

# Lab 2: Instances EC2 dans un VPC

## Cloud Computing

Université Claude Bernard Lyon 1 May 28, 2026

### Assignment Overview

#### Document Contents:

1. Objectif .....	2
2. Pré-requis .....	2
2.1. Conseils .....	2
3. Contexte .....	2
4. Étapes .....	3
4.1. Étape 1: Lire les fichiers Terraform .....	3
4.2. Étape 2: Initialiser le projet et déployer .	3
4.3. Étape 3: Explorer le state .....	3
4.4. Étape 4: Vérifier via awscli .....	3
4.5. Étape 5: Destruction des ressources .....	3
5. Questions .....	5
6. Aller plus loin .....	5

#### Assignment Details:

- **Course:** Cloud Computing
- **Instructor:** Hugo Blanc
- **Software:** Terraform, AWS, LocalStack
- **Duration:** ~ 1 heure
- **Lab Number:** Lab 2

# Objectif

---

Ce lab couvre la création d'une instance EC2 dans un VPC complètement configuré.

## Pré-requis

---

- Avoir Terraform (>= 1.5.0);
- avoir tflocal (pip3 install terraform-local);
- avoir LocalStack qui tourne;
- avoir la CLI AWS (voir la documentation officielle).

## Conseils

Je vous recommande de faire les alias suivants:

```
alias tf=tflocal
alias aws="aws --endpoint-url=http://localhost:4566"
```

Également, pour simplifier l'usage de la CLI AWS, je vous recommande de définir des faux credentials pour éviter les erreurs:

```
export AWS_ACCESS_KEY_ID=test
export AWS_SECRET_ACCESS_KEY=test
export AWS_DEFAULT_REGION=eu-west-1
```

## Contexte

---

**LocalStack** émule des services AWS en local sur la machine, sur le port 4566. La commande `tflocal` est un wrapper autour de Terraform qui permet de rediriger les appels d'API vers LocalStack.

# Étapes

---

## Étape 1: Lire les fichiers Terraform

Avant d'entrer des commandes, il vous faut lire attentivement chaque fichier `.tf` présent dans ce dossier.

### Question

Identifiez:

- Les variables déclarées et leurs valeurs;
- les ressources qui seront créées;
- Les sorties qui seront affichées.

## Étape 2: Initialiser le projet et déployer

```
tflocal init
tflocal plan
tflocal apply -var="student_name=your-name"
```

### Question

Observer l'ordre dans lequel Terraform crée les ressources. Est-ce ce que vous vous attendiez à voir ?

## Étape 3: Explorer le state

```
tflocal state list
tflocal state show aws_instance.web
```

### Question

Identifiez l'adresse IP privée assignée à l'instance, l'identifiant AMI utilisé ainsi que le Security Group associé.

## Étape 4: Vérifier via awscli

```
aws --endpoint-url=http://localhost:4566 ec2 describe-vpcs
aws --endpoint-url=http://localhost:4566 ec2 describe-instances
aws --endpoint-url=http://localhost:4566 ec2 describe-security-groups
```

### Question

Les résultats correspondent-ils à vos attentes ?

## Étape 5: Destruction des ressources

```
tflocal destroy -var="student_name=your-name"
```

**Question**

Observez l'ordre de destruction. Est-il le même que l'ordre de création ?

# Questions

---

1. **Combien de ressources sont créées par Terraform dans ce TP ?** Listez-les et expliquez le rôle de chacune.
2. **Que se passe-t-il si l'on supprime l'Internet Gateway de la configuration ?** Quelles ressources sont impactées, et pourquoi ?
3. **Le Security Group autorise les connexions entrantes sur les ports 22 et 80. Quel est son comportement pour les connexions sortantes ?** Expliquez la règle d'egress présente dans la configuration.
4. **Quel est le but du champ `user_data` dans l'instance EC2 ?** Quand ce script est-il exécuté ? Peut-il être modifié après la création de l'instance ?
5. **Expliquez la différence entre un Security Group et une Network ACL.** Lequel est stateful, lequel est stateless ?
6. **Pourquoi la table de routage est associée avec le subnet plutôt qu'avec le VPC ?** Quel avantage cela offre-t-il dans une architecture multi-subnets ?
7. **Observez les dépendances implicites entre les ressources.** Terraform sait que le subnet dépend du VPC grâce à la référence `aws_vpc.main.id`. Dessinez le graph de dépendance complet.

## Aller plus loin

---

- Ajoutez un second subnet privé (sans routage vers l'Internet Gateway).
- Ajoutez une seconde instance dans ce subnet privé.
- Modifiez le Security Group pour autoriser le port 443 en ingress.
- Ajoutez une Elastic IP et associez-la avec l'instance.