Architecture technique

Dématérialisation d'un processus de paiement

COMETS Jean-Marie
DELMARRE Adrian
REYNOLDS Nicolas
TURPIN Pierre

30 octobre 2014

Table des matières

1 Présentation générale

Dans la suite du document, les sous-systèmes suivront la nomenclature suivante :

serveurs de dialogue borne la machine contenant le serveur de dialogue principal sera noté B, les machines de repli seront notées Bn.

serveurs de base de données la machine contenant le serveur de base de données principal (maître) sera noté BDD, les duplicats seront notés $BDDn$, les archives seront notées $BDDa$.

serveurs d'application la machine contenant le serveur d'application principal sera noté X, les machines de repli Xx, avec X respectivement E, C, U et A pour les applications "gestion commerçant", "gestion entreprise", "gestion utilisateur" et "gestion Aventix".

2 Choix de la solution cloud

3 Passage à l'échelle (scaling)

4 Sécurité

4.1 Infrastructure

En choisissant une solution cloud, la disponibilité de l'infrastructure est garantie par le prestataire cloud, en l'occurence **Amazon AWS**. Le système peut donc être considéré relativement sécurisé vis-à-vis des attaques par déni de service (DoS simple), ou autre attaque d'infrastructure.

De plus, la disponibilité du système est dépendante de la disponibilité d'AWS, en l'occurence celle-ci peut être garantie selon le prix de la prestation. Le taux de panne de 0% ne peut malheureusement pas être garanti, du fait du nombre de facteurs externes entrant en jeu. Cependant, un taux de 99%, voire jusqu'à 99.95% peut être garanti par AWS.

En passant par une solution cloud, le système est aussi protégé des attaques physiques (coupure générale, attaque électromagnétique, etc...), mais encore dépendant de l'infrastructure d'AWS.

4.2 Gestion du trafic indésirable

Le trafic indésirable correspond au trafic qui n'est pas directement lié à l'utilisation normale du système. Il peut être utilisé comme attaque visant à réduire exploiter des failles d'autres services présents sur la VM, ou tout simplement visant à réduire la disponibilité du système en multipliant les accés (DoS).

EC2 met à disposition un firewall pour ses instances, ce qui permet de régler son accés. Cependant, les VM étant installées à l'intérieur d'une instance, elles

FIGURE 1 – Emplacements géographiques possibles des instances EC2

doivent toutes être configurées séparément pour accepter uniquement le trafic qui les concerne.

4.2.1 Fermeture maximale

Un document relatant des conseils de sécurisation d'instance EC2, produit par ce même service, est disponible à l'adresse suivante : `http://aws.amazon.com/articles/1233/` (en date du 30 octobre 2014).