UNIVERSIDADE FEDERAL DO PARÁ
INSTITUTO DE CIÊNCIAS EXATAS E NATURAIS
FACULDADE DE COMPUTAÇÃO
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO
TRABALHO DE CONCLUSÃO DE CURSO

DENISSON RONEY ALVES REIS

AVALIAÇÃO DE FERRAMENTAS DE BACKUP PARA IMPLEMENTAÇÃO EM UMA ORGANIZAÇÃO EMPRESARIAL

Belém
2018

DENISSON RONEY ALVES REIS

AVALIAÇÃO DE FERRAMENTAS DE BACKUP PARA IMPLEMENTAÇÃO EM UMA ORGANIZAÇÃO EMPRESARIAL

Trabalho de Conclusão de Curso apresentada como exigência para obtenção do grau no curso de Bacharelado em Ciência da Computação da Universidade Federal do Pará.

Orientador: Professor Dr. Raimundo Viégas Junior

Conceito: _____

Banca Examinadora:

_____

Prof. Dr. Raimundo Viégas Junior
Faculdade de Computação/UFPA (Orientador)

_____

Profª. MSc. Cassia Maria Carneiro Kahwage
Faculdade de Computação/UFPA

_____

Prof. Dr. Jefferson Magalhães de Moraes
Faculdade de Computação/UFPA

Belém
2018

DEDICATÓRIA

Dedico esse trabalho a minha família que sempre esteve ao meu lado apoiando o meu crescimento, e aos professores que encontrei durante essa caminhada que me possibilitaram obter mais conhecimento.

DENISSON RONEY ALVES REIS

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me dado capacidade para superar os obstáculos encontrados até aqui, mesmo quando achava que não ia conseguir ele me deu forças para continuar e colocou pessoas em meu caminho para me ajudar.

Agradeço a minha mãe Maria Silvina Alves Reis por estar ao meu lado em todos os momentos me mostrando que eu era capaz nunca me deixando desistir, agradeço também ao meu pai Raimundo Nonato Silva Reis que sempre me apoiou e aos meus irmãos Daniel Ruan Alves Reis e Diórgino Rigles Alves Reis que sempre estiveram ao meu lado.

Agradeço ao professor Raimundo Viegas Junior, pelo apoio e por ter acreditado em mim.

DENISSON RONEY ALVES REIS

EPÍGRAFE

“Se algum de vocês tem falta de sabedoria, peça-a a Deus, que a todos dá livremente, de boa vontade; e lhe será concedida.”

Tiago 1:5

RESUMO

Este trabalho tem a finalidade de avaliar as funcionalidades de um sistema de *backup* bem estruturado aplicando-o dentro de uma organização empresarial, demonstrando a importância da configuração, execução, testes periódicos e documentação de todo o processo e mostrado as consequências de quando o *backup* não atende as melhores praticas. Faz-se uma breve explanação sobre o que é backup e como os dados armazenados em servidores têm aumentado significativamente a sua importância. No decorrer do trabalho foram analisadas ferramentas disponíveis no mercado e três delas de software livre foram separadas para uma analise comparativa mostrando vantagens e desvantagens de cada ferramenta, dando ênfase a ferramenta de *backup* Bacula, que foi utilizada neste estudo. Ao aplicar a ferramenta dentro de uma organização em que o sistema de *backup* estava ultrapassado, as qualidades da ferramenta escolhida ficaram mais evidentes, trazendo consigo não apenas a ferramenta visto que isto já torna todo o processo mais fácil, mas também trouxe as politicas de *backup* que deixaram todos os responsáveis cientes sobre as operações realizadas e suas diretrizes para a operação adequada na organização comercial.

Palavras-chave: Cópias de Segurança, Bacula, Segurança da Informação

ABSTRACT

This paper has the goal to evaluate the functionalities of a well structured backup system in a business enterprise, showing the importance of good settings,implementation,periodic tests, documentation and records of the process. Furthermore it is demonstrated the consequences when the best practices are not followed. There is a short explanation about what is backup and how the data stored in servers significantly increased its importance. During the course of this paper, tools were analysed and three open-source software where segregated for a comparative analysis, showing the advantages and disadvantages of each. Emphasis was given to the Bacula software. When applying this tool in a business which the backup system was outdated, the Bacula qualities became more evident. Besides its main function, this tool also brought backup policies, that made all the responsible personnel aware about the performed tasks and its guidelines for the correct operation on this business enterprise.

Keywords: Backup, Bacula, Information Security

Sumário

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AD	*Active Director*
AES	*Advanced Encryption Standard*
AFP	*Apple Filing Protocol*
BAT	*Bacula Administrator Tool*
CD	*Compact Disk*
CIFS	*Common Internet File System*
CPU	*Central Processing Unit*
DVD	*Digital Video Disk*
FTP	*File Transfer Protocol*
GB	*Gigabyte*
GFS	*Grandfather-Father-Son*
GHz	*GigaHertz*
GNU	*Gnu's Not Unix*
HD	*Hard Disk*
HDD	*Hard Disk Drive*
IPv4	*Internet Protocol Version 4*
IPv6	*Internet Protocol Version 6*
ISO	*International Organization for Standardization*
LZMA	*Lempel-Ziv-Markov*
LZO	*Lempel-Ziv-Oberhume*
MB	*Megabytes*
MS	*Microsoft*
NAS	*Network-attached storage*
NFS	*Network File System*
OMV	*Open Media Vault*
RAID	*Redundant Array of Inexpensive/Independent Drives*
RAM	*Random Access Memory*
RHEV	*Red Hat Enterprise Virtualization*
ROM	*Read Only Memory*
SAN	*Storage Area Network*
SAP	*Systeme, Anwendungen und Produkte in der Datenverarbeitung*
SATA	*Serial Advanced Technology Attachment*
SHA	*Secure Hash Algorithm*
SQL	*Structured Query Language*
SSD	*Solid State Drive*
SSH	*Secure Shell*
SSL	*Secure Socket Layer*
TB	Terabytes
USB	*Universal Serial Bus*
ZFS	*Zettabyte File System*

1. INTRODUÇÃO

1.1 JUSTIFICATIVA

Com o avanço da tecnologia diversas atividades que antes eram feitas de forma manual foram automatizadas podendo ser realizadas através de aplicações que facilitam o nosso dia a dia, em todas as áreas do conhecimento, inclusive dentro de organizações e essas mesmas organizações armazenam em seus servidores dados importantes para a empresa.

Segundo o Internacional Data Corpotation (2014) estima-se que na próxima década o universo digital cresça cerca de 40% ao ano, os 4,4 zettabytes em 2013 serão 44 zettabytes em 2020, que equivale a aproximadamente 44 trilhões de gigabytes. Porém com o crescimento da quantidade e da importância dessas aplicações e dados armazenados, tornou-se necessária resguarda-las de eventuais falhas humanas e/ou mecânicas em equipamentos utilizados para conter estas aplicações e dados. Este resguardo tornou-se possível através dos sistemas de *backup*, que realizam copias de segurança dos dados armazenados nos servidores que contém estas aplicações e seus bancos de dados.

1.2 MOTIVAÇÃO

A tecnologia trouxe consigo a virtualização de muitos processos transformando dados que antes eram físicos em dados digitais, aumentando significativamente o universo cibernético, gerando inúmeros dados armazenados em servidores dentro das organizações que muitas vezes se tornam vitais para o funcionamento da mesma, devido à importância destas informações tornou-se necessária a realização de cópias de segurança, ou seja, *backup* dos dados mais relevantes, pois, caso houvesse problema com os dados principais as informações ainda poderiam ser recuperadas.

Na empresa do ramo varejista em que atuo profissionalmente houve da mesma maneira o crescimento exponencial dos dados armazenados e a importância deles aumentou significativamente sendo extremamente necessário resguardo dos dados em *backup*.

Após estudos de desempenho notou-se que a ferramenta Bacula executa tal função de *backup* com excelência, administrando as copias de segurança de maneira simples, melhorando a execução, compressão, restauração, agendamento e monitoramento dos *backups.*

A ferramenta de *backup* Bacula tornou-se objeto de estudo devido a ser uma aplicação de software livre, gratuita, customizável, com uma grande comunidade de desenvolvedores, e capaz de adapta-se as mais diversas necessidades de *backup.*

1.3 OBJETIVO GERAL

Esse trabalho tem como objetivo geral implementar e analisar dentro de uma empresa de varejo uma ferramenta que melhore a sua execução e gestão de *backups*, nos mais diversos servidores e aplicações por meio de um software de gestão de *backups*, e analisar essas melhorias, visando aprimorar a administração, verificação e restauração dos dados armazenados e demonstrar a importância de ter um sistema de *backup* bem estruturado.

1.4 OBJETIVOS ESPECÍFICOS

Este trabalho tem como objetivos específicos:

- Analisar sistemas de *backups*, mostrar o seu funcionamento, indicando seus prós e contras, mostrar a evolução desses sistemas e como eles têm ajudado nos ambientes corporativos,
- Demonstrar a importância da ferramenta Bacula dentro de uma organização, mostrando formas de gerenciar *backups* dentro de uma empresa por meio desta ferramenta e analisar a contribuição após a utilização da mesma.
- Avaliar a relevância que se tem um sistema de *backup* bem estruturado, documentado corretamente por meio das politicas de *backup*.

1.5 CONTRIBUIÇÃO DO TRABALHO

Este trabalho visa contribuir demonstrando a ferramenta de *backup* Bacula e seus benefícios e vantagens comparada à outras ferramentas disponíveis e também explicitar a importância da implantação das politicas de *backup* dentro de uma organização empresarial do ramo varejista.

1.6 ORGANIZAÇÃO DO TRABALHO

No capítulo 2, é feita uma fundamentação teórica para dar base ao trabalho onde é apresentada uma breve descrição sobre o conceito de *backup*, são explicadas de forma concisa as topologias, tipos de dispositivos de armazenamento, e expõe-se a importância desses procedimentos dentro das organizações. De maneira semelhante, no capítulo 3, trata-se de algumas ferramentas utilizadas para a realização dos *backups* destacando seus principais pontos. No capítulo 4, é descrito de maneira mais aprofundada a ferramenta Bacula. – ferramenta utilizada neste estudo. No capitulo 5, são analisadas algumas das ferramentas listadas no capitulo anterior e comparada com a ferramenta principal do estudo, verificando a facilidade de interação, facilidade de configuração, contabilizando os tempos de *backup* e de restauração de cada aplicação. No capítulo 6, é exposta a metodologia proposta para o estudo, explicitando os objetivos almejados e o benefício que a utilização da ferramenta de *backup* poderá trazer. Neste capítulo é descrito como foi realizado o modelo proposto e apresentado o modelo de avaliação que será utilizado. E por fim no capitulo 7 é explanado sobre os principais benefícios que a reestruturação trouxe, comparando a antiga estrutura de *backup* com o novo modelo implantado, foram analisados a nova topologia, o tempo de retenção, a segurança e confiabilidade para os novos *backup* realizados, a implantação das politicas de segurança e a capacidade de automação mais organizada.

2. FUNDAMENTAÇÃO TEÓRICA SOBRE SISTEMAS DE *BACKUP*

Neste capítulo serão apresentados os conceitos relacionados à pesquisa sobre o conceito de *backup*, suas topologias, tipos de *backup* realizados, tipos de dispositivos de armazenamento, a estratégia mais utilizada atualmente Grandfather-Father-Son e evidenciando como as cópias de segurança são importantes para as organizações.

2.1 O QUE É O *BACKUP*?

Backup é um processo de cópia que visa à redundância dos dados para fins de recuperação em caso de perda dos originais. Podendo essa redundância ser armazenada em diversos dispositivos tais como CD, DVD, Blue-ray, Pendrive, HD, Fita magnética, no mesmo computador dos dados originais, o que é pouco recomendado devido à possibilidade de falha mecânica neste equipamento que pode levar a perda dos originais e das cópias dos dados, ou em locais há quilômetros de distancia, através da rede de dados realizando o *backup* em nuvem (FARIA, 2014).

O *backup* visa restabelecer os dados e serviços no menor tempo possível e com a menor diferença de arquivos entre a ultima cópia salva e a ultima alteração de arquivos antes do sinistro acontecer, e este menor tempo e menor diferença é muito relativo, está diretamente relacionado com as operações realizadas pelas organizações e com a importância dos dados a serem salvos no *backup*, observando alguns critérios tais como janelas de *backup*, nem todo *backup* pode ser executado durante a operação da organização, a quantidade de exemplares de *backup* armazenados e o tempo que devem ser mantidos, pois tem um custo para se investir em armazenamento de *backups*, a compressão dos *backups*, sempre tem seus prós e contras, nem sempre a que comprime mais é a mais fácil de recuperar os dados e etc (FARIA, 2014).

As organizações possuem diversos tipos de dados e informações armazenadas em seus servidores e esse número cresce a cada dia, devido à informatização desses dados que os tornam mais acessíveis e de fácil manipulação por parte dos gestores, cabe a cada administrador analisar a criticidade desses dados e verificar quais necessitam estar em um *backup* ou não, para evitar desperdício de recursos em dados que não tem tanta importância para a organização e focar nos dados que tem mais relevância (MORAES, 2007).

2.1.1 Topologias de *backup*

Temos atualmente dois tipos de topologias de *backup*, são elas a descentralizada e a centralizada.

A topologia descentralizada normalmente é utilizada por pequenas empresas, escritórios, organizações de pequeno porte. Este tipo de topologia é quando cada servidor faz seu próprio *backup*, normalmente em fitas onde cada servidor possui seu próprio drive de fitas, podendo ser também em outros dispositivos de armazenamento conectados ao servidor, geralmente esses processos de *backup* tem sua execução mais simples e o servidor não depende de outros para a realização da operação de segurança, mas em geral o custo é mais elevado, pois necessita de um drive de fita e mais fitas para cada servidor, ou mais dispositivos de armazenamento por servidor, caso precise de sistemas de *backups* proprietários o licenciamento sairia mais caro, pois seria por servidor, pode-se ter um ambiente heterogêneo dificultando a manutenção, dificuldade nas alterações dos sistemas de *backup* devido precisar ser feita em cada servidor (GUISE, 2009).

A Figura 2.1 demonstra uma topologia de backup descentralizada, cada servidor realiza seu próprio *backup* sem o auxilio de outros servidores.

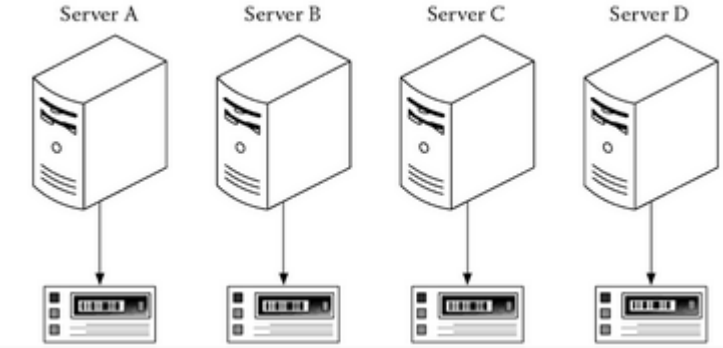


Figura 2.1: Exemplo de *backup* descentralizado.
Fonte: (GUISE, 2009).

A topologia centralizada é quando há um único servidor de *backup* que gerencia e também pode armazenar todos os *backups*, e outra forma seria um servidor central de *backup* gerenciando outros servidores de *backup*. Este tipo de topologia é utilizado na maioria das organizações devido à facilidade de administrar todos os servidores utilizados para realizar a segurança dos dados, se torna mais barato manter, pois não há a necessidade de um drive de fita para cada servidor que terá suas cópias resguardadas, nem mais dispositivos de armazenamento nesses servidores com esse proposito, normalmente possui um único sistema que realiza as copias de segurança o que gera economia caso precise de uma licença, porém geralmente possui um elevado custo inicial de implantação pois necessita de servidores e sistemas apropriados e com um bom desempenho para a administração, execução e restauração dos *backups* (GUISE, 2009).

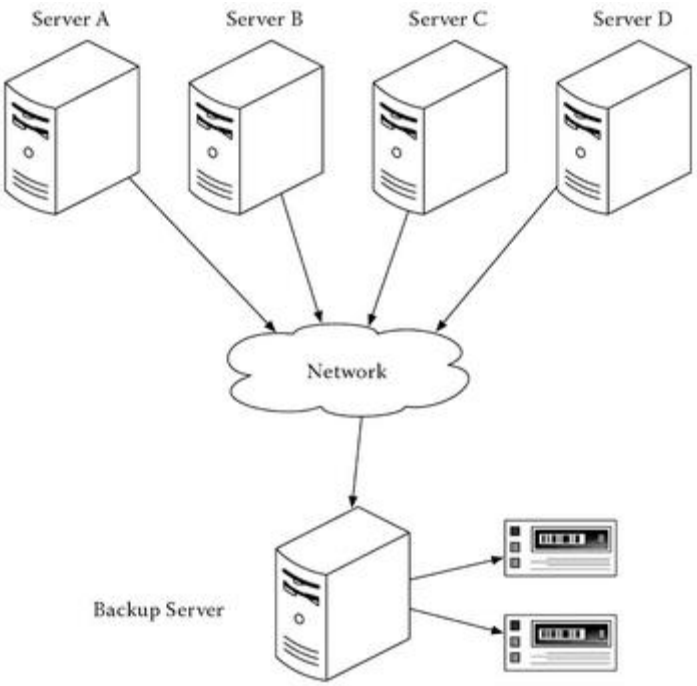


Figura 2.2: Exemplo de *backup* centralizado.
Fonte: (GUISE, 2009).

A Figura 2.2 apresenta uma topologia de *backup* centralizada onde diversos servidores tem sua estrutura de *backup* administrada por apenas um computador central.

2.1.2. Tipos de *backup*

Segundo Faria (2014) existem cinco tipos diferentes de *backup* entre eles estão:

O ***full*** uma cópia completa de todos os dados dos servidores independente de alterações realizadas nos arquivos, normalmente realizado na implantação do sistema de *backup* e no inicio de cada ciclo;

O **diferencial** realiza o *backup* dos dados alterados desde o ultimo *full* incluindo todos os dados dos diferenciais anteriores;

O **incremental** realiza o *backup* dos dados alterados desde o ultimo diferencial, porém um *backup* incremental não possui os dados alterados e salvos no incremental anterior;

A **cópia** que é uma redundância do *backup* que não poderá ser alterada e deve ser guardada separadamente;

E por fim a **migração** quando dados são copiados de uma mídia para outra normalmente quando há suspeitas de problemas na mídia original.

2.1.3 Dispositivos de armazenamento de *backup*

Faria (2017) explica os três principais dispositivos utilizados para armazenar os dados de um *backup*, são eles:

Fitas magnéticas: Possuem uma ótima confiabilidade e baixo custo, porém o uso ideal das fitas magnéticas é em conjunto com um robô de fitas que é bem mais dispendioso em relação a valores, pode ser usado apenas com um drive de fitas para fazer a compressão, leitura ou escrita nas fitas, mas deve ser evitado, pois necessitará de intervenção manual para fazer a troca de fitas.

Possuem velocidades de gravação similares aos discos rígidos entre 80 MB/s e 300 MB/s dependendo da geração da fita e quanto à restauração granular pode se tornar um pouco mais lenta dependendo da posição dos dados na fita.

Discos rígidos: Houve uma grande melhora na confiabilidade dos discos rígidos e o seu valor por gigabyte reduziu significativamente o que levou a diversas organizações adotarem como mídia de *backup* principal.

Podem fazer varias operações ao mesmo tempo, por exemplo, leitura e escrita facilitando a realização e restauração de *backups*. Possui velocidade de gravação que varia de 80-200 MB/s dependendo do modelo de disco rígido

SSD: Ainda possui um alto custo de investimento, mas que pode futuramente se tornar viável para as organizações, tem uma alta durabilidade e sua velocidade é superior à maioria das fitas magnéticas e discos rígidos, atualmente pode ser usado como área de transição entre o cliente e a mídia de *backup* final que pode ser fita, disco rígido, entre outros.

A velocidade de gravação do SSD pode variar de 200 MB/s a 550 MB/s dependendo do modelo.

2.1.3.1 NAS (*Network Attached Storage*).

Conforme Somasundaram, Shrivastava e EMC Education Services (2011) algo crescente dentro das organizações são os servidores de armazenamento, que normalmente contem rolos de fita e/ou blocos de discos que utilizam um sistema operacional especifico para gerencia-los, tornando assim um armazenamento inteligente não apenas transferindo dados, mas também armazenando as informações dessas transferências facilitando assim a administração, e um dos mais utilizados são as soluções NAS(*Network Attached Storage*).

Duas das mais conhecidas soluções NAS de software livre são o Open Media Vault e o Freenas:

O Open Media Vault é uma solução baseada no sistema operacional Debian Linux com suportes a diversos protocolos entre eles o SSH, FTP, NFS, SMB, Rsync entre outros. Possui uma interface gráfica via web que facilita a administração, tem suporte aos mais conhecidos sistemas de arquivos e tem um fácil sistema de atualizações por utilizar pacotes Debian (Open Media Vault, 2018).

Outra solução de software livre é o Freenas que também trabalha com os principais serviços como SMB, CIFS, NFS e AFP que permite compartilhamento de arquivos com os mais diversos sistemas operacionais. Possui uma interface de gerenciamento web e trabalha com os principais protocolos de transferência SSH e FTP (Freenas, 2018).

2.2 ESTRATEGIA GFS (GRANDFATHER-FATHER-SON).

Segundo Faria (2014) a estratégia Grandfather-Father-Son é a mais comum entre os administradores de *backups* que visa a economia de dispositivos de armazenamento e a segurança dos itens do *backup*, por meio de uma rotatividade desses dispositivos, normalmente feito com fitas de *backup*.

O esquema mais simples de GFS baseia-se em três tipos de *backup*, contendo um backup diário, semanal e mensal, sendo um conjunto de fitas para cada tipo de *backup*, abaixo na Figura 2.3 um exemplo simples da estratégia GFS.

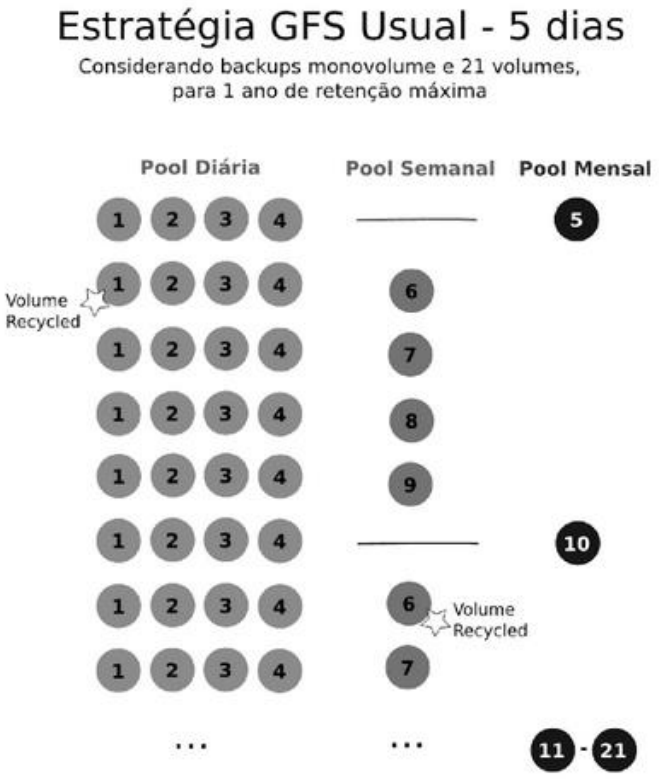


Figura 2.3: Exemplo de estrategia GFS.
Fonte: (FARIA, 2014).

Este esquema consiste em quatro fitas para os backups diários (filho) que serão revezadas diariamente durante quatro dias da semana, no quinto dia será feito o primeiro mensal (avô), na semana seguinte será realizada a inserção e revezamento das diárias novamente e no quinto dia será feita a semanal (pai), essa semanal será feita sempre ao quinto dia de cada semana durante quatro semanas, até iniciar um novo ciclo com uma mensal. Com o uso de vinte e uma fitas nesse esquema tem-se a retenção de *backups* durante um ano (FARIA, 2017).

2.3 A IMPORTÂNCIA DOS SISTEMAS DE *BACKUP* NO ÂMBITO ORGANIZACIONAL.

A perda de dados importantes para a empresa pode levar a dificuldades nas tarefas diárias ou até mesmo paralisação nos serviços, um grande exemplo disso foram os atentados às torres gêmeas em 11 de setembro de 2011 nos Estados Unidos, onde muitas empresas por guardarem seus *backups* no mesmo prédio dos originais ou até na outra torre, perderam muitos dos seus dados essenciais para o funcionamento das tarefas fundamentais da empresa e por esse motivo diversas empresas declararam falência (MORAES, 2007).

Além de documentos diários produzidos pela empresa que precisam ser preservados, também há aqueles documentos necessários para as fiscalizações e auditorias do governo, documentos que a organização precisa obrigatoriamente guardar, pois se ao serem requisitados não forem apresentados, a empresa pode ser multada ou até impedida de funcionar, documentos como notas ficais de venda ou compra de produtos ou serviços, notas fiscais de transporte de produtos entre outros conforme ajuste realizado pelo Sistema Integrado Nacional de Informações Econômico-Fiscais em 30 de setembro de 2005 no art. 199 do código tributário nacional, que necessitam ser mantidos para que futuramente não gerem ônus a organização.

Cada empresa tem diferentes necessidades na hora da realização de *backup*, uma janela de *backup* que seja diferente do tradicional que é à noite, um tempo de retenção que pode ser mais curto ou mais longo, meses ou apenas dias, o tipo de compactação que pode ser maior ou menor, dependendo do espaço disponível nos servidores, entre outras coisas, mas o que a maioria dos estudiosos e profissionais em segurança da informação recomendam é que a empresa ou organização faça um estudo profundo sobre as suas necessidades de *backup*, planejando de maneira que não haja um excessivo gasto de recursos gerando um ônus para quem o financia e nem que haja uma despreocupação com o *backup* não investindo ou

subestimando de maneira que tenha um sistema de *backup* falho que não supre as necessidades da organização.

Para Faria (2014), as organizações devem seguir algumas boas praticas de *backup*, tais como, ter uma politica de *backup* bem definida, documentando como serão realizadas as rotinas de backup, a topologia utilizada, os servidores que estarão inclusos, os responsáveis pela administração, quais dispositivos de armazenamento serão utilizados e etc; outras politicas a serem adotadas são o *backup* condizer com a realidade da organização; realizar testes constantes de recuperação do conteúdo salvo, observando se este conteúdo está de acordo com o tripé de segurança da informação que são confidencialidade, integridade e acessibilidade; descartar de forma adequada os dispositivos utilizados para a realização dos *backups*, para que não haja um posterior *restore* indesejado por terceiros, e a organização precisa se adequar a norma ISO 27002 que trata sobre boas praticas de gestão de segurança da informação.

De acordo com a ISO 27002 (2013, p. 63).

> **12.3 Cópias de segurança**
>
> Objetivo: Proteger contra a perda de dados
>
> **12.3.1 Cópias de segurança das informações**
>
> **Controle**
>
> Convém que cópias de segurança das informações, softwares e das imagens do sistema, sejam efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida.
>
> **Diretrizes para implementação**
>
> Convém que a política de *backup* seja estabelecida para definir os requisitos da organização relativos às cópias de segurança das informações, dos softwares e dos sistemas.
>
> Convém que a política de *backup* defina os requisitos para a proteção e retenção.
>
> Convém que os recursos adequados para a geração de cópias de segurança sejam disponibilizados para garantir que toda informação e *software* essenciais possam ser recuperados após um desastre ou a falha de uma mídia.
>
> Quando da elaboração de um plano de *backup*, convém que os seguintes itens sejam levados em consideração:
>
> a) registros completos e exatos das cópias de segurança e documentação apropriada sobre os procedimentos de restauração da informação, os quais convém que sejam produzidos;
>
> b) a abrangência (por exemplo, completa ou diferencial) e a frequência da geração das cópias de segurança reflitam os requisitos de negócio da

organização, além dos requisitos de segurança da informação envolvidos e a criticidade da informação para a continuidade da operação da organização;

c) convém que as cópias de segurança sejam armazenadas em uma localidade remota, a uma distância suficiente para escapar dos danos de um desastre ocorrido no local principal;

d) convém que seja dado um nível apropriado de proteção física e ambiental das informações das cópias de segurança (ver 11), consistentes com as normas aplicadas na instalação principal;

e) convém que as mídias de *backup* sejam regularmente testadas para garantir que elas são confiáveis no caso do uso emergencial; Convém que isto seja combinado com um teste de restauração e checado contra o tempo de restauração requerido. Convém que os testes da capacidade para restaurar os dados copiados sejam realizados em uma mídia de teste dedicada, não sobrepondo a mídia original, no caso em que o processo de restauração ou *backup* falhe e cause irreparável dano ou perda dos dados;

f) em situações onde a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação.

Convém que cópias de segurança de sistemas e serviços específicos sejam testadas regularmente para garantir que elas estão aderentes aos requisitos definidos nos planos de continuidade do negócio. Para serviços e sistemas críticos, convém que sejam criados mecanismos de geração de cópias de segurança que abranjam todos os sistemas de informação, aplicações e dados necessários para a completa recuperação do sistema em um evento de desastre.

O período de retenção para informações essenciais ao negócio e também qualquer requisito para que cópias de arquivo sejam permanentemente retidas, contém que seja determinado.

2.3.1 Erros comuns referentes a *backup*.

Um grande erro que gestores cometem é tentar valorar um sistema de *backup* sem antes consultar o histórico prévio de desastres e quanto seria recuperado caso tivesse um sistema eficiente, porém não se pode prever se a organização irá precisar futuramente e/ou o quanto irá precisar, isto torna algo praticamente impossível de se calcular o retorno do investimento. O correto é que o investimento feito em sistemas de *backup* com maquinas, licenças, mídias de backup tais como fitas magnéticas, HD’s e etc, tem que ser tratado como uma apólice de seguros, não é possível estimar quando se irá precisar, mas com o sistema de backup eficiente é possível realizar a recuperação com êxito (FARIA, 2014).

Outro erro comum quando se fala em *backup* é confundi-lo com um sistema de tolerância a falhas, normalmente feito por meio de redundância de discos ou servidor cópia,

que ao ocorrer as falhas o outro disco ou outro servidor assume o serviço, o *backup* é um sistema de recuperação após a falha, mesmo que o sistema de redundância falhe os dados ainda poderão ser recuperados por meio do *backup* (FARIA, 2014).

3. SISTEMAS DE *BACKUP* UTILIZADOS ATUALMENTE

3.1 O QUE EXISTE DE SISTEMAS DE *BACKUP*?

Neste capitulo, serão abordadas as ferramentas de sistemas de *backup* que são utilizadas atualmente no mercado mundial, foram selecionadas ferramentas que tivessem grande comunidade e material disponíveis, sendo essas ferramentas proprietárias ou não, com arquiteturas distribuídas e/ou centralizadas, entre elas estão:

3.2 A FERRAMENTA DE *BACKUP* BAREOS

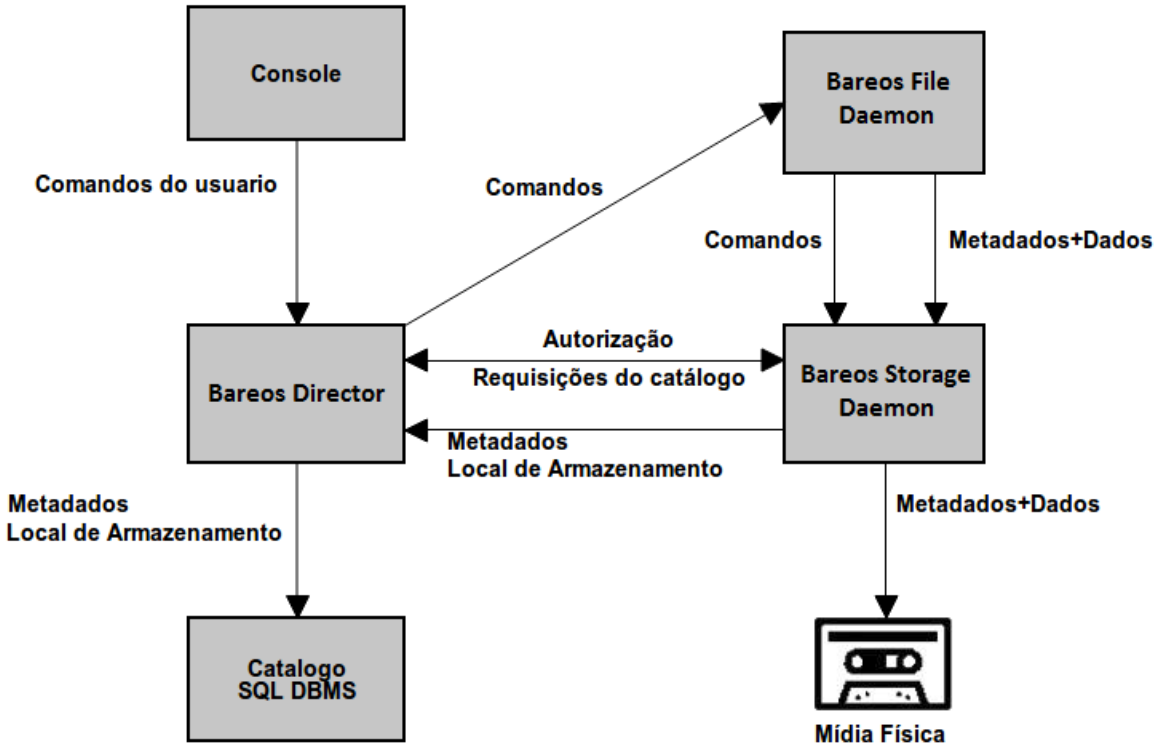


Figura 3.1: Diagrama mostrando o fluxo de trabalho do BAREOS.
Fonte: BAREOS (2017).

BAREOS (Backup Archiving R**e**covery Open Sourced) é um conjunto de programas desenvolvido em 2010 como uma dissidência do Bacula, de código aberto responsáveis por gerenciar *backup*. Por ser de código aberto é possível realizar adaptações as mais diferentes necessidades de *backup* (Bareos, 2017).

A Figura 3.1 mostra as interações entre os programas do BAREOS onde o *Director* administra os fluxos por meio de comandos recebidos via console gráfica ou texto enviando informações para o *file daemon*, que por sua vez envia os dados dos diretórios pré-configurados para o *storage daemon* e registra as interações no catálogo (Bareos, 2017).

No que se refere à recuperação de *backup* o BAREOS possui um catálogo onde são registradas todas as interações realizadas pelo *Director* o que torna a restauração rápida e eficiente, e tem a facilidade de seu catálogo ser compatível com 3 diferentes bancos de dados MySQL, PostgreSQL e SQlite. Seu cliente o *file daemon* e compatível com os sistemas operacionais mais conhecidos atualmente Linux, Unix, Windows e Mac OS o que permite ser configurado para uma rede heterogênea (Bareos, 2017).

3.3 A FERRAMENTA DE *BACKUP* AMANDA

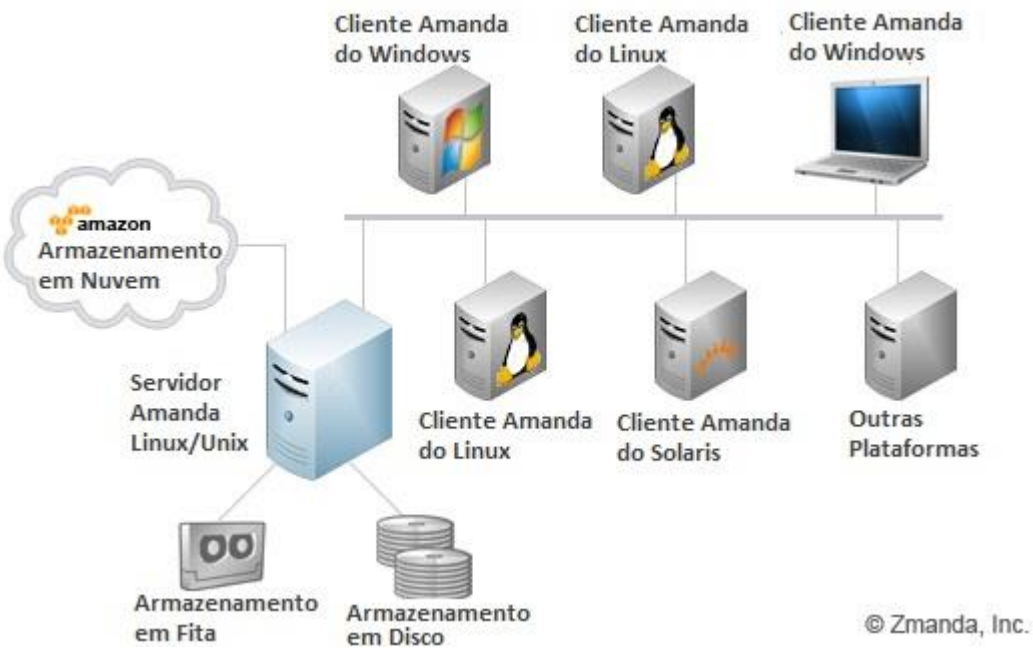


Figura 3. 2: Topologia AMANDA com cliente de diversos sistemas operacionais.
Fonte: http://amanda.zmanda.com/ **(2017)**.

A Figura 3.2 mostra a topologia cliente/servidor do sistema de *backup* Amanda e os mais diversos sistemas operacionais que possuem o cliente Amanda homologado, podendo realizar *backups* em fita, disco e em nuvem, não necessariamente em apenas uma dessas opções, mas também pode ser um *backup* hibrido realizado em mais de uma dessas opções de armazenamento (Zamanda, 2017).

O Amanda (Advanced Maryland Automatic Network Disk Archiver) é um Sistema de *backup* de código aberto desenvolvido em 1992 por James da Silva do departamento de ciência da computação da Universidade de Maryland, e possui uma grande comunidade de

desenvolvedores, seu código está disponível para plataformas Unix e utiliza diversas ferramentas nativas como GNU tar para compactar os dados, Crontab para agendar os *backups* e o Samba para se comunicar com clientes Windows (Preston, 1999).

Por usar ferramentas nativas do Unix a recuperação dos *backups* não depende necessariamente de ter o Amanda instalado, pode-se recuperar apenas utilizando as ferramentas nativas, Amanda utiliza inclusive drives nativos facilitando a comunicação com dispositivos de armazenamento e referindo-se a segurança é possível criptografar os dados no cliente antes de serem enviados ao servidor suportando criptografia de chave publica de 4096 bits (Zamanda, 2017).

3.4 A FERRAMENTA DE *BACKUP* BACKUP EXEC

O Backup exec é um sistema de *backup* proprietário com seu servidor disponível apenas para plataformas Windows e com clientes disponíveis para os sistemas operacionais mais utilizados atualmente Linux, Windows e Mac OS inclusive administradores de maquinas virtuais o VMware e o Hyper-V, possui uma console gráfica de administração intuitiva e que não precisa necessariamente estar instalada no servidor do Backup exec, facilitando a administração, trabalha com a topologia de *backup* centralizada suportando diversos tipos de armazenamento como fitas, discos ou em nuvem se adaptando as mais diferentes necessidades da organização (Veritas, 2017).

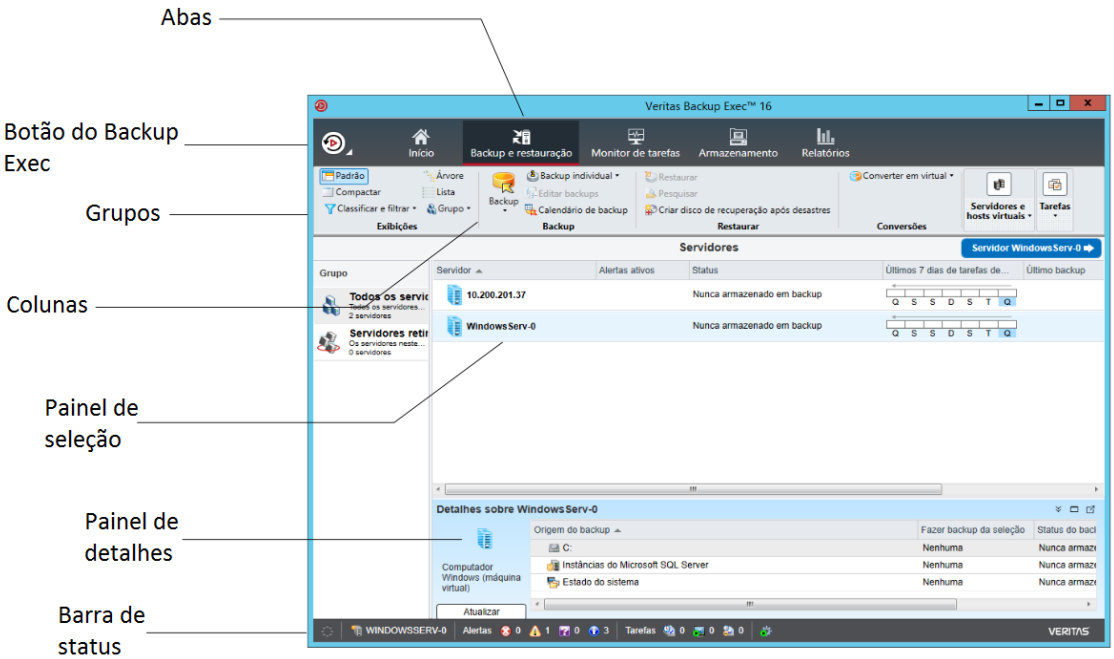


Figura 3.3: Console de administração do Backup exec
Fonte: (VERITAS, 2017).

O Backup Exec possui gerenciamento de ciclo de vida automatizado para que não seja sobrescrito dados antes do fim do seu ciclo, deduplicação de dados que otimiza a utilização do armazenamento, replicação de dados o que torna mais eficiente a tolerância a falhas e possui a capacidade de restaurar um sistema operacional completo, toda operação de *backup* realizada pelo Backup Exec é registrada em um catalogo facilitando na administração e na recuperação dos *backups* e possui suporte à redes IPV4 e IPV6 (Veritas, 2017).

A Figura 3.3 mostra a console gráfica de administração do Backup Exec rotulando os principais campos disponíveis.

3.5 A FERRAMENTA DE *BACKUP* ARCSERVE

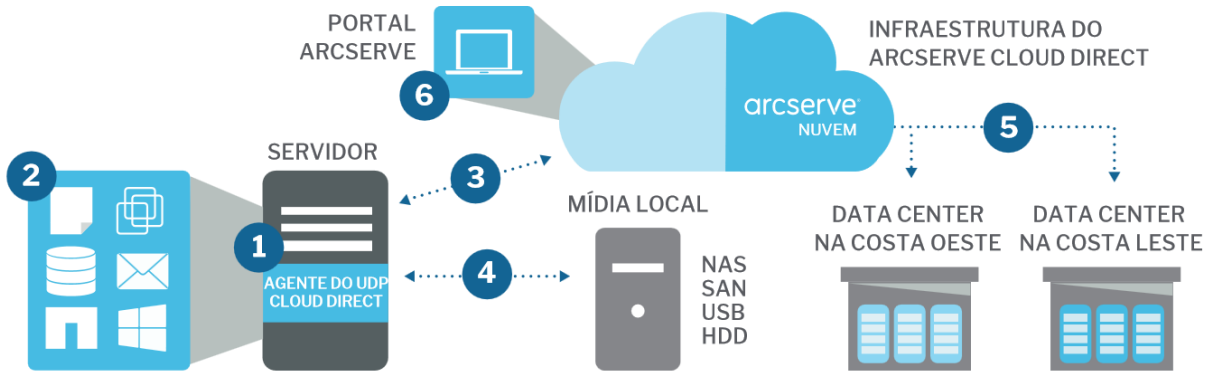


Figura 3.4: Topologia do Arcserve realizando backup local e em nuvem.
Fonte: Arcserve ficha tecnica (2017).

O Arcserve é uma ferramenta de *backup* proprietária com seu maior foco em *backup* em nuvem em seus *data center's*, porém também realiza cópias locais via NAS, SAN, USB e HDD conforme Figura 3.4, possui uma interface de administração *web* que facilita o gerenciamento, tem suporte para os principais sistemas operacionais Windows, Linux, Mac e também para os principais gerenciadores de maquinas virtuais VMware e Hyper-V, possui criptografia com chave publica e privada, por SSL quando os *backups* estão sendo copiados e AES enquanto estão armazenados (Arcserve, 2017).

A replicação dos dados em nuvem torna o sistema mais tolerante a falhas e acaba gerando um sistema com alta disponibilidade, possuindo a capacidade de resguardar desde simples arquivos até imagens completas de sistemas operacionais, com a gerencia centralizada via *WEB* podendo ser feita a administração em qualquer localidade com acesso a internet (Arcserve, 2017).

Segundo Faria (2014) o Arcserve tem um custo elevado devido a cada novo modulo necessitar de um novo licenciamento e cada licença servir apenas para um sistema especifico causando uma dependência e precisa necessariamente de um servidor robusto para que tenha um desempenho aceitável.

3.6 A FERRAMENTA DE *BACKUP* ZBACKUP

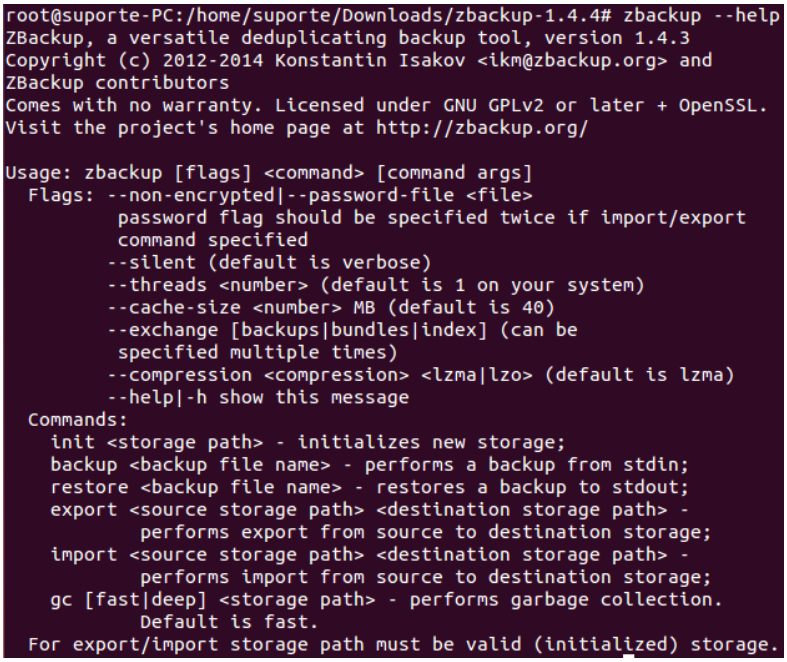


Figura 3.5: Console texto Zbackup
Fonte: Elaborada pelo autor

Este sistema de *backup* utiliza a licença GNU GPLv2, por tanto é um software gratuito e código aberto escrito na linguagem de programação C++ e tem seu projeto compartilhado no GitHub onde pode facilmente receber contribuições de outros desenvolvedores (Zbackup, 2018).

O Zbackup tem seu foco na deduplicação byte a byte dos dados que reduz significativamente o tamanho dos *backups*, tendo dados iguais faz-se o *backup* apenas de um, possui dois parâmetros de compactação o LZO que é rápido devido a sua taxa de compressão ser baixa e o LZMA que por causa da alta taxa de compressão demora mais em relação ao LZO, utiliza criptografia opcional AES para transporte dos dados em segurança e trabalha com a soma SHA256 para verificação da integridade de cada *backup* realizado (Zbackup, 2018).

A Figura 3.5 mostra o Zbackup sendo executado pela console texto do Linux com a *flag* help para mostrar os principais comandos para administração do sistema, tais como o comando backup para executar um novo *backup* de um diretório pré-configurado e o comando

restore para restaurar *backup*, possui também *flags* que especificam o tipo de compressão a ser utilizada e se desejam ou não criptografar os *backups*.

3.7 A FERRAMENTA DE *BACKUP* RDIFF-BACKUP

O Rdiff-backup é uma ferramenta de backup que possui suporte para os 3 mais conhecidos sistemas operacionais Linux, Windows e MAC OS. Uma das suas principais características é o versionamento de arquivos, ele guarda diferentes versões do mesmo arquivo pelos dias configurados pelo administrador, no local onde os *backups* serão armazenados faz o espelhamento dos dados e cria um diretório de versionamento dos mesmos dados onde armazena apenas as alterações realizadas. Diferente de um *backup* incremental convencional que inclui no *backup* apenas os arquivos modificados desde o ultimo, o Rdiff-backup utiliza o librsync para enviar apenas os dados modificados de um arquivos e não o arquivo completo, dessa maneira economizando também largura de banda caso seja um *backup* remoto(Rdiff-backup, 2018).

```
#!/bin/bash

echo "Iniciando rdiff-backup..."  `date` >> /home/rdiff.log
rdiff-backup --force /dados /backup
echo "Backup finalizado..."  `date` >> /home/rdiff.log
```

Figura 3.6: Script para execução via console do Rdiff-backup
Fonte: Elaborada pelo autor

Na Figura 3.6 vemos um exemplo básico de *script* para a execução do Rdiff-backup criando um *log* que indicará o momento da inicialização e o momento do encerramento do *backup* com a data e a hora que foram realizados, sendo ele feito do "/dados" para o "/backup", com o parâmetro "--force" para que o destino seja configurado conforme as especificações do Rdiff-backup.

4. O BACULA

4.1 DESCRIÇÃO

Bacula é um sistema que reúne vários programas e permite gerir *backups*, copiar dados, verifica-los e restaura-los. Esses diversos programas ou módulos podem estar em um único servidor ou espalhados pela rede, são eles *Director Daemon*, *Console Manager*, *File Daemon*, *Storage Daemon*, *Catalog* (FARIAS, 2014), que serão melhor explicados logo abaixo:

4.1.1. *Director Daemon*

Este módulo gerencia todo o sistema de backup, ele é o responsável por enviar as requisições de backup e de *restore*. Ele é que solicita a cópia, restauração e verificação dos dados solicitados pelo administrador, tornando possível também a automação das operações de *backup* (FARIAS, 2014).

4.1.2. *Console Manager*

Este módulo é a interface pela qual o administrador se comunica com o sistema, podendo ser interface de texto ou interface gráfica utilizada tanto em Linux quanto em Windows, não necessitam estar instaladas diretamente no servidor que possui o *Director* instalado. (FARIAS, 2014).

4.1.3. *File Daemon*

Este é o modulo cliente do Bacula, é o que recebe as requisições de *backup* e envia os dados solicitados para serem armazenados no *Storage Daemon*, contém versões para diversos sistemas como Linux, Windows, MAC, entres outros (FARIAS, 2014).

4.1.4. *Storage Daemon*

Modulo responsável por armazenar os dados enviados pelo *File Daemon*, encarregado pela gravação e restauração destes dados nos diversos dispositivos de armazenamento tais como HD, fitas magnéticas, DVD ou CD (FARIAS, 2014).

4.1.5. *Catalog*

Modulo que contem o banco de dados dos Bacula, responsável por indexar os dados gravados tornando mais fácil e rápida a busca por arquivos no momento da restauração (FARIAS, 2014).

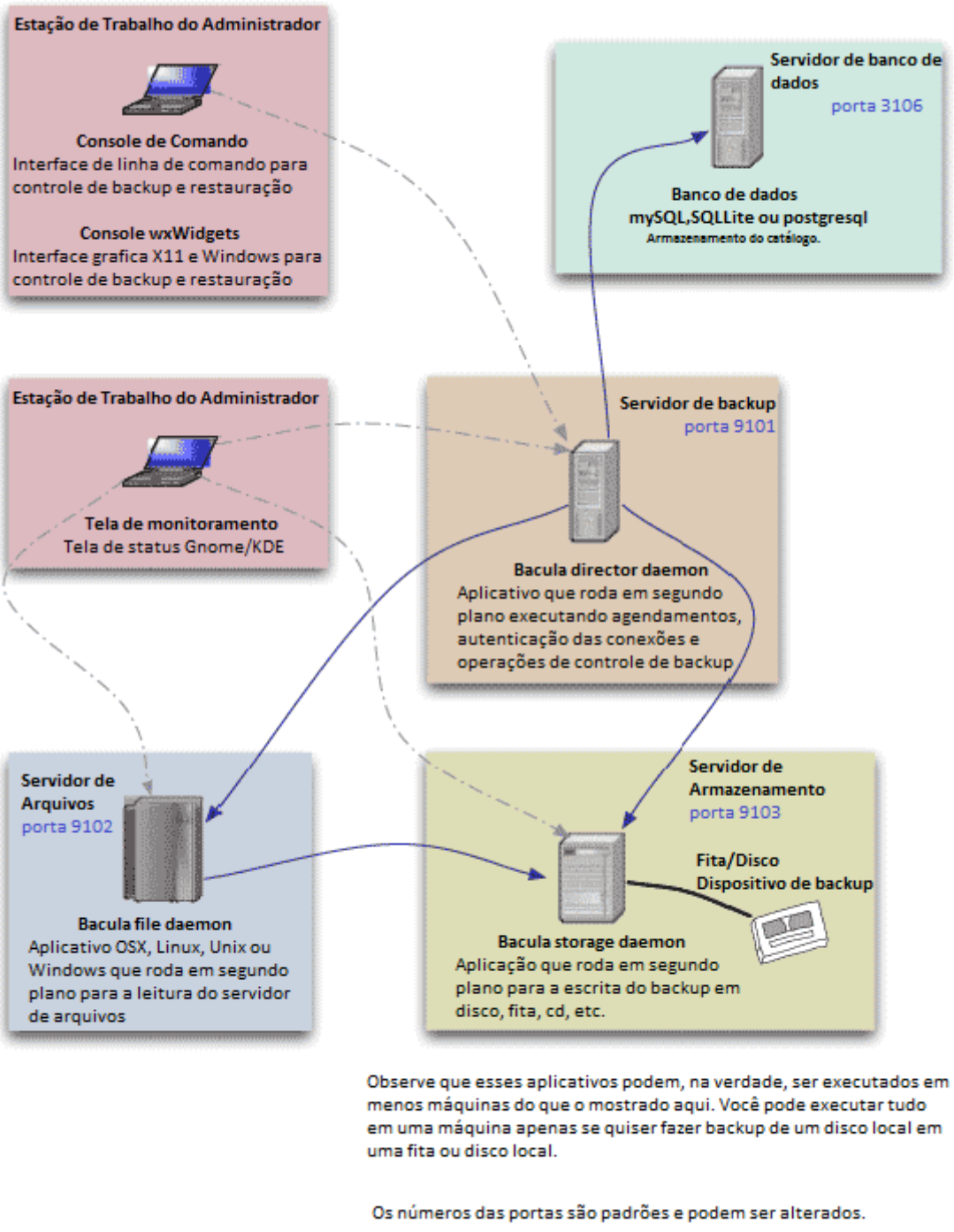


Figura 4.1: Exemplo do funcionamento dos diferentes módulos do bacula.

Fonte: (FARIAS, 2014)

A Figura 4.1 demonstra as iterações entre os módulos do Bacula, onde a estação de trabalho do administrador que contém uma console gráfica ou por linha de comando do Bacula se conecta ao Director que por sua vez se comunica com o File Daemon enviando informações de quais dados devem ser enviado para o Storage Daemon e o Director também envia ao servidor de banco de dados as ações realizadas, o Storage Daemon recebe esses dados armazenando-os em fitas, discos rígidos, pendrives entre outras mídias de armazenamento (FARIAS, 2014).

4.2. CARACTERÍSTICAS DO SISTEMA DE *BACKUP*

O Bacula possui um modelo cliente servidor onde o *Director* é o modulo que determina as ações realizadas pelos demais módulos, como dito anteriormente é um programa com um conjunto de módulos que se interligam, desenvolvido em c e c++ sob a licença GPL (General Public License) uma licença de software livre e de código aberto que torna possível a customização, reduz os gastos com licenciamento e torna possível um melhor conhecimento sobre a ferramenta, possui uma vasta comunidade e fóruns com documentações e suporte sobre a aplicação de *backup*, possui clientes para os mais conhecidos sistemas operacionais como Linux, Windows e MAC OS, sua interface de administração se da tanto via linha de comando quanto pelo Bat aplicação utilizada para administração e por interface web e por ultimo tem a possibilidade de enviar logs e instruções sobre atividades realizadas na aplicação(FARIA, 2014).

O Bacula possui suporte para diversos gerenciadores de bancos de dados como MySQL, PostgreSQL e SQlite e para cada banco de dados existem pacotes diferentes para a instalação do bacula-sd e do bacula-dir, os requisitos de *hardware* exigidos pela aplicação são baixos possibilitando ser executado tanto em servidores com baixas configurações de *hardware* quanto em servidores robustos (FARIA, 2014).

4.3. SUPORTES DO BACULA

Segundo Bacula (2017) a aplicação possui suporte para:

- Armazenamento S3 na Amazon, para realização de backup em nuvem.
- Seu agente possui suporte para diversas aplicações, bancos de dados e sistemas operacionais tais como: MS SQL, SAP, POSTGRES, DB2, MYSQL, AD, HYPERV, KVM, PROXMOX, RHEV, XEN, VMWARE, LINUX, APPLE, WINDOWS SERVER, EXCHANGE, FTP.

- Seu processo de deduplicação dos dados pode ocorrer tanto no cliente como no servidor checando se há dados repetidos para assim evitar a redundância de *backup*.
- Realiza *backup* incremental, diferencial, completo e baremetal.
- Tem suporte para diversos tipos de armazenamento entre eles são *backup* em nuvem, remoto, CD, DVD, HD, fita, NAS.
- É uma aplicação *multi thread*, ou seja, realiza diversas operações ao mesmo tempo.

4.4. REQUISITOS RECOMENDADOS

Segundo Bacula (2015) os recursos recomendados para a instalação do Bacula são:

-Sistema Operacional: Linux 64bits

-Memoria RAM: 4GB

-Processador: 4 núcleos de processamento.

-Banco de dado utilizado pela aplicação: MySQL, PostgreSQL ou SQlite

Apesar de essas serem as configurações recomendadas pelos analistas responsáveis, o Bacula pode ser instalado em um servidor com configurações bem mais modestas e funcionar a contento.

5. COMPARAÇÃO DE DESEMPENHO ENTRE FERRAMENTAS

Neste capitulo será abordada a comparação entre três das ferramentas citadas anteriormente, o requisito principal da escolha foi a ferramenta ser de software livre visando a redução de custos por parte da empresa, Arcserve e Backup Exec são softwares proprietários, Bareos é uma dissidência do Bacula, no entanto a comunidade de desenvolvedores do Bacula é mais ativa e com um numero maior de membros, o Amanda teve a sua implantação dificultada por ser próprio para *backup* em fita então tornou-se necessário criar fitas virtuais no disco rígido tornando a implantação mais morosa. Logo dentre elas foram escolhidas o Bacula, Zbackup e Rdiff-backup. Baseado na analise feita por Tomé e Bellezi (2012) que também executa testes de desempenho em ferramentas de *backup*, os critérios de avaliação realizados são facilidade de interação, facilidade de configuração, facilidade de automação, geração de backup, restauração de backup, restauração de um arquivo e indisponibilidade no backup completo.

O computador a ser utilizado para os testes possui as seguintes configurações:

Processador: Intel(R) Core(TM) I7-6500U CPU @ 2.50GHz

Memoria RAM: 4 GB

Sistema de arquivos em ext4 com a seguinte formatação:

Sist. Arq.	Tam.	Usado	Disp.	Uso%	Montado em
udev	2,0G	4,0K	2,0G	1%	/dev
tmpfs	396M	852K	395M	1%	/run
/dev/sda1	13G	4,8G	7,1G	40%	/
none	4,0K	0	4,0K	0%	/sys/fs/cgroup
none	5,0M	0	5,0M	0%	/run/lock
none	2,0G	18M	2,0G	1%	/run/shm
none	100M	28K	100M	1%	/run/user
/dev/sda5	14G	35M	13G	1%	/dados
/dev/sda6	23G	79M	22G	1%	/backup

Sistema Operacional: Ubuntu 14.04.5

Kernel: 4.4.0-128.154

Os seguintes resultados foram encontrados:

Ferramentas	**Facilidade de Interação**	**Facilidade de configuração**	**Facilidade de automação**	**Geração de backup**	**Restauração de backup**	**Restauração de um arquivo**	**Indisp. no backup completo**
Bacula	Fácil	Intermediária	Fácil	Rápida	Intermediária	Rápida	Não houve
Zbackup	Intermediário	Fácil	Intermediária	Lenta	Intermediária	Lenta	Não houve
Rdiff-backup	Intermediário	Fácil	Intermediária	Intermediaria	Rápida	Rápida	Não houve

Tabela 5.1: Tabela dos resultados obtidos nas avaliações
Fonte: Elaborada pelo autor

Para os testes foi usado um disco rígido de cinquenta gigabytes com o seguinte particionamento treze gigabytes para o "/" que conterá o sistema operacional e os usuários do sistema, quatorze gigas para o "/dados" onde serão armazenados os arquivos a serem salvos no backup e vinte e três gigabytes para o "/backup" onde serão guardados os *backups* durante os testes, foi utilizado o sistema operacional Ubuntu 14.04 e 4 gigabytes de memoria RAM.

Para os testes foram armazenados no "/dados" 345 arquivos entre 4 megabytes e 9 megabytes totalizando 2 gigabytes e 100 megabytes de dados a serem resguardados e todas as 3 aplicações foram configuradas para armazenar os *backups* e *restores* no "/backup".

5.1 FACILIDADE DE INTERAÇÃO

Considerando a interação da ferramenta com o administrador utilizando o console texto seriam consideradas como intermediárias, pois precisam ter o conhecimento sobre a sintaxe de cada um, o que demanda um pouco mais de tempo de estudo para a utilização correta da ferramenta.

O Bacula foi considerado como fácil por ter o BAT (Bacula Administrator Tools), a sua interface gráfica de gerenciamento da ferramenta, o que torna mais simples e prática a sua utilização, uma ferramenta intuitiva que com poucos cliques proporciona a execução de *backups* podendo escolher entre os tipos de *backups*, visualização de *logs*, *restore* de um ou mais arquivos dos mais diversos clientes podendo escolher o local onde será salvo.

O Zbackup foi considerada intermediária, pois conforme dito anteriormente é necessário ter um pouco de conhecimento sobre as sintaxes da ferramenta primeiramente tem-se necessidade de inicializar a base de dados através do comando `zbackup init --non-encrypted /backup` para depois haver a execução do *backup* com o comando `tar c /dados | zbackup backup /backup/backup-`date '+%Y-%m-%d'`` onde o tar transforma o arquivo ou diretório selecionado, em um arquivo reconhecido pelo Zbackup posteriormente realiza o *backup* indicando o diretório que receberá a cópia solicitada, com o ano mês e o dia indicados no arquivo, a restauração se dá por meio da seguinte sintaxe `zbackup restore /backup/backup-`date '+%Y-%m-%d'` > /dados/backup-restored.tar` que executa a restauração de um backup dentro do diretório especificado para reservar os backups e o envia para o diretório informado no comando.

O Rdiff-backup tem interação similar ao Zbackup via console texto com o conhecimento do diretório de origem e de destino e com os parâmetros corretos é possível realizar o *backup* e a restauração dos arquivos, basicamente em linha de comando utilizasse o nome da aplicação o caminho de origem dos dados a serem resguardados e o caminho de destino para onde eles serão copiados, foi utilizado também o parâmetro "--force" para forçar

a criação do diretório conforme o padrão da aplicação então basicamente se usa a comando "rdiff-backup –force /dados /backup" porém para um interação mais avançada é necessário conhecer outros parâmetros.

5.2 FACILIDADE DE CONFIGURAÇÃO

Referente à facilidade de configuração o Zbackup está categorizado como fácil pelo motivo de a configuração estar na própria sintaxe do comando de execução da aplicação, possibilitando escolher os dados a serem inclusos no *backup* e para onde serão copiados, permitindo a introduzir do nome do arquivo, se haverá ou não compactação e o diretório onde poderá ser restaurado e para onde será restaurado.

O Bacula necessita basicamente da configuração de três arquivos específicos que são o bacula-dir.conf, bacula-sd.conf e o bacula-fd.conf. O bacula-dir.conf referencia o nome do cliente, os dados que serão contidos e os que não serão contidos no *backup*, o agendamento das cópias, o envio de *logs* para a analise, tipos de compressão entre outras coisas. No bacula-sd é configurado o item que será usado para o *backup* entre fita, HD, pendrive e etc. E especifica o caminho para onde a cópia deverá ser armazenada. O bacula-fd é o arquivo onde é configurado o nome do cliente, importante salientar que esses arquivos põe em suas configurações senhas que deverão coincidir entre os módulos, e para a configuração do BAT necessitamos informar em seu arquivo de configuração em qual servidor está localizado o Bacula Dir, a senha e a porta a ser utilizada.

O Rdiff-backup tem seu uso básico fácil como mostrado anteriormente, mas para um uso mais avançado despende mais tempo, precisasse conhecer bem os parâmetros utilizados pela aplicação bem como estipular um tamanho máximo para os arquivos de backup, se serão utilizadas ou não compressões nos arquivos, a verificação se um backup foi realizado corretamente, a verificação das estatísticas dos backups, é possível também selecionar a data do versionamento a ser restaurado entre outras coisas.

5.3 FACILIDADE DE AUTOMAÇÃO

As ferramentas Zbackup e Rdiff-backup dependem da configuração da Cron para o agendamento de seus serviços sendo assim é necessário conhecer a sintaxe a ser inserida no arquivo crontab para definir a frequência com que os *backups* serão executados. A automatização do Bacula se da dentro do arquivo de configuração bacula-dir.conf, podendo ser especificado a frequência das cópias, o tipo de *backup* se deve ser completo, diferencial e

incremental, adequando-se as politicas de backup solicitadas pelos gestores da aplicação, o tipo de compressão a ser utilizado entre outras coisas.

5.4 TEMPO DE GERAÇÃO DE BACKUP

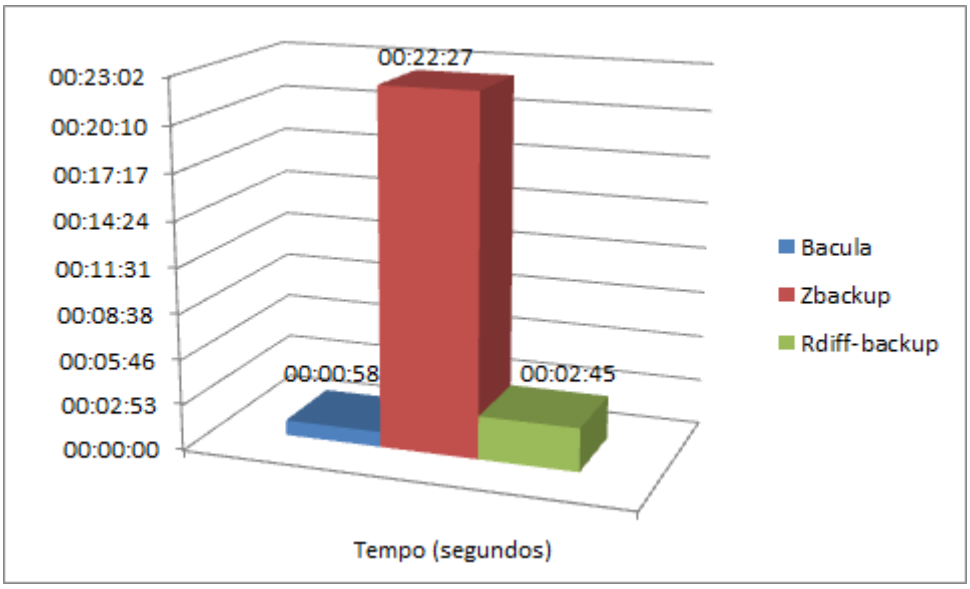


Figura 5.1: Tempo de realização para um backup total
Fonte: Elaborada pelo autor

A Figura 5.1 demonstra que Bacula se sobressai por ter seu backup completo bem rápido que levou cerca de 58 segundos para executar a cópia dos 2,1 gigabytes para o "/backup" e temos uma grande discrepância quando comparamos com o Zbackup que levou cerca de 22 minutos e 27 segundos, essa discrepância se dá devido ao Zbackup ter foco na desduplicação dos dados armazenando em cache, então ao realizar o próximo *backup* haverá uma comparação entre o os itens que constam no atual e os itens que constam no anterior e só serão inclusos os que foram alterados desde o ultimo *backup* completo ou seja o próximo será um *backup* incremental reduzindo assim significativamente o tempo do próximo *backup*.

O Rdiff-backup se aproximou mais do Bacula realizando o backup completo em 2 minutos e 45 segundos, realiza o espelhamento completo no local de armazenado dos backups e guarda versões anteriores dos arquivos copiados.

5.5 TEMPO DE RESTAURAÇÃO DE BACKUP COMPLETO

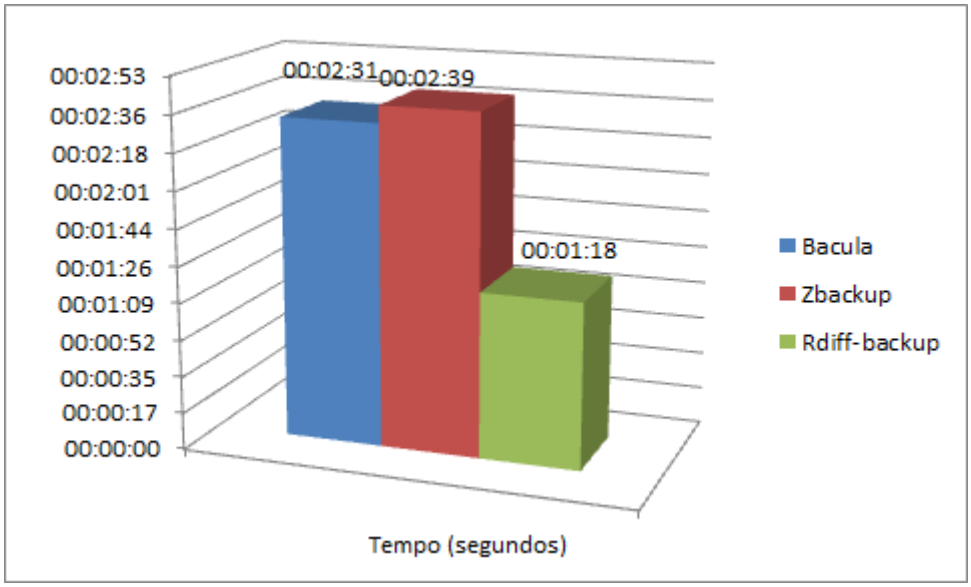


Figura 5.2: Tempo de restauração de um *backup* total
Fonte: Elaborada pelo autor

Na restauração do backup completo dos 2,1 gigabytes realizados anteriormente quem levou a vantagem foi o Rdiff-backup devido a fazer inicialmente apenas o espelhamento dos diretórios, realizou a restauração completa do diretório em um tempo médio de 1 minuto e 18 segundos, logo em seguida vem o bacula que acabou levando cerca de 2 minutos e 31 segundos e em terceiro ficou o zbackup com 2 minutos e 39 segundos sem contar o tempo de descompactação do arquivo que foi finalizado com mais 1 minuto e 40 segundos conforme mostrado na Figura 5.2.

5.6 TEMPO DE RESTAURAÇÃO DE UM ARQUIVO

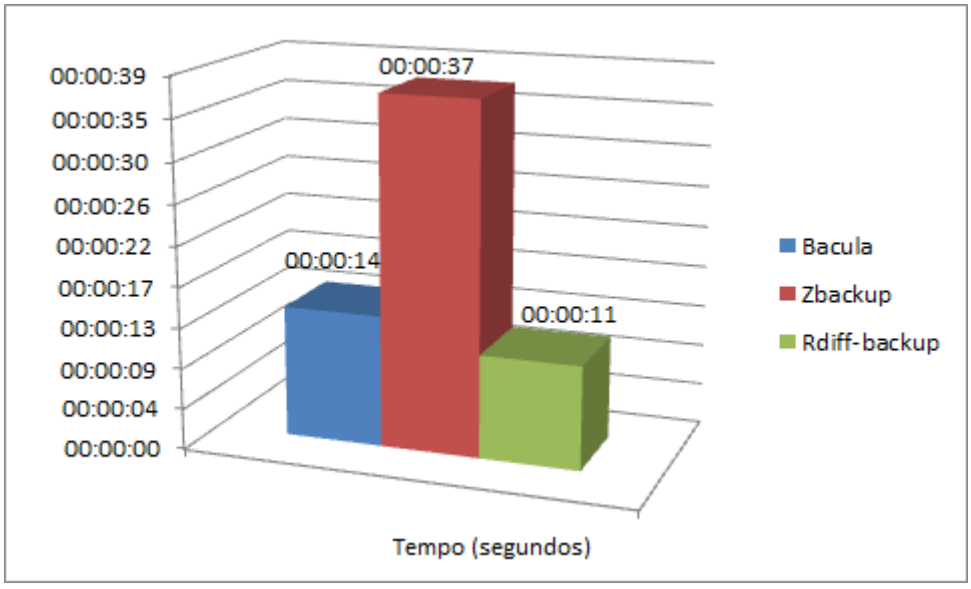


Figura 5.3: Tempo de restauração para apenas um arquivo
Fonte: Elaborada pelo autor

Para os diretórios utilizados anteriormente foram limpos e foi executado a *backup* de apenas um arquivo com 954 megabytes no diretório "/dados" e posteriormente o arquivo foi restaurado e contabilizado o tempo de cada aplicação.

A Figura 5.3 mostra que o Rdiff realizou o processo de restauração desse arquivo em 11 segundos, não muito longe desse tempo ficou o Bacula com apenas 14 segundos sendo executado pelo BAT e em ultimo com uma grande diferença ficou o Zbackup que levou cerca de 37 segundos para cumprir tal tarefa.

5.7 TEMPO DE INDISPONIBILIDADE

Não houve indisponibilidade durante a execução de nenhuma ferramenta, mas todas reduziram significativamente o desempenho dos servidores e serviços nele instalados assim aumentando o tempo de resposta desses serviços.

5.8 DISCUSSÃO DOS TESTES

Em termos gerais o Bacula se sobressai sobre as outras ferramentas pela facilidade de uso, pois além da sua execução via console texto ser facilmente manuseável possui também uma interface gráfica autoexplicativa que com apenas alguns cliques se torna possível gerenciar a ferramenta, diferente das outras duas aplicações que para cada execução fora do padrão necessita de um parâmetro diferente.

A facilidade de automação se dá devido ao Bacula não precisar configurar outros serviços além do Director Daemon que gerencia toda a ferramenta, os outros dois necessitam dos serviços da Crontab para automatizarem suas operações então além do conhecimento sobre a ferramenta necessitasse dispender tempo para conhecer a forma de execução da Crontab.

No tempo de geração de *backup* completo o Bacula mais uma vez toma a frente realizando em pouco mais de um terço do tempo do Rdiff-backup que ficou com o segundo melhor tempo.

Nas demais avaliações o Bacula fica em segundo lugar, porém não muito distante dos resultados do primeiro colocado, com exceção do tempo de restauração do backup completo que fez com quase o dobro de tempo em relação ao Rdiff-backup que teve o melhor tempo por realizar apenas o espelhamento dos diretórios.

6. METODOLOGIA DA PROPOSTA DE IMPLANTAÇÃO DE UMA FERRAMENTA DE *BACKUP*

6.1. CENÁRIO ATUAL E SUAS NECESSIDADES

O cenário atual de *backup* conta com uma topologia descentralizada, onde há vários servidores gerenciando a realização de cópias de segurança, todas as cópias *full*, por meio de arquivos com uma sequência de comandos a serem realizados após sua chamada (scripts). Logo abaixo o detalhamento:

6.1.1. Estrutura dos servidores de armazenamento de *backup*

- **Servidor 1:** Modelo: Dell Power Edge T320; Processador: Intel(R) Xeon(R) CPU E5-2407 v2 2.40GHz; Memoria RAM: 8GB; Memoria ROM: 22 TB – RAID0; Sistema Operacional: Ubuntu 14.04 LTS; Ponto de armazenamento: /media/
- **Servidor 2:** Modelo: Dell Power Edge 840; Processador: Intel(R) Pentium(R) D CPU 3GHz; Memoria RAM: 8GB; Memoria ROM: 4 HDs de 3 TB e 1 HD de 2 TB; Sistema Operacional: Ubuntu 12.04.3 LTS; Ponto de armazenamento: /u1, /u2, /u3, /u4, /u5
- **Servidor 3:** Modelo:Iomega IX4-200d; Processador: Intel(R) Pentium(R) D CPU 3GHz; Memoria RAM: 512 MB; Memoria ROM: 4HDs de 1 TB (RAID5); Sistema Operacional: Ubuntu 14.04 LTS; Ponto de armazenamento: /mnt/pools/A/A0

6.1.2. Topologia atual

A Figura 6.1 mostra a topologia atual utilizada na organização onde três servidores (servidores 1, 2 e 3) são utilizados para *backup* dos demais servidores da matriz e por meio de rsync parte desses dados considerados mais importantes são copiados para um filial de distribuição (servidor 4) que fica a cerca de 20 quilômetros de distancia da matriz para que todos os dados não fiquem no mesmo local físico e dois servidores (servidores 5 e 6) na matriz possuem apenas *backups* em fita realizando seu próprio *backup*.

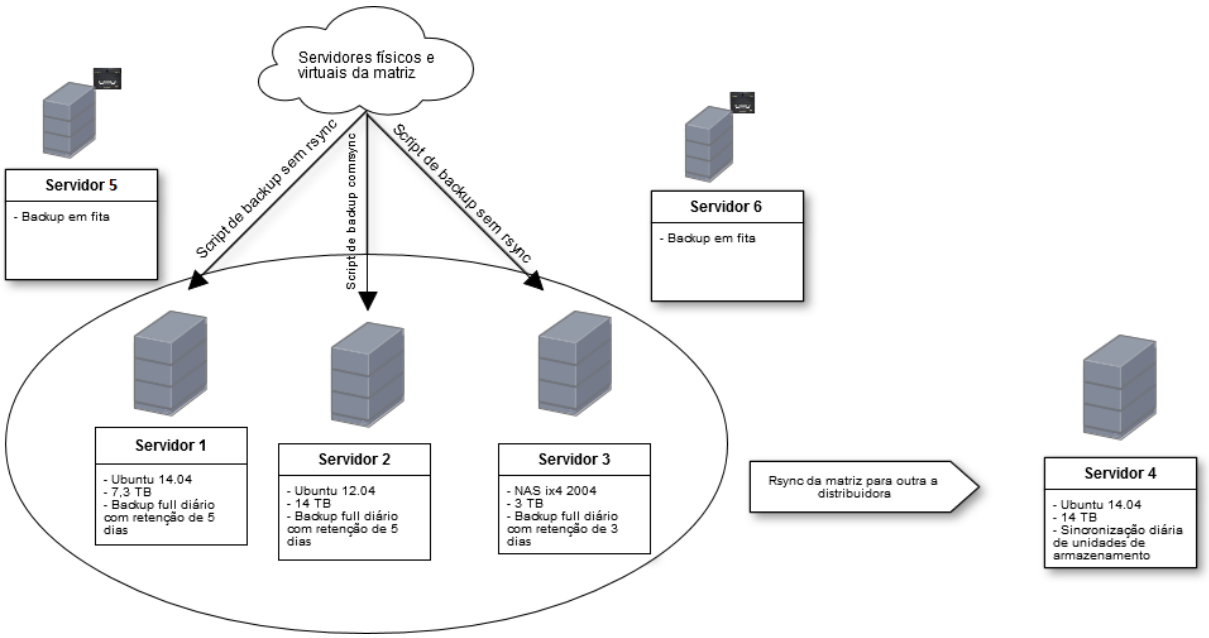


Figura 6.1: Topologia utilizada anteriormente à reestruturação

Fonte: Elaborada pelo autor

6.1.3. Problemas a serem solucionados

Seguem abaixo observações referentes à topologia atual de *backup:*

Scripts de *backup*: Atualmente, todos os *backups* realizados nesta organização são providos por scripts. Entretanto, a elaboração e manutenção de *scripts* consistem em um trabalho oneroso visto que há ferramentas consolidadas no mercado e desenvolvidas sob licenças livres. E a continuação desta solução está prejudicada por falta de documentação correspondente aos scripts utilizados.

Backup *full*: Notou-se que todos os *backups* realizados atualmente pelos scripts são do tipo *full*, ou seja, diariamente são realizados *backups* completos dos servidores ao invés de copiar apenas o que foi incrementado de um dia para o outro. Este tipo de *backup* se mostra extremamente caro sendo realizado diariamente, principalmente pela excessiva quantidade de armazenamento necessária, e pelo trafego demasiado na rede.

Retenção: O tempo de retenção atualmente na organização varia entre três a seis dias dependendo do armazenamento alocado para cada serviço. No entanto, pelo nível de criticidade do negócio, este tempo de retenção não atende as necessidades.

***Backup* descentralizado:** A topologia atual com quatro servidores para armazenamento de *backup* e mais dois servidores que realizam seus *backups* em fita utilizando drive próprio demonstra uma descentralização dos serviços de *backup* que vem a

dificultar a administração, tais como restauração e manutenção, ocorrendo também o uso dispendioso de hardware.

Melhores práticas de *backup*: A organização não atende as exigências das melhores praticas de Backup, tais como, estratégias condizentes com a natureza dos dados armazenados, testes de restauração periódicos e constante atualização da documentação.

6.2. PROPOSTA DA SOLUÇÃO

A proposta de solução que segue neste estudo contou com a restruturação total do ambiente de *backup* da matriz, alterando sua topologia descentralizada para uma topologia centralizada, que será composto por um único servidor responsável por gerenciar todas as atividades de *backup*.

6.2.1. Nova estrutura física

A nova estrutura adotada teve a reutilização de dois dos quatro servidores utilizados na antiga topologia, e os discos foram realocados entre dois servidores de armazenamento, Também contém uma maquina virtual que administrará todas as operações de *backup* e *restore*.

- **Servidor 1:** Modelo: Maquina virtual; Processador: quatro núcleos; memoria RAM: 4GB; Sistema operacional: Ubuntu Server 16.04; Ferramentas instaladas: Bacula Director Daemon, Bacula Estorage Daemon, Bacula File Daemon, Console.
- **Servidor 2 (utilizado como storage):** Modelo: Dell Power Edge T320; Processador: Intel(R) Xeon(R) CPU E5-2407 v2 2.40GHz, Memoria RAM: 8GB, Memoria ROM: 4 HDs de 3TB SATA, 06 HDs de 2TB SATA utilizando RAID com ZFS; Ferramentas instaladas: FreeNas 9.10; Ponto de armazenamento: /mnt/bacula-backup
- **Servidor 3 (utilizado como storage secundário):** Modelo: Dell Power Edge T320; Processador: Intel(R) Xeon(R) CPU E5-2407 v2 2.40GHz, Memoria RAM: 8GB, Memoria ROM: 4 HDs de 3TB SATA, 06 HDs de 2TB SATA utilizando RAID com ZFS; Ferramentas instaladas: FreeNas 9.10; Ponto de armazenamento: /mnt/bacula-backup
- **Switch Dell 24 portas:** Gigabit Ethernet

6.2.2. Nova topologia proposta

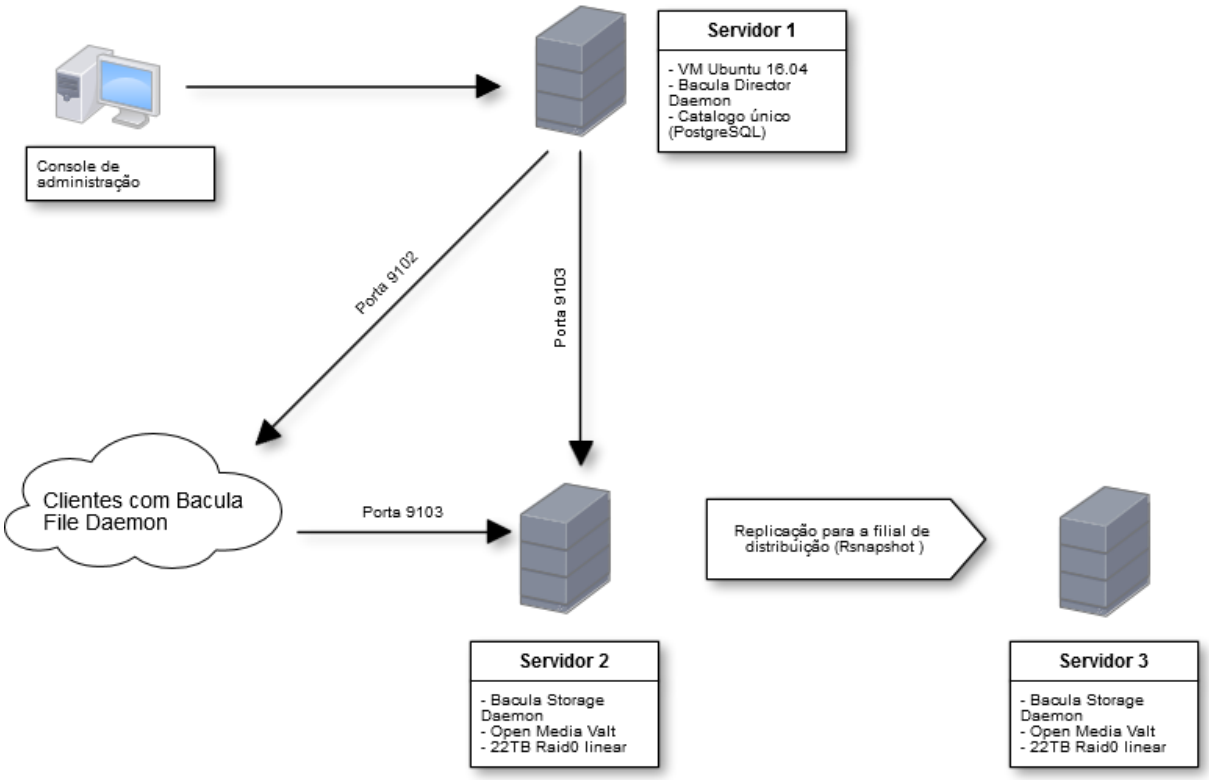


Figura 6.2: Nova topologia proposta

Fonte: Elaborada pelo autor

A Figura 6.2 mostra a nova topologia proposta para a restruturação dos *backups* na matriz, contando com dois servidores físicos que servirão como servidores de armazenamento com as ferramentas Bacula Storage Daemon e Open Media Valt instaladas, um na matriz e outro de replicação na filial de distribuição que fica a cerca de 20 quilômetros dos dados originais e um servidor virtual com o Bacula Director Daemon que será o servidor que administrará todas as operações de *backup*, e o administrador do sistema poderá ter uma console de administração em outro computador não precisando acessar diretamente o servidor de administração.

6.2.3. Nova estrutura de serviços e melhorias

Neste novo cenário temos um sistema de *backup* centralizado, robusto e inteligente, utilizando dois softwares livres: O Bacula para operações de *backup* e o Open Media Vault para armazenamento.

- **Bacula:** Após pesquisa e comparações com outras ferramentas de *backup* chegou-se a conclusão que o Bacula seria a que melhor atenderia as necessidades da organização, pois possui a característica de *backup* centralizado e foi desenvolvido

sob licença de software livre. Atendendo as demandas de administração de backup, restauração atendendo a rede heterogênea da organização com sistemas operacionais variados, além de se adequar à estratégia de *backup* GFS (grandfather, father, son) e às melhores praticas de *backup*.

- **Open Media Vault:** Por meio dessa ferramenta é possível criar um nó de armazenamento de *backup* com desempenho aceitável e tem a possibilidade de aplicar redundância de discos, nos testes realizados tivemos resultados além do que esperávamos tratando-se de desempenho.

6.2.4. Atividades implementadas

Abaixo serão elencadas em ordem cronológica as atividades que foram executadas para garantir a implantação do novo cenário:

- Levantamentos iniciais: dados a serem protegidos, sistemas envolvidos, quantidade de dados a serem armazenados;
- Testes iniciais e instalação do servidor Bacula em uma máquina virtual;
- Migração dos dados do servidor dois para o servidor um do cenário antigo;
- P2V na nova maquina de armazenamento (Dell T320 com gaveteiro);
- Reutilização dos discos do antigo servidor dois para a nova maquina de armazenamento;
- Criação de pool de discos linear no Open Media Valt (Raid0);
- Configuração do Bacula Storage no OMV;
- Instalação do Bacula File Daemon nos servidores que serão “backupeados”;
- Refinar ajuste do Bacula Director
- Teste de *backup* e *restore* na nova estrutura;
- Acompanhamento da operação e ajustes finais;
- Documentação

7. RESULTADOS APÓS A REESTRUTURAÇÃO

Neste capitulo serão mostradas as melhorias que foram obtidas após a implementação da ferramenta tais como a topologia de *backup*, tempo de retenção, segurança, politicas de *backup*.

7.1. NOVA TOPOLOGIA

Como explanado inicialmente no inicio desse trabalho há basicamente duas topologias de *backup*, a utilizada no cenário antigo era descentralizada, cada servidor realizava o seu próprio *backup* via *scripts* podendo ser em fita, *pendrive* ou enviado para outro servidor onde armazenaria as copias de segurança, o que torna muito complexa a administração visto que nem sempre esses *scripts* eram configurados da mesma maneira e nem sempre se encontravam no mesmo lugar, nem havia uma documentação que especificasse a execução de cada um desses *backups.*

A nova topologia centralizada conta com apenas um servidor virtualizado executando o Bacula Director Daemon que administra todas as operações de *backup* e restauração podendo facilmente agenda-las ou executa-las imediatamente e sua console gráfica torna ainda mais simples a gerencia da aplicação. Possui também em sua console gráfica um histórico de todas as operações realizadas pela aplicação que informam o volume de dados copiados, o tempo que levou para copia-los e qual o nome do cliente que teve seus dados resguardados, é possível também verificar quais dados estão resguardados.

7.2. TEMPO DE RETENÇÃO

O tempo de retenção ou período em que ainda é possível recuperar os dados que antes era de 3 a 5 dias passou a durar cerca de um mês, isso se deu devido à forma como os *backups* eram realizados, anteriormente todos os *backup* realizados eram uma cópia completa dos arquivos não importando se já haviam sido copiados ou não em um *backup* anterior o que ocupava muito espaço de armazenamento nas fitas, *pendrives* e servidores de armazenamento disponíveis.

A nova metodologia de *backup* é baseada no modelo GFS, realizou-se inicialmente um *backup* completo de todos os servidores e após isso se realizava apenas incrementais diariamente que tinham a retenção por uma semana e um *backup* completo é realizado todos os meses, assim reduzindo o espaço desnecessário ocupado anteriormente nos dispositivos de armazenamento e consequentemente aumentando significativamente este tempo de retenção.

7.3. SEGURANÇA

A estrutura anterior pecava, por sua descentralização, na realização de restaurações periódicas de *backup* para saber se estavam sendo realizados da maneira correta e com os arquivos e diretórios corretos, esta descentralização tornava inviável a realização dessas restaurações periódicas, visto que os *backups* eram realizados em diversos dispositivos diferentes e sem nenhuma documentação especificando para onde seriam enviados, a única forma de ter essa informação era ler o *scripts* que realizavam essa operação.

Na estrutura em que o Bacula foi aplicado, tornou-se possível essa execução de restaurações periódicas, todas as informações dos *backups* realizados estão em apenas um servidor que mostra em seus *logs* se as copias foram realizadas com sucesso, e as restaurações se tornam mais simples, pois podemos listar os servidores que estão sendo resguardados e escolher o dia que queremos restaurar com apenas alguns cliques, esses testes periódicos asseguram de que os *backups* estão sendo realizados da maneira correta e que serão eficazes em caso de um possível desastre.

7.4. POLITICAS DE *BACKUP*

Com a nova estrutura outro beneficio aplicado foram as politicas de *backup*, um documento detalhado com informações sobre a aplicação utilizada e como administrar por meio dela, especificando os itens e servidores que estarão inclusos nas copias de segurança, informando os servidores que irão armazenar cada uma dessas cópias e indicando as pessoas responsáveis por administrar os serviços da aplicação.

Este documento inexistente no cenário anterior tornava mais onerosa a administração das cópias de segurança visto que não se tinha informações rápidas sobre a realização de cada *backup*, sendo preciso em qualquer manutenção estudar o cenário daquele servidor especifico para então executar a ação desejada.

Outros pontos importantes tratados pela politica de *backup* são a forma de descarte das mídias de *backup* que antes eram acumuladas em depósitos e muitas vezes tratadas apenas como sucata o que põe em perigo a confidencialidade dos dados, na nova estrutura com a implantação das politicas foi possível documentar as ações e especificar o que seriam feitas com essas mídias obsoletas, que serão incineradas, picotadas, sobrescritas e/ou realizar procedimentos que impossibilitem a recuperação dos dados.

E foram documentadas as janelas de *backup*, tempo em que as cópias de segurança podem ser realizadas respeitando a operação da organização, evitando o máximo possível de indisponibilidade das aplicações e arquivos necessários às atividades.

Estas politicas devem ter uma grande importância dentro das organizações que trabalham com *backup*, pois facilitam a administração, é um assunto importante que é tratado inclusive na ISO 27002 de 2013 que recomenda a documentação de todas as diretrizes de *backup*.

No Apêndice A podemos analisar a documentação da politica de *backup* utilizada na organização com algumas alterações por questões de segurança, ficam evidenciados os servidores que terão suas cópias resguardadas, tempo de retenção

7.5. AUTOMAÇÃO

Outra grande mudança entre os cenários foi o processo de automação, quando realizados por *scripts* dependiam da crontab de cada servidor para agendar suas operações não havendo nada padronizado, para fazer qualquer manutenção necessitava acessar os arquivos de configuração deste serviço.

O novo cenário permite por meio da sua estrutura centralizada, automatizar cada operação de *backup* podendo especificar uma operação para cada servidor ou até mesmo criar grupos que possuam as mesmas condições de realização das cópias, isso sem precisar se conectar a cada servidor, todas as configurações são realizadas apenas no servidor principal que contem o Bacula *Director Daemon*.

8. CONCLUSÃO E TRABALHOS FUTUROS

8.1 CONCLUSÃO

Comparando todas as ferramentas de *backup* analisadas neste trabalho a que obteve melhor resultado no ambiente corporativo foi a ferramenta Bacula incorporando diversas aplicabilidades nos mais diversos cenários, atendendo desde pequenas instituições até as mais robustas, a sua facilidade de configuração e gestão mostradas neste estudo visam expor que para ter um ambiente de *backup* integro, confiável e disponível, em conformidade com as melhores praticas de *backup*, não necessariamente se precisa de um software dispendioso, com valores de licenças exorbitantes, que muitas vezes não são de fácil implantação e que tornam o *backup* preso a aplicação comercial.

Dentro da organização houve uma mudança drástica ao ser implantado o Bacula, primeiramente a topologia de *backup* mudou passaram de descentralizados onde vários servidores armazenavam seus dados em dispositivos conectados a eles, tais como fitas e/ou *pendrives* ou até mesmo em outros servidores de armazenamento, e se tornaram *backups* centralizados onde apenas um servidor administra todas as operações direcionando onde os *backups* serão armazenados, facilitando assim a analise e gerencia dessas operações. O tempo de retenção foi aumentado significativamente passando de dias à meses não sendo armazenados apenas em fitas ou *pendrives* mas sim em servidores específicos para armazenamento de dados.

Como dito anteriormente foi possível se adequar as melhores praticas de *backup*, foi implantada uma politica de *backup* contendo todas as informações referentes ao mesmo, como tempo de retenção, quais servidores e seus diretórios estão inclusos para serem resguardados, quais servidores serão usados para armazenar os *backups*, quais pessoas estão responsáveis por gerenciar a aplicação e fazer os testes necessários de integridade destes *backups*, a topologia utilizada e o tipo de *backup* a ser realizado.

8.2 TRABALHOS FUTUROS

Para trabalhos futuros podemos sugerir:

- A melhora das conexões de internet para a implantação de *backup* em nuvem salvaguardando os dados não apenas em servidores locais ou regionais, mas também

sendo possível armazenar em servidores especializados de terceiros tais como Amazon e Google.

- Com a nova implantação do Bacula o *backup* das maquinas virtuais esta sendo feito com a imagem completa podendo ser implantado futuramente o *backup* granular dessas maquinas virtuais podendo armazenar em *backup* apenas os dados mais importantes e definidos na politica.
- Outro ponto a ser estudado seria a implantação de um robô de fitas dentro da organização aumentando a durabilidade dos *backups* e otimizando o processo.
- Por ser uma ferramenta de código aberto é possível também realizar melhorias em seu código contribuindo com o desenvolvimento da aplicação Bacula e disseminando conhecimento com a comunidade.

9. REFERÊNCIAS

ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/27002 – Tecnologia da informação – Técnicas de segurança – Código de pratica para a gestão de segurança da informação**. ABNT, 2013.

ARCSERVE. Site oficial da ferramenta. Disponível em: https://arcserve.com/br/ Acesso em: 03 Mar. 2018

BACULA. Arquitetura e hardware recomendados. Disponível em: http://www.bacula.com.br/arquitetura-e-hardware-recomendados/. 2015. Acesso em: 20 de Abril de 2018

BACULA. Matriz de requisitos. Disponivel em: http://www.bacula.com.br/matriz-de-requisitos/. 2017. Acesso em: 18 de Abril de 2018

BAREOS. Site da Empresa que desenvolve a ferramenta. 2010. Apresenta informações sobre o software, opções para download e guias para utilização. Disponível em: https://www.bareos.com/. Acesso em: 20 Abril 2018

BRASIL. Lei n. 5172, de 25 de out. de 1966. Código tributário nacional, Brasília, DF, out 1966.

BRASIL. Ajuste SINIEF 07/05, de 30 de setembro de 2005, Manaus, AM, out 2005.

DOC.BAREOS in: BAREOS. Site de documentação da aplicação BAREOS. Disponível em: http://doc.bareos.org/master/html/bareos-manual-main-reference.html. Acesso em 22 Abril 2018

FARIA, HEITOR. “Bacula” - Ferramenta Livre de *backup*: 2ª ed.: 2014

FARIA, HEITOR. “Bacula” – O *Software* Livre de *backup*: 3ª ed.: 2017

FREENAS. Site oficial da ferramenta. Disponível em *www.freenas.org/* Acesso em: 22 Junho 2018

GUISE. PRESTON DE. Enterprise Systems Backup and Recovery: A Corporate Insurance Policy. 2009

Internacional Data Corporation. 2014. Disponível em: <https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm> Acesso em: 10 Abril 2018

MORAES. ELIANA MÁRCIA. Planejamento do Backup de Dados. 2007

OPENMEDIAVAULT. Site oficial da ferramenta. Disponível em https://www.openmediavault.org/ Acesso em: 20 Junho 2018

RDIFF-BACKUP. Site oficial da Feramenta. Disponível em: <rdiff-backup.nongnu.org>. Acesso em: 10 Maio 2018

SOMASUNDARAM, G.; SHRIVASTAVA, A; EMC EDUCATION SERVICES. Armazenamento e Gerenciamento de Informações: Como armazenar, gerenciar e proteger informações digitais. 2011

TOMÉ, ANTONIO; BELLEZI,MARCOS. Comparação do Desempenho entre Ferramentas de Código Livre para a Realização de *Backups*. 2012

VERITAS. Guia do Administrador do Veritas Backup Exec. 2017

ZAMANDA. Site oficial da ferramenta. Disponível em: http://amanda.zmanda.com/ Acesso em: 25 Março 2018

ZBACKUP. Site oficial da ferramenta. Disponível em: http://zbackup.org/ Acesso em: 06 Maio 2018

APÊNDICE A – Exemplo de política de backup

Política de Backup e Restauração de Arquivos

Local: XXXXXXXXXXXXXX

Versão 1.01

Histórico de Revisões:

Versão	Data	Autor	
1.00	24/01/18	XXXXXXXXXXXX	Versão Inicial
1.01	17/03/18	XXXXXXXXXXX	

1. INTRODUÇÃO

O presente documento estabelece uma política de cópias de segurança (backup) e restauração de arquivos digitais armazenados no parque tecnológico.

Os donos dos dados deverão ter ciência dos tempos de retenção aqui estabelecidos para cada tipo de informação e os administradores/operadores de backup deverão zelar pelo cumprimento das diretrizes aqui estabelecidas.

2. CONSIDERAÇÕES INICIAIS

O serviço de backup deve ser orientado para a restauração das informações no menor tempo possível, principalmente havendo indisponibilidade de serviços que dependam da operação de restore.

Este documento deverá ter conhecimento e anuência da Diretoria.

3. ORIENTAÇÕES GERAIS:

1. Cabe aos administradores prever a realização de testes periódicos de restauração, no intuito de averiguar os processos de backup e estabelecer melhorias.
2. A administração dos backups também deve ser orientada para que seus trabalhos respeitem as janelas para execução, inclusive realizando previsão para a ampliação da capacidade dos dispositivos envolvidos no armazenamento.
3. As mídias defeituosas ou inservíveis serão encaminhadas para picotamento, incineração, procedimentos de sobrescrita de dados remanescentes (disco rígido) ou outro procedimento que impossibilite a recuperação dos dados por terceiros.
4. As solicitações de restauração de arquivos deverão ser abertas formalmente através de ferramentas de abertura de chamados e / ou formulário que deverá conter os nomes dos arquivos e pastas que deverão ser recuperados e, principalmente, a data do arquivo que se pretende ter acesso.

4. ESTRATÉGIA GERAL DE BACKUP:

De acordo com a natureza dos dados trazemos a seguinte classificação:

- Arquivos dos Sistemas Operacionais;
- Servidores de Arquivos;
- Bancos de Dados;
- Máquinas Virtuais (imagem);

Por padrão será adotada o seguinte esquema de realização de backups:

- Backups incrementais (denominados diários) de **segunda à sábado**, realizados a partir das 20:00h., **com uma semana de retenção;**
- Backups completos (full – denominados mensais) no **primeiro sábado do mês**, realizados a partir das 20:00h., **com um mês de retenção;**

5. NECESSIDADES ESPECIAIS DE BACKUP (EXCEÇÕES):

5.1 Máquinas Virtuais (imagem);

O backup das máquinas virtuais como imagem (adequado para fins de disaster recovery – ou seja: restauração da máquina como um todo), será feito diariamente:

- Backups completos (full – denominados imagem) de segunda à sábado, realizados a partir das 19:00h, **com 2 dias de retenção;**

No mais, as Máquinas Virtuais serão tratadas como outras máquinas físicas, devendo o cliente de backup ser instalado em cada uma delas.

6. DADOS TÉCNICOS

6.1. Topologia de Backup com Bacula

Distribuição dos serviços Bacula em nossa infraestrutura atual (vide figura 1):

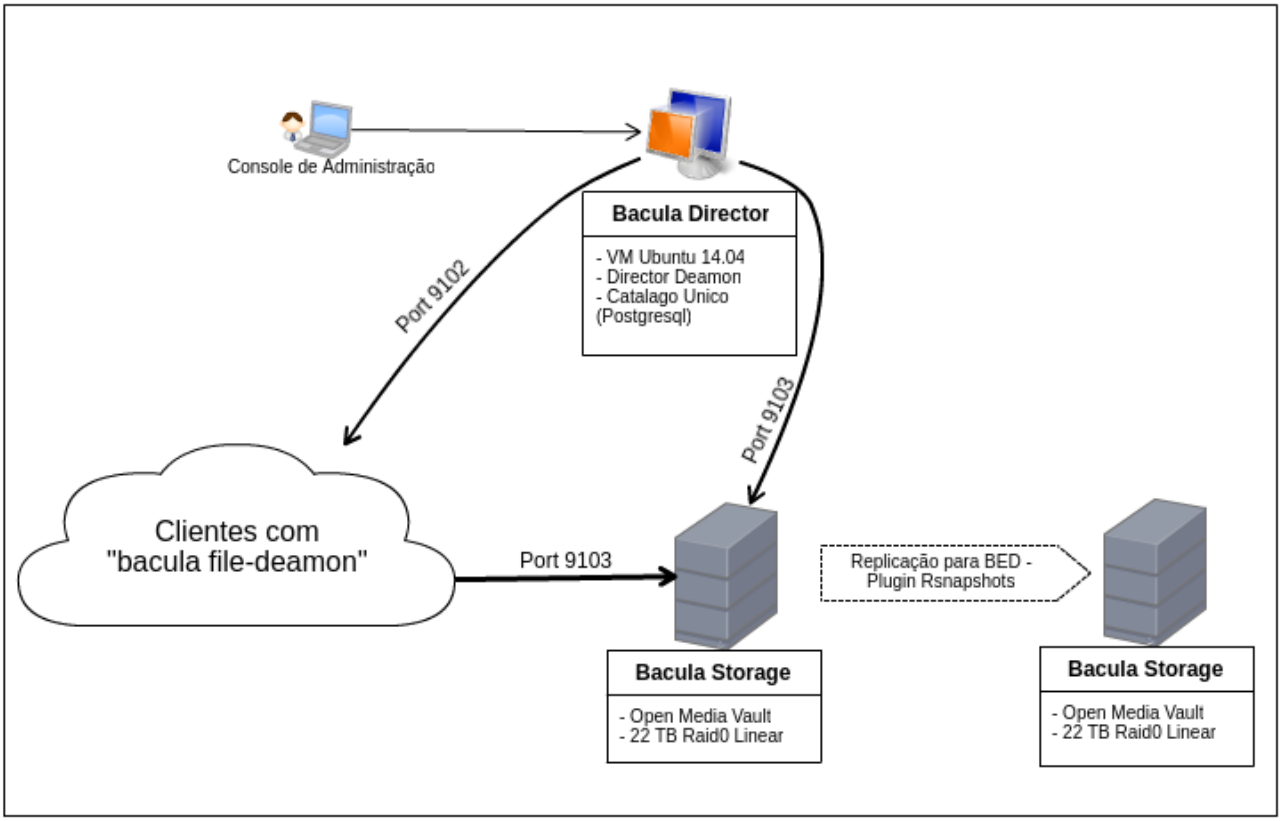


Figura 1 - Topologia de Backup

- **Director Daemon:**

Máquina virtual: Vmware;
Sistema Operacional: Ubuntu Server 16.04 64 bits;
Banco de dados: Postgresql 9.2;
Bacula Director 7.0.5 - Arquivo de configuração: /etc/bacula/bacula-dir.conf;
IP: XXXXXXXXX;
Usuário: XXXXXX;

- **Storage Daemon:**

Servidor: Dell Power Edge T320, 8 GB RAM;
Sistema de Armazenamento: Open Media Vault - 22 TB Raid Linear;
Bacula Storage 7.0.5 - Arquivo de configuração: /etc/bacula/bacula-fd.conf;
IP: XXXXXXXXX;
Archive Device: /media/abf7375f-37ef-494e-984d-2b7fc668213b/bacula-backup;
Usuário: XXXXXXXX

- **File Daemon (vide figura 2):**

Client Name	File Retention	Job Retention	AutoPrune	ClientId	Uname
bacula-fd	1y	1y	Yes	1	7.0.5 (28Jul14) x86_64-pc-linux-gnu,ubuntu,16.04
bnvteste-fd	1y	1y	Yes	3	5.2.5 (26Jan12) x86_64-pc-linux-gnu,ubuntu,12.04
ccpbd-fd	1y	1y	Yes	4	5.2.5 (26Jan12) x86_64-pc-linux-gnu,ubuntu,12.04
contabil-fd	1y	1y	Yes	7	5.2.5 (26Jan12) x86_64-pc-linux-gnu,ubuntu,12.04
fileserver-fd	1y	1y	Yes	2	5.2.5 (26Jan12) x86_64-pc-linux-gnu,ubuntu,12.04
mastersaf-fd	1y	1y	Yes	8	5.2.5 (26Jan12) x86_64-pc-linux-gnu,ubuntu,12.04
proxy-fd	1y	1y	Yes	10	5.0.2 (28Apr10) i686-pc-linux-gnu,ubuntu,10.10
scobmx-fd	1y	1y	Yes	5	5.2.5 (26Jan12) x86_64-pc-linux-gnu,ubuntu,12.04
scoccp-fd	1y	1y	Yes	11	5.2.5 (26Jan12) x86_64-pc-linux-gnu,ubuntu,12.04
scoend-fd	1y	1y	Yes	9	5.2.5 (26Jan12) x86_64-pc-linux-gnu,ubuntu,12.04
empresaap-fd	1y	1y	Yes	6	5.0.0 (26Jan10) i686-pc-linux-gnu,redhat,(Final)

Figura 2 - Máquinas físicas com o cliente bacula instalado

- **Console Bacula (vide figura 3):**

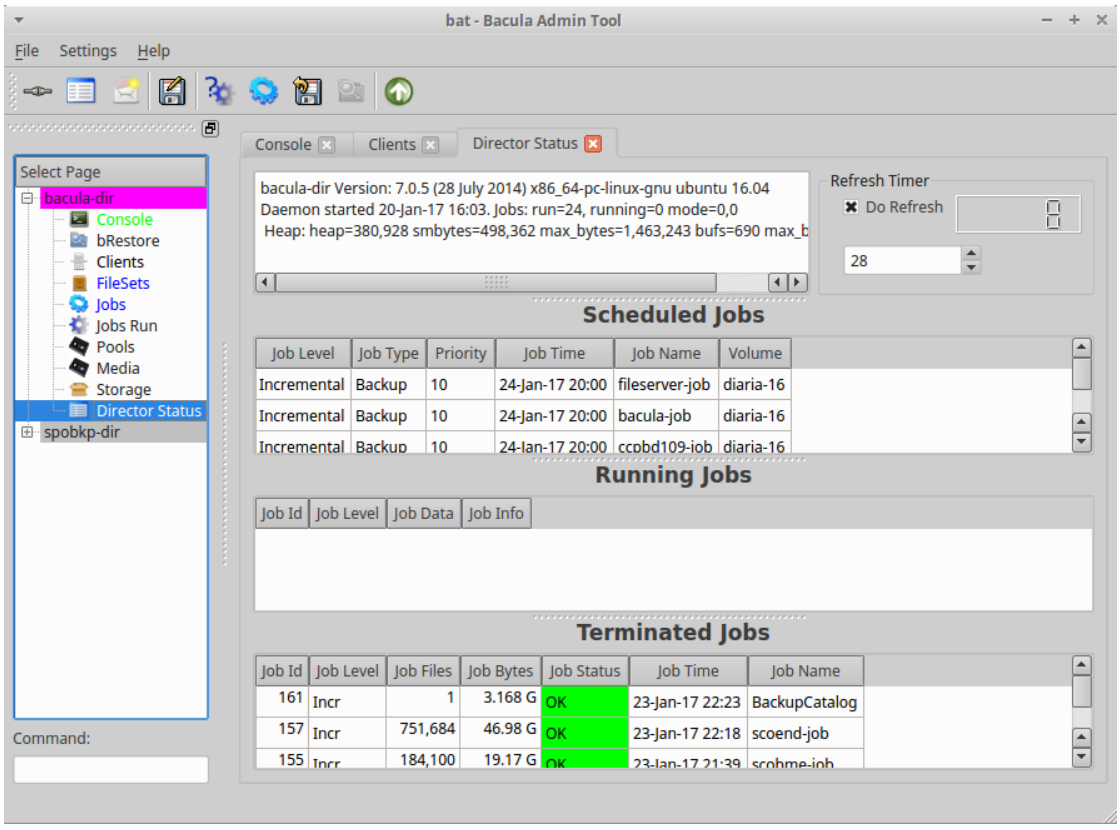


Figura 3 – BAT 7.0.5 (Ferramenta de Administração do Bacula)

6.2. File Set (Arquivos que serão copiados pelo bacula)

SERVIDOR	ARQUIVOS INCLUSOS	ARQUIVOS EXCLUSOS
BACULA	/etc /var /opt	/var/spool/bacula
BACULA CATALOG	/var/lib/bacula/bacula.sql	
CCP (BANCO DE DADOS)	/u1/DBA	
CONTABIL	/u1 /u4	
FILESERVER	/u1/empresa /u1/danfe /u1/scripts /u2/geti /u2/bkpdesenvolvimento /u2/marketing /etc/samba	
MASTERSAF	/etc /bin /usr /dados	
SQUID	/etc	
SCOXXX	/u /u1 /u2 /home	
SCOCCP	/home /var/lib/tomcat6/webapps/*.war	
SCOEND	/etc /bin /usr /u1	
EMPRESAAP	/u1	

Tabela 1 – File Set das Máquinas Físicas

6.3. Backup das máquinas virtuais

Para fins de “disaster e recovery” as maquinas virtuais com aplicações criticas utilizarão o script GhettoVCB.sh – esse script executa backups a quente (snapshot) de máquinas virtuais residentes em servidores Esxi 5.x.

MAQUINA VIRTUAL	IP	SERVIDOR VMWARE ESXI	RETENÇÃO
NFCE	XXXXXXXXX	XXXXXXXXX	2 dias
NFE	XXXXXXXXX	XXXXXXXXX	2 dias
VMFTP	XXXXXXXXX	XXXXXXXXX	2 dias
SRVBACULA	XXXXXXXXX	XXXXXXXXX	2 dias
JAVA-BACKUP	XXXXXXXXX	XXXXXXXXX	2 dias
OBJECTMMRS	XXXXXXXXX	XXXXXXXXX	2 dias
OPENFIRESPARK	XXXXXXXXX	XXXXXXXXX	2 dias
REDMINE	XXXXXXXXX	XXXXXXXXX	2 dias
VMTESTE	XXXXXXXXX	XXXXXXXXX	2 dias
VMEMPRESAPRE	XXXXXXXXX	XXXXXXXXX	2 dias
VMZABBIX	XXXXXXXXX	XXXXXXXXX	2 dias
SRVGLPIOCS	XXXXXXXXX	XXXXXXXXX	2 dias
OWNCLOUD	XXXXXXXXX	XXXXXXXXX	2 dias
SITEF-NOVO	XXXXXXXXX	XXXXXXXXX	2 dias
CTPAGAR-SERVER	XXXXXXXXX	XXXXXXXXX	2 dias

PADAWAN	XXXXXXXXX	XXXXXXXXX	2 dias
HELPDESK	XXXXXXXXX	XXXXXXXXX	2 dias
JGED2	XXXXXXXXX	XXXXXXXXX	2 dias
MIGRAZIM	XXXXXXXXX	XXXXXXXXX	2 dias
MOODLE	XXXXXXXXX	XXXXXXXXX	2 dias
VMPHPIPAM	XXXXXXXXX	XXXXXXXXX	2 dias
BMXPRE	XXXXXXXXX	XXXXXXXXX	2 dias
UB10.04-SRVVPN	XXXXXXXXX	XXXXXXXXX	2 dias

Tabela 2 – Maquinas virtuais com backup ativado

Todo o agendamento é realizado pela cron do **Open Media Vault (Storage – XXXXXXXXX)** como mostra a figura abaixo:

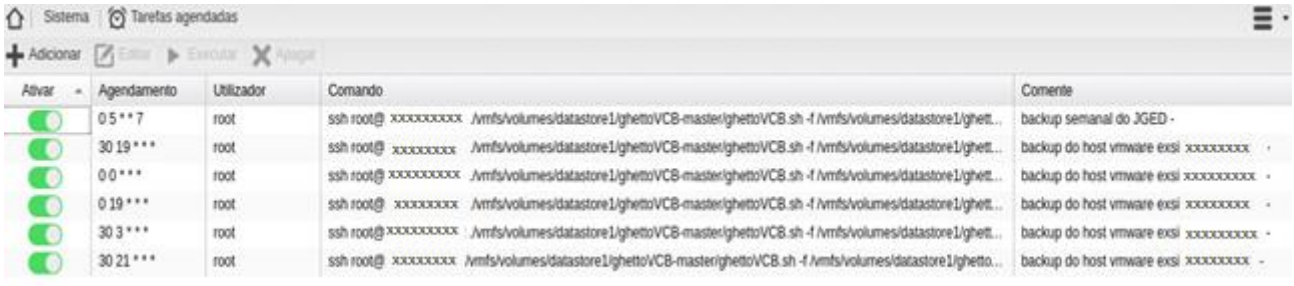


Figura 4 – Tarefas agendadas no OMV

6.4. Armazenamento

Todos os jobs configurados no bacula director armazenam backups no bacula storage **OMV1 (Open Media Vault – XXXXXXXXX)**, cujo "*archive device*" é **/media/abf7375f-37ef-494e-984d-2b7fc668213b/bacula-backup.**

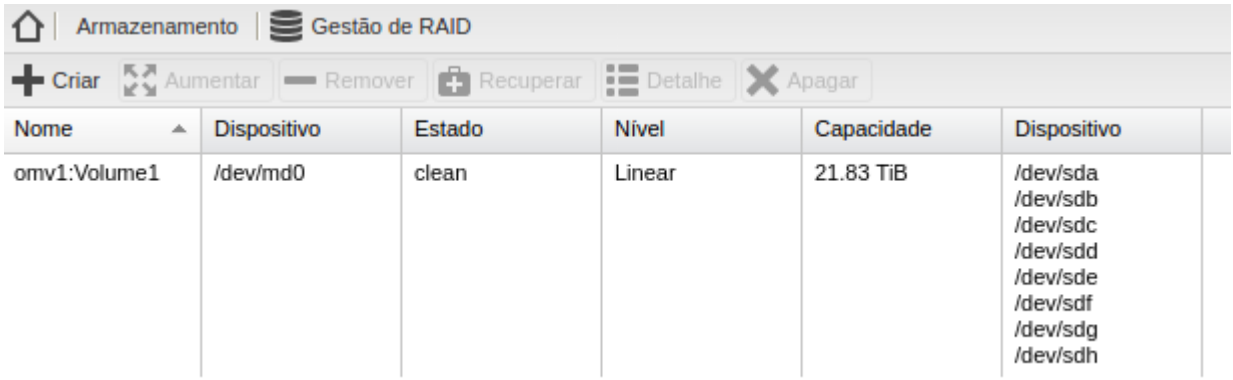
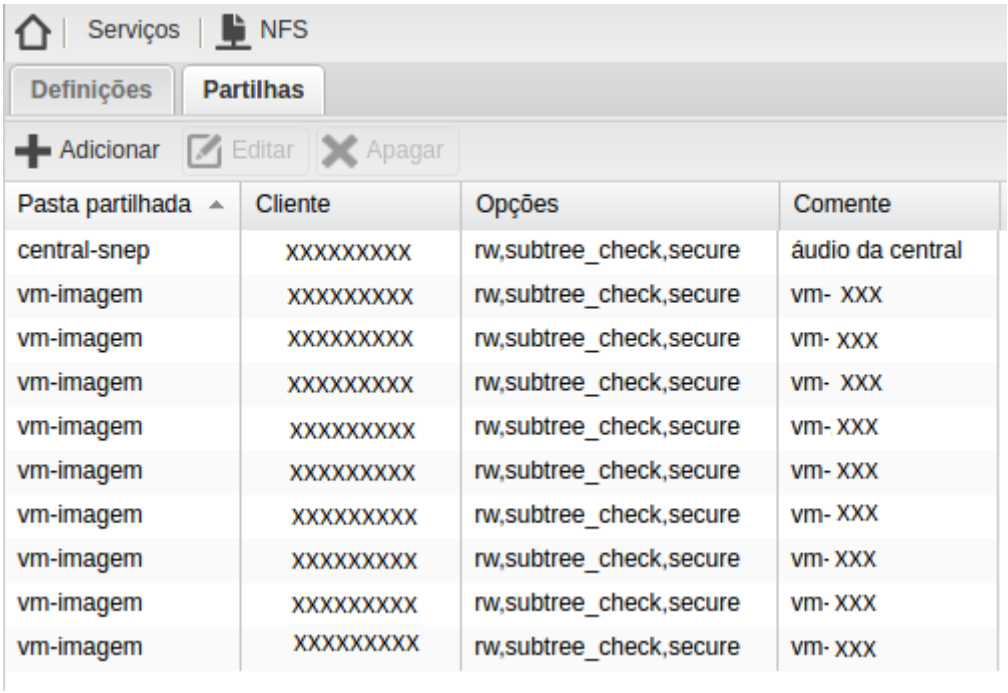


Figura 5 – Raid Linear no OMV

Para armazenamento dos snapshots das **máquinas virtuais e áudio da central** utilizaremos este mesmo Storage (OMV) explorando o recurso de compartilhamento NFS conforme a figura abaixo:



Pasta partilhada	Cliente	Opções	Comente
central-snep	XXXXXXXXX	rw,subtree_check,secure	áudio da central
vm-imagem	XXXXXXXXX	rw,subtree_check,secure	vm- XXX
vm-imagem	XXXXXXXXX	rw,subtree_check,secure	vm- XXX
vm-imagem	XXXXXXXXX	rw,subtree_check,secure	vm- XXX
vm-imagem	XXXXXXXXX	rw,subtree_check,secure	vm- XXX
vm-imagem	XXXXXXXXX	rw,subtree_check,secure	vm- XXX
vm-imagem	XXXXXXXXX	rw,subtree_check,secure	vm- XXX
vm-imagem	XXXXXXXXX	rw,subtree_check,secure	vm- XXX
vm-imagem	XXXXXXXXX	rw,subtree_check,secure	vm- XXX
vm-imagem	XXXXXXXXX	rw,subtree_check,secure	vm- XXX

Figura 6 – Compartilhamento NFS no OMV

6.7. Restauração pelo Bacula

- bat → bRestore → selecione o cliente e o job → arraste os arquivos que serão restaurados → restore

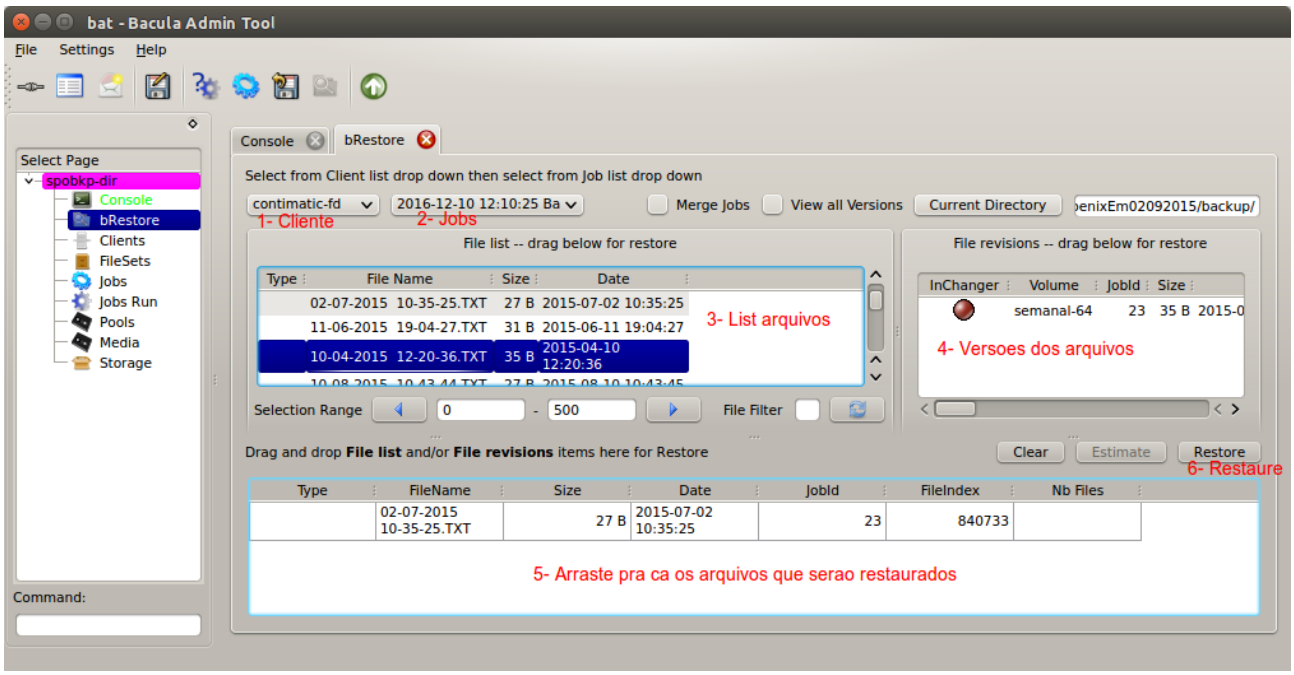


Figura 7 – Restauração com BAT

6.8. Restauração máquinas virtuais

- Leia: **/vmfs/volumes/datastore1/ghettoVCB-master/listavmrestorebkp.txt**
- Executar o script: **/vmfs/volumes/datastore1/ghettoVCB-master/ghettoVCB-restore.sh**