



@server

iSeries

Roadmap de disponibilidade para o seu  
servidor iSeries







@server

iSeries

Roadmap de disponibilidade para o seu  
servidor iSeries



# Índice

<b>Roadmap de disponibilidade para o seu servidor iSeries . . . . .</b>	<b>1</b>
Conceitos de disponibilidade . . . . .	2
Estimar o valor da disponibilidade . . . . .	3
Decidir qual o nível de disponibilidade de que necessita . . . . .	4
Evitar cortes de energia não planeados . . . . .	6
Evitar cortes de energia não planeados: Preparar para falhas do disco . . . . .	6
Evitar cortes de energia não planeados: Planear a perda de energia . . . . .	7
Evitar cortes de energia não planeados: Utilizar práticas de gestão de sistemas eficazes . . . . .	8
Evitar cortes de energia não planeados: Preparar espaço para o seu servidor . . . . .	9
Reduzir cortes de energia não planeados . . . . .	9
Reduzir cortes de energia não planeados: Reduzir o tempo de reinício do servidor . . . . .	10
Reduzir cortes de energia não planeados: Recuperar alterações recentes após um corte de energia não planeado . . . . .	10
Cortes de energia não planeados: Recuperar dados perdidos após um corte de energia não planeado . . . . .	11
Reduzir cortes de energia planeados . . . . .	13
Reduzir cortes de energia planeados: Reduzir janelas de cópia de segurança . . . . .	13
Reduzir cortes de energia planeados: Reduzir janelas de manutenção e actualização de software . . . . .	16
Reduzir cortes de energia planeados: Janelas de manutenção e de actualização de hardware . . . . .	17
Disponibilidade para vários sistemas: Conjuntos de unidades . . . . .	18
Programas de alta disponibilidade . . . . .	18
Informações relacionadas com o roadmap de disponibilidade . . . . .	19



---

# Roadmap de disponibilidade para o seu servidor iSeries

No ambiente ultra-rápido da Internet dos nossos dias, é crucial que os seus dados e aplicações estejam disponíveis para o utilizador quando este necessita deles. Se os clientes não conseguirem aceder ao seu site da Web porque o servidor está em baixo, provavelmente vão dirigir-se à concorrência.

A **Disponibilidade** é a medida da frequência com que os seus dados e aplicações estão prontos para aceder a eles sempre que necessitar. Empresas diferentes têm necessidades de disponibilidade diferentes. Servidores diferentes na mesma empresa podem ter necessidades de disponibilidade diferentes. O objectivo deste tópico é guiá-lo através do mundo da disponibilidade do iSeries e ajudá-lo a decidir quais as ferramentas de disponibilidade que são adequadas para a sua empresa. É importante reparar que a disponibilidade exige um planeamento detalhado; estas ferramentas de disponibilidade são apenas úteis caso as tenha implementado **antes** de ocorrer um corte de energia.

Antes de poder iniciar realmente o planeamento da disponibilidade no seu sistema, existem algumas coisas que tem de compreender. Leia o seguinte para obter mais informações:

## **Conceitos de disponibilidade**

Este tópico contém definições dos termos de disponibilidade utilizados através do tópico.

## **Estimar o valor da disponibilidade**

Este tópico ajuda-o a avaliar quanto poderia custar um corte de energia à sua empresa.

## **Decidir qual o nível de disponibilidade de que necessita**

Este tópico ajuda-o a decidir qual o nível de disponibilidade que é necessário para a sua empresa.

Uma vez que tenha um entendimento básico dos conceitos de disponibilidade e saiba qual o nível de disponibilidade de que necessita, pode iniciar o planeamento para esse nível de disponibilidade no seu servidor. Existem várias formas diferentes de abordar a disponibilidade, com base na sua configuração e nos tipos de cortes de energia que está a antecipar, da seguinte forma:

## **Soluções de disponibilidade para um único servidor**

O iSeries tem um registo incrível no que diz respeito a confiança. No entanto, se tiver grandes necessidades de disponibilidade para o seu servidor, existem algumas ferramentas que pode utilizar para assegurar que vai de encontro aos seus objectivos de disponibilidade.

### **Evitar cortes de energia não planeados**

Este tópico descreve como deve evitar os cortes de energia não planeados sobre os quais tem algum controlo e como se deve preparar para os que não pode controlar.

### **Reduzir cortes de energia não planeados**

Este tópico descreve o que pode fazer para assegurar que os cortes de energia não planeados, caso ocorram, são o mais curtos possível.

### **Reduzir cortes de energia planeados**

Este tópico descreve como pode reduzir os cortes de energia planeados que o utilizador controla.

## **Soluções de disponibilidade utilizando vários servidores**

Caso necessite de um nível de disponibilidade que é superior ao que pode alcançar com um único servidor, deve considerar os conjuntos de unidades. Consulte o seguinte para obter mais informações sobre conjuntos de unidades:

## Disponibilidade para vários servidores: Conjuntos de unidades

Este tópico descreve como os conjuntos de unidade podem ajudar a fornecer aproximadamente 100 por cento de disponibilidade para as suas aplicações e dados críticos.

Para obter informações detalhadas sobre a disponibilidade e as ferramentas de disponibilidade mencionadas neste tópico, consulte Informações relacionadas.

---

## Conceitos de disponibilidade

Antes de poder planejar a disponibilidade do seu servidor iSeries, é importante que o utilizador compreenda alguns conceitos associados a este tópico.

A disponibilidade é medida em termos de **cortes de energia**, que são períodos de tempo em que o servidor não está disponível para os utilizadores. Durante um **corte de energia planeado** (também intitulado um corte de energia programado), o utilizador indisponibiliza deliberadamente o seu sistema aos utilizadores. O utilizador pode utilizar um corte de energia programado para executar trabalho batch, realizar uma cópia de segurança do seu sistema ou aplicar correcções.

Um **corte de energia não planeado** (também intitulado corte de energia não programado) é normalmente originado por uma falha. O utilizador pode recuperar de alguns cortes de energia não planeados (como por exemplo a falha do disco, falha do sistema, falha de energia, falha do programa ou erro humano) caso tenha uma estratégia de cópia de segurança adequada. No entanto, um corte de energia não planeado que origina uma perda total do sistema, como por exemplo um tornado ou um incêndio, exige que o utilizador tenha a postos um plano detalhado de recuperação em caso de acidente para poder recuperar.

A sua **janela de cópia de segurança** é o período de tempo que o seu servidor pode estar indisponível para utilizadores enquanto o utilizador executa as suas operações de cópia de segurança. A sua janela de cópia de segurança é um corte de energia programado que normalmente ocorre durante a noite ou num fim de semana quando o seu servidor tem menos tráfego.

Existem vários níveis de disponibilidade. Estes níveis diferem no tipo e duração dos cortes de energia que podem tolerar. Estes níveis são os que se seguem:

- **Altamente disponível.** O servidor entrega um nível de serviço aceitável ou sob acordo durante o seu período programado da operação. O objectivo é ter o servidor disponível quando o cliente necessitar dele.
- **Alta disponibilidade.** O servidor entrega um nível de serviço aceitável ou sob acordo durante o seu período programado da operação. O objectivo é não ter cortes de energia não planeados; poderão existir alguns cortes de energia planeados.
- **Operações contínuas.** O servidor entrega um nível de serviço aceitável ou sob acordo de 24 horas por dia, 365 dias por ano. O objectivo é que o servidor possa funcionar sem cortes de energia planeados; poderão existir alguns cortes de energia não planeados.
- **Disponibilidade contínua.** O servidor entrega um nível de serviço aceitável ou sob acordo de 24 horas por dia, 365 dias por ano. O objectivo é não ter cortes de energia planeados ou não planeados.

O diagrama seguinte demonstra como estes níveis diferentes de disponibilidade se relacionam uns com os outros e quais os tipos de negócios que se adequam a cada nível.





\*

Para obter mais informações sobre estes conceitos e de como se adequam entre si, consulte os tópicos em Informações relacionadas.

## Estimar o valor da disponibilidade

Ninguém duvida da importância da disponibilidade. No entanto, quando são questionadas para justificar o custo de hardware adicional para suportar a disponibilidade melhorada, muitas pessoas não sabem argumentar. Os passos seguintes descrevem como devem estimar o valor dos seus serviços de informação:

1. **Desenvolver uma lista dos serviços mais importantes que o seu servidor fornece.** O seu servidor existe para que os utilizadores finais possam levar tarefas a cabo. Para calcular correctamente o valor do seu servidor para a organização, tem de identificar o que é que o servidor ajuda os utilizadores a fazer.
2. **Calcular os custos que tem quando estes serviços estão indisponíveis.** Cada aplicação ou serviço tem um efeito nos que utilizam o servidor. O utilizador tem de determinar quais os utilizadores que são afectados e como são afectados.
3. **Comparar custos directos com custos indirectos.** Os custos directos são perdas que podem ser rastreadas directamente para um servidor que está a ficar indisponível. Os custos indirectos são os que incorrem por outro departamento ou função como resultado de um corte de energia.
4. **Comparar custos tangíveis com custos intangíveis.** Os custos tangíveis são os que podem ser medidos em moeda. No entanto, existem outros custos que não se reflectem em dinheiro, como por exemplo o mercado de acções, a perda de oportunidades e a boa vontade.

5. **Analisar custos fixos versus custos variáveis.** Os custos fixos são os que resultam de uma falha e são os mesmos, independentemente da duração do corte de energia. Os custos variáveis são os que variam, com base na duração do corte de energia.

Para obter ajuda no cálculo dos custos que vai ter no tempo em baixo, pode utilizar IT Cost of Downtime Calculator



Outra referência que pode ajudar é *So you want to estimate the value of availability?* (GG22-9318). Pode encomendar esta publicação através de IBM Publications Center



---

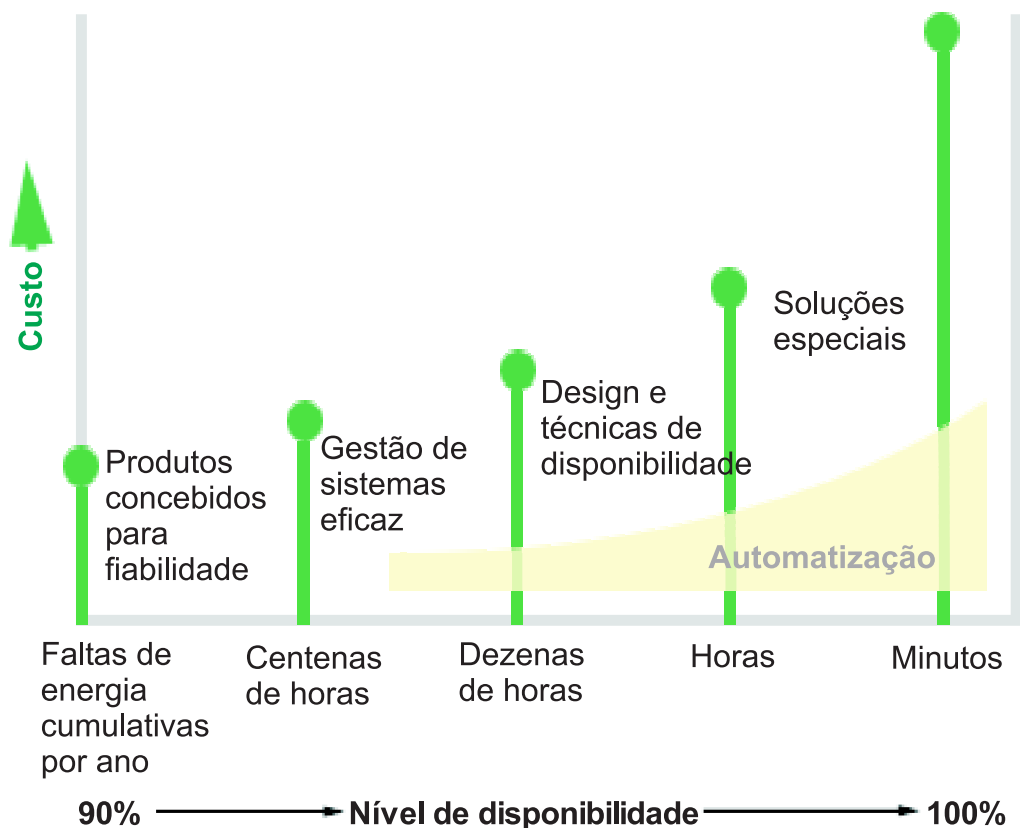
## Decidir qual o nível de disponibilidade de que necessita

Agora que compreende alguns dos conceitos por trás da disponibilidade e que já descobriu a quantidade de tempo em baixo que lhe irá custar, também deve ter em conta que a disponibilidade tem um preço. Quanto maior for o nível de disponibilidade de que necessita, mais alto será esse preço. Deste modo, o utilizador pretende certificar-se de que analisou as necessidades da sua empresa exaustivamente, de forma a poder decidir qual o nível de disponibilidade que tem possibilidades de manter.

Para decidir qual o nível de disponibilidade de que necessita, considere as questões seguintes:

### Tem aplicações que exigem 100% de disponibilidade?

Na maioria dos casos, pode atingir um alto nível de disponibilidade através da implementação de processos sonoros e práticas de gestão de sistemas. Quanto mais perto tiver de estar da disponibilidade contínua, maior será o investimento que terá de fazer. Antes de fazer qualquer tipo de investimento, o utilizador deve certificar-se de que exige esse nível de disponibilidade. A figura seguinte demonstra como várias técnicas podem melhorar a disponibilidade, podendo aumentar o preço que o utilizador terá de despende por ela.



\*

### Quanto tempo em baixo considera aceitável?

Poderá ajudá-lo saber qual a quantidade de tempo em baixo que cada nível de disponibilidade representa. A tabela seguinte demonstra a quantidade de tempo em baixo que deve esperar para diferentes níveis de disponibilidade.

Nível de disponibilidade	Tempo em baixo por ano
90%	36.5 dias
95%	18.25 dias
99%	3.65 dias
99.9%	8.76 horas

Aliado à percepção do tempo em baixo que considera aceitável, o utilizador tem de considerar como pode ocorrer esse tempo em baixo. Por exemplo, pode pensar que 99% de disponibilidade é aceitável caso o tempo em baixo seja uma série de pequenos cortes de energia que são distribuídos ao longo de um ano. No entanto, poderá pensar de modo diferente sobre os 99% de disponibilidade caso o tempo em baixo tenha sido na verdade um único corte de energia que durou 3.65 dias.

### Qual o nível de acesso de que os clientes necessitam para a sua empresa?

Antigamente os clientes entravam na sua empresa das 9 a.m. às 5 p.m., logo era realista esperar que o seu servidor só tivesse de estar disponível durante essas horas. No entanto, a Internet mudou a

expectativa; os clientes podem esperar aceder ao site da Web da sua empresa a qualquer hora do dia ou da noite. O utilizador tem de determinar quais são as expectativas dos seus clientes e o que é realista no que diz respeito a essas expectativas, à medida que determina qual o nível de disponibilidade que irá manter.

---

## Evitar cortes de energia não planeados

Uma forma de abordar a disponibilidade é tentar evitar os cortes de energia não planeados. Este tópico descreve métodos diferentes que pode utilizar para assegurar que o seu servidor sofre menos tempo em baixo não planeado possível.

Para evitar cortes de energia não planeados, deve fazer o seguinte:

### **Preparar para falhas do disco**

A falha do disco é rara, mas é algo para o qual pode estar preparado. Este tópico descreve como pode fazer isso.

### **Planear a perda de dados**

A perda de dados é algo que não é planeado nem evitável, mas o utilizador pode preparar-se para quando acontecer. Este tópico descreve como pode fazer isso.

### **Utilizar práticas de gestão do sistema eficazes**

Este tópico descreve como a supervisão do rendimento do sistema e a gestão das operações do sistema podem contribuir para uma melhor disponibilidade global.

### **Preparar espaço para o seu servidor**

O espaço físico onde o servidor reside tem de ser preparado cuidadosamente para assegurar que as condições promovem uma óptima disponibilidade. Este tópico descreve como deveriam ser as condições físicas para o seu servidor.

Se tiver um único servidor e não poder alcançar o nível de disponibilidade de que necessita com estas estratégias, pode querer considerar os conjuntos de unidades. Para obter mais informações, consulte Disponibilidade para vários servidores: Conjuntos de unidades.

## Evitar cortes de energia não planeados: Preparar para falhas do disco

A memória em disco é a memória que ou é interna do servidor iSeries ou está anexada a ele. O espaço em disco, aliado à memória principal do seu servidor, é encarada pelo servidor como uma grande área de memória. Quando guardar um ficheiro, não tem de o atribuir à localização de uma memória; em vez disso, o servidor coloca o ficheiro na localização que assegura o melhor rendimento. Pode espalhar os dados no ficheiro em várias unidades de disco, caso seja esta a melhor opção. Quando adicionar mais registos ao ficheiro, o sistema atribui espaço adicional a uma ou mais unidades de disco. Esta forma de endereçar memória é conhecida como **memória de nível único**.

Visto que os seus dados estão espalhados pelos seus discos, é importante que considere como deve proteger os dados no caso de um desses discos falhar. O objectivo deste tópico é descrever os métodos que pode utilizar para proteger os seus discos. Para obter informações adicionais sobre os métodos aqui descritos, consulte Protecção de discos.

### **Protecção de paridade dos dispositivos**

A protecção de paridade dos dispositivos permite ao seu servidor continuar a funcionar quando um disco falha ou é danificado. Quando utilizar a protecção de paridade dos dispositivos, o adaptador de entrada/saída (IOA) calcula e guarda um valor de paridade para cada bit de dados. O IOA informatiza o valor de paridade a partir dos dados na mesma localização em cada uma das outras unidades de disco, no conjunto de paridade dos dispositivos. Quando ocorre uma falha no disco, os dados podem ser

reconstruídos através da utilização do valor de paridade e dos valores dos bits nas mesmas localizações nos outros discos. O seu servidor prossegue a execução enquanto que os dados estão a ser reconstruídos.

Para obter detalhes sobre a protecção de paridade dos dispositivos, consulte Protecção de paridade dos dispositivos.

### **Protecção replicada**

A protecção replicada é uma forma de proteger os seus dados no caso de uma falha do disco. Os dados são protegidos porque o sistema mantém duas cópias dos dados em duas unidades de disco separadas. Quando um componente relacionado com um disco falhar, o sistema pode continuar a funcionar sem interrupções, utilizando a cópia exacta dos dados até que o componente danificado seja reparado.

São possíveis níveis diferentes da protecção replicada, dependendo do hardware que seja duplicado. O utilizador pode duplicar:

- Unidades de disco
- Controladores de disco
- Unidade de bus de E/S
- Processadores de E/S de disco
- Um bus

para obter detalhes sobre a protecção replicada, incluindo como funciona e como deve ser planeada, consulte Protecção replicada.

### **Conjuntos de unidades independentes**

Os conjuntos de unidades independentes (também denominados conjuntos de memória auxiliar independentes) permitem-lhe evitar cortes de energia não planeados, visto que os dados que contêm estão isolados do resto do seu servidor. Se um conjunto de discos independentes falhar, o seu servidor pode prosseguir com o funcionamento. Para obter informações detalhadas sobre a utilização dos conjuntos de discos independentes, consulte Conjuntos de discos independentes.

## **Evitar cortes de energia não planeados: Planear a perda de energia**

Para se assegurar de que o seu servidor está disponível quando necessitar dele, tem de se certificar de que tem uma fonte de alimentação adequada e de que está protegido no caso de haver uma perda de energia.

### **Requisitos de energia**

Parte do processo de planeamento para o seu servidor é certificar-se de que tem uma fonte de alimentação adequada. O utilizador tem de compreender os requisitos do seu servidor e em seguida solicitar a ajuda de um electricista qualificado para ajudar a instalar as ligações adequadas. Para obter detalhes sobre como deve certificar-se de que o seu servidor tem a energia adequada, consulte Determinar os seus requisitos de energia.

### **Baterias de segurança**

Alguns servidores iSeries vêm com baterias de segurança. A sua unidade de bateria de segurança fornece 30 segundos de tempo de execução. Se a energia não for restaurada dentro de 30 segundos, o sistema entra imediatamente num encerramento controlado.

### **Fontes de alimentação redundantes**

Alguns servidores iSeries estão disponíveis com fontes de alimentação redundantes. Uma fonte de alimentação redundante é uma função que evita um corte de energia não planeado através do fornecimento de energia caso uma fonte de alimentação falhe.

### Fontes de alimentação ininterruptíveis

Mesmo quando tiver uma fonte de alimentação adequada, por vezes acontecem perdas de energia, como por exemplo, durante uma tempestade. Para evitar cortes de energia não planeados que resultem na perda de energia, o utilizador pode necessitar de investir num hardware concebido especificamente para manter o seu servidor a trabalhar quando se perde energia. Um desses aparelhos de hardware é uma **fonte de alimentação ininterruptível (UPS)**. Pode utilizar uma UPS para fornecer energia auxiliar ao seu processador, discos, consola do sistema e a quaisquer outros dispositivos que ache necessário. As fontes de alimentação ininterruptíveis fornecem as seguintes vantagens:

- Deixa-o prosseguir com as operações durante breves cortes de energia (apagões).
- Protege o servidor de picos de voltagem (descargas).
- Fornece uma conclusão normal de operações, que pode reduzir o seu tempo de recuperação quando reiniciar o servidor. Para obter informações sobre como escrever um programa que o irá ajudar a controlar o encerramento do seu servidor nestas condições, consulte Controlar o encerramento do servidor através de um programa de manuseamento da energia.

Para obter informações sobre em que situações as fontes de alimentação ininterruptíveis são compatíveis com o servidor iSeries, consulte Sistemas de fontes de alimentação ininterruptíveis.

### Energia de gerador

Se pensa que pode acontecer-lhe uma falha de energia prolongada, talvez deva considerar a aquisição de um gerador. Um gerador vai mais além do que uma UPS, no sentido de que lhe permite continuar as operações normais durante longas falhas de energia.

Caso necessite de ajuda a planear as necessidades de energia do servidor iSeries, consulte Power Protection Services



## Evitar cortes de energia não planeados: Utilizar práticas de gestão de sistemas eficazes

Uma das formas mais simples de evitar cortes de energia não planeados é assegurar que está a fazer os possíveis para manter o servidor a executar normalmente. Isto inclui a execução de tarefas preventivas de gestão de manutenção e de sistemas que ajudam o servidor a executar no seu pico. Muitas destas tarefas de gestão de sistemas podem ser automatizadas, o que ajuda o utilizador a evitar falhas que podem ocorrer devido a erro humano ou negligência.

Uma forma de poder ajudar a assegurar a disponibilidade do seu servidor é supervisionar o seu rendimento e reagir prontamente a quaisquer problemas que encontrar. Pode utilizar as funções de Serviços de Recolha e funções de supervisores na Central de Gestão para supervisionar de forma activa e rastrear o rendimento do seu servidor. Pode ser notificado dos problemas que coloquem em risco a capacidade do seu servidor a tempo de reagir e evitar um corte de energia não planeado. Para obter mais informações sobre como planear e gerir o rendimento do seu servidor, consulte Rendimento.

As correcções também são um componente importante de gestão de sistemas que podem ajudá-lo a manter o servidor disponível. Quando se descobrem problemas nos programas iSeries, a IBM emite uma **correção** também conhecida como PTF, ou correcção temporária de programa) para corrigir o problema. Tem de estar atento às correcções e instalá-las no seu servidor para assegurar que o servidor está a

funcionar ao seu melhor nível. O utilizador deveria criar uma estratégia de gestão de correcções e verificar e aplicar correcções como parte da manutenção de rotina do seu servidor. Para obter mais informações sobre como obter e aplicar correcções, consulte Utilizar correcções de software. Para obter ajuda na determinação de uma estratégia para a manutenção preventiva baseada no ambiente e nas aplicações do iSeries, tente em Fix Maintenance Advisor



## Evitar cortes de energia não planeados: Preparar espaço para o seu servidor

Uma forma de evitar os cortes de energia não planeados é assegurar que o espaço onde colocou o servidor promove a disponibilidade. Muitos factores físicos e ambientais contribuem para a forma como o servidor é executado.

A primeira coisa a fazer é familiarizar-se com o seu servidor. Modelos diferentes têm requisitos diferentes relativamente às condições em que estão inseridos, por isso deve ter em conta as necessidades do seu servidor. Para obter mais informações sobre as características físicas de cada modelo, consulte Especificações do servidor. Para obter informações sobre as características físicas do hardware que o utilizador pode anexar ao servidor, consulte Folhas de especificação do hardware.

Uma vez que esteja familiarizado com as características físicas do seu servidor, certifique-se que considera o seguinte sobre o espaço em que ele reside:

- **Localização.** A localização física do servidor pode ter um impacto na sua disponibilidade. Por exemplo, se a sala não estiver protegida, o servidor pode estar vulnerável a vandalismo ou até mesmo a alguém desligar acidentalmente o servidor da tomada. Para obter mais detalhes sobre as precauções a tomar relativamente à localização do servidor, consulte Considerações de localização.
- **Cabos.** Os cabos são frequentemente negligenciados, mas sem eles o servidor seria inútil. O utilizador tem de se certificar de que os cabos estão em boas condições e de que estão a ser utilizados correctamente. Para obter mais informações sobre como assegurar que os seus cabos cumprem a função que lhes compete, consulte Considerações gerais sobre cablagem.
- **Ambiente.** O ambiente que fornece ao seu servidor também é crucial para a disponibilidade. O ambiente inclui a temperatura, humidade e outros factores que podem inibir o rendimento do servidor. Para obter informações mais detalhadas sobre o ambiente que tem de fornecer ao servidor, consulte Referência do ambiente.

---

## Reduzir cortes de energia não planeados

Os cortes de energia não planeados ocorrem mesmo e a chave para a disponibilidade é assegurar que quando ocorrem, o utilizador pode recuperar deles o mais rapidamente possível. O objectivo de todas as estratégias de recuperação é voltar ao ponto em que ficou antes de ocorrer o corte de energia.

Os tópicos seguintes descrevem quais as ferramentas de disponibilidade o irão ajudar a reiniciar o servidor e a recuperar dados o mais rapidamente possível após ocorrer um corte de energia:

### Reiniciar o servidor

Este tópico descreve as ferramentas de disponibilidade que pode utilizar para assegurar que o seu servidor reinicia o mais rapidamente possível após um corte de energia.

### Recuperar alterações recentes

Este tópico descreve as ferramentas de disponibilidade que pode utilizar para recuperar de um corte de energia, quando perde apenas as alterações efectuadas imediatamente antes do corte de energia.

### **Recuperar dados perdidos**

Este tópico descreve as ferramentas de disponibilidade que pode utilizar para recuperar de um corte de energia que o leva a perder dados. A perda pode ser de alguns ficheiros ou pode ser de todo o site, como durante uma catástrofe natural.

Se tiver um único servidor e não conseguir alcançar o nível de disponibilidade de que necessita através destas estratégias, pode querer considerar os conjuntos de unidades. Para obter mais informações, consulte Disponibilidade para vários servidores: Conjuntos de unidades.

## **Reduzir cortes de energia não planeados: Reduzir o tempo de reinício do servidor**

Antes do servidor se desligar, vai executar certas actividades para assegurar que os seus dados estão protegidos e que os trabalhos estão terminados de forma controlada. Quando experimentar um corte de energia não planeado, o seu servidor não pode executar estas actividades. Para obter mais detalhes sobre o que acontece quando o seu servidor termina de forma anómala, consulte Iniciar e parar o iSeries.

O objectivo deste tópico é descrever algumas ferramentas de disponibilidade que irão ajudar o servidor a reiniciar o mais rápido possível.

### **Protecção do caminho de acesso gerido pelo sistema (SMAPP)**

Um **caminho de acesso** é o caminho que uma aplicação toma através de um ficheiro de base de dados para obter os registos de que necessita. Um ficheiro pode ter vários caminhos de acesso, caso programas diferentes necessitem de ver os registos em sequências diferentes. Quando o seu servidor termina de forma anómala, como por exemplo durante um corte de energia não planeado, o servidor tem de reconstruir os caminhos de acesso no início seguinte, o que pode demorar bastante tempo. Quando utilizar a protecção do caminho de acesso gerido pelo sistema, o servidor protege os caminhos de acesso de forma a que não tenham de ser reconstruídos quando o servidor iniciar após um corte de energia não planeado. Isto irá poupar-lhe tempo quando reiniciar o seu servidor, o que lhe permitiria regressar para os seus processos empresariais normais o mais rapidamente possível. Para obter informações detalhadas sobre SMAPP, consulte Protecção de caminho de acesso gerido pelo sistema.

### **Registo de alterações aos caminhos de acesso**

Tal como a SMAPP, o registo de alterações aos caminhos de acesso pode ajudá-lo a assegurar que os ficheiros e os caminhos de acesso críticos estão disponíveis o mais rapidamente possível após reiniciar o servidor. No entanto, quando utiliza a SMAPP, o *servidor decide* quais os caminhos de acesso a proteger. Deste modo, se o servidor não proteger um caminho de acesso que considere crítico, o utilizador pode atrasar-se na recolocação da sua empresa em funcionamento. Quando registar as alterações dos caminhos de acesso, *irá decidir* quais os caminhos a registar as alterações. Para obter mais informações sobre o registo de alterações dos caminhos de acesso, consulte Registo de alterações de SMAPP e caminho de acesso.

## **Reduzir cortes de energia não planeados: Recuperar alterações recentes após um corte de energia não planeado**

Após um corte de energia não planeado, o seu objectivo é voltar a colocar o servidor em funcionamento o mais rápido possível. Quer voltar ao ponto em que ficou antes de ocorrer o corte de energia, sem ter de voltar a inserir as transacções manualmente. Isto pode envolver a reconstrução de alguns dos seus dados. Existem algumas ferramentas de disponibilidade que pode utilizar para o ajudar a voltar ao ponto em que ficou antes de ocorrer o corte de energia.

### **Registo de alterações**



A gestão de diários evita que as transacções se percam caso o seu servidor termine de forma anómala. Quando registar as alterações de um objecto, o servidor mantém um registo das alterações que efectuou a esse objecto. Para obter informações detalhadas sobre a forma de planejar e utilizar o registo de alterações, consulte Gestão de diários.

### **Controlo de consolidação**

O controlo de consolidação ajuda-o a fornecer integridade de dados ao seu servidor. Permite-lhe definir e processar um grupo de alterações a recursos, como por exemplo ficheiros de bases de dados ou tabelas, como uma única transacção. Deste modo, assegura que ocorra todo o conjunto de alterações individuais ou que não ocorra nenhuma das alterações. Por exemplo, se perder energia enquanto estão a ser feitas uma série de actualizações à sua base de dados. Sem controlo de consolidação, o utilizador pode correr o risco de dados incompletos ou danificados. Sem o controlo de consolidação, as actualizações incompletas seriam retiradas da sua base de dados quando reiniciasse o servidor.

Pode utilizar o controlo de consolidação para conceber uma aplicação para que o sistema possa reiniciar a aplicação caso um trabalho, um grupo de activação num trabalho ou o sistema terminarem de forma anómala. Com o controlo de consolidação, pode ter a garantia de que quando a aplicação reiniciar, não estarão na base de dados actualizações parciais devido a transacções incompletas de uma falha anterior.

Para obter informações detalhadas sobre o planeamento e utilização do controlo de consolidação, consulte Controlo de consolidação.

### **Cortes de energia não planeados: Recuperar dados perdidos após um corte de energia não planeado**

O utilizador pode perder dados como resultado de um corte de energia não planeado, como por exemplo uma falha do disco. O exemplo mais extremo da perda de dados é a perda de todo o seu site, como exemplo do que poderia acontecer como resultado de uma inundação ou de um tornado. Existem algumas formas para evitar a perda de dados nestas situações ou pelo menos limitar a quantidade de dados que se perde.

### **Cópia de segurança e recuperação**

É imperativo que tenha uma estratégia provada de elaboração de cópias de segurança do seu servidor; o tempo e dinheiro gastos na criação desta estratégia são mais que recuperados caso necessite de restaurar a perda de dados ou executar uma recuperação. Uma vez que tenha criado uma estratégia, o utilizador deve assegurar de que funciona através de um teste, que envolve a execução de uma cópia de segurança e recuperação e em seguida a validação de que os seus dados foram copiados e restaurados correctamente. Caso altere alguma coisa no seu servidor, terá de decidir se a sua estratégia de cópia de segurança e recuperação tem de ser alterada.

cada servidor e ambiente empresarial é diferente, mas, idealmente, o utilizador deve tentar efectuar uma cópia completa do seu servidor pelo menos uma vez por semana. Caso tenha um ambiente muito dinâmico, também terá de efectuar cópias de segurança das alterações efectuadas ao seu servidor desde a última cópia de segurança. Então, se tiver um corte de energia inesperado e necessitar de recuperar esse objectos, pode recuperar a última versão deles.

Para obter orientação relativamente à forma de criação da estratégia de cópia de segurança e recuperação, consulte Planejar uma estratégia de cópia de segurança e recuperação. Para obter instruções sobre a execução de cópias de segurança no seu servidor, consulte Efectuar cópia de segurança do seu servidor. Para obter informações sobre a modo de restaurar o seu servidor, consulte Recuperar o seu servidor.

Caso pretenda uma solução para o ajudar a gerir a sua estratégia de cópia de segurança e recuperação e o seu suporte de cópia de segurança, pode utilizar Cópia de Segurança, Recuperação e Serviços de

Suporte (BRMS). **BRMS** é um programa que o ajuda a implementar uma abordagem disciplinada para gerir as suas cópias de segurança, fornecendo uma forma organizada de recuperar dados perdidos ou danificados. Ao utilizar BRMS, o utilizador pode gerir as suas cópias de segurança mais críticas e complexas, incluindo cópias de segurança activas dos servidores Lotus, de forma simples e fácil. Também pode recuperar o seu servidor totalmente em caso de um acidente ou falha.

Para além destas funções de cópia de segurança e recuperação, BRMS permitem-lhe rastrear todo o suporte de cópia de segurança desde a criação até à expiração. O utilizador já não tem de rastrear quais os artigos da cópia de segurança que estão em que volumes, ou preocupar-se com a substituição accidental de dados activos. O utilizador também pode rastrear o movimento do seu suporte para e das localizações exteriores ao site.

Para obter informações detalhadas sobre as tarefas que os BRMS podem ajudar o utilizador a executar, consulte Cópias de Segurança, Recuperação e Serviços de Suporte.

Para obter ajuda no planeamento e gestão da sua estratégia de cópia de segurança e recuperação, contacte IBM Business Continuity and Recovery Services



### Limitar a quantidade de dados perdidos

O utilizador pode agrupar as suas unidades de disco em subconjuntos lógicos denominados **conjuntos de discos** (também denominados conjuntos de memória auxiliar ou ASPs). Os dados num conjunto de discos são isolados dos dados noutros conjuntos de discos. Se uma unidade de disco falhar, o utilizador só tem de recuperar os dados que estavam armazenados no conjunto de discos de que fazia parte a unidade de disco que falhou.

Para obter informações detalhadas sobre os conjuntos de discos, tipos de conjuntos de discos e exemplos de como utilizar os conjuntos de discos com diferentes objectivos, consulte Conjuntos de discos. Para obter informações sobre a configuração de unidades de discos e conjuntos de discos, consulte Gerir conjuntos de discos.

Os **conjuntos de discos independentes** são conjuntos de discos que podem ser activados ou desactivados sem quaisquer dependências da estante memória num sistema. Isto é possível porque todas as informações associadas ao conjunto de discos independente estão contidas no conjunto de discos independente. Os conjuntos de discos independentes oferecem uma série de vantagens de disponibilidade e rendimento nos ambientes de sistemas únicos ou múltiplos. Para obter informações detalhadas, consulte Conjuntos de discos independentes.

O servidor iSeries também oferece ao utilizador a capacidade de dividir um servidor em vários servidores independentes. Esta tecnologia denomina-se **partições lógicas**. A utilização de partições lógicas é outra forma de pode isolar dados, aplicações e outros recursos. Pode utilizar partições lógicas para melhorar o rendimento do seu servidor, como por exemplo através da execução de processos batch e interactivos em partições diferentes. Também pode proteger os seus dados através da instalação de uma aplicação crítica numa partição separada de outras aplicações. Logo, se outra partição falhar, esse programa está protegido.

Enquanto que as partições lógicas têm muitas vantagens, existem também algumas desvantagens que tem que considerar. As partições lógicas podem tornar uma recuperação total de um sistema mais complicada, o que aumenta a quantidade de tempo em que o servidor está indisponível.

Para obter informações detalhadas sobre as partições lógicas e como as utilizar, consulte Partições lógicas.

---

## Reduzir cortes de energia planeados

Os cortes de energia planeados são necessários e são inesperados; no entanto, porque são planeados não significa que não tenham provoquem interrupções. Os cortes de energia planeados estão frequentemente relacionados com a manutenção do sistema. Os tópicos seguintes descrevem as formas como pode reduzir os cortes de energia que resultam de tipos de manutenções diferentes.

### Reduzir janelas de cópia de segurança

Este tópico inclui informações sobre como pode reduzir a quantidade de tempo em que o seu servidor está indisponível enquanto efectua cópias de segurança.

### Reduzir janelas de manutenção e de actualização de software

O tempo que gasta a realizar a manutenção e actualizações do software é o tempo que o seu servidor está indisponível para os seus utilizadores. Aprenda a encurtar estes períodos de tempo.

### Reduzir janelas de manutenção e actualização de hardware

O tempo que gasta a realizar a manutenção e actualizações do hardware é o tempo que o seu servidor está indisponível para os seus utilizadores. Aprenda a encurtar estes períodos de tempo.

Se tiver um único servidor e não poder alcançar o nível de disponibilidade de que necessita com estas estratégias, pode querer considerar os conjuntos de unidades. Para obter mais informações, consulte Disponibilidade para vários servidores: Conjuntos de unidades.

## Reduzir cortes de energia planeados: Reduzir janelas de cópia de segurança

Uma forma de reduzir a quantidade de tempo que o seu servidor está indisponível é reduzindo a quantidade de tempo necessária para as suas cópias de segurança: Existem várias acções que o utilizador pode tomar para reduzir a quantidade de tempo que demoram as suas cópias de segurança, incluindo o seguinte:

### Melhorar o rendimento da banda

Se estiver a utilizar a banda para as suas cópias de segurança, é lógico que possa reduzir a sua janela de cópia de segurança aumentando a velocidade em que o utilizador pode efectuar as suas cópias de segurança. Este tópico descreve as suas opções para o fazer.

### Executar cópias de segurança activas

Existem certos tipos de objectos e tipos de dados de que pode efectuar uma cópia de segurança enquanto estão em utilização, com pouca ou nenhuma interrupção das operações do servidor.

### Efectuar cópias de segurança de menos dados

O utilizador também pode reduzir a janela de cópia de segurança ao possuir menos dados para guardar quando surgir a janela do tempo. O utilizador pode efectuar cópias de segurança de alguns objectos em alturas diferentes durante a semana, o que irá reduzir o número de objectos que tem para guardar durante a sua janela.

## Reduzir janelas de cópia de segurança: Melhorar o rendimento da banda

Este artigo descreve como os clientes podem reduzir as suas janelas de cópia de segurança aumentando a velocidade e a capacidade do suporte e do hardware que utilizam.

### Hardware de alto rendimento

Uma forma de reduzir a sua janela de cópia de segurança é utilizar o hardware da banda que fornece um rendimento bastante alto. É lógico que quanto mais rápido conseguir realizar uma cópia de segurança aos dados, mais curta seja a janela de cópia de segurança. Um exemplo deste hardware de alto rendimento é o IBM TotalStorage<sup>(TM)</sup> Enterprise Tape System 3590. Para obter mais informações sobre estas unidades

de banda de alta velocidade, consulte IBM TotalStorage Enterprise Tape System 3590



Outra solução de banda que o pode ajudar a reduzir a sua janela de cópia de segurança é a Linear Tape-Open (LTO). Esta tecnologia fornece um rendimento comparável ao 3590 a um preço que concerteza é mais acessível a empresas de menores dimensões. Para obter mais detalhes sobre a LTO e sobre a forma de a utilizar com o seu iSeries, consulte Linear Tape-Open



Para obter detalhes sobre os graus de dispositivos de cópia de segurança que são suportados no seu servidor iSeries e sugestões para melhorar o rendimento, consulte Performance Capabilities Reference



### **Cópias de segurança simultâneas e em paralelo**

Outra forma de poder utilizar o hardware da banda para melhorar a velocidade das suas cópias de segurança é ter vários dispositivos a realizar cópias de segurança simultâneas e em paralelo. Estes tipos de cópias de segurança podem reduzir consideravelmente a sua janela de cópia de segurança e evitar obstáculos nas suas cópias de segurança.

Quando efectuar uma **cópia de segurança simultânea**, irá enviar vários trabalhos de salvaguarda para vários dispositivos de banda para processar ao mesmo tempo. Por exemplo, ao utilizar uma estratégia de cópia de segurança simultânea, o utilizador pode enviar uma biblioteca ou grupo de bibliotecas para um dispositivo de banda e outro conjunto de bibliotecas para um dispositivo de banda diferente. O que quer que o utilizador possa guardar em simultâneo, pode restaurar em simultâneo, reduzindo deste modo o seu tempo em baixo após uma falha do sistema através da recuperação de várias bibliotecas ou objectos ao mesmo tempo.

Quando efectua uma **cópia de segurança em paralelo**, o utilizador pode realizar cópia de segurança de artigos para dois ou mais dispositivos de uma vez. Existem dois métodos de cópias de segurança em paralelo: suporte de salvaguarda/restauro em paralelo e suporte em paralelo de várias bibliotecas. O suporte de salvaguarda/restauro em paralelo espalha cada objecto através de vários recursos. O suporte de várias bibliotecas espalha bibliotecas através de vários recursos, de forma a que cada biblioteca tenha uma cópia de segurança para um único recurso. Pode utilizar estes métodos para otimizar o rendimento dos seus dispositivos enquanto mantém os seus recursos equilibrados.

Para obter mais informações sobre cópias de segurança simultâneas e em paralelo, consulte Guardar em vários dispositivos para reduzir a sua janela de salvaguarda. O utilizador pode utilizar também a Cópia de Segurança, Recuperação e Serviços de Suporte (BRMS) para executar estes tipos de cópias de segurança.

### **Automatização**

Não surpreendentemente, a janela da cópia de segurança para a maioria das empresas ocorre durante a noite, quando os funcionários não estão a postos para executar operações de cópias de segurança. Existem algumas formas para poder automatizar os seus processos para reduzir o comprimento da sua janela de cópia de segurança e para tornar desnecessária a intervenção humana. Esta automatização reduz os custos e também ajuda a evitar a possibilidade da ocorrência de erro humano ou demora.

A Cópia de Segurança, Recuperação e Serviços de Suporte (BRMS) permitem-lhe programar operações utilizando um **programador de trabalhos**, como por exemplo o programador de trabalhos da Central de Gestão. Por exemplo, poderia programar uma cópia de segurança completa não assistida sempre aos Sábados à noite e em seguida programar tarefas de manutenção imediatamente a seguir a essa cópia de segurança. Também pode programar o movimento do seu suporte da cópia de segurança para localizações exteriores ao site e rastrear a sua localização durante o movimento.

Também pode utilizar **bibliotecas de suporte** para melhorar o processamento de cópias de segurança. Estes dispositivos contêm um grande número de volumes e facilitam muito mais as cópias de segurança automatizadas, porque alteram as bandas na unidade pelo utilizador. Não se perde tempo desnecessário na remoção e inserção de volumes, à medida que prossegue a cópia de segurança. Para obter mais informações sobre as formas de utilização da bibliotecas de banda para melhorar o processamento das cópias de segurança, consulte Gerir bibliotecas de banda.

### **Reduzir janelas de cópia de segurança: Executar cópias de segurança activas**

O utilizador pode reduzir o comprimento dos seus cortes de energia planeados guardando alguns objectos enquanto estão activos.

Este método de realizar cópias de segurança de objectos denomina-se suporte de **guardar enquanto está activo**. Guardar enquanto está activo permite-lhe executar operações de salvaguarda com uma interrupção limitada para trabalhos e subsistemas. Quando utilizar guardar enquanto está activo, os objectos ficam indisponíveis por um breve período no início do processo de cópia de segurança, até que alcançam um certo ponto, denominado ponto de controlo. Uma vez que a cópia de segurança alcance o ponto de controlo, os utilizadores podem voltar a trabalhar com esses objectos. Guardar enquanto está activo é uma operação útil caso pretenda reduzir o seu tempo de corte de energia planeado. No entanto, devia planeá-la com cautela e certificar-se de quaisquer restrições que possam afectar o seu processamento de cópias de segurança. Para obter informações detalhadas sobre guardar enquanto está activo, consulte Guardar o seu servidor enquanto está activo.

Outro método para realizar cópias de segurança de objectos enquanto estão em utilização é conhecido como uma **cópia de segurança activa**. As cópias de segurança activas são semelhantes às cópias de segurança guardar enquanto está activo, excepto que não existem pontos de controlo. Isto significa que os utilizadores podem usar os objectos durante todo o tempo em que se estiver a realizar uma cópia de segurança. Cópia de Segurança, Recuperação e Serviços de Suporte (BRMS) suporta a cópia de segurança dos servidores Lotus, bem como de Domino e QuickPlace. O utilizador pode direccionar estas cópias de segurança activas para um dispositivo de banda, biblioteca de suporte, ficheiros de salvaguarda ou um servidor Tivoli Storage Manager (TSM). Para obter informações detalhadas sobre as cópias de segurança activas do Lotus, consulte Cópia de Segurança, Recuperação e Serviços de Suporte.

**Nota:** É importante que continue a realizar cópias de segurança das informações do sistema, bem como para quaisquer cópias de segurança guardar enquanto está activo ou activas que realizar. Estas são importantes informações do sistema que não podem ter cópias de segurança através de cópias de segurança guardar enquanto está activo ou activas.

### **Reduzir janelas de cópia de segurança: Efectuar cópias de segurança de menos dados**

Este tópico descreve como pode reduzir os cortes de energia planeados ao realizar cópias de segurança de pequenas quantidades de dados em alturas diferentes. Existem algumas formas diferentes para poder isolar os dados no seu servidor para este tipo de operação. Pode utilizar Cópia de Segurança, Recuperação e Serviços de Suporte para executar todos estes tipos de cópias de segurança.

### **Cópias de segurança incrementais**

As cópias de segurança incrementais permitem-lhe guardar alterações para objectos desde a última vez que lhes foi realizada uma cópia de segurança. Existem duas formas de cópias de segurança incrementais: cumulativas e apenas de alterações. As cópias de segurança **cumulativas** guardam as

alterações efectuadas num objecto desde a última cópia de segurança total desse objecto. Isto é útil para objectos que não se alteram com frequência ou que não sofrem grandes alterações entre cópias de segurança totais. As cópias de segurança **apenas de alterações** guardam as alterações a um objecto desde a última vez que foi realizada uma cópia de segurança a esse objecto, independentemente do facto dessa cópia de segurança ter sido total ou incremental. As cópias de segurança incrementais são especialmente úteis para dados que se alteram com frequência. Por exemplo, o utilizador realiza uma cópia de segurança total sempre aos Sábados à noite. Tem algumas bibliotecas que são utilizadas extensivamente e por isso tem de lhes realizar uma cópia de segurança com mais frequência do que uma vez por semana. Pode utilizar as cópias de segurança incrementais nas outras noites da semana em vez de realizar uma cópia de segurança total para as capturar. Isto irá reduzir a sua janela de cópia de segurança enquanto também assegura que o utilizador tenha uma cópia de segurança da última versão dessas bibliotecas.

### Dados de segurança e dados de configuração

O utilizador também pode reduzir cortes de energia planeados através do isolamento de certos tipos de dados e em seguida realizando uma cópia de segurança em separado. Os dados de segurança incluem perfis de utilizador, listas de autorização e detentores de autoridade. Os dados de configuração incluem informações sobre como o seu servidor está configurado, como as descrições de linhas, descrições de dispositivos e listas de configuração. Estes tipos de dados são guardados como parte de uma cópia de segurança total do sistema, mas o utilizador também pode guardá-los à parte sem ter de encerrar o seu servidor. Para obter detalhes sobre como realizar cópias de segurança destes tipos de dados, consulte Guardar partes do seu servidor manualmente.

### Omitir certos artigos

Também pode reduzir a sua janela de cópia de segurança reduzindo o número de objectos que vai guardar ou evitando que os objectos sejam guardados mais do que uma vez. Pode fazer isto escolhendo a omissão de certos objectos de uma cópia de segurança. Por exemplo, pode querer omitir todas as bibliotecas de utilizador, excepto as bibliotecas temporárias. Pode optar a omissão de todas as bibliotecas temporárias da sua cópia de segurança, o que iria reduzir o comprimento do processamento da cópia de segurança. Muitos dos comandos que utilizar para guardar o seu servidor dão-lhe a opção de omitir certos artigos da cópia de segurança. Para obter detalhes sobre estes comandos, consulte Comandos para guardar partes do seu servidor e Comandos para guardar tipos de objectos específicos. Também pode utilizar Cópia de Segurança, Recuperação e Serviços de Suporte para omitir artigos de uma cópia de segurança.

## Reduzir cortes de energia planeados: Reduzir janelas de manutenção e actualização de software

Uma forma de assegurar que o servidor permanece disponível é manter o software actual. Este processo é moroso e exige planeamento. O objectivo deste tópico é descrever como pode manter o servidor disponível através da gestão de correcções e da instalação de novas edições.

### Gerir correcções

Para reduzir a quantidade de tempo que o seu servidor está indisponível, deve certificar-se de que tem uma estratégia de gestão de correcções elaborada. Se se mantiver actualizado em relação às correcções que estão disponíveis e as instalar de forma rotineira, terá menos problemas. Certifique-se de que aplica correcções com a frequência que achar apropriada para as necessidades da sua empresa. Para obter recomendações sobre a criação de uma estratégia de gestão de correcções, consulte Planear a sua estratégia de gestão de correcções.

As correcções individuais podem ser **demoradas** ou **imediatas**. As correcções demoradas podem ser carregadas e aplicadas de duas formas distintas. Podem ser carregadas enquanto o servidor é executado e em seguida aplicadas da próxima vez que reiniciar o servidor. As correcção imediatas não lhe exigem

que reinicie o servidor para que entrem em efeito, o que elimina a necessidade de tempo em baixo. As correcções imediatas podem ter passos de activação adicionais que são descritos na totalidade na carta introdutória que acompanha a correcção. Para obter mais informações sobre a aplicação de correcções, consulte Instalar correcções.

### **Instalar novas edições**

É-lhe pedido que desligue o servidor quando instalar uma nova versão do OS/400. Para minimizar a quantidade de tempo que demora uma actualização do software, é importante que planeie cuidadosamente a sua instalação. Para obter informações sobre o processo de planeamento, consulte Planear a instalação da edição do OS/400. Para obter uma lista de verificação dos passos do planeamento, consulte Planeamento do servidor: Software.

## **Reduzir cortes de energia planeados: Janelas de manutenção e de actualização de hardware**

Existem alturas em que o utilizador tem de executar manutenção de rotina no seu hardware ou aumentar a capacidade do seu hardware. Estas operações podem ser disruptivas para a sua empresa. Mas, com algum planeamento, o utilizador reduz em grande medida ou elimina mesmo alguns destes cortes de energia.

Se estiver a executar uma actualização do sistema, certifique-se de que realiza um planeamento cuidadoso antes de começar. Quanto mais cuidadoso for o planeamento do seu novo servidor, mais rapidamente se executará a actualização. Para obter mais detalhes sobre o processo de planeamento, consulte Actualizações.

### **Manutenção simultânea**

A **Manutenção simultânea** é uma função do servidor iSeries que activa um representante do serviço para reparar ou substituir certos componentes do hardware, enquanto o seu servidor está a ser utilizado para operações normais. Se tiver de substituir ou actualizar um componente elegível, seria capaz de o fazer sem interromper o seu negócio.

### **Actualização da capacidade a pedido**

Com a actualização da capacidade a pedido, o utilizador pode activar processadores adicionais e pagar apenas a nova energia de processamento à medida que aumentam as suas necessidades. O utilizador pode aumentar a sua capacidade de processamento sem interromper nenhuma das operações actuais.

A actualização da capacidade a pedido para o iSeries é uma função que oferece a capacidade de activar sem interrupções um ou mais processadores centrais do seu servidor. A actualização da capacidade a pedido adiciona capacidade em acréscimos de um processador, até ao número máximo de processadores a postos construídos através do seu modelo. A actualização da capacidade a pedido tem um valor significativo para as instalações onde pretende actualizar sem interrupção.

Para obter mais informações sobre a actualização da capacidade a pedido, consulte Actualização da Capacidade a Pedido



---

## Disponibilidade para vários sistemas: Conjuntos de unidades

A principal estratégia de disponibilidade para um ambiente de vários sistemas são os conjuntos de unidades. Um **conjunto de unidades** é uma recolha ou grupo de vários servidores iSeries que trabalham em conjunto como um único servidor. Se a sua empresa necessita de uma alta e contínua disponibilidade, os conjuntos de unidade são a solução que deve ponderar.

Os servidores num conjunto de unidades funcionam de forma cooperativa para fornecer uma única solução informática. O utilizador pode ter até 128 servidores num conjunto de unidades. Isto permite-lhe agrupar de forma eficiente os seus servidores iSeries para configurar um ambiente de forma a fornecer a disponibilidade que se aproxime dos 100 por cento para as suas aplicações importantes e para os seus dados importantes. Isto ajuda a assegurar que os seus servidores e aplicações importantes estejam sempre disponíveis. Os conjuntos de unidades também fornecem gestão de sistemas simplificada e escalabilidade aumentada para, da mesma forma, adicionar novos componentes à medida que o seu negócio floresce.

Enquanto que os benefícios dos conjuntos de unidade são imensos, o custo é significativo. O utilizador tem de ponderar o custo desta solução em contraste com o custo do tempo em baixo do seu servidor para decidir se deve ou não implementar conjuntos de unidades na sua empresa. Para obter informações sobre como determinar o custo do tempo em baixo na sua empresa, consulte Estimar o valor da disponibilidade.

Se optar por utilizar conjuntos de unidades no seu ambiente, é importante que considere os tipos de aplicações que utiliza. Existem algumas aplicações que estão concebidas para suportar alguns dos efeitos de uma falha. Para obter mais informações sobre estas aplicações, consulte “Programas de alta disponibilidade”.

Para aprender mais sobre conjuntos de unidades, incluindo a forma como funcionam e como implementar conjuntos de unidades na sua empresa, consulte Conjuntos de unidades. Para obter mais informações sobre conjuntos de unidades no contexto de outras soluções de alta disponibilidade, consulte Alta disponibilidade e conjuntos de unidades



## Programas de alta disponibilidade

As suas aplicações e os seus dados são essenciais para a sua empresa. Se estiver a utilizar conjuntos de unidades, existem programas que o utilizador pode utilizar que são resilientes num corte de energia do sistema. O próprio utilizador pode conceber estas aplicações, mas também pode adquirir aplicações que correspondem ao critérios necessários. Caso pretenda conceber você mesmo os programas, tem de compreender o que é um programa resiliente e o que são os níveis de disponibilidade da aplicação. Para obter mais informações sobre estes tópicos, consulte Aplicações de conjuntos de unidades.

Se adquirir aplicações, também pode certificar-se de que estão altamente disponíveis. ClusterProven<sup>(R)</sup> é uma marca da IBM que identifica estes tipos de aplicações. Uma aplicação quer é ClusterProven para o iSeries continua a estar disponível no evento de um corte de energia (planeado ou não planeado). Para obter mais informações sobre os critérios que estes programas têm de corresponder e uma lista dos programas que são ClusterProven, consulte Alta Disponibilidade e Conjuntos de Unidades





---

## Informações relacionadas com o roadmap de disponibilidade

Listados abaixo estão os manuais do iSeries e os Redbooks da IBM<sup>(TM)</sup> (no formato PDF) e sites da Web que se relacionam com o tópico do Roadmap de disponibilidade. Pode visualizar ou imprimir qualquer um dos PDFs.

### Tópicos do Centro de Informações do iSeries

- Cópia de Segurança e Recuperação
- Conjuntos de unidades
- Controlo de consolidação
- Gestão do disco
- Gestão do diário
- Partições lógicas
- Soluções de armazenamento

### Manuais

- Cópia de Segurança e Recuperação



- Cópia de Segurança, Recuperação e Serviços de Suporte para iSeries



### Redbooks

- Roadmap to Availability on the iSeries 400



- High Availability on the AS/400 System: A System Manager's Guide



- The System Administrator's Companion to AS/400 Availability and Recovery



- Clustering and IASPs for Higher Availability



- Striving for Optimal Journal Performance on DB2 Universal Database for iSeries



- AS/400 Remote Journal Function for High Availability and Data Replication



### Sites da Web

- High Availability and Clusters



- Backup, Recovery and Media Services



- IBM Business Continuity and Recovery Services



- IT Cost of Downtime Calculator



- Logical Partitioning



- Performance Capabilities Reference



- Tape and Optical Storage



Para guardar um PDF na sua estação para visualizar ou imprimir:

1. Abra o PDF no seu browser (faça clique sobre a ligação acima).
2. No menu do seu browser, faça clique sobre **Ficheiro**.
3. Faça clique sobre **Guardar Como...**
4. Navegue para o directório em que pretende guardar o PDF.
5. Faça clique sobre **Guardar**.

Se necessitar do Adobe Acrobat Reader para visualizar ou imprimir estes PDFs, pode descarregar uma cópia a partir do site da Web do Adobe ([www.adobe.com/prodindex/acrobat/readstep.html](http://www.adobe.com/prodindex/acrobat/readstep.html))







Impresso em Portugal