UNIVERSIDADE DO SUL DE SANTA CATARINA

EDUARDO PHILERENO

BACKUP, RESTORE E ARMAZENAMENTO: CONCEITOS E PRATICAS APLICADOS A SOLUÇÃO HPE DATA PROTECTOR

Palhoça

2017

EDUARDO PHILERENO

BACKUP, RESTORE E ARMAZENAMENTO: CONCEITOS E PRATICAS APLICADOS A SOLUÇÃO HPE DATA PROTECTOR

Relatório apresentado ao Curso **Tecnólogo em Gestão da Tecnologia da Informação,** da Universidade do Sul de Santa Catarina, como requisito parcial à aprovação na disciplina de Estudo de Caso.

Orientador: Prof. Roberto Fabiano Fernandes

Palhoça

2017

EDUARDO PHILERENO

BACKUP, RESTORE E ARMAZENAMENTO: CONCEITOS E PRATICAS APLICADOS A SOLUÇÃO HPE DATA PROTECTOR

Este trabalho de pesquisa na modalidade de Estudo de Caso foi julgado adequado à obtenção do grau de Tecnólogo em Gestão da Tecnologia da Informação e aprovado, em sua forma final, pelo Curso Superior de Tecnologia em Gestão da Tecnologia da Informação, da Universidade do Sul de Santa Catarina.

Palhoça, ____ de _____de _____.

Prof. e orientador Roberto Fabiano Fernandes, Dr
Universidade do Sul de Santa Catarina

AGRADECIMENTOS

Agradeço a Deus por cada dia de vida que me proporciona e a minha família, principalmente aos meus pais João Paulo Philereno e Eva Nunes Philereno, pois nunca deixaram de me incentivar a sempre ser uma pessoa melhor e também a minha amiga, namorada e mulher Kelly da Costa presente em minha vida há tantos anos e pela parceria que estabelecemos e formamos ao longo deste período.

RESUMO

Este estudo de caso visa apresentar os principais conceitos de backup, restore e armazenamento, apontando para o crescente volume de informações e de como o mesmo pode ser administrado e através da solução HPE Data Protector, elaborar um cenário de backup mostrando uma visão geral desta ferramenta bem como realizar um comparativo com outra ferramenta de backup de destaque no cenário de backup e restore.

O estudo se justificou pelo grande desafio que a TI proporciona frente ao grande volume de dados e informações armazenadas atualmente, e de que forma planejá-lo estrategicamente, já que a informação é à base de uma empresa, e a mesma deve ser gerida de forma confiável e segura, tanto por profissionais que detenham o conhecimento quanto por soluções que propiciem esta acessibilidade e facilidade ao armazenar e recuperar uma informação.

O estudo baseou-se na observação direta e analise de documentos e mostra a importância de um ambiente bem planejado para que a recuperação em caso de desastre ocorra de maneira eficiente e segura.

Palavras-chave: Backup. Restore. Armazenamento. Planejamento Estratégico.

SUMÁRIO

1 INTRODUÇÃO

A informação é o bem mais valioso de uma empresa e o armazenamento e proteção destas informações e a base central da TI, porem além de armazenar e proteger estas informações devemos buscar soluções tecnológicas que garantam a disponibilidade, integridade e desempenho destes dados.

À medida que as informações têm uma importância cada vez maior para as empresas, aumentam os desafios relacionados à proteção e ao gerenciamento de dados.

O objetivo deste trabalho é mostrar os principais conceitos de backup, restore e armazenamento bem como descrever um modelo para criar um cenário de backup e restore baseado na solução HPE Data Protector, definindo meios para criar uma política de backup e armazenamento de mídias offsite e realizar um comparativo desta ferramenta com o que o mercado oferece.

2 TEMA

Estarmos na Era da informação também resulta em produzir uma grande quantidade de dados a serem armazenados. Para uma empresa, à medida que as informações se tornam importantes e valiosas estas requerem alto grau de disponibilidade, confiabilidade e confidencialidade. Ao mesmo tempo em que o volume de dados produzido por ela seja gigantesco este precisa estar disponível de forma rápida, pratica e inteligente e este é um enorme desafio que os gestores têm pela frente, já que implica em gerenciar espaço físico, pessoas capacitadas e softwares que tragam segurança e ao mesmo tempo praticidade para gerenciar e disponibilizar as informações armazenadas.

Este trabalho tem como tema evidenciar os principais conceitos de backup, restore e armazenamento, bem como apresentar um cenário de backup com a solução HP Data Protector e elaborar uma estratégia obtendo assim um ambiente de backup com uma administração segura dos dados armazenados. Destina-se a uma organização que busca implementar um ambiente de backup bem como adotar a ferramenta HP Data Protector como modelo, também serve para análise e consulta afim de esclarecer melhores práticas para administração desta ferramenta e adoção deste modelo para um cenário real de backup bem como levantar as vantagens e desvantagens do software com algumas ferramentas de backup no mercado atual.

3 OBJETIVOS

3.1 OBJETIVO GERAL

Analisar conceitos e estratégias de backup, restore e armazenamento de dados e realizar um *overview* de um cenário de backup baseado na solução HPE DATA PROTECTOR.

1.1 OBJETIVOS ESPECÍFICOS

- Descrever conceitos e características gerais de backup e restore.
- Descrever as vantagens e desvantagens deste software em relação as demais ferramentas de mercado
- Descrever a arquitetura em que o cenário foi criado
- Detalhar questões de segurança quanto ao armazenamento das mídias, políticas de backup\restore e o modelo offsite de backup.

4 PROCEDIMENTOS METODOLÓGICOS

4.1 CAMPO DE ESTUDO

Este trabalho tem como pesquisa na forma de Estudo de caso descritivo sobre a implementação de uma arquitetura de backup contemplando software e hardware, os conceitos de backup e restore e respectivos armazenamentos.

O atual modelo de negócio nas empresas de TI é crítico e não permite correr riscos quanto a perda de informações. Planejar o backup significa não só garantir esta cópia de segurança, mas deixar o ambiente totalmente apto para cenários de desastres. Inicialmente parece um processo simples, mas é muito mais complexo do que se possa imaginar pois envolve muitas questões e planejamento, desde a infraestrutura até o software a ser escolhido, da escolha de políticas de backup e políticas de restore de acordo com a regra de negócio, do meio físico e do local de armazenamento das informações, etc.

A ideia deste estudo é disponibilizar esta infraestrutura na teoria e na pratica, esclarecer dúvidas sobre os processos de backup, politicas, mostrar pontos importantes e aos quais o administrador de backup deve ficar atento, pois em caso de perda de informações o restore será crucial para o negócio e deve ser realizado com sucesso.

4.2 INSTRUMENTOS DE COLETA DE DADOS

Os instrumentos de coleta de dados adotados neste trabalho são descritos no quadro a seguir.

Quadro 1- Instrumento de coleta de dados

Instrumento de coleta de dados	Universo pesquisado	Finalidade do Instrumento
Observação Direta ou dos participantes	Definir conceitos e a arquitetura do ambiente de backup e armazenamento assim como a implementação da ferramenta.	Obter um ambiente de backup funcional através da Solução de backup HP data Protector.
Documentos	Políticas de Backup, Politicas de Restore, procedimentos operacionais.	Documentos uteis para fins de auditoria e entendimento e operação do cenário de backup na empresa x.

FONTE: ELABORADO PELO AUTOR.

5 APRESENTAÇÃO E ANÁLISE DA REALIDADE OBSERVADA

A empresa X é uma empresa de tecnologia atuando no mercado de pagamentos eletrônicos no Brasil, oferecendo soluções de pagamento em múltiplos meios de captura, no físico e no digital (mobile e e-commerce) para pessoas físicas e empresas, com diversos serviços e canais de atendimento (Central de Relacionamento 24 horas por dia; Facebook, app e portal). A empresa x iniciou no mercado de tecnologia tendo como principal produto a recarga de telefonia celular, bilhetagem e soluções integradas na plataforma de captura oferecendo meios de soluções como correspondentes bancários e também soluções de TEF (uma solução Ideal para negócios com alto fluxo de transações, onde a máquina de cartão fica conectada ao sistema de automação comercial e à impressora fiscal) e após alguns anos entrou no mercado de adquirência com captura e o processamento de operações com cartões das principais bandeiras; operações de adquirência e operações de antecipação de recebíveis oriundos dos negócios de adquirência. Para trabalhar e oferecer as melhores soluções de mercado a empresa possui um datacenter TIER 3 bem como realiza alto investimento na área de TI anualmente, sempre buscando oferecer o melhor produto final para seus clientes e com alta disponibilidade.

DADOS, INFORMAÇÃO E ARMAZENAMENTO

A informação é à base do nosso dia a dia e muitas vezes não temos ideia do volume de dados gerado através dos dispositivos que utilizamos como celulares, maquinas de cartões, acessos à internet, etc. e o compartilhamento destas informações é o que as torna críticas e valiosas. Mas o que seriam os dados? Os dados são um conjunto de valores em estado bruto (*raw data*) recolhidos e estocados tal qual foram adquiridos, sem terem sofrido o menor tratamento e através deles é que as informações são geradas, para obtenção de benefícios, ou seja, a informação é a inteligência e o conhecimento derivado dos dados. Existem dois tipos de dados, os dados estruturados, os quais são organizados em linhas e colunas em um formato definido de forma rígida, de modo que os aplicativos possam recuperá-los e processá-los com eficiência ou os dados não estruturados, quando seus elementos não puderem ser armazenados como linhas e colunas, e assim são mais difíceis de serem processados, como mensagens e e-mail, doc., txt. As informações, contudo, são classificadas dentro de uma empresa de acordo com o valor dos dados, das regras de negócio estabelecidas entre empresa e cliente e seus SLA’s acordados, e devem ser armazenadas a fim de serem facilmente acessados para posterior processamento, então o tipo de armazenamento está relacionado à característica do negócio. Existem diversos

tipos de opções para armazenar dados, dispositivos de fitas, discos rígidos, *Storage*, virtual tape library (vtl), etc. (Somasundaram, 2011)

DATA CENTER E SUA ESTRUTURA

Tendo como base os principais conceitos de dado, como se transforma em informação e como pode ser armazenado? Onde as empresas mantem todas estas informações? Para isto, existem os chamados Data Center, os quais são centrais de dados que armazenam e gerenciam grandes quantidades de dados de missão crítica. Sua infraestrutura incluem computadores, sistemas de armazenamento, dispositivos de rede, elétrica dedicada, controles ambientais (condicionadores de ar e sistemas anti-incêndio), além do que quando temos dados de alta disponibilidade, os mesmos devem ser contingenciados, o que faz a empresa ter seu ambiente de Data Center distribuído em outra unidade, prevendo assim um balanceamento dos dados armazenados, bem como maior segurança dos mesmos, uma vez que os dados são distribuídos em dois ambientes, existe assim a possibilidade em caso de desastre, de a empresa manter seu negócio ativo. Para um Data Center funcionar ele deve possuir elementos básicos como: aplicativo, banco de dados, servidores e sistemas operacionais, rede, Storage array. Além disso, possuem como características chave fornecer disponibilidade, segurança, escalabilidade, desempenho, integridade dos dados, capacidade e gerenciabilidade. Suas atividades de gerenciamento envolvem monitoramento (O ambiente de Data Center deve ter o mínimo de circulação de pessoas e também deve operar 24 horas, sete dias por semana mantendo as condições ambientais estáveis. Um sistema de monitoramento deve permitir alertar os responsáveis sempre que houver anormalidades), geração e relatórios (normalmente os DC são alvos de auditorias e devem fornecer relatórios de temperatura e umidade diariamente, pois existem temperaturas adequadas para o funcionamento dos equipamentos, também devem fornecer informações de acesso ao DC), provisionamento, que seria fornecer hardware, software e outros recursos necessários para o funcionamento do Data Center, isto envolve planejamento de capacidade e recursos. Por exemplo, ao planejar um Data Center, os quadros elétricos devem ser projetados e montados de acordo com as cargas elétricas específicas do data center e capazes de permitir o acionamento dos sistemas de UPS e geradores sem paralisação no funcionamento do data center.

BACKUP E RESTORE

Backup é uma cópia de segurança de dados de produção, desenvolvimento ou homologação (sim, um ambiente de desenvolvimento ou homologação perdido pode custar muito tempo e dinheiro) que é mantida e armazenada com o propósito de recuperação em casos de

desastre, ou perda acidental de dados. Como o volume de dados cresceu muito e também hoje existem diversas normativas de armazenamento, preservação e disponibilidade de dados, as tarefas de backup aumentam, o volume de dados aumenta e consequentemente o armazenamento cresce, as tecnologias evoluem e propiciam rapidez e praticidade na hora de recuperar um dado. O grande desafio é que o backup dentro de qualquer empresa acaba por ser tratado como um custo, então nem sempre o investimento e alto, ou seja, devemos manter um ambiente de backup com o mínimo de recursos e de baixo custo. Backups são feitos por três motivos: recuperação de desastres, backup operacional e arquivamento. Por exemplo, no caso de recuperação de desastres, as copias de dados são usadas para restaurar dados em um local alternativo. Quando utilizamos a estratégia de backup com fitas físicas, por exemplo, estas devem ser armazenadas em um local diferente, assim num cenário de desastre as fitas são trazidas para que os dados sejam recuperados ou podem ser recuperados em outro local também. Existe a possibilidade também de um site realizar a replicação do dado remotamente. Já o backup operacional é um backup dos dados de um determinado momento e que serve para recuperar o ambiente no caso de perda de dados ou corrupções logicas. Aqui se encaixam situações de rotinas diárias, por exemplo, em um servidor de arquivos, realizamos em um período do dia o backup dos dados, e em caso de perda de um arquivo de um usuário, podemos voltar o último backup em fita realizado. Um backup de um banco de dados também se encaixa nesta situação, realizamos o backup diário de um banco e em caso de este banco ser corrompido, podemos voltar o último backup juntamente com os archives do banco e recupera-lo. Existe também a situação de arquivamento, onde um dado deve ser armazenado por um longo período de tempo, devido a regra de negócio da empresa, por questões de leis, etc. Obviamente, um dado pode ser armazenado em Storage e replicado, porem devemos avaliar o investimento e a estratégia, pois tudo e custo, por isso o negócio da empresa irá ditar o caminho a ser seguido na implementação de backup. O fato é que ao adotarmos a solução de backup devemos levar em conta o período que os dados devem ser armazenados, alguns dados deverão ser mantidos por alguns dias, outros por alguns anos. O tipo de mídia a ser utilizada e um ponto importante já que os dados devem estar disponíveis e acessíveis ao longo do período armazenado, a granularidade do backup, que será detalhada posteriormente. Dentro de uma estratégia de backup, devemos levar em consideração o horário apropriado para que este backup seja feito, o horário em que vamos fazer um restore e importante também para não onerarmos o ambiente de produção gerando trafego de dados quando não temos uma rede dedicada de backup, o tamanho dos arquivos a serem copiados e importante ao definir a estratégia. O tempo de backup e restore e diretamente influenciado quando tratamos de arquivos muito pequenos, ou seja, copiar 100 arquivos de 10GB e muito melhor que copiar 10.000 arquivos de 1kb. A tecnologia de fita e drive utilizada influencia no desempenho do backup e restore, já que se a operação de montar a mídia, iniciar

e parar o backup for lenta ira causar um desempenho ruim na execução do backup ou restore. Um fator importante e utilizado também e a compactação dos dados já que influencia na utilização das mídias, trazendo economia de espaço.

GRANULARIDADE DO BACKUP

A granularidade do backup depende das necessidades da empresa e dos RTO/RPO requeridos. Assim, eles são classificados como completos (*Full*) cumulativos (*DIF*) e incrementais (*INCR*). Normalmente utilizamos estas três combinações dentro de um ambiente para atender ao backup e restore. O backup Full, como o próprio nome diz, faz uma cópia de todos os dados para um conjunto de mídia. A vantagem que teremos é de que a cópia completa estará disponível em um único conjunto de mídias. Isso resulta em uma possibilidade maior recuperar os dados íntegros, menor complexidade da operação de recuperação e o menor tempo para recuperar os dados, métrica conhecida como *Recovery Time Objective* (RTO). No entanto, as principais desvantagens são que leva mais tempo para executar um backup completo do que outros tipos, e requer mais espaço de armazenamento, já que todos os dados são armazenados a cada backup realizado. O backup incremental é a cópia de todos os dados que foram modificados desde o último backup de qualquer tipo. O último backup pode ser um backup Full, diferencial ou incremental. Um backup Full é realizado inicialmente e nos backups subsequentes são copiados apenas os dados alterados ou criados desde o último backup. O benefício de um backup incremental é que será copiada uma menor quantidade de dados do que um completo. Assim, esse backup será realizado mais rápido e necessitará menos espaço de armazenamento, porem o restore será mais lento, pois deve ser restaurado o backup Full mais os incrementais de cada dia até o momento em que houve o incidente. Alguns softwares de backup trabalham com o backup *incremental forever*, significa que este faz um backup full inicial e após trabalha somente com backups incrementais para “o resto da vida”. O backup cumulativo ou diferencial é semelhante a um incremental na primeira vez em que é realizada, na medida em que irá copiar todos os dados alterados desde o backup anterior. No entanto, cada vez que é executado após o primeiro backup, serão copiados todos os dados alterados desde o backup completo anterior e não com relação ao último backup. A cópia será mais lenta do que a cópia do backup incremental, porem o restore será mais rápido. O backup completo sintético é criado a partir de um backup full mais recente e todos os incrementais executados após este backup Full. O backup sintético unifica o backup Full mais incrementais e permite criar um único backup Full off-line, o que facilita na hora do restore. O RPO e o RTO são importantes ao planejarmos uma estratégia de backup. *O* Recovery Point Objective (RPO) irá determinar a frequência dos backups bem como sua retenção, está relacionado à quantidade de dados que a

empresa toleraria perder se, por exemplo, sofresse um incidente no ambiente de produção, ou parada de algum sistema ou um cenário de desastre, ou até mesmo uma parada decorrente de uma ameaça ou de um possível risco de ataque ou invasão de hackers. A pergunta a ser respondida é: com quais perdas a organização consegue lidar com relativa tranquilidade antes que as operações vitais sejam afetadas e os principais resultados de seu trabalho sejam comprometidos? Com relação ao período de retenção, e importante defini-lo com base em uma análise das solicitações de restaurações do passado e no orçamento alocado e com base nas regras de negócio da empresa, bem como a disponibilidade dos dados. Já o RTO (*Recovery Time Objective*) se relaciona ao tempo gasto pelo processo de recuperação. O RTO influencia no tipo de mídia e consequentemente na solução e tecnologia de armazenamento a ser adotada. Devido às restrições de recuperação, as organizações executam mais backups Full do que realmente precisam. Backups cumulativos e incrementais dependem de um backup Full prévio. Quando restauramos um backup incremental ou cumulativo utilizamos mais mídias e com isso o restore e mais demorado. Com um backup Full o RTO será mais baixo e em menos passos na tarefa de restore.

METODOS DE BACKUP

Backup dinâmico e backup estático são dois métodos implantados para a execução de um backup e são baseados no estado do aplicativo no momento da cópia. Em um backup dinâmico, os arquivos estão abertos e sendo acessados pelo usuário, já não backup estático isto não ocorre já que o aplicativo não fica ativo. Com o avanço das soluções de backup a mesma fornece agentes que permitem a cópia com o arquivo aberto, pois interagem com o SO e criam cópia de arquivos abertos, mas imagine casos, por exemplo, em que a copia do arquivo aberto não é possível, por exemplo, em um backup de banco de dados. Para que tenhamos um backup de banco integro, todos os arquivos precisam ser gravados no mesmo estado e existem diversas estratégias para que isso ocorra, mas basicamente um backup de banco pode ser gerado de maneira integrada, off-line, onde o banco e baixado e o backup e realizado, ou podemos usar ferramentas de Job Schedule, onde é criado um Job de dump, que gera o backup do banco via rman em uma área em disco e após outro Job de backup dependente do dump que copia esta área do backup em disco para fita. Uma ferramenta de Job Schedule muito utilizada é o Control-m. Obviamente para gerar backup em disco você devera prover de uma infra mais robusta utilizando *SAN*, área de Storage, e com certeza o custo será maior, porem este método traz segurança, uma vez que o último backup está sempre em disco, assim como os próprios archive, e a recuperação é mais rápida durante um incidente. Existe também o método de cópia point in time (PIT) que é implantado em ambientes nos quais o impacto do

tempo inativo causado por um backup estático ou o desempenho de um backup dinâmico sejam inaceitáveis. Uma cópia PIT baseada em ponteiros consome penas uma fração do espaço de armazenamento e pode ser criada rapidamente. A solução de cópia é baseada em disco na qual uma LUN virtual e criada e armazena ponteiros para os dados armazenados na LUN de produção ou local de gravação. Neste processo o banco e congelado momentaneamente (*Begin* Backup) enquanto a cópia PIT é criada, que é montada em um servidor secundário e o backup ocorre no servidor primário.

O backup com *dedup* é ideal para operações altamente redundantes como o backup que exige copiar e armazenar repetidamente o mesmo conjunto de dados diversas vezes para fins de recuperação durante períodos de 30 a 90 dias. Como resultado, empresas de todos os portes dependem do backup e recuperação com desduplicação para obter backup e recuperação rápidos, seguros e econômicos.

Um arquivo ou volume a partir do qual é feito backup semanal cria um volume significativo de dados duplicados. Os algoritmos de desduplicação analisam os dados e armazenam apenas os segmentos compactados e exclusivos de um arquivo. Esse processo pode fornecer uma média de redução de 10 a 30 vezes nos requisitos de capacidade de armazenamento, com políticas médias de retenção de backup sobre os dados corporativos normais. Isso significa que as empresas podem armazenar de 10 a 30 TB de dados de backup em 1 TB de capacidade de disco físico, o que gera grandes benefícios econômicos. A desduplicação reduz os custos de armazenamento, pois menos discos são necessários. Ela também melhora a recuperação de desastres, pois há muito menos dados a transferir. Em geral, dados de backup e de arquivamento incluem muitos dados duplicados. Os mesmos dados são armazenados repetidas vezes, consumindo espaço de armazenamento desnecessário em disco ou fita, eletricidade para resfriar as unidades de disco ou fita e largura de banda para replicação. Isso cria uma rede de ineficiência de custos e recursos dentro da organização. Não podemos esquecer também que para assegurar a consistência dos dados, certos atributos e propriedades vinculadas a um arquivo, como permissionamento e outros metadados que também precisam ser gravados, eles são tão importantes quanto os próprios dados e devem ser gravados, normalmente a solução de backup tem esta inteligência e garante esta integridade ao copiar um dado. (EMC, 2017)

O PROCESSO DE BACKUP

Uma solução de backup utiliza a arquitetura cliente/servidor, onde temos um Backup Server (servidor de backup rodando a solução) e diversos clientes de backup. O servidor de backup é responsável pela gerencia das operações, nele fica o banco com o catalogo de backup, que contém informações sobre os processos e metadados do backup, também controla toda a questões dos schedules de backup, horários, tipos de backup a serem feitos (Full, INCR ou DIF), restore dos clientes, etc., ou seja, as políticas são definidas no servidor de backup, bem como o fornecimento de relatórios baseados nos dados armazenados no servidor de backup, estes relatórios incluem volume de dados gravados, números de backups completos com sucesso, número de falhas, enfim, uma série de informações para administra o ambiente. Através dos clientes de backup que o servidor de backup irá coletar os dados a serem gravados e armazenados. O servidor de backup inicia o processo enviando uma solicitação ao cliente de backup (um cliente também pode iniciar um backup), onde os metadados são enviados ao servidor de backup e os dados são enviados há um nó de armazenamento, que seria na verdade o responsável por gerenciar o dispositivo de armazenamento, este nó de armazenamento pode ser o próprio servidor de backup ou um servidor especifico. Depois de todos os dados serem gravados, o no de armazenamento encerra a conexão com o dispositivo de backup, e o servidor de backup grava no catalogo de metadados o status de backup encerrado.

OPERAÇÕES DE BACKUP E RESTORE

Basicamente uma operação de backup e restore funcionam da seguinte maneira: o processo de backup é iniciado manualmente ou através de um agendamento, o servidor de backup consulta as informações mantidas em seu catálogo de backup e aciona o nó de armazenamento para que este carregue a mídia no dispositivo de armazenamento, simultaneamente o servidor de backup então orienta os clientes a iniciar o envio dos dados para o nó de armazenamento que envia os dados para a mídia e também os metadados para o servidor de backup, este processo é feito utilizando a infraestrutura de rede. Assim, com os dados em mídia e o catalogo de backup atualizado, o processo de restauração pode ser executado quando necessário. O restore varia de acordo com a solicitação, uma informação pode ser restaurada em seu local de origem ou um local alternativo, tanto no cliente original como em outro cliente.

TOPOLOGIAS DE BACKUP

Existem três topologias básicas utilizadas em um ambiente de backup: o backup de conexão direta, backup baseado em LAN e backup baseado em SAN, podendo existir também e é ate muito comum em grandes empresas, a topologia mista, que inclui LAN e SAN.
Em um backup de conexão direta o dispositivo de backup e ligado imediatamente ao cliente, assim os metadados são enviados ao servidor de backup pela LAN, contudo, o trafego de backup não irá onerar a LAN. Já em um backup baseado em LAN, todos os servidores são conectados a LAN e os dispositivos de armazenamento são anexados diretamente ao nó de armazenamento, com isso, ao realizarmos o backup iremos trafegar os dados pela LAN, podendo impactar no desempenho da rede e onerar os servidores de produção. Claro que podemos também segregar a LAN e criarmos uma LAN de Backup, conhecida as vezes como rede branca, na qual cada servidor esta ligado com "uma perna" na mesma, e termos uma LAN para serviços e outra para produção, assim não iremos trafegar os dados de backup no mesmo caminho dos dados de produção. Além de segregar as redes, é possível instalar nos de armazenamento dedicados para alguns servidores de aplicativos. O backup baseado em SAN é apropriado quando um dispositivo de backup é compartilhado entre clientes. Utilizar uma SAN que seja criada especificamente para backup gera excelente desempenho, pois trata os dados de backup separados e deixa os metadados a serem enviados pela LAN, que no caso, são pequenas informações e não onera o ambiente de produção, já que o maior trafego vai para fita via SAN.

Com uma SAN teremos um host que irá possuir uma área de Storage (array de discos) e poderemos enviar este dado do disco para o dispositivo de armazenamento em fita física ou vtl e assim enviar estas mídias físicas para serem guardadas e armazenadas externamente, para que em caso de perda de um ambiente possamos restaurar os dados em outro local. Esta topologia de SAN é implementada quando buscamos performance e desempenho, cada cliente de backup deverá ter uma Hba que trafegue dados de produção e uma Hba que trafegue dados de backup, e que estas sejam segregadas fisicamente, pois assim teremos um melhor desempenho e não estaremos trazendo riscos ao ambiente e ao próprio cliente, já que impacta em I/O, utilização de memória e recursos de cpu do host.

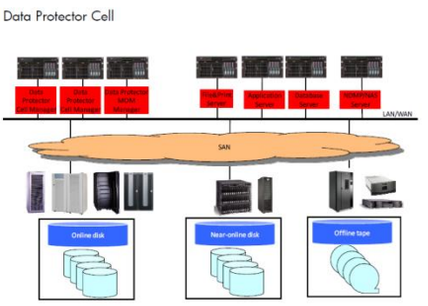
TECNOLOGIAS DE BACKUP

Existem diversas soluções de tecnologia para backup no mercado sendo que as soluções de fita e disco são as mais utilizadas em empresas, assim como as tecnologias de fita virtuais que utilizam discos como mídia que emulam fitas, sendo assim a leitura e montagem tende a ser mais rápida já que todos os dados e mídias estão presentes em disco. O backup em

fita é montado e lido em um drive e é um dispositivo de acesso sequencial, ou seja, os dados são gravados ou lidos sequencialmente. Dependente da Library ou biblioteca que contém os cartuchos e drives, aliado a uma rede de alta performance (SAN) o uma LAN segregada, podemos armazenar uma grande quantidade de dados em fita e numa velocidade considerável. Uma *library* é gerenciada pelo software de backup, ele tem inteligência suficiente para gerenciar o braço robótico e todo o processo de backup. Nestas *library* os drive são responsáveis por ler e escrever nas fitas, que são mantidas dentro da mesma nos slots, enquanto não estão sendo usadas. As fitas são usadas para armazenamento externo e em longo prazo e as mesmas devem ser armazenadas em cofres e em salas com ambiente climatizado de acordo com o fabricante de cada mídia. Já o backup em disco tem sido muito utilizado pois traz vantagens em termos de desempenho, custo de serviço e implementação e uma excelente qualidade. Com uma tecnologia de disco o restore será mais rápido. Usar backup em disco impõe que os administradores estejam cientes da estrutura, fragmentação, tamanho de arquivos, tipos de sistemas de arquivos, tamanho de blocos e cache dos sistemas de arquivos. Já a VTL (*Virtual tape Library*) ou biblioteca virtual, emula uma biblioteca de fitas físicas, o que não traz diferença para o software de backup. Elas utilizam discos como mídia de backup. O software de backup tem um banco de dados com uma lista de fitas virtuais e a cada fita virtual e atribuída uma parte de uma LUN no disco, e uma fita virtual pode se espalhar por várias *LUNs*. Os passos de backup e restore são semelhantes ao de uma biblioteca física, montagem de mídia no drive, leitura dos dados, etc. A replicação sobre IP está disponível com a maioria dos dispositivos de biblioteca de fita virtual. Este recurso permite que fitas virtuais sejam replicadas em uma rede IP barata até um local remoto. Também é possível enviar os dados armazenados nas bibliotecas virtuais para fitas físicas. Usar fitas virtuais oferece diversas vantagens tanto sobre fitas físicas como discos. Fitas virtuais não requerem processos de limpeza ou calibragem dos drives e da *library* e possuem fácil administração.

HPE DATA PROTECTOR – ARQUITETURA E PLANEJAMENTO

Figura 1 - Data Protector Cell



Fonte: (Hewlett Packard Enterprise Development LP, 2010, p. 3)

O HPE Data Protector é uma solução de backup enterprise de arquitetura cliente/servidor e altamente escalável com enorme flexibilidade se ajustando as necessidades e mudanças organizacionais. Trabalha com os principais conceitos de backup (FULL, INCR, SINTETICO) e com os principais agentes de integração (Oracle, SAP, SQL, EXCHANGE, VM e outros mais). O Data Protector atua por meio de um *CELL MANAGER* e nele esta localizado todo o gerenciamento de backup e restauração. Na sua implementação mais simples utiliza apenas duas camadas, o *Cell Manager* e o *Cell Client*. Através de uma console GUI que roda com Java podemos administrar diversos Cell managers a partir de um ponto único. Os principais serviços de um Cell Manager em UNIX são o CRS (*Cell Request Server*), RDS (*Raima Database Server*) e o MMD (*Media Management Daemon*) e no Windows Data Protector CRS, Data Protector RDS e Data Protector Inet. No Unix esta localizado no caminho */opt/omni/lbin* e no Windows em *C:\Program Files\Omniback\Bin.* Geralmente estes serviços são iniciados automaticamente, porem podemos fazê-los via linha de comando, utilizando o comando *omnisv –start, omnisv –stop, omnisv -status.* Há também outros serviços, por exemplo, quando executamos um backup o serviço ativo é o *BSM*, quando executamos um restore, *RSM*, para cópia de dados é C*SM*, e para sessões do banco *DBSM*, para gerenciamento de mídia MSM e para sessões administrativas *ASM* ou *admnistration session manager*. No HPE temos dois agentes de backup, o DISK Agent e o Media Agent: o primeiro, responsável por ações de leitura e gravação das unidades de disco para backup e restore e o segundo, responsável pelas ações de leitura e gravação para mídias de backup, podendo estas serem fita ou disco). Resumindo, ao configurarmos um cliente para fazer um backup de LAN, utilizamos o agente do Disk Agent e para realizar um backup de SAN utilizamos o Disk Agent e o Mídia Agent, o qual ira controlar o dispositivo de mídia e também é necessário para configurar o backup via SAN. No Data Protector podemos dar permissões e criar perfis de usuários para que estes possam gerenciar ou não a ferramenta, ou apenas ter permissão para acessar o cliente e monitorar as sessões de backup sem realizar tarefas administrativas. Através desta opção *USERS* também inserimos os usuários com permissões para utilizar as integrações de backup, como Oracle, SAP, VM, Exchange, etc. O gerenciamento de mídias do Data Protector é responsável pelo gerenciamento dos dispositivos de mídias e pela criação dos pools de mídia, que nada mais são do os locais onde as fitas serão armazenadas e gerenciadas, assim quando criamos um Job de backup devemos associa-lo a um *device*, que seria o dispositivo de mídia, um pool que será responsável por alocar as mídias onde os backups serão gravados. Estes pools são de fácil organização na ferramenta e de fácil administração, sendo assim, ao realizarmos diversos backups diários, podemos associa-los há um pool de mídias diário, então todos os dados de backup diários estarão nestas mídias dentro deste pool, isso facilita a organização e a administração das mídias. Dentro de *um media pool* podemos criar um freepool, que é onde serão armazenadas as mídias novas

ou expirada ou com dados retidos, as quais serão usadas e associadas aos Jobs de backup. No gerenciamento de medias, temos as opções de *device*, que será onde iremos configurar os dispositivos de mídias (tapes) para associarmos aos backups e também gerenciar e administrar as mídias do data Protector e *library* de backup juntamente com os drive. O Data Protector também oferece a opção de realizar a copia de objetos, realizar consolidação dos dados para liberar espaço nas mídias, duplicar mídias, enfim, oferece uma serie de possibilidades para copia dos dados. Na aba reports dentro da console GUI teremos a opção de realizar e configurar diversas formas de relatórios, de sessões de backup, de uso dos drives, de gerar relatórios de monitoria diários para validação dos backups, enfim, teremos varias opções de reports. Dentro da Aba sessions poderemos acompanhar qualquer histórico de sessões de backups já executados, bem como identificar logs de backups com falha e reprocessar os mesmos caso seja necessário, as sessions também auxiliam com informações para fins de auditoria. Para realizar restore das informações backupeados existe a aba restore dentro da console que é muito simples e intuitiva, com diversas opções de restore, seja em local original ou alternativo e diversas possibilidades. No Cell Manager trabalhamos com o conceito de Installation Managers ou servidores de instalação, que serão responsáveis pela instalação remota dos clientes de backup. Por exemplo, quando vamos realizar a instalação de um cliente Windows, realizamos isto remotamente através de um servidor que estará configurado dentro do Cell manager com os agentes de backup e integrações do Data Protector para plataforma Windows. Este processo facilita muito a instalação e *import* do agente para dentro do Cell Manager, pois é pratico e rápido. Lembrando que temos que ter as seguintes portas liberadas para o funcionamento do Data Protector: 5565, 5555, 7112, 7113, 7116 e 9999. Existe um arquivo GLOBAL que podemos realizar diversas alterações de configurações administrativas do Data Protector. Existe um cheklist essencial para que a solução de backup seja efetuada com êxito e para administrarmos de maneira eficiente o Data Protector, como Analisar bem a sua rede e sua estrutura, e definir quais ambientes e que o backup será necessário. Importante verificar se no seu ambiente será realizado backup que necessitam de integrações, como Oracle, SAP, VMware, Exchange, etc., e que você tenha uma ideia de volume de backup a ser realizado nestes ambientes. Outro passo importante é definir para a instalação do seu Cell Manager qual a plataforma em que o mesmo será instalado e configurado, defina os sistemas que você ira instalar o cliente e quem serão os usuários a terem acesso as configurações do *Cell Manager* através da GUI, lembrando que os acessos põem ser restringidos e liberados de acordo com a função do usuário que ira acessar o cliente. Identificar quais os seus dispositivos de mídias, em que locais serão armazenados, bem como se dará por LAN ou SAN, ou uma rede mista. Planeje a segurança através da criptografia dos dados, onde a mesma pode ocorrer via software ou via hardware, onde é feita a criptografia no drive de

backup. Também É importante planejar como será a organização dos backups, quais as retenções e em quais pools de mídias serão armazenados, se ira realizar mais de uma copia destes dados, planeje a configuração dos pools, mídias, relatórios. Crie uma tarefa diária para o backup do banco (IDB) e como se da a administração deste banco do DP e procure entender sobre os processos de desastre e recovery do ambiente, entenda como funcionam a monitoração das sessions, se pode ser integrada com alguma ferramenta de monitoração externa. Em nosso cenário, utilizaremos um ambiente misto, de LAN e SAN com uma rede segregada de backup. A politica foi elaborada baseada num cenário de alta disponibilidade e dados críticos respectivamente, com backup de file system, Oracle, SAP, VMware e Exchange. Para o Cell Manager utilizamos uma vm com Windows Server 2012, e para os servidores de instalações usamos um server para Unix e o servidor de instalação Windows é o próprio servidor de backup ou Cell Manager. Para controlar os dispositivos de mídia utilizamos um servidor físico com Hba com plataforma Linux RedHat que controla uma library IBM 3592JC e também uma tape virtual de backup. Através da console gerenciamos dois sites de backup, com localidades diferentes, todos os ambientes são gerenciados por um único Cell manager, uma vez que a solução oferece esta possibilidade. O backup de banco é feito em parte em vtl e parte em disco (área de Storage) e após enviado para fita.

DEFININDO UMA POLITICA DE BACKUP

Basicamente, para criarmos uma politica de backup, é necessário conhecermos o ambiente envolvido, nos reunirmos com as áreas da empresa e planejarmos quais os dados que devem ser enviados para fita e a criticidade dos servidores envolvidos. A politica a seguir foi elaborada para o ambiente da Empresa X e pode servir como um modelo para um ambiente de alta disponibilidade. Conhecendo o ambiente, podemos criar nomenclaturas relacionadas aos serviços e aplicações, conforme modelo abaixo:

Quadro 1 - Modelo de classificação dos servidores

	DESCRIÇÃO	EXEMPLO
DB_PROD	Banco de Dados – Produção	Oracle, SAP, Sybase, SQL
DB_HDQ	Banco de Dados – Homologação, Desenvolvimento e Qualidade	Oracle, SAP, Sybase, SQL
FS	*File System* (Sistema de Arquivos)	Arquivos de usuários
TL	*Transational Logs*	*Logs* transacionais
APL	Aplicações	Binários de aplicações
SO	Sistema operacional	Arquivos de SO dos servidores
VM	*Virtual Machines* – Máquinas virtuais	Arquivos de extensão *.vmdk* de máquinas virtuais
MAIL	E-mail	Servidores Exchange e Postfix
ARC	*Archives*	*Archives* de bancos de dados

Fonte: Elaborado pelo Autor.

Precisamos definir a frequência em que as cópias de segurança devem ser realizadas e a respectiva retenção de cada uma destas cópias em semanas. Sendo que as colunas indicam quando é feito e as linhas o tempo de retenção.

Tabela 1 - Definições de retenção dos objetos a serem armazenados

Tipo	Diário – 1xD	Semanal – 1xS	Mensal – 1xM	Anual – 1xA
DB_PROD	3 S	-	53 S	261 S
DB_HDQ	3 S	-	27 S	-
FS	3 S	-	53 S	105 S
TL	3 S	-	261 S	-
APL	3 S	-	53 S	-
SO	-	5 S	-	-
VM	-	-	8 S	-
MAIL	3 S	-	53 S	-
ARC	3 S	-	-	-

Fonte: Elaborado pelo Autor.

Tabela 2 - Classificação das retenções

Tempo em Semanas (S)	Tempo em Dias (D)	Tempo em Meses (M)	Tempo em Anos (A)
3 S	21 D	-	-
5 S	35 D	1 M	-
27 S	185 D	6 M	-
53 S	370 D	-	1 A
105 S	735 D	-	2 A
261 S	1835 D	-	5 A

Fonte: Elaborado pelo Autor.

As cópias de segurança em ambientes de homologação e desenvolvimento seguem as mesmas regras para cópias de segurança em ambientes de produção, exceto o tempo de retenção que é menor. Porém, nestes ambientes, as cópias não são prioritárias e jamais podem sobrepor quaisquer cópias de segurança do ambiente de produção.

Os *media pools* são definidos e organizados de acordo com as retenções utilizadas por cada tipo de cópia de segurança. Para facilitar o gerenciamento e padronizar a organização das *medias pools*, é definido o seguinte padrão para a nomenclatura das mesmas:

Empresa X Região: EX_CBM_EXNOMEDOSERVIDORCB_LTO4_007_DIAS
Empresa X Região: EX_SPO_ EXNOMEDOSERVIDORSPO_LTO5_105_SEMANAS

As rotinas de cópia de segurança são organizadas de uma forma semelhante aos *media pools*.

Exemplo de uma Organização de uma rotina de backup e sua respectiva nomenclatura:

Empresa (2 dígitos)_Cidade (3 dígitos)_Tecnologia_Retenção.

DEFININDO UMA POLITICA DE RESTORE

Basicamente a política de restore consiste em Padronizar e orientar sobre um processo para teste de mídias de Backup realizado regularmente, para garantir que elas são confiáveis no caso de uso emergencial. Adotamos um teste de restore baseado na empresa x e que possa servir como modelo para um ambiente de alta disponibilidade e que armazene mídias offsite. Como requisitos para um teste de restore eficiente, devemos prover testes de restore para todos os tipos de aplicações, tais como: *file server*, banco de dados, *logs* transacionais, e-mails, sistemas operacionais e assim estes testes devem contemplar 1% do total de fitas de backup existentes na empresa X, e também devem ser realizados testes de restore com mídias de 1, 3 e 5 anos de retenções. A sugestão de fluxo funciona da seguinte maneira: A cada 3 meses a ferramenta de gerenciamento de serviços abrirá automaticamente um chamado para equipe responsável por administrar a ferramenta de backup para realizar os testes nas mídias de backup, com um SLA de 4 semanas para atendimento. As mídias selecionadas para o teste devem seguir os requisitos citados acima, por tempo de retenção. Para solicitar uma mídia que esteja armazenada no fornecedor deve-se acessar o seu site com login e senha previamente cadastrado, e selecionar as mídias a serem a enviadas. Conforme solicitação realizada pelo site, o fornecedor deve enviar as mídias para o cliente no prazo de até 3 dias uteis. De acordo com a disponibilidade no drive, a equipe responsável deve realizar o teste, efetuando um Restore da mídia e validando se o dado/informação do Backup está íntegro e funcional. Após a realização dos testes, devem ser armazenadas no chamado as evidências, que basicamente consistem em salvar um log contendo (nome do servidor, data, tempo e tamanho do Restore) o nome desse arquivo deve conter o “nome do servidor e da mídia e de cada mídia que foi testada”; após, devemos registrar o resultado do teste. Posteriormente esse chamado deve ser encaminhado para equipe de Segurança da Informação para que as evidências sejam validadas. A equipe de Segurança da Informação deve validar se as evidências registradas estão de acordo, e bem como o resultado do teste. Se os registros estiverem corretos essa equipe deve registrar no chamado o seu “De acordo”, e reenviar o chamado para equipe responsável (Backup). Após receber o chamado com a validação da área de Segurança da Informação, deve iniciar a devolução das mídias testadas para o fornecedor. Essa devolução deve ser realizada dentro do fluxo normal de transferência de mídias que tem data estabelecida por contrato. Tendo concluído as atividades descritas anteriormente o chamado deve ser encerrado na ferramenta de gerenciamento de serviço.

ARMAZENAMENTO DE MÍDIAS OFFSITE:

Consiste em realizar a guarda de mídias de backup de maneira externa, sendo assim, as mídias de backup são armazenadas em cofre local e também com envio para offsite, este envio varia de acordo com as normas e contratos estabelecidos, e também com a criticidade do negocio, também é estabelecido de acordo com o tipo de implementação de backup, por exemplo, se um ambiente possui replicação dos dados e da base de backup, e possui contingencia de todo o site, e esta contingencia funciona numa distancia considerável, é possível armazenar as mídias com menor retenção localmente e mandar para offsite apenas os dados históricos, que são armazenados por um período longo. O modelo adotado pela Empresa X funciona com armazenamento local e externo e tem as seguintes premissas: os backups diários que são realizados com uma retenção menor são armazenados em um cofre local, já os backups históricos são enviados semanalmente, uma vez que as coletas e remessas funcionam uma vez por semana. Por questões de segurança todo o transporte das mídias deve ser feito com maletas adequadas e com carros adequados e que possuem a temperatura dentro das normas do fabricante das mídias. Podemos também adotar, caso o ambiente permita, armazenar os backups em disco e gerar uma copia destes dados em fita e manda-los para offsite, além de ter este ambiente replicado para outro site, e neste outro site também manter estas configurações. Obviamente este tipo de administração requer alto investimento em armazenamento e tecnologia, porem estará 100% garantido em caso de desastre. Uma sugestão de guarda de mídias offsite é a empresa Iron Mountain, que hoje é responsável pelo gerenciamento de mídias de grandes empresas no cenário nacional e internacional.

HPE DATA PROTECTOR: COMPARATIVO ENTRE FERRAMENTAS DP X TSM

Existem algumas soluções de backup bastante utilizadas no cenário nacional e uma delas é o TSM, Tivoli Storage Manager, da IBM, uma ferramenta a qual também utilizamos em nosso ambiente de backup. O TSM esta há bastante tempo no mercado e é uma das principais ferramentas de backup e gerenciamento de armazenamento, por sua estabilidade e confiabilidade, convenhamos, não é nada pratico, mas funciona muito bem no que se propõe a desempenhar. É uma solução enterprise e abrange todos os tipos de plataformas heterogêneas bem como suporta todos os tipos de armazenamento (SAN, LAN, Conexão direta) bem como politicas flexíveis para se adaptar a qualquer tipo de negócio, além de permitir a administração centralizada do ambiente (BROOKS, 2006). Aliás, aí está um ponto positivo para o Data Protector no que diz respeito a acessibilidade e praticidade da ferramenta, o Data Protector possui uma interface muito intuitiva e é muito fácil criar um backup, realizar um restore, instalar um cliente,

enfim, as tarefas administrativas são muito simples para trabalhar no dia a dia e visualizadas através de interface gráfica. O TSM é oriundo do mainframe, então ele difere bastante no que diz respeito a sua utilização e alguns conceitos: ele praticamente é gerenciado por linha de comando, não que isto seja um problema, mas se você esta habituado a interface gráfica somente, ira demorar um tempo a se acostumar com as tarefas administrativas do dia a dia no TSM e entender os seus conceitos e de como ele atua, uma simples instalação de cliente requer alguns passos a mais e diversas configurações entre server e cliente, nada que com o tempo não seja dominado, mas em termos de facilidade deixa a desejar, a parte gráfica do TSM praticamente é nula e este seria um ponto de melhoria na ferramenta, uma vez que hoje, no cenário atual, as ferramentas precisam ser eficazes e praticas, para não perdermos tempo nas atividades de backup restore. O banco do TSM funciona muito bem e se é baseado em DB2, oferecendo a possibilidade de diversas consultas e tarefas administrativas através de *selects* no banco, isto faz com que possamos extrair qualquer informação da ferramenta e banco funciona muito bem, sendo outro aspecto positivo da solução. O TSM possui um ponto positivo no que diz respeito a criptografia já que seu ambiente é criptografado sendo que no Data Protector isto requer licenciamento ou host por host ou no hardware, o que acaba encarecendo um pouco o valor final do produto. Uma vantagem do Data Protector é que em ambientes de desastre recovery é pratico e fácil recuperar um ambiente, uma vez que basta importar a fita com o backup banco no local a ser recuperado e as informações são facilmente recuperadas. Analisando as duas ferramentas e já tendo trabalhado com as duas, não considero uma melhor que a outra, mas são diferentes e em casos de implementação, você deve optar por uma POC com os dois cenários, parar interagir e decidir qual a melhor solução a ser implementada.

6 PROPOSTA DE SOLUÇÃO DA SITUAÇÃO PROBLEMA

6.1 PROPOSTA DE MELHORIA PARA A REALIDADE ESTUDADA

É fundamental destacar a importância do planejamento estratégico antes de realizar uma implementação. Conhecer o seu ambiente e o que é realmente necessário armazenar faz com que os investimentos e custos sejam reduzidos, e permite realizar a escolha da solução de backup ideal para sua empresa, pois não existe uma solução ideal e sim a que melhor se adapta ao seu ambiente. Planejar e executar reuniões com as áreas de negocio da empresa a fim de entender qual é a disponibilidade dos dados a serem armazenados, para assim propiciarmos o tempo de restore adequado garante eficiência quanto a disponibilidade dos dados e dentro do tempo desejado. A escolha de um gerente de projeto mapeando os principais pontos da imple-

mentação trará êxito a mesma e identificara eventuais pontos de falhas durante a implementação, bem como a execução de uma POC com diferentes fornecedores e soluções, para identificar qual se adequa ao seu ambiente. Outro ponto importante a destacar como melhoria é a elaboração das politicas de backup e restore e armazenamento offsite para que os clientes estejam cientes de como funcionam as retenções dos dados armazenados e os prazos de recuperação caso a mídia esteja fora do ambiente, como uma rotina de backup deve ser solicitada, bem como testes e restore que garantam a funcionalidade dos dados armazenados. Um ponto de melhoria para a ferramenta HPE Data Protector esta relacionada ao licenciamento do HPE Data Protector: existem licenças que limitam o uso de drive, o uso de criptografia, licenças para backups simultâneos, enfim, o investimento em uma infraestrutura de grande porte é alto. O ideal é que a ferramenta seja licenciada pelo volume dos dados a serem backupeados, assim não limitara o uso dos dispositivos físicos dentro dela.

6.2 RESULTADOS ESPERADOS

Através do cenário proposto e dos principais conceitos estudados sobre backup, restore e armazenamento, espera-se que ao implementar uma solução de backup baseada na ferramenta HPE Data Protector este trabalho apresentado seja um facilitador para se construir um cenário de backup com uma politica adequada e que se a solução apresentada for a escolhida, que este trabalho sirva como uma base para conhecer e interagir com as principais funções da solução. O treinamento e a difusão do conhecimento sobre a solução apresentada para os administradores serão fundamentais para manter a aplicação estável e tirando o melhor que ela pode oferecer. Apresentar a solução para a empresa e os gestores comprarem a ideia e disseminarem a informação de que o backup não e um custo no orçamento e sim um investimento fundamental e um ponto a ser atingido com este tema, uma vez que a empresa necessita manter a confiabilidade e segurança dos dados armazenados.

6.3 VIABILIDADE DA PROPOSTA

A implementação e arquitetura de um ambiente de backup depende de um estudo dos volumes a serem armazenados, e o investimento poderá variar muito, mas depende de uma linha orçamentaria definida anualmente e seu investimento deve ser justificado junto a diretoria através do planejamento, então acaba sendo uma implementação complexa e demorada, uma vez que também deveremos apresentar POC com no mínimo três cenários e soluções diferentes de backup. A compra da solução de backup requer a utilização de hardware para a instalação do servidor de backup, servidores para utilizar como Installation Server e dispositivos de mídia,

sejam eles de fita física ou virtual e este valor caria de acordo com o fabricante e as configurações de hardware envolvidas. O treinamento sobre a solução e alocação de recursos para participação do projeto deve ser considerado para que se possa administrar o ambiente corretamente.

7 CONSIDERAÇÕES FINAIS

O presente estudo de caso demonstrou a importância da informação e do dado armazenado dentro de uma empresa de TI e como a sua indisponibilidade é critica e pode gerar enormes prejuízos em uma organização e de que uma solução de backup é de suma importância para administrar os dados em com segurança e confiabilidade. As principais falhas ocorrem quando não há planejamento ou inserção de um gerente de projeto frente à atividade, bem como envolvimento de áreas de arquitetura e infraestrutura que conheçam o ambiente e ao adquirir uma solução sem fazer estimativa de volume, do que deve ser copiado e da disponibilidade do dado com certeza isto trará prejuízos à empresa ao adquirir o produto. Talvez a maior dificuldade seja interagir com todas as áreas para definir uma politica de backup e restore e que esta seja seguida para inserção de novos hosts no ambiente, a fim de garantir a restauração de todo o parque de servidores envolvidos no ambiente e uma ferramenta de gerenciamento de serviços tem papel fundamental neste ponto para organização do processo.

REFERÊNCIAS

SOMASUNDARAM, G.; SHRIVASTAVA, Alok; SERVICES, Emc Education. **Armazenamento e Gerenciamento de Informações: Como armazenar, gerenciar e proteger informações digitais**. Porto Alegre: Bookman, 2011.

LP, Hewlett-Packard Enterprise Development, **HP Data Protector Operations Guide**. USA, 2010. 66 p., il. Color. Disponível em: https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-c02029306. Acesso em: 30 out. 2017.

BROOKS, Charlotte et al. **IBM Tivoli Storage Manager Concepts**, 5. ed. São Jose, Califórnia, 2006. 556 p. Disponível em: http://www.redbooks.ibm.com/redbooks/pdfs/sg244877.pdf. Acesso em 01 nov. 2017.