TD Cloud - Romain

1. Différencier cloud privé et cloud public.

I - Le cloud public est un environnement cloud basé sur une infrastructure appartenant à un fournisseur tiers (ex. Microsoft Azure, AWS, Google Cloud).
Ce modèle repose sur le partage des ressources (serveurs, stockage, réseau) entre plusieurs utilisateurs ou entreprises via Internet.
Les utilisateurs accèdent aux services via un navigateur, et ce type de cloud est souvent utilisé pour des services comme la messagerie, le stockage en ligne, ou des environnements de développement et de test.
Tout le matériel et l'infrastructure sous-jacente sont gérés par le fournisseur.

II - Avantages des clouds publics :

- Coûts inférieurs : vous n'avez pas besoin d'acheter du matériel ou des logiciels, et vous payez uniquement le service que vous utilisez.
- Absence de maintenance : votre fournisseur de services assure la maintenance.
- Haute fiabilité : un vaste réseau de serveurs offre une garantie contre les pannes.
- Facile à mettre en place : toute l'infrastructure est gérée par le fournisseur donc l'entreprise n'a pas à s'en soucier.

III - Inconvénients des clouds publics

- Sécurité : La connexion par l'Internet public peut poser des risques de sécurité.
- Limite des paramètres : L'entreprise est dépendante du fournisseur du service cloud pour le paramétrage.
- Autonomie : Une moins grande autonomie qu'avec un cloud privé.

TD Cloud - Romain

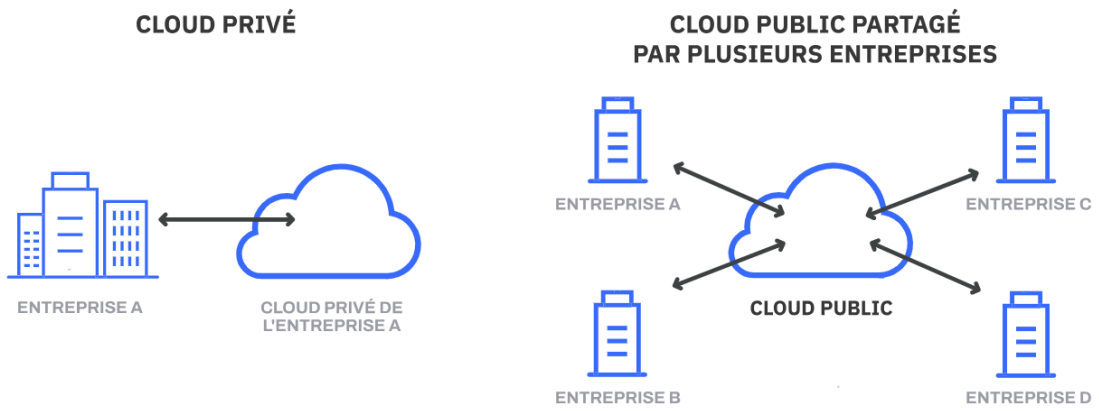
I - Un cloud privé est un environnement cloud réservé à un seul utilisateur ou organisation. Hébergé soit en interne (dans le datacenter de l'entreprise) soit chez un prestataire tiers, il garantit un accès exclusif et sécurisé. Le matériel et les logiciels sont dédiés, et la maintenance est réalisée sur un réseau privé. Ce modèle, offrant un contrôle maximal et une personnalisation poussée, est privilégié par des secteurs sensibles comme les administrations publiques ou les banques, où la sécurité et la confidentialité des données sont prioritaires.

II - Avantages d'un cloud privé :

- Personnalisation accrue : l'entreprise peut facilement personnaliser son environnement cloud pour répondre à des besoins métier spécifiques.
- Contrôle et Sécurité accrus : les ressources n'étant pas partagées, des niveaux supérieurs de contrôle et de confidentialité sont possibles.
- Évolutivité accrue : il est plus facile d'adapter la quantité de ressources selon les besoins.

III - Inconvénients d'un cloud privé :

- Prix : Les coûts sont souvent plus élevés que pour un cloud public.
- Main d'œuvre : La nécessité de posséder en interne les compétences nécessaires, si l'entreprise veut être totalement autonome pour la gestion de son cloud.



Cloud Privé : Privé vs Public

TD Cloud - Romain

2. Fusion du cloud privé et public

On nomme "cloud hybride" la combinaison du cloud public et privé. Grâce à ce modèle, les entreprises peuvent profiter des avantages des deux types de cloud, en combinant les infrastructures de cloud public et privé. Les différents environnements sont reliés entre eux grâce à une technologie qui facilite le transfert de données et d'applications. Une partie des données est stockée dans un cloud privé, ce qui garantit une sécurité accrue, tandis qu'une autre partie, moins importante, est stockée dans un cloud public, ce qui permet une grande souplesse et des coûts plus abordables.

Au lieu de devoir acheter, programmer et gérer des ressources et des équipements supplémentaires qui pourraient rester inutilisés pendant de longues périodes, les entreprises ne paient que les ressources qu'elles utilisent à un moment donné.

Les enjeux du cloud hybrid :

- La sécurité : Les données doivent être protégées lors de leur transfert entre les deux environnements.
  Les entreprises doivent également séparer les données les moins critiques des données sensibles pour que ces dernières ne transitent pas entre les deux environnements.

- Les coûts : Avec le cloud hybride, il est possible d'adapter la quantité de ressources en fonction des besoins.
  Cependant, le suivi des coûts peut être complexe à cause des modèles tarifaires des fournisseurs de cloud publics et des investissements dans l'infrastructure privée.

- La continuité : En cas de panne de l'un des environnements, l'autre peut servir de secours. Il faut pour cela mettre en place un plan de reprise d'activité efficace pour utiliser au mieux les deux infrastructures.

TD Cloud - Romain

3. IaaS, PaaS, SaaS

I - IaaS (Infrastructure-as-a-Service)

L'IaaS, ou Infrastructure-as-a-Service, est la solution la plus proche d'une infrastructure sur site.

L'utilisateur est responsable du système d'exploitation ainsi que des données, des applications, des solutions de middleware et des environnements d'exécution.

Le fournisseur du service, quant à lui, gère le réseau, les serveurs, les fonctions de virtualisation ainsi que le stockage, et vous y donne accès en fonction de vos besoins.
L'utilisateur n'a pas à assurer la maintenance ni la mise à jour de son propre datacenter sur site, car le fournisseur le fait pour lui.

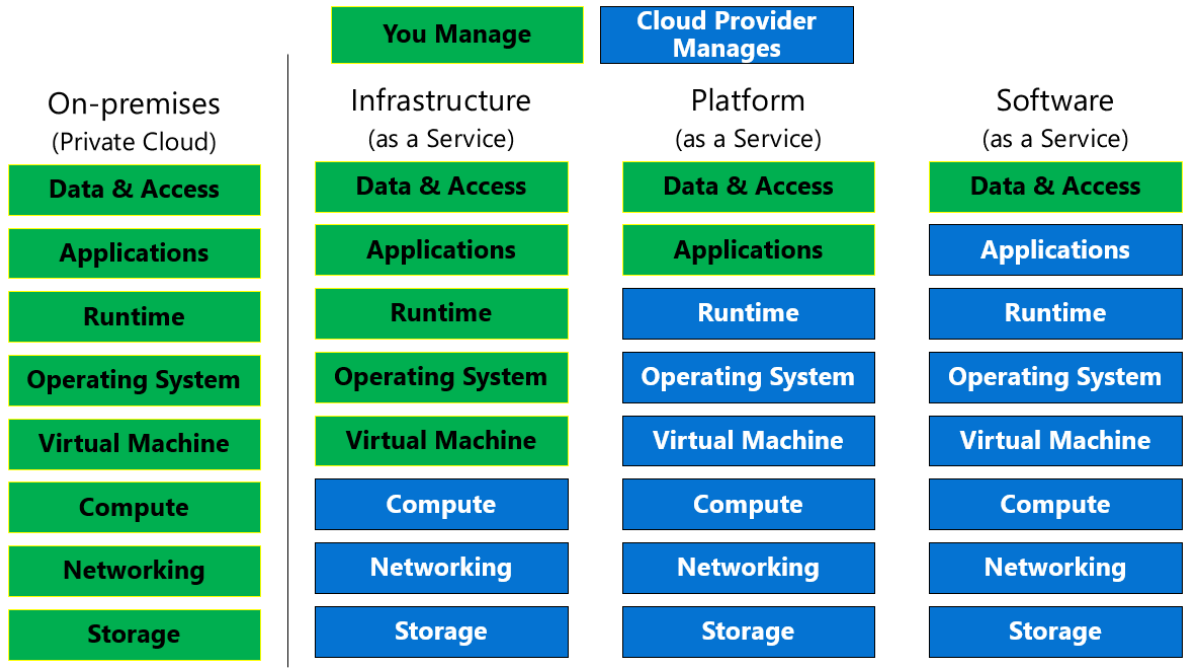
II - PaaS (Platform-as-a-Service)

Le modèle PaaS, ou 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.
Le PaaS permet aux développeurs de créer un framework qui leur sert de base pour développer et personnaliser leurs applications basées sur le Web. Les développeurs peuvent utiliser les composants logiciels intégrés pour créer leurs applications, et ainsi limiter la quantité de code qu'ils doivent écrire eux-mêmes.

TD Cloud - Romain

III - SaaS (Software-as-a-Service)

Le SaaS (Software-as-a-Service), ou 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.
Les mises à jour logicielles, l'application des correctifs et les autres tâches de maintenance logicielle sont gérées par le fournisseur pour le compte de l'utilisateur, qui peut se connecter à l'application à l'aide d'un tableau de bord ou d'une API.
Aucun logiciel n'est installé sur les machines de l'entreprise et l'accès au programme est plus fluide et plus fiable.
Bien qu'il vous fasse gagner du temps et limite les opérations de maintenance, le modèle SaaS réduit le niveau de contrôle et peut nuire à la sécurité et aux performances.



TD Cloud - Romain

4. VPS

Un VPS (ou Virtual Private Server) est une méthode de partitionnement d'un serveur en plusieurs serveurs virtuels indépendants qui ont chacun les caractéristiques d'un serveur dédié, en utilisant des techniques de virtualisation.
Chaque serveur peut fonctionner avec un système d'exploitation différent et redémarrer indépendamment.

Le VPS fait plus référence au cloud public car le VPS est proposé par un fournisseur comme pour le cloud public. De plus, le fournisseur partage les ressources d'un serveur physique en plusieurs serveurs virtuels comme pour le cloud public. Enfin, l'accès au VPS se fait par internet de la même manière que pour un cloud public.

5. VPS et IaaS

Un VPS ressemble à de l'IaaS parce qu'il fournit un environnement virtualisé avec des ressources dédiées, mais il est différent dans son niveau de flexibilité et dans les services qu'il propose.

Avec un VPS, l'utilisateur reçoit un serveur virtualisé dans un environnement prédéfini et limité par des ressources fixes (RAM, stockage). Le contrôle s'étend principalement au niveau du système d'exploitation, mais pas au reste l'infrastructure.
De plus, un VPS est une bonne solution pour des besoins fixes, mais il ne permet pas une augmentation dynamique des ressources.
Enfin, un service de VPS ne fournit que le serveur virtualisé.

L'IaaS, en revanche, fournit une infrastructure complète, y compris la gestion des réseaux, du stockage, et des instances virtualisées, avec des options de personnalisation et de configuration plus avancées.
L'IaaS permet de faire évoluer ou réduire les ressources à la demande, rendant cette solution adaptée aux projets dynamiques et fluctuants.
Les solutions IaaS incluent des outils et des services supplémentaires, comme la gestion DNS, la régulation du trafic, les pare-feu, la surveillance des performances, et des services d'orchestration pour simplifier l'intégration avec d'autres composants.

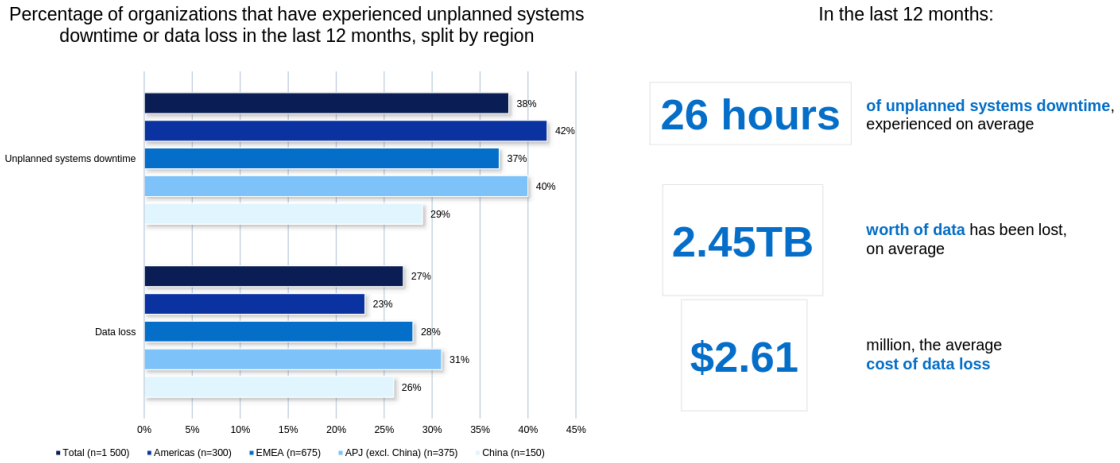
Le VPS est donc une sous-catégorie simplifiée d'IaaS.

TD Cloud - Romain

6. Dell Technologies Global Data Protection Index

En moyenne, en 2024, les entreprises ont subi 26 heures de downtime non prévus. Durant ces downtimes, 2.45 Tera de données ont été perdues occasionnant 2,61 millions de dollars de perte.

Data loss has not only contributed to disruption, but has also impacted the bottom line



Ces chiffres me paraissent étonnamment bas. En effet, lors du précédent TD, nous avons vu le cas de downtime de 48h. Cela signifie donc que de nombreuses entreprises n'ont pas eu le moindre downtime. Cependant le volume de données est impressionnant.

Pour compenser ces pertes les entreprises peuvent :

- communiquer rapidement sur le problème. Une grande transparence peut permettre de garder la confiance des clients.
- faire une analyse des dégâts et des pertes afin d'avoir un bilan et d'identifier la source du problème. Cela permettra à l'entreprise de prévenir ou au moins de limiter les prochaines pannes.
- tenter de récupérer un maximum de données ? (les données encore exploitables)

TD Cloud - Romain

7. PCA et PRA

En informatique, un plan de continuité d'activité (PCA), a pour but de garantir la survie de l'entreprise en cas de sinistre important touchant le système informatique. Il s'agit de redémarrer l'activité le plus rapidement possible avec le minimum de perte de données. Ce plan est un des points essentiels de la politique de sécurité informatique d'une entreprise.

Un plan de reprise d'activité (PRA) est un ensemble de procédures qui permettent à une entreprise de prévoir par anticipation, les mécanismes pour reconstruire et remettre en route un système d'information en cas de sinistre important ou d'incident critique.
En cas de sinistre, Le PRA permet de reconstruire les serveurs en leur affectant les données répliquées et ainsi de redémarrer les applications sous quelques minutes ou quelques heures, suivant les solutions retenues.

(Le PCA opère en 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.

Quant à lui, le PRA intervient seulement une fois que le sinistre a eu lieu.)

Mesures concrètes dans un PCA :

- Avoir plusieurs infrastructures pour pouvoir prendre le relais si l'une tombe en panne
- Faire des copies régulières des données pour limiter au maximum les pertes lors d'une panne.
- Mettre en place un système pour prévenir les clients et les collaborateurs pour les tenir informés de la panne.
- Avoir une solution pour que les employés puissent continuer à travailler même lors d'une panne.

TD Cloud - Romain

Mesures concrètes dans un PRA :

- Simuler des pannes pour s’assurer que le restauration des données est réalisable rapidement.
- Avoir un plan précis et de la documentation pour remettre en route toute l’infrastructure après la panne.
- Avoir des copies sur des supports physiques pour les données les plus importantes
- Prévoir de la main d’oeuvre ou des contacts pour remettre en place l’infrastructure après la panne