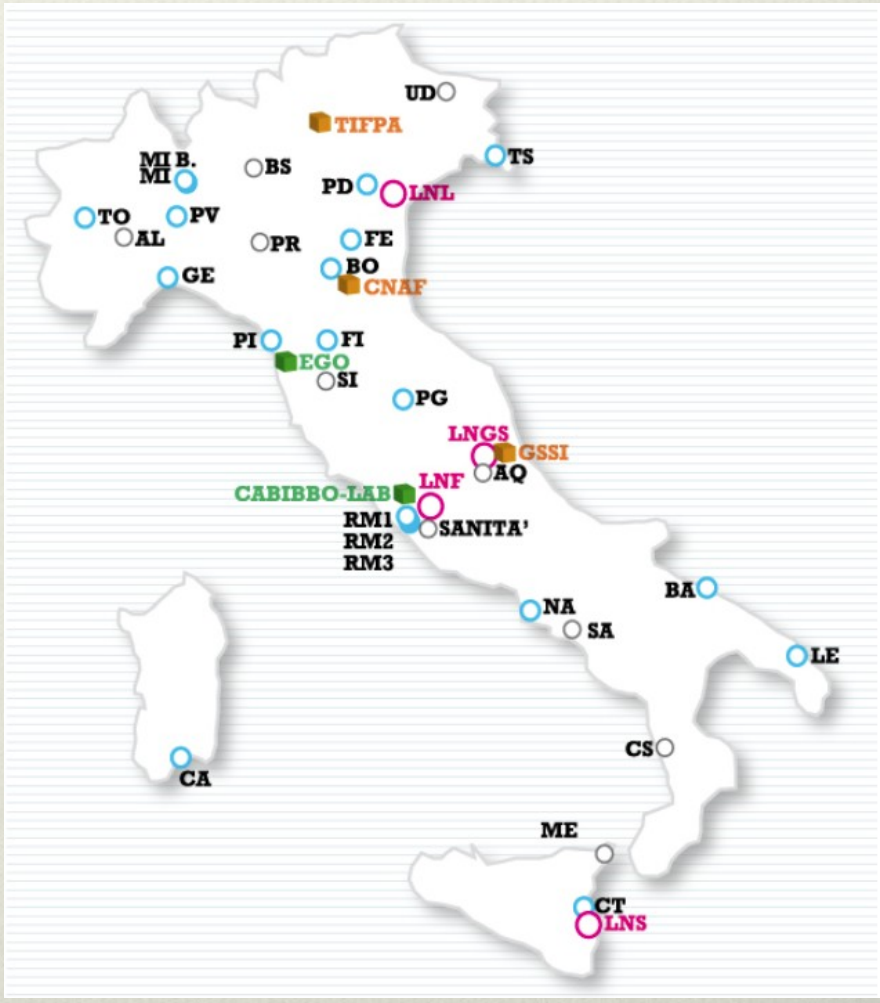
Introduzione alle potenzialità di OpenStack in ambiente multiregione geograficamente distribuito

Cristina Aiftimiei, Stefano Stalio
on behalf of the CloudMr Group
Workshop CCR Cloud
Napoli – 19 Dicembre 2014

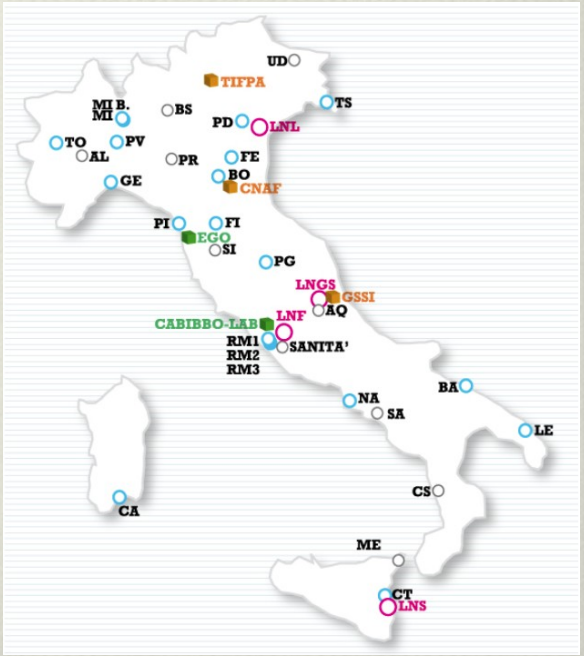
Motivazione

- Ridondanza ed HA dei servizi Cloud
- Ridondanza ed HA dei servizi **sulla** Cloud
- Sfruttamento di risorse distribuite nelle sedi INFN, loro presentazione come entità unica anche dal punto di vista dell'autenticazione e dell'autorizzazione.



Motivazione

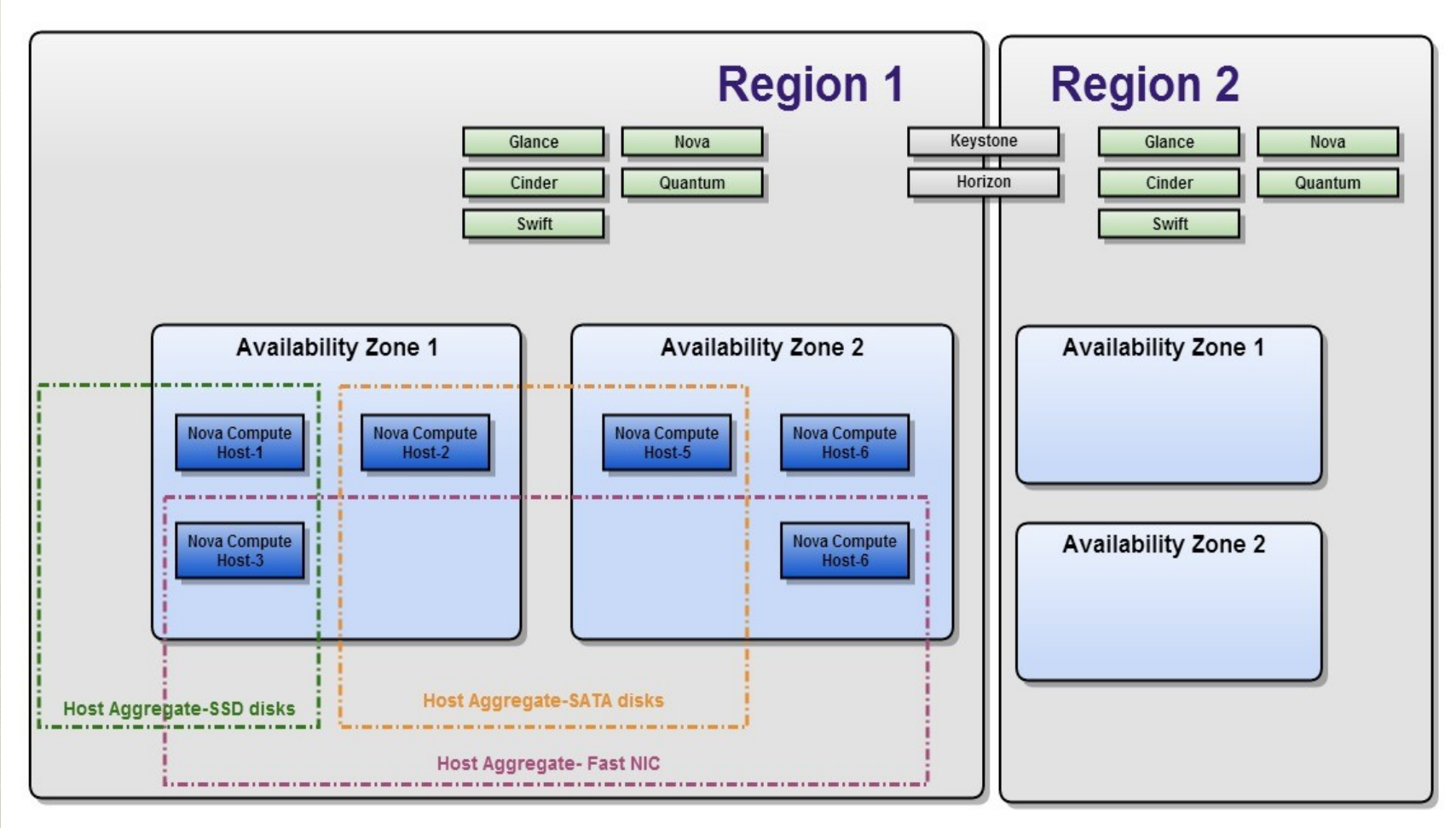
- Consentire ad **utenti INFN** utilizzo di risorse cloud **esterne** alle sedi
  - Cloud pubbliche e/o private di altre istituzioni
  - attraverso lo stesso meccanismo di autenticazione ed autorizzazione
- Consentire ad utenti appartenenti ad enti **esterni all'INFN**
  - L’accesso, a risorse cloud distribuite nelle sedi INFN,
    - attraverso il sistema SSO utilizzato dall'ente di appartenenza.



Possibilità

- I componenti di OpenStack sono scritti utilizzando paradigmi di utilizzo della rete e protocolli che sono quasi sempre agnostici rispetto alle caratteristiche dell'infrastruttura di rete sulla quale insistono.
- Sono pensati per lavorare su reti inaffidabili e, se necessario, poco performanti.
- Per questi motivi è possibile pensare e realizzare installazioni OpenStack distribuite su siti distanti.

Modello Architetturale



Modello Architetturale

- **Regione** – ha la sua infrastruttura OpenStack completa, inclusi API endpoint, risorse di rete e calcolo
  - Regioni diverse **condividono** un servizio **Keystone** e **Horizon**
- **Availability Zone/Host Aggregation** - in una regione, le risorse di calcolo possono essere logicamente raggruppate in **Availability Zones** ed **Host aggregations**.
  - L'utente puo specificare la Availability Zone (e la Regione) all'interno delle quali vuole istanziare la sua risorsa

Progetto Cloud-Multiregione

È un progetto che tende alla realizzazione di una cloud OpenStack con risorse dislocate in più sedi INFN.

Questa infrastruttura si appoggia ad un **unico Identity Service (Keystone)** distribuito e ridondante e si avvale del concetto di “**regione**” per la suddivisione logica delle risorse.

Si appoggia inoltre ad un servizio di **object storage (Swift)**, anch’esso distribuito e replicato su più sedi.

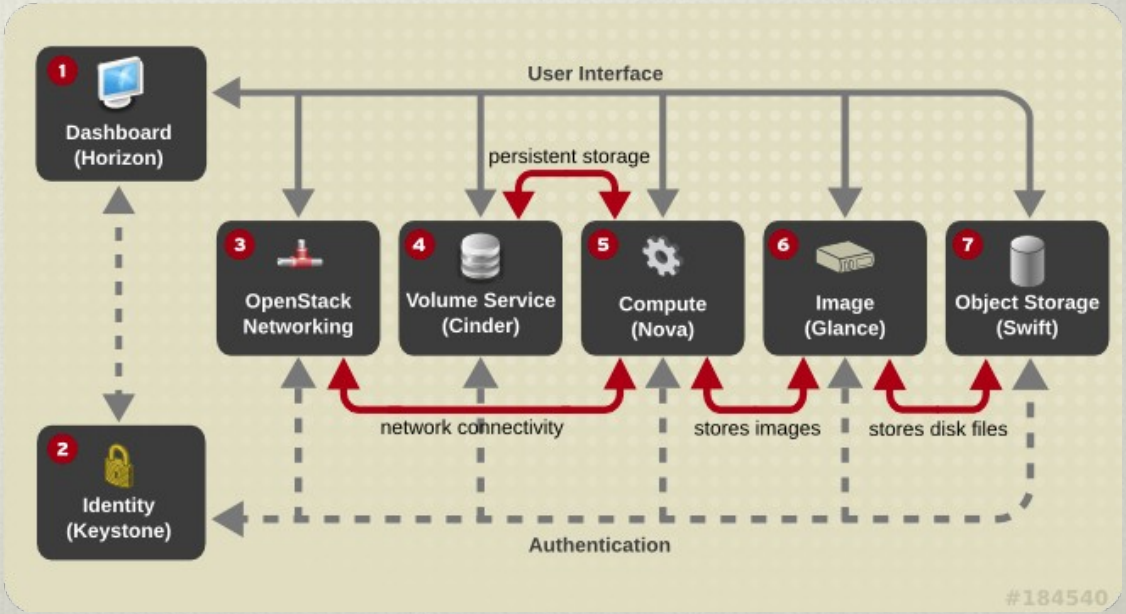
Progetto Cloud-Multiregione

Ad OGGI:

- **Openstack** “funzionante” in 4 sedi, interesse ed attività in più sedi.
- **Keystone** distribuito su 3 sedi (BA, LNGS, PD), su db MySQL nativo
- **Swift** distribuito su 3 sedi (BA, LNGS, PD, ma presto anche RM2)
- **Dashboard** su 3 sedi
- **Monitoring** (Nagios a LNGS, Zabbix a Bari) con syslog, centralizzato (presentazione ieri)

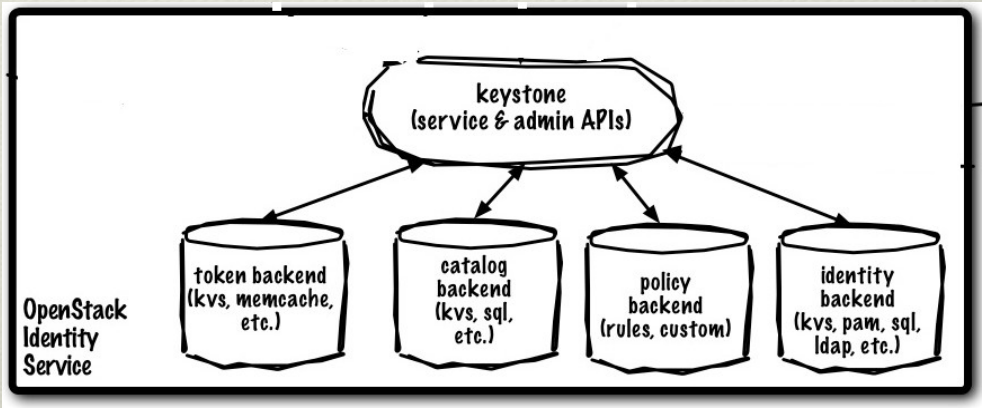
Identity Service - Keystone

- Implementa un unico componente di autenticazione per i diversi moduli di OpenStack
  - si occupa di progetti, utenti, gruppi, ruoli, **autorizzazioni**, autenticazione
    - In un ambiente di produzione **DEVE** funzionare **perfettamente**
  - Fornisce autorizzazioni per credenziali di log–in multiple



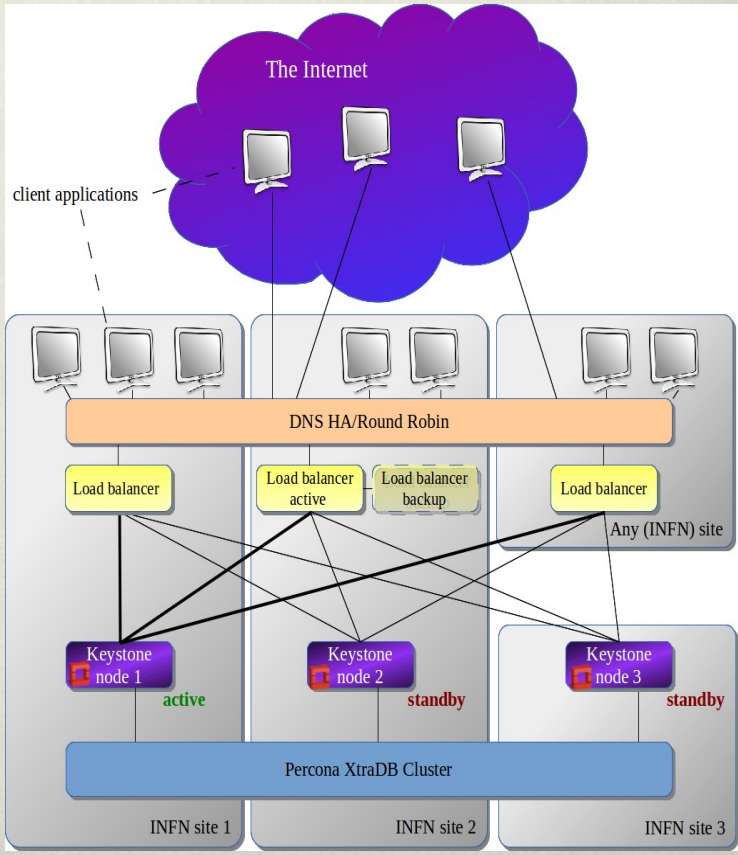
Identity Service - Keystone

- Organizzato come un gruppo di **4 servizi** esposti via API network
  - **Identità**: validazione delle credenziali per gli utenti.
  - **Token** validazione e gestione dei token per l'autenticazione una volta che le credenziali siano stati verificate.
  - **Catalogo dei servizi**, con informazioni sugli endpoint (indirizzi accessibili via rete).
  - Gestione delle **policy** di autorizzazione.
- Supporta diversi **backend-plugins** per l'integrazione con ambienti eterogenei e per esporre diverse funzionalità:
  - KVS, Memcache, SQL, PAM, LDAP



Identity Service – Keystone in CloudMR

- In **HA** geografica, **stabile**, su **Icehouse**
  - Cluster di tre server Keystone in tre sedi diverse sedi INFN:
    - **PD** per il Nord Italia,
    - **LNGS** per il Centro,
    - **Bari** per il Sud Italia
  - DB MySQL, replicato sui tre siti usando **Percona XtraDB Cluster**
  - **HAProxy** e usato come **load balancer** e come **HA provider**
  - Il servizio **DNS riconfigurabile dinamicamente** offerto da **ha.infn.it** garantisce **fault protection** per i server proxy
  - **Comunicazione criptata** (SSL) tra:
    - i client ed i proxy server
    - tra i proxy server e i server Keystone
    - tra i server Keystone



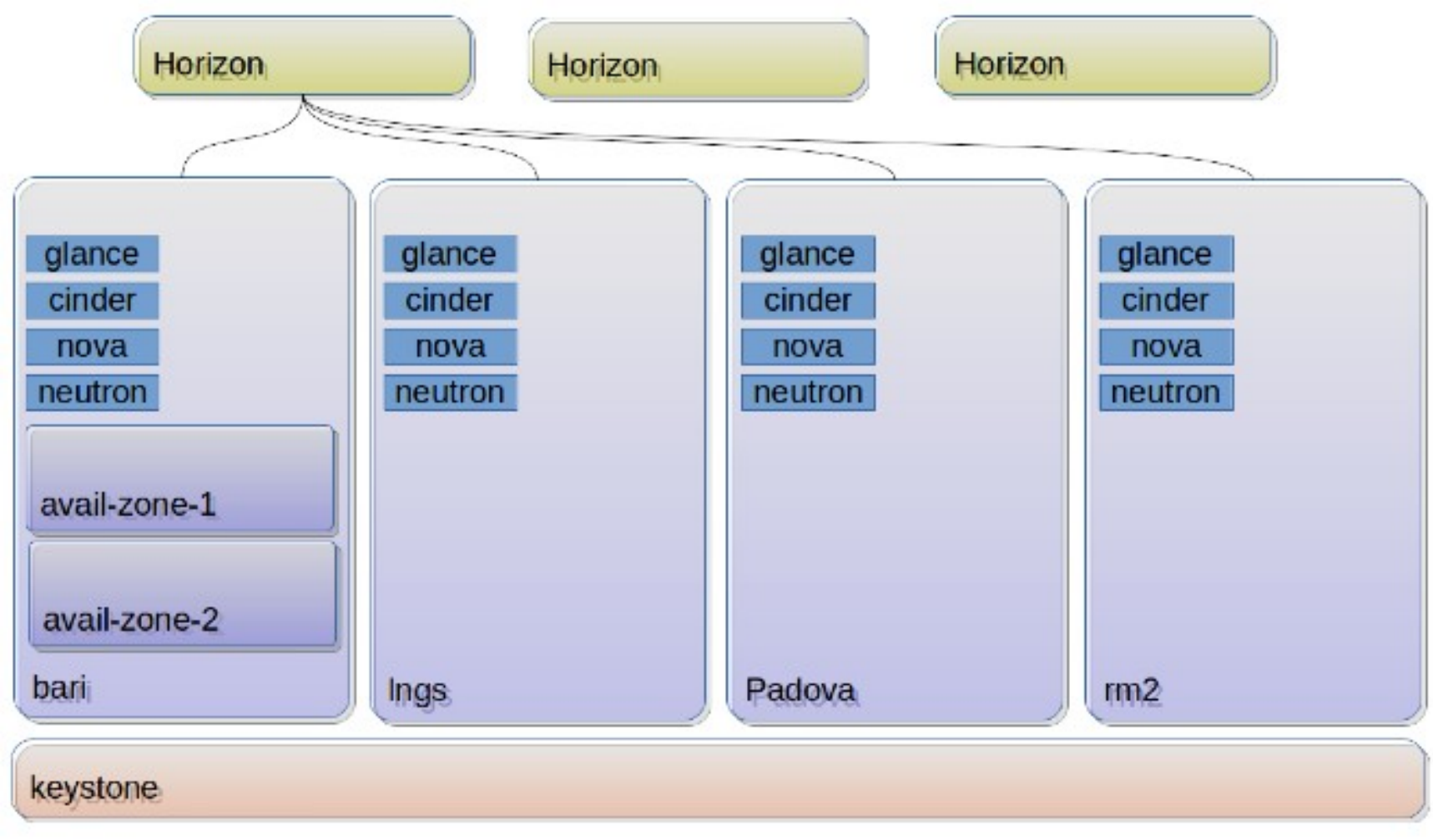
Identity Service – Keystone in CloudMR

- **Problematiche**
  - la gestione di un cluster mysql a master multipli distribuito su piu’ sedi INFN;
  - la gestione di un enorme numero di token keystone di grosse dimensioni;
  - bug vari nel codice Keystone
- **Futuro**
  - Keystone + backend LDAP (AAI)
    - Gia’ implementato a LNGS – da distribuire
  - Esposizione API v3
  - Autenticazione federata - verso altri IdP utilizzando le, relativamente nuove, feature di federated authentication
  - migliorare il deployment dell'infrastruttura di autenticazione –> 5 db server + 3 identity server
  - Keystone & Domains – Domain specific Drivers, unlimited “admin”ness,

Dashboard - Horizon

- Horizon è il modulo che fornisce l'interfaccia utente via Web per amministratori e utenti finali
  - **non siamo limitati ad una sola dashboard** ma ne possiamo realizzare quante vogliamo, in sedi diverse e, al limite, anche sul portatile degli utenti. Ovviamente le dashboard devono ppoter accedere agli api server della Cloud
    - https://havanactl.lngs.infn.it
    - https://blade-03-01.pd.infn.it
    - http://bari-region-ctl.ba.infn.it/horizon

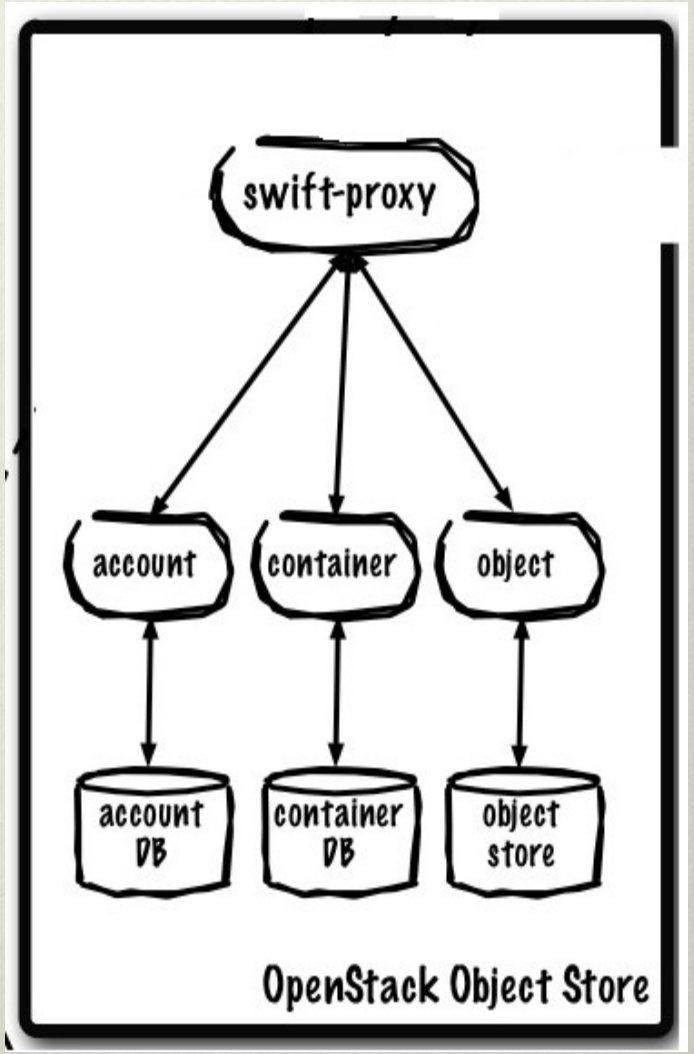
Dashboard - Horizon



Object Storage - Swift

- Sistema distribuito di storage pensato per l'alta affidabilità e la scalabilità.
  - **two-tier storage system**
    - a **proxy tier**, - handles all incoming requests;
    - A **object storage tier** – stores the actual data.
- Caratteristiche importanti:
  - Massive scaling & eventual consistency
  - Consistent hashing -> **Rings**
  - Data duplication: **3 copies**; zones
- Componenti – accounts, containers, objects

Piu' dettagli nella presentazione su Swift

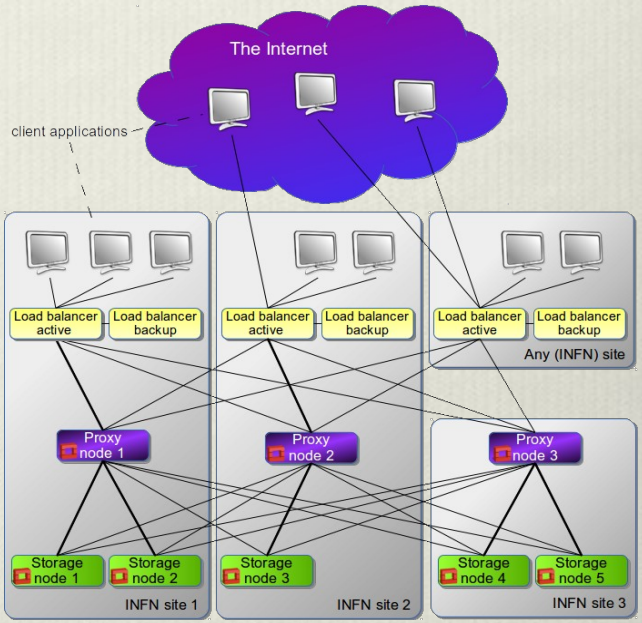


Object Storage – Swift in CloudMR

- In **HA** geografica, stabile
  - Aggiornato a **Juno**

Swift e` il default backend per glance nella cloud MR

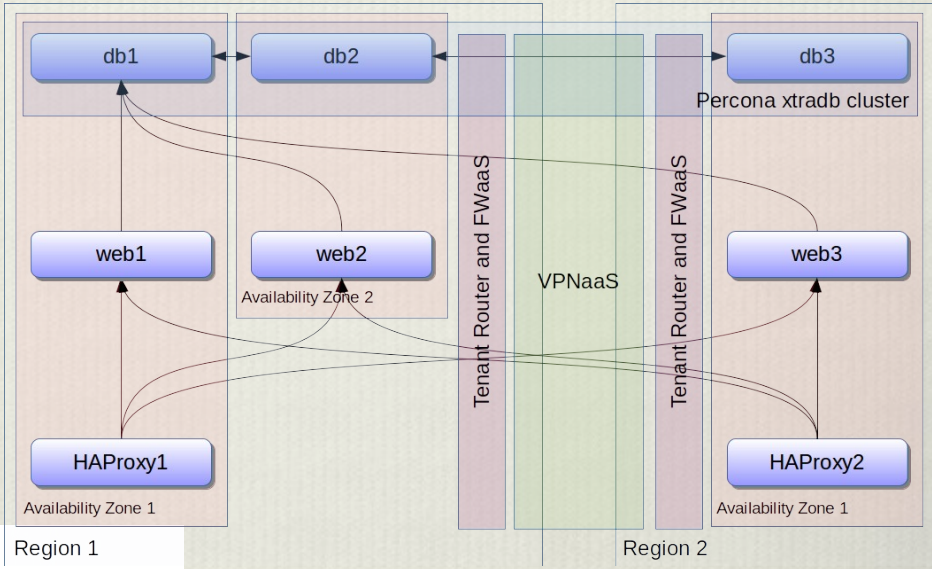
- Swift puo` essere usato come **backend glance** anche per installazioni che non si appoggiano al keystone “mr”
- **Manca la criptazione** del trasferimento di dati e metadati (token compresi)

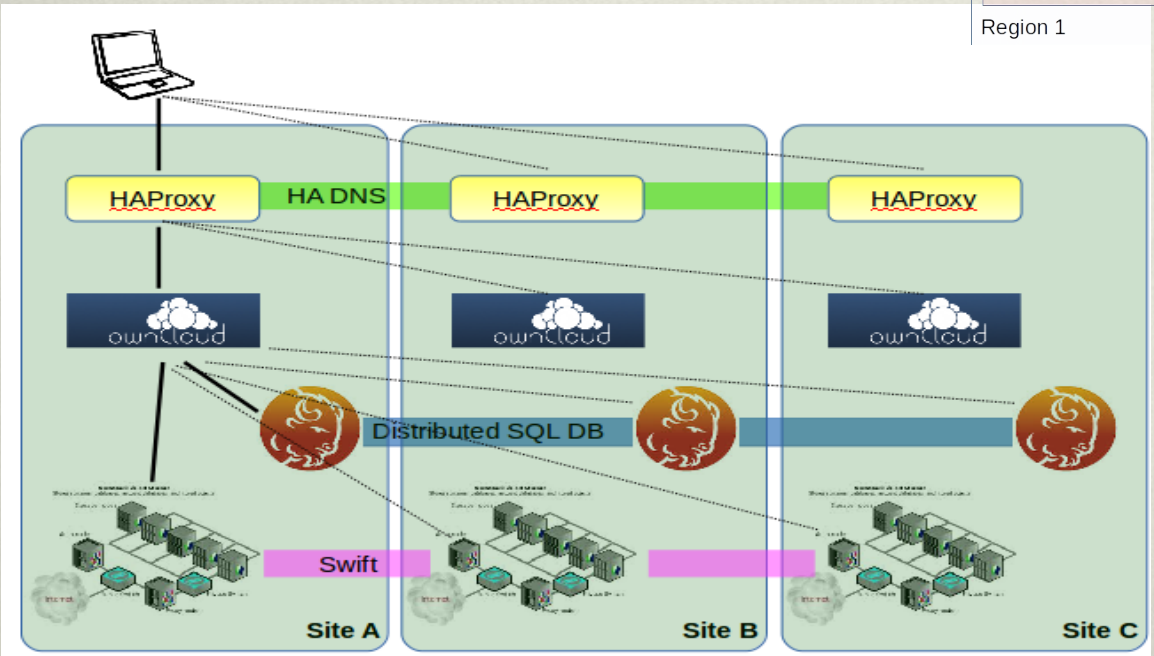


Use Cases

L inux
A pache
M ysql (Percona)
P hp
H aproxy
S wift

distribuito, fully redundant, disaster-proof





Attività in corso

- **Monitoring centralizzato**
- **Syslog centralizzato**
- **Networking**
  - Indagare su hardware capace di funzionare come Network Node OpenStack
  - Test su Distributed Virtual Router – nuove funzionalità in Juno

Attività in corso

- **Glance**
  - VMCaster/VMCatcher (EGI FedCloud TF) per registrazione immagini firmate
  - Automatizzazione registrazione immagini e snapshot su istanze glance remote
- **VPNaaS**
  - Valutazione stabilità/usabilità di VPNaaS per comunicazione interregione
- **Documentatione** (wiki)
  - http://wiki.infn.it/cn/ccr/cloud/cloud_multiregione
- **Infrastruttura**
  - Inserimento nuove regioni, consolidamento infrastruttura allo scopo di abilitare il deployment di use case (!CHAOS ed altri)
  - Gestori risorse locali in regioni nuove e vecchie

Welcome to CLoudMR!