Retour d'expérience sur le déploiement des certificats Harica pour le projet PC-Scol

Gauthier Catteau

Définitions

- Harica: Hellenic Academic and Research Institutions CA
- PC-Scol: Projet Commun de scolarité.

PC-Scol

- 2 tutelles: AMUE et Asso Cocktail + co-construction avec les universités.
- Le projet PC-Scol héberge l'application de scolarité Pégase en mode SaaS pour une centaine d'établissements.
- Environ 500 instances Pégase sont déployées fin 2024 (construction, production).

Contexte

- La migration des instances sur une nouvelle infra Kubernetes est planifiée début janvier 2025.
- L'ensemble des instances utilise un certificat avec 2 wildcards dns (un pour les ressources internes et un pour les externes).
- Les certificats sont déployés par cert-manager sur Kubernetes, et avec certbot pour les VMs.
- Nous utilisons un compte eab Sectigo par cluster.
- Des instances Pégase sont déployées à la demande pour du debug.

Annonces

- Annonce début décembre 2024 de la fin de Sectigo.
- Retour pendant les JRES concernant le planning prévisionnel.
- 10 janvier fin de Sectigo.
- Migration vers Harica mars/avril 2025 (si tout se passe bien...)

Plan d'action

- Renouvellement anticipé des certificats expirants avant juillet 2025.
- Anticipation des créations, si possible, pour les nouvelles instances Pégase.
- Utilisation de Let's Encrypt pour les déploiements à la demande.

À partir du 10 janvier

- Déploiement des nouvelles instances sur la nouvelle infra avec un certificat Let's Encrypt.
- Recopie du secret kubernetes contenant le certificat de l'ancien cluster vers le nouveau.
- Utilisation d'un issuer null pour éviter que le certificat ne soit recréé.

Les grains de sable pendant la période de transition

- Les Rate limits de l'API Let's Encrypt limitent la création ou le renouvellement à 50 certificats sur 7 jours glissants par domaine.
- Les conteneurs et VM Debian 11, n'intègrent pas l'AC Harica.
- Parcoursup n'accepte pas les certificats Let's Encrypt.

Préparation de la migration et solutions temporaires

- Utilisation des certificats Let's Encrypt staging pour les tests.

- Mise à jour des OS dans les conteneurs et les VM + test.
- Génération manuelle des certificats Parcoursup avec Harica pour les instances dont le certificat a expiré entre juillet et octobre 2025.

Pendant ce temps côté Harica

- Fin juin, issue ouverte sur le github de cert-manager
- Finalement côté problème implémentation ACMEv2 côté Harica
- Ouverture de ticket chez Renater
- Fix le 30 juin, on peut commencer à migrer

Migration complète des certificats vers Harica

- Attente que tous les établissements aient déjà surmonté leurs soucis avec des certificats Harica.
- Migration mi-septembre des instances de construction.
- Migration des instances de production début octobre.

Soucis rencontrés post-migration

- Parcoursup vérifie le cn du certificat ...
  - Lors de la création du certificat avec un compte eab, Harica prend la première entrée dns du certificat par ordre alphabétique.
  - Les certificats intègrent le nom technique interne qui parfois passe avant dans l'ordre alphabétique.
  - Solution: utilisation de 2 certificats distincts.

Perte de fonctionnalités

- Il n'est plus possible d'avoir un compte eab par cluster.
- Pas de visibilité des certificats créés avec le compte eab.

Conclusions

- Toujours prévoir le pire des scénarios.
- Prendre son temps, pas de migration dans la précipitation.
- Nous ne nous en sommes pas trop mal sortis.
- Nouveau marché dans un an.

Questions ?