Manual de explotación del sistema

Índice

[1 Calendario de operaciones a realizar 2](#_Toc533345518)

[2 Dispositivos de almacenamiento secundario 2](#_Toc533345519)

[3 Realización de copias de seguridad 2](#_Toc533345520)

[4 Clasificación y acceso de copias de seguridad 2](#_Toc533345521)

[5 Monitorización y gestión de la capacidad 2](#_Toc533345522)

[6 Emisión de informes a petición 2](#_Toc533345523)

[7 Establecimiento de puntos de restauración del sistema 2](#_Toc533345524)

[8 Salvado de la base de datos 2](#_Toc533345525)

[9 Tareas de mantenimiento de los equipos 2](#_Toc533345526)

[10 Responsables directos de cada funcionalidad de sistema 2](#_Toc533345527)

[11 Actuaciones ante sistemas de riesgo 2](#_Toc533345528)

[12 Rotación de logs. Periodicidad 2](#_Toc533345529)

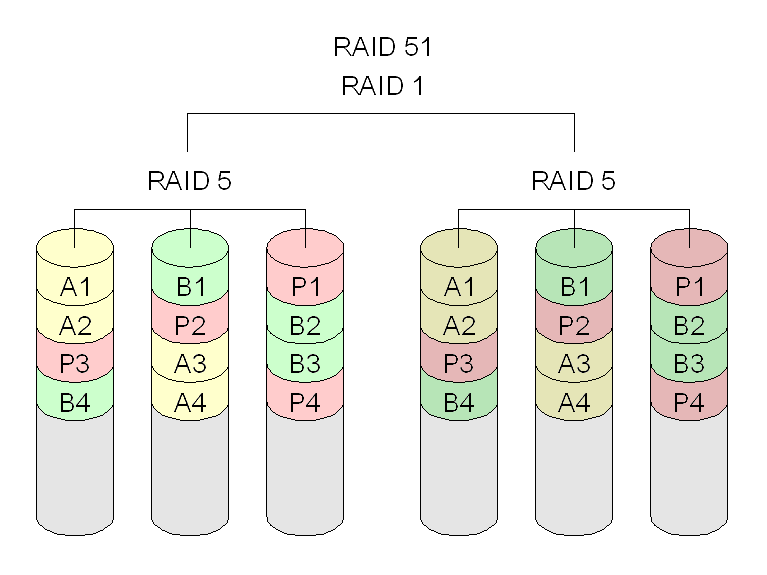
# Calendario de operaciones a realizar

# Dispositivos de almacenamiento secundario

El equipo que tiene la base de datos guardará sus archivos en un RAID1 que montará encima de un RAID5, esta configuración se conoce como RAID51. Se utilizará el RAID5 de forma habitual para el trabajo, ya que este modo de agrupar los discos proporciona seguridad y rendimiento en partes iguales sin comprometer ninguno de los dos. Es especialmente útil cuando se produce un fallo en uno de los discos, pues asi podremos recuperar información de los discos utilizando una operación xor a lo largo del resto de sectores de los discos que se encuentran en el mismo nivel de RAID.

Se aprovechará el RAID1 como un backup de la información almacenada en el RAID 5, de modo que según se está utilizando la base de datos se estará realizando simultáneamente una copia de seguridad a nivel hardware, duplicando todos los datos en el caso de un fallo masivo del sistema este podría afectar a uno de los RAID5, colgando del RAID1. De modo que desde la otra rama del RAID1 se podría restaurar al completo toda la información, sin perder ningún dato.

Esta jerarquía de RAID proporcionaría especiales ventajas en aplicaciones concurrentes, ya que se podrá leer de ambas ramas del RAID1 de forma simultanea en un mismo nivel de disco y sectores distintos.

[](https://upload.wikimedia.org/wikipedia/commons/0/06/RAID_51.png)

# Realización de copias de seguridad

Se realizará una copia de seguridad de la base de datos de forma automática diariamente y una vez al mes se realizará la copia de seguridad de los archivos de la base de datos. De esta forma logramos garantizar la recuperación de los datos ante una posible caída del servidor, pero sin una excesiva sobrecarga de datos.

Las copias de seguridad diarias se realizarán una vez se haya finalizado la jornada laboral de los trabajadores, así logramos almacenar todos los cambios producidos sin afectar a la actividad normal de la empresa. En estas copias, se guardará únicamente el diario del sistema, que garantiza copias de seguridad fiables, pero gastando un tiempo para realizar la recuperación elevado.

Por otro lado, se realizará copias mensuales del cluster de la base de datos se realizarán el último lunes de cada mes.

Mientras que se realizan las copias de seguridad, habrá un técnico de nuestra empresa disponible de forma presencial o telemática con la finalidad de subsanar de manera inmediata los posibles errores que puedan producirse.

# Clasificación y acceso de copias de seguridad

Como se ha mencionado en el punto anterior, tenemos dos tipos de copias de seguridad. Unas hechas sobre el cluster y otras hechas sobre el diario del sistema. Exponemos a continuación como las utilizaremos para restaurar el sistema en caso de fallo.

En caso de fallo, las copias de seguridad serán accesibles mediante una conexión SSH al servidor de modo que de forma remota se podría cambiar el disco de operación de la base de datos de uno de los RAID5 (el que está dañado) al otro quedando el que estaba dañado inutilizado. El disco no dañado, se comenzará a utilizar como si fuera un RAID5 aislado, es decir, fuera de la arquitectura RAID 51. Sobre el disco inutilizado se comenzará a realizar la restauración de la base de datos. Primero se intentará restaurar a partir del diario de sistema, en caso de que esto falle se procederá a restaurar el ultimo cluster guardado y sobre él restaurar con el diario del sistema, en caso de que esto tampoco subsane el problema, se esperaría a la hora de fin de actividad de la empresa para replicar el RAID5 en estado correcto, sobrescribiendo el RAID5 dañado.

La ventaja de este procedimiento es que permite a la empresa mantener su actividad aun en caso de fallo crítico del sistema.

Respecto a las caídas del sistema debido a causas externas, se recurriría al ultimo diario del sistema generado por la base de datos.

# Monitorización y gestión de la capacidad

Se utilizará los recursos proporcionados por el sistema operativo LINUX, utilizado para mantener la base de datos

# Emisión de informes a petición

# Establecimiento de puntos de restauración del sistema

# Salvado de la base de datos

# Tareas de mantenimiento de los equipos

# Responsables directos de cada funcionalidad de sistema

# Actuaciones ante sistemas de riesgo

# Rotación de logs. Periodicidad