

Implementando rotinas de backup

Introdução

O armazenamento de dados em meios eletrônicos é cada vez mais freqüente e esta tendência torna necessária a procura de maneiras de proteção que sejam realmente eficazes, rápidas e de baixo custo. A automatização dos processos de backup e restauração são obrigatórias pois a atividade humana é susceptível ao erro como operação inadequada e esquecimento.

Esta preocupação aumenta quando os dados devem estar disponíveis em tempo integral principalmente quando forem de missão crítica.

Além disso os backups devem ser rápidos para reduzir o grau de interferência no ambiente operacional da organização e a forma mais barata de reduzir o tempo é reduzindo o tamanho e executando o backup certo na hora certa, o que se consegue criando uma ótima arquitetura de backup.

Conheça as possíveis situações de perda de dados:

- Falhas técnicas: falha no disco rígido (HD), falha de energia, sobrecarga na rede de computadores que pode gerar falhas de comunicação e de software;
- Falhas ambientais: descargas elétricas providas de raios, enchentes, incêndios;
- Falhas humanas: detém 84% das perdas de dados e são devidas à exclusão ou modificação de dados acidental ou mal-intencionada, vírus, roubo de equipamentos e sabotagem.

Este manual irá lhe mostrar como criar estratégias eficazes de backup e restauração para a proteção dos dados de missão crítica de uma organização empresarial.

Desafios

- Garantir 99,99% da disponibilidade dos dados;
- Gerenciar o aumento do volume de dados;
- Interferir o menos possível no ambiente operacional da organização, a menos que esta estabeleça uma rede dedicada de backup;
- Descentralizar o armazenamento de dados mantendo-os redundantes em pontos distantes geograficamente.

Design do backup

Para idealizar o design de um plano de serviços de backup e recuperação é necessário elaborar um inventário de todo o ambiente operacional, para isso precisamos considerar as seguintes questões:

- Quais os dados devem ser protegidos e quão importantes e substituíveis são?
- São estruturados (como bancos de dados), semi-estruturados (como dados de e-mails) ou não estruturados (como sistemas de arquivos)?
- Onde estão localizados e qual o seu tamanho?
- Freqüência de alteração? Na ânsia de proteger os dados, muitos usuários acabam programando freqüências superiores às de alteração dos arquivos, gerando um volume muito grande de dados, dificultando e encarecendo o seu armazenamento. Identifique a freqüência correta para evitar backups desnecessários. Para dados com alteração freqüente é preciso saber quanto de trabalho os funcionários podem perder. Por exemplo, se o backup é feito duas vezes por dia (às 12:00 e às 18:00 horas, de segunda à sexta-feira) teremos uma janela de 5 horas de exposição ao risco. Este período fornece a cobertura adequada?
- As informações estão expostas a quais situações de perda de dados, falhas técnicas, ambientais e humanas?
- É mais importante um backup rápido ou uma recuperação rápida?
- Quais são as janelas de tempo disponíveis para realização do backup em cada aplicativo e servidor?

- Qual o período mínimo de retenção de dados para fins legais e/ou operacionais?
- Quais os tipos de mídia que devem ser utilizados, disco, fita ou outros?
- Quando e como podem ser feitos os backups, online ou offline, total ou parcial?
- Qual é o custo por hora de inatividade do ambiente operacional e quais as suas conseqüências?
- Quem é o responsável pelos serviços de backup e recuperação e o que acontece se o responsável deixar a organização?

Agora que já são conhecidos o grau de exposição ao risco, os dados, os prejuízos causados e as necessidades da organização, podemos elaborar as estratégias de backup.

Estratégias de backup

Modos de backup

Backup online: o backup é realizado enquanto os dados estão disponíveis aos usuários.

- Vantagem: não é necessário interromper o sistema;
- Desvantagem: redução no desempenho do servidor e documentos em uso não são atualizados.

Backup offline: o backup é realizado enquanto os dados estão indisponíveis aos usuários.

- Vantagem: alto desempenho do servidor;
- Desvantagem: implica em interrupções do sistema.

Tipos de backup

Backup total: cópia de todos os dados selecionados.

- Vantagem: rápida localização e restauração dos dados;
- Desvantagem: geram um volume muito grande de dados e interferem bastante no ambiente operacional, pois copiam todos os arquivos, modificados ou não.

Atualização do backup total: atualiza o arquivo do backup total, copiando apenas os arquivos modificados.

- Vantagem: rápida realização do backup, pois ele copia somente os arquivos modificados, rápida restauração, pois para a restauração completa do sistema é necessário apenas um arquivo de backup e rápida localização dos dados;
- Desvantagem: como ele atualiza o backup total, os arquivos de backup são maiores.

Backup incremental: cópia de todos os dados que foram alterados desde o último backup total ou incremental mais recente. (em implementação)

- Vantagem: economia de tempo e espaço pois é feito backup apenas dos dados modificados desde o último backup total ou incremental;
- Desvantagem: a restauração completa do sistema é mais lenta e complexa porque é necessário restaurar o backup total inicial e todos os backups incrementais subseqüentes até o mais recente.

Backup diferencial: cópia de todos os dados que foram alterados desde o último backup total. (em implementação)

- Vantagem: para a restauração completa do sistema são necessários apenas o backup total inicial e o diferencial mais recente;
- Desvantagem: são maiores e mais demorados que o incremental, pois copiam todos os arquivos modificados desde o último backup total.

Cópia auxiliar ou replicação: cria cópias exatas dos arquivos de backup para redundância.

- Vantagem: as cópias são geradas mais rapidamente que os backups reais, podendo ser replicados em vários locais diferentes para garantir maior segurança;
- Desvantagem: não há.

Backup total sintético: mescla o backup total mais recente com os backups incrementais subseqüentes e/ou diferencial mais recente, resultando em um único arquivo. (em implementação)

- Vantagem: rapidez na restauração, pois todos os dados estão em apenas um arquivo, redução de interferência no ambiente operacional, pois é possível fazer vários backups menores e em horários variados e a combinação dos backups em um único arquivo é mais rápida que a execução de um backup total;
- Desvantagem: como ele mescla os arquivos de backup em um único arquivo, gera um volume muito grande de dados.

Axis Focus

Locais de armazenamento

Manter dados redundantes em pontos distantes geograficamente evitam desastres causados por falhas técnicas, ambientais e humanas.

- Transmissão pela Internet: comunicações seguras devem fornecer criptografia e bloqueio de portas de rede;
- Proteção de mídia: proteção por senha para a mídia e local de acondicionamento adequado. É importante também a redundância de armazenamento porque nenhuma mídia é inteiramente isenta de riscos de falha.

Horário de realização do backup

Cada organização tem uma maneira peculiar de funcionamento que varia de acordo com seu produto/serviço e características de seu mercado consumidor. Para algumas organizações o melhor horário para realização do backup é fora do horário comercial, para outras, o melhor horário é justamente no horário comercial.

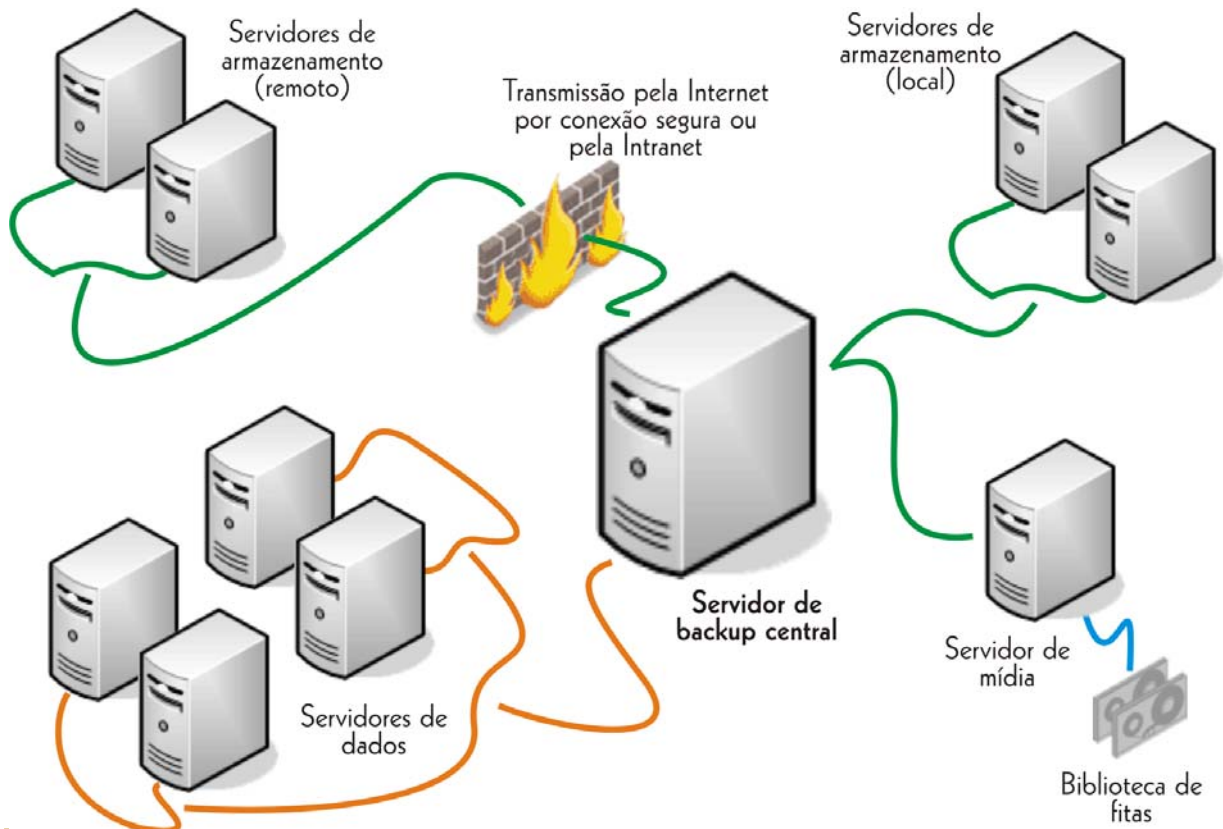
Programa a execução das rotinas de backup sempre em horários de menor utilização do ambiente operacional evitando os horários de pico e faça backup somente dos arquivos estritamente necessários para evitar maiores interferências. Se for necessário efetuar os backups em horários de pico, opte por backups parciais.

Após determinar a estratégia de backup mais apropriada para o ambiente operacional, é necessário executar um teste de restauração para todas as rotinas de backup, e assim identificar e corrigir as possíveis áreas com problemas e se familiarizar com os processos de recuperação de desastres, evitando se deparar com estas situações em uma real recuperação de desastres.

Relatórios ou logs

Com o tempo o design do backup deverá sofrer atualizações pela própria alteração da estrutura dos dados da organização. Utilize os relatórios ou logs de acompanhamento para saber se todos os dados de missão crítica estão devidamente protegidos, de acordo com as políticas da organização de proteção de dados e com as informações já descritas.

Exemplo de topologia de backup



Sobre o Total Protec

O Total Protec fornece todos os recursos necessários para implementar rotinas de backup complexas como as abordadas nos tópicos anteriormente, mas de forma prática, rápida e segura.

Total Protec e seus recursos

O Total Protec é um sistema automático de backup de dados, todos os recursos são independentes, proporcionando grande versatilidade para a criação das estratégias de backup.

Compactação e criptografia

Os arquivos a serem incluídos no backup podem ser selecionados por drive, diretório(s), sub-diretório(s), tipo(s), nome(s) de arquivo(s) e trechos do nome do arquivo (ex: todos os arquivos com a palavra "Pagamento" no nome).

Um recurso fundamental é a possibilidade de excluir sub-diretório(s), tipo(s), nome(s) de arquivo(s) e trechos do nome do arquivo que não devem ser incluídos no backup.

Existem 10 níveis de compactação do arquivo, podendo ser criptografado para garantir sua inviolabilidade.

Execução automática de programas

O Total Protec possibilita a execução de quaisquer programas para DOS e Windows. Entre outras possibilidades, é possível programar backups de bancos de dados (Oracle, SQL Server, MySQL, Interbase, Firebird e outros) utilizando as ferramentas próprias para cada banco de dados.

Gravação em CD/DVD

Grava CDs e DVDs em sessão única ou multi-sessão. Permite apagar o CD/DVD antes de gravá-lo.

Gravação em unidade de fita (em implementação)

Permite o armazenamento em mídia de grande volume de dados.

Replicação

Permite copiar os backups para outras pastas no próprio computador ou outros computadores da rede. Desta forma é possível usar os outros computadores para o armazenamento de dados, aumentando ainda mais a segurança pois o mesmo arquivo estará replicado em vários locais.

Remessa de arquivos

Com este recurso você poderá enviar o backup para qualquer computador do planeta através da Internet. É muito útil para a troca automática de dados entre matriz e filiais. Depende dos recursos de sua conexão à Internet.

Envio por FTP

O Total Protec pode enviar arquivos para servidores de FTP (Internet). É muito útil para armazenar os dados importantes fora das dependências da empresa.

Recuperação

Diversos recursos como a criação da mesma hierarquia de pastas, substituição dos arquivos atuais e a descompactação somente dos arquivos selecionados, tornam fácil e segura a recuperação de dados perdidos.

Relatórios ou logs

O Total Protec possui relatórios de processos realizados, ocorrência de falhas e programação. O relatório de processos realizados apresenta informações detalhadas sobre os processos que foram completados com sucesso. Em caso de falha o relatório de falhas identifica onde e porque a falha ocorreu facilitando sua correção. O relatório de programação permite uma visualização completa dos processos programados.

Axis Focus

Alerta em caso de falha

O Total Protec avisa o(s) responsável(is) pelos backups em caso de ocorrência de falhas, através de e-mail, pela rede ou Internet possibilitando a imediata correção do problema.

Três formas de inicialização

O Total Protec tem três formas de inicialização: manualmente (será executado quando o usuário clicar no ícone do programa), automaticamente antes do logon (ideal para servidores que não são estação de trabalho) e automaticamente após logon.

Manutenção do banco de dados

Todas as configurações do Total Protec estão armazenadas em um banco de dados. Na tela Manutenção de Banco de Dados existem diversos recursos para controlá-lo, inclusive para programar seu backup automático.

Instalando o Total Protec

Para fazer o download da versão shareware do Total Protec entre no site da Axis Focus (www.axisfocus.com).

Requerimentos mínimos de sistema:

Pentium 200 MHz

32 MB de RAM

Drive de CD-ROM

Sistema operacional a partir do Windows® 98

30 MB de espaço livre no disco rígido (HD)

Para instalar o Total Protec insira o CD no drive de CD-ROM do seu computador.

Se o Autorun estiver habilitado a tela de instalação irá aparecer automaticamente. Caso contrário será necessário executar o arquivo Instalar.exe que está na raiz do CD.

Instalando o gerenciador de banco de dados Firebird

Para garantir a segurança dos dados, o Total Protec utiliza o gerenciador de banco de dados Firebird que é fornecido gratuitamente.

Se em seu computador já estiver instalado o Interbase é possível utilizá-lo, já que atualmente é compatível com o Firebird, mas não garantimos esta compatibilidade para as próximas versões do Total Protec. Aconselhamos a instalação do Firebird que acompanha o Total Protec.

Na tela de instalação, clique em Firebird e Prosseguir instalação do Firebird.

Recomendamos instalá-lo na pasta destino padrão.

Instalando o Total Protec Servidor

Clique em Total Protec Servidor e Prosseguir instalação do Total Protec Servidor.

Recomendamos instalá-lo na pasta destino padrão.

Se a opção Inicia o Total Protec Servidor estiver habilitada o Total Protec irá iniciar automaticamente.

Instalando o Total Protec Cliente

Na versão completa o Total Protec Cliente é instalado nos computadores da rede que receberão avisos em caso de falha e nos computadores que receberão backups através da Internet.

Contato

Todas as informações para contato você encontra no site da Axis Focus (www.axisfocus.com).