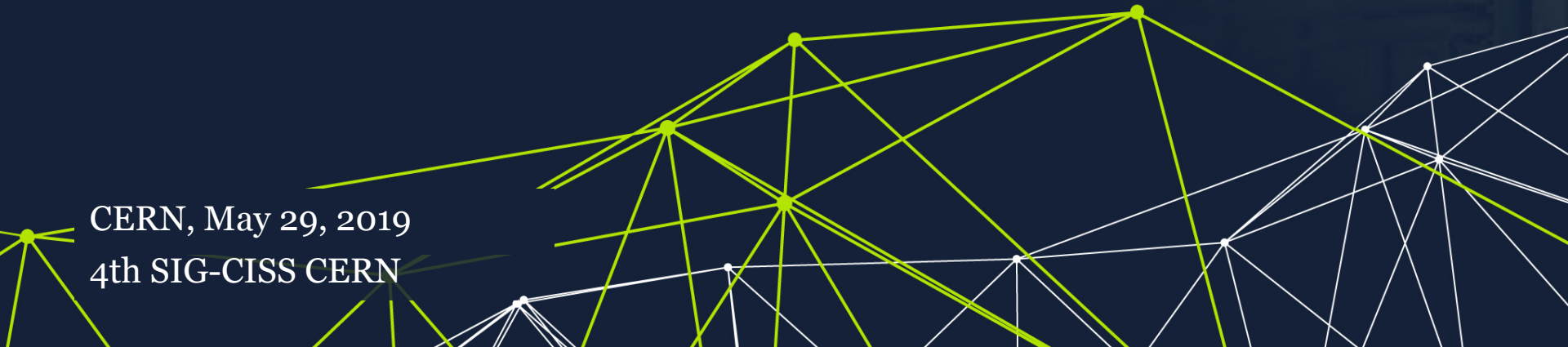
Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

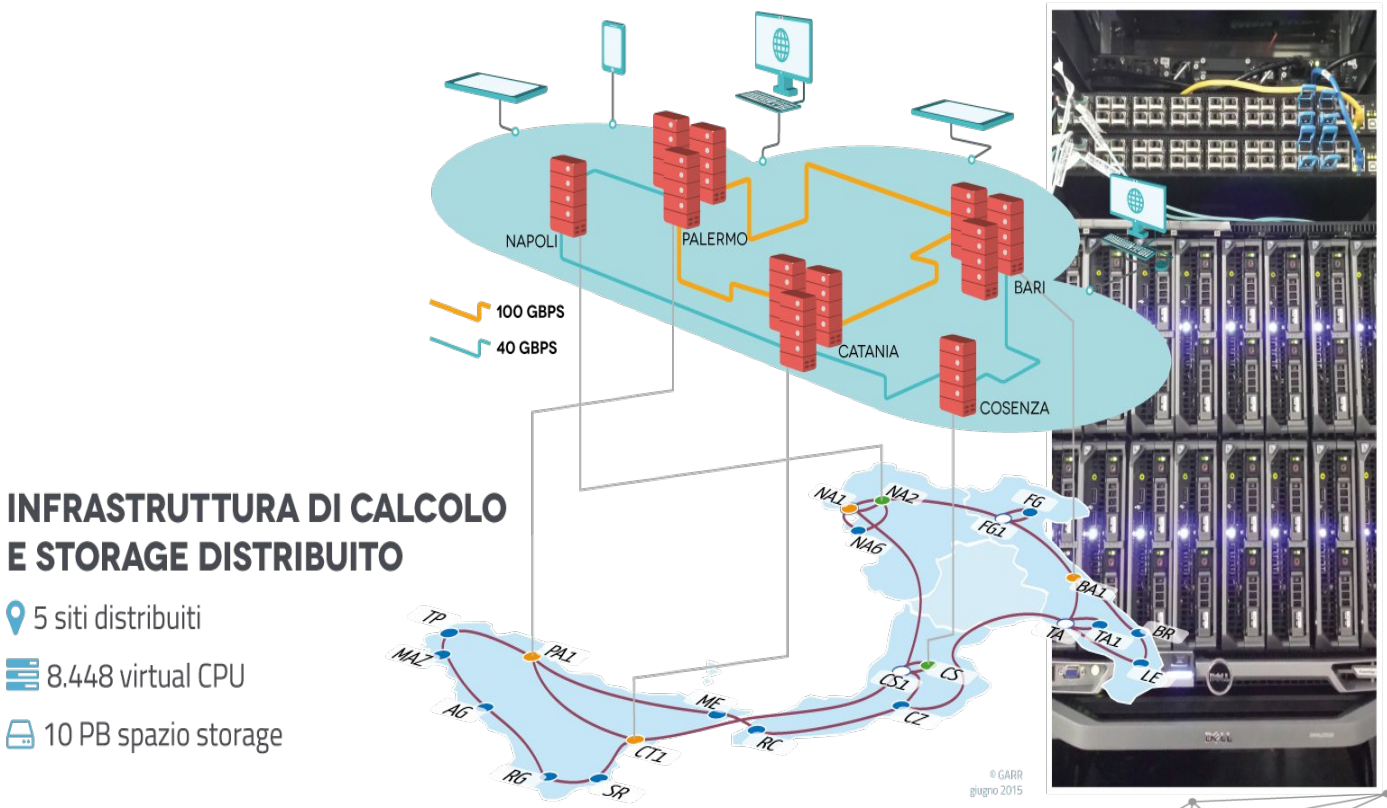
Integrating OpenStack and Kubernetes

ALBERTO COLLA / GARR
SAVERIO PROTO / SWITCH



CERN, May 29, 2019
4th SIG-CISS CERN

GARR Computing and Storage



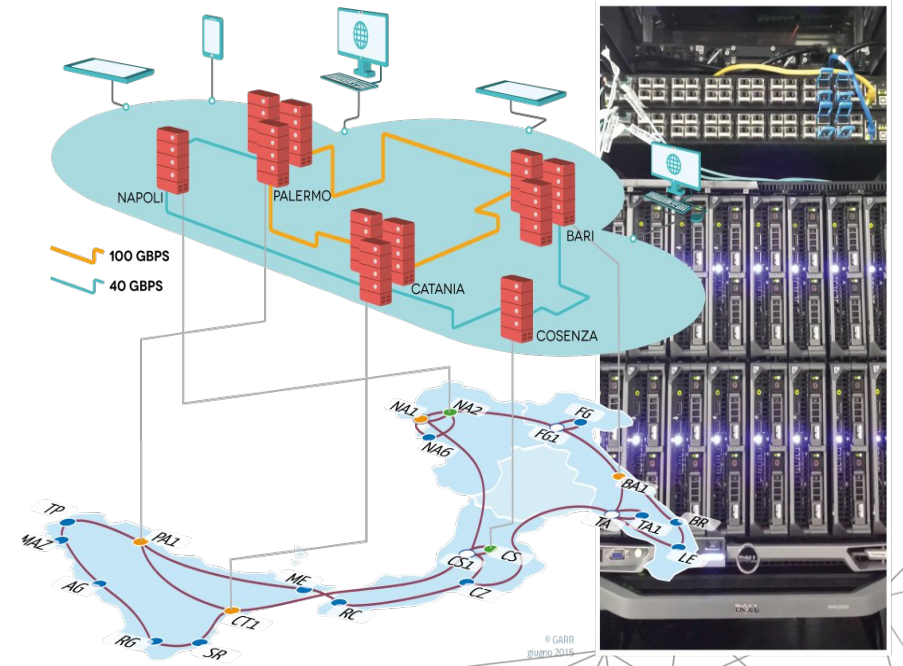
INFRASTRUTTURA DI CALCOLO E STORAGE DISTRIBUITO

- 5 siti distribuiti
- 8.448 virtual CPU
- 10 PB spazio storage

GARR Computing and Storage

The engine

MAAS juju ceph



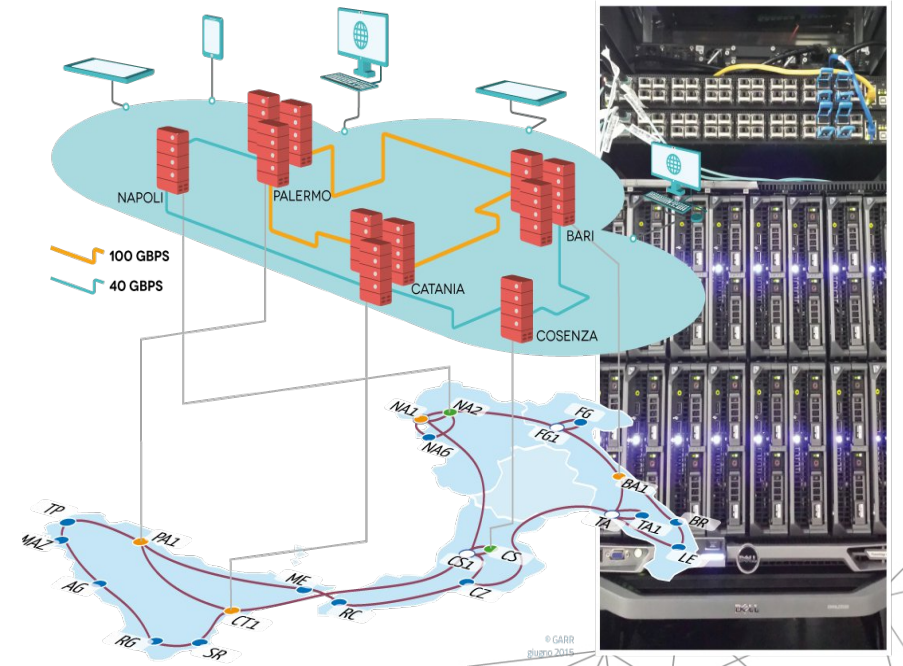
Consortium GARR THE ITALIAN EDUCATION & RESEARCH NETWORK

GARR Computing and Storage

GARR cloud

The engine

MAAS juju ceph



GARR Computing and Storage

GARR cloud

+ Multi-region

Catania + Palermo

+ DaaS

Deployment-as-a-Service

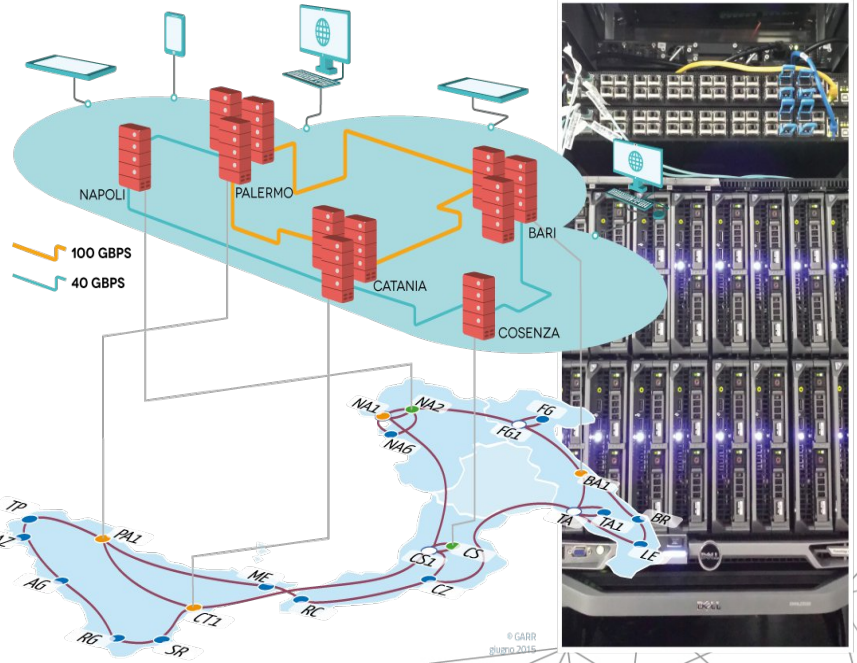
+ Federation

Upcoming:

- University of Padova
- Politecnico di Torino

The engine

MAAS JUJU ceph



Consortium GARR THE ITALIAN EDUCATION & RESEARCH NETWORK

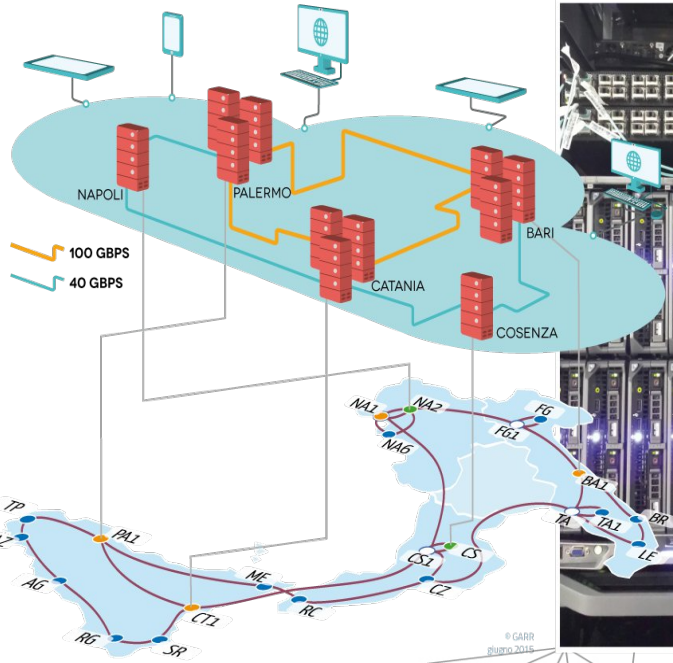
GARR Computing and Storage

GARR cloud

The engine

MAAS juju ceph

600 Users
1100 VM
3500 vCPU 9 TB_RAM
1 PB_storage 850 IP



ONLYOFFICE
CLOUD BUSINESS SOLUTION

IdP in the Cloud

Olimpiadi Italiane di Statistica

GARR TV

moodle

Consortium GARR THE ITALIAN EDUCATION & RESEARCH NETWORK

GARR Computing and Storage

Container platform

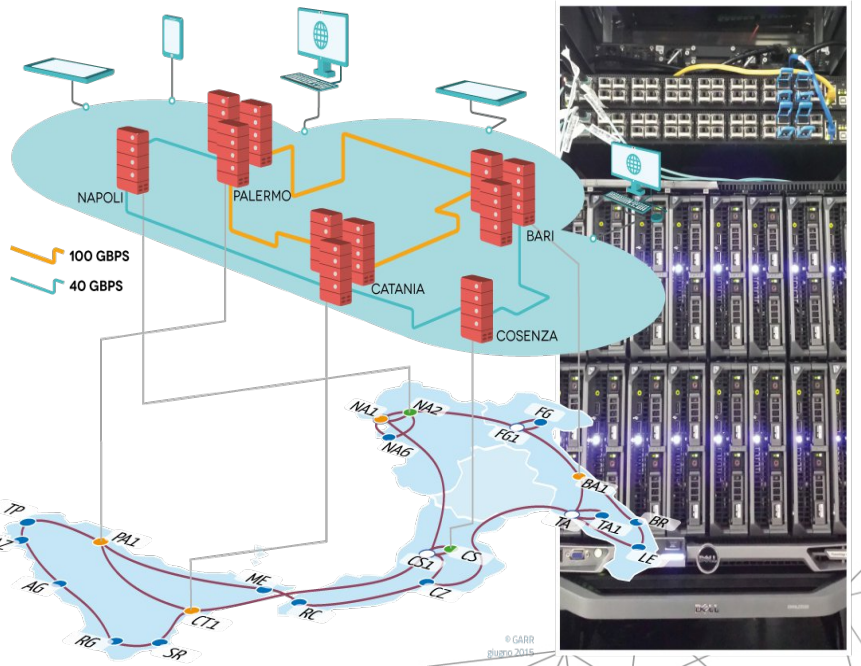
+ GPU inside

The engine

MAAS JUJU ceph

First users/projects

- virgo
- Univ. Milano-Bicocca
- garr-tv



Aim

Let user access GARR Cloud and Container platform using their single personal account

- GARR Cloud user access mainly via Federated authentication
  - IDEM/EduGAIN, OIDC
  - no basic keystone auth (local password)

-> use Keystone as external Identity provider for Kubernetes

  - WebHook token authentication
  - Joint work by GARR and SWITCH within GEANT project GN4-2

    (at GARR mainly by Roberto di Lallo)

SIG-OpenStack in Kubernetes

Changelogs in Kubernetes have a SIG-Openstack section! Heads up !

https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG-1.11.md

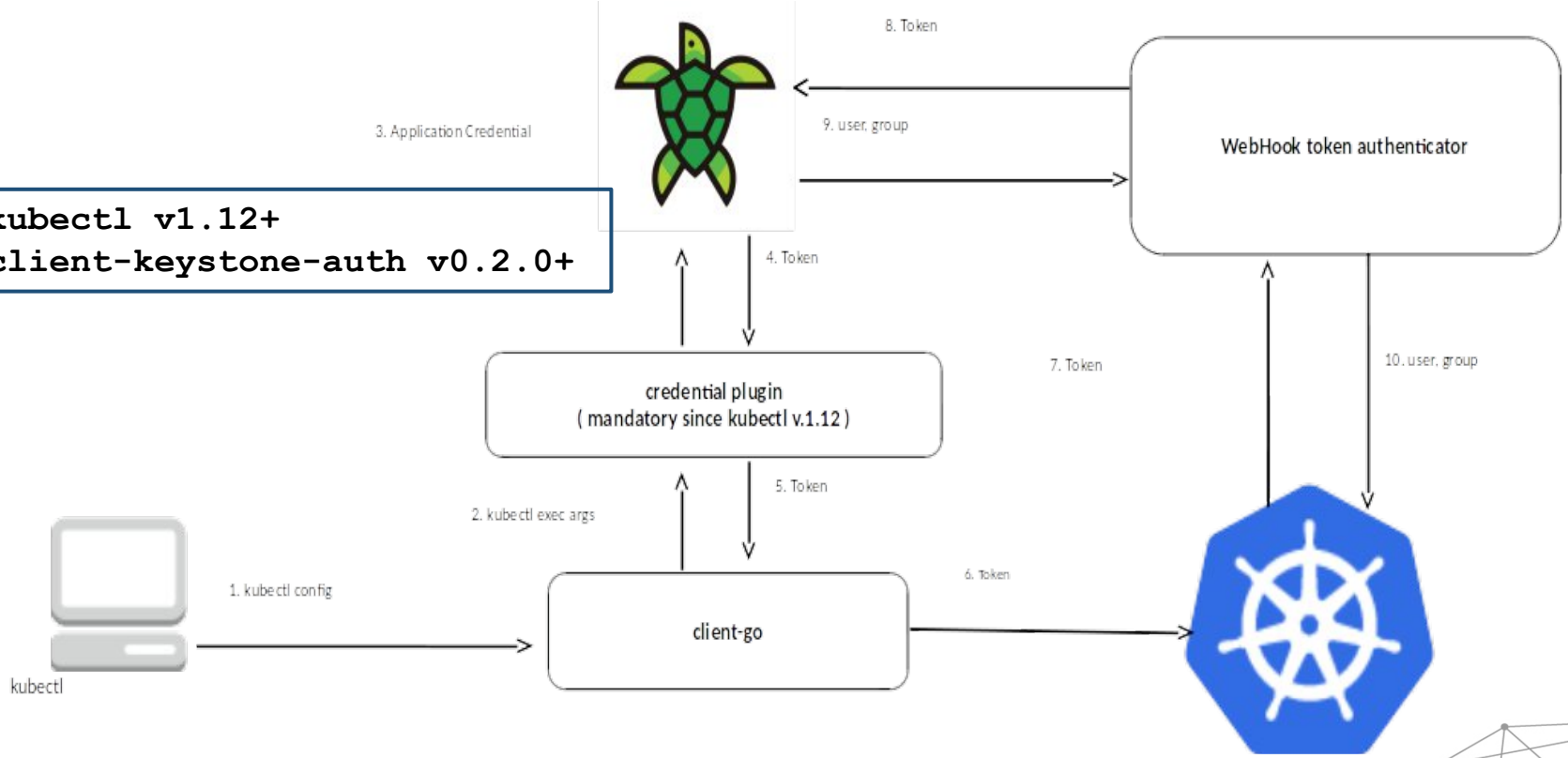
- OpenStack built-in cloud provider is now deprecated. Please use the external cloud provider for OpenStack. (#63524, @dims)

- In-tree support for OpenStack credentials is now deprecated. please use the "client-keystone-auth" from the cloud-provider-openstack repository. details on how to use this new capability is documented here (#64346, @dims)

https://github.com/kubernetes/cloud-provider-openstack/

SIG-OpenStack in Kubernetes

kubectl v1.12+
client-keystone-auth v0.2.0+



Don't use Opensource: ADOPT Opensource

Upstream merged patches by SWITCH and GARR

Get a token using Keystone Application Credential

- https://github.com/kubernetes/cloud-provider-openstack/pull/282

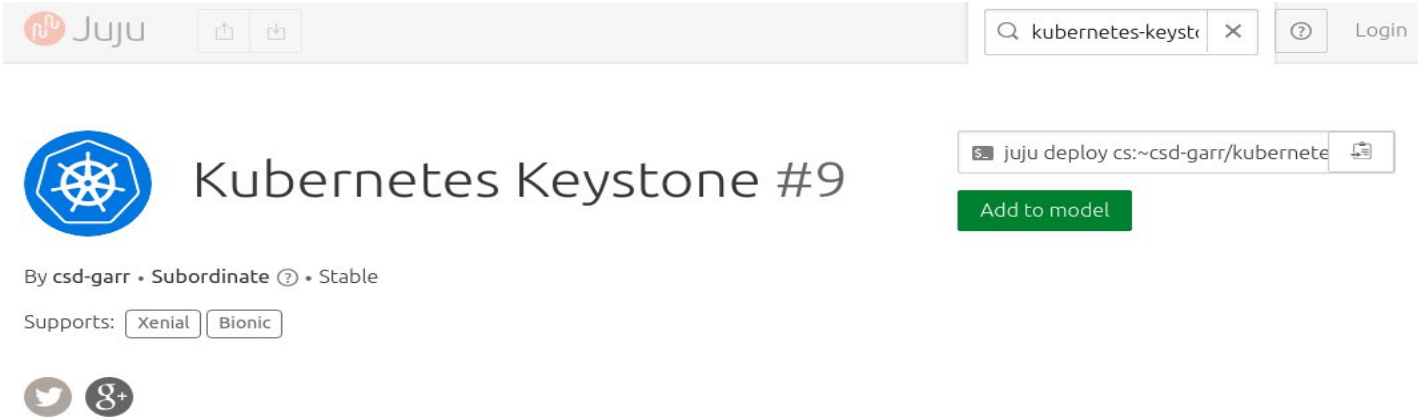
Gophercloud: Add support to authenticate with application credential

- https://github.com/gophercloud/gophercloud/pull/1224
- **(Does not implement CRUD functions)**

Integration on GARR Cloud

1. new Juju charm kubernetes-keystone

-> installs Webhook token authenticator on kubernetes-master



Integration on GARR Cloud

2. Application credentials

-> OpenStack release Rocky

3. OpenStack dashboard

-> Kubeconfig generator from Application Credentials

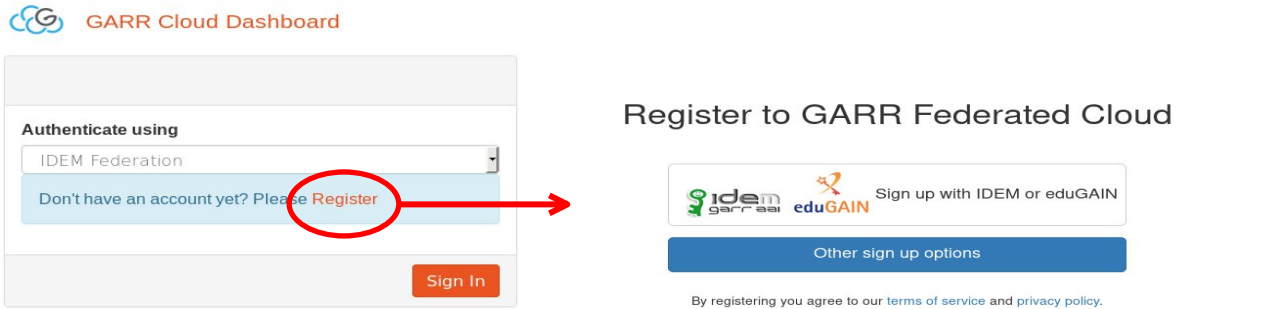
-> Patch to Horizon proposed: https://review.opendev.org/#/c/653794/

-> review in progress, contribute if you like it! :)

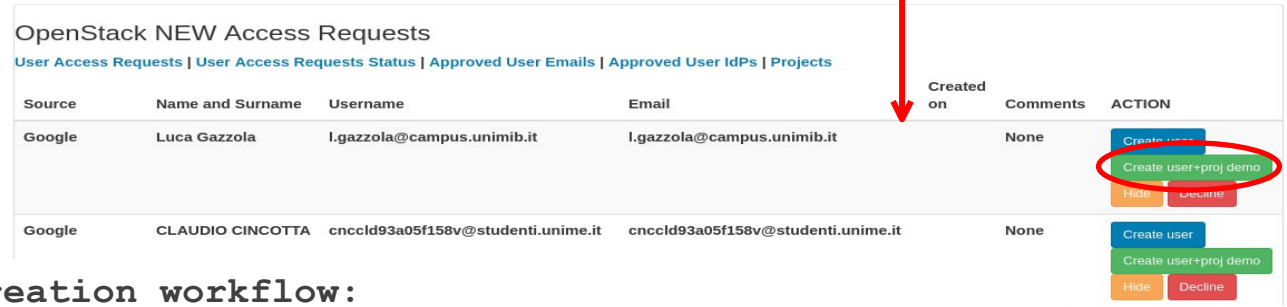
4. User account creation workflow automated

User account creation workflow

User requests account



Admin approves



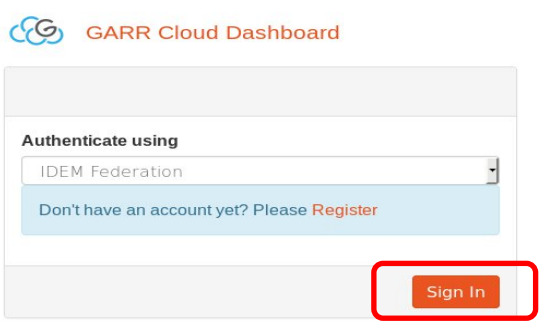
Approval triggers creation workflow:

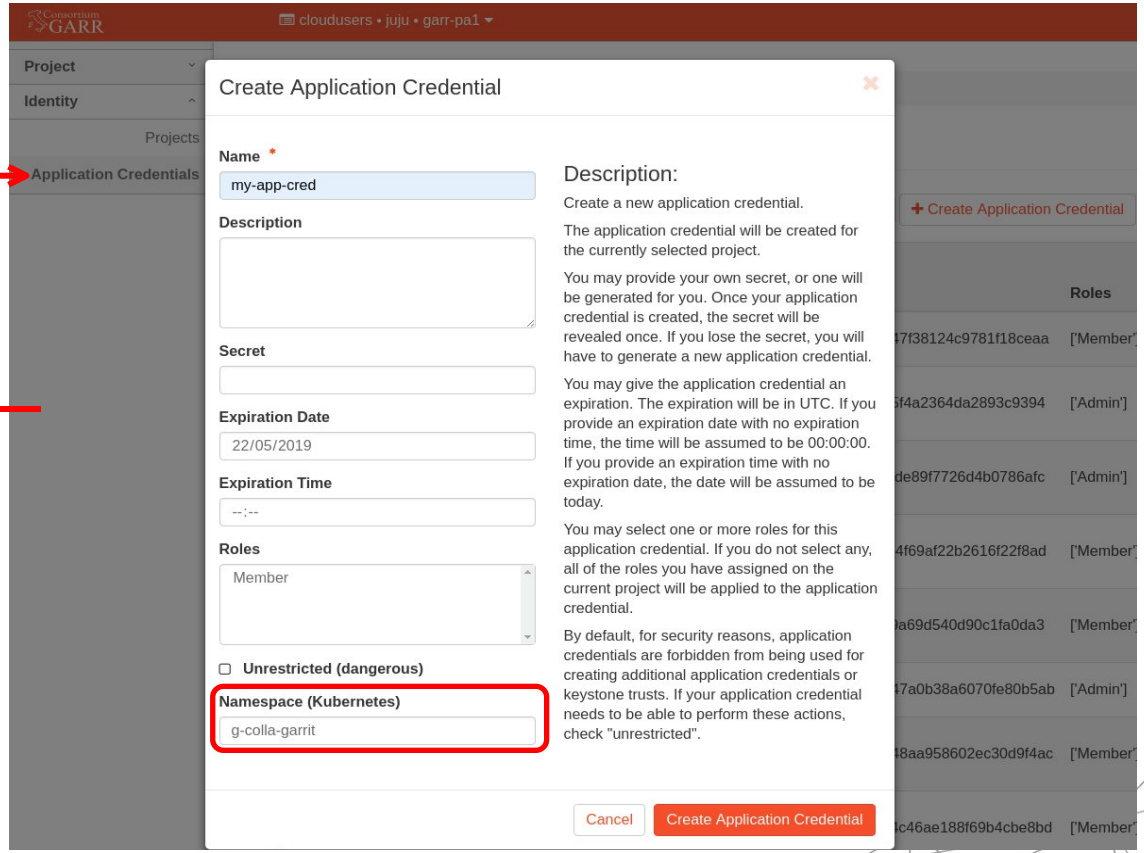
-> OpenStack: username, (garrdemo) project assignment

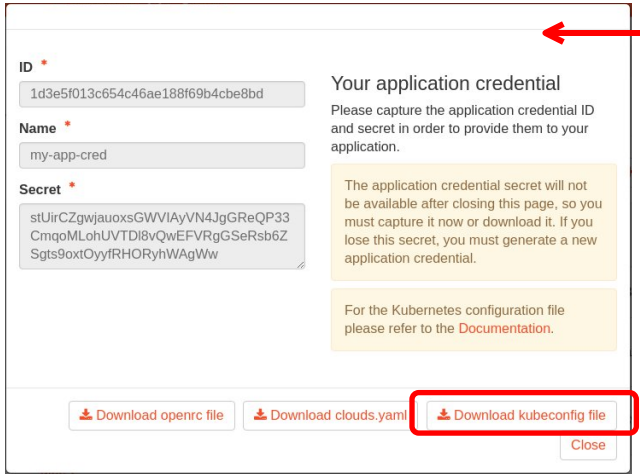
-> k8s: user namespace with quotas, bound to username

-> User notified by email

User access


GARR Cloud Dashboard
Authenticate using
IDEM Federation
Don't have an account yet? Please Register
Sign In


Consortium GARR
cloudusers • juju • garr-pa1
Project
Identity
Projects
Application Credentials
+ Create Application Credential
Roles
['Member']
['Admin']
['Admin']
['Member']
['Admin']
['Member']
['Member']
Create Application Credential
Name *
my-app-cred
Description
Secret
Expiration Date
22/05/2019
Expiration Time
--:--
Roles
Member
Unrestricted (dangerous)
Namespace (Kubernetes)
g-colla-garrit
Description:
Create a new application credential.
The application credential will be created for the currently selected project.
You may provide your own secret, or one will be generated for you. Once your application credential is created, the secret will be revealed once. If you lose the secret, you will have to generate a new application credential.
You may give the application credential an expiration. The expiration will be in UTC. If you provide an expiration date with no expiration time, the time will be assumed to be 00:00:00. If you provide an expiration time with no expiration date, the date will be assumed to be today.
You may select one or more roles for this application credential. If you do not select any, all of the roles you have assigned on the current project will be applied to the application credential.
By default, for security reasons, application credentials are forbidden from being used for creating additional application credentials or keystone trusts. If your application credential needs to be able to perform these actions, check "unrestricted".
Cancel
Create Application Credential


ID *
1d3e5f013c654c46ae188f69b4cbe8bd
Name *
my-app-cred
Secret *
stUirCZgwjauoxsGWVIAyVN4JgGReQP33
CmqoMLohUVTDl8vQwEFVRgGSeRsb6Z
Sgts9oxtOyyfRHORyhWAgWw
Your application credential
Please capture the application credential ID and secret in order to provide them to your application.
The application credential secret will not be available after closing this page, so you must capture it now or download it. If you lose this secret, you must generate a new application credential.
For the Kubernetes configuration file please refer to the Documentation.
Download openrc file
Download clouds.yaml
Download kubeconfig file
Close

Kubeconfig

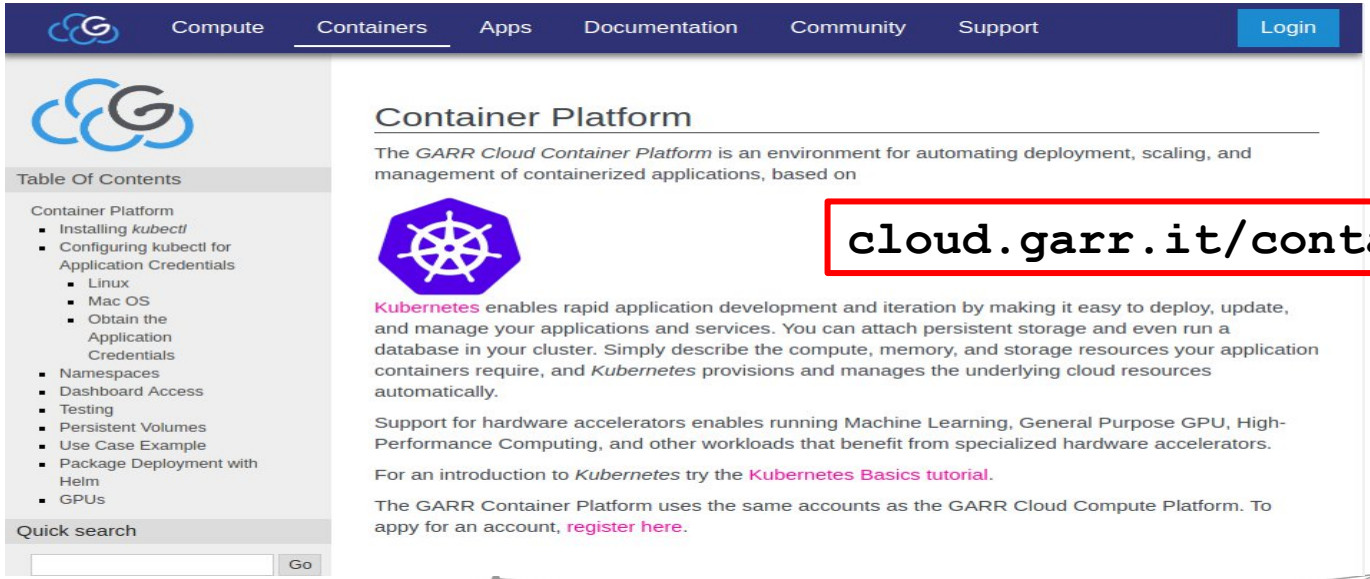
```
apiVersion: v1
kind: Config
clusters:
- name: kubernetes
  cluster:
    server: "https://k8s-api-pa1.cloud.garr.it:443"
    certificate-authority-data:
contexts:
- name: kubernetes
  context:
    cluster: kubernetes
    user: colla@garr.it
    namespace: g-colla-garrit
current-context: kubernetes
```

Kubeconfig (Cont'd)

```
users:
  - name: colla@garr.it
    user:
      exec:
        apiVersion: client.authentication.k8s.io/v1beta1
        command: bin/kubectl-keystone-auth
        args:
        - "--keystone-url=https://keystone.cloud.garr.it:5000/v3"
        - "--domain-name=none"
        - "--user-name=colla@garr.it"
        - "--application-credential-id=f394734..."
        - "--application-credential-secret=XXXXXXX"
```

Kubernetes user access

- Download kubeconfig file in ~/.kube/config
- Download keystone auth plugin (git@GARR) in ~/.kube/bin/kubectl-keystone-auth
- Install kubectl... and work!



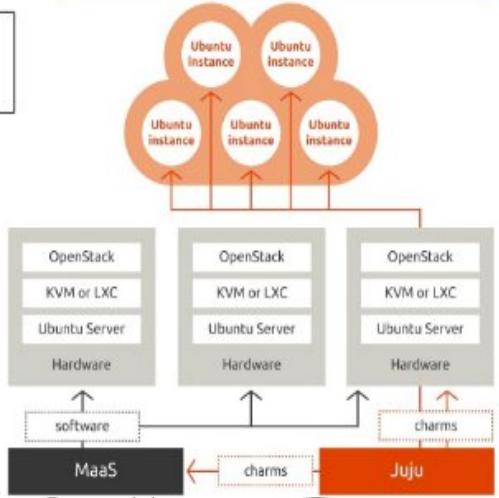
DaaS (deployment as a Service)

more powerful than a PaaS, easier than a IaaS

Frontend UI/CLI

Juju with cloud OpenStack

backend



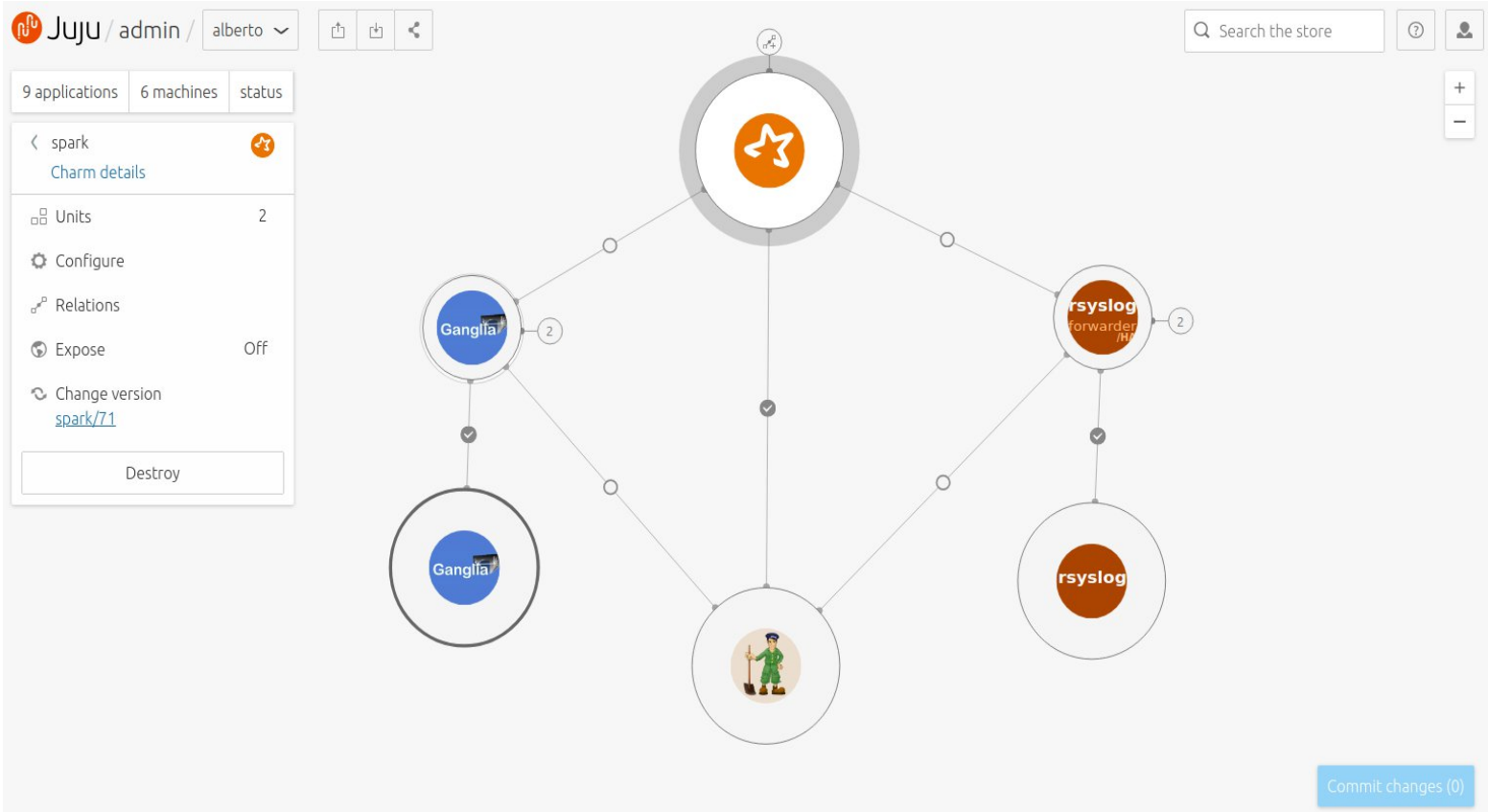
=

DaaS

GARR Cloud

https://daas.cloud.garr:17070

https://daas-pa.cloud.garr.it



multi-region (OpenStack) model

Region:
has its **own deployment** of OpenStack

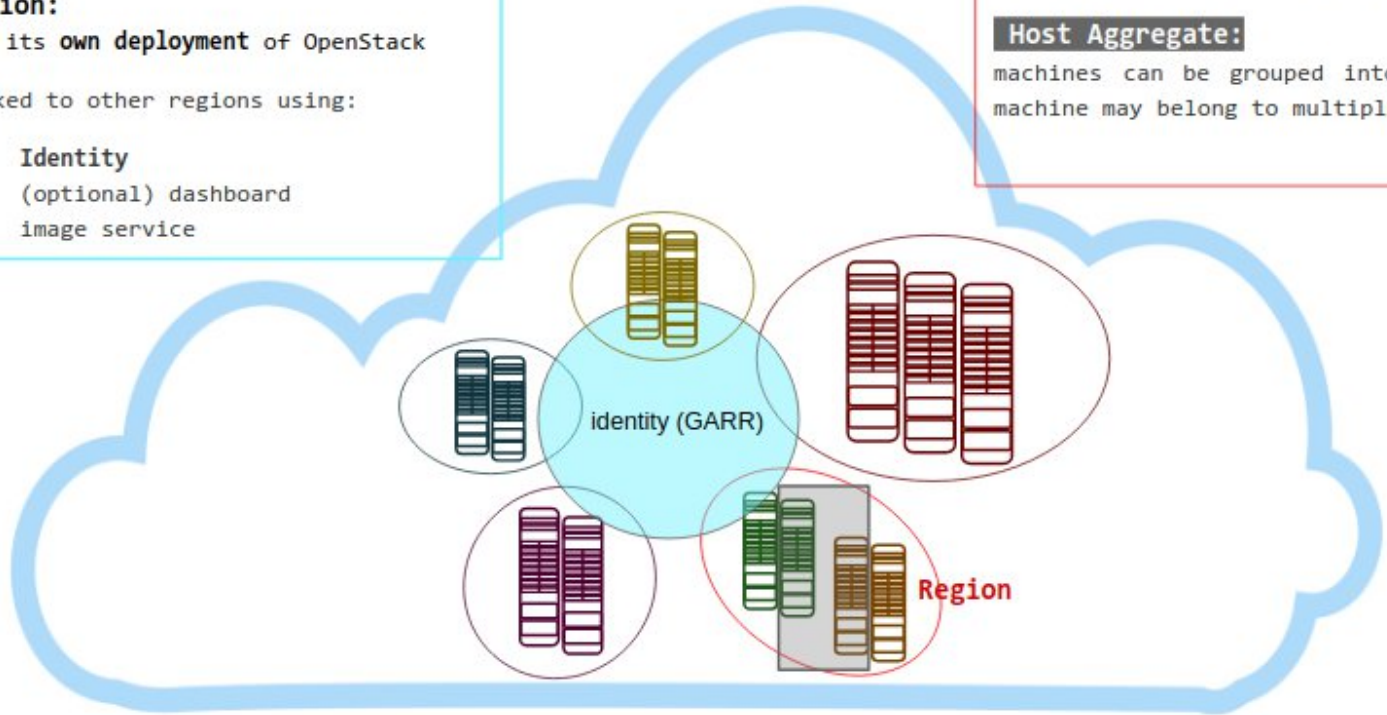
linked to other regions using:

- **Identity**
- (optional) dashboard
- image service

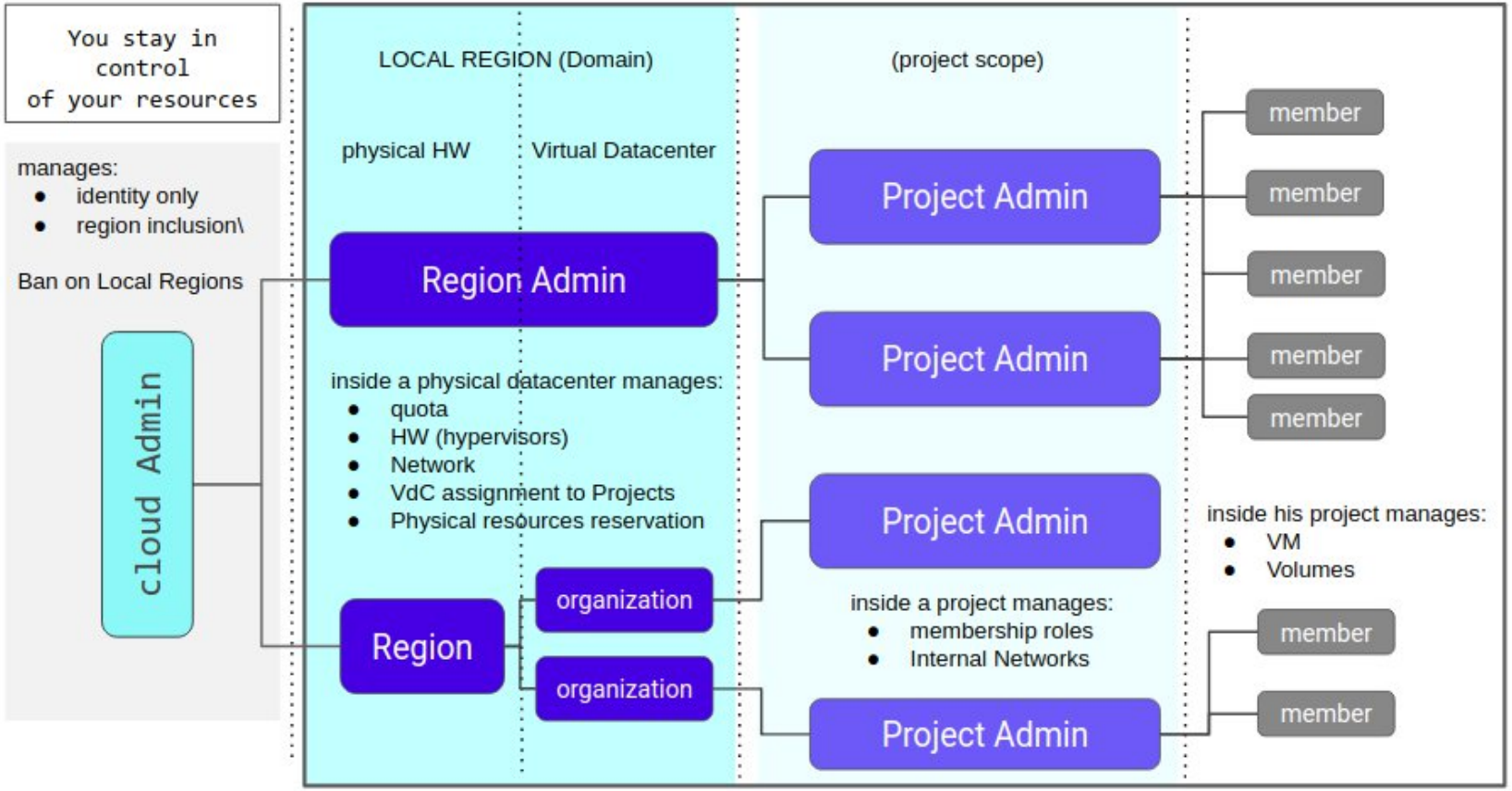
Inside a Region: advanced scheduling

Availability Zone:
nodes can be logically grouped into Availability Zones (AZ) and reserved to projects.

Host Aggregate:
machines can be grouped into Host aggregates. A machine may belong to multiple Host aggregates.



Delegation of authority (via domains, policy and metadata filters)



GARR Workplace

- Based on OnlyOffice, a web based office suite
- Features:
  - document editing
    - text, presentations, spreadsheets
  - file management
  - project management
    - task, milestones, discussions, timesheets, GANTT diagrams
  - customer relationship management (CRM)
    - contacts, sales, invoices
  - communication
    - e-mail, chat, blog, events

GARR Workplace

- OnlyOffice licensing, mainly:
  - community edition
    - AGPL license - free
    - 20 concurrent document editor connections maximum
  - enterprise edition
    - 50, 100, 200 concurrent connections

GARR Workplace

- since October 2018
- 3 production instances
  - community edition (open source)
- ~150 users

Further notes

- OpenStack Release upgrade
  - Queens -> Rocky requires Xenial -> Bionic
- Accounting
  - Ceilometer + Gnocchi, testing in progress
- Ceph
  - upmap balancing (2% spread disk occupancy)
- Renew / Expand hardware
  - Increase SSD, capacity
  - dismiss FiberChannel
  - add GPUs (deep-learning oriented)

Thank you!

Consortium GARR

THE ITALIAN EDUCATION & RESEARCH NETWORK