

## Assignment sheet for IAM Assignment

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

### solution

The screenshot shows the AWS IAM console interface. At the top, a green success message states: "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://aws-nuke143.signin.aws.amazon.com/console>". Below this message is a "Download .csv" button. A table lists the created user:

User	Access key ID	Secret access key
monukumar	AKIAUWMCZIWLHCXBCIMB	***** Show

Below the table, a summary box lists the actions performed:

- Created user monukumar
- Attached policy AdministratorAccess to user monukumar
- Created access key for user monukumar

A "Close" button is located at the bottom right of the console window.

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/iam/home#/users\$new?step=final&accessKey&userNames=monukumar&permissionType=policies&policies=arn:aws:iam:...

imp-in imp project airtel Gmail Terraform Best Pr... Kubesimplify Prometheus Expla... learn track Other Bookmarks

aws Services Search [Option+S] Global tripura

Resource Groups & Tag Editor

**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://aws-nuke143.signin.aws.amazon.com/console>

[Download .csv](#)

User	Access key ID	Secret access key
monukumar	AKIAUWMCZIWLHCXBCIMB	***** <a href="#">Show</a>

Created user monukumar

Attached policy AdministratorAccess to user monukumar

Created access key for user monukumar

[Close](#)

### Summary [Edit](#)

User group name avengers	Creation time November 05, 2022, 21:16 (UTC+05:30)	ARN <a href="#">arn:aws:iam::322933704086:group/avengers</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.

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

<input type="checkbox"/>	User name <a href="#">↗</a>	Groups	Last activity	Creation time
<input type="checkbox"/>	dev2	2	None	1 minute ago
<input type="checkbox"/>	dev1	2	None	2 minutes ago
<input type="checkbox"/>	dev3	2	None	1 minute ago

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

```

1  {
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Effect": "Allow",
6        "Action": "service-prefix:action-name",
7        "Resource": "*",
8        "Condition": {
9          "DateGreaterThan": {
10             "aws:CurrentTime": "2020-04-01T00:00:00Z"
11           },
12          "DateLessThan": {
13             "aws:CurrentTime": "2020-08-30T23:59:59Z"
14           }
15        }
16      }
17    ]
18  }

```

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

1. What is IAM?  
Iam is full form of Identity and access management .
2. How to control IAM ?  
Using policy we can control IAM
3. What is cloudtrail in aws  
It is a service recording all the logs of iam users.
4. What are iam hierarchy of principle?  
Root user  
IAM user  
User with temporary credentials
5. What is sts assume role?  
It is use to login into account with temporary credentials.
6. What is identity?  
Entity that can be authenticated.

**7. What are the best practices you would follow while creating any IAM Policy?**

Give least possible priviledges.

**8. Please explain the IAM Policy Structure.**

We can create IAM policies from the AWS web console and by the visual editor using the JASON-based policy editor. If you take a look into the JASON policy document it basically consists of below elements:

- Effect – Decides whether the resource is allowed or denied (Allow/Deny)
- Action – A set of service-specific parameters
- Resource – Resource names

- Condition (Optional) – Grant conditions

### **9What is a Root user?**

The Root User is the Owner Account (administrator) that is created when the AWS Account is created. By default, it has access to all AWS services and resources. It is not possible for IAM Policies to explicitly deny this user access to AWS services or resources.

10

### **How do you revoke access rights?**

If you need to revoke access rights from an existing user, it's simple. Simply click on Manage Permissions on his or her profile page and select Revoke Access. You'll be presented with a list of all services to which they are granted access; check each service that is correct and then click Revoke Access in the bottom right corner.

11

### **What is MFA in AWS IAM?**

Multi-factor authentication (MFA) adds an extra layer of security for users accessing AWS resources. In addition to a username and password, an MFA-enabled user must provide a one-time code generated by an authenticator app or sent via SMS or voice call before gaining access. An MFA device can be enabled on your computer, phone, or tablet.

12

### **What is Access control to AWS resources?**

The first step in securing your resources is using access control lists (ACLs) to allow or deny access. An AWS account has an owner, so you need an access key and secret key when using ACLs with any service. Make sure you keep these keys safe! The first step in securing your resources is using access control lists (ACLs) to allow or deny access. An AWS account has an owner, so you need an access key and secret key when using ACLs with any service.

13.

### **Which are the key features of AWS IAM?**

- Access control to AWS resources
- Multi-factor authentication (MFA)
- Federated access
- Analytics

14

### **Define AWS users and groups.**

IAM users can be people or applications that interact with the AWS environment services and its resources. An IAM user is an identity created in AWS to access various AWS resources and services. A user has permissions associated with it. The permissions define which actions that user can perform on a specific resource.

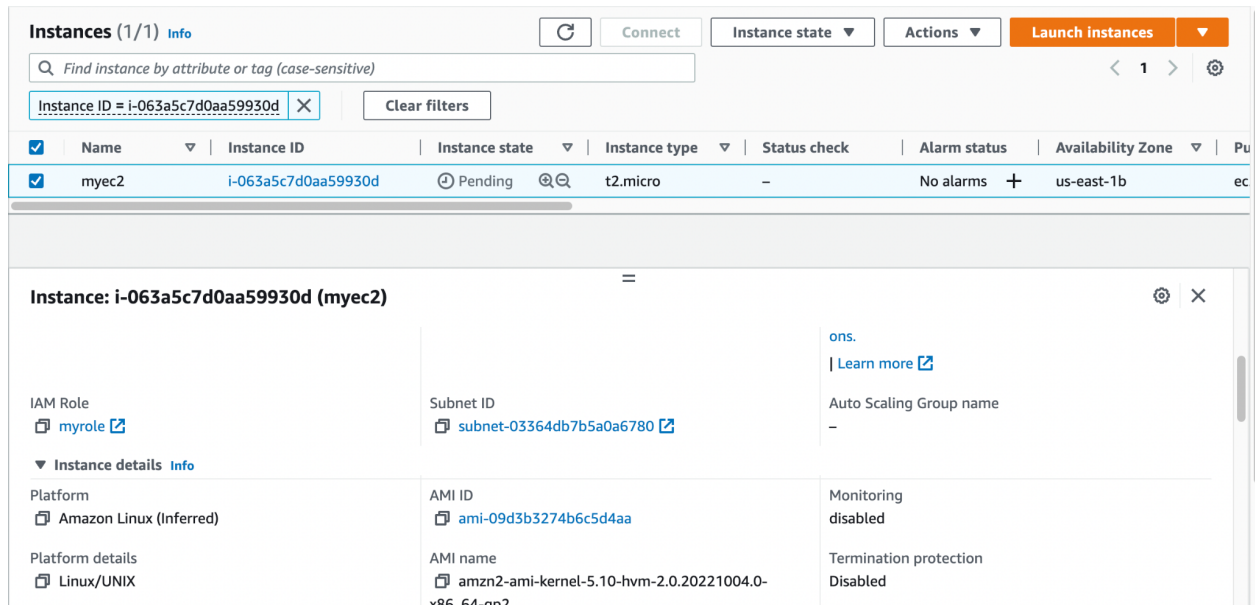
IAM groups are collections of IAM users. Users are organized into groups so you can assign permissions in bulk rather than individually for each user. In addition, permissions are automatically inherited, making it easier to control how resources are accessed within your account. Understand it within [AWS cloud Practitioner](#) course.

15

### What are the best practices you will follow while creating IAM users?

We should always create individual IAM users for each person needing access to AWS services. Even if there are many employees who require the same access, we should create individual IAM users for all of them. This increases the security posture by providing every user of IAM a unique set of credentials.

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



The screenshot displays the AWS Management Console interface for EC2 instances. At the top, there's a search bar and a table of instances. One instance, 'myec2', is listed with ID 'i-063a5c7d0aa59930d' and is in a 'Pending' state. Below the table, the 'Instance details' panel for 'myec2' is expanded, showing various configuration parameters.

Instance: i-063a5c7d0aa59930d (myec2)		
<b>IAM Role</b> myrole	<b>Subnet ID</b> subnet-03364db7b5a0a6780	<b>Auto Scaling Group name</b> -
<b>Platform</b> Amazon Linux (Inferred)	<b>AMI ID</b> ami-09d3b3274b6c5d4aa	<b>Monitoring</b> disabled
<b>Platform details</b> Linux/UNIX	<b>AMI name</b> amzn2-ami-kernel-5.10-hvm-2.0.20221004.0-x86_64-gp2	<b>Termination protection</b> Disabled