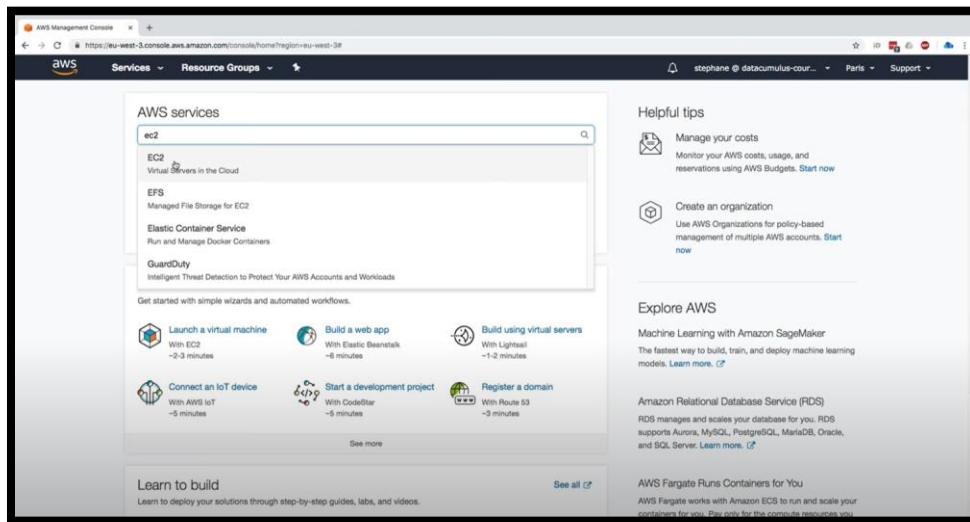
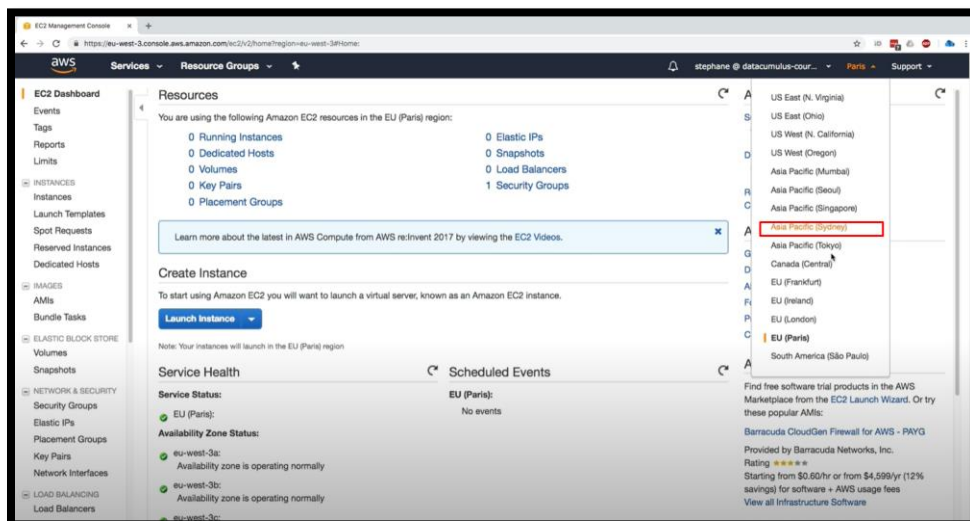


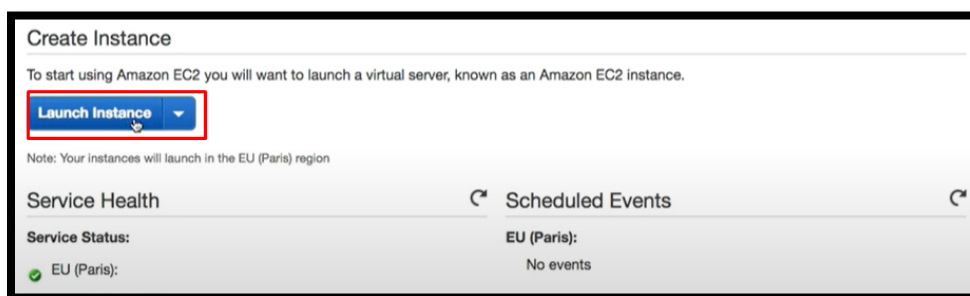
Step1:

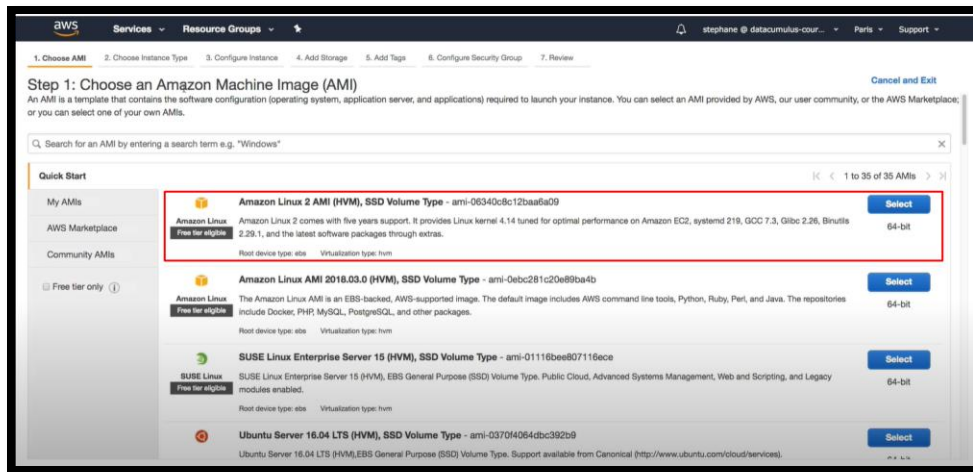


Step 2:



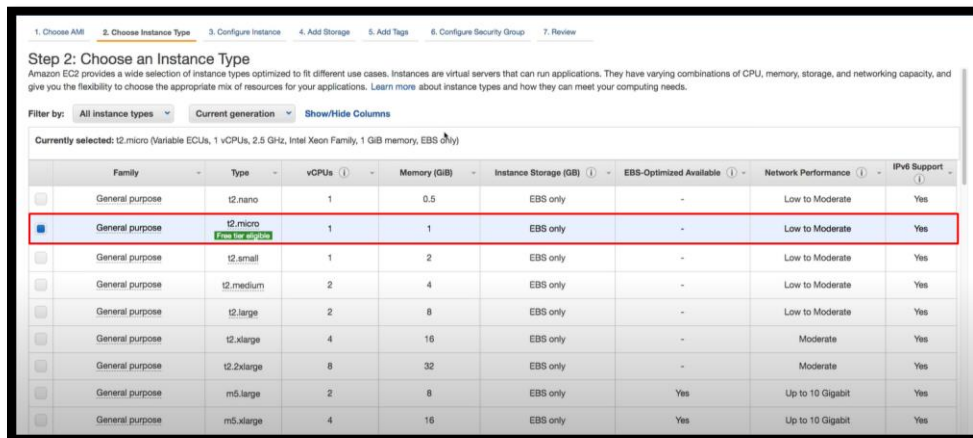
Step 3:



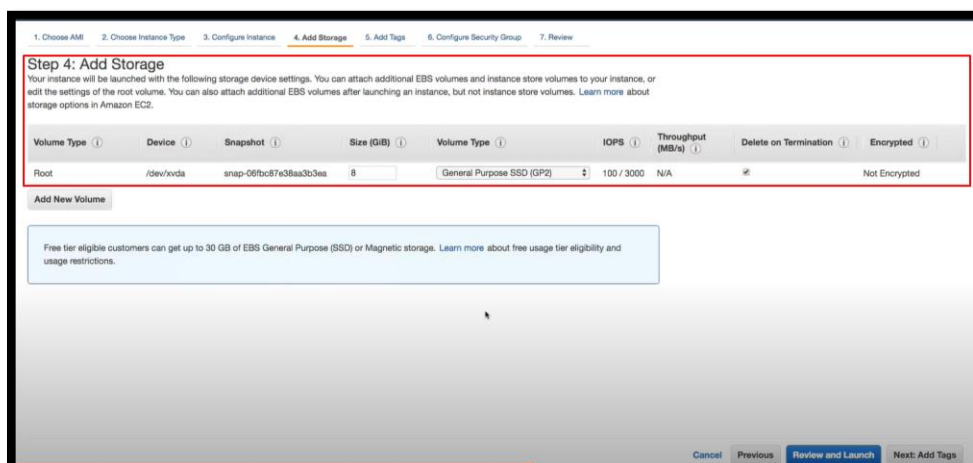


Step 4:

Step 5:



Step 6:



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

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 (1)	Volumes (1)
Name	My First Instance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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

Step 7:

Step 8:

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

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 (1)	Protocol (1)	Port Range (1)	Source (1)	Description (1)
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.

Step 9:

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Improve your instances' security. Your security group, my-first-security-group, is open to the vbrld.

Your instances 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](#)

▼ AMI Details [Edit AMI](#)

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-06340c8c12baaf6a09

Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 218, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras.

Root Device Type: ebs Virtualization type: hvm

▼ Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

▼ Security Groups [Edit security groups](#)

Security group name: my-first-security-group

Description: Created with my first EC2 Instance

Type (1)	Protocol (1)	Port Range (1)	Source (1)	Description (1)
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

[Cancel](#) [Previous](#) [Launch](#)

Step 10:

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](#).

Create a new key pair

Key pair name

EC2 Tutorial

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

Step 11:

aws

Services

Resource Groups

stephane @ datacube-cou... Paris Support

EC2 Dashboard

Launch Instance

Connect

Actions

Filter by tags and attributes or search by keyword

1 to 1 of 1

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv4
My First Instance	i-6c81776	t2.micro	eu-west-3c	running	Initializing	None	ec2-35-180-100-144.eu...	35.180.100.144	-

Instance: i-6c81776 (My First Instance)

Public DNS: ec2-35-180-100-144.eu-west-3.compute.amazonaws.com

Description

Status Checks

Monitoring

Tags

Instance ID	i-6c81776	Public DNS (IPv4)	ec2-35-180-100-144.eu-west-3.compute.amazonaws.com
Instance state	running	IPv4 Public IP	35.180.100.144
Instance type	t2.micro	Private DNS	ip-172-31-34-100.eu-west-3.compute.internal
Elastic IPs	-	Private IP	172.31.34.100
Availability zone	eu-west-3c	Secondary private IP	-
Security groups	my-first-security-group. view inbound rules. view outbound rules	VPC ID	vpc-d74714ba
Scheduled events	No scheduled events	Subnet ID	subnet-391dc774
AMI ID	ami-2-ami-hvm-2.0.20180810-x86_64-gp2 (ami-06340cb12baa6a09)	Network interfaces	eni0
Platform	-		