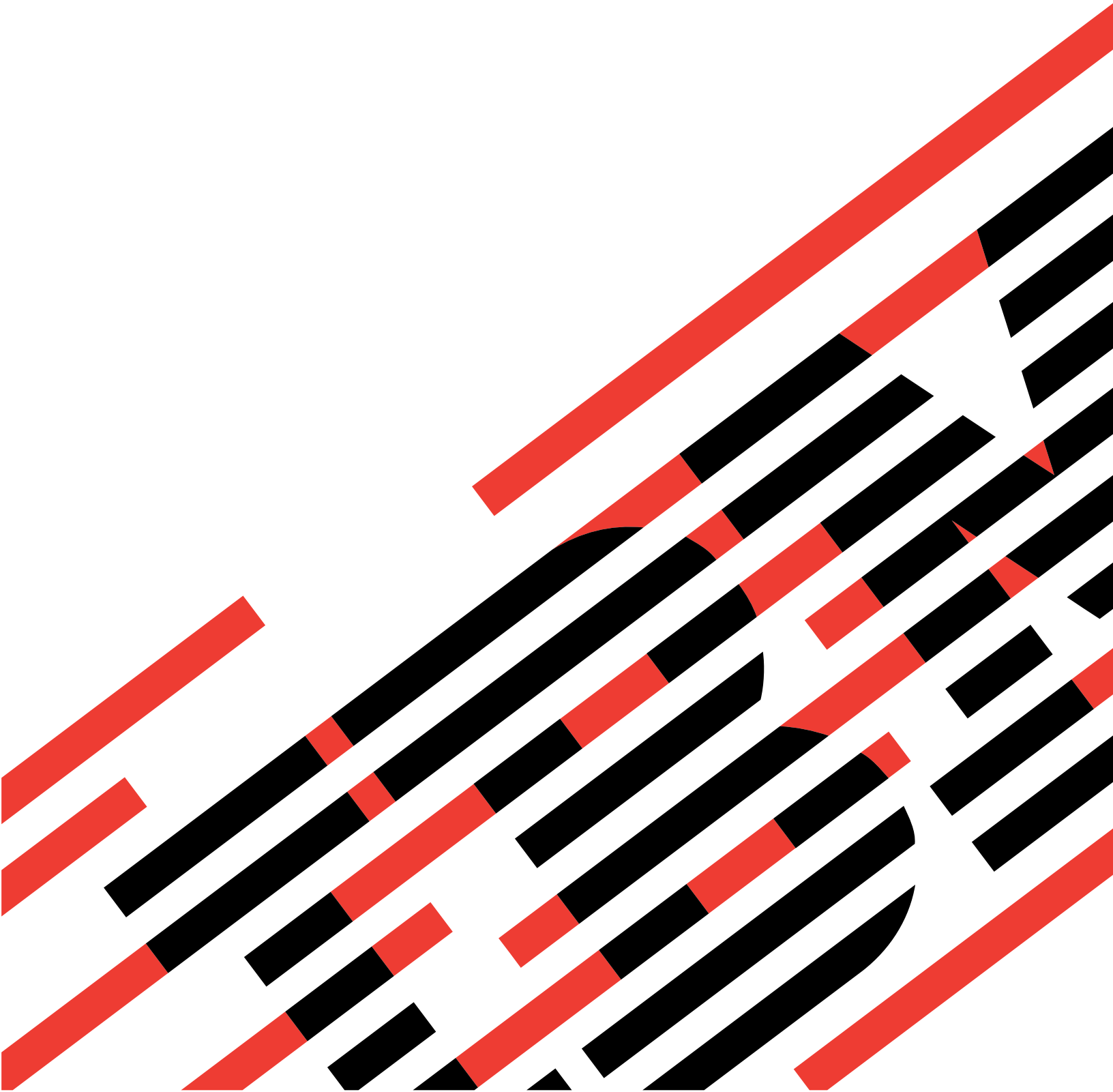
IBM

eserver

iSeries

Protecção do disco



IBM

@server

iSeries

Protecção do disco

Índice

Parte 1. Protecção do disco

Para além de ter uma estratégia de cópia de segurança e recuperação de trabalho, também deverá utilizar qualquer forma de protecção de dados no seu sistema. A forma de o fazer é através da protecção do disco. A protecção do disco pode ajudar a evitar a perda de dados e pode impedir que o sistema pare se ocorrer uma falha do disco. Existem vários métodos de protecção do disco que pode utilizar para proteger melhor os dados. Pode utilizar qualquer combinação destes métodos.

Pode utilizar os assistente de gestão de discos do iSeries Navigator para o ajudar a configurar conjuntos de discos e protegê-los com a protecção por paridade de dispositivos ou protecção por replicação.

Não se esqueça: Embora a protecção do disco possa reduzir o tempo de paragem do sistema ou tornar a recuperação mais rápida, **não** é uma medida de substituição de cópias de segurança regulares. A protecção do disco não poderá ajudá-lo a recuperar de uma perda total do sistema, de uma falha de processador ou de uma falha de programa.

Estes tópicos fornecem informações sobre os diferentes tipos de protecção do disco e sobre como utilizá-los em conjunto:

- Seleccionar ferramentas de protecção do disco
- Seleccionar o seu nível de protecção

Antes de continuar, se desejar, poderá rever estes tópicos:
- Como o sistema gere a memória auxiliar
- Como os discos estão configurados

Capítulo 1. Seleccionar ferramentas de protecção do disco

Quando pensa em proteger o seu sistema contra a perda de dados, tem de considerar o seguinte:

Recuperação
Pode recuperar as informações que perdeu, restaurando-as a partir de um suporte de cópia de segurança ou criando-as de novo?

Disponibilidade
Pode reduzir o tempo durante o qual o sistema está indisponível após ocorrer um problema?

Assistência
Pode prestar-lhe assistência sem afectar o utilizador dos dados?

A sua primeira defesa contra a perda de dados é uma boa estratégia de cópia de segurança e recuperação. Necessita de um plano para guardar regularmente as informações existentes no sistema.

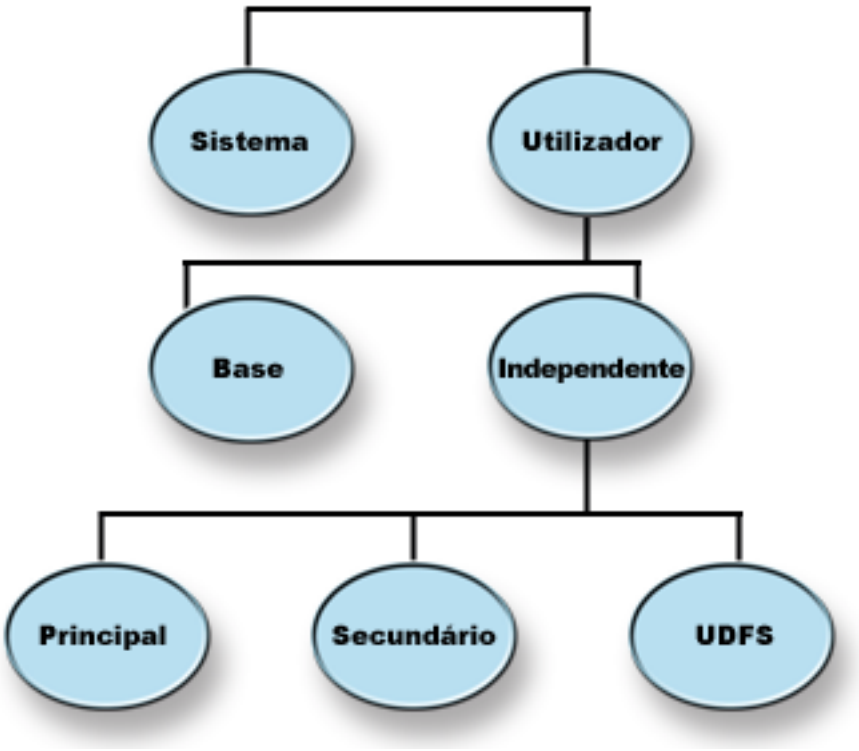
Estão disponíveis várias ferramentas de disponibilidade do disco para reduzir ou eliminar o tempo de paragem do sistema e ajudá-lo a recuperar dados após uma falha do disco:

- Conjuntos de discos
- Protecção por paridade de dispositivos
- Protecção por replicação

Conjuntos de discos

Um conjunto de discos, também referido como conjunto de memória auxiliar(ASP) na interface baseada em caracteres, é uma definição de software de um grupo de unidades de discos do sistema. Isto significa que um conjunto de discos não corresponde necessariamente à disposição física dos discos. Conceptualmente, cada conjunto de discos do seu sistema é um conjunto separado de unidades de discos para armazenamento de nível único. O sistema distribui os dados pelas unidades de discos incluídas num conjunto de discos. Se ocorrer uma falha do disco, só será necessário recuperar os dados no conjunto de discos que continha a unidade em falha. Existem duas categorias principais de conjuntos de discos: o conjunto de discos do sistema e conjuntos de discos do utilizador. Existem dois tipos de conjuntos de discos do utilizador: base e independente. Os conjuntos de discos independentes estão ainda subdivididos em conjuntos de discos principal, secundário e UDFS. Consulte as seguintes ligações e a figura relativa aos conjuntos de discos para compreender os diferentes tipos de conjuntos de discos do utilizador:

- Conjunto de discos do sistema
- Conjuntos de discos do utilizador



O seu sistema pode ter várias unidades de discos anexadas para armazenamento de conjuntos de discos. Para o sistema, as unidades são como uma única unidade de memória. O sistema distribui os dados pelas unidades de discos. Pode utilizar conjuntos de discos para dividir as unidades de discos em subconjuntos lógicos. Para ter mais ideias sobre como utilizar conjunto de discoss no sistema, consulte Conjuntos de discos—exemplos de utilizações.

Quando atribui as unidades de discos no seu sistema a mais do que um conjunto de discos, cada conjunto de discos pode ter estratégias diferentes por questões de disponibilidade, cópia de segurança, recuperação e rendimento.

Os conjuntos de discos oferecem uma vantagem em termos de recuperação no caso de o sistema sofrer uma falha numa unidade, resultando na perda de dados. Se isto acontecer, a recuperação só é necessária para os objectos no conjunto de discos que continham a unidade de discos em falha. Os objectos do sistema e do utilizador noutros conjuntos estão protegidos contra falhas do disco. Também existem benefícios adicionais, bem como certoscustos e limitações que são inerentes à utilização de conjuntos de discos.

Para obter mais informações sobre conjuntos de discos, consulte, os seguintes tópicos:

- Decidir como configurar conjuntos de discos do utilizador
- Considerar a criação de um novo conjunto de discos num sistema activo
- Certificar-se de que o sistema tem espaço de trabalho suficiente
- Contraste entre conjuntos de discos base e independentes

Para obter informações sobre como implementar conjunto de discoss na sua empresa, consulte o manual Cópia de Segurança e Recuperação.

Decidir como configurar conjuntos de discos do utilizador

Pode utilizar conjuntos de discos para várias finalidades diferentes, dependendo das necessidades da sua empresa. Antes de configurar quaisquer conjuntos de discos do utilizador, examine os tópicos que descrevem as várias utilizações.

- Utilizar conjuntos de discos para disponibilidade
- Utilizar conjuntos de discos para aumento do rendimento
- Utilizar conjuntos de discos com objectos da biblioteca de documentos
- Utilizar conjuntos de discos com registo em diário alargado
- Utilizar conjuntos de discos com registo em diário de caminhos de acesso

Utilizar conjuntos de discos para disponibilidade

As diferentes partes do sistema podem ter diferentes requisitos de disponibilidade e recuperação. Por exemplo, pode ter um grande ficheiro do histórico que só seja alterado no final de cada mês. As informações do ficheiro são úteis, mas não são essenciais. Pode colocar este ficheiro numa biblioteca separada num conjunto de discos do utilizador que não tenha qualquer protecção de disco (protecção por replicação ou protecção por paridade de dispositivos). Pode omitir esta biblioteca das suas operações guardar diárias. Guarde-a apenas no fim do mês, quando for actualizada.

Outro exemplo seriam documentos e arquivadores. Alguns são essenciais para a organização. Esses documento e arquivadores devem ser protegidos com protecção por paridade de dispositivos ou protecção por replicação. Eles podem ser colocados num conjunto de discos protegido do utilizador. Outros são mantidos no sistema para fornecer informações, mas não são alterados com frequência. Podem encontrar-se num conjunto de discos de utilizador diferente, com uma estratégia diferente para salvaguarda e protecção.

Utilizar conjuntos de discos para aumento do rendimento

Se estiver a utilizar conjuntos de discos do utilizador para obter um maior rendimento, considere a possibilidade de dedicar o conjunto de discos a um objecto que seja muito activo. Neste caso, pode configurar o conjunto de discos com uma única unidade de discos.

No entanto, normalmente, o facto de colocar uma única unidade protegida por paridade de dispositivo num conjunto de discos do utilizador não aumenta o rendimento, uma vez que o rendimento dessa unidade é afectado por outras unidades de discos no conjunto de paridade de dispositivo.

A atribuição de um conjunto de discos do utilizador exclusivamente para receptores de diário que estejam anexados ao mesmo diário pode aumentar o rendimento do registo em diário. Ao ter o diário e os objectos registados em diário num conjunto de discos separado dos receptores de diário anexados, não existe contenção para as operações de escrita do receptor de diário. As unidades que estiverem associadas ao conjunto de discos não terão de ser reposicionadas antes de cada operação de leitura ou escrita.

O sistema dispersa os receptores de diário por várias unidades de disco para melhorar o rendimento. O receptor de diário pode ser colocado num máximo de dez unidades de discos de um conjunto de discos. Se especificar a opção de diário RCVSIZOPT(*MAXOPT1) ou (*MAXOPT2), o sistema poderá colocar o receptor de diário num máximo de 100 unidades de discos num conjunto de discos. Se adicionar mais unidades de discos ao conjunto de discos enquanto o sistema estiver activo, o sistema determinará se se deverão utilizar as novas unidades de discos para receptores de diário da próxima vez que a função alterar diário for executada.

Outra forma de aumentar o rendimento é certificar-se de que existem unidades de memória suficientes no conjunto de discos do utilizador para suportar o número de operações de input e output físicas que são executadas nos objectos do conjunto de discos do utilizador. Pode ter de experimentar movendo objectos para um conjunto de discos de utilizador diferente e, em seguida, supervisionando o rendimento no conjunto de discos para verificar se as unidades de memória são utilizadas em excesso. Para mais informações sobre como trabalhar com estado do disco (comando WRKDSKSTS), para determinar se as

unidades de memória têm utilização excessiva, consulte o manual *Work Management*. . Se as unidades de forem utilizadas em excesso, deverá considerar a adição de mais unidades de discos ao conjunto de discos do utilizador.

Utilizar conjuntos de discos com objectos da biblioteca de documentos

Pode colocar objectos da biblioteca de documentos (DLOs) em conjuntos de discos do utilizador. Seguem-se as vantagens possíveis da colocação de DLOs em conjuntos de discos do utilizador:

- A capacidade de reduzir tempos de salvaguarda de DLOs e de os separar por requisitos de salvaguarda.
- A capacidade de separar DLOs por requisitos de disponibilidade. Os DLOs críticos podem ser colocados em conjuntos de discos do utilizador que estejam protegidos com a protecção por replicação ou protecção por paridade de dispositivos. Os DLOs que sejam alterados com pouca frequência podem ser colocados em conjuntos de discos não protegidos com unidades mais lentas.
- A capacidade de aumentar o número de documentos.

Se tiver uma edição actual do programa licenciadoOS/400, poderá executar vários procedimentos SAVDLO ou RSTDLO em conjuntos de discos diferentes. Também poderá executar várias operações SAVDLO no mesmo conjunto de discos.

Um método de colocar DLOs em conjuntos de discos do utilizador é deixar apenas DLOs do sistema (arquivadores fornecidos pela IBM) no conjunto de discos do sistema. Mova outros arquivadores para conjuntos de discos do utilizador. Os arquivadores do sistema não mudam com frequência e, por isso, podem ser guardados com pouca frequência. ″Como Transferir um Arquivador para um Conjunto de Discos Diferente″ no manual Cópia de Segurança e Recuperação , descreve o procedimento a seguir ao mover arquivadores do conjunto de discos do sistema para conjuntos de discos do utilizador ou entre conjuntos de discos de utilizador.

Pode especificar um conjunto de discos no comando SAVDLO. Isto permite-lhe guardar todos os DLOs de um conjunto de discos em particular, num determinado dia da semana. Por exemplo, poderia guardar DLOs do conjunto de discos 2 na Segunda-feira, DLOs do conjunto de discos na terça-feira, etc. Pode guardar todos os DLOs alterados diariamente.

Os passos de recuperação, caso utilize este tipo de técnica de salvaguarda, dependem das informações perdidas. Se perdeu um conjunto de discos inteiro, pode restaurar a última cópia guardada completa dos DLOs a partir desse conjunto de discos. Em seguida, deve restaurar os DLOs alterados a partir das cópias diárias.

Quando guardar DLOs de vários conjuntos de discos na mesma operação, será criado um ficheiro e um número de sequência diferentes na banda para cada conjunto de discos. Quando restaurar, terá de especificar o número de sequência correcto. Este facto facilita o restauro dos DLOs alterados apenas para o conjunto de discos que se perdeu, sem ser necessário saber os nomes de todos os arquivadores.

Quando especificar DLO(*SEARCH) ou DLO(*CHG) para o comando SAVDLO, especifique um conjunto de discos, se possível. A especificação de um conjunto de discos poupa recursos do sistema.

Restrições para DLOs em Conjuntos de Discos do Utilizador: Aplicam-se as seguintes restrições e limitações ao colocar DLOs em conjuntos de discos do utilizador:

- Quando utilizar um ficheiro de salvaguarda para uma operação guardar, poderá guardar DLOs de apenas um conjunto de discos.
- Se guardar num ficheiro de salvaguarda e especificar SAVDLO DLO(*SEARCH) ou SAVDLO DLO(*CHG), também terá de especificar um conjunto de discos, mesmo que saiba que os resultados da procura se encontram num único conjunto de discos.

- Os documentos que não se encontram em arquivadores têm de estar no conjunto de discos dos sistema.
- O correio pode ser guardado num arquivador ou num conjunto de discos do utilizador. O correio não arquivado encontra-se no conjunto de discos do sistema.

Utilizar conjuntos de discos com registo em diário alargado

Se os diários e os objectos que estejam a ser registados em diário se encontrarem no mesmo conjunto de discos que os receptores e a capacidade do conjunto de discos for excedida, terá de terminar o registo em diário de todos os objectos e recuperar da condição de excesso de capacidade do conjunto de discos.

O manual Cópia de Segurança e Recuperação descreve como recuperar um conjunto de discos com capacidade excedida.

Se o receptor de diário se encontrar num conjunto de discos diferente do do diário e a capacidade do conjunto de discos do utilizador onde se encontra o receptor for excedida, proceda do seguinte modo:

1. Crie um novo receptor num conjunto de discos de utilizador diferente.
2. Altere o diário (comando CHGJRN) para ligar o recém-criado receptor de diário.
3. Guarde o receptor desligado.
4. Elimine-o.
5. Limpe o conjunto de discos com capacidade excedida sem terminar o registo em diário.
6. Crie um novo receptor no conjunto de discos limpo.
7. Ligue o novo receptor com o comando CHGJRN.

Nota: O manual Cópia de Segurança e Recuperação tem mais informações sobre como trabalhar com receptores de diário quando a capacidade de um conjunto de discos é excedida.

Utilizar conjuntos de discos com registo em diário de caminhos de acesso

Se tenciona utilizar o registo em diário explícito de caminhos de acesso, a IBM® recomenda que, primeiro, mude o diário para um receptor de diário no conjunto de discos do sistema (conjunto de discos 1) durante alguns dias. Inicie o registo em diário de caminhos de acesso para ver os requisitos de memória do receptor antes de atribuir o tamanho específico para um conjunto de discos do utilizador. A secção Gestão de Diários fornece mais informações sobre como avaliar os requisitos de memória para o registo em diário.

Considerar a criação de um novo conjunto de discos num sistema activo

Desde a V3R6 do programa licenciado OS/400 que pode adicionar unidades de disco com o sistema activo. Quando adiciona unidades de discos a um conjunto de discos que ainda não exista, o sistema cria um novo conjunto de discos. Consulte Adicionar uma unidade de discos ou um conjunto de discos para ver os passos para configurar um conjunto de discos. Se optar por criar um novo conjunto de discos enquanto o sistema estiver activo, tenha em conta estas considerações:

- Não poderá iniciar o protecção por replicação para um conjunto de discos base enquanto o sistema estiver activo. Pode iniciar a protecção por replicação para um conjunto de discos independente indisponível quando o sistema estiver activo. O novo conjunto de discos só está totalmente protegido se todas as unidades de discos tiverem oprotecção por paridade de dispositivos.
- Não poderá mover as unidades de discos existentes para um conjunto de discos base quando o sistema estiver activo. O sistema tem de mover os dados quando move unidades de discos. Isso só pode ser feito através das Ferramentas de Serviço Dedicadas (DST). Não é possível mover unidades de discos de um conjunto de discos existente para um conjunto de discos independente.
- O sistema utiliza o tamanho de um conjunto de discos do utilizador para determinar o limiar de memória para os receptores de diário que são utilizados peloprotecção de caminhos de acesso geridos pelo sistema (SMAPP). Quando cria um conjunto de discos enquanto o sistema está activo, o tamanho

das unidades de discos que especificar na operação que cria o conjunto de discos é considerado como o tamanho do conjunto de discos da SMAPP. Por exemplo, suponha que adiciona 2 unidades de discos a um novo conjunto de discos, o conjunto de discos 2. A capacidade total das 2 unidades de discos é 2062MB. Mais tarde, adiciona mais 2 unidades de discos para aumentar a capacidade para 4124MB. Por causa da SMAPP, o tamanho do conjunto de discos continua a ser 2062MB até à próxima vez que executar um IPL ou activar um conjunto de discos independente. Isso significa que o limiar de memória dos seus receptores de SMAPP é inferior e que o sistema terá de mudar de receptores com mais frequência. Normalmente, isso não terá consequências significativas no rendimento do sistema.

O sistema determina a capacidade de cada conjunto de discos quando o utilizador executa um IPL ou activa um conjunto de discos independente. Nessa altura, o sistema faz ajustes aos seus cálculos para requisitos de tamanho de SMAPP. Consulte Protecção de caminhos de acesso geridos pelo sistema para obter mais informações sobre a SMAPP.

Certificar-se de que o sistema tem espaço de trabalho suficiente

Quando efectua alterações à configuração do disco, o sistema poderá necessitar de área de trabalho. Isto é particularmente verdadeiro se tenciona mover unidades de discos de um conjunto de discos para outro. O sistema precisa de mover todos os dados da unidade de discos para outras unidades de discos antes de esta ser movida. A secção ″Como Calcular Requisitos de Espaço para um Conjunto de Memória Auxiliar″, no manual Cópia de Segurança e Recuperação , fornece exemplos de como determinar a memória de trabalho necessária para a sua situação. Também existem limites do sistema para a quantidade de memória auxiliar.

Se o sistema não tiver memória temporária suficiente, comece por limpar o espaço em disco. Muitas vezes, os utilizadores mantêm objectos no sistema, como, por exemplo, documentos ou ficheiros em Spool antigos, quando estes objectos já não são necessários. Considere utilizar a função de limpeza automática da Assistência à Operação para libertar algum espaço em disco no sistema.

Se a remoção de objectos desnecessários da memória auxiliar não fornecer, mesmo assim, espaço temporário em disco suficiente, outra alternativa é remover temporariamente objectos do sistema. Por exemplo, se tenciona mover uma grande biblioteca para um novo conjunto de discos do utilizador, pode guardar a biblioteca e removê-la do sistema. Em seguida, restaure a biblioteca após ter movido unidades de discos. Segue-se um exemplo deste processo:

1. Guarde as autoridades privadas para os objectos do sistema escrevendo:
   `SAVSECDTA DEV(`*`unidade de bandas`*`)`
2. Guarde o objecto utilizando o comando SAVxxx correcto. Por exemplo, para guardar uma biblioteca, use o comando SAVLIB. Pode mesmo considerar a salvaguarda do objecto duas vezes em 2 bandas diferentes.
3. Elimine o objecto do sistema utilizando o comando DLTxxx correcto. Por exemplo, para eliminar uma biblioteca, use o comando DLTLIB.
4. Recalcule a capacidade do disco para determinar se disponibilizou espaço temporário suficiente.
5. Se tiver espaço suficiente, execute as operações de configuração do disco.
6. Restaure os objectos que eliminou.

Conjuntos de discos—exemplos de utilizações

Os conjuntos de discos são utilizados para gerir requisitos de rendimento e cópia de segurança, do seguinte modo:

- Pode criar um conjunto de discos para fornecer recursos dedicados para objectos frequentemente utilizados, tais como receptores de diário.
- Pode criar um conjunto de discos para reter ficheiros de salvaguarda. Pode ser efectuada uma cópia de segurança dos objectos para ficheiros de salvaguarda num conjunto de discos diferente. É improvável que o conjunto de discos que contém o objecto e o conjunto de discos que contém o ficheiro de salvaguarda se percam ambos.

- Pode criar conjuntos de discos diferentes para objectos com requisitos de recuperação e disponibilidade diferentes. Por exemplo, pode colocar ficheiros ou documentos de base de dados importantes num conjunto de discos que tenha protecção por replicação ou protecção por paridade de dispositivos.
- Pode criar um conjunto de discos para colocar objectos pouco frequentemente utilizados, tais como grandes ficheiros do histórico, em unidades de discos com um rendimento mais lento.
- Pode utilizar conjuntos de discos para gerir tempos de recuperação de caminhos de acesso de ficheiros de base de dados críticos e não críticos, utilizando a protecção de caminhos de acesso gerida pelo sistema.
- Um conjunto de discos independente pode ser utilizado para isolar dados utilizados pouco frequentemente, de modo a libertar recursos do sistema que só deverão ser utilizados quando necessário.
- Um conjunto de discos independente num ambiente com conjuntos de unidades pode fornecer armazenamento de disco comutável, o que permite que os recursos estejam continuamente disponíveis.

Conjuntos de discos—benefícios

A colocação de objectos em conjuntos de discos de utilizador, também chamados conjuntos de memória auxiliar (ASPs) na interface baseada em caracteres, pode oferecer várias vantagens. Estas vantagens incluem:

- **Protecção de dados adicional**. Ao separar bibliotecas,documentos ou outros objectos num conjunto de discos do utilizador, poderá protegê-los contra a perda de dados em caso de falha de uma unidade de discos do conjunto de discos do sistema ou de outros conjuntos de discos do utilizador. Por exemplo, se ocorrer uma falha numa unidade de discos e os dados contidos no conjunto de discos do sistema se perderem, os objectos contidos nos conjuntos de discos do utilizador não serão afectados e poderão ser utilizados para recuperar objectos no conjunto de discos do sistema. Pelo contrário, se um falha resultar na perda dos dados contidos num conjunto de discos do utilizador, os dados no conjunto de discos do sistema não serão afectados.
- **Aumento do rendimento do sistema**. A utilização de conjuntos de discos também pode aumentar o rendimento do sistema. Isto acontece porque o sistema dedica as unidades de discos que estão associadas a um conjunto de discos aos objectos desse conjunto de discos. Por exemplo, suponha que está a trabalhar num ambiente de registo em diário extensivo. A colocação de diários e dos objectos registados em diário num conjunto de discos do utilizador pode reduzir a contenção entre os receptores e os objectos registados em diário, caso se encontrem em conjuntos de discos diferentes, o que aumenta o rendimento do registo em diário. Se utilizar conjuntos de discos independentes para reduzir a contenção, coloque os objectos a registar em diário no conjunto de discos principal e os receptores de diário num ou mais conjuntos de discos secundários.

  A colocação de vários receptores de diário activos no mesmo conjunto de discos não é produtiva. A contenção resultante entre a escrita em vários receptores do conjunto de discos pode abrandar o rendimento do sistema. Para obter o máximo rendimento, coloque cada receptor de diário activo num conjunto de discos de utilizador separado.
- **Separação de objectos com requisitos de recuperação e disponibilidade diferentes**. Pode utilizar várias técnicas de protecção de disco para conjuntos de discos diferentes. Também pode especificar diferentes tempos destino para a recuperação de caminhos de acesso. Pode atribuir objectos importantes ou muito utilizados a unidades de discos protegidas de elevado rendimento. Pode atribuir grandes ficheiros pouco utilizados, como ficheiros do histórico, a unidades de discos não protegidas, de baixo rendimento.
- **Maior disponibilidade e flexibilidade**. Consulte a secção Benefícios dos conjuntos de memória independentes para ver mais vantagens que são exclusivas dos conjuntos de discos independentes.

Conjuntos de discos—custos e limitações

Existem algumas limitações específicas que poderá encontrar ao utilizar conjuntos de discos (conjuntos de memória auxiliar):

- O sistema não consegue recuperar directamente dados perdidos numa falha ocorrida num suporte de unidade de discos. Esta situação requer a execução de operações de recuperação.
- A utilização de conjuntos de discos pode requerer dispositivos de disco adicionais.
- A utilização de conjuntos de discos exigir-lhe-á a gestão da quantidade de dados existente num conjunto de discos e evitará o excesso de capacidade de um conjunto de discos.
- Terá de executar passos de recuperação especiais se a capacidade de um conjunto de discos base for excedida.
- A utilização de conjuntos de discos requer a gestão de objectos relacionados. Alguns objectos relacionados, tais como diários e objectos registados em diário, têm de estar no mesmo conjunto de discos do utilizador.

Conjunto de discos do sistema

O sistema cria automaticamente o conjunto de discos do sistema (conjunto de discos 1), que contém a unidade de discos 1 e todos os outros discos configurados que não estão atribuídos a um conjunto de discos do utilizador. O conjunto de discos do sistema contém todos os objectos do sistema referentes ao programa licenciado OS/400 e todos os objectos do utilizador que não estão atribuídos a um conjunto de discos base ou independente.

Nota: Pode ter unidades de discos ligadas ao sistema, mas que não estão configuradas e que não estão a ser utilizadas. Estas unidades são designadas unidades de discos **não configuradas**.

Existem considerações adicionais que deve ter em conta relacionadas com a capacidade do conjunto de discos do sistema e a protecção do seu conjunto de discos do sistema.

Capacidade do conjunto de discos do sistema: Se o conjunto de discos do sistema atingir a capacidade máxima, o sistema terminará as actividades normais. Se isso acontecer, terá de executar um IPL do sistema e as acções necessárias (por exemplo, eliminar objectos) para impedir que volte a acontecer.

Também pode especificar um limiar que, uma vez atingido, avise o operador do sistema de uma possível falta de espaço. Por exemplo, se definir o valor do limiar como 80 para o conjunto de discos do sistema, a fila de mensagens do operador de sistema (QSYSOPR) e a fila de mensagens do sistema (QSYSMSG) serão notificadas quando o conjunto de discos do sistema estiver 80% cheio. Será enviada uma mensagem de hora a hora até que o valor de limiar seja alterado ou até que os objectos sejam eliminados ou transferidos do conjunto de discos do sistema. Se ignorar esta mensagem, o conjunto de discos do sistema atingirá a capacidade máxima e o sistema terminará anormalmente.

Pode utilizar um terceiro método para evitar que o conjunto de discos do sistema atinja a capacidade máxima utilizando os valores de sistema QSTGLOWLMT e QSTGLOWACN. Para mais informações, consulte ″Como Alterar o Limiar de Memória para o Conjunto de Memória Auxiliar do Sistema″, no manual Cópia de Segurança e Recuperação  .

Proteger o conjunto de discos do sistema: A IBM recomenda a utilização da protecção por paridade de dispositivos ou protecção por replicação no conjunto de discos do sistema. A utilização das ferramentas de protecção do disco reduz a possibilidade de perda de dados no conjunto de discos do sistema. Se o conjunto de discos do sistema se perder, também se perderá a capacidade de endereçamento para os objectos existentes em cada conjunto de discos do utilizador.

Pode restaurar a capacidade de endereçamento restaurando todo o sistema ou executando o comando Regenerar Memória (RCLSTG). No entanto, o comando RCLSTG não permite recuperar a propriedade dos objectos. Depois de executar o comando, o perfil do utilizador QDFTOWN fica proprietário de todos os objectos. Pode utilizar o procedimento do comando Regenerar Objecto da Biblioteca de Documentos (RCLDLO) para recuperar a propriedade dos objectos da biblioteca de documentos.

Conjuntos de discos do utilizador

Pode criar um conjunto de discos de utilizador agrupando um conjunto de unidades de discos e atribuindo esse grupo a um conjunto de discos. Os conjuntos de discos do utilizador podem conter bibliotecas, documentos e certos tipos de objectos. Os conjuntos de discos do utilizador existem em duas formas: conjuntos de discos base e conjuntos de discos independentes. Num ambiente com conjuntos de unidades, os conjuntos de discos independentes podem ser comutados entre sistemas sem ser necessário executar um IPL, o que permite que os dados estejam continuamente disponíveis. Pode configurar conjuntos de discos base numerados de 2 a 32. Os conjuntos de discos independentes estão numerados de 33 a 255. Para obter mais informações as diferenças entre conjuntos de discos base e independentes, consulte Conjuntos de discos base e independentes contrastantes.

Consulte os seguintes tópicos para obter mais informações sobre conjuntos de discos de biblioteca e sem ser de biblioteca:

- Conjuntos de discos de biblioteca do utilizador
- Conjuntos de discos de utilizador sem ser de biblioteca

Quando tiver conjuntos de discos configurados, deverá protegê-los utilizando a protecção por replicação ou paridade de dispositivos.

Conjuntos de discos de biblioteca do utilizador: Os conjuntos de discos de biblioteca do utilizador contêm bibliotecas e sistemas de ficheiros definidos pelo utilizador (UDFS). A IBM recomenda a utilização de conjuntos de discos de biblioteca do utilizador porque os passos de recuperação são mais fáceis do que os dos conjuntos de discos de utilizador sem ser de biblioteca. Existem vários factores a considerar ao utilizar conjuntos de discos de biblioteca do utilizador.

O que Deve Saber Acerca dos Conjuntos de Discos de Biblioteca do Utilizador:

- **Não** crie bibliotecas de sistema ou de produtos (bibliotecas que comecem por Q ou #) ou arquivadores (arquivadores que comecem por Q) num conjunto de discos do utilizador. **Não** restaure nenhuma destas bibliotecas ou arquivadores para um conjunto de discos do utilizador. Se o fizer, pode provocar resultados imprevisíveis.
- Os conjuntos de discos de biblioteca podem conter bibliotecas e objectos de biblioteca de documentos. A biblioteca de documentos de um conjunto de discos do utilizador chama-se QDOCnnnn, em que *nnnn* corresponde ao número do conjunto de discos.
- Os diários e objectos que estejam a ser registados em diário **têm** de estar no mesmo conjunto de discos. Coloque os receptores de diário num conjunto de discos diferente. Esta medida permite proteger contra a perda dos objectos e dos receptores se ocorrer uma falha no suporte de disco.

  Para iniciar o registo em diário, o diário (tipo de objecto *JRN) e o objecto a registar no diário têm de se encontrar no mesmo conjunto de discos. Utilize os seguintes comandos para iniciar o registo em diário.
  - Comando Iniciar Registo em Diário de Ficheiro Físico (STRJRNPF) para ficheiros físicos
  - Comando Iniciar Registo em Diário de Caminhos de Acesso (STRJRNAP) para caminhos de acesso
  - Comando Iniciar Diário (STRJRN) para objectos do sistema de ficheiros integrado
  - Comando Iniciar Registo em Diário de Objecto (STRJRNOBJ) para outros tipos de objectos

  O registo em diário não poderá ser reiniciado para um objecto que seja guardado e, em seguida, restaurado para um conjunto de discos diferente do que que continha o diário. O diário e o objecto têm de se encontrar no mesmo conjunto de discos para que o registo em diário do objecto seja automaticamente reiniciado.
- Nenhuma rede de bases de dados pode ultrapassar os limites do conjunto de discos. Não é possível criar um ficheiro num conjunto de discos que dependa de um ficheiro noutro conjunto de discos. Todos os ficheiros físicos baseados referentes a um membro de ficheiro lógico têm de se encontrar no mesmo conjunto de discos que o ficheiro lógico. O sistema constrói caminhos de acesso apenas para ficheiros de base de dados no mesmo conjunto de discos que o ficheiro físico baseado (as consultas temporárias não estão limitadas). Os caminhos de acesso nunca são partilhados por ficheiros em

conjuntos de discos diferentes. Os formatos de registo não são partilhados entre conjuntos de discos diferentes. Em vez disso, é ignorado um pedido de formato, sendo criado um novo formato de registo.

- Pode colocar um conjunto de SQL num conjunto de discos do utilizador. O conjunto de discos destino é especificado quando cria o conjunto.
- Se o conjunto de discos de biblioteca do utilizador não contiver ficheiros de base de dados, defina o tempo de recuperação de caminhos de acesso destino para o conjuntos de discos como *NONE. Isso verificar-se-ia, por exemplo, se o conjunto de discos de biblioteca do utilizador contivesse apenas bibliotecas para receptores de diário. Se definir o tempo de recuperação de caminhos de acesso como *NONE, impedirá o sistema de executar trabalho desnecessário nesse conjunto de discos. A Protecção de caminhos de acesso geridos pelo sistema descreve como definir tempos de recuperação de caminhos de acesso.

Conjuntos de discos de utilizador sem ser de biblioteca: Os conjuntos de discos de utilizador sem ser de biblioteca contêm diários, receptores de diário e ficheiros de salvaguarda cujas bibliotecas não se encontram no conjunto de discos do sistema.

Se estiver a atribuir tempos de recuperação de caminhos de acesso para conjuntos de discos individuais, deverá definir o tempo de recuperação destino para um conjuntos de discos de utilizador sem ser de biblioteca como *NONE. Um conjuntos de discos de utilizador sem ser de biblioteca não pode incluir ficheiros de base de dados e não pode, por isso, tirar proveito da protecção de caminhos de acesso geridos pelo sistema (SMAPP). Se definir um tempo de recuperação de caminhos de acesso para um conjuntos de discos de utilizador sem ser de biblioteca com um valor diferente de *NONE, fará com que o sistema tenha trabalho extra sem qualquer vantagem possível. A secção Protecção de caminhos de acesso geridos pelo sistema descreve como definir tempos de recuperação de caminhos de acesso.

Proteger conjuntos de discos: Tenha em consideração as seguintes questões relacionadas com a protecção de conjuntos de discos:

- Todos os conjuntos de discos, incluindo o do sistema, devem ter protecção por replicação ou consistir inteiramente em unidades de discos com protecção por paridade de dispositivo, para assegurar que o sistema continua em execução após uma falha de disco num conjunto de discos.
- Se ocorrer uma falha de disco num conjunto de discos que não tenha protecção por replicação, o sistema pode não continuar em execução, dependendo do tipo de unidade de discos e do erro.
- Se ocorrer uma falha de disco num conjunto de discos que tenha protecção por replicação, o sistema continuará em execução (a menos que ambas as unidades de memória de uma réplica falhem).
- Se uma unidade de discos falhar num conjunto de discos que tenha oprotecção por paridade de dispositivos, o sistema continuará em execução, desde que nenhuma outra unidade de discos do mesmo conjunto de paridade de dispositivos falhe.

Limites do sistema para a memória do conjunto de discos: Durante um IPL, o sistema determina a quantidade de memória auxiliar configurada no sistema. A quantidade total é a soma da capacidade das unidades configuradas e dos respectivos pares replicados, caso existam. As unidades de discos não configuradas não são incluídas. A quantidade de memória em disco é comparada com o máximo suportado por um determinado modelo.

Se for configurada mais do que a quantidade de memória auxiliar recomendada, será enviada uma mensagem (CPI1158) para a fila de mensagens do operador do sistema (QSYSOPR) e para a fila de mensagens QSYSMSG (caso exista no sistema). Esta mensagem indica que existe demasiada memória auxiliar no sistema. Esta mensagem é enviada uma vez durante cada IPL enquanto a quantidade de memória auxiliar no sistema for superior à quantidade máxima suportada.

Conjuntos de discos independentes

Os termos **conjunto de memória auxiliar independente** e **conjunto de discos independente** são sinónimos.

Um conjunto de discos independente é um conjunto de unidades de discos que pode ser colocado online ou offline de forma independente do resto da memória de um sistema, incluindo o conjunto de discos do sistema, conjuntos de discos do utilizador e outros conjuntos de discos independentes. Os conjuntos de discos independentes são úteis quer em ambientes de sistema único, quer em ambientes de vários sistemas. Para obter informações relacionadas, consulte conjunto de discos do sistema e conjunto de discos do utilizador.

Num ambiente de sistema único, um conjunto de discos independente pode ser colocado offline de forma independente de outros conjuntos de discos porque os dados no conjunto de discos independente estão contidos em si mesmos, ou seja, todas as informações de sistema necessárias associadas aos dados do conjunto de discos independente estão contidas no conjunto de discos independente. O conjunto de discos independente também pode ser colocado online enquanto o sistema está activo (não é necessário um IPL). A utilização de conjuntos de discos independentes desta forma pode ser muito útil, por exemplo, se tiver grandes quantidades de dados que não sejam necessários para o processamento diário das actividades da empresa. O conjunto de discos independente que contém estes dados pode ser deixado em modo autónomo até ser necessário. Quando grandes quantidades de memória são mantidas em modo autónomo, determinadas operações como, por exemplo, um IPL ou uma recuperação de memória poderão ser mais rápidas.

Num ambiente de vários sistemas, o conjunto de discos independente pode ser comutado entre sistemas. Um **conjunto de discos independente comutável** é um conjunto de unidades de discos que é possível comutar entre sistemas de modo a que cada sistema possa ter acesso aos dados. Apenas um sistema poderá aceder aos dados de cada vez. Tal como no ambiente de sistema único, o conjunto de discos independente pode ser comutado porque o conjunto de discos independente está contido em si mesmo. Os conjuntos de discos independentes comutáveis podem ajudá-lo a executar as seguintes tarefas:

- Manter os dados disponíveis para uma aplicação mesmo quando um ocorrer uma falha de sistema (programada ou não programada)
- Eliminar o processo de replicação de dados de um sistema para outro.
- Em certas situações, isolar as falhas das unidades de discos no conjunto de discos independente.
- Conseguir uma elevada disponibilidade e escalabilidade.

Para obter mais informações, consulte o tópico Conjunto de Discos Independente.

Contraste entre conjuntos de discos base e independentes

Os conjuntos de discos base e independentes, também chamados conjuntos de memória auxiliar (ASPs) na interface baseada em caracteres, são igualmente úteis para agrupar unidades de discos que contenham certas informações; no entanto, apresentam algumas diferenças inerentes:

- Quando é executado o IPL do servidor, todas as unidades de discos configuradas para um conjunto de discos base têm de ser consideradas para que o servidor continue o IPL. Os conjuntos de memória auxiliar independentes não são incluídos no IPL. Quando activar os ASPs independentes, o nó verificará se todas as unidades de disco estão presentes.
- Quando uma unidade de discos não protegida num conjunto de discos falha, geralmente, pára todo o processamento normal no servidor, até ser reparada. A perda total de uma unidade de discos num conjunto de discos base requer procedimentos morosos para restaurar os dados perdidos, antes de o servidor poder executar o IPL e retomar o funcionamento normal.
- Os dados num conjunto de discos base pertencem ao nó de ligação e só podem ser directamente acedidos por esse sistema. Num conjunto de discos independente, os dados não pertencem ao nó, mas sim ao conjunto de discos independente. Pode partilhar os dados no conjunto de discos independente entre os nós de um conjunto de unidades, desactivando-o num nó e activando-o noutro nó.
- Quando cria um conjunto de discos base, atribui-lhe um número. Quando cria um conjunto de discos independente, atribui-lhe um nome e o sistema atribui-lhe um número.
- Se um conjunto de discos base ficar cheio, pode transpor os dados excedentes para o conjunto de discos do sistema. Os conjuntos de discos independentes não podem transpor os dados excedentes.

Se o fizessem perderiam a sua independência. Quando o conjunto de discos independente se aproxima do respectivo limiar, é necessário adicionar mais unidades de discos ou eliminar objectos para criar mais espaço de memória.

- Quando efectua alterações restritas à configuração do disco num conjunto de discos base, tem de reiniciar o servidor no modo das Ferramentas de Serviço Dedicadas (DST). Num conjunto de discos independente offline, não é necessário ter o servidor no modo das DST para iniciar ou parar a replicação, iniciar a protecção por paridade de dispositivos, iniciar a compressão, remover uma unidade de discos, etc.

Protecção por paridade de dispositivos

A protecção por paridade de dispositivos é uma função de disponibilidade de hardware que protege contra a perda de dados devido a uma falha da unidade de discos ou a um disco danificado. Para proteger os dados, o adaptador de input/output (IOA) do disco calcula e guarda um valor de paridade para cada bit de dados. Conceitualmente, o IOA calcula o valor de paridade a partir dos dados na mesma localização em cada uma das unidades de discos incluídas no conjunto de paridade de dispositivo. Quando ocorre uma falha do disco, os dados podem ser reconstruídos utilizando o valor de paridade e os valores dos bits nas mesmas localizações nos outros discos. O sistema continua a funcionar enquanto os dados estão a ser reconstruídos. O objectivo geral da protecção por paridade de dispositivos é proporcionar uma elevada disponibilidade e proteger os dados da forma mais económica possível.

Se possível, deve proteger todas as unidades de discos no sistema por protecção por paridade de dispositivos ou protecção por replicação. Terá, assim, uma forma de evitar a perda de informações quando ocorrer uma falha num disco. Em muitos casos, também pode manter o sistema operacional durante a reparação ou substituição de uma unidade de discos.

Não se esqueça: A protecção por paridade de dispositivos **não** substitui uma estratégia de cópia de segurança e recuperação. A protecção por paridade de dispositivos pode impedir que o sistema pare quando ocorrem determinados tipos de falhas. Pode acelerar o seu processo de recuperação para certos tipos de falhas. Mas a protecção por paridade de dispositivos não o protege contra muitos tipos de falhas, como, por exemplo, acidentes nas instalações ou um erro de operador ou de programador. Não protege contra paragens do sistema causadas por falhas de outro hardware relacionado com discos (por exemplo, controladores de discos, processadores de I/O de disco ou bus do sistema).

Antes de utilizar a protecção por paridade de dispositivos, deverá estar ciente dos benefícios a ela associados, bem como dos respectivos custos e limitações.

Para obter informações adicionais sobre protecção por paridade de dispositivos, consulte estes tópicos:
- Planear a protecção por paridade de dispositivos
- Como a protecção por paridade de dispositivos afecta o rendimento
- Utilizar protecção por paridade de dispositivos e protecção por replicação

Para obter informações sobre como começar a utilizar o protecção por paridade de dispositivos na sua empresa, consulte o manual Cópia de Segurança e Recuperação. 

Planear a protecção por paridade de dispositivos

Se o seu objectivo consiste em ter um sistema com protecção contra perda de dados e reparação de manutenção simultânea, considere a utilização de uma combinação de protecção por replicação e replicação por paridade de dispositivo. Para cada conjunto de protecção por paridade de dispositivos, o espaço utilizado para informações de paridade é equivalente a uma unidade de discos. A partir dos adaptadores de input/output (IOAs) da V5R2, o número mínimo de unidades de discos num conjunto de paridade é 3; o número máximo de unidades de discos no conjunto de paridade é 18. Com os IOAs

desenvolvidos antes da V5R2, o número mínimo de unidades de discos num conjunto de paridade é 4; o número máximo de unidades de discos no conjunto de paridade é 10. Na V5R2, pode optimizar os conjuntos de paridade para capacidade, rendimento ou equilíbrio, se tiver um IOA com a V5R2 ou posterior. Para obter mais informações sobre como a protecção por paridade de dispositivos é implementada e como pode ser utilizada em conjunto com a protecção por replicação, consulte os tópicos que se seguem.

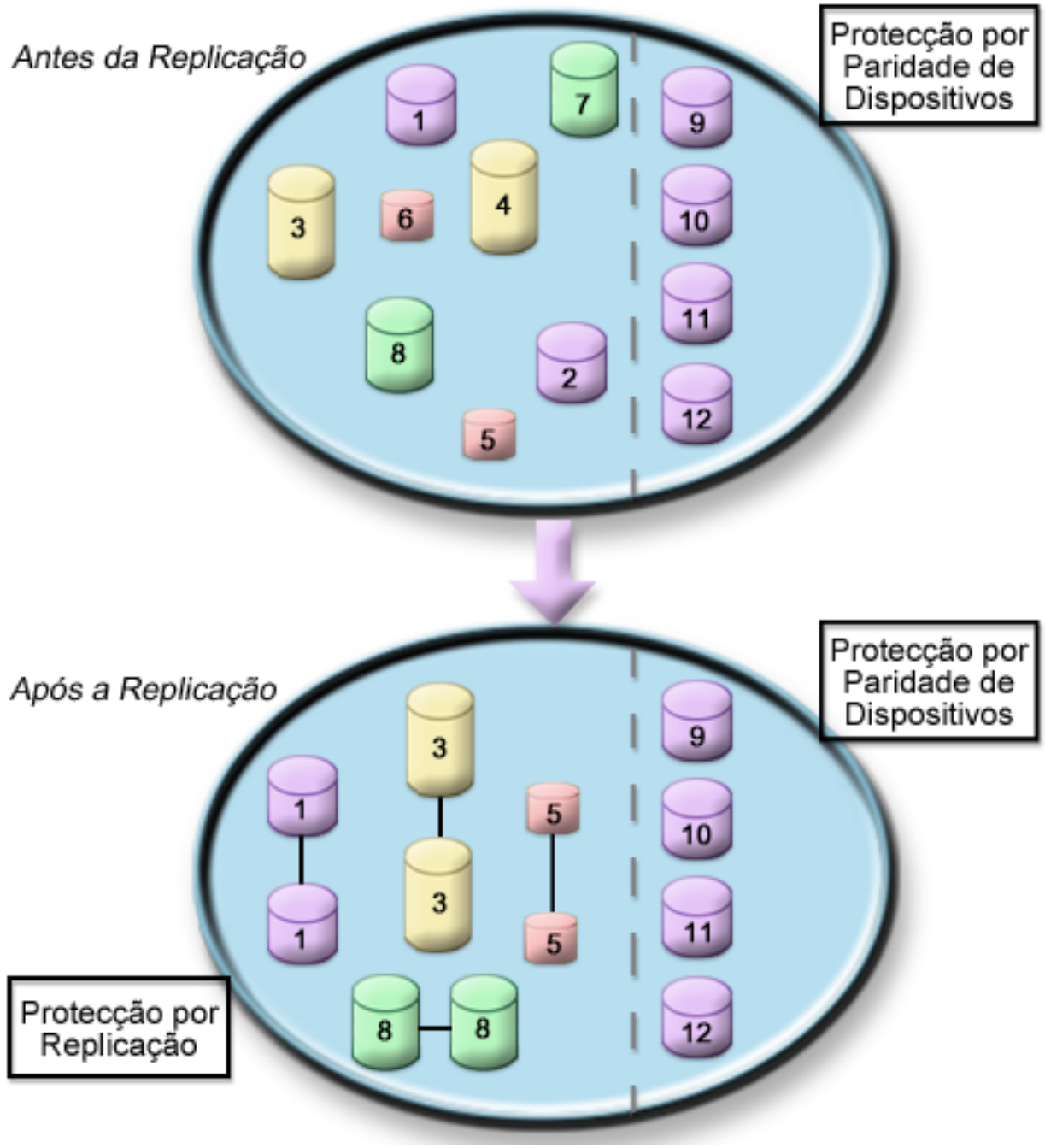
- Como funciona a protecção por paridade de dispositivos
- Exemplos da protecção por paridade de dispositivos e por replicação para conjuntos de discos

Exemplos da protecção por paridade de dispositivos e por replicação para conjuntos de discos

Protecção por replicação e protecção por paridade de dispositivos para proteger o conjunto de discos do sistema

Segue-se um exemplo de um sistema com um único conjunto de discos (conjunto de memória auxiliar)

com protecção por replicação e protecção por paridade de dispositivos.



A figura mostra um único conjunto de discos com doze unidades de discos. As unidades de discos 9–12 têm todas a mesma capacidade e estão protegidas com protecção por paridade de dispositivos. As unidades de discos 1–8 têm capacidades variáveis, mas cada unidade de discos pode ser emparelhada com outra da mesma capacidade quando a protecção por replicação for iniciada. Após o início da protecção por replicação, as unidades de discos que tiverem sido emparelhadas serão ambas identificadas pelo mesmo número; as unidades de discos 1 e 2 passam a ter o nome 1, etc. Quando falha uma das unidades de discos com protecção por paridade de dispositivos, o sistema continua a funcionar. A unidade em falha pode ser reparada simultaneamente. Se uma das unidades de discos replicadas falhar, o sistema continua em execução utilizando a unidade operacional do par replicado.

Protecção por replicação no conjunto de discos do sistema e protecção por paridade de dispositivos nos conjuntos de discos do utilizador

Considere o protecção por paridade de dispositivos se tiver a protecção por replicação no conjunto de discos do sistema e pretender criar conjuntos de discos base ou independentes. O sistema pode tolerar uma falha numa das unidades de discos de um conjunto de discos base ou independente. A falha pode ser reparada enquanto o sistema continua a funcionar.

Protecção por replicação e protecção por paridade de dispositivos em todos os conjuntos de discos
Se tiver todos os conjuntos de discos (conjuntos de memória auxiliar) protegidos com a protecção por replicação e pretender adicionar unidades aos conjuntos de discos existentes, considere também a utilização do protecção por paridade de dispositivos. O sistema pode suportar uma falha numa das unidades de discos com protecção por paridade de dispositivos. A unidade em falha pode ser reparada enquanto o sistema continua a funcionar. Se ocorrer uma falha numa unidade de discos que tenha protecção por replicação, o sistema continuará a funcionar utilizando a unidade operacional do par replicado.

Como funciona o protecção por paridade de dispositivos

Quando inicia a protecção por paridade, os IOAs criam conjuntos de paridade de dispositivos. A partir dos adaptadores de input/output (IOAs) da V5R2, o número mínimo de unidades de discos num conjunto de paridade é 3; o número máximo de unidades de discos no conjunto de paridade é 18. Com os IOAs desenvolvidos antes da V5R2, o número mínimo de unidades de discos num conjunto de paridade é 4; o número máximo de unidades de discos no conjunto de paridade é 10. Um conjunto de paridade só pode tolerar uma falha de disco. Se mais do que um disco falhar, terá de restaurar os dados a partir de suportes de cópia de segurança. Devido aos problemas de escrita, o restauro dos dados para um conjunto de discos que tenha unidades de discos com protecção por paridade de dispositivos pode ser mais demorado do que o de um conjunto de discos que contenha apenas unidades de discos não protegidas.

Em cada conjunto de paridade, o equivalente a uma unidade de disco é dedicado ao armazenamento de dados de paridade. O número de unidades de discos que contêm realmente dados de paridade varia de acordo com o número de unidades de discos no conjunto de paridade. A tabela seguinte mostra quantas unidades de discos em cada conjunto de paridade armazenam dados de paridade:

Número de unidades de discos num conjunto de paridade	Número de unidades de discos que armazenam paridade
3	2
4–7	4
8–15	8
16–18	16

O adaptador de input/output determina como são formados os conjuntos de paridade. Para os adaptadores de input/output da V5R2 e posteriores, tem a possibilidade de escolher como pretende que o conjunto de paridade seja optimizado. Pode optimizá-lo de acordo com a *capacidade*, *rendimento* ou com uma versão *equilibrada*. Se o optimizar por capacidade, o IOA tende a criar conjuntos de paridade com um número maior de unidades de discos. Aumentará o espaço utilizado para armazenar dados do utilizador, mas o rendimento pode não ser tão elevado. Se optimizar o rendimento, o IOA tenderá a criar um conjunto de paridade com menos unidades de discos. Isto deverá contribuir para operações de leitura e escrita mais rápidas, mas também pode dedicar um pouco mais de capacidade de disco para armazenar dados de paridade.

É possível incluir unidades de discos adicionais com a mesma capacidade num conjunto de paridade de dispositivos após o início da protecção por paridade de dispositivos. Pode incluir até duas unidades de discos ao mesmo tempo; no entanto, se existirem três ou mais unidades de discos que sejam elegíveis para a protecção por paridade de dispositivos, o sistema requer que inicie um novo conjunto de paridade, em vez de as incluir num conjunto de paridade existente. No iSeries Navigator, pode visualizar as propriedades de cada unidade de discos. Se o estado de protecção de uma unidade de discos for *não*

protegida, ela não está protegida pela protecção por paridade de dispositivos nem por replicação e pode ser elegível para inclusão num conjunto de paridade ou iniciada num novo conjunto de paridade. Também pode excluir os discos que não armazenem dados de paridade de um conjunto de paridade sem parar a protecção por paridade de dispositivos. Este dado também será indicado pelo número do modelo que deverá ser 050 (ou 060 se se tratar de uma unidade de disco comprimida). Pode excluir uma unidade *protegida* com um número de modelo 070 (ou 080, se se tratar de uma unidade de discos comprimida), uma vez que é uma unidade de discos que não armazena dados de paridade.

Quando um conjunto de paridade de dispositivos aumenta, pode querer considerar a redistribuição dos dados de paridade. Por exemplo, pode começar por 7 ou menos unidades de discos, mas aumentar para 8 ou mais incluindo mais unidades de discos. Quando isso acontece, pode melhorar o rendimento do conjunto de paridade de dispositivos parando a protecção por paridade e reiniciando-a. Esta acção redistribui os dados de paridade por 8 discos, em vez de 4. Em geral, a distribuição de dados de paridade por mais unidades de discos aumenta o rendimento.

Está incluída uma memória cache de escrita no adaptador de input/output (IOA) para cada conjunto de paridade, para aumentar o rendimento das cargas de trabalho de escrita interactivas. Consulte Elementos da protecção por paridade de dispositivo para ver um exemplo de um conjunto de paridade com quatro unidades de discos.

A partir da V5R2, todos os adaptadores de input-output (IOAs) suportam a protecção por paridade de dispositivos. Se tiver um adaptador de modelo anterior, verifique se suporta a protecção por paridade de dispositivos. Para obter informações sobre como actualizar para um adaptador mais recente, consulte Migrar para um novo adaptador de input/output.

Nota: Se possível, inicie o protecção por paridade de dispositivos antes de adicionar unidades de discos a um conjunto de discos. Esta acção reduz significativamente o tempo de configuração das unidades de discos.

Elementos do protecção por paridade de dispositivos: O diagrama que se segue ilustra os elementos de um conjunto de paridade que contém quatro unidades de discos. Cada conjunto de paridade começa por um Processador de Input/Output (IOP) que está associado a um Adaptador de Input/Output (IOA), que contém a memória cache de escrita. O IOA transmite sinais de leitura e escrita às unidades de discos associadas. A primeira figura mostra como a paridade é distribuída com adaptadores anteriores à V5R2. A segunda figura mostra como a paridade é distribuída com os adaptadores da V5R2 e posteriores.

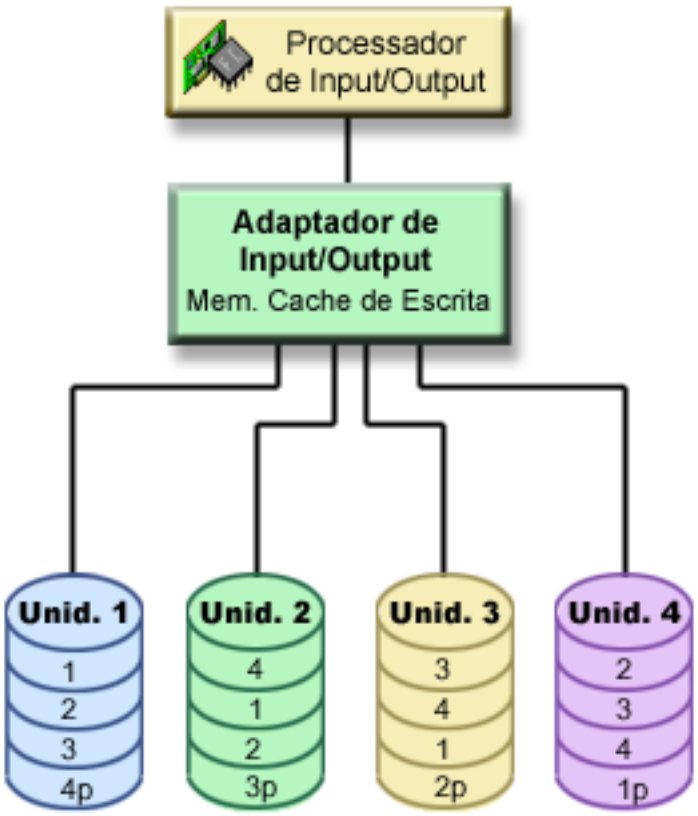


Figura 1. Exemplo da distribuição dos dados de paridade com IOAs anteriores à V5R2

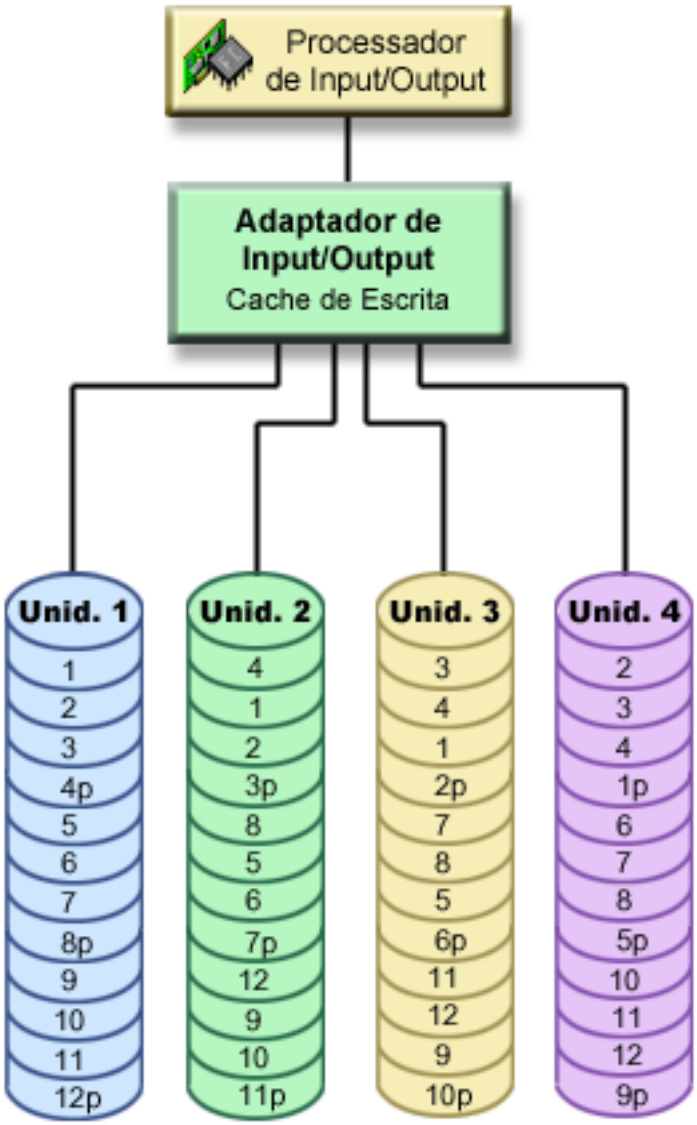


Figura 2. Exemplo da distribuição dos dados de paridade com IOAs da V5R2 e posteriores

Nos exemplos anteriores, *p* indica as secções do disco que contêm dados de paridade. A primeira figura mostra um exemplo de um IOA anterior à V5R2, em que os dados de paridade são distribuídos numa grande porção em cada unidade de discos que armazena dados de paridade. A segunda figura mostra como os IOAs da V5R2 e posteriores distribuem os dados de paridade pelas unidades de discos num pequeno número de grandes porções. O rendimento é melhorado através da distribuição dos dados de paridade por cada uma das unidades de discos.

A memória cache de escrita fornece uma maior integridade dos dados e um aumento do rendimento. Quando o servidor iSeries™ envia uma operação de escrita, os dados são escritos na memória cache. Em seguida, é enviada uma mensagem de conclusão de escrita de volta ao servidor. Mais tarde, os dados serão escritos no disco. A memória cache fornece uma capacidade de escrita mais rápida e assegura a integridade dos dados.

Para uma abordagem mais aprofundada, reveja as informações adicionais acerca damemória cache de escrita acima ilustrada.

Memória cache de escrita: As seguintes acções ocorrem durante um pedido de escrita proveniente do servidor:

1. Os dados são consolidados numa memória cache não volátil suportada por pilha no IOA.
2. É enviada uma mensagem de conclusão de escrita pelo servidor.

As acções que se seguem ocorrem após o envio da mensagem de conclusão de escrita.

1. É enviada uma operação de escrita pela memória cache do IOA para a unidade de discos
   - Relativamente a dados:
     - Lê os dados originais.
     - Calcula a paridade delta por comparação dos dados novos com os originais.
     - Escreve os novos dados.
   - Relativamente a dados de paridade:
     - Lê as informações de paridade originais.
     - Calcula a nova paridade por comparação da paridade delta com a paridade original.
     - Escreve as novas informações de paridade.
2. Os dados são marcados como consolidados quando forem escritos com êxito na unidade de discos de dados e na unidade de discos de paridade.

O rendimento deste tipo de operação de escrita depende da contenção do disco e do tempo que é necessário para calcular as informações de paridade.

Migrar para um novo adaptador de input/output

Antes de iniciar a migração para o novo adaptador de input/output (IOA), tal como acontece com qualquer outra alteração à configuração, é importante encerrar normalmente o sistema. Esta acção assegurará que todos os dados são guardados a partir da memória cache. Quando migrar um conjunto de paridade existente de um IOA anterior à V5R2 para um IOA da V5R2 ou posterior, as suas unidades de discos não serão protegidas pela protecção por paridade de dispositivos, durante a regeneração da paridade.

Nota:
Não poderá migrar o conjunto de paridade de novo para a geração antiga de adaptadores depois de ter mudado para o novo adaptador. Se tiver de voltar atrás, terá de parar a protecção por paridade de dispositivos, associar as unidades ao adaptador antigo e reiniciar a protecção por paridade de dispositivos.

Protecção por paridade de dispositivos—benefícios

Seguem-se os benefícios da protecção por paridade de dispositivos:

- Os dados perdidos são automaticamente reconstruídos pelo controlador de discos após uma falha do disco.
- O sistema continua em execução após a falha de um único disco.
- Pode substituir uma unidade de discos com problemas sem parar o sistema.
- A protecção por paridade de dispositivos reduz o número de objectos danificados quando um disco falha.
- Apenas 1 unidade de discos de capacidade armazena dados de paridade num conjunto de paridade.

Protecção por paridade de dispositivos—custos e limitações

A protecção por paridade de dispositivos tem custos e limitações:

- A protecção por paridade de dispositivos pode requerer unidades de discos adicionais para evitar um rendimento mais lento.
- As operações de restauro podem ser mais morosas, caso utilize protecção por paridade de dispositivos.

Como a protecção por paridade de dispositivos afecta o rendimento

A protecção por paridade de dispositivos requer operações de I/O adicionais para guardar os dados de paridade. Para evitar problemas de rendimento, todos os IOAs contêm uma memória cache de escrita não volátil que assegura a integridade dos dados e fornece uma capacidade de escrita mais rápida. O sistema é notificado sobre a conclusão de uma operação de escrita assim que for guardada uma cópia dos dados na memória cache de escrita. Os dados são reunidos na memória cache antes de serem escritos numa unidade de discos. Esta técnica de recolha reduz o número de operações de escrita físicas na unidade de discos. Devido à memória cache, o rendimento é normalmente semelhante nas unidades de discos protegidas e desprotegidas.

As aplicações que têm muitos pedidos de escrita num breve período de tempo como, por exemplo, programas batch, podem afectar negativamente o rendimento. A falha de uma única unidade de discos pode afectar o rendimento das operações de leitura e de escrita.

O processamento adicional associado a uma falha da unidade de discos num conjunto de paridade de dispositivos pode ser significativo. A diminuição do rendimento verificar-se-á até que a unidade em falha seja reparada (ou substituída) e o processo de reconstrução esteja concluído. Se a protecção por paridade de dispositivos diminuir demasiado o rendimento, considere utilizar a protecção por replicação. Estes tópicos fornecem detalhes adicionais sobre o modo como a falha de uma unidade de discos afecta o rendimento:

- Falha da unidade de discos numa configuração de protecção por paridade de dispositivos
- Operações de leitura numa unidade de discos em falha
- Operações de escrita numa unidade de discos em falha
- Operações de input-output durante um processo de reconstrução

Falha da unidade de discos numa configuração de protecção por paridade de dispositivos

Se uma unidade de discos falhar, os subsistemas com protecção por paridade de dispositivos são considerados como estando expostos até o processo de sincronização ser concluído, após a substituição da unidade de discos em falha. Durante o tempo em que a unidade de discos é considerada como exposta, são necessárias operações de I/O adicionais. Se uma segunda unidade de discos falhar, terá de restaurar os dados a partir de suportes de cópia de segurança.

Operações de leitura numa unidade de discos em falha

Para obter os dados contidos numa unidade de discos em falha, a protecção por paridade de dispositivos terá de ler cada unidade de discos do conjunto de paridade de dispositivos que contém a unidade de discos em falha. Uma vez que as operações de leitura se podem sobrepor, o impacto sobre o rendimento poderá ser diminuto.

Uma vez que uma unidade de discos com protecção por paridade de dispositivos em falha pode conter apenas uma pequena parte de dados do utilizador, é possível que apenas alguns utilizadores sejam afectados pela diminuição do rendimento.

Operações de escrita numa unidade de discos em falha

Existem alguns exemplos disponíveis que mostram o que acontece às operações de escrita quando uma única unidade de discos falha num conjunto de paridade de dispositivos com protecção por paridade de dispositivos. A figura a seguir mostra uma unidade em falha sob um IOA com o protecção por paridade de dispositivos. Utilize a figura para os seguintes exemplos:

- Exemplo: Escrever numa unidade de discos em falha
- Exemplo: Escrever dados numa unidade de discos quando os dados de paridade correspondentes estão numa unidade de discos em falha

Figura 3. Conjunto de paridade de dispositivos com unidade de discos em falha

A figura mostra um conjunto de paridade com quatro unidades de discos. Cada secção da unidade de discos está marcada com um número. Os sectores de paridade estão assinalados com um *p*. A unidade de discos 3 falhou. A unidade de discos 1 mostra os sectores 1, 2, 3 e 4p. A unidade de discos 2 mostra os sectores 4, 1, 2 e 3p. A unidade de discos em falha 3 mostra os sectores 3, 4, 1 e 2p. A unidade de discos 4 mostra os sectores 2, 3, 4 e 1p.

Exemplo: Escrever numa unidade de discos em falha: Uma operação de escrita do servidor iSeries detecta que a unidade de discos que deverá conter os dados falhou. A operação de escrita deverá ser na unidade de discos 3, sector 1. Ocorrem as seguintes acções:

1. Os dados originais perdem-se na unidade de discos 3, sector 1, devido à falha.
2. Os novos dados de paridade são calculados através da leitura da unidade de discos 1, sector 1; e da unidade de discos 2, sector 1.
3. São calculadas novas informações de paridade.
4. Não podem ser escritos novos dados no sector 1 da unidade de discos 3, devido à falha.
5. São escritas novas informações de paridade no sector de paridade 1 da unidade de discos 4.

   As operações de escrita requerem várias leituras (leituras N-2, em que N é o número de unidades de discos) e apenas uma operação de escrita para as novas informações de paridade. Os dados da unidade de discos 3 serão reconstruídos durante a sincronização, após a substituição da unidade de discos 3.

Exemplo: Escrever dados numa unidade de discos quando os dados de paridade correspondentes estão numa unidade de disco em falha: O pedido de escrita do servidor iSeries detecta uma falha do disco na unidade de disco que contém os dados de partição correspondentes. O pedido de escrita deverá ser para o sector 2 da unidade de discos 4. As informações de paridade para a unidade de discos 4, sector 2, encontram-se na unidade de discos em falha 3. Ocorrem as seguintes acções:

1. É detectada uma falha na unidade de discos que contém os dados de paridade, unidade de discos 3.
2. O cálculo das informações de paridade não é necessário porque não é possível escrever no sector de paridade 2 da unidade de discos 3. Deste modo, não existe requisito para ler os dados originais e as informações de paridade.
3. Os dados são escritos na unidade de discos 4, sector 2.

   Uma operação de escrita requer apenas uma escrita para os novos dados. Os dados de paridade para o sector de paridade 2 da unidade de discos 3 serão reconstruídos durante a sincronização após a substituição da unidade de discos 3.

Operações de input-output durante um processo de reconstrução

As operações de I/O durante o processo de reconstrução (sincronização) da unidade de discos em falha poderão não requerer pedidos de I/O de disco adicionais. Isso depende a partir de onde os dados são lidos ou onde são escritos na unidade de discos que se encontra em processo de sincronização. Por exemplo:

- Uma operação de leitura da área de disco que já foi reconstruída requer uma operação de leitura.
- Uma operação de leitura da área de disco que ainda não foi reconstruída é considerada como uma operação de leitura numa unidade de discos em falha. Consulte ″Operações de leitura numa unidade de discos em falha″ para mais informações.
- Uma operação de escrita no disco que já tenha sido reconstruído requer operações de leitura e de escrita normais (duas operações de leitura e duas operações de escrita).
- Uma operação de escrita na área de disco que ainda não tenha sido reconstruída será considerada como uma operação de escrita para uma unidade de discos em falha. Consulte ″Operações de escrita numa unidade de discos em falha″ para mais informações.

Nota: O processo de reconstrução demora mais tempo quando também estiverem a decorrer operações de leitura e de escrita numa unidade de discos substituída. Todos os pedidos de leitura ou de escrita interrompem o processo de reconstrução para executar as operações de I/O necessárias.

Utilizar protecção por paridade de dispositivos e protecção por replicação

A protecção por paridade de dispositivos é uma função de hardware. Conjuntos de discos e protecção por replicação são funções de software. Quando adiciona unidades de discos e inicia a protecção por paridade de dispositivos, o subsistema do disco ou o IOP não reconhece a configuração de software das unidades de discos. O software que suporta a protecção de discos sabe quais as unidades que têm protecção por paridade de dispositivos.

Estas regras e considerações aplicam-se ao combinar protecção por paridade de dispositivos e protecção por replicação:

- O Protecção por paridade de dispositivos não está implementado em limites de conjuntos de discos.
- A protecção por replicação está implementada em limites de conjuntos de discos.
- Pode iniciar a protecção por replicação para um conjunto de discos mesmo que este não contenha actualmente unidades disponíveis para replicação porque todas têm oprotecção por paridade de dispositivos. Isto assegura que o conjunto de discos estará sempre totalmente protegido, mesmo que adicione posteriormente discos sem protecção por paridade de dispositivos.
- Quando uma unidade de discos é adicionada à configuração do sistema, pode ou não ter protecção por paridade de dispositivos.
- Para um sistema totalmente protegido, deverá proteger por inteiro cada unidade de discos, quer através de protecção por paridade de dispositivos, quer protecção por replicação, quer ambas.
- As unidades de discos protegidas por protecção por paridade de dispositivos podem ser adicionadas a um conjunto de discos que tenha protecção por replicação. As unidades de discos protegidas por protecção por paridade de dispositivos não participam na protecção por replicação. O hardware já as protege.
- Quando adiciona uma unidade de discos que não esteja protegida por protecção por paridade de dispositivos a um conjunto de discos com protecção por replicação, a nova unidade de discos participa em protecção por replicação. As unidades de discos têm de ser adicionadas e removidas de um conjunto de discos replicado em pares com capacidades iguais.
- Antes de iniciar o protecção por paridade de dispositivos para unidades de discos que estejam configuradas (atribuídas a um conjunto de discos), terá de parar a protecção por replicação para o conjunto de discos.
- Antes de parar a protecção por paridade de dispositivos, terá de parar a protecção por replicação para quaisquer conjuntos de discos que contenham unidades de discos afectadas.

- Quando parar a protecção por replicação, uma unidade de discos de cada par replicado deixa de estar configurada. Terá de adicionar de novo as unidades não configuradas ao conjunto de discos antes de iniciar a protecção por replicação.

Protecção por replicação

A protecção por replicação é uma função de disponibilidade de software que protege contra a perda de dados devido a uma falha ou a um dano num componente relacionado com discos. Os dados estão protegidos porque o sistema mantém duas cópias dos dados em duas unidades de discos separadas. Quando falha um componente relacionado com discos, o sistema pode continuar a funcionar sem interrupção, utilizando a cópia replicada dos dados até que o componente seja reparado.

Quando inicia a protecção por replicação ou adiciona unidades de discos a um conjunto de discos com aprotecção por replicação, o sistema cria pares replicados utilizando unidades de discos que tenham capacidades idênticas. O objectivo geral é proteger o número máximo possível de componentes relacionados com discos. Para fornecer a máxima redundância e protecção do hardware, o sistema tenta emparelhar unidades de discos que estejam ligadas a diferentes controladores, adaptadores de input/output, processadores de input/output, buses e torres.

Se ocorrer uma falha do disco, a protecção por replicação destina-se a impedir que se percam dados. A protecção por replicação é uma função de software que utiliza duplicados de componentes de hardware relacionados com discos para manter o sistema disponível caso um dos componentes falhe. Pode ser utilizada em qualquer modelo de servidores iSeries e faz parte do Código Interno Licenciado.

São possíveis diferentes níveis de protecção por replicação, consoante o hardware que é duplicado. Pode duplicar:
- Unidades de discos
- Adaptadores de input/output
- Processadores de input/output
- Buses
- Torres
- Ligações de alta velocidade

O sistema fica disponível durante a falha se um componente em falha e os componentes de hardware a ele ligados estiverem duplicados. Para obter mais detalhes técnicos sobre a memória do servidor e a protecção por replicação, consulte a secção Como o sistema endereça a memória e Protecção por replicação—como funciona.

O suporte de replicação remota permite-lhe ter uma unidade replicada num par replicado numa localização local e a segunda unidade replicada numa localização remota. Para alguns sistemas, a replicação de DASD standard continuará a ser a melhor opção; para outros, a replicação de DASD remota possibilita capacidades adicionais importantes. Tem de avaliar as utilizações e necessidades do seu sistema, ter em consideração as vantagens e desvantagens de cada tipo de suporte de replicação e decidir o que é melhor para o seu caso.

Para mais informações sobre protecção por replicação, consulte os seguintes tópicos:
- Protecção por replicação—benefícios
- Protecção por replicação—custos e limitações
- Planear a protecção por replicação
- Replicação de DASD remota

Para obter informações sobre como implementar a protecção por replicação na sua empresa, consulte o manual Cópia de Segurança e Recuperação. 

Protecção por replicação—benefícios

Com a melhor configuração de protecção por replicação possível, o sistema continua a funcionar após uma única falha de hardware relacionada com discos. Em algumas unidades do sistema, o hardware que falhou pode, por vezes, ser reparado ou substituído sem ser necessário desligar o sistema. Se não for possível reparar o componente em falha com o sistema a funcionar (por exemplo, no caso de um bus ou processador de I/O), normalmente o sistema continua a funcionar após a falha. A manutenção pode ser diferida, o sistema pode ser encerrado normalmente e pode ser evitado um longo período de recuperação.

Mesmo que o sistema não seja grande, a protecção por replicação pode constituir uma valiosa protecção. Uma falha do disco ou de hardware relacionado com discos que ocorra num sistema desprotegido deixa o seu sistema inutilizável durante horas. O tempo efectivo depende do tipo de falha, da quantidade de memória em disco, da sua estratégia de cópia de segurança, da velocidade da unidade de bandas e do tipo e quantidade de processamento que o sistema executa. Se o utilizador ou a empresa não puder suportar esta perda de disponibilidade, deve pensar em utilizar a protecção por replicação no sistema, independentemente do tamanho do sistema.

Protecção por replicação—custos e limitações

O custo principal da utilização da protecção por replicação está associado ao hardware adicional. Para obter uma maior disponibilidade e impedir a perda de dados quando uma unidade de discos falha, é necessária a protecção por replicação para todos os conjuntos de discos. Este procedimento necessita, normalmente, do dobro das unidades de discos. Se pretende um funcionamento contínuo e uma prevenção de perda de dados quando falha uma unidade de discos, um controlador ou um processador de I/O, precisa de controladores de discos e de processadores de I/O em duplicado. Pode ser feita uma actualização de modelo para obter um funcionamento quase contínuo e para impedir a perda de dados quando ocorrer alguma destas falhas, bem como a falha de um bus. Se o bus 1 falhar, o sistema não pode continuar a funcionar. Uma vez que as falhas de bus são raras e como a protecção de nível de bus não é significativamente maior do que a protecção de nível de processador de I/O, poderá chegar à conclusão de que uma actualização de modelo não é rentável em termos de custos relativamente às suas necessidades de protecção.

A protecção por replicação tem um efeito mínimo no rendimento. Se os buses, processadores de I/O e controladores não estiverem mais carregados num sistema com protecção por replicação do que estão num sistema equivalente sem protecção por replicação, o rendimento dos dois sistemas deverá ser aproximadamente o mesmo.

Ao decidir se deve ou não utilizar a protecção por replicação no sistema, terá de comparar o custo do tempo de inactividade potencial com o custo de hardware adicional, durante o período de vida do sistema. O custo adicional do rendimento ou da complexidade do sistema é, normalmente, irrisório. Também deve pensar noutras alternativas de disponibilidade e recuperação, como, por exemplo, a protecção por paridade de dispositivos. A protecção por replicação necessita, normalmente, do dobro das unidades de memória. Para manutenção simultânea e maior disponibilidade em sistemas com protecção por replicação, pode ser necessário outro hardware relacionado com discos.

Limitações

Ainda que a protecção por replicação possa manter o sistema disponível após falhas de hardware relacionadas com discos, não substitui os procedimentos de salvaguarda. Podem existir múltiplos tipos de falhas de hardware relacionadas com discos ou desastres (como, por exemplo, inundações ou sabotagens) que requerem um suporte de segurança.

A protecção por replicação não consegue manter o sistema disponível se a unidade de memória restante do par replicado falhar antes de a primeira unidade de memória a falhar ser reparada e de a protecção por replicação ser retomada. Se as duas unidades de memória que falharam estiverem em pares replicados diferentes, o sistema estará, ainda assim, disponível e será feita a recuperação de protecção

por replicação normal, uma vez que os pares replicados não dependem uns dos outros para efeitos de recuperação. Se falhar uma segunda unidade de memória do mesmo par replicado, a falha poderá não resultar numa perda de dados. Se a falha se limitar à tecnologia electrónica do disco ou se o técnico dos serviços de assistência conseguir utilizar com êxito a função Guardar Dados da Unidade de Discos para recuperar todos os dados, não serão perdidos dados.

Se ambas as unidades de memória de um par replicado falharem, causando perda de dados, perder-se-á todo o conjunto de discos e todas as unidades nele contidas serão limpas. É necessário preparar-se para restaurar o conjunto de discos a partir do suporte de cópia de segurança e aplicar quaisquer alterações de diário.

Ao iniciar a operação de protecção por replicação, os objectos criados numa unidade preferencial podem ser movidos para outra unidade. A unidade preferencial poderá já não existir após o início da protecção por replicação.

Planear a protecção por replicação

Se possui um sistema com múltiplos buses ou um sistema grande com um só bus, deve considerar utilizar a protecção por replicação. Quanto maior for o número de unidades de discos ligadas a um sistema, mais frequentes serão as falhas de hardware relacionadas com discos, simplesmente porque há mais componentes individuais de hardware que podem falhar. Por isso, aumenta a possibilidade de perda de dados ou de perda de disponibilidade como resultado de uma falha de disco ou de outro hardware. Por outro lado, à medida que aumenta a quantidade de memória em disco do sistema, o tempo de recuperação após uma falha de memória em disco do hardware de subsistema aumenta significativamente. O tempo de inactividade torna-se mais frequente, mais longo e mais dispendioso.

Quando considerar a protecção por replicação, contacte o seu representante de marketing IBM para o orientar nestes passos de planeamento:

1. Decidir quais os conjuntos de discos a proteger.
2. Determinar os requisitos de capacidade de memória em disco.
3. Determinar o nível de protecção que pretende para cada conjunto de discos replicado.
4. Determinar o hardware extra necessário para a protecção por replicação.
5. Determinar o hardware extra necessário para o rendimento.
6. Encomendar o novo hardware.
7. Planear a instalação do sistema e a configuração das novas unidades.
8. Instalar o novo hardware.

Para mais informações sobre protecção por replicação, consulte os seguintes tópicos:

- Protecção por replicação—benefícios
- Protecção por replicação—custos e limitações
- Protecção por replicação—funcionamento

Protecção por replicação—funcionamento

Uma vez que a protecção por replicação está configurada por conjunto de discos, pode replicar um, alguns ou todos os conjuntos de discos do sistema. Por valor assumido, todos os sistemas têm um conjunto de discos de sistema. Não é necessário criar conjuntos de discos do utilizador para poder utilizar a protecção por replicação. Embora a protecção por replicação seja configurada por conjunto de discos, todos os conjuntos de discos têm de ser replicados de modo a fornecer a máxima disponibilidade do sistema. Se uma unidade de discos falhar num conjunto de discos não replicado, o sistema não poderá ser utilizado enquanto a unidade de discos não for reparada ou substituída.

O algoritmo do par replicado inicial selecciona automaticamente uma configuração replicada que fornece a máxima protecção ao nível do bus, do processador de I/O (input/output) ou do controlador da configuração de hardware do sistema. Quando as unidades de memória de um par replicado se encontram em buses separados, têm a máxima independência ou protecção. Uma vez que não partilham nenhum recurso ao nível do bus, do processador de I/O ou do controlador, uma falha num destes componentes de hardware permite à outra unidade replicada continuar a funcionar.

Todos os dados escritos numa unidade replicada serão escritos em ambas as unidades de memória do par replicado. Quando forem lidos dados de uma unidade replicada, a operação de leitura pode ser feita a partir de qualquer uma das unidades de memória do par replicado. O utilizador não sabe a partir de que unidade replicada os dados estão a ser lidos. Um utilizador não se apercebe da existência de duas cópias físicas dos dados.

Se uma unidade de memória de um par replicado falhar, o sistema *suspende* a protecção por replicação da unidade replicada que falhou. O sistema continua a funcionar utilizando a unidade replicada restante. A unidade replicada que falhou pode ser reparada ou substituída fisicamente.

Depois da reparação ou substituição da unidade replicada que falhou, o sistema *sincroniza* o par replicado copiando as dados actuais da unidade de memória que ficou operacional para a outra unidade de memória. Durante a sincronização, a unidade replicada para a qual as informações estão a ser copiadas encontra-se no estado *a retomar*. A sincronização não necessita de um sistema dedicado e decorre em simultâneo com outros trabalhos do sistema. O rendimento do sistema é afectado durante a sincronização. Quando a sincronização termina, a unidade replicada fica *activa*.

Para obter informações sobre a memória do servidor, consulte Como o servidor endereça a memória.

Como o servidor endereça a memória: As unidades de discos são atribuídas a um conjunto de discos por unidade de memória. O sistema trata cada unidade de memória de uma unidade de discos como uma unidade distinta de memória auxiliar. Quando é ligada uma nova unidade de discos ao sistema, este começa por tratar cada unidade de memória como não configurada. Através das opções das Ferramentas de Serviço Dedicadas (DST), pode adicionar estas unidades de memória não configuradas ao conjunto de discos do sistema ou a um conjunto de discos independente à sua escolha. Ao adicionar unidades de memória não configuradas, utilize as informações do número de série atribuído pelo fabricante para garantir que está a seleccionar a unidade de memória física correcta. Para além disso, as unidades de memória individuais da unidade de discos podem ser identificadas através das informações de Endereço que podem ser obtidas a partir do ecrã das DST Ver Configuração do Disco.

Quando adiciona uma unidade de memória não configurada a um conjunto de discos, o sistema atribui um número de unidade à unidade de memória. O número da unidade pode ser utilizado em vez do número de série e do endereço. É utilizado o mesmo número de unidade para uma unidade específica de memória, mesmo que ligue a unidade de discos ao sistema de um modo diferente.

Quando uma unidade tem protecção por replicação, é atribuído o mesmo número de unidade às duas unidades de memória do par replicado. O número de série e o endereço distinguem as duas unidades de memória de um par replicado.

Para determinar que unidade de discos física está a ser identificada com cada número de unidade, tome nota da atribuição de número de unidade para garantir uma identificação correcta. Se estiver disponível uma impressora, imprima o ecrã das DST ou SST da sua configuração de disco. Se necessitar de verificar a atribuição de números de unidade, utilize o ecrã das DST ou SST Ver Estado da Configuração para ver os números de série e os endereços de cada unidade.

A unidade de memória endereçada pelo sistema como unidade 1 é sempre utilizada pelo sistema para guardar o código interno licenciado e áreas de dados. A quantidade de memória utilizada na unidade 1 é muito grande e varia de acordo com a configuração do sistema. A unidade 1 contém uma quantidade limitada de dados de utilizador. Uma vez que a unidade 1 contém os programas e dados iniciais utilizados durante um IPL do sistema, também é conhecida como a **unidade de origem do carregamento**.

O sistema reserva uma quantidade fixa de memória em todas as unidades, com excepção da unidade 1. O tamanho desta área reservada é de 1,08MB por unidade, reduzindo essa quantidade no espaço disponível em cada unidade.

Replicação remota: O suporte de replicação remota torna possível dividir as unidades de discos do seu sistema num grupo de DASD locais e um grupo de DASD remotos. Os DASD remotos estão ligados a um conjunto de buses ópticos e os DASD locais a outro conjunto de buses. Os DASD locais e remotos podem estar fisicamente separados uns dos outros em locais diferentes, expandindo os buses ópticos adequados ao local remoto, fornecendo desta forma uma grau de protecção mais elevado na eventualidade de um acidente nas instalações.

Manutenção simultânea: A manutenção simultânea é o processo de reparação ou substituição de um componente de hardware relacionado com discos durante a utilização do sistema em operações normais.

Em sistemas sem protecção por replicação ou protecção por paridade de dispositivo, o sistema não estará disponível quando ocorrer uma falha de hardware relacionada com discos e permanecerá indisponível até que o hardware que falhou seja reparado ou substituído. No entanto, com a protecção por replicação, o hardware que falhou pode ser, na maior parte dos casos, reparado ou substituído enquanto o sistema está a ser utilizado.

O suporte de manutenção simultânea é uma função do pacote de hardware da unidade de sistema. O pacote de sistema de entrada (9402) não suporta a manutenção simultânea. A protecção por replicação só possibilita a manutenção simultânea quando o hardware e o conjunto de programas do sistema a suportarem. A melhor configuração de hardware para a protecção por replicação também possibilita o grau máxima de manutenção simultânea.

O sistema pode funcionar com êxito durante muitas falhas e acções de reparação. Por exemplo, uma falha de um conjunto de cabeças/discos não fará com que o sistema pare de funcionar. Pode ocorrer uma substituição do conjunto de cabeças e a sincronização da unidade replicada enquanto o sistema continua a funcionar. Quanto maior for o seu nível de protecção, mais frequentemente poderá ser feita a manutenção simultânea.

Em alguns modelos, o sistema restringe o nível de protecção para a unidade 1 e para a respectiva unidade replicada apenas à protecção de nível de controlador. Consulte ″Protecção por Replicação - Regras de Configuração″ no manual Cópia de Segurança e Recuperação.  para obter mais informações.

Em certas condições, o diagnóstico e a reparação podem requerer a suspensão das unidades replicadas activas. Pode preferir desligar o sistema para minimizar o risco que representa funcionar com menos protecção por replicação. Algumas acções de reparação requerem que o sistema seja desligado. A ***manutenção diferida*** é o processo de espera para reparação ou substituição de um componente de hardware relacionado com discos em falha até o sistema poder ser desligado. O sistema está disponível, ainda que a protecção por replicação seja reduzida pelos componentes de hardware que falharam. A manutenção diferida só é possível com a protecção por replicação ou com a protecção por paridade de dispositivos.

Par replicado: Duas unidades de memória que contêm os mesmos dados e são referenciadas pelo sistema como uma unidade. Uma ***unidade replicada*** é uma unidade de memória que constitui metade de um par replicado.

Unidade de discos: As unidades de discos são os dispositivos que, na prática, contêm as unidades de memória. O hardware é encomendado ao nível de unidade de discos. Cada unidade de discos tem um número de série único.

Uma ***unidade de memória*** é o espaço definido numa unidade de discos que é endereçado pelo sistema.

Uma ***unidade*** é a divisão definida da memória de nível único. Este espaço é a localização de disco mais pequena endereçável pelo utilizador. Um conjunto de discos é uma ou mais unidades que são

identificadas por números de unidade exclusivos. Uma unidade num conjunto de discos não replicado é uma unidade de memória. Uma unidade num conjunto de discos replicado é um par replicado, que corresponde a duas unidades de memória.

Alguns comandos de criação (CRTPF, CRTJRNRCV, etc.) podem criar um objecto numa unidade especificada. No ambiente não replicado, será uma unidade de memória única. Num ambiente replicado, o valor de parâmetro UNIT significa um par replicado.

Para obter informações sobre a memória no servidor, consulte a secção Como o sistema endereça a memória.

Torre: Um suporte que contém unidades de memória e é endereçável em separado pelo sistema.

Bus: O bus é o canal principal de comunicações para transferência de dados de input e output. Um sistema pode ter um ou mais buses.

Processador de I/O: O processador de input/output (IOP) está ligado ao bus. O IOP é utilizado para transferir informações entre a memória principal e grupos específicos de controladores. Alguns IOPs são dedicados a tipos de controladores específicos, como, por exemplo, controladores de discos. Outros IOPs podem ter mais de um tipo de controlador ligado, por exemplo, controladores de bandas e controladores de discos.

Adaptador de I/O: O adaptador de input/output (IOA) está ligado ao processador de input/output (IOP). O adaptador de input/output transfere informações entre o IOP e as unidades de discos.

Controlador: O controlador de discos é ligado ao IOP e gere a transferência de informações entre o IOP e as unidades de discos. Algumas unidades de discos têm controladores incorporados. Outras têm controladores separados.

Decidir quais os conjuntos de discos a proteger

A Protecção por replicação é configurada pelo conjunto de discos porque se trata do nível de controlo do utilizador sobre a memória de nível único. A Protecção por replicação pode ser utilizada para proteger um, alguns ou todos os conjuntos de discos num sistema. No entanto, não são necessários vários conjuntos de discos para utilizar a protecção por replicação. A Protecção por replicação funciona bem se todas as unidades de discos de um sistema estiverem configuradas num único conjunto de discos (o valor assumido no servidor iSeries). De facto, a replicação reduz a necessidade de definir partições na memória auxiliar em conjuntos de discos para fins de protecção e recuperação de dados. No entanto, talvez ainda seja aconselhável ter conjuntos de discos por motivos de rendimento e outros.

Para obter a melhor protecção e disponibilidade para todo o sistema, todos os conjuntos de discos do sistema deverão ter a protecção por replicação:

- Se o sistema tiver uma combinação de alguns conjuntos de discos com, e outros sem a protecção por replicação, uma falha na unidade de discos de um conjunto de discos sem a protecção por replicação compromete seriamente o funcionamento de todo o sistema. Podem perder-se dados no conjunto de discos onde ocorreu a falha. Poderá ser necessário um longo período de recuperação.
- Se um disco de um conjunto de discos replicado falhar e o sistema também contiver conjuntos de discos que não estejam replicados, não se perdem dados. No entanto, em certos casos, a manutenção simultânea pode não ser possível.

As unidades de discos que são utilizadas em conjuntos de discos deverão ser cuidadosamente seleccionadas. Para se obter a melhor protecção e rendimento, um conjunto de discos deverá conter unidades de discos que estejam ligadas a vários processadores de I/O diferentes. O número de unidades de discos no conjunto de discos que estão ligadas a cada processador de I/O deve ser o mesmo (ou seja, equilibrado).

Determinar os requisitos de capacidade de memória em disco

Um conjunto de discos replicado requer o dobro da memória que um conjunto de discos que não esteja replicado, uma vez que o sistema mantém duas cópias de todos os dados no conjunto de discos. Além disso, a protecção por replicação requer um número par de unidades de discos com a mesma capacidade, de modo a que as unidades de discos possam ser organizadas em pares replicados. Num sistema existente, deve dizer-se que não é necessário adicionar os mesmos tipos de unidades de discos já ligadas para fornecer a capacidade de memória adicional necessária. Podem ser adicionadas quaisquer novas unidades de discos, desde que exista uma capacidade de memória total suficiente e um número par de unidades de memória de cada tamanho. O sistema atribuirá pares replicados e moverá automaticamente os dados conforme for necessário. Se um conjunto de discos não contiver capacidade de memória suficiente, ou se não for possível emparelhar as unidades de memória, a protecção por replicação não poderá ser iniciada nesse conjunto de discos.

O processo de determinação das unidades de discos necessárias para a protecção por replicação é semelhante para os sistemas novos e para os já existentes. O utilizador, em conjunto com o representante de marketing da IBM, deverá executar o seguinte procedimento:

1. Planear quantos dados poderá conter cada conjunto de discos.
2. Planear uma percentagem destino da memória utilizada para o conjunto de discos(o grau de preenchimento do conjunto de discos).
3. Planear o número e tipo de unidades de discos necessárias para conseguir a memória necessária. Para um conjunto de discos existente, pode planear um tipo e modelo diferentes de unidade de discos para fornecer a memória necessária. Tem de garantir que existe um número par de cada tipo e modelo de unidade de discos.

Após concluir o planeamento para todos os conjuntos de discos, efectue o planeamento para unidades de reserva, se desejar.

Uma vez na posse de todas as informações, pode calcular as suas necessidades totais de memória.

Planear a capacidade de memória: Para um novo sistema, o seu representante de marketing ou re-marketing da IBM poderá ajudá-lo a analisar os requisitos de memória do seu sistema. Para um sistema existente, a quantidade de dados actual no conjunto de discos que está a ser planeado é um ponto de partida útil. A opção Ver Capacidade de Configuração do Disco das DST ou SST mostra o tamanho total (em milhões de bytes) e a percentagem de memória utilizada para cada conjunto de discos do sistema. Multiplique o tamanho dos conjuntos de discos pela percentagem que é utilizada para calcular o número de megabytes de dados presentemente no conjunto de discos. Num futuro planeamento de requisitos de memória para um conjunto de discos, também deverá ser considerado o crescimento e o rendimento do sistema.

A quantidade planeada de dados e a percentagem planeada de memória utilizada funcionam em conjunto para determinar a quantidade de memória auxiliar real necessária para um conjunto de discos replicado. Por exemplo, se se assumir que um conjunto de discos contém 1GB (GB igual a 1 073 741 824 bytes) de dados reais, este requer 2GB de memória para as cópias replicadas dos dados. Se estiver planeado 50% de preenchimento desse conjunto de discos, o conjunto de discos necessitará de 4GB de memória real. Se a percentagem planeada de memória utilizada for 66%, serão necessários 3GB de memória real. Um gigabyte de dados reais (2GB de dados replicados) num conjunto de discos de 5GB resulta numa utilização de 40% da memória auxiliar.

Planear unidades de discos de reserva: As unidades de discos de reserva podem reduzir o tempo que o sistema funciona sem protecção por replicação para um par replicado após uma falha de unidade de discos. Se uma unidade de discos falhar e estiver disponível uma unidade de reserva com a mesma capacidade, essa unidade de reserva pode ser utilizada para substituir a unidade que falhou. Utilizando a opção de substituição das DST ou SST, o utilizador selecciona a unidade de discos a substituir e, em seguida, selecciona uma unidade de discos de reserva para a substituir. O sistema substitui logicamente a unidade que falhou pela unidade de reserva seleccionada e, em seguida, sincroniza a nova unidade com a unidade operacional restante do par replicado. A protecção por replicação desse par estará de novo

activa quando a sincronização terminar (demora, normalmente, menos de uma hora). No entanto, poderá demorar várias horas entre o momento em que é chamado um técnico dos serviços de assistência e o momento em que a unidade que falhou é reparada e sincronizada e a protecção por replicação fica de novo activa para esse par.

Para tirar total partido das unidades de reserva, necessita de, pelo menos, uma unidade de reserva de cada capacidade que tem no sistema. Isso faz com que exista uma unidade de reserva para qualquer tamanho de unidade de discos que possa falhar. Uma unidade que falhe tem de ser substituída por uma unidade de reserva com a mesma capacidade.

Calcular as suas necessidades totais de memória: Após planear o número e tipo de unidades de memória necessárias para cada conjunto de discos do sistema e quaisquer unidades de memória de reserva, adicione o número total de unidades de memória do tipo e modelo de cada unidade de discos. Lembre-se de que o número planeado é o número de unidades de memória de cada tipo de unidade de discos e não o número de unidades de discos. O utilizador, em conjunto com o representante de marketing da IBM, terá de converter o número planeado de unidades de memória em unidades de discos antes de encomendar o hardware.

O procedimento anterior ajuda-o a planear o número total de unidades de discos necessárias para o seu sistema. Se o planeamento for referente a um novo sistema, esse é o número que precisa de ser encomendado. Se o planeamento for referente a um sistema existente, subtraia o número de cada tipo de disco presentemente existente no seu sistema ao número planeado. Daí resulta o número de novas unidades de discos que devem ser encomendadas.

Determinar o nível de protecção pretendido

O nível de protecção por replicação determina se o sistema continua a funcionar quando falham diferentes níveis de hardware. O nível de protecção é a quantidade de hardware relacionado com discos duplicado de que dispõe. Quanto mais pares replicados com níveis superiores de protecção tiver, maior será a possibilidade de utilização do sistema em caso de falha de hardware relacionada com discos. Pode decidir que um nível inferior de protecção é mais rentável em termos de custos para o seu sistema do que um nível superior. Os quatro níveis de protecção por replicação, do menor para o maior, são os seguintes:

- Protecção de nível de unidade de discos
- Protecção de nível de adaptador de input/output
- Protecção de nível de processador de input/output
- Protecção de nível de bus
- Protecção de nível de torre
- Protecção de nível de anel

Ao determinar qual o nível de protecção adequado, deve ter em consideração as vantagens relativas de cada nível de protecção no que respeita aos seguintes aspectos:

- A capacidade de manter o sistema operacional durante uma falha de hardware relacionada com discos.
- A capacidade de executar a manutenção simultaneamente com as operações do sistema. Para minimizar o tempo em que um par replicado está desprotegido após uma falha, pode ter interesse em reparar o hardware que falhou enquanto o sistema está a funcionar.

Durante a operação de início da protecção por replicação, o sistema forma pares de unidades de discos para possibilitar o nível máximo de protecção para o sistema. Quando são adicionadas unidades de discos a um conjunto de discos replicado, o sistema emparelha apenas as unidades de discos que forem adicionadas sem reorganizar os pares existentes. A configuração de hardware inclui o hardware e o modo como esse hardware é ligado.

Para mais informações sobre os níveis de protecção, consulte Níveis de protecção—mais detalhes.

Níveis de protecção—mais detalhes: O nível de protecção por replicação determina se o sistema continua a funcionar quando falham diferentes níveis de hardware. A protecção por replicação fornece

sempre a protecção de nível de unidade de discos, que mantém o sistema disponível após a falha de uma única unidade de discos. Para manter o sistema disponível após falhas de outros componentes de hardware relacionado com discos, são necessários níveis superiores de protecção. Por exemplo, para manter o sistema disponível quando falha um processador de I/O (IOP), todas as unidades de discos ligadas ao IOP que falhou terão de ter unidades replicadas ligadas a IOPs diferentes.

O nível de protecção por replicação também determina se pode ser feita manutenção simultânea para diferentes tipos de falhas. Determinados tipos de falhas necessitam da manutenção simultânea para diagnosticar níveis de hardware acima do componente de hardware que falhou. Por exemplo, para diagnosticar uma falha de energia numa unidade de discos, será necessário repor o processador de I/O ao qual a unidade de discos que falhou está ligada. Por isso, é necessária protecção de nível de IOP. Quanto mais alto for o nível de protecção por replicação, mais vezes será possível a manutenção simultânea.

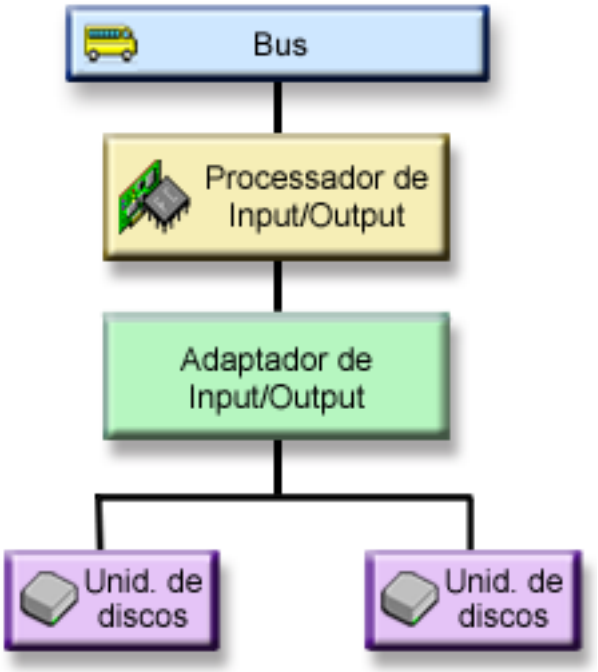
O nível de protecção de que dispõe depende do hardware que duplicar. Se duplicar unidades de discos, terá protecção de nível de unidades de discos. Se também duplicar controladores de unidades de discos, terá protecção de nível de controlador. Se duplicar processadores de input/output, terá protecção de nível de IOP. Se duplicar buses, terá protecção de nível de bus. As unidades replicadas terão sempre, pelo menos, protecção de nível de unidade de discos. Uma vez que a maioria das unidades de discos internas é enviada em conjunto com o controlador, terão, pelo menos, protecção de nível de controlador.

Durante a operação de início da protecção por replicação, o sistema forma pares de unidades de discos para possibilitar o nível máximo de protecção para o sistema. Quando são adicionadas unidades de discos a um conjunto de discos replicado, o sistema emparelha apenas as unidades de discos que forem adicionadas sem reorganizar os pares existentes. A configuração de hardware inclui o hardware e o modo como esse hardware é ligado.

Protecção de nível de unidade de discos: A protecção por replicação fornece sempre a protecção de nível de unidade de discos, uma vez que as unidades de memória são duplicadas. Se a sua principal preocupação reside na protecção dos dados e não na elevada disponibilidade, a protecção de nível de unidade de discos poderá ser a adequada. A unidade de discos é o componente de hardware mais passível de falhar e a protecção de nível de unidade de discos mantém o seu sistema disponível após uma falha de unidade de discos.

A manutenção simultânea é frequentemente possível para certos tipos de falhas da unidade de discos com protecção de nível de unidade de discos.

Esta figura mostra os elementos da protecção de nível de unidade de discos: um bus, ligado a um IOP, ligado a um IOA, que está ligado a duas unidades de discos separadas. As duas unidades de memória formam um par replicado. Com a protecção de nível de unidade de discos, o sistema continua a funcionar após uma falha de unidade de discos. Se o controlador ou o processador de I/O falhar, o sistema não poderá aceder aos dados de nenhuma das unidades de memória do par replicado e o sistema deixará de estar operacional.

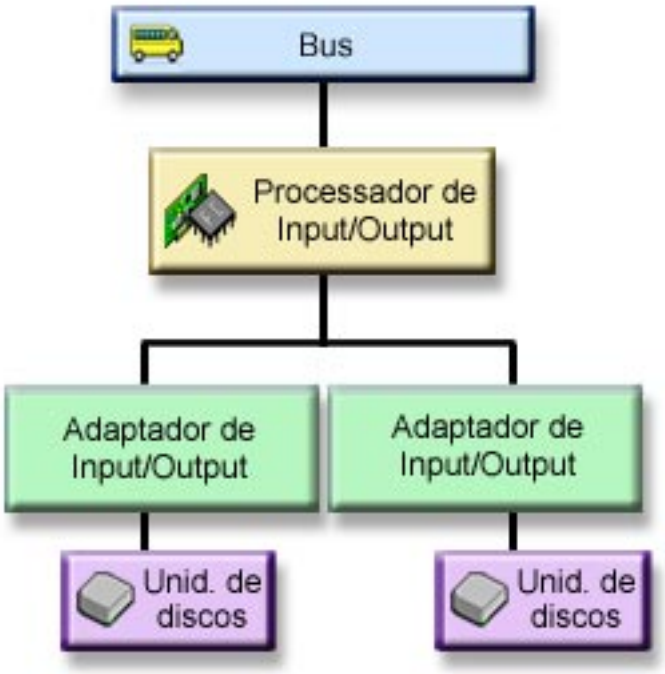


Protecção de nível de adaptador de input/output: Determine se pretende a protecção de nível de adaptador de input/output (IOA) com base no seguinte:

- Manter o seu sistema disponível quando um IOA falha.
- Reparar simultaneamente uma unidade de discos ou IOA em falha. Para utilizar procedimentos de recuperação de problemas na preparação para isolar um item em falha ou para verificar uma acção de reparação, o IOA tem de estar dedicado à acção de reparação. Se quaisquer unidades de discos que estejam anexadas ao IOA não tiverem a protecção de nível de IOA, esta parte da manutenção simultânea não é possível.

Para obter a protecção de nível de IOA, todas as unidades de discos têm de ter uma unidade de discos ligada a um IOA diferente. Esta figura mostra a protecção de nível de IOA. As duas unidades de memória formam um par replicado. Com a protecção de nível de IOA, o sistema pode continuar a funcionar se um IOA falhar. Se o processador de I/O falhar, o sistema não poderá aceder aos dados de nenhuma das unidades de discos e ficará inutilizável.

A fiugura mostra os elementos da protecção de nível de IOA: um bus, ligado a um IOP, ligado a dois IOAs, que estão ligados a duas unidades de discos separadas.

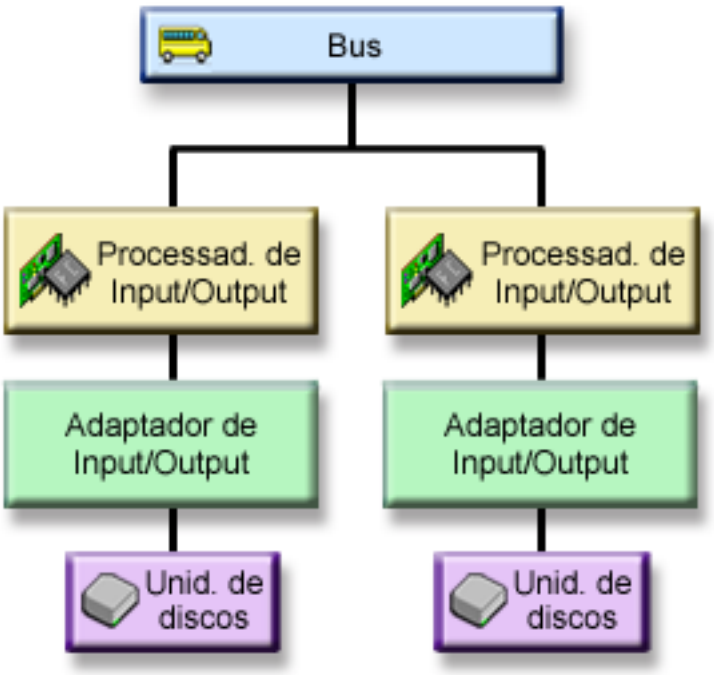


Protecção de nível de processador de input/output: Determine se pretende protecção de nível de IOP com base no seguinte:

- Manter o seu sistema disponível quando falha um processador de I/O.
- Manter o seu sistema disponível quando falha o cabo ligado ao processador de I/O.
- Reparar simultaneamente determinados tipos de falhas de unidades de discos ou de cabos. Para estas falhas, a manutenção simultânea necessita de repor o IOP. Se algumas das unidades de discos ligadas ao IOP não tiverem protecção de nível de IOP, a manutenção simultânea não será possível.

Para conseguir a protecção de nível de processador de I/O, todas as unidades de discos ligadas a um processador de I/O terão de ter uma unidade replicada ligada a um processador de I/O diferente. Em muitos sistemas, a protecção de nível de processador de I/O não é possível para o par replicado, para a unidade 1.

Esta figura mostra os elementos da protecção de nível de IOP: um bus, ligado a dois IOPs, cada um dos quais ligado a dois IOAs separados e a duas unidades de discos separadas. As duas unidades de memória formam um par replicado. Com a protecção de nível de IOP, o sistema pode continuar a funcionar se um processador de I/O falhar. O sistema só ficará inutilizável se o bus falhar.

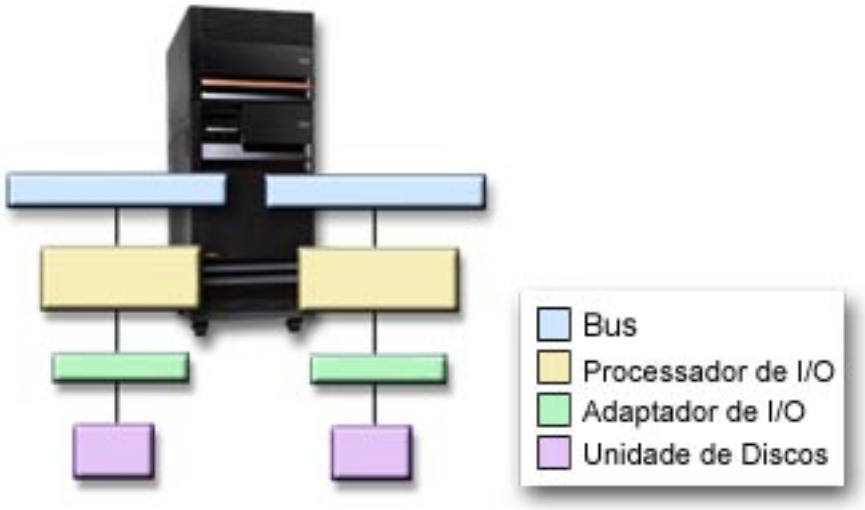


Protecção de nível de bus: A protecção de nível de bus pode permitir ao sistema funcionar quando falha um bus. No entanto, a protecção de nível de bus não costuma ser rentável em termos de custos porque:

- Se o bus 1 falhar, o sistema fica inutilizável.
- Se um bus falhar, as operações de I/O do disco podem continuar, mas perde-se tanto outro hardware (por exemplo, estações de trabalho, impressoras e linhas de comunicações) que, de um ponto de vista prático, o sistema fica inutilizável.
- As falhas de bus são raras quando comparadas com outras falhas de hardware relacionadas com discos.
- A manutenção simultânea não é possível para falhas de bus.

Para conseguir a protecção de nível de bus, todas as unidades de discos ligadas a um bus têm de ter uma unidade replicada ligada a um bus diferente. A protecção de nível de bus não é possível para a unidade 1.

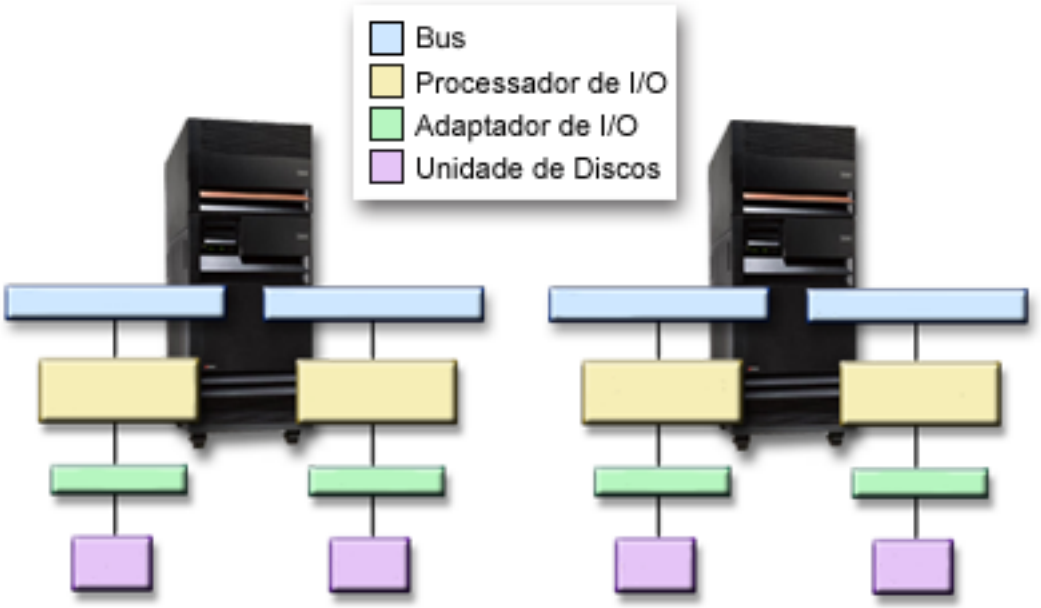
Esta figura mostra os elementos da protecção de nível de bus: uma torre que contém dois buses ligados a dois IOPs, IOAs e unidades de discos separados, respectivamente. As duas unidades de memória formam um par replicado. Com a protecção de nível de bus, o sistema pode continuar a funcionar após uma falha de bus. No entanto, o sistema não pode continuar a funcionar se o bus 1 falhar.



Protecção de nível de torre: A protecção de nível de torre pode permitir ao sistema funcionar quando falhar uma torre. No entanto, a protecção de nível de torre não costuma ser rentável em termos de custos porque:

- Se uma torre falhar, as operações de I/O do disco podem continuar, mas perde-se tanto outro hardware tal como, por exemplo, estações de trabalho, impressoras e linhas de comunicações que, de um ponto de vista prático, o sistema fica inutilizável.
- As falhas de torre são raras quando comparadas com outras falhas de hardware relacionadas com discos.

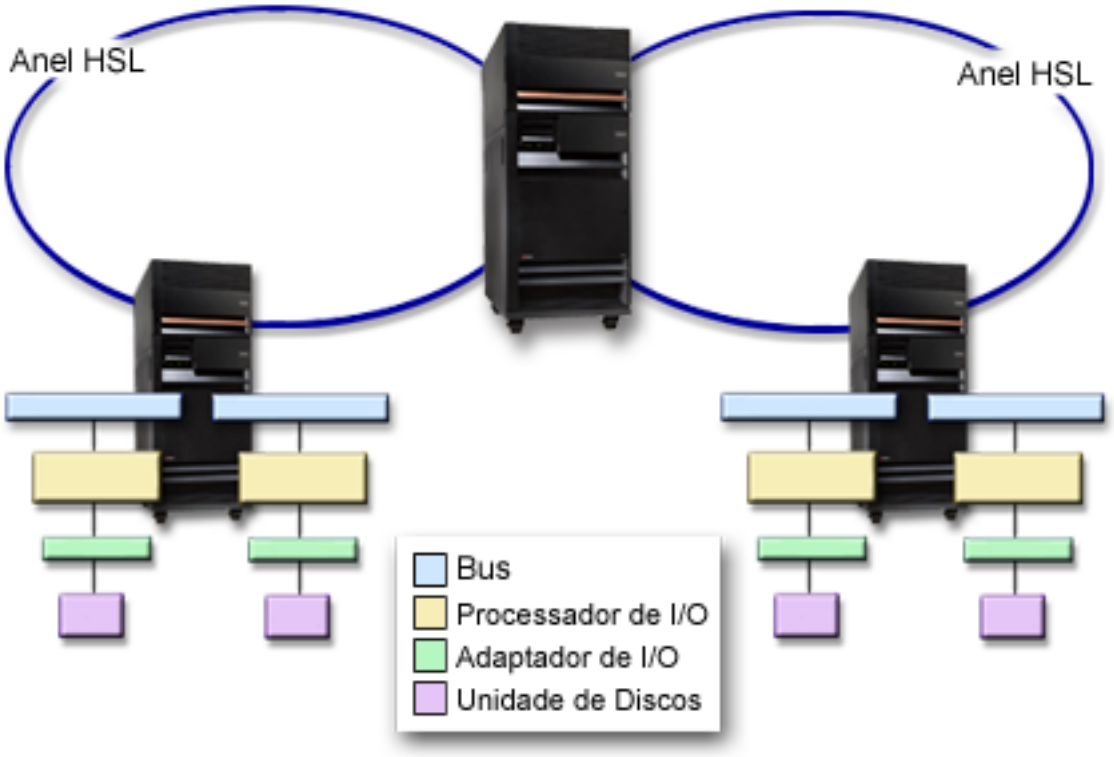
Para conseguir uma protecção de nível de torre, todas as unidades de discos de uma torre têm de ter uma unidade replicada ligada a outra torre. A figura mostra os elementos da protecção de nível de torre: duas torres que contêm, cada uma, dois buses que estão ligados a IOPs, IOAs e unidades de discos separadas, respectivamente.



Protecção de nível de anel: A protecção de nível de anel pode permitir ao sistema funcionar quando falhar uma ligação de alta velocidade (HSL). No entanto, a protecção de nível de anel não costuma ser rentável em termos de custos porque:

- Se falhar uma HSL, as operações de I/O do disco podem continuar, mas perde-se tanto outro hardware tal como, por exemplo, estações de trabalho, impressoras e linhas de comunicações que, de um ponto de vista prático, o sistema fica inutilizável.
- As falhas de HSL são raras quando comparadas com outras falhas de hardware relacionadas com discos.

Para conseguir uma protecção de nível de anel, todas as unidades de discos de uma torre na primeira HSL têm de ter uma unidade replicada ligada a outra torre na segunda HSL. A figura mostra os elementos da protecção de nível de anel: dois anéis HSL, ligados a duas torres que contêm, cada uma, dois buses que estão ligados a IOPs, IOAs e unidades de discos separadas, respectivamente.



Determinar o hardware extra necessário para a protecção por replicação

Para comunicar com o resto do sistema, as unidades de discos são ligadas a controladores, que estão ligados a processadores de I/O, que estão ligados a buses. O número de cada um destes tipos de hardware relacionado com discos disponível no sistema afecta directamente o nível de protecção possível.

Para conseguir a melhor protecção e rendimento, cada nível de hardware deve ser equilibrado sob o nível de hardware seguinte. Isto é, as unidades de discos de cada modelo e tipo de dispositivo devem ser distribuídas de modo igual sob os respectivos controladores. Deve existir o mesmo número de controladores sob cada processador de I/O para esse tipo de disco. Os processadores de I/O devem ser distribuídos igualmente entre os buses disponíveis.

Para planear qual o hardware relacionado com discos necessário para o seu sistema replicado, terá de planear o número total e o tipo de unidades de discos (antigas e novas) que serão necessárias no sistema, bem como o nível de protecção para o sistema. Nem sempre é possível planear e configurar um sistema de modo a que todos os pares replicados respeitem o nível de protecção planeado. No entanto, é possível planear uma configuração em que o nível pretendido de protecção seja atingido por uma percentagem muito grande de unidades de discos do sistema.

Ao planear hardware relacionado com discos adicional, precisa de:

1. Determinar o hardware mínimo necessário para as unidades de discos planeadas funcionarem. Planeie um tamanho de unidade de discos de cada vez.
2. Planear o hardware adicional necessário para o nível de protecção pretendido para cada tipo de unidade de discos.

Determinar o hardware mínimo necessário para as unidades de discos planeadas funcionarem:
Existem várias regras e limites à forma como o hardware de memória pode ser ligado entre si. Os limites podem ser determinados pela concepção de hardware, por restrições de arquitectura, por considerações

sobre rendimento ou por preocupações de assistência. O seu representante de marketing da IBM poderá explicar estes limites de configuração e ajudá-lo a utilizá-los no seu planeamento. Para obter uma listagem dos limites e regras de configuração, consulte Instalação, actualizações e migração.

Para cada tipo de unidade de discos, comece por planear os controladores necessários e, em seguida, os processadores de I/O necessários. Depois de planear o número de processadores de I/O necessários para todos os tipos de unidades de discos, utilize o número total de processadores de I/O para planear o número de buses necessários.

Planear o hardware adicional necessário para o nível de protecção pretendido para cada tipo de unidade de discos:

- Protecção de nível de unidade de discos
  Se planeou a protecção de nível de unidade de discos, não será necessário fazer mais nada. Todos os conjuntos de discos replicados têm um mínimo de protecção de nível de unidade de disco, caso cumpram os requisitos da protecção por replicação inicial.
- Protecção de nível de controlador
  Se as unidades de discos planeadas não necessitarem de um controlador distinto, já terá protecção de nível de controlador para as unidades possíveis e não será necessário fazer mais nada. Se as unidades de discos planeadas necessitarem de um controlador distinto, adicione os controladores possíveis, respeitando os limites do sistema definidos. Em seguida, equilibre as unidades de discos entre os IOPs de acordo com as regras standard de configuração de sistemas.
- Protecção de nível de processador de input/output
  Se pretende a protecção de nível de IOP e ainda não tem o número máximo de IOPs no seu sistema, adicione os IOPs possíveis, respeitando os limites do sistema definidos. Em seguida, equilibre as unidades de discos entre os IOPs de acordo com as regras standard de configuração de sistemas. Poderá ser necessário adicionar mais buses para ligar mais IOPs.
- Protecção de nível de bus
  Se pretende a protecção de nível de bus e já tem um sistema com múltiplos buses, não precisa de fazer nada. Se o seu sistema está configurado de acordo com regras de configuração standard, a função de emparelhamento de pares replicados forma pares de unidades de memória de modo a possibilitar a protecção de nível de bus aos pares replicados possíveis. Se tiver um sistema de bus único, pode adicionar buses adicionais como opção de dispositivo.
- Protecção de nível de torre
  Se o sistema estiver configurado com um número igual de unidades de disco com igual capacidade entre torres, a função de emparelhamento por replicação emparelhará as unidades de disco em torres diferentes para fornecer protecção do nível de torre no maior número de unidades possível.
- Protecção de nível de anel
  Se o sistema estiver configurado com um número igual de unidades de disco com igual capacidade entre ligações de alta velocidade (HSL), a função de emparelhamento por replicação emparelhará as unidades de disco em torres diferentes para fornecer protecção do nível de ligação de alta velocidade (HSL) no maior número de unidades possível.

Determinar o hardware extra necessário para o rendimento

Normalmente, a protecção por replicação requer unidades de discos e processadores de input/output adicionais. No entanto, em alguns casos, poderá necessitar de hardware adicional para obter o nível de rendimento pretendido.

Utilize as seguintes informações para decidir a quantidade de hardware extra que poderá ser necessária:

- **Requisitos da unidade de processamento**

  A protecção por replicação provoca um ligeiro aumento da utilização da unidade central de processamento (aproximadamente 1% a 2%).
- **Requisitos da memória principal**

  Se tem protecção por replicação, necessita de aumentar o tamanho do conjunto de memória máquina. A protecção por replicação necessita de memória no conjunto de memória máquina para objectivos

gerais e para cada par replicado. Deve contar com um aumento do conjunto de memória máquina de aproximadamente 12KB por cada GB de memória de disco replicado (12KB para 1GB DASD, 24KB para 2GB DASD, etc.).

Durante a sincronização, a protecção por replicação utiliza 512 KB adicionais de memória por cada par replicado que está a ser sincronizado. O sistema utiliza o conjunto com o máximo de memória.

- **Requisitos do processador de I/O**

  Para manter um rendimento equivalente após o início da protecção por replicação, o sistema deverá ter a mesma proporção de unidades de discos para processadores de I/O que tinha anteriormente. Para adicionar processadores de I/O, poderá ser necessário actualizar o sistema para ter mais buses.

  Devido ao limite de buses e processadores de I/O, poderá não conseguir manter a mesma proporção de unidades de discos para processadores de I/O. Neste caso, o rendimento do sistema poderá ser menor.

Para mais informações sobre o efeito que a replicação tem sobre o rendimento, consulte Replicação e rendimento.

Replicação e rendimento: Quando a protecção por replicação é iniciada, a maioria dos sistemas mostra pouca diferença no rendimento; em alguns casos, a protecção por replicação pode melhorar o rendimento. Geralmente, as funções que efectuam essencialmente operações de leitura terão um rendimento igual ou melhor com a protecção por replicação. Isso deve-se ao facto de as operações de leitura poderem escolher entre duas unidades de memória para ler e de ser seleccionada a que é suposta ter o tempo de resposta mais rápido. As operações que efectuam essencialmente operações de escrita (como, por exemplo, a actualização de registos de base de dados) poderão assistir a uma ligeira redução do rendimento num sistema que tenha protecção por replicação, uma vez que todas as alterações têm de ser escritas em ambas as unidades de memória do par replicado. Assim se explica o facto de as operações de restauro serem mais lentas.

Em alguns casos, se o sistema terminar anormalmente, o sistema não conseguirá determinar se as últimas actualizações foram escritas para ambas as unidades de memória de cada par replicado. Se o sistema não tiver a certeza de que as últimas alterações foram escritas para ambas as unidades de memória do par replicado, o sistema sincronizará o par replicado copiando as dados em questão de uma unidade de memória de cada par replicado para a outra unidade de memória. A sincronização ocorre durante o IPL que se segue ao fim anormal do sistema. Se o sistema conseguir guardar uma cópia da memória principal antes de terminar, o processo de sincronização demorará apenas alguns minutos. Caso contrário, o processo de sincronização poderá demorar muito mais. Na pior das hipóteses, poderá ser necessária uma sincronização quase total.

Se tiver frequentes cortes de alimentação, talvez seja melhor adicionar uma fonte de alimentação ininterrupta ao seu sistema. Caso a fonte de alimentação principal falhe, a fonte de alimentação ininterrupta permite ao sistema continuar. Uma fonte de alimentação ininterrupta básica dá ao sistema tempo para guardar uma cópia da memória principal antes de terminar, o que evita uma longa recuperação. Ambas as unidades de memória do par replicado da origem de carregamento têm de ser alimentadas pela fonte de alimentação ininterrupta básica.

Encomendar o novo hardware

O seu representante de marketing da IBM ajudá-lo-á a encomendar o novo hardware através do procedimento de encomendas. Esse procedimento de encomenda permite-lhe obter qualquer outro tipo de hardware que possa ser necessário como parte da actualização que vai efectuar, como, por exemplo, bastidores e cabos adicionais.

Planear a instalação do sistema

Tem de trabalhar em conjunto com o seu representante de marketing daIBM para planear a instalação da protecção por replicação no sistema. O representante de marketing ajudá-lo-á a determinar se o seu sistema está equilibrado e cumpre as regras de configuração standard, tal como está definido emInstalação, actualizações e migração. O sistema tem de ser configurado de acordo com as regras standard de modo a que a função de formação de pares replicados emparelhe as unidades de memória

de forma a conseguir a melhor protecção possível a partir do hardware disponível. O seu representante de marketing também o ajudará a planear as novas unidades que é necessário adicionar a cada conjunto de discos.

Se pensa iniciar a protecção por replicação num novo sistema, esse sistema já se encontra configurado de acordo com as regras de configuração standard. Se estiver a utilizar um sistema mais antigo, esse sistema poderá não respeitar as regras standard. No entanto, espere até depois de tentar iniciar a protecção por replicação para reconfigurar qualquer hardware.

Para obter mais informações sobre como planear os conjuntos de discos, consulte Planear quais os conjuntos de discos a criar.

Planear quais os conjuntos de discos a criar: Planeie os conjuntos de discos do utilizador que terão protecção por replicação e determine quais as unidades a adicionar aos conjuntos de discos. O manual Cópia de Segurança e Recuperação  contém informações sobre como atribuir unidades de discos a adicionar a conjuntos de discos.

Em geral, as unidades de um conjunto de discos deverão ser equilibradas ao longo de vários processadores de I/O, em vez de serem todas ligadas ao mesmo processador de I/O. Isso possibilita uma melhor protecção e rendimento.

Instalar o novo hardware

Quando receber o hardware, o seu técnico dos serviços de assistência instalá-lo-á. Após o hardware instalado, consulte Adicionar uma unidade de discos ou conjunto de discos para obter informações sobre como adicionar novas unidades e iniciar a protecção por replicação.

Suporte de replicação de DASD remota

O suporte de replicação de DASD standard necessita que ambas as unidades de discos do par replicado da origem de carregamento (unidade 1) estejam ligadas ao Processador de I/O Multifunção (MFIOP). Isso permite ao sistema executar um IPL a partir de qualquer uma das origens de carregamento do par replicado e permite ao sistema fazer uma cópia da memória principal para qualquer uma das origens de carregamento se o sistema terminar anormalmente. No entanto, uma vez que ambas as origens de carregamento têm de estar ligadas ao mesmo Processador de I/O (IOP), a protecção de nível de controlador é a melhor protecção por replicação possível para o par replicado da origem de carregamento. Para proporcionar um nível de protecção superior para o sistema, pode utilizar a replicação da origem de carregamento remota e a replicação de DASD remota.

O suporte de replicação de DASD remota, quando combinado com a replicação da origem de carregamento remota, replica o DASD de buses ópticos locais com o DASD de buses ópticos que terminam numa localização remota. Nesta configuração, todo o sistema, incluindo a origem de carregamento, pode ser protegido de um desastre da localização. Se houver perda da localização remota, o sistema pode continuar a funcionar no DASD da localização local. Se houver perda do DASD local e da unidade de sistema, pode ser ligada uma nova unidade de sistema ao conjunto de DASD da localização remota e o processamento do sistema pode ser retomado.

A replicação de DASD remota, tal como a replicação de DASD standard, suporta a combinação de unidades de discos protegidas por paridade de dispositivos no mesmo conjunto de discos com unidades de discos replicadas; o DASD de paridade de dispositivos pode encontrar-se na localização local ou remota. No entanto, se ocorrer uma catástrofe na localização que contém o DASD de paridade de dispositivos, perder-se-ão todos os dados nos conjuntos de discos que contenham o DASD de paridade de dispositivos.

O suporte de replicação remota torna possível dividir as unidades de discos do seu sistema num grupo de DASD locais e um grupo de DASD remotos. Os DASD remotos estão ligados a um conjunto de buses ópticos e os DASD locais a outro conjunto de buses. O DASD local e remoto podem estar fisicamente

separados um do outro em locais diferentes, expandindo os buses ópticos adequados ao local remoto. A distância entre os locais está limitada à distância pela qual se pode expandir um bus óptico.

Para mais informações sobre replicação de DASD remota, consulte os seguintes tópicos:
Replicação de DASD remota—vantagens
Replicação de DASD remota—desvantagens
Comparação entre a replicação standard e remota

Se decidir que a replicação de DASD remota é a protecção correcta para o seu sistema, terá de preparar o sistema para replicação remota e, em seguida, iniciar a replicação entre localizações.

Replicação da origem de carregamento remota

O suporte de replicação da origem de carregamento remota permite que as duas unidades de discos da origem de carregamento estejam em IOPs ou buses do sistema diferentes, o que proporciona protecção por replicação de nível de IOP ou bus para a origem de carregamento. No entanto, neste tipo de configuração, o sistema só pode executar um IPL a partir da, ou executar uma cópia de memória principal para a origem de carregamento ligada ao MFIOP. Se a origem de carregamento do MFIOP falhar, o sistema pode continuar a funcionar na outra unidade de discos do par replicado da origem de carregamento, mas o sistema não conseguirá executar um IPL ou uma cópia da memória principal até que a origem de carregamento ligada ao MFIOP esteja reparada e passível de ser utilizada.

Para mais informações sobre replicação da origem de carregamento remota, consulte os seguintes tópicos:

- Activar replicação da origem de carregamento remota
- Desactivar replicação da origem de carregamento remota
- Utilizar replicação da origem de carregamento remota com DASD local

Activar replicação da origem de carregamento remota: Para utilizar o suporte de replicação da origem de carregamento remota, tem de começar por activar a replicação da origem de carregamento remota. Em seguida, terá de ser iniciada a protecção por replicação para o conjunto de discos 1. Se o suporte de replicação da origem de carregamento remota for activado após a protecção por replicação já ter sido iniciada para o conjunto de discos 1, a protecção por replicação e o emparelhamento replicado existentes da origem de carregamento não serão alterados.

O suporte de replicação da origem de carregamento remota pode ser activado no ambiente das DST ou SST no iSeries Navigator ou na interface baseada em caracteres. Se tentar activar a replicação da origem de carregamento remota e esta já estiver activada, o sistema apresentará uma mensagem indicando que a replicação da origem de carregamento remota já se encontra activada. Não existem outros erros ou avisos na activação do suporte de replicação da origem de carregamento remota.

Para activar a replicação da origem de carregamento remota, proceda do seguinte modo:

1. No menu principal das DST, seleccione a opção 4, Trabalhar com unidades de discos.
2. No menu Trabalhar com unidades de discos, seleccione a opção 1, Trabalhar com configuração do disco.
3. No menu Trabalhar com configuração do disco, seleccione a opção 4, Trabalhar com protecção por replicação.
4. No menu Trabalhar com protecção por replicação, seleccione a opção 4, Activar replicação da origem de carregamento remota. Isso fará com que seja apresentado um ecrã de confirmação Activar replicação da origem de carregamento remota.
5. Prima Enter no ecrã de confirmação Activar replicação da origem de carregamento remota. Será apresentado o ecrã Trabalhar com protecção por replicação, com uma mensagem na parte inferior a indicar que a replicação da origem de carregamento remota foi activada.

Desactivar replicação da origem de carregamento remota: Se desejar desactivar o suporte de replicação da origem de carregamento remota, tem de:

- Parar a protecção por replicação e, em seguida, desactivar o suporte de replicação da origem de carregamento remota.

ou

- Mover a origem de carregamento remota para o MFIOP e, em seguida, desactivar o suporte de replicação da origem de carregamento remota.

  Se a origem de carregamento remota for movida para o MFIOP, o IOP e o sistema podem não reconhecê-la devido aos diferentes tamanhos do formato de DASD utilizados por diferentes IOPs. Se a origem de carregamento remota faltar após ter sido movida para o MFIOP, utilize a função de DST Substituir unidade de discos para substituir a origem de carregamento em falta por ela própria. Isso fará com que o DASD seja reformatado de modo a que o MFIOP o possa utilizar e, em seguida, a unidade de discos será sincronizada com a origem de carregamento activa.

A replicação da origem de carregamento remota pode ser desactivada a partir das DST ou das SST. No entanto, a desactivação da replicação da origem de carregamento remota não será permitida se existir no sistema uma unidade de discos da origem de carregamento que não esteja ligada ao MFIOP. Se tentar desactivar o suporte de replicação da origem de carregamento remota e este já estiver desactivado, o sistema mostrará uma mensagem indicando que a replicação da origem de carregamento remota já está desactivada.

Para desactivar o suporte de replicação da origem de carregamento remota, proceda do seguinte modo:

1. No menu principal das DST, seleccione a opção 4, Trabalhar com unidades de discos.
2. No menu Trabalhar com unidades de discos, seleccione a opção 1, Trabalhar com configuração do disco.
3. No menu Trabalhar com configuração do disco, seleccione a opção 4, Trabalhar com protecção por replicação.
4. No menu Trabalhar com protecção por replicação, seleccione a opção 5, Desactivar replicação da origem de carregamento remota. Isso fará com que seja apresentado um ecrã de confirmação Desactivar replicação da origem de carregamento remota.
5. Prima Enter no ecrã de confirmação Desactivar replicação de origem de carregamento remota. Será apresentado o ecrã Trabalhar com protecção por replicação, com uma mensagem na parte inferior a indicar que a replicação da origem de carregamento remota foi desactivada.

Utilizar replicação da origem de carregamento remota com DASD local: A replicação da origem de carregamento remota pode ser usada para conseguir uma protecção ao nível do IOP ou do bus do par replicado da origem do carregamento, mesmo sem DASD ou buses remotos no sistema. Não é necessária configuração especial, para além de assegurar que existe uma unidade de discos com a mesma capacidade da origem de carregamento ligada a outro IOP ou bus no sistema. Se pretender obter a protecção de nível de bus de todos os pares replicados de um conjunto de discos, deverá configurar o sistema de modo a que seja apenas anexada até metade do DADS de qualquer capacidade indicada desse conjunto de discos a qualquer bus único. Se pretender obter a protecção de nível de IOP de todos os pares replicados num conjunto de discos, não poderá ter mais de metade do DADS de qualquer capacidade indicada no conjunto de discos anexada a um IOP único.

Após o hardware do sistema ter sido configurado correctamente, active a replicação da origem de carregamento remota e inicie a replicação para os conjuntos de discos que pretenda proteger. Utilize a função de início de replicação normal. Não existe uma função de replicação especial de início de replicação para o suporte ao carregamento origem remoto. O sistema detectará se a replicação da origem de carregamento remota está activada e formará automaticamente pares de unidades de discos, de modo a obter o melhor nível de protecção possível. Só é possível sobrepor ou influenciar o emparelhamento das unidades de discos alterando a forma como o hardware do sistema está ligado e configurado. Aplicam-se restrições de replicação normais relacionadas com a capacidade total do conjunto de discos, um número par de unidades de discos de cada capacidade, etc.

Replicação de DASD remota—vantagens

- A Replicação de DASD Remota pode fornecer protecção de nível de IOP ou de bus para a origem de carregamento.
- A Replicação de DASD Remota permite ao DASD ser divido em duas localizações, replicando uma localização para outra, de modo a obter protecção contra um desastre de localização.

Replicação de DASD remota—desvantagens

- Um sistema que utilize a Replicação de DASD Remota só consegue executar um IPL a partir de um DASD do par replicado da origem de carregamento. Se esse DASD falhar e não for possível repará-lo simultaneamente, o sistema não poderá executar o IPL enquanto a origem de carregamento em falha não for reparada e enquanto não for executado o procedimento de recuperação da origem de carregamento remota.
- Quando a Replicação de DASD Remota está activa num sistema e a única origem de carregamento que o sistema pode utilizar para executar um IPL falhar, não será possível ao sistema executar um cópia de memória principal se o sistema terminar anormalmente. Isso significa que o sistema não pode utilizar a cópia de memória principal ou a alimentação contínua da memória principal (CPM) para reduzir o tempo de recuperação de uma avaria do sistema. Também significa que a cópia de memória principal não está disponível para diagnosticar o problema que leva o sistema a terminar anormalmente.

Comparação da gestão de DASD com replicação standard e com replicação remota

A maioria das vezes, o modo como gere o DASD com replicação remota é idêntico ao modo como gere o DASD com replicação standard. As diferenças estão no modo como adiciona unidades de discos e como restaura a protecção por replicação depois de uma recuperação.

Adicionar unidades de discos: As unidades de discos desprotegidas têm de ser adicionadas aos pares, tal como acontece com a replicação geral. Para conseguir a protecção remota de todas as unidades adicionadas, metade das novas unidades de cada capacidade de DASD deve existir no grupo remoto e metade no grupo local. As unidades protegidas pela paridade de dispositivos podem ser adicionadas a conjuntos de discos através da replicação remota. No entanto, o conjunto de discos não será protegido contra uma catástrofe nas instalações.

Restaurar protecção por replicação após uma recuperação: Para restaurar a protecção por replicação a seguir aos procedimentos de recuperação, será necessário executar os seguintes passos:

- Obtenha e ligue fisicamente todas as unidades de DASD requeridas.
- Pare ou suspenda a protecção por replicação, se esta estiver actualmente configurada no sistema.
- Adicione as novas unidades de DASD aos conjuntos de discos apropriados.
- Retome a protecção por replicação.

Para obter informações detalhadas sobre como recuperar sistemas com protecção por replicação, consulte o manual Cópia de Segurança e Recuperação  .

Preparar o sistema para replicação remota

Quando inicia a replicação remota do sistema, o DASD local é replicado para o DASD remoto. Se ocorrer um desastre na localização local ou remota, continuará a existir uma cópia completa de todos os dados do sistema, a configuração do sistema pode ser recuperada e o processamento pode continuar. Para fornecer protecção contra uma catástrofe na localização, todos os DASDs de todos os conjuntos de discos do sistema deverão estar replicados em pares local-remoto. Siga estes passos para preparar o sistema para replicação remota:

1. Defina quais os buses ópticos que vão alimentar o DASD na localização remota.
   - Não é funcionalmente necessário que a localização local e remota utilizem a mesma quantidade de buses; no entanto, é mais simples configurar e entender o sistema se o número de buses remotos e locais e de DASD for igual.

- É funcionalmente necessário que ambas as localizações local e remota tenham o mesmo número de cada capacidade de DADS em cada conjunto de discos.

2. Planeie a distribuição do DASD, mova o DASD, se necessário, e verifique se está ligada metade de cada capacidade do DADS em cada conjunto de discos ao conjunto de buses local e remoto.
3. Indique ao sistema que buses controlam o DASD remoto e que buses controlam o DASD local. Para isso, tem primeiro de determinar que buses controlam o DASD remoto e anotar o número desses buses. Em seguida, tem de alterar os IDs de recurso do sistema dos buses remotos para que comecem por *R*.

   Por exemplo, se determinar que o BUS11 controla o DASD remoto, deve alterar o ID do recurso do sistema desse bus para *RBUS11*

Determinar que buses controlam o DASD remoto: Se os buses não estiverem identificados, poderá ter de rastrear os buses manualmente para ver quais se dirigem para localizações remotas. Também pode utilizar o Gestor de Serviços de Hardware para determinar que buses se dirigem para que unidades de expansão.

Para utilizar o Gestor de Serviços de Hardware para determinar os buses que controlam o DASD remoto, execute os seguintes passos:

1. No Menu Principal das DST, seleccione a opção 7 (Iniciar uma ferramenta de serviço).
2. No ecrã Iniciar uma Ferramenta de Serviço, seleccione a opção 4 (Gestor de serviços de hardware).
3. No menu Gestor de Serviços de Hardware, seleccione a opção 2, Recursos lógicos de hardware.
4. No menu Recursos Lógicos de Hardware, seleccione a opção 1, Recursos de bus de sistema.
5. No ecrã Recursos Lógicos de Hardware no Bus de Sistema, introduza a opção 8 antes de cada bus para ver os recursos de pacote associados.
6. Os recursos de pacote associados a um ecrã de recurso lógico apresentam o ID de estrutura e o nome de recurso da unidade de expansão associada ao bus. Se necessitar de mais informações para o ajudar a encontrar e distinguir as unidades de expansão em causa, introduza a opção 5 junto à Unidade de expansão de sistema para ver outros detalhes sobre a unidade de expansão.

   Anote a localização remota ou local do bus. Em seguida, repita este procedimento para todos os buses do sistema.

Alterar nomes de recurso do bus remoto: Depois de saber quais os buses que controlam o DASD remoto, utilize o Gestor de Serviços de Hardware para alterar os nomes de recurso dos buses remotos.

Para alterar os nomes de recurso dos buses remotos, execute estes passos:

1. No Menu Principal das DST, seleccione a opção 7 (Iniciar uma ferramenta de serviço).
2. No ecrã Iniciar uma Ferramenta de Serviço, seleccione a opção 4 (Gestor de serviços de hardware).
3. No menu Gestor de Serviços de Hardware, seleccione a opção 2, Recursos lógicos de hardware.
4. No menu Recursos Lógicos de Hardware, seleccione a opção 1, Recursos de bus de sistema.
5. No ecrã Recursos Lógicos de Hardware no Bus de Sistema, seleccione com o número 2 o bus cujo nome deseja alterar. Será apresentado o ecrã Alterar Detalhe de Recurso Lógico de Hardware.
6. No ecrã Alterar Detalhe de Recurso Lógico de Hardware, na linha identificada como Novo nome de recurso, mude o nome do recurso adicionando a letra *R* ao início do nome de recurso do bus; por exemplo, mude *BUS08* para *RBUS08*. Prima Enter para alterar o nome do recurso.

   Repita este procedimento para cada bus remoto no sistema.

Iniciar a replicação entre localizações

Depois de preparar o sistema para replicação remota, siga estes passos para iniciar a replicação remota:

1. Activar replicação da origem de carregamento remota. Permite ter uma origem de carregamento como parte do grupo de DASD remoto.
2. Iniciar replicação utilizando a função iniciar replicação normal.

Quando a replicação for iniciada, o sistema utilizará o nome do recurso para reconhecer os buses remotos e tentará formar pares com os DASD dos buses remotos e os DASD dos buses locais. Uma vez que a replicação da origem de carregamento remota está activada, o sistema também formará par com a origem de carregamento e um DASD remoto. Aplicam-se restrições de replicação normais relacionadas com a capacidade total do conjunto de discos, um número par de unidades de discos de cada capacidade, etc.

3. No ecrã de confirmação do início da replicação, assegure-se de que todos os pares replicados dispõem de um nível de protecção de *Bus Remoto*. Se não tiverem, prima F12 para cancelar o início da replicação, determine o motivo pelo qual algumas unidades têm um nível de protecção inferior ao esperado, corrija o problema e tente reiniciar a replicação.

Capítulo 2. Seleccionar o seu nível de protecção

Existem várias formas de configurar o sistema de modo a tirar partido das funções de protecção do disco. Antes de seleccionar as opções de protecção do disco que pretende utilizar, compare o âmbito de protecção fornecido por cada uma delas.

- Comparação das opções de protecção do disco
- Protecção por replicação total e protecção por replicação parcial

Após comparar as opções de protecção do disco, seleccione um destes métodos de utilização das opções:

- Protecção total—Conjunto de discos único
- Protecção total—Múltiplos conjuntos de discos
- Protecção parcial—Múltiplos conjuntos de discos
- “Atribuir unidades de discos a conjuntos de discos” na página 54

Comparação das opções de protecção do disco

Deve ter em conta estas considerações quando seleccionar as opções de protecção do disco:

- Com a protecção por paridade de dispositivos e a protecção por replicação, o sistema continua a funcionar após a falha de um disco. Com a protecção por replicação, o sistema poderá continuar a funcionar após uma falha num componente relacionado com o disco como, por exemplo, um controlador ou um IOP.
- Se ocorrer uma segunda falha do disco que origine a falha de dois discos no sistema,é mais provável que o sistema continue em execução com a protecção por replicação do que com a protecção por paridade de dispositivos. Com a protecção por paridade de dispositivos, a probabilidade de o sistema parar durante a segunda falha do disco pode ser expressa como P de n. P corresponde ao número total de discos do sistema e n ao número de discos do conjunto de paridade de dispositivos que sofreu a primeira falha de disco. Com a protecção por replicação, a probabilidade de o sistema parar durante a segunda falha do disco é 1 de n.
- A Protecção por paridade de dispositivos requer um disco de capacidade existente por conjunto de paridade para o armazenamento de informações de paridade. Um sistema com a protecção por replicação requer o dobro da capacidade do disco que o mesmo sistema sem a protecção por replicação porque todas as informações são armazenadas duas vezes. A Protecção por replicação também pode requerer mais buses, IOPs e controladores de disco, dependendo do nível de protecção que deseja. Deste modo, a protecção por replicação é, normalmente, uma solução mais dispendiosa do que a protecção por paridade de dispositivos.
- Normalmente, nem a protecção por paridade de dispositivos, nem a protecção por replicação têm um efeito significativo no rendimento do sistema. Em certos casos, a protecção por replicação melhora, na realidade, o rendimento do sistema.
- O tempo necessário para restaurar dados para as unidades de discos protegidas pela protecção por paridade de dispositivos é superior ao tempo de restauro, para o mesmo disco, de dispositivos sem a protecção por paridade de dispositivos activada, uma vez que os dados de paridade têm de ser calculados e escritos.

Esta tabela fornece uma descrição geral das ferramentas de disponibilidade que podem ser utilizadas no servidor para o proteger contra diferentes tipos de falhas.

Qual o tipo de disponibilidade necessária?	Protecção por Paridade de Dispositivos	Protecção por Replicação	Conjuntos de discos base	Conjunto de discos independente
Proteger contra a perda de dados devido a falha de hardware relacionado com o disco	Sim	Sim	Consulte a nota[2]	Consulte a nota[2]
Manter disponibilidade	Sim	Sim	Não	Sim[4]
Ajuda com recuperação da unidade de discos	Sim	Sim	Sim[2]	Sim[2]
Manter a disponibilidade quando o adaptador de input-output (IOA) falha	Não	Sim[1]	Não	Não
Manter disponibilidade quando o processador de I/O do disco falha	Não	Sim[1]	Não	Não
Manter a disponibilidade quando o bus do sistema falha	Não	Sim[1]	Não	Não
Protecção em caso de acidente nas instalações	Não	Sim[3]	Não	Não
Possibilidade de trocar dados entre sistemas	Não	Não	Não	Sim

Notas:

[1] Depende do hardware utilizado, da configuração e do nível de protecção por replicação.

[2] A configuração dos conjuntos de discos pode limitar a perda de dados e a recuperação de um único conjunto de discos.

[3] Para a protecção em caso de desastre nas instalações, é necessária a replicação remota.

[4] Num ambiente com conjuntos de unidades, um conjunto de discos independente pode ajudar a manter a disponibilidade.

Consulte também:

- “Como o sistema gere a memória auxiliar” na página 51
- “Como os discos estão configurados” na página 51

Protecção por replicação total e protecção por replicação parcial

A protecção por replicação total e a protecção por replicação parcial não fornecem os mesmos resultados em termos de disponibilidade. Estas duas implementações da protecção por replicação são bastante diferentes. Os cenários de uma unidade de discos no servidor iSeries para cada um destes métodos de replicação requerem respostas diferentes por parte do utilizador.

Quer esteja a utilizar apenas o conjunto de discos do sistema (conjunto de discos 1) ou vários conjuntos de discos do utilizador (2 a 255), a protecção por replicação total protege totalmente todas as unidades de discos existentes no servidor iSeries. A protecção por replicação parcial protege apenas uma parte das unidades de discos designadas por um ou mais conjuntos de discos. No entanto, nem todas as unidades de memória da configuração do disco são protegidas. Deste modo, o planeamento da colocação das unidades de discos e de quais os conjuntos de discos seleccionados para a protecção por replicação torna-se mais difícil.

Além do planeamento dos conjuntos de discos, a diferença significativa entre os dois métodos de protecção está relacionada com a disponibilidade. Com a protecção por replicação total, a disponibilidade do servidor iSeries é maximizada quando ocorre uma falha no subsistema de disco. Com este método de protecção por replicação, não é relevante qual o conjunto de discos em que ocorreu a falha. Com a protecção por replicação parcial, o sistema continua em execução enquanto comunica a falha na unidade de memória à fila de mensagens do operador do sistema (QSYSOPR). No entanto, se a falha do disco ocorrer num conjunto de discos que não tenha a protecção por replicação, será enviado o SRC A6xx 0266 quando esse conjunto de discos for acedido por qualquer trabalho do sistema. Como as unidades de memória do conjunto de discos não têm unidades replicadas, o directório de gestão de memória torna-se inutilizável e todas as operações de input e output para o conjunto de discos são suspensas.

O SRC de atenção do disco não significa que o sistema tenha terminado. Todas as operações de input e output são colocadas na fila, de modo a permitir que o técnico dos serviços de assistência investigue a causa da falha do disco. Se o problema não estiver relacionado com os suportes do disco, as placas em falha serão substituídas, a unidade em falha é ligada e o sistema continua a partir do ponto em que ocorreu o erro do equipamento. São retomadas todas as operações de input e output colocadas na fila. No entanto, se tiver ocorrido uma falha num suporte do disco, o técnico dos serviços de assistência executará uma cópia de memória principal para minimizar o tempo do IPL seguinte para o OS/400® e permitirá que o sistema termine o processamento.

Com a protecção por replicação total, o funcionamento do sistema não é interrompido enquanto os diagnósticos e a maioria das reparações para resolver o problema da falha do subsistema de disco estiverem em curso. Com a protecção de nível de processador de I/O, é possível executar a manutenção máxima simultânea, de acordo com o erro. Em qualquer dos casos, o utilizador dispõe de controlo total sobre o encerramento do sistema, no caso de ser necessária uma desligação para resolver o problema do disco; o sistema não terminará anormalmente.

Embora os dados críticos sejam protegidos pela protecção por replicação parcial e não seja necessária uma operação de restauro para os dados no conjunto de discos protegido, o utilizador não dispõe da máxima disponibilidade que é fornecida pela protecção por replicação total, uma vez que o conjunto de discos não protegido fica exposto. Se os seus requisitos de disponibilidade indicarem que o seu sistema terá de estar em execução nos minutos a seguir a uma falha ou permanecer activo durante as horas de expediente, a protecção por replicação parcial não é uma opção, na maioria dos casos.

Como o sistema gere a memória auxiliar

Para compreender a opção de disponibilidade no servidor, é necessário compreender os conceitos básicos da gestão da memória do disco pelo seu servidor iSeries. No servidor, a memória mais importante denomina-se **memória principal**. A memória em disco denomina-se **memória auxiliar**. Também poderá ser designada como **DASD (dispositivo de memória de acesso directo)**.

Muitos outros sistemas de computadores requerem que se responsabilize pela forma como as informações são guardadas em discos. Quando cria um novo ficheiro, tem de indicar ao sistema onde deverá colocar o ficheiro e que tamanho deverá ter. Tem de equilibrar os ficheiros pelas diferentes unidades de discos de modo a obter um bom rendimento do sistema. Se descobrir posteriormente que um ficheiro tem de ser maior, será necessário copiá-lo para uma localização do disco que tenha espaço suficiente para o novo ficheiro maior. Poderá ter de mover ficheiros entre unidades de discos para manter o rendimento do sistema.

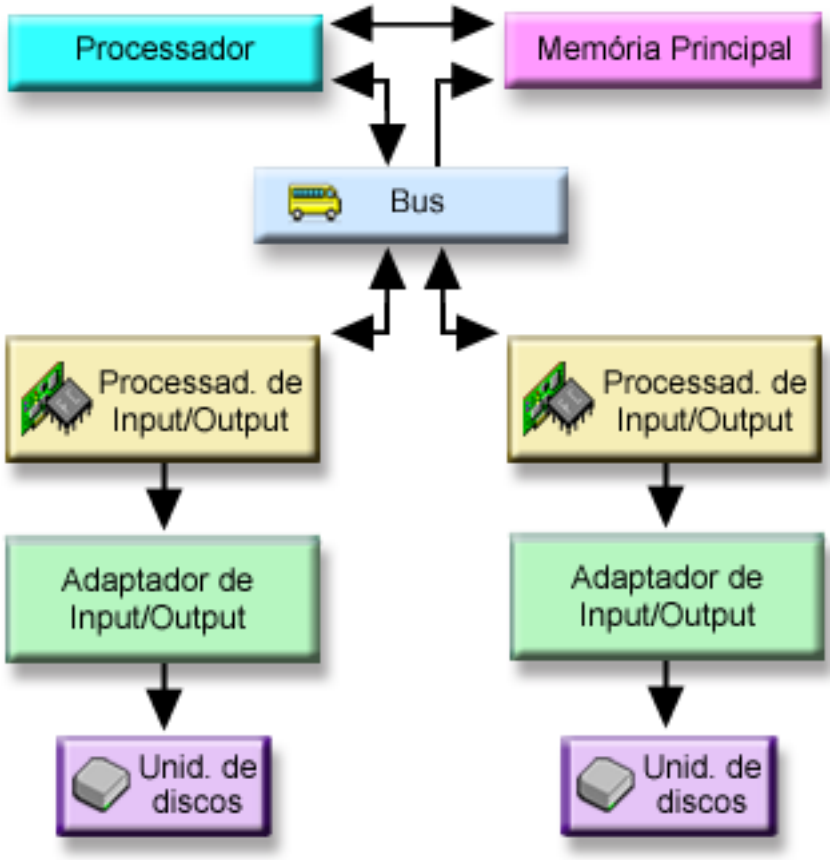
O servidor iSeries é diferente no sentido em que assume a responsabilidade de gestão das informações na memória auxiliar. Quando cria um ficheiro, faz uma estimativa do número de registos que ele deverá ter. O sistema coloca o ficheiro na melhor localização, para obter um bom rendimento. De facto, poderá distribuir os dados do ficheiro por múltiplas unidades de discos. Quando adicionar mais registos ao ficheiro, o sistema atribui espaço adicional numa ou mais unidades de discos.

A **memória de nível único** é a arquitectura exclusiva do servidor iSeries que permite que a memória principal e a memória auxiliar funcionem em conjunto com precisão e eficiência. Com a memória de nível único, os programas e os utilizadores do sistema pedem os dados pelo nome e não pela localização física dos mesmos. O sistema detém o controlo da localização da cópia mais actual de qualquer informação na memória principal ou na memória auxiliar.

Como os discos estão configurados

O sistema utiliza vários componentes electrónicos para gerir a transferência de dados de um disco para a memória principal. Os dados e os programas têm de se encontrar na memória principal antes de poderem

ser utilizados. Esta figura mostra o hardware que é utilizado para a transferência de dados:



Bus: O bus é o canal de comunicações principal para a transferência de dados de input e output. Um sistema pode ter um ou mais buses.

Processador de I/O: O processador de input/output (IOP) está ligado ao bus. O IOP é utilizado para transferir informações entre a memória principal e grupos específicos de controladores. Alguns IOPs são dedicados a tipos de controladores específicos, como, por exemplo, controladores de discos. Outros IOPs podem ter mais do que um tipo de controlador ligado; por exemplo, controladores de banda e controladores de disco.

Adaptador de input-output (IOA): O IOA é ligado ao IOP e trata a transferência de informações entre o IOP e as unidades de discos.

Unidade de discos: As unidades de discos são os dispositivos reais que contêm as unidades de memória. O hardware é encomendado ao nível de unidade de discos. Cada unidade de discos tem um número de série único. Estão disponíveis informações adicionais sobre como o servidor endereça unidades de memória individuais.

Como o Sistema Endereça Unidades de Memória Individuais

Para mover dados de e para a memória auxiliar, o sistema necessita de uma forma para identificar uma única unidade de memória. Cada componente de hardware (bus, processador de I/O, controlador e unidade de memória) tem um endereço exclusivo.

O endereço de uma unidade de memória consiste no bus do sistema, placa principal do sistema, placa de sistema, bus de I/O, controlador e números de dispositivo.

```
      Detalhes de Informações de Recursos de Hardware da Unidade de Discos

Tipo ............: 6603
Modelo ..........: 030
Número de série .: 00-0109928
Nome de recurso .: DD002

Bus de SPD
 Bus do sistema .:   1
 Placa princ. sis:   0
 Placa do sistema:   1

Memória
 Bus de I/O .....:   0
 Controlador ....:   1
 Dispositivo ....:   0
```

Protecção total—conjunto de discos único

Uma forma mais simples de gerir e proteger a sua memória auxiliar é executar o seguinte procedimento:

- Atribua todas as unidades de discos a um único conjunto de discos (o conjunto de discos do sistema).
- Utilizar protecção por paridade de dispositivos para todas as unidades de discos que suportam hardware.
- Utilizar protecção por replicação para as unidades de discos restantes no sistema.

Com este método, o seu sistema continuará em funcionamento se uma única unidade de discos falhar. Quando a unidade em falha for substituída, o sistema reconstrói as informações de modo a não se perderem dados. O sistema também poderá continuar a funcionar quando um componente de hardware relacionado com o disco falhar. O facto de o sistema continuar ou não a funcionar depende da configuração. Por exemplo, o sistema continuará a funcionar se um IOP falhar e todas as unidades de discos ligadas tiverem pares replicados que estejam ligados a um IOP diferente.

Quando utiliza uma combinação de protecção por replicação e protecção por paridade de dispositivos para proteger totalmente o sistema, aumenta os requisitos da capacidade do disco. A Protecção por paridade de dispositivos requer até 25% do espaço nas unidades de discos para armazenar informações de paridade. A Protecção por replicação duplica o requisito de disco para todos os discos que não têm capacidade para a protecção por paridade de dispositivos.

Protecção total—conjuntos de discos múltiplos

Pode desejar dividir as unidades de discos em vários conjuntos de discos(conjuntos de memória auxiliar). Por vezes, o rendimento geral do sistema pode melhorar se tiver conjuntos de discos do utilizador. Por exemplo, pode isolar receptores de diário num conjunto de discos base ou secundário. Também pode colocar ficheiros do histórico ou documentos que são raramente alterados num conjunto de discos que tenha unidades de discos de rendimento inferior.

Pode proteger totalmente um sistema com conjuntos de discos múltiplos executando a seguinte operação:

- Utilizar protecção por paridade de dispositivos para todas as unidades de discos que suportam hardware.
- Configurar a protecção por replicação para todos os conjuntos de discos no sistema. Pode configurar a protecção por replicação mesmo para um conjunto de discos que só tenha unidades de discos com a protecção por paridade de dispositivos. Deste modo, se adicionar no futuro unidades que não tenham a protecção por paridade de dispositivos, essas unidades serão automaticamente replicadas.

  Nota: Para a protecção por replicação, tem de adicionar novas unidades em pares de unidades de igual capacidade.

Antes de configurar este nível de protecção, assegure-se de que sabe como atribuir unidades de discos a conjuntos de discos.

Protecção parcial—múltiplos conjuntos de discos

Por vezes, a protecção total (utilizando uma combinação de protecção por paridade de dispositivos e protecção por replicação) pode tornar-se demasiado dispendiosa. Se isto acontecer, terá de desenvolver uma estratégia para proteger as informações críticas no seu sistema. Os seus objectivos deverão ser minimizar a perda de dados e reduzir o tempo durante o qual as aplicações críticas não estão disponíveis. Provavelmente, a sua estratégia envolverá a divisão do sistema em conjuntos de discos básicos e independentes e a protecção de apenas determinados conjuntos de discos. Note, no entanto, que, se o sistema não for totalmente protegido e uma unidade de discos não protegida falhar, poderão ocorrer graves problemas. Todo o sistema poderá ficar inutilizável, terminar anormalmente, requerer uma longa recuperação e os dados do conjunto de discos que contém a unidade com falha terão de ser restaurados.

Antes de configurar este nível de protecção, assegure-se de que sabe como atribuir unidades de discos a conjuntos de discos.

A lista que se segue tem sugestões para desenvolver a sua estratégia:

- Se proteger o conjunto de discos do sistema com uma combinação de protecção por replicação e protecção por paridade de dispositivos, poderá reduzir ou eliminar o tempo de recuperação. O conjunto de discos de sistema e, particularmente, a unidade origem de carregamento, contêm informações que são críticas para manter o seu sistema operacional. Por exemplo, o conjunto de discos do sistema tem informações sobre segurança, informações sobre configuração e endereços para todas as bibliotecas do sistema.
- Considere como poderá recuperar informações sobre objectos. Se tiver aplicações online e os seus objectos forem constantemente alterados, considere o registo em diário e a colocação de receptores de diário num conjunto de discos de utilizador protegido.
- Pense no tipo de informações que não necessitam de protecção, provavelmente, porque não mudam frequentemente. Por exemplo, os ficheiros do histórico podem ter de estar online para consulta, mas os dados dos ficheiros do histórico podem não ser alterados, excepto no fim do mês. Poderia colocar estes ficheiros num conjunto de discos separado que não tenha qualquer protecção de disco. Se ocorrer uma falha, o sistema ficará inutilizável, mas os ficheiros poderão ser restaurados sem perda de dados. O mesmo se aplica a documentos.
- Considere outras informações que podem não necessitar de protecção do disco. Por exemplo, os seus programas de aplicação podem estar numa biblioteca separada dos dados da aplicação. Provavelmente, os programas mudam com pouca frequência. As bibliotecas de programas podem ser colocadas num conjunto de discos básico que não esteja protegido. Se ocorrer uma falha, o sistema ficará inutilizável, mas os programas poderão ser restaurados.

Duas directrizes simples podem resumir a lista anterior:

1. Para reduzir o tempo de recuperação, proteja o conjunto de discos do sistema.
2. Para reduzir a perda de dados, tome decisões conscientes sobre que bibliotecas e objectos deverão ser protegidos.

Atribuir unidades de discos a conjuntos de discos

Se decidir que pretende mais do que um conjunto de discos, também chamado conjunto de memória auxiliar (ASP) na interface baseada em caracteres, terá de determinar o seguinte para cada conjunto de discos:

- A quantidade de memória de que necessita.
- Qual a protecção do disco a utilizar, se desejar alguma.
- Quais as unidades de discos a atribuir.

- Quais os objectos a colocar no conjunto de discos.

O manual Workstation Customization Programming  fornece informações para ajudá-lo com estas decisões.

Quando trabalhar com a configuração do disco, poderá considerar útil começar por imprimir a configuração de sistema actual. Poderá obter estas informações a partir do Gestor de Serviços de Hardware das ferramentas de serviço do sistema (SST) ou do arquivador Unidades de Discos do iSeries Navigator.