

# Cloud

Partie 2/2

Par M. JEANNIN THOMAS

Pour M. Romaric Thibault

# Présentation des Clouds Privée et des Clouds Publics :

## Cloud Public :

Un cloud public est une infrastructure informatique dans laquelle un fournisseur de services met des ressources à la disposition du public via internet. Les ressources varient selon le fournisseur mais peuvent inclure des capacités de stockage, des applications ou des machines virtuelles.

### Point fort :

- Paiement adaptée, proportionnelle avec les besoins
- Pas de frais de maintenance
- Résiliable à tout moment

Il s'agit d'un abonnement donc pas d'engagements.

Peu de risques de pertes de données :

la plupart des fournisseurs de cloud public disposent de plusieurs solutions de secours en matière d'infrastructure de sauvegarde.

Coût associé à la bande passante et au matériel est pris en charge par le fournisseur

- adaptable aux besoins (Scalabilité):  
si nous voulons momentanément ou dans le temps les clouds publics permettent d'adapter nos besoins instantanément.

### Point Faible :

- Aucune maîtrise de l'infrastructure et de la gestion faites dessus.

- Le matériel ne nous appartient pas  
Nous n'avons pas la main sur le matériel.

## -Sécurité des données

Les fournisseurs mettent un point d'honneur à assurer la confidentialité et la protection des données.

Chaque service est fourni sécurisé mais son utilisation ne l'est peut être pas. C'est pour cette raison que les utilisateurs/clients/entreprises doivent adopter les bonnes pratiques de cybersécurité.

En cas de problème le support est souvent externalisé qui ne fournit pas forcément l'aide nécessaire. Comme par exemple pour les licences d'utilisation non réutilisables ou l'incompatibilité avec la virtualisation.

### Cloud privé :

Le Cloud Privé est un Cloud géré ou financé par la société elle-même. La société peut également faire appel à un prestataire externe spécialisé pour gérer le Cloud. Ce sont les serveurs de l'entreprise qui gèrent les données de celle-ci.

### Point fort :

Améliore la sécurité :

les clouds privées hébergent souvent leurs infrastructures réseaux au sein de leurs locaux ce qui améliore la sécurité (évite les entrées et sorties du réseau)

De ce qui est de la sécurité virtuelle elle est assurée grâce à des pare-feu les liens réseau.

Meilleure personnalisation :

les clouds privées ont été créées pour qu'ils soient personnalisés à souhait afin de répondre au mieux au besoin du client

Coût d'exploitation moins élevé :

moins de coûts cachés.

Conformité :

les fournisseurs de cloud privée proposent une mise en conformité

### Point Faible :

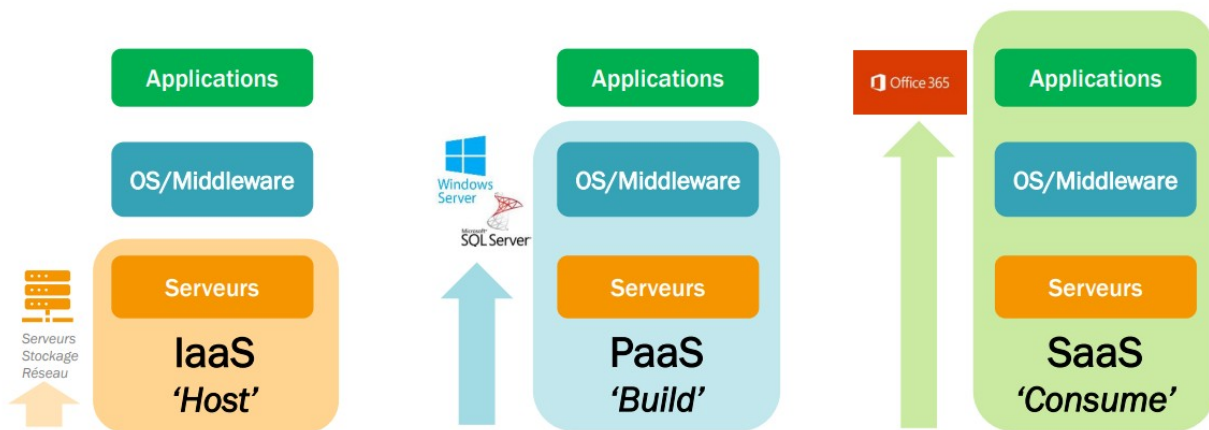
-gros coût de démarrage(achat des serveurs, mise en marche) :

il faut pour pouvoir mettre en place prendre en compte, l'achat des serveurs, les coûts d'électricité.

-frais de maintenance : en cas de maintenance, ce type d'installation nécessite de la maintenance.

-Mobilise des techniciens donc nécessite la compétence.

Il existe plusieurs objectifs à avoir un Cloud : Stockage, hébergement de site internet etc.... Les enjeux sont de garder les points forts du cloud public et ceux également du privée afin par exemple de garder la sécurité du cloud privée et la scalabilité du public.



### Infrastructure as a Service (IaaS) :

Ce type de Cloud gère que le socle de l'infrastructure, il vous laisse administrer le reste tel que l'OS ou l'application, le fournisseur ne prend en charge que le stockage et la virtualisation. Dans cette solution à la différence de la PaaS et le SaaS nous avons en charge

l'OS ou l'environnement d'exécution... comme le montre le schéma de Red hat un peu plus bas.

### Platform as a Service(PaaS) :

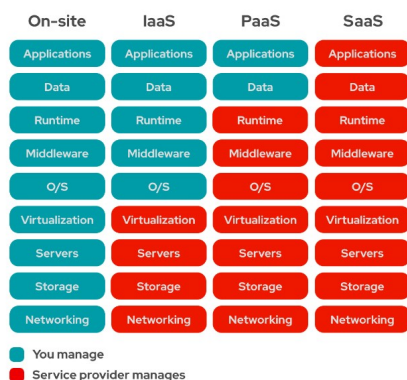
Le Paas est une solution en partie destinée au développeur. Le Paas agit comme un Framework laissant le développeur la liberté de la création et la gestion de ses applications sans avoir à se soucier de la gestion de l'infrastructure, des mises à jour ou de la gestion matériel.

Cette solution offre également une interface à l'utilisateur pour lui permettre l'utilisation du cloud.

### Software as a Service (SaaS) :

ce Cloud est une sorte de « formule tout compris ». Elle fournit un tableau de bord ou même une API afin de centraliser la gestion de l'application que l'on souhaite héberger(rien n'est stocké sur les machines des clients/entreprises/utilisateurs). Le reste est en partie géré par le fournisseur ce qui peut nuire aux contrôles de nos données et donc à la sécurité de celle-ci.

les lettres « aas » signifient que le cloud agit comme un service fournit par un tiers afin que l'on n'ait pas à les gérer et que l'on puisse se concentrer sur les aspects importants.



Comme montrer sur ce schéma affiché sur le site de l'entreprise Red Hat, le nombre de zones ou de tâches à administrer évolue selon le type de cloud que l'on choisit. l'IaaS n'offrant que la machine virtuelle à peu près jusqu'à l'SaaS prenant à sa charge la gestion de toutes les couches.

Un VPS aussi appelé Virtual Private Serveur en anglais et et serveur privé Virtuel en Français.

Un VPS est une machine virtuelle qui fait office de serveur. Elle bénéficie de tous les avantages d'un serveur physiques. Cette solution de stockage peut être mise en place chez soi si l'on en a la possibilité et les compétences ou être un service que l'on confie à des entreprises comme OVH par exemple.

Un VPS rentre dans la catégorie des cloud public car les VPS ne peuvent pas communiquer entre eux même si elle sont administrés par la même entité. À l'inverse d'un VPC

Le VPS et l'IaaS sont très similaires mais l'IaaS offre une meilleure flexibilité au niveau du stockage et de la puissance car elle s'adapte à l'utilisation que l'on en fait comparé au VPS qui a une configuration et une puissance fixe. L'IaaS offrant des possibilités multiples et adaptable à l'utilisation que l'on en fait coûte en moyenne 20 % plus cher.

Le « Dell Technologies Global Data Protection Index » est le rapport annuel de Dell sur la protection des données dans le monde.

#### Nouvelles informations recueillies en 2021

Les risques liés aux cybermenaces, au télétravail et aux charges applicatives modernes sont au premier plan.

62 %

Inquiétude liée à la gestion des logiciels malveillants et des rançongiciels

74 %

Détection d'un risque accru de cybermenaces lié au télétravail

67 %

Difficulté à protéger les applications Cloud natives

La perte des données a coûté en moyenne 959 493 \$.

De ce qui est des interruptions non planifiées des services, ils ont coûté en moyenne 513 076 \$.

S'agissant d'une moyenne, cela veut dire que certaines pertes ont coûté bien plus que cela. Il y a un manque clair de prévention afin de limiter ces coûts

tel que la mise en place de backs ups ou de plateforme de secours en cas de panne.

La compensation des pertes reste une tâche compliquée car quand une donnée est perdue, elle est irrécupérable néanmoins l'on peut essayer de se rapprocher au maximum de ce que l'on a perdu en mettant en place un politique de sauvegarde stricte tel qu'une sauvegarde incrémentielle bi journalière où toutes les 6h avec une sauvegarde complètent tous les 2 jours

### Plan de Continuité d'Activité :

Le PCA est un plan d'action préventif, dans la mesure où il s'agit d'un plan qui permet d'éviter tout arrêt de l'activité dans la mesure du possible. Le plan de continuité d'activité contient donc de nombreuses procédures à suivre pour pallier une situation critique et y répondre à court terme.

Il prévoit beaucoup de situations possibles afin que les pertes soient réduites voire évitées.

Pour cela il doit contenir :

- le contexte (obligation, objectifs de l'entreprise)
- les risques
- Pour chaque activité, la tolérance d'arrêt, les ressources vitales/critiques nécessaire à avoir.

Le Plan Reprise d'Activité, lui est utile une fois l'accident arrivé il doit contenir :

- un état des lieux des enjeux et besoins de l'entreprise.
- le listing des activités qui sont clés pour le bon fonctionnement de l'entreprise.
- l'identification des incidents possibles.
- les actions à mener en amont pour limiter l'impact de ces incidents sur ces activités importantes.
- les ressources-clés qui se révèlent indispensables pour réaliser ces activités clés.
- la démarche et les étapes à suivre pour remettre en route l'activité (surtout dans le cadre d'une reprise progressive).

Il existe néanmoins certains risques :

- Risque humain: une grève ou un accident d'un travailleur.
- Risque naturel: des intempéries ou une pandémie.
- Risque logistique: un délai de livraison ou la faillite d'un fournisseur.
- Risque technique: une panne ou une casse d'une machine.
- Risque data security: un piratage, un vol de données ou un bug.
- Risque matériel: un vol ou un incendie.
- Risque client: un délai de paiement ou une créance douteuse.

Établir un plan de reprise d'activité de qualité est donc essentiel. Même si le tout semble nécessiter un travail titanesque, c'est relativement simple à mettre en place avec les bonnes clés. Vous devez simplement procéder de manière réfléchie et systématique afin d'agir de manière claire dès qu'un incident intervient. Dans tous les cas, créer un plan de reprise d'activité à jour, efficace et fiable vous permettra de favoriser la pérennité de votre entreprise.



Source :

<https://www.obat.fr/blog/plan-continue-activite/>

<https://safetyculture.com/wp-content/media/2019/02/business-continuity-template-report.pdf>

<https://www.oracle.com/fr/cloud/definition-cloud-public/#:~:text=Un%20cloud%20public%20est%20une,applications%20ou%20des%20machines%20virtuelles.>

<https://www.dell.com/fr-fr/dt/data-protection/gdpi/index.htm>

<https://www.ovhcloud.com/fr/vps/definition/>

[https://fr.wikipedia.org/wiki/Serveur dédié virtuel](https://fr.wikipedia.org/wiki/Serveur_d%C3%A9di%C3%A9_virtuel)

<https://www.datacenters.com/news/what-is-the-difference-between-vps-and-cloud-iaas>

<https://www.ailancy.com/wp-content/uploads/2020/07/ailancy-etude-cloud-juin-2020.pdf>

[https://www.redhat.com/fr/topics/cloud-computing/iaas-vs-paas-vs-saas?sc\\_cid=7013a000002pgRTAAY&gclid=Cj0KCQiAg\\_KbBhDLARIsANx7wAwqXe80jFMfc-pZYYDGBG5oU8RQLS8WoJVlX5PMUjP1F2RcriUqHyEaAkA3EALw\\_wcB&gclsrc=aw.ds](https://www.redhat.com/fr/topics/cloud-computing/iaas-vs-paas-vs-saas?sc_cid=7013a000002pgRTAAY&gclid=Cj0KCQiAg_KbBhDLARIsANx7wAwqXe80jFMfc-pZYYDGBG5oU8RQLS8WoJVlX5PMUjP1F2RcriUqHyEaAkA3EALw_wcB&gclsrc=aw.ds)

<https://www.dell.com/fr-fr/dt/data-protection/gdpi/index.htm#scroll=off&pdf-overlay=//www.delltechnologies.com/asset/fr-fr/products/data-protection/briefs-summaries/global-data-protection-index-infographic-global.pdf>

<https://www.economie.gouv.fr/files/hfds-guide-pca-plan-continuite-activite-sgdsn.pdf>

<https://www.obat.fr/blog/plan-de-reprise-d-activite/>

<https://www.ntiva.com/blog/private-cloud-pros-cons#:~:text=A%20private%20cloud%20costs%20more,it%20also%20offers%20greater%20customization.>