

Configurer votre poste local

Modification du fichier /etc/hosts

Pour modifier votre fichier hosts, vous pouvez suivre [cette documentation indiquant le fonctionnement pour différent système d'exploitation](#).

Ajouter les entrées suivantes au fichier /etc/hosts : `vi /etc/hosts`

- SINP PACA :

```
51.91.142.103 db-paca-sinp
51.91.137.130 web-paca-sinp
xxx.xxx.xxx.xxx bkp-paca-sinp
```

- SINP AURA :

```
135.125.89.43 db-aura-sinp
135.125.89.138 web-aura-sinp
51.195.232.41 bkp-aura-sinp
```

Configuration de SSH

Modification du fichier ~/.ssh/config

Une fois les nouveaux port SSH attribué aux serveurs, modifier votre fichier `~/.ssh/config` :

- Éditer/Créer le fichier config avec les droits 600 : `touch ~/.ssh/config ; chmod 600 ~/.ssh/config ; vi ~/.ssh/config`
- Y ajouter : `vi ~/.ssh/config`

```
Host *
  ServerAliveInterval 240
Host web-<region>-sinp
  Port <port-ssh-web-srv>
Host db-<region>-sinp
  Port <port-ssh-db-srv>
Host bkp-<region>-sinp
  Port <port-ssh-bkp-srv>
```

Copier sa clé SSH Public sur les serveurs

- Pour chaque serveur :
 - Copier sa clé SSH Public sur le compte utilisateurs : `ssh-copy-id geonat@<instance>-<region>-sinp`

- Se connecter : ssh `geonat@<instance>-<region>-sinp`
- Afficher les clés autorisées dans la console pour copier sa clé : cat `~/ .ssh/authorized_keys`
- Passer en root : sudo -i
- Depuis root, passer dans l'utilisateur cible. Ex. avec `admin` : su - `admin`
- Éditer le fichier `~/.ssh/authorized_keys` et ajouter sa clé : vi `~/ .ssh/authorized_keys`
- Quitter l'utilisateur cible pour revenir en `root` : exit
- Recommencer pour les différents utilisateurs de l'instance :
 - "web-srv" : `admin` et `geonat`
 - "db-srv" : `admin` et `geonat`.
 - "b kp-srv" : `admin`, `geonat`, `backups`, `provider`

From:

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



Permanent link:

<https://wiki-sinp.cbn-alpin.fr/serveurs/installation/config-poste-local?rev=1622197242>

Last update: **2021/05/28 10:20**