LOGON
Gestion des comptes et groupes
Destruction de données

Xavier Canehan

canehan@cc.in2p3.fr

Libérer des ressources

- Responsabiliser CZARS et Utilisateurs
  - Inciter au suivi
  - Limiter les intervenants
- Minimiser la charge du CC
  - Automatiser
  - Commandes globales
  - Règles claires

Bilan 2013 destruction de comptes

Rappel de la procédure 2013 : séquence et flux

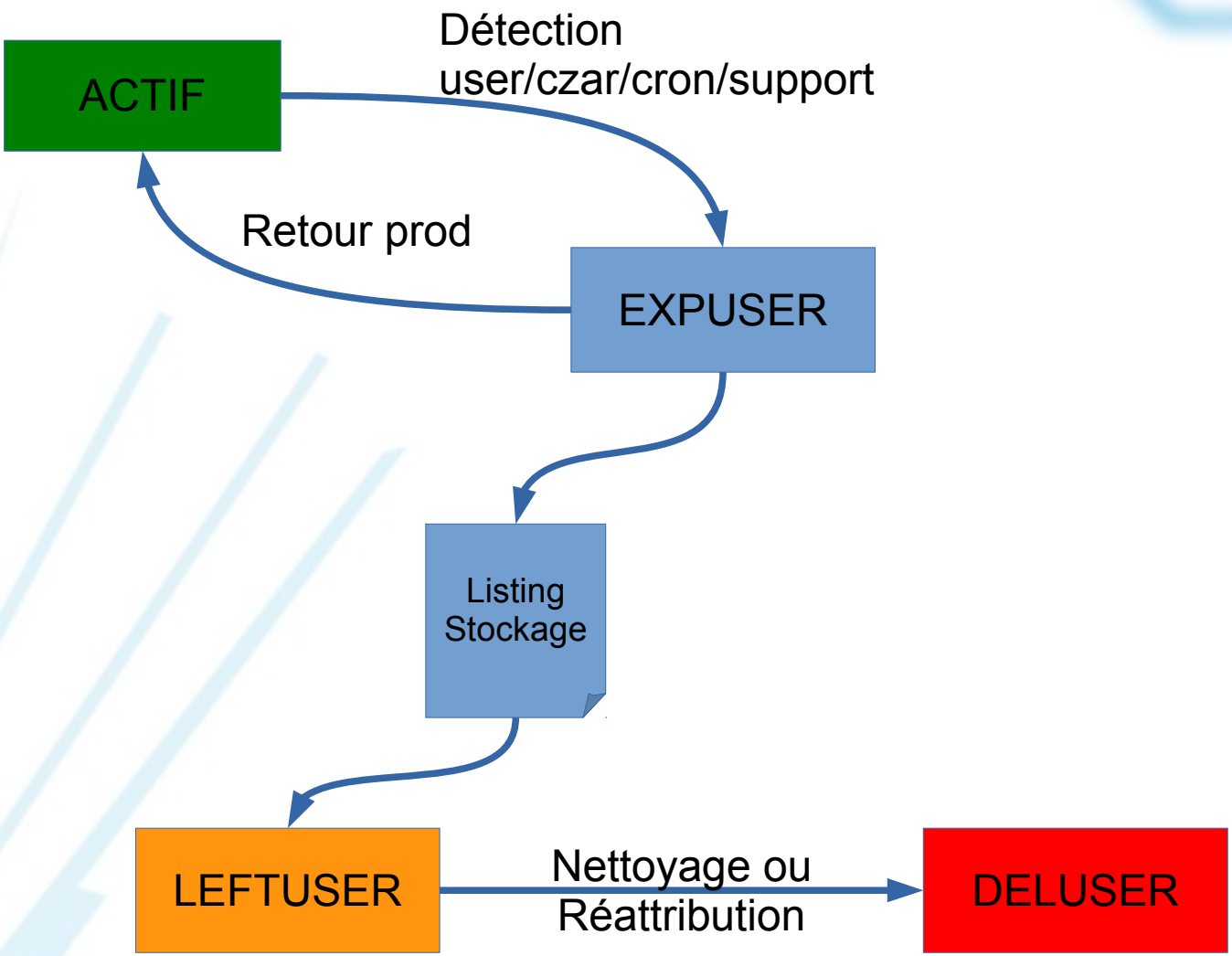
Avantages

- Destruction effective
- Listing des données
- Coopération interne
- Sensibilisation Czars
- Destruction par groupe

Défauts

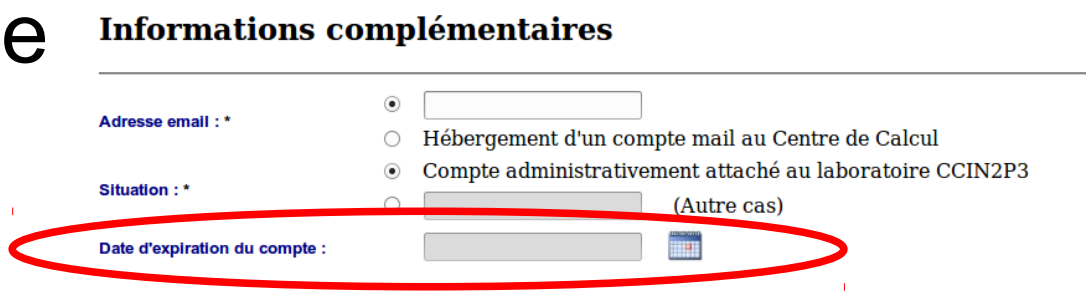
- Mauvais déclencheurs
- Procédures OTRS
- Nombre d'intervenants
- Délais
- Zone de quarantaine
- Outils à disposition

Graphe d'état : EXPIRATION USER



Date d'EXPIRATION du compte

- Information primordiale
- Inciter à sa fourniture
  - La rendre obligatoire
  - Transformer le formulaire
    - L'usage principal définit la valeur par défaut : 1 à 5 ans
      Stage / Doctorant / Post-Doc / CDD / Permanent
    - Une option « départ anticipé » rapproche la date
  - Faciliter sa modification : Czar / Support / Logon
- Introduit la revue régulière



Automatismes déclencheurs

- **Informer** les czars **Compte** de

  LASTLOGIN – EXPIRATION

  et le support dédié / czars **stockage** ?

  et les gestionnaires de stockage ?

  via le Décisionnel ?

- Crons
  - **USER** : mot de passe périmé + compte expiré
  - Synchronisation UDB → KAS
- **Lister** les candidats : tag UDB **EXPUSER**

Déclencheurs secondaires

- Ticket OTRS :
  - Utilisateur ou Czar **Compte**
  - **Support dédié**
- Rapports stockage
  - Gestionnaires de stockage
  - Rapport mensuel aux Czars
  - Décisionnel

Introduction de storageusage

Combien est stocké où, pour qui ?

- *storageusage* est utilisé pendant la destruction

  PoC de Pascal facilitant le travail du support

  Outil précieux qui ouvre de nombreuses possibilités

  Crons qui alimentent une base MRTG

- le groupe Stockage met en place un format unifié des statistiques stockage en JSON
  - Possibilité d'affiner la granularité de storageusage
  - Étendre à d'autres services pour couvrir des manques (DB et sites web connexes?)

Avenir storageusage

- Quel statut lui donner ?
  - Quelle publicité des rapports stockage détaillés ?
  - Ouverture discrétionnaire aux czars Stockage / Compte et aux utilisateurs ?
  - Quel suivi de développement ?
- Quelle délégation de privilèges ?
  - Le support ré-attribue les données
  - Le support détruit des données

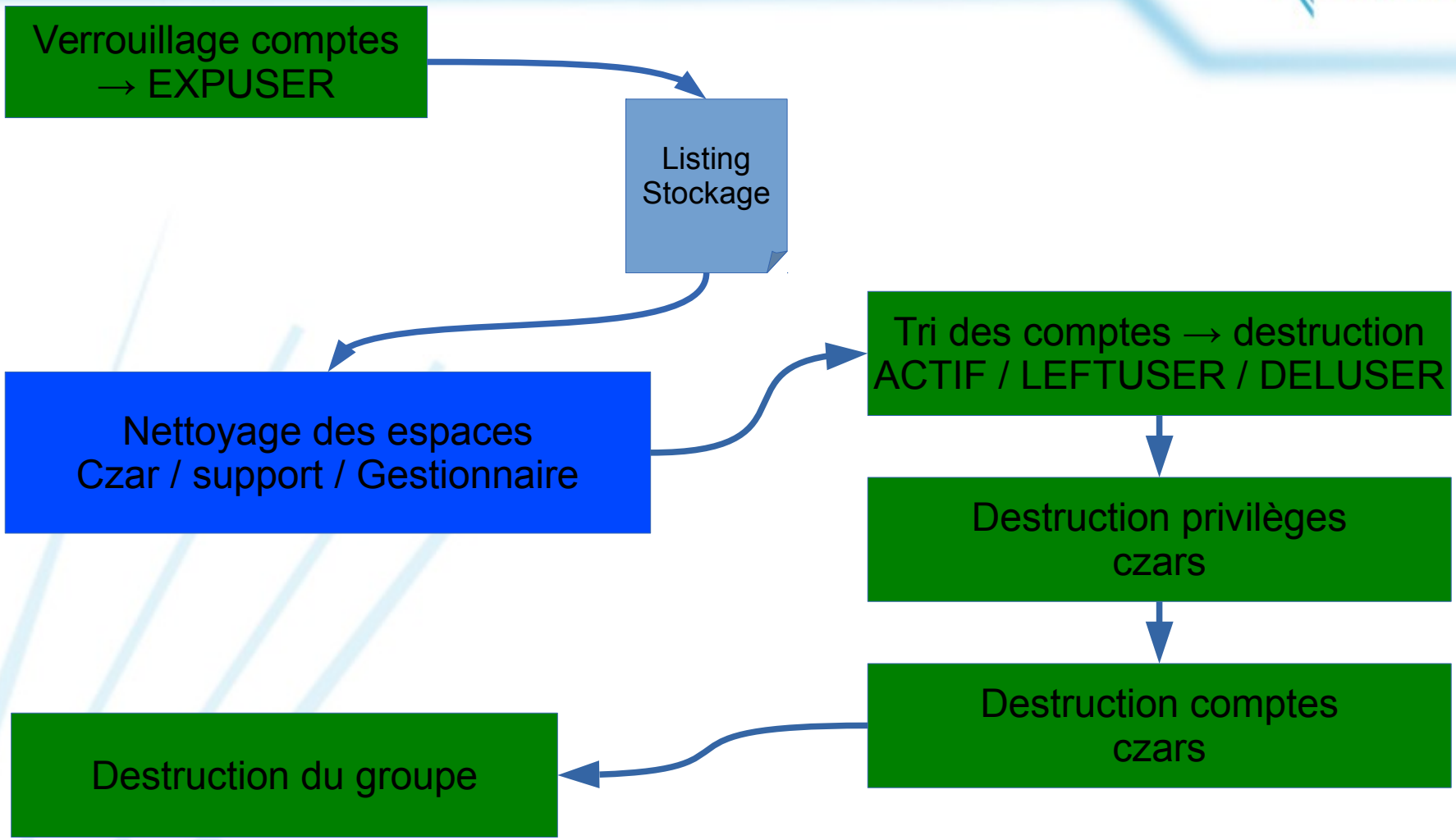
Destruction des données

- Autonomie des **czars stockage** et **utilisateurs**
  - Données localisées : destruction autonome par **l'utilisateur ou ses czars stockage**
  - Fin de compte annoncée → ménage préventif
  - Assistance possible support dédié
- Attribution du reste aux czars stockage
  - Hormis les HOME : à détruire
  - Aucune donnée orpheline
  - Traitement au rythme du czar
  - Surveiller les quotas et listes de données réattribuées

Clarifier les usages

- Distinction entre données personnelles / de groupe
- À la création de compte utilisateur : annoncer la date de destruction, en particulier celle des espaces personnels (pas de données de groupe dans les HOME)
- Préciser et stocker les conditions de fin de vie pour les données de groupe
  - Modifier le formulaire de création de labo/groupe
  - Automatiser leur publication au changement de czar
  - Préciser ce que à quoi le CC s'engage

Exemple destruction de groupe



Attente d'avis de la direction

- Date d'expiration obligatoire, durée par défaut
- Modes d'information aux czars et utilisateurs de la fin de vie des données

  fin de vie de compte, des données, de groupe ?
- Statut, publicité et avenir de storageusage ?
- Modes de définition, avec les groupes des conditions de stockage. Rappel lors des évolutions du groupe.

TODO divers

- Synchro UDB → KAS
- Outil d'expiration par le support : logonc -moduser -expiration
- Renommer les catégories de Czar
- Création Comptes Cloud + czar Cloud
- Réfection des outils logon : Kerberos 5 et remctl
- Création, options de comptes, Bash
  - README à la création de compte
  - Information données personnelles vs données de groupe
  - HOME détruit, donc pas de données utiles au groupe => information czar compte lors destruction
- Conditions de fin de vie de groupe pour les données
  - Automatiser au changement de czar → stocker les attentes du groupe, modifier le formulaire de création
  - Définir les obligations et droits du czar
  - Donc définir les obligations du CC
- Vérification destruction compte et présence de czar
- Cas particulier du czar en EXPUSER