UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANA
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZACÃO SOFTWARE LIVRE APLICADO A TELEMÁTICA

DENILSON AUGUSTO DOMINGUES

BACKUP E RECUPERAÇÃO MAIS EFETIVA

MONOGRAFIA

DENILSON AUGUSTO DOMINGUES

BACKUP E RECUPERAÇÃO MAIS EFETIVA

Monografia apresentada como requisito parcial para obtenção do grau de especialista em Software Livre Aplicado a Telemática, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná. Orientador: Prof. Christian Carlos Souza Mendes

RESUMO

Denilson Augusto Domingues. Backup e recuperação mais efetiva 2012. 40 f. Monografia (Especialização em Software Livre Aplicado a Telemática) – Programa de Pós-Graduação em Tecnologia, Universidade Tecnológica Federal do Paraná. Curitiba, 2012.

O propósito desta monografia é estudar sobre backup e restore, verificar os tipos de backups existentes, bem como os tipos de mídias mais utilizados, os sistemas de backup mais conhecidos como o Rsync, Amanda e o Bacula, estudar a possibilidade da realização do backup e restore não só dos servidores como das estações de trabalho da rede, restauração parcial e total dos backups, realizar a verificação dos backups realizados, explorando as funcionalidades de cada um dos módulos do Bacula e no final optar por uma das tecnologias estudadas.

Palavras-chave: Backup. Restore. Bacula.

Lista de Figuras

Sumário

1. INTRODUÇÃO.

Hoje em dia, o número de catástrofes digitais anda aumentando, e eu não me refiro a catástrofes naturais como enchentes ou incêndios ou até ataques de hackers. O que realmente preocupa são os ataques causados por falhas humanas, como instalações de softwares, erros causados por “teclar” teclas erradas, um gerenciamento de mudanças inadequado ou baixa qualidade de dados.

Estas são coisas que geralmente resultados acidentais ao invés de ações sinistras. Alguém provavelmente diria, depois de todos estes anos de desenvolvimento e operação em serviços de TI, nós deveríamos ser aptos a entregar serviços que são altamente confiáveis. Infelizmente este não é sem-

pre o caso. Atrás de cada incidente, há sempre dezenas de esquecimentos, centenas de incidentes menores e milhares de piores práticas.

Mas a pergunta é, porque isto continua acontecendo? Muitas tendências estão por trás disto. Hardwares podem ser um pouco mais confiáveis (nem sempre), mas sistemas e infraestruturas estão se tornando altamente complexas e difíceis de integrar. Etapas de projetos estão se tornando cada vez mais curtas por causa da pressão continuada que vem do gerenciamento do negocio que querem que sejamos mais ágeis. Também há pressão para que sejam efetuados cortes no custo resultando em grandes demandas nos recursos e constante mudança de fornecedores(**Jardim, 2012**).

O backup de dados e os processos de recuperação são parte das rotinas de todos os departamentos de TI, mas sempre existe espaço para melhorias. Se você enfrenta qualquer um dos itens seguintes, você é um candidato para uma atualização.

1.1. Crescente armazenamento de dados:

O crescimento incessante de dados (20% ou mais anualmente para uma empresa típica de médio porte) pode ultrapassar sua capacidade de armazenamento, banda e recursos de equipe. Você pode simplificar o processo eliminando dados redundantes ou você precisa de uma solução mais robusta e escalável.

1.2. Longos períodos de recuperação:

Uma pesquisa recente pela empresa de pesquisa de mercado Enterprise Strategy Group encontrou que mais da metade das empresas de

médio porte podem tolerar apenas uma hora ou menos de inatividade para missão crítica de dados. Se o seu tempo de recuperação está significativamente mais longo, você pode estar colocando a empresa em risco. Recuperação rápida é especialmente crítica em empresas com muitos empregados remotos. “Trabalhadores remotos necessitam acesso aos dados no escritório, mas seus clientes podem provavelmente estar perdidos para sempre”, dissse Hugo Llorens, gerente de produto da linha SMB EqualLogic™ na Dell. “Para eles, a velocidade de recuperação se torna ainda mais importante.”

1.3. Aumento de complexidade virtual:

A virtualização do servidor pode simplificar sua infraestrutura física do servidor, mas pode tornar o backup e a recuperação mais complexos. Você precisa decidir a melhor metodologia de backup e de recuperação dos dados, e se usará ferramentas especializadas de diversos fornecedores ou uma ferramenta única, padronizada para os recursos virtuais e físicos. “Se você está consolidando 20 servidores em máquinas virtuais, você tem que repensar o backup”, disse Greg Schulz, fundador e consultor sênior no Grupo Server and StorageIO. “A última coisa que você quer é consolidá-los e ainda ter 20 cópias de backup rodando na máquina física.”

1.4. Tecnologia obsoleta:

Muitos avanços recentes em tecnologia podem melhorar o desempenho de backup e recuperação, incluindo a desduplicação de dados, backup em disco, compressão, replicação off-site, na nuvem entre outros. Embora os

> preços tenham baixado, esses avanços devem ser equilibrados em relação ao quanto a TI tem para investir. Backup e recuperação devem ser feitos dentro de um orçamento, e os orçamentos de TI têm sido consistentemente reduzidos nos últimos anos.

A boa notícia é que a implantação de uma solução efetiva pode estabelecer retornos sólidos de investimento. De acordo com um relatório sobre backup e recuperação do Grupo Alchemy Solutions, “Quanto melhor a solução de backup e recuperação de uma organização, mais seguros os seus dados estarão e maior a eficiência gerada pelo seu pessoal, processos e equipamento.” Pesquisas revelam que soluções eficientes de backup e recuperação reduzem em 72% o tempo gasto gerenciando backups, refazendo backups falhos e coisas do tipo, com efeitos positivos nos custos de trabalho e produtividade da equipe.

Qual é o resultado final? Melhorar sua tecnologia e processos para backup e recuperação pode ter impacto na alta disponibilidade de informação crítica para o negócio, assim como em ganhos de eficiência para a equipe de TI. (**Farre, 2012**)

2. JUSTIFICATIVA.

Identificar um sistema de backup, que atenda os seguintes requisitos operacionais da empresa GNU General Public License (Licença Pública Geral), GNU GPL ou simplesmente GPL, o sistema deve ser centralizado, possuir Interface Web, ser multi plataforma, possibilidade de gerar arquivos compactado, e criptografado, gerar log de todas as atividades executadas pelo sistema de backup, realizar a verificação e validação de todos os arquivos gerados no backup, enviar a cópia do backup realizado para outras estações remotas, realizar o restore parcial e completo dos arquivos.

3. O QUE É BACKUP.

É um termo inglês que tem o significado de cópia de segurança. É frequentemente utilizado em informática para indicar a existência de cópia de um ou mais arquivos guardados em diferentes dispositivos de armazenamento. Se, por qualquer motivo, houver perda dos arquivos originais, a cópia de segurança armazenada pode ser restaurada para repor os dados perdidos. (**Significados.com.br,2012**)

4. FERRAMENTAS.

4.1. Rsync:

É um grande aliado na hora de fazer backups ou quando é necessário sincronizar duas pastas com um grande volume de arquivos. Ele permite sincronizar o conteúdo de duas pastas, transferindo apenas as modificações. Ele não trabalha apenas comparando arquivo por arquivo, mas também comparando o conteúdo de cada um. Se apenas uma pequena parte do arquivo foi alterada, o rsync transferirá apenas ela, sem copiar novamente todo o arquivo.Ele é uma forma simples de fazer backups incrementais de grandes quantidades de arquivos, ou mesmo partições inteiras, mantendo uma única cópia atualizada de tudo em um HD externo ou num servidor remoto. Este backup incremental pode ser atualizado todo dia e complementado por um backup completo (para o caso de um desastre

acontecer), feito uma vez por semana ou uma vez por mês.Para instalar o rsync, procure pelo pacote "rsync" no gerenciador de pacotes. No Debian instale com um "apt-get install rsync" e no Mandriva com um "urpmi rsync".Para fazer um backup local, basta informar a pasta de origem e a pasta de destino, para onde os arquivos serão copiados, como em:

$ rsync -av /mnt/hda6/trabalho/ /mnt/backup/

A opção "-a" (archive) faz com que todas as permissões e atributos dos arquivos sejam mantidos, da mesma forma que ao criar os arquivos com o tar, e o "v" (verbose) mostra o progresso na tela.

A cópia inicial vai demorar um pouco, mais do que demoraria uma cópia simples dos arquivos, mas, a partir da segunda vez, a operação será muito mais rápida, já que serão copiadas apenas as mudanças.

Note que neste comando estamos copiando a pasta "trabalho" recursivamente para dentro da "/mnt/backup", de forma que seja criada a pasta "/mnt/backup/trabalho". Se omitíssemos a barra, como em "rsync -av /mnt/hda6/trabalho /mnt/backup/", o rsync copiaria o conteúdo interno da pasta diretamente para dentro da "/mnt/backup". Como pode ver, a barra final é importante dentro da sintaxe do rsync. Se algum desastre acontecer e você precisar recuperar os dados, basta inverter a ordem das pastas no comando, fazendo com que a pasta com o backup seja a origem e a pasta original seja o destino, como em:

$ rsync -av /mnt/backup/trabalho/ /mnt/hda6/trabalho

O rsync é bastante prático para automatizar backups locais, como em casos em que o servidor possui dois HDs e você deseja que o segundo armazene uma cópia completa dos arquivos do primeiro, para o caso de qualquer eventualidade. Um exemplo de script de backup simples para esta função seria:

```
#! /bin/sh

mount /dev/sdb1 /mnt/sdb1

rsync -av --delete /var/ /mnt/sdb1/ >> /tmp/rsync.logrsync -av --delete /home/ /mnt/sdb1/ >> /tmp/rsync.log

rsync -av --delete /etc/ /mnt/sdb1/ >> /tmp/rsync.log

umount /mnt/sdb1

hdparm -S 24 /dev/sdb
```

Neste exemplo, estou salvando cópias das pastas "var", "home" e "etc" na partição "/dev/sdb1", montada pelo script dentro da pasta "/mnt/sdb1". O ">> /tmp/rsync.log" faz com que a saída dos comandos seja salva no arquivo especificado, de forma que você possa verificar as mensagens no dia seguinte, em busca de erros.

O "--delete" faz com que arquivos apagados na pasta original sejam apagados também na pasta do backup, fazendo com que ela se mantenha como uma cópia fiel. Naturalmente, a opção pode ser removida do comando se o objetivo é fazer com que o backup mantenha arquivos antigos, de forma que você possa recuperá-los posteriormente, caso necessário.

Uma peculiaridade do script é que a partição é montada no início do script e desmontada no final. A ideia seria que o segundo HD fosse usado apenas para o

backup e ficasse desativado no restante do tempo, de forma que o desgaste (e a possibilidade de qualquer defeito mecânico) seja reduzido. O comando "hdparm -S 24 /dev/sdb" executado no final do script ajusta o gerenciamento de energia para o HD, fazendo com que ele entre em modo standby (onde os discos param de girar, as cabeças de leitura ficam estacionadas e apenas parte dos componentes da placa lógica ficam ativos) depois de 2 minutos de inatividade. Com isso, o HD será ativado no início da backup e ficará dormindo todo o resto do tempo, praticamente sem consumir energia. (**Morimoto, 2012)**

Fazendo a copia entre máquinas remotas, copiando o /home da máquina 172.16.1.200 para o /backup da máquina local:

rsync -avz –progress –partial -e ssh user@172.16.1.200:/home /backups

Com a opção -e o rsync utiliza como shell remoto o SSH, fazendo com que toda a transferência seja criptografada, garantindo maior segurança para o transporte dos dados.

Se quisermos que a transferência entre os hosts ocorra pelo SSH mas sem o uso de senhas, podemos estabelecer uma relação de confiança entre as máquinas utilizando chaves assimétricas.

Se você criar um script de backup com Rsync e SSH que seja executado com direito de root na máquina local faça o seguinte logado como root:

debian:~# ssh-keygen

Pode pressionar enter para tudo, isso coloca o nome padrão *id_rsa* nas chaves e dispensa o uso de senhas.

Para copiar a chave para a máquina remota faremos o seguinte:

ssh-copy-id user@172.16.1.200

Forneça a senha e isso fará com que as conexões feitas da máquina local, usando a conta de **root** para a máquina remota com a conta de **user** a autenticação será feita pelo uso das chaves e não pela senha, portanto seus scripts de backup poderão ser agendados e serem transferidos de forma segura sem que precise de alguém fornecer senha pra isso. (**Fonseca, 2012**).

4.2. Amanda:

> É comumente utilizado para realizar backup em fita, esse recurso nem sempre é econômico, já que hoje em dia HDs são muito baratos e certamente mais práticos para uma pequena empresa utilizar. É perfeitamente possível ter o Amanda realizando backups no disco rígido, O Amanda pode realizar backups completos (full) e incrementais. Você pode decidir a frequência e a retenção (por quanto tempo ficarão armazenados) desse backup de acordo com as necessidades da empresa. (**VIEIRA, 2012**).

O provedor de backup online Carbonite anunciou que está adquirindo a empresa de backup em código aberto Zmanda e vai incorporar as ofertas da empresa adquirida em seu portfólio de produtos Carbonite Business. A aquisição prevê que o nome Zmanda deve deixar de existir.

Fundado em 2005, a Zmanda dedica-se a suportar e desenvolver o projeto em código aberto para backup Amanda, oferecendo o Amanda Enterprise Edition e o Zmanda Recovery Manager para backups corporativos centralizados, além de um serviço de backup em nuvem para empresas pequenas e médias que foram baseadas nesses produtos. Versões do Amanda existem para Windows, Mac OS X, Linux e Solaris; eles oferecem backup para sistemas de arquivos de servidores e desktops. Ele também trabalha com aplicativos de servidor e produtos de base de dados como o Microsoft SQL Server, Exchange Server, SharePoint, Oracle, PostgreSQL e MySQL através de um servidor centralizado de backup, abaixo segue figura 01 do console do Zmanda (**Carbonite, 2012**)

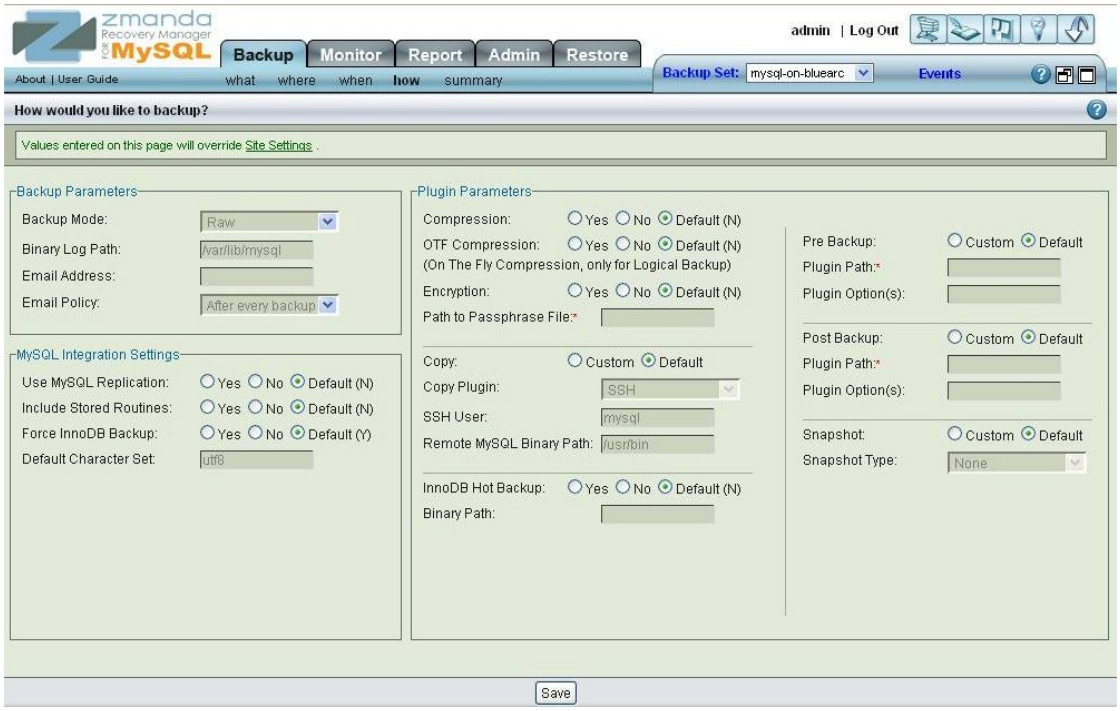

Fig. 01 Console do Zmanda

4.3. Bacula:

É um conjunto de programas que permite você (ou o administrador de sistema) administrar backup, restauração e verificação dos dados de computadores em uma rede de sistemas mistos. Em termos técnicos, o Bacula é um programa de backup em rede, conforme mostra o Figura 02 a seguir:

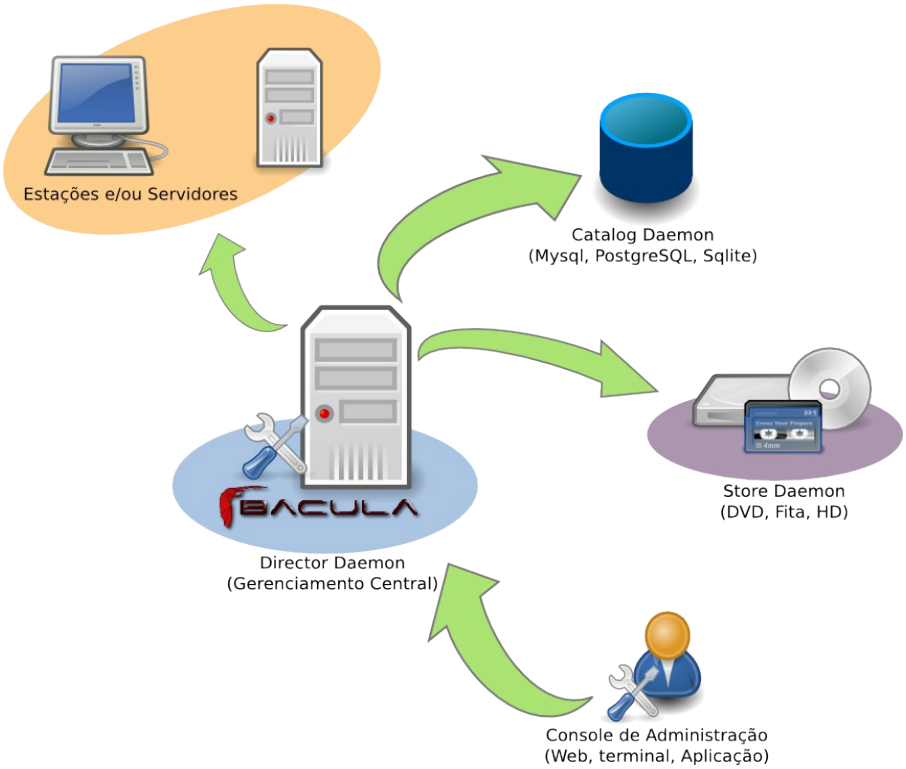

Fig. 02 sistema modular de backup

4.3.1. Bacula Director.

O programa que supervisiona todo o backup, restauração, verificação e operações de arquivo. O administrador do sistema usa o Director Bacula para agendar backups e recuperar arquivos. O Diretor é executado como um daemon (ou serviço) em segundo plano.

4.3.2. Bacula Console.

É o programa que permite ao administrador ou usuário se comunicar com o Bacula Director, podendo ser executado em qualquer computador da rede e sistemas operacionais diferentes, podendo ser executado de três maneiras, em texto puro (TTy), em Interface gráfica usando as bibliotecas do Gnome, ou as bibliotecas wxWdgets (tanto no formato Unix como em Windows).

4.3.3. Bacula-fd.

Este serviço (também conhecido como o programa Cliente) é o programa de que é instalado na máquina que será feito o backup. Ele é específico para o sistema operacional em que será instalado, e é responsável por enviar os arquivos quando solicitado pelo Director. O File Daemon também é responsável por administrar a gravação dos arquivos de restauração comandados pelo Bacula Director. Este programa é executado como um daemon na máquina que será realizado o backup. Existe daemons Unix / Linux, Windows (NT, 2000, XP, 2003 e, Me e 98)e Macintosh (OSX).

4.3.4. Bacula.sd.

É o serviço administra a gravação e a restauração dos dados e atributos dos backups fisicamente em mídias apropriadas (dispositivo de backup geralmente uma unidade de fita, CD, DVD, disco rígido, etc...).

4.3.5. Catálogo.

Software responsável pela manutenção dos índices de arquivos que são armazenados pelo backup e gerar uma base de dados dos volumes

gerenciados pelo Director. O Catálogo mantém um registro de todos os volumes utilizados, e todos os arquivos salvos, permitindo a restauração e gestão eficiente do volume. O Bacula atualmente suporta três diferentes bases de dados, MySQL, PostgreSQL e SQLite, um dos quais deve ser escolhido na instalação do Bacula (**GUSTAVO, 2012**).

5. COMPARATIVO.

Comparando as funcionalidades entre o Rsync, Amanda e o Bacula

A Fig 03 abaixo mostra um rápido comparativo entre Rsync, Amanda e o Bacula. Levando em consideração as principais características de um sistema de backup.

Pacote	Licença	Linguagem	Versão para o Windows	Versão para Mac OS X	Versão paraLinux	Interface gráfica de usuário	Interface web	Webmin módulo	Última actualização
rsync	GPL		Parcial [3]	Sim	Sim	Não	?	Opcional (downloads separados)	26 de março de 2011
AMANDA	BSD	C , Perl	Sim	Sim	Sim	Sim (com Amanda Enterprise)	?	Opcional (download separado custo +)	25 de julho de 2012
Bacula	AGPLv3.0	C + +	Sim	Sim	Sim	Sim	Sim	Sim	28 de junho de 2012

Fig 03 comparativo de funcionalidades básica

6. FUNCIONALIDADES PRINCIPAIS DO SISTEMAS DE BACKUP:

6.1. Principais tipos backup, dentre os sistemas de backup os mais utilizados são:

6.1.1. Backup de cópia, copia todos os arquivos selecionados, mas não os marca como arquivos que passaram por backup (ou seja, o atributo de arquivo não é desmarcado). A cópia é útil caso você queira fazer backup de

arquivos entre os backups normal e incremental, pois ela não afeta essas outras operações de backup.

6.1.2. Backup diário copia todos os arquivos selecionados que foram modificados no dia de execução do backup diário. Os arquivos não são marcados como arquivos que passaram por backup (o atributo de arquivo não é desmarcado).

6.1.3. Backup diferencial copia arquivos criados ou alterados desde o último backup normal ou incremental. Não marca os arquivos como arquivos que passaram por backup (o atributo de arquivo não é desmarcado). Se você estiver executando uma combinação dos backups normal e diferencial, a restauração de arquivos e pastas exigirá o último backup normal e o último backup diferencial. Ex: Se o Backup full ocorreu no sábado; um backup diferencial for realizado na segunda feira, só conterá os dados alterados ou criados na segunda feira; se na terça for gravado outro backup diferencial, ele conterá os dados gravados ou alterados desde que se gravou o backup full, isto é os arquivos de segunda e terça feira

6.1.4. Backup incremental copia somente os arquivos criados ou alterados desde o último backup normal ou incremental. e os marca como arquivos que passaram por backup (o atributo de arquivo é desmarcado). Se você utilizar uma combinação dos backups normal e incremental, precisará do último conjunto de backup normal e de todos os conjuntos de backups incrementais para restaurar os dados.

6.1.5. Backup normal(Full) copia todos os arquivos selecionados e os marca como arquivos que passaram por backup (ou seja, o atributo de arquivo é

desmarcado). Com backups normais, você só precisa da cópia mais recente do arquivo ou da fita de backup para restaurar todos os arquivos. Geralmente, o backup normal é executado quando você cria um conjunto de backup pela primeira vez.

6.1.6. A combinação de backup que utiliza uma combinação de backups normal e incremental exige menos espaço de armazenamento e é o método mais rápido para ser gravado. No entanto, a recuperação de arquivos pode ser difícil e lenta porque o conjunto de backup pode estar armazenado em vários discos ou fitas.

6.1.7. Backup que utiliza uma combinação dos backups normal e diferencial é mais longo, principalmente se os dados forem alterados com frequência, mas facilita a restauração de dados, porque o conjunto de backup geralmente é armazenado apenas em alguns discos ou fitas (**Windows Server,2012**).

6.2. CRIPTOGRAFIA.

6.2.1. Criptografia dos dados, se os dados forem expostos devido ao roubo ou perda de fitas, as empresas terão de enfrentar os danos causados à sua reputação, além da possibilidade de grandes multas de órgãos governamentais, diz Jon Oltsik, analista sênior da Enterprise Strategy Group. "Por isso recomendamos que as empresas façam da criptografia um componente padrão do seu processo de backup quando fitas são retiradas de seus escritórios". Devido à recente inundação de casos importantes em que fitas de backup roubadas ou perdidas expuseram milhares de registros de saúde e finanças confidenciais, a necessidade de criptografar os dados

sigilosos tornou-se ainda mais urgente. Existem várias opções para a execução de criptografia de backup. Algumas delas realizam a criptografia no cliente. O software realiza a criptografia de dados no cliente usando um dos vários tipos de cifras (algoritmos de criptografia), transfere os dados pela rede e os armazena em fita no formato criptografado. Para os usuários com pouca necessidade de criptografia, essa é uma boa opção. Entretanto, ela talvez não seja eficiente para empresas de grande porte com necessidades mais amplas. Outras opções, como appliances de criptografia e unidades de fita que oferecem criptografia(**Symantec, 2012**).

6.2.2. Criptografia da comunicação o principal objetivo do protocolo TLS é garantir a privacidade e a integridade dos dados em uma comunicação entre duas aplicações. O protocolo é composto de duas camadas: o protocolo de Registro (*TLS Record Protocol*) e os protocolos Handshaking (*TLS Handshaking Protocols*) . A Figura 4 apresenta a arquitetura to TLS.

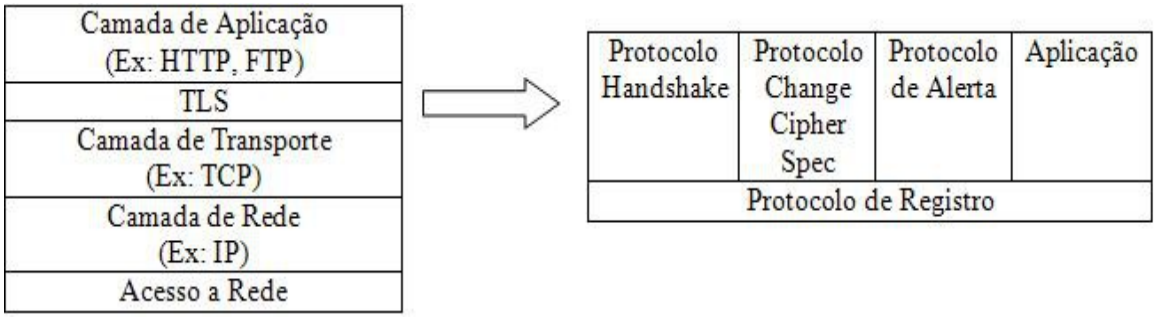

Fig. 4 Arquitetura do TLS

O primeiro se localiza acima de um protocolo de transporte confiável (por ex: TCP), provendo a segurança da conexão que apresenta duas propriedades:

6.2.2.1. A conexão é privada. É utilizada criptografia simétrica para encriptação dos dados, por exemplo. As chaves para esta encriptação simétrica são geradas unicamente para cada conexão e são baseadas em um segredo negociado (ou negociação secreta) por um outro protocolo, neste caso o protocolo Handshake. O protocolo de Registro pode ser usado sem criptografia.

6.2.2.2. A conexão é confiável. O transporte da mensagem inclui uma verificação da integridade da mensagem, utilizando uma keyed-HMAC (Hashing Message Authentication Code). Funções hash seguras são utilizadas para computação da MAC. O protocolo de Registro pode operar sem uma MAC, porém geralmente, só é utilizado desta maneira, enquanto outro protocolo está usando o protocolo de Registro como transporte para a negociação dos parâmetros de segurança. O protocolo de Registro é usado para o encapsulação de vários protocolos de níveis acima, por exemplo, o protocolo Handshake, que permite a autenticação entre cliente e servidor e a negociação de algoritmos de encriptação e de chaves criptográficas antes da transmissão ou recepção do primeiro octeto de dados por parte de um protocolo de aplicação. Os p rotocolos Handshaking provêem segurança da conexão que apresenta três propriedades:

6.2.2.2.1. A identificação de uma das partes pode ser autenticada através da criptografia assimétrica. Esta autenticação pode ser opcional, mas geralmente é exigida para pelo menos uma das partes.

6.2.2.2.2. A negociação de um segredo compartilhado é segura. O segredo

negociado fica indisponível para bisbilhoteiros, e para qualquer conexão autenticada o segredo não pode ser obtido, mesmo por um atacante que pode se colocar no meio da conexão.

6.2.2.2.3. A negociação é confiável. Nenhum atacante pode modificar a comunicação da negociação sem ser detectado pelas partes legítimas da comunicação (**Coutinho, Silva,2012**).

6.2.3. Tipos de mídias mais utilizadas.

6.2.3.1. Fitas foi o primeiro meio de armazenamento de dados removível amplamente utilizado. Tem uma capacidade razoavelmente boa de armazenamento. Entretanto, a fita tem algumas desvantagens. Ela está sujeita ao desgaste s 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. (**Morimoto, 2012**)

6.2.3.2. HD’s são uma opção muito mais atrativa, já que já existem no mercado HDs de 1 TB a preços competitivos.Surge então a figura do NAS, um servidor de arquivos dedicado, que frequentemente utiliza vários HDs em RAID de forma a obter a capacidade necessária. Além das inúmeras opções de produtos comerciais, você pode montar seu próprio NAS usando um PC com Linux. Ao utilizar um NAS, ou outro tipo de servidor de armazenamento, os backups tornam-se mais simples, pois podem ser feitos via rede. Com isso, todo o trabalho manual de trocar as fitas de armazenamento, ou plugar e desplugar HDs externos é eliminado e os backups podem se tornar um

processo inteiramente automatizado. (**Morimoto, 2012**)

6.2.3.3. Mídias ópticas. existem também os casos em que o volume de dados a armazenar é pequeno, o que torna viável utilizar DVDs ou mesmo CD-ROMs para realizar os backups. A vantagem nesse caso é que as mídias são baratas e você pode simplesmente queimar uma nova mídia a cada backup, armazenando todas as cópias antigas. Os CDs e DVDs possuem também uma boa longevidade, mídias de boa qualidade, armazenadas em um ambiente sem luz e com baixa umidade duram cerca de 20 anos ou, em muitos casos, até mais. (**Morimoto, 2012**)

7. FUNCIONALIDADES DO BACULA.

7.1. Estrutura cliente/servidor, Estrutura modular independente (director, client, database, administration console).

7.2. GPL – economia de custos com licenças, conhecimento e possibilidade de customização da ferramenta.

7.3. Inúmeros canais de suportes pela comunidade (mailing lists, forums, IRC channel, etc.)

7.4. Farta documentação disponível na Internet.

7.5. Portabilidade (módulos para diferentes sistemas operacionais – Windows, Linux, MAC, etc. – são compatíveis.

7.6. Infinidade de recursos para a customização de backups.

7.7. Funcionalidade que permite a execução de scripts (ou executáveis) antes / depois do início de jobs (backup/restore), tanto no cliente quanto servidor Bacula.

7.8. Operação via linha de comando ou GUI (inclusive, com diferentes interfaces web desenvolvidas pela comunidades. Destaques: webacula e o bacula-web – ferramentas de visibilidade gerencial, com gráficos, etc., sendo que a primeira ainda possibilita operações de backup, restore…)

7.9. Suporte a maioria dos dispositivos de storage do mercado (inclusive mídias ópticas).

7.10. Funcionalidade para o envio de mensagens de log dos trabalhos de backup/restore ou ainda instruções para o operador de backup (diferentes perfis).

7.11. 100% compatível com o esquema GFS.

7.12. Única ferramenta de backup multi-banco-de-dados.

7.13. **Pelo fato de ser livre, permite o desenvolvimento de uma série de "addons", por terceiros inclusive, potencializando os recursos da ferramenta. Inclusive, já existe plugin para o Nagios (monitoração).**

8. RELACIONAMENTO DOS MODULOS DO BACULA.

APRESENTAMOS NA FIGURA 05 DIAGRAMA DE CONFIGURAÇÃO DO BACULA-DIR.CONF COM OS PRINCIPAIS RELACIONAMENTOS COM O BACULA –FD.CONF, BACULA-SD.CONF E O BCONSOLE.CONF. (**MILK, 2012**)

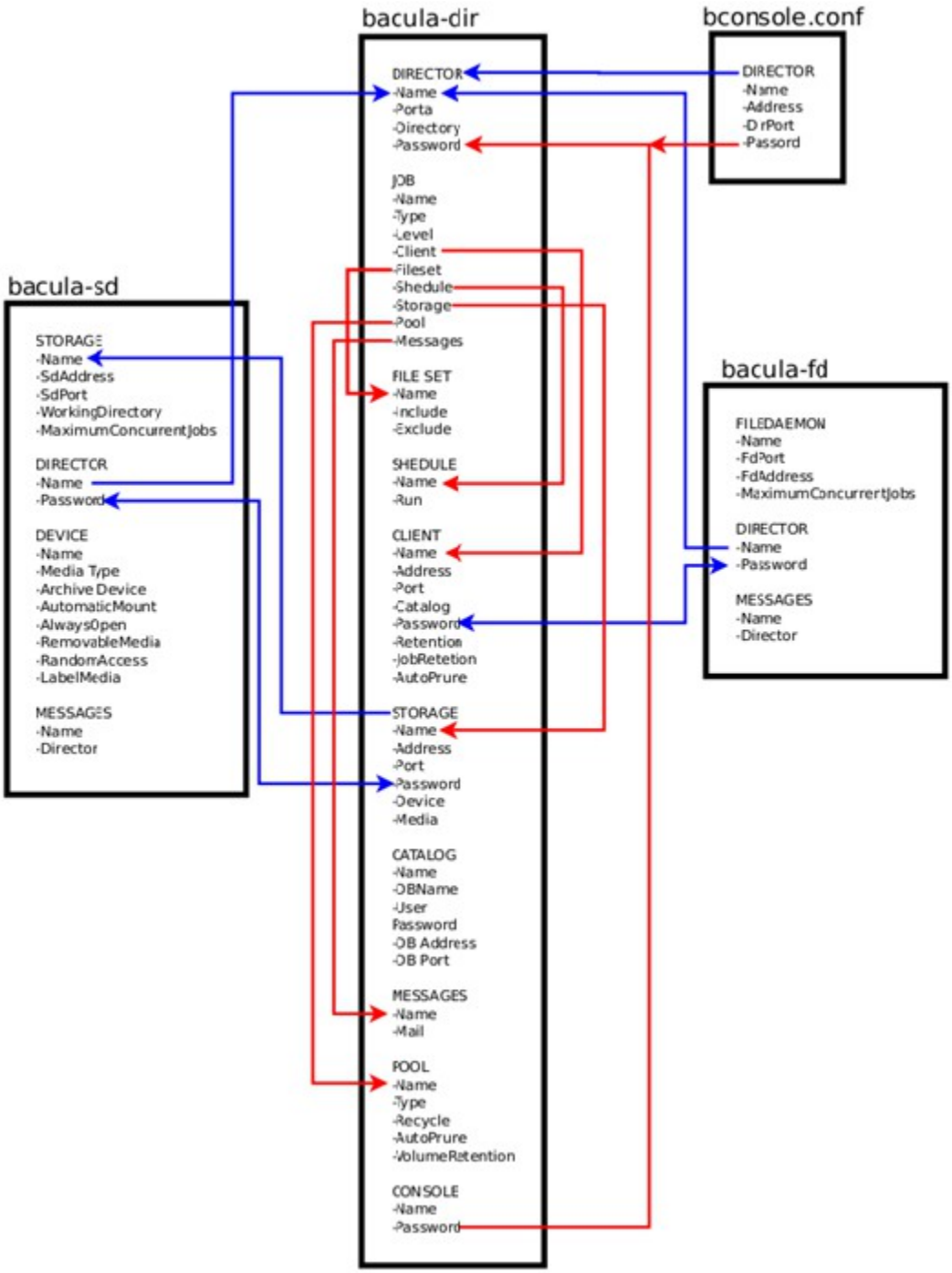

FIG. 05 DIAGRAMA RELACIONAMENTO DOS MÓDULOS DO BACULA.

9. CONFIGURANDO NOVOS CLIENTES DO BACULA.

9.1. bacula-dir.conf:

9.1.1. Criar um novo job para o cliente a ser criado.

9.1.2. Criar um novo recurso”Client”. A senha (password) será a mesma que consta do bacula-fd.conf do cliente correspondente.

9.1.3. Criar um novo “File Set”, caso os arquivos a serem “backupeados” sejam diferentes do “File Set” que já existe. Obs.: (no caso do Windows, lembrar que deve ser utilizada / (barra) ao invés de \ (barra invertida).

9.1.4. No recurso “storage”, certificar-se de que o endereço utilizado seja um IP ou de que o nome da máquina esteja num servidor DNS.

9.1.5. Reiniciar os serviços do “Bacula”.

9.2. bacula-fd.conf

9.2.1. Colocar o nome do “director”.

9.2.2. Modificar a senha que o “director” irá utilizar para se conectar ao cliente.

9.2.3. Reiniciar o “daemon” ou serviço (bacula-fd).

Obs.1: no Windows, acessar o Gerenciador de Serviços (services.msc) para reiniciar os serviços do “Bacula”.

Obs.2: caso o serviço “Bacula” no Windows termine em erro, execute o comando correspondente (botão direito no serviço, Propriedades, nestecaso retirando o trecho “/services”), na linha de comando (CMD), para visualizar a mensagem de erro (**Faria,2012**).

10. Bacula Admin Tool (Bat).

10.1. Trata-se da GUI mais avançada para o Bacula, esta interface foi desenhada para facilitar ao máximo operações de restauração em comparação ao console de texto básico como mostra a figura06

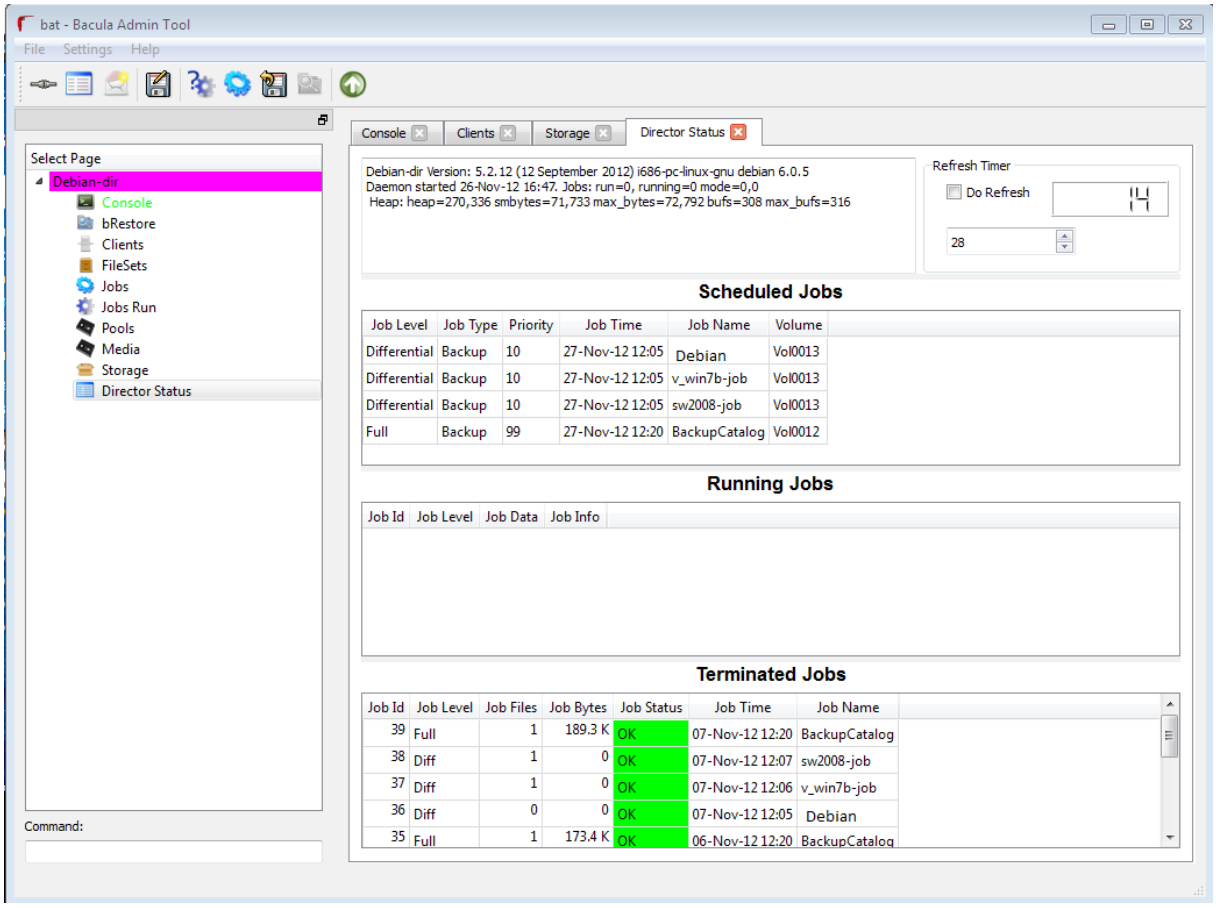

Fig. 06 Bacula Admin Tool (Bat)

10.2. Dentre as funcionalidades, é possível a submissão de Jobs, visualização de estatísticas, mudança dos estados de e atributos dos volumes, comandos como o Purge, etc. Sua instalação pode ser facilmente realizada através do comando: *# apt_get install bacula-console-qt*

11. RESTORE.

Trata se da recuperação dos dados salvos pelo backup

Bacula – restoure files. Segue abaixo figura 07 mostra o Print screen de um exemplo de restore

```
[root@file01 ~]#
bconsole

Connecting to Director director.server.world:9101
1000 OK: bacula-dir Version: 5.0.0 (26 January 2010)
Enter a period to cancel a command.
*
restore
# restore

Automatically selected Catalog: MyCatalog
Using Catalog "MyCatalog"
First you select one or more JobIds that contain files
to be restored. You will be presented several methods
of specifying the JobIds. Then you will be allowed to
select which files from those JobIds are to be restored.
To select the JobIds, you have the following choices:
     1: List last 20 Jobs run
     2: List Jobs where a given File is saved
     3: Enter list of comma separated JobIds to select
     4: Enter SQL list command
     5: Select the most recent backup for a client
     6: Select backup for a client before a specified time
     7: Enter a list of files to restore
     8: Enter a list of files to restore before a specified time
     9: Find the JobIds of the most recent backup for a client
     10: Find the JobIds for a backup for a client before a
specified time
     11: Enter a list of directories to restore for found JobIds
     12: Select full restore to a specified Job date
     13: Cancel

Select item: (1-13):


5
# select 5
```

```
Automatically selected Client: bacula-fd
Automatically selected FileSet: Full Set
+-------+-------+----------+----------+---------------------+--------------+
| JobId | Level | JobFiles | JobBytes | StartTime           | VolumeName   |
+-------+-------+----------+----------+---------------------+--------------+
|     1 | F     |        5 |      279 | 2011-05-16 22:36:32 | Vol-20110515 |
+-------+-------+----------+----------+---------------------+--------------+
You have selected the following JobId: 1
Building directory tree for JobId(s) 1 ...
3 files inserted into the tree.
You are now entering file selection mode where you add (mark) and
remove (unmark) files to be restored. No files are initially added, unless
you used the "all" keyword on the command line.
Enter "done" to leave this mode.
cwd is: /
$
ls
# show backup files

home/
$
mark home
# mark to files you'd like to restore

5 files marked.
$
lsmark
# list files which is marked

*home/
*fermi/
*.bash_logout
*.bash_profile
*.bashrc
$
done
# finished to set restoring

Bootstrap records written to /var/spool/bacula/bacula-dir.restore.1.bsr

The job will require the following
   Volume(s)                 Storage(s)                SD Device(s)
===========================================================================
```

```
   Vol-20110515          File                FileStorage

Volumes marked with "*" are online.

5 files selected to be restored.

Run Restore job
JobName:          RestoreFiles
Bootstrap:        /var/spool/bacula/bacula-dir.restore.1.bsr
Where:                 /tmp/bacula-restore
Replace:          always
FileSet:               Full Set
Backup Client:    bacula-fd
Restore Client:   bacula-fd
Storage:          File
When:                  2011-05-16 22:56:17
Catalog:          MyCatalog
Priority:         10
Plugin Options:   *None*
OK to run? (yes/mod/no):
yes
# execute

Job queued. JobId=2
*
# the results like follows are shown for few minutes later

16-May 22:59 bacula-dir JobId 2: Start Restore Job
RestoreFiles.2011-05-16_22.59.21_05
16-May 22:59 bacula-dir JobId 2: Using Device "FileStorage"
16-May 22:59 bacula-sd JobId 2: Ready to read from volume
"Vol-20110515" on device "FileStorage" (/tmp).
16-May 22:59 bacula-sd JobId 2: Forward spacing Volume "Vol-
20110515" to file:block 0:210.
16-May 22:59 bacula-sd JobId 2: End of Volume at file 0 on
device "FileStorage" (/tmp), Volume "Vol-20110515"
16-May 22:59 bacula-sd JobId 2: End of all volumes.
16-May 22:59 bacula-dir JobId 2: Bacula bacula-dir 5.0.0
(26Jan10): 16-May-2011 22:59:23
  Build OS:                    x86_64-koji-linux-gnu redhat
Enterprise release
  JobId:                       2
  Job:                         RestoreFiles.2011-05-
16_22.59.21_05
  Restore Client:              bacula-fd
  Start time:                  16-May-2011 22:59:23
  End time:                    16-May-2011 22:59:23
```

```
  Files Expected:              5
  Files Restored:              5
  Bytes Restored:              318
  Rate:                        0.0 KB/s
  FD Errors:                   0
  FD termination status:       OK
  SD termination status:       OK
  Termination:                 Restore OK

16-May 22:59 bacula-dir JobId 2: Begin pruning Jobs older than
40 years 11 months 13 hours 59 mins 23 secs.
16-May 22:59 bacula-dir JobId 2: No Jobs found to prune.
16-May 22:59 bacula-dir JobId 2: Begin pruning Jobs.
16-May 22:59 bacula-dir JobId 2: No Files found to prune.
16-May 22:59 bacula-dir JobId 2: End auto prune.

*
exit
# quit
[root@file01 ~]#
ll /tmp/bacula-restore

total 4
drwxr-xr-x 3 root root 4096 Mar 14 22:04 home
# backup files are restored
```

Fig 07 Print Screen da tela de um restore.

12. CONSIDERAÇÕES FINAIS.

Um serviço de backup pode se tornar um pesadelo para qualquer administrador de sistemas, e cabe a este apresentar e estabelecer boas práticas e normas de segurança e restauração da informação, estabelecer o uso de parâmetros e periodicidade e retenção da Informação, a definição do tempo máximo (aceitável) de retorno e restauração da base. Definir a metodologia que o plano de contingência deve abranger, levando em conta o tempo para reestruturação do ambiente, equipe técnica disponível, configuração de S.O., instalação do SGBD, restauração do Backup e/ou disponibilidade do arquivo de Backup. Com estes fatores em mente e analisando as ferramentas apresentadas concluímos que:

12.1. Rsync.

Trata-se de um comando que devidamente implementado em um script pode suprir as necessidades básica de um sistema de backup, mas devido a certas limitações da ferramenta torna-se de difícil manutenção por não ser centralizada e ter uma certa dificuldade em implementar esta ferramenta em sistemas operacionais distintos, tornou-se inviável a utilização desta ferramenta.

12.2. Amanda.

Se trata de uma ferramenta muito difundia e tem várias características essenciais para um sistema de backup como o suporte mídias tais fitas magnéticas, autochargers(robôs de fitas) e ultimamente HD’s, tem vários clientes tanto para Windows como Linux entre outros o tornaram reconhecido e citado quando se fala em backup, mas devido a falta de documentação, e ter seu

projeto meio que abandonado por vários anos, foi aos poucos perdendo lugar para outros serviços, recentemente foi divulgada uma atualização com uma nova nomenclatura Zmanda com várias atualizações, por se tratar de uma nova ferramenta reestilizada e com pouco tempo de utilização, adquirida este ano pela Carbonite, o Zmanda tornando o futuro do Amanda um tanto incerto. Descartamos esta ferramenta

12.3. Bacula

Durante as pesquisas a utilização do bacula se tornou cada vez mais propicia, por possuir um sistema modular e ser centralizado facilitando a gerencia do sistema de backup, bem como sua versatilidade de uso ser compatível com a maioria dos sistemas operacionais utilizados hoje em dia como o Linux, Freebsd, Windows Server 2003, 2008, Windows Xp, Windows7, Solaris, Mac, o suporte mídias tais fitas magnéticas, autochargers(robôs de fitas), HD's, CD's, DVD's, Pendrives o tornam bastante versátil, executar backup e restore cruzados, possuir uma fonte de documentação e farta na internet, bem como uma comunidade de desenvolvedores de plugins, ativa o tornaram apto a gerir qualquer sistema de backup.

13. REFERÊNCIAS BIBLIOGRÁFICAS.

Bacula restoure - files. 18 jul 2011 <http://www.serverworld.info/en/note?os=CentOS_6&p=bacula&f=5>
Acessado 15/10/2012

Carbonite compra a empresa de backup Zmanda

<http://www.linuxnewmedia.com.br/lm/noticia/carbonite_compra_a_empresa_de_backup_zmanda>
Acesso em: 12 nov. 2012

Faria, Heitor Medrado – Passo a passo Instalação do Bacula Server. 01/Dez/2009
<http://www.bacula.com.br/?p=151>
Acesso 20 set. 2012

Faria, Heitor Medrado – Configurando novos clientes do Bacula. 01/Dez/2009
<http://www.bacula.com.br/?p=377 >
Acesso 20 set. 2012

Farre, Tom Revisado 9/nov/2010 às 16h14. Sua estratégia para recuperação e backup mais efetiva.
<http://i.dell.com/sites/doccontent/business/smb/sb360/pt/Documents/0512-catalyst-9.pdf >
Acesso em: 27 out. 2012

Fonseca, Vagner. Backup com Rsync - 24 nov.2011
<http://www.cooperati.com.br/wordpress/2011/11/24/backup-com-rsync/>
Acesso em: 12 nov. 2012

Coutinho, Gustavo Lacerda e Silva, Renan Galvão Machado e
Redes de Computadores I Tema: SSL / TLS
<http://www.gta.ufrj.br/grad/06_1/ssl/func_tls.htm>
Acesso 05 nov. 2012

GUSTAVO, Luiz Bacula: Breve Introdução + Instalação no FreeBSD
<http://www.luizgustavo.pro.br/blog/2009/09/30/bacula-breve-introducao/>
Acesso 07 set. 2012

Jardim , Andre - Catástrofes e TI publicado 08 nov 2012
<http://www.purainfo.com.br/artigos/catastrofes-e-ti/>
Acesso 21/11/2012

MILK, Marcos Diagrama de Configuração dos Módulos do Bacula Postado em julho 25th, 2011 <HTTP://www.bacula.com.br/?p=698>
Acesso 07 nov. 2012

MORIMOTO, Carlos E. - Backup: escolhendo a mídia Revisado 10/Nov/2010 as 16:47 <http://www.hardware.com.br/ /dicas/backup-escolhendo-midia.html >
Acesso em: 13 nov. 2012

MORIMOTO, Carlos E. Revisado 9/nov/2010 às 16h14. Usando RSYNC
<http://www.hardware.com.br/dicas/usando-rsync.html >
Acesso 03 nov. 2012

Significados.com.br. O que é backup
<http://www.significados.com.br/backup/>
Acesso 29 de out. 2012

Symantec - Criptografando importantes dados de backup - 23 de Fevereiro de 2007
<http://www.symantec.com/pt/br/library/article.jsp?aid=encrypting_critical_backup_data>
Acesso 08 nov. 2012

VIEIRA, Gabriel R. Realizando backups em HD com Amanda - 22 mai. 2003
<http://www.prefirolinux.com/backups/108-realizando-backups-em-hd-com-amanda.html>
Acesso 03 nov. 2012

Windows Server. Tipos de backup
<http://technet.microsoft.com/pt-br/library/cc784306(v=ws.10).aspx>
Acesso 03 nov. 2012