Authentification SSH par clé entre un client Windows et un serveur Windows

1. Contexte et objectif

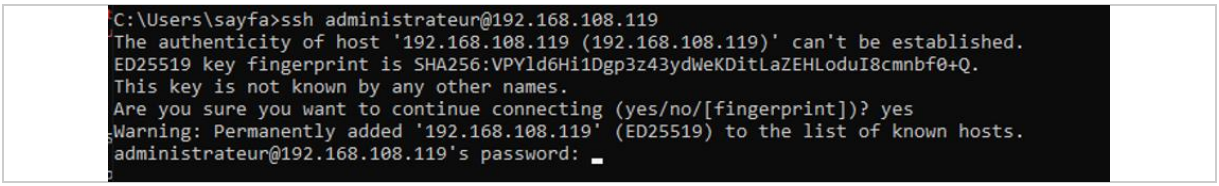
SSH est un protocole réseau permettant d'administrer à distance un système via un terminal chiffré. Par défaut, la connexion s'effectue par identifiant et mot de passe. Il est cependant recommandé de passer à l'authentification par clé cryptographique, qui offre un niveau de sécurité nettement supérieur.

2. Authentification par mot de passe vs par clé

Le tableau suivant compare les deux méthodes d'authentification SSH :

Critère	Authentification par mot de passe	Authentification par clé
Sécurité	Vulnérable au brute-force et au phishing	Immune au brute-force ; clé privée jamais transmise sur le réseau
Automatisation	Impossible sans stocker le mot de passe en clair dans un script	Compatible avec les scripts et les pipelines CI/CD
Traçabilité	Difficile : un mot de passe peut être partagé entre plusieurs personnes	Chaque clé identifie un utilisateur précis
Attaques réseau	Exposé aux attaques de dictionnaire	Aucune donnée sensible ne transite sur le réseau
Révocation d'accès	Nécessite de changer le mot de passe sur tous les systèmes	Suppression de la clé publique uniquement

La connexion SSH par mot de passe, illustrée ci-dessous, nécessite de saisir le mot de passe à chaque connexion et expose le serveur aux attaques par force brute si des règles de blocage ne sont pas mises en place.



3. Installation et configuration d'OpenSSH Server sur Windows Serveur

OpenSSH Server est une fonctionnalité optionnelle de Windows, disponible depuis Windows Server 2019 et Windows 10. Elle s'installe via PowerShell en administrateur :

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

Une fois installé, le service SSH est démarré et configuré pour démarrer automatiquement à chaque reboot du serveur :

```
Start-Service sshd
Set-Service sshd -StartupType Automatic
```

La bonne installation est vérifiée avec la commande suivante, qui doit afficher le service en statut Running :

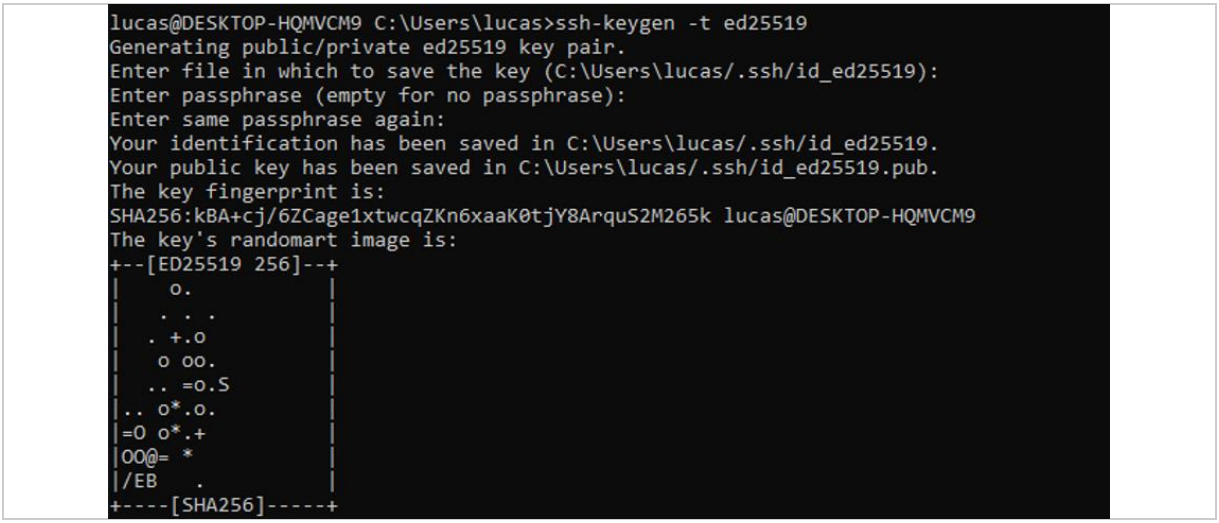
```
Get-Service sshd
```

4. Génération de la paire de clés sur le client Windows

La paire de clés est générée sur le poste client (celui depuis lequel on veut se connecter), jamais sur le serveur. L'algorithme ed25519 est utilisé car il offre un excellent niveau de sécurité avec des clés courtes et des opérations rapides :

```
ssh-keygen -t ed25519
```

L'outil demande l'emplacement de sauvegarde (C:\Users\lucas\.ssh\id_ed25519 par défaut) et une passphrase optionnelle pour protéger la clé privée. Deux fichiers sont créés : id_ed25519 (clé privée, à ne jamais partager) et id_ed25519.pub (clé publique, à déposer sur le serveur).



5. Récupération de la clé publique

La clé publique est affichée avec la commande type. C'est la valeur complète de cette ligne qui doit être copiée et déposée sur le serveur :

```
type %USERPROFILE%\.ssh\id_ed25519.pub
```



6. Dépôt de la clé publique sur le serveur Windows

Sur le serveur Windows, pour les connexions aux comptes membres du groupe Administrateurs, OpenSSH utilise un fichier spécifique : C:\ProgramData\ssh\administrators_authorized_keys. Ce fichier est créé et la clé publique y est inscrite depuis une session PowerShell administrateur sur le serveur :

```
New-Item -ItemType File -Path "C:\ProgramData\ssh\administrators_authorized_keys" -Force
"ssh-ed25519 AAAA...lucas@DESKTOP" | Set-Content
"C:\ProgramData\ssh\administrators_authorized_keys"
```



7. Configuration des permissions du fichier de clés

OpenSSH refuse d'utiliser le fichier administrators_authorized_keys si ses permissions ne sont pas strictement restreintes. Les ACL (Access Control Lists) sont configurées pour n'accorder l'accès qu'aux Administrateurs et au système, en supprimant d'abord tout héritage de permissions :

```
icacls "C:\ProgramData\ssh\administrators_authorized_keys" /inheritance:r
icacls "C:\ProgramData\ssh\administrators_authorized_keys" /grant "Administrateurs:F"
/grant "SYSTEM:F"
```



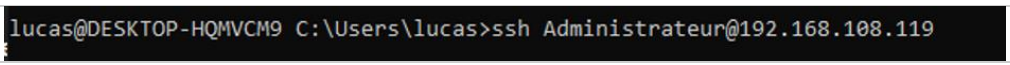
Le service SSH est ensuite redémarré pour prendre en compte la nouvelle configuration :

```
Restart-Service sshd
```

8. Test de la connexion SSH par clé

La connexion est établie depuis le client Windows en spécifiant explicitement la clé privée à utiliser avec le paramètre -i. Si tout est correctement configuré, la connexion s'établit sans demande de mot de passe :

```
ssh -i C:\Users\lucas\.ssh\id_ed25519 Administrateur@192.168.108.119
```



Une fois la clé déposée et les permissions correctement configurées, les connexions suivantes ne nécessitent plus de saisir le paramètre -i si la clé est dans l'emplacement par défaut (~/.ssh/id_ed25519). La commande ssh Administrateur@IP suffit alors.