Offre sites internet

V1.4

De nombreuses sociétés de service et agences multimédia proposent le développement et l'hébergement de sites Web.

Peu d'entre elles se soucient réellement de la sécurité de vos données et de la continuité de service dont dépend votre activité.

Derrière la façade :

- Que se passe-t-il quand vous souhaitez changer de prestataire ?
- Où se trouvent vos données ?
- Combien de temps votre site va rester coupé suite à des problèmes d'infrastructure serveurs et réseaux ?
- Combien de temps pour restaurer une sauvegarde vous faut-il ?
- etc…

Découvrez les solutions à valeur ajoutée de JMS Informatique.

Sommaire

1. La sécurité de vos données – le modèle JMS
2. L'offre d'hébergement sécurisé
3. Sauvegarde (réplication et rétention) – continuité de service
4. La sécurité de fonctionnement – la politique
5. Pare-feu pour les applications Web (WAF)

Sécurité des données

Le modèle JMS

Le concept JMS

- La réflexion du modèle de sécurisation des données sur internet JMS s'est architecturée autour de 3 axes principaux :
  - Proposer à nos clients des coûts accessibles en conservant des niveaux de service optimaux
  - Garantir une continuité de service proche du 100% à nos clients qui ont leur activité sur Internet
  - Assurer la protection des données en ligne et être capable de redémarrer l'activité immédiatement en cas de désastre site

Choix et solutions

- Un constat s'est imposé rapidement :
  - Les coûts d'infrastructure des solutions traditionnelles de continuité de service (clustering, stockage répliqué, …) et de sécurisation (firewalls matériel, load balancers, dispositifs de filtrage, …) sont importants et incompressibles sauf à dégrader le service rendu.
  - Nos clients ont besoin de solutions simples et sécurisées n'engendrant pas de coûts d'exploitation supplémentaires, en formation et personnel.
- Les solutions JMS à ces questions :
  - De multiples sites sécurisés à travers le monde
  - Une infrastructure agile, simple, facile à dupliquer
  - Une sécurisation par la copie, avec une fréquence de réplication adaptée au besoin client
  - Des composants applicatifs de sécurisation de qualité
  - Le cryptage des sauvegardes, garantie d'une confidentialité des données pendant les transferts, et un niveau de rétention flexible

Offre d’hébergement sécurisé

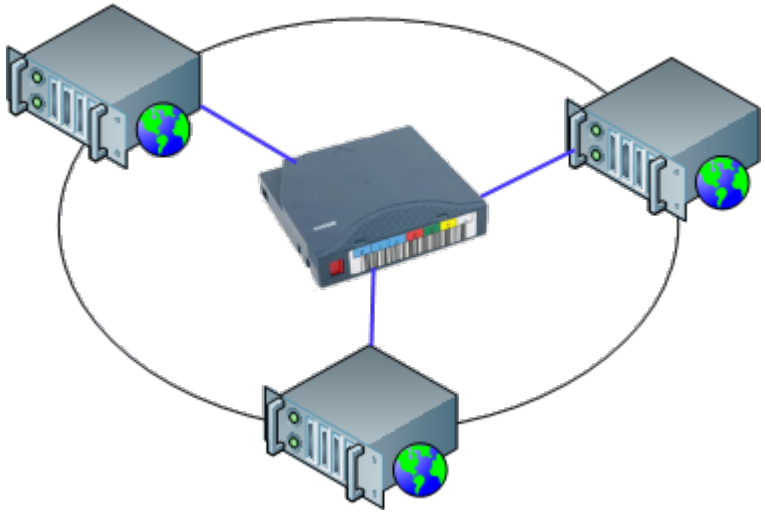
L’infrastructure JMS Informatique

- 4 localisations indépendantes pour 100% de continuité de service
  - Serveur principal dédié : OVH France (Roubaix)
  - Serveur secondaire dédié (1/2) : planetHoster (Paris)
  - Serveur secondaire dédié (2/2) : iCloudHosting dans le nord de Londres (Hemel Hempstead), TIER-4, 100% résilient sur les données avec un data centre secondaire situé à Birmingham dans les Midlands
  - 1 VPS situé à Phoenix, Arizona, chez I/O Flood (supervision et gestion des bascules)

100% uptime – localisations indépendantes – marchés US et européens

Sauvegardes & réplication

Continuité de service garantie



Localisations

- Fort de ses 4 localisations indépendantes et géographiquement éloignées, JMS Informatique garantit :
  - une disponibilité maximale de vos sites Web
  - Un site maitre actif et 2 sites secondaires prêts à reprendre le service en cas de défaillance du maitre, de quelque nature que ce soit, hardware ou liée à une défaillance logicielle
  - Une plateforme de supervision temps réel et une gestion des bascules manuelle ou automatisée suivant les besoins.

100% de disponibilité

avec une infrastructure légère et peu coûteuse

Mécanismes de réplication

- Tous les jours, votre site complet est répliqué du maitre vers les 2 emplacements secondaires.

- La fréquence peut même être portée à plusieurs fois par jour suivant la criticité de votre activité.

- Des copies locales peuvent être envoyées sur votre infrastructure de sauvegarde, et sur le stockage dans le cloud (Dropbox, Sugarsync, Amazon S3, …) , cryptées pour toujours plus de sécurité.

100% de garantie

de conservation de données par la copie

Rétentions

- JMS Informatique dispose d'une grande flexibilité sur ses équipements de stockage, vous garantissant une rétention sur mesure.

- De plusieurs backups par jour, à une conservation allant jusqu'à une année, vous gardez l'historique de vos évolutions et de vos datas

Remontez de 1 jour à 1 an vos sauvegardes

Sécurité de fonctionnement

Dispositifs de sécurité applicatifs

- JMS Informatique a développé une politique de sécurité adapté aux besoin de chacun de ses clients, dont les grandes lignes directrice sont :
  - Maintien en conditions opérationnelles
  - Protection des front-end et back-end d'administration
  - Optimisation des codes et des bases de données

Détails des opérations (1/2)

- Derrière les mots, JMS Informatique a intégré des solutions du marché pour garantir la meilleure sécurité de fonctionnement à ses clients, et ses actions au quotidien sont concrètes :

  - Maintien en conditions opérationnelles (MCO) :
    - ↪ Application des patchs d'évolution et des patchs de sécurité des frameworks, CMS et extensions utilisées, dès leur mise à disposition, afin de prendre des mesures préventives sur les failles découvertes
    - ↪ Application de gestions des droits sur les fichiers et dossiers
    - ↪ Vérification quotidienne des états de réplication et de sauvegardes
    - ↪ Tests de plan de reprise d'activité à intervalles réguliers

Détails des opérations (2/2)

- Protection des front-end et back-end d'administration
  - ↪ Gestion de listes blanches et listes noires d'IP (adresses et ranges) d'accès au site
  - ↪ Masquage de l'accès au back-end d'administration par URL secrète
  - ↪ Protection par .htaccess
  - ↪ Blocage géographique
  - ↪ Protection contre le brute force : blocage des IP automatique sur des logins répétitifs infructueux
  - ↪ Génération automatique de rapports d'exception de sécurité
  - ↪ Alertes en temps réel au support niveau 1 JMS Informatique

- Optimisation des codes et des bases de données
  - ↪ Analyse de modification des codes source par rapport à un état validé sain
  - ↪ Alerte automatique générée sur les modifications de fichiers par rapport à l'état initial
  - ↪ Optimisation quotidienne des bases de données (MySQL et PostgreSQL)

Pare-feu applicatif WEB

--== WAF ==--

[*Web Application Firewall*]

Quel est son rôle ?

En plus de fonctionner comme un pare-feu standard, un WAF exerce des fonctions traditionnellement assurées par plusieurs systèmes tels que :

- le filtrage des contenus et le filtrage antispam,
- la détection d'intrusion,
- et l'antivirus.

A travers différents modules décrits après, le WAF permet une automatisation de l'analyse des trames, des requêtes et des fichiers téléchargés, et un blocage des comportements suspects.

Doté d'une fonction d'apprentissage et d'une fonction de gestion des exceptions, il permet de séparer finement les comportements autorisés de ceux qui menacent votre site et votre activité.

Zoom sur les protections du WAF (1/3)

Protection contre les injections SQL :

- Détecte les attaques contre votre site par injection SQL communes et les bloque.

Protection contre les attaques de type ‘script cross-site’ (XSS shield) :

- Détecte les attaques contre votre site de type 'script cross-site' (XSS) et les bloque. Le filtrage est capable de détecter les attaques les plus courantes de ce genre, comprenant les codes malicieux Javascript et PHP.

Protection contre les robots malveillants (MUA shield) :

- De nombreux pirates vont essayer d'accéder à votre site en utilisant un navigateur configuré pour envoyer du code malicieux dans sa chaîne d'agent utilisateur (un petit morceau de texte utilisé pour décrire le navigateur à votre serveur). Leur intention est que le logiciel de traitement du journal 'buggy' analyse et permette la prise le contrôle du site web. Cette protection détecte de telles attaques et bloquent ces demandes.

Zoom sur les protections du WAF (2/3)

Protection contre les attaque de type 'Request Forgery' (CSRFShield) :

- L'une des principales préoccupations concernant les formulaires web tels ceux de connexion, de contact, etc… est qu'ils peuvent être exploités par des scripts automatisés (bots) pour envoyer des spams ou des mots de passe par force brute. Notre outil dispose de deux méthodes pour prévenir de tels abus :
  - Il effectue un filtrage de base sur la provenance de la requête. Si le navigateur du visiteur indique que la page précédente n'appartenait pas à votre site, le processus du formulaire sera bloqué.
  - en plus de la protection de base, un champ caché est automatiquement ajouté dans tous les formulaires du site.

Protection contre l'inclusion de fichier à distance (RFIShield) :

- Certains pirates vont essayer de forcer le chargement de code directement à partir de leur serveur. Cela se fait par le passage d'une requête http(s):// ou ftp:// dans l'URL pointant vers leur site malveillant. Notre solution va réagir face à ces cas en cherchant l'URL distante et en analysant son contenu. S'il est avéré qu'il contient du code, le WAF va bloquer la demande.

Zoom sur les protections du WAF (3/3)

Protection contre l'inclusion de fichier direct (DFI shield) :

- Lorsque cette option est activée, le WAF va chercher les paramètres de requête qui ressemblent à un chemin de fichier. S'il en trouve, il sera numérisé, et s'il s'avère contenir du code, la demande sera rejetée.

Protection contre les envois par scan (Upload shield) :

- Le WAF va analyser de façon proactive tous les fichiers qui sont téléchargés vers le site. Si l'un des fichiers trouvé contient une seule ligne de code malicieux exécutable, la demande est bloquée.

Filtre anti-spam basé sur une liste de mots interdits :

- Toutes les requêtes contenant un des mots mis en liste des ‘Mots interdits’ seront bloquées.

Nos points forts

- Vous être propriétaire de votre site, vous disposez en temps réel de sa structure et de ses données, et vous êtes libre de choisir votre partenaire hébergeur.
- A moindre coût et avec une infrastructure agile, JMS Informatique vous garantit une continuité de service proche du 100% par la réplication et ses implantations géographiques indépendantes.
- Votre site est protégé contre les attaques extérieures et le hacking grâce à notre pare-feu applicatif.
- En cas de désastre site, le redémarrage du site se résume à une bascule immédiate sur un des 2 sites secondaires.