Protección de datos de Oracle

Enterprise applications

NetApp
February 10, 2026

Tabla de contenidos

Protección de datos de Oracle

Protección de datos con ONTAP

NetApp sabe que los datos más críticos se encuentran en las bases de datos.

Una empresa no puede operar sin acceso a sus datos y, a veces, los datos definen el negocio. Estos datos deben protegerse; sin embargo, la protección de datos no solo garantiza un backup utilizable; se trata de realizar backups de forma rápida y fiable, además de almacenarlos de forma segura.

El otro lado de la protección de datos es la recuperación de datos. Cuando no se puede acceder a los datos, la empresa se ve afectada y puede dejar de funcionar hasta que se restauren los datos. Este proceso debe ser rápido y fiable. Por último, la mayoría de las bases de datos deben protegerse frente a desastres, lo que significa mantener una réplica de la base de datos. La réplica debe estar lo suficientemente actualizada. También debe ser rápido y sencillo hacer de la réplica una base de datos completamente operativa.

Esta documentación sustituye al informe técnico *TR-4591 publicado anteriormente: Protección de datos de Oracle: Backup, recuperación y replicación.*

Planificación

La arquitectura de protección de datos empresariales adecuada depende de los requisitos empresariales relacionados con la retención de datos, la capacidad de recuperación y la tolerancia a interrupciones durante diversos eventos.

Por ejemplo, piense en el número de aplicaciones, bases de datos y conjuntos de datos importantes. Crear una estrategia de backup para un único conjunto de datos que garantice el cumplimiento de los acuerdos de nivel de servicio típicos es bastante sencillo, ya que no hay muchos objetos que gestionar. A medida que aumenta el número de conjuntos de datos, la supervisión se hace más complicada y los administradores pueden verse forzados a invertir cada vez más tiempo en solucionar los fallos de backup. A medida que un entorno llega al cloud y escala el proveedor de servicios, se necesita un enfoque totalmente diferente.

El tamaño del conjunto de datos también afecta a la estrategia. Por ejemplo, existen muchas opciones para backup y recuperación con una base de datos 100GB porque el conjunto de datos es tan pequeño. La simple copia de los datos de los medios de backup con herramientas tradicionales suele proporcionar un objetivo de tiempo de recuperación suficiente para la recuperación. Una base de datos de 100TB suele necesitar una estrategia completamente diferente a menos que el objetivo de tiempo de recuperación permita una interrupción de varios días, en cuyo caso puede ser aceptable un procedimiento tradicional de backup y recuperación basado en copia.

Por último, existen factores fuera del propio proceso de backup y recuperación. Por ejemplo, ¿existen bases de datos que respalden actividades de producción críticas, lo que convierte la recuperación en un evento raro que solo realizan los administradores de bases de datos cualificados? Alternativamente, ¿las bases de datos forman parte de un entorno de desarrollo de gran tamaño en el que la recuperación es una ocurrencia frecuente y gestionada por un EQUIPO de TECNOLOGÍA generalista?

Planificación de objetivos de tiempo, objetivos de punto de recuperación y acuerdos de nivel de servicio

ONTAP le permite adaptar con facilidad una estrategia de protección de datos de base de datos de Oracle a sus requisitos empresariales.

Entre estos requisitos se incluyen factores como la velocidad de recuperación, la pérdida de datos máxima permitida y las necesidades de retención de backup. El plan de protección de datos también debe tener en cuenta varios requisitos normativos para la retención y restauración de datos. Por último, deben tenerse en cuenta diferentes escenarios de recuperación de datos, que van desde la recuperación típica y previsible que se produce por errores de usuarios o aplicaciones hasta escenarios de recuperación de desastres que incluyen la pérdida completa de un sitio.

Los cambios pequeños en las políticas de protección y recuperación de datos pueden tener un efecto significativo en la arquitectura general de almacenamiento, respaldo y recuperación. Es crucial definir y documentar los estándares antes de comenzar a trabajar de diseño, para evitar complicar la arquitectura de protección de datos. Las funciones o niveles de protección innecesarios generan costes innecesarios y gastos generales de gestión, y un requisito que al principio se pasa por alto puede dirigir un proyecto en la dirección equivocada o requerir cambios de diseño de última hora.

Objetivo de tiempo de recuperación

El objetivo de tiempo de recuperación (RTO) define el tiempo máximo permitido para la recuperación de un servicio. Por ejemplo, una base de datos de recursos humanos podría tener un objetivo de tiempo de recuperación de 24 horas porque, si bien sería un inconveniente perder el acceso a estos datos durante la jornada laboral, la empresa aún puede seguir funcionando. Por el contrario, una base de datos que respalde el libro mayor general de un banco tendría un RTO medido en minutos o incluso segundos. Un RTO de cero no es posible, porque debe haber una manera de diferenciar entre una interrupción real del servicio y un evento rutinario, como un paquete de red perdido. Sin embargo, un objetivo de tiempo de recuperación de casi cero es un requisito típico.

Objetivo de punto de recuperación

El objetivo de punto de recuperación (RPO) define la pérdida de datos máxima tolerable. En muchos casos, el objetivo de punto de recuperación solo viene determinado por la frecuencia de las copias Snapshot o las actualizaciones de snapmirror.

En algunos casos, el objetivo de punto de recuperación puede hacerse más agresivo ya que protege de forma selectiva ciertos datos con mayor frecuencia. En un contexto de base de datos, el RPO suele ser una cuestión de cuántos datos de registro se pueden perder en una situación específica. En un escenario típico de recuperación en el que una base de datos está dañada debido a un error de producto o de usuario, el RPO debe ser cero, lo que significa que no debe haber pérdida de datos. El procedimiento de recuperación implica restaurar una copia anterior de los archivos de base de datos y, a continuación, volver a reproducir los archivos de registro para que el estado de la base de datos alcance el momento deseado. Los archivos de registro necesarios para esta operación ya deben estar en su lugar en la ubicación original.

En escenarios inusuales, los datos de registro pueden perderse. Por ejemplo, un ataque accidental o malintencionado `rm -rf *` de archivos de base de datos podría resultar en la eliminación de todos los datos. La única opción sería restaurar desde la copia de seguridad, incluidos los archivos de registro, y algunos datos inevitablemente se perderían. La única opción para mejorar el RPO en un entorno de backup tradicional sería realizar backups repetidos de los datos de registro. Sin embargo, esto tiene limitaciones debido al movimiento constante de datos y la dificultad de mantener un sistema de backup como un servicio en constante ejecución. Una de las ventajas de los sistemas de almacenamiento avanzados es la capacidad de proteger los datos frente a daños accidentales o malintencionados en los archivos para proporcionar, de este modo, un mejor objetivo de punto de recuperación sin transferir datos.

Recuperación tras siniestros

La recuperación tras desastres incluye la arquitectura de TI, las políticas y los procedimientos necesarios para recuperar un servicio en caso de desastre físico. Esto puede incluir inundaciones, incendios o personas que

actúen con intención maliciosa o negligente.

La recuperación ante desastres va más allá de un conjunto de procedimientos de recuperación. Se trata del proceso completo de identificar los diversos riesgos, de definir los requisitos de recuperación de datos y continuidad del servicio, y de proporcionar la arquitectura correcta con los procedimientos asociados.

Cuando se establecen requisitos de protección de datos, es fundamental diferenciar entre los requisitos típicos de RPO y RTO, así como los requisitos de RPO y RTO necesarios para la recuperación ante desastres. Algunos entornos de aplicaciones requieren un objetivo de punto de recuperación de cero y un objetivo de tiempo de recuperación de casi cero para situaciones de pérdida de datos, que van desde un error relativamente normal del usuario hasta un incendio que destruya un centro de datos. Sin embargo, estos altos niveles de protección tienen consecuencias administrativas y de costes.

En general, los requisitos de recuperación de datos sin desastre deben ser estrictos por dos motivos. En primer lugar, los errores en las aplicaciones y los errores de los usuarios que dañan los datos son previsibles hasta el punto de que son casi inevitables. En segundo lugar, no es difícil diseñar una estrategia de backup que proporcione un RPO de cero y un RTO bajo, siempre que el sistema de almacenamiento no esté destruido. No hay motivo para no abordar un riesgo significativo que sea fácil de solucionar, por lo que los objetivos de RPO y RTO para la recuperación local deben ser agresivos.

Los requisitos del objetivo de tiempo de recuperación ante desastres y del objetivo de punto de recuperación varían mucho más según la probabilidad de que se produzca un desastre y las consecuencias de la pérdida de datos o las interrupciones de un negocio. Los requisitos del objetivo de punto de recuperación y del objetivo de tiempo de recuperación deben basarse en las necesidades reales de la empresa, no en los principios generales. Deben explicar múltiples escenarios de desastre lógicos y físicos.

Desastres lógicos

Entre los desastres lógicos se encuentra la corrupción de datos causada por los usuarios, errores de la aplicación o del SO y mal funcionamiento del software. Los desastres lógicos también pueden incluir ataques maliciosos de terceros con virus o gusanos, o mediante la explotación de las vulnerabilidades de las aplicaciones. En estos casos, la infraestructura física permanece intacta, pero los datos subyacentes ya no son válidos.

Un tipo cada vez más común de desastre lógico se conoce como ransomware, en el que se utiliza un vector de ataque para cifrar los datos. El cifrado no daña los datos, pero no los hace disponibles hasta que se realiza el pago a un tercero. Un número cada vez mayor de empresas se dirigen específicamente a ataques de ransomware. Para esta amenaza, NetApp ofrece copias Snapshot a prueba de manipulaciones donde ni siquiera el administrador de almacenamiento puede cambiar los datos protegidos antes de la fecha de caducidad configurada.

Desastres físicos

Los desastres físicos incluyen la falla de los componentes de una infraestructura que supera sus capacidades de redundancia y dan lugar a una pérdida de datos o una prolongada pérdida de servicio. Por ejemplo, la protección RAID proporciona redundancia de unidades de disco y el uso de HBA proporciona redundancia de puertos FC y cables FC. Los errores de hardware de dichos componentes son previsibles y no afectan a la disponibilidad.

En un entorno empresarial, generalmente es posible proteger la infraestructura de todo un sitio con componentes redundantes hasta el punto en que el único escenario de desastre físico previsible es la pérdida completa del sitio. En ese caso, el plan de la recuperación ante desastres depende de la replicación entre sitios.

Protección de datos síncrona y asíncrona

En un mundo ideal, todos los datos se replicarían de forma sincrónica en sitios dispersos geográficamente. Dicha replicación no siempre es factible o incluso posible por varias razones:

- La replicación síncrona aumenta inevitablemente la latencia de escritura porque todos los cambios deben replicarse en ambas ubicaciones antes de que la aplicación o base de datos pueda continuar con el procesamiento. El efecto sobre el rendimiento resultante es a veces inaceptable, lo que descarta el uso del mirroring síncrono.
- Al aumentar la adopción del almacenamiento SSD del 100 %, es más probable que se note latencia de escritura adicional, ya que las expectativas de rendimiento incluyen cientos de miles de IOPS y latencia inferior al milisegundo. Para obtener todas las ventajas del uso del 100 % de las unidades SSD es necesario volver a analizar la estrategia de recuperación ante desastres.
- Los conjuntos de datos siguen creciendo en términos de bytes, generando retos que exigen un ancho de banda suficiente para sostener la replicación síncrona.
- Los conjuntos de datos también crecen en términos de complejidad, lo que genera retos con la gestión de la replicación síncrona a gran escala.
- Las estrategias basadas en cloud a menudo implican mayores distancias de replicación y latencia, lo que excluye aún más el uso del mirroring síncrono.

NetApp ofrece soluciones que incluyen replicación sincrónica para las exigencias de recuperación de datos más exigentes y soluciones asincrónicas que permiten un mejor rendimiento y flexibilidad. Además, la tecnología de NetApp se integra sin problemas con muchas soluciones de replicación de terceros, como Oracle DataGuard

Tiempo de retención

El aspecto final de una estrategia de protección de datos es el tiempo de retención, que puede variar drásticamente.

- Normalmente, se requieren 14 días de backups nocturnos en el sitio principal y 90 días de backups almacenados en un sitio secundario.
- Muchos clientes crean archivos trimestrales independientes almacenados en diferentes medios.
- Es posible que una base de datos constantemente actualizada no necesite datos históricos y que las copias de seguridad solo se conserven durante unos pocos días.
- Los requisitos normativos pueden requerir la capacidad de recuperación hasta el punto de cualquier transacción arbitraria en un periodo de 365 días.

Disponibilidad de bases de datos

ONTAP se ha diseñado para ofrecer la máxima disponibilidad de las bases de datos de Oracle. Este documento no incluye una descripción completa de las funciones de alta disponibilidad de ONTAP. Sin embargo, al igual que sucede con la protección de datos, un conocimiento básico de esta funcionalidad es importante cuando se diseña una infraestructura de base de datos.

Parejas de HA

La unidad básica de alta disponibilidad es el par de alta disponibilidad. Cada pareja contiene enlaces

redundantes para admitir la replicación de datos hacia NVRAM. NVRAM no es una caché de escritura. La RAM dentro de la controladora funciona como caché de escritura. El objetivo de la NVRAM es registrar temporalmente los datos como protección frente a un fallo inesperado del sistema. En este sentido, es similar a un redo log de base de datos.

Tanto la NVRAM como un redo log de base de datos se utilizan para almacenar datos rápidamente, lo que permite que los cambios en los datos se confirmen lo más rápidamente posible. La actualización de los datos persistentes en las unidades (o archivos de datos) no se realiza hasta más adelante durante un proceso denominado punto de control en las plataformas ONTAP y en la mayoría de las bases de datos. Ni los datos de NVRAM ni los registros de recuperación de bases de datos se leen durante las operaciones normales.

Si una controladora falla abruptamente, es posible que existan cambios pendientes almacenados en la NVRAM que aún no se hayan escrito en las unidades. La controladora asociada detecta el fallo, toma el control de las unidades y aplica los cambios requeridos que se han almacenado en NVRAM.

Toma de control y retorno al nodo primario

La toma de control y la devolución hace referencia al proceso de transferencia de la responsabilidad de los recursos de almacenamiento entre los nodos de un par de alta disponibilidad. La toma de control y el retorno al nodo primario tienen dos aspectos:

- Gestión de la conectividad de red que permite el acceso a las unidades
- Gestión de las unidades en sí

Las interfaces de red que admiten el tráfico CIFS y NFS están configuradas tanto con un directorio raíz como con una ubicación de recuperación tras fallos. Una toma de control incluye mover las interfaces de red a su directorio raíz temporal en una interfaz física ubicada en las mismas subredes que la ubicación original. Un retorno primario incluye mover las interfaces de red de vuelta a sus ubicaciones originales. El comportamiento exacto se puede ajustar según sea necesario.

Las interfaces de red que admiten protocolos de bloques SAN como iSCSI y FC no se reubican durante la toma de control y el retorno al nodo primario. En su lugar, los LUN se deben aprovisionar con rutas que incluyan un par de HA completo, lo que da como resultado una ruta primaria y una secundaria.

> También se pueden configurar rutas adicionales a controladoras adicionales para admitir la reubicación de datos entre nodos de un clúster más grande, pero esto no forma parte del proceso de alta disponibilidad.

El segundo aspecto de la toma de control y la restauración es la transferencia de la propiedad del disco. El proceso exacto depende de múltiples factores, incluyendo la razón de la toma de control/devolución y las opciones de la línea de comandos emitidas. El objetivo es realizar la operación de la manera más eficiente posible. Aunque parezca que el proceso general requiera varios minutos, el momento en el que la propiedad de la unidad se realiza la transición de nodo a nodo generalmente se puede medir en segundos.

Tiempo de toma de control

El host de I/O experimenta una breve pausa en I/O durante operaciones de toma de control y devolución; pero no debe producirse una interrupción en las aplicaciones en un entorno configurado correctamente. El proceso de transición real en el que se demora I/O suele medirse en segundos, pero el host puede requerir más tiempo para reconocer el cambio en las rutas de datos y volver a enviar las operaciones de I/O.

La naturaleza de la interrupción depende del protocolo:

- Una interfaz de red que admite problemas de tráfico NFS y CIFS una solicitud de Protocolo de resolución de direcciones (ARP) a la red después de la transición hacia una nueva ubicación física. Esto hace que los conmutadores de red actualicen sus tablas de direcciones de control de acceso a medios (MAC) y reanuden el procesamiento de E/S. Las interrupciones en el caso de toma de control y devolución planificadas suelen medirse en segundos y, en muchos casos, no se pueden detectar. Puede que algunas redes sean más lentas para reconocer completamente el cambio en la ruta de red y algunos sistemas operativos pueden poner en cola muchas E/S en muy poco tiempo que deben reintentarse. Esto puede ampliar el tiempo necesario para reanudar la actividad de I/O.
- Una interfaz de red que admite protocolos SAN no realiza la transición a una nueva ubicación. Un SO host debe cambiar la ruta o las rutas en uso. La pausa en I/O observada por el host depende de varios factores. Desde el punto de vista de un sistema de almacenamiento, el período en el que no se puede ofrecer I/O es solo unos segundos. Sin embargo, los sistemas operativos de host diferentes pueden requerir más tiempo para permitir que se agote el tiempo de espera de una E/S antes de volver a intentarlo. Los sistemas operativos más nuevos son más capaces de reconocer un cambio de ruta mucho más rápido, pero los sistemas operativos más antiguos normalmente requieren hasta 30 segundos para reconocer un cambio.

En la siguiente tabla, se muestran los tiempos de toma de control esperados durante el que el sistema de almacenamiento no puede ofrecer datos a un entorno de aplicación. No debe haber ningún error en ningún entorno de aplicación, la toma de control debería aparecer como una breve pausa en el procesamiento de E/S.

	NFS	AFF	ASA
Toma de control planificada	15 seg	6-10 seg	2-3 seg
Respaldo no planificado	30 seg	6-10 seg	2-3 seg

Sumas de comprobación e integridad de los datos

ONTAP y sus protocolos admitidos incluyen varias funciones que protegen la integridad de las bases de datos de Oracle, incluidos los datos en reposo y la transmisión de datos a través de la red.

La protección de datos lógicos en ONTAP consta de tres requisitos clave:

- Los datos deben protegerse contra la corrupción de datos.
- Los datos deben protegerse contra un fallo de unidad.
- Los cambios en los datos deben protegerse contra la pérdida.

Estas tres necesidades se tratan en las siguientes secciones.

Corrupción de la red: Sumas de comprobación

El nivel más básico de protección de datos es la suma de comprobación, que es un código especial de detección de errores almacenado junto con los datos. La corrupción de datos durante la transmisión de red se detecta con el uso de una suma de comprobación y, en algunos casos, varias sumas de comprobación.

Por ejemplo, una trama de FC incluye una forma de suma de comprobación denominada comprobación de redundancia cíclica (CRC) para asegurarse de que la carga útil no está dañada en tránsito. El transmisor envía tanto los datos como el CRC de los datos. El receptor de una trama FC vuelve a calcular el CRC de los

datos recibidos para asegurarse de que coincida con el CRC transmitido. Si el CRC recién calculado no coincide con el CRC conectado a la trama, los datos están dañados y se descarta o rechaza la trama de FC. Las operaciones de I/O iSCSI incluyen sumas de comprobación en las capas TCP/IP y Ethernet y, para una protección adicional, también se puede incluir protección CRC opcional en la capa SCSI. Cualquier daño de bit en el cable se detecta mediante la capa TCP o la capa IP, lo que provoca la retransmisión del paquete. Al igual que con FC, los errores en el CRC de SCSI provocan un descarte o el rechazo de la operación.

Daños en unidades: Sumas de comprobación

También se utilizan sumas de comprobación para verificar la integridad de los datos almacenados en las unidades. Los bloques de datos escritos en las unidades se almacenan con una función de suma de comprobación que genera un número impredecible ligado a los datos originales. Cuando se leen datos de la unidad, la suma de comprobación se vuelve a calcular y se compara con la suma de comprobación almacenada. Si no coincide, los datos se han dañado y deben ser recuperados por la capa RAID.

Datos dañados: Escrituras perdidas

Uno de los tipos de daños más difíciles de detectar es una escritura perdida o ubicada incorrectamente. Cuando se reconoce una escritura, se debe escribir en el soporte en la ubicación correcta. Los datos dañados in situ son relativamente fáciles de detectar usando una sencilla suma de comprobación almacenada con los datos. Sin embargo, si la escritura simplemente se pierde, es posible que aún exista la versión anterior de los datos y la suma de comprobación sea correcta. Si la escritura se realiza en una ubicación física incorrecta, la suma de comprobación asociada sería una vez más válida para los datos almacenados, aunque la escritura haya destruido otros datos.

La solución a este reto es la siguiente:

- Una operación de escritura debe incluir metadatos que indiquen la ubicación donde se espera que se encuentre la escritura.
- Una operación de escritura debe incluir algún tipo de identificador de versión.

Cuando ONTAP escribe un bloque, incluye los datos donde pertenece el bloque. Si una lectura posterior identifica un bloque, pero los metadatos indican que pertenece a la ubicación 123 cuando se encontró en la ubicación 456, la escritura se ha colocado de forma incorrecta.

Detectar una escritura totalmente perdida es más difícil. La explicación es muy complicada, pero básicamente ONTAP almacena los metadatos de manera que una operación de escritura da como resultado actualizaciones en dos ubicaciones distintas en las unidades. Si se pierde una escritura, una lectura posterior de los datos y los metadatos asociados muestra dos identidades de versión diferentes. Esto indica que la unidad no completó la escritura.

Los daños en la escritura perdidos o mal ubicados son extremadamente raros, pero, a medida que las unidades siguen creciendo y los conjuntos de datos pasan a la escala de exabytes, el riesgo aumenta. La detección de escritura perdida debe incluirse en cualquier sistema de almacenamiento que admita cargas de trabajo de base de datos.

Fallos de unidad: RAID, RAID DP y RAID-TEC

Si se detecta que un bloque de datos en una unidad está dañado, o que toda la unidad falla y no está totalmente disponible, los datos deben reconstituirse. Esto se realiza en ONTAP utilizando unidades de paridad. Los datos se dividen entre varias unidades de datos y, a continuación, se generan datos de paridad. Se almacena por separado de los datos originales.

ONTAP utilizó originalmente RAID 4, que utiliza una sola unidad de paridad para cada grupo de unidades de

datos. El resultado fue que cualquier unidad del grupo podría fallar sin producir una pérdida de datos. Si se produjo un error en la unidad de paridad, no se dañaron los datos y se pudo construir una nueva unidad de paridad. Si falla una unidad de datos única, las unidades restantes podrían usarse con la unidad de paridad para volver a generar los datos ausentes.

Cuando las unidades eran pequeñas, la posibilidad estadística de que fallaran en dos unidades a la vez era insignificante. A medida que aumenta la capacidad de las unidades, también aumenta el tiempo necesario para reconstruir los datos tras un fallo de unidad. Esto ha aumentado el intervalo en el que un segundo fallo de unidad provocaría la pérdida de datos. Además, el proceso de recompilación crea una gran cantidad de I/O adicionales en las unidades supervivientes. A medida que las unidades envejecen, también aumenta el riesgo de la carga adicional que produce un segundo fallo de unidad. Por último, incluso si el riesgo de pérdida de datos no aumentara con el uso continuado de RAID 4, las consecuencias de la pérdida de datos serían más graves. Cuantos más datos se pierdan en caso de un fallo de un grupo RAID, más tiempo se necesitaría para recuperar los datos, lo que prolonga la interrupción del negocio.

Estos problemas llevaron a NetApp a desarrollar la tecnología NetApp RAID DP, una variante de RAID 6. Esta solución incluye dos unidades de paridad, lo que significa que dos unidades cualesquiera de un grupo RAID pueden fallar sin crear pérdida de datos. El tamaño de las unidades ha continuado creciendo, lo que finalmente llevó a NetApp a desarrollar la tecnología NetApp RAID-TEC, que introduce una tercera unidad de paridad.

Algunas mejores prácticas históricas de bases de datos recomiendan el uso de RAID-10, también conocido como mirroring segmentado. Esto ofrece menos protección de datos que RAID DP, ya que existen varias situaciones de fallo de dos discos, mientras que en RAID DP no hay ninguna.

También hay algunas mejores prácticas históricas de bases de datos que indican que se prefiere RAID-10 a las opciones de RAID-4/5/6 debido a cuestiones de rendimiento. En ocasiones, estas recomendaciones se refieren a una penalización de RAID. Aunque estas recomendaciones son generalmente correctas, no son aplicables a las implementaciones de RAID en ONTAP. El problema de rendimiento está relacionado con la regeneración de paridad. Con las implementaciones de RAID tradicionales, procesar las escrituras aleatorias rutinarias realizadas por una base de datos requiere varias lecturas de disco para regenerar los datos de paridad y completar la escritura. La penalización se define como las IOPS de lectura adicional necesarias para ejecutar operaciones de escritura.

ONTAP no incurre en una penalización de RAID, ya que las escrituras se almacenan en memoria donde se genera la paridad y se escriben en el disco como una única franja de RAID. No se requieren lecturas para completar la operación de escritura.

En resumen, en comparación con RAID 10, RAID DP y RAID-TEC ofrecen mucha más capacidad utilizable, una mejor protección ante fallos de unidad y sin sacrificios de rendimiento.

Protección contra fallos del hardware: NVRAM

Cualquier cabina de almacenamiento que sirva a una carga de trabajo de base de datos debe procesar operaciones de escritura lo más rápido posible. Además, una operación de escritura debe protegerse contra pérdidas provocadas por eventos inesperados, como un fallo de alimentación. Esto significa que cualquier operación de escritura debe almacenarse de forma segura en al menos dos ubicaciones.

Los sistemas AFF y FAS confían en NVRAM para cumplir estos requisitos. El proceso de escritura funciona de la siguiente manera:

1. Los datos de escritura entrantes se almacenan en la RAM.
2. Los cambios que se deben realizar en los datos del disco se registran en NVRAM en el nodo local y el asociado. NVRAM no es una caché de escritura, sino un diario similar a un redo log de base de datos. En

condiciones normales, no se lee. Solo se utiliza para recuperación, como después de un fallo de alimentación durante el procesamiento de I/O.

3. A continuación, la escritura se reconoce en el host.

El proceso de escritura en esta fase se completa desde el punto de vista de la aplicación y los datos están protegidos contra pérdidas debido a que están almacenados en dos ubicaciones diferentes. Eventualmente, los cambios se escriben en el disco, pero este proceso es fuera de banda desde el punto de vista de la aplicación, porque se produce una vez que se reconoce la escritura y, por lo tanto, no afecta a la latencia. Este proceso es una vez más similar al registro de la base de datos. Un cambio en la base de datos se registra en los redo logs lo antes posible y el cambio se confirma como confirmado. Las actualizaciones de los archivos de datos se producen mucho más tarde y no afectan directamente a la velocidad de procesamiento.

En caso de que se produzca un fallo en la controladora, la controladora asociada toma la propiedad de los discos necesarios y reproduce los datos registrados en la NVRAM para recuperar las operaciones de I/O que estuvieran en curso al producirse el fallo.

Protección contra fallos de hardware: NVFAIL

Como hemos visto anteriormente, la escritura no se reconoce hasta que se haya iniciado sesión en la NVRAM local y NVRAM en al menos otra controladora. Este método garantiza que un fallo de hardware o una interrupción del suministro eléctrico no provoquen la pérdida de operaciones de I/O en tránsito Si la NVRAM local falla o la conectividad con el partner de alta disponibilidad falla, estos datos en curso ya no se duplicarán.

Si la NVRAM local informa de un error, el nodo se apaga. Este apagado hace que se produzca una conmutación al nodo de respaldo con una controladora asociada de alta disponibilidad. No se pierden datos porque la controladora que experimenta el fallo no reconoció la operación de escritura.

ONTAP no permite una conmutación por error cuando los datos no están sincronizados a menos que se vean obligados a recurrir a la conmutación por error. Al forzar un cambio en las condiciones de esta manera, se reconoce que los datos podrían dejarse atrás en la controladora original y que la pérdida de datos es aceptable.

Las bases de datos son especialmente vulnerables a los daños si se fuerza una conmutación por error porque las bases de datos mantienen grandes cachés internos de datos en el disco. Si se produce una conmutación por error forzada, los cambios previamente aceptados se descartan efectivamente. El contenido de la cabina de almacenamiento retrocede efectivamente en el tiempo y el estado de la caché de base de datos ya no refleja el estado de los datos del disco.

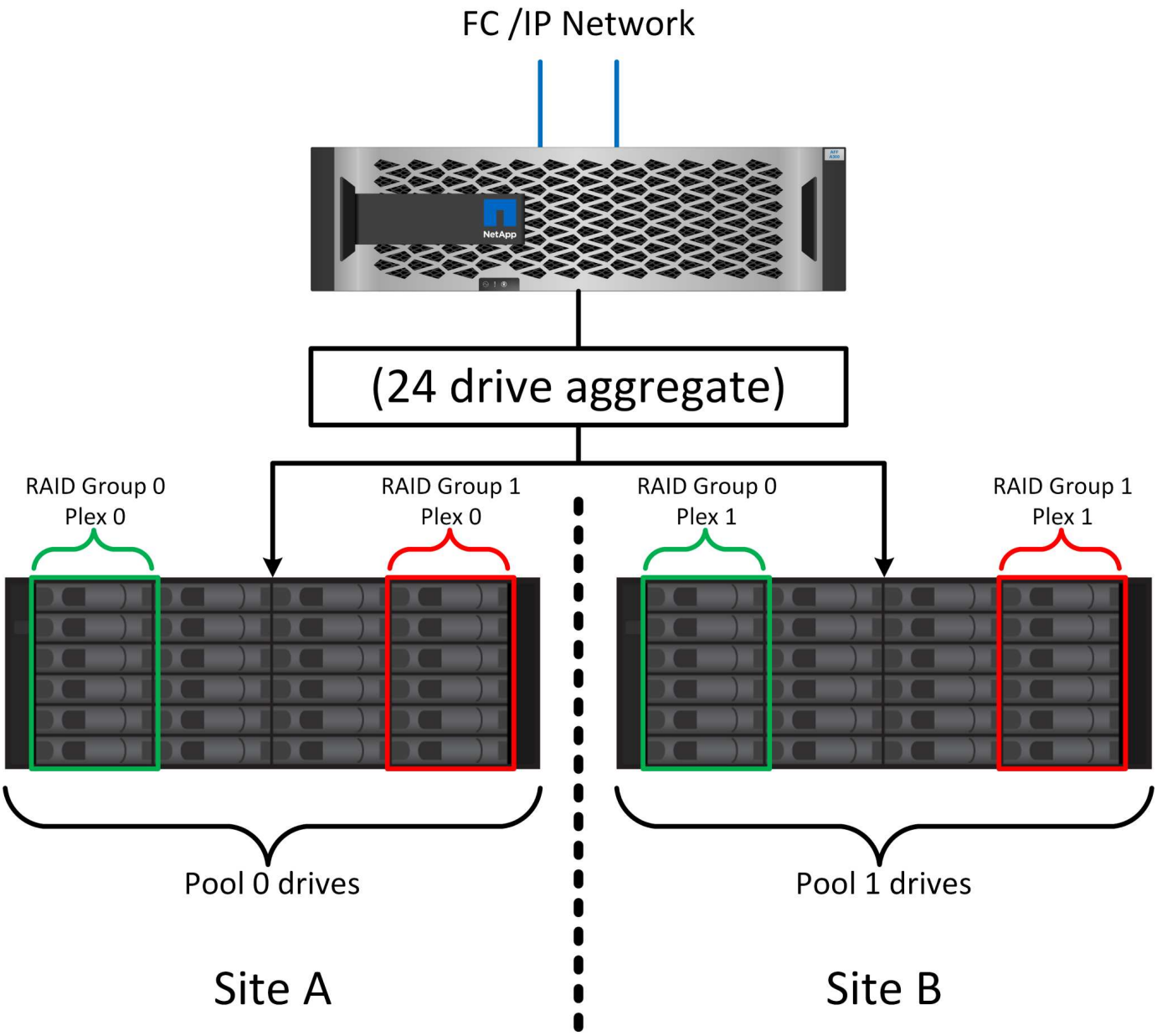
Para proteger datos contra esta situación, ONTAP permite configurar volúmenes para una protección especial contra un fallo NVRAM. Cuando se activa, este mecanismo de protección hace que un volumen entre en un estado denominado NVFAIL. Este estado provoca errores de I/O que provocan el cierre de una aplicación para que no utilicen datos obsoletos. No se deben perder los datos porque debe haber alguna escritura reconocida en la cabina de almacenamiento.

Los siguientes pasos habituales son para que un administrador apague completamente los hosts antes de volver a poner manualmente los LUN y los volúmenes de nuevo en línea. Aunque estos pasos pueden implicar cierto trabajo, este enfoque es la manera más segura de garantizar la integridad de los datos. No todos los datos requieren esta protección, por lo que el comportamiento NVFAIL se puede configurar volumen por volumen.

Protección frente a fallos de sitios y bandejas: SyncMirror y complejos

SyncMirror es una tecnología de mirroring que mejora, pero no sustituye, RAID DP ni RAID-TEC. Refleja el contenido de dos grupos RAID independientes. La configuración lógica es la siguiente:

- Las unidades se configuran en dos pools según la ubicación. Un pool se compone de todas las unidades en el sitio A, y el segundo pool se compone de todas las unidades en el sitio B.
- A continuación, se crea un pool de almacenamiento común, conocido como agregado, basado en conjuntos reflejados de grupos RAID. Se extrae un número igual de unidades en cada sitio. Por ejemplo, un agregado SyncMirror de 20 unidades estaría compuesto por 10 unidades del sitio A y 10 unidades del sitio B.
- Cada conjunto de unidades en un sitio determinado se configura automáticamente como uno o varios grupos RAID-DP o RAID-TEC completamente redundantes, independientemente del uso del mirroring. Esto proporciona una protección de datos continua, incluso después de la pérdida de un sitio.



La figura anterior muestra una configuración de SyncMirror de ejemplo. Se creó un agregado de 24 unidades en la controladora con 12 unidades de una bandeja asignada en el sitio A y 12 unidades de una bandeja asignada en el sitio B. Las unidades se agruparon en dos grupos RAID reflejados. RAID Group 0 incluye un plex de 6 unidades en el sitio A duplicado en un plex de 6 unidades en el sitio B. Del mismo modo, RAID Group 1 incluye un plex de 6 unidades en el sitio A duplicado en un plex de 6 unidades en el sitio B.

Normalmente, SyncMirror se utiliza para proporcionar mirroring remoto con sistemas MetroCluster, con una copia de los datos de cada sitio. En ocasiones, se ha utilizado para proporcionar un nivel adicional de redundancia en un único sistema. En particular, proporciona redundancia a nivel de bandeja. Una bandeja de unidades ya contiene fuentes de alimentación y controladoras duales y en general es poco más que chapa metálica, pero en algunos casos, la protección adicional puede estar garantizada. Por ejemplo, un cliente de NetApp ha puesto en marcha SyncMirror para una plataforma móvil de análisis en tiempo real que se usa durante las pruebas de automoción. El sistema se separó en dos racks físicos alimentados por fuentes de alimentación independientes de sistemas UPS independientes.

Sumas de comprobación

El tema de las sumas de comprobación es de particular interés para los administradores de bases de datos que están acostumbrados a usar backups en streaming de Oracle RMAN, que migran a backups basados en instantáneas. Una función de RMAN es que realiza comprobaciones de integridad durante las operaciones de copia de seguridad. Aunque esta función posee cierto valor, su principal ventaja es en una base de datos que no se utiliza en una cabina de almacenamiento moderna. Cuando se utilizan unidades físicas en una base de datos de Oracle, resulta casi seguro que los daños eventualmente se producen cuando las unidades envejecen, un problema que resuelven las sumas de comprobación basadas en cabinas de almacenamiento reales.

Con una cabina de almacenamiento real, la integridad de los datos se protege utilizando sumas de comprobación en varios niveles. Si los datos están dañados en una red basada en IP, la capa Protocolo de control de transmisión (TCP) rechaza los datos del paquete y solicita la retransmisión. El protocolo FC incluye sumas de comprobación, al igual que los datos SCSI encapsulados. Después de que se encuentra en la cabina, ONTAP tiene protección RAID y suma de comprobación. La corrupción puede ocurrir, pero, como en la mayoría de las matrices empresariales, se detecta y corrige. Normalmente, falla una unidad completa, solicita una reconstrucción de RAID y la integridad de la base de datos no se ve afectada. Todavía es posible que los bytes individuales en una unidad sean dañados por la radiación cósmica o las células flash que fallan. Si esto sucede, se producirá un error en la comprobación de paridad, se producirá un error en la unidad y se iniciará la recompilación de RAID. Una vez más, la integridad de los datos no se ve afectada. La última línea de defensa es el uso de sumas de control. Si, por ejemplo, un error catastrófico de firmware en una unidad daña datos que de algún modo no se detectó mediante una comprobación de paridad de RAID, la suma de comprobación no coincidiría y ONTAP evitaría la transferencia de un bloque dañado antes de que la base de datos de Oracle pudiera recibirlo.

La arquitectura de archivo de datos y redo log de Oracle también está diseñada para ofrecer el nivel más alto posible de integridad de datos, incluso en circunstancias extremas. En el nivel más básico, los bloques de Oracle incluyen suma de comprobación y comprobaciones lógicas básicas con casi todas las E/S. Si Oracle no se ha bloqueado o ha puesto un tablespace fuera de línea, los datos estarán intactos. El grado de comprobación de la integridad de los datos es ajustable y Oracle también puede configurarse para confirmar las escrituras. Como resultado, casi todos los escenarios de accidente y fallo se pueden recuperar, y en el caso extremadamente raro de una situación irrecuperable, la corrupción se detecta rápidamente.

La mayoría de los clientes de NetApp que utilizan bases de datos Oracle interrumpen el uso de RMAN y otros productos de backup después de la migración a backups basados en snapshots. Todavía hay opciones en las que se puede utilizar RMAN para realizar la recuperación a nivel de bloque con SnapCenter. Sin embargo, en el día a día, RMAN, NetBackup y otros productos sólo se utilizan ocasionalmente para crear copias de archivado mensuales o trimestrales.

Algunos clientes eligen correr `dbv` periódicamente para realizar comprobaciones de integridad de sus bases de datos existentes. NetApp desaconseja esta práctica porque crea una carga de I/O innecesaria. Como se mencionó anteriormente, si la base de datos no estaba experimentando problemas anteriormente, la posibilidad de `dbv` La detección de un problema es cercana a cero, y esta utilidad crea una carga secuencial de I/O muy elevada en la red y el sistema de almacenamiento. A menos que exista un motivo para creer que

existe corrupción, como la exposición a un bug de Oracle conocido, no hay motivo para ejecutarse `dbv`.

Conceptos básicos de backup y recuperación

Backups basados en Snapshot

La base de la protección de datos de bases de datos de Oracle en ONTAP es la tecnología Snapshot de NetApp.

Los valores clave son los siguientes:

- **Simplicidad.** Una instantánea es una copia de solo lectura del contenido de un contenedor de datos en un momento específico.
- **Eficiencia.** Las instantáneas no requieren espacio en el momento de la creación. El espacio solo se consume cuando se modifican los datos.
- **Capacidad de gestión.** Una estrategia de copia de seguridad basada en instantáneas es fácil de configurar y administrar porque las instantáneas son una parte nativa del sistema operativo de almacenamiento. Si el sistema de almacenamiento está encendido, está listo para crear backups.
- **Escalabilidad.** Se pueden conservar hasta 1024 copias de seguridad de un único contenedor de archivos y LUN. En el caso de conjuntos de datos complejos, es posible proteger varios contenedores de datos con un único conjunto coherente de copias Snapshot.
- El rendimiento no se ve afectado, independientemente de que un volumen contenga 1024 snapshots o ninguna.

Aunque muchos proveedores de almacenamiento ofrecen tecnología Snapshot, la tecnología Snapshot dentro de ONTAP es única y ofrece beneficios importantes para los entornos de aplicaciones y bases de datos empresariales:

- Las copias Snapshot forman parte del sistema de archivos WAFL (Write-Anywhere File Layout) subyacente. No son una tecnología complementaria ni externa. Esto simplifica la gestión, ya que el sistema de almacenamiento es el sistema de backup.
- Las copias Snapshot no afectan al rendimiento, a excepción de algunos casos periféricos como cuando se almacenan tantos datos en copias snapshot que el sistema de almacenamiento subyacente llena.
- El término «grupo de coherencia» se utiliza a menudo para referirse a una agrupación de objetos de almacenamiento que se gestionan como una colección consistente de datos. Una Snapshot de un volumen ONTAP determinado constituye un backup de grupo de coherencia.

Las copias Snapshot de ONTAP también ofrecen una escalabilidad mejor que la tecnología de la competencia. Los clientes pueden almacenar 5, 50 o 500 copias Snapshot sin que esto afecte al rendimiento. El número máximo de snapshots que se permite actualmente en un volumen es 1024. Si se requiere más retención de instantáneas, existen opciones para configurar las instantáneas en cascada a volúmenes adicionales.

Como resultado, proteger un conjunto de datos alojado en ONTAP es sencillo y altamente escalable. Los backups no requieren el traslado de datos, por lo que puede adaptarse a las necesidades del negocio en lugar de a las limitaciones de las tasas de transferencia de red, un gran número de unidades de cinta o áreas de almacenamiento provisional de discos.

¿Una snapshot es un backup?

Una pregunta frecuente acerca del uso de las copias Snapshot como estrategia de protección de datos es el hecho de que los datos «reales» y los datos de copias Snapshot se encuentran en las mismas unidades. La

pérdida de esas unidades provocaría la pérdida de los datos primarios y el backup.

Este es un problema válido. Los snapshots locales se usan para necesidades de backup y recuperación diarias y, en ese sentido, la snapshot es un backup. Cerca del 99 % de todos los escenarios de recuperación en entornos NetApp utilizan copias Snapshot para satisfacer incluso los requisitos de objetivo de tiempo de recuperación más agresivos.

Sin embargo, las copias Snapshot locales nunca deberían ser la única estrategia de backup, por lo que NetApp ofrece tecnología como la replicación de SnapMirror y SnapVault para replicar de forma rápida y eficiente copias Snapshot en un conjunto de unidades independiente. En una solución correctamente diseñada con copias Snapshot y replicación Snapshot, el uso de la cinta puede minimizarse tal vez a un archivo trimestral o eliminarse totalmente.

Backups basados en Snapshot

Existen muchas opciones para usar las copias Snapshot de ONTAP para proteger los datos, y las copias Snapshot son la base de muchas otras funciones de ONTAP, como replicación, recuperación ante desastres y clonación. Una descripción completa de la tecnología de instantáneas está fuera del alcance de este documento, pero en las siguientes secciones se proporciona una descripción general.

Existen dos métodos principales para crear una copia Snapshot de un conjunto de datos:

- Backups coherentes con los fallos
- Backups para aplicaciones

Un backup coherente con los fallos de un conjunto de datos hace referencia a la captura de toda la estructura del conjunto de datos en un único punto de tiempo. Si el conjunto de datos se almacena en un único volumen, el proceso es sencillo; se puede crear una copia Snapshot en cualquier momento. Si un conjunto de datos abarca volúmenes, es necesario crear una snapshot de grupo de coherencia (CG). Existen varias opciones para crear snapshots de CG, como el software NetApp SnapCenter, funciones nativas del grupo de coherencia ONTAP y scripts que se mantienen por el usuario.

Los backups coherentes con los fallos se utilizan principalmente cuando la recuperación punto del backup es suficiente. Cuando se necesita una recuperación más granular, por lo general se necesitan backups coherentes con las aplicaciones.

A menudo, la palabra «consistente» en «coherente con las aplicaciones» resulta una denominación errónea. Por ejemplo, colocar una base de datos de Oracle en modo de backup se denomina backup coherente con las aplicaciones, pero los datos no se hacen coherentes ni se ponen en modo inactivo de ninguna forma. Los datos siguen cambiando durante el backup. Por el contrario, la mayoría de los backups de MySQL y Microsoft SQL Server realmente ralentizan los datos antes de ejecutar el backup. VMware puede o no hacer que ciertos archivos sean consistentes.

Grupos de consistencia

El término «grupo de coherencia» hace referencia a la capacidad de una cabina de almacenamiento para gestionar varios recursos de almacenamiento como una sola imagen. Por ejemplo, una base de datos puede consistir en 10 LUN. La cabina debe ser capaz de realizar backup, restaurar y replicar esos 10 LUN de forma coherente. La restauración no es posible si las imágenes de las LUN no eran consistentes en el punto de backup. Para replicar estos 10 LUN es necesario que todas las réplicas estén perfectamente sincronizadas entre sí.

El término «grupo de coherencia» no se utiliza con frecuencia cuando se habla de ONTAP, porque la coherencia siempre ha sido una función básica del volumen y de la arquitectura de agregado en ONTAP. Muchas otras cabinas de almacenamiento gestionan LUN o sistemas de archivos como unidades individuales.

Podrían configurarse opcionalmente como «grupo de consistencia» para fines de protección de datos, pero este es un paso adicional en la configuración.

ONTAP siempre ha podido capturar imágenes de datos replicadas y locales coherentes. Aunque los distintos volúmenes de un sistema ONTAP no suelen describirse formalmente como un grupo de coherencia, eso es lo que son. Una copia Snapshot de ese volumen es una imagen de grupo de coherencia, la restauración de esa copia Snapshot es una restauración de grupo de coherencia, y tanto SnapMirror como SnapVault ofrecen replicación de grupo de coherencia.

Snapshots de grupo de coherencia

Las snapshots de grupo de consistencia (cg-snapshots) son una extensión de la tecnología Snapshot básica de ONTAP. Una operación Snapshot estándar crea una imagen coherente de todos los datos dentro de un único volumen, pero a veces es necesario crear un conjunto coherente de instantáneas en varios volúmenes e incluso entre varios sistemas de almacenamiento. El resultado es un conjunto de instantáneas que se pueden utilizar de la misma manera que una instantánea de un solo volumen individual. Se pueden utilizar para la recuperación de datos locales, replicar para la recuperación ante desastres o clonar como una única unidad coherente.

El mayor uso conocido de cg-snapshots es para un entorno de base de datos de aproximadamente 1PB GB de tamaño que abarca 12 controladoras. Las cg-snapshots creadas en este sistema se han utilizado para backup, recuperación y clonado.

La mayoría de las veces, cuando un conjunto de datos abarca volúmenes y se debe conservar el orden de escritura, el software de gestión elegido utiliza automáticamente una instantánea de cg. No es necesario comprender los detalles técnicos de cg-snapshots en estos casos. No obstante, hay situaciones en las que los complejos requisitos de protección de datos requieran un control detallado del proceso de protección y replicación de datos. Los flujos de trabajo de automatización o el uso de scripts personalizados para llamar a las API de cg-snapshot son algunas de las opciones. Para comprender la mejor opción y el rol de cg-snapshot se requiere una explicación más detallada de la tecnología.

La creación de un conjunto de cg-snapshots es un proceso de dos pasos:

1. Establezca el aislamiento de escritura en todos los volúmenes de destino.
2. Crear snapshots de dichos volúmenes mientras se encuentra en estado protegido.

El cercado de escritura se establece en serie. Esto significa que, a medida que se configura el proceso de barrera en varios volúmenes, las operaciones de I/O de escritura se congelan en el primer volumen de la secuencia, a medida que sigue confirmándose con los volúmenes que aparecen más adelante. Esto puede parecer que, en un principio, no cumple el requisito de conservación de la orden de escritura, pero eso solo se aplica a I/O que se emite de forma asíncrona en el host y no depende de ninguna otra escritura.

Por ejemplo, una base de datos puede emitir muchas actualizaciones de archivos de datos asíncronos y permitir que el sistema operativo vuelva a ordenar la I/O y completarlas de acuerdo con su propia configuración del programador. El orden de este tipo de I/O no se puede garantizar porque la aplicación y el sistema operativo ya han liberado el requisito de conservar el orden de escritura.

Como ejemplo de contador, la mayor parte de la actividad de registro de la base de datos es síncrona. La base de datos no continúa con más escrituras de registro hasta que se reconozca la E/S y se mantenga el orden de esas escrituras. Si un registro de I/O llega a un volumen cercado, no se reconoce y la aplicación se bloquea en otras escrituras. Del mismo modo, la I/O de metadatos del sistema de archivos suele ser síncrona. Por ejemplo, no se debe perder una operación de eliminación de archivos. Si un sistema operativo con un sistema de archivos xfs suprimió un archivo y la E/S que actualizó los metadatos del sistema de archivos xfs para eliminar la referencia a ese archivo aterrizó en un volumen cercado, la actividad del sistema de archivos se detendría. De este modo se garantiza la integridad del sistema de archivos durante las operaciones cg-

snapshot.

Después de configurar el control de escritura en los volúmenes de destino, están listos para la creación de las copias Snapshot. No es necesario crear las copias Snapshot precisamente al mismo tiempo, ya que el estado de los volúmenes se congela desde un punto de vista de escritura dependiente. Para protegerse frente a un defecto en la aplicación que crea las copias cg-snapshots, la barrera de escritura inicial incluye un tiempo de espera configurable en el que ONTAP libera automáticamente la barrera y reanuda el procesamiento de escritura transcurridos un número de segundos definido. Si todas las Snapshot se crean antes de que se agote el tiempo de espera, el conjunto de snapshots resultante es un grupo de coherencia válido.

Orden de escritura dependiente

Desde un punto de vista técnico, la clave para un grupo de consistencia es preservar el orden de escritura y, específicamente, el orden de escritura dependiente. Por ejemplo, una base de datos que escribe en 10 LUN escribe simultáneamente en todas ellas. Muchas escrituras se emiten de forma asíncrona, por lo que el orden en que se completan no es importante y el orden en que se realizan varía según el comportamiento del sistema operativo y de la red.

Algunas operaciones de escritura deben estar presentes en el disco antes de que la base de datos pueda continuar con escrituras adicionales. Estas operaciones de escritura cruciales se denominan escrituras dependientes. La E/S de escritura posterior depende de la presencia de estas escrituras en el disco. Cualquier snapshot, recuperación o replicación de estas 10 LUN debe asegurarse de que la orden de escritura dependiente está garantizada. Las actualizaciones del sistema de archivos son otro ejemplo de escrituras dependientes del orden de escritura. El orden en el que se realizan los cambios en el sistema de archivos debe conservarse o todo el sistema de archivos podría dañarse.

Estrategias

Existen dos enfoques principales para los backups basados en Snapshot:

- Backups coherentes con los fallos
- Backups activos protegidos de Snapshot

Una copia de seguridad coherente con los fallos de una base de datos se refiere a la captura de toda la estructura de la base de datos, incluidos archivos de datos, redo logs y archivos de control, en un único punto en el tiempo. Si la base de datos se almacena en un único volumen, el proceso es sencillo; se puede crear una copia Snapshot en cualquier momento. Si una base de datos abarca volúmenes, debe crearse una snapshot de grupo de coherencia (CG). Existen varias opciones para crear snapshots de CG, como el software NetApp SnapCenter, funciones nativas del grupo de coherencia ONTAP y scripts que se mantienen por el usuario.

Los backups de Snapshot coherentes con los fallos se usan principalmente cuando es suficiente con la recuperación punto del backup. Los registros de archivos se pueden aplicar bajo ciertas circunstancias, pero cuando se requiere una recuperación puntual más granular, es preferible un backup online.

El procedimiento básico para un backup en línea basado en Snapshot es el siguiente:

1. Coloque la base de datos en `backup` modo.
2. Cree una instantánea de todos los volúmenes que alojan archivos de datos.
3. Salga `backup` modo.
4. Ejecute el comando `alter system archive log current` para forzar el archivado de registros.
5. Crear instantáneas de todos los volúmenes que alojan los archive logs.

Este procedimiento produce un juego de instantáneas que contienen archivos de datos en modo de backup y los archive logs críticos generados durante el modo de backup. Estos son los dos requisitos para recuperar una base de datos. Los archivos, como los archivos de control, también deben protegerse por conveniencia, pero el único requisito absoluto es la protección de los archivos de datos y los registros de archivos.

Aunque los diferentes clientes pueden tener estrategias muy diferentes, casi todas estas estrategias se basan en última instancia en los mismos principios descritos a continuación.

Recuperación basada en Snapshot

Al diseñar diseños de volúmenes para bases de datos Oracle, la primera decisión es si utilizar tecnología NetApp SnapRestore basada en volúmenes (VBSR).

El SnapRestore basado en volúmenes permite revertir un volumen casi instantáneamente a un momento específico anterior. Debido a que se revierten todos los datos del volumen, es posible que VBSR no sea apropiado para todos los casos de uso. Por ejemplo, si se almacena una base de datos completa, incluidos archivos de datos, registros de recuperación y registros de archivos, en un solo volumen y este volumen se restaura con VBSR, los datos se pierden porque se descartan los datos de archive log y redo más recientes.

VBSR no se requiere para la restauración. Muchas bases de datos pueden restaurarse utilizando SnapRestore de archivo único (SFSR) basado en archivos o simplemente copiando archivos del snapshot al sistema de archivos activo.

Se prefiere VBSR cuando una base de datos es muy grande o cuando se debe recuperar lo antes posible, y el uso de VBSR requiere aislamiento de los archivos de datos. En un entorno NFS, los archivos de datos de una base de datos determinada deben estar almacenados en volúmenes dedicados que no estén contaminados por ningún otro tipo de archivo. En un entorno SAN, los archivos de datos deben almacenarse en LUN dedicadas en volúmenes dedicados. Si se utiliza un gestor de volúmenes (incluido Oracle Automatic Storage Management [ASM]), el grupo de discos también debe estar dedicado a los archivos de datos.

El aislamiento de archivos de datos de esta manera permite que se reviertan a un estado anterior sin dañar otros sistemas de archivos.

Reserva de Snapshot

Para cada volumen con datos de Oracle en un entorno SAN, el `percent-snapshot-space` Debe establecerse en cero porque reservar espacio para una snapshot en un entorno de LUN no es útil. Si la reserva fraccionaria se establece en 100, una copia snapshot de un volumen con unidades lógicas requiere suficiente espacio libre en el volumen, excluida la reserva de snapshot, para absorber un 100% de renovación de todos los datos. Si la reserva fraccionaria se define en un valor menor, se requiere una cantidad de espacio libre correspondiente menor, pero siempre excluye la reserva de instantáneas. Esto significa que se desperdicia el espacio de reserva de snapshot en un entorno de LUN.

En un entorno NFS, hay dos opciones:

- Ajuste la `percent-snapshot-space` basado en el consumo de espacio esperado de la instantánea.
- Ajuste la `percent-snapshot-space` a cero y gestione el consumo de espacio activo y snapshot de forma colectiva.

Con la primera opción, `percent-snapshot-space` se establece en un valor distinto de cero, normalmente alrededor del 20%. Este espacio se oculta al usuario. Sin embargo, este valor no crea un límite de utilización. Si una base de datos con una reserva del 20% experimenta una rotación del 30%, el espacio de la instantánea puede crecer más allá de los límites de la reserva del 20% y ocupar espacio sin reservar.

La principal ventaja de establecer una reserva en un valor como 20% es verificar que algo de espacio esté siempre disponible para las instantáneas. Por ejemplo, un volumen de 1TB GB con una reserva del 20% solo permitiría que un administrador de bases de datos (DBA) almacene 800GB TB de datos. Esta configuración garantiza al menos 200GB MB de espacio para el consumo de snapshots.

Cuando `percent-snapshot-space` se establece en cero, todo el espacio del volumen está disponible para el usuario final, lo que proporciona una mejor visibilidad. Un administrador de bases de datos debe comprender que, si ve un volumen de 1TB GB que aprovecha las copias Snapshot, este espacio de 1TB TB se compartirá entre los datos activos y la rotación de copias Snapshot.

No hay una preferencia clara entre la opción uno y la opción dos entre los usuarios finales.

Snapshots de ONTAP y de terceros

El ID de documento de Oracle 604683,1 explica los requisitos para la compatibilidad con Snapshot de terceros y las múltiples opciones disponibles para las operaciones de backup y restauración.

El proveedor externo debe garantizar que las copias Snapshot de la empresa cumplen con los requisitos siguientes:

- Las copias Snapshot deben integrarse con las operaciones de restauración y recuperación recomendadas de Oracle.
- Las instantáneas deben ser consistentes con los fallos de la base de datos en el punto de la instantánea.
- El orden de escritura se conserva para cada archivo dentro de una instantánea.

Los productos de gestión de Oracle de ONTAP y NetApp cumplen estos requisitos.

SnapRestore

Restauración de datos rápida en ONTAP a partir de una copia Snapshot realizada por la tecnología NetApp SnapRestore.

Cuando un conjunto de datos críticos no está disponible, las operaciones empresariales fundamentales no funcionan. Las cintas pueden romperse e incluso las restauraciones de backups basados en discos pueden ser lentas para transferirse por la red. SnapRestore evita estos problemas al ofrecer una restauración casi instantánea de conjuntos de datos. Incluso las bases de datos con capacidad de petabytes se pueden restaurar por completo con tan solo unos minutos.

Hay dos formas de SnapRestore: Basado en archivos/LUN y basado en volúmenes.

- Pueden restaurarse archivos o LUN individuales en segundos, tanto si se trata de un LUN de 2TB GB como de un archivo 4KB.
- El contenedor de archivos o LUN se puede restaurar en segundos, ya sea 10GB o 100TB TB de datos.

Un «contenedor de archivos o LUN» normalmente hace referencia a un volumen FlexVol. Por ejemplo, puede tener 10 LUN que componen un grupo de discos LVM en un único volumen o un volumen puede almacenar los directorios iniciales NFS de 1000 usuarios. En lugar de ejecutar una operación de restauración para cada archivo o LUN individuales, puede restaurar el volumen completo como una única operación. Este proceso también funciona con contenedores de escalado horizontal que incluyen múltiples volúmenes, como una FlexGroup o un grupo de consistencia ONTAP.

La razón por la que SnapRestore funciona tan rápido y eficientemente se debe a la naturaleza de una copia Snapshot, que es esencialmente una vista paralela de solo lectura del contenido de un volumen en un

momento determinado. Los bloques activos son los bloques reales que se pueden cambiar, mientras que la copia Snapshot es una vista de solo lectura del estado de los bloques que constituyen los archivos y la LUN en el momento de crear la copia Snapshot.

ONTAP solo permite el acceso de solo lectura a los datos de snapshots, pero los datos se pueden reactivar con SnapRestore. La copia de Snapshot se vuelve a habilitar como una vista de lectura y escritura de los datos, lo que devuelve los datos a su estado anterior. SnapRestore puede funcionar a nivel de volumen o archivo. La tecnología es esencialmente la misma con algunas pequeñas diferencias en el comportamiento.

SnapRestore de volumen

La SnapRestore basada en volúmenes devuelve todo el volumen de datos a un estado anterior. Esta operación no requiere el movimiento de datos, lo que significa que el proceso de restauración es esencialmente instantáneo, aunque la operación de la API o la CLI puede tardar unos segundos en procesarse. La restauración de 1GB TB de datos no es más complicada ni requiere más tiempo que restaurar 1PB TB de datos. Esta funcionalidad es el principal motivo por el que muchos clientes empresariales migran a los sistemas de almacenamiento de ONTAP. Proporciona un objetivo de tiempo de recuperación que se mide en segundos incluso para los conjuntos de datos de mayor tamaño.

Una desventaja de la SnapRestore basada en el volumen se debe al hecho de que los cambios dentro de un volumen son acumulativos con el tiempo. Por lo tanto, cada instantánea y los datos del archivo activo dependen de los cambios que conduzcan a ese punto. Revertir un volumen a un estado anterior implica descartar todos los cambios posteriores que se habían realizado en los datos. Sin embargo, lo que no resulta tan obvio es que se incluyen las instantáneas creadas posteriormente. Esto no siempre es deseable.

Por ejemplo, un acuerdo de nivel de servicio de retención de datos puede especificar 30 días de backups nocturnos. Si se restaura un conjunto de datos en una snapshot creada hace cinco días con SnapRestore para volúmenes, se descartarán todas las snapshots creadas en los cinco días anteriores, lo que infringe el acuerdo de nivel de servicio.

Hay varias opciones disponibles para abordar esta limitación:

1. Los datos se pueden copiar a partir de una snapshot anterior, en lugar de realizar una SnapRestore de todo el volumen. Este método funciona mejor con conjuntos de datos más pequeños.
2. Una copia Snapshot puede clonarse en lugar de restaurarse. La limitación de este enfoque es que la copia Snapshot de origen depende del clon. Por lo tanto, no se puede eliminar a menos que también se elimine el clon o se divida en un volumen independiente.
3. Uso de SnapRestore basado en archivos.

SnapRestore de archivos

La SnapRestore basada en archivos es un proceso de restauración más granular basado en Snapshot. En lugar de revertir el estado de un volumen completo, se revierte el estado de un archivo individual o LUN. No es necesario eliminar ninguna instantánea, ni esta operación crea ninguna dependencia de una instantánea anterior. El archivo o el LUN estarán disponibles de inmediato en el volumen activo.

No es necesario mover datos durante una restauración SnapRestore de un archivo o una LUN. Sin embargo, se requieren algunas actualizaciones internas de metadatos para reflejar el hecho de que los bloques subyacentes de un archivo o LUN ahora existen tanto en una snapshot como en el volumen activo. No debería afectar el rendimiento, pero este proceso bloquea la creación de snapshots hasta que se completa. La tasa de procesamiento es de aproximadamente 5Gbps (18TB TB/hora) en función del tamaño total de los archivos restaurados.

Backups en línea

Se necesitan dos conjuntos de datos para proteger y recuperar una base de datos de Oracle en modo de backup. Tenga en cuenta que esta no es la única opción de copia de seguridad de Oracle, pero es la más común.

- Instantánea de los archivos de datos en modo de copia de seguridad
- Los registros de archivos creados mientras los archivos de datos estaban en modo de backup

Si se necesita una recuperación completa, incluidas todas las transacciones confirmadas, se requiere un tercer elemento:

- Juego de redo logs actuales

Existen varias formas de impulsar la recuperación de un backup en línea. Muchos clientes restauran snapshots mediante la interfaz de línea de comandos de ONTAP y, a continuación, usando Oracle RMAN o sqlplus para completar la recuperación. Esto es especialmente habitual en entornos de producción de gran tamaño en los que la probabilidad y frecuencia de las restauraciones de bases de datos es extremadamente baja y cualquier procedimiento de restauración lo gestiona un administrador de bases de datos cualificado. Para obtener una automatización completa, las soluciones como NetApp SnapCenter incluyen un complemento de Oracle con interfaces gráficas y de línea de comandos.

Algunos clientes a gran escala han adoptado un enfoque más simple mediante la configuración de secuencias de comandos básicas en los hosts para colocar las bases de datos en modo de backup en un momento específico de preparación para una copia Snapshot programada. Por ejemplo, programe el comando `alter database begin backup` a las 23:58, `alter database end backup` a las 00:02, y después programe copias snapshot directamente en el sistema de almacenamiento a medianoche. El resultado es una estrategia de backup sencilla y altamente escalable que no requiere software ni licencias externas.

Distribución de datos

El diseño más sencillo es aislar los archivos de datos en uno o varios volúmenes dedicados. No deben estar contaminados por ningún otro tipo de archivo. De este modo, se garantiza que los volúmenes de archivos de datos puedan restaurarse rápidamente mediante una operación SnapRestore sin destruir un registro de recuperación, un archivo de control o un archivo importante.

SAN tiene requisitos similares para aislamiento de archivos de datos en volúmenes dedicados. Con un sistema operativo como Microsoft Windows, un único volumen puede contener varios LUN de archivos de datos, cada uno con un sistema de archivos NTFS. Con otros sistemas operativos, generalmente hay un administrador de volúmenes lógicos. Por ejemplo, con Oracle ASM, la opción más sencilla sería confinar los LUN de un grupo de discos ASM en un único volumen del que se pueda incluir y restaurar como unidad en un backup. Si se necesitan volúmenes adicionales por motivos de rendimiento o gestión de capacidad, crear un grupo de discos adicional en el nuevo volumen simplifica la gestión.

Si se siguen estas directrices, se pueden programar Snapshot directamente en el sistema de almacenamiento sin requisitos para realizar una snapshot de grupo de coherencia. El motivo es que las copias de seguridad de Oracle no necesitan que se realice una copia de seguridad de los archivos de datos al mismo tiempo. El procedimiento de backup online se diseñó para permitir que los archivos de datos sigan actualizándose a medida que se transmiten lentamente a la cinta durante horas.

Se produce una complicación en situaciones como el uso de un grupo de discos de ASM que se distribuye entre volúmenes. En estos casos, se debe realizar una cg-snapshot para garantizar que los metadatos de ASM sean coherentes en todos los volúmenes constituyentes.

Precaución: Verifique que el ASM `spfile` y.. `passwd` los archivos no están en el grupo de discos que aloja los archivos de datos. Esto interfiere con la capacidad de restaurar selectivamente archivos de datos y solo archivos de datos.

Procedimiento de recuperación local: NFS

Este procedimiento se puede realizar manualmente o a través de una aplicación como SnapCenter. El procedimiento básico es el siguiente:

1. Cierre la base de datos.
2. Recupere los volúmenes del archivo de datos en la instantánea inmediatamente antes del punto de restauración deseado.
3. Reproduzca los archive logs en el punto deseado.
4. Reproduzca los redo logs actuales si desea una recuperación completa.

En este procedimiento se asume que los archive logs deseados siguen presentes en el sistema de archivos activo. De lo contrario, se deben restaurar los archive logs o se puede dirigir rman/sqlplus a los datos del directorio de instantáneas.

Además, para bases de datos más pequeñas, un usuario final puede recuperar archivos de datos directamente desde `.snapshot` directorio sin la ayuda de herramientas de automatización o administradores del almacenamiento para ejecutar un `snaprestore` comando.

Procedimiento de recuperación local: San

Este procedimiento se puede realizar manualmente o a través de una aplicación como SnapCenter. El procedimiento básico es el siguiente:

1. Cierre la base de datos.
2. Desactive los grupos de discos que alojan los archivos de datos. El procedimiento varía en función del gestor de volúmenes lógico elegido. Con ASM, el proceso requiere desmontar el grupo de discos. Con Linux, los sistemas de archivos deben desmontarse y los volúmenes lógicos y los grupos de volúmenes deben desactivarse. El objetivo es detener todas las actualizaciones en el grupo de volúmenes objetivo que se va a restaurar.
3. Restaure los grupos de discos de archivos de datos en la instantánea inmediatamente antes del punto de restauración deseado.
4. Vuelva a activar los grupos de discos recién restaurados.
5. Reproduzca los archive logs en el punto deseado.
6. Vuelva a reproducir todos los redo logs si desea realizar una recuperación completa.

En este procedimiento se asume que los archive logs deseados siguen presentes en el sistema de archivos activo. Si no lo son, los registros de archivos se deben restaurar desconectando las LUN del registro de archivos y ejecutando una restauración. Este es también un ejemplo en el que la división de archive logs en volúmenes dedicados es útil. Si los registros de archivos comparten un grupo de volúmenes con registros de recuperación, se deben copiar en otro lugar los registros de recuperación antes de restaurar el conjunto general de LUN. Este paso evita la pérdida de las transacciones registradas finales.

Backups optimizados para Snapshot de almacenamiento

Cuando se lanzó Oracle 12c, ya que no es necesario colocar una base de datos en

modo de backup dinámico, se simplificaron aún más las tareas de backup y recuperación basadas en Snapshots. El resultado es la capacidad de programar backups basados en snapshots directamente en un sistema de almacenamiento y mantener la capacidad para realizar una recuperación completa o de un momento específico.

Aunque el procedimiento de recuperación de backup dinámico es más familiar para los administradores de bases de datos, durante mucho tiempo ha sido posible usar snapshots que no se crearon mientras la base de datos estaba en modo de backup dinámico. Oracle 10g y 11g requerían pasos manuales adicionales durante la recuperación para hacer que la base de datos fuera coherente. Con Oracle 12c, `sqlplus` y.. `rman` contienen la lógica adicional para reproducir archive logs en copias de seguridad de archivos de datos que no estaban en modo de copia de seguridad activa.

Como hemos visto anteriormente, la recuperación de un backup en caliente basado en instantáneas requiere dos conjuntos de datos:

- Instantánea de los archivos de datos creados en modo de backup
- Los registros de archivos generados mientras los archivos de datos estaban en modo de backup dinámico

Durante la recuperación, la base de datos lee los metadatos de los archivos de datos para seleccionar los archive logs requeridos para la recuperación.

La recuperación optimizada para snapshot de almacenamiento requiere conjuntos de datos ligeramente diferentes para lograr los mismos resultados:

- Una instantánea de los archivos de datos, además de un método para identificar la hora a la que se creó la instantánea
- Archive logs desde la hora del punto de control del archivo de datos más reciente hasta la hora exacta de la instantánea

Durante la recuperación, la base de datos lee metadatos de los archivos de datos para identificar el primer archive log necesario. Se puede realizar una recuperación completa o a un momento específico. Al realizar una recuperación puntual, es fundamental conocer la hora de la instantánea de los archivos de datos. El punto de recuperación especificado debe ser posterior a la hora de creación de las instantáneas. NetApp recomienda añadir al menos unos minutos al tiempo de la snapshot para justificar la variación de reloj.

Para obtener más información, consulte la documentación de Oracle sobre el tema «Recuperación mediante la optimización de instantáneas de almacenamiento» disponible en varias versiones de la documentación de Oracle 12c. Además, consulte el ID de documento de Oracle 604683,1 con respecto al soporte de instantáneas de terceros de Oracle.

Distribución de datos

El diseño más sencillo es aislar los archivos de datos en uno o varios volúmenes dedicados. No deben estar contaminados por ningún otro tipo de archivo. De este modo, se garantiza que los volúmenes de archivos de datos se puedan restaurar rápidamente con una operación de SnapRestore sin destruir un registro de recuperación, un archivo de control o un archivo importante.

SAN tiene requisitos similares para aislamiento de archivos de datos en volúmenes dedicados. Con un sistema operativo como Microsoft Windows, un único volumen puede contener varios LUN de archivos de datos, cada uno con un sistema de archivos NTFS. Con otros sistemas operativos, generalmente hay un gestor de volúmenes lógicos también. Por ejemplo, con Oracle ASM, la opción más sencilla sería restringir los grupos de discos en un único volumen del que se pueda realizar un backup y restaurar como unidad. Si se necesitan volúmenes adicionales por motivos de rendimiento o gestión de capacidad, crear un grupo de

discos adicional en el nuevo volumen simplifica la gestión.

Si se siguen estas directrices, se pueden programar Snapshot directamente en ONTAP sin requisitos para realizar una snapshot de grupo de coherencia. El motivo es que las copias de seguridad optimizadas para instantáneas no necesitan que se realice una copia de seguridad de los archivos de datos al mismo tiempo.

Se produce una complicación en situaciones como un grupo de discos de ASM que se distribuye entre volúmenes. En estos casos, se debe realizar una cg-snapshot para garantizar que los metadatos de ASM sean coherentes en todos los volúmenes constituyentes.

[Nota]Verifique que los archivos spfile y passwd de ASM no estén en el grupo de discos que aloja los archivos de datos. Esto interfiere con la capacidad de restaurar selectivamente archivos de datos y solo archivos de datos.

Procedimiento de recuperación local: NFS

Este procedimiento se puede realizar manualmente o a través de una aplicación como SnapCenter. El procedimiento básico es el siguiente:

1. Cierre la base de datos.
2. Recupere los volúmenes del archivo de datos en la instantánea inmediatamente antes del punto de restauración deseado.
3. Reproduzca los archive logs en el punto deseado.

En este procedimiento se asume que los archive logs deseados siguen presentes en el sistema de archivos activo. Si no lo son, se deben restaurar los registros de archivos `rman` o. `sqlplus` se puede dirigir a los datos de la `.snapshot` directorio.

Además, para bases de datos más pequeñas, un usuario final puede recuperar archivos de datos directamente desde `.snapshot` Directorio sin ayuda de las herramientas de automatización o de un administrador del almacenamiento para ejecutar un comando de la SnapRestore.

Procedimiento de recuperación local: San

Este procedimiento se puede realizar manualmente o a través de una aplicación como SnapCenter. El procedimiento básico es el siguiente:

1. Cierre la base de datos.
2. Desactive los grupos de discos que alojan los archivos de datos. El procedimiento varía en función del gestor de volúmenes lógico elegido. Con ASM, el proceso requiere desmontar el grupo de discos. Con Linux, los sistemas de archivos deben desmontarse y los volúmenes lógicos y los grupos de volúmenes están desactivados. El objetivo es detener todas las actualizaciones en el grupo de volúmenes objetivo que se va a restaurar.
3. Restaure los grupos de discos de archivos de datos en la instantánea inmediatamente antes del punto de restauración deseado.
4. Vuelva a activar los grupos de discos recién restaurados.
5. Reproduzca los archive logs en el punto deseado.

En este procedimiento se asume que los archive logs deseados siguen presentes en el sistema de archivos activo. Si no lo son, los registros de archivos se deben restaurar desconectando las LUN del registro de archivos y ejecutando una restauración. Este es también un ejemplo en el que la división de archive logs en volúmenes dedicados es útil. Si los registros de archivos comparten un grupo de volúmenes con redo logs, los

redo logs se deben copiar en otro lugar antes de restaurar el conjunto general de LUN para evitar perder las transacciones finales registradas.

Ejemplo de recuperación completa

Supongamos que los archivos de datos se han dañado o destruido y se necesita una recuperación completa. El procedimiento para hacerlo es el siguiente:

```
[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>
```

Ejemplo de recuperación a un momento específico

Todo el procedimiento de recuperación es un único comando: `recover automatic`.

Si se requiere una recuperación a un momento específico, es necesario conocer la marca de hora de las instantáneas y se puede identificar de la siguiente manera:

```
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
```

La hora de creación de la copia Snapshot se muestra como 9th de marzo y 10:10:06. Para estar seguro, se añade un minuto a la hora de la copia 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 recuperación se inicia ahora. Especificó una hora de instantánea de 10:11:00, un minuto después del tiempo registrado para contabilizar la posible variación de reloj y un tiempo de recuperación objetivo de 10:44. A continuación, sqlplus solicita los archive logs necesarios para alcanzar el tiempo de recuperación deseado 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>
```

Recuperación completa de una base de datos utilizando instantáneas utilizando el `recover automatic` el comando no requiere una licencia específica, sino un uso de recuperación puntual `snapshot time` Necesita la licencia de Oracle Advanced Compression.

Herramientas de automatización y gestión de base de datos

El valor principal de ONTAP en un entorno de bases de datos de Oracle proviene de las tecnologías principales de ONTAP, como las copias Snapshot instantáneas, la replicación simple de SnapMirror y la creación eficiente de los volúmenes FlexClone.

En algunos casos, la simple configuración de estas funciones básicas directamente en ONTAP satisface los requisitos, pero las necesidades más complicadas requieren una capa de orquestación.

SnapCenter

SnapCenter es el producto estrella de protección de datos de NetApp. A un nivel muy bajo, es similar a los productos de SnapManager en cuanto a cómo se ejecutan backups de bases de datos, pero se creó desde cero para proporcionar un panel único para la gestión de la protección de datos en sistemas de almacenamiento de NetApp.

SnapCenter incluye las funciones básicas, como los backups y restauraciones basados en Snapshot, la replicación de SnapMirror y SnapVault, y otras funciones necesarias para funcionar a escala para grandes empresas. Estas funciones avanzadas incluyen una funcionalidad ampliada de control de acceso basado en roles (RBAC), API RESTful para integrarse con productos de orquestación de terceros, gestión central no disruptiva de complementos de SnapCenter en hosts de bases de datos y una interfaz de usuario diseñada para entornos a escala de cloud.

DESCANSO

ONTAP también contiene un amplio conjunto de API RESTful. Esto permite que 3rd proveedores de partes creen protección de datos y otras aplicaciones de gestión con la profunda integración con ONTAP. Además, los clientes que desean crear sus propios flujos de trabajo y utilidades de automatización pueden consumir fácilmente la API RESTful.

Información de copyright

Información de la marca comercial