



Vie et mort des comptes utilisateurs

François Legrand

Rencontres de la fédération,
3/10/2017

Problématique

- Maîtriser la gestion des comptes utilisateurs

Recommandation du « GUIDE DE L'INTELLIGENCE ÉCONOMIQUE POUR LA RECHERCHE » → Tout compte devenu inutile doit être immédiatement supprimé.
http://www.cil.cnrs.fr/CIL/IMG/pdf/2012_03_15_Guide_IE_de_la_recherche_D2IE.pdf

- Sécuriser nos infrastructures

- Maîtriser la gestion de l'espace disque

Ne pas conserver les données inutiles



Méthode

- Définir une politique claire de gestion des comptes et des données
- Informer les utilisateurs
- Mettre en œuvre des outils pour appliquer cette politique



Politique de gestion des comptes

- La création des comptes (labo et mail) intervient quelques jours avant l'arrivée de la personne
- Identifiants provisoires communiqués à son responsable
- Obligation de changer le mot de passe à la première connexion
- Règles de solidité des mots de passe
(10 caractères mini)
- Vérification régulière de la solidité des mots de passe + hash fort (sha512)



Politique de gestion des comptes

- La fermeture du **compte « labo »** intervient 1 mois après le départ de la personne
- Les utilisateurs sont notifiés 1 mois avant la fermeture
- La fermeture du **compte mail** intervient 3 mois après le départ de la personne et sa destruction 1 mois après
- Les utilisateurs sont notifiés 1 mois avant la fermeture



Politique de gestion des comptes



- A la fermeture/destruction du compte mail, une redirection peut-être mise en place vers sa nouvelle adresse
- Les utilisateurs peuvent demander une prolongation de leur compte → formulaire à valider par le chef de groupe et soumis à l'approbation du directeur

Politique de gestion des données

- A la création des comptes, deux espaces « home » sont créés (linux et windows) avec 20 Go de quota (netapp)
- Les utilisateurs ont aussi accès aux espaces « data » sur les serveurs (pas de quota)
- Les données « home » sont backupées + snapshots accessibles en lecture seule



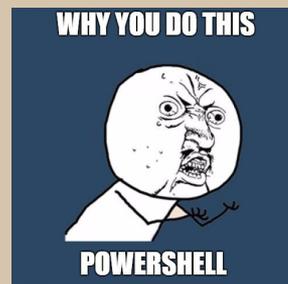
Politique de gestion des données

- Trois mois après la fermeture des comptes, les données « home » sont « archivées »
- Les utilisateurs sont notifiés un mois avant
- Gestion des espaces « data » à la main
- Pour l'instant pas de destruction des données « home »



Outils pour la mise en oeuvre

- Interface avec Gesper pour la création des comptes
 - Validation manuelle
 - Scripts bash déportés pour création ldap + homedir linux + inscription aux listes
 - Script powershell déporté pour création AD et home windows
- Scripts bash/python + cron pour notification, fermeture des comptes, suppression des listes et archivage des home



Conclusion

- Gain de temps et de fiabilité
- Meilleure gestion du stockage (passage de 82 % à 45 % d'utilisation sur le netapp)
- Gain en sécurité

