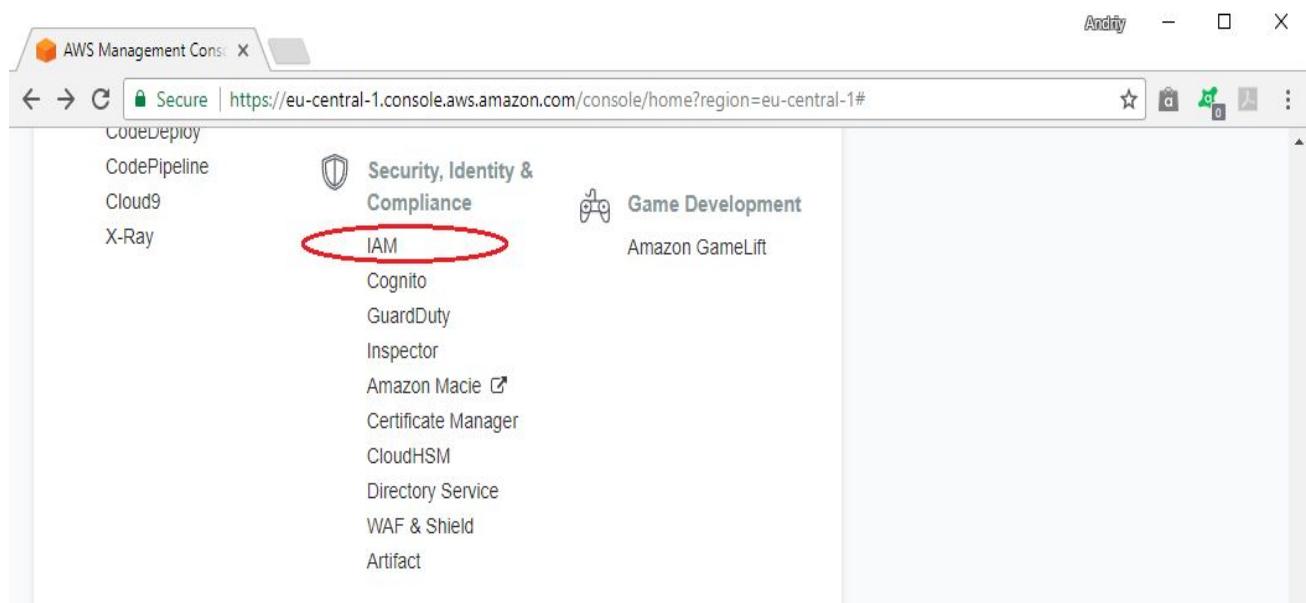


MODULE 5 – LAB EXERCISES

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 main dashboard. The left sidebar has a 'Dashboard' section with links for Groups, Users, Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The 'Users' link is highlighted with a yellow oval. The main content area displays a 'Welcome to Identity and Access Management' message, an 'IAM Resources' summary (Users: 12, Groups: 4, Roles: 8, Identity Providers: 0), a 'Customer Managed Policies' count of 5, and a 'Security Status' bar indicating 5 out of 5 complete. A 'Feature Spotlight' video titled 'Introduction to AWS IAM' is playing. The bottom navigation bar includes 'Feedback', 'English (US)', and links to Privacy Policy and Terms of Use.

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

The screenshot shows the AWS IAM Management Console users list page. The left sidebar has a 'Users' link highlighted with a yellow oval. The main content area shows an 'Add user' and 'Delete user' button, a search bar with 'student', and a table listing users. The table has columns for User name, Groups, Access key age, Password age, and Last activity. One user, 'student1', is listed with the group 'aws_course'. A red arrow points from the 'User name' column of the 'student1' row to the 'student1' value. The bottom navigation bar includes 'Feedback', 'English (US)', and links to Privacy Policy and Terms of Use.

User name	Groups	Access key age	Password age	Last activity
student1	aws_course	None	17 days	17 days

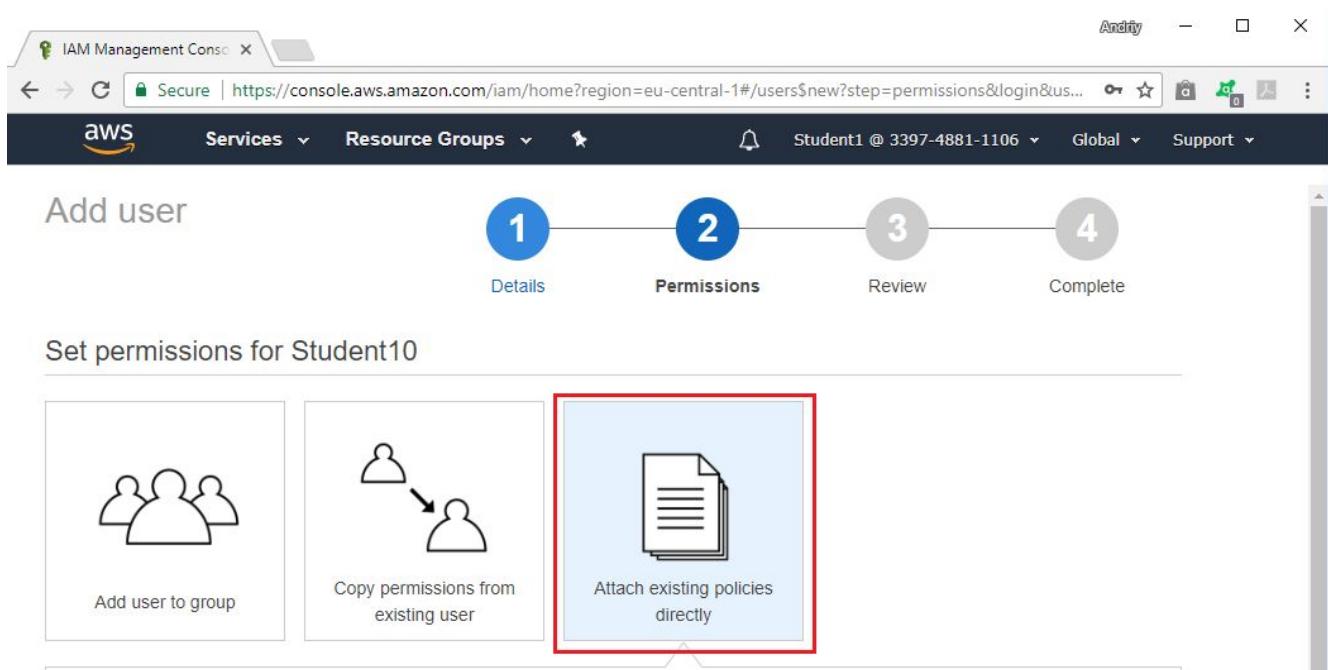
Click on “Add User” button to start creation of new user:

The screenshot shows the AWS IAM Management Console interface. On the left, there's a navigation sidebar with options like Dashboard, Groups, Users (which is selected and highlighted in orange), Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area has a search bar at the top with the query "student". Below it is a table with columns: User name, Groups, Access key age, Password age, and Last activity. One row is visible for "Student1" who is part of the "aws_course" group. At the top of the main area, there are two buttons: "Add user" (highlighted with a red box) and "Delete user".

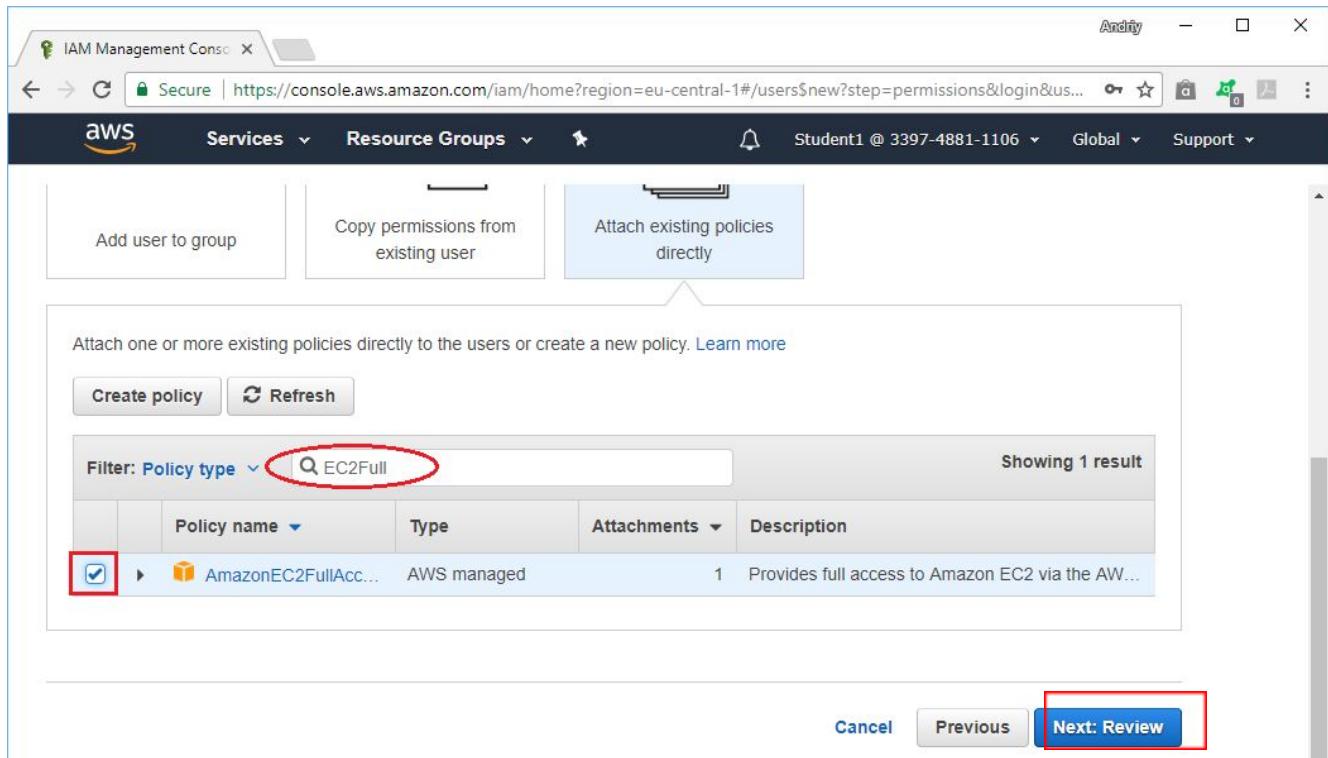
On the next page specify user details as shown below:

The screenshot shows the "Set user details" step of the user creation process. It starts with a "User name" field containing "Student10". Below it is a "User name" link and an "Add another user" button. The "Select AWS access type" section contains two options: "Programmatic access" (unchecked) and "AWS Management Console access" (checked). The "AWS Management Console access" option is described as enabling a password for sign-in to the AWS Management Console. The "Console password" section shows "Custom password" selected (radio button checked), with the password "Straining0" entered into the field. A "Show password" checkbox is checked. The "Require password reset" checkbox is unchecked. At the bottom, there are "Required" and "Next: Permissions" buttons.

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:

Type	Name
Managed policy	AmazonEC2FullAccess

Create user

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

User name	Groups	Access key age	Password age	Last activity
Student1	aws_course	None	Today	Today
Student10	None	None	Today	None

Sign-out from your current account using top menu:

The screenshot shows the AWS IAM service interface. In the top navigation bar, the user's name "Student1 @ 3397-4881-1106" is highlighted with a red oval. On the right side of the page, there is a sidebar with various links. At the bottom of this sidebar, the "Sign Out" button is also highlighted with a red rectangle.

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

The left side of the image shows the AWS sign-in form. It includes fields for "Account ID or alias" (339748811106), "IAM user name" (Student10), and "Password". Below the password field is a "Sign In" button. The right side of the image shows the AWS Elemental Media Services landing page, featuring a video camera icon and the text "AWS Elemental Media Services Accelerate innovation, engage audiences and reduce total".

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:

The screenshot shows the AWS S3 Management Console interface. At the top, there's a banner about Amazon Glacier. Below it, the main header includes the AWS logo, navigation links like 'Services', 'Resource Groups', and user information ('Student10 @ 3397-4881-1106'). A search bar and a 'Discover the new console' link are also present. The main content area is titled 'Amazon S3'. It features a search bar, three buttons ('Create bucket', 'Delete bucket', 'Empty bucket'), and status indicators ('Buckets 0', 'Regions 0'). A prominent red-bordered box contains an 'Error' message: 'Access Denied'. Below this, there are filters for 'Bucket name', 'Access', 'Region', and 'Date created'. A note at the bottom states: '* Objects might still be publicly accessible due to object ACLs. Learn more'.

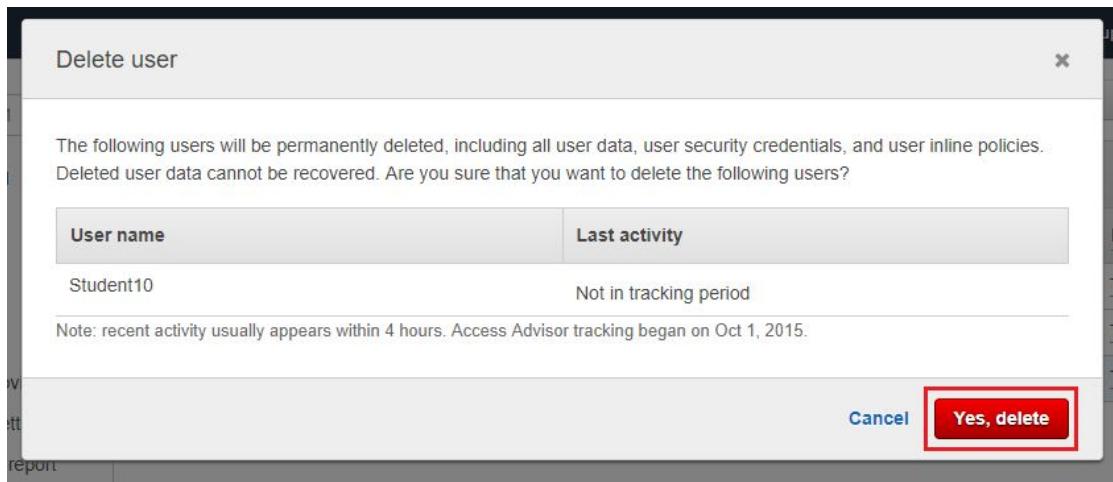
So Student 10 is restricted to access S3 due to corresponding privilege is not allowed explicitly in the attached managed policy.

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:

The screenshot shows the AWS IAM Management Console. The left sidebar has a 'Users' item selected, indicated by a red arrow. The main content area shows a table of users with columns: 'User name', 'Groups', 'Access key age', 'Password age', and 'Last activity'. The table lists three users: 'a.polyanichko', 'Student1', and 'Student10'. The 'Delete user' button is highlighted with a red border. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', user info ('Student1 @ 3397-4881-1106'), and standard navigation links.

User name	Groups	Access key age	Password age	Last activity
a.polyanichko	None	None	Today	Today
Student1	aws_course	None	Today	Today
Student10	None	None	Today	Today

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:

The screenshot shows the AWS IAM Management Console. The top navigation bar includes the AWS logo, Services dropdown, Resource Groups dropdown, a notification bell, and user information (a.polyanichko @ 6364-2164-4...). Below the navigation is a search bar with 'Search IAM' and a 'User name' dropdown set to 'student'. There are 'Add user' and 'Delete user' buttons. To the left is a sidebar with 'Dashboard', 'Groups', 'Users' (which is highlighted and circled in red), 'Roles', and 'Policies'. The main content area displays a table with one user entry: student1, aws_course, None, 17 days, 17 days. A red arrow points to the 'student1' link in the table.

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 with the URL https://console.aws.amazon.com/iam/home?region=eu-central-1#/users/student1. The top navigation bar and sidebar are identical to the previous screenshot. The main content area is titled 'Summary' for the user 'student1'. It shows the User ARN (arn:aws:iam::636421644744:user/student1) and Creation time (2017-11-16 16:17 UTC+0300). Below this is a 'Permissions' tab (which is highlighted and circled in red), followed by 'Groups (1)', 'Security credentials', and 'Access Advisor'. Under the 'Permissions' tab, there is an 'Add permissions' button and a table showing attached policies. One policy, 'StudentAccess', is listed under 'Attached directly' and is identified as a 'Managed policy'. A red circle highlights the 'Attached directly' section.

The screenshot shows the AWS IAM Management Console interface. The URL in the browser is <https://console.aws.amazon.com/iam/home?region=eu-central-1#/users/student1?section=groups>. The left sidebar is collapsed, and the main area shows the 'Summary' tab for the user 'student1'. The 'Groups (1)' tab is selected, highlighted with a red circle. Below it, there is a table with one row, where the 'Group name' column contains 'aws_course' and the 'Attached permissions' column contains the text '(No attached permissions for the Group)'. A red circle also highlights the 'aws_course' entry in the 'Group name' column.

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 with the URL https://console.aws.amazon.com/iam/home?region=eu-central-1#/users/student1?section=security_credentials. The left sidebar is collapsed, and the main area shows the 'Summary' for user 'student1'. The 'Security credentials' tab is active. The 'Sign-in credentials' section shows:

- Console password: Enabled (Manage password)
- Console login link: <https://triangu.signin.aws.amazon.com/console>
- Last login: 2017-11-16 16:31 UTC+0300
- Assigned MFA device: No
- Signing certificates: None

The 'Access keys' section contains a 'Create access key' button and a table with the following columns: Access key ID, Created, Last used, and Status. The table currently displays 'No results'.

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

! 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:

User ARN: arn:aws:iam::636421644744:user/student1
Path: /
Creation time: 2017-11-16 16:17 UTC+0300

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:

User ARN: arn:aws:iam::636421644744:user/student1
Path: /
Creation time: 2017-11-16 16:17 UTC+0300

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 shows the AWS IAM Management Console interface. The left sidebar is collapsed. The main header bar has tabs for Services, Resource Groups, Global, and Support. The URL in the address bar is https://console.aws.amazon.com/iam/home?region=eu-central-1#/policies/arn:aws:iam::636421644744:policy/StudentAccess. The title bar says "IAM Management Consc". The top navigation bar includes "Andify", a user icon, and a close button.

The main content area is titled "Summary" for the policy "StudentAccess". It shows the "Policy ARN" as arn:aws:iam::636421644744:policy/StudentAccess and the "Description" as StudentAccess. Below this, there are four tabs: "Permissions" (selected), "Attached entities (1)", "Policy versions", and "Access Advisor".

The "Permissions" tab contains 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 the message are three buttons: "Policy summary", "{} JSON", and "Edit policy".

The main table area has columns for "Service", "Access level", "Resource", and "Request". At the top of this table, there are filters: "Service", "Access level", "Resource", and "Request".

At the bottom of the table, there is a row with the text "Allow (0 of 123 services) Show remaining 123" followed by a red arrow pointing to the "Show remaining 123" link.

The footer of the page includes links for "Feedback", "English (US)", "© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved.", "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 shows the AWS IAM console. On the left, a sidebar menu is open with the following options: Users, Roles, Policies (which is selected and highlighted in orange), Identity providers, Account settings, Credential report, and Encryption keys. The main area is titled "Permissions" and contains tabs for "Description", "STRUCTURAL ACCESS", "Attached entities (1)", "Policy versions", and "Access Advisor". Below these tabs is a "Policy summary" section with a "JSON" button, which is highlighted with a red box. To the right of the JSON button is an "Edit policy" button. The main content area displays a JSON document with line numbers from 1 to 17 on the left. The JSON code 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:

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.

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:

The screenshot shows the AWS IAM Management Console. On the left, the navigation menu is visible with 'Users' selected. In the main area, under 'Summary', it 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, there are tabs for 'Permissions', 'Groups (1)', 'Security credentials', and 'Access Advisor'. The 'Groups (1)' tab is active, showing a button 'Add user to groups' and a table with a single row for 'aws_course'. The 'aws_course' entry is circled in red.

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:

The screenshot shows the AWS IAM Management Console with the 'Groups' item in the left sidebar circled in red. The current view is the 'Summary' section for the 'aws_course' group. It displays the Group ARN as arn:aws:iam::636421644744:group/aws_course, Users (in this group) as 1, Path as /, and Creation Time as 2017-11-16 16:15 UTC+0300. Below this, there are tabs for 'Users', 'Permissions', and 'Access Advisor'. The 'Permissions' tab is active, showing sections for 'Managed Policies' and 'Inline Policies'. The 'Managed Policies' section states 'There are no managed policies attached to this group.' and has a 'Attach Policy' button. The 'Inline Policies' section is currently collapsed.

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:

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.

1 Effect Allow Deny

2 AWS Service AWS Application Discovery S...

3 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 S...

3 Actions 1 Action(s) Selected

Amazon Resource Name (ARN)

All Actions (*)

CreateTags

DeleteTags

DescribeAgents

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

Effect Allow Deny

AWS Service AWS Application Discovery S...

Actions -- Select Actions --

Amazon Resource Name (ARN) *

Add Conditions (optional)

4 Add Statement

Effect	Action	Resource
Allow	discovery:CreateTags	*

5

Cancel Previous **Next Step**

5) Click on “Next Step button”:

IAM Management Console X

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

aws Services Resource Groups 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": "Stmt1512330735000",
6       "Effect": "Allow",
7       "Action": [
8         "discovery:CreateTags"
9       ],
10      "Resource": [
11        "*"
12      ]
13    }
14  }
15 }
```

Use autoformatting for policy editing

Cancel Validate Policy **Apply Policy** 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):

IAM Management Console Andrey

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

aWS Services Resource Groups a polyanichko @ 6364-2164-4... Global Support

Search IAM

Groups Groups

Users Roles Policies Identity providers Account settings Credential report

Encryption keys

IAM > Groups > aws_course

Summary

Group ARN: arn:aws:iam::636421644744:group/aws_course

Users (in this group): 1

Path: /

Creation Time: 2017-11-16 16:15 UTC+0300

Users Permissions Access Advisor

Managed Policies

There are no managed policies attached to this group.

Attach Policy

Inline Policies

This view shows all inline policies that are embedded in this group.

Create Group Policy

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

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