

RÉSUMÉ THÉORIQUE – FILIÈRE INFRASTRUCTURE DIGITALE

M207 - Établir une stratégie de maintien d'un SI dans un Cloud propriétaire en ligne public

45 heures

SOMMAIRE



1. REPRENDRE UNE ACTIVITE APRÉS SINISTRE SUR LE CLOUD
   - Identifier les mécanismes de récupération
   - Appréhender le concept de Multi-Cloud
2. RÉPLIQUER UNE ACTIVITÉ SUR LE CLOUD
   - Créer des plans de récupération
   - Appliquer la géo-réplication
3. MIGRER LE SI DANS LE CLOUD
   - Identifier les stratégies de migration du SI dans le Cloud
   - Adopter une approche DevOps

MODALITÉS PÉDAGOGIQUES



1

LE GUIDE DE SOUTIEN

Il contient le résumé théorique et le manuel des travaux pratiques



2

LA VERSION PDF

Une version PDF est mise en ligne sur l'espace apprenant et formateur de la plateforme WebForce Life



3

DES CONTENUS TÉLÉCHARGEABLES

Les fiches de résumés ou des exercices sont téléchargeables sur WebForce Life



4

DU CONTENU INTERACTIF

Vous disposez de contenus interactifs sous forme d'exercices et de cours à utiliser sur WebForce Life

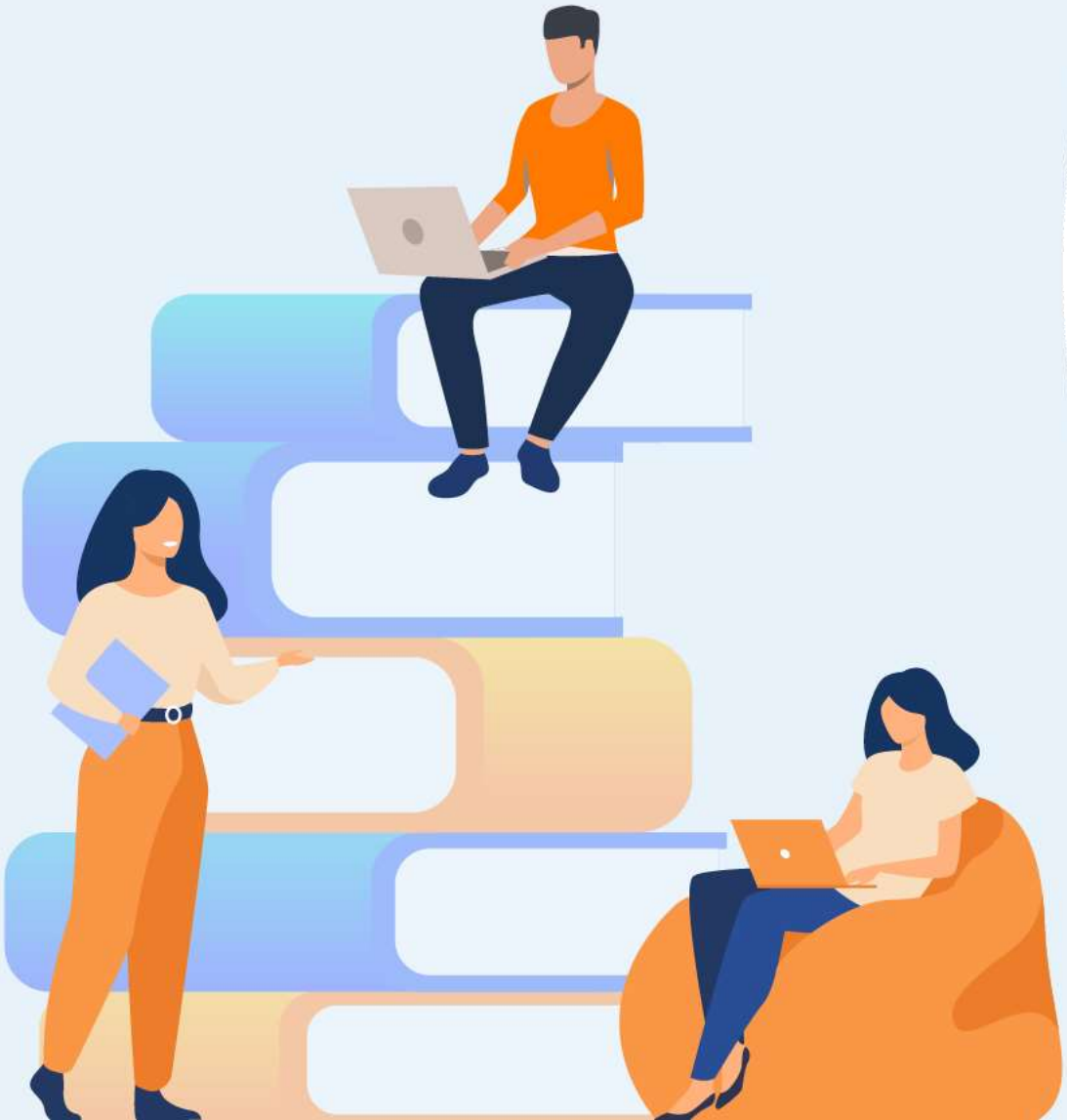


5

DES RESSOURCES EN LIGNES

Les ressources sont consultables en synchrone et en asynchrone pour s'adapter au rythme de l'apprentissage

Copyright - Tout droit réservé - OFPPT



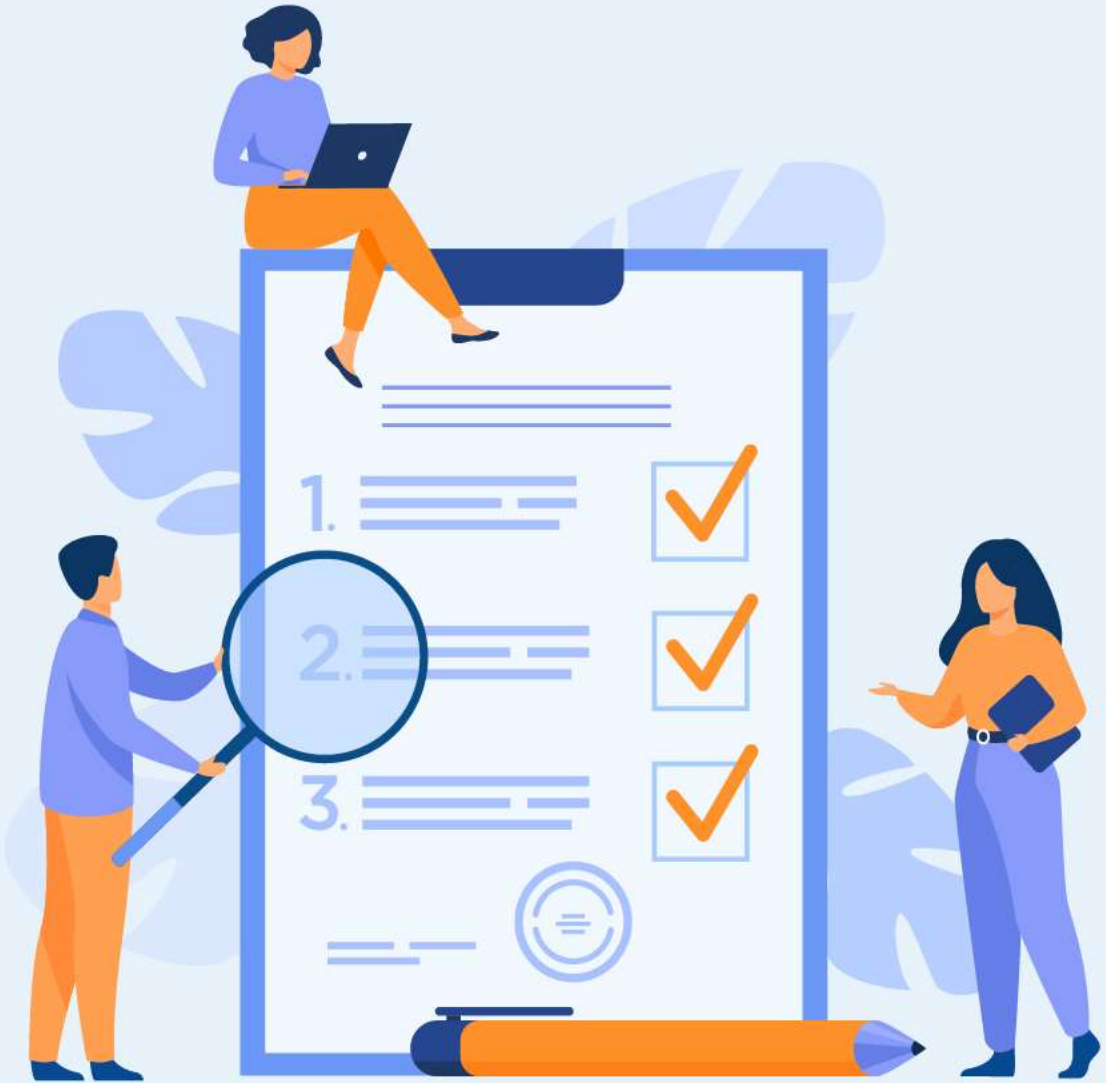
PARTIE 1

REPRENDRE UNE ACTIVITE APRÉS SINISTRE SUR LE Cloud

Dans ce module, vous allez :

- Identifier les mécanismes de récupération
- Appréhender le concept de Multi-Cloud

13,5 heures



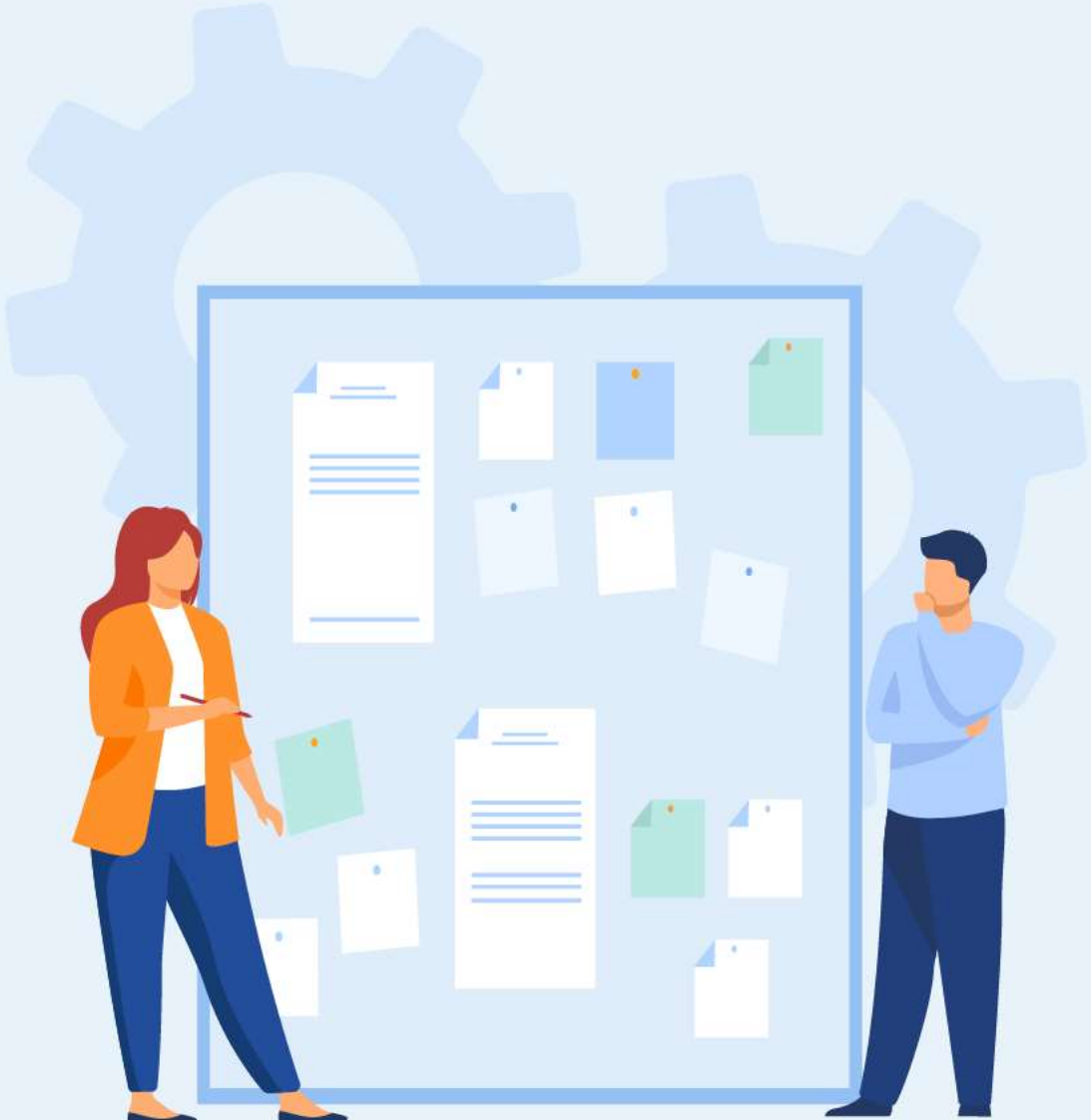
CHAPITRE 1

Décrire les mécanismes de récupération

Ce que vous allez apprendre dans ce chapitre :

- Connaitre l’objectif de point de récupération (RPO)
- Connaitre l’objectif de temps de récupération (RTO)
- Mettre en place un plan de reprise d’activité (RPA)
- Mettre en place un plan de continuité d’activité (PCA)

8 heures



CHAPITRE 1

Décrire les mécanismes de récupération

1. **Connaitre l’objectif de point de récupération (RPO)**
2. Connaitre l’objectif de temps de récupération (RTO)
3. Mettre en place un plan de reprise d’activité (RPA)
4. Mettre en place un plan de continuité d’activité (PCA)

PARTIE 1

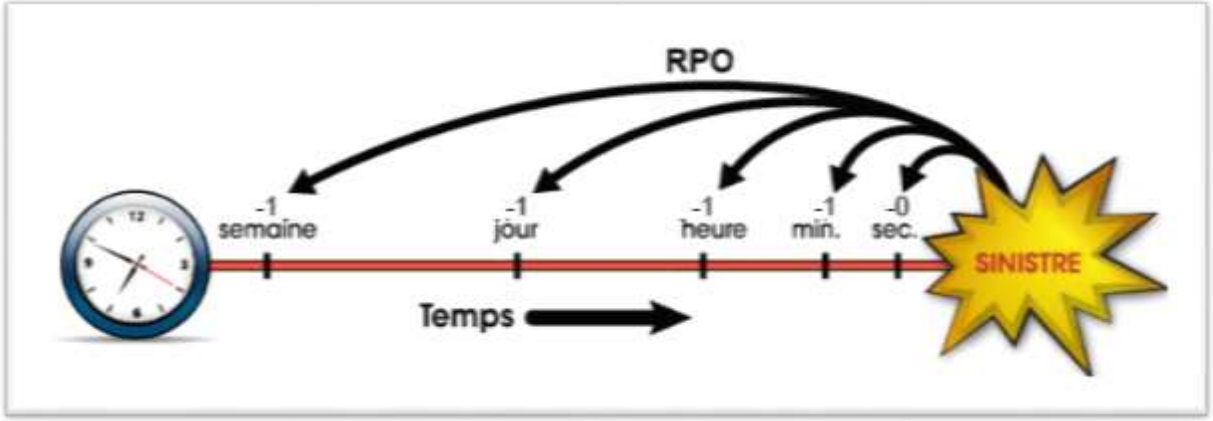
Définition de la RPO (Recovery Point Objective)

L'objectif de point de récupération (**RPO**) est la quantité maximum acceptable de perte de volume/données après un incident non planifié, exprimé à temps. On considère généralement qu'il s'agit de la date antérieure à l'événement pour laquelle les données peuvent être récupérées avec succès, c'est-à-dire le temps écoulé depuis la plus récente sauvegarde fiable.

Dans la plupart des systèmes de gestion du Cloud, les données sont capturées et stockées régulièrement grâce à une certaine forme de protection des données. Le point de récupération désigne la dernière fois que les données ont été capturées. En cas de défaillance d'un système, celui-ci peut être restauré uniquement au point de récupération le plus récent.

Si un système a un objectif de point de récupération mesuré en heures ou en jours, une défaillance du système entraînerait la perte de données pour ces heures ou jours entre le dernier point de récupération et la panne. Un objectif de point de récupération d'un jour entraînerait théoriquement la perte de toutes les transactions de la journée précédant la défaillance.

Pour les systèmes stratégiques, l'utilisation d'un RPO mesuré en minutes ou en secondes peut être plus appropriée pour éviter une perte de revenus. Toutefois, un RPO plus court entraîne généralement une augmentation des coûts de gestion globaux.

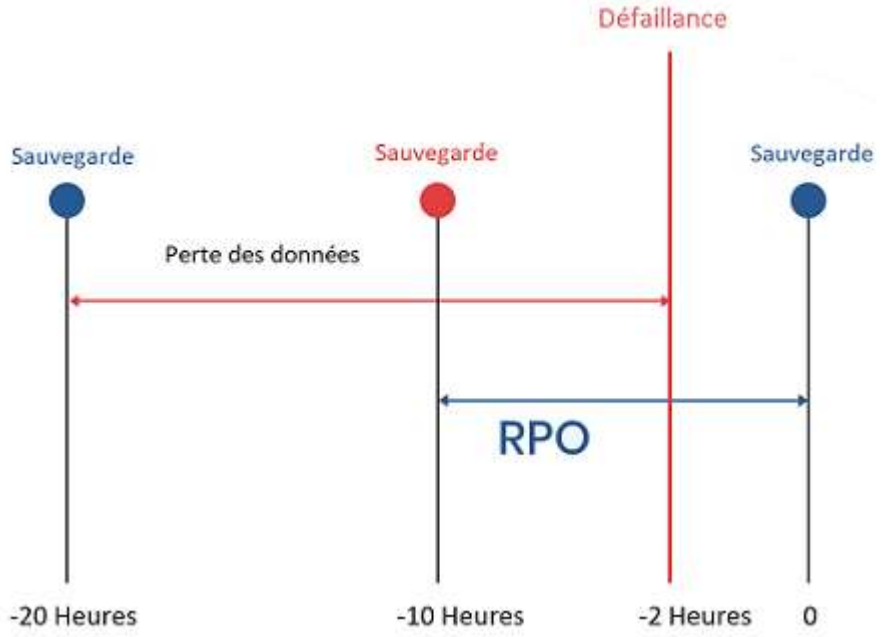


Copyright - Tout droit réservé - OFPPT

Exemple de RPO

Lorsqu'un sinistre survient et que la copie de sauvegarde la plus récente des données remonte à 8 heures et que le RPO standard pour l'entreprise est de 10 heures, nous sommes toujours dans la limite du RPO tel que spécifié dans le BCP (Le plan de continuité des activités).

Dans ce cas, les données et transactions réalisées avant le sinistre de 8 heures seront perdues et doivent être réintégrées dans le système défaillant. Ceci est vrai seulement si la sauvegarde réalisée de 8 heures avant le sinistres est récupérable et exploitable. Auquel cas, la perte de données peut s'étendre jusqu'à la dernière sauvegarde valide de la plateforme (18 heures).



Copyright - Tout droit réservé - OFPPT

01 - Décrire les mécanismes de récupération

Objectif de point de récupération (RPO)

Que détermine le RPO ?

L'objectif de point de récupération ou RPO est basé sur le temps et constitue une mesure cruciale pour déterminer la tolérance aux pertes de l'entreprise. Dans sa forme la plus élémentaire, il vous aidera à déterminer la fréquence à laquelle vous devez sauvegarder l'ensemble du système pour assurer la continuité des activités. RPO aide à déterminer ce qui suit :

Quelle est la fréquence de planification de sauvegarde minimale?

Combien de données peuvent être perdues après qu'une catastrophe a causé un préjudice important à l'organisation?

Jusqu'où l'équipe informatique doit remonter pour utiliser des techniques de récupération sans retarder la perte de données par rapport au RTO attendu?

PARTIE 1

Copyright - Tout droit réservé - OFPPT

01 - Décrire les mécanismes de récupération

Objectif de point de récupération (RPO)

Importance de la RPO

Le RPO calcule le temps que peut mettre une entreprise avant que la quantité de données perdues ne dépasse la tolérance ou seuil maximal autorisé au niveau du plan de reprise après sinistre (DRP). La première étape consiste à définir le délai RPO qui détermine les fréquences de sauvegarde. L'idée est de s'assurer qu'il y a toujours une sauvegarde disponible avant le sinistre. Cependant, vous devez évaluer la valeur des données qui doivent être récupérées. En fonction du niveau de criticité des données, vous devez définir le RPO pour une sauvegarde continue. Il est évident que les entreprises perdent des données pendant les temps d'arrêt. Mais, en définissant le délai RPO, vous pouvez définir la fréquence des sauvegardes de données pour perdre le moins de données possible, ce qui est assez tolérable.

Vous pouvez également automatiser les sauvegardes de données avec des RPO individuels. Bien que le maintien d'un RPO proche de zéro soit possible grâce à des stratégies de basculement/restauration, mais c'est une entreprise coûteuse.

Il est très critique car il aide une organisation à :

- Améliorer l'efficacité du Plan de Continuité d'Activité (PCA)
- Protéger les applications essentielles sans lesquelles l'entreprise ne peut fonctionner
- Aider à déterminer votre accord de niveau de service (SLA) pendant l'interruption

PARTIE 1

Copyright - Tout droit réservé - OFPPT

01 - Décrire les mécanismes de récupération

Objectif de point de récupération (RPO)

Calcul de la RPO

Pour calculer le RPO, vous devez d'abord définir la quantité de données que vous êtes prêt à perdre si le système de production n'est pas disponible. Vous devez également comprendre le coût des temps d'arrêt, c'est-à-dire le temps pendant lequel une application ou un système est indisponible.

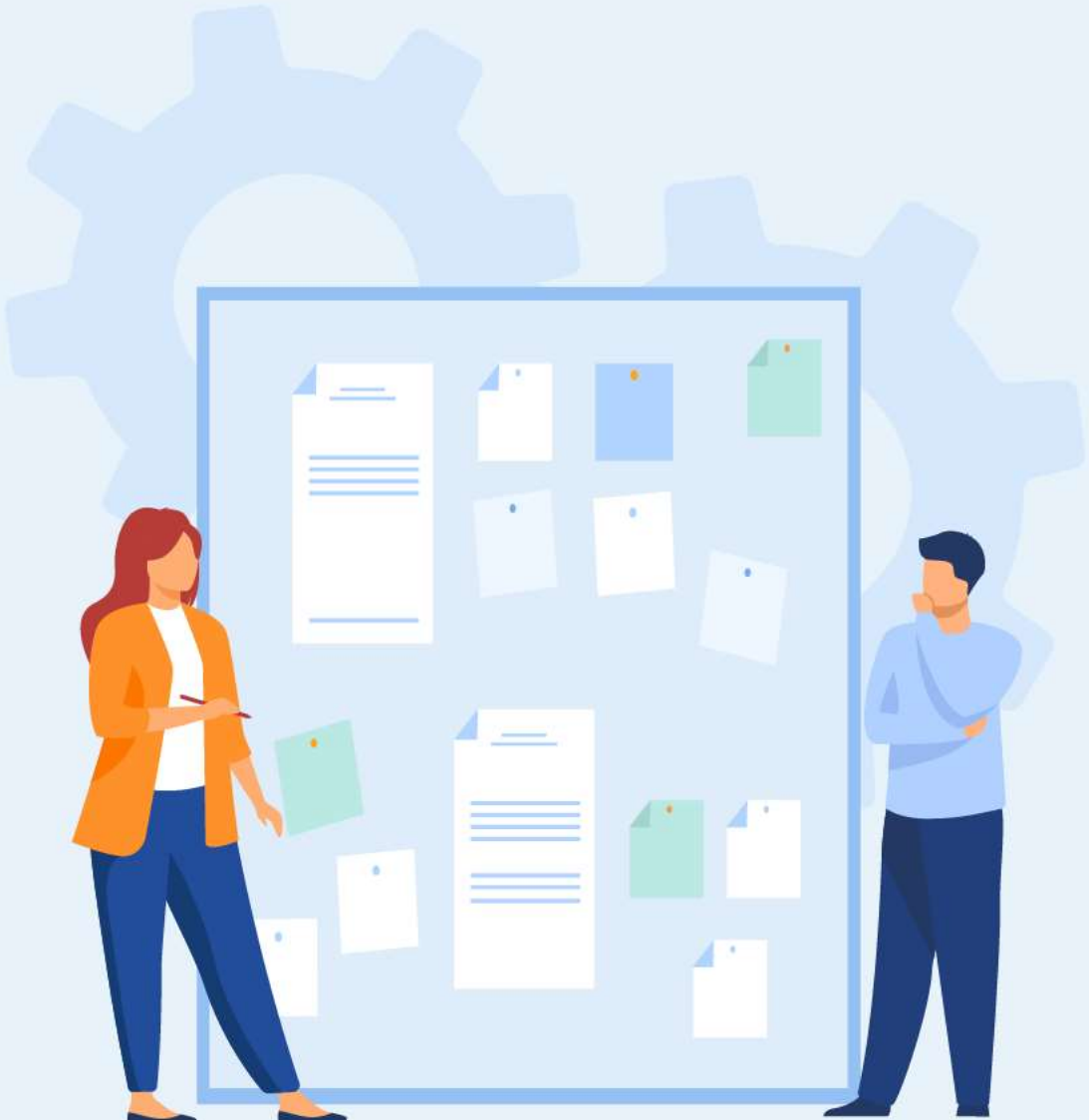
Ensuite, dressez un inventaire de chaque système et application utilisé par votre entreprise dans le cadre de votre plan de continuité des activités et de reprise après sinistre (BCDR). De plus, vous devez calculer combien de temps votre entreprise peut se permettre de rester hors ligne, ce qui risque de compromettre la confiance des clients et les relations avec les partenaires.

N'oubliez pas de prendre en compte les équipes internes et les utilisateurs finaux susceptibles d'être affectés par des systèmes rendus inaccessibles. Ces systèmes sont classés selon des niveaux de criticités.

Par exemple:

- ✓ **Niveau 1 :** 0 min - 1 h - Ce niveau comprend les opérations commerciales critiques qui ne peuvent pas se permettre de perdre plus d'une heure de données. Par exemple, les transactions bancaires, les dossiers des patients des systèmes CRM, etc.
- ✓ **Niveau 2 :** 1 h - 4 h - Ce niveau représente les unités commerciales semi-critiques qui peuvent se permettre de perdre des données jusqu'à 4 heures. Par exemple, les serveurs de fichiers et les journaux de discussion des clients.
- ✓ **Niveau 3 :** 4 h - 12 h - Ce niveau comprend les entreprises qui ne peuvent pas se permettre de perdre plus de 12 heures de données. Par exemple, les données de vente et de marketing.
- ✓ **Niveau 4 :** 13h - 24h Les entreprises qui traitent des informations semi-critiques nécessitant un RPO d'au moins 24 heures relèvent de ce niveau. Par exemple, les données sur les ressources humaines (RH) et les services d'achat.

Copyright - Tout droit réservé - OFPPT



CHAPITRE 1

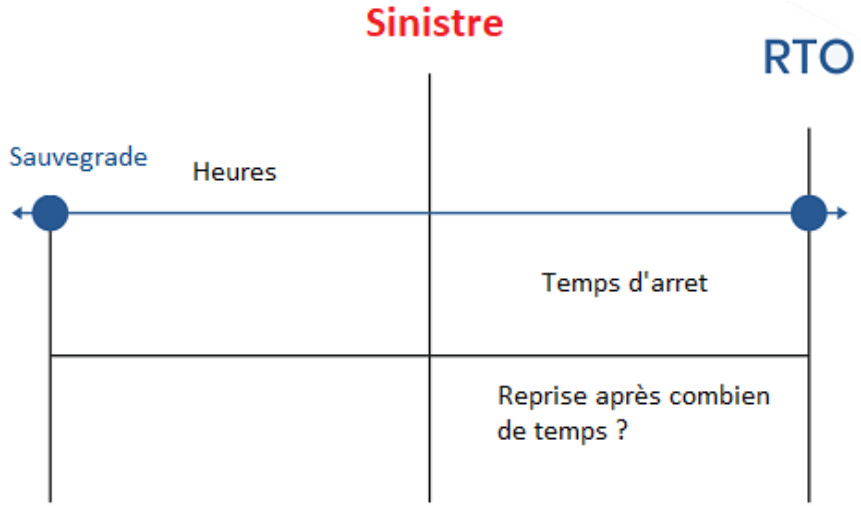
Décrire les mécanismes de récupération

1. Connaitre l’objectif de point de récupération (RPO)
2. **Connaitre l’objectif de temps de récupération (RTO)**
3. Mettre en place un plan de reprise d’activité (RPA)
4. Mettre en place un plan de continuité d’activité (PCA)

Définition de la RTO

L'objectif de temps de récupération (RTO) est défini comme la durée maximale acceptable pendant laquelle une application peut être indisponible ou la panne maximale tolérable que l'organisation endure sans causer de dommages importants à une entreprise après qu'un sinistre, une panne ou tout autre événement inacceptable se soit produit.

Le temps RTO suggère le temps nécessaire pour récupérer et terminer la restauration du système d'un système défaillant tel que défini dans l'accord de niveau de service (SLA). L'objectif de niveau de service tient compte du temps de récupération défini par l'organisation pour récupérer/restaurer ses processus/opérations informatiques critiques à la normale à partir du moment où un sinistre se produit afin d'assurer la continuité des activités.



Remarques

Vous devez toujours chercher à atteindre le RTO le plus bas possible afin de minimiser l'impact d'un sinistre. Pour déterminer votre RTO, vous devez d'abord identifier l'effet de la durée sur votre entreprise pendant laquelle les données ne sont pas disponibles.

PARTIE 1

Copyright - Tout droit réservé - OFPPT

Exemple de la RTO

Exemple 1 :

Supposons que vous soyez une société de transactions en ligne comme PayPal ou Pioneer confrontée à des événements imprévisibles. Dans ce cas, votre RTO sera assez rapide pour récupérer l'opération.

En d'autres termes, une entreprise fixe son RTO à une heure ou deux pour éviter les conséquences sous forme de finances ou de données.

- Si 30% des données doivent être disponibles dans 1 heure,
- Et après une perte complète de la base de données, 60% des données doivent être disponibles sous 2 heures,
- Les 10 % de données restantes doivent être disponibles dans l'heure suivante,
  - **Votre RTO total est = 4 Heures.**

Exemple 2 :

Supposons que le serveur Exchange est en panne. Si votre RTO est de 5 heures, le temps d'arrêt maximal tolérable auquel votre entreprise peut survivre est de 5 heures, et votre RTO pour le serveur Exchange doit être inférieur à 5 heures. Votre politique de reprise après sinistre doit inclure les mesures nécessaires prises par le service informatique pour sauvegarder et restaurer les données.

Par conséquent, tout en fixant l'objectif de temps de récupération, il n'y a pas de solution unique pour un plan de continuité des activités. Les RTO peuvent être définis pour récupérer les données après un sinistre. Cependant, en cas d'incident, les aspects pratiques de votre plan de reprise après sinistre dépendent également des outils et de la technologie spécifiques utilisés pour assurer la reprise. Ainsi, la capacité d'atteindre le RTO varie en fonction des différentes technologies et des différents outils de reprise après sinistre dans leurs capacités. Le RTO est mesuré avant même le début de la panne et inclut le temps nécessaire pour réparer les serveurs, installer les applications prioritaires et restaurer les données. Il inclut également les méthodes de récupération et les données sauvegardées qui doivent être récupérées.

Copyright - Tout droit réservé - OFPPT

01 - Décrire les mécanismes de récupération

Objectif de temps de récupération (RTO)

Que détermine le RTO ?

L'objectif de temps de récupération est une durée ciblée pendant laquelle les applications, les systèmes et/ou les processus survivent aux temps d'arrêt et ne fonctionnent pas avant le début de l'interruption.

Le RTO est d'une importance primordiale pour déterminer la durée de hiérarchisation des applications et des processus dans les paramètres RTO. Dans le plan de protection des données et la stratégie de reprise après sinistre, RTO répond à la question : "Quel est le délai cible établi pour la restauration des services après une notification d'interruption de service ?"

Les RTO peuvent déterminer :

La durée en temps réel à définir pour récupérer un site à partir du moment où l'incident interrompt le flux normal des opérations jusqu'à sa restauration

Quelles préparations informatiques doivent être conçues pour la mise en œuvre du plan de reprise après sinistre

Le niveau acceptable de risque de perte de données, lorsque le système ou les applications clés sont hors ligne.

PARTIE 1

Copyright - Tout droit réservé - OFPPT

01 - Décrire les mécanismes de récupération

Objectif de temps de récupération (RTO)

Comment calculer le RTO ?

Une métrique RTO définit à l'avance l'attente cible pour l'équipe informatique, car elle détermine le seuil de rapidité avec lequel le système ou l'application peut être récupéré après le temps d'arrêt et remettre votre système en ligne. Après avoir défini cette mesure en termes de quantité de « temps réel » pour restaurer le système, vous pouvez alors planifier votre stratégie de récupération pour remettre le service en marche.

Pour calculer le RTO, vous devez prendre en compte les pertes associées à une interruption de l'objectif de temps de récupération du plan de continuité d'activité (BCP). Incluez également une analyse d'impact qui explique les effets à court ou à long terme de l'interruption des services. Cela inclut les risques, les pertes de revenus, les dépenses, les applications destinées aux clients, les applications critiques et les applications moins prioritaires qui sont affectées ou qui deviendront indisponibles. RTO est plus préoccupé par les temps d'arrêt et les limites de temps pour le processus de récupération de données.

Pour déterminer un RTO, vous aurez peut-être besoin de plusieurs catégories de RTO, car certaines pannes peuvent ne pas nécessiter beaucoup de temps de récupération, tandis que d'autres peuvent nécessiter différentes solutions de protection à long terme.

Par exemple, le RTO peut être beaucoup plus long pour les applications moins critiques (peu utilisées). En fonction des niveaux de complexité de plusieurs systèmes de sécurité en fonctionnement, vous devrez peut-être définir le RTO en fonction de sauvegardes à intervalles courts et longs. Cela peut se produire en raison d'un événement de ransomware ou d'un autre incident catastrophique massif.

Facteurs principaux à prendre en compte lors du calcul du RTO

- Équation coût/bénéfice des solutions de récupération
- Applications prioritaires des systèmes et données individuels
- Mesures à prendre par le service informatique en fonction des processus, des techniques automatisées ou des technologies pour restaurer l'infrastructure informatique
- Coût de la panne et de l'atténuation
- La complexité de la procédure de recouvrement

PARTIE 1

Copyright - Tout droit réservé - OFPPT

01 - Décrire les mécanismes de récupération

Objectif de temps de récupération (RTO)

Comment calculer le RTO ?

Pour calculer le RTO en fonction de la priorité des applications métier, il est essentiel de rendre votre RTO aussi précis que possible :

- **RTO proche de zéro (Applications critiques Niveau 1) :** nécessite des services de basculement pour les applications critiques
- **RTO de 4 heures (Applications critiques Niveau 2) :** restauration sur site à partir d'une restauration bare metal se terminant par une disponibilité complète des applications et des données
- **RTO de plus de 8 heures :** pour les applications non critiques qui peuvent être indisponibles pendant des jours sans causer de dommages sérieux à l'entreprise
- Si le temps de restauration minimum possible est de 2 heures, un RTO d'une heure ne peut pas être respecté.
- Dans un autre cas, si vous avez défini un RTO de 4 heures et qu'il y a une panne du système à 12 h 4, le serveur sera réparé et opérationnel à XNUMX h XNUMX, ce qui signifie que le RTO cible est atteint.
- **Si votre RTO est fixé à 2 semaines**, l'investissement serait beaucoup plus faible car vous disposez de suffisamment de temps pour récupérer les données une fois la perturbation survenue.

PARTIE 1

Copyright - Tout droit réservé - OFPPT

Intervalles d'échantillonnage RTO

Atteindre un RTO proche de zéro est coûteux pour la plupart des entreprises informatiques, mais il est possible d'y parvenir si vous accordez la priorité aux applications et aux données. Pour les applications moins critiques pour l'entreprise, l'horloge RTO peut consommer des temps objectifs plus longs que d'habitude. Les plans RTO proches de zéro pour les applications critiques peuvent vous obliger à envisager une capacité de basculement immédiate.

En fonction de la gravité de la panne, vous pouvez définir le temps RTO cible réalisable. Cependant, le temps de restauration du RTO dépend également des limites de l'organisation informatique. Par exemple, si la restauration de toutes les fonctions et opérations informatiques prend 3 heures, le RTO doit être d'au moins 3 heures.

NB : Du point de vue de la reprise après sinistre (DR), l'horloge RTO démarre juste au moment où les processus de récupération démarrent.

Lorsque vous calculez le RTO (Recovery Time Objective) pour vos unités commerciales, tenez compte des exemples d'intervalles suivants :

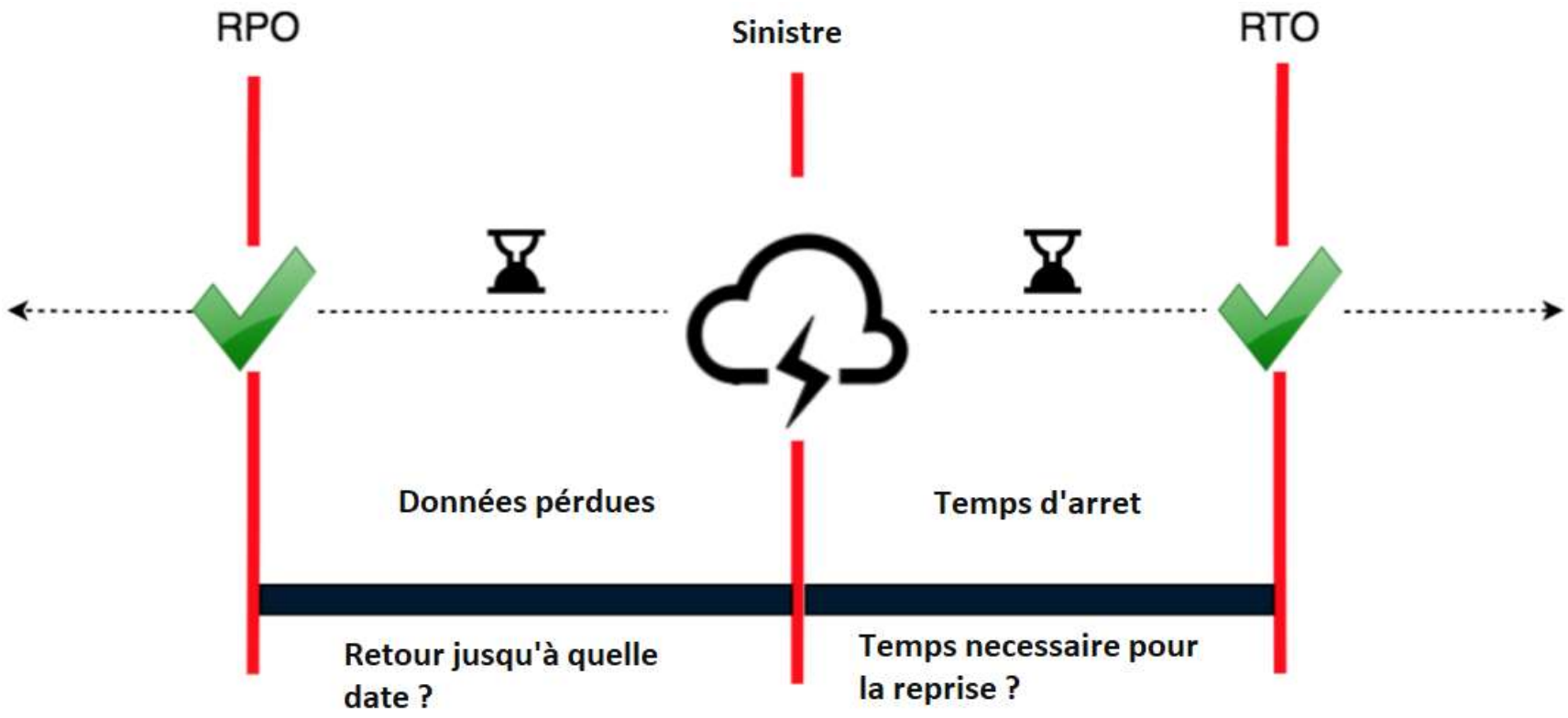
1 heure : Cet intervalle nécessite la sauvegarde des données redondantes sur les disques durs externes.

5 Jours : Dans ce cas, la solution la plus rentable serait de sauvegarder les données à l'aide d'un disque compact, d'une bande ou d'un stockage sur disque hors site.

Copyright - Tout droit réservé - OFPPT

Différences entre RTO et RPO

Ci-dessous un schéma représentant les deux concepts et à quoi il permettent de répondre :



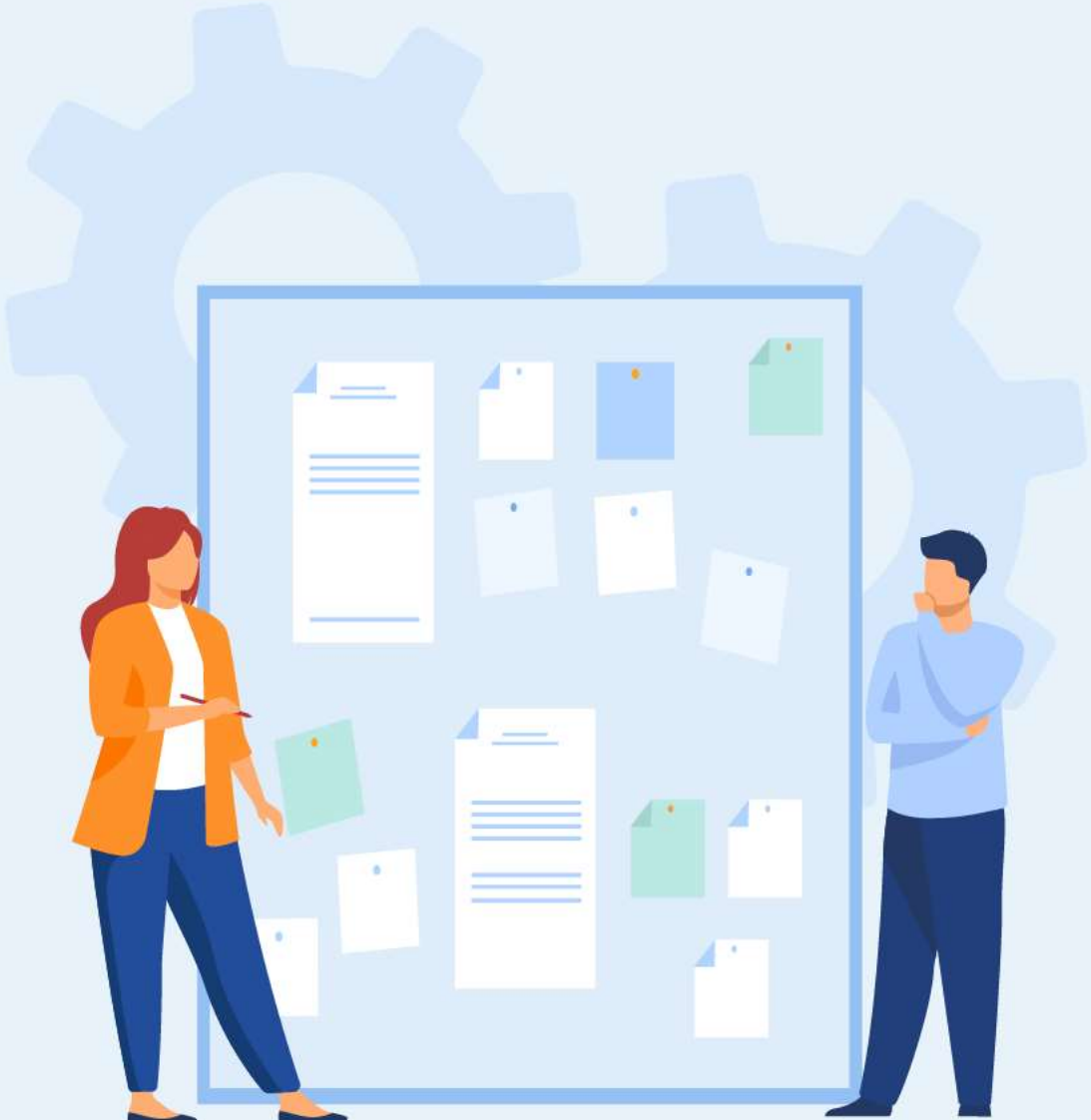
Copyright - Tout droit réservé - OFPPT

Différences entre RTO et RPO

Une solide compréhension de l'objectif de temps de récupération par rapport à l'objectif de point de récupération peut vous aider à atteindre vos objectifs de récupération. Jetez un coup d'œil aux points clés des différences entre le RTO et le RPO.

- Avec RTO, vous pouvez mesurer la durée d'indisponibilité des applications métier pendant un temps d'arrêt. Alors que le RPO mesure la quantité variable de perte de données acceptable pendant un temps d'arrêt.
- Vous pouvez mesurer le RTO en prenant le point de départ d'une panne. Mais, pour mesurer le RPO, vous devez remonter dans le temps pour déterminer la perte de données que l'entreprise peut tolérer à partir de la dernière sauvegarde créée.
- Le RTO inclut les étapes que le service informatique doit suivre pour réduire les temps d'arrêt et remettre les applications en marche. Le RPO détermine jusqu'où le service informatique est prêt à remonter pour récupérer les données en revenant à la dernière sauvegarde effectuée.
- Lors du calcul du RTO, les temps de restauration du RTO varient car plusieurs facteurs doivent être pris en compte. Par exemple, les délais linéaires, le jour de la catastrophe, etc. compliquent encore son calcul. Le RPO est plus facile à calculer et à mettre en œuvre lorsque vous prenez les dernières variables d'utilisation des données et de sauvegarde.
- Étant donné que le RTO inclut la récupération de l'ensemble de l'infrastructure, le coût de récupération augmente considérablement pour répondre à l'exigence de RTO proche de zéro. Cependant, avec une réplication RPO granulaire proche de zéro, vous pouvez répliquer les données en continu pour une perte de données proche de zéro. Cela simplifiera les coûts et accélérera la récupération des applications nécessitant une haute disponibilité. De plus, un RPO plus long devient abordable, contrairement à la restauration de l'ensemble de l'infrastructure.

Copyright - Tout droit réservé - OFPPT



CHAPITRE 1

Décrire les mécanismes de récupération

1. Connaitre l’objectif de point de récupération (RPO)
2. Connaitre l’objectif de temps de récupération (RTO)
3. **Mettre en place un plan de reprise d’activité (RPA)**
4. Mettre en place un plan de continuité d’activité (PCA)

Définition du plan de reprise d'activité

Un **Plan de Reprise d'Activité** (**PRA**) représente un ensemble de procédures, sous forme de plan d'actions structuré et documenté, qui vise à aider une entreprise à faire face à une catastrophe ou un incident tout en relançant rapidement son activité professionnelle.

Il peut s'agir d'incidents informatiques, de catastrophes naturelles, d'accidents humains, etc. Initialement, on parlait de **PRA informatique** pour retrouver des données informatiques perdues et relancer un système d'information.

Toutefois, le plan de reprise d'activité est un document qui peut être utilisé pour répondre à n'importe quelle **situation de crise**. Il s'intègre dans la formalisation d'un PCA, un Plan de Continuité d'Activité.

➢ À qui s'adresse un RPA ?

Le **Plan de Reprise d'Activité** s'adresse à toutes les entreprises, quelles que soient leurs tailles ou leurs activités. Les petites comme les plus grosses peuvent être confrontées **à une crise** ou **un danger** (nous l'avons récemment constaté avec la crise sanitaire du Covid-19), ce qui nécessite de prévoir différents scénarios afin de se protéger.

Copyright - Tout droit réservé - OFPPT

Plan de reprise d'activité : Intérêt et Conséquence

Quel intérêt de réaliser un PRA ?

Pour faire face aux **incertitudes conjoncturelles** et aux risques (qu'ils soient économiques, financiers ou sanitaires), le plan de reprise d'activité repose **sur l'anticipation**.

Il consiste à **adopter une posture agile** pour s'adapter à un environnement changeant. Les enjeux sont importants et multiples pour la société :

- ✓ **Garantir un niveau de chiffre d'affaires minimum** en assurant la reprise d'une activité (même partielle) et assurer la survie de l'entreprise ;
- ✓ **Satisfaire ses clients**, même en période de crise, **et les fidéliser** pour améliorer son image ;
- ✓ **Fidéliser les collaborateurs et fluidifier l'organisation interne** de l'entreprise en garantissant la bonne gestion et le bon fonctionnement de la structure.

Les conséquences négatives d'une interruption d'activité :

Une **interruption de l'activité** à cause d'une panne des systèmes ou des machines (ou autre cause) peut entraîner de nombreuses conséquences négatives comme :

- ✓ Un ralentissement de l'activité opérationnelle, puisque les équipes ne disposent plus des ressources indispensables pour mener à bien leur travail ;
- ✓ Une baisse du chiffre d'affaires à cause de l'impossibilité de signer de nouveaux contrats ;
- ✓ Une perte des données qui peut être dangereuse pour l'activité ;
- ✓ Une diminution de la satisfaction client puisque le consommateur ne peut plus profiter du produit ou du service ;
- ✓ Le renvoi d'une image négative auprès des partenaires et prospects ;
- ✓ Des risques de poursuites judiciaires pour manquement aux obligations.

Copyright - Tout droit réservé - OFPPT

Mise en place du plan de reprise d'activité

La structure d'un **plan de reprise d'activité** après sinistre (alias *PRA*, ou, en anglais, DR plan, pour « *disaster recovery* ») est constante, quel que soit le cas d'usage, ce qui facilite l'organisation et la réalisation. Examinons de plus près le processus. La figure 1 est une adaptation de la norme internationale ISO **27031 (2011)**, développée par l'Organisation internationale de normalisation (ISO).

Cette structure reprend le modèle PDCA (plan-do-check-act, ou planifier, réaliser, vérifier, agir) déjà utilisé par d'autres normes ISO.

Une analyse d'impact (**BIA, business impact analysis**) est généralement réalisée avant l'évaluation des risques, afin d'identifier les fonctions métier les plus importantes ainsi que les systèmes et actifs informatiques dont elles dépendent.

L'évaluation des risques techniques (RA, risk assessment) examine ensuite les menaces et les vulnérabilités internes et externes susceptibles d'avoir des répercussions négatives sur les actifs informatiques. Le recours à des services Cloud, généralement basés ailleurs, hors du contrôle du service informatique, rappelle l'importance de ces deux analyses.

Une fois définis les systèmes et fonctions métier essentiels ainsi que les risques associés, l'étape suivante consiste à définir des stratégies visant à limiter les risques et les menaces pour ces actifs.

Vous pouvez par exemple envisager de stocker les données et systèmes stratégiques hors site, en faisant appel à une société de services Cloud, comme AWS ou Microsoft Azure. Vous pouvez aussi diversifier les fournisseurs de composants informatiques critiques comme les serveurs ou les routeurs.

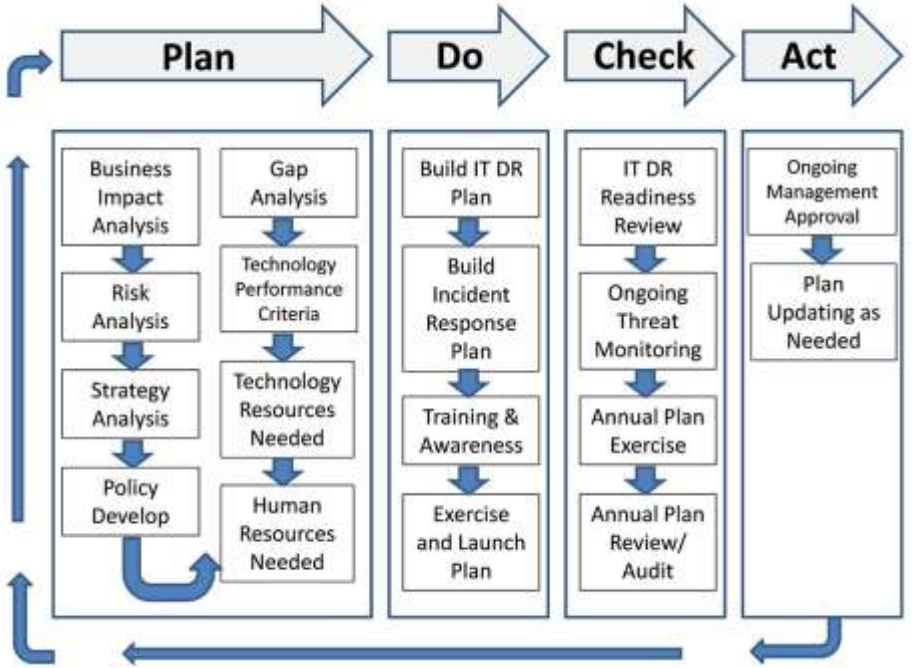


Figure 1: Le modèle plan-do-check-act.

PARTIE 1

Copyright - Tout droit réservé - OFPPT

Mise en place du plan de reprise d'activité

Les grandes lignes du processus

Les RPA comprennent un processus détaillé, étape par étape, pour réagir en cas d'incident grave (tel que défini dans l'évaluation des risques). Ces étapes fournissent une procédure simple à utiliser et reproductible. Elle est destinée à récupérer les actifs informatiques endommagés et à les rendre de nouveau opérationnels le plus vite possible. Il s'agit là d'un défi intéressant, étant donné que le département informatique n'a absolument aucun contrôle sur les services fournis depuis le Cloud et qu'il doit être particulièrement proactif lors de l'évaluation, puis lors de la gestion d'un fournisseur de services Cloud.

Plusieurs exercices permettent de déterminer si les procédures de reprise d'activité après sinistre fonctionnent comme prévu, qu'il s'agisse d'une évaluation point par point des plans et procédures de reprise (par exemple dans une salle de conférences) ou d'un exercice de simulation grandeur nature permettant de déterminer les conséquences réelles d'une panne du système.

Dans un environnement Cloud, le fournisseur de services de reprise d'activité peut proposer ses propres exercices de reprise. Il est alors important d'examiner les mesures à prendre éventuellement avant de signer un contrat de service Cloud. Il est notamment primordial de savoir quelles ressources le fournisseur utilisera, quelle quantité de données de performance l'exercice permettra d'obtenir, et quel pourra être le degré d'implication des utilisateurs pendant l'exercice.

Lors des mises à jour du plan, un processus doit permettre de prendre en compte la gestion des modifications, les changements de personnel, et toute autre situation pouvant altérer l'efficacité ou le contenu du plan. Les mises à jour permettent de vérifier que le plan est adapté aux objectifs et qu'il est en phase avec les effectifs et les activités métier en cours.

Les fournisseurs de services de PRA en Cloud peuvent assurer une certaine dose de flexibilité pendant le développement et la mise à jour du plan. Il est indispensable de passer au peigne fin tous les services proposés par un fournisseur de Cloud, et de comparer le coût d'une gestion par un prestataire externe à celui d'une gestion en interne.

Copyright - Tout droit réservé - OFPPT

Mise en place du plan de reprise d'activité

Analyse d'impact métier (BIA)

Pour la réalisation d'une analyse d'impact, l'ISO **22317 (2015)** fournit des conseils utiles de planification et d'exécution. Elle consiste à déterminer les processus métier les plus indispensables à l'activité et les actifs informatiques dont ils dépendent. Cette étape permet aussi de détecter d'autres conséquences inattendues pour l'entreprise en cas de perturbation de fonctions métier clés, comme la perte de clients, la baisse des performances financières, la dégradation de la réputation, et leurs effets sur les employés et les chaînes d'approvisionnement.

Après avoir identifié les principales activités métier ainsi que les systèmes et données dont elles dépendent, il convient de lister leurs risques. Une BIA utilise une série de questions présentées à des managers et à des spécialistes de chacune des unités opérationnelles de l'entreprise, service informatique compris. Ces questions doivent porter au minimum sur les points suivants :

- ❖ Connaissance du mode de fonctionnement de chaque unité opérationnelle.
- ❖ Identification des processus essentiels, au sein de ces unités opérationnelles, qui dépendent de l'infrastructure informatique (sur site).
- ❖ Identification des processus essentiels, au sein de ces unités opérationnelles, qui dépendent de l'infrastructure informatique (dans le Cloud).
- ❖ Valeur financière des processus métier essentiels (par exemple, revenus horaires générés).
- ❖ Dépendances vis-à-vis des organisations internes.
- ❖ Dépendances vis-à-vis des prestataires externes, notamment les fournisseurs de services Cloud.
- ❖ Exigences en matière de données.

Copyright - Tout droit réservé - OFPPT

Mise en place du plan de reprise d'activité

Analyse d'impact métier (BIA)

- Conditions système requises.
- Temps minimum nécessaire pour récupérer les données et restaurer leur état d'utilisation antérieur.
- Temps minimum requis pour rétablir l'état de fonctionnement normal ou quasi normal de l'infrastructure informatique à la suite d'un incident.
- Nombre minimum d'employés nécessaires à la poursuite des opérations.
- Technologie minimale nécessaire à la poursuite des opérations.
- Durée maximale d'indisponibilité des technologies, avant que l'entreprise cesse de pouvoir fournir ses produits et services.

Les résultats de l'analyse d'impact donnent un aperçu clair des retombées réelles sur l'activité, en termes de problèmes éventuels et de coûts prévisibles. Ils permettent de déterminer les éléments à protéger, le degré de tolérance de l'entreprise aux perturbations, les niveaux minimums de service informatique requis et le temps maximum d'indisponibilité avant que l'entreprise commence à dysfonctionner.

Copyright - Tout droit réservé - OFPPT

Mise en place du plan de reprise d'activité

Évaluation des risques techniques (RA)

Pour l'analyse des risques techniques, il existe également une norme américaine formulée par le NIST (National Institute for Standards and Technology) : **NIST SP 800-30 (2012)**. Les responsables informatiques se focalisent généralement sur l'un ou plusieurs des scénarios de risque suivants, dont la survenue aurait très certainement un impact négatif sur la capacité de l'entreprise à poursuivre ses opérations :

- ❑ Perte d'accès
- ❑ Perte de données
- ❑ Perte de fonction
- ❑ Perte de compétences
- ❑ Perte de contrôle

Le recours à des services dans le Cloud implique un risque de perte de contrôle certain pour les départements informatiques. Sur site, il est possible de planifier et de gérer la reprise d'activité après sinistre de bout en bout, tandis que dans le Cloud, le contrôle de nombreuses fonctions revient au prestataire externe. Il incombe aux directeurs informatiques de décider si le risque lié à l'utilisation du Cloud en vaut la chandelle.

L'évaluation des risques techniques permet de définir les menaces et les vulnérabilités susceptibles d'entraîner les conséquences mentionnées plus haut. Il existe de nombreuses méthodes d'analyse des risques. Le tableau ci-dessous à droite fournit néanmoins une approche simple, facile à mettre en œuvre. La difficulté consiste à faire valider les estimations de facteurs de risque par les dirigeants.

Copyright - Tout droit réservé - OFPPT

Mise en place du plan de reprise d'activité

Évaluation des risques techniques (RA)

L'évaluation des risques techniques permet de définir les menaces et les vulnérabilités susceptibles d'entraîner les conséquences mentionnées plus haut. Il existe de nombreuses méthodes d'analyse des risques. Le tableau ci-dessous fournit néanmoins une approche simple, facile à mettre en œuvre. La difficulté consiste à faire valider les estimations de facteurs de risque par les dirigeants.

Table 1: A simple risk assessment

Event	Likelihood (a)	Impact (b)	Risk weight factor (a x b)
Fire in datacentre	0.4	0.9	0.36
Loss of power	0.5	0.8	0.40
Loss of staff (eg, from Covid)	0.8	0.5	0.40
Severe weather	0.4	0.9	0.36
Water leak in datacentre	0.3	0.6	0.18
Theft of user data caused by rogue cloud service employee	0.4	0.9	0.36
Employee forgot to log off from workstation	0.6	0.3	0.18
Cloud vendor had a major security breach	0.7	0.9	0.63

Ce tableau présente des exemples réalistes d'événements à risque dans des environnements sur site ou dans le Cloud. D'après des expériences réelles et les statistiques disponibles, issues par exemple de compagnies d'assurances ou de données actuarielles, il est possible d'estimer la probabilité de certains événements sur une échelle de 0 à 1 (0,0 = ne se produira jamais, et 1,0 = se produira toujours). On peut ensuite appliquer la même procédure à l'impact de l'événement, toujours sur une échelle de 0 à 1 (0,0 = aucun impact, et 1,0 = perte totale d'exploitation).

La dernière colonne indique le produit de la probabilité (Likelihood) multipliée par l'impact. On obtient ainsi le « facteur de pondération du risque ». Les situations présentant le facteur de pondération du risque le plus élevé sont à inscrire dans le plan de reprise d'activité après sinistre.

Copyright - Tout droit réservé - OFPPT

Mise en place du plan de reprise d'activité

Évaluation des risques techniques (RA)

Voici des exemples de traitement des risques :

- **Prévenir** – événements à probabilité et à impact élevés (tenter activement de les limiter)
- **Accepter** – événements à probabilité et à impact faibles (rester vigilant)
- **Limiter** – événements à probabilité élevée et à impact faible (réduire leur probabilité de survenue)
- **Transférer** – événements à probabilité moyenne et à impact moyen à élevé (transférer le risque à un tiers, comme une compagnie d'assurances)
- **Planifier** – événements à probabilité faible et à impact élevé (planifier les mesures à prendre en cas de survenue)

Copyright - Tout droit réservé - OFPPT

Mise en place du plan de reprise d'activité

Corréler BIA et RA

Une fois l'analyse d'impact et l'évaluation des risques terminées, l'étape suivante consiste à corréler les données de ces activités dans un tableau (ou sous une autre forme) qui illustre les menaces et les impacts critiques pour l'entreprise que représente chaque risque. Ce tableau inclut en outre l'objectif de délai de récupération (RTO, recovery time objective). Cette métrique développée à partir de la BIA indique pendant combien de temps un système ou un processus peut rester indisponible avant que cela empêche l'entreprise de fonctionner normalement. Le tableau 2 ci-dessous à droite illustre l'une des façons de présenter les résultats de la BIA et de la RA dans un rapport destiné à la direction.

Table 2: Example analysis of results of BIA and RA

Risk identified	Business activity affected	Potential operational loss	Potential financial loss	Recovery time objective
Pipe burst in datacentre	All or most activities, based on affected assets	Inability to function normally	£3,000-£4,000 revenue loss per hour	4-8 hours
Loss of staff	Activities that need specific staff	Reduced ability to function normally	None, assuming backup staff available	2-4 hours
Loss of data due to security breach by cloud vendor	Activities needing the lost data	Reduced ability to function normally	£3,000-£4,000 revenue loss per hour	4-8 hours
Loss of infrastructure by a cloud vendor	Activities needing the lost systems and data	Inability to function normally	£3,000-£4,000 revenue loss per hour	24-48 hours

Copyright - Tout droit réservé - OFPPT

Mettre à jour le plan de reprise d'activité

Pour mettre en place un plan de reprise d'activité, commencez par nommer un chef de projet en charge du PRA. Il s'occupera de son élaboration et effectuera les tests et ajustements nécessaires. Ces phases de tests et les remontées d'échecs doivent être systématiquement documentées.

Ensuite, pensez à mettre à jour régulièrement le PRA pour garantir sa pertinence et son application rapide, mais aussi son efficacité dans le temps. Documentez avec précision votre PRA, notamment en encourageant le retour d'expériences des acteurs qui sont garants de la fiabilité du plan.

En effet, le partage des connaissances va directement impacter les performances du plan.

Copyright - Tout droit réservé - OFPPT

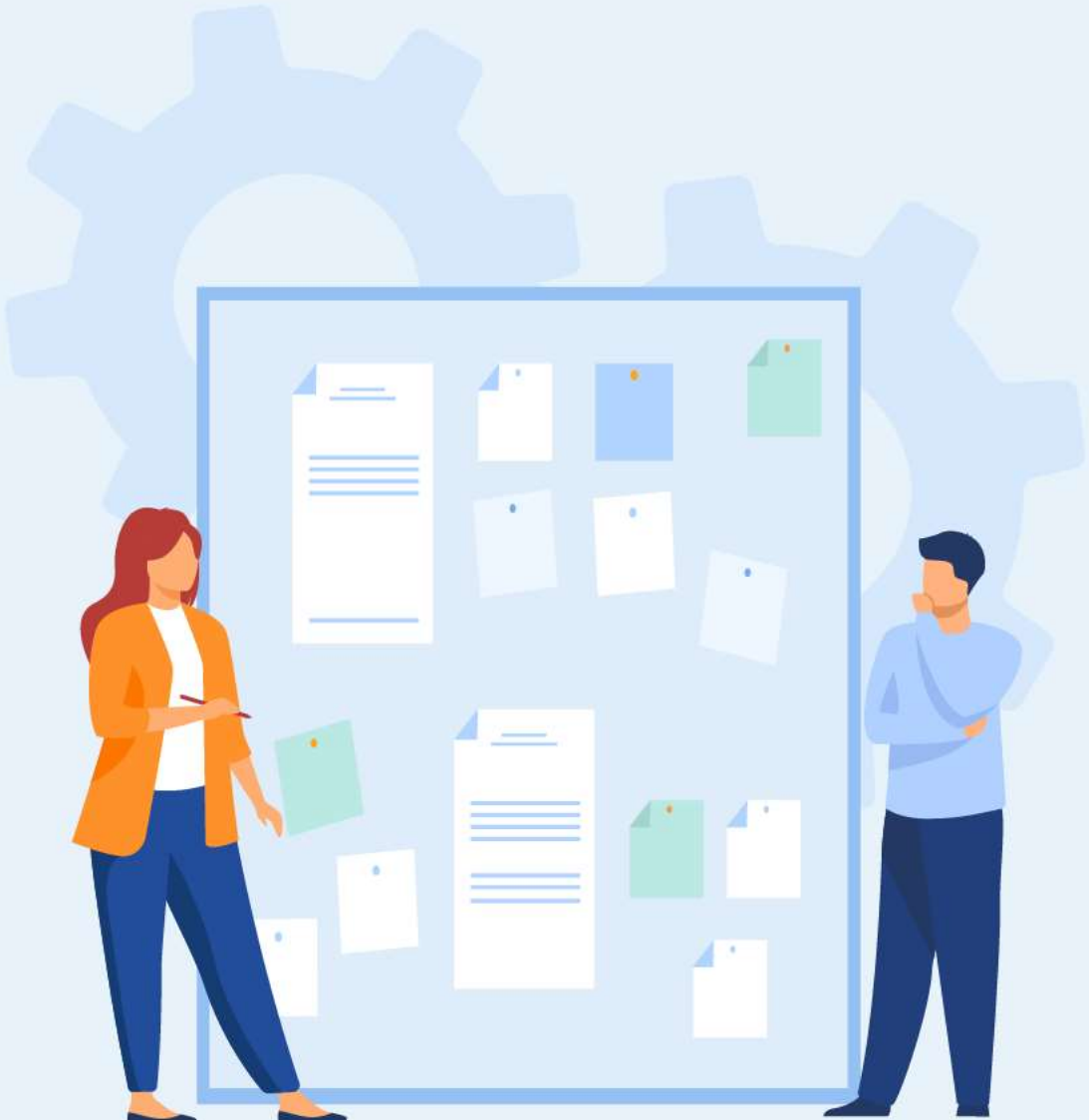
Mise en place du plan de reprise d'activité

Établir un **plan de reprise d'activité de qualité** est donc essentiel. Vous devez simplement procéder de manière **réfléchie** et **systématique**, pour n'oublier aucun élément et agir de manière claire (et rapide) dès qu'un incident intervient. Dans tous les cas, créer un plan de reprise d'activité fonctionnel et fiable vous permettra **de favoriser la pérennité de votre entreprise**.

Pour résumer, l'analyse d'impact et l'évaluation des risques sont des activités primordiales associées à la création et à la gestion du plan de reprise d'activité après sinistre technologique.

Le recours à des services dans le Cloud donne lieu à de nouvelles formes d'analyse, qui ne s'appuient plus systématiquement sur les datacenters. Lors du développement d'un plan de reprise d'activité après sinistre, il est essentiel de se familiariser avec les risques informatiques, notamment en ce qui concerne les services Cloud, ainsi que leur incidence sur les opérations de l'entreprise.

Copyright - Tout droit réservé - OFPPT



CHAPITRE 1

Décrire les mécanismes de récupération

1. Connaitre l’objectif de point de récupération (RPO)
2. Connaitre l’objectif de temps de récupération (RTO)
3. Mettre en place un plan de reprise d’activité (RPA)
4. **Mettre en place un plan de continuité d’activité (PCA)**

Définition du plan de continuité d'activité (PCA)

Le **PCA (Plan de Continuité d'Activité),** appelé BCP (Business Continuity Planning) est un processus permettant d'identifier les menaces et risques potentielles pour une entreprise, et de définir les actions à maintenir de façon prioritaire pour continuer d'atteindre ses objectifs et honorer ses obligations.

Selon la définition donnée par la norme ISO **22301**, la gestion de la continuité d'activité constitue un « processus de management holistique qui identifie les menaces potentielles pour une organisation, ainsi que les impacts que ces menaces, si elles se concrétisent, peuvent avoir sur les opérations liées à l'activité de l'organisation, et qui fournit un cadre pour construire la résilience de l'organisation, avec une capacité de réponse efficace préservant les intérêts de ses principales parties prenantes, sa réputation, sa marque et ses activités productrices de valeurs ».

Concrètement, un Plan de Continuité d'Activité permet donc à une entreprise de préparer l'organisation de son activité en cas de crise. Il peut s'agir de crises internes (incendie, grève, panne informatique) ou de crises externes (crise financière, sanitaire, mouvement social, Covid-19). En l'anticipant, l'entreprise augmente son niveau de résilience et peut ainsi en limiter l'impact.

En résumé, le plan de continuité de l'activité permet de :

- Identifier les risques, les menaces et les vulnérabilités de l'entreprise,
- Mettre en place une réaction opérationnelle adaptée à la situation,
- Maintenir les activités indispensables, éventuellement en mode dégradé,
- Préparer la sortie de crise et retrouver rapidement une situation normale.

Copyright - Tout droit réservé - OFPPT

Pourquoi mettre en place un PCA ?

Le **PCA (Plan de Continuité d'Activité)** a été créé pour être bien préparé et savoir faire face à une situation critique. Il contribue à renforcer la résistance et la durabilité d'une entreprise en cas de crise grave.

Il permet notamment de :

- Minimiser les pertes et réduire (si possible) la durée de la crise,
- Tenir ses engagements auprès de ses clients et partenaires,
- Maintenir sa position et sa visibilité sur le marché.

De la même manière que vous préparez votre plan de communication pour diffuser le bon message aux bons destinataires, vous devez mettre en place une gestion des risques pour savoir comment réagir en cas de problème. Vous serez ainsi capable d'identifier et d'évaluer tous les aléas, les menaces et les incertitudes potentiels, leur occurrence et leurs impacts sur le fonctionnement de votre entreprise.

Lorsqu'un événement inattendu et critique survient, il est difficile de réagir de manière réfléchie, en évitant de se laisser guider par la peur, la panique ou la colère. D'où l'importance et la nécessité d'avoir un PCA qui permet d'analyser tous les risques potentiels et leurs conséquences afin de pouvoir affronter différents scénarios en étant réactif, efficace et surtout objectif.

Copyright - Tout droit réservé - OFPPT

Elaboration d'un plan de continuité d'activité

En période de crise et de nécessité de maintien de l'activité, la principale problématique des entreprises est d'assurer la continuité de l'activité malgré une perte de ressources. L'entreprise doit en effet composer avec une perte de revenus, une diminution de ses effectifs, une dimension logistique revue à la baisse.

Compte tenu des multiples aspects - et conséquences - que peut revêtir une crise, le plan de continuité de l'activité doit présenter la stratégie adoptée ainsi que les procédures à suivre pour faire face à cette situation. C'est le document de référence pour répondre au mieux aux perturbations rencontrées et reprendre un niveau de fonctionnement prédéfini.

La démarche méthodologique permettant l'élaboration concrète d'un PCA est l'objet principal du guide élaboré par le SGDSN (SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE) , qui a pour ambition de favoriser une telle démarche par la délivrance de conseils méthodologiques et la diffusion de bonnes pratiques.

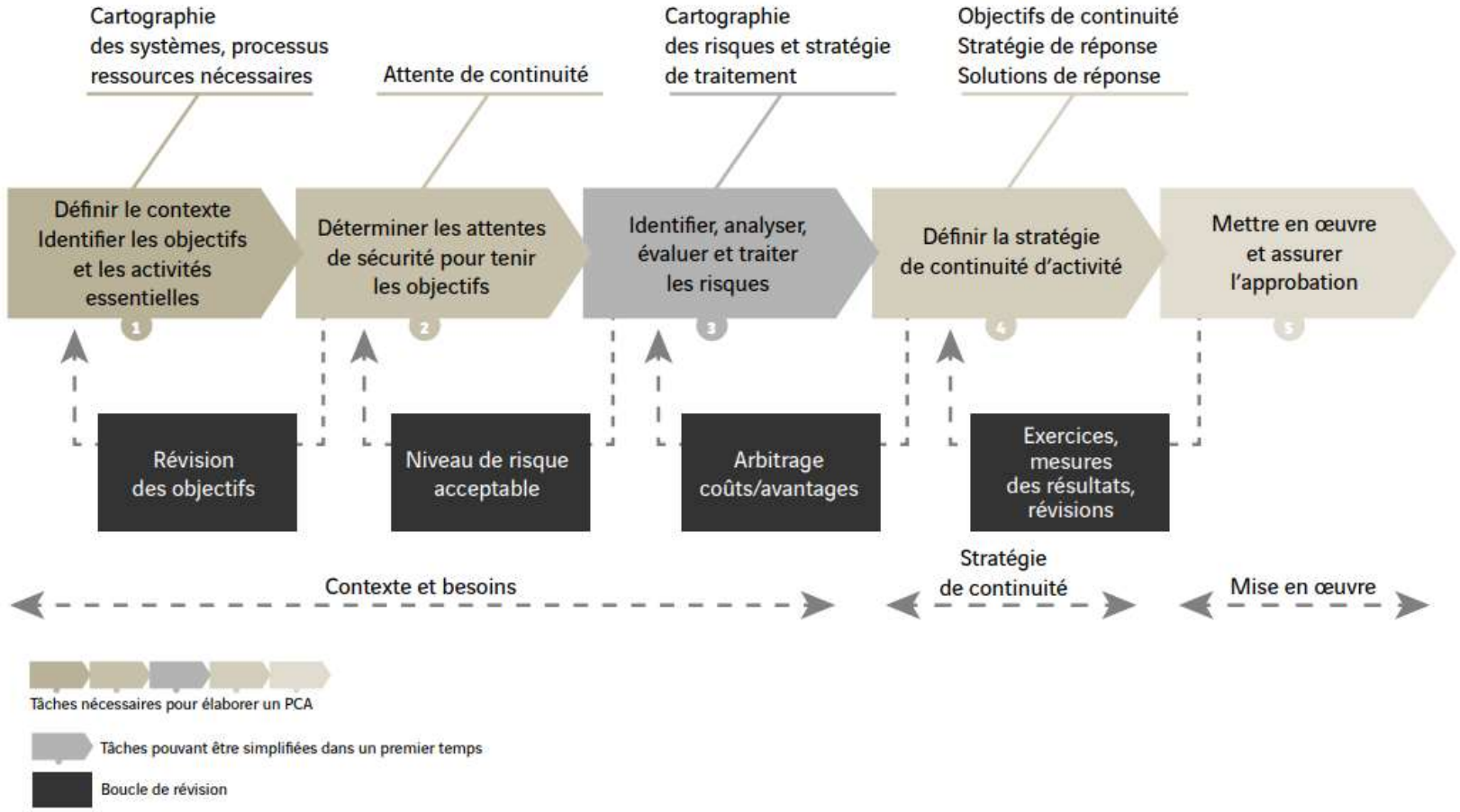
Remarques

Notez que le PCA est évolutif car il doit s'adapter aux priorités changeantes de l'entreprise en période de crise.

Copyright - Tout droit réservé - OFPPT

Elaboration d'un plan de continuité d'activité

Le guide de la SGDSN présente une démarche en 5 étape :



PARTIE 1

Copyright - Tout droit réservé - OFPPT

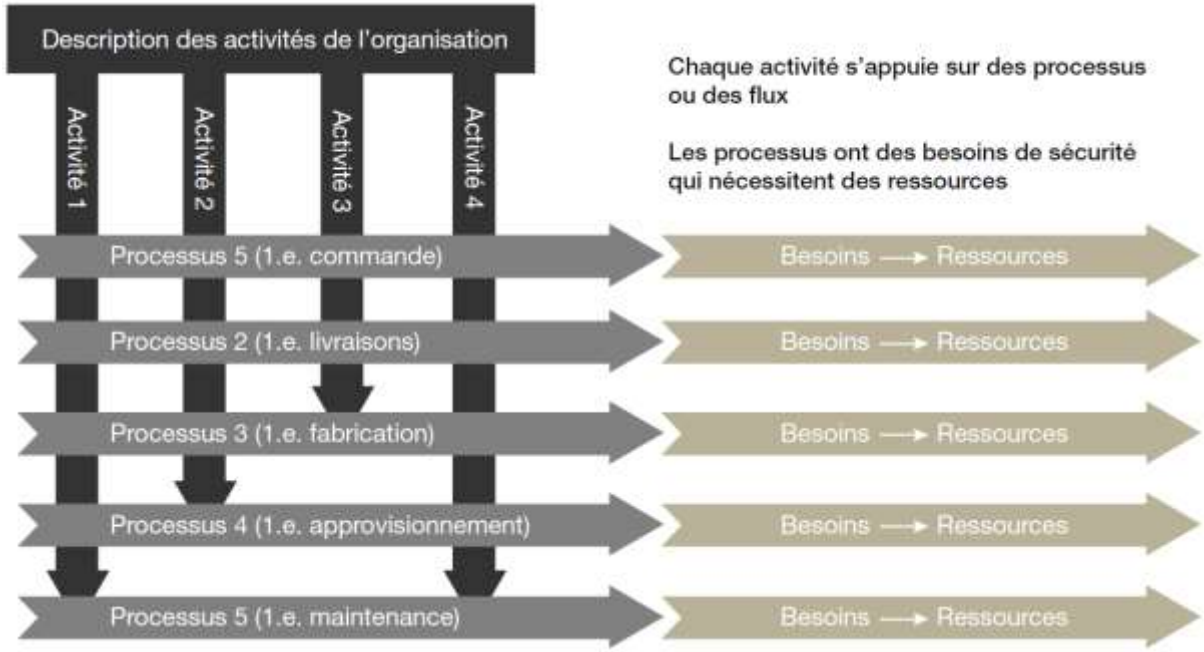
Elaboration d'un plan de continuité d'activité

1 - Définir le contexte, identifier les objectifs et les activités essentielles

Cette première étape est importante et conditionne l'efficacité de l'ensemble de la démarche. Elle vise à préciser le périmètre géographique et fonctionnel de l'organisation et à identifier tout ce qui peut orienter ses choix stratégiques en fonction de sa spécificité et de ses relations avec l'environnement dans lequel elle s'inscrit.

L'analyse du contexte vise également à identifier les activités essentielles pour l'atteinte des objectifs de l'organisation et le respect de ses obligations. Ces activités essentielles supposent l'existence de processus et de flux (financements, matières premières, interfaces avec les systèmes d'information…) dont les plus critiques doivent être cartographiés et décrits pour la suite de la démarche.

De l'analyse des activités essentielles de ce travail doit découler une première analyse des ressources dites également « critiques » pour l'atteinte des objectifs de l'organisation (ressources humaines, infrastructures, système d'information, procédures, ressources intellectuelles et fournisseurs externes).



ACTIVITÉS ET PROCESSUS

PARTIE 1

Copyright - Tout droit réservé - OFPPT

Elaboration d'un plan de continuité d'activité

2 - Déterminer les attentes de sécurité pour tenir les objectifs

La deuxième étape vise à préciser, pour chaque activité essentielle et chaque processus ou flux critiques, à fixer les objectifs à atteindr en matière de continuité d'activités. Ces derniers sont formalisés par des indicateurs qui quantifient :

1 - L'exigence concernant les systèmes en place (pour rendre possible la continuité d'activité) ;

2- L'exigence concernant les modalités de la réponse mise en œuvre à la suite d'un sinistre (pour assurer une continuité d'activité conforme aux objectifs de l'organisation).

Les indicateurs clés qui doivent permettre de quantifier le niveau minimum qui doit subsister juste après le sinistre pour permettre la mise en œuvre des solutions de continuité sont les suivants :

- ✓ Perte de Ressources Maximale Admissible (**PRMA**) pour permettre une reprise;
- ✓ Durée Maximale d'Interruption Acceptable (**DMIA**), avant de disposer d'une solution de contournement palliative (qui mobilise des processus spécifiques et fait généralement appel à des procédures manuelles).

A ce stade, il est déjà possible de quantifier les conséquences d'une interruption de l'activité. Des objectifs relatifs au niveau des ressources critiques doivent être également définis.

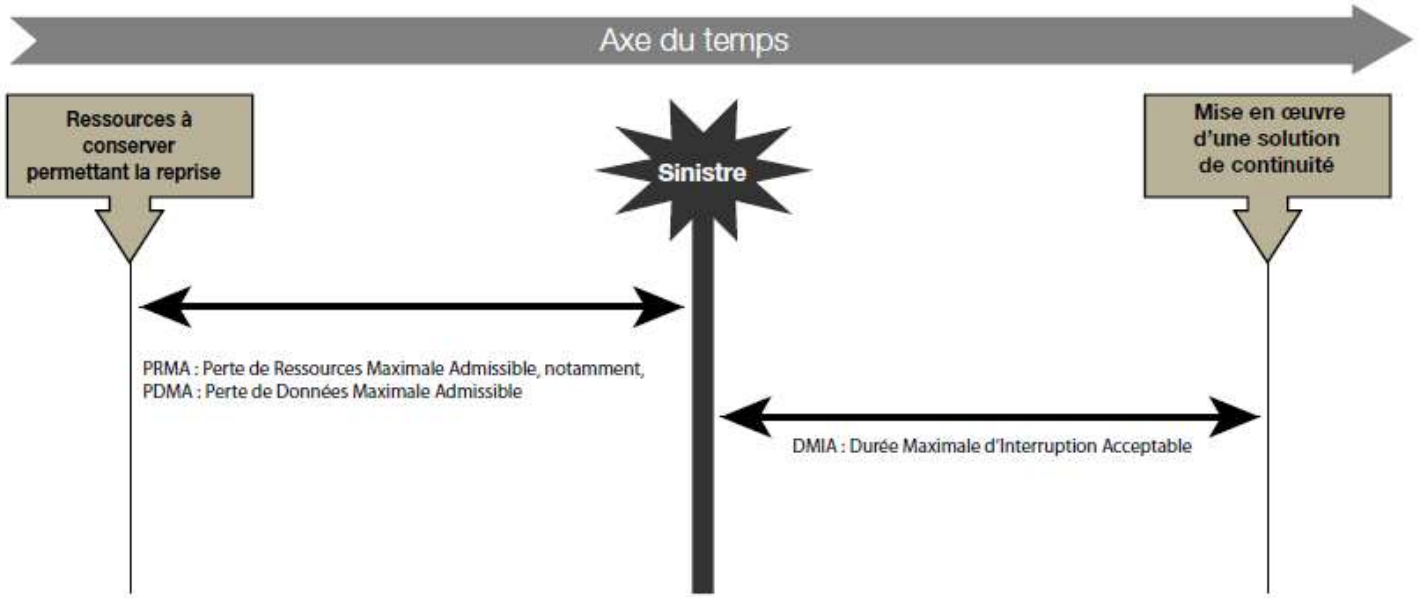
Pour simplifier le travail, l'analyse des besoins en ressources sera effectuée sur la base d'un nombre limité de scénarios (ou situations de crise) retenus comme prioritaires, à l'issue de la démarche de gestion de risque et compte tenu des besoins de continuité.

Copyright - Tout droit réservé - OFPPT

Elaboration d'un plan de continuité d'activité

2 - Déterminer les attentes de sécurité pour tenir les objectifs

Ci-dessous une figure permettant de schématiser les indicateurs pour mesurer les attentes en matière de continuité d'activité :



PDMA mesure le temps maximum admissible durant lequel les données sont perdues, car elles ne peuvent pas être reconstituées; il est nécessaire de recourir aux dernières données sauvegardées.

DMIA mesure la durée d'interruption de fonctionnement du processus au-delà duquel les conséquences deviennent intolérables ; plusieurs DMIA peuvent être définis quand il y a différents modes de service dégradés (i.e. une reprise par palliers).

Copyright - Tout droit réservé - OFPPT

Elaboration d'un plan de continuité d'activité

3 - Identifier, analyser, évaluer et traiter les risques

Au cours de cette troisième étape, il faut concrètement :

- **Apprécier** les différents risques, c'est-à-dire les identifier ;
- Les **analyser** (selon les critères de probabilité et de gravité) en les intégrant à des scénarios significatifs (exemple : une crue majeure de la Seine à Paris, une pandémie grippale, une attaque informatique en déni de service…etc.) ;
- **Evaluer** ces risques en fonction du contexte et des enjeux pour l'organisation.

Exemple de matrice pour l'évaluation des risques

Une fois appréciés et classés, les risques doivent faire l'objet d'une stratégie de traitement intégrant différentes approches (prise, refus, maîtrise, transfert, partage) :

	Impacts				
Probabilité	Catastrophique 5	Majeur 4	Modéré 3	Mineur 2	Insignifiant 1
Très forte 5	10	9	8	7	6
Forte 4	9	8	7	6	5
Moyenne 3	8	7	6	5	4
Faible 2	7	6	5	4	3
Très faible 1	6	5	4	3	2

Niveau de risque encouru

9 ≤ Risque extrême ≤ 10	7 ≤ Risque élevé ≤ 8	5 ≤ Risque moyen ≤ 6	1 ≤ Risque faible ≤ 4

PARTIE 1

Copyright - Tout droit réservé - OFPPT

Elaboration d'un plan de continuité d'activité

4 - Définir la stratégie de continuité d'activité

4.1 - Choisir les scénarios à prendre en compte

Les actions de prévention et de protection évoquées précédemment ont permis de réduire les risques, mais pas de les supprimer. Des risques résiduels demeurent. Ils ont une probabilité d'occurrence et peuvent conduire à une perte de ressources critiques susceptible d'entraîner une interruption d'activité au-delà du seuil acceptable, ou une diminution du niveau de service en deçà du seuil minimum prédéfini. Ces risques, constitutifs de scénarios, devront être traités dans le cadre du PCA.

Exemple de cartographie synthétique de scénarios de risques

		Probabilité d'occurrence			
		Faible	**Modérée**	**Forte**	**Elevée**
Risque	**Elévé**		*R2 : Site informatique indisponible*	**R1 : Batiment impraticable R3 : Cyber attaque**	
	Fort		R8 : Coupure alimentation electrique	*R4 : Fournisseur défaillant R9 : Coupure physique fibre optique*	
	Modéré		R6 : Indisponibilité massive RH	R10 : Interdiction préfectorale d'accès dans les locaux	*R5 : Inondation fluviale*
	Faible		R7 : Mouvement social		

Le travail de gestion des risques a permis de les caractériser en termes de vraisemblance et d'impact.
Les données correspondantes seront prises en compte pour élaborer la stratégie du plan de continuité. Mais auparavant il est nécessaire de formaliser les moyens et procédures nécessaires et d'apprécier leurs coûts.

PARTIE 1

Copyright - Tout droit réservé - OFPPT

Elaboration d'un plan de continuité d'activité

4 - Définir la stratégie de continuité d'activité

4.2 - Identifier les moyens et décliner les effets à obtenir sous forme de procédures

La mise en œuvre d'un PCA repose sur des moyens identifiés et des procédures déclinées avant la survenue d'un scénario de crise. Après le sinistre, la cellule de crise pourra activer ces moyens et procédures du PCA afin de permettre une reprise partielle puis totale de l'activité. Les moyens et procédures à mettre en place couvrent en premier lieu les ressources critiques identifiées. La reprise d'activité doit par conséquent se préparer :

- ✓ En identifiant ou en créant des ressources redondantes non susceptibles d'être affectées par le sinistre ;
- ✓ En s'offrant la possibilité de faire appel, dans des délais adaptés, à des ressources externes ;
- ✓ En appliquant des procédures de sauvegarde des données adaptées aux exigences en termes de perte de données maximale admissible ;
- ✓ En disposant d'une organisation, d'une architecture technique et de procédures qui vont permettre le fonctionnement du centre de secours dans les délais prescrits et pour les applications prioritaires.

❖ ***Prendre en compte les interdépendances pour limiter les effets en cascade***

La problématique des interdépendances et des effets en cascade impose d'adopter une stratégie spécifique vis-à-vis des partenaires (prestataires et fournisseurs externes) afin de transposer les exigences internes de continuité vers l'extérieur. Ces exigences pouvant être quantifiées, l'enjeu est alors de les internaliser ou de les traduire en termes contractuels accompagnés de contrôles et de dispositifs de coordination durant une crise. Elles peuvent aussi se traduire par des mécanismes de travail en mode collaboratif avec le partage des analyses et du traitement du risque, l'élaboration coordonnée de la stratégie de continuité et la conduite d'exercices communs.

Copyright - Tout droit réservé - OFPPT

Elaboration d'un plan de continuité d'activité

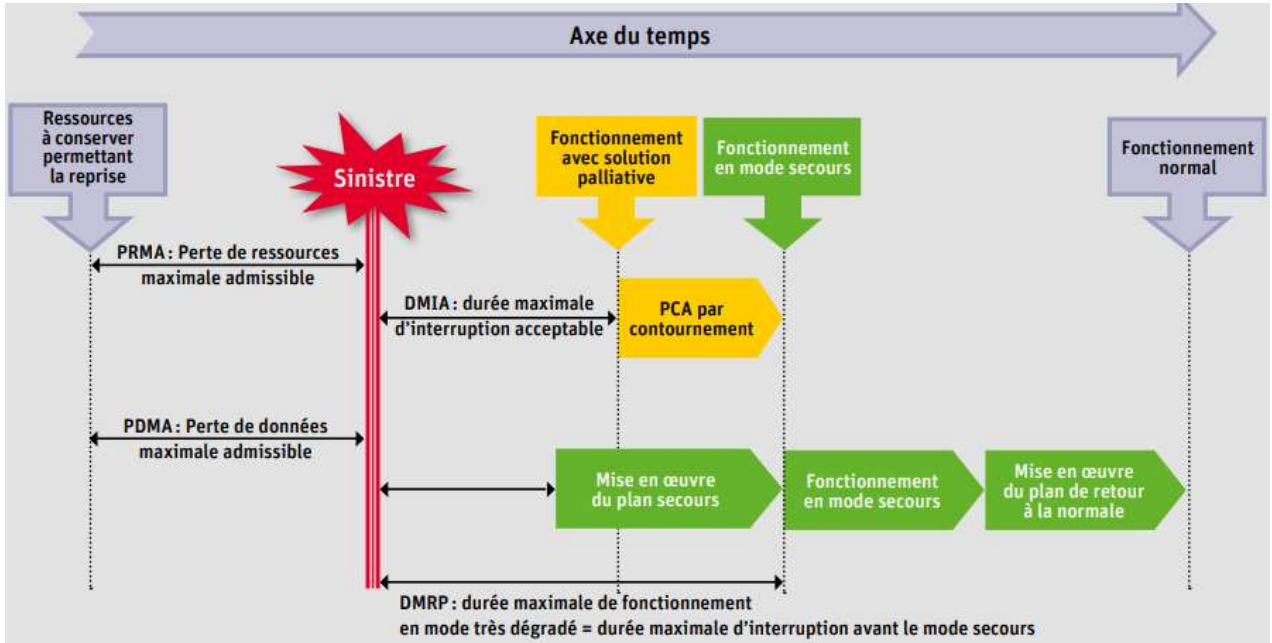
4 - Définir la stratégie de continuité d'activité

4.3 - Arrêter et décliner la stratégie de continuité

La détermination de la stratégie de continuité d'activité consiste en l'identification des effets à produire et à coordonner dans l'espace et dans le temps afin de maintenir l'activité de l'organisation à un niveau prédéfini malgré l'occurrence des scénarios de risques qui ont été retenus.

L'optimisation fonctionnelle de cette stratégie résulte d'une analyse comparée des avantages et des inconvénients. D'un point de vue économique, cette optimisation peut être caractérisée en comparant le coût de mise en place du PCA avec les bénéfices attendus (absence d'interruption d'activité au-delà du seuil défini pondéré par la probabilité de survenance, nouvelles opportunités générées par la continuité de cette activité, etc.). Voir figure ci-contre.

Une fois la stratégie arrêtée et déclinée en plan d'actions, les moyens à mettre en place et le dispositif de déclenchement doivent être définis afin de garantir le respect des objectifs de continuité fixés, dans le cadre du budget dédié. Les procédures associées doivent être intégrées dans les procédures de l'organisme en temps normal et durant la phase de gestion de crise.



PDMA mesure le temps maximum acceptable durant lequel les données sont perdues, car elles ne peuvent pas être reconstituées ; il est nécessaire de recourir aux dernières données sauvegardées.

DMIA mesure la durée d'interruption de fonctionnement du processus au-delà duquel les conséquences deviennent intolérables.

DMRP (délai maximum de reprise technique prévu) mesure la durée d'interruption de fonctionnement des parties techniques du processus avant la reprise en mode secours. Cela correspond à la durée maximale de fonctionnement acceptable en mode très dégradé.

PARTIE 1

Copyright - Tout droit réservé - OFPPT

Elaboration d'un plan de continuité d'activité

5 - Mettre en œuvre et assurer l'appropriation

5.1 - Mise en place du plan

Au terme des travaux décrits précédemment, il est possible de rédiger le plan de continuité d'activité qui va décrire la démarche logique ayant conduit au choix de la stratégie de continuité et de la réponse aux différents scénarios de crise retenus. Cette réponse consiste à préciser les moyens et à documenter les procédures qu'il conviendra de mettre en œuvre en fonction des dispositifs du PCA qui seront activés par la cellule de crise.

Les procédures spécifiques au PCA doivent être parfaitement intégrées aux procédures normales afin d'être comprises et aisément activées en situation d'urgence. Les responsables de ces moyens et procédures doivent être clairement identifiés ainsi que leur rôle et les actions attendues de leur part. La documentation doit être facilement accessible en cas de besoin et être aisément comprise. Elle doit être modifiable facilement pour permettre au PCA d'évoluer.

A ce stade il est nécessaire de s'assurer de :

- ✓ La disponibilité effective des ressources ;
- ✓ La connaissance et la bonne compréhension des procédures.

Cette tâche est beaucoup plus difficile quand on s'adresse à des prestataires externes, qui ne sont pas sous le contrôle de l'organisation. Cependant, les mêmes principes doivent s'appliquer, avec, selon le cas, un contrôle direct, un contrôle documentaire, une certification par un tiers et/ou la participation à des tests ou exercices.

Copyright - Tout droit réservé - OFPPT

Elaboration d'un plan de continuité d'activité

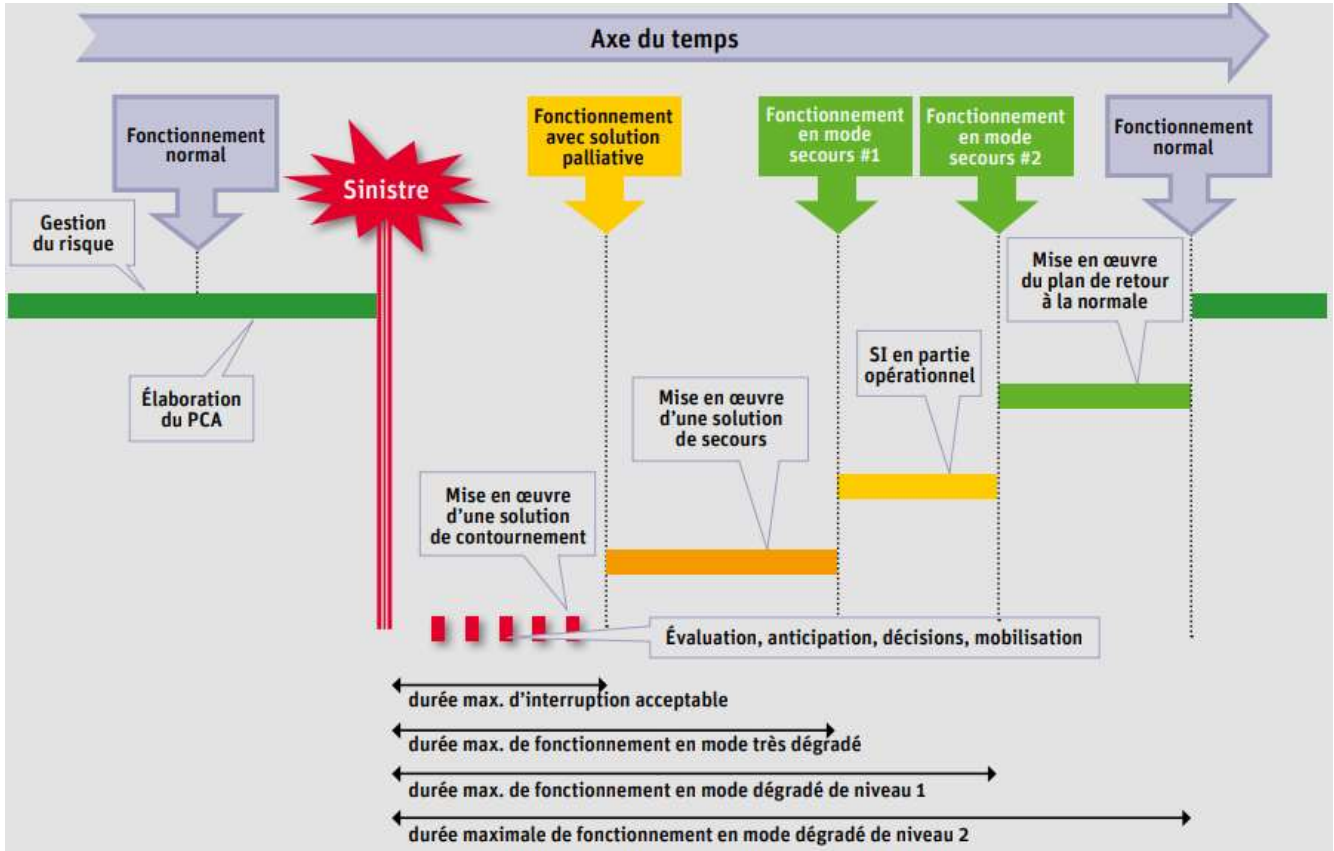
5 - Mettre en œuvre et assurer l'appropriation

5.2 - Déclenchement du plan

La cellule de crise joue un rôle clé dans l'activation des dispositifs du PCA les plus adaptés à la situation. Elle doit assurer la coordination des parties prenantes, en donnant les consignes de déclenchement des procédures préétablies et en s'assurant de leur bonne mise en œuvre.

A contrario, dans le cas d'événements fréquents, des PCA peuvent être activés en mode « réflexe », sans qu'il y ait nécessairement besoin de disposer d'une cellule de crise. Le PCA permet alors de gérer l'urgence et d'éviter la crise.

Ci-après la figure relative au déroulement du PCA.



Exemple d'un arrêt de l'activité suite à un sinistre, d'une reprise en mode dégradé, d'abord par une solution de contournement, puis par un fonctionnement en mode secours, avec deux paliers successifs, avant le retour à la normale.

PARTIE 1

Copyright - Tout droit réservé - OFPPT

Elaboration d'un plan de continuité d'activité

5 - Mettre en œuvre et assurer l'appropriation

5.3 - Déclenchement du plan, mesurer l'efficacité et faire évoluer le plan

Une fois que le PCA a été réalisé et que sa capacité à être mis en œuvre est garantie, il est nécessaire d'en vérifier l'efficacité. Le fonctionnement en mode dégradé et la reprise d'activité doivent se préparer en disposant de procédures testées préalablement. Afin de mesurer l'efficacité du PCA, il faut vérifier que la stratégie répond aux objectifs fixés, tels que :

- Maintenir la disponibilité des activités essentielles (tenir un niveau de DMIA spécifié pour chaque activité essentielle),
- Disposer d'indicateurs pour mesurer le niveau de l'activité normale et de l'activité en mode dégradé,
- Protéger le patrimoine applicatif et informationnel,
- Tenir la durée et le niveau de service assuré en mode dégradé, pour chaque activité essentielle, en cas de déclenchement du plan,
- Limiter la durée d'indisponibilité des activités essentielles de l'organisation et la quantité de données perdues en cas de déclenchement du plan, tant au moment de la bascule vers le site de secours qu'au retour vers le site principal,

Copyright - Tout droit réservé - OFPPT

Elaboration d'un plan de continuité d'activité

5 - Mettre en œuvre et assurer l'appropriation

5.3 - Déclenchement du plan, mesurer l'efficacité et faire évoluer le plan

- Assurer le traitement des besoins par ordre de priorité,
- Assurer le mode secours et le rétablissement selon les priorités établies,
- Ne pas dépasser le coût du PCA et réduire la complexité des solutions du PCA,
- S'appuyer sur l'analyse de risque des activités et des processus de l'organisation,
- Revoir cette analyse de risque en cas de découverte de nouveaux risques importants,
- Améliorer la résilience en étendant progressivement les scénarios pris en compte,
- Disposer d'une organisation rôdée et bien entrainée à réagir aux événements, y compris aux problèmes imprévus …

Différentes approches sont possibles mais en règle générale, il s'agit d'abord de faire vérifier les documents, idéalement par un « tiers de confiance », puis de tester la mise en œuvre des dispositifs (par exemple le basculement de certaines fonctions sur un site de secours), et enfin de vérifier par des exercices que les dispositifs et procédures de continuité sont connus, compris et peuvent être mis en œuvre dans les délais prescrits. Des indicateurs, tels que ceux proposés ci-dessus à titre indicatif, devront être définis et vérifiés à l'occasion d'exercices.

Copyright - Tout droit réservé - OFPPT

Quiz : Plan de continuité d'activité (PCA)

Question 1

Qu'est-ce que la continuité d'activité ?

1. La poursuite de l'activité d'une entreprise suite à une cession ou une transmission.
2. La poursuite de l'activité d'une entreprise suite à des incidents mineurs.
3. La poursuite des activités d'une entreprise, à la suite d'un événement perturbateur majeur.

Question 2

Quelle est la finalité de la continuité d'activité ? *Attention, plusieurs réponses sont possibles.*

1. Réduire des situations de crise.
2. Identifier les événements perturbateurs non maîtrisables dans un délai défini comme grave.
3. Assurer un fonctionnement normal de l'activité sans aucune dégradation de service.

Question 3

Pourquoi une entreprise doit-elle se préoccuper de continuité d'activité ? *Attention, plusieurs réponses sont possibles.*

1. C'est demandé par des clients.
2. C'est une amélioration de la productivité des activités.
3. C'est un avantage concurrentiel.

Copyright - Tout droit réservé - OFPPT

Quiz : Plan de continuité d'activité (PCA)

Question 4

Qu'apporte la norme ISO 22301 à une entreprise ? *Attention, plusieurs réponses sont possibles.*

1. Un gain de temps dans la mise en œuvre du SMCA.
2. La certitude que votre PCA fonctionnera en cas de besoin.
3. Un avantage concurrentiel.

Question 5

Quels sont les arguments utiles pour convaincre votre Direction générale de la nécessité d'assurer la continuité des activités ?

1. C'est est un moyen d'assurer la créativité des collaborateurs de notre entreprise.
2. C'est un moyen d'améliorer la productivité de notre entreprise.
3. C'est un moyen de protéger notre image publique et notre perte financière en cas de sinistre.

Question 6

Quelle fonction de l'entreprise doit réaliser le BIA ?

1. La Direction générale
2. Les directions d'activité de l'entreprise
3. Le responsable du plan de continuité d'activité
4. Le directeur de l'audit

Copyright - Tout droit réservé - OFPPT

Quiz : Plan de continuité d'activité (PCA)

Question 7

Parmi les solutions listées ci-dessous, quelles sont les solutions de prévention ? *Attention, plusieurs réponses sont possibles.*

1. Les systèmes de contrôle d'accès dans un bâtiment
2. Le secours informatique
3. La mise à jour régulière des logiciels de sécurité
4. Le site de repli des positions de travail

Question 8

Par quel scénario de risques faut-il commencer dans la mise en œuvre d'un PCA ?

1. Le plus fréquent
2. Le plus grave
3. Le plus risqué sur l'indisponibilité des activités critiques
4. Celui décidé par la Direction générale

Copyright - Tout droit réservé - OFPPT

Quiz : Plan de continuité d'activité (PCA) - Réponses

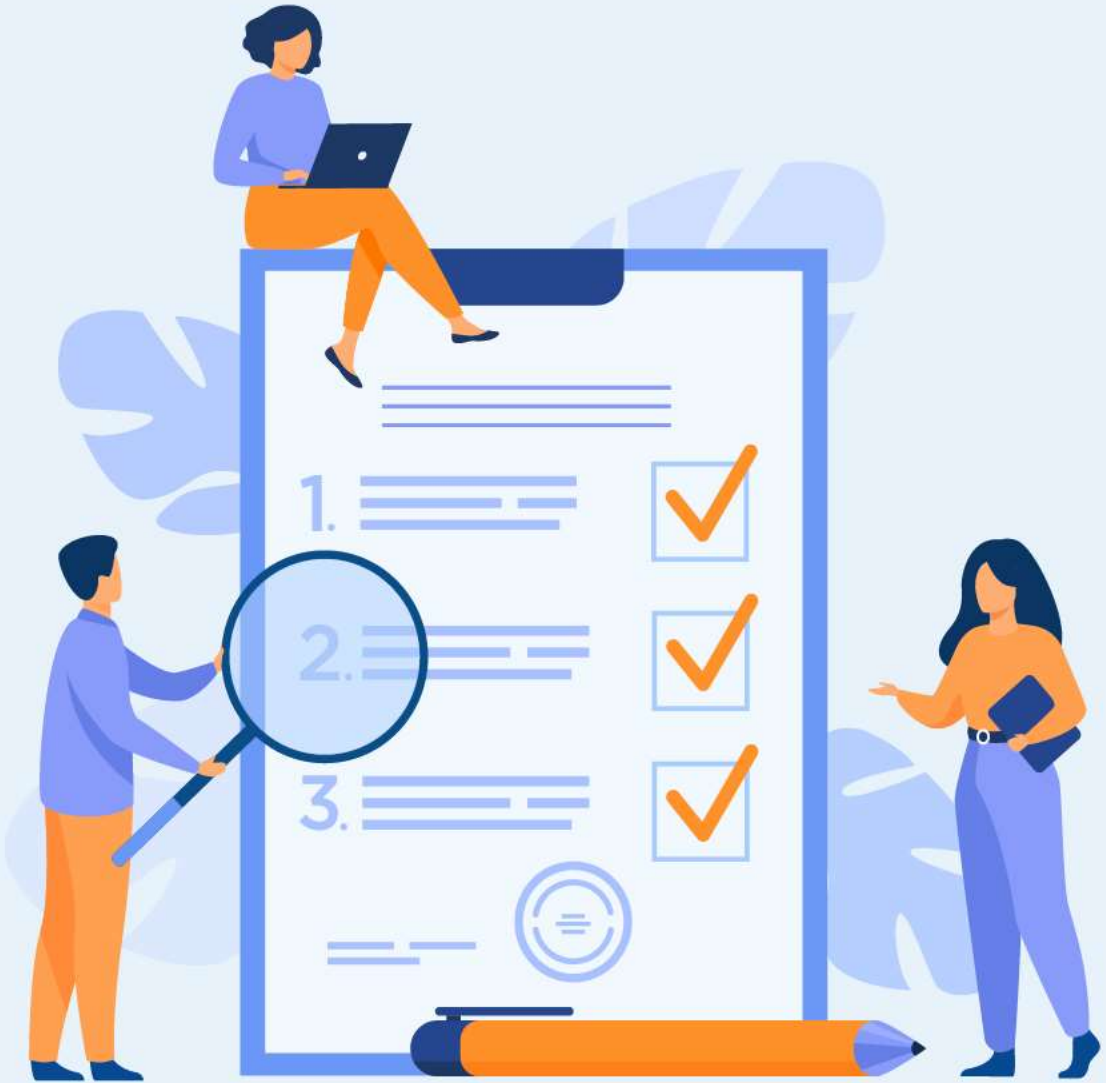
Questions	Réponses	Commentaires
1	3	*Un incident courant et non majeur est généralement traité dans le cadre du fonctionnement quotidien, et non dans le cadre de la continuité d'activité. La continuité d'activité concerne les activités d'une entreprise, à la suite d'un événement perturbateur majeur.*
2	1 et 2	*La continuité d'activité, par la mise en place de plans de continuité d'activité, anticipe la survenance de certains événements perturbateurs. Les situations de crise pour ces cas-là n'existent plus, le PCA prévu assurant la continuité d'activité.* *Les PCA sont prévus pour assurer la continuité d'activité au bout d'un délai maximum d'interruption admissible qui a été validé par la Direction générale.* *Le PCA est prévu pour assurer la continuité d'activité avec obligatoirement une dégradation de service validée par la Direction générale.*
3	1 et 3	*Les clients de l'entreprise peuvent exiger qu'elle se préoccupe de continuité d'activité pour que les produits ou services achetés soient fournis dans les délais. Cela peut être un critère choix de l'entreprise.* *Cela est un avantage concurrentiel qui peut faire l'objet de publicité commerciale.*
4	1 et 3	*Une norme est une bonne pratique définie par des experts internationaux. Son utilisation fait gagner du temps dans la mise en œuvre du SMCA et assure des plans de continuité d'activité de qualité.* *Bien que votre SMCA ait été construit selon ISO 22301, il est fort probable que les plans de continuité d'activité assureront la continuité d'activité dans le temps imparti. Mais, cela n'est pas certain à 100 %. Le risque humain, c'est-à-dire, par exemple, le manque d'une compétence à un moment donné pour exécuter une partie du plan de continuité d'activité, peut retarder la reprise d'activité. La gestion de crise doit traiter ce cas-là.* *Avoir un SMCA et des PCA est un avantage concurrentiel qui peut être communiqué.*

Copyright - Tout droit réservé - OFPPT

Quiz : Plan de continuité d'activité (PCA) - Réponses

Questions	Réponses	Commentaires
5	3	*La continuité d'activité n'a pas pour objet d'améliorer la productivité de l'entreprise. Son objectif est d'assurer la continuité d'activité de l'entreprise à la suite d'un sinistre.*
6	2	*Ce sont les directions des différentes activités de l'entreprise qui produisent des produits ou services, ou qui participent à cette production, qui sont consultées pour déterminer leurs besoins de continuité d'activité.* *La Direction générale intervient pour valider les besoins exprimés.* *Le RPCA – responsable du plan de continuité d'activité – et la direction de l'audit n'ont pas d' activités qui peuvent s'arrêter sans mettre en péril l'entreprise.*
7	1 et 3	*Les solutions de prévention sont mises en œuvre avant la survenance de l'événement perturbateur. Elles ont pour objectif de réduire sa probabilité de survenance.* *Les systèmes de contrôle d'accès dans un bâtiment réduisent la probabilité d'entrée dans le bâtiment.* *La mise à jour régulière des logiciels de sécurité réduit le nombre de cyberattaques pouvant réussir à perturber le SI.* *Par contre, les moyens de secours informatique et les positions de travail du site de repli ne sont pas des moyens de prévention, car ils ne réduisent pas la probabilité de survenance d'un événement perturbateur. Ils sont mis en place pour assurer la protection de l'entreprise.*
8	4	*C'est à la Direction générale de décider de la stratégie de continuité d'activité. En particulier, c'est elle qui doit décider par quel PCA il faut commencer.*

Copyright - Tout droit réservé - OFPPT



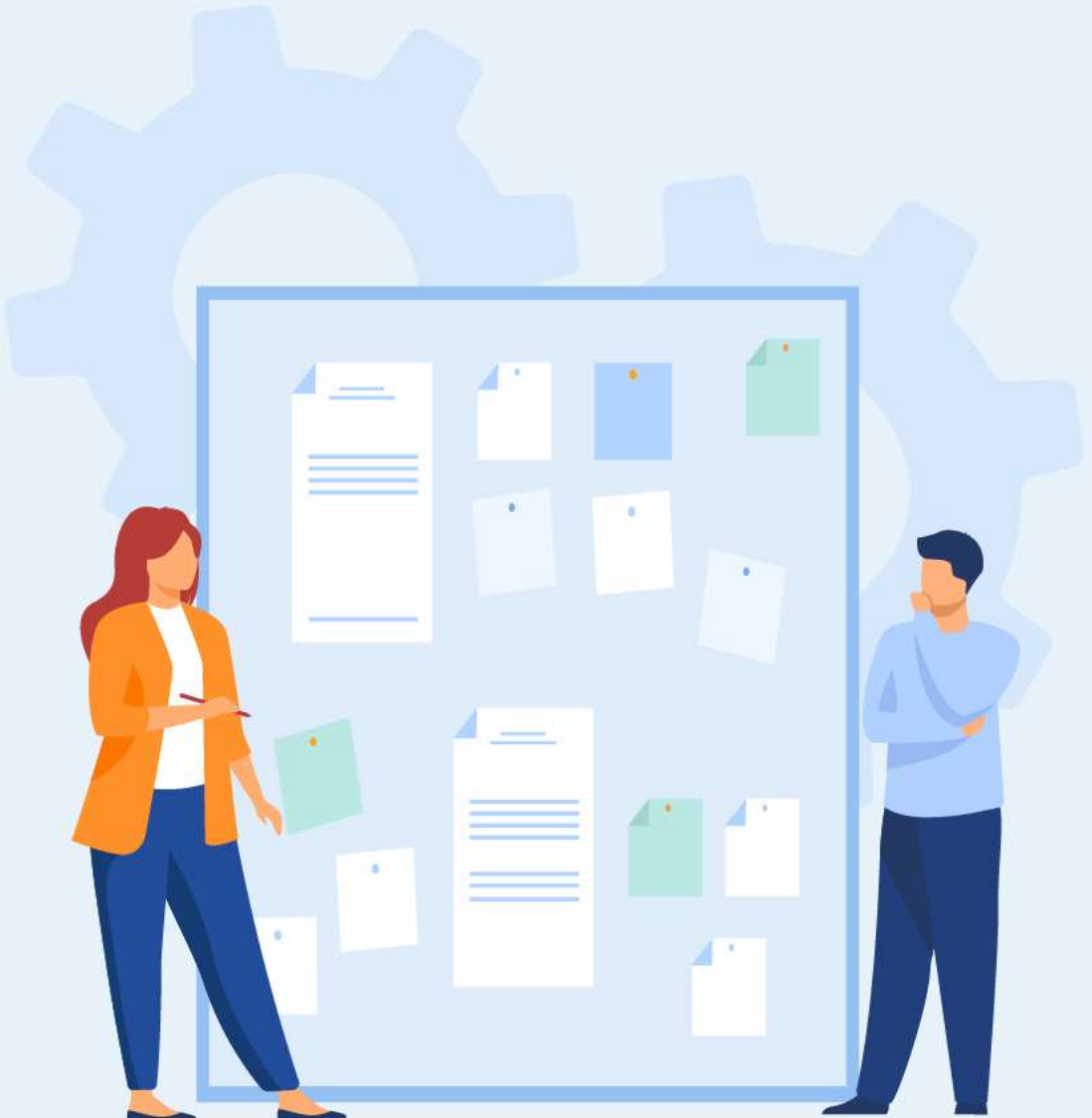
CHAPITRE 2

Appréhender le concept de Multi-Cloud

Ce que vous allez apprendre dans ce chapitre :

- Utiliser des solutions interopérables
- Connaître le principe d’un Cloud-Broker

5,5 heures



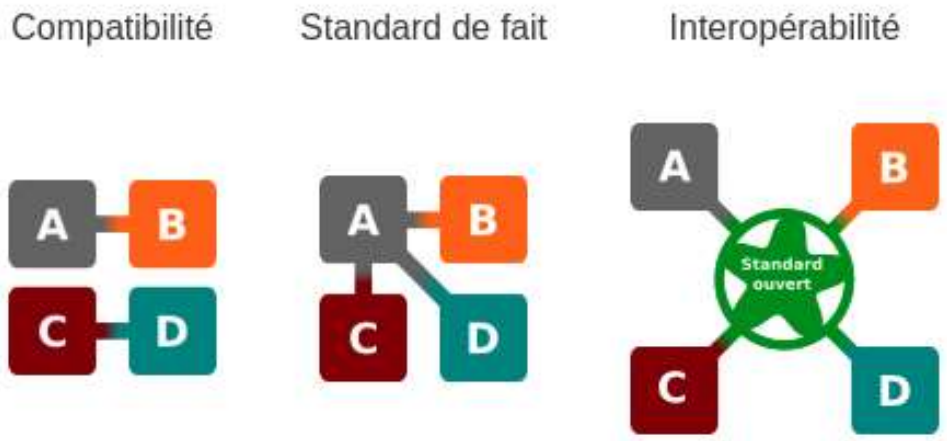
CHAPITRE 2

Appréhender le concept de Multi-Cloud

1. **Utilisation des solutions interopérables**
2. Connaitre le principe d’un Cloud-Broker

Définition de l'interopérabilité

L'interopérabilité est la capacité que possède un produit ou un système, dont les interfaces sont intégralement connues, à fonctionner avec d'autres produits, systèmes ou fournisseurs Cloud existants ou futurs et ce sans restriction ni surcoût ou perte de données.



Degré d'interopérabilité

Copyright - Tout droit réservé - OFPPT

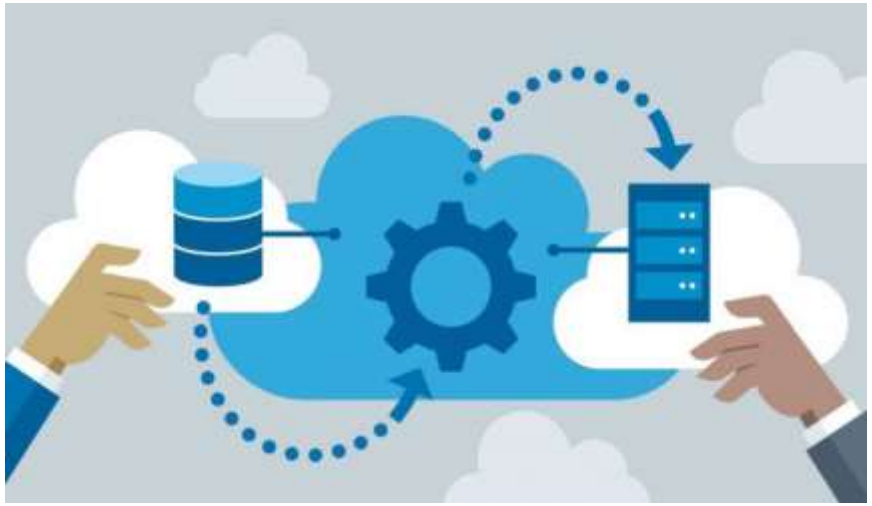
L'interopérabilité dans une stratégie Multi-Cloud

Les organisations qui ont opté pour une stratégie Multi-Cloud rencontrent des challenges en matière d'interopérabilité. Les experts proposent 4 bonnes pratiques pour traiter ces défis et favoriser la mise en place d'environnements Multi-Cloud efficaces.

Aujourd'hui, une majorité d'entreprises ont opté pour des stratégies Multi-Cloud : selon **Gartner**, plus de **80%** des entreprises utilisant le Cloud public ont plus de deux fournisseurs. Dans ce type d'environnement, l'interopérabilité est primordiale. Pour les entreprises, c'est un moyen de limiter le risque de dépendance vis-à-vis des fournisseurs, tout en assurant une meilleure continuité des activités et en offrant une plus grande flexibilité.

Pour mettre en place l'interopérabilité entre plusieurs Cloud, il faut des API, des conteneurs ainsi que des modèles communs de données. Des processus partagés sont bien évidemment requis pour que les composants hébergés sur des Cloud distants puissent communiquer efficacement et de manière fluide.

En outre, mettre en place une réelle interopérabilité passe forcément par la synchronisation des données en temps réel et par l'usage des composants de manière dynamique. Toute cela sans nuire aux performances des applications ni à leur sécurité. Raison pour laquelle les experts s'accordent à dire que l'interopérabilité en mode Multi-Cloud est un défi pour les entreprises.



Copyright - Tout droit réservé - OFPPT

Les principaux challenges de l'interopérabilité en environnement Multi-Cloud

En premier lieu elle parait évidente, la mise en place de l'interopérabilité n'est pas chose aisée. Les entreprises se heurtent à quelques réalités qui se dressent comme des freins, particulièrement de la part des fournisseurs qui ne jouent pas vraiment le jeu. Parmi lesquelles :

1. La disparité des technologies utilisées par chaque fournisseur Cloud qui se traduit par une grande diversité d'APIs et de modèles d'intégration de données, peu standardisée
2. La complexité des configurations entre applications SaaS qui rend la portabilité des données et des configurations entre applications SaaS encore peu assurée;
3. L'impact négatif de la portabilité des applications modulaires à base de microservices complexe à mettre en œuvre sur les performances;
4. Des technologies spécifiques à chaque fournisseur de Cloud qui préfèreraient conserver une exclusivité et privilégient les solutions propriétaires, qui nécessitent des investissements lourds en formation pour les clients;
5. Des notions de partage des responsabilités qui peuvent vite déboucher sur une situation confuse en termes de sécurité;
6. La spécialisation des développeurs sur une technologie Cloud donnée;
7. Le risque en matière de cybersécurité entrainé par la confusion autour du partage des responsabilités au niveau de l'écosystème Multi-Cloud.

Copyright - Tout droit réservé - OFPPT

Quatre bonnes pratiques pour aborder les challenges de l'interopérabilité

Pour résoudre ces problématiques, les entreprises peuvent se fier aux bonnes pratiques permettant de relever le défi de l'interopérabilité. Parmi les plus connues voici celles qui ont maintes fois fait leurs preuves :

1 - Evaluer le bon niveau d'adhérence avec les fournisseurs de Cloud actuels

Si ces derniers offrent la flexibilité et la résilience nécessaires pour répondre aux besoins de l'entreprise, l'interopérabilité n'est pas forcément une priorité. En revanche, si les fournisseurs actuels ne répondent pas à ces besoins, les organisations ont intérêt à évaluer ce qui peut rester chez ces derniers et ce qui peut être porté sur une autre plateforme.

2 - Recourir à des adaptateurs publics

Pour porter des applications d'une plateforme à une autre : de tels adaptateurs permettent de réduire de façon importante les coûts associés à l'interopérabilité.

3 - Recourir à des technologies standard (comme Open source)

En cours de développement, utiliser quand c'est possible des APIs et des conteneurs non liés à une plateforme spécifique. A l'heure actuelle, plusieurs acteurs travaillent pour élaborer ce type d'outils, afin d'aider les entreprises à partager des données et à assurer l'interopérabilité entre différentes plateformes Cloud.

4 - Privilégier les standards ouverts pour le Cloud

Citons notamment les initiatives du projet OpenStack, celle de l'IEEE et du NIST (Standard for InterCloud Interoperability and Federation) et celles de la Cloud Native Computing Foundation et de la Cloud Security Alliance. A noter cependant, certains de ces projets sont encore émergents et ont besoin d'être adoptés par les grands fournisseurs pour s'imposer plus largement.

Copyright - Tout droit réservé - OFPPT

Interopérabilité et la portabilité dans le Cloud

Les deux composants cruciaux de l'interopérabilité du Cloud sont la convivialité et la connectivité, qui sont elles-mêmes divisées en plusieurs couches dont la plus importantes est la portabilité.

La portabilité c'est le processus de transfert des données ou d'une application d'un fournisseur à un autre, en le rendant exécutable ou utilisable. La portabilité peut être séparée en deux types : la portabilité des données Cloud et la portabilité des applications Cloud.

1 - Portabilité des données Cloud

C'est la capacité de déplacer des informations d'un service Cloud à un autre et ainsi de suite sans s'attendre à ressaisir les données.

2 - Portabilité des applications Cloud

C'est la capacité de déplacer une application d'un service Cloud à un autre ou entre l'environnement d'un client et un service Cloud.

Copyright - Tout droit réservé - OFPPT

Catégories d'interopérabilité et de portabilité du Cloud

La portabilité et l'interopérabilité du Cloud peuvent être divisées en :

Portabilité des données

La portabilité des données, également appelée portabilité Cloud, fait référence au transfert de données d'une source à une autre source ou d'un service à un autre service, c'est-à-dire d'une application à une autre application ou d'un service Cloud à un autre service Cloud dans le but de fournir un meilleur service au client sans affecter sa convivialité. De plus, cela facilite le processus de migration vers le Cloud.

Portabilité des applications

Elle permet la réutilisation de divers composants d'application dans différents services Cloud PaaS. Si les composants sont indépendants de leur fournisseur de services Cloud, la portabilité des applications peut être une tâche difficile pour l'entreprise. Mais si les composants ne sont pas spécifiques à une plate-forme, le portage vers une autre plate-forme est simple et sans effort.

Portabilité de la plateforme

Il existe deux types de portabilité de la plateforme : la portabilité de la source de la plate-forme et la portabilité de l'image machine. Dans le cas de la plate-forme, la portabilité des sources, par exemple UNIX OS, qui est principalement écrit en langage C, peut être implémentée en recompilant sur différents matériels et en réécrivant des sections dépendantes du matériel qui ne sont pas codées en C. Image machine la portabilité lie l'application à la plate-forme en portant le bundle résultant qui nécessite une représentation de programme standard.

Copyright - Tout droit réservé - OFPPT

Catégories d'interopérabilité et de portabilité du Cloud

Interopérabilité des applications

Il s'agit de l'interopérabilité entre les composants déployés d'une application déployée dans un système. Généralement, les applications construites sur la base de principes de conception présentent une meilleure interopérabilité que celles qui ne le sont pas.

Interopérabilité de la plateforme

Il s'agit de l'interopérabilité entre les composants déployés des plates-formes déployées dans un système. C'est un aspect important, car l'interopérabilité des applications ne peut être atteinte sans l'interopérabilité des plates-formes.

Interopérabilité de gestion

Ici, les services Cloud tels que SaaS, PaaS ou IaaS et les applications liées au libre-service sont évalués. Il serait prédominant car les services Cloud permettent aux entreprises de travailler en interne et d'éradiquer la dépendance vis-à-vis des tiers.

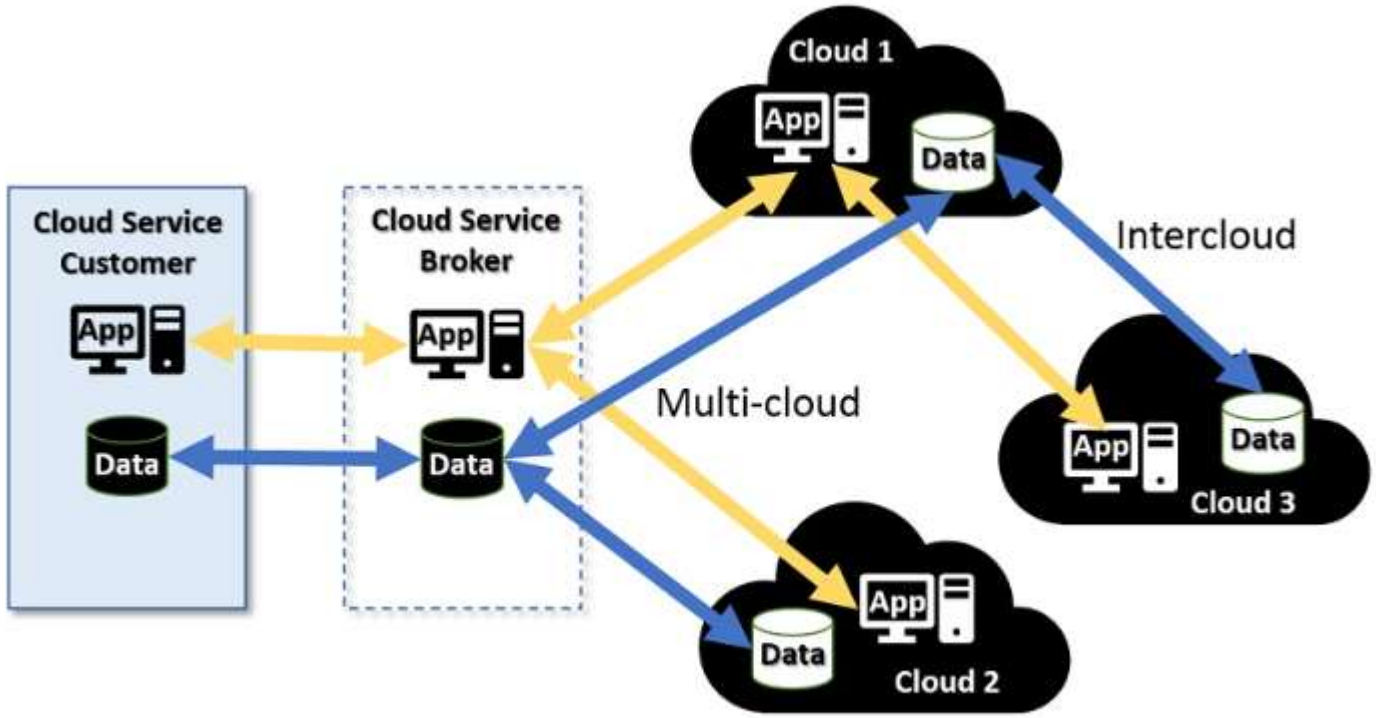
Interopérabilité de publication et d'acquisition

Généralement, il s'agit de l'interopérabilité entre différentes plates-formes telles que les services PaaS et le marché en ligne.

Copyright - Tout droit réservé - OFPPT

Principaux scenarios interopérabilité et de portabilité du Cloud

La figure ci-dessous représente un aperçu des scénarios où l'interopérabilité et la portabilité sont requises dans le Cloud : (Selon guide établi par le Cloud Standards Custom Council - **CSCC**)



PARTIE 1

Copyright - Tout droit réservé - OFPPT

Principaux scenarios interopérabilité et de portabilité du Cloud

Cloud Standards Custom Council (CSCC) a identifié certains des scénarios de base où la portabilité et l'interopérabilité sont requises.

1. **Basculement entre les fournisseurs de services Cloud :** Le client souhaite transférer des données ou des applications du Cloud 1 vers le Cloud 2.
2. **Utilisation de plusieurs fournisseurs de services Cloud** : Le client peut s'abonner au même service ou à des services différents, par exemple Cloud 1 et 2.
3. **Services Cloud directement liés :** Le client peut utiliser le service en se connectant au Cloud 1 et au Cloud 3.
4. **Configuration de Cloud hybride :** Ici, le client se connecte à un système hérité non pas dans un Cloud public, mais privé, c'est-à-dire Cloud 1, qui est ensuite connecté aux services de Cloud public, c'est-à-dire Cloud 3.
5. **Migration Cloud :** Les clients migrent vers une ou plusieurs applications internes vers le Cloud 1.

Copyright - Tout droit réservé - OFPPT

Solutions interopérables

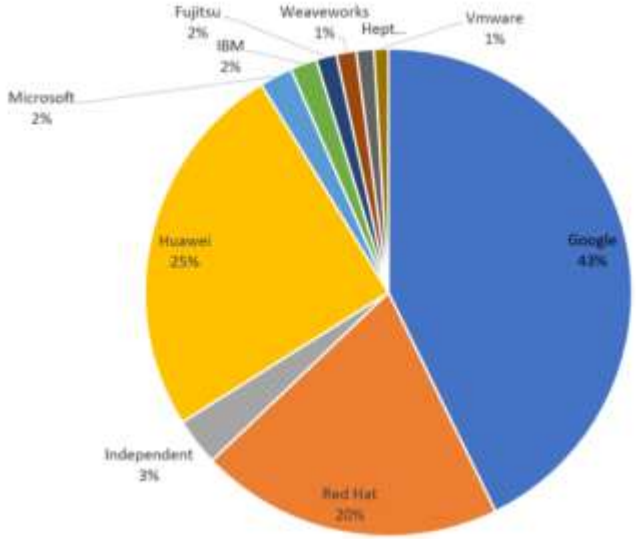
L'interopérabilité Cloud élimine les parties complexes en fournissant des interfaces personnalisées. Passer d'un fournisseur à un autre peut être concevable avec un service de conteneur qui améliore l'évolutivité. Avoir quelques obstacles, une adaptabilité au changement des fournisseurs de services, une meilleure assistance aux clients du Cloud renforceront l'amélioration de l'interopérabilité du Cloud.

Afin d'augmenter le niveau d'interopérabilité des solution, il faut que les développeurs prennent en considération lors de la mise en œuvre du projet, l'utilisation des standards ainsi que l'adoption des solution Open source indépendantes des fournisseurs Cloud.

Aussi, l'adoption des technologies de **conteneurisation et d'orchestration à base de Kubernetes** favorisent l'interopérabilité des solutions.

Bien que poussé au tout départ par Google, Kubernetes devient un standard de fait. En particulier parce que Red Hat, Huawei, Microsoft… sont nombreux à avoir rejoint le projet.

Ci-après le top 10 des contributeurs Kubernetes par organisation.

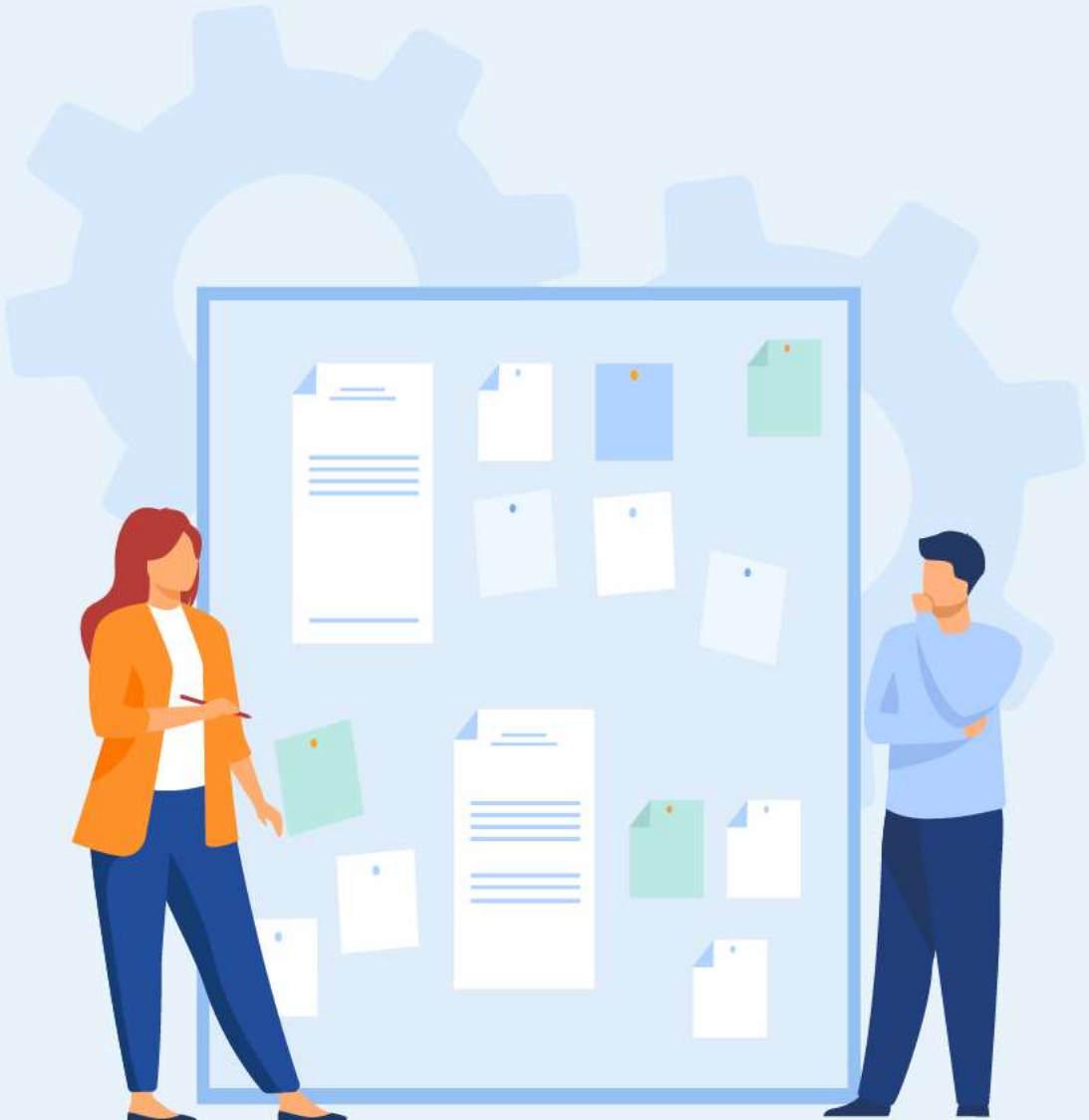


Aujourd'hui, s'appuyer sur Kubernetes, que containeriser la solution proposée, permet de garder la main quant à sa stratégie d'hébergement : Cloud, en prémisse, Multi-Cloud, Couplé à cette vision, vos projets de gestion de données trouvent immédiatement portabilité, modularisation, mises à jour régulières (livraison continue), fort niveau de service (SLA, haute disponibilité, réplication…), sécurisation (sécurité réseau, chiffrement des données…).

Kubernetes offre une nouvelle manière de voir le Cloud et rassure grandement quant à l'interopérabilité.

PARTIE 1

Copyright - Tout droit réservé - OFPPT



CHAPITRE 2

Appréhender le concept de Multi-Cloud

1. Utiliser des solutions interopérables
2. **Connaitre le principe d’un Cloud-Broker**

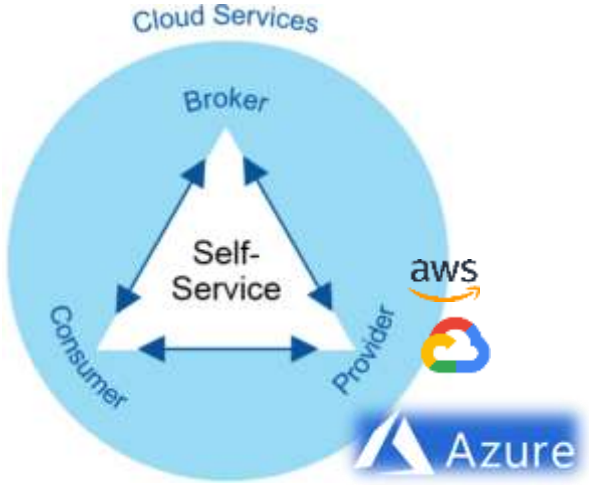
C'est quoi un Cloud-Broker ?

Un **Cloud broker**, ou **courtier** de services dans le Cloud, fait office **d'intermédiaire** entre le fournisseur Cloud et l'utilisateur. Ainsi au lieu de s'adresser directement à un fournisseur de services Cloud, une entreprise qui souhaite utiliser de tels services peut s'adresser à un Cloud Broker.

En fonction des besoins, du secteur d'activité, et du budget de son client, le Cloud Broker **passera en revue différents fournisseurs Cloud** afin de choisir celui qui convient le mieux. En règle générale, il fournira aussi à son client des conseils et des informations sur la façon d'utiliser le Cloud Computing pour atteindre ses objectifs. Il peut donc aussi lui suggérer différents types de services Cloud.

Par la suite, le client peut contacter les fournisseurs de services sélectionnés par le broker. Cependant, certains brokers proposent aussi de négocier directement les contrats avec les fournisseurs. D'ailleurs, le Cloud Broker peut décider de répartir les services entre plusieurs vendeurs pour réduire les coûts au maximum. Il s'agit là d'une stratégie multi-Cloud.

Certains d'entre eux vont encore plus loin, en fournissant à leurs clients des interfaces propriétaires permettant d'utiliser des services Cloud de multiples fournisseurs sans aucune difficulté comme s'ils étaient tous fournis par le même vendeur. On peut alors aussi parler d'un « agrégateur de Cloud » .



Copyright - Tout droit réservé - OFPPT

Les rôles d'un Cloud-Broker

Il y a trois domaines principaux qu'un courtier en services de Cloud peut aborder pour accélérer l'adoption du Cloud :

Le négociateur

il peut être mandaté pour négocier des contrats. Dans ce cas, il peut répartir les services entre divers fournisseurs dans un souci d'économie maximale, malgré les éventuelles complexités engendrées par les négociations impliquant plusieurs fournisseurs. Une fois la recherche terminée, le courtier présente au client une liste de fournisseurs recommandés ainsi qu'une comparaison des caractéristiques du service, des ventilations des coûts, des SLA et d'autres critères.

L'agrégateur de services

il combine et intègre plusieurs services en un ou plusieurs nouveaux services. Il assure l'intégration des données et les connexions sécurisées entre son client et les multiples fournisseurs de Cloud. Il peut choisir les services de plusieurs fournisseurs, selon les critères déterminés auparavant avec son client.

La personnalisation

il peut améliorer un service donné en optimisant certaines capacités spécifiques ou en proposant des services à valeur ajoutée ou personnalisés. Cette amélioration peut concerner la gestion de l'accès aux services Cloud, le contrôle des identités, les rapports de performance, etc.

Copyright - Tout droit réservé - OFPPT

Les avantages à recourir à un Cloud-Broker

De manière générale, faire appel à un Cloud broker peut présenter trois intérêts principaux :

Amélioration de la continuité des activités

En réduisant la dépendance à l'égard d'un seul fournisseur de Cloud. Si c'est l'un des souhaits de l'entreprise, ce courtier sélectionnera les services les mieux adaptés et disponibles sur différentes plates-formes. Il proposera également des outils permettant à ses clients de surveiller l'évolution des performances des services retenus tout en faisant abstraction de la complexité fonctionnelle et technique.

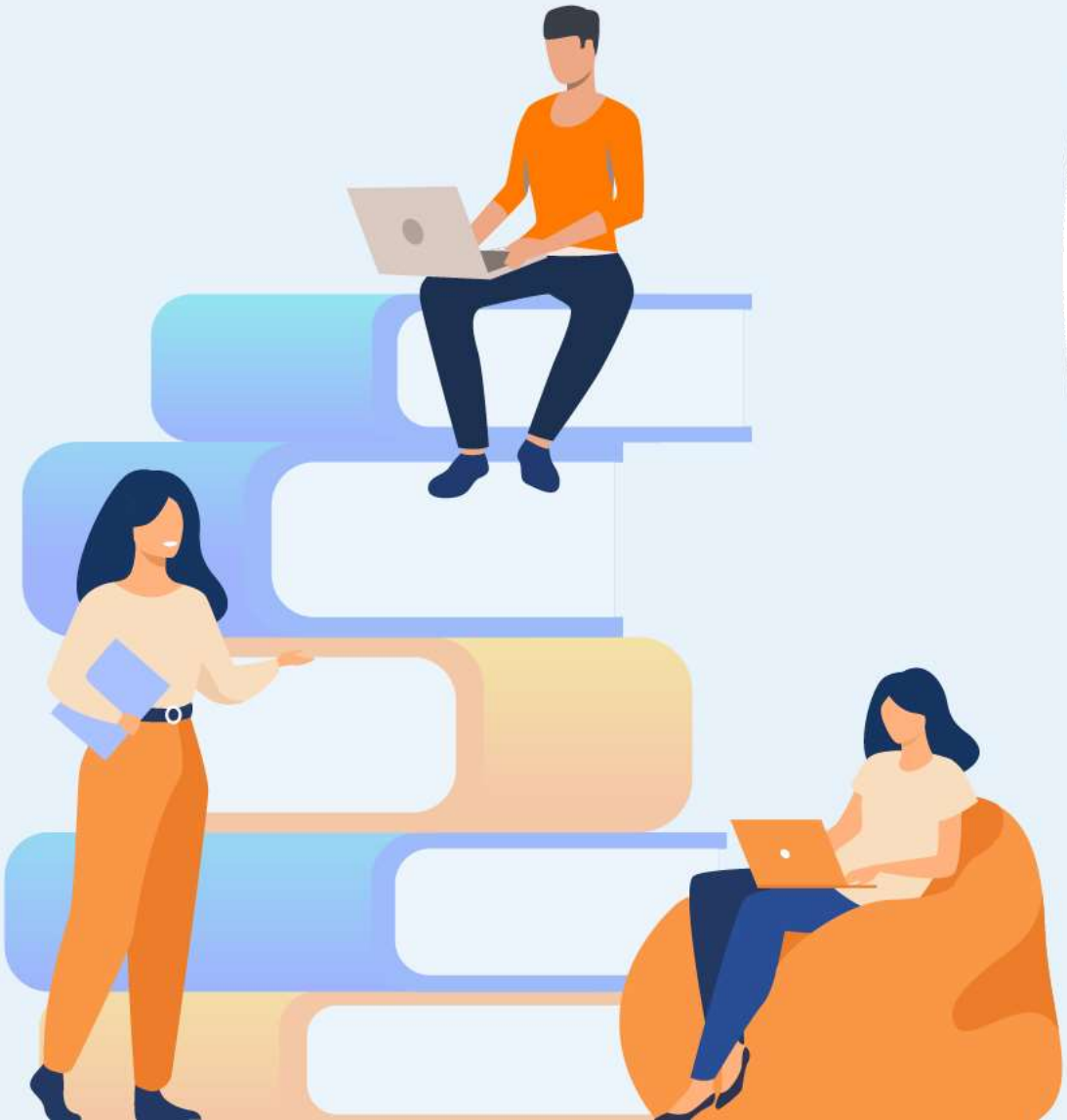
Réduction des coûts

Un courtier peut obtenir plus facilement des réductions, car il négocie de plus gros volumes de services. Parallèlement, ce spécialiste doit fournir une visibilité complète sur les coûts et établir des projections budgétaires de consommation de services en fonction des projets.

Renforcement de la sécurité des données

Avant d'entamer la migration d'applications ou d'informations vers une plate-forme, le Cloud broker peut vérifier si les fournisseurs sélectionnés répondent parfaitement aux normes de sécurité exigées. Il peut s'agir de normes ou de certifications imposées dans des secteurs très réglementés tels que la santé et les services financiers.

Copyright - Tout droit réservé - OFPPT



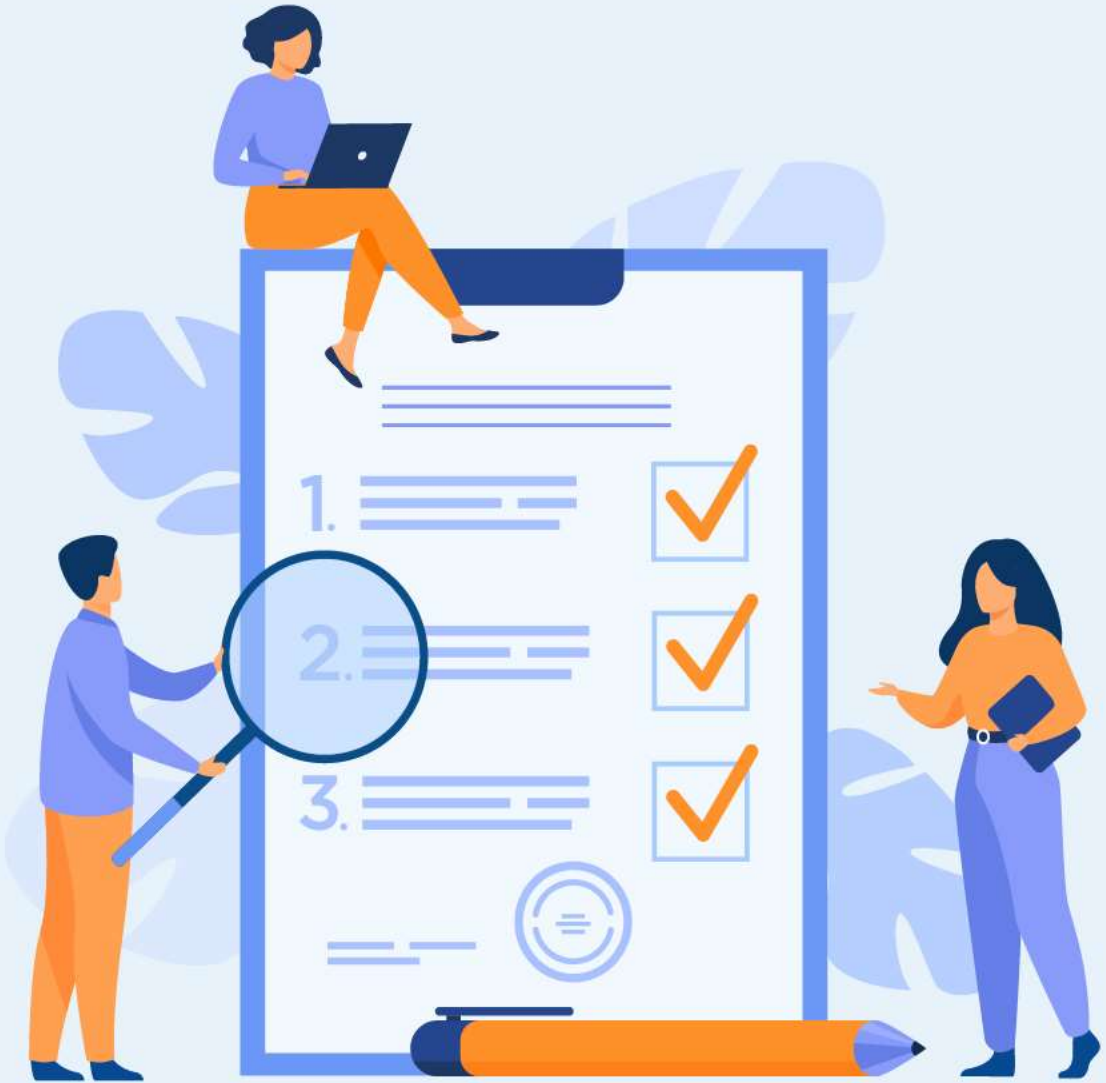
PARTIE 2

Répliquer une activité sur le Cloud

Dans ce module, vous allez :

- Découvrir les plans de récupération sur Azure
- Apprendre les notions de réplication et de basculement
- Différencier entre une réplication asynchrone et synchrone
- Découvrir la notion géo basculement

18 heures



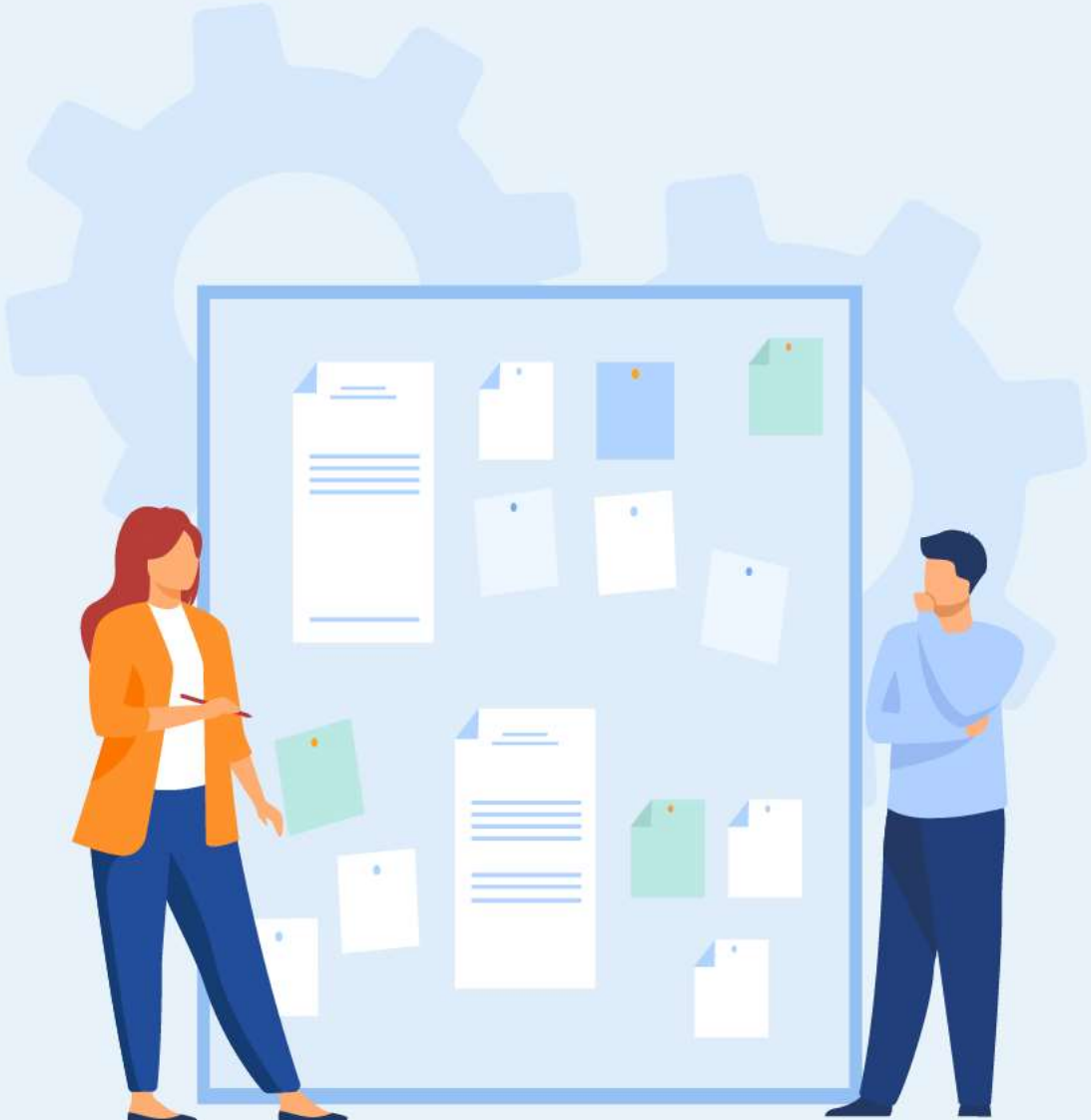
CHAPITRE 1

Créer des plans de récupération

Ce que vous allez apprendre dans ce chapitre :

- Processus de basculement
- Auto-déploiement
- Réplication synchrone
- Réplication asynchrone

10 heures



CHAPITRE 1

Créer des plans de récupération

1. **Processus de basculement**
2. Auto-déploiement
3. Réplication synchrone
4. Réplication asynchrone

À propos du plan de récupération

Un plan de récupération rassemble les machines dans des groupes de récupération à des fins de basculement. Il permet aussi de définir un processus de récupération systématique en créant de petites unités indépendantes qu'on peut basculer. Une unité représente généralement une application dans un environnement.

- Un plan de récupération définit comment les machines basculent et l'ordre dans lequel elles démarrent après un basculement.
- On peut utiliser des plans de récupération pour le basculement vers Azure et la restauration automatique à partir d'Azure.
- On peut ajouter jusqu'à 100 instances protégées à un même plan de récupération.
- On peut personnaliser un plan en y ajoutant un ordre, des instructions et des tâches.
- Lorsqu'un plan est défini, on peut basculer vers celui-ci.
- Les machines peuvent être référencées dans plusieurs plans de récupération, dans lesquels les plans suivants ignoreront le déploiement/démarrage d'une machine si elle a été déployée au préalable à l'aide d'un autre plan de récupération.

Pourquoi utiliser un plan de récupération ?

Utilisez des plans de récupération pour :

- Modéliser une application autour de ses dépendances.
- Automatiser les tâches de récupération pour réduire l'objectif de délai de récupération (RTO).
- Vérifier qu'on est prêt pour la migration ou la récupération d'urgence en s'assurant que les applications font partie d'un plan de récupération.
- Exécuter des tests de basculement sur des plans de récupération, pour s'assurer que la récupération d'urgence ou la migration fonctionne comme prévu.

Copyright - Tout droit réservé - OFPPT

Fonctionnement du basculement

Lorsqu'un serveur de restauration est créé, il reste en mode Veille. La machine virtuelle correspondante n'existe pas avant le lancement du basculement. Avant de lancer le processus de basculement, on doit créer au moins une sauvegarde d'image de disque (avec volume démarrable) de votre machine d'origine.

Lors du lancement du processus de basculement, on sélectionne le point de reprise de l'ordinateur d'origine depuis lequel la machine virtuelle contenant les paramètres prédéfinis est créée. L'opération de basculement utilise la fonctionnalité « exécution d'une machine virtuelle à partir d'une sauvegarde ». Le serveur de restauration reçoit l'état de transition Finalisation. Ce processus implique le transfert des disques virtuels du serveur du stockage des sauvegardes (stockage « froid ») vers le stockage pour reprise d'activité après sinistre (stockage « chaud »).

Une fois la Finalisation terminée, les performances du serveur sont rétablies. L'état du serveur est modifié en Basculement. La ressource est désormais basculée de l'ordinateur d'origine vers le serveur de restauration du site dans le Cloud.

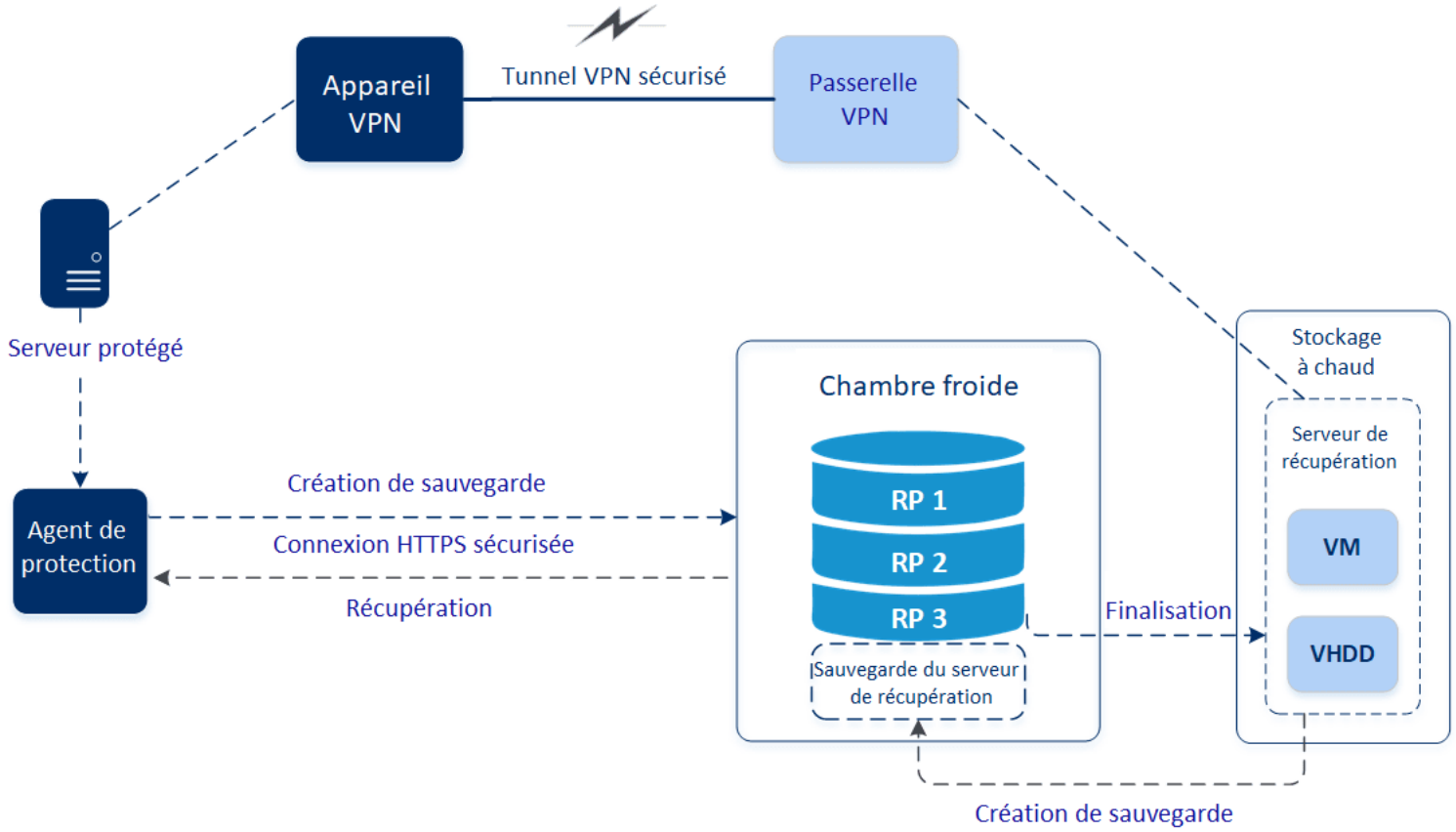
Si le composant de restauration possède un agent de protection, le service de l'agent est interrompu pour éviter toute interférence (notamment le démarrage d'une sauvegarde ou le signalement de statuts obsolètes au composant de sauvegarde).

Copyright - Tout droit réservé - OFPPT

PARTIE 2

Fonctionnement du basculement

Le diagramme ci-dessous, détaille le processus de basculement et de restauration automatique.



Copyright - Tout droit réservé - OFPPT

Tester un basculement

Lors d'un basculement test, une machine virtuelle n'est pas finalisée. Cela signifie que l'agent lit le contenu des disques virtuels directement depuis la sauvegarde, c-à-d. qu'il accède aléatoirement aux différentes parties de la sauvegarde. Ses performances peuvent être plus lentes que d'habitude.

Un basculement test consiste à démarrer un serveur de restauration dans un VLAN de test isolé du réseau de production. On peut tester plusieurs serveurs de restauration à la fois et vérifier leur interaction. Dans le réseau de test, les serveurs communiquent à l'aide de leur adresse IP de production, mais ils ne peuvent pas démarrer de connexions TCP ou UDP à des ressources situées sur le réseau local.

Bien que le basculement test soit facultatif, Il est recommandé de l'exécuter régulièrement, à une fréquence adéquate en matière de coût et de fiabilité. Une bonne pratique consiste à créer un **runbook** (dossier d'exploitation), c'est-à-dire un ensemble d'instructions décrivant comment lancer l'environnement de production dans le Cloud.

Copyright - Tout droit réservé - OFPPT

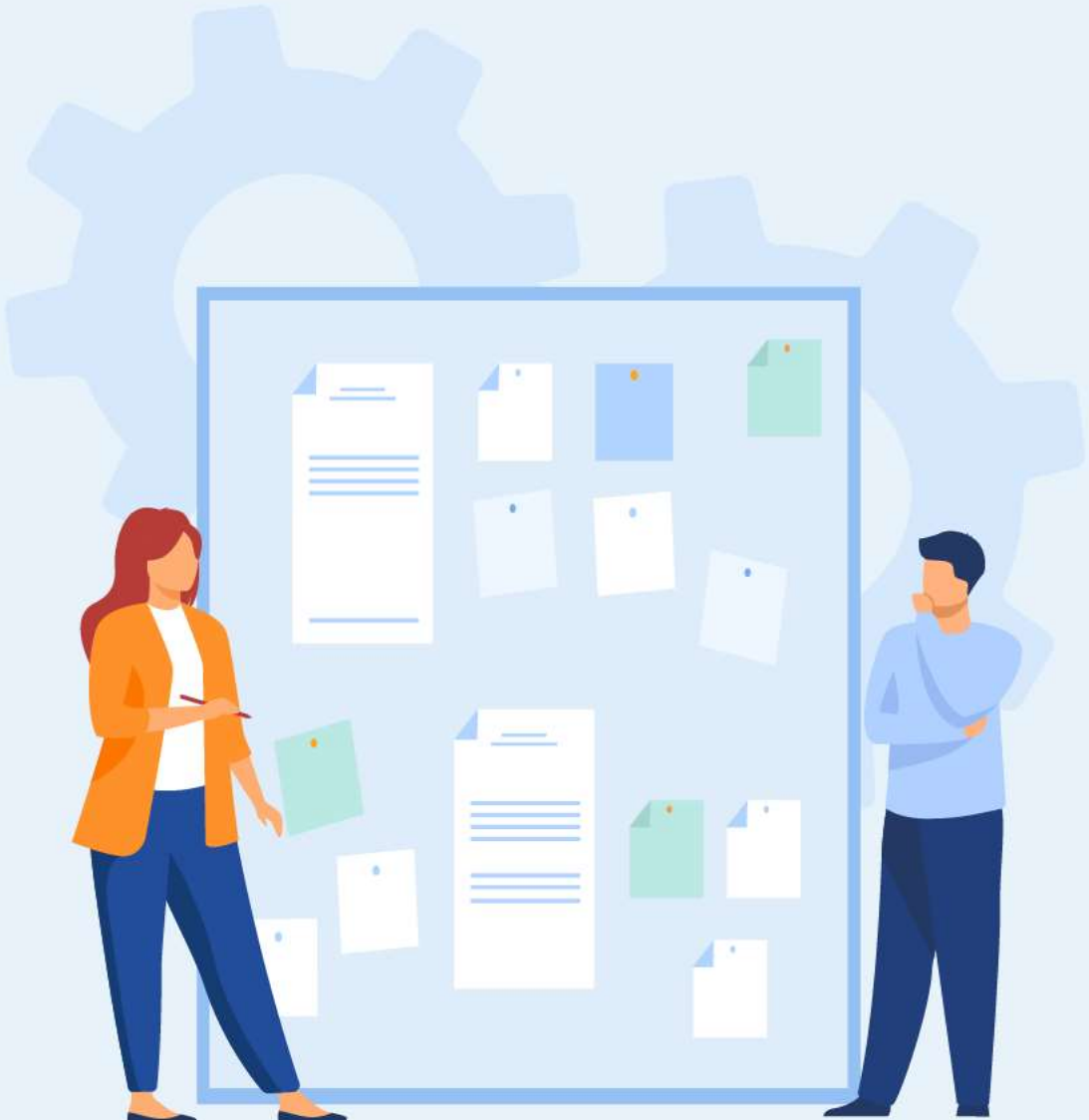
Configuration du basculement test automatisé

En configurant le basculement test automatisé, on peut tester le serveur de restauration tous les mois, sans aucune intervention manuelle.

Pour configurer le basculement test automatisé.

- ✓ Dans la console, accéder à **Reprise d'activité après sinistre > Serveurs > Serveurs de restauration**, puis sélectionner le serveur de restauration.
- ✓ Cliquer sur **Éditer**.
- ✓ Dans la section **Basculement test automatisé**, dans le champ **Planification**, sélectionner **Mensuel**.
- ✓ Dans la zone **Délai d'attente de capture d'écran**, indiquer la durée maximale (en minutes) pendant laquelle le système essaie d'effectuer un basculement test automatisé ou conserver la valeur par défaut.
- ✓ Si on veut conserver la valeur **Délai d'attente de capture d'écran** par défaut et on veut qu'elle soit renseignée automatiquement lorsqu'on active le basculement test automatisé des autres serveurs de restauration, sélectionner **Définir comme délai d'attente par défaut**.
- ✓ Enregistrer.

Copyright - Tout droit réservé - OFPPT



CHAPITRE 1

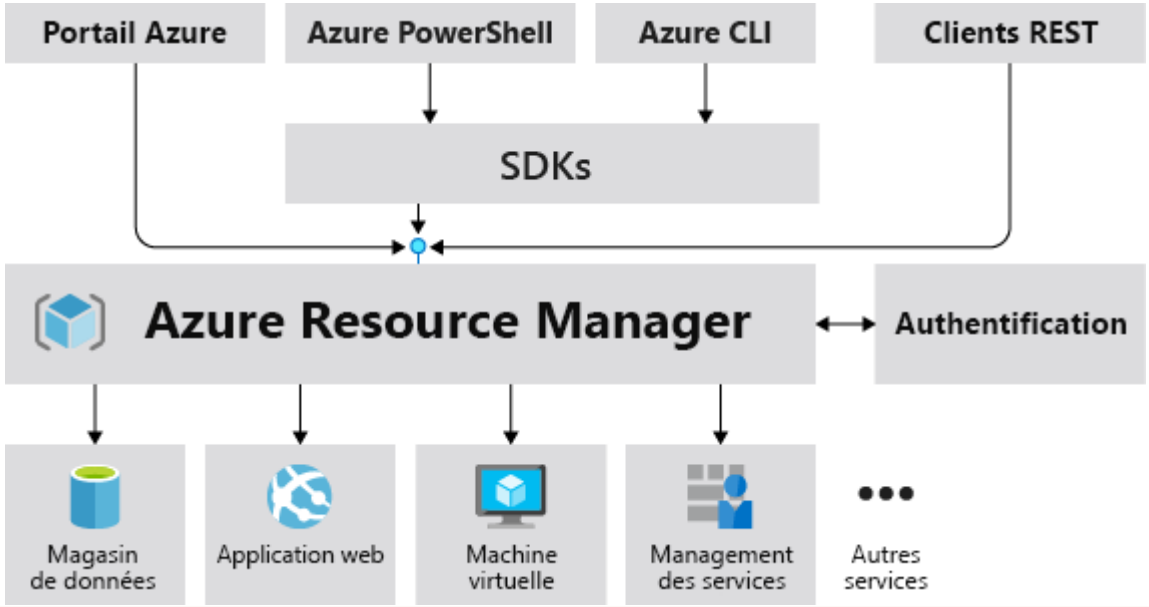
Créer des plans de récupération

1. Processus de basculement
2. **Auto-déploiement**
3. Réplication synchrone
4. Réplication asynchrone

Définition

L'auto-déploiement, également connu sous le nom de déploiement continu (Continuous Deployment en anglais), est une méthode de développement logiciel qui permet de déployer automatiquement les changements apportés à une application ou à une infrastructure sur un environnement de production. Cela peut être fait à l'aide d'outils d'automatisation tels que des scripts, des pipelines de livraison continue, ou des services de cloud computing.

Dans Azure, l'auto-déploiement peut être effectué en utilisant **Azure Resource Manager (ARM)**. ARM est un service de gestion des ressources Azure qui permet de déployer, de gérer et de surveiller les ressources Azure de manière cohérente et prévisible. Avec ARM, on peut créer des modèles de déploiement pour vos applications et votre infrastructure, ce qui permet de déployer facilement et rapidement ces modèles sur différents environnements.



Copyright - Tout droit réservé - OFPPT

Définition

L'auto-déploiement avec Azure ARM peut être effectué à l'aide de la fonctionnalité de déploiement continu de Azure DevOps. Cette fonctionnalité permet de configurer des pipelines de déploiement continus pour vos applications et votre infrastructure, ce qui permet de déployer automatiquement les changements apportés au code ou à une infrastructure sur un environnement de production. Cette fonctionnalité peut être utilisée pour déployer des applications web, des services cloud, des bases de données et d'autres types de ressources Azure.

En résumé, l'auto-déploiement avec Azure ARM est une méthode de déploiement continu qui utilise **Azure Resource Manager** pour déployer automatiquement des applications et des infrastructures sur des environnements de production. Cette méthode peut être mise en œuvre en utilisant la fonctionnalité de déploiement continu de Azure DevOps.

Copyright - Tout droit réservé - OFPPT

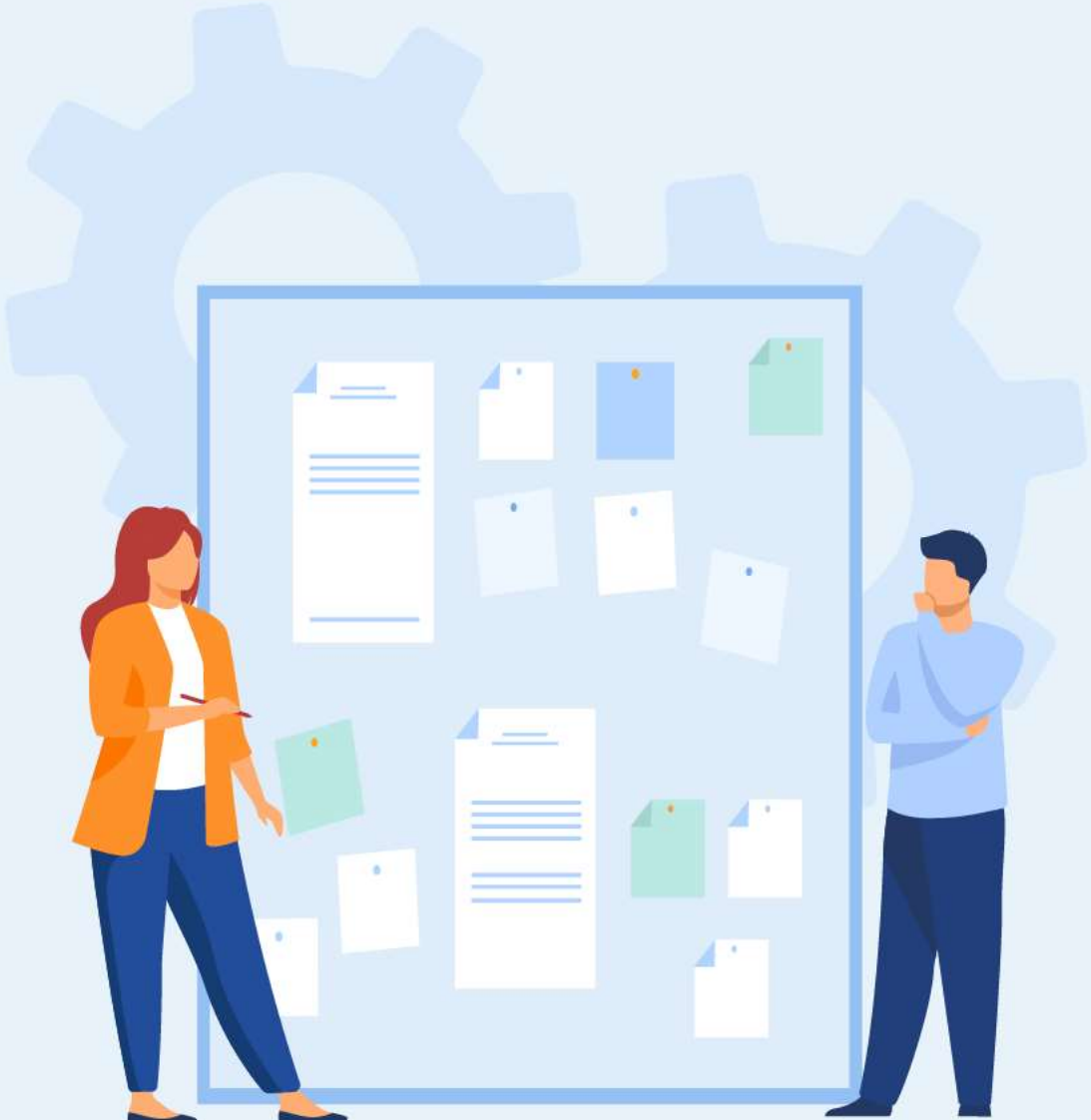
Auto-déploiement vs Modèle ARM

L'auto-déploiement et l'Infrastructure en tant que code (**IaC**) sont étroitement liés. En effet, l'IaC est une méthode de gestion de l'infrastructure qui consiste à utiliser du code pour décrire et automatiser le déploiement de l'infrastructure. L'auto-déploiement utilise également des scripts ou un code pour automatiser le déploiement de l'application et de l'infrastructure.

L'IaC permet de déployer l'infrastructure de manière cohérente et reproductible, en utilisant des scripts ou un code pour décrire l'infrastructure de manière détaillée. L'auto-déploiement permet de déployer des applications de manière cohérente et reproductible, en utilisant des scripts ou un code pour automatiser le processus de déploiement.

En combinant l'IaC et l'auto-déploiement, il est possible de déployer des applications et des infrastructures de manière efficace et cohérente. L'utilisation de l'IaC pour décrire l'infrastructure permet de déployer rapidement des environnements de test, de développement et de production, tandis que l'auto-déploiement permet de déployer automatiquement les changements apportés à l'application ou à l'infrastructure.

Copyright - Tout droit réservé - OFPPT



CHAPITRE 1

Créer des plans de récupération

1. Processus de basculement
2. Auto-déploiement
3. **Réplication synchrone**
4. Réplication asynchrone

Réplica de stockage : Définition

Le réplica de stockage est la technologie de Windows Server qui permet une réplication de volumes entre des serveurs ou des clusters en cas de récupération d'urgence. Il permet également de créer des clusters de basculement étendus qui englobent deux sites, tout en maintenant l'ensemble des nœuds synchronisés.

Le réplica de stockage prend en charge la réplication synchrone et asynchrone :

- **La réplication synchrone** permet la mise en miroir des données dans des sites en réseau à faible latence avec des volumes cohérents en cas d'incident, ce qui garantit l'absence de perte de données au niveau du système de fichiers en cas de panne.
- **La réplication asynchrone** assure la mise en miroir des données entre des sites situés hors des zones métropolitaines sur des liaisons de réseau à latence élevée, mais sans garantie que les deux sites aient des copies identiques des données au moment de la panne.

Copyright - Tout droit réservé - OFPPT

Pourquoi utiliser le réplica de stockage ?

Le réplica de stockage offre des fonctionnalités de préparation aux situations d'urgence et de récupération d'urgence dans Windows Server. Windows Server garantit l'absence totale de perte de données, avec la possibilité de protéger de façon synchrone les données dans différents racks, étages, bâtiments, campus, régions et villes.

Après un incident, toutes les données sont intactes ailleurs sans aucune perte. Il en est de même avant un incident. En effet, le réplica de stockage offre la possibilité de placer les charges de travail en lieu sûr avant une catastrophe, si on en est averti quelques instants avant, encore une fois sans perte de données.

Le réplica de stockage permet une utilisation plus efficace de plusieurs centres de données. En étendant ou en répliquant des clusters, les charges de travail peuvent être exécutées dans plusieurs centres de données pour un accès plus rapide aux données par des applications et utilisateurs de proximité locaux, ainsi qu'une meilleure distribution de la charge et utilisation des ressources de calcul. Si un incident met un centre de données hors connexion, on peut déplacer temporairement ses charges de travail classiques sur l'autre site.

Copyright - Tout droit réservé - OFPPT

Pourquoi utiliser le réplica de stockage ?

Le réplica de stockage peut permettre de mettre hors service des systèmes de réplication de fichiers tels que DFS, qui ont été activés dans des solutions de récupération d'urgence d'entrée de gamme. Même si la réplication DFS fonctionne bien sur des réseaux à très faible bande passante, sa latence est élevée (souvent mesurée en heures ou en jours). Cela est dû à l'obligation de fermer les fichiers et à ses limitations artificielles destinées à empêcher l'encombrement du réseau. Étant donné ces caractéristiques de conception, les fichiers les plus récents et les plus sensibles d'un réplica DFSR sont les moins susceptibles d'être répliqués. Le réplica de stockage fonctionne sous le niveau de fichier et ne présente aucune de ces restrictions.

Le réplica de stockage prend également en charge la réplication asynchrone pour des plages plus importantes et des réseaux à latence plus élevée. Comme il n'est pas basé sur un point de contrôle et effectue plutôt une réplication en continu, le delta des modifications a tendance à être beaucoup plus faible par rapport aux produits basés sur un instantané. Le réplica de stockage fonctionne au niveau de la partition et réplique donc tous les instantanés VSS créés par Windows Server ou par le logiciel de sauvegarde. En utilisant des instantanés VSS, il permet d'utiliser des instantanés de données cohérents avec l'application pour une récupération à un point dans le temps, en particulier les données utilisateur non structurées répliquées de manière asynchrone.

Copyright - Tout droit réservé - OFPPT

Fonctionnalités de réplica de stockage

- **Aucune perte de données, réplication au niveau du bloc.** Avec la réplication synchrone, il n'existe aucun risque de perte de données. Avec la réplication au niveau du bloc, il n'existe aucun risque de verrouillage de fichier.
- **Déploiement et gestion simples.** Le réplica de stockage est spécialement conçu pour être simple d'utilisation. La création d'un partenariat de réplication entre deux serveurs peut utiliser Windows Admin Center. Le déploiement de clusters étendus utilise un Assistant intuitif de l'outil familier Gestionnaire du cluster de basculement.
- **Invité et hôte.** Toutes les fonctions du réplica de stockage sont exposées à la fois dans les déploiements basés sur l'invité et sur l'hôte virtualisés. Cela signifie que les invités peuvent répliquer leurs volumes de données même s'ils sont exécutés sur des plateformes de virtualisation autres que Windows ou dans des clouds publics, tant qu'ils utilisent Windows Server dans l'invité.
- **SMB3.** Le réplica de stockage utilise la technologie mature et reconnue de SMB3, commercialisée pour la première fois dans Windows Server 2012. Cela signifie que toutes les caractéristiques avancées de SMB (telles que la prise en charge de Multichannel et SMB Direct sur les cartes réseau RoCE, iWARP et RDMA InfiniBand) sont disponibles pour le réplica de stockage.
- **Sécurité.** Contrairement aux produits de nombreux fournisseurs, une technologie de sécurité de pointe est intégrée au réplica de stockage. Cela inclut la signature des paquets, le chiffrement intégral des données AES-128-GCM, la prise en charge de l'accélération du chiffrement AES-NI d'Intel et la prévention des attaques de l'intercepteur « man in the middle » de l'intégrité de l'authentification préalable. Le réplica de stockage utilise Kerberos AES256 pour toutes les authentifications entre les nœuds.

Copyright - Tout droit réservé - OFPPT

Fonctionnalités de réplica de stockage

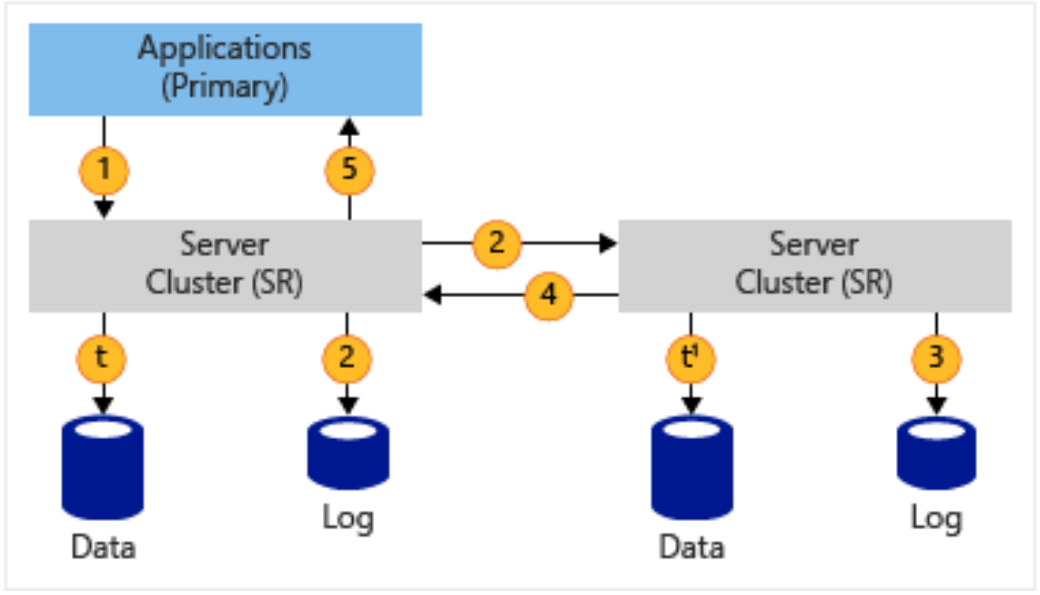
- **Synchronisation initiale hautes performances.** Le réplica de stockage prend en charge la synchronisation initiale amorcée, où il existe déjà un sous-ensemble de données sur une cible provenant de copies, de sauvegardes ou de lecteurs livrés plus anciens. La réplication initiale copie uniquement les blocs différents, ce qui peut raccourcir la durée de synchronisation initiale et empêcher que les données n'utilisent une bande passante limitée. Les réplicas de stockage bloquent le calcul de la somme de contrôle et l'agrégation signifie que les performances de la synchronisation initiale sont limitées uniquement par la vitesse du réseau et du stockage.
- **Groupes de cohérence.** La demande d'écriture garantit que des applications telles que Microsoft SQL Server peuvent écrire dans plusieurs volumes répliqués et savoir que les données sont écrites sur le serveur de destination de façon séquentielle.
- **Délégation d'utilisateur.** Des autorisations peuvent être déléguées aux utilisateurs pour gérer la réplication sans être membres du groupe Administrateurs intégré sur les nœuds répliqués, ce qui limite leur accès à des zones non liées.
- **Contrainte de réseau.** Le réplica de stockage peut être limité à des réseaux individuels par serveur et par volumes répliqués, afin de fournir la bande passante à l'application, à la sauvegarde et au logiciel de gestion.
- **Allocation dynamique.** L'allocation dynamique des appareils SAN et des espaces de stockage est prise en charge afin de fournir des temps de réplication initiale presque instantanés dans de nombreuses situations. Une fois la réplication initiale lancée, le volume ne peut pas être réduit ni tronqué
- **Compression.** Le réplica de stockage propose la compression des données transférées sur le réseau entre le serveur source et le serveur de destination. La compression du réplica de stockage pour le transfert de données est uniquement prise en charge dans Windows Server Datacenter : Édition Azure à compter de la build du système d'exploitation 20348.1070.

Copyright - Tout droit réservé - OFPPT

Réplication synchrone

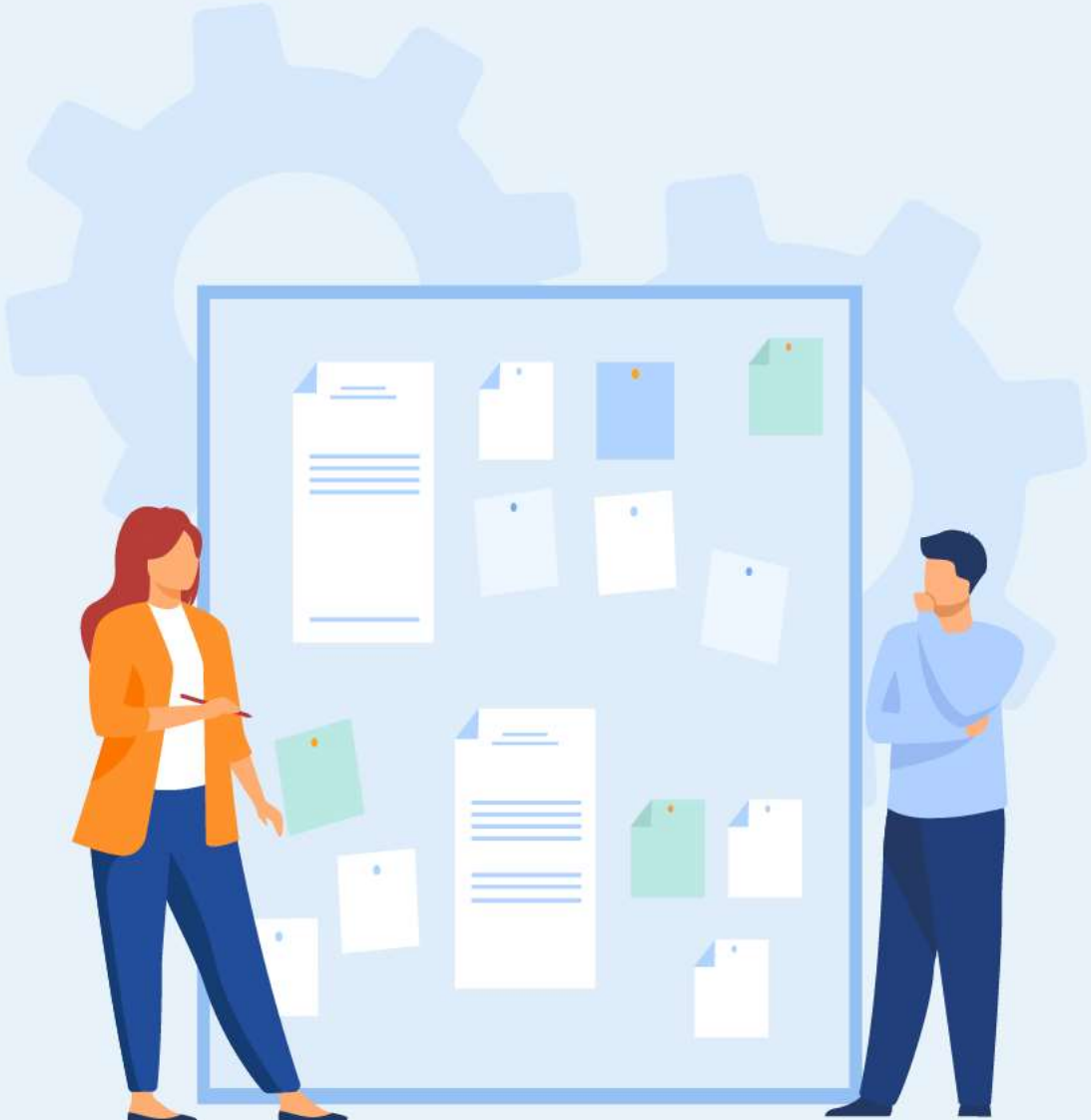
La réplication synchrone garantit que l'application écrit les données à deux emplacements à la fois avant la fin de l'opération d'E/S. Cette réplication est plus adaptée aux données stratégiques, car elle nécessite des investissements dans le réseau et le stockage, et risque de dégrader les performances des applications en imposant l'écriture dans deux emplacements.

Quand des écritures d'application se produisent sur la copie des données sources, le stockage d'origine n'accuse pas immédiatement réception des E/S. Au lieu de cela, ces modifications de données sont répliquées sur la copie de destination distante et renvoient un accusé de réception. Ce n'est qu'à ce moment-là que l'application reçoit l'accusé de réception des E/S. Cela garantit une synchronisation constante du site distant avec le site source, tout en étendant les E/S de stockage sur le réseau. Dans le cas d'une défaillance du site source, les applications peuvent basculer vers le site distant et reprendre leurs opérations avec l'assurance de ne perdre aucune donnée.



PARTIE 2

Copyright - Tout droit réservé - OFPPT



CHAPITRE 1

Créer des plans de récupération

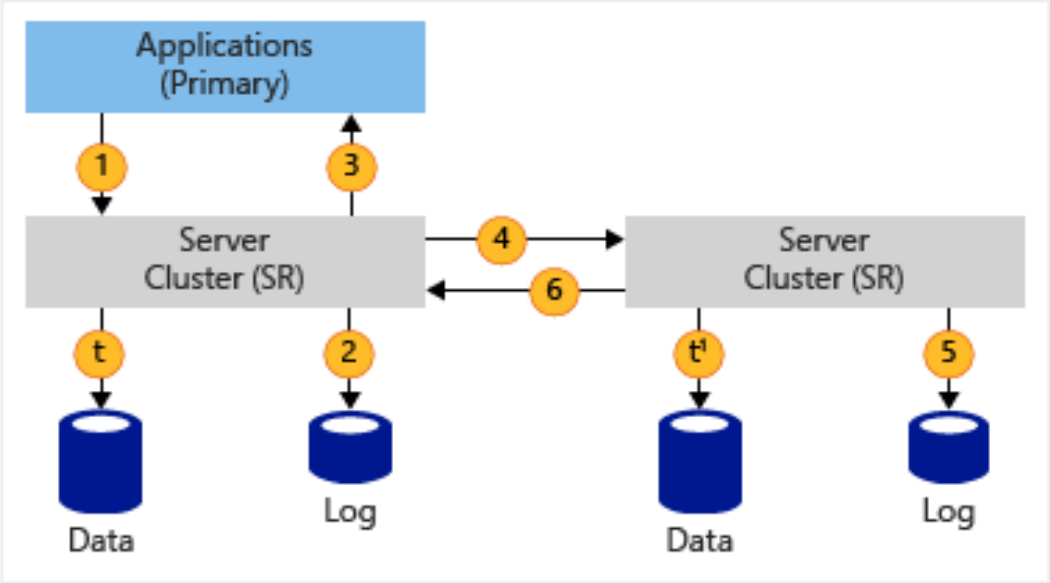
1. Processus de basculement
2. Auto-déploiement
3. Réplication synchrone
4. **Réplication asynchrone**

Réplication asynchrone

À l'inverse, la réplication asynchrone signifie que, quand l'application écrit des données, ces données sont répliquées sur le site distant sans garantie de recevoir un accusé de réception immédiatement. Ce mode permet de répondre plus rapidement à l'application et propose une solution de récupération d'urgence qui fonctionne géographiquement.

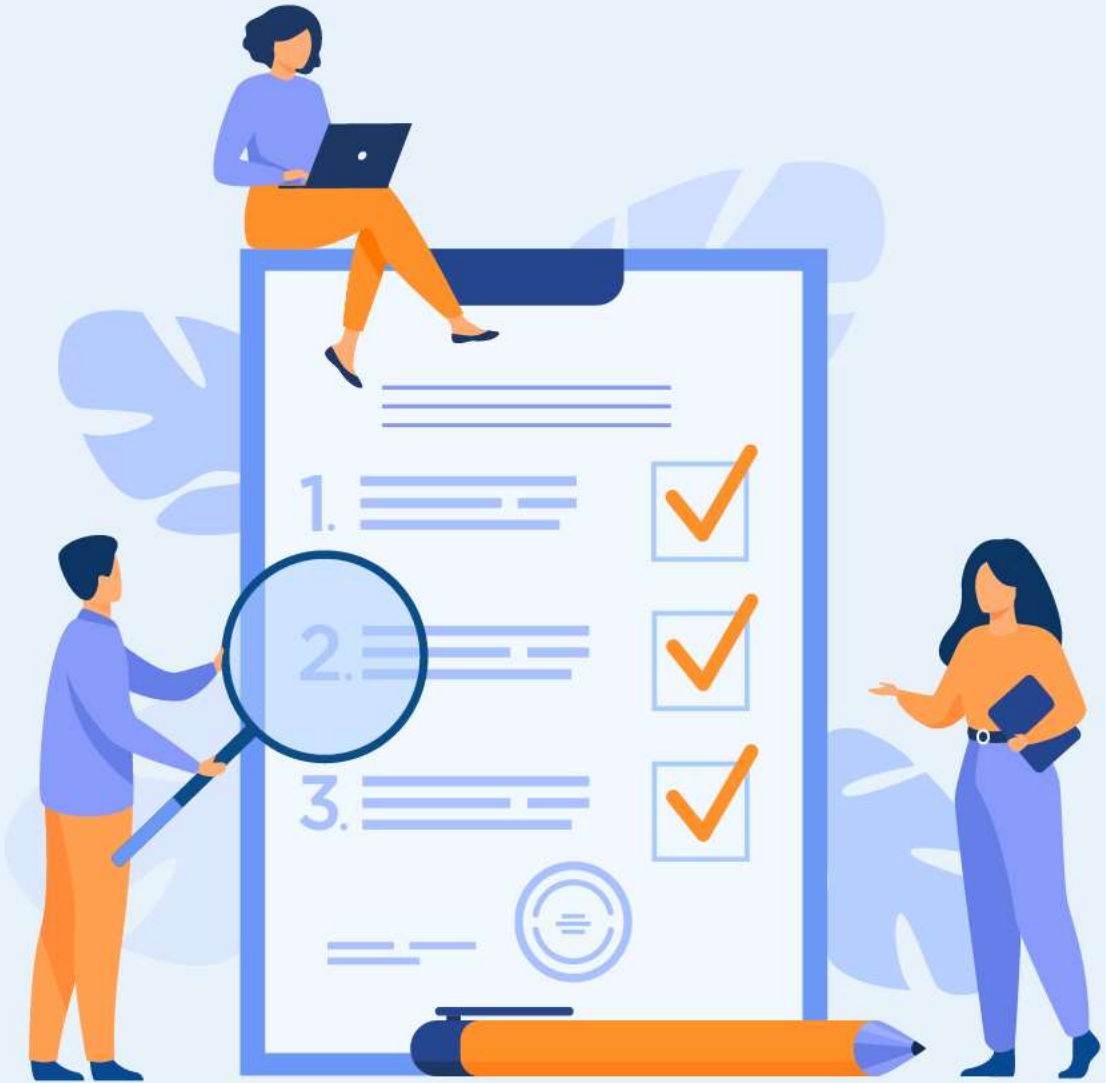
Quand l'application écrit des données, le moteur de réplication capture l'écriture et confirme immédiatement réception à l'application. Les données capturées sont ensuite répliquées vers l'emplacement distant. Le nœud distant traite la copie des données et renvoie tardivement un accusé de réception à la copie source. Étant donné que les performances de la réplication ne sont plus dans le chemin d'accès E/S de l'application, la réactivité et la distance du site distant sont des facteurs moins importants. Il existe un risque de perte de données si la source de données est perdue et que la copie de destination des données est toujours en mémoire tampon sans quitter la source.

Avec son objectif de point de récupération supérieur à zéro, la réplication asynchrone est moins adaptée pour les solutions HA (haute disponibilité) telles que les clusters de basculement, car elles sont conçues pour un fonctionnement continu avec redondance et sans perte de données.



PARTIE 2

Copyright - Tout droit réservé - OFPPT



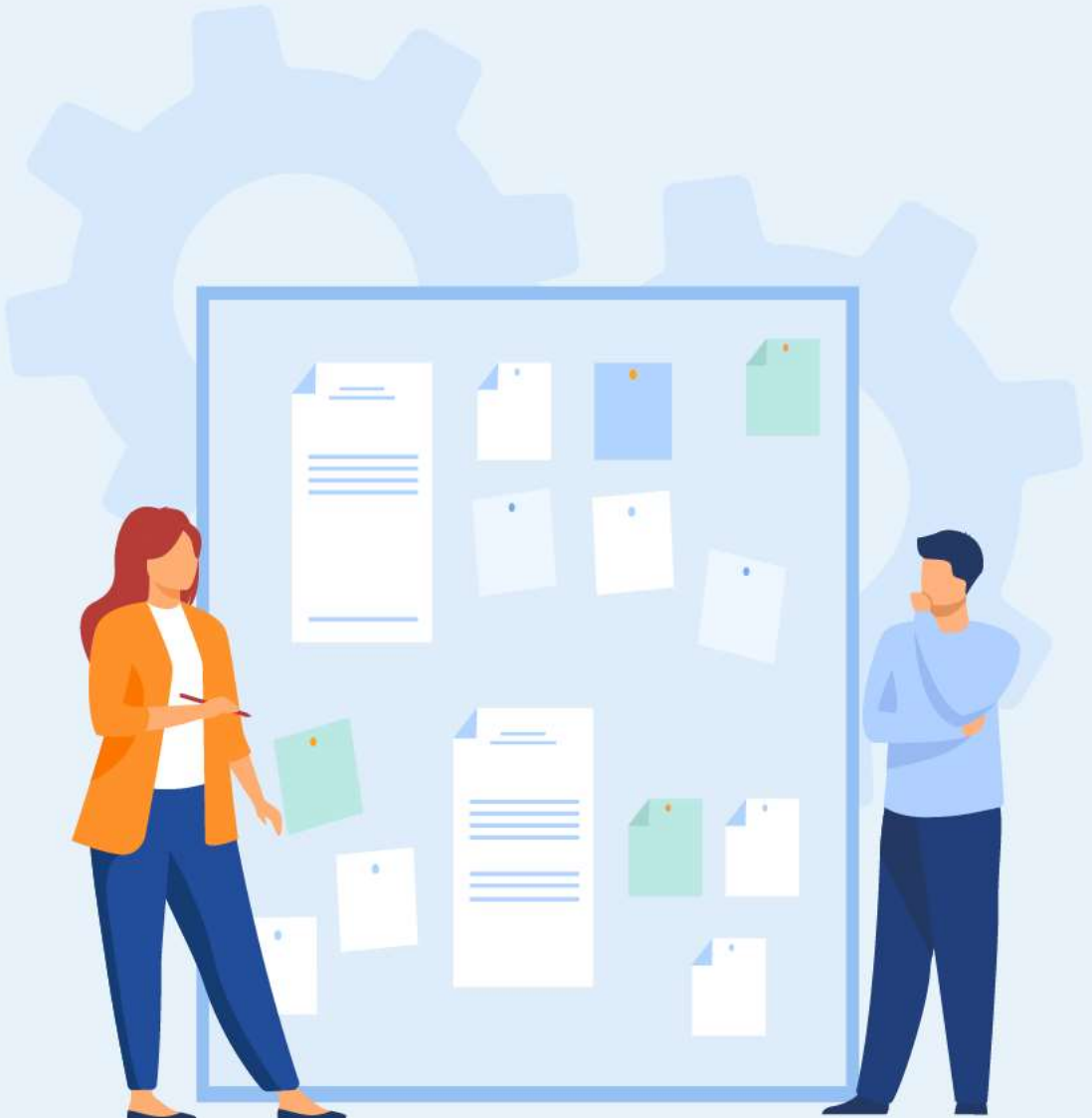
CHAPITRE 2

Appliquer la géo-réplication

Ce que vous allez apprendre dans ce chapitre :

- Comprendre qu'est ce qu'une base de donnée secondaire
- Appréhender la notion de géo-basculement

8 heures



CHAPITRE 2

Appliquer la géo-réplication

1. **Base de donnée secondaire**
2. Géo-basculement

Définition

Au contraire des données primaires, dont le chargé d'études est à l'origine, les données secondaires sont, à la base, recueillies pour d'autres raisons. Les données secondaires sont rapidement accessibles et relativement peu dispendieuses. Les deux ont cependant des limites qu'il faut analyser afin de déterminer leur pertinence. Les critères d'analyse portent sur les paramètres pris en compte dans la méthodologie, les erreurs, l'actualité, les objectifs, la nature, et la fiabilité des données.

Les entreprises regorgent d'informations existantes que l'on nomme données secondaires internes. Les données externes proviennent, pour leur part, de sources extérieures à l'entreprise que l'on trouve généralement soit sur Internet gratuitement ou non, soit via des prestations d'instituts d'études.

La base de données secondaire à le même nom que la base de données primaire et, par défaut, le même niveau de service et la même taille de calcul. La base de données secondaire peut être une base de données unique ou une base de données mise en pool. Une fois la base de données secondaire créée et amorcée, une réplication des données de la base de données primaire vers la base de données secondaire commence.

Copyright - Tout droit réservé - OFPPT

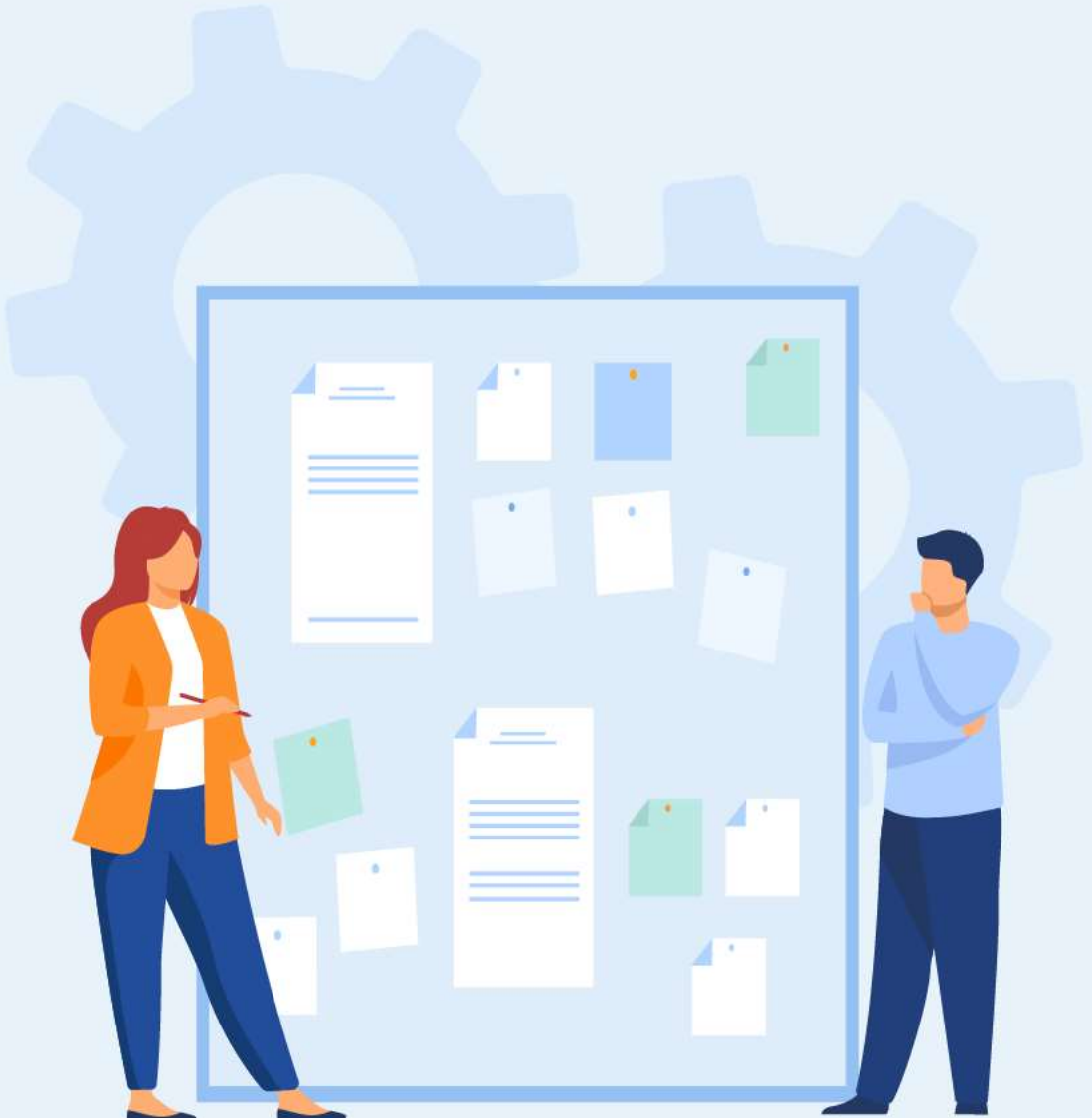
Le rôle de base de donnée secondaire

Dans le contexte de la géo-réplication, une base de données secondaire peut jouer un rôle important en fournissant une copie de la base de données principale qui est située dans un autre emplacement géographique.

La géo-réplication consiste à répliquer la base de données principale sur une base de données secondaire située dans un autre emplacement géographique, généralement pour des raisons de disponibilité ou de récupération après sinistre. La base de données secondaire peut être utilisée pour effectuer des lectures ou des requêtes, tandis que la base de données principale est réservée aux écritures. Cela peut permettre d'améliorer les performances et la disponibilité du système, tout en réduisant les temps d'arrêt potentiels.

En cas de panne ou d'incident, la base de données secondaire peut être activée pour prendre en charge les opérations de production, ce qui permet d'assurer la continuité des activités et de minimiser les temps d'arrêt. La base de données secondaire peut également être utilisée pour la récupération après sinistre, en permettant de restaurer rapidement la base de données principale à partir de la copie de sauvegarde stockée dans un autre emplacement géographique.

Copyright - Tout droit réservé - OFPPT



CHAPITRE 2

Appliquer la géo-réplication

1. Base de donnée secondaire
2. **Géo-basculement**

Définition

Le géo-basculement est une technique utilisée pour assurer la continuité de service dans un environnement distribué, en particulier dans le cadre de la géo-réplication de bases de données.

Le géo-basculement consiste à basculer automatiquement le trafic d'un site principal vers un site de secours distant en cas d'incident sur le site principal. Cette technique permet de minimiser les temps d'arrêt en redirigeant automatiquement les utilisateurs et les applications vers un site de secours qui contient une copie à jour des données de production.

Le géo-basculement nécessite une infrastructure de réseau et de réplication de données sophistiquée pour garantir une continuité de service sans interruption, ainsi que des processus et des procédures rigoureux pour assurer la cohérence des données entre les différents sites.

Cette technique est couramment utilisée dans les environnements distribués pour garantir la continuité de service, notamment pour les applications critiques et les services en ligne qui nécessitent une disponibilité permanente. Le géo-basculement peut également être utilisé pour éviter les pannes planifiées, comme lors des opérations de maintenance sur le site principal.

Copyright - Tout droit réservé - OFPPT

La géo-réplication active: Définition

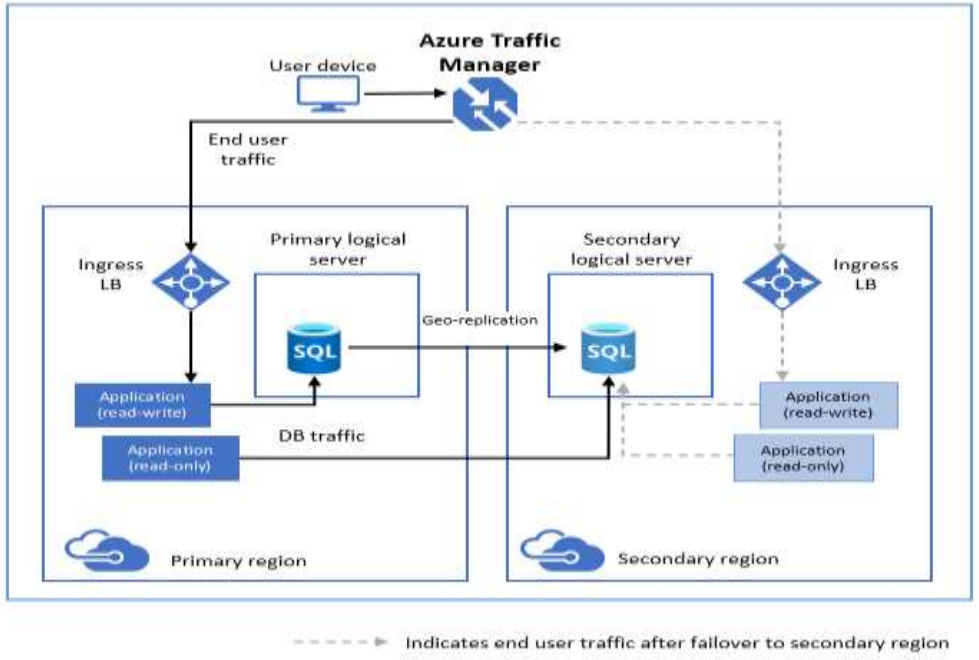
La géo-réplication active est une fonctionnalité qui permet de créer une base de données secondaire accessible en lecture et synchronisée en continu pour une base de données primaire. La base de données secondaire accessible en lecture peut être dans la même région Azure que la base de données primaire, ou, plus communément, dans une autre région. Ce type de base de données secondaire accessible en lecture est également appelé géo-secondaire ou géo-réplica.

La géo-réplication active est conçue comme une solution de continuité d'activité qui permet d'effectuer une reprise d'activité rapide au niveau des bases de données individuelles en cas de panne régionale ou à plus grande échelle. Une fois la géo-réplication configurée, on peut lancer un basculement géographique vers une zone géographique secondaire dans une autre région Azure. Le géo-basculement est initié par programme par l'application ou manuellement par l'utilisateur.

Le diagramme suivant illustre la configuration standard d'une application cloud géo-redondante avec la géo-réplication active:

Il est possible de gérer la géo-réplication et initier un basculement géographique à l'aide des éléments suivants :

- Portail Azure
- PowerShell : base de données unique
- PowerShell : pool élastique
- Transact-SQL : base de données unique ou pool élastique
- API REST : base de données unique



PARTIE 2

Copyright - Tout droit réservé - OFPPT

Le géo-basculement vs la géo-réplication

La géo-réplication est une technique de réplication de données qui permet de copier des données d'un emplacement géographique à un autre pour assurer la disponibilité, la continuité de service, la reprise après sinistre ou tout autre objectif commercial. La géo-réplication implique la synchronisation en temps réel ou quasi-réel des données entre les sites géographiquement éloignés pour assurer la cohérence et la fiabilité des données.

Le géo-basculement, quant à lui, est une stratégie de reprise après sinistre qui permet de basculer rapidement et automatiquement le trafic d'un site primaire vers un site secondaire distant en cas d'incident sur le site primaire. Le géo-basculement est conçu pour minimiser les temps d'arrêt et assurer une continuité de service en redirigeant automatiquement le trafic des utilisateurs vers un site secondaire qui contient une copie à jour des données de production.

En résumé, la géo-réplication est une technique de réplication de données qui permet de copier les données entre des sites géographiquement éloignés, tandis que le géo-basculement est une stratégie de reprise après sinistre qui permet de basculer rapidement et automatiquement le trafic d'un site primaire vers un site secondaire distant en cas d'incident sur le site primaire.

Copyright - Tout droit réservé - OFPPT

Terminologies

➢ **Réplication asynchrone automatique**

On peut uniquement créer une zone géographique secondaire pour une base de données existante. La zone géo-secondaire peut être créée sur n'importe quel serveur logique, autre que le serveur avec la base de données primaire. Une fois créé, le géo-réplica est rempli avec les données de la base de données primaire. Ce processus est appelé amorçage. Une fois la base de données géo-secondaire créée et amorcée, les mises à jour de la base de données primaire sont automatiquement répliquées de manière asynchrone sur le géo-réplica. La réplication asynchrone signifie que les transactions sont validées sur la base de données primaire avant leur réplication.

➢ **Accès en lecture aux réplicas géo-secondaires**

Une application peut accéder à un géo-réplica pour exécuter des requêtes en lecture seule avec des principaux de sécurité identiques ou différents de ceux utilisés pour accéder à la base de données primaire.

➢ **Basculement géographique planifié**

Le géo-basculement planifié bascule les rôles des bases de données primaire et géo-secondaires après avoir effectué la synchronisation complète des données. Un basculement planifié n'entraîne pas de perte de données. La durée du basculement géographique planifié dépend de la taille du journal des transactions sur la base de données primaire qui doit être synchronisée avec la base géo-secondaire. Le géo-basculement planifié est conçu pour les scénarios suivants :

- Simuler des récupérations d'urgence (DR) en production lorsque la perte de données n'est pas acceptable ;
- Déplacer les bases de données vers une autre région ;
- Renvoyer les bases de données vers la région primaire une fois la panne éliminée (restauration automatique).

Copyright - Tout droit réservé - OFPPT

Terminologies

➢ **Basculement géographique non planifié**

Un géo-basculement non planifié ou forcé fait immédiatement basculer la base de données géo-secondaire vers le rôle primaire sans synchronisation avec la base de données primaire. Toutes les transactions validées sur la base de données primaire qui ne sont pas répliquées sur la base de données secondaire sont perdues. Cette opération est conçue comme une méthode de récupération pendant les pannes lorsque le serveur principal n'est pas accessible, mais que la disponibilité de la base de données doit être restaurée rapidement. Lorsque la base de données primaire d'origine est de nouveau disponible, elle est automatiquement reconnectée et réalimentée avec les données primaires actuelles, et elle devient une nouvelle base de donnée géo-secondaire.

➢ **Bases de données géo-secondaires accessibles en lecture**

Jusqu'à quatre zones géographiques secondaires peuvent être créées pour une base de données primaire. S'il n'existe qu'une seule base de données secondaire, en cas d'échec de celle-ci, l'application est exposée à un risque plus élevé jusqu'à la création d'une nouvelle base de données secondaire. S'il existe plusieurs bases de données secondaires, l'application reste protégée même en cas d'échec de l'une des bases de données secondaires. Des bases de données secondaires supplémentaires peuvent également être utilisées pour effectuer un scale-out des charges de travail en lecture seule.

➢ **Géo-réplication des bases de données dans un pool élastique**

Chaque base de données géo-secondaire peut être une base de données autonome ou une base de données dans un pool élastique. Le choix du pool élastique pour chaque base de données géo-secondaire est séparé et ne dépend pas de la configuration de tous les autres réplicas dans la topologie (primaire ou secondaire). Chaque pool élastique est contenu dans un serveur logique unique. Étant donné que les noms de bases de données sur un serveur logique doivent être uniques, plusieurs géo-réplicas de la même base de données primaire ne peuvent jamais partager un pool élastique.

Copyright - Tout droit réservé - OFPPT

Configuration de la base de données géo-secondaire

Les bases de données primaire et géo-secondaire doivent offrir le même niveau de service. Il est également vivement recommandé de configurer la base de données géo-secondaire avec les mêmes redondances de stockage de sauvegarde et taille de calcul (DTU ou vCores) que la base de données primaire.

En cas de charge de travail d'écriture importante de la base de données primaire, une base de données géo-secondaire dotée d'une taille de calcul inférieure peut ne pas suivre. Cela entraînera un décalage de réplication sur le géo-réplica et peut entraîner une indisponibilité de la base de données géo-secondaire.

Pour atténuer ces risques, la géo-réplication active réduit si nécessaire le taux de journalisation des transactions de la base de données primaire pour permettre à ses bases de données secondaires de rattraper le retard.

Après un basculement, une configuration de base de données géo-secondaire déséquilibrée peut aussi altérer le niveau de performance de l'application en raison de la capacité de calcul insuffisante de la nouvelle base de données primaire. Dans ce cas, il est nécessaire d'effectuer un scale-up de la base de données, afin qu'elle puisse bénéficier des ressources suffisantes, ce qui peut nécessiter beaucoup de temps. Un basculement à haute disponibilité est également nécessaire à la fin du processus de scale-up, pouvant interrompre les charges de travail de l'application.

Copyright - Tout droit réservé - OFPPT

Configuration de la base de données géo-secondaire

Si on décide de créer le géo-réplica avec une taille de calcul inférieure, on doit surveiller le taux d'E/S de journal sur le serveur principal dans le temps. Cela permet d'estimer la taille de calcul minimale du géo-réplica requis pour supporter la charge de réplication.

Par exemple, si la base de données primaire est P6 (1 000 DTU) et si son taux d'E/S du journal est maintenu à 50 %, la base de données géo-secondaire doit être au moins P4 (500 DTU). Pour récupérer les données d'E/S historiques du journal, utiliser la vue **sys.resource_stats**. Pour récupérer les données d'E/S récentes dans le journal avec une granularité plus élevée qui reflète mieux les pics à court terme, utiliser la vue **sys.dm_db_resource_stats**.

Copyright - Tout droit réservé - OFPPT

Mise en place de la géo-réplication

Les étapes nécessaires pour appliquer la géo-réplication peuvent différer en fonction de la technologie de base de données utilisée. Toutefois, voici des étapes générales à suivre pour mettre en place la géo-réplication:

- ✓ **Évaluer les exigences de l'application :** Il est important de déterminer les exigences de l'application en termes de disponibilité, de performance et de reprise après sinistre. Cela permettra de déterminer les besoins en matière de réplication de données et de choisir la bonne technologie de réplication.

- ✓ **Choisir une technologie de réplication de données :** Il existe plusieurs technologies de réplication de données disponibles, telles que la réplication synchrone, la réplication asynchrone, la réplication basée sur les journaux, etc. Choisir la bonne technologie dépendra des exigences de l'application, du volume de données, de la latence acceptable et des coûts.

- ✓ **Mettre en place l'infrastructure de réplication de données :** La géo-réplication nécessite une infrastructure de réseau et de réplication sophistiquée pour assurer une réplication efficace des données entre les différents sites. Il est important de configurer les paramètres de réseau, les pare-feu, les groupes de disponibilité, etc. pour assurer une réplication fiable des données.

- ✓ **Configurer la réplication de données :** La configuration de la réplication de données dépendra de la technologie de réplication choisie. Il est important de configurer la réplication de manière qu'elle soit fiable, cohérente et efficace.

Copyright - Tout droit réservé - OFPPT

Mise en place de la géo-réplication

- ✓ **Tester et valider la configuration :** Il est important de tester et de valider la configuration de géo-réplication pour s'assurer que tout fonctionne correctement. Il est recommandé de tester la récupération après sinistre et de vérifier la cohérence des données entre les différents sites.
- ✓ **Surveiller et maintenir la configuration :** Il est important de surveiller en permanence la configuration de géo-réplication pour s'assurer que tout fonctionne correctement. Les tâches de maintenance régulières, telles que les mises à jour de sécurité, les correctifs de bogues, etc. doivent également être effectuées pour garantir la continuité de service et la sécurité des données.

Copyright - Tout droit réservé - OFPPT



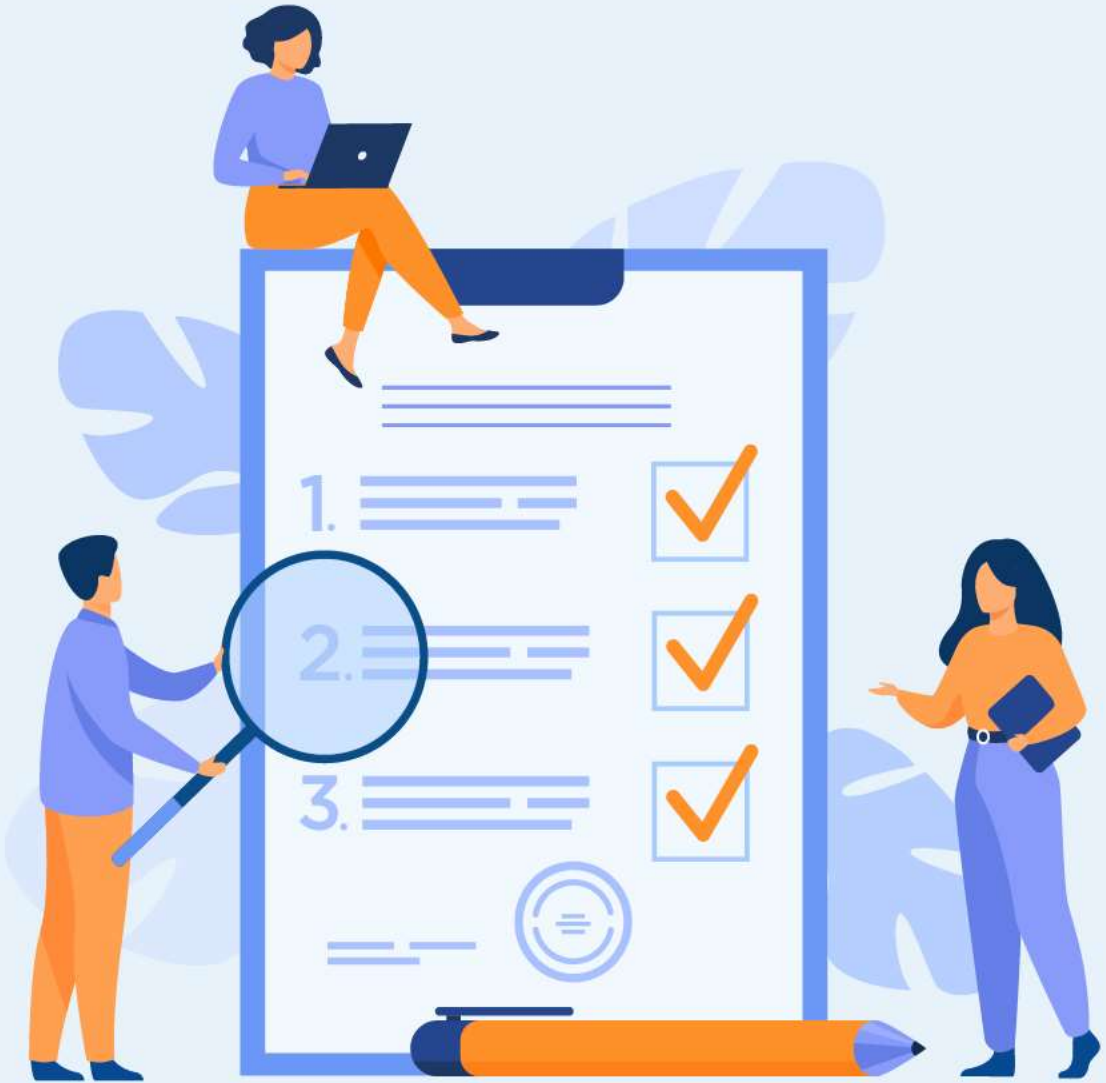
PARTIE 3

MIGRER LE SI DANS LE Cloud

Dans ce module, vous allez :

- Connaitre les stratégies de migration du SI dans le Cloud
- Adopter une approche DevOps

13,5 heures



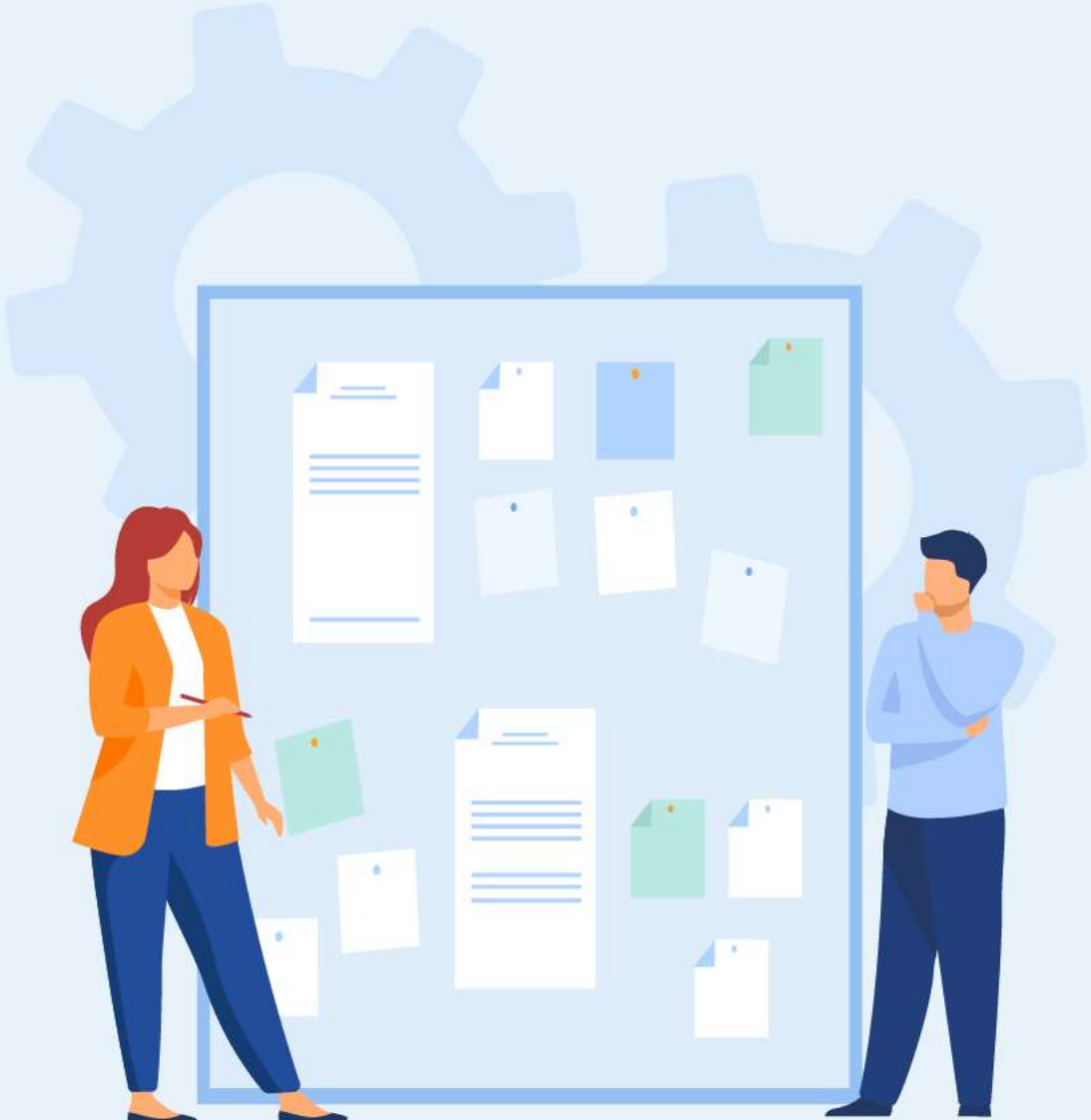
CHAPITRE 1

Identifier les stratégies de migration du SI dans le Cloud

Ce que vous allez apprendre dans ce chapitre :

- Connaitre la méthode du minimum d'efforts (Lift and shift, Rehost)
- Appréhender la Modification de la couche technique (Replateform, Redeploy)
- Connaitre la Réécriture de l'application (Rearchitect) et remplacement (Replace, Repurchasing)
- Conservation (Retain) et décommissionnement (retire)

6,5 heures



CHAPITRE 1

Identifier les stratégies de migration du SI dans le Cloud

1. **Méthode du minimum d'efforts (Lift and shift, Rehost)**
2. Modification de la couche technique (Replateform, Redeploy)
3. Réécriture de l'application (Rearchitect) et remplacement (Replace, Repurchasing)
4. Conservation (Retain) et décommissionnement (retire)

Les stratégies de migration vers le Cloud

Tout plan d'adoption du Cloud à l'échelle de l'entreprise comprend une stratégie de migration du SI vers le Cloud. Ces stratégies peuvent être réalisées suivant différentes approches : **lift-and-shift**, **lift-and-optimize** ou **modernisation**. Chaque approche est considérée comme une migration.

Le « **lift and shift** » est une approche parmi d'autres permettant de migrer vos applications vers le Cloud. Elle consiste à déplacer une application et les données associées vers une plateforme Cloud, sans modifier l'application.

L'approche « **lift and shift** » est fréquemment adoptée pour répliquer des applications sur site dans le Cloud en faisant l'économie d'une refonte fastidieuse et coûteuse.

Il n'y a pas de solution unique et universelle pour déplacer une application depuis votre data center sur site vers le Cloud. Mais il existe des parcours de migration établis et reconnus. Le « **lift and shift** », aussi appelé réhébergèrent, est l'un d'entre eux. C'est un moyen pour les entreprises de protéger leurs investissements dans le workflow, la logique et les données métier confinés dans le matériel sur site.

L'approche « **lift and shift** » ouvre la voie à la modernisation de l'IT en permettant la transition vers une architecture ouverte plus extensible dans le Cloud. Les entreprises l'envisagent pour de multiples raisons commerciales, notamment la réduction des coûts et l'amélioration des performances et de la résilience.



Copyright - Tout droit réservé - OFPPT

Quand utiliser la méthode (Lift and shift, Rehost) ?

Avec l'approche « **lift-and-shift** », les applications sur site peuvent être migrées vers le Cloud sans repenser la conception. Mais elles ne bénéficient pas toujours pleinement des fonctionnalités Cloud, et cette approche n'est donc pas la plus économique.

Gartner estime qu'en **2020**, les organisations dépourvues de processus d'optimisation des coûts dépenseront en moyenne **40%** de plus dans le Cloud public (Ed Anderson, 2018).
Pour éviter la mauvaise surprise d'un surcoût, les entreprises ont besoin d'une stratégie d'allocation des coûts, ainsi que des rôles bien définis au sein de l'organisation afin de surveiller les dépenses liées au Cloud. Il faudra probablement pour cela des outils supplémentaires.

Avantages de l'approche « **lift-and-shift** » pour les applications :

- **Des économies rapides :** ***Down Jones*** a diminué les coûts IT de plus de 25 %. ***GE Oil & Gas*** a réalisé 52 % d'économies grâce au « **lift-and-shift** ».
- **Une migration immédiate vers le Cloud :** En 2008, **Netflix** a connu une panne majeure qui a empêché l'envoi des DVD aux clients et déclenché la transition vers le Cloud de cette entreprise en plein essor.
- **Reprise d'activité dans le Cloud :** Le déplacement des données vers le Cloud fournit aux entreprises un deuxième site hautement disponible. On constate fréquemment une réduction des coûts par rapport au plan de reprise d'activité précédent.
- **Allègement de la dette technique :** Les anciens systèmes peuvent être lents et coûter cher à l'entretien. De la puissance supplémentaire, comme l'instance x1e.32xlarge d'Amazon, peut vous donner l'impulsion dont vous avez besoin dans l'immédiat.

Copyright - Tout droit réservé - OFPPT

Cas d'utilisation du (Lift and shift, Rehost)

Etant donné que les technologies Cloud continuent d'augmenter la productivité des équipes et d'améliorer les modèles de tarification du Cloud, il est de moins en moins logique et coûte de plus en plus cher à long terme de migrer une solution qui tourne sur le Cloud et qui ne tire pas parti de l'environnement Cloud. Mais, il existe encore quelques cas dans lesquels le **lift and shift** est intéressant :

- Vos coûts d'infrastructure sur site montent en flèche, mais vous n'êtes pas tout à fait prêt à reconcevoir vos applications . Dans ce cas, il peut être avantageux de « déplacer » brièvement les applications sur le Cloud jusqu'à ce que vous soyez prêt ou capable de reconstruire/reconcevoir les solutions. Les exceptions sont les applications héritées gourmandes en ressources telles que l'analyse de données volumineuses, l'animation numérique ou l'imagerie médicale ou les techniques qui ont tendance à augmenter les frais de Cloud payés à l'utilisation plus rapidement que vous ne pouvez le prévoir.

- Vous souhaitez migrer des applications prêtes à l'emploi : Vous ne pouvez pas les reconcevoir, donc la seule vraie alternative est de les déplacer tels quels vers le Cloud.

- Vous avez besoin d' une sauvegarde et d'une restauration moins coûteuses et plus évolutives. La transition des sauvegardes sur site vers le Cloud est un cas d'utilisation courant dans tous les secteurs sauf les plus fortement réglementés ou pour les applications avec les RPO/RTO les plus stricts (objectifs de point de récupération/objectifs de temps de récupération).

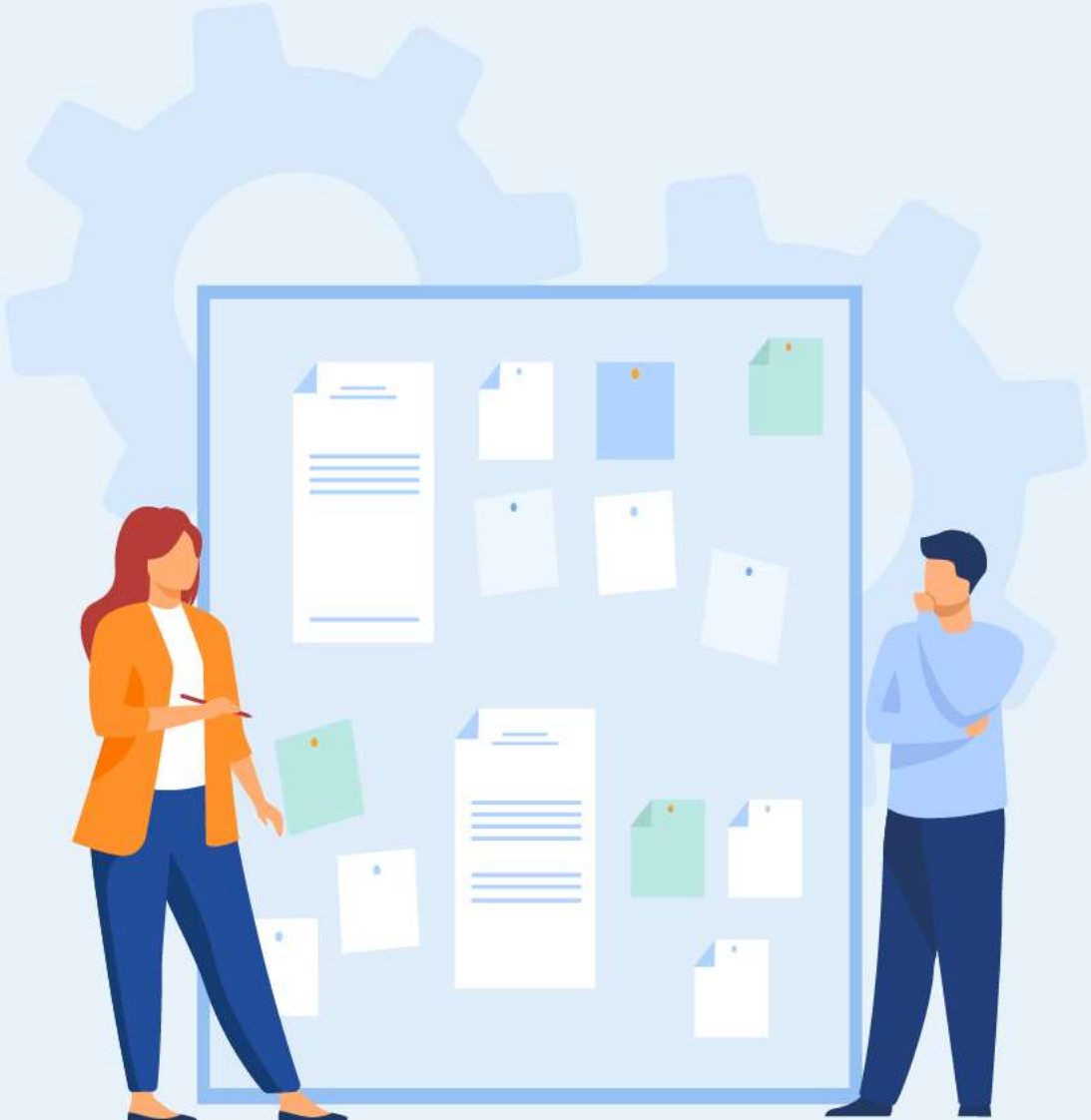
Copyright - Tout droit réservé - OFPPT

Evaluer et planifier la migration (Lift and shift, Rehost)

Avant d'entreprendre toute migration par « **lift and shift** », évaluez soigneusement et préparez-vous aux facteurs qui peuvent avoir un impact sur la difficulté, le coût et la valeur ajoutée pour l'entreprise. Ceux-ci peuvent inclure, mais ne sont pas limités à ce qui suit :

Durée de vie de l'application	Combien de temps encore continuerez-vous à utiliser cette application ou à exécuter cette charge de travail ? Dans la plupart des cas, il n'est pas logique de migrer une application que vous allez supprimer dans les 12 prochains mois.
Restrictions d'accès aux API	Assurez-vous que votre migration vers le Cloud n'entraînera pas de goulots d'étranglement pour vos outils d'API actuels.
Outils d'automatisation de la migration	Identifiez si votre fournisseur d'hébergement Cloud propose des outils automatisés pour les migrations et prévoyez de les utiliser dans la mesure du possible.
Priorité de migration	Si vous prévoyez de migrer plusieurs applications, créez un runbook pour vous assurer que les applications critiques sont migrées en premier (ou quel que soit l'ordre le plus logique pour votre entreprise).
Conformité	Avant de migrer de votre environnement privé sur site vers un Cloud privé ou public, évaluez votre plan de migration et l'infrastructure du fournisseur de Cloud pour vous assurer que toutes les exigences de conformité seront respectées pendant et après la migration.
Dépassement de la portée ou des fonctionnalités	Les environnements Cloud riches en fonctionnalités peuvent facilement vous inciter à intégrer des fonctionnalités à la volée, ce qui entraîne des retards et des pertes de ressources. Ayez un projet clairement défini et respectez-le tout au long de la migration.

Copyright - Tout droit réservé - OFPPT



CHAPITRE 1

Identifier les stratégies de migration du SI dans le Cloud

1. Méthode du minimum d'efforts (Lift and shift, Rehost)
2. **Modification de la couche technique (Replateform, Redeploy)**
3. Réécriture de l'application (Rearchitect) et remplacement (Replace, Repurchasing)
4. Conservation (Retain) et décommissionnement (retire)

La stratégie de migration Replateform ou "lift-and-optimize"

Le re-plateforme ou réhébergement, autrement connu sous le nom de « **lift-tinker-and-shift** » ou « **lift-and-optimize** » est une stratégie qui vous permet d'apporter quelques modifications de configuration aux applications pour mieux s'adapter à l'environnement Cloud sans changer leur architecture de base afin d'obtenir des avantages tangibles.

Le re-platforming implique de modifier la façon dont les applications interagissent ensemble. Vous cherchez par exemple à réduire le temps que vous passez à gérer les instances de base de données en migrant vers une plateforme de base de données en tant que service comme Amazon RDS (Relational Database Service) ou Google CloudSQL.

En conséquence, vous pouvez tirer parti de plus d'avantages du Cloud, remodeler l'environnement d'approvisionnement et le rendre compatible avec le Cloud, affiner les fonctionnalités de l'application et éviter le travail de post-migration.

Avant de mettre en œuvre certaines améliorations du produit, il est important de garder à l'esprit que la base de code sous-jacente sera modifiée. Cela signifie que même des modifications insignifiantes nécessitent un nouveau test approfondi des performances de votre application. Une fois que vous avez mis en œuvre les ajustements et la mise à niveau planifiés, l'application peut être déplacée vers la plate-forme optimisée et les serveurs Cloud.

La stratégie de re-plateforme se situe quelque part entre un simple lift-and-shift et une réarchitecture plus profonde de l'application. Ainsi, les modifications dans la base de code sont plus susceptibles d'être mineures et ne sont pas censées modifier les fonctionnalités de base de l'application.

Copyright - Tout droit réservé - OFPPT

Les avantages de la stratégie Replateform

Les avantages d'une stratégie de migration du SI vers le Cloud suivant la méthode de réhébergement sont les suivants :

1. **Rentable** : cette approche est rentable et ne nécessite pas de projet de développement majeur.
2. **Commencez petit et évoluez selon vos besoins** : la reformulation vous permet de déplacer certaines charges de travail vers le Cloud, d'expérimenter l'environnement Cloud, de tirer des leçons, puis de passer à d'autres charges de travail, sans s'engager dans un effort de migration important.
3. **Fonctionnalité Cloud native :** la redéploiement permet aux applications de tirer parti des fonctionnalités Cloud telles que la mise à l'échelle automatique, les services de stockage et de traitement de données gérés, l'infrastructure en tant que code (IaaC), etc.

Copyright - Tout droit réservé - OFPPT

Les inconvénients de la stratégie Replateform

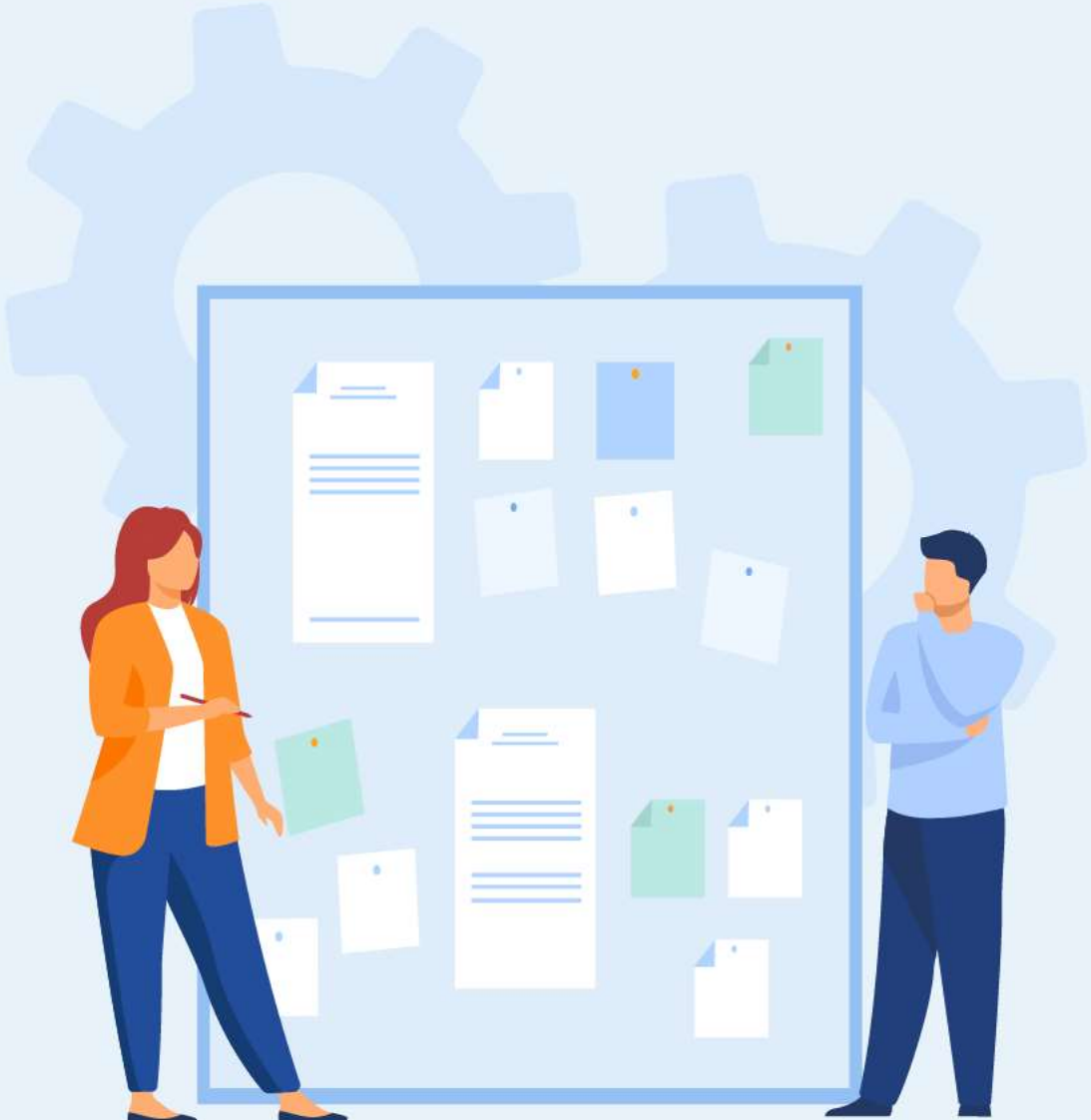
Les inconvénients d'une stratégie de migration du SI vers le Cloud suivant la méthode de réhébergement sont les suivants :

1. **La portée du travail peut s'étendre** : la « dérive de la portée » peut transformer un projet de re-plateforme en un projet de refactorisation à part entière. La gestion de la portée et la prévention des modifications inutiles sont essentielles pour atténuer ce problème.

2. **Changements agressifs :** pour minimiser le travail, vous devez vous en tenir à des composants Cloud communs et bien connus. Les composants spécialisés nécessitent souvent des modifications radicales de l'application et peuvent ne pas être utiles à moins qu'ils n'offrent une valeur commerciale élevée ou que leur utilisation ne soit inévitable.

3. **L'automatisation est nécessaire :** la re-plateforme est extrêmement limitée si la charge de travail résultante dans le Cloud est gérée manuellement. Cela signifie que vous devez investir dans une automatisation de base qui offre un certain niveau de flexibilité lors de l'exploitation du système dans le Cloud.

Copyright - Tout droit réservé - OFPPT



CHAPITRE 1

Identifier les stratégies de migration du SI dans le Cloud

1. Méthode du minimum d'efforts (Lift and shift, Rehost)
2. Modification de la couche technique (Replateform, Redeploy)
3. **Réécriture de l'application (Rearchitect) et remplacement (Replace, Repurchasing)**
4. Conservation (Retain) et décommissionnement (retire)

La stratégie de migration Réécriture de l'application (Rearchitect)

La **Réécriture** de l'application ou **Réarchitecture**, aussi connu sous le nom de «**Refactoring** » est une stratégie qui est motivée par un fort désir d'améliorer votre produit et représente le contraire de la migration lift-and-shift. Il est supposé qu'un objectif commercial spécifique sera défini dès le départ, par exemple en termes de disponibilité ou de fiabilité des performances de l'application. Parfois, cela signifie que vous devez repenser complètement la logique de votre application et développer la version Cloud native à partir de zéro pour la rendre native au Cloud.

En optant pour ce modèle de migration vers le Cloud, vous devez tenir compte du fait qu'il peut nécessiter plus de ressources en raison de la complexité accrue de sa mise en œuvre. D'autre part, il permet d'exploiter pleinement les avantages du Cloud natif, tels que la reprise après sinistre ou la conteneurisation de l'environnement applicatif.

Cette approche est aussi la plus coûteuse, la plus gourmande en ressources et la plus longue par rapport aux autres, mais elle s'avérera la plus intéressante à long terme. Certains autres défis auxquels vous pourriez être confronté peuvent être le manque de compétences en matière de Cloud, la livraison de projets et de programmes complexes, ou une interruption d'activité potentiellement importante.

La clé est de hiérarchiser les petits morceaux de votre application monolithique en tant que **microservices**, puis de les refactoriser. Autorisez également les applications héritées à s'exécuter sur site pendant que vous reconstruisez dans le Cloud pour éviter les interruptions.

Copyright - Tout droit réservé - OFPPT

Les avantages de la stratégie Rearchitect

Les avantages d'une stratégie de migration du SI vers le Cloud suivant la méthode de Réarchitecture sont les suivants :

1. **Économies à long terme** : peuvent réduire les coûts en faisant correspondre les besoins réels en ressources avec l'infrastructure Cloud. La possibilité d'évoluer selon les besoins réduit la consommation de ressources et offre un retour sur investissement durable de vos efforts de refactorisation.

2. **S'adapter à l'évolution des besoins :** les architectures Cloud natives et de microservices permettent aux applications de changer rapidement pour s'adapter aux nouvelles exigences des clients, en ajoutant de nouvelles fonctionnalités ou en modifiant les fonctionnalités existantes.

3. **Résilience accrue** : En découplant les composants de l'application et en connectant ensemble des solutions gérées qui offrent une haute disponibilité, l'application hérite de la durabilité de ce Cloud.

Copyright - Tout droit réservé - OFPPT

Les inconvénients de la stratégie Rearchitect

Les inconvénients d'une stratégie de migration du SI vers le Cloud suivant la méthode de Rearchitect sont les suivants :

1. **Verrouillage du fournisseur :** plus votre application est native du Cloud, plus elle est susceptible de consommer de fonctionnalités Cloud. Cela rend les applications étroitement couplées au Cloud public que vous utilisez.
2. **Temps** : la réarchitecture est gourmande en ressources et beaucoup plus complexe qu'une migration lift-and-shift, ce qui signifie que les projets prennent beaucoup plus de temps pour commencer à montrer de la valeur commerciale.
3. **Compétences** : la réarchitecture n'est pas pour les débutants. Cela nécessite des compétences avancées en matière de codage, d'automatisation et de DevOps.
4. **Se tromper** : la réarchitecture signifie modifier de nombreux aspects de l'application, il existe donc un risque élevé d'erreurs au niveau du code, de la configuration et de l'infrastructure. Chaque erreur peut entraîner des retards, des augmentations de coûts et d'éventuelles pannes.

Copyright - Tout droit réservé - OFPPT

La stratégie de migration Remplacement (Replace, Repurchasing)

Le **Remplacement** de l'application ou **Réachat**, également connu sous le nom de stratégie « **drop and shop** », remplace l'application sur site par un logiciel fourni par le fournisseur natif du Cloud. Cela signifie, que dans cette stratégie, vous modifiez l'application propriétaire utilisée pour la nouvelle plate-forme ou le nouveau service basé sur le Cloud.

Souvent, cela signifie que vous abandonnez le contrat de licence existant (ou qu'il expire) et optez pour une nouvelle plate-forme ou un nouveau service à sa place. Par exemple, vous pouvez choisir de passer de votre ancien système CRM à un nouveau CRM SaaS qui répond mieux aux exigences de votre organisation.

La nouvelle version Cloud mise à niveau vous offre un meilleur rapport qualité-prix avec une efficacité accrue, des économies sur le stockage des applications et les coûts de maintenance. Cependant vous pourriez être confronté à certains obstacles qui peuvent apparaître lors du rachat qui sont la formation de votre personnel au nouveau logiciel ou au verrouillage du fournisseur. Les plates-formes **SaaS** offrent une personnalisation et un contrôle limités en comparaison. Vous pourriez donc ressentir de perdre une solution personnalisée sur site hautement adaptée.

Cas d'utilisation :

Utilisez la stratégie Réachat si :

- Vous remplacez un logiciel pour des fonctions standard comme la finance, la comptabilité, le CRM, la GRH, l'ERP, la messagerie électronique, le CMS, etc.
- Une ancienne application n'est pas compatible avec le Cloud

Copyright - Tout droit réservé - OFPPT

Les avantages de la stratégie Remplacement (Replace, Repurchasing)

Ci-dessous quelques avantages pour l'adoption de la stratégie de Remplacement/Réachat :

Abandonnez le passé, saisissez l'avenir	Remplacez les systèmes obsolètes par des appareils modernes et SaaS.
Simplifiez l'approvisionnement	Par exemple AWS Marketplace offre un mécanisme d'approvisionnement unifié pour acheter des solutions prédéfinies auprès d'un large éventail de fournisseurs. La place de marché comprend des produits SaaS, des modèles de machine virtuelle, des appliances virtuelles, des modèles d'apprentissage automatique, etc.
Réduisez les compétences internes requises	Les systèmes achetés sont construits (et, dans le cas du SaaS, exploités) par des spécialistes. Vous n'avez pas besoin d'embaucher, de former et de conserver ces compétences en interne.
Réduire les efforts/augmenter la vitesse de migration	Moins il y a à migrer et à opérer, plus c'est rapide, moins cher et moins risqué.

Copyright - Tout droit réservé - OFPPT

Les risques liés à la stratégie Remplacement (Replace, Repurchasing)

Ci-dessous quelques risques liés à l'adoption de la stratégie de Remplacement/Réachat :

Perte de contrôle	L'organisation ne peut plus influencer le calendrier des nouvelles fonctionnalités, l'abandon des anciennes fonctionnalités ou le moment de la mise à niveau vers de nouvelles versions. Le fournisseur ne peut pas s'engager sur un SLA acceptable pour le service. Ils peuvent subir des pannes ou des pertes de données qui ne peuvent pas être atténuées en interne. Leurs violations de données peuvent exposer vos clients à des préjudices et votre organisation à des sanctions et à des atteintes à la réputation.
Risques commerciaux	Le fournisseur que vous avez choisi peut faire faillite. Ils peuvent être acquis par l'un de vos concurrents. Ils peuvent augmenter les prix ou résilier un service dont vous dépendez.
Souveraineté des données	où résident les données (et leurs sauvegardes) et comment sont-elles gérées ? Cela répond-il à vos besoins de conformité ?
Accès au système	quels autres systèmes doivent se connecter au système acheté ? Comment fonctionnent l'authentification unique (SSO) et l'autorisation ? Y a-t-il des implications en matière de réseau et de sécurité ?

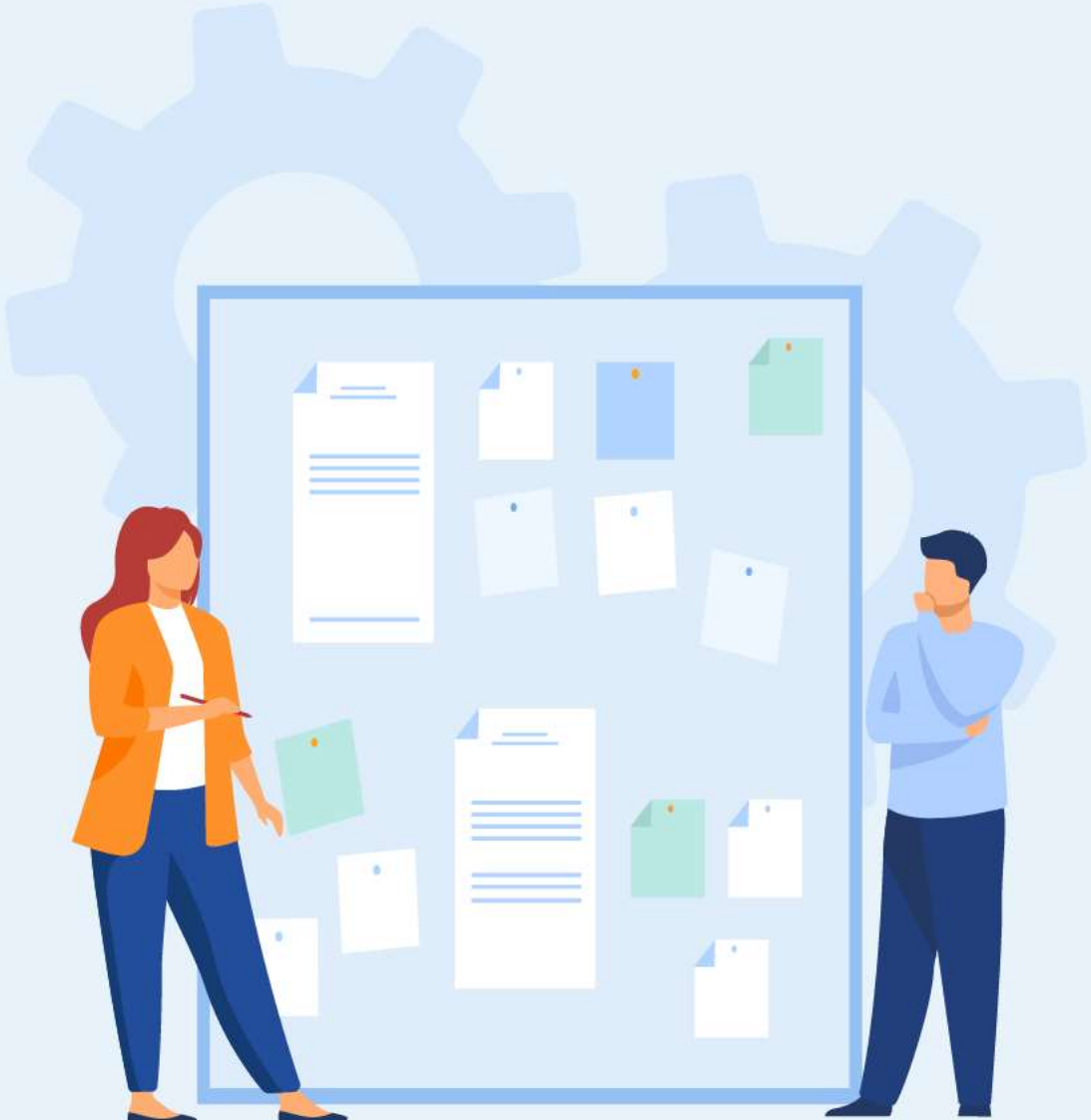
Copyright - Tout droit réservé - OFPPT

Les risques liés à la stratégie Remplacement (Replace, Repurchasing)

Ci-dessous quelques risques liés à l'adoption de la stratégie de Remplacement/Réachat :

Intégrations et dépendances	le passage au SaaS vous obligera-t-il à mettre à niveau et à reconfigurer vos systèmes ? Les mêmes versions et options de configuration sont-elles disponibles, ou la mise à niveau sera-t-elle rétrocompatible ?
Friction d'approvisionnement	votre équipe et vos procédures d'approvisionnement peuvent être incompatibles avec cette nouvelle façon d'acheter des applications. Ils devront envisager des appareils (licence louée), Apportez votre propre licence, SaaS et offres privées.
Finance	La finance est-elle prête à gérer des coûts futurs imprévisibles ? Jetez un œil à la gestion financière dans le Cloud avec FinOps.
Opérations	votre équipe des opérations peut-elle s'adapter pour administrer le système acheté ? Les migrations concernent tout autant les personnes et les processus que le code d'application et les données.

Copyright - Tout droit réservé - OFPPT



CHAPITRE 1

Identifier les stratégies de migration du SI dans le Cloud

1. Méthode du minimum d'efforts (Lift and shift, Rehost)
2. Modification de la couche technique (Replateform, Redeploy)
3. Réécriture de l'application (Rearchitect) et remplacement (Replace, Repurchasing)
4. **Conservation (Retain) et décommissionnement (retire)**

La stratégie de migration Conservation (Retain)

La **stratégie de conservation** de l'application ou **Retain**, aussi connu sous le nom de « **Re-visite** » consiste à revisiter certaines applications/parties critiques de vos actifs numériques qui nécessitent une refactorisation importante avant de les migrer vers le Cloud.

En effet, certains composants de votre infrastructure informatique peuvent être conservés sur votre infrastructure existante. Une organisation peut souhaiter conserver certaines charges de travail et bases de données autonomes en raison de problèmes de sécurité, d'exigences de latence, de conformité ou de contraintes réglementaires, ou ce n'est tout simplement pas rentable.

Par exemple, vous devrez peut-être vous conformer aux exigences réglementaires régissant les emplacements dans lesquels certaines informations sont stockées. Lors de la catégorisation de la charge de travail pour ce type de migration, vous créez une infrastructure hybride dans laquelle certaines charges de travail sont hébergées dans le Cloud et certaines charges de travail sont conservées sur site.

Cette stratégie est souvent utilisée dans le déploiement de Cloud hybride par les organisations pour assurer la continuité des activités lors de migrations à grande échelle qui prennent plusieurs années.

Cas d'utilisation :

- Vous adoptez un modèle de Cloud hybride lors de la migration;
- Une application héritée n'est pas compatible avec le Cloud et fonctionne bien sur site;
- Vous décidez de revisiter une application plus tard.

Copyright - Tout droit réservé - OFPPT

La stratégie de migration décommissionnement (retire)

Dans cette stratégie, vous vous débarrassez des applications qui ne sont plus nécessaires ou productives pour votre portefeuille informatique. En effet, pour de nombreuses applications et environnements complexes, certains composants de l'infrastructure peuvent être facilement désactivés sans aucune diminution de productivité ou perte de valeur pour les consommateurs finaux.

Ceci est réalisé en mettant hors service ou en archivant les pièces inutiles tout en remplaçant leurs fonctionnalités par d'autres services et composants. En conséquence, vous pouvez réduire considérablement la complexité de votre IT, de votre architecture, de votre stockage, de vos licences et de votre sauvegarde, ce qui rend votre infrastructure plus légère.

Bien que cela semble facile, la mise hors service des applications est un processus complexe et essentiel pour décider quelles applications retirer. Cela doit être fait dans les premières étapes de la planification afin que vous puissiez migrer des applications ou des services essentiels, réduire la portée des applications à migrer et économiser des ressources.

Cas d'utilisation :

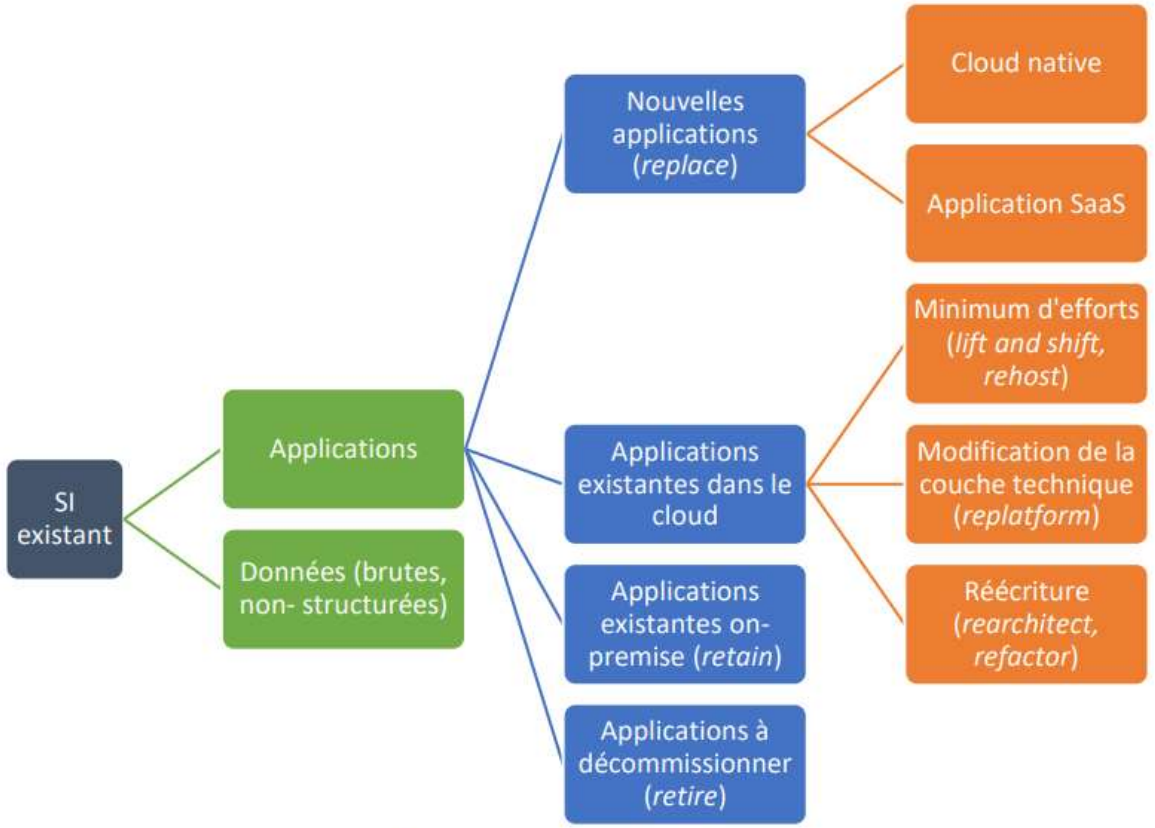
- Archivez les applications qui contiennent des données utiles.
- Supprimez les applications avec des capacités de duplication pour réduire les coûts.
- Retirez les applications dont les fonctionnalités peuvent être ajoutées à une autre via des microservices.

Copyright - Tout droit réservé - OFPPT

PARTIE 3

Arborescence de migration des applications

De façon très générale, non exhaustive, on peut représenter cette arborescence simplifiée ainsi :



Arborescence de décisions possibles
Source : GT Cigref

Copyright - Tout droit réservé - OFPPT

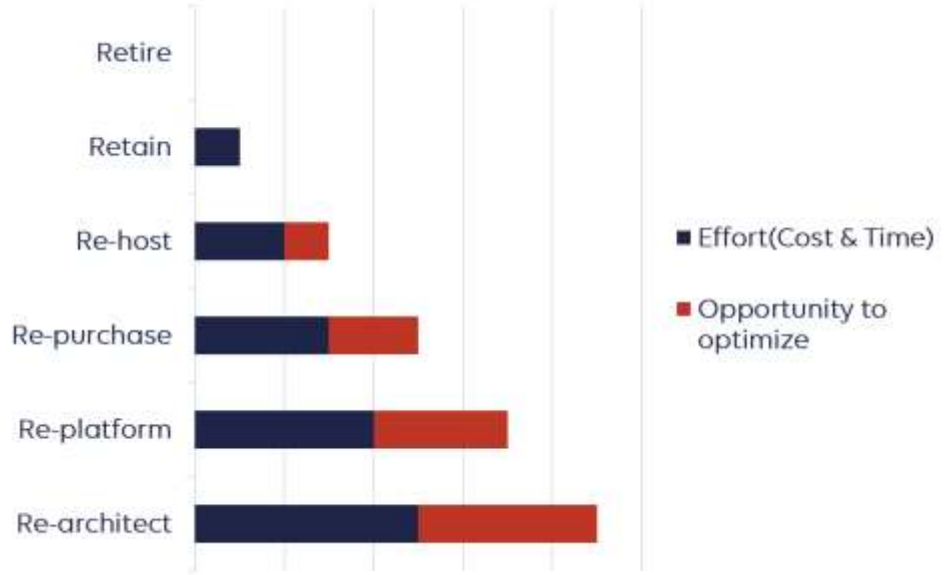
Conclusion

Lorsque vous évaluez laquelle des stratégies convient aux besoins de migration de votre organisation, gardez à l'esprit que chaque migration vers le Cloud est unique.

Les types de migration vers le Cloud mentionnés ci-dessus ne sont pas des solutions toutes faites pour chaque organisation. Ces options doivent servir de base à l'élaboration de la stratégie finale, qui sera adaptée aux besoins spécifiques de votre entreprise. Pour développer une stratégie de migration réussie , il est recommandé d'examiner le processus de migration d'un point de vue centré sur l'application plutôt que sur l'infrastructure.

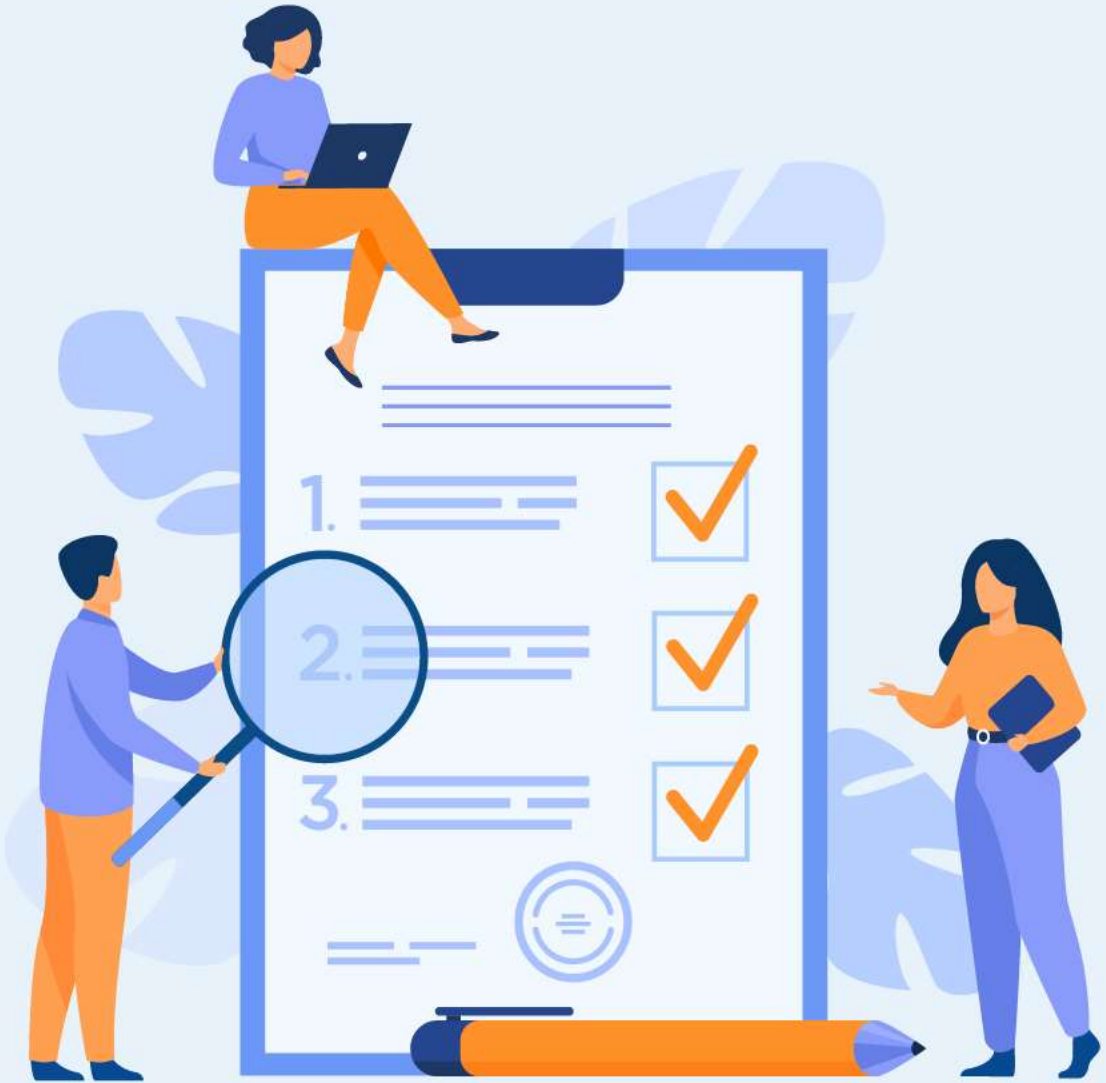
Prendre la bonne décision implique également de comprendre comment votre nouvel environnement fonctionnera une fois que vous aurez transféré vos données dans le Cloud et quels sont les avantages spécifiques de l'utilisation d'un environnement Cloud pour votre entreprise.

Ces six stratégies diffèrent par leur complexité, leur opportunité d'optimisation et leurs efforts (argent et temps). Le graphique ci-après devrait vous aider à comprendre laquelle des stratégies est la plus simple et laquelle est la plus complexe.



PARTIE 3

Copyright - Tout droit réservé - OFPPT



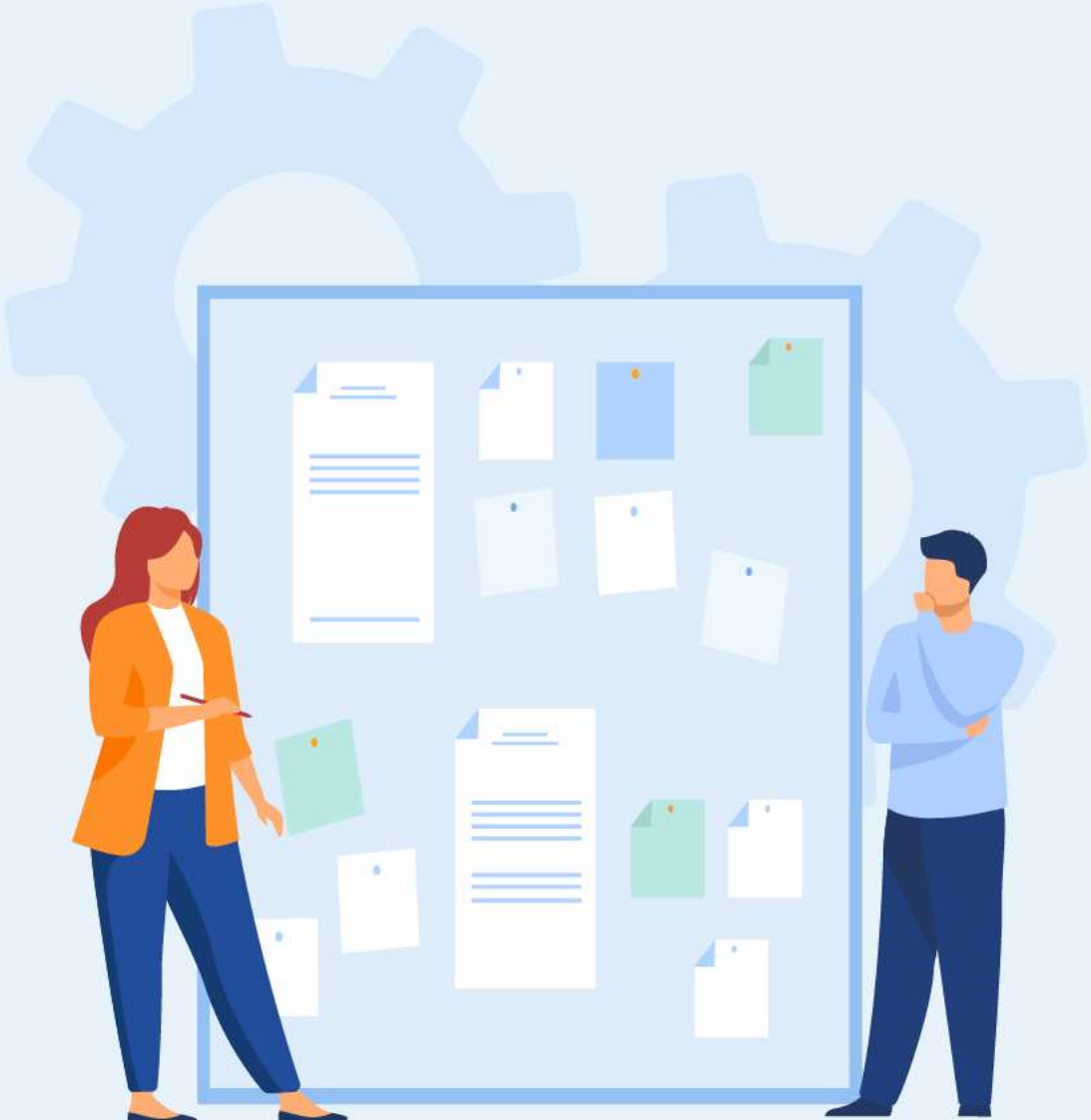
CHAPITRE 2

Adopter une approche DevOps

Ce que vous allez apprendre dans ce chapitre :

- Méthodes d’agiles
- Intégration continue (CI)
- Déploiement continue (CD)
- DevOps vs DevSecOps

7 heures



CHAPITRE 2

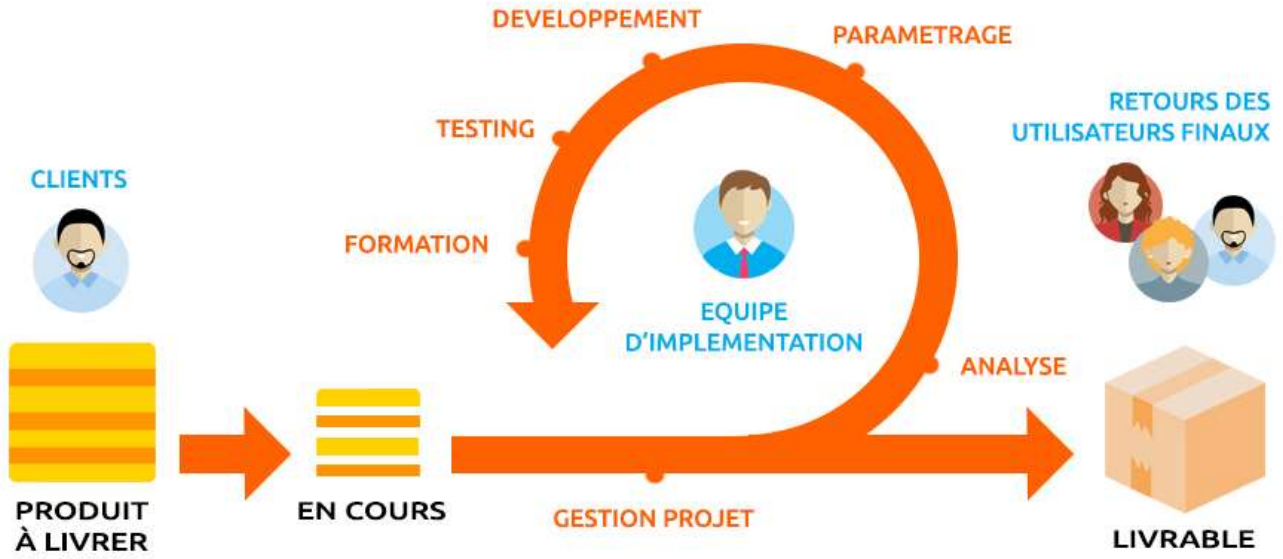
Adopter une approche DevOps

1. **Méthodes d’agiles**
2. Intégration continue (CI)
3. Déploiement continue (CD)
4. DevOps vs DevSecOps

Présentation

En développement logiciel, les méthodes Agiles disponibles sont nombreuses et peuvent être source de confusion. Les méthodes Agiles les plus populaires en usage aujourd'hui sont :

- l'eXtrême Programming (XP),
- Scrum,
- Feature Driven Development (FDD),
- Lean Software Development,
- Agile Unified Process (Agile UP ou AUP),
- Crystal
- Dynamic Systems Development Method (DSDM).



Copyright - Tout droit réservé - OFPPT

Extreme Programming (XP)

Extreme Programming, ou XP, est une méthode agile de gestion de projet particulièrement bien adaptée aux projets de développement informatique. Elle a été conçue par Kent Beck pour accélérer les développements alors qu'il travaillait pour la société Chrysler. L'idée lui est venue alors qu'il devait intervenir sur un logiciel de paie écrit en langage Smalltalk ayant accumulé une dette technique considérable, le rendant particulièrement complexe à maintenir et à faire évoluer.

Le principe fondamental de la méthode XP est de faire collaborer étroitement tous les acteurs du projet et d'opter pour des itérations de développement très courtes. La planification des tâches reste très souple et l'estimation des charges simplifiée par des projections à très court terme. Ainsi la correspondance entre ce qu'attend le client et les réalisations est garantie. Les fonctionnalités sont livrées régulièrement, afin d'être testées et validée au travers de prototypes opérationnels.

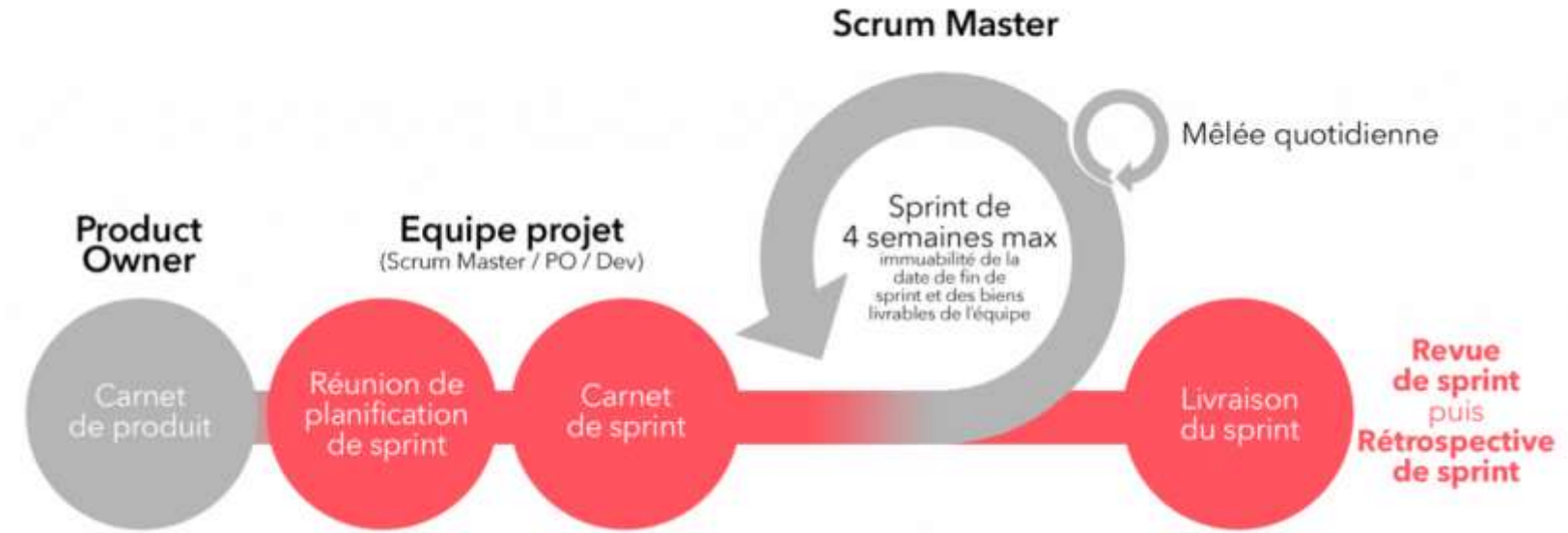
L'Extreme Programming préconise également le travail en binôme des développeurs, facilitant ainsi la production d'un code simple, facilement lisible et maintenable.

Copyright - Tout droit réservé - OFPPT

Scrum

La méthode agile Scrum particulièrement destinée à la gestion de projets informatiques tient son nom du monde du rugby. Le principe de Scrum est de pouvoir modifier la direction prise par le projet au fur et à mesure de son avancement. C'est exactement ce qui se passe lors d'un match de rugby, lors d'une mêlée (« scrum » en anglais).

La mêlée est donc une phase essentielle au rugby comme dans la gestion de projet. Si les conditions de réussite ne sont pas remplies, alors il faut réorienter le projet pour repartir sur de meilleures bases. Le client est étroitement impliqué grâce à la livraison régulière de prototypes opérationnels permettant de valider les développements. Cette gestion dynamique permet de s'assurer de la correspondance entre le besoin exprimé et le produit livré, et de réorienter au besoin les futurs développements.



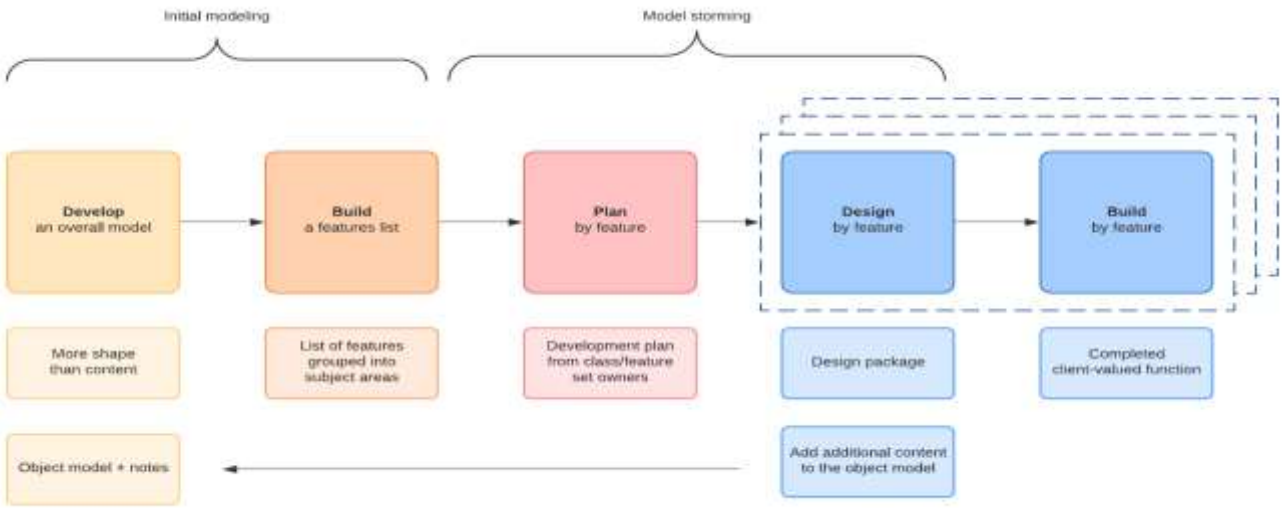
Copyright - Tout droit réservé - OFPPT

Feature Driven Development (FDD)

Le Développement Dirigé par les Fonctionnalités, en français, est une méthode de gestion de projet basée sur la gestion des risques. Les développements sont organisés en itérations courtes autour de fonctionnalités testables par l'utilisateur. L'utilisateur est ainsi impliqué dans les développements, peut suivre l'avancement du projet et la validation des fonctionnalités. Aucune méthode de programmation n'est préconisée, c'est réellement la fonctionnalité qui est mise en avant.

Un projet géré par FDD est découpé en plusieurs grandes étapes. La première consiste en la constitution d'un modèle général du produit, qui va définir le périmètre global de réalisation. Vient ensuite la construction de la liste complète des fonctionnalités à réaliser. Il est impératif lors de cette étape d'impliquer au maximum le client. Ces fonctionnalités sont finalement regroupées en fonction de leurs caractéristiques communes et priorisées. Les deux dernières étapes verront le jour sous la forme d'itérations, et englobent d'une part la conception technique des fonctionnalités, puis leur réalisation.

Cette méthode donne une importance plus grande à la phase de conception, quitte à démarrer la réalisation plus lentement, afin d'avoir un modèle plus solide.



Copyright - Tout droit réservé - OFPPT

Lean Software Development

Le Lean Software Development est basé sur sept grands principes.

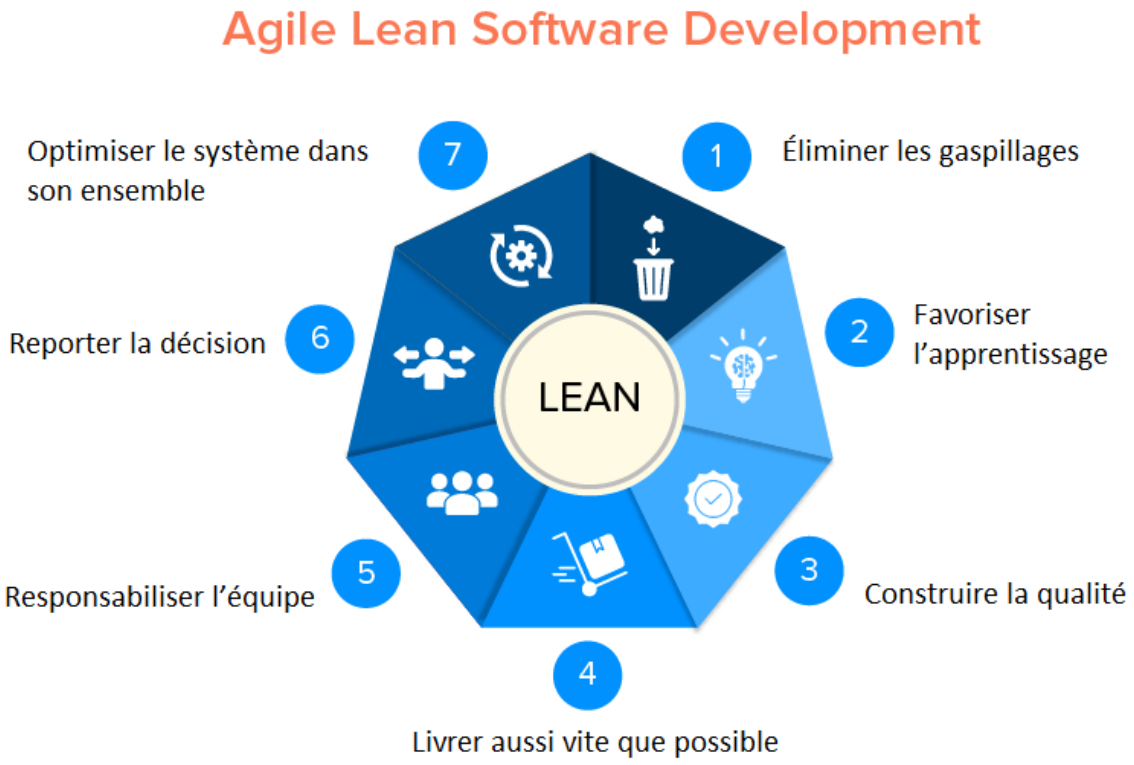
- Éliminer les gaspillages (finition partielle, processus inutiles, fonctionnalités non nécessaires, modification de l'équipe, retards…),
- Favoriser l'apprentissage (multiplication des sources d'apprentissage, synchronisation des équipes…),
- Construire la qualité (elle doit être placée au cœur du projet, de la conception à la réalisation),
- Livrer vite (livraisons rapides et régulières de façon à avoir un retour client rapide également),
- Responsabiliser l'équipe (favoriser l'autonomie et le leadership des équipes, partir du principe que les intervenants connaissent leur travail, faciliter le développement de l'expertise),
- Reporter les décisions (jusqu'au dernier moment raisonnable, pour éviter de longues discussions sources de pertes de temps et les décisions irrévocables),
- Optimiser le système dans son ensemble (mise en place de mesures de performances complètes, pour avoir en permanence une vision globale du produit, et gérer les différentes interactions et dépendances).

Avec la méthode Lean, la qualité est réellement placée au cœur de la gestion du projet, en optimisant notamment l'ensemble des processus d'apprentissage, de décision, de livraison et de mesure de performances.

Copyright - Tout droit réservé - OFPPT

Lean Software Development

La figure suivante représente les sept grands principes précédents:



Copyright - Tout droit réservé - OFPPT

Agile Unified Process (Agile UP or AUP)

Agile Unified Process (ou Processus Unifié Agile) est une version simplifiée du Rational Unified Process, ou RUP. Il s'agit d'une méthode de développement d'applications métier utilisant les techniques agiles du TDD (Test Driven Development ou développement piloté par les tests), du MDD (Model Driven Development ou développement piloté par le modèle) et de la gestion du changement.

La méthode est divisée en quatre phases :

- Lancement : identification du périmètre du projet, définition de la ou des architectures potentielles pour le système, implication des intervenants et obtention du budget.
- Conception : définir l'architecture du système et démonstration de sa pertinence.
- Réalisation : développement du logiciel lors d'un processus incrémental dans l'ordre de priorité des fonctionnalités.
- Livraison : validation et déploiement du système en production.

Copyright - Tout droit réservé - OFPPT

Crystal (Clear/Orange)

La méthode Crystal Clear est particulièrement adaptée aux petites équipes de développement. Idéalement, l'équipe est composée d'un architecte et de deux à six ou sept développeurs, situés à proximité les uns des autres, de façon à faciliter la communication, dans un local calme. Des tableaux blancs servent de supports afin que tous aient un accès rapide à toutes les informations. Les rythmes de développement et de livraison sont rapides (toutes les deux semaines ou une fois par mois) afin que les utilisateurs puissent passer les tests.

Durant tout le processus de développement, l'équipe se remet en question en permanence afin d'améliorer continuellement sa façon de travailler.

Les 7 axes qu'il faudra suivre avec le Crystal Clear

- Faire des livraisons fréquentes
- Avoir des réflexions d'amélioration dès que le besoin est présent
- Avoir une communication osmotique
- L'équipe doit se sentir sécurisée : transparence, communication orale, chaque membre peut répondre aux questions
- Concentration dédiée (objectifs connus de tous, temps de travail sans distraction disponible)
- Accès facilité aux utilisateurs clés
- Environnement technique favorable (tests automatisés, gestions des confs)

Copyright - Tout droit réservé - OFPPT

Dynamic Systems Development Method (DSDM)

Cette méthode s'articule autour de neufs grands principes qui sont la participation des utilisateurs, l'autonomie de l'équipe projet, la transparence des développements, l'adéquation avec le besoin, le développement itératif et incrémental, la réversibilité permanente, la synthèse du projet, les tests automatisés et continus et enfin la coopération entre tous les intervenants.

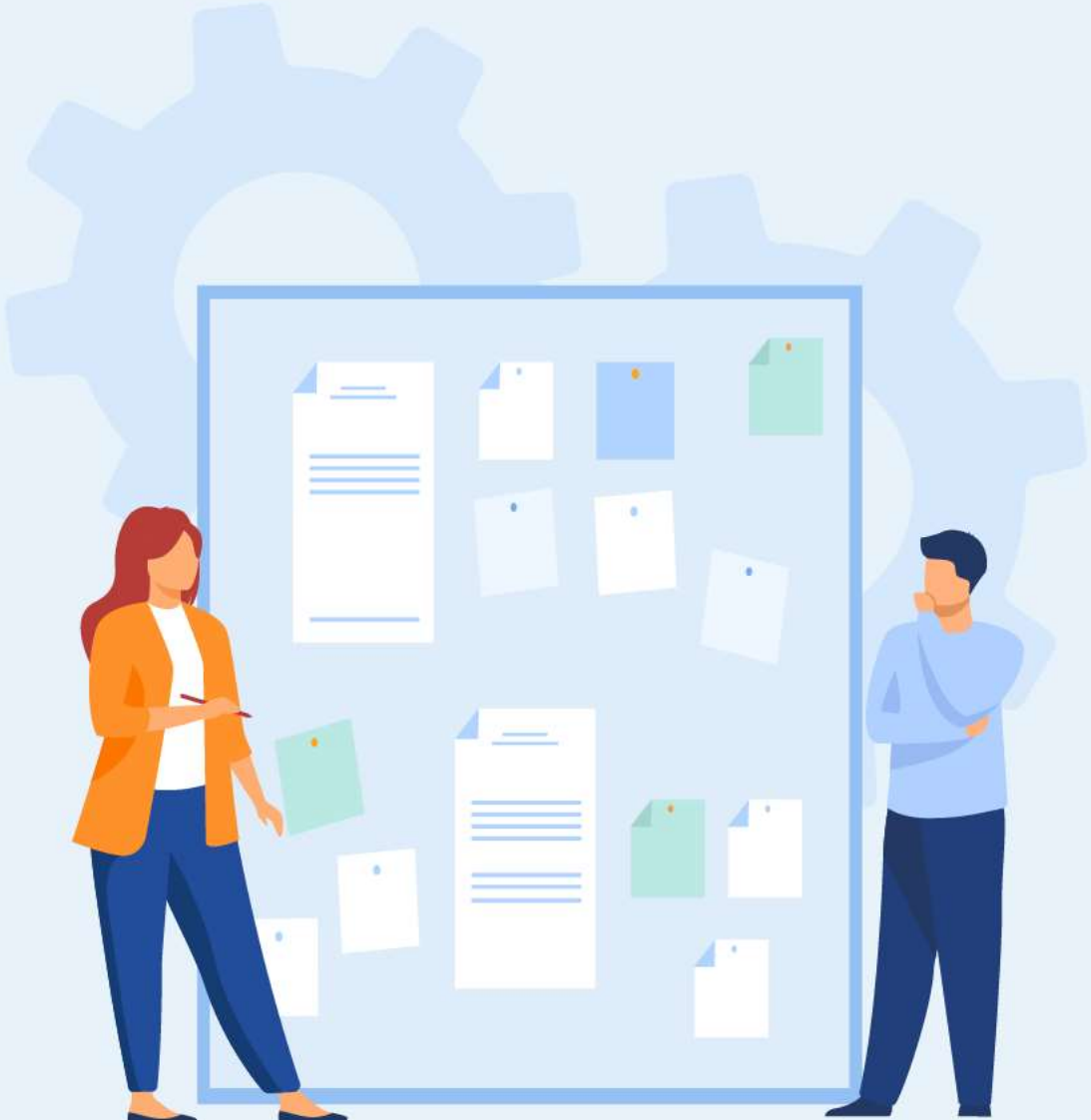
Le projet commence par une étude de faisabilité afin de décider s'il faut le faire ou non. Un rapport est rédigé, et éventuellement, un prototype est créé pour démontrer la faisabilité de l'application. S'il a été décidé de continuer, une analyse fonctionnelle est réalisée et les spécifications sont rédigées. A partir de ce moment-là, des itérations de conception technique et de développement sont mises en place, puis pour finir, l'application est livrée en production.

Copyright - Tout droit réservé - OFPPT

Dynamic Systems Development Method (DSDM)

- **Implication des utilisateurs** : ils doivent être présents tout au long du développement du projet voire les considérer comme membres de l'équipe.
- **Valorisation de l'autonomie** : L'équipe prend part dans le processus décisionnel
- **Visibilité du résultat** : livrer régulièrement les porteurs de projet et recevoir ses feedbacks.
- **Adéquation** : le livrable doit être fonctionnel et en adéquation avec les exigences du client.
- **Développement itératif et incrémental** : l'amélioration continue du projet à partir des feedbacks.
- **Réversibilité des incréments** : Le travail de développement doit se faire de manière à ce que le retour en arrière soit possible.
- **Synthèse** : Un schéma directeur esquisse les niveaux objectif et vision du projet avant de commencer le travail de développement.
- **Validation des tests** : il faut garantir le fonctionnement du livrable par l'automatisation de tests.
- **Coopération** : Les éventuels changement doivent être acceptés par l'équipe de travail.

Copyright - Tout droit réservé - OFPPT



CHAPITRE 2

Adopter une approche DevOps

1. Méthodes d’agiles
2. **Intégration continue (CI)**
3. Déploiement continue (CD)
4. DevOps vs DevSecOps

Présentation

L'intégration continue (CI) est le processus de génération et de test automatique du code chaque fois qu'un membre de l'équipe valide les modifications apportées au code dans le contrôle de version. Une validation de code dans la branche principale ou de jonction d'un référentiel partagé déclenche le système de génération automatisé pour générer, tester et valider la branche complète.

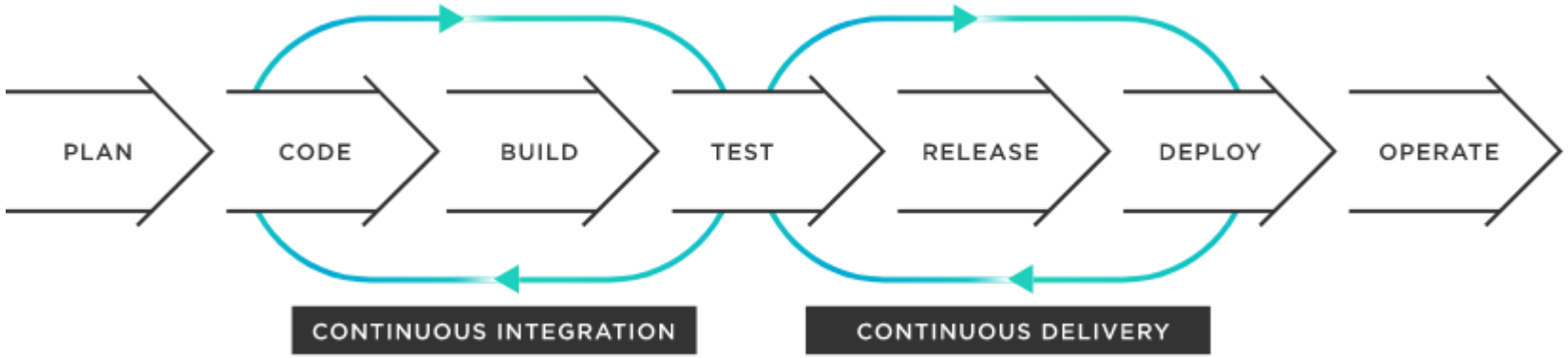
CI encourage les développeurs à partager leur code et leurs tests unitaires en fusionnant leurs modifications dans le référentiel de contrôle de version partagé chaque fois qu'ils terminent une tâche.

Les développeurs de logiciels travaillent souvent de manière isolée, puis doivent intégrer leurs modifications au reste de la base de code d'une équipe. Les jours ou semaines d'attente pour intégrer le code peuvent créer de nombreux conflits de fusion, résoudre difficilement les bogues, les stratégies de code divergentes et les efforts dupliqués. CI évite ces problèmes, car il nécessite que le code de l'équipe de développement se fusionne en continu vers la branche de contrôle de version partagée.

Copyright - Tout droit réservé - OFPPT

Présentation

L'intégration continue est la pratique consistant à intégrer en continu les modifications du code de différents développeurs travaillant sur le même code dans un seul projet logiciel. Cette intégration se met généralement à jour automatiquement comme un processus continu tout au long de la journée afin de garantir que toutes les modifications apportées au code sont correctement enregistrées. Cette stratégie est un élément essentiel d'un système de développement logiciel Agile, qui s'articule autour du concept de collaboration, de conception à l'échelle et de construction durable.



Copyright - Tout droit réservé - OFPPT

Avantages de l'intégration continue

La raison pour laquelle tant d'équipes Agile utilisent l'intégration continue est qu'elle fonctionne incroyablement bien pour résoudre de nombreux problèmes de développement logiciel. Elle garantit que deux développeurs ne travaillent pas en même temps sur le même morceau de code, ce qui évite les doublons inutiles.

L'intégration continue garantit également que l'équipe travaille toujours sur la mise à jour la plus récente du logiciel et qu'elle s'appuie donc sur les changements les plus récents. Cela signifie qu'il n'y a pas de chaos de dernière minute à la date de la sortie, alors que chacun télécharge son code et essaie de vérifier ses versions par rapport à d'autres tâches et sections de travail.

En matière de développement, une modification de ligne, ou même quelque chose d'aussi minime qu'un point ou une parenthèse erronée, peut par inadvertance casser d'autres parties du logiciel. Des mises à jour fréquentes permettent d'identifier plus facilement la cause du problème et de le corriger avant de passer à d'autres domaines. Elles obligent également les développeurs à sauvegarder fréquemment leur travail et garantissent que les morceaux de code finis sont stockés dans un référentiel partagé, souvent dans le cloud, où ils sont à l'abri des perturbations locales d'électricité ou de connexion à Internet.

L'intégration continue permet d'éviter les conflits et les échecs d'intégration. Lorsque d'autres développeurs mettent à jour leur travail, cela affecte d'autres travaux qui n'ont pas encore été soumis. Les mises à jour régulières minimisent ces conflits potentiels. En fait, tout changement, conflit ou problème peut être rapidement identifié peu après la soumission du code. Cela signifie que le développeur peut revenir immédiatement à son travail pour le corriger, tant qu'il est encore frais dans sa mémoire.

Les vérifications constantes du code aident également les développeurs à créer un code modulaire moins complexe, et la nature automatisée de l'intégration continue permet de réduire les tests manuels qui prennent beaucoup de temps. Enfin, il y a l'avantage d'avoir la disponibilité constante de la version finale actuelle pour le déploiement continu.

Copyright - Tout droit réservé - OFPPT

Piliers de l'intégration continue

L'intégration continue s'articule autour d'un certain nombre de bonnes pratiques logicielles. Elle englobe des techniques telles que les tests automatisés, l'automatisation du build, le contrôle de version et les déploiements automatisés. Chacune de ces techniques possède son propre écosystème de philosophies et d'outils:

- **Gestion du contrôle des versions:**

Le contrôle des versions est un pilier essentiel de l'intégration continue. La gestion de la source de la version permet de communiquer et de résoudre les conflits entre les développeurs travaillant simultanément sur la même base de code.

- **Tests automatisés:**

Tout projet logiciel nécessite des tests approfondis et répétés. Cela peut prendre énormément de temps et s'avérer répétitif, c'est pourquoi des outils ont été développés pour automatiser certaines parties du processus de test. Ces outils de test exécutent automatiquement des cas de test sur des parties spécifiques du système. Lorsqu'un développeur introduit du code dans le référentiel, cela déclenche le démarrage des tests automatisés.

- **Automatisation du build:**

Les builds sont souvent désignés comme l'instantané du module de la version actuelle. Ce sont ces builds qui sont finalement distribués aux utilisateurs finaux via un certain nombre de canaux potentiels différents. Les outils d'intégration continue permettent de rationaliser le processus de création d'une version. Les automates de builds peuvent également configurer les versions pour qu'elles soient déclenchées par certains événements. Par exemple, lorsqu'un nouveau morceau de code est fusionné dans la branche de production de la base de code, cela déclenche l'automatisation du téléchargement du build vers un serveur distant, auquel les utilisateurs peuvent accéder pour le télécharger.

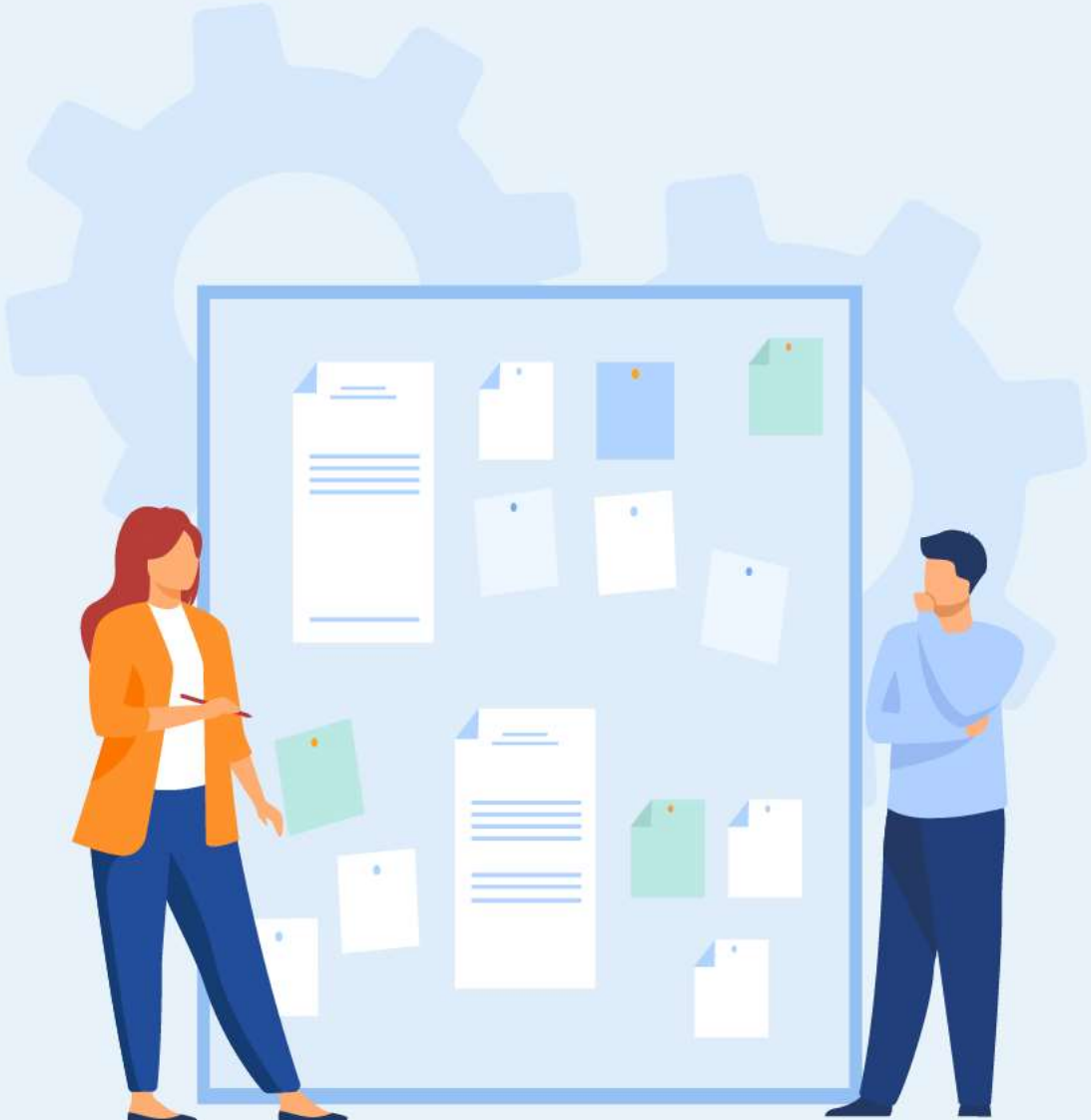
Copyright - Tout droit réservé - OFPPT

Piliers de l'intégration continue

- **Déploiements automatisés:**

Chaque processus de déploiement est différent en fonction de ce qui est construit. Par exemple, un logiciel automatisé déploiera une page Web sur un serveur Web. Le build créé à l'étape précédente sera automatiquement copié sur des serveurs Web pour un projet Web, téléchargé sur un magasin pour une mise à jour d'application, ainsi que sur tout autre canal sur lequel il doit être déployé.

Copyright - Tout droit réservé - OFPPT



CHAPITRE 2

Adopter une approche DevOps

1. Méthodes d’agiles
2. Intégration continue (CI)
3. **Déploiement continue (CD)**
4. DevOps vs DevSecOps

Définition

Le déploiement continu (Continuous Deployment, CD) est un processus de publication de logiciels utilisant des tests automatisés pour valider que toutes les modifications apportées à une base de code sont exactes et prêtes à être déployées de manière autonome dans un environnement de production. Ce cycle de publication de logiciels a progressé et évolué au cours des dernières années.

Une approche d'ingénierie logicielle, le CD fournit fréquemment des fonctionnalités logicielles par le biais de déploiements automatisés.

En tant que processus de publication de logiciels, le CD teste et vérifie automatiquement les nouveaux morceaux de code et les pousse dans un environnement de production s'ils passent les tests automatisés.

Le développement continu est une extension de l'intégration continue. Alors que l'intégration continue garantit que les bogues sont trouvés et corrigés, le déploiement continu garantit que vos clients disposent toujours du logiciel le plus à jour en diffusant automatiquement les modifications du code. Le déploiement continu permet de diffuser des mises à jour pour vos clients de manière rapide et fiable. Contrairement au déploiement traditionnel, le déploiement continu doit avoir lieu sans aucune intervention manuelle. L'objectif principal du déploiement continu est de réduire le délai de mise à jour des logiciels et d'accélérer leur disponibilité pour les utilisateurs finaux.

Copyright - Tout droit réservé - OFPPT

Etapes du déploiement continu

Étape 1 : test et vérification

Les tests automatisés du nouveau code sont une étape cruciale du déploiement continu. Les tests automatisés comprennent un ensemble de scénarios de test qui ressemblent étroitement aux cas d'utilisation en temps réel. La suite de tests exerce le nouveau code et le fait passer par tous ces cas d'utilisation. Un système de vérification robuste et automatisé teste non seulement la fonctionnalité du nouveau code, mais aussi les exigences non fonctionnelles telles que les performances, la sécurité et la convivialité.

Les tests automatisés garantissent que le nouveau code se comporte comme prévu et qu'il n'introduit pas de nouveaux problèmes dans le logiciel, connus sous le nom de problèmes de régression. Lorsque le nouveau code passe tous les tests automatisés, il est automatiquement mis à la disposition des utilisateurs finaux. Cependant, le déploiement continu ne s'arrête pas là.

Étape 2 : suivi constant

Dans le cadre du déploiement continu, un système permet de surveiller en permanence le comportement et les performances du nouveau code dans l'environnement de production. Ce n'est pas seulement le nouveau code, mais l'ensemble du système logiciel qui est surveillé en temps réel. Une infrastructure de déploiement continu robuste déclenche des alarmes si et quand le nouveau code provoque un problème dans le logiciel au sein de l'environnement de production. Il peut s'agir de déclencher le cadre de test ou d'appeler le propriétaire du code. Cette surveillance et ces alertes sont réalisées rapidement et en temps réel, de sorte que tout retour en arrière nécessaire peut être effectué sans accroc.

Copyright - Tout droit réservé - OFPPT

Etapes du déploiement continu

Étape 3 : annulation des modifications

Un pipeline de déploiement continu robuste doit être capable de répondre aux problèmes de production et de s'en remettre rapidement, efficacement et durablement. Cela a souvent lieu en retirant automatiquement les nouvelles modifications du code, ce que l'on appelle le retour en arrière des modifications. La possibilité de revenir à une version stable du logiciel est cruciale, car le plus souvent les utilisateurs finaux utilisent activement le logiciel. Dans le cadre de ce processus de retour en arrière, le « temps moyen de récupération (Mean Time To Recovery, MTTR) » est une mesure importante de la maturité des systèmes de déploiement continu. Il s'agit du temps écoulé entre la détection d'une défaillance et la remise en état de fonctionnement du logiciel. Plus le MTTR est élevé, plus les risques de pertes commerciales sont importants.

Copyright - Tout droit réservé - OFPPT

Avantages du déploiement continu

Une mise sur le marché plus rapide

L'un des principaux avantages du déploiement continu est qu'il permet aux nouvelles fonctionnalités et aux corrections d'atteindre rapidement le marché et vos clients. Dans un environnement de plus en plus concurrentiel, le délai de mise sur le marché est une mesure cruciale de la réussite. Dans le cas d'un déploiement manuel traditionnel, il y a un retard considérable dans le test du code, les approbations et enfin la mise à disposition du logiciel pour les utilisateurs.

Amélioration de la satisfaction des clients

Grâce au déploiement continu, les éditeurs de logiciels peuvent répondre rapidement aux commentaires des clients. Il peut s'agir de rapports de bogues ou de demandes de nouvelles fonctionnalités. Quoi qu'il en soit, dès que l'entreprise développe une nouvelle fonctionnalité ou corrige un bogue (généralement à l'aide de l'intégration continue), le processus de déploiement continu lui permet d'atteindre rapidement les clients et donc d'améliorer leur satisfaction.

Pas de grands échecs

Dans le cadre du déploiement continu, les développeurs ajoutent du nouveau code de manière incrémentielle. Cela se fait en continu, par petits morceaux. Avant de valider les traditionnels, le développeur les teste et documente les résultats. De plus, des systèmes surveillent en permanence ces nouvelles modifications. Les modifications sont immédiatement annulées lorsqu'un problème est signalé. Dans le processus traditionnel de déploiement, où une fonctionnalité importante est publiée sous la forme d'une modification importante du code, il est difficile de localiser la source d'un problème. Mais avec le déploiement continu, les problèmes des entreprises sont rapidement traités et les gros échecs sont moins fréquents.

Copyright - Tout droit réservé - OFPPT

Avantages du déploiement continu

Augmente l'efficacité de la main-d'œuvre

Le déploiement continu automatise la plupart des tâches fastidieuses du développement logiciel. Le développeur n'a pas à se soucier de la manière dont le code est intégré, déployé ou testé. Les ingénieurs peuvent simplement se concentrer sur l'amélioration de la qualité de leur travail. Cela permet également de réduire le temps nécessaire à l'introduction de nouvelles fonctionnalités sur le marché. Les développeurs peuvent désormais terminer rapidement une tranche de code et la déployer, sans avoir à attendre des changements importants.

Copyright - Tout droit réservé - OFPPT

Défis de la mise en œuvre du déploiement continu

Cadre solide d'intégration continue

Pour que le déploiement continu fonctionne, il doit y avoir un cadre d'intégration continue solide à toute épreuve. Cela inclut le processus et les flux de travail pour l'enregistrement continu du code, la construction automatisée et les tests (manuels ou automatisés). Ce processus doit être fluide et sans faille. La mise en place d'un tel cadre est un défi pour de nombreuses entreprises. Une intégration continue réussie nécessite le soutien des développeurs, des testeurs et des ingénieurs de builds.

Défis humains et organisationnels

Les propositions de déploiement continu peuvent se heurter à des frictions de la part des employés et même des clients. Le déploiement continu nécessite de nombreux changements dans le processus de développement et de test. Il faut un certain temps pour que les employés prennent confiance dans le pipeline de déploiement continu. Il en va de même pour les clients. Les clients peuvent insister sur un nombre réduit de versions bien testées, craignant que le déploiement continu ne perturbe certaines fonctionnalités. De même, d'une équipe à l'autre, la maturité de la mise en œuvre peut varier. Certaines équipes peuvent suivre religieusement les paradigmes de déploiement continu, d'autres non.

Disponibilité et coût des outils et des ressources

Le déploiement continu nécessite un grand nombre d'outils et de logiciels pour fonctionner correctement. L'achat et l'installation de ces outils peuvent s'avérer coûteux. De nombreux outils sont disponibles sur le marché pour le déploiement continu. C'est un défi de déterminer ce qui fonctionne et ce qui ne fonctionne pas. Certains outils peuvent ne pas être compatibles avec les systèmes existants d'une organisation. De plus, la mise en œuvre du déploiement continu nécessite beaucoup de ressources, telles que des serveurs et de la puissance de calcul. Acquérir ces ressources et les partager entre les équipes peut constituer un autre défi.

Copyright - Tout droit réservé - OFPPT

Déploiement continu vs développement continu

Dans le déploiement continu, chaque étape, de l'enregistrement du code au déploiement dans l'environnement de production, est automatisée.

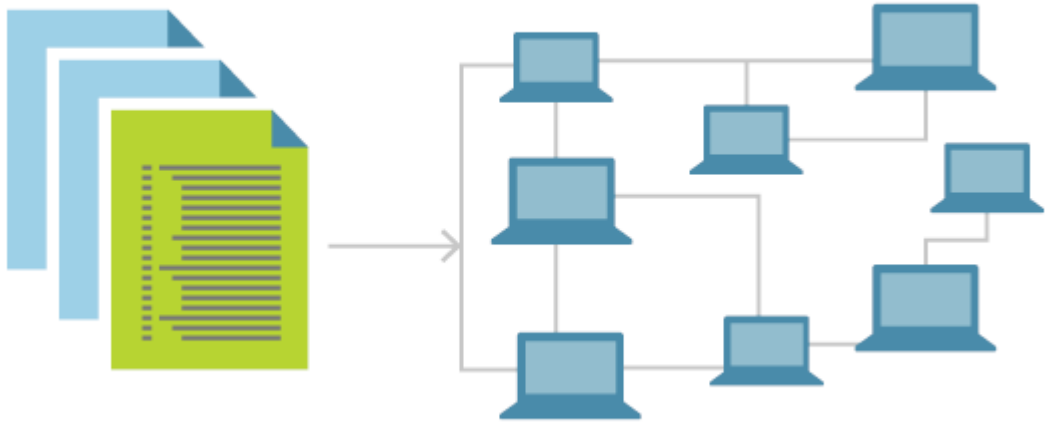
Dans le développement continu, la dernière étape, à savoir le déploiement vers l'environnement de production, est manuelle. Toutes les étapes jusqu'à l'approbation finale à la production sont automatisées. Mais pour que le nouveau code soit intégré à l'environnement de production, une authentification manuelle/un laissez-passer est nécessaire. En résumé, le déploiement continu est une étape avancée en termes d'automatisation.

Copyright - Tout droit réservé - OFPPT

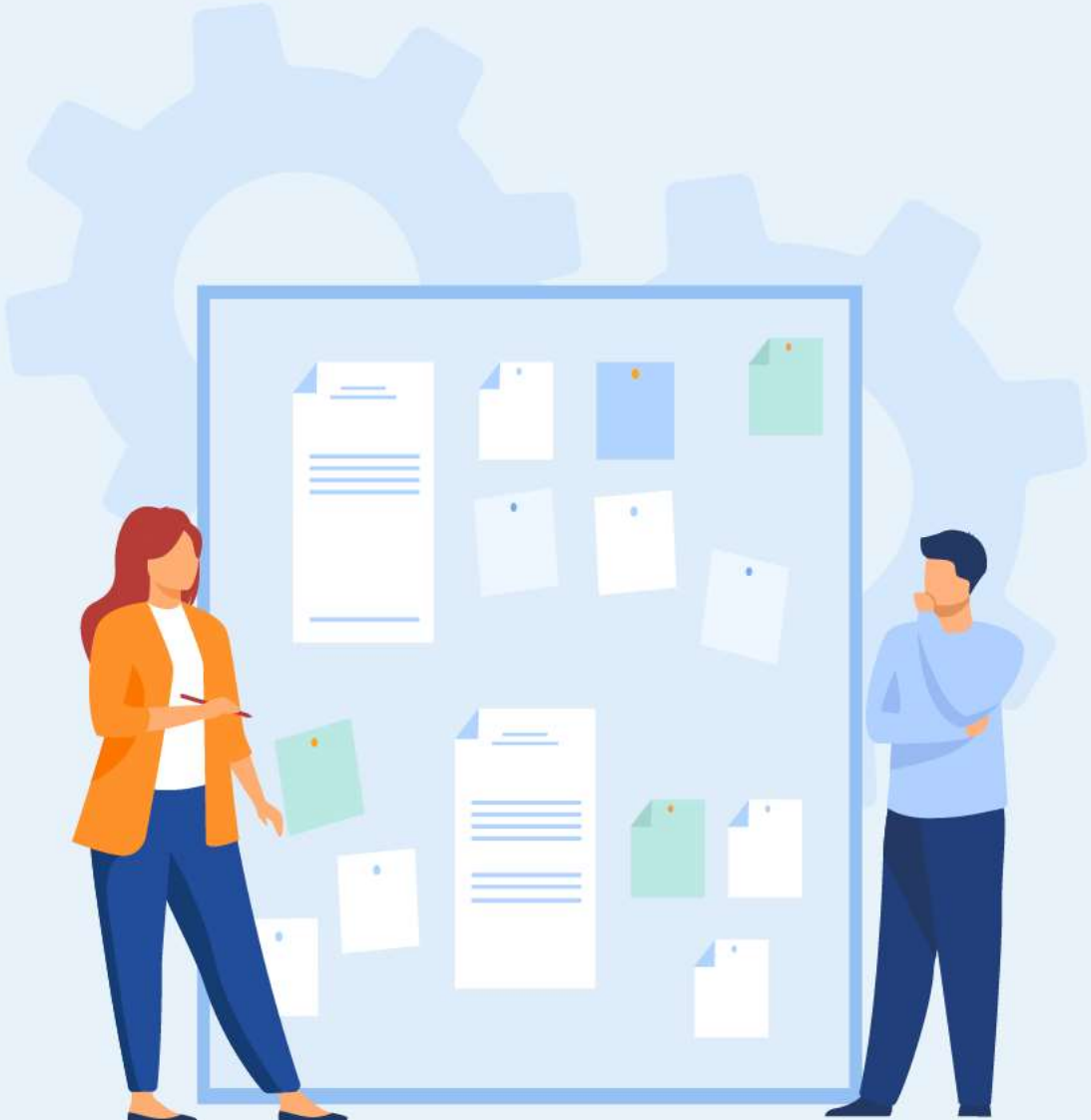
l'infrastructure en tant que code (IaC)

L'infrastructure en tant que code (IaC) utilise la méthodologie DevOps et le contrôle de version avec un modèle descriptif pour définir et déployer des infrastructures, telles que des réseaux, des machines virtuelles, des équilibreurs de charge et des topologies de connexion. Tout comme le même code source génère toujours le même binaire, un modèle IaC génère le même environnement à chaque déploiement.

IaC est une pratique DevOps clé et un composant de la livraison continue. Avec IaC, les équipes DevOps peuvent collaborer avec un ensemble unifié de pratiques et d'outils pour fournir des applications et leur infrastructure de prise en charge rapidement et de manière fiable à grande échelle.



Copyright - Tout droit réservé - OFPPT



CHAPITRE 2

Adopter une approche DevOps

1. Méthodes d’agiles
2. Intégration continue (CI)
3. Déploiement continue (CD)
4. **DevOps vs DevSecOps**

Différences entre DevOps et DevSecOps

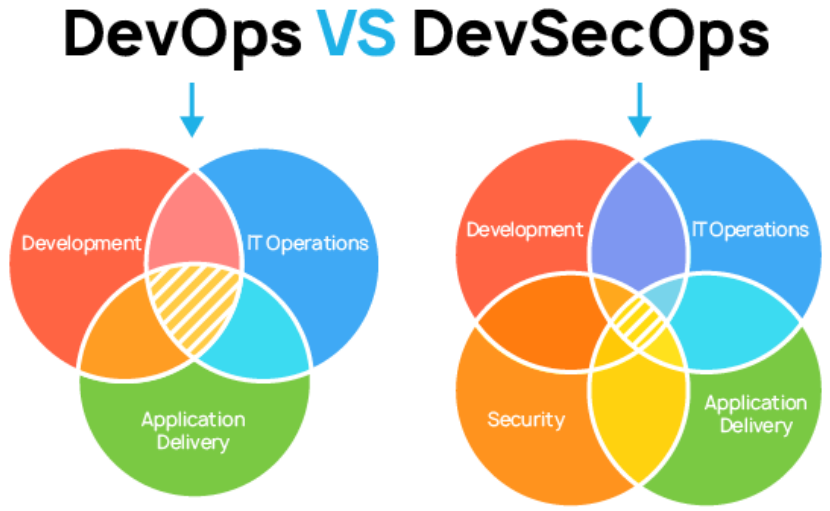
DevOps et DevSecOps se distinguent principalement à travers leur objectif.

Pour les DevOps, le but premier est de fournir un produit de qualité rapidement. L'accent est mis sur la rapidité de livraison et l'efficacité du logiciel. In fine, sur la satisfaction globale de l'utilisateur final. À cette fin, les équipes développement et exploitation partagent des objectifs, des outils et des indicateurs de performance communs.

Mais en focalisant leur attention sur ces aspects, les DevOps ont parfois tendance à négliger la sécurité. Ce qui peut mettre en danger les actifs, les données des utilisateurs finaux et les applications de l'organisation.

C'est pourquoi le DevSecOps intervient. Il s'agit d'une évolution du premier, puisqu'ici, l'accent est mis sur la sécurité. Désormais, les considérations cyber sont pleinement intégrées dans le pipeline. Et non pas à la finalisation du développement logiciel, mais dès le début. Sécurité, développement et exploitation sont alors liés tout au long du projet.

L'utilisateur final reçoit ainsi un logiciel conforme, efficace, livré rapidement et sécurisé. Sa satisfaction est maximale.



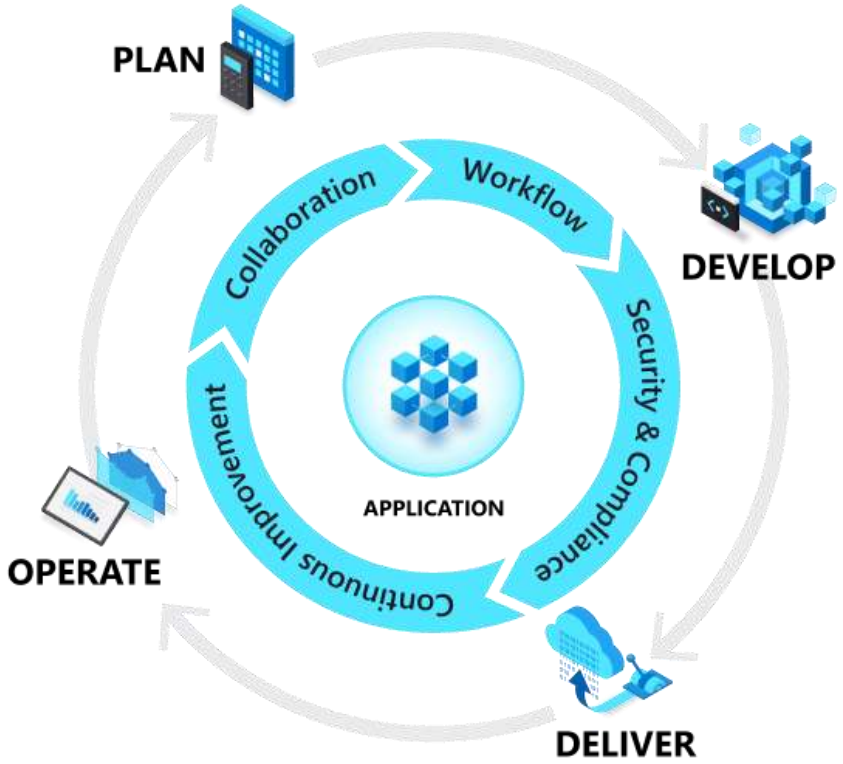
PARTIE 3

Copyright - Tout droit réservé - OFPPT

DevOps et le cycle de vie de l'application

DevOps influence le cycle de vie de l'application tout au long de ses phases de planification, de développement, de livraison et d'exploitation. Chaque phase s'appuie sur les autres phases, et les phases ne sont pas spécifiques au rôle. Une culture DevOps implique tous les rôles de chaque phase dans une certaine mesure.

Le diagramme suivant illustre les phases du mode de vie de l'application DevOps :



Copyright - Tout droit réservé - OFPPT

Objectifs et avantages DevOps

Lorsqu'une équipe adopte la culture, les pratiques et les outils DevOps, elle peut réaliser des choses étonnantes :

- Accélérer le délai de commercialisation



Grâce à des efficacités accrues, à une collaboration d'équipe améliorée, à des outils d'automatisation et à un déploiement continu, les équipes sont en mesure de réduire rapidement le délai entre le lancement du produit et le lancement sur le marché.

- S'adapter au marché et à la concurrence



Une culture DevOps exige que les équipes se concentrent sur le client. En combinant agilité, collaboration d'équipe et concentration sur l'expérience client, les équipes peuvent continuellement fournir de la valeur à leurs clients et accroître leur compétitivité sur la place de marché.

- Maintenir la stabilité et la fiabilité du système



En adoptant des pratiques d'amélioration continue, les équipes sont en mesure d'améliorer la stabilité et la fiabilité des produits et services qu'elles déploient. Ces pratiques permettent de réduire les défaillances et les risques.

- Améliorer le temps moyen de récupération



La métrique de récupération moyenne indique le temps nécessaire à la récupération d'une défaillance ou d'une violation. Pour gérer les défaillances logicielles, les violations de sécurité et les plans d'amélioration continue, les équipes doivent mesurer et travailler à l'amélioration de cette métrique.

Copyright - Tout droit réservé - OFPPT

Présentation de Azure DevOps

Azure DevOps est une plateforme cloud complète de développement logiciel qui propose un large éventail d'outils pour la CI/CD (Intégration continue / Livraison continue). Voici une liste des principaux outils de CI/CD proposés par Azure DevOps :

- Azure Pipelines : un service de CI/CD entièrement géré et hautement évolutif qui permet aux équipes de créer, tester et déployer des applications en utilisant une variété de langages et de plates-formes.
- Azure Artifacts : un référentiel de package qui permet aux équipes de stocker, gérer et partager des packages de code et de dépendances pour leurs projets.
- Azure Test Plans : un service de test complet qui permet aux équipes de planifier, exécuter et suivre des tests manuels et automatisés pour leurs applications.
- Azure Boards : un service de gestion de projet agile qui permet aux équipes de planifier, suivre et gérer les travaux et les problèmes de leurs projets.
- Azure Repos : un service de contrôle de version qui permet aux équipes de stocker, gérer et partager le code source de leurs projets.

En utilisant ces outils, les équipes peuvent mettre en place des pipelines de CI/CD complets pour leurs projets, de la création et de la compilation du code à la livraison continue de nouvelles versions d'application en production.



Copyright - Tout droit réservé - OFPPT