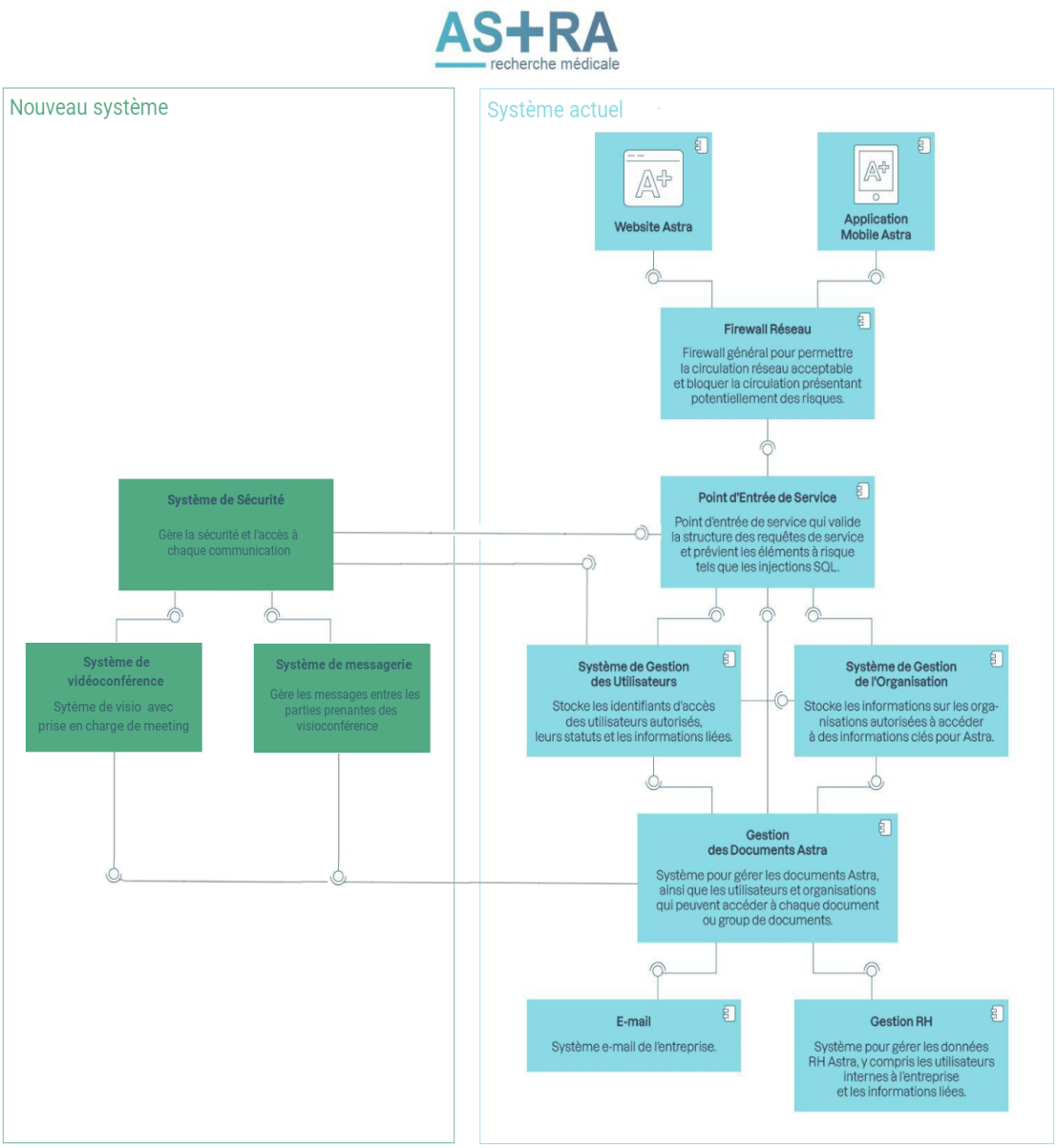
AS+RA recherche médicale

Document de définition d'architecture

Système de vidéo-conférence

Table des matières

1. Modification de l’architecture existante



Framework d’architecture

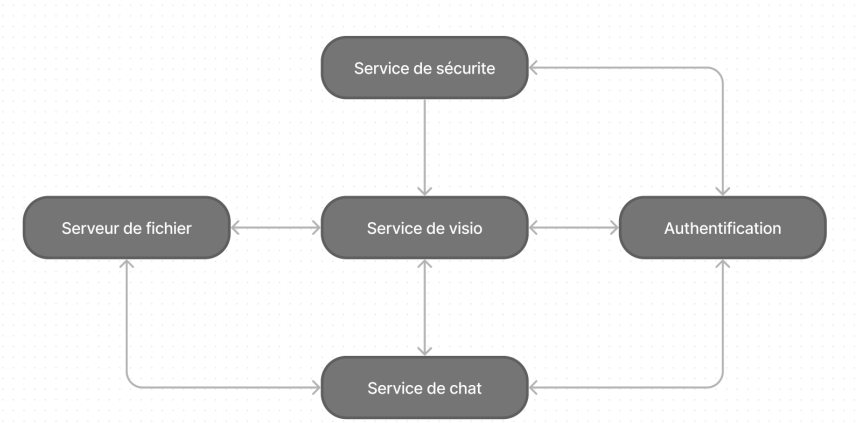
L’architecture existante d'Astra intégrera un système de vidéo-conférence sous la forme d’un service indépendant. Les modifications incluent l'ajout de services dédiés à la visioconférence et à la sécurisation des communications. Ces services sont conçus pour être interopérables, modulaires et conformes aux exigences strictes en matière de protection des données.

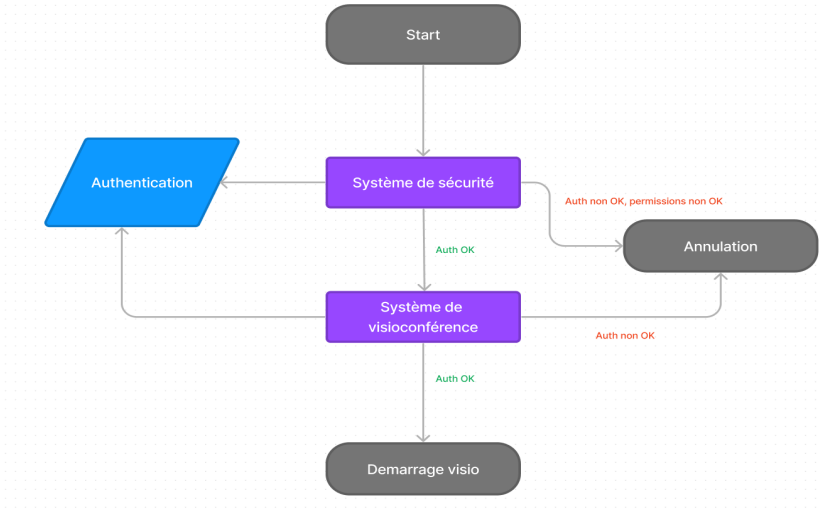
Composants et interactions

- **Service de Gestion des Utilisateurs et des Organisations**: Interagit avec le système de gestion des utilisateurs et l'application pour authentifier les participants.
- **Service de Visioconférence**: Communique avec les clients web et mobiles pour fournir des capacités de réunion en temps réel et gère le streaming audio et vidéo.
-
- **Service de Messagerie Chat**: Communique avec les clients web et mobiles pour fournir des capacités de messagerie en temps réel.

- **Service de Gestion des Documents**: Interagit avec le service de gestion des utilisateurs pour autoriser l'accès aux documents sur la base du rôle et de l'organisation.

- **Service de Sécurité**: Fournit des fonctionnalités transversales pour assurer la sécurité à tous les niveaux de l'architecture.





Mise en place des changements

Phase 1 : Feuille de route architecturale, mise en place serveurs

1. **Configuration du Serveur :** Installation et configuration des serveurs nécessaires, adaptés à l'approche d'hébergement choisie (locale ou cloud).
2. **Installation :** Mise en place et configuration des instances pour la visioconférence et et le système de messagerie.
3. **Intégration avec les Systèmes Existant :** Assurer une intégration harmonieuse avec le système d'authentification actuel et le serveur de fichiers.

Phase 2 : Microservices personnalisés, interface utilisateur

1. **Développement des Microservices :** Création de microservices sur mesure pour répondre aux besoins spécifiques d'Astra.
2. **Personnalisation de Jitsi et Matrix :** Adapter ces solutions pour qu'elles s'intègrent de manière transparente dans l'environnement d'Astra.
3. **Conception de l'Interface Utilisateur :** Développement d'interfaces utilisateur intuitives pour faciliter l'accès et l'utilisation par les employés d'Astra.

Phase 3 : Système de sécurité, permissions, audit

1. **Mise en Œuvre de la Sécurité :** Implémenter des mesures de sécurité complètes, y compris le chiffrement et la gestion des accès.
2. **Audits et Tests de Sécurité :** Réalisation d'audits pour détecter et corriger les vulnérabilités.
3. **Assurance de la Conformité :** Veiller à ce que le système respecte les réglementations pertinentes.

Phase 4 : Rapport de tests, tests techniques

1. **Tests Unitaires et d'Intégration :** Effectuer des tests approfondis pour vérifier le bon fonctionnement de chaque composant et leur intégration.
2. **Tests de Performance :** Évaluer la robustesse du système sous différents niveaux de charge.
3. **Tests Utilisateur :** Conduire des essais avec les utilisateurs finaux pour s'assurer de l'ergonomie et de l'efficacité du système.

Phase 5 : Déploiement sur serveur, mise à disposition

1. **Mise en Service Progressive :** Déployer le système par étapes, en intégrant progressivement les nouvelles fonctionnalités.
2. **Surveillance et Optimisation :** Monitorer le système pour identifier et résoudre les problèmes de performance ou fonctionnels.
3. **Formation des Utilisateurs :** Organiser des sessions de formation pour les employés, afin de les familiariser avec le nouveau système de visioconférence.

2. Nouvelle solution de l’architecture

Nous avons opté pour l'architecture orientée microservices pour le système de visioconférence en raison de sa flexibilité et de son adaptabilité aux besoins évolutifs du secteur de la santé. Les microservices facilitent l'intégration et permettent ainsi une gestion et une mise à jour simplifiées des composants logiciels. Cette architecture modulaire soutient l'objectif d'Astra de fournir des services sécurisés et conformes aux réglementations strictes du domaine de la santé, tout en assurant une interopérabilité fluide avec les dispositifs mobiles et autres plateformes, essentielle pour les professionnels de la santé en déplacement.

WebRTC est une technologie open source qui permet des communications en temps réel comme la vidéo et l'audio directement dans les navigateurs web, sans plugins additionnels. Elle est sécurisée, interopérable et permet une connectivité peer-to-peer rapide.

Nous avons décidé d'adopter Jitsi comme framework WebRTC pour notre système de vidéoconférence pour Astra. Jitsi est une plateforme open source qui a fait ses preuves en offrant des solutions de communication vidéo de haute qualité qui sont à la fois sécurisées et facilement personnalisables.

Matrix sera utilisé pour la gestion de la messagerie en temps réel et permettra aux utilisateurs du nouveau système d’envoyer des messages et liens utiles.

Ces deux frameworks peuvent être intégrés sans problème dans une architecture de type microservices et répondront à tous les besoins d’Astra pour son nouveau système de vidéoconférence. Ils viendront s’agréger au système actuelle sans apporter de modifications aux services existants.

Exigences

Type	Catégorie	Description
Exigences Techniques	Infrastructure Haute Disponibilité	Serveurs et réseaux robustes pour soutenir les services de visioconférence en continu.
	Optimisation pour la Visioconférence	Serveurs adaptés pour gérer des flux vidéo et audio de haute qualité, y compris des codecs et des algorithmes d'optimisation de bande passante.
	Compatibilité WebRTC	Intégration complète avec les technologies WebRTC pour une communication fluide dans les navigateurs sans nécessiter de plugins.
	Interopérabilité avec Jitsi et Matrix	Assurer une intégration transparente avec Jitsi pour les fonctionnalités de visioconférence et Matrix pour la messagerie en temps réel.
Exigences Opérationnelles	Formation et Support Utilisateur	Programmes de formation complets pour les employés d'Astra, assurant une adoption rapide et efficace du nouveau système.
	Maintenance et Mises à Jour Régulières	Plan de maintenance pour les mises à jour régulières des microservices, garantissant la sécurité et l'efficacité opérationnelle.
	Stratégies de Surveillance et d'Intervention	Mise en place de systèmes de surveillance pour détecter et réagir rapidement aux problèmes techniques ou aux menaces de sécurité.
	Gestion de la Sécurité des Données	Protocoles stricts pour la gestion sécurisée des données, en conformité avec les réglementations du secteur de la santé, telles que le GDPR et le HIPAA.
	Planification de la Continuité d'Activité	Mise en place de procédures pour assurer la continuité des services en cas de panne ou d'interruption majeure.
	Gestion des Changements	Processus clairs pour gérer les modifications et les mises à jour du système, minimisant les perturbations opérationnelles.

Bonnes pratiques implémentées

Bonne Pratique	Description
Authentification	Utilisez des tokens, tels que JWT (JSON Web Tokens), pour sécuriser et vérifier l'identité des utilisateurs à travers les différents services de manière indépendante, tout en maintenant un système cohérent et sécurisé.
Encapsulation des services	Assurez l'encapsulation de chaque service en un système indépendant, l'isolation limite l'impact d'une défaillance sur le système.
Scalabilité	Conception des services pour qu'ils soient facilement scalables, en réponse à la demande changeante.
Découpage métier	Concevez chaque microservice autour d'une fonctionnalité ou d'un domaine métier spécifique pour favoriser la modularité.
Fiabilité et tests	Effectuez des tests réguliers du système pour résoudre les problèmes, les micro services doivent être testables indépendant les uns des autres.
Déploiement continu	Mettre en place l'intégration continue (CI) et le déploiement continu (CD) pour automatiser les tests et les déploiements des services.
Base de données	Chaque microservice doit avoir sa propre base de données pour éviter les dépendances inter-services.
Expérience utilisateur	Assurez une interface utilisateur intuitive et accessible, avec des options d'accessibilité pour les utilisateurs handicapés, et offrez formation et support technique.
Réglementation du secteur	Assurez que la mise en place du nouveau service respecte les standards du secteur de la santé tels que définis par plusieurs réglementations qui diffèrent selon les pays

Maintenabilité

Avec une architecture microservices, le système est divisé en plusieurs services indépendants. Chacun de ces services doit être maintenu, mis à jour et surveillé séparément, ce qui peut augmenter la complexité globale de la gestion du système.

Bien que les services soient indépendants, ils communiquent souvent entre eux. Les mises à jour ou modifications dans un service peuvent affecter d'autres services, nécessitant une coordination minutieuse.

Pour Astra, la maintenabilité d'un système de visioconférence avec une architecture microservices implique de jongler avec la complexité technique, la sécurité des données sensibles, l'intégration avec d'autres systèmes, la garantie de performance et de disponibilité, la gestion des coûts, ainsi que le support et la formation des utilisateurs.

Chacun de ces aspects doit être soigneusement géré pour assurer un système fiable et efficace, conforme aux exigences strictes du secteur de la santé.

Sécurité

L'architecture assure la sécurité des données en transit et au repos à travers le cryptage SSL/TLS, les pare-feu, et les services d'authentification et d'autorisation robustes. Les services doivent être régulièrement mis à jour pour corriger les vulnérabilités de sécurité, ce qui nécessite une attention constante et des procédures de déploiement sûres.

Toutes les communications, y compris les flux vidéo et audio, doivent être chiffrées pour prévenir l'interception ou l'écoute clandestine. La gestion sécurisée des clés de chiffrement est cruciale pour éviter les failles de sécurité.

La mise en place des systèmes d'authentification multi-facteurs peut garantir que seuls les utilisateurs autorisés peuvent accéder aux sessions de visioconférence et aux données sensibles, il faut s’assurer que les utilisateurs n'ont accès qu'aux informations et fonctionnalités nécessaires à leur rôle.

Chaque microservice doit être isolé pour limiter les risques de propagation d'une faille de sécurité à l'ensemble du système, ils doivent être régulièrement mis à jour pour corriger les vulnérabilités de sécurité.

Dans l'ensemble, pour Astra, la sécurité dans un système de visioconférence utilisant une architecture microservices implique une approche multi-facettes. Elle nécessite non seulement de protéger les données des patients, mais aussi d'assurer la sécurité des communications, de gérer efficacement les identités et les accès, de maintenir l'isolation et la sécurité des microservices, de surveiller continuellement les menaces, et de répondre rapidement aux incidents afin de garantir la sécurité de l'infrastructure.

Intégration

Pour intégrer avec succès le nouveau système de visioconférence au sein de l'architecture existante d'Astra, une approche méticuleuse et interopérable est essentielle. L'objectif principal est de garantir une connexion fluide et sécurisée avec les systèmes actuels, notamment le système d'authentification et le serveur de fichiers. Cela implique l'adoption de protocoles standardisés pour l'échange de données et l'authentification, assurant ainsi une gestion cohérente des identités des utilisateurs et un accès sécurisé au système de visioconférence.

En outre, une attention particulière doit être portée à l'intégration du service de gestion des documents avec le serveur de fichiers existant, permettant un partage efficace des ressources tout en respectant les contrôles d'accès basés sur les rôles. Cette intégration doit également tenir compte de la conformité aux normes de confidentialité et de sécurité des données dans le secteur de la santé.

Par ailleurs, l'interopérabilité avec d'autres applications et services utilisés par Astra est cruciale pour améliorer l'expérience utilisateur globale et optimiser les processus opérationnels. L'utilisation d'APIs et de connecteurs facilitera cette intégration, tout en soutenant les flux de travail existants relatifs à la gestion des informations de santé.

Enfin, l'architecture microservices du système de visioconférence devrait offrir la flexibilité nécessaire pour des ajustements futurs et une mise à l'échelle adaptée aux besoins croissants d'Astra, sans perturber les opérations en cours. L'accent sur l'échange de données sécurisé et l'adhésion aux standards de l'industrie de la santé garantira que le système reste non seulement fonctionnel et évolutif, mais aussi conforme aux exigences réglementaires strictes du secteur de la santé.