



Cloud federation

Prelude to Hybrid Clouds

- › **CHEP 2015**
- › **Okinawa, Japan**

Marek Denis
CERN
Geneva, Switzerland



Basic definitions

OpenStack:

An Open Source Cloud Managing System which allows implementors to:

- Provision and manage compute, network, and storage resources quickly
- Monitor and alert on those resources
- Auto-scale cloud resources
- Standardize and control disk & server images

Keystone:

The Identity service that comes bundled with OpenStack.

Keystone allows implementors to:

- Provision users, projects, roles
- Manage their authorization (and authentication)
- Programmatically discover implemented cloud services

Cloud Federation:

Deployment and management of multiple external and internal cloud computing services to match business needs. A federation is the union of several smaller parts that perform a common action.

OS-FEDERATION timeline



**OpenStack Summit
(November 2013)**

Basic concept and
initial discussions
during design
sessions

**OpenStack
Icehouse
(April 2014)**

Server-side
OS-
FEDERATION
delivered
(located in the
extensions
namespace)

**OpenStack Juno
(October 2014)**

OS-FEDERATION
marked as stable.
Client code
integrated with
official OpenStack
libraries and CLIs
(CERN uses
OS-FEDERATION
internally since
September 2014)

**OpenStack Kilo
(April 2015)**

Added WebSSO
support in
keystone.
Mapping engine
enhancements

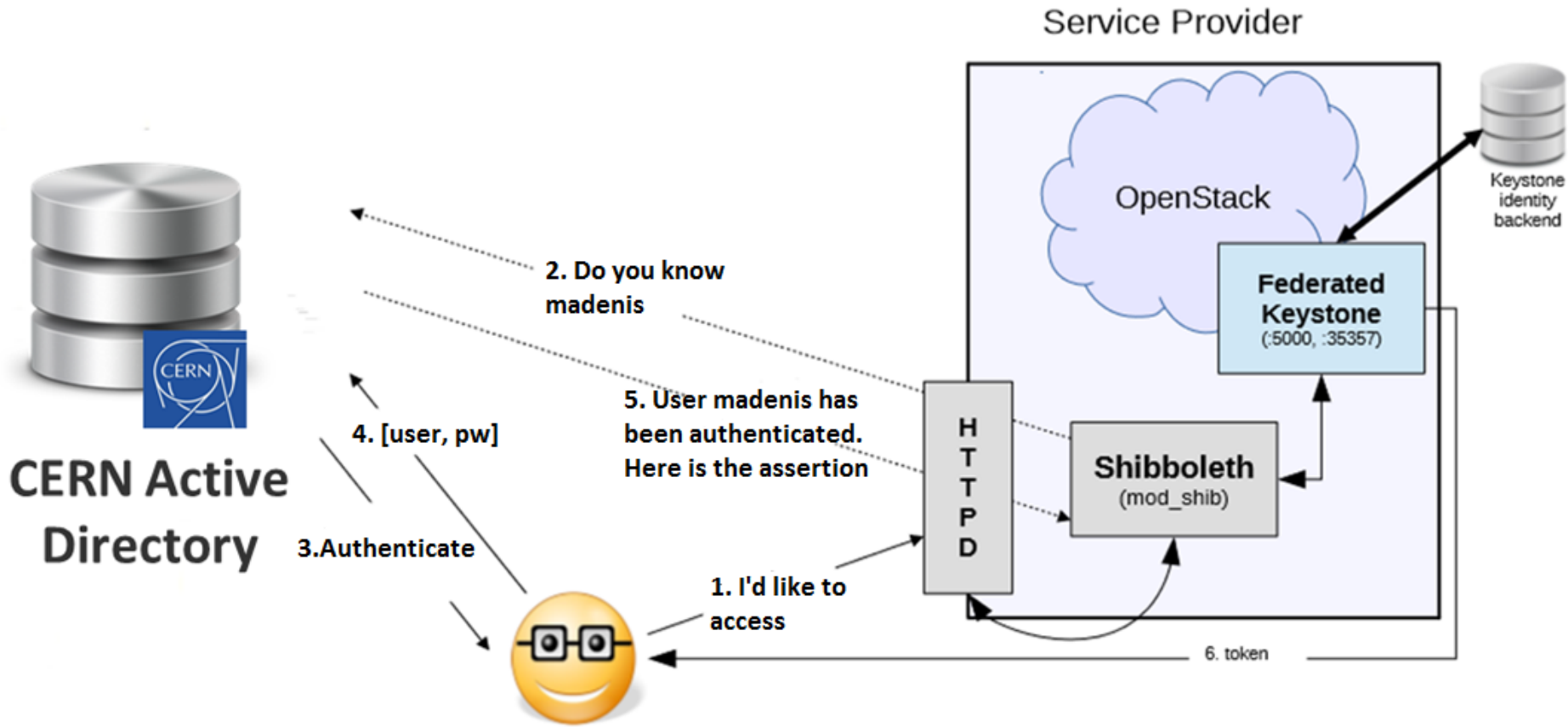
OS-FEDERATION advantages

- › **One account per multiple remote clouds**
- › **Better user experience**
- › **Easier to burst into remote clouds**
- › **Increased overall security**

- › **User identities are stored in the Identity Provider, not in the OpenStack backend**
- › **Identity Provider can be trusted by multiple Service Providers (clouds)**
- › **Cloud federated users are ephemeral (they don't exist in the cloud infrastructure)**
- › **Ephemeral users are granted access to the resources by dynamically assigned group membership.**
- › **OpenStack utilizes a *Mapping Engine* for translating external assertions/claims into set of local parameters. This is used for other authN mechanisms e.g. *X509, Kerberos*.**
- › **OpenStack utilizes “Cloud Auditing Data Format” (CADF) for cloud auditing.**

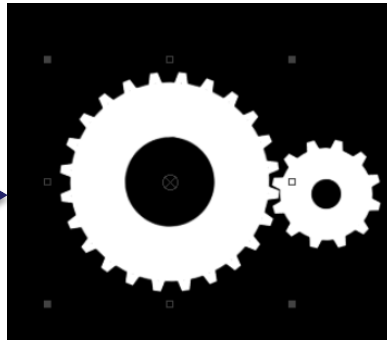
- › **Deployments recommended and tested with established protocols**
 - SAML2
 - OpenID Connect
- › **Keystone must be deployed on top of Apache HTTPD webserver...**
 - ...and corresponding modules must be installed
 - mod_shib/mod_mellon for SAML2
 - mod_oidc for OpenID Connect
- › **Keystone is federation protocol agnostic...**
 - ...however it understands the concept of Identity Provider and Protocol
- › **Works with**
 - Shibboleth IdP
 - Microsoft ADFS
 - IBM TFIM

Federated authN & authZ



Credits Luca Tartarini

Transforming assertion into local credentials



LOGIN: madenis
LANGUAGE: EN
DEPARTMENT: IT/OIS
FULLNAME: Marek Denis

```
[  
  {"local":  
    [{"user": {"name": "{0}"}]},  
    "remote":  
    [{"type": "ADFS_LOGIN"}]  
  },  
  {  
    "local":  
    [{"group": {"id": "devs"}},  
     {"group": {"id": "openlab"}}],  
    "remote":  
    [{"type": "DEPARTMENT",  
     "any_one_of": ["IT/OIS"]}]}  
]
```

```
{  
  name: madenis  
  groups: [  
    "devs",  
    "openlab"  
  ]  
}
```


Cloud Federation at CERN

- › **OpenStack@CERN** web access utilizes Web Single-Sign-On
- › **Command Line Interface access also available with help of SAML ECP**
- › **Successful tests with INFN**
- › **CERN is a member of eduGAIN federation
(cloud resources sharing to be available soon)**
- › **Many academic institutions and universities are also interested**
 - (INFN, SLAC, University of Victoria, UTSA, EMBL)

More information

“Cloud Federation – Are we there yet?”

Presentation from OpenStack Summit in Paris
(with a federation demo)

<http://goo.gl/7x91Eb>

OpenStack OS-FEDERATION API

<http://goo.gl/cQSrfD>

Thank you

Marek Denis
marek.denis@cern.ch



Backup slides

Keystone2Keystone federation

- › **Keystone can also act as an Identity Provider**
- › **Transform your project scoped token into corresponding SAML assertion**
- › **Burst into other non-OpenStack services or operators**