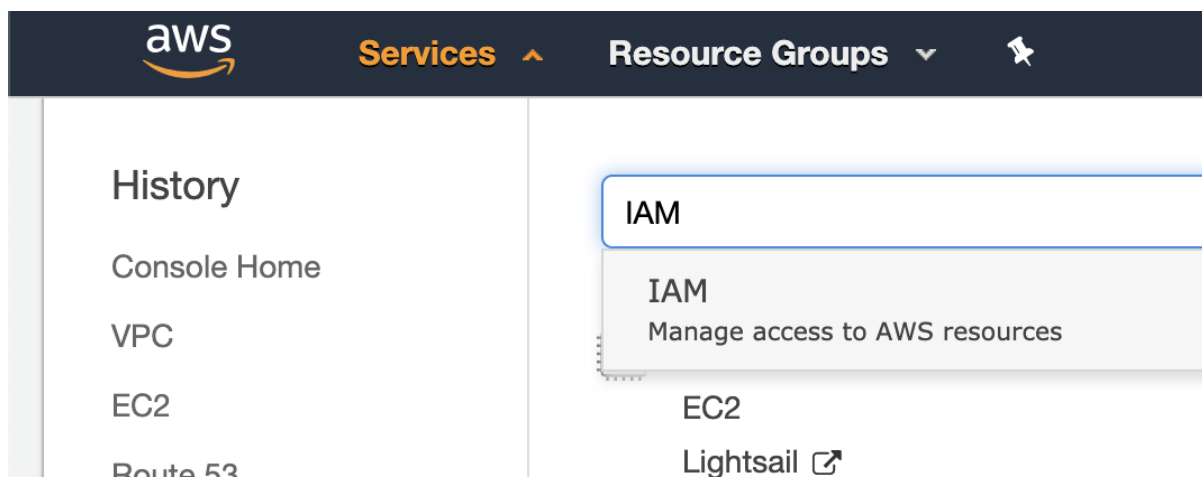


Assignment sheet for IAM

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

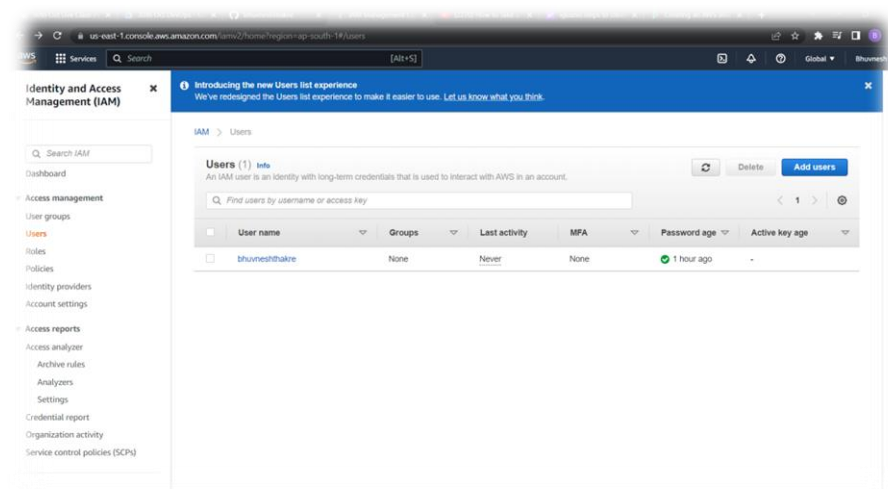
Step 1: AWS Login

Log into your AWS Management Console and select the IAM service.



Step 2: Create a New User

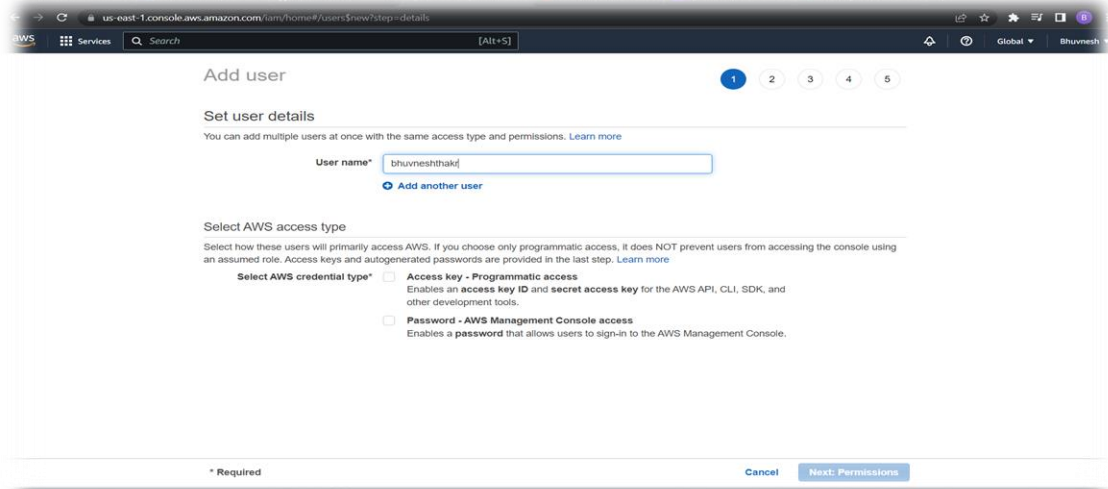
In the side navigation menu, select Access management | Users, and then select Add user.



Step 3: Set the User's Access Permissions and Name

In the Set user details section,

- In the User name field, enter the name of the new user (for example, "bhuvnesh" — recommended).
- In the Access type field, check the Programmatic access option to allow the user only programmatic access.

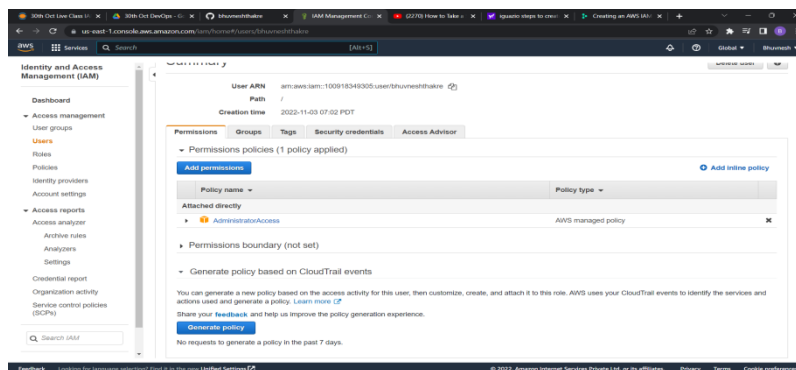


The screenshot shows the AWS IAM 'Add user' console. The 'Set user details' section is active, showing the 'User name' field with the value 'bhuvneshthakur'. Below this, the 'Select AWS access type' section is visible, with the 'Access key - Programmatic access' option selected. The 'Next: Permissions' button is located at the bottom right of the form.

When you're done, select Next: Permissions.

Step 4: Create a Policy

Select Attach existing policies directly, and then select Create policy.



The screenshot shows the AWS IAM console's 'Permissions' section for a user. The 'Attach existing policies directly' option is selected, and the 'AdministratorAccess' policy is attached. The 'Create policy' button is visible at the bottom.

Step 5: Create the User

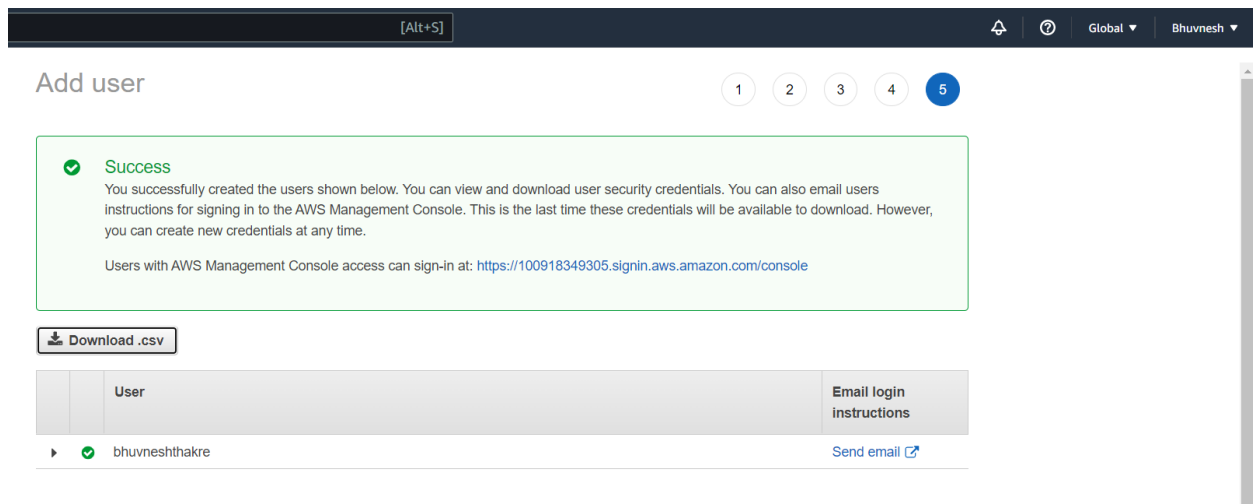
Filter the policies for the name of the policy that you created and select the policy.

Select Next: Tags and optionally assign user tags.

Select Next: Review and review your role definition. When you're ready, select Create user.

Step 6: Save the User Credential

Download and save the credentials of the new user (Access key iD and Secret access key).



The screenshot shows the AWS IAM console 'Add user' page. At the top, there's a navigation bar with '[Alt+S]', a bell icon, a question mark icon, 'Global', and 'Bhuvnesh'. Below the navigation bar, the page title 'Add user' is followed by a progress indicator with five steps, where step 5 is highlighted. A green success message box 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://100918349305.signin.aws.amazon.com/console>'. Below the message is a 'Download .csv' button. A table lists the created users, with one user 'bhuvneshthakre' shown. The table has columns for 'User' and 'Email login instructions'. A 'Send email' link is next to the user name.

User	Email login instructions
▶ bhuvneshthakre	Send email

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.

Step 1: Create 3 New User

Add user 1 2 3 4 5

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

avengers1

avengers2

avengers3

[Add another user](#)

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Select AWS credential type*

☐ **Access key - Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☒ **Password - AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password*

☐ Autogenerated password

☒ Custom password

* Required

[Cancel](#) [Next: Permissions](#)

[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](#)

Step 2: Set the User's Access Permissions and Name

Here, you could directly **Add an user to a group** or could **copy permissions from existing user** or could **attach existing policies directly**.

You could directly create groups and assign permissions here. This is more useful while creating a Single user. Lets follow the topic order and create user now. We would create group in next section of this article.

Add user 1 2 3 4 5

Set permissions

[Add users to group](#) [Copy permissions from existing user](#) [Attach existing policies directly](#)

Add users to an existing group or create a new one. Using groups is a best-practice way to manage users' permissions by job functions. [Learn more](#)

Add user to group

[Create group](#) [Refresh](#)

Search Showing 2 results

Group	Attached policies
<input type="checkbox"/> Avengers	None
<input type="checkbox"/> developersteam	AdministratorAccess

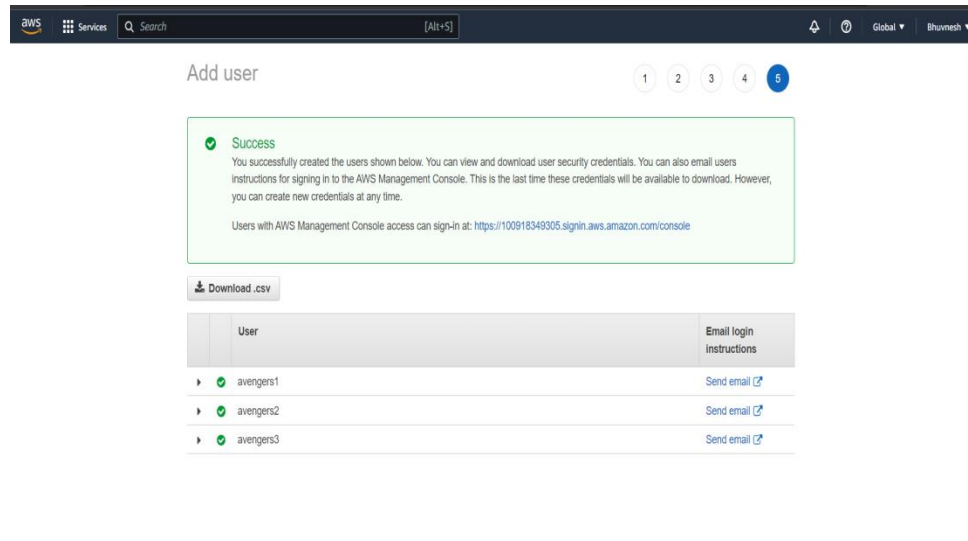
Set permissions boundary

[Cancel](#) [Previous](#) [Next: Tags](#)

[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](#)

Step 3: Save the User Credential



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



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

1. 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

2. 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 tothe EC2 Instance.

C. UseIAM Access Keys with the right permissions to interact with DynamoDB and assignit to the EC2 Instance.

D. UseIAM Access Groups with the right permissions to interact with DynamoDB andassign it to the EC2 Instance.

3.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.

4. 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.

5. Your application consists of a set of EC2 Instances which are spun up as part of an Autoscaling Group. These Instances need to access objects in an S3 bucket. Which of the following is the ideal approach to ensure this access is set in place?

A. Ensure that the Access Keys are picked up from another S3 bucket. The Access Keys can be embedded in the User data during Instance Launch.

B. Ensure that the Autoscaling Group attaches an IAM Role attached to the underlying EC2 Instances.

C. Ensure that an IAM policy is attached to the S3 bucket which allows access to the S3 buckets.

D. Ensure that the Autoscaling Group attaches an IAM User attached to the underlying EC2 Instances.

6. Which of the following is not a feature of AWS Security Token Service?

A. STS enables you to request temporary, limited-privilege credentials.

B. STS enables users to assume role.

C. STS generates Git Credentials for IAM users.

D. STS generates Federated Credentials for IAM users.

7. You are deploying an application on Amazon EC2, which must call AWS APIs. What method should you use to securely pass credentials to the application?

A. PassAPI credentials to the instance using Instance userdata.

B. StoreAPI credentials as an object in Amazon S3.

C. Embedthe API credentials into your application.

D. AssignIAM roles to the EC2 Instances.

8. You are developing a mobile application that needs to issue temporary security credentials to users. This is essential due to security concerns. Which of the below services can help achieve this?

A. AWS STS

B. AWS Config

C. AWS Trusted Advisor

D. AWS Inspector

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 DynamoDBprivileges.

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.

10. 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

11. Your organization has an AWS setup and planning to build Single Sign On for users to authenticate with on-premise Microsoft Active Directory Federation Services (ADFS) and let users login to AWS console using AWS STS Enterprise Identity Federation. Which of the following service you need to call from AWS STS service after you authenticate with your on-premise?

- A. **AssumeRoleWithSAML**
- B. GetFederationToken
- C. AssumeRoleWithWebIdentity
- D. GetCallerIdentity

12. Your application consists of a set of EC2 Instances which are spun up as part of an Autoscaling Group. These Instances need to access objects in an S3 bucket. Which of the following is the ideal approach to ensure this access is set in place?

- A. Ensure that the Access Keys are picked up from another S3 bucket. The Access Keys can be embedded in the User data during Instance Launch.

B. Ensure that the Autoscaling Group attaches an IAM Role attached to the underlying EC2 Instances.

C. Ensure that an IAM policy is attached to the S3 bucket which allows access to the S3 buckets.

D. Ensure that the Autoscaling Group attaches an IAM User attached to the underlying EC2 Instances.

13. what are IAM policies written in?

A. YAML

B. XML

C. JSON

D. simple text

14. what is the best way to protect your root account?

A. user name and password

B. Multi factor authentication (MFA)

C. AWS access key

D. Temporary security credentials

15. 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.

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

```
aws
Services
Search
[Alt+S]
Tokyo
bhuvneshthakre @ 1009-1834-9305

Get:16 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 c-n-f Metadata [544 B]
Get:17 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [743 kB]
Get:18 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [122 kB]
Get:19 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 c-n-f Metadata [4404 B]
Get:20 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 Packages [13.7 kB]
Get:21 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse Translation-en [4228 B]
Get:22 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 c-n-f Metadata [420 B]
Get:23 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main amd64 Packages [3008 B]
Get:24 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main Translation-en [1432 B]
Get:25 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main amd64 c-n-f Metadata [272 B]
Get:26 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/restricted amd64 c-n-f Metadata [116 B]
Get:27 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 Packages [6748 B]
Get:28 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe Translation-en [9360 B]
Get:29 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 c-n-f Metadata [352 B]
Get:30 http://ap-northeast-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 amd64 Packages [461 kB]
Get:32 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [101 kB]
Get:33 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [372 kB]
Get:34 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [57.4 kB]
Get:35 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [602 kB]
Get:36 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [76.6 kB]
Get:37 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 c-n-f Metadata [2408 B]
Get:38 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 Packages [4192 B]
Get:39 http://security.ubuntu.com/ubuntu jammy-security/multiverse Translation-en [900 B]
Get:40 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 c-n-f Metadata [228 B]
Fetched 24.6 MB in 4s (6399 KB/s)
```

i-015a40e7195c0d250 (devopspro)

PublicIPs: 18.183.129.154 PrivateIPs: 172.31.0.140

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

