PROJET DE PLATEFORME COLLABORATIVE ET DE VISIOCONFÉRENCE

ETUDE EXPLORATOIRE

SITUATION INITIALE

Description générale de l'architecture

L'architecture actuelle (1*) est organisée autour du point d'entrée de service, lui-même placé après le firewall et est donc sécurisée.

Cette architecture contient 5 services (dont 3 dédiés à la gestion des accès). Tous sont accessibles en passant par le service de gestion des documents après avoir passé le firewall puis le point d'entrée de service (voir *2).

Tous les services sont atteignables par les applications web et mobiles en passant par le firewall.

L'architecture actuelle respecte les exigences et standards suivants :

- Sécurité
  - Toutes les nouvelles fonctionnalités sont placées derrière le firewall
  - Toutes les anciennes fonctionnalités sont placées derrière le firewall
  - Le firewall gère le chiffrement des données en utilisant le protocole SSL (postulat)
- Authentification
  - Toutes les nouvelles fonctionnalités sont soumises à authentification et les utilisateurs doivent être autorisés à les utiliser
  - Toutes les anciennes fonctionnalités sont soumises à authentification et les utilisateurs doivent être autorisés à les utiliser
- L'intégration web et mobile est assurée par un portail web réactif permettant de s'adapter à tous types de supports et de tailles d'écran et une application mobile déjà adaptée aux appareils Android et iOS.

(*1) Voir annexe Diagramme de l'architecture métier initiale
(*2) Voir annexe Diagramme de l'architecture technique initiale

Présentation des fonctionnalités

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.

Relations entre les services

Tous les services sont accessibles par le point d'entrée de service et la gestion des documents consomme tous les autres services.

Avantages et inconvénients

Avantages

Elle est connue et maîtrisée des utilisateurs et administrateurs. Elle a un haut niveau de disponibilité de fait de la redondance possible de chaque service.

Les standards internes d'architecture décrits dans le document "Description d'architecture informatique de haut niveau" sont réputés couverts par cette architecture.

Inconvénients

Elle contient un illogisme fonctionnel où tous les composants sont dépendants du service de gestion des documents. En cas d'indisponibilité de ce service (malgré la redondance possible), l'ensemble du SI devient indisponible.

Elle duplique les services de sécurité, augmentant ainsi la complexité et le coût de maintenance (chaque évolution/correction devant répliquée sur chaque composants gérant les accès utilisateurs).

PREMIÈRE SOLUTION

Description générale de l'architecture

La nouvelle architecture (1*) s'appuie sur l'architecture actuelle. Elle est toujours organisée autour du point d'entrée de service, lui-même placé après le firewall et est donc sécurisée.

Cette architecture contient 7 services (dont 3 dédiés à la gestion des accès). Tous, à l'exception du service de streaming, sont accessibles en passant par le service de gestion des documents.(après avoir passé le point d'entrée de service). Le service de streaming est, quand à lui, accessible directement depuis le firewall (voir *2). Tous les services sont atteignables par les applications web et mobiles en passant par le firewall.

L'architecture cible respecte les exigences et standards suivants :

- Sécurité
  - Toutes les nouvelles fonctionnalités sont placées derrière le firewall
  - Toutes les anciennes fonctionnalités sont placées derrière le firewall
  - Le firewall gère le chiffrement des données en utilisant le protocole SSL
- Authentification
  - Toutes les nouvelles fonctionnalités sont soumises à authentification et les utilisateurs doivent être autorisés à les utiliser
  - Toutes les anciennes fonctionnalités sont soumises à authentification et les utilisateurs doivent être autorisés à les utiliser
- L'intégration web et mobile est assurée par un portail web réactif (appliquant le RWD - responsive web design) permettant de s'adapter à tous types de supports et de tailles d'écran et une application mobile déjà adaptée aux appareils Android et iOS.
- La compatibilité multiplateforme des nouveaux services sera couverte par l'utilisation de solutions open source gérant déjà cette problématique. Les anciens services sont supposés déjà compatibles.

Les données sont protégées de plusieurs façons :

- Le transit ne se fait avec des données cryptées par le firewall
- Les accès et autorisations utilisateurs sont sécurisés par une fonction spécifique ne donnant accès qu'aux données prévues en fonction de droits utilisateurs
- Les données ne sont pas stockées dans le cloud mais dans stockage local dont Astra maîtrise la protection

(*1) Voir annexe Diagramme de l'architecture métier cible (solution 1)
(*2) Voir annexe Diagramme de l'architecture technique cible (solution 1)

Présentation des nouvelles fonctionnalités

Plateforme collaborative

Ce nouveau service permettra d'animer des réunions web interactives, sur invitation, avec streaming audio/vidéo, enregistrement du flux de streaming, partage d'écran et chat.

Cette plateforme permettra d'organiser des présentations web avec streaming audio/vidéo, sur invitation, avec chat. Le nombre d'invitations ira de 10 à plus de 500 utilisateurs.

Plateforme de streaming

Ce nouveau service permettra la visualisation de vidéo live ou enregistrées et ne permettra pas le téléchargement local à l'exception du cache nécessaire à la bonne exécution du service..

L'accès aux différentes ressources vidéos se fera selon les droits de chaque utilisateur y compris pour les utilisateurs ayant un accès public.

Modifications apportées aux services existants

Gestion des documents

La gestion des documents reste le service central permettant d'accéder à tous les autres services.

La gestion des documents est étendue pour tenir compte des nouveaux types de documents (vidéos provenant de la plateforme de streaming) pouvant être référencés et recherchés.

Applications front

Les 2 applications front (web et mobile) sont modifiées pour prendre en compte les accès à aux plateformes collaborative et de streaming.

La version mobile pourra être limitée en termes de fonctionnalités en fonction de l'outil open-source choisi.

Relations entre les services

Tous les services sont accessibles depuis les outils front par le point d'entrée de service à l'exception de la plateforme de streaming accessible à la fois directement depuis le firewall et par le point d'entrée de service.

La gestion des documents consomme la plateforme collaborative et la plateforme de streaming.

La plateforme collaborative consomme la plateforme de streaming afin de stocker et référencer les vidéos.

La plateforme collaborative et la plateforme de streaming consomment le service d'email afin d'envoyer des messages aux utilisateurs pour les inviter à visualiser une ressource vidéo.

Avantages et inconvénients de la solution

Avantages

L'architecture initiale est globalement préservée dans l'architecture cible (en conservant la gestion des documents comme point central d'articulation des services) et les utilisateurs ne seront pas déstabilisés par une nouvelle IHM.

Les coûts de développement sont contenus par l'ajout de seulement deux services permettant de couvrir l'essentiel des besoins fonctionnels exprimés.

Inconvénients

L'architecture cible conserve l'illogisme constaté dans l'architecture initiale.

La plateforme collaborative n'est pas complète car elle n'intègre pas les services optionnels permettant une collaboration plus étendue (discussion instantanée, planification de réunion).

DEUXIÈME SOLUTION

Description générale de l'architecture

La nouvelle architecture (1*) est une architecture microservices. Elle est organisée autour d'une passerelle d'API (en remplacement du point d'entrée de service). Cette passerelle d'API est placée après le firewall et est donc sécurisée.

Tous les services sont accessibles directement en passant par la passerelle d'API (*2). Il n'y a pas de dépendances entre services. Un service peut en consommer un autre en passant par la passerelle d'API sans avoir besoin de l'atteindre directement, faisant ainsi en sorte d'avoir un couplage faible entre services.

La sécurité de l'architecture est assurée par :

- Le firewall du système d'information :
  - qui filtre les requêtes pour éviter le trafic non autorisé
  - qui effectue le chiffrement des données en utilisant le protocole SSL
- Le nouveau système d'identification unique exploitant un service d'authentification et d'autorisation de type SSO

L'intégration web et mobile est assurée par un portail web réactif (appliquant le RWD - responsive web design) permettant de s'adapter à tous types de supports et de tailles d'écran et une application mobile déjà adaptée aux appareils Android et iOS.

La compatibilité multiplateforme des nouveaux services sera couverte par l'utilisation de solutions open source gérant déjà cette problématique. Les anciens services sont supposés déjà compatibles.

Les données sont protégées de plusieurs façons :

- Le transit ne se fait qu'avec des données cryptées par le firewall
- Les accès et autorisations utilisateurs sont sécurisés par une fonction spécifique ne donnant accès qu'aux données prévues en fonction de droits utilisateurs
- Les données ne sont pas stockées dans le cloud mais dans stockage local dont Astra maîtrise la protection

(*1) Voir annexe Diagramme de l'architecture métier cible (solution 2)
(*2) Voir annexe Diagramme de l'architecture technique cible (solution 2)

Présentation des nouvelles fonctionnalités

Passerelle d'API

Le point d'entrée de service est remplacé par une passerelle d'API. Une passerelle d'API est un outil de gestion des interfaces de programmation d'application (API) qui se positionne entre un client et une collection de services back-end.

Elle agit comme un proxy inversé qui accepte tous les appels des API, rassemble les différents services requis pour y répondre et renvoie le résultat souhaité.

L'objectif principal d'une passerelle API est de simplifier et de stabiliser les interfaces exposées aux clients (mobiles, navigateurs...). De plus, en raison de la position unique d'une passerelle API dans l'architecture, divers avantages complémentaires sont activés, tels que la surveillance, la journalisation, la sécurité, l'équilibrage de charge et la manipulation du trafic.

Service unique de gestion des accès et des identités (IAM)

Ce nouveau service d'IAM (Identity and Access Management) unique sera mis en place en remplacement des 3 systèmes actuellement utilisés, afin de :

- gérer les profils individuels et les groupes d'utilisateurs
- gérer les profils internes et externes
- gérer les droits d'accès aux différents services et ressources fournis par Astra

Il contiendra un profil invité permettant d'accéder aux ressources publiques uniquement depuis l'application mobile et le site internet d'Astra.

.

Il contiendra les anciennes données de l'architecture actuelle soient :

- pour les utilisateurs internes :
    - le rôle
    - le département
    - le statut de l'utilisateur (salarié/prestataire/stagiaire)
- pour les utilisateurs externes :
    - le rôle
    - le groupe auquel l'utilisateur appartient (pré-requis)

Afin de sécuriser les accès et les données, l'exploitation, pour les profils externes comme internes, d'une double authentification sera faite.

Plateforme collaborative

Ce nouveau service permettra d'animer des réunions web interactives, sur invitation, avec streaming audio/vidéo, enregistrement du flux de streaming, partage d'écran et chat.

Cette plateforme permettra d'organiser des présentations web avec streaming audio/vidéo, sur invitation, avec chat. Le nombre d'invitations ira de 10 à plus de 500 utilisateurs.

Plateforme de streaming

Ce nouveau service permettra la visualisation de vidéo live ou enregistrées et ne permettra pas le téléchargement local à l'exception du cache nécessaire à la bonne exécution du service..

L'accès aux différentes ressources vidéos se fera selon les droits de chaque utilisateur y compris pour les utilisateurs ayant un accès public.

Outil de chat

Ce nouvel outil permettra les discussions instantanées entre membres d'une réunion/présentation ou entre l'animateur d'une réunion/présentation et les membres d'une réunion.

Outil de planification

Ce nouvel outil servira à organiser et planifier les réunions et présentations en envoyant des mails d'invitation aux utilisateurs privés concernés.

Modifications apportées aux services existants

Gestion des documents

La gestion des documents n'est plus le service central permettant d'accéder à tous les autres services.

Ceci permet de sécuriser les données contenues dans la gestion des documents car les services ouverts sur l'extérieur (plateforme collaborative et plateforme de streaming) ne passent plus par ce point.

Cela permet également de supprimer un illogisme fonctionnel qui fait que désormais la plateforme collaborative et la plateforme de streaming ne dépendent plus de la gestion des documents ainsi les services sont tous indépendants (avec un couplage le plus faible possible).

Point d'entrée de service

Comme expliqué dans le chapitre précédent, le point d'entrée de service est remplacé par une passerelle d'API qui gérera les accès aux différents services en fonction des droits d'accès des utilisateurs en se basant sur le service d'identification et gérera l'accès aux différents services entre eux.

Relations entre les services

Tous les services sont accessibles par la passerelle d'API.
Les droits d'accès utilisateurs définissent les accès aux services.

Contrôles faits sur les outils front existants

Les deux portails front (site web et application mobile) sont conservés, a priori en l'état, car ils sont déjà dits réactifs. Ils permettent donc de s'adapter à tous types de supports ou de tailles d'écran.

Les applications utilisant un client dit léger (un navigateur web), elles ne sont que peu impactées par les OS et seront donc uniquement tributaire du choix du navigateur en termes de compatibilité.

Cependant, afin de s'assurer que le site web répond bien à ce besoin de compatibilité, des tests de compatibilité-navigateur (cross-browser testing en anglais) seront effectués et les éléments frontend non compatibles feront l'objet d'une "normalisation" (la normalisation consiste à ré-ajuster les styles par défaut des navigateurs afin d'éviter les différences de styles et de positionnement).

Avantages et inconvénients de la solution

Avantages

L'architecture cible est une architecture microservices qui a pour principal avantage de respecter les principes SOLID :

- Responsabilité unique (Single responsibility principle) : chaque service du SI n'a qu'une seule responsabilité
- Ouvert/fermé (Open/closed principle) : chaque service est fermé à la modification directe mais ouverte à l'extension
- Substitution de Liskov (Liskov substitution principle) : en étant stockés dans les conteneurs dans le cloud, chaque service peut être instancié autant de fois que nécessaire en fonction de la charge de travail
- Ségrégation des interfaces (Interface segregation principle) : chaque client (web et mobile) a une interface spécifique
- Inversion des dépendances (Dependency inversion principle) : en supprimant le point central l'organisation de l'architecture initiale (tous les services n'étaient accessibles qu'à travers la gestion des documents) et en utilisant une passerelle d'API, aucun service ne dépend d'un autre

Elle répond également aux exigences techniques et fonctionnelles requises par la direction d'Astra :

- elle est sécurisée grâce à un système d'authentification, à l'utilisation d'un firewall ainsi qu'à un chiffrement des données
- elle contient un plateforme collaborative permettant d'organiser des réunions avec un nombre variable d'utilisateur et en exploitant, en fonction de chaque réunion, des outils de communication instantanée.
- elle contient une plateforme de streaming permettant de visualiser des ressources vidéos (en direct ou à la demande) et incluant une fonction de recherche
- elle permet de planifier et d'inviter facilement des utilisateurs à des réunions ou à visualiser des ressources vidéos grâce à un outil de planification et à un service mail
- elle s'adapte à tous types de matériels, de navigateurs ou encore de systèmes d'exploitation

Inconvénients

La notion “micro” dans le terme microservice est relative et chaque microservice pourrait avoir une taille différente (plus ou moins grande) mais adaptée à son contexte fonctionnel.

La maintenance et la mise à jour des bases de données peut être plus complexe car chaque microservice aura sa propre base de données mais ceci pourra être solutionné en utilisant des bases de données partagées entre plusieurs microservices (en limitant le nombre de services exploitant une base de données partagée pour faciliter l'évolutivité des ces bases de données).

La charge des tests est plus lourde car chaque microservice devra être testé à la fois individuellement et dans un contexte “global” (de bout en bout) avec tous les autres microservices.

L’application globale (utilisation de l’ensemble des microservices dans un contexte utilisateur) pourrait apparaître moins performante (phénomène de latence dans les temps de réponse) car dépendante du réseau. Ceci peut être optimisé en utilisant un protocole de communication asynchrone exploitant un broker de messages .

CONCLUSION

La meilleure solution à mettre en place est la deuxième solution car en plus de couvrir les 5 principes SOLID, elle répond autant aux exigences techniques que fonctionnelles requises par la direction d'Astra

De plus, l'architecture microservices proposée dans cette solution a pour avantage :

- de faciliter le déploiement et de permettre une mise sur le marché rapide grâce à sa modularité et la légèreté de chaque service
- d'avoir une haute évolutivité et d'être scalable en utilisant des conteneurs cloud facilement adaptables lors d'augmentation de charge de travail
- d'être résiliente en séparant les responsabilité et en faisant en sorte que tous les microservices sont indépendants les uns des autres
- d'être ouverte techniquement en pouvant choisir la technologie la plus adaptée pour chaque microservice

Il conviendra cependant d'être organisé afin de pouvoir tester les microservices dans leur intégralité dans les temps prévus pour ce projet.

Il faudra également tenir compte de la latence possible dans les délais de réponses en prévoyant un protocole de communication adapté utilisant un broker de messages.

ANNEXES

Diagramme de l'architecture métier initiale

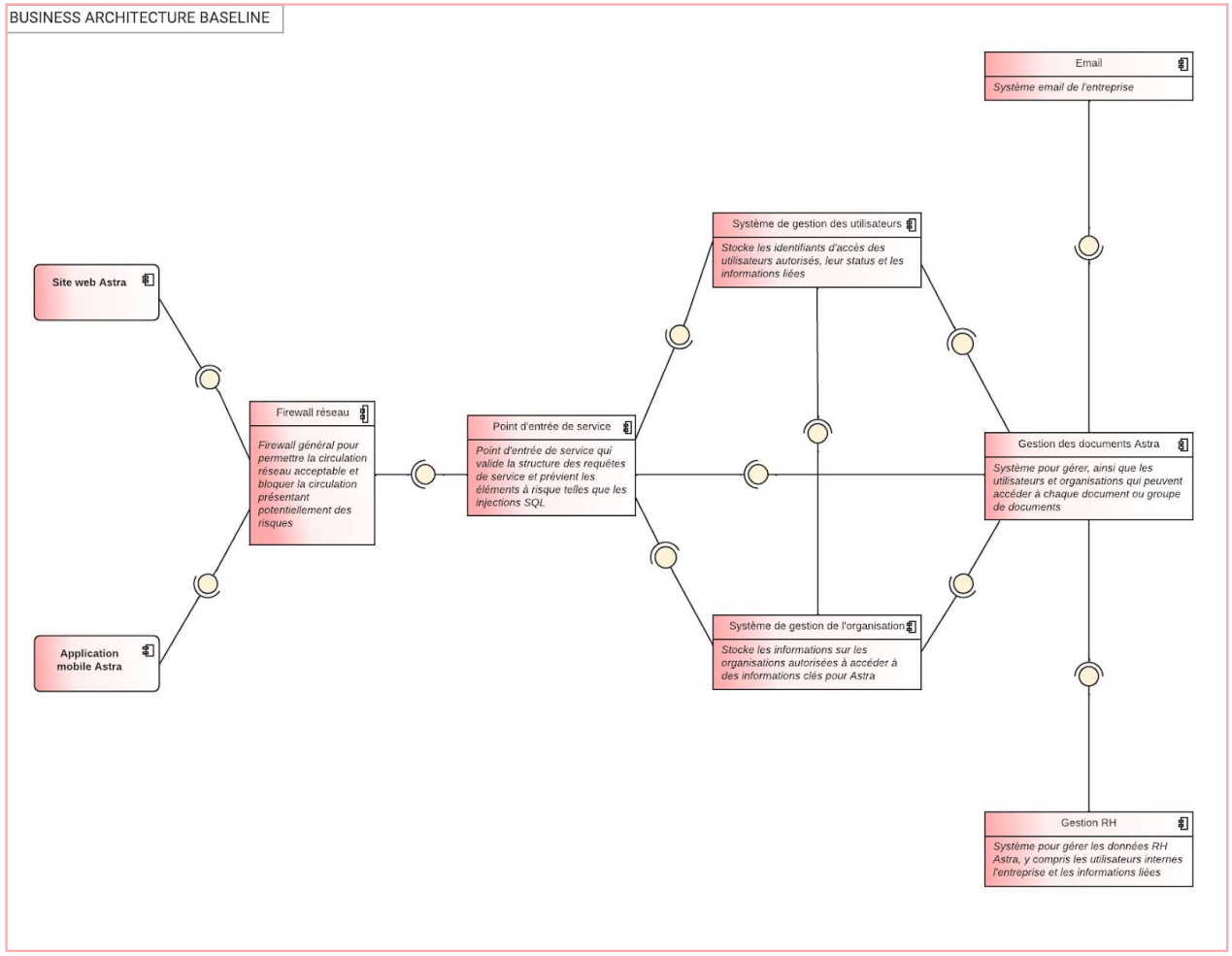


Diagramme de l'architecture technique initiale

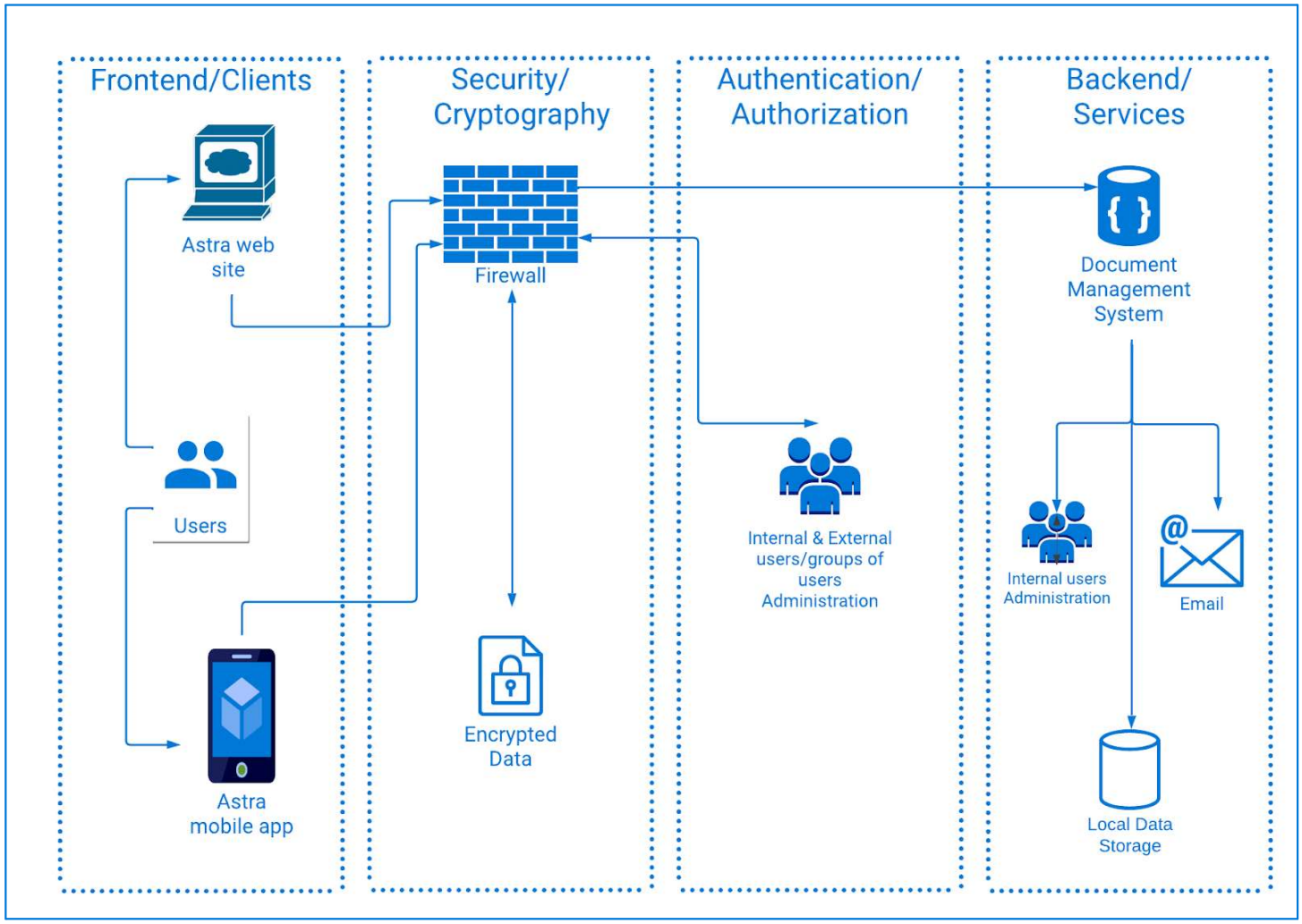


Diagramme de l'architecture métier cible (solution 1)

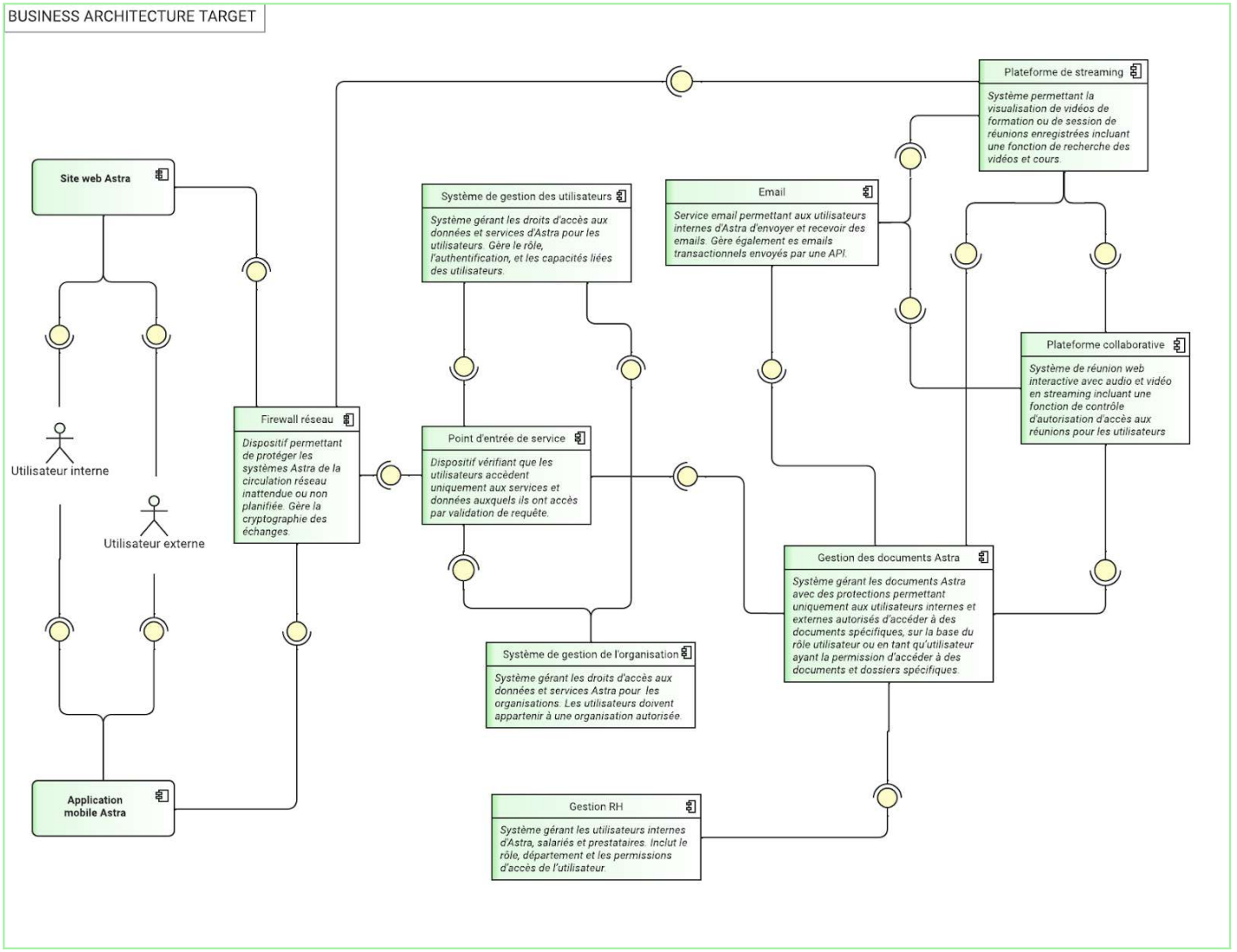
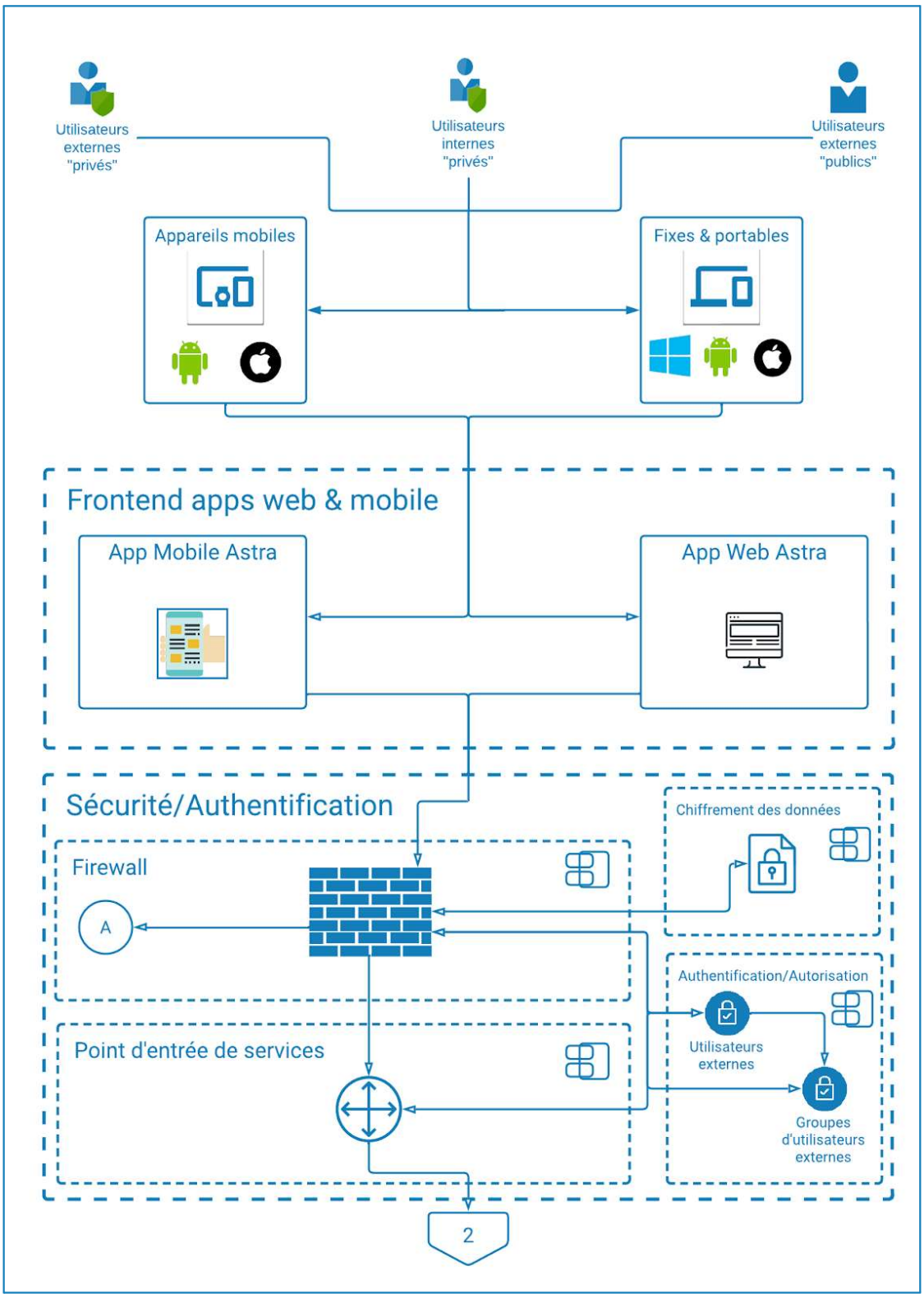


Diagramme de l'architecture technique cible (solution 1)



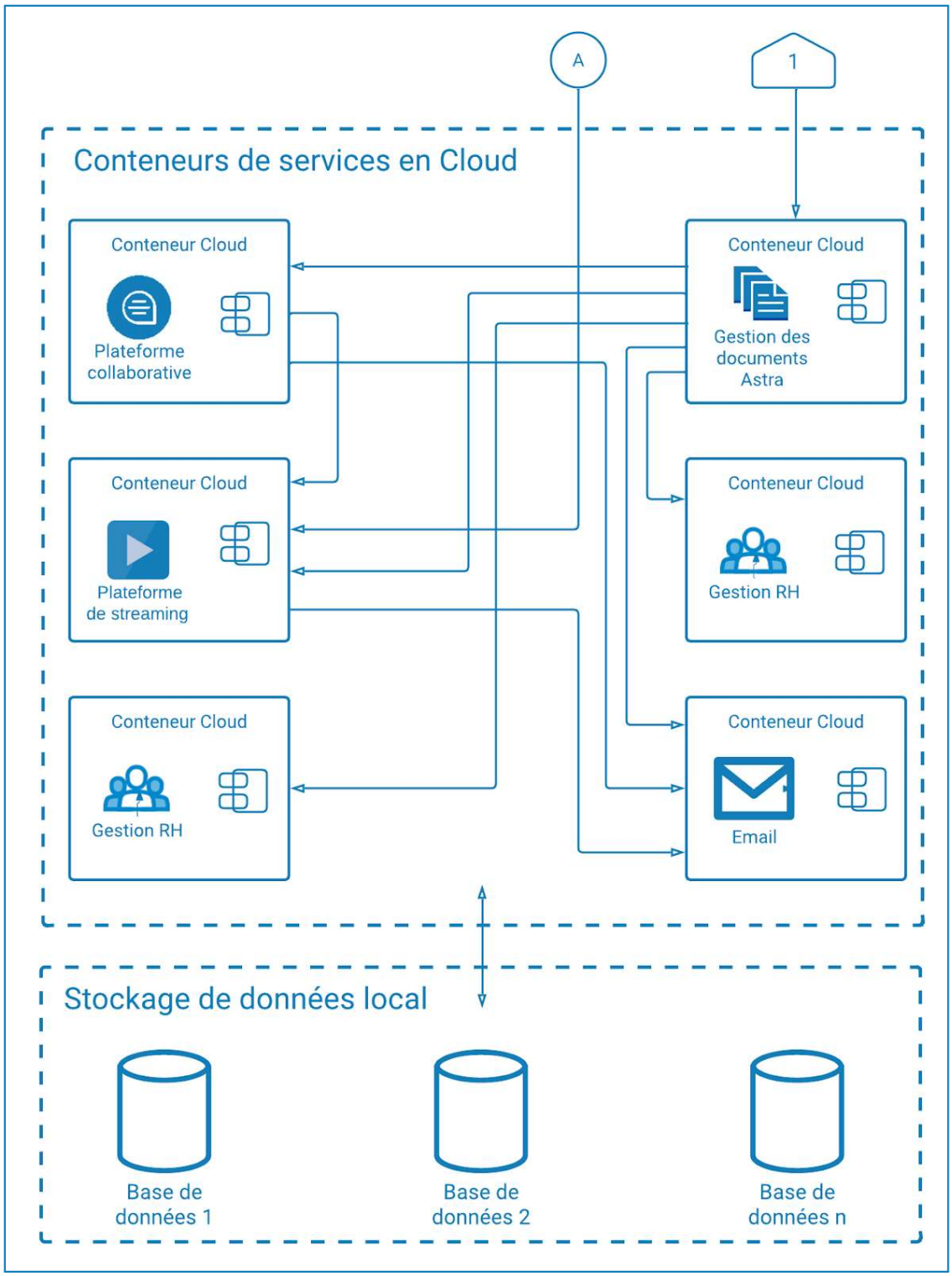

A
1
Conteneurs de services en Cloud
Conteneur Cloud
Plateforme collaborative
Conteneur Cloud
Gestion des documents Astra
Conteneur Cloud
Plateforme de streaming
Conteneur Cloud
Gestion RH
Conteneur Cloud
Gestion RH
Conteneur Cloud
Email
Stockage de données local
Base de données 1
Base de données 2
Base de données n

Diagramme de l'architecture métier cible (solution 2)

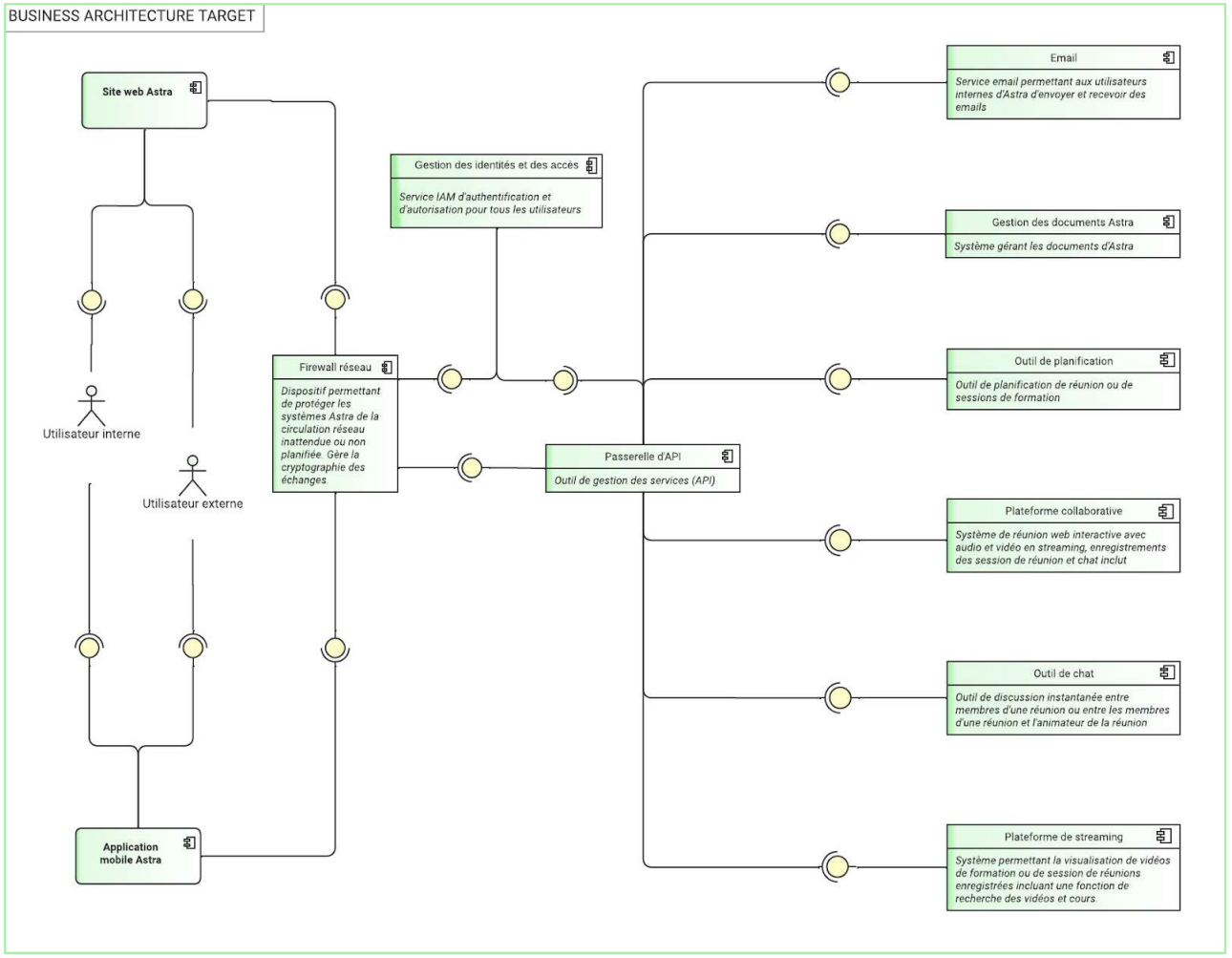
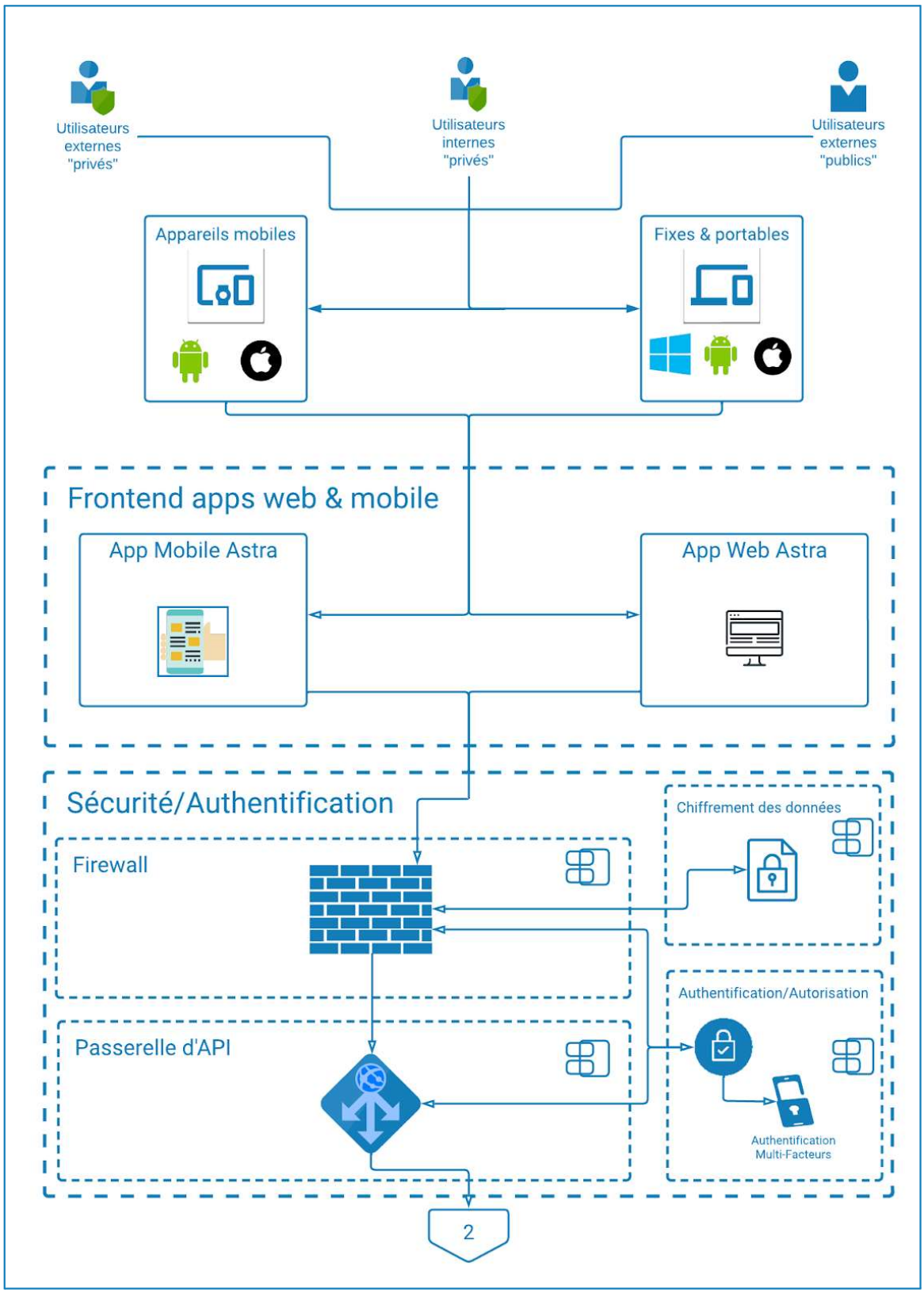
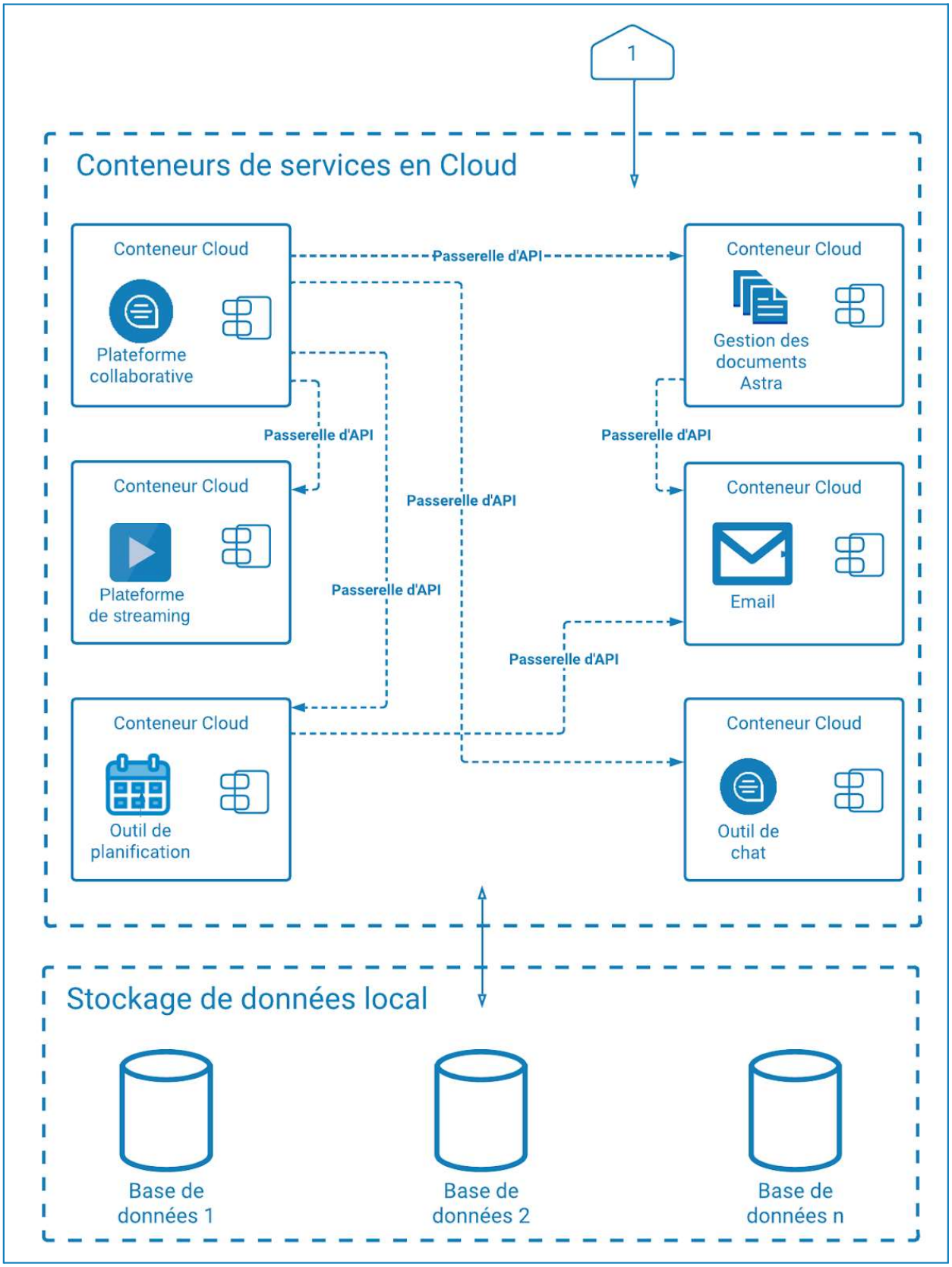


Diagramme de l'architecture technique cible (solution 2)




1
Conteneurs de services en Cloud
Conteneur Cloud
Plateforme collaborative
Passerelle d'API
Conteneur Cloud
Gestion des documents Astra
Passerelle d'API
Passerelle d'API
Conteneur Cloud
Plateforme de streaming
Passerelle d'API
Passerelle d'API
Conteneur Cloud
Email
Passerelle d'API
Conteneur Cloud
Outil de planification
Conteneur Cloud
Outil de chat
Stockage de données local
Base de données 1
Base de données 2
Base de données n