TechTarget | ComputerWeekly.com.br

5 RISCOS APÓS A MIGRAÇÃO PARA NUVEM E COMO EVITÁ-LOS

Risco 1: Arquitetura ruim leva a custos de computação exorbitantes

Para evitar o risco de que a migração para a nuvem aumente significativamente os custos, os CIOs e sua equipe de TI devem avaliar as cargas de trabalho para essas oportunidades de adaptação como parte de seu processo de integração da carga de trabalho à nuvem.

A chave para reduzir custos é adaptar as cargas de trabalho aos ambientes de nuvem. Mesmo um salto rápido para a nuvem deve evitar uma abordagem "levantar e mudar" não ponderada e sempre deve incluir exercícios de dimensionamento correto para reduzir a sobreconfiguração. A adaptação mínima às vezes pode também gerar economias enormes.

Risco 2: Má compreensão do ecossistema da carga de trabalho

É importante lembrar que o fluxo de dados que entram é gratuito e que o fluxo que sai tem custos. O mesmo processo de incorporação da carga de trabalho que pode ajudar a identificar oportunidades e assim adaptar uma carga de trabalho para execução de modo eficiente na nuvem. Também deve-se mapear quais outros sistemas estão executando o aplicativo para entender melhor onde e quantos dado terão de deixar o ambiente da nuvem e quanto isso custará.

Uma vez que isso é resolvido, o departamento de TI pode decidir como mitigar o risco de aumentar os custos. As opções para eliminar este tipo de problema, seja como parte do processo ou depois do fato, incluem redesenhar o aplicativo para remover fluxos, implementar compressão, a migração de outros sistemas envolvidos para evitar a saída da nuvem e adicionar uma conexão direta com a nuvem ou um entreposto à nuvem para reestruturar e estabilizar o custo.

Risco 3: Ambientes de nuvem não sincronizados com a política de segurança

Ter a segurança configurada corretamente durante a migração é apenas o primeiro passo. Se profissionais de TI não incorporam de maneira sólida a auditoria e manutenção de cada ambiente de segurança em seus processos e sistemas de gestão de mudanças regulares, inevitavelmente verão seus vários ambientes, na nuvem e locais, desmoronar. Isso deixa a organização em risco de inadimplência e aumento o risco de comprometimento.

O processo de incorporação à nuvem deve incluir a confirmação de que cada nova oferta está vinculada ao processo de gestão de mudanças, assim como também atualizar as políticas de segurança e auditoria como necessário quando ambientes de nuvem completamente novos são agregados ao mix. Ferramentas como Flexera, Scalr e Tufin também estão disponíveis para ajudar a implementar a segurança de forma consistente em todos os ambientes.

Risco 4: Visibilidade inadequada de desempenho e uso

O foco em uma migração para a nuvem é mais intenso do que o foco sobre o gerenciamento contínuo de operações na nuvem. Quando os administradores têm de usar um conjunto de ferramentas de forma diferente para adquirir os dados incorporados em um portal de provedores, isso diminui a probabilidade de que as informações sejam compiladas e usadas de forma consistente.

Um bom processo de integração deve levar a uma preparação adequada para operações na nuvem em cada carga de trabalho migrada. O ideal é ter como resultado a integração de dados do sistema de administração da nuvem no conjunto de ferramentas de gestão existentes. Isto também pode ser implementado depois do fato, mas em muitos casos, não será até que ocorra um problema significativo com o desempenho ou disponibilidade.

Risco 5: A gestão inadequada do ciclo de vida leva à perda de dinheiro

Por fim, após a migração para a nuvem existe o risco que a TI não acompanhe os sistemas recentemente implementados até o final de sua vida útil. Este é um problema familiar para a nuvem: sistemas "zumbi" são um problema desde o nascimento da virtualização de servidores e a nuvem o amplifica, já que é mais fácil perder de vista um sistema que não tem características físicas visíveis; em outras palavras, sem um servidor sentado em uma prateleira. Não é raro que equipes de TI estabeleçam novos ambientes de teste e desenvolvimento sem desmontar completamente os antigos ou substituir um servidor por um serviço; por exemplo, substituir um banco de dados SQL DIY por uma oferta DBaaS do provedor da nuvem, mas apenas desligando o aplicativo de banco de dados original, sem fechar a instância na qual está sendo executado.

Além de desperdiçar dinheiro, esses zumbis podem criar riscos de segurança onde os sistemas em funcionamento não possuem patches e as configurações não são mantidas, entre outros.