

The Bastion

SSH

fichier de conf hardening ssh

nano /etc/ssh/sshd_config.d/ssh-hardening.conf

```
Port 60222
PermitRootLogin no
PasswordAuthentication no
PubkeyAuthentication yes
Protocol 2
Ciphers aes256-ctr,aes192-ctr,aes128-ctr
MACs hmac-sha2-512,hmac-sha2-256
AllowUsers sysadmin
#AllowGroups
X11Forwarding no
AllowAgentForwarding no
LoginGraceTime 1m
MaxAuthTries 3
ClientAliveInterval 300
ClientAliveCountMax 0
KexAlgorithms curve25519-sha256@libssh.org
LogLevel VERBOSE
```

création des clés ssh

```
Get-Service ssh-agent | Set-Service -StartupType Automatic

Start-Service ssh-agent

Get-Service ssh-agent
```

```
ssh-keygen -t ed25519 -C "mon_commentaire"
```

```
ssh-add $env:USERPROFILE\.ssh\id_ed25519
```

Alias ssh

il est possible de faire un fichier configuration qui permet de faciliter la connexion ssh

```
# Configuration globale
Host *
    ForwardAgent no
    ForwardX11 no
    IdentitiesOnly yes ## n'autorise les connexion qu'avec des clés ssh

# Alias pour un autre serveur avec clé spécifique
Host bssh
    HostName 192.168.0.25
    User bastion
    Port 60222
    IdentityFile ~/.ssh/bastion ## la clé privé
    Compression yes
    LogLevel INFO
```

ajout de de la clé ssh dans le authorized keys

rajouter la clé dans le dossier de l'utilisateur avec lequel vous voulez vous connecter

```
cd /home/sysadmin/.ssh
```

```
sudo nano authorized_keys
```

rajouter dans ce fichier votre clé publique

Qu'est-ce que The Bastion ?

The Bastion est un bastion (ou jump server) SSH conçu pour sécuriser et contrôler l'accès aux serveurs d'une organisation. Il agit comme un point central par lequel toutes les connexions SSH passent, permettant une surveillance et un contrôle stricts des accès.

Fonctionnalités principales :

1. **Contrôle d'accès centralisé** : The Bastion permet de centraliser et de gérer l'accès à tous les serveurs via SSH à partir d'un seul point d'entrée. Les utilisateurs doivent se connecter au bastion avant d'accéder aux serveurs finaux.
2. **Auditabilité** : Chaque connexion SSH passant par The Bastion est enregistrée, ce qui permet une traçabilité complète des actions des utilisateurs. Les logs détaillés facilitent les audits de sécurité et la conformité réglementaire.
3. **Sécurité renforcée** : En limitant les accès SSH directs aux serveurs, The Bastion réduit la surface d'attaque et ajoute une couche supplémentaire de sécurité. Il peut également appliquer des politiques de sécurité strictes, telles que l'authentification multifactorielle (MFA).
4. **Isolation des environnements** : The Bastion peut être configuré pour isoler différents environnements (production, développement, etc.), permettant ainsi de restreindre les accès en fonction des rôles des utilisateurs.
5. **Facilité d'utilisation** : Il fournit des outils conviviaux pour les utilisateurs finaux et les administrateurs, facilitant la gestion des accès sans compromettre la sécurité.

Comment fonctionne The Bastion :

1. **Connexion initiale** : L'utilisateur se connecte au bastion via SSH avec ses informations d'authentification.
2. **Vérification d'accès** : The Bastion vérifie les permissions de l'utilisateur et enregistre la tentative de connexion.
3. **Redirection sécurisée** : Une fois l'authentification réussie, l'utilisateur peut se connecter aux serveurs cibles via The Bastion. Toutes les connexions sont redirigées et surveillées.
4. **Enregistrement des sessions** : Les sessions SSH sont enregistrées pour audit et analyse. Les actions des utilisateurs peuvent être rejouées si nécessaire pour des vérifications postérieures.
5. **Déconnexion** : Lorsque l'utilisateur termine sa session, The Bastion enregistre la déconnexion et met à jour les logs.

Avantages de l'utilisation de The Bastion :

- **Sécurité accrue** grâce à la centralisation des accès et à la surveillance des sessions.
- **Auditabilité** facilitée par les logs détaillés et l'enregistrement des sessions.
- **Contrôle d'accès simplifié** grâce à la gestion centralisée des permissions.
- **Réduction de la surface d'attaque** en empêchant les accès SSH directs aux serveurs sensibles.

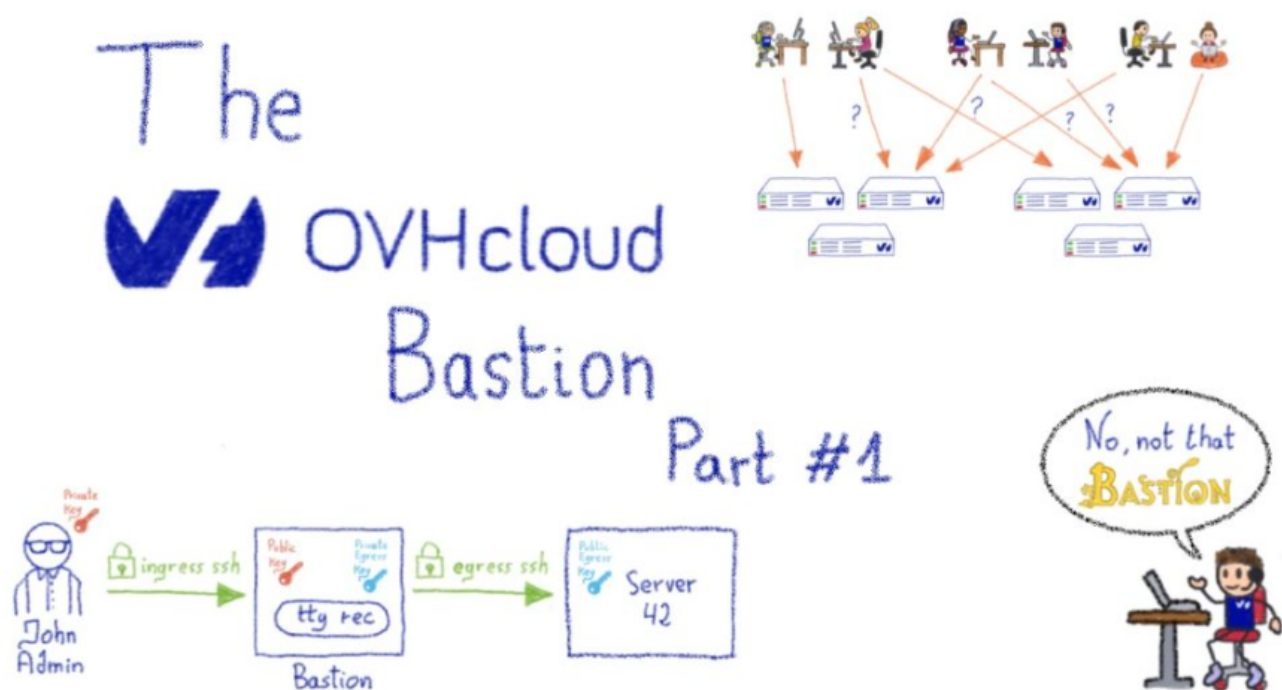


Image avec un petit dessin que j'aime bien pour son petit dessin en bas à gauche qui illustre bien le fonctionnement de the bastion

Pour mieux comprendre ce schéma, je vous invite à aller sur la page de lien ci-dessous
<https://blog.ovhcloud.com/the-ovhcloud-bastion-part-1/>

Installation de the bastion

Cette commande télécharge le code source de "The Bastion" depuis le dépôt GitHub officiel et le place dans le répertoire /opt/bastion sur le serveur

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

Cette commande change le répertoire de travail en /opt/bastion et bascule le code sur le tag le plus récent du dépôt.

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

Installation des paquets nécessaires

Ce script vérifie les paquets nécessaires pour le bon fonctionnement de "The Bastion" et les installe si nécessaire.

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

Installe **tttyrec**, un outil pour enregistrer les sessions de terminal.

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

Installe le **Yubico PIV Checker**, un outil pour vérifier les YubiKeys (dispositifs d'authentification physique).

```
| /opt/bastion/bin/admin/install-yubico-piv-checker.sh -a
```

Installe le helper **mkhash** pour la gestion des mots de passe et des hashes.

```
| /opt/bastion/bin/admin/install-mkhash-helper.sh -a
```

Chiffrement de la partition home

Ce script configure le chiffrement du dossier home pour protéger les clés SSH et autres données sensibles.

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

Installation de The bastion

Lance le processus d'installation de "The Bastion" sur le système.

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

Revoir la configuration

Modifier le nom de votre bastion

```
| sudo nano /etc/bastion/bastion.conf
```

```
# bastionName (string)
#   DESC: This will be the name advertised in the aliases admins will give to bastion users, and also in the banner of
#   DEFAULT: "fix-my-config-please-missing-bastion-name"
"bastionName": "TheBastion",
#
```

Vérifie les modules Perl nécessaires au bon fonctionnement de "The Bastion"

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

Crée son premier compte bastion

Ce script crée le premier compte administrateur sur "The Bastion". Le USERNAME doit être remplacé par le nom d'utilisateur souhaité

```
sudo nano /opt/bastion/bin/admin/setup-first-admin-account.sh USERNAME auto
```

```
sysadmin@bastion: /opt/bastion$ sudo /opt/bastion/bin/admin/setup-first-admin-account.sh bastion auto
Bastion the-bastion-3.16.99-rc1
> create a new bastion account

Please paste the SSH key you want to add.
A quick overview of the different algorithms:
FIDO2 Ed25519: robustness[✓✓✓] speed[✓✓✓], generate: 'ssh-keygen -t ed25519-sk -O resident -O application=ssh:2024-07-30.TheBastion'
Ed25519      : robustness[✓✓✓] speed[✓✓✓], generate: 'ssh-keygen -t ed25519'
FIDO2 ECDSA  : robustness[✓✓ ] speed[✓✓✓], generate: 'ssh-keygen -t ecdsa-sk -b 521 -O resident -O application=ssh:2024-07-30.TheBastion'
ECDSA        : robustness[✓✓ ] speed[✓✓✓], generate: 'ssh-keygen -t ecdsa -b 521'
RSA          : robustness[✓ ] speed[✓ ], generate: 'ssh-keygen -t rsa -b 4096'

Note that FIDO2 algorithms require a FIDO2-compatible hardware Security Key.

This table is meant as a quick cheat-sheet, you're warmly advised to do
your own research, as other constraints may apply to your environment.

Please ensure your private key is encrypted using a proper passphrase (your paste won't be echoed).
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIz2nw+It5J4DjVbqlKuh+o7XbRB0oxIRNuNuluXy1sV bastion
Creating group bastion with GID 99998...
Creating user bastion with UID 99998...
useradd warning: bastion's uid 99998 outside of the UID_MIN 1000 and UID_MAX 60000 range.
Creating tty group of account...
Adding account to potential supplementary groups...
Creating needed files and directories with proper permissions in home...
Creating some more directories...
Applying proper ownerships...
Adding provided public key in authorized_keys file...
Generating account personal bastion key...
Account successfully created!
Configuring sudoers for this account
*** Regenerating account 'bastion' sudoers file from templates
^> ... generating /etc/sudoers.d/osh-account-bastion_fe9ea7
^> [ OK ]
==> alias TheBastion='ssh bastion@Bastion -t -- '
To test his access, ask this user to set the above alias in their .bash_aliases, then run 'TheBastion --osh info'
```

Configuration d'une connexion ssh avec le bastion

Se connecter premièrement avec l'utilisateur crée avant sur le bastion

```
ssh bastion@192.168.0.49 -p 22 -i ~/.ssh/bastion
```

Cette commande vérifie le bon fonctionnement du bastion et affiche ses informations général

```
bssh --osh info
```

```
afin de récupérer la clé publique
```

```
selfListEgressKeys
```

```

bastion@TheBastion(master)> selfListEgressKeys
-----the-bastion-3.16.99-rc1-----
▶ your account's public egress keys

You can copy one of those keys to a remote machine to get access to it through your account
on this bastion, if it is listed in your private access list (check selfListAccesses)

Always include the from="192.168.0.49,172.17.0.1" part when copying the key to a server!

fingerprint: SHA256:/PKa6/OXFtLwivNOKrSTJSHDAks1dOKsTQbTKhN5bJM (RSA-4096) [ID = id6a80f40b]
keyline follows, please copy the *whole* line:
from="192.168.0.49,172.17.0.1" ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAQCFwAx2t1S2KArCLTexdoEYR9HALcUE/pmkidgWb9KcE6E8x8thbnIuHz9AvJMoJ+2kHppLr4S8kdSy85jctJ5W8ISuDtYuV4PQ16GAFAAk/LsoLwz6oYh8rAQCRzcr2+SVQjbyu9R1L1
Eydhl2kOLeXESBjccKgj6VXKk1DMPPLKFVjWz2TfVvKHw2Dw1CWBlnedJtLaBXLTAUX7ZT8/cpy8J5qQBHGdg0FUF1JoAp03z8H4Gu9Ltn/whRoj7VcFU29TNJv5GeFDTRIs+1j61Ae2VQF69TgJJXUfHn9zUu2EUTdBU1L/V7uLEvFfxCKUkApkKoyKXBRn9n3zxcLhrD3ow
qk802augb4TtwirW4UjzIDKsS80WuWk4dKCF33XQy5vzcZt53FmH79108BChQ3kVUqCtNR18L3m26dhrhapT8qHToyqB0P0hZu3USJkC3hu7G1j2Ep+vZ4HhCD-AR12cc0H2-0P7MGR14/468YFctL0AuEe9+bECeLRAB8qDP0ZyNZTu+hSP0pTou48IT6Fp+LT
PT0BS1U1V9BrdNnqMDFgxwfilKcAYP+EyAd+OdrWtWmbrLzL4L9NZRMGAYlj3LQuee8yRfFs+43oYJ5Xj4D71Voz5w/RxgZPkqLK8ZBSR5675U71Sm1t0856TmFzw== bastion@TheBastion:1722372142
-----</selfListEgressKeys>-----
bastion@TheBastion(master)> |

```

- Copier la clé publique
- Aller sur le client sur lequel on souhaite se connecter en ssh
- Rajouter la clé publique dans le authorized keys de votre utilisateur

Maintenant, nous pouvons enregistrer la connexion dans the bastion

```
selfAddPersonalAccess --host 192.168.0.35 --port 60222 --user sysadmin
```

```

bastion@TheBastion(master)> selfAddPersonalAccess --host 192.168.0.35 --port 60222 --user sysadmin
-----the-bastion-3.16.99-rc1-----
▶ adding personal access to a server on your account

Testing connection to sysadmin@192.168.0.35, please wait...
Warning: Permanently added '[192.168.0.35]:60222' (ED25519) to the list of known hosts.

Access to sysadmin@192.168.0.35:60222 was added to account bastion
-----</selfAddPersonalAccess>-----
bastion@TheBastion(master)> |

```

Connexion au client

```
ssh sysadmin@192.168.0.35 -p 60222
```

```

bastion@TheBastion(master)> ssh sysadmin@192.168.0.35 -p 60222
Welcome to TheBastion, bastion, your last login was 00:00:15 ago (mar. 2024-07-30 23:07:46 CEST) from 192.168.0.16(192.168.0.16)

192.168.0.16:58719 => bastion@192.168.0.49:22 => sysadmin@192.168.0.35:60222 ...
allowed ... log on(/home/bastion/ttyrec/192.168.0.35/2024-07-30.23-08-02.182986.c0bbfb8c0a84.bastion.sysadmin.192.168.0.35.60222.ttyrec)

will try the following accesses you have:
- personal access with RSA-4096 key SHA256:/PKa6/OXFtLwivNOKrSTJSHDAks1dOKsTQbTKhN5bJM [2024/07/30]

Connecting...
The authenticity of host '[192.168.0.35]:60222 ([192.168.0.35]:60222)' can't be established.
ED25519 key fingerprint is SHA256:v+Edbxnh0eWli7eJoX0kedhsg/Gftkm/X4RzQtWtHJH4.
No matching host key fingerprint found in DNS.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.0.35]:60222' (ED25519) to the list of known hosts.
Linux SSH1 6.1.0-23-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.99-1 (2024-07-15) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jul 30 22:55:50 2024 from 192.168.0.16
sysadmin@SSH1:~$ |

```

Utilisation de ttyrec

Cette outils va vous permettre d'enregistrer les sessions ssh effectués et de la regarder

Récupération de l'id de session ssh

```
selfListSessions --type ssh --detailed
```

Lancement de l'enregistrement de la session

```
selfPlaySession --id [id-de-votre-session]
```

```

bastion@TheBastion(master)> selfPlaySession --id c0bbfb8c0a84
Bastion the-bastion-3.16.99-rc1
▶ replay a past session

ID: c0bbfb8c0a84
Started: 2024/07/30 23:08:02
Ended: 2024/07/30 23:09:05
Duration: 0d+00:01:03.306576
Type: ssh
From: 192.168.0.16:58719 (192.168.0.16)
Via: bastion@192.168.0.49:22
To: sysadmin@192.168.0.35:60222 (192.168.0.35)
RetCode: 32512

Press '+' to play faster
Press '-' to play slower
Press '1' to restore normal playing speed

When you're ready to replay session c0bbfb8c0a84, press ENTER.
Starting from the next line, the Total Recall begins. Press CTRL+C to jolt awake.
The authenticity of host '[192.168.0.35]:60222 ([192.168.0.35]:60222)' can't be established
ED25519 key fingerprint is SHA256:v+Edbxnh0eWLi7eJoX0kedhsg/GFtkm/X4RzQtwHJH4.
No matching host key fingerprint found in DNS.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.0.35]:60222' (ED25519) to the list of known hosts.
Linux SSH1 6.1.0-23-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.99-1 (2024-07-15) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jul 30 22:55:50 2024 from 192.168.0.16
sysadmin@SSH1:~$ voila pour l'installation et la configuration d'un client
-bash: voila : commande introuvable
sysadmin@SSH1:~$ exit
déconnexion
Connection to 192.168.0.35 closed.

</selfPlaySession>
bastion@TheBastion(master)> |

```

Utilisateur et groupe

Lors de la création d'utilisateur ou de groupe, nous pouvons choisir d'utiliser une clé publique pour tout le groupe et d'en avoir pour chaque utilisateur

Création d'un groupe


```
groupCreate --group Tech --owner Test --encrypted --algo Ed25519
```

Création d'un compte

```
account Create --account Test --uid-auto --no-key
```

```
accountCreate --account Test --uid-auto --public-key "ssh-ed25519  
AAAAC3NzaC1lZDI1NTE5AAAAILkyp9jeTMvTv378WQUST9tJSZt3qAd0hqjFTn6p0sku SSH2"
```

Suivant ce que vous avez choisi vous pouvez récupérer la clé publique de votre utilisateur ou de votre groupe et l'ajouter sur la machine sur laquelle vous souhaitez vous connecter

Maintenant, nous pouvons enregistrer la connexion dans the bastion

```
`selfAddPersonalAccess --host 192.168.0.35 --port 60222 --user Test
```

Pour aller plus loin

Il y a une grosse partie d'hardening de the bastion avec du MFA, chiffrement, PGP, Remote Backup.

Il est possible de mettre en place une connexion avec un mot de passe généré et stocké par the bastion si besoin.

Webographie

Lien de la documentation officiel de the bastion

<https://ovh.github.io/the-bastion/>