ANÁLISE DE DESEMPENHO DO *SECURE PRODUCTION IDENTITY FRAMEWORK FOR EVERYONE* (SPIFFE)[1]

Henrique Zanela Cochak[2], Charles Christian Miers[3]

[1] Vinculado ao projeto "Análise de segurança de recursos virtualizados em nuvens computacionais IaaS baseadas em OpenStack usando *honeypots* de baixa interatividade"
[2] Acadêmico do Curso de Ciência Da Computação – CCT – Bolsista PROBITI
[3] Orientador, Departamento de Ciência Da Computação – CCT – charles.miers@udesc.br

A computação em nuvem, uma tecnologia capaz de entregar serviços computacionais e o uso de seus recursos de uma forma mais distribuída, está constantemente sendo adotada por novas corporações, tanto acadêmicas quanto comerciais. Esta tecnologia proporcionou a possibilidade de uma significativa mudança de aplicações monolíticas para aplicações baseadas em microsserviços, devidos às questões de como os recursos computacionais são mais bem distribuídos na nuvem. Apesar disso, as aplicações requerem um maior cuidado na segurança das transações realizadas, tanto internamente quanto externamente. Com este propósito, considera-se o uso de identidades digitais para fins de identificação e seu uso por uma prática denominada gerenciamento de identidades. Tais soluções não apenas protegem o acesso a software e dados, mas também protegem os recursos de hardware em uma empresa, assim, ganhando bastante importância na última década devido ao número crescente de mandatos regulatórios que buscam proteger dados confidenciais de qualquer tipo de exposição. Estes gerenciadores são capazes de estender seu uso para identidades federadas e transitivas. A identidade federada facilita o compartilhamento controlado de informações sobre pessoas, além das fronteiras organizacionais, evitando o registro redundante de principais que operam em vários domínios. As identidades transitivas são as autenticações, a partir de domínios confiáveis, no qual estes domínios podem novamente fornecer acessos para outros domínios, de forma recursiva. Os gerenciadores de identidades mais conceituados no mercado utilizam destes conceitos para garantir a segurança de ambientes em nuvem. Contudo, não são capazes de gerenciar identidades de não usuários, tais como as cargas de trabalho ou processos encapsulados em ambientes conteinerizados. Para solucionar este problema, surge o padrão SPIFFE e seu ambiente de execução SPIRE proporcionando autenticações entre cargas de trabalhos. O SPIFFE é um conjunto de especificações de código aberto para uma estrutura capaz de inicializar e emitir identidade para serviços em ambientes heterogêneos e limites organizacionais. O cerne dessas especificações define documentos de identidade criptográfica de curta duração chamados de SVID, nos quais as cargas de trabalhos podem usar estes documentos de identidade para autenticar outras cargas de trabalho. Este trabalho apresenta um caso de uso detalhado concentrando na delegação de credenciais dentro do ambiente SPIRE. Este cenário consiste em permitir que uma instância de serviço, ao receber uma mensagem de outra instância, possa verificar não apenas a identidade da carga de trabalho, mas também de outra entidade que fez a requisição inicial, e.g., usuário final humano, assim levantando um novo documento chamado DA-SVID, que consiste na tradução de uma credencial externa em uma credencial SPIFFE. Dentro deste cenário, é proposto um *benckmark* do consumo computacional em duas partes da aplicação: na função de cunhar o DA-SVID e na transmissão deste documento para outra carga de trabalho. É testado de forma opcional o *Mint* da prova de conhecimento zero (ZKP) e na sua transmissão em

conjunto com o DA-SVID para outra carga de trabalho. Ambos os cenários são executados na ferramenta Docker e na ferramenta Kubernetes.

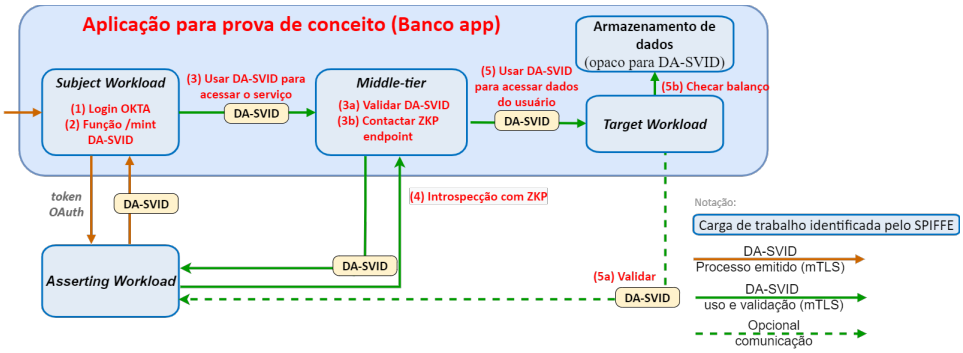

Figura 1. *Prova de conceito: requisição a um banco de dados remoto.*

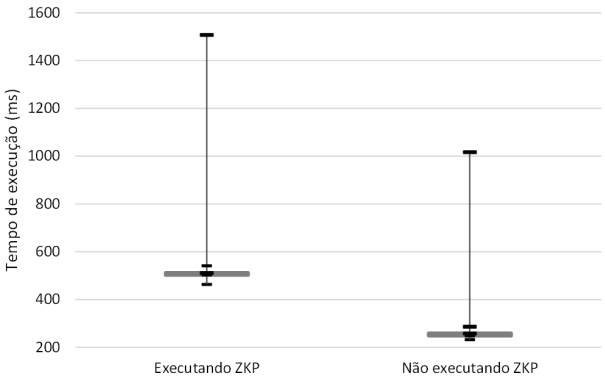

Figura 2. *Tempo de execução Mint no Docker.*

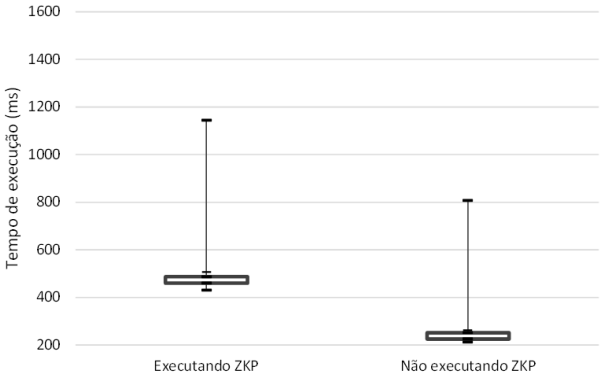

Figura 3. *Tempo de execução Mint no Kubernetes.*

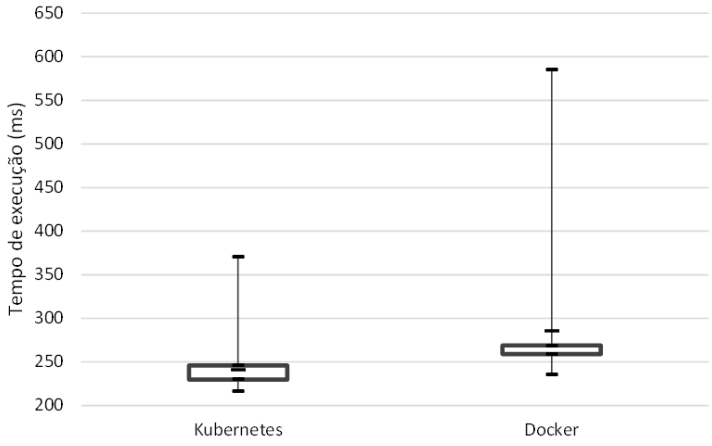

Figura 4. *Custo da transmissão do DA-SVID por outra carga de trabalho.*

Palavras-chave: Computação em nuvem. Segurança. SPIFFE.