Astra Recherche

Description d'architecture informatique de haut niveau

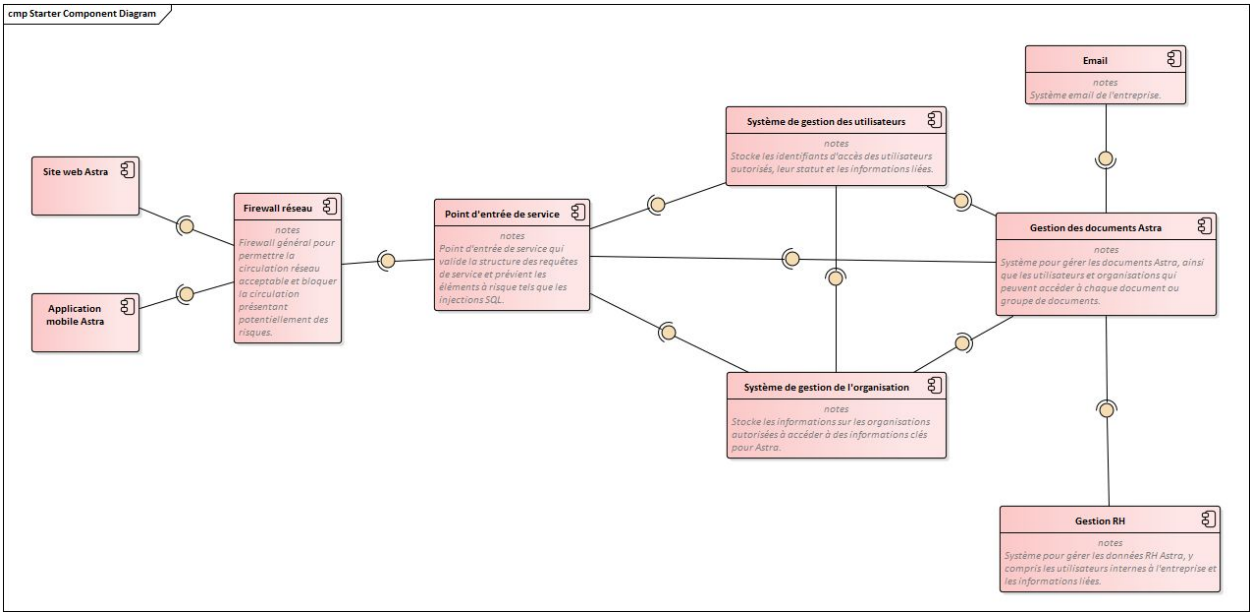
V 2.8

Introduction

Ce document fournit une description haut niveau de l'architecture des opérations IT Astra. Notez qu'il décrit des composants, mais que chaque composant peut être déployé de manière redondante pour garantir un haut niveau de disponibilité.

Description de composant IT

Le diagramme de composant UML ci-dessous montre les composants clés de l'architecture des opérations IT Astra. Les descriptions des composants suivent le diagramme. (Voir la version agrandie.)



Les composants clés sont les suivants :

- **Site web Astra.** Le site web Astra qui affiche des informations publiques sur l'entreprise de même que des informations protégées par login basées sur l'organisation et le rôle de l'utilisateur. Le site web est construit comme une application web réactive permettant l'accès depuis une variété d'appareils et de tailles d'écran.
- **Application mobile Astra.** Une application mobile pour les appareils Android et iOS permettant aux utilisateurs mobile d'accéder aux informations Astra autorisées par leur login et leur rôle d'utilisateur depuis un appareil mobile. L'application mobile permet un stockage limité de documents et d'autres fonctionnalités spécifiques à une application mobile au-delà de ce qui est permis par le site web.
- **Firewall réseau.** Le firewall général du réseau configuré pour protéger les systèmes Astra de la circulation réseau inattendue ou non planifiée. Fournit l'accès port 80 aux systèmes et services

exposés alors que les systèmes internes peuvent utiliser différents ports HTTP pour la protection des données.

- **Point d'entrée de service.** Un dispositif qui vérifie que les utilisateurs accèdent uniquement aux services auxquels ils ont accès.
- **Système de gestion des utilisateurs.** Système pour gérer les utilisateurs ayant la permission d'accéder aux services et à d'autres systèmes internes. Gère le rôle, l'authentification, et les capacités liées des utilisateurs.
- **Système de gestion de l'organisation.** Gère les organisations ayant accès aux données et services Astra. Les utilisateurs doivent appartenir à une organisation autorisée. Certains services permettent à tout utilisateur d'une organisation d'accéder à des données et documents limités.
- **Email.** Service email typique pour recevoir et envoyer des emails, pour les utilisateurs internes à Astra. Gère les emails transactionnels envoyés par une API.
- **Gestion des documents Astra.** Gère les documents Astra avec des protections permettant uniquement aux utilisateurs internes et externes autorisés d'accéder à des documents spécifiques, sur la base du rôle utilisateur ou en tant qu'utilisateur ayant la permission d'accéder à des documents et dossiers spécifiques.
- **Gestion RH.** Système pour gérer les utilisateurs, salariés et prestataires internes à Astra. Inclut le rôle, département et les permissions d'accès de l'utilisateur.

Standards d'architecture informatique

La liste ci-dessous fournit une description de haut niveau des standards internes pour l'architecture informatique.

- Toutes les données doivent être encryptées lors de leur transfert.
- Les utilisateurs finaux ne doivent pas pouvoir stocker des données localement sur leur ordinateur ou appareil, à l'exception des fichiers qui peuvent être mis en cache dans l'application mobile Astra. Toutes les données à partager avec d'autres utilisateurs doivent respecter nos standards de partage de données et notre système de gestion de contenu.
- Tous les composants internes doivent être protégés derrière notre firewall et autres services de données. Les modifications de ces dispositifs peuvent être effectuées pour la solution dès lors qu'elles respectent nos standards de sécurité. Les modifications recommandées devront être identifiées et passées en revue par nos équipes de direction.
- Notre environnement IT est construit sur des serveurs Linux physiques et virtuels. Tous les composants de la solution doivent être conformes à cette combinaison.
- Toutes les interfaces de service doivent être construites selon les standards de l'industrie pour l'authentification utilisateur et les meilleures pratiques de sécurité.
- Tous les utilisateurs accédant à une réunion collaborative doivent avoir un compte utilisateur dans notre système et être validés lorsqu'ils accèdent à la réunion web.
- À l'exception des informations disponibles publiquement, tout accès à un service ou document doit être validé par les systèmes utilisateur et organisation.

- Le système d’email permettra aux systèmes authentifiés d’envoyer automatiquement des emails transactionnels par le biais d’une API. Les utilisateurs authentifiés peuvent envoyer des emails.
- Tous les accès aux services et aux composants doivent correspondre au rôle et à l’authentification de l’utilisateur.
- Tout accès à un composant doit se faire à travers le firewall.
- Tout accès à un service doit passer par le point d’entrée de service.