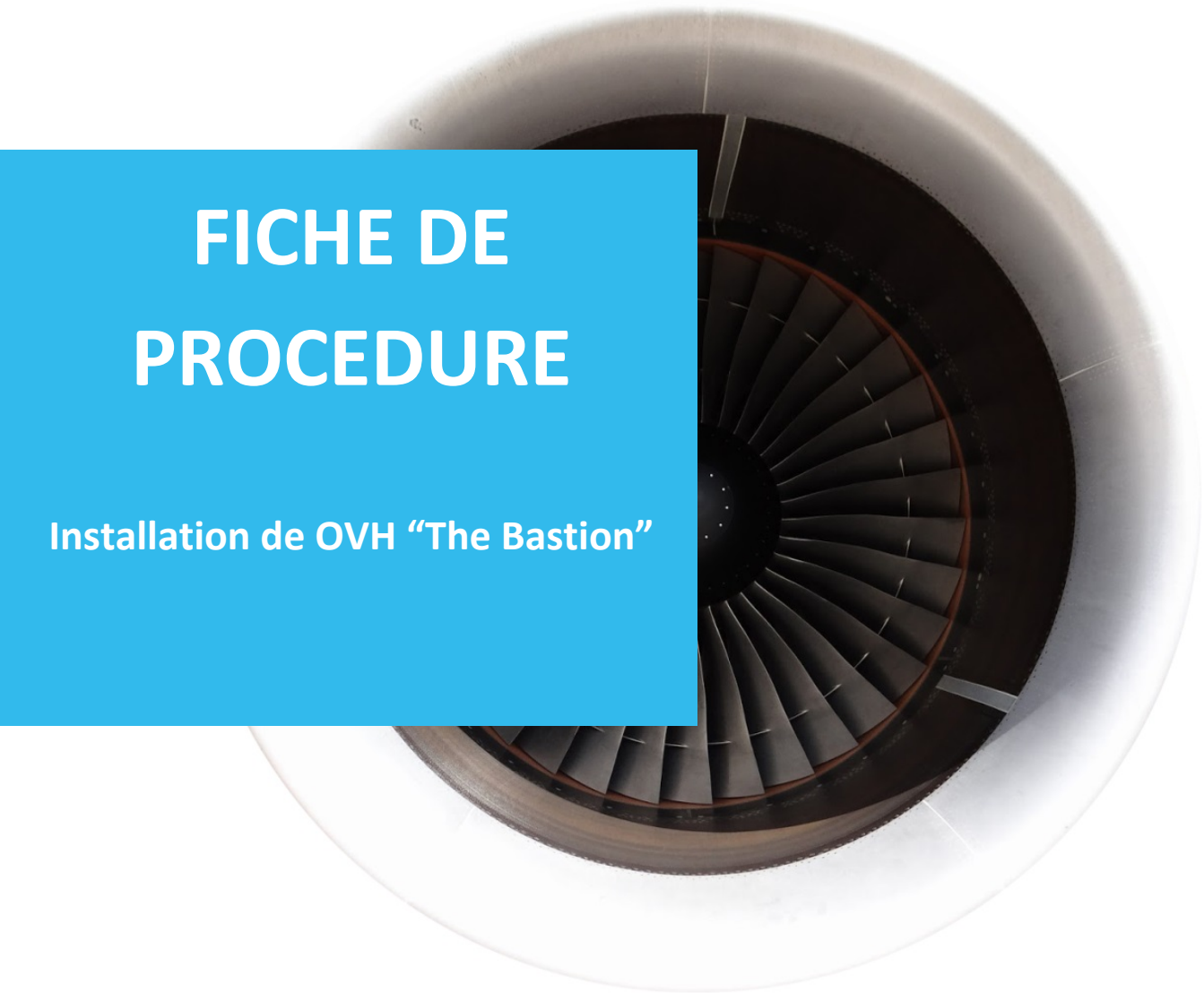
Kyrian PAINAULT – SIO2



FICHE DE PROCEDURE

Installation de OVH “The Bastion”

Ecole Nationale Supérieure de Mécanique et d'Aérotechnique
Téléport 2 - 1 avenue Clément Ader
BP 40109
86961 Futuroscope Chasseneuil Cedex
Tél : +33 (0)5 49 49 80 80

Installation manuelle sous Debian 11/12

Prérequis

Une distribution Linux récente. Il existe une fiche de compatibilité officielle :

- Debian 12 (Bookworm), 11 (Bullseye), 10 (Buster)
- CentOS 7.x
- RockyLinux 8.x, 9.x
- Ubuntu LTS 22.04, 20.04, 18.04, 16.04
- OpenSUSE Leap 15.5

Paquets :

- git

Si The Bastion sera installé de manière virtualisée, il est préférable de l'installer dans une VM plutôt qu'un conteneur du type LXC, pour des raisons de support du changement d'utilisateurs.

Il est également important de connaître le fonctionnement du système de clés publiques et privées ainsi que leur fonctionnement sur SSH de manière à ne pas être confus lors de la mise en place du Bastion.

Des informations additionnelles sont disponibles sur la documentation officielle :

Création du couple de clés du client administrateur

Il préférable à ce moment de mettre en place l'authentification par clé publique, pour ne pas être bloqué en dehors de la machine par la suite dû au durcissement des règles de sécurité SSH par The Bastion lui même.

Coté client : `ssh-keygen -t ed25519` ou `ssh-keygen -t ecdsa -b 521` ou `ssh-keygen -t rsa -b 4096`

Coté serveur :

- scp root@addr_client:~/.ssh/id_ed25519.pub .
- mv id_ed25519.pub admin_id_ed25519.pub
- cat admin_id_ed25519.pub >> ~/.ssh/authorized_keys

Connexion au serveur

Connectez vous au serveur en tant que root.

```
ssh root@addr_bastion
```

Clonage du dépot

En ayant installé git au préalable, cloner le dépot et l'extraire dans /opt/bastion, où il vivra.

```
git clone https://github.com/ovh/the-bastion /opt/bastion
```

```
git -C /opt/bastion checkout $(git -C /opt/bastion tag | tail -1)
```

Installation des dépendances

The Bastion dispose d'un script automatisant l'installation de ses dépendances sur les distributions compatibles, il peut être exécuté comme ceci :

```
/opt/bastion/bin/admin/packages-check.sh -i
```

OVH recommande également l'installation de syslog-ng pour la collecte de logs, ce qui peut être fait via l'aj

out de l'argument `-s`

The Bastion requiert l'installation de son fork de ttyrec, qui permet d'enregistrer les sessions terminal. Il peut être installé via le biais d'un script fourni :

```
/opt/bastion/bin/admin/install-ttyrec.sh -a
```

L'outil pour la compatibilité Yubico (`yubico-piv-checker`) et l'outil de génération de mots de passe avancés (`mkhash-helper`) peuvent être installés de la même manière si nécessaire.

Chiffrement du /home

OVH recommande le chiffrement de la partition home afin de protéger les clés et paramètres générés par The Bastion.

Générez ou choisissez un mot de passe sécurisé, puis exécutez le script :

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

Lire les instructions et confirmer si nécessaire. Rechargez les paramètres de systemd avec :

```
systemctl daemon-reload
```

Installation de The Bastion

Une aide est disponible :

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

Exécuter, pour une nouvelle installation :

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

Pour une mise à niveau :

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

OVH recommande de durcir la configuration soi-même en cas de mise à niveau. La comparaison du fichier actuel par rapport au modèle peut être effectuée de la manière suivante (exemple pour Debian 11, d'autres modèles sont disponibles) :

```
vimdiff /opt/bastion/etc/ssh/ssh_config.debian11 /etc/ssh/ssh_config
```

```
vimdiff /opt/bastion/etc/ssh/sshd_config.debian11 /etc/ssh/sshd_config
```

Modifier le fichier de configuration si nécessaire

Utilisez l'éditeur de votre choix.

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

Vérifier la bonne installation des modules Perl requis

Exécuter :

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

Créer le premier compte bastion

Préparer la clé publique de l'utilisateur qui devra se connecter, celle-ci devra être collée dans l'interface :

```
/opt/bastion/bin/admin/setup-first-admin-account.sh nom_utilisateur
auto
```

Les utilisateurs créés par The Bastion peuvent être testés en faisant un `su - utilisateur` et en se connectant avec l'utilisateur distant du Bastion avec son couple de clés privée/publique. Pour réaliser cette manipulation sur le serveur lui-même, on peut effectuer la commande SSH suivante :

- ssh –o "IdentitiesOnly=yes" –i ~/.ssh/id_rsa *utilisateur@nom_hôte*
  - "IdentitiesOnly=yes" sert à forcer la connexion par couple de clés.