Taller Noviembre 21 de 2024:

**Respaldo y Recuperación en Bases de Datos**

**1.Preguntas Teóricas**

**1.1. Diferencias entre respaldos completos, incrementales y diferenciales.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Tipo de Respaldo** | **Características** | **Ventajas** | **Desventajas** |
| ***Completo*** | Copia todos los datos en un único archivo o conjunto. | **-** Implementación simple.  **-** Recuperación rápida y autónoma. | **-** Alto consumo de tiempo y espacio.  **-** Poco eficiente para bases dinámicas. |
| ***Incremental*** | Copia solo los cambios desde el último respaldo. | **-** Optimiza espacio y tiempo.  **-** Ideal para datos con cambios frecuentes. | **-** Recuperación más compleja (requiere respaldo completo y todos los incrementales). |
| ***Diferencial*** | Copia cambios desde el último respaldo completo. | **-** Recuperación más rápida que el incremental.  **-** Menos espacio que respaldos completos. | **-** Se incrementa el tamaño del respaldo hasta el próximo completo. |

**1.2. RPO y RTO**

|  |  |  |
| --- | --- | --- |
| **Concepto** | **Descripción** | **Ejemplo** |
| **RPO (Recovery Point Objective)** | Define la cantidad máxima de datos que se pueden "perder" sin afectar gravemente al negocio. | Un RPO de 15 minutos implica configuraciones de respaldo cada 15 minutos. |
| **RTO (Recovery Time Objective)** | Determina el tiempo máximo permitido para restaurar la operación tras un fallo. | Un RTO de 2 horas exige que los sistemas vuelvan a estar operativos en ese plazo o menos. |

**2.Caso Practico 1: Plan de Respaldo**

**Propuesta de Método de Respaldo:**

**Método:** Recomendaría usar un método de respaldo incremental combinado con respaldos completos periódicos.

**Respaldo Completo:** Se hace una copia de seguridad completa de todos los datos.

Esto proporciona una base completa de la cual partir.

**Respaldo Incremental:** Solo copia los datos que han cambiado desde el ultimo respaldo (ya sea completo o incremental). Esto ahorra tiempo y espacio de almacenamiento.

**Resumen del Plan:**

**·Método:** Respaldo Completo semanal + Respaldo Incremental diario.

**·Frecuencia:** Completo cada semana e Incremental cada día.

**·Recursos:** Al menos 9.4 TB de espacio (8 TB para completos y 1.4 TB para incrementales), costos de almacenamiento y software de respaldo, y tiempo de respaldo variando de 33 minutos a 5.5 horas según el tipo.

**Justificación:**

Este plan balancea la necesidad de tener una copia de seguridad completa y actualizada con la eficiencia en términos de espacio y tiempo.

**3. Caso Práctico 2: Estrategia de Recuperación**

**Pasos para Recuperación tras Ransomware:**

1. Desconectar el sistema afectado para contener el ataque.
2. Verificar respaldos en un entorno aislado.
3. Restaurar datos siguiendo el orden: respaldo completo > incrementales.
4. Auditar el sistema para asegurar la limpieza total del ransomware.

**Prevención Futura**

*Medidas Técnicas:*

**·** Respaldos fuera de línea.

**·** Monitoreo avanzado con detención en tiempo real

*Medidas Organizativas:*

**·** Pruebas periódicas de restauración.

**·** Formación continua para prevenir phishing y amenazas similares.

**4.Evaluacion de Simulación**

**Pasos para la Prueba:**

1. **Planificación:** Definir objetivos y seleccionar un entorno de prueba.
2. **Preparación:** Configurar un entorno de prueba similar al de producción
3. **Respaldo:** Realizar un respaldo completo de la base de datos actual.
4. **Simulación de Fallo:** Simular un fallo en la base de datos.
5. **Recuperación:** Restaurar la base de datos usando los respaldos.
6. **Validación:** Verificar la integridad y consistencia de los datos restaurados.

**Indicadores de Éxito:**

1. **Tiempo de Recuperación (RTO):** Medir el tiempo total de recuperación.
2. **Punto de Recuperación (RPO):** Evaluar la perdida de datos.
3. **Consistencia e Integridad:** Verificar que todos los datos sean correctos y completos.

**Documentos:**

1. **Informe:** Resumen del objetivo, alcance y pasos seguidos.
2. **Resultados:** Tiempos de recuperación (RTO y RPO) y observaciones.
3. **Lecciones Aprendidas:** Problemas encontrados y recomendaciones.
4. **Plan de Acción:** Pasos para corregir deficiencias y actualizaciones necesarias.

**5.Reflexion Final**

Una estrategia solida de respaldo y recuperación es clave para garantizar la continuidad del negocio.   
Tomemos el ejemplo de una tienda en línea. Puede evitar pérdidas económicas al restaurar sus operaciones rápidamente tras un incidente. Este enfoque no solo protege los ingresos, sino que también mantiene la confianza del cliente y asegura el cumplimiento de los acuerdos de nivel de servicio (SLA).