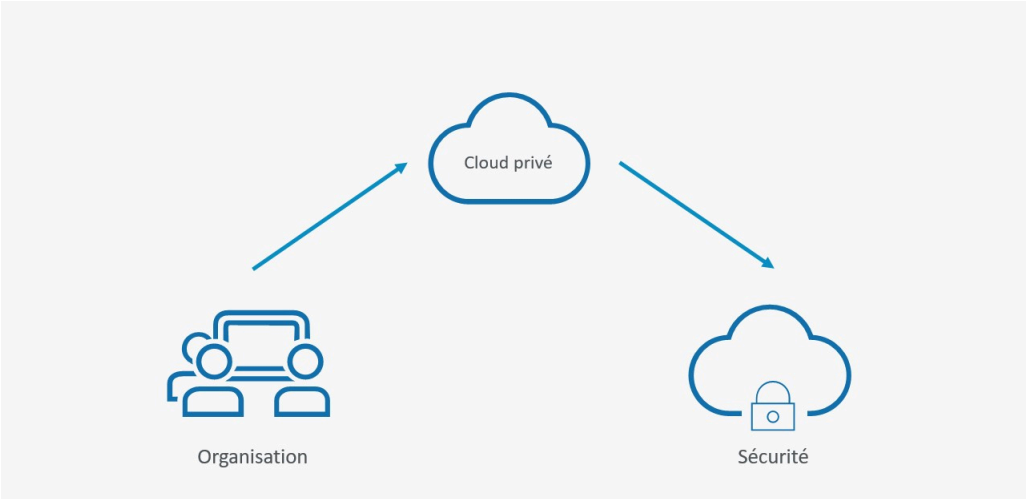
Fiche de Présentation Cloud Privé et Cloud Public

LOOTEN Axel

Cloud Privé :

Définition : Un cloud privé est un **modèle de déploiement de cloud computing dans lequel toutes les ressources cloud sont dédiées à un seul client ou une seule organisation utilisateur**.

- Une seule organisation gère et fournit l'infrastructure informatique sur le réseau pour un usage interne.
- Il n'est pas possible de répliquer la portée et l'échelle du cloud public dans un cloud privé. La qualité et la variété des infrastructures sont limitées.
- L'organisation est responsable de la sécurité de l'infrastructure matérielle et logicielle, ainsi que des données et des applications.
- Requiert des technologies complexes et une expertise informatique considérable.
- Investissement initial élevé dans les licences matérielles et logicielles. Coûts permanents élevés pour la maintenance, la sécurité et les mises à niveau de l'infrastructure.



Cloud Public:

Définition : Le cloud public est un type de calcul dans lequel les ressources sont proposées par un fournisseur tiers via Internet, et sont partagées par les organisations et les personnes qui souhaitent les utiliser ou les acheter.

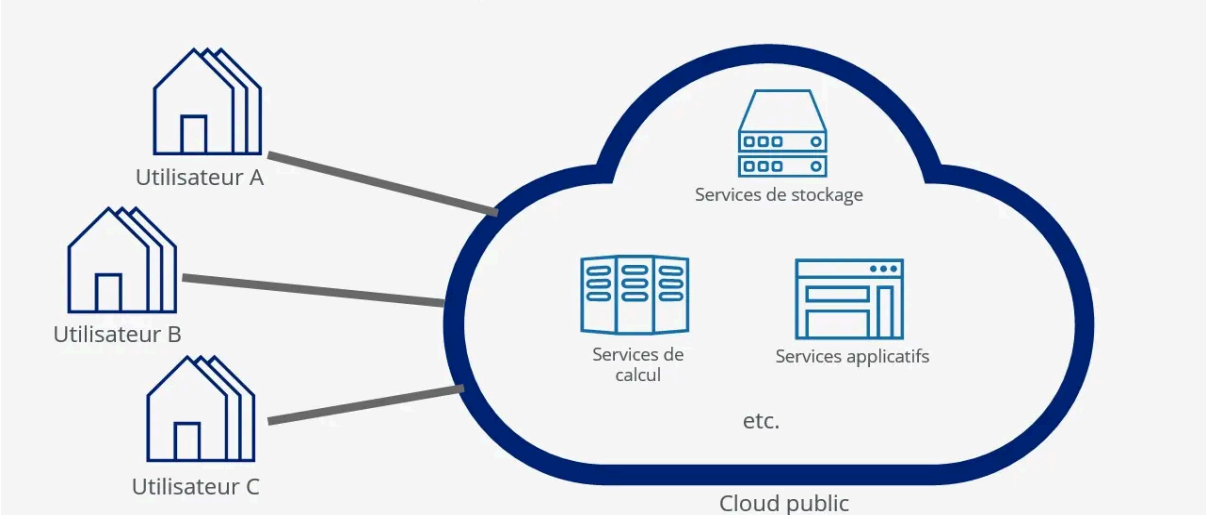
- Un fournisseur cloud gère et fournit l'infrastructure informatique sur le réseau pour un usage externe.

- Les capacités de mise à l'échelle, la variété et la qualité des ressources sont très élevées.

- Le fournisseur cloud est responsable de la sécurité de l'infrastructure physique et virtuelle. L'utilisateur est responsable de la sécurité de ses données et applications.

- Directe, à l'aide d'appels d'API ou de quelques clics sur l'interface utilisateur graphique.

- Aucun coût initial. Potentiellement gratuitement pendant une période ou une plage d'utilisation limitée. Faibles coûts permanents en fonction de l'utilisation exacte grâce aux économies d'échelle.



Les différente manières de « consommer » des services cloud :

LaaS : Infrastructure-as-a-Service, est la solution la plus proche d'une infrastructure sur site. Les services d'infrastructure, tels que le stockage et la virtualisation, sont fournis par un tiers lorsque vous en avez besoin par l'intermédiaire d'un cloud sur Internet. Ces services sont facturés selon votre utilisation

PaaS : Platform-as-a-Service, s'éloigne un peu plus de la gestion d'infrastructure entièrement sur site. Le fournisseur héberge le matériel et les logiciels sur sa propre infrastructure et met à disposition de l'utilisateur une plateforme via Internet, sous la forme d'une solution intégrée, d'une pile de solutions ou d'un service

SaaS : Services d'applications cloud, est la forme la plus globale des services de cloud computing. Il fournit une application complète gérée par un fournisseur par l'intermédiaire d'un navigateur web.

Caractéristiques	Ce que fournit le fournisseur	Ce que gère l'utilisateur / client	Ce que ne gère pas le client	À qui s'adresse le modèle
IaaS	Infrastructure (serveurs, stockage, virtualisation, réseau)	Infrastructure	c'est le fournisseur qui s'en charge	Scénarios flexibles : environnements de dev/test dynamiques, besoin de contrôle fin de l'infrastructure, infrastructures personnalisées.
PaaS	Plateforme complète (matériel + OS + environnement de dev + services de base) sur le cloud	Le code de l'application, la logique métier, les données de l'application	Gestion de l'infrastructure, des serveurs, du virtualisation, des middleware ou runtime	Développement et déploiement d'applications sans s'occuper de l'infrastructure. Pratique pour les équipes de dev, les start-ups, les projets nécessitant rapidité et simplicité.
SaaS	Application complète prête à l'emploi, hébergée et maintenue par le fournisseur	Usage de l'application (fonctionnalités), données utilisateurs éventuellement	Serveurs, infrastructure, maintenance logicielle, mises à jour, installation tout est géré par le fournisseur	Utilisateurs finaux, petites ou moyennes entreprises, cas où l'on veut éviter toute gestion IT

Etude de Dell Technologies Global Data Protection Index :

Présentation : Dell Technologies Global Data Protection est un logiciel qui protège les charges applicatives modernes dans les environnements sur site, virtuels et multi cloud, y compris dans le Cloud et les applications Cloud natives.

Selon leurs dernier rapport en moyenne les pertes de données et les interruptions de services non planifiées ont coûté 2,61 millions de dollars aux entreprises
dans le monde et cela pour des incidents d'indisponibilité d'en moyenne 26 heures et une moyenne de perte de donné près de 2,45 téraoctets (To) .

Je pense que ces chiffres sont très élevés, mais ils sont logiques.
Aujourd'hui, presque toute l'activité d'une entreprise dépend de l'informatique : sites web, logiciels internes, données clients, commandes, production, etc.
Si les systèmes sont bloqués pendant plus d'une journée pour une entreprise cela pourrait poser un réelle problème car pendant que le système est bloquer l'entreprise ne peut plus vendre son produit et perd aussi de la réputation auprés de c'est client qui ne pourais plus effectuer leurs achat chez eux pendant une durée de 26h .

Les entreprises pourraient compenser leurs pertes en mettant en place des meilleures solutions de sauvegarde des données ainsi que renforcer leurs sécurité et choisir une solution qui est réellement adaptée à leurs besoins.

Comment se prémunir des conséquences des pannes majeures et des cyberattaques :

PCA : Plan de **C**ontinuité **d'A**ctivité

Le PCA est un ensemble de mesures mises en place par une entreprise pour assurer le maintien de ses activités essentielles, même en cas de panne, d'incident majeur ou de cyberattaque.

PRA : Plan de **R**eprise d**'A**ctivité

Le PRA est un plan qui permet de relancer les systèmes informatiques et le fonctionnement normal après un incident.
Il intervient après la panne ou l'attaque, une fois que le problème est maîtrisé.

Exemple d'application pour le PCA :

Identifier les services / fonctions critiques : lister ce qui est indispensable (base de données, réseau, applications métier…) pour prioriser les efforts en cas d'incident.

Bascule automatique ou manuelle vers le secours : des mécanismes de bascule (failover) si le site principal tombe — pour que l'impact soit invisible ou minimal.

Procédures de crise documentées + rôles clairement définis : savoir qui fait quoi, comment alerter, comment communiquer, etc.

Moyens d'accès alternatifs : accès distant sécurisé (VPN, cloud), matériel de secours, etc., pour permettre la continuité même si le site physique est indisponible.

Exemple d'application pour le PRA :

Sauvegardes régulières + restauration testée : sauvegarder les données, les configurations, les serveurs, et tester régulièrement la restauration pour s'assurer que tout fonctionne en cas de besoin.

Définition d'objectifs RTO / RPO : fixer le temps maximum d'indisponibilité acceptable (RTO) et la perte maximale de données tolérables (RPO). Ces indicateurs guident la stratégie de restauration.

Procédure de redémarrage documentée : liste des étapes à suivre, ordre de redémarrage des services, responsabilités, vérifications, etc.
Utilisation d'une infrastructure de secours ou cloud distant : héberger les sauvegardes ou les services critiques sur un site externe, cloud, ou infrastructure distante pour pouvoir relancer rapidement.