ssh-agent

Agent d'authentification

ssh-agent maintient les clé privées utilisées pour l'authentification à clé publique. ssh-agent est généralement démarré au début d'une session X ou d'une session login, et toutes les autres fenêtres ou programmes sont démarrés comme client du programme ssh-agent. Via l'utilisation de variables d'environnement l'agent peut être localisé et utilisé automatiquement pour l'authentification en se connectant dans d'autres machines via ssh.

OPTIONS

-a bind_address Lie l'agent au socket UNIX. Défaut : $TMPDIR/ssh-XXXXXXXXXX/agent.<ppid>

-c Génère des commande C-shell sur stdout.

-D Ne bascule pas en tâche de fond

-d mode debug

-E fingerprint_hash md5|sha256 Spécifie l'algorithme de hashage utilisé en affichant les empreintes de clé.

-k Termine l'agent en cours (donné par $SSH_AGENT_PID)

-P pkcs11_whitelist Spécifie une liste de motif de chemins acceptables pour les libraires PKCS#11 qui peuvent être ajoutés en utilisant l'option -s. Défaut : /usr/lib/, /usr/local/lib/

-s Génère des commandes bash sur stdout. Mode par défaut si le shell n'est pas csh

-t life Durée de vie des identités ajoutées à l'agent.

Si une ligne de commande est donnée, elle est exécutée comme sous-processus de l'agent. Quand la commande se termine, l'agent également. L'idée est que l'agent est lancé sur la machine de l'utilisateur. Les données d'authentification n'ont pas besoin d'être stockées dans d'autres machines, et les passphrases d'authentification ne sont jamais envoyés sur le réseau. Cependant, la connexion à l'agent est forwardée via les logins distants, et l'utilisateur peut donc utiliser les privilèges donnés par les identités dans le réseau de manière sécurisée.

Il y a 2 manières de définir l'agent : la première est que l'agent démarre une nouvelle sous-commande dans laquelle certaines variables sont exportée. La seconde est que l'agent affiche les commandes shell nécessaire. ssh recherche ensuite ces variables et les utilise pour établir une connexion à l'agent.

L'agent n'envoie jamais de clé privée, les opérations qui nécessitent une clé privée sont gérés par l'agent, et le résultat est retourné au demandeur. Un socket unix est créé et le nom de ce socket est stocké dans SSH_AUTH_SOCK. Ce socket est accessible à l'utilisateur courant.