ANÁLISE DE SEGURANÇA DE RECURSOS VIRTUALIZADOS EM NUVENS COMPUTACIONAIS IAAS BASEADAS EM OPENSTACK

Raphael Marcos Huss Pennacchi[1], Charles Christian Miers[2].

[1] Acadêmico do Curso de Bacharelado de Ciência da Computação CCT - bolsista PIBITI/CNPq.
[2] Orientador, Departamento de Ciência da Computação - CCT – charles.miers@udesc.br

Palavras-chave: Segurança. Nuvem. Contêineres.

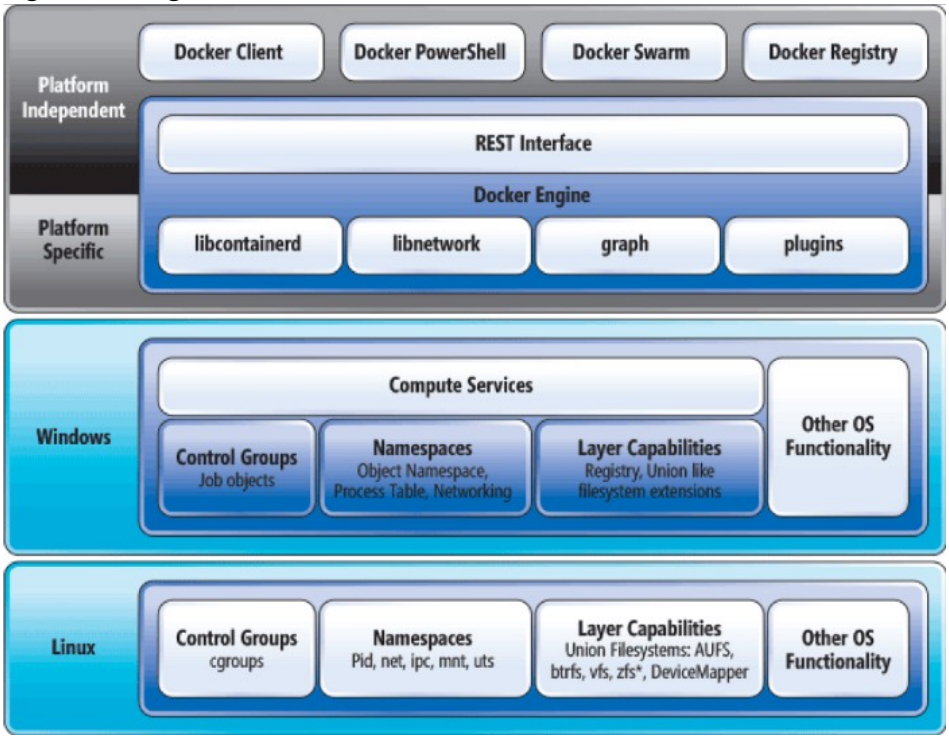
O uso de contêineres tornou-se popular em diversos cenários em função de seu alinhamento com tecnologias de desenvolvimento recentes e baixo consumo de recursos. Neste cenário a solução de contêineres Docker sobressaiu-se em relação às demais, sendo baseada essencialmente em sistemas operacionais com o núcleo Linux. Recentemente, a Microsoft buscou ingressar nesse mercado oferecendo meios de executar contêineres nos seus sistemas operacionais da linha server. Contudo, já há uma preocupação sobre as operações e segurança da rede em contêineres baseados em sistemas Linux e o surgimento de Windows Containers realça essa preocupação. Neste sentido, a presente pesquisa faz uma análise sobre aspectos de controle de recursos, segurança de imagens de contêineres e segurança na comunicação entre contêineres. A análise revelou questões preocupantes quanto a segurança da comunicação entre os contêineres.

Nesta pesquisa foi utilizada a nuvem do LabP2D, sendo expregadas nos experimentos as versões dos sistemas operacionais GNU/Linux Ubuntu 18.04 e MS-Windows Server 16 para a realização dos testes de segurança com contêineres. A solução de conteinerização Docker é compatível somente um número reduzido de versões do MS-Windows, sendo a única versão que o suporta nativamente o MS-Windows Server 2016. Cada conjunto de experimentos utilizou o Docker referente ao sistema operacional, sendo realizados testes de segurança baseados na etapa anterior desta pesquisa, *e.g.,* teste de controle/limtação de acesso e limitação de memória don contêiner.

Os resultados dos testes revelaram que, se configurado erroneamente, tanto as permissões básicas como a memória máxima disponível de um contêiner podem ser afetados. Além disso, outras consequências indesejadas pode ocorrer com outros contêineres que estão em execução na mesma máquina.

No presente momento há dois artigos em desenvolvimento. Um artigo tem por objetivo analisar sob ótica de segurança as diferenças entre as arquiteturas de contêineres Docker empregando os sistemas operacionais GNU/Linux Ubuntu 18.04 e MS-Windows Server 16 (Fig. 1). O segundo artigo foca mais nosReferências aspectos de segurança dos contêineres Docker em MS-Windows Server 16.

Fig. 1: Visão geral das arquiteturas de execução de conteiner: Windows vs. Linux



Referências

Abdelmassih, Christian. 2018. Container Orchestration in Security Demanding Environments at the Swedish Police Authority. http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-228531.

Lingayat, Ashish, Ranjana R. Badre, and Anil Kumar Gupta. 2018. "Integration of Linux Containers in OpenStack: An Introspection." Indonesian Journal of Electrical Engineering and Computer Science 12 (3): 1094–1105. https://doi.org/10.11591/ijeecs.v12.i3.pp%p.

Microsoft. n.d. "Sobre contêineres do Windows." Accesso em 02/Julho/2019. https://docs.microsoft.com/pt-br/virtualization/windowscontainers/about/.

Sarkale, V. V., P. Rad, and W. Lee. 2017. "Secure Cloud Container: Runtime Behavior Monitoring Using Most Privileged Container (MPC)." In 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), 351–56. https://doi.org/10.1109/CSCloud.2017.68.

Walker, Justen. 2018. "A Short Introduction to Windows Containers." Medium. December 20, 2018. https://medium.com/jettech/a-short-introduction-to-windows-containers-db5adc0db536.