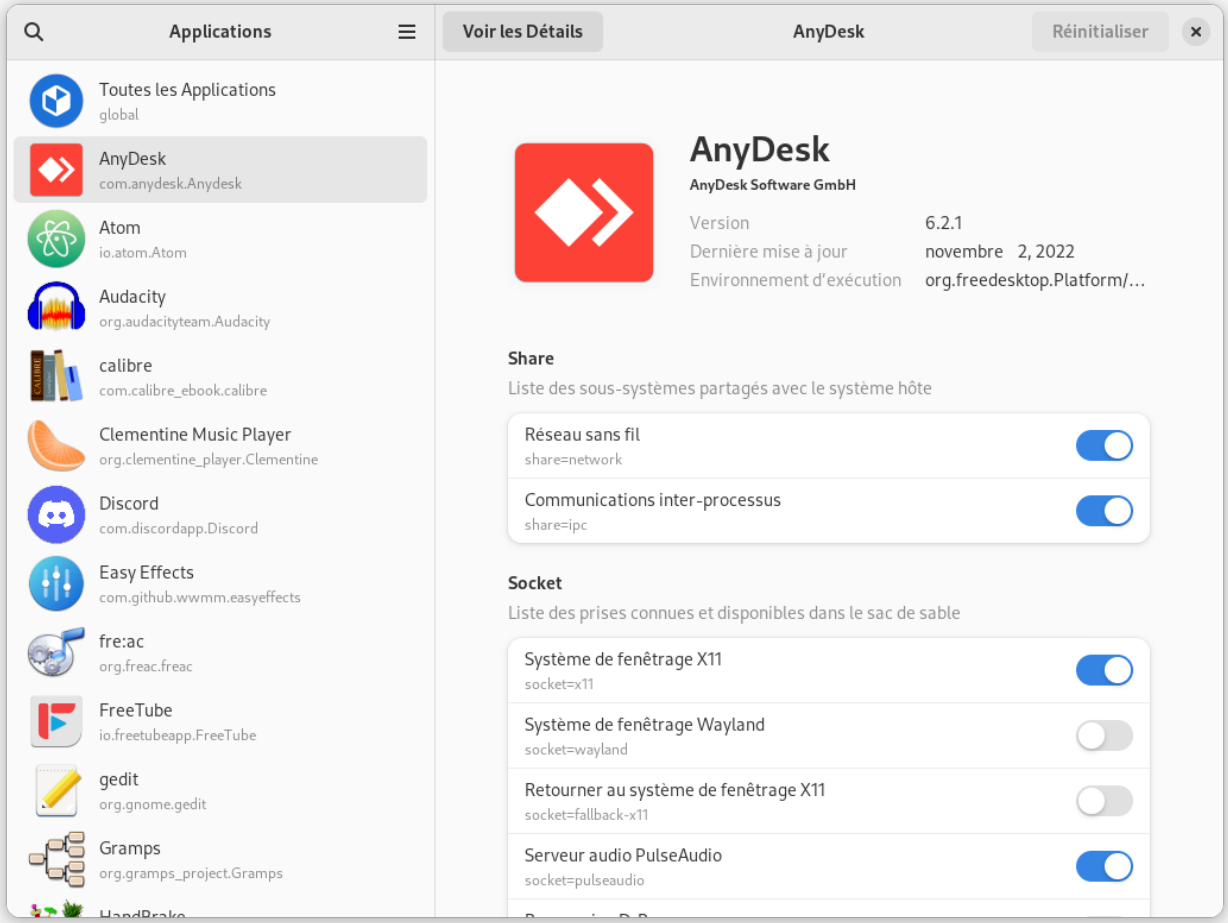
L'isolation (sandboxing) avec Flatpak et Snap

Une des caractéristiques attrayantes offertes à la fois par les packages Snap et Flatpak est la capacité de placer les applications en cours d'exécution dans un environnement contrôlé (sandbox). Cela signifie que l'application est limitée dans les types d'actions qu'elle peut effectuer et les informations auxquelles elle peut accéder. Tout ce qui se trouve en dehors de l'environnement contrôlé est inaccessible pour l'application.

Les technologies Flatpak et Snap fournissent chacune des méthodes pour limiter les actions de leurs packages. Par exemple, nous pouvons empêcher un package Snap ou Flatpak de reproduire du son, d'accéder à certains fichiers, d'afficher des informations sur le bureau ou de communiquer avec d'autres applications en cours d'exécution sur le bureau.

Bien qu'il soit techniquement possible de définir les limites de l'environnement contrôlé pour ces deux types de packages à partir de la ligne de commande, la syntaxe n'est pas particulièrement intuitive et la documentation officielle pour les deux formats de package est moins qu'idéale en termes d'exemples pratiques. C'est pourquoi les utilisateurs de packages Flatpak et Snap utilisent généralement des utilitaires graphiques qui permettent de définir facilement les limites des applications.

Pour les utilisateurs de Flatpak, l'environnement contrôlé est généralement géré avec l'application Flatseal, elle-même disponible en tant que Flatpak. Flatseal affiche les packages Flatpak installés sur la gauche de sa fenêtre. Sur la droite, une longue liste de permissions que nous pouvons accorder ou refuser pour l'application sélectionnée.



La liste est longue et parfois subtile. Par exemple, nous pourrions désactiver la possibilité pour une application de produire du son et être surpris qu'elle puisse quand même générer du son. Cependant, un examen plus approfondi révélera que l'application peut toujours envoyer des données audio à PulseAudio pour être jouées, nous devons donc désactiver cette option également. En d'autres termes, l'interface de Flatseal est simple, mais les options de sécurité interconnectées peuvent ne pas être immédiatement évidentes.

Pour les utilisateurs de Snap, le moyen le plus simple d'ajuster les permissions est généralement l'application Software. Snap s'intègre automatiquement au centre logiciel d'Ubuntu et des distributions apparentées. Lorsque nous installons une application ou visitons sa page d'information dans le centre logiciel, un bouton en haut de la page intitulé “Permissions” apparaît. En cliquant sur ce bouton, une fenêtre s'ouvre dans laquelle nous pouvons activer ou désactiver les permissions de l'environnement contrôlé pour l'application sélectionnée.

La liste des permissions Snap est plus courte que celle présentée par Flatseal, mais je trouve que les options sont bien libellées et, peut-être, plus claires dans leur signification. Les libellés à côté de chaque bascule sont affichés dans un langage que je considère comme plus clair. Sur Flatseal, par exemple, nous verrons des options comme “Fallback to X11 windowing system” ou “PulseAudio sound server”, tandis que pour Snap, nous verrons des options comme “Play audio” et “Access files in your home folder”. Ce dernier est plus facile à comprendre avec moins de connaissances techniques, tandis que la longue liste d'options de Flathub offre peut-être plus de flexibilité.

Les deux formats offrent une isolation (sandboxing) flexible et puissante. Les deux environnements isolés offrent des capacités similaires pour limiter les applications.

— *Cédric ABONNEL dit Cédrix* *Édition initiale du mardi 25 juillet 2023*