**DOCUMENT DE DÉFINITION D’ARCHITECTURE**

**- WEBSTREET -**



**David EVAN**

**12/11/2022**

**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 | 12/11/2022 |
|  |  |  |  |
|  |  |  |  |

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. *Pour un descriptif complet, le lecteur est invité à se référer au référentiel d’architecture de l’entreprise.*

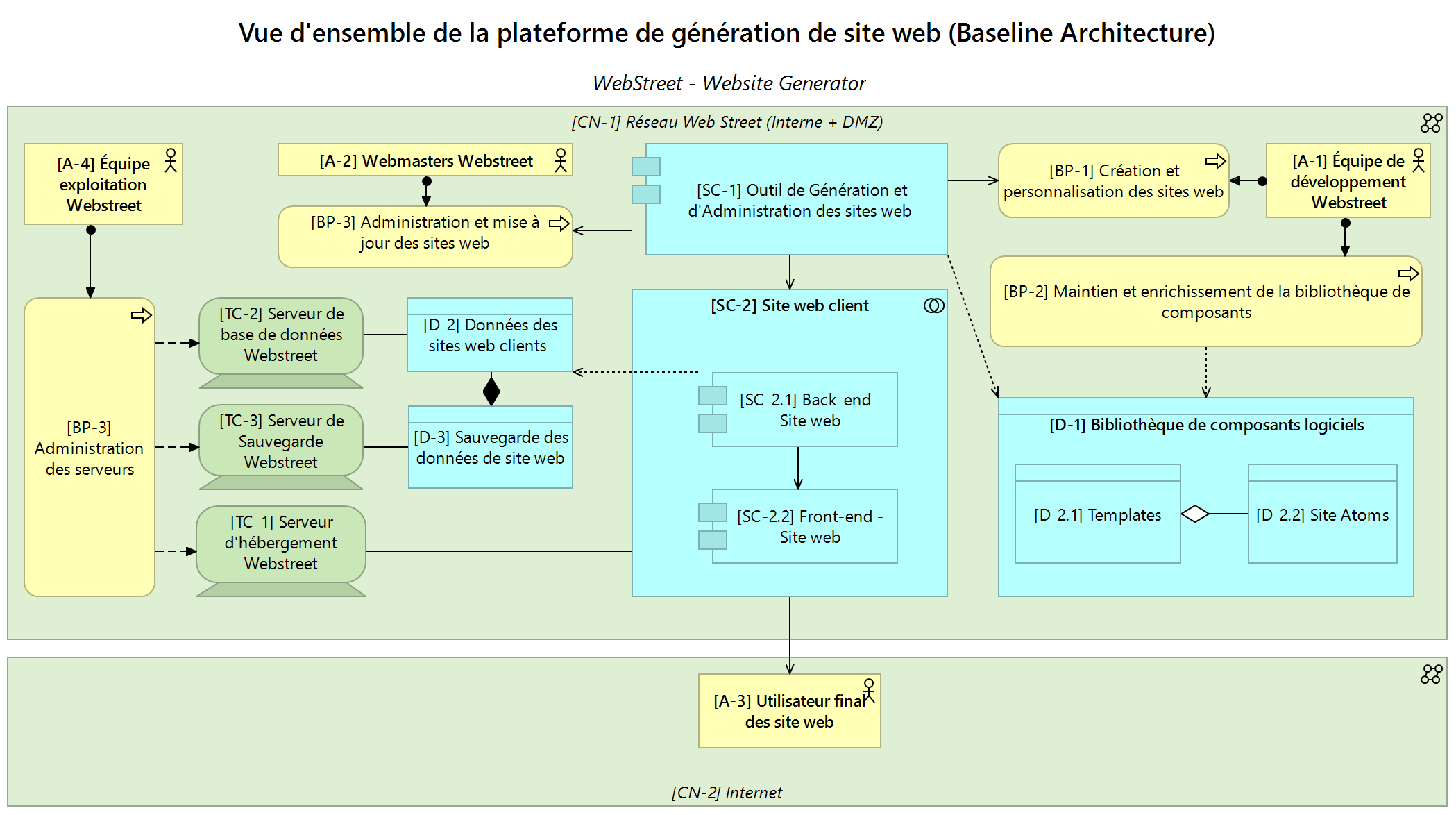


Figure 1 : Vue d'ensemble de la Baseline Architecture

## 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*).

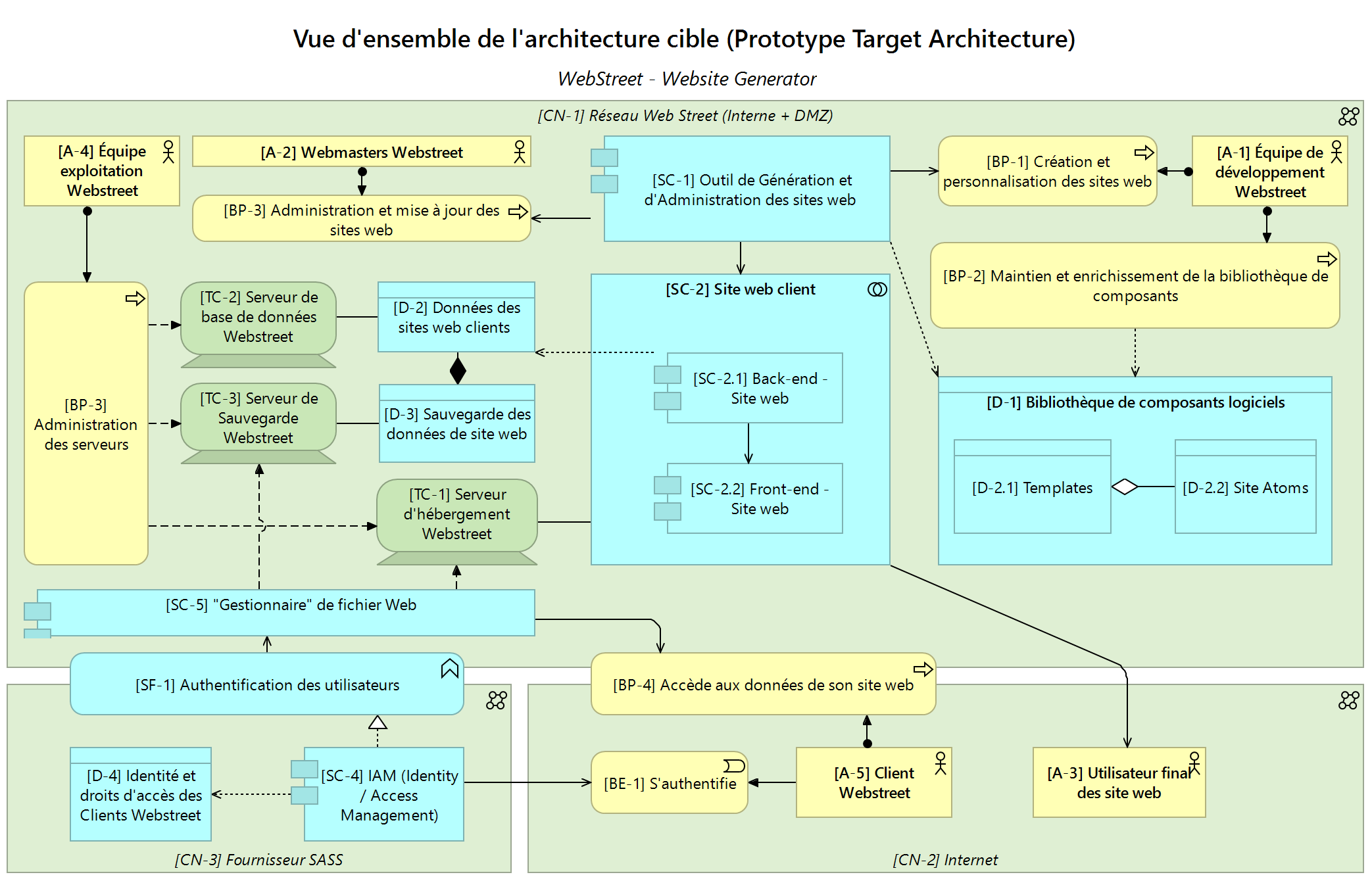


Figure 2 : Vue d'ensemble de l'architecture cible (Prototype Target Architecture)

## 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 utilisateurs 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.

Il est à noter qu’en fonction des précisions apportées aux exigences fonctionnelles / non fonctionnelles et de l’environnement dans lequel s’intégrera cette solution (ex : plateforme cloud AWS), un outil alternatif pourra être utilisé en remplacement du choix présenté ci-avant.

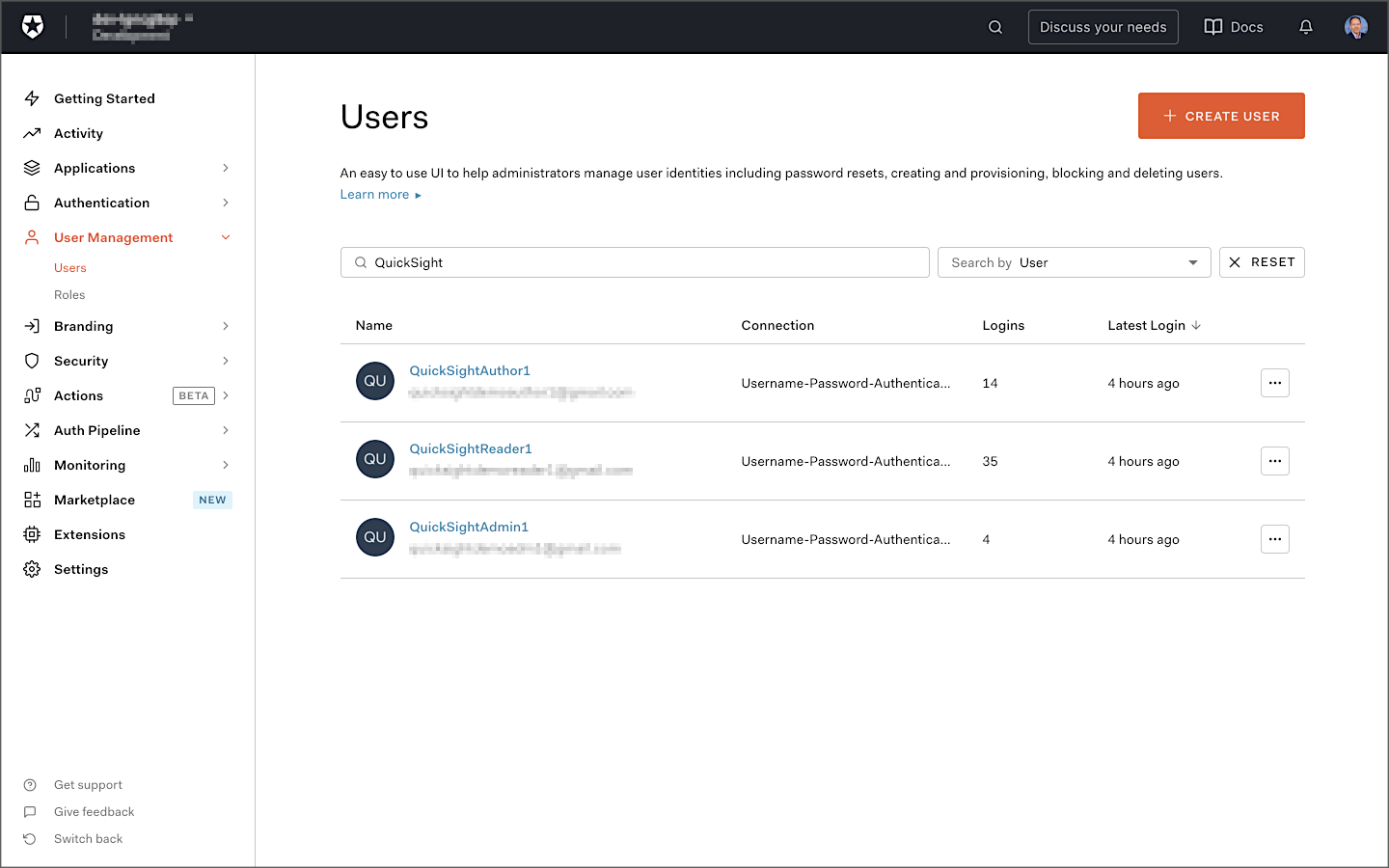


Figure 3 : Vue d'ensemble de la plateforme Auth0

##### Documentation complémentaire :

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

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

Afin de permettre aux utilisateurs de disposer d’un accès simple et familiers à leurs fichiers sans nécessiter de configuration complexe, l’utilisation d’un gestionnaire de fichier web a été retenu.

Le gestionnaire de fichier web se présente sous la forme d’une application web permettant de visualiser des fichiers dans une arborescence de dossiers de la même manière qu’un explorateur de fichier implémenté dans l’OS.

Cet outil doit délivrer les principales fonctionnalités suivantes :

* Fournir une interface graphique web permettant depuis un navigateur **desktop ou mobile** d’accéder à un fichier à la manière d’un explorateur de fichier « classique » (Windows, Mac, linux …).
* Téléchargement des fichiers, y compris volumineux, vers le PC.
* Gestion des droits d’accès pour faire varier les autorisations et le périmètre de données accessibles en fonction du contexte d’authentification.
* Disposer d’un moteur de recherche permettant de trouver un fichier dans l’arborescence à partir de son nom.

L’étude des fonctionnalités montre qu’il s’agit d’une solution très simple et générique. Le délai accordé pour la réalisation du projet ne permet d’envisager le développement d’une solution « From Scratch ».

Toutefois, afin de permettre de disposer de la capacité à faire évoluer facilement l’outil et permettre un déploiement rapide, la solution open-source « **Web File Browser** » sera retenue.

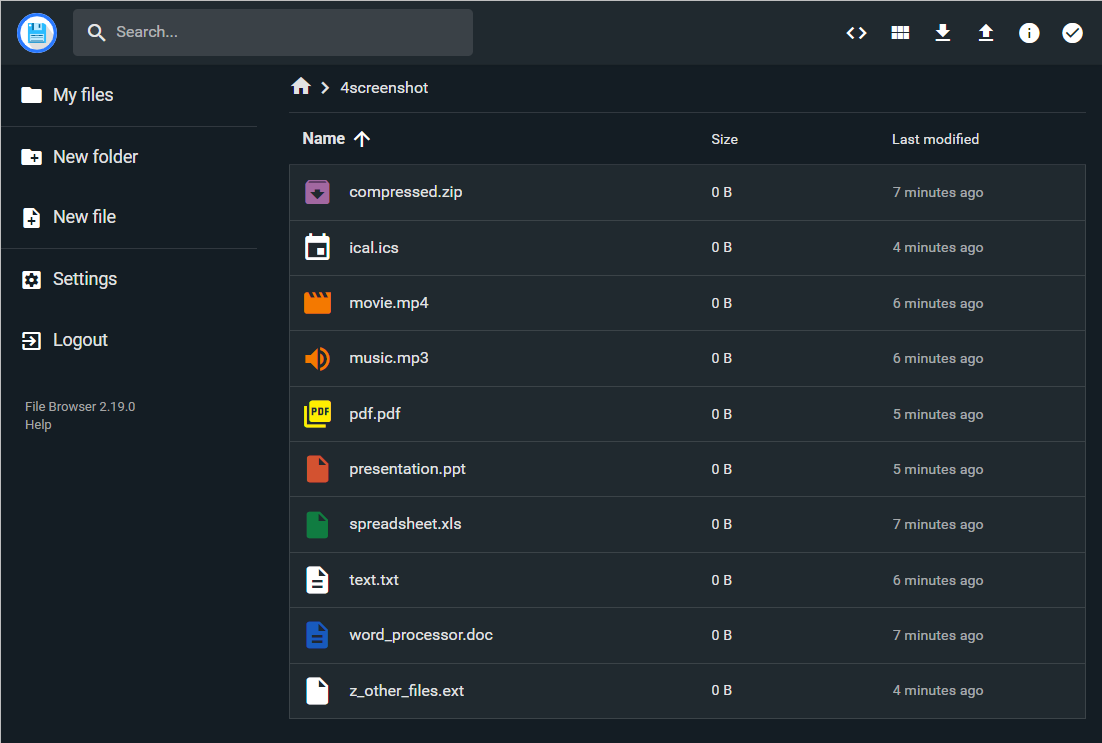


Figure 4 : Vue d'ensemble du logiciel opensource WebFile Browser

Ce projet libre fourni un outil « clé en main » pour lequel les besoins en personnalisations se limiteront à personnaliser la gestion des autorisations (déjà implémenté dans l’outil) pour les baser sur les *access\_tokens* délivréspar la solution d’authentification.

L’outil étant libre et sous licence Apache 2.0, son intégration dans les outils Webstreet ne nécessite pas l’acquisition de licence spécifique. Il est recommandé que les personnalisations apportés (gestion des autorisations basé sur token OAuth) fassent l’objet d’une demande de *merge request* sur le projet original afin de permettre à la communauté de bénéficier des améliorations apportées par Webstreet.

En dernier lieu, il est à noter que l’outil ne nécessite aucune spécification matérielle / logicielle particulière, permettant d’envisager l’installation sous n’importe quel environnement.

##### Documentation complémentaire :

* <https://github.com/filebrowser/filebrowser>

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

Le catalogue ci-après présente en synthèse les briques de solution misent en relation avec les briques d’architectures définies pour le projet.

|  |  |  |  |
| --- | --- | --- | --- |
| **Id. SBB** | **Référence  aux ABB** | **Solution** | **Rôle** |
| **SBB-1** | ABB-1 | Auth0 | Authentification / Autorisation |
| **SBB-2** | ABB-2 | Web File Browser | Explorateur de fichier web |

Tableau : Catalogue des briques de solution de référence (SBB)

# ARCHITECTURE CIBLE

Cette section fourni un descriptif des nouveaux processus, logiciels, données et infrastructures qui seront ajoutés à l’architecture de référence.

## Business

Le schéma ci-après présente les nouveaux processus métiers, acteurs et différents artefacts business ajoutés à l’architecture de référence.

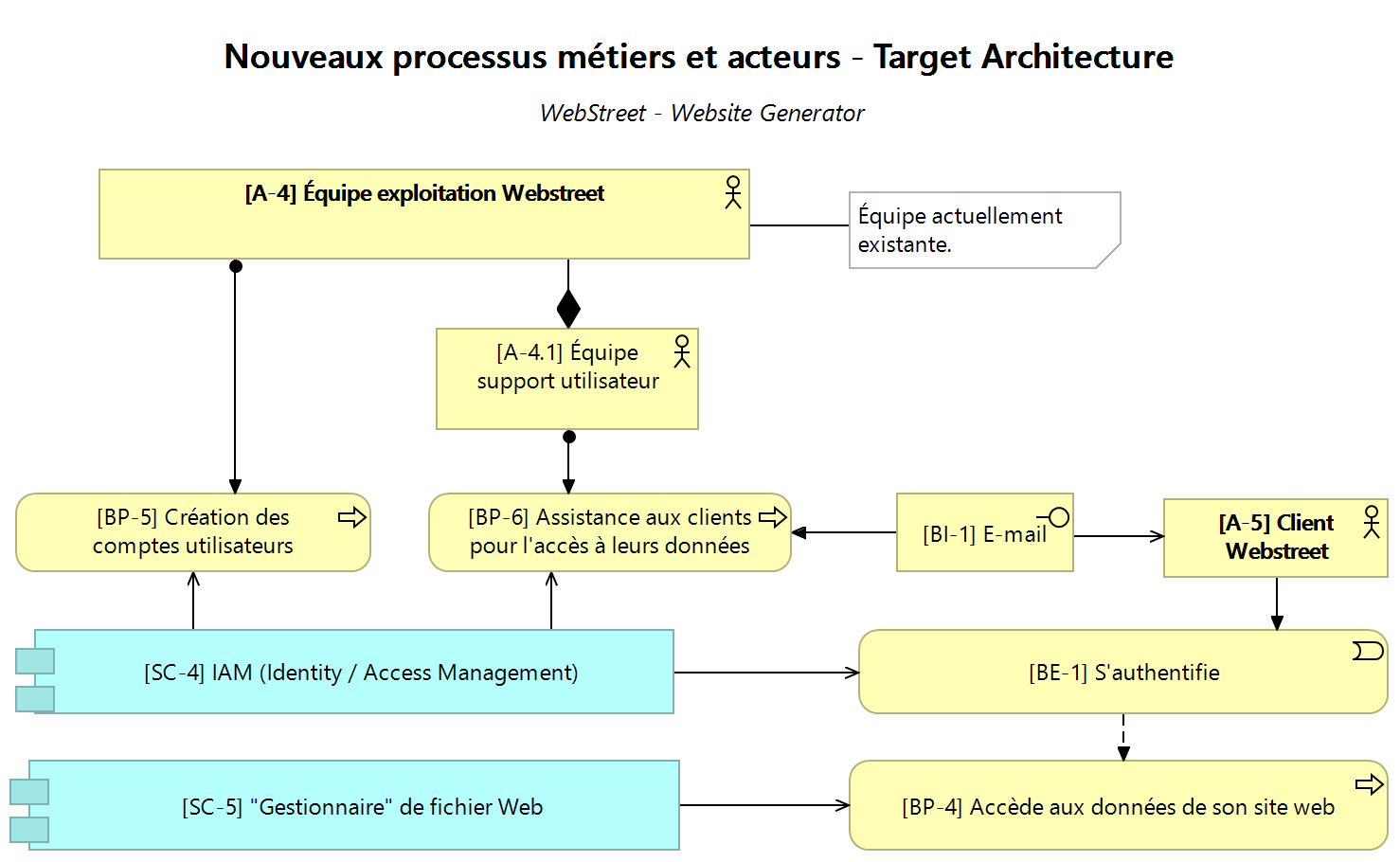


Figure 5 : Business view - Target Architecture

Le catalogue ci-après fourni la description des nouveaux artefacts ajoutés.

|  |  |  |  |
| --- | --- | --- | --- |
| **Type d’artefact** | **Id.** | **Nom** | **Description** |
| **Acteur** | **A-4.1** | Équipe support utilisateur | Nouvelle équipe de support client pour l’accès à leurs données. Peut être composé de l’équipe support actuel (non identifié) ou de membres de l’équipe exploitation intervenant par roulement. Cette nouvelle équipe assiste les clients pour l’accès à leurs données (BP-6) via l’adresse e-mail de support dédié (BI-1). |
| **A-5** | Client Webstreet | Client webstreet. Peut s’authentifier (BE-1) pour accéder à ses données (BP-4) et contacter par e-mail (BI-1) l’équipe support (A-4.1) pour obtenir une assistance en cas de difficultés. |
| **Processus Business** | **BP-4** | Accède aux données de son site web | Nouveau processus client permettant l’accès à ses données par l’intermédiaire du gestionnaire de fichier web (SC-5). Requière une authentification préalable du client (BE-1). |
| **BP-5** | Création des comptes utilisateurs | Processus métier d’entreprise assigné à l’équipe d’exploitation Webstreet (A-4). Ce processus permet la création des comptes utilisateurs des clients webstreet (A-5) sur l’IAM (SC-4). Ce processus sera à intégrer à la conception des sites web. |
| **BP-6** | Assistance aux clients pour l'accès à leurs données | Processus métier d’entreprise assigné à l’équipe de support utilisateur (A-4.1) permettant aux clients (A-5) d’obtenir une assistance pour l’accès à leurs données (BP-4). Les demandes d’assistance proviennent de l’adresse e-mail de support dédié (BI-1). |
| **Interface** | **BI-1** | E-mail | Nouveau canal de communication pour les clients (A-5). Adresse e-mail de support dédié aux demandes d’assistance clients pour l’accès aux données (BP-6). |
| **Evénement métier** | **BE-1** | S’authentifie | Événement client. Authentification des clients (A-5) à travers l’IAM (SC-4). Obligatoire pour les clients avant d’accéder à leurs données (BP-4). |

Tableau : Catalogue des nouveaux artefacts business – Target Architecture

## Logiciel et données

Le schéma ci-après présente les nouveaux composants logiciels, fonctions et données ajoutés à l’architecture de référence.

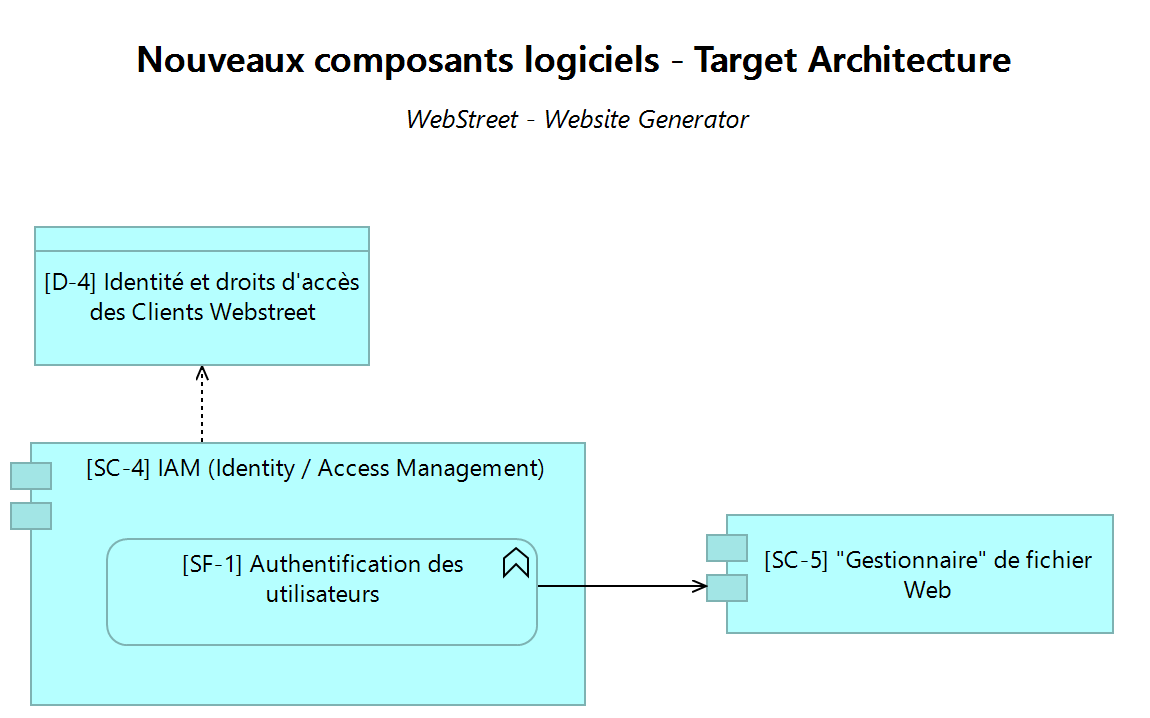


Figure 6 : Software view - Target Architecture

Le catalogue ci-après fourni la description des nouveaux artefacts ajoutés.

|  |  |  |  |
| --- | --- | --- | --- |
| **Type d’artefact** | **Id.** | **Nom** | **Description** |
| **Composant logiciel** | **SC-4** | IAM (Identity and Access Management) | Logiciel d’authentification des utilisateurs et de gestion des droits d’accès. Assure l’authentification des utilisateurs (SF-1) sur le Gestionnaire de fichier (SC-5). Les droits d’accès (D-4) sont transmis à travers les scopes OAuth2. |
| **SC-5** | "Gestionnaire" de fichier Web | Logiciel permettant de consulter les fichiers présents sur les serveurs web Webstreet. Est accessible uniquement après authentification (SF-1) sur l’IAM (SC-4). Le périmètre de données est variable en fonction du contexte d’authentification. |
| **Fonction logicielle** | **SF-1** | Authentification des utilisateurs | Fonction logicielle implémentée par l’IAM permettant d’assurer l’authentification des utilisateurs. Basé sur le framework d’autorisation OAuth2. |
| **Données** | **D-4** | Identité et droits d'accès des Clients Webstreet | Données l’exploité par l’IAM. Contient les informations d’identification et d’autorisation pour chaque utilisateur. Accessible uniquement au travers de l’IAM (SC-4). |

Tableau : Catalogue des nouveaux artefacts softwares - Target Architecture

## Plateforme technique

Le schéma ci-après présente les nouveaux flux de transferts et réseaux de communication et machines ajoutés à l’architecture de référence.

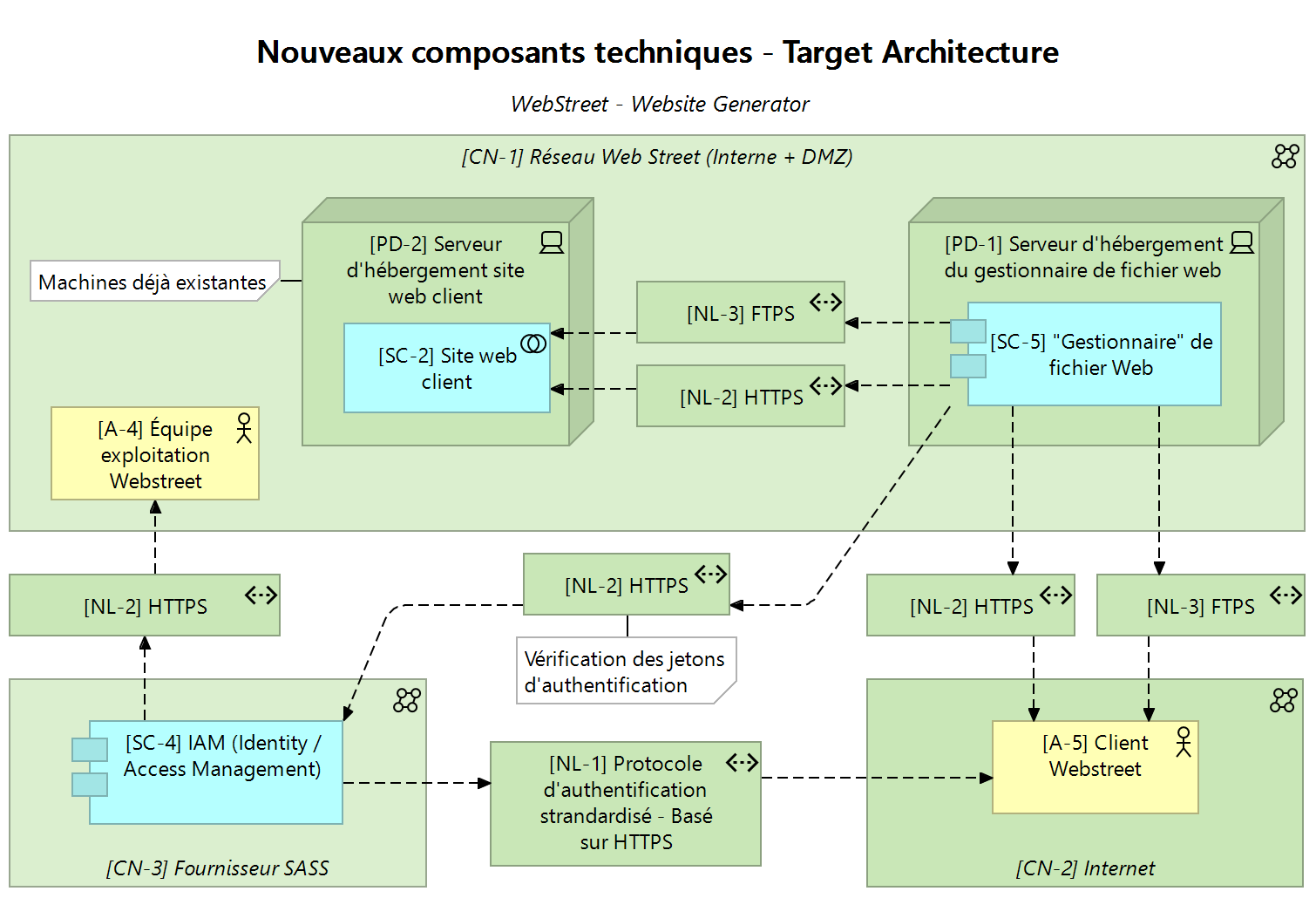


Figure 7 : Technical view - Target Architecture

Le catalogue ci-après fourni la description des nouveaux artefacts ajoutés.

|  |  |  |  |
| --- | --- | --- | --- |
| **Type d’artefact** | **Id.** | **Nom** | **Description** |
| **Machine physique** | **PD-1** | Serveur d'hébergement site web client | Serveurs d’hébergement des sites web des clients Webstreet. Stocke les fichiers accessibles par l’intermédiaire du Gestionnaire de fichier web (SC-5) Actuellement existant dans l’architecture. |
| **PD-2** | Serveur d'hébergement du gestionnaire de fichier web | Serveur assurant l’hébergement du gestionnaire de fichier web (SC-5). |
| **Protocoles d’échanges** | **NL-1** | Protocole d'authentification standardisé - Basé sur HTTPS | Protocole d’authentification standardisé (échange de jetons d’authentification OAuth 2 dans le cas présent) permettant à l’IAM (SC-4) de délivrer le contexte d’authentification. |
| **NL-2** | HTTPS | Échange réseau basé sur le protocole HTTPS. |
| **NL-3** | FTPS | Échanges réseaux basé sur le protocole FTPS. Utilisé pour l’échange de fichier volumineux. |
| **Réseau** | **CN-1** | Réseau Webstreet (interne + DMZ) | Réseau interne à l’entreprise Webstreet. Relie notamment le serveur déhebrgement du gestionnaire de fichier (PD-1) aux serveurs d’hébergement des sites web client (PD-2). |
| **CN-2** | Internet | Réseau internet. |
| **CN-3** | Fournisseur SASS | Fournisseur du logiciel IAM (SC-4) fonctionnant en mode SASS. Auth0 dans le cas présent. |

Tableau : Catalogue des nouveaux artefacts techniques – Target Architecture

# ANALYSE DES ÉCARTS

Les écarts entre l’architecture de référence et l’architecture cible sont présenté dans le tableau ci-après.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Id Comp.** | **Catégorie** | **Nom** | **Ajouté** | **Modifié** | **Supprimé** | **Inchangé** |
| **A-4** | **Business** | Équipe exploitation Webstreet |  |  |  | X |
| **A-4.1** | Équipe support utilisateur | X |  |  |  |
| **A-5** | Client Webstreet | X |  |  |  |
| **BP-4** | Accède aux données de son site web | X |  |  |  |
| **BP-5** | Création des comptes utilisateurs | X |  |  |  |
| **BP-6** | Assistance aux clients pour l'accès à leurs données | X |  |  |  |
| **BI-1** | E-mail | X |  |  |  |
| **BE-1** | S’authentifie | X |  |  |  |
| **SC-4** | **Software** | IAM (Identity and Access Management) | X |  |  |  |
| **SC-5** | "Gestionnaire" de fichier Web | X |  |  |  |
| **SF-1** | Authentification des utilisateurs | X |  |  |  |
| **D-4** | Identité et droits d'accès des Clients Webstreet | X |  |  |  |
| **PD-1** | **Physical** | Serveur d'hébergement site web client |  |  |  | X |
| **PD-2** | Serveur d'hébergement du gestionnaire de fichier web | X |  |  |  |
| **NL-1** | Protocole d'authentification standardisé - Basé sur HTTPS | X |  |  |  |
| **NL-2** | HTTPS | X |  |  |  |
| **NL-3** | FTPS | X |  |  |  |
| **CN-1** | Réseau Webstreet (interne + DMZ) | X |  |  |  |
| **CN-2** | Internet |  |  |  | X |
| **CN-3** | Fournisseur SASS | X |  |  |  |

Tableau : Catalgoue des écarts d'architecture

# ANALYSE DES IMPACTS

## Opérationnels

## Organisationnels

## Techniques

## Financiers

## Juridiques

# TABLES DES RÉFÉRENCES

## Figures

[Figure 1 : Vue d'ensemble de la Baseline Architecture 4](#_Toc119119194)

[Figure 2 : Vue d'ensemble de l'architecture cible (Prototype Target Architecture) 5](#_Toc119119195)

[Figure 3 : Vue d'ensemble de la plateforme Auth0 9](#_Toc119119196)

[Figure 4 : Vue d'ensemble du logiciel opensource WebFile Browser 10](#_Toc119119197)

[Figure 5 : Business view - Target Architecture 12](#_Toc119119198)

[Figure 6 : Software view - Target Architecture 14](#_Toc119119199)

[Figure 7 : Technical view - Target Architecture 15](#_Toc119119200)

## Tableaux

[Tableau 1 - Historique des révisions 2](#_Toc119119201)

[Tableau 2 : Catalogue des briques d'architecture de référence ajoutées (ABB) 6](#_Toc119119202)

[Tableau 3 : Catalogue des briques de solution de référence (SBB) 11](#_Toc119119203)

[Tableau 4 : Catalogue des nouveaux artefacts business – Target Architecture 13](#_Toc119119204)

[Tableau 5 : Catalogue des nouveaux artefacts softwares - Target Architecture 14](#_Toc119119205)

[Tableau 6 : Catalogue des nouveaux artefacts techniques – Target Architecture 16](#_Toc119119206)

[Tableau 7 : Catalgoue des écarts d'architecture 17](#_Toc119119207)