Texto, Tabla

Descripción generada automáticamente con confianza media

Prevenir la pérdida de datos es una tarea fundamental en la administración de bases de datos. Las copias de seguridad son un mecanismo de recuperación con el cual los administradores pueden restaurar una base de datos que ha perdido información por cualquier circunstancia. La responsabilidad que conlleva garantizar la calidad y privacidad de la información por parte de las organizaciones es relevante en todo aspecto, por lo que es necesario mitigar los riesgos que provoquen cualquier tipo de ataque como accesos no autorizados, sustracción de información o pérdida de datos por fallas humanas o del sistema.

Texto, Escala de tiempo

Descripción generada automáticamente

La protección de los datos debe llevarse a cabo contra fallos físicos, lógicos, humanos, intencionados o no, y cada uno debe ser tratado de forma distinta. Hay paradas catastróficas del sistema debido a errores de hardware o de software con la consecuente pérdida de contenido en la memoria, fallos del soporte físico que ocasionan la pérdida de la información guardada, errores de software de las aplicaciones que causan fallo en una o más transacciones, desastres físicos naturales como incendios, inundaciones o apagones, destrucción intencionada o no de datos o instalaciones por operarios o usuarios, y sabotaje o destrucción intencionada de los datos o del hardware.

Es indispensable que en una organización se planifiquen estrategias que permitan anticipar la mayoría de los posibles desastres o fallos y así obtener una rápida recuperación mientras continúa operando. Para ello existen dos conceptos que son fundamentales y que influyen en este proceso: el Recovery Time Objective, que determina la mayor cantidad de tiempo que la organización está dispuesta a asumir en la restauración por un error o un fallo mientras una actividad se encuentra sin ejecutar, teniendo en cuenta que el impacto dentro de la operatividad del negocio será bajo; es decir, especifica la demora máxima hasta que el servicio de aplicaciones se instaure; y el Recovery Point Objective, que establece el volumen de datos en riesgo de pérdida que la organización está dispuesta a asumir, lo cual dependerá de la cantidad de transacciones realizadas a la base de datos por unidad de tiempo.

La recuperación puede requerir revertir a un punto consistente antes del fallo, descartando las actualizaciones emitidas después de ese punto de recuperación. El objetivo del punto de recuperación es definir la ventana de tiempo máxima permitida para las recientes actualizaciones que pueden perderse, que inclusive puede ser cero; o sea, ninguna pérdida es tolerable.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

La política de retención especifica la forma en que se gestionará la creación de backups de una base de datos, teniendo en cuenta los requerimientos por parte de la organización. Es decir, la frecuencia y el tipo de copia se determinará principalmente con respecto a los cambios en la información. Debe determinarse, a tal fin, la redundancia que establece un número fijo de backups que debe mantenerse.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

La recuperación de fallos equivale a una restauración de la base de datos a algún estado anterior, de modo que sea posible reconstruir un estado correcto cercano al momento del fallo. A partir de tal estado anterior, si hay daños físicos, el método de recuperación restaurará una copia anterior y reconstruirá el estado rehaciendo las operaciones confirmadas restantes hasta el momento del fallo. Si la base de datos no presenta daños físicos pero los datos se han vuelto inconsistentes, no es necesario restaurar una copia completa de la base, solo las últimas operaciones registradas que pudieran haber causado la inconsistencia. Se deben entonces deshacer operaciones y rehacer las necesarias a fin de restaurar un estado consistente.

Texto

Descripción generada automáticamente

Un sistema gestor de base de datos debe proporcionar las siguientes funcionalidades como ayuda a la recuperación: un mecanismo de copia de seguridad mediante el cual se hagan copias de seguridad periódicas de la base de datos fuera de la base de datos, facilidades de registro que mantengan el control del estado actual de las transacciones y de los cambios realizados en la base de datos, funcionalidad de puntos de comprobación (Checkpoints) que permita que las actualizaciones de la base de datos que estén llevándose a cabo se hagan permanentes, y un gestor de recuperación que permita al sistema restaurar la base de datos a un estado coherente después del fallo.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Las estrategias típicas de recuperación de una base de datos son básicamente tres: copias de respaldo en otros medios de almacenamiento, los backups, operaciones específicas de rehacer y deshacer, y registrar los movimientos realizados en un archivo diario o bitácora llamado log de las transacciones.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

El archivo log es una tabla de la base de datos que contiene una lista secuencial de todas las modificaciones a cada objeto de la base de datos. Es el administrador de la base de datos quien define qué datos son registrados, por ejemplo, fecha y hora, usuario, tabla accedida, operación realizada, terminal desde donde se conecta, etc., guardándose el estado anterior y posterior del objeto accedido. Contiene los datos completos de los cambios desde el último backup, y cada registro de cambio del log contiene el identificador de la transacción que ejecutó el cambio, el identificador del ítem de datos modificado (típicamente la ubicación en el disco), el valor viejo que fue sobreescrito, el valor nuevo luego de la escritura y, opcionalmente, tiempo de comienzo de la transacción, tiempo del commit (cuando la transacción está confirmada), un tiempo de aborto, etc.

Diagrama

Descripción generada automáticamente

En este esquema podemos seguir visualmente ese proceso: cuando comienza una transacción T, se registra su inicio en el log, guardándose el valor existente. Cuando todas las acciones de la transacción T se ejecutan exitosamente, se escribe el commit en el log con el nuevo valor, y por último se realizan las operaciones de escritura en la base de datos.

Imagen que contiene pájaro, ave, flor, árbol

Descripción generada automáticamente

La operación de recuperación usa dos primitivas: rehacer, que rehace la actualización registrada en el log (es decir, escribe el valor nuevo sobre el ítem de datos modificados) y deshacer, que deshace la actualización registrada en el log (es decir, escribe el valor antiguo sobre el ítem de datos modificado).

Texto

Descripción generada automáticamente

Las técnicas de recuperación son dos: vía reprocesamiento en la base de datos, que retorna a un estado correcto previo conocido y reprocesa las transacciones ejecutadas hasta el momento del fallo; y la recuperación basada en el contenido del log, que puede adoptar tres estrategias. Por actualización diferida, las transacciones no cambian la base de datos hasta que alcanzan el punto de confirmación, y lo alcanzan cuando el log ha sido actualizado. La estrategia en este caso es no deshacer, rehacer. La actualización inmediata actualiza la base de datos usando el registro de escritura anticipada, forzando las escrituras en el log antes de escribir en la base de datos, ejecutando el commit de la transacción después de escribir en el log. La estrategia es deshacer, rehacer. Y vía rollback o roll forward, que salva la base de datos periódicamente y mantiene un archivo log auxiliar con los cambios producidos en orden cronológico: rollback deshace los cambios erróneos y reprocesa las transacciones válidas, y roll forward rehace los cambios en la base de datos usando datos salvados y transacciones desde el último backup.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Cuando se produce un fallo, debe determinarse qué transacciones hay que rehacer y cuáles hay que deshacer. La inspección del archivo log completo es costosa en tiempo, y muchas transacciones ya habrán estado confirmadas en la base de datos, es decir, ya son persistentes. Para reducir la carga de trabajo que implica la restauración, se utilizan los Checkpoints. Un checkpoint registra un punto antes del cual el sistema gestor de la base de datos estaba en un estado consistente y todas las transacciones fueron confirmadas. Siguen el siguiente procedimiento: se graban todos los registros del log actualmente en memoria principal en un almacenamiento estable, se graban en la base de datos todos los bloques de registros almacenados en el buffer, y se escribe en el log entonces un registro de tipo checkpoint.

Texto

Descripción generada automáticamente

Los algoritmos de recuperación son técnicas que garantizan las propiedades de atomicidad, consistencia y durabilidad de los datos a pesar de las fallas. Durante la recuperación diferida se consideran los siguientes pasos: recorrer hacia atrás desde el final del log hasta alcanzar el checkpoint más reciente, continuar recorriendo hasta encontrar el momento de comienzo de control, considerar la parte del log que sigue a este registro, para todas las transacciones comenzadas desde el punto de control o después que no hayan registrado commit, ejecutar deshacer; recorrer el log hacia delante para todas las transacciones comenzadas desde el punto de control que hayan registrado commit, ejecutando rehacer.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

El backup es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de pérdida. El objetivo principal de los backups es justamente preservar información por un periodo de tiempo determinado para ser recuperada y restaurada en caso de problemas o fallas que se presenten en la base de datos a nivel físico o lógico. La operación ideal consiste en que las copias de seguridad sean generadas sin necesidad de intervención manual. La automatización de dicho proceso disminuye la probabilidad de errores que dependan del factor humano.

Tenemos los siguientes tipos de backups: la copia de seguridad parcial (Partial Database Backup), que es una copia de una parte de la base de datos. Se debe considerar que después de restaurar una copia de este tipo es necesario sincronizarla con el resto de la base de datos. El Whole Database Backup preserva todos los datos generados a la fecha desde el último archivo de control. Los archivos de control almacenan el estado de la estructura física de una base de datos; en ellos se guarda el estado actual de la base de datos y son utilizados para mantener la consistencia interna y guiar las operaciones de recuperación.

El Full Backup, que es la copia de seguridad completa, también conocido como Backup Nivel Cero, es la copia de todos El backup incremental, también conocido como backup de nivel 1, es una copia de los cambios realizados en la base de datos desde el anterior backup catalogado. Este se divide en acumulativo, que genera una copia desde el último backup nivel cero (full backup) a la fecha, y diferencial, que genera una copia desde el último backup nivel 1 a la fecha.

Gráfico, Escala de tiempo, Gráfico de cajas y bigotes

Descripción generada automáticamente

Texto

Descripción generada automáticamente

El sistema gestor de la base de datos debe proveer técnicas que permitan a ciertos usuarios tener acceso a porciones específicas de una base de datos sin tener acceso al resto mediante un subsistema de seguridad, autorización de acceso y cifrado de datos. Este aspecto se relaciona con la protección de datos contra accesos no autorizados y para protegerlos de una posible corrupción durante todo su ciclo de vida. El usuario administrador de la base de datos es el responsable de la seguridad global de la base de datos, ya que cuenta con funciones de privilegio para crear cuentas con claves de usuario, conceder privilegios de acceso, revocar o modificar estos privilegios, establecer niveles de seguridad para que las cuentas accedan solo al nivel asignado o gestionar el archivo de auditoría donde quedan registradas las operaciones que realizan los usuarios. La seguridad se mide según la protección implementada para hacer frente a ataques externos, fallas de software y hardware, y la manipulación de datos por los usuarios.

Las medidas de seguridad abarcan seguridad física, como controlar el acceso a los equipos, acceso a lugares donde están instalados terminales clientes, servidores y bases de datos, horarios donde es permitido realizar las operaciones, etc. También incluye seguridad de usuarios, con acceso solo al personal autorizado mediante uso de códigos de acceso, palabras claves, huella digital, reconocimiento de voz, etc., y la seguridad lógica, como discos replicados, control de calidad y desempeño del hardware, y encriptación de los datos de las operaciones en el archivo de auditoría, entre otros.

Tabla

Descripción generada automáticamente

Los siguientes requisitos son esenciales para la seguridad de una base de datos: el sistema debe tener capacidad para verificar que sus acciones han sido autorizadas, las acciones de los usuarios deben ser supervisadas para descubrir cualquier acción indebida o errónea, el sistema debe diseñarse a prueba de intromisiones, los datos deben poder ser sometidos a procesos de auditoría, y la base de datos debe ser protegida contra incendio, robo, agresión y otras formas de destrucción.

Veamos ahora algunos conceptos relevantes a la seguridad de base de datos.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente La encriptación es un procedimiento que utiliza un algoritmo de cifrado con una clave llamada clave de cifrado para transformar un mensaje, de tal forma que sea incomprensible o al menos difícil de comprender para quienes no tienen la clave de descifrado. En esquemas de clave simétrica, las claves de cifrado y descifrado son las mismas. En los esquemas de cifrado asimétrico o de clave pública, la clave de cifrado se publica para que cualquiera pueda usarla, pero solo la parte receptora tiene acceso a la clave de descifrado.

Texto

Descripción generada automáticamente

El hackeo, vulnerabilidad o intrusión refiere a ataques posibles desde el exterior mediante virus, que es un trozo de código que se adosa a un programa legítimo contaminándolo; cuando un programa contaminado se ejecuta, también ejecutará el código del virus. El troyano es un programa aparentemente útil que contiene un código que brinda a un atacante acceso remoto al equipo infectado. La puerta trasera es un punto de entrada secreto dejado por los implementadores del sistema para saltarse los procedimientos normales de seguridad. Phishing deja un programa corriendo en una terminal que pide login y luego password para engañar a los usuarios y obtener sus credenciales.

Imagen que contiene Diagrama

Descripción generada automáticamente

Un firewall es un elemento basado en hardware, software o una combinación de ambos que controla el flujo de datos que entra y sale de una red. Con el firewall podemos definir tamaños de paquetes, direcciones IP permitidas, deshabilitar el envío o recogida de paquetes para ciertos puertos, entre otros. Un proxy es un sistema de software que controla el flujo de datos hacia el exterior.

Imagen que contiene Escala de tiempo

Descripción generada automáticamente

La seguridad en internet se basa en el uso de protocolos SSL (Secure Sockets Layer), traducido como capa de conexiones seguras. Este protocolo usa certificados digitales para establecer comunicaciones seguras a través de internet y ha sido sustituido por TLS (Transport Layer Security), que es compatible con SSL. HTTPS es una combinación del protocolo HTTP con SSL/TLS, usado para establecer comunicaciones cifradas en sitios web. Prácticamente todos los principales servicios de internet cifran sus datos, como Gmail, Facebook o Twitter, incluyendo sistemas operativos como Android.