Une Architecture de Bureaux Graphiques Distants Sécurisée et Distribuée

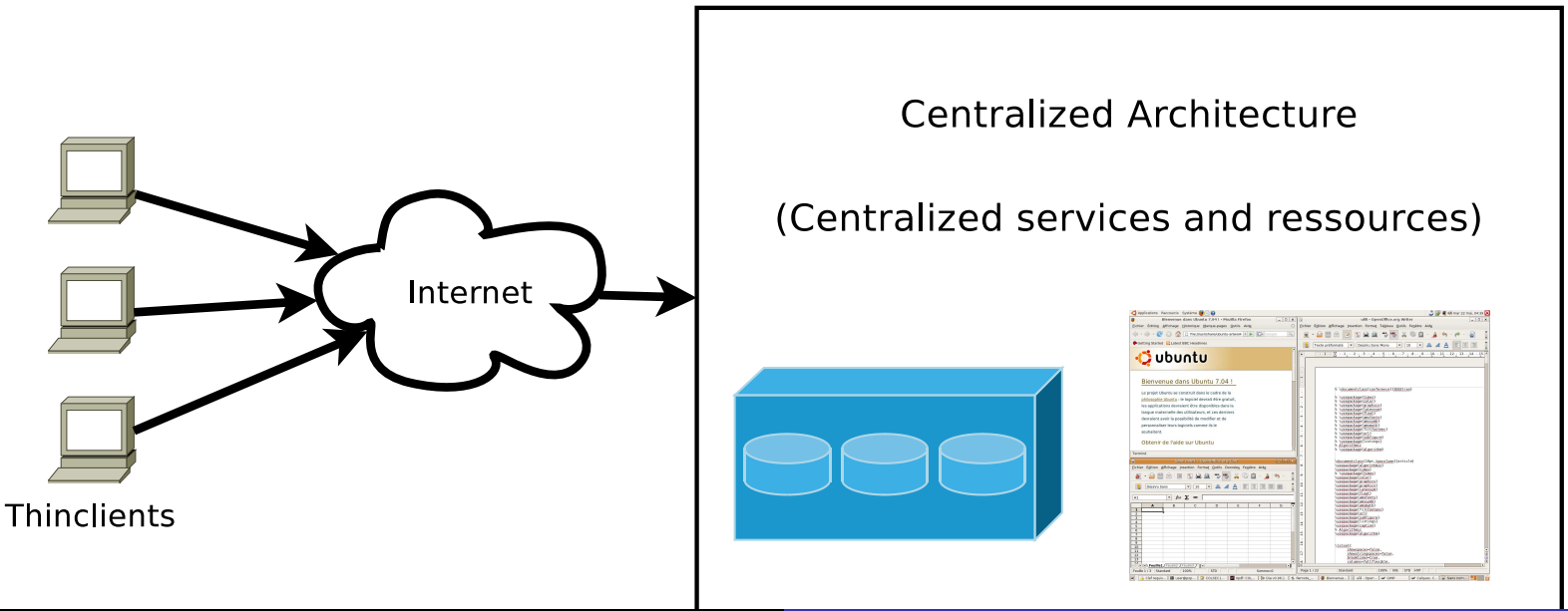
J. Rouzaud-Cornabas

Laboratoire d'Informatique Fondamentale d'Orléans
Université d'Orléans
Batiment IIIA, Rue Léonard de Vinci
45067 Orléans, France
jonathan.rouzaud-cornabas@univ-orleans.fr

June 6, 2008

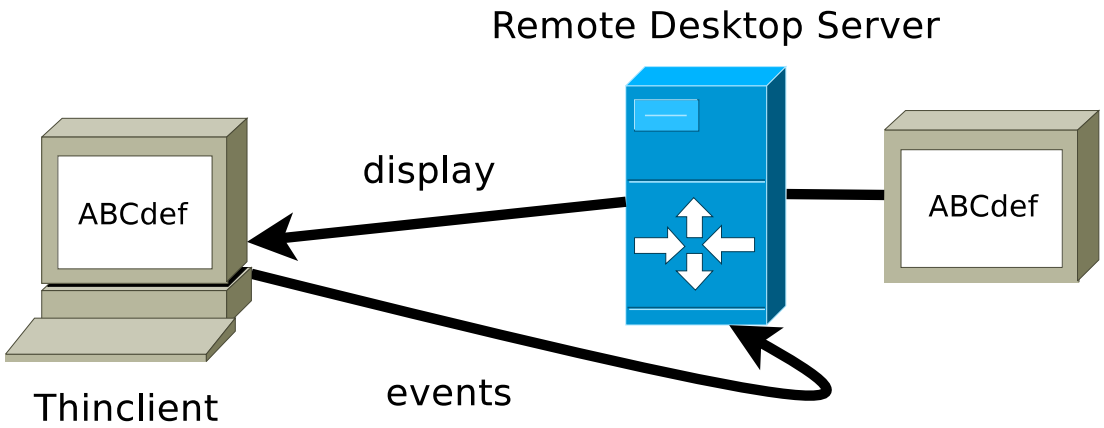
Approche des Bureaux Distants

- Augmentation de la taille de la bande passante.
- Clients Légers.
- Centralisation (mutualisation, économie d'énergie, consolidement)..
- Augmentation de la sécurité.



Remote Display

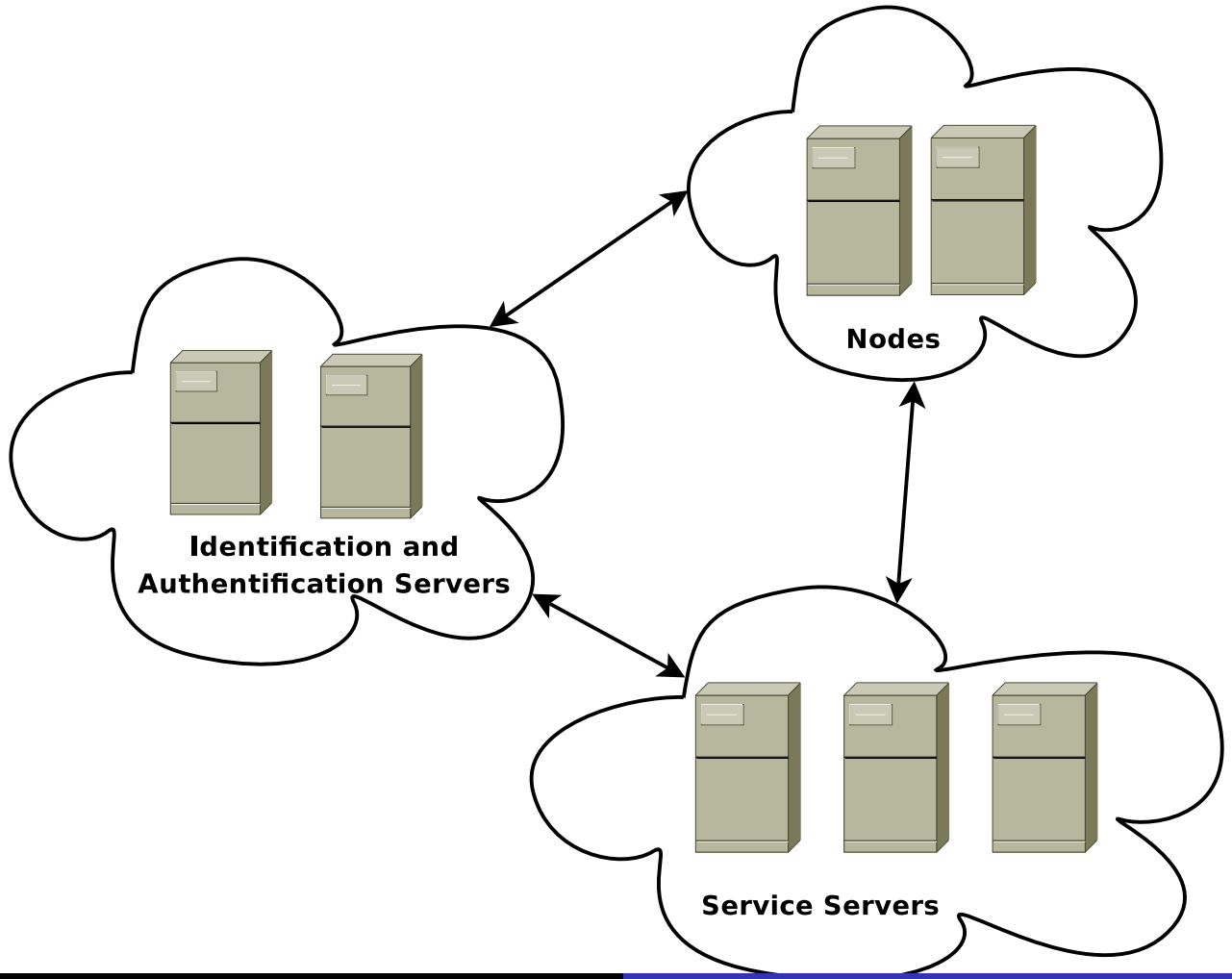
- Représentation distante d'un bureau.
- Envoi les frappes claviers et les mouvements de la souris.
- Besoin: une technologie et une architecture efficace et sécurisé.
- Technologie NX: moins de 10 Ko/s par utilisateur.



Motivation

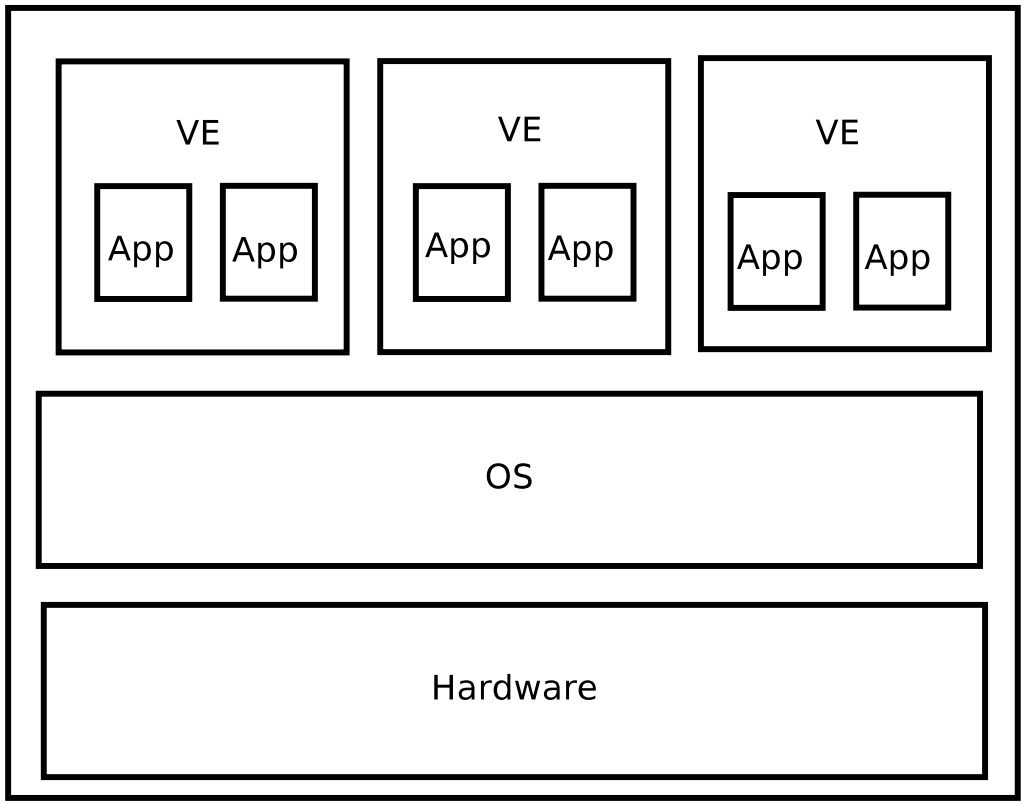
- Augmenter la sécurité des utilisateurs.
- Créer une architecture sécurisé pour ce type de service.
- Principaux buts:
  - Répartition de charges avancées.
  - Séparation des utilisateurs pour éviter les conflits.
  - Limiter la sur-utilisation du à la séparation des utilisateurs.
  - Une sécurité poussée.
  - Détecter les intrusions via la corrélation.

Authentification, Identification et SSO

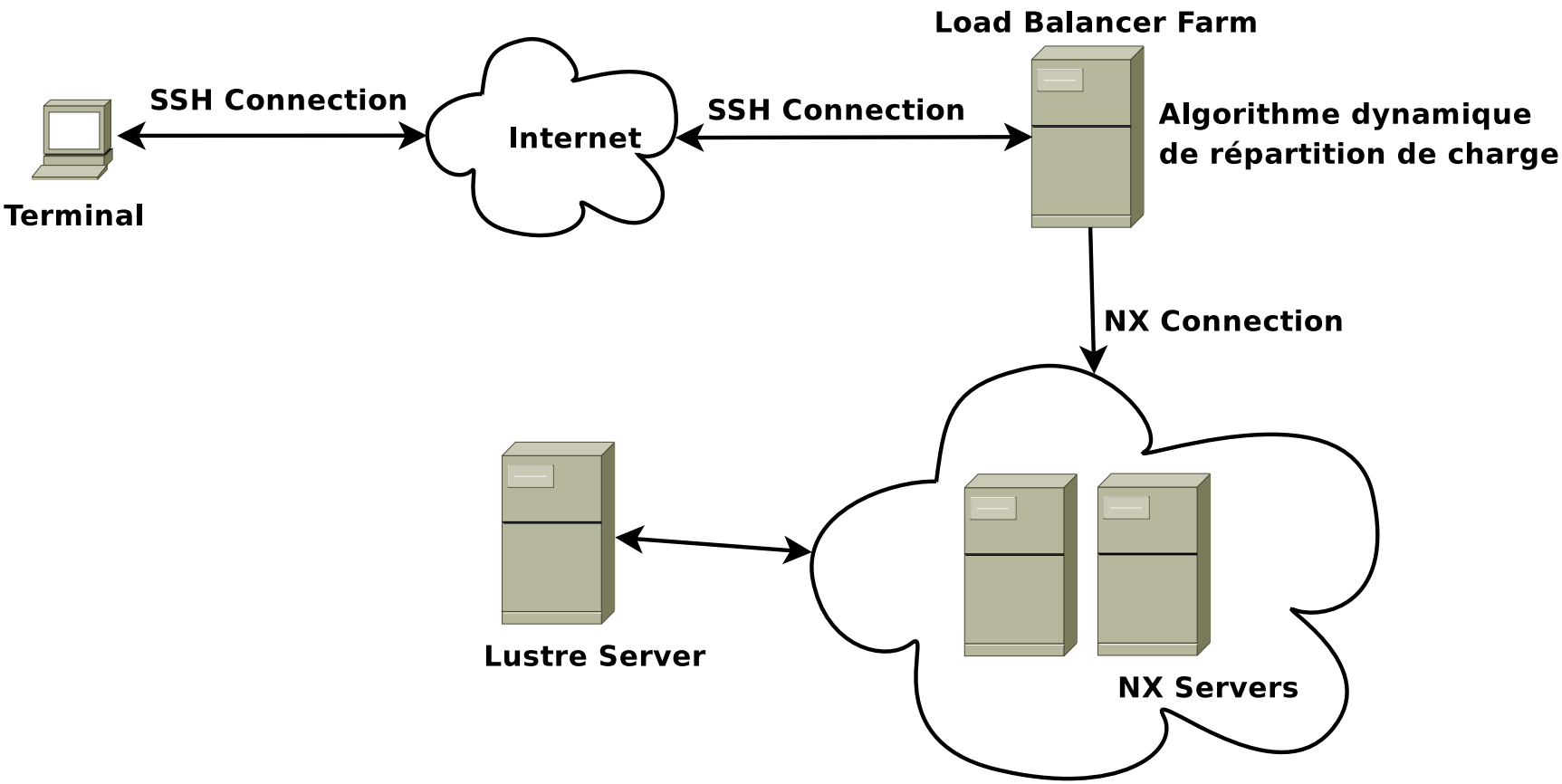


Virtualization: OpenVZ

- Virtualisation Légère.
- Isolation des utilisateurs.
- Gestion des quotas.
- Live Migration.



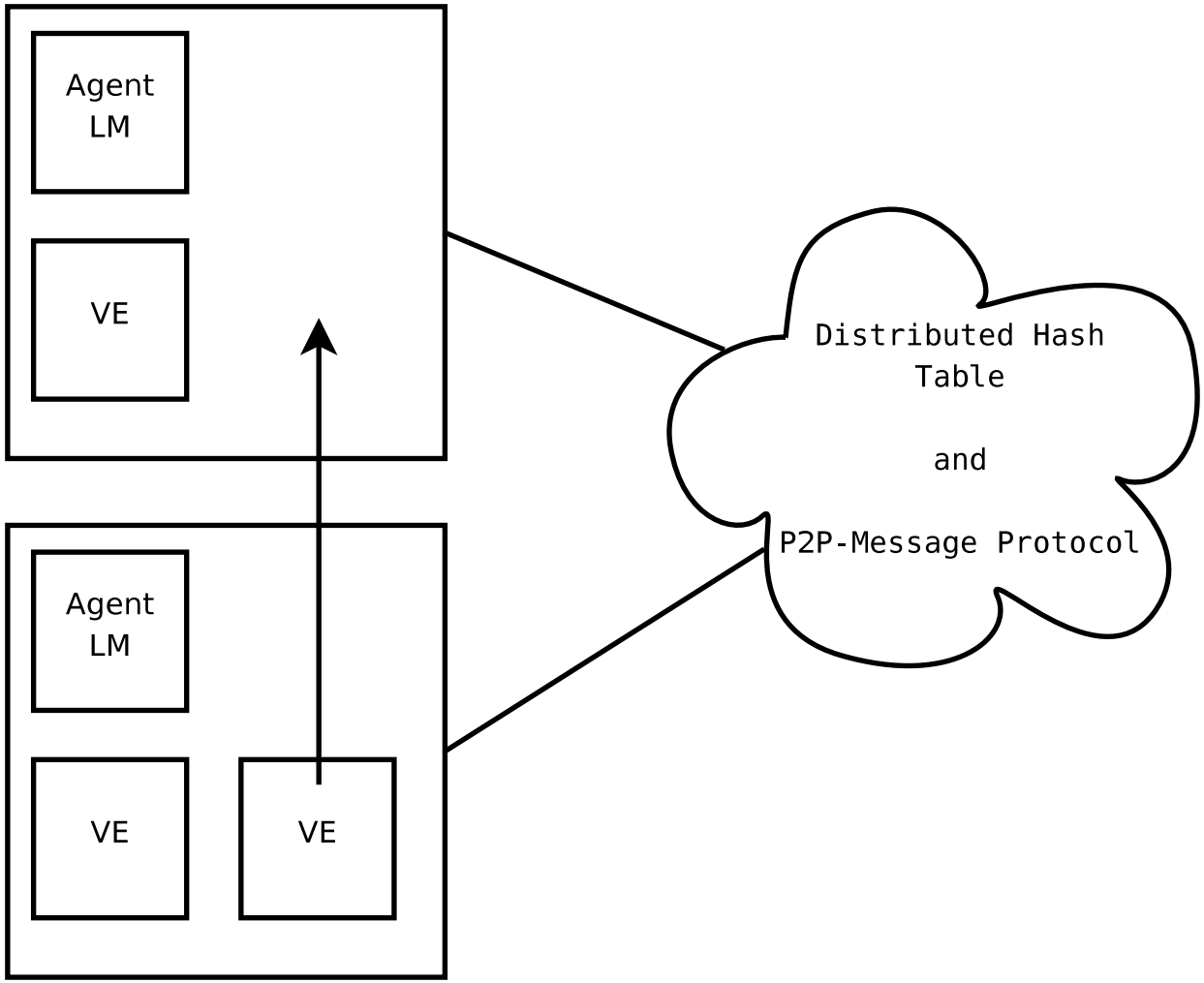
Load Balancing: Connexion d'un utilisateur



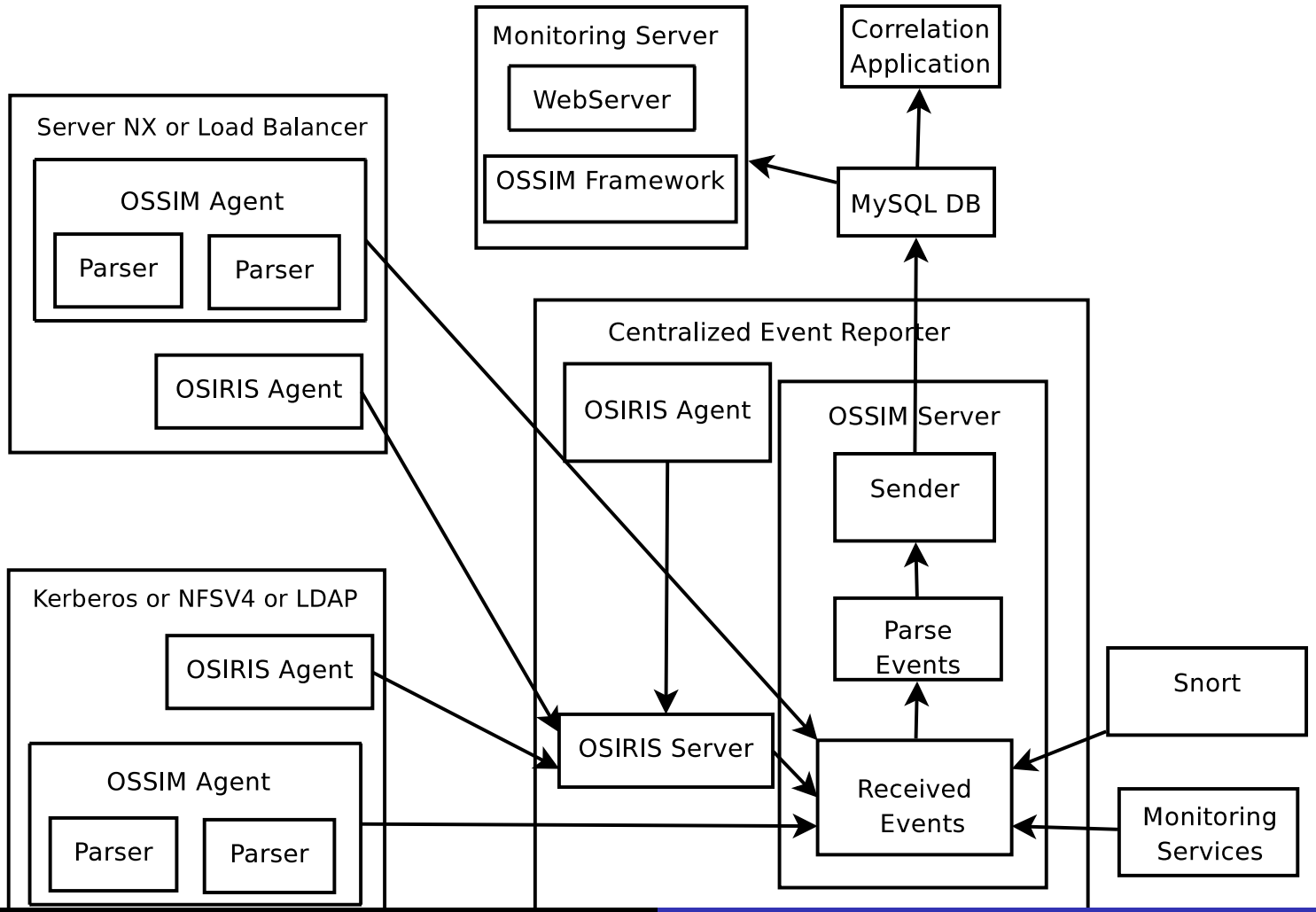
Continuité de service

- Reprise sur panne/crash.
- Répartition de la charge à l'ajout d'une nouvelle node.
- Répartition de la charge lors du départ d'une node.

Live Migration



IDS Architecture



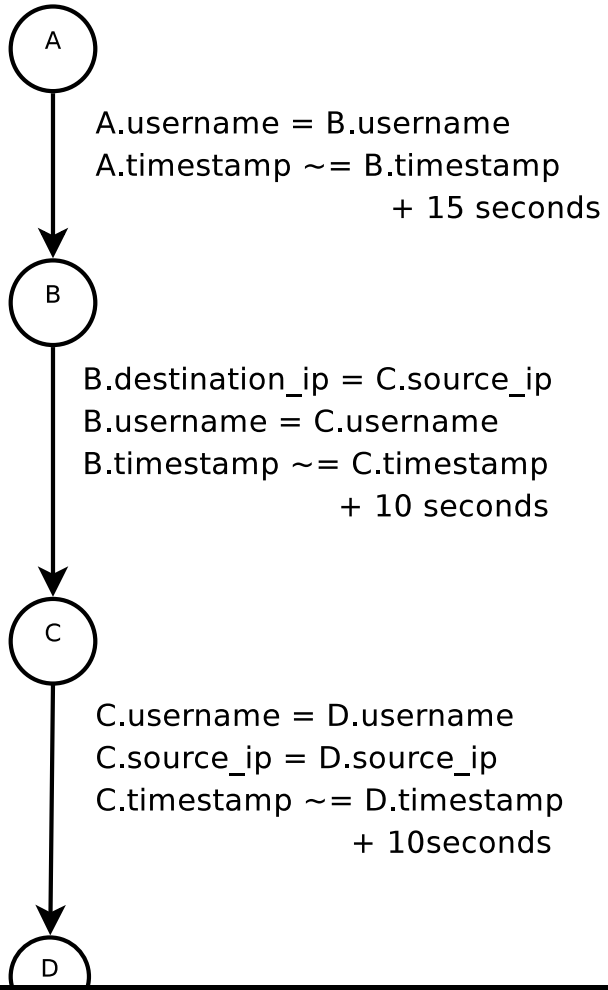
IDS Correlation

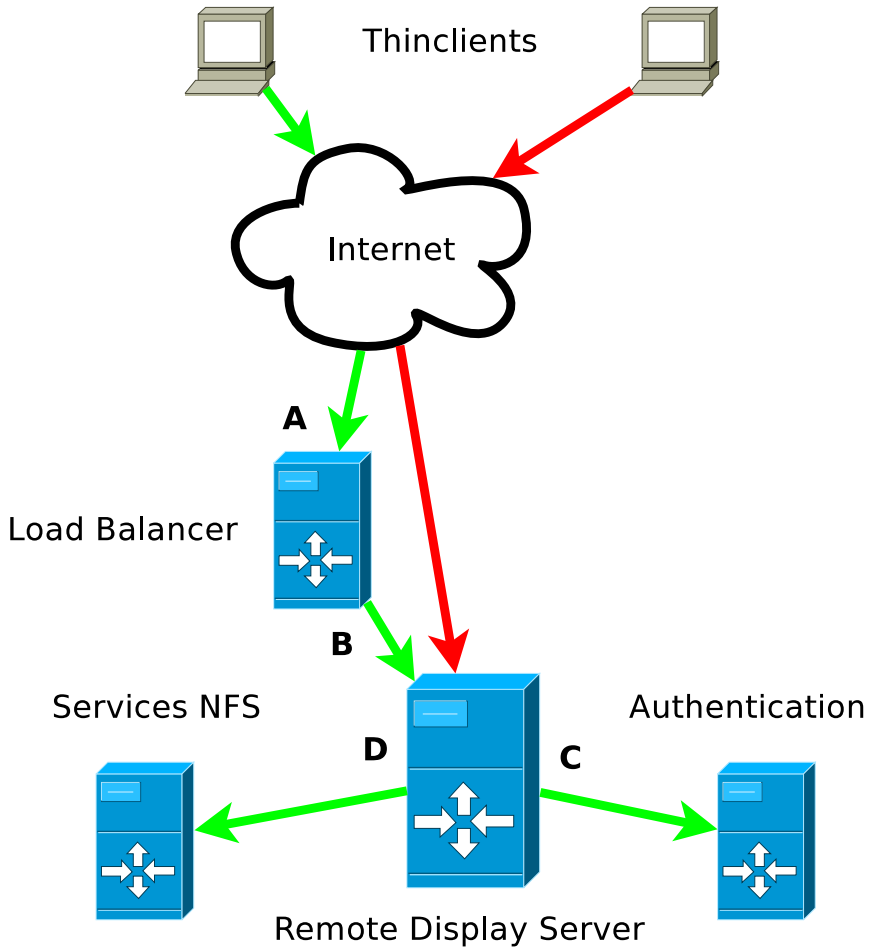
- Enormément d'alarmes générées.
- Besoin de les corréler pour avoir des informations de meilleurs qualité et un meilleur vue de la globalité des scénarios d'attaques.
- Moins de faux positifs qu'une alarme seule IDS.
- Permet de reconstruire une session compléte se déplaçant d'un ordinateur à un autre.

IDS Correlation: Algorithme

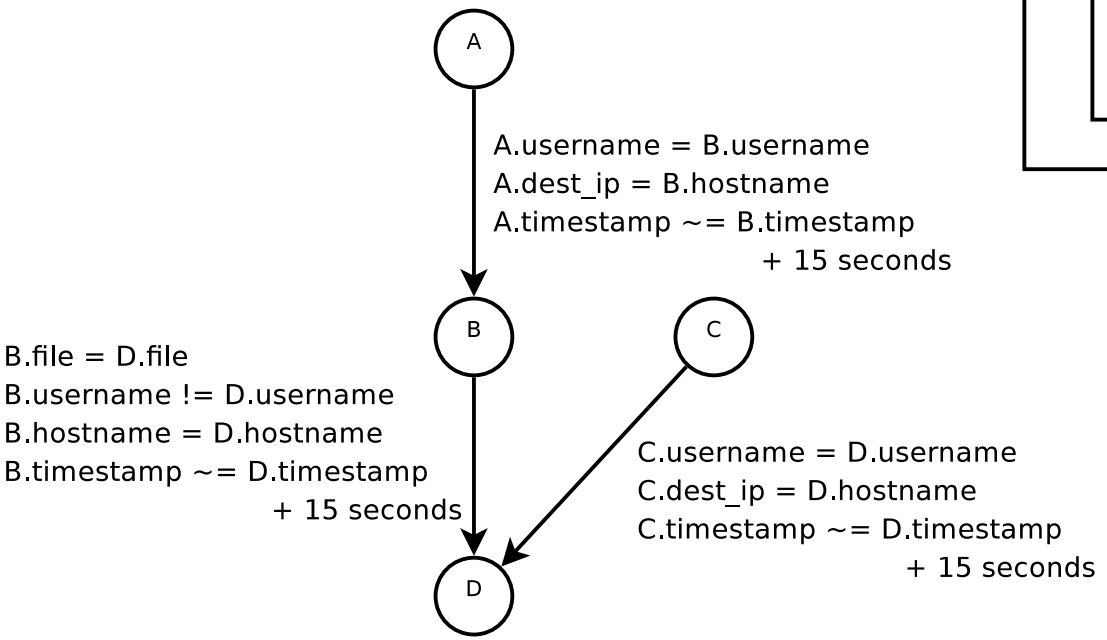
- Système se basant sur les automates: modélisation
  - Noeud: Evénement.
  - Arc:
    - Une transition chronologique.
    - Autoriser si toutes les conditions sont respectées.
- Algorithme de corrélation implémenté dans ossim:
  - Collection des événements.
  - Vérification du respect des conditions des automates.

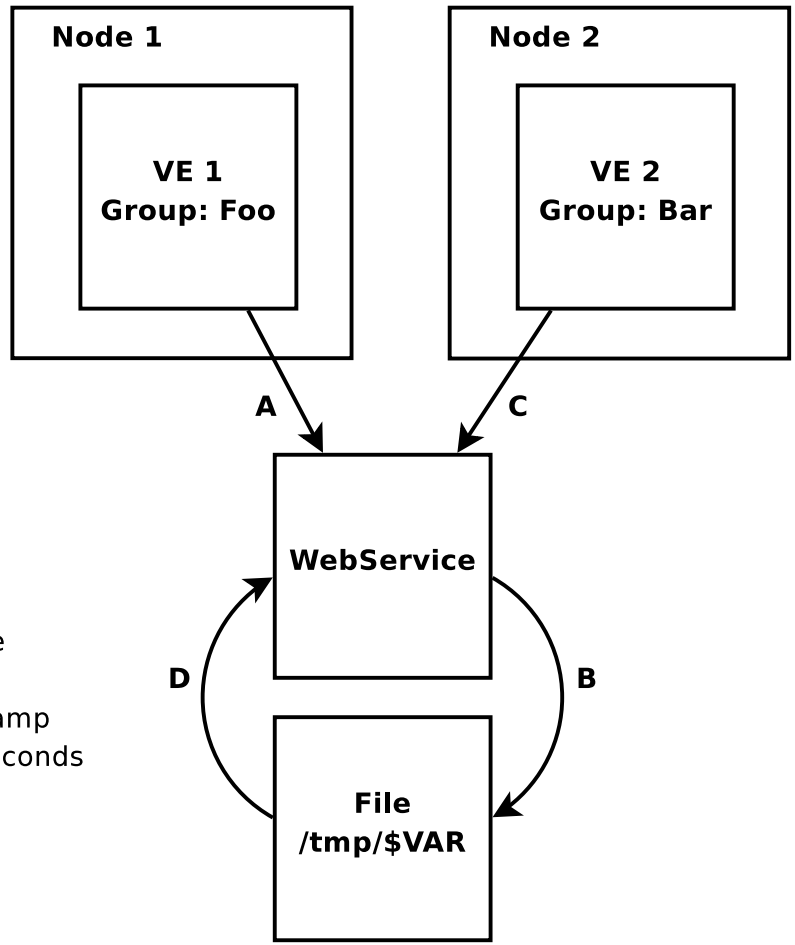
IDS Correlation: Automate de comportement normal





IDS Correlation: Automate de comportement anormal





Implémentation

- Architecture compléte mise en place en se basant uniquement sur des briques logiciels libres.
- Développement proposé (ou en cours) pour un reversement des contributions.
- Etude d'implémentation de la migration automatique en se basant sur libvirt et Distributed Hash Table.

Conclusion

- Solution en évolution constante.
- Amélioration de la mutualisation et du consolidation des ressources.
- Sécurité au coeur du système et à tous les niveaux.
- Système permettant l'audit automatique pour les intrusions et facilitant les opérations de forensic.

Perspectives

- Amélioration de la surveillance système.
- Mise en place de politique de sécurité se basant sur le respects des propriétés de sécurité.
- Développement d'une version stable de la live migration automatique.

Q & A

Q & A ?

Jonathan ROUZAUD-CORNABAS

jonathan.rouzaud-cornabas@univ-orleans.fr