INFN corporate cloud

stato e prospettive

cloud-mr

cloud-mr inizia come attività R&D a fine 2013

- indagine su scelte tecnologiche e architetturali da adottare per la realizzazione di una cloud OpenStack distribuita su più siti INFN
- implementazione di un ambiente di test funzionante

da cloud-mr a INFN corporate cloud

dopo il mini-workshop CCR/evento formativo a Napoli (dicembre 2014) ed una riunione ristretta (marzo 2015)

- riconosciuto il valore di questo approccio per l'INFN
- CCR supporta il progetto
- le sue sedi saranno datacenter INFN già dotati di infrastrutture adeguate e collegati al GARR attraverso fibra proprietaria

obiettivi

- realizzare una infrastruttura **IaaS** dove dati e servizi possano essere replicati su scala geografica in maniera semplice o, dove possibile, assolutamente trasparente all'utente
- questa infrastruttura deve poter essere gestita anche da persone che non risiedono nelle sedi ospitanti
- permettere la realizzazione di servizi sulla rete che non soffrano di discontinuità operative
- rendere i dati accessibili sempre e dovunque
- **PaaS** e **SaaS** realizzabili come sovrastrutture

perché?

- **ottimizzazione delle risorse**
- miglioramento della **qualità e della continuità operativa dei servizi** di/sulla rete
- **HA geografica** e **Disaster Recovery**

attività pregresse

le attività del gruppo di lavoro cloud-mr, ora INFN-CC, sono state documentate periodicamente

- CCR workshop - autumn 2013
- CCR Workshop - winter 2014
- CCR Workshop - spring 2014
- CCR Workshop on Cloud - autumn 2014
- CCR Workshop - spring 2015

- Documento architetturale

(in fase di stesura)

attività attuali

rispetto a questa primavera non ci sono grandi novità dal punto di vista implementativo

- stiamo pensando a come affrontare problemi gestionali ed amministrativi
- in base alle esperienze pregresse, stiamo dettagliando l'architettura finale
- scrittura documento tecnico architetturale

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**
- **servizi** nazionali (e non) **pensati e costruiti su cloud**
- alcuni use case di **calcolo scientifico**

t

orientata ai servizi

- l'esistenza della corporate cloud non è una costrizione ma un'**opportunità** per tutti i gestori di servizi locali o nazionali all'interno dell'INFN
- ci aspettiamo che, come spesso accade, sia la disponibilità della piattaforma a stimolarne l'utilizzo ...
- … se dimostrerà di funzionare bene

utenti

- utenti INFN
  - end user che vogliano istanziare risorse disponibili su INFN-CC
  - gestori di servizi che vogliano utilizzare INFN-CC come infrastruttura di supporto
- siti INFN con infrastrutture cloud locali

high level overview


Computing resources


Storage resources

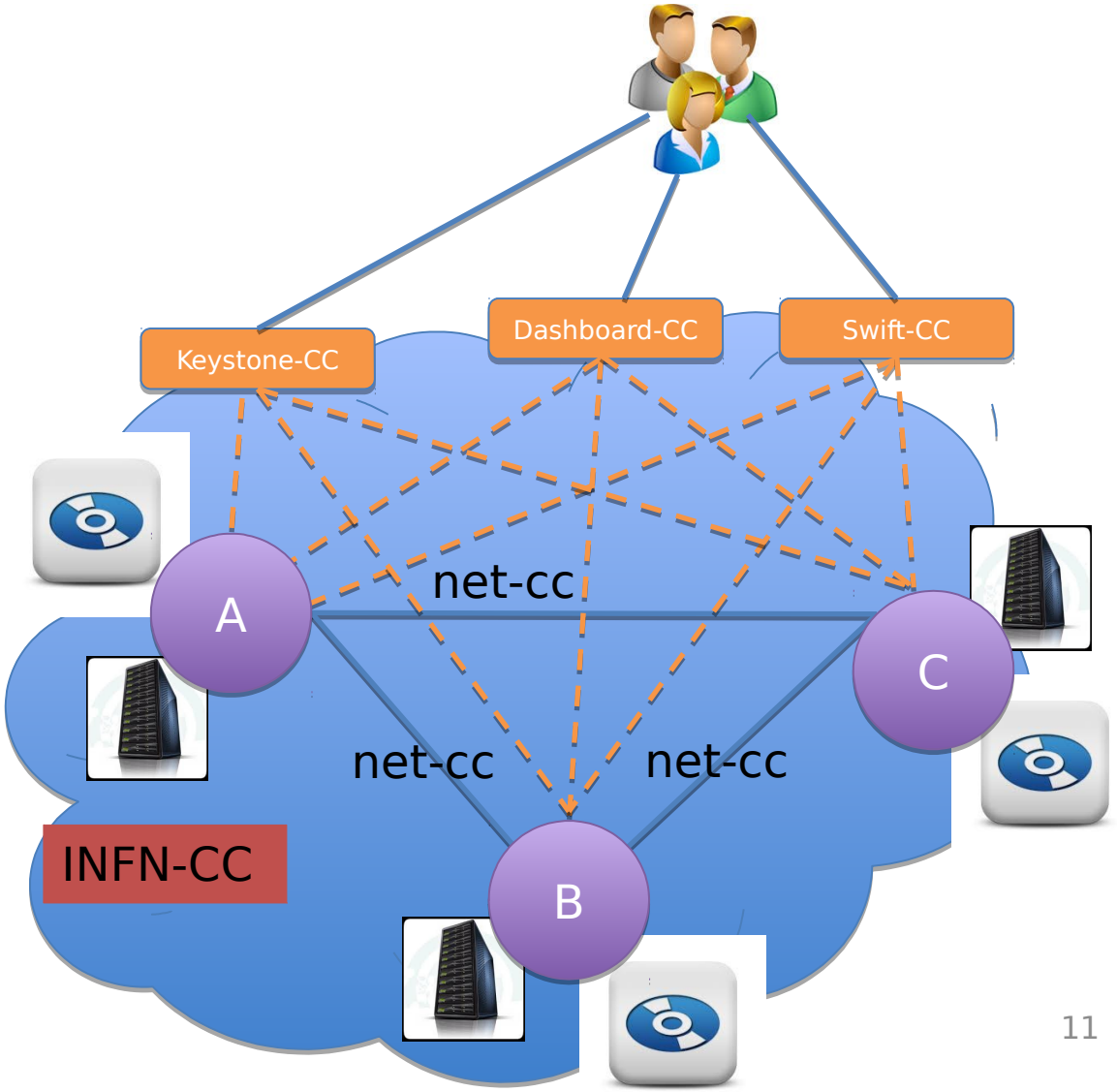
net-cc INFN-CC internal network

INFN-CC core site


INFN users


Non-INFN users

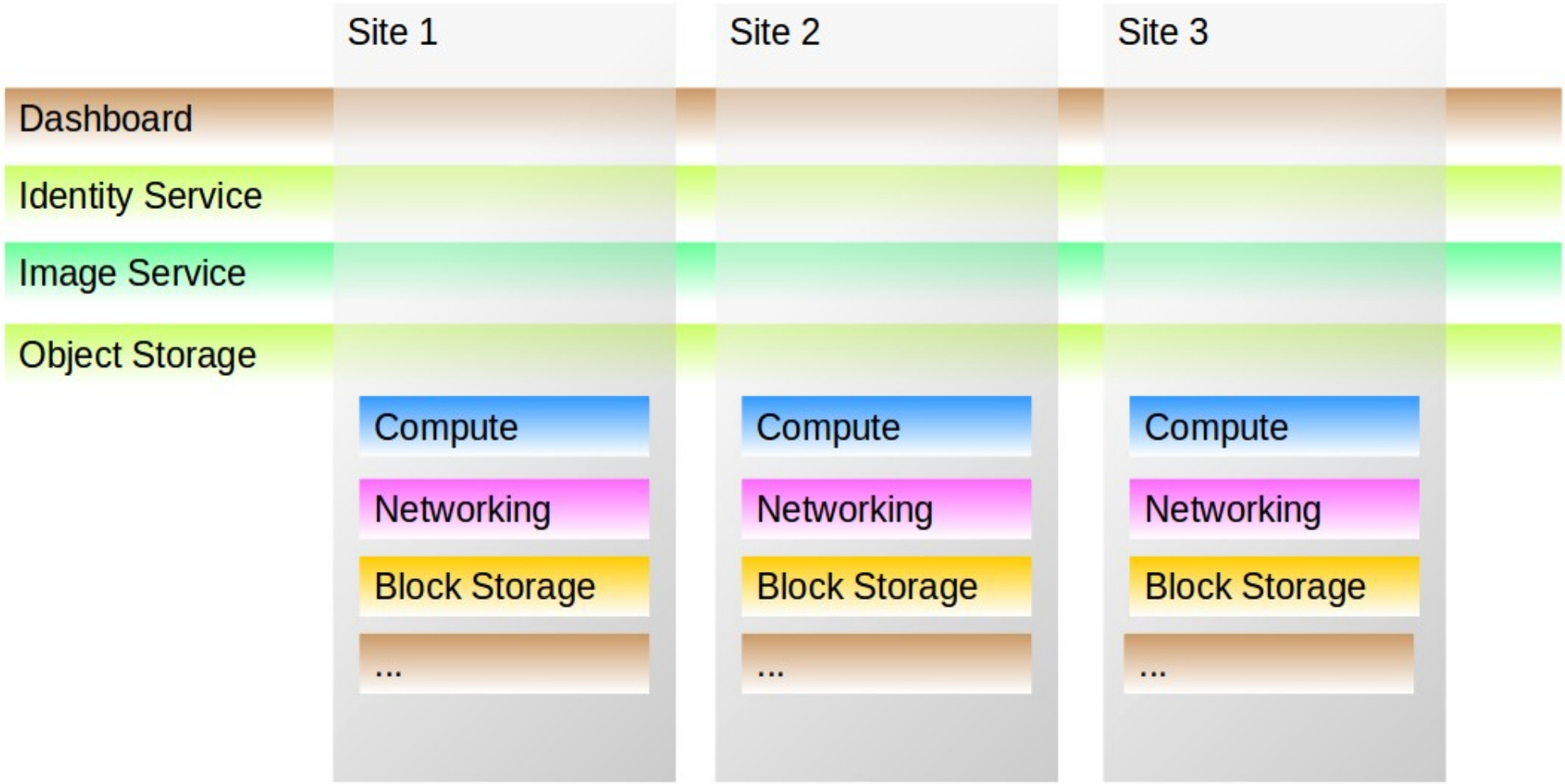
xx-CC INFN-CC service



core services

- i servizi Keystone, Swift, Dashboard e Glance sono comuni tra i core site
- i servizi Nova, Cinder e Neutron sono implementati indipendentemente da ogni core site
- La modalità di implementazione di altri servizi che verranno aggiunti in futuro dipenderà dalle caratteristiche del servizio
- i servizi di infrastruttura e gli API endpoint sono parte di una DMZ
- i servizi di infrastruttura sono ridondati utilizzando DNS HA

architettura



core services “comuni”

- Keystone e Dashboard **devono** essere comuni in una cloud a più regioni per esigneze architetturali
- Swift e Glance non devono essere comuni in una cloud a più regioni ma la convenienza di una simile implementazione è abbastanza evidente

swift

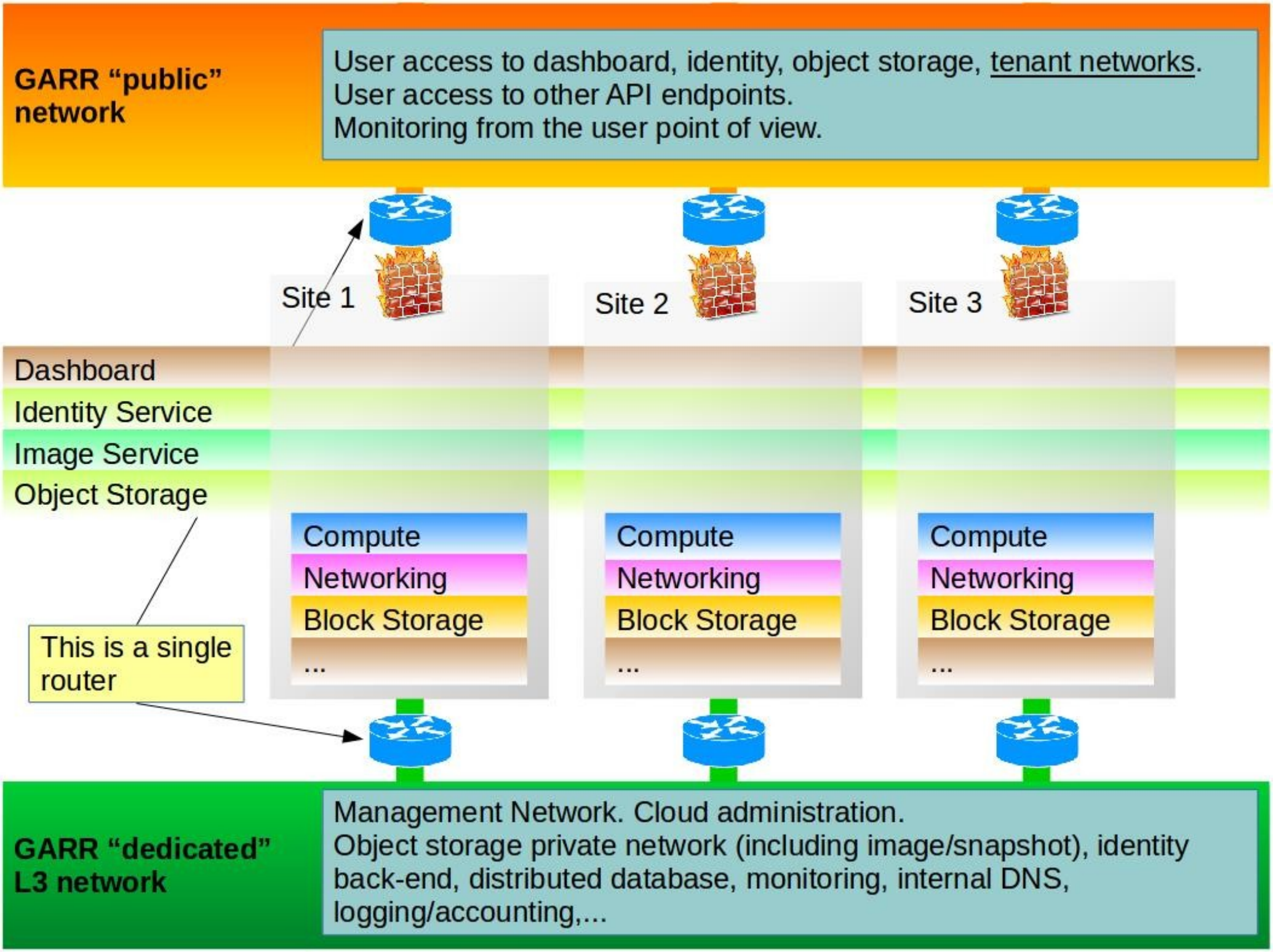
- gli utenti possono caricare dati che poi saranno distribuiti e replicati geograficamente
- backup di block device cinder, poi accessibili in tutte le regioni
- immagini e snapshot glance disponibili in tutte le regioni

glance

- le stesse immagini e gli stessi snapshot sono disponibili sull'intera INFN-CC
- una VM può essere migrata (cold migration) da una regione all'altra
- è possibile per un utente creare un HAProxy per load balancing su istanze collocate su regioni diverse di INFN-CC
- in una seconda fase sarà possibile definire un servizio di orchestrazione di servizi con Heat, disponibile multi-region da Kilo in poi.

network layout

una delle idee è quella di isolare le reti di gestione dalla rete GARR, seguendo la strada già percorsa da Rmlab, attraverso una L3 “vlan” che interconnetta le sedi della INFN corporate cloud. questo permetterebbe una gestione più snella dell'infrastruttura


GARR “public” network
User access to dashboard, identity, object storage, tenant networks.
User access to other API endpoints.
Monitoring from the user point of view.
Site 1
Site 2
Site 3
Dashboard
Identity Service
Image Service
Object Storage
Compute
Networking
Block Storage
...
Compute
Networking
Block Storage
...
Compute
Networking
Block Storage
...
This is a single router
GARR “dedicated” L3 network
Management Network. Cloud administration.
Object storage private network (including image/snapshot), identity back-end, distributed database, monitoring, internal DNS, logging/accounting,...

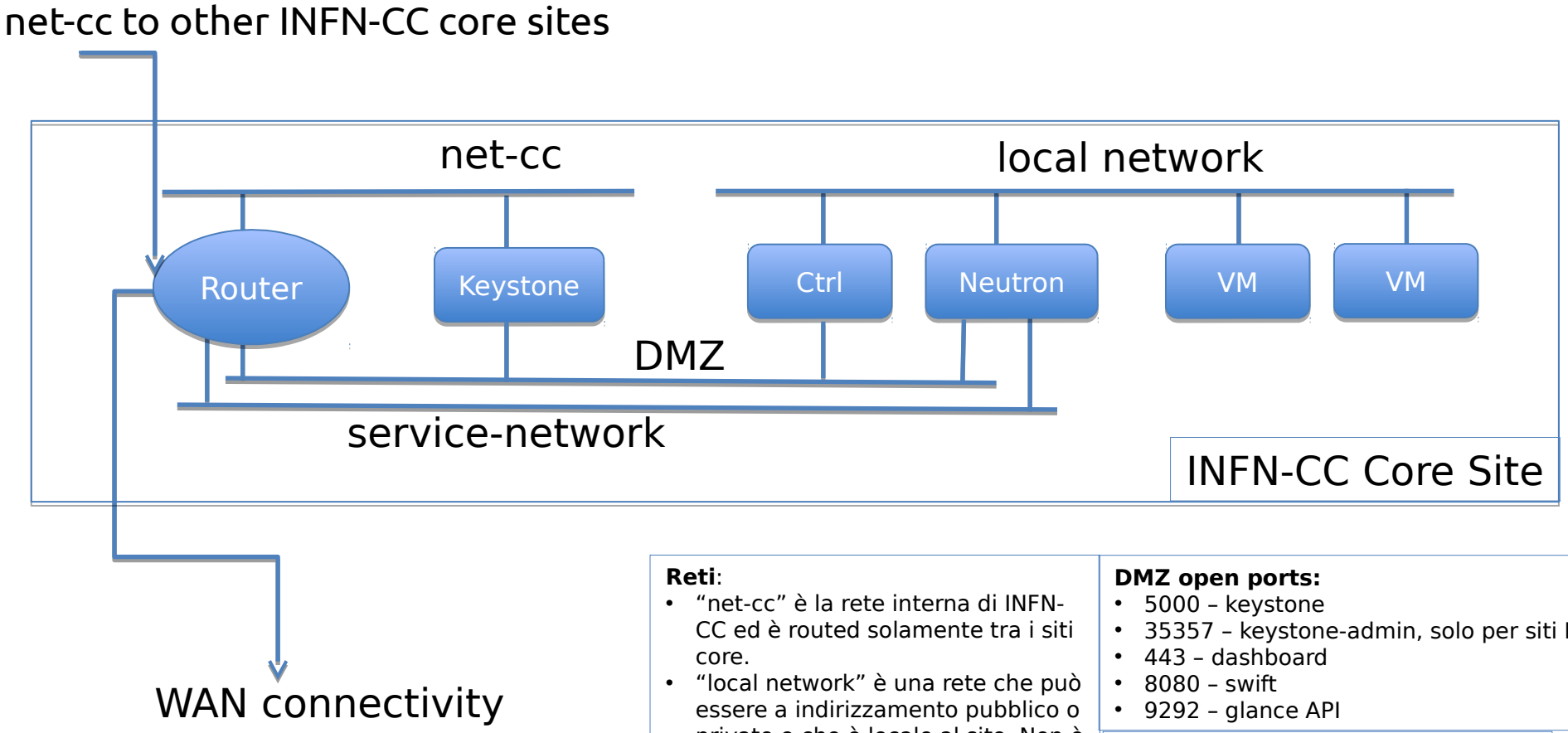
network layout

le reti di accesso (quelle che permettono di accedere ai servizi cloud e le reti dei tenant) potrebbero essere attestate su un link dedicato verso il GARR ed, in principio, potrebbero avere APM e responsabili diversi rispetto alla rete del sito.

network layout

- per ogni sito core viene definita una rete dedicata al traffico pubblico delle istanze degli utenti. questa rete è separata dalla DMZ per consentire flessibilità nella definizione delle policy di rete e di firewalling.
- vengono identificati tre siti core (INFN-CC Core Sites) che espongono i servizi indicati. i siti core appartengono a diverse regioni OpenStack.
- i collegamenti interni a INFN-CC non sono visibili all'esterno e stanno su rete privata. il GARR è disponibile a collaborare per realizzare una connessione tra i siti core anche con banda minima garantita

setup 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" è una rete pubblica dedicata ad esporre i servizi degli utenti

DMZ open ports:

- 5000 – keystone
- 35357 – keystone-admin, solo per siti INFN
- 443 – dashboard
- 8080 – swift
- 9292 – glance API

service-network open ports (example):

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

network security

- proponiamo la **creazione di un gruppo di lavoro** composto di persone con esperienze diverse (persone di corporate cloud e di altri progetti cloud, responsabili dei servizi, gestori della rete, ...)
- compito di questo gruppo di lavoro sarà di definire i requirement che la INFN corporate cloud dovrà soddisfare in termini di ***network security***, di aiutarci ad individuare le criticità che presenta l'architettura proposta e di proporre soluzioni atte a superarle
- abbiamo bisogno di una risposta in tempi brevi (due mesi) per poter inserire il risultato del loro lavoro nel documento architetturale di INFN corporate cloud

modello di gestione

- abbiamo cominciato a pensare ad un modello di gestione dell'infrastruttura e ad abbozzare un testo da includere all'interno del documento di descrizione architetturale di INFN corporate cloud.
- non è scritto sulla pietra, anzi necessita di feedback e modifiche

https://docs.google.com/document

ruoli

- **site admin**
  - system administrator c/o datacenter
  - gestisce l'infrastruttura
- **cloud admin**
  - system administrator presso servizio calcolo e reti in sede INFN
  - gestisce il middleware OpenStack

ruoli

- **domain admin**
- **tenant admin**
- **instance admin**
  - system administrator in forze presso l'esperimento o progetto
  - sono utenti OpenStack
  - realizzano, gestiscono e rispondono dei servizi IT sulla cloud

ruoli

- **user**
  - accede ai servizi forniti attraverso la cloud senza esserne utente diretto
  - non ha ruoli amministrativi

interazioni

sono di fondamentale importanza per la riuscita di INFN corporate cloud l'interazione, la collaborazione e lo scambio di know-how con altri progetti cloud INFN: !CHAOS, Cloud Padovana, INDIGO-DataCloud, Prisma, OCP, Rmlab, ...

nonché la **partecipazione diretta** delle persone coinvolte nei progetti suddetti col nostro e viceversa.

a breve

completeremo la stesura formale del progetto per sottoporlo all'attenzione della dirigenza in modo da ottenere un supporto concreto in tempi brevi