

Installation and Usage of the Federated OpenStack Client – Icehouse Version

Version	Date	Author	Comments
0.1	16/09/14	Kristy Siu	Initial Draft

Introduction

A modified version of the OpenStack client has been produced which enables federation via WebSSO using the command line client. This guide explains where to get the code, how to install it and notes on using the client.

Download

The client code requires both an alternative OpenStack command line client, which can be found at:

<http://github.com/kingBenny/python-openstackclient.git>

And a modified python-keystoneclient library, which is available at:

https://github.com/kingBenny/python-keystoneclient/tree/icehouse_compatible

Installation



You should ensure that the following steps are followed in order.

- 1) Install Git at the command line with *sudo apt-get install git*
- 2) Install setuptools with *sudo apt-get install python-setuptools*
- 3) Install pip with *sudo easy_install pip*
- 4) Clone a local copy from the python-openstackclient repository, from branch: master
- 5) Install the openstack universal client with *sudo python setup.py install*
- 6) In most cases an error message will be reported “No module named pbr.version” is reported.
- 7) To resolve, install pbr with *sudo pip install pbr*. Remove the reference to *python-keystoneclient>=0.10.0* on line 5 of *requirements.txt*. It can be commented out with a # sign at the start of the line.
- 8) Clone a local copy from the python-keystoneclient repository, from branch: icehouse_compatible
- 9) Install the openstack keystone client with *python setup.py install*

Usage



For general usage commands users should refer to the official OpenStack documentation located [here](#).

In order to use federation in your client the following environment variable should be set:

```
OS_IDENTITY_API_VERSION=3
```

To authenticate using federation you must append the federated flag (-F) to each request. E.g:

```
openstack -F --os-auth-url http://keystone:5000/v3 user list
```

This will initiate the federated login flow and the following steps will ensue:

1. A list of available federated identity providers will be presented e.g.
2. Select your desired Identity Provider using the correct number.
3. A list of supported protocols will be presented e.g.
4. Select your desired protocol.
5. Your browser will open at your identity providers' website.
6. Authenticate following the identity providers' instructions.
7. On successful authentication you will be redirected to a success page and can return to your command prompt.
8. Normal client usage can now be resumed.