



### POSICIONAMENTO DO PRODUTO

Permitindo a operação contínua de negócios, o BrightStor High-Availability Manager desempenha papel-chave em sua estratégia IT e é um componente necessário em sua proteção de dados e na disponibilidade de arsenal para assegurar que ele seja sempre funcional como usualmente.

### RECURSOS-CHAVE: POR QUE ELES SÃO IMPORTANTES E POR QUE CHAMAM A ATENÇÃO DOS CLIENTES

**Duplicação de dados de alta performance.** O *BrightStor High Availability for Windows NT/2000* usa captura de transação patenteada e técnicas de transmissão de alta velocidade para atingir a mais eficiente performance de rede sem sacrificar a integridade dos dados. Minimiza o efeito sobre a performance da rede e do servidor primário.

**Transações de espelhamento em tempo real.** Mudanças feitas para o servidor primário são imediatamente duplicadas para o servidor secundário. Isso ocorre no nível da transação (somente transações reais, e não arquivos inteiros, são duplicadas) usando um processo patenteado. Nenhum *scanning* de diretório é exigido. O servidor secundário contém a versão atual de todos os arquivos; a inatividade é reduzida ao mínimo. A duplicação ao nível de transação minimiza o tráfego adicional da rede.

**Failover transparente.** O *failover* é imediato e ocorre prontamente se uma condição de falha for encontrada. O servidor secundário assume o nome, *shares* selecionados e endereço de IP do servidor primário com problemas (acrescidos a seus próprios nomes, *shares* e endereços de IP correntes). Os usuários continuam a trabalhar como de costume. Eles não precisam fazer *log-in* novamente e tipicamente nem notam que um failover ocorreu. Trilhas de arquivos e locações aparecem completamente intactas (sem mudanças).

**Deteção inteligente de falhas.** O *BrightStor High-Availability Manager* inclui script para *failover* de aplicações populares que requerem acesso contínuo do usuário, abrangendo banco de dados, *groupware*, e aplicações com base na *web*. Se o *BrightStor High-Availability Manager* detectar uma falha em potencial, ele pode buscar a confirmação através de um link alternativo de uma porta serial entre os servidores primário e secundário e/ou "rastreado" (*pinging*) máquinas selecionadas da rede ou dispositivos para determinar se a rede ainda está funcionando para aquela máquina ou dispositivo. A determinação de falha da rede pode ser adaptada a cada instalação, assegurando portanto que o *failover* somente ocorra quando necessário e não apenas porque as máquinas primárias e secundárias perderam comunicação de rede. A falsa detecção de falhas presente em produtos da concorrência é efetivamente eliminada.

**Reinicialização automatizada em um único comando.** Depois de substituir ou consertar qualquer *hardware* defeituoso, os dados do servidor primário são reconstituídos com um simples comando. A integridade dos arquivos é checada, e eles são atualizados ou recopiados se necessário. Os dados restaurados são mantidos atualizados até que ocorra reversão no comando ou em um tempo predeterminado. A restauração e a reversão para o servidor primário original são obtidas simples e facilmente.

### POR QUE ESCOLHER BRIGHTSTOR HIGH-AVAILABILITY MANAGER?

O *BrightStor High-Availability Manager* apresenta as exclusivas vantagens mostradas a seguir:

- **Proteção de dados e disponibilidade imbatível.** O BrightStor High-Availability Manager garante alta disponibilidade de dados, graças à duplicação de dados dos servidores primários designados para um servidor secundário em tempo real. Se o servidor primário falhar, o *SurviveIT* imediatamente, e de forma transparente, direciona os usuários para o servidor secundário.
- **Integridade transacional assegurada.** Técnicas patenteadas são usadas para garantir que somente transações completas sejam executadas no servidor secundário. Em situação de *failover*, os arquivos terão integridade transacional completa, evitando muitos dos problemas de corrupção dos arquivos que podem ocorrer com os produtos oferecidos pela concorrência.
- **Múltiplas proteções em uma.** Um único servidor secundário pode proteger múltiplos servidores primários. Na eventualidade de um primário falhar, o secundário automaticamente o substituirá, enquanto continuará a proteger outros servidores primários.
- **Nenhum servidor dedicado é exigido como stand by.** O servidor secundário pode simultaneamente operar como um servidor normal mesmo quando substituindo um ou mais servidores primários defeituosos. Não há obrigatoriedade de se comprar novo *hardware* para um servidor secundário dedicado.