

FRAMEWORK D'ARCHITECTURE

- WEBSTREET -



WEBSTREET

David EVAN

16/12/2022

Version 1.1

Website Generator – WebStreet

Historique des révisions

Numéro de version	Auteur	Description	Date de modification
1.0	WebStreet	Livraison initiale	XX/XX/2022
1.1	EVAN David (Architecte logiciel)	Mise à jour du Framework pour inclure les deux nouvelles options d'architecture.	16/12/2022

Tableau 1 - Historique des révisions

Objectif du document

Ce document a pour objectif de présenter le cadre de travail pour le développement de la nouvelle architecture Webstreet et plus particulièrement de son nouvel outil de génération de site web.

Ce document rappelle les principes d'architecture de haut niveau, les grands principes fondateurs de l'outil de génération de site web, les parties prenantes et responsabilités des différents acteurs.

La dernière section présente deux alternatives pour répondre aux nouveaux besoins identifiés au cours du développement du projet.

Note :

La majeure partie des modèles présentés sont issus d'un projet « Archi » (Modélisation Archimate) auquel il est possible d'accéder à partir du lien ci-après :

<https://github.com/david-evan/oc-al-p12-webstreet/blob/main/Models/webstreet.archimate>

TABLE DES MATIERES

PRÉSENTATION GÉNÉRALE.....	4
RAPPEL SYNTHETIQUE DU CADRE D'ARCHITECTURE.....	4
PRINCIPES D'ARCHITECTURES.....	4
DESCRIPTION DES ARTEFACTS.....	5
OUTILS CONFIGURES ET DEPOSES.....	5
ARCHITECTURE EXISTANTE.....	6
PARTIES PRENANTES ET GOUVERNANCE	7
PARTIES PRENANTES	7
GOUVERNANCE.....	7
IDENTIFICATION DES RESPONSABILITES (RACI)	9
ADAPTATION AUX NOUVEAUX BESOINS.....	10
CONTEXTE DU CHANGEMENT	10
NOUVEAUX BESOINS IDENTIFIES	10
SYNTHESE DES SOLUTIONS POSSIBLES.....	11
SOLUTION A : ORIENTATION BUSINESS.....	12
PRESENTATION DE LA SOLUTION	12
IMPACTS METIERS (BUSINESS).....	13
IMPACTS LOGICIELS.....	14
IMPACTS SUR LES DONNEES	14
IMPACTS TECHNIQUES (INFRASTRUCTURE)	14
IMPACTS SUR LA SECURITE DES LOGICIELS ET DES DONNEES	15
IMPACTS JURIDIQUES	15
MISE EN ŒUVRE ET ADEQUATION DE LA SOLUTION.....	15
SOLUTION B : ORIENTATION TECHNIQUE.....	17
PRESENTATION DE LA SOLUTION	17
IMPACTS METIERS (BUSINESS).....	18
IMPACTS LOGICIELS.....	19
IMPACTS SUR LES DONNEES	19
IMPACTS TECHNIQUES (INFRASTRUCTURE)	20
IMPACTS SUR LA SECURITE DES LOGICIELS ET DES DONNEES	20
IMPACTS JURIDIQUES	21
MISE EN ŒUVRE ET ADEQUATION DE LA SOLUTION.....	22
CONCLUSION – SOLUTION RETENUE	24
ANNEXES	25
TABLES DES RÉFÉRENCES	28

PRÉSENTATION GÉNÉRALE

Rappel synthétique du cadre d'architecture

WebStreet dispose d'un cadre de travail pour le développement de son architecture directement lié à son activité.

Ce cadre de travail et ses outils constituent un avantage concurrentiel majeur pour l'entreprise, car ils permettent de personnaliser et de mettre en place un site Web client en moins de 72 heures.

La stratégie marketing de WebStreet a toujours communiqué ce message au marché, et le marché y a répondu favorablement. Le conseil d'administration de l'entreprise s'est toujours efforcé de sensibiliser les équipes techniques à cet avantage et d'accompagner les équipes pour les aider à respecter ces délais.

Principes d'architectures

Les principes de la méthodologie d'architecture de Webstreet sont rappelés dans le tableau ci-après :

Id.	Principe
AP-1	Aucun code n'est écrit à partir de zéro. Toutes les personnalisations doivent maximiser l'utilisation des <i>Template</i> et des <i>Atomes de site</i> .
AP-2	Lorsqu'une partie du site est personnalisée, elle doit être documentée avant de démarrer le développement logiciel, à l'aide du Dictionnaire de Personnalisation , qui décrit les personnalisations qui ont été effectuées pour un client, quel <i>Template</i> ou <i>Atome de site</i> a été personnalisé, et comment.
AP-3	Toute la documentation doit être rédigée selon une approche d'équipe globale : plusieurs équipes WebStreet situées dans des fuseaux horaires différents vont développer le site web pour un client spécifique et en assurer la maintenance par la suite.
AP-4	Les <i>Templates</i> sont une collection d' <i>Atomes de site</i> . Les <i>Template</i> ne contiennent pas de code spécifique à un produit client.
AP-5	Les <i>Atomes de site</i> peuvent recevoir des paramètres tels que la langue, la couleur, le style, le placement, etc.
AP-6	Tous les sites Web des clients sont une collection de <i>Template</i> associés à une configuration. Diagramme de présentation .

Tableau 2 : Liste des principes d'architecture

Description des artefacts

Les *Templates* et les *Atomes de site* sont divisés en deux groupes :

- *Templates* et *Atomes de site* back-end (Composants logiques).
- *Templates* et *Atomes de site* front-end (Composants graphiques).

Exemples d'artefacts

Exemple d'un *Template* back-end : Module d'enregistrement d'un nouvel utilisateur. Ce *Template* valide un nouvel utilisateur enregistré et envoie un email pour valider que l'utilisateur est réel, en demandant de changer le mot de passe pour un nouveau. Ce modèle utilise l'*Atome de site* « login » mentionné ci-dessus, ainsi que d'autres composants back-end.

Exemple d'un *Template* front-end : un style de site. Ce module affiche une page entière du site Web à l'aide de composants front-end tels que l'en-tête et le pied de page du site, la colonne de gauche du site, les menus déroulants, etc.

Exemple d'un *Atomes de site* back-end : un composant de connexion (login). Ce composant reçoit un nom d'utilisateur et un mot de passe et valide l'entrée dans une base de données d'utilisateurs.

Exemple d'un *Atomes de site* front-end : un header de site. Ce composant affiche un en-tête de site avec un style, une couleur et une police standard. Il existe des en-têtes de site pour les pages de connexion, les landing pages et les pages internes du site.

Outils configurés et déployés

Les outils suivants sont déployés dans l'entreprise pour aider au développement et à la configuration du site web. Ils sont à la disposition de toutes les équipes de développement :

- **Dictionnaire des *Atomes de Site*** : une base de données de tous les *Atomes de Site* pour commencer la conception et le développement d'un site web pour un client. Chaque entrée du dictionnaire décrit l'objectif de chaque *Atomes de Site*, fournit sa description, l'historique des mises à jour du composant, les paramètres qu'il peut recevoir, les cas d'utilisation et les liens vers les projets où ce composant a été utilisé. ([Exemple](#))
- **Dictionnaire du contrôle de la configuration** : une base de données des relations entre les *Templates* et les *Atomes de Site* (qui appelle quoi, et qui est appelé par quoi). ([Exemple](#))
- **Dictionnaire des personnalisations** : une description détaillée de toutes les personnalisations apportées aux sites des clients Webstreet, accompagné des liens vers des sites Web réels. ([Exemple](#))

Architecture existante

Le schéma ci-après (Figure 1) fournit une vue d'ensemble de la plateforme de génération de site web développée par Webstreet.

Vue d'ensemble de la plateforme de génération de site web

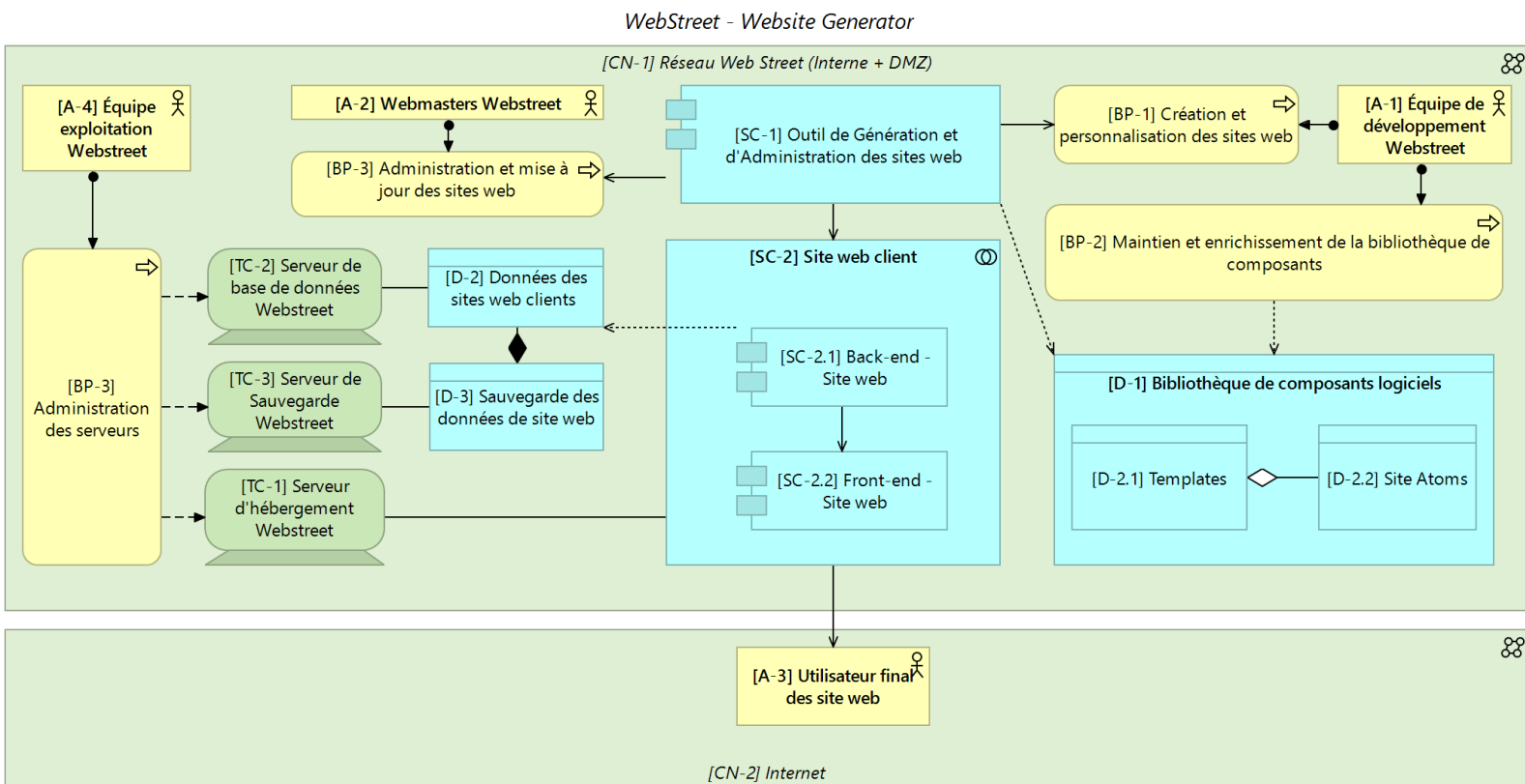


Figure 1 : Baseline Architecture - Vue d'ensemble de la plateforme de génération de site web

Il est à noter que :

- L'hébergement des outils, des sites web clients, de leurs données et des sauvegardes associées sont assurés par l'entreprise (sur le réseau interne ou au sein de la DMZ).
- La gestion de l'infrastructure est assurée par l'équipe « exploitation » de Webstreet.
- Les clients Webstreet **n'ont pas d'accès direct** à leurs sites web ou aux données qui le composent.

PARTIES PRENANTES ET GOUVERNANCE

Parties prenantes

Cartographie des parties prenantes

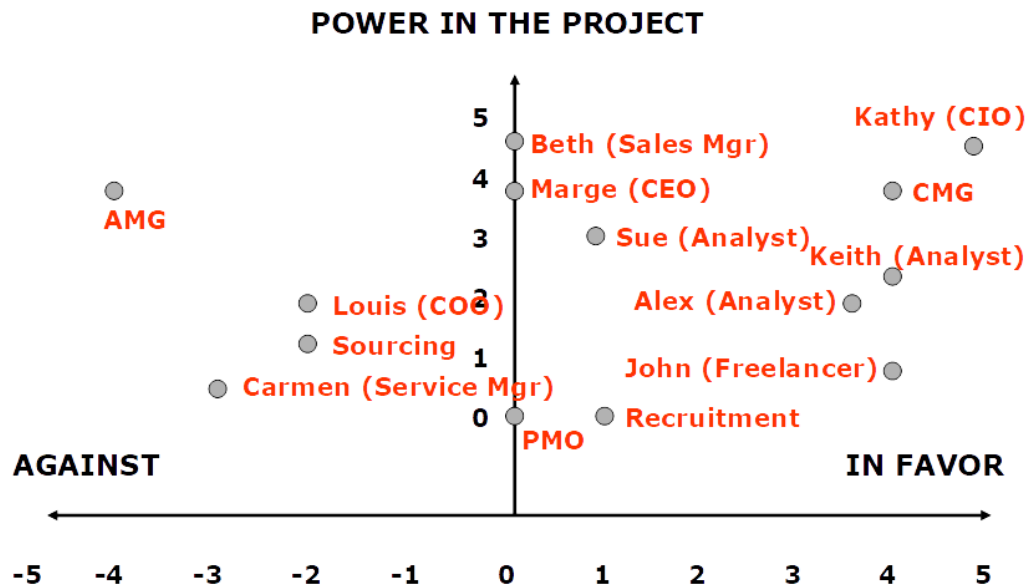


Figure 2 : Cartographie des parties prenantes et intérêts pour le projet

Gouvernance

La gouvernance de l'architecture de la plateforme Webstreet est répartie entre les différents services présentés ci-après :

Département de recrutement : Aucun programmeur ou concepteur n'écrit une ligne de code s'il n'est pas formé à la méthodologie d'architecture WebStreet. Celle-ci est soigneusement synchronisée entre les équipes techniques et le département de recrutement de WebStreet (qui est un sous-ensemble du département RH).

Groupe AMG (Architecture Method Guardians) : Le groupe AMG a pour responsabilité de maintenir la cohérence et d'améliorer le dictionnaire des Atomes de site et des Templates. Le groupe AMG agit en tant qu'expert métier sur les sujets relatifs aux modèles, aux *Atomes de site* et aux méthodes de construction. Les groupes techniques les consultent de manière informelle sur de nombreux sujets. Le groupe AMG est généralement chargé de dispenser des formations sur la méthodologie de l'architecture WebStreet aux nouvelles recrues ainsi qu'aux développeurs expérimentés.

Groupe CMG (Customization Dictionary Guardians) : Le groupe *CMG* a pour principale responsabilité d'enregistrer toutes les personnalisations pour tous les clients. Ce groupe est un lien entre l'équipe technique de WebStreet qui a développé le site Web et l'équipe commerciale qui a été en contact avec le client. Ils rejoignent généralement la dernière partie du cycle de vente afin d'évaluer la quantité et la portée des modifications pour un client. Ils travaillent ensuite avec les équipes techniques sur la documentation du processus de personnalisation. Aucun site web n'est livré à un client sans l'approbation du *CMG*.

Département "Sourcing" : Tous les fournisseurs externes doivent être certifiés pour travailler avec l'architecture logicielle existante. Ce processus de certification est mis en œuvre conjointement par les équipes "*Sourcing*" et l'*AMG*.

Département des ventes : Les équipes du département des ventes ont pour principale mission l'établissement du formalisme contractuel de la vente avec le client. Le groupe *CMG* participe activement au processus de vente et conseille l'équipe de vente sur la portée des modifications.

E-PMO (Enterprise Project Management Office) : Le groupe E-PMO gère le portefeuille de projets déployés dans toutes les succursales de l'entreprise. Ces projets sont internes et n'impliquent pas de clients.

Ce nouveau projet devra être inclus dans ce portefeuille et sera observé et suivi par les équipes E-PMO.

Identification des responsabilités (RACI)

Stakeholders	David	Kathy	Keith	Alex	Sue	Marge	Beth	Louis	Group	Group	Group	Group	Group	Carmen
Position	Freelancer	CIO	Analyst	Analyst	Analyst	CEO	Sales Mgr	COO	AMG	CMG	Recruit.	Sourcing	E-PMO	Service Mgr
Business requirements analysis	P	A	R	P	P	I	C	C	C	C	I	P	P	C
Basic software architecture design	R	P	P	P	I	I	I	I	A	C	I	I	I	I
Detailed software architecture design	R	I	P	P	P	I	I	I	A	C	I	I	I	I
Software development	C	I	P	R	P	I	I	I	I	I	I	I	I	I
Unit tests	C	I	P	A	R	I	I	I	P	P	P	I	I	I
Integral tests	I	I	R	A	P	I	I	I	P	P	P	I	I	I
Production Rollout	P	A	R	C	C	I	I	I	P	P	P	I	I	I

Tableau 3 : Matrice RACI (Rôle et responsabilité des parties prenantes)

Légende :	I Informed
A Accountable	P Participates
C Consulted	R Responsible

ADAPTATION AUX NOUVEAUX BESOINS

Contexte du changement

Lors de la phase de développement de l'outil de génération et d'administration des sites web, la direction de Webstreet a identifiée de nouveaux besoins pour les clients. Ces nouveaux besoins ne peuvent pas être satisfait par la construction actuelle. Des modifications doivent être apportées au produit avant la livraison finale.

Il est à noter que ce changement ne doit pas avoir d'impact significatif sur les délais de livraison ou le budget du produit. Les modifications apportées devront pouvoir être livrées dans un délai maximal de 2 semaines, excluant de fait une refondation complète du produit.

Nouveaux besoins identifiés

Id.	Besoin client identifié	Description (Notes de réunion transmises)
BR-1	Permettre aux clients de réaliser une copie de tout ou partie de leur site.	Un module doit être développé et installé sur le serveur de l'acheteur, afin de lui permettre de récupérer le site.
BR-2	Hébergement des Templates de site web par Webstreet.	Notre hébergeur contiendra toutes les données structurales du site client ainsi que les commentaires (fiches produites, etc.). Toutes les validations seront envoyées au serveur de l'acheteur.
BR-3	Hébergement des données volumineuses par les clients.	Tout contenu volumineux sera sur les serveurs de l'acheteur.
BR-4	Déploiement des mises à jour des sites web à partir de l'infrastructure de Webstreet.	Toute mise à jour du contenu se fera via nos serveurs (sur demande de l'acheteur).
BR-5	Mise à jour centralisée des sites web.	Les mises à jour seront centralisées et envoyées à tous nos clients en même temps.

Tableau 4 : Liste des nouveaux besoins identifiés

Synthèse des solutions possibles

Avant d'envisager la réponse à apporter pour satisfaire aux demandes transmises, il est nécessaire de comprendre les motivations des clients concernant ces besoins nouvellement identifiés.

L'analyse de l'architecture existante (*Figure 1*, présentée dans la section précédente) permet de visualiser que dans la configuration actuelle, le client se positionne uniquement en donneur d'ordre, sans jamais prendre part aux processus d'exploitation du site web ni avoir accès à ses données.

Deux solutions pour y répondre présentant toutes deux avantages et inconvénients sont envisagées. Il est à noter qu'aucune solution couvrant 100% des besoins ne pourra être livrée dans les délais imposés

Solution A : Explorateur de fichier + IAM (Business)

La solution A consiste en le maintien de l'hébergement dans l'infrastructure Webstreet en y ajoutant un explorateur de fichier « web » permettant aux clients de pouvoir accéder à distances à leurs données. Un IAM est implémenté pour gérer l'authentification des clients et les droits d'accès.

Cette solution est relativement simple à mettre en œuvre et permet de couvrir la plupart des besoins du client. Son couplage avec l'architecture est très faible.

Solution B : Hébergement chez le client + Mise à jour à distance (Technique)

La solution B vise à déléguée l'hébergement aux clients pour répondre ma manière plus « stricte au besoin ». Les mises à jour seront déployées via l'implémentation d'une fonction de mise à jour implémentée dans les sites web des clients (via Atome de site) et se déclenchant à intervalle régulier.

Les clients seront responsables de leur hébergement. De l'automatisme devra être ajouté pour faciliter les opérations de déploiement chez le client.

Cette solution nécessite de prendre en compte de nombreux impacts indirects pouvant influencer sur les délais de délivrance d'un site web et pouvant remettre partiellement en cause l'objectif de livraison en 72h.

SOLUTION A : ORIENTATION BUSINESS

Présentation de la solution

Comme abordé dans les sections précédentes de ce document, la principale motivation sous-jacente aux besoins exprimés par les clients est d'obtenir un accès à leurs données (site web + données du site) afin de ne pas créer un couplage trop fort entre leur entreprise et Webstreet.

Les besoins peuvent être couverts en permettant aux clients de disposer d'un accès sécurisé à leurs différentes données à l'aide d'un outil de type « gestionnaire de fichier » accessible depuis n'importe quel navigateur web. Afin de garantir la sécurité de l'accès et de contrôler le périmètre de données accessible, un gestionnaire d'identité et d'accès (IAM) pourrait être mis en place pour assurer l'authentification et contrôler les autorisations de l'utilisateur.

Implémentation dans l'architecture Webstreet

Le schéma ci-après (Figure 3) fournit une vue d'ensemble sur les modifications apportées à l'architecture Webstreet pour y intégrer les modifications introduites par la solution A.

Vue d'ensemble de la Solution A : Explorateur de fichier + IAM ("Commerciale")

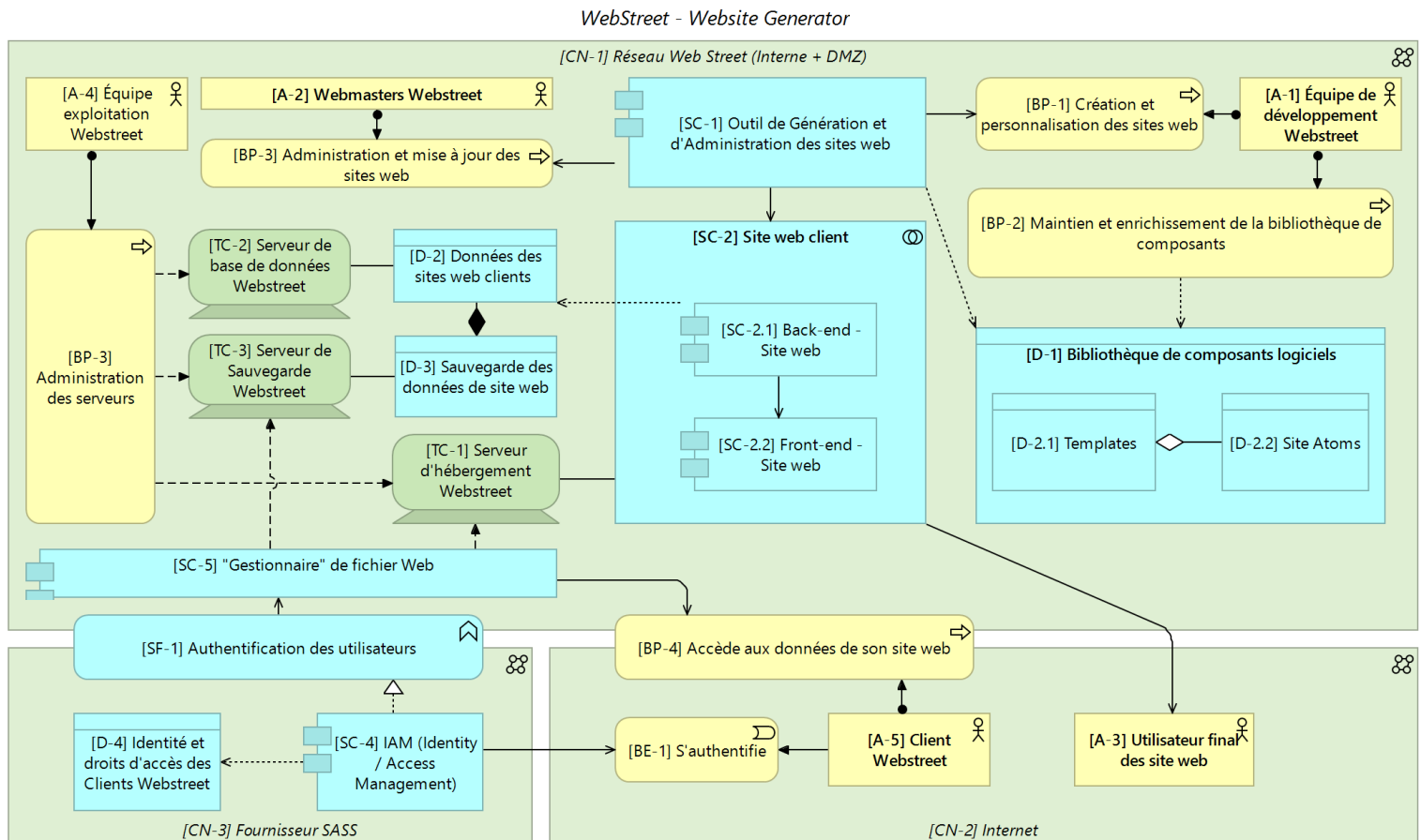


Figure 3 : Vue d'ensemble de l'implémentation de la solution A (Schéma HD en annexe)

Dans cette construction, le client Webstreet (A-5) peut désormais accéder en toute autonomie à ses différentes données (BP-4) sans modification majeure de l'architecture existante.

Le recours à un fournisseur SAAS pour fournir l'IAM assurant l'authentification et la gestion des droits d'accès permet de réduire fortement le coût de mise en œuvre et d'exploitation de la solution (d'un point de vue des ressources financières et humaines nécessaires).

Points forts / Points faibles de la solution

Points forts	Points faibles
<ul style="list-style-type: none"> - Solution très simple pour les clients (pas de formation préalable à prévoir). - L'accès aux sauvegardes des bases de données peut être réalisé à partir du même outil. - Sécurité des données garantie par l'authentification via l'IAM. (Authentification multi-facteur à intégrer obligatoirement) - Contrôle total de Webstreet sur l'infrastructure avec la possibilité de continuer à garantir un SLA pour le client. - Protection possible de la propriété intellectuelle de Webstreet en autorisant uniquement certains répertoires définis préalablement. - La solution introduit peu de couplage dans l'architecture, que ce soit entre les applicatifs ou les acteurs / processus. - Le délai de mise à disposition d'un site web en 72h ne sera pas impacté par cette solution. 	<ul style="list-style-type: none"> - Le besoin « BR-3 » identifié (Hébergement des données volumineuses par les clients) n'est pas totalement satisfait par cette solution. Toutefois, ce point est à nuancer par le fait que le client peut, s'il le souhaite, créer des copies de ses données et les héberger sur sa propre infrastructure. - Un flux d'accès au serveur doit être ouvert et géré par l'intermédiaire du gestionnaire de fichier web. La sécurité de ce flux dépendra de l'attention portée par l'utilisateur.

Tableau 5 : Synthèse des points forts / points faibles de la solution A.

Impacts métiers (business)

La solution A comporte peu d'impacts métiers pour l'entreprise Webstreet. Un processus de « création et gestion des comptes utilisateur », géré par les équipes d'exploitation Webstreet, devra être ajouté.

Les aspects commerciaux et les impacts sur le processus de vente des sites web ne seront pas impactés par cette solution. Une petite documentation pour les clients (document unique et non personnalisé) expliquant l'usage de l'explorateur de fichier devrait cependant être créée et remise au client lors de la livraison de son produit.

Impacts logiciels

Deux nouveaux composants logiciels seront à ajouter à l'architecture :

- Le portail d'authentification et gestion des droits d'accès « IAM » (SC-4)
- Le gestionnaire de fichier web (SC-5)

Concernant l'IAM, il est préconisé de se tourner vers une solution externe accessible en SAAS afin de réduire le coût de déploiement et d'exploitation de la solution. Afin d'améliorer l'interopérabilité et l'évolutivité, l'utilisation d'une solution basée sur un protocole d'authentification et d'identification standardisé paraît indispensable (SAML 2.0 / OAuth 2.0 / OpenID Connect).

Dans le cas présent une solution basée sur le Framework OAuth 2.0 semble paraître adaptée pour assurer l'authentification (via l'*access token*) et le contrôle des droits d'accès (en exploitant les *scopes* associés au *token*). Bien que non indispensable, la couche d'identité *OIDC* pourrait être ajoutée si nécessaire.

Concernant le gestionnaire de fichier, l'utilisation d'un outil open source existant et nécessitant une légère personnalisation est fortement recommandé. Cette approche permet de réduire fortement le coût de mise en œuvre pour un produit ne nécessitant finalement que très peu de personnalisation. Seule l'intégration du mécanisme de gestion des droits d'accès est à prévoir.

Impacts sur les données

Un nouveau périmètre de données sera à intégrer dans l'architecture :

- L'identité et les droits d'accès des clients Webstreet (D-4).

Ces données seront directement associées à l'outil IAM. Seul un accès en lecture / écriture à l'équipe d'exploitation Webstreet (A-4) devrait être accordé. L'accès devrait être possible uniquement en utilisant le portail d'administration de la solution IAM retenue et lors de la création (ou éventuelle suppression) des comptes utilisateurs.

Le stockage des données qui incluront indubitablement des DCP devra être totalement sécurisé et conforme au RGPD. Le choix du fournisseur devra tenir compte de ce critère.

Afin d'assurer l'intégrité des données, seul un accès en lecture sera fourni au client des différentes données. Les règles de gestion et de stockage (type de données, cryptage) seront transmises au client à la livraison de son site web.

Impacts techniques (infrastructure)

Aucun impact direct sur l'infrastructure n'est à prévoir pour cette solution. Les sites web continueront d'être hébergés chez Webstreet et l'exploitation des machines assurée par l'équipe d'exploitation (A-4).

Les accès aux données stockées sur les machines n'auront lieu qu'à travers le gestionnaire de fichier web en s'appuyant sur les droits d'accès délivrés par l'IAM.

Impacts sur la sécurité des logiciels et des données

La robustesse de la sécurité de la solution reposera principalement sur l'authentification assurée par l'IAM. Il est impératif que du 2FA soit imposé. Il est par ailleurs fortement recommandé que l'accès nécessite un 3FA via OTP + Code via SMS ou E-mail.

D'autres mécanismes peuvent être facilement mise en place pour renforcer la sécurité :

- Activation à la demande du client de l'accès à distance (non activé par défaut pour tous les sites web)
- Notification de connexion systématique par e-mail.
- Blocage automatique des connexions « suspectes » (à partir d'un pays différent par exemple) avec demande de validation manuelle par les exploitants Webstreet.
- Désactivation des comptes utilisateurs sans activités depuis, par exemple, 90 jours avec validation manuelle de la réactivation par les exploitants Webstreet.

Il est à noter que les flux de données devront par ailleurs s'appuyer uniquement sur des protocoles sécurisés (HTTPS, FTPS ...) à l'aide d'une version à jour de TLS et que les données dites « sensibles » devront être chiffrée à l'aide d'un algorithme robuste (type : AES-256).

Impacts juridiques

Le principal impact juridique de la solution porte sur le transfert d'une partie de la propriété intellectuelle de Webstreet, notamment par l'accès au code source des sites web, aux clients.

Cet impact peut être modulé en définissant des restrictions d'accès à certains dossiers du site web en fonction des accords de licence signés avec les clients. Une analyse de ce point par les équipes juridique devrait être demandée.

Des modifications des conditions générales applicables aux clients devront probablement être à prévoir en ce sens.

Mise en œuvre et adéquation de la solution

Capacité de mise en œuvre / Coût de la solution

Les modifications apportées par cette solution ne requièrent pas de compétences spécifiques autres que celle déjà disponible dans un projet de cette envergure.

En s'appuyant sur les recommandations définies dans ce document, le calendrier défini pour le projet semble compatible avec les modifications d'architecture à apporter.

Le coût financier de mise en œuvre est fortement dépendant de la solution finale retenue pour l'IAM et n'est pas nul. Toutefois, l'offre disponible sur le marché (Google IAM, Amazon IAM, Azure AD, Auth0, Okta Identity Cloud ...) permet d'affirmer que les coûts seront relativement faibles (< 1K€/an).

Évaluation des risques identifiés pour la solution

Id.	Risque	Effet	Fréq.	Impact	Mesure d'atténuation
RSA-1	Risque projet : Dépassement des délais de livraison. Origine : Changement d'architecture au cours des développements.	Crit.	Seldom	Medium	#1 : Renforcement des équipes. #2 : POC de la solution retenue avant de commencer le nouveau sprint.
RSA-2	Risque solution : Vol des identifiants d'un client aboutissant à un accès non autorisé à ses données. Origine : Flux de données accessible depuis internet.	Cat.	Unlikely	Medium	#1 : Mise en application des différentes recommandations formulés dans ce document.
RSA-3	Risque solution : Défaillance (totale ou partielle) du fournisseur IAM. Origine : Dépendance à un fournisseur tiers non défini.	Marg.	Unlikely	Low	#1 : Choix d'un fournisseur disposant d'un SLA > 99,95%.
RSA-4	Risque projet : Incohérence du produit livré avec les besoins réels des clients. Origine : Exigences fonctionnelles mal définies.	Marg.	Seldom	Low	#1 : Conduite d'un atelier de réévaluation des besoins.
RSA-5	Risque solution : Incapacité du client à utiliser la solution. Origine : Manque de connaissance du produit.	Marg.	Unlikely	Low	#1 : Améliorer la documentation fournie.
RSA-6	Risque solution : Non-conformité à de la gestion des DCP des identités avec la réglementation (Ex : RGPD). Origine : Dépendance à un fournisseur tiers non défini.	Crit.	Unlikely	Low	#1 : Vérification de la conformité du fournisseur IAM retenu.

Tableau 6 : Évaluation des risques associés à la Solution A

Voir [Annexe](#) pour définition du modèle d'évaluation.

Adéquation avec les besoins exprimés

Id.	Besoin client identifié	Besoin couvert par la solution
BR-1	Permettre aux clients de réaliser une copie de tout ou partie de leur site.	OUI ✓
BR-2	Hébergement des Templates de site web par Webstreet.	OUI ✓
BR-3	Hébergement des données volumineuses par les clients.	EN PARTIE !
BR-4	Déploiement des mises à jour des sites web à partir de l'infrastructure de Webstreet.	OUI ✓
BR-5	Mise à jour centralisée des sites web.	OUI ✓

Tableau 7 : Évaluation de l'adéquation des besoins exprimés avec la Solution A

SOLUTION B : ORIENTATION TECHNIQUE

Présentation de la solution

La solution B est une construction plus « technique » de l'architecture qui vise à déléguer l'hébergement de son site web au client pour ainsi satisfaire aux différents besoins. L'outil de génération de site web serait utilisé pour la création d'un artefact de type « archive » (JAR par exemple) définissant différents conteneurs applicatifs permettant de « monter » la solution chez le client.

Les mises à jour des sites web seront appliqués automatiquement à l'aide d'une fonction implémentée dans les sites client (fonction elle-même fournie par un Atome de site back-end)

Implémentation dans l'architecture Webstreet

Le schéma ci-après (Figure 4) fournit une vue d'ensemble sur les modifications apportées à l'architecture Webstreet pour y intégrer les modifications introduites par la solution B.

Vue d'ensemble de la Solution B : Hébergement par le client + Mises à jour à distance ("Technique")

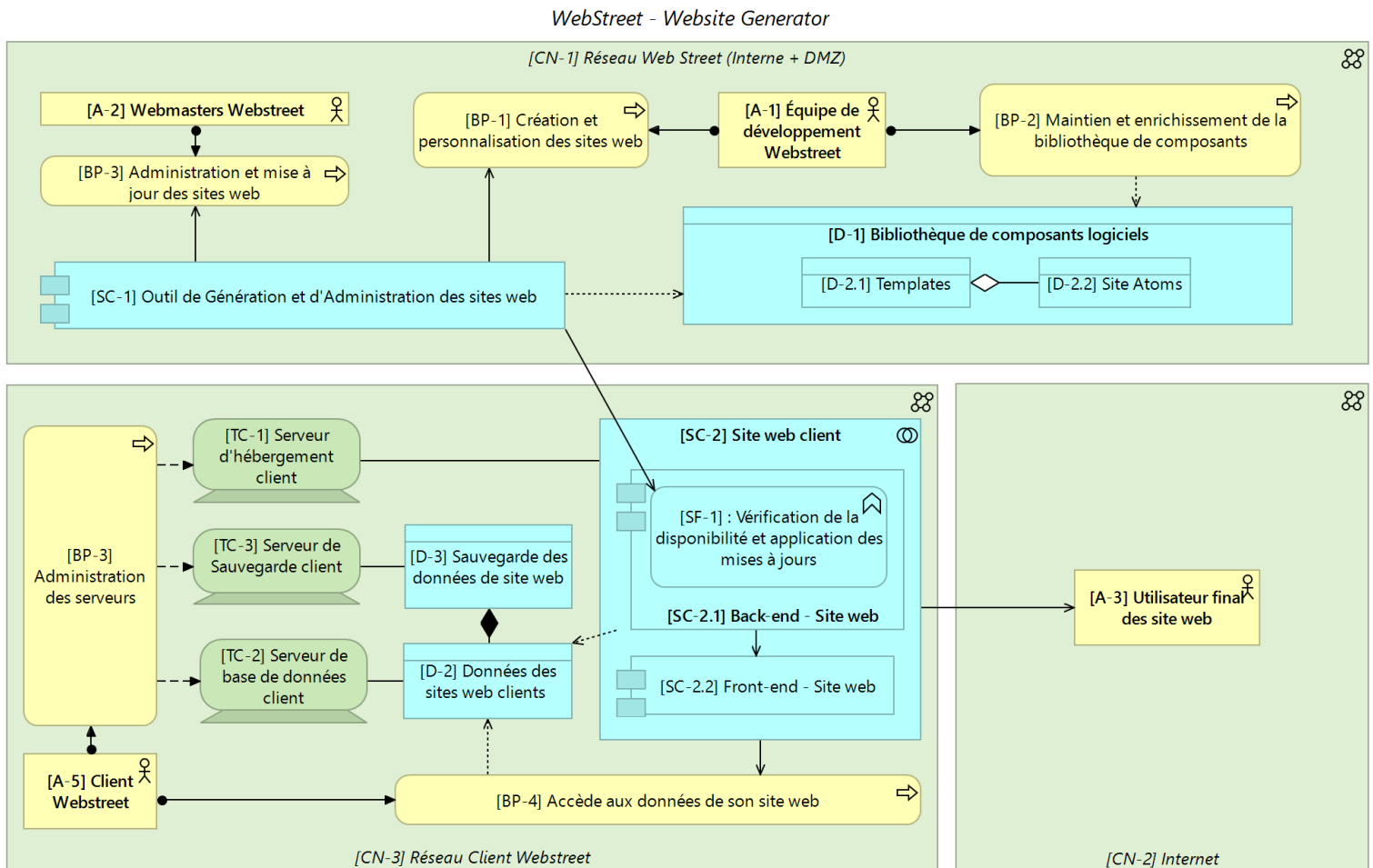


Figure 4 : Vue d'ensemble de l'implémentation de la solution B (Schéma HD en annexe)

Points forts / Points faibles de la solution

Points forts	Points faibles
<ul style="list-style-type: none"> - Solution permettant de couvrir la totalité des besoins exprimés. - La délégation de l'hébergement aux clients représente une source d'économie potentielle pour Webstreet. 	<ul style="list-style-type: none"> - Solution nécessitant pour les clients de compétences techniques avancées pour le déploiement / l'installation de leur produit. - La solution entraîne de nombreux impacts qui peuvent remettre en cause le délai de 72h pour la livraison d'un site. - L'absence de maîtrise de l'infrastructure empêche de garantir des SLA aux clients. - Il existe des risques quant au transfert d'une partie de la propriété intellectuelle Webstreet chez les clients. - Les développements pour l'automatisation du déploiement de la plateforme sont assez conséquents et ne paraissent difficilement compatibles avec le calendrier imposé.

Tableau 8 : Synthèse des points forts / points faibles de la solution B.

Impacts métiers (business)

D'un point de vue direct, la solution B comporte relativement peu d'impact métiers pour Webstreet. Il est possible de noter que le processus d'administration des serveurs (BP-3) sera transféré des exploitants Webstreet vers le client.

Toutefois, plusieurs impacts non direct sont à prévoir :

La clientèle Webstreet n'est pas une clientèle issue des métiers de la technologie, le déploiement, la configuration et la mise en réseau de machines pour un hébergement interne et en adéquation avec les spécifications imposées par Webstreet (notamment sur la capacité à pouvoir lancer des conteneurs web) peuvent être des opérations complexes à réaliser.

Ce point pourrait être atténué en vendant directement le matériel et un forfait de configuration aux clients, toutefois, cette solution aurait pour effet de déplacer la complexité de déploiement aux équipes WebStreet qui devront intervenir dans un environnement non maîtrisé. Il est aussi à noter que dans un contexte de tension sur les marchés des composants électroniques et la livraison de serveur, il paraît difficile de pouvoir garantir la capacité à livrer des grappes de serveur « rapidement » au client.

Une autre alternative pourrait consister à imposer une configuration matérielle « type » auprès d'un fournisseur cloud. Dans tous les cas, les équipes Webstreet devront fournir aux clients une solution conteneurisée afin de permettre un déploiement rapide.

En dernier lieu, les équipes Webstreet disposent de mécanismes d'intégration et de déploiement continu permettant d'automatiser l'ensemble de ses opérations. Ces opérations devront désormais être assurées au moins en partie manuellement.

L'objectif des 72h entre la signature d'un devis et la mise à disposition du site web **semble être difficile à tenir** en prenant en compte ces nouvelles actions.

Un autre impact indirect à prévoir concerne le processus de vente. L'hébergement par le client de son propre site web devra forcément être abordé au cours du processus de vente. Les commerciaux devront être formés pour être en mesure de fournir suffisamment d'information technique au client avant la signature du contrat.

Une documentation complète devra être remise au client lors de la livraison de son produit afin qu'il puisse réaliser les opérations de déploiements de manière la plus autonome possible.

Un processus de support dédié aux questions de déploiement et d'exploitation devra probablement être créé et géré par les équipes d'exploitation Webstreet.

Impacts logiciels

Aucuns nouveaux composants n'ont été ajoutés dans l'architecture de la solution B. Une nouvelle fonction (SF-1) de doit toutefois être ajoutée au Site web des clients pour qu'ils puissent se mettre à jour automatiquement via une connexion à l'outil de Génération et d'Administration des sites web (SC1).

Afin de réaliser leurs mises à jour, les sites web devront se connecter à l'outil Webstreet à intervalle régulier (quelques heures) pour vérifier si une mise à jour est disponible et, le cas échéant, la télécharger. *Les questions de sécurité relative à ce flux sont abordées dans la section « Sécurité des logiciels et des données ».*

Impacts sur les données

Dans l'architecture de la solution B, les données sont transférées sur les serveurs du client. Peu d'impact sont à prévoir chez Webstreet.

Les données de mise à jour (fichiers binaires, fichiers sources ...) devront être stockées sur l'infrastructure Webstreet. La connexion pour les mises à jour des sites web (via SSH idéalement) nécessitera le stockage de clefs SSH qui devront être placées dans des répertoires dont les accès devront être strictement contrôlés.

Impacts techniques (infrastructure)

La plateforme d'hébergement étant administrée par le client, les impacts sur l'infrastructure Webstreet seront forcément réduits. Il sera nécessaire de s'assurer que la plateforme accueillant l'outil de Génération et d'Administration disposera des capacités nécessaires pour déployer les mises à jour sur de nombreux sites web clients à la fois.

Les impacts techniques pour le client seront bien plus nombreux. Chaque client devra disposer d'une plateforme (ou d'un cloud provider) qui sera en capacité de pouvoir déployer / maintenir en service l'ensemble des composants du site web. Par ailleurs, des redondances devront exister chez les clients afin de garantir la disponibilité du site web.

L'ensemble des spécifications techniques liées à la plateforme, aux exigences non fonctionnelles (version des OS, liste des protocoles implémentés, SGBD supportés ...) devra être fourni au client avant la livraison du produit.

L'automatisation des déploiements pourrait être améliorée en fournissant aux clients une extension à Kubernetes. Toutefois il est à noter que les délais imposés rendent difficile d'envisager cette solution pour la livraison initiale de l'architecture.

Impacts sur la sécurité des logiciels et des données

La sécurité de cette architecture sera principalement soumise à deux points de tension :

- La sécurité des échanges entre les sites web (hébergés chez les clients) et les serveurs de mise à jour (hébergés chez Webstreet).
- La sécurité de l'infrastructure et de la configuration des logiciels (serveur web, orchestrateur, ouvertures des ports ...) chez le client.

Les échanges entre les sites web et les serveurs de mise à jour devront être authentifiés afin de s'assurer que seuls les sites web des clients pourront consommer les mises à jour. La quantité de fichier à transférer ne semble pas compatible avec le protocole HTTP(S). Le protocole SSH et des transferts via SCP seront retenus.

Dans tous les cas, la sécurité de ces échanges reposera sur la capacité des clients à garantir la confidentialité des clefs SSH. Les clefs SSH devront être renouvelées à intervalle régulier. Le serveur de mise à jour devra être sécurisé et isoler au maximum du reste de la DMZ Webstreet pour éviter les propagations d'attaque en cas de connexion malicieuses. Il est à noter que les clefs SSH devront être unique pour chaque client et que leur privilège devra se limiter à la copie de données situées sur des répertoires autorisés. Des contrôles par audit de sécurité et vérification de la configuration devront être mis en place régulièrement.

La sécurité de l'infrastructure chez le client est un point crucial de cette construction d'architecture. L'hébergement de leur site web par les clients suppose qu'ils disposent des capacités à maîtriser la sécurité de leur propre plateforme d'hébergement (interne ou cloud). Un D.A.T (Document d'Architecture Technique) devra être remis au client lors de la commande du produit afin de lui permettre de disposer d'une liste exhaustive d'éléments à configurer, notamment concernant la sécurité de la plateforme d'hébergement.

Les bases de données devront par ailleurs stocker les données conformément à la politique de conception définie par Webstreet, notamment en ce qui concerne le stockage des DCP ou des données sensibles.

Le client devra par ailleurs être incité à mener une politique active de sécurité, notamment par la conduite d'audit sur sa plateforme, afin de garantir la sécurité des sites web.

Afin de limiter les impacts en cas de cyberattaque et étant donnée l'impossibilité pour Webstreet de pouvoir limiter l'accès à certains répertoires, le code source des sites web devra être fourni de manière obfusquée, à minima en ce qui concerne le code du moteur non personnalisé et les codes des Templates / Atome de site.

Impacts juridiques

L'hébergement par le client de son site va nécessiter une révision des contrats actuellement en vigueur. Les SLA actuellement en vigueur ne pourront plus être garanti étant donné l'impossibilité de maîtriser l'infrastructure.

Tout comme dans la solution A, le transfert de la propriété intellectuelle de Webstreet vers les clients est un aspect important à prendre en compte dans cette construction architecturale.

L'obfuscation (recommandation préconisée dans la section précédente) du code source permet de limiter l'impact de ce transfert en rendant complexe l'usage du code source. Toutefois, cette solution n'est que partielle et il semble difficile de se protéger totalement contre le risque de réutilisation de la technologie Webstreet. Des clauses limitatives sur les licences accordées devront probablement être ajoutées aux contrats (point à confirmer par l'équipe juridique).

Bien que les sites web livrés par Webstreet répondent à des normes de qualité particulièrement élevées, il existe tout de même un risque non nul qu'une faille de sécurité (dans le code source du site web ou une bibliothèque tierce) puisse être livrée en production. Dans un tel scénario, si la faille en question permettait un accès non autorisé à l'infrastructure du client, la responsabilité de Webstreet pourrait être engagée et la réparation des dommages en résultant pourrait être réclamée. Ce point devrait être abordé avec les équipes juridique pour inclure des clauses limitatives dans les contrats avec les clients afin de protéger Webstreet contre d'éventuels recours juridiques.

Mise en œuvre et adéquation de la solution

Capacité de mise en œuvre / Coût de la solution

D'un point de vue logiciel, dans le cadre du transfert de l'hébergement vers les clients les impacts directs se limitent à la mise à la mise à disposition du serveur de mise à jour et au développement d'un module permettant d'effectuer ces mises à jour chez le client.

Toutefois, l'implémentation de cette modification d'architecture nécessite de prendre en compte l'ensemble des impacts qui vont nécessiter des modifications majeures dans la manière de travailler avec les clients et de vendre les produits. Ces impacts représentent un coût important.

Il sera nécessaire d'améliorer au maximum l'automatisation des processus de déploiement et d'être capable de les industrialiser pour, à minima, les principaux fournisseurs de cloud. Ces modifications nécessitent des compétences qu'il n'a pas été actuellement possible d'identifier au sein des équipes Webstreet.

Le calendrier imposé (deux semaines) semble difficilement compatible avec la portée des modifications à apporter sans sacrifier la qualité et la sécurité habituelle des produits livrés aux clients.

Évaluation des risques identifiés pour la solution

Id.	Risque	Effet	Fréq.	Impact	Mesure d'atténuation
RSA-1	Risque projet : Dépassement des délais de livraison. Origine : Changement d'architecture au cours des développements.	Crit.	Freq.	Extreme	#1 : Renforcement des équipes. #2 : POC de la solution retenue avant de commencer le nouveau sprint.
RSA-2	Risque solution : Incapacité du client à déployer son site web. Origine : Manque de connaissance des besoins d'infrastructure.	Crit.	Likely	High	#1 : Améliorer la documentation fournie (à travers le D.A.T) #2 : Automatisation au maximum du processus de déploiement.
RSA-3	Risque solution : Défaillance (totale ou partielle) de la plateforme d'hébergement. Origine : Absence de maîtrise de l'infrastructure.	Crit.	Occasio.	High	#1 : Fournir des recommandations d'architecture technique et une configuration standardisée aux clients.
RSA-4	Risque solution : Vol des clefs SSH stockées chez un client aboutissant à un accès non autorisé à aux serveurs Webstreet. Origine : Environnement client non maîtrisé.	Cat.	Seldom	High	#1 : Mise en application des différentes recommandations formulés dans ce document.
RSA-5	Risque solution : Dépassement du délai de 72h pour mise en ligne d'un site web (objectif d'entreprise). Origine : Configuration de la plateforme d'hébergement par le client.	Crit.	Likely	High	#1 : Renforcement de l'automatisation de la plateforme.
RSA-6	Risque projet : Incohérence du produit livré avec les besoins réels des clients. Origine : Exigences fonctionnelles mal définies.	Marg.	Unlikely	Low	#1 : Conduite d'un atelier de réévaluation des besoins.

Tableau 9 : Évaluation des risques associés à la Solution B

Voir [Annexe](#) pour définition du modèle d'évaluation.

Adéquation avec les besoins exprimés

Id.	Besoin client identifié	Besoin couvert par la solution
BR-1	Permettre aux clients de réaliser une copie de tout ou partie de leur site.	OUI ✓
BR-2	Hébergement des Templates de site web par Webstreet.	OUI ✓
BR-3	Hébergement des données volumineuses par les clients.	OUI ✓
BR-4	Déploiement des mises à jour des sites web à partir de l'infrastructure de Webstreet.	OUI ✓
BR-5	Mise à jour centralisée des sites web.	OUI ✓

Tableau 10 : Évaluation de l'adéquation des besoins exprimés avec la Solution B

CONCLUSION – SOLUTION RETENUE

Les solutions A et B présentent toutes les deux avantages et inconvénients. Cependant, il est possible de noter que la solution « A » (Orientation Business – Gestionnaire de fichier web + IAM) se distingue par sa simplicité de mise en œuvre et par son très faible couplage à l'architecture. Les possibilités offertes par l'explorateur de fichiers permettent de répondre aux besoins des clients sans modifier les fondamentaux de l'entreprise.

Bien que la solution B présente une meilleure adéquation aux besoins, la complexité transférée aux clients pour le déploiement du site web entre en contradiction avec l'un des objectifs concurrentiels de l'entreprise : La mise à disposition d'un site web en 72h. Par ailleurs, les coûts de développements importants pour l'automatisation de la plateforme de déploiement adapté à de multiples fournisseurs et les nombreux impacts sur de plusieurs services de l'entreprise ne permettent pas d'envisager la possibilité de conduire ces travaux avec un niveau de qualité suffisant dans les délais imposés.

Pour ces raisons, **la solution A sera retenue comme solution à développer et à implémenter.**

Le document de définition d'architecture présente les détails de cette architecture.

ANNEXES

Méthodologie d'évaluation des risques

Le modèle d'évaluation des risques utilisé dans ce document utilise la terminologie définie par les publications de l'Open Group dans le cadre du Framework TOGAF¹ qui se basent sur deux critères :

- Les conséquences d'un risque sur le projet / la solution.
- La probabilité de survenue du risque.

La combinaison de ces deux facteurs permet d'aboutir à la matrice de classification ci-après :

Corporate Risk Impact Assessment					
Effect	Frequency				
	Frequent	Likely	Occasional	Seldom	Unlikely
Catastrophic	E	E	H	H	M
Critical	E	H	H	M	L
Marginal	H	M	M	L	L
Negligible	M	L	L	L	L

© The Open Group

Figure 5 : Modèle TOGAF d'évaluation des risques

La classification prévoit une notation du risque sur une échelle de 4 valeurs possibles :

- - **EXTREME** : Indique un risque extrême. Doit être impérativement atténué (en effet et / ou en probabilité).
- - **HIGH** : Indique un risque fort. Doit être atténué.
- - **MEDIUM** : Indique un risque moyen. Devrait être atténué par des mesures peu coûteuse.
- - **LOW** : Indique un risque faible. Ne nécessite pas de mesure d'atténuation, mais un suivi régulier est nécessaire.

Cette notation sera utilisée classer les risques du projet « Website Generator ».

Note :

Il est important de noter que cette évaluation se base sur une vision « instantanée » du projet. Un suivi régulier et une réévaluation des risques tout au long du projet est nécessaire pour garantir leur parfaite maîtrise.

¹ Source : <https://pubs.opengroup.org/architecture/togaf9-doc/arch/chap27.html>

Schéma HD : Solution A (Orientation Business)

Vue d'ensemble de la Solution A : Explorateur de fichier + IAM ("Commerciale")

WebStreet - Website Generator

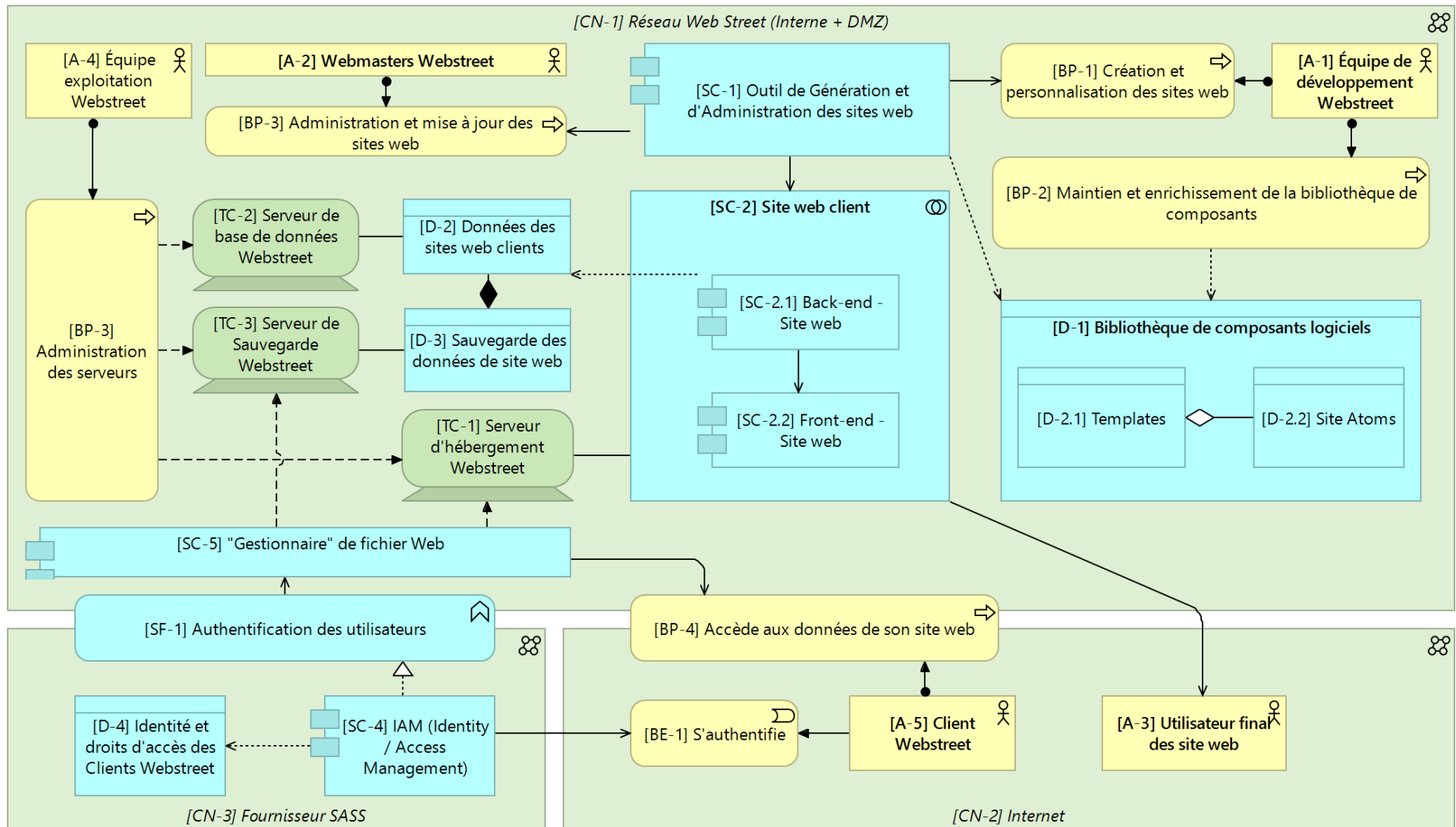


Figure 6 : Schéma HD - Solution A (Orientation Business)

Schéma HD : Solution B (Orientation Technique)

Vue d'ensemble de la Solution B : Hébergement par le client + Mises à jour à distance ("Technique")

WebStreet - Website Generator

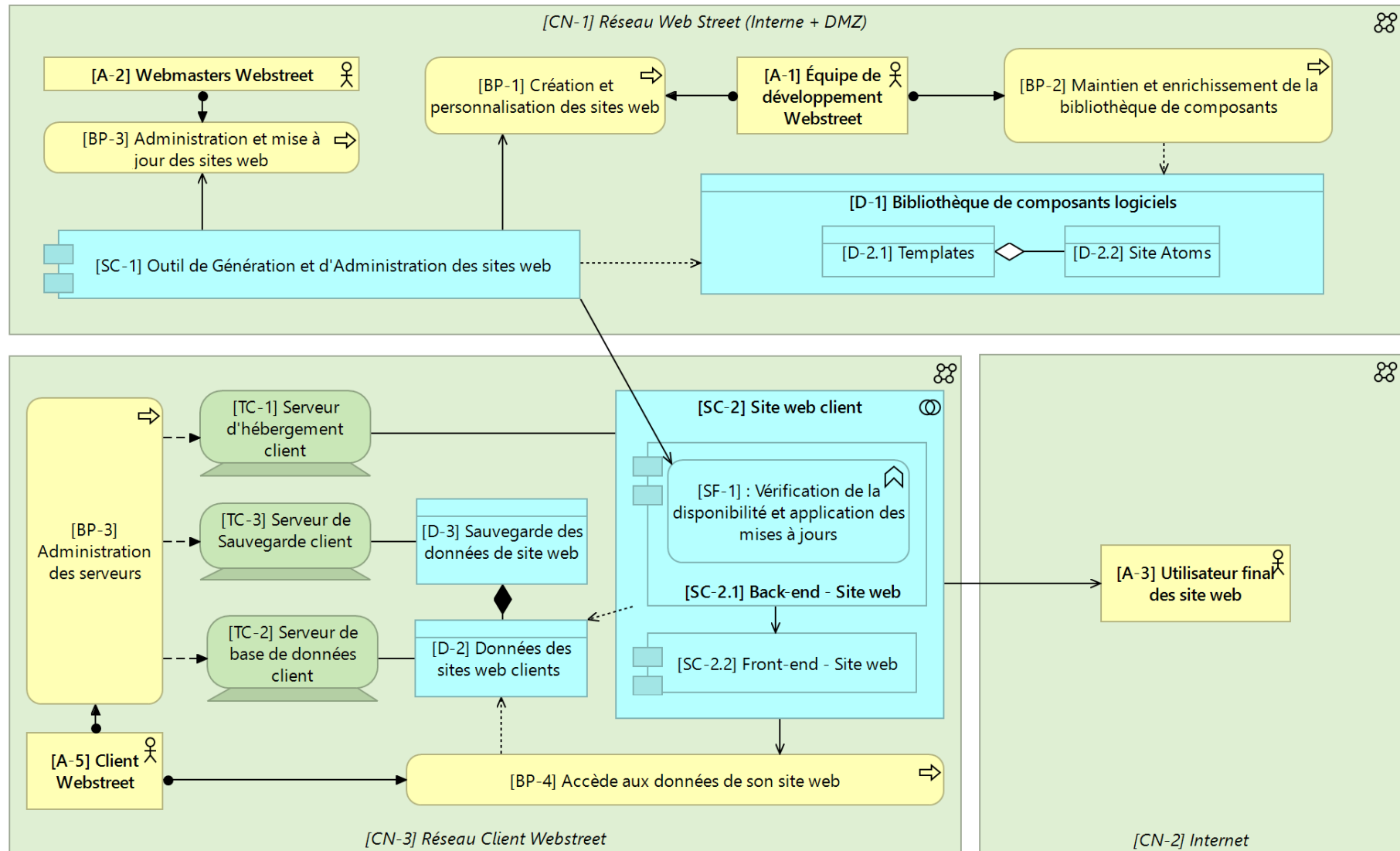


Figure 7: Schéma HD : Solution B (Orientation Technique)

TABLES DES RÉFÉRENCES

Figures

Figure 1 : Baseline Architecture - Vue d'ensemble de la plateforme de génération de site web	6
Figure 2 : Cartographie des parties prenantes et intérêts pour le projet.....	7
Figure 3 : Vue d'ensemble de l'implémentation de la solution A (Schéma HD en annexe)	12
Figure 4 : Vue d'ensemble de l'implémentation de la solution B (Schéma HD en annexe).....	17
Figure 5 : Modèle TOGAF d'évaluation des risques	25
Figure 6 : Schéma HD - Solution A (Orientation Business).....	26
Figure 7 : Schéma HD : Solution B (Orientation Technique).....	27

Tableaux

Tableau 1 - Historique des révisions	2
Tableau 2 : Liste des principes d'architecture	4
Tableau 3 : Matrice RACI (Rôle et responsabilité des parties prenantes)	9
Tableau 4 : Liste des nouveaux besoins identifiés	10
Tableau 5 : Synthèse des points forts / points faibles de la solution A.	13
Tableau 6 : Évaluation des risques associés à la Solution A.....	16
Tableau 7 : Évaluation de l'adéquation des besoins exprimés avec la Solution A.....	16
Tableau 8 : Synthèse des points forts / points faibles de la solution B.	18
Tableau 9 : Évaluation des risques associés à la Solution B.....	23
Tableau 10 : Évaluation de l'adéquation des besoins exprimés avec la Solution B.....	23

Nwcavertingoureyes