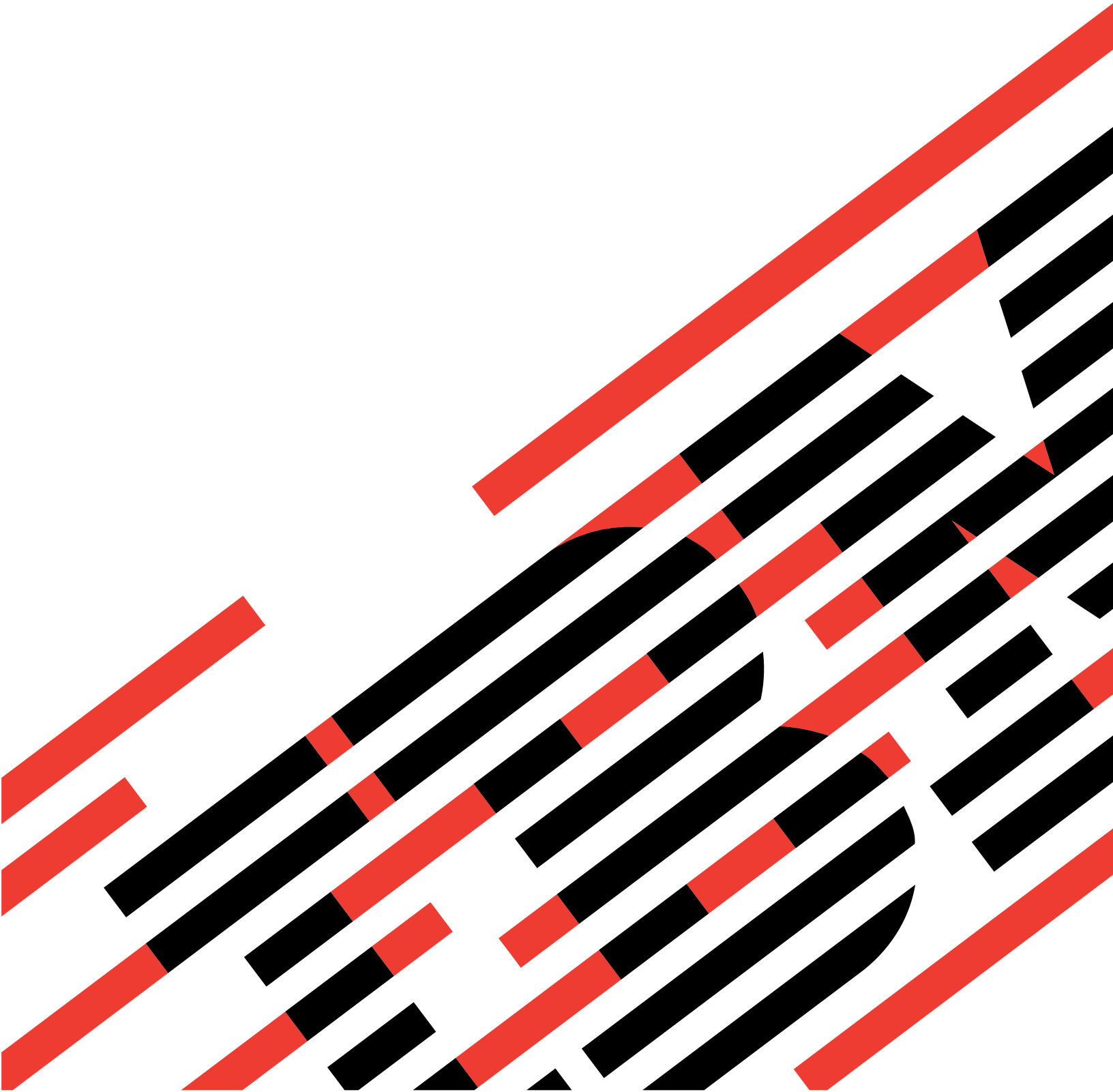
IBM

eserver

iSeries

Protección de disco



IBM

@server

iSeries

Protección de disco

Contenido

Parte 1. Protección de disco

Además de tener una estrategia de copia de seguridad y recuperación operativa, también es conveniente utilizar algún tipo de protección para los datos del sistema. La manera de hacerlo es utilizar protección de disco. La protección de disco puede ayudar a evitar una pérdida de datos, y puede mantener el sistema en funcionamiento si se produce una anomalía de disco. Hay varios métodos de protección de disco que puede utilizar como ayuda para proteger los datos. Puede utilizar estos métodos combinándolos de diferentes maneras.

Puede utilizar los asistentes de gestión de discos de iSeries Navigator como ayuda para configurar las agrupaciones de discos y protegerlas con protección por paridad de dispositivos o protección por duplicación de disco.

Recuerde: aunque la protección de disco puede reducir el tiempo de inactividad o acelerar la recuperación, **no** deja de ser necesario efectuar copias de seguridad regulares. La protección de disco no puede ayudarle a efectuar una recuperación de una pérdida total del sistema, una anomalía de procesador o una anomalía de programa.

Los siguientes temas proporcionan información sobre diferentes tipos de protección de disco, así como de su utilización combinada:

- Elección de las herramientas de protección de disco
- Elección del nivel de protección

Antes de continuar, puede que desee consultar los siguientes temas:

- Cómo gestiona el sistema el almacenamiento auxiliar
- Cómo se configuran los discos

Capítulo 1. Elección de las herramientas de protección de disco

Cuando piense en la protección del sistema contra las pérdidas de datos, deberá tener en cuenta lo siguiente:

Recuperación
¿Puede recuperar la información perdida, ya sea restaurándola desde un medio de copia de seguridad o creándola de nuevo?

Disponibilidad
¿Puede reducir o eliminar el tiempo que el sistema deja de estar disponible cuando aparece un problema?

Servicio
¿Puede dar servicio al sistema sin que esto afecte al usuario de los datos?

La principal defensa contra las pérdidas de datos es una estrategia de copia de seguridad y recuperación adecuada. Es necesario realizar una planificación para guardar con regularidad la información del sistema.

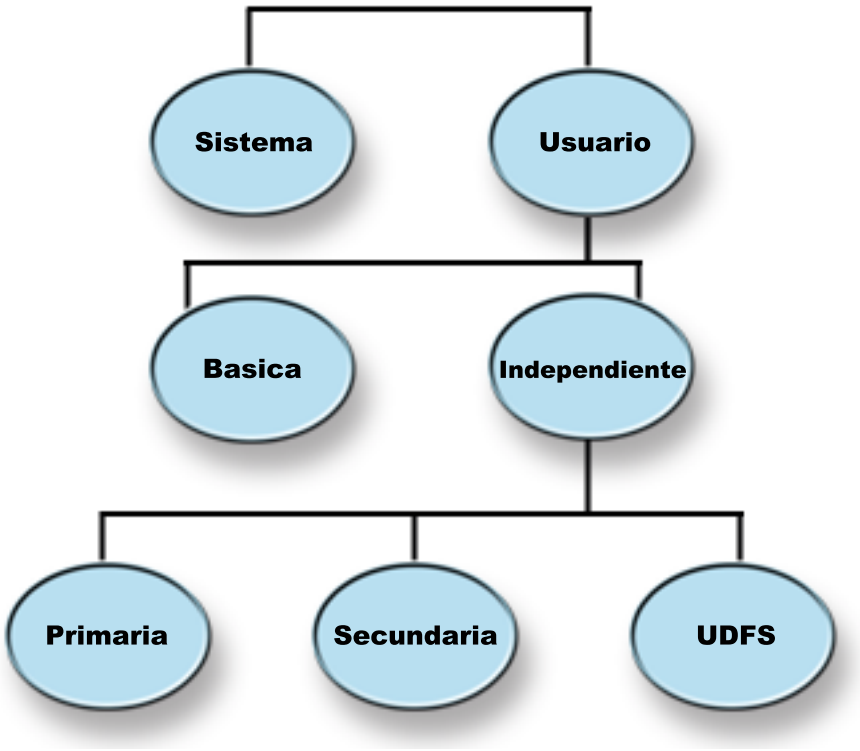
Existen varias herramientas de disponibilidad de disco para reducir o eliminar el tiempo de inactividad del sistema, y contribuir a la recuperación de los datos tras una anomalía de disco:

- Agrupaciones de discos
- Protección por paridad de dispositivos
- Protección por duplicación de disco

Agrupaciones de discos

Una agrupación de discos, también denominada agrupación de almacenamiento auxiliar (ASP) en la interfaz basada en caracteres, es una definición de software de un grupo de unidades de disco del sistema. Esto significa que una agrupación de discos no se corresponde necesariamente con la disposición física de los discos. Conceptualmente, cada agrupación de discos del sistema es una agrupación separada de unidades de discos para almacenamiento de nivel único. El sistema reparte los datos entre las unidades de disco de una agrupación de discos. Si se produce una anomalía de disco, sólo deberá recuperar los datos de la agrupación de discos en la que se ha producido la anomalía. Hay dos categorías principales de agrupaciones de discos: la agrupación de discos del sistema y las agrupaciones de discos de usuarios. Hay dos tipos de agrupaciones de discos de usuario: básicas e independientes. Las agrupaciones de discos independientes se dividen, a su vez, en agrupaciones de discos primarias, secundarias y UDFS. Consulte los siguientes enlaces y la figura de la agrupación de discos para comprender los distintos tipos de agrupaciones de discos de usuario:

- Agrupación de discos del sistema
- Agrupaciones de discos de usuario



El sistema puede tener muchas unidades de discos conectadas para el almacenamiento de la agrupación de discos. No obstante, el sistema las ve como una única unidad de almacenamiento. El sistema reparte los datos por todas las unidades de discos. Puede utilizar las agrupaciones de discos para separar las unidades de discos en subconjuntos lógicos. Si desea conocer más ideas sobre cómo utilizar las agrupaciones de almacenamiento auxiliar en el sistema, consulte el enlace Agrupaciones de discos — ejemplos de uso.

Cuando asigna las unidades de disco del sistema a más de una agrupación de discos, cada agrupación de discos puede tener distintas estrategias de disponibilidad, copia de seguridad/recuperación y rendimiento.

Las agrupaciones de discos proporcionan una ventaja en la recuperación si el sistema sufre una anomalía en la unidad de discos que provoca la pérdida de datos. Si esto ocurre, la recuperación sólo se necesita para los objetos de la agrupación de discos que contiene la unidad de discos anómala. Los objetos de sistema y los objetos de usuario de las demás agrupaciones de discos están protegidos de la anomalía del disco. También hay ventajas adicionales, así como ciertos costes y limitaciones, inherentes a la utilización de agrupaciones de discos.

Si desea obtener más información sobre las agrupaciones de discos de usuario, consulte los siguientes temas:

- Decidir cómo configurar las agrupaciones de discos de usuario
- Considerar la creación de una agrupación de discos nueva en un sistema activo
- Comprobar que el sistema dispone del suficiente espacio de trabajo
- Comparar las agrupaciones de discos básicas e independientes

Si desea obtener información sobre cómo implementar las agrupaciones de almacenamiento auxiliar en su empresa, consulte la Guía de copia de seguridad y recuperación.

Decidir cómo configurar las agrupaciones de discos de usuario

Puede utilizar las agrupaciones de discos para varios propósitos distintos, en función de las necesidades de la empresa. Antes de configurar cualquier agrupación de discos de usuario, examine los siguientes temas que describen sus distintos usos.

- Utilización de agrupaciones de discos para tener disponibilidad
- Utilización de agrupaciones de discos para tener un mayor rendimiento
- Utilización de agrupaciones de discos con objetos de biblioteca de documentos
- Utilización de agrupaciones de discos con registro por diario extensivo
- Utilización de agrupaciones de discos con registro por diario de vías de acceso

Utilización de agrupaciones de discos para tener disponibilidad

Cada parte del sistema puede tener unos requisitos de disponibilidad y recuperación diferentes. Por ejemplo, puede que tenga un archivo histórico grande que sólo se modifica al final de cada mes. La información de este archivo es útil pero no indispensable. Podría poner este archivo en una biblioteca separada en una agrupación de discos de usuario que no tenga ninguna protección de disco (protección por duplicación o protección por paridad de dispositivos). Podría asimismo omitir esta biblioteca cuando realiza las operaciones de salvar diarias. Sálvela únicamente al final de cada mes después de que se actualice.

Otro ejemplo serían los documentos y las carpetas. Algunos son indispensables para la organización; estos documentos y carpetas debería estar protegidos mediante protección por paridad de dispositivos o protección por duplicación de disco. Pueden ponerse en una agrupación de discos de usuario protegida. Otros documentos y carpetas se conservan en el sistema para proporcionar información, pero cambian con poca frecuencia. Pueden estar en una agrupación de discos de usuario distinta, con una estrategia para salvar y para protección diferentes.

Utilización de agrupaciones de discos para tener un mayor rendimiento

Si utiliza agrupaciones de discos de usuario para tener un mejor rendimiento del sistema, considere la dedicación de la agrupación de discos a un objeto que sea muy activo. En este caso, puede configurar la agrupación de discos con una sola unidad de discos.

No obstante, habitualmente no se aumenta el rendimiento cuando se sitúa una sola unidad protegida por paridad de dispositivo en una agrupación de discos de usuario, porque el rendimiento de dicha unidad se ve afectado por las demás unidades de disco del conjunto de paridad de dispositivo.

La asignación de una agrupación de discos exclusivamente para los receptores de diario conectados al mismo diario puede aumentar el rendimiento del registro por diario. Al tener el diario y los objetos del diario en una agrupación de discos separada de los receptores de diario conectados, no hay oposición a las operaciones de grabación de los receptores de diario. Las unidades asociadas a la agrupación de discos no tienen que reposicionarse antes de cada operación de grabación o lectura.

El sistema reparte los distintos receptores de diario entre varias unidades de discos para aumentar el rendimiento. El receptor de diario puede situarse en hasta diez unidades de disco de una agrupación de discos. Si especifica la opción de diario RCVSIZOPT(*MAXOPT1) o (*MAXOPT2), el sistema puede situar el receptor de diario en hasta 100 unidades de disco de una agrupación de discos. Si añade más unidades de disco a la agrupación de discos mientras el sistema está activo, el sistema determina si se utilizarán las nuevas unidades de disco para los receptores de diario la próxima vez que se realice la función de cambio de diario.

Otro modo de aumentar el rendimiento consiste en asegurarse de que hay suficientes unidades de almacenamiento en la agrupación de discos de usuario para dar soporte al número de operaciones de entrada y salida físicas que se realizan en los objetos de la agrupación de discos de usuario. Quizás deba emplear un método de ensayo y error moviendo los objetos a una agrupación de discos distinta y, después, supervisar el rendimiento de la agrupación de discos para ver si las unidades de almacenamiento se utilizan de modo excesivo. Si desea obtener más información sobre el trabajo con el

estado del disco (mandato WRKDSKSTS) para determinar si las unidades de almacenamiento tienen un uso excesivo, puede consultar la publicación *Gestión de trabajos* . Si se hace un uso excesivo de las unidades, debe considerar la adición de más unidades de disco a la agrupación de discos de usuario.

Utilización de agrupaciones de discos con objetos de biblioteca de documentos

Puede situar objetos de biblioteca de documentos (DLO) en agrupaciones de discos de usuario. A continuación se indican las posibles ventajas que pueden obtenerse al situar los DLO en agrupaciones de discos de usuario:

- La posibilidad de reducir el tiempo para salvar los DLO y separarlos según sus necesidades relativas a las operaciones de salvar.
- La posibilidad de separar los DLO según sus necesidades de disponibilidad. Los DLO críticos pueden situarse en agrupaciones de discos de usuario que estén protegidas mediante una protección por duplicación o una protección por paridad de dispositivos. Los DLO que cambian con poca frecuencia pueden situarse en agrupaciones de discos no protegidas con unidades más lentas.
- La posibilidad de crecimiento para dar cabida a un número mayor de documentos.

Si tiene un release actual del programa bajo licencia OS/400, puede ejecutar varios procedimientos SAVDLO o RSTDLO contra distintas agrupaciones de discos. También puede ejecutar varias operaciones SAVDLO en la misma agrupación de discos.

Un enfoque para situar objetos DLO en las agrupaciones de discos de usuario es dejar sólo los DLO de sistema (carpetas suministradas por IBM) en la agrupación de discos del sistema. Mueva las demás carpetas a agrupaciones de discos de usuario. Las carpetas de sistema no cambian frecuentemente, por lo que pueden salvarse con poca frecuencia. En el capítulo ″Cómo transferir una carpeta a una agrupación de discos distinta″ de la publicación Copia de seguridad y recuperación , se describe el procedimiento que debe seguirse para mover carpetas de la agrupación de discos del sistema a agrupaciones de discos de usuario o entre agrupaciones de discos de usuario.

En el mandato SAVDLO puede especificar una agrupación de discos. De este modo puede guardar todos los DLO de una agrupación de discos particular en un día concreto de la semana. Por ejemplo, puede guardar los DLO de la agrupación de discos 2 los lunes, los DLO de la agrupación de discos 3 los martes, etc. Puede salvar diariamente todos los DLO que han cambiado.

Los pasos de recuperación, si utiliza este tipo de técnica de salvar, dependerán de la información que se haya perdido. Si ha perdido una agrupación de discos entera, puede restaurar la última copia salvada completa de los DLO de dicha agrupación de discos. A continuación, restaurará los DLO cambiados desde las copias diarias salvadas.

Cuando salva los DLO de más de una agrupación de discos en la misma operación, se creará un archivo y un número de secuencia distintos en la cinta para cada agrupación de discos. Al restaurar, deberá especificar el número de secuencia correcto. Esto simplifica la restauración de los DLO cambiados sólo a la agrupación de discos que se perdió sin necesidad de conocer todos los nombres de carpetas.

Cuando especifica DLO(*SEARCH) o DLO(*CHG) en el mandato SAVDLO, especifique una agrupación de discos, si es posible. La especificación de una agrupación de discos ahorra recursos del sistema.

Restricciones para los DLO de agrupaciones de discos de usuario: Estas restricciones y limitaciones son aplicables cuando se sitúan DLO en agrupaciones de discos de usuario:

- Al utilizar un archivo de salvar en una operación de salvar, puede salvar los DLO de una única agrupación de discos.
- Si salva en un archivo de salvar y especifica SAVDLO DLO(*SEARCH) o SAVDLO DLO(*CHG), también debe especificar una agrupación de discos, aunque sepa que el resultado de la búsqueda se encuentra en una única agrupación de discos.

- Los documentos que no están en carpetas debe estar en la agrupación de discos del sistema.
- El correo puede archivarse en una carpeta de una agrupación de discos de usuario. El correo no archivado se encuentra en la agrupación de discos del sistema.

Utilización de agrupaciones de discos con registro por diario extensivo

Si los diarios y los objetos que se registran por diario están en la misma agrupación de discos que los receptores y la agrupación de discos se desborda, debe finalizar el registro por diario de todos los objetos y efectuar una recuperación de la condición de desbordamiento para la agrupación de discos. En la publicación Copia de seguridad y recuperación se describe cómo recuperar una agrupación de discos desbordada.

Si el receptor de diario se encuentra en una agrupación de discos distinta a la del diario y la agrupación de discos de usuario en el que se encuentra el receptor se desborda, efectúe lo siguiente:

1. Cree un nuevo receptor en una agrupación de discos de usuario diferente.
2. Cambie el diario (mandato CHGJRN) para conectar el receptor de diario recién creado.
3. Salve el receptor desconectado.
4. Suprímalo (desconéctelo).
5. Borre la agrupación de discos desbordada sin finalizar el registro por diario.
6. Cree un receptor nuevo en la agrupación de discos borrada.
7. Conecte el receptor nuevo mediante el mandato CHGJRN.

Nota: En la publicación Copia de seguridad y recuperación encontrará más información acerca del trabajo con receptores de diario cuando una agrupación de discos se desborda.

Utilización de agrupaciones de discos con registro por diario de vías de acceso

Si piensa utilizar el registro por diario de vías de acceso explícito, IBM le recomienda que primero cambie el diario por un receptor de diario de la agrupación de discos del sistema (agrupación de discos 1) durante unos días. Inicie el registro por diario de vías de acceso para conocer los requisitos de almacenamiento del receptor antes de asignar el tamaño específico para una agrupación de discos de usuario. En el apartado Gestión de diarios se proporciona más información acerca de cómo evaluar los requisitos de almacenamiento para el registro por diario.

Considerar la creación de una agrupación de discos nueva en un sistema activo

A partir de la V3R6 del programa bajo licencia OS/400, puede añadir unidades de discos mientras el sistema está activo. Cuando añade unidades de disco a una agrupación de discos que no existe actualmente, el sistema crea una agrupación de discos nueva. Consulte el apartado Añadir una unidad de discos o una agrupación de discos para conocer los pasos que deben seguirse para configurar una agrupación de discos. Si elige crear una agrupación de discos de usuario nueva mientras el sistema está activo, asegúrese de que comprende las siguientes consideraciones:

- No puede iniciar la protección por duplicación de disco para una agrupación de discos básica mientras el sistema está activo. Puede iniciar la protección por duplicación en una agrupación de discos independiente no disponible cuando el sistema está activo. La nueva agrupación de discos no está totalmente protegida a no ser que todas las unidades de disco tengan protección por paridad de dispositivos.
- No puede mover unidades de disco existentes a una agrupación de discos básica mientras el sistema está activo. El sistema tiene que trasladar los datos cuando traslada unidades de discos. Esto sólo se puede llevar a cabo mediante las Herramientas de Servicio Dedicado (DST). No es posible mover unidades de disco desde una agrupación de discos existente a una agrupación de discos independiente.

- El sistema utiliza el tamaño de una agrupación de discos de usuario para determinar el umbral de almacenamiento de los receptores de diario que utiliza la protección de vía de acceso gestionada por el sistema (SMAPP). Cuando crea una agrupación de discos mientras el sistema está activo, el tamaño de las unidades de disco que especifica en la operación que crea la agrupación de discos se considera que es el tamaño de la agrupación de discos para la SMAPP. Por ejemplo, supongamos que añade 2 unidades de disco a una agrupación de discos nueva, la agrupación de discos 2. La capacidad total de las 2 unidades de disco es de 2062 MB. Posteriormente, añade otras 2 unidades de discos para aumentar la capacidad a 4124 MB. A efectos de SMAPP, el tamaño de la agrupación de discos sigue siendo 2062 MB hasta la siguiente vez que se realiza una IPL o se activa una agrupación de discos independiente. Esto quiere decir que el umbral de almacenamiento para los receptores de la SMAPP es menor y el sistema tiene que cambiar los receptores más a menudo. Normalmente, esto no repercutirá de manera significativa en el rendimiento del sistema.

El sistema determina la capacidad de cada agrupación de discos al efectuar una IPL o activar una agrupación de discos independiente. En ese momento, el sistema ajusta sus cálculos para los requisitos de tamaño de la SMAPP. Consulte el apartado Protección por vía de acceso gestionada por el sistema para obtener más información acerca de la SMAPP.

Comprobar que el sistema dispone del suficiente espacio de trabajo

Si cambia la configuración de disco, el sistema probablemente necesitará espacio de trabajo. Esto es particularmente cierto si piensa mover unidades de disco de una agrupación de discos a otra. El sistema tiene que trasladar todos los datos de la unidad de discos a otras unidades de discos antes de trasladarla. En el apartado ″Cómo calcular los requisitos de espacio de una agrupación de almacenamiento auxiliar″ de la publicación Copia de seguridad y recuperación se proporcionan ejemplos de cómo determinar el almacenamiento de trabajo necesario para distintas situaciones. También existen límites del sistema para la cantidad de almacenamiento auxiliar.

Si el sistema no dispone del almacenamiento suficiente para la operación intermedia, empiece por realizar una limpieza del almacenamiento en disco. En muchas ocasiones, los usuarios guardan objetos viejos en el sistema, tales como archivos de spool o documentos, que han dejado de ser necesarios. Considere la posibilidad de utilizar la función de limpieza automática de Operational Assistant para liberar algo de espacio en disco en el sistema.

Si la eliminación de objetos innecesarios del almacenamiento auxiliar sigue sin proporcionar el suficiente espacio en disco para la operación intermedia, otra alternativa es eliminar objetos temporalmente del sistema. Por ejemplo, si piensa mover una biblioteca grande a una nueva agrupación de discos de usuario, puede salvar la biblioteca y eliminarla del sistema. A continuación, después de haber trasladado las unidades de discos, restaure la biblioteca. A continuación se muestra un ejemplo de cómo hacerlo:

1. Salve las autorizaciones de uso privado sobre los objetos del sistema especificando lo siguiente:
   `SAVSECDTA DEV(dispositivo_cintas)`
2. Salve el objeto utilizando el mandato SAVxxx apropiado. Por ejemplo, para salvar una biblioteca, utilice el mandato SAVLIB. Considere la posibilidad de salvar el objeto dos veces en dos cintas distintas.
3. Suprima el objeto del sistema utilizando el mandato DLTxxx apropiado. Por ejemplo, para suprimir una biblioteca, utilice el mandato DLTLIB.
4. Vuelva a calcular la capacidad en disco para averiguar si ha creado suficiente espacio disponible para la operación intermedia.
5. Si dispone del suficiente espacio, realice las operaciones de configuración de disco.
6. Restaure los objetos que ha suprimido.

Agrupaciones de discos — ejemplos de usos

Las agrupaciones de discos se utilizan para gestionar el rendimiento del sistema y los requisitos de la copia de seguridad, como se indica a continuación:

- Puede crear una agrupación de discos para proporcionar recursos dedicados a objetos que se utilizan con frecuencia, como por ejemplo receptores de diario.
- Puede crear una agrupación de discos para conservar archivos de salvar. Se pueden crear copias de seguridad de los objetos en archivos de salvar de una agrupación de discos distinta. No es probable que se pierdan a la vez tanto la agrupación de discos que contiene el objeto como la agrupación de discos que contiene el archivo de salvar.
- Puede crear distintas agrupaciones de discos para objetos con diferentes requisitos de recuperación y disponibilidad. Por ejemplo, puede poner los archivos de base de datos o documentos críticos en una agrupación de discos que tenga protección por duplicación de disco o protección por paridad de dispositivos.
- Puede crear una agrupación de discos para situar objetos que se utilizan con muy poca frecuencia, como por ejemplo grandes archivos históricos, en unidades de disco con un rendimiento inferior.
- Puede utilizar agrupaciones de discos para gestionar tiempos de recuperación de vías de acceso para archivos de base de datos críticos y no críticos, utilizando la protección por vía de acceso gestionada por el sistema.
- Puede utilizarse una agrupación de discos independiente para aislar datos que se utilizan con muy poca frecuencia para liberar recursos del sistema que se utilizarán sólo cuando sea necesario.
- Una agrupación de discos independiente en un entorno de clusters puede proporcionar almacenamiento de disco conmutable, que permite tener una disponibilidad continua de los recursos.

Agrupaciones de discos — ventajas

La colocación de objetos en agrupaciones de discos de usuario, también denominadas agrupaciones de almacenamiento auxiliar (ASP) en la interfaz basada en caracteres, puede proporcionar varias ventajas. Estos son algunos ejemplos:

- **Protección adicional de los datos**. Al separar las bibliotecas, documentos u otros objetos en una agrupación de discos, se protegen contra la pérdida de datos cuando una unidad de discos de la agrupación de discos del sistema u otra agrupación de discos de usuario sufre una anomalía. Por ejemplo, si tiene una anomalía de una unidad de discos y los datos contenidos en la agrupación de discos del sistema se pierden, los objetos contenidos en las agrupaciones de discos de usuario no se ven afectados y pueden utilizarse para recuperar objetos en la agrupación de discos del sistema. Por el contrario, si una anomalía provoca la pérdida de los datos contenidos en una agrupación de discos de usuario, los datos de la agrupación de discos del sistema no se ven afectados.
- **Mejora del rendimiento del sistema**. La utilización de las agrupaciones de discos también pueden aumentar el rendimiento del sistema. Esto se debe a que el sistema dedica las unidades de disco asociadas a una agrupación de discos a los objetos de dicha agrupación de discos. Por ejemplo, suponga que está trabajando en un entorno de registro por diario intensivo. La colocación de diarios y objetos registrados por diario en una agrupación de discos de usuario puede reducir el conflicto entre los receptores y los objetos registrados por diario si se encuentran en agrupaciones de discos distintas, lo que aumenta el rendimiento del registro por diario. Si utiliza agrupaciones de discos independientes para reducir la contienda, sitúe los objetos que deben registrarse por diario en la agrupación de discos primaria y los receptores de diario en una o varias agrupaciones de discos secundarias.

  La colocación de muchos receptores de diario activos en la misma agrupación de discos no es productiva. La contienda resultante de efectuar grabaciones en más de un receptor de la agrupación de discos puede disminuir el rendimiento del sistema. Para obtener el rendimiento máximo, sitúe cada receptor de diario activo en una agrupación de discos de usuario separada.
- **Separación de objetos con requisitos de disponibilidad y recuperación distintos**. Puede utilizar distintas técnicas de protección de disco para diferentes agrupaciones de discos. También puede especificar objetivos de tiempo diferentes para la recuperación de vías de acceso. Puede asignar los objetos indispensables o muy utilizados a unidades de discos protegidas y de alto rendimiento. Del mismo modo, asignaría archivos grandes y de poca utilización (por ejemplo, archivos históricos) a unidades de discos no protegidas y de rendimiento inferior.
- **Mayor disponibilidad y flexibilidad**. Consulte el apartado Ventajas de las agrupaciones de discos independientes para obtener más información exclusiva de las agrupaciones de discos independientes.

Agrupaciones de discos — costes y limitaciones

Puede encontrarse con algunas limitaciones concretas cuando utilice las agrupaciones de discos (agrupaciones de almacenamiento auxiliar):

- El sistema no puede recuperar directamente los datos perdidos como consecuencia de una anomalía de medio de unidad de discos. Esta situación requiere que se lleven a cabo operaciones de recuperación.
- La utilización de las agrupaciones de discos pueden requerir dispositivos de disco adicionales.
- La utilización de agrupaciones de disco requerirá gestionar la cantidad de datos de una agrupación de discos y evitar que una agrupación de discos se desborde.
- Será necesario realizar pasos especiales de recuperación si se desborda una agrupación de discos básica.
- La utilización de agrupaciones de discos requiere la gestión de los objetos relacionados. Algunos objetos relacionados, como por ejemplo los diarios y los objetos registrados por diario, deben estar en la misma agrupación de discos de usuario.

Agrupación de discos del sistema

El sistema crea automáticamente la agrupación de discos del sistema (agrupación de discos 1), que contiene la unidad de discos 1 y todos los demás discos configurados que no se han asignado a la agrupación de discos de usuario. La agrupación de discos del sistema contiene todos los objetos del sistema del programa bajo licencia OS/400 y todos los objetos del usuario que no se han asignado a una agrupación de discos básica o independiente.

Nota: puede tener unidades de discos conectadas al sistema que no estén configuradas y no se utilicen. Dichas unidades se denominan unidades de discos **no configuradas**.

Existen consideraciones adicionales que debe tener presente, relativas a la capacidad de la agrupación de discos del sistema y la protección de la agrupación de discos del sistema.

Capacidad de la agrupación de discos del sistema: Si se alcanza el límite de capacidad de la agrupación de discos del sistema, el sistema terminará las actividades normales. Si ocurre esto, deberá realizar una IPL del sistema y llevar a cabo acciones correctivas (por ejemplo, suprimir objetos) para evitar que vuelva a suceder.

También puede especificar un umbral que, si se alcanza, avise al operador del sistema de una falta potencial de espacio. Por ejemplo, si establece el valor del umbral en 80 para la agrupación de discos del sistema, cuando la agrupación de discos del sistema llegue al 80% de su capacidad se notificará a la cola de mensajes del operador de sistema (QSYSOPR) y la cola de mensajes del sistema (QSYSMSG). Se envía un mensaje cada hora hasta que se cambia el valor del umbral o hasta que se suprimen o se transfieren los objetos fuera de la agrupación de discos del sistema. Si hace caso omiso de este mensaje, la agrupación de discos del sistema agotará su capacidad y el sistema finalizará de forma anómala.

Puede utilizar un tercer método para evitar que la agrupación de discos del sistema agote su capacidad, utilizando los valores del sistema QSTGLOWLMT y QSTGLOWACN. Si desea obtener más información, consulte el apartado ″Cómo cambiar el umbral de almacenamiento de la agrupación de almacenamiento auxiliar del sistema″ de la publicación Copia de seguridad y recuperación  .

Protección de la agrupación de discos del sistema: IBM recomienda utilizar la protección por paridad de dispositivos o la protección por duplicación en la agrupación de discos del sistema. La utilización de las herramientas de protección de discos reduce la probabilidad de que la agrupación de discos del sistema pierda todos sus datos. Si la agrupación de discos del sistema se pierde, también se perderá la posibilidad de direccionamiento de todos los objetos de cada agrupación de discos de usuario.

Puede recuperar la posibilidad de direccionamiento restaurando todo el sistema o ejecutando el mandato Reclamar almacenamiento (RCLSTG). Sin embargo, el mandato RCLSTG no puede recuperar la

información del propietario del objeto. Después de ejecutar el mandato, el perfil de usuario QDFTOWN será el propietario de todos los objetos. Puede utilizar el mandato Reclamar objeto de biblioteca de documentos (RCLDLO) para recuperar la información del propietario de los objetos de biblioteca de documentos.

Agrupaciones de discos de usuario

Puede crear una agrupación de discos de usuario agrupando un conjunto de unidades de disco y asignando este grupo a una agrupación de discos. Las agrupaciones de discos de usuario pueden contener bibliotecas, documentos y ciertos tipos de objetos. Existen dos tipos de agrupaciones de discos de usuario: agrupaciones de discos básicas y agrupaciones de discos independientes. En un entorno en clusters, las agrupaciones de discos independientes pueden pasarse de un sistema a otro sin tener que realizar una IPL, lo que permite tener datos continuamente disponibles. Puede configurar agrupaciones de discos básicas con números comprendidos entre 2 y 32. La numeración de las agrupaciones de discos independientes va de 33 a 255. Para conocer con más detalle las diferencias existentes entre las agrupaciones de discos básicas e independientes, consulte el apartado Comparación entre las agrupaciones de discos básicas e independientes.

Consulte los siguientes temas para obtener más información acerca de las agrupaciones de discos de biblioteca y de no biblioteca:

- Agrupaciones de discos de usuario de biblioteca
- Agrupaciones de discos de usuario de no biblioteca

Cuando haya configurado las agrupaciones de discos, debe protegerlas utilizando la duplicación de disco o la protección por paridad de dispositivos.

Agrupaciones de discos de usuario de biblioteca: Las agrupaciones de discos de usuario de biblioteca contiene bibliotecas y sistemas de archivos definidos por el usuario (UDFS). IBM recomienda utilizar agrupaciones de discos de usuario de biblioteca, porque los pasos para la recuperación son más fáciles que los de las agrupaciones de discos de usuario de no biblioteca. Deben considerarse varios factores al utilizar agrupaciones de discos de usuario de biblioteca.

Qué debe saber de las agrupaciones de discos de usuario de biblioteca:

- **No** cree bibliotecas de sistema o de producto (bibliotecas que empiezan por Q o #) ni carpetas (carpetas que empiezan por Q) en una agrupación de discos de usuario. **No** restaure ninguna de estas bibliotecas o carpetas en una agrupación de discos de usuario. Hacerlo puede provocar resultados imprevisibles.
- Las agrupaciones de discos de biblioteca pueden contener tanto bibliotecas como objetos de biblioteca de documentos. La biblioteca de documentos de una agrupación de discos de usuario se denomina QDOCnnnn, donde *nnnn* es el número de la agrupación de discos.
- Los diarios y los objetos que se registran por diario **deben** estar en la misma agrupación de discos. Sitúe los receptores de diario en una agrupación de discos distinta. Con esto se protege contra la pérdida tanto de los objetos como de los receptores en caso que se produzca una anomalía del medio de disco.

  Para iniciar el registro por diario, el diario (tipo de objeto *JRN) y el objeto que debe registrarse por diario deben estar en la misma agrupación de discos. Utilice los siguientes mandatos para iniciar el registro por diario.
  - Mandato Arrancar registro por diario de PF (STRJRNPF) para archivos físicos
  - Mandato Arrancar registro por diario de vía de acceso (STRJRNAP) para vías de acceso
  - Mandato Arrancar diario (STRJRN) para objetos de sistema de archivos integrado
  - Mandato Arrancar registro por diario de objeto (STRJRNOBJ) para los demás tipos de objeto

El registro por diario no se puede volver a iniciar para un objeto que se ha salvado y se ha restaurado en una agrupación de discos distinta que no contenga el diario. El diario y el objeto deben residir en la misma agrupación de discos para que el registro por diario vuelva a iniciarse automáticamente para el objeto.

- Ninguna red de bases de datos puede cruzar límites de agrupaciones de discos. No puede crear un archivo en una agrupación de discos que dependa de un archivo que resida en una agrupación de discos distinta. Todos los archivos físicos de los que dependa un archivo lógico deben estar en la misma agrupación de discos que el archivo lógico. El sistema construye vías de acceso sólo para los archivos de base de datos que residan en la misma agrupación de discos que el archivo físico del que dependen (las consultas temporales no tienen limitación)). Los archivos situados en distintas agrupaciones de discos nunca comparten vías de acceso. Los formatos de registro no se comparten entre agrupaciones de discos diferentes. En cambio, se pasa por alto la petición de formato y se crea un nuevo formato de registro.
- Una colección SQL se puede poner en una agrupación de discos de usuario. Al crear la colección se especifica la agrupación de discos destino.
- Si la agrupación de discos de usuario de biblioteca no contiene ningún archivo de base de datos, establezca el objetivo de tiempo de recuperación de vías de acceso de la agrupación de discos en *NONE. Esto es cierto, por ejemplo, cuando la agrupación de discos de usuario de biblioteca sólo contiene bibliotecas para receptores de diario. Si se establece el tiempo de recuperación de vías de acceso en *NONE, se evita que el sistema haga trabajo innecesario para dicha agrupación de discos. En el apartado Protección de vía de acceso gestionada por el sistema se describe cómo se establecen los tiempos de recuperación de vías de acceso.

Agrupaciones de discos de usuario de no biblioteca: Las agrupaciones de discos de usuario de no biblioteca contienen diarios, receptores de diario y archivos de salvar cuyas bibliotecas residen en la misma agrupación de discos.

Si asigna tiempos de recuperación de vías de acceso individualmente a cada agrupación de discos, debe establecer el objetivo de tiempo de recuperación de una agrupación de discos de usuario no de biblioteca en *NONE. Una agrupación de discos de usuario no de biblioteca no puede contener archivos de base de datos y, en consecuencia, no puede beneficiarse de la protección de vías de acceso gestionada por el sistema (SMAPP) Si establece el tiempo de recuperación de vías de acceso para una agrupación de discos de usuario no de biblioteca en un valor diferente de *NONE, el sistema tendrá que realizar un trabajo adicional que no sirve para nada. En el apartado Protección de vía de acceso gestionada por el sistema se describe cómo se establecen los tiempos de recuperación de vías de acceso.

Protección de agrupaciones de discos: Tenga en cuenta los siguientes puntos en relación con la protección de las agrupaciones de discos:

- Todas las agrupaciones de discos, incluida la agrupación de discos del sistema, deben tener una protección por duplicación o estar formadas completamente por unidades de disco con protección por paridad de dispositivos para garantizar que el sistema continúe en ejecución después de una anomalía de disco en una agrupación de discos.
- Si se produce una anomalía de disco en una agrupación de discos que no tiene protección por duplicación, puede que el sistema no continúe su ejecución, en función del tipo de unidad de discos y el error.
- Si se produce una anomalía de disco en una agrupación de discos que tiene protección por duplicación, el sistema continúa su ejecución (a menos que ambas unidades de almacenamiento de la duplicación hayan sufrido una anomalía).
- Si una unidad de discos sufre una anomalía en una agrupación de discos que tiene protección por paridad de dispositivos, el sistema continúa su ejecución siempre y cuando ninguna otra unidad de discos del mismo conjunto de paridad de dispositivo sufra una anomalía.

Límites del sistema para el almacenamiento de las agrupaciones de discos: Durante una IPL, el sistema determina la cantidad de almacenamiento auxiliar configurado en el sistema. La cantidad total es

la suma de la capacidad de las unidades configuradas y sus pares duplicados, si los hay. No se incluyen las unidades de discos no configuradas. La cantidad de almacenamiento en disco se compara con el máximo aceptado para el modelo de sistema en particular.

Si la cantidad de almacenamiento auxiliar configurado sobrepasa la cantidad recomendada, se envía un mensaje (CPI1158) a la cola de mensajes del operador del sistema (QSYSOPR) y a la cola de mensajes QSYSMSG (si existe en el sistema). Este mensaje indica que en el sistema hay demasiado almacenamiento auxiliar, y se envía una vez por cada IPL en caso de que la cantidad de almacenamiento auxiliar del sistema sobrepase la cantidad máxima aceptada.

Agrupaciones de discos independientes

Los términos **agrupación de almacenamiento auxiliar independiente** y **agrupación de discos independiente** son sinónimos.

Una agrupación de discos independiente es una colección de unidades de disco que puede ponerse en línea o sacarse fuera de línea independientemente del resto del almacenamiento de un sistema, incluida la agrupación de discos del sistema, las agrupaciones de discos de usuario y las demás agrupaciones de discos independientes. Las agrupaciones de discos independientes son útiles tanto en entornos de sistema único como entornos multisistema. Si desea obtener información relacionada, puede consultar los apartados agrupación de discos del sistema y agrupación de discos de usuario.

En un entorno de sistema único, una agrupación de discos independiente puede sacarse fuera de línea independientemente de las demás agrupaciones de discos, porque los datos de la agrupación de discos independiente están autocontenidos, es decir, toda la información de sistema necesaria asociada a los datos de la agrupación de discos de discos independiente está contenida dentro de la agrupación de discos independiente. La agrupación de discos independiente también puede ponerse en línea mientras el sistema está activo (no se necesita una IPL). La utilización de las agrupaciones de discos independientes de este modo puede resultar muy útil, por ejemplo, si tiene grandes cantidades de datos que no son necesarios para el proceso cotidiano normal de la empresa. La agrupación de discos independiente que contiene estos datos puede dejarse fuera de línea hasta que sean necesarios. Cuando las grandes cantidades de almacenamiento se mantienen fuera de línea normalmente, puede reducirse el tiempo de proceso para operaciones tales como la IPL o la reclamación de almacenamiento.

En un entorno multisistema, la agrupación de discos independiente puede pasarse de un sistema a otro. Una **agrupación de discos independiente conmutable** es un conjunto de unidades de disco que puede pasar de un sistema a otro para que cada sistema pueda acceder a los datos. Sólo un sistema puede acceder a los datos a la vez. Como sucede en un entorno de sistema único, la agrupación de discos independiente puede pasar de un sistema a otro porque la agrupación de discos independiente está autocontenida. Las agrupaciones de discos independientes conmutables pueden resultar de ayuda en las siguientes situaciones:

- Hacer que los datos estén disponibles a una aplicación aún en el caso de un corte de alimentación en un único sistema (planificado o no).
- Eliminar el proceso de duplicación de datos de un sistema a otro.
- En algunas situaciones, aislar anomalías de unidades de disco de la agrupación de discos independiente.
- Lograr una alta disponibilidad y escalabilidad.

Para obtener más información, consulte el tema Agrupación de discos independiente.

Comparar las agrupaciones de discos básicas e independientes

Las agrupaciones de discos básicas y las agrupaciones de discos independientes, también denominadas agrupaciones de almacenamiento auxiliar (ASP) en la interfaz basada en caracteres, son útiles ambas para agrupar unidades de disco que contengan cierta información; sin embargo, tienen algunas diferencias inherentes:

- Cuando el servidor hace una IPL, es necesario tener una cuenta de todas las unidades de disco configuradas en una agrupación de discos básica para que el servidor pueda continuar la IPL. Las

agrupación de discos independiente no se incluyen en la IPL. Cuando se activan las agrupación de discos independiente, el nodo verifica que estén presentes todas las unidades de discos.

- Cuando una unidad de discos no protegida de una agrupación de discos sufre una anomalía, típicamente se detienen todos los procesos normales del servidor hasta que pueda repararse. La pérdida total de una unidad de discos de una agrupación de discos básica requiere dilatados procedimientos de recuperación para restaurar los datos perdidos antes de que el servidor pueda hacer una IPL y reanudar las operaciones normales.
- Los datos de una agrupación de discos básica pertenecen al nodo al que se conecta y sólo pueden ser accedidos directamente por dicho sistema. En una agrupación de discos independiente, los datos no pertenecen al nodo, si no que pertenecen a la agrupación de discos independiente. Puede compartir los datos de una agrupación de discos independiente entre varios nodos de un cluster, desactivándola de un nodo y activándola en otro.
- Cuando crea una agrupación de discos básica, se asigna un número a la agrupación de discos. Cuando crea una agrupación de discos independiente, se da un nombre a la agrupación de discos y el sistema le asigna un número.
- Si una agrupación de discos básica supera su capacidad puede desbordar el exceso de datos en la agrupación de discos del sistema. Las agrupaciones de discos independientes no se pueden desbordar. Si lo hicieran perderían su independencia. Cuando la agrupación de discos independiente se acerca a su umbral, deberá añadir más unidades de disco o suprimir objetos para crear más espacio de almacenamiento.
- Cuando realiza cambios restringidos en la configuración de discos de una agrupación de discos básica, debe reiniciar el servidor en la Herramientas de servicio dedicadas (DST). En una agrupación de discos independiente fuera de línea no es necesario tener el servidor en modalidad DST para iniciar o detener la duplicación de disco, iniciar la protección por paridad de dispositivo, iniciar la compresión, eliminar una unidad de discos, etc.

Protección por paridad de dispositivos

La protección por paridad de dispositivos es una función de disponibilidad del hardware que protege los datos contra las pérdidas debidas a las anomalías de las unidades de discos o a los daños en los discos. Para proteger los datos, el adaptador de E/S (IOA) del disco calcula y salva un valor de paridad para cada bit de datos. Conceptualmente, el IOA calcula el valor de paridad a partir de los datos situados en la misma ubicación en cada uno de las demás unidades de disco del conjunto de paridad de dispositivo. Cuando se produce una anomalía en un disco, los datos se pueden reconstruir utilizando el valor de paridad y los valores de los bits de las mismas ubicaciones en los demás discos. El sistema sigue funcionando mientras se reconstruyen los datos. El objetivo global de la protección por paridad de dispositivos es proporcionar una alta disponibilidad y proteger los datos de la manera menos costosa posible.

Si es posible, hay que proteger todas las unidades de discos del sistema mediante la protección por paridad de dispositivos o la protección por duplicación de disco. Esto impide la pérdida de información cuando se producen anomalías en los discos. En muchos casos, también se puede conseguir que el sistema siga funcionando mientras se repara o sustituye una unidad de discos.

Recuerde: la protección por paridad de dispositivos **no** sustituye a la estrategia de copia de seguridad y recuperación. La protección por paridad de dispositivos puede impedir que el sistema se detenga cuando se producen determinados tipos de anomalías. También es capaz de acelerar el proceso de recuperación para ciertos tipos de anomalías. Pero la protección por paridad de dispositivos no le protege contra numerosos tipos de anomalías como, por ejemplo, los siniestros en las instalaciones o los errores del operador o el programador. No protege contra los apagones del sistema provocados por las anomalías del otro hardware relacionado con los discos (por ejemplo, los controladores de disco, los procesadores de E/S de disco o un bus del sistema).

Antes de utilizar la protección por paridad de dispositivos debe tener en cuenta las ventajas que conlleva, así como sus costes y limitaciones.

Para obtener información adicional acerca de la protección por paridad de dispositivos, revise los siguientes temas:
- Planificación de la protección por paridad de dispositivos
- Cómo afecta la protección por paridad de dispositivos al rendimiento
- Utilización conjunta de la protección por paridad de dispositivos y la protección por duplicación de disco

Si desea obtener información de cómo empezar a utilizar la protección por paridad de dispositivos en su empresa, puede consultar la publicación Copia de seguridad y recuperación. 

Planificación de la protección por paridad de dispositivos

Si el objetivo es tener un sistema con una protección contra pérdida de datos y reparación de mantenimiento concurrente, considere la utilización de una combinación de protección por duplicación de disco y protección por paridad de dispositivos. En cada conjunto de protección por paridad de dispositivos, el espacio que se utiliza para la información de paridad es equivalente a una unidad de discos. A partir de los adaptadores de E/S (IOA) V5R2, el número mínimo de unidades de disco de un conjunto de paridad es 3; el número máximo de unidades de disco del conjunto de paridad es 18. En los IOA desarrollados antes de la V5R2, el número mínimo de unidades de disco de un conjunto de paridad es 4; el número máximo de unidades de disco del conjunto de paridad es 10. En la V5R2 puede optimizar los conjuntos de paridad en cuanto a capacidad, rendimiento o equilibrio de carga, si dispone de adaptadores IOA V5R2 o posterior. Para conocer con más detalle cómo se implementa la protección por paridad de dispositivos y cómo puede utilizarse conjuntamente con la protección por duplicación de disco, consulte los siguientes temas:

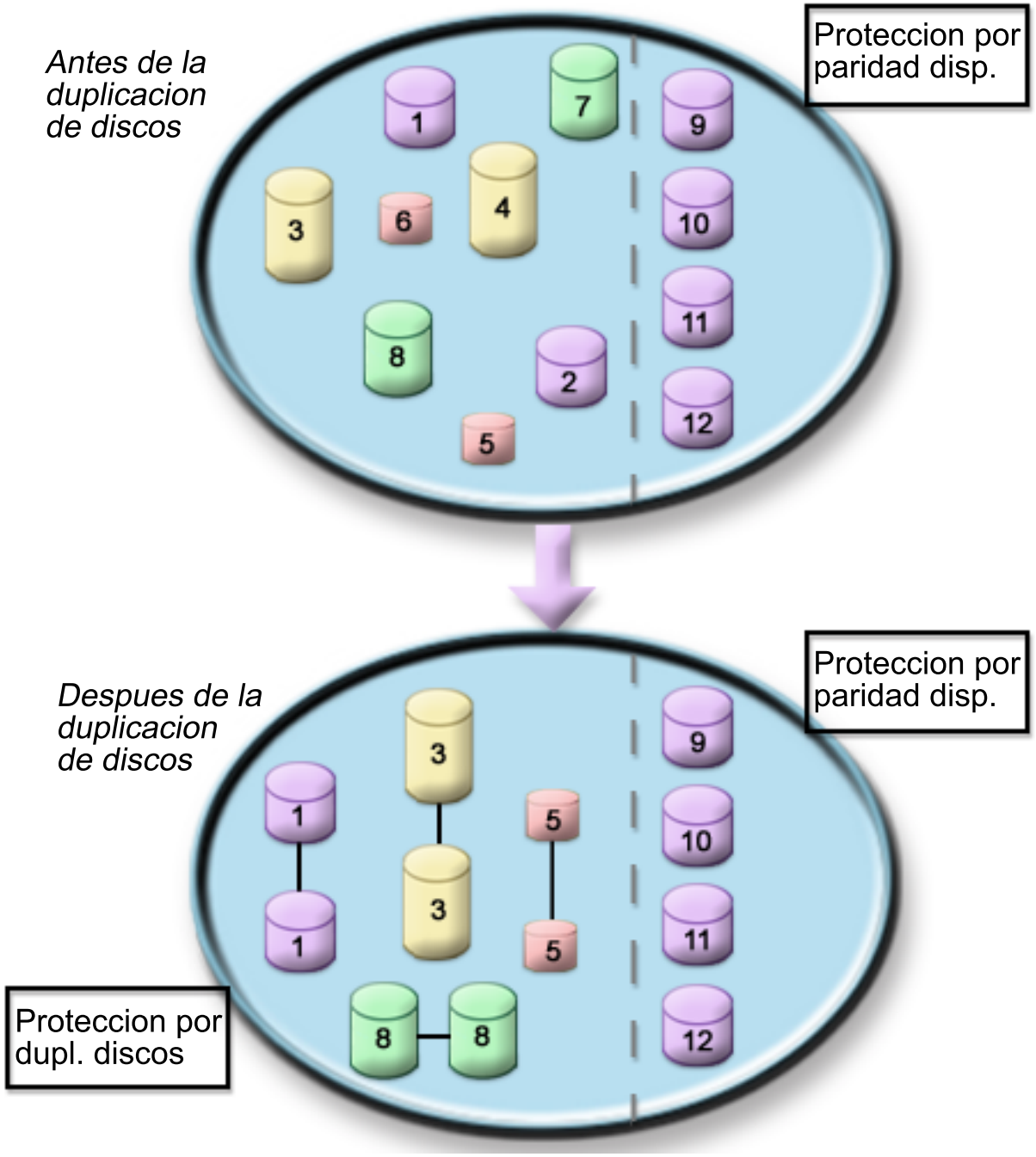
- Cómo funciona la protección por paridad de dispositivos
- Ejemplos de protección por paridad de dispositivos y duplicación de discos para agrupaciones de discos

Ejemplos de protección por paridad de dispositivos y duplicación de discos para agrupaciones de discos

Protección por duplicación de disco y protección por paridad de dispositivos para proteger la agrupación de discos del sistema

A continuación encontrará un ejemplo de sistema con una agrupación de discos (agrupación de almacenamiento auxiliar) tanto con protección por duplicación de disco como protección por paridad de

dispositivos.



En la figura se muestra una agrupación de discos con doce unidades de disco. Las unidades de disco 9–12 tienen todas la misma capacidad y tienen protección por paridad de dispositivos. Las unidades de disco 1–8 tienen capacidades variables, pero cada unidad de discos puede emparejarse con otra unidad de discos de la misma capacidad cuando se inicia la protección por duplicación de disco. Después de haberse iniciado la protección por duplicación de disco, las unidades de disco que se han emparejado se identifican mediante el mismo número; las unidades de disco 1 y 2 se denominan ahora 1, y así sucesivamente. Cuando se produce una anomalía en una de las unidades de discos que tiene protección por paridad de dispositivos, el sistema sigue funcionando. La unidad que ha sufrido la anomalía se puede reparar concurrentemente. Si se produce una anomalía en una de las unidades de discos protegidas por duplicación de disco, el sistema sigue funcionando porque utiliza la unidad operativa del par duplicado.

Protección por duplicación de disco en la agrupación de discos del sistema y protección por paridad de dispositivos en las agrupaciones de discos de usuario
Considere la protección por paridad de dispositivos si tiene protección por duplicación de disco en la agrupación de discos del sistema y va a crear agrupaciones de discos básicas o independientes. El sistema puede tolerar una anomalía en una de las unidades de disco de una agrupación de discos básica o independiente. La anomalía se puede reparar mientras el sistema sigue funcionando.

Protección por duplicación de disco y protección por paridad de dispositivos en todas las agrupaciones de discos
Si tiene todas las agrupaciones de discos (agrupaciones de almacenamiento auxiliar) protegidas con protección por duplicación de disco y desea añadir unidades a las agrupaciones de discos existentes, considere también la utilización de la protección por paridad de dispositivos. El sistema puede tolerar una anomalía en una de las unidades de discos que tienen protección por paridad de dispositivos. La unidad que ha sufrido la anomalía se puede reparar mientras el sistema sigue funcionando.Si se produce una anomalía en una unidad de discos que tiene protección por duplicación de disco, el sistema sigue funcionando porque utiliza la unidad operativa del par duplicado.

Cómo funciona la protección por paridad de dispositivos
Cuando se inicia la protección por paridad, los IOA crean conjuntos de paridad de dispositivos. A partir de los adaptadores de E/S (IOA) V5R2, el número mínimo de unidades de disco de un conjunto de paridad es 3; el número máximo de unidades de disco del conjunto de paridad es 18. En los IOA desarrollados antes de la V5R2, el número mínimo de unidades de disco de un conjunto de paridad es 4; el número máximo de unidades de disco del conjunto de paridad es 10. Un conjunto de paridad sólo puede tolerar una anomalía de disco. Si se produce más de una anomalía de disco, debe restaurar los datos desde el medio de copia de seguridad. Debido a la penalización de grabación, la restauración de datos en una agrupación de discos que tiene unidades de discos con protección por paridad de dispositivos puede tardar más que en una agrupación de discos que sólo contiene unidades de discos no protegidas.

En cada conjunto de paridad, el equivalente a una unidad de discos se dedica a almacenar los datos de paridad. El número de unidades de discos que realmente contienen datos de paridad varía en función de las unidades de discos que tenga el conjunto de paridad. En la siguiente tabla se muestra el número de unidades de discos de cada conjunto de paridad que almacenan datos de paridad:

Número de unidades de discos de un conjunto de paridad	Número de unidades de discos que almacenan paridad
3	2
4–7	4
8–15	8
16–18	16

El adaptador de entrada/salida determina el número de conjuntos de paridad que se forman. En los adaptadores de entrada/salida V5R2 y superior tiene la posibilidad de elegir cómo desea que se optimice el conjunto de paridad. Puede optimizar en función de la *capacidad*, *rendimiento* o una versión *equilibrada*. Si optimiza por capacidad, el IOA tiende a crear conjuntos de paridad con un mayor número de unidades de discos. Aumentará el espacio utilizado para almacenar datos del usuario, pero puede ser que el rendimiento no sea tan alto. Si optimiza por rendimiento, el IOA tiende a crear un conjunto de paridad con menos unidades de discos. Esto contribuirá a tener operaciones de lectura y grabación más rápidas, pero también puede dedicar un poco más de capacidad de disco a almacenar datos de paridad.

Es posible incluir unidades de discos adicionales de la misma capacidad en un conjunto de paridad de dispositivo después de que se haya iniciado la protección por paridad de dispositivos. Puede incluir hasta dos unidades de discos a la vez; no obstante, si existen tres o más unidades de discos elegibles para la protección por paridad de dispositivos, el sistema requiere que se inicie un nuevo conjunto de paridad, en lugar de incluirlas en un conjunto de paridad existente. En iSeries Navigator puede ver las propiedades de cada unidad de discos. Si el estado de la protección de una unidad de discos es *no protegido*, no está

protegida mediante la protección por paridad de dispositivos o la duplicación de disco y son elegibles para incluirse en un conjunto de paridad o iniciarse en un nuevo conjunto de paridad. También puede excluir de un conjunto de paridad discos que no almacenen datos de paridad sin detener la protección por paridad de dispositivos. Esta situación también la indicará el número de modelo, que debe ser 050 (o 060 si es una unidad de discos comprimidos). Puede excluir una unidad *protegida* con un número de modelo 070 (o 080 si es una unidad de discos comprimidos), porque se trata de una unidad de discos que no almacena datos de paridad.

Cuando un conjunto de paridad de dispositivos crece, es conveniente considerar la redistribución de los datos de paridad. Por ejemplo, puede empezar con 7 unidades de discos o menos, pero pasar a 8 o más incluyendo más unidades de discos. Cuando sucede esto, el rendimiento del conjunto de paridad de dispositivos puede mejorar deteniendo la protección por paridad de dispositivos y volviendo a iniciarla. Esta acción redistribuye los datos de paridad entre 8 discos en lugar de 4. En general, el reparto de los datos de paridad entre más unidades de discos aumenta el rendimiento.

En el adaptador de entrada/salida (IOA) se incluye una antememoria de grabación para cada conjunto de paridad para aumentar el rendimiento de las cargas de trabajo de grabación interactivas. Consulte el apartado Elementos de la protección por paridad de dispositivos para ver un ejemplo de un conjunto de paridad con cuatro unidades de discos.

A partir de la V5R2, todos los adaptadores de entrada/salida (IOA) tienen posibilidad de protección por paridad de dispositivos. Si tiene un adaptador de un modelo anterior, compruebe si tiene posibilidad de protección por paridad de dispositivos. Para obtener información acerca de pasar a un adaptador de una generación más nueva, consulte el tema Migración a un adaptador de entrada/salida nuevo.

Nota: si es posible, inicie la protección por paridad de dispositivos antes de añadir unidades de discos a una agrupación de discos. De este modo se reduce significativamente el tiempo necesario para configurar las unidades de discos.

Elementos de la protección por paridad de dispositivos: En los siguientes diagramas se ilustran los elementos de un conjunto de paridad que contiene cuatro unidades de discos. Cada conjunto de paridad empieza con un procesador de entrada/salida (IOP) conectado a un adaptador de entrada/salida (IOA), el cual contiene la antememoria de grabación. El IOA transmite las señales de lectura y grabación a las unidades de discos conectadas. En la primera figura se muestra cómo se distribuye la paridad con adaptadores anteriores a la V5R2. En la segunda figura se muestra cómo se distribuye la paridad con adaptadores V5R2 y superior.

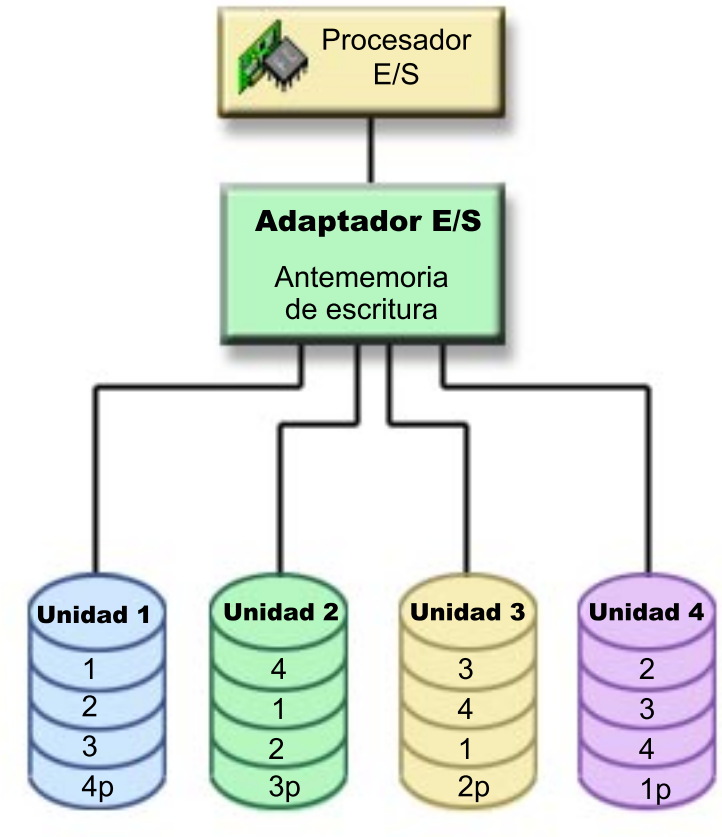


Figura 1. Ejemplo de cómo se distribuyen los datos de paridad con IOA anteriores a V5R2

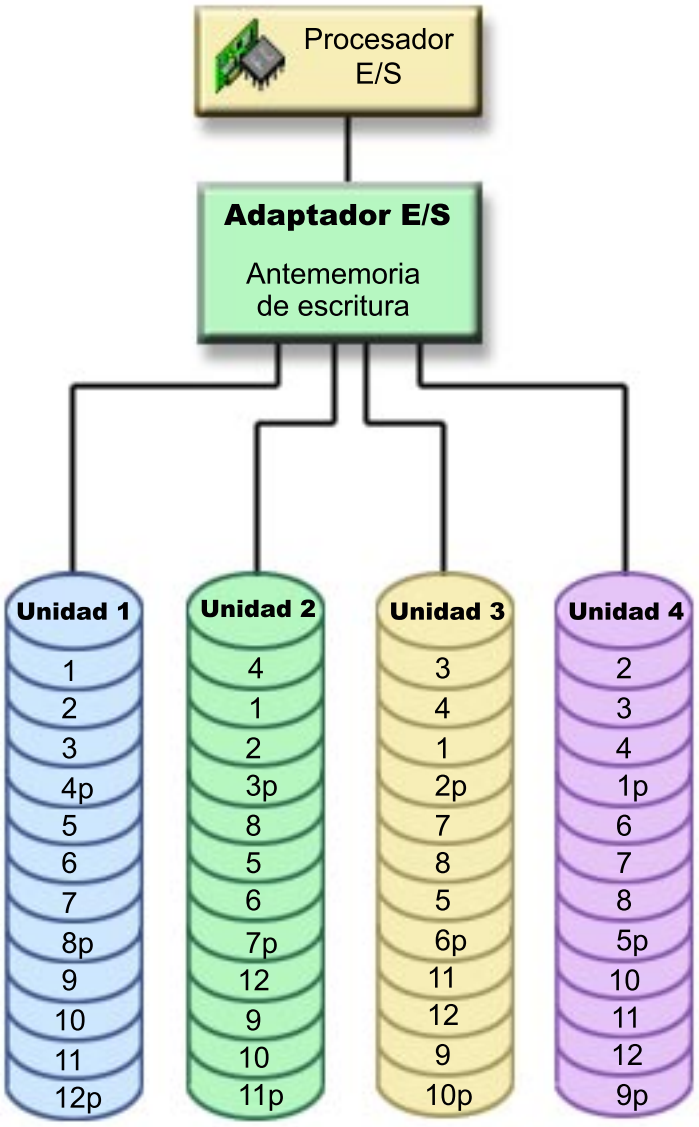


Figura 2. Ejemplo de cómo se distribuyen los datos de paridad con IOA V5R2 y superior

En los ejemplos anteriores, *p* indica las secciones del disco que contienen datos de paridad. En la primera figura se muestra un ejemplo de un IOA anterior a V5R2 en el que los datos de paridad se distribuyen en un gran segmento en cada unidad de discos que almacena datos de paridad. En la segunda figura se muestra cómo los IOA V5R2 y superior distribuyen los datos de paridad entre las unidades de discos en un número pequeño de segmentos grandes. El rendimiento se aumenta repartiendo los datos de paridad entre cada una de las unidades de discos.

La antememoria de grabación proporciona una mayor integridad de los datos y un mayor rendimiento. Cuando el servidor iSeries envía una operación de grabación, los datos se graban en la antememoria. A continuación, se envía un mensaje de finalización de grabación al servidor. Más adelante, los datos se graban en el disco. La antememoria proporciona una posibilidad de grabación más rápida y garantiza la integridad de los datos.

Si desea tener una visión general más detallada, consulte la información adicional acerca de la antememoria de grabación descrita anteriormente.

Antememoria de grabación: Durante una petición de grabación procedente del servidor se producen las siguientes acciones:

1. Los datos se comprometen en una antememoria respaldada por una batería no volátil del IOA.
2. Se envía un mensaje de finalización de grabación desde el servidor.

Las siguientes acciones se producen después de enviarse el mensaje de finalización de grabación.

1. Se envía una operación de grabación desde la antememoria del IOA a la unidad de discos
   - Para los datos:
     - Lee los datos originales.
     - Calcula la paridad delta comparando los datos nuevos y originales.
     - Graba los datos nuevos.
   - Para los datos de paridad:
     - Lee la información de paridad original.
     - Calcula la nueva paridad comparando la paridad delta y la paridad original.
     - Graba la nueva información de paridad.
2. Los datos se marcan como comprometidos cuando se graban satisfactoriamente en la unidad de discos de datos y la unidad de discos de paridad.

El rendimiento para este tipo de operación de grabación depende de la contención de disco y del tiempo necesario para calcular la información de paridad.

Migración a un adaptador de entrada/salida nuevo

Antes de empezar la migración al adaptador de entrada/salida (IOA) nuevo, al igual que con cualquier cambio de configuración, es importante efectuar un apagado normal del sistema. De este modo se tiene la garantía de que los datos de la antememoria se salvan. Cuando se hace la migración de un conjunto de paridad existente desde un IOA anterior a V5R2 a un IOA V5R2 o posterior, las unidades de discos no estarán protegidas por la protección por paridad de dispositivos mientras la paridad se está regenerando.

Nota:
no puede volver a hacer la migración del conjunto de paridad a la generación anterior de adaptadores una vez haya realizado el cambio al adaptador nuevo. Si necesita volver atrás, debe detener la protección por paridad de dispositivos, asociar los controladores al adaptador anterior y reiniciar la protección por paridad de dispositivos.

Protección por paridad de dispositivos: ventajas

Las ventajas que proporciona la protección por paridad de dispositivos son las siguientes:

- El controlador de disco reconstruye automáticamente los datos perdidos después de una anomalía de disco.
- El sistema sigue funcionando después de una única anomalía de disco.
- Es posible sustituir una unidad de discos anómala sin detener el sistema.
- La protección por paridad de dispositivos reduce el número de objetos que se dañan cuando se produce una anomalía de disco.
- En un conjunto de paridad sólo 1 unidad de discos de capacidad almacena los datos de paridad.

Protección por paridad de dispositivos: costes y limitaciones

Los costes y limitaciones de la protección por paridad de dispositivos son los siguientes:

- La protección por paridad de dispositivos puede necesitar unidades de discos adicionales para impedir que el rendimiento sea más lento.
- Las operaciones de restauración pueden tardar más tiempo cuando se utiliza la protección por paridad de dispositivos.

Cómo afecta la protección por paridad de dispositivos al rendimiento

La protección por paridad de dispositivos requiere operaciones de E/S adicionales para guardar los datos de paridad. Para evitar problemas de rendimiento, todos los IOA contienen una antememoria de grabación no volátil que garantiza la integridad de datos y proporciona una posibilidad de grabación más rápida. Se notifica al sistema que se ha completado una operación de grabación tan pronto como se almacena una copia de los datos en la antememoria de grabación. Los datos se recogen en la antememoria antes de que se graben en una unidad de discos. Esta técnica de recogida reduce el número de operaciones de grabación físicas que deben realizarse en la unidad de discos. Debido a la antememoria, el rendimiento suele ser casi el mismo en las unidades de discos protegidas y no protegidas.

Las aplicaciones que tienen muchas peticiones de grabación en un breve periodo de tiempo (por ejemplo, los programas de proceso por lotes) pueden afectar negativamente al rendimiento. Una anomalía en una única unidad de discos puede afectar negativamente al rendimiento de las operaciones de lectura y de grabación.

El proceso adicional asociado con una anomalía en una unidad de discos del conjunto de paridad de dispositivos puede ser considerable. La disminución del rendimiento permanece efectiva hasta que la unidad anómala se repara (o se sustituye) y el proceso de reconstrucción se completa. Si la protección por paridad de dispositivos disminuye demasiado el rendimiento, considere la posibilidad de utilizar la protección por duplicación de disco. Los siguientes temas proporcionan información detallada y adicional acerca de cómo afecta una anomalía de unidad de discos al rendimiento:

- Anomalía de unidad de discos en una configuración de protección por paridad de dispositivos
- Operaciones de lectura en una unidad de discos anómala
- Operaciones de grabación en una unidad de discos anómala
- Operaciones de entrada/salida durante un proceso de reconstrucción

Anomalía de unidad de discos en una configuración de protección por paridad de dispositivos

Si una unidad de discos sufre una anomalía, los subsistemas con protección por paridad de dispositivos se consideran que están expuestos hasta que finalice el proceso de sincronización después de sustituir la unidad de discos anómala. Durante el tiempo en que se considera que la unidad de discos está expuesta son necesarias operaciones de E/S adicionales. Si una segunda unidad de discos sufre una anomalía, debe restaurar los datos desde el medio de copia de seguridad.

Operaciones de lectura en una unidad de discos anómala

Para obtener los datos que contenía la unidad de discos anómala, la protección por paridad de dispositivos debe leer cada unidad de discos del conjunto de paridad de dispositivos que contiene la unidad de discos anómala. Como las operaciones de lectura pueden solaparse, las repercusiones en el rendimiento pueden ser escasas.

Como una unidad de discos anómala que tiene protección por paridad de dispositivos posiblemente contenga únicamente una pequeña parte de datos de usuario, es posible que sólo unos cuantos usuarios se vean afectados por la disminución del rendimiento.

Operaciones de grabación en una unidad de discos anómala

Hay algunos ejemplos disponibles que muestran lo que sucede en las operaciones de grabación cuando una única unidad de discos sufre una anomalía en un conjunto de paridad de dispositivos que tiene protección por paridad de dispositivos. En la siguiente figura se muestra una unidad anómala conectada a un IOA con protección por paridad de dispositivos. Utilice la figura para los siguientes ejemplos:

- Ejemplo: operaciones de grabación en una unidad de discos anómala
- Ejemplo: grabar datos en una unidad de discos cuyos datos de paridad correspondientes se encuentran en una unidad de discos anómala

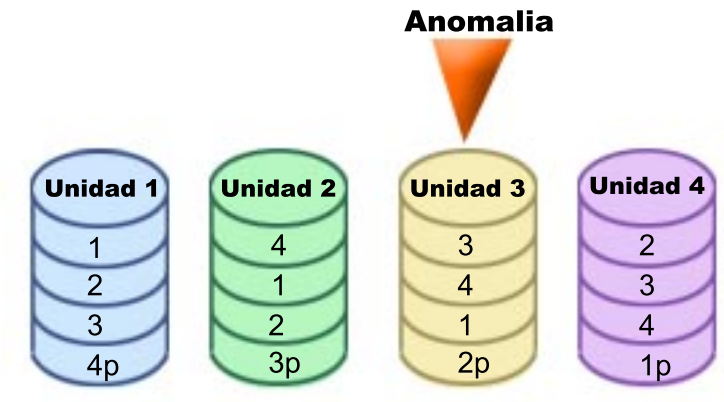


Figura 3. Conjunto de paridad de dispositivos con una unidad de discos anómala

En la figura se muestra un conjunto de paridad con cuatro unidades de discos. Cada sección de la unidad de discos se marca con un número. Los sectores de paridad se indican con una *p*. La unidad de discos 3 sufre una anomalía. La unidad de discos 1 muestra los sectores 1, 2, 3 y 4p. La unidad de discos 2 muestra los sectores 4, 1, 2 y 3p. La unidad de discos 3 anómala muestra los sectores 3, 4, 1 y 2p. La unidad de discos 4 muestra los sectores 2, 3, 4 y 1p.

Ejemplo: operaciones de grabación en una unidad de discos anómala: Una operación de grabación del servidor iSeries detecta que la unidad de discos que debe contener los datos sufre una anomalía. La operación de grabación se realiza en la unidad de discos 3, sector 1. Se producen las siguientes acciones:

1. Los datos originales se pierden en la unidad de discos 3, sector 1, debido a la anomalía.
2. Los nuevos datos de paridad se calculan leyendo la unidad de discos 1, sector 1 y la unidad de discos 2, sector 1.
3. Se calcula la nueva información de paridad.
4. Los nuevos datos no se pueden grabar en el sector 1 de la unidad de discos 3, debido a la anomalía.
5. La nueva información de paridad se graba en el sector de paridad 1 de la unidad de discos 4.

   La operaciones de grabación requieren varias lecturas (N-2 lecturas, donde N es el número de unidades de discos) y sólo una operación de grabación para la nueva información de paridad. Los datos de la unidad de discos 3 se reconstruirán durante la sincronización que se produce después de la sustitución de la unidad de discos 3.

Ejemplo: grabar datos en una unidad de discos cuyos datos de paridad correspondientes se encuentran en una unidad de discos anómala: La operación de grabación del servidor iSeries detecta una anomalía de disco en la unidad de discos que contiene los correspondientes datos de paridad. La operación de grabación se realiza en el sector 2 de la unidad de discos 4. La información de paridad para la unidad de discos 4, sector 2, se encuentra en la unidad de discos 3 anómala. Se producen las siguientes acciones:

1. Se detecta una anomalía en la unidad de discos que contiene los datos de paridad, la unidad de discos 3.
2. No es necesario realizar el cálculo de la información de paridad, porque no se puede efectuar una operación de grabación en el sector de paridad 2 de la unidad de discos 3. Por lo tanto, no es necesario leer los datos originales y la información original.
3. Los datos se graban en la unidad de discos 4, sector 2.

   Una operación de grabación sólo requiere una grabación para los datos nuevos. Los datos de paridad para el sector de paridad 2 en la unidad de discos 3 se reconstruirá durante la sincronización que se realiza después de sustituir la unidad de discos 3.

Operaciones de entrada/salida durante un proceso de reconstrucción

Es posible que las operaciones de E/S que tienen lugar durante el proceso de reconstrucción (sincronización) de la unidad de discos anómala no requieran peticiones adicionales de E/S de disco. Esto depende del lugar donde se leen o se graban los datos en la unidad de discos que está en proceso de sincronización. Por ejemplo:

- Una operación de lectura del área del disco que ya se ha reconstruido requiere una operación de lectura.
- Una operación de lectura del área del disco que no se ha reconstruido se considera como una operación de lectura en una unidad de discos anómala. Consulte el apartado ″Operaciones de lectura en una unidad de discos anómala″ para obtener más información.
- Una operación de grabación en el disco que ya se ha reconstruido requiere las operaciones de lectura y grabación normales (dos de lectura y dos de grabación).
- Una operación de grabación en el área del disco que no se ha reconstruido se considera como una operación de grabación en una unidad de discos anómala. Consulte el apartado ″Operaciones de grabación en una unidad de discos anómala″ para obtener más información.

Nota: el proceso de reconstrucción tarda más en completarse si también tienen lugar operaciones de lectura y grabación en una unidad de discos sustituida. Cada petición de lectura o de grabación interrumpe el proceso de reconstrucción para realizar las operaciones de E/S necesarias.

Utilización conjunta de la protección por paridad de dispositivos y la protección por duplicación de disco

La protección por paridad de dispositivos es una función de hardware. Las agrupaciones de discos y la protección por duplicación de disco son funciones de software. Cuando se añaden unidades de discos y se inicia la protección por paridad de dispositivos, el subsistema de discos o el IOP no tienen constancia de ninguna configuración de software para las unidades de discos. El software que proporciona soporte a la protección de disco tiene constancia de cuáles son las unidades que tienen protección por paridad de dispositivos.

Las siguientes reglas y consideraciones son aplicables cuando se combina la protección por paridad de dispositivos con la protección por duplicación de disco:

- No se implementa la protección por paridad de dispositivos en los límites de las agrupaciones de discos.
- La protección por duplicación de disco se implementa en los límites de las agrupaciones de discos.
- Puede iniciar la protección por duplicación de disco para una agrupación de discos aunque actualmente no tenga unidades disponibles para la duplicación de disco, porque todas ellas tienen protección por paridad de dispositivos. Esto garantiza que la agrupación de discos siempre estará totalmente protegida, aunque añada posteriormente discos sin protección por paridad de dispositivos.
- Cuando se añade una unidad de discos a la configuración del sistema, puede tener protección por paridad de dispositivos o puede no tenerla.
- Para un sistema totalmente protegido, debe proteger completamente cada agrupación de discos, ya sea mediante protección por paridad de dispositivos, mediante protección por duplicación de disco o ambos.
- Las unidades de discos protegidas mediante protección por paridad de dispositivos pueden añadirse a una agrupación de discos que tenga protección por duplicación de disco. Las unidades de discos que están protegidas mediante protección por paridad de dispositivos no participan en la protección por duplicación de disco; el hardware ya las protege.
- Cuando añade una unidad de discos que no está protegida por protección por paridad de dispositivos a una agrupación de discos que tiene protección por duplicación de disco, la nueva unidad de discos participa en la protección por duplicación de disco. Las unidades de discos deben añadirse y deben retirarse de una agrupación de discos protegida por duplicación de disco por parejas con la misma capacidad.

- Antes de iniciar la protección por paridad de dispositivos para las unidades de discos configuradas (asignadas a una agrupación de discos), debe detener la protección por duplicación de disco para la agrupación de discos.
- Antes de detener la protección por paridad de dispositivos, debe detener la protección por duplicación de disco para todas las agrupaciones de discos que contienen las unidades de discos afectadas.
- Cuando se detiene la protección por duplicación de disco, una unidad de discos de cada par duplicado pasa a estar no configurada. Debe volver a añadir las unidades no configuradas a la agrupación de discos antes de iniciar la protección por duplicación de disco.

Protección por duplicación de disco

La protección por duplicación de disco es una función de disponibilidad del software que protege los datos contra las pérdidas debidas a las anomalías o los daños de los componentes relacionados con discos. Los datos están protegidos porque el sistema guarda dos copias, cada una de ellas en una unidad de discos independiente. Cuando se produce una anomalía en un componente relacionado con disco, el sistema sigue funcionando sin interrupción utilizando la copia de los datos duplicada hasta que se repara el componente anómalo.

Cuando se inicia la protección por duplicación de disco o se añaden unidades de discos a una agrupación de discos que tiene protección por duplicación de disco, el sistema crea pares de duplicación utilizando unidades de discos que tengan capacidades idénticas. El objetivo global es proteger tantos componentes relacionados con discos como sea posible. Para proporcionar la máxima redundancia de hardware y protección, el sistema intenta emparejar unidades de discos conectadas a distintos controladores, adaptadores de entrada/salida, procesadores de entrada/salida, buses y torres.

Si se produce una anomalía de disco, la protección por duplicación de disco tiene por finalidad impedir que se pierdan datos. La protección por duplicación de disco es una función de software que utiliza duplicados de los componentes de hardware relacionados con disco para que el sistema siga estando disponible si falla uno de los componentes. Puede utilizarse en cualquier modelo de servidor iSeries y forma parte del código interno bajo licencia.

Existen diferentes niveles de protección por duplicación de disco, que varían en función del hardware que se duplica. Se puede duplicar lo siguiente:
- Unidades de discos
- Adaptadores de entrada/salida
- Procesadores de entrada/salida
- Buses
- Torres
- Enlaces de alta velocidad

Durante la anomalía, el sistema permanece disponible si se duplican el componente anómalo y los componentes de hardware que tiene conectados. Para obtener información técnica más detallada acerca del almacenamiento del servidor y la protección por duplicación de disco, consulte los apartados Cómo direcciona el sistema el almacenamiento y Protección por duplicación de disco: Cómo funciona.

El soporte de duplicación de disco remota le permite tener en la sede local una unidad duplicada del par duplicado, y la otra unidad duplicada en una sede remota. En algunos sistemas, la duplicación de disco de DASD estándar sigue siendo la mejor opción; en otros, la duplicación de disco de DASD remota proporciona importantes posibilidades adicionales. Debe evaluar los usos y necesidades de su sistema, considerar las ventajas y desventajas de cada tipo de soporte de duplicación de disco, y decidir cuál es el que más le conviene.

Para obtener más información acerca de la protección por duplicación de disco, consulte los siguientes apartados:
- Protección por duplicación de disco: ventajas

- Protección por duplicación de disco: costes y limitaciones
- Planificación de la protección por duplicación de disco
- Duplicación de disco DASD remota

Si desea obtener información sobre cómo implementar la protección por duplicación de disco en su empresa, puede consultar la publicación Copia de seguridad y recuperación. 

Protección por duplicación de disco: ventajas

Con la mejor configuración de protección por duplicación de disco que es posible, el sistema sigue funcionando después de una anomalía de hardware relacionado con disco. En algunas unidades del sistema, el hardware anómalo a veces puede repararse o sustituirse sin tener que apagar el sistema. Si el componente anómalo es de los que no pueden repararse mientras sigue funcionando el sistema, como es el caso de un bus o un procesador de E/S, el sistema suele seguir funcionando después de la anomalía. El mantenimiento puede diferirse, el sistema puede concluir con normalidad, y se puede evitar un tiempo de recuperación prolongado.

Incluso si el sistema no es grande, la protección por duplicación de disco puede proporcionarle una valiosa protección. Una anomalía de disco o de hardware relacionado con disco en un sistema desprotegido lo deja inutilizable durante varias horas. El tiempo real dependerá de la clase de anomalía, la cantidad de almacenamiento en disco, la estrategia de copia de seguridad, la velocidad de la unidad de cintas, y el tipo y la cantidad de proceso que el sistema lleva a cabo. Si usted o su empresa no pueden permitirse esta pérdida de disponibilidad, debe considerar la posibilidad de utilizar la protección por duplicación de disco en el sistema, independientemente de su tamaño.

Protección por duplicación de disco: costes y limitaciones

El coste principal que conlleva utilizar la protección por duplicación de disco radica en el hardware adicional. Para conseguir una alta disponibilidad y evitar la pérdida de datos cuando una unidad de discos sufre una anomalía, necesitará la protección por duplicación de discos para todas las agrupaciones de discos. Esto suele requerir el doble de unidades de discos. Si desea un funcionamiento continuo y quiere impedir que se pierdan datos cuando se produce una anomalía en una unidad de discos, un controlador o un procesador de E/S, tiene que duplicar los controladores de disco y los procesadores de E/S. Se puede llevar a cabo una actualización de modelo para obtener un funcionamiento casi continuo y para impedir que se pierdan datos cuando se produce una de estas anomalías, así como cuando se produce una anomalía en un bus. Si se produce una anomalía en el bus 1, el sistema no puede seguir funcionando. Como las anomalías de bus son infrecuentes, y la protección a nivel de bus no es mucho mayor que la protección a nivel de procesador de E/S, es posible que la inversión económica necesaria para una actualización de modelo no le resulte interesante teniendo en cuenta sus necesidades de protección.

La protección por duplicación de disco tiene un efecto mínimo sobre el rendimiento. Si los buses, procesadores de E/S y controladores no están más cargados en un sistema que tiene protección por duplicación de disco de lo que lo están en un sistema equivalente que no la tiene, el rendimiento de los dos sistemas será aproximadamente el mismo.

Para decidir si va a utilizar o no la protección por duplicación de disco en el sistema, debe evaluar el coste asociado al posible tiempo de inactividad y compararlo con el coste del hardware adicional, para todo el tiempo de vida del sistema. El coste adicional asociado al rendimiento o la complejidad del sistema suele ser insignificante. También debe tener en consideración otras alternativas de disponibilidad y recuperación como, por ejemplo, la protección por paridad de dispositivos. La protección por duplicación de disco suele requerir el doble de unidades de almacenamiento. Para llevar a cabo el mantenimiento concurrente y obtener una mayor disponibilidad en sistemas con protección por duplicación de disco, puede ser necesario otro hardware relacionado con disco.

Limitaciones

Aunque con la protección por duplicación de disco el sistema puede seguir estando disponible después de las anomalías de hardware relacionado con disco, esta protección no sustituye a los procedimientos de salvar. Puede haber varios tipos de anomalías relacionadas con los discos, o varias clases de siniestros (por ejemplo, inundaciones o sabotajes) que requieren medios de copia de seguridad.

La protección por duplicación de disco no puede hacer que el sistema siga estando disponible si la otra unidad de almacenamiento del par duplicado sufre una anomalía antes de que se reparare la unidad de almacenamiento que ha fallado primero y se reanude la protección por duplicación de disco. Si dos unidades de almacenamiento anómalas se encuentran en diferentes pares duplicados, el sistema sigue disponible y se lleva a cabo una recuperación de protección por duplicación de disco normal, debido a que los pares duplicados no dependen uno de otro para la recuperación. Si se produce una anomalía en una segunda unidad de almacenamiento del mismo par duplicado, tal vez la anomalía no tenga como consecuencia una pérdida de datos. No se pierde ningún dato si la anomalía se limita a los componentes electrónicos del disco, o el servicio técnico puede utilizar satisfactoriamente la función Salvar datos de unidad de discos para recuperar todos los datos.

Si las dos unidades de almacenamiento de un par duplicado sufren una anomalía y provocan la pérdida de datos, se pierde toda la agrupación de discos y se borran todas las unidades de la agrupación de discos. Debe estar preparado para restaurar la agrupación de discos desde el medio de copia de seguridad y aplicar los cambios de diario.

Cuando se inicia la operación de protección por duplicación de disco, los objetos que se crean en una unidad preferente se pueden trasladar a otra unidad. La unidad preferente puede dejar de existir una vez iniciada la protección por duplicación de disco.

Planificación de la protección por duplicación de disco

Si tiene un sistema multibus o un sistema grande con un único bus, debe considerar la posibilidad de utilizar la protección por duplicación de disco. Cuanto mayor sea el número de unidades de discos que están conectadas a un sistema, más frecuentes serán las anomalías de hardware relacionado con disco, sencillamente porque hay más componentes de hardware independientes que pueden sufrir anomalías. Por tanto, la posibilidad de perder datos o de perder disponibilidad como resultado de una anomalía de disco o de otro hardware es más probable. Asimismo, a medida que aumenta la cantidad de almacenamiento en disco de un sistema, aumenta considerablemente el tiempo de recuperación después de producirse una anomalía en el hardware del subsistema de almacenamiento en disco. El tiempo de inactividad se hace más frecuente, más prolongado y más costoso.

Al considerar la protección por duplicación de disco, póngase en contacto con su representante de ventas de IBM, que le guiará por los siguientes pasos de planificación:

1. Decidir qué agrupaciones de discos deben protegerse.
2. Determinar los requisitos de capacidad de almacenamiento en disco.
3. Determinar el nivel de protección que desea tener en cada agrupación de discos duplicada.
4. Averiguar cuál es el hardware adicional que necesita para la protección por duplicación de disco.
5. Averiguar cuál es el hardware adicional que necesita para el rendimiento.
6. Pedir el hardware.
7. Planificar la instalación del sistema y la configuración de las nuevas unidades.
8. Instalar el nuevo hardware.

Para obtener más información acerca de la protección por duplicación de disco, consulte los siguientes apartados:

Protección por duplicación de disco: ventajas
Protección por duplicación de disco: costes y limitaciones
Protección por duplicación de disco: cómo funciona

Protección por duplicación de disco: cómo funciona

Dado que la protección por duplicación de disco se configura por cada agrupación de discos, puede duplicar una, algunas o todas las agrupaciones de discos del sistema. Por omisión, cada sistema tiene

una agrupación de discos del sistema. No es necesario crear agrupaciones de discos de usuario para utilizar la protección por duplicación de disco. Aunque la protección por duplicación de disco se configura por cada agrupación de discos, es necesario duplicar todas las agrupaciones de discos para proporcionar la máxima disponibilidad del sistema. Si una unidad de discos sufre una anomalía en una agrupación de discos que no está duplicada, el sistema no podrá utilizarse hasta que se repare o se sustituya la unidad de discos.

El algoritmo de inicio de par duplicado selecciona automáticamente una configuración duplicada que proporciona la máxima protección para la configuración del hardware del sistema a nivel de bus, procesador de E/S (entrada/salida) o controlador. Cuando las unidades de almacenamiento de un par protegido están en buses separados, tienen la máxima independencia o protección. Como no comparten ningún recurso a nivel de bus, procesador de E/S o controlador, una anomalía en alguno de estos componentes de hardware permite a la otra unidad duplicada seguir funcionando.

Los datos que se graban en una unidad que está protegida por duplicación de disco se graban en ambas unidades de almacenamiento del par duplicado. Cuando los datos se leen en una unidad que está protegida por duplicación de disco, la operación de lectura puede tener lugar en cualquiera de las unidades de almacenamiento del par duplicado. Es transparente para el usuario cuál es la unidad duplicada en la que se leen los datos. El usuario no tiene constancia de la existencia de dos copias físicas de los datos.

Si se produce una anomalía en una unidad de almacenamiento de un par duplicado, el sistema *suspende* la protección por duplicación de disco en la unidad duplicada que ha sufrido la anomalía. El sistema sigue funcionando ya que utiliza la otra unidad duplicada. La unidad duplicada que sufre la anomalía se puede reparar o sustituir físicamente.

Después de reparar o sustituir la unidad duplicada que ha sufrido la anomalía, el sistema *sincroniza* el par duplicado copiando los datos que contiene la unidad de almacenamiento que ha seguido funcionando en la otra unidad de almacenamiento. Durante la sincronización, la unidad duplicada en la que se copia la información se encuentra en estado de *reanudación*. La sincronización no requiere un sistema dedicado y se ejecuta concurrentemente con otros trabajos del sistema. El rendimiento del sistema se ve afectado durante la sincronización. Cuando la sincronización se ha completado, la unidad duplicada pasa a estar *activa*.

Si desea obtener información detallada sobre el almacenamiento en el servidor, puede consultar el tema Cómo direcciona el servidor el almacenamiento.

Cómo direcciona el servidor el almacenamiento: Las unidades de discos se asignan a una agrupación de discos a partir de las unidades de almacenamiento. El sistema trata cada unidad de almacenamiento de una unidad de discos como una unidad de almacenamiento auxiliar independiente. Cuando se conecta una nueva unidad de discos al sistema, éste trata inicialmente todas las unidades de almacenamiento que contiene la unidad de discos como no configuradas. A través de las opciones de las Herramientas dedicadas de servicio (DST), puede añadir estas unidades de almacenamiento no configuradas a la agrupación de discos del sistema, la agrupación de discos básica o la agrupación de discos independiente que elija. Cuando añada unidades de almacenamiento no configuradas, utilice la información de número de serie asignada por el fabricante para asegurarse de que está seleccionando la unidad de almacenamiento físico correcta. Además, cada unidad de almacenamiento que hay dentro de la unidad de discos se puede identificar mediante la información de dirección que se puede obtener en la pantalla Visualizar configuración de disco de DST.

Cuando añada una unidad de almacenamiento no configurada a una agrupación de discos, el sistema asigna un número de unidad a la unidad de almacenamiento. El número de unidad se puede utilizar en lugar del número de serie y la dirección. El mismo número de unidad se utiliza para cada unidad de almacenamiento específica, aunque la unidad de discos se conecte al sistema de forma distinta.

Cuando una unidad tiene protección por duplicación de disco, a las dos unidades de almacenamiento del par duplicado se les asigna el mismo número de unidad. El número de serie y la dirección permiten diferenciar las dos unidades de almacenamiento de un par duplicado.

Para saber qué unidad de discos física se identifica con cada número de unidad, tome nota de la asignación del número de unidad con el fin de garantizar una identificación correcta. Si hay una impresora disponible, imprima la pantalla DST o SST de su configuración de disco. Si tiene que comprobar la asignación del número de unidad, utilice la pantalla Visualizar estado de configuración de DST o SST para mostrar los números de serie y las direcciones de cada unidad.

El sistema siempre utiliza la unidad de almacenamiento que direcciona como la unidad 1 para almacenar las áreas de datos y de código interno bajo licencia. La cantidad de almacenamiento que se utiliza en la unidad 1 es bastante grande, y varía en función de la configuración del sistema. La unidad 1 contiene una cantidad limitada de datos de usuario. Como la unidad 1 contiene los datos y programas iniciales que se utilizan durante una IPL del sistema, también se llama la **unidad de origen de carga**.

El sistema reserva una cantidad fija de almacenamiento en las unidades que no son la unidad 1. El tamaño de esta área reservada es de 1,08 MB por unidad, lo que reduce en dicha cantidad el espacio disponible de cada unidad.

Duplicación de disco remota: La duplicación de disco remota permite dividir las unidades de discos del sistema en un grupo de DASD locales y un grupo de DASD remotos. Los DASD remotos se conectan a un conjunto de buses ópticos y los DASD locales a otro conjunto de buses. Los DASD locales y remotos pueden estar separados físicamente y encontrarse en diferentes ubicaciones extendiendo los buses ópticos adecuados a la ubicación remota, ofreciendo así un nivel superior de protección en el caso de que se produzca un siniestro en la ubicación.

Mantenimiento concurrente: El mantenimiento concurrente es el proceso de reparar o sustituir un componente anómalo de hardware relacionado con disco mientras se utiliza el sistema para operaciones normales.

Los sistemas que no tienen protección por duplicación de disco o protección por paridad de dispositivos no están disponibles cuando se produce una anomalía de hardware relacionado con disco, y siguen sin estar disponibles hasta que el hardware que sufre la anomalía se repara o sustituye. Sin embargo, cuando se utiliza la protección por duplicación de disco, a menudo es posible reparar o sustituir el hardware mientras el sistema se está utilizando.

El soporte de mantenimiento concurrente es una función del paquete de hardware de la unidad del sistema. El sistema más bajo de la gama (9402) no proporciona soporte al mantenimiento concurrente. La protección por duplicación de disco sólo proporciona mantenimiento concurrente cuando el hardware y el sistema lo aceptan. La mejor configuración de hardware para la protección por duplicación de disco también proporciona la cantidad máxima de mantenimiento concurrente.

El sistema tiene la posibilidad de funcionar sin problemas cuando se producen numerosas anomalías distintas y se llevan a cabo las acciones de reparación correspondientes. Por ejemplo, una anomalía en el cabezal de un disco no hará que el sistema deje de funcionar. Se puede sustituir el conjunto del cabezal y sincronizar la unidad duplicada mientras el sistema sigue funcionando. Cuanto mayor sea el nivel de protección, mayor será la frecuencia con que se pueda llevar a cabo el mantenimiento concurrente.

En algunos modelos, el sistema limita el nivel de protección de la unidad 1 y su unidad duplicada exclusivamente a la protección a nivel de controlador. Consulte el tema ″Protección por duplicación de disco - Reglas de configuración″ de la publicación Copia de seguridad y recuperación  para obtener más información.

Bajo ciertas condiciones, el diagnóstico y la reparación pueden requerir que las unidades duplicadas que están activas se suspendan. Tal vez prefiera apagar el sistema para reducir al mínimo el riesgo que conlleva trabajar con menos protección por duplicación de disco. Algunas acciones de reparación requieren que el sistema se apague. El ***mantenimiento diferido*** es el proceso de esperar a que se pueda apagar el sistema para reparar o sustituir un componente anómalo de hardware relacionado con disco. El sistema está disponible, aunque la protección por duplicación de disco queda reducida en función de los componentes de hardware que han sufrido anomalías. El mantenimiento diferido sólo es posible con la protección por duplicación de disco o la protección por paridad de dispositivos.

Par duplicado: Son dos unidades de almacenamiento que contienen los mismos datos y a las que el sistema hace referencia como si de una unidad se tratase. Una ***unidad duplicada*** es una unidad de almacenamiento que es la mitad de un par duplicado.

Unidad de discos: Las unidades de discos son los dispositivos reales que contienen las unidades de almacenamiento. El hardware se pide a nivel de unidad de discos. Cada unidad de discos tiene un número de serie exclusivo.

Una ***unidad de almacenamiento*** es el espacio definido dentro de una unidad de discos direccionable por el sistema.

Una ***unidad*** es la subdivisión definida de almacenamiento de único nivel. Este espacio es la ubicación de disco más pequeña direccionable por el usuario. Una agrupación de discos son una o varias unidades identificadas por números de unidad únicos. Una unidad de una agrupación de discos no duplicada es una unidad de almacenamiento. Una unidad de una agrupación de discos duplicada es un par duplicado, que son dos unidades de almacenamiento.

Con algunos mandatos de creación (CRTPF, CRTJRNRCV, etc.), es posible crear un objeto en una unidad especificada. En el entorno no protegido por duplicación de disco se trata de una única unidad de almacenamiento. En el entorno protegido por duplicación de disco, el valor del parámetro UNIT significa un par duplicado.

Para obtener información detallada acerca del almacenamiento en el servidor, consulte el tema Cómo direcciona el sistema el almacenamiento.

Torre: Un alojamiento que contiene unidades de almacenamiento y que puede el sistema puede direccionar de forma separada.

Bus: El bus es el canal principal de comunicaciones para la transferencia de datos de entrada y salida. Un sistema puede tener uno o más buses.

Procesador de E/S: El procesador de entrada/salida (IOP) está conectado al bus. El IOP se utiliza para transferir información entre el almacenamiento principal y grupos específicos de controladores. Algunos IOP están dedicados a tipos específicos de controladores, por ejemplo, los controladores de disco. Otros IOP pueden conectar más de un tipo de controlador, por ejemplo, controladores de cinta o controladores de disco.

Adaptador de E/S: El adaptador de entrada/salida (IOA) se conecta al procesador de entrada/salida (IOP). El adaptador de entrada/salida transfiere información entre el IOP y las unidades de discos.

Controlador: El controlador de disco está conectado al IOP y maneja la transferencia de información entre el IOP y las unidades de discos. Algunas unidades de discos tienen controladores incorporados; otras tienen controladores independientes.

Decidir qué agrupaciones de discos deben protegerse

La protección por duplicación de disco se configura por cada agrupación de discos porque es el nivel de control del usuario sobre el almacenamiento de nivel único. La protección por duplicación de disco puede utilizarse para proteger una, varias o todas las agrupaciones de discos de un sistema. No obstante, no

son necesarias varias agrupaciones de discos para utilizar la protección por duplicación de disco. La protección por duplicación de disco funciona bien si todas las unidades de discos de un sistema se configuran en una sola agrupación de discos (el valor por omisión en el servidor iSeries). En realidad, la duplicación de disco reduce la necesidad de partir el almacenamiento auxiliar en agrupaciones de discos para la protección y recuperación de datos. No obstante, las agrupaciones de discos pueden ser aún necesarias por motivos de rendimiento y otros.

Para proporcionar la mejor protección y disponibilidad de todo el sistema, todas las agrupaciones de discos del sistema deben tener protección por duplicación de disco:

- Si el sistema tiene una mezcla de agrupaciones de discos con protección por duplicación de disco y otras agrupaciones de discos sin ella, una anomalía de una unidad de discos en una agrupación de discos sin protección por duplicación de disco limita gravemente la operación de todo el sistema. Pueden perderse datos en la agrupación de discos en la que se ha producido la anomalía. Tal vez sea necesaria una recuperación prolongada.
- Si un disco de una agrupación de discos duplicada sufre una anomalía y el sistema también contiene agrupaciones de discos que no están duplicadas, los datos no se pierden. Sin embargo, en algunos casos, puede que el mantenimiento concurrente no sea posible.

Las unidades de discos que se utilizan en las agrupaciones de discos deben seleccionarse detenidamente. Para obtener la mejor protección y el mayor rendimiento, una agrupación de discos debe contener unidades de discos conectadas a varios procesadores de E/S. El número de unidades de discos de una agrupación de discos que se conectan a cada procesador de E/S debe ser el mismo (es decir, equilibrado).

Cómo determinar cuántas unidades de discos se necesitan

Una agrupación de discos duplicada requiere el doble de almacenamiento que una agrupación de discos que no esté duplicada, porque el sistema mantiene dos copias de todos los datos de la agrupación de discos. Asimismo, la protección por duplicación de disco requiere un número par de unidades de discos con la misma capacidad, de tal manera que las unidades de discos se puedan emparejar en pares duplicados. En un sistema existente, hay que tener en cuenta que no es preciso añadir los mismos tipos de las unidades de discos ya conectadas con el fin de proporcionar la capacidad de almacenamiento adicional que es necesaria. Se pueden añadir todas las unidades de discos nuevas que se desee siempre que la capacidad total del almacenamiento sea suficiente y que haya un número par de unidades de almacenamiento de igual tamaño. El sistema asignará pares duplicados y trasladará los datos automáticamente según convenga. Si una agrupación de discos no contiene suficiente capacidad de almacenamiento o si no se pueden emparejar las unidades de almacenamiento, no se puede iniciar la protección por duplicación de disco para dicha agrupación de discos.

El proceso de determinación del número de unidades de discos que son necesarias para la protección por duplicación de disco es similar en los sistemas nuevos y en los existentes. Usted y el representante de ventas de IBM deben realizar las siguientes acciones:

1. Planificar la cantidad de datos que contendrá cada agrupación de discos.
2. Planificar un objetivo de porcentaje de capacidad que utilizará la agrupación de discos (cuán llena estará la agrupación de discos).
3. Planificar el número y el tipo de unidades de discos que se precisan para proporcionar el almacenamiento necesario. Para una agrupación de discos existente, puede planificar un tipo y modelo de unidad de discos distintos para proporcionar el almacenamiento necesario. Debe asegurarse de que hay un número par de cada modelo y tipo de unidad de discos.

Después de realizar la planificación de todas las agrupaciones de discos, puede planificar las unidades de repuesto, si así lo desea.

Cuando conozca toda esta información podrá calcular las necesidades totales de almacenamiento.

Planificación de la capacidad del almacenamiento: Para un sistema nuevo, el representante de ventas o reventas de IBM puede ayudarle a analizar los requisitos de almacenamiento del sistema. Para

un sistema existente, la cantidad actual de datos de la agrupación de discos que se desea planificar constituye un buen punto de partida. La opción Mostrar capacidad de configuración de disco de DST o SST muestra el tamaño total (en millones de bytes) y el porcentaje de almacenamiento que se utiliza en cada agrupación de discos del sistema. Multiplique el tamaño de las agrupaciones de discos por el porcentaje que se utiliza, para calcular el número de megabytes de datos que hay actualmente en la agrupación de discos. En la planificación de los requisitos de almacenamiento futuros de una agrupación de discos, también debe considerarse el crecimiento y el rendimiento del sistema.

La cantidad de datos planificada y el porcentaje de almacenamiento utilizado planificado influyen en la determinación de la cantidad de almacenamiento auxiliar real necesario para una agrupación de discos duplicada. Por ejemplo, si una agrupación de discos debe contener 1 GB (1 GB es igual a 1 073 741 824 bytes) de datos reales, requiere 2 GB de almacenamiento para las copias duplicadas de los datos. Si se planifica un 50% de la capacidad para dicha agrupación de discos, la agrupación de discos necesita 4 GB de almacenamiento real. Si el porcentaje planificado del almacenamiento que se utiliza es del 66%, se necesitan 3 GB de almacenamiento real. Un gigabyte de datos reales (2 GB de datos duplicados) en una agrupación de discos de 5 GB es igual a un 40% de utilización de almacenamiento auxiliar.

Planificación de unidades de discos de repuesto: Las unidades de discos de repuesto pueden reducir el tiempo que el sistema funciona sin protección por duplicación de disco para un par duplicado después de producirse una anomalía en una unidad de discos. Si se produce una anomalía en una unidad de discos y hay disponible una unidad de repuesto con la misma capacidad, esta unidad de repuesto se puede utilizar para sustituir la unidad de discos que ha sufrido la anomalía. Utilizando la opción de sustitución de DST o SST, el usuario selecciona la unidad de discos anómala que hay que sustituir, y luego selecciona una unidad de discos de repuesto para sustituirla. El sistema sustituye lógicamente la unidad anómala por la unidad de repuesto seleccionada, y luego sincroniza la nueva unidad con la unidad buena que queda del par duplicado. La protección por duplicación de disco de este par vuelve a estar activa cuando se completa la sincronización (normalmente en menos de una hora). Sin embargo, pueden pasar varias horas desde el momento en que se llama al servicio técnico hasta que se repara y sincroniza la unidad anómala y la protección por duplicación de disco vuelve a estar activa para dicho par.

Para una utilización plena de las unidades de repuesto, como mínimo se necesita una unidad de repuesto de cada una de las capacidades que tenga en el sistema. De este modo se dispone de una unidad de repuesto para cualquiera de los tamaños de las unidades de discos que pueden sufrir anomalías. Toda unidad anómala debe sustituirse por una unidad de repuesto que tenga la misma capacidad.

Requisitos totales de capacidad de almacenamiento planificada: Después de planificar el número y tipo de unidades de almacenamiento necesarias para cada agrupación de discos del sistema y el número de unidades de almacenamiento de repuesto, añada el número total de unidades de almacenamiento de cada tipo y modelo de unidad de discos. Recuerde que el número planificado es el número de unidades de almacenamiento de cada tipo de unidad de discos, no el número de unidades de discos. Usted y el representante de ventas de IBM deberán convertir el número planificado de unidades de almacenamiento en unidades de discos antes de solicitar el hardware.

El procedimiento anterior le ayuda a planificar el número total de unidades de discos que necesita el sistema. Si lleva a cabo la planificación en un sistema nuevo, éste será el número de unidades de discos que hay que pedir. Si la planificación se realiza en un sistema existente, reste el número correspondiente a cada tipo de disco que hay actualmente en el sistema del número planificado; el resultado es el número de unidades de discos nuevas que hay que pedir.

Determinación del nivel de protección deseado

El nivel de protección por duplicación de disco determina si el sistema sigue funcionando cuando se producen anomalías en diferentes niveles de hardware. El nivel de protección es la cantidad de hardware relacionado con disco duplicado de que se dispone. Cuanto mayor es el número de pares duplicados que tienen niveles más altos de protección, mayor será la frecuencia con que se podrá utilizar el sistema cuando se produzca una anomalía de hardware relacionado con disco. Quizá descubra que un nivel más

bajo de protección del sistema le resulta más rentable que un nivel superior. Los cuatro niveles de protección por duplicación de disco, en orden de menor a mayor, son los siguientes:
- Protección a nivel de unidad de discos
- Protección a nivel de adaptador de entrada/salida
- Protección a nivel de procesador de entrada/salida
- Protección a nivel de bus
- Protección a nivel de torre
- Protección a nivel de anillo

Cuando decida qué nivel de protección es el más adecuado, deberá tener en cuenta las ventajas relativas que proporciona cada nivel en función de lo siguiente:
- La capacidad de mantener el sistema operativo durante una anomalía de hardware relacionada con disco.
- La capacidad de llevar a cabo el mantenimiento concurrentemente con las operaciones del sistema. Para reducir al mínimo el tiempo que un par duplicado permanece desprotegido después de una anomalía, tal vez desee reparar el hardware anómalo mientras funciona el sistema.

Durante la operación de inicio de protección por duplicación de disco, el sistema empareja las unidades de discos para proporcionar el máximo nivel de protección al sistema. Cuando se añaden unidades de discos a una agrupación de discos duplicada, el sistema sólo empareja aquellas unidades de discos que se añaden sin reordenar los pares existentes. La configuración del hardware también incluye la forma en que éste se conecta.

Para obtener más información sobre los niveles de protección, consulte el apartado Niveles de protección: información detallada.

Niveles de protección: información detallada: El nivel de protección por duplicación de disco determina si el sistema sigue funcionando cuando se producen anomalías en diferentes niveles de hardware. La protección por duplicación de disco siempre proporciona protección a nivel de unidad de discos, lo que hace que el sistema siga estando disponible cuando se produce una anomalía en una unidad de discos. Para que el sistema siga estando disponible cuando se producen anomalías en otro hardware relacionado con disco se requieren niveles más altos de protección. Por ejemplo, para que el sistema siga estando disponible cuando se produce una anomalía en un procesador de E/S (IOP), todas las unidades de discos conectadas al IOP anómalo deben tener unidades duplicadas conectadas a diferentes IOP.

El nivel de protección por duplicación de disco también determina si se puede llevar a cabo el mantenimiento concurrente para tipos diferentes de anomalías. Algunos tipos de anomalía requieren mantenimiento concurrente para efectuar el diagnóstico de los niveles de hardware situados por encima del componente de hardware anómalo. Por ejemplo, para diagnosticar una anomalía de alimentación en una unidad de discos se requiere restablecer el procesador de E/S al que está conectado la unidad de discos anómala. Por tanto, se requiere protección a nivel de IOP. Cuanto mayor sea el nivel de protección por duplicación de disco, mayor será la frecuencia con que será posible el mantenimiento concurrente.

El nivel de protección que se obtiene depende del hardware que se duplica. Si se duplican unidades de discos, se dispondrá de protección a nivel de unidad de discos. Si también se duplican controladores de unidad de discos, se dispondrá de protección a nivel de controlador. Si se duplican procesadores de entrada/salida, se dispone de protección a nivel de IOP. Si se duplican buses, se dispone de protección a nivel de bus. Las unidades duplicadas siempre tendrán como mínimo protección a nivel de unidad de discos. Como la mayoría de las unidades de discos internas tienen el controlador empaquetado junto con la unidad de discos, como mínimo tendrán protección a nivel de controlador.

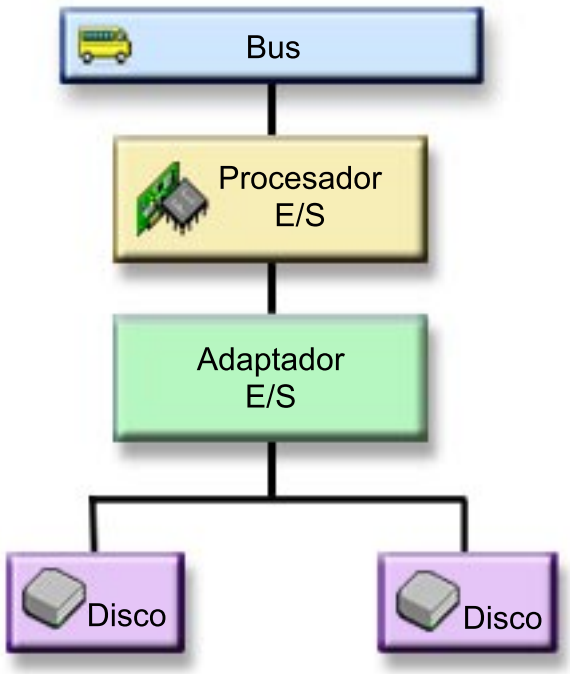
Durante la operación de inicio de protección por duplicación de disco, el sistema empareja las unidades de discos para proporcionar el máximo nivel de protección al sistema. Cuando se añaden unidades de

discos a una agrupación de discos duplicada, el sistema sólo empareja aquellas unidades de discos que se añaden sin reordenar los pares existentes. La configuración del hardware también incluye la forma en que éste se conecta.

Protección a nivel de unidad de discos: La protección por duplicación de disco siempre proporciona protección a nivel de unidad de discos, porque las unidades de almacenamiento están duplicadas. Si su principal preocupación es proteger los datos y no es disponer de una alta disponibilidad, la protección a nivel de unidad de discos puede ser la adecuada. La unidad de discos es el componente de hardware que tiene más posibilidades de sufrir anomalías, y la protección a nivel de unidad de discos hace que el sistema siga estando disponible después de producirse una anomalía en una unidad de discos.

Con la protección a nivel de unidad de discos, el mantenimiento concurrente suele ser posible para determinados tipos de anomalías de unidad de discos.

En la siguiente figura se muestran los elementos de la protección a nivel de unidad de discos: un bus, conectado a un IOP, conectado a un IOA, que se conecta a dos unidades de discos separadas. Las dos unidades de almacenamiento constituyen un par duplicado. Con la protección a nivel de unidad de discos, el sistema sigue funcionando después de producirse una anomalía en una unidad de discos. Si se producen anomalías en el controlador o en el procesador de E/S, el sistema no puede acceder a los datos de ninguna de las unidades de almacenamiento del par duplicado, y el sistema no puede utilizarse.

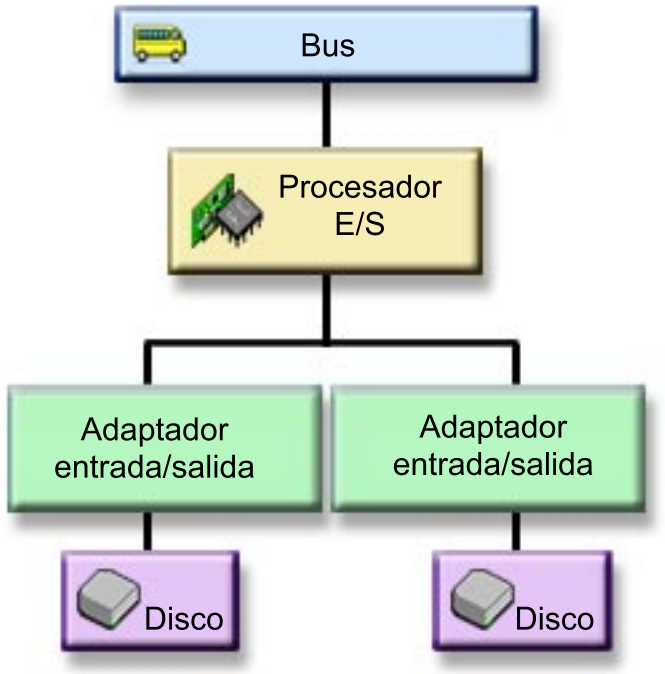


Protección a nivel de adaptador de entrada/salida: Decida si le conviene la protección a nivel de adaptador de entrada/salida (IOA) en función de los siguientes objetivos:

- Para que el sistema siga estando disponible cuando se produce una anomalía en un IOA.
- Para reparar concurrentemente una unidad de discos o IOA anómalos. Para utilizar los procedimientos de recuperación de problemas en la preparación del aislamiento de un elemento anómalo o para verificar una acción de reparación, el IOA debe estar dedicado a la acción de reparación. Si hay unidades de discos conectadas al IOA que no tienen protección a nivel de IOA, el mantenimiento concurrente de esta pieza no es posible.

Para obtener la protección a nivel de IOA, todas las unidades de discos deben tener una unidad duplicada conectada a un IOA distinto. En la siguiente figura se muestra la protección a nivel de IOA. Las dos unidades de almacenamiento constituyen un par duplicado. Con la protección a nivel de IOA, el sistema puede seguir funcionando si uno de los IOA sufre una anomalía. Si se producen anomalías en el procesador de E/S, el sistema no puede acceder a los datos de ninguna de las unidades de discos, por lo que no puede utilizarse.

En la figura se muestran los elementos de la protección a nivel de IOA: un bus, conectado a un IOP, conectado a dos IOA, cada uno de ellos conectado a dos unidades de discos separadas.

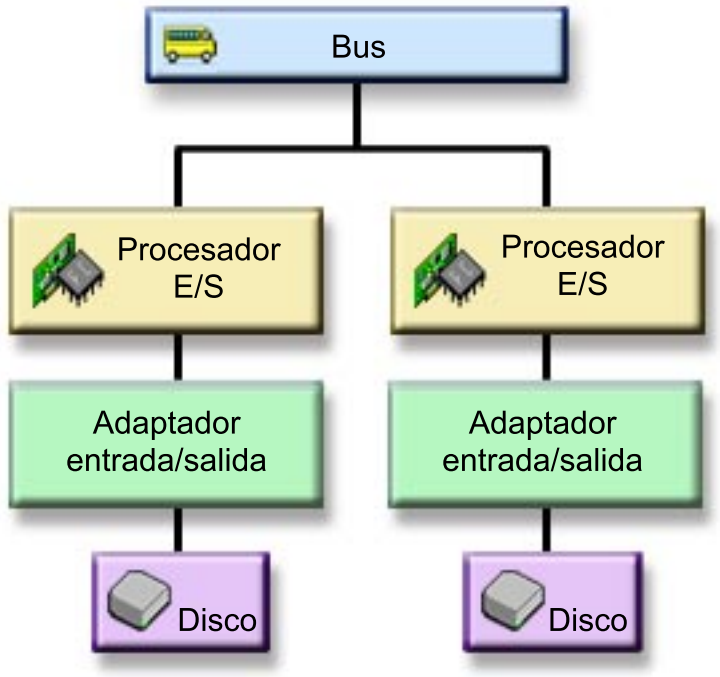


Protección a nivel de procesador de entrada/salida: Decida si le conviene la protección a nivel de IOP en función de los siguientes objetivos:

- Para que el sistema siga estando disponible cuando se produce una anomalía en un procesador de E/S.
- Para que el sistema siga estando disponible cuando el cable conectado al procesador de E/S sufre una anomalía.
- Para reparar concurrentemente determinados tipos de anomalías de las unidades de discos o los cables. En estas anomalías, el mantenimiento concurrente tiene que restablecer el IOP. Si hay unidades de discos conectadas al IOP que no tienen protección a nivel de IOP, el mantenimiento concurrente no es posible.

Para obtener la protección a nivel de procesador de E/S, todas las unidades de discos que están conectadas a un procesador de E/S deben tener una unidad duplicada conectada a un procesador de E/S diferente. En muchos sistemas, la protección a nivel de procesador de E/S no es posible para el par duplicado de la unidad 1.

En la siguiente figura se muestran los elementos de la protección a nivel de IOP: un bus, conectado a dos IOP, cada uno de ellos conectado a dos IOA separados y dos unidades de discos separadas. Las dos unidades de almacenamiento constituyen un par duplicado. Con la protección a nivel de IOP, el sistema puede seguir funcionando si uno de los procesadores de E/S sufre una anomalía. El sistema pasa a no estar disponible únicamente si se produce una anomalía en el bus.

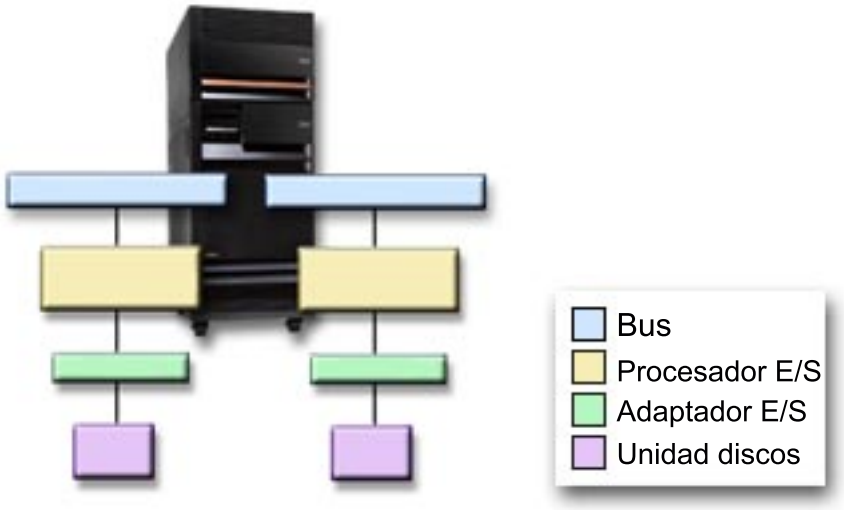


Protección a nivel de bus: La protección a nivel de bus puede permitir que el sistema funcione cuando se produce una anomalía en un bus. Sin embargo, este tipo de protección no suele resultar rentable debido a las siguientes razones:

- Si se produce una anomalía en el bus 1, el sistema no puede seguir funcionando.
- Si se produce una anomalía en un bus, las operaciones de E/S de disco pueden continuar, pero se pierde tanto hardware de otras clases (por ejemplo, estaciones de trabajo, impresoras y líneas de comunicaciones) que, desde un punto de vista práctico, el sistema no se puede utilizar.
- Las anomalías de bus son infrecuentes en comparación con otras anomalías de hardware relacionado con disco.
- El mantenimiento concurrente no es posible cuando se producen anomalías de bus.

Para obtener la protección a nivel de bus, todas las unidades de discos que están conectadas a un bus deben tener una unidad duplicada conectada a un bus diferente. La protección a nivel de bus no es posible en la unidad 1.

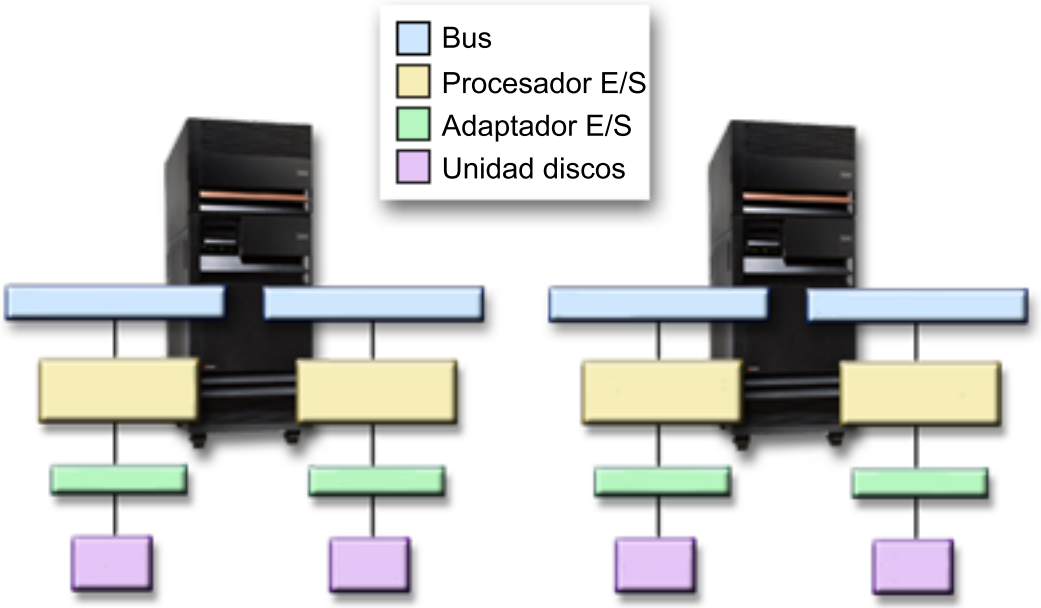
En esta figura se muestran los elementos de la protección a nivel de bus: una torre que contiene dos buses conectados a varios IOP, IOA y unidades de discos separados, respectivamente. Las dos unidades de almacenamiento constituyen un par duplicado. Con la protección a nivel de bus, el sistema puede seguir funcionando después de producirse una anomalía en un bus. Sin embargo, el sistema no puede seguir funcionando si la anomalía tiene lugar en el bus 1.



Protección a nivel de torre: La protección a nivel de torre puede permitir que el sistema funcione cuando se produce una anomalía en una torre. Sin embargo, este tipo de protección no suele resultar rentable debido a las siguientes razones:

- Si se produce una anomalía en una torre, las operaciones de E/S de disco pueden continuar, pero se pierde tanto hardware de otras clases (por ejemplo, estaciones de trabajo, impresoras y líneas de comunicaciones) que, desde un punto de vista práctico, el sistema no se puede utilizar.
- Las anomalías de torre son infrecuentes en comparación con otras anomalías de hardware relacionado con disco.

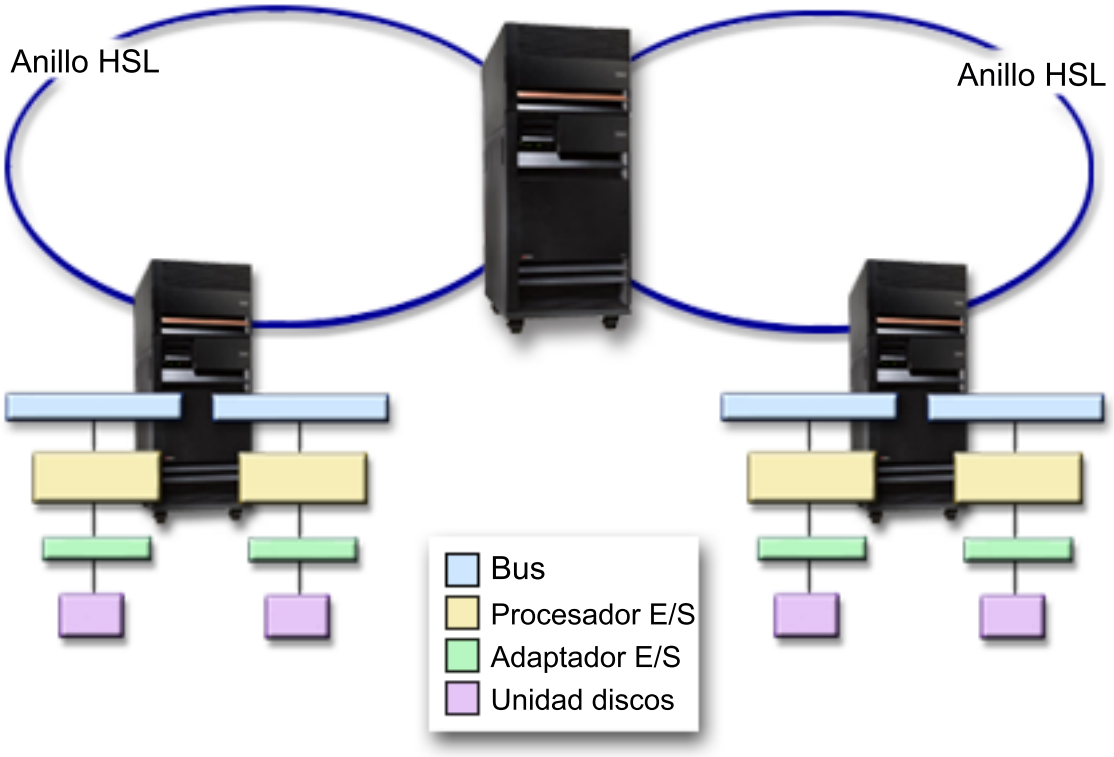
Para lograr una protección a nivel de torre, todas las unidades de discos presentes en la torre deben tener una unidad protegida por duplicación de disco presente en otra torre. En la figura se muestran los elementos de la protección a nivel de torre: dos torres que contienen cada una de ellas dos buses, conectados a varios IOP, IOA y unidades de discos separados, respectivamente.



Protección a nivel de anillo: La protección a nivel de anillo puede permitir que el sistema funcione cuando se produce una anomalía en un enlace de alta velocidad (HSL). Sin embargo, este tipo de protección no suele resultar rentable debido a las siguientes razones:

- Si se produce una anomalía en un HSL, las operaciones de E/S de disco pueden continuar, pero se pierde tanto hardware de otras clases (por ejemplo, estaciones de trabajo, impresoras y líneas de comunicaciones) que, desde un punto de vista práctico, el sistema no se puede utilizar.
- Las anomalías de HSL son infrecuentes en comparación con otras anomalías de hardware relacionado con disco.

Para lograr una protección a nivel de anillo, todas las unidades de discos presentes en una torre del primer HSL deben tener también una unidad protegida por duplicación de disco presente en otra torre del segundo HSL. En la figura se muestran los elementos de la protección a nivel de anillo: dos anillos HSL, conectados a dos torres que contienen cada una de ellas dos buses, conectados a varios IOP, IOA y unidades de discos separados, respectivamente.



Determinación del hardware necesario para la duplicación de disco

Para comunicarse con el resto del sistema las unidades de discos se conectan a controladores, que a su vez se conectan a procesadores de E/S, los cuales se conectan a buses. El número de cada uno de estos tipos de hardware relacionado con disco que están disponibles en el sistema afecta directamente al nivel de protección posible.

Para proporcionar la mejor protección y el mejor rendimiento, cada nivel de hardware debe equilibrarse por debajo del siguiente nivel. Es decir, las unidades de discos de cada modelo y tipo de dispositivo deben distribuirse equitativamente bajo sus controladores. Tiene que haber el mismo número de controladores bajo cada procesador de E/S de cada tipo de disco. Los procesadores de E/S deben distribuirse equilibradamente entre los buses que hay disponibles.

Para planificar el hardware relacionado con disco que es necesario en su sistema protegido por duplicación de disco, debe planificar el número total y los tipos de las unidades de discos (viejas y nuevas) que serán necesarias en el sistema, así como el nivel de protección del mismo. No siempre es posible planificar y configurar un sistema de tal manera que todos los pares duplicados se ajusten al nivel planificado de protección. No obstante, es posible planificar una configuración en la que un porcentaje muy grande de las unidades de discos del sistema obtengan el nivel deseado de protección.

Cuando se planifica hardware adicional relacionado con disco, es preciso realizar las siguientes tareas:

1. Determinar el hardware mínimo que es necesario para que las unidades de discos planificadas funcionen. Planificar los tamaños de las unidades de discos de uno en uno.
2. Planificar el hardware adicional que es necesario para proporcionar el nivel deseado de protección en cada tipo de unidad de discos

Planificación del hardware mínimo necesario para funcionar: Existen varias reglas y límites para la forma de conectar el hardware de almacenamiento. Los límites se pueden determinar en función del diseño del hardware, las restricciones de la arquitectura, las consideraciones del rendimiento o las

cuestiones relacionadas con el soporte. El representante de ventas de IBM puede explicarle estos límites de configuración y ayudarle a utilizarlos en la planificación. Si desea obtener una lista de los límites y reglas de configuración, puede consultar el apartado Instalación, actualizaciones y migración.

En cada tipo de unidad de discos, planifique primero los controladores que son necesarios y después los procesadores de E/S que se necesitan. Después de planificar el número de procesadores de E/S que se necesitan para todos los tipos de unidades de discos, utilice el número total de procesadores de E/S para planificar el número de buses necesario.

Planificación del hardware adicional que es necesario para obtener el nivel de protección deseado:

- Protección a nivel de unidad de discos
  Si ha planificado protección a nivel de unidad de discos, no es necesario que haga nada más. Todas las agrupaciones de discos duplicadas tienen un mínimo de protección a nivel de unidad de discos si cumplen los requisitos para iniciar la protección por duplicación de discos.
- Protección a nivel de controlador
  Si las unidades de discos planificadas no requieren un controlador independiente, ya tendrá protección a nivel de controlador para tantas unidades como sea posible y no será necesario que haga nada más. Si las unidades de discos planificadas requieren un controlador independiente, añada tantos controladores como sea posible, manteniéndose dentro de los límites definidos del sistema. A continuación, distribuya equilibradamente las unidades de discos entre ellos en función de las reglas estándares de configuración del sistema.
- Protección a nivel de procesador de entrada/salida
  Si desea disponer de protección a nivel de IOP y todavía no tiene el número máximo de IOP del sistema, añada tantos IOP como sea posible, manteniéndose dentro de los límites definidos del sistema. A continuación, distribuya equilibradamente las unidades de discos entre ellos en función de las reglas estándares de configuración del sistema. Tal vez tenga que añadir buses adicionales para conectar más IOP.
- Protección a nivel de bus
  Si desea tener protección a nivel de bus y ya tiene un sistema con varios buses, no es necesario que haga nada. Si el sistema está configurado de acuerdo con las reglas estándares de configuración, la función de par duplicado empareja las unidades de almacenamiento con el fin de proporcionar protección a nivel de bus para tantos pares duplicados como sea posible. Si tiene un sistema con un único bus, puede añadir buses adicionales como opción de característica.
- Protección a nivel de torre
  Si el sistema se configura con un número igual de unidades de discos de igual capacidad entre torres, la función de par reflejado empareja las unidades de discos de torres distintas para proporcionar protección a nivel de torre para tantas unidades de discos como sea posible.
- Protección a nivel de anillo
  Si el sistema se configura con un número igual de unidades de discos de igual capacidad entre enlaces de alta velocidad (HSL), la función de par reflejado empareja las unidades de discos de configuraciones de enlaces de alta velocidad (HSL) distintas para proporcionar protección a nivel de anillo para tantas unidades de discos como sea posible.

Determinación del hardware adicional que es necesario para el rendimiento

Normalmente, la protección por duplicación de disco requiere unidades de discos y procesadores de entrada/salida adicionales. Sin embargo, en algunos casos puede ser necesario hardware adicional para alcanzar el nivel de rendimiento deseado.

Utilice la siguiente información para decidir cuánto hardware adicional puede necesitar:

- **Requisitos de la unidad de proceso**

  La protección por duplicación de disco provoca un incremento poco significativo en la utilización de la unidad central de proceso (aproximadamente del 1% al 2%).
- **Requisitos del almacenamiento principal**

Si dispone de protección por duplicación de disco, deberá aumentar el tamaño de la agrupación de máquina. La protección por duplicación de disco necesita almacenamiento en la agrupación de máquina para finalidades de carácter general y para cada par duplicado. Hay que tener previsto un incremento de la agrupación de máquina de aproximadamente 12 KB por cada GB de almacenamiento de disco protegido por duplicación de disco (12 KB para 1 GB DASD, 24 KB para 2 GB DASD, etc.).

Durante la sincronización, la protección por duplicación de disco utiliza 512 KB adicionales de memoria para cada par duplicado que se sincroniza. El sistema utiliza la agrupación que tiene más almacenamiento.

- **Requisitos del procesador de E/S**

  Para mantener un rendimiento equivalente después de iniciar la protección por duplicación de disco, el sistema debe tener la misma proporción que tenía de unidades de discos en relación con los procesadores de E/S. Si quiere añadir procesadores de E/S, tal vez sea preciso que actualice el sistema para incluir buses adicionales.

  Debido al límite impuesto para los buses y procesadores de E/S, es posible que no pueda mantener la misma proporción entre unidades de discos y procesadores de E/S. En tal caso, el rendimiento del sistema puede disminuir.

Para obtener más información acerca del efecto que la duplicación de disco tiene sobre el rendimiento, consulte el apartado Duplicación de disco y rendimiento.

Duplicación de disco y rendimiento: Cuando se inicia la protección por duplicación de disco, la mayoría de los sistemas muestran escasas diferencias en el rendimiento; en algunos casos, la protección por duplicación de disco puede mejorarlo. Por lo general, las funciones que principalmente llevan a cabo operaciones de lectura tienen un rendimiento igual o mejor con la protección por duplicación de disco. Esto se debe a que las operaciones de lectura tienen la opción de elegir entre dos unidades de almacenamiento en las que leer, seleccionándose la que tiene un tiempo de respuesta previsto más rápido. En las operaciones que principalmente llevan a cabo operaciones de grabación (por ejemplo, la actualización de registros de bases de datos) el rendimiento puede verse ligeramente disminuido si el sistema tiene protección por duplicación de disco, ya que todos los cambios deben grabarse en ambas unidades de almacenamiento del par duplicado. Por consiguiente, las operaciones de restauración son más lentas.

En algunos casos, si el sistema finaliza de forma anómala no es capaz de averiguar si las últimas actualizaciones se grabaron en ambas unidades de almacenamiento de cada par duplicado. Si el sistema no está seguro de que los últimos cambios se grabaron en ambas unidades de almacenamiento del par duplicado, el sistema sincroniza el par duplicado copiando los datos en cuestión de una unidad de almacenamiento del par duplicado en la otra unidad de almacenamiento del mismo par. La sincronización tiene lugar durante la IPL que se realiza tras la finalización anómala del sistema. Si el sistema puede guardar una copia del almacenamiento principal antes de finalizar, el proceso de sincronización sólo dura unos cuantos minutos. En caso contrario, el proceso de sincronización puede tardar mucho más tiempo. El caso extremo podría estar cercano a una sincronización completa.

Si sufre apagones con frecuencia, tal vez le interese estudiar la posibilidad de añadir una fuente de alimentación ininterrumpible al sistema. Si se interrumpe la fuente de alimentación principal, la fuente de alimentación ininterrumpible permitirá al sistema seguir funcionando. Una fuente de alimentación ininterrumpible básica proporciona el tiempo que necesita el sistema para guardar una copia del almacenamiento principal antes de finalizar, lo que evita las recuperaciones prolongadas. Ambas unidades de almacenamiento del par duplicado de origen de carga deben ser alimentadas por la fuente de alimentación ininterrumpible básica.

Pedido del nuevo hardware

El representante de ventas de IBM le ayudará a solicitar el hardware nuevo utilizando el proceso de pedido habitual. Este proceso de pedido permite solicitar el hardware que pueda ser necesario como parte de la actualización; por ejemplo, bastidores y cables adicionales.

Planificación de la instalación
Debe trabajar con el representante de ventas de IBM para planificar la instalación de la protección por duplicación de discos en el sistema. El representante de ventas le ayudará a determinar si el sistema está equilibrado y cumple las reglas de configuración estándares, tal como se definen en el apartado Instalación, actualizaciones y migración. El sistema debe estar configurado de acuerdo con las reglas estándares para que la función de par duplicado empareje las unidades de almacenamiento, con el fin de proporcionar la mejor protección posible a partir del hardware que hay disponible. El representante de ventas también le ayudará a planificar las unidades nuevas que deben añadirse a cada agrupación de discos.

Si planifica iniciar la protección por duplicación de disco en un sistema nuevo, dicho sistema ya estará configurado de acuerdo con las reglas estándares de configuración. Si utiliza un sistema antiguo, tal vez no se ajuste a las reglas estándar. No obstante, espere hasta que haya intentado iniciar la protección por duplicación de disco para volver a configurar el hardware.

Para obtener más información sobre cómo realizar la planificación de las agrupaciones de discos, consulte el tema Planificación de las agrupaciones de discos que deben crearse.

Planificación de las agrupaciones de discos que deben crearse: Planifique las agrupaciones de discos de usuario que tendrán protección por duplicación de discos y determine las unidades que se añadirán a las agrupaciones de discos. En la publicación Copia de seguridad y recuperación encontrará información sobre cómo asignar unidades de discos para añadirlas a las agrupaciones de discos.

En general, las unidades de una agrupación de discos deben guardar un equilibrio entre varios procesadores de E/S, en lugar de estar todas conectadas al mismo procesador de E/S. Esto proporciona más protección y un rendimiento mejor.

Instalación del nuevo hardware
Cuando llegue el hardware, el servicio técnico lo instalará. Después de haber instalado el hardware, consulte el apartado Añadir una unidad de discos o una agrupación de discos para obtener información sobre cómo añadir unidades nuevas e iniciar la protección por duplicación de discos.

Soporte de duplicación de disco DASD remota
El soporte de duplicación de disco DASD estándar requiere que ambas unidades de discos del par duplicado de origen de carga (unidad 1) estén conectadas al Procesador de E/S Multifunción (MFIOP). Esto permite al sistema efectuar una IPL desde uno de los orígenes de carga del par duplicado, y también le permite volcar almacenamiento principal en uno de los orígenes de carga si el sistema finaliza con anomalías. Sin embargo, como ambos orígenes de carga deben estar conectados al mismo procesador de E/S (IOP), la mejor protección por duplicación de disco posible para el par duplicado de origen de carga es la protección a nivel de controlador. Para proporcionar un nivel más alto de protección al sistema, puede utilizar la duplicación de disco de origen de carga remoto y la duplicación de disco DASD remota.

El soporte de duplicación de disco DASD remota, si se combina con la duplicación de disco de origen de carga remoto, duplica el DASD de los buses ópticos locales con el DASD de los buses ópticos que terminan en una ubicación remota. En esta configuración, la totalidad del sistema, incluido el origen de carga, se puede proteger en caso de que se produzca un siniestro en el local. Si se pierde la ubicación remota, el sistema puede continuar funcionando en el DASD de la ubicación local. Si se pierden el DASD local y la unidad del sistema local, se puede conectar una unidad del sistema nueva al conjunto de DASD de la ubicación remota, y se puede reanudar el proceso en el sistema.

La duplicación de disco DASD remota, al igual que la duplicación de disco DASD estándar, soporta la mezcla de unidades de discos protegidas por paridad de dispositivo en la misma agrupación de discos con unidades de discos protegidas por duplicación de discos; el DASD de paridad de dispositivos puede

ubicarse en el sitio local o remoto. No obstante, si se produce un siniestro en el sitio que contiene el DASD de paridad de dispositivo, se perderán todos los datos de las agrupaciones de discos que contienen el DASD de paridad de dispositivo.

La duplicación de disco remota permite dividir las unidades de discos del sistema en un grupo de DASD locales y un grupo de DASD remotos. Los DASD remotos se conectan a un conjunto de buses ópticos y los DASD locales a otro conjunto de buses. Los DASD locales y remotos pueden estar separados físicamente y encontrarse en diferentes ubicaciones extendiendo los buses ópticos adecuados a la ubicación remota. La distancia entre las ubicaciones está limitada por la distancia hasta la que se puede extender un bus óptico.

Para obtener más información acerca de la duplicación de disco DASD remota, consulte los siguientes temas:

Duplicación de disco DASD remota: ventajas
Duplicación de disco DASD remota: desventajas
Comparación de la duplicación de disco estándar o remota

Si decide que la duplicación de disco DASD remota es conveniente para su sistema, tendrá que preparar el sistema y después iniciar la duplicación de disco de ubicación a ubicación.

Duplicación de disco de origen de carga remoto

El soporte de duplicación de disco de origen de carga remoto permite a las dos unidades de discos del origen de carga estar en IOP o buses del sistema diferentes, lo que proporciona protección por duplicación de disco a nivel de IOP o a nivel de bus para el origen de carga. Sin embargo, en este tipo de configuración el sistema sólo puede realizar la IPL y los vuelcos de almacenamiento principal en el origen de carga conectado al MFIOP. Si el origen de carga conectado al MFIOP sufre una anomalía, el sistema puede continuar funcionando en la otra unidad de discos del par duplicado de origen de carga, pero no podrá realizar IPL o vuelcos de almacenamiento principal hasta que el origen de carga conectado al MFIOP se repare y pueda utilizarse.

Para obtener más información acerca de la duplicación de disco de origen de carga remoto, consulte los siguientes temas:

- Habilitación de la duplicación de disco de origen de carga remoto
- Inhabilitación de la duplicación de disco de origen de carga remoto
- Utilización de la duplicación de disco de origen de carga remoto con DASD locales

Habilitación de la duplicación de disco de origen de carga remoto: Para utilizar el soporte de duplicación de disco de origen de carga remoto, primero hay que habilitarlo. A continuación, debe iniciarse la protección por duplicación de disco en la agrupación de discos 1. Si se habilita el soporte de duplicación de disco de origen de carga remoto después de que se haya iniciado la protección por duplicación de disco en la agrupación de discos 1, la protección por duplicación de disco y el emparejamiento de duplicación de disco existentes del origen de carga no se cambiarán.

El soporte de duplicación de disco de origen de carga remoto puede habilitarse en el entorno DST o SST en iSeries Navigator o la interfaz basada en caracteres. Si intenta habilitar la duplicación de disco de origen de carga remoto y ya está habilitada, el sistema visualizará un mensaje que indica que la duplicación de disco de origen de carga remoto ya está habilitada. No hay ningún otro error o aviso para la habilitación del soporte de duplicación de disco de origen de carga remoto.

Para habilitar la duplicación de disco de origen de carga remoto haga lo siguiente:

1. En el menú principal de DST seleccione la opción 4, Trabajar con unidades de discos.
2. En el menú Trabajar con unidades de discos seleccione la opción 1, Trabajar con configuración de disco.
3. En el menú Trabajar con configuración de disco seleccione la opción 4, Trabajar con protección por duplicación de disco.

4. En el menú Trabajar con protección por duplicación de disco seleccione la opción 4, Habilitar duplicación de disco de origen de carga remoto. Se muestra una pantalla de confirmación Habilitar duplicación de disco de origen de carga remoto.
5. Pulse Intro en la pantalla de confirmación Habilitar duplicación de disco de origen de carga remoto. Se muestra la pantalla Trabajar con protección por duplicación de disco, con un mensaje en la parte inferior que indica que se ha habilitado la duplicación de disco de origen de carga remoto.

Inhabilitación de la duplicación de disco de origen de carga remoto: Si desea inhabilitar el soporte de duplicación de disco de origen de carga remoto, debe elegir entre una de las siguientes opciones:

- Detener la protección por duplicación de disco y luego inhabilitar el soporte de duplicación de disco de origen de carga remoto

o

- Trasladar el origen de carga remoto al MFIOP y luego inhabilitar el soporte de duplicación de disco de origen de carga remoto.

  Si el origen de carga remoto se traslada al MFIOP, el IOP y el sistema pueden no reconocerlo debido a los diferentes tamaños de formato de DASD que utilizan los distintos IOP. Si el origen de carga remoto falta después de haberse trasladado al MFIOP, utilice la función de DST Sustituir unidad de discos para sustituir el origen de carga que falta por él mismo. Esto hará que se vuelva a dar formato al DASD para que el MFIOP pueda utilizarlo, y luego la unidad de discos se sincronizará con el origen de carga activo.

La duplicación de disco de origen de carga remoto se puede inhabilitar desde las DST o las SST. Sin embargo, inhabilitar la duplicación de disco de origen de carga remoto no está permitido si en el sistema hay una unidad de discos de origen de carga que no está conectada al MFIOP. Si intenta inhabilitar el soporte de duplicación de disco de origen de carga remoto y actualmente ya está inhabilitado, el sistema visualizará un mensaje que indica que la duplicación de disco de origen de carga remoto ya está inhabilitada.

Para inhabilitar el soporte de duplicación de disco de origen de carga remoto haga lo siguiente:

1. En el menú principal de DST seleccione la opción 4, Trabajar con unidades de discos.
2. En el menú Trabajar con unidades de discos seleccione la opción 1, Trabajar con configuración de disco.
3. En el menú Trabajar con configuración de disco seleccione la opción 4, Trabajar con protección por duplicación de disco.
4. En el menú Trabajar con protección por duplicación de disco seleccione la opción 5, Inhabilitar duplicación de disco de origen de carga remoto. Se muestra una pantalla de confirmación Inhabilitar duplicación de disco de origen de carga remoto.
5. Pulse Intro en la pantalla de confirmación Inhabilitar duplicación de disco de origen de carga remoto. Se muestra la pantalla Trabajar con protección por duplicación de disco, con un mensaje en la parte inferior que indica que se ha inhabilitado la duplicación de disco de origen de carga remoto.

Utilización de la duplicación de disco de origen de carga remoto con DASD locales: La duplicación de disco de origen de carga remoto se puede utilizar para obtener protección a nivel de IOP o a nivel de bus para el par duplicado de origen de carga, incluso sin buses o DASD remotos en el sistema. No se requiere ninguna configuración especial, aparte de garantizar que una unidad de discos con la misma capacidad que el origen de carga esté conectada a otro IOP o bus del sistema. Si desea obtener una protección a nivel de bus de todos los pares duplicados de una agrupación de discos, debe configurar el sistema de forma que no haya más de la mitad de los DASD de una capacidad dada de una agrupación de discos conectadas a un bus. Si desea obtener una protección a nivel de IOP de todos los pares duplicados de una agrupación de discos, no debe conectar más de la mitad de los DASD de una capacidad dada de la agrupación de discos a un IOP.

Después de haber configurado correctamente el hardware del sistema, habilite la duplicación de disco de origen de carga remoto e inicie la duplicación de disco de las agrupaciones de discos que desea proteger. Utilice la función de inicio de duplicación de disco normal. No existe una función de inicio de duplicación de disco especial para el soporte de origen de carga remoto. El sistema detectará que la duplicación de disco de origen de carga remoto está habilitada y emparejará automáticamente las unidades de discos con el fin de proporcionar el mejor nivel de protección posible. No es posible alterar temporalmente o influir en los pares de las unidades de discos a menos que sea cambiando la manera de configurar y conectar el hardware del sistema. Se aplicarán las restricciones normales de la duplicación de disco concernientes a la capacidad total de la agrupación de discos, como por ejemplo que debe haber un número par de unidades de discos de cada capacidad.

Duplicación de disco DASD remota: ventajas

- La duplicación de disco DASD remota puede proporcionar protección a nivel de IOP o a nivel de bus para el origen de carga.
- La duplicación de disco DASD remota permite repartir los DASD entre dos ubicaciones, siendo una el duplicado de la otra, con el fin de obtener protección en caso de que se produzca un siniestro.

Duplicación de disco DASD remota: desventajas

- Los sistemas que utilizan la duplicación de disco DASD remota sólo pueden realizar la IPL desde un DASD del par duplicado de origen de carga. Si el DASD sufre una anomalía y no se puede reparar concurrentemente, el sistema no puede hacer una IPL hasta que se arregle el origen de carga anómalo y se realice el procedimiento de recuperación del origen de carga remoto.
- Cuando la duplicación de disco DASD remota está activa en un sistema y el origen de carga que éste puede utilizar para realizar IPL sufre una anomalía, el sistema no puede realizar vuelcos de almacenamiento principal si no finaliza satisfactoriamente. Esto significa que el sistema no puede utilizar el vuelco de almacenamiento principal o la alimentación continua del almacenamiento principal (CPM) para reducir el tiempo de recuperación después de una caída del sistema. También significa que el vuelco de almacenamiento principal no está disponible para el diagnóstico del problema que provoca la finalización anómala del sistema.

Comparación de la gestión de DASD en la duplicación de disco estándar y remota

En su mayor parte, la manera de gestionar los DASD en la duplicación de disco remota es equivalente a la manera de gestionar los DASD en la duplicación de disco estándar. Las diferencias consisten en la forma de añadir unidades de discos y en la manera de restaurar la protección por duplicación de disco después de una recuperación.

Adición de unidades de discos: Las unidades de discos desprotegidas deben añadirse en pares, al igual que sucede con la duplicación de disco en general. Para obtener una protección remota de todas las unidades añadidas, la mitad de las nuevas unidades de cada capacidad de los DASD debe estar en el grupo remoto y la otra mitad en el grupo local. Pueden añadirse unidades protegidas por paridad de dispositivo a las agrupaciones de discos utilizando la duplicación de disco remota. No obstante, la agrupación de discos no se protegerá contra siniestros en el sitio.

Restauración de la protección por duplicación de disco remoto después de una recuperación:
Para restaurar la protección por duplicación de disco a continuación de los procedimientos de recuperación, será necesario que realice los siguientes pasos:

- Obtenga y conecte físicamente todas las unidades de DASD necesarias.
- Detenga o suspenda la protección por duplicación de disco si actualmente está configurada en el sistema.
- Añada las unidades DASD nuevas en las agrupaciones de discos correctas.
- Reanude la protección por duplicación de disco.

Si desea obtener información detallada sobre cómo recuperar sistemas con protección por duplicación de disco, puede consultar la publicación Copia de seguridad y recuperación  .

Preparación del sistema para la duplicación de disco remota

Cuando inicia la duplicación de disco remota en el sistema, el DASD local se duplica en el DASD remoto. Si se produce un siniestro en la ubicación local o remota, sigue existiendo una copia completa de todos los datos del sistema, se puede recuperar la configuración del sistema y el proceso puede continuar. Para proporcionar protección contra siniestros en el sitio, todos los DASD de todas las agrupaciones de discos del sistema deben duplicarse formando pares local-remoto. Realice los siguientes pasos con el fin de preparar el sistema para la duplicación de disco remota:

1. Planifique cuáles van a ser los buses ópticos que controlarán el DASD de la ubicación remota.
   - Desde el punto de vista funcional, no es necesario que la ubicación local y la ubicación remota utilicen el mismo número de buses; no obstante, resulta más sencillo configurar y comprender el sistema si el número de DASD y buses remotos y locales es el mismo.
   - Es funcionalmente necesario que tanto el sitio local como el remoto tengan el mismo número de cada capacidad de DASD en cada agrupación de discos.
2. Planifique la distribución de los DASD, muévalos si es necesario y verifique que la mitad de cada capacidad de DASD de cada agrupación de discos se conecta al conjunto local y remoto de buses.
3. Indique al sistema qué buses controlan el DASD remoto y qué buses controlan el DASD local. Para ello, primero tiene que buscar los buses que controlan el DASD remoto y anotar estos números de bus. Luego tiene que cambiar los ID de recurso del sistema de los buses remotos para que empiecen por *R*.

   Por ejemplo, si el BUS11 controla el DASD remoto, cambiará el ID de recurso del sistema de dicho bus por *RBUS11*

Cómo buscar buses remotos: Si los buses no están etiquetados, tal vez tenga que rastrearlos a mano para ver cuáles de ellos van a las ubicaciones remotas. También puede utilizar el Gestor de servicios de hardware para averiguar qué buses van a qué unidades de expansión.

Para utilizar el Gestor de servicios de hardware con el fin de buscar los buses que controlan el DASD remoto, realice los siguientes pasos:

1. En el menú principal de DST, seleccione la opción 7 (Iniciar una herramienta de servicio).
2. En la pantalla Iniciar una herramienta de servicio, seleccione la opción 4 (Gestor de servicios de hardware).
3. En el menú Gestor de servicios de hardware seleccione la opción 2, Recursos de hardware lógico.
4. En el menú Recursos de hardware lógico seleccione la opción 1, Recursos de bus del sistema.
5. En la pantalla Recurso de hardware lógico de bus del sistema, especifique la opción 8 delante de cada bus para visualizar los recursos empaquetados asociados.
6. La pantalla Recursos empaquetados que están asociados con un recurso lógico muestra el ID de trama y el nombre de recurso de la unidad de expansión que está asociada con el bus. Si necesita más información como ayuda para buscar y distinguir la unidad de expansión en cuestión, especifique la opción 5 para la Unidad de expansión del sistema a fin de visualizar más información detallada acerca de la unidad de expansión.

   Anote la ubicación remota o local del bus. Luego repita este procedimiento para todos los buses del sistema.

Cambio de los nombres de recurso de bus remoto: Cuando sepa cuáles son los buses que controlan el DASD remoto, utilice el Gestor de servicios de hardware para cambiar los nombres de recurso de los buses remotos.

Para cambiar los nombres de recurso de los buses remotos, realice los siguientes pasos:

1. En el menú principal de DST, seleccione la opción 7 (Iniciar una herramienta de servicio).
2. En la pantalla Iniciar una herramienta de servicio, seleccione la opción 4 (Gestor de servicios de hardware).
3. En el menú Gestor de servicios de hardware seleccione la opción 2, Recursos de hardware lógico.

4. En el menú Recursos de hardware lógico seleccione la opción 1, Recursos de bus del sistema.
5. En la pantalla Recurso de hardware lógico de bus del sistema, seleccione con el número 2 el bus cuyo nombre desea cambiar. Se mostrará la pantalla Cambiar detalle de recurso de hardware lógico.
6. En la línea Nuevo nombre de recurso de la pantalla Cambiar detalle de recurso de hardware lógico, cambie el nombre de recurso añadiendo la letra *R* al principio del nombre de recurso del bus; por ejemplo, cambie *BUS08* por *RBUS08*. Pulse Intro para cambiar el nombre de recurso.

   Repita este procedimiento en cada bus remoto del sistema.

Inicio de la duplicación de disco de ubicación a ubicación

Cuando haya preparado el sistema, realice los siguientes pasos para iniciar la duplicación de disco remota:

1. Habilite la duplicación de disco de origen de carga remoto. Esto le permite tener un origen de carga como parte del grupo remoto de DASD.
2. Inicie la duplicación de disco utilizando la función de inicio de duplicación de disco normal.

   Cuando se inicie la duplicación de disco, el sistema utilizará el nombre de recurso para reconocer los buses remotos e intentará emparejar el DASD de los buses remotos con el DASD de los buses locales. Como la duplicación de disco de origen de carga remoto está habilitada, el sistema también emparejará el origen de carga con un DASD remoto. Se aplicarán las restricciones normales de la duplicación de disco concernientes a la capacidad total de la agrupación de discos, como por ejemplo que debe haber un número par de unidades de discos de cada capacidad.
3. En la pantalla de confirmación para iniciar la duplicación de disco, compruebe que todos los pares duplicados tienen un nivel de protección de *Bus remoto*. Si no lo tienen, pulse F12 para cancelar el inicio de la duplicación de disco, averigüe el motivo por el que algunas unidades tienen un nivel de protección más bajo del esperado, arregle el problema e intente iniciar de nuevo la duplicación de disco.

Capítulo 2. Elección del nivel de protección

Existen varias maneras de configurar el sistema para sacar partido de las funciones de protección de disco. Antes de seleccionar las opciones de protección de disco que desea utilizar, compare el alcance de la protección que cada una de ellas proporciona.

- Comparación de las opciones de protección de disco
- Comparación entre la protección por duplicación completa y la protección por duplicación parcial

Después de comparar las opciones de protección de disco, seleccione uno de los siguientes métodos de utilización de las opciones:

- Protección completa — Una única agrupación de discos
- Protección completa — Varias agrupaciones de discos
- Protección parcial — Varias agrupaciones de discos
- “Asignación de las unidades de discos a las agrupaciones de discos” en la página 55

Comparación de las opciones de protección de disco

Al seleccionar las opciones de protección de disco deberá tener en cuenta las siguientes consideraciones:

- Con la protección por paridad de dispositivos y la protección por duplicación de disco, el sistema sigue funcionando después de una única anomalía de disco. Con la protección por duplicación de disco, el sistema puede seguir funcionando después de una anomalía de un componente relacionado con disco, por ejemplo, un controlador o un IOP.
- Si se produce una segunda anomalía de disco que provoca que el sistema tenga dos discos anómalos, es más probable que el sistema siga ejecutándose con la protección por duplicación de disco que con la protección por paridad de dispositivos. Con la protección por paridad de dispositivos, la probabilidad de que el sistema deje de funcionar después de producirse la segunda anomalía de disco se puede expresar como P entre n, siendo P el número total de discos del sistema y n el número de discos del conjunto de paridad de dispositivos que sufrió la primera anomalía de disco. Con la protección por duplicación de disco, la probabilidad de que el sistema deje de funcionar al producirse la segunda anomalía de disco es de 1 entre n.
- La protección por paridad de dispositivos requiere un disco de capacidad de disco existente por grupo de paridad para el almacenamiento de información de paridad. Un sistema con protección por duplicación de disco requiere el doble de capacidad de disco que el mismo sistema cuando no tiene protección por duplicación de disco, porque toda la información se almacena dos veces. La protección por duplicación de disco también puede necesitar más buses, IOP y controladores de disco, en función del nivel de protección deseado. Por lo tanto, la protección por duplicación de disco es típicamente una solución más cara que la protección por paridad de dispositivos.
- Normalmente, ni la protección por paridad de dispositivos ni la protección por duplicación de disco tienen un efecto significativo en el rendimiento del sistema. De hecho, en algunos casos la protección por duplicación de disco lo mejora.
- El tiempo necesario para restaurar datos en unidades de disco protegidas mediante protección por paridad de dispositivos es superior al tiempo necesario para realizar la restauración en los mismos dispositivos sin la protección por paridad de dispositivos activada, porque es necesario calcular y grabar los datos de paridad.

La siguiente tabla proporciona una visión general de las herramientas de disponibilidad que se pueden utilizar en el servidor para la protección contra diferentes tipos de anomalías.

¿Qué tipo de disponibilidad es necesaria?	Protección por paridad de dispositivos	Protección por duplicación de disco	Agrupaciones de discos básicas	Agrupación de discos independiente
Protección contra pérdidas de datos debidas a anomalías de hardware relacionado con disco	Sí	Sí	Ver nota[2]	Ver nota[2]
Mantener la disponibilidad	Sí	Sí	No	Sí[4]
Ayuda en la recuperación de la unidad de discos	Sí	Sí	Sí[2]	Sí[2]
Mantener disponibilidad durante anomalía de adaptador de E/S (IOA)	No	Sí[1]	No	No
Mantener disponibilidad durante anomalía de procesador de E/S disco	No	Sí[1]	No	No
Mantener disponibilidad durante anomalía de bus de sistema	No	Sí[1]	No	No
Protección contra siniestros en el local	No	Sí[3]	No	No
Posibilidad de conmutar datos entre sistemas	No	No	No	Sí

Notas:

1. Depende del hardware utilizado, de la configuración y del nivel de protección por duplicación de disco.
2. Configurar las agrupaciones de discos puede limitar la pérdida de datos y la recuperación a una única agrupación de discos.
3. Para la protección contra los siniestros en el local, se requiere la duplicación de disco remota.
4. En un entorno agrupado en clusters, una agrupación de discos independiente puede ayudar a mantener la disponibilidad.

Vea también:

- “Cómo gestiona el sistema el almacenamiento auxiliar” en la página 51
- “Cómo se configuran los discos” en la página 52

Comparación entre la protección por duplicación completa y la protección por duplicación parcial

La protección por duplicación completa y la protección por duplicación parcial no proporcionan los mismos resultados de disponibilidad. Estas dos implementaciones de la protección por duplicación son bastante distintas. Los escenarios de una unidad de discos en el servidor iSeries para cada uno de estos dos métodos de duplicación requieren respuestas de usuario diferentes.

Independientemente de si utiliza sólo la agrupación de discos del sistema (agrupación de discos 1) o varias agrupaciones de discos de usuario (de la 2 a la 255), la protección por duplicación completa protege todas las unidades de disco del servidor iSeries. La protección por duplicación parcial sólo protege una parte de las unidades de disco designadas por una o varias agrupaciones de discos. No obstante, no se protegen todas las unidades de almacenamiento de la configuración de discos. En consecuencia, la planificación de la ubicación de las unidades de discos y de las agrupaciones de discos que se seleccionan para su protección por duplicación es más difícil.

Dejando a un lado la planificación de las agrupaciones de discos, las diferencias más significativas entre los dos métodos de protección por duplicación se refieren a la disponibilidad. En la protección por duplicación completa, se maximiza la disponibilidad del servidor iSeries cuando se produce una anomalía del subsistema de discos. En este método de protección por duplicación, no importa cuál es la agrupación de discos en la que se produce la anomalía. En la protección por duplicación parcial, el sistema continúa ejecutándose mientras informa de la unidad de almacenamiento anómala a la cola de mensajes del operador del sistema (QSYSOPR). No obstante, si la anomalía del disco se produce en una agrupación de discos que no tiene protección por duplicación, se envía el SRC A6xx 0266 cuando un trabajo del sistema acceda a dicha agrupación de discos. Dado que las unidades de almacenamiento de la

agrupación de discos no tienen unidades duplicadas, el directorio de la gestión del almacenamiento se vuelve inutilizable y todas las operaciones de entrada y salida de la agrupación de discos se suspenden.

El SRC de atención de disco no significa que el sistema haya finalizado. Todas las operaciones de entrada y salida se ponen en cola para que el representante del servicio técnico pueda investigar la causa de la anomalía del disco. Si el problema no reside en el medio del disco, se sustituyen las tarjetas anómalas, se activa la alimentación de la unidad de discos y el sistema retoma la operación desde el punto en el que se produjo el error del equipo. Se reanudan todas las operaciones de entrada y salida que están en la cola. Sin embargo, si se produce una anomalía en el medio del disco, el representante del servicio técnico realiza un vuelco del almacenamiento principal para minimizar el tiempo necesario para efectuar la siguiente IPL de OS/400 y permite que el sistema finalice el proceso.

En la protección por duplicación completa, la operación del sistema no se ve interrumpida mientras se llevan a cabo los diagnósticos y la mayoría de reparaciones para resolver el problema que causa la anomalía del subsistema de discos. En la protección a nivel de procesador de E/S, el mantenimiento concurrente máximo es posible, en función del error. En todo caso, el usuario tiene un control completo sobre la conclusión del sistema en caso de que sea necesario realizar un apagado para resolver el problema del disco; el sistema no finaliza de forma anómala.

Aunque la protección por duplicación parcial protege los datos críticos y no es necesaria una operación de restauración para los datos de la agrupación de discos protegida, no se dispone de la máxima disponibilidad que ofrece la protección por duplicación completa, debido a la exposición de la agrupación de discos no protegida. Si los requisitos de disponibilidad indican que el sistema debe estar en operación en pocos minutos después de una anomalía o permanecer activo durante la jornada laboral, en muchos casos la protección por duplicación parcial no es una opción válida.

Cómo gestiona el sistema el almacenamiento auxiliar

Para comprender la opción de disponibilidad en el servidor, se necesita un conocimiento básico de cómo el servidor iSeries gestiona el almacenamiento en disco. En el servidor, a la memoria principal se le llama **almacenamiento principal**. El almacenamiento en disco se denomina **almacenamiento auxiliar**. También es posible que se haga referencia al almacenamiento en disco como **DASD (dispositivo de almacenamiento de acceso directo)**.

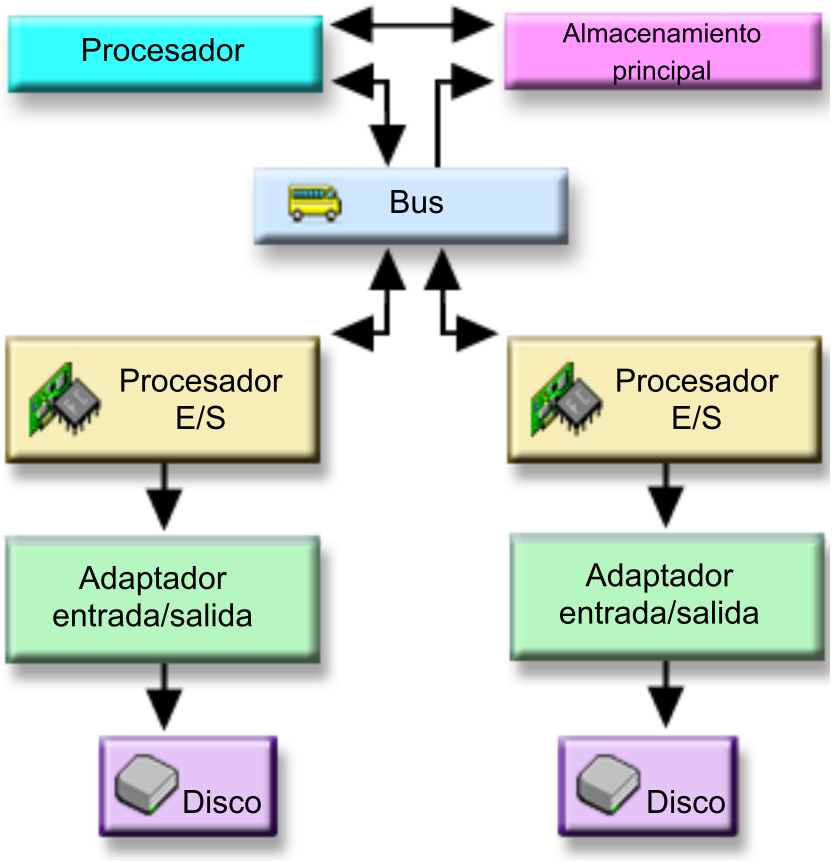
En muchos otros sistemas informáticos usted es el responsable de cómo se almacena la información en los discos. Cuando crea un archivo nuevo, debe indicarle al sistema dónde ponerlo y qué tamaño quiere que tenga. Para proporcionar un buen rendimiento al sistema, tiene que distribuir los archivos equilibradamente entre las distintas unidades de discos. Si más adelante descubre que el tamaño de un archivo debe aumentar, deberá copiarlo en una ubicación del disco que tenga espacio suficiente para el nuevo archivo, que es más grande. Quizás deba pasar archivos de una unidad de discos a otra para mantener el rendimiento del sistema.

El servidor iSeries es diferente, en el sentido de que se responsabiliza de la gestión de la información del almacenamiento auxiliar. Cuando crea un archivo, usted calcula cuántos registros debe tener. El sistema coloca el archivo en la mejor ubicación desde el punto de vista de un buen rendimiento. De hecho, puede repartir los datos del archivo entre varias unidades de discos. Cuando añade más registros al archivo, el sistema asigna espacio adicional a una o más unidades de discos.

El **almacenamiento de nivel único** es la arquitectura exclusiva del servidor iSeries que permite que el almacenamiento auxiliar y el almacenamiento principal trabajen juntos de forma precisa y eficaz. Con el almacenamiento de nivel único, los usuarios de programas y del sistema solicitan los datos por su nombre, no por donde se ubican físicamente. El sistema mantiene un registro del lugar en el almacenamiento principal o el almacenamiento auxiliar en el que se ubica la operación de copia más reciente.

Cómo se configuran los discos

El sistema utiliza varios componentes electrónicos para gestionar la transferencia de datos de un disco al almacenamiento principal. Los datos y los programas deben residir en el almacenamiento principal antes de que puedan utilizarse. En la siguiente ilustración se muestra el hardware utilizado para la transferencia de datos:



Bus: El bus es el canal principal de comunicaciones para la transferencia de datos de entrada y salida. Un sistema puede tener uno o más buses.

Procesador de E/S: El procesador de entrada/salida (IOP) está conectado al bus. El IOP se utiliza para transferir información entre el almacenamiento principal y grupos específicos de controladores. Algunos IOP están dedicados a tipos específicos de controladores, por ejemplo, los controladores de disco. Otros IOP pueden conectar más de un tipo de controlador, por ejemplo, controladores de cinta y controladores de disco.

Adaptador de entrada y salida (IOA): El IOA se conecta al IOP y maneja la transferencia de información entre el IOP y las unidades de discos.

Unidad de discos: Las unidades de discos son los dispositivos reales que contienen las unidades de almacenamiento. El hardware se pide a nivel de unidad de discos. Cada unidad de discos tiene un número de serie exclusivo. Existe información adicional disponible acerca de cómo el servidor direcciona las unidades de almacenamiento por separado.

Cómo direcciona el sistema las unidades de discos por separado

Para trasladar datos a y desde el almacenamiento auxiliar, el sistema necesita una forma de identificar a cada unidad de almacenamiento. Todo componente de hardware (bus, procesador de E/S, controlador y unidad de almacenamiento) tiene una dirección exclusiva.

La dirección de una unidad de almacenamiento consta del bus del sistema, la placa del sistema, la tarjeta del sistema, el bus de E/S, el controlador y los números de dispositivo.

```
      Información detallada de los recursos de hardware de una unidad de discos

Tipo.............: 6603
Modelo...........: 030
Número de serie..: 00-0109928
Nombre de recurso: DD002

Bus SPD
 Bus del sistema.:   1
 Placa sistema...:   0
 Tarjeta sistema.:   1

Almacenamiento
 Bus de E/S......:   0
 Controlador.....:   1
 Dispositivo.....:   0
```

Protección completa — Una única agrupación de discos

Un modo más sencillo de gestionar y proteger el almacenamiento auxiliar es el que se expone a continuación:

- Asigne todas las unidades de discos a una única agrupación de discos (la agrupación de discos del sistema).
- Utilice la protección por paridad de dispositivos en todas las unidades de discos que tengan la posibilidad de hardware.
- Utilice la protección por duplicación de disco para las demás unidades de discos del sistema.

Con este método el sistema sigue funcionando si se produce una anomalía en una unidad de discos. Cuando se sustituye el disco anómalo, el sistema reconstruye la información para evitar la pérdida de datos. El sistema también puede seguir funcionando cuando se produce una anomalía en un componente de hardware relacionado con disco. La configuración determina si el sistema sigue o no funcionando. Por ejemplo, el sistema seguirá funcionando si se produce una anomalía en un IOP y todas las unidades de discos conectadas tienen pares duplicados conectados a un IOP diferente.

Cuando se utiliza una combinación de protección por duplicación de disco y protección por paridad de dispositivos para proteger completamente el sistema, aumentan los requisitos de capacidad de disco. La protección por paridad de dispositivos requiere hasta el 25% del espacio de las unidades de discos para almacenar la información de paridad. La protección por duplicación de disco dobla los requisitos de disco para todos los discos que no tienen la posibilidad de protección por paridad de dispositivos.

Protección completa — Varias agrupaciones de discos

Puede dividir las unidades de discos en varias agrupaciones de discos (agrupaciones de discos auxiliares). A veces, el rendimiento global del sistema puede aumentar al utilizar agrupaciones de discos de usuario. Por ejemplo, puede aislar los receptores de diario en una agrupación de discos básica o secundaria. También puede situar los archivos de históricos o los documentos que raramente sufren modificaciones en una agrupación de discos que tenga unas unidades de disco con un rendimiento menor.

Para proteger completamente el sistema con varias agrupaciones de discos, haga lo siguiente:

- Utilice la protección por paridad de dispositivos en todas las unidades de discos que tengan la posibilidad de hardware.
- Configure la protección por duplicación de disco para cada agrupación de discos del sistema. Puede configurar la protección por duplicación de disco incluso para una agrupación de discos que sólo tenga

unidades de discos con protección por paridad de dispositivos. De este modo, si en el futuro añade unidades que no tienen protección por paridad de dispositivos, estas unidades se protegen por duplicación de disco automáticamente.

Nota: En la protección por duplicación debe añadir unidades nuevas en parejas de unidades con igual capacidad.

Antes de configurar este nivel de protección, asegúrese de que sabe cómo asignar las unidades de discos a las agrupaciones de discos.

Protección parcial — Varias agrupaciones de discos

A veces, la protección completa (utilizando una combinación de protección por paridad de dispositivos y protección por duplicación de disco) puede resultar demasiado cara.Si éste es el caso, tendrá que elaborar una estrategia para proteger la información más importante del sistema. Sus objetivos deben ser reducir al mínimo la pérdida de datos, así como la cantidad de tiempo en que las aplicaciones más importantes no están disponibles. Normalmente, la estrategia conllevará la subdivisión del sistema en agrupaciones de discos básicas e independientes y la protección sólo de unas determinadas agrupaciones de discos. No obstante, tenga en cuenta que pueden aparecer problemas graves si el sistema no está completamente protegido y se produce una anomalía en una unidad de discos desprotegida. Es posible que todo el sistema quede inutilizable, finalice de forma anómala, requiera una recuperación prolongada y haya que restaurar datos de la agrupación de discos que contiene la unidad anómala.

Antes de configurar este nivel de protección, asegúrese de que sabe cómo asignar las unidades de discos a las agrupaciones de discos.

La siguiente lista contiene sugerencias para desarrollar la estrategia:

- Si protege la agrupación de discos del sistema con una combinación de protección por duplicación de disco y protección por paridad de dispositivos, puede reducir o eliminar el tiempo de recuperación. La agrupación de discos del sistema y, en particular, la unidad de origen de carga, contienen información que es fundamental para que el sistema pueda seguir funcionando. Por ejemplo, la agrupación de discos del sistema tiene información de seguridad, información de configuración y direcciones de todas las bibliotecas del sistema.
- Considere cómo puede recuperar la información de los objetos. Si tiene aplicaciones en línea y los objetos cambian constantemente, considere la utilización del registro por diario y la ubicación de los receptores de diario en una agrupación de discos de usuario protegida.
- Piense en la información que no necesita protección, probablemente porque cambia con poca frecuencia. Por ejemplo, tal vez sea necesario que los archivos del registro histórico estén en línea por motivos de consulta, pero los datos de estos archivos pueden no cambiar mas que a fin de mes. Podría poner estos archivos en una agrupación de discos independiente que no tenga ningún tipo de protección de disco. Si se produce una anomalía el sistema no se podrá utilizar, pero los archivos se podrán restaurar sin que se pierdan datos. Lo mismo puede valer para los documentos.
- Considere el resto de información que quizás no necesite protección de disco. Por ejemplo, los programas de aplicación pueden estar en una biblioteca aparte en relación con los datos de aplicación. Probablemente los programas cambiarán con poca frecuencia. Las bibliotecas de programa podrían ponerse en una agrupación de discos básica que no esté protegida. Si se produce una anomalía el sistema no podrá utilizarse, pero los programas se podrán restaurar.

Dos sencillas directrices pueden resumir la lista anterior:

1. Para reducir el tiempo de recuperación, proteja la agrupación de discos del sistema.
2. Para reducir la pérdida de datos, tome decisiones conscientes acerca de cuáles son las bibliotecas y los objetos que deben protegerse.

Asignación de las unidades de discos a las agrupaciones de discos

Si decide que desea tener más de una agrupación de discos, también denominada agrupación de almacenamiento auxiliar (ASP) en la interfaz basada en caracteres, debe determinar la siguiente información para cada agrupación de discos:

- Cuánto almacenamiento necesita.
- Qué protección de disco va a utilizar, si va a utilizarla.
- Qué unidades de discos va a asignar.
- Qué objetos va a poner en la agrupación de discos.

En la publicación Workstation Customization Programming  se proporciona información que le ayudará a tomar estas decisiones.

Cuando trabaje con la configuración de disco, le será de utilidad empezar imprimiendo la configuración actual del sistema. Puede obtener esta información en el Gestor de servicios de hardware en las herramientas de servicio del sistema (SST) o en la carpeta Unidades de disco de iSeries Navigator.

Impreso en España