ssh-keygen

Générateur, gestionnaire et convertisseur de clé d'authentification

- ssh-keygen génère des clés utilisables par le protocole sshv2. ssh-keygen peut également être utilisé pour générer des groupes à utiliser dans les échanges Diffie-Hellman.
- ssh-keygen peut être utilisé pour générer et mettre à jours des listes de révocation de clé, et pour tester si les clés données ont été révoquées.
- Normallement chaque utilisateur souhaitant utiliser ssh avec une authentification par clé publique le lance une fois pour créer la clé d'authentification dans ~/ .ssh/id_dsa, ~/.ssh/id_ecdsa, ~/.ssh/id_ed25519 ou ~/.ssh/id_rsa. Additionnellement, les administrateurs système peuvent l'utiliser puor générer des clé hôte, comme dans /etc/rc.
- Normallement ce programme génère la clé et demande un nom de fichier pour stocker la clé privée. La clé publique est stockée dans un fichier de même nom suffixé avec ".pub". Le programme demande également une passphrase.
- Il n'y a pas de manière de récupérer une passphrase perdue. Si la passphrase est perdue ou oubliée, une nouvelle clé doit être générée et la clé publique correspondante copiée dans les autres machines
- Pour les clés stockées dans le nouveau format openssh, il y a également un champs commentaire pour aider à identifier la clé.

OPTIONS

-A Pour chaque types de clé (rsa,-sa,ecdsa et ed25519) pour laquelle les clés hôte n'existent pas, génère les clés hôte avec le fichiers spécifié, une passphrase vide, la taille par défaut, et le commentaire par défaut.

-a rounds En sauvant une clé privée au nouveau format, spécifie le nombre de KDF (fonction de dérivation de clé) utilisé.

-B Affiche le digest de la clé privée spécifiée

-b bits Taille de la clé à créer

-C comment Fournis un nouveau commentaire

-D pkcs11 Charge les clés publique fournis par la librairie pkcs#11. Utilisé avec -s, indique qu'une clé CA réside dans le jeton PKCS#11.

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

-e Lit une clé privée ou publique OpenSSH et l'affiche sur stdout dans un des formats de l'option -m

-F hostname Recherche le nom d'hôte spécifié dans un fichier known_hosts.

-f filename Spécifie le nom du fichier de clé

-G output_file Génère des premiers candidats pour DH-GEX.

-g Utilise le format DNS pour afficher les enregistrements de ressource d'empreinte en utilisant -r

-H Hash le fichier known_hosts. Remplace les hostnames et adresses avec les représentations hashés.

-h En signant une clé, créé un certificat hôte au lieu d'un certificat utilisateur.

-l certificate_identity Spécifie l'identité de clé en signant une clé publique.

-i Cette option lit une clé privée ou publique non-chiffrée au format spécifié par -m et l'affiche au format compatible OpenSSH sur stdout.

-J num_lines Quitte après n ligne pendant l'exécution du screening des candidats DH en utilisant l'option -T.

-j start_line Défarre le screening à la ligne spécifiée

-K checkpt Écris la dernière ligne traitée dans le fichier spécifié en effectuant le screening de candidat DH.

-k Génère un fichier KRL

-L Affiche le contenu d'un ou plusieurs certificats

-l Affiche l'empreinte du fichier de clé publique spécifié.

-M memory Quantité de mémoire à utiliser (en Mo) en générant le moduli candidat pour DH-GEX

-m RFC4716|PKCS8|PEM Format de clé pour -i et -e

-N new_passphrase Fournis une nouvelle passphrase

-n principals Spécifie un ou plusieurs principaux à inclure dans un certificat en signant une clé.

-O option Spécifie une option de certificat, en signant une clé. Peut être spécifié plusieurs fois. Les options valides sont :

clear Efface toutes les permissions permises

critical :name [=contents]

Extension :name [=contents] Inclus une option ou une extension arbitraire

force-command=command Force l'exécution de la commande au lieu d'un shell ou de la commande spécifié par l'utilisateur quand le certificat est utilisé pour l'authentification

no-agent-forwarding Désactive le forwarding ssh-agent

no-port-forwarding Désactive le forwarding de port

no-pty Désactive l'allocation pty

no-user-rc Désactive l'exécution -e ~/.ssh/rc

no-x11-forwarding Désactive le forwarding X11

permit-agent-forwarding Autorise le forwarding ssh-agent

permit-port-forwarding Autorise le port forwarding

permit-pty Autorise l'allocation pty

permit-user-rc Autorise l'exécution de ~/.ssh/rc

permit-x11-forwarding Autorise le forwarding X11

source-address=address_list Restreint les adresses sources depuis lequel le certificat est considéré valide.

-o Sauve la clé privée en utilisant le nouveau format au lieu de PEM

-P passphrase Fournis l'ancienne passphrase

-p Demande de changer la passphrase de la clé privée au lieu de créer une nouvelle clé

-Q Teste si les clé ont été révoqués

-q mode silencieux

-R hostname Supprime toutes les clé appartenant à hostname dans known_hosts

-r hostname Affiche le RR SSHFP pour la clé publique spécifiée

-S start Spécifie le point de départ en hexa en générant un moduli candidat pour DH-GEX

-s ca_key Signe un clé publique en utilisant la clé CA spécifiée

-T output_file Teste les premiers candidats à l'échange DH

-t dsa|ecdsa|ed25519|rsa Spécifie le type de clé à créer

-u Met à jours une KRL

-V validity_interval Spécifie un interval de validité en signant un certificat.

-v mode verbeux

-W generator Spécifie le générateur souhaité en testant le moduli pour DH-GEX

-y Lit une clé privée au format OpenSSH et affiche une clé publique sur stdout

-z serial_number Spécifie un numéro de série à embarquer dans le certificat.

Génération de moduli

ssh-keygen peut être utilisé pour générer des groupes pour le protocole de groupe d'échange Diffie-Hellman (DH-GEX). Générer ces groupes se fait en 2 étapes : Les premiers candidats sont générés en utilisant un processus rapide mais consommateur de mémoire. La génération des premiers sont effectués en utilisant -G :

ssh-keygen -G moduli-2048.candidates -b 2048

Par défaut, la recherche des premiers commence au point aléatoire dans la plage de longueur souhaitée, mais peut être changé avec -S. Une fois un jeu de candidats généré, ils doivent être screené, avec l'option -T. Dans ce mode, ssh-keygen lit les candidats depuis l'entrée standard, ou depuis un fichier avec -f, par exemple :

ssh-keygen -T moduli-2048 -f moduli-2048.candidates

Par défaut, chaque candidat est sujet à 100 test de primalité. Cela peut être changé avec -a. La valeur de générateur DH est choisie automatiquement pour le premier en considération. -W permet de choisir un générateur spécifique. Les valeur de générateur sont 2, 3 et 5.

Les groupes DH screenés peuvent être installés dans /etc/moduli. Il est important que ce fichier contienne le moduli d'une plage de longueur de bit et que les partis d'une connections partage un moduli commun.

Certificats

ssh-keygen suppporte la signature de clé pour produire des certificats qui peuvent être utilisés pour l'authentification utilisateur et hôte. Les certificats consistent d'une clé publique, des informations d'identité, 0 ou plusieurs principaux et un jeu d'options qui sont signés par une clé d'autorité de certification. Les clients ou serveurs peuvent ainsi truster seulement la clé CA et vérifier la signature des certificats. Noter que les certificats OpenSSH sont différents et plus simple que les certificats X.509.

sh-keygen support 2 types de certificats : utilisateur et hôte. Les certificats utilisateur authentifient les utilisateurs auprès des serveurs, et les certificats hôte authentifient les serveurs auprès des utilisateurs. Pour générer un certificat utilisateur :

ssh-keygen -s /path/to/ca.key -I key_id /path/to/user_key.pub

Le certificat résultant sera placé dans /path/to/user_key-cert.pub. Un certificat hôte nécessite l'option -h :

ssh-keygen -s /path/to/ca_key -I key_id -h /path/to/host_key.pub

Il est possible de signer en utilisant une clé CA stockée dans un jeton PKCS#11 en fournissant la librairie avec -D

ssh-keygen -s ca_key.pub -D libpkcs11.so -I key_id user_key.pub

Dans tous les cas, key_id est un identifiant de clé qui est loggé par le serveur quand le certifica est utilisé pour l'authentification. Les certificats peuvent être limités pour être valide pour un jeu de principaux. Par défaut, les certificats générés sont valides pour tous les utilisateurs et tous les hôte. Pour générer un certificat pour un jeu spécifié de principaux :

ssh-keygen -s ca_key -I key_id -n user1,user2 user_key.pub

ssh-keygen -s ca_key -I key_id -h -n host.domain host_key.pub

Des limitation aditionneles sur la validité et l'utilisation des certificats utilisateur peuvent être spécifiés. L'option -V permet de spécifier les dates de validité.

KRL

ssh-key est capable de gérer des listes de révocation de clé. Ces fichiers binaire spécifient des clés ou certificats qui sont révoqués en utilisant un format compacte.

Les KRL peuvent être générés en utilisant le flag -k. Cette option lit un ou plusieurs fichiers depuis la ligne de commande et génère une nouveau KRL. Les fichiers peuvent contenir une spécification KRL, ou des clé publique, listées une par ligne. Les clés publique sont révoquées en listant leur hash ou leur contenu dans la KRL et les certificats révoqués par numéro de série ou ID de clé.

Révoquer les clé en utilisant une spécification KRL offre un contrôle explicite sur les types d'enregistrements utilisés pour révoquer les clé et peut être utilisé pour révoquer directement les certificats par numéro de série ou ID de clé sans avoir le certificat original complet. Une spécification KRL consiste de lignes contenant une des directives suivantes :

serial : serial_number[-serial_number] Révoque un certificat avec le numéro de série spécifié

id : key_id Révoque un certificat avec l'ID de clé spécifié

key : public_key Révoque la clé spécifiée

sha1 : public_key Révoque la clé spécifiée par son hash sha1

Les KRL peuvent être mises à jours avec -u. Qunad cette option est spécifiée, les clés listées via la ligne de commande sont fusionnées dans la KRL. Il est également possible de tester si un clé particulière est révoquée avec -Q.