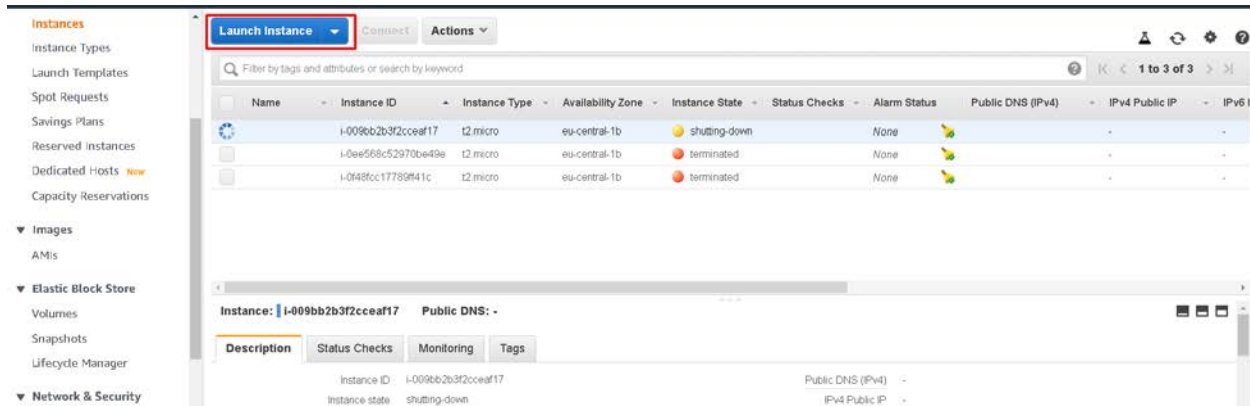
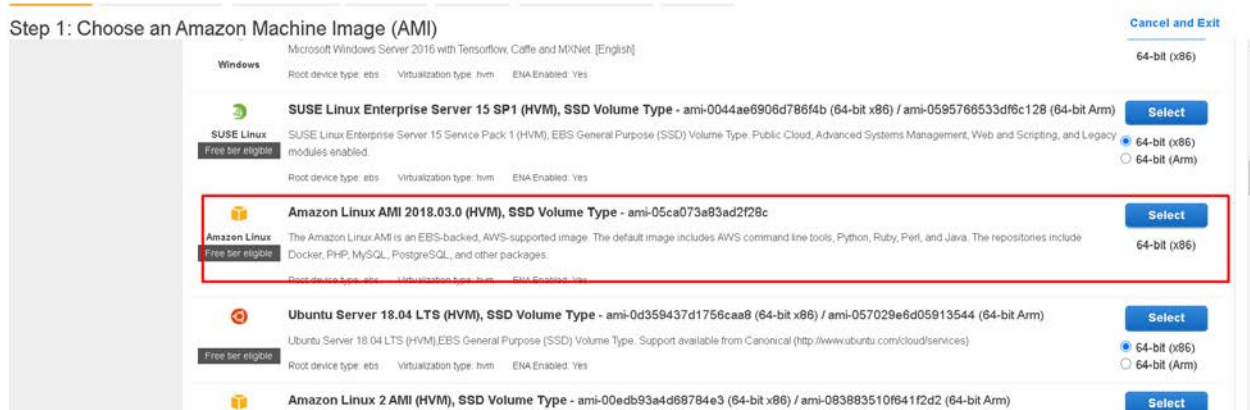


## Launch an instance and replace the default server page content

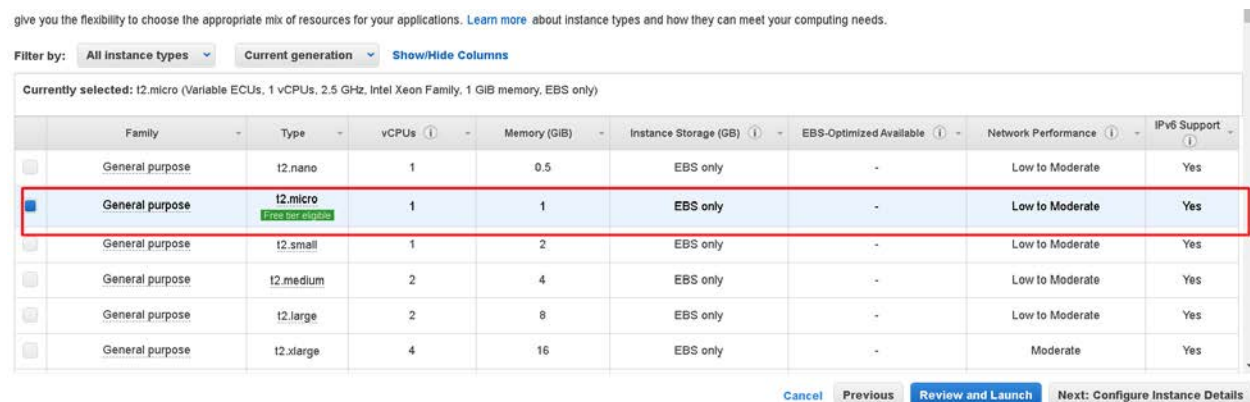
1. Go to AWS Console EC2 section and click Launch Instances



2. From the list of AMIs choose Amazon Linux AMI 2018 – its free tier



3. Choose General Purpose t2.micro instance



4. Make sure the Auto-assign Public IP is Enabled
  - IAM Role – here you can connect EC2 with S3 with the role that you have created in IAM

### 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  [Launch into Auto Scaling Group](#)

Purchasing option ☐ Request Spot instances

Network  [Create new VPC](#)

Subnet  [Create new subnet](#)

Auto-assign Public IP

Placement group ☐ Add instance to placement group

Capacity Reservation  [Create new Capacity Reservation](#)

IAM role  [Create new IAM role](#)

Shutdown behavior

Stop - Hibernate behavior ☐ Enable hibernation as an additional stop behavior

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

5. On the same page scroll down and add the following commands :

```
#!/bin/bash
sudo yum update -y
sudo yum install -y httpd24 php56 php56-mysqlnd
sudo service httpd start
```

### Step 3: Configure Instance Details

Instance type  [Additional charges may apply when launching Dedicated instances.](#)

T2/T3 Unlimited ☐ Enable [Additional charges may apply](#)

File systems [Add file system](#) [Create new file system](#)

Advanced Details

Metadata accessible

Metadata version

Metadata token response hop limit

User data ☒ As text ☐ As file ☐ Input is already base64 encoded

```
#!/bin/bash
sudo yum update -y
sudo yum install -y httpd24 php56 php56-mysqlnd
sudo service httpd start
```

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

## 6. Just skip the next page

### 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-04f43736c550f372f	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

[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.

## 7. Optionally add some tags

### Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes
Department	Software Development	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[Add another tag](#) (Up to 50 tags maximum)

## 8. Edit the security group and add new rule to allow HTTP access

### 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

Security group name:   
Description:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop
HTTP	TCP	80	Custom 0.0.0.0/0, ::0	e.g. SSH for Admin Desktop

[Add Rule](#)



#### 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.

Change the security group description?

9. If you don't already have a key, create a new one and download it to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Create a new key pair

Key pair name

myKey

Download Key Pair

You have to download the **private key file** (\*.pem file) before you can continue. Store it in a secure and accessible location. You will not be able to download the file again after it's created.

Cancel Launch Instances

10. From the main page copy the public IP and navigate to it in the browser

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6
	i-009bb2b3f2ccea1f17	t2.micro	eu-central-1b	terminated		None			
	i-0367fae1b7ad53fd1	t2.micro	eu-central-1b	running	2/2 checks ...	None	ec2-18-196-145-170.eu-central-1.compute.amazonaws.com	18.196.145.170	

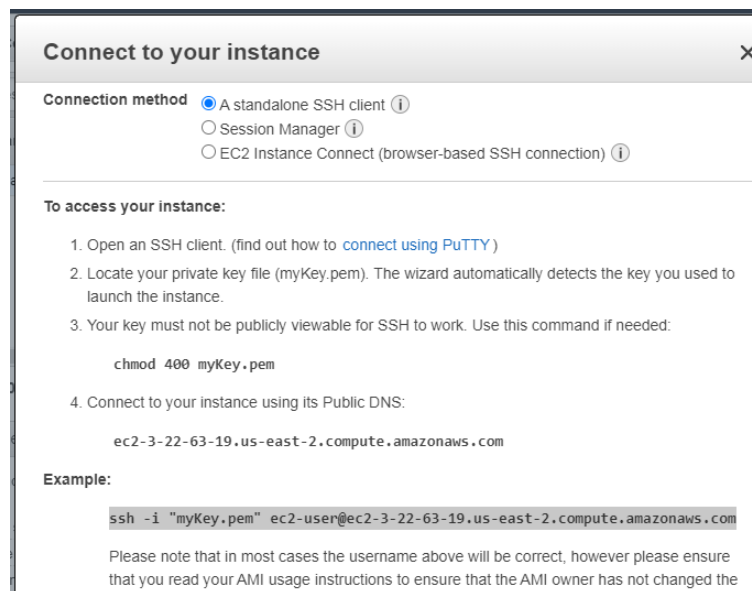
Instance: i-0367fae1b7ad53fd1 Public DNS: ec2-18-196-145-170.eu-central-1.compute.amazonaws.com

Instance ID	i-0367fae1b7ad53fd1	Public DNS (IPv4)	ec2-18-196-145-170.eu-central-1.compute.amazonaws.com
Instance state	running	IPv4 Public IP	18.196.145.170
Instance type	t2.micro	IPv6 IPs	-
Finding	Opt-in to AWS Compute Optimizer for recommendations. <a href="#">Learn more</a>	Elastic IPs	
Private DNS	ip-172-31-40-160.eu-central-1.compute.internal	Availability zone	eu-central-1b

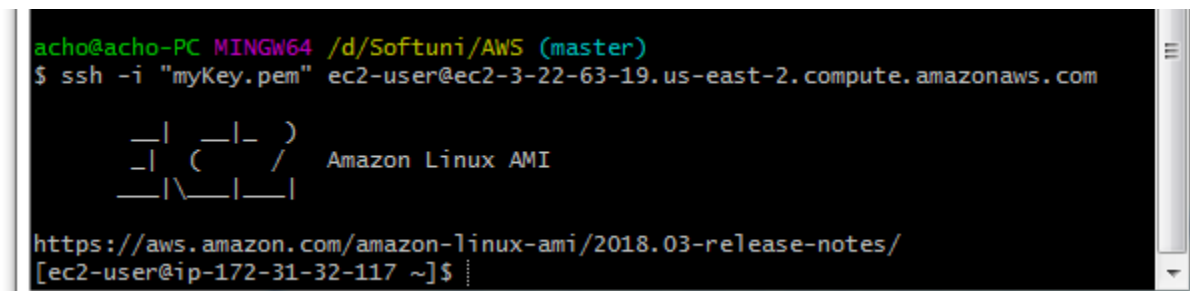
Copy-Paste public DNS-a to open the below page



Click on Connect (to instance). Open gitbash and navigate to the folder. Copy-paste first the `chmod 400 myKey` command and then the ssh key (in gitbash).



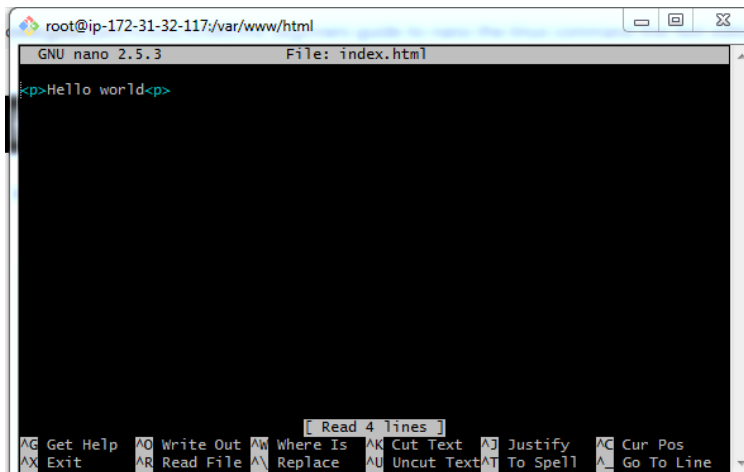
Results in the below:



Commands to be entered in gitbash:

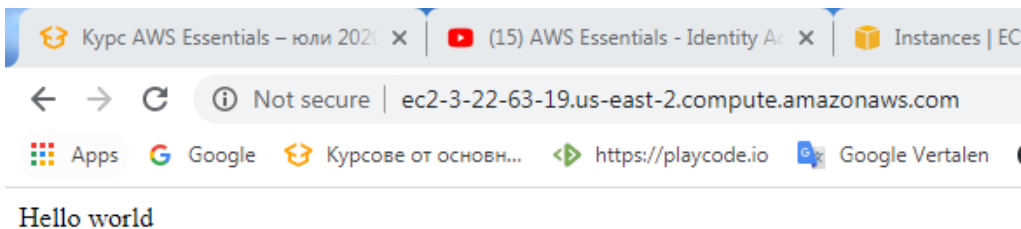
```
sudo su
cd /var/www/html – navigira do html-a
clear
nano index.html
```

After the last command the below opens – fill in the html to replace the default page



```
ctrl+x
Y
Enter
```

Now the default page content is replaced.



Terminate your instance – Actions – Instance State - Terminate

Link with S3 Actions – Instance Setting – Attach IAM Role

IAM => Roles=> Create Role

Click on EC2=>Next

Search for S3 full access and select it, create role.