Backup y Recuperación de Bases de datos

Colihuinca Matias, Correa Matias E. , del Valle Lucas M.

Universidad Tecnológica Nacional

Base de Datos II

Eduardo Mónaco

19 de Mayo de 2025

Índice

Backup y Recuperación de Bases de Datos

Introducción

El respaldo (backup) y la recuperación de bases de datos son procesos fundamentales para garantizar la disponibilidad y la integridad de la información en sistemas de gestión de bases de datos. Estos procesos permiten proteger los datos contra pérdidas debido a fallos del sistema, errores humanos o desastres naturales. Implementar una estrategia efectiva de backup y recuperación es esencial para la continuidad del negocio y el cumplimiento de normativas de seguridad de la información.

Marco teórico

Backup:

Proceso de crear una copia de seguridad de los datos almacenados en una base de datos para protegerlos contra pérdidas.

Recuperación de datos:

Proceso de restaurar los datos desde una copia de seguridad a su estado original o a un punto específico en el tiempo.

¿Qué es la copia de seguridad de la base de datos?

La copia de seguridad de la base de datos es el proceso de crear una copia de datos estructurados, incluidos los archivos de datos maestros y de transacciones de una empresa, dentro de las cargas de trabajo de la base de datos, lo que garantiza la protección y recuperación de datos en entornos locales y en la nube.

La importancia de realizar una copia de seguridad de la base de datos

- **Recuperación en caso de desastre:**

  Fallos de hardware, errores humanos o ciberataques (como ransomware) pueden causar la pérdida de datos. Las copias de seguridad permiten restaurar la base de datos a un estado anterior, minimizando el tiempo de inactividad.

- **Protección contra errores:**

  Errores como la eliminación accidental de información pueden corregirse fácilmente si se dispone de un respaldo.

- **Continuidad del negocio:**

  Permite que las operaciones empresariales continúen con la menor interrupción posible.

- **Cumplimiento normativo:**

  Algunas industrias requieren legalmente la implementación de copias de seguridad regulares.

Tipos de backups:

Existen varios tipos de backups, cada uno adecuado para diferentes necesidades y escenarios. A continuación, se detallan los tipos fundamentales de backups en una base sólida de datos de los cuales se pueden hacer otros tipos de respaldos.

Backup incremental:

Guarda solo los datos que han cambiado desde el último backup (completo o incremental). Muy utilizado en bases como SQL. Es eficiente en espacio y tiempo, pero más complejo de restaurar.

Backup completo:

Crea una copia total de todos los datos de la base en un punto específico en el tiempo. Aunque consume más espacio y tiempo, es el más sencillo de restaurar.

Backup diferencial:

Incluye todos los cambios desde el último backup completo. Aunque requiere más espacio que el incremental, es más fácil de restaurar (solo necesita el último completo y el último diferencial).

Backup de registro de transacción:

Guarda todas las transacciones realizadas desde el último backup. Es esencial para entornos transaccionales que requieren recuperación precisa.

Backup de archivo:

Utilizado principalmente para bases de datos de gran tamaño, permite respaldar archivos o grupos de archivos específicos dentro de la base de datos. Esto es particularmente útil cuando ciertas partes de la base de datos necesitan ser respaldadas y restauradas de forma independiente.

Backup sintético:

Crea una copia "completa" combinando backups incrementales o diferenciales, reduciendo el tiempo de ejecución.

Backup de espejo:

Duplica la información en otro dispositivo o ubicación, lo que permite una recuperación rápida en caso de fallas.

Backup en la nube (BaaS):

Utiliza un proveedor de servicios en la nube para realizar el backup de los datos. AWS, Azure o Google Cloud serían algunos ejemplos.

Backup Local (On-site Backup)

Los datos se almacenan en dispositivos locales, como discos duros externos, servidores locales o cintas magnéticas. Es comúnmente utilizado en empresas para mantener copias de seguridad dentro de las instalaciones.

Backup Remoto (Off-site Backup)

Similar al backup en la nube, pero no necesariamente en un servicio de nube pública. Los datos se almacenan en ubicaciones remotas, que pueden ser servidores en otro centro de datos o en otros edificios de la misma empresa.

Backup en Tiempo Real (Real-time Backup)

Este tipo de backup realiza copias continuas de los archivos conforme estos cambian, lo que asegura que siempre haya una copia actualizada.

Diversidad de bases de datos y su impacto en las estrategias de respaldo

Muchas empresas tienen varias bases de datos. Por ejemplo, Oracle puede ofrecer una solución para contabilidad, pero una aplicación (y base de datos) diferente podría ser más adecuada para el control de inventario.

Las bases de datos también se presentan en diferentes formas estructurales o esquemas, como las bases de datos relacionales tipo tabla (Oracle, Microsoft SQL, MySQL, SAP HANA) o como bases de datos distribuidas las que podrían ser NoSQL, Hadoop y plataformas de software como servicio (SaaS) como Microsoft 365, Azure o Amazon Web Services (AWS).

Con tantas opciones de bases de datos, contar con el software de respaldo adecuado es esencial. Las soluciones de respaldo de bases de datos suelen ser proporcionadas por múltiples proveedores mediante diferentes procesos manuales y automatizados que residen en infraestructuras obsoletas. Estos sistemas heredados pueden causar fragmentación de datos y tiempos de recuperación drásticamente lentos.

Debido a que los datos son tan valiosos para las organizaciones, un servicio o un software de respaldo de bases de datos moderno es esencial.

Frecuencia de realización de una copia de seguridad

La frecuencia de las copias de seguridad depende de la frecuencia con la que cree o modifique sus archivos y de la importancia que tengan para su trabajo o uso personal. En general, debe seguir la regla 3-2-1: tenga al menos tres copias de sus datos, guárdalos en dos medios diferentes y mantenga uno fuera del sitio. Dependiendo del tipo de copia de seguridad,

puede programar las copias de seguridad diarias, semanales, mensuales o manualmente. Por ejemplo, puede hacer una copia de seguridad completa una vez al mes, una copia de seguridad incremental todos los días y una copia de seguridad de archivos cuando sea necesario. También puede utilizar las herramientas integradas de Windows, como Copia de seguridad y restauración, Historial de archivos o Imagen del sistema; o software de terceros para automatizar sus copias de seguridad y establecer recordatorios.

Estrategia de copia de seguridad 3-2-1

Una estrategia de copia de seguridad 3-2-1 es un método para garantizar que sus datos estén adecuadamente duplicados y puedan recuperarse de forma fiable. En esta estrategia, se crean tres copias de sus datos en al menos dos medios de almacenamiento diferentes y al menos una copia se almacena de forma remota:

Tres copias de datos:

Las tres copias incluyen los datos originales y dos duplicados. Esto garantiza que una copia de seguridad perdida o un soporte dañado no afecten a la capacidad de recuperación.

Dos tipos de almacenamiento diferentes:

Reduce el riesgo de fallos relacionados con un medio específico utilizando dos tecnologías diferentes. Las opciones más comunes incluyen discos duros internos y externos, medios extraíbles o almacenamiento en la nube.

Una copia externa:

Elimina el riesgo asociado a un único punto de fallo. Los duplicados externos son necesarios para estrategias sólidas de recuperación de datos en caso de desastre y pueden permitir la conmutación por error durante interrupciones locales.

La mayoría de los expertos en seguridad de la información y las autoridades gubernamentales consideran que esta estrategia es una buena práctica. Protege tanto de accidentes como de amenazas maliciosas, como el ransomware, y garantiza la fiabilidad de las copias de seguridad y la restauración de los datos.

La importancia del rendimiento de un backup

El backup de las bases de datos es una tarea crucial, pero también puede afectar en el rendimiento y la disponibilidad del sistema. El rendimiento del backup no se trata solo de rapidez en la que se completara la misma, sino también los recursos que consumirá y el tiempo de inactividad que causara.

Una backup lenta o ineficiente puede degradar el rendimiento del servidor en el que está alojada la base de datos afectando así el tiempo de respuesta de las operaciones que necesitemos.

¿Cómo ajustar y optimizar el rendimiento del backup?

Puntos a tomar en cuenta para mejorar el rendimiento de las copias de seguridad:

- **Programar backups durante períodos de baja actividad**: Realizar las copias de seguridad durante las horas de menor uso para minimizar el impacto en los usuarios.

- **Elegir el tipo de backup adecuado**: Usar estrategias que equilibren velocidad, consumo de recursos y facilidad de restauración.
- **Optimizar la configuración del sistema**: Ajustar parámetros del sistema y de la base de datos para mejorar la eficiencia del proceso de copia de seguridad.
- **Evitar la sobrecarga en el almacenamiento**: Implementar estrategias para gestionar el espacio, como eliminar versiones obsoletas o comprimir archivos.

Cifrado de los backups

El cifrado de los backups es el proceso de convertir los datos de backup de un formato legible a un formato seguro que es ilegible sin una clave de descifrado o contraseña especial. Esto garantiza que, aunque personas no autorizadas accedan a los datos de backups, no puedan ser leídos, utilizados o expuestos sin las credenciales adecuadas, que sólo están disponibles para los usuarios autorizados. El cifrado de los backups es una medida de seguridad clave para proteger la información confidencial de robos, pérdidas o exposición durante su almacenamiento y transferencia.

Importancia de cifrar los backups

- **Cumplimiento y normativa**:

Algunas categorías de empresas deben cumplir determinados requisitos normativos, como el Reglamento General de Protección de Datos (RGPD) de la UE, el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS), la Ley de Privacidad del Consumidor de California (CCPA), la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA), la Ley de Informes para Infraestructuras Críticas (CIRCIA), SOC 3 (Controles de Sistemas y Organización 3), etc. Estas normas reglamentarias imponen a las organizaciones el cifrado de los datos durante su almacenamiento y transferencia.

- **Mejora de la seguridad general**:

Los backups cifrados añaden una capa a la seguridad y mejoran la estrategia de protección de datos. Almacenar los backups en un formato cifrado hace que sea más seguro transportar los datos de backup en soportes de almacenamiento extraíbles, como discos duros, a otra ubicación (por ejemplo, un sitio de recuperación ante desastres situado en otra región geográfica). Si se pierde o roban un soporte portátil con backups cifrados, un tercero no podrá acceder a datos críticos y confidenciales.

- **Algoritmos de cifrado**

Para cifrar los datos se utilizan complejos algoritmos matemáticos y claves de cifrado y descifrado. Para mayor comodidad, el software puede transformar una contraseña o frase de contraseña en una clave de cifrado de la longitud adecuada. Este método permite a los usuarios memorizar sus contraseñas, lo que resulta más fácil que aprender largas claves de cifrado. La eficacia del cifrado para los backups, al igual que para otros datos, depende del algoritmo de cifrado.

Existen algoritmos de cifrado simétricos y asimétricos. En los algoritmos simétricos, se utiliza una sola clave para cifrar y descifrar datos. En los algoritmos asimétricos, se utiliza un par de claves: una clave pública para cifrar los datos y una clave privada para descifrarlos.

Advanced Cifrado Standard (AES) es uno de los algoritmos de cifrado más utilizados en la actualidad por su alto nivel de seguridad. La longitud de la clave es importante y define durante cuánto tiempo los datos cifrados pueden considerarse seguros y protegidos. Una clave de 128 bits debería bastar para proteger los datos hasta tres años. Las claves más largas compatibles son las de 192 y 256 bits.

AES-256 garantiza el máximo nivel de seguridad con una longitud de clave de 256 bits. Se necesitan miles de años para forzar una clave de descifrado AES-256 (teniendo en cuenta el rendimiento máximo de los ordenadores modernos). El gobierno estadounidense lleva utilizando AES para proteger datos desde 2003. Este algoritmo criptográfico fue bien probado y aprobado por expertos en criptografía.

Ventajas de las copias de seguridad

- **Prevención de pérdidas de datos:**

  Los backups evitan la pérdida de información valiosa, como archivos de clientes, documentos importantes o datos de la empresa.

- **Seguridad de los datos:**

  Protegen los datos de posibles ataques cibernéticos, errores humanos o fallos técnicos, lo que reduce el riesgo de comprometer la información.

- **Facilidad de recuperación:**

  Permiten restaurar la información rápidamente en caso de pérdida o daño, minimizando el tiempo de inactividad y los costos de recuperación.

- **Ahorro de tiempo y recursos:**

  Automatizan el proceso de copia de seguridad, liberando a los usuarios de la tarea de realizar copias manualmente y permitiendo un uso más eficiente de los recursos.

- **Accesibilidad:**

  Facilita el acceso a la información desde cualquier lugar y dispositivo, lo que permite una gestión más flexible y una recuperación rápida en caso de problemas con el sistema principal.

- **Mejora la confianza de los clientes:**

  La protección de los datos es una prioridad para muchos clientes, y la realización de backups demuestra el compromiso de la empresa con la seguridad de la información.

Desventajas de la copia de seguridad de la base de datos

Las copias de seguridad requieren un espacio de almacenamiento considerable, especialmente si se conservan varias versiones de datos.

- **Tiempo de ejecución:** La copia completa de la base de datos tarda más tiempo que las copias incrementales o diferenciales.
- **Dependencia de Internet:** Las copias de seguridad en la nube requieren acceso a Internet, lo que puede causar problemas con el ancho de banda y la disponibilidad de los datos.
- **Costo:** El costo de almacenamiento en la nube puede ser significativo para grandes cantidades de datos.
- **Vulnerabilidad a desastres:** Las copias de seguridad locales son susceptibles a desastres naturales, incendios, robos, etc.
- **Problemas de configuración:** Una configuración incorrecta del sistema de copia de seguridad puede provocar la pérdida de datos o la corrupción de archivos.
- **Fallos de hardware y software:** Los sistemas de copia de seguridad dependen del hardware y software, ambos vulnerables a fallos por parte de distintas fuentes.

Conclusión

La implementación de estrategias de respaldo y recuperación de bases de datos constituye una práctica esencial en la gestión de la información organizacional. Estas estrategias no solo mitigan riesgos asociados a fallos técnicos, errores humanos o ciberataques, sino que también aseguran la continuidad operativa y el cumplimiento de normativas legales. En este contexto, el uso de diferentes tipos de copias de seguridad, como los respaldos completos, incrementales, entre otros, permite adaptar los procedimientos a las características y necesidades específicas de cada entorno tecnológico.

Asimismo, la frecuencia de ejecución de las copias de seguridad, la adopción de esquemas como la estrategia 3-2-1, y la elección entre almacenamiento local, remoto o en la nube, son factores determinantes para una política de respaldo eficiente. La automatización del proceso, la optimización del rendimiento y la incorporación de mecanismos de cifrado contribuyen significativamente a garantizar la seguridad y disponibilidad de los datos.

Igualmente, es importante reconocer que los sistemas de respaldo también traen complicaciones varias, tales como el consumo de recursos, la dependencia de la conectividad en entornos en la nube, los costos asociados y los posibles errores de configuración. Por tanto, resulta indispensable realizar pruebas periódicas de restauración y mantener actualizados los procedimientos técnicos y operativos. En conclusión, una estrategia integral de backup no solo protege la información crítica de una organización, sino que fortalece su resiliencia frente a incidentes imprevistos.

Referencias:

Cohesity. (s.f.)
¿Que es un backup?

Fivetran. (2023)
Beneficios de un backup

DigitalOcean. (2024)
¿Que es un backup? de Digital Ocean

AWS, Amazon. (s.f.)
¿Cuál es la diferencia entre las copias de seguridad incrementales, diferenciales y otras?

NetApp. (s.f.)
¿Que es un backup?

ADR Formación. (s.f.)
Tipos de backups

Linkedin. (s.f.)
Impacto de los backups en el rendimiento de la base de datos

Nakivo. (2024)
Cifrado de backups