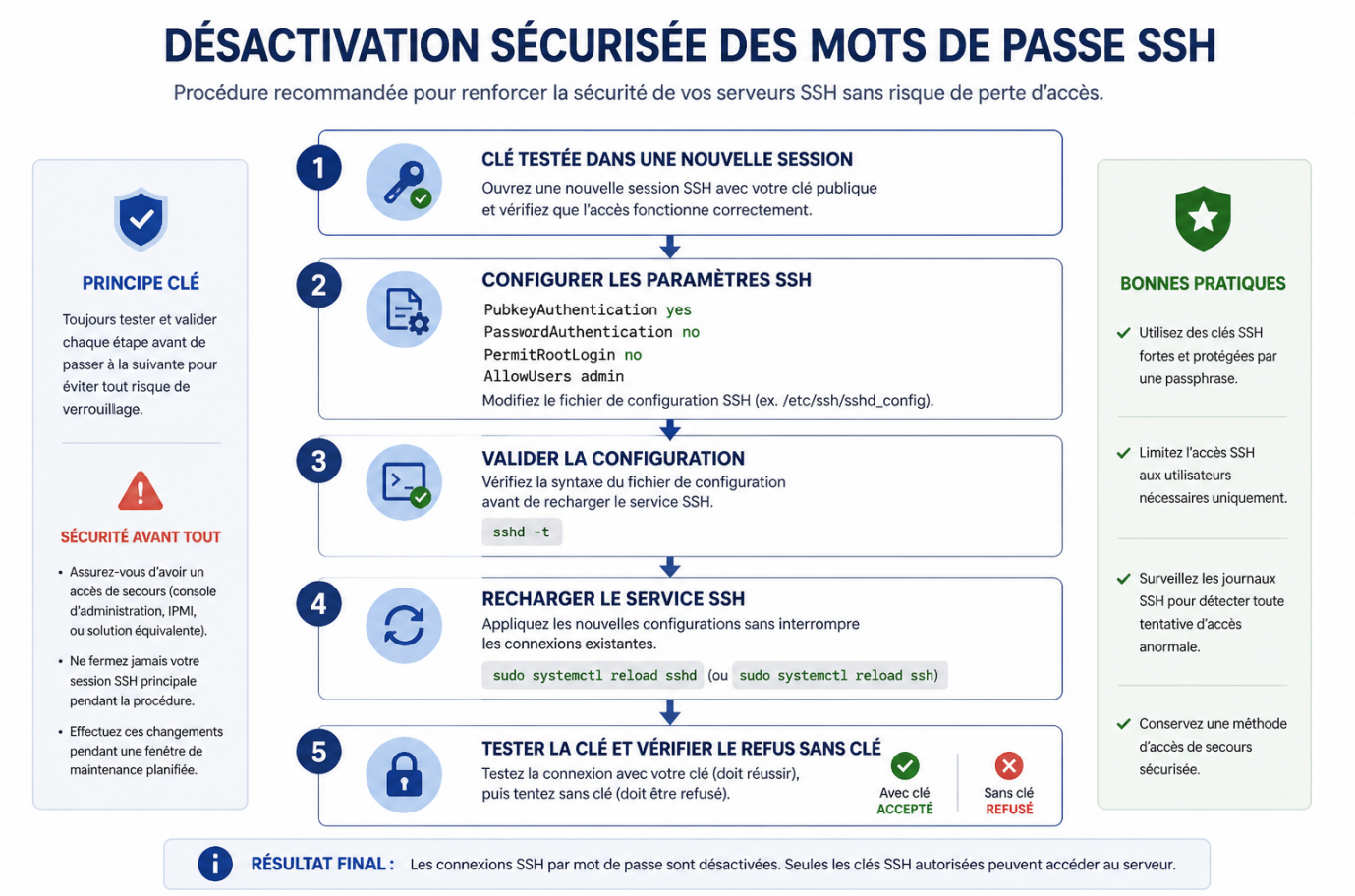
Passer à la clé SSH sans se verrouiller hors du serveur

Suivez cet ordre de vérification pour renforcer l'accès SSH tout en gardant une porte de secours. Le principe clé : la connexion par clé doit être validée dans une seconde session avant toute désactivation des mots de passe.

Au sommaire

> **! Règle anti-verrouillage**
> Conservez votre session SSH actuelle ouverte jusqu'à la fin. Avant toute modification restrictive, vérifiez qu'une console d'hébergement, une console virtuelle ou un accès physique au serveur est disponible.

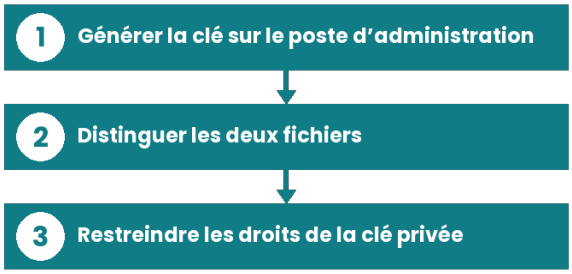


INFOGRAPHIE *Schéma de sécurisation SSH avec clé publique et désactivation des mots de passe.*

Préparer l'intervention

- [ ] **Noter l'adresse IP ou le nom DNS, le compte d'administration et le port SSH actuel.**
- [ ] **Vérifier un accès de récupération hors SSH**
  Console de l'hébergeur, KVM, console locale ou accès physique.
- [ ] **Identifier le service SSH actif**
  Utiliser selon la distribution : sudo systemctl status ssh ou sudo systemctl status sshd.
- [ ] **Repérer la configuration effectivement utilisée**
  Vérifier notamment les éventuels fragments chargés depuis sshd_config.d.
- [ ] **Sauvegarder le fichier de configuration avant édition**
  Exemple : sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.bak.

Créer et protéger la paire de clés



1 **Générer la clé sur le poste d'administration**
Exécutez ssh-keygen -t ed25519 sur l'ordinateur client, pas sur le serveur. Ajoutez une phrase secrète lorsque l'outil le propose.

2 **Distinguer les deux fichiers**
La clé privée, par exemple ~/.ssh/id_ed25519, reste exclusivement sur le poste client. La clé publique ~/.ssh/id_ed25519.pub est celle qui peut être installée sur le serveur.

3 **Restreindre les droits de la clé privée**
Exécutez chmod 600 ~/.ssh/id_ed25519 sur le poste client afin que seul votre compte local puisse la lire.

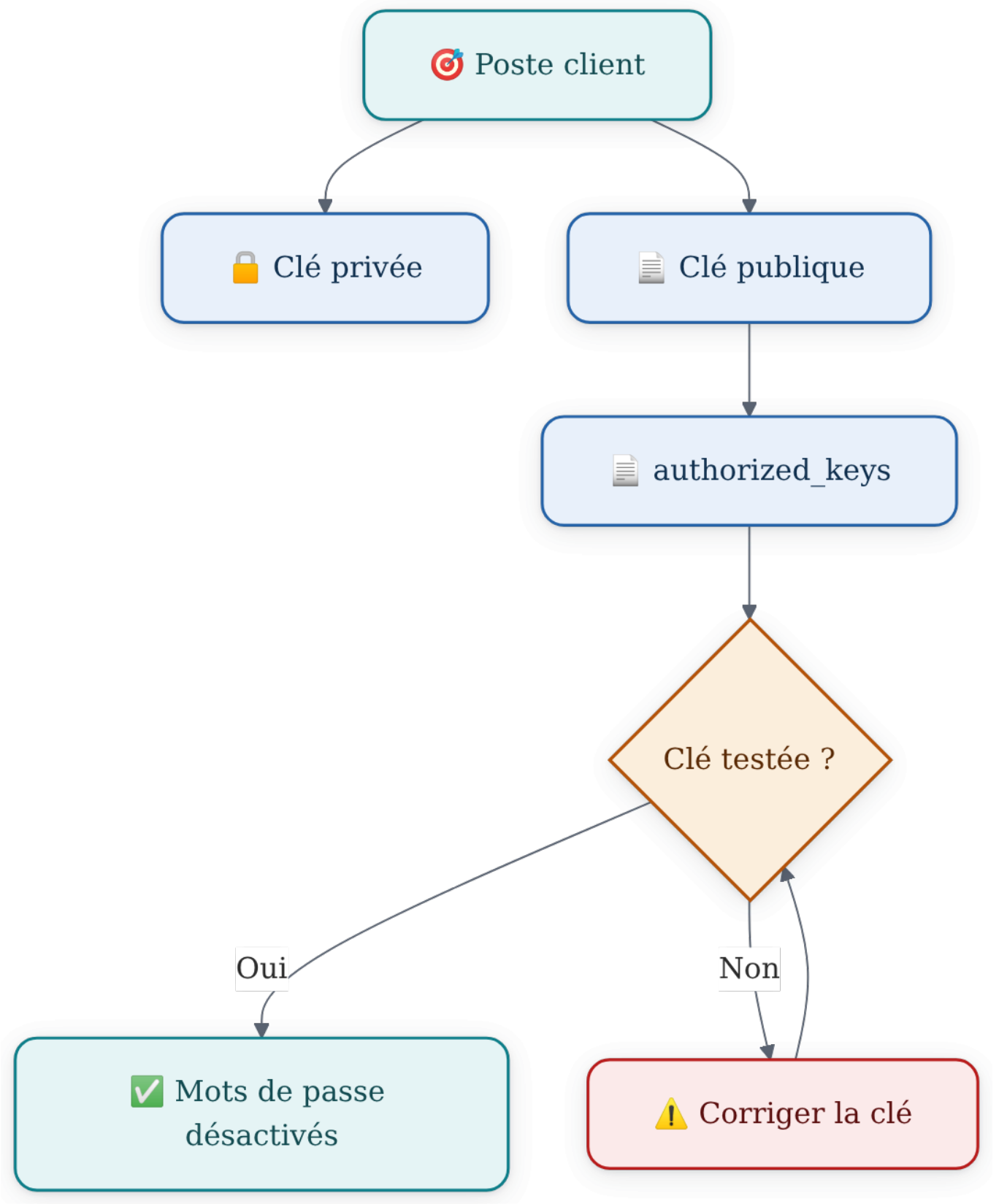
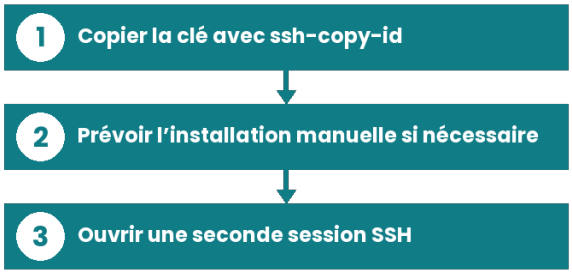


SCHÉMA *La clé privée reste côté administration ; seule la clé publique est autorisée sur le serveur.*

Installer puis tester la clé publique



1 **Copier la clé avec ssh-copy-id**
Depuis le poste client, utilisez ssh-copy-id -i ~/.ssh/id_ed25519.pub admin@adresse_du_serveur. Le mot de passe peut encore être demandé à cette étape.

2 **Prévoir l'installation manuelle si nécessaire**
Sur le serveur, créez ~/.ssh avec chmod 700 ~/.ssh, puis ajoutez la ligne complète de la clé publique dans ~/.ssh/authorized_keys et appliquez chmod 600 ~/.ssh/authorized_keys.

3 **Ouvrir une seconde session SSH**
Testez une nouvelle connexion par clé dans une autre fenêtre de terminal. Ne fermez pas la session existante tant que ce test n'est pas concluant.

Réglages SSH à appliquer après le test de clé

Directive	Valeur visée	But
PubkeyAuthentication	yes	Autoriser l'authentification par clé publique.
PasswordAuthentication	no	Désactiver l'authentification par mot de passe après validation de la clé.
PermitRootLogin	no	Empêcher la connexion SSH directe du compte root.

Validation finale et retour arrière

- [ ] **Vérifier la syntaxe de la configuration avant de recharger le service SSH.**
- [ ] **Recharger le bon service SSH identifié sur le serveur.**
- [ ] **Confirmer depuis une nouvelle session que la connexion par clé fonctionne toujours.**
- [ ] **Limiter les comptes autorisés à se connecter si cela correspond à votre besoin d'administration.**
- [ ] **En cas de perte d'accès SSH, utiliser la console de récupération pour restaurer la sauvegarde de configuration.**
- [ ] **Ne jamais copier, publier ou transmettre la clé privée**
  Ni dans un ticket, ni dans un dépôt Git, ni par messagerie.

Les emplacements de configuration et le nom du service SSH peuvent varier selon la distribution Linux. Vérifiez toujours la configuration réellement chargée avant de recharger le service.