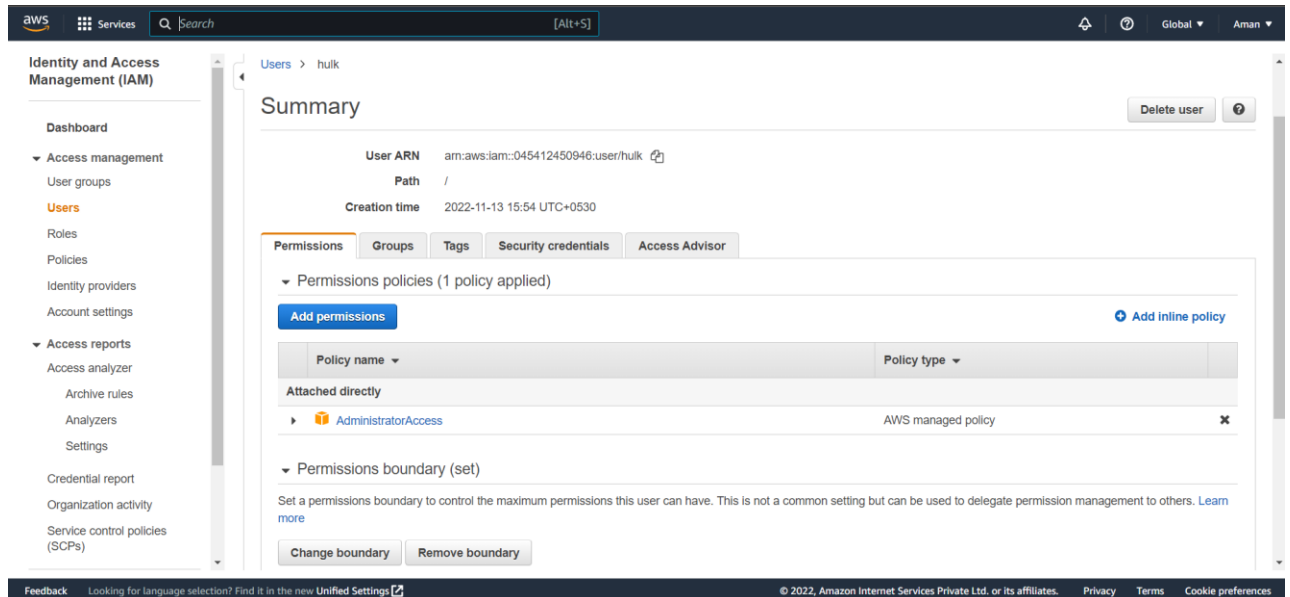


Name: Aman Kumar  
Email id: ang22911@gmail.com

## Assignment 3

Q1: Create an IAM user with username of your own wish and grant administrator policy.

Solution:

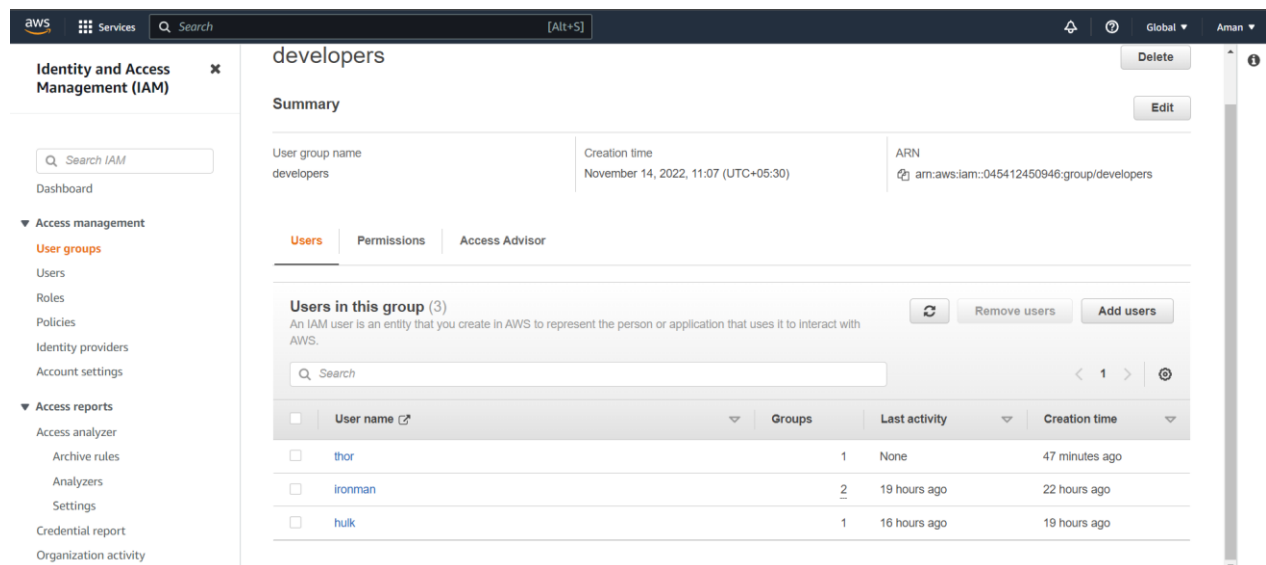


As you can see, in above image I created an **IAM** user named **hulk** and I provided that user **Administrator Access** policy.

Q2: 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.

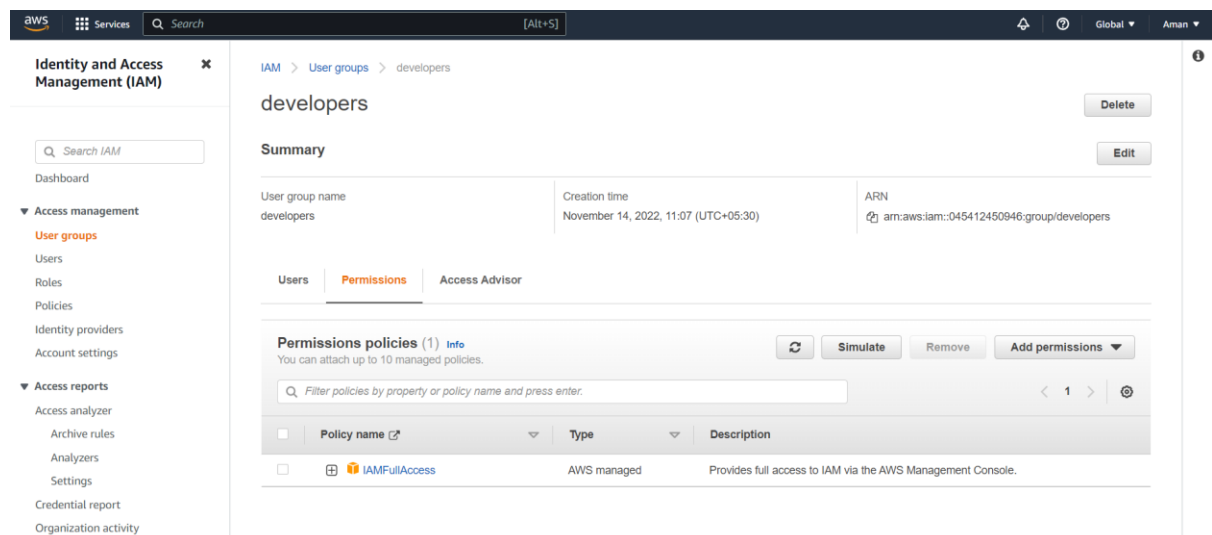
Solution:

Name: Aman Kumar  
Email id: ang22911@gmail.com



The screenshot shows the AWS IAM console interface. On the left is a navigation menu with 'Identity and Access Management (IAM)' selected. The main content area is titled 'developers' and shows a 'Summary' section with details like 'User group name: developers', 'Creation time: November 14, 2022, 11:07 (UTC+05:30)', and 'ARN: arn:aws:iam::045412450946:group/developers'. Below this, the 'Users' tab is active, displaying 'Users in this group (3)'. A table lists the users: 'thor' (1 group, last activity 47 minutes ago), 'ironman' (2 groups, last activity 19 hours ago), and 'hulk' (1 group, last activity 16 hours ago).

I created 3 users and named them hulk, thor, ironman and I also created developers named group. I add those users into that group and gave that group IAM full access policy.

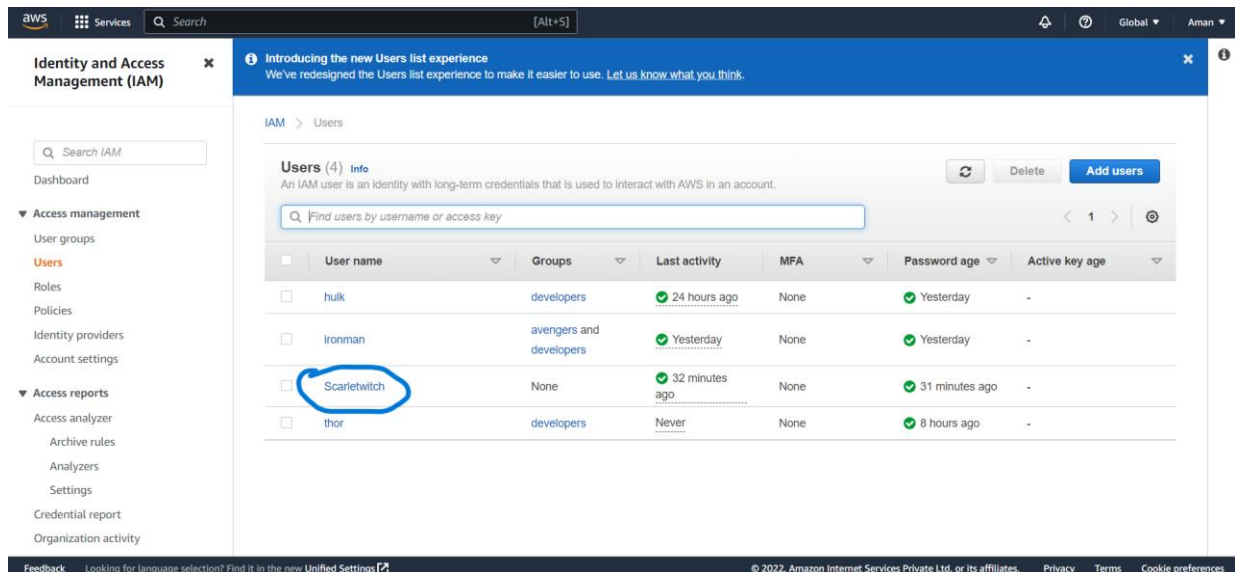


This screenshot shows the 'Permissions' tab for the 'developers' user group. It displays 'Permissions policies (1)' and a table with one policy: 'IAMFullAccess' (AWS managed, provides full access to IAM via the AWS Management Console). The interface includes search bars, filters, and buttons for 'Simulate', 'Remove', and 'Add permissions'.

Q3: 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.

Solution:

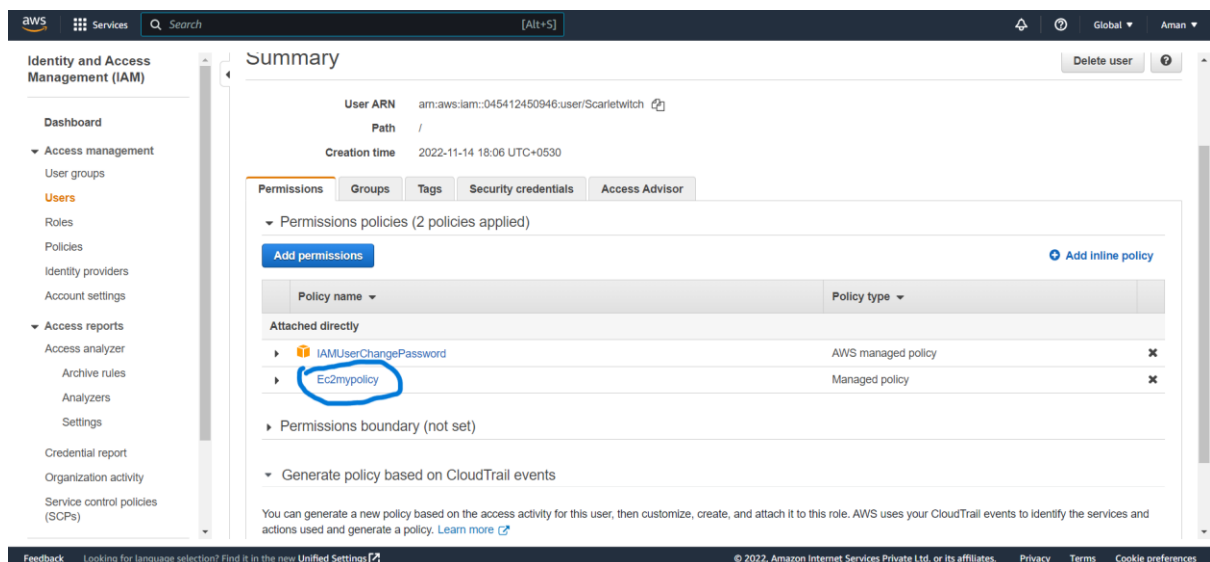
Name: Aman Kumar  
Email id: ang22911@gmail.com



The screenshot shows the AWS IAM console's 'Users' page. A notification banner at the top reads 'Introducing the new Users list experience'. The left sidebar contains navigation links for 'Access management' (User groups, Users, Roles, Policies, Identity providers, Account settings), 'Access reports' (Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity), and 'Dashboard'. The main content area shows a list of 4 users. The 'Scarletwitch' user is circled in blue. Below the list, a 'Summary' tab is selected, showing details for the 'Scarletwitch' user, including their ARN, path, and creation time. The 'Permissions' tab is also visible, showing that two policies are applied: 'IAMUserChangePassword' (AWS managed) and 'Ec2mypolicy' (Managed policy).

	User name	Groups	Last activity	MFA	Password age	Active key age
<input type="checkbox"/>	hulk	developers	24 hours ago	None	Yesterday	-
<input type="checkbox"/>	Ironman	avengers and developers	Yesterday	None	Yesterday	-
<input type="checkbox"/>	Scarletwitch	None	32 minutes ago	None	31 minutes ago	-
<input type="checkbox"/>	thor	developers	Never	None	8 hours ago	-

Here I created a user named Scarletwitch .

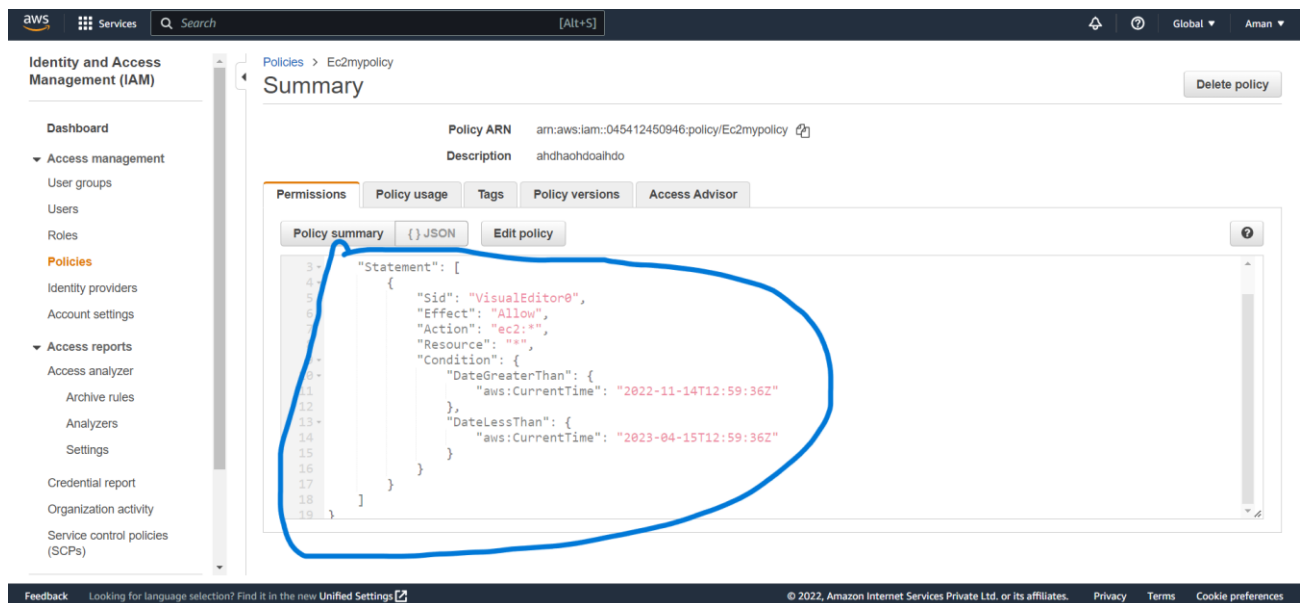


The screenshot shows the 'Summary' page for the 'Scarletwitch' user in the AWS IAM console. The 'Permissions' tab is selected, showing that two policies are applied: 'IAMUserChangePassword' (AWS managed) and 'Ec2mypolicy' (Managed policy). The 'Ec2mypolicy' is circled in blue. The 'Permissions boundary' is set to '(not set)'. The 'Generate policy based on CloudTrail events' section is also visible, with a note that you can generate a new policy based on the access activity for this user.

Policy name	Policy type
IAMUserChangePassword	AWS managed policy
Ec2mypolicy	Managed policy

Here I also created my policy named **Ec2mypolicy**. And I also add the condition of time limit of 4 months.

Name: Aman Kumar  
Email id: ang22911@gmail.com



Q4: - Prepare 15 authentic MCQ questions related to IAM.

Solution:

1) Which of the following is not a component of IAM?

- a. Roles
- b. Users
- c. Which Organizational Units
- d. Group

Ans: b - Organization Units is part of AWS Organization.

2) Which of the following is not a feature of IAM?

- a. IAM allows you to setup biometric authentication, so that no passwords are required.
- b. IAM offers fine-grained access control to AWS resources.
- c. IAM offers centralized control of your AWS account.
- d. IAM integrates with existing active directory account allowing single sign-on.

Ans. a

3) IAM policy access is allowed by default?

- a) True
- b) False

Name: Aman Kumar  
Email id: ang22911@gmail.com

Ans. False (access is denied by default and is allowed only when a policy explicitly grants access.)

4) Why should we use IAM roles?

- a) use IAM roles to grant access to your AWS accounts by relying on short-term credentials, a security best practice
- b) Use IAM roles to use EC2 instance.
- c) Use IAM roles for granting policies to users.

Ans. a

5) Which documents define permission in IAM policy?

- a) XML
- b) JSON
- c) YAML
- d) HTML

Ans. b

6) IAM provides role based access control

- a) True
- b) False

Ans. a

7) A Solutions Architect is designing a shared service for hosting containers from several customers on Amazon ECS. These containers will use several AWS services. A container from one customer should not be able access data from another customer. Which of the below solutions should the architect use to meet these requirements?

- a) IAMroles for tasks
- b) IAMroles for EC2 Instances
- c) IAMInstance profile for EC2 Instances
- d) SecurityGroup rules

Ans. a

8) An EC2 Instance hosts a Java based application that accesses a DynamoDB table. This EC2 Instance is currently serving production users. Which of the following is a secure way for the EC2 Instance to access the DynamoDB table?

- a) UseIAM Roles with permissions to interact with DynamoDB and assign it to the EC2Instance.
- b) UseKMS Keys with the right permissions to interact with DynamoDB and assign it to the EC2 Instance.
- c) UseIAM Access Keys with the right permissions to interact with DynamoDB and assign it to the EC2 Instance.

Name: Aman Kumar  
Email id: ang22911@gmail.com

- d) Use IAM Access Groups with the right permissions to interact with DynamoDB and assign it to the EC2 Instance.

Ans. a - Use IAM Roles with permissions to interact with DynamoDB and assign it to the EC2 Instance

- 9) You have created an AWS Lambda function that will write data to a DynamoDB table. Which of the following must be in place to ensure that the Lambda function can interact with the DynamoDB table?

- a) Ensure an IAM Role is attached to the Lambda function which has the required DynamoDB privileges.
- b) Ensure an IAM User is attached to the Lambda function which has the required DynamoDB privileges.
- c) Ensure the Access keys are embedded in the AWS Lambda function.
- d) Ensure the IAM user password is embedded in the AWS Lambda function.

Ans. a

- 10) You have both production and development based instances running on your VPC. It is required to ensure that people responsible for the development instances do not have access to work on production instances for better security. Which of the following would be the best way to accomplish this using policies? Choose the correct answer from the options given below.

- a) Launch the test and production instances in separate VPCs and use VPC Peering.
- b) Create an IAM Policy with a condition that allows access to only those instances which are used for production or development.
- c) Launch the test and production instances in different Availability Zones and use Multi-Factor Authentication.
- d) Define the tags on the test and production servers and add a condition to the IAM Policy which allows access to specific tags.

Ans. d

- 11) One plans on using SQS queues and AWS Lambda to leverage the serverless aspects of the AWS Cloud. Each invocation to AWS Lambda will send a message to an SQS queue. In order for messages to be sent, which of the following must be in place?

- a) The queue must be a FIFO queue.
- b) An IAM Role with the required permissions.
- c) The code for Lambda must be written in C#.
- d) An IAM Group with the required permissions.

Ans. b

Name: Aman Kumar  
Email id: ang22911@gmail.com

12) Your company is planning on hosting their development, test and production applications on EC2 Instances in AWS. They are worried about how access control would be given to relevant IT Admins for each of the above environments. As an architect, what would you suggest for managing the relevant accesses?

- a) Add tags to the instances marking each environment and then segregate access using IAM Policies.
- b) Add User data to the underlying instances to mark each environment.
- c) Add Metadata to the underlying instances to mark each environment.
- d) Add each environment to a separate Auto Scaling Group.

Ans. a

13) An EC2 Instance setup in AWS will host an application which will make API calls to the Simple Storage Service. What is an ideal way for the application to access the Simple Storage Service?

- a) Pass API credentials to the instance using instance user data.
- b) Store API credentials as an object in a separate Amazon S3 bucket.
- c) Embed the API credentials into your application.
- d) Create and Assign an IAM role to the EC2 Instance.

Ans. d)

14) Your company is planning on using the API Gateway service to manage APIs for developers and users. There is a need to segregate the access rights for both developers and users. How can this be accomplished?

- a) Use IAM permissions to control the access.
- b) Use AWS Access keys to manage the access.
- c) Use AWS KMS service to manage the access.
- d) Use AWS Config Service to control the access.

Ans. a

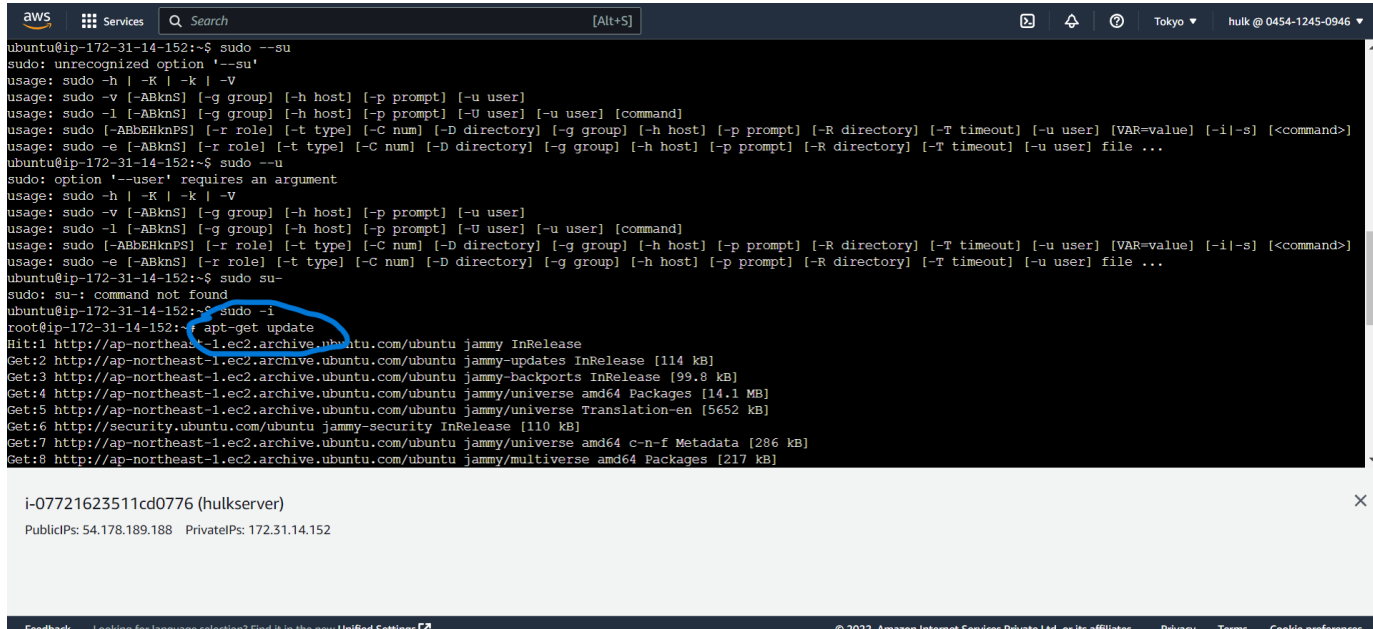
15) You have currently contacted an AWS partner to carry out an audit for your AWS account. You need to ensure that the partner can carry out an audit on your resources. Which one of the following steps would you ideally carry out?

- a) Create an IAM user for the partner account for login purposes
- b) Create a cross account IAM Role
- c) Create an IAM group for the partner account for login purposes
- d) Create an IAM profile for the partner account for login purposes

Ans. b

Name: Aman Kumar  
Email id: ang22911@gmail.com

## Q5: - Launch your linux instance in IAM and update your machine.



```
aws
Services
Search
[Alt+S]
Tokyo
hulk @ 0454-1245-0946

ubuntu@ip-172-31-14-152:~$ sudo --su
sudo: unrecognized option '--su'
usage: sudo -h | -K | -k | -V
usage: sudo -v [-ABkns] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-ABkns] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-ABbEHknps] [-r role] [-t type] [-C num] [-D directory] [-g group] [-h host] [-p prompt] [-R directory] [-T timeout] [-u user] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-ABkns] [-r role] [-t type] [-C num] [-D directory] [-g group] [-h host] [-p prompt] [-R directory] [-T timeout] [-u user] file ...
ubuntu@ip-172-31-14-152:~$ sudo --u
sudo: option '--user' requires an argument
usage: sudo -h | -K | -k | -V
usage: sudo -v [-ABkns] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-ABkns] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-ABbEHknps] [-r role] [-t type] [-C num] [-D directory] [-g group] [-h host] [-p prompt] [-R directory] [-T timeout] [-u user] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-ABkns] [-r role] [-t type] [-C num] [-D directory] [-g group] [-h host] [-p prompt] [-R directory] [-T timeout] [-u user] file ...
ubuntu@ip-172-31-14-152:~$ sudo su-
sudo: su: command not found
ubuntu@ip-172-31-14-152:~$ sudo -i
root@ip-172-31-14-152:~# apt-get update
Hit:1 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease [114 kB]
Get:3 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease [99.8 kB]
Get:4 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 Packages [14.1 MB]
Get:5 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy/universe Translation-en [5652 kB]
Get:6 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:7 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 c-n-f Metadata [286 kB]
Get:8 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse amd64 Packages [217 kB]

i-07721623511cd0776 (hulkserver)
PublicIPs: 54.178.189.188 PrivateIPs: 172.31.14.152

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
```

Above pic you can see I launched a Linux instance on my IAM user and updated my machine.