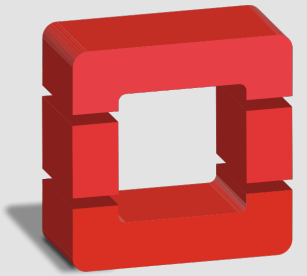
Openstack Administration 101

Infrastruttura Openstack: realizzazione e accesso

Diego Michelotto (INFN-CNAF)



openstack
CLOUD SOFTWARE

29/11/2021

Indice

- Infrastrutture per studenti
- VPN
- Accesso risorse
- Risorse per infrastrutture
- Perché sono state fatte così
- Come sono state realizzate
  - Alternative
- Hands-on

Infrastrutture per studenti

- Per i laboratori ogni studente ha a disposizione un'infrastruttura Openstack composta da 2 macchine
  - oa101-##-ctrl
    - controller node con tutti i servizi necessari per il funzionamento di Openstack (DB, RabbitMQ, ecc.) e tutti i servizi di Openstack che vedremo nel corso
  - oa101-##-hv
    - hypervisor node con i soli servizi di virtualizzazione
- Le infrastrutture sono così assegnate:
  - https://corso_oa101.baltig-pages.infn.it/hands-on/infra/overview/
  - Nella tabella sono riportati per ogni studente
    - gli IP delle macchine assegnate
    - il nome della chiave ssh da utilizzare
    - il link alla dashboard della propria infrastruttura

VM	IP	Student	SSH key file	OS project name	OS daskboard link
oa101-01-ctrl	10.10.0.10	Chierici	oa101_1	chierici	dashboard
oa101-01-hv	10.10.0.13	Chierici	oa101_1		

VPN

- Server OpenVPN interno al tenant TRAINING che ospita le infrastrutture del corso
  - Mappa client su rete virtuale 10.8.0.0/24
  - Split tunnel
    - Push della solo rete delle infrastrutture 10.10.0.0/24
    - Traffico che non è per rete 10.10.0.0/24 passa per la connessione del vostro PC
  - Autenticazione tramite certificato
    - Certificati emessi da CA interna al VPN server
    - Gestisce CRL per revoca client
  - Realizzato tramite il tool disponibile su github: https://github.com/angristan/openvpn-install
- Client
  - Windows: OpenVPN GUI: https://openvpn.net/community-downloads
  - MacOS:
    - OpenVPN Connect: https://openvpn.net/vpn-client/
    - Tunnelblick: https://tunnelblick.net/downloads.html
  - Linux:
    - Probabilmente già integrato nel desktop manager
    - Necessario il pacchetto openvpn 2.4.X ed eventuali plugin per proprio Desktop manager

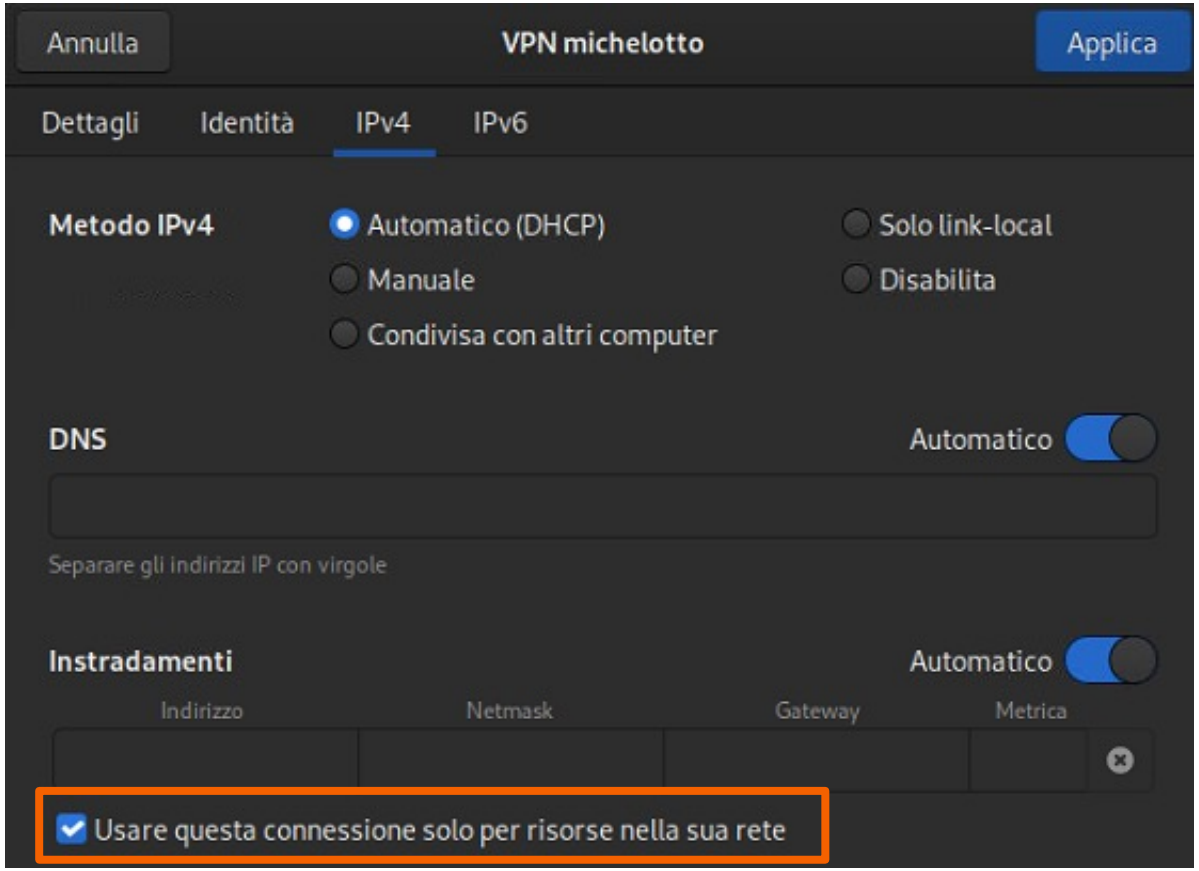
VPN

- Connessione
  - Inviato per e-mail un file di configurazione
    - Nome file: `cognome.ovpn`
- Configurazione client
  - Windows/MacOS: doppio click sul file di configurazione
  - Linux:
    - Utilizzando l'interfaccia grafica andare nelle configurazioni di rete e nella sessione VPN importare configurazione da file
    - Da terminale dare il comando `sudo openvpn --config ~/Downloads/cognome.ovpn`
      - Per terminare la sessione CTRL+C

VPN

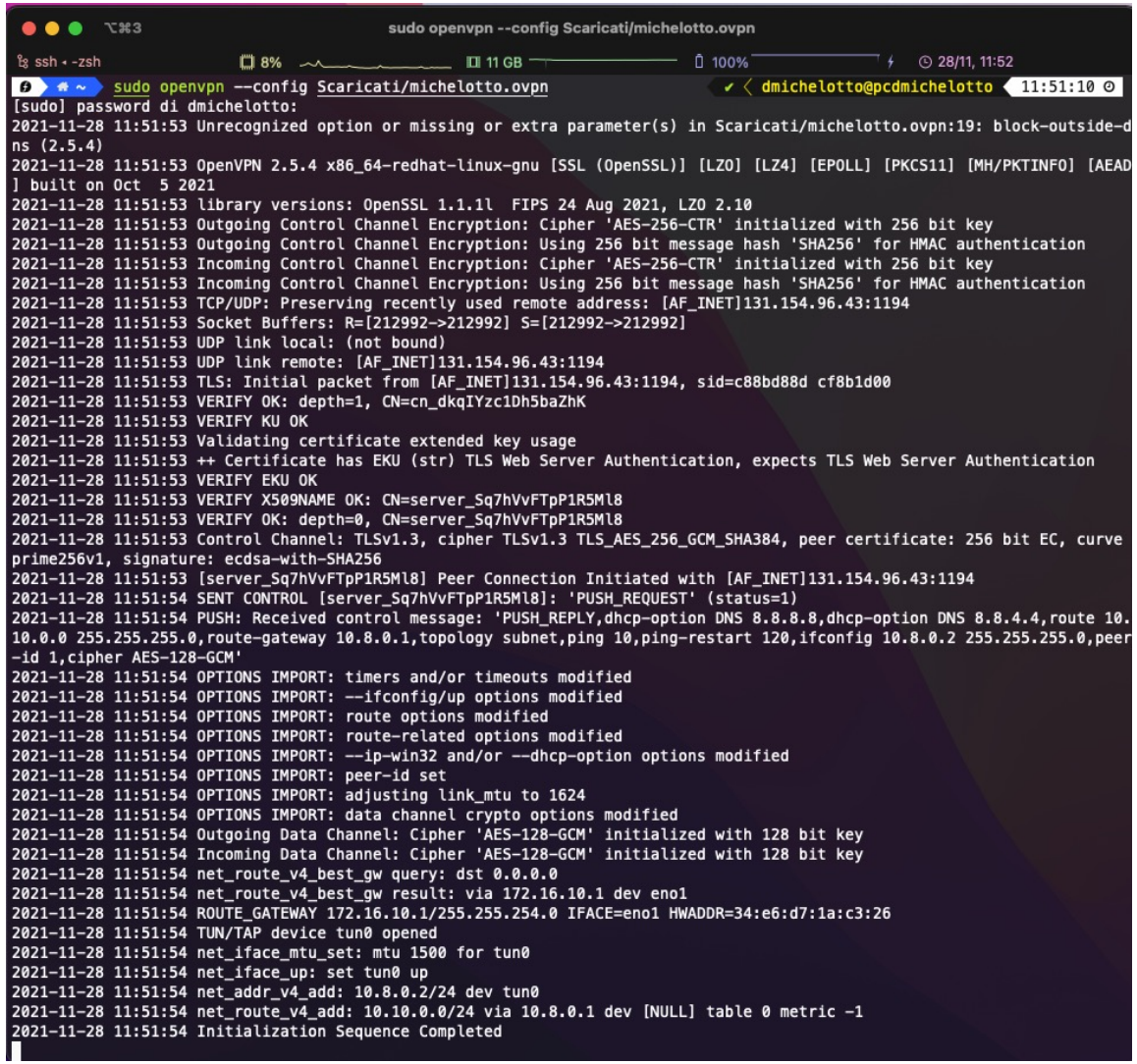
- Possibili problemi
  - Se si usa l'interfaccia grafica linux per configurare la vpn assicurarsi che sia selezionata l'opzione che redireziona il traffico verso il vpn server solo per le reti propagate dal vpn server.
    - Effetto indesiderato se non si selezione l'opzione, potrebbe non essere possibile accedere ad alcune risorse internet.
  - Per verificare controllare che non sia presente la default route verso 10.8.0.1

```
~ ip r
default via 10.8.0.1 dev tun0 proto static metric 50
default via 172.16.10.1 dev eno1 proto dhcp metric 100
```

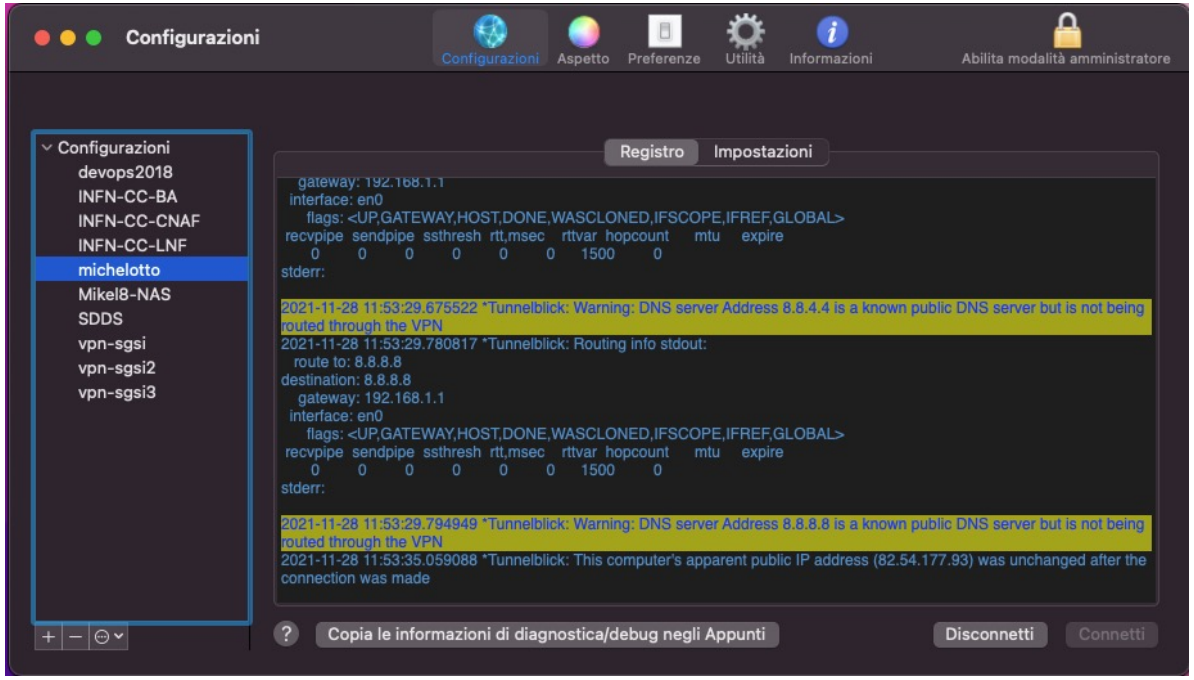


VPN

openvpn - Linux

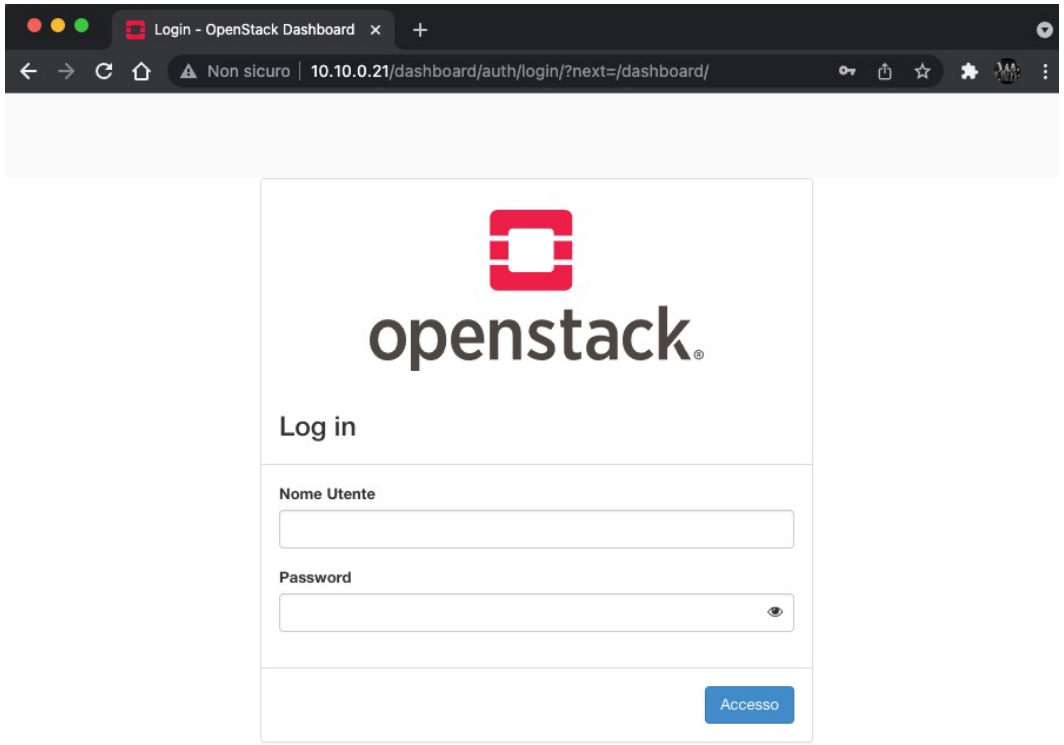


Tunnelblick - MacOS



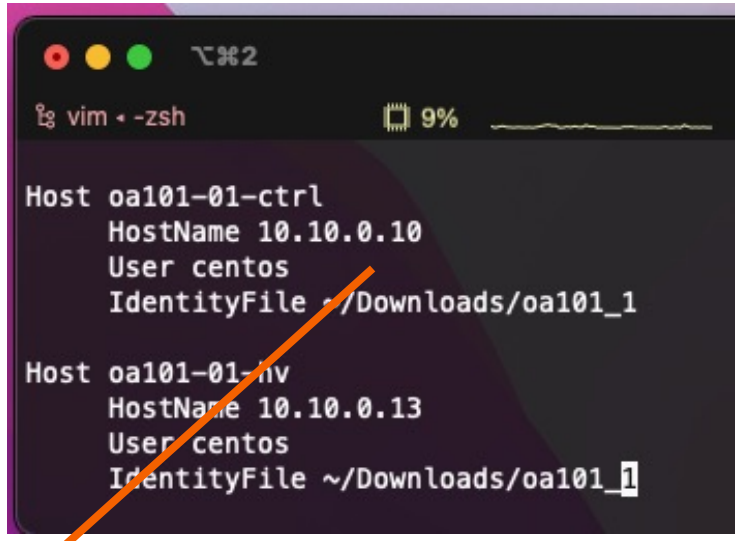
Accesso risorse

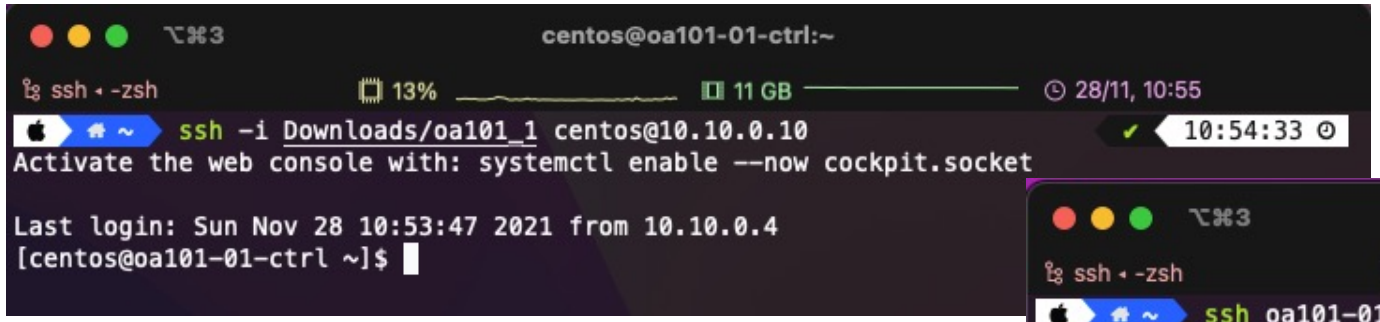
- Per raggiungere la dashboard Openstack si può
  - utilizzare il link nella tabella
  - ricavare utilizzando l'ip della macchina controller che vi è stata assegnata aggiungendo `/dashboard` dopo l'IP, il protocollo usato è `http`
    - `http://10.10.0.XX/dashboard`
- Per ogni infrastruttura Openstack ci sono due tenant/progetti
  - Un progetto «Utente»
    - Username e password inviati via email
  - Un progetto «Admin»
    - openrc file sulla macchine controller da usare con Openstack CLI.
      - Questo file contiene username e password per accedere come utente amministratore all'infrastruttura

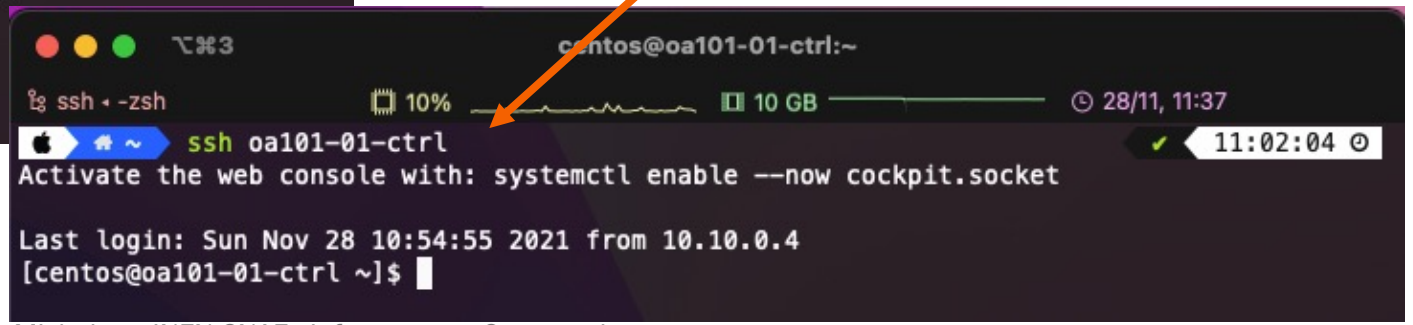


Accesso risorse

- Per accedere alle VM è necessario:
  - Essere in possesso della chiave ssh privata che avete ricevuto per e-mail
    - La chiave va salvata localmente nel posto che più vi piace
    - Per windows: la chiave va importata in base al client ssh che si utilizza
    - Per linux: si può configurare `~/.ssh/.config` per semplificare la connessione ssh, in alternativa si può usare ssh-agent ed aggiugnere la chiave
  - La connessione ssh va fatta usando l'utente `centos`
    - `chmod 600 ~/Download/oa101_1`
    - `ssh -i ~/Download/oa101_1 centos@10.10.0.XX`
  - Poi è possibile diventare root con `sudo -i`







Risorse per infrastrutture

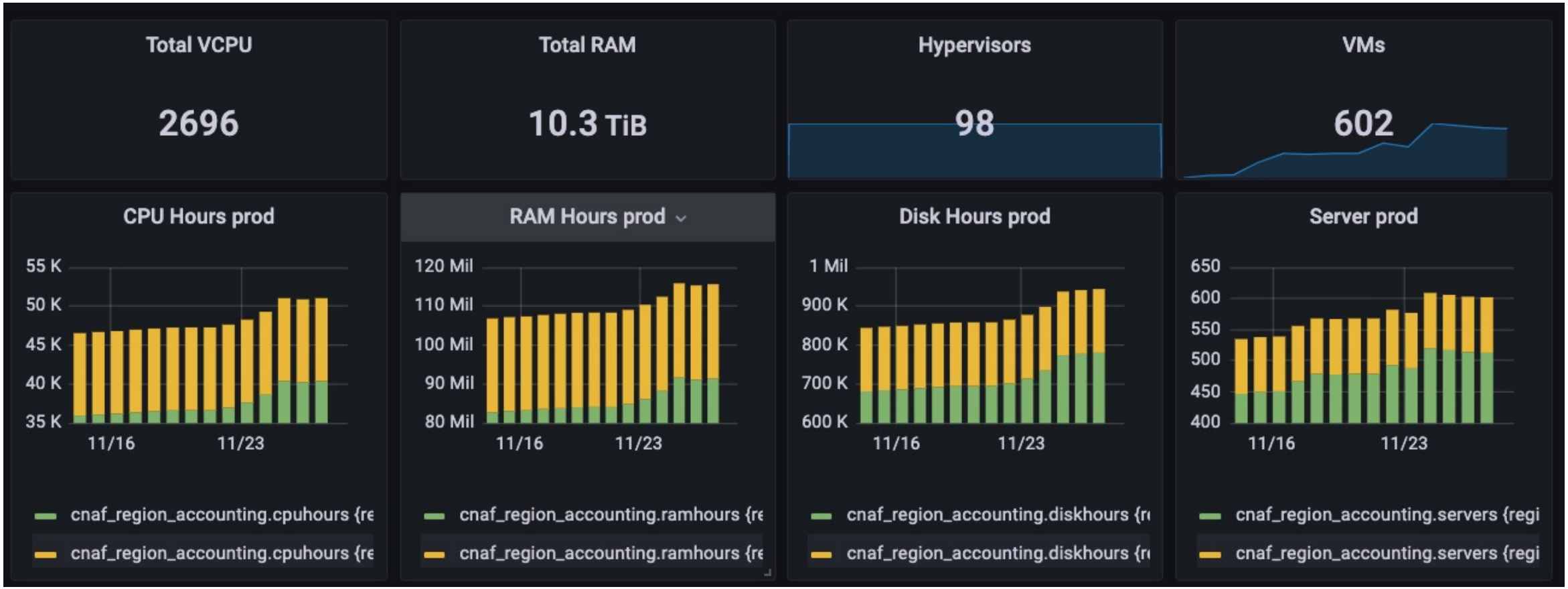
- Le infrastrutture Openstack per i laboratori sono ospitate su Cloud@CNAF
- Cloud@CNAF è l'infrastruttura Openstack del CNAF
  - Composta da 2 regioni
    - Tier1: per utilizzo cloud di risorse sotto pledge e risorse relativa al mondo WLCG
    - SDDS: per fornire interfaccia IaaS a:
      - gruppi di sviluppo del CNAF, es. servizi IAM, BIG DATA PLATFORM;
      - progetti a cui CNAF partecipa come ioTwins, ML_INFN, SUPER, CHNET, ecc.;
      - federazione con altre infrastrutture cloud come INFN-CLOUD e EGI FedCloud;
      - testbed interni come lo studio di integrazione tra sistemi di storage e K8s, testbed infrastruttura di provisioning del CNAF, ecc.
      - Staff del CNAF
      - Training
  - Risorse dispiegate in alta affidabilità tramite l'utilizzo di cluster di database, cluster di broker di messaggi, infrastrutture di storage resilienti e servizi replicati
  - …

Risorse per infrastrutture

- Cloud@CNAF è l'infrastruttura Openstack del CNAF
  - …
  - Le risorse a disposizione per gli utilizzatori sono:
    - ~2700 CPU e ~ 10TB RAM forniti da ~ 100 Hypervisor (non considerato overbooking x4 per CPU e x1.2 per RAM)
    - ~2 PB di spazio netto tra GPFS e Ceph
    - 18 GPU (V100, T4, A100)
    - Self-service network con 400 VLAN e 1500 Floating IP
  - Accesso:
    - Autenticazione tramite diverse istanze di IAM e OpenID-Connect
      - 1 specifica per cnaf integrata con INFN-AAI
      - Diverse altre istanze per progetti e federazione con INFN-Cloud
      - EGI Check-In per federazione con EGI FedCloud
    - Rete pubblica Tier1
      - Porte chiuse sotto la 1024 compresa e alcune well known, come 3306 e 8443, da general internet
      - Tutto aperto da LHCOPN/ONE
    - Rete pubblica SDDS
      - Rispetta le RoP di INFN-Cloud con porte 22, 80 443 aperte anche da general internet (lista non esaustiva)
      - Accesso limitato e controllato verso il resto del CNAF per motivi di sicurezza e isolamento.

Risorse per infrastrutture

- Cloud@CNAF è l'infrastruttura Openstack del CNAF
  - ...
  - Gestisce dalle 500 alle 600 istanzie giornalmente di cui circa 450 costantemente running
  - Fornisce risorse per cluster K8s di produzione, es. cluster che ospita servizi IAM



Perché sono fatte così

- Perché non aprire le porte invece di usare la VPN?
  - Principalmente per sicurezza
    - Per rendere pienamente utilizzabile le infrastrutture e permettere il corretto funzionamento delle reti private e pubbliche è necessario disattivare alcune funzionalità di sicurezza di Openstack (port security).
    - Per aumentare isolamento da possibili attacchi malevoli dall'esterno su risorse non protette
  - Per utilizzare correttamente tutte le funzioanlità della dashboard, come la console delle VM.
    - Vengono fatti redirect su indirizzi interni al tenant che ospitata le risorse
  - Per poter utilizzare i Floating IP all'interno del'infrastruttura Cloud@CNAF

Come sono state realizzate

- Tutte le infrastrutture per i laboratori sono:
  - Alla versione Wallaby
    - l'ultima versione è Xena rilasciato ad Ottobre
  - Installate su CentOS Stream 8
    - Dipendenza di Wallaby
      - CentOS 8 supportato fino a Victoria (versione precedente a Wallaby)
      - CentOS 7 supportato fino a Train (3 versioni precedenti a Wallaby)
    - L'alternativa era Ubuntu 20, ma abbiamo maggiore esperienza con le release CentOS
      - Le funzionalità di Openstack, che sono lo scopo del corso, non cambiano in base alla distribuzione.
  - Configurate utilizzando Packstack
    - Rispetto al default:
      - non è stato installato aodh: allarmistica
      - non è stato installato ceilometer: accounting uso risorse
      - Installato heat: orchestrazione di risorse
      - Installato magnum: cluster as a service
      - disattivato OVN in favore di OVS come provider di virtual networking

Come sono state realizzate

- Packstack
  - Parte del progetto RDO
    - Comunità di persone che utilizzano e installano Openstack su sistemi RedHat e derivati come CentOS e Fedora
    - https://www.rdoproject.org/
  - Tool per installare un'infrastruttura cloud proof of concept
    - https://www.rdoproject.org/install/packstack/
    - Basato su puppet headless, e moduli puppet distribuiti con i repository RDO
      - http://mirror.centos.org/centos/8-stream/cloud/x86_64/openstack-wallaby/Packages/p/
  - Possibilità di installare infrastruttura all-in-one
  - Possibile aggiungere altri nodi, hypervisor
    - Connessione tramite ssh per configurare il secondo nodo utilizzando sempre puppet
  - Possibilità di installare tutti i servizi Openstack
    - Tutti i servizi sono in versione demo, per es. utilizzano storage locale e loop device per condividere storage
    - Non sono contemplate installazioni in alta affidabilità

Come sono state realizzate

- Packstack
  - Alternative all-in-one
    - Microstack per Ubuntu
  - Alternative per installazione automatica di Openstack
    - TripleO: Parte di RDO usato per installazione Openstack/RHOSP su sistemi operativi ReHat based
      - Installa componeti di alta affidabilità
      - Fa il setup anche dello storage basato su Ceph
      - Openstack On Openstack: usa un controller Openstack per fare il provisioing, configurazione e upgrade dell'infrastrttura Openstack
      - Basato su ansible
      - Misto rpm e container
    - JuJu: Parte di Canonical usato per installare Openstack su sistemi operativi Ubuntu Server
      - Installa componeti di alta affidabilità
      - Fa il setup anche dello storage basato su Ceph
      - Usa un controller per fare il provisioing, configurazione e upgrade dell'infrastrttura Openstack tramite l'utilizzo di LXD containers, ogni servizio cloud è un Charm https://charmhub.io/?base=all&filter=cloud
    - Puppet
    - Ansible
    - Ref: https://docs.openstack.org/wallaby/deploy/

Domande

Hands-on

- Trovare le informazioni relative alle proprie macchine
- Installare e configurare VPN client
- Stabilire connessione con VPN server
- Accedere alla propria dashboard con le credenziali
- Accedere via ssh alle proprie macchine

- Ref: https://corso_oa101.baltig-pages.infn.it/hands-on/infra/overview/