

Articles HOWTO - Sécurité

Sécuriser votre ordinateur est un processus continu. Les guides suivants vous aideront à sécuriser votre installation de la Slackware, que ce soit pour les besoins serveur, poste de travail ou ordinateur portable. Assurez-vous de vous abonner à la [mailing list](#) slackware-security. Toutes les annonces de sécurité depuis 1999 sont disponibles sur <http://www.slackware.com/security/>.

Cette section contient des articles relatifs à la sécurisation de votre système et réseau basé sur Slackware.



Inspiré ? Vous voulez écrire un HOWTO ?

Entrez un nom de page (pas d'espaces - utilisez les tirets_bas à la place) et commencez votre article ! You are not allowed to add pages

Sécurité

Sécurité physique

Sécurité réseau

- Pare-feu
- Protection des connexions SSH contre les attaques par force brute: [Install DenyHosts on Slackware](#)
- Utilisez uniquement des clés SSH au lieu de mots de passe pour les connexions SSH: [Utiliser des clés SSH](#)
- Services réseau: les services suivants peuvent être améliorés:
 - [inetd](#)
 - [OpenSSH](#)

Sécurité du système de fichiers

- Chiffrement
 - Chiffrer l'espace de swap pour protéger le contenu sensibles [Activer le cryptage du swap](#)
- Permissions de fichier
- Suivre les changements système avec OSSEC

Vue d'ensemble des HOWTOS sur la Sécurité

Page	Description	Tags
------	-------------	------

hosts.allow , hosts.deny	hosts.allow, hosts.deny Ces deux fichiers dans /etc sont le lieu commun pour stocker les règles qui permettront d'autoriser des hôtes à se connecter à des services sur votre machine. Alors qu'un pare-feu peut être considéré comme cachant une porte, ces fichiers contrôlent qui est autorisé à ouvrir la porte.	howtos , security , slackware allversions , inetd , translator cedric
---	--	--

[howtos](#), [topic page](#), [translator cedric](#)

From:
<https://docs.slackware.com/> - **SlackDocs**

Permanent link:
<https://docs.slackware.com/fr:howtos:security:start>

Last update: **2016/05/22 14:50 (UTC)**

