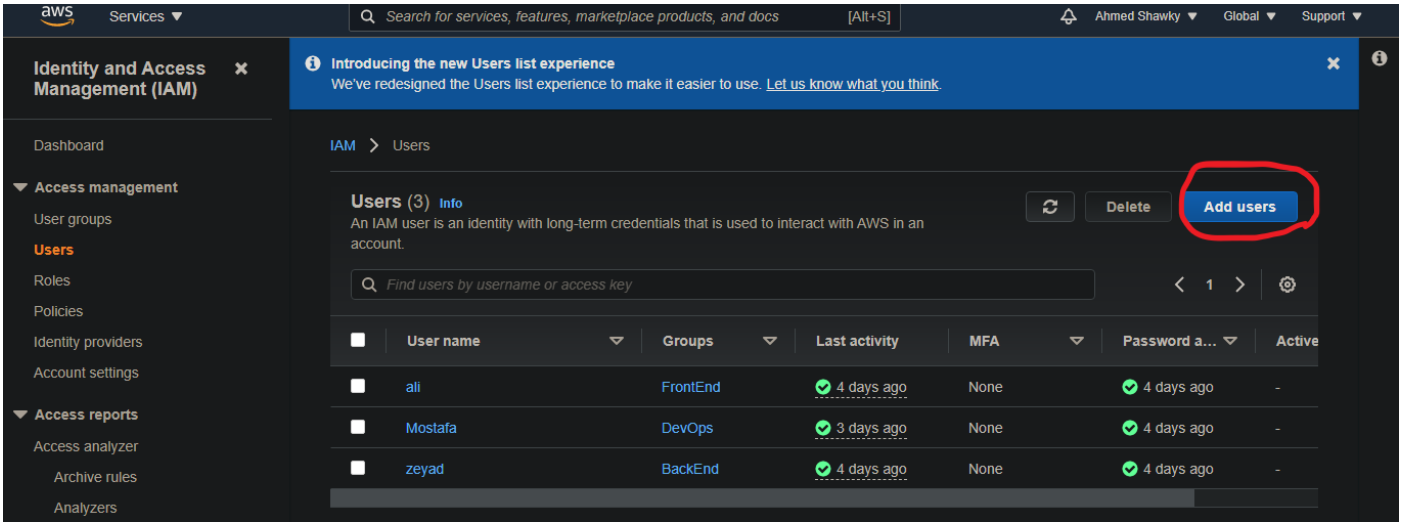
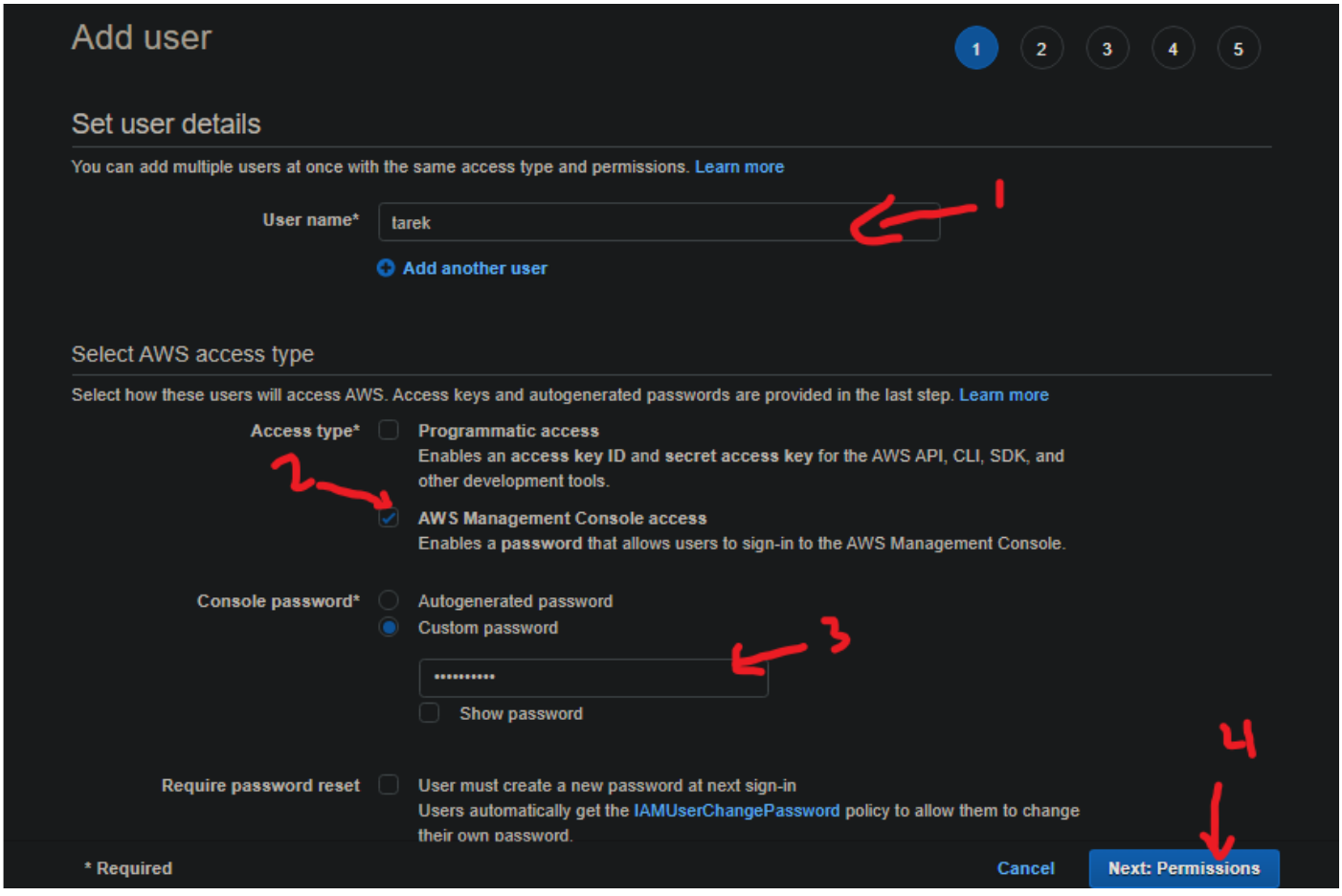
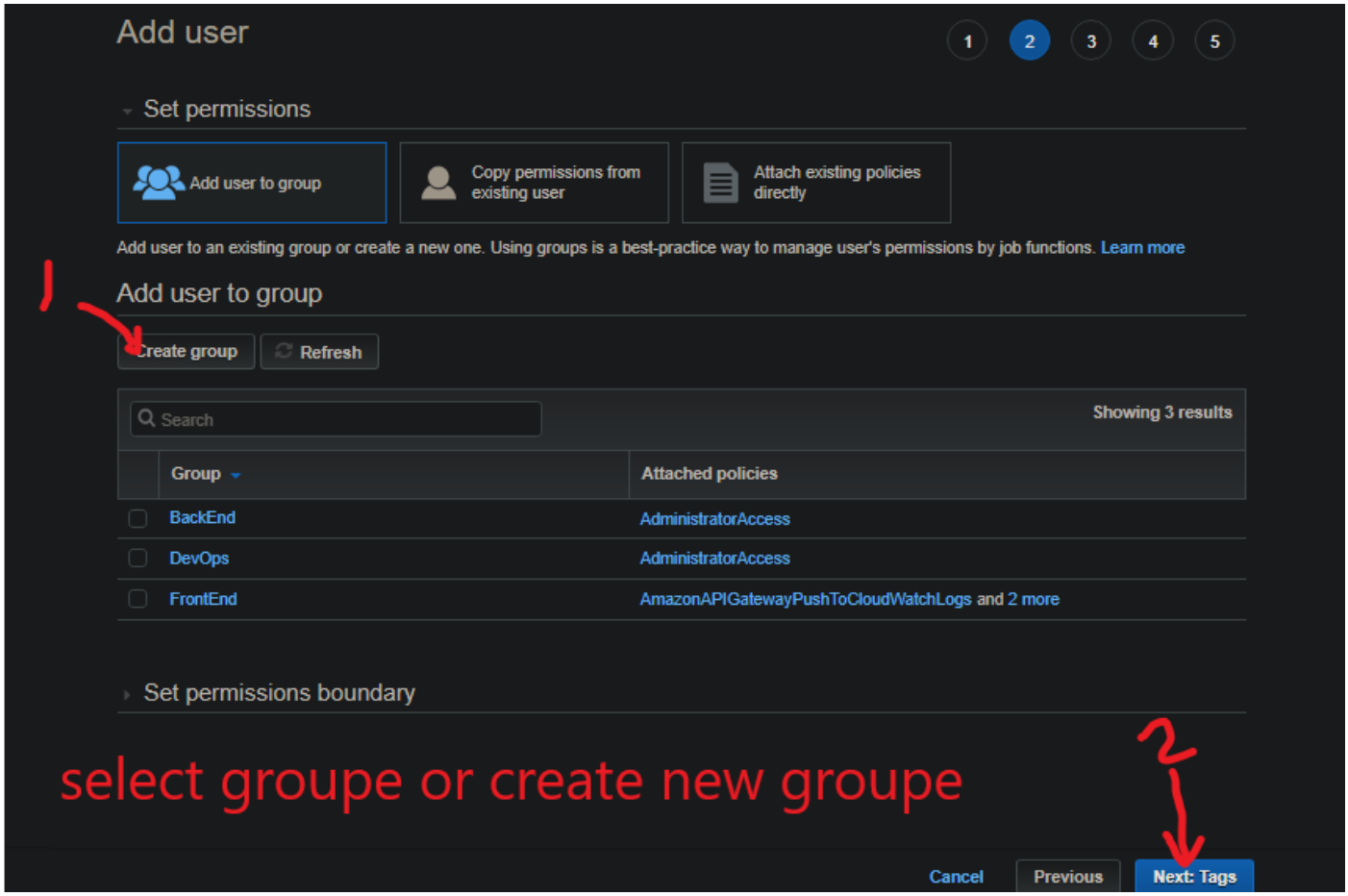
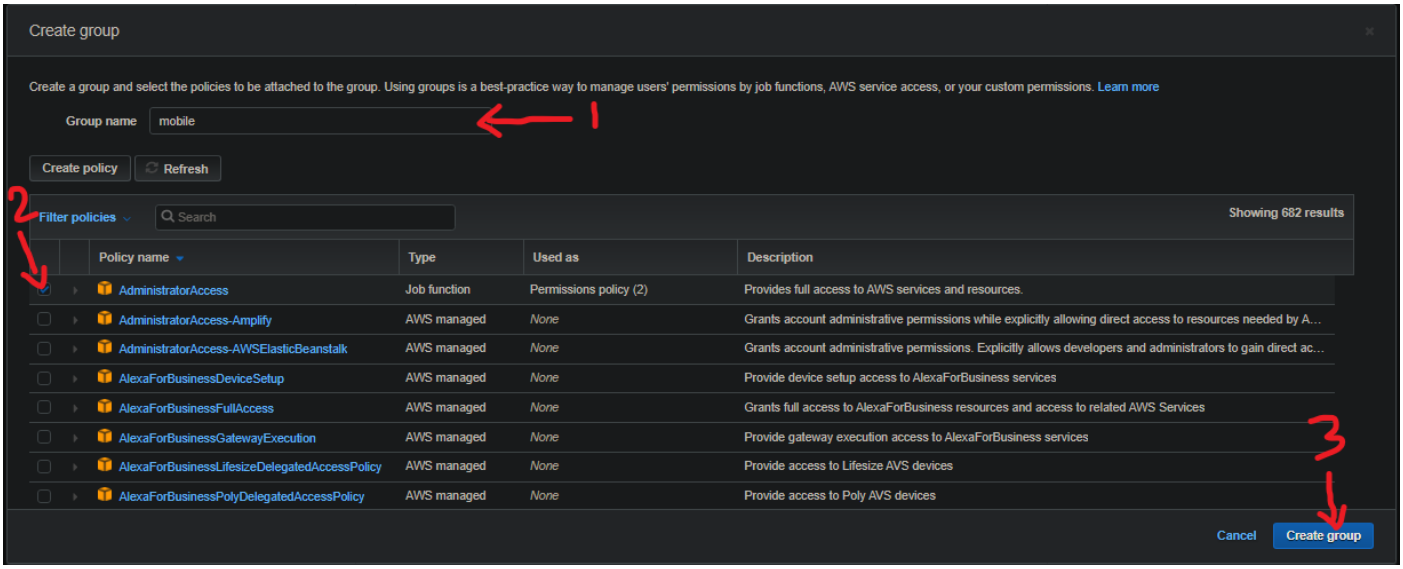
Ahmed Shawky: Task 1

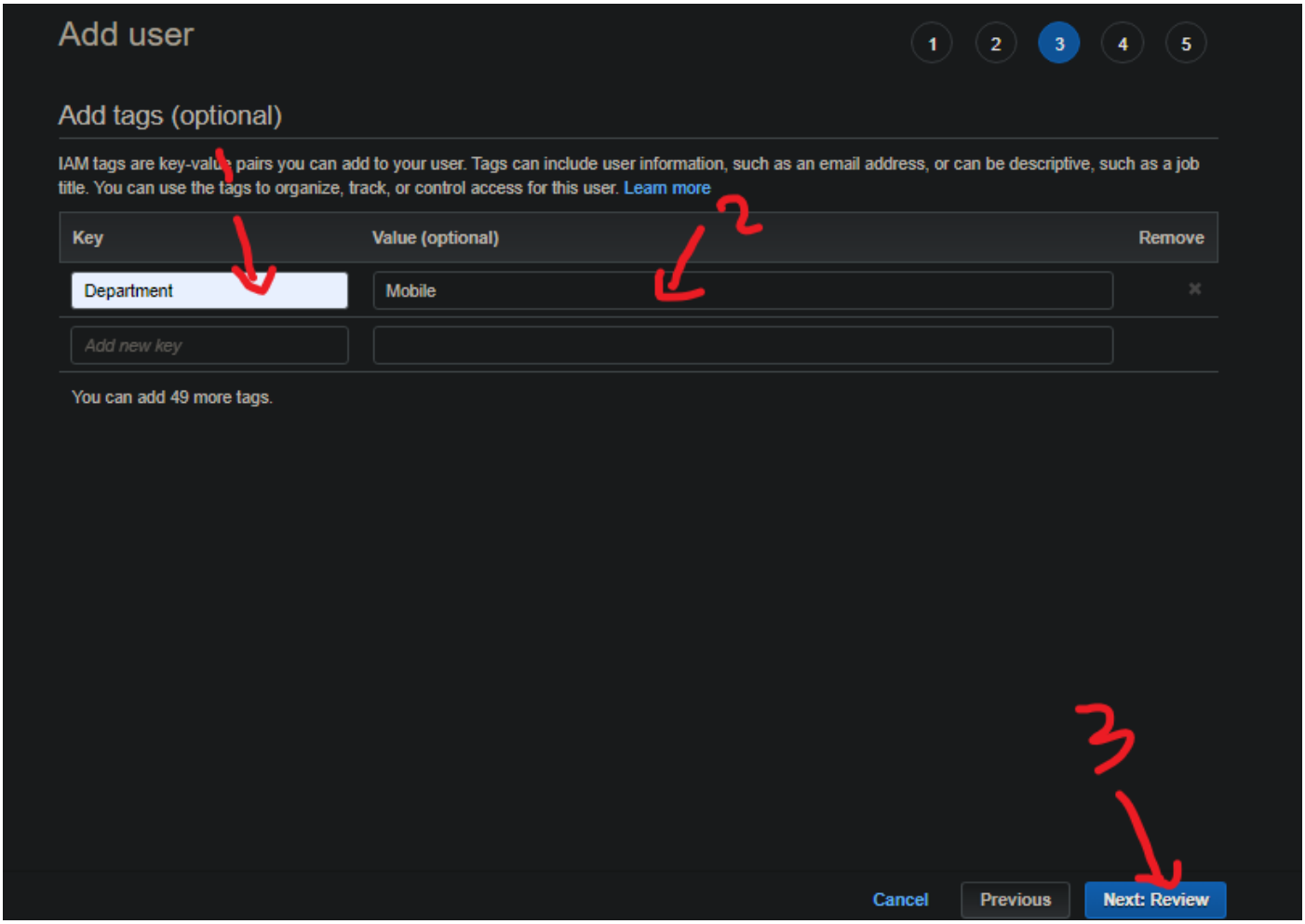
1- Create 2 IAM users and 2 groups and assign a user to each group:

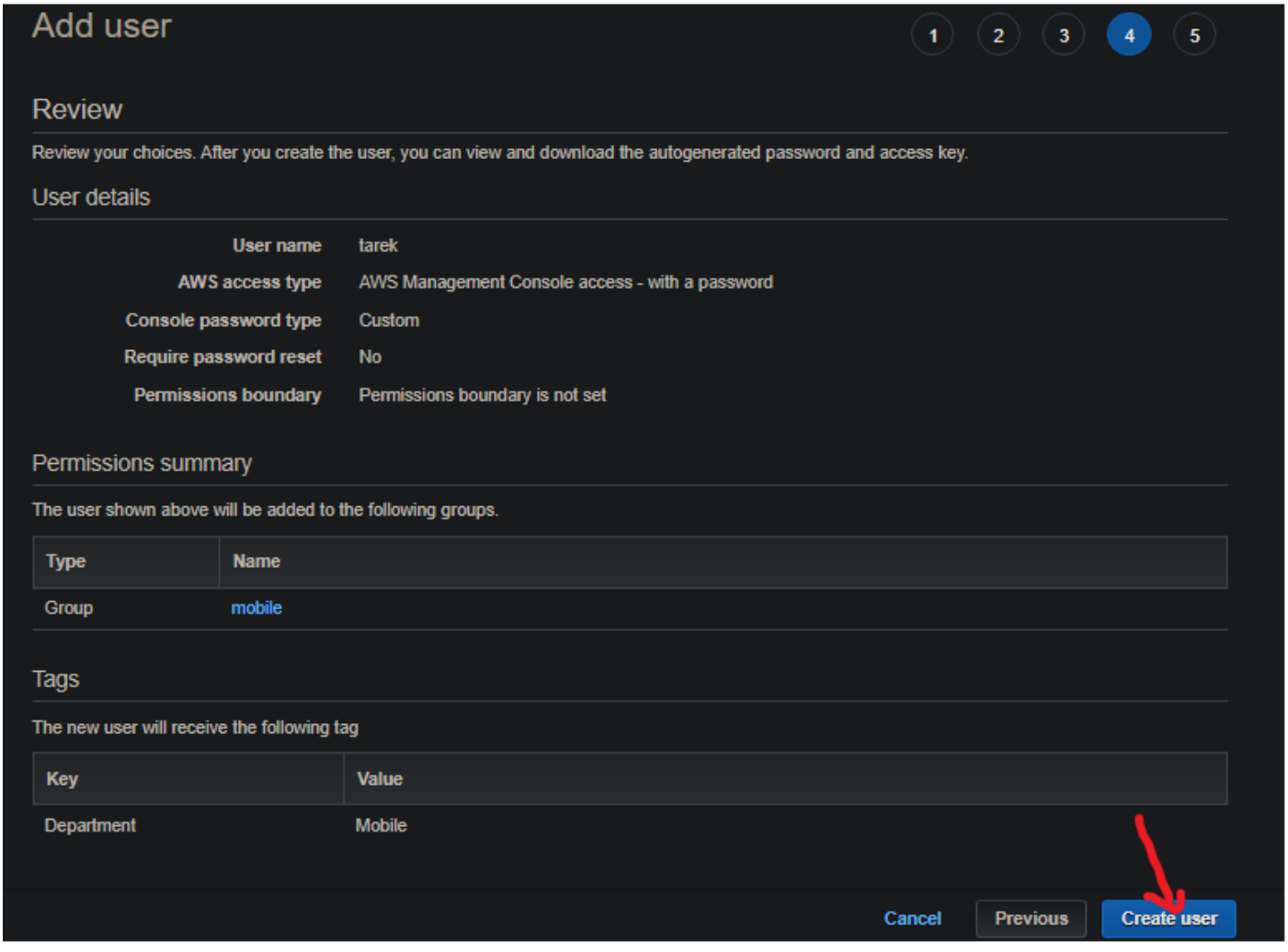




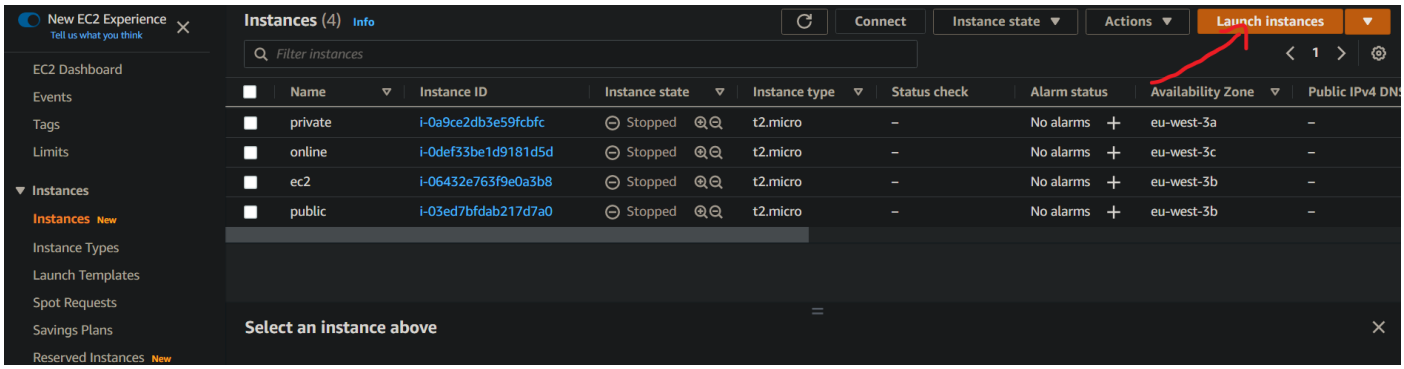

Add user
1 2 3 4 5
Set permissions
Add user to group
Copy permissions from existing user
Attach existing policies directly
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more
1
Add user to group
Create group
Refresh
Search
Showing 3 results
Group
Attached policies
BackEnd
AdministratorAccess
DevOps
AdministratorAccess
FrontEnd
AmazonAPIGatewayPushToCloudWatchLogs and 2 more
Set permissions boundary
select groupe or create new groupe
2
Cancel
Previous
Next: Tags

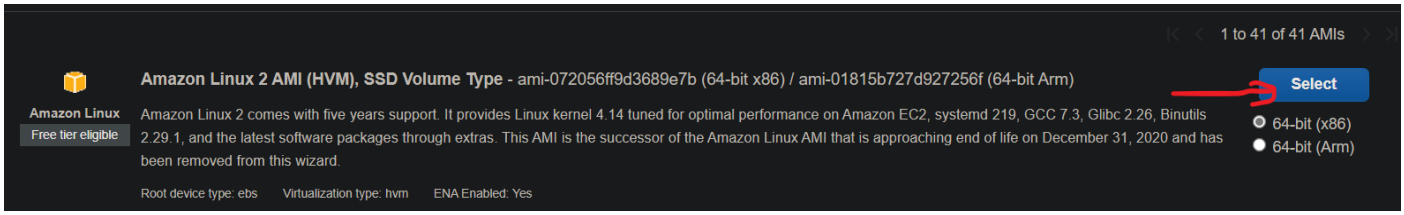

Create group
Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Learn more
Group name
mobile
1
Create policy
Refresh
2
Filter policies
Search
Showing 682 results
Policy name
Type
Used as
Description
AdministratorAccess
Job function
Permissions policy (2)
Provides full access to AWS services and resources.
AdministratorAccess-Amplify
AWS managed
None
Grants account administrative permissions while explicitly allowing direct access to resources needed by A...
AdministratorAccess-AWSElasticBeanstalk
AWS managed
None
Grants account administrative permissions. Explicitly allows developers and administrators to gain direct ac...
AlexaForBusinessDeviceSetup
AWS managed
None
Provide device setup access to AlexaForBusiness services
AlexaForBusinessFullAccess
AWS managed
None
Grants full access to AlexaForBusiness resources and access to related AWS Services
AlexaForBusinessGatewayExecution
AWS managed
None
Provide gateway execution access to AlexaForBusiness services
AlexaForBusinessLifesizeDelegatedAccessPolicy
AWS managed
None
Provide access to Lifesize AVS devices
AlexaForBusinessPolyDelegatedAccessPolicy
AWS managed
None
Provide access to Poly AVS devices
3
Cancel
Create group

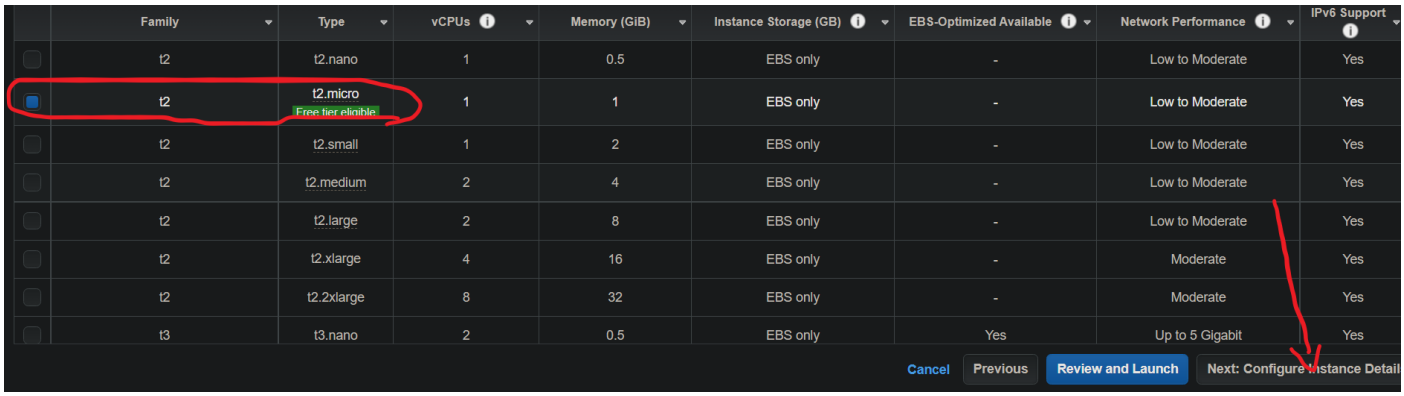

Add user
1 2 3 4 5
Add tags (optional)
IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. Learn more
Key
Value (optional)
Remove
Department
Mobile
Add new key
You can add 49 more tags.
1
2
3
Cancel
Previous
Next: Review

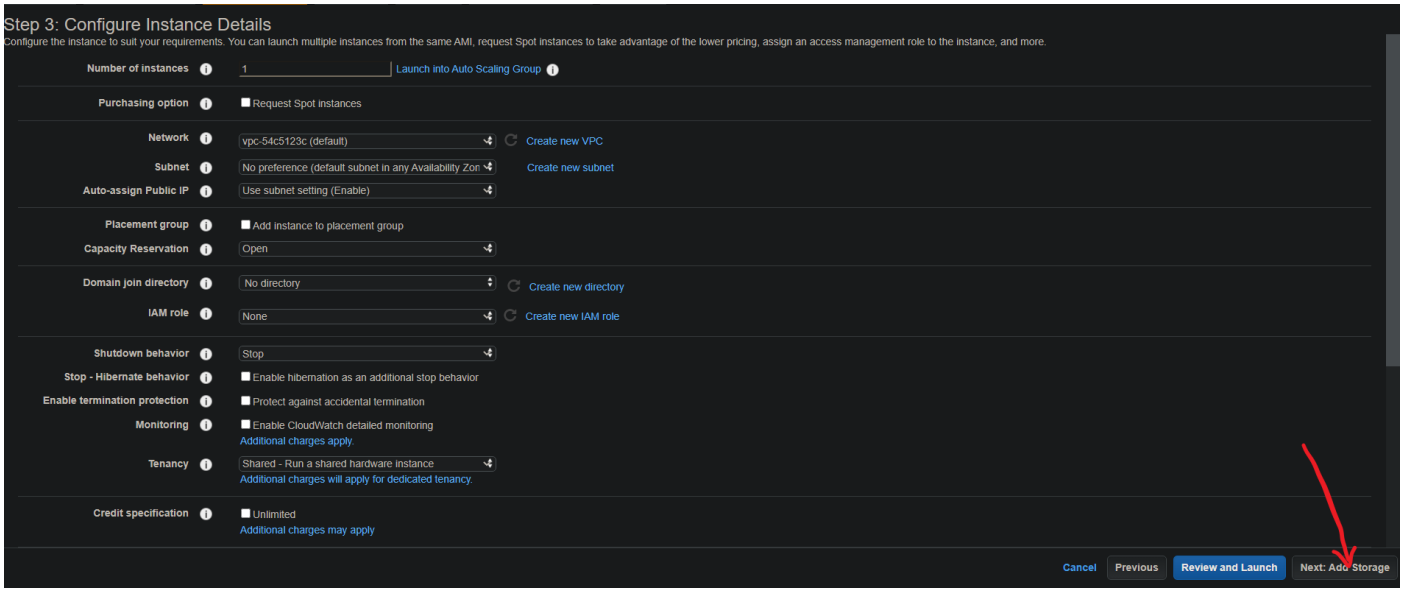

Add user
1 2 3 4 5
Review
Review your choices. After you create the user, you can view and download the autogenerated password and access key.
User details
User name tarek
AWS access type AWS Management Console access - with a password
Console password type Custom
Require password reset No
Permissions boundary Permissions boundary is not set
Permissions summary
The user shown above will be added to the following groups.
Type
Name
Group
mobile
Tags
The new user will receive the following tag
Key
Value
Department
Mobile
Cancel
Previous
Create user

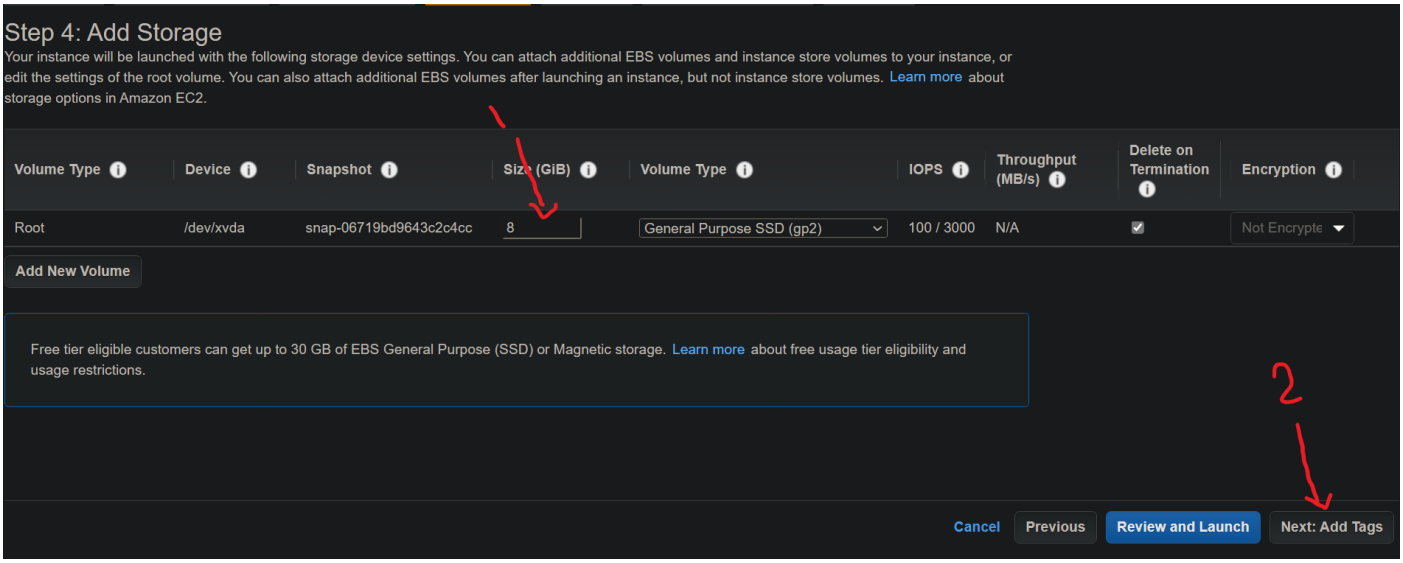
2- Launch an EC2 instance, install apache webserver and pit something in the /var/www/ folder to be served when an http request is served:

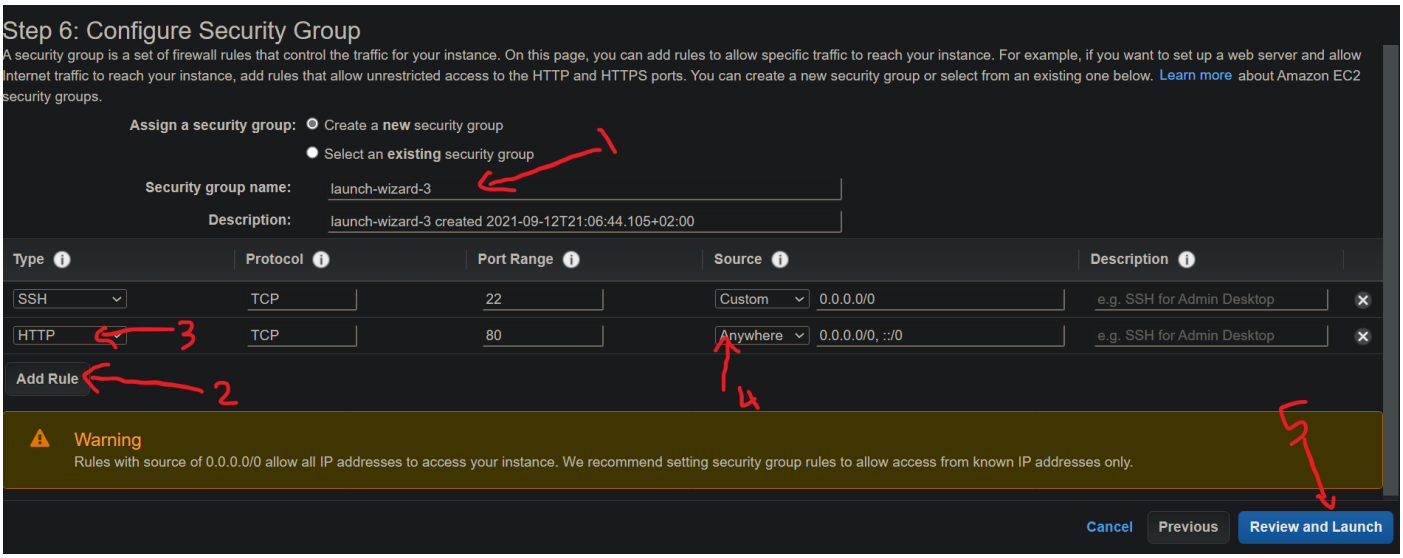







Step 3: Configure Instance Details
Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.
Number of instances
1
Launch into Auto Scaling Group
Purchasing option
Request Spot instances
Network
vpc-54c5123c (default)
Create new VPC
Subnet
No preference (default subnet in any Availability Zon
Create new subnet
Auto-assign Public IP
Use subnet setting (Enable)
Placement group
Add instance to placement group
Capacity Reservation
Open
Domain join directory
No directory
Create new directory
IAM role
None
Create new IAM role
Shutdown behavior
Stop
Stop - Hibernate behavior
Enable hibernation as an additional stop behavior
Enable termination protection
Protect against accidental termination
Monitoring
Enable CloudWatch detailed monitoring
Additional charges apply.
Tenancy
Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.
Credit specification
Unlimited
Additional charges may apply
Cancel
Previous
Review and Launch
Next: Add Storage


Step 4: Add Storage
Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.
Volume Type
Device
Snapshot
Size (GiB)
Volume Type
IOPS
Throughput (MB/s)
Delete on Termination
Encryption
Root
/dev/xvda
snap-06719bd9643c2c4cc
8
General Purpose SSD (gp2)
100 / 3000
N/A
Not Encrypte
Add New Volume
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.
2
Cancel
Previous
Review and Launch
Next: Add Tags


Step 6: Configure Security Group
A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.
Assign a security group:
Create a new security group
Select an existing security group
1
Security group name:
launch-wizard-3
Description:
launch-wizard-3 created 2021-09-12T21:06:44.105+02:00
Type
Protocol
Port Range
Source
Description
SSH
TCP
22
Custom
0.0.0.0/0
e.g. SSH for Admin Desktop
HTTP
3
TCP
80
Anywhere
0.0.0.0/0, ::/0
e.g. SSH for Admin Desktop
Add Rule
2
4
Warning
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
5
Cancel
Previous
Review and Launch

```
root@ip-172-31-29-125:/var/www/html
Microsoft Windows [Version 10.0.19043.1165]
(c) Microsoft Corporation. All rights reserved.

F:\AWS>ssh -i "myec2.pem" ec2-user@ec2-15-188-232-211.eu-west-3.compute.amazonaws.com
Last login: Sun Sep 12 19:14:19 2021 from 197.43.234.22
Last login: Sun Sep 12 19:14:19 2021 from 197.43.234.22

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-29-125 ~]$ sudo su
[root@ip-172-31-29-125 ec2-user]# yum install httpd
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core
Package httpd-2.4.48-2.amzn2.x86_64 already installed and latest version
Nothing to do
[root@ip-172-31-29-125 ec2-user]# cd /var/www
[root@ip-172-31-29-125 www]# ls
html
[root@ip-172-31-29-125 www]# cd html
[root@ip-172-31-29-125 html]# ls
index.html
[root@ip-172-31-29-125 html]# touch index.html
[root@ip-172-31-29-125 html]# ls
index.html
[root@ip-172-31-29-125 html]# nano index.html
```