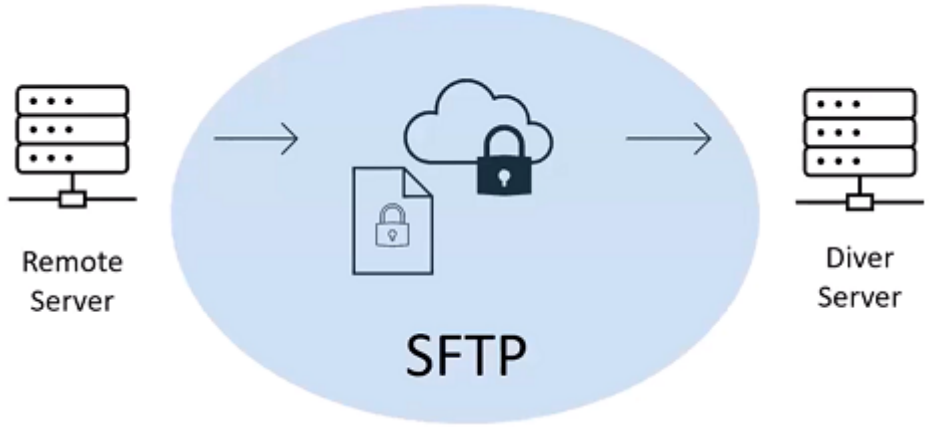
Utilisation de SFTP avec WorkBench

Description

Il est commun d'avoir des fichiers de données (CSV, XML, ...) allant de manière sécurisée d'un serveur de fichier distant à un serveur Diver et vice-versa.



SSH File Transfer Protocol ou Secure File Transfert Protocol (SFTP) est un protocole réseau qui fournit :

- l'accès de fichier
- le transfert de fichier
- la gestion de fichier

Il utilise un cryptage / chiffrement pour s'assurer que les données restent confidentielles et non modifiées.

Il y a deux méthodes d'authentification SFTP :

- authentification avec mot de passe
- authentification par clé SSH (clé privée / clé publique)

Un utilisateur peut être authentifié par :

- mot de passe
- clé privée (fichier identité)
- clé privée (fichier identité) + passphrase (version 7.1.35 ou supérieure)

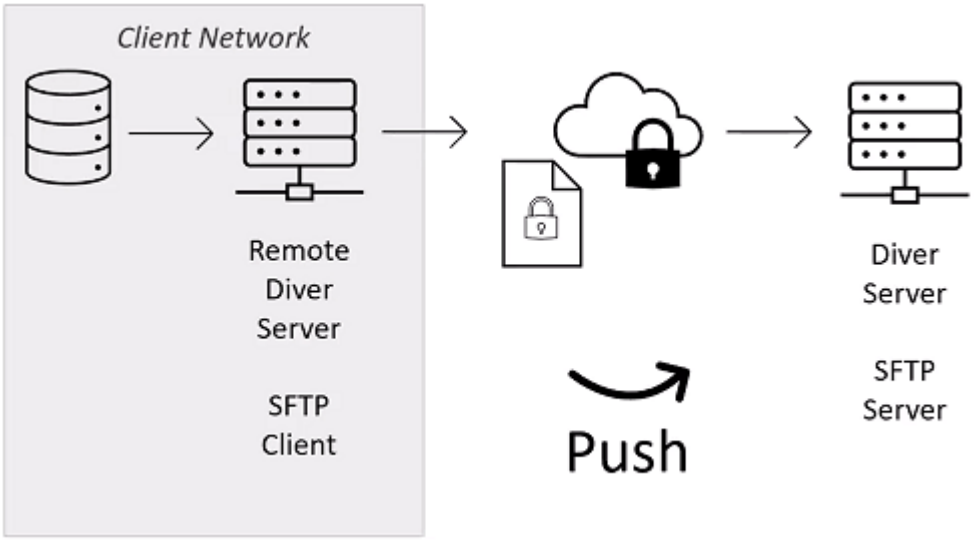
La dernière option est la plus sécurisée.

Authentification SFTP : clé SSH ou fichier identité

Authentification SFTP : clé SSH ou fichier identité

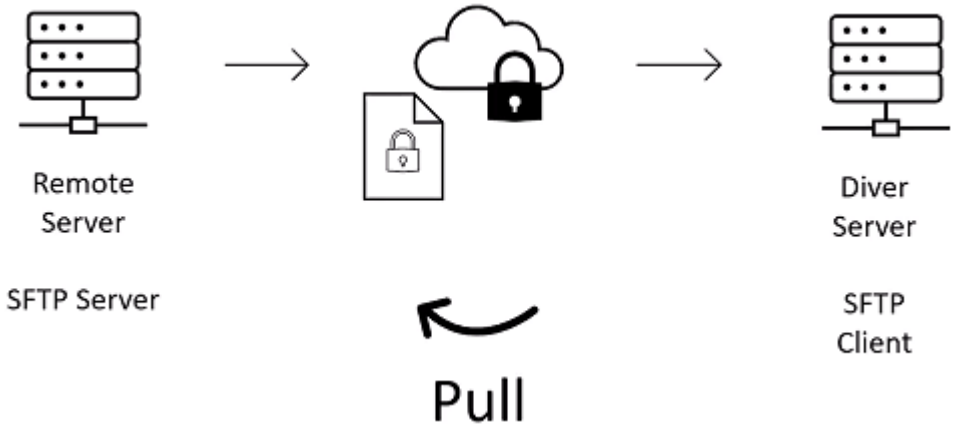
SFTP en pratique : Push

Un serveur à distance Diver pousse les données sur un autre serveur Diver.

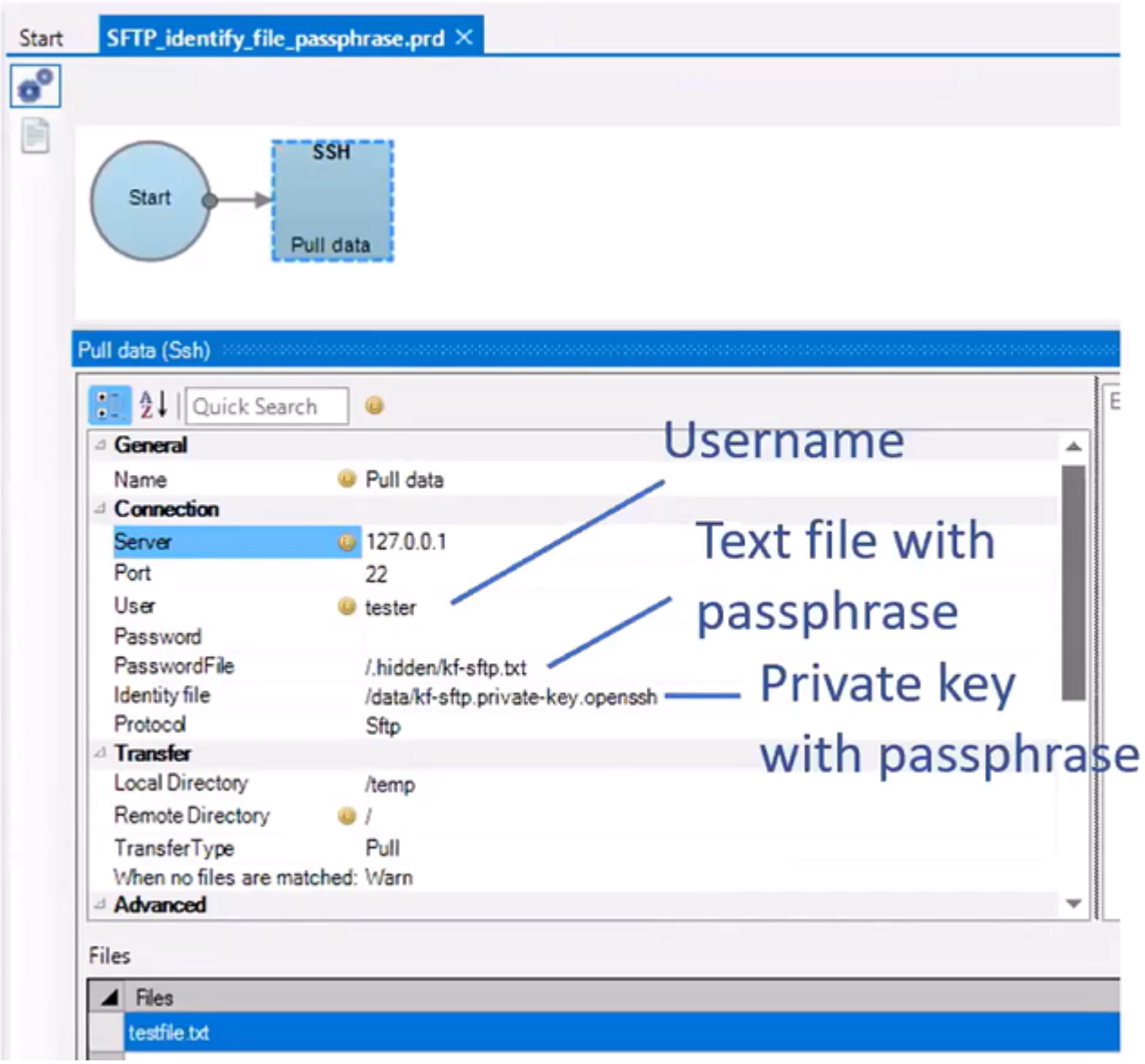


SFTP en pratique : Pull

Parfois nous devons récupérer les données depuis un serveur SFTP distant qui a été paramétré par un client



Pour utiliser SFTP, le nœud SSH est nécessaire dans un script Production ***.prd***



Points essentiels à retenir :

- utiliser le nœud SSH pour SFTP dans Production
- protéger les clés d'identité avec une phrase secrète (passphrase) - disponible à partir de la version 7.1(35)
- ne jamais publier les mots de passe et phrases secrètes dans la fonctionnalité contrôle de version (version control). Obtenez les mots de passe et phrases secrètes à partir d'un fichier de mot de passe (PasswordFile)
- utiliser plusieurs niveaux de sécurité : clé d'identité avec phrase secrète, liste blanche des adresses IP
- dernière astuce : nettoyage des fichiers après échanges

Tags

1. DI-Production
2. script
3. Workbench