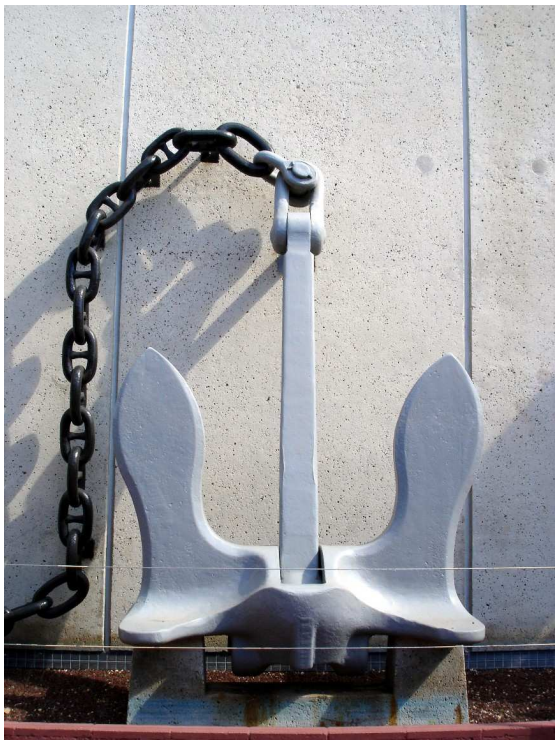
Enezis



Oracle Data Guard
Une solution complète de haute disponibilité

Sommaire

1 Bref historique et description de Data Guard

Les solutions de réplications de bases de données à base de logs d'archive existent depuis plusieurs années. Ce type de solution était connu sous le nom de « bases standby » dans le monde Oracle. L'ajout d'un nombre important de fonctionnalités (en particulier le Broker) a justifié sous Oracle 9i le changement de nom de cette solution en « Data Guard ». Les bases standby sont essentiellement destinées à gérer le risque de corruption des données : mauvaise manipulation applicative (un job passé à la mauvaise heure), un « drop table » passé par erreur sur la base de production, etc. Le principe de base de ce mécanisme est de copier sur le système secondaire les fichiers d'archive logs au fur et à mesure de leur production, ce qui signifie que les transactions présentes dans les redo logs courants sont potentiellement perdus. Il a fallu voir apparaître Data Guard en Oracle 9i pour que les logs puissent être mis simultanément à jour sur les systèmes primaires et secondaires, et qu'un délai de mise à jour de la base secondaire puisse être introduit.

Oracle 10g, et en particulier la Release 2, dispose à travers de Data Guard de fonctionnalités souvent supérieures à celles des réplications traditionnelles à base de stockage ou de gestionnaires de volumes.

2 Une solution complète de haute disponibilité pour Oracle

Deux technologies de réplications sont proposées par Data Guard : réplications des blocks des logs d'archive d'une part, réplication des ordres SQL d'autres part. Les bases de données produites dans le premier cas sont nommées « bases standby physique», les secondes « bases standby logiques ».

Les bases standby physiques sont en fait des bases de données qui se trouvent constamment en mode recouvrement, donc non accessibles, tandis que les bases logiques sont elles utilisables pour un accès en lecture. Les bases physiques peuvent à vrai dire être ouvertes elles aussi en mode lecture, mais cela impose la suspension de la réplication.

Des considérations de performances entrent également dans le choix de ces types de réplication de bases de données : les débits des blocks modifiés peut être tels que la solution de réplication SQL soit la seule option afin d'éviter de trop forts débits TCP/IP sur le réseau. A l'inverse, la base de donnée en mode de réplication physique consomme généralement moins de ressources sur la machine secondaire que

3 Data Guard et les autres solutions de réplications

Les deux autres possibilités de réplications sont :

1. Les solutions dites « host based », c'est-à-dire basée sur un mécanisme installé sur le serveur. Il peut s'agir de solutions Fiber Channel tel que les miroirs de volumes (ex : VxVm) ou de groupes de volumes, ou encore d'un miroir de file system (ex : SNFS d'Adic). D'autres solutions basées sur IP permettent d'intercepter des appels d'écritures, pour envoyer les mises à jour des fichiers sur le système secondaire.
2. Les solutions dites « array-based », qui sont basées sur des réplication de raid groups de baies de stockage (EMC SRDF, HP Continuous Access, etc.). Les protocoles sous-jacents peuvent être basés sur le Fiber Channel, mais aussi sur IP (iSCSI en particulier).

Comment peut-on comparer une solution telle que Data Guard avec les réplications « host » ou « array » ? La première évidence est que DG ne s'adresse qu'aux bases Oracle et pas aux fichiers « ordinaires » ou aux messageries. Mais pour les bases de données qui représentent la grande majorité

sinon l'intégralité du stockage sur nombre de SANs dans les grands centre de données, la réplication DG peut être avantageusement comparée aux autres mécanismes.

1. Périmètre de protection

   DG permet de différer les mises à jour, ce que ne permettent pas les systèmes de réplications basés sur le stockage ou les Volume Managers. On peut à la fois configurer DG pour qu'une copie synchrone des mises à jour dans les logs distants soit effectuée, ce qui garanti l'intégrité des mises à jours sur le système distant, tout en différant la mise à jour effective de la base miroir. Le delta de mise à jour peut être de plusieurs heures. Ce mécanisme permet par exemple de ramener la base de données à une heure donnée dans le passé en effectuant un roll forward qui ne prendra généralement pas plus que quelques minutes. La fonctionnalité de Flashback en Oracle 9i ne permet pas de défaire un « drop table », tandis que DG offre une protection contre les DDL intempestifs. Le Flashback en Oracle 10g autorise en revanche le « roll back » du DDL. Il est donc possible de conserver d'améliorer DG en 10g en le couplant aux Flashbacks au lieu de laisser un délai d'application des mises à jour.

2. Utilisation du réseau

   Seuls les redo logs sont copiés par DG. Pour une mise de jour de la base, les autres types de réplications imposeront la réplication des logs, mais également celle des achivelogs, des control files et des fichiers de données. Les débits et les rounds trips seront donc nettement plus forts, ce qui n'est pas négligeable pour les WAN et/ou pour les bases qui connaissent de forts débits de mises à jour.

3. Cluster

   DG est une alternative à l'utilisation d'un cluster basé sur une réplication hôte ou baie de stockage. Les clusters ont l'avantage de pouvoir détecter la perte d'un serveur et de basculer les volumes et/ou les file systems sur le système de secours. Pour les bases de données, DG possède en 10g une option dite « fast start failover » qui est un cluster pour les bases de données : un process surveille les connexions réseau et déclenche un failover en cas de défaillance du système primaire.

4 Conclusion

Data Guard en release 2 d'Oracle 10g est une solution complète de clustering pour les bases de données Oracle. Elle peut également être utilisée en complément d'un cluster classique ou de réplications « host » ou « array » qui permettent la mise à disposition sur un site de secours de tous les fichiers, en particuliers ceux qui sont accédés par les NAS. DG apporte dans ce cas des fonctionnalités de couvertures de risques de mauvaises manipulations, et peut être utilisé en complément des systèmes de flashback. On utilise également Data Guard pour couvrir les risques d'erreurs humaines dans les configurations Real Application Clusters : ces dernières permettent une protection physique en même temps que des possibilités de surcroît de puissance CPU et mémoire, mais n'offre aucune parade contre la corruption logique des données.