



BACKUP
Conceitos Básicos

Symmetry

RECURSOS INCRÍVEIS PARA TECNOLOGIA

Presente no mercado desde 1996 ocupa posição de destaque entre as principais integradoras e provedoras de soluções de Tecnologia da Informação do país.

Áreas de atuação:

Infraestrutura de LAN e Wi-Fi

Segurança da Informação

Alta Disponibilidade

Backup e Storage

Telefonia IP

Network Analytics

Análise, Site Survey e indicadores de desempenho em tempo real



A Symmetry traz uma visão inovadora, voltada a aumentar a eficiência da TI nos mais diversos tipos de ambientes.

Flexibilidade para seu negócio

Segundo publicação do anuário INFORMÁTICA HOJE:

Eleita como a "Integradora Mais Eficiente do País"

CONFIRA NOSSOS PARCEIROS

FORTINET

aruba
NETWORKS



COMMVAULT

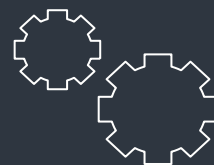
SOPHOS

Aerohive
NETWORKS

IS Decisions

peplink

Hewlett Packard
Enterprise



SOLUÇÕES CUSTOMIZADAS

Soluções como serviço (IaaS)

Serviços gerenciados de Segurança

Serviços gerenciados de Infraestrutura

Operação (Parcial ou Full)

Outsourcing



GESTÃO E MONITORAMENTO

A melhor equipe **focada na sua solução**

Profissionais certificados nas tecnologias que melhor se ajustam às necessidades do seu negócio

Você pode contar com nosso **NOC** que realiza monitoramento remoto em tempo real dos seus serviços e aplicações



TREINAMENTO HANDS-ON

Através da **Symmetry Academy** ofertamos diversos cursos e treinamentos de forma prática e extensiva para profissionais que necessitem de qualificação técnica para se diferenciar no mercado de TI.

Backup: Conceitos Básicos

A criação de uma arquitetura de backup é uma tarefa complexa devido à heterogeneidade dos elementos que o compõe. O objetivo principal é realizar backup dos sistemas em produção mantendo-os disponíveis para a necessidade da recuperação dos dados armazenados.

Para este objetivo fundamental ser atingido diversos vetores técnicos e organizacionais devem ser considerados e, como não poderia deixar de ser, há a questão de concorrência por disponibilidade de recursos.

Para que decisões possam ser tomadas com assertividade e coerência é necessário que todos os fatores envolvidos no backup corporativo sejam entendidos e levados em consideração. Vamos a seguir abordar estes vetores.

Recursos de infraestrutura

A infraestrutura de backup é composta por diversos componentes como os drives, mídias, a library, o servidor de backup, as interfaces de rede, a rede de dados, o storage de backup e inclusive o hardware dos clientes que efetuam backup. Podemos analisar estes recursos sob três pontos de vista: arquitetura, dimensionamento e utilização.

Sob o ponto de vista de arquitetura estes recursos devem ser combinados ou integrados de maneira a possibilitar a utilização de sua máxima capacidade bem como oferecer flexibilidade de utilização. É importante ressaltar que em um backup corporativo, diferentemente do backup de um determinado servidor ou conjunto discreto de servidores, as condições de trabalho não são totalmente conhecidas ou pré-estabelecidas.

A infraestrutura do backup corporativo deve ser criada para conforme as mais diferentes realidades assim como reconfigurar continuamente às necessidades dos servidores, volumes e tecnologias. Por isto é importante à elaboração, uma arquitetura de backup e não somente o dimensionamento e aquisição de equipamentos.

A diferença básica entre as duas abordagens (arquitetura e dimensionamento) é que quando olhamos o problema sob o ponto de vista de arquitetura, nós focamos em como vamos estruturar a solução para atender a demanda atual e como os recursos que dimensionamos poderão se adaptar a condições não planejadas.

Sob o ponto de vista de dimensionamento, também existe previamente alguma avaliação de arquitetura, mas obrigatoriamente quem tem foco em dimensionamento, não compromete que, além destes recursos serem configurados de modo a oferecer a capacidade de vazão necessária para que as tarefas de backups sejam feitas dentro das janelas definidas, estes mesmos recursos sejam reutilizados e continuamente adaptados e integrados com novos recursos que se fizerem necessários.

De qualquer forma, quando estamos lidando com backup corporativo, além de ser necessária a elaboração de um projeto de arquitetura, também é imprescindível o correto dimensionamento dos recursos. Uma variável complexa e importante é a vazão de dados que será necessária, porque ela resume, através de uma proporção, duas outras variáveis que são o volume de dados a ser backupeado e a janela de tempo para isto ser feito.

O último fator é a utilização e nesse caso estamos lidando com a vazão de dados que resume na forma de resultado o que foi planejado, mas, não se pode ter uma infraestrutura de backup sem contínua medição da sua utilização. Para determinar a vazão real é muito importante estar atento que este atributo não é determinado pela capacidade instalada no servidor e na Library de backup, ou seja, não é determinada pela quantidade de drives, interfaces e processadores. A vazão é um número mínimo obtido percorrendo-se uma cadeia integrada que parte do cliente indo até a library de fitas.

Estamos lidando com uma cadeia de componentes que se inicia no disco do cliente e passa pelo barramento, interface de rede, rede de dados, interface do servidor de backup, processador, memória, barramento, interface de storage, library, drive e mídia. É uma cadeia longa, com muitos componentes e o melhor desempenho vai ser determinada pelo pior componente. Isto significa também que em uma mesma instalação poderemos ter números diferentes em função do cliente. Este fator é o que determina as vazões reais serem menores do que as especificadas pelos fabricantes dos equipamentos.

Além disso, devemos estar atentos, porque estamos lidando com um sistema de equilíbrio hiperestático, onde uma variável influencia as outras. Sob o ponto de vista de utilização, nossa obrigação é configurar a programação do backup para atingir a capacidade máxima de cada componente. Para isto temos que garantir que o fluxo de dados vá do cliente à mídia sem interrupção e sem gargalos em sua máxima capacidade.

Para obter isso, temos que saturar os diversos componentes da cadeia e sempre ter certeza que esta saturação é sustentável. Capacidade ociosa significa subutilização de recursos, perda de tempo valioso na janela de backup e principalmente, no caso de backup corporativo, subutilização de recursos compartilhados.

Este último elemento que adicionamos, a gestão do compartilhamento de recursos é que torna o problema do backup corporativo mais complexo e diferente dos backups discretos. No backup corporativo, além da questão do desempenho, temos que administrar com extrema atenção a competição por recursos.

Na equação do backup corporativo, o excesso de capacidade de alguns recursos em relação a outros ou um desbalanceamento na programação dos backups, pode fazer com que a vazão de todos os backups caia, prejudicando a eficiência do sistema.

Janelas de Backup

A janela, ou seja, o tempo disponível para backupar um determinado volume de dados parece sempre ser o foco da programação e do dimensionamento do backup. Isto não deixa de ser uma verdade, entretanto, quando lidamos com backup corporativo, não pode existir somente uma janela de backup, que normalmente é relacionada a um evento de calendário (dia, semana, mês, etc.). A determinação de uma janela esta ligada ao ciclo de atualização de dados de uma aplicação. É claro que o problema é simplificado pelo fato de termos servidores funcionalmente equivalentes bem como aplicações que por acompanharem o mesmo processo de negócios da empresa vão ter ciclos muito similares de atualização.

Todo o backup é uma cópia de segurança de dados que será utilizada quando uma perda ocorrer. Assim, literalmente, estaremos usando um backup para reestabelecer a condição operacional de um sistema a partir de uma imagem temporal anterior. Para muitas aplicações poderá haver a perda de dados entre o momento da imagem armazenada no backup e o momento atual.

Cada aplicação tem um determinado ciclo de operação e funcionamento que determina o período onde os seus dados são consultados e atualizados. Algumas aplicações tem um ciclo contínuo de operação, ou seja, funcionam 24x7, outras tem um ciclo discreto onde existe horário de total ou quase total inatividade. O backup, bem programado, deve ser posicionado para capturar e preservar um volume de atualizações que represente a menor perda aceitável. Assim, não existe um conceito absoluto de quando um backup deve ser realizado.

De fato esta também é uma equação com diversas variáveis, mas que o resultado, sempre, é o que se admite perder. Um backup será utilizado para recuperar uma situação de perda de dados. A perda de dados diz respeito com a atualização e não com os dados estáticos ou não modificados.

Política de Backup

Para solucionar este problema existem diversas estratégias, técnicas e recursos. O conjunto desta análise chama-se muito simplificada de Política de Backup, que é um termo pequeno para um problema complexo. Normalmente, se erra ao se fazer uma política de backup, porque o foco da política não é apenas determinar como será o backup diário, semanal e mensal (completo, incremental ou diferencial) e qual seria a política de retenção dos dados. Quando estabelecemos uma Política de Backup não podemos nos deter simplesmente na tarefa de salvar dados em fitas magnéticas. Esta tarefa é uma das estratégias que usamos de preservação de dados, mas não é a única. Devemos analisar e especificar como poderemos, através de backups, preservar a disponibilidade das aplicações através da segurança dos dados armazenados.

Definir uma janela de backup é a tarefa de conciliar o ciclo de atividade da aplicação, com a necessidade de salvamento de dados versus o impacto de realizar a atividade de backup. Não podemos ignorar que realizar um backup sempre vai ter um impacto sobre o funcionamento da aplicação e vice e versa, isto é, a desempenho do backup será impactado pela concorrência da aplicação.

Quando tratamos de backup corporativo este é um fator importante porque estamos compartilhando recursos entre diversas aplicações e um backup que seja mais demorado do que deveria vai reter recursos que podem fazer falta para outra tarefa. No backup corporativo temos sempre que olhar o conjunto e buscar maximizar a utilização dos recursos.

Cada aplicação vai ter o seu próprio equilíbrio entre segurança de dados e impacto sobre desempenho e, também, será beneficiada pela tecnologia de armazenamento utilizada, assim para aplicações que funcionam em storage redundante, tipo Raid-1 ou Raid-5, podemos ser mais tolerantes, mas, mesmo estes sistemas não protegem totalmente a aplicação de incidentes de origem lógica e não física.

Ao buscarmos a definição de uma janela de backup, temos que entender o ciclo de operação da aplicação para obter o entendimento de qual será a estratégia e janela ideal e também, qual o limite de tolerância da aplicação uma vez que em caso de problema na programação diária, poderemos ter que fazer ou refazer backups fora da janela ideal.

Sempre existirá a tendência de alinhar a política de backup com eventos de calendário, como dias e semanas, isso é natural, mas não é correto. Em sistemas que funcionam 24x7 não existe o conceito de dia. Em sistema que funcionam mundialmente na Internet idem. Sistemas comerciais que funcionam 7x5 podem ter a necessidade de ter pelos menos 2 backups neste período uma vez que ninguém gostaria de perder todo um dia de vendas e faturamento, por exemplo.

Após analisarmos todas as aplicações, suas necessidades e definirmos os volumes de dados e as janelas, obteremos certa coincidência de tarefas para um determinado horário. Chamaremos este horário, onde existe uma intensa concorrência de recursos de tal forma que o atraso em uma tarefa impacta diretamente as demais, de janela crítica de produção ou janela de produção.

Devemos lembrar que esta é apenas uma convenção e ressaltar que somente backups muito importantes e totalmente estáveis, seguros e otimizados para desempenho podem ser executados nesta faixa de horário. Em backup corporativo todo o horário do dia é uma janela de produção de alguma aplicação.

Ao levantarmos as necessidades de cada aplicação, devemos ser muito rigorosos para apurar não somente a vontade do desenvolvedor ou usuário da aplicação, mas, realmente entender a aplicação para podermos ter flexibilidade de programação do backup.

Rigorosamente, quem deve definir como será o backup é a área de produção e não a de aplicação. É a área de produção que define os recursos de armazenamento para cada aplicação e é ela que conhece os riscos de perda de dados. A área de aplicação é fundamental para definir o ciclo de operação e atualização de dados que em função da

criticidade e volume vão determinar a técnica de salvamento e o tipo de mídia mais adequado.

A determinação da política de backup passa pelo entendimento da aplicação, do seu ciclo de operação e dos seus volumes. Em função disso, devemos definir a estratégia e a periodicidade de backup de dados.

Tipos de Backup

Em relação à estratégia temos: o backup pode ser completo quando todos os dados são salvados, diferencial quando somente os dados que mudaram depois do último backup são salvos ou incremental quando os dados modificados entre o último backup completo e cada incremental são salvos, pode se entender como Backup Cumulativo.

Estas três estratégias determinam tempos muito diferentes para realizar o backup, mas, principalmente afetam o tempo de recuperação de dados. Por exemplo, o backup mais rápido sempre será o diferencial, mas a operação de recuperação, dependendo do que se perde envolverá muito mais volumes de armazenamento.

Entretanto, pode ser uma alternativa muito atraente quando se tem um grande volume de atualização de dados.

Dependendo do volume de dados que são modificados o incremental pode ser uma alternativa muito atraente, conciliando velocidade e simplicidade.

Apesar de parecer o pior caso, o backup completo em grande parte das vezes é a única alternativa, uma vez que nem todas as aplicações foram feitas ou preparadas para os backups parciais (incremental e diferencial).

Quando somente o backup completo é a alternativa torna-se necessário usar uma infraestrutura de backup de maior desempenho ou mesmo, o uso de tecnologias mais modernas de armazenamento, como as imagens de disco e as conexões de alta velocidade.

Além disso, hoje em dia com o barateamento do custo do armazenamento de dados, existem muitas alternativas de mídias on-line para implementação de cópias de segurança, o que diminuiu bastante a demanda pela mídia semi-online.

Todos estes recursos permitem que possamos promover políticas de backup baseadas em estratégias muito criativas e que podem contribuir enormemente para a segurança e disponibilidade das aplicações.

O ponto de partida para a definição da política de backup é a necessidade de minimizar a perda de dados e acelerar a sua recuperação. A estratégia do backup vai depender da disponibilidade de infraestrutura de storage, dos volumes de atualização e da criticidade do sistema.

Por exemplo, em sistemas de missão crítica que usam banco de dados relacionais, podemos usar mídia on-line para salvar os “archive logs” possibilitando assim rapidez na recuperação e minimizando as perdas. Para servidores de arquivo ou sistema de correio eletrônico que armazenam arquivos planos, a estratégia pode ser o uso dos archive logs de file system, transaction logs dos aplicativos, HSM ou backup diferencial.

Sempre haverá a possibilidade de termos recursos na aplicação para geração de logs de atualização ou eventualmente ser necessário que a própria aplicação tenha uma funcionalidade específica para a preservação dos dados. Assim, fechando este ponto, não é possível definir e implementar um backup sem se conhecer e analisar cada aplicação que será “backupeada”.

Para finalizar este assunto é importante voltar ao princípio. Definir uma Política de backup é uma atividade principal da área de produção. Não é uma atividade de suporte e não é uma atividade da área de aplicação. A política tem ligação com a infraestrutura de armazenamento existente no datacenter.

O ambiente distribuído nos permite utilizar e integrar recursos de diferentes tecnologias e adequando desta forma a equação de custo x benefício. O mesmo vale para a tecnologia de armazenamento. A grande habilidade do profissional de storage é utilizar o recurso (estratégia e tecnologia) mais adequado para cada aplicação e o grande benefício da arquitetura é suportar e integrar isso.

Administração de recursos

Como foi dito no princípio, os recursos do backup administrativo iniciam no próprio servidor hospedeiro da aplicação cliente. Este servidor é parte da infraestrutura de backup porque ele irá executar a principal atividade no backup que é extrair os dados a serem “backupeados”.

Administrar um backup corporativo significa tomar diariamente novas decisões em função da realidade corrente. Não existe programação estática no backup corporativo, seja pela inclusão de novos clientes que podem requerer a reprogramação de vários backups como também a alteração do volume de dados e desempenho dos clientes pode alterar significativamente os resultados. É necessário então, uma administração contínua dos recursos e uma tomada constante de decisões visando readequar os recursos, estratégias e programação da própria realidade do dia a dia das empresas, ou seja, é necessária uma equipe para tal atividade.

O armazenamento na nuvem e o backup em nuvem já despontam como realidade na computação mundial. Contudo, muita gente ainda não entende a diferença que existe entre o armazenamento e o backup na nuvem. O fato é que conhecer esses conceitos pode prevenir sua empresa de riscos, como a perda de dados, por exemplo. O objetivo deste post é explicar qual a diferença entre armazenamento na nuvem e backup na nuvem, além de mostrar qual modelo é mais indicado para cada situação. Confira!

Armazenamento na nuvem

Armazenamento na nuvem significa guardar os dados na nuvem. Assim, quando o usuário envia arquivos para um disco virtual ele está fazendo armazenamento na nuvem. Essa forma de salvar arquivos é muito comum entre os usuários domésticos. No entanto, algumas empresas também costumam adotar esse modelo.

A principal vantagem dos discos virtuais é que os usuários podem acessar os arquivos de qualquer lugar com conexão à internet, seja qual for o dispositivo. Diante do exposto, no modelo de armazenamento na nuvem, caso um arquivo seja apagado pelo usuário, ele será automaticamente apagado do disco virtual através da sincronização — é preciso muito cuidado para não cometer um engano e apagar algum arquivo importante, podendo gerar prejuízos à empresa, já que não será possível a recuperação dos dados.

Backup na Nuvem

O backup na nuvem pode ser entendido como a cópia de segurança dos arquivos. Nesse formato, é feita uma cópia dos dados presentes nos computadores da empresa e essa cópia é gravada na nuvem, propiciando maior segurança às informações corporativas. Esse é um modelo muito utilizado por empresas, contudo, também existem soluções voltadas aos usuários comuns, principalmente no que se refere a fotos pessoais.

A grande vantagem do backup na nuvem em relação aos antigos backups realizados em servidores é o custo. Manter equipamentos locais gera despesas e mão de obra especializada — para a manutenção dos servidores e para a elaboração das rotinas de backup. Na cloud computing, os servidores estão online e fora das empresas contratantes, o que reduz os custos, mas mantendo o nível de qualidade na entrega da solução.

Qual a melhor opção?

A utilização dessas ferramentas apresentadas varia de acordo com a necessidade de cada organização. Se o foco é compartilhar arquivos para realização de trabalho colaborativo e garantir o acesso em variados pontos e dispositivos, o recomendado é uma ferramenta de armazenamento em nuvem, os discos virtuais. Por outro lado, caso o objetivo seja manter cópias de segurança dos dados com registros de versões e modificações feitas, o mais indicado é escolher uma solução de backup na nuvem.

Para ambos os casos, é ideal conhecer os conceitos e particularidades de nuvem pública e privada para fundamentar ainda mais a sua decisão. Leia nosso outro artigo sobre “nuvens”.