

Laboratorio

Paolo Veronesi, Enrico Fattibene, Fabio Capannini

Formazione Cloud@CNAF
13/6/2014

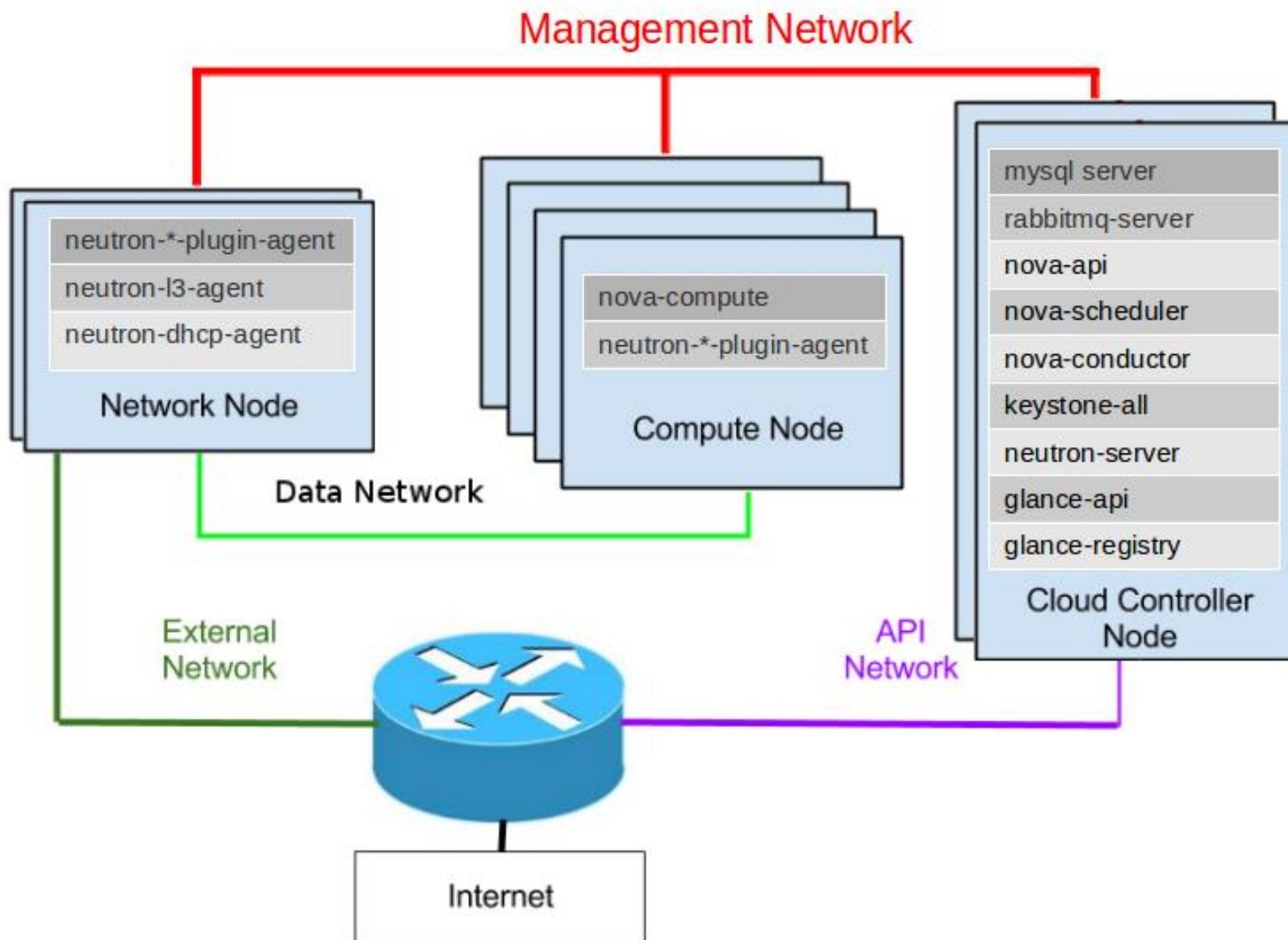
Sommario

- 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

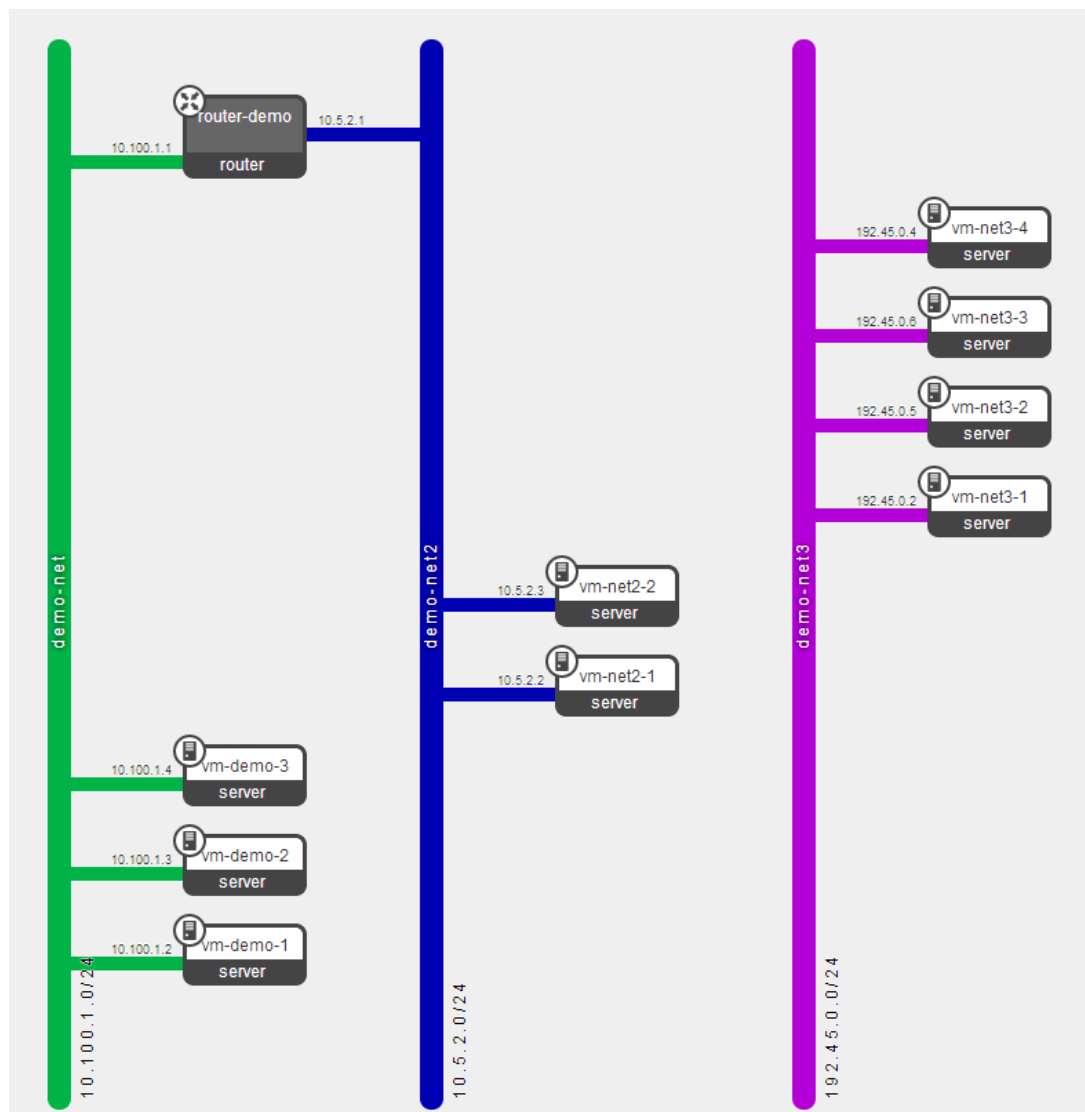
Infrastruttura



Tipologie di rete (1/3)

- Private Tenant Network
 - All'interno di ogni progetto (Tenant), gli utenti possono creare una o più reti private e uno o più 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 è 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



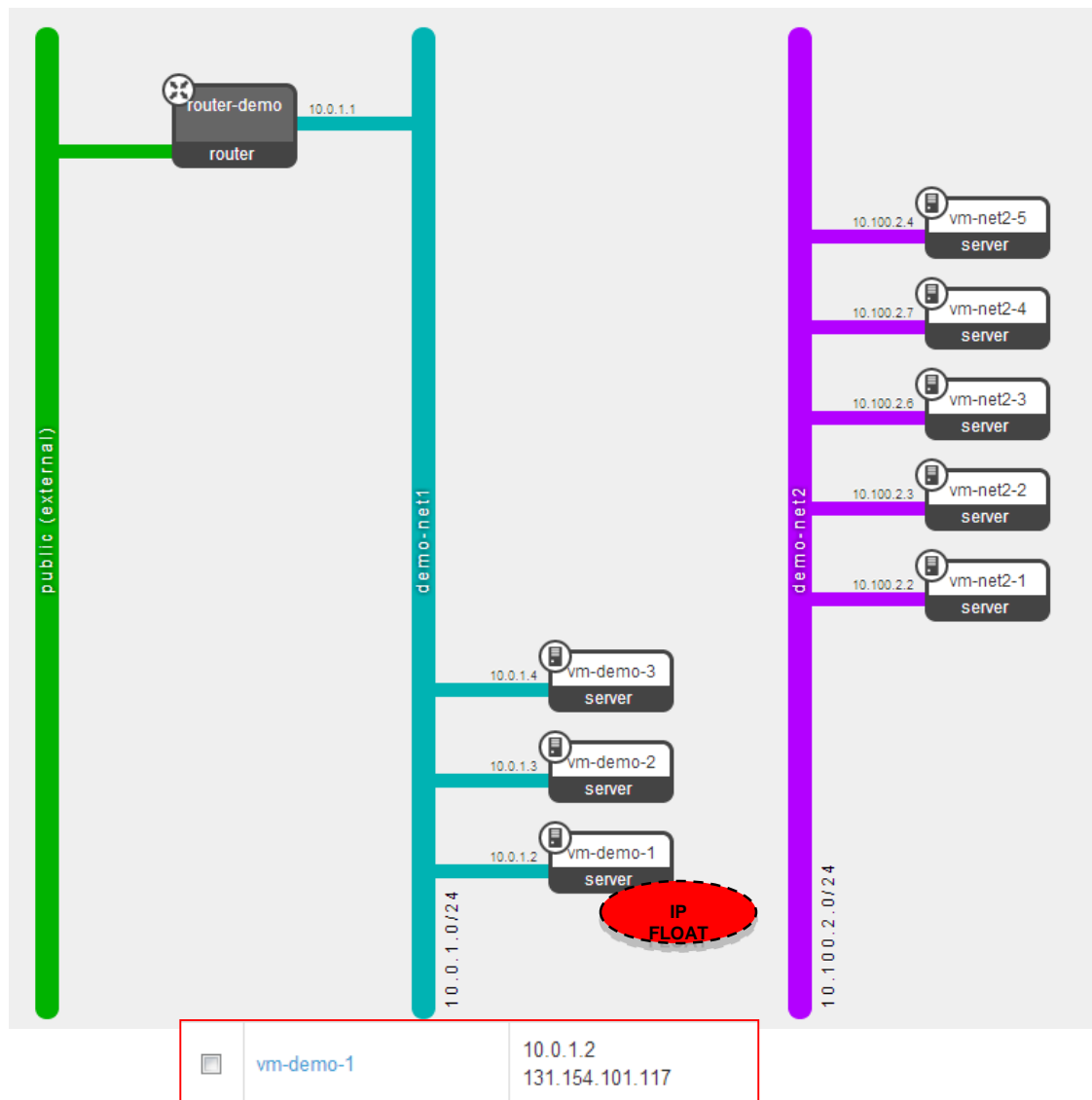
Tipologie di rete (2/3)

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.

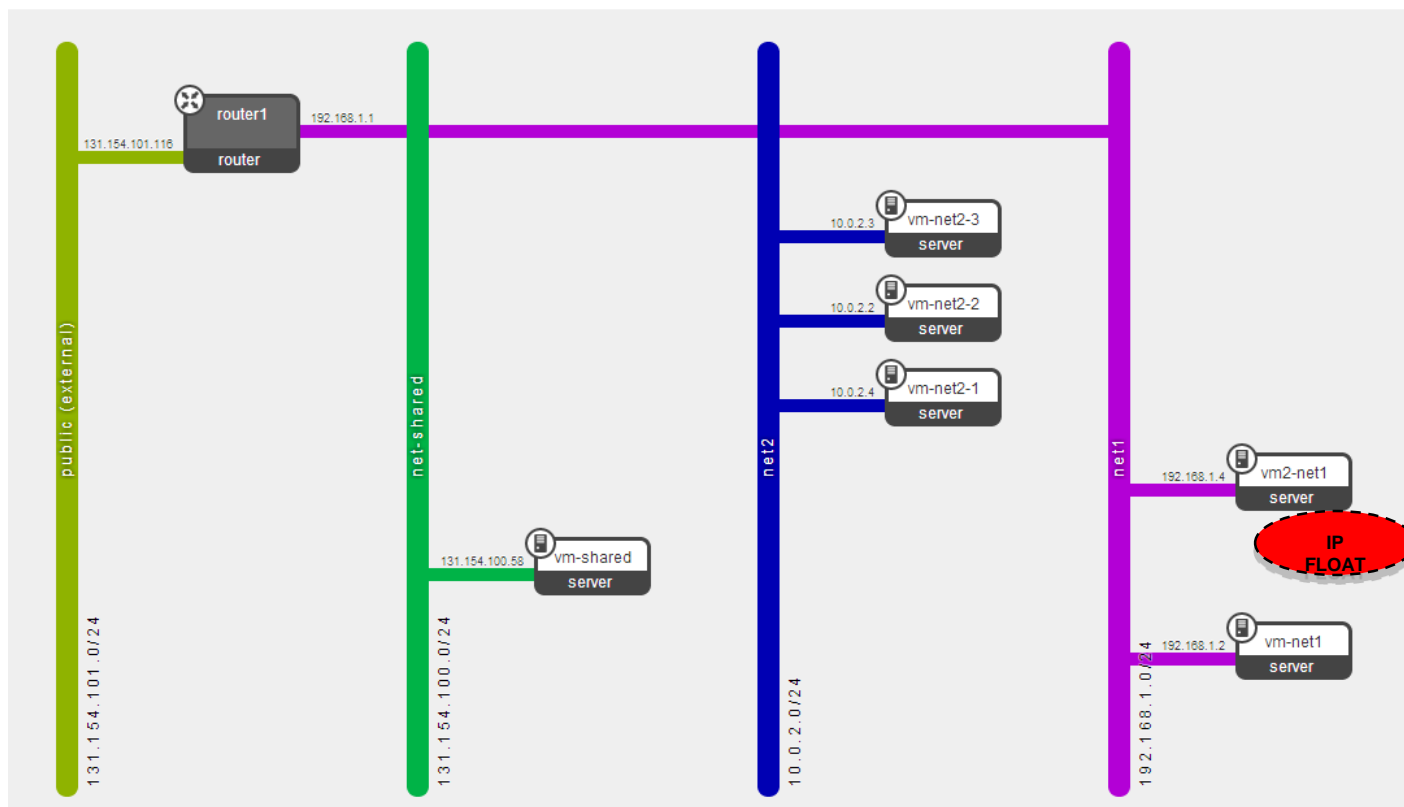
Workflow

- 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)

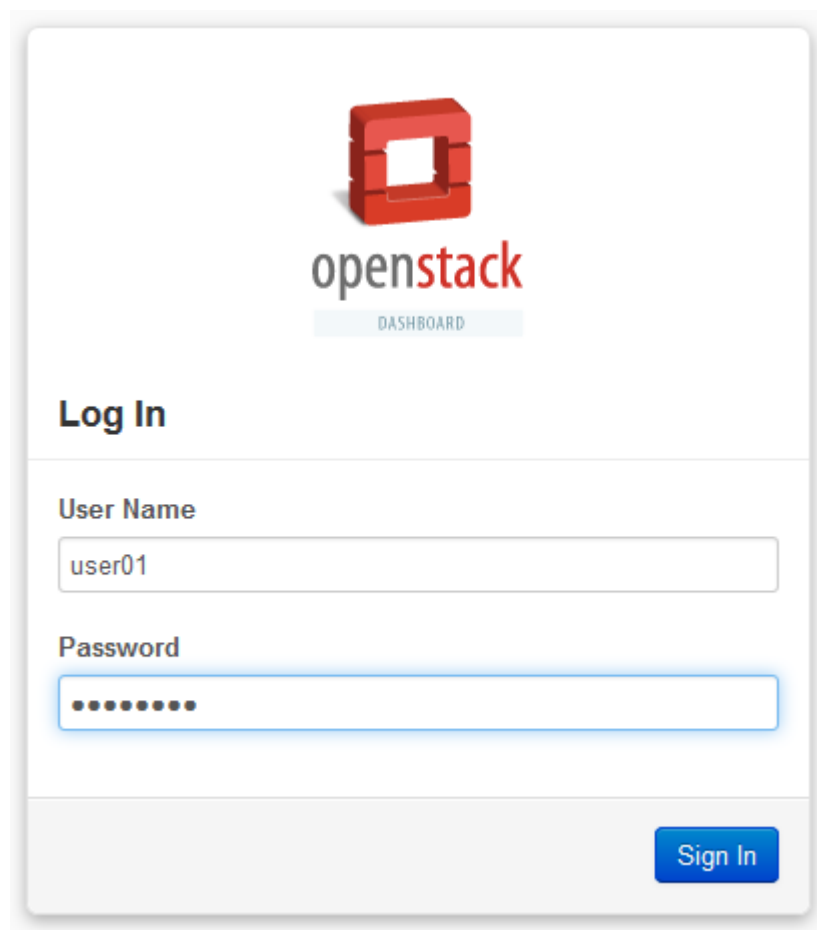
- Shared Network
- La shared network e' una tipologia di rete attraverso la quale si mette a disposizione dell'infrastruttura OpenStack una rete esistente nel centro di calcolo per poter creare delle VM sulla rete stessa.
- Le VM possono essere istanziate sulla rete shared, l'IP viene loro fornito da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



Connessione alla dashboard

Dashboard via web:

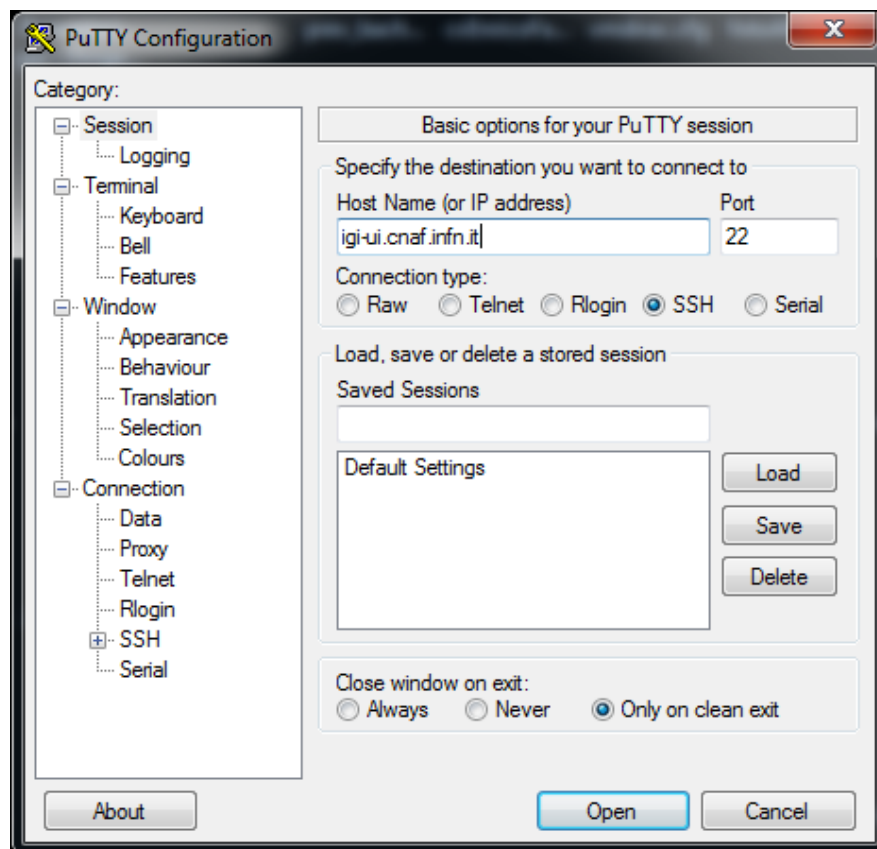
<https://cloudctrl02.cloud.cnaf.infn.it/dashboard>



The image shows a screenshot of the OpenStack Dashboard login page. At the top, there is the OpenStack logo (a red cube) and the text "openstack" in a sans-serif font, with "DASHBOARD" in a smaller font below it. Below the logo, the heading "Log In" is displayed. Underneath, there are two input fields: "User Name" with the text "user01" entered, and "Password" with a masked password represented by eight dots. A blue "Sign In" button is located at the bottom right of the form.

Connessione alla UI

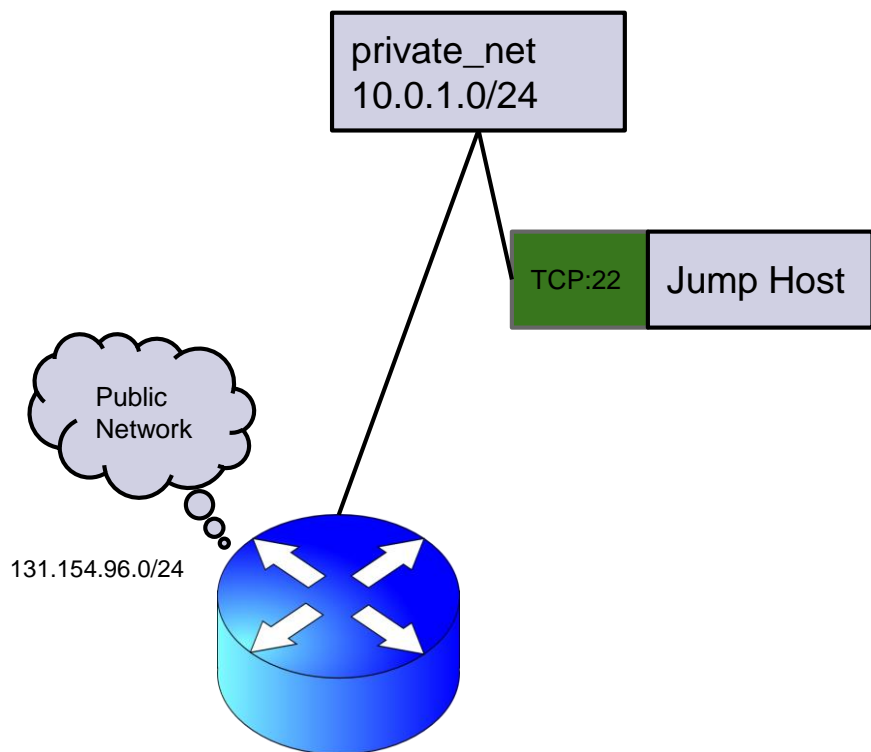
UI di riferimento (ad es. igi-ui.cnaf.infn.it)



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
- Instance
 - 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

Change Password

Current password *

New password *

Confirm new password *

Description:

From here you can change your password. We highly recommend you create a strong one.

Change

Creazione di rete privata

neutron net-create private_net

Creazione di una rete privata



Create Network

Network

Subnet

Subnet Detail

Network Name

private_net

Admin State

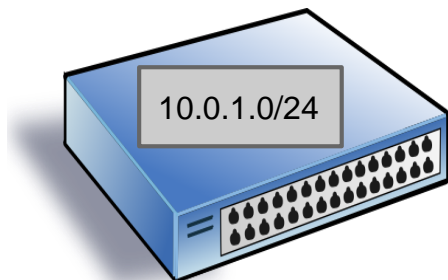
☒

From here you can create a new network. In addition a subnet associated with the network can be created in the next panel.

Cancel

Create

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



Create Network

Network

Subnet

Subnet Detail

Create Subnet

☒

Subnet Name

private_subnet

Network Address

10.0.1.0/24

IP Version

IPv4

Gateway IP (optional)

Disable Gateway

☐

You can create a subnet associated with the new network, in which case "Network Address" must be specified. If you wish to create a network WITHOUT a subnet, uncheck the "Create Subnet" checkbox.

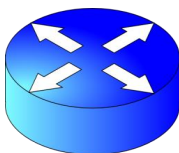
Cancel

Create

Creazione di un router

neutron router-create myrouter

Creazione di un router



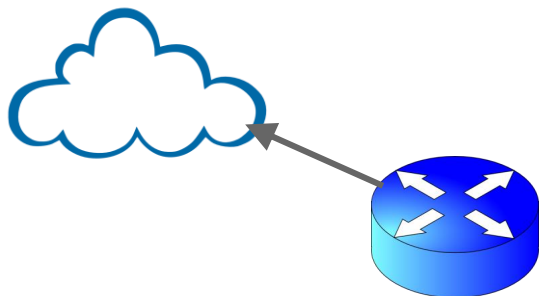
Create router

Router Name

Cancel Create router

neutron router-gateway-set myrouter public

Collega il router alla rete public



Set Gateway

External Network *

public

Router Name *

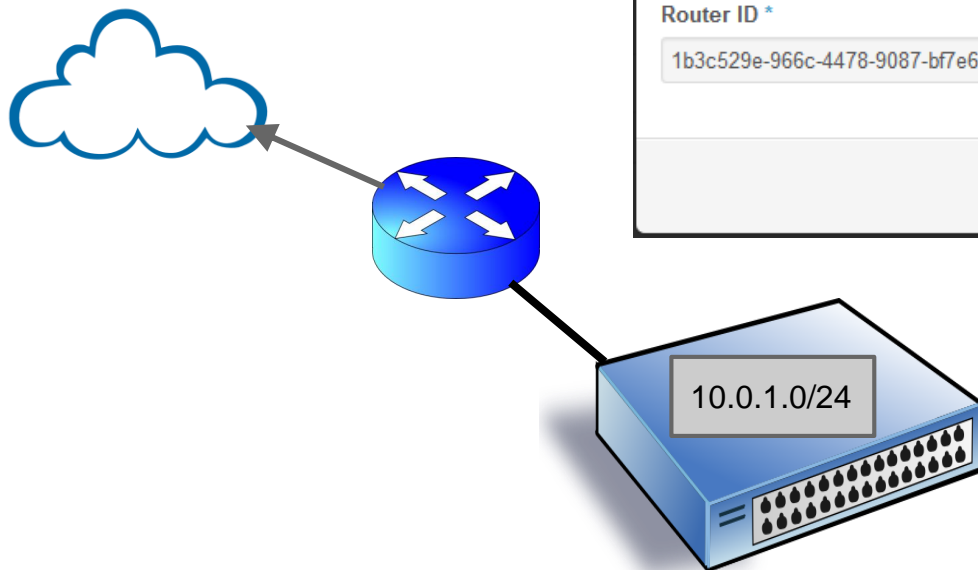
Router ID *

Description:
You can connect a specified external network to the router. The external network is regarded as a default route of the router and the router acts as a gateway for external connectivity.

Cancel Set Gateway

Interfaccia del router

neutron router-interface-add myrouter private_subnet



Add Interface

Subnet *

private_net: 10.0.1.0/24 (private_subnet)

IP Address (optional)

Router Name *

myrouter

Router ID *

1b3c529e-966c-4478-9087-bf7e6ddc5cb1

Description:

You can connect a specified subnet to the router.

The default IP address of the interface created is a gateway of the selected subnet. You can specify another IP address of the interface here. You must select a subnet to which the specified IP address belongs to from the above list.

Cancel

Add interface

Security Group

Create Security Group

Name: jumphost

Description: From here you can create a new security group

Description: Additional information here...

Cancel Create Security Group

neutron security-group-create jumphost

1) Creazione del gruppo jumphost

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

2) Permette il ping

Add Rule

Rule *: SSH

Remote *: CIDR

CIDR: 0.0.0.0/0

Description:

Rules define which traffic is allowed to instances assigned to the security group. A security group rule consists of three main parts:

Rule: You can specify the desired rule template or use custom rules, the options are Custom TCP Rule, Custom UDP Rule, or Custom ICMP Rule.

Open Port/Port Range: For TCP and UDP rules you may choose to open either a single port or a range of ports. Selecting the "Port Range" option will provide you with space to provide both the starting and ending ports for the range. For ICMP rules you instead specify an ICMP type and code in the spaces provided.

Remote: You must specify the source of the traffic to be allowed via this rule. You may do so either in the form of an IP address block (CIDR) or via a source group (Security Group). Selecting a security group as the source will allow any other instance in that security group access to any other instance via this rule.

Cancel Add

Add Rule

Rule *: Custom ICMP Rule

Direction: Ingress

Type: -1

Code: -1

Remote *: CIDR

CIDR: 0.0.0.0/0

Description:

Rules define which traffic is allowed to instances assigned to the security group. A security group rule consists of three main parts:

Rule: You can specify the desired rule template or use custom rules, the options are Custom TCP Rule, Custom UDP Rule, or Custom ICMP Rule.

Open Port/Port Range: For TCP and UDP rules you may choose to open either a single port or a range of ports. Selecting the "Port Range" option will provide you with space to provide both the starting and ending ports for the range. For ICMP rules you instead specify an ICMP type and code in the spaces provided.

Remote: You must specify the source of the traffic to be allowed via this rule. You may do so either in the form of an IP address block (CIDR) or via a source group (Security Group). Selecting a security group as the source will allow any other instance in that security group access to any other instance via this rule.

Cancel Add

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)

Create Keypair

Keypair Name *

mykey

Description:

Keypairs are ssh credentials which are injected into images when they are launched. Creating a new key pair registers the public key and downloads the private key (a .pem file).

Protect and use the key as you would any normal ssh private key.

Cancel

Create Keypair

Istanziamento 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)

Launch Instance

Details *

Access & Security *

Networking *

Post-Creation

Availability Zone

nova

Instance Name *

jumphost

Flavor *

m1.small

Instance Count *

1

Instance Boot Source *

Boot from image

Image Name

SL-65 (2.0 GB)

Specify the details for launching an instance.

The chart below shows the resources used by this project in relation to the project's quotas.

Flavor Details

Name	m1.small
VCPUs	1
Root Disk	20 GB
Ephemeral Disk	0 GB
Total Disk	20 GB
RAM	2,048 MB

Project Limits

Number of Instances	0 of 10 Used
Number of VCPUs	0 of 10 Used
Total RAM	0 of 26,000 MB Used

Launch Instance

Details *

Access & Security *

Networking *

Post-Creation

Keypair

mykey

+

Control access to your instance via keypairs, security groups, and other mechanisms.

Admin Pass

.....

Confirm Admin Pass

.....

Security Groups *

☐ default
 ☒ jumphost

Cancel

Launch

Launch Instance

Details *

Access & Security *

Networking *

Post-Creation

Selected Networks

nic1

private_net

0aec380f5-a51e-4c7e-b679-269547257320

+

Available networks

Choose network from Available networks to Selected Networks by push button or drag and drop, you may change nic order by drag and drop as well.

Cancel

Launch

Verifica via console

Instance Console

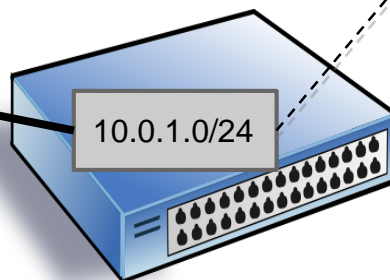
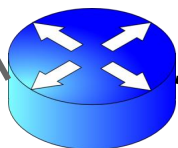
If console is not responding to keyboard input: click the grey status bar below. [Click here to show only console](#)

Connected (unencrypted) to: QEMU (instance-00000072)

Send CtrlAltDel

```
Scientific Linux release 6.5 (Carbon)
Kernel 2.6.32-431.17.1.el6.x86_64 on an x86_64

jumphost login: _
```



10.0.1.0/24

jumphost

Floating IP

nova list

neutron port-list --device_id=<instance_ID>

neutron floatingip-create public --port-id <port_ID>

Allocate Floating IP

Pool *

public

Description:
Allocate a floating IP from a given floating IP pool.

Project Quotas
Floating IP (0) 50 Available

Cancel

Allocate IP

Manage Floating IP Associations

IP Address *

IP Address *

131.154.96.114

+

Port to be associated *

jumphost: 10.0.1.2

Select the IP address you wish to associate with the selected instance.

Cancel

Associate

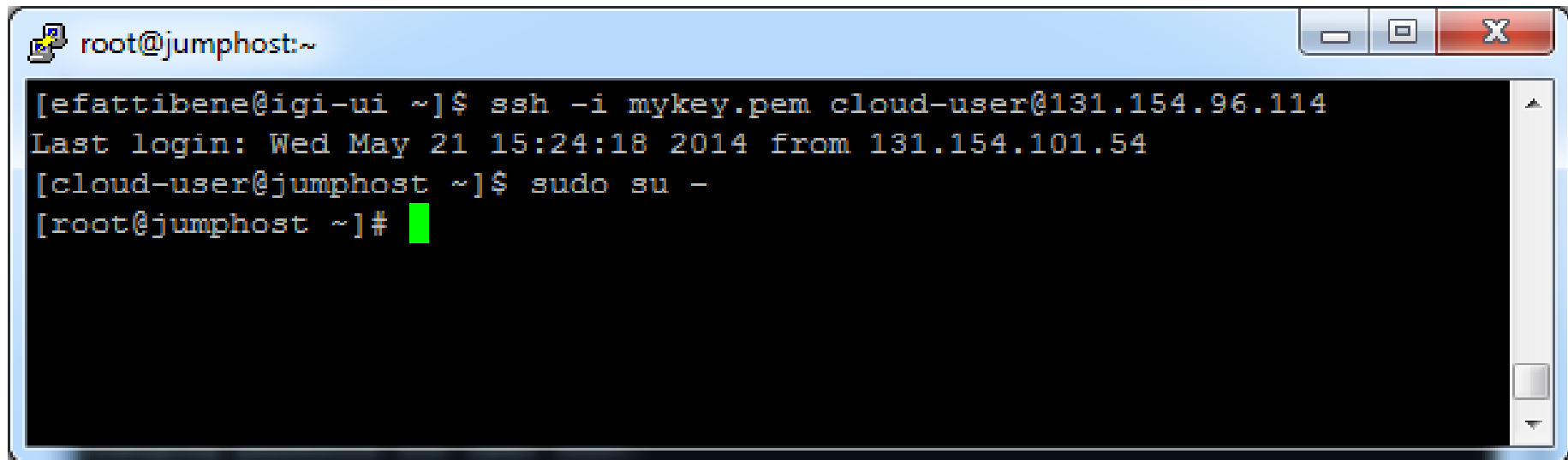
Accesso via SSH

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

Login attraverso chiavi SSH con utente cloud-user

```
sudo su -
```

Cambio identità a root

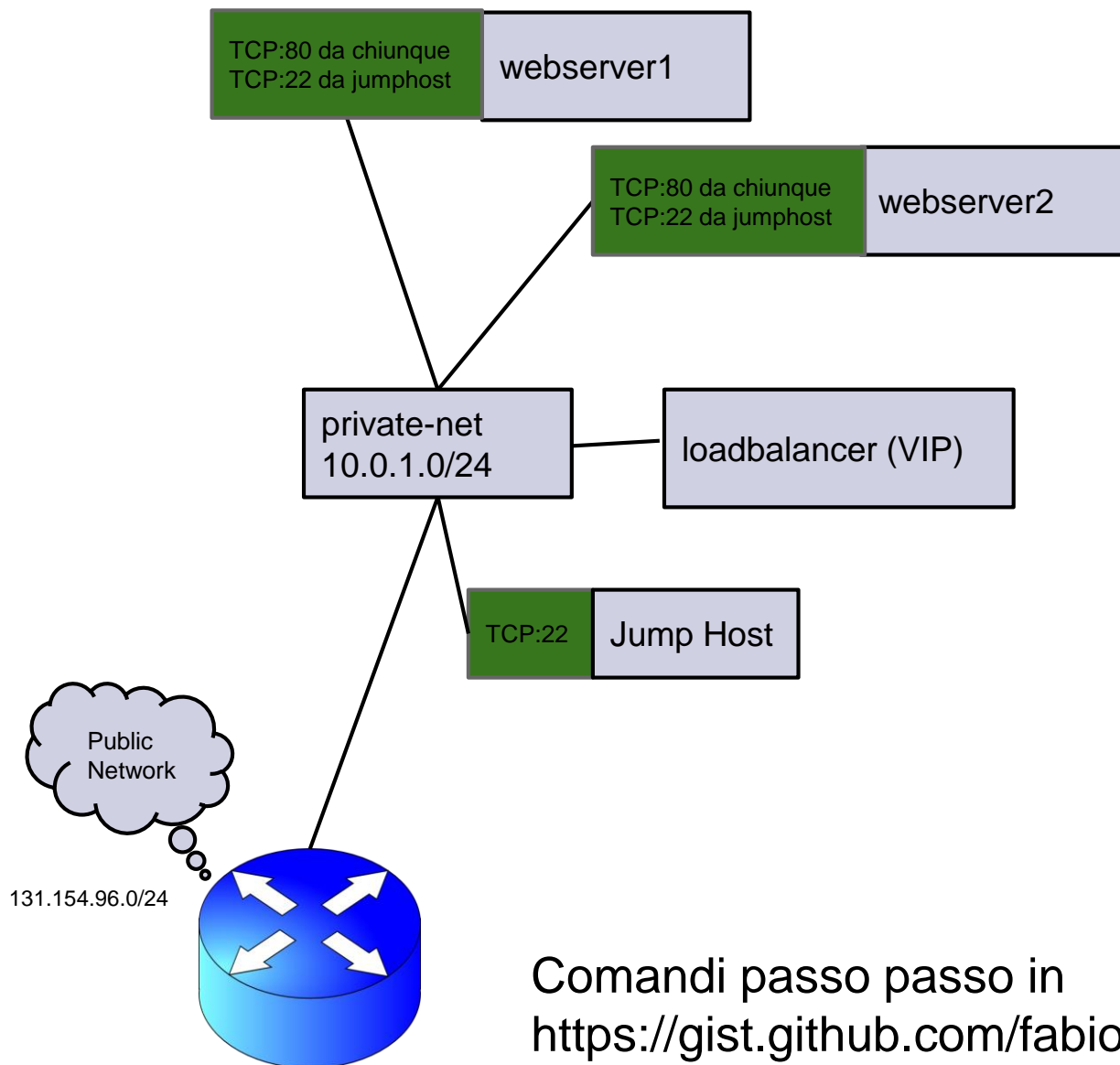


```
root@jumphost:~  
[efattibene@igi-ui ~]$ ssh -i mykey.pem cloud-user@131.154.96.114  
Last login: Wed May 21 15:24:18 2014 from 131.154.101.54  
[cloud-user@jumphost ~]$ sudo su -  
[root@jumphost ~]#
```

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

Access & Security

Logged in as: fattibene

[Settings](#)

[Help](#)

[Sign Out](#)


[Security Groups](#)

[Keypairs](#)

[Floating IPs](#)


[API Access](#)

API Endpoints

 Download OpenStack RC File

 Download EC2 Credentials

Service	Service Endpoint
Compute	http://10.10.96.3:8774/v2/1ce97bfa1927415a9b2bc834100eb331
Network	http://10.10.96.3:9696/

 Download OpenStack RC File

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"
```

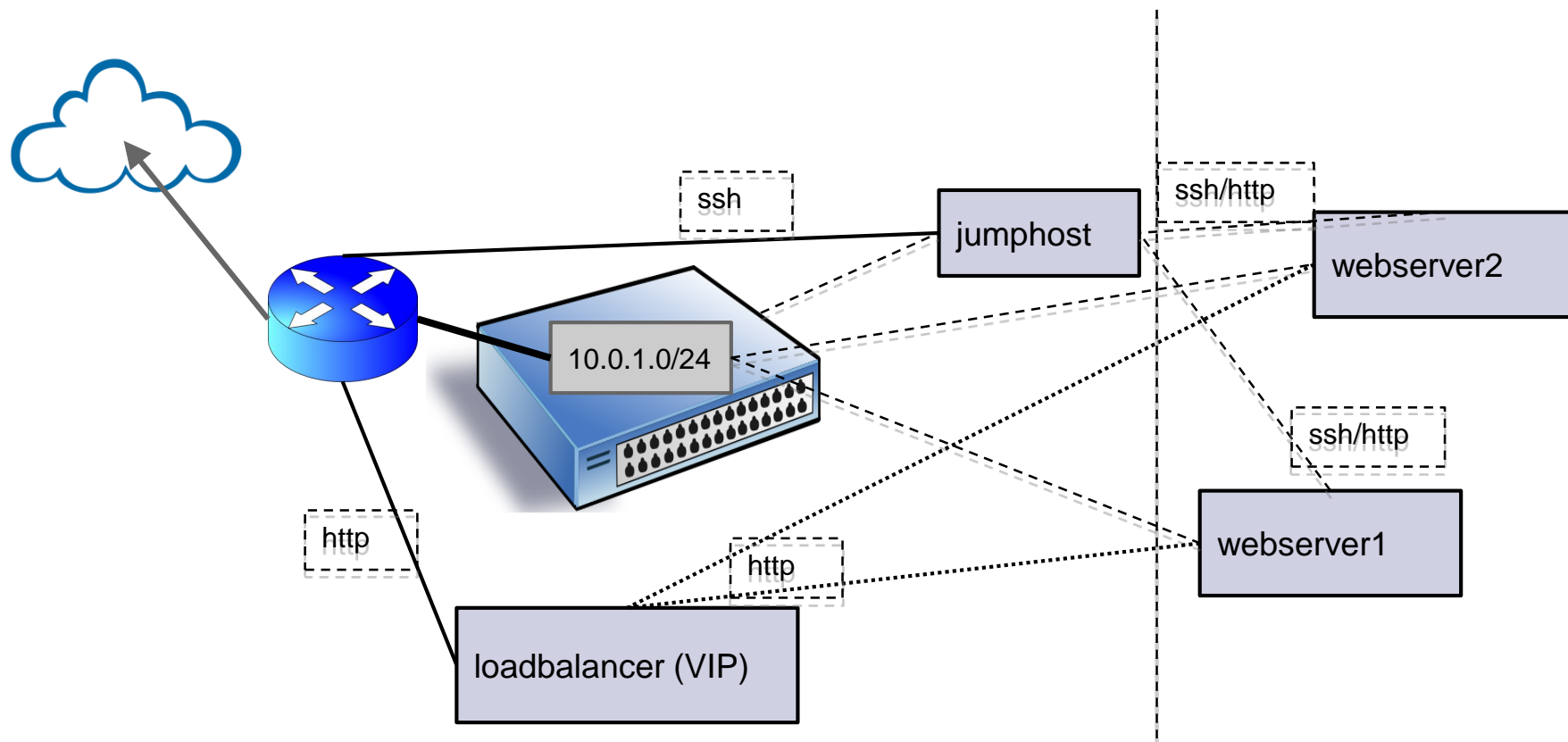
```
# In addition to the owning entity (tenant), openstack stores the entity
# performing the action as the **user**.
export OS_USERNAME="fattibene"
```

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

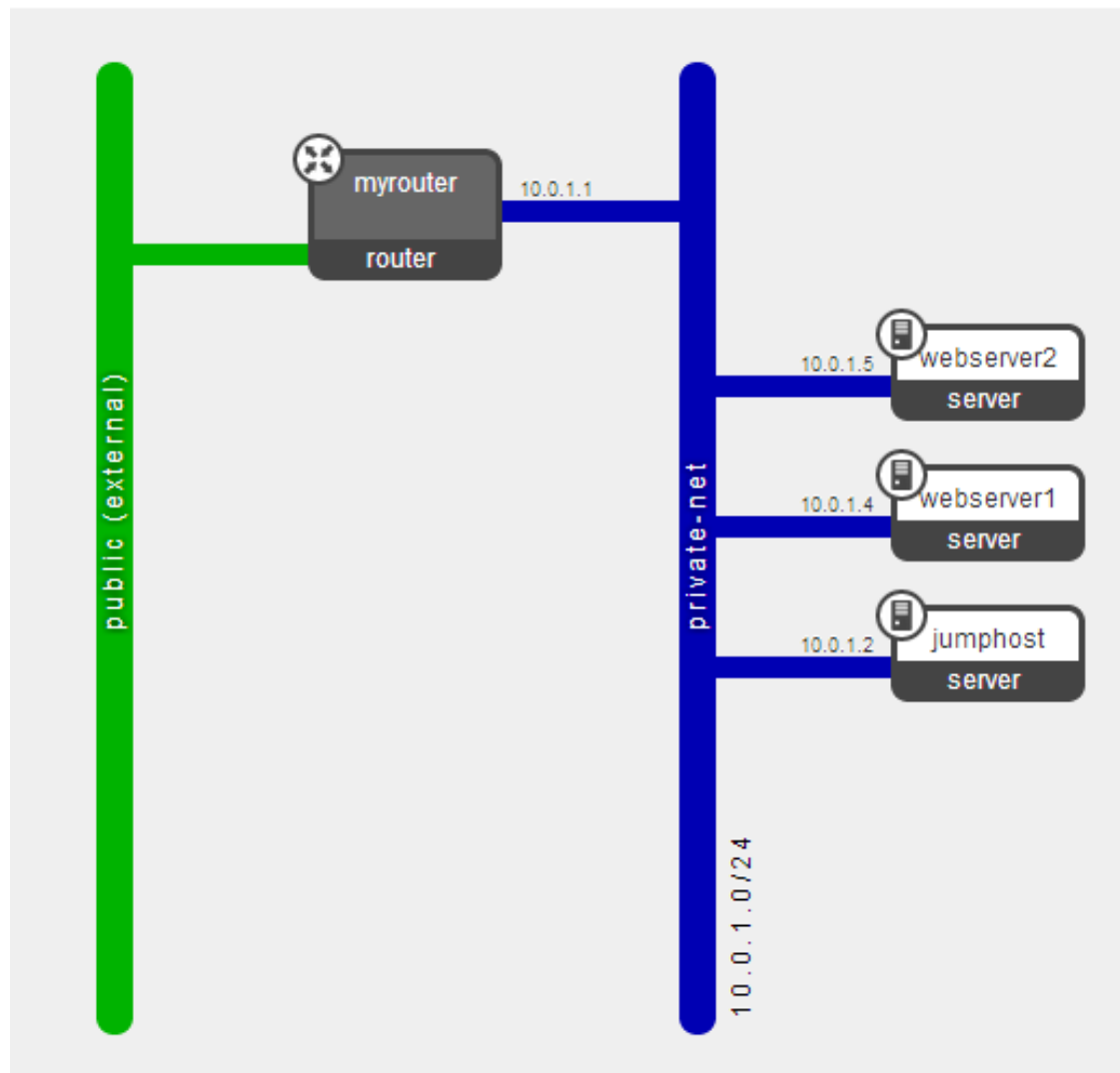
Piccola accortezza

- 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

Pools Members **Monitors**

Monitors

+ Add Monitor

Delete Monitors

<input type="checkbox"/>	ID	Monitor Type	Actions
<input type="checkbox"/>	ae19ea58-491e-4ded-928c-2f86ba75b3f1	HTTP	<div>Edit Monitor More ▾</div> <div>Delete Monitor</div>

Displaying 1 item

Pools **Members** Monitors

Members

+ Add Member

Delete Members

<input checked="" type="checkbox"/>	IP Address	Protocol Port	Pool	Actions
<input checked="" type="checkbox"/>	10.0.1.4	80	mypool	<div>Edit Member More ▾</div>
<input checked="" type="checkbox"/>	10.0.1.5	80	mypool	<div>Edit Member More ▾</div>

Displaying 2 items

LBaaS VIP e pool

Pools
Members
Monitors

Pools

+ Add Pool
Delete Pools

<input type="checkbox"/>	Name	Description	Provider	Subnet	Protocol	VIP	Actions
<input type="checkbox"/>	mypool		haproxy	10.0.1.0/24	HTTP	myvip	Edit Pool More ▼

Displaying 1 item

Edit VIP
Delete VIP
Delete Pool

Pools
Members
Monitors

Pools

+ Add Pool
Delete Pools

<input checked="" type="checkbox"/>	Name	Description	Provider	Subnet	Protocol	VIP	Actions
<input checked="" type="checkbox"/>	mypool		haproxy	10.0.1.0/24	HTTP	-	Edit Pool More ▼

Displaying 1 item

VM webserver e sec group web

Instances

[+ Launch Instance](#)
[Soft Reboot Instances](#)
[Terminate Instances](#)

<input type="checkbox"/>	Instance Name	Image Name	IP Address	Size	Keypair	Status	Task	Power State	Uptime	Actions
<input checked="" type="checkbox"/>	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
<input checked="" type="checkbox"/>	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
<input type="checkbox"/>	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](#)

<input type="checkbox"/>	Name	Description	Actions
<input type="checkbox"/>	default	default	Edit Rules
<input type="checkbox"/>	jumphost		Edit Rules More
<input checked="" type="checkbox"/>	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>