Scaling beyond your cloud
Hybrid OpenStack Clouds

Marek Denis

CERN openlab Board of Sponsors, June 10th 2015, Geneva, Switzerland

Hybrid clouds - the future of clouds

Cloud computing at CERN

CERN deploys an OpenStack to provide resources to its users. Currently spanning across two data centers, with over 100 000 cores, 200 TB of accumulated RAM and 6PB of Ceph based storage, the OpenStack infrastructure is used for LHC experiments data processing workloads, IT services as well as employees' personal projects. Keeping up with the releases, CERN runs OpenStack Juno on both KVM and Hyper-V based hypervisors. With the security and organisation policies in mind users have variety of authentication methods to choose from, including Kerberos, X509 and Web Single-Sign-On.

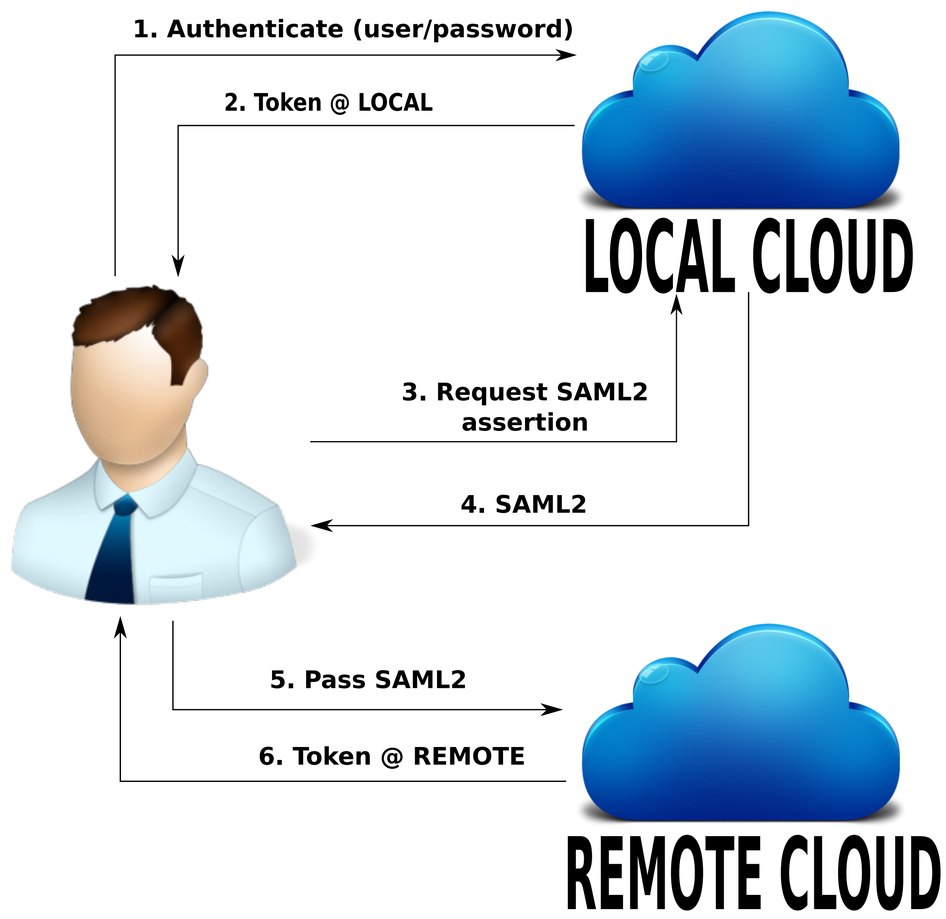
Identity Federation in OpenStack

Identity Federation has been available since Icehouse version. From that initial release Identity Service (Keystone) has been capable of acting as a Service Provider, dynamically authorizing credentials issued by trusted Identity Providers. Assertions are translated, based on mapping rules defined per Identity Provider, into ephemeral user identities and local groups membership. The remote user is granted access to local resources. With OpenStack Kilo release federation is core part of the system and new features are delivered - Web Single-Sign-On, mapping enhancements, as well as seamless, on premise cloud bursting capabilities (Keystone2Keystone).

Seamless cloud bursting

Keystone2Keystone

Since OpenStack Kilo release Keystone can act as a simple SAML2 Identity Provider. The user is able to exchange his local OpenStack token for a signed SAML2 assertion. The list of available trusted clouds is now stored in the Service Catalog. For reasons of security, an OpenStack token cannot be used across multiple clouds, however user experience can be satisfied with clients handling multiple tokens at the same time. Remote Keystone acts as a Service Provider, where trusted Identity Providers, Protocols and corresponding Mapping Rulesets must be configured. Keystone2Keystone leverages the SAML2 protocol - an established and open standard allowing for the secure transport of credentials between the trusted peers. With SAML2 being used, an integration with non-OpenStack products will be much easier. Keystone2Keystone functionality provides a solid building block for other services to communicate seamlessly across multiple clouds.



OpenStack Hybrid Clouds

Hybrid clouds models

Hybrid cloud architectures allow users to use login from their local OpenStack cloud and boot Virtual Machines on other trusted clouds. Depending on the priorities and budget some parts of infrastructure need better parameters (higher cost), whereas others are less important. Those can be provisioned on cloud providing cheaper but also less strict SLA in terms of e.g. latency or durability.
Bursting into remote clouds can help in providing sufficient, on demand capacity within private clouds. Instead of adding new bare-metal compute nodes to the private cloud infrastructure, administrators can simply buy virtual resources from public cloud provider.Currently over 30 OpenStack based public cloud providers are planning to offer distributed identity federation as part of their business model.

CERN and Rackspace joint project

During openlab phase IV, CERN and Rackspace demonstrated a fully working federated setup spanning across CERN Private Cloud and the Rackspace Private Cloud. All code used for the demo is merged into the official OpenStack distribution. CERN uses identity federation at their production servers since September 2014, whereas Rackspace plans to offer federated access to their customers due to end of 2015. Further cooperation includes expanding to other services. Currently there is anongoing work towards automatized sharing images between trusted clouds. This brings new value in automatic propagation of new versions of custom images or snapshots including new configuration for distributed systems.