# LAB: Create an Elastic File System and connect it to EC2 Instances

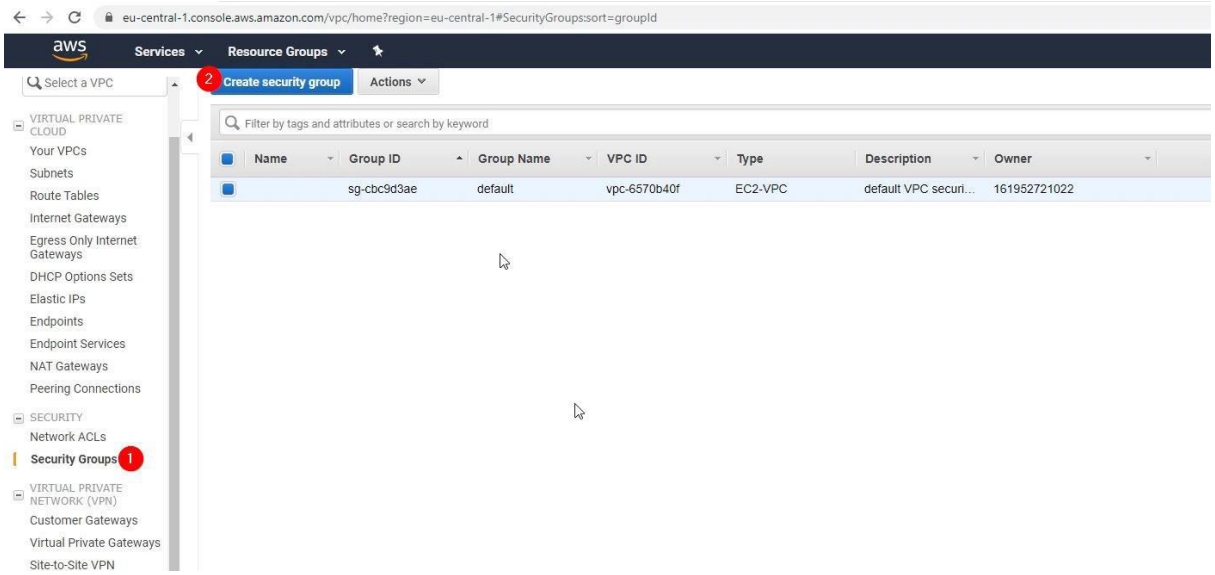
**You need:**

- An AWS Account

**Duration of the Lab**: 30 Minutes.

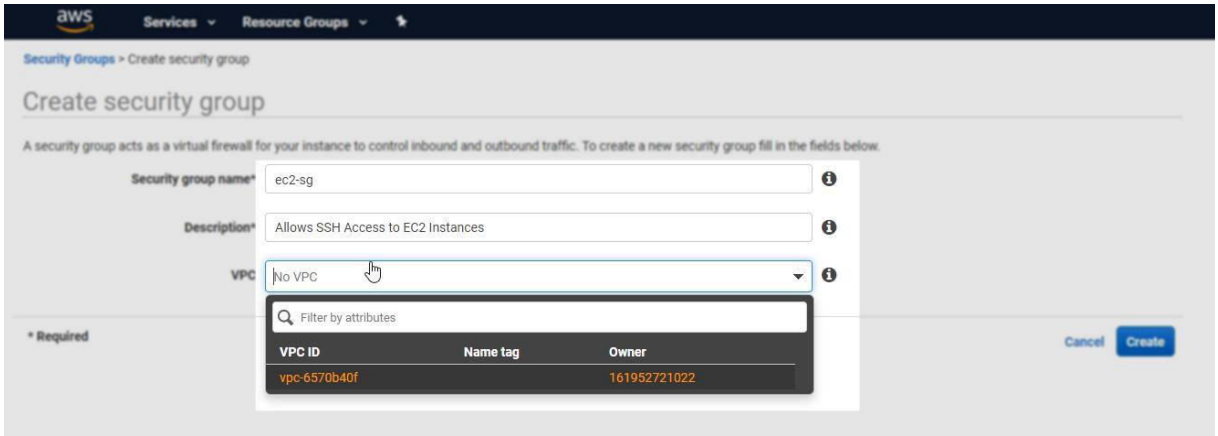
**Difficulty**: medium

## Create a new Security Group for the EFS and the EC2 instances



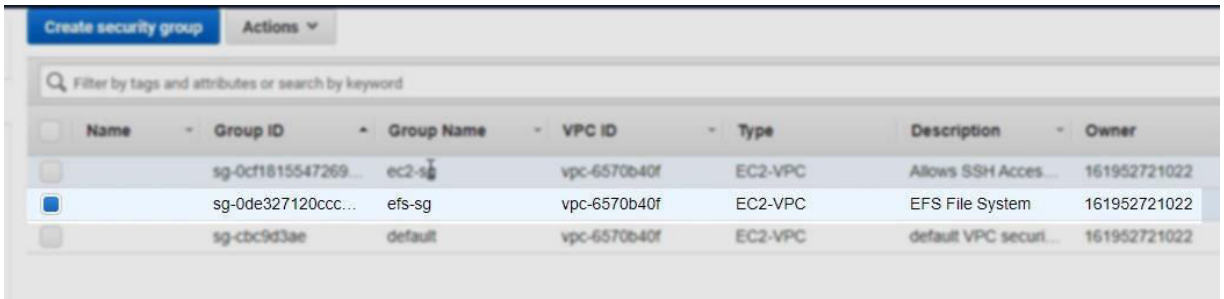

First the EFS:


Another one for the EC2 Instances:



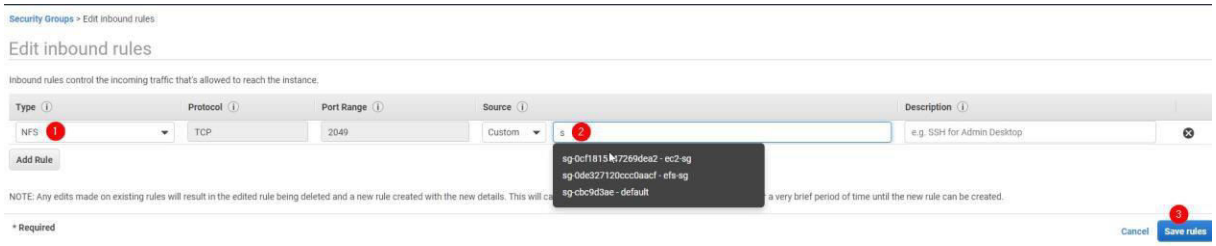

## Configure EFS Security Group

Edit the Inbound Rules from the EFS Security Rule:



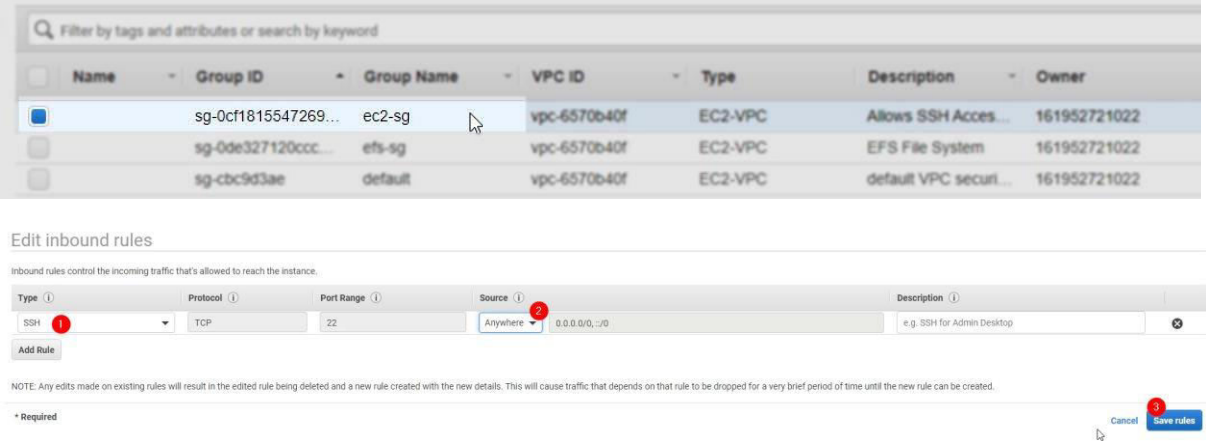


Add the EC2 security group as NFS:



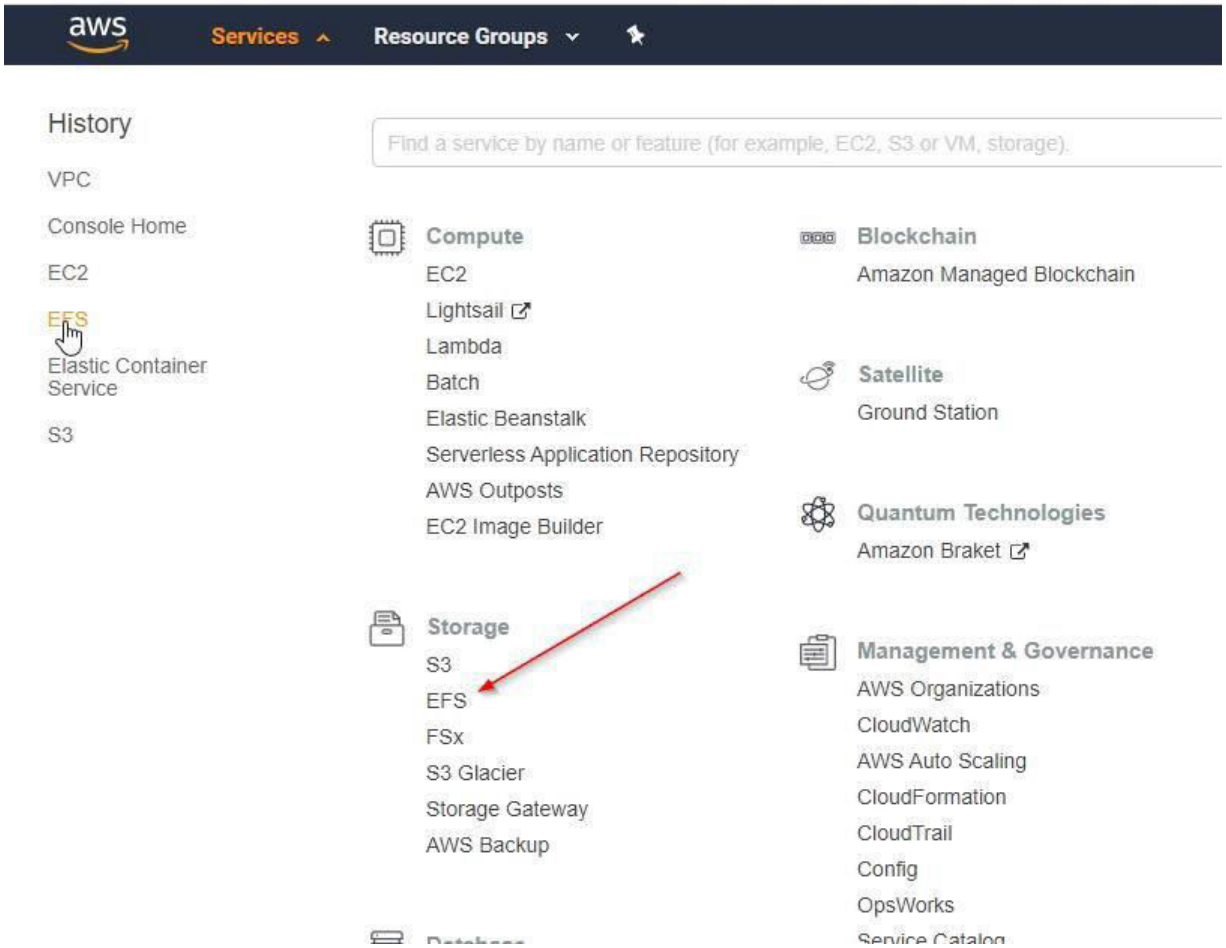

## Configure EC2 Security Group

Edit the EC2 Security Group to allow inbound SSH access from anywhere:

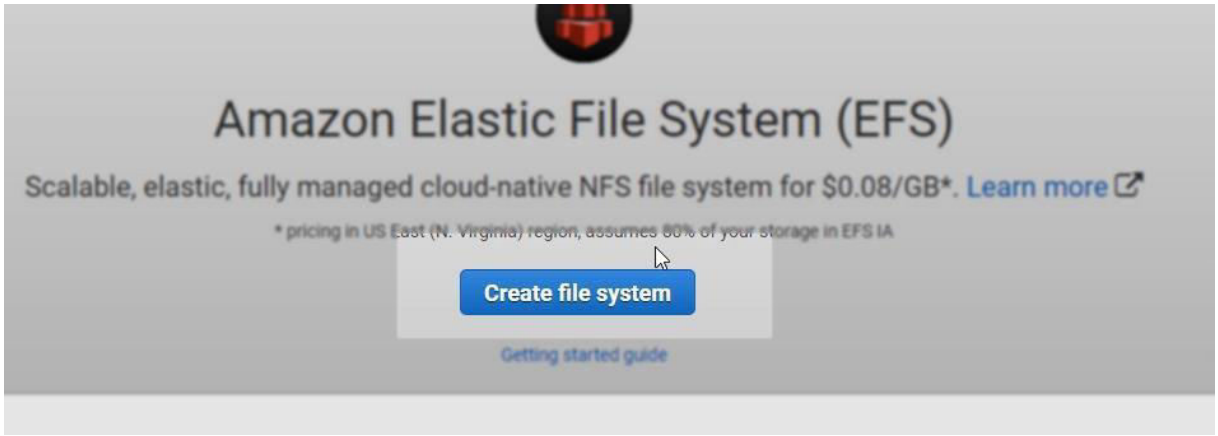



## Create an EFS File System

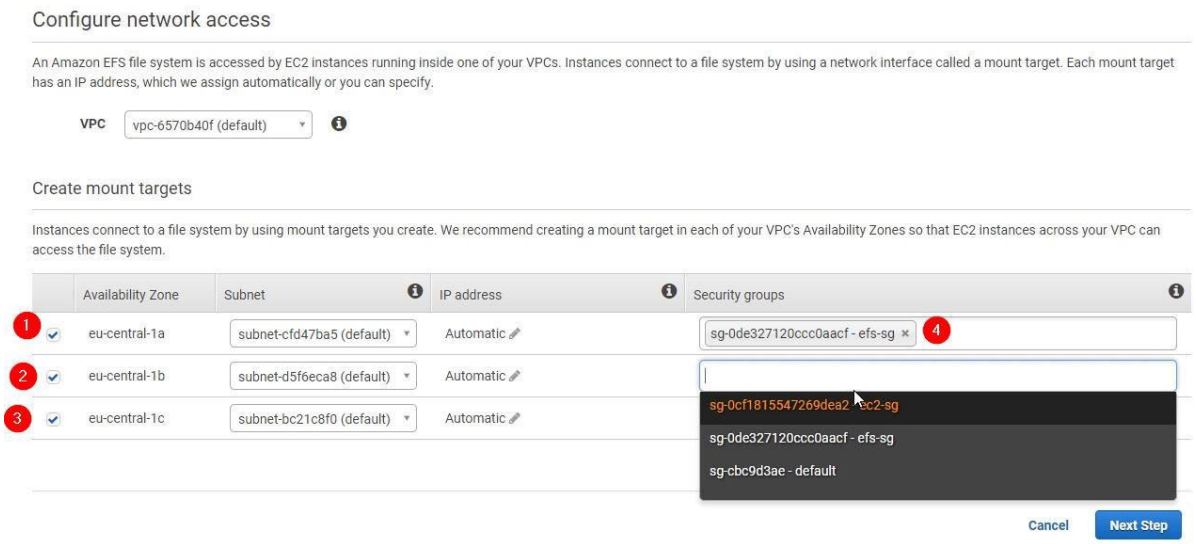
Open the EFS Dashboard:




Let's use the creation wizard:




Place the EFS in all availability zones and assign the EFS Security Group to all mount points:




Leave all settings at their default value for file system settings:

Enable lifecycle management NEW!

**Automatically save up to 92%** on your EFS bill as your access patterns change by enabling **Lifecycle Management** for your file system. Based on the policy you choose, any files in your file system that are not accessed for a period of time will automatically move to the EFS Infrequent Access (EFS IA) storage class. EFS IA provides price/performance that's cost-optimized for files not accessed every day. Learn more

**Lifecycle policy** None

Choose throughput mode

We recommend **Bursting** throughput mode for most file systems. Use **Provisioned** throughput mode for applications that require more throughput than allowed by **Bursting** throughput. Learn more

- **Bursting**
- **Provisioned**

Choose performance mode

We recommend **General Purpose** performance mode for most file systems. **Max I/O** performance mode is optimized for applications where tens, hundreds, or thousands of EC2 instances are accessing the file system — it scales to higher levels of aggregate throughput and operations per second with a tradeoff of slightly higher latencies for file operations.

- **General Purpose**
- **Max I/O**

Enable encryption

If you enable encryption for your file system, all data on your file system will be encrypted at rest. You can select a KMS key from your account to protect your file system, or you can provide the ARN of a key from a different account. Encryption of data at rest can only be enabled during file system creation. Encryption of data in transit is configured when mounting your file system. Learn more

- **Enable encryption of data at rest**

Cancel | Previous | Next Step

Lave all settings at their default value for client access:

Configure client access

File system policy

A file system policy is an IAM resource policy that applies to all NFS clients connecting to this file system. You can use the check boxes below to create a simple file system policy. You can also use the JSON editor to create a more advanced policy, such as one that grants permissions to different IAM roles or a different AWS account. Learn more

Policy settings | {} JSON

Select a combination of policy statements and set your policy.

- **Disable root access by default***
- **Enforce read-only access by default***
- **Enforce in-transit encryption for all clients**

* Identity-based policies can override these default permissions.

Set policy

Access points

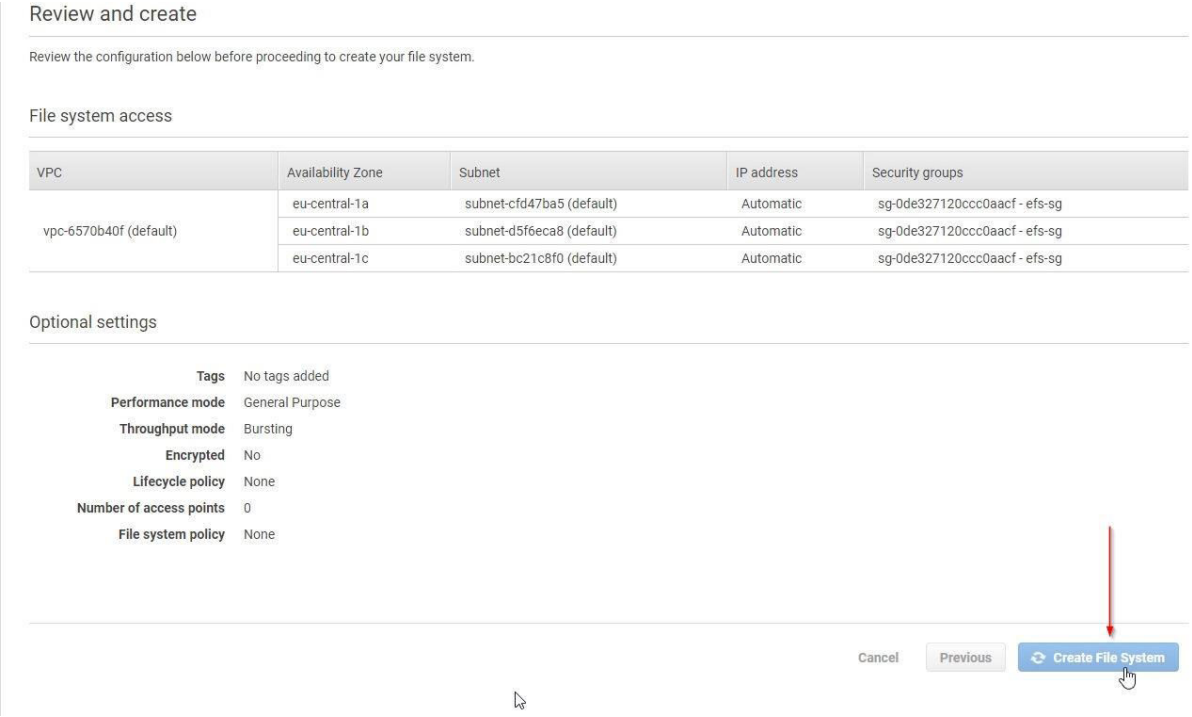
You can create access points to provide applications access to your file system. Optionally, you can configure the POSIX identity and root directory for all connections to this access point. If you specify the owner for root directory, EFS will automatically create it with the ownership and permissions that you specify once a client connects to the access point. Once you create your file system, you can update its policy to apply to access points. Learn more

| | Name | Posix User | Directory | Owner | |
|---|---|---|---|---|---|
| | | | Add access points for your file system. | | |

+ Add access point

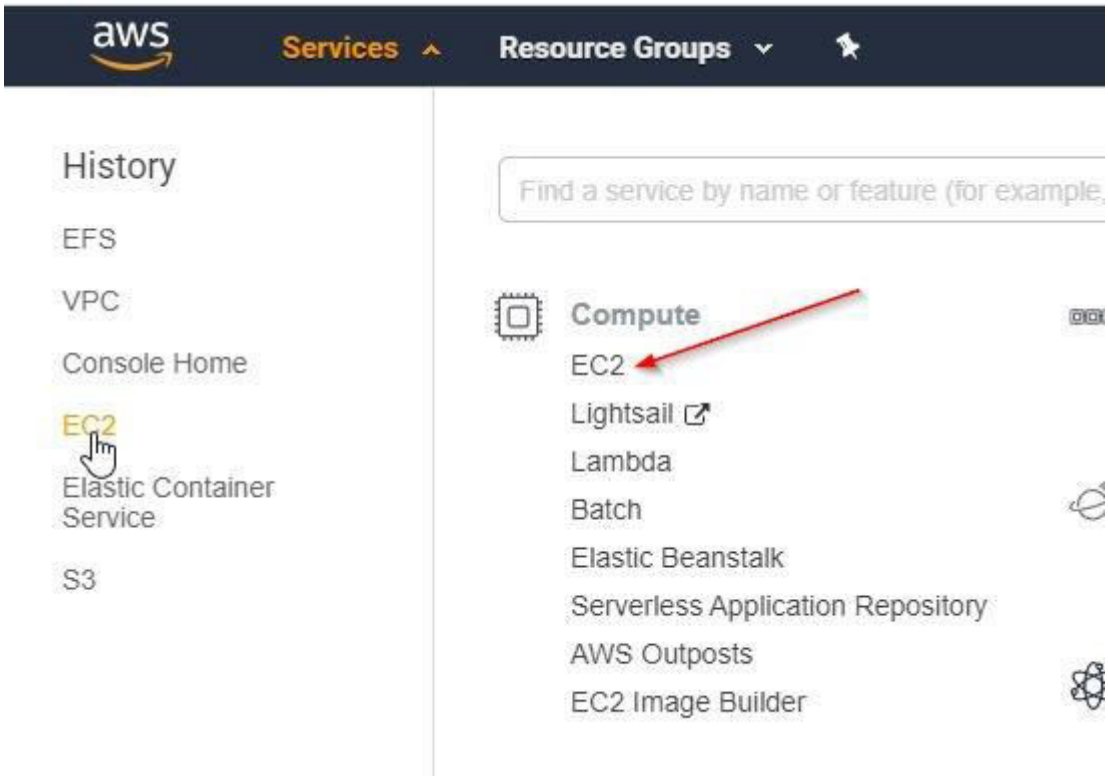
Cancel | Previous | Next Step

Review and Create the EFS:



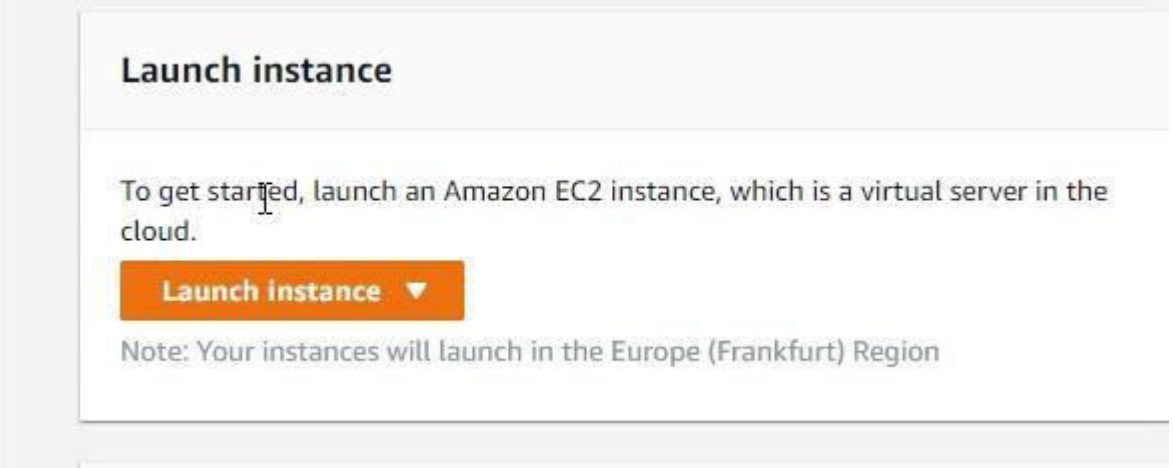

## EC2 Creation

Head over to the EC2 Dashboard:



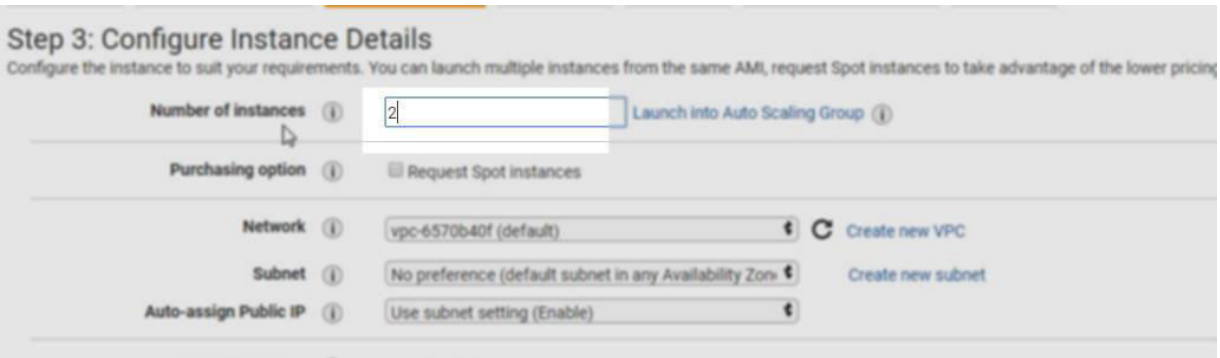

### Launch an Instance

Launch a new Instance.

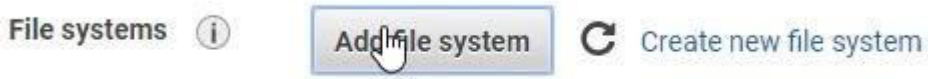



Select the Amazon Linux 2 AMI and the t2.micro instance type.

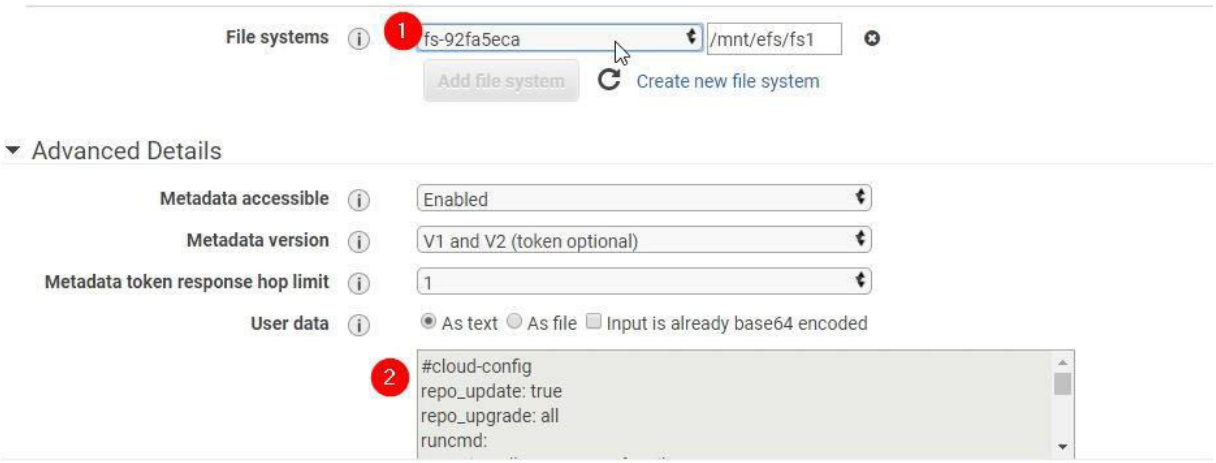
Start 2 Instances right away:




## Add a File System

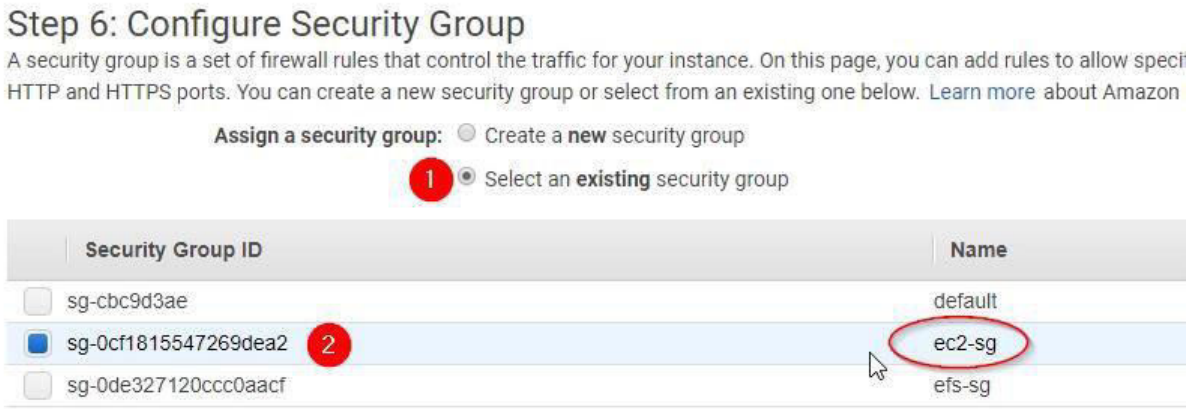



Observe that a script is automatically inserted into the user-data field:



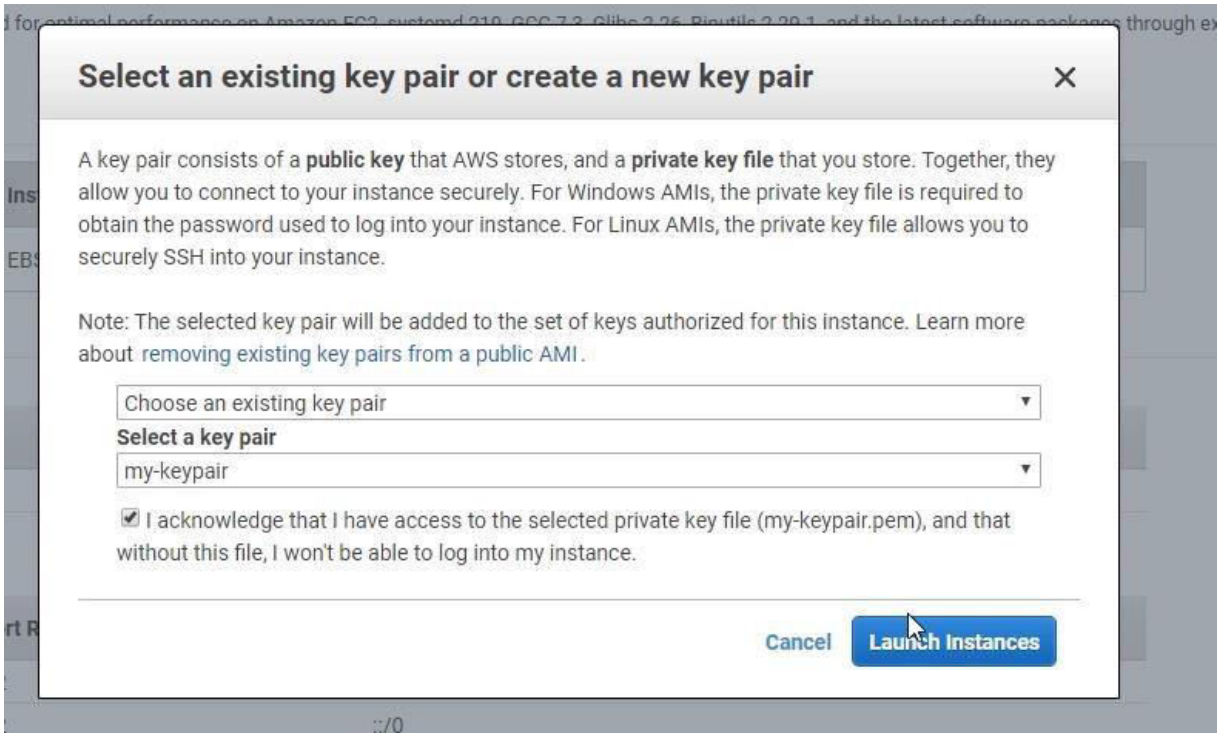

## Security Group

Make sure you select the EC2 Security group we created earlier:




## Launch instances

Launch the instances and select your key-pair so you can login via ssh:




# Use Elastic File System

## Login to EC2 Instance 1

Login to your first instance:

```
Course 14 - Understanding Docker with AWS ECS and Fargate> ssh -i "my-keypair.pem" ec2-
user@ec2-52-59-253-174.eu-central-1.compute.amazonaws.com
The authenticity of host 'ec2-52-59-253-174.eu-central-1.compute.amazonaws.com (52.59.2
53.174)' can't be established.
ECDSA key fingerprint is SHA256:OkY9dPs3jucJHD4HnqUSrW3kBmi8s5DhatdtYhLoVRk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ec2-52-59-253-174.eu-central-1.compute.amazonaws.com,52.59.
253.174' (ECDSA) to the list of known hosts.

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
1 package(s) needed for security, out of 1 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-37-175 ~]$ cd /mnt/efs/fs1/
[ec2-user@ip-172-31-37-175 fs1]$ ls
[ec2-user@ip-172-31-37-175 fs1]$
```

And change to the directory /mnt/efs/fs1

```
cd /mnt/efs/fs1
```

## Change the permissions

For the ec2-user to be able to write files from the EFS we need to change the permissions.

```
sudo chown ec2-user:ec2-user .
```

Then login to the second instance:

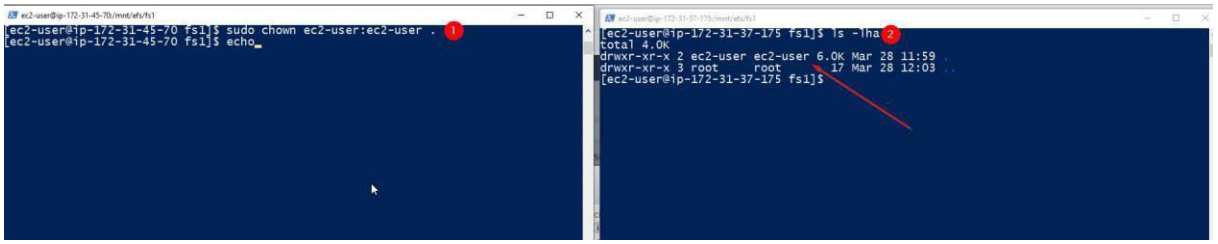
## Login to EC2 Instance 2

Open a second powershell/terminal and login to instance 2.

Cd into the same directory /mnt/efs/fs1.

Observe that the directory now already has the correct permissions

```
ls -lha
```




## Create a file

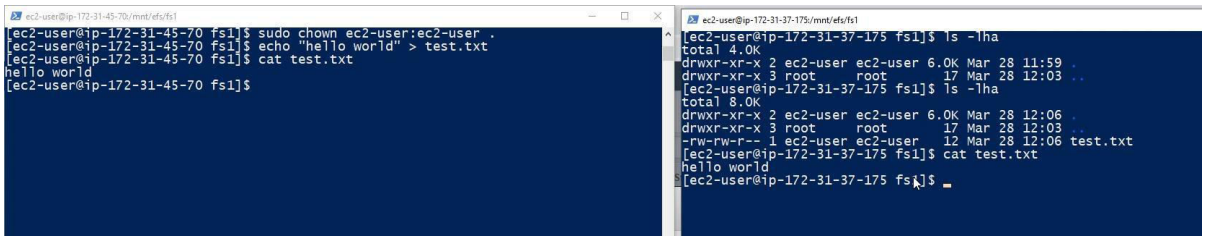
Let's create a file on instance 1 and observe the same file appearing on instance 2:

On Instance 1 run:

```
echo "hello world" > test.txt
```

On Instance 2 run:

```
cat test.txt
```




## Cleanup

1. Terminate both Instances
2. Delete the EFS File System (costs might occur otherwise)
3. Delete the security groups