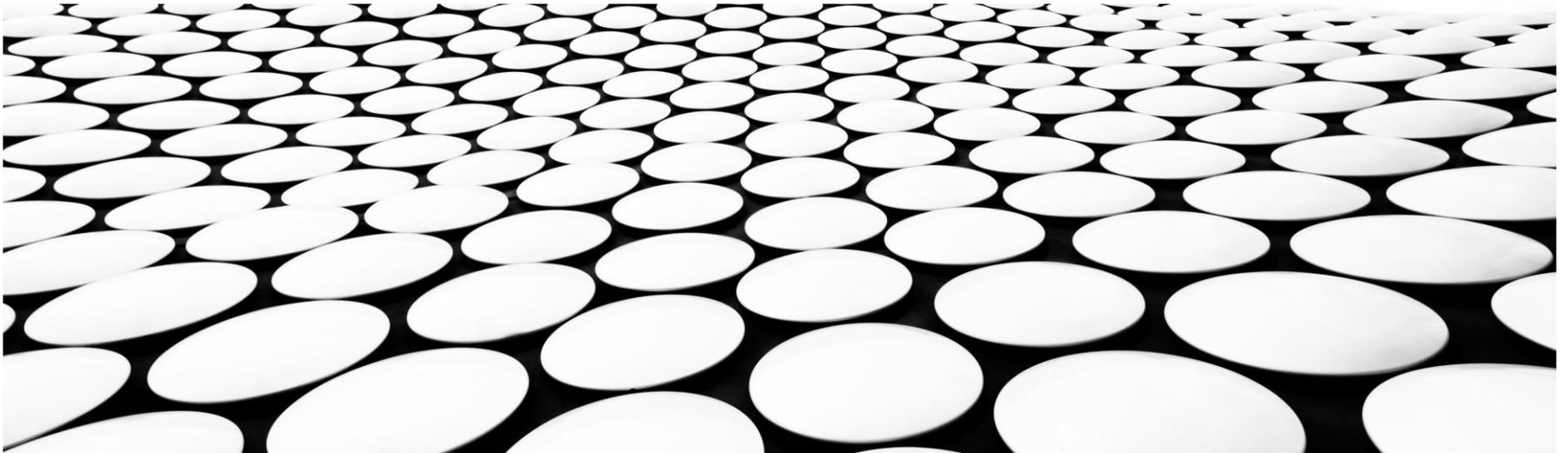


---

---

# INFRASTRUCTURE AS A SERVICE (IAAS)

VINCENZO CALABRÒ



# Cloud Computing: IaaS

- ▶ Utente gestisce interamente processing (CPU), memoria, storage, rete, e risorse di computazione aggiuntive
  - ▶ Amazon, Google, Nuvola Italiana
- ▶ Utente in grado di installare ed eseguire codice generico incluso sistemi operativi e applicazioni
- ▶ Utente non gestisce o controlla l'infrastruttura cloud, mentre controlla sistemi operativi, storage, e applicazioni installate
  - ▶ Nessuna necessità di controllare hw con tutte le problematiche di obsolescenza, malfunzionamenti, danni...
- ▶ Utente ha controllo limitato di componenti di rete (ad es., host firewall)

# Cloud Computing: IaaS

- ▶ Offre risorse virtualizzate on demand
- ▶ Fornisce diversi server con diversi sistemi operativi e uno stack software ad hoc
- ▶ Amazon offre macchine virtuali con diverse combinazioni di sistemi operativi
  - ▶ EC2 Service
  - ▶ È come gestire un server fisico
  - ▶ Utenti possono far partire e bloccare una VM, installare software, collegare dischi virtuali

# Cloud Computing: Top20 IaaS Provider



<http://www.clouds360.com/iaas.php>

# Amazon EC2



- ▶ Amazon ElasticCompute Cloud (Amazon EC2) è un servizio web che fornisce capacità computazionale sulla cloud (<http://aws.amazon.com/ec2/>)
- ▶ Rende disponibili API e servizi aggiuntivi per semplificare il web-based computing
- ▶ Fornisce accesso a capacità computazionale in modo semplice e intuitivo
- ▶ Fornisce una gestione completa dell'ambiente di esecuzione
- ▶ Pay-per-use

- ▶ Caratteristiche principali
  - ▶ Multi-tenancy
  - ▶ Massima scalabilità in termini di capacità computazionale delle VM
  - ▶ High performance clustering e load balancing
  - ▶ Elastic IP Addresses
  - ▶ Supporta i più comuni hypervisor
  - ▶ Object storage ridondato e scalabile
  - ▶ Replica delle immagini delle VM nella cloud
  - ▶ Supporta modelli flessibili di rete virtuali per la separazione di server e traffico
  - ▶ AWS Marketplace

# Google Compute Engine

- ▶ Google Compute Engine permette di creare ed eseguire machine virtuali sulla Google infrastructure
- ▶ Compute Engine offre scalabilità, performance e funzionalità per eseguire grandi cluster sulla Google infrastructure
- ▶ Nessun costo iniziale
- ▶ Permette di eseguire migliaia di vCPU su un sistema veloce, consistente e performante

# Google Compute Engine

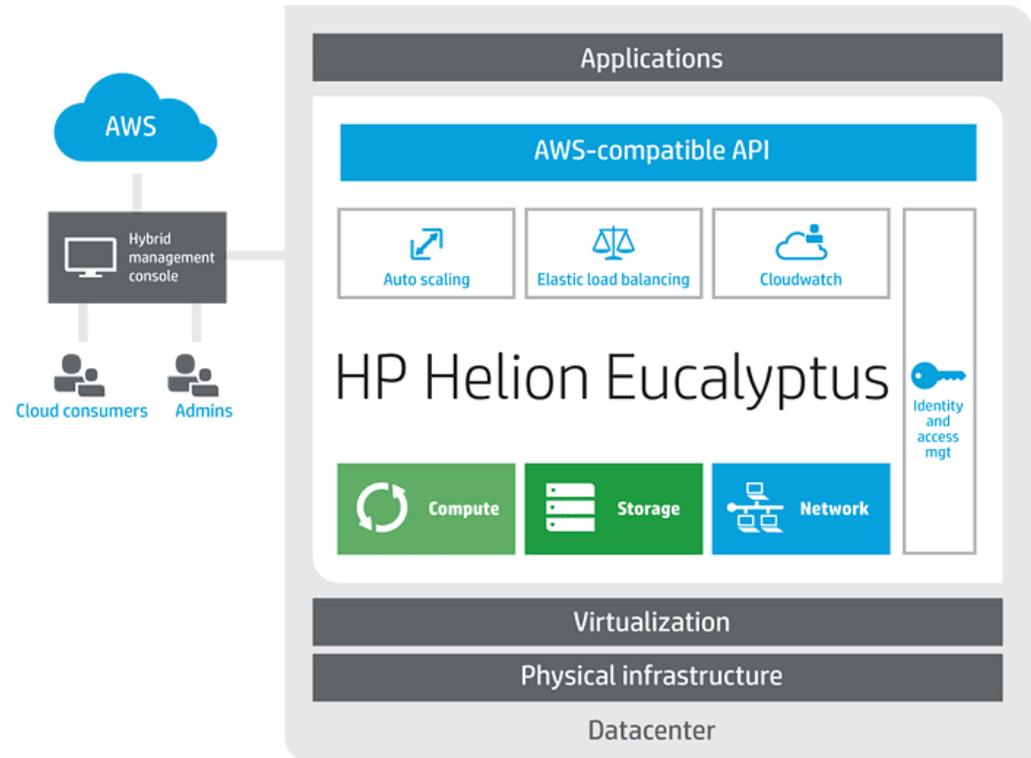
- ▶ Funzionalità
  - ▶ High-performance virtual machines
  - ▶ Powered by Google's global network
  - ▶ Pay for what you use
  - ▶ Global load balancing
  - ▶ Fast and easy provisioning
  - ▶ Compliance and security
  - ▶ Flexible Batch Processing

# HP Helion Eucalyptus

- ▶ Open source framework che supporta la creazione di cloud ibride e private (<http://www.eucalyptus.com/>)
- ▶ Compatibile con Amazon Web Services (AWS)
  - ▶ Supporta AWS APIs
  - ▶ Supporta EC2, S3, Amazon EBS, e Amazon Identity and Access Management (IAM)
  - ▶ Supporta AWS Elastic Load Balancing (ELB), Auto Scaling, CloudWatch e CloudFormation
- ▶ Funzionalità avanzate per la definizione di cloud elastiche all'interno di datacenter integrati nell'infrastruttura IT
- ▶ Fornisce meccanismi automatici per la scalabilità di risorse

# HP Helion Eucalyptus

- ▶ Utenti possono usare comandi Eucalyptus per gestire istanze Amazon o Eucalyptus
- ▶ Utenti possono migrare istanze di macchine tra una private cloud Eucalyptus e la cloud pubblica Amazon creando una hybrid cloud
- ▶ Garantisce isolation e non interferenza tra applicazioni e stack



# HP Helion Eucalyptus

- ▶ Caratteristiche principali
  - ▶ Compatibilità AWS API
  - ▶ Hybrid cloud management
  - ▶ Cloud management console
  - ▶ Flexible and scalable virtual networking capabilities
    - ▶ Network management, security groups, e traffic isolation
  - ▶ High-availability per componenti cloud
  - ▶ Web-based cloud account management
  - ▶ Flexible clustering
  - ▶ Image and instance management
  - ▶ Quota management e accounting
  - ▶ User group e role-based access management
  - ▶ Integrazione LDAP e Active Directory
  - ▶ Supporto per i principali sistemi operativi
  - ▶ Supporto per i principali hypervisor
  - ▶ Supporto per le SAN
  - ▶ Molti altri... <https://www.eucalyptus.com/eucalyptus-cloud/iaas/features>

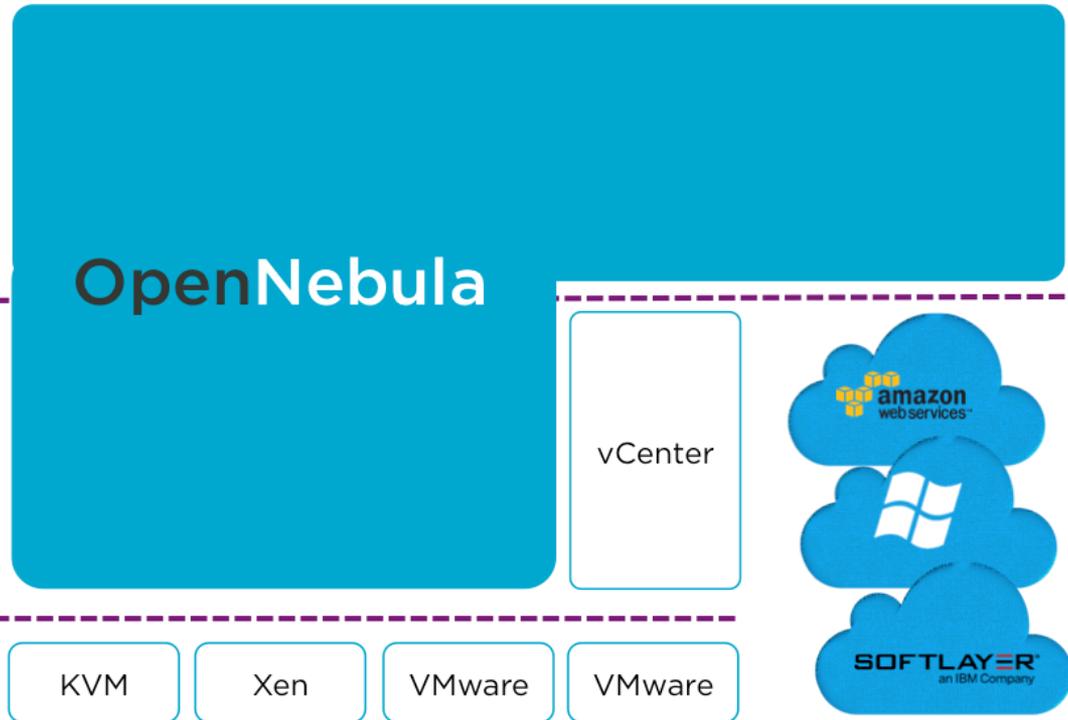
- ▶ Open source toolkit per la gestione di datacenter virtuali e hybrid, private e public cloud
- ▶ Gestisce storage, network, virtualization, monitoring, e security per il deploy di sistemi multi-tier
- ▶ Supporta la combinazione di risorse locali del datacenter e risorse remote sulla cloud

## Cloud Management

- Multi-tenancy
- Simple cloud GUI and interfaces
- Service elasticity/provisioning
- Federation

## Virtual Infra Management

- Capacity management
- Virtual appliance management
- Resource optimization
- HA and business continuity



- ▶ Caratteristiche principali
  - ▶ Interfacce per cloud consumer
    - ▶ Compatibilità AWS API
  - ▶ Service management e catalog
  - ▶ Interfaccia CLI avanzata
  - ▶ Open Nebula Marketplace
  - ▶ Accounting e monitoring di risorse e applicazioni
  - ▶ High availability e Business continuity
  - ▶ Configurazione e installazione automatica di servizi
  - ▶ Network management, security groups, traffic isolation
  - ▶ Supporto cluster
  - ▶ Supporto per i principali sistemi operativi
  - ▶ Supporto per i principali hypervisor
  - ▶ Fine-grained ACL e multi-tenancy
  - ▶ E molto altro... <http://opennebula.org/about/key-features/>



# OpenStack

# OpenStack – Un po' di storia

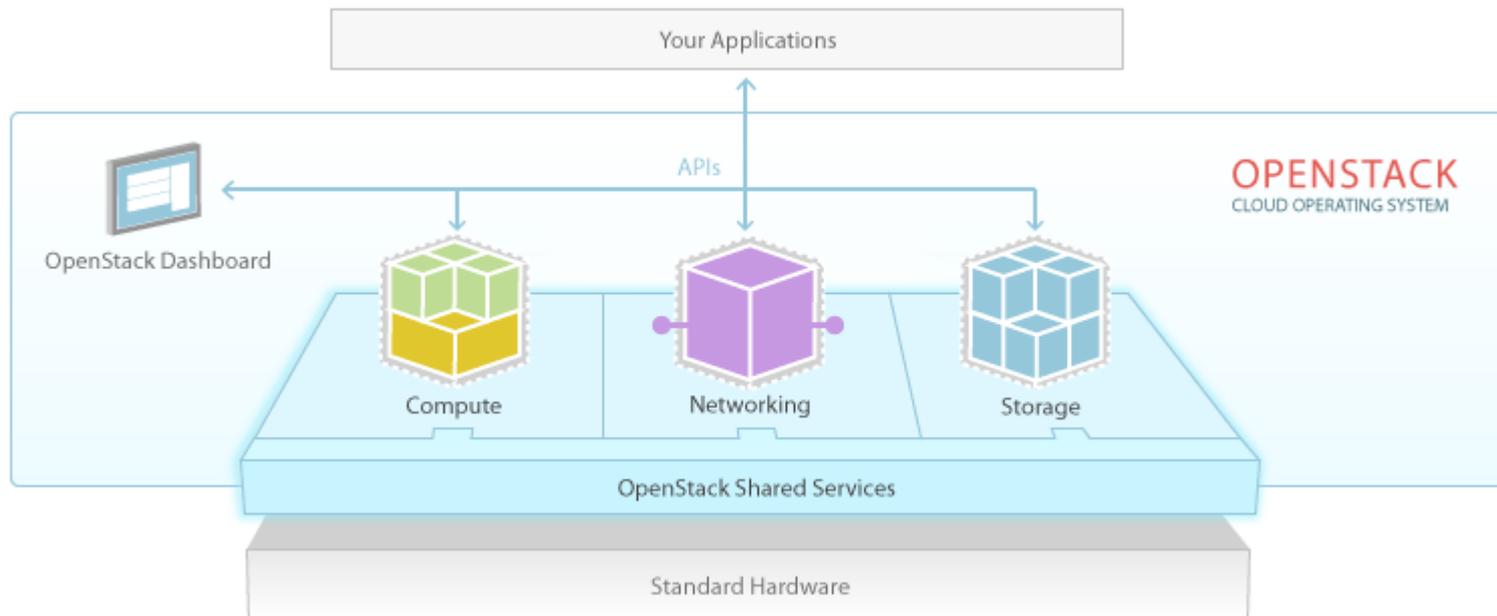
- ▶ Luglio 2010: Rackspace e NASA lanciano un'iniziativa chiamata OpenStack
  - ▶ Destinato ad agevolare l'adozione di una soluzione di cloud computing per l'offerta dei servizi da parte delle aziende
- ▶ Ottobre 2010: prima versione OpenStack *Austin*
  - ▶ Integra la piattaforma Nebula della NASA e Cloud Files di Rackspace
- ▶ 2011: sviluppatori di Ubuntu Linux adottano Openstack verso il rilascio della seconda versione *Bexar*
  - ▶ Supporto completo dalla terza versione *Cactus*
    - ▶ Disponibile anche per la release di sviluppo Debian
- ▶ 2012: Debian 7.0 include OpenStack *Essex*, RedHat distribuisce OpenStack basata su release *Essex*

# OpenStack – Un po' di storia

- ▶ 2013: supporto commerciale di RedHat a OpenStack Grizzly
- ▶ Luglio 2013: NASA lascia lo sviluppo attivo del progetto
  - ▶ Mancanza di progresso tecnico e altri fattori
  - ▶ Si concentra sull'utilizzo di cloud pubblici
- ▶ Agosto del 2013: Avaya decide di utilizzare OpenStack al fine di creare un'infrastruttura di rete virtuale end-to-end
- ▶ Maggio 2014: HP rilascia HP Helion che si basa su OpenStack IceHouse
- ▶ Ultime release: Juno, Kilo

# OpenStack

- ▶ Open source software per creare cloud pubbliche e private
- ▶ Cloud operating system che controlla insieme di risorse di compute, storage, networking
  - ▶ Amministratore gestisce risorse attraverso dashboard
  - ▶ Utenti accedono a risorse attraverso interfaccia web
- ▶ [http://docs.openstack.org/admin-guide-cloud/content/ch\\_getting-started-with-openstack.html](http://docs.openstack.org/admin-guide-cloud/content/ch_getting-started-with-openstack.html)



# OpenStack

- ▶ Fornisce agli utenti una soluzione cloud affidabile e configurabile per tutte le esigenze
- ▶ Facilità di implementazione, grandi capacità di scalabilità ed estensione, e una varietà di funzionalità avanzate
- ▶ Servizi interconnessi che implementano i vari componenti che compongono l'infrastruttura cloud
  - ▶ Accessibili tramite API o dashboard

# OpenStack Dashboard

- ▶ Fornisce un'interfaccia grafica per accedere, fornire e automatizzare risorse cloud
- ▶ Permette di esporre servizi di terze parti come billing e monitoring
- ▶ Applicazione web estendibile per controllare compute, storage e networking resources
- ▶ Fornisce un'overview sulla dimensione e stato della cloud
  - ▶ Permette di creare utenti e progetti, assegnare utenti a progetti e limitare l'uso di risorse

# OpenStack Compute

- ▶ OpenStack permette ai provider di rilasciare computing resource on demand
  - ▶ Risorse accedute via API o web interface
- ▶ Sviluppata per scalare orizzontalmente
- ▶ Fornisce architettura flessibile
  - ▶ Open source
  - ▶ Si integra con terze parti e sistemi legacy
- ▶ Gestisce e automatizza distribuzione di risorse e supporta tecniche di virtualizzazione
  - ▶ Xen, KVM

# OpenStack Compute

- ▶ Funzionalità
  - ▶ Gestisce risorse virtualizzate
  - ▶ Supporta LAN (DHCP, IPv6)
  - ▶ Autenticazione e limitazione di utilizzo API
  - ▶ Architettura sincrona e distribuita
  - ▶ Gestione delle immagini di VM (anche live)
  - ▶ Floating IP
  - ▶ Security group
  - ▶ RBAC
  - ▶ Progetti e quota
  - ▶ ...

# OpenStack Storage

- ▶ Supporta sia Object Storage che Block Storage
- ▶ Object Storage usato per fornire storage con costi ottimizzati e capacità di scale out
  - ▶ Piattaforma di storage pienamente distribuita, accessibile tramite API, integrabile con applicazioni o utilizzabile per archiviazione
  - ▶ Non è un file system tradizionale, memorizza dati in oggetti
  - ▶ OpenStack gestisce la replica e supporta scalabilità orizzontale
- ▶ Block Storage permette di collegare block device a compute instance per maggiori performance e integrazione con piattaforme di storage aziendali
  - ▶ Gestisce creazione, mounting e unmounting di storage a blocchi
  - ▶ File divisi in blocchi di dati fissi
  - ▶ Integrato con OpenStack compute e dashboard

# OpenStack Storage

- ▶ Funzionalità
  - ▶ Si basa su hardware comune
  - ▶ Supporto per la scalabilità
  - ▶ Storage illimitato
  - ▶ Supporto per la replicazione
  - ▶ Nessun DB centrale
  - ▶ Integrabile con compute
  - ▶ Supporta S3 API
  - ▶ Snapshot e backup per block volume

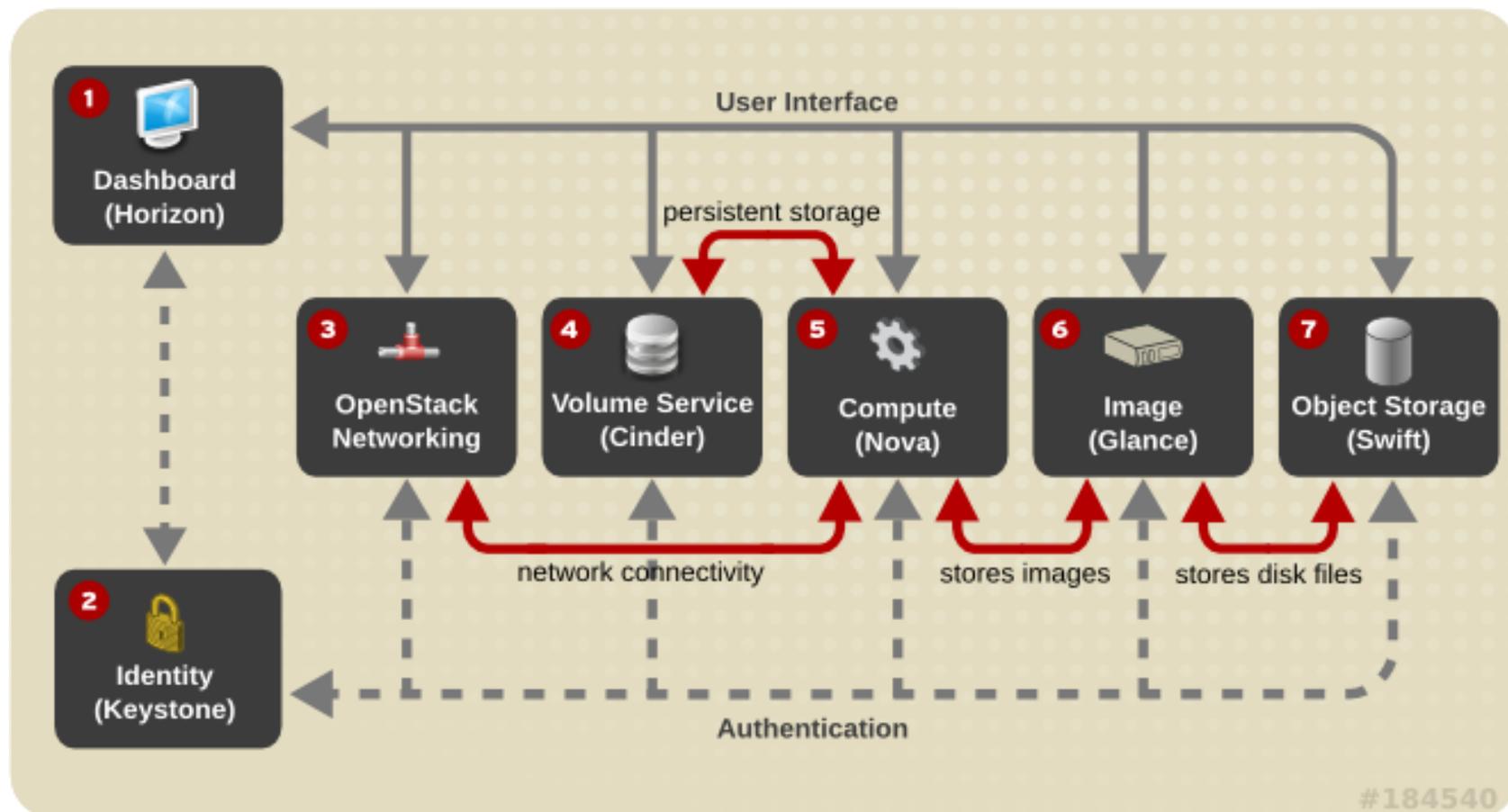
# OpenStack Networking

- ▶ La rete di un datacenter contiene server, network equipment, storage system e security appliance in numero sempre maggiore
  - ▶ Tali device sono divisi in VM e virtual network
  - ▶ Indirizzi IP, configurazioni di routing, regole di sicurezza crescono esponenzialmente
  - ▶ Soluzioni di gestione della rete tradizionali non forniscono un supporto automatico e scalabile per gestire queste reti
  - ▶ Utenti pretendono più controllo e flessibilità
- ▶ OpenStack Networking è scalabile, basata su API e “pluggable”
  - ▶ Gestisce reti e indirizzi IP
  - ▶ Assicura che non ci siano colli di bottiglia o fattori limitanti in un deployment cloud
  - ▶ Utenti creano la loro rete, controllano il traffico e connettono server e device

# OpenStack Shared Service (excerpt)

- ▶ Identity Service
- ▶ Image Service
- ▶ Telemetry Service
- ▶ Orchestration Service
- ▶ Database Service

# Servizi OpenStack



# Mapping servizi/progetti

- ▶ Dashboard -> Horizon
- ▶ Compute -> Nova
- ▶ Networking -> Neutron
- ▶ Object storage -> Swift
- ▶ Block storage -> Cinder
- ▶ Identity -> Keystone
- ▶ Image -> Glance
- ▶ Telemetry -> Ceilometer
- ▶ Orchestration -> Heat
- ▶ Database -> Trove

# Horizon – Dashboard

- ▶ Applicazione web modulare basata su Django (web framework basato su linguaggio python)
- ▶ Servizio accessibile a clienti e API di qualunque servizio OpenStack
- ▶ Admin endpoint forniscono funzionalità di amministrazione attraverso la dashboard
- ▶ Permette di eseguire tutte le operazioni per la gestione dell'infrastruttura e dell'account
- ▶ Pochi click per deploy/undeploy di VM, creare volumi, gestire sicurezza

# Horizon – Dashboard

openstack laboratorioReti ardayna Sign Out

Project

- Compute
- Overview
- Instances**
- Volumes
- Images
- Access & Security
- Network
- Object Store
- Orchestration
- Database
- Data Processing
- Identity

## Instances

Instance Name Filter Filter Launch Instance Soft Reboot Instances Terminate Instances

	Instance Name	Image Name	IP Address	Size	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
<input type="checkbox"/>	prova	CentOS-7		m1.tiny	-	Error	nova	Deleting	No State	6 minutes	

Displaying 1 item

# Compute – Nova

- ▶ Servizio fondamentale dell'infrastruttura OpenStack
- ▶ Gestisce l'intero ciclo di vita delle istanze nell'ambiente virtuale
  - ▶ Creazione, coordinamento, eliminazione delle macchine virtuali
- ▶ Interagisce con il servizio di Identity per l'autenticazione, con il servizio di Image per le immagini disco e server, e la dashboard per fornire interfaccia utente e amministratore
- ▶ Scala orizzontalmente su hardware standard e recupera immagini per la creazione di istanze
- ▶ Contiene un demone nova-network per la gestione della rete

# Networking – Neutron

- ▶ Servizio di networking (neutron-server)
- ▶ Permette di creare e implementare nella rete virtuale dispositivi e interfacce gestite da altri servizi di OpenStack
- ▶ Plug-in possono essere implementati per gestire e interconnettere diverse apparecchiature di rete e software fornendo una completa flessibilità per l'architettura OpenStack e la sua implementazione
- ▶ Interagire con il servizio Compute per fornire un'infrastruttura di rete e permettere la connettività alle istanze
- ▶ Accetta e indirizza le richieste API a plug-in predefiniti per implementare determinate operazioni

# Networking – Neutron

- ▶ Operazioni principali: plug e unplug di porte, creazione di reti e sotto-reti, operazioni di indirizzamento IP
- ▶ Plug-in e agenti differiscono in base al provider e alle tecnologie usate per l'implementazione dell'ambiente cloud
- ▶ Versione evoluta e più efficace di nova-network
  - ▶ Aggiunge molte funzionalità
  - ▶ Difficile da gestire
- ▶ Nova-network e Neutron sono due diverse implementazioni del paradigma networking-as-a-service per OpenStack
- ▶ Neutron gestisce una grande quantità di plug-in che permettono configurazione complesse ben oltre le capacità

# Storage concept

- ▶ On-instance / ephemeral
  - ▶ Fornisce spazio da zero
  - ▶ Associato con VM
  - ▶ Accedibile fino a quando la VM è attiva
  - ▶ Supporta restrizioni basate su flavor
  
- ▶ Block Storage
  
- ▶ Object Storage

# Block storage (cinder)

- ▶ Aggiunge storage persistente a una VM
- ▶ Persiste fino a quando la macchina non è cancellata
- ▶ Fornisce un'infrastruttura per gestire i volumi e snapshot di volumi
- ▶ Interagisce con OpenStack Compute
- ▶ Accesso tramite VM
- ▶ Montato attraverso OpenStack Block Storage controlled protocol (ad es., iSCSI)
- ▶ Dimensionamento dello storage basato sulle necessità

# Object storage (swift)

- ▶ Multi-tenant object storage system
  - ▶ Usato per memorizzare dati e immagini di macchine virtuali
- ▶ Persiste fino a quando non viene cancellato
- ▶ Accedibile da dovunque
- ▶ Gestisce grandi quantità di dati ed è in grado di scalare tramite RESTful HTTP API
- ▶ Fornisce funzionalità per la gestione delle VM, non per la memorizzazione
  - ▶ Fornisce astrazione a metodi di memorizzazione, non lo storage stesso
- ▶ Può eseguire indipendentemente da Compute Nova

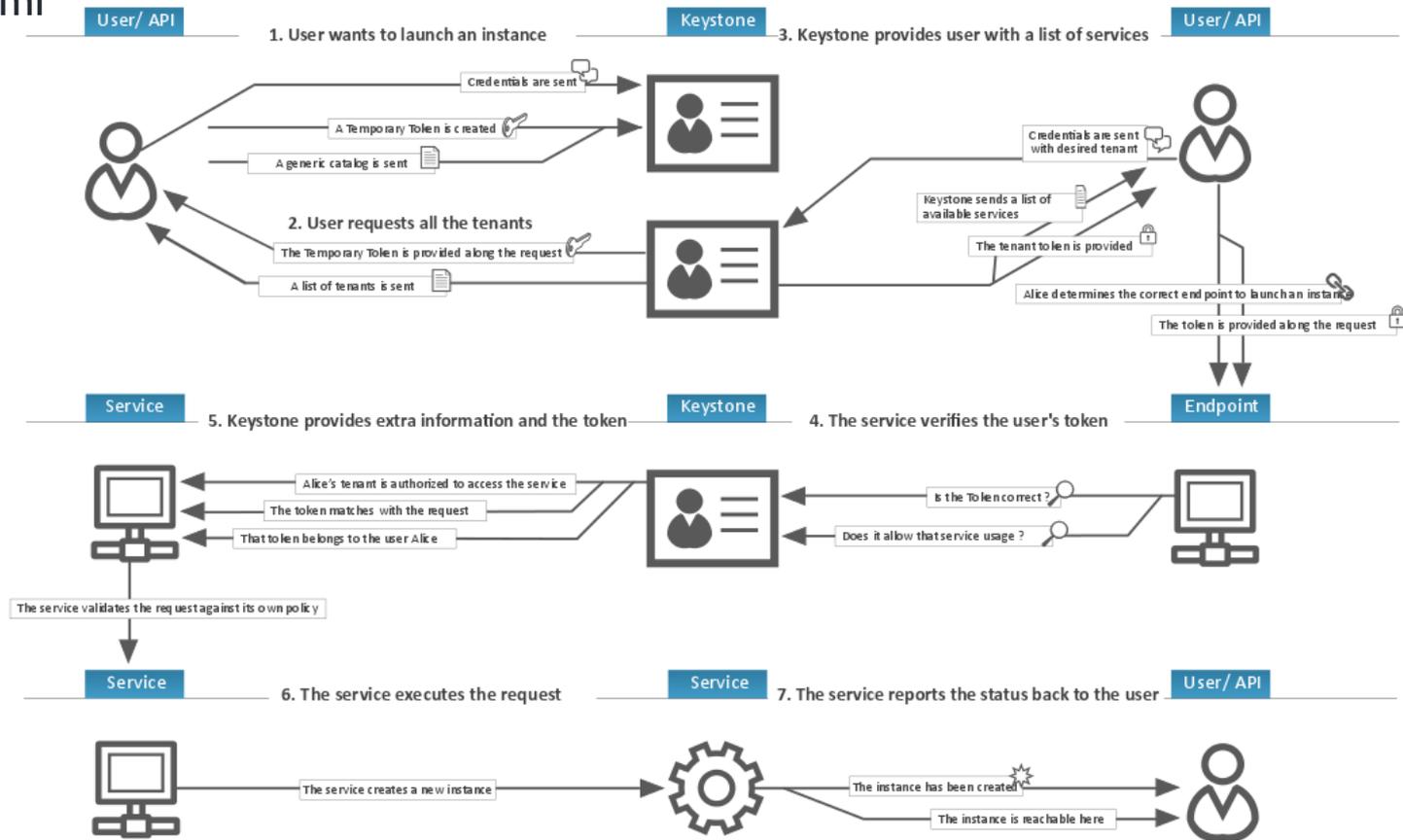
# Identity – Keystone

- ▶ Svolge essenzialmente due funzioni
  - ▶ Tracciamento degli utenti e dei relativi permessi
  - ▶ Fornitura di una lista di servizi disponibili con API endpoint
- ▶ Al momento dell'installazione del servizio per la gestione delle identità è necessario registrare ogni servizio presente nell'infrastruttura OpenStack
  - ▶ A quel punto il servizio di identity riconosce quali sono i servizi attivi in OpenStack e dove sono localizzati nella rete
- ▶ Keystone genera token di autorizzazione per gli utenti
  - ▶ Attraverso le API di keystone utente sottometta credenziali e riceve token di autenticazione
  - ▶ Mantiene tabella utenti e privilegi

# Identity – Keystone

<http://docs.openstack.org/kilo/install-guide/install/apt/content/keystone-concepts.html>

The Keystone Identity Manager



# Image – Glance

- ▶ Importante per una soluzione IaaS
- ▶ Accetta richieste per immagini di disco o server, o metadati relativi a immagini da end users o OpenStack Compute component
- ▶ Supporta storage di immagini di disco e server su vari tipi di repository incluso OpenStack Object Storage
- ▶ Supporta caching, replication per fornire consistency e availability, auditing

# Telemetry – Ceilometer

- ▶ Raccoglie dati di metering da servizi OpenStack
  - ▶ CPU, utilizzo di rete
  - ▶ Utile per stabilire il pagamento in base al consumo (pay-as-you-go)
- ▶ Collezione eventi e dati di metering monitorando notifiche inviate dai servizi
- ▶ Pubblica dati attraverso data store e message queue
- ▶ Crea allarmi quando dati collezionati violano certe regole
- ▶ Contiene: compute-agent, central-agent, notification-agent, collector, alarm evaluator, alarm notifier, API server

# Orchestration – Heat

- ▶ Fornisce un'orchestrazione basata su template
  - ▶ Permette di descrivere e automatizzare il deployment dell'infrastruttura
  - ▶ Esecuzione di call a OpenStack API per generare applicazioni cloud eseguibili
- ▶ Il linguaggio del template permette di
  - ▶ Specificare configurazioni del compute, storage e network
  - ▶ Specificare attività post-deployment per automatizzare il provisioning di infrastruttura, servizi, applicazioni
  - ▶ Creare molti dei tipi di risorse OpenStack: istanze, floating IP, volumi, security group e utenti
- ▶ Heat permette agli sviluppatori di integrare il modulo di orchestrazione direttamente o attraverso custom plug-in
  - ▶ Fornisce high availability, instance auto-scaling, e nested stack

# La rete

## ▶ Quattro reti differenti

### ▶ Management network

- ▶ Dedicata a comunicazioni interne tra processi
- ▶ Scambio di informazioni tra servizi OpenStack e servizi di sistema (MySQL, KVM)
- ▶ Isolata e sicura, solo per accesso da servizi che compongono l'infrastruttura

### ▶ Data network

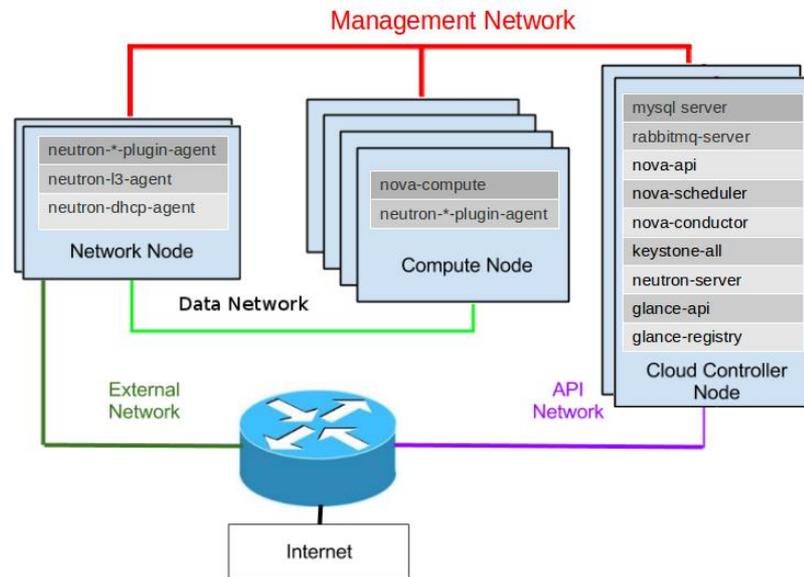
- ▶ Comunicazioni a livello 3 ISO/OSI
- ▶ Isolata e sicura
- ▶ Mappata su una rete fisica disponibile a Neutron o Nova-Network

### ▶ External network

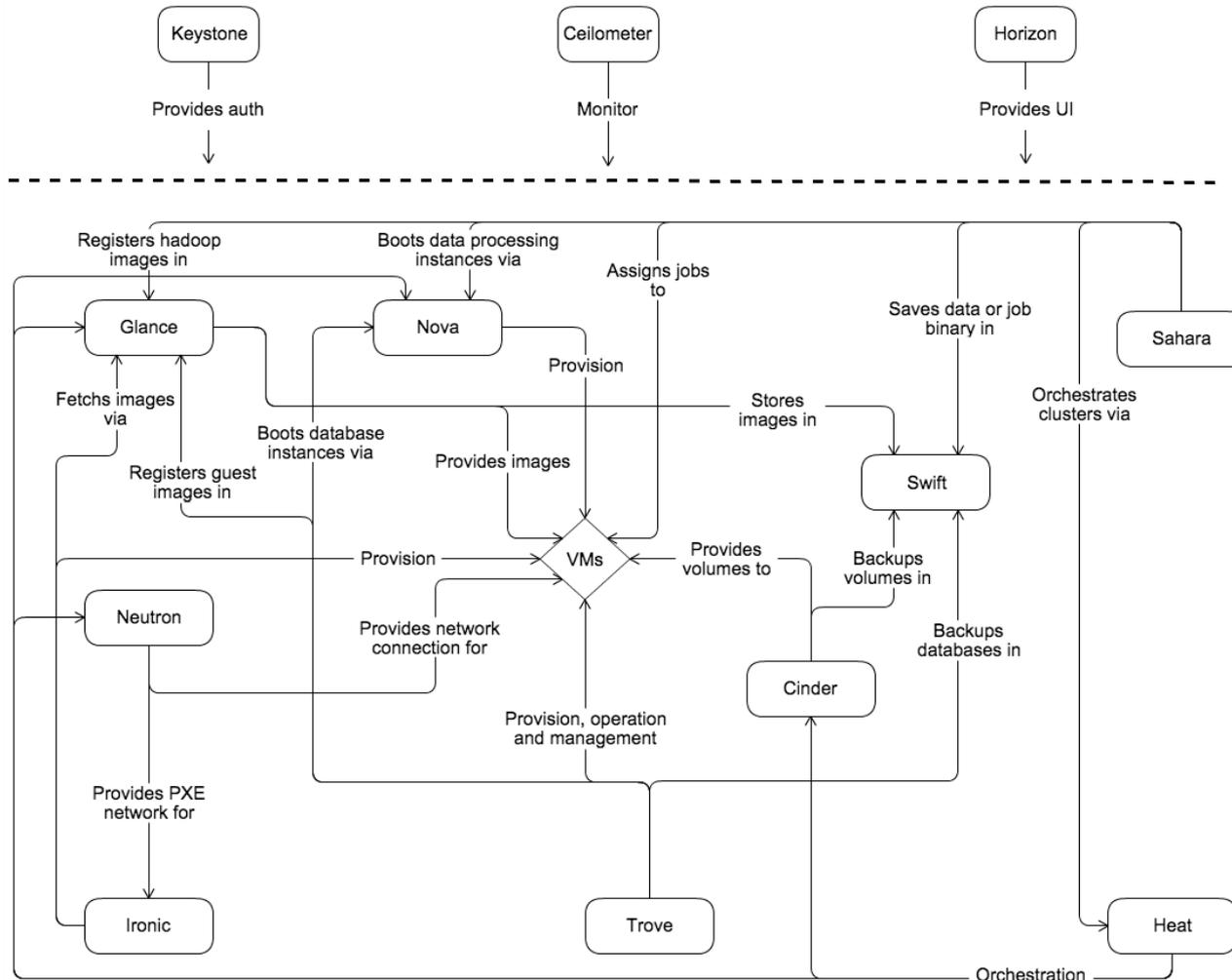
- ▶ Espone servizi OpenStack a utenti esterni
- ▶ Accesso alle istanze da rete esterna

### ▶ API network

- ▶ Rete dedicata per messaggi diretti alle API pubbliche dei servizi

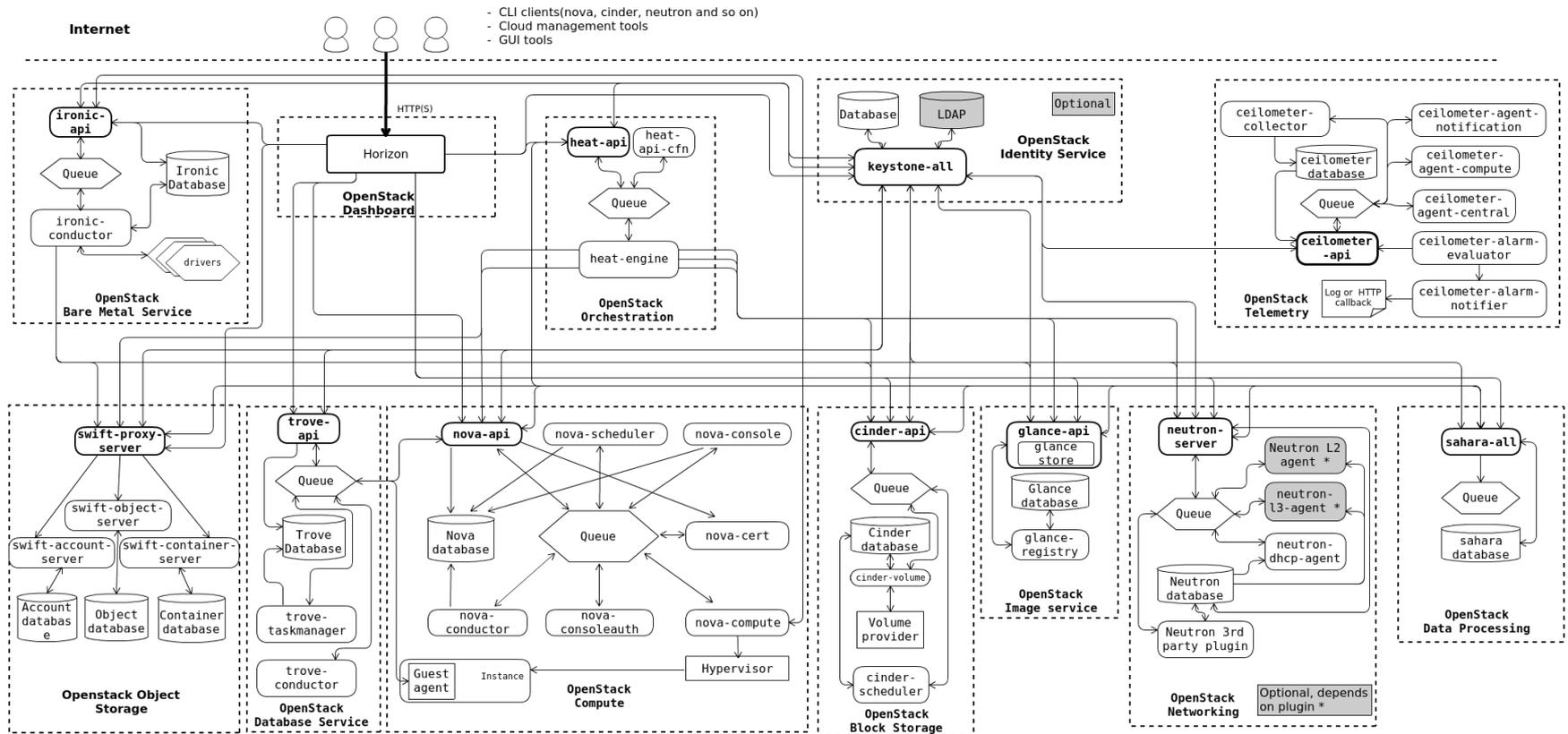


# Architettura concettuale



# Architettura logica

- Comunicazione attraverso API REST
- Interazione tra servizi



# Architettura logica

- ▶ Tutti i servizi si autenticano con Identity service
- ▶ Servizi interagiscono attraverso API pubbliche
  - ▶ Unica eccezione comandi di amministrazione privilegiati
- ▶ Servizi OpenStack composti da diversi processi
  - ▶ Tutti i servizi hanno un API process che è in ascolto per eventuali richieste, preprocessa le richieste e le distribuisce a chi deve gestirle
- ▶ Comunicazioni tra processi avvengono con un AMQP message broker e stato di un servizio memorizzato in un database
  - ▶ Diverse opzioni RabbitMQ, Qpid, MySQL, MariaDB, and SQLite
- ▶ Accesso a OpenStack attraverso interfaccia web (implementata da dashboard service), client da linea di comando, e richieste API con plug-in del browser o curl

# Conclusioni

- ▶ Abbiamo analizzato le caratteristiche di una soluzione IaaS
- ▶ Diversi approcci disponibili
- ▶ OpenStack fornisce una soluzione OpenSource molto utilizzata

**QUESITI?**

[vincenzocalabro.it](http://vincenzocalabro.it)

