Protection des données Oracle

Enterprise applications

NetApp
February 10, 2026

Sommaire

Protection des données Oracle

Protection des données avec ONTAP

NetApp sait que les bases de données contient les données les plus stratégiques.

Une entreprise ne peut pas fonctionner sans accéder à ses données, et parfois l'activité repose sur les données. Ces données doivent être protégées, mais la protection ne se limite pas à garantir une sauvegarde utilisable. Elle consiste également à effectuer des sauvegardes rapidement et de manière fiable en plus de les stocker en toute sécurité.

L'autre côté de la protection des données est la restauration des données. Lorsque les données ne sont pas accessibles, l'entreprise est affectée et peut ne pas fonctionner tant qu'elle n'est pas restaurée. Ce processus doit être rapide et fiable. Enfin, la plupart des bases de données doivent être protégées contre les incidents, ce qui signifie maintenir une réplique de la base de données. La réplique doit être suffisamment à jour. Il doit également être rapide et simple de faire de la réplique une base de données entièrement opérationnelle.

Cette documentation remplace le rapport technique *TR-4591 : protection des données Oracle : sauvegarde, restauration et réplication.*

Planification

Une architecture de protection des données d'entreprise adaptée dépend des exigences de l'entreprise concernant la conservation des données, la restauration et la tolérance aux perturbations à divers moments.

Prenons l'exemple du nombre d'applications, de bases de données et de datasets importants pris en compte. Il est relativement simple d'élaborer une stratégie de sauvegarde pour un seul dataset afin d'assurer la conformité aux SLA standard, car la gestion ne comporte pas beaucoup d'objets. À mesure que le nombre de jeux de données augmente, la surveillance devient plus complexe et les administrateurs peuvent être obligés de consacrer de plus en plus de temps aux pannes de sauvegarde. Dès qu'un environnement évolue, il faut adopter une approche totalement différente.

La taille des datasets affecte également la stratégie. Par exemple, le jeu de données étant si petit, de nombreuses options sont possibles pour la sauvegarde et la restauration avec une base de données de 100 Go. En général, la simple copie des données à partir du support de sauvegarde avec des outils classiques permet d'atteindre un RTO suffisant pour la restauration. Une base de données de 100 To a généralement besoin d'une stratégie totalement différente, sauf si le RTO autorise une panne de plusieurs jours. Dans ce cas, une procédure classique de sauvegarde et de restauration basée sur des copies peut être acceptable.

Enfin, il y a des facteurs en dehors du processus de sauvegarde et de restauration lui-même. Par exemple, existe-t-il des bases de données qui prennent en charge les activités de production stratégiques, faisant de la restauration un événement rare uniquement effectué par des administrateurs de bases de données qualifiés ? Ou bien, les bases de données font-elles partie d'un vaste environnement de développement dans lequel la restauration est fréquente et gérée par une équipe INFORMATIQUE généraliste ?

Planification des objectifs de durée de restauration, de point de récupération et des SLA

ONTAP vous permet d'adapter facilement une stratégie de protection des données des bases de données Oracle aux besoins de votre entreprise.

Ces exigences comprennent des facteurs tels que la vitesse de restauration, la perte de données maximale autorisée et les besoins de conservation des sauvegardes. Le plan de protection des données doit également tenir compte de diverses exigences réglementaires en matière de conservation et de restauration des données. Enfin, différents scénarios de restauration des données doivent être pris en compte, allant de la restauration classique et prévisible résultant d'erreurs d'utilisateurs ou d'applications à des scénarios de reprise sur incident incluant la perte complète d'un site.

Les modifications mineures apportées aux règles de protection et de restauration des données peuvent avoir un impact significatif sur l'architecture globale du stockage, de la sauvegarde et de la restauration. Il est essentiel de définir et de documenter des normes avant de commencer le travail de conception afin d'éviter de compliquer une architecture de protection des données. Des fonctions ou des niveaux de protection inutiles entraînent des coûts et des frais de gestion inutiles. Par ailleurs, une exigence initialement négligée peut conduire un projet dans la mauvaise direction ou nécessiter des modifications de conception de dernière minute.

Objectif de délai de restauration

L'objectif de délai de restauration (RTO) définit le temps maximal autorisé pour la restauration d'un service. Par exemple, une base de données de ressources humaines peut atteindre un objectif de délai de restauration de 24 heures. En effet, même s'il ne serait pas très pratique de perdre l'accès à ces données pendant les jours de travail, l'entreprise peut tout de même fonctionner. En revanche, une base de données prenant en charge le grand livre d'une banque aurait un RTO mesuré en minutes, voire en secondes. Un objectif RTO de zéro n'est pas possible, car il doit y avoir un moyen de faire la différence entre une panne de service réelle et un événement de routine tel qu'un paquet réseau perdu. Toutefois, un objectif RTO quasi nul est généralement requis.

Objectif de point de récupération

L'objectif de point de récupération (RPO) définit la perte de données maximale tolérable. Dans de nombreux cas, l'objectif de point de récupération est uniquement déterminé par la fréquence des copies Snapshot ou des mises à jour snapmirror.

Dans certains cas, le RPO peut être rendu plus agressif, car il permet de protéger certaines données de manière sélective plus fréquemment. Dans un contexte de base de données, le RPO correspond généralement à la quantité de données perdues dans un journal spécifique. Dans un scénario de restauration typique dans lequel une base de données est endommagée en raison d'un bogue de produit ou d'une erreur utilisateur, le RPO doit être égal à zéro, ce qui signifie qu'il ne doit pas y avoir de perte de données. La procédure de restauration implique la restauration d'une copie antérieure des fichiers de base de données, puis la relecture des fichiers journaux pour ramener l'état de la base de données au point dans le temps souhaité. Les fichiers journaux requis pour cette opération doivent déjà être en place à l'emplacement d'origine.

Dans des scénarios inhabituels, les données des journaux peuvent être perdues. Par exemple, un accident ou un acte malveillant `rm -rf *` des fichiers de base de données peuvent entraîner la suppression de toutes les données. La seule option serait de restaurer des données à partir de sauvegardes, y compris des fichiers journaux, et certaines seraient inévitablement perdues. Dans un environnement de sauvegarde classique, la seule option permettant d'améliorer le RPO consiste à effectuer des sauvegardes répétées des données du journal. Cela a toutefois ses limites en raison du déplacement constant des données et de la difficulté à maintenir un système de sauvegarde en tant que service en continu. L'un des avantages des systèmes de stockage avancés est la capacité à protéger les données contre les dommages accidentels ou malveillants aux fichiers et à fournir ainsi un meilleur RPO sans déplacement des données.

Reprise après incident

La reprise après incident comprend l'architecture INFORMATIQUE, les règles et les procédures requises pour restaurer un service en cas d'incident physique. Cela peut inclure les inondations, les incendies ou les personnes agissant avec une intention malveillante ou négligente.

La reprise sur incident est bien plus qu'un ensemble de procédures de restauration. Il s'agit du processus complet d'identification des différents risques, de définition des exigences en matière de restauration des données et de continuité des services, et de mise à disposition de l'architecture appropriée avec les procédures associées.

Lors de l'établissement des exigences de protection des données, il est essentiel de faire la différence entre les objectifs RPO et RTO types et les exigences RPO et RTO requises pour la reprise après incident. Pour les situations de perte de données, allant d'une erreur utilisateur relativement normale à un incendie qui détruit un data Center, certains environnements applicatifs nécessitent un RPO nul et un RTO quasi nul. Cependant, il y a des conséquences administratives et des coûts pour ces niveaux élevés de protection.

En général, les exigences de restauration des données non liées aux incidents doivent être strictes pour deux raisons. Tout d'abord, les bogues d'application et les erreurs d'utilisateur qui endommagent les données sont prévisibles au point qu'ils sont presque inévitables. Deuxièmement, il n'est pas difficile de concevoir une stratégie de sauvegarde capable de fournir un RPO nul et un RTO faible tant que le système de stockage n'est pas détruit. Il n'y a aucune raison de ne pas traiter un risque important facilement résolu. C'est pourquoi les objectifs RPO et RTO pour la reprise locale doivent être agressifs.

Les exigences en termes de RTO et de RPO pour la reprise d'activité varient plus largement en fonction du risque d'incident et des conséquences de la perte de données ou de l'interruption pour une entreprise. Les exigences en matière de RPO et de RTO doivent être basées sur les besoins réels de l'entreprise et non sur des principes généraux. Ils doivent prendre en compte plusieurs scénarios de catastrophe physique et logique.

Incidents logiques

Les incidents logiques incluent la corruption des données provoquée par les utilisateurs, les bogues des applications ou du système d'exploitation et les dysfonctionnements logiciels. Les incidents logiques peuvent également inclure des attaques malveillantes de tiers contenant des virus ou des vers, ou encore en exploitant les vulnérabilités des applications. Dans ces cas, l'infrastructure physique n'est pas endommagée, mais les données sous-jacentes ne sont plus valides.

Les ransomwares sont un type de catastrophe logique de plus en plus courant qui sert à chiffrer les données à l'aide d'un vecteur d'attaque. Le chiffrement n'endommage pas les données, mais il les rend indisponibles jusqu'à ce que le paiement soit effectué à un tiers. De plus en plus d'entreprises sont spécifiquement la cible de piratage. Face à cette menace, NetApp propose des snapshots inviolables où même l'administrateur du stockage ne peut pas modifier les données protégées avant la date d'expiration configurée.

Incidents physiques

Les incidents physiques incluent la défaillance de composants d'une infrastructure qui dépasse ses capacités de redondance et entraînent une perte de données ou une perte de service prolongée. Par exemple, la protection RAID assure la redondance des disques durs et l'utilisation de HBA assure la redondance des ports FC et des câbles FC. Les pannes matérielles de ces composants sont prévisibles et n'ont pas d'incidence sur la disponibilité.

Dans un environnement d'entreprise, il est généralement possible de protéger l'infrastructure d'un site entier avec des composants redondants au point où le seul scénario de catastrophe physique prévisible est la perte complète du site. La planification de la reprise d'activité dépend alors de la réplication de site à site.

Protection des données synchrone et asynchrone

Dans l'idéal, toutes les données seraient répliquées de manière synchrone sur des sites dispersés géographiquement. Une telle réplication n'est pas toujours possible, voire possible pour plusieurs raisons :

- La réplication synchrone entraîne inévitablement une augmentation de la latence d'écriture, car toutes les modifications doivent être répliquées vers les deux emplacements avant que l'application/la base de données ne puisse poursuivre le traitement. L'effet de performance qui en résulte est parfois inacceptable, excluant l'utilisation de la mise en miroir synchrone.
- En raison de l'adoption accrue de 100 % de stockage SSD, il est plus probable que l'on remarque une latence d'écriture supplémentaire, car les attentes en termes de performances comprennent des centaines de milliers d'IOPS et une latence inférieure à la milliseconde. Pour tirer pleinement parti de l'utilisation de 100 % des SSD, il peut être nécessaire de revoir la stratégie de reprise sur incident.
- La croissance des datasets en octets continue, ce qui engendre des défis en garantissant une bande passante suffisante pour soutenir la réplication synchrone.
- La croissance des datasets s'accompagne également de défis liés à la gestion de la réplication synchrone à grande échelle.
- Les stratégies basées sur le cloud impliquent souvent des distances de réplication et une latence plus importantes, ce qui exclut davantage l'utilisation de la mise en miroir synchrone.

NetApp propose des solutions qui incluent à la fois la réplication synchrone pour satisfaire les besoins les plus exigeants en matière de restauration des données et des solutions asynchrones qui assurent des performances et une flexibilité accrues. De plus, la technologie NetApp s'intègre en toute transparence à de nombreuses solutions de réplication tierces, telles qu'Oracle DataGuard

Durée de conservation

Le dernier aspect d'une stratégie de protection des données est la durée de conservation des données, qui peut varier considérablement.

- Il est généralement nécessaire d'effectuer 14 jours de sauvegardes nocturnes sur le site principal et 90 jours de sauvegardes sur un site secondaire.
- De nombreux clients créent des archives trimestrielles autonomes stockées sur différents supports.
- Une base de données constamment mise à jour n'a peut-être pas besoin de données historiques, et les sauvegardes ne doivent être conservées que pendant quelques jours.
- Pour des raisons réglementaires, une capacité de restauration peut être nécessaire au point de toute transaction arbitraire dans une fenêtre de 365 jours.

Disponibilité de la base de données

ONTAP est conçu pour offrir une disponibilité maximale des bases de données Oracle. Ce document ne contient pas de description complète des fonctionnalités de haute disponibilité de ONTAP. Cependant, comme pour la protection des données, il est important de bien comprendre cette fonctionnalité lors de la conception d'une infrastructure de base de données.

Paires HA

L'unité de base de la haute disponibilité est la paire haute disponibilité. Chaque paire contient des liens

redondants pour prendre en charge la réplication des données vers la mémoire NVRAM. La NVRAM n'est pas un cache d'écriture. La RAM à l'intérieur du contrôleur sert de cache d'écriture. L'objectif de la mémoire NVRAM est de journaliser temporairement les données afin de prévenir toute panne système inattendue. À cet égard, il est similaire à un fichier redo log de base de données.

La mémoire NVRAM et le journal de reprise de base de données sont utilisés pour stocker des données rapidement, ce qui permet d'y apporter les modifications le plus rapidement possible. La mise à jour des données persistantes sur les disques (ou fichiers de données) n'a lieu qu'une fois plus tard lors d'un processus appelé point de contrôle sur ONTAP et la plupart des plateformes de bases de données. Les données NVRAM et les redo logs de base de données ne sont pas lus pendant les opérations normales.

Si un contrôleur tombe en panne brusquement, des modifications sont susceptibles d'être en attente de stockage dans la mémoire NVRAM qui n'ont pas encore été écrites sur les disques. Le contrôleur partenaire détecte la panne, prend le contrôle des disques et applique les modifications requises qui ont été stockées dans la mémoire NVRAM.

Takeover et Giveback

Le basculement et le rétablissement font référence au processus de transfert de la responsabilité des ressources de stockage entre les nœuds d'une paire HA. Le basculement et le rétablissement sont deux aspects :

- Gestion de la connectivité réseau permettant l'accès aux lecteurs
- Gestion des disques eux-mêmes

Les interfaces réseau prenant en charge le trafic CIFS et NFS sont configurées avec un emplacement de home et de basculement. Il inclut le déplacement des interfaces réseau vers leur domicile temporaire sur une interface physique située sur le(s) même(s) sous-réseau que l'emplacement d'origine. Le rétablissement inclut le déplacement des interfaces réseau vers leurs emplacements d'origine. Le comportement exact peut être réglé selon les besoins.

Les interfaces réseau prenant en charge les protocoles de bloc SAN, tels que iSCSI et FC, ne sont pas déplacées pendant le basculement et le rétablissement. Les LUN doivent plutôt être provisionnées avec des chemins qui incluent une paire HA complète entraînant un chemin principal et un chemin secondaire.

Des chemins d'accès supplémentaires vers des contrôleurs supplémentaires peuvent également être configurés pour prendre en charge le déplacement des données entre les nœuds d'un cluster plus grand, mais cela ne fait pas partie du processus de haute disponibilité.

Le deuxième aspect du Takeover et Giveback est le transfert de la propriété de disque. Le processus exact dépend de plusieurs facteurs, notamment la raison du Takeover/Giveback et les options de ligne de commande émises. L'objectif est de réaliser l'opération aussi efficacement que possible. Bien que le processus global puisse sembler durer plusieurs minutes, le moment réel où la propriété du disque est transférée d'un nœud à un autre peut généralement se mesurer en secondes.

Temps de reprise

Les E/S de l'hôte font l'objet d'une courte pause au niveau des E/S lors des opérations de basculement et de rétablissement. Cependant, la configuration de l'environnement ne doit pas provoquer d'interruption des applications. Le processus de transition réel dans lequel les E/S sont retardées se mesure généralement en secondes, mais l'hôte peut avoir besoin de plus de temps pour reconnaître la modification des chemins de données et renvoyer les opérations d'E/S.

La nature de la perturbation dépend du protocole :

- Une interface réseau prenant en charge le trafic NFS et CIFS émet une requête ARP (Address Resolution Protocol) vers le réseau après la transition vers un nouvel emplacement physique. Les commutateurs réseau mettent ainsi à jour leurs tables d'adresses MAC (Media Access Control) et reprennent le traitement des E/S. L'interruption dans le cas d'un basculement et d'un rétablissement planifiés se mesure généralement en secondes et, dans la plupart des cas, elle n'est pas détectable. Certains réseaux peuvent être plus lents à reconnaître pleinement le changement de chemin réseau et certains systèmes d'exploitation peuvent mettre en file d'attente beaucoup d'E/S dans un délai très court qui doit être réessayé. Cela peut prolonger le temps nécessaire pour reprendre les E/S.
- Une interface réseau prenant en charge les protocoles SAN ne peut pas être mise à niveau vers un nouvel emplacement. Un système d'exploitation hôte doit modifier le ou les chemins utilisés. La pause des E/S observée par l'hôte dépend de plusieurs facteurs. Du point de vue du système de stockage, la période pendant laquelle les E/S ne peuvent pas être servies ne prend que quelques secondes. Cependant, des systèmes d'exploitation hôtes différents peuvent nécessiter plus de temps pour permettre à une E/S de se déconnecter avant de réessayer. Les systèmes d'exploitation les plus récents sont mieux à même de reconnaître un changement de chemin beaucoup plus rapidement, mais les systèmes d'exploitation plus anciens nécessitent généralement jusqu'à 30 secondes pour reconnaître un changement.

Les délais de basculement attendus lors desquels le système de stockage ne peut pas transmettre de données à un environnement applicatif sont indiqués dans le tableau ci-dessous. Aucun environnement applicatif ne doit contenir d'erreurs ; le basculement doit alors apparaître sous forme de courte pause dans le traitement des E/S.

	NFS	AFF	ASA
Basculement planifié	15 s	6-10 s	2-3 s
Basculement non planifié	30 s	6-10 s	2-3 s

Checksums et intégrité des données

ONTAP et les protocoles qu'il prend en charge incluent de nombreuses fonctionnalités qui protègent l'intégrité des bases de données Oracle, notamment les données au repos et les données transmises sur le réseau.

La protection logique des données dans ONTAP comprend trois exigences clés :

- Les données doivent être protégées contre la corruption.
- Les données doivent être protégées contre les pannes disques.
- Les modifications de données doivent être protégées contre la perte.

Ces trois besoins sont abordés dans les sections suivantes.

Corruption du réseau : checksums

Le niveau de protection de données le plus élémentaire est la somme de contrôle, qui est un code spécial de détection d'erreur stocké avec les données. La corruption des données lors de la transmission du réseau est détectée grâce à l'utilisation d'un checksum et, dans certains cas, de multiples checksums.

Par exemple, une trame FC inclut une forme de somme de contrôle appelée contrôle de redondance cyclique (CRC) pour s'assurer que la charge utile n'est pas corrompue en transit. L'émetteur envoie les données et le CRC des données. Le récepteur d'une trame FC recalcule le CRC des données reçues pour s'assurer qu'il correspond au CRC transmis. Si le nouveau CRC calculé ne correspond pas au CRC joint à la trame, les

données sont corrompues et la trame FC est supprimée ou rejetée. Une opération d'E/S iSCSI comprend des checksums au niveau des couches TCP/IP et Ethernet. Pour une protection supplémentaire, elle peut également inclure la protection CRC facultative au niveau de la couche SCSI. Toute corruption de bit sur le fil est détectée par la couche TCP ou la couche IP, ce qui entraîne la retransmission du paquet. Comme avec FC, les erreurs dans le CRC SCSI entraînent une suppression ou un rejet de l'opération.

Corruption de disque : checksums

Des checksums sont également utilisés pour vérifier l'intégrité des données stockées sur les disques. Les blocs de données écrits sur les disques sont stockés avec une fonction de checksum qui génère un nombre imprévisible lié aux données d'origine. Lorsque les données sont lues à partir du lecteur, la somme de contrôle est recalculée et comparée à la somme de contrôle stockée. Si elle ne correspond pas, les données sont corrompues et doivent être restaurées par la couche RAID.

Corruption des données : écritures perdues

L'un des types de corruption les plus difficiles à détecter est une écriture perdue ou mal placée. Lorsqu'une écriture est reconnue, elle doit être écrite sur le support à l'emplacement correct. La corruption des données sur place est relativement facile à détecter à l'aide d'une simple somme de contrôle stockée avec les données. Cependant, si l'écriture est simplement perdue, alors la version précédente des données peut toujours exister et le total de contrôle serait correct. Si l'écriture est placée au mauvais emplacement physique, la somme de contrôle associée sera à nouveau valide pour les données stockées, même si l'écriture a détruit d'autres données.

La solution à ce défi est la suivante :

- Une opération d'écriture doit inclure des métadonnées indiquant l'emplacement où l'écriture est attendue.
- Une opération d'écriture doit inclure une sorte d'identifiant de version.

Lorsque ONTAP écrit un bloc, il inclut les données à l'emplacement où ce bloc appartient. Si une lecture ultérieure identifie un bloc, mais que les métadonnées indiquent qu'il appartient à l'emplacement 123 lorsqu'il a été trouvé à l'emplacement 456, l'écriture a été déplacée.

Il est plus difficile de détecter une écriture entièrement perdue. L'explication est très complexe, mais ONTAP stocke les métadonnées de façon à ce qu'une opération d'écriture entraîne des mises à jour vers deux emplacements différents sur les disques. En cas de perte d'une écriture, une lecture ultérieure des données et des métadonnées associées affiche deux identités de version différentes. Cela indique que l'écriture n'a pas été effectuée par le lecteur.

La corruption des écritures perdues ou déplacées est extrêmement rare. Cependant, avec la croissance continue des disques et l'expansion des jeux de données en exaoctets, le risque augmente. La détection des pertes en écriture doit être incluse dans tout système de stockage prenant en charge les charges de travail de la base de données.

Panne de disque : RAID, RAID DP et RAID-TEC

Si un bloc de données sur un disque est détecté comme étant corrompu, ou si l'ensemble du disque tombe en panne et est totalement indisponible, les données doivent être reconstituées. Cette opération est réalisée dans ONTAP à l'aide de disques de parité. Les données sont réparties sur plusieurs disques, puis des données de parité sont générées. Ces données sont stockées séparément des données d'origine.

ONTAP utilisait à l'origine RAID 4, qui utilise un seul lecteur de parité pour chaque groupe de lecteurs de données. Le résultat a été qu'un disque du groupe pouvait tomber en panne sans entraîner de perte de données. En cas de panne du disque de parité, aucune donnée n'a été endommagée et un nouveau disque de

parité a pu être construit. En cas de panne d'un seul lecteur de données, les lecteurs restants peuvent être utilisés avec le lecteur de parité pour régénérer les données manquantes.

Lorsque les disques étaient petits, le risque statistique de défaillance simultanée de deux disques était négligeable. Avec l'augmentation des capacités des disques, la reconstruction des données suite à une panne disque s'est également accompagnée d'un temps considérable. Cela a augmenté la fenêtre au cours de laquelle une panne de second disque entraînerait la perte de données. De plus, le processus de reconstruction crée une grande quantité d'E/S supplémentaires sur les disques survivants. Au fur et à mesure du vieillissement des disques, le risque d'une charge supplémentaire entraînant une panne de second disque augmente également. Enfin, même si le risque de perte de données n'augmente pas avec l'utilisation continue de RAID 4, les conséquences de la perte de données deviendront plus graves. Plus la perte de données en cas de panne d'un groupe RAID est importante, plus la restauration des données est longue, ce qui entraîne une interruption de l'activité prolongée.

Ces problèmes ont conduit NetApp à développer la technologie NetApp RAID DP, une variante de RAID 6. Cette solution comprend deux disques de parité, ce qui signifie que deux disques d'un groupe RAID peuvent tomber en panne sans générer de perte de données. Les disques ont continué de croître en taille, ce qui a conduit NetApp à développer la technologie NetApp RAID-TEC, qui introduit un troisième disque de parité.

Certaines meilleures pratiques en matière de bases de données historiques recommandent l'utilisation de RAID-10, également appelée mise en miroir par bandes. Cela offre une protection des données inférieure à celle de RAID DP, car il existe plusieurs scénarios de défaillance de deux disques, alors que dans RAID DP, il n'en existe aucune.

Par ailleurs, certaines bonnes pratiques en matière d'historique de bases de données indiquent que RAID-10 est préféré aux options RAID-4/5/6 en raison de problèmes de performances. Ces recommandations font parfois référence à une pénalité RAID. Bien que ces recommandations soient généralement correctes, elles ne s'appliquent pas aux implémentations de RAID dans ONTAP. Le problème de performances est lié à la régénération de parité. Dans les implémentations RAID traditionnelles, le traitement des écritures aléatoires de routine effectuées par une base de données nécessite plusieurs lectures de disque pour régénérer les données de parité et terminer l'écriture. La pénalité est définie comme les IOPS de lecture supplémentaires requises pour exécuter les opérations d'écriture.

ONTAP n'engendre pas de pénalité RAID, car les écritures sont placées dans la mémoire où la parité est générée, puis écrites sur le disque sous la forme d'une seule bande RAID. Aucune lecture n'est requise pour terminer l'opération d'écriture.

En résumé, par rapport à RAID 10, les systèmes RAID DP et RAID-TEC fournissent une capacité utilisable nettement plus importante, une meilleure protection contre les pannes disque et sans sacrifier les performances.

Protection contre les pannes matérielles : NVRAM

Toute baie de stockage servant de charge de travail de base de données doit traiter les opérations d'écriture le plus rapidement possible. En outre, une opération d'écriture doit être protégée contre la perte d'un événement inattendu tel qu'une coupure de courant. Cela signifie que toute opération d'écriture doit être stockée en toute sécurité dans au moins deux emplacements.

Les systèmes AFF et FAS utilisent la mémoire NVRAM pour répondre à ces exigences. Le processus d'écriture fonctionne comme suit :

1. Les données d'écriture entrantes sont stockées dans la mémoire RAM.
2. Les modifications à apporter aux données du disque sont journalisées dans la mémoire NVRAM sur le nœud local et le nœud partenaire. La mémoire NVRAM n'est pas un cache d'écriture. Il s'agit plutôt d'un

journal similaire à un redo log de base de données. Dans des conditions normales, il n'est pas lu. Il est utilisé uniquement pour la restauration, par exemple après une coupure de courant pendant le traitement des E/S.

3. L'écriture est alors validée par l'hôte.

À ce stade, le processus d'écriture est complet du point de vue de l'application. Les données sont protégées contre les pertes, car elles sont stockées dans deux emplacements différents. Finalement, les modifications sont écrites sur le disque, mais ce processus est hors bande du point de vue de l'application, car il se produit après l'acquittement de l'écriture et n'affecte donc pas la latence. Ce processus est une fois de plus similaire à la journalisation de la base de données. Une modification de la base de données est enregistrée dans les journaux de reprise aussi rapidement que possible, et la modification est alors reconnue comme validée. Les mises à jour des fichiers de données sont effectuées beaucoup plus tard et n'affectent pas directement la vitesse de traitement.

En cas de panne de contrôleur, le contrôleur partenaire prend possession des disques requis et lit à nouveau les données consignées dans la mémoire NVRAM pour récupérer toutes les opérations d'E/S en cours de fonctionnement au moment de la défaillance.

Protection contre les défaillances matérielles : NVFAIL

Comme nous l'avons vu précédemment, une écriture n'est pas validée tant qu'elle n'a pas été connectée à la NVRAM et à la NVRAM locales sur au moins un autre contrôleur. Cette approche évite toute panne matérielle ou de courant qui entraîne une perte des E/S à la volée En cas de panne de la mémoire NVRAM locale ou de la connectivité au partenaire de haute disponibilité, ces données à la volée ne seront plus mises en miroir.

Si la mémoire NVRAM locale signale une erreur, le nœud s'arrête. Cet arrêt entraîne le basculement vers un contrôleur partenaire de haute disponibilité. Aucune donnée n'est perdue parce que le contrôleur qui connaît la défaillance n'a pas acquitté l'opération d'écriture.

ONTAP n'autorise pas le basculement lorsque les données sont désynchronisées, sauf si le basculement est forcé. Le fait de forcer une modification des conditions de cette manière reconnaît que les données peuvent être laissées pour compte dans le contrôleur d'origine et que la perte de données est acceptable.

Les bases de données sont particulièrement vulnérables à la corruption en cas de basculement forcé, car elles conservent de grands caches internes de données sur disque. En cas de basculement forcé, les modifications précédemment reconnues sont effectivement supprimées. Le contenu de la baie de stockage recule dans le temps et l'état du cache de la base de données ne reflète plus l'état des données sur le disque.

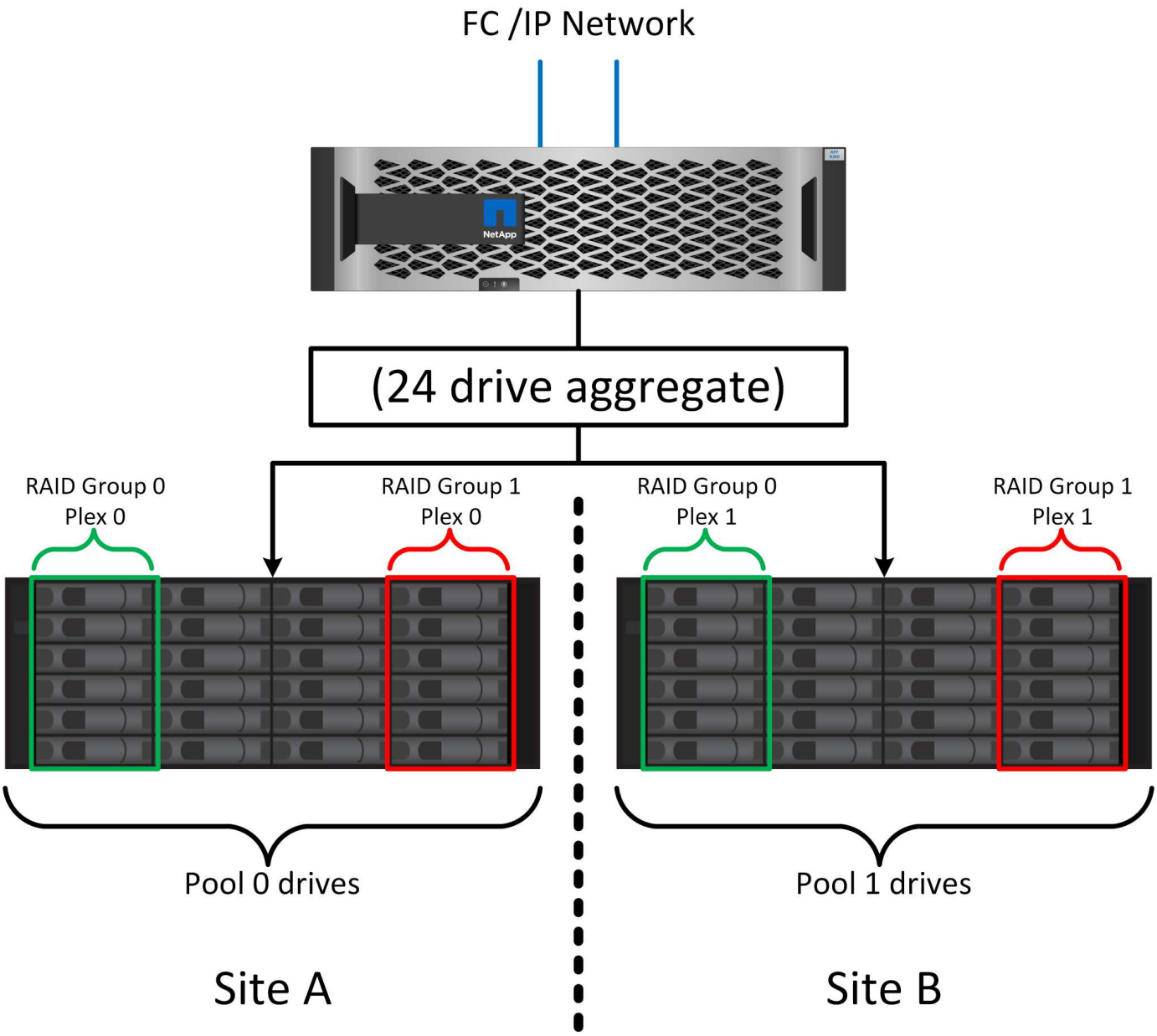
Afin de protéger les données de cette situation, ONTAP permet de configurer les volumes pour une protection spéciale contre les défaillances de mémoire NVRAM. Lorsqu'il est déclenché, ce mécanisme de protection entraîne l'entrée d'un volume dans un état appelé NVFAIL. Cet état entraîne des erreurs d'E/S qui entraînent l'arrêt d'une application et n'utilisent donc pas de données obsolètes. Les données ne doivent pas être perdues car une écriture reconnue doit être présente sur la matrice de stockage.

Les étapes suivantes habituelles sont qu'un administrateur arrête complètement les hôtes avant de remettre manuellement en ligne les LUN et les volumes. Bien que ces étapes puissent impliquer un certain travail, cette approche est le moyen le plus sûr d'assurer l'intégrité des données. Toutes les données n'ont pas besoin de cette protection. C'est pourquoi NVFAIL peut être configuré volume par volume.

Protection contre les pannes de site et de tiroir : SyncMirror et plexes

SyncMirror est une technologie de mise en miroir qui améliore, mais ne remplace pas, RAID DP ou RAID-TEC. Il met en miroir le contenu de deux groupes RAID indépendants. La configuration logique est la suivante :

- Les disques sont configurés en deux pools en fonction de leur emplacement. Un pool est composé de tous les disques du site A et le second est composé de tous les disques du site B.
- Un pool de stockage commun, appelé agrégat, est ensuite créé à partir de jeux en miroir de groupes RAID. Un nombre égal de lecteurs est tiré de chaque site. Par exemple, un agrégat SyncMirror de 20 disques se compose de 10 disques du site A et de 10 disques du site B.
- Chaque jeu de disques d'un site donné est automatiquement configuré comme un ou plusieurs groupes RAID-DP ou RAID-TEC entièrement redondants, indépendamment de l'utilisation de la mise en miroir. Les données sont ainsi protégées en permanence, même après la perte d'un site.



La figure ci-dessus illustre un exemple de configuration SyncMirror. Un agrégat de 24 disques a été créé sur le contrôleur avec 12 disques à partir d'un tiroir alloué sur le site A et 12 disques à partir d'un tiroir alloué sur le site B. Les disques ont été regroupés en deux groupes RAID en miroir. Le groupe RAID 0 comprend un plex de 6 disques sur le site A mis en miroir sur un plex de 6 disques sur le site B. De même, RAID Group 1 inclut un plex de 6 disques sur le site A mis en miroir sur un plex de 6 disques sur le site B.

SyncMirror est généralement utilisé pour assurer la mise en miroir à distance avec les systèmes MetroCluster,

avec une copie des données sur chaque site. Il a parfois été utilisé pour fournir un niveau supplémentaire de redondance dans un seul système. Il assure en particulier la redondance au niveau du tiroir. Un tiroir disque contient déjà deux blocs d'alimentation et contrôleurs. Dans l'ensemble, il ne s'agit pas d'une simple tôlerie, mais dans certains cas, une protection supplémentaire peut être garantie. Par exemple, un client NetApp a déployé SyncMirror sur une plateforme mobile d'analytique en temps réel utilisée lors des tests automobiles. Le système a été séparé en deux racks physiques alimentés par des alimentations indépendantes provenant de systèmes UPS indépendants.

Checksums

Le thème des checksums est particulièrement intéressant pour les administrateurs de bases de données habitués à l'utilisation de sauvegardes en continu Oracle RMAN qui migrent vers des sauvegardes basées sur des snapshots. RMAN permet notamment de procéder à des contrôles d'intégrité lors des opérations de sauvegarde. Bien que cette fonctionnalité présente un certain intérêt, son principal avantage est une base de données qui n'est pas utilisée sur une baie de stockage moderne. Lorsque des disques physiques sont utilisés pour une base de données Oracle, il est presque certain que la corruption finit par se produire lorsque les disques vieillissent, un problème qui est résolu par les checksums basés sur les baies dans les baies de stockage réelles.

Avec une baie de stockage réelle, l'intégrité des données est protégée par des checksums à plusieurs niveaux. Si les données sont corrompues dans un réseau IP, la couche TCP (transmission Control Protocol) rejette les données de paquets et demande la retransmission. Le protocole FC inclut des checksums, tout comme les données SCSI encapsulées. Une fois sur la matrice, ONTAP dispose d'une protection RAID et checksum. Une corruption peut se produire, mais, comme dans la plupart des baies d'entreprise, elle est détectée et corrigée. En général, un disque entier tombe en panne, ce qui invite à une reconstruction RAID et l'intégrité de la base de données n'est pas affectée. Il est toujours possible que des octets individuels sur un disque soient endommagés par le rayonnement cosmique ou par des cellules flash défectueuses. Si cela se produit, la vérification de parité échoue, le disque est mis hors service et la reconstruction RAID démarre. Là encore, l'intégrité des données n'est pas affectée. La dernière ligne de défense est l'utilisation de checksums. Si, par exemple, une erreur de micrologiciel catastrophique sur un disque a corrompu des données d'une manière qui n'a pas été détectée par un contrôle de parité RAID, le checksum ne correspond pas et ONTAP empêche le transfert d'un bloc corrompu avant que la base de données Oracle puisse le recevoir.

L'architecture des fichiers de données et des redo log Oracle est également conçue pour offrir le plus haut niveau possible d'intégrité des données, même dans des circonstances extrêmes. Au niveau le plus élémentaire, les blocs Oracle incluent un checksum et des contrôles logiques de base avec presque toutes les E/S. Si Oracle ne s'est pas écrasé ou n'a pas mis un tablespace hors ligne, les données sont intactes. Le degré de vérification de l'intégrité des données est réglable et Oracle peut également être configuré pour confirmer les écritures. Par conséquent, la quasi-totalité des scénarios de panne et de panne peuvent être restaurés, et dans le cas extrêmement rare d'une situation irrécupérable, la corruption est rapidement détectée.

La plupart des clients NetApp qui utilisent des bases de données Oracle cessent d'utiliser RMAN et d'autres produits de sauvegarde après la migration vers des sauvegardes snapshot. Il existe encore des options permettant d'utiliser RMAN pour effectuer une restauration au niveau des blocs avec SnapCenter. Toutefois, au quotidien, RMAN, NetBackup et d'autres produits ne sont utilisés qu'occasionnellement pour créer des copies d'archivage mensuelles ou trimestrielles.

Certains clients choisissent d'exécuter `dbv` périodiquement pour effectuer des contrôles d'intégrité sur leurs bases de données existantes. NetApp déconseille cette pratique, car elle entraîne une charge d'E/S inutile. Comme indiqué ci-dessus, si la base de données ne rencontrait pas de problèmes auparavant, le risque de `dbv` La détection d'un problème est proche de zéro et cet utilitaire entraîne une charge d'E/S séquentielles très élevée sur le réseau et le système de stockage. À moins qu'il n'y ait de raison de croire qu'il existe une corruption, comme l'exposition à un bogue connu d'Oracle, il n'y a aucune raison de s'exécuter `dbv`.

Notions de base sur la sauvegarde et la restauration

Sauvegardes basées sur des snapshots

La technologie Snapshot de NetApp constitue le socle de la protection des données des bases de données Oracle sur ONTAP.

Les valeurs clés sont les suivantes :

- **Simplicité.** Un instantané est une copie en lecture seule du contenu d'un conteneur de données à un moment donné.
- **Efficacité.** les instantanés ne nécessitent pas d'espace au moment de la création. L'espace n'est consommé que lorsque des données sont modifiées.
- **Gérabilité.** Une stratégie de sauvegarde basée sur les snapshots est facile à configurer et à gérer car les snapshots font partie intégrante du système d'exploitation du stockage. Si le système de stockage est sous tension, il est prêt à créer des sauvegardes.
- **Évolutivité.** vous pouvez conserver jusqu'à 1024 sauvegardes d'un seul conteneur de fichiers et de LUN. Dans le cas de jeux de données complexes, plusieurs conteneurs de données peuvent être protégés par un ensemble unique et cohérent de snapshots.
- Les performances ne sont pas affectées, qu'un volume contienne ou non 1024 snapshots.

Bien que de nombreux fournisseurs de stockage proposent la technologie Snapshot, la technologie Snapshot de ONTAP est unique et offre des avantages significatifs pour les environnements applicatifs et de bases de données d'entreprise :

- Les copies Snapshot font partie de la WAFL (Write-Anywhere File Layout) sous-jacente. Il ne s'agit pas d'une technologie complémentaire ou externe. La gestion est donc simplifiée, car le système de stockage est le système de sauvegarde.
- Les copies Snapshot n'affectent pas les performances, sauf dans certains cas en périphérie, par exemple lorsque le volume de données est stocké dans des snapshots que le système de stockage sous-jacent se remplit.
- Le terme « groupe de cohérence » fait souvent référence à un regroupement d'objets de stockage gérés comme un ensemble cohérent de données. La copie Snapshot d'un volume ONTAP donné constitue une sauvegarde de groupe de cohérence.

Les copies Snapshot ONTAP ont également une meilleure évolutivité que la technologie concurrente. Les clients peuvent stocker 5, 50 ou 500 copies Snapshot sans affecter les performances. Le nombre maximal de snapshots actuellement autorisés dans un volume est de 1024. Si une conservation supplémentaire des snapshots est nécessaire, il existe des options pour les transmettre en cascade à des volumes supplémentaires.

Par conséquent, la protection d'un dataset hébergé sur ONTAP est simple et hautement évolutive. Les sauvegardes ne nécessitent pas de déplacement de données. Par conséquent, une stratégie de sauvegarde peut être adaptée aux besoins de l'entreprise plutôt qu'aux limites des taux de transfert réseau, du grand nombre de lecteurs de bande ou des zones de transfert de disque.

Un snapshot est-il une sauvegarde ?

La question couramment posée sur l'utilisation des snapshots en tant que stratégie de protection des données est le fait que les données « réelles » et les données de snapshot se trouvent sur les mêmes disques. La perte de ces disques entraînerait la perte des données primaires et de la sauvegarde.

Ce problème est valide. Les snapshots locaux sont utilisés pour les besoins quotidiens de sauvegarde et de restauration, et dans ce sens, le snapshot est une sauvegarde. Dans les environnements NetApp, près de 99 % des scénarios de restauration s'appuient sur des copies Snapshot pour répondre aux exigences de RTO les plus strictes.

Toutefois, les snapshots locaux ne doivent jamais être la seule stratégie de sauvegarde. C'est pourquoi NetApp propose des technologies telles que la réplication SnapMirror et SnapVault pour répliquer rapidement et efficacement des copies Snapshot sur un ensemble indépendant de disques. Dans une solution bien conçue avec des snapshots et une réplication Snapshot, l'utilisation des bandes peut être réduite au minimum, voire même à une archive trimestrielle, ou totalement éliminée.

Sauvegardes basées sur des snapshots

Vous pouvez utiliser les copies Snapshot ONTAP pour protéger vos données, et les copies Snapshot sont la base de nombreuses autres fonctionnalités ONTAP, notamment la réplication, la reprise d'activité et le clonage. Une description complète de la technologie Snapshot ne fait pas partie du présent document, mais les sections suivantes offrent un aperçu général.

Il existe deux approches principales pour créer un snapshot d'un dataset :

- Sauvegardes cohérentes après panne
- Sauvegardes cohérentes au niveau des applications

Une sauvegarde cohérente après panne d'un dataset fait référence à la capture de l'ensemble de la structure du dataset à un point dans le temps. Si le dataset est stocké dans un seul volume, le processus est simple ; il est possible de créer une copie Snapshot à tout moment. Si un dataset s'étend sur plusieurs volumes, un snapshot de groupe de cohérence doit être créé. Plusieurs options sont disponibles pour la création des snapshots de groupe de cohérence, notamment le logiciel NetApp SnapCenter, les fonctionnalités natives de groupe de cohérence ONTAP et les scripts gérés par l'utilisateur.

Les sauvegardes cohérentes après panne sont principalement utilisées lorsque la restauration au point de sauvegarde est suffisante. Lorsqu'une restauration plus granulaire est nécessaire, des sauvegardes cohérentes au niveau des applications sont généralement nécessaires.

Le mot "cohérent" dans "application-cohérente" est souvent un mal nommer. Par exemple, le placement d'une base de données Oracle en mode de sauvegarde est appelé sauvegarde cohérente au niveau des applications, mais les données ne sont en aucun cas rendues cohérentes ou suspendues. Les données continuent de changer tout au long de la sauvegarde. En revanche, la plupart des sauvegardes MySQL et Microsoft SQL Server ont effectivement mis les données au repos avant d'exécuter la sauvegarde. VMware peut rendre certains fichiers cohérents ou non.

Groupes de cohérence

Le terme « groupe de cohérence » fait référence à la capacité d'une baie de stockage à gérer plusieurs ressources de stockage comme une seule image. Par exemple, une base de données peut comprendre 10 LUN. La baie doit pouvoir sauvegarder, restaurer et répliquer ces 10 LUN de manière cohérente. La restauration n'est pas possible si les images des LUN n'étaient pas cohérentes au point de sauvegarde. La réplication de ces 10 LUN nécessite que tous les réplicas soient parfaitement synchronisés.

Le terme « groupe de cohérence » n'est pas souvent utilisé lors des discussions sur ONTAP, car la cohérence a toujours été une fonction de base de l'architecture de volumes et d'agrégats au sein de ONTAP. De nombreuses autres baies de stockage gèrent des LUN ou des systèmes de fichiers en tant qu'unités individuelles. Ils peuvent ensuite être configurés en tant que « groupe de cohérence » pour la protection des données, mais cette étape supplémentaire est nécessaire dans la configuration.

ONTAP a toujours pu capturer des images locales et répliquées cohérentes de données. Bien que les différents volumes d'un système ONTAP ne soient généralement pas officiellement décrits comme des groupes de cohérence, c'est ce qu'ils sont. Une copie Snapshot de ce volume est une image de groupe de cohérence. La restauration de ce Snapshot correspond à une restauration de groupe de cohérence. SnapMirror et SnapVault proposent tous deux une réplication de groupe de cohérence.

Snapshots de groupes de cohérence

Les copies Snapshot de groupe de cohérence (cg-snapshots) sont une extension de la technologie Snapshot ONTAP de base. Une opération de snapshot standard crée une image cohérente de toutes les données d'un même volume, mais il est parfois nécessaire de créer un ensemble cohérent de snapshots sur plusieurs volumes et même sur plusieurs systèmes de stockage. Il en résulte un ensemble de snapshots qui peuvent être utilisés de la même manière qu'un snapshot d'un seul volume individuel. Elles peuvent être utilisées pour la restauration des données locales, répliquées à des fins de reprise après incident ou clonées sous la forme d'une unité cohérente unique.

L'utilisation la plus connue des cg-snapshots concerne un environnement de base de données d'environ 1 po de capacité couvrant 12 contrôleurs. Les snapshots de groupe de cohérence créés sur ce système ont été utilisés pour la sauvegarde, la restauration et le clonage.

La plupart du temps, lorsqu'un dataset s'étend sur des volumes et que l'ordre d'écriture doit être préservé, le logiciel de gestion choisi utilise automatiquement un snapshot de groupe de cohérence. Dans ce cas, il n'est pas nécessaire de comprendre les détails techniques des cg-snapshots. Toutefois, les exigences complexes en matière de protection des données nécessitent un contrôle détaillé du processus de protection et de réplication des données. Certains workflows d'automatisation ou scripts personnalisés permettent d'appeler les API cg-Snapshot. Pour comprendre la meilleure option et le rôle de cg-snapshot, vous devez fournir une explication plus détaillée de la technologie.

La création d'un ensemble de snapshots des groupes de cohérence s'effectue en deux étapes :

1. Établir une clôture d'écriture sur tous les volumes cibles.
2. Créez des instantanés de ces volumes à l'état clôturé.

L'escrime d'écriture est établi en série. Cela signifie que lorsque le processus de recel est configuré sur plusieurs volumes, les E/S d'écriture sont bloquées sur le premier volume de la séquence au fur et à mesure qu'elles continuent d'être validées sur les volumes qui apparaissent plus tard. Cela peut sembler initialement contraire à l'exigence de préservation de l'ordre d'écriture, mais cela s'applique uniquement aux E/S émises de manière asynchrone sur l'hôte et ne dépend pas d'autres écritures.

Par exemple, une base de données peut émettre de nombreuses mises à jour asynchrones des fichiers de données et permettre au système d'exploitation de réorganiser les E/S et de les compléter selon sa propre configuration de planificateur. L'ordre de ce type d'E/S ne peut pas être garanti car l'application et le système d'exploitation ont déjà libéré l'obligation de conserver l'ordre d'écriture.

Par exemple, la plupart des activités de journalisation de la base de données sont synchrones. La base de données ne procède pas à d'autres écritures de journal tant que les E/S n'ont pas été acquittées et que l'ordre de ces écritures doit être conservé. Si une E/S de journal arrive sur un volume clôturé, elle n'est pas validée et l'application se bloque lors d'écritures ultérieures. De même, les E/S des métadonnées du système de fichiers sont généralement synchrones. Par exemple, une opération de suppression de fichier ne doit pas être perdue. Si un système d'exploitation doté d'un système de fichiers xfs supprime un fichier et que les E/S qui ont mis à jour les métadonnées du système de fichiers xfs pour supprimer la référence à ce fichier ont été reçues sur un volume isolé, l'activité du système de fichiers est alors interrompue. Cela garantit l'intégrité du système de fichiers pendant les opérations cg-Snapshot.

Une fois l'isolation d'écriture configurée sur les volumes cibles, ils sont prêts pour la création d'instantanés. Les snapshots n'ont pas besoin d'être créés précisément en même temps, car l'état des volumes est figé du point de vue de l'écriture dépendant. Pour éviter toute faille dans l'application qui crée les instantanés cg, l'escrime d'écriture initiale inclut un délai configurable dans lequel ONTAP libère automatiquement l'escrime et reprend le traitement d'écriture après un nombre défini de secondes. Si tous les snapshots sont créés avant l'expiration du délai, le jeu de snapshots résultant est un groupe de cohérence valide.

Ordre d'écriture dépendant

Du point de vue technique, la préservation de l'ordre d'écriture et, plus particulièrement, de l'ordre d'écriture dépendant constitue la clé d'un groupe de cohérence. Par exemple, une base de données qui écrit 10 LUN écrit simultanément sur toutes ces LUN. De nombreuses écritures sont émises de manière asynchrone, ce qui signifie que l'ordre dans lequel elles sont effectuées n'est pas important et que l'ordre dans lequel elles sont effectuées varie en fonction du système d'exploitation et du comportement du réseau.

Certaines opérations d'écriture doivent être présentes sur le disque avant que la base de données puisse procéder à des écritures supplémentaires. Ces opérations d'écriture critiques sont appelées écritures dépendantes. Les E/S d'écriture suivantes dépendent de la présence de ces écritures sur le disque. Tout snapshot, restauration ou réplication de ces 10 LUN doit garantir l'ordre d'écriture dépendant. Les mises à jour du système de fichiers sont un autre exemple d'écritures dépendantes de l'ordre d'écriture. L'ordre dans lequel les modifications du système de fichiers sont effectuées doit être conservé, sinon l'ensemble du système de fichiers pourrait être corrompu.

Stratégies

Il existe deux approches principales des sauvegardes basées sur des snapshots :

- Sauvegardes cohérentes après panne
- Sauvegardes à chaud protégées pour les snapshots

Une sauvegarde cohérente après panne d'une base de données fait référence à la capture à un moment précis de l'ensemble de la structure de la base de données, y compris les fichiers de données, les journaux de reprise et les fichiers de contrôle. Si la base de données est stockée sur un seul volume, le processus est simple ; il est possible de créer un Snapshot à tout moment. Si la base de données s'étend sur plusieurs volumes, un snapshot de groupe de cohérence doit être créé. Plusieurs options sont disponibles pour la création des snapshots de groupe de cohérence, notamment le logiciel NetApp SnapCenter, les fonctionnalités natives de groupe de cohérence ONTAP et les scripts gérés par l'utilisateur.

Les sauvegardes Snapshot cohérentes après panne sont principalement utilisées lorsque la restauration au point de sauvegarde est suffisante. Les journaux d'archivage peuvent être appliqués dans certains cas, mais lorsqu'une restauration granulaire à un point dans le temps est nécessaire, il est préférable d'effectuer une sauvegarde en ligne.

La procédure de base pour une sauvegarde en ligne basée sur un snapshot est la suivante :

1. Placez la base de données dans `backup` mode.
2. Créez un Snapshot de tous les volumes qui hébergent les fichiers de données.
3. Quitter `backup` mode.
4. Lancer la commande `alter system archive log current` pour forcer l'archivage des journaux.
5. Créer des instantanés de tous les volumes hébergeant les journaux d'archivage.

Cette procédure permet d'obtenir un ensemble de snapshots contenant les fichiers de données en mode de

sauvegarde et les journaux d'archivage critiques générés en mode de sauvegarde. Il s'agit des deux conditions requises pour restaurer une base de données. Il est également conseillé de protéger les fichiers tels que les fichiers de contrôle, mais la seule condition absolue est la protection des fichiers de données et des journaux d'archivage.

Même si différents clients peuvent avoir des stratégies très différentes, la quasi-totalité de ces stratégies s'appuient sur les mêmes principes que ceux décrits ci-dessous.

Restauration basée sur des snapshots

Lors de la conception d'infrastructures de volumes pour les bases de données Oracle, la première décision est d'utiliser ou non la technologie VBSR (Volume-Based NetApp SnapRestore).

La fonction SnapRestore basée sur les volumes permet de rétablir quasi instantanément un volume à un point antérieur. Toutes les données du volume étant rétablies, VBSR peut ne pas convenir à toutes les utilisations. Par exemple, si l'intégralité d'une base de données, y compris les fichiers de données, les journaux de reprise et les journaux d'archivage, est stockée sur un seul volume restauré avec VBSR, les données sont perdues, car les nouveaux journaux d'archivage et les données de reprise sont supprimés.

La technologie VBSR n'est pas requise pour la restauration. De nombreuses bases de données peuvent être restaurées avec SFSR (Single File SnapRestore) ou en copiant simplement les fichiers du snapshot vers le système de fichiers actif.

La technologie VBSR est recommandée pour les bases de données très volumineuses ou si une restauration doit être effectuée le plus rapidement possible et que l'utilisation de VBSR nécessite l'isolement des fichiers de données. Dans un environnement NFS, les fichiers de données d'une base de données doivent être stockés sur des volumes dédiés non endommagés par d'autres types de fichiers. Dans un environnement SAN, les fichiers de données doivent être stockés sur des LUN dédiés sur des volumes dédiés. Si un gestionnaire de volumes est utilisé (y compris Oracle Automatic Storage Management (ASM)), le groupe de disques doit également être dédié aux fichiers de données.

Cette méthode d'isolement des fichiers de données permet de rétablir leur état antérieur sans endommager d'autres systèmes de fichiers.

Réserve Snapshot

Pour chaque volume contenant des données Oracle dans un environnement SAN, le `percent-snapshot-space` Doit être défini sur zéro car il n'est pas utile de réserver de l'espace pour un snapshot dans un environnement LUN. Si la réserve fractionnaire est définie sur 100, un snapshot d'un volume avec des LUN nécessite suffisamment d'espace libre dans le volume, à l'exception de la réserve Snapshot, pour absorber 100 % de CA de toutes les données. Si la réserve fractionnaire est définie sur une valeur inférieure, une quantité d'espace libre correspondante est nécessaire, mais elle exclut toujours la réserve snapshot. Cela signifie que l'espace de réserve du snapshot dans un environnement de LUN est gaspillé.

Dans un environnement NFS, deux options sont possibles :

- Réglez le `percent-snapshot-space` basé sur la consommation d'espace prévue du snapshot.
- Réglez le `percent-snapshot-space` pour zéro et gérer collectivement l'espace utilisé actif et snapshot.

Avec la première option, `percent-snapshot-space` est défini sur une valeur différente de zéro, généralement autour de 20 %. Cet espace est alors masqué par l'utilisateur. Toutefois, cette valeur ne crée pas de limite d'utilisation. Si une base de données avec une réservation de 20 % connaît un chiffre d'affaires de 30 %, l'espace snapshot peut dépasser les limites de la réserve de 20 % et occuper un espace non réservé.

Le principal avantage de la définition d'une réserve sur une valeur telle que 20 % est de vérifier qu'un peu d'espace est toujours disponible pour les snapshots. Par exemple, un volume de 1 To avec une réserve de 20 % permettrait uniquement à un administrateur de base de données (DBA) de stocker 800 Go de données. Cette configuration garantit au moins 200 Go d'espace pour la consommation de snapshots.

Quand `percent-snapshot-space` est défini sur zéro, tout l'espace du volume est disponible pour l'utilisateur final, ce qui offre une meilleure visibilité. L'administrateur de base de données doit comprendre que, s'il constate qu'un volume de 1 To exploite les snapshots, cet espace de 1 To est partagé entre les données actives et le renouvellement du Snapshot.

Il n'existe pas de préférence claire entre l'option 1 et l'option 2 parmi les utilisateurs finaux.

ONTAP et snapshots tiers

Oracle Doc ID 604683.1 décrit les conditions requises pour la prise en charge des snapshots tiers et les nombreuses options disponibles pour les opérations de sauvegarde et de restauration.

Les fournisseurs tiers doivent garantir la conformité de leurs snapshots à plusieurs exigences :

- Les snapshots doivent intégrer les opérations de restauration et de reprise recommandées par Oracle.
- Les snapshots doivent être cohérents après panne de la base de données au point du Snapshot.
- L'ordre d'écriture est conservé pour chaque fichier d'un snapshot.

Les produits de gestion Oracle de ONTAP et NetApp sont conformes à ces exigences.

SnapRestore

La technologie NetApp SnapRestore assure la restauration rapide des données dans ONTAP à partir d'une copie Snapshot.

Lorsqu'un dataset stratégique n'est pas disponible, les opérations stratégiques de l'entreprise ne sont pas disponibles. Les bandes peuvent se rompre, et même les restaurations à partir de sauvegardes sur disque peuvent être lentes à transférer sur le réseau. SnapRestore évite ces problèmes en offrant une restauration quasi instantanée des datasets. Même les bases de données de plusieurs pétaoctets peuvent être entièrement restaurées en quelques minutes à peine.

Il existe deux types d'SnapRestore : basés sur les fichiers/LUN et sur les volumes.

- Il est possible de restaurer des fichiers individuels ou des LUN en quelques secondes, qu'il s'agisse d'un LUN de 2 To ou d'un fichier de 4 Ko.
- Le conteneur de fichiers ou de LUN peut être restauré en quelques secondes, qu'il s'agisse de 10 Go ou 100 To de données.

Un « conteneur de fichiers ou de LUN » fait généralement référence à un volume FlexVol. Par exemple, vous pouvez avoir 10 LUN qui composent un groupe de disques LVM dans un seul volume, ou un volume peut stocker les home directories NFS de 1000 utilisateurs. Au lieu d'exécuter une opération de restauration pour chaque fichier ou LUN individuel, vous pouvez restaurer le volume entier en une seule opération. Ce processus fonctionne également avec des conteneurs scale-out qui incluent plusieurs volumes, tels qu'un FlexGroup ou un groupe de cohérence ONTAP.

La rapidité et l'efficacité de SnapRestore sont dues à la nature d'une copie Snapshot, qui offre essentiellement une vue en lecture seule parallèle du contenu d'un volume à un moment donné. Les blocs actifs sont les blocs réels qui peuvent être modifiés, tandis que le snapshot offre une vue en lecture seule de l'état des blocs qui

constituent les fichiers et les LUN au moment de la création du snapshot.

ONTAP permet uniquement un accès en lecture seule aux données instantanées, mais les données peuvent être réactivées avec SnapRestore. L'instantané est réactivé en tant que vue en lecture-écriture des données, renvoyant les données à leur état précédent. SnapRestore peut fonctionner au niveau du volume ou du fichier. La technologie est essentiellement la même avec quelques différences mineures de comportement.

SnapRestore du volume

La fonction SnapRestore basée sur les volumes renvoie la totalité du volume de données à un état antérieur. Cette opération ne nécessite pas de déplacement de données. Le processus de restauration est donc pratiquement instantané, bien que le traitement des opérations via l'API ou l'interface de ligne de commande puisse prendre quelques secondes. La restauration de 1 Go de données n'est pas plus compliquée et chronophage que la restauration de 1 po de données. Cette fonctionnalité est la principale raison pour laquelle de nombreux clients grands comptes migrent vers des systèmes de stockage ONTAP. Il assure un RTO se mesure en quelques secondes, même pour les datasets les plus volumineux.

L'un des inconvénients des SnapRestore sur volume est le fait que les modifications au sein d'un volume sont cumulées dans le temps. Par conséquent, chaque snapshot et les données de fichier actives dépendent des modifications apportées jusqu'à ce point. Le rétablissement d'un volume à un état antérieur implique la suppression de toutes les modifications ultérieures apportées aux données. Ce qui est moins évident, cependant, c'est qu'il s'agit d'instantanés créés par la suite. Ce n'est pas toujours souhaitable.

Par exemple, un SLA de conservation des données peut spécifier 30 jours de sauvegardes nocturnes. La restauration d'un dataset sur un snapshot créé il y a cinq jours avec SnapRestore du volume abandonnerait tous les snapshots créés les cinq jours précédents, en violation du SLA.

Un certain nombre d'options sont disponibles pour résoudre cette limitation :

1. Les données peuvent être copiées à partir d'un instantané précédent, au lieu d'effectuer une SnapRestore du volume entier. Cette méthode fonctionne mieux avec les jeux de données plus petits.
2. Un snapshot peut être cloné plutôt que restauré. La limitation à cette approche est que le snapshot source dépend du clone. Par conséquent, elle ne peut pas être supprimée si le clone n'est pas également supprimé ou s'il est divisé en volume indépendant.
3. Utilisation d'un SnapRestore basé sur des fichiers.

Fichier SnapRestore

SnapRestore basé sur les fichiers est un processus de restauration plus granulaire basé sur des snapshots. Au lieu de rétablir l'état d'un volume entier, l'état d'un fichier ou d'une LUN individuel est rétabli. Il n'est pas nécessaire de supprimer des snapshots et cette opération ne crée aucune dépendance vis-à-vis d'un instantané précédent. Le fichier ou la LUN est immédiatement disponible dans le volume actif.

Aucun déplacement des données n'est nécessaire lors de la restauration d'un fichier ou d'une LUN par SnapRestore. Cependant, des mises à jour internes des métadonnées sont nécessaires pour refléter le fait que les blocs sous-jacents d'un fichier ou d'une LUN existent désormais à la fois dans un snapshot et dans le volume actif. Les performances ne doivent pas être affectées, mais ce processus bloque la création de snapshots jusqu'à ce qu'elle soit terminée. Le taux de traitement est d'environ 5 Gbit/s (18 To/heure) en fonction de la taille totale des fichiers restaurés.

Sauvegardes en ligne

Deux datasets sont nécessaires pour protéger et restaurer une base de données Oracle

en mode de sauvegarde. Notez qu'il ne s'agit pas de la seule option de sauvegarde Oracle, mais qu'elle est la plus courante.

- Un Snapshot des fichiers de données en mode de sauvegarde
- Les journaux d'archivage créés pendant que les fichiers de données étaient en mode de sauvegarde

Si une récupération complète incluant toutes les transactions validées est requise, un troisième élément est requis :

- Les journaux de reprise en cours

Il existe plusieurs façons de restaurer une sauvegarde en ligne. De nombreux clients restaurent les snapshots à l'aide de l'interface de ligne de commande ONTAP, puis à l'aide d'Oracle RMAN ou de sqlplus pour terminer la restauration. Cette approche est particulièrement fréquente dans les environnements de production de grande taille. En effet, la probabilité et la fréquence des restaurations de bases de données sont extrêmement faibles et les restaurations sont gérées par un administrateur de bases de données qualifié. Pour une automatisation totale, des solutions telles que NetApp SnapCenter intègrent un plug-in Oracle avec une ligne de commande et des interfaces graphiques.

Certains grands clients ont adopté une approche plus simple en configurant des scripts de base sur les hôtes afin de placer les bases de données en mode de sauvegarde à un moment spécifique en préparation d'un snapshot planifié. Par exemple, planifiez la commande `alter database begin backup` à 23:58, `alter database end backup` à 00:02, puis planifiez les snapshots directement sur le système de stockage à minuit. Résultat : une stratégie de sauvegarde simple et hautement évolutive ne nécessite aucun logiciel ni licence externe.

Disposition des données

La disposition la plus simple consiste à isoler les fichiers de données dans un ou plusieurs volumes dédiés. Ils doivent être non contaminés par tout autre type de fichier. Cela permet de s'assurer que les volumes de fichiers de données peuvent être rapidement restaurés via une opération SnapRestore sans détruire un journal de reprise, un fichier de contrôle ou un journal d'archivage important.

LE SYSTÈME SAN présente des exigences similaires en matière d'isolation des fichiers de données dans des volumes dédiés. Avec un système d'exploitation tel que Microsoft Windows, un seul volume peut contenir plusieurs LUN de fichiers de données, chacune avec un système de fichiers NTFS. Avec d'autres systèmes d'exploitation, il existe généralement un gestionnaire de volumes logiques. Par exemple, avec Oracle ASM, l'option la plus simple consiste à limiter les LUN d'un groupe de disques ASM à un seul volume pouvant être sauvegardé et restauré en tant qu'unité. Si des volumes supplémentaires sont nécessaires pour des raisons de performance ou de gestion de la capacité, la création d'un groupe de disques supplémentaire sur le nouveau volume simplifie la gestion.

Si ces instructions sont respectées, les snapshots peuvent être planifiés directement sur le système de stockage sans avoir à créer de snapshot de groupe de cohérence. En effet, les sauvegardes Oracle ne nécessitent pas la sauvegarde simultanée de fichiers de données. La procédure de sauvegarde en ligne a été conçue pour assurer la mise à jour des fichiers de données, qui seront ensuite transmis progressivement sur bande en quelques heures.

Une complication se produit dans des situations telles que l'utilisation d'un groupe de disques ASM distribué sur des volumes. Dans ce cas, un snapshot de groupe de cohérence doit être réalisé pour s'assurer que les métadonnées ASM sont cohérentes sur tous les volumes constitutifs.

Attention : Vérifiez que l'ASM `spfile` et `passwd` les fichiers ne se trouvent pas dans le groupe de disques hébergeant les fichiers de données. Cela interfère avec la capacité à restaurer de manière sélective les

fichiers de données et uniquement les fichiers de données.

Procédure de restauration locale : NFS

Cette procédure peut être conduite manuellement ou via une application telle que SnapCenter. La procédure de base est la suivante :

1. Arrêtez la base de données.
2. Restaurez le ou les volumes de fichiers de données sur l'instantané immédiatement avant le point de restauration souhaité.
3. Réexécutez les journaux d'archivage au point souhaité.
4. Relire les journaux de reprise en cours si vous souhaitez effectuer une restauration complète.

Cette procédure suppose que les journaux d'archive souhaités sont toujours présents dans le système de fichiers actif. Si ce n'est pas le cas, les journaux d'archivage doivent être restaurés ou rman/sqlplus peut être dirigé vers les données du répertoire d'instantanés.

En outre, dans le cas de bases de données plus petites, l'utilisateur peut restaurer les fichiers de données directement à partir du système `.snapshot` répertoire n'ayant pas besoin des outils d'automatisation ou des administrateurs de stockage pour exécuter une `snaprestore` commande.

Procédure de restauration locale—SAN

Cette procédure peut être conduite manuellement ou via une application telle que SnapCenter. La procédure de base est la suivante :

1. Arrêtez la base de données.
2. Arrêter le ou les groupes de disques hébergeant les fichiers de données. La procédure varie en fonction du gestionnaire de volumes logiques choisi. Avec ASM, le processus nécessite de démonter le groupe de disques. Sous Linux, les systèmes de fichiers doivent être démontés et les volumes logiques et les groupes de volumes doivent être désactivés. L'objectif est d'arrêter toutes les mises à jour du groupe de volumes cible à restaurer.
3. Restaurez les groupes de disques de fichiers de données sur l'instantané immédiatement avant le point de restauration souhaité.
4. Réactivez les groupes de disques récemment restaurés.
5. Réexécutez les journaux d'archivage au point souhaité.
6. Relire tous les journaux de reprise si vous souhaitez procéder à une restauration complète.

Cette procédure suppose que les journaux d'archive souhaités sont toujours présents dans le système de fichiers actif. Si ce n'est pas le cas, les journaux d'archivage doivent être restaurés en mettant les LUN du journal d'archivage hors ligne et en effectuant une restauration. Il s'agit également d'un exemple dans lequel il est utile de diviser les journaux d'archivage en volumes dédiés. Si les journaux d'archivage partagent un groupe de volumes avec les journaux de reprise, les journaux de reprise doivent être copiés ailleurs avant la restauration de l'ensemble global des LUN. Cette étape empêche la perte de ces transactions finales enregistrées.

Sauvegardes optimisées pour les snapshots de stockage

La sauvegarde et la restauration basées sur des snapshots sont devenues encore plus simples au moment du lancement d'Oracle 12c. En effet, il n'est pas nécessaire de placer

une base de données en mode de sauvegarde à chaud. Il est possible de planifier des sauvegardes Snapshot directement sur un système de stockage et d'effectuer des restaurations complètes ou à un point dans le temps.

Les administrateurs de bases de données maîtrisent mieux la procédure de restauration à partir d'une sauvegarde à chaud, mais il est depuis longtemps possible d'utiliser des snapshots qui n'ont pas été créés pendant que la base de données était en mode de sauvegarde à chaud. Pour assurer la cohérence de la base de données, des étapes manuelles supplémentaires ont été nécessaires avec Oracle 10g et 11g. Avec Oracle 12c, `sqlplus` et `rman` contiennent la logique supplémentaire permettant de relire les journaux d'archivage sur des sauvegardes de fichiers de données qui n'étaient pas en mode de sauvegarde à chaud.

Comme nous l'avons vu précédemment, la restauration d'une sauvegarde à chaud basée sur des snapshots nécessite deux jeux de données :

- Un Snapshot des fichiers de données créés en mode de sauvegarde
- Les journaux d'archivage générés pendant que les fichiers de données étaient en mode de sauvegarde à chaud

Lors de la restauration, la base de données lit les métadonnées à partir des fichiers de données pour sélectionner les journaux d'archivage requis à des fins de restauration.

La restauration optimisée pour les snapshots de stockage nécessite des jeux de données légèrement différents pour obtenir les mêmes résultats :

- Un Snapshot des fichiers de données et une méthode d'identification de l'heure de création du Snapshot
- Archiver les journaux à partir de l'heure du point de contrôle du fichier de données le plus récent jusqu'à l'heure exacte du snapshot

Lors de la restauration, la base de données lit les métadonnées à partir des fichiers de données pour identifier le premier journal d'archivage requis. Il est possible d'effectuer une restauration complète ou instantanée. Lors de l'exécution d'une restauration à un point dans le temps, il est essentiel d'connaître l'heure du Snapshot des fichiers de données. Le point de restauration spécifié doit être après l'heure de création des snapshots. NetApp recommande d'ajouter au moins quelques minutes à l'heure du snapshot pour tenir compte des variations d'horloge.

Pour plus de détails, consultez la documentation d'Oracle sur la rubrique « Restauration à l'aide de l'optimisation des snapshots de stockage » disponible dans les différentes versions de la documentation d'Oracle 12c. Consultez également le document Oracle document ID Doc ID 604683.1 concernant la prise en charge des snapshots tiers par Oracle.

Disposition des données

La disposition la plus simple consiste à isoler les fichiers de données dans un ou plusieurs volumes dédiés. Ils doivent être non contaminés par tout autre type de fichier. Cela permet de s'assurer que les volumes de fichiers de données peuvent être rapidement restaurés lors d'une opération SnapRestore sans détruire un journal de reprise, un fichier de contrôle ou un journal d'archivage important.

LE SYSTÈME SAN présente des exigences similaires en matière d'isolation des fichiers de données dans des volumes dédiés. Avec un système d'exploitation tel que Microsoft Windows, un seul volume peut contenir plusieurs LUN de fichiers de données, chacune avec un système de fichiers NTFS. Avec d'autres systèmes d'exploitation, il existe généralement un gestionnaire de volumes logiques. Par exemple, avec Oracle ASM, l'option la plus simple consiste à limiter les groupes de disques à un volume unique pouvant être sauvegardé et restauré comme une unité. Si des volumes supplémentaires sont nécessaires pour des raisons de performance ou de gestion de la capacité, la création d'un groupe de disques supplémentaire sur le nouveau

volume simplifie la gestion.

Si ces instructions sont respectées, les snapshots peuvent être planifiés directement sur ONTAP sans avoir à créer de snapshot de groupe de cohérence. En effet, les sauvegardes optimisées pour les snapshots ne nécessitent pas la sauvegarde simultanée de fichiers de données.

Une complication se produit dans des situations telles qu'un groupe de disques ASM distribué sur des volumes. Dans ce cas, un snapshot de groupe de cohérence doit être réalisé pour s'assurer que les métadonnées ASM sont cohérentes sur tous les volumes constitutifs.

[Remarque]Vérifiez que les fichiers spfile et passwd ASM ne se trouvent pas dans le groupe de disques hébergeant les fichiers de données. Cela interfère avec la capacité à restaurer de manière sélective les fichiers de données et uniquement les fichiers de données.

Procédure de restauration locale : NFS

Cette procédure peut être conduite manuellement ou via une application telle que SnapCenter. La procédure de base est la suivante :

1. Arrêtez la base de données.
2. Restaurez le ou les volumes de fichiers de données sur l'instantané immédiatement avant le point de restauration souhaité.
3. Réexécutez les journaux d'archivage au point souhaité.

Cette procédure suppose que les journaux d'archive souhaités sont toujours présents dans le système de fichiers actif. Si ce n'est pas le cas, les journaux d'archive doivent être restaurés, ou `rman` ou `sqlplus` peut être dirigé vers les données dans le `.snapshot` répertoire.

En outre, dans le cas de bases de données plus petites, l'utilisateur peut restaurer les fichiers de données directement à partir du système `.snapshot` Répertoire n'ayant pas besoin des outils d'automatisation ou d'un administrateur du stockage pour exécuter une commande SnapRestore.

Procédure de restauration locale—SAN

Cette procédure peut être conduite manuellement ou via une application telle que SnapCenter. La procédure de base est la suivante :

1. Arrêtez la base de données.
2. Arrêter le ou les groupes de disques hébergeant les fichiers de données. La procédure varie en fonction du gestionnaire de volumes logiques choisi. Avec ASM, le processus nécessite de démonter le groupe de disques. Sous Linux, les systèmes de fichiers doivent être démontés et les volumes logiques et les groupes de volumes désactivés. L'objectif est d'arrêter toutes les mises à jour du groupe de volumes cible à restaurer.
3. Restaurez les groupes de disques de fichiers de données sur l'instantané immédiatement avant le point de restauration souhaité.
4. Réactivez les groupes de disques récemment restaurés.
5. Réexécutez les journaux d'archivage au point souhaité.

Cette procédure suppose que les journaux d'archive souhaités sont toujours présents dans le système de fichiers actif. Si ce n'est pas le cas, les journaux d'archivage doivent être restaurés en mettant les LUN du journal d'archivage hors ligne et en effectuant une restauration. Il s'agit également d'un exemple dans lequel il est utile de diviser les journaux d'archivage en volumes dédiés. Si les journaux d'archivage partagent un

groupe de volumes avec les journaux de reprise, les journaux de reprise doivent être copiés ailleurs avant la restauration de l'ensemble global de LUN afin d'éviter de perdre les transactions enregistrées finales.

Exemple de récupération complète

Supposons que les fichiers de données ont été corrompus ou détruits et qu'une restauration complète est requise. La procédure à suivre est la suivante :

```
[oracle@host1 ~]$ sqlplus / as sysdba
Connected to an idle instance.
SQL> startup mount;
ORACLE instance started.
Total System Global Area 1610612736 bytes
Fixed Size                  2924928 bytes
Variable Size            1040191104 bytes
Database Buffers          553648128 bytes
Redo Buffers               13848576 bytes
Database mounted.
SQL> recover automatic;
Media recovery complete.
SQL> alter database open;
Database altered.
SQL>
```

Exemple de restauration instantanée

Toute la procédure de restauration est une commande unique : `recover automatic`.

Si une restauration à un point dans le temps est requise, l'horodatage des snapshots doit être connu et peut être identifié comme suit :

```
Cluster01::> snapshot show -vserver vserver1 -volume NTAP_oradata -fields
create-time
vserver   volume        snapshot   create-time
--------  ------------  ---------  ------------------------
vserver1  NTAP_oradata  my-backup  Thu Mar 09 10:10:06 2017
```

L'heure de création de l'instantané est répertoriée comme 9 mars et 10:10:06. Pour être sûr, une minute est ajoutée à l'heure du snapshot :

```
[oracle@host1 ~]$ sqlplus / as sysdba
Connected to an idle instance.
SQL> startup mount;
ORACLE instance started.
Total System Global Area 1610612736 bytes
Fixed Size                  2924928 bytes
Variable Size            1040191104 bytes
Database Buffers          553648128 bytes
Redo Buffers               13848576 bytes
Database mounted.
SQL> recover database until time '09-MAR-2017 10:44:15' snapshot time '09-
MAR-2017 10:11:00';
```

La restauration est maintenant lancée. Il a spécifié une heure d'instantané de 10:11:00, une minute après l'heure enregistrée pour tenir compte de la variation d'horloge possible, et un temps de récupération cible de 10:44. Ensuite, sqlplus demande les journaux d'archivage requis pour atteindre le délai de restauration souhaité de 10:44.

```
ORA-00279: change 551760 generated at 03/09/2017 05:06:07 needed for
thread 1
ORA-00289: suggestion : /oralogs_nfs/arch/1_31_930813377.dbf
ORA-00280: change 551760 for thread 1 is in sequence #31
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
ORA-00279: change 552566 generated at 03/09/2017 05:08:09 needed for
thread 1
ORA-00289: suggestion : /oralogs_nfs/arch/1_32_930813377.dbf
ORA-00280: change 552566 for thread 1 is in sequence #32
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
ORA-00279: change 553045 generated at 03/09/2017 05:10:12 needed for
thread 1
ORA-00289: suggestion : /oralogs_nfs/arch/1_33_930813377.dbf
ORA-00280: change 553045 for thread 1 is in sequence #33
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
ORA-00279: change 753229 generated at 03/09/2017 05:15:58 needed for
thread 1
ORA-00289: suggestion : /oralogs_nfs/arch/1_34_930813377.dbf
ORA-00280: change 753229 for thread 1 is in sequence #34
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
Log applied.
Media recovery complete.
SQL> alter database open resetlogs;
Database altered.
SQL>
```

Restauration complète d'une base de données à l'aide de snapshots à l'aide de `recover automatic` la commande ne nécessite pas de licence spécifique, mais une restauration à un point dans le temps via `snapshot time` Requiert la licence Oracle Advanced compression.

Outils d'automatisation et de gestion de la base de données

Dans un environnement de base de données Oracle, la principale valeur de ONTAP provient des principales technologies ONTAP, telles que les copies Snapshot instantanées, la réplication simple SnapMirror et la création efficace de volumes FlexClone.

Dans certains cas, une configuration simple de ces fonctionnalités principales directement sur ONTAP répond aux exigences, mais les besoins plus complexes requièrent une couche d'orchestration.

SnapCenter

SnapCenter est le produit phare de la protection des données NetApp. À un niveau très bas, il est similaire aux produits SnapManager en termes d'exécution des sauvegardes de base de données, mais il a été conçu dès le départ pour proposer une gestion de la protection des données centralisée sur les systèmes de stockage NetApp.

SnapCenter inclut les fonctions de base telles que les sauvegardes et restaurations basées sur des snapshots, SnapMirror et la réplication SnapVault, ainsi que d'autres fonctionnalités nécessaires pour fonctionner à grande échelle pour les grandes entreprises. Ces fonctionnalités avancées incluent un contrôle d'accès basé sur des rôles (RBAC) étendu, des API RESTful pour l'intégration de produits d'orchestration tiers, une gestion centralisée et sans interruption des plug-ins SnapCenter sur des hôtes de base de données et une interface utilisateur conçue pour les environnements à l'échelle du cloud.

REPOS

ONTAP contient également un jeu d'API RESTful riche. Les fournisseurs tiers peuvent ainsi créer une application de protection des données et de gestion grâce à une intégration étroite avec ONTAP. De plus, l'API RESTful est facile à utiliser par les clients qui souhaitent créer leurs propres workflows et utilitaires d'automatisation.

Informations sur le copyright

Informations sur les marques commerciales