Integrating OpenStack and Kubernetes

ALBERTO COLLA / GARR
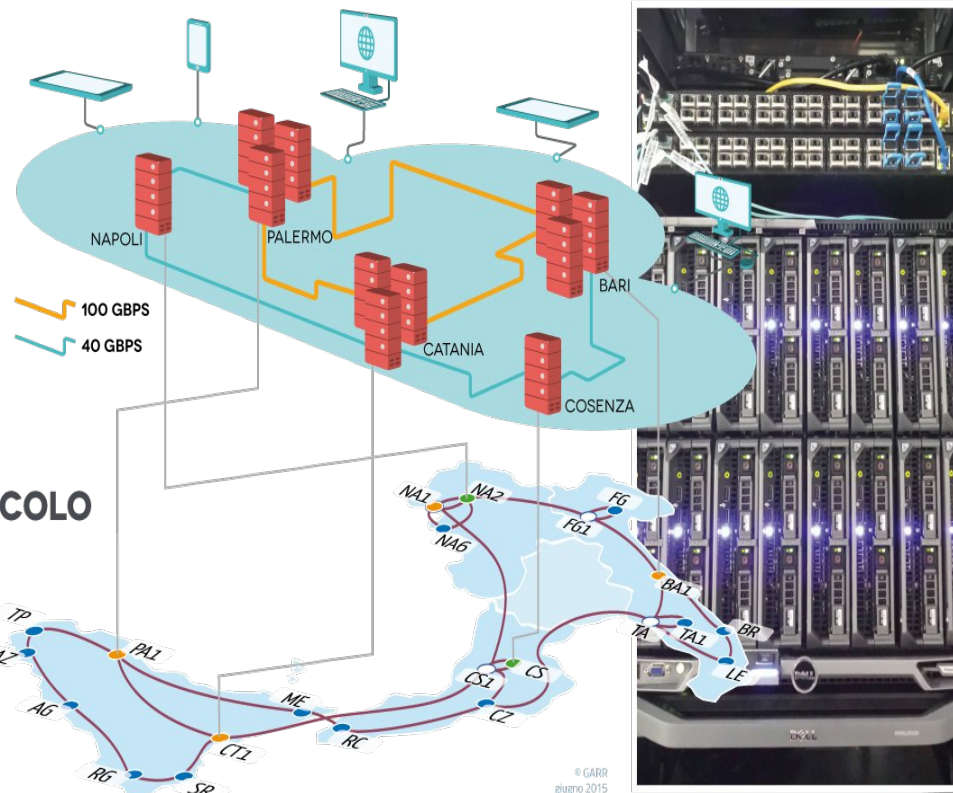
Saverio Proto / SWITCH

CERN, May 27, 2019
OpenStack Day CERN

GARR Computing and Storage

INFRASTRUTTURA DI CALCOLO
E STORAGE DISTRIBUITO

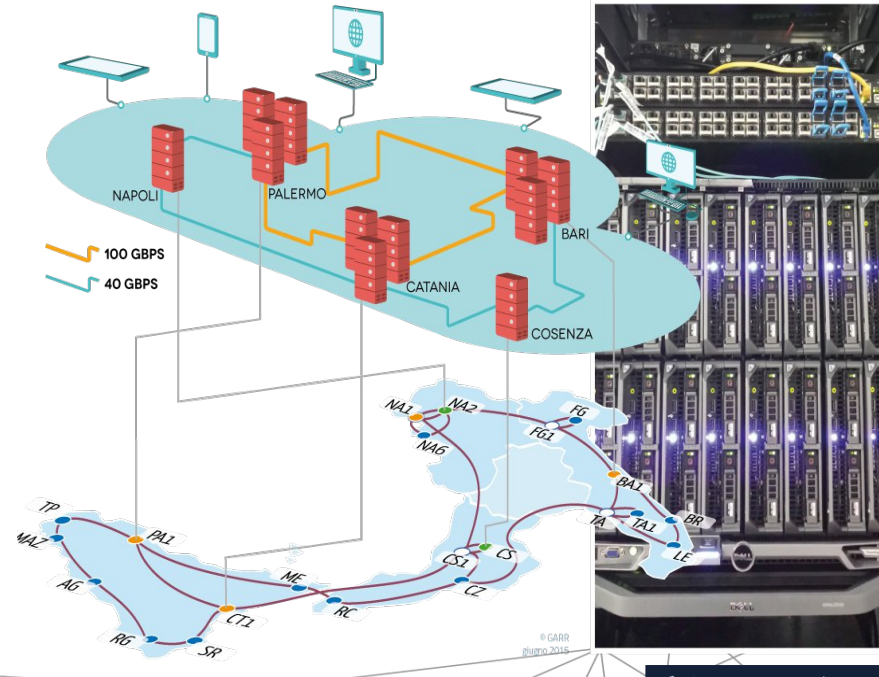- 5 siti distribuiti
- 8.448 virtual CPU
- 10 PB spazio storage

100 GBPS
40 GBPS

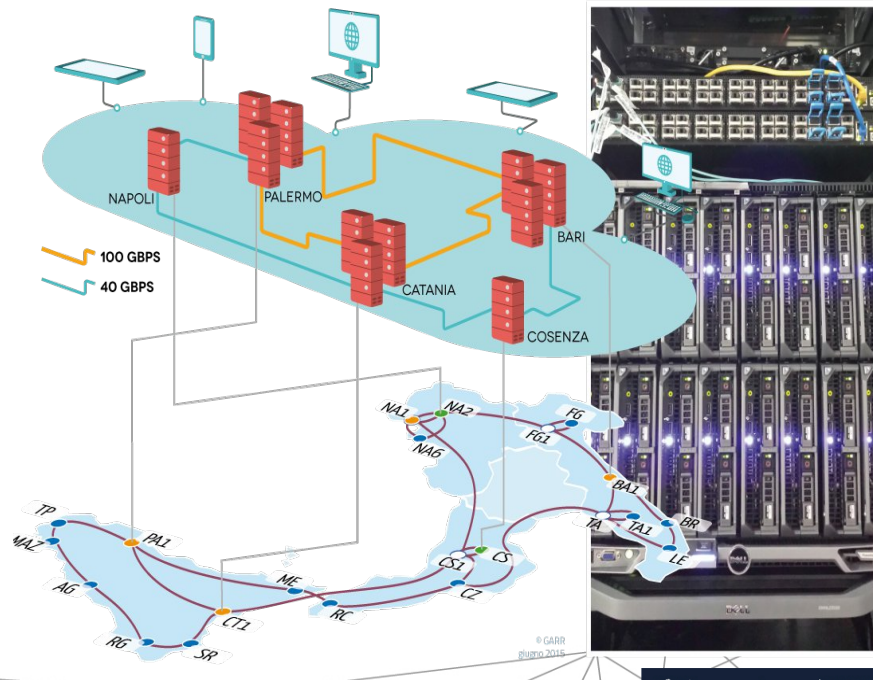# GARR Computing and Storage

The engine
MAAS   JUJU   ceph

GARR Computing and Storage

GARR cloud

Powered by openstack.

The engine

MAAS   JUJU   ceph

100 GBPS
40 GBPS

NAPOLI   PALERMO   BARI   CATANIA   COSENZA

GARR Computing and Storage

GARR cloud

Powered by openstack

The engine

MAAS   JUJU   ceph

600 Users

1100 VM

3500 vCPU 9 TB_RAM

1 PB_storage 850 IP

100 GBPS
40 GBPS

Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK

GARR Computing and Storage

GARR cloud

Powered by openstack

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

Container platform

Powered by kubernetes
+ GPU inside

The engine

MAAS   JUJU   ceph

Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK
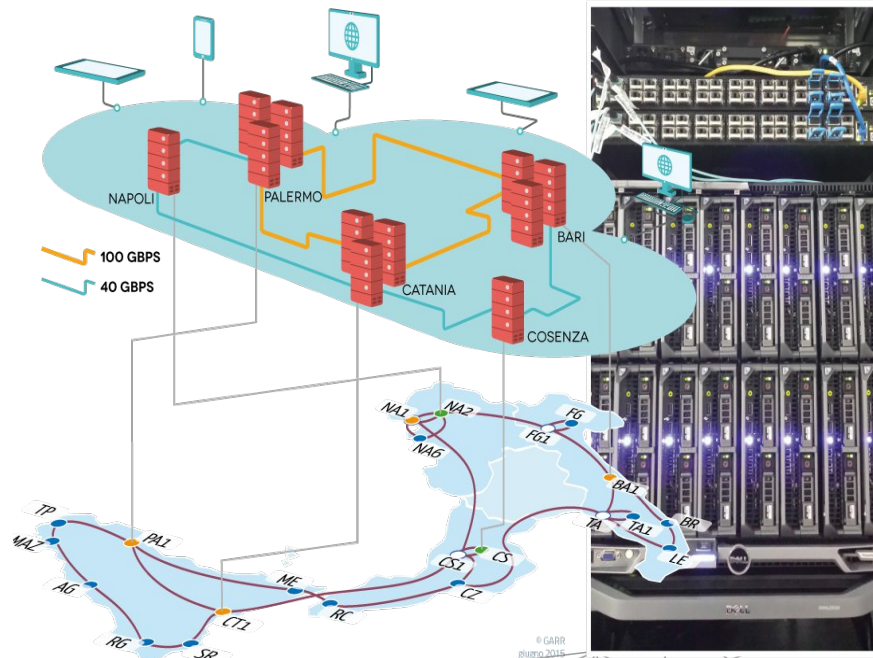
Aim

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
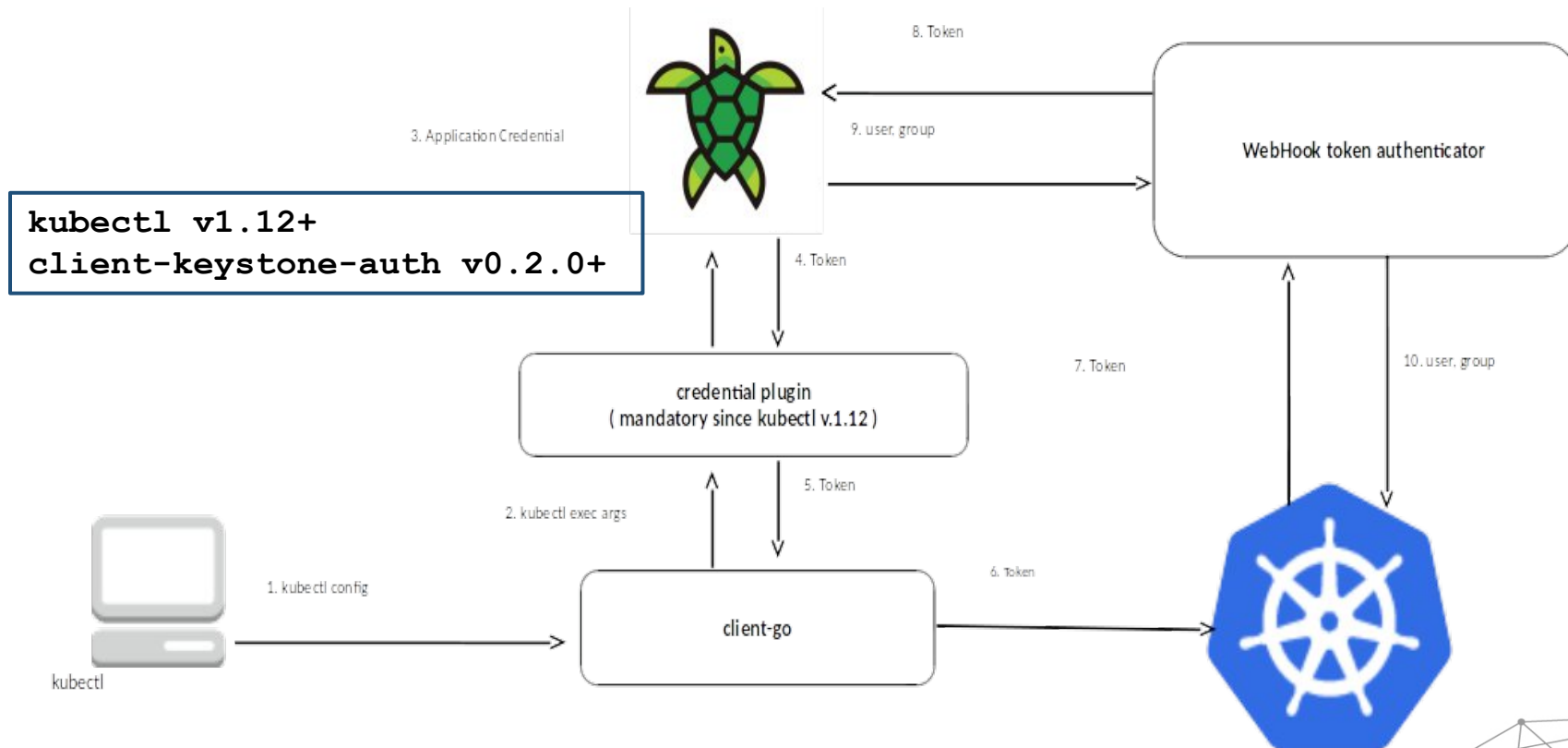
    (at GARR mainly by Roberto di Lallo)

Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK

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/

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

8. Token

9. user, group

WebHook token authenticator

3. Application Credential

4. Token

7. Token

10. user, group

credential plugin
(mandatory since kubectl v.1.12)

2. kubectl exec args

5. Token

1. kubectl config

6. Token

client-go

kubectl

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**
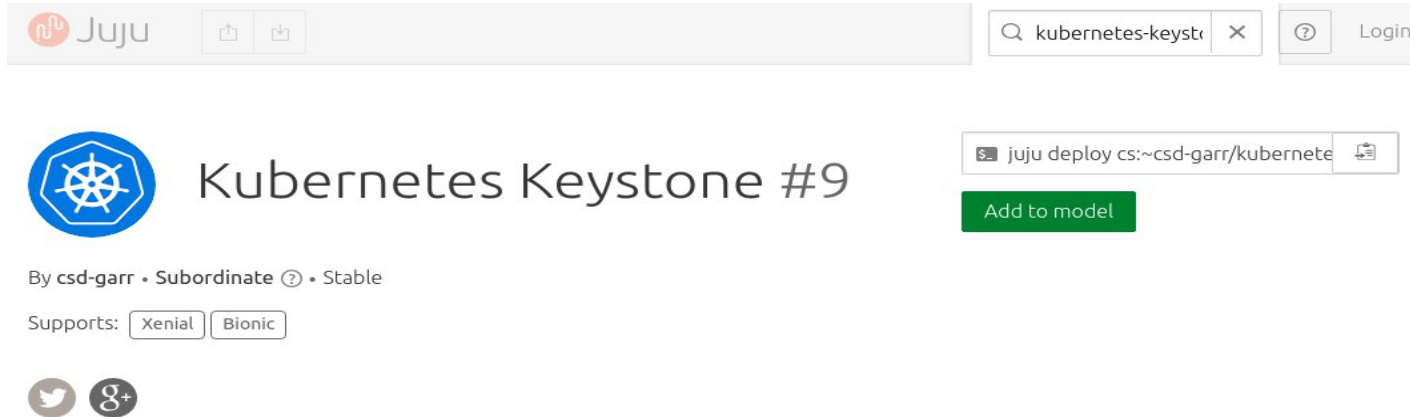
- **(Does not implement CRUD functions)**

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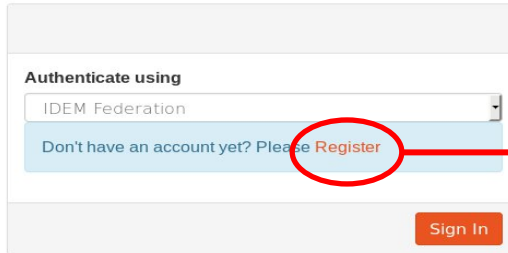
-> review in progress, **contribute if you like it! :)**

4. User account creation workflow automated
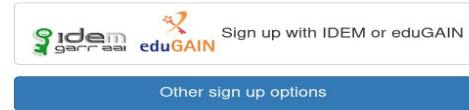
User account creation workflow

User requests account

GARR Cloud Dashboard

Authenticate using

IDEM Federation

Don't have an account yet? Please Register

Sign In

Register to GARR Federated Cloud

Sign up with IDEM or eduGAIN

Other sign up options

By registering you agree to our terms of service and privacy policy.

Admin approves

OpenStack NEW Access Requests

User Access Requests | User Access Requests Status | Approved User Emails | Approved User IdPs | Projects

Source	Name and Surname	Username	Email	Created on	Comments	ACTION
Google	Luca Gazzola	l.gazzola@campus.unimib.it	l.gazzola@campus.unimib.it		None	Create user / Create user+proj demo / Hide / Decline
Google	CLAUDIO CINCOTTA	cnccld93a05f158v@studenti.unime.it	cnccld93a05f158v@studenti.unime.it		None	Create user / Create user+proj demo / Hide / Decline

Approval triggers creation workflow:

-> OpenStack: username, (garrdemo) project assignment

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

-> User notified by email

Consortium GARR — THE ITALIAN EDUCATION & RESEARCH NETWORK

User access

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
```

Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK

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!**

cloud.garr.it/containers

Thank you!