Title: An Authentication Model towards Cloud Federation in the Enterprise

Author: M. Noureddine R. Bashroush

PII: S0164-1212(12)00340-8
DOI: doi:10.1016/j.jss.2012.12.031
Reference: JSS 9080

To appear in:

Received date: 2-3-2012
Revised date: 18-10-2012
Accepted date: 6-12-2012

Please cite this article as: Noureddine, M., Bashroush, R., An Authentication Model towards Cloud Federation in the Enterprise, *The Journal of Systems and Software* (2010), doi:10.1016/j.jss.2012.12.031

An Authentication Model towards Cloud Federation in the Enterprise

M. Noureddine[a]*, R. Bashroush[b]

[a]*Microsoft Corporation, Seattle,USA*
[b]*University of East London, London, UK*

Abstract

Cloud Computing has emerged as a new paradigm which brought business opportunities as well as software engineering challenges. In The Cloud computing, business participants such as service providers, enterprise solutions, and marketplace applications are required to adopt a cloud architecture engineered for security and performance. Marketplace applications offer a great opportunity for enterprises to employ new Cloud capabilities to add value and extend business functionality. One of the major hurdles of formal adoption of Marketplace in the Enterprise is performance. Enterprise applications (e.g. Lync Server, SAP, SharePoint, and Exchange Server) require a mechanism to predict and manage performance expectations. In previous research, we provided optimization for OAuth 2.0 adoption in the Enterprise. In this research, we extend the optimization to include identity federation in the Marketplace. This optimization is achieved by introducing provisioning steps to pre-establish trust amongst enterprise applications' Resource Servers, its associated Authorization Server and the clients interested in access to protected resources. We then introduce the notion of referral tokens to enable Marketplace applications federation across organizations. In this architecture, trust is provisioned and synchronized as a pre-requisite step to authentication amongst all communicating entities in OAuth protocol, and referral tokens are used to establish trust federation for Marketplace applications across organizations. A real-life case study and a simulation test were used to validate the results.

Keywords: Cloud Computing; Engineering for federated clouds; Cloud Security; OAuth; Authentication and Authorization; Cloud Performance.

1. Introduction

As they leverage Cloud computing, one of the important topics in the Enterprise is the Marketplace integration. Whether the enterprise application is hosted in a dedicated tenancy or shared tenancy, the challenges are similar, that is to adopt the right security protocol engineered for security and performance. OAuth protocol is becoming a popular choice for solving such challenges. OAuth is a claim-based security protocol that enables users to grant third-party access to their protected resources without sharing their passwords. OAuth implements this by using a data structure, called token, that decouples the access right (Authorization) from the client login credentials (Authentication). Clients request tokens from authorization server and present the token to the service provide. OAuth 1.0 [1] was published in December 2007 and quickly became the industry standard for web-based access delegation. However, OAuth 1.0 was faced by many challenges to make its way into the enterprise domain mainly

* Corresponding author. Tel.: +1 (425)706 9073.
E-mail address: Moustafa.Noureddine@Microsoft.com