

Assignment sheet for IAM Assignment

1. Create an IAM user with username of your own wish and grant administrator policy

- Create user name with **Batman**

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name* Batman

[Add another user](#)

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Select AWS credential type*

☐ Access key - Programmatic access
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☒ Password - AWS Management Console access
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password*

☐ Autogenerated password

☒ Custom password

☐ Show password

* Required

[Cancel](#) [Next: Permissions](#)

1. Created a group **Shoaib_IBM** and grant administrator policy

Set permissions

[Add user to group](#) [Copy permissions from existing user](#) [Attach existing policies directly](#)

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Add user to group

[Create group](#) [Refresh](#)

Search Showing 1 result

Group	Attached policies
<input checked="" type="checkbox"/> Shoaib_IAM	AdministratorAccess

[Set permissions boundary](#)

[Cancel](#) [Previous](#) [Next: Tags](#)

- Click on create user and user is created

Add user

[Success](#)

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://607897239025.signin.aws.amazon.com/console>

[Download .csv](#)

User	Email login instructions
<input checked="" type="checkbox"/> Batman	Send email

[Close](#)

Feedback [Looking for language selection? Find it in the new Unified Settings](#)

© 2022 Amazon Internet Services Private Ltd. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

2. Hello students, in this assignment you need to prepare a developers team of avengers. - Create 3 IAM users of avengers and assign them in developer's groups with IAM policy.

- Add 3 user name using add username button

The screenshot shows the 'Add user' console in the AWS IAM console. The 'Set user details' step is active, showing the 'User name' field with three entries: 'Ironman', 'Thor', and 'groot'. Below this, the 'Select AWS access type' section shows 'Password - AWS Management Console access' selected. The 'Console password' section shows 'Custom password' selected with a masked password field. The 'Next: Permissions' button is visible at the bottom right.

- Create a group name **developer** and add IAM Policy .

The screenshot shows the 'Create group' console in the AWS IAM console. The 'Group name' field is set to 'developers'. The 'Filter policies' section shows a search for 'iam' with 9 results. The 'IAMFullAccess' policy is selected. The 'Create group' button is visible at the bottom right.

The screenshot shows the 'Set permissions' console in the AWS IAM console. The 'Add user to group' step is active, showing the 'Add user to group' button. The 'Add user to group' section shows a search for 'group' with 2 results. The 'developers' group is selected. The 'Set permissions boundary' section is visible below.

- Check the user created in the User tab at the right side of the console

The screenshot shows the AWS IAM console interface. On the left is the navigation menu with sections like 'Access management', 'Access reports', and 'Related consoles'. The main content area is titled 'IAM > User groups > developers'. Below the title is a 'Summary' section with details like 'User group name: developers', 'Creation time: November 27, 2022, 15:51 (UTC+05:30)', and 'ARN: arn:aws:iam:607897239025:group/developers'. The 'Users' tab is active, showing a table of users in the group. The table has columns for 'User name', 'Groups', 'Last activity', and 'Creation time'. Three users are listed: Ironman, groot, and Thor, each with 1 group, no last activity, and a 'Now' creation time.

3. Define a condition in policy for expiration like

"DateGreaterThan": {"aws:CurrentTime": "2020-04-01T00:00:00Z"}, "DateLessThan": {"aws:CurrentTime": "2020-06-30T23:59:59Z"}

- Created new policy for expiration

The screenshot shows the 'Create policy' page in the AWS IAM console. The 'JSON' tab is selected, displaying a policy document. The policy has an 'Effect' of 'allow', an 'Action' of 'iam:*', and a 'Resource' of '*'. The 'Condition' is defined with two rules: 'DateGreaterThan' with value 'aws:CurrentTime: 2020-04-01T00:00:00Z' and 'DateLessThan' with value 'aws:CurrentTime: 2020-06-30T23:59:59Z'. The policy is named 'Date_expiration'. Below the JSON editor, there are tabs for 'Security', 'Errors', 'Warnings', and 'Suggestions'. The 'Warnings' tab shows one warning: 'Character count: 554 of 5,120. The current character count includes character for all inline policies in the group: developers.' There are 'Cancel' and 'Review policy' buttons at the bottom.

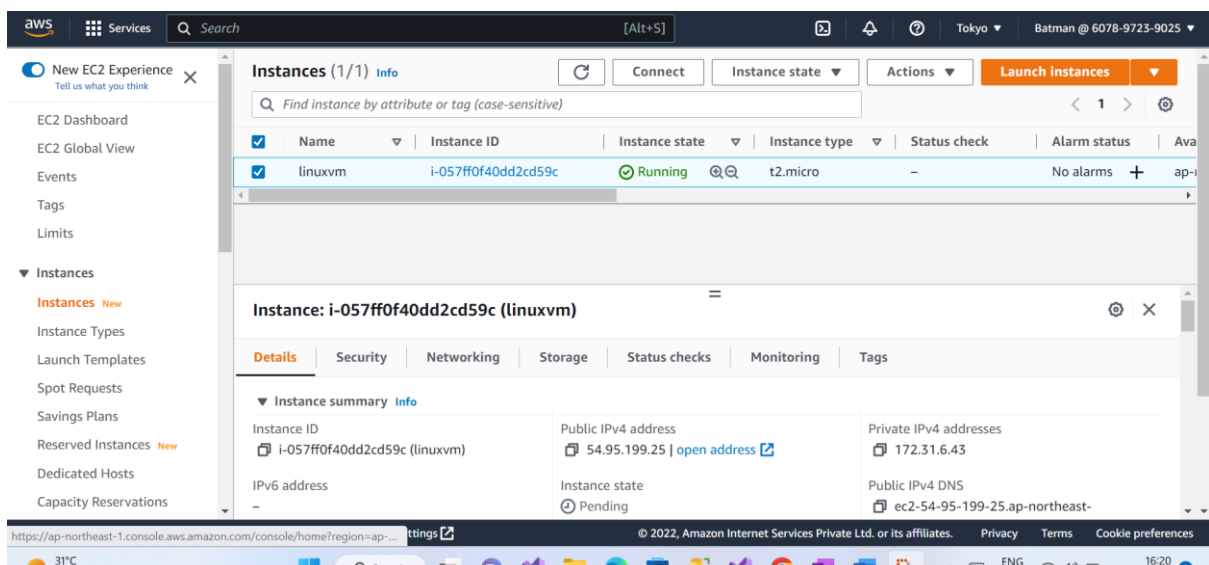
The screenshot shows the AWS IAM console interface, similar to the first screenshot. The 'Permissions' tab is now selected for the 'developers' user group. It shows a table of 'Permissions policies (2)'. The table has columns for 'Policy name', 'Type', and 'Description'. Two policies are listed: 'IAMFullAccess' (AWS managed) and 'Date_expiration' (Customer inline). The 'Date_expiration' policy is highlighted in blue. There are 'Simulate', 'Remove', and 'Add permissions' buttons at the top right of the table.

4. Prepare 15 authentic MCQ questions related to IAM.

1. IAM policy documents are written in which format? **JSON**
2. Which user has no permission by default? **IAM user**
3. One of the elements is an optional element of an IAM policy document, which one is it? **Condition**
4. What you need to allow a lambda function to do an action on S3 Bucket? **IAM Role and IAM Policy**
5. This IAM resource can be reused across multiple identities, guess who? **IAM Managed Policies**
6. What are managed by using IAM? **MFA, Role**
7. What is the name of the tool which tells if identities within your account would be able to take actions? **The Policy Simulator**
8. Which of these are features of IAM? **Access Advisor, Password policy**
9. This is not a component of IAM? **Organizational Units**
10. This is not a feature of IAM? **IAM allows you to setup biometric authentication, so that no passwords are required**
11. describes IAM? **IAM allows you to manage users, groups, roles, and their corresponding level of access to the AWS Platform.**
12. IAM principal? **User, role and application**
13. IAM role Does not have any credentials (password or access keys) associated with it
14. AWS evaluates _____ when an IAM principal makes a request.? **Security Policies**
15. Names of IAM identities (users, roles, and groups)? **Must be unique within the AWS account**

5. -Launch your linux instance in IAM and update your machine

1. Linux instance created



- Update the system

```
aws Services Search [Alt+S] Tokyo Batman @ 6078-9723-9025
Package Arch Version Repository Size
-----
Installing:
kernel x86_64 5.10.149-133.644.amzn2 amzn2extra-kernel-5.10 32 M
Transaction Summary
-----
Install 1 Package

Total download size: 32 M
Installed size: 136 M
Downloading packages:
Delta RPMs disabled because /usr/bin/applydeltarpm not installed.
kernel-5.10.149-133.644.amzn2.x86_64.rpm | 32 MB 00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : kernel-5.10.149-133.644.amzn2.x86_64 1/1
  Verifying : kernel-5.10.149-133.644.amzn2.x86_64 1/1
Installed:
kernel.x86_64 0:5.10.149-133.644.amzn2
Complete!
ec2-user@ip-172-31-6-43 ~]$
```