**AS FUNDAMENTOS CLOUD COMPUTING**

**MATHEUS HENRIQUE BUTKOSKI SILVA**

**RESUMO PÁGINAS 247-257**

**Desafios da Computação em Nuvem**

**Segurança e Privacidade em Ambientes de Nuvem.**

A ampla utilização da computação em nuvem não traz apenas benefícios, visto que novas preocupações surgem a todo momento. Como parte da tecnologia fica à disposição do contratante a segurança se torna fragilizada representando uma ameaça independente da forma que o serviço é utilizado.

Existem diferentes abordagens quando se trata de segurança da operação em nuvem. As mais genéricas normalmente representam desafios frequentes para os responsáveis. Para Hiran os desafios são os seguintes:

**Violação de Dados:** Acesso para aqueles que não possuem permissão, utilizando métodos fraudulentos.

**Falha no Gerenciamento de identidade:** Falhas que podem resultar em liberação de dados para aqueles que não possuem acesso, mesmo n]ao havendo má-fé.

**Vulnerabilidade do sistema:** Fragilidades que podem ser evitadas utilizando formas de atualização frequente do sistema.

**Sequestro de Conta:** Efetivado como roubo e uso de dados para fins maliciosos.

Esses desafios podem ocorrer de forma diferente dependendo de cada caso. Entretanto é sempre necessário prezar três elementos básicos se segurança independente dos casos. Eles são:

**Confidencialidade:** Somente aqueles que possuem acesso aos dados poderão acessá-los.

**Integridade:** As alterações pretendidas nos dados só serão salvas caso um usuário com permissão a tenha feito.

**Disponibilidade:** Tempo em que o dado pode ser acessado pelo usuário.

Esses filtros de segurança não surgiram com o advento dos serviços de nuvem, porém são importantes para entender planejar e implementar um sistema em nuvem.

A oferta de Software como Serviço (SaaS), embora com muitos benefícios, abre flancos permitindo ações maliciosas e ameaças para o serviço em nuvem. Elementos como a **incapacidade de monitorar dados em trânsito entre aplicativos e a falta de visibilidade sobre a importância dos dados que estão na nuvem** auxiliam para o fenômeno dos roubos de informações virtuais, visto que por muitas vezes o provedor não é capaz de evitar todos os tipos de ataques.

Portanto, cabe aos provedores de SaaS cuidar e saber de que tipo e quais são os dados que seus clientes colocam na nuvem e aplicar a segurança necessária para evitar contratempos e atividades maliciosas por terceiros.

A respeito da Infraestrutura como Serviço (IaaS) a responsabilidade da segurança cabe tanto ao provedor quanto ao cliente, visto que os servidores, nesse modelo de serviço, passam a ser de propriedade do cliente. Basicamente o provedor deve assegurar a segurança e infraestrutura em si dos dados, enquanto o cliente deve certificar que todas as medidas de seguranças foram tomadas pelo provedor.

A Plataforma como Serviço (PaaS) tem características parecidas com o SaaS quando se trata de responsabilidades de segurança. Ambos não devem compartilhar com o cliente detalhes da plataforma, como sistema operacional, visando evitar vulnerabilidades nesses sistemas. Isso não isenta o cliente de salvar os seus dados de acesso.

**Desempenho de Nuvem**

No momento em que uma organização decide por mudar sua computação para a nuvem surgem comparações para verificar o “antes e depois” do serviço. Entretanto, a medição para comparar o desempenho antigo e o atual deve se basear em métricas padronizadas e ferramentas.

Para entender os aspectos técnicos do desempenho deve-se antes compreender como a operação do serviço se comporta. Assim, também será necessário diferenciar as questões de desempenho entre os diferentes tipos de serviço.

Em IaaS as máquinas virtuais são as que operam os discos, configuradas conforme necessidade do cliente. Deve-se basear em alguns fatores para tornar a experiência de desempenho a melhor possível:

- Região de Operação;

- Definição de Sistema Operacional;

- Instâncias de Computação;

Após esses fatores serem levados em consideração, os recursos serão alocados em máquinas físicas. Porém, essas máquinas raramente vão ser designadas apenas a um cliente, o que pode acarretar em queda de rendimento e desempenho, se o hardware que compõe a máquina não for o suficiente para suportar uma carga elevada de processamento e o alto fluxo de troca de informações.

Um estudo, realizado por Leitner e Cito (2016), formulou 4 grupos de hipóteses que geram as variações de desempenho:

**Previsibilidade de desempenho**: O desempenho das aplicações varia de acordo onde elas estão alocadas. Na CPU varia conforme o modelo, já em aplicações de entrada e saída de informações, varia conforme o fluxo e comportamento dos outros usuários do servidor.

**Variabilidade nas Instâncias**: O desempenho de aplicações de entrada e saída tende a variar dentro da mesma instância. Por outro lado, o desempenho das aplicações vinculadas a CPU não varia de maneira relevante em instâncias de CPU dedicada.

**Fatores Temporais e Geográficos**: A hora e o dia que as aplicações são utilizadas alteram o desempenho. Isso ocorre, pois, certos serviços tem uma maior demanda em horários ou dias da semana específicos, o que acarreta em alto uso em um espaço de tempo, afetando o desempenho. Além disso, fatores geográficos podem interferir de acordo com a capacidade de hardware aplicada em diferentes servidores alocados em diferentes regiões com diferentes demandas de utilizadores.

**Seleção do Tipo de Instância**: Os autores do estudo criaram uma métrica para medir a proporção de custo e desempenho das instâncias, o U$/hora (dólar por hora). Foi observado que não há relação direta e necessária entre valor do equipamento e seu desempenho. Uma instância duas vezes mais cara não será duas vezes mais rápida e vice-versa.

Dessa forma, também é importante conhecer as ferramentas e os recursos que monitoram o desempenho. Essas ferramentas oferecem base de avaliação tanto para o contratante quanto ao provedor do serviço.

São Elas:

**Amazon Cloud Watch:** oferece o processamento de dados, além de vários tipos de estatísticas e configurações.

**PCMONS (Private Cloud Monitoring Systems):** Oferece acessos separados a gerentes e usuários, o que torna atrativa para organizações que não desejam investir em uma ferramenta própria.

**RMCM (Runtime Model for Cloud Monitoring):** Monitora o serviço na nuvem e entrega funcionalidades para o operador, desenvolvedor e usuário.

**Flex-ACMS (Flexible Automated Cloud Monitoring Slices):** Resultado da composição de um conjunto integrado de soluções de monitoramento.

Essas são algumas ferramentas, porém não são os únicos meios de averiguação. Logo, cabe ao provedor fornecer ferramentas para que o usuário teste por conta própria o desempenho técnico dos serviços.

**Vantagens e Desvantagens da Computação em Nuvem**

Com o avanço das manutenções de segurança e o atingimento de altos níveis computacionais, as empresas tem optado por aderir a computação em nuvem como forma de resolver desafios com mais recursos e possibilidades.

Dessa forma, algumas vantagens e desvantagens que surgem ao se aderir à computação em nuvem serão descritas.

É importante pontuar que a adoção da computação em nuvem não significa certamente que existirá um barateamento com custos de manutenção em infraestrutura de TI, e também não certifica que um serviço dará flexibilidade para nas necessidades de armazenamento do contratante.

Um dos maiores interesses nas organizações que pensam em adotar a computação em nuvem é a questão econômica, visto que os gastos com aquisições e manutenções de estrutura própria podem ser sanados. Porém existem vantagens econômicas em todos os casos?

Para efeito de comparação, a Microsoft com seu produto Azure. Foi feita uma simulação em que usando certas configurações de região e armazenamento, o custo de uma conta simulada gira em torno de U$ 165,00 para a companhia, enquanto o usuário paga U$ 81,75 mensais a cada 1 TB armazenado, o que pode significa um custo excessivo para pequenas e médias organizações que pretendem aderir ao serviço em nuvem.

Porém, visando reduzir os gastos com infraestrutura de TI, muitos gestores acabam por esquecer uma crucial desvantagem da computação em nuvem: a dependência da internet para a operação. Deve-se sempre analisar as conexões disponíveis e se a velocidade oferecida será capaz de atender ao uso da nuvem.

Além disso, outra desvantagem que pode surgir em alguns casos consiste na necessidade de mudança de provedor de computação em nuvem. Transferir dados de um provedor A para um provedor B nem sempre será tarefa fácil dependendo da quantidade armazenada, assim necessitando de configurações e ajustes adicionais.

Outras desvantagens que podem ser consideradas são: Controle limitado sobre a infraestrutura utilizada, a falta de meios para intervir caso o serviço seja encerrado e a maior vulnerabilidade a ataque.

Cada um desses problemas, é claro podem ser evitados, logo cabe a cada organização se planejar com conhecimento e entender suas realidades para evitar constrangimentos e muitas vezes podendo perder oportunidades.

Assim conclui-se que, adotar a computação em nuvem na maioria dos casos trará vantagens, mas claramente existem dúvidas e hesitações que são compreensíveis na contratação do serviço, porém estas podem ser crucias e evitando uma possível prospecção da organização. Cada caso deve ser avaliado com conhecimento e dessa forma a computação em nuvem pode ser alvo para cada vez mais usuários.