Les impacts de la cloudification sur la surveillance opérationnelle

Laurent Cordival, Fabien Thurot, Florian Boudot, Matthieu Riche, Edouard Weber

Beijaflore, 11-13 Avenue du Recteur Poincaré, 75016 Paris, France

Abstract.
Les évolutions technologiques liées à l'utilisation du cloud (comme la conteneurisation et les micros-services) et aux changements des pratiques des services IT (comme le DevOps [1]) sont autant d'évolutions auxquelles les centres opérationnels de sécurité (SOC) doivent faire face.
Afin de maintenir la qualité de leur dispositif de cyberdéfense, les responsables sécurité et responsables SOC [2] doivent gérer les impacts de l'utilisation de services Cloud. L'étude ci-dessous est un état de l'art des pratiques mises en œuvre par les différents SOC pour répondre à ces nouvelles contraintes.
Les difficultés d'adaptation des processus et des organisations aux Clouds par les services IT compliquent la tâche du responsable SOC dans l'intégration des applications Cloud dans les outils de supervision de sécurité.
Pour pallier ces problématiques, ainsi que le modèle multi-cloud, les SOCs s'adaptent et se tournent vers les capacités de surveillance dont disposent les Cloud Security Providers (CSP). Ces services ne suffisent pas à établir une surveillance complète, mais permettent au SOC de se concentrer davantage sur le déploiement d'outils de surveillance applicative et de gestion des accès (Cloud Access Security Broker).
Les évolutions et travaux entrepris par les CSP tendent vers la standardisation des services de détection, une modélisation des alertes détectées et le développement d'interface d'investigation. Ces services représentent une grande opportunité de renforcer le niveau de détection et de réaction des entreprises

Keywords: Cloud, SOC, SIEM, SOAR, Puits de données, sondes de détection, CASB, intégration de service Cloud, CSP, SaaS, cyber défense, Machine Learning

1 Introduction

Les fournisseurs de services Cloud (CSP) sont depuis quelques années une cible de choix pour les cyber-attaques. Ces attaques sont essentiellement liées à la multiplication des services utilisés par les clients à tous les niveaux (Infrastructure as a Service - IaaS, Platform as a Service - PaaS ou Software as a Service - SaaS).

Aujourd'hui au cœur de la transformation digitale, les applications Cloud sont fortement utilisées par les entreprises. Ces applications sont considérées comme un levier

important pour la production de services internes et externes. Les Clouds offrent d'avantages de flexibilité comparés aux infrastructures on-premises et sont aussi une solution simple et efficace aux besoins croissants d'innovation des entreprises.

Pour supporter les services selon la demande, les CSP présentent plusieurs alternatives d'utilisation et de coût : Cloud public et Cloud privé. Le premier s'adapte rapidement à l'augmentation des besoins et permet l'hébergement mutualisé entre les clients : chacun dispose de son propre accès à une sous-partie du Cloud sans visibilité sur une autre sous-partie. Le dernier est entièrement dédié : il n'admet qu'une seule entreprise, permet d'avoir une maîtrise plus complète sur le contrôle des données et l'infrastructure, pour un coût supérieur et une adaptation moins réactive. L'état de l'art présenté ici se focalisera sur les Clouds publics, indifféremment du modèle de service utilisé (SaaS, PaaS, IaaS).

Du fait de la migration progressive des environnements IT dans les Clouds, la sécurisation du Cloud est essentielle pour garantir la sécurité des données et la confiance accordée à ces services. Dès lors, la supervision sécurité se doit d'anticiper cette migration en déployant des moyens de contrôle sur les environnements Clouds. La problématique actuelle est d'assurer un niveau de contrôle satisfaisant sans remettre en question le modèle économique lié à l'utilisation de ces services. Cette évaluation du niveau de contrôle sur les environnements Cloud doit également s'interroger sur la délégation de la supervision aux fournisseurs de Cloud.

2 Les impacts de la cloudification sur la surveillance opérationnelle

Les impacts de la cloudification sont de deux types. La première est l'adaptation au changement des procédures et des outils des SOC. La deuxième est l'utilisation très fréquente de multiples fournisseurs de services Cloud.

2.1 Les grandes problématiques du Cloud pour la supervision

L'utilisation du Cloud entraine une complexification des risques et enjeux liés à la gouvernance et à la maitrise du SI. La diversification des environnements se traduit par une augmentation de la surface d'attaque sur quatre niveaux distincts :

- La couche hyperviseur, avec un risque de perte de contrôle sur les différentes Machines virtuelles (VMs). Une grande variété d'attaques est possible dont notamment : HyperJacking, BLUEPILL, Vitriol, SubVir, DKSM ;
- Les vSwitch, présentant des risques et des attaques similaires aux infrastructures réseaux on-premises ;
- Les VMs en elles-mêmes, vulnérables aux attaques traditionnelles. Elles permettent de plus la possibilité d'attaques VM-to-VM (VM jumping), complexifiant la détection ;
- Les applications ou services au travers d'usages frauduleux ou malveillants.

En plus de cette augmentation de la surface d'attaque, la nature complexe et dynamique du Cloud est également source de nouvelles menaces à prendre en compte pour le SI :

- Différents utilisateurs peuvent partager la même infrastructure ;
- La complexification et l'augmentation des charges dues au Cloud peuvent être difficiles à gérer ;
- Le risque de perte de contrôle sur les données et systèmes ;
- La virtualisation des systèmes et la scalabilité dynamique engendrent une topologie du réseau variable, rendant difficile la réalisation d'un inventaire fiable sur lequel s'appuyer et donc de mettre en place une politique efficiente de gestion des risques et des vulnérabilités.

L'utilisation partagée de ses nouveaux environnements induit une augmentation des risques de cyber-sécurité. Ces risques, qui pèsent sur l'ensemble des infrastructures et ses utilisateurs, doivent être surveillés et contrôlés par le SOC.

Il faut alors repenser la stratégie de détection et de réponse aux incidents.

La cloudification pose de nouvelles problématiques pour l'analyse et la réponse aux incidents. Certaines entreprises sont tentées de se reposer sur les méthodes et moyens techniques traditionnels que l'on peut retrouver sur des environnements on-premises. Avec l'usage de micro-services, les VMs et containers sont créés et détruits en permanence, leur durée de vie se compte en jours voire en heures. L'installation et l'enrôlement d'agents deviennent alors une contrainte et non plus un avantage.

Aussi, ces derniers ne sont pas déployables sur des environnements SaaS. Le périmètre maîtrisé peut vite se réduire lors d'un déploiement Cloud si les bonnes méthodes ne sont pas employées.

Au-delà de la récupération des évènements et des logs, il faut être en capacité de les interpréter. Il peut être difficile d'obtenir un niveau de logs satisfaisant sur les infrastructures Cloud, pour des raisons contractuelles ou pour des raisons d'usage ou de fonctionnalités (IaaS, PaaS, SaaS…).

La vitesse d'évolution des outils et services consommés dans le Cloud peut poser des problèmes lors de la phase de collecte voire de stockage pour investigation. Dans un monde où la donnée est produite par de nombreux services à différentes échelles, la maîtrise de la volumétrie peut rapidement devenir un enjeu pour assurer un traitement par le SOC (sur le coût, la charge de travail, etc.).

La dernière des grandes problématiques du Cloud pour le SOC est la difficulté de répondre à un incident. Cette difficulté peut notamment provenir des points suivants :

- La délégation de contrôle sur les infrastructures Cloud qui complexifie la réponse à incident. Suivant le niveau de contractualisation, il est nécessaire de passer par le CSP pour effectuer des actions techniques ;
- La maîtrise des fonctionnalités Cloud et la modularité disponible pouvant limiter les possibilités d'intervention du SOC ;
- La capacité de communication et d'échange entre les équipes de réponse à incident et celle du CSP.

2.2 Comment les SOC répondent à ces contraintes lors du déploiement de l'infrastructure Cloud ?

En amont de l'intégration du Cloud dans la surveillance de sécurité, il est nécessaire de mettre en place une gouvernance sécurité autour du Cloud. Celle-ci doit définir les politiques suivantes :

- Gouvernance des usages du Cloud ;
- Gouvernance du Prestataire de Services.

Une fois la gouvernance établie, le responsable SOC devra établir une politique de détection et de réaction sur les environnements Clouds.

Pour cela, il est nécessaire de répondre aux problématiques de maîtrise du périmètre, de la gestion à la réponse à incident grâce à une intégration technique du Cloud au SOC. Ces points seront traités par la suite.

Cette intégration permettra de revenir sur des processus déjà mis en place et plus ou moins maîtrisés en fonction de la maturité de l'entreprise. Ces processus ne seront pas traités ici et comprennent :

- La création de scénarios de détection prenant en compte les risques et scénarios redoutés ainsi que les contraintes techniques et fonctionnelles du périmètre ;
- Le triage et l'analyse des alertes remontées ;
- Le processus d'escalade technique ou fonctionnel ;
- La réponse à incident au travers d'actions de confinement et de retour à la normale ;
- L'amélioration continue du SOC sur les aspects techniques et fonctionnels ;
- Le maintien d'une base de connaissances ;
- La montée en compétence des équipes.

Cependant, certains processus devront faire l'objet d'une adaptation : en particulier, la création des scénarios de détection doit faire l'objet d'une phase de recette renforcée compte tenu du manque de maîtrise de ces environnements.

La gouvernance des usages du Cloud

La définition des usages du Cloud est nécessaire au travers d'une politique spécifique sur la base de référentiels connus tel que l'ISO 27002 ou des référentiels plus adaptés au Cloud comme SecNumCloud, l'ISO 27017, l'ISO 27018 ou l'ISO27036. Cette politique permettra d'assurer une base saine pour la surveillance opérationnelle ce qui s'apparente à de la prévention.

Cette politique complètera la PSSI au travers de l'ensemble des exigences à respecter pour les projets Cloud notamment sur les points suivants :

- Définition des projets/données éligibles à un usage Cloud ;
- Intégration de la sécurité dans les projets Cloud ;
- Mise à disposition d'une analyse de risque qui aidera par la suite à définir la stratégie de détection voire de réponse des incidents de sécurité ;
- Activités de suivi, de mise à jour des projets et des livrables associés ;
- Audit des projets pour assurer la bonne application des exigences de sécurité ;

- Obligations techniques et fonctionnelles d'hygiène IT à respecter dans les environnements Cloud.

Une fois ce cadre d'utilisation défini, le SOC sera en mesure de suivre la conformité des projets lancés dans le Cloud. Aussi, les documents de suivi des aspects de sécurité des projets faciliteront la définition des activités de détection et de réponse sur les différents périmètres.

La gouvernance du partenaire

Au-delà de la politique Cloud définie plus tôt et de la PSSI, plusieurs aspects sont à prendre en compte avec le CSP.

Le CSP doit répondre à l'ensemble des exigences techniques et fonctionnelles de la PSSI et de la politique Cloud. L'ensemble devra faire l'objet de clauses dans le contrat et devra être revu régulièrement.

Le client doit s'assurer de la réponse aux exigences au travers d'audits réguliers à différents niveaux (nécessite une clause spécifique d'auditabilité) complétés par des certifications du CSP qui attesteront de sa maturité sur certains sujets. Attention à néanmoins maîtriser ce qu'impliquent les certifications et le niveau de sécurité/service qu'elles attestent.

La bonne gestion d'incidents Cloud nécessite de définir l'organisation et les processus de communication entre le SOC et le CSP. Dans un premier temps, il faut définir les typologies d'incidents qui feront l'objet d'une notification. Ensuite, pour chacun des types d'incident, la méthode de communication, le niveau de détail et les délais de notification seront définis. La communication peut prendre plusieurs formes :

- Définition d'un contact privilégié pour le SOC, permettant un échange régulier sur les vulnérabilités et incidents à traiter ;
- Mise à disposition d'une interface technique de supervision pour récupérer les informations/alertes sur l'environnement Cloud permettant au SOC de récupérer les notifications du CSP et/ou plus rarement de suivre l'implémentation des correctifs sur les différentes couches de l'environnement ;
- Ces interfaces seront notamment indispensables dans des environnements multi-Cloud pour s'interfacer avec les fonctionnalités ou les services de détection et/ou réponse offerts par les CSP. Le terme Hyper SOC (ou inter SOC) sera alors utilisé ;
- L'intégration du Cloud au SOC.

Approche conventionnelle

Les méthodes conventionnelles peuvent être envisagées sans être recommandées sur des déploiements Cloud de faible complexité au travers des méthodes suivantes :

- Utilisation de scripts ;
- Installation d'agents (hors ceux fournis par le CSP) ;

- Usage des fonctionnalités des briques OS ou Software portées par l'infrastructure cliente (hors fonctionnalités Cloud qui sont traités dans la partie suivante).

Elles seront notamment intéressantes lors d'usages de type IaaS et/ou PaaS qui in fine restent assez proches d'un déploiement on-premise. Le SOC traitera alors le Cloud comme une extension de son périmètre initial permettant ainsi de revenir assez rapidement à un schéma connu et plus ou moins maîtrisé en fonction de la maturité du client.

Néanmoins pour des déploiements Cloud plus complexe, avec notamment l'usage de micro-services, de conteneurs ou de SaaS, un changement d'approche serait nécessaire et permettrait d'atteindre un tout autre niveau de maturité.

Nouvelle approche

Les services Clouds fonctionnent sous forme d'Application Programming Interface (API) permettant d'exécuter des charges de travail sur l'environnement du CSP. Ces appels d'API sont la principale source d'information pour la surveillance de l'utilisation, la modification et la configuration des services au sein d'un CSP.

Certains CSP fournissent des fonctionnalités avancées spécialement pensées pour répondre aux enjeux de sécurité du SOC (Maîtrise du périmètre, détection et réponse à incident).

Ces fonctionnalités/services permettront de répondre à différentes problématiques identifiées précédemment :

- Maîtrise du scope

En vue de donner une vue globale et/ou détaillée en fonction du besoin sur tout le périmètre avec par exemple sur Amazon, AWS Config et AWS System Manager Inventory ou sur Azure les services Azure Resource Management en complément de Azure Service Map.

- Traçabilité

Les évènements (Service, réseau, système, utilisateur, requête API, etc.) sur l'ensemble du périmètre Cloud pourront être récupérés via CloudTrail, CloudWatch, et flux VPC sur Amazon et sur Azure via Activity log, Monitor, Network Watcher. Une fois en possession des logs, le SOC pourra appliquer une méthodologie standard de détection via création de scénarios de détection ou d'application d'approche de Threat Hunting.

- Surveillance de sécurité et analyse (détection de sécurité)

Pour renforcer la capacité de détection au-delà des éléments qui ont été évoqués précédemment, le SOC pourra faire appel à des fonctionnalités de détection avancées sur les

périmètres Cloud au travers par exemple de Azure Security Center ou de AWS GuardDuty. Ces services assureront la surveillance du périmètre à la recherche d'anomalies (UEBA), d'erreurs humaines, d'actes malveillants ou d'indices de compromission (IOC) et notifieront le client en cas d'alertes (via alertes standards ou via réinjection dans le SIEM ou SOAR).

A noter que ces solutions ne facilitent l'investigation (au-delà de la détection en temps réel) que si les fonctionnalités de stockage d'évènements sont utilisées sur les environnements Cloud respectifs.

- Réponse à incident

La stratégie de réponse débutera sur une phase de confinement pour aboutir à une phase de remédiation.

- Confinement

  Cette thématique pourra être abordée à différents niveaux (système, réseau, service/applicatif). Au niveau réseau et système, le SOC pourra s'intéresser au Network Security Group pour Azure ou Security Group pour Amazon en vue de confiner les environnements avec granularité (du simple système à un ensemble de systèmes voire de réseaux).
  Les autres techniques de confinement restent similaires aux fonctionnalités conventionnelles (Azure AD ou AWS Organisation sur l'aspect identité et accès, utilisation de pare-feu virtuel sur la réponse réseau, etc.).
  L'usage de solutions type EDR n'est pas propre au Cloud mais reste une bonne réponse à la problématique dans le cadre de IaaS et de PaaS.
  Concernant la réponse applicative notamment sur du SaaS, tout dépendra de la solution utilisée. Le plus souvent la gestion des identités et des accès répond à la majorité des besoins. Le cas échéant, il sera nécessaire de s'assurer en amont du choix de la solution qu'elle répond au besoin de sécurité via des fonctionnalités et API.

- Réponse à incident

  En vue de faciliter la réponse à incident le SOC devrait s'assurer la mise en œuvre des bonnes pratiques suivantes sur les parties système et donnée (même si elles ne sont pas nécessairement à la main du SOC) :

  - Assurer la présence de snapshots pour faciliter la reconstruction de VM au niveau du système, de la configuration voire de la donnée (via AWS Session Manager ou Azure Backup).
  - Avoir scripté/automatisé la construction/reconstruction des environnements à la volée (Infrastructure as code). Cela nécessite néanmoins des applications stateless ou un point d'attention devra être accordé pour la récupération de la donnée.

Au-delà de la partie système et donnée, le retour à l'état initial (ou avant compromission) devra être assuré sur l'environnement Cloud dans sa globalité. Le SOC pourra s'appuyer sur la définition de référentiels ou sur la sauvegarde des éléments importants pour répondre à la problématique. Ces derniers seront utilisés si identifiés nécessaires lors de l'analyse (identification de changements malveillants de l'environnement Cloud, au niveau des droits, des configurations, des codes de déploiement, etc.).

Il est important de connaître l'ensemble des fonctionnalités proposées, notamment au travers de leurs forces et faiblesses. Plusieurs possibilités seront envisageables :

- Accepter la solution avec ses forces et ses faiblesses ;
- Développer des méthodes/processus pour pallier les limites identifiées ;
- Trouver une autre solution ou utiliser plusieurs solutions pour répondre au besoin.

Attention néanmoins à ne pas complexifier les déploiements Cloud plus que nécessaire.

Les CSP permettent souvent de tester ces fonctionnalités pendant plusieurs jours, ce qui permet facilement au SOC d'évaluer le gain par rapport à la complexité et aux limites des fonctionnalités.

Des solutions propriétaires peuvent aussi être envisagées pour compléter les capacités du Cloud et du SOC. Il sera alors intéressant de regarder les partenaires des CSP en vue d'identifier les solutions qui seront le plus facilement intégrables dans l'environnement CSP et par la même occasion les plus faciles à maintenir dans le temps.

2.3 Les challenges des environnements Multi-Cloud

L'interopérabilité des plateformes et la standardisation des évènements

L'absence actuelle de standardisation sur les solutions de supervision des CSP amène les responsables de SOC à devoir intégrer les différentes sources de log au sein d'une même plateforme SIEM, permettant de globaliser la détection. L'intégration d'événements de différents types au sein du SIEM se fait en plusieurs étapes :

- Identification des journaux d'événements pertinents à collecter pour les différents services ;
- Déploiement d'agents de collecte, interrogation d'APIs de log management, lorsqu'elles sont disponibles ou configuration d'envois réguliers des évènements générés ;
- Mise en place d'un puits de données assurant le parsing, la normalisation, l'enrichissement, l'indexation et le stockage des événements (e.g. ELK).

Le SIEM assure ensuite la détection via des règles de corrélation sur les événements présents dans sa base de données. Les données sont également accessibles pour les enquêtes réalisées par les différentes équipes SOC et CSIRT (analyse et investigation).

La multiplication des solutions Cloud et l'absence de standardisation des événements entraine la nécessité d'une différenciation des différentes règles implémentées en fonction des technologies supervisées, empêchant le déploiement de use cases globaux. En effet, l'utilisation de services de Cloud/SaaS public limite la capacité à customiser le niveau de logs, et rend donc la supervision dépendante du niveau de service offert par le CSP. Les règles de corrélation du SIEM deviennent donc nombreuses et très spécifiques, rendant plus difficile le suivi de la supervision.

En conséquence, les solutions de supervision évoluent actuellement afin de faciliter ces différents types d'interconnexion et le maintien en condition opérationnel et de sécurité, et ainsi tenter de résoudre ces problématiques. Les choix technologiques bénéficient des avancées autour des puits de données, permettant de renforcer la scalabilité des plateformes.

La dernière étape nécessaire à cette mutation est la standardisation des évènements communiqués aux clients des CSP afin de faciliter l'implémentation transverses de use cases de détection et d'éviter cette problématique d'adaptation des use cases aux différentes technologies.

L'orchestration des services de « Managed Detection and Response »

Les équipes SOC en constante recherche de gain d'efficacité vont devoir à terme utiliser des services mettant à disposition un niveau abstraction supérieur à la collecte de logs chez les différents CSP. Ces services vont permettre à chaque fournisseur CSP de déployer des solutions d'analyse automatisées à base de Machine Learning sur des use cases conçus spécialement pour les usages classiques de leurs services, permettant une spécialisation et une amélioration de la détection. L'utilisation de ces services de MDR va donc se développer, mais nécessitera un certain nombre d'évolutions afin de s'adapter à ce nouveau paradigme.

On observe tout d'abord un processus de standardisation des différentes formalisations : use cases (e.g. ETSI), Threat Intelligence (e.g. STIX/TAXII), référentiels TTP (e.g. Killchain, MITRE ATT&CK). Cette standardisation facilite l'orchestration entre les différents services et technologies, ainsi que l'automatisation de la réponse vers des processus « end-to-end », en permettant à des acteurs pluriels de se comprendre et de communiquer plus facilement.

Dans un second temps, de nouveaux outils sont nécessaires à l'orchestration et l'automatisation de services de MDR: SOAR, EDR, plateformes de Threat Intelligence. Ces outils reprennent des technologies existantes en les enrichissant avec les dernières

évolutions en matière d'intégration de standards, de frameworks, et profitent notamment du développement de l'IA. Ces outils visent à soulager les équipes SOC et CSIRT des tâches bas niveaux, leur permettant de se concentrer sur les actions à plus hautes valeurs ajoutées, et d'améliorer l'interopérabilité entre les différentes entités de la détection et de la réponse.

Autre enjeu, l'accessibilité aux sources de données des différents outils et plateformes, à des fins d'investigation, se présente comme un challenge majeur avec de multiples acteurs à faire inter opérer. A cela s'ajoute l'ensemble des contraintes réglementaires et d'entreprise, notamment de confidentialité et d'anonymisation. Des protocoles tels que le TLP (Traffic Light Protocol) visent à apporter des solutions à ces problématiques.

Enfin, il est aujourd'hui difficile d'avoir une vision claire sur le marché des MDR. Un besoin de certification des différents services devient donc crucial et d'un intérêt majeur pour les prochaines années, sur le modèle des initiatives de l'ANSSI avec les certifications PDIS et PRIS pour les prestataires de détection et de réponse à incident dans le cadre de la LPM.

Le renforcement des services d'investigation

Les environnements Cloud développent des services de détection et de réponse à incident dédiés et spécifiques sur leur périmètre et leurs technologies. Ces services seront spécialisés et disposeront de compétences de pointes avec des développements spécifiques pour répondre au besoin de leur environnement et des clients communs au CSP. Ils pourront s'interconnecter au SOC interne central des entreprises qui souhaitent profiter de ces services.

Le SOC interne à l'entreprise pourrait se placer alors en interface ou en coordination avec les SOC CSP pour gérer les incidents de bout-en-bout en disposant de compétences pointues sur les environnements impactés via les services du CSP tout en apportant de leur côté la connaissance transverse du contexte et du métier si nécessaire.

3 Conclusion

Le développement rapide du Cloud s'accompagne aujourd'hui de changements profonds : standardisation des services de détection, modélisation des alertes détectées, moteur commun de détection d'attaques, et développement d'interfaces d'investigation fiables et automatisables pour les clients chez les fournisseurs.

La règlementation sur la sécurité des tiers et des services numériques doit pouvoir faciliter cette convergence de service de détection, absolument nécessaire à la réduction des risques de cyber sécurité : cybercriminalité, espionnage et sabotage…

Les fournisseurs de services Clouds auront tout intérêt à suivre cette évolution en investissant dans la certification de leur service de détection et dans leur interopérabilité pour assurer la protection des données contre des attaques toujours plus avancées et renforcer ainsi la confiance de leurs clients.

References

1. Willis, J., Debois, P., Humblej J., Kim, G.: The DevOps Handbook. IT Revolution Press, Release Date: October 2016, ISBN: 9781457191381
2. Zimmerman, C,: Ten Strategies of a World-Class Cybersecurity Operations Center, In: The MITRE Corporation (2014).
3. Exigences SecNumCloud, v3.1 Agence Nationale de la Sécurité des Systèmes d'information, https://www.ssi.gouv.fr/
4. Latifa Ben Arfa Rabaia, Mouna Jouini, Anis Ben Aissa, Ali Mili: A cybersecurity model in cloud computing environments. In: Journal of King Saud University - Computer and Information Sciences, Vol. 25, pp. 63-75 (2013).
5. Amani S. Ibrahim, James Hamlyn-Harris, John Grundy: Emerging Security Challenges of Cloud Virtual Infrastructure. In: Proceedings of APSEC 2010 Cloud Workshop (2010).