**DOCUMENT DE DÉFINITION D’ARCHITECTURE**

**- WEBSTREET -**



**David EVAN**

**28/10/2022**

**Version 1.0**

**Website Generator – WebStreet**

**Historique des révisions**

|  |  |  |  |
| --- | --- | --- | --- |
| **Numéro de version** | **Auteur** | **Description** | **Date de modification** |
| 1.0 | EVAN David  *(Architecte logiciel)* | Livraison initiale | 28/10/2022 |
|  |  |  |  |
|  |  |  |  |

Tableau - Historique des révisions

**Objectif du document**

Ce document présente la nouvelle architecture retenue dans le cadre des modifications d’architecture à apporter au projet de création d’un outil de génération de site web.

Une rapide introduction de l’approche architecturale retenue précède la présentation de l’architecture cible.

Une analyse des impacts de la nouvelle architecture conclu ce document.

La lecture de ce document suppose une connaissance préalable du *Framework d’Architecture* qui présente et justifie la plus part des choix retenus dans ce document.

**Table des matières**

[ARCHITECTURE DE RÉFÉRENCE 4](#_Toc117835874)

[Vue d’ensemble 4](#_Toc117835875)

[Contexte du changement d’architecture 4](#_Toc117835876)

[APPROCHE ARCHITECTURALE 5](#_Toc117835877)

[Briques d’architecture de références (ABB) 6](#_Toc117835878)

[Étude exploratoire de la stack technologique 7](#_Toc117835879)

[Choix préférés pour les outils et technologies 7](#_Toc117835880)

[Technologies pour l’authentification / l’autorisation 7](#_Toc117835881)

[Documentation complémentaire : 7](#_Toc117835882)

[Briques de solution de référence (SBB) 8](#_Toc117835883)

[Solution : IAM (SBB-1) 8](#_Toc117835884)

[Documentation complémentaire : 8](#_Toc117835885)

[Solution : Gestionnaire de fichier web (SBB-2) 9](#_Toc117835886)

[Synthèse de l’étude de la stack technologique 10](#_Toc117835887)

[ARCHITECTURE CIBLE 11](#_Toc117835888)

[Business 11](#_Toc117835889)

[Logiciel et données 11](#_Toc117835890)

[Plateforme technique 11](#_Toc117835891)

[ANALYSE DES IMPACTS 12](#_Toc117835892)

[Opérationnels 12](#_Toc117835893)

[Organisationnels 12](#_Toc117835894)

[Techniques 12](#_Toc117835895)

[Financiers 12](#_Toc117835896)

[Juridiques 12](#_Toc117835897)

[TABLES DES RÉFÉRENCES 13](#_Toc117835898)

[Figures 13](#_Toc117835899)

[Tableaux 13](#_Toc117835900)

# ARCHITECTURE DE RÉFÉRENCE

## Vue d’ensemble

Le schéma ci-avant présente une vue d’ensemble de l’architecture actuelle (dite « de référence ») de la plateforme de génération de site web en cours de développement.

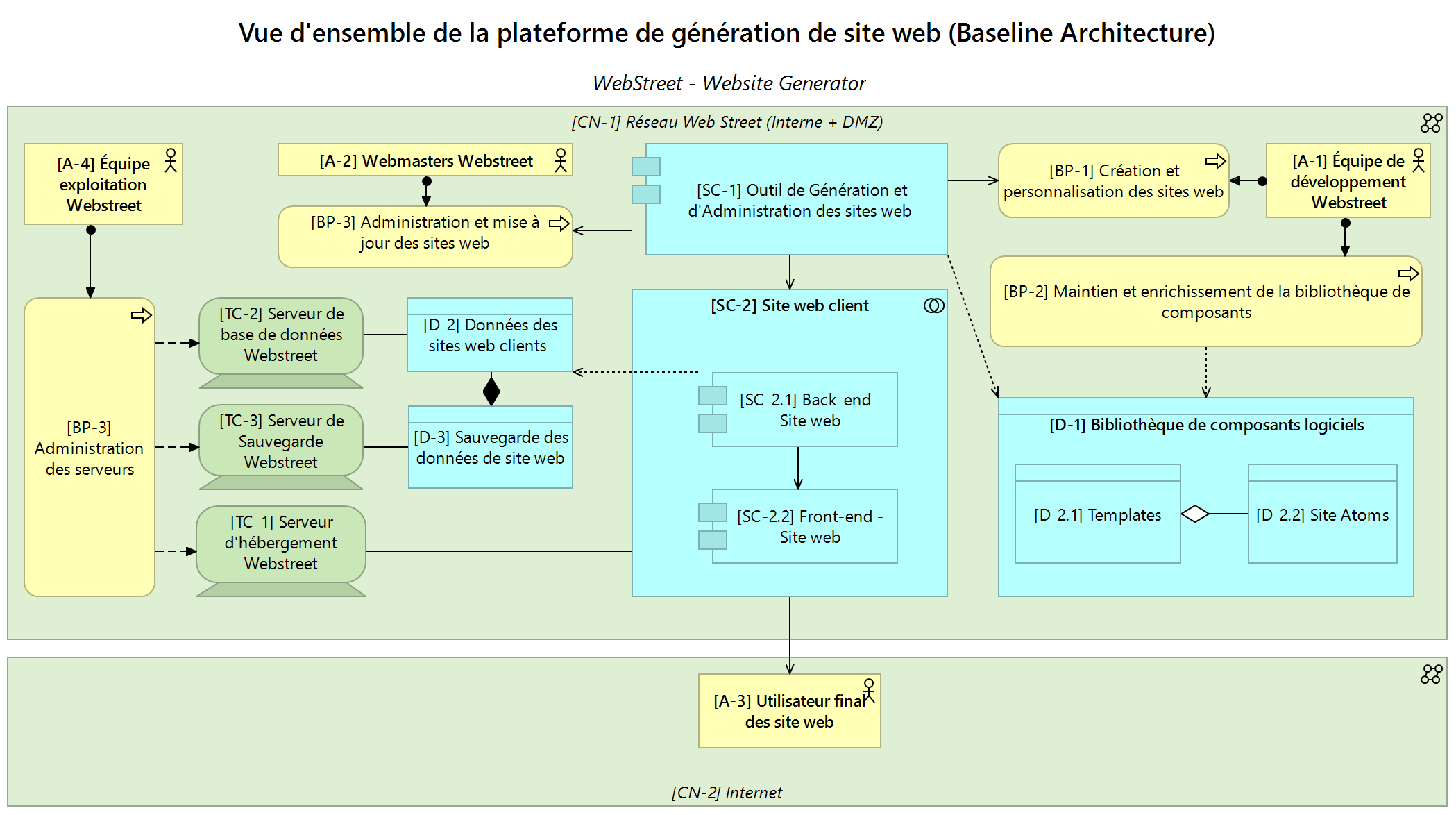


Figure : Vue d'ensemble de la Baseline Architecture

## Contexte du changement d’architecture

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 conception actuelle. Des modifications doivent être apportées au produit avant la livraison finale.

La section ***« Adaptation aux nouveaux besoins »*** du *Framework d’Architecture* décrit en détail ces nouveaux besoins.

# APPROCHE ARCHITECTURALE

Les choix justifiant l’approche architecturale retenue pour les modifications sont décrits dans le *Framework d’Architecture*.

Cette section présente les nouvelles briques d’architecture de référence (Architecture Building Blocks) à développer pour apporter ces modifications et compare les solutions sur lesquelles il est possible de s’appuyer pour l’implémentation de ces briques.

De manière synthétique, l’approche retenue consiste à ouvrir un accès aux serveurs de Webstreet à travers un « gestionnaire de fichier web » permettant aux clients de pouvoir disposer d’un accès direct à leurs site web et à leurs données sans modification dans l’hébergement. L’authentification et les droits d’accès sont gérés par un IAM.

Pour rappel, l’architecture cible retenue peut être représentée par la vue d’ensemble disponible ci-après (*Figure 2*).

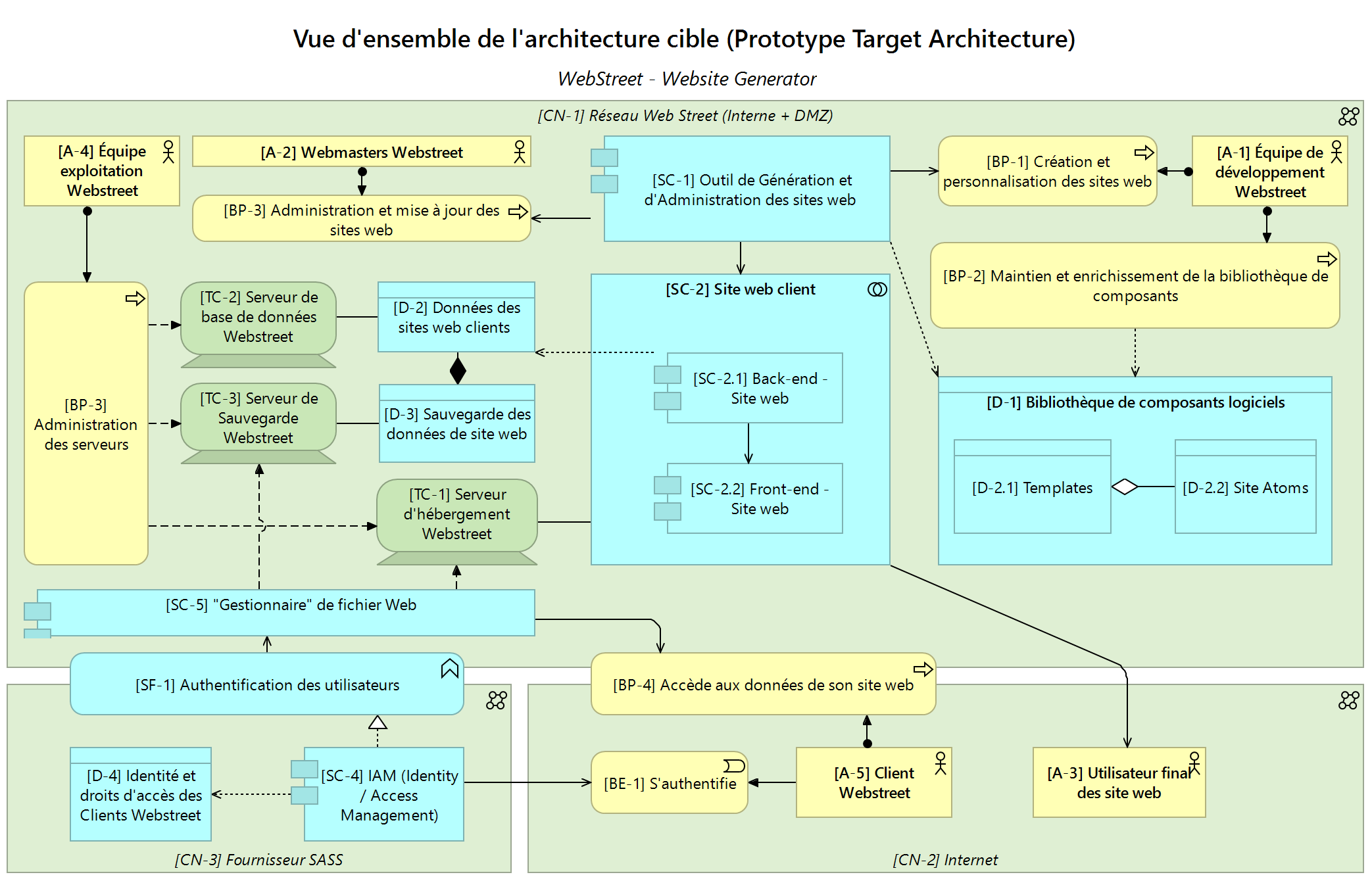


Figure : Vue d'ensemble de l'architecture cible (Prototype Target Architecture)

## Briques d’architecture de références (ABB)

La nouvelle architecture ne modifie aucun des composants développés dans l’architecture de référence.

Les nouvelles briques d’architecture (logicielles) à ajouter à la solution sont décrites dans le catalogue présenté ci-après :

|  |  |  |  |
| --- | --- | --- | --- |
| **Id.** | **ABB** | **Description** | **Type** |
| **ABB-1 (SC-4)** | IAM (IDENTITY AND ACCESS MANAGER) | Brique logicielle assurant l’authentification et la gestion des droits d’accès des utilisateurs.  Deux cas d’usage sont possibles :   * Permet aux utilisateurs de s’authentifier (MFA imposé) et de se voir accorder des droits d’accès en fonction de leur profil. * Permet aux ayant droits (administrateurs) de gérer les différents profils utilisateurs (création, modification, gestion des droits accordés, suppression …) | Logiciel |
| **ABB-2**  **(SC-5)** | GESTIONNAIRE DE FICHIER WEB | Brique logicielle permettant de visualiser, depuis un navigateur web, une liste de fichiers (indépendamment du format) stockés sur une machine distante.  Le périmètre de données accessible dépendant des droits d’accès attribué à l’utilisateur et fourni par le contexte d’authentification. | Logiciel |

Tableau : Catalogue des briques d'architecture de référence ajoutées (ABB)

De nombreuses solutions peuvent être retenue pour l’implémentation de ces briques d’architectures. Plusieurs solutions sont étudiées dans la section suivante.

## Étude exploratoire de la stack technologique

### Choix préférés pour les outils et technologies

Bien que les solutions puissent être des conceptions « from scratch », **les solutions préexistantes seront favorisées** dès lorsqu’ils répondent aux nouveaux besoins définis et que la tarification est adaptée. Cette approche vise à permettre d’assurer une livraison dans les délais imposés, une réduction des coûts de mise en œuvre et favorise une approche modulaire.

Les choix d’outils et de technologies retenues devront répondre à des critères de cohérence d’ensemble. Les solutions compatibles les unes par rapport aux autres et/ou facilement interopérables seront préférées. Ainsi, les solutions utilisant des protocoles standardisés et ouverts seront toujours préférées aux outils implémentant des protocoles non standardisés. Cette approche vise à favoriser l’évolutivité de l'architecture retenue.

Il est bien entendu indispensable que les solutions retenues garantissent un niveau de sécurité adéquat basé sur l’implémentation de technologies reconnues pour leurs fiabilités.

L’expérience utilisateur (que ce soit pour les clients ou les collaborateur) faisant partie intégrante de l’acceptation d’un outil dans un nouvel environnement, cet aspect, bien que subjectif, sera pris en compte pour le choix de la solution.

Notons que les critères de popularité des outils, de simplicité à trouver des ressources et des profils de collaborateurs expérimentés seront aussi analysés pour déterminer le choix de la solution.

Le coût des licences et l’adéquation au budget du projet (non défini au moment de la rédaction de ce document) seront pris en compte pour le choix final des solutions.

### Technologies pour l’authentification / l’autorisation

Afin de disposer d’une solution évolutive et pour permettre de simplifier l’ensemble des mécanismes d’authentification et d’autorisation, les technologies OAuth2 et sa couche d’identité OIDC (*Open ID Connect*) seront utilisées pour la gestion des accès aux ressources via un mécanisme de jeton d’accès (*access\_tokens*).

Les niveaux d’autorisation seront gérés à l’aide des *scopes* embarqués dans les jetons OAuth2 et les profils utilisateurs à l’aide des jetons d’identité (*id\_tokens). Étant hors du scope de ce document de définition d’architecture, le fonctionnement des mécanismes de l’authentification / autorisation seront abordés dans les spécifications techniques.*

##### Documentation complémentaire :

* <https://datatracker.ietf.org/doc/html/rfc6749>
* <https://openid.net/connect/>

### Briques de solution de référence (SBB)

#### Solution : IAM (SBB-1)

L’autorisation et l’authentification nécessite de faire appel à une solution IAM (Identity Access Manager) compatible avec les standards OAuth2 et OIDC afin de disposer d’une couche « universelle » d’authentification / d’identification / d’autorisation.

L’utilisation des technologies OAuth2 / OIDC permet de pouvoir facilement exploiter dans le gestionnaire de fichiers les contextes d’authentification transmis, incluant les droits d’accès.

Le recours à un fournisseur SAAS pour fournir 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).

Il est à noter que la solution doit embarquer plusieurs fonctionnalités avancées de sécurité parmi :

* Authentification MFA (OTP / Email / SMS …)
* Notification de connexion systématique par e-mail au client.
* 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.
* Politique de changement de mot de passe tous les 90 jours.

Bien que de nombreuses solutions soient envisageables (Okta, Gravitee, Azure AD, AWS IAM, Google Cloud IAM…), la solution SaaS **Auth0** sera retenue.

Ce choix se justifie par sa couverture totale des besoins associés à l’IAM, par simplicité d’utilisation pour les clients de Webstreet et par sa simplicité de configuration pour les administrateurs. Sa tarification peu élevée (< 500 € / an – jusqu’à 10.000 users actifs / mois) est compatible avec le projet.

En dernier lieu, l’outil est totalement personnalisable (avec le logo de la société Webstreet) et peut utiliser des noms de domaines personnalisés permettant un renforcement de l’image de marque et de la confiance des utilisateurs.

##### Documentation complémentaire :

* <https://auth0.com/docs/>

#### Solution : Gestionnaire de fichier web (SBB-2)

### Synthèse de l’étude de la stack technologique

# ARCHITECTURE CIBLE

## Business

## Logiciel et données

## Plateforme technique

# ANALYSE DES ÉCARTS

# ANALYSE DES IMPACTS

## Opérationnels

## Organisationnels

## Techniques

## Financiers

## Juridiques

# TABLES DES RÉFÉRENCES

## Figures

## Tableaux

[Tableau 1 - Historique des révisions 2](#_Toc94255517)

[Tableau 2 : Objectifs de chaque phases de l'ADM TOGAF 4](#_Toc94255518)