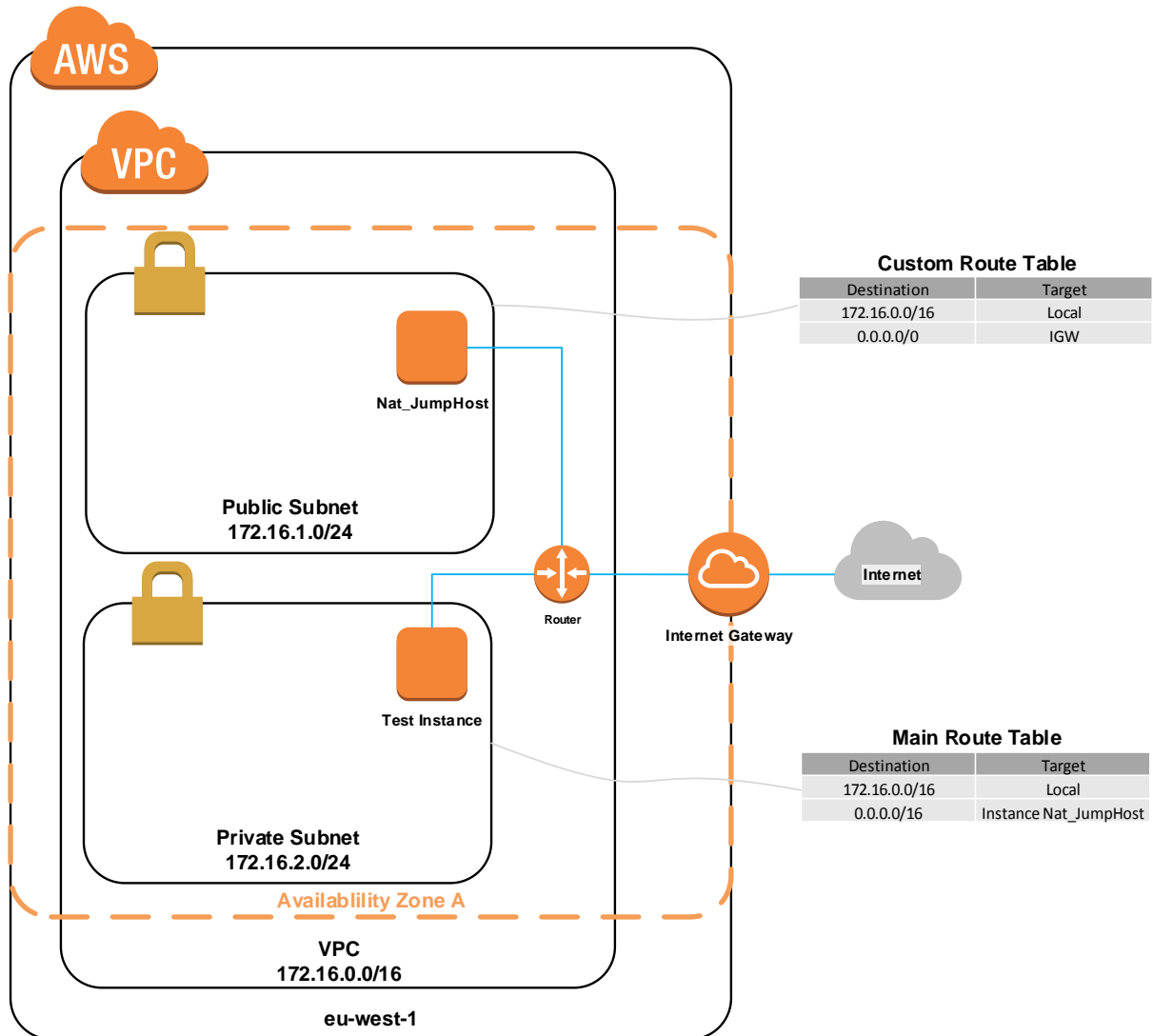
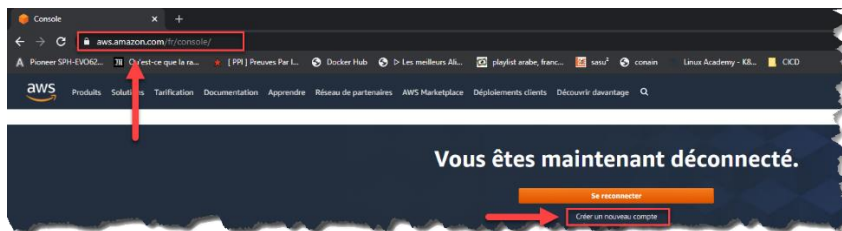


TP-1 Déploiement sous AWS

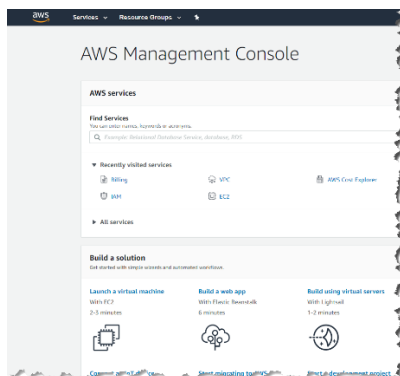


AWS Account

Créer un compte AWS Education avec un email EFREI pour obtenir un code promotionnel de 100\$ de crédit AWS offert.



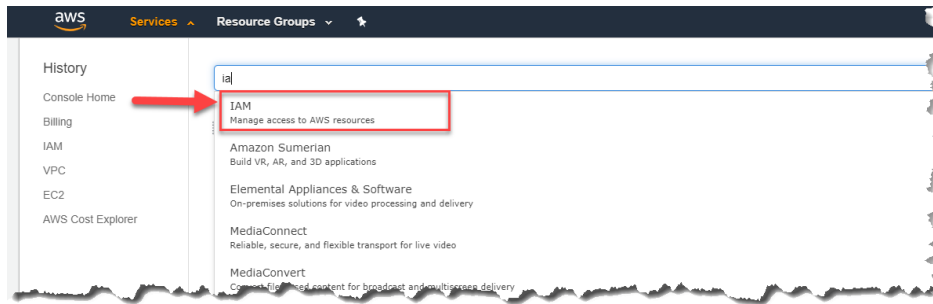
Se connecter ensuite avec les identifiants root du compte. (email + password).



Ajouter le code promotionnel dans le service « Billing » de votre compte AWS personnel.

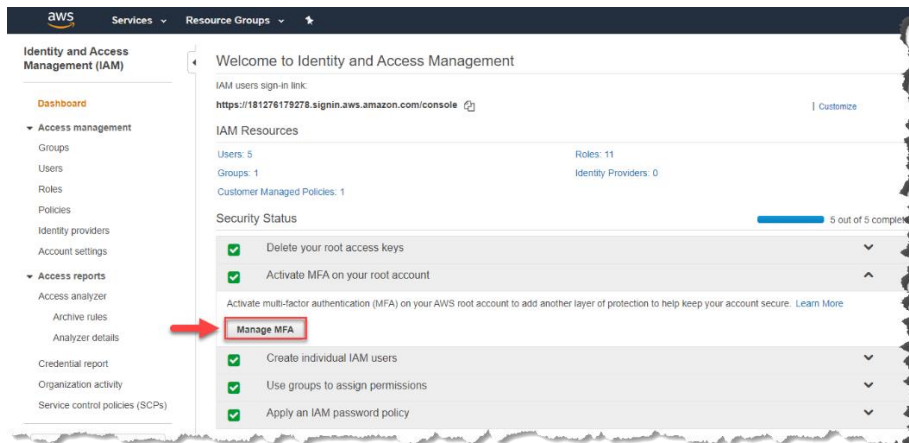
<https://aws.amazon.com/premiumsupport/knowledge-center/add-aws-promotional-code/>

Root user



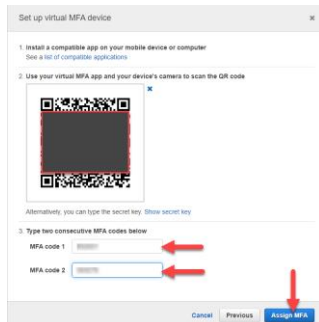
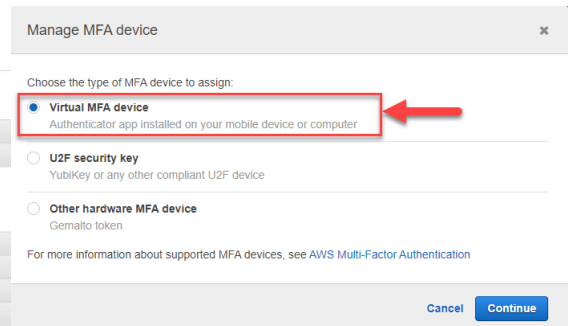
Pour des raisons de sécurité, prendre l'habitude de toujours configurer un MFA pour le user « root » que pour les utilisateurs créés dans IAM.

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



Your Security Credentials

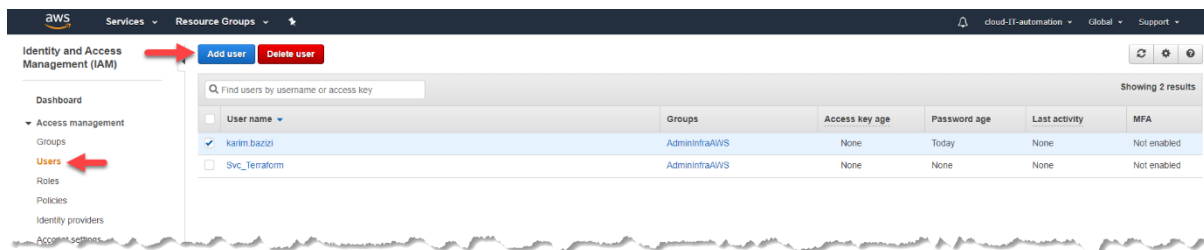
Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the IAM Console.



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 :

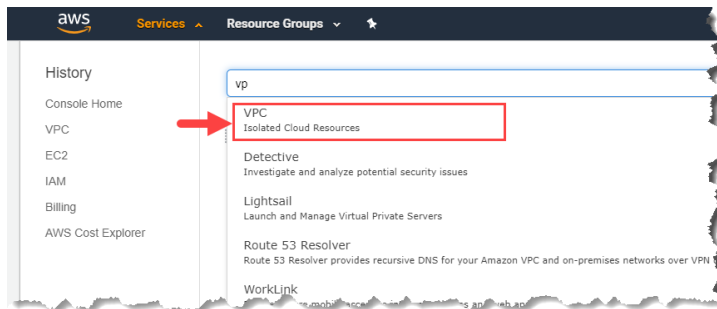
https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_aws_my-sec-creds-self-manage.html

VPC (Virtual Private Cloud)

https://docs.aws.amazon.com/fr_fr/vpc/latest/userguide/VPC_Subnets.html

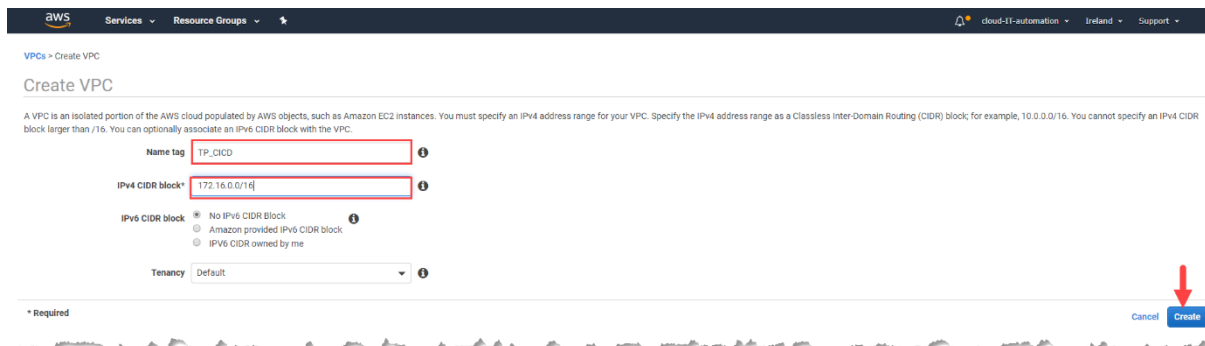
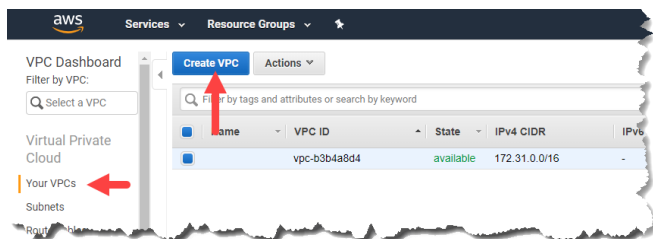
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html

Se rendre dans le service VPC.

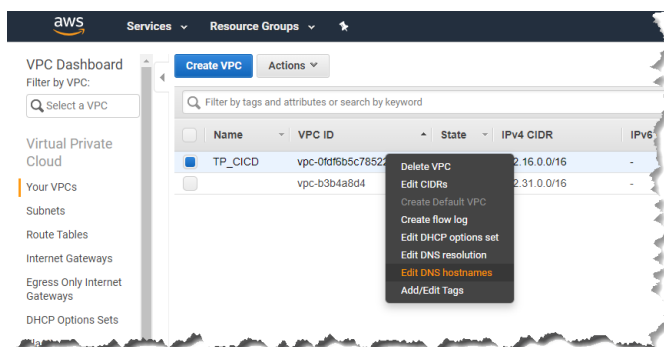


Créer un VPC avec le CIDR suivant : 172.16.0.0/16

Name Tag	CIDR
TP_CICD	172.16.0.0/16



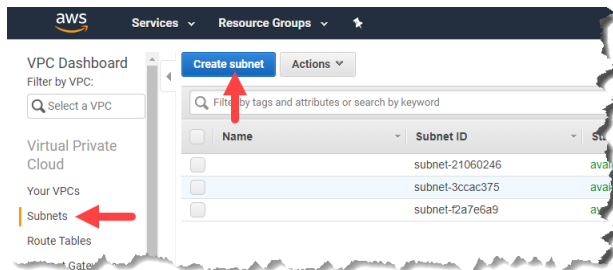
Une fois le VPC créé, activer la fonctionnalité **DNS hostnames**.



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: TP_CICD_Public

VPC*: vpc-0f9f6b5c785220db6

Availability Zone: eu-west-1a

VPC CIDRs	CIDR	Status	Status Reason
	172.16.0.0/16	associated	

IPv4 CIDR block*: 172.16.1.0/24

* 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: TP_CICD_Private

VPC*: vpc-0f9f6b5c785220db6

Availability Zone: eu-west-1a

VPC CIDRs	CIDR	Status	Status Reason
	172.16.0.0/16	associated	

IPv4 CIDR block*: 172.16.2.0/24

* Required

Cancel Create

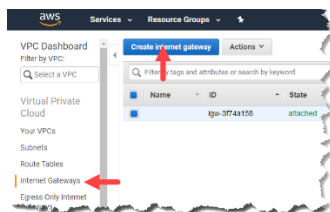
Subnets > Create subnet

Create subnet

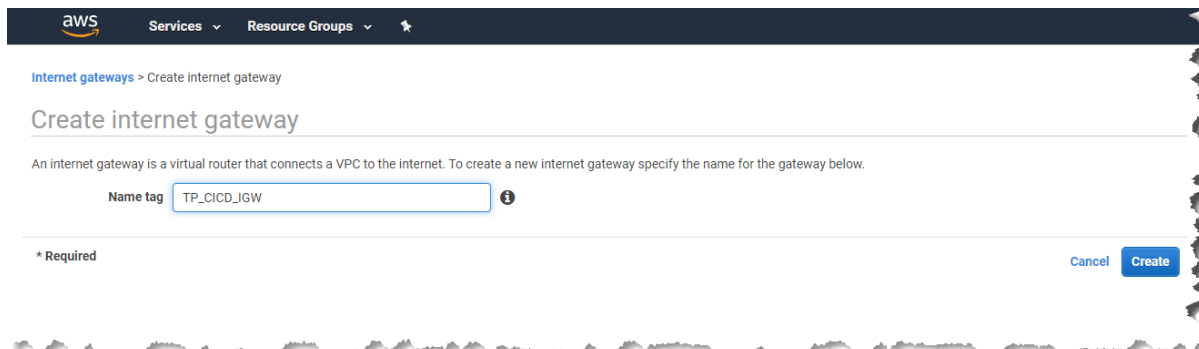
Specify your subnet's IP address block in CIDR format, for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone	Availability Zone ID	Route table
	subnet-21060246	available	vpc-b3b4a8d4	172.31.0.0/20	4091	-	eu-west-1a	euw1-az1	rtb-750a5513
	subnet-3ccac375	available	vpc-b3b4a8d4	172.31.16.0/20	4091	-	eu-west-1b	euw1-az2	rtb-750a5513
	subnet-f2a7e6a9	available	vpc-b3b4a8d4	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-09e061ab81ad5ffdd
TP_CICD_Public	subnet-0e916f3e2feed988	available	vpc-0f9f6b5c785220db6	172.16.1.0/24	251	-	eu-west-1a	euw1-az1	rtb-09e061ab81ad5ffdd

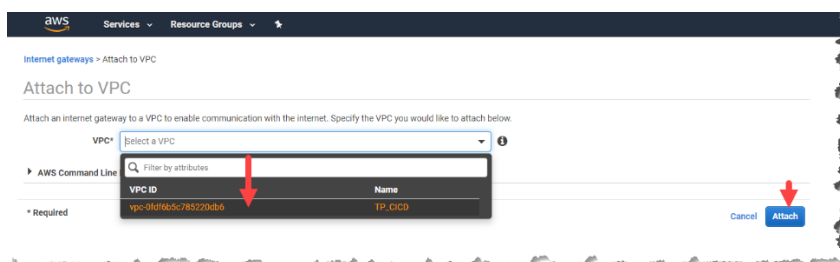
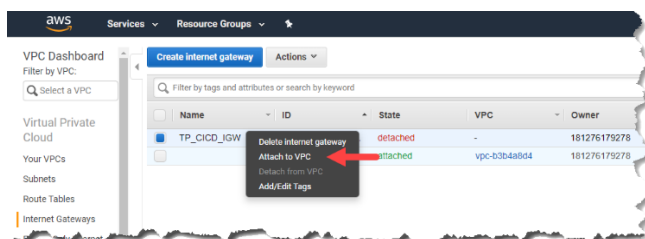
Internet Gateway



Créer une Internet Gateway, la rattacher au VPC TP_CICD et la nommer TP_CICD_IGW

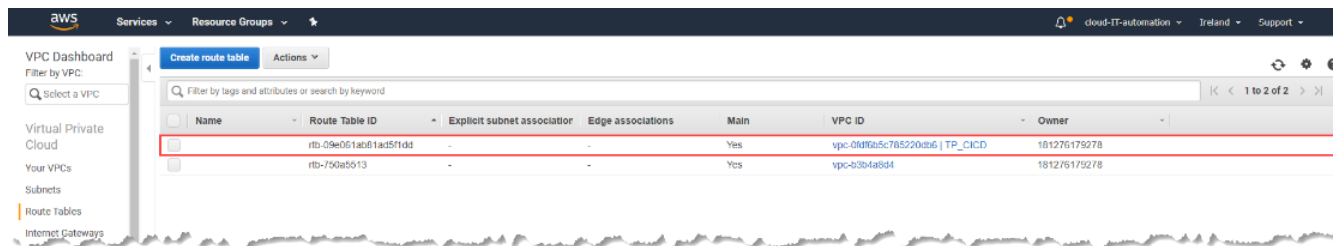


Rattacher l'internet Gateway au VPC.



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.

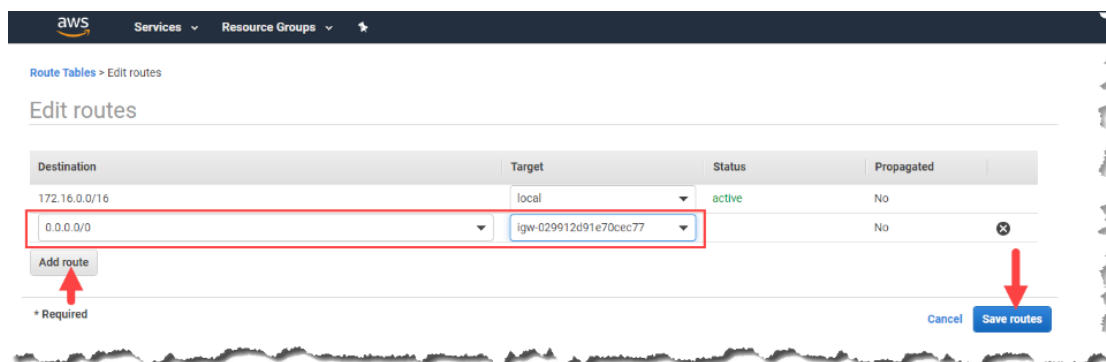
« Route table » publique

Créer la « route table » TP_CICD_Public

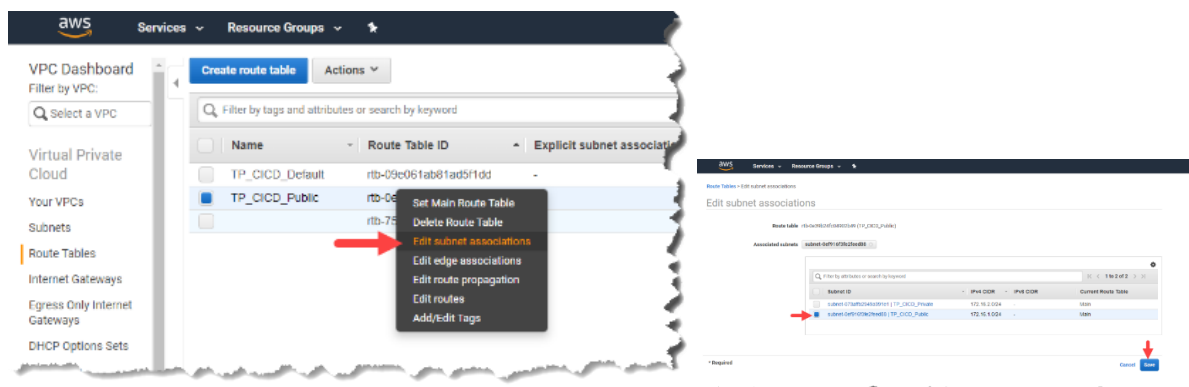
Ajouter la route suivante dans la table de routage.

Destination	Target
0.0.0.0/0	TP_CICD_IGW

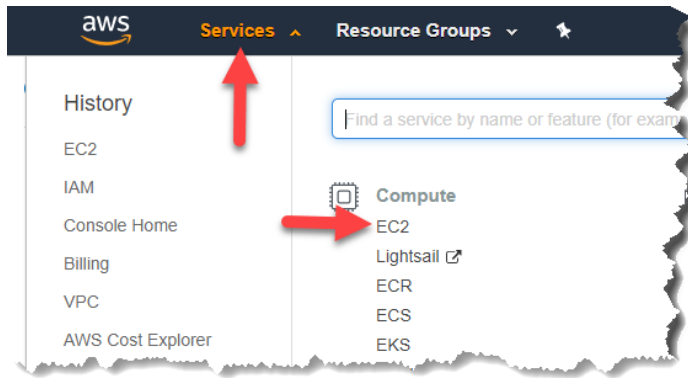
Le fait d'avoir cette route rends mon « subnet » public lorsque je l'attache à ma route table.



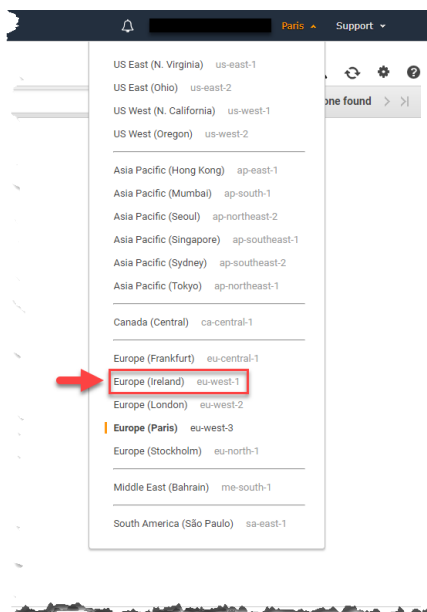
Attacher la route table « TP_CICD_Public » au subnet « TP_CICD_Public »



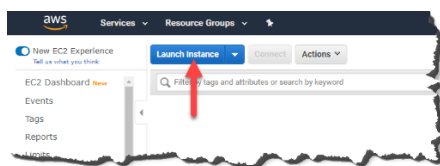
Jump Host/NAT instance



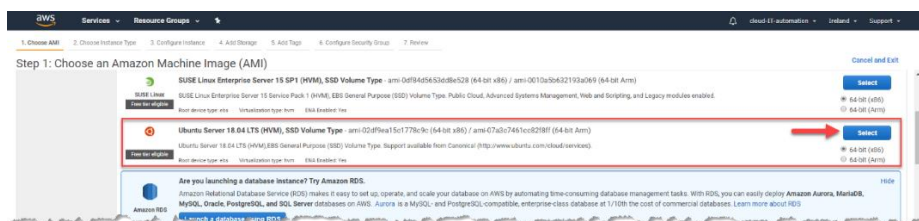
Sélectionner la région eu-west-1



Démarrer une EC2.



Utiliser une AMI Publique Ubuntu.



Utiliser une instance de type T2 Micro.

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

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

Currently selected: t2.micro (Variable ECU, 1 vCPU, 2.5 GHz, Intel Xeon Family, 1 GB memory, EBS only)

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
General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
General purpose	t3a.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
General purpose	t3a.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes
General purpose	t3a.small	2	2	EBS only	Yes	Up to 5 Gigabit	Yes
General purpose	t3a.medium	2	4	EBS only	Yes	Up to 5 Gigabit	Yes
General purpose	t3a.large	2	8	EBS only	Yes	Up to 5 Gigabit	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

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

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 access management role to the instance, and more.

Number of instances: 1 Launch into Auto Scaling Group

Purchasing option: ☐ Request Spot instances

Network: vpc-0e8e48356e554547d | TP_CICD Create new VPC

Subnet: subnet-0be648d03d28a0e86 | TP_CICD_Public | eu-w Create new subnet
251 IP Addresses available

Auto-assign Public IP: Enable

Cancel Previous Review and Launch Next: Add Storage

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
```

Advanced Details

User data: ☒ As text ☐ As file ☐ Input is already base64 encoded

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

Cancel Previous Review and Launch Next: Add Storage

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 (MiB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snap-0c33d8edfcc8ae943	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 GB 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.

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 193.46.193.193	e.g. SSH for Admin Desktop

[Add Rule](#)

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

aws Services Resource Groups

cloud IT automation Ireland Support

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-02df9ea15c1778c9c

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	198.51.100.0/24	

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_CIDC

Download Key Pair

You have to download the **private key file** (*.pem file) before you can continue. **Save 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.

aws Services Resource Groups

cloud IT automation Ireland Support

New EC2 Experience

Launch Instance Connect Actions

EC2 Dashboard

Events

Tags

Reports

Limits

INSTANCES

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Scheduled Instances

Capacity Reservations

IMAGES

AMIs

Bundle Tasks

ELASTIC BLOCK STORE

Volumes

Snapshots

Lifecycle Manager

NETWORK & SECURITY

Security Groups

Launch Instance

search: i-004beca4e1173afbcb Add filter

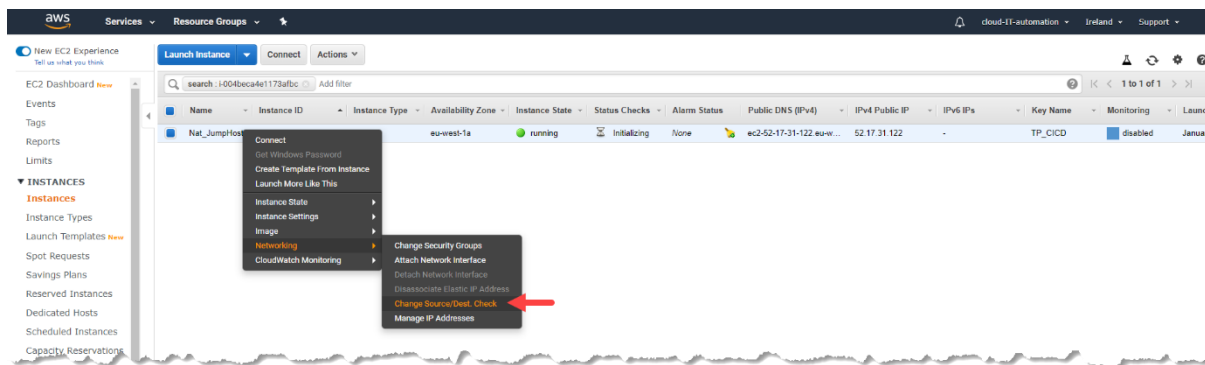
Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs	Key Name	Monitoring	Launch
Nat_JumpHost	i-004beca4e1173afbcb	t2.micro	eu-west-1a	running	Initializing	None	ec2-52-17-31-122.eu-west-1.compute.amazonaws.com	52.17.31.122	-	TP_CIDC	disabled	Januar

Instance: i-004beca4e1173afbcb (Nat_JumpHost) Public DNS: ec2-52-17-31-122.eu-west-1.compute.amazonaws.com

Description	Status Checks	Monitoring	Tags
Instance ID: i-004beca4e1173afbcb	Instance state: running	Instance type: t2.micro	Finding: Opt-in to AWS Compute Optimizer for recommendations. Learn more
Private DNS: ip-172-16-1-231.eu-west-1.compute.internal	Private IPs: 172.16.1.231	Availability zone: eu-west-1a	Security groups: Nat_Jump, view inbound rules, view outbound rules

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

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

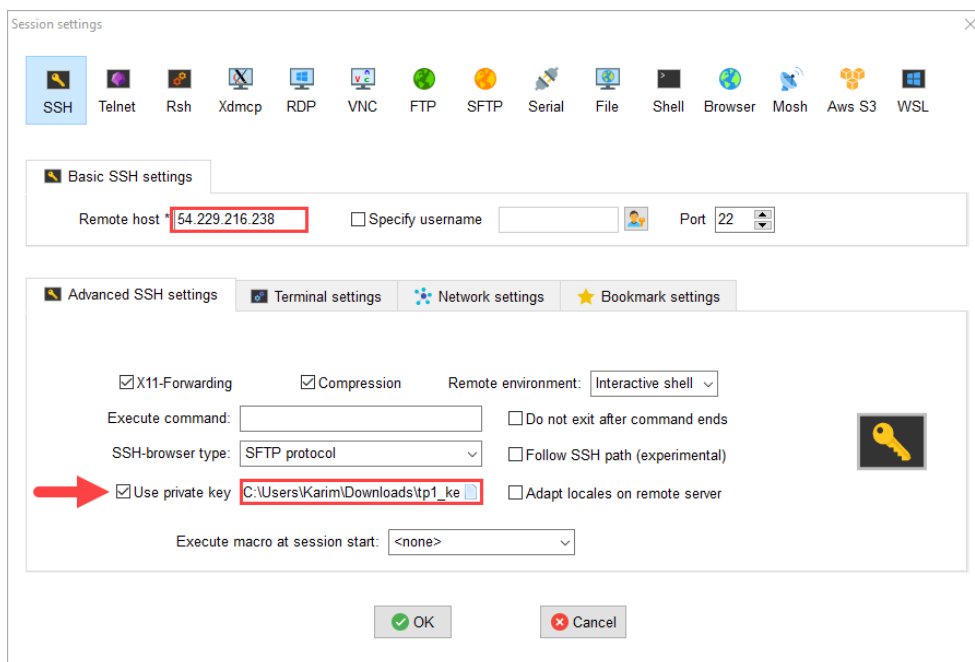


Maintenant, ajouter la route vers la « NAT Instance » dans la « main route table ».

Destination	Target
0.0.0.0/0	NAT Instance

Tests

Se connecter au bastion à l'aide de mobaXterm ou de putty.



Lancer une EC2 « T2.micro » dans le private subnet, depuis la console.

Créer un « Sécurité Group » et autoriser le port 22 entrant depuis l'IP privée 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_PrivateHost>
```

Exécuter un ping vers 8.8.8.8

Eteindre ou détruire vos instances à la fin de votre travail pour éviter de gaspiller du crédit AWS inutilement !!!