

# IAM(Identity and Access Management)

1) Create one IAM user and assign ec2,s3 full access role.

The top screenshot shows the AWS Management Console EC2 Dashboard. A blue notification bar at the top states: "You can change your default landing page for EC2. Permanently dismiss Change landing page". The left sidebar shows the navigation menu with "Instances" and "Images" expanded. The main content area displays "Resources" for the Europe (Stockholm) Region, listing various EC2 resources and their counts:

Resource	Count
Instances (running)	0
Capacity Reservations	0
Elastic IPs	0
Key pairs	0
Placement groups	0
Snapshots	0
Auto Scaling Groups	0
Dedicated Hosts	0
Instances	0
Load balancers	0
Security groups	2
Volumes	0

The right sidebar shows "Account attributes" including the Default VPC (vpc-0f3f1d4f183b330fa) and various settings like Data protection and security, Allowed AMIs, Zones, EC2 Serial Console, Default credit specification, and EC2 console preferences.

The bottom screenshot shows the Amazon S3 Buckets page. A green notification bar at the top states: "Successfully created bucket 'oman8008'. To upload files and folders, or to configure additional bucket settings, choose View details." The page shows a table of General purpose buckets with one bucket listed:

Name	AWS Region	Creation date
oman8008	Europe (Stockholm) eu-north-1	August 1, 2025, 14:38:48 (UTC+05:30)

The right sidebar shows "Account snapshot" and "External access summary - new" sections.

2) Create one Group in IAM and Assign Read access for ec2.

The screenshot shows the AWS IAM console interface. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, User groups, Users, Roles, Policies, Identity providers, Account settings, and Root access management. The main content area is titled 'Summary' for the user group 'dev'. It shows the creation time as 'August 01, 2025, 14:41 (UTC+05:30)' and the ARN as 'arn:aws:iam::211125448409:group/dev'. Below the summary, the 'Permissions' tab is selected, showing 'Permissions policies (1)'. A table lists the attached policies:

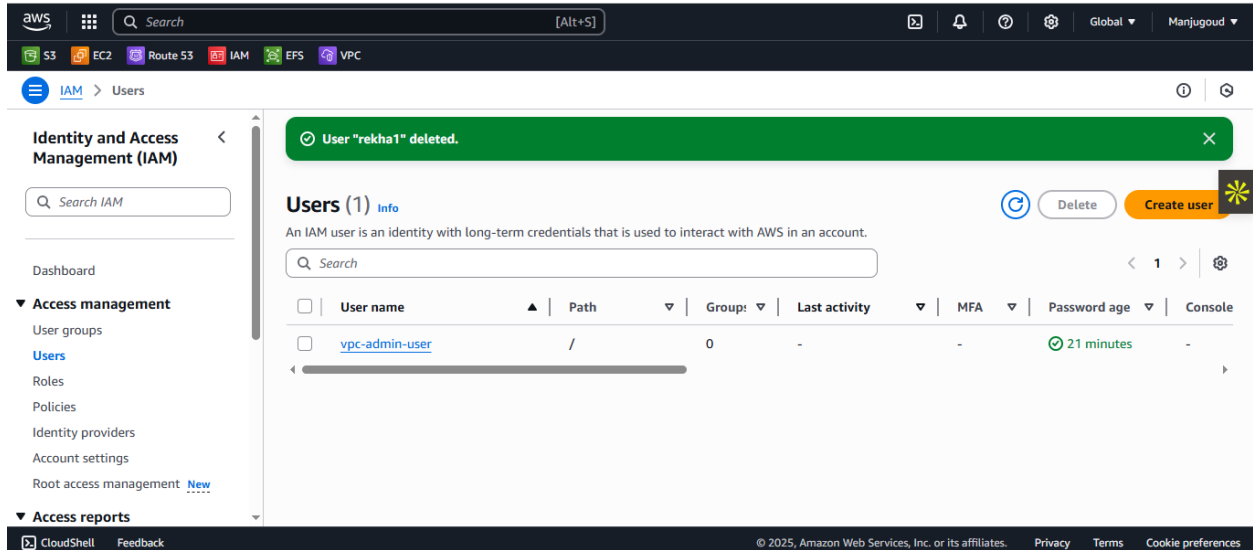
Policy name	Type	Attached entities
AmazonEC2ReadOnlyAccess	AWS managed	1

3) Create a new user with name Devops and add to the group created in task2.

The screenshot shows the AWS IAM console interface, now displaying the 'Users' tab for the user group 'dev'. It shows the creation time as 'August 01, 2025, 14:41 (UTC+05:30)' and the ARN as 'arn:aws:iam::211125448409:group/dev'. Below the summary, the 'Users' tab is selected, showing 'Users in this group (1)'. A table lists the users in the group:

User name	Groups	Last activity	Creation time
devops	1	None	Now

4) Write a bash script to create a IAM user with VPC full access.



```
#!/bin/bash
```

```
USER_NAME="vpc-admin-user"
```

```
POLICY_ARN="arn:aws:iam::aws:policy/AmazonVPCFullAccess"
```

```
echo "Creating IAM user: $USER_NAME" aws iam create-user --user-name "$USER_NAME"
```

```
echo "Attaching VPC full access policy to user: $USER_NAME" aws iam attach-user-policy  
--user-name "$USER_NAME" --policy-arn "$POLICY_ARN"
```

```
echo "Setting password for console login (optional)" aws iam create-login-profile
```

```
--user-name "$USER_NAME"
```

```
--password 'Welcome@123'
```

```
--password-reset-required
```

```
echo "Creating access keys for user: $USER_NAME" aws iam create-access-key --user-  
name "$USER_NAME"
```

```
echo "IAM user '$USER_NAME' created and VPC full access policy attached."
```

Here we need to create an IAM user using AWS CLI.

5) Create a IAM policy to access ec2 for a specific user in specific regions only.

**Policy ec2policy created.**

**Permissions policies (2)**

Permissions are defined by policies attached to the user directly or through groups.

Policy name	Type	Attached via
ec2policy	Customer inline	Inline
IAMUserChangePassword	AWS managed	Directly

**You can change your default landing page for EC2.**

**Resources**

You are using the following Amazon EC2 resources in the Europe (Stockholm) Region:

Resource	Count
Instances (running)	0
Capacity Reservations	0
Elastic IPs	0
Key pairs	0
Placement groups	0
Snapshots	0
Auto Scaling Groups	API Error
Dedicated Hosts	0
Instances	0
Load balancers	API Error
Security groups	3
Volumes	0

**Account attributes**

**Default VPC**  
vpc-0f3f1d4f183b330fa

**Settings**

- Data protection and security
- Allowed AMIs
- Zones
- EC2 Serial Console
- Default credit specification
- EC2 console preferences

**Explore AWS**

6) We have two accounts Account A and Account B, Account A user should access s3 bucket in Account B. (Collaborate with team member and execute this. Mostly asked in every interview)

aws

Search

[Alt+S]

Europe (Stockholm)

accountA @ network-alias-manjunath

EC2 > Instances > i-077ff8e7f917e373b > Connect to instance

Connect Info

Connect to an instance using the browser-based client.

EC2 Instance Connect

Session Manager

SSH client

EC2 s

Instance ID

i-077ff8e7f917e373b (accA)

1. Open an SSH client.

2. Locate your private key file. The key used to launch this instance is acc.pem

3. Run this command, if necessary, to ensure your key is not publicly viewable.  
chmod 400 "acc.pem"

4. Connect to your instance using its Public DNS:  
ec2-user@ip-172-31-20-109-157.eu-north-1.compute.amazonaws.com

Command copied

ssh -i "acc.pem" ec2-user@ec2-13-60-209-157.eu-north-1.compute.amazonaws.com

Note: In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

ec2-user@ip-172-31-20-109:~

Amazon Linux 2023

https://aws.amazon.com/linux/amazon-linux-2023

[ec2-user@ip-172-31-20-109 ~]\$ ls

[ec2-user@ip-172-31-20-109 ~]\$ aws configure

AWS Access Key ID [None]: ^C

[ec2-user@ip-172-31-20-109 ~]\$ aws s3 ls

Unable to locate credentials. You can configure credentials by running "aws configure".

[ec2-user@ip-172-31-20-109 ~]\$ aws configure

AWS Access Key ID [None]: AKIAWSTLMUG6FRQ6NTP5

AWS Secret Access Key [None]: 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

Default region name [None]:

Default output format [None]:

[ec2-user@ip-172-31-20-109 ~]\$ aws s3 ls

2025-08-01 10:58:58 bi-account

[ec2-user@ip-172-31-20-109 ~]\$

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

