Picasoft - Bilan Technique

Rémy Huet

19 juin 2019

Services

Maintenance

- Mises à jour régulières de Mattermost, ajout de Plugins
- Mise à jour d'etherpad, introduction d'un nouveau thème, ajout de fonctionnalités (tableaux).
- Maintient et mise à jour du Wekan.
- Accès au Wiki par le LDAP
- Support de la syntaxe Markdown pour le Wiki

Mise en place de nouveaux services

TX Service P19

- Script de suppression automatique des vieux kanban
- Mise en place d'un service de formulaires (tellform) (pas encore en production)

Services internes

Serveur LDAP

- Mise en place début A18 d'un annuaire LDAP sur `monitoring`
- Connexion sur les machines passe par ce serveur uniquement
- Gestion des clés ssh dans le serveur
- Mise en place d'un pare-feu pour restreindre les accès aux machines autorisées

Serveur LDAP

- Mise en place début A18 d'un annuaire LDAP sur `monitoring`
- Connexion sur les machines passe par ce serveur uniquement
- Gestion des clés ssh dans le serveur
- Mise en place d'un pare-feu pour restreindre les accès aux machines autorisées

- Pas de moyen de modifier son mot de passe autrement que depuis un service ou une machine pour le moment

Serveur de mails

TX mail A18

- Mise en place d'un serveur de mail sur `monitoring`
- Utilisation de ce serveur pour les services (Mattermost, Tellform)
- Connexion par le LDAP uniquement

Serveur de mails

TX mail A18

- Mise en place d'un serveur de mail sur `monitoring`
- Utilisation de ce serveur pour les services (Mattermost, Tellform)
- Connexion par le LDAP uniquement

- Pas de comptes mail personnels
- Évolution future : mise en place d'alias

Cloud interne

- Mise en place d'un Nextcloud interne
- Partage d'agenda avec différents accès
  - Public
  - Asso
  - Bureau
- Gestion de la connexion par le LDAP

Sécurité

Motivations

- Respect des données des utilisateurs

Motivations

- Respect des données des utilisateurs
- => Respect des CGU

Motivations

- Respect des données des utilisateurs
- => Respect des CGU
- => Respect de la loi

Motivations

- Respect des données des utilisateurs
- => Respect des CGU
- => Respect de la loi
- => Chaque porte ouverte représente une faille potentielle

TX Sécu A18

- Audit des images Docker utilisées par Picasoft et recommandations
- Mise en place d'une **chaîne d'intégration** pour les images :
  - Construction
  - Tests de vulnérabilités
  - Déploiement automatique

TX Sécu P19

- Correction des permissions sur l'infrastructure

TX Sécu P19

- Correction des permissions sur l'infrastructure
- Suppression de certains services

TX Sécu P19

- Correction des permissions sur l'infrastructure
- Suppression de certains services
- Étude de la restriction du démon Docker

TX Sécu P19

- Correction des permissions sur l'infrastructure
- Suppression de certains services
- Étude de la restriction du démon Docker
- Mise en place d'`auditd`

TX Sécu P19

- Correction des permissions sur l'infrastructure
- Suppression de certains services
- Étude de la restriction du démon Docker
- Mise en place d'`auditd`
- Centralisation des journaux

TX Sécu P19

- Correction des permissions sur l'infrastructure
- Suppression de certains services
- Étude de la restriction du démon Docker
- Mise en place d'`auditd`
- Centralisation des journaux
- Initiation à `tmux` demain

TX Sécu P19

- Correction des permissions sur l'infrastructure
- Suppression de certains services
- Étude de la restriction du démon Docker
- Mise en place d'`auditd`
- Centralisation des journaux
- Initiation à `tmux` demain
- Limitation des droits `root`

Gestion des identifiants

Modification du RI votée en réunion de bureau

- Suppression des identifiants du Wiki
- Mise en place d'un `pass`
  - Stockage chiffré par OpenPGP
  - Partage simplifié grâce à `git`
  - Discrimination des types de mot de passe
  - Différents niveaux d'accès possibles

Identification des points critiques

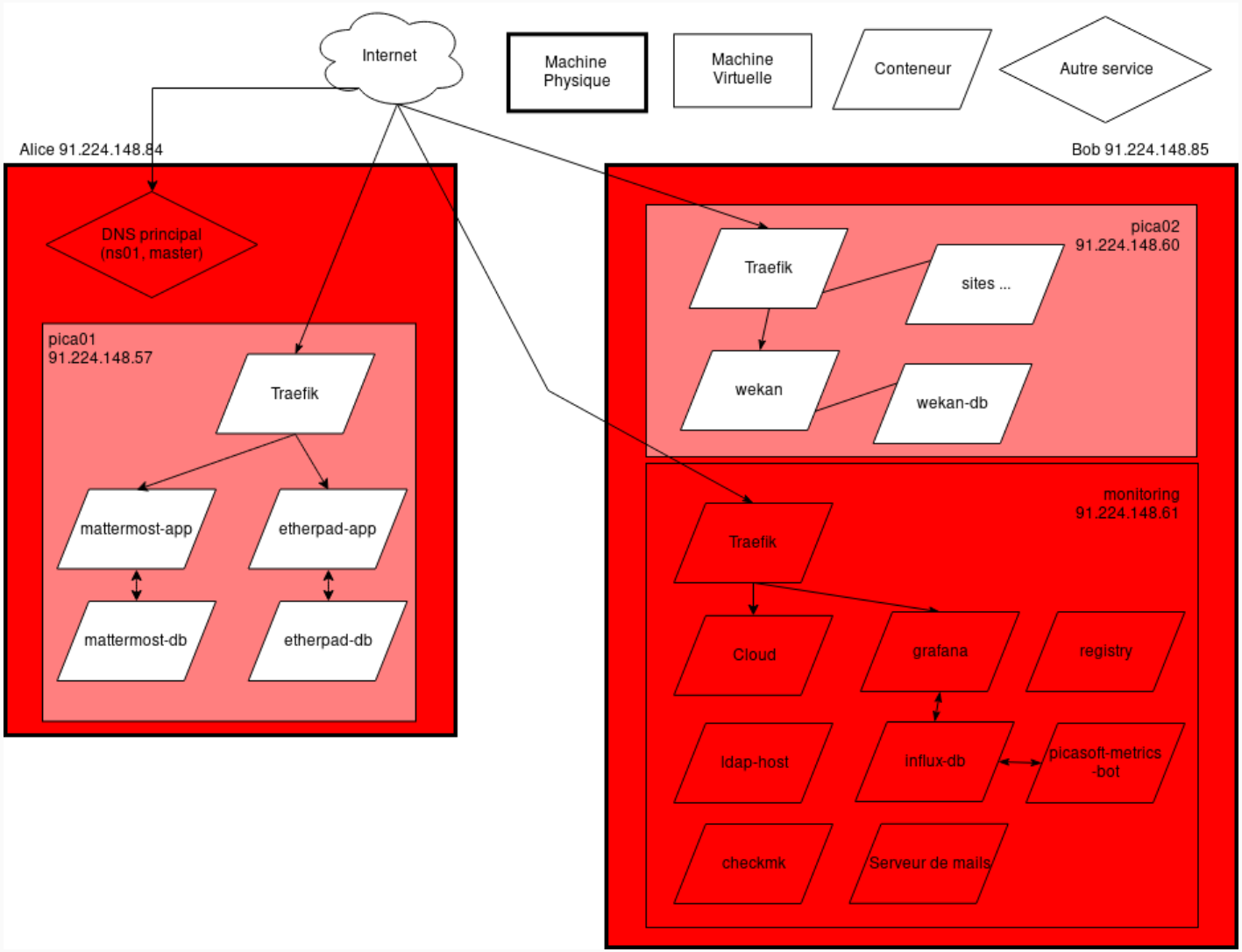

Figure 1: Infrastructure et points critiques

Gestion des accès en conséquence

- Utilisation du LDAP pour les accès aux machines. Contrôle depuis `monitoring`
- Un compte par personne avec une **date d'expiration**
- Liste des hôtes et services autorisés pour chaque personne
- Deux groupes pour les accès machines, sur recommandation de la TX sécurité P19
  - Un groupe **administrateur service** (groupe `docker`): permet l'administration totale des services
  - Un groupe **administrateur système** (groupe `sudo`): permet la gestion des machines
- Accès distribués sur besoin pour les services que chacun souhaite gérer

Incidents

17 mai 2019

Alice, 22h-1h

- Mauvaise mise à jour du noyau => Impossible de redémarrer la machine
- Rebond sur Bob pour accéder au VNC de la machine
- Reboot sur un ancien noyau
- Suppression du noyau corrompu, mise à jour, redémarrage

Conséquences

- Downtime de 3h sur les services
- Identification de points critiques

30 mai 2019

Alice, Bob, 5h-12h

- Coupure d'électricité chez Tetraneutral
- Retour à 12h et redémarrage automatique réussi des machines et services (aucune intervention manuelle)

Conséquences

- Downtime de 7h sur l'ensemble de l'infrastructure
- On sait que tout est capable de redémarrer tout seul (sauf éventuelle corruption)

16-17 juin 2019

Pica01, 22h-12h

- Lors du reboot des machines, des conteneurs de backup ont pris la place des bons conteneurs pour Etherpad
- Remise en production d'une ancienne base de donnée => disparition de certains pads / modifications
- Remise en place des bons conteneurs

Conséquences

- « Perte » de toute les modifications sur la durée de l'incident: possible de les remettre mais pas automatiquement
- Identification d'une réelle mauvaise pratique : le `restart: always`

Conclusion

Conclusion

Services

- Améliorations continue des servies déjà proposés
- Mise en place d'un nouveau service en cours
- Ajout de services internes pour simplifier la gestion

Sécurité

- Amélioration de la sécurité des données

Disponibilité

- Un bon SLA (plus de 99.5% d'uptime)