

# LAB: Start and Stop an EC2 Instance

## You need:

- An active AWS Account

**Duration of the Lab:** 15 Minutes.

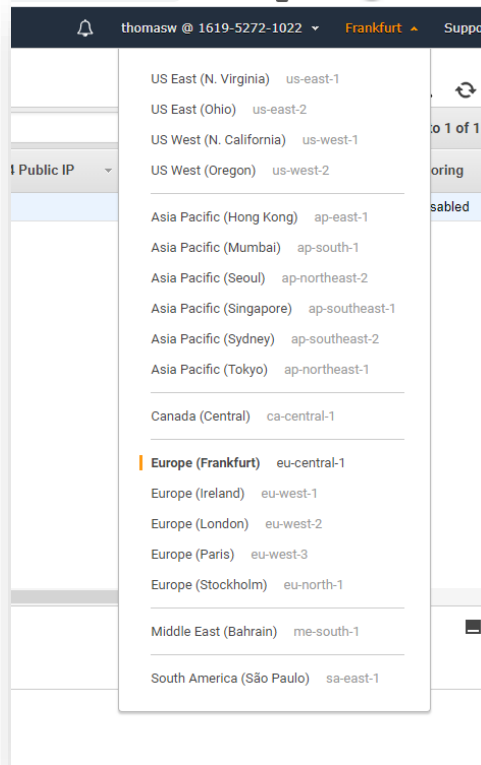
**Difficulty:** Very easy.

## Contents

Select the right Region .....	2
Create a new OpenSSH KeyPair.....	2
Start a new EC2 Instance.....	4
Choose an AMI .....	5
Choose and Instance Type.....	6
Configure Instance Details.....	6
Security Group.....	7
Start and Choose a KeyPair .....	7
SSH Into your Instance .....	8
Cleanup.....	10
Remove the Instance again .....	10

## Select the right Region

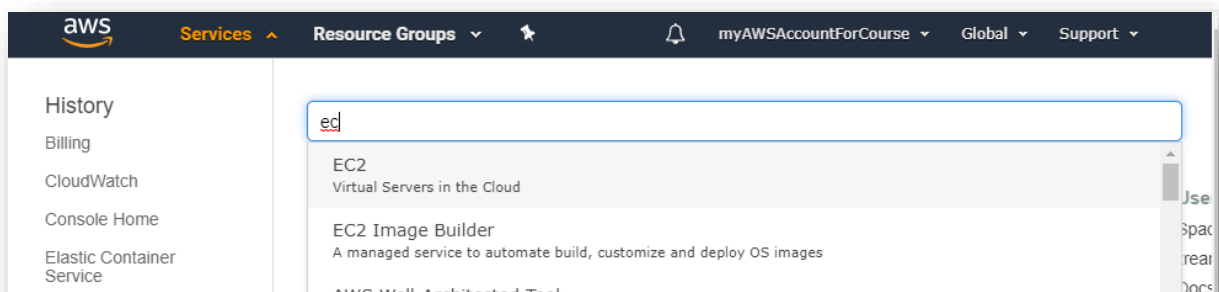
From the Region Dropdown select a region that is near you. I will work with the Europe (Frankfurt) Region throughout the course, because I am in Austria. If you are in a different Region then make sure you remember the short name (e.g. eu-central-1) and substitute it throughout the course with the right region whenever necessary (e.g. CodeCommit)



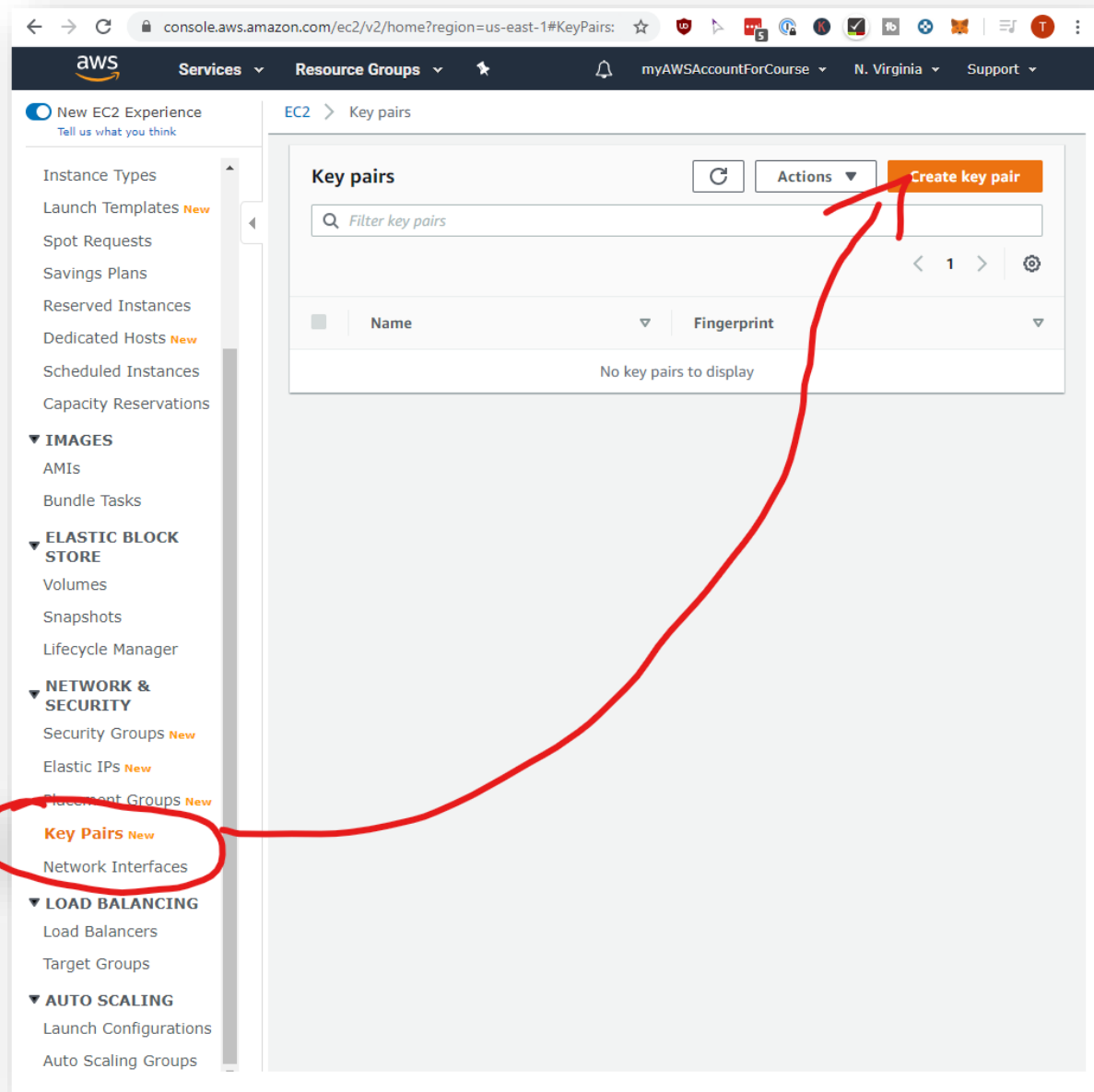
## Create a new OpenSSH Keypair

In this lab you are going to start your first EC2 Instance. Before we do this, we have to create a new KeyPair. The KeyPair is used to connect to your EC2 Instance securely.

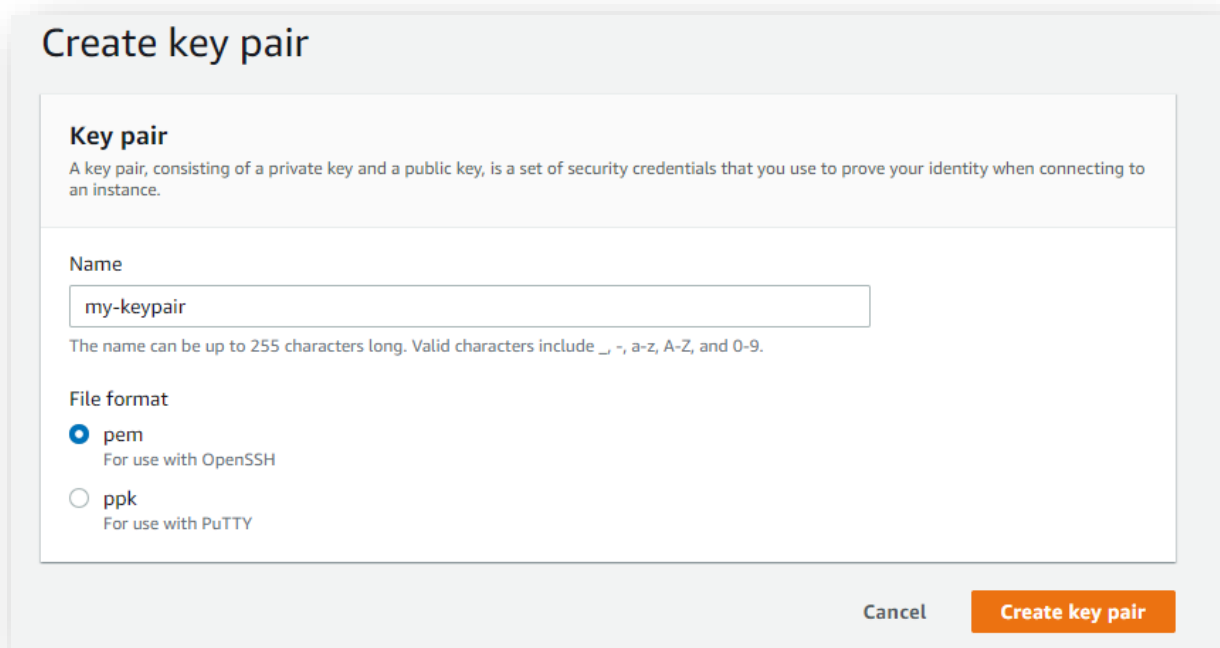
Open the EC2 Dashboard:



Scroll down until you see “Key Pairs”:

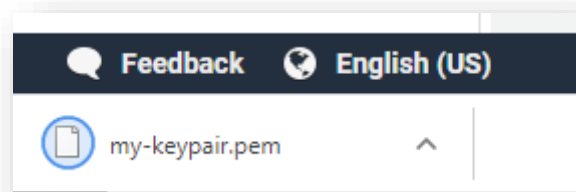


Click on Create Key Pair. Give it a Name and choose pem, because we are going to use OpenSSH for the rest of the tutorial. If you already know that you will use PuTTY then download ppk. Note: You can also use tools to convert a private key in pem-format to a ppk-format using PuttyGen. If all of this doesn't tell you anything, then simply follow along.



The screenshot shows the 'Create key pair' interface in the AWS Management Console. At the top, the title 'Create key pair' is displayed. Below it, a section titled 'Key pair' explains that a key pair consists of a private key and a public key used for authentication. The 'Name' field contains 'my-keypair', with a note stating the name can be up to 255 characters long and includes specific character restrictions. Under 'File format', the 'pem' option is selected (marked with a blue dot), indicating it is for use with OpenSSH, while the 'ppk' option is unselected (marked with a grey dot) and for use with PuTTY. At the bottom right, there are two buttons: 'Cancel' and 'Create key pair' (highlighted in orange).

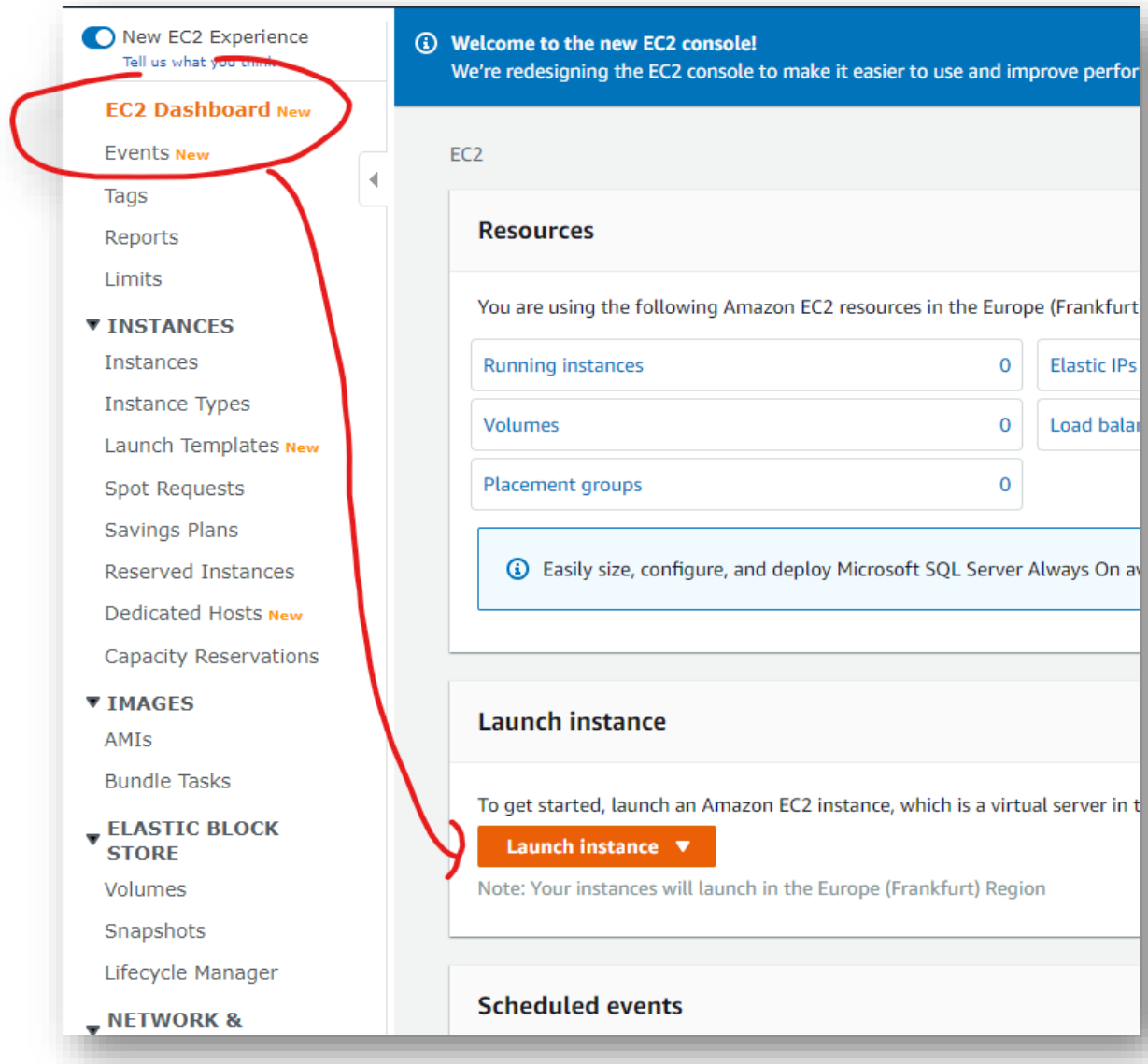
When you click “Create Key Pair” it will automatically download the file:



Store this file somewhere *safe*! You will need this throughout the course.

## Start a new EC2 Instance

Now you are ready to start your first instance. Go back to the dashboard:



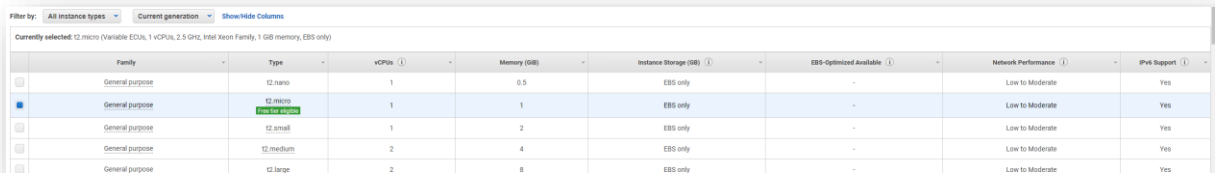
## Choose an AMI

Then choose an AMI – an Amazon Machine Image. I choose the Amazon Linux AMI, the first in the list:



## Choose and Instance Type

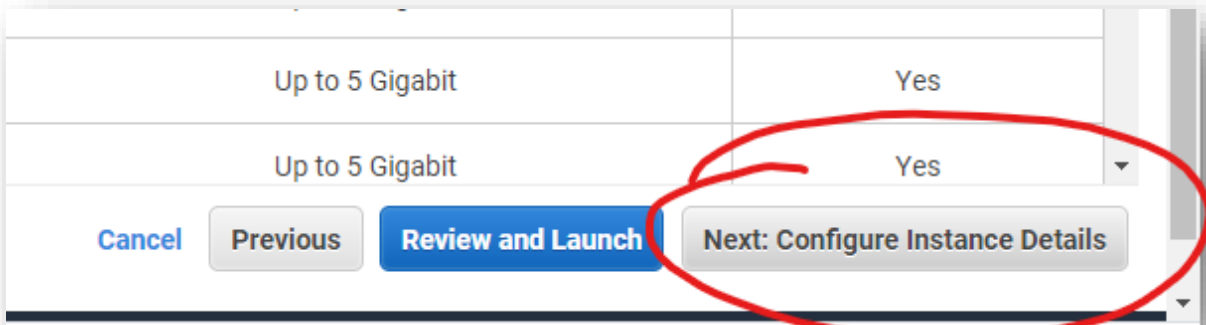
Next choose an Instance Type you want this image to be run on. If you want keep it free, then simply choose the t2.micro instance, which is free for 750 hours.



Family	Type	vCPUs	Memory (GB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
General purpose	t2.micro	1	1	EBS only	-	Low to Moderate	Yes
General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes

## Configure Instance Details

Next, we are going to configure the instance details. **Do not** click on “Review and Launch”, instead take it one step at a time.



Up to 5 Gigabit	Yes
Up to 5 Gigabit	Yes

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Instance Details](#)

Choose a specific subnet, make sure you get a public IP assigned and Terminate the instance on shutdown:

### 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

**Number of instances** ⓘ 1 [Launch into Auto Scaling Group](#) ⓘ

**Purchasing option** ⓘ ☐ Request Spot instances

**Network** ⓘ vpc-6570b40f (default) [Create new VPC](#)

**Subnet** ⓘ subnet-cfd47ba5 | Default in eu-central-1a [Create new subnet](#)  
4091 IP Addresses available

**Auto-assign Public IP** ⓘ Enable

**Placement group** ⓘ ☐ Add instance to placement group

**Capacity Reservation** ⓘ Open [Create new Capacity Reservation](#)

**IAM role** ⓘ None [Create new IAM role](#)

**Shutdown behavior** ⓘ Terminate

**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.](#)

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

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

▼ **Network interfaces** ⓘ

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface ▼	subnet-cfd47ba5 ▼	Auto-assign	<a href="#">Add IP</a>	<a href="#">Add IP</a>

[Add Device](#)

### Security Group

Next we configure a security group. A Security group is like a firewall sitting right in front of the instance. In this case we will let only port 22 through, so we can ssh into the instance:

**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

**Security group name:** launch-wizard-1

**Description:** launch-wizard-1 created 2020-03-18T16:14:13.060+01:00

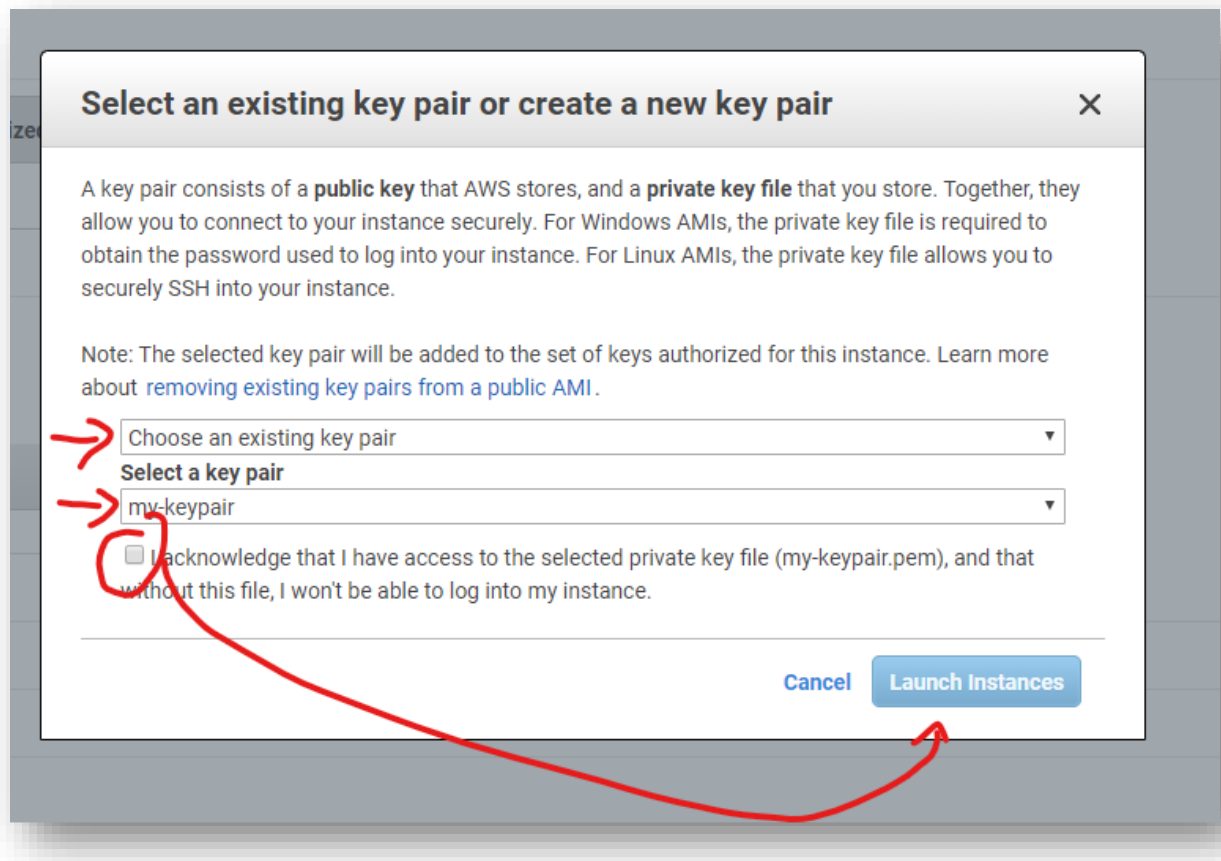
Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

[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.

### Start and Choose a KeyPair

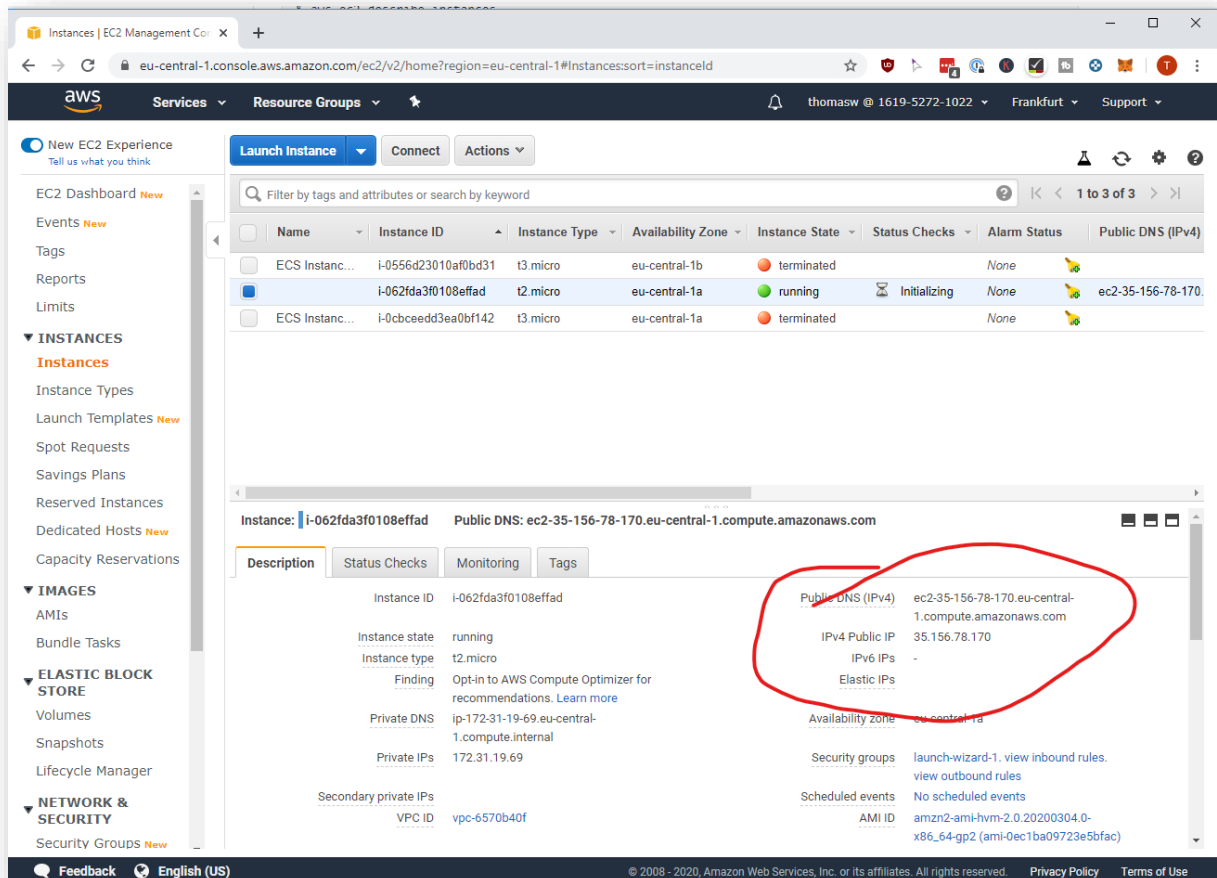
Then start the instance. A Popup should appear asking you which Key you want to use to login into the instance. Select the key you created before, check the checkbox and click "Launch Instance"



### SSH Into your Instance

Wait a bit until your instance has the "Instance State" running. Then a public DNS should appear including a public IP4 Address.





Copy the Public DNS. Open a terminal (Linux/Mac) or PowerShell (Windows) and enter the following command:

```
ssh -i ./my-keypair.pem ec2-user@[publicDNS]
```

Alternatively, you can click on the “Connect” button on the top of the Instance List and go through the tutorial.

The following output should appear:

```
Course 14 - Understanding Docker with AWS ECS and Fargate> ssh -i ~/.my-keypair.pem ec2-user@ec2-35-156-78-170.eu-central-1.compute.amazonaws.com
The authenticity of host 'ec2-35-156-78-170.eu-central-1.compute.amazonaws.com (35.156.78.170)' can't be established.
ECDSA key fingerprint is SHA256:xrSK0SDBkfJPYfRqr9DfuifSApVGIQ5sArOGXJ0uQ8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ec2-35-156-78-170.eu-central-1.compute.amazonaws.com,35.156.78.170' (ECDSA) to the list of known hosts.

  _ | _ | _ |
  _ | ( _ | _ | /
  _ | \ _ | _ |
      Amazon Linux 2 AMI

https://aws.amazon.com/amazon-linux-2/
No packages needed for security; 6 packages available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-19-69 ~]$
```

Note for Windows users: SSH should be included in Windows 10, if you need to install SSH first (if an error appears), then follow this guide: [https://docs.microsoft.com/en-us/windows-server/administration/openssh/openssh\\_install\\_firstuse#installing-openssh-from-the-settings-ui-on-windows-server-2019-or-windows-10-1809](https://docs.microsoft.com/en-us/windows-server/administration/openssh/openssh_install_firstuse#installing-openssh-from-the-settings-ui-on-windows-server-2019-or-windows-10-1809)

<https://vomtom.at>

Type in

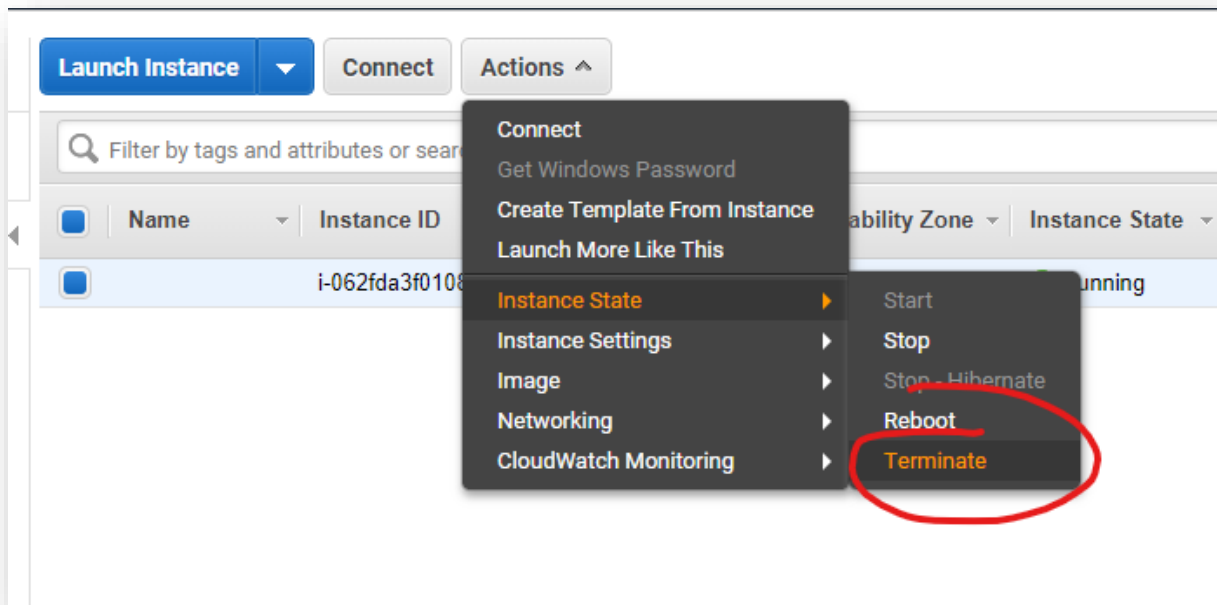
```
exit
```

Congratulations, you successfully connected to your first Instance!

## Cleanup

Remove the Instance again

Now remove the instance to clean up.



---

*Lab Finished*

---