Comment établir un PRA efficace

Architecture solution de PRA · https://preview.nuabee.fr/documents/etablir-plan-reprise-activite-efficace/

Le bon usage des classes de protection Nuabee

Un Plan de Reprise d'Activité (PRA) s'apparente à une police d'assurance : tant qu'aucun sinistre ne survient, son utilité peut sembler abstraite. Comme pour toute assurance, l'enjeu consiste à optimiser le rapport coût-bénéfice pour obtenir une protection adaptée sans surdimensionner l'investissement.

C'est précisément dans cette logique que s'inscrit le système de classes de protection proposé par la solution Nuabee, qui permet une approche graduée et économiquement rationnelle :

- **Applications critiques** : Indispensables au fonctionnement des processus métiers essentiels. Leur indisponibilité entraîne un arrêt immédiat de l'activité.
- **Applications importantes** : Nécessaires dans un second temps si l'interruption se prolonge au-delà de quelques jours. Leur absence devient critique après cette période.
- **Autres applications** : Souhaitables uniquement en cas d'interruption prolongée. Leur restauration peut être différée sans impact majeur sur l'activité.

Méthodologie pour choisir les applications à protéger

Approche simplifiée sans BIA complet

Si vous souhaitez éviter une démarche de type **Business Impact Analysis** (**BIA**), qui nécessite des ressources expérimentées (RSSI, consultant externe) et peut s'avérer particulièrement structurante, une approche allégée reste possible pour définir le périmètre de protection.

Cette méthodologie simplifiée se décompose en deux étapes :

Étape 1 : Identification et classification des applications métiers

- Prioriser les applications métiers critiques et importantes selon leur impact opérationnel
- En déduire la liste exhaustive des serveurs métiers à inclure dans le PRA

Étape 2 : Analyse des dépendances

- Examiner les interdépendances avec les applications transverses et techniques
- Arbitrer leur niveau de criticité spécifiquement dans le contexte du PRA

Scénarios de risques à couvrir par le PRA

La définition des scénarios de risques constitue un élément déterminant dans l'établissement du périmètre du PRA. Le déploiement peut être phasé selon les différents types de menaces à couvrir.

Famille de scénario	Origine(s)	Type d'impact	A couvrir par PRA
Destruction du ou des datacenters	• Catastrophe naturelle • Risques industriels • Incendie • Actes de malveillance • …	Indisponibilité totale et prolongée du système d'information	Déploiement du périmètre du PRA peut être phasé par rapport aux scénarios de risques à couvrir.
Cyberattaque	• Cyber attaque ciblée • Compromission hyperviseur • Ransomware (filer)	Indisponibilité partielle du SI. Composants WAN/ sécurité non impactés	
Crise Humaine	• Mouvements sociaux • Crises sanitaires Pandémies	Absence du personnel pour gérer le SI	
Incident IT complexe	• Panne complexe infra technique • Défaillances techniques majeures	Indisponibilité plus ou moins courte du SI sur quelques composants	

Définition des RTO et RPO : impact économique

Comprendre les enjeux financiers

Les choix de **RTO** (Recovery Time Objective) et **RPO** (Recovery Point Objective) influencent directement les coûts récurrents de la solution :

Impact des RTO courts : Plus les objectifs de temps de reprise sont ambitieux, plus les composants impliqués dans le redémarrage (machines virtuelles, systèmes de stockage,

interfaces réseau) doivent être performants, entraînant des coûts proportionnellement plus élevés.

Impact des RPO courts : Des objectifs de perte de données minimisés nécessitent une fréquence de sauvegarde accrue, générant une augmentation du volume de stockage requis et de la consommation de bande passante pour réaliser les sauvegardes.

Personnalisation par serveur

La solution de PRA Nuabee propose généralement des paramètres globaux de RTO et RPO, tout en offrant la possibilité de personnaliser ces valeurs pour des serveurs particulièrement sensibles :

Personnalisation en RTO : Exemple : application de support hotline devant redémarrer impérativement sous 4 heures

Personnalisation en RPO : Exemple : base de données critique nécessitant une sauvegarde toutes les heures pour limiter la perte potentielle de données

Cette approche modulaire permet d'optimiser l'investissement en concentrant les ressources sur les éléments réellement critiques pour la continuité d'activité.