Bilan technique Picasoft A20

picasoft

03 février 2020

Table des matières

1 Introduction

Ce document présente l'activité de l'association Picasoft sur le semestre d'automne 2020 (du 1er Août au 31 janvier). Il a pour but de donner un aperçu complet des actions menées par l'association et de son état courant.

Ce bilan ne détaille pas les tâches "classiques", à savoir :

— Les mises à jour des services (ou ajouts de fonctionnalités...)
— Les migrations mineures (passage d'une base de donnée à une autre...)
— Les opérations de maintenance (renouveller des clés...)

2 Guides pour l'équipe technique

Le wiki reflète à présent l'ensemble de ce qui tourne en production. Mais même avec une description de l'infrastructure, il est difficile pour une nouvelle personne de savoir ce qu'il faut faire pour veiller à son bon fonctionnement.

Des tutoriels ont été rédigés pour aider les membres à vérifier que tout fonctionne bien, prévenir les problèmes avant qu'ils ne soient visibles et garder les systèmes à jour.

Un résumé technique, un guide d'arrivée et un guide des tâches d'administration système synthétise l'accès aux informations du wiki technique.

3 Administration système

3.1 Monitoring

Ce semestre a été l'occasion de revoir le fonctionnement de base de tout notre système de monitoring.

Historiquement Picasoft stockait les métriques des services (nombre de pads...) dans une base InfluxDB en s'appuyant sur un petit bot en Python. Les métriques des machines étaient, elles, récoltées en utilisant un serveur Prometheus et des `node-exporters`. Les deux bases étaient ensuite consultées en utilisant Grafana.

Pour la nouvelle stack, nous avons mis en place Victoria Metrics pour remplacer InfluxDB et Prometheus. Cette solution est beaucoup plus performante que InfluxDB, et complètement compatible avec Prometheus. Grafana est toujours utilisé pour consulter les métriques.

Une vue d'ensemble de cette stack se trouve sur le wiki.

Les métriques de Wekan, de CodiMD et de Proxmox ont été ajoutées et sont visibles via un dashboard dédié.

3.2 Suppression de la chaîne d'intégration

La chaîne d'intégration est un système mis en place par la TX sécurité en automne 2018. Son objectif était d'automatiser la construction, l'analyse de sécurité et le déploiement des conteneurs Docker de nos services à chaque push sur un dépôt Gitlab dédié (`dockerfiles`).

Une première simplification a supprimé l'étape de déploiement, qui générait trop de frustrations et dépossédait les membres de l'équipe technique d'une vraie capacité de comprendre ce qu'il se passe et de résoudre les problèmes.

Finalement, l'étape qui restait (construction et analyse des images) a été jugée trop complexe, trop opaque et avec beaucoup trop de petits bugs dévitalisants.

La chaîne d'intégration a donc été totalement supprimée au profit d'opérations manuelles.

Elle aura eu pour point positif d'uniformiser la structure du dépôt et de systématiser le versionnage des fichiers nécessaires à lancer n'importe lequel de nos services.

4 Sécurité

4.1 Mises à jour automatiques

Les failles de sécurité sont un risque majeur pour l'infrastructure. Une faille connue mais non patchée est dangereuse : dès qu'elle est rendue publique, des robots commencent à tenter de les exploiter sur les machines connectées à Internet.

Nos machines tournent sur Debian, une distribution Linux pensée pour la stabilité. Les mises à jour sont donc relativement rares, à l'exception de celles qui concernent la sécurité, distribuées via un canal dédié.

Nos machines reçoivent et appliquent automatiquement ces mises à jour, une fois par jour. Le risque d'instabilité est donc très légèrement accru pour un important bénéfice.

4.2 Pare-feu

Un pare-feu simple, n'autorisant l'accès qu'aux ports en liste blanche (exemple : DNS, ports du web), a été généralisé à l'ensemble des machines.

L'accès aux métriques des machines n'est autorisé qu'à la machine de `monitoring`.

4.3 TLS

L'accès à l'ensemble des services de Picasoft est maintenant sécurisé par TLS. Le dernier manquant était LDAP.

Le renouvellement des certificats TLS des services non-web (Mumble, mail, LDAP) est maintenant automatique.

4.4 Ouverture du dépôt dockerfiles

Le dépôt `dockerfiles`, qui contient l'ensemble des fichiers utilisés pour déployer nos services, a été rendu public par souci d'essaimage et de transparence.

Cette opération révèle des informations sur nos services (images Docker utilisées, paquets installés, configuration, etc) qui pourraient servir à un attaquant.

Ceci étant :
- La sécurité par l'obscurité n'est clairement pas plus efficace
- Le caractère public du dépôt incite à faire attention et être rigoureux

5 Infrastructure

5.1 Nouvelle machine virtuelle

Une nouvelle machine, `media`, a été mise en place pour accueillir les services potentiellement consommateurs d'espace disque. Pour le moment, elle héberge Peertube et Lufi.

Les données sont stockées sur des disques durs, car le point de congestion le plus probable est le réseau, pas besoin de "gâcher" de la mémoire SSD.

5.2 Mise à jour des hyperviseurs

Alice et Bob, nos deux machines physiques, ont été mises à jour vers Proxmox 6, une version majeure basée sur Debian 10 et apportant de nombreuses améliorations, dont un nouveau format de backup.

5.3 Achat de disques supplémentaires

Sur Alice, les disques durs commençaient à être plein, en particulier à cause des backups des machines virtuelles hébergées sur Bob. De plus, le projet d'hébergement d'une machine virtuelle `multimedia` laissait présager un usage disque encore plus important.

Picasoft a pour ce faire acheté deux disques dur de 2To, montés en RAID1, installés sur Alice.

5.4 Projet d'achat d'une nouvelle machine

Le précédent bilan technique présentait une réflexion préliminaire sur l'achat d'une troisième machine.

Cette machine va être achetée au semestre prochain, grâce aux subventions du FSDIE obtenue ce semestre.

L'idée est de l'héberger dans le datacenter associatif de Rhizome situé dans les locaux du Centre d'Innovation de l'UTC. Les objectifs sont les suivants :

— Facilité d'intervention physique en cas de panne
— Renforcement du côté "local" de Picasoft
— Fiabilisation de l'infrastructure : en cas de panne à Toulouse, il nous reste une partie
— Échanges de sauvegardes : en l'état, si Toulouse brûle, toutes les données sont perdues

Une des idées évoquées est de rapatrier les services les plus utilisés à l'UTC sur les machines stockées à l'UTC, pour toutes les raisons évoquées ci-dessus.

Un plan d'action a été établi pour mettre en place un nouveau système de sauvegardes et de correctement les externaliser. Une fois la machine achetée, il sera rapidement mis en place.

6 Incidents

Deux incidents se sont produits ce semestre :

— Le 10 octobre 2020, lors de la mise à jour vers Proxmox 6, Alice ne redémarre pas. Un bénévole de Tetaneutral redémarre la machine physiquement, tout se passe bien.
— Le 11 novembre 2020, un bug dans Docker entraîne la suppression d'une partie des données de production. Grâce aux backups, les données sont rapidement rétablies.