


Dans ce premier TP nous allons créer le compte AWS, configurer les éléments de sécurité de base de votre compte AWS et nous allons nous familiariser avec quelques concepts d'AWS (IAM, VPC, EC2) qui nous permettront d'aborder les TPs suivants.

Documentation AWS :  
<https://docs.aws.amazon.com/>

## Création d'un compte AWS

<https://portal.aws.amazon.com/billing/signup#/start>



### Create an AWS account

**AWS Accounts Include 12 Months of Free Tier Access**

Including use of Amazon EC2, Amazon S3, and Amazon DynamoDB  
Visit [aws.amazon.com/free](https://aws.amazon.com/free) for full offer terms

Email address

Password

Confirm password

AWS account name ⓘ

**Continue**

[Sign in to an existing AWS account](#)

© 2020 Amazon Web Services, Inc. or its affiliates. All rights reserved.  
[Privacy Policy](#) | [Terms of Use](#)

Dans cette étape il sera nécessaire d'associer un moyen de paiement à votre compte AWS.

Comment créer et activer un compte AWS ?




<https://aws.amazon.com/fr/premiumsupport/knowledge-center/create-and-activate-aws-account/>

AWS Accounts Include 12 Months of Free Tier Access:

<https://aws.amazon.com/free/>

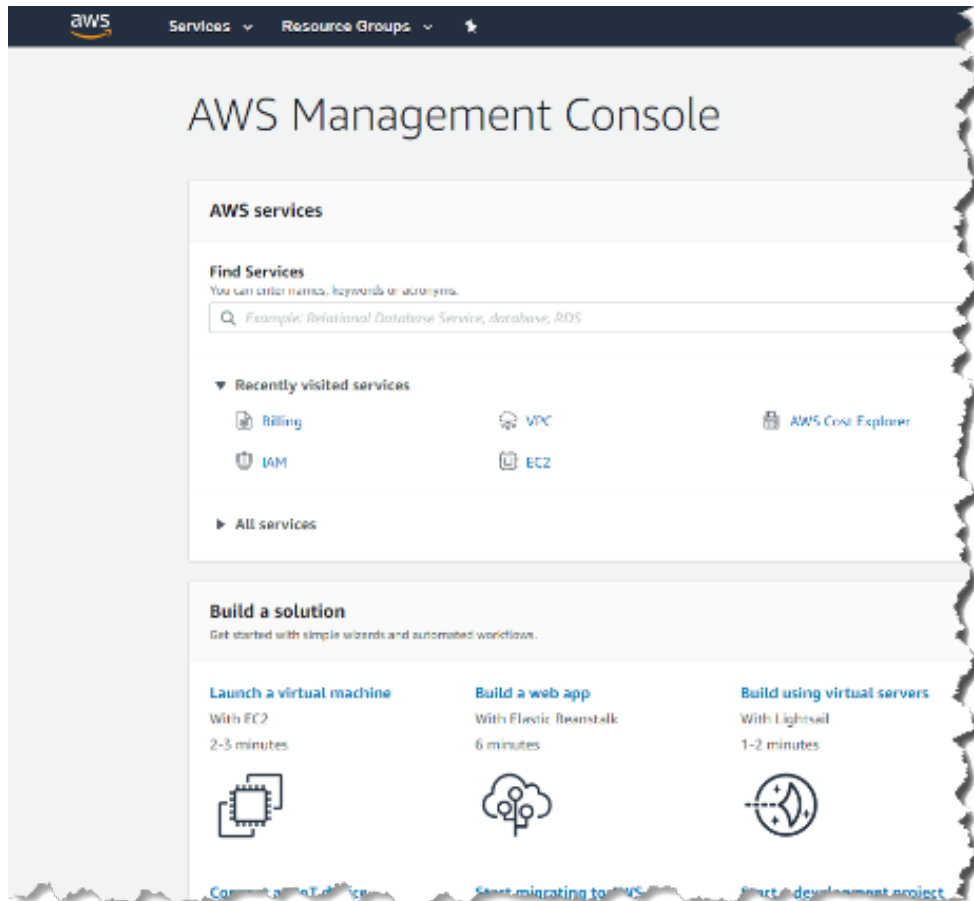
### Select a Support Plan

AWS offers a selection of support plans to meet your needs. Choose the support plan that best aligns with your AWS usage. [Learn more](#)

 <b>Basic Plan</b>	 <b>Developer Plan</b>	 <b>Business Plan</b>
<b>Free</b>	<b>From \$29/month</b>	<b>From \$100/month</b>
<ul style="list-style-type: none"><li>Included with all accounts</li><li>24/7 self-service access to forums and resources</li><li>Best practice checks to help improve security and performance</li><li>Access to health status and notifications</li></ul>	<ul style="list-style-type: none"><li>For early adoption, testing and development</li><li>Email access to AWS Support during business hours</li><li>1 primary contact can open an unlimited number of support cases</li><li>12-hour response time for non-production systems</li></ul>	<ul style="list-style-type: none"><li>For production workloads &amp; business-critical dependencies</li><li>24/7 chat, phone, and email access to AWS Support</li><li>Unlimited contacts can open an unlimited number of support cases</li><li>1-hour response time for production systems</li></ul>

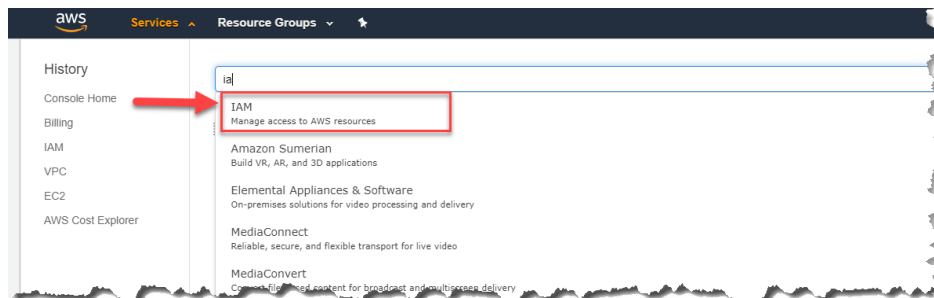
**Need Enterprise level support?**  
Contact your account manager for additional information on running business and mission critical-workloads on AWS (starting at \$15,000/month). [Learn more](#)

Lorsque qu'il vous est demandé de choisir une formule de support sélectionner «Basic Plan» qui est sans aucun frais.



Lorsque le compte AWS est créé, se connecter avec les identifiants Root du compte. (email + password).

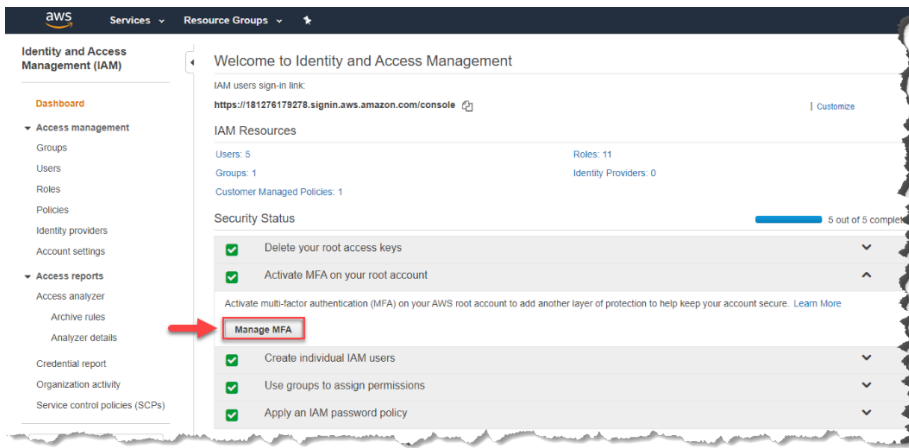
### Root user



Pour des raisons de sécurité, prendre l'habitude de toujours configurer un MFA pour le user « root » que pour les utilisateurs créés dans IAM.

Télécharger l'application Authy depuis votre smartphone pour la gestion des MFA.





## Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the IAM Console .

To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.

- Password
- ▼ Multi-factor authentication (MFA)
  - Use MFA to increase the security of your AWS environments. Signing in to MFA-protected accounts requires a user name, password, and an authentication code from an MFA device.
  - [Activate MFA](#)
- Access keys (access key ID and secret access key)
- CloudFront key pairs
- X.509 certificate
- Account Identifiers

**Manage MFA device**

Choose the type of MFA device to assign:

☒ **Virtual MFA device**  
Authenticator app installed on your mobile device or computer


☐ **U2F security key**  
YubiKey or any other compliant U2F device

☐ **Other hardware MFA device**  
Gemalto token

For more information about supported MFA devices, see [AWS Multi-Factor Authentication](#)

[Cancel](#) [Continue](#)

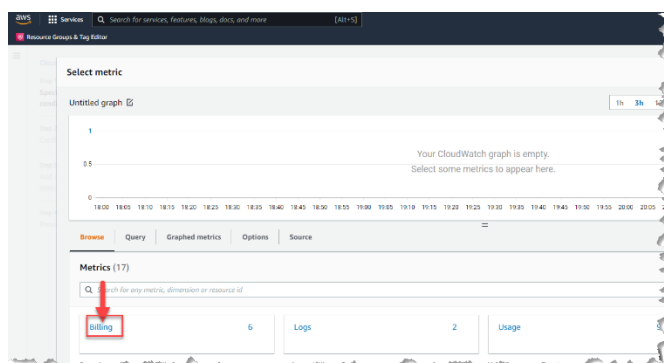
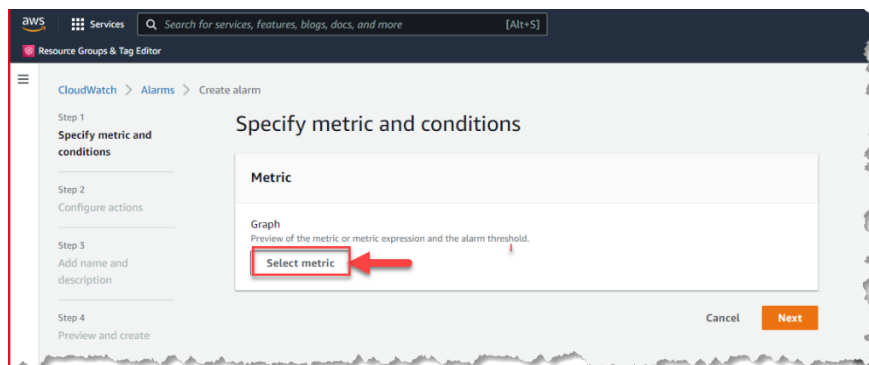
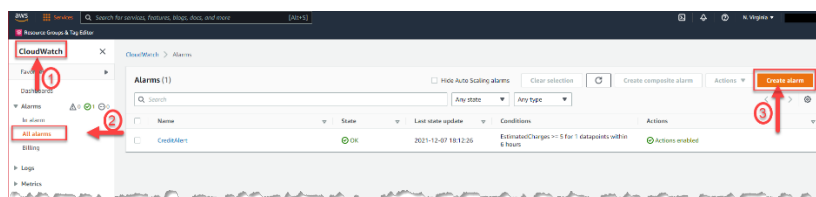
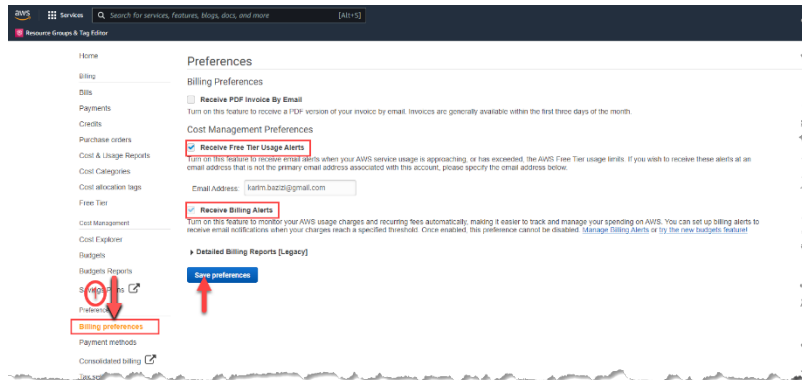
Set up virtual MFA device

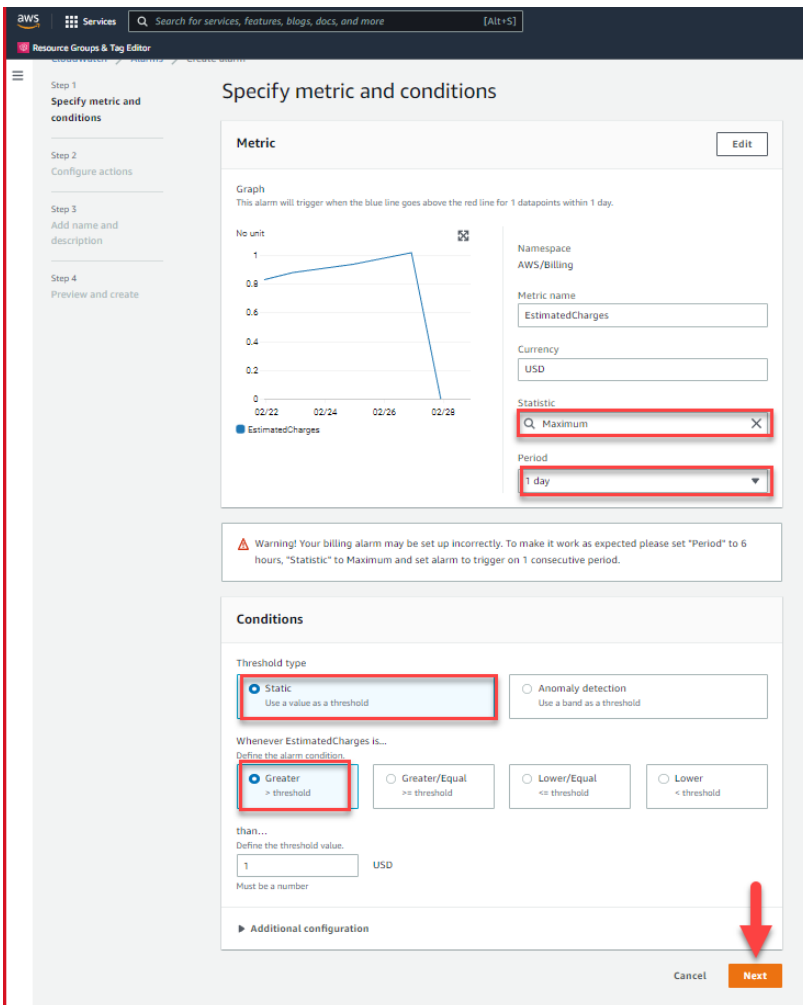
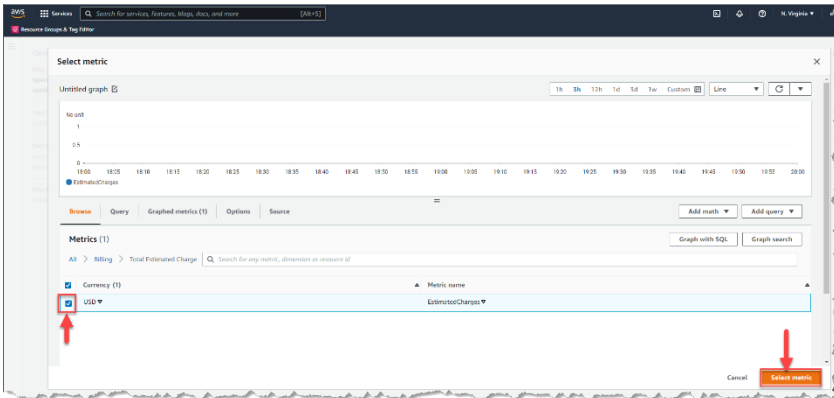
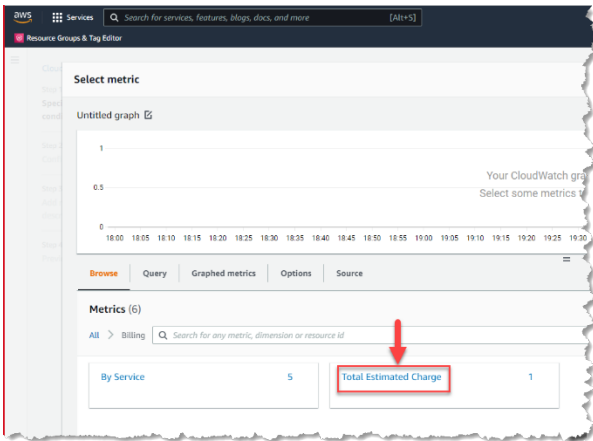
1. Install a compatible app on your mobile device or computer  
[See a list of compatible applications](#)
2. Use your virtual MFA app and your device's camera to scan the QR code  

3. Type two consecutive MFA codes below  
Alternatively, you can type the secret key. [Show secret key](#)  
MFA code 1:   
MFA code 2:

[Cancel](#) [Previous](#) [Assign MFA](#)

## Billing alerts

Dans cette étape nous allons mettre une alerte sur votre compte AWS, pour détecter toute anomalie de facturation sur votre compte.





CloudWatch > Alarms > Create alarm

Step 1  
Specify metric and conditions

Step 2  
Configure actions

Step 3  
Add name and description

Step 4  
Preview and create

### Configure actions

#### Notification

Alarm state trigger  
Define the alarm state that will trigger this action.

☒ In alarm  
The metric or expression is outside of the defined threshold.

☐ OK  
The metric or expression is within the defined threshold.

☐ Insufficient data  
The alarm has just started or not enough data is available.

Remove

Select an SNS topic  
Define the SNS (Simple Notification Service) topic that will receive the notification.

☐ Select an existing SNS topic

☒ Create new topic

☐ Use topic ARN

Create a new topic...  
The topic name must be unique.

billing\_alert

SNS topic names can contain only alphanumeric characters, hyphens (-) and underscores (\_).

Email endpoints that will receive the notification...  
Add a comma-separated list of email addresses. Each address will be added as a subscription to the topic above.

karim.bazizi@gmail.com

user1@example.com; user2@example.com

Create topic

Add notification

CloudWatch > Alarms > Create alarm

Step 1  
Specify metric and conditions

Step 2  
Configure actions

Step 3  
Add name and description

Step 4  
Preview and create

### Add name and description

#### Name and description

Alarm name

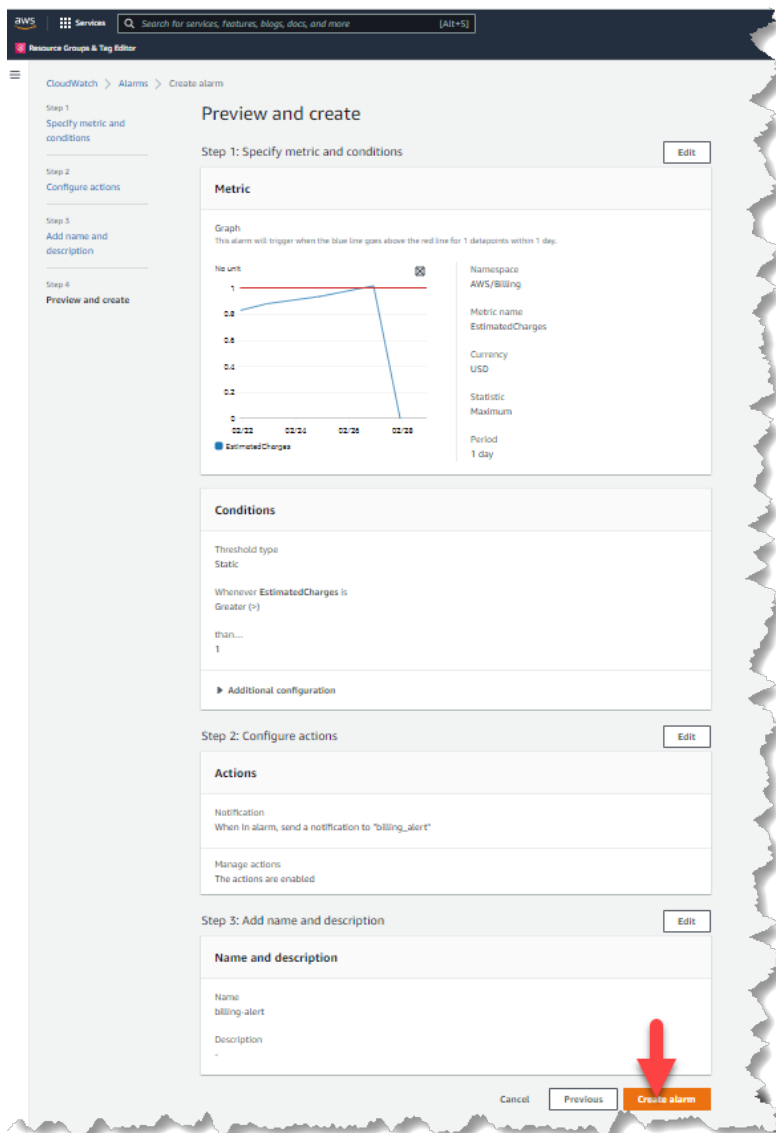
billing-alert

Alarm description - optional

Alarm description

Up to 1024 characters (0/1024)

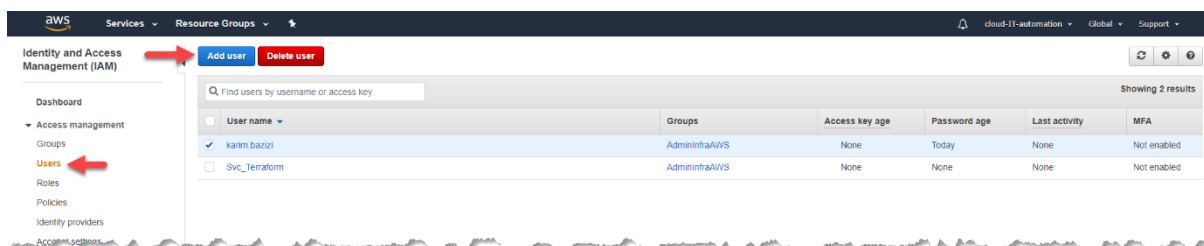
Cancel Previous Next



## Users

Créer un utilisateur auquel nous donnons le droit Administrateur.

Se connecter ensuite avec cet utilisateur (Id du compte ou alias / User / Password).



Ne pas oublier d'assigner un MFA à vos utilisateurs.

La bonne pratique est d'appliquer une « policy » aux utilisateurs qui interdit toutes actions si l'utilisateur n'a pas de MFA configuré. Pour plus de détails suivre le lien ci-dessous :

[https://docs.aws.amazon.com/IAM/latest/UserGuide/reference\\_policies\\_examples\\_aws\\_my-sec-creds-self-manage.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_aws_my-sec-creds-self-manage.html)

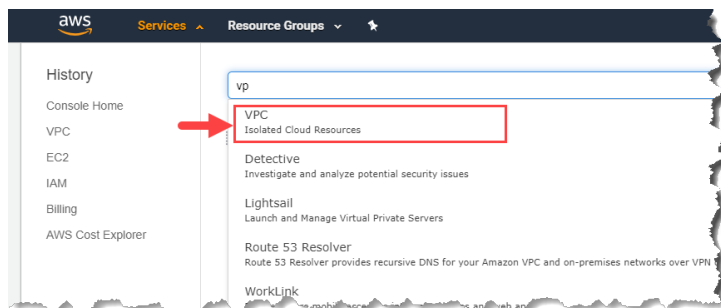


## VPC (Virtual Private Cloud)

[https://docs.aws.amazon.com/fr\\_fr/vpc/latest/userguide/VPC\\_Subnets.html](https://docs.aws.amazon.com/fr_fr/vpc/latest/userguide/VPC_Subnets.html)

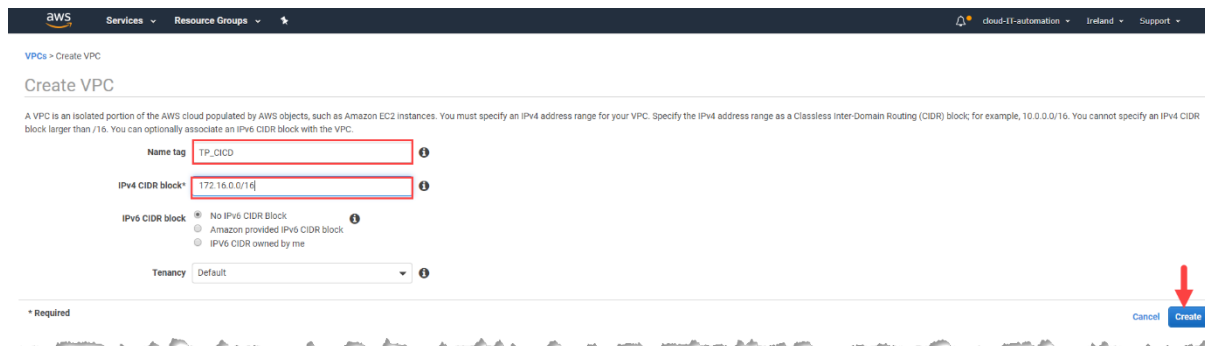
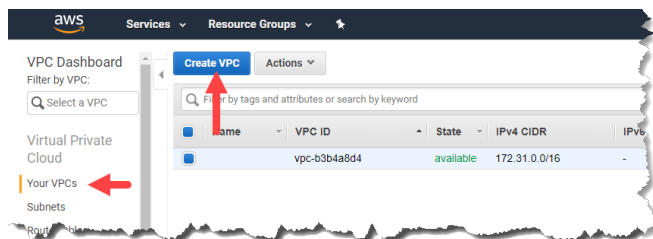
[https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_Scenario2.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html)

Se rendre dans le service VPC.

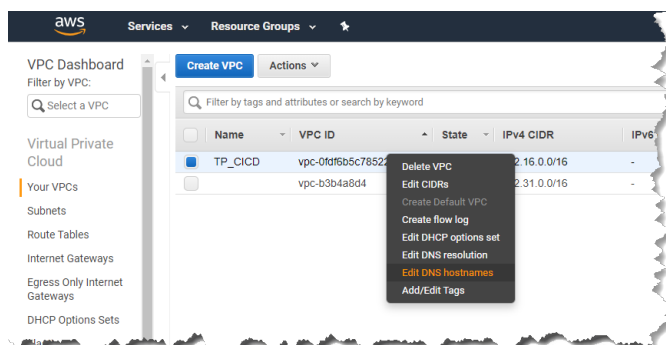


Créer un VPC avec le CIDR suivant : 172.16.0.0/16

Name Tag	CIDR
TP_CICD	172.16.0.0/16



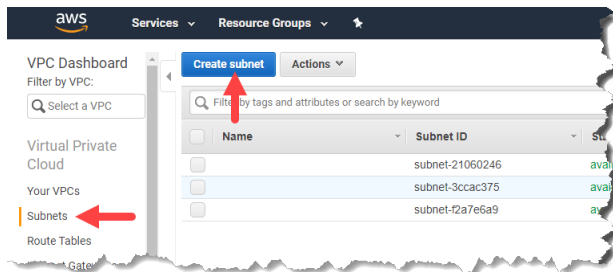
Une fois le VPC créé, activer la fonctionnalité **DNS hostnames**.



## Subnets

Créer les 2 subnets suivants.

Name Tag	VPC	Availability Zone	CIDR
TP_CICD_Public	172.16.1.0/24	eu-west-1a	172.16.1.0/24
TP_CICD_Private	172.16.2.0/24	eu-west-1a	172.16.2.0/24



Subnets > Create subnet

### Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag:

VPC:

Availability Zone:

VPC CIDRs	CIDR	Status	Status Reason
	172.16.0.0/16	associated	

IPv4 CIDR block:

\* Required

[Cancel](#) [Create](#)

Subnets > Create subnet

### Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag:

VPC:

Availability Zone:

VPC CIDRs	CIDR	Status	Status Reason
	172.16.0.0/16	associated	

IPv4 CIDR block:

\* Required

[Cancel](#) [Create](#)

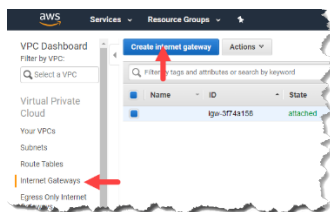
Subnets > Create subnet

### Create subnet

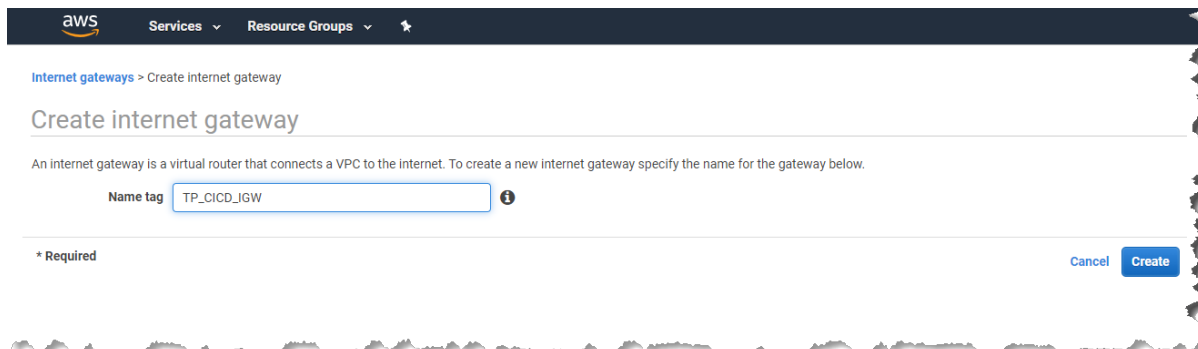
Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone	Availability Zone ID	Route table
	subnet-21060246	available	vpc-b3b-4a8d4	172.31.0.0/20	4091	-	eu-west-1a	euw1-az1	rtb-750a5513
	subnet-3ccac375	available	vpc-b3b-4a8d4	172.31.16.0/20	4091	-	eu-west-1b	euw1-az2	rtb-750a5513
	subnet-f2a7e6a9	available	vpc-b3b-4a8d4	172.31.32.0/20	4091	-	eu-west-1c	euw1-az3	rtb-750a5513
TP_CICD_Private	subnet-073a8b2949a391e1	available	vpc-0f9f6b5c785220db6	172.16.2.0/24	251	-	eu-west-1a	euw1-az1	rtb-09e061ab81ad5f1d3
TP_CICD_Public	subnet-0ef916f3e2feed88	available	vpc-0f9f6b5c785220db6	172.16.1.0/24	251	-	eu-west-1a	euw1-az1	rtb-09e061ab81ad5f1d3

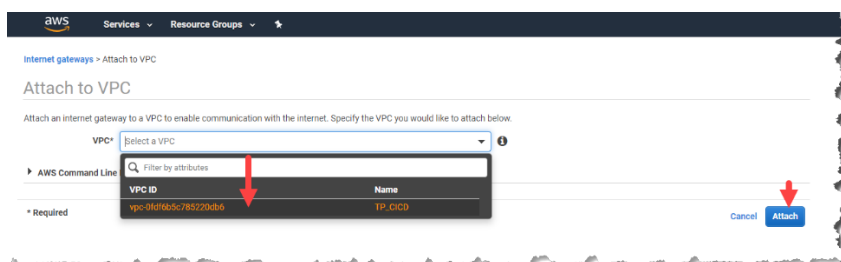
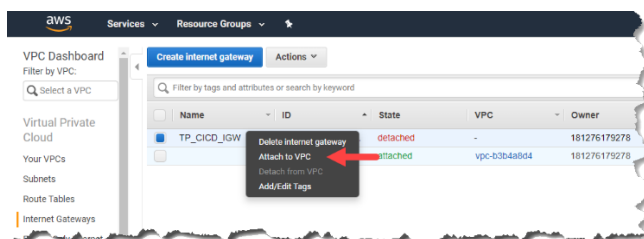
## Internet Gateway



Créer une Internet Gateway, la rattacher au VPC TP\_CICD et la nommer TP\_CICD\_IGW

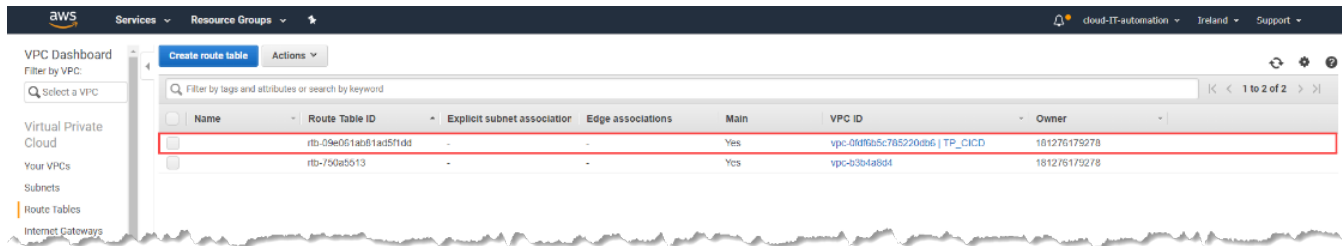


Rattacher l'Internet Gateway au VPC.



## Route Tables

### « Route table » par défaut



Renommer le « Name Tag » de la « route table » créée par default avec le VPC par « TP\_CICD\_Default »

La route par défaut de la route table « TP\_CICD\_Default », pourra être déclarée lorsque nous aurons créé l'instance NAT.

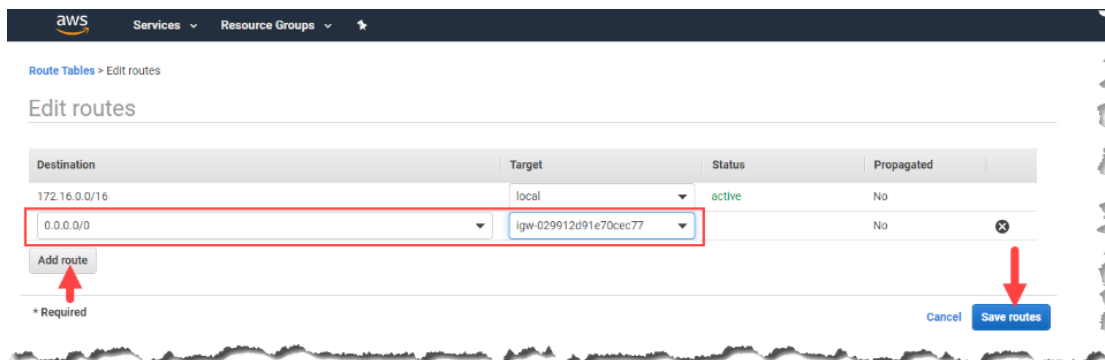
### « Route table » publique

Créer la « route table » TP\_CICD\_Public

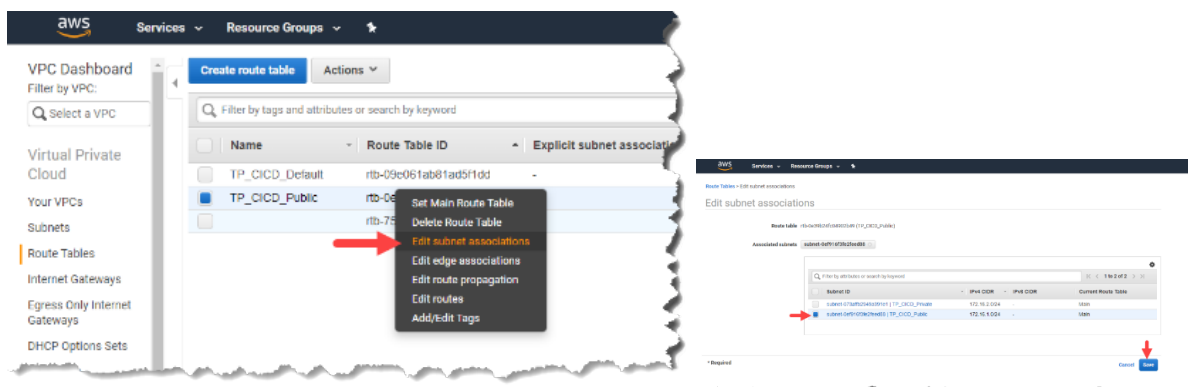
Ajouter la route suivante dans la table de routage.

Destination	Target
0.0.0.0/0	TP_CICD_IGW

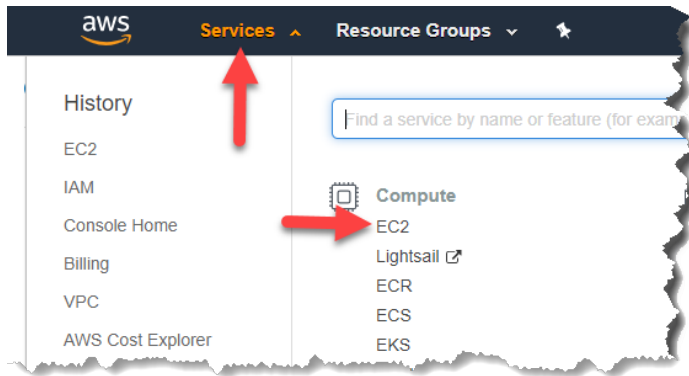
Le fait d'avoir cette route rends mon « subnet » public lorsque je l'attache à ma route table.



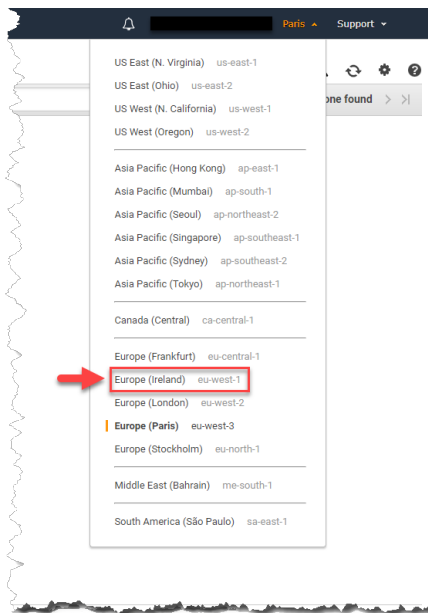
Attacher la route table « TP\_CICD\_Public » au subnet « TP\_CICD\_Public »



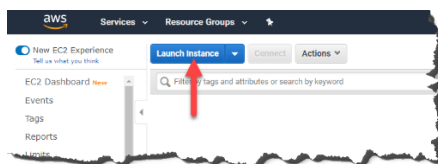
## Jump Host/NAT instance



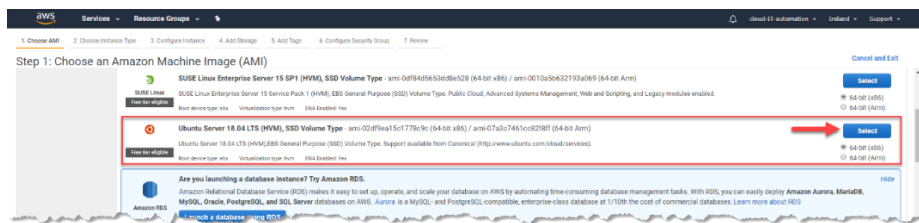
## Sélectionner la région eu-west-1



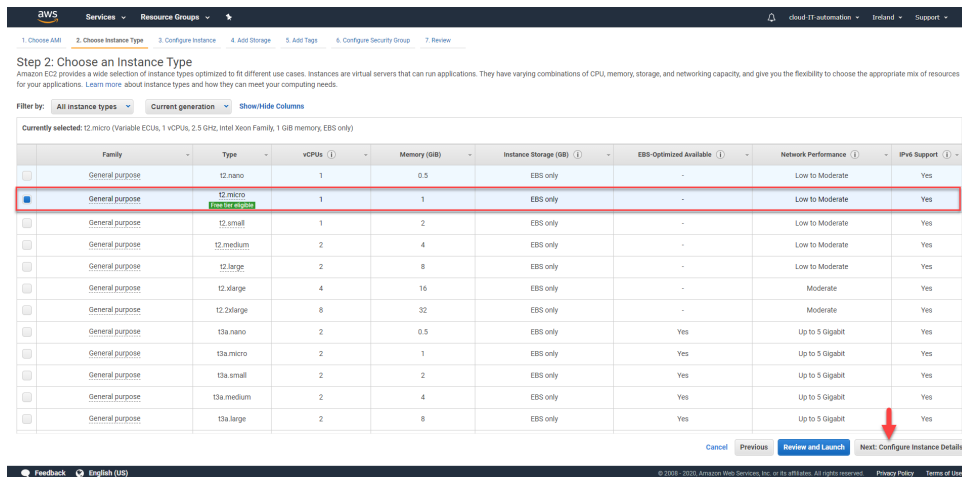
## Démarrer une EC2.



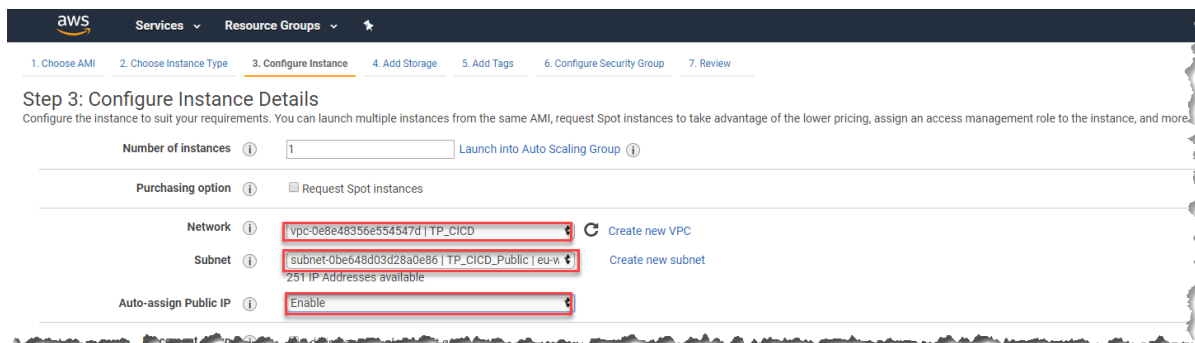
## Utiliser une AMI Publique Ubuntu.



## Utiliser une instance de type T2 Micro.



## Sélectionner votre VPC et le subnet « Public » et activer l'affectation d'une IP publique.



## Insérer les « user data » pour activer l'IP Forwarding sur l'instance :

```
#!/bin/bash
sysctl -w net.ipv4.ip_forward=1
/sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```



Concernant le stockage, laisser les paramètres par défaut.

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snap-0c538ed6cc8ae943	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

[Add New Volume](#)

Free tier eligible customers can get up to 30 GiB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Tags](#)

Définir un « Name Tag » « Nat\_JumpHost »

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 (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes
Name	Nat_JumpHost	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security Group](#)

Autoriser les connexions entrantes sur le port 22 depuis sa propre IP publique (EFREI).

Autoriser toutes les connexions entrantes depuis le sous-réseau privé pour autoriser les flux provenant des futures instances déployées dans le réseau privé vers l'instance de NAT.

aws Services Resource Groups

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: Nat\_Jump

Description: Allow 22 from My IP & Allow All from Private Subnet

Type	Protocol	Port Range	Source	Description
All traffic	All	0-65535	Custom 172.16.2.0/24	e.g. SSH for Admin Desktop
SSH	TCP	22	My IP 192.168.1.100/32	e.g. SSH for Admin Desktop

Add Rule

Cancel Previous **Review and Launch**

Feedback English (US) © 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

aws Services Resource Groups

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

### 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.

AMI Details [Edit AMI](#)

**Ubuntu Server 18.04 LTS (HVM), SSD Volume Type - ami-02d9ea15c1778c9c**  
 Free tier eligible Ubuntu Server 18.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).  
 Root device type: ebs Virtualization type: hvm

Instance Type [Edit instance type](#)

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

Security Groups [Edit security groups](#)

Security group name: Nat\_Jump  
 Description: Allow 22 from My IP & Allow All from Private Subnet

Type	Protocol	Port Range	Source	Description
All traffic	All		172.16.2.0/24	
SSH	TCP	22	192.168.1.100/32	

Instance Details [Edit instance details](#)

Storage [Edit storage](#)

Tags [Edit tags](#)

Cancel Previous **Launch**

Feedback English (US) © 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

## Générer et télécharger une « key pair »

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: TP\_CID

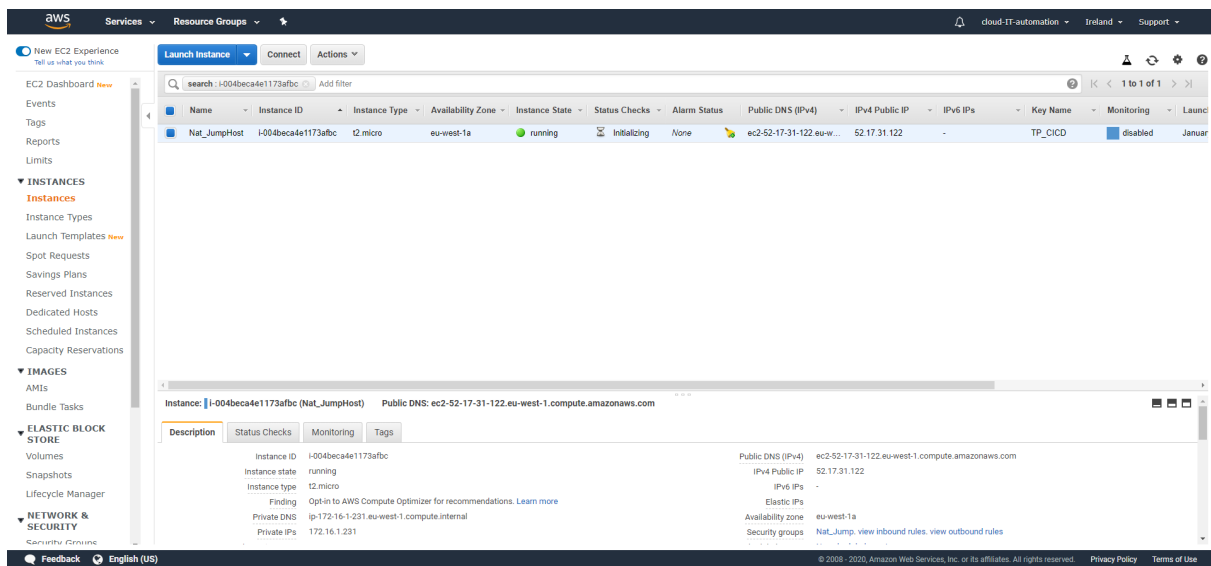
Download Key Pair

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.

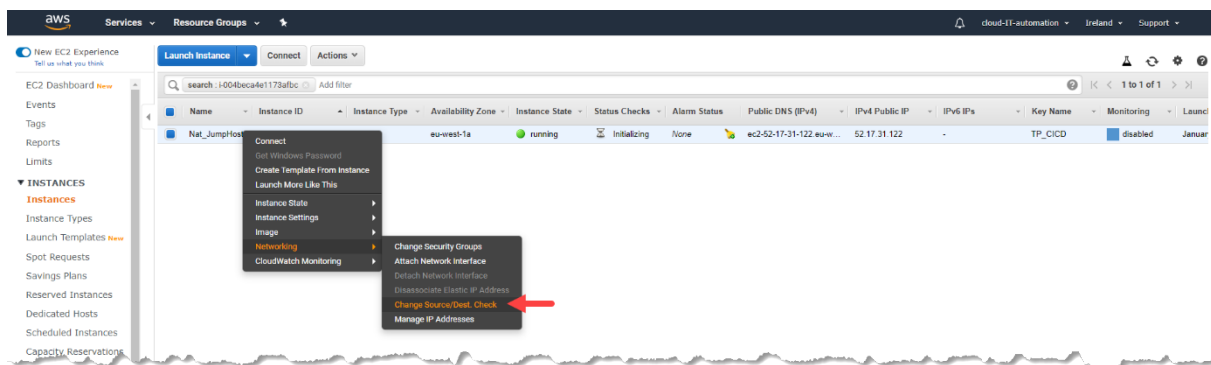
Cancel **Launch Instances**

Retrouver l'instance en cours de démarrage.





## Désactiver source/destination check de l'instance depuis la console



Maintenant, ajouter la route vers la « NAT Instance » dans la « main route table ».

Destination	Target
0.0.0.0/0	NAT Instance

### Tests :

Se connecter au bastion à l'aide de mobaXterm au JumpHost.

Lancer une EC2 dans le private subnet, depuis la console.

Autoriser le 22 depuis l'IP du Nat\_JumpHost.

Se connecter en SSH à votre machine à l'aide de la « private key » précédemment copiée sur le JumpHost.

```
ssh -i <private_key> ubuntu@<ip_publique_JumpHost>
```

Executer un ping vers 8.8.8.8

Naviguer maintenant entre vos instances et déployer des services (Web, ...).

### Quelques questions :

Comment contrôler et limiter l'accès à une instance ?

Quel élément réseau est nécessaire pour que les instances d'un réseau privé puissent communiquer vers internet pour récupérer les packages et updates ?

Sur AWS quelles sont les propriétés qui caractérisent un « Public Subnet » ?

Les « Security Groups » sont-ils stateless ou statefull ?

Qu'est-ce qu'une « Default Route » Table ?

Comment faire pour me connecter à une instance dans un sous-réseau privé ?

Détruire toutes vos instances à la fin de votre travail pour éviter de gaspiller du crédit AWS inutilement !!!