DESK BACKUP – Segurança na Gestão de Informações Corporativas

Graycielli A. Mendes, Ana Carolina Xaves Ferreira, Rafael Couto dos S .Lima, Diogo Florenzano Avelino da Silva.

mendes.grace@gmail.com, anacarolina.ferreira@mpsa.com, rafaelcoutolima@yahoo.com.br, diogo.avelino@gmail.com

Associação Educacional Dom Bosco, FCEACDB – Resende, RJ, Brasil

RESUMO

Com o aumento gradual de informações críticas dentro das corporações, cresce a demanda por técnicas de armazenamento cada vez mais confiáveis. É comum a dificuldade de padronização de processos e como conseqüência o risco de perda de dados por diversos motivos. O sistema Desk Backup surge como uma solução de backup e recuperação confiável e transparente para usuários de desktops e laptops corporativos.

Palavras-Chave: Backup Corporativo, Segurança, Recuperação de Informação.

1. INTRODUÇÃO

Diante de um intenso avanço tecnológico e com a expansão global física e mercadológica das empresas houve um grande aumento em seus ambientes computacionais móveis e remotos. Cada dia mais os funcionários armazenam importantes propostas, planejamentos, especificações técnicas e informações confidenciais em seus laptops ou palmtops. Apesar da flexibilidade e melhor produtividade que estes equipamentos portáteis oferecem, há também um risco significativo, visto que na maioria das vezes as informações não ficam protegidas como se estivessem em servidores corporativos.

Em grande parte dos casos o backup é negligenciado, pois as pessoas acreditam não estarem sujeitas ao risco de perdas de informações, devido ao processo de backup é demorado ou porque preferem simplesmente manter os dados apenas em discos rígidos locais, sendo que existe a possibilidade de apresentarem erros físicos e lógicos. Além disto, existe a chance de ocorrer a exclusão acidental de arquivos, desastres naturais, ataques de vírus e até mesmo roubo ou perda de laptops. A proteção dos dados em uma Estação de Trabalho, remota ou móvel, exige cuidados diferentes de um PC que esteja permanentemente conectado à rede e conseqüentemente a um servidor de arquivos.

Devido às dificuldades relacionadas ao gerenciamento da segurança dos dados dentro das corporações, surge a necessidade de novas soluções, que sejam flexíveis e adequadas à realidade atual das empresas. Para criar um sistema que se ajuste ao cenário de que falamos, primeiramente, precisamos conhecer profundamente os processos que vêm sendo aplicados dentro do meio corporativo contemporâneo. Através de um levantamento de requisitos será possível analisar os procedimentos empregados e apontar seus pontos fortes e falhos.

2. BACKUP CORPORATIVO

Analisaremos, a seguir, alguns fatores típicos relacionados aos recursos de armazenamento de dados, que envolvem principalmente o ramo corporativo. Palavras como integridade, segurança e confiabilidade estão diretamente ligadas aos procedimentos de backup. Logo, se o termo backup está diretamente associado à segurança de dados, deve receber atenção diferenciada.

2.1. GERENCIAMENTO

A eficiência em relação à segurança no tráfego de informações envolve o gerenciamento dentro da arquitetura de rede, ou seja, para que uma empresa seja capaz de prover segurança e velocidade para os dados dos seus usuários é imprescindível um perfeito gerenciamento desses dados.

Essa atividade consiste basicamente em identificar a maneira como os dados devem ser armazenados, o volume de informações críticas existentes, a quantidade de dados desprezíveis que são armazenados assim como questões importantes para se definirem regras de armazenamento e a necessidade ou não de expansão dos componentes de armazenamento. Além disso, o ato de gerenciar a arquitetura, componentes e práticas de backup constitui o desenvolvimento de uma infra-estrutura capaz de operar sobre os padrões abertos e independentes de plataformas de hardware de armazenamento.

Uma das soluções utilizadas para o problema do gerenciamento é a consolidação de *storage*, onde diversos ambientes de armazenamento são centralizados em um único local, facilitando a administração e o gerenciamento dos dados armazenados. Dessa forma, o gerenciamento permite que toda a configuração e monitoração dos processos de backup e *recovery* seja centralizada em um único ponto, independente de localização física do mesmo.

Estão disponíveis no mercado soluções completas e abrangentes, contando com uma infra-estrutura de hardware e software para maximizar a disponibilidade de níveis de serviço (SLA – *Service Level Agreement* ou Acordo de Nível de Serviço) visando operações de ambiente de missão crítica. A existência de mecanismos para atender às necessidades de janela de tempo de backup, sem a interrupção da operação normal e para situações de recuperação de desastres complementa a arquitetura de backup corporativo.

É necessário realizar também um levantamento relacionando todos os servidores que serão os clientes do backup/*restore* e todos os sistemas operacionais, bancos de dados e aplicativos envolvidos e da rede de interligação dos mesmos, objetivando garantir a confiabilidade da operação, mesmo em situações de falha de alguns dos componentes. O dimensionamento e configuração dos servidores de backup e dos dispositivos de backup (incluindo número de unidade de fitas para cada dispositivo) devem ser indicados, assim como a arquitetura de rede e política de compartilhamento de unidades de fita (uso ou não de *Storage Area Network* – Área de Armazenamento em Rede).

2.2. FALHAS COMUNS EM PROJETOS

Atualmente, são comuns casos de implementação de backup, onde o crescimento constante e veloz do volume de dados requer um novo projeto de *storage* em pouquíssimo tempo. Geralmente, isso ocorre devido a várias situações de falha, tais como: dimensionamento equivocado dos dispositivos de backup, utilização de softwares com insuficiência de funcionalidades e a falta de planejamento na utilização da rede.

As restrições de compatibilidade são observadas principalmente em softwares dependentes de plataformas de hardware de armazenamento, implicando na utilização de backup com características proprietárias e que simplesmente não funcionam ou funcionam mal quando há inclusão de outras plataformas de hardware de armazenamento no ambiente de backup.

Uma infra-estrutura de hardware e software de backup deve ser flexível para suportar o maior número possível de sistemas operacionais, além de utilizar as interfaces e utilitários nativos das principais aplicações do mercado.

3. PROJETO DESK BACKUP

Os produtos de backup corporativo que estão disponíveis no mercado são diversificados e projetados para uso ótimo com uma biblioteca de fita, atendendo as necessidades do administrador de rede de maneiras diferentes. Porém, considerando que a demanda por backup de dados é universal, é importante oferecer funcionalidade e confiabilidade juntamente com uma interface amigável apropriada para administradores e usuários com variados níveis de experiência. A flexibilidade também é um ponto fundamental diante da necessidade dos administradores de editar tarefas existentes e reconfigurar parâmetros com rapidez e facilidade quando as circunstâncias assim o exigirem.

Por fim, um bom produto deve ser capaz de lidar com a diversidade de marcas e padrões normalmente encontrados em um ambiente de rede heterogêneo.

O projeto Desk Backup apresenta uma nova solução de backup e recuperação confiável e transparente para o usuário. Elaborado de forma a permitir que os administradores de departamentos ou TI agendem backups automáticos que irão acontecer em segundo plano, ou seja, enquanto os usuários continuam a executar suas atividades normalmente. Os backups poderão ser agendados de acordo com a necessidade de cada usuário. Além disso, os administradores de departamento ou TI poderão definir a cota de armazenamento de informações no servidor por usuário. No caso de laptops, os quais nem sempre estão conectados à rede, a transmissão de seus dados para o servidor, será feita quando o software detectar a conexão TCP/IP, no momento em que o usuário verificar seus e-mails ou utilizar o acesso a websites, por exemplo.

Recursos e funções diferenciados:

- Otimização da largura de banda: Serão utilizadas algumas técnicas como a thread para o aumento do desempenho no envio e recebimento de pacotes durante o backup e recuperação de arquivos.

- Gestão centralizada das regras para backup das estações: o administrador do sistema terá acesso a todas as funcionalidades do sistema, sendo algumas exclusivas a ele.
- Conjunto de backups predefinidos: O sistema oferecerá a opção de agendamento para backups freqüentes e rotineiros.
- Recuperação de arquivos por usuários ou administradores: Além do administrador o usuário também poderá realizar a recuperação de arquivos de acordo com sua necessidade.
- Interface amigável para o usuário do produto: Para que o usuário possa utilizar o sistema com sucesso ele deve saber quais as funções da aplicação são oferecidas pelo sistema e como ele pode interagir com cada uma delas, por isso a interface do Desk Backup está sendo elaborada de forma que o usuário possa explorar os recursos do sistema sem maiores dificuldades.

4. ARQUITETURA DO SISTEMA

Os arquivos de backup serão enviados do computador remoto (seja laptop ou desktop) através da rede para o servidor, após prévia identificação. O procedimento de backup é agendado pelo administrador. O usuário poderá salvar suas preferências de diretórios a serem enviados a cada backup, sendo permitido também que altere suas preferências sempre que desejar.

O administrador estipulará uma cota de armazenamento de arquivos no servidor para cada usuário, portanto a seleção de diretórios feita pelo usuário deve estar de acordo com a cota estabelecida pelo administrador. O sistema também proporciona ao usuário a recuperação de arquivos.

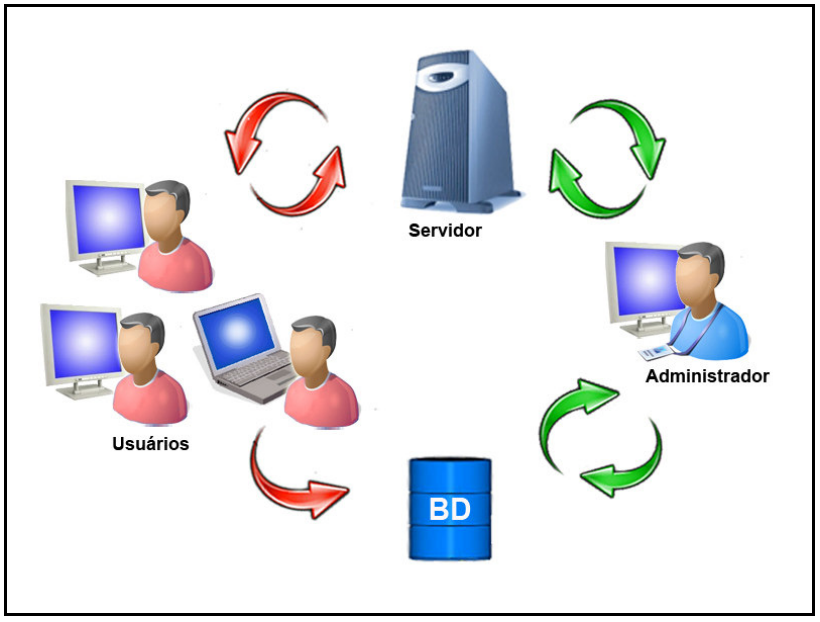

Fig. 4.1 – Arquitetura Desk Backup

5. MECANISMOS UTILIZADOS

Para a implementação deste sistema são necessários alguns mecanismos que viabilizam os processos necessários para o pleno funcionamento do software. Mecanismos de quebra em fluxos de execução, estabelecimento de canais de comunicação e controle de duplicidade de arquivos, tais como threads, sockets e MD5.

5.1. THREADS

Os sistemas operacionais atuais adotam o conceito de que processos são de uma forma simplificada programas diferentes e independentes executados pelo sistema operacional. Um *Threading* pode ser entendido como um artifício que possibilita a existência simultânea de diversas atividades dentro de um mesmo processo.

Threads (linha de execução em português) podem ser conhecidos também como *lightweight processes* (processos leves), já que assim como os processos se apresentam independentes possuindo sua própria pilha de execução, seu próprio *program counter* e suas próprias variáveis locais. Entretanto, threads de um mesmo processo compartilham memória, descritores de arquivos (*file handles*) e outros atributos que são específicos daquele processo.

Um processo pode conter múltiplas threads que parecem executar ao mesmo tempo e de forma assíncrona em relação às outras threads.

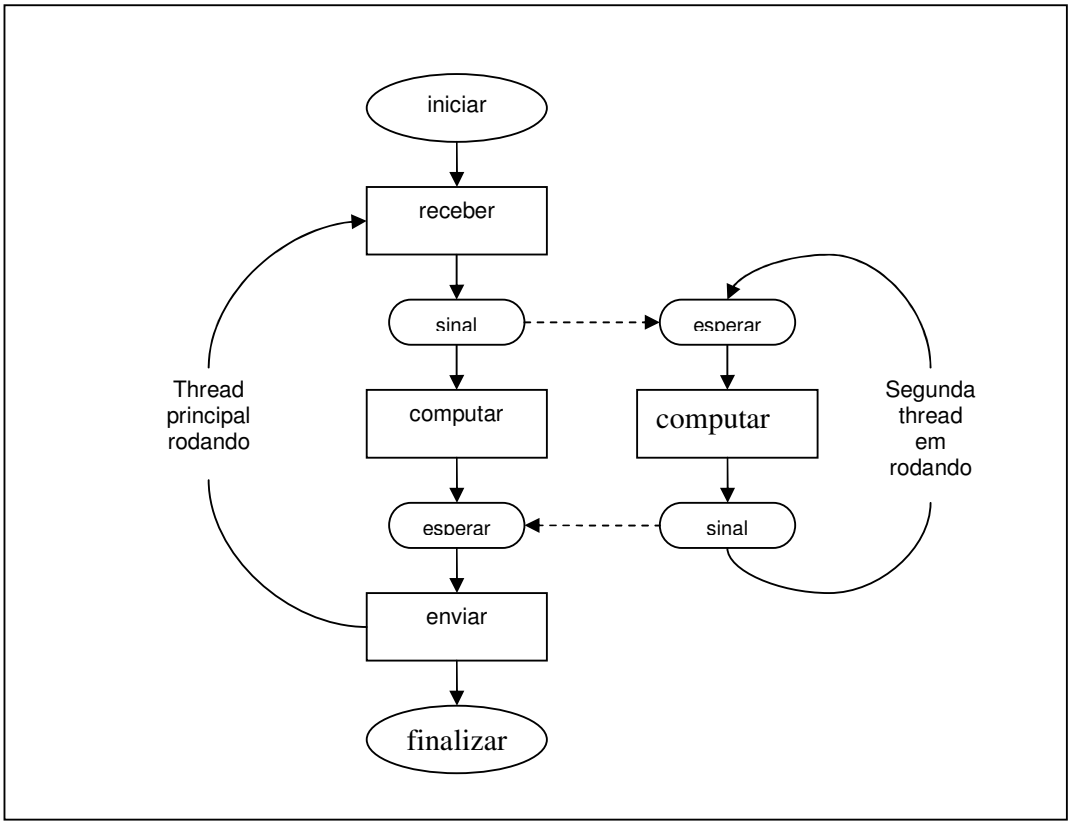

Fig. 5.1 – Esquema de funcionamento de uma Thread

Em vista do grande tráfego de dados em um sistema de backup, a utilização de threads torna-se uma um mecanismo estratégico, já que possibilitará, a permanência de alguns processos em espera enquanto outros serão executados, permitindo desta forma um processamento em segundo plano.

5.2. MD5

Funções *hash* criptográficas são funções bastante difundidas no contexto das aplicações computacionais. Por se tratar de uma ferramenta de segurança e por possuir propriedades como resistência a colisões e unidirecionalidade, propriedades construídas a partir de premissas matemáticas e computacionais completamente não-triviais.

Um MD5 é uma seqüencia de letras ou números geradas por um algorítimo de Hash.

Na criptografia, o *hash* serve para garantir a integridade da mensagem, onde o gerador (ou emissor) da mensagem, submete-a a um algoritmo *hash*, o qual produzirá um valor hash (este é outro nome pelo qual é conhecido o MD).

O algoritmo hash é composto por fórmulas matemáticas complexas, para poder garantir a irreversibilidade e a unicidade do MD gerado. Textos diferentes não produzem o mesmo MD. A alteração de um simples bit na mensagem gera um MD completamente diferente e o valor de conferência ("check-sum") muda se um único bit for alterado, acrescentado ou retirado da mensagem.

A utilização de MD5 em um sistema de backup corporativo permite ao software verificar se o arquivo que está sendo copiado para o servidor já foi enviado previamente, evitando assim o desperdício de espaço com arquivos em duplicidade e implantando um conceito de backup diferencial.

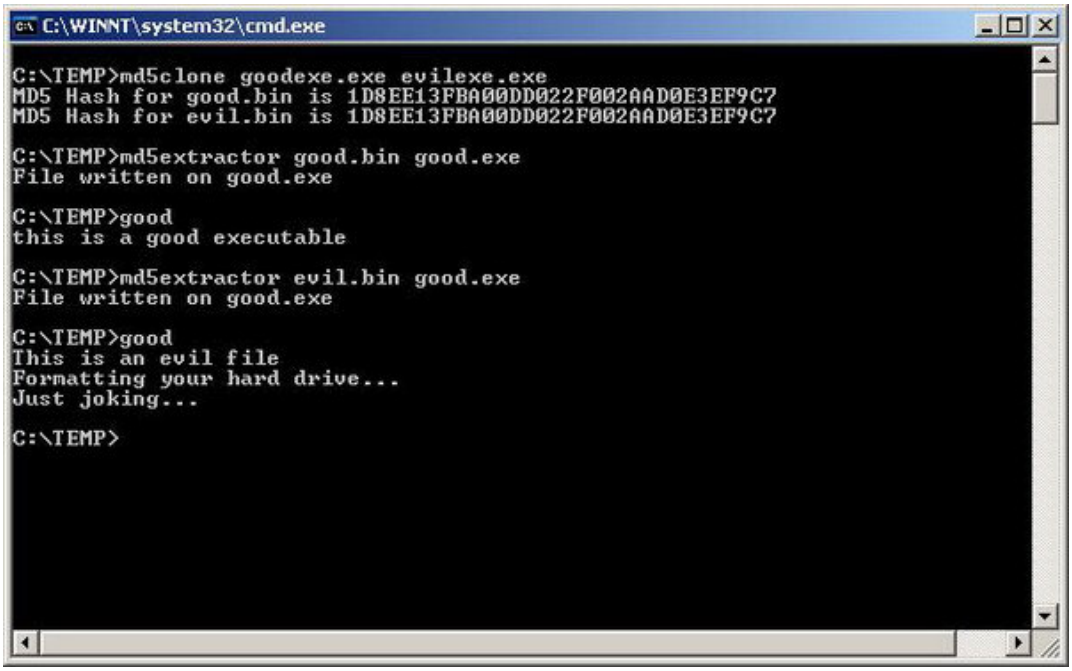

Fig. 5.2 – Verificação de MD através do prompt

5.3. SOCKETS

Em computação especificamente um socket pode ser utilizado para realizar uma conexão entre redes de computadores com o objetivo de estabelecer um elo bidirecional entre dois programas. É também uma abstração computacional que mapeia diretamente a uma porta de transporte (TCP ou UDP) e mais um endereço de rede. Com esse conceito é possível identificar unicamente um aplicativo ou servidor na rede de comunicação IP.

O processo de comunicação no modo orientado a conexão ocorre da seguinte forma: servidor escolhe uma determinada porta e fica aguardando conexões nesta porta. O cliente deve saber previamente qual máquina servidora (*host*) e a porta que o servidor está aguardando conexões. Se nenhum problema ocorrer, o servidor aceita a conexão gerando um socket em uma porta qualquer do lado do servidor, criando assim um canal entre o cliente e servidor.

Tipicamente o comportamento do servidor é ficar em um loop aguardando novas conexões e gerando sockets para atender as solicitações de clientes.

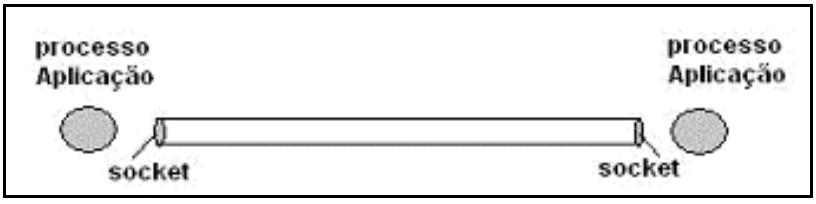

Figura 5.3 – Esquema de funcionamento de Sockets

Em documentos de RFC (*Request for Comments*) relacionado a TCP ou UDP, um socket em um computador é definido como a combinação de um endereço IP, um protocolo, e o número da porta do protocolo.

Sockets e RPCs têm a função de implementar numa aplicação as funções de rede, mas fazem isto de maneiras diferentes.

Para o envio de arquivos do módulo cliente para o módulo servidor, procedimento vital para a realização do backup, será necessário realizar a comunicação entre ambos, utilizando para isso o mecanismo socket que estabelecerá a comunicação entre as máquinas remotas e o servidor através do número de porta, do endereço IP e do protocolo das máquinas.

6. ESTUDO DE CASO NA ASSOCIAÇÃO EDUCACIONAL DOM BOSCO – AEDB

Especificamente, foram coletadas informações relativas ao processo de backup realizado atualmente no nosso domínio de aplicação; a Associação Educacional Dom Bosco, o que inclui a área administrativa e rede acadêmica. Para isso foram realizadas entrevistas com os responsáveis e funcionários do setor de informática da AEDB.

O processo de backup hoje adotado funciona basicamente da seguinte forma: o backup de dados é realizado diariamente na rede acadêmica. Os arquivos são armazenados inicialmente em um servidor. Todas as sextas-feiras os dados são retirados do HD e gravados em um DVD que será reutilizado quinzenalmente. A rede acadêmica conta com um mapeamento de pastas, nas quais os usuários são instruídos a

armazenarem os arquivos que desejam guardar. Este processo conta com a utilização do Windows 2003 para o agendamento dos backups e definição de cota de armazenamento.

Segundo o responsável pelo Departamento de Informática e Coordenador do Curso de Sistemas de Informação, Prof. Msc Eduardo Barrére, a instituição já enfrentou diversos problemas com perdas de informações ocasionadas muitas vezes por erro de usuários, problemas físicos ou lógicos nos discos ou simplesmente falta do backup.

O projeto Desk Backup visa automatizar este processo, disponibilizando recursos para usuários e administradores e permitindo uma gestão centralizada.

7. CONSIDERAÇÕES FINAIS

Gerenciar informações de forma eficiente é um desafio encontrado por empresas de todos os portes e segmentos. Um mau gerenciamento dos dados pode ocasionar prejuízos muitas vezes ocultos, como baixa velocidade de acesso, má utilização dos componentes de armazenamento e um alto custo total de propriedade (TCO).

Nenhum sistema de armazenamento está completo sem uma solução adequada de cópias de segurança. Assegurar a integridade dos dados é um dos maiores desafios da área de Tecnologia da Informação de uma empresa, principalmente porque soluções como espelhamento remoto e cópia de dados não conseguem garantir essa integridade em situações de erros humanos, sabotagens ou mesmo desastres de proporções não previstas. Em muitos destes casos, somente uma cópia ou solução de backup pode resolver a situação.

Atualmente, é possível encontrar diversas soluções para backup e recuperação. Desk Backup atende todas as necessidades do mercado corporativo, incluindo em seus controles dados provenientes de equipamentos portáteis.

A nova visão que as corporações precisam ter em relação à gestão de TI é que a mesma constitui uma necessidade vital da empresa, devido à disponibilidade das máquinas, do acesso à rede e, principalmente, das informações armazenadas em seus servidores. Aos profissionais de TI, cabe garantir que estes recursos estejam disponíveis, a fim de evitar perdas mais graves.

8. REFERÊNCIAS BIBLIOGRÁFICAS

O passo-a-passo do backup corporativo. Disponível em: <http://www.s2.com.br/scripts/artigos_texto.asp?clienteId=370&artigoId=72> Acesso em: 24 mar. 2007.

PINHEIRO, José Mauricio Santos. **Políticas de Backup Corporativo**. Disponível em: <http://www.metrored.com.br/artigos/artigo_politicas_de_backup_corporativo.php> 02/02/2005. Acesso em: 12 mar. 2007.

CORDEIRO, Daniel de Angelis**. Introdução ao uso de Threads em Java** Disponível em: <http://www.ime.usp.br/~gold/cursos/2004/mac438/threadsEmJava.pdf> 26/03/2004. Acesso em: 30 jun. 2007.

NUNES, Leonardo R**. Sockets em Java**
Disponível em: < http://www.sumersoft.com/publicacoes/SocketsEmJAVA.pdf> Acesso em: 30 jun. 2007.

VALADARES Francisco de Assis Mesquita**. Uma avaliação crítica sobre os ataques às funções MD5 e SHA1.**
Disponível em: < http://www.cin.ufpe.br/~tg/2005-2/famv.pdf>
27/03/2006 Acesso em: 24 mar. 2007.