Mise en place de pic2 : Propositions d'architecture

Version du 1er Juillet 2017, validée techniquement et moins onéreuse que la version discutée le 27 Juin

Les principes de base sont les suivants :

- **Mise en conteneurs** (Docker) des services web, afin de maintenir aisément plusieurs configurations de php et de serveurs web
- Pas d'accès ftp, mais **accès sftp systématique**, et accès ssh aux utilisateurs qui le demandent
- Installation de mysql sur un **serveur différent** des services web afin d'améliorer les performances.

Nous proposons donc de mettre en place deux serveurs, tous les deux sous Debian 9 :

1. **`pic2`** exécute exclusivement les services **`mysql`** (ou **`mariadb`**) et **`ldap.`**
   Une petite configuration devrait être suffisante, typiquement 512 Mo de RAM (à vérifier), 10 Go de disque et si possible (*non encore validé*) pas d'interface IPv4 publique (interface privée IPv4, gratuite).
   `ldap` est indispensable car les services web sont dispersés sur plusieurs conteneurs, et ils doivent avoir accès à la base de données des utilisateurs (par l'intermédiaire du module **`mpm-itk`** d'apache)
2. **`pic2s`** exécute tout le reste, à savoir tous les services qui nécessitent encore aujourd'hui une adresse publique IPv4. **`pic2s`** a donc 4 Go de mémoire, 10Go de disque système et 100 Go de disque de données, et tous les services nécessitant soit un conteneur docker, soit une IPv4, tournent sur cette machine :
   - Postfix
   - sympa
   - Services Web
   - *Eluna (supervision web, dans un conteneur si possible)*
   - Application de changement de mot de passe (à écrire)

Les conteneurs en production au début seront les suivants :

- pic-phpmyadmin
- pic-ssh
- pic-itk56s (php 5.6 pour spip 3.0)
- pic-itk56 (php 5.6 pour les autres sites web)
- pic-itk70s (php 7.0 pour spip 3.1)
- pic-itk07 (pour les autres sites web qui sont validé sous php 7.0)
- Un conteneur de reverse proxy
- Un conteneur pour l'application de mots de passe
- phpmyadmin
- *Eluna (supervision web, s'il peut fonctionner dans un conteneur)*

La situation évoluera dans le temps, on peut d'ores et déjà imaginer d'autres conteneurs :

- Conteneur wordpress
- Test d'autres configurations

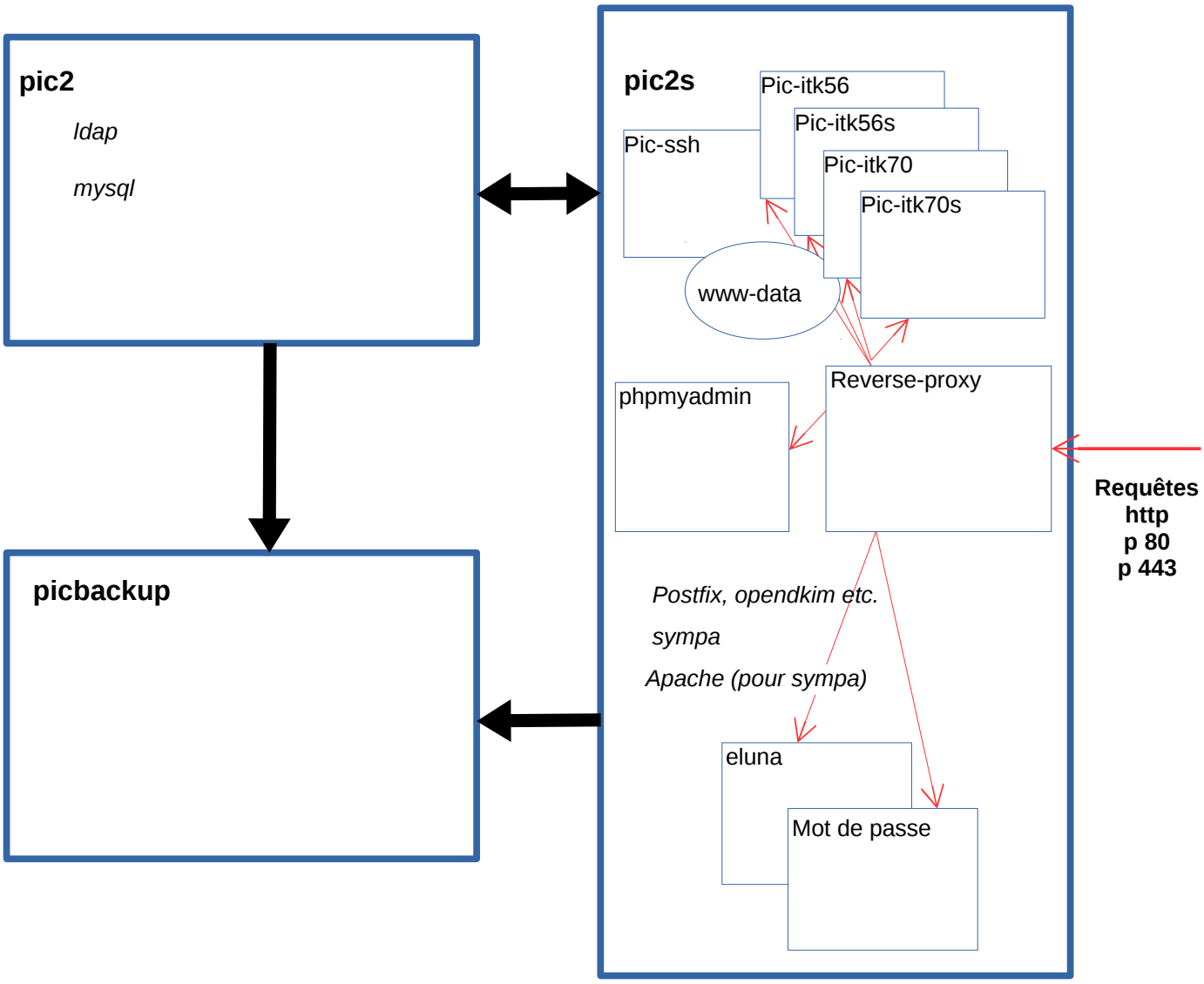
Coût de la proposition :

- **`pic2s`** = 569 c/h soit **15,00 €/mois** qui se décomposent de la manière suivante :
  - 1 cpu : 42 c/h soit **1,06 €/mois**
  - RAM 4 Go : 384 c/h soit **9,68 €/mois**
  - 1 disque de 100 Go : 100 c/h soit **2,50 €/mois**
  - 1 IPv4 : 70 c/h soit **1,76 €/mois**
- **`pic2`** = 100 c/h soit **2,27 €/mois** qui se décomposent de la manière suivante :
  - 1 cpu : 42 c/h soit **1,06 €/mois**
  - RAM 512 Mo : 48 c/h soit **1,21 €/mois**

On arrive donc à **17,28 €/mois**, soit **207 € par an** (ou encore un peu plus de 10 adhésions).

La proposition en graphique :

- Pic2 et pic2s communiquent en IP ou IPv6
- Les services web sont embarqués dans quatre conteneurs (pic-itkxx)
- ssh (et sftp) est également dans un conteneur (pic-ssh), ces 5 conteneurs partagent le volume de data
- Le reverse proxy route les requêtes web en provenance d'internet vers le bon container (ie vers le bon port réseau)
- pic2 et pic2s sont sauvegardés par picbackup
- postfix, sympa etc. tournent sur pic2s, mysql et ldap sur pic2



Propositions pour une migration sereine

La migration proposée ici consiste à recopier sur **`pic2s`** la configuration actuelle de **`pic`**, afin de simplifier le processus de migration et permettre d'arrêter rapidement **`pic`**.

Les services seraient toutefois dégradés jusqu'à la migration définitive qui devrait se faire rapidement :

- pas de **`phpmyadmin`**
- pas d'accès **`ftp/sftp/ssh`**
- pas de sauvegarde.

La migration pourrait se dérouler en 5 phases :

Phase I *- Création de deux conteneurs supplémentaires*

Création de deux conteneurs (appelés **`vpic-xxx`**, v comme vieux)

- **`vpic-mysql`** pour déposer les bases de données des sites actuels
- **`vpic-itk56`** pour déposer les fichiers des sites web ainsi que les configurations apache

NOTE – L'objectif étant de reprendre la configuration actuelle de tous les sites du pic sans rien modifier, on fera communiquer les deux conteneurs par le biais du socket unix **`mysql.`**

Courant été 2017

Phase II *– Copie des fichiers par* ***`rsync`***

Envoi (par utilisation de **`rsync`**) des données (fichiers + bd) sur **`pic2s`**

- Chargement des bases de données dans le conteneur **`vpic-mysql`**
- Recopie du fichier **`/etc/passwd`** dans le conteneur **`vpic-itk56`**
- Configuration du reverse-proxy
- Cela nécessite pour plus de fiabilité l'écriture de scripts afin d'automatiser la procédure
- Génération d'un fichier **`/etc/hosts`** que les admins pourront intégrer à leur poste de travail pour tester.
- Passage (par **`rsync`** également) des fichiers relatifs à **`sympa`** et de la B.D. associée
- Introduction temporaire de nouveaux robots virtuels type pic2.le-pic.org
- Installation de sympa, et (espérons-le!) lancement de la procédure d'upgrade. Sympa passe de 6.1.23 à 6.2.16 (dernière version actuellement)
- Modification du DNS afin que le mail @pic2s.le-pic.org soit renvoyé sur **`pic2s`**

Juste après la phase I

Phase III *– Test des sites migrés et de sympa*

- Chacun des admins (ou éventuellement d'autres testeurs) teste chaque site afin de vérifier que tout fonctionne correctement.
- Les testeurs testent également l'interface web de **`sympa`** et font vivre la liste de tests de **`sympa`**

Septembre – Octobre

Phase IV *– Migration définitive des fichiers*

- Un Mercredi soir :
  - arrêt de tous les services de **`pic`**
  - Changement du DNS, **`pic.le-pic.org`** pointera sur l'IPv4 et v6 de pic2s
  - Nouvelle exécution des scripts de **`rsync`** de la phase I et nouveau chargement de la B.D. rsync ne copiera que les fichiers ayant déjà changé depuis la dernière fois, donc cela devrait être rapide.
- Le vendredi soir suivant :
- Arrêt de **`pic`** (et suppression de **`l'IPv4`** pour économiser des sous)
  - Configuration définitive de postfix et sympa, mise en place des conteneurs sur pic2s
  - Suppression des modifications apportées au fichiers /etc/hosts des admins et à nouveau test et retest

1er Novembre → 3 Novembre 2017

Phase V *– Migration des sites sur les conteneurs définitifs*

- Site par site, migrer les fichiers, la B.D. etc. sur leurs conteneurs définitifs. Cela suppose pour les sites que nous ne maîtrisons pas un contact avec les utilisateurs, pour modifier la configuration d'accès à la base de données. Les utilisateurs utiliseront l'application de mot de passe pour se faire un mot de passe **`sftp`** ou **`ssh`**
- On s'occupera en premier des sites de velobs et d'arto qui ont un accès **`ssh`**

Du 1er Novembre au 30 Novembre

Communication vers les utilisateurs

Elle reste à définir , mais cet aspect est très important : lors de la phase V ils devront au moins modifier leurs paramètres d'accès à la base de données, nous avons donc besoin de leur concours. Pour ce qui est du DNS, les utilisateurs qui gèrent eux-mêmes le DNS peuvent avoir des surprises dès la phase IV si malgré nos conseils ils ont faire pointer une adresse IP et pas un CNAME sur pic.le-pic.org. Ils doivent donc être prévenus.

Ce qu'il reste à faire avant la migration

- Finir l'installation des conteneurs et la configuration de **`pic2s`** et de **`pic2`**
- Mettre en place le reverse proxy
- Écrire l'application web de gestion de mots de passe
- Finir le portage de picgs

Emmanuel et le groupe des admins

26 Juin 2017