ANÁLISE DA UTILIZAÇÃO DA TECNOLOGIA DE CONTÊINERES EM NUVEM COMO MODELO DE SEGURANÇA

Eduardo Silva dos Santos [1]
Lafayette Batista Melo [2]

INTRODUÇÃO

Ao longo do tempo, a expansão no volume de acesso dos serviços *web* tornou a infraestrutura de TI existente arcaica. A utilização de infraestruturas de provedores desse tipo de serviço acarretava custos elevados de manutenção com baixos níveis de utilização e estes não eram suficientes para manter a o dinamismo das aplicações em picos de acesso.

Dessa forma, empresas capazes de oferecer infraestrutura de TI em grande escala se tornaram uma alternativa muito atrativa para a grande maioria dos provedores de serviços *web*. Os preços competitivos e as baixas taxas de indisponibilidade garantidas por SLA's (*Service Level Agreement*), possíveis devido a grande escalabilidade e controle de granularidade, permitiram que aplicações com elevada capacidade de atendimento pudessem existir. Esses operadores, que ficaram conhecidos como “nuvem", atualmente hospedam a maioria das aplicações e dados disponíveis na *web*.

A expansão da *web*, e posteriormente da nuvem, ocasionou um aumento exponencial no fluxo de dados presentes nos nós da rede, entre os quais aqueles constituídos de informações de alto valor. Possíveis vazamentos desses dados ocasionariam perdas financeiras e de outras naturezas para seus proprietários e, consequentemente, para os provedores dessas aplicações.

Para o processamento, memória, armazenamento e proteção de dados nos níveis de rede, foram empregadas soluções de *software*, e assim, evoluíram para atender ao amplo ambiente da *web*. Essas soluções possuem o intuito de resguardar esses dados de intenções maliciosas.

[1] Graduando do Curso de Redes de Computadores do Instituto Federal de Educação, Ciência e Tecnologia da Paraíba - IFPB, silva.eduardo@academico.ifpb.edu.br;
[2] Professor orientador: Doutor, Instituto Federal de Educação, Ciência e Tecnologia da Paraíba - IFPB, lafayette.melo@ifpb.edu.br;

Tais alternativas de modernização de infraestrutura de TI, apesar de melhorar consideravelmente os serviços [b], acarretam para os provedores de serviços *web* e outros sistemas de informação um aumento no Custo Total de Propriedade de suas aplicações.

Logo, este trabalho busca apresentar uma breve análise dos problemas de segurança acima citados utilizando-se a tecnologia de contêineres em nuvem.

METODOLOGIA (OU MATERIAIS E MÉTODOS)

Como processo metodológico, foi realizada análise comparativa das aplicações. Foram analisados o *auto scaling* e a instanciação de serviços do SCO e do Google Kubernetes, solução que se apresentou melhor desempenho que o Docker Swarm (que é uma das principais no mercado) no comparativo.

DESENVOLVIMENTO

Em sua essência, o conceito de computação em nuvem é um serviço terceirizado. Segundo Fernandez (2017),

> Na era dos serviços *web* em infraestruturas proprietárias, a atividade final de um proprietário de uma aplicação não era oferecer uma infraestrutura de TI, mas um produto ou serviço acessível através dessa aplicação. Provedores de Serviço de Nuvem (PSN) apareceram no final dos anos 2000 oferecendo infraestrutura de TI no formato de um serviço, prática que passou a ser conhecida como Infrastructure as a Service (IaaS). Os PSN possuem um alto nível de especialização e grande escala, o que diminui seus custos operacionais para hospedar cada aplicação. A nuvem oferece também a possibilidade de aumentar o poder de atendimento da aplicação com um aumento relativamente pequeno do custo total, devido ao decréscimo progressivo no custo por unidade computacional [d].

Dentre os fatores que se revelaram mais significativos para manter uma elevada utilização dos recursos de um PSN, foi o multiinquilinismo, que é a capacidade de manter aplicações de mais de um cliente numa mesma máquina hospedeira. Contudo, em questão de segurança esse método é muito falho, o que gera preocupação com os dados armazenados.

Para resolver esse problema, uma solução viável encontrada foi a virtualização. Virtualização nada mais é do que uma técnica que consiste em criar espaços computacionais

virtuais isolados. Nesses espaços os recursos são disponibilizados criando a ilusão de que há um único cliente presente no ambiente virtual.

A virtualização, desde sua origem, passou por diversas variações. Com a chegada dos serviços de computação em nuvem e PSN a virtualização utilizada era a de nível *Hypervisor*, que atua em unidades denominadas máquinas virtuais. Esta técnica envolvia a utilização de uma camada de *software*, o Hipervisor, que era responsável por mediar os acessos dos sistemas operacionais, isolados entre si, ao *hardware* [c].

Em meados de 2010, surge uma nova tecnologia de virtualização que atua em nível de kernel que, mantendo a vantagem do multiinquilinismo, rapidamente se popularizou. Dessa forma, tornou-se viável a utilização desse novo nível, pois com grande adesão de provedores PSN, a segurança também possui mais robustez.

Apesar de serviços de hospedagem em nuvem serem bastantes seguros, há também vulnerabilidades que devem ser cuidadas, pois se algum agente malicioso explorá-las conseguirá ter acesso a dados de clientes. Havendo essa problemática, algumas soluções que fortalecem a segurança nesse ambiente foram desenvolvidas afim de não comprometer a segurança dos sistemas e arquivos. Dentre essas soluções, existe o *Secure Container Orchestration*, um *software* orquestrador de contêineres desenvolvido no Laboratório de Sistemas Distribuídos da Universidade Federal de Campina Grande, LSD/UFCG.

RESULTADOS E DISCUSSÃO

Em ambos os cenários o SCO mostrou-se mais eficiente que o Kubernetes, o que faz dele, em relação aos demais *softwares* citados neste trabalho, uma melhor opção para organizar contêineres na nuvem.

Analisando algumas dessas soluções que foram estudadas ao longo da construção deste trabalho, chegou-se à conclusão de que o SCO é a melhor alternativa para essa implementação na computação em nuvem, pois este *software* dispõe de uma arquitetura que se mostra mais eficiente em relação às demais soluções apresentadas neste trabalho.

CONSIDERAÇÕES FINAIS

Esse trabalho buscou analisar, através de pesquisa bibliográfica, modelos de ornamentação de contêineres e indicar uma solução que atenda o máximo necessário de segurança.

Concluído a análise, este trabalho permite direcionar o leitor para uma perspectiva de seguraça na nuvem, abordando alguns pontos de destaque em segurança do SCO. Uma outra alternativa promissora, como o SCONE, não leva em consideração aspectos complexos da orquestração de contêineres seguros, abordados com minúncia no SCO, portanto, está adequada aos mais altos níveis de exigência de segurança.

Palavras-chave: Contêineres, Nuvem, SCO, Segurança, Serviços *web*.

REFERÊNCIAS

[a] Peter Géczy, Noriaki Izumi, and Koiti Hasida. Cloudsourcing: managing cloud adoption. 2011.

[b] Borja Sotomayor, Ruben S. Montero, Ignacio M. Llorente, and Ian Foster. Virtual infrastructure management in private and hybrid clouds. IEEE Internet computing, 13(5), 2009.

[c] Mendel Rosenblum. The reincarnation of virtual machines. Queue, 2(5):34, 2004.

[d] Gabriel Pereira Fernandez. Orquestração de Contêineres na Nuvem: Um Modelo de Segurança, 2017.