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. Facebook Connect. OpenStack.

Uma nuvem computacional é um modelo de prestação de serviço por meio de *commodities* que fornece acesso ubíquo, conveniente e sob demanda a um conjunto de recursos configuráveis que podem ser rapidamente provisionados e liberados com o mínimo de esforço. Entre as diversas soluções de nuvens computacionais o OpenStack se destaca pela participação da comunidade, por ser gratuito e de código aberto, pela integração com demais soluções existentes e principalmente pela alta adoção por diversas organizações nos últimos anos. Contudo, ao passo que as organizações adotam uma solução de nuvem, um novo sistema de autenticação e autorização é necessário para liberar o acesso aos recursos computacionais. 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 todas as suas credenciais para autenticação. Assim, como grande parte dos serviços na Internet, as nuvens computacionais se deparam com problemas similares e algumas empregam mecanismos *Single Sign-On* (SSO) para auxiliar no gerenciamento de identidades dos usuários. A principal característica de um mecanismo SSO é prover um identificador único ao usuário, que será utilizado para negociar a autenticação em qualquer serviço que suporte o mecanismo. Nos últimos anos, os mecanismos SSO centrados no usuário (*e.g.*, OpenID Connect, Facebook Connect) se destacaram por proporcionarem uma possibilidade mais dinâmica e acessível às organizações que fornecem serviços de computação em nuvem. Devido a variedade dos mecanismos de autenticação única, a escolha do mecanismo mais adequado não é uma tarefa simples, principalmente porque não foi encontrada uma classificação desses mecanismos com ênfase em nuvens computacionais ou uma análise de segurança dos potenciais riscos de uma solução. Dessa forma o objetivo dessa 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 TCHE, do Laboratório de Processamento Paralelo e Distribuído (LabP2D). Para o desenvolvimento do trabalho, foram realizadas duas etapas com dos métodos distintos de pesquisa: referenciada e aplicada. Na pesquisa referenciada foi realizado o levantamento bibliográfico dos assuntos correlatos à segurança da informação, em específico ao processo de autenticação e autorização. Ao final dessa pesquisa foi elaborada uma taxonomia em forma de artigo, que permite classificar os mecanismos SSO com foco em nuvens computacionais. Esse artigo teve colaboração do Laboratório de Arquitetura e Redes de Computadores (LARC), da Universidade de São Paulo (USP). Na pesquisa aplicada, dois mecanismos SSO foram implementados no OpenStack, utilizando Provedores de Identidade (IdP) externos. O primeiro mecanismo já se encontra nos pacotes oficiais do OpenStack e permite a

configuração do OpenID Connect para a autenticação SSO. O IdP utilizado é o do Google. Contudo, o objetivo em usar esse mecanismo é permitir apenas que usuários autorizados acessem a nuvem, e não qualquer pessoa com uma conta do Google. O primeiro meio de realizar esse filtro foi a utilização de um grupo no Google Groups. Contudo, no decorrer da pesquisa foi verificado que o IdP do Google não oferecia suporte ao uso do Google Groups para a autenticação. Dessa forma, a recomendação do Google é utilizar um domínio registrado no Google Apps e criar um grupo dentro deste domínio. Assim, foi utilizado um domínio existente no Google Apps e os usuários deste grupo puderam se autenticar na nuvem. Porém, nem todas as organizações utilizam domínios do Google Apps e esse meio pode não ser viável para a autenticação. Dessa forma, foram pesquisados mecanismos similares ao OpenID Connect para a implementação na nuvem e o Facebook Connect foi escolhido, devido a alta adoção das aplicações na Internet e por fazer parte de uma das redes sociais mais utilizadas atualmente. Assim, foi encontrada uma solução de autenticação com o Facebook Connect usada pelo TryStack, a nuvem de testes do OpenStack. Porém, essa abordagem não funcionou corretamente por utilizar APIs descontinuadas e problemas de segurança que não verificavam de fato se o usuário estava apto a se autenticar, liberando o acesso à qualquer membro do Facebook. Assim, foi criado um *proxy* de autenticação chamado OpenStack-Facebook-LinkedIn (OFL), que permite a autenticação com o Facebook e corrige os problemas encontrados na solução do TryStack. Portanto, somente os usuários que pertencem a um grupo específico do Facebook podem se autenticar na nuvem e essa validação é realizada da forma correta, obtendo todos os membros do grupo e verificando a associação do membro. Por fim, foram realizadas duas análises de segurança, uma com cada mecanismo, para a verificação de problemas de segurança e privacidade ao utilizar tais mecanismos. Os resultados obtidos geraram quatro trabalhos científicos e um Trabalho de Conclusão de Curso (TCC). O primeiro trabalho é um artigo aprovado no XXVII Congresso Regional de Iniciação Científica e Tecnológica em Engenharia (CRICTE 2016), tendo destaque como um dos melhores trabalhos do congresso. O segundo trabalho é um artigo aceito e apresentado no *XLII Latin American Computing Conference* (CLEI 2016). O terceiro trabalho é um artigo apresentado na Escola Regional de Alto Desempenho (ERAD-RS 2017). O quarto trabalho foi um minicurso ministrado no XXXV Simpósio Brasileiro de Redes de Computadores (SBRC 2017). Como esperado, ambas as soluções apresentaram um nível maior de segurança para a autenticação e acesso aos recursos, sendo que a solução com o Facebook Connect apresentou menos problemas de segurança. O ponto negativo em utilizar tais mecanismos é a utilização de um IdP externo, visto que o mesmo pode coletar informações durante a autenticação, comprometendo a privacidade dos usuários e infringindo a política interna da organização.