Installation serveur SFTP et espace d'hébergement des données

Principe: nous allons utiliser un container Docker qui hébergera le serveur SFTP. L'utilisateur *provider* de l'hôte hébergera les dossiers des utilisateurs du serveur SFTP du container. L'utilisateur *provider* pourra être accéder uniquement via une clé SSH préalablement autorisé. Les utilisateurs du serveur SFTP seront accessibles par mot de passe. Les dossiers chrootés des utilisateurs du serveur SFTP devront être accessible par l'utilisateur *provider*.

TODO

• Il serait intéressant de rajouter un utilisateur au SFTP avec des droits en lecture seulement. — Jean-Pascal MILCENT-2021/12/16 15:07 — Jean-Pascal MILCENT 2023/06/08 08:25

Création d'un utilisateur "provider"

- Se connecter au serveur "bkp-srv" en tant qu'admin : ssh admin@bkp-<region>-sinp
- Passer en root : sudo -i
- Créer l'utilisateur "provider" sans mot de passe (connexion par clé SSH) avec son dossier /home/provider: useradd provider --create-home --home-dir /home/provider/ --shell /bin/bash
- Créer le dossier qui contiendra les infos concernant SSH: mkdir /home/provider/.ssh;
 chmod 700 /home/provider/.ssh
- Créer le fichier des clés SSH autorisées à partir de celui de l'utilisateur admin : cp /home/admin/.ssh/authorized_keys /home/provider/.ssh/authorized_keys
- Attribuer la propriété du dossier et de son contenu à l'utilisateur provider : chown -R provider: /home/provider/.ssh
- Créer le dossier qui hébergera les données du serveur SFTP :
 - Si le serveur n'a pas de disque additionnel monté sur /data : mkdir /home/provider/data
 - o Si le serveur a un disque additionnel monté sur /data :
 - Créer le dossier : mkdir /data/sftp-data
 - Donner les bons droits : chown provider:users /data/sftp-data
 - Créer le lien symbolique : ln -s /data/sftp-data /home/provider/data

Mise en place du serveur SFTP via Docker

- En local sur votre machine placer vous à la racine de votre dépôt sinp-<region>-srv : cd ~/workspace/sinp-<region>-srv/
 - À l'aide de Rsync uploader les fichiers pour Docker :

```
rsync -av ./bkp-srv/home/admin/docker/sftp/ admin@bkp-<region>-
sinp:/home/admin/docker/sftp/ --dry-run
```

(si tout est ok, supprimer l'option --dry-run)

- Se connecter au serveur "bkp-srv" en tant gu'admin : ssh admin@bkp-<region>-sinp
- Placer vous dans le dossier du docker SFTP : cd ~/docker/sftp/
- Générer les clés SSH qui seront utilisées par le serveur SFTP sur l'hôte afin d'éviter que les utilisateurs recoivent un avertissement MITM après chaque redémarrage du container. Lancer les commandes suivantes en acceptant toutes les valeurs par défaut des différentes questions :
 - ∘ ssh-keygen -t ed25519 -f ssh host ed25519 key < /dev/null
 - ∘ ssh-keygen -t rsa -b 4096 -f ssh host rsa key < /dev/null
- Créer le fichier .env et le remplir : cp .env.sample .env ; vi .env
- Lancer le docker : docker compose up
- Si tout est OK, arrêter le container avec CTRL+C puis le redémarrer en tant que service : docker compose up -d
- Passer en root : sudo -i
- Aller dans le dossier : cd /home/provider/data/
- Créer les dossiers qui hébergeront les données à intégrer :
 - Pour PACA: mkdir cbna cbnmed cbna-cbnmed cen-paca
 - Pour AURA: mkdir cbna cbnmc flavia lpo
- Donner les droits à l'utilisateur provider d'y accéder en lecture et écriture : chown provider:users ./*

Tester la connexion SFTP

- En local sur votre machine, installer un client SFTP: aptitude install filezilla
- Configurer votre client SFTP:
 - o Protocole: SFTP
 - Hôte : IP du serveur "bkp-srv"
 - Port : indiquer la valeur du paramètre HOST_SSH_PORT du fichier . env du container Docker SFTP configuré via l'utilisateur admin.
 - Type d'authentification : Normale
 - Identifiant : indiquer la valeur du paramètre SFTP_USER_NAME du fichier .env du container Docker SFTP configuré via l'utilisateur admin.
 - Mot de passe : indiquer la valeur du paramètre SFTP_USER_PWD du fichier .env du container Docker SFTP configuré via l'utilisateur admin.
 - Enregistrer
- Tenter de vous connecter et d'uploader un fichier dans un des dossiers préalablement créé.
- Normalement, il est impossible d'uploader des fichiers ou de créer de nouveaux dossiers à la racine.

Ajouter un utilisateur du SFTP en lecture seule

From:

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

Permanent link:

https://sinp-wiki.cbn-alpin.fr/serveurs/installation/bkp-srv/install-sftp?rev =1686212762



Last update: 2023/06/08 08:26