



WEBSTREET

Les frameworks de la solution modifiée

Client : Webstreet

Projet : Génération et maintenance de sites web

Table des matières

Objet du document.....3

Solution A : Gestionnaire d'utilisateur.....4

 Business.....5

 Données.....6

 Application.....6

 Technologie.....6

Solution B : Hébergement chez le client.....7

 Business.....8

 Données.....8

 Application.....8

 Technologie.....9

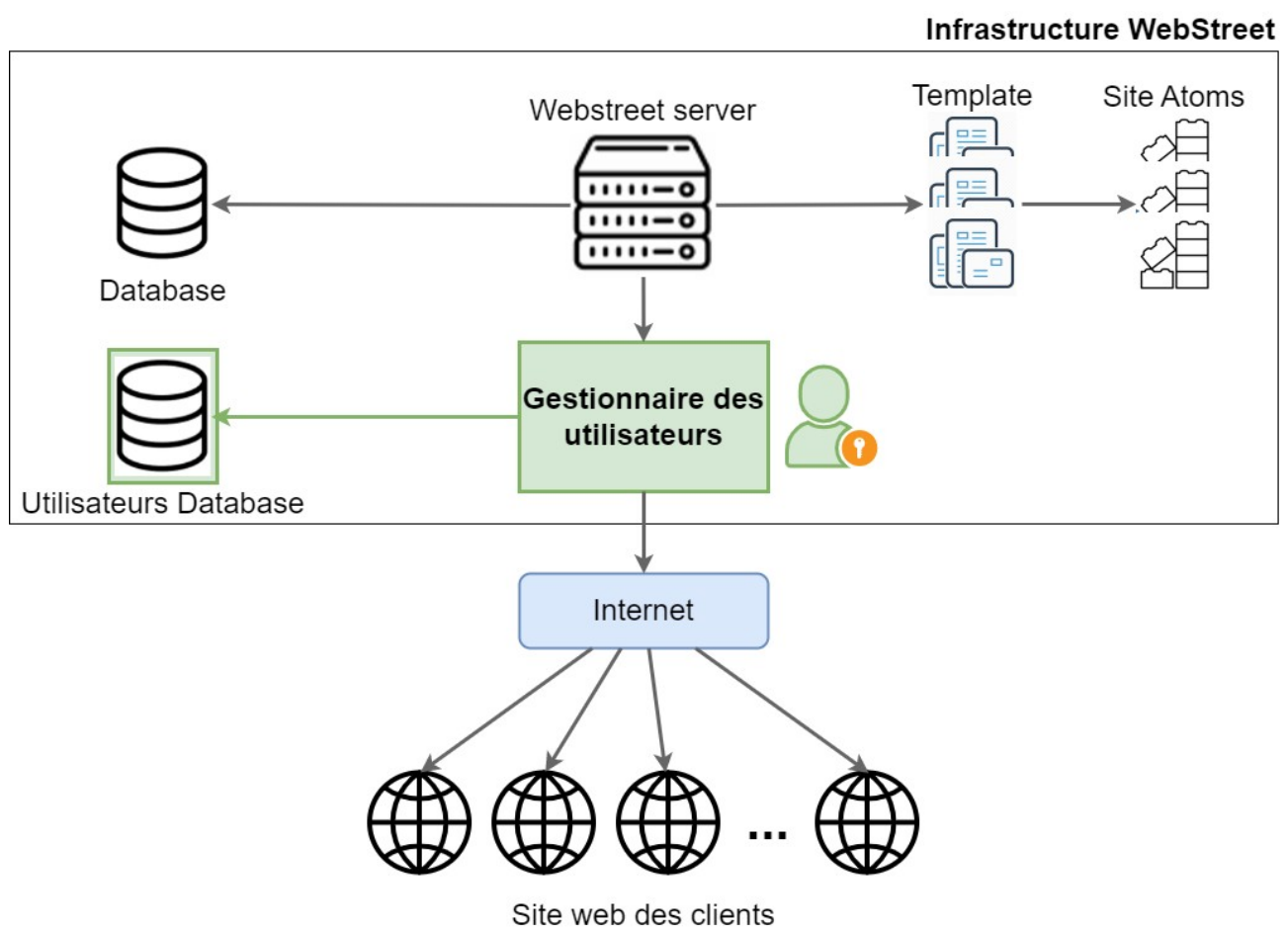
Objet du document

Le document suivant décrit deux solutions pour répondre aux nouveaux besoins du projet de génération et maintenance de sites web.

Pour rappel, les nouveaux besoins sont les suivants :

- Un module doit être développé et installé sur le serveur de l'acheteur, afin de lui permettre de récupérer le site.
- L'hébergeur de Webstreet contiendra toutes les données structurales du site client ainsi que les commentaires (fiches produits, etc.). Toutes les validations seront envoyées au serveur de l'acheteur.
- Tout contenu volumineux sera sur les serveurs de l'acheteur.
- Toute mise à jour du contenu se fera via nos serveurs (sur demande de l'acheteur).
- Les mises à jour seront centralisées et envoyées à tous nos clients en même temps.
- Les sites webs générés devront être divisés en deux :
 - L'infrastructure et administration du site sera hébergés chez WebStreet
 - les parties contenant des données sensibles et confidentielles devront être hébergé dans le centre de données du client.

Solution A : Gestionnaire d'utilisateur



Business

Cette solution consiste à **renforcer la gestion des utilisateurs au travers de l'usage d'un framework de sécurité.**

Aussi, l'entreprise WebStreet devra se doter d'un service de protection des données et cybersécurité. Ce service aura la charge de s'assurer que le maintien des données sensibles et confidentielles des clients soient en accord avec le business et les standards de sécurité des données. Ainsi, il devra :

- **Identifier les risques et s'en prémunir**
- **Faire respecter la conformité RGPD et d'autres standards internationaux de protection des données sensibles et de confidentialité**
- **Adopter et encourager l'usage de bonnes pratiques préventives afin de renforcer la cybersécurité de WebStreet.**

La liste suivante présente les actions que pourront réaliser le nouveau service de cybersécurité :

- **Adopter des outils efficaces** : pour prévenir des risques – par exemple, le stockage de données en ligne, l'authentification par signature électronique, l'emploi de pare-feux, le filtrage de flux.
- **Mettre à jour les logiciels** : les mises à jour permettent aux logiciels de corriger leurs faiblesses et leurs failles pour parer les menaces les plus récentes.
- **Protéger les données sensibles** : certaines données sont plus à risques que d'autres. Il est donc important de les identifier et de les mettre en sécurité. Il en va de même pour les ressources.
- **Sauvegarder les données** : dans le cas où ces données sont altérées, dérobées, ou supprimées, la sauvegarde au préalable peut limiter les dégâts causés par une panne ou une cyberattaque.
- **Renforcer les droits d'accès** : les accès aux données, à la fois pour les collaborateurs que les clients, doivent être protégées par des processus d'authentification complexe et des mots de passe qui doivent être régulièrement changés.
- **Créer un plan de continuité d'activité** : cette précaution est impérative pour les entreprises car elle permet de maintenir l'activité en cas d'interruption.
- **Sensibiliser les équipes à la cybersécurité** : la maladresse humaine est l'une des principales causes de défaillances dans la sécurité informatique. La formation des collaborateurs aux cyber-menaces et aux bonnes pratiques par un expert formé constitue un rôle clé dans le renforcement de la cybersécurité.

Données

Un nouveau gisement de données dédié à la sécurité des données doit être mis en place. Il devra correspondre à prérogative sécurisation des données sensibles et confidentielles comme convenu par la [RGDP](#) en europe ou d'autre standards de protection des données.

Ainsi, au travers d'une évaluation, le service en cybersécurité établira une politique de sécurité des données à l'échelle internationale répondant aux questions de :

- Quelles sont les données collectées et leurs durées de conservation ?
- Quelles sont les mesures techniques et organisationnelles de protection des données sensibles et confidentielles ?
- Pourquoi et comment seront utiliser ou traiter les données personnelles ?
- Qui pourra accès aux données sensibles et confidentielles ?
- Où sont stockées vos données sensibles et confidentielles ?
- Existe-il des transferts de données vers des pays tiers ? Quelles sont les garanties concernant la protection de la vie privée et des libertés et droits fondamentaux des clients lors de ce flux de données en cas de prestation ?
- Quelles sont les droits de l'entreprise Webstreet concernant les données de ses clients ?

Application

La solution applicative suggéré peut être interfacé facilement à l'architecture nouvellement créé dans le cadre ce projet.

Cette solution est constitué d'un framework de sécurité [KeyClock](#). Ainsi, lors de l'authentification, le site Webstreet interrogera l'API Keycloak afin de valider que l'utilisateur est autorisé à accéder à son web.

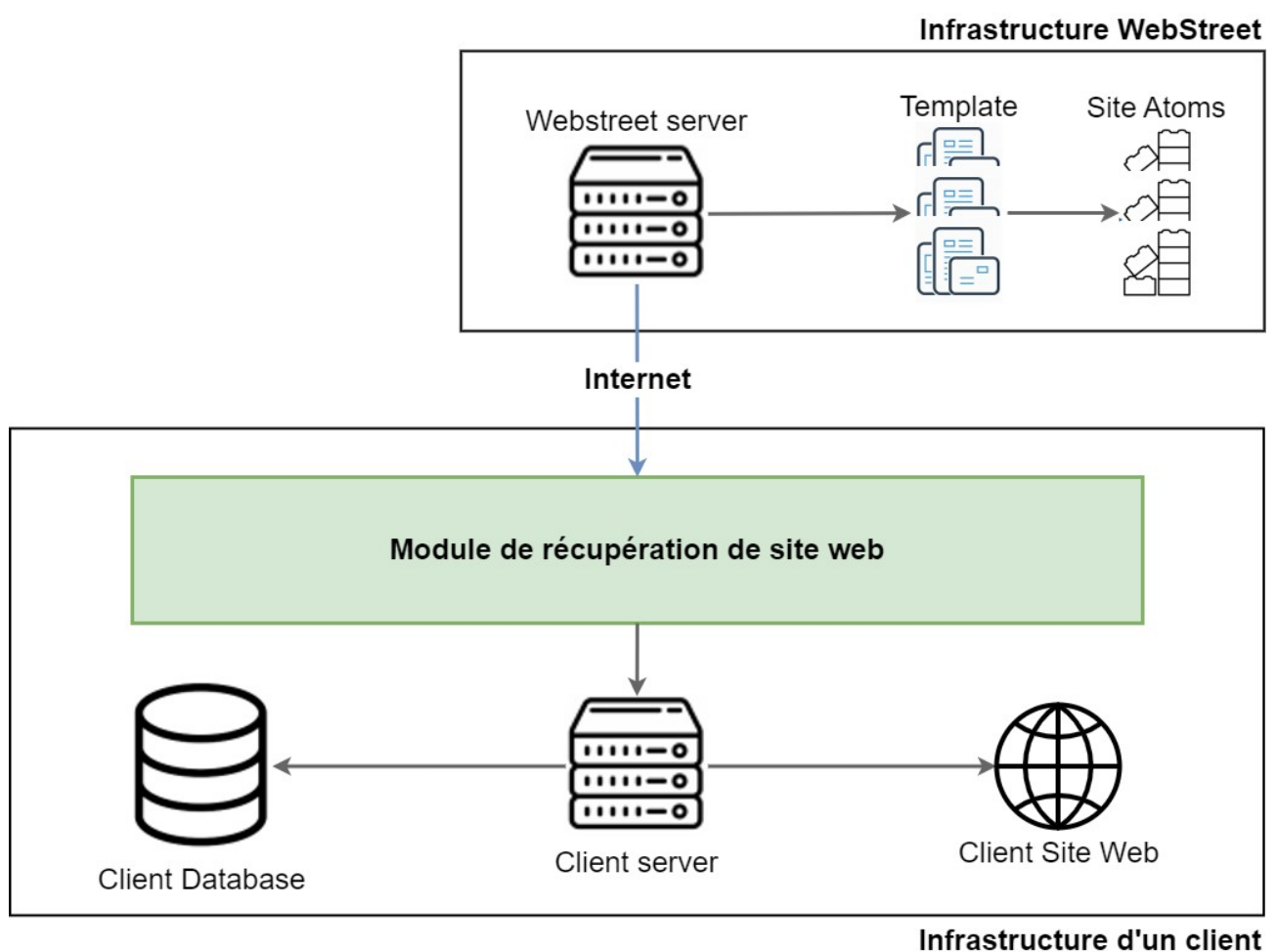
Grace à ce framework, les clients auront la certitude qu'aucune fuite ou malveillance de la part d'un tiers pourra être réaliser sur leur site web hébergé par Webstreet.

Le service de cybersécuerité aura la charge de mettre en œuvre et de maintenir le framework de gestion des utilisateurs.

Technologie

- Un serveur de données sensibles et Keycloak :
 - Un serveur contenant une interface graphique et une API.
 - L'adaptateur applicatif Keycloak : un ensemble de bibliothèques pour appeler le serveur.

Solution B : Hébergement chez le client



Business

Cette solution est composée d'un module de génération d'un site web directement dans l'infrastructure du client. Du côté de **Webstreet**, des développements devront être faits pour réaliser ce module. Du côté des **Clients**, ils devront posséder une infrastructure physique capable d'accueillir ce module.

L'organisation de Webstreet devra changer de manière à ce qu'un service prenne en charge les déploiements de site web sur le module de chaque client. Ainsi, les déploiements en masse pourront être réalisés quand toutes les préconfigurations de module sont validées **pour chaque Client**.

Aussi, un **service de support** devra être créé afin de résoudre les problématiques autour de la mise en service du module chez le client, panne serveur chez le client ou toutes autres opérations sur le terrain.

Données

Cette solution déportera les gisements de données sensibles et confidentielles **chez le client**.

Une fois déployés, les sites web seront construits à partir des fronts téléchargés depuis les serveurs de **Webstreet** et des données backend issues du serveur local des clients.

Application

Ce module de génération des sites web est un **lanceur d'infrastructure as code hébergé chez le client**, il réalisera les actions automatiques suivantes :

1. Vérification et mise à jour du lanceur lui-même.
2. Le téléchargement des conteneurs, OS, middlewares, des mises à jours.
3. Le téléchargement des templates et fronts dédiés aux clients.
4. Mettre à jour ou construire une infrastructure client web légère incluant :
 1. La mise à jour ou la création d'une infrastructure LAMP.
 2. La mise à jour des déploiements du serveur d'application web (contenant le site web du client).
 3. La mise à jour ou les déploiements du site web au travers d'un processus de création de site fournie par AMG et aussi du **Configuration Control Dictionary**.
 4. Test automatique permettant de confirmer que l'infrastructure finale et le site web soit stable et opérable sur le serveur du client.

5. La mise en service du site web client.

Une fois que l'infrastructure matériel et le module sont installés chez le client, celui-ci n'a rien d'autre à faire que d'attendre que le site soit opérationnel. Il pourra éventuellement être notifié quand le site est en ligne.

Technologie

Comme décrit dans le schéma et dans les sections précédentes, **le client devra posséder une infrastructure** chez lui afin que l'entreprise WebStreet vienne y installer le module.

Idéalement et pour des soucis de configuration et de compatibilité matérielle, il est recommandé que **chaque client possède le même matériel** chez lui. WebStreet devra imposer (ou vendre) du matériel dédié à cet usage.

Le client ne devra en aucun cas interférer avec le matériel qui lui sera fourni, toutes transformations réalisées par le client sur son serveur pourraient nuire au bon fonctionnement. Ainsi, si une opération de transformation doit être réalisée sur le serveur du client, c'est WebStreet qui s'en chargera à travers de son service de support.

Durant les opérations d'installation du module chez le client, un protocole de connexion sécurisé entre les serveurs de WebStreet et du client devra être mis en place. OpenSSH peut être utilisé.