

# AWS CLI



## GOAL

1. Install AWS CLI
2. Create EC2 Instance from CLI

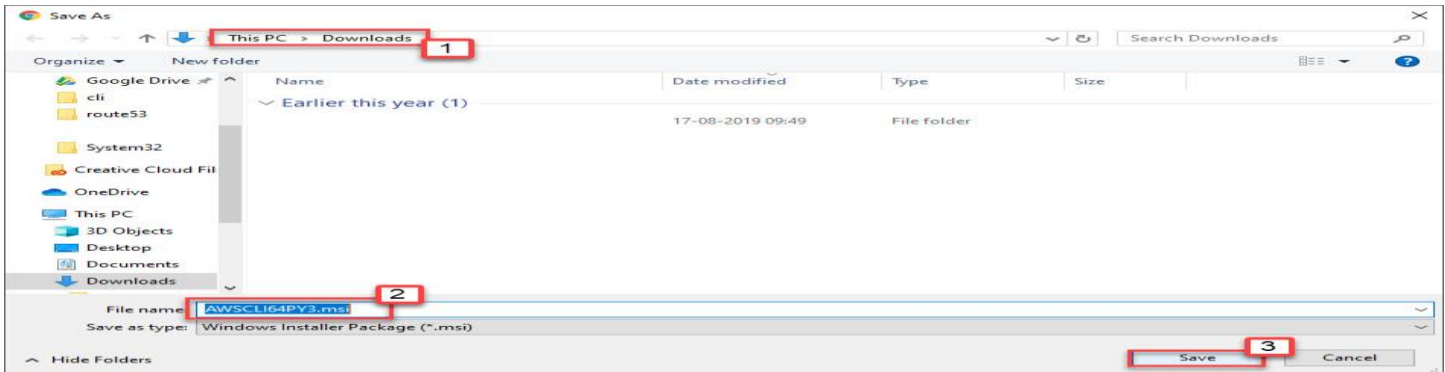
Download aws CLI Installer from the aws website.

1. In to google search bar type aws cli installer for windows
2. Open First Searched link
3. Make Sure that Link must be amazon website.

1. From the aws cli website go to Install AWS CLI Using the MSI Installer
2. Select download AWS CLI installer (Select installer as per your desktop configuration)

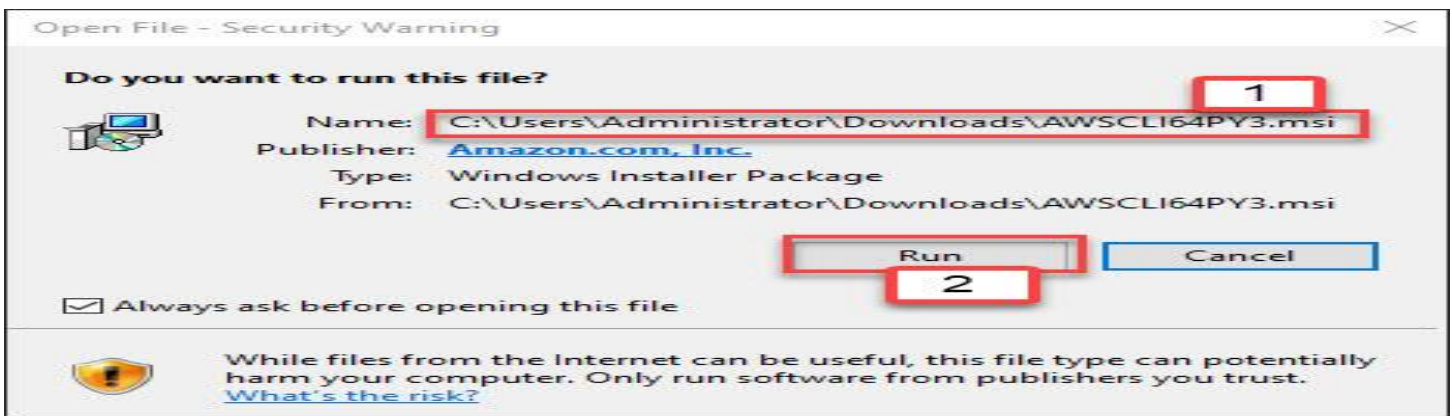
# AWS CLI

1. Select download location and note down.
2. Now down MST File Name
3. Click Save

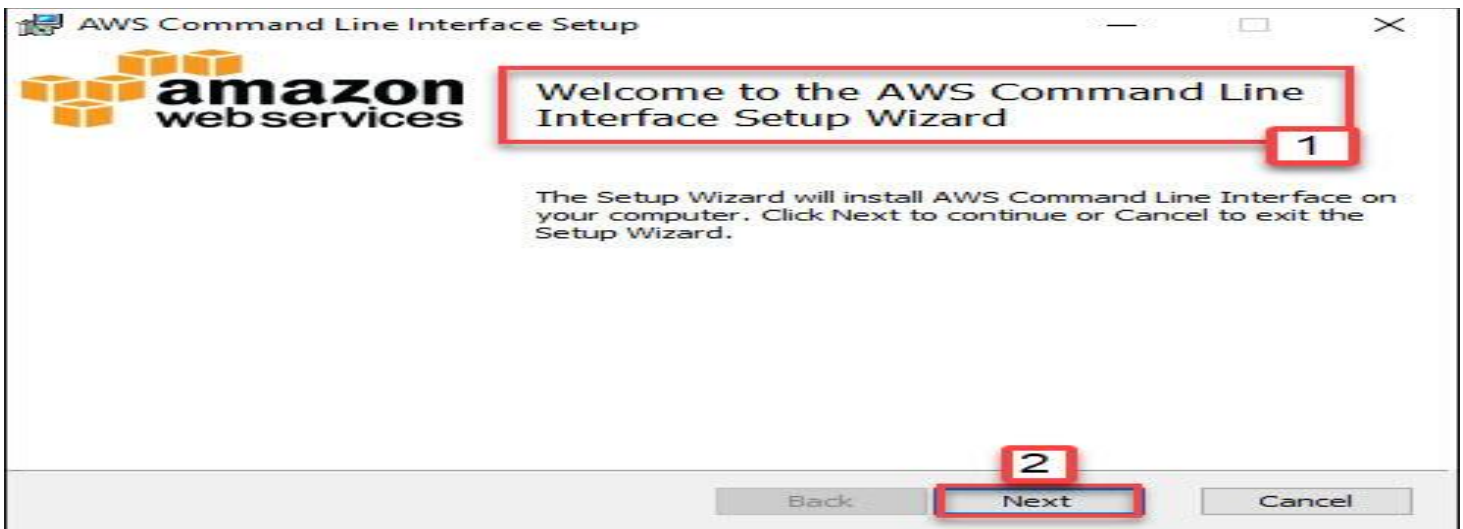


Double Click AWSCLI64PY3.MSI once download completed

1. Make Sure about file name.
2. Click Run



1. Make sure you are installing aws CLI
2. Click Next

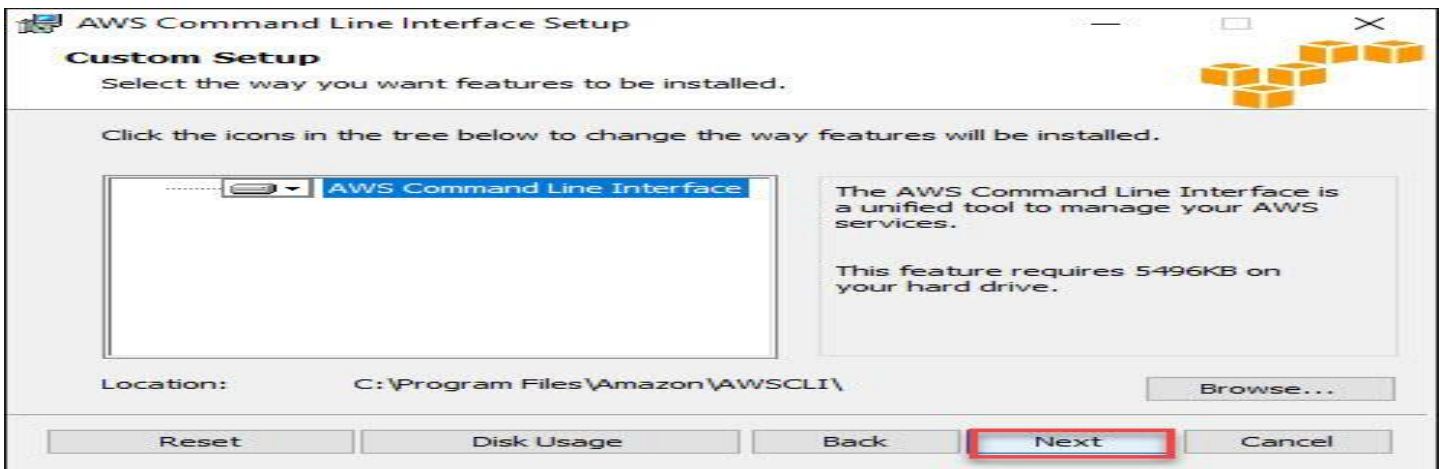


# AWS CLI

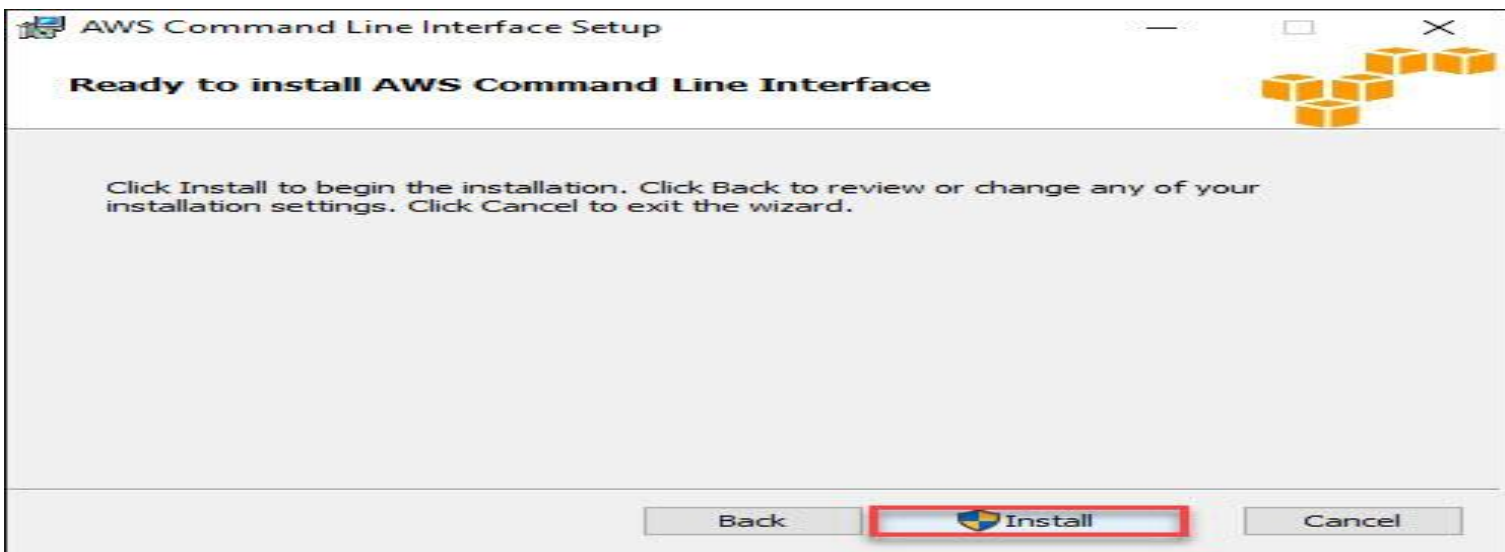
1. Accept the terms in the License Agreement
2. Next



Click Next



Click Install



Wait for installation to complete.

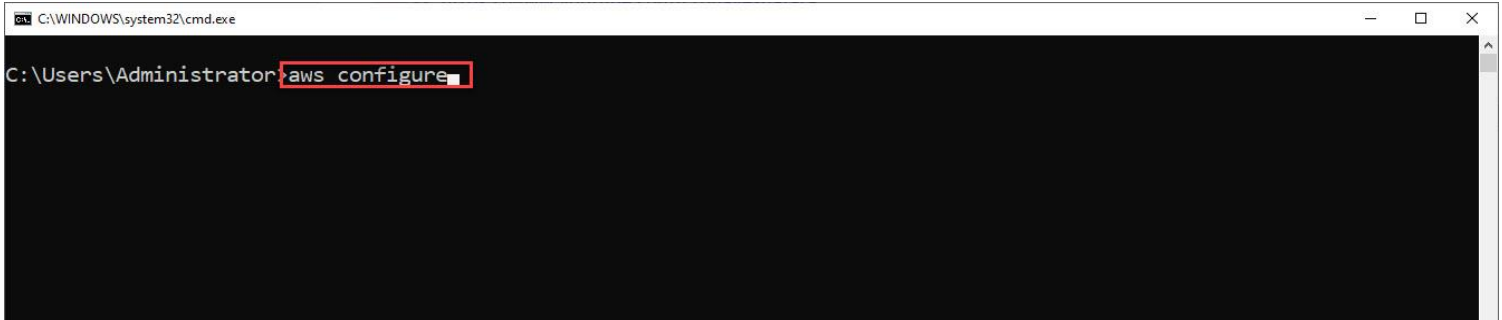
# AWS CLI

AWS CLI is Installed in our system.

Now in the following step we will create EC2 Instance from CLI.

To Open AWS CLI

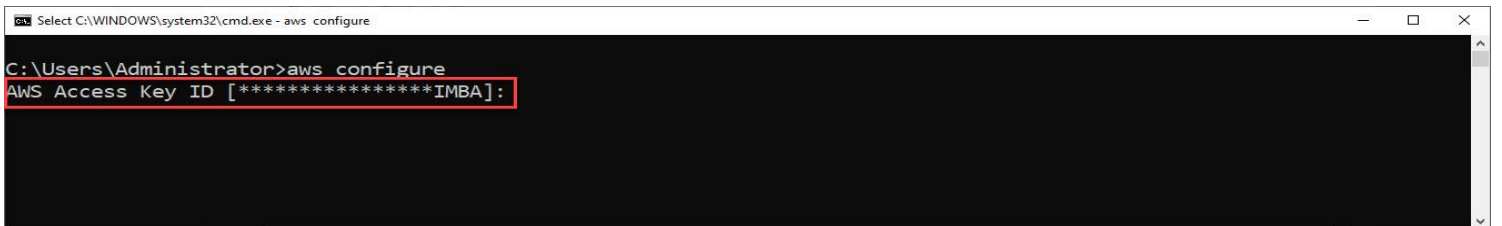
1. Type AWS Configure on windows command prompt and press enter.



Here you have to provide Access Key ID and Security Key

If you already having Access Key ID and Security Key enter it here

If You don't have Access Key ID and Security Key for Your root account minimize command line windows here and go for next step in which you will get access key and security key.

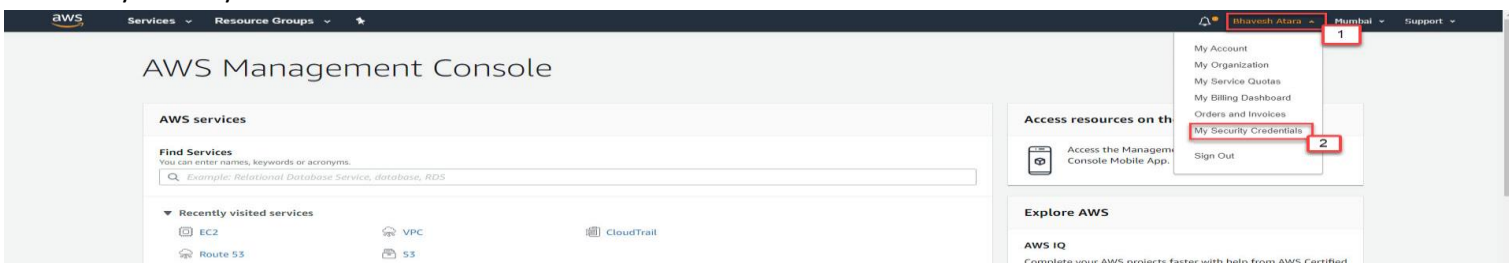


To Download Access Key and Security Key

Log on to your aws GUI console using your username and password.

1. Click On your account name (Upper right corner)

2. Click My Security Credentials



1. Continue to Security Credentials

You are accessing the security credentials page for your AWS account. The account credentials provide unlimited access to your AWS resources.

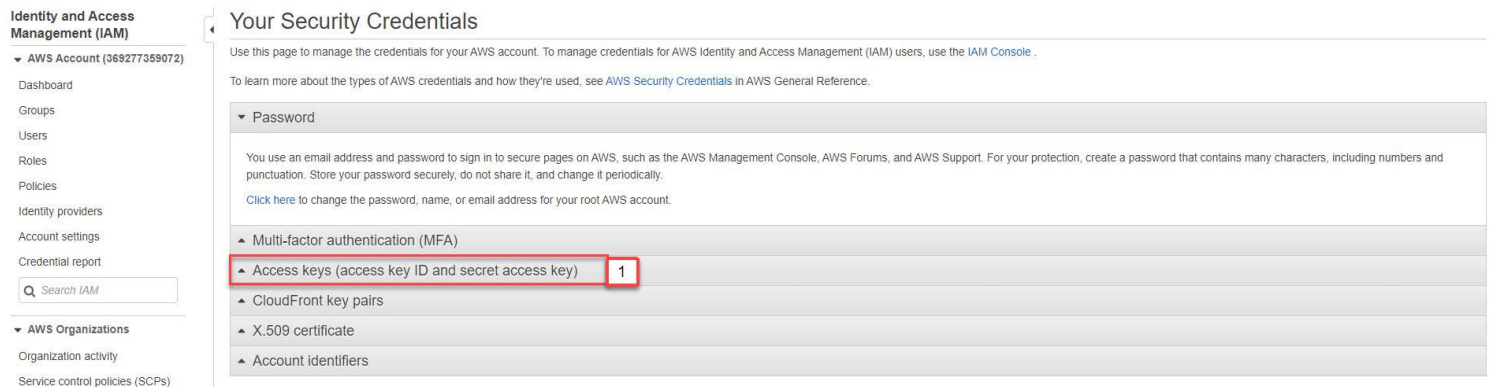
To help secure your account, follow an [AWS best practice](#) by creating and using AWS Identity and Access Management (IAM) users with limited permissions.





# AWS CLI

## 1. Click On Access-Keys



**Identity and Access Management (IAM)**

- AWS Account (369277359072)
  - Dashboard
  - Groups
  - Users
  - Roles
  - Policies
  - Identity providers
  - Account settings
  - Credential report
  - Search IAM
- AWS Organizations
  - Organization activity
  - Service control policies (SCPs)

### Your Security Credentials

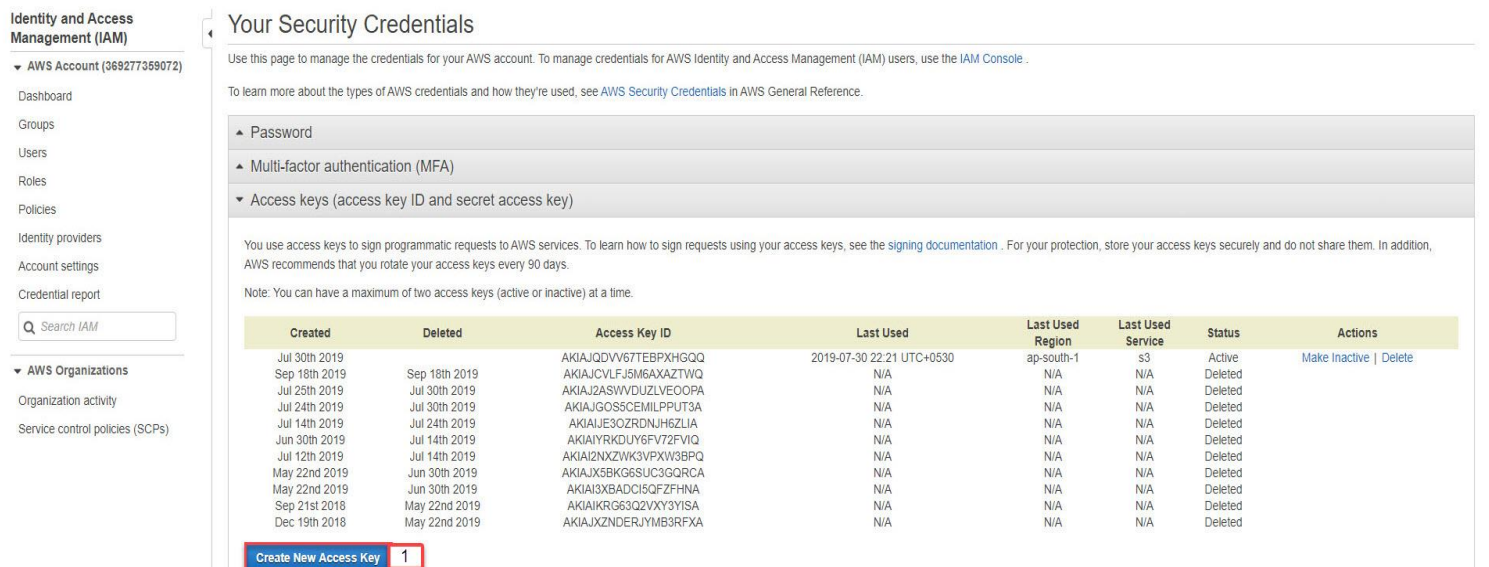
Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the [IAM Console](#).

To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.

- Password
- Multi-factor authentication (MFA)
- Access keys (access key ID and secret access key)** 1
- CloudFront key pairs
- X.509 certificate
- Account identifiers

## 1. Click Create New Access Key

Note – If Create New Access Key is Greyed out it means you are already having 2 active key in this case either you have to use your old key or you can delete existing active key and create new.  
as per aws rule use can create maximum 2 access key.



**Identity and Access Management (IAM)**

- AWS Account (369277359072)
  - Dashboard
  - Groups
  - Users
  - Roles
  - Policies
  - Identity providers
  - Account settings
  - Credential report
  - Search IAM
- AWS Organizations
  - Organization activity
  - Service control policies (SCPs)

### Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the [IAM Console](#).

To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.

- Password
- Multi-factor authentication (MFA)
- Access keys (access key ID and secret access key)**

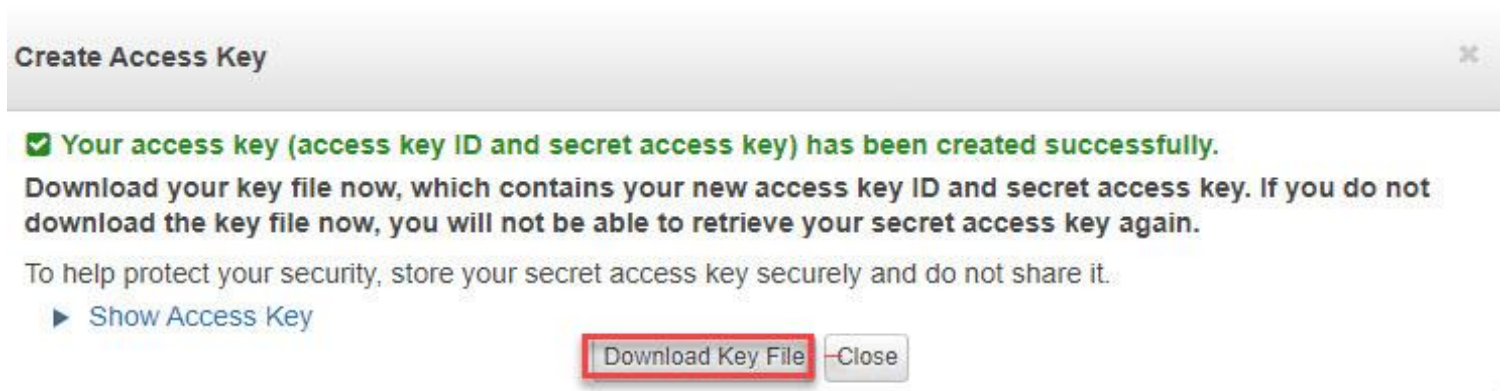
You use access keys to sign programmatic requests to AWS services. To learn how to sign requests using your access keys, see the [signing documentation](#). For your protection, store your access keys securely and do not share them. In addition, AWS recommends that you rotate your access keys every 90 days.

Note: You can have a maximum of two access keys (active or inactive) at a time.

Created	Deleted	Access Key ID	Last Used	Last Used Region	Last Used Service	Status	Actions
Jul 30th 2019		AKIAJQDVV67TEBPXHGQQ	2019-07-30 22:21 UTC+0530	ap-south-1	s3	Active	<a href="#">Make Inactive</a>   <a href="#">Delete</a>
Sep 18th 2019	Sep 18th 2019	AKIAJCVLFJ5M6AXAZTWQ	N/A	N/A	N/A	Deleted	
Jul 25th 2019	Jul 30th 2019	AKIAJ2ASWVDU2LVEOOPA	N/A	N/A	N/A	Deleted	
Jul 24th 2019	Jul 30th 2019	AKIAJGOSCEMILPPUT3A	N/A	N/A	N/A	Deleted	
Jul 14th 2019	Jul 24th 2019	AKIAJIE3OZRDNIH6ZLIA	N/A	N/A	N/A	Deleted	
Jun 30th 2019	Jul 14th 2019	AKIAIYRKDUY6FV72FVIQ	N/A	N/A	N/A	Deleted	
Jul 12th 2019	Jul 14th 2019	AKIAI2NXZWK3VPXW3BPQ	N/A	N/A	N/A	Deleted	
May 22nd 2019	Jun 30th 2019	AKIAJ5BK6SUC3GGORCA	N/A	N/A	N/A	Deleted	
May 22nd 2019	Jun 30th 2019	AKIAJ3XBADCI5QFZFHNA	N/A	N/A	N/A	Deleted	
Sep 21st 2018	May 22nd 2019	AKIAIKRG63Q2VXY3YISA	N/A	N/A	N/A	Deleted	
Dec 19th 2018	May 22nd 2019	AKIAJXZNDERJYMB3RFXA	N/A	N/A	N/A	Deleted	

[Create New Access Key](#) 1

Click Download Key File.



**Create Access Key**

✓ Your access key (access key ID and secret access key) has been created successfully.

Download your key file now, which contains your new access key ID and secret access key. If you do not download the key file now, you will not be able to retrieve your secret access key again.

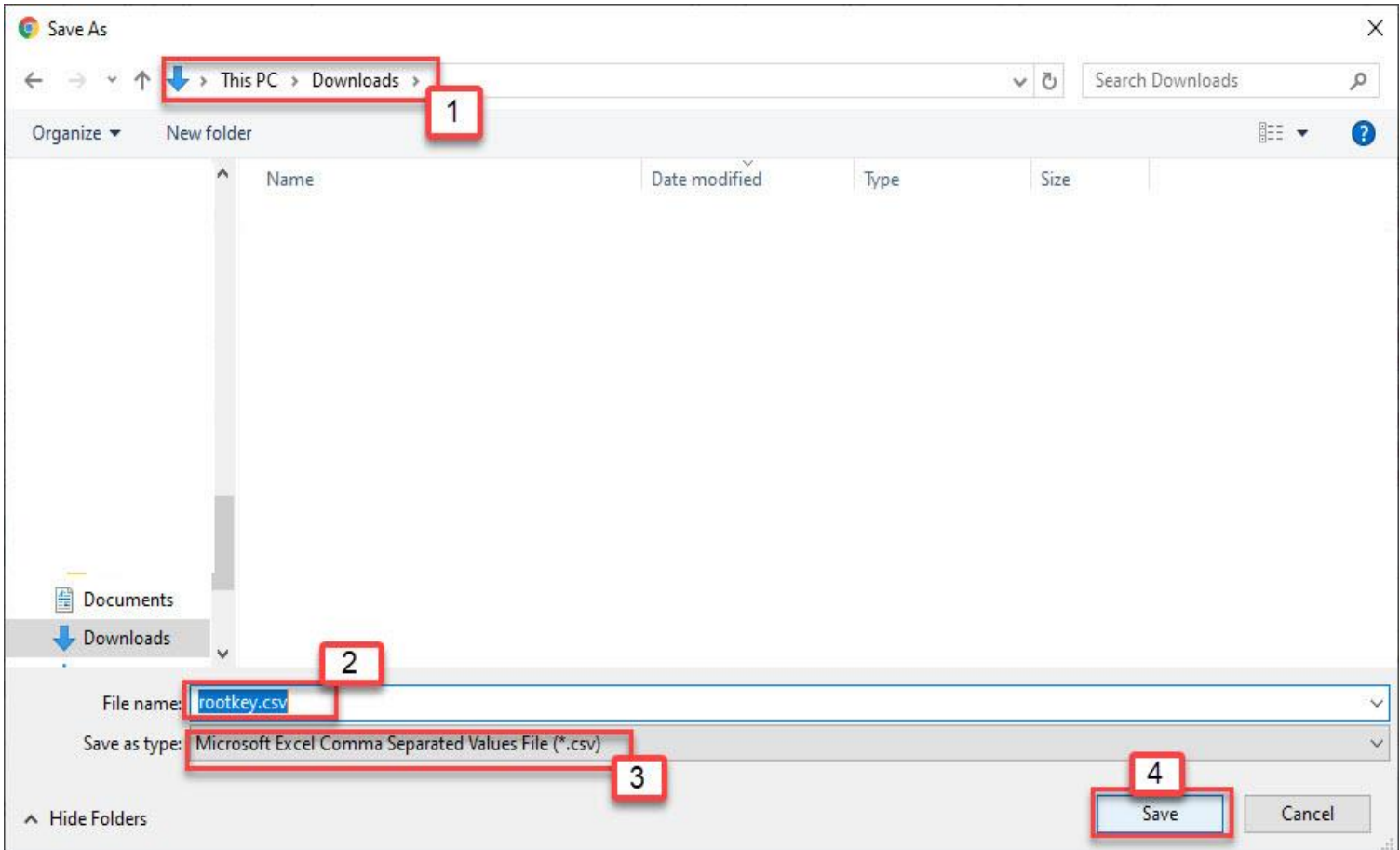
To help protect your security, store your secret access key securely and do not share it.

[Show Access Key](#)

[Download Key File](#) [Close](#)

# AWS CLI

1. Select and note down location of Root key files.
2. Note down name of Root Key Files.
3. Note down format of Root Key files.
4. Click Save.



Now You have root access key and secret key open CSV file. Copy both key step by step and paste it into aws CLI.

1. Access Key you will get from rootkey.csv file we downloaded earlier
2. Secret Key you will get from rootkey.csv we downloaded earlier.
3. If you want to set region you can write here but make sure that **region code should be 100% right**. Or you can press enter for default region.
4. Output format make sure that output format file name must be in lowercase. **Sometime default selection is in upper case which creates problem so if default selection is in upper case write down in lowercase and press enter.**

```
C:\Users\Administrator>aws configure
AWS Access Key ID [*****IMBA]: AKIAIAYMPOXSOW3NIMBA
AWS Secret Access Key [*****sjUx]: 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
Default region name [ap-south-1]:
Default output format [JSON]: json
```

# AWS CLI

Now we will create EC2 Windows Instance Using command line.

But before we create instance we required to create

1. Security group.
2. Add Rule to Security Group.
3. Create Key Pair.

To create Security Group type following command on aws cli

1. Give following command

```
aws ec2 create-security-group --group-name awsclitraining --description "test sg from cli"
```

For error free practice copy command from here and paste it at aws cli

You can change security group name and description as per you convince.

Do not forget to notedown Security Group ID.

```
C:\Users\Administrator>aws configure
AWS Access Key ID [*****IMBA]: AKIAJ3AJAWULIRE3UVYQ
AWS Secret Access Key [*****sjUx]: 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
Default region name [ap-south-1]:
Default output format [json]:

C:\Users\Administrator>aws ec2 create-security-group --group-name awsclitraining --description "test sg from cli"
{
  "GroupId": "sg-028026cc8df2faaeb"
}

C:\Users\Administrator>
```

Security Group Name You can Give Any

Description you can give any

Note Down GroupID

Now Security Group has been created we will go to GUI mode and to check security group is available or not.

1. From EC2 Dashboard Click on Security Gorup.
2. Here is our security group detail we have group name awsclitraining and groupid is also matching.

EC2 Dashboard

Name	Group ID	Group Name	VPC ID	Owner	Description
sg-028026cc8df2faaeb	awsclitraining	vpc-0236f2364842a7653	369277359072	test sg from cli	
sg-0530e9e173cad73bb	default	vpc-0236f2364842a7653	369277359072	default VPC security group	

```
C:\Users\Administrator>aws configure
AWS Access Key ID [*****IMBA]: AKIAJ3AJAWULIRE3UVYQ
AWS Secret Access Key [*****sjUx]: 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
Default region name [ap-south-1]:
Default output format [json]:

C:\Users\Administrator>aws ec2 create-security-group --group-name awsclitraining --description "test sg from cli"
{
  "GroupId": "sg-028026cc8df2faaeb"
}

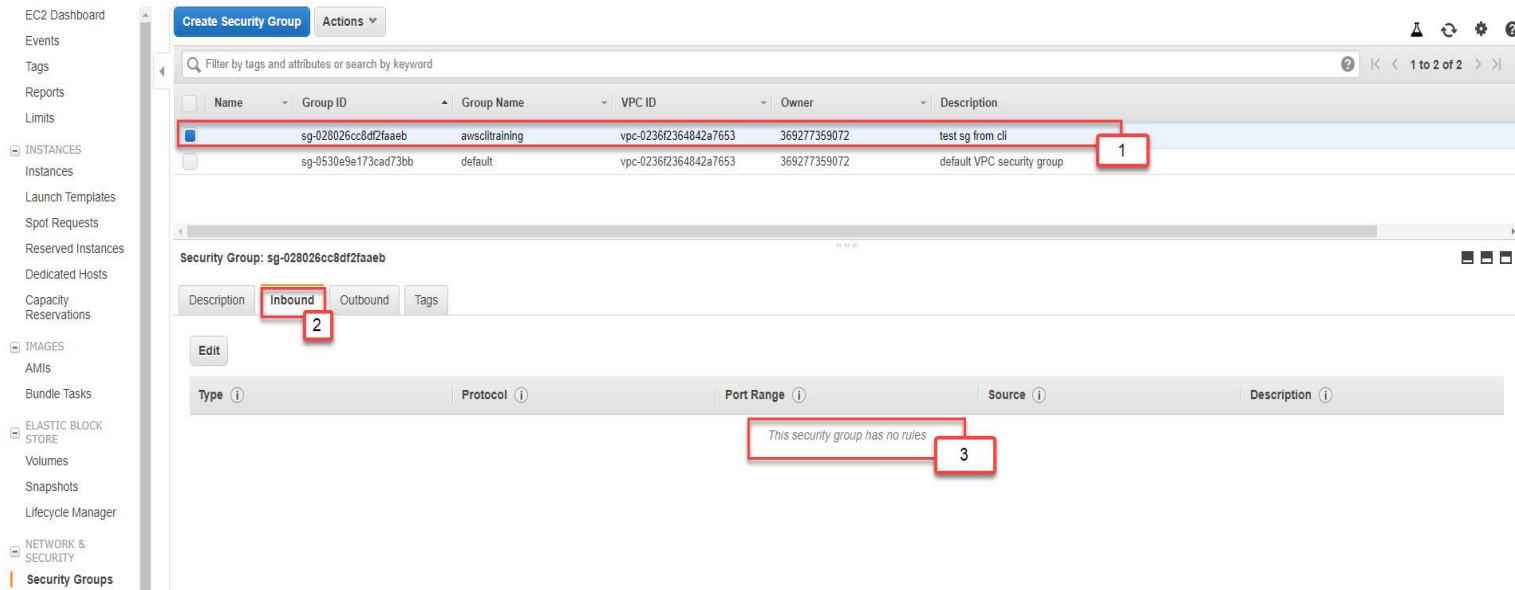
C:\Users\Administrator>
```

Note Down GroupID

# AWS CLI

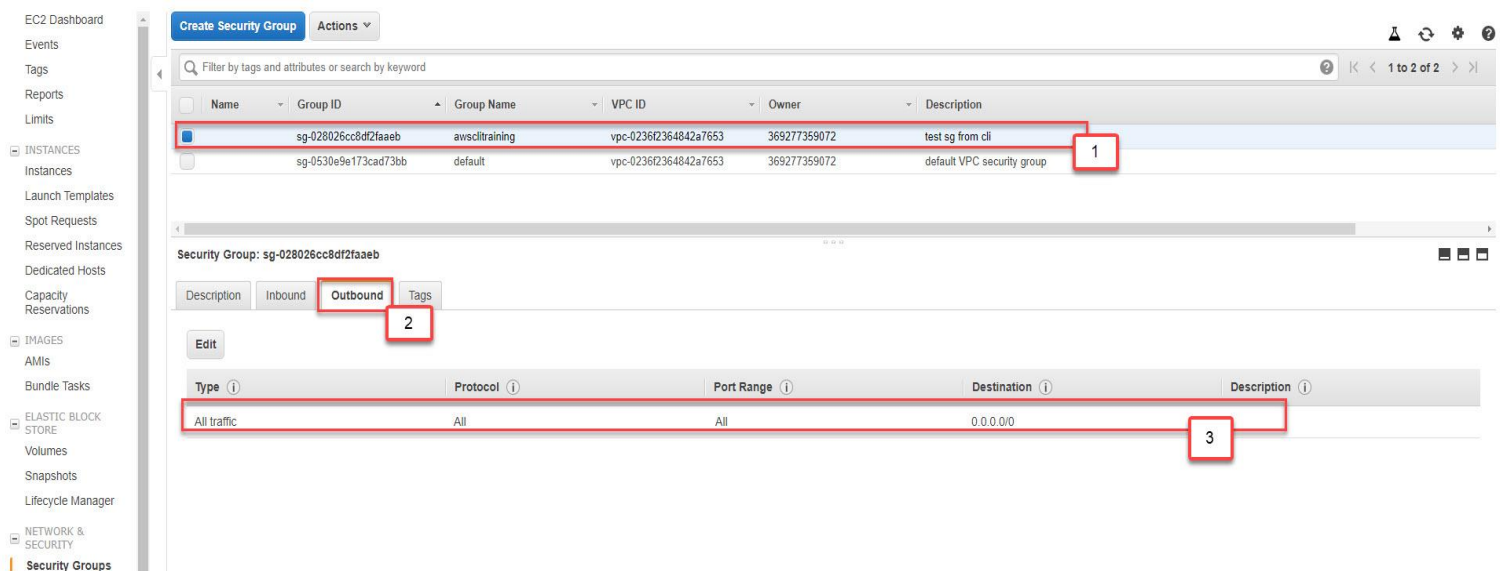
Now we will check if there are any inbound rules in our newly created group.

1. Select Group
2. Select Inbound
3. Here we don't have any security rule.



Now we will check if there are any outbound rules in our newly created group.

1. Select Group
2. Select outbound
3. Here we have rule allow all outbound traffic to any destination.



We have an outbound rule but we don't have any inbound rule, so we have to allow RDP (TCP Port 3389) so we can manage our EC2.

In the next step we will add an inbound rule to the security group.



# AWS CLI

Give following command

```
aws ec2 authorize-security-group-ingress --group-name awslitraining --protocol tcp --port 3389 --cidr 0.0.0.0/0
```

For error free practice copy above command from here and paste it at aws cli

```
C:\Users\Administrator>aws configure
AWS Access Key ID [*****IMBA]: AKIAJ3AJAWULIRE3UVYQ
AWS Secret Access Key [*****sjUx]: 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
Default region name [ap-south-1]:
Default output format [json]:

C:\Users\Administrator>aws ec2 create-security-group --group-name awslitraining --description "test sg from cli"
{
  "GroupId": "sg-028026cc8df2faaeb"
}

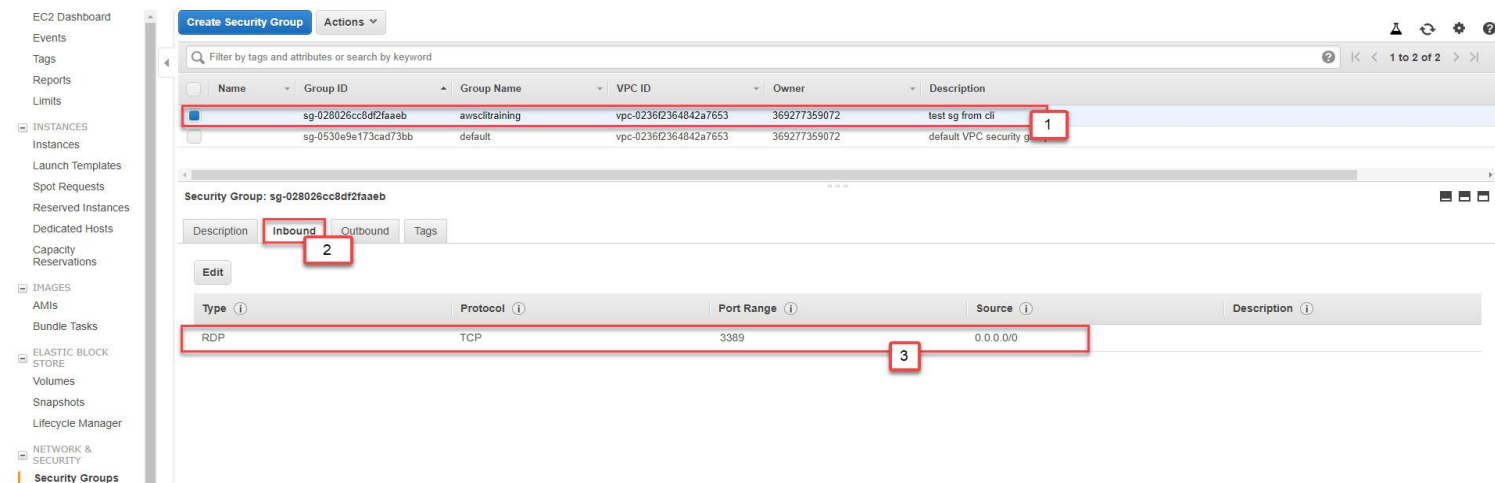
C:\Users\Administrator>aws ec2 authorize-security-group-ingress --group-name awslitraining --protocol tcp --port 3389 --cidr 0.0.0.0/0
C:\Users\Administrator>
```

Security Group Name      Security Group Name      source

Now we will verify that rule is added or not.

1. Select Group
2. Select outbound
3. Here we have rule allow RDP inbound traffic to any source.

Note: If you have old windows open do not forget to refresh the window



Give following command to create security key for our ec2 instance.

```
aws ec2 create-key-pair --key-name cliKeyPair --query "KeyMaterial" --output text > clikeyPair.pem
```

For error free practice copy above command from here and paste it at aws cli

```
C:\Users\Administrator>aws ec2 create-key-pair --key-name cliKeyPair --query "KeyMaterial" --output text > clikeyPair.pem
C:\Users\Administrator>
```

Key Pairs Name      This file will be store in our PC

# AWS CLI

At this command prompt give dir command to verify clikeyPair.pem is there in our directory.

Note down location of pem file.

```
C:\Users\Administrator>dir
Volume in drive C has no label.
Volume Serial Number is A8E0-D863

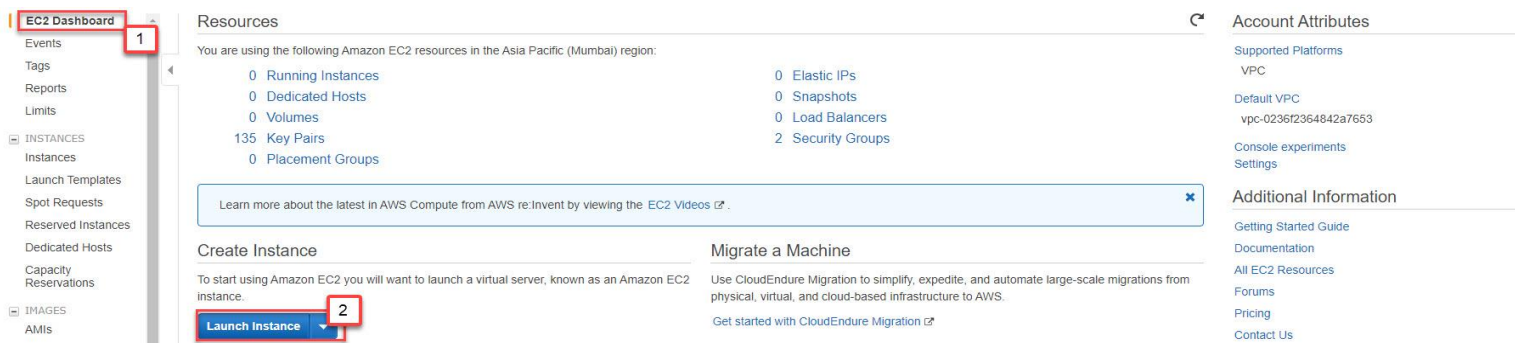
Directory of C:\Users\Administrator

11-10-2019 13:59 <DIR>          .
11-10-2019 13:59 <DIR>          ..
12-07-2019 19:38 <DIR>          .aws
04-10-2019 09:58 <DIR>          3D Objects
05-10-2019 09:21 <DIR>
16-09-2019 20:09 <DIR>
11-10-2019 13:59 1,694 clikeyPair.pem
```

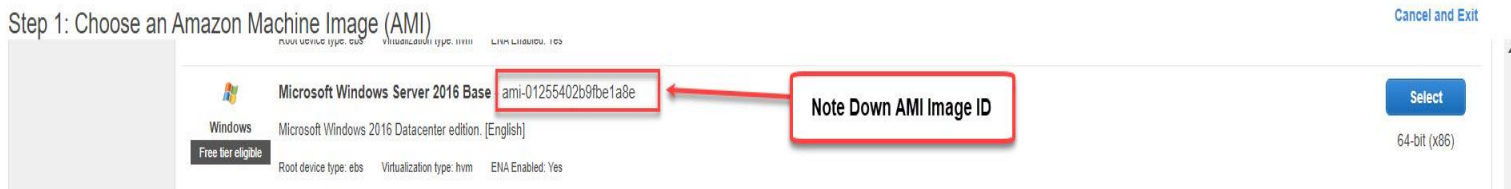
All set now we can create EC2 using above security group and key pairs. But before we create security group we have to note down AMI image ID and subnet ID so let's find out AMI ID of Windows Server 2016 base image.

Click On EC2 Dashboard

Click Launch Instance

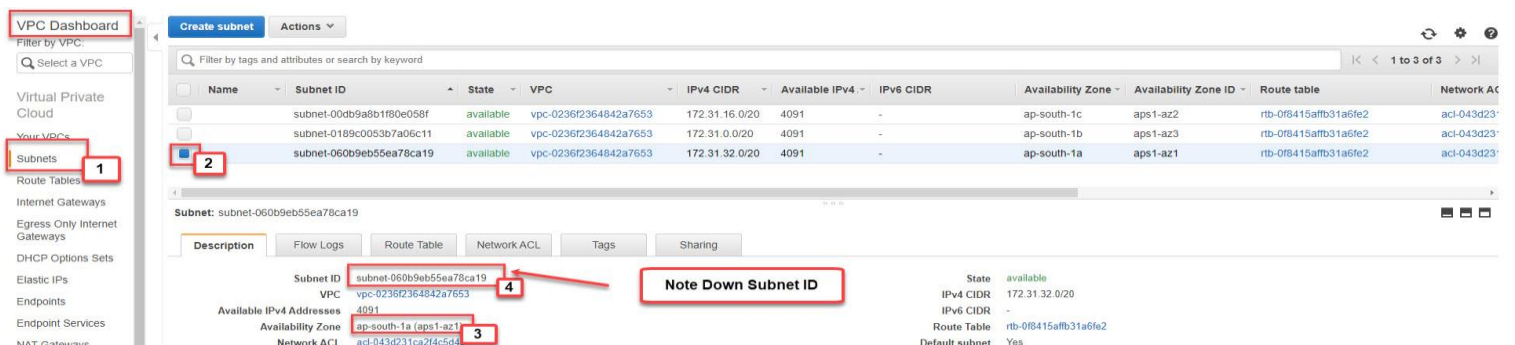


Select any AMI image for Your ec2 and Note down Image id copy and paste into wordpad



Now we will copy subnet id in which we are going to create our EC2 Instance.

1. From VPC Dashboard Click Subnets
2. Select Subnet
3. Make Sure subnet AZ
4. Copy and paste subnet id into wordpad file.



# AWS CLI

Give following command to create EC2 instance from CLI

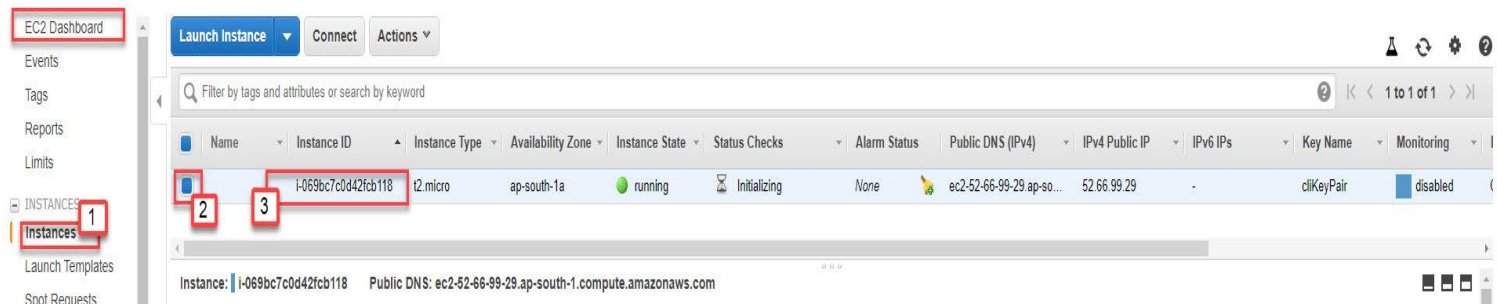
```
aws ec2 run-instances --image-id ami-01255402b9fbe1a8e --count 1 --instance-type t2.micro --key-name cliKeyPair --security-group-ids sg-028026cc8df2faaeb --subnet-id subnet-060b9eb55ea78ca19
```

For error free practice copy above command from here and paste it at aws cli do not forget to edit ami id, security group id and subnet id as per your lab.



Verify New EC2 has been Created Go to EC2 has been Created.

1. From EC2 Dashboard Click Instances
2. Here is our newly Created Instance Select it
3. Note Down Instance ID



Wait for some time till instance be ready you can login to verify we are able to login using same private key we created earlier.

To Stop Running EC2 instance we can use following command.

```
aws ec2 stop-instances --instance-ids i-069bc7c0d42fcb118
```

For error free practice copy above command from here and paste it at aws cli do not forget to edit ami id, security group id and subnet id as per your lab.



Go to GUI and Check Status of Instance it must be in Stop State.

# AWS CLI

To Start Running EC2 instance we can use following command.

```
aws ec2 start-instances --instance-ids i-069bc7c0d42fcb118
```

For error free practice copy above command from here and paste it at aws cli do not forget to edit ami id, security group id and subnet id as per your lab.

```
C:\Users\Administrator>aws ec2 start-instances --instance-ids i-069bc7c0d42fcb118cb118
```

EC2 Instance ID Noted in  
Previous Step

Go to GUI and Check Status of Instance it must be in Start State.

To Terminate EC2 instance we can use following command.

```
aws ec2 terminate-instances --instance-ids i-069bc7c0d42fcb118
```

For error free practice copy above command from here and paste it at aws cli do not forget to edit ami id, security group id and subnet id as per your lab.

```
C:\Users\Administrator>aws ec2 terminate-instances --instance-ids i-069bc7c0d42fcb118
```

EC2 Instance ID Noted in  
Previous Step

Go to GUI and Check Status of Instance it must be Terminated.