LAB: Start and Stop an EC2 Instance

You need:

- An active AWS Account

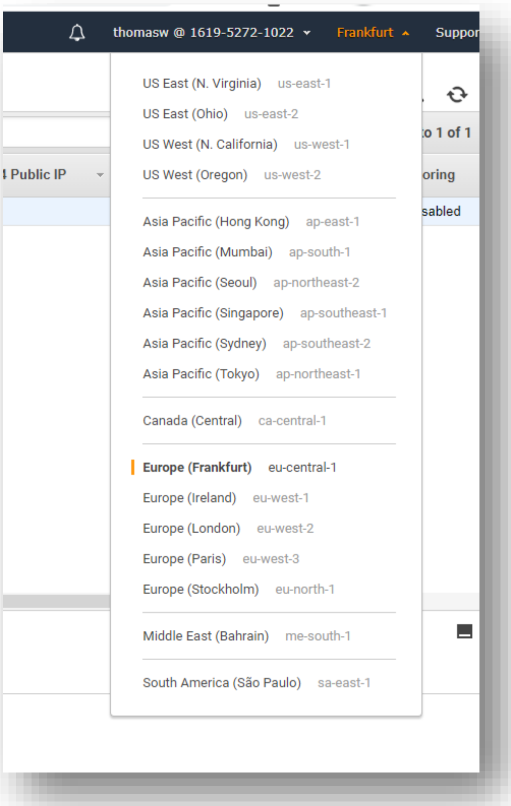
Duration of the Lab: 15 Minutes.

Difficulty: Very easy.

Contents

Select the right Region

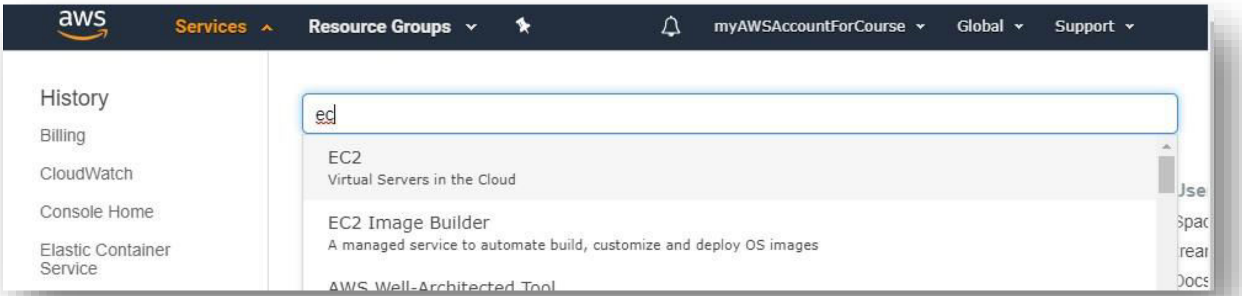
From the Region Dropdown select a region that is near you. I will work with the Europe (Frankfurt) Region throughout the course, because I am in Austria. If you are in a different Region then make sure you remember the short name (e.g. eu-central-1) and substitute it throughout the course with the right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


thomasw @ 1619-5272-1022
Frankfurt
Suppor
Public IP
o 1 of 1
oring
sabled
US East (N. Virginia) us-east-1
US East (Ohio) us-east-2
US West (N. California) us-west-1
US West (Oregon) us-west-2
Asia Pacific (Hong Kong) ap-east-1
Asia Pacific (Mumbai) ap-south-1
Asia Pacific (Seoul) ap-northeast-2
Asia Pacific (Singapore) ap-southeast-1
Asia Pacific (Sydney) ap-southeast-2
Asia Pacific (Tokyo) ap-northeast-1
Canada (Central) ca-central-1
Europe (Frankfurt) eu-central-1
Europe (Ireland) eu-west-1
Europe (London) eu-west-2
Europe (Paris) eu-west-3
Europe (Stockholm) eu-north-1
Middle East (Bahrain) me-south-1
South America (São Paulo) sa-east-1

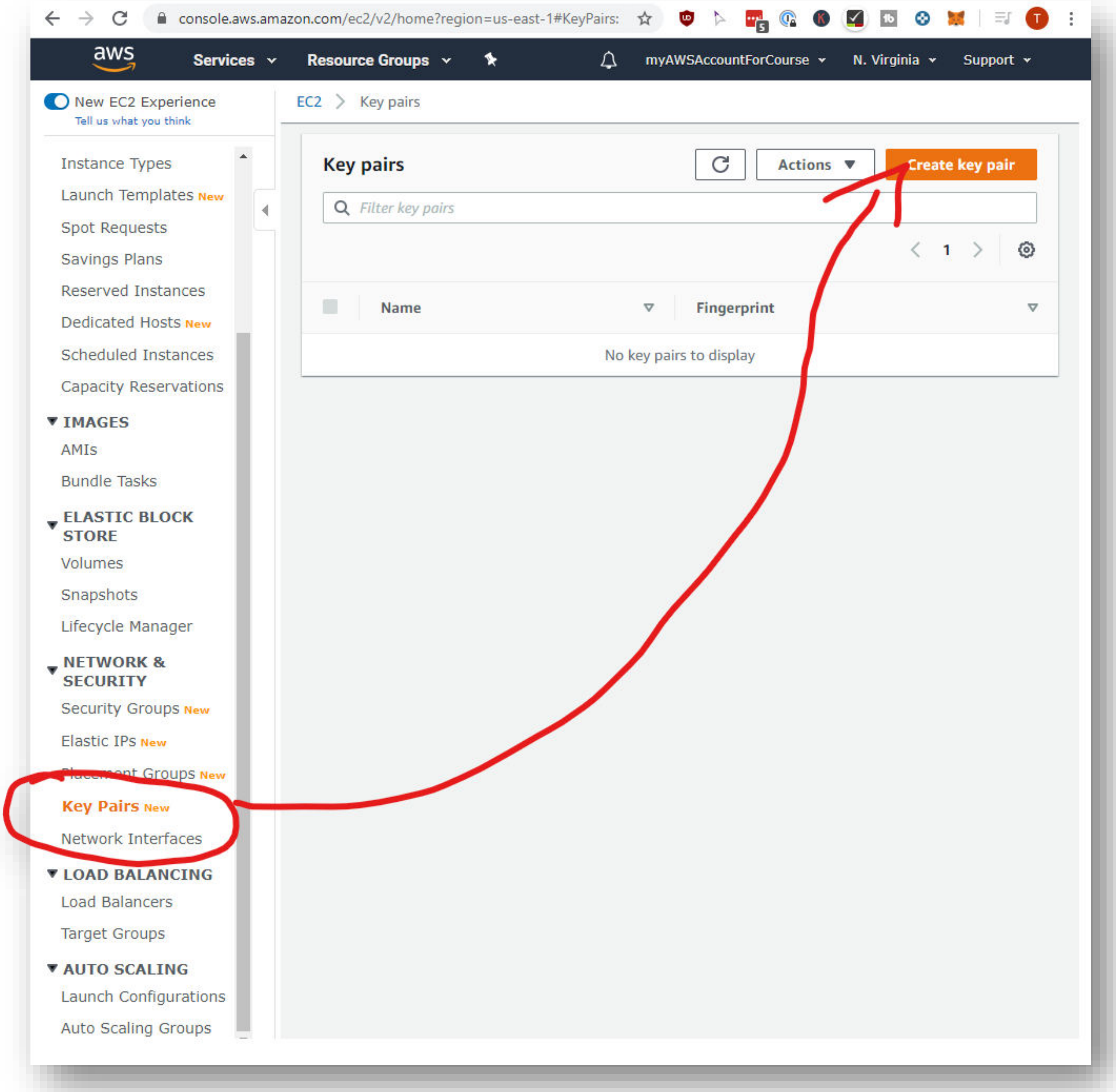
Create a new OpenSSH Keypair

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:

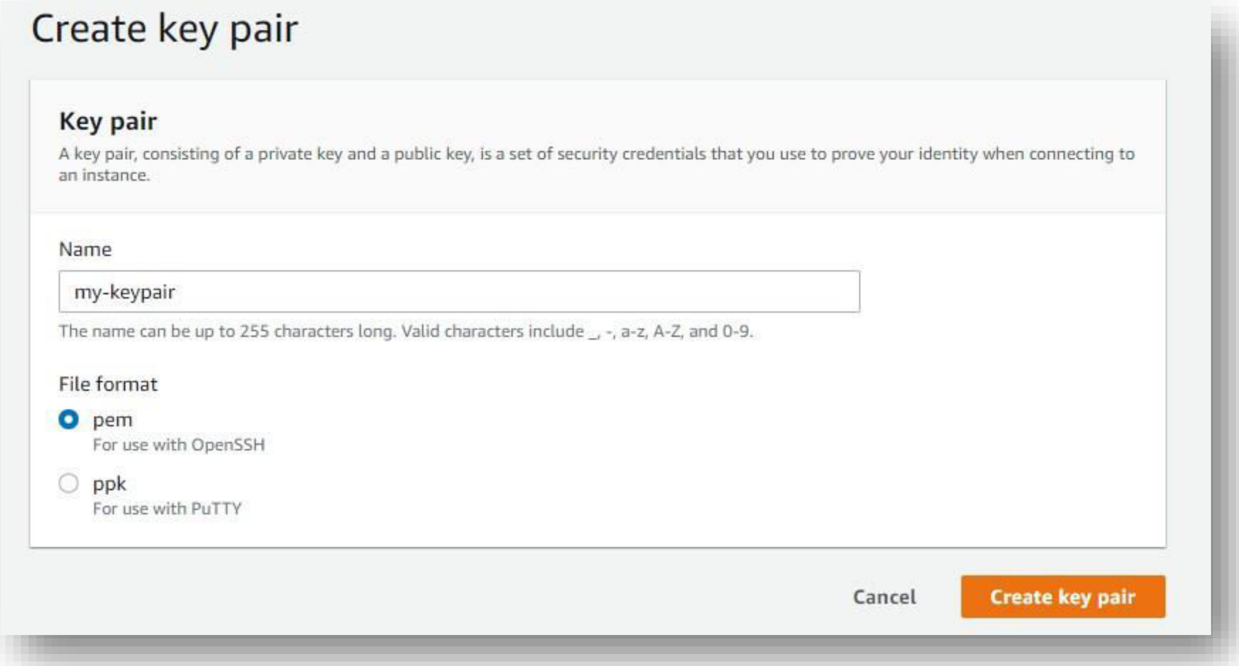

aws
Services
Resource Groups
myAWSAccountForCourse
Global
Support
History
Billing
CloudWatch
Console Home
Elastic Container Service
ec
EC2
Virtual Servers in the Cloud
EC2 Image Builder
A managed service to automate build, customize and deploy OS images
AWS Well-Architected Tool

Scroll down until you see “Key Pairs”:



No key pairs to display

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.



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

my-keypair

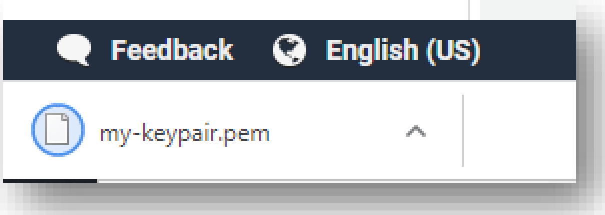
The name can be up to 255 characters long. Valid characters include _, -, a-z, A-Z, and 0-9.

File format

● pem
For use with OpenSSH

○ ppk
For use with PuTTY

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

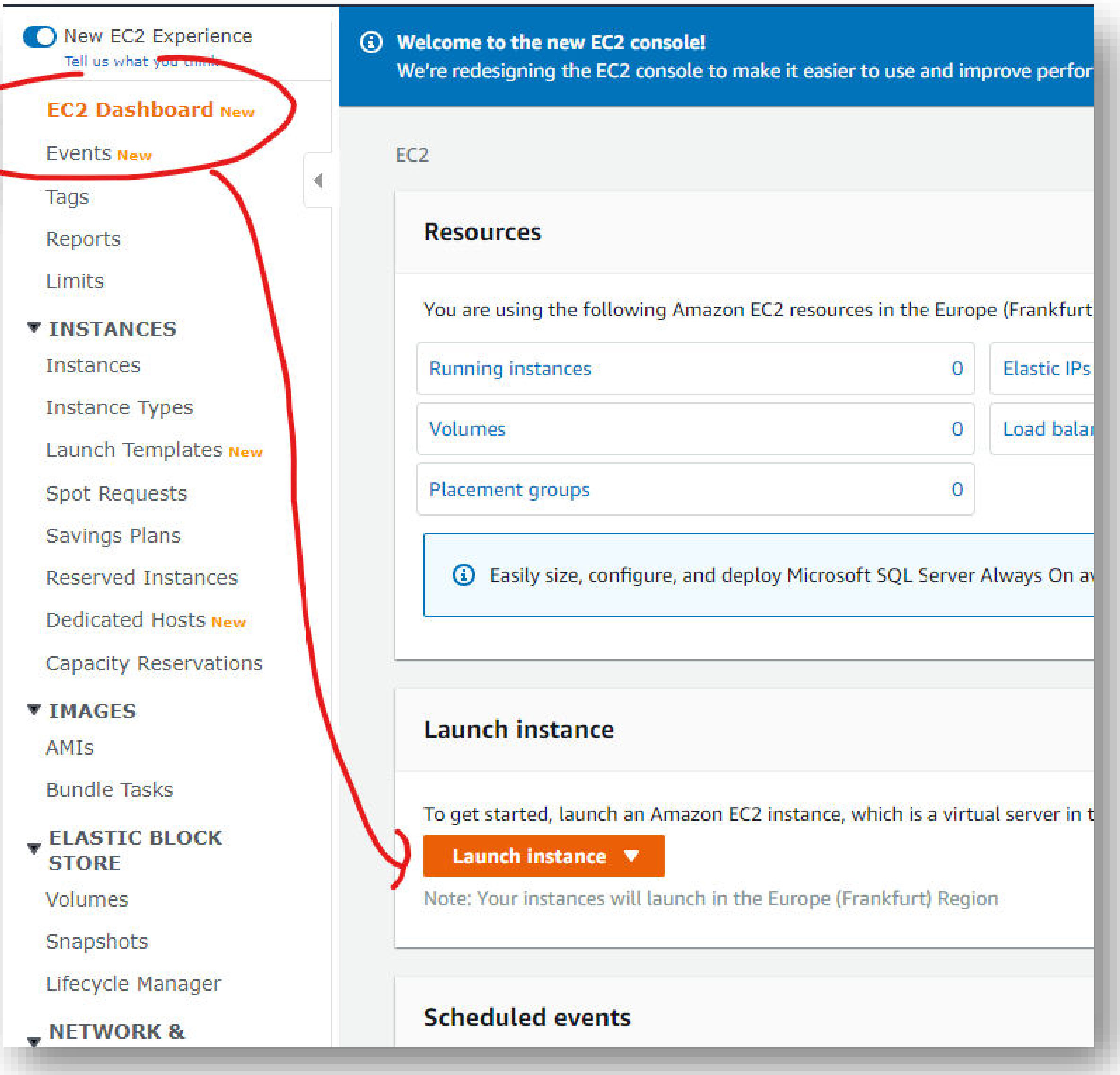


my-keypair.pem

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:



Welcome to the new EC2 console!
We're redesigning the EC2 console to make it easier to use and improve perfor

Resources

You are using the following Amazon EC2 resources in the Europe (Frankfurt

Running instances	0
Volumes	0
Placement groups	0
Elastic IPs	
Load balar	

Easily size, configure, and deploy Microsoft SQL Server Always On av

Launch instance

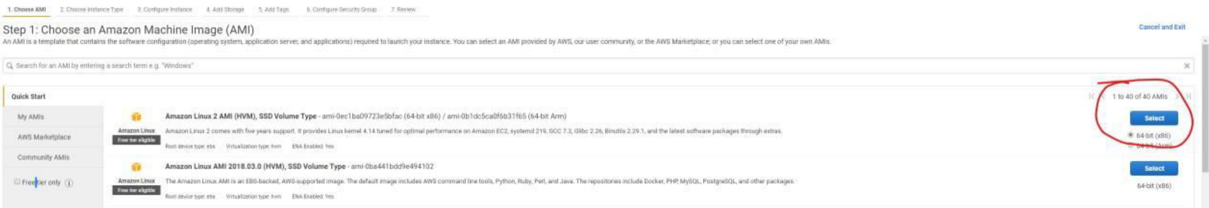
To get started, launch an Amazon EC2 instance, which is a virtual server in t

Note: Your instances will launch in the Europe (Frankfurt) Region

Scheduled events

Choose an AMI

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



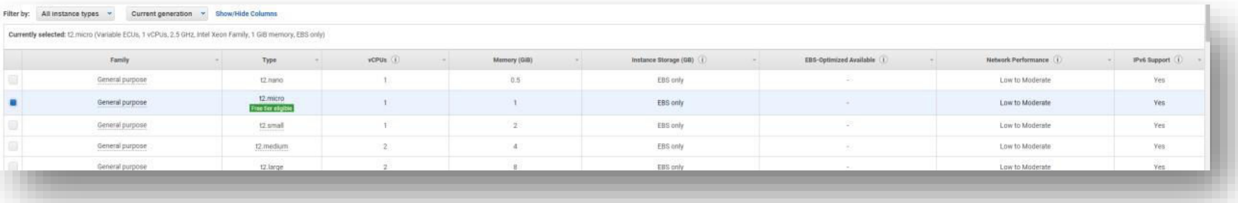
Step 1: Choose an Amazon Machine Image (AMI)
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0ec1ba09723e5bfac (64-bit x86) / ami-0b1dc5ca0f6b31f65 (64-bit Arm)
Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras.
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes
● 64-bit (x86)
○ 64-bit (Arm)

Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type - ami-0ba441bdd9e494102
The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes
64-bit (x86)

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.



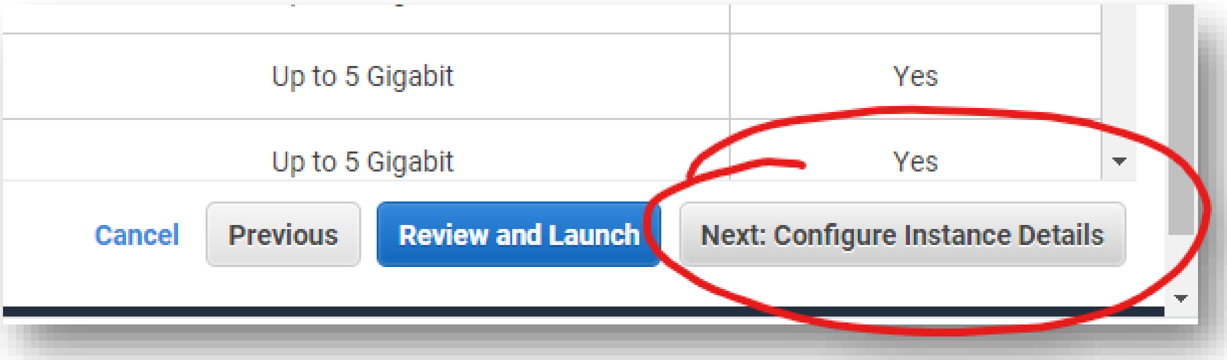
Filter by: All instance types Current generation Show/Hide Columns

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	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 Free tier eligible	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

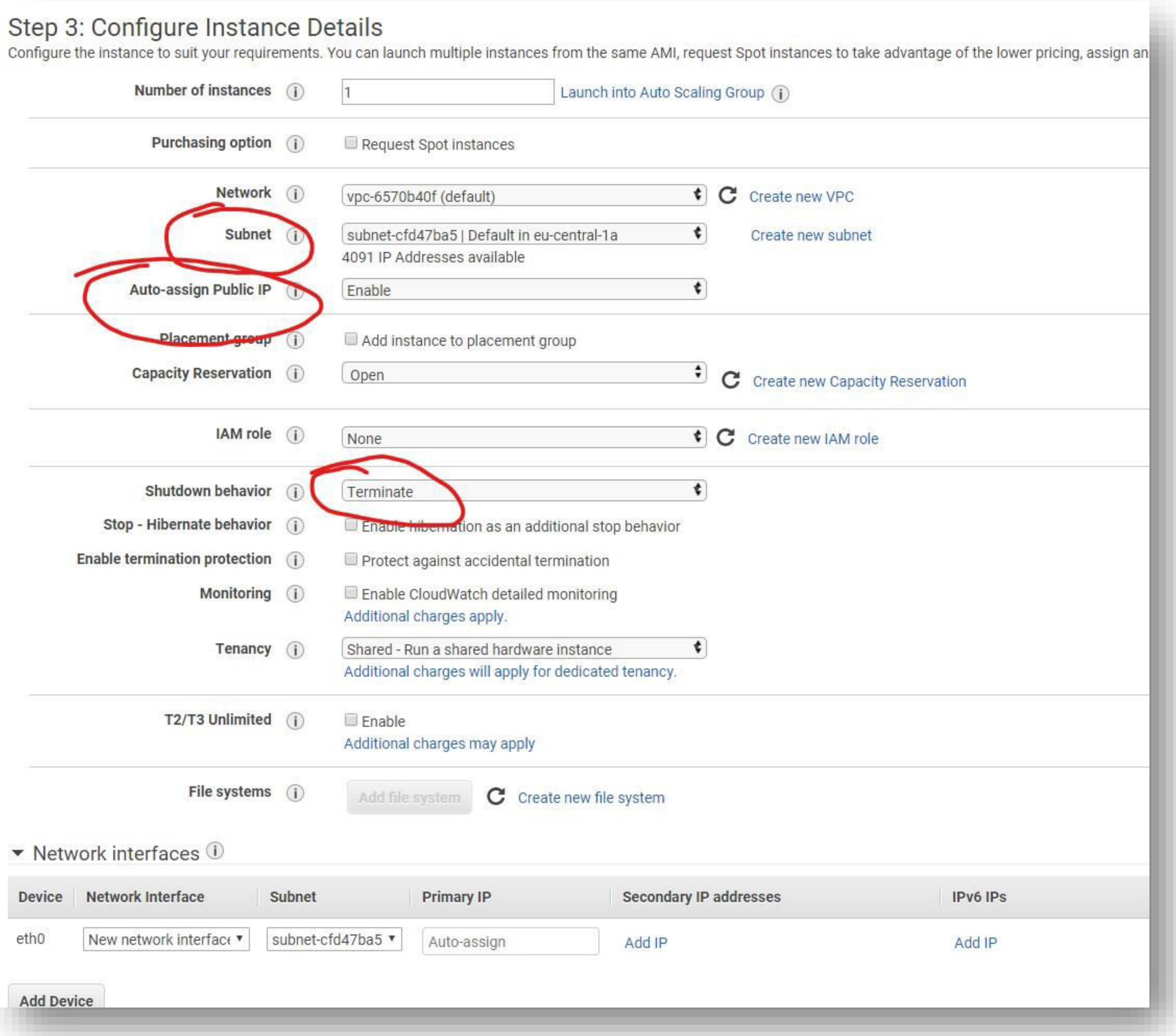
Configure Instance Details

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

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

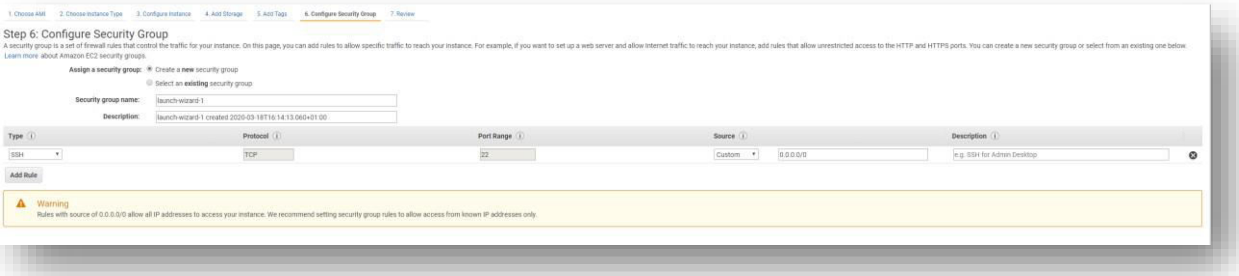
Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-cfd47ba5	Auto-assign	Add IP	Add IP

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

○ Select an **existing** 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

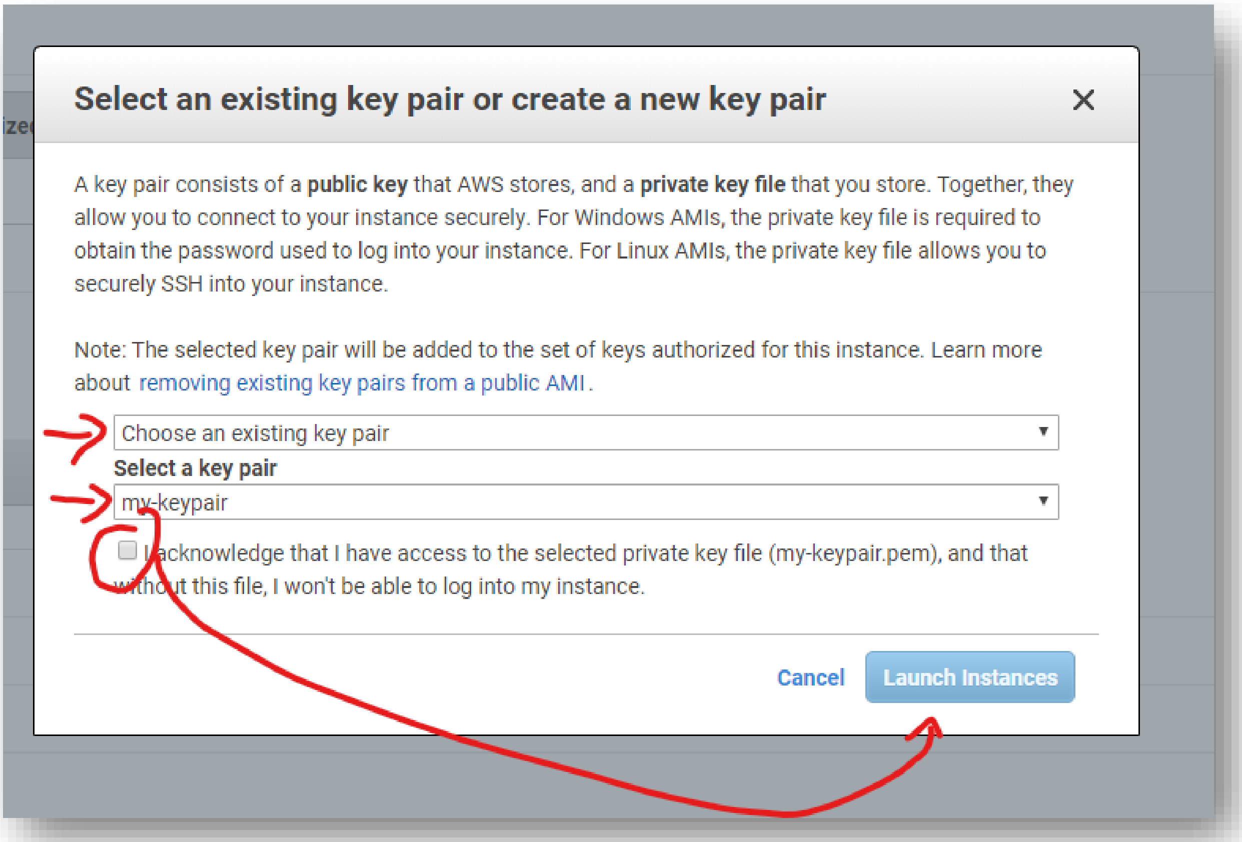
Add Rule

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”



Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required 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.

Choose an existing key pair

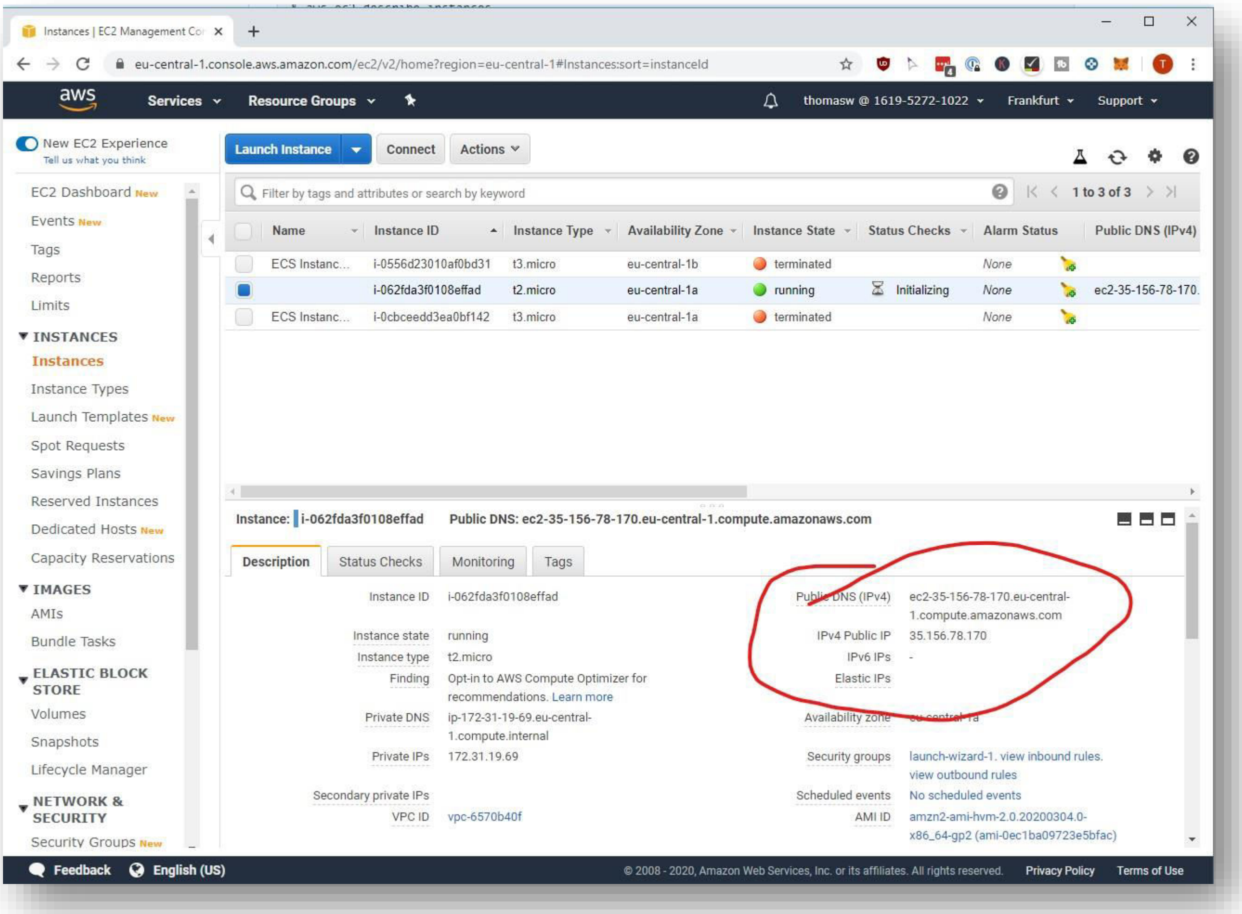
Select a key pair

my-keypair

□ I acknowledge that I have access to the selected private key file (my-keypair.pem), and that without this file, I won't be able to log into my 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.



	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
□	ECS Instanc...	i-0556d23010af0bd31	t3.micro	eu-central-1b	● terminated		None	
■		i-062fda3f0108effad	t2.micro	eu-central-1a	● running	Initializing	None	ec2-35-156-78-170.
□	ECS Instanc...	i-0cbceedd3ea0bf142	t3.micro	eu-central-1a	● terminated		None	

Instance: i-062fda3f0108effad Public DNS: ec2-35-156-78-170.eu-central-1.compute.amazonaws.com

Description | Status Checks | Monitoring | Tags

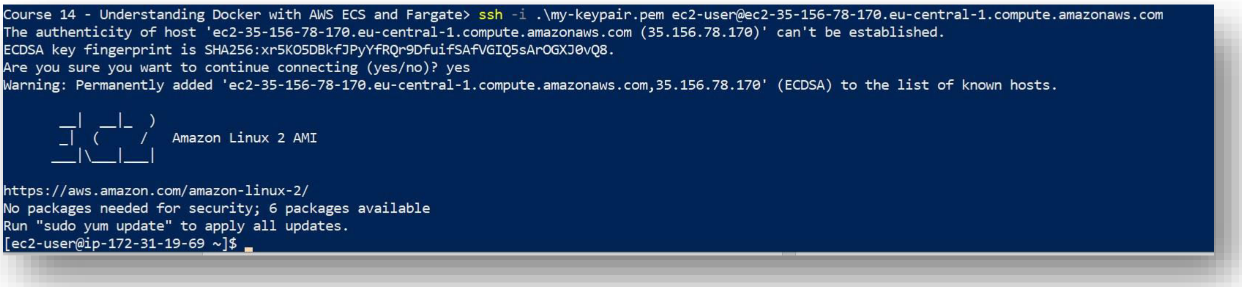
Instance ID	i-062fda3f0108effad	Public DNS (IPv4)	ec2-35-156-78-170.eu-central-1.compute.amazonaws.com
Instance state	running	IPv4 Public IP	35.156.78.170
Instance type	t2.micro	IPv6 IPs	-
Finding	Opt-in to AWS Compute Optimizer for recommendations. Learn more	Elastic IPs	
Private DNS	ip-172-31-19-69.eu-central-1.compute.internal	Availability zone	eu-central-1a
Private IPs	172.31.19.69	Security groups	launch-wizard-1. view inbound rules. view outbound rules
Secondary private IPs		Scheduled events	No scheduled events
VPC ID	vpc-6570b40f	AMI ID	amzn2-ami-hvm-2.0.20200304.0-x86_64-gp2 (ami-0ec1ba09723e5bfac)

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:xr5KO5DBkfJPyYfRQr9DfuifSAfVGIQ5sArOGXJ0vQ8.
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

Type in

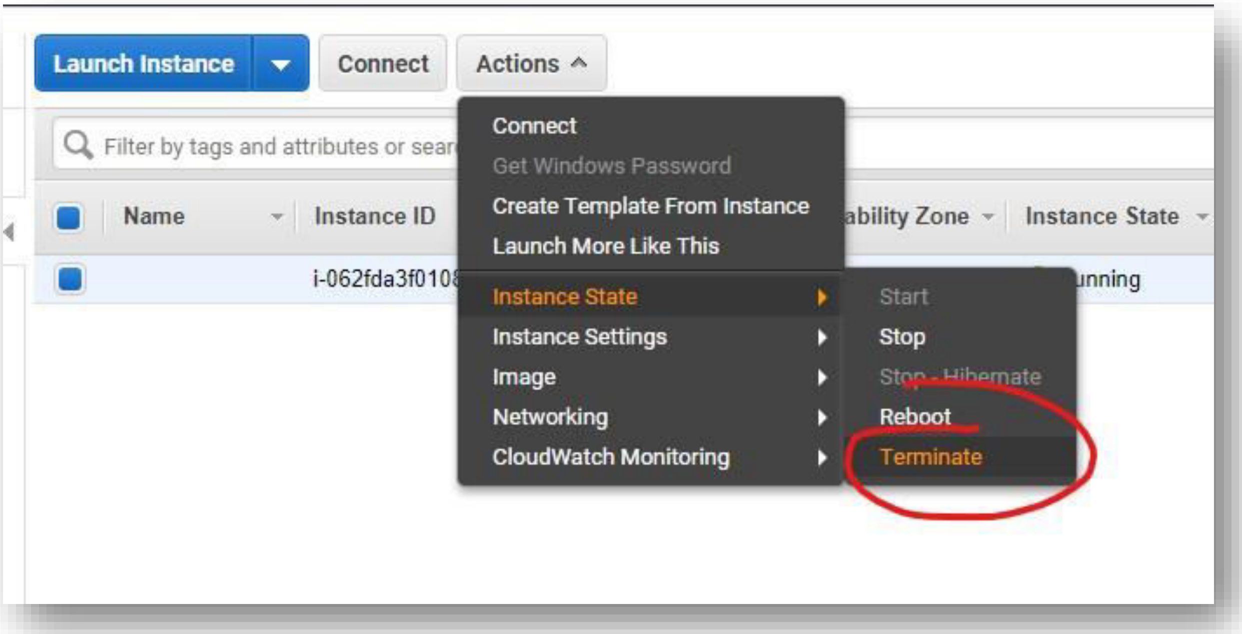
```
exit
```

Congratulations, you successfully connected to your first Instance!

Cleanup

Remove the Instance again

Now remove the instance to clean up.



Lab Finished