

Mise en place de PRA/PCA

1. Différenciation entre cloud privé et cloud public :

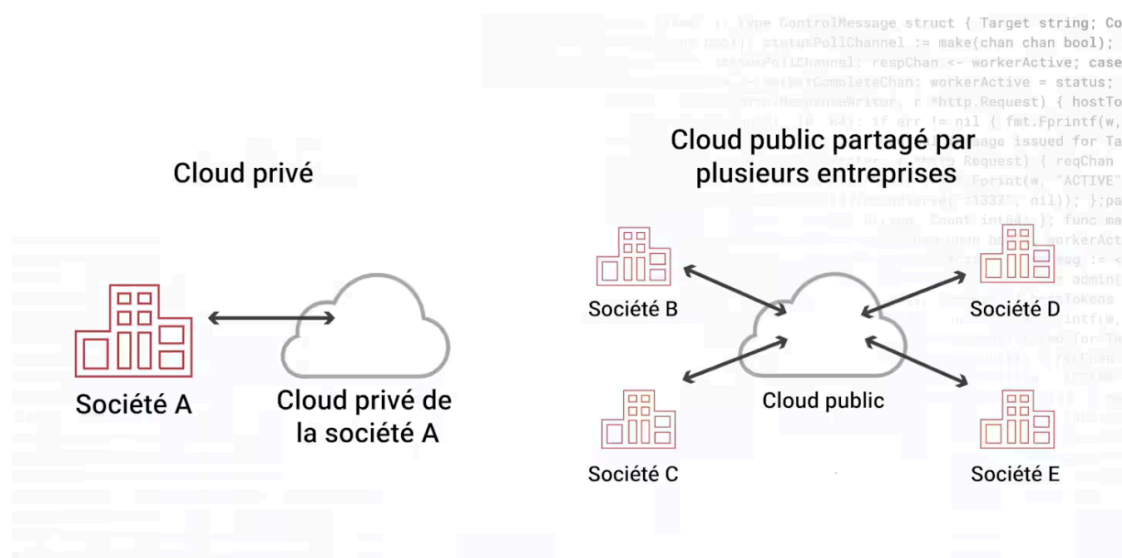
CLOUD PRIVÉ :

- Cloud privé : Un cloud privé est comme un espace informatique spécial réservé à une seule entreprise. Cette entreprise possède et contrôle tout cet espace, qui peut être situé sur ses propres ordinateurs (sur site) ou dans un centre de données qui lui est dédié. Cela donne à l'entreprise un contrôle total sur son espace informatique, elle peut le personnaliser selon ses besoins et renforcer la sécurité. Cependant, cela peut coûter cher au départ, et il pourrait être un peu difficile d'ajuster la taille de cet espace rapidement.

CLOUD PUBLIC :

- Cloud public : Un cloud public, c'est comme louer de l'espace informatique sur Internet. Ce "terrain" numérique est géré par une entreprise tierce et utilisé par plusieurs entreprises différentes. Les points positifs sont que c'est rapide à mettre en place, on peut l'ajuster facilement selon les besoins, et ça coûte moins cher. Cependant, on ne peut pas le personnaliser autant qu'on le voudrait, et il peut y avoir des inquiétudes concernant la sécurité et les règles à respecter.

SCHÉMA ILLUSTRANT LES DIFFÉRENCES :



2. Fusion du cloud privé et public (Cloud hybride) :

La fusion du cloud privé et public, également appelée cloud hybride, vise à combiner les avantages des deux solutions. Les enjeux de cette approche sont la flexibilité, la capacité à étendre des charges de travail vers le cloud public lorsque nécessaire, la réduction des coûts, et une meilleure continuité opérationnelle. Cela permet aux entreprises de conserver le contrôle sur les données sensibles tout en profitant de la scalabilité et de la diversité des services du cloud public.

3. Notions IaaS, PaaS et SaaS :

L'IaaS:

- L'IaaS, ou Infrastructure en tant que Service, offre une sorte de "location virtuelle" d'équipements informatiques. Cela inclut des serveurs, des espaces de stockage et des réseaux, que les utilisateurs peuvent utiliser comme un service. En général, les clients de l'IaaS sont responsables de la gestion des systèmes d'exploitation, des applications et des données, tandis que l'entreprise qui fournit l'IaaS s'occupe de l'infrastructure physique sous-jacente. C'est un peu comme louer des ordinateurs virtuels et du matériel en ligne, tout en gardant le contrôle sur ce que vous faites avec ces ressources.

Le PaaS:

- Le PaaS, ou Plateforme en tant que Service, fournit une sorte de terrain de jeu prêt à l'emploi pour les développeurs. Cela inclut non seulement les outils pour construire des applications, mais aussi les services nécessaires comme les bases de données. Les clients qui utilisent le PaaS peuvent se concentrer entièrement sur le développement de leurs applications, sans avoir à se préoccuper de la gestion détaillée de l'infrastructure sous-jacente. C'est comme disposer d'un atelier entièrement équipé avec tout le nécessaire pour construire quelque chose, sans avoir à se soucier de la propriété et de la maintenance de l'atelier lui-même.

Le SaaS :

- Le SaaS, ou Logiciel en tant que Service, offre des applications informatiques complètes comme un service. Au lieu de télécharger et d'installer un logiciel sur votre ordinateur, vous pouvez accéder à ces applications directement via un navigateur web. Ce service gère non seulement le logiciel lui-même, mais aussi toute l'infrastructure nécessaire à son fonctionnement. Les clients utilisent simplement l'application sans avoir à se soucier de l'installation, de la maintenance ou de l'arrière-plan technique. C'est un peu comme utiliser un programme directement en ligne, sans vous préoccuper de son installation ou de sa mise à jour sur votre propre ordinateur.

TABLEAU DE DIFFÉRENCIATION :

	IaaS	PaaS	SaaS
Gestion de l'OS	Client	Fournisseur	N/A
Gestion des apps	Client	Client	Fournisseur
Scalabilité	Oui	Oui	Limitée
Exemples	Amazon EC2, Azure VM	Google App Engine	Gmail, Office 365

4. VPS (Virtual Private Server) :

Un VPS :

- Un VPS, ou serveur privé virtuel, est comme un petit morceau de l'Internet que vous pouvez personnaliser selon vos besoins. Il fonctionne à l'intérieur d'un grand système informatique partagé, souvent lié au cloud public. Alors que vous pouvez le configurer comme si c'était votre propre serveur dédié, il reste en réalité sur des ressources partagées gérées par la même entreprise qui gère le cloud. C'est un peu comme avoir votre propre espace privé dans un immeuble partagé, où vous avez le contrôle sur certaines choses, mais partagez certaines ressources communes avec d'autres.

5. Différence entre VPS et IaaS :

- Alors, même si les VPS et l'IaaS semblent similaires en termes d'isolement et de personnalisation, la grande différence réside dans la gestion de l'infrastructure de base. Dans un environnement IaaS, les clients ont un contrôle plus direct sur les ressources sous-jacentes, c'est comme s'ils avaient leur propre terrain sur lequel construire. En revanche, un VPS repose toujours sur une infrastructure partagée gérée par la même entreprise qui gère le cloud. Par conséquent, bien que vous puissiez personnaliser un VPS, il y a des limites à ce que vous pouvez faire, car vous partagez les ressources avec d'autres utilisateurs. En comparaison, avec l'IaaS, vous avez une flexibilité et une personnalisation

potentiellement plus importantes, car vous avez un contrôle plus direct sur votre propre morceau d'infrastructure.

6. Dell Technologies Global Data Protection Index :

Voici les chiffres de 2021 sur les pertes de données et à l'interruption de service non planifiée pour les entreprises :

- 959493\$: Coût moyen de la perte de données au cours des 12 derniers mois (en USD)

- 513067\$: Coût moyen de l'interruption de service non planifiée des systèmes au cours des 12 derniers mois (en USD)

Pour compenser ces pertes, les entreprises peuvent mettre en œuvre plusieurs mesures :

1. Plan de Continuité d'Activité (PCA) et Plan de Reprise d'Activité (PRA) :

- Mettre en place des plans solides pour assurer la continuité des opérations en cas d'interruption.

- Établir des protocoles de récupération rapides pour minimiser les temps d'arrêt.

2. Sauvegardes Régulières :

- Mettre en œuvre des procédures régulières de sauvegarde des données critiques.

- Assurer la sécurité et la disponibilité des sauvegardes pour une récupération rapide en cas de besoin.

3. Sécurité Informatique Renforcée :

- Investir dans des solutions de sécurité avancées pour prévenir les pertes de données liées à des cyberattaques.

- Sensibiliser et former le personnel à la sécurité informatique pour réduire les risques d'incidents.

4. Redondance et Haute Disponibilité :

- Mettre en place des systèmes redondants pour assurer la disponibilité continue des services.

- Utiliser des centres de données multiples pour répartir les charges de travail et minimiser les risques.

5. Tests Réguliers :

- Effectuer des tests réguliers des plans de continuité et de reprise d'activité pour s'assurer de leur efficacité.

- Identifier et corriger les éventuelles lacunes dans les plans de manière proactive.

6. Assurance Cyber et Pertes de Données :

- Souscrire à des assurances couvrant les pertes de données et les interruptions de service pour atténuer les coûts financiers en cas d'incident.

En adoptant une approche proactive en matière de gestion des risques et en mettant en place des mesures de sécurité robustes, les entreprises peuvent réduire les risques de pertes financières liées à la perte de données et aux interruptions de service. La prévention, la préparation et la réponse rapide sont des éléments clés pour minimiser l'impact financier de tels incidents.

7. Plan de Continuité d'Activité (PCA) et Plan de Reprise d'Activité (PRA) :

PCA:

- PCA (Plan de Continuité d'Activité) : Un Plan de Continuité d'Activité (PCA) a pour objectif de s'assurer que l'entreprise puisse maintenir ses opérations essentielles même en cas d'événements majeurs perturbateurs, comme des pannes matérielles, des catastrophes naturelles, ou d'autres incidents imprévus. Pour ce faire, des mesures spécifiques sont mises en place. Cela peut inclure la duplication des systèmes (redondance), la création de sites de secours où l'entreprise peut continuer à fonctionner en cas de problème majeur, la formation du personnel pour faire face à des situations d'urgence, et la documentation claire des procédures à suivre en cas de besoin immédiat. En résumé, le PCA vise à assurer une préparation efficace et une réponse organisée face à des événements qui pourraient interrompre normalement les activités de l'entreprise.

PRA :

- PRA (Plan de Reprise d'Activité) : Un Plan de Reprise d'Activité (PRA) se focalise sur la restauration des services informatiques après une interruption, comme une panne, un sinistre, ou tout autre événement qui a stoppé temporairement les opérations. Pour accomplir cela, le PRA comprend des procédures spécifiques visant à remettre en marche les systèmes, applications et données de l'entreprise. Ces procédures peuvent inclure des activités telles que la sauvegarde et la récupération des données, la réplication des systèmes critiques pour assurer une disponibilité rapide, la planification de la reprise des activités en fonction de leur importance, et la réalisation de tests réguliers pour s'assurer que tout fonctionne correctement en cas de besoin réel. En résumé, le PRA vise à minimiser le temps d'arrêt des activités suite à une interruption en restaurant rapidement les fonctionnalités informatiques essentielles.

En combinant un PCA et un PRA, une entreprise peut renforcer sa capacité à faire face à diverses situations d'urgence, allant des pannes informatiques aux catastrophes naturelles, et assurer une reprise efficace des opérations.