Bilan technique Picasoft P20

picasoft

03 juillet 2020

Table des matières

1 Compte rendu technique P20

Ce document présente l'activité de l'association Picasoft sur le semestre de printemps 2020 (du 1er février au 31 juillet). Il a pour but de donner un aperçu des actions menées par l'équipe technique.

1.1 Encadrements de TX

1.1.1 TX Monitoring

Picasoft a co-encadré une TX visant à améliorer le système de monitoring et d'alerting de l'infrastructure, en particulier dans le but de détecter les pannes au niveau des services et des machines, et de remonter l'information à l'équipe technique.

Une solution clé en main basée sur une stack ELK a été livrée. Cette solution prend la forme d'un squelette fonctionnel mais ne produisant aucune alerte par défaut. L'équipe technique devra se charger de l'implémentation.

1.1.2 TX CHATONS

Picasoft a co-encadré une TX visant à concevoir un système de référencement et de recherche des services proposés par les différents membres du CHATONS. Nous avons mis à disposition une machine virtuelle aux étudiant.e.s. Ce système a été livré sous forme de preuve de concept, où chaque CHATONS héberge un fichier JSON décrivant ses services, et où un système agrège régulièrement les données pour alimenter un système d'affichage et de recherche.

1.2 Services

1.2.1 Nouveautés

Mumble Un serveur Mumble a été hébergé sur une machine virtuelle tournant chez l'hébergeur Gandi. Cette machine virtuelle est assez différente du reste de notre infrastructure : Docker n'est pas utilisé, et ne tourne pas sur une machine physique qui nous appartient. EN revanche, des discussions sont en cours pour rapatrier ce service sur nos machines.

Instance hebdomadaire d'Etherpad Une nouvelle instance d'Etherpad a été déployée, avec une durée de rétention des pads plus faible que l'instance

principale (deux semaines). Les deux instances renvoient sur un portail permettant de sélectionner l'instance sur laquelle créer le pad.

L'instance bi-hebdomadaire est référencée sur entraide.chatons.org et absorbe la plupart de la charge engendrée par la crise sanitaire.

Plume Un travail a été réalisé pour préparer le déploiement de Plume, un logiciel de blogging fédéré. La mise en production a été réalisée. (backups, mise à jour, initialisation...).

1.2.2 Maintenance

Etherpad Pendant la crise du COVID-19, l'instance d'Etherpad a été saturée et la base de données a explosé. Il a été décidé de bloquer la création de nouveaux pads et de privilégier l'instance hebdomadaire pour un temps.

Plus tard, l'instance classique d'Etherpad a été mise à jour et les performances de sa base de données ont été largement améliorées. La performance des backups a également été améliorée : elle ne dégrade plus du tout la performance de l'application.

Une rétention de 2 ans a été ajoutée pour éviter de conserver des pads beaucoup trop vieux et préserver les performances de l'instance.

1.3 Incidents sur l'infrastructure

Quelques incidents ont été à déplorer, la plupart sont courts et concernent une coupure de courant.

1.3.1 27/05/2020

Notre hébergeur Tetaneutral subit une coupure de courant. Lors du rétablissement du courant, Alice ne se rallume pas tandis que Bob redémarre rapidement. Le lendemain, une intervention électrique à lieu dans la salle associative TLS00 où sont hébergées nos machines, visant à remplacer des onduleurs défectueux. À cette occasion, Alice est redémarrée.

Nous pensons que le changement de ces onduleurs diminuera drastiquement le nombre de pannes à l'avenir.

1.4 Wiki

Le Wiki a été partiellement ré-organisé pour automatiser la génération d'index (barre latérale). Cette génération automatique permet de référencer l'ensemble des pages et de limiter les pages orphelines.

De plus, les catégories ont été remaniées pour faciliter la navigation et un guide d'utilisation du Wiki a été rédigé.

1.5 CI

La migration vers l'utilisation de la chaîne d'intégration se poursuit : elle a pour objectif d'uniformiser la construction des nos images Docker et d'obliger l'exécution d'analyses de sécurité avant la mise en production.

Les fichiers de configuration sont également versionnés sur le dépôt concerné, ce qui permet de démarrer une nouvelle instance de n'importe lequel de nos services sur n'importe quelle machine virtuelle, pourvu que l'on ait accès au dépôt. La reproductibilité des services est améliorée en ce sens.

De plus, ce système permet de revenir très simplement à une version antérieure en cas de problème.

De manière générale, les bonnes pratiques au niveau de la création et du lancement des images Docker sont de plus en plus respectées : séparation des réseaux, utilisation des volumes Docker, utilisateur non-privilégié...

À terme, ce dépôt pourra être ouvert pour servir à l'ensemble de la communauté et par souci de transparence : c'est d'ailleurs son but initial.

1.6 Infra

1.6.1 Mise à jour

L'ensemble des machines virtuelles a été mise à jour vers Debian 10.

1.6.2 Mémoire

Le partitionnement des machines virtuelles a été entièrement revu, pour séparer les données issues de Docker des données systèmes. Les backups sont également gérés dans une partition à part. Ce système permet d'utiliser les disques durs pour les backups, plus lents, et les SSD pour les services critiques. Aussi, l'explosion de la mémoire utilisée par un service Docker n'impacte pas le reste du système.

1.6.3 Métrologie

Un système Prometheus/Grafana a été mis en place sur la plupart des machines virtuelles pour suivre l'évolution de la mémoire utilisée, la bande passante utilisée ou la charge du processeur. Ces métriques ne sont pas associées à un système d'alertes, mais permettent néanmoins de mieux suivre les pics de consommation éventuels.

1.6.4 Backups

Les backups des machines virtuelles ont été revus afin de :

— Garantir qu'il existe toujours un backup des machines virtuelles sur une autre machine physique
— Diminuer la taille nécessaire pour réaliser l'ensemble des backups

Les backups des services ont été améliorés (plus rapides et rotation plus fiable).

1.6.5 Sécurité

Un fail2ban a été mis en place pour les connexions SSH, suite à des tentatives de bruteforce. Même si ces tentatives n'ont aucune chance d'aboutir, il est préférable de les bloquer en amont.

1.6.6 Rhizome

Picasoft héberge une instance d'InfluxDB et un compte Grafana pour permettre à Rhizome de gérer ses métriques systèmes en dehors de son infrastructure, afin de pouvoir notamment détecter les pannes.

1.7 Réflexions autour d'une troisième machine

Il apparaît très souhaitable d'acheter une troisième machine physique pour compléter notre infrastructure, afin de palier à une éventuelle panne complète de TLS00. Cette machine pourrait héberger une copie des bases de données de nos services critiques (Mattermost et Etherpad), qui sont de plus en plus utilisés par des personnes extérieures à l'UTC.

1.8 Réflexions autour d'une VM supplémentaire

Nous avons loué une nouvelle IP à Tetaneutral, éventuellement dans le but d'ouvrir une nouvelle VM dédiée aux médias (PeerTube, Funkwhale, etc...).

Tous les services multimédias ayant en commun une grande demande en stockage, il sera sans doute souhaitable d'acheter un nouveau disque dur pour nos machines physiques.

1.9 Coût d'entrée

Le problème de la désirabilité et du coût d'entrée de l'équipe technique n'a toujours pas été résolu : la plupart des tâches envisagées pour ce semestre n'ont pas été menées à leur terme.