Backup

O Backup ajuda a proteger os dados de perdas acidentais se ocorrerem falhas de hardware ou de mídia de armazenamento no sistema. Por exemplo, você pode usar o utilitário Backup para criar uma cópia dos dados que estão no disco rígido e arquivá-los em outro dispositivo de armazenamento.

A mídia de armazenamento de backup pode ser uma unidade lógica, como um disco rígido, um dispositivo de armazenamento separado, como um disco removível, ou uma biblioteca inteira de discos ou fitas organizados e controlados por alterador robótico.

Se os dados originais do disco rígido forem apagados ou substituídos acidentalmente ou se ficarem inacessíveis devido a um defeito do disco rígido, você poderá restaurar facilmente os dados usando a cópia arquivada.

Tipos de Backup

Fazer um backup é simples. Você vai, copia os arquivos que você usa para outro lugar e pronto, está feito o backup. Mas e se eu alterar um arquivo? E se eu excluir acidentalmente um arquivo? E se o arquivo atual corrompeu? Bem, é aí que a coisa começa a ficar mais legal. É nessa hora que entram as estratégias de backup.

Se você perguntar a alguém que não é familiarizado com backups, a maioria pensará que um backup é somente uma cópia idêntica de todos os dados do computador. Em outras palavras, se um backup foi criado na noite de terça-feira, e nada mudou no computador durante o dia todo na quarta-feira, o backup criado na noite de quarta seria idêntico àquele criado na terça. Apesar de ser possível configurar backups desta maneira, é mais provável que você não o faça. Para entender mais sobre este assunto, devemos primeiro entender os tipos diferentes de backup que podem ser criados. Estes são:

- Backups completos;

- Backups incrementais;

- Backups diferenciais;

- Backups delta;

Backups Completos

O backup completo é simplesmente fazer a cópia de todos os arquivos para o diretório de destino (ou para os dispositivos de backup correspondentes), independente de versões anteriores ou de alterações nos arquivos desde o último backup. Este tipo de backup é o tradicional e a primeira idéia que vêm à mente das pessoas quando pensam em backup: guardar TODAS as informações.

Outra característica do backup completo é que ele é o ponto de início dos outros métodos citados abaixo. Todos usam este backup para assinalar as alterações que deverão ser salvas em cada um dos métodos.

A vantagem dessa solução é a facilidade para localizar arquivos que porventura devam ser restaurados. A grande desvantagem dessa abordagem é que leva-se muito tempo fazendo a cópia de arquivos, quando poucos destes foram efetivamente alterados desde o último backup.

Este tipo consiste no backup de todos os arquivos para a mídia de backup. Conforme mencionado anteriormente, se os dados sendo copiados nunca mudam, cada backup completo será igual aos outros. Esta similaridade ocorre devido o fato que um backup completo não verifica se o arquivo foi alterado desde o último backup; copia tudo indiscriminadamente para a mídia de backup, tendo modificações ou não.

Esta é a razão pela qual os backups completos não são feitos o tempo todo Todos os arquivos seriam gravados na mídia de backup. Isto significa que uma grande parte da mídia de backup é usada mesmo que nada tenha sido alterado. Fazer backup de 100 gigabytes de dados todas as noites quando talvez 10 gigabytes de dados foram alterados não é uma boa prática; por este motivo os backups incrementais foram criados.

Backups Incrementais

Ao contrário dos backups completos, os backups incrementais primeiro verificam se o horário de alteração de um arquivo é mais recente que o horário de seu último backup. Se não for, o arquivo não foi modificado desde o último backup e pode ser ignorado desta vez. Por outro lado, se a data de modificação é mais recente que a data do último backup, o arquivo foi modificado e deve ter seu backup feito. Os backups incrementais são usados em conjunto com um backup completo frequente (ex.: um backup completo semanal, com incrementais diários).

A vantagem principal em usar backups incrementais é que rodam mais rápido que os backups completos. A principal desvantagem dos backups incrementais é que para restaurar um determinado arquivo, pode ser necessário procurar em um ou mais backups incrementais até encontrar o arquivo. Para restaurar um sistema de arquivo completo, é necessário restaurar o último backup completo e todos os backups incrementais subsequentes. Numa tentativa de diminuir a necessidade de procurar em todos os backups incrementais, foi implementada uma tática ligeiramente diferente. Esta é conhecida como backup diferencial.

Primeiramente, os backups incrementais são muito mais eficientes que os backups completos. Isto acontece porque um backup incremental só efetivamente copia os arquivos que foram alterados desde o último backup efetuado (incremental ou diferencial). Todo backup incremental se inicia a partir de um backup completo e a partir dele pode se criar os backups incrementais. Para restaurar os arquivos, você precisará do backup mais atual e de todos os backups anteriores desde o último backup completo.

A vantagem dessa solução é a economia tanto de espaço de armazenamento quanto de tempo de backup, já que o backup só será feito dos arquivos alterados desde o último backup. A desvantagem é que para procurar e restaurar os arquivos, se gasta muito tempo recriando a estrutura original, que se encontra espalhada entre vários backups diferentes, o que pode tornar o processo lento e suscetível à riscos, se houver algum problema em um dos backups incrementais entre o backup completo e o último backup incremental.

Backups Diferenciais

Da mesma forma que o backup incremental, o backup diferencial também só copia arquivos alterados desde o último backup. No entanto, a diferença deste para o integral é o de que cada backup diferencial mapeia as alterações em relação ao último backup completo.

Como o backup diferencial é feito com base nas alterações desde o último backup completo, a cada alteração de arquivos, o tamanho do backup vai aumentando, progressivamente. Em determinado momento pode ser necessário fazer um novo backup completo pois nesta situação o backup diferencial pode muitas vezes ultrapassar o tamanho do backup integral.

Em relação ao backup completo, ele é mais rápido e salva espaço e é mais simples de restaurar que os backups incrementais. A desvantagem é que vários arquivos que foram alterados desde o último backup completo serão repetidamente copiados.

Backups diferenciais são similares aos backups incrementais pois ambos podem fazer backup somente de arquivos modificados. No entanto, os backups diferenciais são acumulativos, em outras palavras, no caso de um backup diferencial, uma vez que um arquivo foi modificado, este continua a ser incluso em todos os backups diferenciais (obviamente, até o próximo backup completo). Isto significa que cada backup diferencial contém todos os arquivos modificados desde o último backup completo, possibilitando executar uma restauração completa somente com o último backup completo e o último backup diferencial. Assim como a estratégia utilizada nos backups incrementais, os backups diferenciais normalmente seguem a mesma tática: um único backup completo periódico seguido de backups diferenciais mais frequentes.

O efeito de usar backups diferenciais desta maneira é que estes tendem a crescer um pouco ao longo do tempo (assumindo que arquivos diferentes foram modificados entre os backups completos). Isto posiciona os backups diferenciais em algum ponto entre os backups incrementais e os completos em termos de velocidade e utilização da mídia de backup, enquanto geralmente oferecem restaurações completas e de arquivos mais rápidas (devido o menor número de backups onde procurar e restaurar). Dadas estas características, os backups diferenciais merecem uma consideração cuidadosa

Backups Delta

Este tipo de backup armazena a diferença entre as versões correntes e anteriores dos arquivos. Este tipo de backup começa a partir de um backup completo e, a partir daí, a cada novo backup são copiados somente os arquivos que foram alterados enquanto são criados hardlinks para os arquivos que não foram alterados desde o último backup. Esta é a técnica utilizada pela Time Machine da Apple e por ferramentas como o rsync.

A grande vantagem desta técnica é que ao fazer uso de hardlinks para os arquivos que não foram alterados, restaurar um backup de uma versão atual é o equivalente à restaurar o último backup, com a vantagem que todas as alterações de arquivos desde o último backup completo são preservadas na forma de histórico. A desvantagem deste sistema é a dificuldade de se reproduzir esta técnica em unidades e sistemas de arquivo que não suportem hardlinks.

Mídias

A fita foi o primeiro meio de armazenamento de dados removível amplamente utilizado. Tem os benefícios de custo baixo e uma capacidade razoavelmente boa de armazenamento. Entretanto, a fita tem algumas desvantagens. Ela está sujeita ao desgaste e o acesso aos dados na fita é sequencial por natureza. Estes fatores significam que é necessário manter o registro do uso das fitas (aposentá-las ao atingirem o fim de suas vidas úteis) e também que a procura por um arquivo específico nas fitas pode ser uma tarefa longa.

Por outro lado, a fita é uma das mídias de armazenamento em massa mais baratas e carrega uma longa reputação de confiabilidade. Isto significa que criar uma biblioteca de fitas de tamanho razoável não abocanha uma parcela grande de seu orçamento, e você pode confiar no seu uso atual e futuro.

As unidades de fita são uma opção interessante apenas para quem precisa armazenar uma grande quantidade de dados, pois o custo por megabyte das mídias é bem mais baixo que o dos HDs e outras mídias. O problema é que o custo do equipamento é relativamente alto e as fitas não são muito confiáveis, o que acaba obrigando o operador a fazer sempre pelo menos duas cópias para ter um nível maior de segurança. Para quem tem um pequeno negócio ou para usuários domésticos elas definitivamente não valem à pena.

Nos últimos anos, os drives de disco nunca seriam usados como um meio de backup. No entanto, os preços de armazenamento caíram a um ponto que, em alguns casos, usar drives de disco para armazenamento de backup faz sentido. A razão principal para usar drives de disco como um meio de backup é a velocidade. Não há um meio de armazenamento em massa mais rápido. A velocidade pode ser um fator crítico quando a janela de backup do seu centro de dados é curta e a quantidade de dados a serem copiados é grande.

Armazenamento

O que acontece após completar os backups? A resposta óbvia é que os backups devem ser armazenados. Entretanto, não é tão óbvio o que deve ser armazenado e onde. Para responder a estas questões, devemos considerar primeiro sob quais circunstâncias os backups devem ser usados. Há três situações principais:

1. Pequenos e rápidos pedidos de restauração dos usuários

2. Grandes restaurações para recuperar de um desastre

3. Armazenamento em arquivos, pouco provável de ser usado novamente

Infelizmente, há diferenças irreconciliáveis entre os números 1 e 2. Quando um usuário apaga um arquivo acidentalmente, ele pretende recuperá-lo imediatamente. Isto siginifca que a mídia de backup não pode estar há mais de dois passos distante do sistema para o qual os dados devem ser restaurados. No caso de um desastre que precisa de uma restauração completa de um ou mais computadores do seu centro de dados, se o desastre foi de natureza física, o que quer que tenha destruído seus computadores, também destruiria os backups localizados próximos dos computadores. Isto seria uma situação terrível.

O armazenamento em arquivos é menos controverso. Já que a chance de ser utilizado para qualquer propósito é baixa, não haveria problema se a mídia de backup estivesse localizada há quilômetros de distância do centro de dados. As táticas para resolver estas diferenças variam de acordo com as necessidades da empresa em questão. Uma tática possível é armazenar o backup de diversos dias na empresa; estes backups são então levados para um local de armazenamento mais seguro fora da empresa quando os backups diários mais novos forem criados.

Uma outra tática seria manter dois conjuntos diferentes de mídia:

Um conjunto no centro de dados estritamente para pedidos imediatos de restauração

Um conjunto fora da empresa para armazenamento externo e recuperação de desastres

Obviamente, ter dois conjuntos significa ter a necessidade de rodar todos os backups duas vezes para fazer uma cópia dos backups. Isto pode ser feito, mas backups duplos podem levar muito tempo e copiar requer diversos drives de backup para processar (e provavelmente um sistema dedicado a executar as cópias).

O desafio do administrador de sistemas é encontrar um equilíbrio que atenda adequadamente às necessidades de todos, e também assegurar que os backups estejam disponíveis para a pior das situações.

Enquanto os backups são uma ocorrência diária, as restaurações normalmente representam um evento menos frequente. No entanto, as restaurações são inevitáveis; elas serão necessárias, portanto é melhor estar preparado. É importante atentar para os vários cenários de restauração detalhados ao longo desta seção e determinar maneiras para testar sua habilidade em resolvê-los. E tenha em mente que o mais dfiícil de testar também é o mais crítico.

Testando os Backups

Todos os tipos de backup devem ser testados periodicamente para garantir que os dados podem ser lidos através deles. É fato que, às vezes, os backups executados são por algum motivo ilegíveis. O pior é que muitas vezes isto só é percebido quando os dados foram perdidos e devem ser restaurados pelo backup. As razões para isto ocorrer podem variar desde alterações no alinhamento do cabeçote do drive de fita, software de backup mal-configurado a um erro do operador.

Independente da causa, sem o teste periódico você não pode garantir que está gerando backups através dos quais poderá restaurar dados no futuro.

Questões de Concursos

(Prova: CESPE – 2011 – FUB – Técnico de Tecnologia da Informação – Específicos) A utilização do espelhamento de disco RAID 1 como forma de cópia de segurança é suficiente para a garantia da redundância do ambiente, o que torna desnecessária a realização de backup normal.

( ) Certo ( ) Errado

A periodicidade de realização de um backup deve ser definida por meio de uma política de segurança da informação, devendo-se observar as normas de classificação da informação, o gerenciamento de mídias removíveis e tabelas de temporalidade.

( ) Certo ( ) Errado

(Prova: CESPE – 2011 – TRE-ES – Técnico – Operação de Computadores – Específicos) Os procedimentos de recuperação devem ser verificados regularmente para que se garanta que sejam confiáveis; e as mídias utilizadas nas cópias de segurança devem ser testadas e armazenadas em local distante da fonte original das informações para não serem afetadas caso ocorra algum desastre na localidade principal.

( ) Certo ( ) Errado

(Prova: CESPE – 2010 – BRB – Escriturário) Em um ambiente computacional, a perda das informações por estragos causados por vírus, invasões indevidas ou intempéries pode ser amenizada por meio da

realização de cópias de segurança (backup) periódicas das informações, as quais podem ser feitas da máquina do usuário, de servidores e de todos os demais dispositivos de armazenamento, local ou remoto, de dados.

( ) Certo ( ) Errado

(Prova: CESPE – 2011 – FUB – Técnico de Tecnologia da Informação – Específicos) Após realização do backup, as cópias de segurança devem ser armazenadas em local seguro, em ambiente diferente do ambiente de armazenamento dos dados originais, e ser acessadas somente em caso de perda dos dados originais

( ) Certo ( ) Errado

(Prova: CESPE – 2010 – TRE-MT – Técnico Judiciário – Operação de Computador) Com relação a cópias de segurança, assinale a opção correta.

a) As cópias de segurança, juntamente com o controle consistente e atualizado dessas cópias e a documentação dos procedimentos de recuperação, devem ser mantidas no mesmo local da instalação principal, em local suficientemente próximo para sua imediata recuperação em caso de falha.

b) Três gerações, ou ciclos, de cópias de segurança das aplicações críticas é a quantidade mínima recomendada que deve ser mantida em local seguro (ambiente debackup) com os mesmos controles adotados para as mídias no ambiente principal.

c) As mídias utilizadas para cópias não precisam ser periodicamente testadas, pois são usadas somente em caso de falha.

d) Uma vez aprovados, os procedimentos de recuperação não devem ser modificados nem verificados periodicamente; a segurança do procedimento inicialmente acordada não será violada.

e) Segurança da informação é obtida a partir da implementação de uma série de controles que podem ser políticos, práticos,

procedimentos, estruturas organizacionais e funções de software, sendo caracterizada pela preservação da continuidade, confiabilidade e criptografia dos dados.

(Prova: FCC – 2010 – MPE-RN – Analista de Tecnologia da Informação – Suporte Técnico) Na implementação de uma solução de backup, a escolha e o ajuste das estratégias de backup são fundamentais na obtenção de um sistema eficaz. Nesse contexto,

considere:

I. Os recursos de armazenamento, quando encarados sob o ponto de vista da sua integridade e necessidade de proteção devem assegurar que informações, mesmo aquelas com baixa taxa de consulta e com razoável grau de desatualização, sejam integradas ao conjunto de dados de um sistema de backup otimizado.

II. A escolha criteriosa do que deve ser protegido leva em conta não a classificação da informação sempre nos mesmos padrões, mas sim a otimização do tempo para a operação de backup, volume de dados a armazenar e congestionamento da rede, entre outros fatores.

III. A periodicidade das operações de backup está intimamente ligada à taxa de crescimento da informação e ao esforço que é necessário despender para repor a informação, desde a última operação de backup. Nesse sentido, um backup semanal pode ser suficientemente aplicado em sistemas de aquisição em tempo real ou a processamentos de dados relativos a eventos únicos.

IV. Do ponto de vista da escalabilidade, uma solução de backup deve ser dimensionada de acordo com a medida da previsão de crescimento dos sistemas e do ambiente em que ela se insere.

Por outro lado, em termos de sistema protegido, a janela dedicada ao backup é definida pelo tempo que um sistema fica dedicado exclusivamente à operação de backup, levando em conta a paralisação total ou parcial dos seus serviços.

Está correto o que se afirma APENAS em **a)** I e II.

b) I e III. c) II e III. d) II e IV. e) III e IV.

(Prova: FCC – 2010 – TRF – 4ª REGIÃO – Técnico Judiciário – Informática) Desde a última reformulação da política de backups, realizada pela empresa JáVai, há alguns meses, a rotina baseia-se em backups normais e incrementais. Se dados forem perdidos, o processo de recuperação necessitará

a) apenas do último backup incremental.

b) pelo menos do último backup normal.

c) do primeiro backup normal realizado após a reformulação.

d) do último backup normal e do último backup incremental.

e) do primeiro backup normal realizado após a reformulação e do último backup incremental.

Comentários e Gabarito

(Prova: CESPE – 2011 – FUB – Técnico de Tecnologia da Informação – Específicos) A utilização do espelhamento de disco RAID 1 como forma de cópia de segurança é suficiente para a garantia da redundância do ambiente, o que torna desnecessária a realização de backup normal.

Errado. Mesmo com RAID 1 (Espelhamento de discos) é necessário fazer um backup normal, pois pode acontecer os discos queimarem ao mesmo tempo e a redundância RAID não se aplica por estarem no mesmo ambiente.

A periodicidade de realização de um backup deve ser definida por meio de uma política de segurança da informação, devendo-se observar as normas de classificação da informação, o gerenciamento de mídias removíveis e tabelas de temporalidade.

Certo. ISO 27002 diz que “Convém que procedimentos de rotina sejam estabelecidos para implementar as políticas de estratégias para a geração de cópias de segurança (ver 14.1) e possibilitar a geração das cópias de segurança dos dados e sua recuperação em um tempo aceitável”

(Prova: CESPE – 2011 – TRE-ES – Técnico – Operação de Computadores – Específicos) Os procedimentos de recuperação devem ser verificados regularmente para que se garanta que sejam confiáveis; e as mídias utilizadas nas cópias de segurança devem ser testadas e armazenadas em local distante da fonte original das informações para não serem afetadas caso ocorra algum desastre na localidade principal.

Certo. Vimos aqui na postagem que os backups devem ser testados e armazenados em local diferente.

(Prova: CESPE – 2010 – BRB – Escriturário) Em um ambiente computacional, a perda das informações por estragos causados por vírus, invasões indevidas ou intempéries pode ser amenizada por meio da realização de cópias de segurança (backup) periódicas das informações, as quais podem ser feitas da máquina do usuário, de servidores e de todos os demais dispositivos de armazenamento, local ou remoto, de dados.

Certo. Aqui foi explicado todo o conceito de backup em si.

(Prova: CESPE – 2011 – FUB – Técnico de Tecnologia da Informação – Específicos) Após realização do backup, as cópias de segurança devem ser armazenadas em local seguro, em ambiente diferente do ambiente de armazenamento dos dados originais, e ser acessadas somente em caso de perda dos dados originais

Errado. Quando ele afirma “somente em caso de perda dos dados originais” fica uma afirmativa muito restritiva para tal afirmação. Afinal, podemos acessar o backup para pegar uma versão anterior a atual, por exemplo.

(Prova: CESPE – 2010 – TRE-MT – Técnico Judiciário – Operação de Computador) Com relação a cópias de segurança, assinale a opção correta.

Letra “B”.

(Prova: FCC – 2010 – MPE-RN – Analista de Tecnologia da Informação – Suporte Técnico) Na implementação de uma solução de backup, a escolha e o ajuste das estratégias de backup são fundamentais na obtenção de um sistema eficaz. Nesse contexto, considere:

I. Os recursos de armazenamento, quando encarados sob o ponto de vista da sua integridade e necessidade de proteção devem assegurar que informações, mesmo aquelas com baixa taxa de consulta e com razoável grau de desatualização, sejam integradas ao conjunto de dados de um sistema de backup otimizado.

II. A escolha criteriosa do que deve ser protegido leva em conta não a classificação da informação sempre nos mesmos padrões, mas sim a otimização do tempo para a operação de backup, volume de dados a armazenar e congestionamento da rede, entre outros fatores.

III. A periodicidade das operações de backup está intimamente ligada à taxa de crescimento da informação e ao esforço que é necessário despender para repor a informação, desde a última operação de backup. Nesse sentido, um backup semanal pode ser suficientemente aplicado em sistemas de aquisição em tempo real ou a processamentos de dados relativos a eventos únicos.

IV. Do ponto de vista da escalabilidade, uma solução de backup deve ser dimensionada de acordo com a medida da previsão de crescimento dos sistemas e do ambiente em que ela se insere. Por outro lado, em termos de sistema protegido, a janela dedicada ao backup é definida pelo tempo que um sistema fica dedicado exclusivamente à operação de backup, levando em conta a paralisação total ou parcial dos seus serviços.

Está correto o que se afirma APENAS em

Letra “D”. A afirmativa I está ERRADA quando ele diz que devem assegurar que as informações, mesmo aquelas com baixa taxa de consulta e com razoável grau de desatualização, devem ser mantidas a integridade e proteção. Neste caso, os arquivos “dinâmicos” é que devem ir pro backup. Já os mais “estáticos” devem ficar no sistema de arquivos mesmo por não precisar ocupar mais espaço do backup em si, e já estarem no backup completo inicial.

III – ERRADO quando afirma que um backup semanal é o suficiente para sistema de aquisição em tempo real ou a processamento de dados relativos a eventos únicos. Em alguns ambientes, um backup semanal poderá ser suficiente, nomeadamente quando a informação criada durante uma semana pode ser readquirida ou recriada sem grandes custos.

(Prova: FCC – 2010 – TRF – 4ª REGIÃO – Técnico Judiciário – Informática) Desde a última reformulação da política de backups, realizada pela empresa JáVai, há alguns meses, a rotina baseia-se em backups normais e incrementais. Se dados forem perdidos, o processo de recuperação necessitará

Letra “B”. A resposta especifica o que irá precisar no MÍNIMO, que neste caso é o último backup normal, mas não se RESTRINGINDO a ele em si. Ou seja, na prática, precisaria dele e dos demais backups incrementais até antes da data da perda dos arquivos.