Laboratorio

Paolo Veronesi, Enrico Fattibene, Fabio Capannini

Formazione Cloud@CNAF
13/6/2014

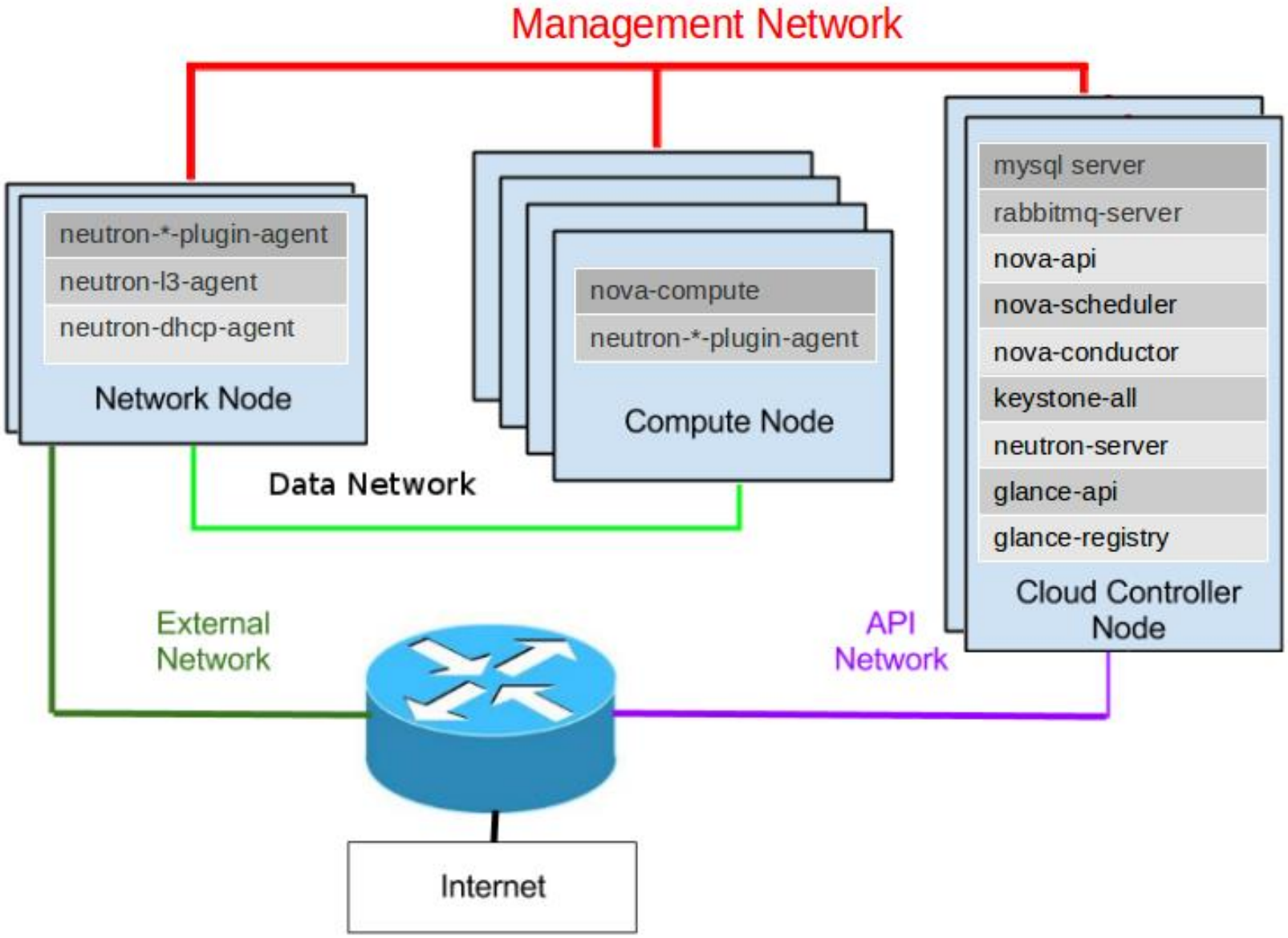
Sommario

- Panoramica della dashboard
- Demo basic via dashboard
- Demo advanced via command line: multi tier app
  - Questa parte del lab e' stata riadattato prendendo come spunto **Neutron Hands on Lab** (http://bit.ly/1cFKPoV)

Scopo del laboratorio

- Basic: Prendere familiarita' con la dashboard
- Advanced: prendere familiarita' con le api
  - Ogni utente arrivera' a costruire un ambiente multi tier con una applicazione web in load balancing
  - Comandi passo passo in https://gist.github.com/fabiok/e8fcc717de738240eec5
- Viene usata l'infrastruttura Cloud@CNAF, basata su OpenStack Havana con le seguenti caratteristiche:
  - Per-Tenant router con reti private
  - LBaaS abilitato

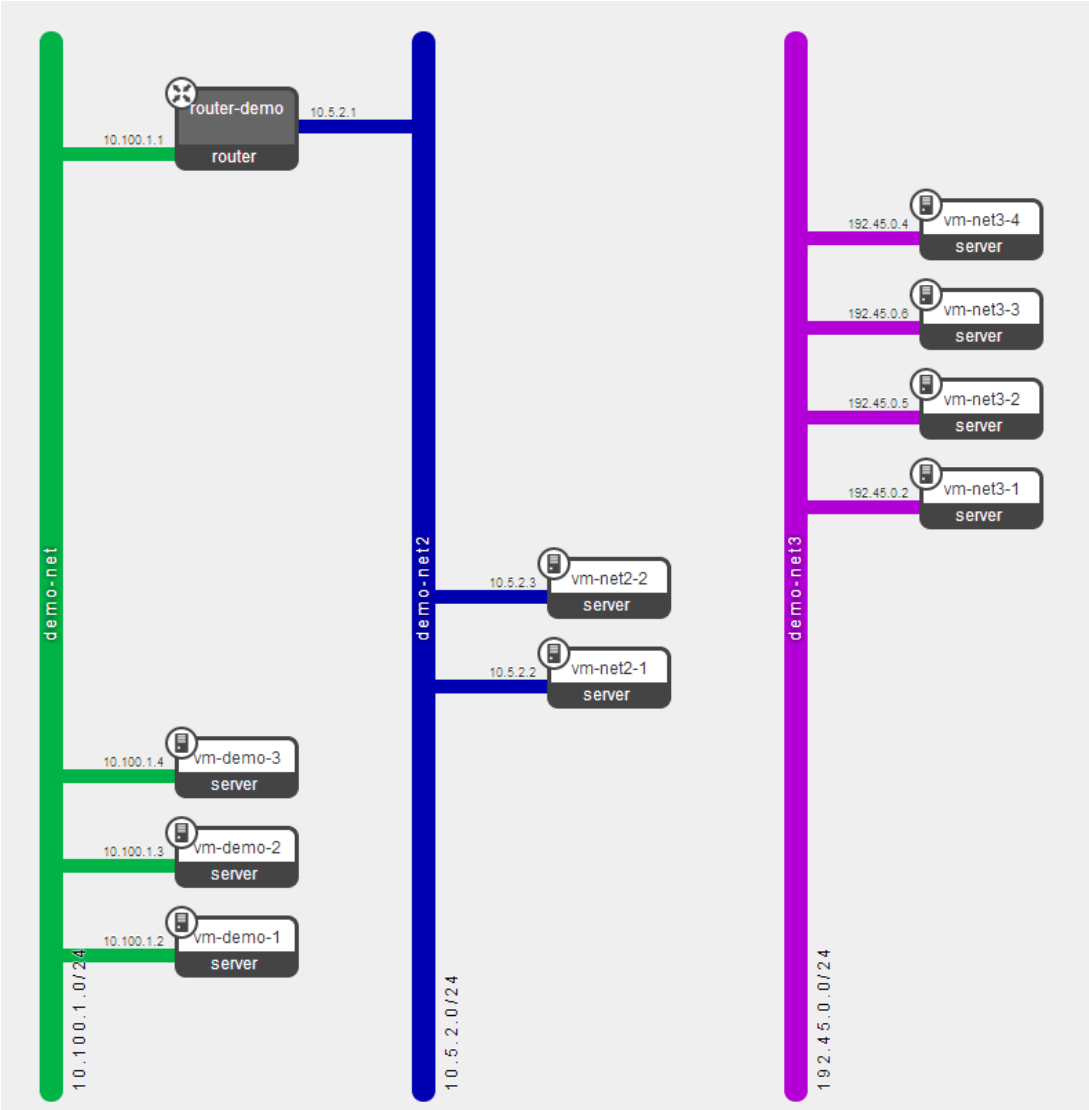
Infrastruttura



Tipologie di rete (1/3)

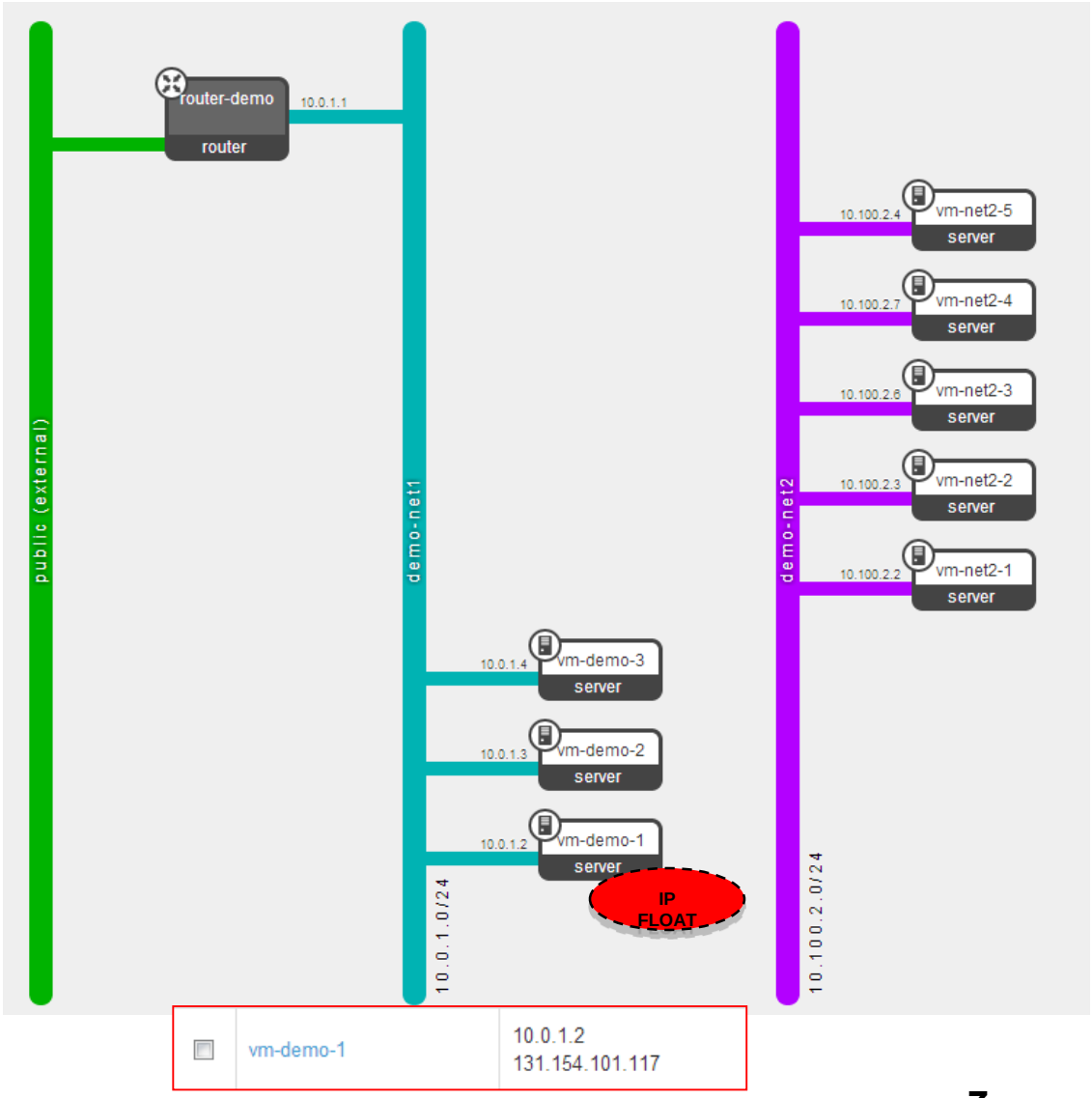
- Private Tenant Network
  - All'interno di ogni progetto (Tenant), gli utenti possono creare una o piu' reti private e uno o piu' apparati di rete (router) con cui connettere le reti in vario modo.
  - La definizione delle reti in ogni tenant non richiede l'intervento di un amministratore dell'infrastruttura ed e' garantito l'isolamento delle VM sia tra progetti diversi che tra reti diverse all'interno dello stesso progetto.
  - Le VM possono (o meno) avere outbound connectivity (Masquerade NAT), ma non sono raggiungibili dall'esterno se non hanno un floating IP assegnato (vedi slide successive).

Private Tenant Network



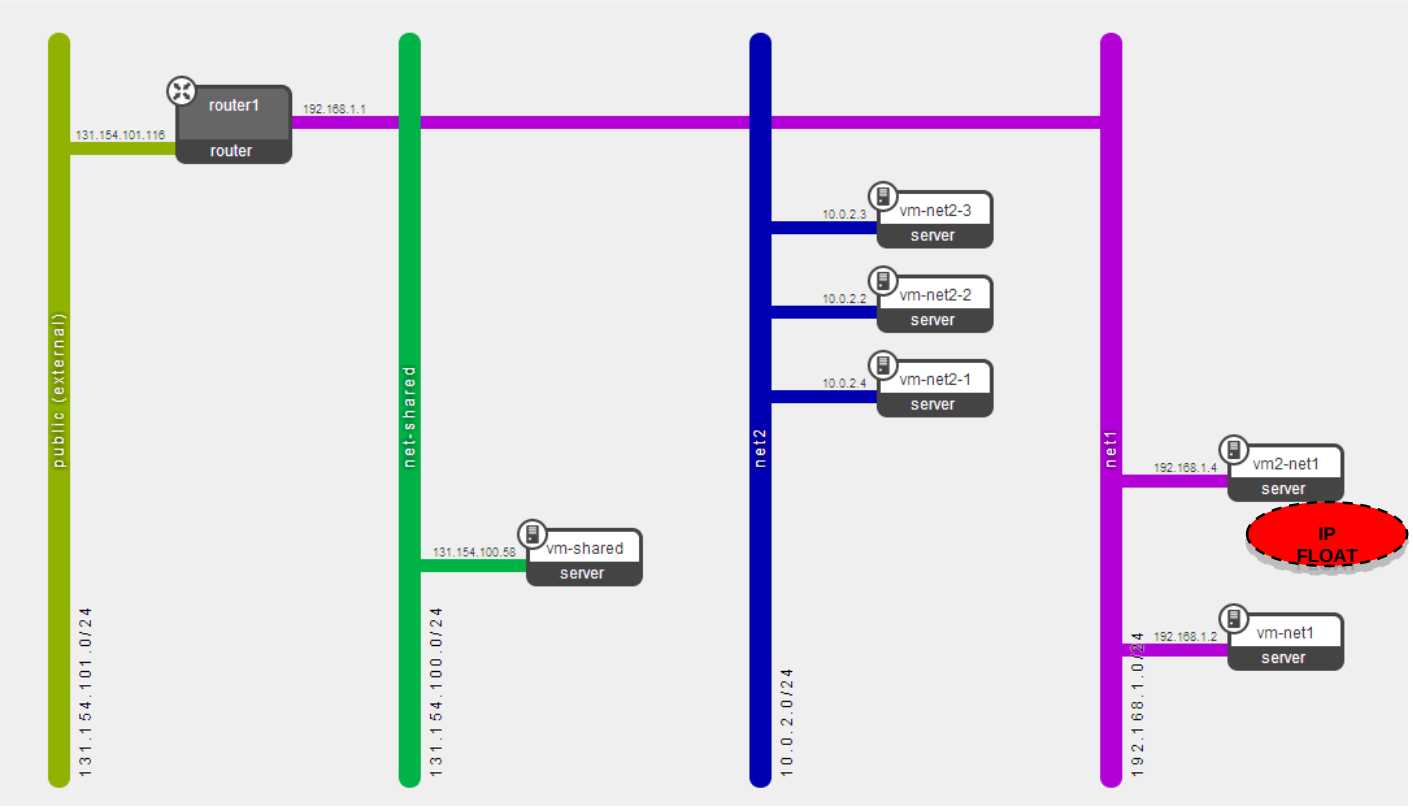
Tipologie di rete (2/3)

- External Network
  - Tipologia di rete necessaria per assegnare floating IP a VM istanziate sulle Private Tenant Network e renderle quindi accessibili via NAT dall'esterno.
  - Le reti External sono condivise tra tutti i progetti e definite dall'amministratore dell'infrastruttura.
  - Le VM non possono partire con un ip assegnato su una rete External, deve esistere una rete Private.
- Workflow
  - L'utente crea una rete privata
  - L'utente crea un router che connette la rete External con la rete privata
  - L'utente fa partire una VM sulla rete privata a cui assegna anche un floating IP
  - La VM ha due IP: uno privato e uno pubblico



Tipologie di rete (3/3)

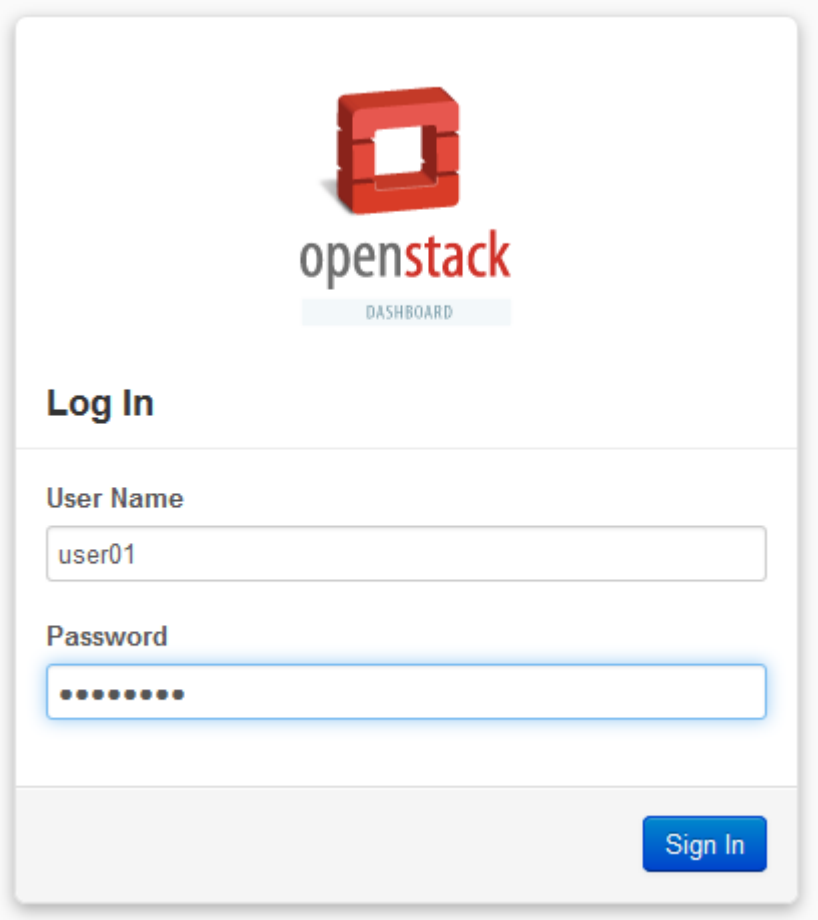
- Shared Network
- La shared network e' una tipologia di rete attraverso la quale si mette a disposizione dell'infrastruttura OpenStack una rete esistente nel centro di calcolo per poter creare delle VM sulla rete stessa.
- Le VM possono essere instanziate sulla rete shared, l'IP viene loro fornito da un DHCP esterno.
- Le policy della rete shared non sono gestite da OpenStack. No NAT a nessun livello.



Connessione alla dashboard

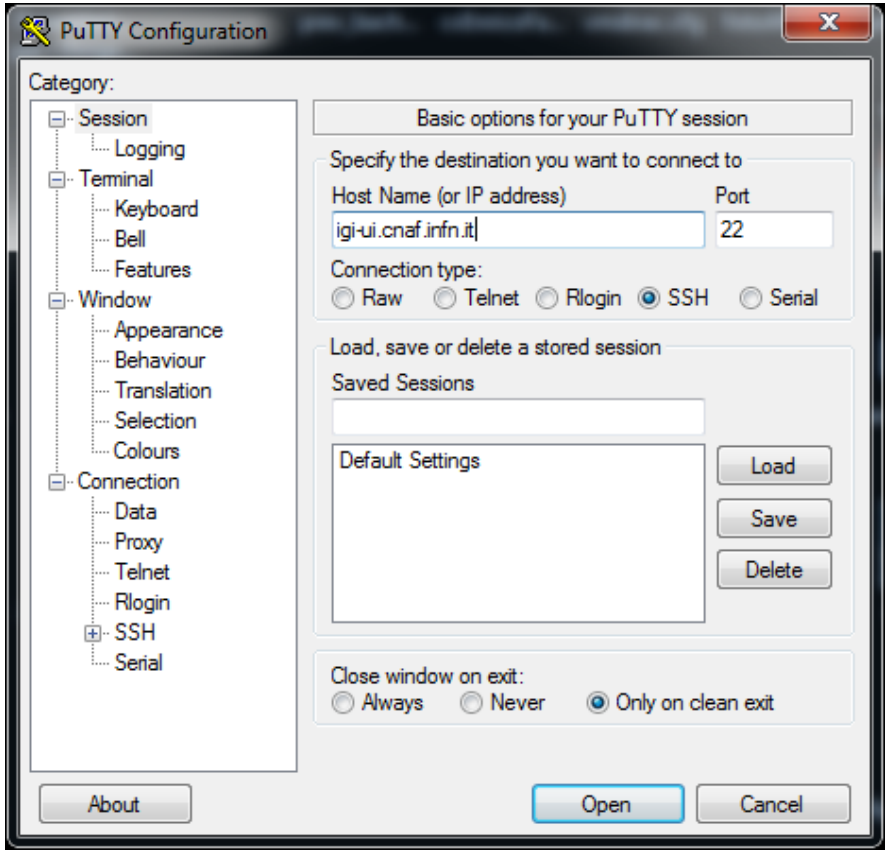
Dashboard via web:

https://cloudctrl02.cloud.cnaf.infn.it/dashboard



Connessione alla UI

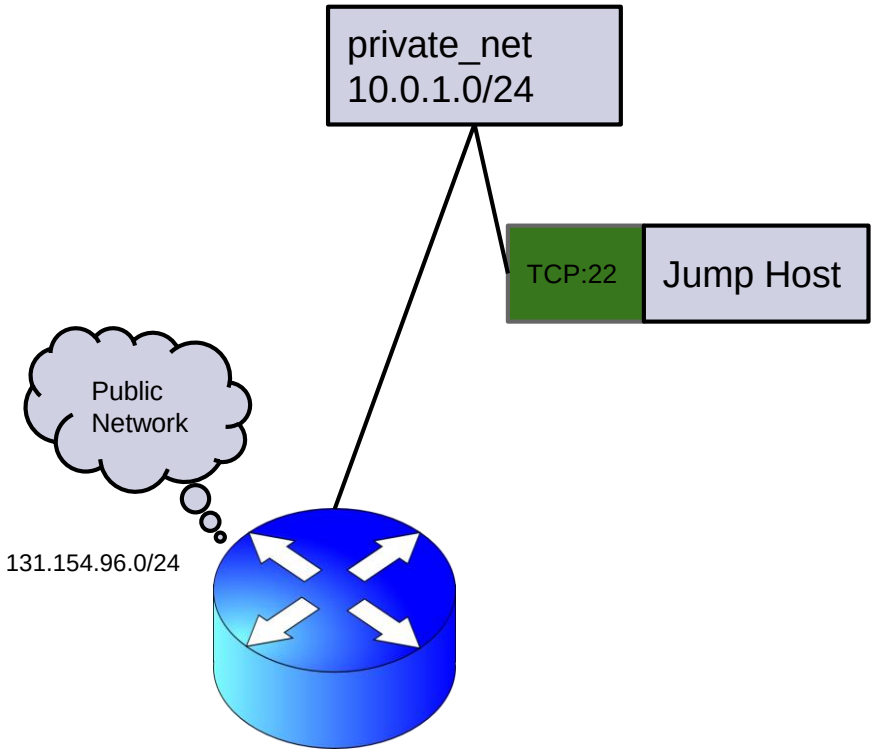
UI di riferimento (ad es. igi-ui.cnaf.infn.it)



Panoramica della dashboard

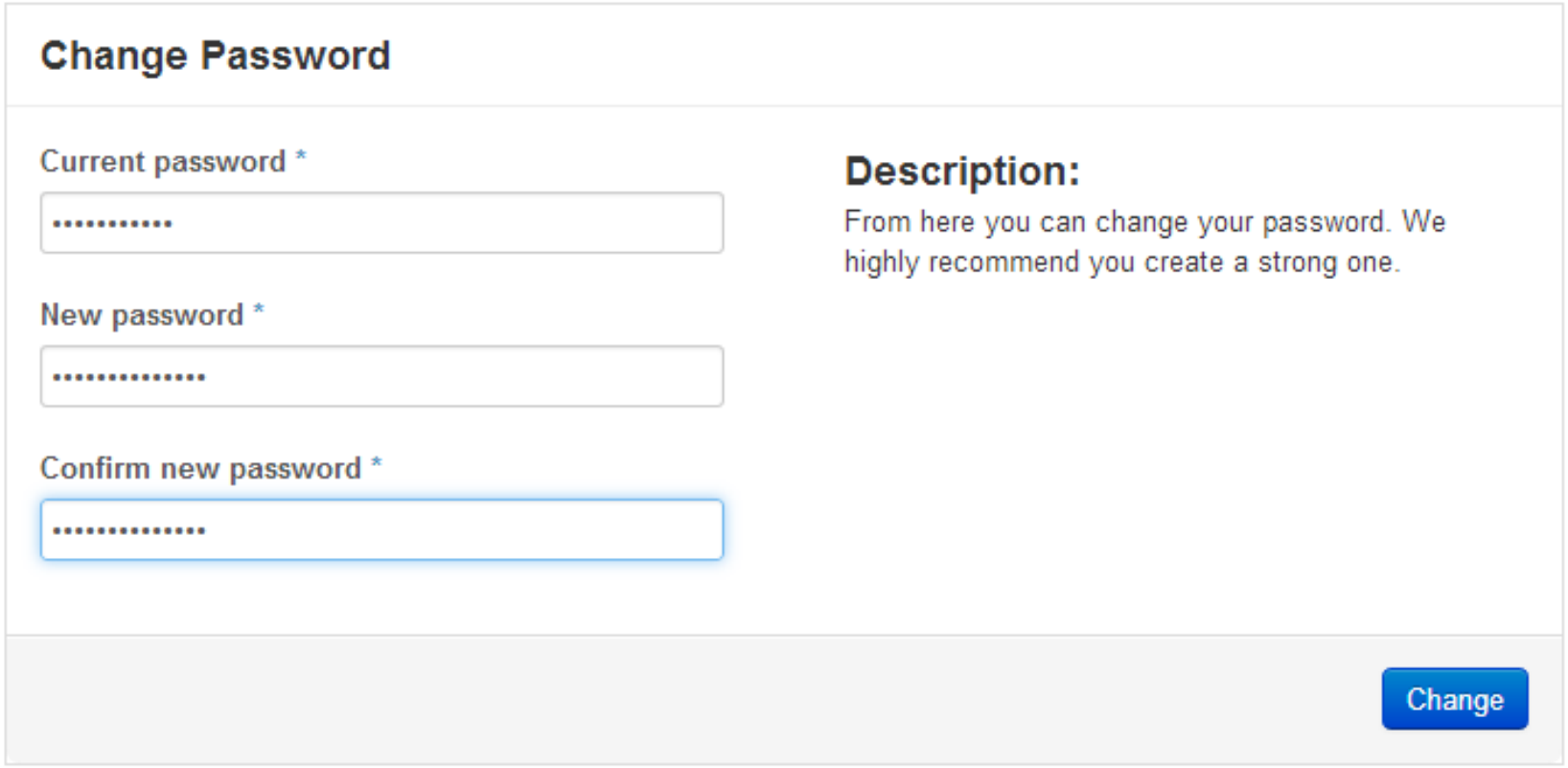
- Reti
  - Creazione di una rete privata con sottorete e router
- Security groups
  - Creazione di security group
  - Definizione di regole in security group
- Instanze
  - Creazione di una VM
  - Operazioni sulla VM
- Floating IP
  - Assegnazione di floating IP al progetto
  - Assegnazione di floating IP alla VM

Demo parte I - basic



Cambio password

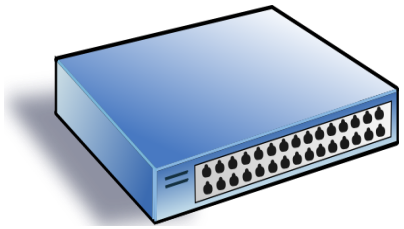
keystone password-update

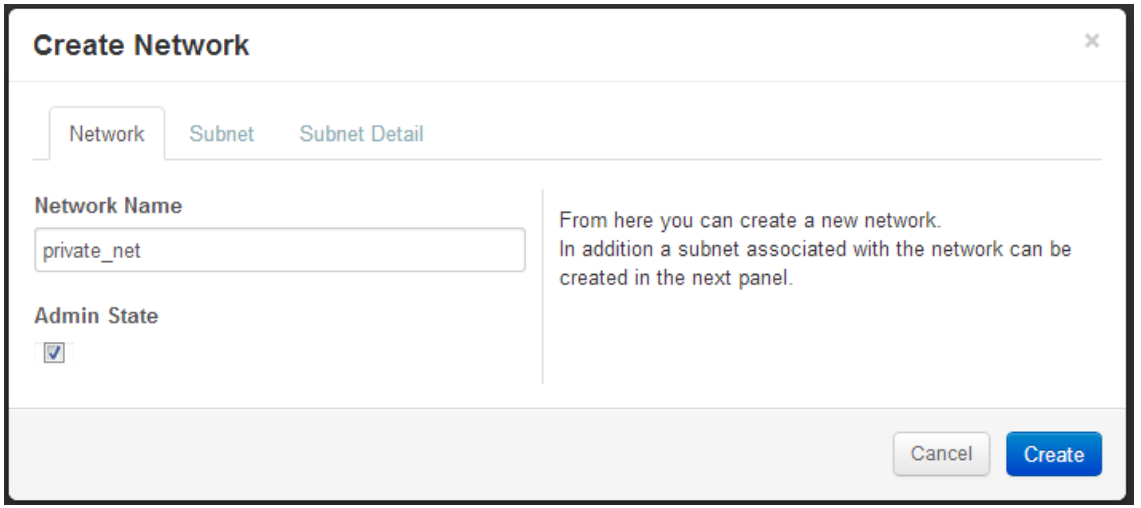


Creazione di rete privata

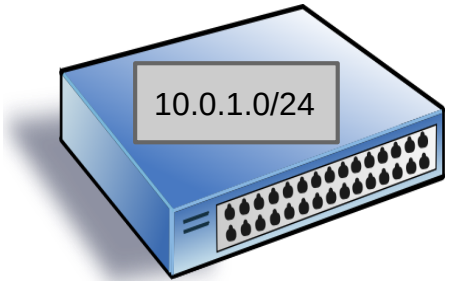
neutron net-create private_net

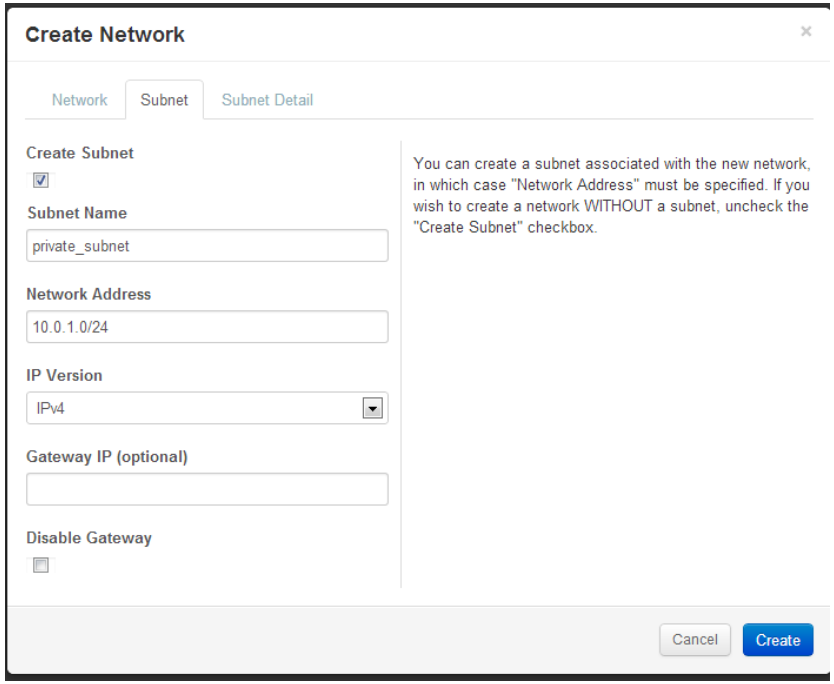
Creazione di una rete privata





neutron subnet-create --name private_subnet private_net 10.0.1.0/24

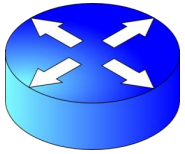


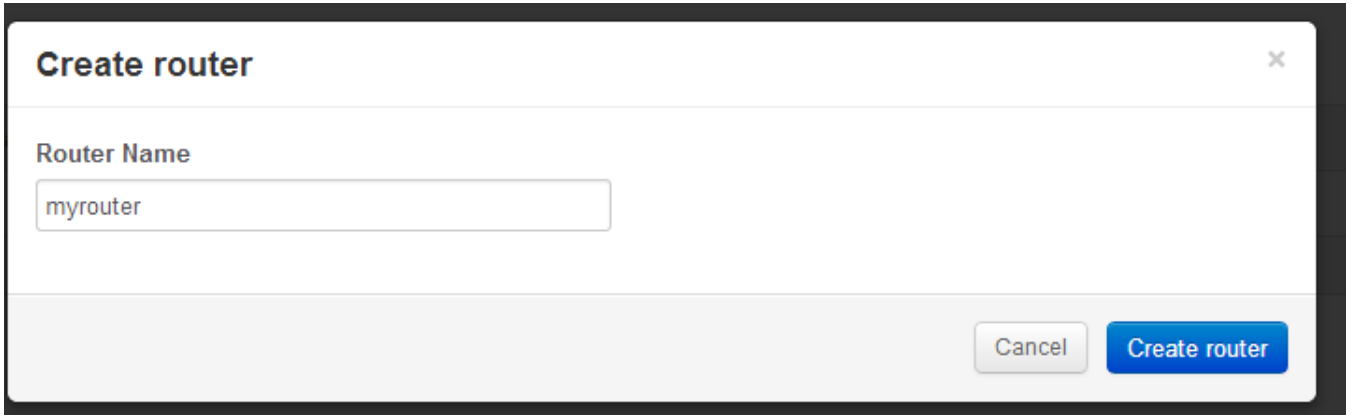


Creazione di un router

neutron router-create myrouter

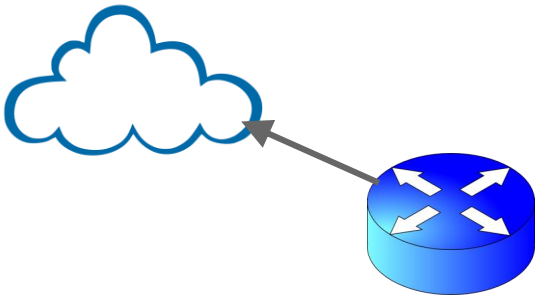
Creazione di un router

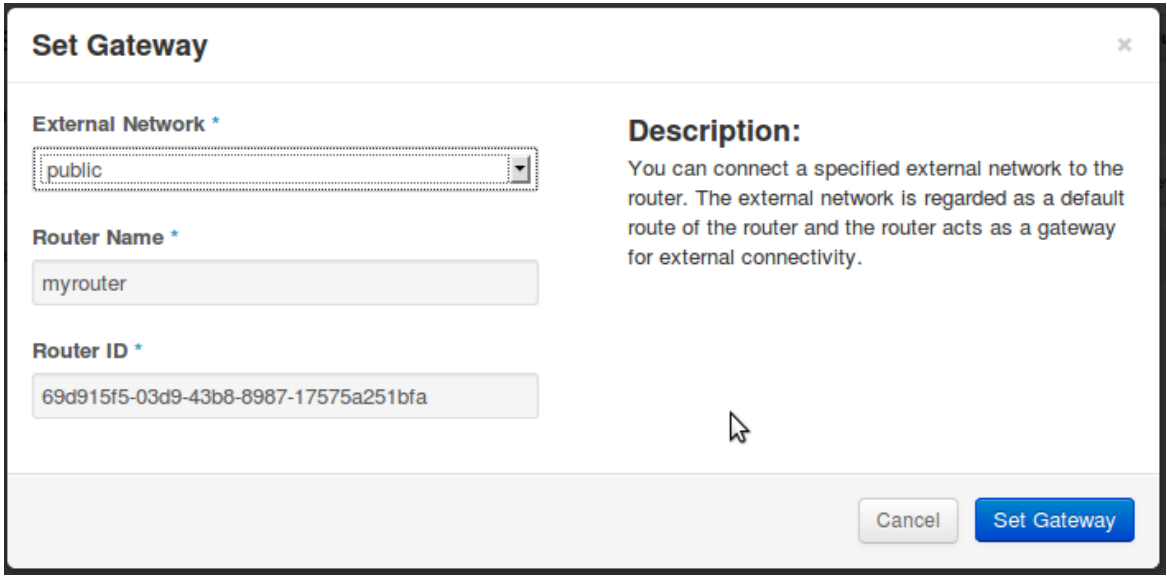




neutron router-gateway-set myrouter public

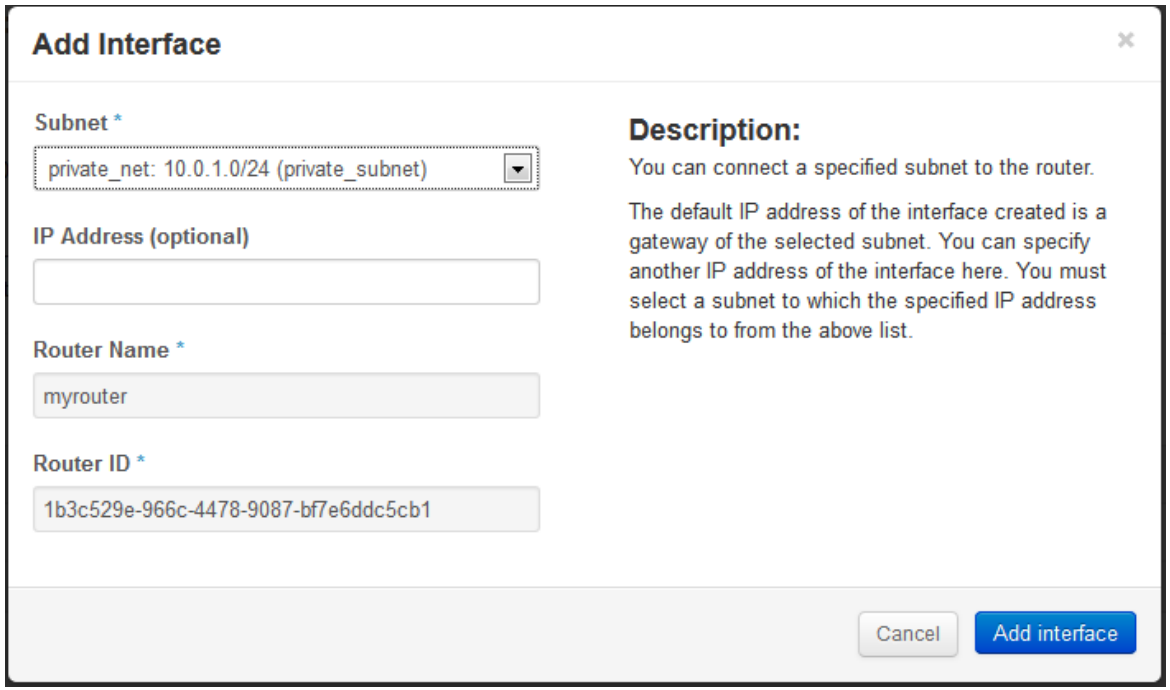
Collega il router alla rete public

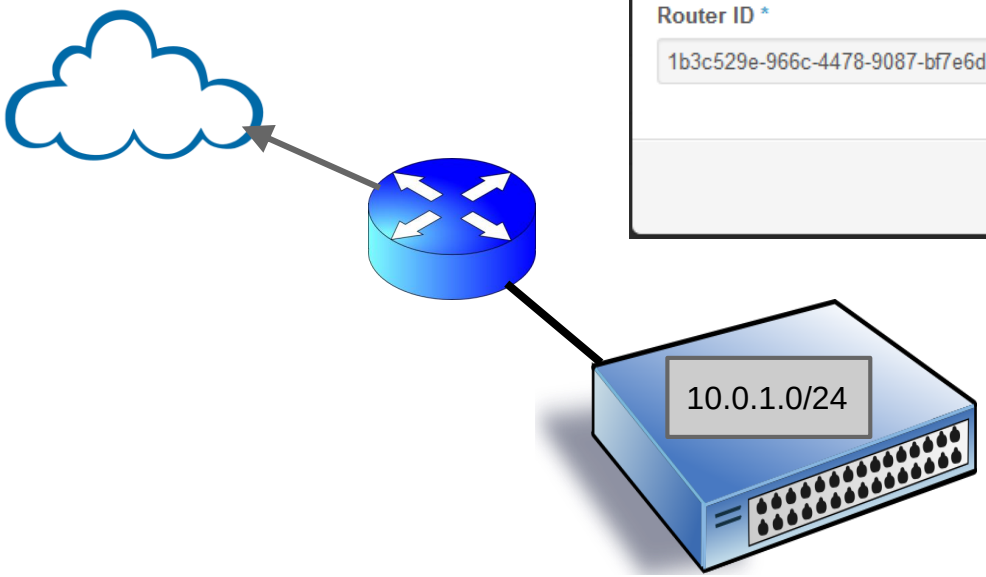




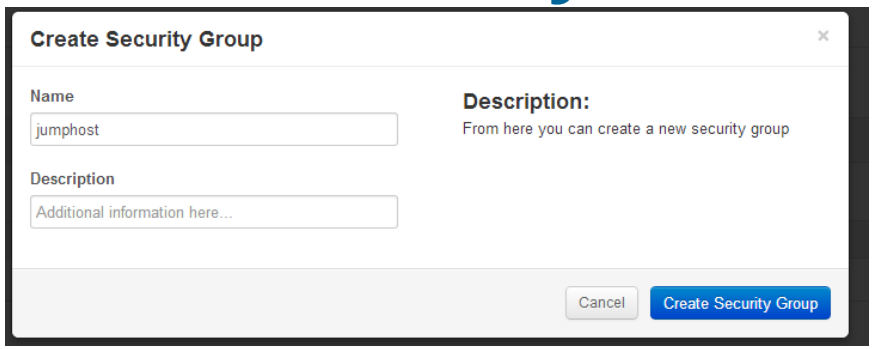
Interfaccia del router

neutron router-interface-add myrouter private_subnet





Security Group

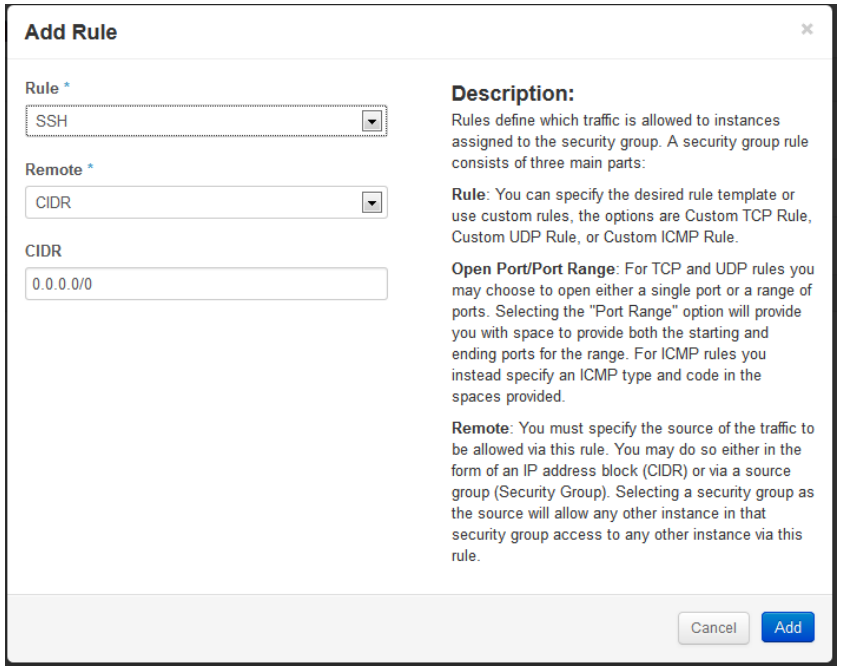


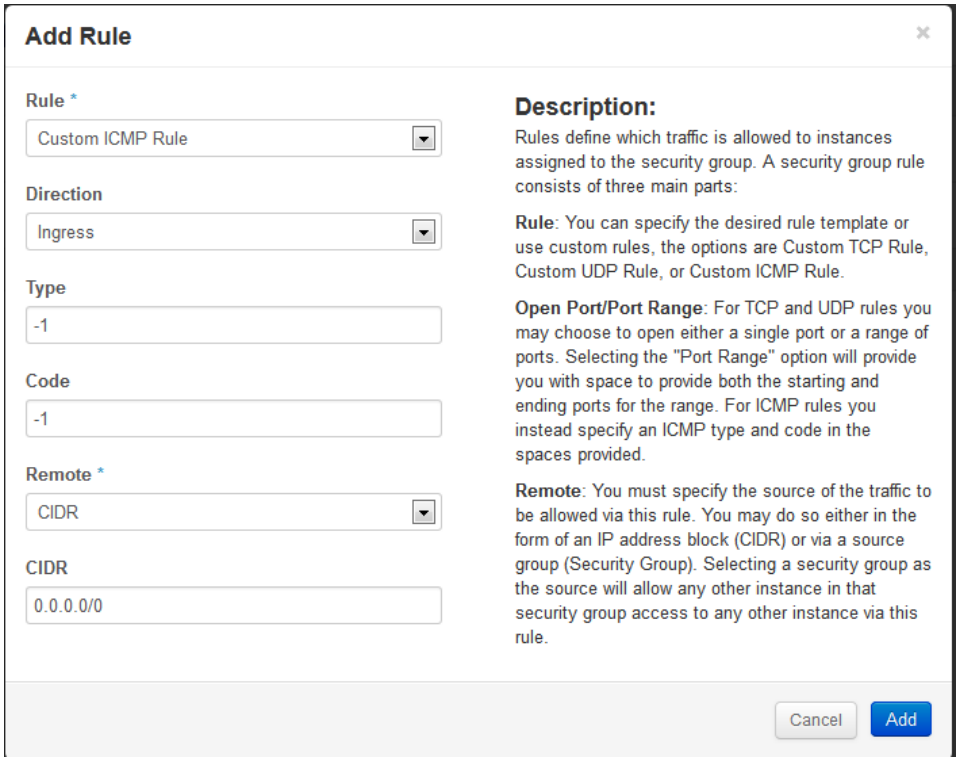
neutron security-group-create jumphost

1) Creazione dell gruppo **jumphost**

neutron security-group-rule-create --protocol icmp jumphost

2) Permette il **ping**





neutron security-group-rule-create --protocol tcp --port-range-min 22 --port-range-max 22 jumphost

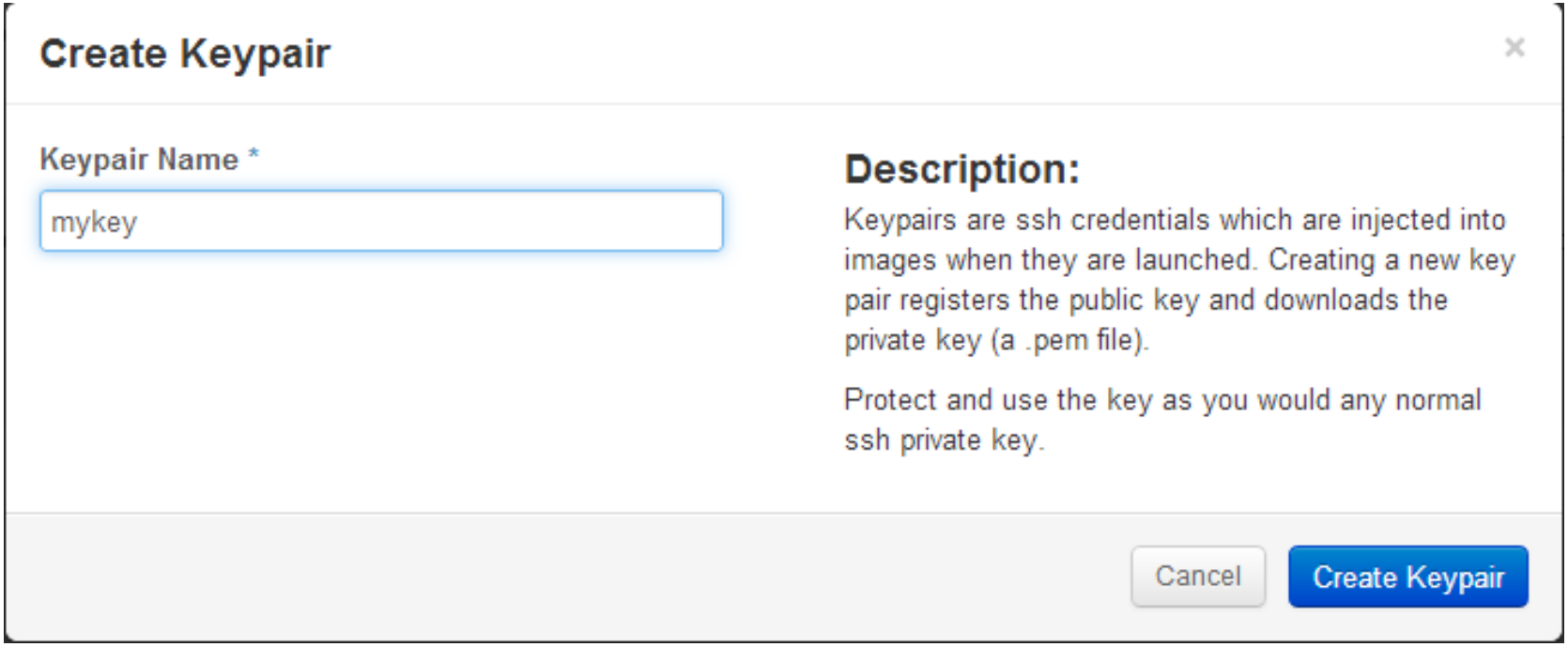
3) Permette la connessione **ssh**

Chiavi SSH

nova keypair-add mykey
chmod 600 mykey.pem

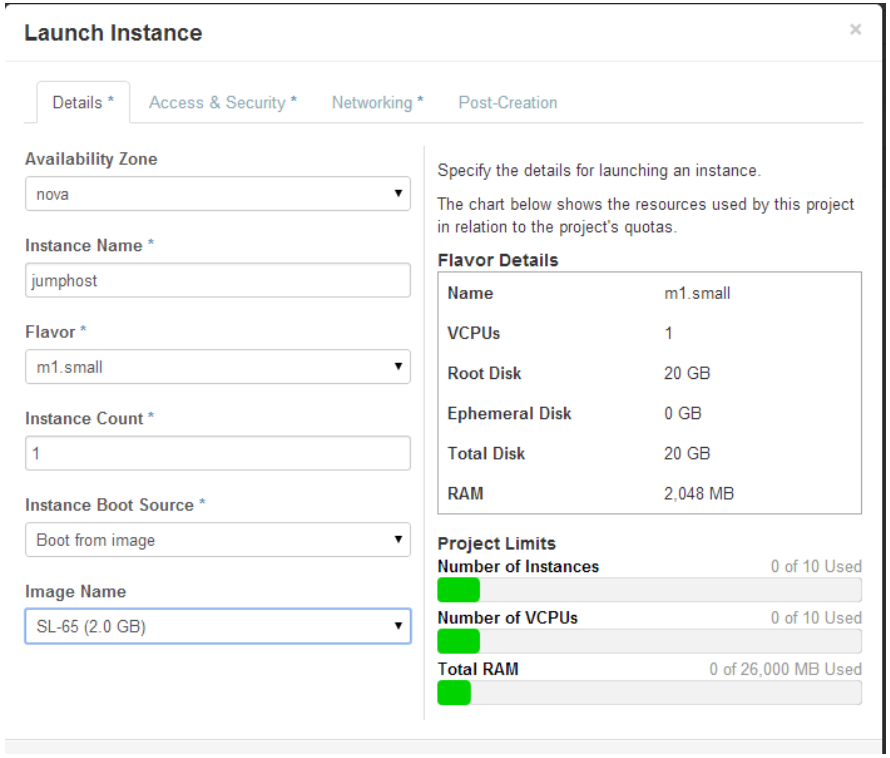
Generazione di una coppia di chiavi SSH

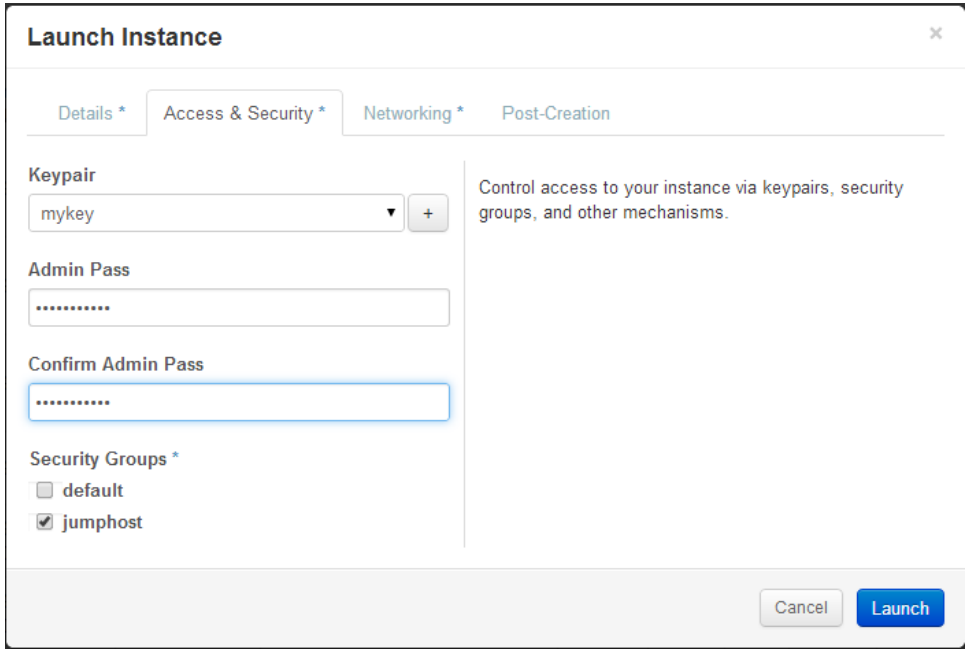
Download della chiave privata sulla UI (da command-line bisogna copiare la chiave privata che è l'output del comando)

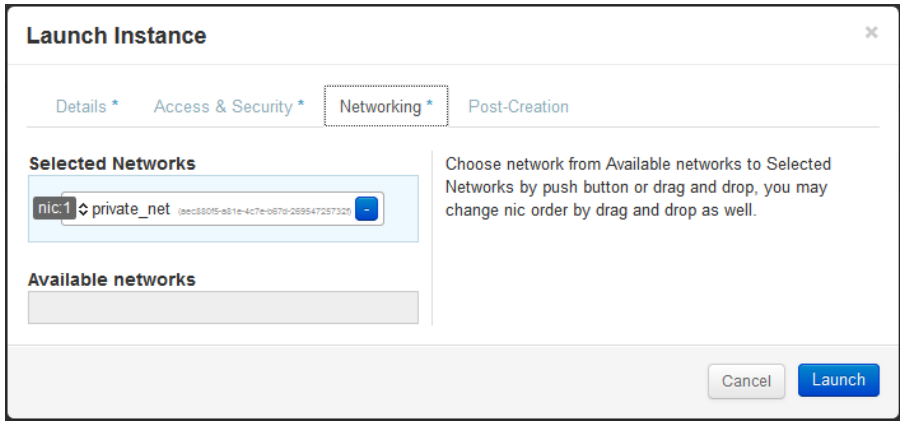


Istanziazione di VM

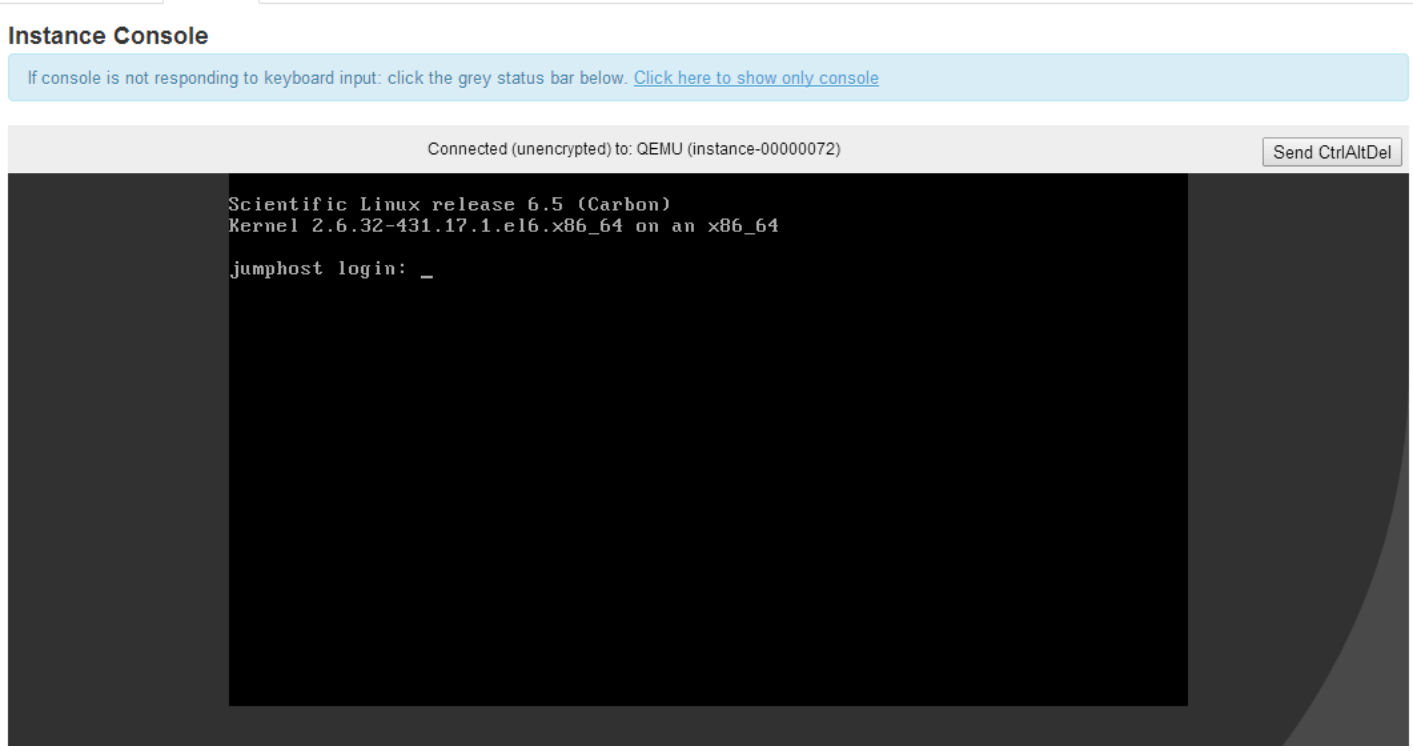
nova boot --image SL-65 --flavor m1.small jumphost --security_groups jumphost –key-name mykey
(recuperare la password di root dall'output del comando nova boot)

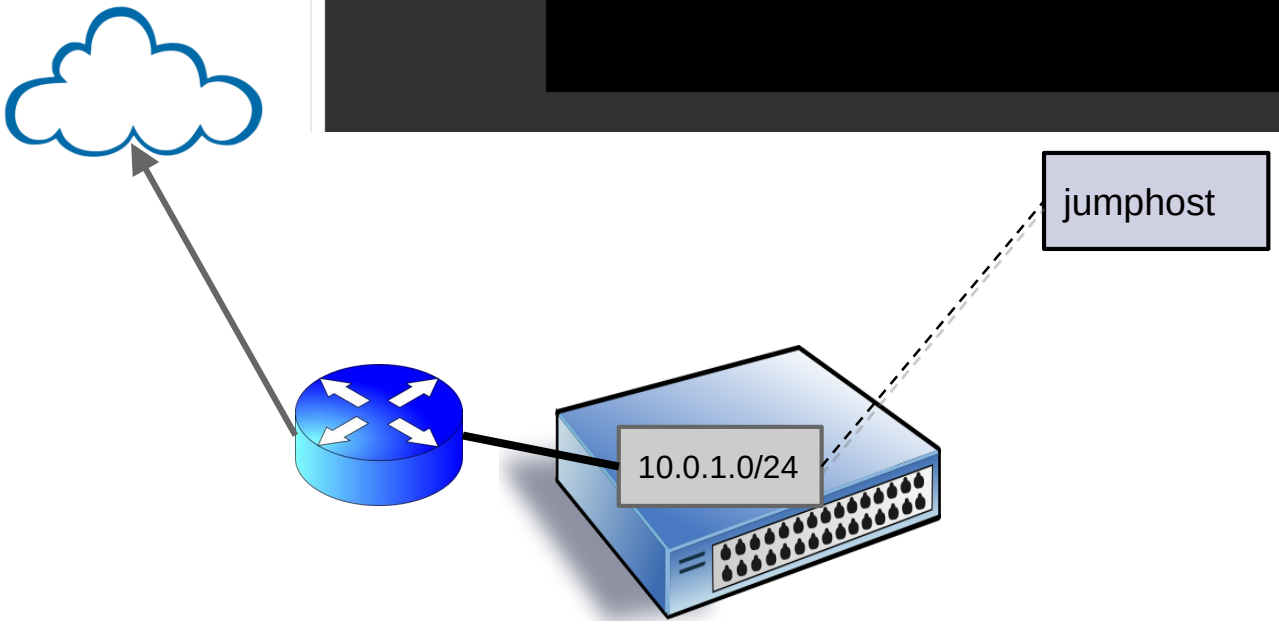






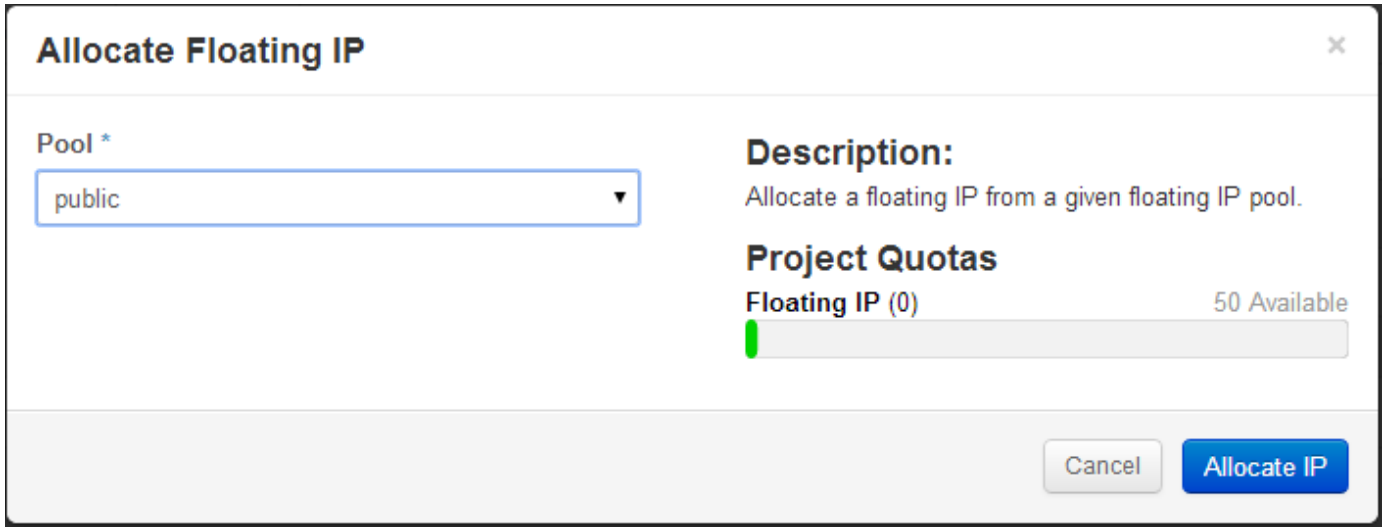
Verifica via console

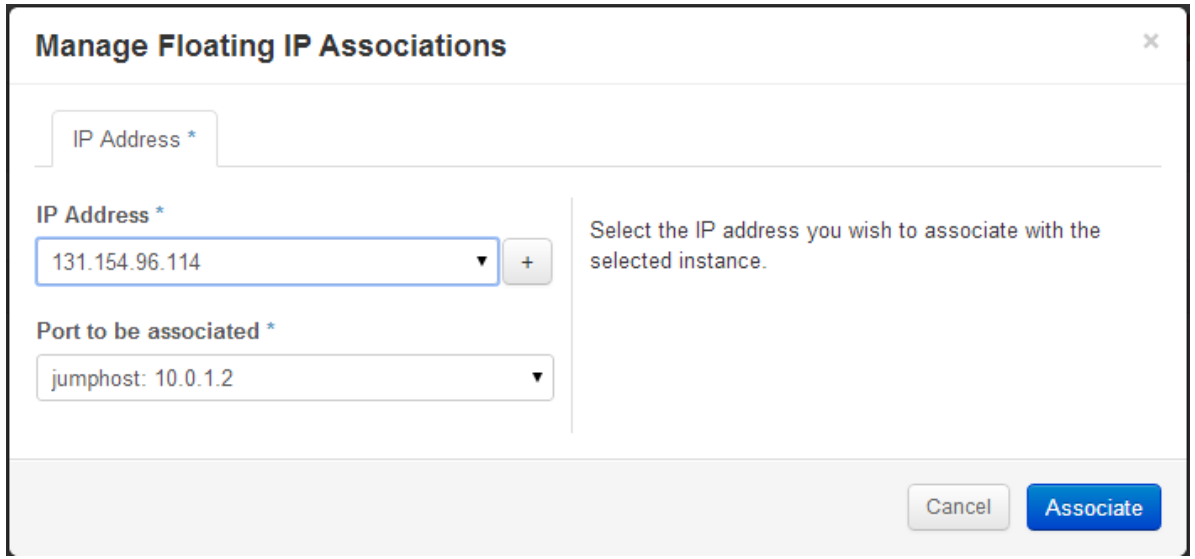




Floating IP

nova list
neutron port-list --device_id=<instance_ID>
neutron floatingip-create public --port-id <port_ID>





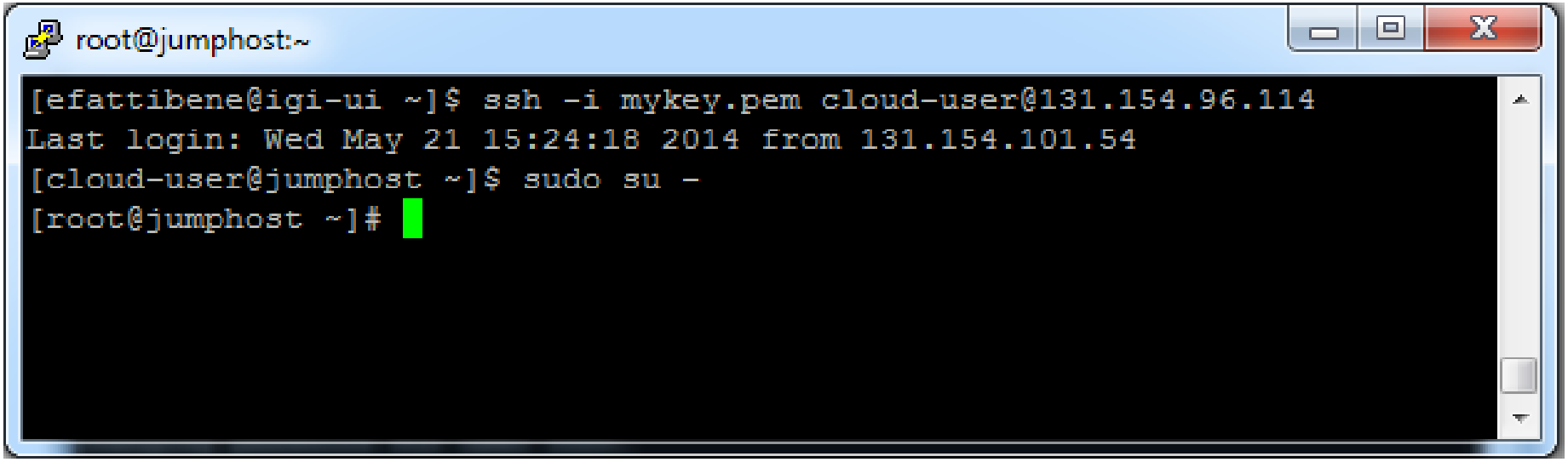
Accesso via SSH

ssh -i mykey.pem cloud-user@131.154.96.xxx

Login attraverso chiavi SSH con utente cloud-user

sudo su -

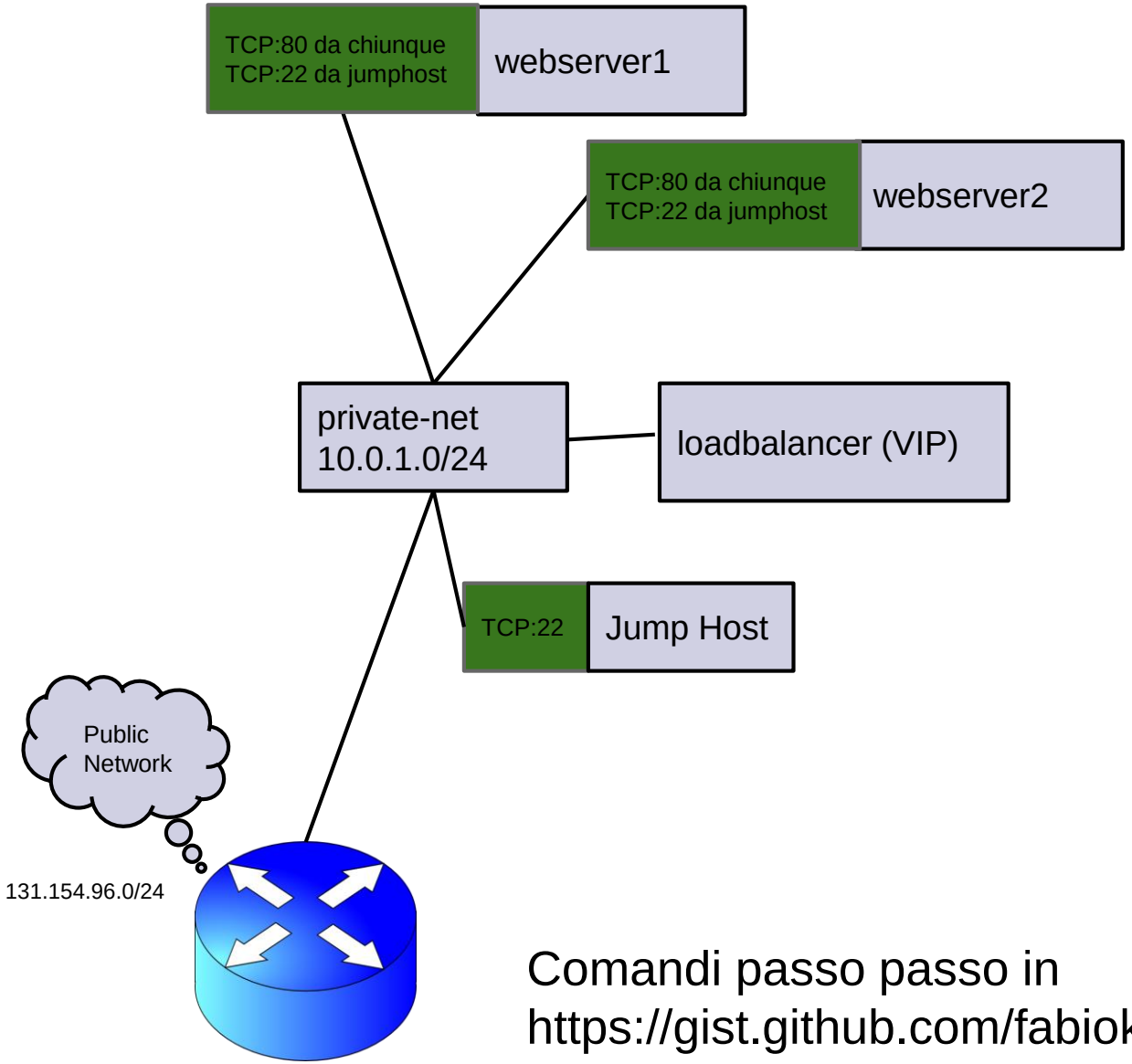
Cambio identità a root



Riassumendo

- Da dashboard (console)
  - accesso solo come root e solo con password (da indicare in fase di generazione della VM)
- Da remoto
  - accesso solo via chiave SSH e solo con account non privilegiati (cloud-user)

Demo parte II - advanced

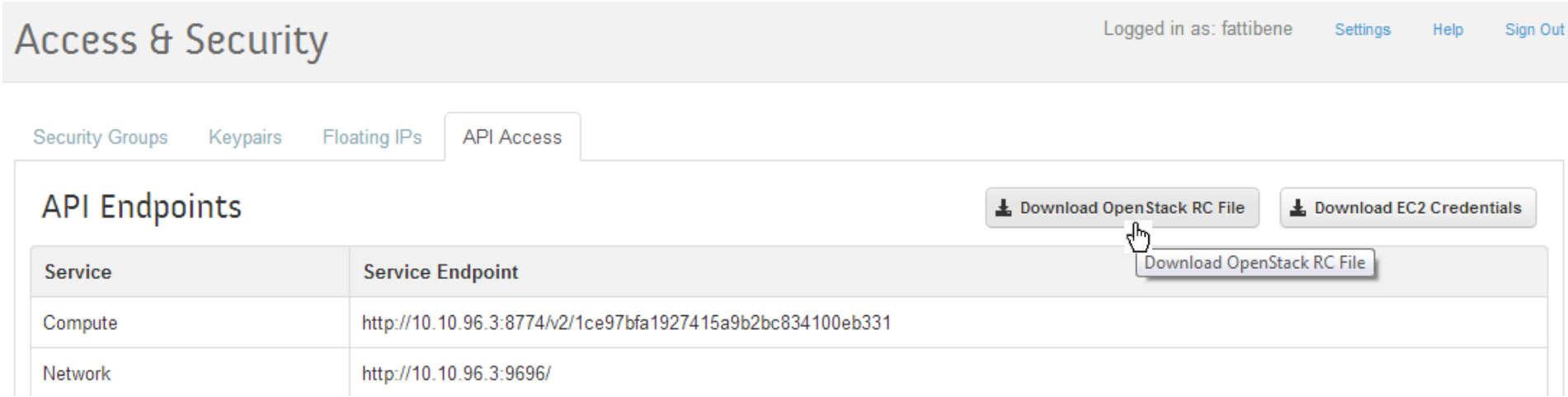


Comandi passo passo in
https://gist.github.com/fabiok/e8fcc717de738240eec5

Download file credenziali

Download RC file dalla dashboard

Upload RC file nella propria home della UI di riferimento



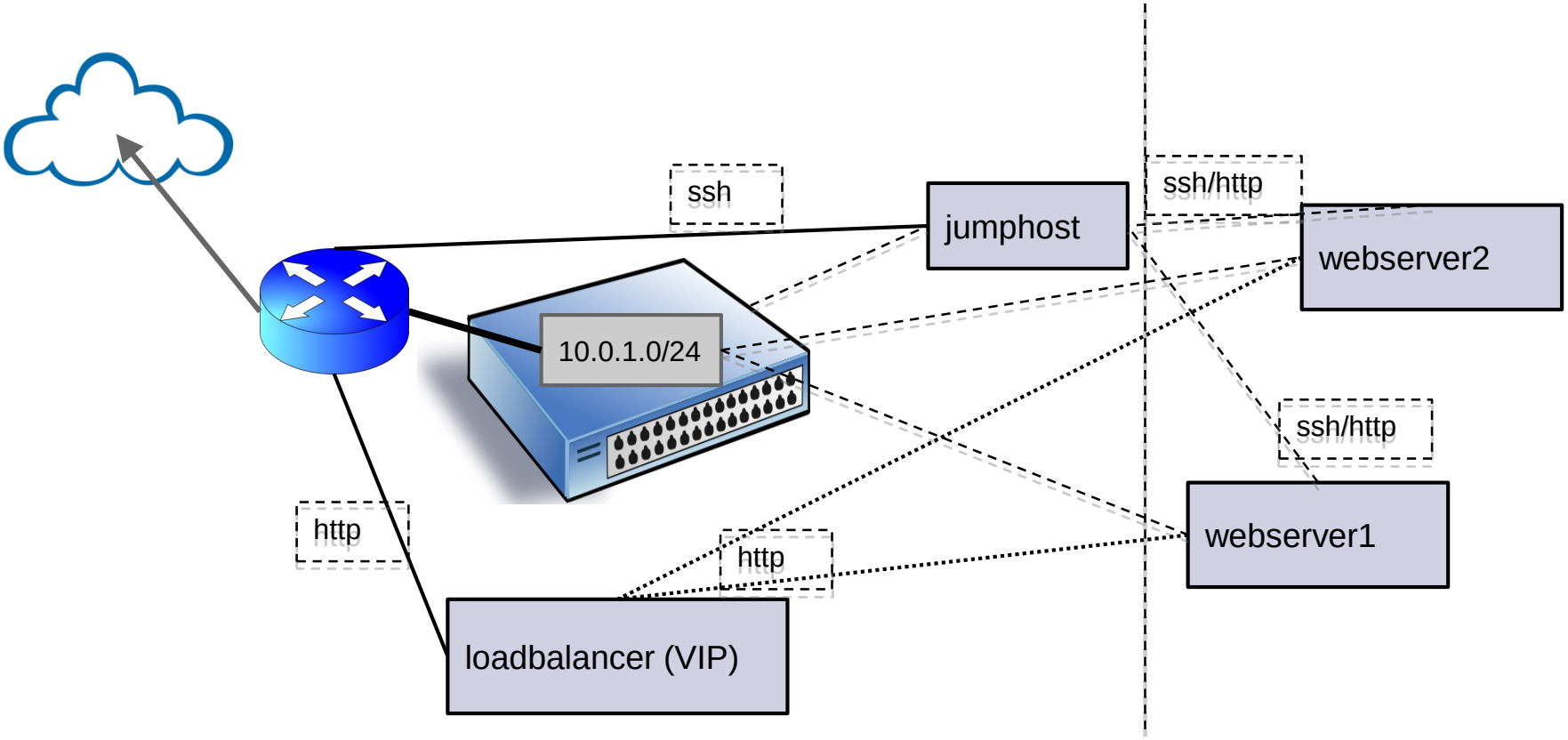
Contenuto RC file

```
#!/bin/bash

# With the addition of Keystone, to use an openstack cloud you should
# authenticate against keystone, which returns a **Token** and **Service
# Catalog**.  The catalog contains the endpoint for all services the
# user/tenant has access to - including nova, glance, keystone, swift.
#
# *NOTE*: Using the 2.0 *auth api* does not mean that compute api is 2.0.  We
# will use the 1.1 *compute api*
export OS_AUTH_URL=http://10.10.96.3:5000/v2.0

# With the addition of Keystone we have standardized on the term **tenant**
# as the entity that owns the resources.
export OS_TENANT_ID=1ce97bfa1927415a9b2bc834100eb331
export OS_TENANT_NAME="Fattibene"

# In addition to the owning entity (tenant), openstack stores the entity
# performing the action as the **user**.
export OS_USERNAME="fattibene"

# With Keystone you pass the keystone password.
echo "Please enter your OpenStack Password: "
read -sr OS_PASSWORD_INPUT
export OS_PASSWORD=$OS_PASSWORD_INPUT
```

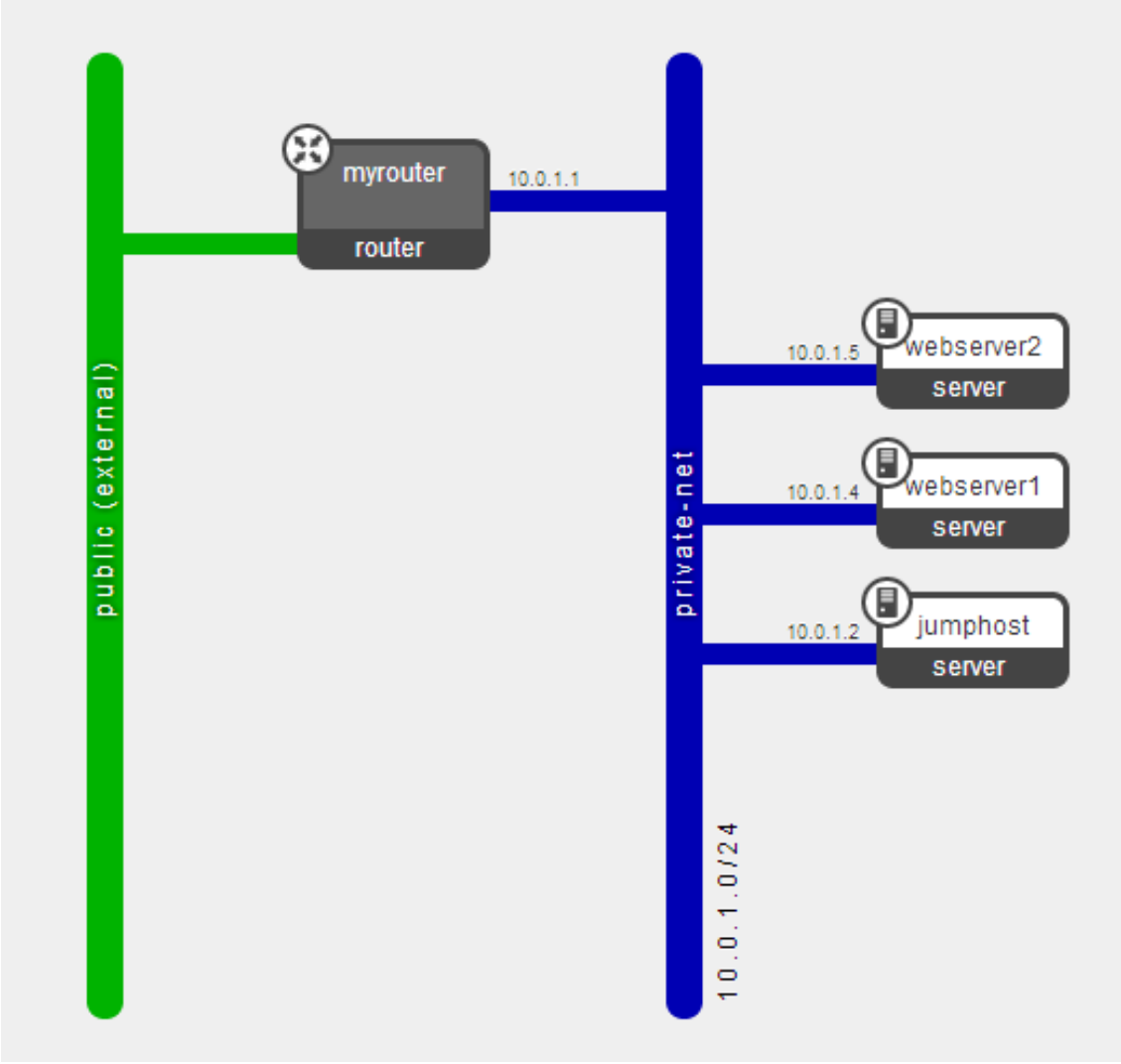
Piccola accortezza

- In caso di richiesta di digitare la password ad ogni comando
  - Per evitare la richiesta continua, aggiungere questa riga nel file .bash_profile:
  - export OS_NO_CACHE=1

Security groups e LBaaS



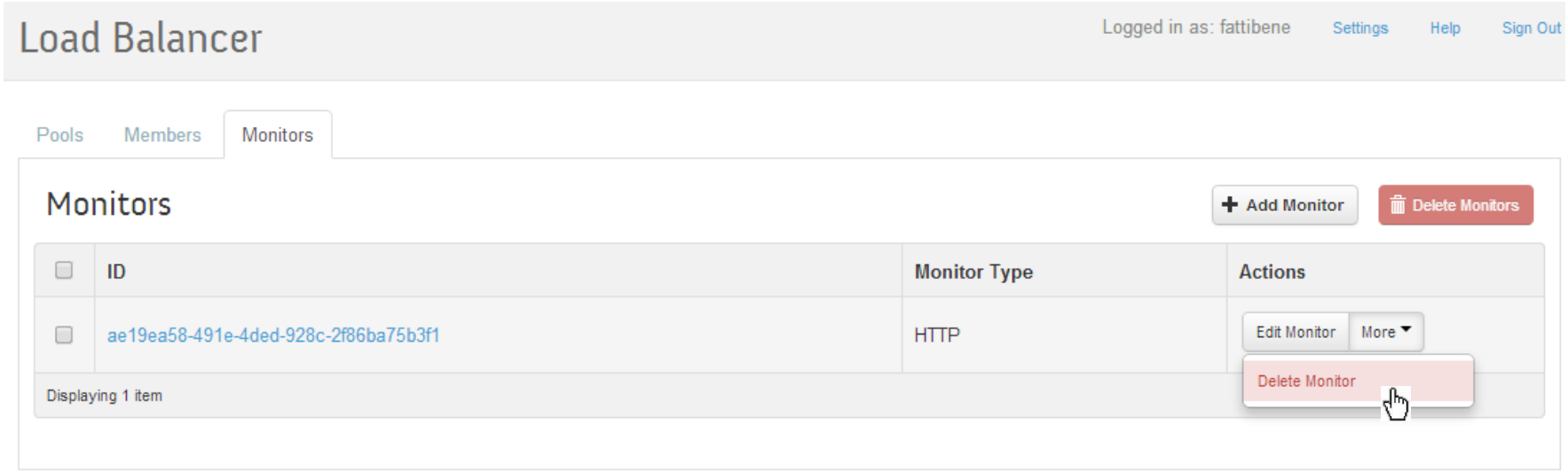
Topologia di rete finale

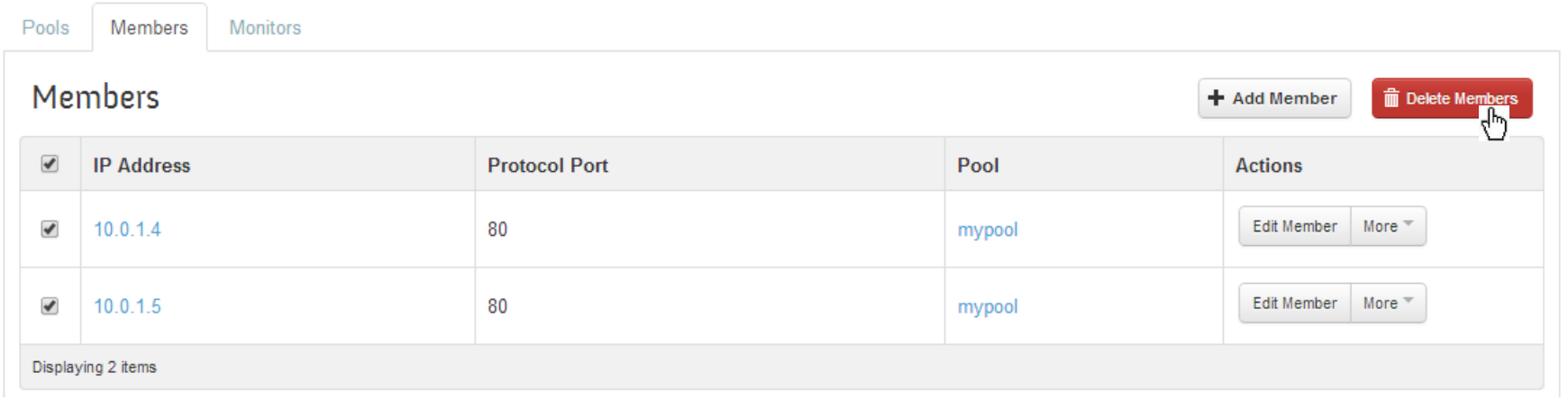


Pulizia della demo advanced

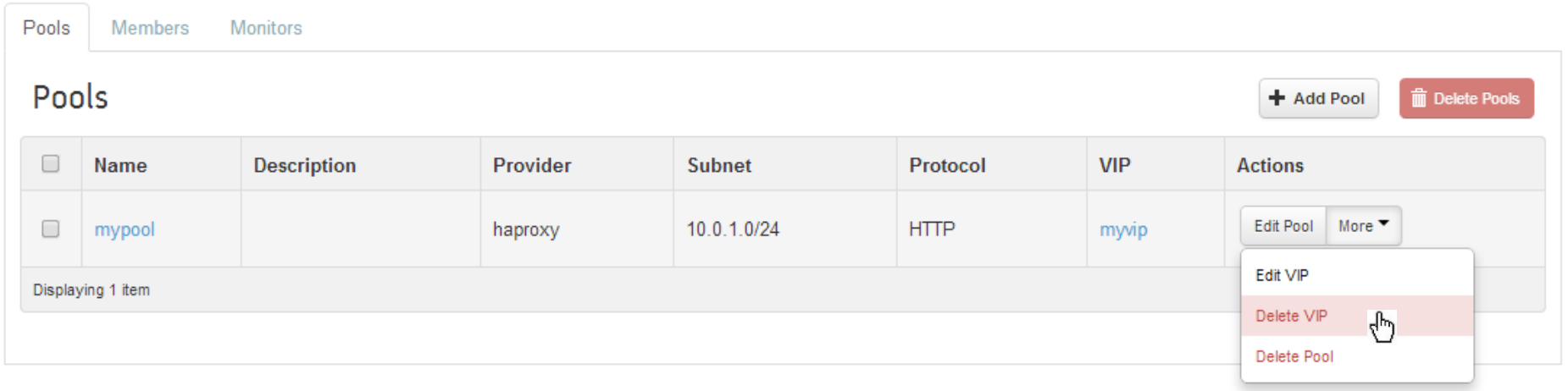
- Da cancellare via dashboard
  - LBaaS
  - Le due VM webserver
  - Security group web

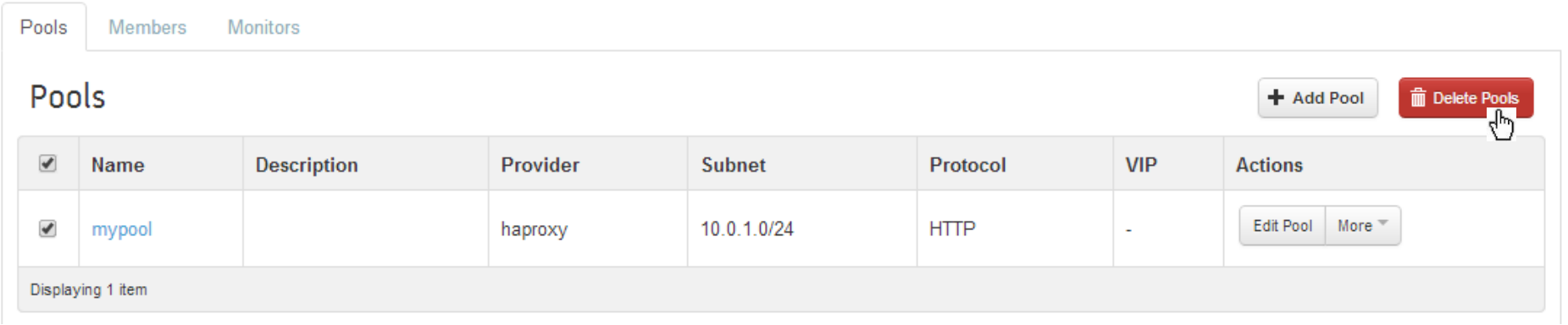
LBaaS monitor e membri del pool





LBaaS VIP e pool





VM webserver e sec group web

Instances

Filter | Filter | + Launch Instance | Soft Reboot Instances | Terminate Instances

Instance Name	Image Name	IP Address	Size	Keypair	Status	Task	Power State	Uptime	Actions
webserver2	SL-65	10.0.1.5	m1.small | 2GB RAM | 1 VCPU | 10.0GB Disk	mykey	Active	None	Running	18 hours, 57 minutes	Create Snapshot | More
webserver1	SL-65	10.0.1.4	m1.small | 2GB RAM | 1 VCPU | 10.0GB Disk	mykey	Active	None	Running	18 hours, 58 minutes	Create Snapshot | More
jumphost	SL-65	10.0.1.2 131.154.96.114	m1.small | 2GB RAM | 1 VCPU | 10.0GB Disk	mykey	Active	None	Running	19 hours, 4 minutes	Create Snapshot | More

Displaying 3 items

Security Groups | Keypairs | Floating IPs | API Access

Security Groups

+ Create Security Group | Delete Security Groups

Name	Description	Actions
default	default	Edit Rules
jumphost		Edit Rules | More
web		Edit Rules | More

Displaying 3 items

Supporto

- Per inviare una richiesta di supporto utilizzare JIRA
- L'unità di supporto è CLOUDCNAF

https://issues.infn.it/jira/browse/CLOUDCNAF

Questionario di valutazione

- Lo scopo è di poter migliorare i prossimi eventi di formazione e raccogliere informazioni sugli aspetti che più si desidera vengano trattati
- La forma è anonima
- Accesso con password

https://it.surveymonkey.com/s/6BRGJVP