



Plan d'implémentation

Rep' Aero

L'enjeux principal de ce document est de décrire avec précision la migration de l'architecture existante vers l'architecture cible.

Table des matières

1. Objectif	3
2. Parties prenantes	4
3. Migration	5
3.1 Stratégie	5
3.2 Impacts	5
3.3 Récupération des données	6
3.4 Coûts de la migration	6
3.4.1 Tableau des coûts	6
3.4.2 Tableau des coûts	6
4. Backlogs	7
4.1 Backlog n°1	7
4.2 Backlog n°2	8
4.3 Backlog n°3	9
4.4 Backlog n°4	10
5. Modalités	11
5.1 Disponibilité	11
5.2 Intégrité	11
5.3 Sécurité	11
5.4 Récupération des données	11

1

Objectif

L'objectif de cette migration vers l'architecture cible qui est déjà développée, est de s'assurer que le nouveau système fournisse parfaitement les services qui sont attendus. Avec les conditions de performances exigées et que les données de l'ancien système soient correctement reprises pour y être intégrée. Une attention particulière sera apportée sur ce point.

Les collaborateurs devront être capable de maintenir leurs activités dans les conditions d'exploitation habituelles, sans coupure de service ni de dégradation de la qualité du service rendu.

2

Partie prenante

Rappel des parties prenantes du projet de migration :

Partie prenante	Rôle	Responsabilité
Steve Lambort	CEO	Responsabilité juridique et financière. Suivi du processus de migration
Alain Duplanc	Responsabilité informatique	Maintien du système actuel en condition opérationnel. Expertise sur le système actuel
Marie Blanc	Architecte logiciel	Définition du plan de migration, identification des travaux et réalisation de la roadmap.
Chef d'équipe	Chef de l'équipe de maintenance	Organisation des équipes pour se former aux nouveaux outils. Gestion ressources et prod. Se former aux nouveaux outils.
Techniciens	Techniciens de maintenance en aéronautique	Maintien de l'activé, adaptation aux nouveaux outils, expertise métier
Cabinet IT	Spécialisé en développement et intégration de progiciel	Respect du contrat signé avec l'entreprise. Mise en place de l'architecture

3

Migration

3.1 Stratégie

La stratégie de migration est simple et classique, vise donc à fournir un résultat optimal, conforme aux attentes et aux exigences de qualité, de sécurité, fonctionnelles et réglementaires.

On peut le résumer de manières suivantes :

- Déploiement de la nouvelle plateforme
- Configuration de celle-ci
- Déploiement de nouveaux applicatifs de la plateforme technique
- Préparation des données avec la migration
- Test
- Audit de sécurité
- Formation
- Migration réelle des données sur la nouvelle plateforme

Nous mettons en place tous de suite le service de gestion des ressources et l'application réservations afin de libérer du temps aux techniciens pour se former, il sera donc plus simple de réserver du temps pour que les techniciens puissent se former.

La migration intégrera un plan de sauvegarde, pouvant être activé au cours du processus de migration réelle et visant à rétablir les anciens services.

3.2 Impacts

Les impacts de la migration sont principalement d'ordre fonctionnels. La nouvelle plateforme fournit un ensemble de services, d'outils et de méthodologies de travail qui diffèrent de l'ancienne.

L'adaptation des différents utilisateurs (client, fournisseurs et collaborateurs) à ces nouveaux outils et procédure est à prendre en compte dans la migration.

Aucune perte de données n'est prévue au cours de cette migration.

3.3 Récupération des données

Cette étape sera réalisée uniquement après la validation complète du bon fonctionnement de la plateforme.

Un contrat de maintenance spécifique, signé avec le Cabinet IT chargée du développement de la nouvelle solution permettra d'assurer la suivi et la maintenance à long terme.

3.4 Coûts de la migration

3.4.1 Tableau des coûts :

Voici un tableau qui récapitulatif les coûts de la migration en fonction des tâches :

Collaborateurs	Coût horaire	Temps en heure	Coût total en euros
CEO	110€/h	49	5390€
Responsable informatique	60€/h	112	6790€
Architecte logiciel	40€/h	140	5600€
Chef d'équipe	22€/h	70	1540€
Techniciens	14€/h	19	266€
Cabinet IT	N/A	N/A	N/A

Total : 19 586€

Avec un audit de sécurité de 10 000 euros.

3.4.2 Conclusion

Pour conclure, l'étude coûts nous montre que nous nous en sortons avec un total de 19 586 euros pour la planification et la migration de notre SI. Cela est largement dans notre budget et nous pouvons envisager un audit de sécurité externe. HTTPCS est le leader de la sécurité en Europe et un audit d'une semaine coûte 10 000 euros. Donc on peut dire que l'on s'en sort avec un budget de 29 586 euros

4

Backlogs

4.1 Backlog n°1 : Automatiser les rendez-vous et rationaliser l'emploi du temps des techniciens.

Objectifs	Description	Responsable	Note
Installation serveur	Mise en place du serveur d'application et de base de données	Cabinet IT	Centraliser les serveurs d'applications et les base de données.
Test de sécurité	Test de la configuration et de la sécurité du serveur	Cabinet IT	Sécuriser les applications et les données
Installation serveur d'application ressources	Mise en place du serveur d'application ressources et de sa base	Cabinet IT	Faire fonctionner l'IHM de l'application ressources
Installation de l'IHM ressources	Installation de l'IHM ressources sur le pc du chef d'équipe	Cabinet IT et chef d'équipe	Utilisation de l'application ressources. Permet au chef d'équipe de gérer l'emploi du temps des techniciens
Installation de l'application réservation	Installation de l'application réservation et mise en place du nom de domaine. Fonctionnalité alertes/notification non présent	Cabinet IT, CEO	Permet la prise de RDV automatisé déléstant le CEO de cette charge.
Test de l'application de réservations et ressources	Vérification de toutes les fonctionnalités de l'application de réservation et de ressources	Cabinet IT, architecte logiciel	S'assure du bon fonctionnement de la prise de RDV et de la gestion ressources
Formation de l'application réservation	Permet de prendre en main l'application réservation	Cabinet IT, CEO	Expertise dans l'utilisation de l'app réservation. Permet de former à son tour les clients
Formation de application ressources	Prise en main de l'application ressources	Cabinet IT, Chef d'équipe	Expertise dans l'utilisation des ressources entreprises.

4.2 Backlog n°2 : Gestion et vérification des stocks.

Objectifs	Description	Responsable	Note
Installation application gestion des stocks	Installation de l'IHM stock sur le pc du bras droit et création de la base de données BDD stock sur le serveur	Cabinet IT, responsable informatique	Gestion des stocks plus simple avec l'application. Etat de l'inventaire et Suivi temps réel.
Test application stock	Test du tableau de bord et des alertes	Cabinet IT, Architecte logiciel	S'assure du bon fonctionnement des alertes et du tableau de bord
Installation lecteur code-barres	Mise en place du lecteur de code-barres	Cabinet IT, responsable informatique	Entrée/sortie des pièces détachées par lecteur de code-barres.
Test lecteur et api	Test des entrée/sortie de stock et de l'api vers domaine de production	Cabinet IT, Architecte logiciel	S'assure du bon fonctionnement des lecteurs et de la communication de l'application avec domaine production
Test sécurité	Test de la configuration et de la sécurité du serveur	Cabinet IT	Sécurisé les applications et les données
Formation sur l'application stocks	Permet de prendre en main l'app stock	Cabinet IT, responsable informatique	Expertise dans l'utilisation de l'app Stock
Formation lecteur code barres	Permet de prendre en main les lecteurs de code-barres	Cabinet IT, Chef d'équipe, technicien, responsable informatique	Expertise dans l'utilisation des lecteurs de code-barres
Audit des stocks	Peuplement de la BDD grâce aux lecteurs de code-barres, comparaison avec le fichier Excel.	Chef d'équipe, technicien	Informations de la BDD stocks correspond exactement aux stock réels

4.3 Backlog n°3 : Gestion de l'entreprise.

Objectifs	Description	Responsable	Note
BDD client et fournisseurs	Migration de la BDD fournisseur bon de commande et suivi de paiements sur le serveur. Création et peuplement de la BDD Clients	Cabinet IT	Moins de faille de sécurité
Installation app fournisseur et clients	Installation de l'IHM clients sur le pc du CEO et fournisseurs sur le pc du CEO	Cabinet IT, CEO, responsable d'informatique	Gestion catalogues fournisseurs Suivi temps réel des livraisons Gestion et suivi des paiements Gestion coordonnées fournisseurs Tableau de bord fournisseurs Gestion et suivi des clients Tableau de bord client
Test sécurité	Test de la configuration et de la sécurité de l'application	Cabinet IT	Sécuriser les applications et les données
Sauvegarde	Mise en place de la politique de sauvegarde des données	Cabinet IT, Architecte logiciel	Respect RGPD.
Formation fournisseur	Permet de prendre en main l'application fournisseur	Cabinet IT, CEO, responsable d'informatique	Expertise dans l'utilisation de l'app fournisseurs.
Formation l'app clients	Permet de prendre en main l'app production	Cabinet IT, CEO	Expertise dans l'utilisation de l'app clients.
Migration facturation	Mise en place de la facturation. Migration donnée facturation dans le cloud	Cabinet IT, Architecte logiciel	Gestion de la facturation Suivi des paiements
Test facturation	Test de La communication entre facturation et production.	Cabinet IT	S'assure du bon fonctionnement de la facturation
Formation facturation	Permet de prendre en main l'app facturation	Cabinet IT, CEO	Expertise dans l'utilisation de l'app facturation.
Audit sécurité	Audit complet de sécurité	Cabinet IT	L'application est sécurisée

4.4 Backlog n°4 : Production de l'entreprise.

Objectifs	Description	Responsable	Note
Installation application backend production	Installation du serveur d'application production. Création de la BDD workflow, outil, doc technique	Cabinet IT, Architecte logiciel	Faire fonctionner l'IHM de l'application production
Installation IHM production	Installation de l'IHM sur le pc du chef d'équipe	Cabinet IT, Chef d'équipe	Gestion et suivi des ordres de maintenance Gestion de la documentation Constructeur Gestion outillage
Test application production	Test Fonctionnalité api réservation, doc constructeur, Api facturation, api stock et IHM	Cabinet IT, Architecte logiciel	S'assure du bon fonctionnement de l'IHM et de la communication de l'application avec stocks, app. Réservation et facturation
Mise en place des tablettes	Test des entrée/sortie de stock et de l'api vers domaine de production	Cabinet IT, Architecte logiciel	Tablettes avec bon de commande
Test tablettes	Test de l'ensemble des fonctionnalités de la production	Cabinet IT, Architecte logiciel	S'assure du bon fonctionnement de la production
Formation IHM production	Permet de prendre en main l'app production	Cabinet IT, responsable informatique	Expertise dans l'utilisation de l'app production.
Formation Tablette	Permet de prendre en main les lecteurs de code-barres	Cabinet IT, Chef d'équipe, technicien	Expertise dans l'utilisation des tablettes
Remplissage de la BDD	Migration des données grâce à un ETL de la BDD Microsoft Access suivi Prod et outillage vers workflow et outil. Peuplement grâce à ETL de la BDD doc technique	Cabinet IT, Architecte logiciel	Pleine capacité opérationnelle de l'application production.
Test sécurité	Test de la configuration et de la sécurité de l'application	Cabinet IT	Sécuriser les applications et les données

5

Modalités

5.1 Disponibilité

Le serveur de base de données est accessible depuis le réseau de l'entreprise donc on peut garantir la disponibilité des données. Les données de facturation, eux, sont garantie par le contrat signée avec le provider cloud.

5.2 Intégrité

Zone 1

La BDD ressources à son intégrité des données assuré par le fait qu'il sera rempli par l'application réservation (N'ayant aucune donnée au départ). Elle coexistera avec la BDD suivi prod jusqu'à la zone 3.

Zone 2

L'intégrité des données est assurée par un audit des stocks et ses KPI associés.

Zone 3

L'intégrité des données est assurée par le suivi des incidents de migration et le contrôles d'exactitude des données.

Zone 4

L'intégrité des données est assurée par le suivi des incidents de migration et le contrôles d'exactitude des données. Une vérification manuelle peut être envisager.

5.3 Sécurité

La sécurité des données est garantie par des tests de sécurité constant lors du déploiement et par un audit de sécurité à la fin de la migration.

5.4 Récupération des données

Le contrat de maintenance préalablement signé avec le cabinet extérieur permettra d'assurer une réactivation des services, les modalités de réactivation des services sont décrites dans un document spécifique mis à disposition du CEO. La récupération des données est assurée par une politique de sauvegarde interne à l'entreprise et par le contrat signé avec le provider Cloud.