FP
CREATION D'UN BASTION

Table des matières

Introduction

Le bastion utilisé ici est le bastion d'OVH. Il est installé sur une distribution Linux qui est Rocky Linux.

La mise en place de ce bastion permettra une meilleure gestion des différents serveurs. C'est-à-dire que les administrateurs auront un meilleur historique des actions effectuées par les utilisateurs sur les différents serveurs. De plus, les utilisateurs n'auront accès qu'au serveur utile à leur domaine.

I/ Installation du Bastion

1. Récupérer le code nécessaire à l'installation du Bastion

```
git clone https://github.com/ovh/the-bastion /opt/bastion
git -C /opt/bastion checkout $(git -C /opt/bastion tag | tail -1)
```

2. Installer les paquets nécessaires au Bastion

```
/opt/bastion/bin/admin/packages-check.sh -i            # Vérifie la distribution et les fichiers
/opt/bastion/bin/admin/install-ttyrec.sh -a            # Installe le service d'enregistrement
```

3. Installer le bastion

```
/opt/bastion/bin/admin/install --new-install
```

4. Chiffrer les /homes

```
/opt/bastion/bin/admin/setup-encryption.sh
```

5. Vérifier la configuration et la modifier si besoin

```
nano /etc/bastion/bastion.conf
```

6. Vérifier que le code fonctionne

```
/opt/bastion/bin/dev/perl-check.sh
```

II/ Configuration du Bastion

1. Création du premier utilisateur

```
/opt/bastion/bin/admin/setup-first-admin-account.sh USERNAME auto    #Remplacer USERNAME par le nom voulu
```

2. Générer la clé GPG du Bastion

```
/opt/bastion/bin/admin/setup-gpg.sh --generate
```

3. Générer la clé GPG du ou des admins

```
myname='test'                                  #Rentrer le nom de l'admin
email='test@test.test'                         #Rentrer l'e-mail de l'admin
bastion='bastion.test.org'                     #Rentrer l'URL du Bastion
pass=$(pwgen -sy 12 1)                         #Génère un mot de passe
echo "The passphrase for the key will be: $pass"
gpg --batch --pinentry-mode loopback --passphrase-fd 0 --quick-generate-key "$myname <$email>" ed25519
sign 0 <<< "$pass"
fpr=$(gpg --list-keys "$myname <$email>" | grep -Eo '[A-F0-9]{40}')
gpg --batch --pinentry-mode loopback --passphrase-fd 0 --quick-add-key "$fpr" cv25519 encr 0 <<< "$pass"
```

4. Récupérer la clé publique, l'importer et exporter la clé privée pour la sécuriser

```
gpg -a --export "$myname <$email>"          #Copier le résultat et le coller lors de la commande suivante
/opt/bastion/bin/admin/setup-gpg.sh –import
gpg --export-secret-keys --armor "$myname <$email>"
```

5. Ajouter dans le fichier la clé du bastion, sa passphrase, et la clé GPG des admins dans :

```
/etc/bastion/osh-encrypt-rsync.conf
```

```
"signing_key": "FFFFFFFF",

"signing_key_passphrase": "BBBBBBBB",

"recipients": [                              #Possibilité d'en mettre plusieurs
    [ "AAAAAAA" ]
],
```

6. Vérification du fichier de configuration

```
/opt/bastion/bin/cron/osh-encrypt-rsync.pl --config-test
/opt/bastion/bin/cron/osh-encrypt-rsync.pl -dry-run
```

7. Mise en place des sauvegardes à distance

```
nano /etc/bastion/osh-backup-acl-keys.conf    # Mettre une valeur dans PUSH_REMOTE et PUSH_OPTIONS
/opt/bastion/bin/cron/osh-backup-acl-keys.sh
```

8. Activer syslog

```
nano /etc/bastion/bastion.conf       # Activer le paramètre enableSyslog
```

III/ Mise à jour

1. Mise à jour du bastion pour avoir les ajustements de la dernière version

```
/opt/bastion/bin/admin/install --upgrade
```

IV/ Tests

1. Commande de tests

```
/opt/bastion/tests/functional/launch_tests_on_instance.sh <IP> <port> <remote_user_name> <ssh_key_path>
```