Architecture technique

Dématérialisation d'un processus de paiement

COMETS Jean-Marie
DELMARRE Adrian
REYNOLDS Nicolas
TURPIN Pierre

3 novembre 2014

Table des matières

1 Présentation générale **3**

2 Choix de la solution cloud **4**

3 Passage à l'échelle (scaling) **4**

4 Sécurité **4**
4.1 Sécurité d'infrastructure 4
4.2 Sécurité du trafic 4

1 Présentation générale

La figure 1 détaille l'architecture technique choisie. Cependant, certains points doivent être justifiés ou davantage expliqués.

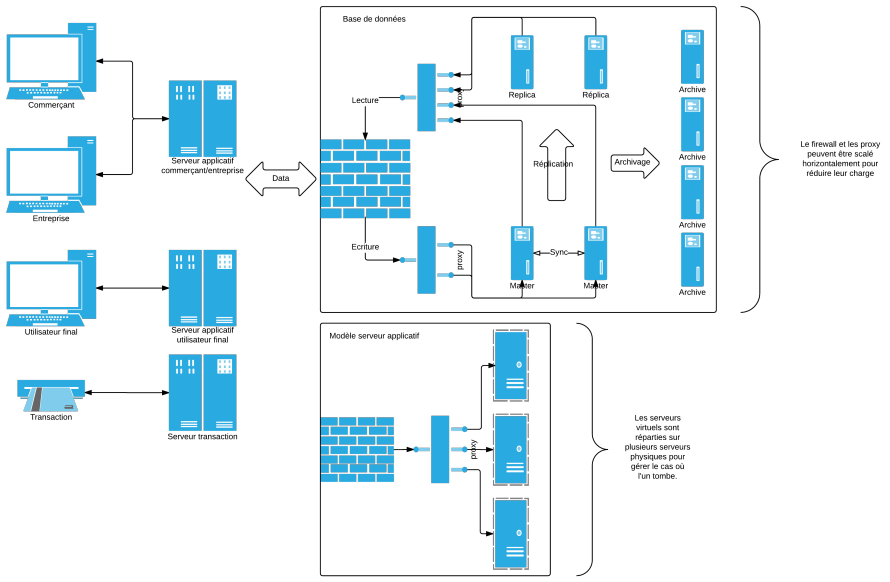

FIGURE 1 – Schéma général de l'architecture technique choisie

Serveurs applicatifs L'accès aux serveurs applicatifs est gouverné par une couche **firewall** et une couche **proxy**. La couche firewall est nécessaire pour gérer le trafic indésirable (se référer à la section 4.2 pour plus de détails). La couche proxy permet de gérer le passage à l'échelle des serveurs applicatifs.

Le principe général du passage à l'échelle des serveurs applicatifs est basé sur la duplication et synchronisation de plusieurs instances des serveurs applicatifs, avec balance de charge sur ces dernières, régie par le proxy (se référer à la section **TODO** pour plus de détails).

Base de données L'accès au sous-système de base de données est régi par un firewall, spécifiquement conçu pour le SGBD choisi. L'idée est de bloquer l'accès au sous-système de base de données au monde extérieur, autorisant uniquement l'accès au proxy servant à répartir les accès aux différentes base de données "maîtres".

De plus, cache est configuré sur les serveurs de bases de données, pour réduire la latence due à l'accès au sous-système de base de données, ainsi que de réduire la charge qui lui est soumise.

2 Choix de la solution cloud

3 Passage à l'échelle (scaling)

4 Sécurité

4.1 Sécurité d'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 assurée selon le prix de la prestation. Le taux de panne de 0% ne peut malheureusement pas l'être, du fait du nombre de facteurs externes entrant en jeu. Cependant, un taux de 99%, voire jusqu'à 99.95% peut l'être par AWS (source : `http://aws.amazon.com/ec2/sla/`).

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.

Toutefois, une exception aux propositions demeure : le **sous-système de base de données ne réside pas intégralement dans le cloud**. Ce problème n'est pas d'une ampleur catastrophique, il faut noter qu'on est relativement bien protégé des attaques DoS grâce au pare-feu conçu spécifiquement pour contrôler l'accès et donc empêcher le trafic intempestif.

Malheureusement les attaques physiques peuvent atteindre le sous-système de base de données, c'est la faiblesse majeure du système. Pour limiter davantage la vulnérabilité physique du système, deux baies de serveurs en syncronisation multi-master seront installées sur deux locaux différents (détaillé dans la section **TODO**.

4.2 Sécurité du trafic

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 exploiter des failles d'autres services présents sur la VM, ou tout simplement à réduire la disponibilité du système en multipliant les accès (DoS).

EC2 met à disposition un firewall pour ses instances, ce qui permet de régler son accès. Cependant, les VM étant installées à l'intérieur d'une instance, elles doivent toutes être configurées séparément pour accepter uniquement le trafic qui les concerne.

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 3 novembre 2014). L'idée est simplement de n'autoriser que le trafic qui est attendu, et par défaut de bloquer toute connexion entrante ne correspondant pas à une règle spécifiée.

Chiffrement des messages La totalité des échanges de messages avec le système sera effectuée en utilisant une authentification par clé. Il faudra par exemple acheter un **certificat SSL** pour permettre l'utilisation du protocole HTTPS pour accéder aux différentes applications web. Le dialogue avec les bornes sera quant à lui chiffré par une méthode utilisant la cryptographie asymétrique (clé publique).