# INDIC : Supervision de sécurité à la carte pour les utilisateurs de cloud IaaS

Louis Rilling, Christine Morin

# INDIC: Supervision de sécurité à la carte pour les utilisateurs de cloud IaaS

Louis Rilling*†[1] and Christine Morin*‡[2]

[1]DGA Maîtrise de l'information (DGA.MI) – Direction générale de l'Armement (DGA) – BP7 - 35998 Rennes CEDEX 7, France

[2]Inria Rennes - Bretagne - Atlantique (Inria / Myriads) – INRIA – Campus de Beaulieu 35042 Rennes cedex, France

**Résumé**

Dans le contexte de l'informatique en cloud, des organisations clientes externalisent une partie de leur système d'information (SI) dans des infrastructures virtualisées (ensemble de machines virtuelles et de réseaux virtuels) et hébergées sur l'infrastructure physique d'un opérateur de cloud. Afin d'assurer à une organisation cliente un minimum de garanties sur le service rendu par l'opérateur de cloud, et afin de permettre à l'opérateur de cloud de maîtriser le coût de ses services, les garanties sur le service rendu sont définies dans un contrat (appelé Service-Level Agreement ou SLA) entre chaque organisation cliente et l'opérateur de cloud. Parmi les intérêts du cloud, il est possible de mutualiser les coûts des ressources physiques, notamment les réseaux d'interconnexion et les machines physiques. Sur une même machine physique (de l'opérateur de cloud), sont ainsi exécutées plusieurs machines virtuelles (VM) (d'une ou plusieurs organisations clientes). Cette mutualisation des ressources s'accompagne d'une flexibilité relative au nombre de machines virtuelles déployées, qui peut varier dynamiquement et à court terme en fonction de l'évolution des besoins de chaque organisation cliente, avec un parc de machines physiques évoluant sur un plus long terme en fonction des demandes reçues par l'opérateur de cloud. Enfin, souvent pour des raisons d'optimisation d'utilisation des ressources physiques, l'opérateur de cloud met en place des politiques de migration de machines virtuelles, qui déplacent les machines virtuelles, en cours d'exécution, entre les machines physiques.

Comparé à un SI implanté directement sur une infrastructure physique, un SI externalisé dans un cloud présente une configuration très dynamique, et est exposé à davantage de menaces, notamment en raison de la cohabitation des infrastructures virtualisées de différentes organisations clientes. La sécurisation des clouds est donc l'objet de nombreux travaux de recherche, pour la protection contre les menaces (authentification, contrôle d'accès, confidentialité des communications, isolation, etc.) [2, 3, 5] comme pour la supervision de sécurité (souvent résumée à la détection d'intrusion) [1, 2, 3, 4, 6].

Nous nous intéressons à la supervision de la sécurité (SdS). Tout système d'information ayant des vulnérabilités, la SdS consiste à surveiller le SI aux endroits où des vulnérabilités sont identifiées, afin d'être en mesure de détecter les attaques, en informer les administrateurs du SI, et éventuellement réagir. La SdS est donc cruciale dans la gestion de la sécurité

*Intervenant

†Auteur correspondant: louis.rilling@irisa.fr

‡Auteur correspondant: christine.morin@inria.fr

d'un SI. Dans un SI implanté directement sur une infrastructure physique, la SdS est implantée sur la même infrastructure et est entièrement maîtrisée par l'organisation propriétaire du SI. Dans un contexte de cloud, la SdS d'un SI externalisé ne peut pas être totalement sous le contrôle de l'organisation cliente et gagne – en terme de robustesse face à la menace, de couverture de la menace, et de coût –, à être implantée en partie à l'extérieur de l'infrastructure virtualisée, par exemple dans le système de virtualisation (hyperviseur) des machines physiques [1, 3]. D'autre part, les reconfigurations potentiellement fréquentes de l'infrastructure virtualisée (migration de VM) mais également du SI externalisé (création ou destruction de VM) imposent que la SdS s'adapte automatiquement aux reconfigurations de l'infrastructure virtualisée. La SdS doit donc, au moins partiellement, être effectuée par l'infrastructure de cloud.

Notre objectif est de permettre à l'opérateur de cloud d'offrir dans ses SLAs un volet sur la SdS (une forme de Security as a Service). Une organisation cliente devrait être capable de spécifier simplement ses besoins en SdS (vulnérabilités à surveiller) et de définir, dans son contrat avec l'opérateur de cloud, un compromis entre l'efficacité de la SdS et ses coûts (e.g. dégradation de performance fonctionnelle, allocation de parties de ressources partagées). L'opérateur de cloud devrait donc disposer pour cela d'un service qui, à partir des SLAs des organisations clientes, configure automatiquement les composants de SdS qui sont sous son contrôle, et les adapte automatiquement aux reconfigurations des infrastructures virtualisées.

Grâce à cette capacité de l'opérateur de cloud à automatiser la configuration de la SdS dans son périmètre, les organisations clientes d'une part conservent une maîtrise de la sécurisation de leur SI, et d'autre part ne voient qu'une complexité supplémentaire minime pour sécuriser un SI externalisé. Ce dernier point est d'autant plus important que la SdS intervient lorsque le coût pour corriger des vulnérabilités est déraisonnable.

## Références


Tal Garfinkel and Mendel Rosenblum. A Virtual Machine Introspection Based Architecture for Intrusion Detection. 10th ISOC Annual Symposium on Network and Distributed Systems Security Symposium (NDSS'03). February 2003, San Diego, California, USA.

Angelos D. Keromytis, Roxana Geambasu, Simha Sethumadhavan, Salvatore J. Stolfo, Junfeng Yang, Azzedine Benameur, Marc Dacier, Matthew Elder, Darrell Kienzl, Angelos Stavrou. The Meerkats Cloud Security Architecture. 3rd IEEE International Workshop on Security and Privacy in Cloud Computing (ICDCS-SPCC), June 2012, Macao, China.

Sylvie Laniepce, Marc Lacoste, Mohammed Kassi-Lahlou, Fabien Bignon, Kahina Lazri, and Aurélien Wailly. Engineering Intrusion Prevention Services for IaaS Clouds: The Way of the Hypervisor. 7th IEEE International Symposium on Service-Oriented System Engineering (SOSE 2013), March 2013, Redwood City, California, USA.

Damien Riquet, Gilles Grimaud, and Micha´el Hauspie. DISCUS: A massively distributed IDS architecture using a DSL-based configuration. 2014 International Conference on Information Science, Electronics and Electrical Engineering (ISEEE 2014), April 2014, Sapporo City, Hokkaido, Japan.

Laurent Bobelin, Aline Bousquet, Jérémy Briffaut, Jean-Francçois Couturier, Christian Toinard, Eddy Caron, and Arnaud Lefray. An Advanced Security-Aware Cloud Architecture. 2014 IEEE International Conference on High Performance Computing & Simulation (HPCS 2014), July 2014, Bologna, Italia.

Yangyi Chen, Vincent Bindschaedler, Xiaofeng Wang, Stefan Berger, Dimitrios Pendarakis. Elite: Automatic Orchestration of Elastic Detection Services to Secure Cloud Hosting. 18th International Symposium on Research in Attacks, Intrusions, and Defenses (RAID 2015),

November 2015, Kyoto, Japan.

**Mots-Clés:** supervision de sécurité, détection d'intrusion, virtualisation, cloud, SLA, auto, adaptation