

Explique-moi ce dilemme claudé. En effet j'utilise putty key generator pour générer une clé SSH-2 (rsa) pour l'importer sur une instance infomaniak et malgré une copie propre.

Je vois que vous rencontrez un problème avec l'importation de votre clé SSH générée par PuTTY Key Generator vers une instance Infomaniak. Votre message semble coupé, mais je peux déjà identifier les points potentiels du problème.

Voici les causes les plus courantes et leurs solutions :

Format de clé incompatible PuTTY génère des clés au format .ppk (PuTTY Private Key), mais la plupart des serveurs Linux attendent le format OpenSSH. Dans PuTTY Key Generator :

- Allez dans "Conversions" → "Export OpenSSH key" pour la clé privée
- Pour la clé publique, copiez le texte dans la zone "Public key for pasting into OpenSSH authorized_keys file"

Problème de copie-collé La clé publique doit être copiée en une seule ligne continue. Assurez-vous de :

- Sélectionner tout le contenu de la zone publique dans PuTTYgen
- Ne pas introduire de retours à la ligne supplémentaires
- Vérifier qu'elle commence par "ssh-rsa" et se termine par votre commentaire

Emplacement sur le serveur La clé doit être placée dans le bon fichier :

```
~/.ssh/authorized_keys
```

Avec les permissions correctes (600 pour le fichier, 700 pour le dossier .ssh).

Caractères invisibles Parfois des caractères invisibles s'ajoutent lors du copier-coller. Essayez de sauvegarder la clé publique depuis PuTTYgen puis l'ouvrir avec un éditeur de texte simple.

Pouvez-vous me dire exactement quelle erreur vous obtenez lors de l'importation ? Cela m'aiderait à vous donner une solution plus précise.

J'ai essayé via le menu key SSH-2 RSA key et testerSSH-1 (rsa) mais tout bloque. Donc je change de menu, je valide SSH-2 (rsa) mais je choisis via conversion le format OpenSSH. tout cela copié sans coupure. S'il on a un écran petit, y a t-il un risque ?

Excellente question ! Votre approche est correcte en utilisant SSH-2 RSA avec conversion OpenSSH, mais l'écran petit peut effectivement poser problème.

Le risque avec un petit écran : Oui, il y a un risque réel ! Quand l'écran est petit, la zone de texte de la clé publique dans PuTTYgen peut ne pas afficher toute la clé d'un coup. Si vous ne voyez qu'une partie et que vous copiez seulement la portion visible, la clé sera incomplète et donc inutilisable.

Solutions pour éviter ce piège :

1. **Utiliser Ctrl+A puis Ctrl+C** dans la zone de texte de PuTTYgen pour être sûr de tout sélectionner, même ce qui n'est pas visible à l'écran.
2. **Sauvegarder plutôt que copier :**
 - Cliquez sur "Save public key" dans PuTTYgen
 - Ouvrez le fichier sauvegardé avec Notepad/Bloc-notes
 - Copiez depuis là (vous verrez toute la clé d'un coup)
3. **Vérifier la longueur :** Une clé RSA 2048 bits fait environ 370-400 caractères. Si votre copie fait moins de 300 caractères, elle est probablement tronquée.
4. **Agrandir la fenêtre :** Redimensionnez la fenêtre PuTTYgen ou utilisez la barre de défilement pour vérifier qu'il n'y a rien après.

La clé doit commencer par `ssh-rsa AAAAB3NzaC1yc2E...` et se terminer par votre commentaire (souvent votre nom d'utilisateur). Entre les deux, c'est une longue chaîne de caractères sans espaces.

Avez-vous vérifié la longueur de votre clé copiée ?

Parfait, prenez votre temps pour vérifier.

En attendant, voici un moyen simple de contrôler si votre clé est complète :

Vérification rapide :

- Collez votre clé dans un éditeur de texte (Notepad)
- Comptez les parties : vous devez avoir exactement 3 éléments séparés par des espaces :
 1. `ssh-rsa` (le type)
 2. Une très longue chaîne de caractères (la clé elle-même)
 3. Le commentaire (souvent votre nom d'utilisateur)

Signes d'une clé tronquée :

- Elle se termine brutalement au milieu de caractères aléatoires
- Elle fait moins de 300 caractères au total
- Il manque le commentaire à la fin

Une fois que vous aurez vérifié, dites-moi ce que vous trouvez et nous pourrons résoudre le problème d'importation sur Infomaniak si nécessaire !

Erreur qui n'est ni stupide, ni rare :

C'est un effet classique du contexte hybride Windows / Linux, où les outils GUI (PuTTY, Windows 11, etc.) brouillent les réflexes d'un environnement open source bien cadré.

Résumé de ton erreur (logique, pas idiote) :

1. **Tu es sur Windows 11** → tu utilises PuTTY par défaut (ou tu génères des .ppk, .pub non standards pour Linux/OpenStack).
2. **Tu travailles avec OpenStack chez Infomaniak**, donc attendent une **clé publique au format OpenSSH**.
3. Tu as oublié que **OpenStack ≠ environnement Microsoft** → donc un id_rsa.pub Linux-like est **attendu**.
4. Tu as généré une **clé valide mais mal encodée pour le provider**.

Correction immédiate :

Depuis **PuTTYgen** :

1. Choisis **SSH-2 RSA** (2048 ou 4096 bits).
2. Copie **uniquement** le champ :
3. Public key for pasting into OpenSSH authorized_keys file

(Pas de .pub exporté, ni de fichier .ppk à ce stade)
4. Colle cette clé dans **OpenStack** → **Import Key Pair**.
5. Utilise **Save private key** si tu veux te connecter ensuite avec PuTTY (fichier .ppk).

À retenir :

Plateforme	Clé publique attendue	Format attendu
OpenStack / Linux	ssh-rsa AAAAB...	OpenSSH format
Windows / PuTTY	.ppk (privée) + .pub	Propriétaire PuTTY
AWS, GCP, Infomaniak	ssh-rsa via interface ou .pem	OpenSSH recommandé

Astuce CLI : sur Linux ou WSL, tu peux générer directement avec :

```
ssh-keygen -t rsa -b 2048 -C "monuser@machine"
```

Cela te donne :

- `~/.ssh/id_rsa` (clé privée)
- `~/.ssh/id_rsa.pub` (clé publique à importer dans OpenStack)

Tu veux que je t'écrive une **procédure rapide en ligne de commande** ou une **checklist OpenStack/Windows** pour la génération, importation et connexion ?

Voici une **checklist complète et claire** pour utiliser **une paire de clés SSH RSA** dans un environnement **OpenStack (Infomaniak)** tout en travaillant sous **Windows 11**.

CHECKLIST : Connexion OpenStack avec Windows 11 via SSH

1. Génération de la clé SSH

Outil recommandé : [PuTTYgen](#)

- ☐ Lancer **PuTTYgen**
- ☐ Type de clé : SSH-2 RSA
- ☐ Taille : 2048 bits ou 4096 bits (selon politique)
- ☐ (Optionnel) Ajouter un **commentaire** (nom-clé-date)
- ☐ (Optionnel) Ajouter une **passphrase** pour sécurité renforcée
- ☐ Cliquer sur `Generate` et **bouger la souris** dans la zone blanche.

Avant de quitter :

- ☐ **Copier** la clé complète dans le champ Public key for pasting into OpenSSH authorized_keys file (⌘ c c'est cette version qu'attend OpenStack !)
- ☐ Sauvegarder :
 - ☐ Save private key → fichier .ppk pour PuTTY
 - ☐ Save public key si besoin de backup

2. Importer la clé dans OpenStack

Dans l'interface Infomaniak :

- ☐ Aller dans Project > Compute > Key Pairs
- ☐ Cliquer sur Import Key Pair
- ☐ Donner un nom (ex: benoit-ssh-2025)
- ☐ Coller le contenu **OpenSSH** depuis PuTTYgen dans la zone
- ☐ Valider

✓ Tu verras la **clé dans la liste** avec son **empreinte (fingerprint)**.

3. Créer l'instance avec la clé

Dans Project > Compute > Instances :

- ☐ Cliquer sur Launch Instance
- ☐ Onglet **Key Pair** : sélectionner benoit-ssh-2025
- ☐ Terminer les autres onglets :
 - Source (image)
 - Flavor
 - Networks
 - Security Groups : ⚠ ☐ **ouvrir le port 22 en Ingress IPv4** si pas déjà fait
- ☐ Lancer l'instance

4. Connexion à l'instance via PuTTY

1. **Ouvrir PuTTY**
2. Dans Host Name, saisir l'adresse IP publique (retrouvée dans OpenStack)
3. Aller dans Connection > SSH > Auth
 - ☐ Charger le fichier .ppk de ta clé privée
4. Revenir sur Session
 - ☐ Sauvegarder la session (ex: openstack-test)
5. Cliquer sur Open
 - Login : généralement ubuntu, debian ou centos selon l'image choisie

5. Dépannage rapide

Problème	Vérification
Connexion refusée	Port 22 ouvert dans Security Group
Clé non reconnue	Mauvais format collé dans OpenStack
Login incorrect	Vérifie l'utilisateur par défaut
Timeout / pas de ping	IP flottante manquante / mal routée