

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

Users > **test_user**

Summary Delete user

User ARN: am:aws:iam::796732298572:user/test_user
Path: /
Creation time: 2022-11-12 08:44 UTC+0530

Permissions Groups Tags Security credentials Access Advisor

Permissions policies (1 policy applied)

[Add permissions](#) [Add inline policy](#)

Policy name	Policy type
Attached directly	
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.

us-east-1.console.aws.amazon.com/iamv2/home#/groups/details/Developers?section=users

Identity and Access Management (IAM)

Search IAM

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analizers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Related consoles

- IAM Identity Center

Developers Delete

Summary Edit

User group name: Developers
Creation time: November 12, 2022, 09:06 (UTC+05:30)
ARN: am:aws:iam::796732298572:group/Developers

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.

[Refresh](#) [Remove users](#) [Add users](#)

Search

	User name	Groups	Last activity	Creation time
<input type="checkbox"/>	Ironman	1	None	Now
<input type="checkbox"/>	Thor	1	None	Now
<input type="checkbox"/>	spiderman	1	None	2 minutes ago

IAM > User groups > Developers

Developers

Delete

Summary

Edit

User group name	Creation time	ARN
Developers	November 12, 2022, 09:06 (UTC+05:30)	arn:aws:iam::796732298572:group/Developers

Users **Permissions** Access Advisor

Permissions policies (1) [Info](#)

You can attach up to 10 managed policies.

[Refresh](#) [Simulate](#) [Remove](#) [Add permissions](#)

Filter policies by property or policy name and press enter.

< 1 > [Settings](#)

<input type="checkbox"/>	Policy name Info	Type	Description
<input type="checkbox"/>	PowerUserAccess	AWS managed - job function	Provides full access to AWS services and resources, but does not allow management of Users and groups.

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

Users > test_user

Summary

Delete user

?

User ARN [arn:aws:iam::796732298572:user:test_user](#)

Path /

Creation time 2022-11-12 09:14 UTC+0530

Permissions Groups Tags Security credentials Access Advisor


Permissions policies (2 policies applied)

[Add permissions](#)

[Add inline policy](#)

Policy name	Policy type	
Attached directly		
IAMUserChangePassword	AWS managed policy	X
custom	Managed policy	X

Summary

Policy ARN `arn:aws:iam::796732298572:policy/custom` 

Description

Permissions Policy usage Tags Policy versions Access Advisor

Policy summary {} JSON Edit policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "*",
7       "Resource": "*",
8       "Condition": {
9         "DateGreaterThan": {
10          "aws:CurrentTime": "2022-11-12T00:00:00Z"
11        },
12        "DateLessThan": {
13          "aws:CurrentTime": "2023-03-11T23:59:59Z"
14        }
15      }
16    }
17  ]
18 }
```

Assignment 4 :- Prepare 15 authentic MCQ questions related to IAM.

1. Identify the wrong statement.

- (a) Identity and access management (IAM) is a framework for business processes that facilitates the management of electronic or digital identities
- (b) With IAM technologies, IT managers can control user access to critical information within their organizations
- (c) Identity and access management products offer role-based access control
- (d) In IAM roles are defined according to the ability of an individual user to perform a specific task, such as view, create or modify a file**

2. Which of these is Identity in IAM?

- (a) Users
- (b) Groups
- (c) Roles

(d) All of these

3. When you first create an Amazon Web Services (AWS) account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account. This identity is called:

(a) Root user

(b) Main user

(c) Super user

(d) None of these

4. An IAM user:

(a) is an entity that you create in AWS

(b) is to give people the ability to sign in to the AWS Management Console for interactive tasks and to make programmatic requests to AWS services using the API or CLI

(c) A and B both

(d) None of these

5. Choose the below statements are true or false for AWS:

1. When you create an IAM user, you grant it permissions by making it a member of a group that has appropriate permission policies attached (recommended), or by directly attaching policies to the user

2. You can also clone the permissions of an existing IAM user, which automatically makes the new user a member of the same groups and attaches all the same policies.

(a) 1. True, 2. True

(b) 1. True, 2. False

(c) 1. False, 2. True

(d) 1. False, 2. False

6. IAM group:

(a) Is same as IAM users

(b) Can be used to specify permissions for a collection of users

(c) Is truly an identity

(d) All of these

7. Which of these is IAM principal?

- (a) A user
- (b) A role
- (c) An application
- (d) All of these**

8. IAM role:

- (a) Have credentials (password or access keys) associated with it
- (b) Does not have any credentials (password or access keys) associated with it**
- (c) May or may not have credentials (password or access keys) associated with it
- (d) None of these

9. Temporary credentials:

- (a) It expires automatically after a specified time
- (b) Have a same set of permissions that your standard IAM user have
- (c) We can have control over the duration that the credentials are valid
- (d) A and C both**

10. AWS evaluates _____ when an IAM principal makes a request.

- (a) Username and Password
- (b) MAC Address
- (c) Security Policies**
- (d) IP Address

11. Identify the wrong statement.

- (a) IAM can provide shared access to the AWS account
- (b) IAM is paid service in AWS**
- (c) IAM can provide granular permissions
- (d) IAM supports multifactor authentication

12. Names of IAM identities (users, roles, and groups):

- (a) Must be unique within the AWS account**
- (b) Must be unique within the availability zone
- (c) Must be unique within the region
- (d) Must be unique within the AWS cloud whole

13. How many maximum groups can be created in an AWS account?

- (a) 25
- (b) 300**
- (c) 100
- (d) 200

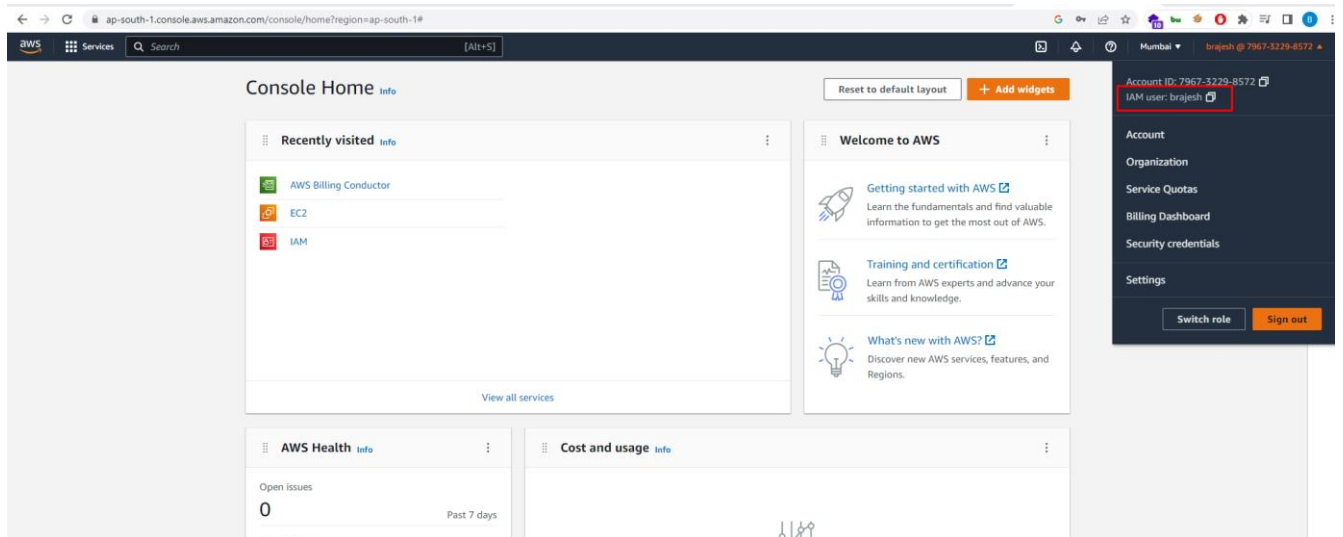
14. An IAM user cannot be a member of more than ___ groups.

- (a) 10**
- (b) 20
- (c) 50
- (d) 100

15. How many maximum managed policies can be assigned to an IAM entity?

- (a) 2
- (b) 5
- (c) 10
- (d) 20**

Assignment 5: - Launch your linux instance in IAM and update your machine



```
root@ip-172-31-8-101:/home/ec2-user
login as: ec2-user
Authenticating with public key "mumbai_ec2"

  _ | _ | _ )
  _ | ( _ | /   Amazon Linux 2 AMI
  _ | \ _ | _ |

https://aws.amazon.com/amazon-linux-2/
18 package(s) needed for security, out of 27 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-8-101 ~]$ su
Password:

aaa
su: Authentication failure
[ec2-user@ip-172-31-8-101 ~]$
[ec2-user@ip-172-31-8-101 ~]$ aaa
-bash: aaa: command not found
[ec2-user@ip-172-31-8-101 ~]$ sudo su
[root@ip-172-31-8-101 ec2-user]#
```

```
Complete:
[root@ip-172-31-8-101 ec2-user]# yum update -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Existing lock /var/run/yum.pid: another copy is running as pid 6567.
Another app is currently holding the yum lock; waiting for it to exit...
  The other application is: yum
    Memory : 171 M RSS (390 MB VSZ)
    Started: Sat Nov 12 05:41:49 2022 - 00:07 ago
    State   : Running, pid: 6567
No packages marked for update
[root@ip-172-31-8-101 ec2-user]#
```