

# 第五章 云操作系统OpenStack

云计算导论和应用实践

OpenStack架构与核心组件详解

# 目录

- 5.1 OpenStack概述与发展历程
- 5.2 OpenStack架构与核心组件
- 5.3 OpenStack与虚拟化技术
- 5.4 Keystone身份认证服务
- 5.5 Glance镜像服务
- 5.6 Placement资源管理服务
- 5.7 Nova计算服务
- 5.8 Neutron网络服务

# OpenStack概述

- **定义**：开源的云基础设施平台，提供IaaS服务
  - **发展历程**：2010年由NASA和Rackspace联合发起
  - **核心特点**：
    - 模块化架构，组件可独立部署
    - 支持多种虚拟化技术(KVM、Xen、VMware)
    - RESTful API接口，易于集成；多租户支持，资源隔离
  - **中国市场**：企业级应用广泛，成为主流云平台选择
- 推荐操作系统**：RHEL、Ubuntu、OpenEuler等主流Linux发行版

# OpenStack核心架构

## 核心组件(16个主要服务)

组件	功能	端口
Keystone	身份认证服务	5000
Nova	计算服务	8774
Neutron	网络服务	9696
Glance	镜像服务	9292
Cinder	块存储服务	8776

**通信机制：**组件间通过RESTful API和RabbitMQ消息队列通信

# OpenStack节点架构

## 控制节点

- Keystone认证服务
- Nova API和调度器
- Neutron网络管理
- Glance镜像服务
- Horizon Web界面
- 数据库(MariaDB)
- 消息队列(RabbitMQ)

## 计算节点

- Nova-compute服务
- Hypervisor(KVM/Xen)
- Neutron网络代理
- 虚拟机实例运行
- 本地存储管理

**部署建议：**生产环境推荐多控制节点高可用部署

# OpenStack与虚拟化技术

## 支持的虚拟化技术

- **KVM**: Linux内核虚拟化, 性能优异, 默认选择
- **Xen**: Type-1 Hypervisor, 企业级应用
- **VMware vSphere**: 商业虚拟化平台集成
- **Hyper-V**: 微软虚拟化技术支持

## 虚拟化层次关系

架构层次: 物理硬件 → Hypervisor → OpenStack → 虚拟机实例

**注意**: OpenStack是云管理平台, 依赖底层虚拟化技术提供资源抽象

# Keystone身份认证服务

## 核心概念

- **Users**: 系统用户, 具有登录凭证
- **Domains**: 用户和项目的命名空间
- **Projects**: 资源容器, 实现租户隔离
- **Roles**: 权限角色, 定义操作权限

## 认证流程

- 用户提供认证凭证(用户名/密码)
- Keystone验证凭证有效性
- 生成临时访问令牌(Token)
- 其他服务验证Token获取用户权限

**服务端点**: 提供public、internal、admin三种API端点

# Keystone部署配置 - 基础配置

## 关键配置步骤

- 创建keystone数据库并授权用户
- 安装keystone软件包
- 配置数据库连接和消息队列
- 初始化Fernet密钥存储库

**部署前提：**确保MariaDB数据库和RabbitMQ消息队列服务正常运行

**默认端口：**5000 (HTTP)，生产环境建议启用SSL



# Keystone部署配置 - 服务引导

## 后续配置步骤

- 设置引导身份服务
- 配置Apache HTTP服务
- 验证服务可用性
- 创建初始域、项目和用户

```
# 引导身份服务示例
keystone-manage bootstrap \
  --bootstrap-password 'Keystone!2023' \
  --bootstrap-admin-url http://$controller:5000/v3/ \
  --bootstrap-region-id RegionOne
```

**注意事项：**请妥善保存bootstrap密码，用于后续管理操作

# Glance镜像服务概述

## 服务功能

- 提供虚拟机镜像的集中存储和管理
- 支持镜像发现、注册和下载
- 镜像元数据管理(数据库存储)
- 支持多种后端存储(本地文件系统、Ceph、Swift)

**服务特点：**统一管理、高可用性、灵活扩展

**默认配置：**监听端口9292，RESTful API接口

# Glance镜像格式支持

## 镜像格式类型

格式	特点	应用场景
qcow2	压缩存储，节省空间	开发测试环境
raw	原始格式，性能最佳	生产环境，Ceph后端
vmdk	VMware格式	VMware环境迁移
vhd	Hyper-V格式	Windows虚拟化环境

**默认存储路径：** /var/lib/glance/images/

**存储建议：** 生产环境推荐使用分布式存储后端

# Glance配置要点

## 核心配置项

- **数据库连接**: 配置MySQL/MariaDB连接参数
- **Keystone认证**: 集成身份认证服务
- **存储后端**: 支持file、ceph、swift等多种存储
- **消息队列**: RabbitMQ配置用于组件通信

## 配置文件位置

主配置文件: /etc/glance/glance-api.conf

## 服务端口

**默认端口**: 9292 (API服务)

# Glance镜像管理

## 镜像上传示例

```
# 上传Cirros测试镜像
openstack image create "cirros-0.6.3" \
  --file /root/cirros-0.6.3-x86_64-disk.raw \
  --disk-format raw --container-format bare --public
```

## 支持的镜像格式

- **raw**: 原始磁盘镜像
- **qcow2**: QEMU写时复制格式
- **vmdk**: VMware磁盘格式
- **vhd**: Hyper-V磁盘格式

# Placement资源管理服务

## 服务职责

- 管理和跟踪资源提供者的资源使用情况
- 帮助调度器寻找满足资源需求的主机
- 支持CPU、内存、磁盘等资源的统一管理
- 为Nova、Neutron、Cyborg等项目提供资源管理

## 发展历程

**版本演进：**Stein版本前集成在Nova中，之后独立为单独项目

**默认端口：**8778，依赖Apache HTTP服务

# Placement典型应用场景

## 资源查询示例

**典型查询：**"寻找一台主机：至少4个空闲CPU + 8G空闲内存 + 100G空闲硬盘"

## 资源类型管理

- **VCPU**：虚拟CPU资源
- **MEMORY\_MB**：内存资源(MB)
- **DISK\_GB**：磁盘资源(GB)
- **CUSTOM\_\***：自定义资源类型

## 与其他服务集成

为Nova计算、Neutron网络、Cyborg加速器等服务提供统一的资源管理接口

# Nova计算服务概述

## 核心地位

Nova是OpenStack最核心的服务模块，负责管理和维护云计算环境的计算资源，管理虚拟机的完整生命周期。

## 主要功能

- 虚拟机生命周期管理（创建、启动、暂停、关闭、删除）
- 计算资源调度和分配
- 虚拟机在不同计算节点间迁移
- 虚拟机安全控制
- 虚拟机磁盘镜像和快照管理

**架构特点：**模块化设计，各组件通过消息队列通信，支持水平扩展



## Nova主要组件

组件	功能
Nova-api	RESTful API服务，外部访问唯一入口
Nova-scheduler	调度服务，决定虚拟机创建位置
Nova-conductor	数据库访问中间件，RPC服务
Nova-compute	计算节点核心服务，管理虚拟机生命周期
Nova-novncproxy	VNC代理服务，提供控制台访问

**通信机制：**组件间通过RabbitMQ消息队列通信

**默认端口：**8774 (API)，6080 (VNC代理)

# Nova数据库结构

## 数据库组成

- **nova**: 主数据库, 存储大部分信息
  - 实例信息、计算节点状态
  - 镜像元数据、网络配置
- **nova\_api**: API相关数据
  - 请求日志、API版本信息
  - 用户会话数据
- **nova\_cell0**: 未分配到cell的实例信息
  - 失败的实例创建记录
  - 调度失败的实例

# Nova部署架构

## 控制节点配置

- Nova-api服务
- Nova-scheduler调度器
- Nova-conductor数据库代理
- Nova-novncproxy VNC代理
- 三个数据库：nova、nova\_api、nova\_cell0

# 发现新计算节点

```
nova-manage cell_v2 discover_hosts --verbose
```

## 计算节点配置

- Nova-compute服务
- Libvirt虚拟化管理
- KVM Hypervisor
- VNC配置
- Placement服务集成

# Neutron网络服务概述

## 服务功能

Neutron是OpenStack网络模块，负责创建和管理L2、L3网络，为虚拟机提供虚拟网络和物理网络连接。

## 基本概念

概念	说明
Network	隔离的二层广播域
Subnet	IPv4/IPv6地址段，IP分配来源
Port	虚拟交换机端口，绑定MAC和IP

**默认端口：**9696，支持多种网络后端

# Neutron架构特点

## 设计特点

- **插件化架构**：支持多种网络实现
  - ML2插件：模块化二层网络
  - L3插件：三层路由服务
- **网络隔离**：支持二层隔离和三层路由
  - 租户网络隔离
  - 安全组规则管理
- **高级服务**：提供企业级网络功能
  - 负载均衡(LBaaS)
  - 防火墙(FWaaS)
  - VPN服务(VPNaaS)

# Neutron网络类型

## 基础网络类型

- **Local**: 单机隔离网络，测试用
  - 与其他网络和节点完全隔离
  - 仅支持同一节点上实例通信
- **Flat**: 无VLAN标记的平面网络
  - 支持二层直接通信
  - 可跨多个节点

## 企业级网络类型

- **VLAN**: 802.1q标记网络
  - 二层广播域隔离
  - 应用最广泛的网络类型

# Neutron隧道网络

## Overlay网络技术

- **VXLAN**: 虚拟可扩展局域网
  - 24位网络标识符, 支持1600万个网络
  - UDP封装, 穿越三层网络
  - 适用于大规模云环境
- **GRE**: 通用路由封装
  - IP封装技术
  - 简单配置, 性能较好
  - 适用于中小规模部署

## 应用场景

**适用环境:** 大型数据中心、跨三层网络部署、需要大量租户隔离的场景

# OpenStack环境准备

## 操作系统选择

- **RHEL/CentOS**: 企业级稳定性
- **Ubuntu**: 社区支持丰富
- **OpenEuler**: 国产化选择

## 基础服务配置

- **数据库**: MariaDB/MySQL集群
  - 主从复制配置
  - 高可用集群部署
- **消息队列**: RabbitMQ高可用配置
  - 集群模式部署
  - 镜像队列配置
- **缓存服务**: Memcached分布式部署



# OpenStack网络规划

## 管理网络

- API服务访问
- 组件间通信
- 数据库连接
- 消息队列通信

## 数据网络

- 虚拟机流量
- 存储网络流量
- 外部网络接入
- 隧道网络封装

## 网络分离建议

**最佳实践：**管理网络与数据网络物理分离，提高安全性和性能

## 安全配置

启用SSL/TLS加密，配置防火墙规则，定期更新密钥

# 本章总结

## 学习要点

- **OpenStack架构**：理解模块化设计和组件协作关系
- **核心服务**：掌握Keystone、Nova、Neutron、Glance等关键组件
- **部署实践**：了解控制节点和计算节点的配置差异
- **网络概念**：理解虚拟网络的基本概念和类型

## OpenStack价值

**企业级云平台**：提供完整的IaaS解决方案，支持大规模部署，具备良好的扩展性和可靠性

# OpenStack发展趋势

## 技术发展方向

- **容器化部署**: Kolla项目支持容器化安装
  - 简化部署和运维
  - 提高服务可移植性
- **边缘计算集成**: StarlingX项目
  - 支持边缘场景部署
  - 低延迟计算需求
- **AI/ML工作负载**: GPU资源管理
  - 支持GPU直通和虚拟化
  - 机器学习平台集成

**未来展望**: OpenStack将继续演进, 适应云原生和边缘计算需求