Create AWS EC2 Instance in 4 Simple Steps

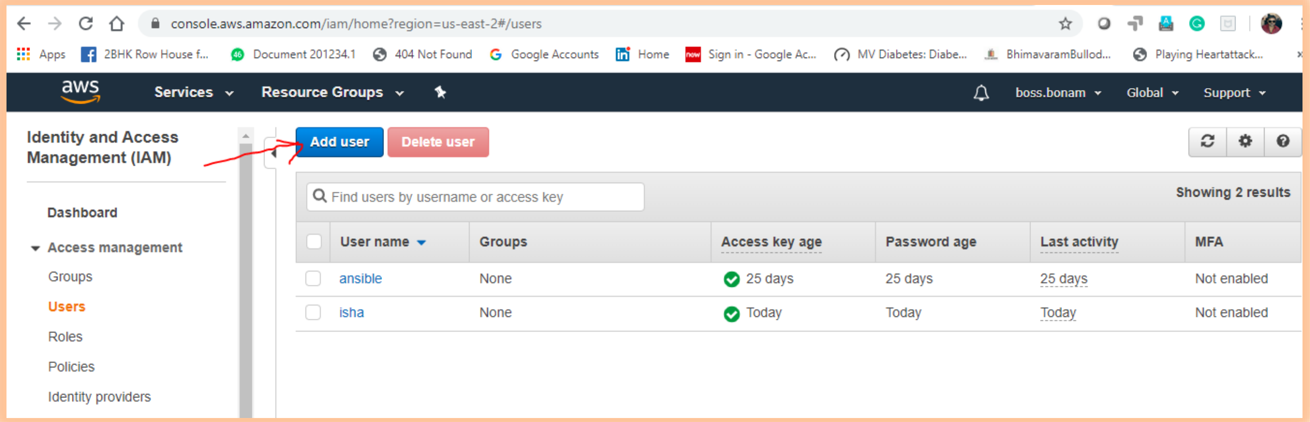
1. **Create a User and get AWS Access ID and Secret Key.**
2. **Configure AWS Credentials Locally**
3. **Create Key Pair for EC2 Instance**
4. **Create a New EC2 Instance**

1. Create a User and get AWS Access ID and Secret Key

1. Launch the Identity and Access Management console (IAM) in AWS.

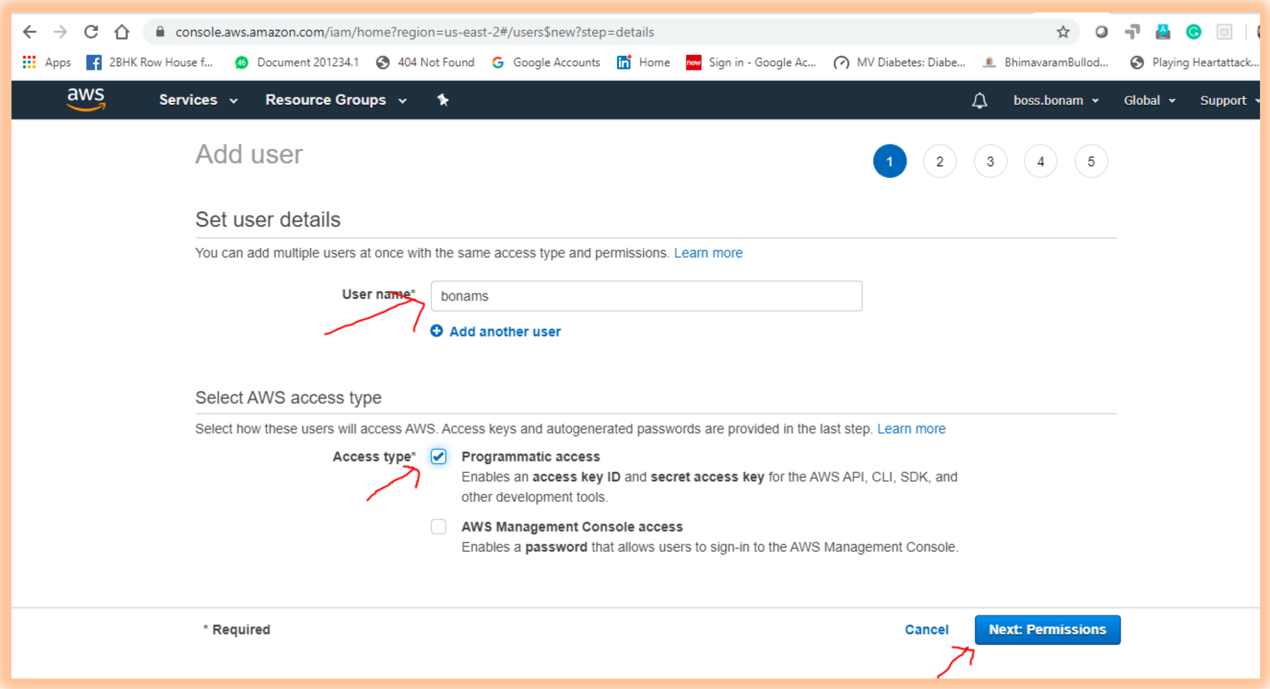
2. Click **Users** on the navigation menu on the left of the screen.

3. In the popup window, click on **Add User.**



User name	Groups	Access key age	Password age	Last activity	MFA
ansible	None	✓ 25 days	25 days	25 days	Not enabled
isha	None	✓ Today	Today	Today	Not enabled

Provide Username and click next



Add user

Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* bonams

Add another user

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

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

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

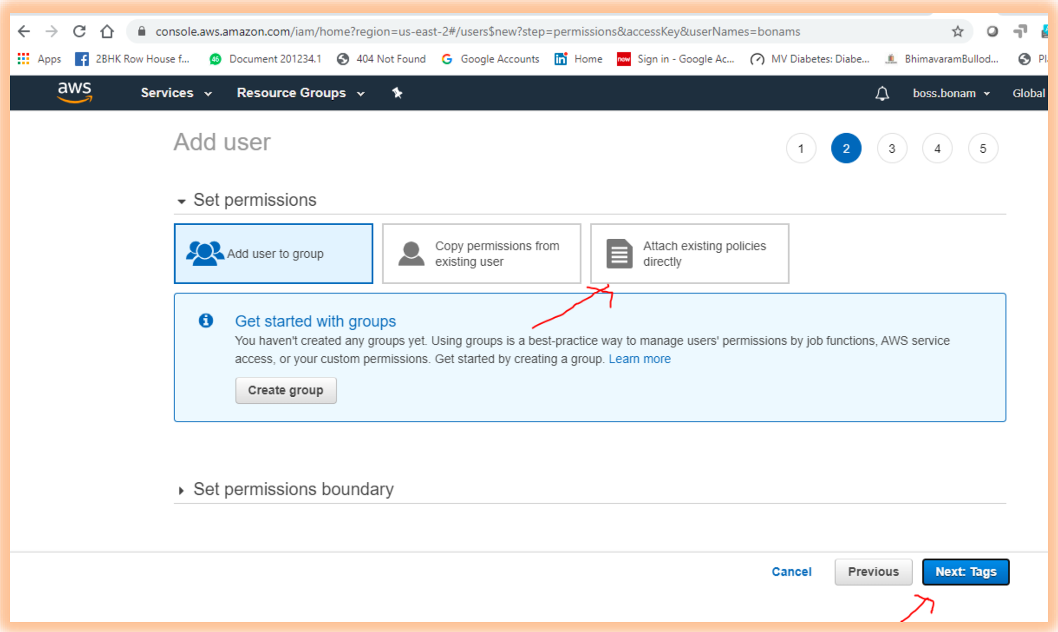
* Required

Cancel

Next: Permissions

Please don't forgot to check box **Programmatic access**

Click on Attaching existing policies



Add user

Set permissions

Add user to group

Copy permissions from existing user

Attach existing policies directly

Get started with groups

You haven't created any groups yet. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Get started by creating a group. Learn more

Create group

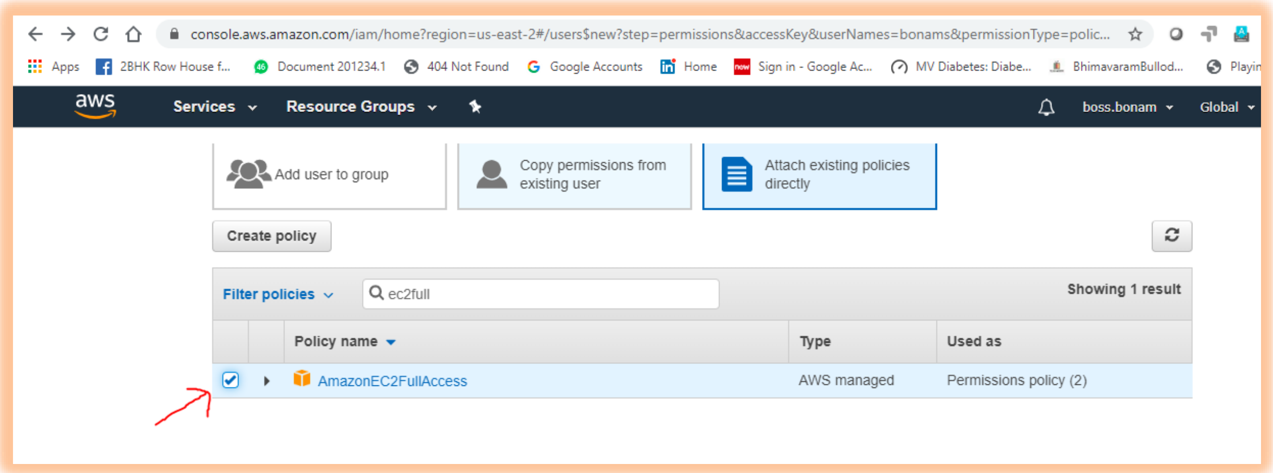
Set permissions boundary

Cancel

Previous

Next: Tags

Find for AmazonEC2FullAccess and select



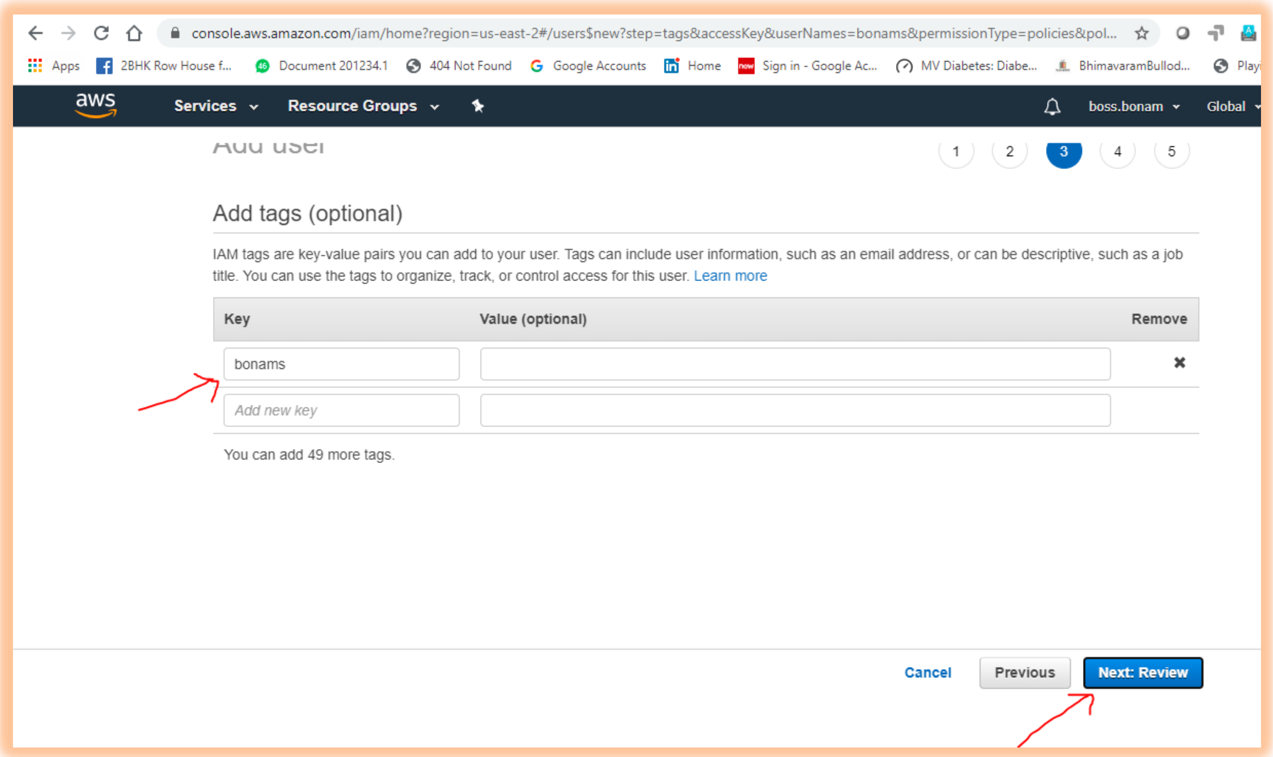
console.aws.amazon.com/iam/home?region=us-east-2#/users$new?step=permissions&accessKey&userNames=bonams&permissionType=polic...

ec2full

Showing 1 result

		Policy name	Type	Used as
☑	▸	AmazonEC2FullAccess	AWS managed	Permissions policy (2)

Tags are optional



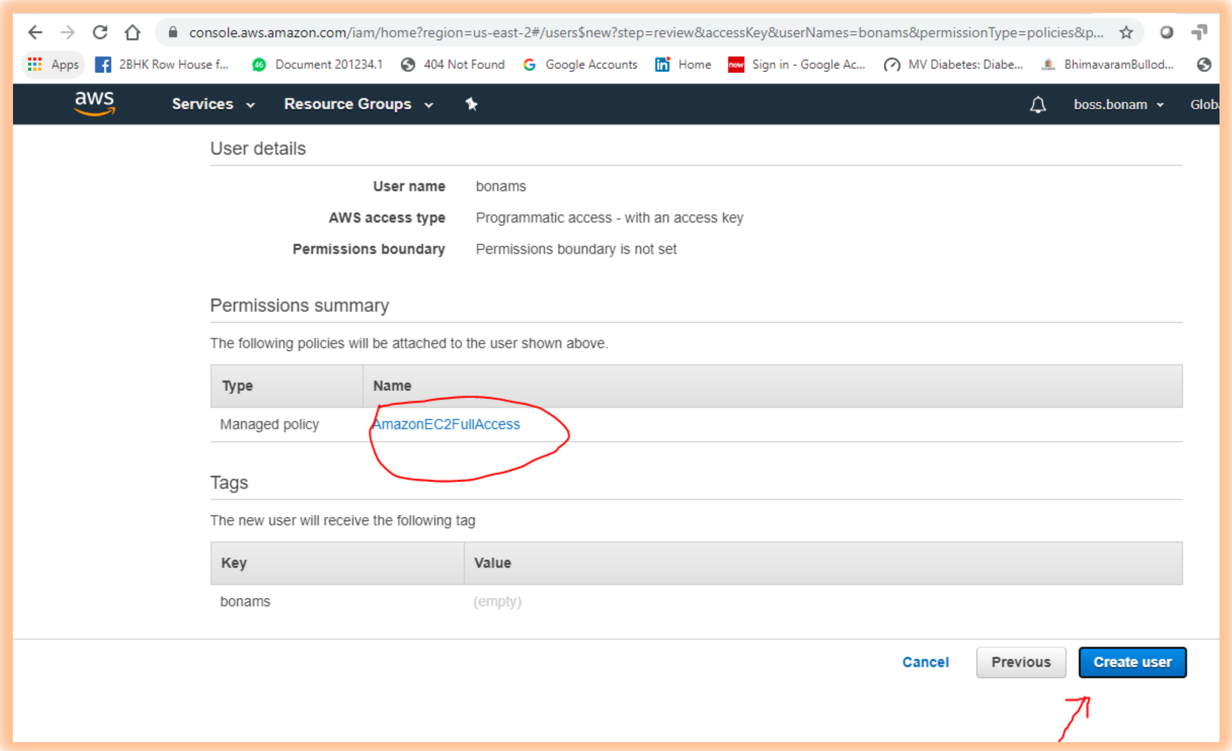
console.aws.amazon.com/iam/home?region=us-east-2#/users$new?step=tags&accessKey&userNames=bonams&permissionType=policies&pol...

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
bonams		✖
Add new key		

You can add 49 more tags.



User details

User name	bonams
AWS access type	Programmatic access - with an access key
Permissions boundary	Permissions boundary is not set

Permissions summary

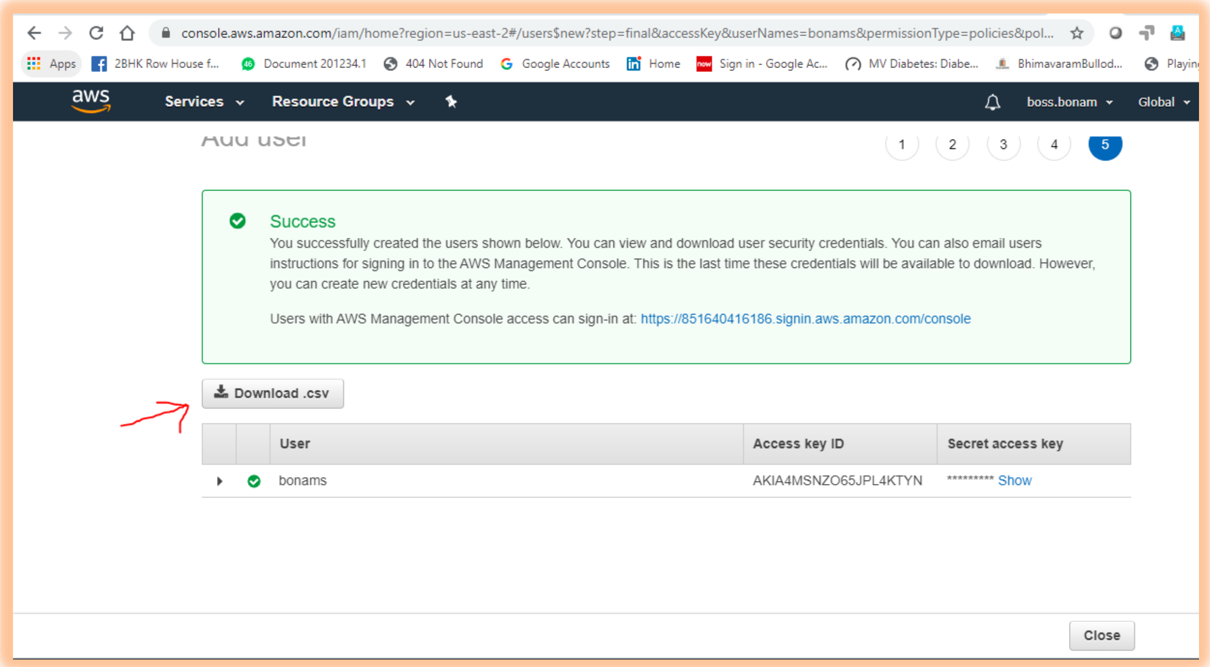
The following policies will be attached to the user shown above.

Type	Name
Managed policy	AmazonEC2FullAccess

Tags

The new user will receive the following tag

Key	Value
bonams	(empty)



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://851640416186.signin.aws.amazon.com/console

User	Access key ID	Secret access key
bonams	AKIA4MSNZO65JPL4KTYN	********* Show

Please download CSV file this file contains Access key ID and Secret access key

2. Configure AWS Credentials Locally

AWS CI tool should be configured to execute following commands

aws configure -- execute in CMD promt after AWS CL install

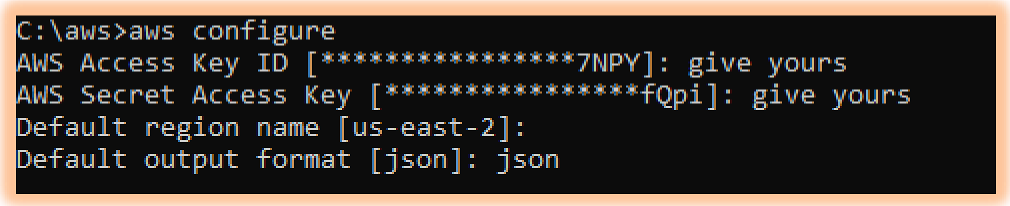
<u>It will prompt for below inputs</u>

AWS Key ID: you can get it from CSV file which we downloaded after user creation

AWS Access Key: you can get it from CSV file which we downloaded after user creation

Default Region Name: please provide your AWS region Name

Default Output: json



```
C:\aws>aws configure
AWS Access Key ID [****************7NPY]: give yours
AWS Secret Access Key [****************fQpi]: give yours
Default region name [us-east-2]:
Default output format [json]: json
```

To validate Connection to AWS

aws ec2 describe-instances

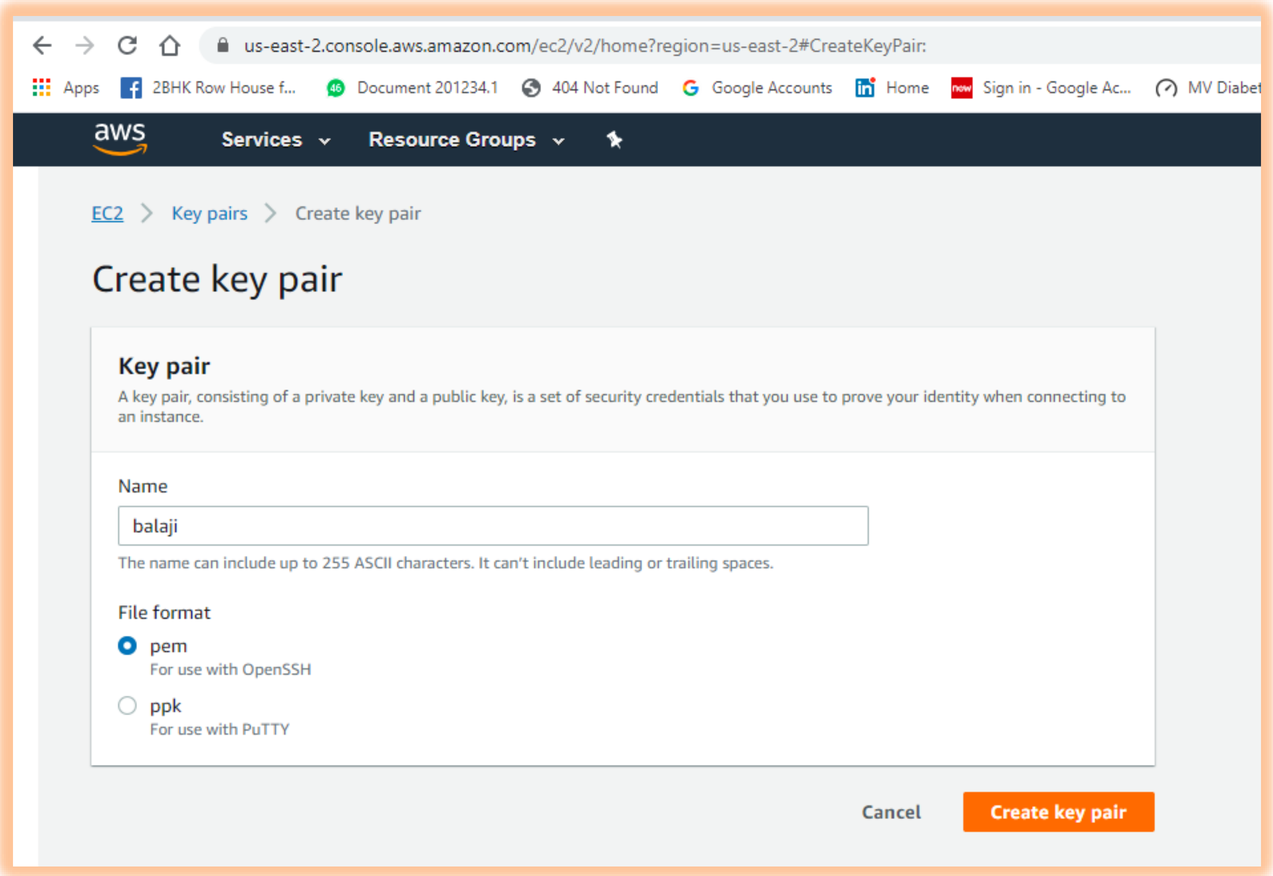
Should Display your existing AWS instance details

3. Create Key Pair for EC2 Instance

Go to AWS EC2 console

Services → ec2 → Key Pairs

Create New Keypair.



EC2 > Key pairs > Create key pair

Create key pair

Key pair

A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.

Name

balaji

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

File format

● pem
For use with OpenSSH

○ ppk
For use with PuTTY

pem File automatically download to your local machine please save in secured location and this will use to create ec2 instance

Your local server use this key file to create and connect to aws instance

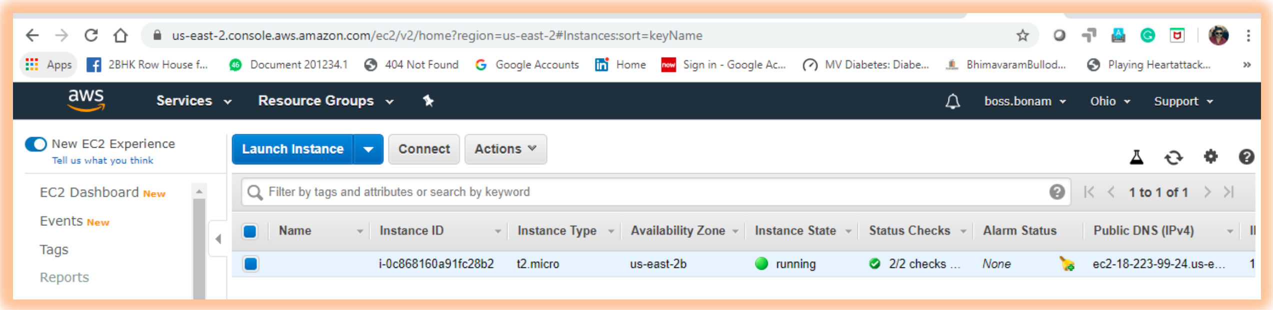
4. Create a New EC2 Instance

Got to location where you saved pem file and open python shell and run below

Note: ImageId='ami-0f7919c33c90f5b58' type of image you can get this from aws console

KeyName='balaji' is name of your keyfile (extension not required)

```
import boto3
ec2 = boto3.resource('ec2')
# create a new EC2 instance
instances = ec2.create_instances(
    ImageId='ami-0f7919c33c90f5b58',
    MinCount=1,
    MaxCount=1,
    InstanceType='t2.micro',
    KeyName='balaji'
 )
```



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	I
	i-0c868160a91fc28b2	t2.micro	us-east-2b	● running	✓ 2/2 checks ...	None	ec2-18-223-99-24.us-e...	1

Thanks

Bonams