LAPP
Laboratoire d'Annecy-le-Vieux
de Physique des Particules

Bastion d'administration

22 Juin 2026

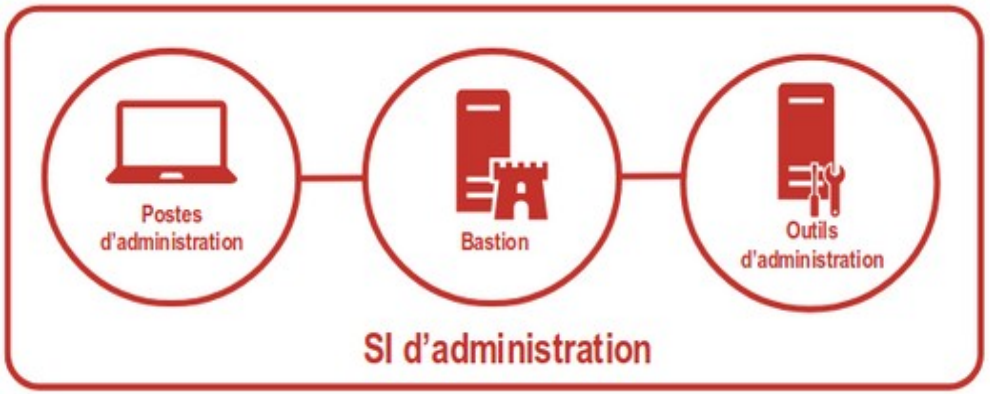
Julia Rojkovska

cnrs
UNIVERSITÉ SAVOIE MONT BLANC

Introduction

Les bastions sont un ensemble de machines utilisées comme **point d'entrée unique** par les équipes opérationnelles (telles que les administrateurs système, les développeurs, les administrateurs de bases de données, etc.) pour **se connecter en toute sécurité à des appareils** (serveurs, machines virtuelles, instances cloud, équipements réseau, etc.), généralement à l'aide du protocole **SSH**.

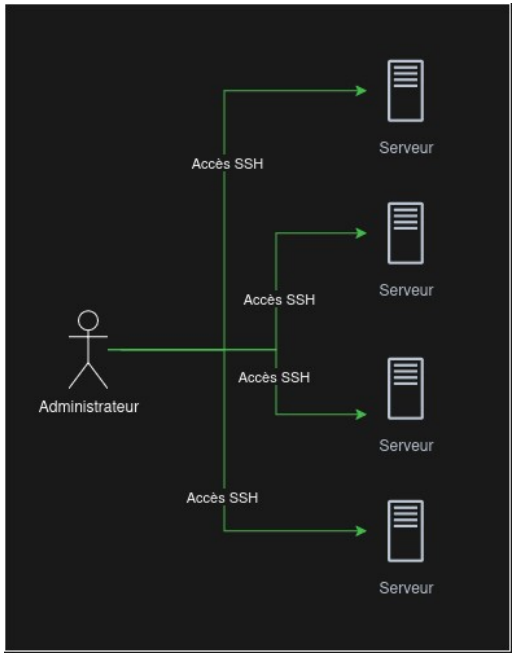
Le bastion fournit des mécanismes d'authentification, d'autorisation, de traçabilité pour l'ensemble de l'infrastructure.



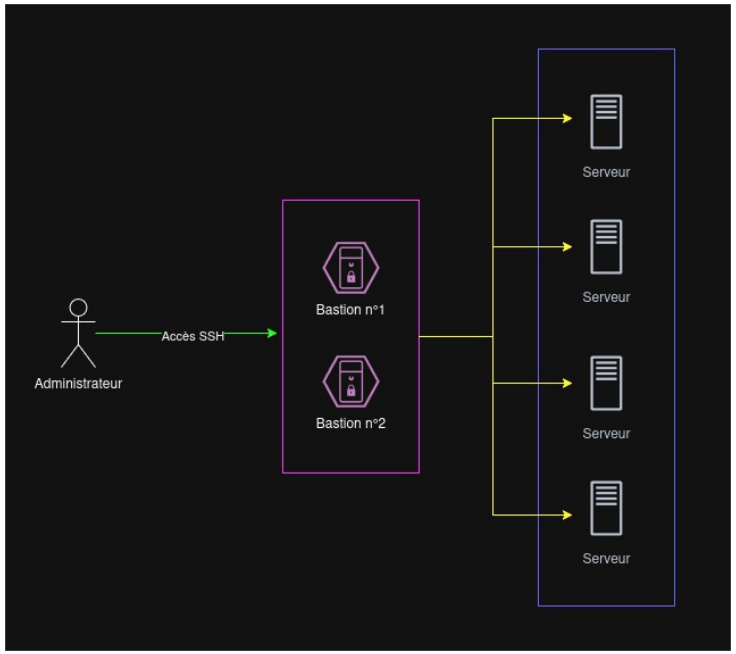
Contexte

- Actuellement, la plupart des accès SSH permettant l'administration de serveurs est disponible directement depuis un poste utilisateur.

- L'objectif est de revoir l'architecture interne de gérer les comptes utilisateurs de manière granulaire ainsi que de tracer et enregistrer toutes actions.



devient



Sélection d’une solution - 1

L’objectif est de comparer différentes solutions en se basant sur plusieurs critères :

- Open-source
- SSH en ligne de commande (RDP facultatif)
- Possibilité de mettre en place du 2FA
- Prise en charge Yubikey
- Enregistrement des sessions

Solutions possibles : Teleport, Warpgate, TheBastion, Guacamole

Sélection d'une solution - 2

Apache Guacamole :

- Application web développée en Java, sortie en 2010
- Accès aux serveurs uniquement via une interface graphique

Warpgate :

- Développé en rust
- Unique binaire agissant comme un bastion acceptant les connections SSH, HTTPS, MySQL et PostgreSQL

Teleport :

- Unique binaire développé en Go
- Gère les accès SSH, RDP, bases de données et Kubernetes
- Il comporte une version payante et gratuite

TheBastion :

- Développé en Perl par OVH
- Unique binaire publié en open-source en 2020, après un certain temps d'utilisation en interne
- Prends en charge SSH, Proxy HTTP, SFTP, RSYNC, SCP et les yubikeys

Sélection d’une solution - 3

La solution sélectionnée est **TheBastion**.

Comparée aux solutions, elle a l’avantage d’être :

- en ligne de commande (contrairement à Guacamole)
- entièrement open-source (contrairement à Teleport qui limite ses fonctionnalités)
- et de prendre en charge les yubikeys (contrairement à Warpgate)

TheBastion d'OVH - Présentation

Fonctionnalités principales :

- Gestion granulaire des droits par groupes, et des utilisateurs
- Enregistrement des sessions (format ttyrec) et journalisation
- Prise en charge SFTP, SCP, RSYNC et proxy HTTP
- Support MFA/TOTP et clés PIV (Yubikey)
- Haute-disponibilité
- Hardening system (SELinux, chiffrement /home, chiffrement des backups et sessions...)

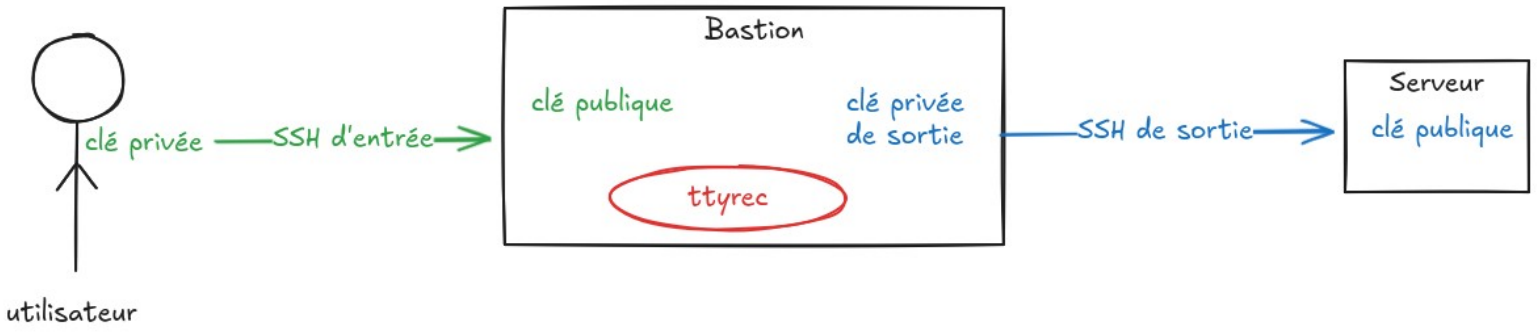
TheBastion - Connexion

Chaque utilisateur fournit sa clé publique afin de se connecter au bastion.

La connexion à un autre serveur distant utilise **une clé différente**: une clé personnelle associée à son utilisateur local sur le bastion ou celle du groupe auquel il appartient.

L'utilisateur se connecte avec le compte local **must** ayant des droits roots. Il n'y aura **plus d'accès au compte root** en direct.

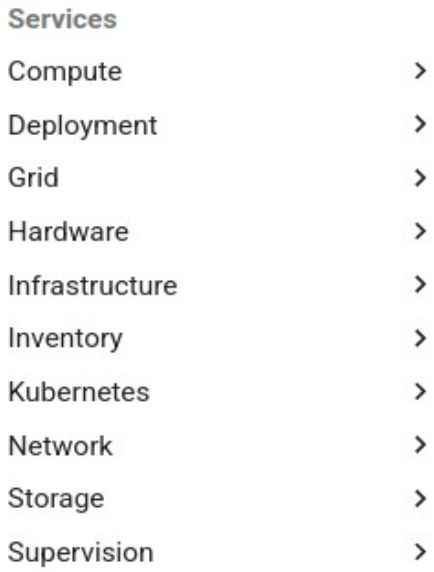
Chaque session est **enregistrée** et accessible par l'administrateur ou l'utilisateur lui-même.



TheBastion - Groupes

Pour rendre la configuration plus granulaire et structurée, différents groupes ont été créés (basés sur les services définis dans les documentations internes pour être cohérent).

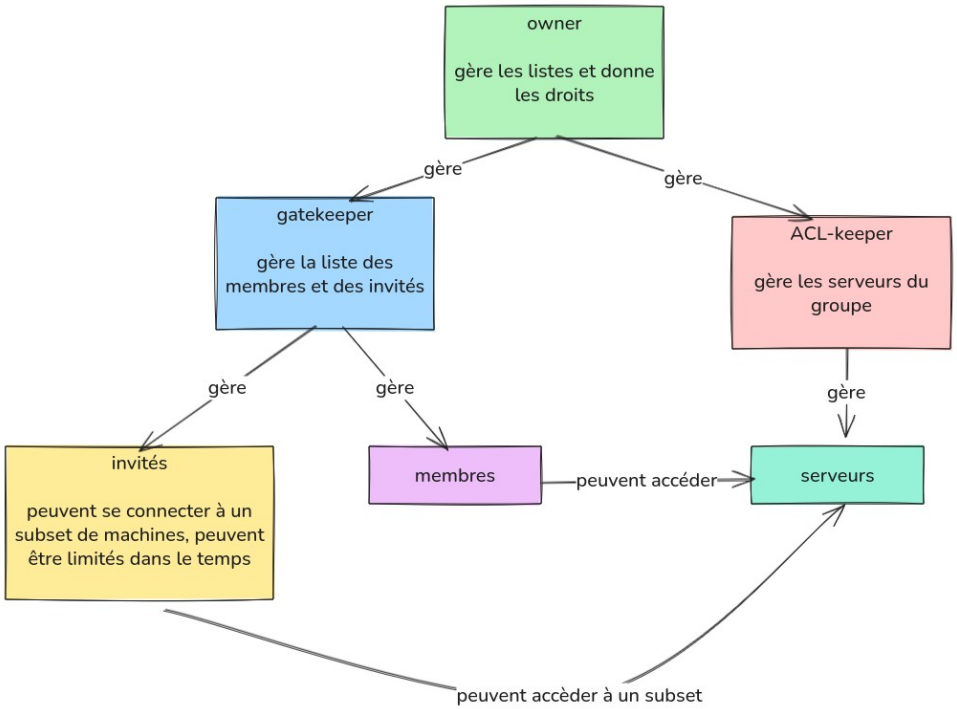
Au quotidien, le système de groupe restera transparent pour un utilisateur.




```
▶ group list

          compute Owner GateKeeper ACLKeeper Member      -
       deployment Owner GateKeeper ACLKeeper Member      -
             grid Owner GateKeeper ACLKeeper Member      -
         hardware Owner GateKeeper ACLKeeper Member      -
   infrastructure Owner GateKeeper ACLKeeper Member      -
        inventory Owner GateKeeper ACLKeeper Member      -
       kubernetes Owner GateKeeper ACLKeeper Member      -
          network Owner GateKeeper ACLKeeper Member      -
          storage Owner GateKeeper ACLKeeper Member      -
      supervision Owner GateKeeper ACLKeeper Member      -
```

TheBastion – Rôles



3 rôles sont disponibles:

owner : permet de modifier le groupe (suppression, ajout de clé ou de mot de passe) et de modifier les rôles des utilisateurs

gatekeeper : permet d'ajouter/supprimer l'accès à des utilisateurs et des invités

aclkeeper : permet d'ajouter/supprimer l'association des serveurs au groupe

Les utilisateurs peuvent avoir plusieurs rôles à la fois au sein d'un groupe.

TheBastion – Rôle invité

Il est possible de créer un compte invité **au sein d'un groupe** qui accordera un accès temporaire à une liste de serveurs pré-définis.

Également, un **compte global** au bastion peut être créé avec une utilisation temporaire.

Dans les 2 cas il faudra créer un compte au sein du bastion. Puis, soit:

- lui attribuer un rôle **guest** au sein d'un groupe (utile pour accorder un accès spécifique à un serveur).

- le traiter comme un utilisateur lambda avec un **timeout défini** et l'ajouter dans les groupes pertinents.

Cas d'usage chez MUST : création de compte dans le cadre d'un **stage** ou administration à distance par un **prestataire**

TheBastion - Utilisation

L’accès au bastion s’établit uniquement en ligne de commande.

Il est possible de faire un alias :

```
> alias bssh='ssh -t NOM_UTILISATEUR@SERVEUR_BASTION.in2p3.fr --'
```

Et d’utiliser cette commande pour tout accès :

```
> bssh UTILISATEUR_PAR_DEFAUT@SERVEUR_1.in2p3.fr
```

Démonstration par OVH : https://asciinema.org/a/369555?autoplay=1

TheBastion - Automatisation

Pour éviter un grand nombre d'actions manuelles, des scripts sont en place:

- **Ajout des serveurs depuis Foreman**

Ce script utilise l'API de foreman pour récupérer tous les hôtes en fonction de leur rôle. Grâce à un mapping prédéterminé, ils sont ajoutés dans le bastion dans le groupe adéquat.

> python3 add_host_from_foremann.py

- **Création de compte administrateurs**

Ce script ajoute récupère automatiquement les groupes existants, ajoute l'utilisateur et l'associe en tant que owner, aclkeeper, gatekeeper à chaque groupe.

> python3 create_user_bastion.py <nom_utilisateur> '<clé_publique>'

Problématiques

L’installation et la prise en main de TheBastion se fait de manière simple, rapide et intuitive.

Cependant quelques problématiques ont été rencontrées :

- Fonctionne en IPv6 ou IPv4 seulement
- L’utilisation des yubikeys est contraignante (PIN à taper pour chaque connexion), la solution d’une clé SSH id25519-sk est envisageable
- Proxy HTTP limité, notamment dans le cadre de l’utilisation de Kubernetes (authentification par certificat)

Conclusion

Actuellement :

- Pré-production depuis plusieurs mois, utilisé quotidiennement
- Haute-disponibilité sur 2 machines virtuelles

Actions à réaliser :

- Hébergement sur 2 serveurs physiques
- Restriction de l'administration des serveurs
- Centralisation des logs et des sauvegardes