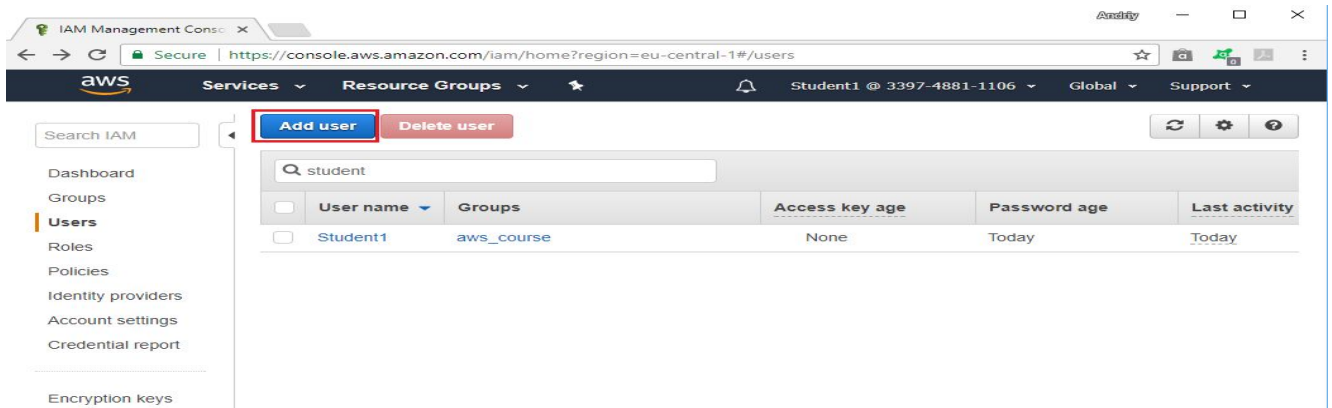
The screenshot shows the AWS IAM Management Console home page. The left sidebar contains a search bar and a menu with links to Dashboard, Groups, Users, Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area is titled "Welcome to Identity and Access Management" and displays IAM resources: Users: 12, Roles: 8, Groups: 4, Identity Providers: 0, and Customer Managed Policies: 5. A "Security Status" section shows five items with green checkmarks: Activate MFA on your root account, Create individual IAM users, Use groups to assign permissions, Apply an IAM password policy, and Rotate your access keys. A "Feature Spotlight" video titled "Introduction to AWS IAM" is shown on the right, along with "Additional Information" links for IAM best practices, IAM documentation, Web Identity Federation Playground, Policy Simulator, and Videos, IAM release history and additional resources.

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

The screenshot shows the AWS IAM Management Console Users page. The left sidebar is the same as the previous screenshot, but the "Users" link is highlighted with a red circle and a red arrow points to it. The main content area has a search bar with "student" entered. Below the search bar is a table with columns: User name, Groups, Access key age, Password age, and Last activity. The table contains one row with the user "student1" in the "User name" column, "aws_course" in the "Groups" column, "None" in the "Access key age" column, "17 days" in the "Password age" column, and "17 days" in the "Last activity" column.

	User name	Groups	Access key age	Password age	Last activity
<input type="checkbox"/>	student1	aws_course	None	17 days	17 days

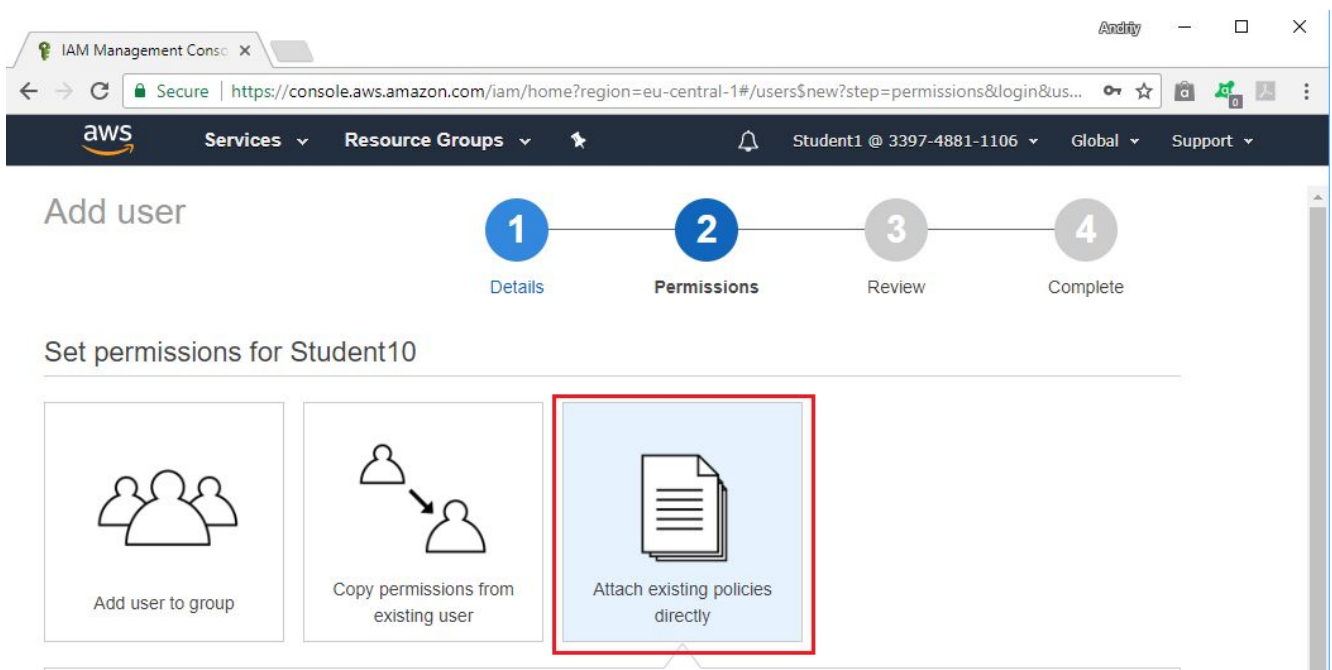
Click on “Add User” button to start creation of new user:



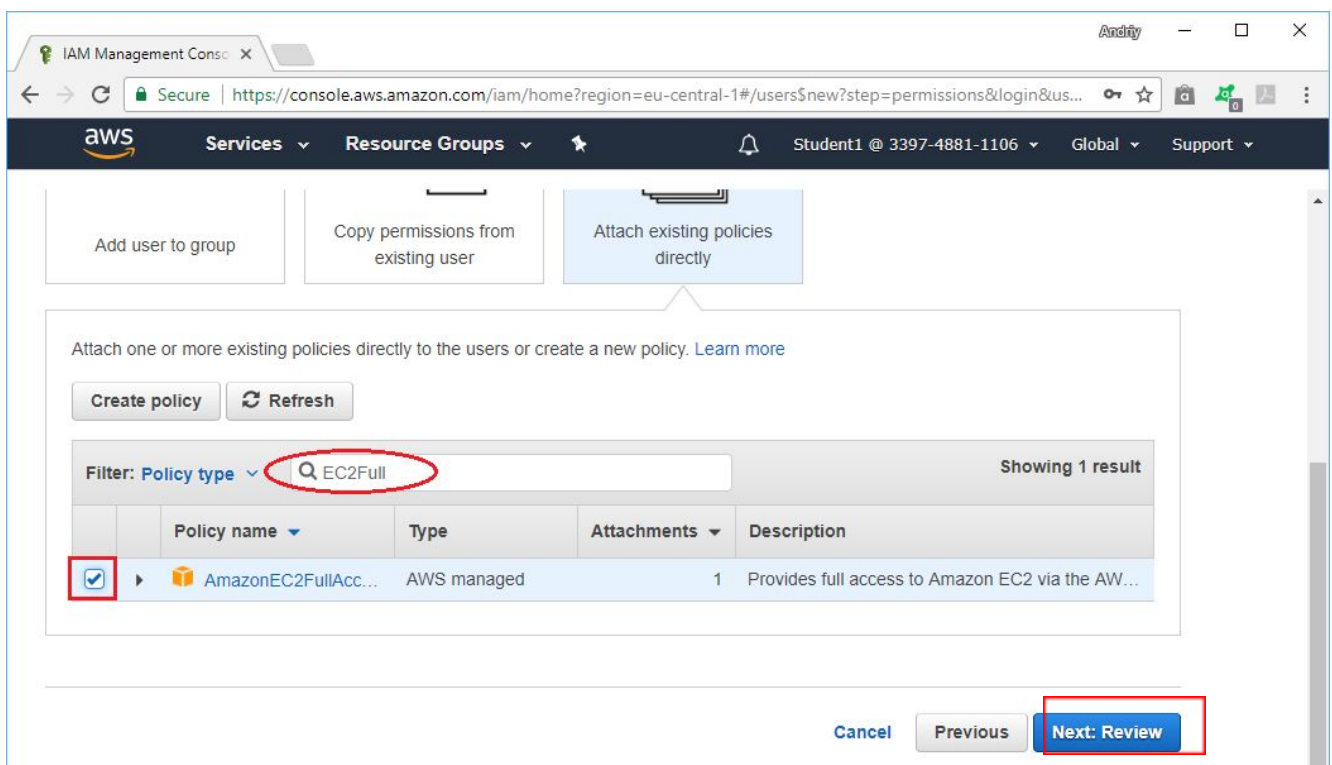
On the next page specify user details as shown below:

The screenshot shows the 'Set user details' page in the AWS IAM Management Console. The page has a title 'Set user details' and a subtitle 'You can add multiple users at once with the same access type and permissions. [Learn more](#)'. The 'User name*' field contains 'Student10'. Below it is a link '+ Add another user'. The 'Select AWS access type' section has a subtitle 'Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)'. Under 'Access type*', 'AWS Management Console access' is selected with a red box. Under 'Console password*', 'Custom password' is selected with a red box. The password field contains '\$training0' and the 'Show password' checkbox is checked with a red box. The 'Require password reset' checkbox is unchecked with a red box. At the bottom right, there is a 'Next: Permissions' button.

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:

Add user

1 Details 2 Permissions 3 **Review** 4 Complete

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	Student10
AWS access type	AWS Management Console access - with a password
Console password type	Custom
Require password reset	No

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	AmazonEC2FullAccess

Cancel Previous **Create user**

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

Search IAM

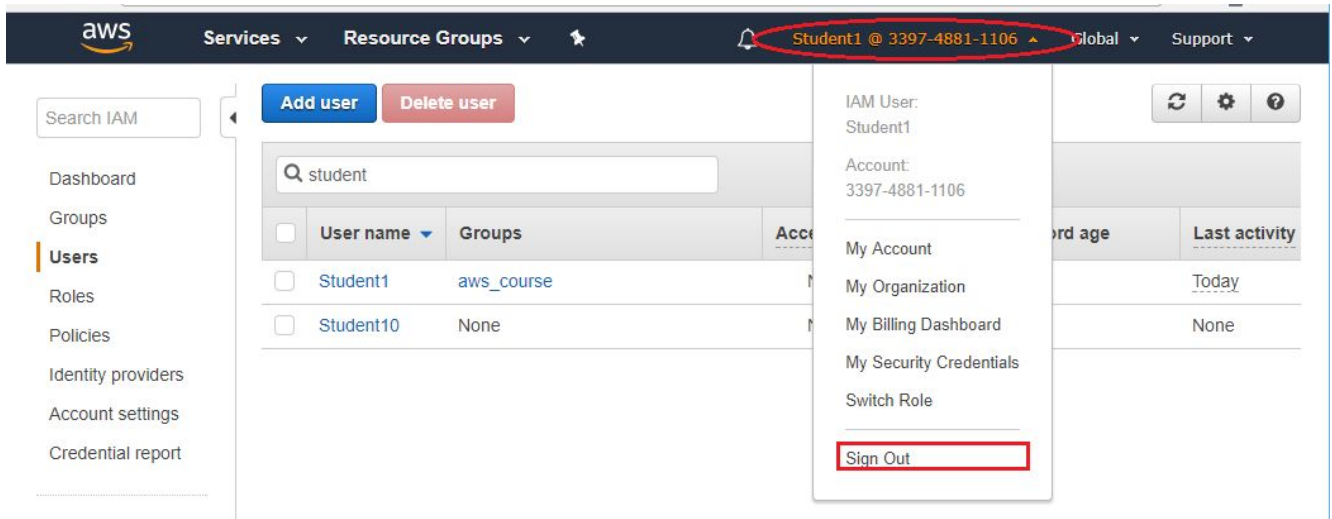
Dashboard
Groups
Users
Roles
Policies
Identity providers
Account settings

Add user Delete user

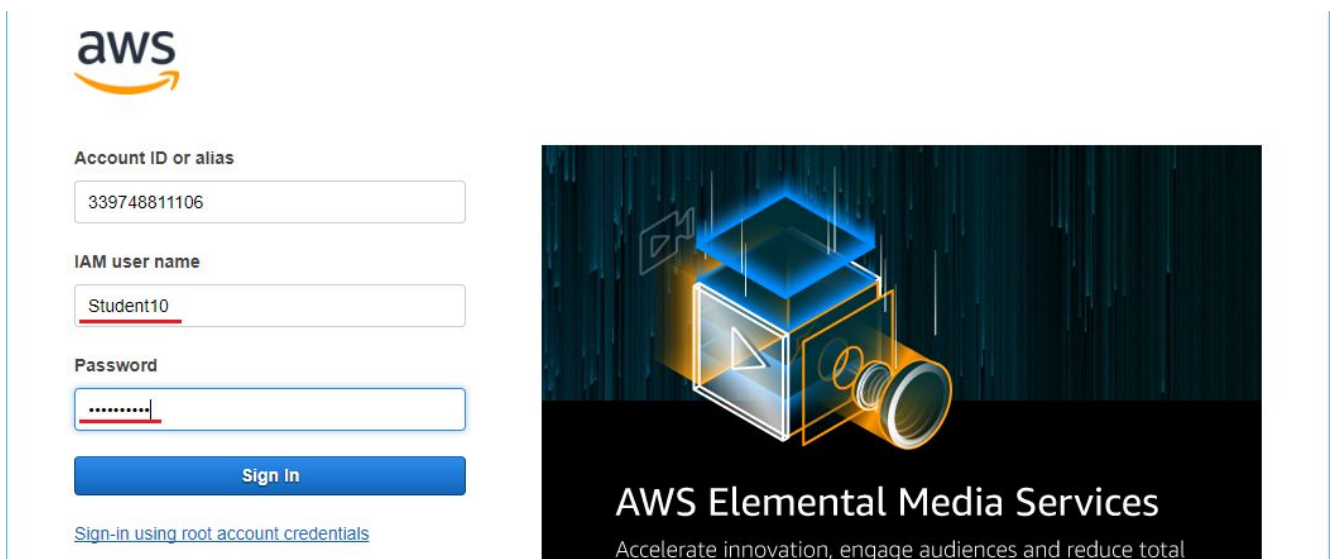
student

	User name	Groups	Access key age	Password age	Last activity
<input type="checkbox"/>	Student1	aws_course	None	Today	Today
<input type="checkbox"/>	Student10	None	None	Today	None

Sign-out from your current account using top menu:



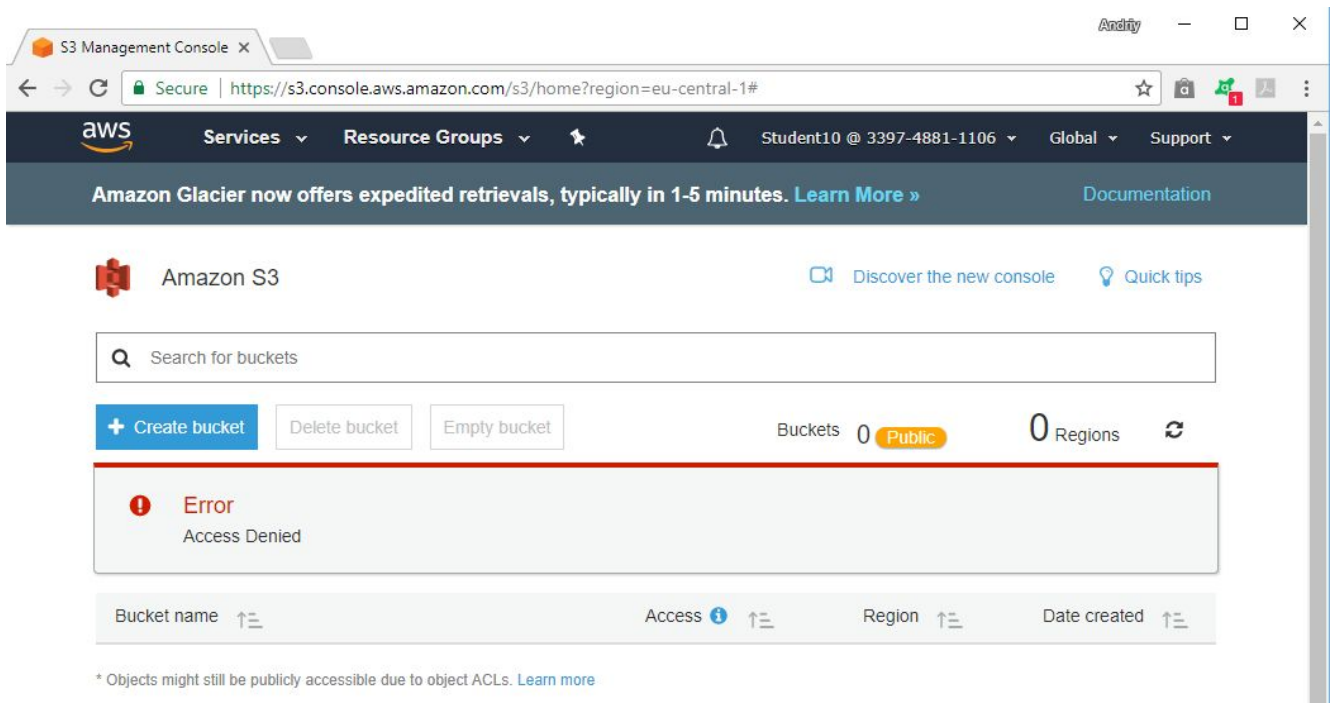
and log in again using Username and password of user you've created before:



You will enter AWS Management Console as usual.

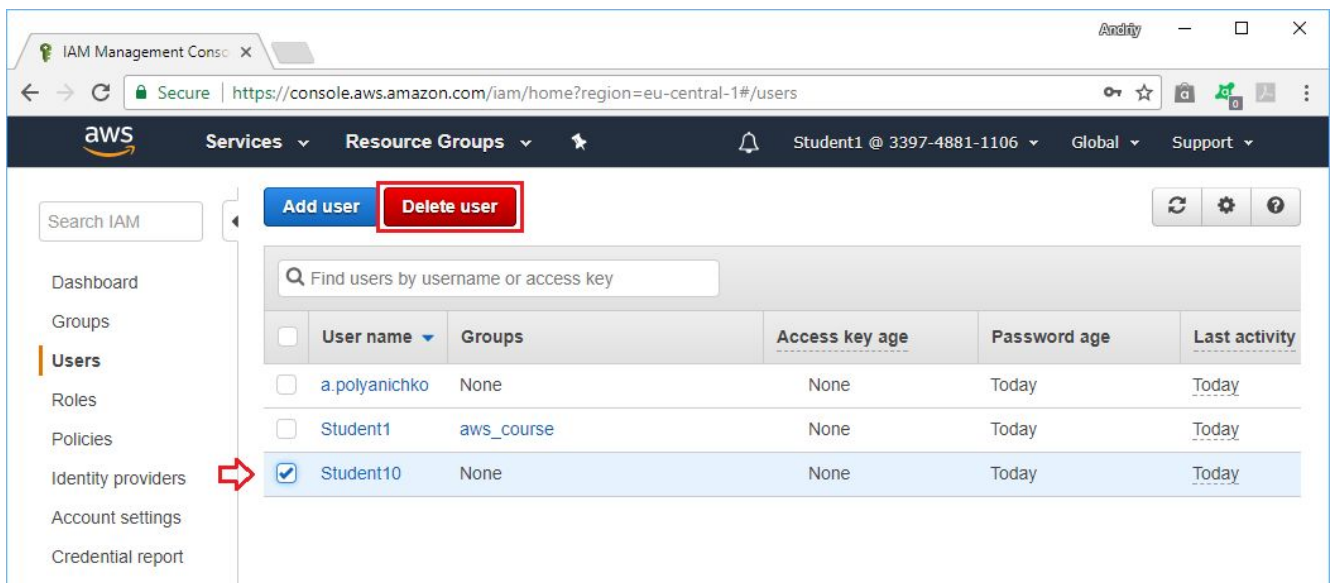
Now, if you will try to access EC2 services, you may consider that Student10 has complete access to all EC2 service functionalities (please check the availability of links which we had used in previous modules, hopefully everything is working).

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

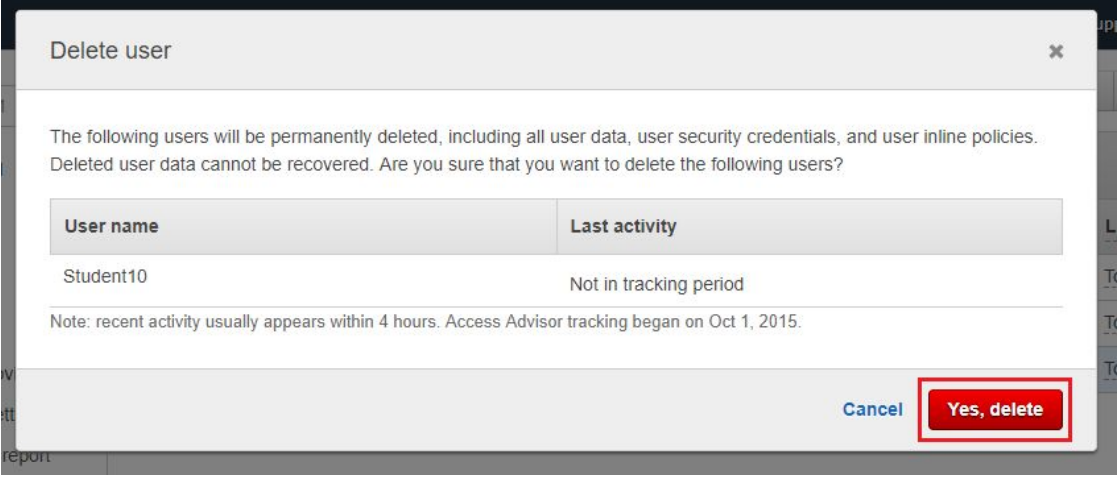


So Student 10 is restricted to access S3 due to corresponding privilege is not allowed explicitly in the attached managed policy.

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:



A screenshot of a 'Delete user' confirmation dialog box. The dialog has a title bar 'Delete user' with a close button. The main text reads: 'The following users will be permanently deleted, including all user data, user security credentials, and user inline policies. Deleted user data cannot be recovered. Are you sure that you want to delete the following users?'. Below this is a table with two columns: 'User name' and 'Last activity'. The table contains one row with 'Student10' and 'Not in tracking period'. A note below the table states: 'Note: recent activity usually appears within 4 hours. Access Advisor tracking began on Oct 1, 2015.' At the bottom right, there are two buttons: 'Cancel' and 'Yes, delete'. The 'Yes, delete' button is highlighted with a red rectangular border.

User name	Last activity
Student10	Not in tracking period

Note: recent activity usually appears within 4 hours. Access Advisor tracking began on Oct 1, 2015.

Cancel Yes, delete

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:

The screenshot shows the AWS IAM Management Console. The left sidebar has a search bar and a list of navigation items: Dashboard, Groups, **Users** (circled in red), Roles, and Policies. The main content area shows a table of users. The first user is 'student1' with the group 'aws_course'. The 'Add user' and 'Delete user' buttons are at the top. The URL in the browser is <https://console.aws.amazon.com/iam/home?region=eu-central-1#/users>.

	User name	Groups	Access key age	Password age	Last activity
<input type="checkbox"/>	student1	aws_course	None	17 days	17 days

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

The screenshot shows the AWS IAM Management Console 'Summary' page for the user 'student1'. The breadcrumb 'Users > student1' has 'student1' circled in red. The 'Permissions' tab is selected. The 'Attached policies: 1' section shows a table with one policy: 'StudentAccess' (Managed policy). The 'Attached directly' section is circled in red. The 'Add permissions' button is at the top left of the permissions section. The URL in the browser is <https://console.aws.amazon.com/iam/home?region=eu-central-1#/users/student1>.

Summary

User ARN: arn:aws:iam::636421644744:user/student1 *(This is an example of ARN)*

Path: /

Creation time: 2017-11-16 16:17 UTC+0300

Permissions | Groups (1) | Security credentials | Access Advisor

Attached policies: 1

Policy name	Policy type
StudentAccess	Managed policy

Attached directly

[Add inline policy](#)

The screenshot shows the AWS IAM Management Console interface. The browser address bar displays the URL: `https://console.aws.amazon.com/iam/home?region=eu-central-1#/users/student1?section=groups`. The left sidebar contains navigation links: Search IAM, Dashboard, Groups, Users (highlighted), Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area shows the 'Summary' page for user 'student1'. The 'Groups (1)' tab is selected, displaying a table with one group: 'aws_course'. The 'Attached permissions' column for this group shows '(No attached permissions for the Group)'. A red circle highlights the 'student1' link in the breadcrumb, and another red circle highlights the 'aws_course' group name. A blue button 'Add user to groups' is visible above the table.

Group name	Attached permissions
aws_course	(No attached permissions for the Group)

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:

The screenshot shows the AWS IAM Management Console interface. The breadcrumb navigation at the top indicates the path: **Users** > **student1**. The left sidebar contains a search bar and a list of navigation items: Dashboard, Groups, **Users**, Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area displays the 'Summary' page for the user 'student1'. The 'Security credentials' tab is selected, showing the 'Sign-in credentials' section. This section includes the following information:

- Console password:** Enabled (with a pencil icon) and a link to 'Manage password'.
- Console login link:** <https://trianqu.signin.aws.amazon.com/console>
- Last login:** 2017-11-16 16:31 UTC+0300
- Assigned MFA device:** No (with a pencil icon)
- Signing certificates:** None (with a pencil icon)

Below the sign-in credentials, there is an 'Access keys' section with a warning message: 'Use access keys to make secure REST or HTTP Query protocol requests to AWS service APIs. For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation. [Learn more](#)'. A 'Create access key' button is present. At the bottom, there is a table with the following headers: Access key ID, Created, Last used, and Status.



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:

The screenshot shows the AWS IAM Management Console interface. The left-hand navigation menu includes options like Dashboard, Groups, Users, Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The 'Users' section is selected, and the user 'student1' is chosen. The 'Summary' page for this user is displayed, with the 'Access Advisor' tab highlighted. The summary shows the User ARN as 'arn:aws:iam::636421644744:user/student1', Path as '/', and Creation time as '2017-11-16 16:17 UTC+0300'. Below this, a table lists the permissions granted to the user. The table has three columns: 'Service Name', 'Policies Granting Permissions', and 'Last Accessed'. One result is shown: 'Amazon EC2' with policy 'StudentAccess' last accessed '17 days ago'.

Service Name	Policies Granting Permissions	Last Accessed
Amazon EC2	StudentAccess	17 days ago

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 screenshot shows the AWS IAM Management Console interface, similar to the previous one, but with the 'Permissions' tab selected. The 'Summary' page for user 'student1' is shown. The 'Permissions' tab is active, displaying a table of attached policies. The table has two columns: 'Policy name' and 'Policy type'. One policy is listed: 'StudentAccess' with a type of 'Managed policy'. The 'StudentAccess' policy name is circled in red. There is an 'Add permissions' button and an 'Add inline policy' button at the bottom right of the table.

Policy name	Policy type
StudentAccess	Managed policy

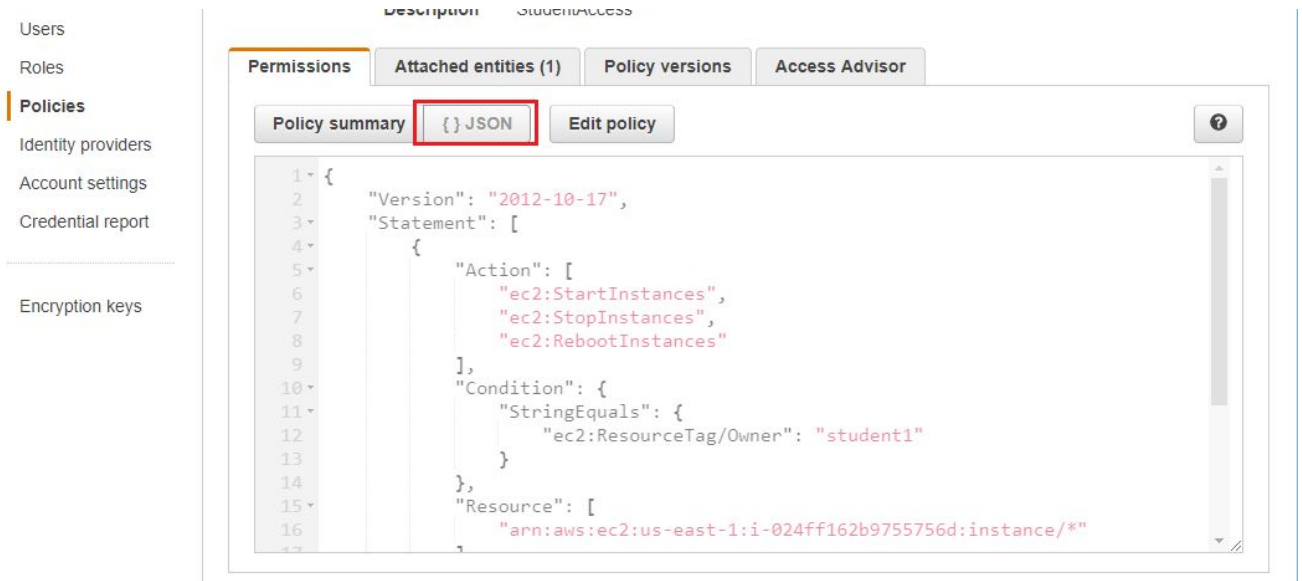
The next page will navigate you to "Policies" item on left-side menu ribbon and will show the

summary of your policy:

The screenshot displays the AWS IAM Management Console interface. The browser address bar shows the URL: <https://console.aws.amazon.com/iam/home?region=eu-central-1#/policies/arn:aws:iam::636421644744:policy/StudentAccess>. The left sidebar contains navigation links: Search IAM, Dashboard, Groups, Users, Roles, Policies (selected), Identity providers, Account settings, Credential report, and Encryption keys. The main content area shows the 'Summary' page for the 'StudentAccess' policy. The policy details are: Policy ARN: `arn:aws:iam::636421644744:policy/StudentAccess`, Description: StudentAccess. The 'Permissions' tab is selected, showing a message: 'This policy does not grant any permissions. To grant access, policies must have an action that has an applicable resource or condition. For details, choose [Show remaining](#). [Learn more](#)'. Below this, there are buttons for 'Policy summary', '{ } JSON', and 'Edit policy'. A table with columns 'Service', 'Access level', 'Resource', and 'Request' is shown. The table content is empty, with a summary row indicating 'Allow (0 of 123 services)' and a link 'Show remaining 123' with a red arrow pointing to it. The footer includes 'Feedback', 'English (US)', copyright information, and links to 'Privacy Policy' and 'Terms of Use'.

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:



The screenshot displays the AWS IAM console interface. On the left, a navigation menu lists 'Users', 'Roles', 'Policies' (highlighted with an orange bar), 'Identity providers', 'Account settings', 'Credential report', and 'Encryption keys'. The main content area is titled 'Description' and 'studentaccess'. It features four tabs: 'Permissions', 'Attached entities (1)', 'Policy versions', and 'Access Advisor'. Below these tabs, there are three buttons: 'Policy summary', '{ } JSON' (highlighted with a red rectangle), and 'Edit policy'. The '{ } JSON' button is selected, displaying the policy's JSON document in a text area. The JSON document is as follows:

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Action": [
6         "ec2:StartInstances",
7         "ec2:StopInstances",
8         "ec2:RebootInstances"
9       ],
10      "Condition": {
11        "StringEquals": {
12          "ec2:ResourceTag/Owner": "student1"
13        }
14      },
15      "Resource": [
16        "arn:aws:ec2:us-east-1:i-024ff162b9755756d:instance/*"
17      ]
18    }
19  ]
20 }
```

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

IAM Management Console

Secure | https://console.aws.amazon.com/iam/home?region=eu-central-1#/policies/arn:aws:iam::636421644744:policy/StudentAccess

aws Services Resource Groups

a.polyanichko @ 6364-2164-4... Global Support

Edit StudentAccess

1 Editor 2 Review

A policy defines the AWS permissions that can be assigned to a user, group, role, or resource. You can construct a policy using the visual editor or create a policy document using the JSON editor.

Option A Visual editor JSON **(Option B)** Import managed policy

Your policy might have been restructured for the visual editor, but the permissions have not changed.

Documentation

Use the visual editor to create and edit a policy by choosing services, actions, resources, and request conditions to add permissions to your policy. You can add multiple permission blocks to define complex permissions or to grant access to more than one service. [Learn more](#)

Expand all | Collapse all

EC2 (3 actions) 1 warning	Clone Remove
EC2 (68 actions) 1 warning	Clone Remove

Add additional permissions

* Required Cancel Review policy

Feedback English (US) © 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

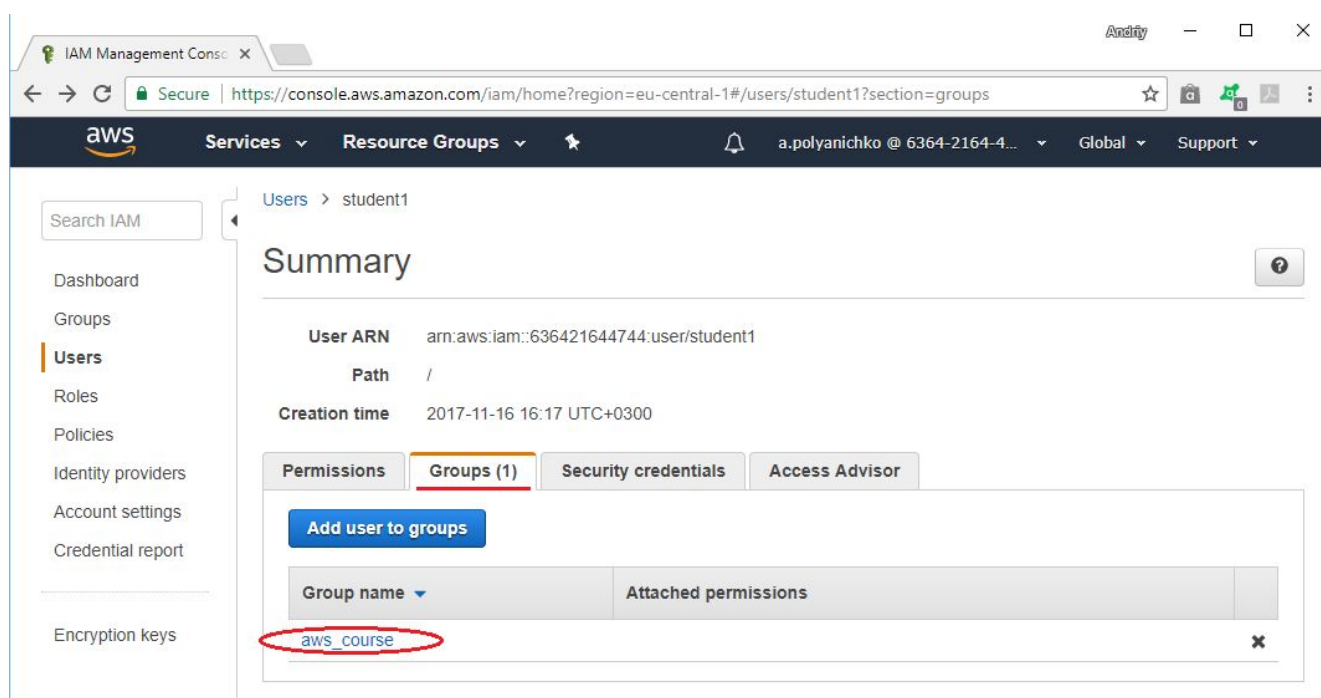


On this page you may select Visual editor or JSON editor depending on what is preferable edit option for you. Finally the result will be the same for any edit options. Also we will have the point to review and check the policy before it will be saved.

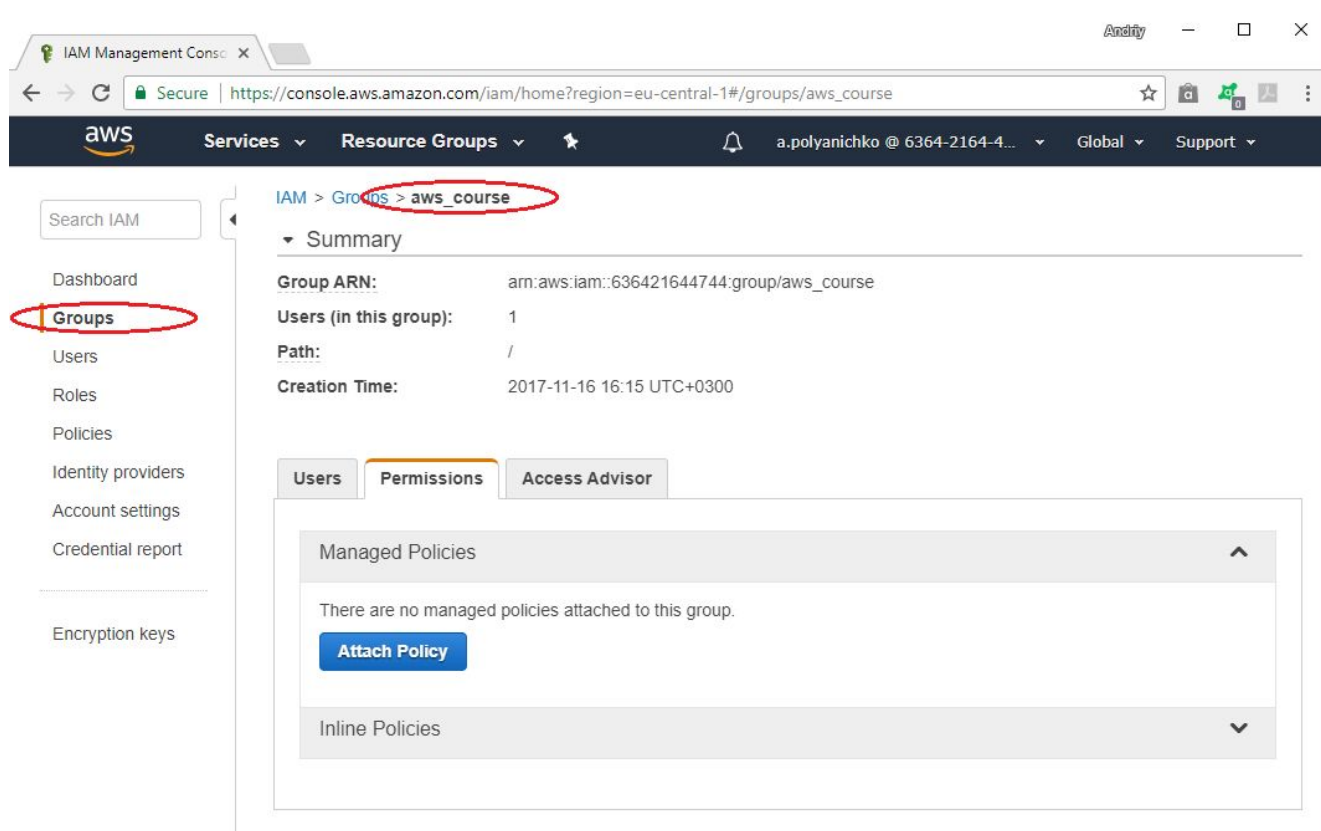


Perhaps, depending on what are your privileges in training account, you will not be able to save your changing in the policy.

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

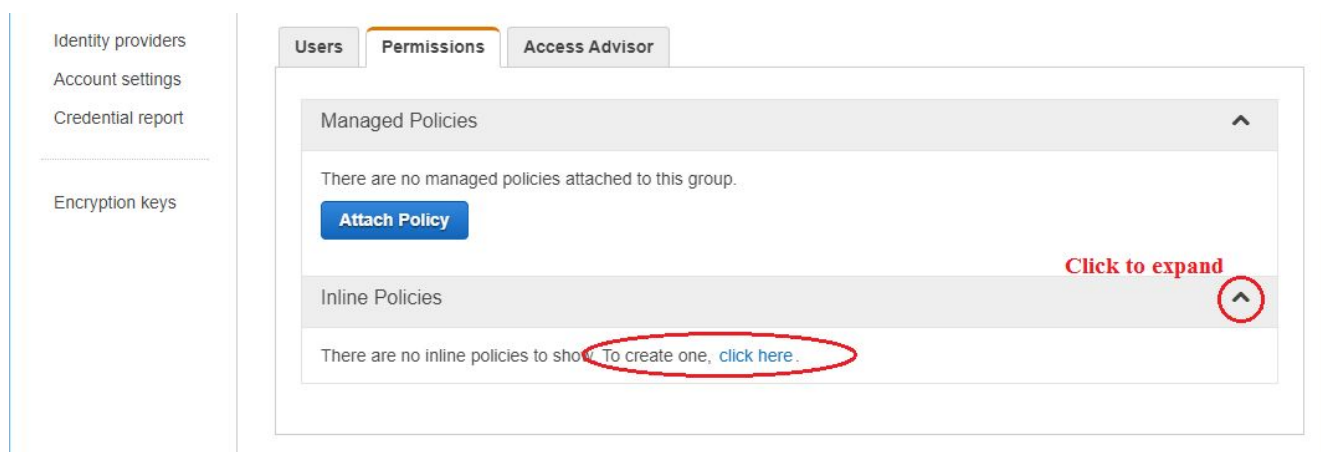


On the next page you will be navigated to “Groups” item on left-side menu ribbon and “permission” tab for the group will be opened:

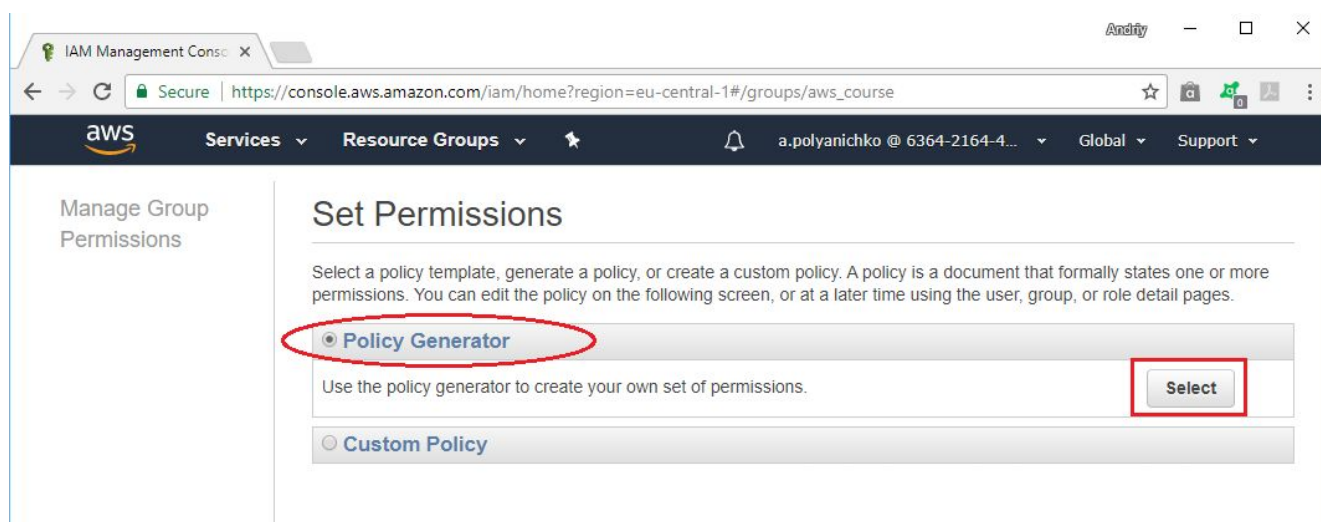


Starting from here let's try to create Inline Policy for the group.

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:

Manage Group Permissions

Edit Permissions

The policy generator enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see [Overview of Policies](#) in Using AWS Identity and Access Management.

- Effect** ☒ Allow ☐ Deny
- AWS Service** AWS Application Discovery Service
- Actions** -- Select Actions --

Amazon Resource Name (ARN)

[Add Conditions \(optional\)](#)

Add Statement

[Cancel](#) [Previous](#) [Next Step](#)

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

AWS Service AWS Application Discovery Service

3 Actions 1 Action(s) Selected

Amazon Resource Name (ARN)

- ☒ CreateTags
- ☐ DeleteTags
- ☐ DescribeAgents

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

Effect ☒ Allow ☐ Deny

AWS Service

Actions

Amazon Resource Name (ARN)

[Add Conditions \(optional\)](#)

4

Effect	Action	Resource
Allow	discovery:CreateTags	*

[Remove](#)

5

5) Click on “Next Step button”:

IAM Management Console

Secure | https://console.aws.amazon.com/iam/home?region=eu-central-1#/groups/aws_course

Services Resource Groups

a.polyanichko @ 6364-2164-4... Global Support

Manage Group Permissions

Review Policy

Customize permissions by editing the following policy document. For more information about the access policy language, see [Overview of Policies](#) in the *Using IAM* guide. To test the effects of this policy before applying your changes, use the [IAM Policy Simulator](#).

Policy Name

policygen-aws_course-201712032308

Policy Document

```

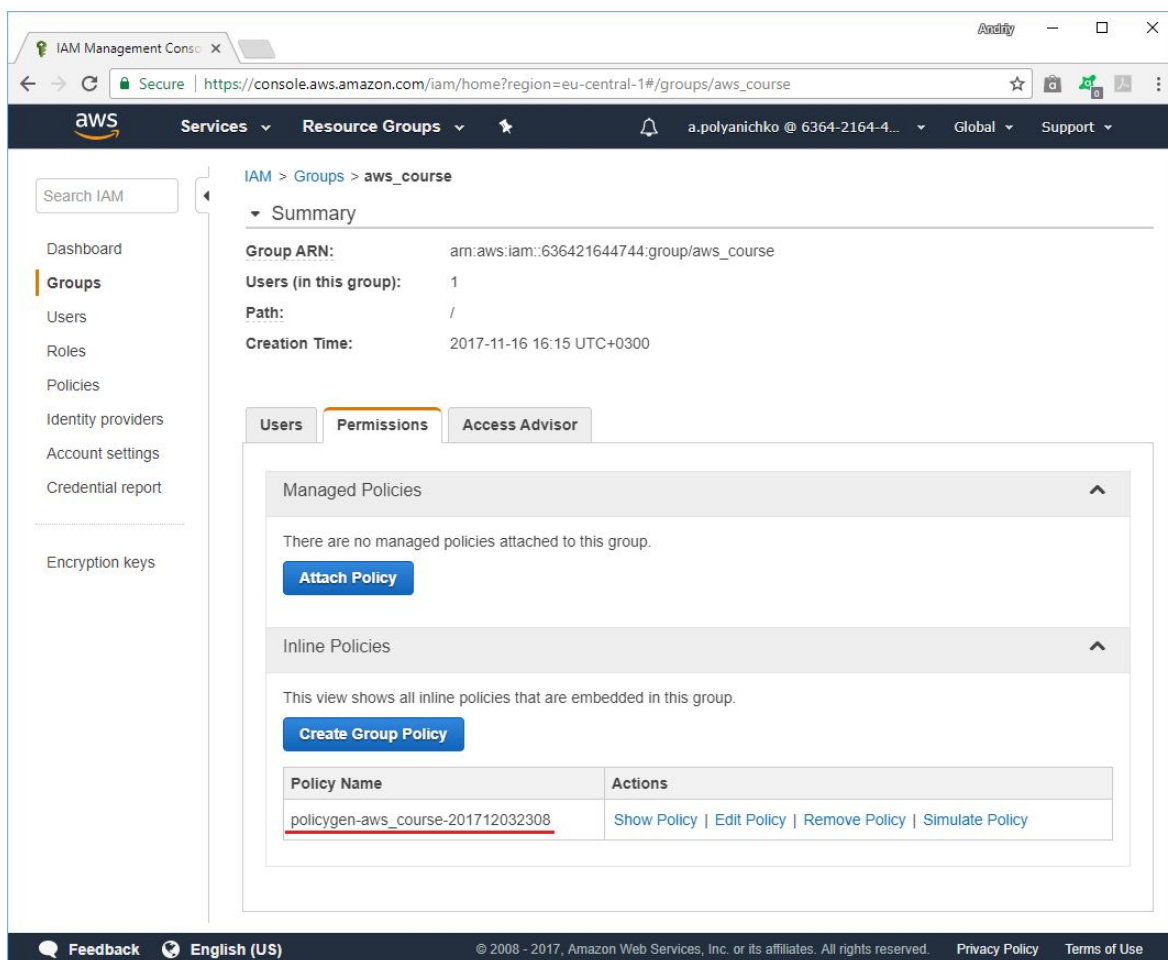
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "Stmnt1512330735000",
6       "Effect": "Allow",
7       "Action": [
8         "discovery:CreateTags"
9       ],
10      "Resource": [
11        "*"
12      ]
13    }
14  ]
15 }
```

☒ Use autoformatting for policy editing

6

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):



The screenshot shows the AWS IAM Management Console interface. The breadcrumb navigation at the top indicates the path: IAM > Groups > aws_course. The left-hand navigation menu includes options like Dashboard, Groups (which is selected), Users, Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area is titled 'Summary' and displays the following details for the 'aws_course' group:

- Group ARN:** arn:aws:iam::636421644744:group/aws_course
- Users (in this group):** 1
- Path:** /
- Creation Time:** 2017-11-16 16:15 UTC+0300

Below the summary, there are three tabs: 'Users', 'Permissions' (which is active), and 'Access Advisor'. The 'Permissions' tab is divided into two sections:

- Managed Policies:** A message states 'There are no managed policies attached to this group.' with an 'Attach Policy' button.
- Inline Policies:** A message states 'This view shows all inline policies that are embedded in this group.' with a 'Create Group Policy' button.

Below these sections is a table listing the inline policies:

Policy Name	Actions
policygen-aws_course-201712032308	Show Policy Edit Policy Remove Policy Simulate Policy

The footer of the console includes a 'Feedback' link, the language 'English (US)', and copyright information: '© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved.' along with links to 'Privacy Policy' and 'Terms of Use'.