Cloud privé, cloud public

Lors de la réalisation de votre travail sur le rétablissement d'un service, vous avez pu remarquer l'un des risques du cloud : l'indisponibilité imprévisible et incontrôlable d'un service informatique. C'est l'un des risques de l'externalisation : on perd la main sur tout ou partie du processus de mise en disponibilité, ce qui peut occasionner à terme, en cas de panne majeure, des pertes de données et des pertes financières énormes pour les entreprises impactées, qu'elles soient fournisseurs de services cloud ou bien clientes de ces dernières.

1. Différenciez cloud privé et cloud public. Argumentez sur les différences, les points positifs et négatifs de chacune des deux solutions et illustrez-les à l'aide de schémas d'infrastructure simples.

	Cloud Privé	Cloud Public
Propriété	Appartient et est géré par une seule organisation.	Partagé entre plusieurs organisations.
Emplacement physique	Souvent hébergé dans le centre de données interne.	Hébergé dans des centres de données externes.
Contrôle	Contrôle total sur la configuration et la sécurité.	Moins de contrôle direct sur la configuration.
Personnalisation	Grande personnalisation possible.	Limitée en raison de la mutualisation des ressources.
Évolutivité	L'évolutivité peut être limitée.	Évolutivité élevée, capacité à augmenter/diminuer.
Coût	Généralement plus coûteux en raison de la médication.	Souvent plus économique en raison de la mutualisation.
Avantage	Contrôle totale sur le cloud	sécurité et autre géré par une organisation externe Le coût, évolutivité
Inconvénient	Nécessite d'avoir ou de faire appel à un technicien pour faire cette infrastructure. Plus coûteux	Contrôle limité par l'hébergeur

2. Les SI tendent aujourd'hui à évoluer vers une fusion du cloud privé et public. De quoi est-il alors question et quels sont les enjeux de ce nouveau type de cloud ?

La fusion du cloud privé et public est appelée cloud hybride. Cela permet aux entreprises d'avoir des avantages des deux modèles. Les enjeux sont la flexibilité, pour ajuster rapidement et efficacement les ressources informatiques en fonction des besoins changeants de l'entreprise tels que déployer de nouveaux services, d'ajuster la capacité de stockage, ou de modifier la configuration du réseau de manière agile.

La scalabilité et une meilleure optimisation des coûts en utilisant le cloud public pour des charges de travail temporaires et le cloud privé pour des données sensibles nécessitant un contrôle accru.

3. Il existe plusieurs manières de « consommer » des services cloud. Expliquez les notions **IaaS**, **PaaS** et **SaaS** et différenciez-les à l'aide d'un tableau ou d'un schéma

	IaaS (Infrastructure as a Service)	PaaS (Platform as a Service)	SaaS (Software as a Service)
Description	Fournit une infrastructure informatique virtuelle (serveurs, stockage, réseau).	Offre une plateforme de développement complète sans se soucier de l'infrastructure sous-jacente.	Fournit des applications logicielles accessibles en ligne sans nécessiter d'installation.
Exemples	Amazon Web Services (AWS), Microsoft Azure	Google App Engine, Heroku	Salesforce, Google Workspace

4. Définissez le terme VPS et indiquez s'il fait plutôt référence au cloud privé ou bien au cloud public ? Pour quelle raison ?

VPS qui veut dire Virtual Private Server fait référence au cloud privé.C'est une machine virtuelle créée sur une infrastructure de cloud privé, offrant davantage de contrôle et de personnalisation par rapport au cloud public.

5. Expliquez précisément en quoi un VPS qui ressemble pourtant à de l'IaaS n'en est pourtant pas vraiment.

Bien que les VPS ressemblent à de l'IaaS, la principale différence réside dans le niveau de virtualisation. Les VPS partagent souvent la même infrastructure physique, ce qui peut entraîner une certaine dépendance vis-à-vis du matériel sous-jacent. En IaaS, les ressources sont complètement virtualisées et isolées.

6. Recherchez ce qu'est le **Dell Technologies Global Data Protection Index** et consultez leur dernier rapport pour l'année 2021. Cherchez dans ce rapport combien, en moyenne, les pertes de données d'une part et les interruptions de services non planifiées d'une autre part ont coûté aux entreprises dans le monde en 2021. Que pensez-vous de ces chiffres ? Comment les entreprises peuvent, selon-vous, compenser ces pertes ?

Le Dell Technologies Global Data Protection Index est une enquête et un rapport réalisés par Dell Technologies pour évaluer l'état de la protection des données dans les entreprises à l'échelle mondiale.

En 2021, en moyenne, les pertes de données ont coûté aux entreprises 3,86 millions de dollars et les interruptions de services non planifiées ont coûté 4,24 millions de dollars. Pour compenser ces pertes, les entreprises peuvent investir dans des solutions de sauvegarde, de reprise après sinistre, et renforcer leurs protocoles de sécurité pour minimiser les risques.

7. Pour se prémunir des risques de pannes majeures, les entreprises sont censées avoir adopté un **Plan de Continuité d'Activité (PCA)** ou le cas échéant, au moins un **Plan de Reprise d'Activité (PRA)**. Définissez ces termes et donnez des exemples de mesures concrètes pouvant être mises en place dans chacun des deux plans.

- PRA (Plan de Reprise d'Activité): vise à restaurer les activités normales après une perturbation. Mesures: stratégies de reprise après sinistre, systèmes redondants, formation du personnel. Ces plans contribuent à minimiser les temps d'arrêt et à assurer la résilience de l'entreprise face aux interruptions

- PCA (Plan de Continuité d'Activité): vise à garantir la continuité des activités essentielles pendant et après une perturbation. Mesures: sauvegarde régulière des données, plans de sauvegarde, sites de secours.