

Votre connexion SSH depuis Windows, sans faux pas

Préparez les bonnes informations, vérifiez l'identité du serveur et ouvrez votre session Linux depuis PowerShell en toute confiance. Gardez cette fiche à portée de main lors de chaque première connexion.

Au sommaire

1. Réunir les informations indispensables
2. Se connecter avec PowerShell ou Windows Terminal
3. Diagnostiquer un échec de connexion
4. Les réflexes de sécurité à conserver

1. Réunir les informations indispensables



Noter l'adresse IP ou le nom de domaine du serveur

Ex. : serveur.exemple.net ; une adresse privée exige souvent le bon réseau ou un VPN.



Noter le nom du compte Linux autorisé

Il peut être différent de votre identifiant Windows.



Confirmer le port SSH

Le port 22 est habituel, mais seul le port communiqué par l'administrateur est valable.



Identifier la méthode d'authentification attendue

Mot de passe Linux ou clé privée SSH.

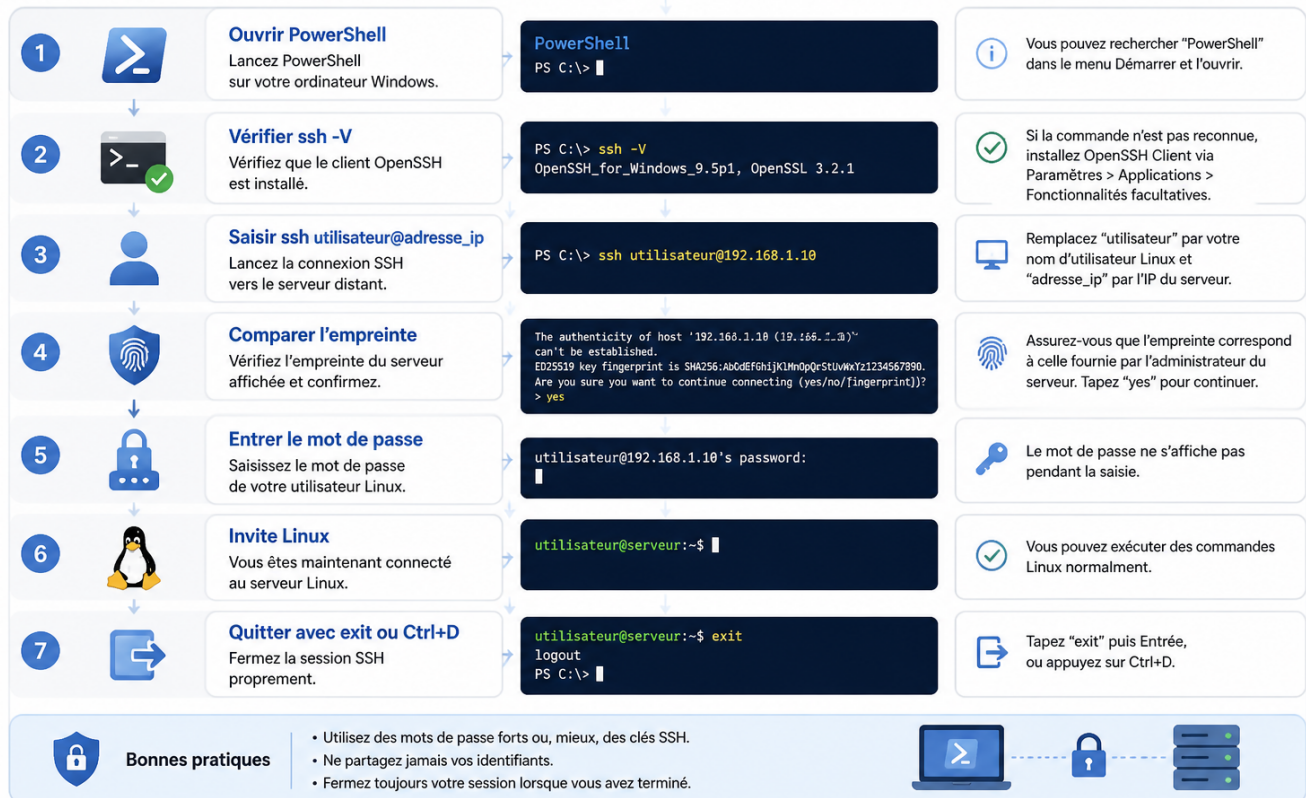


Obtenir l'empreinte du serveur par un canal fiable

Indispensable pour contrôler son identité lors de la première connexion.

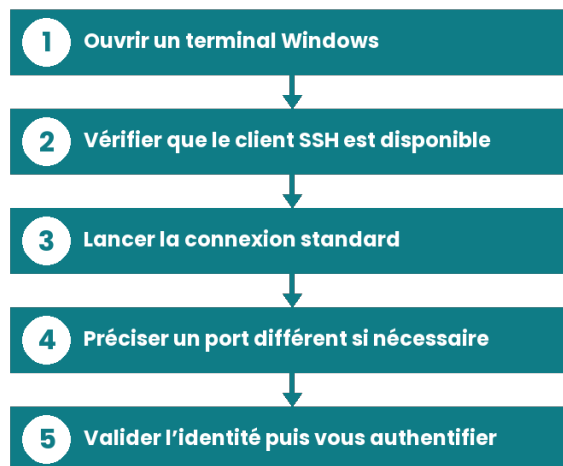
Connexion SSH Windows avec PowerShell

Accédez en toute sécurité à un serveur Linux depuis Windows



INFOGRAPHIE Schéma de connexion SSH Windows avec PowerShell pour accéder à un serveur Linux à distance.

2. Se connecter avec PowerShell ou Windows Terminal



1 Ouvrir un terminal Windows

Lancez PowerShell ou Windows Terminal depuis le menu Démarrer.

2 Vérifier que le client SSH est disponible

Saisissez : `ssh -V`. Si une version d'OpenSSH s'affiche, le client est prêt.

3 Lancer la connexion standard

Saisissez : `ssh <utilisateur_linux>@<adresse_du_serveur>`. Remplacez les éléments entre chevrons par les informations reçues.

4 **Préciser un port différent si nécessaire**

Utilisez : `ssh -p <port> <utilisateur_linux>@<adresse_du_serveur>`.

5 **Valider l'identité puis vous authentifier**

Comparez d'abord l'empreinte affichée avec celle fournie par l'administrateur. Après validation, saisissez le mot de passe si le serveur le demande ou utilisez votre clé privée configurée.

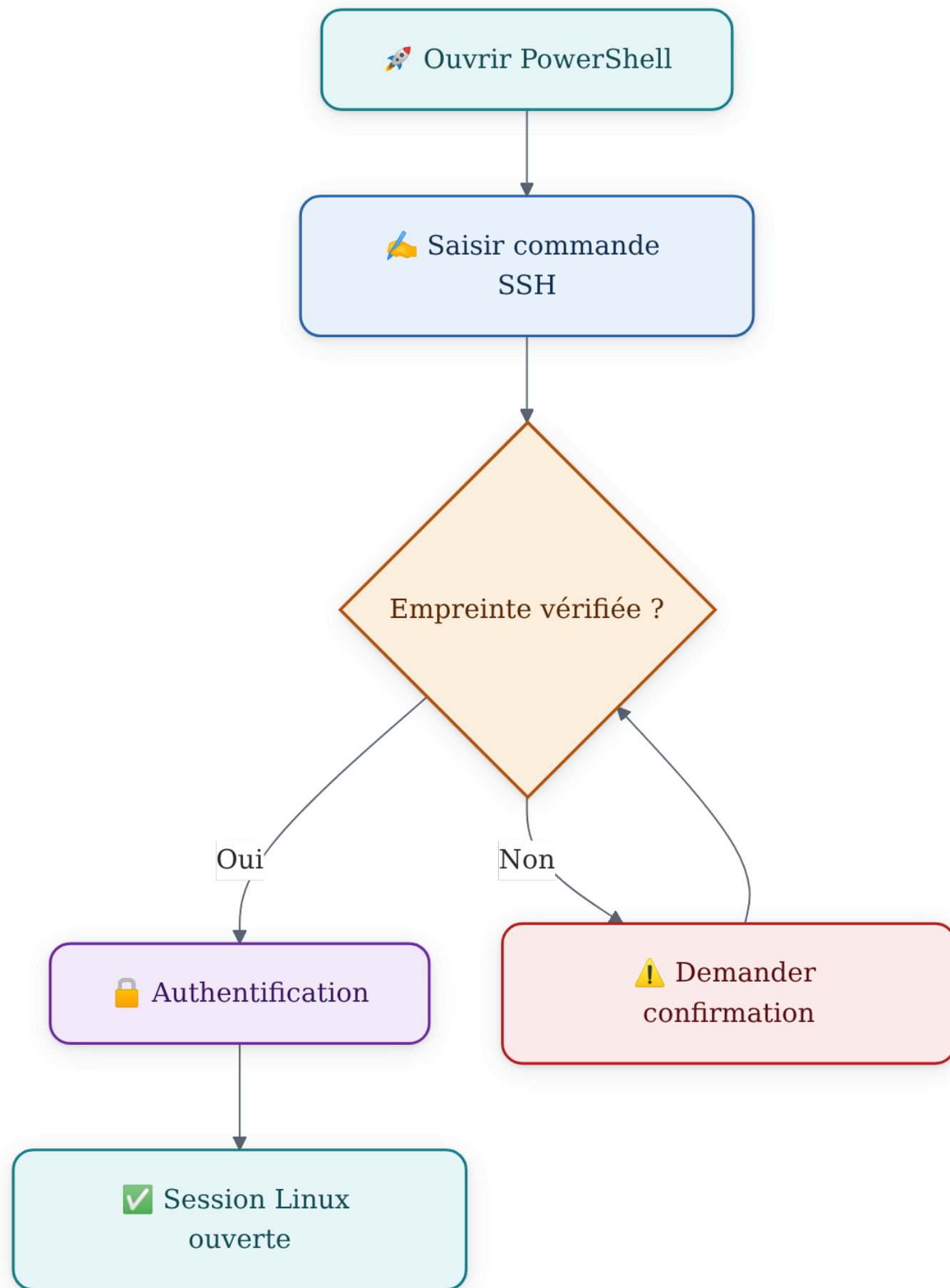


SCHÉMA Le parcours sûr : connexion, contrôle de l'empreinte, puis authentification.

! Ne validez pas une empreinte inconnue à l'aveugle

À la première connexion, répondez « yes » seulement après avoir comparé l'empreinte avec une valeur confirmée par l'administrateur. Si une empreinte déjà connue change, demandez confirmation avant de supprimer une ancienne entrée.

4. Diagnostiquer un échec de connexion

Message ou situation	Piste de vérification
« Connection refused »	Le service SSH n'écoute probablement pas sur le port visé, ou le mauvais port est utilisé.
Délai de connexion dépassé	Vérifiez l'adresse, le port, le filtrage réseau et la nécessité éventuelle d'un VPN.
Adresse privée du type 192.168.* , 10.* ou 172.16 à 172.31.*	Vérifiez que votre poste est sur le réseau autorisé ou connecté au VPN requis.
Mot de passe refusé	Contrôlez le compte Linux utilisé et la méthode d'authentification autorisée.
Alerte sur une empreinte modifiée	Ne poursuivez pas sans confirmation : l'adresse, le serveur ou son identité peuvent avoir changé.

5. Les réflexes de sécurité à conserver

SSH ouvre une session en ligne de commande sur Linux : ce n'est pas un accès à un bureau graphique.

Ne partagez jamais une clé privée SSH par messagerie.

Après validation, l'identité du serveur est mémorisée sur le poste Windows pour les connexions suivantes.

Ne devinez ni le nom d'utilisateur ni le port : demandez les paramètres exacts à l'administrateur ou à l'hébergeur.

Une clé publique doit être associée au compte Linux visé pour permettre une authentification par clé.

Pour un serveur sensible ou un message inattendu, interrompez la connexion et confirmez les paramètres auprès de l'administrateur.