Exemples

Pour un RPO de 24 heures, une sauvegarde journalière est la technique généralement utilisée. Pour un RPO de quelques heures, les techniques employées sont les snapshots ou la réplication asynchrone. Un RPO de 0 implique la mise en place d'un mode de réplication synchrone et correspond à une demande 'aucune perte de données'.

– Le **RTO** (*Recovery Time Objective*) correspond à la durée maximale d'interruption admissible. Le temps de redémarrage des applicatifs et leur mise en service détermine le RTO.

Exemples

Pour un RTO de 48 heures, il est possible d'utiliser des bandes situées sur un site distant protégé. Pour un RTO de 24 heures, la restauration à partir de bandes sur un site local peut être utilisée. Pour un RTO de 4 heures ou moins plusieurs techniques complémentaires doivent être mises en place : Clustering, réplication, techniques propres à VMware HA, FT, SRM, virtualisation du stockage...

La virtualisation simplifie certains process permettant d'atteindre des RTO réduits. Le RTO est fonction des techniques mises en place et dépend fortement du redémarrage des applications et de leur **consistance applicative** lorsque des arrêts brutaux surviennent sur le site de production. Si celle-ci n'est pas garantie, le RTO est variable et est difficilement prévisible.

Bien évidemment, toute entreprise souhaiterait pouvoir disposer de solutions permettant de ne perdre aucune donnée avec une remise en production la plus rapide possible en cas de problème. Mais il n'y a pas de secret, plus les temps de RPO et RTO sont faibles et plus la mise en place de telles solutions est coûteuse. **Il est donc fondamental d'engager les responsables et dirigeants afin de déterminer avec eux, les RTO et RPO qu'ils souhaitent en fonction des contraintes métiers et business**. On parle également de **BIA** (*Business Impact Analysis*) qui permet de quantifier la valeur réelle d'une donnée pour l'entreprise. Il n'est pas rare d'avoir trop d'investissement sur la protection des mauvaises données (importantes pour l'administrateur mais pas forcément pour l'entreprise) et pas assez sur les bonnes. Une décision collégiale est à privilégier pour valider ensemble les risques encourus en fonction des solutions choisies.

© Editions ENI - All rights reserved

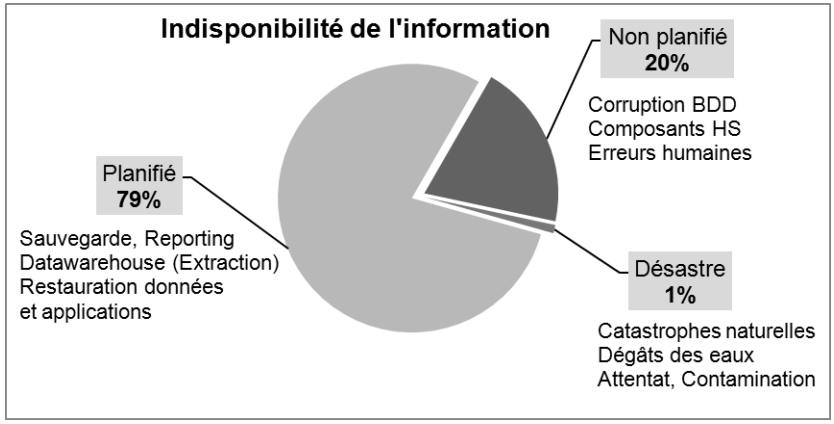
Le **SLA** (*Service Level Agreement*) est un contrat spécifiant des niveaux de services. Il s'agit d'un engagement formel et contraignant, établi entre un prestataire et son client. Les notions de RTO et RPO sont importantes lorsque ce contrat s'établit.

1.2 La disponibilité de l'information

Remarque

***Statistiques** : 93 % des entreprises ayant perdu leur Datacenter pendant dix jours ou plus à la suite d'une panne majeure ont fait faillite dans l'année suivante (NARA : National Archives and Records Administration).*

Le système d'information est essentiel pour une entreprise. Celui-ci permet aux utilisateurs d'être productifs et de disposer de moyens de communication efficaces tels que l'usage d'une messagerie, d'outils collaboratifs, réseaux sociaux… Pour l'entreprise le système d'information fournit les applications métiers pour accompagner le Business. Une indisponibilité même partielle de tel ou tel service peut faire perdre beaucoup d'argent à une entreprise. Il est donc crucial de mettre en place des dispositifs qui réduisent les interruptions de service et de pouvoir remettre le système en fonctionnement en cas d'incidents majeurs survenant sur le site de production.



Causes de l'indisponibilité de l'information généralement constatées.

Comme on peut le constater sur ce graphique, la plus grande part du temps d'indisponibilité (79 % du temps) vient de maintenances planifiées pour des opérations de sauvegarde, rajout de matériel, migration, extraction de données (Datawarehouse) qui sont donc prévisibles mais qui peuvent provoquer malgré tout des indisponibilités de service. Les autres types d'indisponibilité concernent des événements imprévisibles qui ne peuvent être anticipés dont les conséquences peuvent être dramatiques si des mesures et procédures fiables ne sont pas mises en place.

La disponibilité de l'information est établie selon le calcul suivant :

IA = MTBF / (MTBF + MTTR)

IA (*Information Availability*) : disponibilité de l'information.

MTBF (*Mean Time Between Failure*) : temps moyen pour un système ou un composant avant de tomber en panne.

MTTR (*Mean Time To Repair*) : temps moyen pour réparer un composant HS. MTTR inclut le temps passé à détecter le composant HS, planifier l'intervention d'un technicien, diagnostiquer le composant, obtenir le composant de remplacement (Spare) puis réparer et remettre en production le système.

La disponibilité de l'information se mesure en pourcentage, en nombre de 9 et permet de répondre aux besoins métiers pour une durée déterminée. Plus le nombre de 9 est élevé et plus la disponibilité est haute. On parle généralement de Haute Disponibilité à partir de 99,999 %.

Voici un tableau de correspondance entre la disponibilité (en nombre de 9) et le temps d'indisponibilité que cela représente.

Pourcentage de disponibilité	Temps d'indisponibilité
98 %	7,3 jours
99 %	3,65 jours
99,80 %	17 hrs 31 min
99,90 %	8 hrs 45 min
99,99 %	52,5 min
99,999 %	5,25 min
99,9999 %	31,5 sec

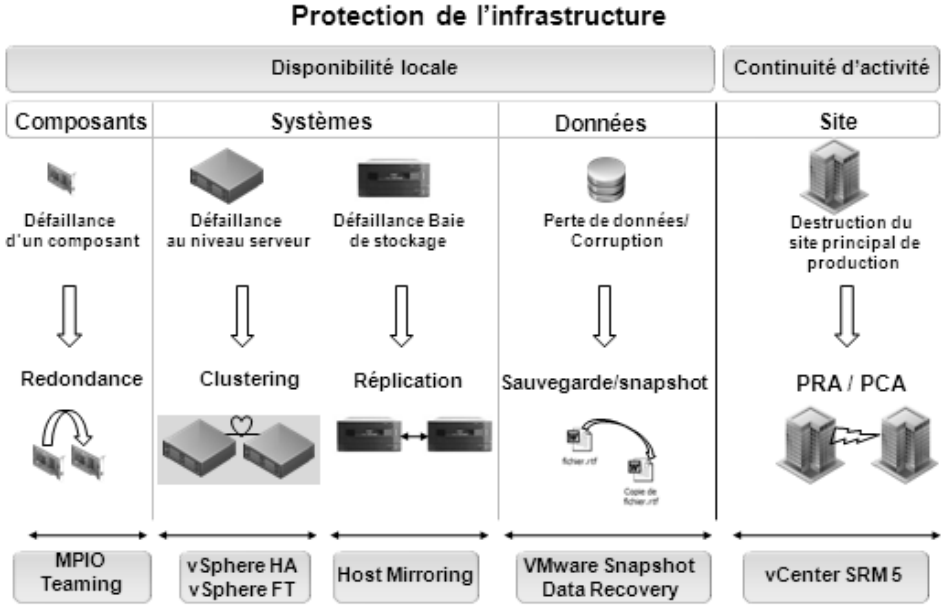
© Editions ENI - All rights reserved

Remarque

Un système ayant une disponibilité de 99,999 représente 5,25 minutes maximum d'arrêt par an. À noter que cette durée est très courte puisqu'elle représente moins que le temps de reboot d'un serveur physique !

1.3 Protection de l'infrastructure

La protection du système d'information peut être classée en deux catégories : la **disponibilité locale** sur un site et la **continuité d'activité** lorsqu'un incident majeur survient sur le site de production.



– La **disponibilité locale** a pour objet de supprimer les interruptions de service lorsqu'un composant tombe en panne, grâce à :
  – La mise en place de redondance **matérielle** pour éliminer les SPOF (*Single Point of Failure*).
  – La mise en place de systèmes de clustering pour remettre rapidement en production des **applications** en cas de crash de serveurs.

  - La sécurisation des **données** au travers de sauvegarde pour faire face à la perte de données ou à des mécanismes de réplication pour faire face à la perte d'une baie de stockage.
  - La mise en place de snapshots pour un retour arrière rapide vers un état sain lorsqu'un **applicatif est corrompu**.
- La **continuité d'activité** a pour objet de remettre en fonctionnement rapidement un site de production lorsqu'un événement majeur survient. Les notions de **PRA** (Plan de Reprise d'Activité), **PCA** (Plan de Continuité d'Activité) ou **PSI** (Plan de Secours Informatique) sur un site de secours permettent de faire face à ces événements survenant au niveau du Datacenter de production.

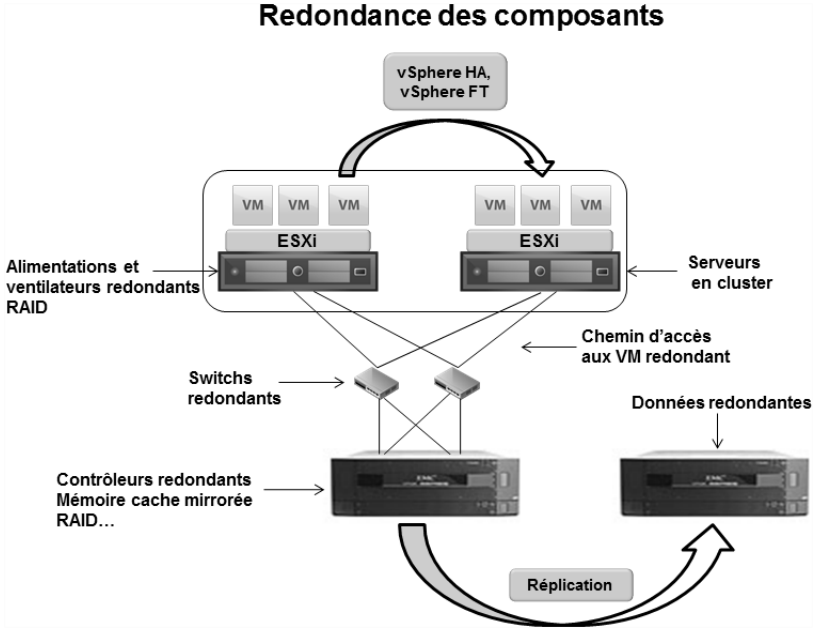
La sauvegarde faisant partie intégrante de la protection et étant un sujet important à traiter, un chapitre lui est consacré.

2. La disponibilité locale

2.1 Suppression de SPOF (Single Point of Failure)

La virtualisation de l'infrastructure engendre une consolidation sur un nombre réduit d'équipements. Ces équipements hébergeant un nombre important de VM, ils deviennent donc hautement critiques. Un arrêt d'un seul de ces équipements peut engendrer une interruption de plusieurs VM dont les conséquences pour le système d'information peuvent être dramatiques. Un **SPOF** représente un composant qui peut rendre indisponible le système d'information s'il tombe en panne. Plusieurs techniques permettent de se prémunir contre cette éventualité en mettant en place de la redondance matérielle. En environnement virtualisé, les bonnes pratiques préconisent de redonder tous les éléments matériels afin de réduire les interruptions de service.

© Editions ENI - All rights reserved



Techniques permettant de supprimer les SPOF.

Les **disques durs** sont les composants les plus importants à protéger car ils contiennent les données et ils sont sollicités en permanence. Pour pallier des pannes de disques durs, il faut mettre des cartes **RAID**.

Les alimentations et ventilateurs sont susceptibles de chauffer et de tomber en panne. Pour pallier ces problèmes, il faut mettre des alimentations et ventilateurs redondants.

La **mémoire** peut être sécurisée grâce à des techniques de mirroring bien que cela soit peu répandu.

Les cartes réseau peuvent être sécurisées en suivant le protocole IEEE 802.3ad permettant d'agréger les liens.

Le processeur et la carte mère ne contiennent pas de mécaniques ils sont donc moins soumis à des dysfonctionnements. Cependant ces composants étant critiques, il est possible de les sécuriser au travers de solutions matérielles comme le **Fault Tolerant** de **NEC** ou **Stratus** dont l'architecture met en redondance la carte mère.