

Plan de Reprise d'Activités

Doit être testé obligatoirement au minimum 2 à 3 fois par an pour vérifier son fonctionnement et le mettre à jour si besoin.

Sommaire

1.	Condition d'application.....	2
2.	Durée de la reprise d'activité.....	2
3.	Quantités maximales de données perdues	3
4.	Acteurs identifiés et scénario de tests.....	3
A.	Scénario 1.....	3
B.	Scénario 2.....	3
C.	Scénario 3.....	3
D.	Scénario 4.....	4
E.	Scénario 5.....	4
5.	Application des éléments techniques	4

Plan de reprise d'activités du lundi 12 février 2018

1. Condition d'application

- Vous, CarnoFluxe, entreprise proposant un service Web de e-commerce.
- Votre infrastructure comportant :
 - Un serveur HTTP
 - Un serveur DNS et DHCP
 - Un serveur DNS Esclave
- Ce PRA (Plan de reprise d'activité) pourra seulement être mis en place si et seulement si une des conditions ci-dessous est remplie :
 - En cas d'acte de malveillance comme vol, attentats, piratage, corruption des données...
 - En cas de catastrophe naturelle tel qu'un incendie, tremblement de terre, tsunami...
 - En cas de panne matériel.
 - En cas de coupure des ressources tel que l'électricité ou le refroidissement des serveurs.

Alors votre entreprise pourra mettre en place le plan de reprise d'activité.

2. Durée de la reprise d'activité

Le temps de constater le problème et de voir les possible remise en service, il vous faut compter 3h minimum pour que la décision de la mise en place du Plan de reprise d'activité.

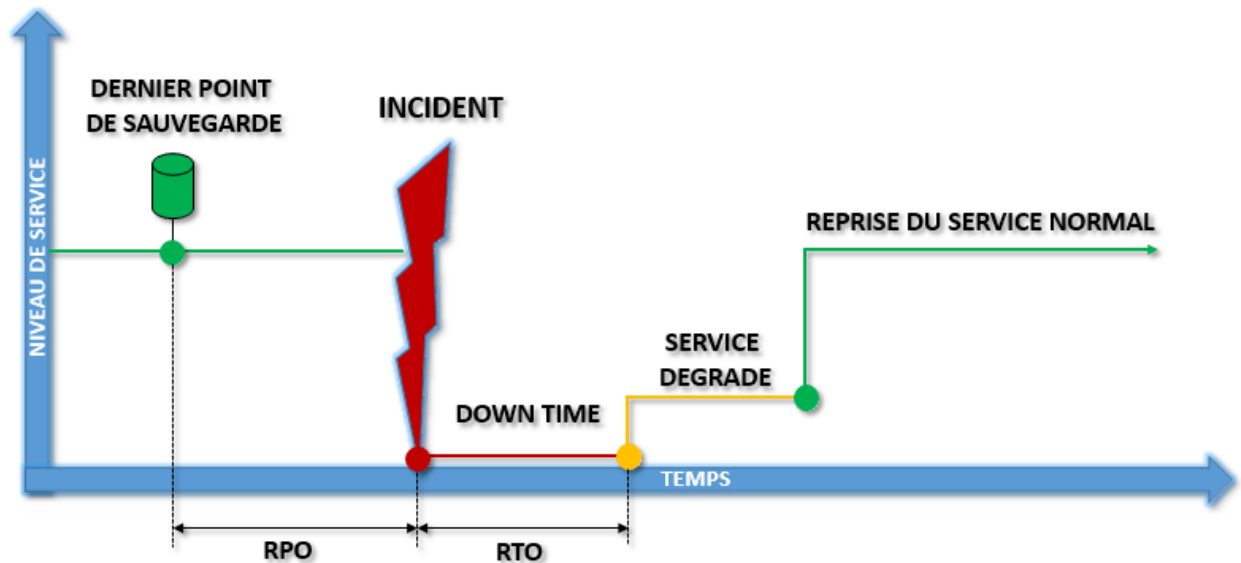
Il faudra compter de plus d'une demi-journée à 3 jours maximum pour la réalisation de celui-ci au-delà de ce délai les statistiques disent qu'environ 60% des entreprises dont faillites.

- En fonction du type d'incident cela peut changer pour une coupure d'électricité cela peut prendre plusieurs jours comme juste quelques minutes.
- S'il y a obligation de changer l'équipement et de le reconfigurer cela peut prendre de 2 à 3 jours.

Durant cette période, deux durées seront les plus importantes le RPO (*Recovery Point Objective*) et RTO (*Recovery Time Objective*).

Le RPO est la durée maximale des données perdues qu'on s'autorise à avoir généralement depuis la dernière sauvegarde.

Le RTO qui est lié au RPO est lui la durée à partir de l'incident jusqu'à la remise partielle des services c'est là que nous recherchons une durée le plus petit possible pour éviter des pertes financières.



3. Quantités maximales de données perdues

S'il y a des pertes de données importantes par exemple un problème survient quelques jours avant la sauvegarde complète du mois on peut avoir perdu 1 mois de données et une semaine de données sur le site sachant qu'il y a une sauvegarde complète mensuelle et une sauvegarde hebdomadaire.

4. Acteurs identifiés et scénario de tests

A. Scénario 1

En cas d'acte de malveillance vos équipes de sécurité vont s'en charger pour remettre en place le site ou alors les équipements réseau.

B. Scénario 2

En cas de catastrophes naturelles, les équipements si endommagés devront être remplacé faire un bilan des dégâts et remplacer en priorité les équipements vitaux au bon fonctionnement de votre service interne et externe.

C. Scénario 3

En cas de pannes de matériels, trouver le problème (appareils mal branchés, etc...) et si impossibilité alors remplacer le matériel.

D. Scénario 4

En cas de coupure de ressource comme l'électricité mettre en route si disponible le générateur de secours puis contacter le fournisseur pour savoir la durée d'interruption. Si impossibilité de mettre en place un générateur de secours alors déplacer l'infrastructure sur un site temporaire.

E. Scénario 5

En cas de test, l'idéal est de faire des tests lors de surcharge et lors de nuits en testant plusieurs scénarios de plus vérifier que les sauvegardes sont fonctionnelles.

5. Application des éléments techniques

Pour appliquer ce Plan de Reprise d'Activités, il va falloir impérativement une stratégie de sauvegarde.

La stratégie de sauvegarde utilisé est de sauvegarder les différents fichiers de configurations du serveur Apache et des sites web, des différents fichiers de configurations du serveur DNS. Puis ensuite en faire un back-up sur un serveur distant pour que si un des disque dur tombe en panne les données des sauvegardes ne soient pas perdues de plus il y'aura une sauvegarde complète mensuelle de tous les services puis une sauvegarde hebdomadaire du site web.