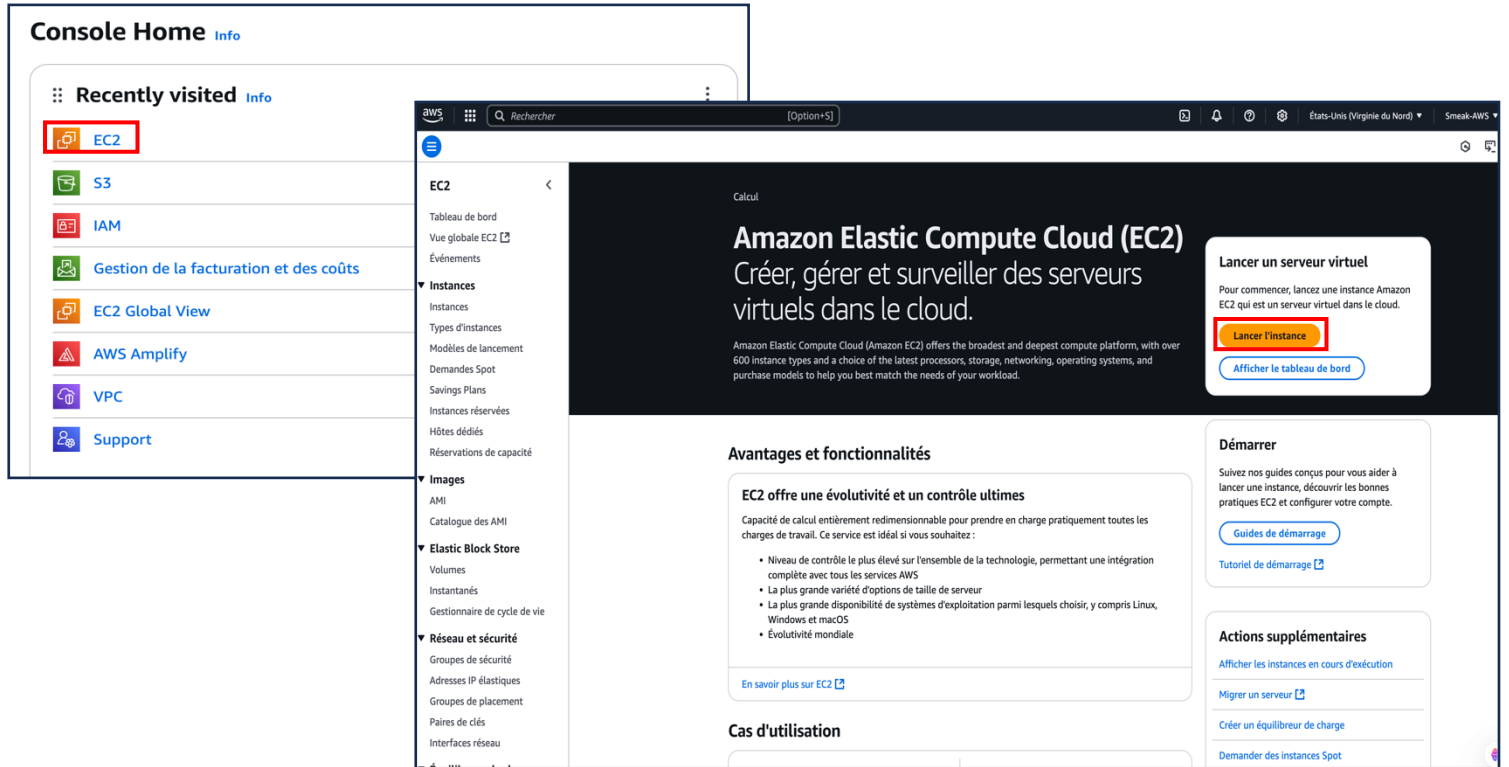


# Étapes pour installer le serveur Web Apache sur Amazon Linux 2

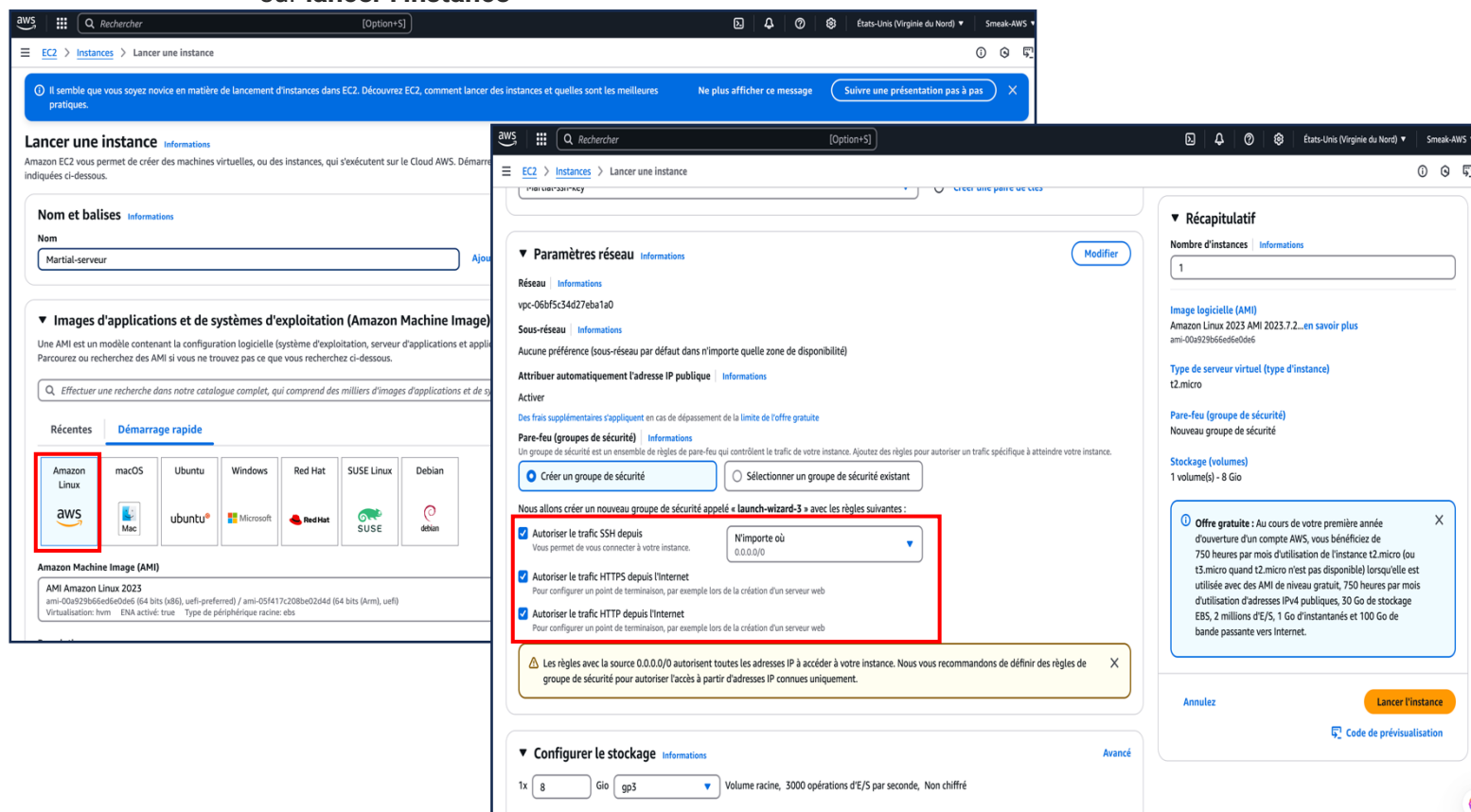
## 1. Lancer une instance EC2 (Linux 2)

On ouvre EC2 en tapant « EC2 » dans la barre de recherche



Cliquez sur le bouton « lancer une instance »

Après avoir fait les configurations nécessaires selon les besoins personnel cliquer sur lancer l'instance



Créer une paire de clés

Nom de la paire de clés

Les paires de clés vous permettent de vous connecter à votre instance en toute sécurité.

Martial-ssh-key

La longueur maximale du nom est de 255 caractères ASCII. Il ne peut pas inclure d'espaces avant ou après.

Type de paire de clés

RSA

Paire de clés privée et publique chiffrée RSA

ED25519

Paire de clés privée et publique chiffrée ED25519

Format de fichier de clé privée

.pem

À utiliser avec OpenSSH

.ppk

À utiliser avec PuTTY

Lorsque vous y êtes invité, stockez la paire de clés dans un emplacement sécurisé et accessible sur votre ordinateur. Vous en aurez besoin ultérieurement pour vous connecter à votre instance. En savoir plus

Annulez

Créer une paire de clés

Rechercher

[Option+S]

EC2 > Instances > Lancer une instance

Créer une paire de clés

Paramètres réseau

Modifier

Réseau Informations

vpc-06b5c34d27eba1a0

Sous-réseau Informations

Aucune préférence (sous-réseau par défaut dans n'importe quelle zone de disponibilité)

Attribuer automatiquement l'adresse IP publique Informations

Activer

Des frais supplémentaires s'appliquent en cas de dépassement de la limite de l'offre gratuite

Pare-feu (groupes de sécurité) Informations

Un groupe de sécurité est un ensemble de règles de pare-feu qui contrôlent le trafic de votre instance. Ajoutez des règles pour autoriser un trafic spécifique à atteindre votre instance.

Créer un groupe de sécurité

Sélectionner un groupe de sécurité existant

Nous allons créer un nouveau groupe de sécurité appelé « launch-wizard-3 » avec les règles suivantes :

Autoriser le trafic SSH depuis

N'importe où

Autoriser le trafic HTTPS depuis l'internet

Pour configurer un point de terminal, par exemple lors de la création d'un serveur web

Autoriser le trafic HTTP depuis l'internet

Pour configurer un point de terminal, par exemple lors de la création d'un serveur web

Les règles avec la source 0.0.0.0/0 autorisent toutes les adresses IP à accéder à votre instance. Nous vous recommandons de définir des règles de groupe de sécurité pour autoriser l'accès à partir d'adresses IP connues uniquement.

Configurer le stockage

Informations

Avancé

1x 8 Gio gp3

Volume racine, 3000 opérations d'E/S par seconde, Non chiffré

Récapitulatif

Nombre d'instances Informations

1

Image logicielle (AMI)

Amazon Linux 2023 AMI 2023.7.2...en savoir plus

ami-00a929b66de6e0de6

Type de serveur virtuel (type d'instance)

t2.micro

Pare-feu (groupe de sécurité)

Nouveau groupe de sécurité

Stockage (volumes)

1 volume(s) - 8 Gio

Offre gratuite : Au cours de votre première année d'ouverture d'un compte AWS, vous bénéficiez de 750 heures par mois d'utilisation de l'instance t2.micro (ou t3.micro quand t2.micro n'est pas disponible) lorsqu'elle est utilisée avec des AMI de niveau gratuit, 750 heures par mois d'utilisation d'adresses IPv4 publiques, 30 Go de stockage EBS, 2 millions d'E/S, 1 Go d'instantanés et 100 Go de bande passante vers Internet.

Annulez

Lancer l'instance

Code de prévisualisation

Patienter un moment .....

Rechercher

[Option+S]

EC2 > Instances > Lancer une instance

Lancement d'une instance

Création de groupes de sécurité

27%

Détails

Veillez patienter pendant que nous lançons votre instance.

Ne fermez pas votre navigateur pendant ce chargement.

Rechercher

[Option+S]

EC2 > Instances > Lancer une instance

Succès

Lancement de l'instance réussi (i-04c663069db302341)

Journal de lancement

Étapes suivantes

Créer des alertes de facturation et d'utilisation de l'offre gratuite

Pour gérer les coûts et éviter les factures surprises, configurez des notifications par e-mail pour la facturation et les seuils d'utilisation de l'offre gratuite.

Créer des alertes de facturation

Connectez-vous à votre instance

Une fois que votre instance est en cours d'exécution, connectez-vous à celle-ci à partir de votre ordinateur local.

Connectez-vous à l'instance

En savoir plus

Connecter une base de données RDS

Configurez la connexion entre une instance EC2 et une base de données pour autoriser le flux de trafic entre elles.

Connecter une base de données RDS

Créer une nouvelle base de données RDS

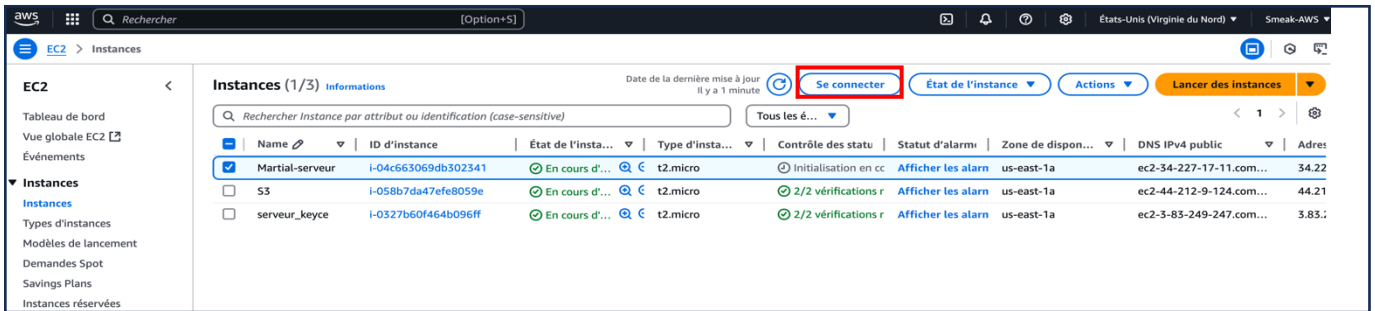
En savoir plus

Afficher toutes les instances

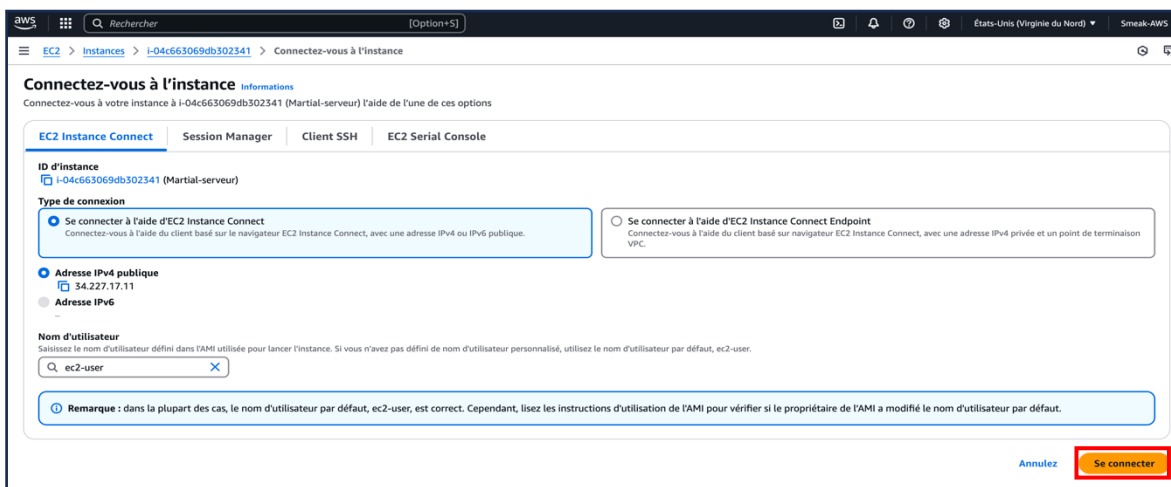
### Installer le serveur Web Apache

Pour vous connecter en SSH depuis le navigateur à l'aide d'Instance Connect, suivez les étapes ci-dessous.

## 1. Sélectionnez votre instance et cliquez sur Connecter comme indiqué ci-dessous

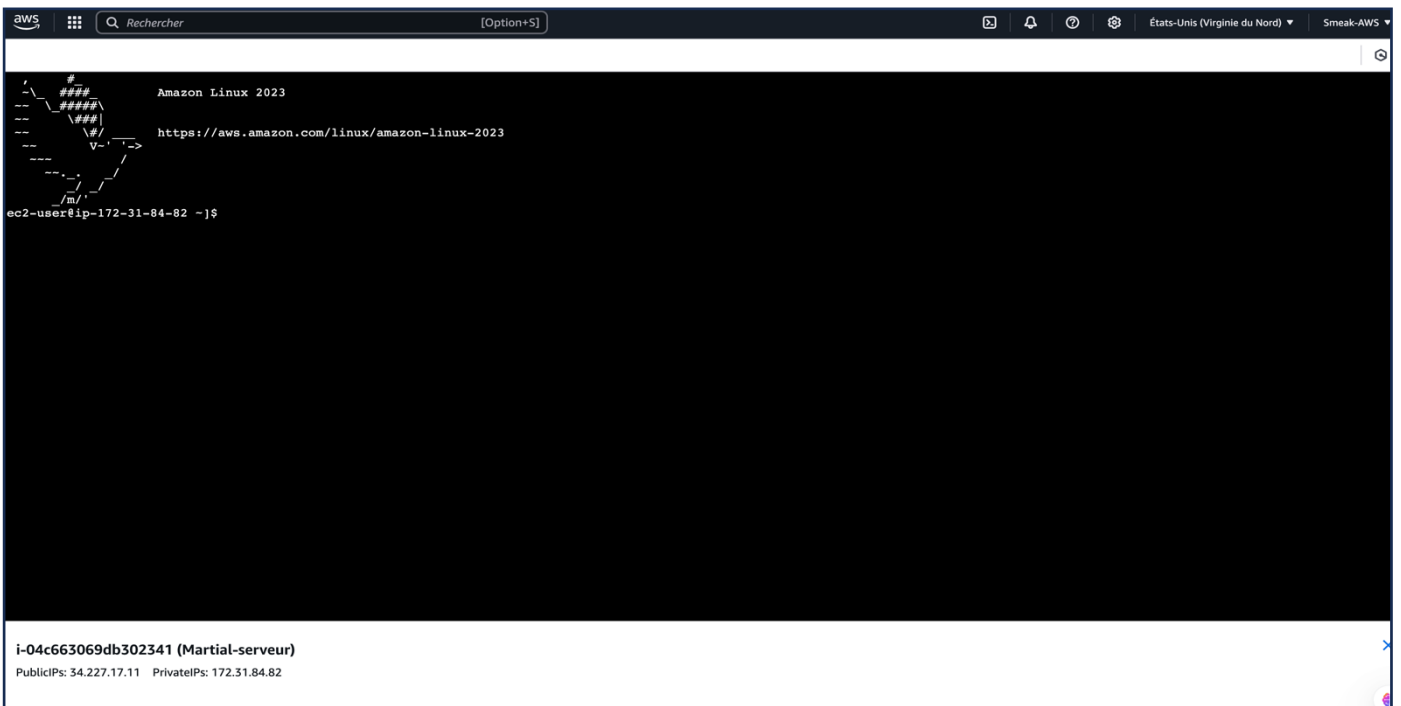


## 2. Une fois que vous avez cliqué sur Connecter, vous verrez un écran avec le nom d'utilisateur par défaut pour une instance .



Vérifiez que **ec2-user** s'affiche dans le champ du nom d'utilisateur et cliquez sur **Connecter** .

Une nouvelle fenêtre de navigateur s'ouvrira et vous serez connecté à votre instance comme ci-dessous.



Nous devons maintenant exécuter les commandes ci-dessous, une par une, pour installer le serveur web Apache sur notre instance. Veuillez noter que nous utiliserons sudo(root privilege) pour exécuter toutes ces commandes. En effet, chaque installation, suppression ou modification d'un logiciel nécessite les privilèges root.

```
sudo yum update -y
```

```
sudo yum install -y httpd.x86_64
```

```
sudo systemctl start httpd.service
```

```
sudo systemctl enable httpd.service
```

## Configurer Apache pour qu'il s'exécute au démarrage du système

Pour que le serveur web démarre automatiquement avec le système, une commande permet d'activer ce lancement automatique.

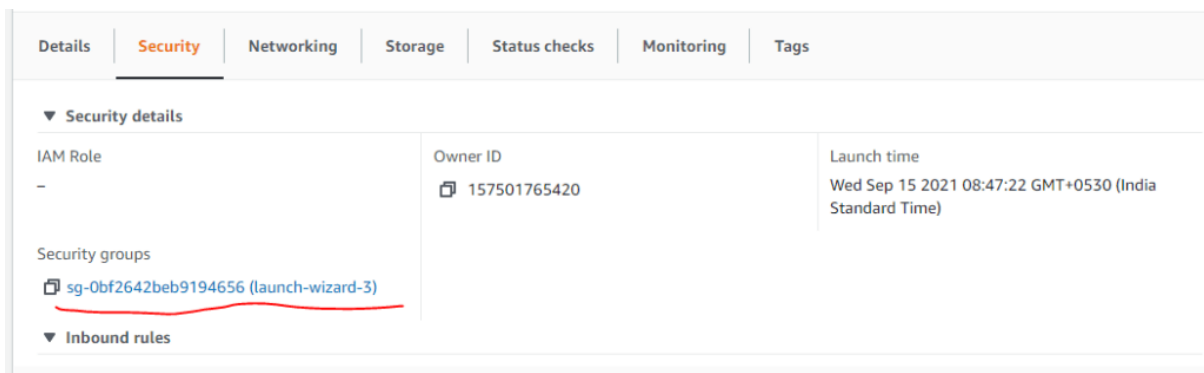
```
sudo systemctl enable httpd.service
```

Le serveur Apache est bien installé sur l'instance Linux 2, mais l'accès web est bloqué car seul le port SSH est autorisé dans le groupe de sécurité. Il faut modifier cela pour autoriser le trafic Web.

## Modifiez le groupe de sécurité de l'instance pour autoriser les ports 80 et 443

Autorisons le trafic Web sur les ports 80 et 443 (trafic Internet pour HTTP et HTTPS).

Cliquez sur l'ID de votre instance pour afficher ses détails. Faites défiler la page vers le bas et cliquez sur l' **onglet Sécurité** . Vous devriez voir le groupe de sécurité comme ci-dessous.



Cliquez sur le lien ID du groupe de sécurité -> Cliquez sur Modifier la règle entrante

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Security group rule ID	Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>	
sgr-0bbc226a5798a7c43	SSH	TCP	22	Custom <input type="text" value="0.0.0.0/0"/>	Allow SSH from Anywhere	Delete
-	HTTP	TCP	80	Anywh... <input type="text" value="0.0.0.0/0"/>	Allow HTTP Web traffic	Delete
-	HTTPS	TCP	443	Anywh... <input type="text" value="0.0.0.0/0"/>	Allow HTTPS Web Traffic	Delete

[Add rule](#)

Cancel [Preview changes](#) [Save rules](#)

Utilisez le bouton **Ajouter une règle** pour ajouter d'autres règles une par une.

Spécifiez les règles pour le trafic Web HTTP et HTTPS depuis n'importe où comme ci-dessus.

## Vérifier l'installation

Nous avons installé et démarré le serveur Web Apache.

Notre instance autorise désormais le trafic Web, il est temps de récupérer l'IP publique ou le DNS public de l'instance.

Tapez l'adresse IP public sur votre navigateur. Voici le resultat !!!!

