

Points à vérifier concernant la sécurité des instances

- Suivre les recommandations suivantes :
 - <https://docs.ovh.com/fr/vps/conseils-securisation-vps/>
 - La bonne configuration pour protéger un serveur
- S'abonner au flux RSS des annonces de sécurité *Debian* : <https://www.debian.org/security/dsa>
- N'installer pas plus de paquets/logiciels que nécessaire.
- Mettre à jour régulièrement les paquets manuellement : aptitude update ; aptitude upgrade
 - Ou mieux, automatiser la mise à jour des paquets via *unattended-upgrades* et recevoir les changements via *apt-listchanges*. Tester : unattended-upgrades --dry-run --verbose
- Utiliser des mots de passe forts pour les utilisateurs systèmes et des différents logiciels : 16 caractères comprenant lettres, chiffres et caractères spéciaux.
- Utiliser un gestionnaire de mots de passe (tel que KeePassX) pour stocker tous les **differents** mots de passes créés.
- **Changer la valeur par défaut du port SSH** qui doit avoir une valeur différente de 22 dans /etc/ssh/sshd_config
- Désactiver la connexion SSH pour les utilisateurs root : PermitRootLogin doit être commenté dans /etc/ssh/sshd_config
- Notifier l'administrateur système (adminsys@<domaine-sinp>) par email à chaque connexion SSH sur chaque instance.
- Limiter l'utilisation des installateurs et compilateurs à l'utilisateur root.
- **Installer Fail2ban** pour surveiller les accès réseau grâce aux logs des serveurs et bannir les IP correspondantes aux erreurs d'authentification répétées.
- Installer Rootkit-Hunter pour détecter les éventuelles installations présentes et futures de *rootkits*.
- Désactiver les ports inutilisés avec l'installation du parefeu *Nftables* et de sa surcouche de gestion *Firewalld*.
- Réaliser manuellement un *snapshot* de chaque instance via l'interface OVH une fois l'installation réalisée et à chaque modification importante du système
- Mettre en place une sauvegarde automatique des instances via l'interface OVH
- Réaliser manuellement un *snapshot* du volume *BlockStorage* via l'interface OVH une fois l'intégration des données réalisées et à chaque nouvelle intégration
- Mettre en place une sauvegarde automatique des volumes *BlockStorage* via l'interface OVH → ne semble pas possible via l'interface au 2021-03-22.
- Mettre en place un *dump* automatique des bases de données (*Postgresql*, *MariaDB*) avec export externalisé
- Mettre en place une sauvegarde automatique des principaux dossiers systèmes (/etc, /home, ...) avec export externalisé

From:
<https://wiki-sinp.cbn-alpin.fr/> - **CBNA SINP**



Permanent link:
<https://wiki-sinp.cbn-alpin.fr/serveurs/installation/points-securite?rev=1616423315>

Last update: **2021/03/22 14:28**