

Plan de Reprise d'Activité Cloud managé

**pour les ETI, PME et
organismes publics**

Livre Blanc

Introduction

Les entreprises sont toujours plus dépendantes de l'informatique et du numérique. Une indisponibilité durable de leur Système d'Information (SI) peut engendrer des pertes financières, un manque à gagner ou encore une perte de réputation très importante, voire mettre leur existence en danger.

Il s'avère donc souvent indispensable de mettre en place un Plan de Reprise d'Activité (**PRA**). Il s'agit d'un ensemble de mesures qui vise à assurer, en cas d'incident majeur ou de sinistre, le maintien des prestations de services essentiels de l'entreprise, puis la reprise planifiée des activités.

Pour beaucoup d'entreprises, la mise en place d'un PRA était considérée comme hors d'atteinte. Il s'agissait, d'un projet coûteux et compliqué à réaliser, surtout à tester régulièrement et à maintenir dans le temps.

Les possibilités offertes par le Cloud vont conduire beaucoup de ces entreprises à modifier leur vision du Plan de Reprise d'Activité.

De nouvelles menaces

Le domaine de la reprise d'activité a beaucoup évolué en termes de besoins depuis quelques années. Avant, on disposait d'un plan de secours pour se prémunir des catastrophes majeures ou d'incident critiques avec **très faible probabilité** et impacts importants.

On est de plus en plus dans une notion de Reprise d'Activité où on intègre les menaces liées à des malwares, des cyber-attaques avec une augmentation importante de la probabilité de survenance et des besoins de redémarrage courts.

Dans le domaine de la cybersécurité, on évoque souvent le terme de « cyber-résilience » qui est la capacité d'une entreprise à se préparer et répondre à des cybermenaces.

Malgré les mécanismes de protection, d'anticipation et de détection mis en œuvre dans les entreprises, il peut être nécessaire d'activer des mécanismes de reprise d'activité. C'est à cette étape là que l'on trouve les solutions de Plan de Reprise d'Activité

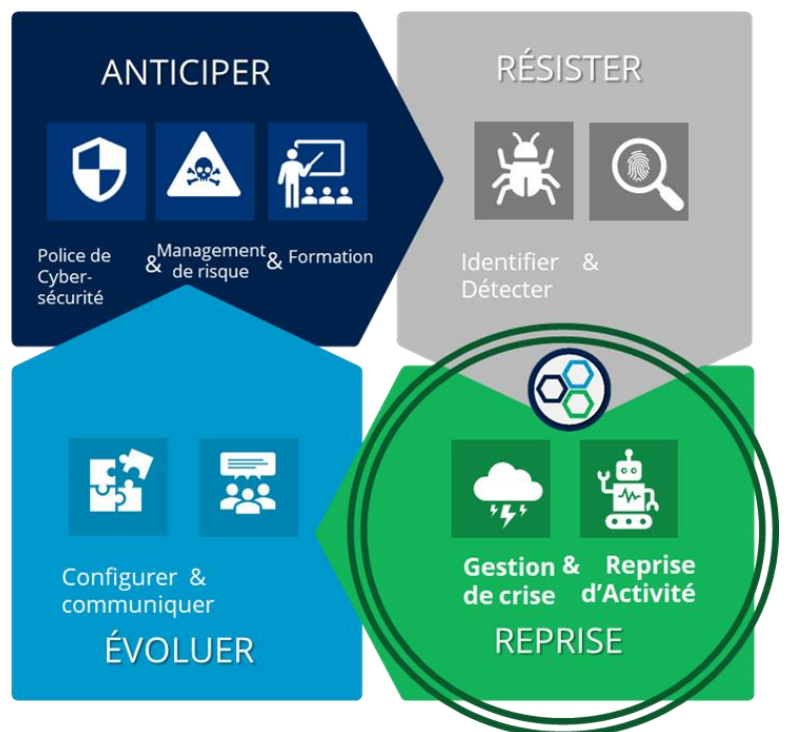




Table des matières

Introduction.....	2
De nouvelles menaces	2
Comprendre la Reprise d'Activité.....	4
Reprise d'Activité ou Continuité Informatique ?.....	4
Un besoin de rupture technologique pour les sauvegardes	5
Complexité, coût et rigidité : les 3 handicaps des solutions traditionnelles de PRA.....	6
Qu'apporte le Cloud dans la reprise d'activité ?	7
Les principes du PRA dans le Cloud	7
Comment fonctionne un Plan de Reprise d'Activité dans le Cloud ?	8
Mode de fonctionnement nominal (hors mode secours)	8
Mode secours	8
Le retour au mode Nominal	9
Le modèle des coûts du PRA dans le Cloud	9
Les délais de redémarrage du PRA dans le Cloud.....	10
Synthèse du rapport coût / confiance	10
Les bénéfices du PRA dans le Cloud	11
Les 5 principaux avantages du PRA dans le Cloud	11
Les différents modes de PRA Cloud.....	12
Le modèle « <i>as a Service</i> » est-il une bonne solution pour le PRA ?	12
Les risques, les freins et les limites au PRA Cloud	13
Les risques	13
Les limites	13
Les points de vigilance.....	13
La solution Nuabee de Plan de Reprise d'Activité <i>as a Service</i>	14
La solution de Nuabee.....	14
Un service de PRA Cloud managé (PRA <i>as a Service</i>)	14
Le périmètre couvert par la solution de PRA Cloud de Nuabee.....	15
Des mécanismes de sécurité renforcés	15
Une architecture multi-locataire (<i>multi-tenant</i>)	15
Un tarif adapté aux ETI et PME.....	16
Conclusion	16

Comprendre la Reprise d'Activité

Le **Plan de Reprise d'Activité (PRA)** est le processus et les moyens techniques mis en œuvre pour garantir la reprise de l'activité informatique d'une entreprise lors d'un sinistre ou d'un incident majeur (par exemple une indisponibilité de la salle informatique ou une attaque de ransomware) grâce à la remise en route du système d'information dans des délais acceptables par les métiers.

Les données sont répliquées régulièrement de manière sécurisée vers un autre site, interne ou externe à l'entreprise, de manière à préserver le Système d'Information.

Grâce à la mise en œuvre d'un PRA, les utilisateurs peuvent accéder à nouveau aux applications et ressources hébergées dans le site de secours.

Traditionnellement, les entreprises ont recours à un deuxième site physique, soit interne avec une deuxième salle informatique, soit externe chez un hébergeur.

Ce site de secours peut être classé en fonction du niveau de secours qu'il offre :

Le site froid 	Le site chaud 	Le site très chaud 
C'est une salle informatique distante, disponible en cas de déclenchement du PRA, qui ne dispose d'aucun matériel informatique (ou de très peu) installé à l'avance. Il faut alors approvisionner de nouveaux matériels en cas de sinistre. Il faut compter plusieurs jours au minimum pour reconstruire le système d'information de l'entreprise.	C'est une salle informatique distante qui est déjà équipée de matériel informatique de secours. Cela permet la reprise des applications les plus importantes. Les délais de reprise (RTO) varient de quelques heures, sur le périmètre secouru, à plusieurs jours pour les applications qui sont hors du plan de reprise.	C'est une salle informatique distante qui est redondante par rapport à la salle à secourir. L'équipement informatique est dupliqué. Tous les équipements nécessaires à la reprise du SI, sont présents et prêts à fonctionner. Les délais de reprise varient alors de quelques minutes à quelques heures suivant les technologies utilisées.
 €	 € - €€	 €€ - €€€€

Reprise d'Activité ou Continuité Informatique ?

Le **Plan de Reprise d'Activité** est à distinguer du **Plan de continuité d'activité informatique (PCA)** dont l'objectif est de permettre la poursuite de l'activité de l'infrastructure informatique sans aucune interruption de la disponibilité des applications et des données, quels que soient les incidents ou sinistres rencontrés.

La mise en place d'un PCA informatique requiert des investissements coûteux (comme une salle miroir) et des moyens humains importants pour le maintenir en fonctionnement. Ces coûts rarement supportables pour une PME ou une ETI.

La salle Miroir

Assez similaire à un site très chaud mais avec des mécanismes de réplication des données en mode continu ou quasi continu.

La complexité des solutions nécessaires n'est pas adaptée aux PME et ETI.

Ce type de solution ne traite, en général, pas les scénarios de cybermenaces (ransomware, ...), elle est plus considérée comme une solution de haute disponibilité que de continuité d'activité.

Un besoin de rupture technologique pour les sauvegardes

La règle d'or actuelle de la sauvegarde préconise 3 copies des données sur 2 supports de technologie différents dont une copie hors site.

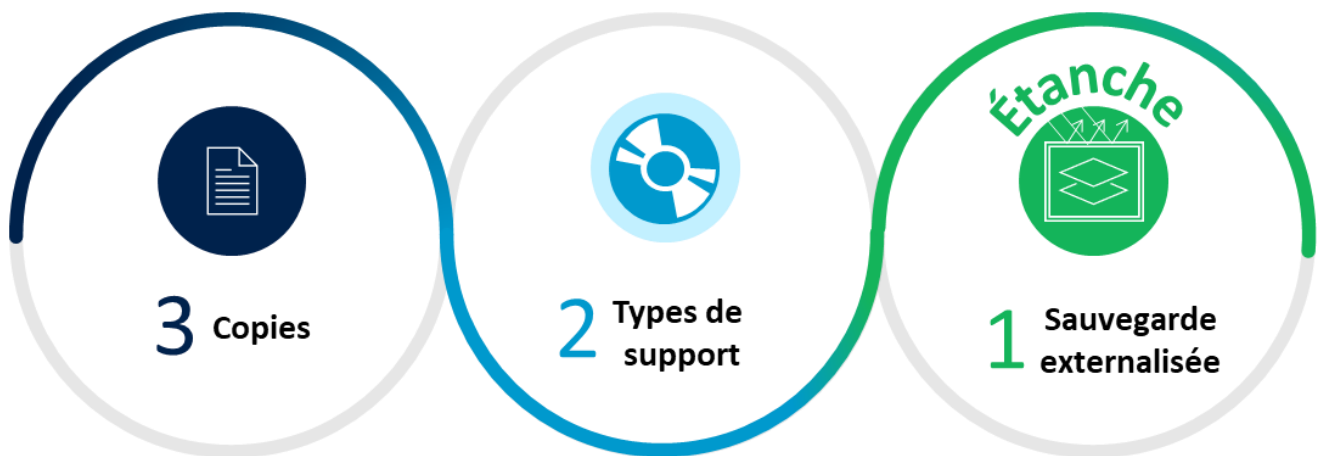
Cette règle n'est plus suffisante pour répondre aux nouvelles cybermenaces. Dans de nombreux cas, des attaques ont permis à des hackers de chiffrer les données et les sauvegardes locales, rendant indisponibles les sauvegardes externalisées, par exemple :

- en rendant indisponible le catalogue des sauvegardes,
- en supprimant ou en chiffrant les données externalisées.

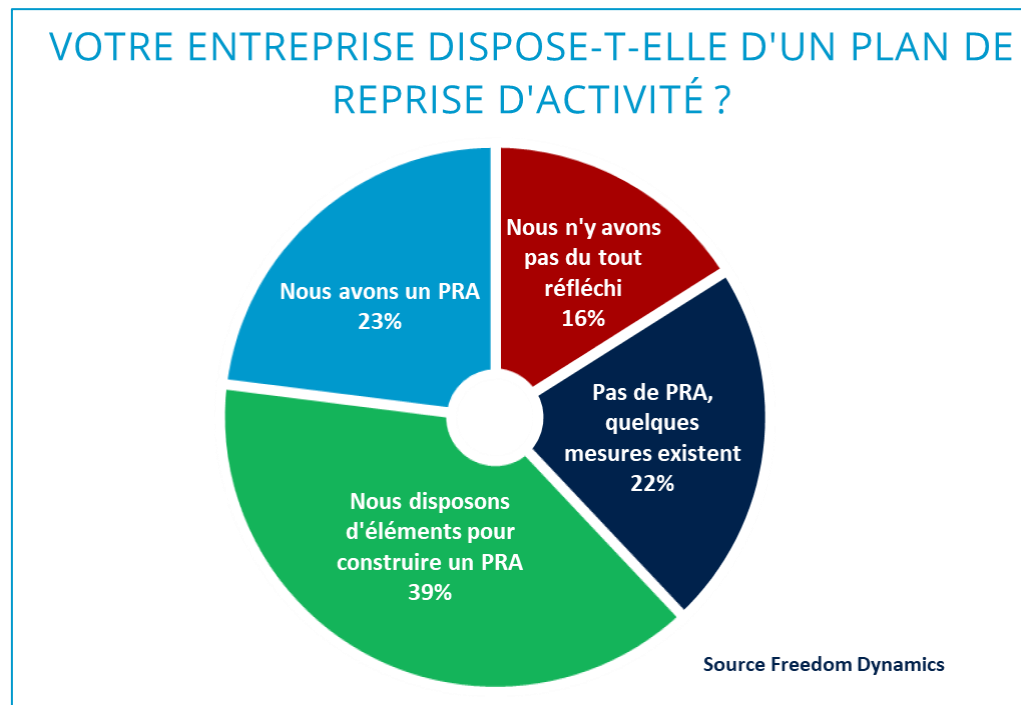
Il faut donc impérativement garantir une étanchéité des sauvegardes externalisées, en d'autres mots garantir qu'un attaquant ayant pris le contrôle de votre Système d'Information ne puisse pas avoir accès à vos sauvegardes externalisées.

Plusieurs solutions technologiques sont disponibles mais il est indispensable de le prendre en compte.

Règle des 3-2-1



Complexité, coût et rigidité : les 3 handicaps des solutions traditionnelles de PRA



Moins de 50% des PME européennes disposent actuellement d'un Plan de Reprise d'Activité.

Alors pourquoi les entreprises ne construisent-elles pas leur PRA ?

1/La démarche est perçue comme étant complexe :

- quel périmètre de l'entreprise adresser ?
- quels sont les besoins des métiers ?
- quels sont les délais de redémarrage acceptables ?

2/La solution technique est elle aussi perçue comme étant complexe :

- Une solution interne nécessite le doublement de la salle informatique et des technologies de réplication qui ont de forts impacts sur l'architecture technique
- Qui plus est, une solution externe pose, en plus, les questions des engagements, de sécurité, de l'évolutivité de l'infrastructure et des tests.

3/Quand bien même la solution de Plan de Reprise d'Activité traditionnelle est mise en œuvre, il faut gérer :

- la mobilisation des compétences internes pour faire fonctionner le PRA et le tester régulièrement,
- la complexité et le coût de la maintenance au même niveau des deux infrastructures (matériel, espace disque, licences logicielles...).
- la difficulté de faire évoluer les solutions de secours en fonction des besoins des métiers et de ceux de l'infrastructure (ajout et retrait d'applications, de serveurs, de réseaux...),
- l'incapacité, pour des raisons de complexité, de coût et de risques à organiser des tests réguliers de secours (à peine 50% des entreprises testent leur PRA au moins annuellement).

Tous ces motifs induisent une faible confiance dans la solution de secours.

Pour les entreprises qui ne testent pas régulièrement leur PRA, un faux sentiment de sécurité s'instaure. Il entraîne les équipes dans des choix de mise en œuvre de reprise d'activité dangereux : plans de reprise corrompus et incohérents, dépendances incorrectes entre serveurs, impossibilité de basculer en secours... La situation est pire que s'il n'avait pas de PRA.

Les solutions traditionnelles de PRA sont donc souvent hors de portée des PME, essentiellement pour des raisons financières et de complexité. Quand ces entreprises arrivent à surmonter ces obstacles, il leur faut encore adapter leur PRA aux nombreuses évolutions de leur Système d'Information et les tester...

Qu'apporte le Cloud dans la reprise d'activité ?

Le Cloud est un nouveau modèle d'accès à la puissance informatique qui offre self-service, paiement à l'usage et élasticité garantie.

Les caractéristiques du Cloud sont :

- l'**ouverture**, en offrant notamment des services standardisés tels que l'accès depuis le réseau Internet ou d'un réseau MPLS/SD-WAN, le stockage de masse et la **puissance de machines virtuelles**,
- le **libre-service** et la **flexibilité**, avec la faculté de consommer les services dont il est besoin au moment et pendant la durée dont il est nécessaire,
- le **paiement à l'usage**, afin de moduler le coût d'exploitation en fonction des besoins réels des ressources informatiques,
- la mutualisation des moyens, pour réaliser des **économies d'échelle** qui se répercutent sur le prix de vente des services offerts.

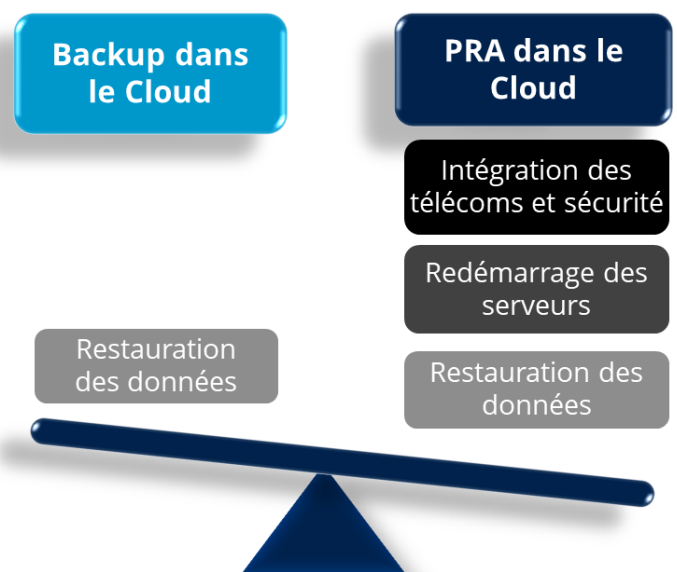
Les principes du PRA dans le Cloud

Tout d'abord, il est important de faire la différence entre sauvegarde externalisée dans le Cloud et PRA dans le Cloud.

La sauvegarde consiste uniquement dans la copie des données du Système d'Information dans un Cloud.

Alors que la notion de PRA dans le Cloud englobe, en plus de la sauvegarde des données, les fonctions de reprise des serveurs, de télécommunications et de sécurité, afin de reconnecter les utilisateurs aux applications qui redémarrent dans le Cloud.

Un Backup externalisé ne permet aucunement de garantir un redémarrage des activités dans des délais acceptables pour les métiers, ce qui est l'objet d'un PRA.



Comment fonctionne un Plan de Reprise d'Activité dans le Cloud ?

Dans l'exemple décrit par le schéma suivant, nous voulons assurer un PRA pour 3 applications :

- un contrôleur de domaine AD,
- un logiciel ERP,
- un service de fichiers bureautiques.

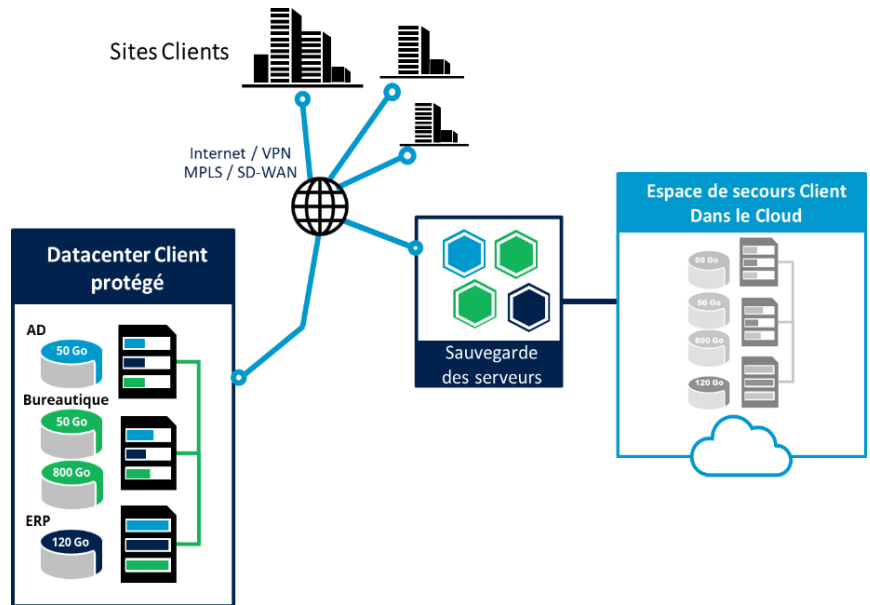
Le fonctionnement nominal est le fonctionnement de la solution au jour le jour, en mode normal.

Mode de fonctionnement nominal (hors mode secours)

L'environnement de Reprise d'Activité fonctionne dans le mode nominal pendant la très grande majorité du temps.

La base de données de l'ERP et les fichiers de bureautique sont répliqués depuis la salle informatique principale de l'entreprise vers le stockage Cloud. Les 3 serveurs sont aussi répliqués sous forme virtuelle.

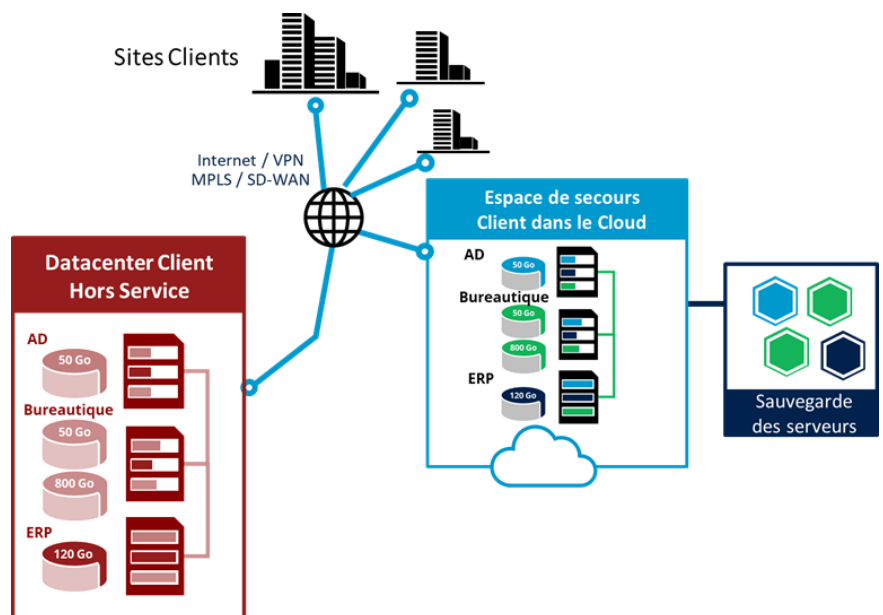
La duplication est incrémentale. Après une première copie complète, seules les modifications sont transférées vers le Cloud, en mode bloc.



Mode secours

En cas de sinistre, d'incident critique ou simplement de test, le site informatique principal est déclaré hors service.

Pour la Reprise d'Activité, tout se passe maintenant dans le Cloud. Les données, d'applications et de systèmes, qui avaient été répliquées dans le Cloud pendant la phase de sauvegarde, y sont restaurées sous forme de disques virtuels. Ils sont attachés aux serveurs virtuels (VM) qui sont maintenant réveillés dans le Cloud.



Les réseaux qui ont été configurés au préalable (pendant la création du PRA), sont activés pour permettre la reconnexion des utilisateurs.

Le retour au mode Nominal

L'entreprise a lancé un PRA en réel. Elle a donc fonctionné en mode dégradé pendant un certain temps. Les données ont continué à être sauvegardées dans le Cloud durant le temps d'indisponibilité de son SI.

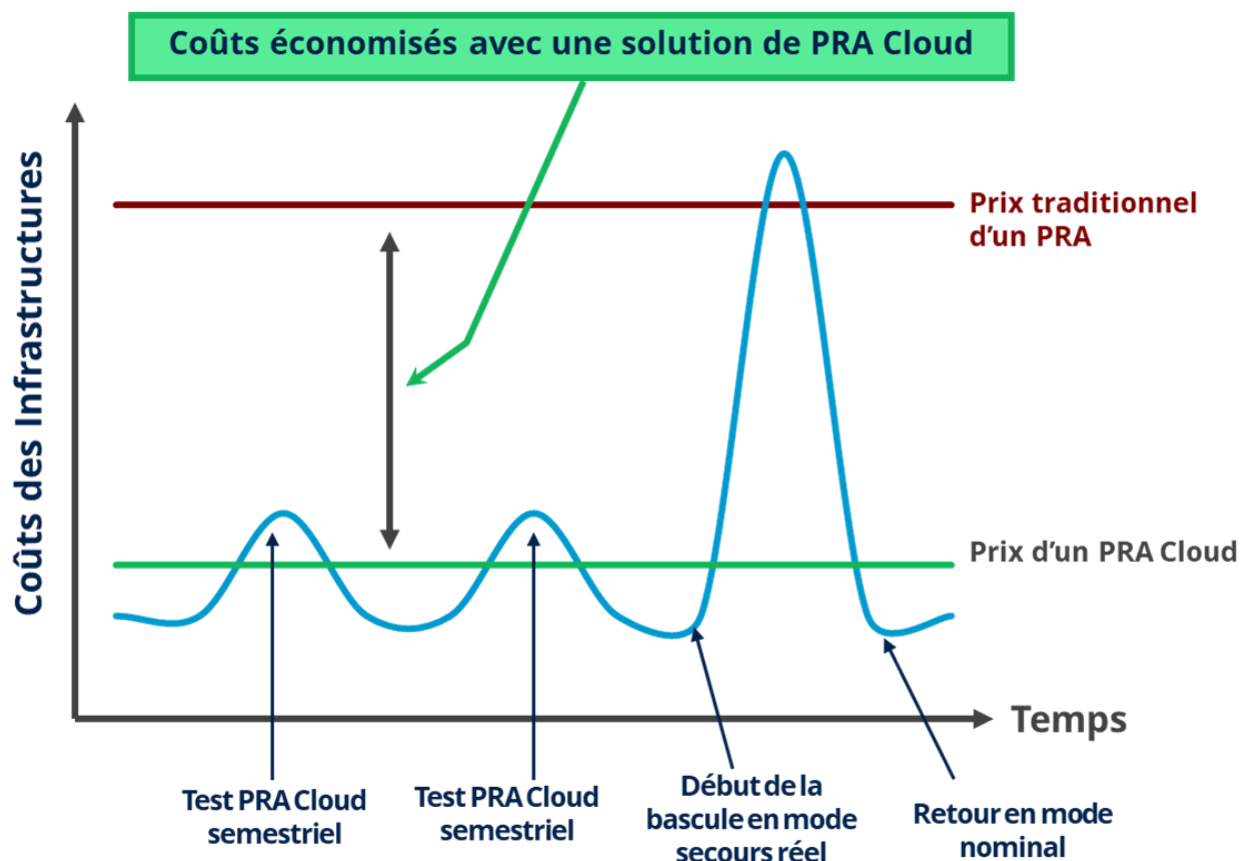
Dès que le SI principal redevient fonctionnel, l'entreprise souhaite reprendre les activités normales sur son site principal, qu'il soit *on-premise* ou dans le Cloud. Un retour arrière doit être organisé avec les données présentes dans le Cloud. Ceci peut nécessiter l'usage de dispositifs de transport des données depuis le Cloud vers le site principal.

Le modèle des coûts du PRA dans le Cloud

En mode de fonctionnement nominal, les coûts portent sur le stockage dont le prix du marché a fortement diminué ces dernières années. La facturation est continue, mais faible.

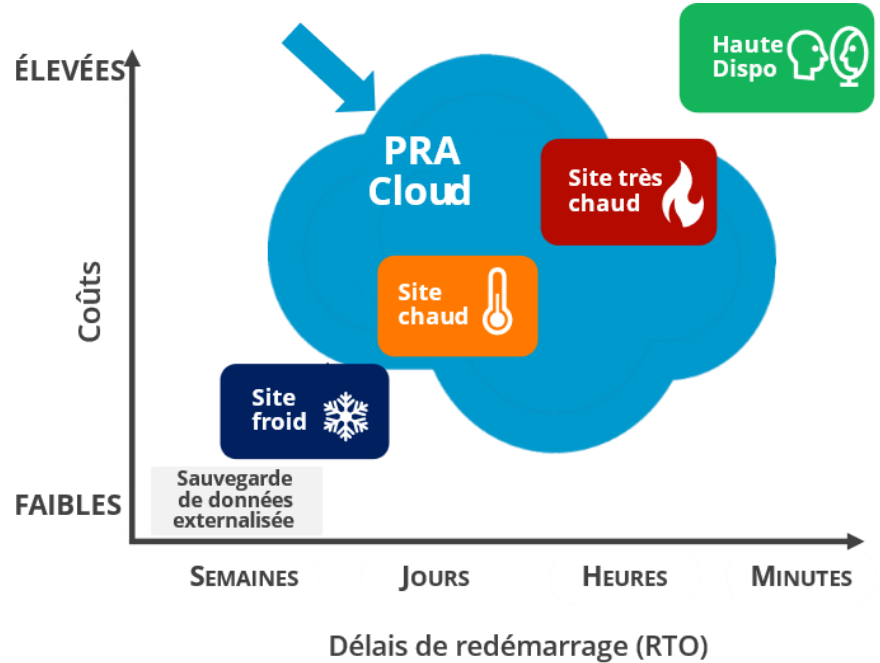
En mode de secours, les coûts portent plus sur la puissance de calcul mise à disposition des machines virtuelles activées. La facturation est provoquée uniquement en cas de besoin (test ou sinistre avéré). C'est tout l'avantage de l'élasticité du Cloud.

Si le PRA est activé par suite d'un sinistre, il faut noter que la prise en charge du coût d'utilisation du Cloud peut être couverte par un contrat d'assurance.



Les délais de redémarrage du PRA dans le Cloud

Le PRA dans le Cloud permet d'obtenir un délai de reprise (en anglais *Recovery Time Objective*, RTO) de quelques heures, notamment en fonction de l'investissement qui est consenti en matière d'automatisation.



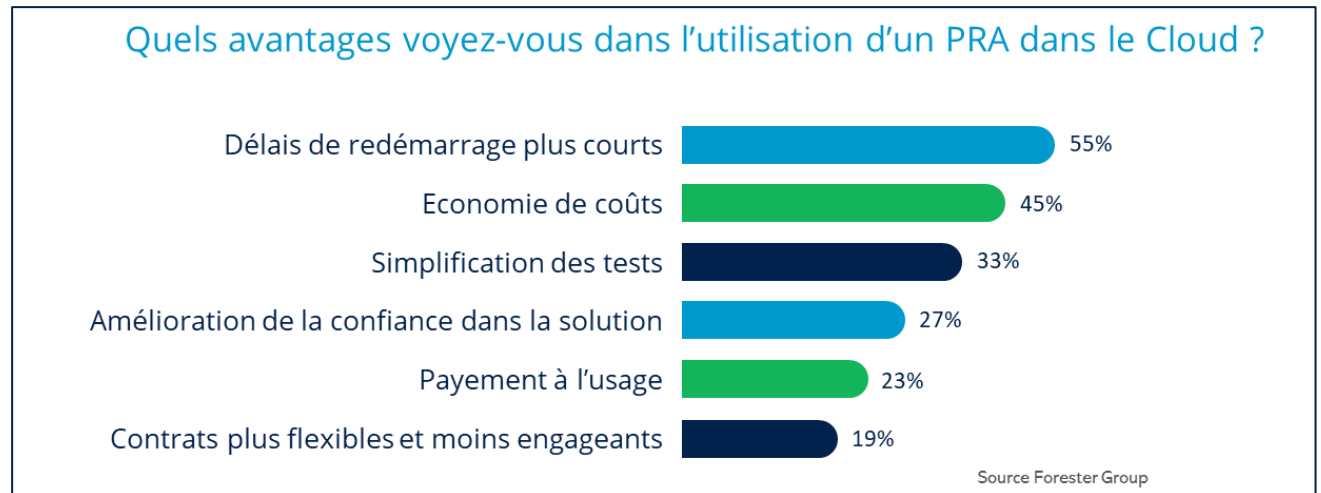
Synthèse du rapport coût / confiance

Comparaison des services traditionnels et du PRA dans le Cloud, eu égard aux critères financier et de niveau de confiance :

PRA Traditionnel				PRA Cloud	
Site froid ❄️	Site chaud 🌡️	Site très chaud 🔥	Salle Miroir 👤👤	PRA Cloud ☁️	
Coûts : €	Coûts : €€	Coûts : €€€ à €€€€	Coûts : €€€€	Coûts : € à €€	
Confiance : 1/5	Confiance : 2/5	Confiance : 4/5 ^(*)	Confiance : 4/5 ^(*)	Confiance : 4/5 ^(*)	

(*) Un indice de confiance de 5/5 ne peut être obtenu que par des tests de PRA a minima semestriels, incluant les tests de reconnexion des utilisateurs et des sites distants au site informatique de secours.

Les bénéfices du PRA dans le Cloud



Les 5 principaux avantages du PRA dans le Cloud

1	Le premier avantage concerne les délais de redémarrage . Ils sont plus courts qu'avec des PRA traditionnels et cela grâce à l'élasticité du Cloud. Il devient possible d'atteindre un délai de redémarrage complet de l'infrastructure en quelques heures.
2	Le PRA dans le Cloud présente un bien meilleur rapport qualité-prix par rapport aux solutions classiques, grâce au principe du paiement à l'usage. Les entreprises nord-américaines qui ont opté pour le PRA dans le Cloud (DRaaS) ont atteint une réduction de 30 à 70% de leur budget PRA (source AWS).
3	L'amélioration du contrôle de son PRA et notamment la possibilité de le lancer depuis une console d'administration (de façon automatisée) sans requérir l'intervention du fournisseur de PRA a un effet très positif sur les délais de redémarrage. Il devient alors plus facile de réaliser des tests de la solution, ce qui améliore la confiance que l'on place dans son PRA.
4	L'évolution de périmètre, à la hausse comme à la baisse , est beaucoup plus aisée, puisqu'il ne s'agit plus d'investir dans du matériel mais plus simplement de répliquer des données.
5	Enfin, les fournisseurs offrent des contrats beaucoup plus flexibles , en termes de durée : 3 ans minimum pour des solutions classiques, contre 1 an, en général, pour des solutions de PRA dans le Cloud, avec des clauses de réversibilité peu onéreuses.

Les différents modes de PRA Cloud

Le modèle « *as a Service* » est-il une bonne solution pour le PRA ?

Alors que de plus en plus de prestations informatiques et des sécurité sont fournies en tant que service (*as a Service*), il semblerait logique que la reprise après sinistre devienne un de ces services.

Plusieurs approches existent dans le PRA Cloud. Il est possible de classer en modes :

- Mode **self-service** : le Client achète un service Cloud de PRA et gère seul la mise en œuvre et le Maintien en Conditions Opérationnelles de son PRA.
- Mode **Managé (partiellement ou totalement)** : un tiers gère tout ou partie du cycle du PRA du Client.

	Mode de management de PRA		
	Mode Self-Service	Partiellement Managé	Totalement Managé
Déploiement du service de PRA	Client	Client avec support du prestataire	Prestataire
Monitoring des répliquions des données vers le Cloud	Client	Client ou Prestataire	Prestataire
Relancement de l'infrastructure de secours pour les tests fonctionnels du PRA	Client	Client avec support du prestataire	Prestataire
Correction des erreurs (répliquions des données, ressources indisponibles ...)	Client	Client avec support du prestataire	Prestataire
Adaptation du PRA à l'évolution du périmètre IT du Client (MCO PRA)	Client	Client avec support du prestataire	Prestataire avec des informations venant du Client
Cible en termes de type d'entreprises	Grandes entreprises	ETI ou Organismes avec équipe informatique spécialisée PRA	ETI, PME ou organismes qui n'ont pas de ressource informatique dédiée PRA

Pour les PME et ETI, le mode managé apporte de réels avantages :

- la garantie de tests réguliers (semestriels, voire trimestriels),
- le maintien en conditions opérationnelles (MCO) du PRA pour s'adapter à l'évolution du périmètre du Système d'Information.
- la libération de l'équipe informatique de la gestion quotidienne des sauvegardes et du PRA pour l'affecter à des tâches à valeur ajoutée pour les métiers de l'entreprise.

Les risques, les freins et les limites au PRA Cloud

Les risques

Les risques liés au PRA dans le Cloud sont similaires à ceux du Cloud en général, mais également à celles d'un prestataire traditionnel de PRA :

- **Risques liés à la confidentialité des données** : les données très critiques d'une entreprise, ainsi que celles sensibles vis-à-vis de la législation RGPD, devront être protégées par des solutions de chiffrement.
- **Risques liés au contrat** : clauses de réversibilité, engagements concernant les niveaux de services, durée d'engagement...
- **Risques de performances** : sur les vitesses de réplication, sur les temps de redémarrage, l'accès aux données...



Certains risques sont spécifiques au modèle de PRA dans le Cloud :

- La capacité du Cloud à fournir une architecture de sécurité de même niveau que le système d'information origine : équivalent VLAN, règles de pare-feu adaptées, monitoring des serveurs, filtrage d'URL, logs des infrastructures...
- L'architecture du Cloud qui doit offrir des débits importants en interne entre les disques de stockage de données et son infrastructure de serveurs virtuels (VM).

Les limites

Il existe encore des limites à la mise en œuvre d'un PRA dans le Cloud :

- Certains systèmes d'exploitation propriétaires (OS/400, AIX, MacOS...) ne sont pas supportés dans les principaux Cloud publics.
- Les coûts télécoms, liés à la zone d'implantation de la salle informatique principale sont trop élevés pour permettre la réplication des données en mode asynchrone.
 - Dans ces cas particuliers, il faut alors adopter des offres classiques de PRA (au moins pour les applications impactées par ces limites).

Les points de vigilance

Dans tous les cas (PRA traditionnels et PRA Cloud) les sujets qui doivent être vérifiés et testés :

- le fonctionnement du PRA par des **tests au minimum semestriels**,
- la reconnexion des utilisateurs au site de secours informatique par un moyen de télécommunication adapté (réseau MPLS ou SD-WAN, lien de secours 4G...).

Il est donc important d'analyser ces différents points lors du choix d'un prestataire de PRA Cloud.

La solution Nuabee de Plan de Reprise d'Activité *as a Service*

La solution de Nuabee

Parce que les PME, ETI et collectivités sont souvent mal équipées au niveau de la sauvegarde externalisée et du PRA, il était important d'avoir une solution complète et performante adaptée au niveau des coûts. Nuabee a développé une solution, qui couvre la totalité de l'infrastructure avec 3 classes de protection pour serveurs :

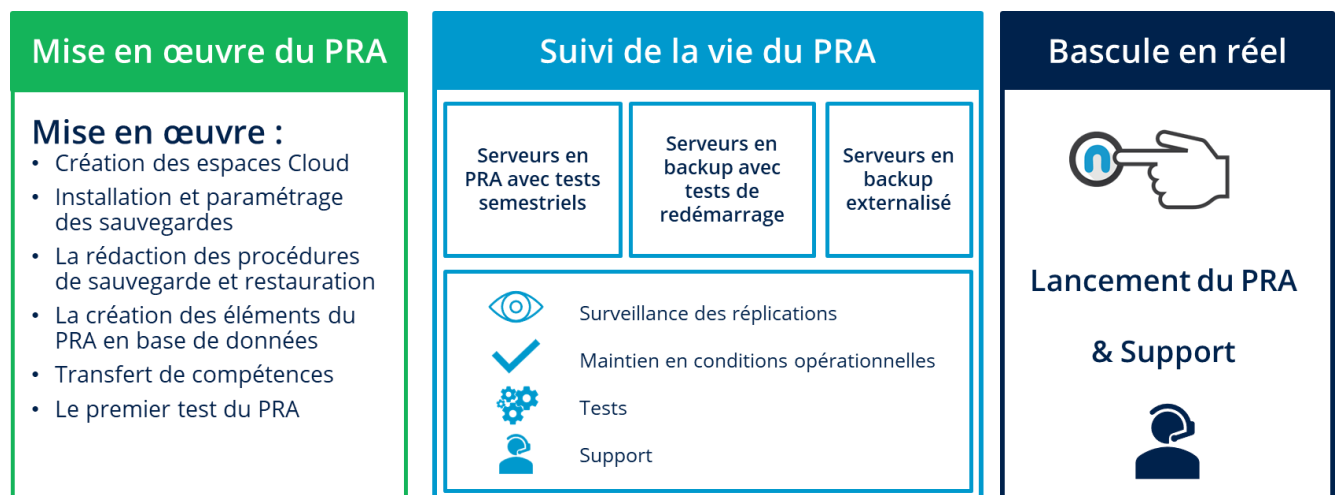
- la classe **sauvegarde externalisée dans le Cloud**,
- la classe **sauvegarde externalisée dans le Cloud avec test de redémarrage**,
- la classe de protection **Plan de Reprise d'Activité Cloud**.

Parce que tous les serveurs n'ont pas la même criticité et n'ont pas tous besoin d'être en protection PRA, il est possible de choisir la bonne classe pour chaque serveur, au bon tarif. Si les besoins évoluent, il est très simple de changer de classe de protection. Cette progressivité des classes de protection est un premier élément de réponse aux problématiques de budgets des PME, ETI et collectivités.

Un service de PRA Cloud managé (PRA *as a Service*)

Nuabee a, dès l'origine, fait le choix d'offrir un service de PRA **totalelement managé** pour permettre aux entreprises qui n'avaient pas de PRA (ou qui avaient un PRA non testé) de pouvoir s'offrir un PRA en lequel elles puissent avoir confiance, sans la nécessité d'une équipe dédiée au PRA en interne.

Nuabee assure le management de la solution à chaque étape du PRA, de la mise en place du PRA, à sa surveillance quotidienne :

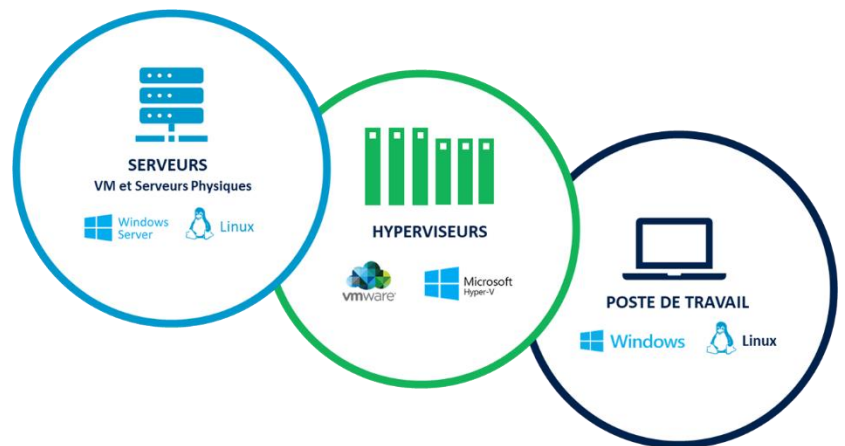


Le périmètre couvert par la solution de PRA Cloud de Nuabee

La solution de PRA Cloud de Nuabee couvre aussi bien des infrastructures traditionnelles (*on premise*) que des infrastructures Cloud publiques ou privées

Les environnements couverts sont :

- les Machines Virtuelles (VM),
- les Serveurs Physiques,
- les VM via hyperviseurs (VMware et Hyper-V),
- les Postes de travail.



Des mécanismes de sécurité renforcés

Toute l'information sauvegardée, qu'il s'agisse des systèmes ou des données, fait l'objet d'un **chiffrement à la source (AES 256)**. L'information circule donc sur les réseaux et est stockée dans le Cloud sans que soit rompu son chiffrement. Chaque client possède sa propre clé qu'il est le seul à détenir.

Toutes les données sont stockées dans des Datacenters Européens, avec des contrats de droit européens non soumis aux lois d'extraterritorialité des données (FISA, Cloud Act, ...).

En plus de la solution de chiffrement de données à la source, qui garantit que seul le client peut avoir accès à ses données, Nuabee s'appuie sur de nombreuses autres solutions ou règles de sécurité :

- isolation des différents environnements Clients par design (espaces de stockage, espaces de secours) grâce au socle *open source* renforcé du Cloud, basé sur OpenStack,
- monitoring des différents composants de la solution : réalisation de la sauvegarde, fonctionnement du Cloud, fonctionnement du VPN...
- politique de sécurité du Cloud supervision par une Security Operating Center (SOC), protection anti-déni de service, détection d'intrusion multi-niveaux...

Une architecture multi-locataire (*multi-tenant*)

L'architecture de la solution Nuabee est structurée en plusieurs espaces qui permettent de fonder les mécanismes de la reprise d'activité.

Le site du client contient l'ensemble de l'infrastructure du système informatique d'origine. Cet espace est divisé en deux parties disjointes :

- le **Datacenter Client protégé par le PRA**, dont l'activité pourra continuer dans le Cloud en cas de sinistre ; il s'agit des serveurs et applications dont la disponibilité est essentielle au fonctionnement des services offerts par le système d'information du Client.
- les **Espaces utilisateurs**, qui sont constitués d'un ou plusieurs bâtiments sur un ou plusieurs sites.

Chaque client dispose d'une espace de sauvegarde et d'un espace de secours dédiés.



Un tarif adapté aux ETI et PME

La solution Nuabee permet d'obtenir des gains financiers importants par rapport aux solutions traditionnelles.

Cela est possible grâce :

- aux **3 classes de protections serveurs** qui permettent de protéger en fonction de leur criticité, la classe PRA étant la plus chère, la classe sauvegarde externalisée étant la moins chère.
- aux **tarifs particulièrement bas de stockage** du Cloud, notamment via l'utilisation du **stockage objet**.
- au recours à **l'activation des VM** dans le Cloud (et donc à l'activation de la puissance de calcul) **uniquement lors des phases de test de PRA**.
- à **notre industrialisation** qui permet de lancer un PRA complet 100% automatisé, sans aucune intervention humaine, grâce à **un launcher de PRA**.
- au service complètement managé qui s'occupe de la gestion complète du PRA permettant aux équipes informatiques internes de se concentrer sur le métier.

Conclusion

La reprise d'activité est un sujet qui préoccupe de plus en plus les PME, ETI et collectivités.

Ainsi, les solutions de PRA évoluent pour bénéficier des possibilités offertes par le Cloud public et offrir des solutions bien plus avantageuses :

- un service de meilleure qualité : délais de redémarrage plus faibles, lancement automatisé du PRA, tests très réguliers, moins d'erreurs humaines grâce à l'industrialisation des processus.
- baisse importante des coûts grâce aux prix de stockage très faibles et à la tarification des VM à l'usage.
- des contrats plus flexibles et moins contraignants sur leur durée.

Les nouvelles solutions de PRA dans le Cloud permettent, grâce à leur modèle économique, à leur capacité à s'adapter aux évolutions de l'entreprise et à la simplification des solutions techniques, d'adresser enfin le marché des petites et moyennes entreprises et des collectivités.

Merci de votre lecture

Vous avez un projet de PRA, nous pouvons vous accompagner pour :

1. Étudier la faisabilité d'utiliser le Cloud dans votre contexte,
2. Identifier les solutions et options compatibles avec vos besoins,
3. Définir l'architecture et valider les points clefs de la solution,
4. Vous présenter notre solution Nuabee

Pour tout contact, merci de nous envoyer un courriel à sales@nuabee.com

ou par téléphone au **+33 (0)4.28.29.79.01**