Análise de mecanismos de autenticação e autorização para nuvens computacionais baseadas na solução OpenStack

Glauber Cassiano Batista[1], Charles Christian Miers[2]

[1] Acadêmico do Curso de Bacharelado em Ciência da Computação – DCC/CCT - glauber@colmeia.udesc.br - bolsista PIPES/UDESC Edital 2015-1
[2] Orientador, Departamento de Ciência da Computação – DCC/CCT – charles.miers@udesc.br

Palavras-chave: OpenID Connect. Single Sign-On. OpenStack.

Uma nuvem computacional é um modelo que permite acesso ubíquo, conveniente e sob demanda a um conjunto de recursos configuráveis que podem ser rapidamente provisionados e liberados com o mínimo de esforço. O modo de operação de uma nuvem, através de um modelo de *commodities*, possibilita uma nova abordagem aos provedores de utilizarem e oferecerem seus recursos computacionais à comunidade. O OpenStack tem obtido destaque como solução de nuvem computacional, no intuito de beneficiar e aumentar o aprendizado da comunidade, seja dentro de uma única organização ou na integração de várias organizações. Vários sistemas em um mesmo departamento ou organização comumente utilizam serviços de autenticação distintos, o que resulta em dificuldades para o usuário, que deve lembrar de suas várias informações de autenticação. Assim, como grande parte dos serviços na Internet, as nuvens computacionais se deparam com problemas similares e algumas já empregam mecanismos *Single Sign-On* (SSO). A principal característica de um mecanismo SSO é prover um identificador único ao usuário para que este possa autenticar-se em qualquer serviço que o suporte. O uso de tecnologias de autenticação/autorização centradas no usuário (*e.g.*, OpenID Connect) proporcionam uma possibilidade mais dinâmica e acessível às organizações que fornecem serviços de computação em nuvem à comunidade externa. Contudo, a escolha dos mecanismos SSO mais adequados não é uma tarefa simples, pois não foi identificada uma classificação desses mecanismos com ênfase em nuvens computacionais, tampouco foi encontrada uma análise de segurança que informe os potenciais riscos de uma solução. Dessa forma, o objetivo desta pesquisa é prover um sistema e método de autenticação SSO baseado em software livre que auxilie no processo de autenticação e gerenciamento de usuários de uma plataforma de nuvem. Como estudo de caso é utilizada a nuvem computacional do Laboratório de Processamento Paralelo e Distribuído (LabP2D). Também buscou-se aumentar a segurança do processo de autenticação e acesso aos recursos de nuvens computacionais baseadas em OpenStack por meio da identificação de procedimentos seguros e correções. Por fim, os resultados obtidos podem ser utilizados como referência em projetos de nuvens computacionais abertas. Para o desenvolvimento do trabalho, foram realizadas duas etapas com dois métodos distintos de pesquisa: referenciada e aplicada. Na pesquisa referenciada foi realizado o levantamento bibliográfico dos assuntos que permeiam esta área pesquisa. Ao final da pesquisa, uma taxonomia foi elaborada em forma de artigo, classificando os mecanismos SSO com foco nas nuvens computacionais. Este artigo teve colaboração do Laboratório de Arquitetura e Redes de Computadores (LARC), da Universidade de São Paulo (USP) e está atualmente em fase de revisão na *8th IEEE International Conference on Cloud Computing Technology and Science* - CloudCom. Na pesquisa aplicada, foi implementado um

mecanismo SSO no OpenStack, utilizando um Provedor de Identidades (IdP) externo. Para isso, foi instalado o *plugin* de autenticação do OpenID Connect no *Keystone*, o componente de gerenciamento de identidades do OpenStack. O IdP utilizado é o do Google. Contudo, esse método de autenticação deveria permitir apenas que os usuários autorizados tivessem acesso à nuvem, e não qualquer pessoa com uma conta no IdP. Dessa forma, os usuários autorizados devem ter uma forma de identificação exclusiva, como um grupo de usuários autorizados. Inicialmente foi realizado uma tentativa de autenticar os usuários que estavam em um determinado grupo do *Google Groups*, mas no decorrer da pesquisa foi verificado que o IdP do Google não suportava o uso do *Groups* para a autenticação. Dessa forma, a recomendação do Google é de utilizar um domínio do *Google Apps* e inserir os usuários em um grupo dentro desse domínio. Dessa forma, foi possível autenticar os usuários da nuvem. Assim, com o ambiente configurado, foi realizado uma análise de segurança da integração do OpenID Connect em nuvens computacionais baseadas no OpenStack que utilizam um IdP externo (*i.e.*, Google). Com base na análise realizada, foram produzidos dois artigos científicos. O primeiro foi submetido, aceito e já apresentado no Congresso Regional de Iniciação Científica e Tecnológica em Engenharia (CRICTE2016), tendo destaque por ser um dos cinco melhores trabalhos do congresso. O segundo foi submetido e aceito no *Lat.Am.Symp. on Infrastructure, Hardware and Software* (SLIHS) do *XLII Latin American Computing Conference* (CLEI 2016) e será apresentado em outubro deste ano. Como esperado, a análise apresentou um nível de segurança maior para a autenticação e acesso aos recursos. O ponto negativo está na utilização de um IdP externo, visto que este pode coletar dados de uso, comprometendo a privacidade dos usuários e infringindo a política interna da organização. O projeto de pesquisa terá continuidade e abordará a integração com provedores de identidades de redes sociais (*i.e.*, Facebook), uma vez que os grupos podem ser utilizados como identificadores no processo de autenticação, além de atuarem como fóruns de discussão e suporte. Adicionalmente, esse projeto de pesquisa serviu de base para o desenvolvimento de um trabalho de conclusão de curso.