Ibercloud: orchestrating services to provide virtualized access to IberGrid

C. Fernandez, A. Simón (CESGA)

I. Campos, E. Fernández, A. Lopez Garcia, J. Marco De Lucas, M.A. Nuñez Vega (IFCA)

C. Alfonso, I. Blanquer, M. Caballer, G. Molto (GRyCAP)

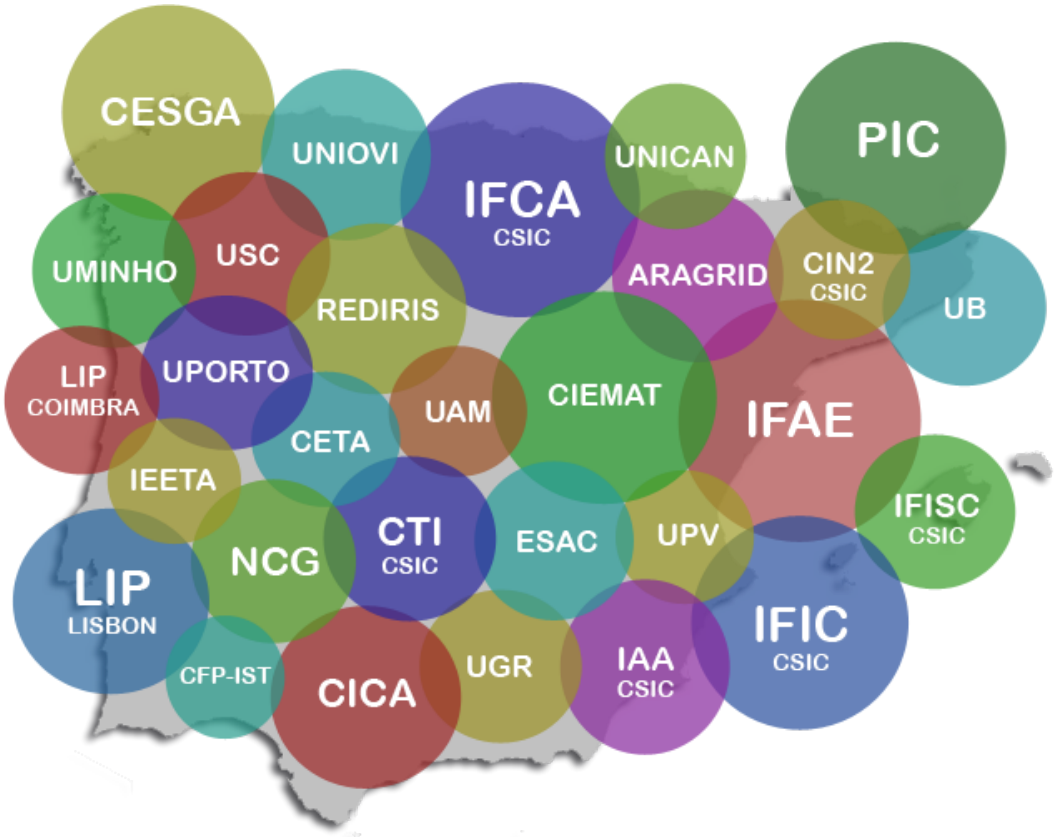
G. Borges, M. David, J. Gomes (LIP)

IberGrid

Protugal & Spain NGIs joint operations

24,000 cores and 20PBytes storage available to Grid user community

Wide usage of virtualization techniques



Ibercloud Objectives

- Investigate the requirements of scientific users of cloud technologies
- Deploy a federated cloud IaaS testbed for scientific computing within the Ibergrid collaboration
  - based on existing local deployments
- Provide a unique user friendly interface for the services

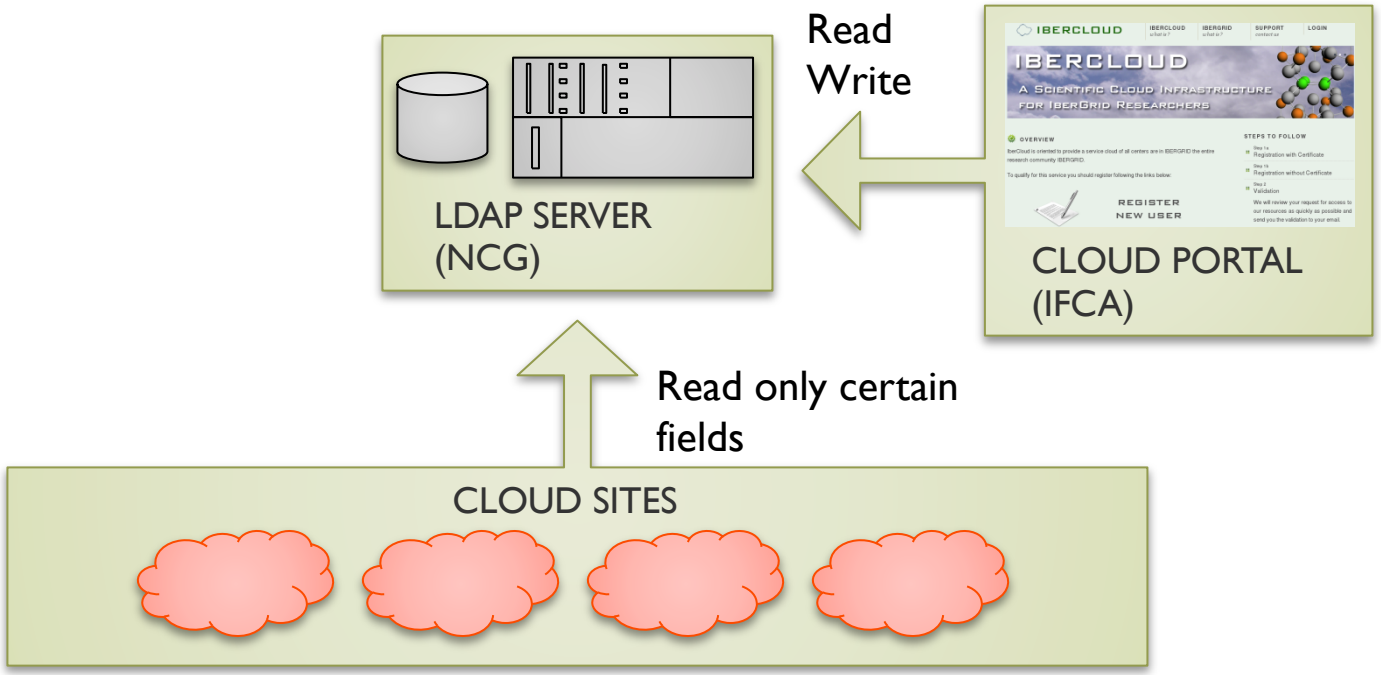
Ibercloud Sites

Authorization

- Users should be able to use a single identity at all sites
- Grid experience
  - VOMS ☺
  - User certificates ☹
- We want a working solution *fast*
  - working across cloud implementations
  - easy enough to be quickly deployable
  - Flexible for different models of federation (country, site)

Architecture

- Start with centralized LDAP authentication:
  1. Cloud service portal adds users do main LDAP instance
  2. Sites can read LDAP records and authenticate against LDAP server

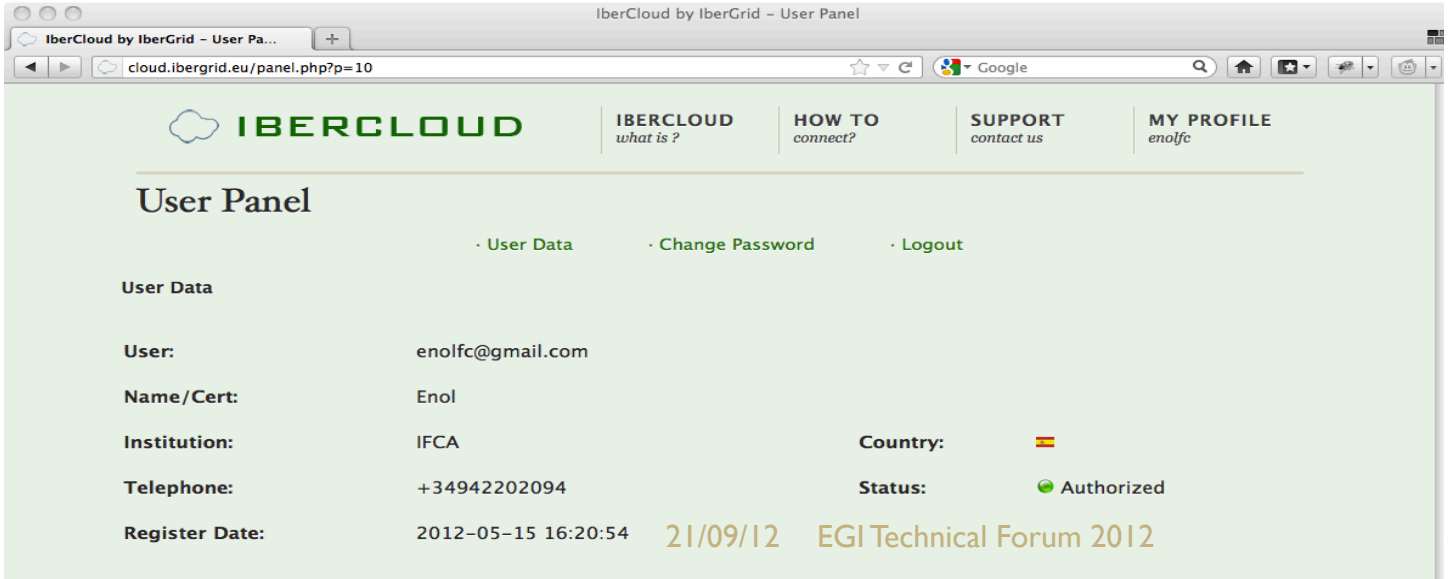


Registration Portal (I)

- Web portal to add users to the infrastructure
- http://cloud.ibergrid.eu

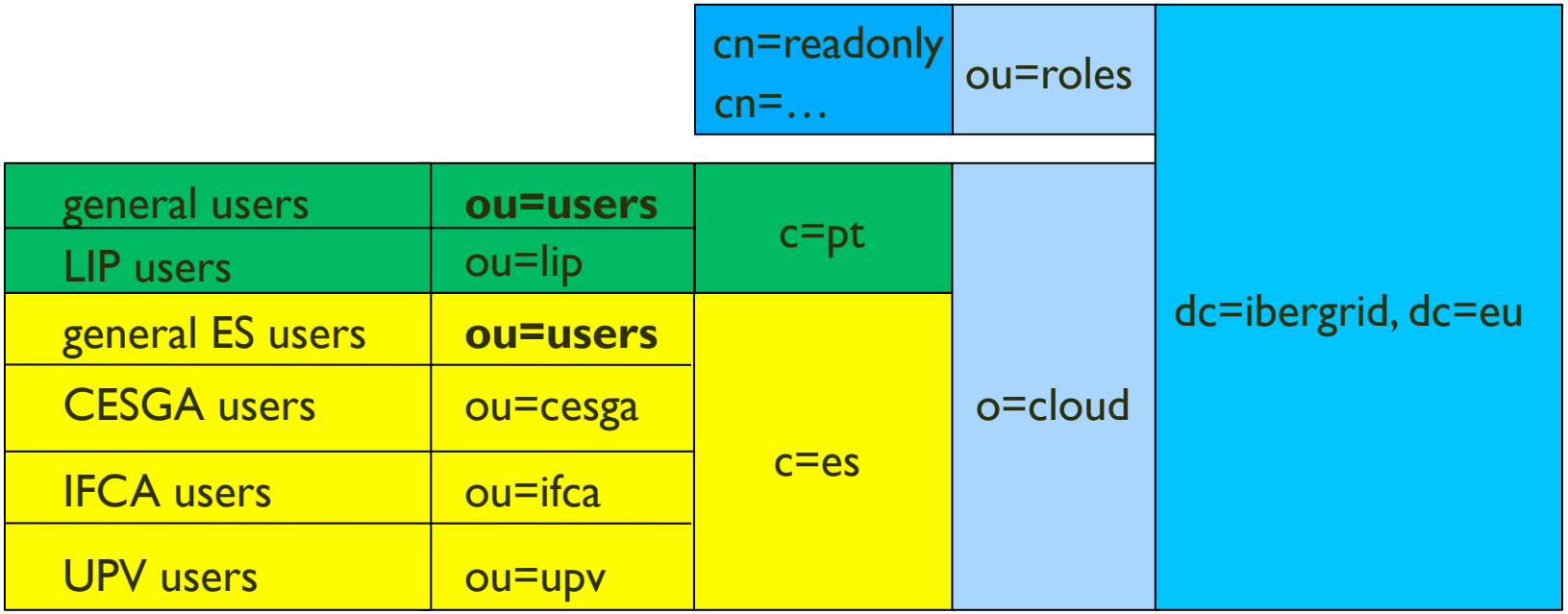
Registration Portal (II)

- Registration consists on filling a survey with intended usage
  - Not needed if already part of IBERGRID
- Each request is evaluated and approved independently



LDAP tree and namespaces (I)

- Tree with country and site branches



uid=aaa@xxx.pt, ou=users, c=pt, o=cloud,dc=ibergrid, dc=eu

uid=bbb@yyy.es, ou=users, c=es, o=cloud,dc=ibergrid, dc=eu

uid=ccc@cesga.es, ou=cesga, c=es, o=cloud,dc=ibergrid, dc=eu

LDAP tree and namespaces (II)

- Users are "uniquely" identified by e-mail with a common suffix:

uid=xxxx@yyyy.pt,	o=cloud, dc=ibergrid, dc=eu

- Internal remapping within the openldap server
  - All users remapped to o=cloud,dc=ibergrid,dc=eu
  - uid=xxxx@yyyy.pt is also a valid DN

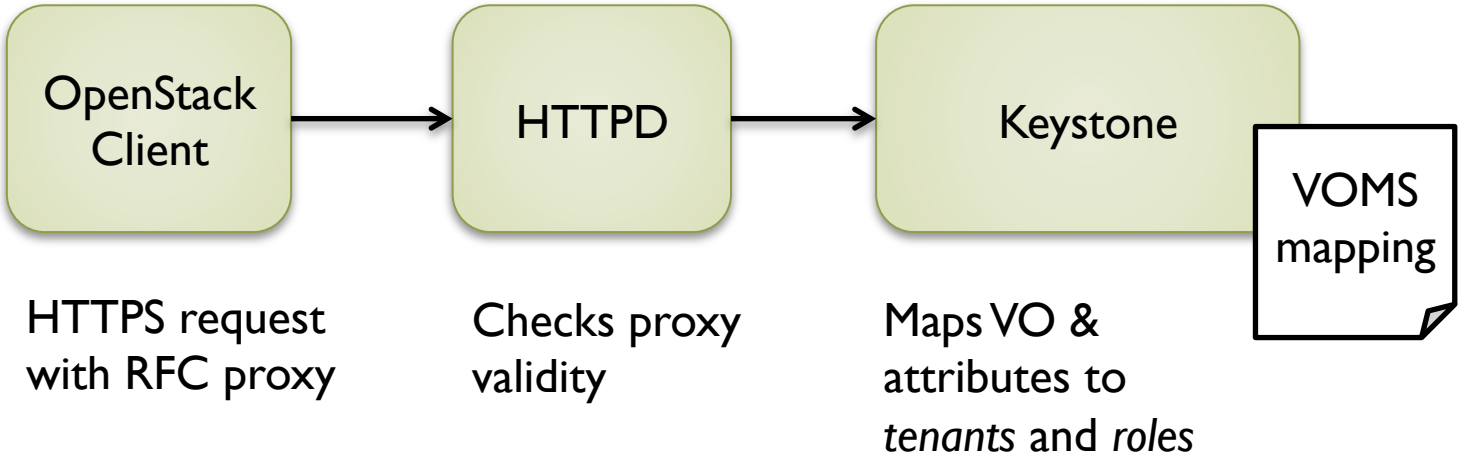
- We get the advantages of a hierarchical namespace with the simplicity of a flat namespace

LDAP Support

- OpenStack:
  - Authentication is performed by a dedicated service named "keystone"
    - Changed architecture while deploying our testbed
    - LDAP support required particular schema
  - IFCA has extended it for LDAP authentication
    - LDAP + LDAPS support
    - No restrictions on DN or LDAP schema
- OpenNebula:
  - Common DN for all users → remapping at the LDAP server
  - Secure LDAPS needed tweaks but worked
  - LDAP authentication with the APIs
    - Does not work → major show-stopper for us !

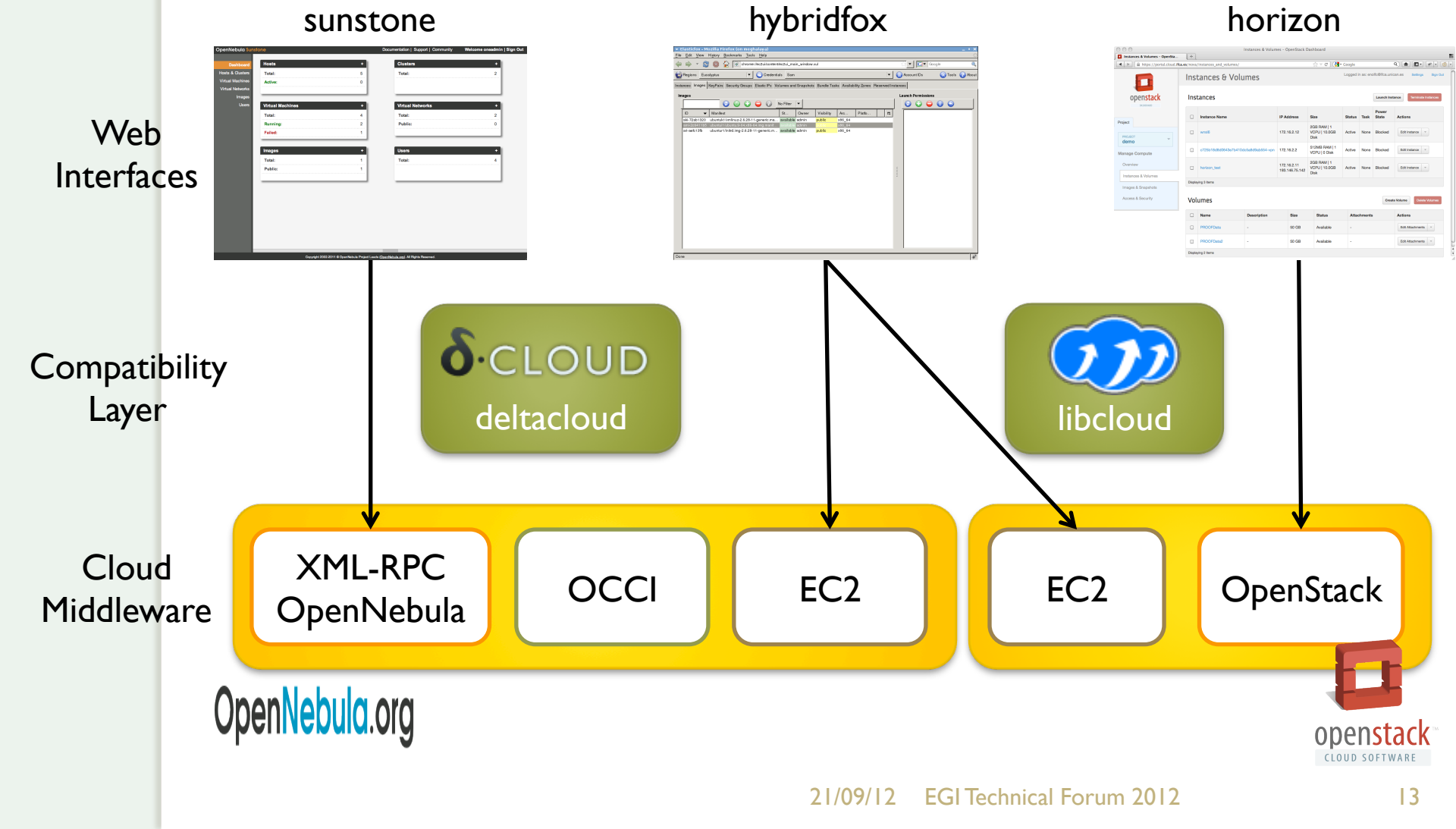
VOMS AuthN

- IFCA+CNRS Started to develop VOMS AuthN in OpenStack Keystone
  - Ibercloud will evaluate if it fits the deployment



Code on github: https://github.com/alvarolopez/keystone/tree/voms_auth
Docs: http://keystone-voms.readthedocs.org/en/latest/voms.html

Accessing the Resources



Site Capabilities (I)

CESGA

Name	small	medium	large	small-kvm	small-occi
Number of Cores	1	4	8	1	1
Memory (RAM)	1024	4096	8192	1024	1024
Disk	40GB	60GB	80GB	40GB	40GB
Intranet Network	10G Eth.				
Public/Private IP	Pool of public IPs with a maximum of 254				

IFCA

Name	m1.tiny	m1.small	m1.medium	m1.large	m1.xlarge
Number of Cores	1	1	2	4	8
Memory (RAM)	512	2048	4096	8192	16384
Disk	0	20	40	80	160
Intranet Network	GB Eth				
Public/Private IP	VLAN and VPN per project, no public IPs currently				

Site Capabilities (II)

LIP

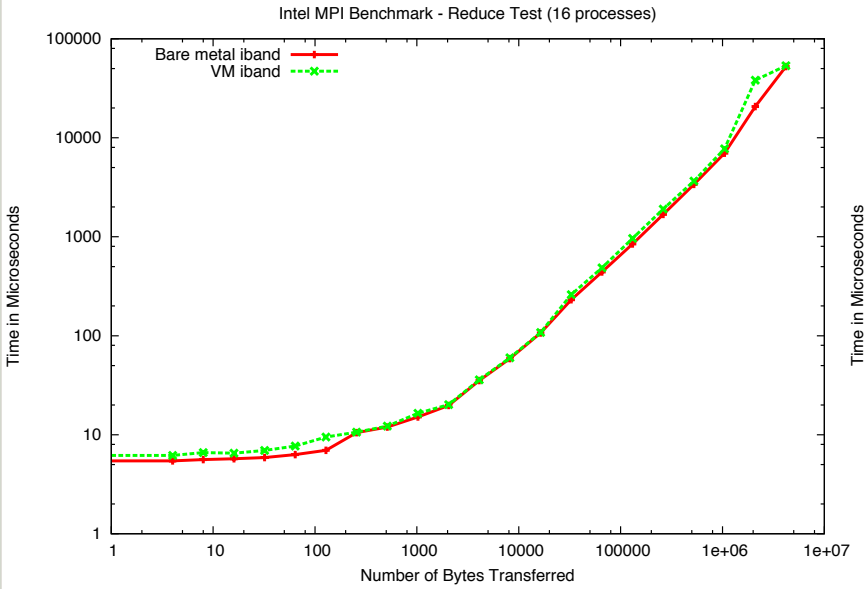
Name	small	medium	large
Number of Cores	1	2	4
Memory (RAM)	512	1024	4096
Disk	10	40	100
Intranet Network	GB Eth		
Public/Private IP	VLAN and VPN per project, no public IPs currently		

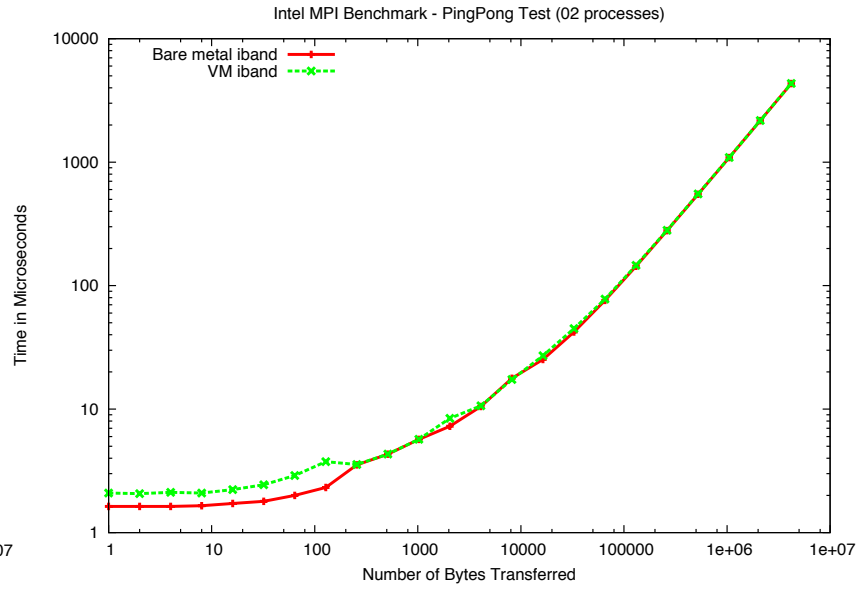
GRyCAP

Name	tiny	small	medium	large
Number of Cores	1	1	2	4
Memory (RAM)	512	1024	2048	4096
Disk	20	40	80	80
Intranet Network	GB Eth			
Public/Private IP	Pool of public IPs with a maximum of 32			

Use case: MPI Applications

- Good I/O performance with PCI Passthrough

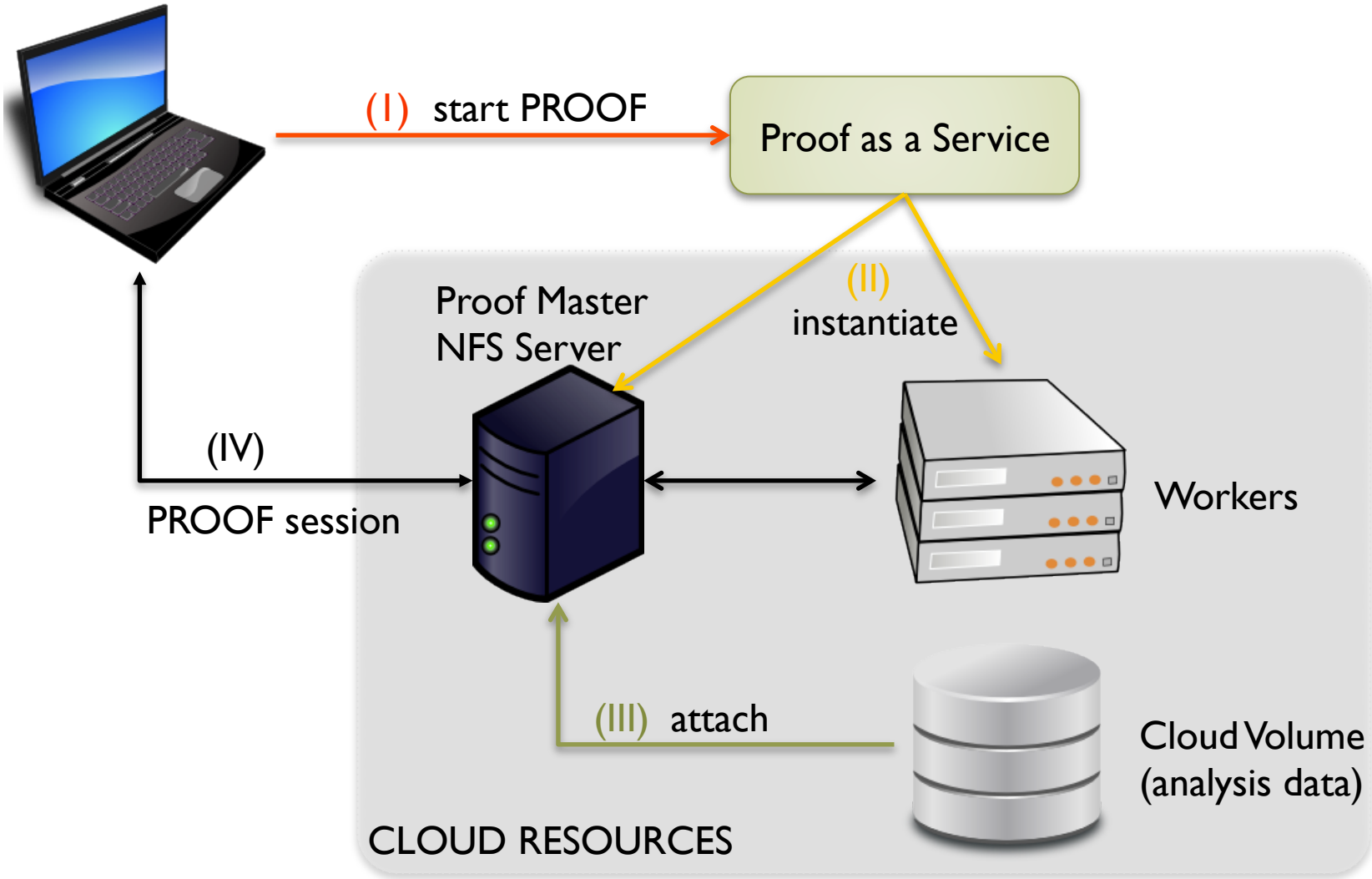




Use Case: PROOF as a Service (I)

- PROOF is a parallel mode for ROOT (HEP analysis software)
- PROOF requires the deployment of a set of services on the executing hosts
  - Not trivial for users
  - Dynamic demand of resources
- PaaS on top of the IaaS service
  - Builds PROOF cluster automatically from the ROOT interface

Use Case: PROOF as a Service (II)



Use Case: Mathematica

- Used at IFCA for physics phenomenology simulations
- Very specific machine configuration
  - not grid friendly
  - too heavy for desktops
- Researchers start VMs with Mathematica as needed
  - hardware independent environment
  - ability to test and execute various software configurations
  - better reliability and availability

Next steps…

- Continue working on federated identity
  - VOMS
  - SAML
- Investigate user interfaces/API compatibility
  - OCCI now also available in OpenStack
- Open infrastructure to pilot users
  - Get feedback and requirements
- VM Image Management
  - Image catalogues & repositories
- Monitoring & Accounting
  - following the EGI Cloud TF developments

Thanks

Questions?