

Commentaires de l'AFNUM

Consultation de l'ARCEP afin de favoriser l'interopérabilité du Cloud

Juillet 2025

L'Alliance Française des Industries du Numérique (AFNUM) représente, en France, les entreprises fabricants les équipements et appareils numériques (serveurs, téléphones, ordinateurs, antennes réseaux) etc...) sur lesquels reposent les couches hautes du numérique (applications, logiciels etc...).

En tant que représentante des industriels du numérique l'AFNUM est particulièrement engagée sur les enjeux liés à l'informatique en nuage (Cloud) et suit depuis de nombreuses années les évolutions réglementaires en liens avec le cloud tant au niveau national (loi SREN) qu'europpéen (Data Act).

A ce titre, l'AFNUM avait participé aux premiers travaux de l'ARCEP relatifs à l'interopérabilité du cloud découlant de la loi SREN et souhaite partager ses nouveaux commentaires sur les recommandations actuelles de l'autorité.

Question 1 : Les informations proposées couvrent-elles selon vous les besoins des clients pour comprendre les modalités de portabilité et d'interopérabilité d'un service cloud ? Sinon, comment cette liste devrait-elle être modifiée selon vous ?

Tout d'abord l'AFNUM recommande à l'ARCEP de s'appuyer sur les normes existantes en matière de cloud et notamment la norme « ISO/IEC 19941 :2017 Technologies de l'information – Informatique en nuage – Interopérabilité et portabilité ».

Les sections 5 et 10 de cette norme contiennent des informations utiles afin de permettre aux utilisateurs de comprendre les caractéristiques d'interopérabilité du cloud.

S'agissant plus concrètement des recommandations l'AFNUM tient à partager les commentaires suivants :

1. Données (brutes ou dérivées) et actifs numériques qui peuvent être transférés dans le cadre d'une migration ou d'une utilisation simultanée des services de différents fournisseurs

Ces informations sont en générales disponibles dans la section « migration » dédiée à chaque produit mais celles-ci conservent une approche « indicative », elles ne peuvent assurer que lors de la migration le client se retrouve dans une situation identique.

Par exemple, dans le cadre de la migration d'une base de données les fournisseurs de cloud peuvent indiquer les modalités d'extraction de la base ainsi que les formats des données mais ne peuvent garantir que celles-ci fonctionneront dans le nouvel environnement. En outre, il est possible que des données provenant de logiciels tiers opérant dans le cloud ne puissent être extraites et migrées du fait de contrat de licence par exemple. Dans cette situation le fournisseur de service de cloud ne peut intervenir.

2. Procédures pour initier une migration depuis le service cloud

L'AFNUM tient à rappeler que les processus de migration sont profondément dépendant des clients et il est impossible de fournir une stratégie de migration « neutre » qui conviendrait à l'ensemble des clients même si des documentations générales peuvent exister.

Ces informations sont fournies en l'état et n'altèrent en rien le modèle de responsabilité partagée.

En effet, les migrations dépendent de facteurs qui ne sont pas nécessairement entre les mains du fournisseur de cloud tels que :

- Les capacités réseau du client
- Les volumes et types de données
- L'architecture des applications
- Les exigences d'intégration
- Les cas d'usage spécifiques du client

S'agissant plus largement du modèle de responsabilité partagée nous tenons à rappeler les points suivants :

- Les fournisseurs sont responsables de la sécurité et de la résilience de l'infrastructure
- Les clients sont responsables de leur stratégie de migration, notamment :
 - La planification et l'exécution
 - Les exigences de continuité d'activité
 - Les configurations de sécurité
 - Les procédures de testing, si le client a besoin de faire un test

Afin de fournir des informations précises aux clients et d'aligner l'offre de référence technique

avec le modèle de responsabilité partagée, nous recommandons de préciser dans les recommandations d'ARCEP de la liste des actions que restent sous la responsabilité du client.

3. Procédure pour initier une migration vers le service cloud

Même réponse qu'à la question 2.

4. Méthodes (téléversement, API, expédition de disques) disponibles pour la migration et l'utilisation simultanée des services de différents fournisseurs, y compris les protections disponibles (chiffrement) et les restrictions et limitations techniques connues

S'il est là encore possible de fournir des informations d'ordre général l'AFNUM tient à rappeler que les fournisseurs de cloud utilisent en majorité des outils tiers dans le cadre des processus de migration de leurs clients.

Si ces outils sont bien évidemment listés dans la documentation déjà accessible celle-ci peut ne pas être totalement à jour et il revient au client d'analyser ces différentes options et de choisir laquelle apparaît la plus pertinente. Bien évidemment, le fournisseur de cloud aide l'utilisateur lors de cette étape et apporte ses conseils au regard de la situation.

5. Méthode de migration recommandées en fonction du volume de données à transférer

Les méthodes de migration à privilégier dépendent avant tout du volume de données concerné. Ainsi, pour de faibles volumes, une migration en ligne est utilisée, tandis que pour de très grandes quantités de données, des solutions physiques (par disque dur ou bande magnétique) peuvent être envisagée même si ces mesures ne sont pas généralisées.

En conséquence, des recommandations générales sur ce point auraient une portée très limitée pour les utilisateurs qui, dans l'écrasante majorité des cas, vont privilégier une migration en ligne.

L'AFNUM considère qu'une telle exigence dans l'offre de référence technique ne serait pas réalisable en pratique car elle ne tient pas compte des multiples facteurs spécifiques aux clients qui vont au-delà du volume de données, tels que le type de données, les exigences de performance et les interdépendances entre applications et ensembles de données.

6. Méthodes pour garantir la sécurité des données lors du transfert (contrôle d'accès, authentification des utilisateurs, confidentialité et intégrité)

Ces informations dépendent grandement des solutions tierces retenues par le client qui doit ainsi se référer à cette documentation.

7. Procédures pour tester les différents mécanismes de migration, notamment ceux de sauvegarde (snapshot), de restauration (rollback) et de vérification de l'intégrité des données

Les fournisseurs de cloud fournissent déjà des informations relatives aux sauvegardes et aux procédures de restauration.

Néanmoins, ces informations demeurent de nature générale et ne correspondent pas forcément à la réalité d'une migration. Si l'on souhaitait avoir une telle documentation il faudrait que le fournisseur initial connaisse à l'avance le nouveau fournisseur et connaisse avec précision son environnement technique.

Une telle exigence nous apparaît disproportionnée et l'AFNUM considère qu'il revient au client de tester les différentes méthodes tout en mettant en œuvre les moyens nécessaires à ces tests.

8. Processus disponibles pour garantir l'intégrité des données, la continuité de service et prévenir la perte de données pendant la migration

La encore les fournisseurs de cloud accompagnent de manière personnalisée l'ensemble de leurs clients et il apparaît difficilement envisageable de fournir une documentation générale qui permettrait de fournir une réponse fiable.

Suivant les outils choisis par les clients les processus de protections peuvent varier et c'est pourquoi il est important de se référer à la documentation de ces outils.

9. Processus de résiliation d'un service cloud existant, lorsque le client souhaite mettre fin à son utilisation du service après migration

Ces processus sont décrits et énumérés dans les contrats, les accords de licence et les conditions générales.

Si certaines informations ne peuvent pas être rendues publiques les conditions générales contiennent en générales les conditions de résiliation.

10. Outils de supervision disponibles pour la migration et coûts associés à leur usage

La plupart des fournisseurs de cloud recommandent des outils de migration tiers/open source même si certains ont développé leurs propres solutions.

Il appartient au client d'exploiter l'ensemble des fonctionnalités des outils mis à sa disposition et de suivre les coûts liés à la migration.

11. Formats disponibles, recommandés ou utilisés dans le cadre d'une migration ou d'une utilisation simultanée des services de différents fournisseurs, ainsi que les spécifications et la documentation relatives à ces formats ;

Les fournisseurs Cloud ne peuvent pas fournir ces informations de manière exhaustive et systématique : les formats disponibles pour l'importation et l'exportation de données et d'actifs numériques dépendent du service concerné, du service de destination, ainsi que de l'outil de migration utilisé.

12. Référence de la documentation des API permettant la mise en œuvre de la portabilité et de l'interopérabilité ;

Les fournisseurs de cloud documentent l'ensemble de leurs API afin de permettre aux clients de déterminer comment adopter un service équivalent chez un autre fournisseur de cloud.

Cependant, un fournisseur Cloud ne devrait pas être contraint de maintenir la liste actuelle des API pendant toute la durée du contrat, car cette liste (ainsi que les options de migration associées) est susceptible d'évoluer dans le temps.

13. Description et documentation des dépendances, dont les bibliothèques de code, les données connectées à d'autres services cloud du fournisseur, et les services et outils tiers nécessaires à l'export des données dans le cadre d'une migration ou d'une utilisation multi- cloud

Les différentes dépendances qu'il peut exister au sein des environnements cloud sont déjà documentées par les fournisseurs de service.

Les dépendances entre la charge de travail et les services Cloud, ou entre les différentes charges de travail du client, ne sont connues que du client. Le modèle de responsabilité partagée décrit ce qui relève du fournisseur cloud et ce qui relève des clients.

14. Délais de migration et durée de transfert de données

L'AFNUM considère que ce point ne devrait pas être inclus dans l'offre de référence technique. Les fournisseurs ne sont pas en mesure de préciser le temps nécessaire aux clients pour effectuer leur migration ou transférer leurs données. La planification et l'exécution du processus de migration, y compris l'estimation des délais, relèvent principalement de la responsabilité du client. Ces durées varient considérablement selon de nombreux facteurs hors du contrôle du fournisseur : bande passante et connectivité réseau du client, volume et type de données transférées, transformations de données nécessaires, ainsi que l'architecture spécifique des applications du client.

L'obligation du fournisseur concernant la durée de migration se limite à garantir qu'il dispose des capacités techniques nécessaires pour permettre à ses clients d'effectuer leur migration dans le délai transitoire maximal prévu par la réglementation. Cette approche est conforme à la nature du processus de migration centré sur le client.

Question 2 : Le délai de préavis vous semble-t-il approprié ? Dans le cas contraire, quel délai préconisez-vous ? Pourquoi ?

L'AFNUM considère le délai de 12 mois comme approprié dans la plupart des situations néanmoins il serait pertinent **que l'ARCEP souligne que des délais plus courts peuvent être nécessaires dans certaines situations comme la nécessité de se conformer à des obligations légales.**

Entre outre, l'AFNUM estime que des précisions complémentaires sont nécessaires. Tout d'abord, la notion de « modification majeur » devrait être expressément définies comme lorsque des changements risqueraient de provoquer l'échec d'une requête qui fonctionnait avant la mise à jour.

Ensuite, et comme souligné plus haut, des exceptions au délai de préavis doivent exister afin de permettre de déployer des correctifs de sécurité ou pour préserver l'intégrité des services.

Question 3 : L'adoption généralisée de la spécification OpenAPI vous semble-t-elle souhaitable, notamment afin de permettre une documentation des API harmonisée ?

Si OpenAPI est très utilisé dans l'industrie l'AFNUM émet quelques réserves quant à sa généralisation via les recommandations.

En effet, OpenAPI n'est pas forcément adapté aux services de cloud les plus complexes et ne supporte pas certaines fonctionnalités. D'un point de vue plus technique l'utilisation d'OpenAPI pourrait nécessiter des réécritures et engendrer de l'instabilité pour certains services.

En particulier, OpenAPI est fondamentalement lié au protocole HTTP et aux formats de données comme JSON, limitant ainsi son applicabilité à tous les services cloud. Des protocoles comme MQTT utilisés pour l'Internet des Objets ou des services nécessitant une diffusion bidirectionnelle sur HTTP/2 ne peuvent pas être correctement décrits par OpenAPI. Les fournisseurs de cloud utilisent donc souvent des solutions plus adaptées comme Smithy ou TypeSpec qui permettent de décrire plus précisément leurs services complexes tout en maintenant une compatibilité ascendante.

C'est pourquoi, l'AFNUM recommande :

- De prendre en considération que certains fournisseurs pourraient nécessiter un délai pour adopter les dernières versions de la spécification ;
- De mentionner OpenAPI "et/ou des certifications équivalentes", sans exclure la possibilité de recourir à d'autres spécifications qui satisferaient aux exigences réglementaires. Il conviendrait d'ailleurs de discuter de ces options au sein du CEN-CENELEC JTC 25.

Par ailleurs, imposer une unique spécification pourrait pénaliser certains secteurs, notamment les télécommunications, qui utilisent des API répondant à des logiques métiers spécifiques.

Une approche plus souple, tenant compte de ces particularités, paraît donc préférable.

