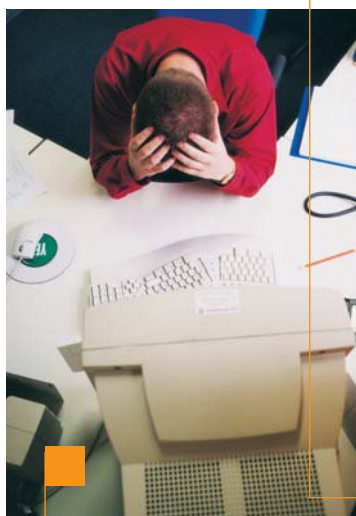


Le Plan de Reprise d'Activité ou PRA



Une réflexion inéluctable

La moitié des entreprises victimes d'un sinistre majeur de leur système d'information disparaissent dans les trois ans qui suivent l'incident.



L'activité des entreprises et organismes publics est aujourd'hui intimement liée à la disponibilité de leur système d'information. Au-delà de l'extension de la couverture fonctionnelle, la préoccupation première des responsables informatiques est devenue d'assurer la disponibilité maximale du service.

Incendie, malveillance, panne électrique, virus, inondation... les sinistres menaçant l'entreprise sont multiples et leurs conséquences financières peuvent être importantes, de par l'arrêt des services fournis à ses clients ou l'interruption de la production, voire la perte de données.

La continuité de l'activité devient un élément stratégique de la politique informatique de l'entreprise. Pour les serveurs existants ou pour tout nouveau projet, la priorité pour les directions informatiques est de mettre en perspective l'aspect disponibilité, et notamment de réfléchir à la mise en place d'un Plan de Continuité d'Activité (PCA) ou d'un PRA (Plan de Reprise d'Activité), destiné à pallier la perte totale ou partielle des équipements informatiques du site de production.

Un plan de reprise d'activité (PRA), ou plan de récupération après sinistre (DRP), consiste à mettre en place l'infrastructure matérielle et logicielle, les procédures de transfert de données, les procédures d'accès au système, ainsi que les processus humains permettant le redémarrage des services, en cas de perte partielle ou totale, du site informatique de production.

Le plan de secours : conditions et paramètres

Pour qu'un plan de secours soit opérationnel, il faut pouvoir, en cas d'activation :

- Disposer des plates-formes matérielles sur lesquelles relancer les applications concernées.
- Disposer d'une copie des données concernées les plus à jour possible.
- Garantir la disponibilité d'un réseau d'accès aux services en termes de liens de télécommunications.
- Disposer de procédures écrites et validées, connues des utilisateurs.

Les solutions techniques mises en œuvre pour répondre à ces pré-requis dépendront de nombreux paramètres parmi lesquels :

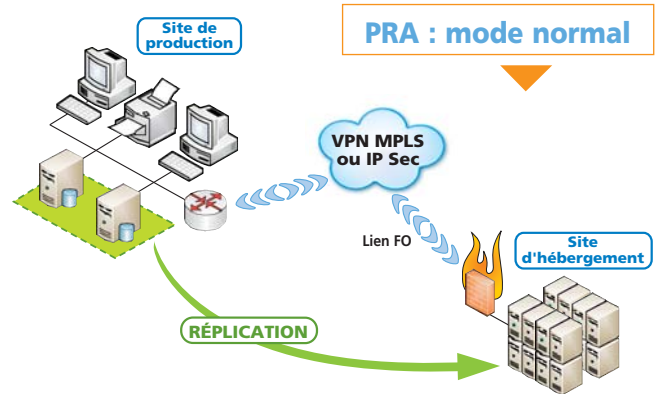
- Les applications et systèmes d'exploitation concernés. Le Return Time Objective (RTO) : délai dans lequel la solution de reprise doit être capable de restaurer le niveau de service attendu. Le Return Point Objective (RPO) : point de reprise en matière de données (fraîcheur des données après reprise).
- L'architecture télécommunication et réseau du ou des sites.
- Le niveau de service (SLA) attendu en mode secours.

Fort de son expérience d'opérateur de télécommunications (licence 21/0442), spécialiste de l'hébergement, Adista vous accompagne pour transformer l'innovation technologique des réseaux haut débit en avantages concrets. Nos compétences sont à votre disposition pour concevoir le PCA ou le PRA adapté à votre structure. Et nous vous proposons une large offre de services, s'appuyant sur nos salles d'hébergement sécurisées et leurs équipes d'exploitation, et sur notre offre télécommunications (fibre, xDSL...).

Architecture type du plan de secours

Le principe généralement mis en œuvre consiste en l'hébergement d'un ou plusieurs serveurs de secours, répliqués en temps réel à partir des serveurs de production, et hébergés dans un de nos datacenters. Ce centre d'hébergement est également un nœud télécoms, ce qui permet non seulement de redémarrer les services mais aussi de les mettre à disposition des utilisateurs.

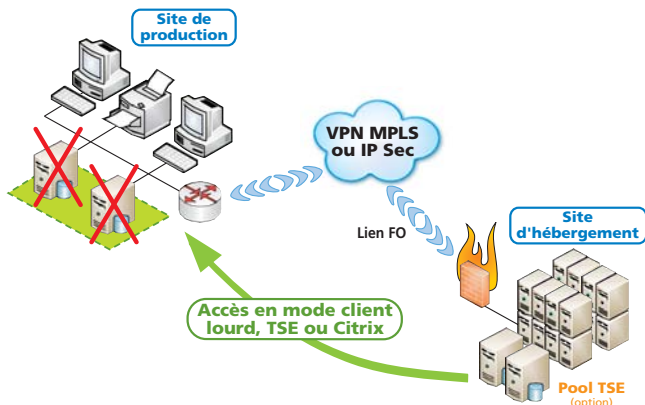
Le mécanisme de réplication dépend de la nature des serveurs et applications à protéger. Il peut s'agir d'une réplication applicative (par exemple : mécanismes de répliquations intrinsèques des SGBD), d'une réplication au niveau du système d'exploitation (Double-Take de NSI, Volume Replicator de Veritas), voire d'une réplication matérielle (réplication des baies SAN ou miroir iSCSI...).



Scénario de basculement site de l'entreprise opérationnel

Dans ce scénario, un RTO de 2 heures et un RPO quasi nul (pas de perte de données) sont parfaitement atteignables.

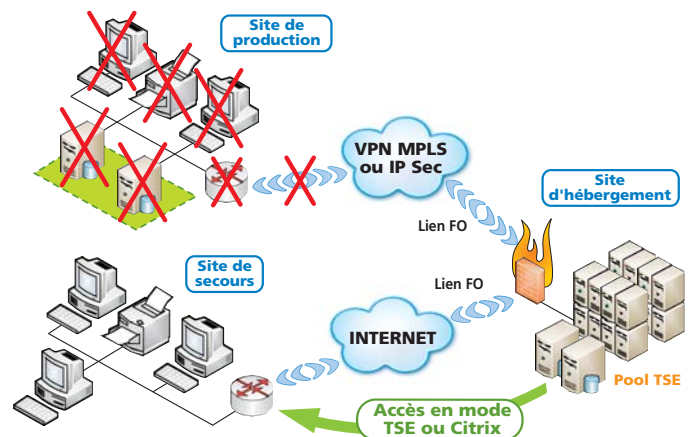
Scénario de basculement site opérationnel



Scénario de basculement vers un nouveau site utilisateurs

Si besoin est, lors du basculement en mode secours, des serveurs frontaux d'accès en mode client léger, disponibles dans notre parc de prêts, peuvent être intégrés dans la configuration (ce qui permet de conserver l'ensemble des authentifications et droits d'accès), autorisant ainsi l'accès aux serveurs de secours à travers de simples navigateurs Web.

Scénario de basculement vers un nouveau site utilisateurs



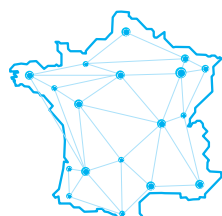
Accès des utilisateurs aux services rétablis

Dans tous les cas, une fois les services rétablis, deux scénarios doivent être envisagés pour l'accès des utilisateurs à ces services, selon le niveau de panne subi par le site de production :

Site opérationnel : le lien habituellement utilisé pour la réplication est utilisé dans le sens inverse pour permettre aux utilisateurs de se connecter aux services rétablis. Dans le cas d'un VPN multi-sites, tous les sites distants retrouvent l'accès au système d'information à travers ce même lien.

Site ou réseau indisponible : dans ce cas, l'accès au système d'information s'effectue à travers nos accès à Internet haut débit en mode terminal Windows. La localisation géographique des postes de travail n'a plus d'importance, ce qui offre une grande souplesse dans le choix du site de repli pour les utilisateurs.

Nos compétences sont à votre disposition afin de vous accompagner dans l'amélioration continue de votre système d'information.



Siège national
NANCY
1, rue Blaise Pascal
Site Technologique Saint-Jacques
54320 Maxéville
Tél. 03 57 54 54 00 - contact@adista.fr
www.adista.fr