

# AWS – EC2 Instance

## Lab manual – EC2 Instance

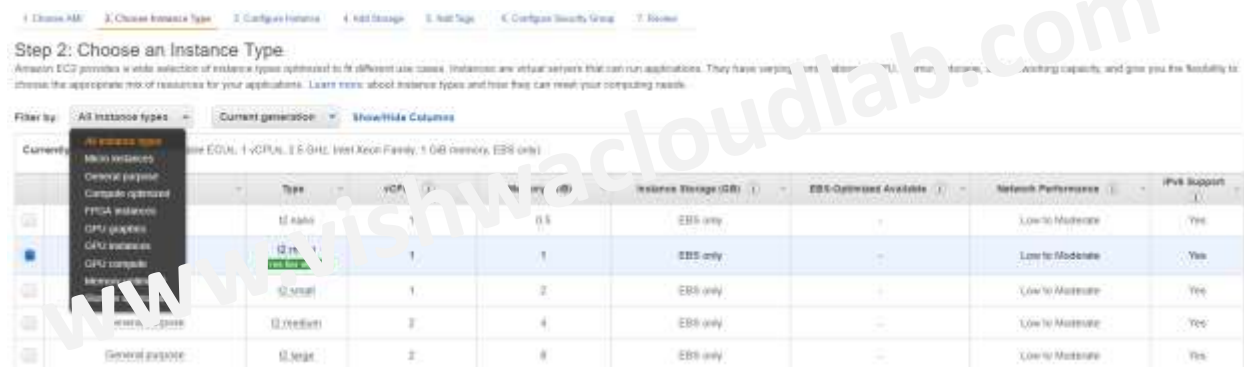
### 1. Select the AMI image

Options → AMI, Custom AMI, AWS Marketplace, Community AMI



### 2. Select “instance Type”

Options → CPU, RAM, Instance storage, Network performance.



Type → t2, t3, m2, c3, c4 .....

### 3. Instance Configuration

## AWS – EC2 Instance

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### 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

Number of instances  [Launch into Auto Scaling Group](#)

Purchasing option ☐ Request Spot instances

Network  [Create new VPC](#)

Subnet  [Create new subnet](#)  
507 IP Addresses available

Auto-assign Public IP

Auto-assign IPv6 IP

Placement group ☐ Add instance to placement group

IAM role  [Create new IAM role](#)

Shutdown behaviour

Enable termination protection ☐ Protect against accidental termination

Monitoring ☐ Enable CloudWatch detailed monitoring  
[Additional charges apply.](#)

Tenancy   
[Additional charges will apply for dedicated tenancy](#)

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

Options →

Number of Instance

Networking

Shutdown Behaviour

Tenancy

T2 unlimited

Network interfaces

| Device                     | Network Interface     | Subnet          | Primary IP  | Secondary IP addresses | IPv6 IPs               |
|----------------------------|-----------------------|-----------------|-------------|------------------------|------------------------|
| eth0                       | New network interface | subnet-0b617f71 | Auto-assign | <a href="#">Add IP</a> | <a href="#">Add IP</a> |
| <a href="#">Add Device</a> |                       |                 |             |                        |                        |

We could assign an “Static Private IPv4” or “static Public IPv6” (allocated by AWS)

Also we can add one more network adapter.

### 4. Add Storage

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance storage options in Amazon EC2.

| Volume Type | Device    | Snapshot | Volume Type               | IOPS | Throughput (MB/s) | Delete on Termination    | Encrypted     |
|-------------|-----------|----------|---------------------------|------|-------------------|--------------------------|---------------|
| Root        | /dev/xvda | snap: No | General Purpose SSD (GP2) | 100  | 100               | <input type="checkbox"/> | Not Encrypted |

[Add New Volume](#)

Option →

Volume Size → For root volume we can go upto 2TB, and for additional data volume upto 16TB

Volume Type →

General Purpose SSD → AWS provides, 3 IOPS for every 1 GB, MAX IOPS -- 10000

Provisioned SSD → 50 IOPS are provided for every 1GB. Max IOPS -- 32000

Delete on Termination → do u want to delete the Disk once the Instance is terminated.

Note: -- Best practice “keep it Unchecked” if you need the volumes in the future for ever.

Encryption → Root volume CANNOT be encrypted.

Data volume can be , either AWS Encryption or custom Encryption

### 5. Add 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 (127 characters maximum) | Value (255 characters maximum) | Instances                           | Volumes                             |
|------------------------------|--------------------------------|-------------------------------------|-------------------------------------|
| Name                         | VKS01                          | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Project                      | JS                             | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

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

Provide an proper TAGS , that would be very useful on a long run.

Think we are managing 1000 VM's and you have to manage it.

### 6. Add Security

The screenshot shows the 'Configure Security Group' step in the AWS Management Console. It includes a breadcrumb trail at the top: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags, 6. Configure Security Group, 7. Review. Below the breadcrumb, there's a section titled 'Step 6: Configure Security Group' with a description of security groups. The 'Assign a security group' section has two options: 'Create a new security group' (selected) and 'Select an existing security group'. The 'Create a new security group' section shows a form with 'Security group name' (launch-wizard-3) and 'Description' (launch-wizard-3 created 2018-08-23T12:46:29+05:30). Below this is a table of rules with columns: Type, Protocol, Port Range, Source, and Description. The table shows a single rule for SSH (Type: Inbound, Protocol: TCP, Port Range: 22, Source: 0.0.0.0, Description: e.g. SSH for Admin Desktop). There is an 'Add Rule' button and a warning message at the bottom: 'Warning: 0.0.0.0 will allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.'

The above is the inbound traffic that is listed for this instance. (SSH is allowed for Linux OS, to be access from outside), we would talk about this more in the “AWS SECURITY” session.

By Default ALL TRAFFIC is ALLOWED for outbound traffic.

### 7. Review

The screenshot shows the 'Review Instance Launch' step in the AWS Management Console. It includes a breadcrumb trail at the top: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags, 6. Configure Security Group, 7. Review. Below the breadcrumb, there's a section titled 'Step 7: Review Instance Launch' with a description of the review process. The 'Review Instance Launch' section shows a warning message: 'Warning: Improve your instances' security. Your security group, launch-wizard-3, is open to the world. Your instance may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups.' Below this is a section titled 'AMI Details' showing 'Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type - ami-0f8a160777867'. The 'Instance Type' section shows a table with columns: Instance Type, ECUs, vCPUs, Memory (GB), Storage, EBS-Optimized Available, and Network Performance. The table shows a single row for 't2.micro' with values: Variable, 1, 1, 8 GB, 0, and Low to Moderate. The 'Security Groups' section shows a table with columns: Type, Protocol, Port Range, Source, and Description. The table shows a single row for SSH (Type: Inbound, Protocol: TCP, Port Range: 22, Source: 0.0.0.0, Description: e.g. SSH for Admin Desktop).

### 8. Key Selection

For EC2 Instance we would need to assign an “KEY” to access it. This would be the password. There is an DEFAULT “Username” for every IMAGE that we select in the beginning.

The key has 2 parts, Public and Private.

The private key is downloadable only ONCE and AWS DOES NOT STORAGE it.



Until we download the key pair for the first time, “Launch Instance” button does not get activated.

After the download of the key, Click on “Launch”.

Output →

The screenshot displays the AWS Management Console interface for an EC2 instance. At the top, there are buttons for 'Launch Instance', 'Connect', and 'Actions'. Below this is a search bar and a table listing instances. The instance 'WS01' with ID 'i-0c5cc5791d104e756' is highlighted. Below the table, the instance details are shown for 'i-0c5cc5791d104e756 (WS01)' with a private IP of '10.20.0.152'. The 'Description' tab is active, showing various attributes:

- Instance ID: i-0c5cc5791d104e756
- Instance state: running
- Instance type: t2.micro
- Elastic IPs: None
- Availability zone: us-east-1a
- Security groups: launch-wizard-3, sg-01234567
- Scheduled events: No scheduled events
- AMI ID: ami-01234567
- Platform: Linux
- OS: Amazon Linux 2
- Lab-key: Lab-key1
- EC2-optimized: False
- Root device type: ebs
- Root device: /dev/xvda
- Block devices: /dev/xvda
- Elastic GPU: None
- Elastic GPU type: None
- Elastic GPU status: None
- Public DNS (IPv4): None
- Private DNS: ip-10-20-0-152.ec2.internal
- Private IPs: 10.20.0.152
- Secondary private IPs: None
- VPC ID: vpc-01234567
- Subnet ID: subnet-01234567
- Network interfaces: eni0
- SourceDestCheck: True
- T2/T3 Unlimited: Disabled
- Owner: AWS
- Launch time: Aug 1, 2023 (less than one hour)
- Termination protection: False
- Lifecycle: normal
- Monitoring: basic
- Alarm status: None
- Kernel ID: None
- RAM disk ID: None
- Placement group: None