# Prise en compte d'une politique de sécurité pour le déploiement dans le Cloud

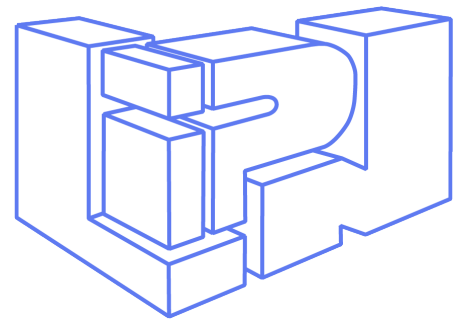
## Rencontres : Calcul intensif et Sciences des données

Timothée Ravier

Doctorant au LIFO (INSA-CVL) et au LIPN (Paris XIII)

LABORATOIRE D'INFORMATIQUE FONDAMENTALE D'ORLEANS

Vichy, 3 juin 2014



# Plan global

# Plan

# Définitions : Cloud Computing

- Modèle d'accès à la demande à un ensemble de ressources (e.g. réseau, stockage, serveurs, applications ou services).
- Ces ressources peuvent être mises à disposition et libérées rapidement avec une effort minimal de la part du fournisseur de service.

Référence : P. Mell et al., The NIST definition of cloud computing, 2011

# Définitions : Cloud Computing

- Plusieurs types de Clouds :
  - Software as a Service (SaaS) ;
  - Platform as a Service (PaaS) ;
  - Infrastructure as a Service (IaaS).

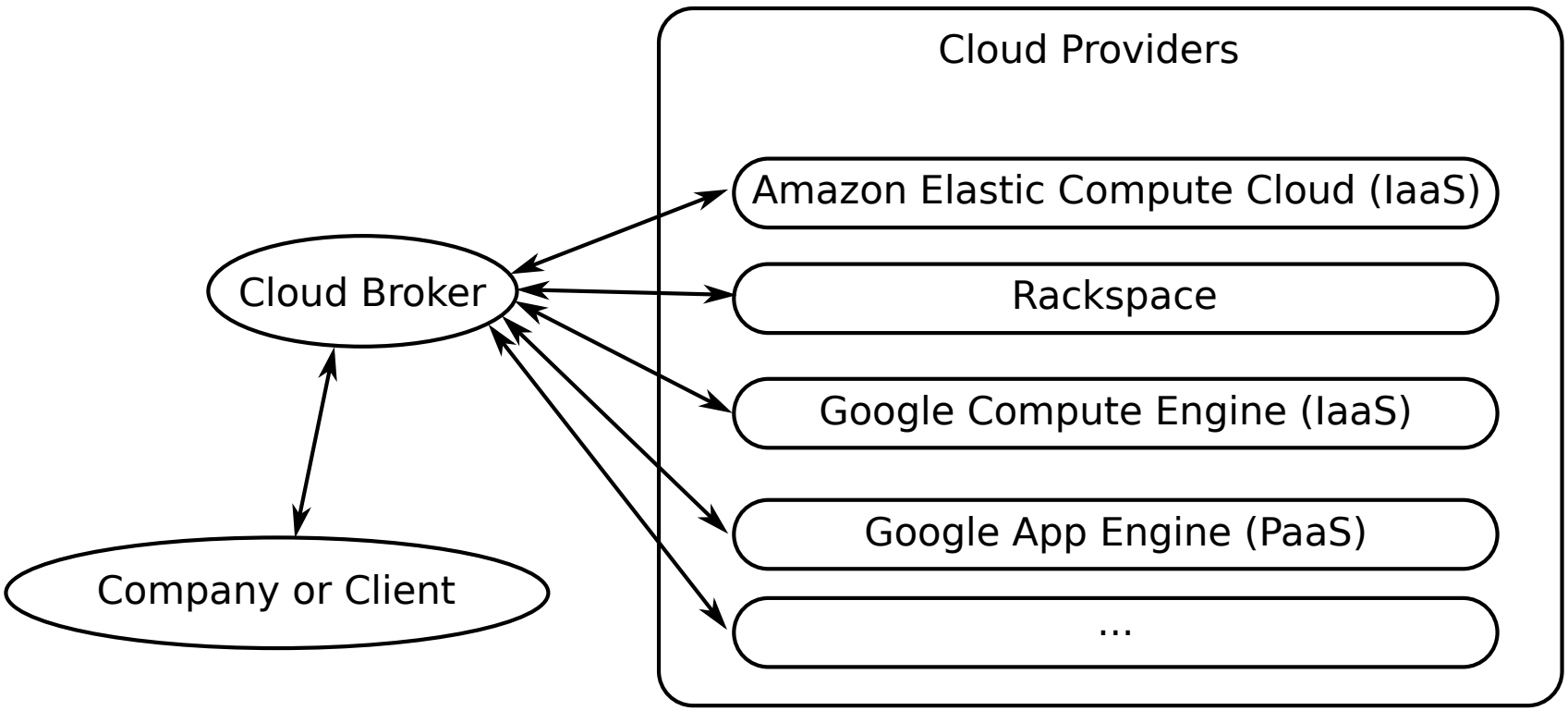
Référence : P. Mell et al., The NIST definition of cloud computing, 2011

# Définitions : Acteurs du Cloud Computing

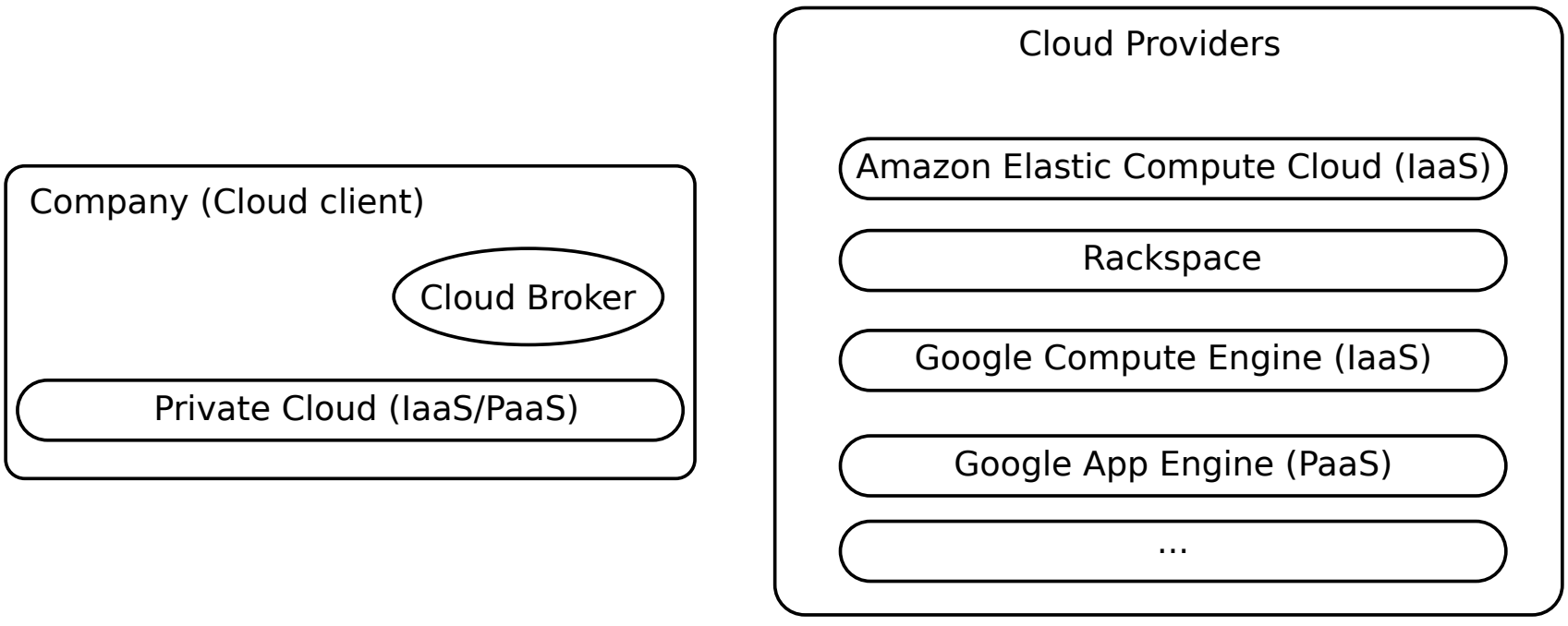
- Consommateur ;
- Fournisseur (Cloud Provider ou CP) ;
- Auditeur ;
- Intermédiaire et agrégateur (Cloud Broker ou CB) ;
- Fournisseur de réseau inter-Clouds.

Référence : M. Hogan et al., Nist cloud computing standards roadmap, 2011

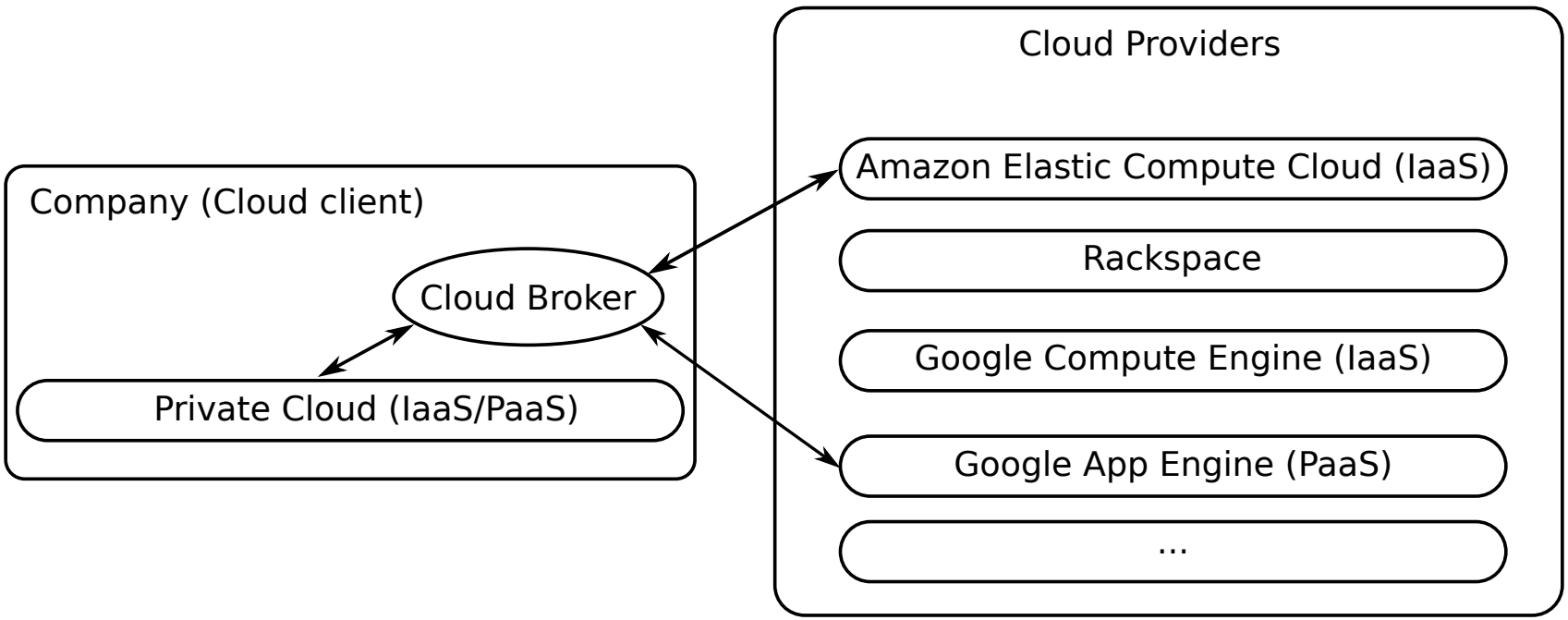
# Définitions : Principe du Cloud Broker (externe)



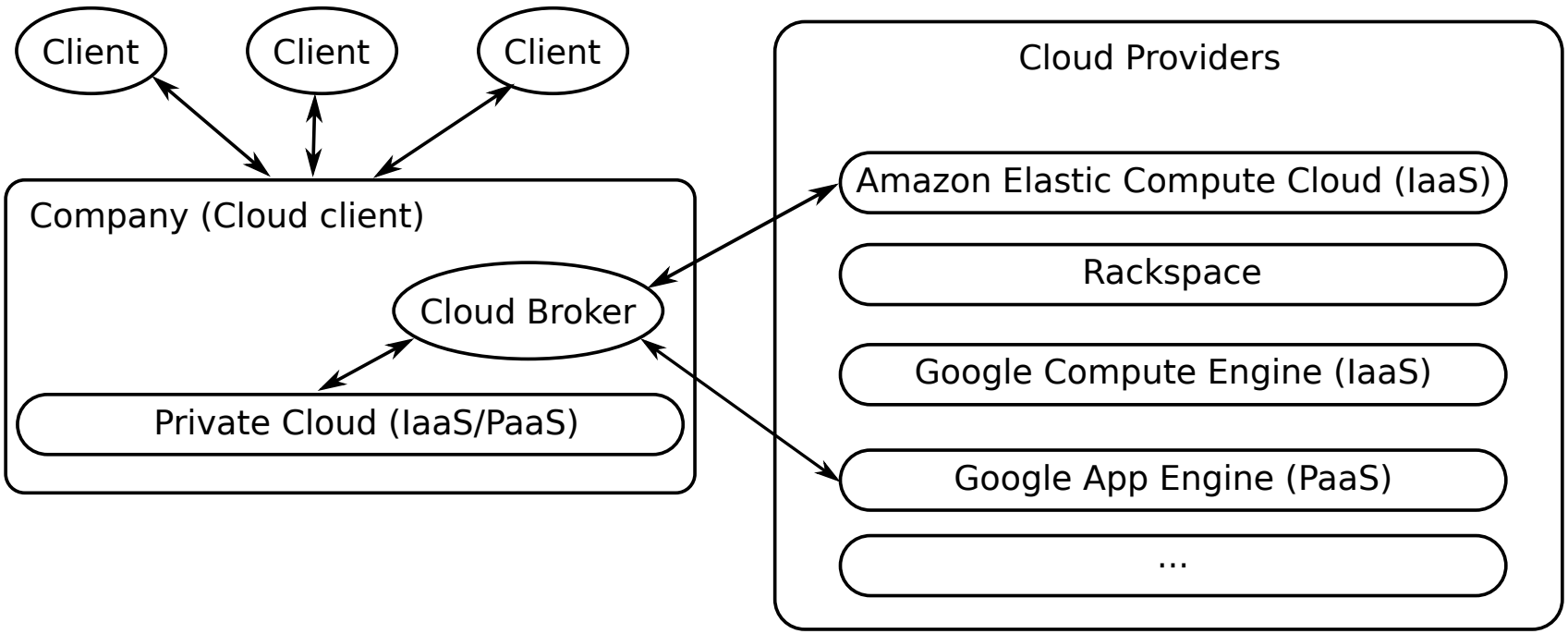
# Définitions : Principe du Cloud Broker (interne)



# Définitions : Principe du Cloud Broker (interne)



# Définitions : Principe du Cloud Broker (interne)



# Définitions : Sécurité

- Politique de sécurité : ensemble de propriétés de sécurité ;
- Principales propriétés de sécurité :
  - Confidentialité ;
  - Intégrité ;
  - Disponibilité (inclut les performances) ;
  - Traçabilité (authentification, imputation, non-répudiation).

Références :


- D.C. Latham. Department of Defense Trusted Computer System Evaluation Criteria, 1986
- D. D. Clark et al., A comparison of commercial and military computer security policies, 1987

# Définitions : Service

- Ensemble de processus liés à l'exécution d'une application ;
- Ne se limite pas au concept de service Web ;
- Exemples :
  - Base de données ;
  - Serveur web ;
  - Démon d'envoi de mails ;
  - ...

# Plan

# Principales menaces impactant les clients

- Généralisation aux Clouds de menaces conventionnelles :
  - Vol de données : menace extérieure ou intérieure (employé malicieux) ;
  - Perte ou corruption de donnés ;
  - Dénis de service (Denial of Service ou DoS) ;
  - Vulnérabilité dans l'infrastructure d'un fournisseur de Cloud.

Référence : Cloud Security Alliance, The Notorious Nine Cloud Computing Top Threats, 2013

# Principales menaces impactant les clients

- Ce qui correspond aux :
  - attaques directes extérieures / intérieures ;
  - attaques suite à la compromission d'un service ;
  - attaques suite à la compromission d'un système.

Référence : Cloud Security Alliance, The Notorious Nine Cloud Computing Top Threats, 2013

# Choix d'un fournisseur de service Cloud

- Choix toujours plus grand ;
- Standardisation limitée : multiplicité des contrats ;
- Disponibilité de l'infrastructure à la discrétion du fournisseur (Service Level Agreement ou SLA) ;
- Méthodes pour comparer les offres suivant un ensemble de critères.

Références : S. K. Garg et al., SMICloud : A framework for comparing and ranking cloud services, 2011

# Limites des contrats et des SLAs

- Négociation d'un SLA quasi impossible pour un client ;
- Défaut ? Remboursement en crédits chez le fournisseur ;
- Impacte aussi les plus gros fournisseurs ;
- Besoins en sécurité variables suivant les services ;
- Importance grandissante des Cloud Brokers.

Référence : Trust Management Forum, Cloud Service Broker, 2010

# Sécurité des fournisseurs de Cloud

- Outils actuels de gestion de Cloud : pas de politique de sécurité ;
- Prise en compte des contraintes de sécurité par le fournisseur ?
- Isolation entre les clients d'un fournisseur ?
- Méthodes pour juger de la confiance à accorder à un fournisseur.

Références :


- A Framework for Realizing Security on Demand in Cloud Computing, P Jamkhedkar et al. 2013
- Intel Cloud Finder : `http://www.intelcloudfinder.com/`
- CSA Security, Trust & Assurance Registry (STAR) : `https://cloudsecurityalliance.org/star/`

# Gestion du déploiement de services dans un Cloud

- Plusieurs projets pour gérer le déploiement ou les interactions entre services dans les Clouds ;
- Nécessite la modification des services pour les adapter à ces modèles ;
- Gestion partielle la sécurité ;
- Pas de garantie de l'application des propriétés de sécurité ;
- Basé sur une notion de confiance.

Références :


- A. J. Ferrer et al., OPTIMIS : A holistic approach to cloud service provisioning, 2012
- P. H. Meland et al., The challenges of secure and trustworthy service composition in the Future Internet (ANIKETOS), 2011
- R. Buyya et al., Market-oriented cloud computing and the cloudbus toolkit, 2010

# Plan

# Objectifs

- S'affranchir des contraintes de SLAs imposées par les Clouds Providers :
  - Se positionner en Cloud Broker (interne) ;
  - Intégrer un Cloud privé si disponible.
- Définir et maintenir une politique de sécurité :
  - Suivre les évolutions de l'architecture ;
  - Certains éléments déployés sont chargés de l'application de la politique.

Références :


- J. Carpentier et al. CompatibleOne : Designing an energy efficient open source cloud broker, 2012
- M Casassa Mont et al., Security and Privacy Governance In Cloud Computing via SLAs and a Policy Orchestration Service, 2012

# Extension du principe d'interaction

- PIGA : modèle fort pour la protection d'un système ;
- PIGA-SYSTRANS : protection coordonnée d'un système ;
- PIGA-VIRT : protection forte de plusieurs systèmes. Pas de gestion de la disponibilité ;
- Considérer directement les interactions entre les services dans le Cloud, quelque soit leur emplacement ;
- Prendre en compte le medium permettant l'interaction entre deux services.

Références :


- J. Briffaut et al., Formalization of security properties : enforcement for mac operating systems and verification of dynamic mac policies
- J. Briffaut et al., PIGA-VIRT : An advanced distributed mac protection of virtual systems

# Critères / propriétés

- Représentation de l'architecture et des interactions entre les services sous forme de graphe ;
- Applications de critères sur les arrêtes et sur les nœuds ;
- Deux types de critères pris en compte dans la politique de sécurité :
  - Fonctionnel : e.g. CPU, RAM, stockage, contrainte légale ou arbitraire ;
  - Non fonctionnel : e.g. intégrité du stockage associé à un service, confidentialité du lien entre deux services.

# Propriétés de sécurité avec niveaux

- Propriétés plus ou moins contraignantes en fonction de leurs niveaux ;
- Niveaux non nécessairement linéaires ;
- Pas liés à une technologie mais à un objectif de sécurité ;
- L'implémentation effective peut mettre en œuvre plusieurs systèmes ou technologies.

Références :


- E Caron et al., Definition of security metrics for the Cloud Computing and security-aware virtual machine placement algorithms, 2013
- J. Briffaut et al., A dynamic end-to-end security for coordinating multiple protections within a Linux desktop, 2010

# Propriétés de sécurité avec niveaux : exemple

- Niveaux de garantie de disponibilité du stockage associé à un service en fonction de la sévérité du risque à mitiger :
  - Aucune garantie de disponibilité particulière ou garantie offerte par le fournisseur de Cloud (PaaS) ;
  - Garantie à l'échelle du service : contrôle de la priorité d'accès au stockage ;
  - Garantie à l'échelle du système : réplication des données ;
  - Garantie à l'échelle géographique : réplication sur des sites géographiquement distants ;
  - Garantie à l'échelle d'un fournisseur de Cloud : réplication sur des fournisseurs distincts.

# Résolution du placement d'un service en fonction des contraintes de sécurité

- Modélisation : système d'équations linéaires représentant les différentes contraintes (fonctionnelles et non fonctionnelles) et leur niveau ;
- Il est possible qu'il n'y ai pas de solution parfaite dans certains cas.

# Résolution du placement d'un service en fonction des contraintes de sécurité

- Prise en compte de la disponibilité : décision prise en fonction des critères non fonctionnels :
  - Contraintes d'intégrité ou de confidentialité prioritaires ;
  - Contraintes de disponibilité prioritaires.

# Plan

# Passer des machines virtuelles...

- La gestion de machines virtuelles complexifie inutilement la tâche :
  - Maintient de l'environnement à jour ;
  - Harmonisation des configurations ;
  - Couches inutiles (e.g. noyau) ;
  - Nombreuses interactions difficiles à contrôler à l'intérieur d'une machine virtuelle ;
  - Difficile de réduire l'impact d'une vulnérabilité.
- Certaines propriétés de sécurité requièrent le contrôle complet du système pour pouvoir être appliquées.

# . . . aux conteneurs

- Le système hôte assure donc l'application de la politique ;
- Chaque service est placé dans un conteneur dont on va contrôler les interactions :
  - Simplifie la création des politiques de sécurité ;
  - Plus léger qu'une machine virtuelle : envisageable de créer une instance de conteneur par client ;
  - Ensemble minimal pour faire fonctionner un service.

# Projets en cours et contributions potentielles

- Support des conteneurs : inclus dans le noyau Linux ;
- Gestionnaire de conteneurs : Docker ;
- Systèmes hôtes : CoreOS, Project Atomic ;
- Importance du système de fichier dans l'application de certaines propriétés de sécurité (e.g. Ceph, GlusterFS, XtreemFS).

Références :

- Docker : https ://www.docker.io/
- CoreOS : https ://coreos.com/
- Project Atomic : http ://www.projectatomic.io/
- Ceph : http ://ceph.com/
- GlusterFS : http ://www.gluster.org/
- Contrail project (XtreemFS) : http ://contrail-project.eu/

# Aspects non pris en compte

- Gestion de l'énergie ;
- Minimisation des coûts.

# Questions ?

Merci de votre attention.

# Références I

[1] C. S. Alliance. Cloud security alliance warns providers of'the notorious nine'cloud computing top threats in 2013. *Top Threats Working Group The Notorious Nine Cloud Computing Top Threats in*, 2013 :8, 2013.

[2] J. Briffaut, E. Lefebvre, J. Rouzaud-Cornabas, and C. Toinard. PIGA-Virt : an advanced distributed mac protection of virtual systems. In *Euro-Par 2011 : Parallel Processing Workshops, Lecture Notes in Computer Science*, pages 8–19, Aug 2011.

# Références II

[3] J. Briffaut, M. Peres, and C. Toinard. A dynamic end-to-end security for coordinating multiple protections within a linux desktop. In *CTS*, pages 509–515, 2010.

[4] R. Buyya, S. Pandey, and C. Vecchiola. Market-oriented cloud computing and the cloudbus toolkit. *Large Scale Network-Centric Distributed Systems*, pages 319–358, 2010.

[5] E. Caron, A. D. Le, A. Lefray, and C. Toinard. Definition of security metrics for the cloud computing and security-aware virtual machine placement algorithms. In *Cyber-Enabled Distributed Computing and Knowledge Discovery*

# Références III

*(CyberC), 2013 International Conference on*, pages 125–131. IEEE, 2013.

[6] J. Carpentier, J.-P. Gelas, L. Lefevre, M. Morel, O. Mornard, and J.-P. Laisne. CompatibleOne : Designing an energy efficient open source cloud broker. In *Cloud and Green Computing (CGC), 2012 Second International Conference on*, pages 199–205. IEEE, 2012.

[7] M. Casassa Mont, K. McCorry, N. Papanikolaou, and S. Pearson. Security and privacy governance in cloud computing via SLAs and a policy orchestration service. In *Proceedings of the 2textsuperscriptnd International Conference on*

# Références IV

*Cloud Computing and Services Science (CLOSER 2012)*. SciTePress, Jan 2012.

[8] A. J. Ferrer, F. Hernández, J. Tordsson, E. Elmroth, A. Ali-Eldin, C. Zsigri, R. Sirvent, J. Guitart, R. M. Badia, K. Djemame, et al. OPTIMIS : A holistic approach to cloud service provisioning. *Future Generation Computer Systems*, 28(1) :66–77, 2012.

[9] S. K. Garg, S. Versteeg, and R. Buyya. SMICloud : A framework for comparing and ranking cloud services. In *Utility and Cloud Computing (UCC), 2011 Fourth IEEE International Conference on*, pages 210–218. IEEE, 2011.

# Références V

[10] M. Hogan, F. Liu, A. Sokol, and J. Tong. Nist cloud computing standards roadmap. *NIST Special Publication*, 35, 2011.

[11] P. H. Meland, J. B. Guerenabarrena, and D. Llewellyn-Jones. The challenges of secure and trustworthy service composition in the future internet. In *System of Systems Engineering (SoSE), 2011 6th International Conference on*, pages 329–334. IEEE, 2011.

[12] P. Mell and T. Grance. The NIST definition of cloud computing. *NIST special publication*, 800(145) :7, Sept 2011.