

# Chiffrement de zones de stockage centralisées en environnement Linux (HPC)

ZIRRI Yassine

<yaszirri@etu.u-bordeaux1.fr>

Master CSI, Université de Bordeaux, France

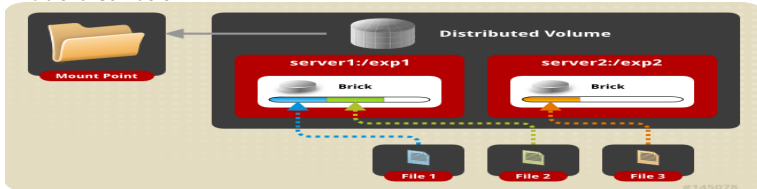
April 16, 2015



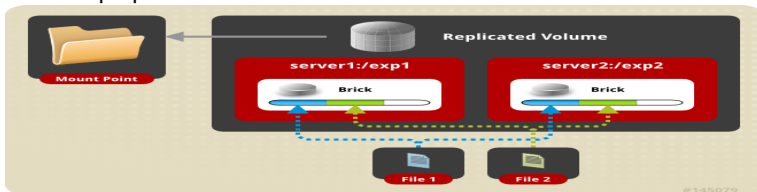


- GlusterFS est un système de fichiers libre distribué en parallèle.
- Les serveurs sont déployés comme des « briques de stockage ». Chaque serveur exécutant un daemon `glusterfsd` qui exporte un système de fichier local comme « volume ».
- Le processus client `glusterfs` regroupe les volumes distants en un unique volume.  
Le volume résultant est alors monté par un mécanisme FUSE.
- La plupart des fonctionnalités sont implémentées comme "traducteurs" :
  - Duplication et Réplication par fichier.
  - Partage de charge par fichier.
  - Gestion des pannes.

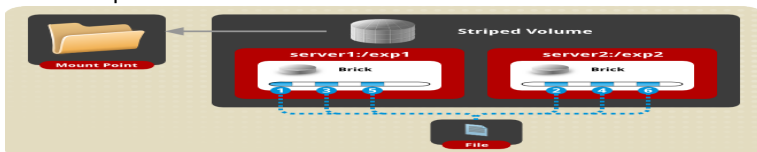
- Mode distribué :



- Mode répliqué :



- Mode striped :



- Il n'utilise pas de serveur central pour le stockage des metadata.
- Il peut grandir plus simplement que les autres DFS.
- GlusterFS server est conçu très simplement.
- Pour la confiance dans les nœuds (trust me).

- EncFS est un système de chiffrement qui fonctionne de façon simple sur tout système de fichiers grâce à FUSE.
- SECU : il utilise les algorithmes de la bibliothèques Libgcrypt de OpenSSL (AES, Blowfish,...).
- KERB : oui.
- GRAN : répertoire, fichier.
- ADMIN : facile.
- PRIX : open source (LGPL).
- Avantages :
  - Installation facile et durable.
  - Les performances semblent correctes.
  - Fonctionnement possible sur différents types de système de fichier.
- Défauts :
  - Le dossier de stockage est visible => accès à quelques metadata (nombre de fichiers chiffrés, leur taille et droits d'accès).
  - Absence de volume caché.

- VeraCrypt est un logiciel libre qui permet le cryptage des fichiers et partitions sous forme de conteneur global ou fichier unique.
- SECU : il utilise des algorithmes comme AES, Blowfish, Serpent...
- KERB : ...
- GRAN : disque, partition, répertoire et fichier.
- ADMIN : facile.
- PRIX : open source.
- Avantages :
  - Installation facile et durable.
  - Le logiciel et les fichiers sont compatibles multiplateformes.
- Défauts :
  - La robustesse de la protection est liée à la clef (minimum 15 caractères).
  - le container est de taille fixe.