C2C : l'obligation de l'inter-Clouds

23 Septembre 2022

claude@lemarson.com
https://www.lemarson.com

Sommaire

C2C (Cloud-to-Cloud) : l'obligation du secours inter-clouds

Le marché global du Cloud est attendu à 1 025 G$ en 2028 (Facts and factors), contre 429 G$ en 2021, dans lequel le C2C représentera 12,88 G$ en 2029 (MMR)

Cloud, une certitude, mais…

- Les Mega-Providers : IBM, Google, Microsoft et AWS et une multitude de petits acteurs locaux…nationalistes (souverains)
- Les acronymes « everything as a service » se multiplient à l'infini
- Les grosses applications arrivent dans le nuage : SAP, Spark et Splunk chez AWS…
- Le nuage, ce n'est pas de l'impartition (externalisation) : c'est un TI à part entière, avec ses règles, ses contraintes et ses modes de fonctionnement
- Montée des nuages « verticaux » : santé, assurances, finance…
- La disponibilité des services atteint un très haut niveau, proche des 100 %
- Mais…
  - Manque de standards clairs : la confiance en Open Stack s'effrite
  - La sécurité reste un gros point faible…
  - Le nuage n'est pas gratuit. Contradiction entre la nécessité de planifier la charge pour obtenir des coûts intéressants et le côté imprévisible du Cloud
  - Doutes sur certaines architectures mises en œuvre : bases de données, containers
  - Inadéquation (pour l'instant) entre les Clouds et les objets (capteurs)
  - Inutilité de certains Clouds souverains

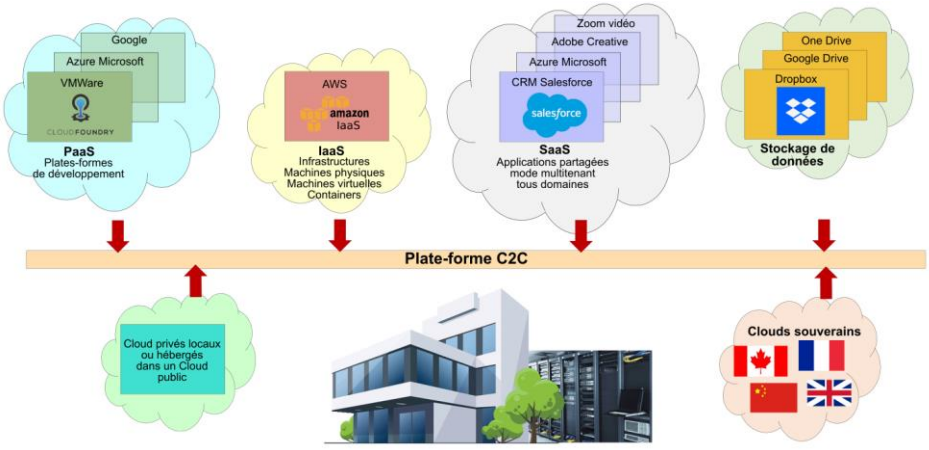
Les objectifs à se fixer

- C'est le TI de demain, dont il s'agit
- Datacenter dans le Cloud
- Ce n'est pas un projet de TI, mais celui de l'entreprise
- Il faut le construire sur des bases solides, incontestables
- … quitte à surseoir à certains investissements
- Ne pas confondre protection et reprise des données, avec couverture globale : traitements, données, sécurité : backup contre PCA/PRA
- Personne n'aurait imaginé un TI mainframe centré uniquement sur les données de bureautique
- Il faudra prendre son temps et étaler les projets en fonction de la disponibilité des solutions : entre 5 et 10 ans !
- Les risques sont grands de se précipiter et de construire des "usines à gaz", qu'il faudra ensuite détruire

Conseil au management : être patient

Les infrastructures à prendre en compte

Le TI de demain



Les sinistres : ça arrive même aux GAFAM

- Foudre tombée sur un datacenter Google en 2015
- Incendie du centre OVH de Strasbourg en 2021 : 3,6 millions de comptes bloqués
- Panne mondiale AWS en 2022
- La faute consisterait à ne pas imaginer le pire
- **La première chose à faire après le choix d'un prestataire de Cloud est d'envisager sa faillite, son rachat… même s'il s'agit de Google, Microsoft ou AWS**

C2C et la gestion des risques

Un management impatient : le ROI se fait attendre...

Les situations de crises ne sont pas à exclure, même avec des prestataires majeurs : risques financiers importants

Non respect des contraintes règlementaires qui exposent l'entreprise à de lourdes sanctions financières

Le cadre sécuritaire du Cloud n'est pas conforme aux règles internes de l'entreprise

Perte de contrôle de la qualité des prestations fournies

Compatibilité et remise en cause de pans entiers du TI actuel

Perte de maîtrise de la confidentialité des données : on ne peut rien faire en dehors du cadre prévu

Récupération de données sensibles du fait de la faible maturité du chiffrement homomorphe

Incapacité à répondre à des besoins nouveaux et urgents, car non prévus par les prestataires

Une grande complexité matérielle et logicielle : plusieurs Clouds + local + Clouds de secours, qui induit des coûts élevés et incontrôlables et une équipe expérimentée

Le non respect des standards empêche l'entreprise de s'organiser et de faire face aux défaillances

Dépendance vis-à-vis d'un prestataire : à terme coûte très cher...

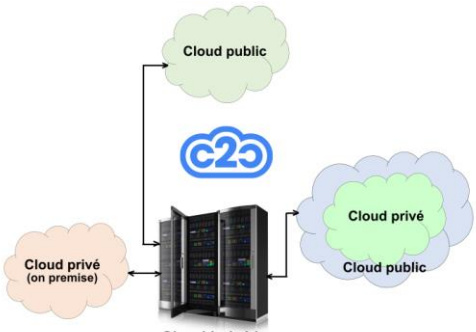
Perte de contrôle des performances du TI... même si les prestataires sont plus crédibles que les TI internes

Vol de données d'authentification

Incapacité de l'entreprise à faire son métier, par faillite du prestataire

Un choix d'architecture :

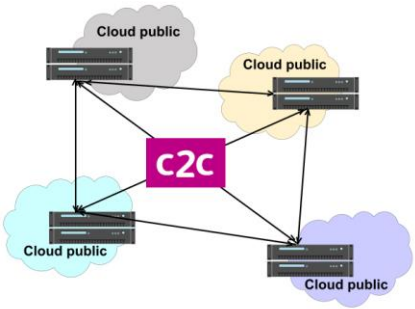
MultiCloud ou hybride



Cloud hybride

(bonnes et mauvaises raisons)

- Certaines ressources ne doivent pas "sortir" de l'entreprise
- Tests de services Cloud avant de les adopter
- Nécessité de mettre en place un service d'authentification "mieux" maîtrisé
- La multiplicité des fournisseurs contribue à la fragilité du TI (on peut la contrôler en partie)



Multi-Cloud

(bonnes et mauvaises raisons)

- Une entreprise ne trouve pas certains services chez son fournisseur principal… et regarde ailleurs…
- Extension des ressources matérielles et logicielles pour des questions de sécurité et performances
- Mise en place d'un PCA/PRA
- Application du principe de "best of breed"
- Respect de contraintes politiques et obligation d'utiliser des Clouds souverains… quand ils sont disponibles
- Haute disponibilité 7/24

Si on n'y prend pas garde...

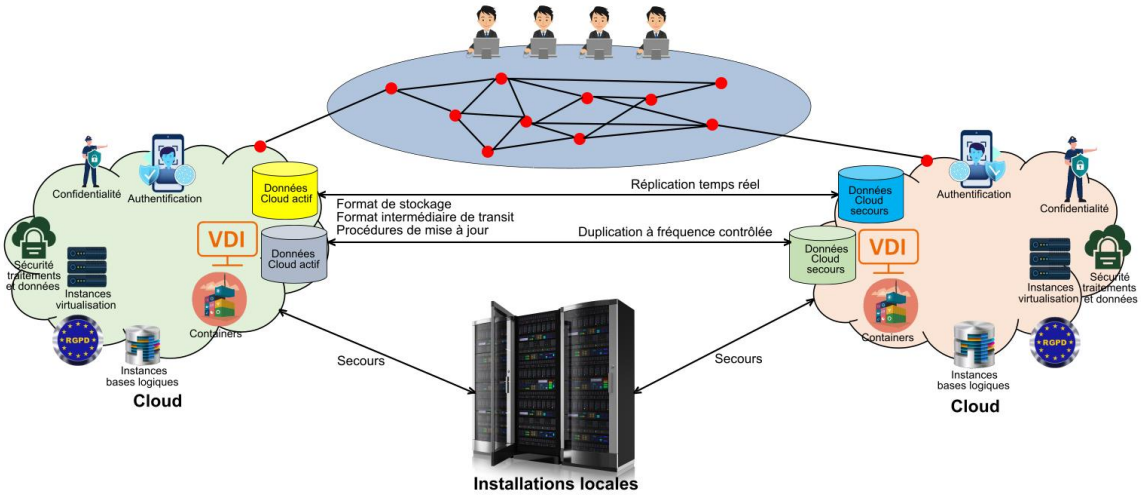
Ce qui nous attend

Des recommandations de bon sens

- Attendre du management des entreprises qu'il se détermine sur ce qu'il attend du Cloud dans le futur.
- Ne jamais faire confiance à un seul prestataire, fut-il aussi "installé" qu'AWS ou Microsoft. Aucun prestataire n'offre une couverture suffisamment diversifiée et robuste, pour garantir la pérennité complète des services (risque de SPOF : "Single Point Of Failure", point unique de fragilité).
- Ne pas faire confiance à un seul pays d'implantation, même s'il s'agit des Etats-Unis et se méfier du zonage théorique des implantations, qui pourraient dépendre de décisions politiques et intégrer dans la boucle des solutions locales ("Clouds souverains"), à condition que celles-ci existent.
- Ne faire affaire qu'avec des prestataires qui respectent les standards. Si ces standards sont insuffisamment matures (Open Stack), on restreindra les investissements à des solutions provisoires.
- Etre totalement **paranoïaques** et tester systématiquement les solutions mises en place.
- Ne pas s'enferrer dans des solutions propriétaires sous prétexte de traiter **UN** problème : le C2C est une perspective globale
- Intégrer le C2C dans un plan plus général de PCA (Plan de Continuité d'Activité) et PRA (Plan de Reprise d'Activité) et définir un périmètre minimum de fonctionnement du TI, pour assurer la permanence des services "régaliens" de l'entreprise.
- Procéder à une mise à niveau sérieuse des infrastructures internes, pour ne pas dégrader les conditions d'accès aux services.

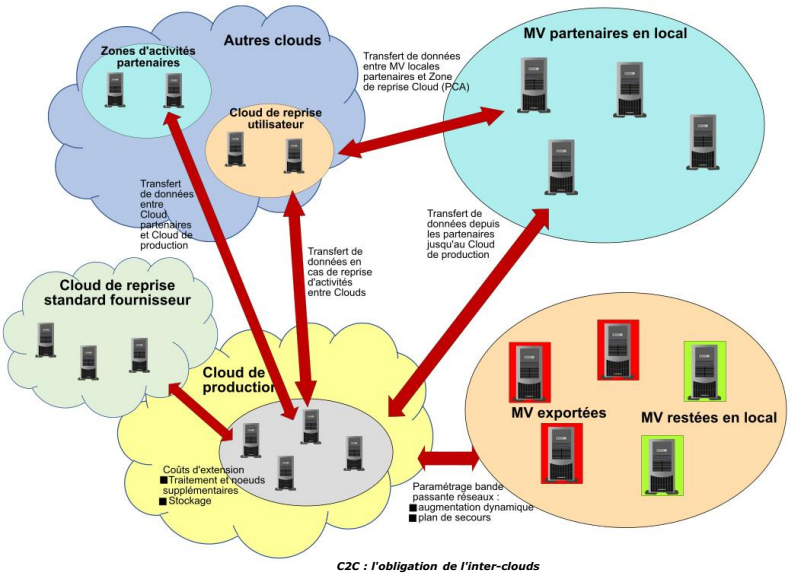
Etre paranoïaque...

Les "vrais" problèmes à traiter

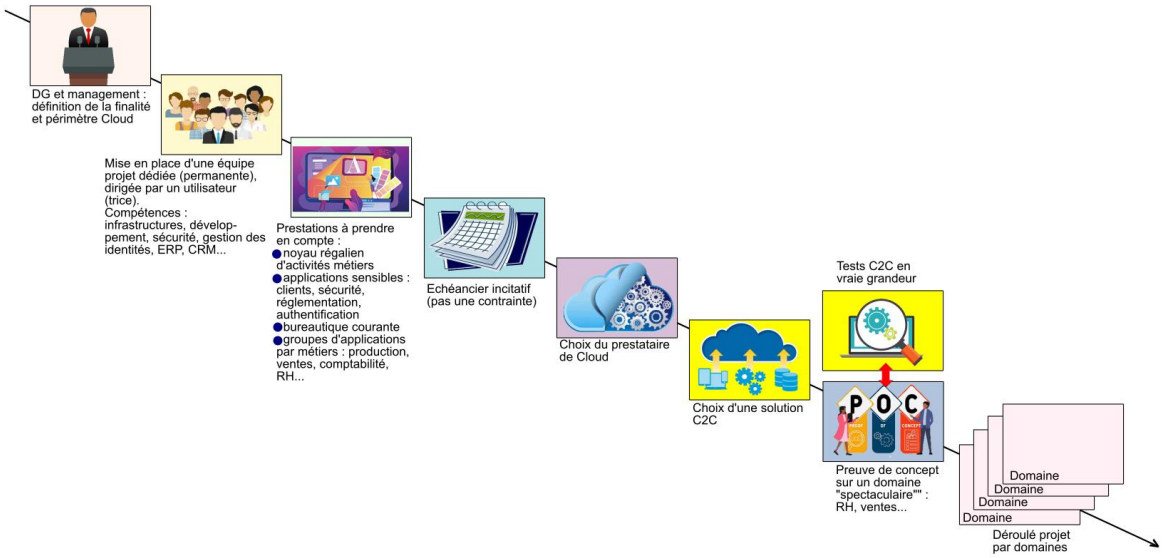


Un modèle classique

Deux cas principaux de transfert de données sont à envisager : activité normale et situation de crise (bascule partielle ou totale chez un autre hébergeur de Cloud ou le même prestataire).

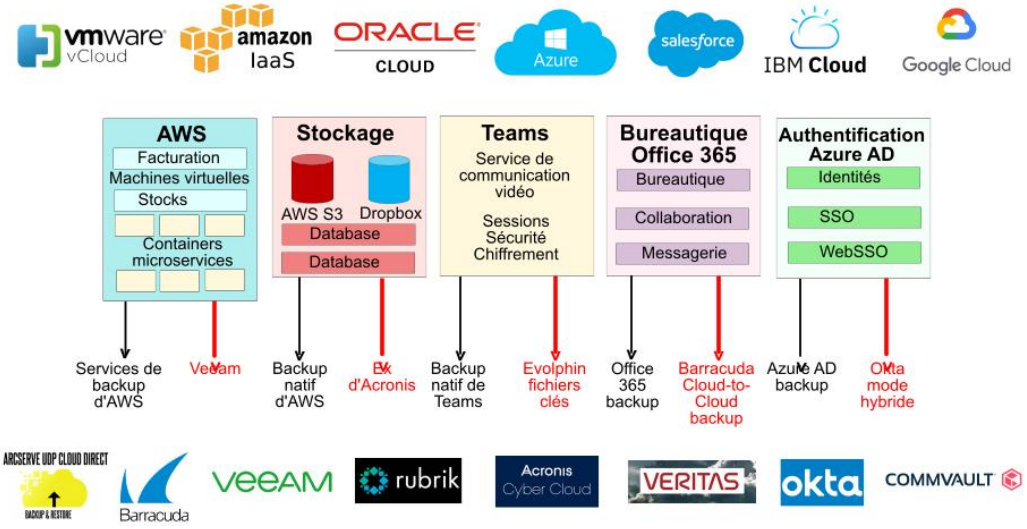


Une stratégie en plusieurs phases



La spécificité des prestataires

Des solutions trop parcellaires et dédiées



Les solutions génériques arrivent…

- Des solutions apparaissent plus ou moins génériques.
- Des solutions qui se diversifient : poste de travail et serveurs.

Acronis
Acronis Cyber Backup Cloud sauvegarde des espaces virtuels, physiques et Cloud. Il comporte un système de paiement "pay-as-you-go".

arcserve
Arcserve dispose d'UDP Cloud Direct, pour la sauvegarde et la restauration Cloud. Elle est destinée aux systèmes moyens.

IDrive
IDrive est un backup Cloud, doté d'outils de synchronisation.

Azure Backup
Microsoft Azure Backup envoie les backups sur Azure. Possibilité de réplications d'infrastructures privées Windows.

UNITRENDS
Unitrends est une solution de backup vers le Cloud privé Forever Cloud. Plusieurs services de récupération.

Asigra est un pionnier de la sauvegarde C2C.

CARBONITE
Carbonite s'adresse aux usagers Windows et Mac. Très populaire. Acquis par OpenText.

BACKBLAZE
Backblaze propose une solution de backup Cloud. Les données sont stockées dans une infrastructure Open Source. La restauration lancée via Web, s'effectue en SSL.

druva
Druva propose Druva InSync pour le Cloud public et Phoenix, un agent de sauvegarde et restauration. A acquis CloudRanger, un spécialiste AWS.

veeam Cloud Connect
Veeam Software fournit un service de backup via son "Cloud Connect". Fonctionne en partenariat avec plusieurs FAI (accès Internet).

- Mais aussi StorageCraft, Sophos, Veritas Technologies, VMWare, CommVault, Actifio, N-able backup, Barracuda, Carbonite, Code42, Datto, Efolder, IBM, Oracle…
- Le marché spécifique du backup Office 365 est très actif : Acronis Cyber Backup, Altaro Office 365 backup, Barracuda Cloud-to-Cloud backup, Veeam Backup for Microsoft Office 365, Synology Active Backup for Microsoft 365
- De même pour le marché AWS

En résumé, avant de se quitter…

- Ne pas éluder la question : c'est le TI de demain
- Ne pas se lancer sans un "feu vert" clair du management
- Ne pas se précipiter, on procèdera par touches homéopathiques
- Le marché n'a pas encore décollé
- Les standards (Open Stack) sont contournés (Microsoft et Azure Stack), ce qui risque de créer la confusion
- Risque d' "unixisation"
- Attention aux coûts, les grilles sont très différentes : exemple des données, volumes de stockage, facturation des données échangées
- Il subsiste des problèmes techniquement non résolus : traitement sur le Cloud de données chiffrées (chiffrement homomorphe)
- Les fournisseurs sont très (trop) nombreux, fonctionnellement spécialisés (données), voire dédiés à un "hyperscaler" donné comme Google, Microsoft Azure ou AWS : leur nombre va diminuer
- Avec un seul fournisseur Cloud, le risque de SPOF est grand, ainsi que de dépendance
- C'est un problème d'infrastructure qui doit être piloté par l'entreprise et les utilisateurs
- Les initiatives sectorielles indépendantes ("shadow IT", une ânerie) sont à proscrire formellement : le Cloud est un projet global
- Se préparer dès maintenant

C2C : L'obligation de l'inter-Clouds

23 Septembre 2022

Nos prochains webinaires

30 Septembre 2022 :	**Pleins feux sur les "smart contracts"**
7 Octobre 2022 :	**Non, Cobol n'est pas un "gros mot"...**
14 Octobre 2022 :	**L'autisme au service du TI**
21 Octobre 2022 :	**Le cellulaire privé contre Wi-Fi**
28 Octobre 2022 :	**WebAssembly et LLVM, pour de meilleures performances Web**
4 Novembre 2022 :	**Les bases de données distribuées**
18 Novembre 2022 :	**Les algorithmes de chiffrement, ces inconnus**
25 Novembre 2022 :	**Vers l'authentification invisible et permanente**
2 Décembre 2022 :	**Les nouvelles protections périmétriques du TI**
9 Décembre 2022 :	**Kubernetes, le Windows des conteneurs**
23 Décembre :	**La programmation du comportement des réseaux**

claude@lemarson.com
https://www.lemarson.com