Configuration des comptes utilisateurs

Configurer le compte debian

- Se connecter au serveur depuis la machine dont la clé SSH a été enregistrée lors de la création de l'instance Public Cloud. Utiliser la commande : `ssh debian@<ip-public>`
  - **Note** : si vous avez modifier votre fichier */etc/hosts*, vous pouvez utiliser : '' ssh debian@web-<region>-sinp '' puis '' ssh debian@db-<region>-sinp ''
- Modifier le fichier *.bashrc* de l'utilisateur *debian* : `vi /home/debian/.bashrc`
  - Décommenter les lignes d'alias
  - Ajouter le prompt en couleur :

```
PS1='${debian_chroot:+($debian_chroot)}\[\033[1;33m\]\u@\h\[\033[00m\]:\[\033[01;34m\]\w\[\033[00m\]\$ '
```

Configurer le compte root

- Pas d'accès direct *root* par SSH (⇒ sécurité !), se connecter en utilisant la commande : `ssh debian@<ip-public>`
- Depuis l'utilisateur *debian*, passer en root : `sudo -i`
- Définir un mot de passe pour root (stocker ses infos dans Keepass) : `passwd`
- Configuration du compte *root* :
  - Modifier le fichier *.bashrc* de root : `vi /root/.bashrc`
    - Décommenter les lignes d'alias
    - Ajouter le prompt en couleur :

```
PS1='${debian_chroot:+($debian_chroot)}\[\033[01;31m\]\u@\h\[\033[00m\]:\[\033[01;34m\]\w\[\033[00m\]\$ '
```

    - Ajouter la prise en charge du fichier *.bash_aliases* :

```
# Charger les alias depuis le fichier .bash_aliases
if [ -f ~/.bash_aliases ]; then
    . ~/.bash_aliases
fi
```

- Ajouter le fichier *.bash_aliases* :
  - `vi ~/.bash_aliases`
  - Y mettre le contenu suivant :
    - Pour *web-srv* :

```
alias nginx-reload='nginx -t && nginx -s reload'
```

    - Pour *db-srv* :

```
alias pga='sudo -u postgres pg_activity -U postgres'
```

- Installer la coloration syntaxique pour les fichiers de conf Nginx avec Vim :
  - Créer un dossier qui contiendra les fichiers de syntaxe : `mkdir -p ~/.vim/syntax`
  - Créer le fichier indiquant les syntaxes à utilsier : `vim ~/.vim/filetype.vim`
    - Y placer le contenu suivant :

```
au BufRead,BufNewFile /etc/nginx/*,/usr/local/nginx/conf/* if &ft == '' | setfiletype nginx | endif
```

  - Télécharger la dernière version de la syntaxe : `wget -O ~/.vim/syntax/nginx.vim https://www.vim.org/scripts/download_script.php?src_id=27919`
    - Rechercher la dernière version à installer sur cette page : https://www.vim.org/scripts/script.php?script_id=5999

Création utilisateur geonat

- L'utilisateur *debian* (= *admin*) est l'administrateur système du serveur. Il possède des droits *sudo* avancés.
- Il est nécessaire de le créer sur les 2 instances (*web-srv* et *db-srv*).
- L'utilisateur *geonat* va servir d'utilisateur système permettant d'accéder à la base de données de GeoNature qui aura pour administrateur *geonatadmin* :
  - Créer un utilisateur *geonat* : `adduser geonat`
  - L'ajouter au groupe *sudo* : `usermod -aG sudo geonat`
- Activer la connexion par mot de passe avant d'appliquer la commande `ssh-copy-id geonat@<server>`
  - Dans le serveur → modification du fichier de config ssh :

```
vi /etc/ssh/sshd_config
```

    - Ajouter à la fin du fichier :

```
Match User geonat
   PasswordAuthentication yes
```

- Redémarrer ssh :

```
systemctl restart sshd
```

- Ajouter votre clé SSH public au fichier *~/.ssh/authorized_keys* pour pouvoir s'y connecter directement :
  - Depuis votre machine locale lancer la commander : `ssh-copy-id geonat@<ip-public-instance>`
  - Vérifier que la connexion fonctionne et qu'aucun mot de passe n'est demandé : `ssh geonat@<ip-public-instance>`

Changer le nom du compte debian en admin

- Par défaut, les instances public cloud sous Debian Buster, possède un utilisateur *debian*, nous allons lui changer son nom pour *admin*.
- **ATTENTION PRÉ-REQUIS** : veiller à avoir préalablement :

    - ajouter votre clé SSH à l'utilisateur *geonat* afin de pouvoir vous connecter
    - créer un mot de passe pour *root* afin de pouvoir y accéder au choix depuis :
        - l'utilisateur *geonat* et la commande `su -`
        - la console VNC disponible sur le Manager OVH et Horizon OpenStack. Attention, cette console est en quwerty par défaut !
- Se connecter au serveur depuis votre machine locale, utiliser la commande : `ssh geonat@<ip-public-instance>`
- Passer en *root* : `su -`
- Changer le nom de l'utilisateur *debian* pour *admin* :
    - Vérifier qu'aucune console n'est connecté via SSH à l'utilisateur *debian* sinon les commandes suivantes sont refusées
    - Modifier le nom et le *home* : `usermod -l admin -d /home/admin -m debian`
    - Modifier le groupe : `groupmod -n admin debian`
- Mettre à jour le fichier de config Cloud : `vi /etc/cloud/cloud.cfg`
    - Remplacer *debian* par *admin* : `system_info:` > `default_user:` > `name: admin`
- Mettre à jour les fichiers sudoers :
    - Donner les droits d'écriture à root aux fichiers concernés : `chmod -R 740 /etc/sudoers.d/*`
    - Remplacer *debian* par *admin* dans tous les fichiers présents dans le dossier `/etc/sudoers.d/`
    - Remettre les droits par défaut : `chmod -R 440 /etc/sudoers.d/*`
- Redémarrer la machine : `reboot`
- Attendre le redémarrage de la machine : visible depuis l'interface VNC de l'instance sur le Manager OVH
- Se connecter à la machine : `ssh admin@<ip-public-instance>`
- Vérifier que la possibilité de passer en root fonctionne avec : `sudo -i`

Configurer les alertes de Sudo

- En *root*, éditer le fichier de config sudo principal : `visudo`
    - Vérifier que la ligne suivante à la fin du fichier ne commence pas par un #, si c'est le cas le retirer : `includedir /etc/sudoers.d`
- Créer un fichier */etc/sudoers.d/10-config-email* avec : `visudo -f /etc/sudoers.d/10-config-email`
    - Ajouter le contenu suivant :

```
# Name of this file do not end in '~' or contain a '.' character.
# This file should be mode 0440: `chmod 440 <this-file-name>`

Defaults mailto = "adminsys@<domaine-sinp>"
Defaults mailfrom = "mailer@<domaine-sinp>"
Defaults mail_badpass
Defaults mail_always
Defaults mail_no_user
Defaults mailsub = "*** Command run via sudo on %h ***"
Defaults badpass_message = "Please Provide Correct Password"
Defaults !lecture,tty_tickets,!fqdn,!syslog
Defaults logfile=/var/log/sudo.log
```

- Vérifier les droits du fichier : `ls -al /etc/sudoers.d/`

- S'ils ne sont pas *0440*,donner les bons droits au fichier : `chmod 440 /etc/sudoers.d/10-config-email`

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

Permanent link:
https://sinp-wiki.cbn-alpin.fr/serveurs/installation/utilisateurs?rev=1686209126

Last update: **2023/06/08 07:25**