

Connexion avec SSH à une instance AWS EC2

v1.0.0 | 02/09/2025 | Auteur : Bauer Baptiste

Chapitre | Durée de réalisation : 1 heures

Table des matières

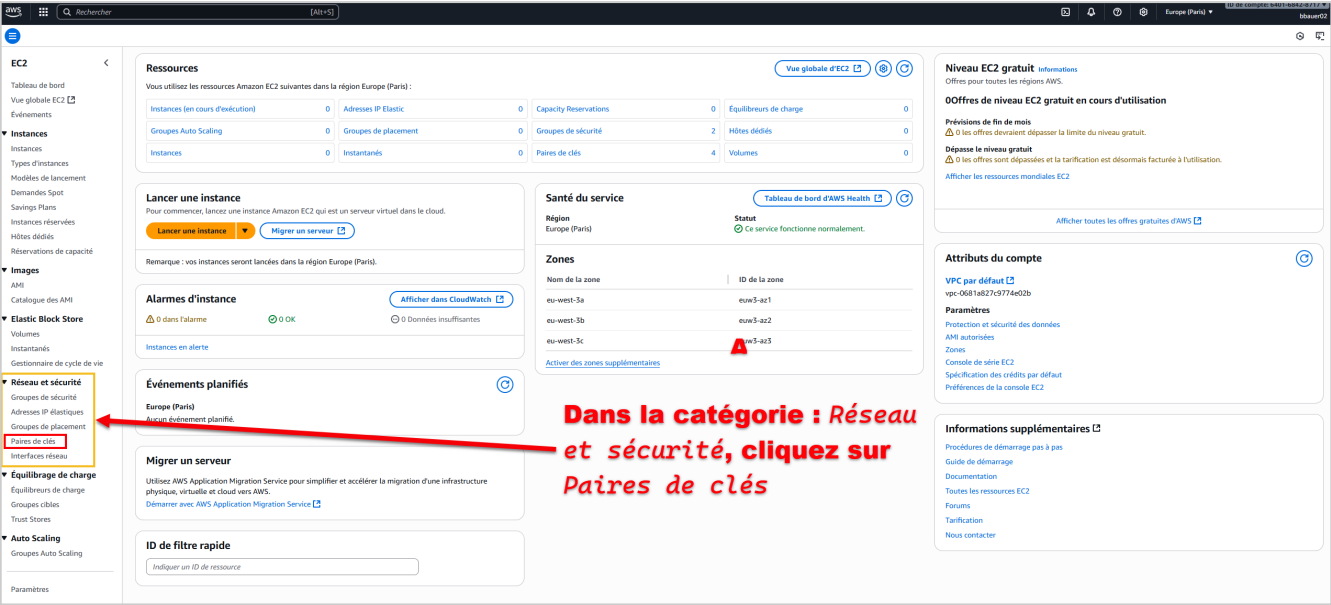
1. Création de la paire de clés SSH	2
2. Vérifier si SSH est installé	4
3. Installer un client OpenSSH sur Windows	5
4. Installer un client OpenSSH sur Linux	6
5. Configurer les permissions de la clé privée	7
6. Test maintenant la connexion depuis votre machine vers votre instance EC2	8

Dans ce chapitre, nous allons voir comment se connecter à une instance AWS EC2 en utilisant SSH. Nous allons couvrir les étapes nécessaires pour configurer votre environnement, générer une paire de clés SSH, et établir une connexion sécurisée à votre instance EC2.

1. Création de la paire de clés SSH

Pour se connecter à une instance EC2 via SSH, vous devez d’abord créer une paire de clés SSH. Voici comment le faire :

Dans le panneau de contrôle AWS, allez dans la section "EC2" puis "Key Pairs" sous "Network & Security".



Cliquez sur **Create Key Pair**, donnez un nom à votre paire de clés, et choisissez le format PEM pour une utilisation avec OpenSSH. Cliquez ensuite sur "Create Key Pair" pour télécharger le fichier .pem.

- **RSA** : ancien standard, très répandu, fiable, mais lourdes (clés et signatures volumineuses, calculs plus lents).
- **ED25519** : moderne, rapide, signatures compactes, sécurité forte, mais parfois moins compatible avec les environnements anciens.

□ Pour SSH : **ED25519 est recommandé par défaut**, sauf si vous devez gérer des systèmes anciens qui ne le supportent pas.

Table 1. Comparatif RSA vs ED25519

Critère	RSA	ED25519
Type d’algorithme	Basé sur la factorisation de grands nombres premiers	Basé sur les courbes elliptiques (Edwards Curve 25519)
Sécurité équivalente	RSA 2048 ≈ 112 bits RSA 4096 ≈ 150 bits	Clé 256 bits ≈ 128 bits (équivalent RSA 3072–4096)
Taille de clé	Grande (2048–4096 bits)	Petite (256 bits)
Performance	Plus lent (génération, signature, vérification) Lourd sur petits appareils	Très rapide, constant-time (protège contre attaques par timing)

Critère	RSA	ED25519
Robustesse future	Ancien, éprouvé, universellement supporté	Moderne, conçu pour éviter erreurs d'implémentation
Compatibilité	Supporté partout (anciens systèmes, logiciels propriétaires)	Supporté par OpenSSH >= 6.5 (2014), moins universel sur vieux systèmes
Taille des signatures	Grandes (plusieurs centaines d'octets)	Petites (64 octets)
Simplicité d'usage	Paramètres nombreux (taille de clé, padding) → risques de mauvaise config	Safe by default, peu de paramètres

Créer une paire de clés [Informations](#)

Paire de clés
Une paire de clés, composée d'une clé privée et d'une clé publique, est un ensemble d'informations d'identification de sécurité que vous utilisez pour prouver votre identité lors de la connexion à une instance.

Nom

Le nom peut avoir un maximum de 255 caractères ASCII. Il ne peut pas inclure d'espaces avant ou après.

Type de paire de clés [Informations](#)
☐ RSA ☒ ED25519

Format de fichier de clé privée
☒ .pem
À utiliser avec OpenSSH
☐ .ppk
À utiliser avec PuTTY

Balises - facultatif
Aucune balise n'est associée à cette ressource.
[Ajouter une balise](#)
Vous pouvez ajouter jusqu'à 50 identifications supplémentaires.

Choisissez .pem pour une utilisation avec votre client SSH OpenSSH

[Annulez](#) [Créer une paire de clés](#)

Quand vous cliquez sur "Create Key Pair", le fichier **.pem** est automatiquement téléchargé.




Ce fichier contient votre clé privée, que vous devez garder en sécurité.

Il faut ensuite s'assurer que SSH soit bien installé sur votre machine locale. Sur la plupart des systèmes Unix (Linux, macOS), SSH est préinstallé. Pour Windows, vous pouvez utiliser PowerShell ou le nouveau Terminal Windows que je conseille d'installer.

2. Vérifier si SSH est installé

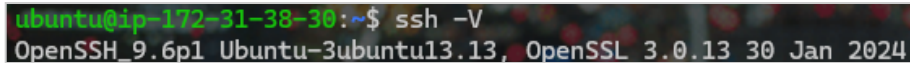
- Ouvrez un terminal et tapez la commande suivante :

```
ssh -V
```



```
PS C:\Users\baptiste> ssh -V
OpenSSH_for_Windows_9.5p1, LibreSSL 3.8.2
```

Figure 1. Sur Windows



```
ubuntu@ip-172-31-38-30:~$ ssh -V
OpenSSH_9.6p1 Ubuntu-3ubuntu13.13, OpenSSL 3.0.13 30 Jan 2024
```

Figure 2. Sur Ubuntu

3. Installer un client OpenSSH sur Windows

- Dans un Powershell en mode administrateur, exécutez la commande suivante pour installer le client OpenSSH :

```
Add-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0
```

4. Installer un client OpenSSH sur Linux

- Dans un Terminal en mode `sudo`, exécutez la commande suivante pour installer le client OpenSSH :

```
sudo apt install openssh-client
```


5. Configurer les permissions de la clé privée

- Le fichier `.pem` devrait être déplacé dans un répertoire sécurisé sur votre machine locale, par exemple `~/.ssh/` sur Linux et macOS, ou `C:\Users\VotreNom\.ssh\` sur Windows.
- Avant d'utiliser la clé privée, vous devez configurer les permissions du fichier `.pem` pour qu'il soit lisible uniquement par vous. Utilisez la commande suivante :

Pour Linux et macOS :

```
$k = "/chemin/vers/.ssh/votre-cle.pem"
takeown /F "$k"
icacls "$k" /reset
icacls "$k" /inheritance:r
icacls "$k" /grant:r "mon_compte_utilisateur_windows:R"
icacls "$k" /remove:g "Everyone" "BUILTIN\Users" "BUILTIN\Administrators" "NT
AUTHORITY\Authenticated Users" "NT AUTHORITY\SYSTEM"
Unblock-File "$k"
```

Pour Linux et macOS :

```
chmod 400 /chemin/vers/.ssh/votre-cle.pem
```

6. Test maintenant la connexion depuis votre machine vers votre instance EC2

- Pour se connecter à votre instance EC2, vous aurez besoin de l'adresse IP publique ou du nom DNS public de l'instance. Vous pouvez trouver cette information dans le panneau de contrôle AWS sous la section "Instances".
- Cliquez ensuite sur "se connecter" :

Se connecter Informations

Connectez-vous à une instance à l'aide du client basé sur un navigateur.

EC2 Instance Connect

Session Manager

Client SSH

EC2 Serial Console

ID d'instance
i-070e0b946133b4a25 (srvDevops)

1. Ouvrez un client SSH.
2. Recherchez votre fichier de clé privée. La clé utilisée pour lancer cette instance est 092025-ssh.pem
3. Exécuter, si nécessaire, cette commande pour vous assurer que votre clé n'est pas visible publiquement.
`chmod 400 "092025-ssh.pem"`
4. Connectez-vous à votre instance à l'aide de son DNS public :
`ec2-52-47-185-227.eu-west-3.compute.amazonaws.com`

Exemple :
`ssh -i "092025-ssh.pem" ubuntu@ec2-52-47-185-227.eu-west-3.compute.amazonaws.com`

Remarque : Dans la plupart des cas, le nom d'utilisateur deviné est correct. Cependant, lisez les instructions d'utilisation de l'AMI pour vérifier si le propriétaire de l'AMI a modifié le nom d'utilisateur par défaut.

- Copier la commande SSH fournie par AWS, qui ressemble à ceci :

```
ssh -i "092025-ssh.pem" ubuntu@ec2-52-47-185-227.eu-west-3.compute.amazonaws.com
```

Ouvrez un terminal et placez vous dans le répertoire où se trouve votre fichier `.pem`, puis exécutez la commande SSH en remplaçant le chemin vers votre fichier `.pem` et l'adresse de votre instance EC2.

- La première fois que vous vous connectez, vous recevrez un avertissement concernant l'authenticité de l'hôte. Tapez `yes` pour continuer.
- Si tout est configuré correctement, vous devriez maintenant être connecté à votre instance EC2 via SSH.

```
PS C:\Users\baptiste\.ssh> ssh -i "092025-ssh.pem" ubuntu@ec2-52-47-185-227.eu-west-3.compute.amazonaws.com
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-1011-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Tue Sep  2 11:42:30 UTC 2025

System load:  0.0          Processes:            114
Usage of /:   36.8% of 6.71GB Users logged in:          1
Memory usage: 27%         IPv4 address for enX0: 172.31.38.30
Swap usage:   0%

 * Ubuntu Pro delivers the most comprehensive open source security and
   compliance features.

   https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

19 updates can be applied immediately.
17 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
Vous êtes connecté à votre instance
Last login: Tue Sep  2 08:08:42 2025 from 88.186.92.132
ubuntu@ip-172-31-38-30:~$
```