Opening Up OpenStack's Identity Service

Authors:
David W Chadwick, Ioram S Sette, Kristy W Siu
Author Affiliations
University of Kent. Tel: +44 1227 82 3221
Email: d.w.chadwick@kent.ac.uk, iss7@kent.ac.uk, k.w.s.siu@kent.ac.uk
Keywords: Clouds, federated access, ABFAB, Virtual Organisations

Abstract

OpenStack is a relatively new open source cloud computing project. It has rapidly become very popular since its first release on 21st October 2010. It has thousands of members, comprising technologists, developers, researchers, and cloud computing experts from 87 countries [1]. Over 140 organisations are members of the OpenStack foundation, including many well-known multinational computer companies such as HP, Intel, IBM, AT&T, Cisco and Dell. OpenStack issues new stable releases every six months, usually in April and September, and the alphabet is used to determine the first character of each named release. **I**cehouse was released in April 2014 and **J**uno in September 2014. **K**ilo is scheduled for April 2015.

OpenStack provides several cloud services, which are all accessible via RESTful APIs [2].It provides a compute service (codenamed Nova) that is used for the provisioning and managing of large networks of virtual machines. It provides two storage services: Swift - a fully distributed, object storage platform, capable of storing petabytes of data, and used for the storage, backup and retrieval of files; and Cinder - a block storage service for use by the compute instances. The networking service (codenamed Neutron) is used for managing networks and IP addresses. Glance is the virtual machine image service that provides for the taking of snapshots of images, and for their storage, registration, discovery and delivery to virtual machines. It can use Swift to store its images, Neutron to transfer them, and Nova to run them. OpenStack also supports a telemetry service (codenamed Ceilometer) for aggregating usage and performance data across the cloud; an orchestration service (codenamed Heat) to allow application developers to describe and automate the deployment of their cloud infrastructure through templates; a data processing service (codenamed Sahara) and database as a service (code named Trove). Horizon is a web based graphical user interface (or dashboard) which allows administrators to manage their OpenStack installation.

Keystone is the identity service which authenticates users and provides them with an authorisation token to access the various OpenStack services. The services use the token to get authorisation information about the user, in terms of the user's ID, the project and domain the user is a member of, and the role he has in the project. The services use either role based access control to determine which privileges are available to each role, or access control lists to give direct access to users. Despite is openness, nevertheless, until the University of Kent started to work with OpenStack, Keystone had no federated identity management capabilities, and all user accounts and passwords had to be stored in Keystone, usually in a backend LDAP directory. This is clearly not appropriate for widescale open access to clouds, as is required by European universities. Federated access is essential.

A previous paper [3] describes how we first added protocol independent federation to OpenStack. This was achieved by modifying Keystone and adding two different sets of functionality to it: a set of federation protocol handling modules that returned common output, and a protocol independent federation trust management capability. We then worked within the OpenStack Keystone community to encourage them to adopt our protocol independent approach to federated access. This they did, but decided to use an Apache front end to handle the federation protocols, rather than Keystone. The first public release of federated Keystone was issued in April 2014, but due to the short release cycles, this only supported SAML, using the mod_shib plugin to Apache. The Juno release was made fully protocol independent, and Kilo will have inbuilt support for the ABFAB and OpenID Connect protocols (at least) using appropriate Apache plugins. Other federation protocols should be relatively trivial to add now that the design is finalised.

This talk will describe the way that protocol independent federated access has been integrated into the core release of Keystone. It will also describe our latest work, which has been to add virtual organisation management to Keystone. Our long term objective is to make Keystone a generic VO management service for any type of cloud or web service, so that it can replace VOMS [4], the VO management system currently used by grids.

Acknowledgements

This research was funded by the EC, under the Geant Open Call Project, CLASSe

References

[1] http://www.openstack.org/ (last accessed 26 Nov 2012)

[2] Roy Thomas Fielding. “Representational State Transfer (REST)”. Chapter 5 of "Architectural Styles and the Design of Network-based Software Architectures". PhD Dissertation submitted to Univeristy of California, Irvine, 2000. Available from http://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm

[3] David W. Chadwick, Kristy Siu, Craig Lee, Yann Fouillat, Damien Germonville. “Adding Federated Identity Management to OpenStack”. Journal of Grid Computing: ISSN: 1570-7873 (Print) 1572-9184 (Online). Volume 12, Issue 1 (2014), Page 3-27. http://dx.doi.org/10.1007/s10723-013-9283-2

[4] Alfieri, R., Cecchini, R., Ciaschini, V., Dell'Agnello, L., Frohner, A., Lorentey, K., Spataro, F., “From gridmap-file to VOMS: managing authorization in a Grid environment”. Future Generation Computer Systems. Vol. 21, no. 4, pp. 549-558. Apr. 2005

Author Biographies

David Chadwick is Professor of Information Systems Security at the University of Kent. He has published widely, with over 150 publications in international journals, conferences and workshops. A full list can be obtained here (http://www.cs.kent.ac.uk/people/staff/dwc8/pubs.html). He has successfully managed over 30 research projects, with a value over £2 million and is the PI for Kent in the Geant Open Call Project CLASSe, which is adding generic federated identity management (including the ABFAB and SAML protocols), and Virtual Organisation management, to OpenStack. He has served as a PC member of over 200 international conferences and been the PC Chair or Co-Chair for over 10 (including TNC).

Ioram Sette is a PhD student from the Federal University of Pernambuco, Brazil, on a one year internship with Prof Chadwick at Kent. He is researching the distributed management of policies in clouds, and is using OpenStack as the exemplar to implement his ideas.

Kristy Siu was a research associate at the University of Kent, working on the CLASSe project. She implemented the VO management software, and has recently left to take up a career as a computer science teacher.