Infrastructure nécessaire à un hébergement sur site

Entr'ouvert assure l'installation et la maintenance de la partie applicative. Le reste de l'infrastructure (stockage, sauvegardes, sécurisation réseau, etc) est sous la responsabilité de l'hébergeur.

Les applicatifs Publik fonctionnent sur un serveur Debian. Pour le stockage, Publik a besoin d'accéder à :

- des bases PostgreSQL ; version 9.4 ou supérieure
- un système de fichier monté en NFSv4

Serveur applicatif

Le serveur applicatif qui va contenir les logiciels composant Publik doit avoir les caractéristiques minimales suivantes :

- processeur x86-64 4 coeurs
- 16Go de RAM
- 20 Go d'espace disque

Cela peut tout à fait être une machine virtuelle, nous conseillons même cette approche qui permet d'augmenter les capacités de façon souple.

Ce serveur est infogéré par Entr'ouvert. Cependant, sauvegarde et restauration (PRA) restent à la charge de l'hébergeur.

Un système Debian 9.x minimal doit être installé, en version amd64. Le seul logiciel nécessaire par défaut est le serveur ssh (voir plus bas). Pour simplifier l'installation, pas de partitionnement : une seule partition racine / contiendra système et données.

NB : deux machines de ce type doivent être mise à disposition, production et pré-production (nommée aussi "recette"), les plus identiques possibles, principalement en terme d'environnement réseau.

Composants de stockage

Publik gère des données dans des bases PostgreSQL et dans des répertoires sur le système de fichier. Le serveur applicatif doit donc avoir accès à :

- un SGBD PostgreSQL version 9.4 ou supérieure
- un espace disque, qui sera monté en NFSv4

Ces composants sont à la charge de l'hébergeur.

Infrastructure réseau

Idéalement, le serveur d'application est placé derrière un mandataire inverse (reverse-proxy frontal). Ce dernier :

- assure la terminaison SSL ;
- doit être le plus transparent possible, principalement au niveau des headers des requêtes.

Par ailleurs, le serveur d'application doit pouvoir :

- accéder directement et sans filtrage à tout Internet pour ce qui concerne DNS (53/udp+tcp) et Web (443/tcp et 80/tcp)
- envoyer des mails au nom des clients, via le MTA de l'hébergeur (relais SMTP) ou directement (déconseillé)
- accéder au LDAP de Entr'ouvert (ldap.entrouvert.org, port tcp/389 pour les accès support/maintenance)
- accéder aux LDAP des collectivités le cas échéant (389/tcp ou 636/tcp)
- et comme vu plus haut, accéder aux services PostgreSQL et NFS mis à sa disposition

Attention : les composants Publik installés sur le serveur application doivent se parler "entre eux", car ils échangent via webservices. Puisque la terminaison SSL se fait sur reverse proxy frontal, toutes les communications repasseront par ce reverse proxy.

Un domaine DNS sera dédié, dont le nom et tous les sous-domaines pointerons vers le reverse-proxy.

Note : si l'hébergeur ne dispose pas d'un reverse-proxy, le serveur d'application Publik devra gérer la terminaison SSL : les certificats seront à fournir à Entr'ouvert et à renouveler avant échéance.

Accès support/maintenance via SSH

Afin d'assurer maintenance et support de Publik, Entr'ouvert doit avoir un accès au serveur via le protocole SSH.

- il doit s'agir d'accès SSH, les outils de gestion d'Entr'ouvert ne supportant que ce protocole.
- Entr'ouvert pourra fournir une adresse IP source qui sera la seule à accéder aux SSH (vpn.entrouvert.org)
- il peut aussi être envisagé de travailler via un "bastion SSH", ie un rebond SSH, porte d'accès unique chez l'hébergeur
- dans tous les cas, l'accès devra suivre les possibilités du protocole SSH. En d'autres termes, un accès via une surcouche de type VPN est exclu
- l'accès devra se faire avec utilisation de clés SSH, sans mot de passe ou de code spécifique à saisir
- les accès se feront sur des comptes individuels, chacun disposant ensuite d'un accès root (via sudo). Entr'ouvert fournira la liste de ses travailleurs concernés, avec pour chacun sa clé SSH publique.

Voir aussi SupportEtInfogerance

George Abitbol