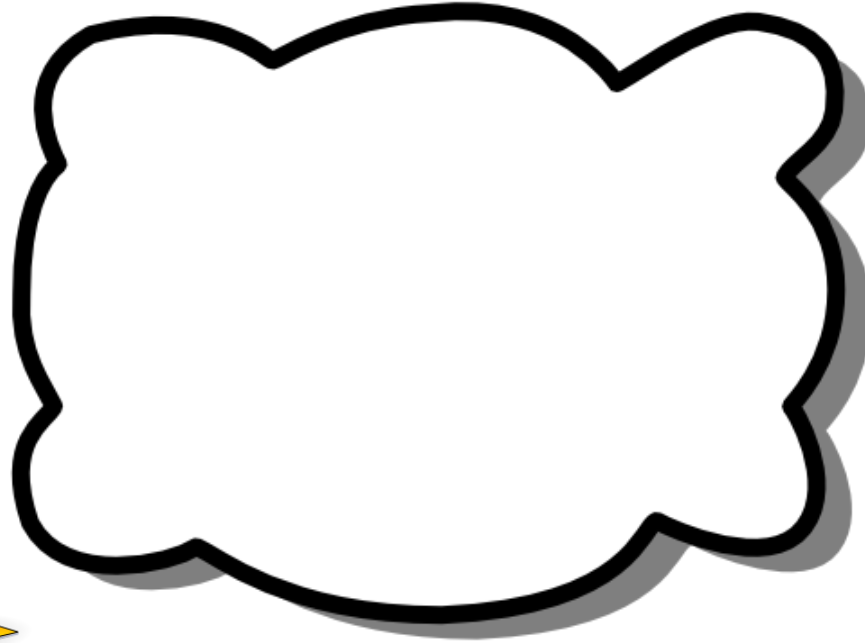
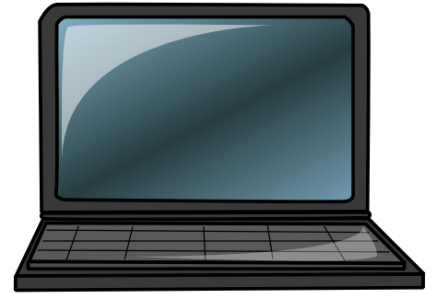
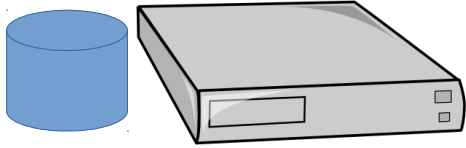


# **FUNDAMENTOS DE CLOUD COMPUTING**

# CLOUD COMPUTING



# DIRIGIDO A

- Desarrolladores 50%.
- Administradores 50%.



# Dev-Ops

# 80-20

# CONTENIDO DEL CURSO

- INTRODUCCIÓN
- COMPONENTES
- MODELOS DE NUBES
- SEGURIDAD, AUDITORÍA Y CUMPLIMIENTO (NORMATIVO)
- PLATAFORMAS VARIAS
- AMAZON WEB SERVICES
- OPENSTACK
- OPENSIFT

# INDICE

- INTRODUCCIÓN

- Qué es Cloud Computing.
- Diferentes tipos de Cloud Computing.
- Modelos básicos en la nube.

- COMPONENTES DE LA NUBE

- Hardware Cloud.
- Virtualización.
- Cloud Storage.
- Grid Computing.
- Computing Transaccional
- Software Cloud.
- SaaS
- Disponibilidad On-Demand.
- Pago por uso.
- SOA y la nube.

- MODELOS DE NUBES

- PaaS.
- IaaS.
- SaaS.
- Nubes privadas.
- Nubes públicas.
- Nubes híbridas.

- SEGURIDAD, AUDITORÍA Y CUMPLIMIENTO (NORMATIVO)

- Puntos clave.
- La seguridad en la nube.
- Gestión de identidades.
- Disaster Recovery.
- Escalar una infraestructura en la nube.
- SLAs en la nube.
- Aspectos legales.
- Estándares nebulosos.

- PLATAFORMAS VARIAS

- Amazon Web Services.
- Microsoft Azure.
- Rackspace Cloud.
- HP Cloud Services.
- Google Cloud Platform.
- Red Hat OpenShift.
- Heroku.
- Open Nebula.

- AMAZON WEB SERVICES

- Qué es AWS.
- Una visión integral.
- Qué podemos hacer con AWS.
- Infraestructura.
  - Amazon EC2.
  - S3.
  - SimpleDB.
  - CloudFront.
  - SQS.
  - Elastic Map Reduce.
  - RDS
- Amazon Virtual Private Cloud.
- Soluciones AWS.

- OPENSTACK.

- Introducción a OpenStack.
- Componentes de OpenStack.
- Hardware.
- Ejemplos de arquitectura.
- Implantación de la infraestructura de OpenStack.
- Almacenamiento.
- Redes.
- Introducción a OpenStack Horizon.
- Trabajar con instancias GNU/Linux.
- Trabajar con instancias Windows.

- OPENSIFT

- Introducción a OpenShift.
- Componentes.
- Instalación.
- Uso y configuración.
- Herramientas asociadas.

## APP

- Uso externo
- Muchos clientes



## Navegador

- Uso interno
- Pocos clientes



**API  
Server**



**Web  
Server**



**DB  
Server**



**BD  
páginas**



**Usuarios**

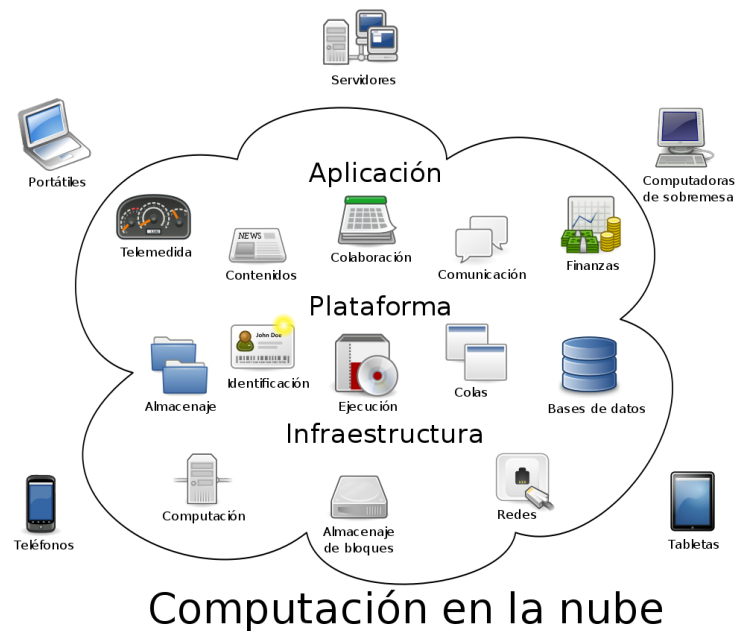
# 1. INTRODUCCIÓN

Que es cloud computing

Diferentes tipos de Cloud Computing

Modelos Básicos en la nube

# Qué es Cloud Computing





# AWS



- Cloud computing is the on-demand delivery of compute power, database, storage, applications, and other IT resources via the internet with pay-as-you-go pricing. Whether you are using it to run applications that share photos to millions of mobile users or to support business critical operations, a cloud services platform provides rapid access to flexible and low cost IT resources
- Agilidad
- Elasticidad
- Reducción de costes
- Rápido despliegue global

# Google Cloud



- In cloud computing, the capital investment in building and maintaining data centers is replaced by consuming IT resources as an elastic, utility-like service from a cloud “provider” (including storage, computing, networking, data processing and analytics, application development, machine learning, and even fully managed services).
- COST
  - Resources can be purchased and consumed on a “pay-as-you-go” basis, and increased or decreased as needed for optimal utilization.
  - Capital expenses can be converted into operating expenses.
- SPEED
  - Cloud customers can focus on rapid innovation without the expense and complexities of hardware procurement and infrastructure management.
- PRODUCTIVITY
  - End-user productivity is likely enhanced because no software is installed, configured, or upgraded on personal devices, and services can be accessed from anywhere.
- PERFORMANCE
- RELIABILITY
- SECURITY
  - Infrastructure functionality, performance, reliability, and security are likely to improve because customers can benefit from “vertically integrated” stacks that are customized at every level — which would be out of reach for on-premises deployments built from off-the-shelf components.



# Azure

- Simply put, cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet (“the cloud”) to offer faster innovation, flexible resources, and economies of scale. You typically pay only for cloud services you use, helping you lower your operating costs, run your infrastructure more efficiently, and scale as your business needs change.
- COST
- GLOBAL SCALE
- PERFORMANCE
- SECURITY
- SPEED
- PRODUCTIVITY
- RELIABILITY

# IBM



- Cloud computing, often referred to as simply “the cloud,” is the delivery of on-demand computing resources — everything from applications to data centers — over the internet on a pay-for-use basis.
- ELASTICIDAD
  - Elastic resources: Scale up or down quickly and easily to meet changing demand.
- COSTE
  - Metered services: Pay only for what you use.
- Self-service
  - Find all the IT resources you need, with self-service access.

# USOS

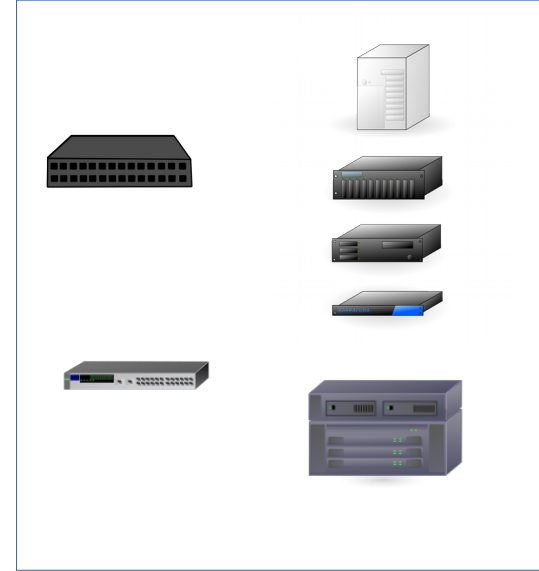
- Creación aplicaciones nativas para cloud.
- Almacenar, Guardar y Recuperar Datos.
- Audio y Video Stream.
- Proporcionar Software on demand.
- Desarrollar y Probar aplicaciones.
- Analizar Datos.
- Aportar inteligencia.

# BENEFICIOS

- Eficiencia de costes
- Posibilidad de elegir entre muchas posibilidades
- Escalado: flexibilidad y elasticidad.
- Rapidez para poner productos en el mercado.
- Integración.
- Reutilización.
- Auditoria y Cumplimiento.
- Continuidad en la planificación de negocio.

# Descomposición en elementos.

- Componentes de uso de un “servicio cloud”
  - Puesto de trabajo para acceso.
  - Infraestructura de Comunicaciones.
  - Servicio.



# Puesto de acceso

- Laptop o desktop
- Comunicaciones seguras
  - ssh
  - vpn
- Terminal de comandos.
- Escritorio remoto.
- Navegador.
- IDE integrado.



# Comunicaciones

- Seguridad extremo a extremo.
  - Por software
    - Certificado de identidad.
    - Cifrado (encriptado).
    - SSH
    - VPN
  - Por hardware (?)
    - Mediante router VPN.
    - Línea dedicada.
- Ancho de banda adecuado.

# Servicio

- Punto de entrada.
  - Identificación y seguridad.
  - Consola web
  - Terminal de comandos.
- Punto de destino.
  - Equipo para desarrollo.
  - Equipo especializado: BD, Web, etc.
- Punto de destino ejecución.
  - Load Balancer.
  - Equipo de ejecución de la aplicaciones.
  - Equipo especializado: BD, Web, etc.
- Punto de destino disco.

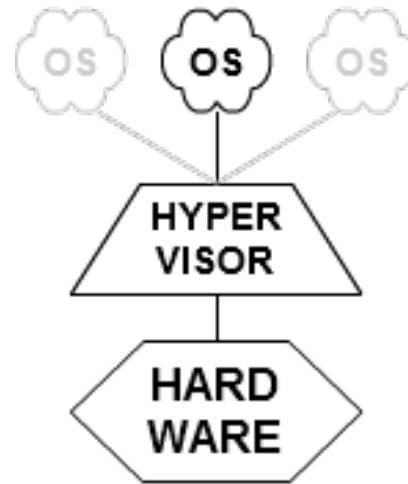
# Componentes y Tecnologías

- Virtualización.
- Contenedores.
- Redes Virtuales.
- Volúmenes.
- Orquestación (de contenedores).
- Load Balancing.
- Escalado.
- Serverless (lambda).
- Topología geográfica.
- SDK.
- Repositorio.

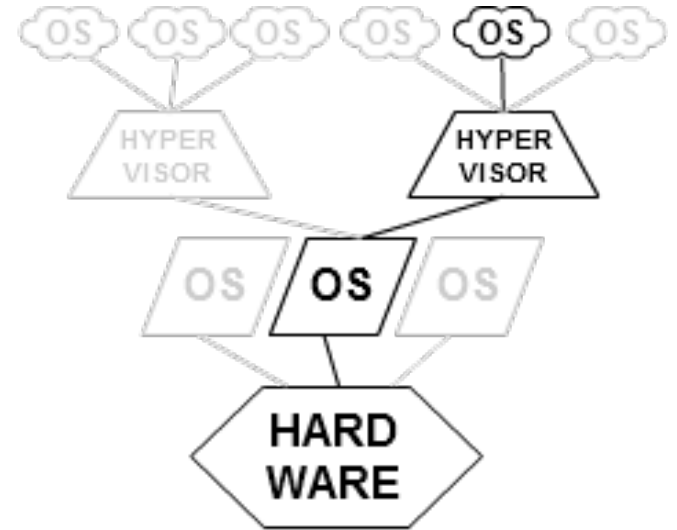
# Virtualización.

- Compartir procesador entre diferentes sistemas operativos
  - Transparentemente.
- Hypervisor. Virtual Machine Monitor.
- Máquina virtual.

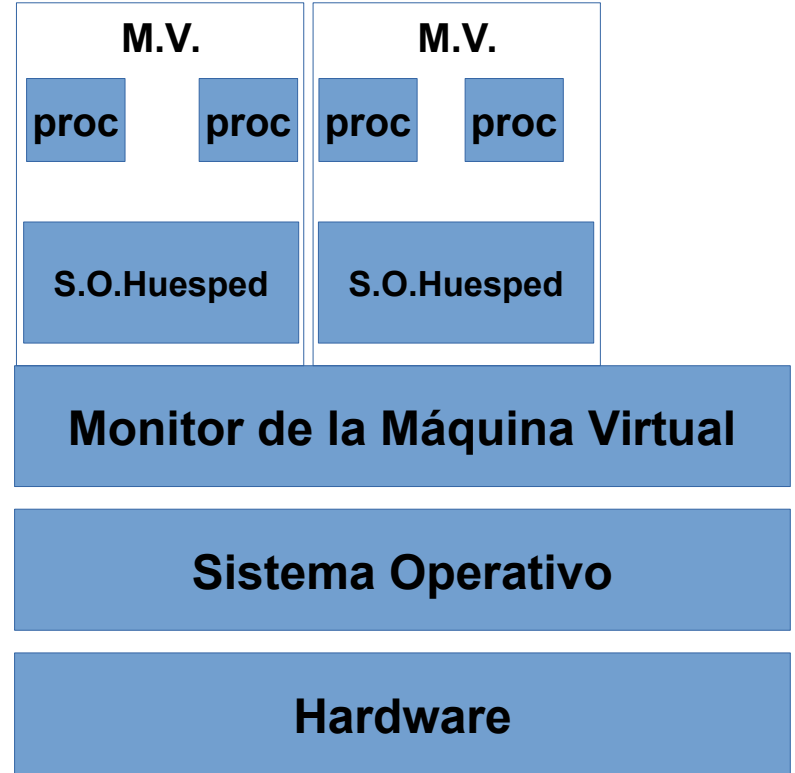
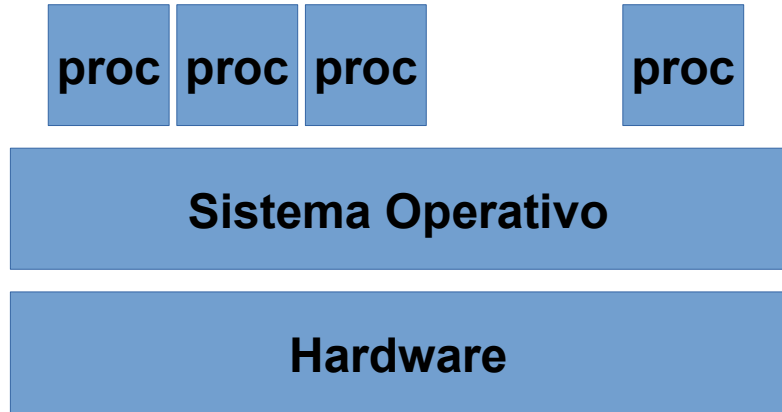
- Productos
  - Xen
  - Vmware
  - VirtualBox
  - Parallels
  - QEMU
- Kernel modules
  - KVM (Linux)
  - Bhyve (freeBSD)



**TYPE 1**  
*native*  
(bare metal)



**TYPE 2**  
*hosted*

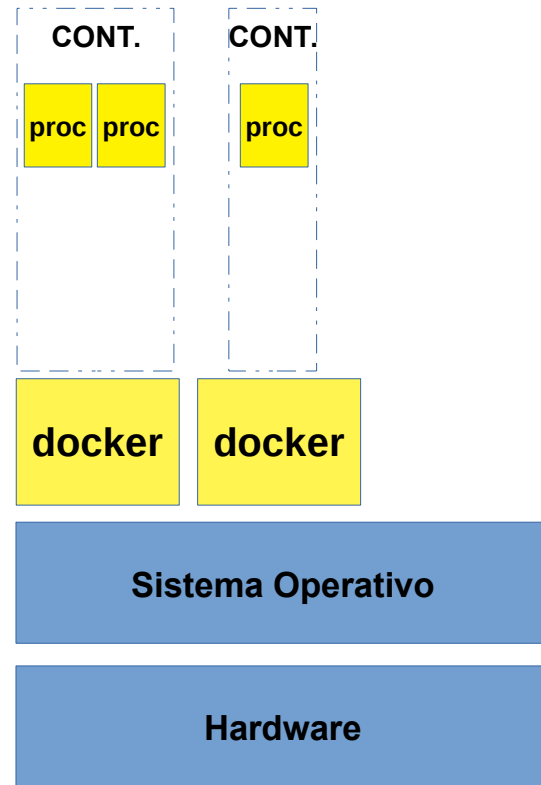
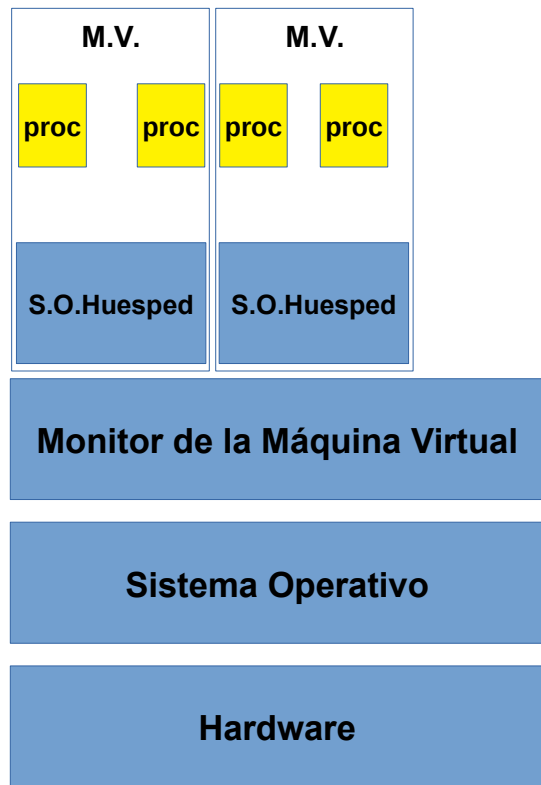
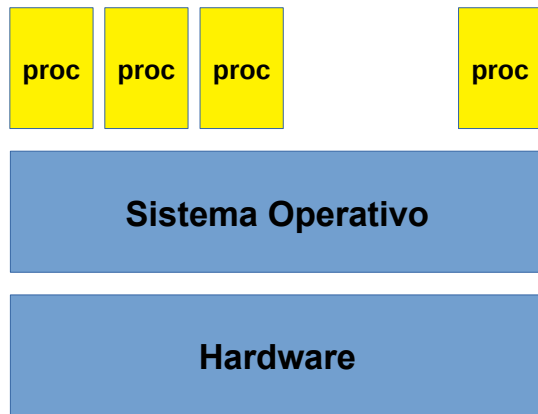


# Contenedores.

- OS-level virtualización.
  - Coexistencia de múltiples espacios de usuario, aislados, gestionados por el kernel.
  - Chroot
  - Docker
  - Linux-Vserver
  - LXC
  - FreeBSD jail
  - WPARs (AIX)
  - RKT
- Cgroups y namespaces en Linux.







# Redes Virtuales.

- Red implementada en software.
  - No necesita una tarjeta de red física.
- Tantas como se necesite.
- Facilita topologías adecuadas a la estructura de la aplicación.

# ssh y VPN

- Protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente.
  - La conexión se hace encriptada.
- Se recomienda utilizar protocolo 2.
- VPN
  - Túnel que encapsula la comunicaciones entre dos nodos.

# Archivos de configuración OpenSSH

- **ssh\_config**
  - El archivo de configuración del sistema cliente SSH por defecto que se sobrescribe si hay alguno ya presente en el directorio principal del usuario (~/.ssh/config).
- **sshd\_config**
  - El archivo de configuración para el demonio sshd.
- **ssh\_host\_dsa\_key**
  - La clave privada DSA usada por el demonio sshd.
- **ssh\_host\_dsa\_key.pub**
  - La clave pública DSA usada por el demonio sshd.
- **ssh\_host\_key**
  - La clave privada RSA usada por el demonio sshd para la versión 1 del protocolo SSH.
- **ssh\_host\_key.pub**
  - La clave pública RSA usada por el demonio sshd para la versión 1 del protocolo SSH.
- **ssh\_host\_rsa\_key**
  - La clave privada RSA usada por el demonio sshd para la versión 2 del protocolo SSH.
- **ssh\_host\_rsa\_key.pub**
  - La clave pública RSA usada por el demonio sshd para la versión 2 del protocolo SSH.

# Información específica por usuario

- **authorized\_keys**

- Este archivo que contiene una lista de claves públicas "autorizadas". Cuando un cliente se conecta al servidor, el servidor valida al cliente chequeando su clave pública firmada almacenada dentro de este archivo.

- **id\_dsa**

- Contiene la clave privada DSA del usuario.

- **id\_dsa.pub**

- Contiene la clave pública DSA del usuario.

- **id\_rsa**

- La clave RSA privada usada por ssh para la versión 2 del protocolo SSH.

- **id\_rsa.pub**

- La clave pública RSA usada por ssh para la versión 2 del protocolo SSH.

- **Identity**

- La clave privada RSA usada por ssh para la versión 1 del protocolo SSH.

- **identity.pub**

- La clave pública RSA usada por ssh para la versión 1 del protocolo SSH.

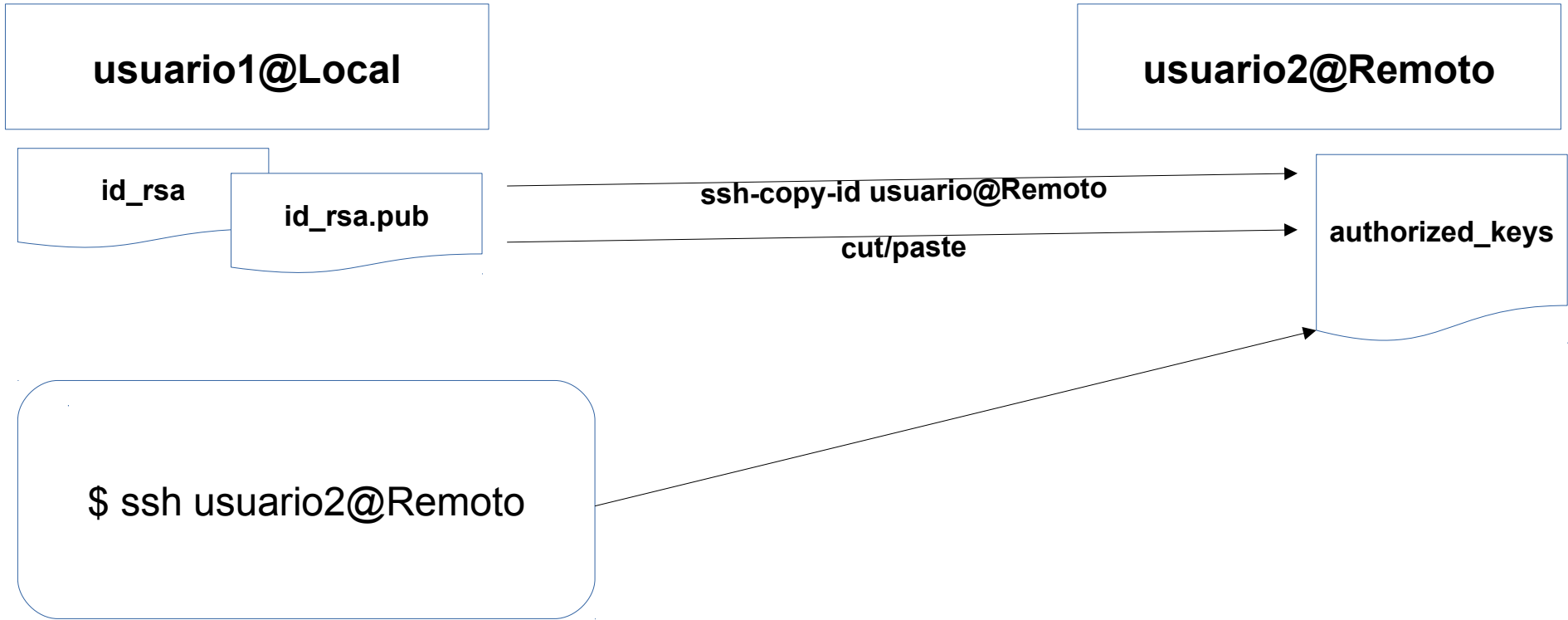
- **known\_hosts**

- Este archivo contiene las claves de host DSA de los servidores SSH accedidos por el usuario. Este archivo es muy importante para asegurarse de que el cliente SSH está conectado al servidor SSH correcto.

# Autenticación del cliente

- Por password.
- Por clave pública.

# Certificados



# Port forwarding

- Port forwarding (ssh tunneling).
  - `ssh -L 127.0.0.1:9991:host.domain:9091 user@host.domain`
- Acceso a una aplicación remota a través de un puerto local.
- Acceso a una aplicación local desde un puerto remoto.



# Volúmenes.

- Un volumen es almacenamiento permanente, que se puede compartir entre los contenedores de un pod.
  - El sistema de ficheros es efímero. Los datos no se guardan después de una parada/finalización.
- Cada proveedor proporciona al menos dos tipos:
  - Almacenamiento persistente por tamaño.
  - Almacenamiento persistente escalable/elástico.

# Orquestación.

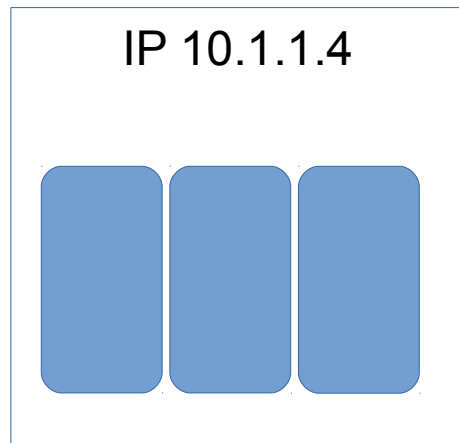
- Configuración automatizada, coordinación y gestión de sistemas de computación y de software.
  - Ansible, Puppet, Salt, Terraform, AWS Cloud Formation
  - Kubernetes, AWS EKS, AWS ECS, Amazon Fargate, OpenStack Heat,
- Kubernetes
  - Plataforma para automatización del despliegue, escalado y gestión de contenedores de aplicación en clusters de hosts.

# Objetos de Kubernetes.

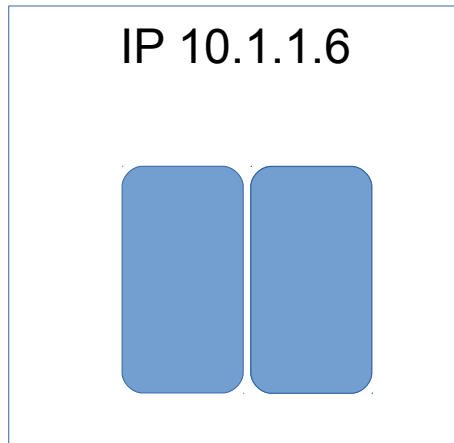
- Pods.
  - Conjunto de contenedores alojados en el mismo nodo.
- Servicio.
  - Conjunto de pods trabajando conjuntamente.
- Replica Sets
  - Agrupación de instancias de un mismo pod.
- StatefulSets
- DaemonSets
- Replication Controller.
  - Gestor de réplicas de pods que asegura que en todo momento están ejecutando las réplicas indicadas del pod.
- Deployment
  - Equivalente a una aplicación.

# Service

**Servicio**



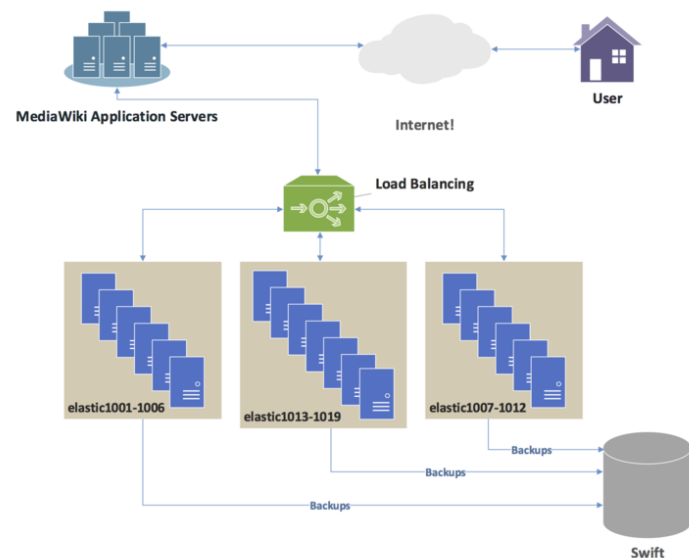
Pod WEB

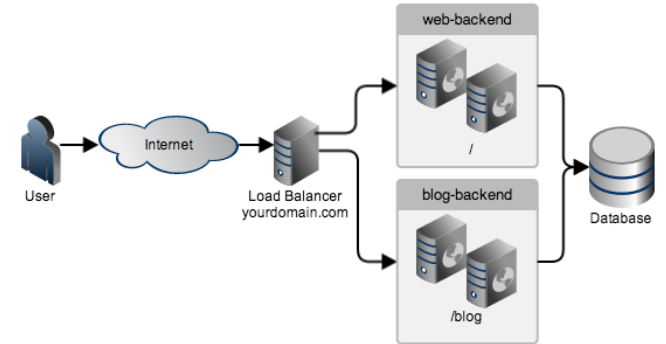
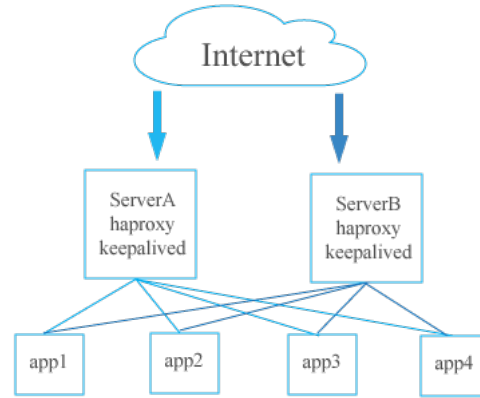
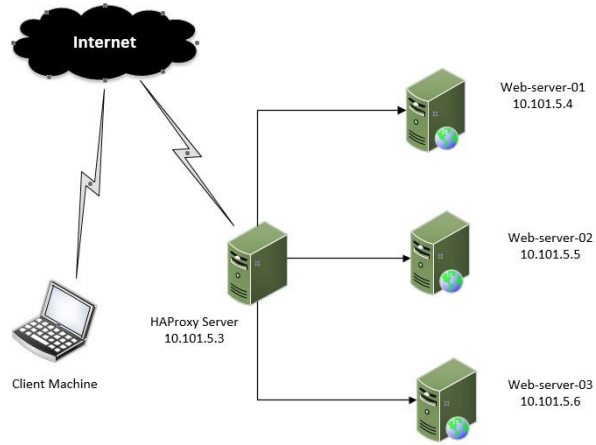


Pod  
API

# Load Balancing.

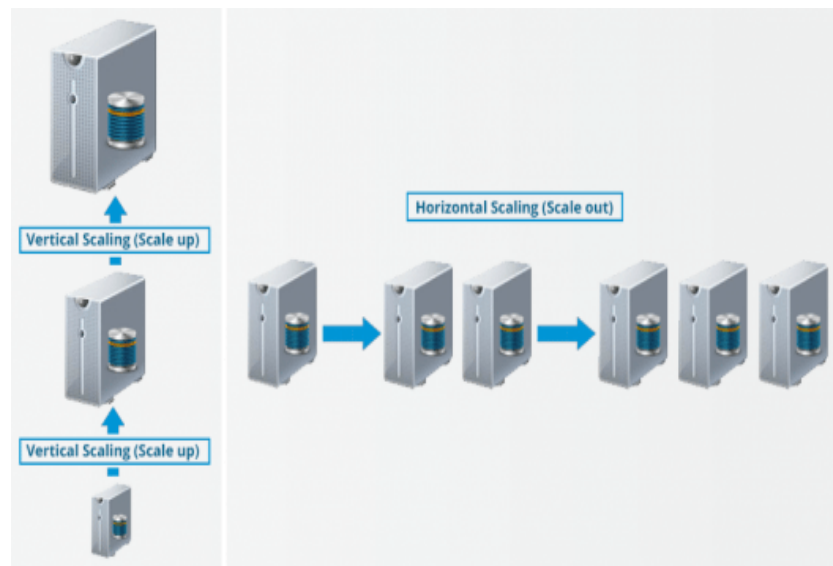
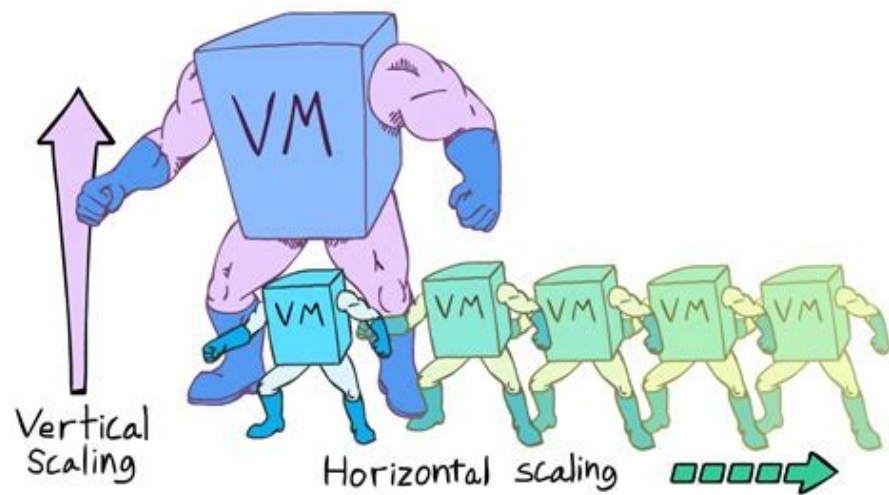
- Distribuir las peticiones entre distintos servidores (o ventanillas).
- Algoritmos
  - Round-Robin.
  - Prioridad.
  - Contenido.
- Reconfiguración de los servidores según la carga de trabajo: autoescalado.
  - Health-check





# Escalado.

- Aumentar (o Reducir) los recursos de una aplicación.
  - En el contexto de cloud computing.
- Horizontal
  - Aumentar las réplicas o los nodos.
  - No todas las aplicaciones admiten escalado horizontal
  - La aplicación debe recoger en su diseño esta propiedad.
    - Contenedores y Pods de Kubernetes lo tienen por construcción.
- Vertical
  - Aumentar la “potencia” de un nodo o una réplica.





# Escalado de la Base de Datos.

- Transacciones distribuidas con “two-phase commit”.
- Database replication.
  - Master-Slave.
    - El “Master” consolida los cambios, que envia a los “Slaves”.
  - Multi-Master.
    - Varios “Master” consolidan cambios e informan a los restantes nodos.
  - Distribuida.
    - Red de servidores.

# Storage Replication

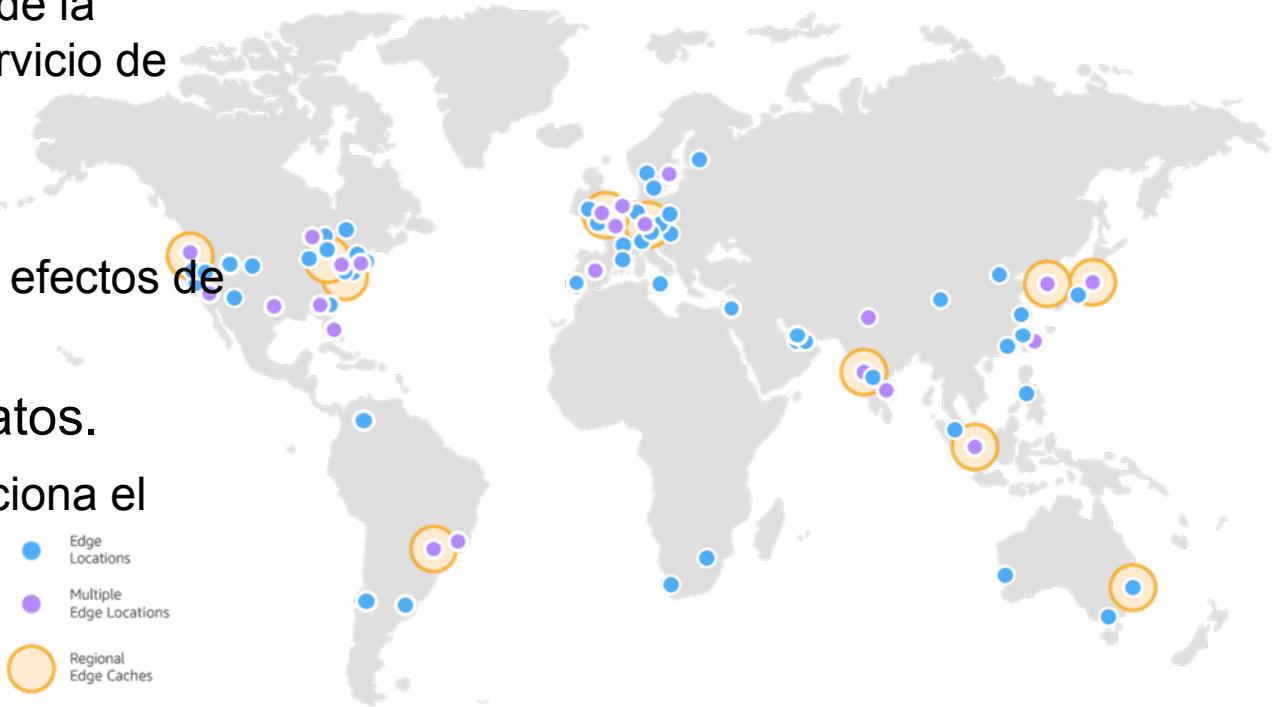
- A nivel hardware
  - Hardware disk mirroring, RAID
  - Por software en red o con un driver software.
- Por software

# Serverless/lambda

- Ejecución de código
  - Sin gestión de la infraestructura.
  - Con escalado automático.

# Topología Geográfica

- Regiones
  - Particiones independientes de la geografía para prestar el servicio de Cloud Computing.
- Zonas de Disponibilidad
  - Subdivisión de una región a efectos de redundancia.
- Ubicaciones/Centros de Datos.
  - Sitio físico donde se proporciona el servicio.



# SDK

- Conjunto de componentes software que permiten a una aplicación utilizar y gestionar los servicios de provisión, configuración, mantenimiento y gestión de productos y servicios de cloud computing.
  - La funcionalidad de la consola de gestión del cloud disponible en una aplicación.

# Repositorio

- Almacen.
- Control de versión.
- Proveedores
  - Github
  - Bitbucket

# Diferentes tipos de Cloud Computing

- Infraestructura.
- Plataforma.
- Software.
- Serverless.

# Modelos básicos en la nube

- Pública.
- Privada.
- Híbrida.



## **2. COMPONENTES DE LA NUBE**

# Hardware Cloud

- Elementos físicos.
  - Host, Disco, Red.

# Virtualización

- Compartir un host “anfitrión” entre varios host “invitados”.
  - Independencia.
  - Aislamiento.

# Cloud Storage

- Discos
- Discos orientados a volúmenes.
  - Bucket, Blobs, etc.
- Storage Area Network.

# Grid Computing

- Red de computadores operando coordinadamente para realizar un trabajo.
  - Sistema distribuido.
  - Cada nodo realiza una parte del trabajo global.
- Balanceo/Distribución de la carga de trabajo
  - Estática o Dinámica.
- Disponibilidad Alta, con tolerancia a fallos.

# Computing transaccional

- Operaciones indivisibles denominadas transacciones.
- Una transacción no puede finalizar en un estado indefinido.
  - Commit
    - Finaliza, consolida, llevando al sistema a un nuevo estado conocido.
  - Rollback
    - No Finaliza, dejando al sistema en el estado previo al comienzo de la transacción.
- ACID
  - Atomicidad.
  - Consistencia.
  - Isolation/Aislamiento.
  - Durabilidad.
- Deadlock, Interbloqueo de transacciones.
- Transaction Log.
- Two Phase Commit.
  - Votación + Consolidación.
- Tecnología clave para recursos compartidos, típicamente una Base de Datos, pero no exclusivamente.
  - Registro de información (usuarios, certificados, etc.)
  - Sistema de ficheros.

# Software Cloud

- Aplicación (o programa) que ejecuta en un servicio Cloud Computing.
  - Reside en el cloud.
- Se accede desde un puesto de trabajo mediante un navegador o similar.
  - Infraestructura local mínima.
- Dependencia de las comunicaciones.

# SaaS

- Un modelo de Cloud Computing para utilizar Software
  - Aplicaciones, paquetes, entornos.
- Google Docs.
- Office 365.



# Disponibilidad On-Demand

- Asignación de recursos en función de la carga de trabajo a lo largo del tiempo.
  - Absorción de picos y valles.
- Ajuste de costes según la carga.

## Pago por uso

- Pago por los recursos realmente utilizados durante un periodo de tiempo.
- Ahorro de costes frente a una infraestructura permanente.

# SOA y la nube

- Service Oriented Architecture
  - Paradigma basado en componentes de aplicaciones que ofrecen servicios a otros componentes.
  - Un servicio es una unidad funcional que encapsula un componente de negocio.
  - Protocolo de comunicaciones.
- Puede implementarse en un Cloud Computing.
- Microservicios.

# **3. MODELOS DE NUBES**

# MODELOS DE NUBES

## DESPLIEGUE

### **Nubes Públicas**

Proporciona servicios a cualquiera.

### **Nubes Privadas**

Proporciona servicios internamente a una organización.

### **Nubes Híbridas**

Parte pública y parte privada.

### **Nubes Múltiples**

Utilizar los servicios de varias nubes.

## MODO DE SERVICIO

### **SaaS**

Uso de Aplicaciones.

### **PaaS**

Desarrollo, Paquetes, IDE, BD, Web Server

### **Serverless**

Desarrollo de aplicaciones sin necesidad de manipular servidores.

### **IaaS**

M. Virtual, Servidor, Almacenamiento, Red, Distribuidores

# Nubes públicas

- Modelo de negocio que ofrece servicio de Cloud Computing.
  - Infraestructura.
  - Plataforma.
  - Software.
- Ahorro de costes.

# Nubes privadas

- Implantación interna en una organización de servicios de Cloud Computing.
- Seguridad.
- Ventaja competitiva.

# Nubes híbridas

- Uso simultáneo de nubes públicas y privadas.
- Google Cloud Platform emplea (dice) los mismos servidores que utilizan sus propios servicios.
- La parte privada retiene los activos sensibles.
- La parte pública emplea
  - SaaS para incorporar las últimas aplicaciones.
  - IaaS para elasticidad y ahorro en costes.



# MÚLTIPLES NUBES

- Una compañía que utiliza Cloud Computing de varios proveedores.
  - 85% ya operan con dos o más Cloud

# IaaS Infrastructure as a Service

- Infrastructure as a Service, sometimes abbreviated as IaaS, contains the basic building blocks for cloud IT and typically provide access to networking features, computers (virtual or on dedicated hardware), and data storage space. Infrastructure as a Service provides you with the highest level of flexibility and management control over your IT resources and is most similar to existing IT resources that many IT departments and developers are familiar with today.

# PaaS Platform as a Service

- Platforms as a service remove the need for organizations to manage the underlying infrastructure (usually hardware and operating systems) and allow you to focus on the deployment and management of your applications. This helps you be more efficient as you don't need to worry about resource procurement, capacity planning, software maintenance, patching, or any of the other undifferentiated heavy lifting involved in running your application.

# SaaS Software as a Service

- Software as a Service provides you with a completed product that is run and managed by the service provider. In most cases, people referring to Software as a Service are referring to end-user applications. With a SaaS offering you do not have to think about how the service is maintained or how the underlying infrastructure is managed; you only need to think about how you will use that particular piece software.

# Serverless

- Ejecutar código sin gestionar o provisionar servidores.
  - El proveedor de Cloud Computing proporciona transparentemente
    - Provisión.
    - Escalado.
    - Gestión de la Infraestructura.
- No hay que gestionar la infraestructura.
- Escalado dinámico.
- Reducción del time to market.
- Reducción de recursos.

# **4. SEGURIDAD, AUDITORÍA Y CUMPLIMIENTO EN LA NUBE**

**Puntos claves**

**La seguridad en la nube**

**Gestión de identidades**

**Disaster Recovery**

**Escalar una infraestructura en la nube**

**SLAs en la nube**

**Aspectos legales**

**Estándares nebulosos**

# Puntos claves

- Trabajar con un proveedor de Cloud Computing.
- Riesgos que hay que valorar.
- Minimizar los riesgos.
- Confidencialidad de la información.
- Responsabilidad derivada de incidentes relacionados con la infraestructura.
- Responsabilidad legal.

# Cuestiones legales clave (ENISA)

- Protección de datos
  - Disponibilidad e integridad
  - Normas mínimas o garantía
- Confidencialidad
- Propiedad intelectual
- Negligencia profesional
- Servicios de subcontratación y cambios de control



# Riesgos Politicos y organizativos.

- Vinculación.
- Pérdida de gobernanza.
- Desafíos de cumplimiento.
- Pérdida del renombre empresarial a raíz de actividades de prestación conjunta.
- Cancelación del servicio cloud.
- Adquisición del proveedor del servicio cloud.
- Fallo en la cadena de suministro del proveedor del servicio cloud..

# Riesgos Técnicos.

- Agotamiento de recursos (por exceso o insuficiencia).
- Fallo de aislamiento.
- Miembros maliciosos.
- Compromiso de la interfaz de gestión.
- Interceptación de datos en tránsito.
- Fuga de datos (carga /descarga).
- Supresión de datos insegura o ineficaz.
- Distribución de denegación de servicio (DdoS).
- Denegación económica de servicio (EdoS).
- Pérdida de claves de codificación.
- Realización de escaneados o detecciones maliciosas (sniffing).
- Motor de servicio comprometido.
- Conflictos entre los procedimientos de refuerzo del cliente y el entorno de la nube.

# Riesgos Legales.

- Órdenes judiciales y descubrimiento electrónico.
- Riesgo derivado del cambio de jurisdicción.
- Riesgos de la protección de datos.
- Riesgos relativos a la licencia.

# Riesgos no específicos del servicio cloud.

- Brechas.
- Gestión de la red (congestión, fallo en la conexión, uso no óptimo).
- Modificación del tráfico de la red.
- Escalada de privilegios.
- Ataque de ingeniería social.
- Pérdida o compromiso de los registros operativos.
- Pérdida o compromiso de los registros de seguridad.
- Pérdida o robo de las copias de seguridad.
- Acceso no autorizado a los locales (acceso físico).
- Robo de equipos informáticos.
- Catástrofes naturales.

# Gestión de identidades

- Controles de seguridad
  - Evitar el uso de la cuenta root, la primera cuenta creada en AWS, que tiene derechos administrativos.
  - Forzar un segundo factor de autenticación para acceder a la consola.
  - Deshabilitar credenciales no utilizadas en los últimos 90 días (o menos).
  - Rotación de claves de acceso.
  - Contraseñas fuertes.
  - Monitorizar accesos a los puertos 22 y 3389.

- Gestión de registros (logs).
- Monitorización.
- Redes.

# SLAs en la nube

- Máxima concreción.
  - Seguridad.
  - Privacidad.
  - Disponibilidad.
- Derecho a realizar auditorias.
- Penalizaciones por incumplimiento
  - Tiempos.
  - Requisitos regulatorios.
  - Disponibilidad.

# Vulnerabilidades (ENISA)

- AAA (Autenticación, Autorización y Auditoria).
- Alta y Baja de usuarios.
- Acceso remoto a la interfaz de gestión.
- Hypervisor.
- Aislamiento de los recursos.



- Aislamiento de la reputación.
- Codificación de la codificación de la comunicación.
- Codificación de archivos y datos en tránsito.
- Imposibilidad de procesar datos codificados.
- Procedimientos insuficientes de gestión de claves.

- Generación de claves.
- Falta de tecnologías y soluciones estándar. Dependencia de un proveedor.
- Ausencia de un acuerdo de depósito de fuentes. Quiebra del proveedor.
- Modelado inadecuado del uso de recursos.
- Falta de control en el proceso de evaluación de vulnerabilidad.
- Análisis interno de la red por otros clientes.

- Comprobaciones de coresidencia, por falta de aislamiento.
- Ausencia de disponibilidad experta (logs, instantáneas de disco, etc.).
- Limpieza de medios sensibles, con fuga de datos.
- Sobreinterpretación de las responsabilidades del proveedor de cloud.
- Aplicaciones inter-cloud que provocan dependencia oculta.

- Cláusulas SLA en conflicto con otras cláusulas del contrato.
- Cláusulas SLA con riesgo para el negocio.
- Auditoria o certificación no disponible para los clientes.
- Sistemas de certificación no adaptados para los servicios en cloud.
- Provisión de recursos inadecuada.

- Ausencia de políticas de limitación de recursos.
- Almacenamiento de datos en jurisdicciones múltiples con falta de transparencia.
- Falta de información sobre jurisdicciones.
- Falta de integridad y transparencia en los términos de uso.

# Vulnerabilidades no específicas de la nube.

- Ausencia de conciencia de seguridad.
- Falta de procesos de investigación.
- Funciones y responsabilidades confusas.
- Aplicación deficiente de las definiciones de funciones.
- No aplicación del principio de “Need-To-Know”.

- Procedimientos de seguridad física inadecuados.
- Configuración deficiente.
- Vulnerabilidades del sistema operativo, o del sistema de gestión del cloud.
- Software que no es de confianza.

- Falta de plan de continuidad del negocio y de recuperación de desastres, o plan deficiente y no puesto a prueba.
- Propiedad de los activos confusa.
- Identificación insuficiente de los requisitos del proyecto.



- Selección de proveedores insuficiente.
- Ausencia de redundancia de suministrador.
- Vulnerabilidades de la aplicación o de la gestión de parches.
- Vulnerabilidades en el consumo de recursos.

- Incumplimiento del acuerdo de no divulgación por el proveedor.
- Responsabilidad por pérdida de datos.
- Falta de políticas o procedimientos insuficientes para la recopilación y retención de registros (logs).
- Recursos de filtrado inadecuados o mal configurados.

# Aspectos legales España.

- Ley de Protección de datos LOPD 15/1999 y Reglamento de Desarrollo.
  - El contrato debe recoger las garantías a las que obliga la LOPD.
  - Si intervienen terceras empresas (subcontratistas) en la prestación de servicios de Cloud Computing, el cliente debe dar su conformidad.
- Localización de los recursos físicos que emplea el proveedor de Cloud. Se aplican las garantías legales del país.

# Cumplimiento Legal y Auditoría.

- Evaluar el nivel de cumplimiento legal
  - políticas de seguridad internas.
  - Requisitos de cumplimiento normativos, legislativos y de otro tipo

Para demostrar el cumplimiento legal durante una auditoria.

- El cliente podrá comprobar las medidas de seguridad o el proveedor del Cloud debe acreditar una certificación de seguridad adecuada.
- Mecanismos para garantizar el borrado seguro de los datos cuando lo solicite el cliente, o al finalizar el contrato.
  - Certificación de destrucción.

# Derechos ARCO (a ejercitar por una persona).

- **Acceso:** Conocer si tus datos personales se están manejando (tratando).
  - 30 días de plazo para resolver.
  - No necesita justificación si no se ha ejercido en los últimos 12 meses.
- **Rectificación:** Solicitar la modificación cuando sean inexactos o incompletos.
  - 10 días hábiles para resolver.
- **Oposición:** al tratamiento de datos personales o al cese de estos cuando:
  - No sea necesario su consentimiento.
  - Cuando se usen con fines publicitarios.
  - Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado,
  - 10 días hábiles para resolver.
- **Cancelación:** solicitar la supresión de los datos que resulten inadecuados o excesivos, sin perjuicio del deber de bloqueo.
  - Aportando justificación documentada, el dato y el motivo.
  - 10 días hábiles para resolver.

# RGPD

- Derecho a la portabilidad de los datos.
  - Solicitar el traslado de los datos a otro responsable.
- Derecho al olvido.
  - Suprimir los datos personales del interesado, sin dilación:
    - No sean necesarios para la finalidad
    - Retire el consentimiento.
    - Derecho a oposición.
    - Tratamiento ilícito.
    - Supresión para cumplimiento de una obligación legal.

# Estándares Nebulosos

- Portabilidad e Interoperabilidad
- Seguridad Física, Continuidad de Negocio y Recuperación de Desastres
- Respuesta, Notificación y resolución de incidentes
- Seguridad de las Aplicaciones
- Cifrado y gestión de claves
- Gestión de Identidades y de Acceso
- Virtualización

# Estándares nebulosos

- No existen estándares específicos para cloud computing.
- Forzar el cumplimiento de los estándares existentes.



# **5. PLATAFORMAS VARIAS**

**Amazon Web Services**

**Microsoft Azure**

**RackSpace Cloud**

**HP Cloud Services**

**Google Cloud Platform**

**Red Hat OpenShift**

**Heroku**

**Open Nebula**

- **Amazon Web Services**
  - IaaS, PaaS
- **Windows Azure**
  - IaaS, SaaS, PaaS
- **RackSpace Cloud**
- **HP Cloud Services**
- **Google App Engine/Google Cloud Platform**
  - IaaS, PaaS
- **Red Hat OpenShift**
- **Heroku**
  - Platform as a Service
- **Open Nebula**
  - IaaS



- **Oracle**
  - **PaaS**
- **IBM**
  - **IaaS, SaaS**
- **Cloud Foundry**
  - **PaaS**
- **Heroku**
  - **PaaS**
- **Apache CloudStack**

- Amazon Web Services
  - Proporciona plataformas de cloud computing bajo demanda (on-demand) y APIs facturado según uso.
    - Computación.
    - Almacenamiento.
    - Base de datos.
    - Redes.
    - Analytics.
    - Servicios de aplicación.
    - Despliegue.
    - Gestión.
    - Herramientas de desarrollo.
  - Amazon Elastic Compute Cloud es un cluster virtual de computadores.
    - Con aplicaciones software precargadas
      - Web servers.
      - Bases de datos.
      - CRM.
- Microsoft Azure
  - Servicio de cloud-computing para construir, probar, desplegar y gestionar aplicaciones y servicios.
    - SaaS, PaaS, IaaS
  - Computación.
  - Almacenamiento.
  - Datos.
  - Media.
  - Mensajes.
  - CDN.
  - Desarrollo.
  - Móvil.
- RackSpace Cloud
  - Conjunto de productos y servicios de cloud computing.
- HP Cloud Services
  - Conjunto de servicios cloud.
- Google Cloud Platform
  - Conjunto de servicios cloud.
- Red Hat OpenShift
  - Familia de productos software para gestión de contenedores
    - OpenShift Container Platform
      - PaaS on-premises para contenedores docker orquestados por kubernetes.
  - OpenShift Online
    - SaaS
  - OpenShift Dedicated
    - Servicio gestionado apoyado en AWS, GCP, Azure.
  - OpenShift Enterprise.
- Heroku
  - PaaS para lenguajes
    - Ruby, java, node.js, scala, clojure, python, php, go.
- Open Nebula
  - Plataforma de cloud computing para gestionar infraestructuras distribuidas de centros de datos heterogéneos.
- Apache CloudStack
  - Software open-source para crear, gestionar y desplegar infraestructura de servicios cloud.

# 6. AMAZON WEB SERVICES



**Qué es AWS**

**Una visión integral**

**Qué podemos hacer con AWS**

**Infraestructura: Amazon EC2, S3, SimpleDB, CloudFront, SQS, Elastic MapReduce, RDS**

**Amazon Virtual Private Cloud**

**Soluciones AWS.**

# Qué es AWS

# Una visión integral

# Qué podemos hacer con AWS



# Infraestructura: EC2 – Elastic Compute Cloud

- Proporciona capacidad de computación segura y redimensionable en la nube.
- Volátiles.
- Reservados.

# S3 - Simple Storage Service

- Almacenamiento. Bucket.
  - Para aplicaciones.
  - Copia de seguridad.
  - Disaster Recovery.
  - Archivo de datos.



# EBS - Elastic Block Store

- Almacenamiento masivo escalable.
- Orientado a sistemas “mission-critical”.
  - El tiempo de respuesta debe estar acotado siempre.
- Volúmenes replicados.

# SimpleDB

- Base de datos NoSQL.
- Alta disponibilidad.
- Replicas transparentes,
- Coste
  - Almacenamiento usado.
  - Distribución de solicitudes.

# CloudFront

- CDN Content Delivery Network
  - Datos.
  - Videos.
  - Aplicaciones.
  - API.

# SQS

- Servicio de Mensajes.
  - Intercomunicación de aplicaciones sin necesidad de servidor
    - Sistema distribuido.
    - Microservicios.

# Elastic MapReduce

- Servicio Web orientado a procesar grandes volúmenes de datos.
  - Cluster Hadoop
  - EC2 + S3.
- Analisis de Datos.
- Investigación.
- Desarrolladores.
- MapReduce de Hadoop.
  - División de los datos en subsegmentos que se procesan en paralelo en los distintos nodos del cluster.

# RDS – Relational Database Service

- Gestión de Base de Datos Relacional.
  - Amazon Aurora
  - PostgreSQL
  - MySQL
  - MariaDB
  - Oracle Database
  - SQL Server
- AWS Database Migration Service
  - Migrar bases de datos existentes.
  - Realizar Replicas.




# VPC - Virtual Private Cloud

- Gestión de una red virtual aislada.
  - IPv4 y/o IPv6.
  - Direcciones IP.
  - Subredes con acceso público o privadas sin acceso.
  - Tablas de routing.
  - Gateways/Puertas de enlace.

▼ All services

🖥️ Compute

EC2  
Lightsail   
ECR  
ECS  
EKS  
Lambda  
Batch  
Elastic Beanstalk  
Serverless Application Repository

💾 Storage

S3  
EFS  
FSx  
S3 Glacier  
Storage Gateway  
AWS Backup


🗄️ Database

RDS  
DynamoDB  
ElastiCache  
Neptune  
Amazon Redshift  
Amazon QLDB  
Amazon DocumentDB

🔄 Migration & Transfer

AWS Migration Hub  
Application Discovery Service  
Database Migration Service  
Server Migration Service  
AWS Transfer for SFTP  
Snowball  
DataSync


🌐 Networking & Content Delivery

VPC  
CloudFront  
Route 53  
API Gateway  
Direct Connect  
AWS App Mesh  
AWS Cloud Map  
Global Accelerator 

🔧 Developer Tools

CodeStar  
CodeCommit  
CodeBuild  
CodeDeploy  
CodePipeline  
Cloud9  
X-Ray

👤 Customer Enablement

AWS IQ   
Support  
Managed Services

🤖 Robotics

AWS RoboMaker


🔗 Blockchain

Amazon Managed Blockchain

📡 Satellite

Ground Station

🏢 Management & Governance

AWS Organizations  
CloudWatch  
AWS Auto Scaling  
CloudFormation  
CloudTrail  
Config  
OpsWorks  
Service Catalog  
Systems Manager  
Trusted Advisor  
Control Tower  
AWS License Manager  
AWS Well-Architected Tool  
Personal Health Dashboard   
AWS Chatbot  
Launch Wizard


🎬 Media Services

Elastic Transcoder  
Kinesis Video Streams  
MediaConnect  
MediaConvert  
MediaLive  
MediaPackage  
MediaStore  
MediaTailor  
Elemental Appliances & Software


🧠 Machine Learning

Amazon SageMaker  
Amazon Comprehend  
Amazon Forecast  
Amazon Lex  
Amazon Machine Learning  
Amazon Personalize  
Amazon Polly  
Amazon Rekognition  
Amazon Textract  
Amazon Transcribe  
Amazon Translate  
AWS DeepLens  
AWS DeepRacer

📊 Analytics

Athena  
EMR  
CloudSearch  
Elasticsearch Service  
Kinesis  
QuickSight   
Data Pipeline  
AWS Data Exchange  
AWS Glue  
AWS Lake Formation  
MSK

🛡️ Security, Identity, & Compliance

IAM  
Resource Access Manager  
Cognito  
Secrets Manager  
GuardDuty  
Inspector  
Amazon Macie   
AWS Single Sign-On  
Certificate Manager  
Key Management Service  
CloudHSM  
Directory Service  
WAF & Shield  
Artifact  
Security Hub

💰 AWS Cost Management

AWS Cost Explorer  
AWS Budgets  
AWS Marketplace Subscriptions

📱 Mobile

AWS Amplify  
Mobile Hub  
AWS AppSync  
Device Farm

🎮 AR & VR

Amazon Sumerian


🔗 Application Integration

Step Functions  
Amazon EventBridge  
Amazon MQ  
Simple Notification Service  
Simple Queue Service  
SWF

👥 Customer Engagement

Amazon Connect  
Pinpoint  
Simple Email Service

🏢 Business Applications

Alexa for Business  
Amazon Chime   
WorkMail

👤 End User Computing

WorkSpaces  
AppStream 2.0  
WorkDocs  
WorkLink

🌐 Internet of Things

IoT Core  
Amazon FreeRTOS  
IoT 1-Click  
IoT Analytics  
IoT Device Defender  
IoT Device Management  
IoT Events  
IoT Greengrass  
IoT SiteWise  
IoT Things Graph

🎮 Game Development

Amazon GameLift

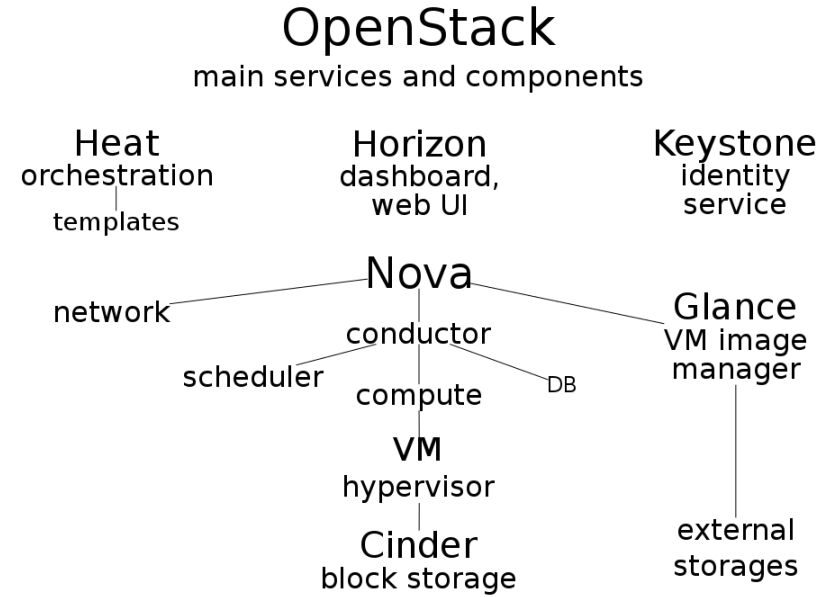
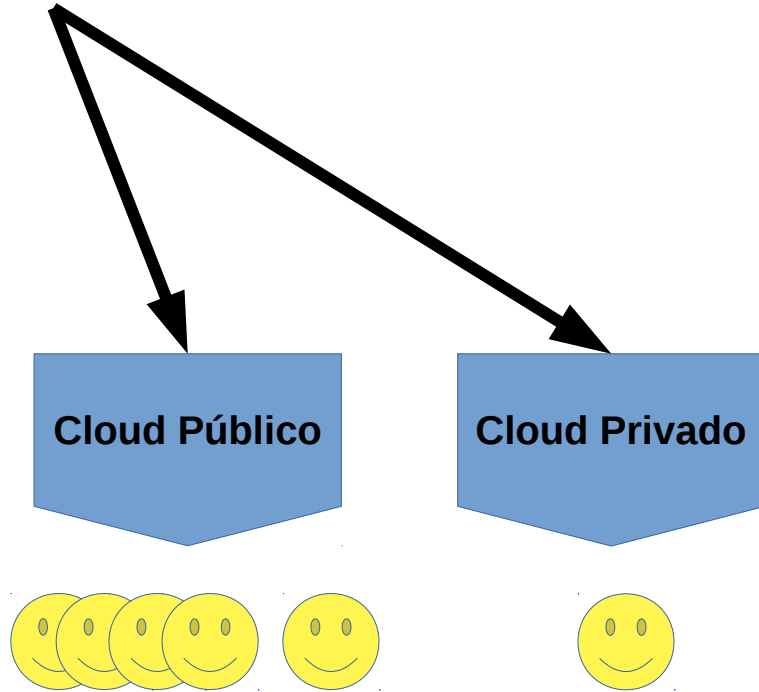


## 7. OPENSTACK



# OPENSTACK

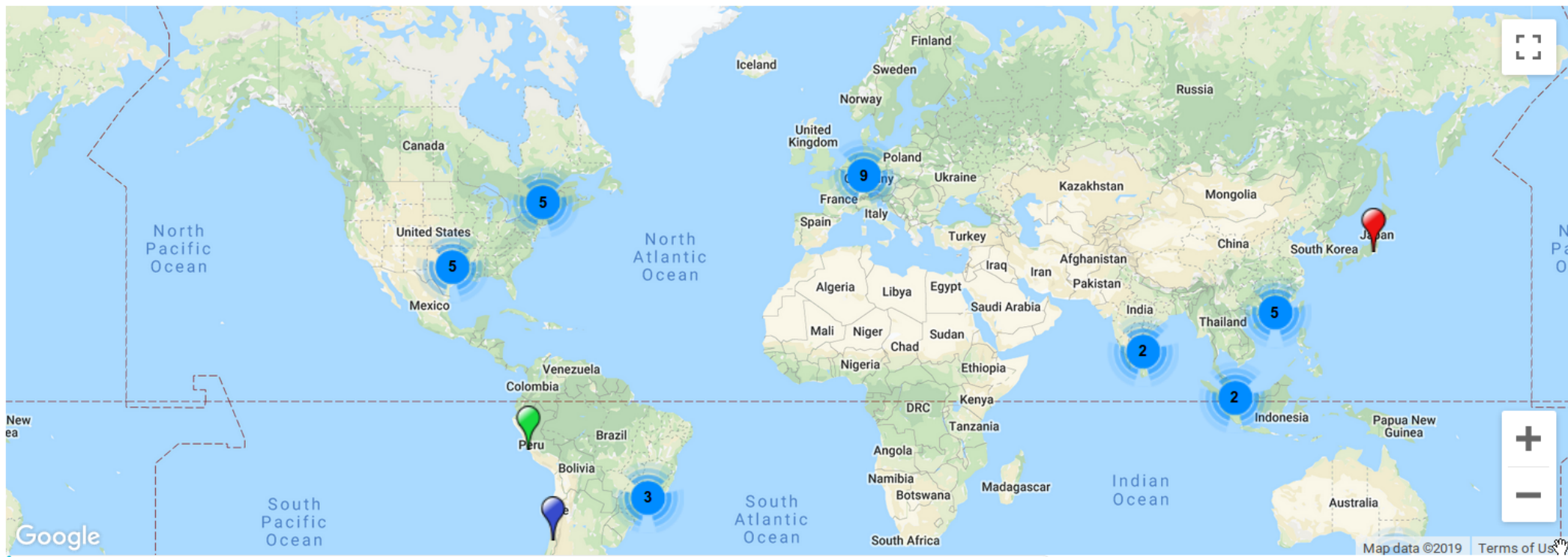
- Plataforma software open-source para crear nubes públicas y privadas.
- Orientada principalmente en IaaS
- Es un conjunto de componentes interrelacionados que controlan los pools de hardware de procesamiento (hosts), de almacenamiento y los recursos de red en un centro de procesamiento de datos.
- La interfaz con el usuario puede ser:
  - Dashboard web.
  - Línea de comandos
  - API RESTful



# NUBES PÚBLICAS



# NUBES PRIVADAS



# Componentes de OpenStack

- Rule-based alarm actions (Aodh)
- Key manager (Barbican)
- Telemetry (Ceilometer)
- Block storage (Cinder)
- DNS (Designate)
- Image (Glance)
- Orchestration (Heat)
- Dashboard (Horizon)
- Bare metal (Ironic)
- Identity (Keystone)
- Container orchestration (Magnum)
- Shared file system (Manila)
- Workflow (Mistral)
- Networking (Neutron)
- Compute (Nova)
- Elastic map reduce (Sahara)
- Object storage (Swift)
- Search (Searchlight)
- Database (Trove)
- Root Cause Analysis (Vitrage)
- Messaging (Zaqar)



# Service Navigator

- <https://www.openstack.org/software/project-navigator/openstack-components#openstack-services>

## Rule-based alarm actions (Aodh)



- Realizar acciones según reglas sobre eventos o datos recopilador por Ceilometer.

# Key manager (Barbican)



- Servicio de gestión de claves.
- Almacenamiento seguro, provisionamiento y gestión de datos “secretos”
  - Passwords
  - Claves de cifrado
  - Certificados X.509
  - Binarios

## Resource Reservation Service (Blazar)



- Permite que los usuarios reserven recursos durante periodos de tiempo
  - Cobra al usuario por los recursos reservados por tiempo.

# Telemetry (Ceilometer)



- Recolectar eficientemente datos producidos por los servicios de OpenStack.

# Billing (Cloudkitty)



- Rating-as-a-Service
- Traduce métricas en precios.
- Múltiples recolectores.
- Múltiples esquemas de tarificación (“rating”).
- Múltiples esquemas de facturación.

# Lifecycle management of accelerators (Cyborg)



- Gestión de aceleradores
  - GPU
  - FGPA
  - ASIC

# Block storage (Cinder)



- Servicio de Almacenamiento en bloques (Block Storage).
- Virtualiza los dispositivos de almacenamiento.
- Proporciona a los usuarios con un API autoservicio para pedir y consumir recursos.



# DNS (Designate)



- Proporciona el servicio DNS en OpenStack

# EC2 API Proxy (EC2API)



- API para compatibilizar Nova con EC2.

## Backup, Restore, Disaster Recovery (Freezer)



- Plataforma para copia de seguridad distribuida y recuperación as-a-service
  - Multi-OS
  - Block-based backups.
  - File based incremental backups.

# Image (Glance)



- Servicios de imagenes de máquinas virtuales
  - Búsqueda
  - Registro
  - Descarga
- API para procesar metadata de las imagenes y la obtención de la imagen.

# Orchestration (Heat)



- “Orquesta” la infraestructura de recursos del cloud.
- API Rest.
- Servicio de autoescalado integrado con el servicio de Telemetry.

# Dashboard (Horizon)



- Implementación canónica del dashboard de OpenStack.
  - Interfaz de usuario web para los servicios de OpenStack.
- Extensible.

# Bare metal (Ironic)



- Provisión de hardware (desnudo)
- Implementa los servicios y librerías asociadas para proporcionar acceso autoservicio masivamente escalable, bajo demanda, a recursos de computación
  - Hardware
  - Maquinas virtuales
  - Contenedores

# Application Data Protection as a Service (Karbor)



- Copia de Seguridad.
- Replicas de datos.
- API y servicios.



# Identity (Keystone)



- Identificación con API de cliente.
- Service discovery.
- Autorización multi-tenant
- Soporta
  - OAuth
  - OpenID Connect
  - SAML
  - SQL

# Networking Integration for container (Kuryr)

- Puente entre “containers framework networking models” con la abstracción de red de OpenStack
  - Paraguas adaptador.

# Container orchestration (Magnum)



- Gestiona motores de orquestación de contenedores
  - Docker Swarm
  - Kubernetes
  - Apache Mesos
- Se apoya en Heat

# Shared file system (Manila)



- Acceso coordinado a sistemas de ficheros
  - Compartidos
  - Distribuidos

## High Availability Instance (Masakari)



- Servicio de alta disponibilidad de instancias.
- Recuperación de instancias fallidas.
- API para gestionar y controlar el mecanismo de rescate automático.

# Workflow (Mistral)



- Servicio de workflow para procesos de negocio.
  - Tareas
  - Interrelación entre tareas.

# Application Catalog (Murano)

- Catalogo navegable para publicar aplicaciones.

# Networking (Neutron)



- Proyecto de red SDN (Software Defined Networking) para proporcionar “networking-as-a-service” NaaS en entornos virtuales.



# Compute (Nova)



- Implementar servicios y librerías asociadas para proporcionar recursos de computación escalables masivamente, bajo petición (on-demand) o en auto-servicio, incluyendo el propio hardware, máquinas virtuales y contenedores

# Load Balancer (Octavia)



- Gestión de reparto de carga.
  - Flota de máquina virtuales o reales (amphorae) que activa bajo demanda horizontalmente.

# Functions service (Qinling)



- Plataforma para soporte de funciones “serverless/lambda”

# Elastic map reduce (Sahara)



- Proporciona entornos de procesamiento de datos en OpenStack
  - Hadoop
  - Spark
  - Storm

# Indexing and Search (Searchlight)



- Capacidades de indexado y de búsqueda en los recursos de OpenStack.
- Altas prestaciones.
- Query flexible.
- Indexado casi-en-tiempo-real.
  - Elasticsearch.
  - Apache Lucene.

# Software Lifecycle (Solum)

- Simplifica la integración del proceso de desarrollo de una aplicación, automatizando el proceso de convertir el fuente en imagen (source to image).

# Compuable Object Storage (Storlets)



- Extensión de Swift para ejecutar computaciones definidas por el usuario (storlets)
- Enjaulamiento con contenedores Docker.

# Object storage (Swift)



- Almacenamiento de objetos/blob.
  - Alta disponibilidad
  - Distribuidos
  - Consistentes
- Alto volumen de datos.
- Escalable.



# Database (Trove)



- Database as a Service.
- SQL y NoSQL.

# Root Cause Analysis (Vitrage)



- Organizar, Analizar y Visualizar alarmas y eventos.
- Deducir la existencia del problema antes que se detecte directamente.

# Messaging (Zaqar)

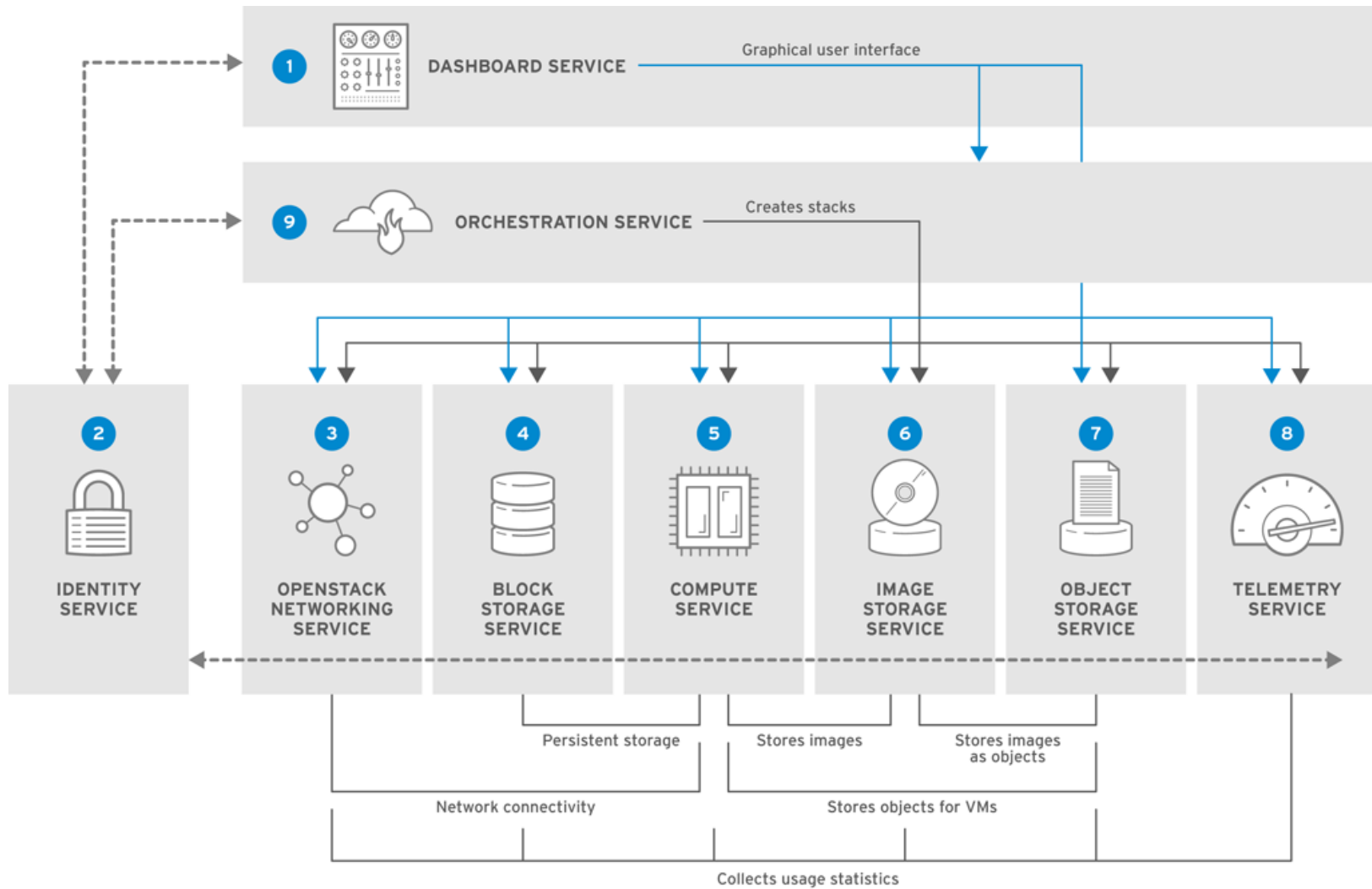


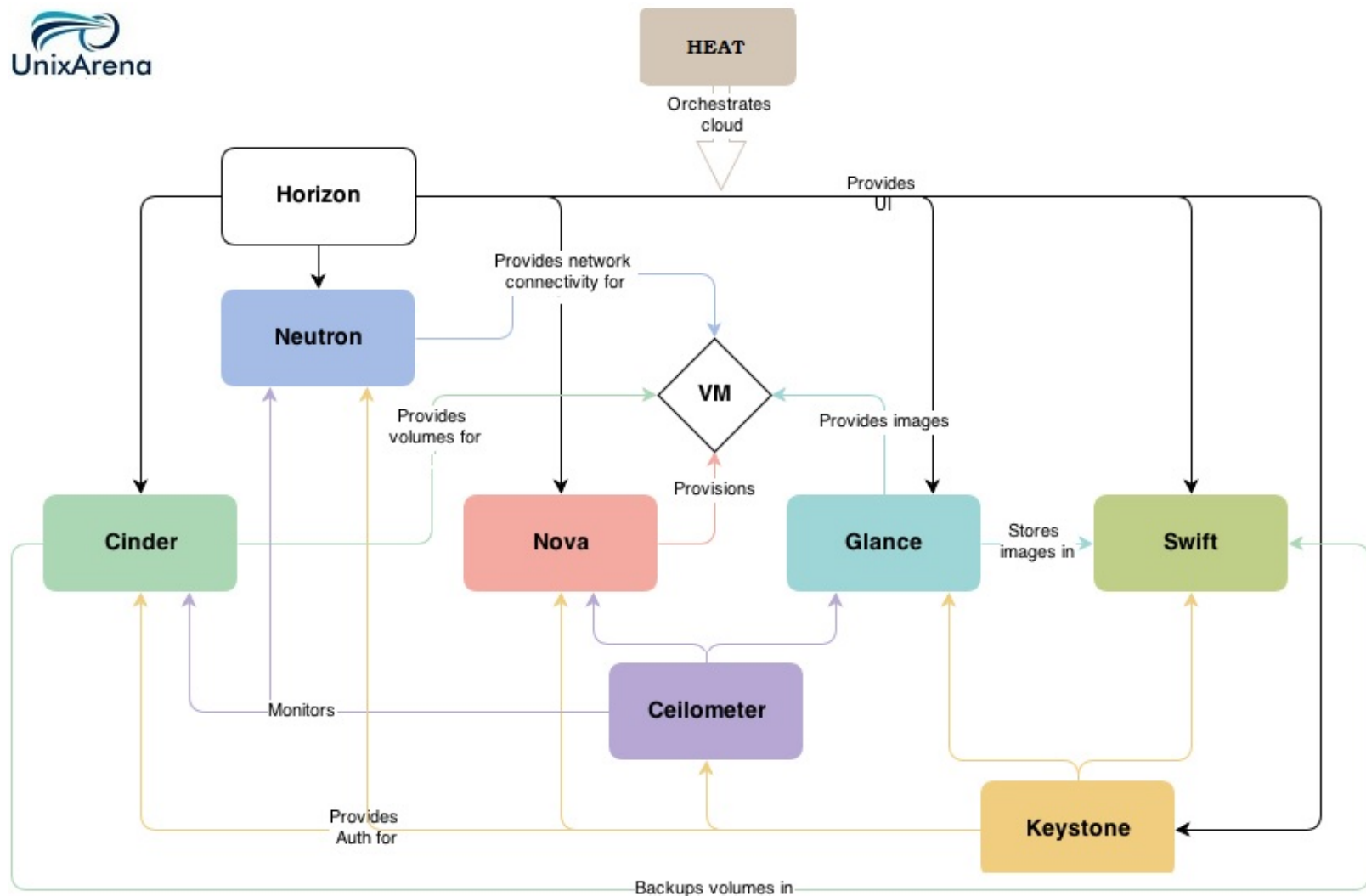
- Servicio multi-inquilino de mensajes en el cloud para desarrolladores web y mobile.
- API

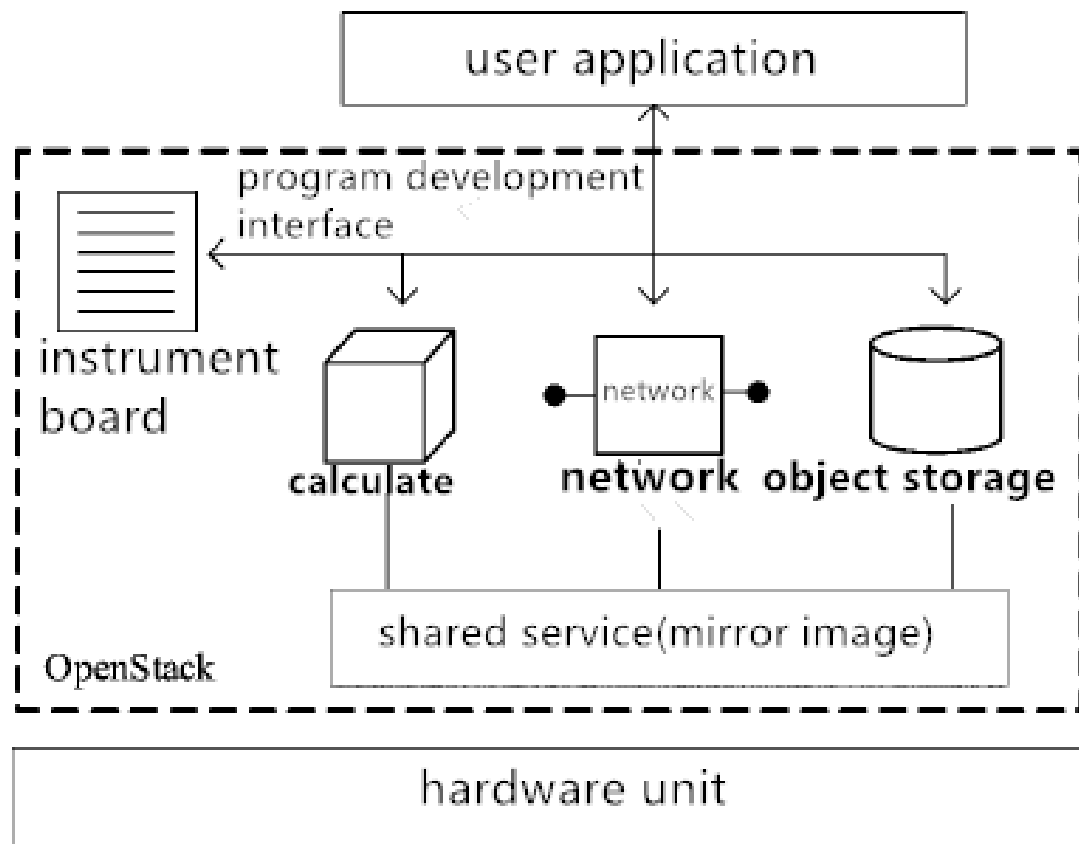
# Container Service (Zun)



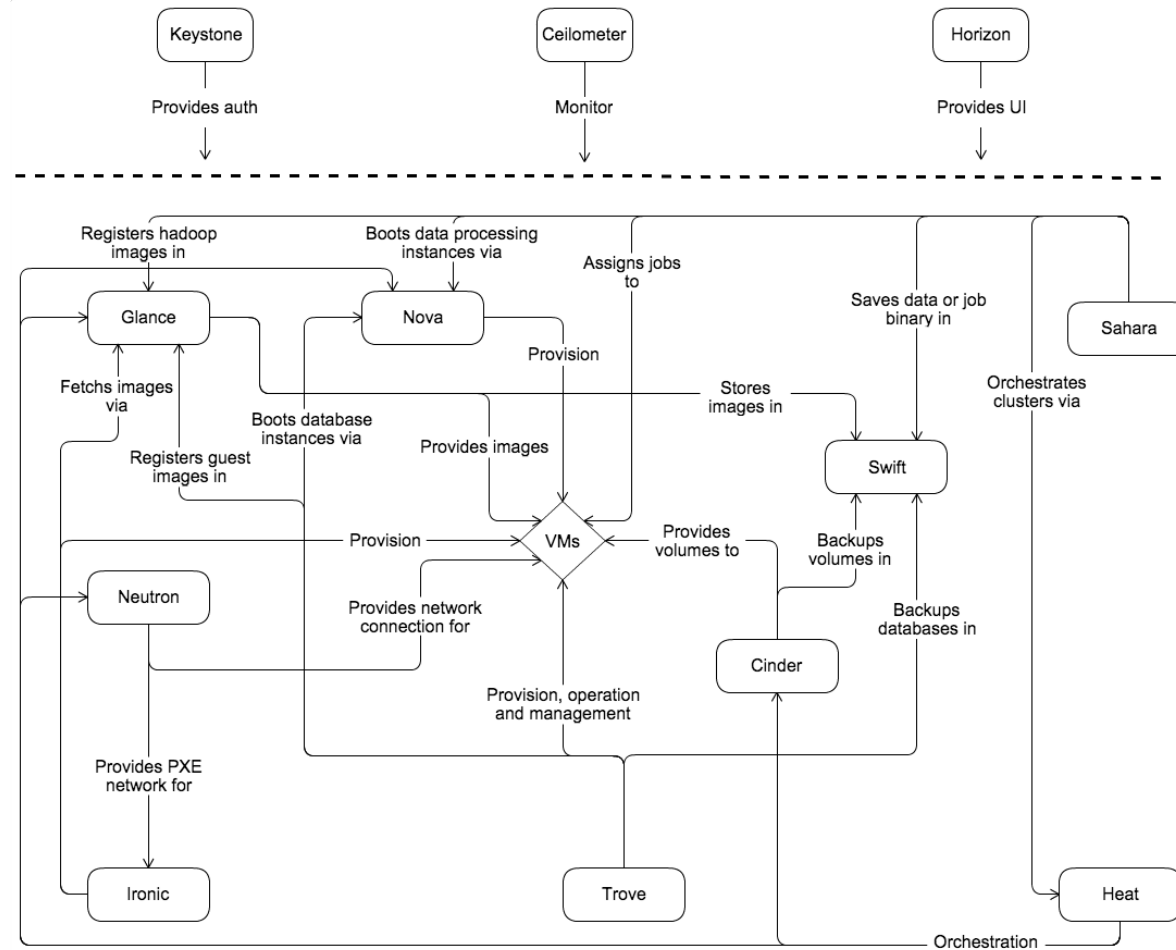
- API para lanzar y gestionar contenedores soportando diferentes tecnologías de contenedor.
  - Simplificada ocultando las complejidades de las tecnologías de contenedores.
- Orientado a usuarios que quieren gestionar contenedores como un recurso gestionado de OpenStack.





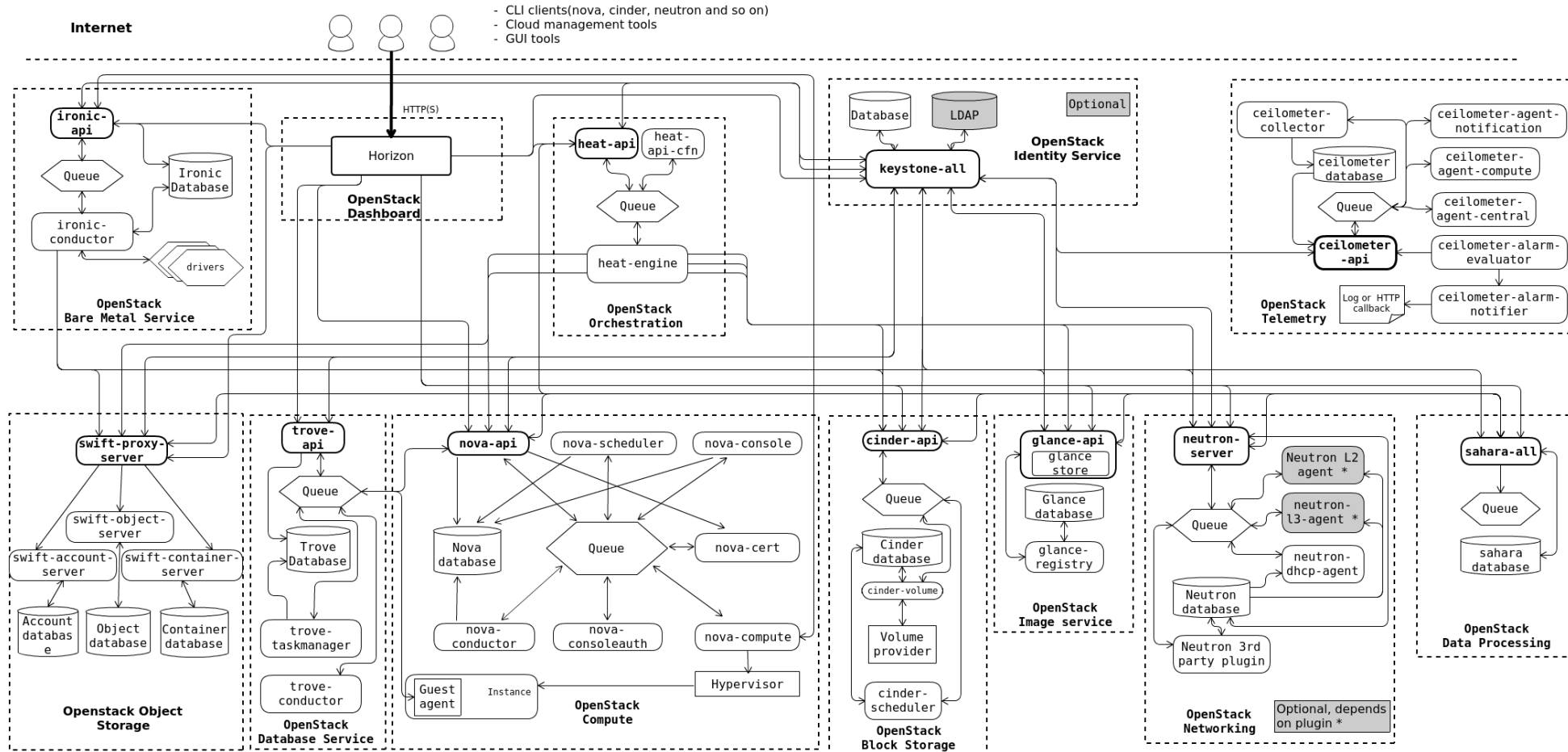


# Arquitectura Conceptual



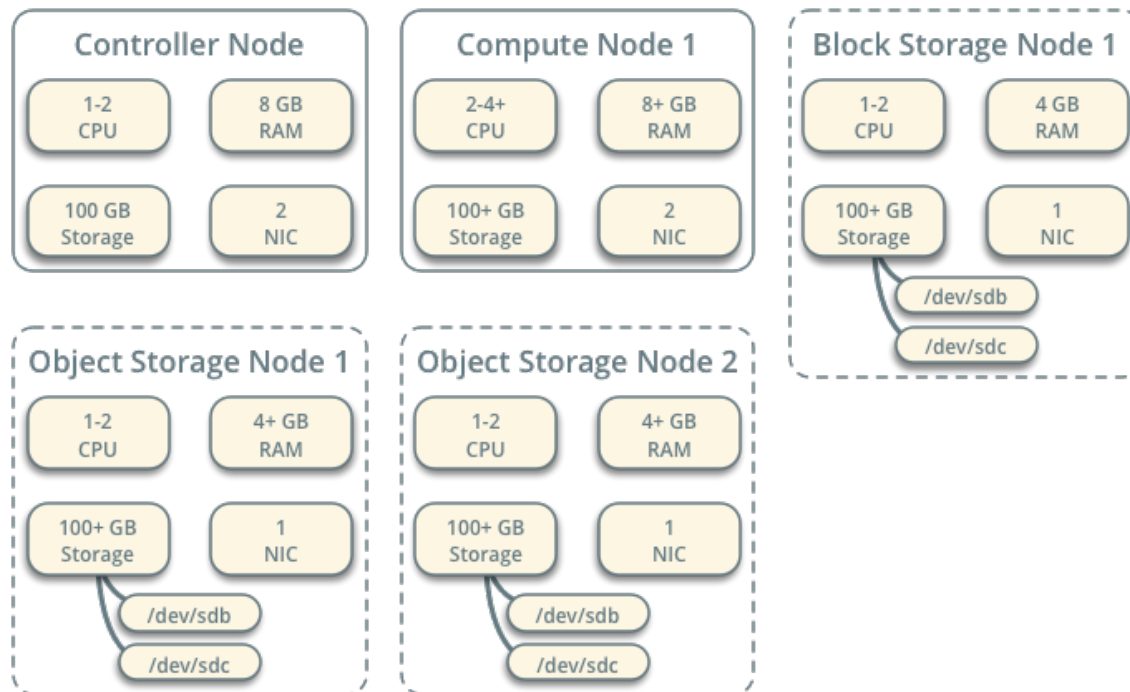


# Arquitectura Lógica



# Hardware

## Hardware Requirements



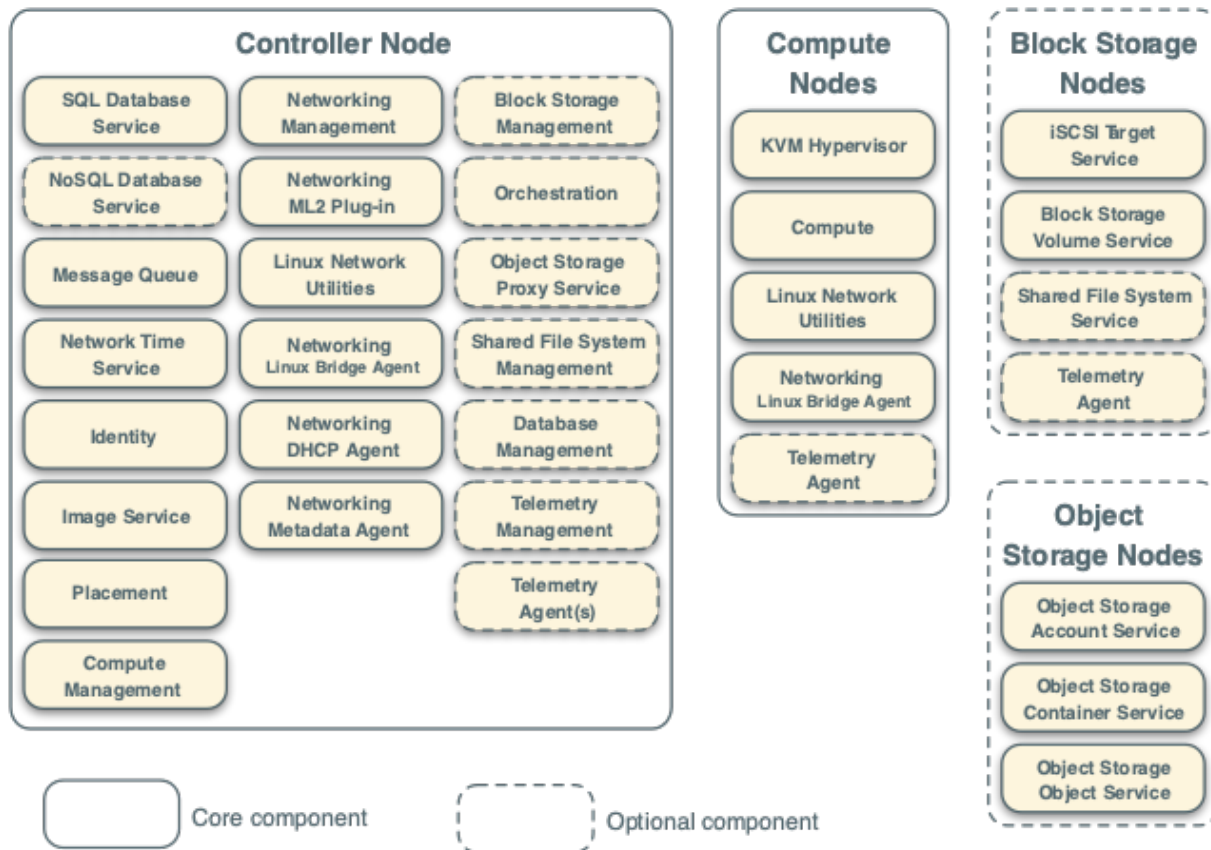
Core component



Optional component

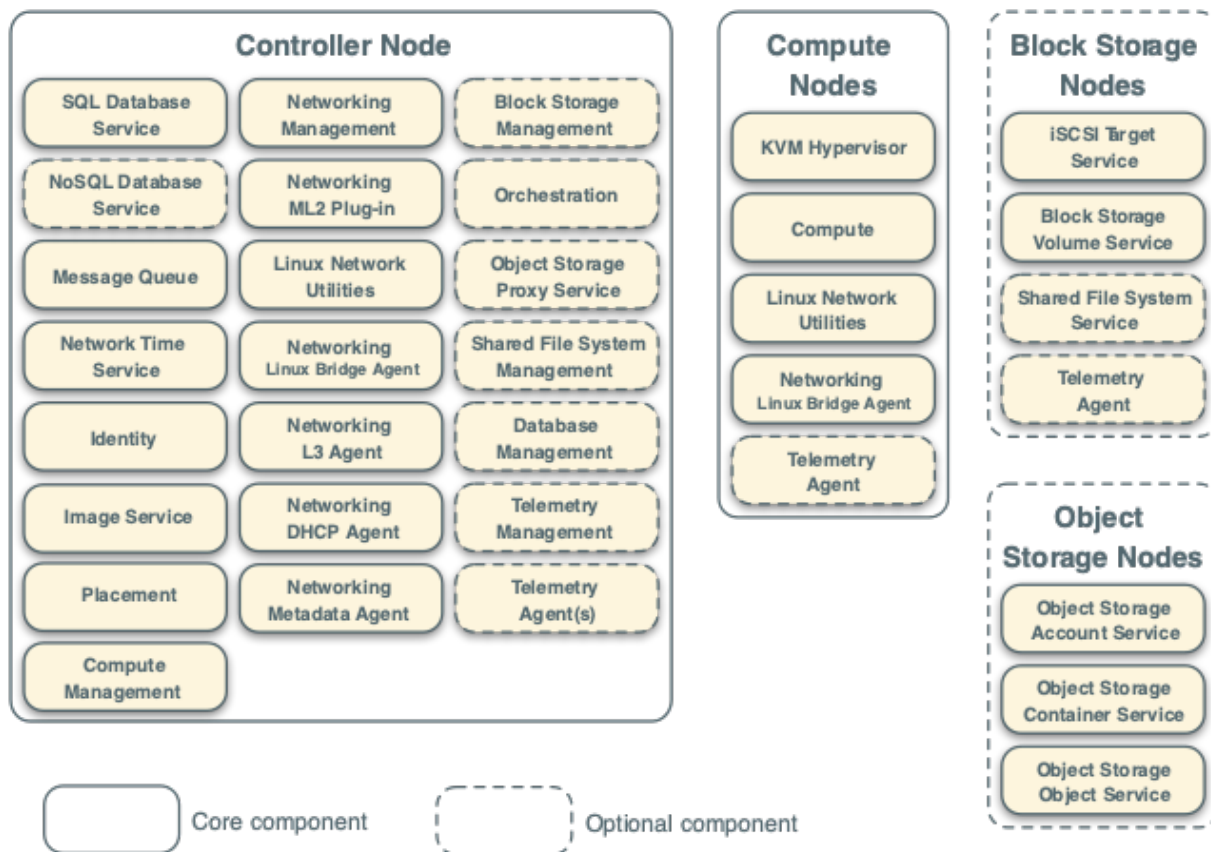
## Networking Option 1: Provider Networks

### Service Layout



## Networking Option 2: Self-Service Networks

### Service Layout



# 8. OPENSIFT

**Introducción a OpenShift**  
**Componentes**  
**Instalación**  
**Uso y configuración**  
**Herramientas asociadas**



**OPENSIFT**

# OpenShift Container Platform OCP

- Plataforma para desarrollo despliegue y ejecución de aplicaciones en contenedores.
  - Contenedores Docker.
  - Orquestados y Gestionados por Kubernetes.
- Orientada a desarrollo.
  - Énfasis en el código, y abstrae de la problemática de los contenedores y de la orquestación.
- Kubernetes.
- Disponible en RHEL, CentOS

- OpenShift Origin
  - Versión open source.
- OpenShift Online como servicio SaaS.
- OpenShift Dedicated disponible en
  - AWS
  - GCP
  - Azure
- OpenShift Enterprise.



# Entornos de programación.

- Node.js
- Ruby
- Python
- PHP
- Perl
- Java
- MySQL
- PostgreSQL
- MongoDB
- CouchBase



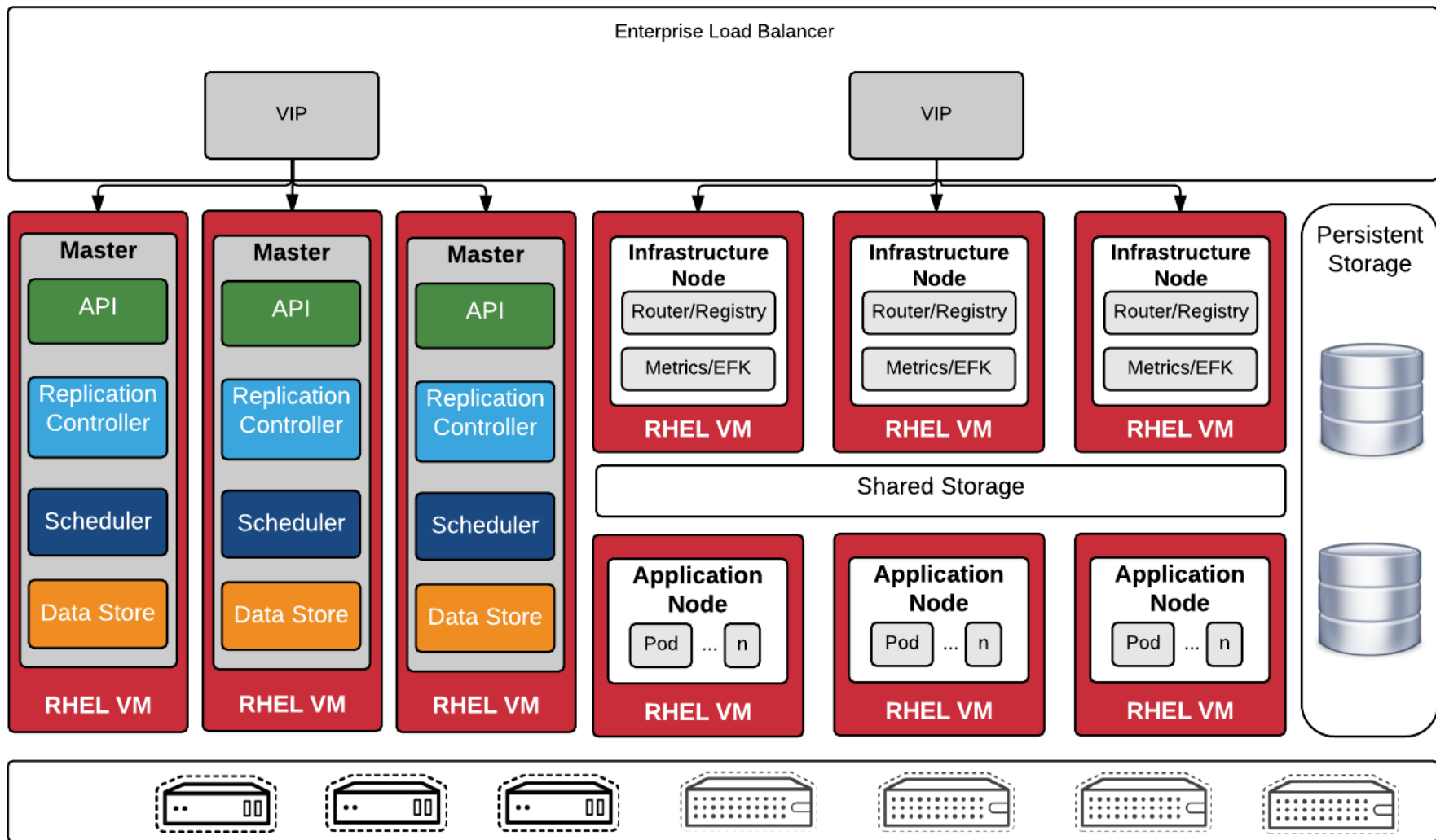
# Entidades de kubernetes

- Pods: conjunto de uno o más contenedores.
- ReplicationControllers: garantizan la ejecución de las réplicas de los pods.
- Services: Objetos internos que asocian y representan puerto/daemon/programa en ejecución.
- Routes: Exposición de servicios al exterior (URL).
- PersistentVolumeClaims: Petición de almacenamiento, tipo y cantidad. Definido en desarrollo.
- PersistentVolume: Almacenamiento real. Definido en administración.

- Soporte a Volúmenes:
  - Gluster
  - Ceph
  - AWS EBS Volumes
  - NFS
  - iSCSI
  - ...

# Interfaz de usuario

- Dashboard.
- Terminal de comandos: oc.
- API.



# Load Balancer Two Planes

