# Corporate Cloud: stato e sviluppi

Giacinto Donvito

INFN Sez. di Bari

On behalf of the INFN-CC Group

# Agenda

- Stato dei siti
- Stato delle attività
- Roadmap (??)
- Problemi previsti
- Considerazioni e Conclusioni

# Reminder sugli use-case

## quali use case?

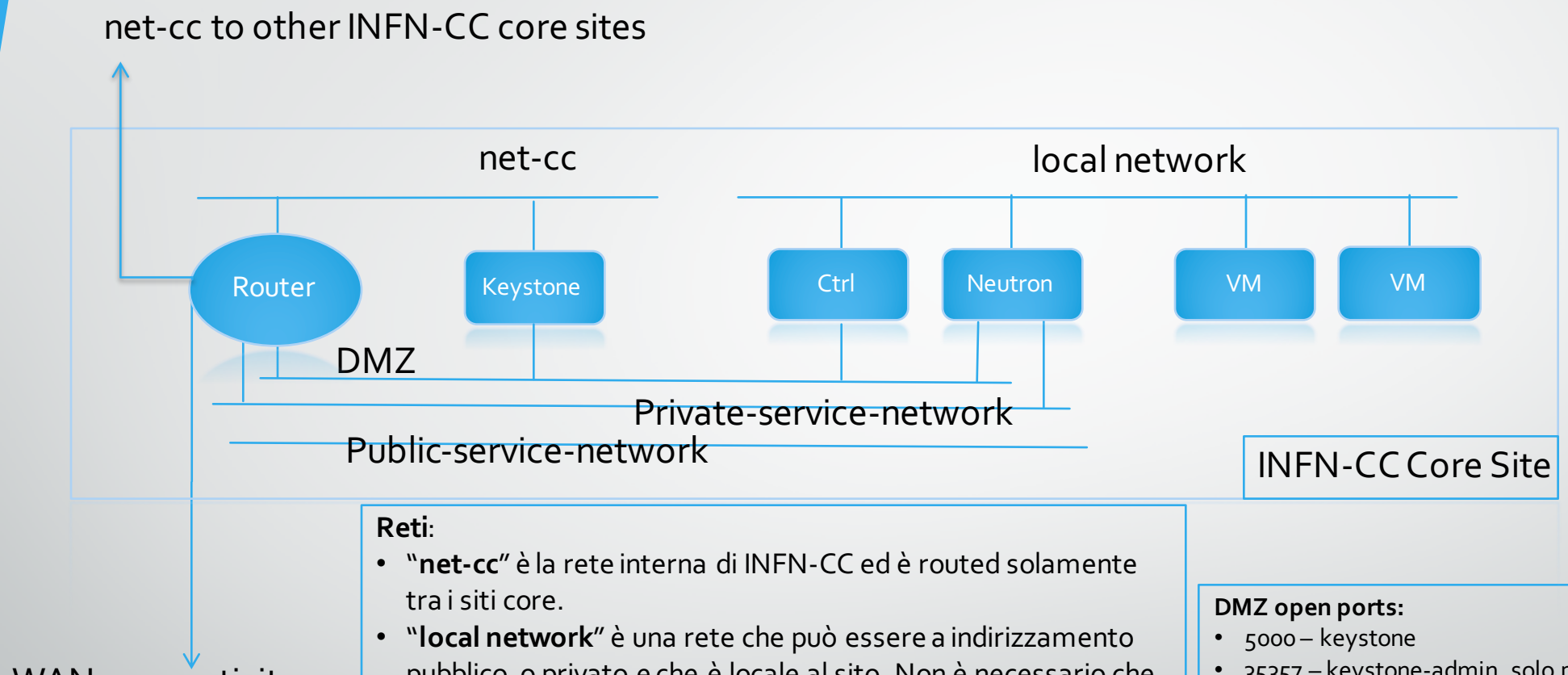
- il **backup dei servizi locali** può essere un primissimo uso, per fare da battistrada
- **servizi locali** (web sites, web applications, mailing lists, e-learning, collaborative tools, data backup)
- **servizi nazionali** (quelli adatti), **trasferiti su cloud** → **INFNBox**
- **servizi** nazionali (e non) **pensati e costruiti su cloud**
- alcuni use case di **calcolo scientifico**

*t*

# Stato dei siti

- Finalmente sono stati **individuati** i **tre siti** con cui partire:
  - **INFN-CNAF, INFN-LNF, INFN-Bari**
- Anche il gruppo di persone che si impegneranno a vario titolo nel progetto:
  - **INFN-LNGS:** Stefano Stalio
  - **INFN-CNAF:** Stefano Zani, Donato de Girolamo, Lorenzo Chiarelli, Cristina Aiftimiei, Matteo Panella, Diegno Michelotto, e altre persone (ancora da definire)
  - **INFN-Bari:** Giacinto Donvito, Alessandro Italiano, Marica Antonacci, Roberto Valentini
  - **INFN-LNF:** Massimo Pistoni, Dario Spigone, Tommaso Tonto e altre persone (ancora da definire)
  - **INFN-Roma 2/3**: Federico Zani, Antonio Budano

# INFN-CC: set-up di un core site




**Reti**:

- "**net-cc**" è la rete interna di INFN-CC ed è routed solamente tra i siti core.
- "**local network**" è una rete che può essere a indirizzamento pubblico o privato e che è locale al sito. Non è necessario che sia esposta all'esterno.
- "**DMZ**" è una rete pubblica specifica di ogni sito core, esposta verso l'esterno e con un set controllato di porte aperte.
- "***-service-network**" sono le reti (pubblica e privata) dedicata ad esporre i servizi degli utenti
  - La "**private**" può essere usata per servizi raggiungibili con una VPN lato user

**DMZ open ports:**

- 5000 – keystone
- 35357 – keystone-admin, solo per siti INFN
- 443 – dashboard
- 8080 – swift

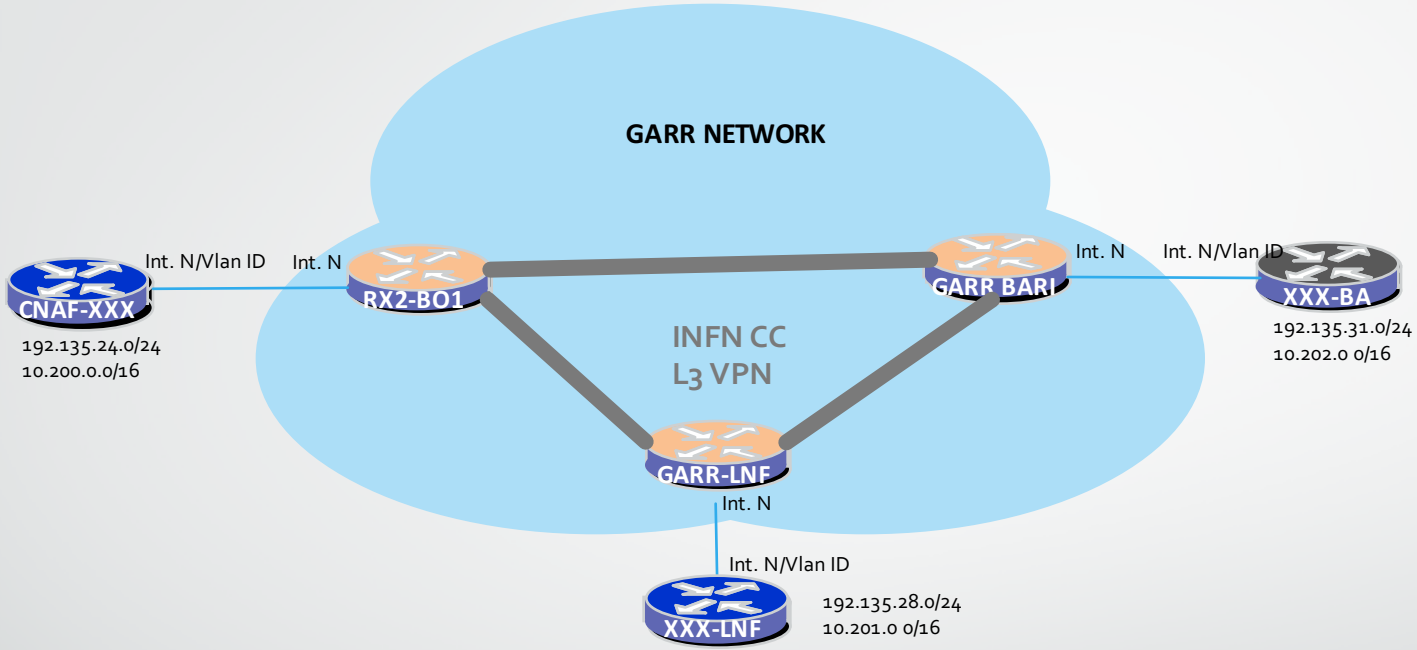
**service-network open ports (example):**

- 22 – ssh
- 80, 443 – www
- Altre porte su richiesta

# Stato dei siti: Networking

- Sono state individuate le configurazioni di rete almeno ad alto livello:
  - Accordo di massima con il GARR per una L3 VPN fra i tre siti
  - Sulla VPN passano tutte le reti private fra i tre siti
  - Tutte le comunicazioni sulle reti private sono quindi isolate, e sarà possibile rilassare tutti i requirements di sicurezza
- Ogni pubblic-service-network sarà allocata staticamente ad un sito.
- La private-service-network sarà disponibile per gli utenti che non hanno bisogno di una macchina su IP pubblico
  - Sarà necessario predisporre "VPN server" in tutte e tre le sedi con la visibilità delle tre reti private in modo assolutamente trasparente
- La DMZ sarà un quarto di una Classe C routata
  - un quarto per sito

# INFN CC -- Network Layout




## CNAF

Ptp:
Public:192.135.28.0/24
DMZ: un quarto di 192.135.32.0/24
Private:10.200.0.0/16

Si usa una nuova interfaccia dedicata sul VDX

## LNF

Ptp:
Public:192.135.24.0/24
DMZ: un quarto di 192.135.32.0/24
Private:10.201.0.0/16

Proposta VLAN 929 Subinterface (logic)
-> Interfaccia fisica 10Gbit/s non quella del Tier2

## BARI

Ptp:
Public:192.135.31.0/24
DMZ: un quarto di 192.135.32.0/24
Private:10.202.0.0/16

Si usa una nuova interfaccia dedicata su Huawei

**Thank to Stefano Zani**

# Stato delle attività

- Individuate alcune persone che si occuperanno di tirare le file delle attività:
  - **Tecnologia**: Stefano Stalio, Cristina Aiftimiei
  - **Infrastruttura**: Giacinto Donvito
- Le classi di indirizzamento sono tutte quasi confermate (sia pubbliche che private)
- Le configurazioni sugli apparati dei tre siti sono quasi confermate
  - Per Bari e LNF possono sia supportare una infrastruttura di test che di produzione
  - Per il CNAF sarà necessario una migrazione ad una configurazione diversa per la messa in produzione dell'infrastruttura

# Stato delle attività

- Nei prossimi giorni sarà inviato un documento al GARR con tutti i dettagli tecnici per chiedere formalmente l'attivazione della L3 VPN
- Non appena il set-up della VPN sarà implementato, partiranno dei test di funzionalità
  - Anche con sw diversi da OpenStack

# Roadmap (??)

- Test L3 VPN
- Test di file-system distribuiti (CEPH, GPFS) in un ambiente con latenza ~9ms
- Decisione finale sulla configurazione di OpenStack (multi-regione, unica istanza)
- Installazione dei servizi core prima di OpenStack: Foreman/Puppet, private DNS, Mysql, AAI LDAP slave, Log Server, Storage
- Decisione sulla release di OpenStack da installare: Liberty?

# Problemi Previsti

- I siti sono ad una latenza "interessante" per sperimentare nuove configurazioni
- Il team è "nuovo" e piuttosto numeroso
- Capire come si comportano i sistemi di storage a questa latenza
- Implementare procedure di HA furbe per i servizi utenti (DNS, Replica asyncrona, etc)
- Richiederà uno sforzo importante passare da un ambiente di test ad un sistema in produzione e supportato con una certa SLA
  - Da definire in base agli use-case che vorremo ospitarci

# Considerazioni e Conclusioni

- Oltre all'esperienza del Cloud-MultiRegione, RMLab è un bagaglio di know-how importantissimo
- (IMO) L'unica possibilità per far funzionare il progetto è un approccio basato su:
  - Amministrazione distribuita e condivisa
  - Automazione completa (Foreman/Puppet) di tutti gli step
- È importante cominciare subito con degli use-case, magari semplici che siano implementabili in produzione per invogliare le persone ad usare il sistema.
- Mi aspetto un contributo importante in termini di nuove tecnologie e nuovi sw anche dal progetto INDIGO