

---

## Rapport TP4

INF8102 - Sécurité dans les environnements infonuagiques

---

Eric-Pascal TIONFE

(2471139)

Lucas VINCENT

(2486417)

Novembre-Décembre 2025

## Table des matières

|  |    |
|--|----|
| 1. Introduction .....                            | 2  |
| 2. Déploiement à l'aide de Cloud Formation ..... | 3  |
| 2.1. Mise en place du VPC .....                  | 3  |
| 2.2. Mise en place de l'instance EC2 .....       | 4  |
| 2.3. Mise en place du compartiment S3 .....      | 5  |
| 2.4. Scan des vulnérabilités .....               | 5  |
| 3. Déploiement à l'aide de boto3 .....           | 6  |
| 3.1. Question 1 .....                            | 6  |
| 3.2. Question 2 .....                            | 7  |
| 3.3. Question 3 .....                            | 8  |
| 3.3.1. Partie 1 .....                            | 8  |
| 3.3.2. Partie 2 .....                            | 9  |
| 3.3.3. Partie 3 .....                            | 9  |
| 3.4. Question 4 .....                            | 10 |

## 1. Introduction

L'objectif de ce laboratoire est d'apprendre à mettre en œuvre une architecture en **Infrastructure as Code**. Au cours de cette séance pratique, nous avons travaillé les points suivants :

- Mise en place d'un Virtual Private Cloud (VPC) et ses périphériques à l'aide CloudFormation.
- Mise en place d'un compartiment S3 à l'aide de CloudFormation.
- Mise en place d'une instance EC2 à l'aide de CloudFormation.
- Scan des vulnérabilités à partir des fichiers de configuration à l'aide de trivy.
- Mise en place d'un Virtual Private Cloud (VPC) et ses périphériques à l'aide de *boto3*.
- Sécurisation du VPC en modifiant le *script python boto3*.
- Mise en place d'un compartiment S3 à l'aide de *boto3*.
- Sécurisation du compartiment S3 à l'aide de *boto3*.

## 2. Déploiement à l'aide de Cloud Formation

### 2.1. Mise en place du VPC

**Prérequis - Préparer le modèle**

Vous pouvez également créer un modèle en analysant vos ressources existantes dans le [Générateur IaC](#).

**Préparer le modèle**

Chaque pile est basée sur un modèle. Un modèle est un fichier au format JSON ou YAML qui contient les informations de configuration sur les ressources AWS que vous souhaitez inclure dans la pile.

Choissez un modèle existant  
Téléchargez ou choisissez un modèle existant.

Créez à partir d'Infrastructure Composer  
Créez un modèle à l'aide d'un créateur visuel.

**Spécifier un modèle** [Infos](#)

Ce Référentiel GitHub contient des exemples de modèles CloudFormation qui peuvent vous aider à démarrer de nouveaux projets d'infrastructure. [En savoir plus](#).

**Source du modèle**

La sélection d'un modèle génère un URL Amazon S3 où il sera stocké. Un modèle est un fichier JSON ou YAML qui décrit les ressources et les propriétés de votre pile.

URL Amazon S3  
Fournissez une URL Amazon S3 à votre modèle.

Charger un fichier de modèle  
Chargez votre modèle directement sur la console.

Synchronisation depuis Git  
Synchronisez un modèle depuis votre référentiel Git.

**Charger un fichier de modèle**

Choisir un fichier

Fichier au format JSON ou YAML

URL S3 : <https://s3.us-east-1.amazonaws.com/cf-templates-1lv4lsbhg3rh-us-east-1/2025-12-01T234944.684Z1bl-vpc.yaml>

[Afficher dans Infrastructure Composer](#)

Fig. 1. – Création à partir du modèle json.

**Indiquer le nom de la pile**

**Nom de la pile**

cloudformation-114-vpc

Le nom de la pile doit contenir uniquement des lettres (a-z, A-Z), des chiffres (0-9) et des tirets (-) et commencer par une lettre. 128 caractères maximum. Nombre de caractères : 22/128.

**Paramètres**

Les paramètres sont définis dans votre modèle et vous permettent de saisir des valeurs personnalisées lorsque vous créez ou mettez à jour une pile.

**EnvironmentName**  
environment is prefixed to resource names.  
*Saisir String*

**PrivateSubnet1CIDR**  
private subnet in Availability Zone 1  
*10.0.128.0/24*

**PrivateSubnet2CIDR**  
private subnet in Availability Zone 2  
*10.0.144.0/24*

**PublicSubnet1CIDR**  
public subnet in Availability Zone 1  
*10.0.0.0/24*

**PublicSubnet2CIDR**  
public subnet in Availability Zone 2  
*10.0.16.0/24*

**VpcCIDR**  
VPC polystudent-vpc  
*10.0.0.0/16*

Fig. 2. – Validation des paramètres.

| Événements d'opération (6)   |  |                                 |                                     |                                      |                        |  |
|------------------------------|--|---------------------------------|-------------------------------------|--------------------------------------|------------------------|--|
|                              | ID logique                               | Statut                          | Statut détaillé                     | Motif du statut                      | Invocations de crochet | Actions                                  |
| 01-12-2025 18:54:35 UTC-0500 | InternetGateway <a href="#">🔗</a>        | <span>CREATE_IN_PROGRESS</span> | <span>CONFIGURATION_COMPLETE</span> | Eventual consistency check initiated | -                      | <a href="#">🔗</a> <a href="#">Copier</a> |
| 01-12-2025 18:54:34 UTC-0500 | InternetGateway <a href="#">🔗</a>        | <span>CREATE_IN_PROGRESS</span> | -                                   | Resource creation Initiated          | -                      | <a href="#">🔗</a> <a href="#">Copier</a> |
| 01-12-2025 18:54:34 UTC-0500 | VPC <a href="#">🔗</a>                    | <span>CREATE_IN_PROGRESS</span> | -                                   | Resource creation Initiated          | -                      | <a href="#">🔗</a> <a href="#">Copier</a> |
| 01-12-2025 18:54:33 UTC-0500 | VPC                                      | <span>CREATE_IN_PROGRESS</span> | -                                   | -                                    | -                      | <a href="#">🔗</a> <a href="#">Copier</a> |
| 01-12-2025 18:54:33 UTC-0500 | InternetGateway                          | <span>CREATE_IN_PROGRESS</span> | -                                   | -                                    | -                      | <a href="#">🔗</a> <a href="#">Copier</a> |
| 01-12-2025 18:54:30 UTC-0500 | cloudformation-114-vpc <a href="#">🔗</a> | <span>CREATE_IN_PROGRESS</span> | -                                   | User Initiated                       | -                      | <a href="#">🔗</a> <a href="#">Copier</a> |

Fig. 3. – Crédit de VPC.

## 2.2. Mise en place de l'instance EC2

### Examiner et créer

#### Étape 1: Spécifier un modèle

[Modifier](#)

##### Prérequis - Préparer le modèle

###### Modèle

Le modèle est prêt

###### Modèle

###### URL modèle

<https://s3.us-east-2.amazonaws.com/cf-templates-1lv4ilsbhg3rh-us-east-2/2025-12-01T231236.568Z40b-ec2.json>

###### Description de la pile

Deploy a secure EC2 instance on the public subnet of AZ1

Fig. 4. – Crédit à partir d'un modèle json.

### Événements d'opération (7)

[Rechercher des événements](#)
[Afficher uniquement les échecs](#)


| Horodatage                   | ID logique                               | Statut                          | Statut détaillé                     | Motif du statut                      | Invocations de crochet |
|------------------------------|--|---------------------------------|-------------------------------------|--------------------------------------|------------------------|
| 01-12-2025 19:00:15 UTC-0500 | cloudformation-114-ec2 <a href="#">🔗</a> | <span>CREATE_COMPLETE</span>    | -                                   | -                                    | -                      |
| 01-12-2025 19:00:14 UTC-0500 | EC2Instance <a href="#">🔗</a>            | <span>CREATE_COMPLETE</span>    | -                                   | -                                    | -                      |
| 01-12-2025 19:00:14 UTC-0500 | cloudformation-114-ec2 <a href="#">🔗</a> | <span>CREATE_IN_PROGRESS</span> | <span>CONFIGURATION_COMPLETE</span> | Eventual consistency check initiated | -                      |
| 01-12-2025 19:00:14 UTC-0500 | EC2Instance <a href="#">🔗</a>            | <span>CREATE_IN_PROGRESS</span> | <span>CONFIGURATION_COMPLETE</span> | Eventual consistency check initiated | -                      |
| 01-12-2025 19:00:02 UTC-0500 | EC2Instance <a href="#">🔗</a>            | <span>CREATE_IN_PROGRESS</span> | -                                   | Resource creation Initiated          | -                      |
| 01-12-2025 19:00:00 UTC-0500 | EC2Instance                              | <span>CREATE_IN_PROGRESS</span> | -                                   | -                                    | -                      |
| 01-12-2025 18:59:58 UTC-0500 | cloudformation-114-ec2 <a href="#">🔗</a> | <span>CREATE_IN_PROGRESS</span> | -                                   | User Initiated                       | -                      |

Fig. 5. – Crédit de l'instance EC2.

## 2.3. Mise en place du compartiment S3

**Examiner et créer**

**Étape 1: Spécifier un modèle**

**Prérequis - Préparer le modèle**

**Modèle**  
Le modèle est prêt

**Modèle**

**URL modèle**  
<https://s3.us-east-2.amazonaws.com/cf-templates-1lv4ilsbhg3rh-us-east-2/2025-12-01T230713.81926cp-s3.json>

**Description de la pile**  
S3 bucket

Fig. 6. – Crédit à partir du modèle json.

| Événements d'opération (5)   |            |                    |                 |                             |                        |
|------------------------------|------------|--------------------|-----------------|-----------------------------|------------------------|
| Horodatage                   | ID logique | Statut             | Statut détaillé | Motif du statut             | Invocations de crochet |
| 01-12-2025 18:10:54 UTC-0500 | s3-114 ↗   | CREATE_COMPLETE    | -               | -                           | -                      |
| 01-12-2025 18:10:53 UTC-0500 | S3Bucket ↗ | CREATE_COMPLETE    | -               | -                           | -                      |
| 01-12-2025 18:10:39 UTC-0500 | S3Bucket ↗ | CREATE_IN_PROGRESS | -               | Resource creation Initiated | -                      |
| 01-12-2025 18:10:38 UTC-0500 | S3Bucket   | CREATE_IN_PROGRESS | -               | -                           | -                      |
| 01-12-2025 18:10:37 UTC-0500 | s3-114 ↗   | CREATE_IN_PROGRESS | -               | User Initiated              | -                      |

Fig. 7. – Crédit du compartiment S3.

## 2.4. Scan des vulnérabilités

Nous avons exécuté la commande suivante sur le dossier des configurations avec CloudFormation :

```
trivy fs --scanners vuln,secret,misconfig CloudFormation
```

|                           |  |
|---------------------------|--|
| 2025-12-01T19:05:25-05:00 | INFO [vuln] Vulnerability scanning is enabled  |
| 2025-12-01T19:05:25-05:00 | INFO [misconfig] Misconfiguration scanning is enabled  |
| 2025-12-01T19:05:26-05:00 | INFO [secret] Secret scanning is enabled   |
| 2025-12-01T19:05:26-05:00 | INFO [secret] If your scanning is slow, please try '--scanners vuln,misconfig' to disable secret scanning  |
| 2025-12-01T19:05:26-05:00 | INFO [secret] Please see <a href="https://trivy.dev/v0.67/docs/scanner/secret#recommendation for faster secret detection">https://trivy.dev/v0.67/docs/scanner/secret#recommendation for faster secret detection</a> |
| 2025-12-01T19:05:26-05:00 | WARN [cloudformation parser] Missing parameter values file_path="vpc.yaml" parameters="EnvironmentName"  |
| 2025-12-01T19:05:26-05:00 | INFO Number of language-specific files num=0   |
| 2025-12-01T19:05:26-05:00 | INFO Detected config files num=3   |

Report Summary

| Target   | Type           | Vulnerabilities | Secrets | Misconfigurations |
|----------|----------------|-----------------|---------|-------------------|
| ec2.json | cloudformation | -               | -       | 2                 |
| s3.json  | cloudformation | -               | -       | 1                 |
| vpc.yaml | cloudformation | -               | -       | 15                |

Legend:  
- '-' : Not scanned  
- '0' : Clean (no security findings detected)

Fig. 8. – Extrait du résultat du scan de trivy.

### 3. Déploiement à l'aide de boto3

#### 3.1. Question 1

Le VPC, ses deux sous-réseaux, sa passerelle Internet, ses passerelles NAT, ses quatre instances et son groupe de sécurité ont été construit à l'aide de boto3. Les images ci-dessous illustrent le bon fonctionnement du Script.

```
[INFO] Connection to aws session
[INFO] Create VPC
VPC Id : vpc-002aee732e8e99a7a
[INFO] Create subnets
Subnets Id : ['public_az1': 'subnet-0f6a4a61821b5e1c0', 'private_az1': 'subnet-0e4da2f6a79ec398d', 'public_az2': 'subnet-0c0fefef3cd7db1c5a4', 'private_az2': 'subnet-04b3e9debe3d0315d']
[INFO] Create internet gateway
[INFO] Create nat gateways
[INFO] Create security group
[INFO] Security group : sg-0c23b88b9c5036c41
[INFO] Enable automatic public IP
[INFO] Create EC2 in private and public subnets
[INFO] End
```

Fig. 9. – L'exécution s'est déroulée sans erreurs. Le terminal décrit les étapes.



Fig. 10. – Le VPC a été créé.



Fig. 11. – Les sous-réseaux publics sont reliés par une passerelle internet avec le réseau extérieur et les sous-réseaux privés sont reliés avec deux passerelles NAT.

|   | Name                    | ID d'instance       | État de l'in... | Type d'insta... | Contrôle des statu... | Statut d'alarm...  | Zone de dispon... | DNS IP |
|---|-------------------------|---------------------|-----------------|-----------------|-----------------------|--------------------|-------------------|--------|
| □ | tp4-windows-private-AZ2 | i-0f31ed627eb5315f7 | En cours...     | t3.micro        | 3/3 vérifications r   | Afficher les alarm | us-east-1b        | -      |
| □ | tp4-linux-public-AZ1    | i-0c9997cacdc0a9f89 | En cours...     | t3.micro        | 3/3 vérifications r   | Afficher les alarm | us-east-1a        | -      |
| □ | tp4-windows-private-AZ1 | i-07b1447048723e671 | En cours...     | t3.micro        | 3/3 vérifications r   | Afficher les alarm | us-east-1a        | -      |
| □ | tp4-linux-public-AZ2    | i-0214149410d49fa2e | En cours...     | t3.micro        | 3/3 vérifications r   | Afficher les alarm | us-east-1b        | -      |

Fig. 12. – Les quatre instances EC2 ont été créées et affectées aux bonnes zones de disponibilités.

| ▼ Détails de sécurité   |                               | ID du propriétaire                             | Heure de lancement  |           |  |
|---|-------------------------------|--|---|-----------|--|
| Rôle IAM  | -                             | 107079351100                                   | Sun Nov 30 2025 18:05:54 GMT-0500 (heure normale de l'Est nord-américain) |           |  |
| Groupes de sécurité   |                               |  |   |           |  |
| <a href="#">sg-0c23b88b9c5036c41 (vpc-114-security-group)</a> |                               |  |   |           |  |
| ▼ Règles entrantes  |                               |  |   |           |  |
| <input type="text" value="Filtrer les règles"/>               |                               | <span style="float: right;">&lt; 1 &gt;</span> |   |           |  |
| Nom   | ID de règle du groupe de s... | Plage de ports                                 | Protocole   | Source    | Groupes de sécurité                    |
| -   | sgr-0a182322b7fe6921          | 5432   | TCP   | 0.0.0.0/0 | <a href="#">vpc-114-security-group</a> |
| -   | sgr-0c194ba2f273af39b         | 3306   | TCP   | 0.0.0.0/0 | <a href="#">vpc-114-security-group</a> |
| -   | sgr-0291c292a8c0e62a7         | 80   | TCP   | 0.0.0.0/0 | <a href="#">vpc-114-security-group</a> |
| -   | sgr-0643fb5e147991892         | 53   | TCP   | 0.0.0.0/0 | <a href="#">vpc-114-security-group</a> |
| -   | sgr-0e052671a5ba67c5f         | 3389   | TCP   | 0.0.0.0/0 | <a href="#">vpc-114-security-group</a> |
| -   | sgr-00af0c36028bc05b8         | 22   | TCP   | 0.0.0.0/0 | <a href="#">vpc-114-security-group</a> |
| -   | sgr-0e55ca1c3015188e8         | 1514   | TCP   | 0.0.0.0/0 | <a href="#">vpc-114-security-group</a> |
| -   | sgr-0ebb3d4f35d8db96e         | 9200 - 9300                                    | TCP   | 0.0.0.0/0 | <a href="#">vpc-114-security-group</a> |
| -   | sgr-030c6a7feb24a79f          | 443  | TCP   | 0.0.0.0/0 | <a href="#">vpc-114-security-group</a> |
| -   | sgr-07df630791b46eccf         | 1433   | TCP   | 0.0.0.0/0 | <a href="#">vpc-114-security-group</a> |

Fig. 13. – Le groupe de sécurité est associé aux instances EC2.

### 3.2. Question 2

Le compartiment S3, avec son chiffrement statique et dynamique, son versionnement et le scan de ses vulnérabilités a été construit à l'aide de boto3. Les images ci-dessous illustrent le bon fonctionnement du Script.

```
[INFO] Connection to aws session
[INFO] Create S3
[INFO] Enable encryption
[INFO] Enable versionning
[INFO] Upload sourcefile to bucket
[INFO] Execute a scan on sourcecode
[INFO] End
```

Fig. 14. – L'exécution s'est déroulée sans erreurs. Le terminal décrit les étapes.

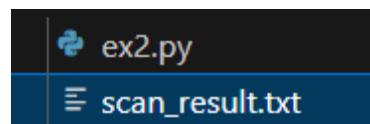


Fig. 15. – Un fichier d'analyse du fichier python avec bandit.

| Nom                           | Région AWS                           | Date de création            |
|-------------------------------|--------------------------------------|-----------------------------|
| <a href="#">s3-114-python</a> | USA Est (Virginie du Nord) us-east-1 | 30 Nov 2025 06:18:30 PM EST |

Fig. 16. – Le compartiment S3 a été créé.

### Gestion des versions de compartiment

[Modifier](#)

La gestion des versions est un moyen de conserver plusieurs variantes d'un objet dans le même compartiment. Vous pouvez utiliser la gestion des versions pour conserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. Grâce à la gestion des versions, vous pouvez aisément récupérer en cas d'actions involontaires des utilisateurs et de défaillances des applications. [En savoir plus ↗](#)

#### Gestion des versions de compartiment

Activé

#### Suppression de Multi-Factor Authentication (MFA)

Une couche de sécurité supplémentaire qui nécessite une authentification multi-facteurs afin de modifier les paramètres de gestion des versions des compartiments et de supprimer définitivement les versions des objets. Pour modifier les paramètres de suppression MFA, utilisez l'interface de ligne de commande AWS (CLI), le kit SDK AWS ou l'API REST Amazon S3. [En savoir plus ↗](#)

Désactivé

Fig. 17. – Le versionnage est actif.

### Objets (1)

| <input type="checkbox"/>   | Copier l'URI S3             | <input type="checkbox"/> Copier l'URL | <input type="checkbox"/> Télécharger | Ouvrir     | Supprimer              | Actions ▾ | <a href="#">Créer un dossier</a> | <a href="#">Charger</a> |
|--|-----------------------------|---------------------------------------|--------------------------------------|------------|------------------------|-----------|----------------------------------|-------------------------|
| Les objets sont les entités fondamentales stockées dans Amazon S3. Vous pouvez utiliser l' <a href="#">inventaire Amazon S3 ↗</a> pour obtenir une liste de tous les objets de votre compartiment. Pour que d'autres personnes puissent accéder à vos objets, vous devez leur accorder explicitement des autorisations. <a href="#">En savoir plus ↗</a> |                             |                                       |                                      |            |                        |           |                                  |                         |
| <input type="checkbox"/> Rechercher des objets en fonction du préfixe  |                             |                                       |                                      |            |                        |           |                                  |                         |
| <input type="checkbox"/>   | Nom                         | ▲   Type                              | ▼   Dernière modification            | ▼   Taille | ▼   Classe de stockage |           |                                  |                         |
| <input type="checkbox"/>   | <a href="#">sourcecode/</a> | Dossier                               | -                                    | -          | -                      |           |                                  |                         |

Fig. 18. – Le dossier de stockage du code source a été créé.

### Chiffrement par défaut

[Modifier](#)

Le chiffrement côté serveur est **automatiquement appliqué aux nouveaux objets stockés dans ce compartiment**.

#### Type de chiffrement

[Infos](#)

Chiffrement côté serveur avec des clés AWS Key Management Service (SSE-KMS)

#### ARN de la clé de chiffrement

[arn:aws:kms:us-east-1:107079351100:key/f5ae5842-83c1-4d5c-bf68-7a878fa5587 ↗](#)

Fig. 19. – Le chiffrement du compartiment S3 est actif.

## 3.3. Question 3

### 3.3.1. Partie 1

```
[INFO] Connection to aws session
[INFO] Create VPC
VPC Id : vpc-0c0f1e51aa95265ba
[INFO] Create subnets
Subnets Id : {'public_az1': 'subnet-073c2bc221126de7d', 'private_az1': 'subnet-0a2067e7f6b89fd13', 'public_az2': 'subnet-09fa86fa7ba0095b2', 'private_az2': 'subnet-023c7ad6aa877e09a'}
[INFO] Create internet gateway
[INFO] Create nat gateways
[INFO] Create security group
[INFO] Security group : sg-0d491911f334e92f
[INFO] Enable automatic public IP
[INFO] Enable flow logs
[INFO] Create EC2 in private and public subnets
[INFO] End
```

Fig. 20. – L'exécution s'est déroulée sans erreurs. Le terminal décrit les étapes.

### Journaux de flux (1)

[Actions ▾](#)
[Créer un journal de flux](#)

| <input type="checkbox"/> | Name | ID de journal de flux                | Type de trafic | Type de destination | Nom de la destination           |
|--------------------------|------|--------------------------------------|----------------|---------------------|---------------------------------|
| <input type="checkbox"/> | -    | <a href="#">fl-0c0ed31625fe81de8</a> | Rejeter        | s3                  | <a href="#">s3-114-python ↗</a> |

Fig. 21. – Le flowlog pour le VPC est actif est transmis dans le compartiment S3.

### 3.3.2. Partie 2

| ▼ Détails de sécurité                   |  |   |
|---|--|---|
| Rôle IAM<br><a href="#">Labrole_tp4</a> | ID du propriétaire<br><a href="#">107079351100</a> | Heure de lancement<br>Mon Dec 01 2025 14:50:38 GMT-0500 (heure normale de l'Est nord-américain) |

Fig. 22. – Le rôle de sécurité est associé aux instances EC2.

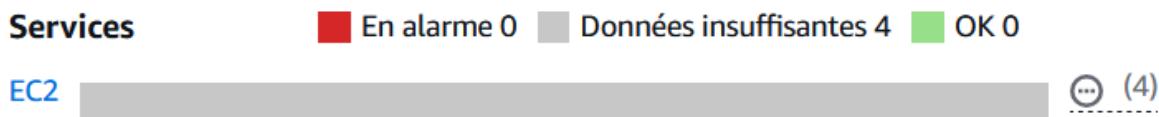


Fig. 23. – Les instances ont une alarme associée.

| □ | Nom  | ▼   État                | ▼   Dernière mise à jour de l'état (UTC) | ▼   Conditions  | Actions   |
|---|--|-------------------------|--|---|---|
| □ | <a href="#">alarm-packetsIn-i-066e3cdce000c27-python</a>   | ⊖ Données insuffisantes | 2025-12-01 21:27:01                      | NetworkPacketsIn > 1000 pour 1 points de données dans 5 minutes | <a href="#">Actions activées</a><br><a href="#">Avertissement</a> |
| □ | <a href="#">alarm-packetsIn-i-0f74d889c6dc62a1c-python</a> | ⊖ Données insuffisantes | 2025-12-01 21:27:00                      | NetworkPacketsIn > 1000 pour 1 points de données dans 5 minutes | <a href="#">Actions activées</a><br><a href="#">Avertissement</a> |
| □ | <a href="#">alarm-packetsIn-i-08e254abb81d310e1-python</a> | ⊖ Données insuffisantes | 2025-12-01 21:27:00                      | NetworkPacketsIn > 1000 pour 1 points de données dans 5 minutes | <a href="#">Actions activées</a><br><a href="#">Avertissement</a> |
| □ | <a href="#">alarm-packetsIn-i-080b385907f046bd-python</a>  | ⊖ Données insuffisantes | 2025-12-01 21:26:59                      | NetworkPacketsIn > 1000 pour 1 points de données dans 5 minutes | <a href="#">Actions activées</a><br><a href="#">Avertissement</a> |

Fig. 24. – Les alarmes sont actives et associées aux instances EC2.

### 3.3.3. Partie 3

```
[INFO] Connection to aws session
[INFO] Create S3
[INFO] Enable encryption
[INFO] Enable versionning
[INFO] Upload sourcefile to bucket
[INFO] Enable cloudtrail for S3 bucket
[INFO] Execute a scan on sourcecode
[INFO] Create replication S3
[INFO] Enable encryption
[INFO] Enable versionning
[INFO] Enable replication
[INFO] End
```

Fig. 25. – L'exécution s'est déroulée sans erreurs. Le terminal décrit les étapes..

|                                  |                                      |                               |     |  |           |     |                                    |                                     |
|----------------------------------|--------------------------------------|-------------------------------|-----|--|-----------|-----|------------------------------------|-------------------------------------|
| <input checked="" type="radio"/> | <a href="#">cloudtrail-s3-python</a> | USA Est<br>(Virginie du Nord) | Non | arn:aws:clou<br>dtrail:us-<br>east-1:1070<br>79351100:tr<br>ail/<br>cloudtrail-<br>s3-python | Désactivé | Non | <a href="#">s3-114-<br/>python</a> | <a href="#">Journalis<br/>ation</a> |
|----------------------------------|--------------------------------------|-------------------------------|-----|--|-----------|-----|------------------------------------|-------------------------------------|

Fig. 26. – Cloudtrail est actif et associé au compartiment S3.

|   |                                      |                             |
|---|--------------------------------------|-----------------------------|
| <input type="radio"/> <a href="#">s3-114-replicate-python</a> | USA Est (Virginie du Nord) us-east-1 | 30 Nov 2025 06:23:48 PM EST |
|---|--------------------------------------|-----------------------------|

Fig. 27. – La réplication est active et un compartiment de réplication a été créé.

| <b>Règles de réplication (1)</b>                               |  |   |   |   |  |                       |                         |                                  |   |
|--|--|---|---|---|--|-----------------------|-------------------------|----------------------------------|---|
|  |  Afficher les détails |  Modifier la règle |  Supprimer |  Actions ▾ |  Créer une règle de réplication |                       |                         |                                  |   |
| Nom de règle de réplication                                    | Statut   | Compartiment de destination   | Région de destination   | Priorité  | Portée   | Classe de stockage    | Propriétaire du réplica | Contrôle du délai de réplication | Objets chiffrés par KMS (SSE-KMS ou DSSE-KMS) |
| <a href="#">OTU2ZmJmNzYtMDA1Yi00YjYyLTkyMjltMmVkJlZDlhMTg2</a> |  Activé               | s3://s3-114-replicate-python  | USA Est (Virginie du Nord) us-east-1  | 1   | Compartiment complet   | Identique à la source | Identique à la source   | Désactivé                        | Ne pas répliquer                              |

Fig. 28. – La réplication est bien active dans le compartiment s3-114-python.

### 3.4. Question 4

Le script *ex4.py* permet de scanner les scripts de génération en python et génère un fichier avec les résultats. *Trivy ne permet pas de réaliser un scan d'un fichier python, nous avons donc utilisé **bandit** en remplacement. Ce logiciel crée un rapport semblable à trivy. Malheureusement, bandit se concentre sur les vulnérabilités du code python et non de l'architecture générée.*

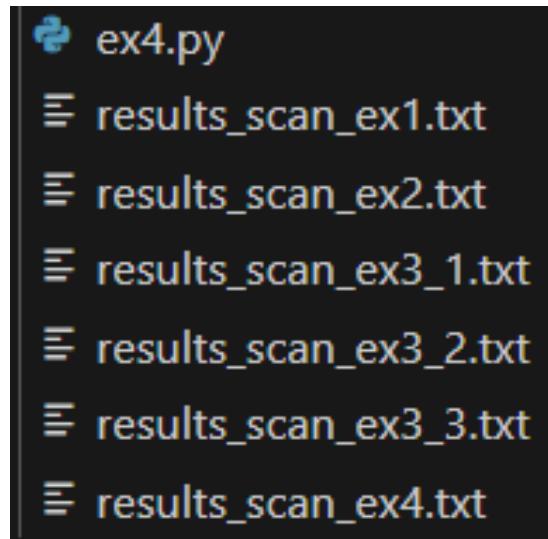


Fig. 29. – Les fichiers d'analyse de bandit ont été générés.

```
Run started:2025-12-01 21:40:03.625556+00:00

Test results:
>> Issue: [B404:blacklist] Consider possible security implications associated with the subprocess module.
  Severity: Low  Confidence: High
  CWE: CWE-78 (https://cwe.mitre.org/data/definitions/78.html)
  More Info: https://bandit.readthedocs.io/en/1.9.2/plugins/blacklist\_imports.html#b404-import-subprocess
  Location: .\..\Ex4/ex4.py:2:0
1 # Librairies
2 import subprocess
3

-----
>> Issue: [B603=subprocess_without_shell_equals_true] subprocess call - check for execution of untrusted input.
  Severity: Low  Confidence: High
  CWE: CWE-78 (https://cwe.mitre.org/data/definitions/78.html)
  More Info: https://bandit.readthedocs.io/en/1.9.2/plugins/b603\_subprocess\_without\_shell\_equals\_true.html
  Location: .\..\Ex4/ex4.py:15:13
14     scan_command = f"bandit -r {filename}" .split(" ") # Trivy cannot scan python object, so we use bandit instead
15     output = subprocess.run(scan_command, capture_output=True, text=True, encoding='utf-8', errors='replace')
16

-----
Code scanned:
Total lines of code: 17
Total lines skipped (#nosec): 0
Total potential issues skipped due to specifically being disabled (e.g., #nosec BXXX): 0

Run metrics:
  Total issues (by severity):
    Undefined: 0
    Low: 2
    Medium: 0
    High: 0
  Total issues (by confidence):
    Undefined: 0
    Low: 0
    Medium: 0
    High: 2
Files skipped (0):
```

Fig. 30. – Exemple d'un fichier d'analyse de bandit.

**Mesures de mitigation :** (voir Tableau 1 ci-dessous)

| Vulnérabilité                | Gravité   | Script  | Stratégie de mitigation   |
|------------------------------|---|---------|---|
| Vulnérabilités & Mitigations | AVD-AWS-0028 → Instance does not require IMDS access to require a token.          | HAUTE   | ec2.json<br><br>Metadata Service (IMDS) permet à l'instance de récupérer des informations utiles à son fonctionnement. Actuellement, cette connexion se fait sans gestion des accès. Une bonne pratique serait d'activer l' <b>IMDSv2</b> pour gérer les accès par token.   |
|                              | AVD-AWS-0107 Security group rule allows unrestricted ingress from any IP address. | HAUTE   | vpc.yaml<br><br>Les ports sont restreint, mais un utilisateur peut se connecter depuis n'importe quelle adresse IP. Pour assurer une défense en profondeur, il faut restreindre l'accès à certaines IP de l'entreprise. De plus, il faut mettre en place une gestion du cycle de vie pour cette table d'adresses, de manière à retirer les accès lorsque l'opérateur n'en a plus besoin. L'objectif est d'appliquer le <b>minimum de priviléges pour une durée minimale</b> . |
|                              | AVD-AWS-0178 : VPC does not have VPC Flow Logs enabled                            | Moyenne | vpc.yaml<br><br>Pour garantir une sécurité maximale, il faut qu'un audit du système soit possible. Pour réaliser cet audit, il est préférable d'activer <b>VPC Flow Logs</b> et de le lier à un compartiment chiffré pour garantir l' <b>intégrité des informations</b> . <i>La question 3.2 corrige cette vulnérabilité.</i>   |
|                              | VD-AWS-0131 : Root block device is not encrypted.                                 | Haute   | ec2.json<br><br>Le disque racine n'est pas chiffré. Un acteur malveillant peut donc récupérer les données écrites en clair dans l'instance. Pour empêcher cette action, il faudrait mettre en place un <b>chiffrement statique</b> des données du disque grâce à une paire de clef KMS ou une paire stockée sur un HSM (Hardware Security Module).  |
|                              | AVD-AWS-0089 : Bucket has logging disabled  | Faible  | s3.json<br><br>Le compartiment n'enregistre pas les requêtes. Dans un objectif d'audit du système, il est préférable de stocker les activités. Le <b>logging est une fonctionnalité activable du compartiment S3 AWS</b> .  |

Tableau 1. – Table de cinq vulnérabilités et mitigations associées