

# Assignment sheet for IAM

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

The screenshot shows the 'Add user' page in the AWS IAM console, specifically the 'Review' step (step 4 of 5). The page title is 'Add user'. Below the title, there's a 'Review' section with a sub-header 'Review your choices. After you create the user, you can view and download the autogenerated password and access key.' The 'User details' section shows the following information:

Property	Value
User name	Rahul_DevOps
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	No
Permissions boundary	Permissions boundary is not set

The 'Permissions summary' section shows: 'The following policies will be attached to the user shown above.'

Type	Name
Managed policy	AdministratorAccess

The 'Tags' section shows: 'No tags were added.'

At the bottom, there are three buttons: 'Cancel', 'Previous', and 'Create user'.

## After Creation

The screenshot shows the 'Summary' page for the user 'Rahul\_DevOps' in the AWS IAM console. At the top, there's a notification banner: 'New feature to generate a policy based on CloudTrail events. AWS uses your CloudTrail events to identify the services and actions used and generate a least privileged policy that you can attach to this user.' Below the notification, the breadcrumb 'Users > Rahul\_DevOps' is visible. The 'Summary' section shows the following information:

Property	Value
User ARN	arn:aws:iam::563684797122:user/Rahul_DevOps
Path	/
Creation time	2022-11-04 00:27 UTC+0530

Below the summary, there are tabs for 'Permissions', 'Groups', 'Tags', 'Security credentials', and 'Access Advisor'. The 'Permissions' tab is selected, showing 'Permissions policies (1 policy applied)'. There are two buttons: 'Add permissions' and 'Add inline policy'. Below these buttons, there's a table showing the attached policy:

Policy name	Policy type
AdministratorAccess	AWS managed policy

Assignment 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.

### 3 IAM Users of Avengers in Developers Group

[IAM](#) > [User groups](#) > [Developers](#)

## Developers

Delete

### Summary

Edit

User group name	Creation time	ARN
Developers	November 05, 2022, 12:02 (UTC+05:30)	<a href="#">arn:aws:iam::563684797122:group/Developers</a>

[Users](#) | [Permissions](#) | [Access Advisor](#)

### Users in this group (3)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.



Remove users

Add users

Search

< 1 > ⚙

<input type="checkbox"/>	User name <a href="#">↗</a>	Groups	Last activity	Creation time
<input type="checkbox"/>	StarLord	1	None	30 minutes ago
<input type="checkbox"/>	Spiderman	1	None	35 minutes ago
<input type="checkbox"/>	Black_Panther	1	None	31 minutes ago

### IAM Policy of Developers group

[IAM](#) > [User groups](#) > [Developers](#)

## Developers

Delete

### Summary

Edit

User group name	Creation time	ARN
Developers	November 05, 2022, 12:02 (UTC+05:30)	<a href="#">arn:aws:iam::563684797122:group/Developers</a>

[Users](#) | [Permissions](#) | [Access Advisor](#)

### Permissions policies (1) [Info](#)

You can attach up to 10 managed policies.



Simulate

Remove

Add permissions ▼

Filter policies by property or policy name and press enter.

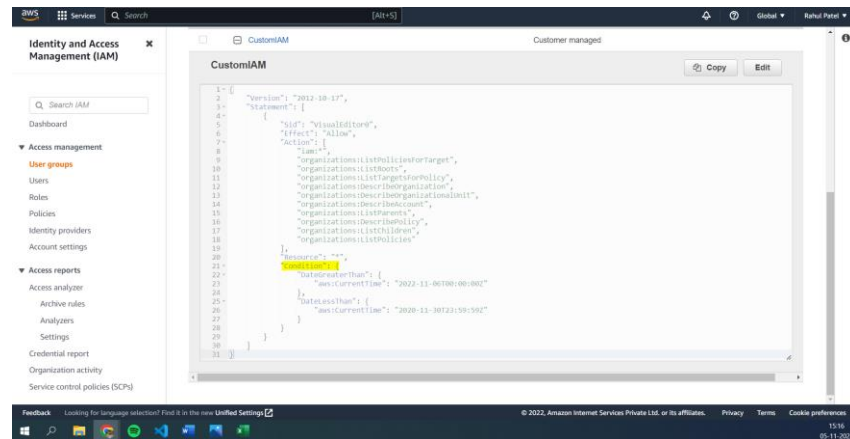
< 1 > ⚙

<input type="checkbox"/>	Policy name <a href="#">↗</a>	Type	Description
<input type="checkbox"/>	IAMFullAccess	AWS managed	

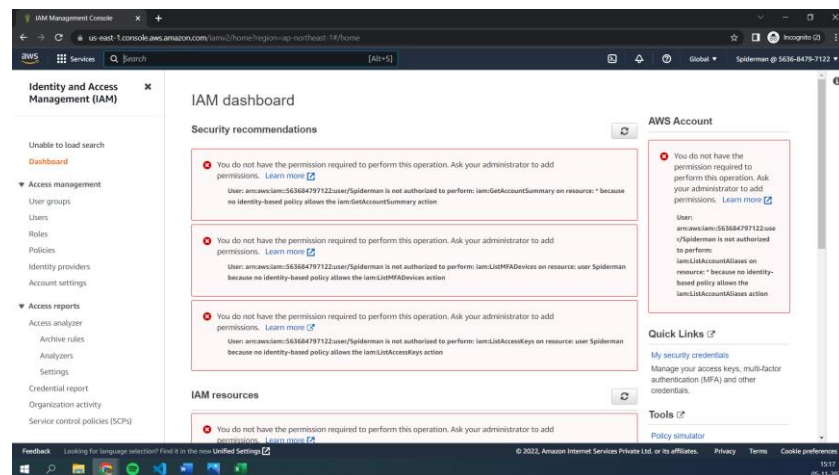
Assignment 3 :- Define a condition in policy for expiration like  
 "DateGreaterThan": {"aws:CurrentTime": "2020-04-01T00:00:00Z"},  
 "DateLessThan": {"aws:CurrentTime": "2020-06-30T23:59:59Z"}

Define the span of 4 months as per your wish

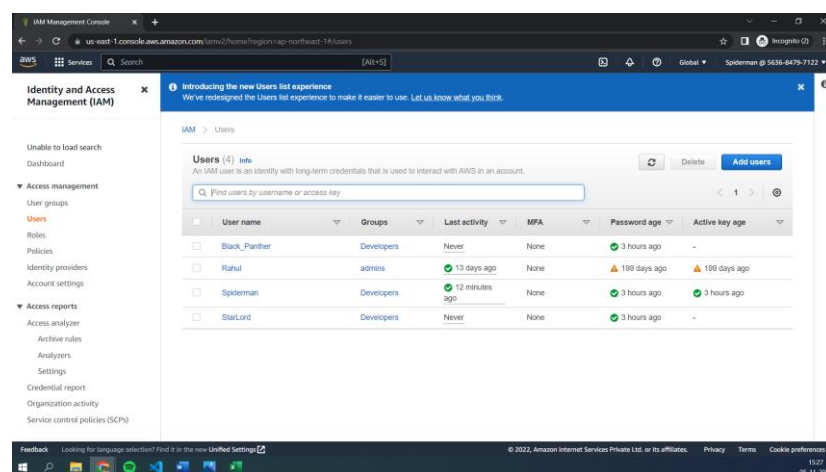
Created IAM policy for IAM and added condition



As per the policy user can access IAM date starting from 6-Nov-2022 to 30-Nov-2022 but today is 5-Nov so user can't access.



After changing the date to 05-Nov-2022

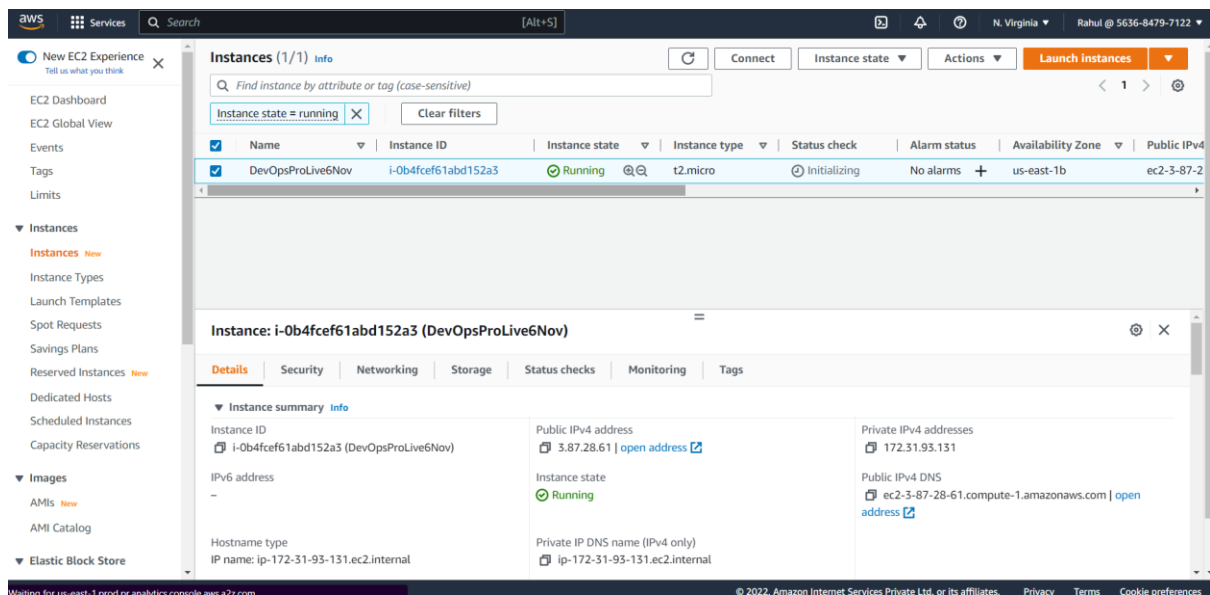


### Assignment 3 :- Prepare 15 authentic MCQ questions related to IAM.

1. In which you can give access control by tag?
  - A. Attribute-based
  - B. Role based
  - C. Resource based**
  - D. All of them
2. Which default IAM policy applied to IAM user?
  - A. AWS managed
  - B. Customer managed
  - C. Inline Policy
  - D. None of above**
3. Is IAM service region-specific?
  - A. True
  - B. False**
4. In which file format you can write IAM policy?
  - A. XML
  - B. JSON**
  - C. txt
  - D. All of above
5. Which of the following credentials are needed to login as IAM user?
  - A. Account ID or Account Alias
  - B. Password
  - C. IAM user name
  - D. B and C
  - E. A, B and C**
6. What are the ways you can access IAM? (Select two)
  - A. AWS SDKs**
  - B. AWS EC2
  - C. AWS S3
  - D. AWS Command Line tools**
7. Which of the following section in policy defined the entities to who access to a resource is allowed or not?
  - A. Resource
  - B. Principal**
  - C. Conditions
  - D. Statement ID
8. Which of the following is not feature of AWS IAM?
  - A. IAM offers centralized control of your AWS account
  - B. Free to use
  - C. Multi-Factor authentication
  - D. IAM allows you to setup biometric authentication**
9. What is the length of account id of IAM user?
  - A. 10 digits
  - B. 14 digits
  - C. 12 digits**
  - D. 15 digits

10. When a principal tries to use the AWS management console, the AWS API, or the AWS CLI, that principal sends a request to AWS. And that request includes which of the following information? (Select All that apply)
- A. Resources
  - B. Environment data
  - C. User Password
  - D. Action or operations
11. Which of the following is not an IAM best practice?
- A. Delete user account not in use
  - B. **Attach policies to individual user**
  - C. Manage permission by adding users to groups
  - D. Enable MFA on user accounts
12. Which of the following is not correct with respect to IAM user?
- A. IAM user can belong to multiple groups
  - B. IAM user don't have to belong to a group
  - C. IAM user can have policies assigned to them
  - D. **IAM user access AWS with the root account credentials**
13. What are IAM policies?
- A. AWS service performable action
  - B. **JSON document to define user, resource or roles permission**
  - C. Rules to set up password for IAM users
14. You are a developer at a fast growing start up. Until now, you have used the root account to log in to the AWS console. However, as you have taken on more staff, you will now need to stop sharing the root account to prevent accidental damage to your AWS infrastructure. What should you do so that everyone can access the AWS resources they need to do their jobs? (Choose 2)
- A. **Create individual user accounts with minimum necessary rights and tell the staff to log in to the console using the credentials provided.**
  - B. Give your users the root account credentials so that they can also sign in.
  - C. **Create a customized sign in link such as "yourcompany.signin.aws.amazon.com/console" for your new users to use to sign in with.**
  - D. Create an additional AWS root account for each new user.
15. You have a client who is considering a move to AWS. In establishing a new account, what is the first thing the company should do?
- A. Set up an account using Cloud Search.
  - B. Set up an account via SNS (Simple Notification Service)
  - C. Set up an account via SQS (Simple Queue Service).
  - D. **Set up an account using their company email address.**

## Assignment 4 :- Launch your Linux instance in IAM and update your machine.



Command to update machine -> `sudo yum update`

