MANUAL DE EXPLOTACIÓN DEL SISTEMA

Índice

1 Calendario de operaciones a realizar

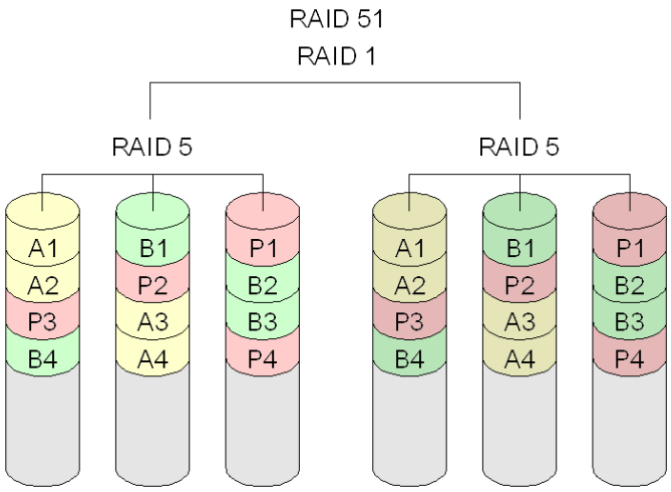
Realizaremos tres copias de seguridad: una de los archivos log del sistema (una del diario del sistema que se realiza una vez a la semana y otra del cluster, que se realiza una vez al mes), además guardaremos otra serie de logs que almacene los emails enviados y los ficheros descargados (que se realizarán al producirse uno de estos eventos).

2 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.



3 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.

Se incluirá un archivo de script copiaSeguridad.sh mediante el cual se mostrará toda la información de las copias de seguridad almacenadas, así como el estado del sistema en el momento de la ejecución del script. Mediante la opción -s del script se forzará la creación de una copia de seguridad del diario del sistema nueva y con la opción -c también se guardará el cluster.

4 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.

5 Monitorización y gestión de la capacidad

Se utilizará los recursos proporcionados por el sistema operativo LINUX, utilizado para mantener la base de datos como método de monitorización de la capacidad. El servidor periódicamente tomará el estado de la capacidad para generar una gráfica de la evolución de esta, calculando la derivada del crecimiento se podrá estimar el estado de llenado de los discos en un futuro. Cuando los discos alcancen una capacidad del 80%, se notificará en nuestra oficina central, momento en el cual nos pondremos en contacto con la empresa para notificarles la situación y las posibilidades de expansión de su capacidad. En el caso general, se expandirá ambos discos RAID5 con discos nuevos adicionales que podrán insertarse mientras el sistema sigue activo. El total de discos a añadir dependerá de la configuración de RAID51 aplicada, siendo estos un mínimo de 4 discos.

Vm_stat : mediante este comando podremos obtener información de la memoria ocupada por los programas en curso. Podremos usar esta información, en concreto, la referente a páginas ocupadas y buffers ocupados para estimar la repercusión en disco de los programas, ya sea, por el uso en memoria en swap o por la memoria que ocupará al guardar sus datos cuando termine su ejecución.

Top: mediante este comando obtendremos información de las cachés que nos permitirá gestionar la cantidad de RAM que deberemos instalar en función del tamaño de disco que tengamos (debemos contar solo una de las ramas del RAID1)

Df: mediante este comando podremos ver el peso de los archivos en disco. Gracias a el, podremos determinar cada cuanto borrar los log, según su crecimiento. También nos servirá para estimar cuantas copias de seguridad guardar, de modo que podamos maximizar el tiempo que las guardemos dentro de unos márgenes de disco ocupado. Además, utilizaremos el comando para realizar las estimaciones explicadas al principio, pues nos permite conocer la cantidad de disco que esta asignada a cada archivo.

Se incluirá un archivo de script monitor.sh mediante el cual se mostrará toda la información almacenada, así como el estado del sistema en el momento de la ejecución del script.

Mediante la opción -i del script se forzará la creación de una copia de seguridad nueva en la cual se almacene la información almacenada y añadiendo la opción -e se almacenará también el estado en el que se encontraba.

6 Emisión de informes a petición

Nuestro sistema se encarga de la emisión de los informes de beneficios, resumen de trabajo e informes de trabajo de cada uno de los técnicos.

Dichos informes serán visibles para el coordinador técnico y se generarán automáticamente por parte del sistema. El periodo de generación de dichos informes es configurable desde la clase timer. Para poder hacerlo, hay que cambiar las suscripción del sistema a los timer que genera. Cuando generamos una suscripción timer debemos configurar en su constructor dos parámetros: el periodo de llamada y el método que será llamado en plazos del periodo.

El informe de beneficios se genera mensualmente (por defecto), en él encontramos un resumen económico del mes. Podemos consultar los ingresos totales y un control de gastos (podemos ver la cantidad de dinero que se ha destinado a la compra de las piezas, el pago a los trabajadores y los gastos adicionales que se hayan producido), también podemos consultar el salario medio de los técnicos y el beneficio medio.

El resumen de trabajo se genera semanalmente (por defecto), en él se refleja la cantidad de peticiones de trabajo nuevas recibidas, la media de peticiones que se suele recibir (para ello se usan resúmenes de trabajo generados anteriormente), el numero de partes de trabajo finalizados y en estado pendiente de realizar. También obtenemos una tasa de acumulación (muy útil a la hora de decidir si es necesario contratar personal adicional) y el personal extra que se ha tenido que contratar ese mes.

7 Establecimiento de puntos de restauración del sistema

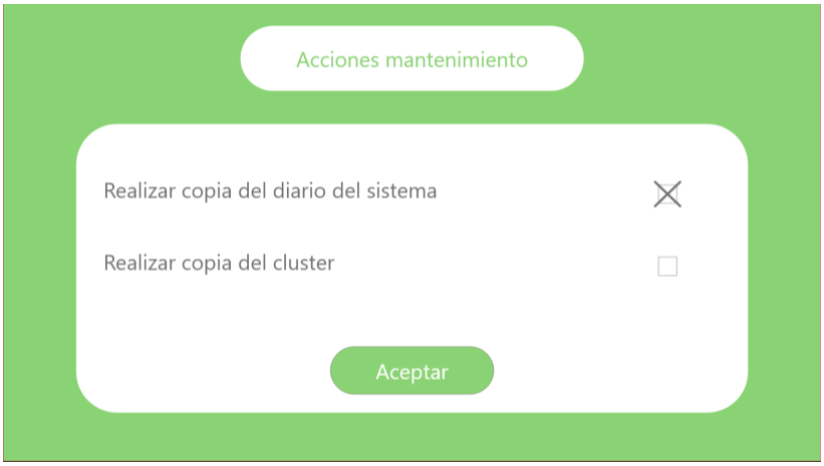
Con la utilidad systemback podremos crear puntos de recuperación de todo el sistema. Ya que la mayoría de la información esta almacenada en una base de datos de la que realizamos copias de seguridad con gran frecuencia, solo se realizara punto de restauración de todo el sistema antes de realizar actualizaciones de este y como mínimo una vez al año. La creación de los puntos de restauración utiliza el mismo patrón que la creación de copias de seguridad, es decir, se harán durante las horas de inactividad de la empresa con uno de nuestros técnicos disponibles de manera presencial o telemáticamente.

Se incluirá un archivo de script restauracion.sh mediante el cual se mostrara toda la información almacenada, asi como el estado del sistema en el momento de la ejecución del script.

Ejecutando este script se realizará un systemback de modo que el personal de mantenimiento podrá ejecutarlo cuando sea necesario. Mediante la opción -i del script se forzará la creación de una copia de seguridad nueva en la cual se almacene la información almacenada y añadiendo la opción -e se almacenará también el estado en el que se encontraba.

8 Salvado de la base de datos

Los datos almacenados en la base de datos se salvarán tras finalizar la jornada laboral. Dicha información incluye clusters (realizados mensualmente) y diarios del sistema (realizados semanalmente). Antes de realizar cualquier tipo de copia de seguridad, aparecerán a lo largo del día avisos de la necesidad de realizar una copia de seguridad dicho día. En caso de que se deniegue la realización de la copia de seguridad se guardará un archivo donde esto se indicará. Adicionalmente, y solo en el caso de las copias de seguridad del cluster se continuará solicitando realizar una copia de seguridad hasta que esta sea realizada.



Ejemplo de interfaz para guardar las copias de seguridad

9 Tareas de mantenimiento de los equipos

Los equipos de escritorio se hará un mantenimiento en el que se eliminaran los archivos temporales que haya podido generar el sistema en el caso de que se reporte una ralentización. Durante el primer año de la implantación del sistema, una vez al mes y a partir del primer año de manera anual, un técnico de nuestra empresa visitará a los coordinadores técnicos y responsables de almacén y a un total de 10 técnicos informáticos de NOANDA para obtener un feedback de su experiencia de usuario. Con dicha información se implementarán mejoras de la aplicación, de modo que se adapte a las necesidades de los usuarios. Adicionalmente, se pretende encontrar posibles fallos o malfuncionamientos de la aplicación que serán subsanados según sean detectados.

10 Responsables directos de cada funcionalidad de sistema

Ante posibles fallos que hayan podido producirse en las aplicaciones móviles utilizadas por los técnicos, estos deberán ponerse en contacto con su coordinador técnico. Sin embargo, si los fallos producidos se dan en las aplicaciones de escritorio encontramos dos responsables funcionales: en caso de que los fallos sean relativos a la gestión de las peticiones, de los técnicos o de los clientes quien debería solucionarlo sería el coordinador técnico de la empresa mientras que si dichos errores son relativos a la gestión de piezas o proveedores deberá ser el jefe de los responsables de almacén quién trate de subsanar el problema.

Además, ante posibles errores de mayor complejidad que pudieran darse se contará con el apoyo de uno de los miembros que hayan participado en el proceso de desarrollo de la aplicación, ya que dichos miembros conocerán más a fondo el funcionamiento interno de la aplicación y el motivo por el cuál podrían estar produciéndose los fallos. Dicho responsable garantizará que tratará de resolver el problema lo más rápido posible para así garantizar la satisfacción del cliente con el servicio de mantenimiento dado.

11 Actuaciones ante sistemas de riesgo

Ante cualquier situación anómala que pudiera darse que necesite una restauración de la base de datos, se tratará de rehalizar con la mayor rapidez posible usando la última copia del diario de sistema que se encuentre disponible, en caso de que no fuera posible se trataría de restaurar el sistema utilizando el último cluster del que se tenga una copia creada.

RECURSO	PROBLEMA RELACIONADO (riesgo asumido)	
	Posibilidad de ocurrencia del sistema	Periodo de para aceptable
Aplicación de escritorio	Media	2 horas
Sistema con la base de datos central	Baja	30 minutos
Aplicación móvil	Media/alta	1 día

Tanto las aplicaciones de escritorio como las móviles estarán cometidas a fuertes medidas de testeo con la finalidad de evitar la mayor cantidad de fallos posible.

En caso de fallo de una aplicación móvil, deberá estar presente el superior del usuario al que el sistema le haya dado fallo. Al técnico podrá proporcionársele otro dispositivo por o que la reparación de la aplicación no es tan urgente y podrá retrasarse hasta un día laboral.

Fase 1 Acudirá un técnico de nuestra empresa a la oficina donde se haya producido el error
Fase 2 Se proporcionará un dispositivo de reemplazo para el técnico afectado
Fase 3 Se procederá a la reparación de la aplicación
3.1 Un técnico de nuestra empresa procederá a guardar manualmente los registros de los cambios ocurridos en el sistema
3.2 Se procederá a la reinstalación de la aplicación en el dispositivo afectado
Fase 4 Se procederá a la devolución del dispositivo reparado y se retirará el dispositivo de sustitución.

En el caso de las aplicaciones de escritorio, el procedimiento es similar a las aplicaciones móviles, aunque tendrán mayor prioridad debido a que los sistemas de escritorio no son reemplazables. El periodo estimado de inactividad se corresponde con el tiempo estimado que se tardara en reinstalar el sistema.

Fase 1 Un técnico de nuestra empresa procederá a guardar manualmente los registros de los cambios ocurridos en el sistema
Fase 2 Se procederá a la reinstalación de la aplicación en el dispositivo afectado

En caso del sistema con la base de datos central, existirá un control exhaustivo de toda la actividad producida en el de modo que se puedan prevenir los fallos antes de que ocurran en el, adicionalmente y debido a que este es un sistema crítico será la parte sobre la que mayor cantidad de pruebas se realicen. El tiempo de inactividad indicado se corresponde con el que, en el peor de los casos, se debería tardar en cambiar manualmente la configuración RAID51 para sacar los discos dañados, dejando únicamente aquellos discos en estado correcto.

12 Rotación de logs. Periodicidad

Con la información obtenida de df (comando explicado en el apartado de la monitorización y gestión de la capacidad), se establecerá un tamaño de ventana de tamaño máximo de un 1Gbyte para la suma de las capacidades de os archivos de log. Una vez esta ventana se complete se procederá a eliminar cronológicamente los logs (por lo que los primero en eliminarse serán los más antiguos).

Se creará un log para cada email enviado y otro para cada informe descargado, dichos logs serán almacenados en el sistema que este hosteando la base de datos central.

Los log de la base de datos (el diario del sistema) lo manejamos como ya ha sido explicado anteriormente y dichos log se almacenan durante el periodo de un trimestre.