Documentation de l'architecture

Projet : Création d'une PoC

Sommaire

Ce document définit le plan de test de la nouvelle architecture

Historique

Date	Version	Commentaires
01/02/2023	0.1	Création du document
08/02/2023	0.2	Analyse des contraintes et risques
15/02/2023	0.3	Architecture cible
22/02/2023	1.0	Finalisation du document

Description de l’architecture cible

Microservices

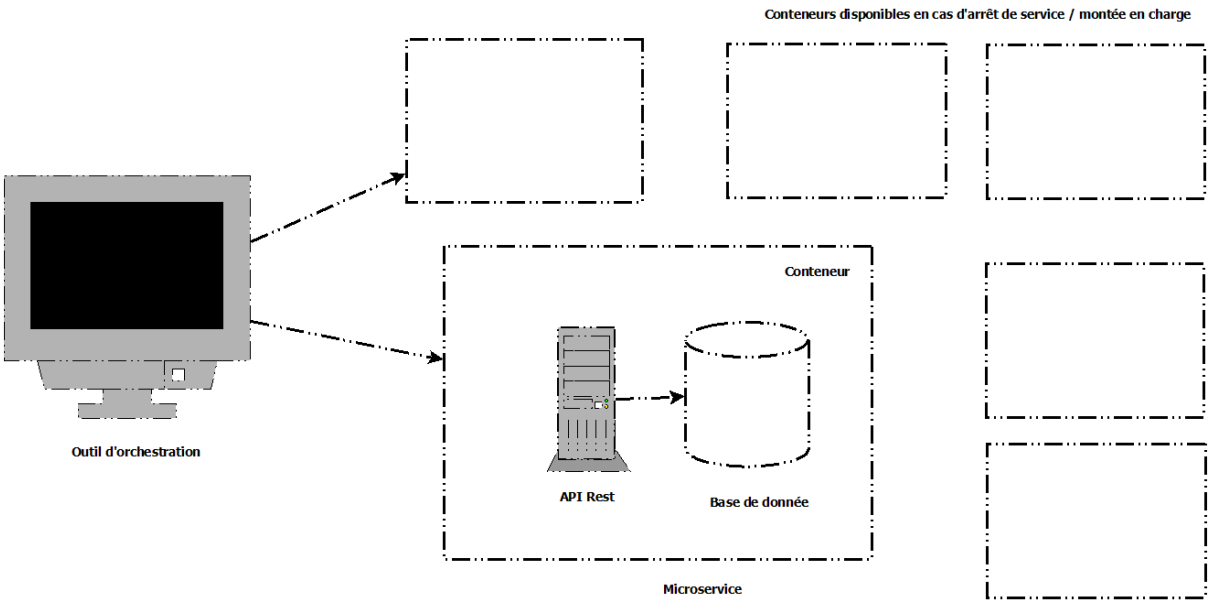
Les services seront développés en suivant le pattern architectural de microservices, qui consiste à regrouper les différents services et fonctionnalités en microservices. Chaque service ne doit pas dépendre des autres services pour fonctionner.

Chaque microservice consiste en une API Rest et une base de données qui lui est associée. Ainsi, dans notre cas, nous prévoyons d’avoir, à termes, un microservice pour :

- La gestion des hôpitaux;
- La gestion des docteurs;
- La gestion des patients;
- La gestion des rendez-vous;
- La gestion des urgences;

Ces microservices pourront bien évidemment avoir besoin d'interagir, mais tout le processus de CI/CD contenant notamment la build, les tests, le déploiement, le packaging et ensuite l’orchestration devront être totalement indépendants.

Chaque microservice est hébergé dans un docker qui lui est dédié, et plusieurs instances de dockers peuvent être orchestrées pour permettre de gérer les arrêts de service ou les situations de stress.



Orchestration de microservices

Front-end

Le front-end devra être développé en collaboration avec les développeurs back-end car il sera l'intermédiaire entre les APIs et l'utilisateur.
En développant des front-end compatibles avec différents navigateurs, sous forme de client lourd voir même avec des objets connectés, on permet une accessibilité presque totale que l'on peut adapter en fonction des différents acteurs et intervenants du monde de la santé.

On peut par exemple imaginer les médecins et les infirmiers utiliser des tablettes pour mettre à jour les données du patients, les lits disponibles ou pour visionner leur rendez-vous. Par contre, la gestion de certaines ressources, la prise de rendez-vous ou la gestion d'urgence seront potentiellement supervisées sur des clients lourds. Finalement, les patients pourront signaler une urgence via leur navigateur ou une application mobile, voir tout simplement un numéro de téléphone.

API Gateway

L'API Gateway est un outil de management d'API qui s'introduit entre les interfaces graphiques et le back-end et facilite notamment la gestion des requêtes HTTPS. Son but est de rediriger les requêtes vers les APIs concernées après avoir analysé et déterminé la nature de la requête.
L'API Gateway peut également jouer un rôle en matière de sécurité, en refusant tous les appels à l'API dont l'origine ou le contenu serait douteux.

Authentification

L’authentification est effectuée via un SSO et en suivant la norme OAuth 2.0. Cette norme consiste à gérer les identifiants, l’identité et les autorisations de l’utilisateur via un système de token OAuth 2.0 dont la validité est limitée dans le temps.
Ce système d’authentification est la norme actuelle de l’industrie en matière d'authentification et peut être couplée à un système d’identification forte. Cela permet également à l’application de ne pas avoir à gérer l’authentification, ce qui simplifie le code et à de nombreux avantages de sécurité.

Cloud

Nous conseillons fortement l’utilisation d’un Cloud pour les nombreux avantages qu’il présente. Pour n’en citer que quelques uns :

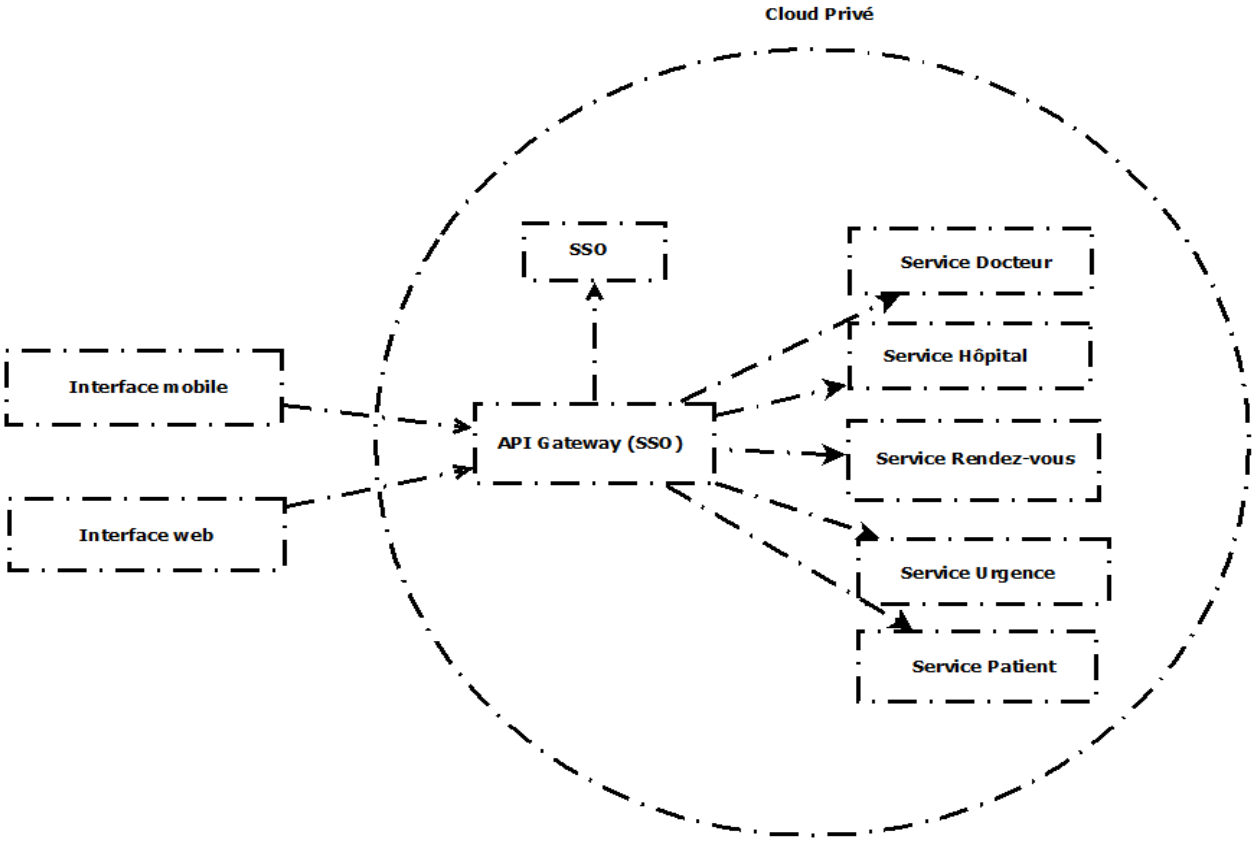
- Rapidité de déploiement et de modification de l’architecture ou du code;
- Sous-traitance des infrastructures par le fournisseur Cloud;
- Utilisation des nombreuses offres Cloud (back-up, failover, archivage..);
- Avantage de sécurité à ne pas être hébergé sur site;

Il faut cependant faire attention à choisir l’offre avec soin et à bien évaluer chacune des options qui peuvent s’avérer rapidement coûteuses.

Le choix du type de Cloud est également très important; les trois possibilités sont un cloud public, un cloud privé ou un cloud hybride. La qualité de la protection des données sensibles dépendra largement du choix du type du Cloud.
Si le budget le permet, nous conseillons le choix d’un Cloud privé.

Certaines certifications existent pour les hébergeurs de données de santé. Nous conseillons de prêter une attention particulière lors du choix du ou des fournisseurs.

Architecture Cible



Architecture haut niveau

Key Performance Indicator

KPI	Niveau attendu
Respect des SLA	100%
Rapidité de déploiement	Moins d'une demi-heure
Rapidité de traitement des requêtes HTTPS	10 000 par secondes
Mise à jour des composants utilisés	100%
Fail-over des composants primordiaux	100%
Validation des tests O'Wasp	100%
Validation de la sécurité des données par le DPO	100%
Cryptage des données passantes	100%

Signature

Responsable	Signature
Kara Trace	
Conseil d'administration de MedHead	