

# Nuove funzionalità di OpenStack (Icehouse, Juno)

Enrico Fattibene  
INFN – CNAF

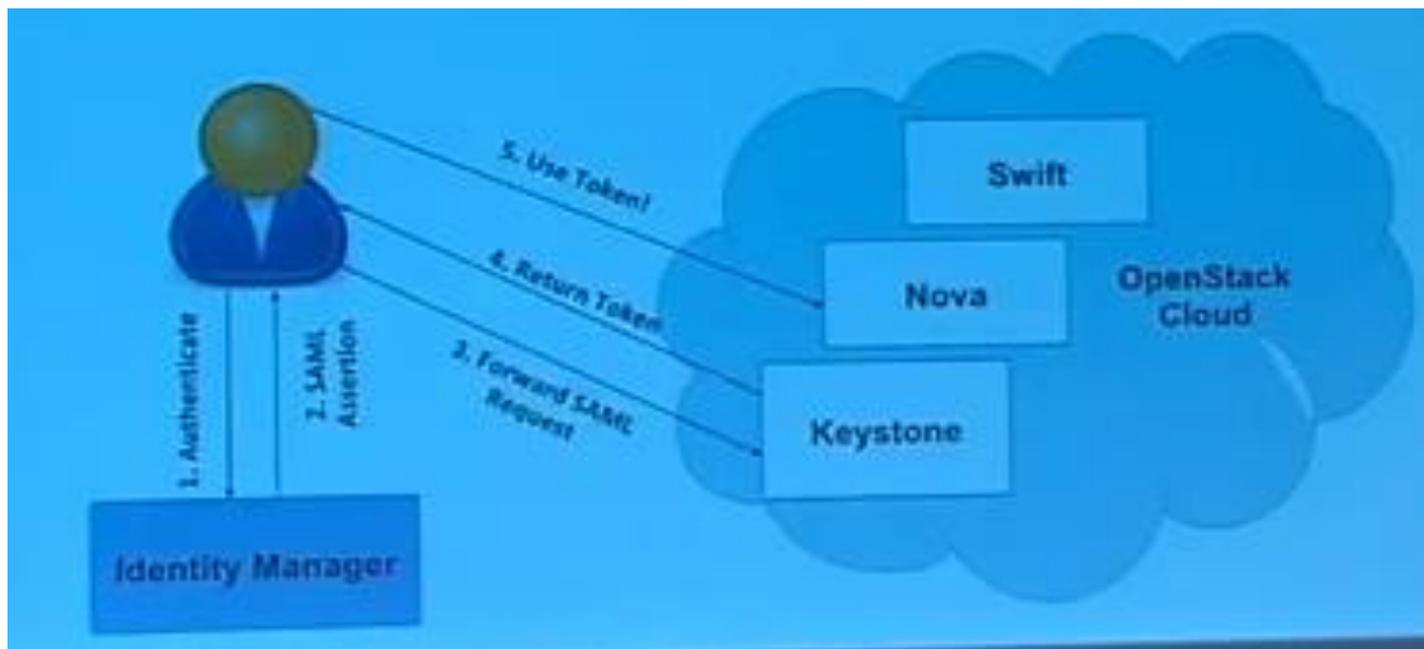
Tutorial Days di CCR  
Napoli 17/12/2014

# Juno

- Crescita nei contributori
  - 1,419 contributori da 133 organizzazioni
  - 16% in più rispetto ad Icehouse
- Features
  - 342 nuove features integrate nel software di Juno
- Bug risolti
  - 3,219 bugs risolti durante il ciclo di rilascio di Juno (6 mesi)
  - 10% in più rispetto ad Icehouse
- Documentazione
  - Modificate circa 500,000 righe di documentazione
- Driver e plugin
  - 97 drivers e plugins supportati

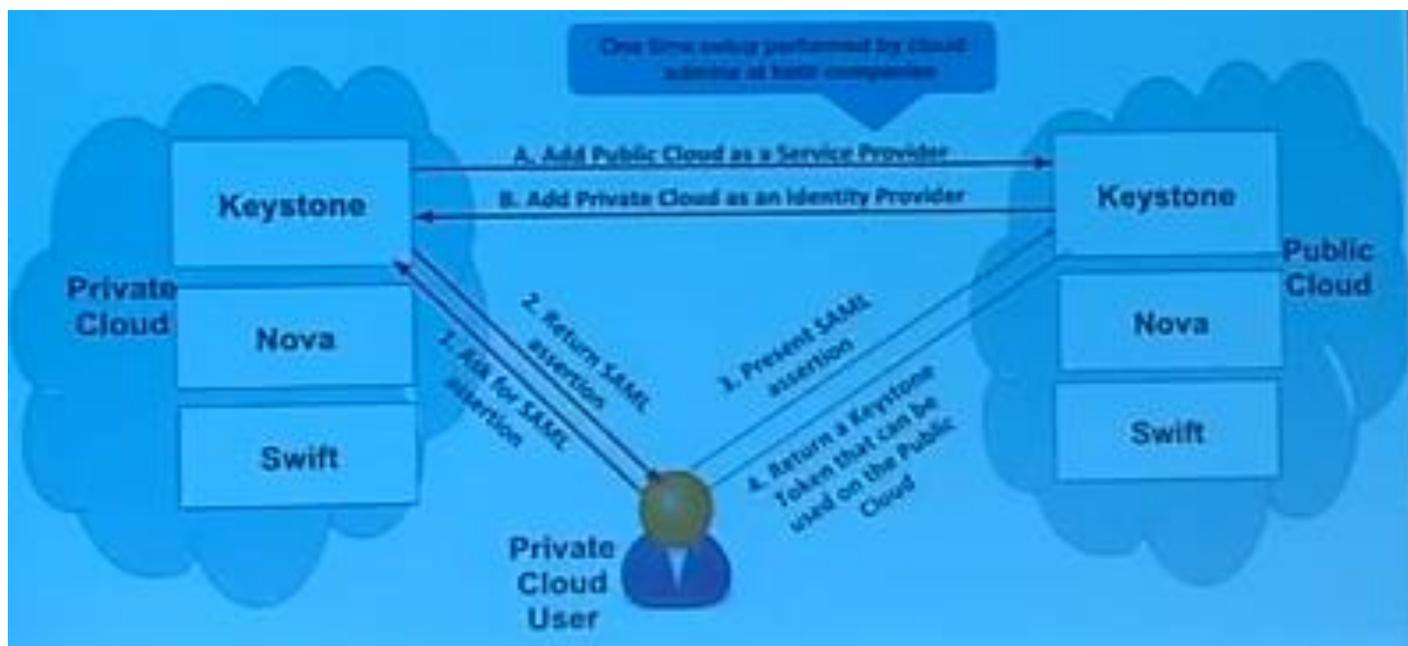
# Identità federata

- In Icehouse una o più cloud OpenStack possono integrarsi con un Identity Provider
  - Single sign-on su diverse cloud
  - Asserzioni SAML (standard aperto per il formato dati nelle federazioni) trasformate in attributi Keystone (che agisce da Service Provider)



# Identità federata

- Federazione in Juno
  - Funzionalità sperimentale in Juno
  - Critica per poter usare cloud ibride
  - Keystone di una cloud privata diventa IdP e keystone di altre cloud private/pubbliche diventa SP
  - Attributi Keystone trasformati in asserzioni SAML



# Glance

- Aggiunto metadata service
  - Gestione di metadati aggiuntivi per diversi servizi OpenStack
  - Definiti come coppie chiave/valore
  - Le proprietà possono essere raggruppate in namespace, associati a uno o più tipi di risorsa (Image, Flavor, Volume, etc.)

# Neutron L3 agent

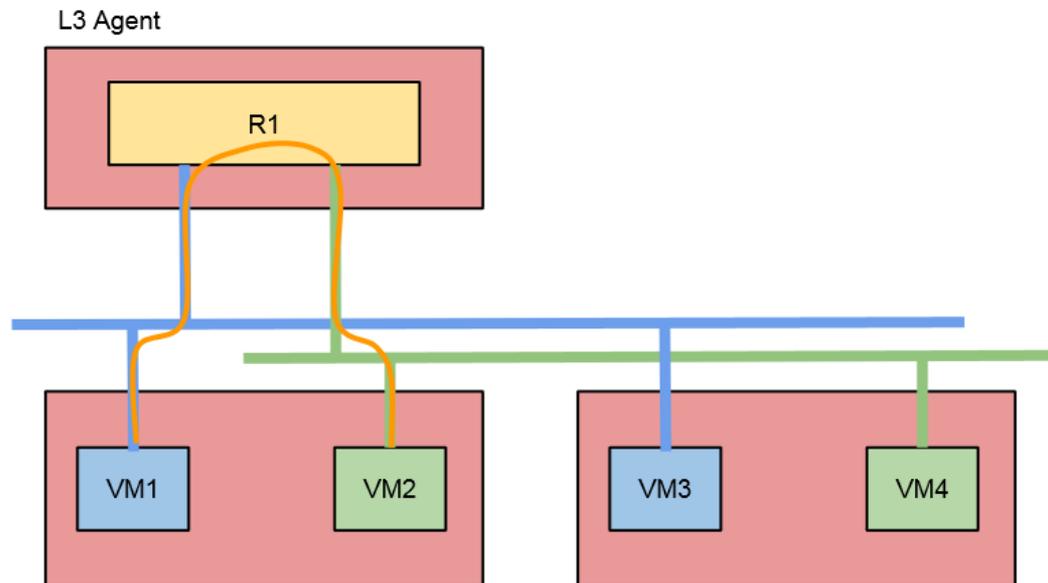
- **Prima di Juno**
  - Era possibile avere Network Node multipli per dividere il carico, con diversi router virtuali su diversi nodi
  - Non era possibile HA o ridondanza dei nodi
  - Tutto il traffico era passante per un unico punto:
    - Il Network Node era un single point of failure. In caso di problem non era più possibile il traffico verso l'esterno e quello east-west tra le VM
    - Il routing centralizzato provocava un collo di bottiglia nel flusso di traffico
- **In Juno**
  - **High Availability del Network Node**
    - Virtual Router Redundancy Protocol (VRRP)
    - Il router viene assegnato a due l3-agent, uno attivo e uno passivo
    - Keepalived gestisce l'assegnazione di un Virtual IP all'istanza attiva
  - **Distributed Virtual Router (DVR)**
    - Funzionalità dell' l3-agent sui Compute node

# DVR

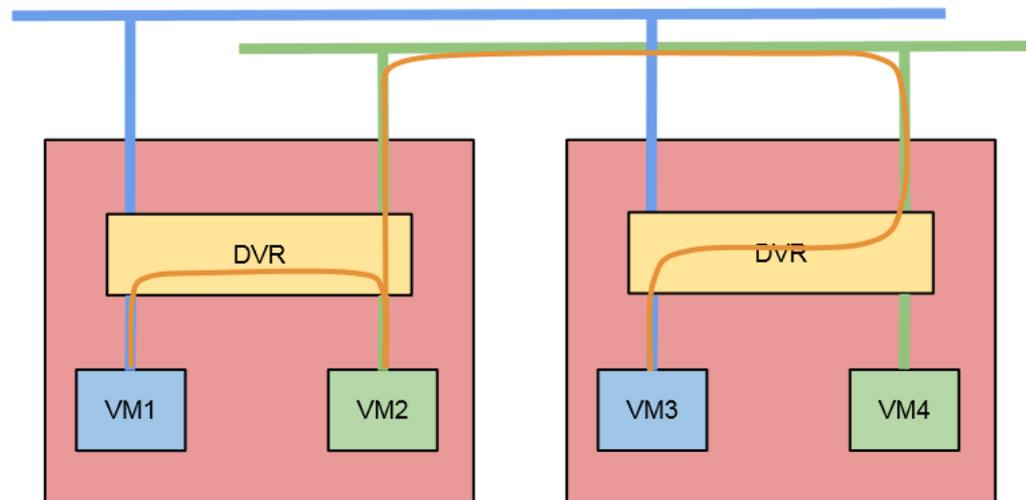
- Distributed Virtual Router
  - Funzionalità dell'I3-agent non più in network node ma distribuite sui compute; per un dato router, c'è Internal Router (IR) per ogni Compute Node che ospita VM sulle sottoreti connesse a quel router, quindi il singolo router sarà composto dai diversi IR.
  - Gestisce traffic da e verso l'esterno in presenza di floating IP
  - In assenza di floating IP, SNAT è gestito da I3 agent su Network node
  - I compute node devono essere connessi con l'external network
  - Eliminato il traffico east-west sul Network node

# Traffico east-west

Senza DVR



Con DVR



# Neutron

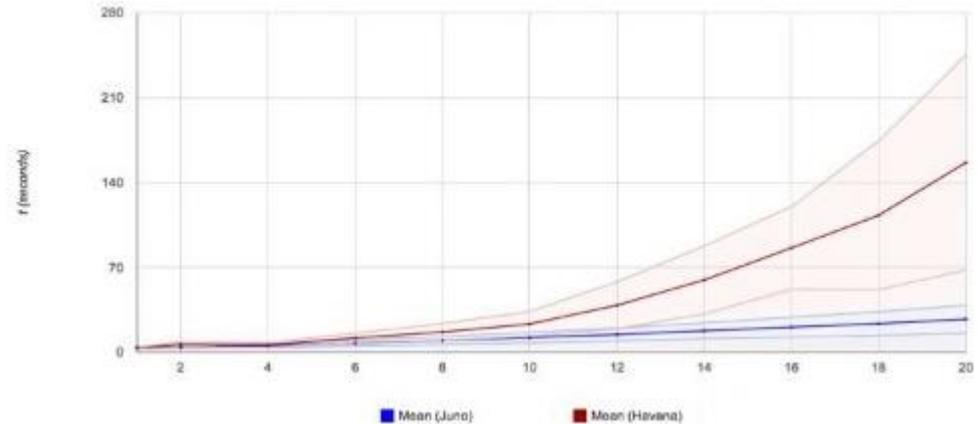
- In linea di principio si potrebbero usare le funzionalità di DVR e di HA dell'I3 agent insieme:
  - Il traffico dei floating IP passerebbe attraverso il compute node, mentre il traffico SNAT (senza floating IP) passerebbe attraverso gli I3 agent sui network node in HA
  - Forse nelle future release
- DVR e I3 HA saranno production ready in Kilo
- FWaaS ancora sperimentale
  - Un solo Firewall per tenant

# Neutron

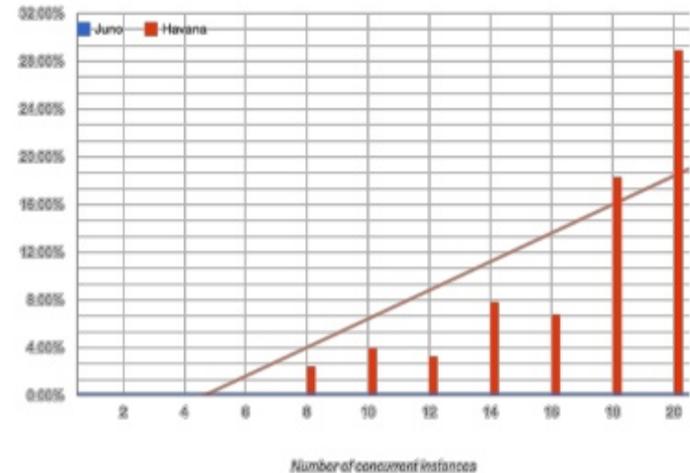
- Test L2 agent

- facendo partire da 1 a 20 VM su una OpenStack all-in-one
- Il tempo perché l'interfaccia di rete della VM è up è lineare in Juno (con 20 istanze, 25 secondi per partire ognuna di esse), in Havana non era scalabile
- Quasi nessun fallimento in Juno facendo partire 20 VM, mentre in Havana non era così

$t_{up}$  in Havana and Juno - a rather remarkable difference!



- VM failure rate analysis
  - Failure == error while creating VM or unable to ping within 3 min timeout
- Juno is infallible decently reliable (Havana not as much...)



# Neutron

- (Alcuni) problemi risolti in Juno
  - L'associazione di un floating IP a una VM non era subito visibile in Horizon/CLI
    - Neutron manda le info a Nova ad ogni cambiamento
  - Una VM poteva divenire Active prima che la rete fosse up
    - Neutron manda gli eventi a Nova solo dopo che la rete è pronta
  - Non c'era modo di conoscere lo stato di un floating IP assegnato, se non pingandolo
    - L3 agent invia al Neutron server lo stato dell'assegnazione dell'IP (active o down)

# Nova

- In Icehouse:
  - Supporto «limitato» per live upgrade
    - Dopo aver fatto upgrade del controller è possibile fare upgrade dei compute node senza downtime dell'intera Cloud
  - Scheduler supporta filtri di affinity e anti-affinity
  - Nuovo parametro per assegnare una immagine ad un certo host aggregation

# Nova

- In Juno:
  - Si può far partire una VM corrotta con una immagine diversa dalla originale
  - Aggiunto driver per Ironic
  - Il driver Docker è stato tolto da Nova, ma continua il suo sviluppo
    - Ci si aspetta ritorni in-tree in Kilo
  - Scheduling
    - Permette l'evacuazione completa di un nodo
    - I nodi di destinazione delle istanze sono scelte dallo scheduler

# Trove

- Inserito nella release ufficiale da Icehouse
- In Icehouse
  - Supporto a MySQL singola istanza
  - Supporto sperimentale per DB NoSQL
  - VM con porta MySQL aperta e accesso dell'utente al server
  - Poco usabile da esperienze INFN
- In Juno
  - Supporto a MySQL cluster con Galera
  - Supporto a PostgreSQL
  - Supporto iniziale modalità cluster per MongoDB
  - Funzionalità di backup e restore solo su Swift

# Ceilometer / Heat

- Ceilometer
  - Miglioramenti nelle performance
  - Metering di nuovi servizi di rete:
    - LBaaS, FWaaS e VPNaaS
- Heat
  - Rollback di deployment falliti
    - Prima bisognava cancellare gli elementi dello stack
  - Amministratori possono delegare utenti per la creazione di certe risorse (come autoscaling)
  - Aggiunti nuovi resource type (per Sahara e non solo)

# Cinder / Swift

- Cinder
  - Notifiche a Ceilometer in caso di attach/detach dei volumi
  - Replica dei volumi
- Swift
  - Storage policies
    - L'utente può controllare:
      - su quale hardware risiedono i dati (tipo di dischi)
      - come i dati sono archiviati su quell'hardware (tipo di repliche)
      - dove è posizionato lo storage (regioni)
    - un oggetto meno importante e poco acceduto potrebbe essere copiato una sola volta su hardware storage a basse prestazioni, mentre le informazioni più richieste e sensibili potrebbero essere copiate più volte, su hardware ad alte prestazioni di accesso e con ridondanza geografica.

# Sahara 1/2

- Hadoop as a Service
- Permette di creare e gestire cluster Hadoop su OpenStack
- Specificando versione, topologia del cluster e altre configurazioni
- Supporta anche Apache Spark
- Durante il setup del cluster deve accedere alle istanze via ssh (attraverso IP fissi o floating)
- Supporta il dimensionamento dinamico del cluster

# Sahara 2/2

- Può usare Cinder come backend dei volumi
- Si integra (tramite patch su Hadoop) con Swift per fornire funzionalità di MapReduce
- Anti-affinity
  - Volumi su compute node diversi per garantire ridondanza
- Data-locality
  - Favorisce l'accesso ai dati che sono sullo stesso rack, sullo stesso compute node o anche sulla stessa
- Multi-region
- Integrato in Heat e Horizon

# Horizon Icehouse

- Migliore usabilità
  - Possibilità di editare inline i valori nelle tabelle
  - Filtri di ricerca meno generici
  - Menu di navigazione più estendibile
- Nova
  - Live Migration
  - Gestione di host aggregation e availability zone
- Cinder
  - Estensione di un volume
  - Creazione di un volume come copia di un altro

# Horizon Icehouse

- Ceilometer
  - Report dell'uso giornaliero per tenant visibile agli amministratori
- Supporto per RBAC (Role Based Control Access)
  - Per Glance e Cinder
  - Si possono implementare regole di accesso alle risorse più fini dei semplici ruoli "member" e "admin"
  - E' possibile ad esempio definire se un utente può creare, accedere, o cancellare immagini

# Horizon Juno

- Nova
  - Mostra ad un utente le eventuali azioni svolte da altri utenti sulle VM del tenant
  - Evacuazione di un hypervisor
    - Live migration di *tutte* le VM da un hypervisor agli altri
- Supporto per Sahara
- Supporto per l'editing dei metadata tags di Glance
  - Catalogo di metadati che possono essere usati per immagini, flavor, etc.

# Horizon Juno

- Migliorato il supporto per RBAC (role based control access)
  - Per compute, network e orchestration (oltre che per Glance e Cinder come già in IceHouse)
- Neutron
  - Possibilità di configurare i router con DVR
  - Possibilità di usare L3 agent HA

# Nuovi progetti

- Sarà integrato in Kilo (30 Apr 2015):
  - Ironic (bare metal)
- Ci si aspetta vengano integrati nelle release successive a Kilo:
  - Manila (shared file system)
  - Zaqar (servizio di messaggistica)
    - ex-Marconi
  - Designate (DNS service)
  - Barbican (key management)