Configuration de SSH (serveur et poste local)

Commencer par définir de nouveaux ports SSH pour chaque instance et les stocker dans un outil tel que *Keepass* par exemple.

Configuration de SSH sur le serveur

- Éditer le fichier */etc/ssh/sshd_config* : `vi /etc/ssh/sshd_config`
- Refuser la connexion SSH pour le compte *root*, en modifiant la propriété *PermitRootLogin* comme suit : `PermitRootLogin prohibit-password`
- Maintenir les connexions SSH pendant 15mn, en décommentant et modifiant les propriétés suivantes :

```
ClientAliveInterval 300
ClientAliveCountMax 3
```

- Modification du port SSH par défaut pour renforcer la sécurité :
  - Remplacer la valeur 22 de la propriété `Port` par les nouveaux ports sélectionnés
  - Vérifier que le port n'est pas utilisé par d'autres services avec le registre des noms de services et des numéros de port : https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml
- Redémarrer le serveur SSH : `systemctl restart sshd`

Configuration de SSH sur le poste local

- Éditer/Créer le fichier *config* avec les droits *600* : `touch ~/.ssh/config ; chmod 600 ~/.ssh/config ; vi ~/.ssh/config`
- Pour maintenir les connexion SSH, y placer le contenu :

```
Host *
     ServerAliveInterval 240
```

- Pour faire correspondre les nouveaux port des instances :

```
Host web-<region>-sinp
    Port <port-ssh-web>
Host db-<region>-sinp
    Port <port-ssh-db>
Host bkp-<region>-sinp
    Port <port-ssh-bkp>
```

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

Permanent link:
https://sinp-wiki.cbn-alpin.fr/serveurs/installation/ssh?rev=1690902783

Last update: **2023/08/01 15:13**