PROJET D'ARCHITECTURE

Plan d'implémentation

Rep'Aero

24 mars 2021

SOMMAIRE

1. INTRODUCTION

Rep’Aero

Rep' Aero travaille avec ses clients pour assurer la maintenance corrective et préventive des pièces d'avion sous sa responsabilité (y compris les pièces motorisées, structurelles et avioniques).

L’entreprise joue un rôle clé dans le maintien de la navigabilité des avions, en garantissant le suivi sécurisé des données constructeurs, ainsi que l'application des réglementations françaises et européennes.

Cette analyse de faisabilité décrit les résultats sur la migration de l’architecture, les besoins du projet, le coût financier, les scénarios possibles et le scénario le plus adapté.

Dans les pages suivantes, nous trouverons les détails tout au long de cet analyse.

2. NATURE DES DONNÉES COLLECTÉES

Dans tout système avec des utilisateurs et des clients, il est nécessaire de collecter certains nombres et types de données. Ceci afin de faciliter le contact avec le client, de faciliter la communication avec les fournisseurs, de rationaliser le processus de facturation et de pouvoir effectuer un contrôle détaillé des commandes, de l'historique de chaque client, des responsables de la maintenance demandée par un client et de la quantité de pièces envoyées par les fournisseurs.

Ces données ne sont pas utilisées à d'autres fins que celles mentionnées ci-dessus, mais il est important que les clients et les utilisateurs en soient informés et expriment leur consentement à leur enregistrement dans les bases de données de l'entreprise.

Une fois ceci dit, la nature des données sera détaillée :

- Nom, adresse électronique, adresse et numéro de téléphone.
- Numéro de pièce, fournisseur, prix, mesures, disponibilité.
- Numéro de commande, client, fournisseur, employé.
- Ordre de service, employé, client, détails.
- Numéro de service, date du service, employé, client, motif.

Ces données seront extraites de la base de données existante et migrées vers les nouvelles bases de données afin de réaliser l'automatisation du nouveau système. De cette manière, les objectifs fixés par l'entreprise peuvent être atteints.

2.1. Obligations légales <<RGPD>>

Le RGPD, réglementation européenne sur la protection des données à caractère personnel avec une entrée en vigueur le 25 mai 2018. A ce titre, les sanctions encourues par la CNIL pour infraction peuvent s'élever jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire de l'entreprise.

La portée du RGPD considère comme donnée à caractère personnel toute information se rapportant à une « personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne (…). » (art. 4(1)). Les moindres références client, informations RH, données associées à un badge numérique, etc. constituent donc des données personnelles.

L'entreprise doit prendre les mesures nécessaires pour sécuriser le traitement des données à caractère personnel. Cela inclut « la protection contre le traitement non autorisé ou illicite et contre la perte, la

destruction ou les dégâts d'origine accidentelle » (art. 5(1)f)). Au-delà de la protection des données, le RGPD prévoit que l'entreprise mette en œuvre « des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique » (art. 32(1)c)).

La récupération de données n'est donc en rien une composante anecdotique du RGPD. Outre les dispositions de l'article 32, le RGPD enjoint les entreprises à déclarer auprès de la CNIL tout incident impliquant une violation de données à caractère personnel. Cette déclaration obligatoire doit, entre autres, « décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives » (art. 33(3)d)).

La confidentialité, l'intégrité, la disponibilité et la résilience des données telles que définies par le RGPD influent désormais sur la politique de gestion des risques de l'entreprise. Elles conditionnent également l'élaboration du PCA/PRA (Plan de Continuité et Plan de Reprise d'Activité) et, le cas échéant, de PRI et PCI (Plan de Continuité et Plan de Reprise Informatique).

La perte de données est en effet la conséquence la plus récurrente des sinistres qui peuvent toucher l'entreprise. L'objet d'un PCA/PRA étant de permettre la reprise ou tout au moins le fonctionnement en mode dégradé de l'entreprise en cas de sinistre, la disponibilité des données demeure un enjeu prioritaire. Naturellement conseillé pour limiter l'impact sur le chiffre d'affaire et l'image de marque de l'entreprise, son élaboration vise désormais à en limiter les impacts légaux.

3. RÉCUPÉRATION DES DONNÉES

La récupération de données consiste à retrouver les données perdues à la suite d'une erreur humaine, une défaillance matérielle, un accident ou au moment opportun d'un test de récupération de données défini dans une procédure de stratégie de sauvegarde et d'archive.

La difficulté de la restauration de donnée varie beaucoup, pouvant être une simple formalité ou au contraire, un défi technologique. Des logiciels spécifiques existent et plusieurs entreprises se spécialisent dans le domaine.

3.1. Enjeux

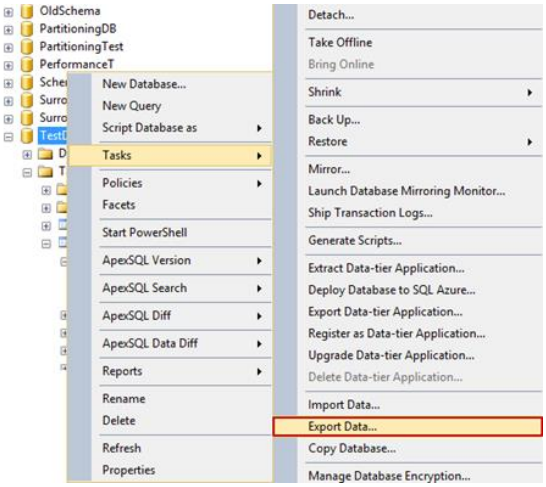
La perte de donnée non maîtrisée comporte des enjeux différents selon la nature des fichiers disparus et du contexte de leurs utilisation. Si l'entreprise perdre des données pourra être impactée financièrement.

3.2. Phases

Copier des données en utilisant l'assistant d'import et d'export de SQL Server

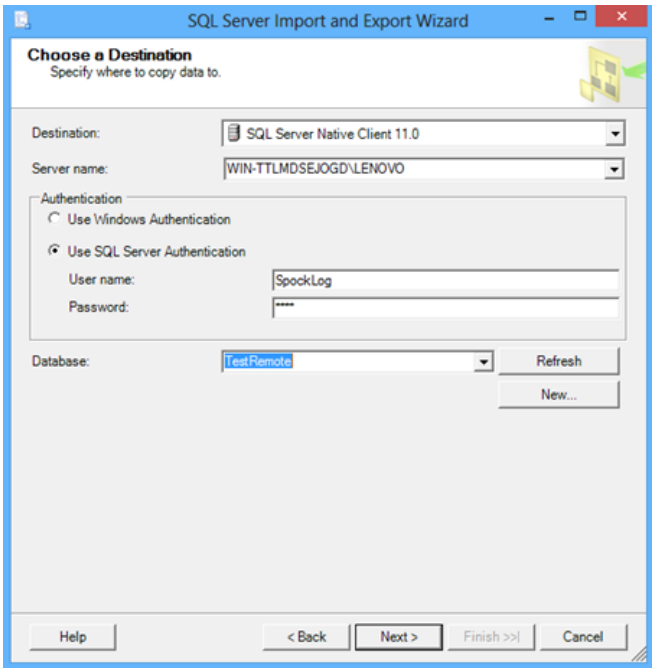
L'assistant d'importation et d'exploration crée un package SSIS (SQL Server Integration Services) qui peut être programmé pour fonctionner selon certains critères et modifié en utilisant les outils de données SQL Server.

Pour démarrer l'assistant d'import-export, faites un clic droit sur la base de données et sélectionnez **Tasks** (Tâches) puis **Export Data Command** (Commande d'exportation de données):



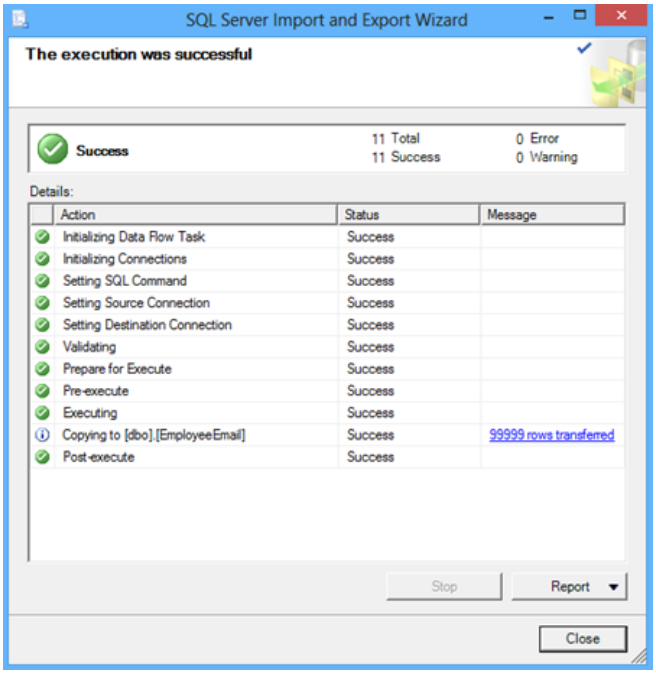
Dans la fenêtre **Choose a Data Source** (Choisir une source de données), connectez-vous à la base de données source. Des permissions suivantes sont nécessaires pour faire usage de l'utilitaire d'importation et d'exploration à partir de la source : lecture des données de la base de données ou du fichier et permission de la commande INSERT sur la base de données msdb pour sauvegarder le package SSIS

Dans la fenêtre **Choose a destination** (choisir une destination), connectez-vous à la base de données de destination. Des permissions requises pour l'accès à la base de données sont nécessaires pour les actions suivantes : écrire des données dans une base de données et créer une base de données ou une table si nécessaire :

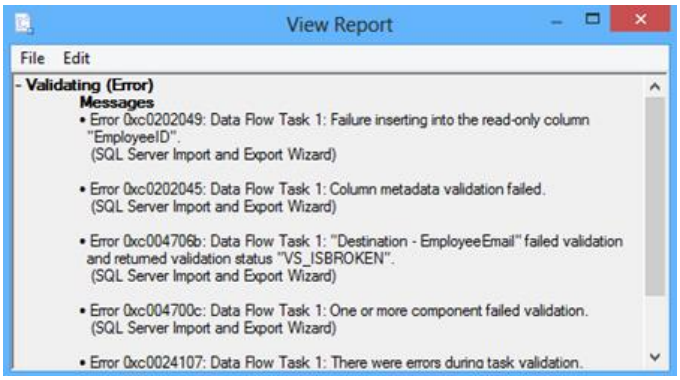


Dans la fenêtre **Specify Table Copy or Query** (Spécifier une copie de table ou une requête), choisissez l'option Copy data from one or more tables or views.

Choisissez les tables et les vues et sélectionnez l'option **Run immediately**:



Remarquez que l'utilitaire ne traitera pas une colonne de type IDENTITY différemment d'une autre colonne. Le système ne parviendra pas à insérer des données dans une table qui possède une colonne de type IDENTITY :



Si une table source a une clé de contrainte étrangère (Foreign Key Constraint), faites attention que l'utilitaire ne chargera pas les tables dans un ordre spécifique. Il est possible que la table contenant une clé étrangère soit chargée avant la table contenant la clé primaire qu'elle référence. Cela causera une défaillance au niveau de contrainte de clé étrangère. Une clé étrangère est une clé utilisée pour lier deux tables entre elles. C'est un champ dans une table qui se réfère à la clé primaire d'une autre table.

3.3. Sauvegarde des données

Dans cette partie, nous expliquerons les principales mesures à prendre lors de la sauvegarde de données importantes et de la plus haute importance pour l'entreprise.

- **Identifier et classer toutes les données** : Certaines présentent une importance capitale : brevets, fichiers clients et prospects, factures, documents administratifs et tous ceux intégrant des données à caractère personnel. Après avoir repéré leur lieu exact de stockage (prestataire Cloud), il est indispensable de les classifier par ordre d'importance selon une échelle de 1 à 5, 1 étant « insignifiant » et 5 « catastrophique ». Toutes celles qui ont 4 au minimum doivent bénéficier d'une sécurité renforcée : authentification et surveillance des accès, chiffrement, sauvegardes régulières.
- **Programmer des sauvegardes** : Il est important d'effectuer des sauvegardes fréquentes pour éviter la perte d'information. Selon le volume d'informations à protéger, il peut être opportun de prévoir des sauvegardes incrémentales à une fréquence quotidienne et des sauvegardes complètes à une fréquence moindre.
- **Des tests de restauration** : Cette pratique est essentielle. Tous les mois vous devrez vérifier que les données restaurées sont utilisables en l'état.

3.4. Types de sauvegarde

Il existe trois principaux types de stockage de données, qui sont brièvement détaillés ci-dessous :

- **Complète :** Toutes les données sont copiées indépendamment des modifications depuis la précédente sauvegarde.
- **Différentielle :** Elle permet de conserver toutes les modifications depuis la sauvegarde complète, quel que soit le type de modification.
- **Incrémentale :** Elle permet de conserver toutes les modifications depuis la précédente sauvegarde. Ce qui signifie que la préservation des données est effectuée depuis les sauvegardes incrémentales précédentes.

3.5. Conseils pour assurer la sauvegarde des données

Voici quelques conseils sur ce qu'il ne faut pas faire pour éviter les problèmes de toutes sortes qui peuvent mettre en danger vos données et votre entreprise.

- **Conserver les sauvegardes dans votre entreprise** : Imaginez un incendie dans nos locaux ; nos sauvegardes ont certainement brûlé sauf si vous les avez mises dans un coffre ignifugé et étanche. Pensons donc à héberger vos données dans le Cloud ou chez un prestataire informatique local.
- **Sauvegarder sur un DVD ou des clés USB** : Ces supports sont fragiles, ils ne sont pas éternels et nous pourrons les égarer facilement. L'usage des clés USB est par ailleurs fortement déconseillé, car elles peuvent contenir des virus informatiques et infecter les postes de travail.
- **Ne pas lire les Conditions générales de service** : Avant d'effectuer des sauvegardes sur des plateformes sur Internet (dans le Cloud) ou chez un prestataire informatique local, nous devrons vérifier les clauses du contrat concernant les procédures de sécurité mises en place. Il faut être attentif aussi à la présence d'une clause de réversibilité. Elle doit indiquer précisément comment et sous quel format nous pourrons récupérer nos fichiers si nous souhaitons changer de fournisseur.

4. ACTIVATION DES SERVICES

En première instance nous devrons identifier les parties pouvant être dissociées et transférées vers des micro services distincts. Une application bien structurée présente généralement des divisions très naturelles. Une classe de service fonctionne déjà comme une interface vers une couche de stockage de données et de logique métier. Elle représente la solution idéale pour connecter les appels de clients au micro service.

Nous pouvons adopter plusieurs approches pour séparer les fonctionnalités de notre application :

- Rechercher dans notre application une logique métier pouvant être séparée.
- Identifier le code isolé naturellement, par exemple en utilisant des outils d'analyse de code statique permettant d'identifier les sections.
- Examiner notre application afin de déceler une logique nous permettant de définir des paramètres de configuration du scalabilité ou des besoins en mémoire distincts de ceux du reste de l'application. Nous pourrons ainsi éventuellement réduire les coûts, ce qui peut contribuer à une meilleure utilisation des ressources.

Nous vous recommandons de refactoriser l'ancien code et de le déployer en production avant de diviser l'application en services distincts.

4.1. Étapes

Voici les étapes à suivre après avoir identifié un ensemble de classes pouvant devenir un micro service :

- Le code existant doit être conservé et opérationnel dans l'ancienne application de façon à faciliter le rollback.
- Créez un dépôt de code ou au moins un sous-répertoire dans le dépôt existant.
- Copiez les classes dans le nouvel emplacement.
- Créez une couche d'affichage qui fournit les hooks d'API HTTP et met en forme les documents de réponse de manière appropriée.
- Formulez le nouveau code sous la forme d'une application distincte (créer un app.yaml).
- Déployez votre nouveau micro service en tant que service ou projet séparé.
- Testez le code pour vous assurer qu'il fonctionne correctement.
- Effectuez la migration des données de l'ancienne application vers le nouveau micro service.
- Modifiez l'ancienne application afin d'utiliser la nouvelle application de micro services.
- Déployez l'ancienne application modifiée.
- Vérifiez que tout fonctionne comme prévu et qu'il n'est pas nécessaire de rétablir l'ancienne application.
- Supprimez tout le code mort de l'ancienne application.

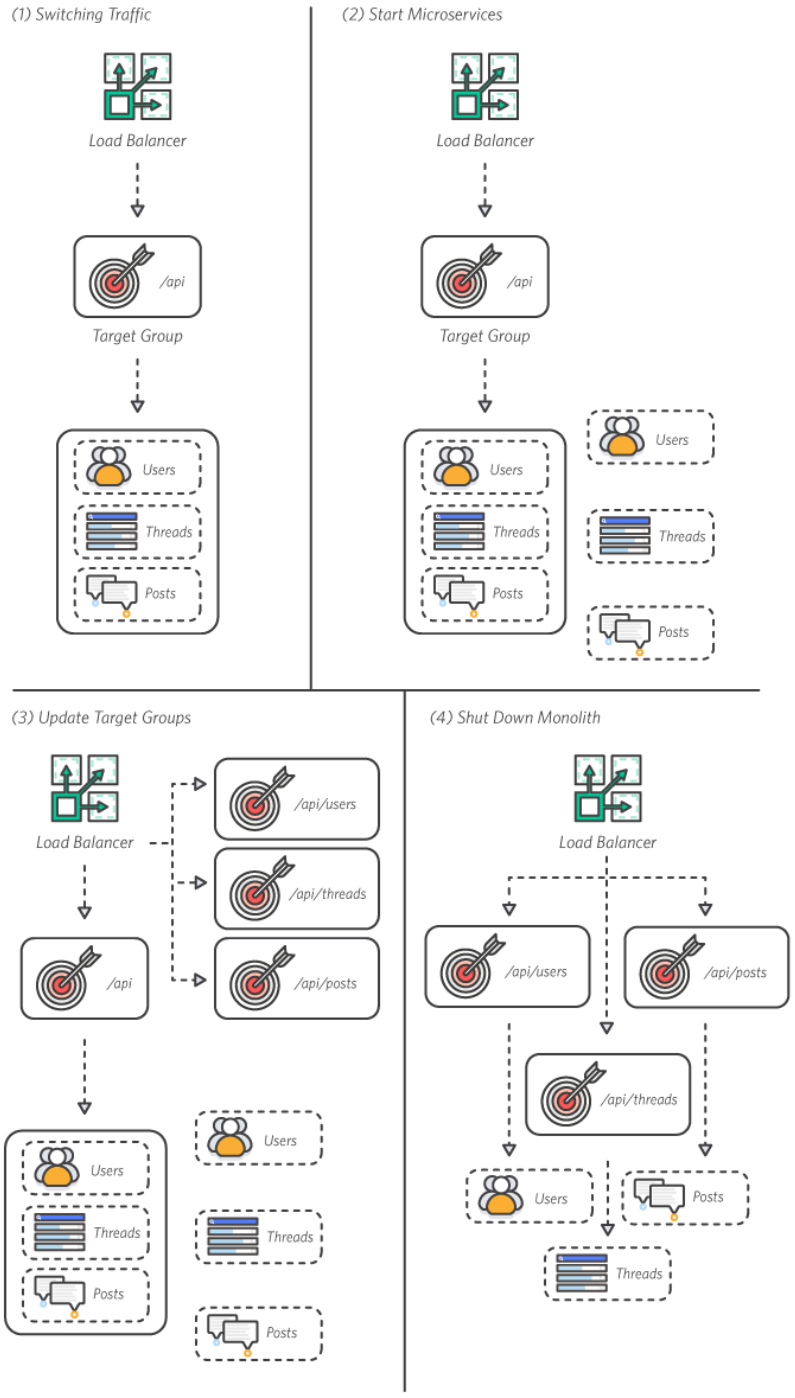
4.2. Migration en direct

La migration des données d'une application en live peut s'avérer délicate et dépend fortement de notre situation. Pour faciliter le déploiement et le rollback, il convient d'écrire du code qui est inséré à la fois dans les anciennes et les nouvelles entités Cloud Datastore, éventuellement à l'aide d'une API temporaire sur le micro service.

Il faut ensuite créer du code qui migre l'ensemble de données existant. Ce processus implique généralement l'utilisation de code temporaire et de données redondantes. En fonction de notre situation, nous devrons également exécuter une migration de données de rattrapage après le lancement. Nous devrons aussi faire attention à ne pas écraser les données récentes avec les données anciennes.

Même si ces tâches semblent nécessiter beaucoup de travail, elles sont courantes. Il faut pouvoir procéder au déploiement et au rollback dans le cas où la transition vers le nouveau micro service échoue. Nous ne pouvons pas nous débarrasser du code temporaire et supprimer les données de l'ancien emplacement de stockage qu'après avoir vérifié que tous les éléments ont été migrés correctement et que tout fonctionne comme prévu. Il faut faire des sauvegardes tout au long du processus.

Ici nous trouverons une image explicative de ce processus :



4.3. Responsabilités des acteurs pendant la migration

À ce stade, l'équipe de développement sera chargée de tout le travail technique, car ce sont eux qui possèdent les connaissances nécessaires pour mener à bien le processus du début à la fin. Cependant, ils seront sujets à des changements et/ou des commentaires de la part de l'équipe interne puisque ce sont eux qui ont le contact avec les clients et sont donc sensibles aux besoins de l'utilisateur final.