



Assignment sheet for IAM.

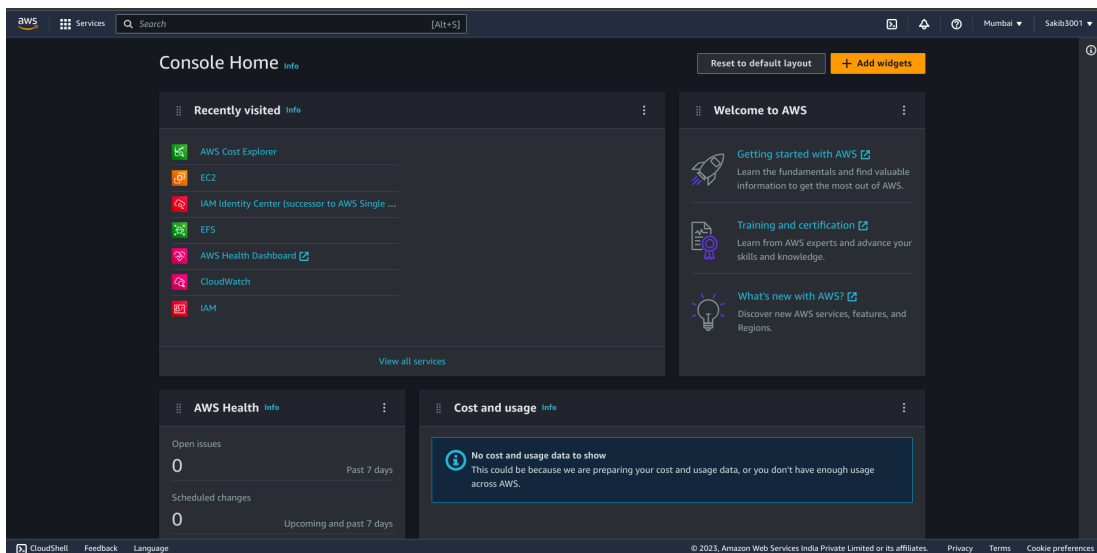
Sakib

NIT Kurukshetra, Haryana
B.Tech in IT (5th Semester)

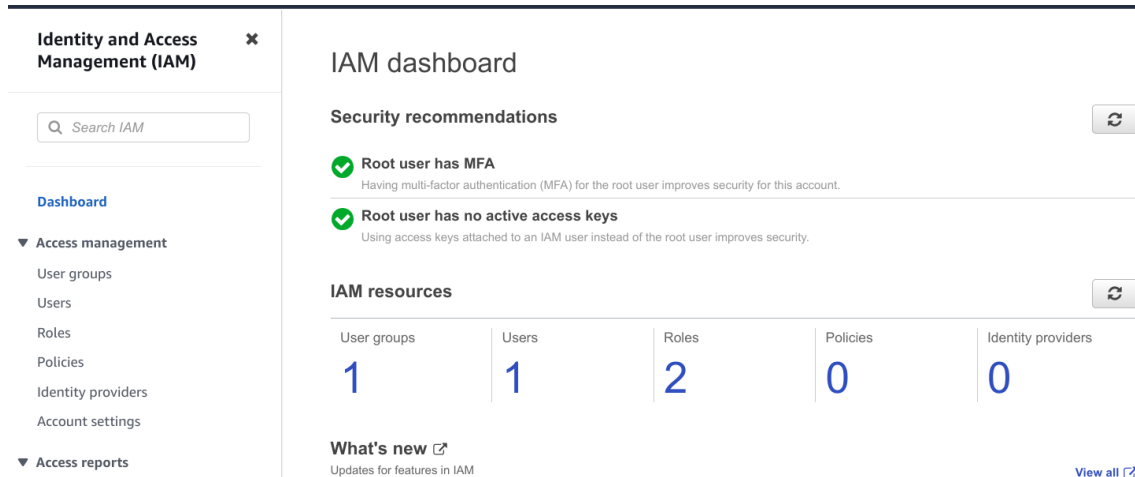
ikasakib1@gmail.com

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

Here I have logged in with my root account.



Now I have gone to the IAM (Identity and Access Management) dashboard.



Here I am creating a user named → Sakib_3001

The screenshot shows the 'Specify user details' step of the AWS IAM 'Create user' process. The user name 'Sakib_3001' is entered. The 'Provide user access to the AWS Management Console - optional' checkbox is checked. A blue box highlights the 'Are you providing console access to a person?' section, where 'I want to create an IAM user' is selected. The 'Console password' section shows 'Autogenerated password' is selected.

Specify user details

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

User details

User name
Sakib_3001
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = . _ - (hyphen)

☒ Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

Are you providing console access to a person?

User type

☐ Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

☒ I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

☒ Autogenerated password
You can view the password after you create the user.

☐ Custom password
Enter a custom password for the user.

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Here the AdministratorAccess policy has been given separately.

The screenshot shows the 'Set permissions' step of the AWS IAM 'Create user' process. The 'Attach policies directly' option is selected. A search for 'Admi' shows 37 matches. The 'AdministratorAccess' policy is selected from the list of results.

Set permissions

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](#)

Permissions options

☐ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

☐ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

☒ Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (Selected 1/1102)

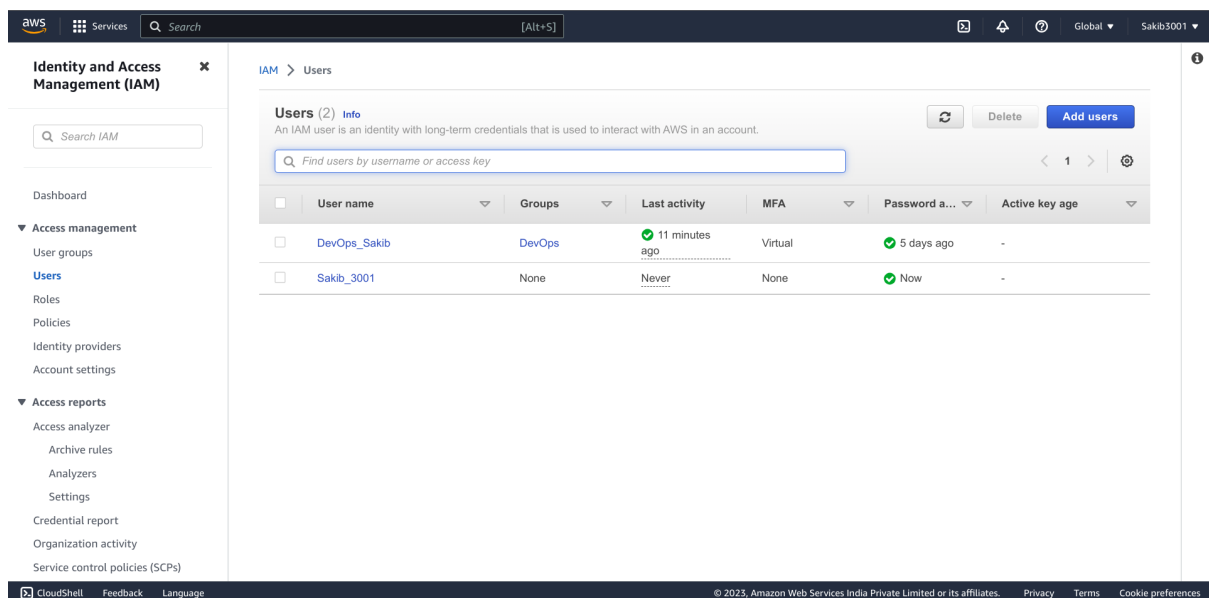
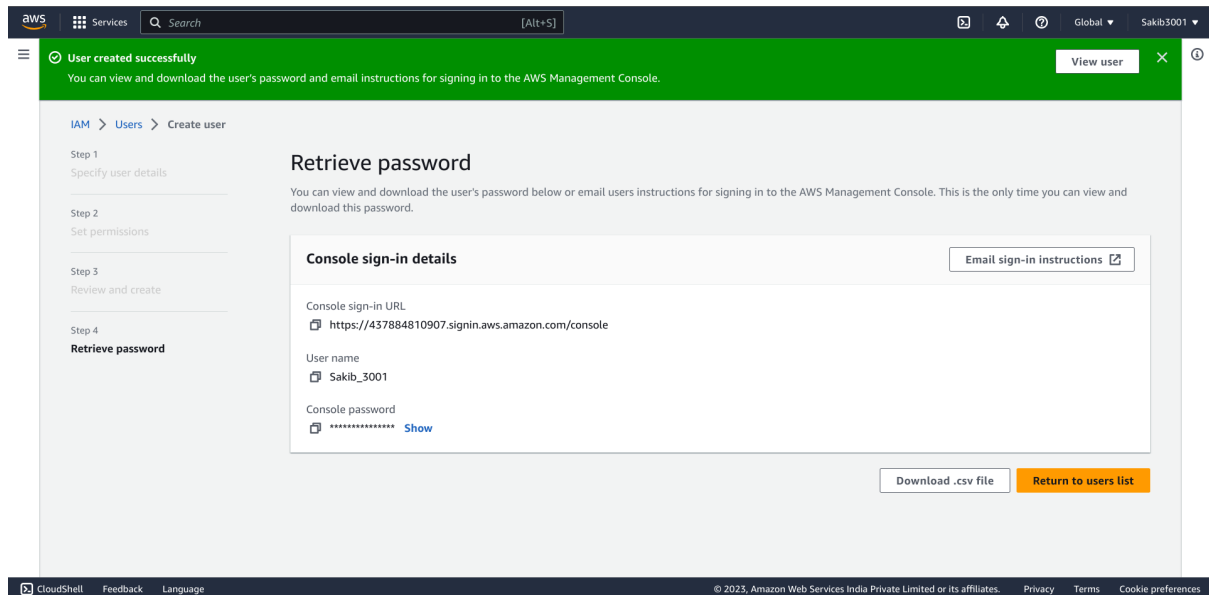
Choose one or more policies to attach to your new user.

Admi 37 matches

Policy name	Type	Attached entities
<input checked="" type="checkbox"/> AdministratorAccess	AWS managed - job function	1
<input type="checkbox"/> AdministratorAccess-Amplify	AWS managed	0
<input type="checkbox"/> AdministratorAccess-AWSElasticBea...	AWS managed	0

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

The user has been created successfully.



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.

A group named → developer_group with AdministratorAccess, IAMReadOnlyAccess, AmazonAppStreamAccess has been added.

The screenshot shows the 'Create user group' page in the AWS IAM console. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and CloudShell. The main content area is titled 'Create user group' and includes a section 'Name the group' with a text input field containing 'Developer_Group'. Below this is a section 'Add users to the group - Optional (1)' with a table listing users. The table has columns for 'User name', 'Groups', 'Last activity', and 'Creation time'. One user, 'DevOps_Sakib', is listed with 1 group, last activity 19 minutes ago, and creation time 5 days ago. At the bottom, there is a section 'Attach permissions policies - Optional (Selected 3/856)' with a 'Create policy' button.

Create user group

Name the group

User group name
Enter a meaningful name to identify this group.

Maximum 128 characters. Use alphanumeric and '*-._@:' characters.

Add users to the group - Optional (1) [Info](#)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user can belong to up to 10 groups.

<input type="checkbox"/>	User name	Groups	Last activity	Creation time
<input type="checkbox"/>	DevOps_Sakib	1	19 minutes ago	5 days ago

Attach permissions policies - Optional (Selected 3/856) [Info](#)

[Create policy](#)

The screenshot shows the 'Developer_Group' page in the AWS IAM console. The left sidebar is the same as the previous screenshot. The main content area is titled 'Developer_Group' and includes a 'Summary' section with a table showing 'User group name', 'Creation time', and 'ARN'. Below this is a section 'Permissions policies (3)' with a table listing policies. The table has columns for 'Policy name', 'Type', and 'Description'. Three policies are listed: 'AdministratorAccess', 'AmazonAppStreamFullAccess', and 'IAMReadOnlyAccess'. The 'Permissions' tab is selected, and there are buttons for 'Simulate', 'Remove', and 'Add permissions'.

Developer_Group [Delete](#) [Edit](#)

Summary

User group name	Creation time	ARN
Developer_Group	June 17, 2023, 11:10 (UTC+06:00)	arn:aws:iam::437884810907:group/Developer_Group

Permissions policies (3) [Info](#)

You can attach up to 10 managed policies.

[Filter policies by property or policy name and press enter.](#)

<input type="checkbox"/>	Policy name	Type	Description
<input type="checkbox"/>	AdministratorAccess	AWS managed - job function	Provides full access to AWS services and resources.
<input type="checkbox"/>	AmazonAppStreamFullAccess	AWS managed	Provides full access to Amazon AppStream via the AWS Management Console.
<input type="checkbox"/>	IAMReadOnlyAccess	AWS managed	Provides read only access to IAM via the AWS Management Console.

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

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": "s3:GetObject",  
7       "Resource": "arn:aws:s3::sakib-3001-bucket/*",  
8       "Condition": {  
9         "DateGreaterThan": {  
10          "aws:CurrentTime": "2023-01-01T00:00:00Z"  
11        },  
12        "DateLessThan": {  
13          "aws:CurrentTime": "2023-04-30T23:59:59Z"  
14        }  
15      }  
16    ]  
17 }  
18 }  
19 }
```

The policy has been created named ExpirationPolicy:

The screenshot displays the AWS IAM console interface. On the left is a navigation sidebar with sections for 'Identity and Access Management (IAM)', 'Access management', 'Access reports', and 'Service control policies (SCPs)'. The main content area is titled 'IAM > Policies > ExpirationPolicy'. Below the title is a 'Delete' button. The 'Policy details' section shows the policy is 'Customer managed', created on 'June 19, 2023, 08:43 (UTC+06:00)', and edited on 'June 19, 2023, 08:45 (UTC+06:00)'. The ARN is 'arn:aws:iam::437884810907:policy/ExpirationPolicy'. Below this is a tabbed interface with 'Permissions' selected. The 'Permissions defined in this policy' section shows the JSON policy document, which is identical to the one provided in the assignment. At the bottom of the console, there is a footer with 'CloudShell', 'Feedback', 'Language', and copyright information for Amazon Web Services India Private Limited.

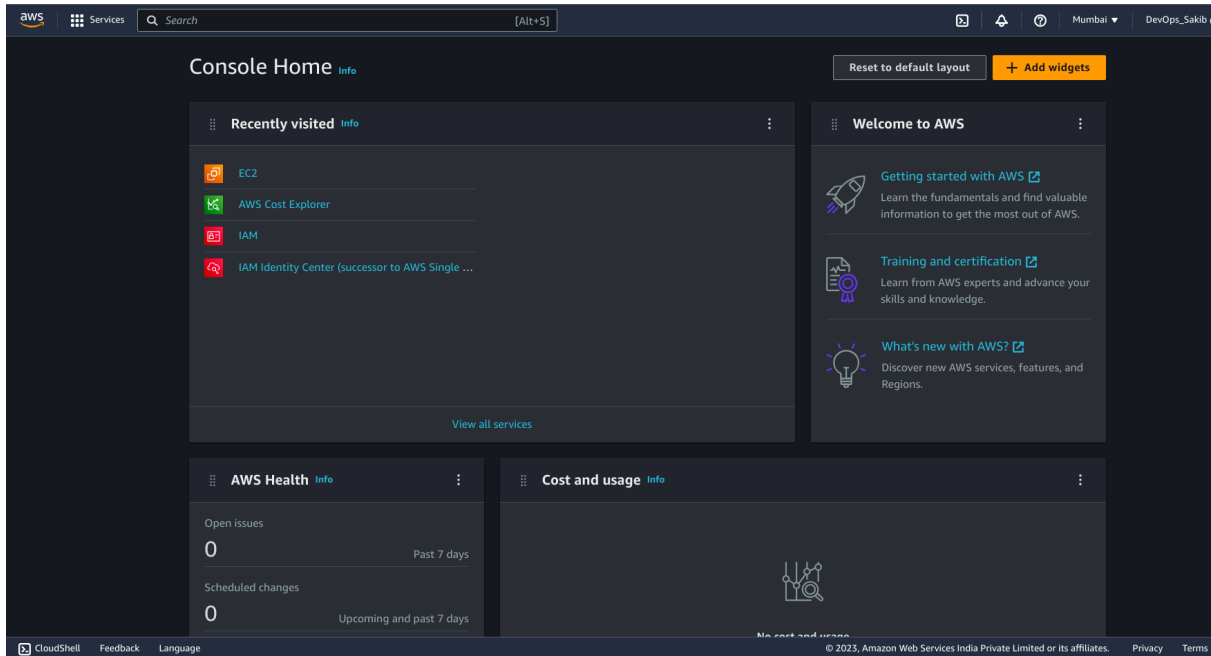
15 MCQ questions related to IAM

1. Which AWS service is used for identity and access management?
 - a) S3
 - b) EC2
 - c) IAM
 - d) RDS
2. Which of the following statements best describes IAM roles?
 - a) IAM roles are used to assign permissions to AWS services.
 - b) IAM roles are used to grant permissions to IAM users.
 - c) IAM roles are used to manage access keys for IAM users.
 - d) IAM roles are used to enable multi-factor authentication for IAM users.
3. What is the maximum number of IAM users that can be created per AWS account by default?
 - a) 5
 - b) 10
 - c) 20
 - d) There is no default limit.
4. Which of the following actions can be performed using IAM policies?
 - a) Grant permissions to IAM users and groups.
 - b) Assign AWS resource tags to IAM users.
 - c) Manage access keys for IAM users.
 - d) Create and manage IAM roles.
5. Which statement best describes IAM groups in AWS?
 - a) IAM groups are used to manage IAM users.
 - b) IAM groups are used to manage IAM policies.
 - c) IAM groups are used to manage AWS resources.
 - d) IAM groups are used to manage access keys.
6. What is the purpose of an IAM policy simulator in AWS?
 - a) To simulate the performance of IAM roles.
 - b) To simulate the cost of IAM policies.
 - c) To simulate the effects of IAM policies.
 - d) To simulate the access key rotation for IAM users.
7. Which of the following authentication methods is supported by IAM?
 - a) Username and password
 - b) Access key and secret key
 - c) Biometric authentication
 - d) SMS-based one-time password (OTP)

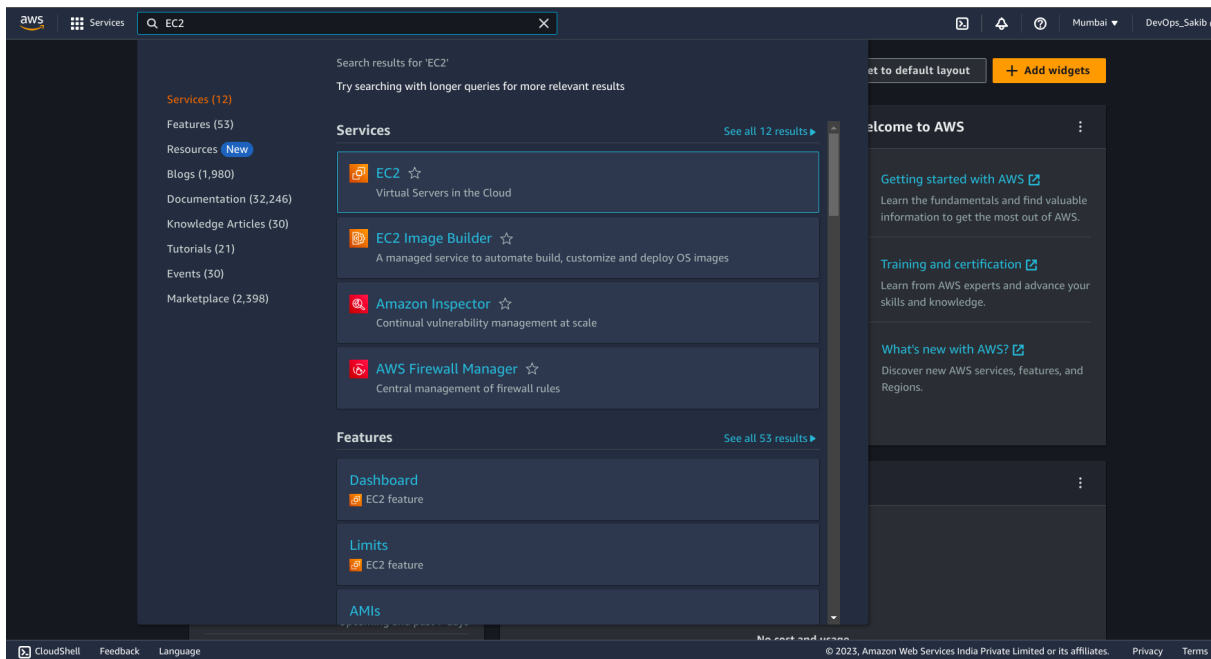
8. Which of the following is NOT a valid IAM permission boundary?
- a) Allow
 - b) Deny
 - c) Pass
 - d) Condition
9. Which of the following statements is true about IAM roles?
- a) IAM roles can be associated with multiple users.
 - b) IAM roles are only used for temporary access.
 - c) IAM roles can be used across AWS accounts.
 - d) IAM roles have access keys and secret keys.
10. Which AWS service can be used to audit and monitor IAM events?
- a) AWS CloudFormation
 - b) AWS Config
 - c) AWS CloudTrail
 - d) AWS CloudWatch
11. What is the purpose of an IAM policy condition in AWS?
- a) To define the actions that can be performed by an IAM user.
 - b) To specify the resources that can be accessed by an IAM user.
 - c) To define the context in which an IAM policy is evaluated.
 - d) To specify the time period during which an IAM policy is valid.
12. Which of the following AWS resources can be assigned tags?
- a) IAM users
 - b) IAM policies
 - c) IAM roles
 - d) All of the above
13. Which of the following is NOT a valid IAM policy element?
- a) Statement
 - b) Action
 - c) Resource
 - d) Condition
14. What is the purpose of an IAM instance profile?
- a) To manage IAM roles for EC2 instances.
 - b) To manage IAM users for EC2 instances.
 - c) To manage access keys for EC2 instances
 - d) To manage permissions for EC2 instances.
15. What is the purpose of an IAM access key?
- a) To authenticate IAM users.
 - b) To encrypt IAM policies.
 - c) To grant temporary access to IAM users.
 - d) To generate IAM user names.

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

I have logged in as an IAM user account but not as a root account.



Searching for the EC2 service



Here an instance named My_Ubuntu_One is going to be created:

Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Name: My_Ubuntu_One

Application and OS Images (Amazon Machine Image)

Canonical, Ubuntu, 22.04 LTS

Instance type

t2.micro

Key pair (login)

New security group

Summary

Number of instances: 1

Software Image (AMI): Canonical, Ubuntu, 22.04 LTS

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage.

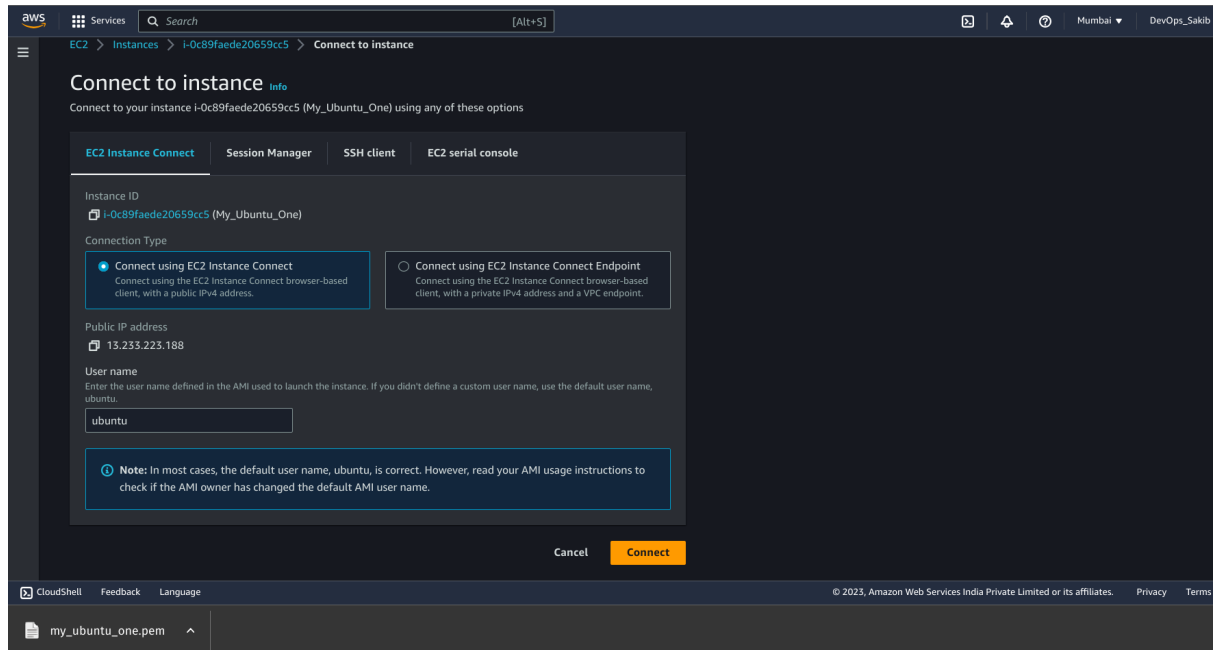
[Launch instance](#)

The instance has been created successfully and it is in running state:

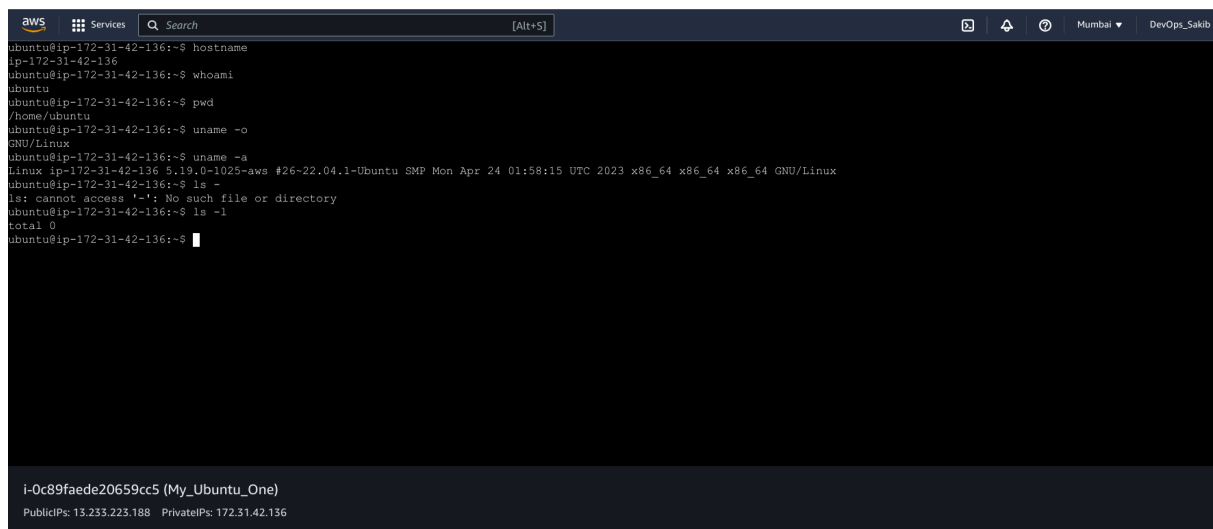
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
My_Ubuntu_One	i-0c89faede20659cc5	Running	t2.micro	Initializing	No alarms	ap-south-1a	ec2-13-233-223-188.ap-south-1.amazonaws.com

Instance: i-0c89faede20659cc5 (My_Ubuntu_One)

Now the running instance has been connected via EC2 instance connect:



The instance has been successfully connected and the terminal appears on the browser window:



Sudo apt update → has been given for update the instance.

```
aws
Services Search [Alt+S]
Mumbai DevOps_Sakib
ubuntu@ip-172-31-42-136:~$ sudo apt update
i-0c89faede20659cc5 (My_Ubuntu_One)
PublicIPs: 13.233.223.188 PrivateIPs: 172.31.42.136
```

The updation of EC2 instance machine has been done successfully:

```
aws
Services Search [Alt+S]
Mumbai DevOps_Sakib
Get:16 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [63.8 kB]
Get:17 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [927 kB]
Get:18 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [197 kB]
Get:19 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 c-n-f Metadata [20.4 kB]
Get:20 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 Packages [35.3 kB]
Get:21 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse Translation-en [8452 B]
Get:22 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 c-n-f Metadata [468 B]
Get:23 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main amd64 Packages [40.9 kB]
Get:24 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main Translation-en [10.2 kB]
Get:25 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main amd64 c-n-f Metadata [388 B]
Get:26 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/restricted amd64 c-n-f Metadata [116 B]
Get:27 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 Packages [23.4 kB]
Get:28 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe Translation-en [15.0 kB]
Get:29 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 c-n-f Metadata [548 B]
Get:30 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/multiverse amd64 c-n-f Metadata [116 B]
Get:31 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [129 kB]
Get:32 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c-n-f Metadata [10.3 kB]
Get:33 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [415 kB]
Get:34 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [63.3 kB]
Get:35 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [737 kB]
Get:36 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [130 kB]
Get:37 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 c-n-f Metadata [15.6 kB]
Get:38 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 Packages [30.2 kB]
Get:39 http://security.ubuntu.com/ubuntu jammy-security/multiverse Translation-en [5828 B]
Get:40 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 c-n-f Metadata [252 B]
Fetched 25.4 MB in 5s (4898 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
66 packages can be upgraded. Run 'apt list --upgradable' to see them.
ubuntu@ip-172-31-42-136:~$
i-0c89faede20659cc5 (My_Ubuntu_One)
PublicIPs: 13.233.223.188 PrivateIPs: 172.31.42.136
```

End of Assignment

