Créer un disque portable de clés pour GnuPG

Gazette Linux n°102 - Mai 2004

Rob Mitchell

Article paru dans le n°102 de la Gazette Linux de mai 2004.
Traduction française par Sylvain Baron <sb CHEZ sylvain TIRET baron POINT net>.
Relecture de la traduction française par Joëlle Cornavin <jcornavi CHEZ club TIRET internet POINT fr>.

Table des matières

L'un des premiers problèmes que j'ai rencontrés lorsque j'ai commencé à utiliser gnupg était la nécessité de recevoir des messages électroniques chiffrés sur plusieurs machines. Si vous avez l'expérience de gnupg, vous avez constaté que les clés sont stockées dans des trousseaux de clés, lesquels se trouvent dans le répertoire `.gnupg` de votre répertoire personnel. Vous pourriez vous contenter de copier votre clé privée sur les deux machines, mais cette solution ne vous conviendra peut-être pas car vous pourriez ne pas être en mesure de protéger physiquement les deux machines en permanence.

L'autre possibilité serait d'utiliser plusieurs clés publiques. Dans mon cas, je créerais une clé pour la maison et une pour le travail. L'opération est certainement réalisable mais elle limite mon usage des clés à deux machines. Quid si je souhaitais déchiffrer un message électronique obtenu via une interface web sur une autre machine ? Pour cela, vous devez prendre votre clé privée avec vous.

Nous allons voir comment transporter en toute sécurité des clés d'une machine à l'autre à l'aide de commandes et de techniques Linux de base.

1. Vérifier l'existence des clés

Dès que vous avez créé vos clés publique et privée, voici à quoi ressemble votre répertoire `.gnupg` :

Il semble que nous ayons au moins une clé publique dans `pubring.gpg` et au moins une dans `secring.gpg`. Vous pouvez vérifier l'existence des clés nécessaires avec deux commandes **gnupg**.

Vérifiez la clé publique avec l'option `--list-keys` :

Et la clé secrète avec l'option `--list-secret-keys` :

Vous pouvez importer autant de clés publiques que vous en avez besoin ou que vous en utilisez régulièrement avant de les lister. Une fois que vous avez vérifié que toutes les clés que vous souhaitiez rendre portables sont dans le trousseau de clés, vous pouvez passer à la production des supports.

2. Produire une disquette

La méthode la plus rapide (et la moins onéreuse) pour produire un disque de clés est d'utiliser une disquette. La création de la disquette implique de :

1. Formater la disquette
2. Déplacer les trousseaux de clés sur la disquette

2.1. Formater la disquette

Insérez une disquette dans votre lecteur. Cette opération supprimant toutes données existantes, assurez-vous au préalable de n'avoir plus besoin de son contenu. Le fichier de périphérique associé à la disquette est `/dev/fd0`. Tout ce dont nous avons besoin est la commande **mke2fs**, les paramètres par défaut et un shell root.

Après que le formatage est achevé, montez la disquette. La commande **mount** ne devra rien retourner.

2.2. Déplacer les trousseaux de clés sur la disquette

Cette étape doit en fait démarrer par une copie des fichiers du trousseau de clés sur la disquette. Si vous employez la commande **mv** pour les déplacer, la destruction des fichiers restants sur le disque dur ne peut être garantie. Par conséquent, avec l'aide d'un script simple sur la ligne de commande, vous pouvez copier les fichiers sur la disquette et recourir à l'utilitaire **shred** pour détruire ce qui reste.

L'option `z` ordonne à **shred** de remplir de zéros l'espace sur disque qu'occupe le fichier ; l'option `u` lui ordonne de supprimer le fichier à la fin de l'opération. Il n'y a maintenant plus de fichiers dans le répertoire `.gnupg` et voici à quoi ressemble le disque de clés :

Démontez la disquette. Vous pouvez vous en servir sur n'importe quelle machine sur laquelle il suffira de la monter. La commande **umount** ne devra rien retourner.

3. Utiliser le disque de clés

Lorsque vous serez prêt à utiliser le disque de clés, montez-le simplement dans le répertoire `.gnupg` sur le disque dur. La commande **df** vous permet de vérifier le montage :

Vous êtes maintenant à même d'utiliser gpg avec le trousseau de clés portable sur la disquette. [1]

4. Notes de fin

L'emploi de cette technique empêche quiconque ayant un accès physique à votre machine de voler votre clé privées Il va sans dire qu'il est d'une importance vitale de ne pas perdre votre disque de clés.

Un autre avantage de cette technique est que vous pouvez retirer votre trousseau de clés de la machine lorsqu'elle est connectée à l'Internet ou à un autre réseau.

D'autres supports pourraient être produits pour la portabilité des clés. Un CD-R est un support plus « permanent » qu'une disquette. Les distributions exécutant la version actuelle de Gnome ou KDE font appel à une fonctionnalité d'automontage pour les cédéroms qui rendraient l'utilisation d'un CD-R plus pratique que de monter manuellement une disquette. Cependant, comme le recours à un CD-R dans ce but gaspillerait beaucoup d'espace, je recommanderais d'employer un CD-RW si cela vous concerne. Vous pourriez également faire appel à une clé USB (ou *flashdrive*) avec cette technique. [2]

Notes

1. La méthode proposée nécessite d'être *root*. Pour une méthode générique, il me semble plus avisé de monter la disquette dans `/mnt/floppy` (ou `/floppy` pour les utilisateurs de la Debian), puis de créer un lien symbolique :

   Si un répertoire gnupg existe déjà, renommez-le le temps de l'opération. (N. d. T.)

2. L'usage de l'automontage semble se heurter au fait qu'il ne s'effectuera vraisemblablement pas dans `~/.gnupg`. Dans ce cas, le lien symbolique susmentionné serait une solution. (N. d. T.)