



华为云服务能力介绍

时空云中心
2020年1月

文档版本记录

序号	作者	日期	版本	纪要
1	周恣	2019.12.10	0.1	整理华为 IaaS、PaaS 层服务能力与天启各系统业务需求
2	周恣	2020.01.04	0.2	整理华为大数据、AI 服务能力，结合天启业务系统需求，编写平台建设建议
3	赵贤威、赵伟、蒋兴秋、周恣	2019.01.15	0.3	结合天启技术架构体系图，编制演进方案 A、演进方案 B
4				
5				

目 录

1. IaaS 层服务能力	1
1.1 ECS 服务	1
1.2 BMS 服务	3
1.3 IMS 服务	5
1.4 EVS 云硬盘服务	8
1.5 OBS 存储服务	10
1.6 SFS (NAS) 存储服务	13
1.7 VPC 网络服务	18
1.8 网络安全组	22
1.9 VFW 服务	24
1.10 ELB 负载均衡服务	26
1.11 AS 弹性伸缩服务	29
1.12 vAPP 服务	31
2. PaaS 层服务能力	39
2.1 RDS 数据库服务	39
2.2 DRS 数据迁移服务	45
2.3 API 网关服务	47
2.4 分布式消息中间件	49
2.5 分布式缓存中间件	50
2.6 分布式事务中间件	51
2.7 CPE 服务	51
2.8 容器管理	52
2.9 微服务云管理	56
2.10 云服务市场	61
2.11 SaaS 服务能力	61
3. FusionInsight HD 大数据服务能力	62
3.1 交互式查询	64
3.2 离线处理	65
3.3 实时流处理	66
3.4 融合数仓	67
3.5 实时检索	68
4. FusionInsight ModelArts AI 服务能力	69
4.1 Miner 工作流可视化建模	69
4.2 Miner 交互式笔记本建模	72
4.3 DLS 大规模训练平台	74

4.4 DLS 预置算法训练平台	76
4.5 在线推理平台.....	77
4.6 批量推理平台.....	79

云计算，是一种按使用量付费的模式，这种模式提供可用的、便捷的、按需的网络访问，进入可配置的计算资源共享池（资源包括网络、服务器、存储、应用软件、服务），这些资源能够被快速提供，只需投入很少的管理工作，或与服务提供商进行很少的交互。



图 云计算基础架构图

华为云遵循业界标准，所提供的服务分为 IaaS 服务、PaaS 服务、SaaS 服务。

1. IaaS 层服务能力

IaaS 层服务能力包括 ECS 计算服务、存储服务、网络服务、备份服务、容灾服务、安全服务等基础服务与功能。

1.1 ECS 服务

ECS 弹性云服务器可以使用户可以在几分钟之内迅速地获得虚拟机设施，并且这些基础设施是弹性的，可以根据需求进行扩展和收缩。

ECS 服务适用如下几类场景：

通用型场景：通用型弹性云服务器主要提供基本水平的 vCPU 性能、平衡的计算、内存和网络资源，同时可根据工作负载的需要实现性能的突增，具有短期发挥更高性能的能力。适用于那些不会经常（或始终不会）用尽 vCPU 性能，但会偶尔突然使用的场景，特别适合通用工作负载，如 Web 服务器、开发人员环境和小型数据库等，是很多应用程序的上好选择。

GPU 加速型场景：应用：深度学习、科学计算、CAE、3D 动画渲染、CAD 等。场景特点：适合高实时、高并发的海量计算场景。

适用场景：深度学习特殊优化，可在短时间内完成海量计算

超高 I/O 型：超高 I/O 型弹性云服务器使用高性能 NVMe SSD 本地磁盘，提供高存储 IOPS 以及低读写时延，CPU 和内存配比为 1:8（60vCPU 规格除外），您可以通过管理控制台创建挂载有高性能 NVMe SSD 盘的弹性云服务器。

超高 I/O 型弹性云服务器适用于高性能关系型数据库，NoSQL 数据库 (Cassandra、MongoDB 等)以及 ElasticSearch 搜索等场景。

通用计算增强型：相比通用计算型，通用计算增强型弹性云服务器提供了更大规格的 CPU 和内存组合，可选范围更广。搭载 Xeon SkyLake 全新一代 CPU，全新网络加速引擎以及 DPDK(Data Plane Development Kit)快速报文处理机制，综合性能及稳定性全面提升，满足对业务稳定性及计算性能要求较高的企业级应用诉求。

USB 直通型：选择 USB 直通型弹性云服务器，可支持创建附带物理服务器上 USB 的虚拟机实例，也支持管理员在 Service OM 上动态挂载或者卸载 USB。某些应用软件需要 USB 加密狗等 license 设备配合才能正常使用，要部署此类应用，可以使用 USB 直通型弹性云服务器。

通用独享型：提供性能稳定且资源独享的 CPU、内存运行环境，适用于对 CPU、内存性能有较高诉求 Web 服务、小型数据库运行环境。

内存优化型：内存优化型弹性云服务器基于 KVM 虚拟化平台，特别适合处理内存中的大型数据集。提供最大 512GB 基于 DDR4 的内存实例，是高内存计算应用的最佳选择。适用于对内存要求高，数据量大并且数据访问量大，同时要求快速的数据交换和处理的应用，适用于广告精准营销、电商、车联网等大数据分析场景。

密集存储型：密集存储型弹性云服务器采用本地存储设计，提供更高的顺序读写能力及更低的时延，提升文件读写性能；提供 1:8 的 CPU、内存配比，具有强大而稳定的计算能力，保障计算作业的高效处理；提供更高的内网性能，包括高内网带宽和 pps(packet per second)，满足业务高峰期弹性云服务器间数据交互需求。

密集存储型弹性云服务器适用于处理海量数据、需要高 I/O 能力，要求快速数据交换和处理的场景，如 MapReduce 计算、Hadoop 分布式计算、大型数据仓库、分布式文件系统、日志或数据处理应用。

超大内存型：超大内存型弹性云服务器内存要求高，数据量大并且数据访问量大，同时要求快速的数据交换和处理以及低延迟的存储资源。主要支持 OLAP 场景，如内存数据库（如 SAP HANA BWoH）、大数据处理引擎以及数据挖掘等应用。

目前仅 RH2288H V5 服务器及 RH2488H V5 服务器支持创建超大内存型弹性云服务器。

1.2 BMS 服务

1、应用场景

BMS 服务提供了一种裸金属服务器的使用形态，裸金属服务器上不运行虚拟化层，直接安装用户 OS。对于不适合 VM 部署的应用可以使用 BMS 服务，例如：数据库集群、OLAP 型应用（大数据、重载应用）。BMS 服务与 ECS 服务使用场景区别如下：

虚拟机部署选择建议

- 根据业务请求的会话量和处理复杂度，会话量小，复杂度低的业务适合采用虚拟机部署；
- 根据业务系统运行时的资源占用情况，资源占用低的业务适合采用虚拟机部署；

裸金属服务器部署选择建议

- 对服务器运算性能要求特别高，在单个服务器上配置最大计算能力的虚拟机依然不能满足业务应用的计算能力要求；
- 现有软件许可加密方式不支持虚拟化的场景；
- 业务应用对服务器的板卡有特殊要求，且板卡不支持在虚拟化环境中运行；
- 软件厂家不支持虚拟化部署的应用。

2、服务能力介绍

裸金属服务器服务通过 Web 管理控制台，让用户自主的完成服务的开通与关闭，让用户灵活使用裸金属服务器，达到即开即用，用完归还的目标。

裸金属服务器服务（BMS）具有以下功能：

BMS 服务极致性能，支持多种实例规格 BMS 服务

BMS 资源池可根据需要规划多种物理服务器规格（CPU、内存、硬盘）。用户可以根据不同场景的业务需求进行选择不同类型的物理服务器。

BMS 服务实例相对于裸金属服务器没有性能损失，专属于单个用户。可以提供显着的计算性能和 I/O 吞吐量。

快速部署，BMS 实例开通只需 30 分钟左右，满足用户的紧急需求。

支持华为 SDI 技术的服务器快速发放时间只需要 5 分钟左右，并支持在硬件故障时进行重建。

支持 KunLun9008/9016 满足高性能、高可靠的超大型关键业务、核心数据库的裸金属服务器需求。

支持自助申请和挂载云硬盘

支持云硬盘，除本地硬盘之外，最大还可以支持挂载 60 块云硬盘，满足用户不同的 IO 以及容量需求。

网络自定义，自由规划 BMS IP 地址

BMS 实例可以与 ECS 实例规划到同一个 VPC(虚拟私有云网络)，用户可以方便的管理、配置内部网络；

为每个 BMS 实例提供公网 IP 和私网 IP，用于不同的连接场景。公网 IP 可以对外连接互联网；私网 IP 可以内部连接使用，私网 IP 地址个数取决于物理服务器的网卡个数。

丰富的镜像，免安装快速部署操作系统与软件。

公共镜像：公共镜像由管理员制作和注册，所有用户可见。包含操作系统以及预装的公共应用。用户可见根据实际情况自助配置应用环境或相关软件。

管理

管理方便，用户可以通过 Web 页面或者开放 API，同时管理一个、数百个、甚至数千个 BMS 实例。

支持裸金属服务器实例关键性能监控，以便快速发现定位主机故障。

安全

完全控制，用户可以完全控制自己创建的 BMS 实例，拥有每个实例的管理员或者 root 用户访问权。

BMS 实例支持多种登陆方式（密码、证书），密码防暴力破解，满足用户的登陆安全需求。对于 Windows 的 BMS 实例，用户只能使用密钥登陆。

3、服务约束条件

部署场景	约束条件	备注
软件 SDN	BMS 需配置 BMGW 做 VTEP 功能，BMGW 与裸金属服务器配比建议为 2:30，可以支持平均每台裸金属服务器 2Gbps 业务带	-

部署场景	约束条件	备注
	宽,可以结合具体的业务要求评估 BMGW 的数量。	
软件 SDN 硬件 SDN 无 SDN	BMS 对应的存储可以采用 FC SAN 或 FusionStorage Block。BMS 对应的存储采用 FusionStorage Block 时,裸金属服务器需配置 SDI 卡,可配置 SDI 卡的服务器为 RH 2288H V3, RH 5885H V3, 2288H V5, 5885H V5。	-
软件 SDN	BMS 对服务器的 TOR 设备有型号要求,支持 CE6850-48S6Q-HI、CE6851-48S6Q-HI、CE6855-48S6Q-HI 和 CE6856-48S6Q-HI,且交换机系统的版本不低于 V100R005C10、不高于 V200R003C00,对于 V200R002 的版本,需要打补丁 http://support.huawei.com/enterprise/zh/software/23048487-SW2000020176 。如果使用其他的 CE 系列交换机,需要项目提前验证。	-

1.3 IMS 服务

1、应用场景

镜像是弹性云主机实例可选择的运行环境模板,一般包括操作系统和预装的软件(可包括公共应用软件以及用户私有应用软件)。镜像分为公共镜像和私有镜像,镜像应用场景如下图所示。

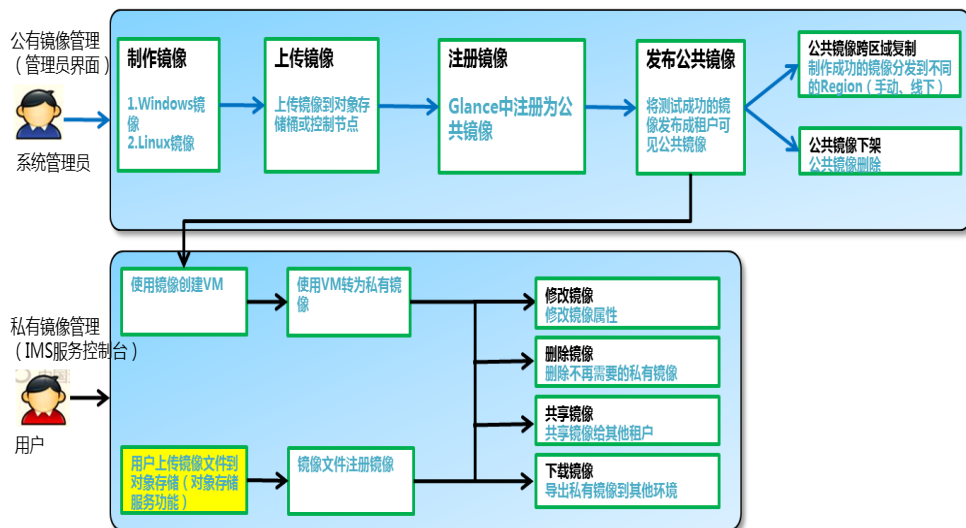


图 IMS 服务场景

镜像分类：

公共镜像：公共镜像由系统管理员制作并注册到系统中，一般提供常见的标准操作系统镜像，所有用户可见。包含操作系统以及预装的公共应用。

私有镜像：私有镜像用于满足用户个性化需求。选择私有镜像创建云主机，可以节省您重复配置云主机的时间。私有镜像仅用户自己可见。包含操作系统、预装的公共应用以及用户的私有应用。用户可基于 ECS 实例或者已有的镜像文件创建的私有镜像。

镜像服务（Image Management Service）提供对私有镜像的自助管理能力，用户可以从丰富的公共镜像库中选择或创建私有镜像，快速创建或批量复制弹性云服务器。

2、IMS 服务架构

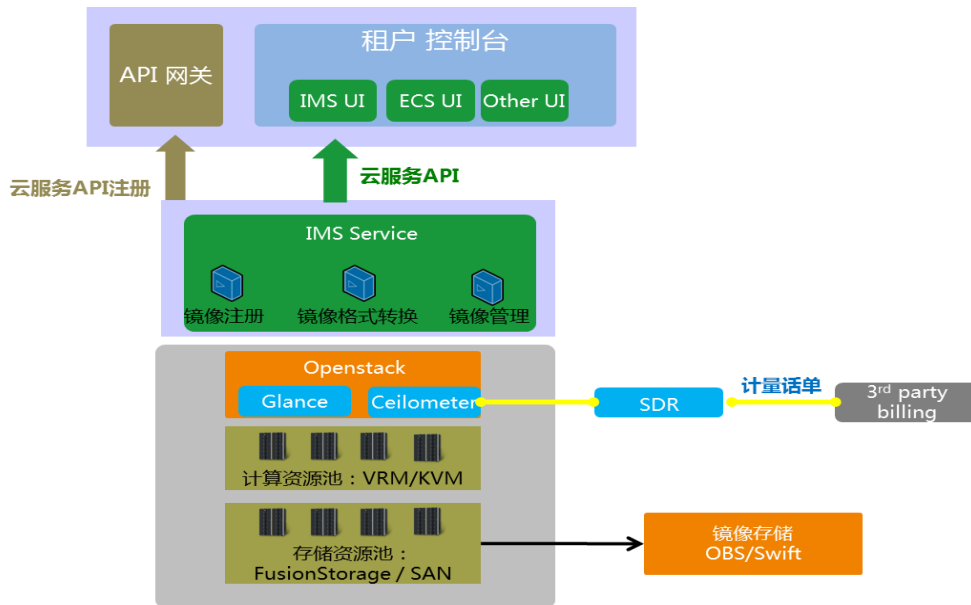


图 IMS 服务架构

3、IMS 服务能力

(1) 创建私有镜像

用户可通过云服务器创建新的私有镜像：私有镜像把 ECS 实例中的磁盘全部完整的复制到私有镜像中。

上传私有镜像：用户可以将本地的物理镜像文件上传到 OBS 服务中，然后在 IMS 控制台把 OBS 桶中的文件注册为私有镜像。用户可以在某 region 导出的私有镜像，上传到另一个 region。实现不同 Region 间使用相同的私有镜像。

(2) 管理镜像

自定义私有镜像信息：用户可以自定义镜像的名称和描述信息。

共享镜像：当用户将自己的私有镜像共享给其他用户使用，可以使用镜像服务的共享镜像功能，被共享用户可以使用共享镜像创建 ECS 实例。

导出镜像到本地：用户可以将私有镜像导出到指定 OBS 租户桶中或本地 CIFS 共享目录，并指定导出镜像的格式，OBS 场景导出格式支持 VMDK、VHD、QCOW2 和 ZVHD，CIFS 共享支持 QCOW2 和 ZVHD2 格式。在镜像在导出过程中，不同的导出格式会导致镜像的大小不同。

(3) 通过私有镜像创建云服务器

用户可以通过已有的私有镜像创建云服务器。使用私有镜像与公共镜像创建云服务器的区别是：私有镜像创建的云服务器除了包含操作系统，还包括租户预装的公共应用以及用户的私有应用。

1.4 EVS 云硬盘服务

1、服务应用场景

EVS 云硬盘是一种基于分布式架构的，可弹性扩展的虚拟块存储设备。您可以在线进行操作，使用方式与传统服务器硬盘完全一致，您可以对挂载到云服务器上的云硬盘做格式化、创建文件系统等操作，并对数据持久化存储。同时，云硬盘具有更高的数据可靠性，更高的 I/O 吞吐能力和更加简单易用等特点，适用于文件系统、数据库或者其他需要块存储设备的系统软件或应用。

EVS 云硬盘支持分布式存储和企业存储，并通过选择不同 SLA 的 EVS 服务实例满足不同业务应用的需求：

NoSQL/关系型数据库（超高 IO 存储类型）：适用于高性能，高读写速率要求，数据密集型应用场景。

数据仓库（超高 IO 存储类型）：满足高带宽吞吐能力的应用场景。

企业办公应用（通用 IO 存储类型）：适用于大容量、读写速率要求不高、事务性处理较少的应用场景。

2、服务架构

EVS 服务包括 EVS 控制台界面，EVS 服务 API，OpenStack cinder，FusionStorage，企业存储等组件。

EVS console 对租户提供云硬盘服务入口，租户可以通过 console 执行云硬盘创建、挂载、卸载、扩容、删除等操作。

EVS 服务 API 在原生 cinder 接口基础上封装或组合逻辑完成云硬盘部分功能，其接口可被 EVS Console 或租户调用。

部分 OpenStack cinder 原生接口也可直接给 EVS console 或租户调用。

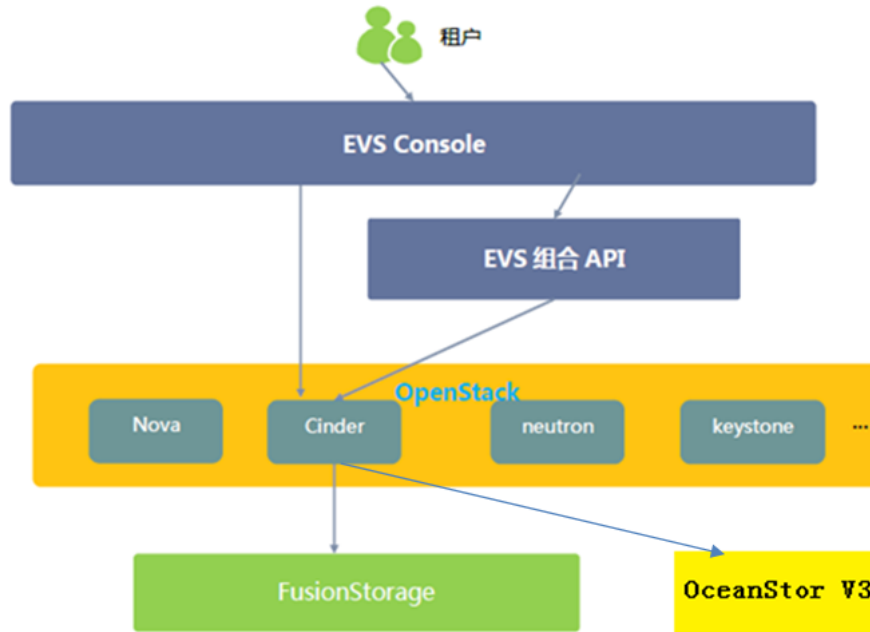


图 EVS 服务架构图

3、服务能力介绍

云硬盘服务具有以下能力：

支持用户自助管理，包括创建、挂载、卸载、删除。

- 创建单个空白云硬盘：用户可以创建一块云硬盘。
- 基于已有快照创建云硬盘：申请云硬盘时，用户可以选择快照作为云硬盘的来源。
- 基于已有云硬盘创建云硬盘：申请云硬盘时，用户可以选择已有云硬盘作为云硬盘的来源。
- 基于镜像创建系统盘：申请云硬盘时，用户可以选择镜像作为系统盘的来源。
- 基于镜像创建数据盘：申请云硬盘时，用户可以选择镜像作为数据盘的来源。
- 挂载云硬盘到云主机：用户可以将一块云硬盘挂载到某个弹性云服务器上。
- 从云主机卸载云硬盘：用户可以把一块已经挂载的云硬盘进行卸载。
- 删除单个云硬盘：用户可以删除一块云硬盘。

支持不同类型（例如：普通 IO、高 IO、超高 IO）的 EVS 磁盘，用户可以根据应用场景对 IO 的需求进行选择。

支持云硬盘快照管理：用户可以为云硬盘创建快照，提供云硬盘快照管理界面，展示快照列表，快照详细信息，支持删除快照、快照回滚到原云硬盘、从快照创建新云硬盘。

弹性扩容可以随时根据用户的需求扩展 EVS 磁盘的容量，满足不断增长的業務对更多存储容量的需求。

动态变更云硬盘的磁盘类型，在单套存储设备内的不同性能的 Pool 之间热迁移。

支持创建磁盘类型时，配置企业存储的 SmartTier 和重删压缩特性，提供丰富的企业级增值特性。

单块 EVS 磁盘支持 64TB，最大限度满足用户对不同存储容量云硬盘的需求。

支持云硬盘 QoS 功能，支持对硬盘的带宽和 IOPS 限速。

云硬盘迁移，可以保证在不中断业务的前提下，在同一 AZ 内对云硬盘在存储阵列内或阵列间迁移，以精确匹配业务需求。

1.5 OBS 存储服务

1、服务应用场景

对象存储服务（OBS，Object Storage Service）是一个基于对象的海量存储服务，为客户提供海量、安全、高可靠、低成本的数据存储能力，包括：创建、修改、删除桶，上传、下载、复制、修改、删除、加密对象等。对象存储服务的应用场景如下。

对接大数据服务

为华为云 Stack 大数据服务提供高可靠、安全、高性能、高扩展性的存储服务。

备份/活跃归档

对象存储服务提供了高持久性、高扩展性以及安全的解决方案来备份和归档用户的关键数据。用户可以使用对象存储服务的版本控制功能，为存储的数据提供进一步的保护。高持久性、安全的基础设施旨在提供高级数据保护的稳固灾难恢复解决方案，支持第三方备份和归档软件。

分布式数据中心内部云服务

如镜像服务 IMS、云硬盘备份 VBS、RDS 数据库等服务，使用对象存储作为各自服务的存储资源池或备份存储等。

对象存储服务的访问方式主要有：

通过对象存储服务租户 Console 直接上传和下载对象。

对象存储服务支持 S3 客户端/SDK，第三程序等通过内外网访问。

同时提供给内部服务，如镜像（公有镜像和私有镜像保存在对象存储），大数据，备份（EVS 硬盘备份数据保存在对象存储）等服务作为存储空间。

2、服务架构

OBS 是一个基于对象的海量存储服务，为客户提供海量、安全、高可靠、低成本的数据存储能力。OBS 用户可以通过 ManageOne（运营中心）登录 OBS Console 进行基本的数据存储操作。用户在使用 OBS Console 服务的过程中，会通过 IAM 进行鉴权保证数据安全，下图运营中心服务的 IAM 负责帐户/用户/角色/AK/SK 信息分配，用户通过 AK/SK 访问 S3 服务时通过 IAM 做认证。OBS 对象存储服务还可以通过 S3 客户端、S3 SDK 进行访问。OBS 对象存储服务可以提供创建桶、删除桶、对象上传、下载、删除等操作。

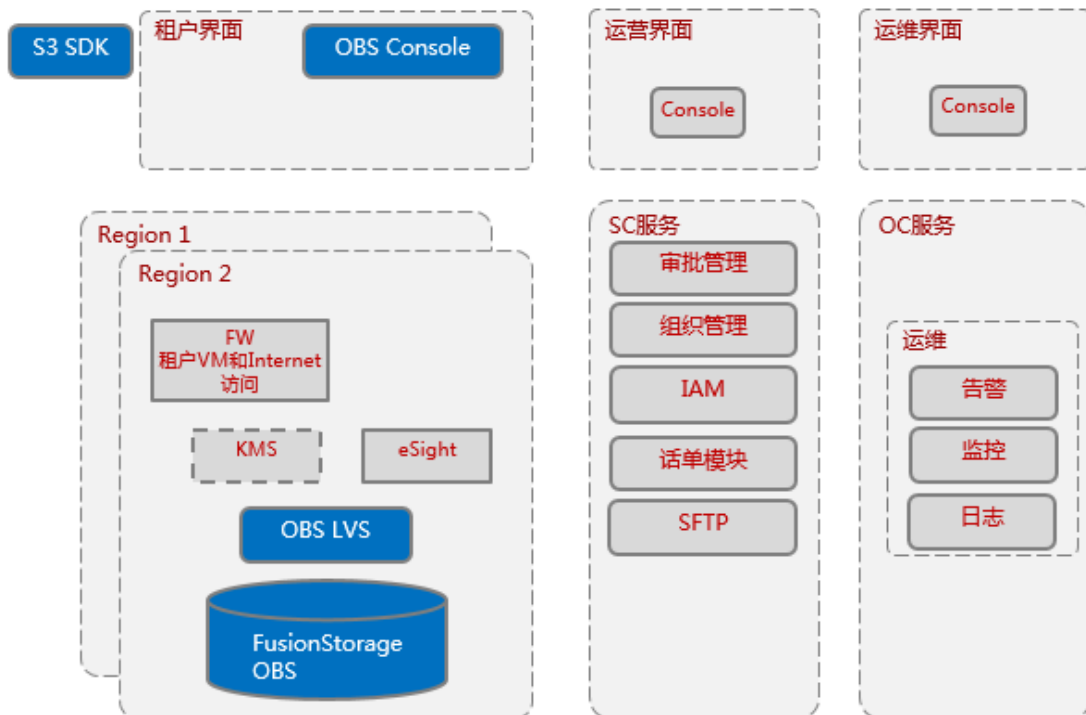


图 OBS 对象服务逻辑架构图

3、服务能力介绍

支持创建、删除、查看桶和 AK/SK 密钥。支持桶 ACL 设置、对象 ACL 设置和桶策略设置。

支持存储资源池在线扩展。

支持数据加密：通过 KMS 服务提供的密钥，对文件进行服务端加密。

支持数据检查：存储前一致性检查，确保存入数据是上传数据。

支持全局命名空间，无需指定区域即可访问全部桶和对象。

生命周期管理：用户可以为某个桶定义生命周期管理规则，来为该桶的对象定义各种生命周期规则。

支持查看用户配额（容量）、桶配额（容量）。

支持最大 48.8TB 的超大文件存储，轻松搞定大数据存储。

多版本控制：开启多版本控制后。

– 上传对象时，OBS 自动为每个对象创建唯一的版本号。上传同名的对象将以不同的版本号同时保存在 OBS 中。

– 可以指定版本号下载对象，不指定版本号默认下载最新的对象。

支持大文件分段上传和合并。

批量上传、删除对象。

支持桶日志管理：支持对桶的访问请求创建并保存访问日志信息，可用于请求分析或者日志审计。

支持防盗链设置：为了防止用户在 OBS 的数据被其他人盗链，OBS 支持基于 HTTP header 中表头字段 refer 的防盗链方法。OBS 同时支持访问白名单和访问黑名单的设置。

支持静态网站托管：OBS 支持 CORS 规范，允许跨域请求访问 OBS 中的资源，通过 CORS 支持，使用 JavaScript 和 HTML5 来构建 Web 应用，直接访问 OBS 中的资源，而不再需要代理服务器做中转。托管在不同域中的外部网页、样式表和 HTML5 应用，现在可以引用存储在 OBS 中的 Web 字体或图片，让这些资源能被多个网站共享。

OBS 服务规格。

规格项	规格
单租户可创建桶数量	最大 100
单桶可支持对象数量	最大 100 亿个

规格项	规格
可上传单文件大小（OBS Browser）	最大 48.8TB 文件
可上传单文件大小（OBS Console）	最大 5GB 文件

4、服务约束

存储仅支持 Fusionstorage OBS 7.0，存储节点仅支持特定配置的 2288H V5、5288 V5、TaiShan 2280 v2、TaiShan 5280 v2 服务器。

负载均衡默认采用 LVS，推荐使用 2288H V5 和 TaiShan 2280 v2 服务器部署，当前只支持基于 2288H V5 和 TaiShan 2280 v2 服务器的自动化部署。

Internet 用户访问对象存储(Internet 面)，需要使用边界防火墙 NAT 转换功能。

对象存储集群后端业务交换机建议单独使用，不建议和其他业务共用。

OBS 服务当前只能支持 S3 协议，不支持 Swift 协议。

OBS 服务界面最大支持 5GB 的文件上传，对于大于 5GB 的文件，用户可以选择第三方工具或者针对 S3 的接口自行开发工具进行上传。。

为了保证客户上传对象可持续性体验，OBS 默认不限制使用，采用先使用后计量机制。若需限制租户使用量，需在创建租户时设置 OBS 配额。

OBS 配额只能在一级组织上配置管理，不支持在二级及以下组织中配置管理。

默认的 VDC 管理员和 VDC 业务员角色，拥有 OBS 资源的管理权限，可管理其所在一级组织内（包括下级组织）的所有 OBS 资源。要限制用户 OBS 权限需另创建自定义角色。

OBS 服务部分基本功能基于域名访问，需要将 OBS 域名注册至域名服务器，客户端也需要配置域名服务器 IP 地址。

KMS 加密功能依赖 KMS 服务，KMS 服务只支持在 TypeI 和 TypeII 场景部署，不支持 TypeIII。

1.6 SFS（NAS）存储服务

1、服务应用场景

支持视频云、遥感云应用场景，为卡口图片、视频监控图像、遥感影像存储等提供可横向扩展的存储空间。

为高带宽、海量数据视频云、遥感云场景的应用提供文件存储。

2、服务架构

SFS 服务包含以下组件并介绍如下：

SFS Console: 提供租户访问界面，供租户创建、管理文件共享

OceanStor DJ: 基于 OpenStack Manila 提供创建/查询/删除等文件共享 API

OceanStor 9000 driver: 配合 Manila API，调用 OceanStor 9000 接口实现创建/查询/删除文件共享等功能

OceanStor 9000 : 分布式 NAS 存储，提供基础的创建/查询/删除文件共享等能力

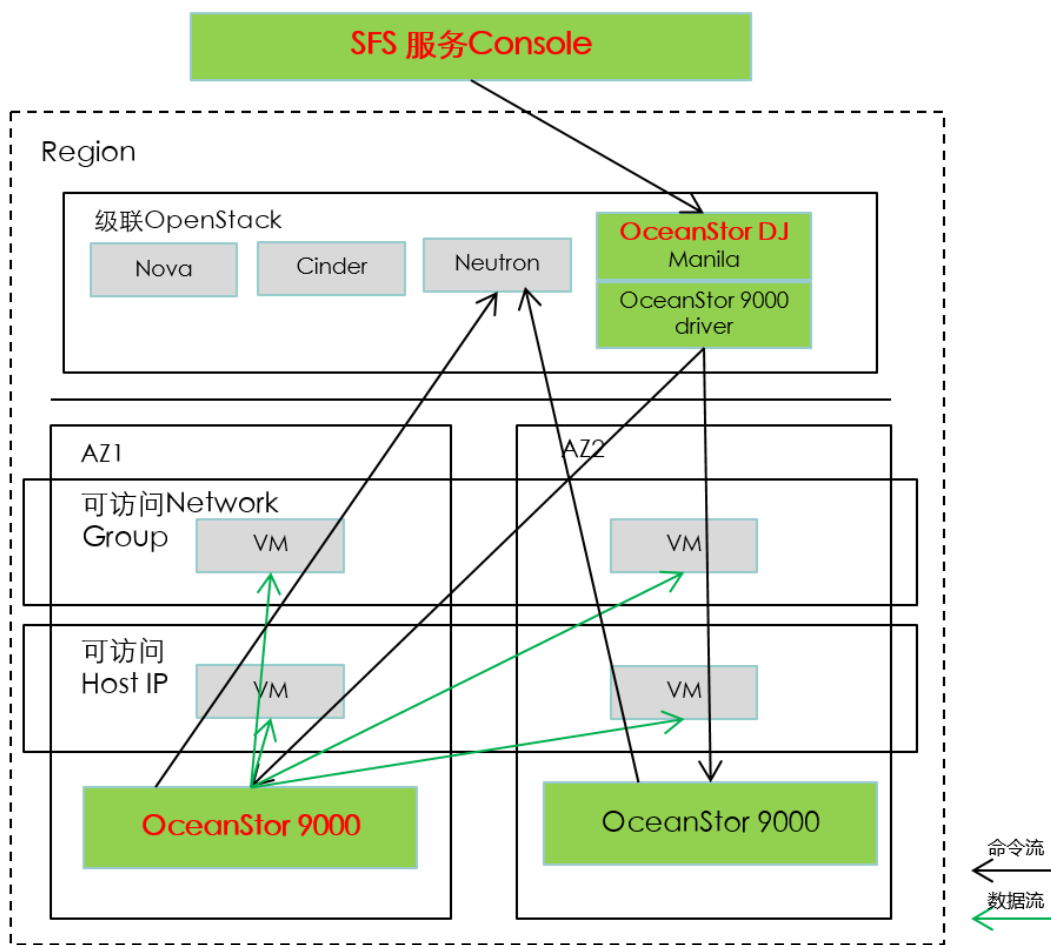


图 SFS 服务架构图

3、服务能力介绍

软件 SDN (Type1)	硬件 SDN (Type2)	无 SDN (Type3)	接入 ManageOne 运营框架
√	√	√	√

功能点	功能点描述	功能实现约束（含组合约束）
存储兼容性	华为云 Stack SFS 仅 NFS 共享支持 OceanStor 9000 V300R006C20SPC300, CIFS 和 NFS 同时支持, 需要 OceanStor 9000 V5 7.0.1 版本才能支持。	不支持其他华为存储及第三方文件存储
支持创建文件存储	输入创建文件系统所需参数: 文件共享名称(非全局唯一, 同一集群内不重复, 批量创建加四位数字升序)、AZ、容量(可指定也可以无限制)、数量(>1 就批量创建)、文件存储服务等级、协议(NFSv3、CIFS)、访问网络(SDN 组网填虚拟私有云-VPC,无 SDN, NFS 填主机 IP 或 IP 段, CIFS 填用户名)	<ol style="list-style-type: none"> 1. 创建文件共享时, 如在同一个集群已存在同名文件共享, 则在末尾添加数字+字母的随机码, 避免冲突 2. 无 SDN 组网, 创建时指定访问规则不超过 20 条, 支持 IPv4, IPv6 地址 3. 无 SDN 组网, NFS 不支持设置为* (默认所有主机都可以访问该共享)
支持删除文件存储	文件存储删除后到回收站, 回收站的文件存储可恢复和永久删除。回收站的文件存储不可挂载使用。冻结期的资源不可删除, 但可以恢复。	<ol style="list-style-type: none"> 1. 文件服务控制台不支持批量删除 2. 软删除状态的文件共享不允许挂载访问, 所占用配额及文件共享名称均不释放, 软删除资源可在回收站->文件服务的列表中可以查看。 3. 软删除状态的文件共享恢复后, 可挂载访问, 在文件服务控制台可查看, 回收站不显示已恢复的文件共享。 4. 彻底删除的文件共享, 释放文件共享名称, 释放配额, 在回收站界面和文件服务控制台均无显示。
查询文件共享	文件存储的详细信息, 包括名称、ID、状态、可用分区、创建时间、挂载路径、可用分区、创建时间	-
修改挂载权限	无 SDN 组网, NFS 支持添加	无 SDN 组网, 支持一次修改 20 条

功能点	功能点描述	功能实现约束（含组合约束）
	<p>或删除允许访问文件共享的主机 IP 地址，CIFS 支持添加允许访问的用户或用户组名。</p> <p>软件 SDN 和硬件 SDN 组网，支持添加允许访问文件共享的 VPC 网络，支持指定 VPC 网络中允许访问文件共享的主机 IP，支持指定文件共享的用户权限。</p>	<p>访问规则指定客户端 IP 地址，每个文件共享可以有 2000 条访问规则。</p> <p>软件 SDN 和硬件 SDN 组网，同一个文件共享，最多只能添加 20 个 VPC，同一个文件共享，设置的允许访问的主机 IP 总数量，不能超过 400 条。</p>
文件存储容量调整	支持文件存储容量在线扩容/缩容（不限容量的文件存储不能扩容，不限容量的文件存储可缩容成限制容量，限制容量的文件存储可以扩容成不限制）	<p>1、不能缩容到小于实际数据存储空间占用的大小。</p> <p>2、有指定容量的共享，扩容成不限容量时，实际失效时间最长会延迟一个小时。</p>
使用文件存储（手动挂载）	<p>1.用户登录弹性云服务器，第一次挂载，在 /etc/resolv.conf 中添加域名解析 DNS</p> <p>2.使用 showmount 命令查看或者使用 VDC 业务员登录租户面 portal，查看文件服务控制台中，所要挂载的文件存储的共享路径并复制</p> <p>3.输入 NFSv3 的挂载命令，例如 mount -t nfs -o vers=3,timeo=600,nolock xxx.xxxx.xxx.com:/share-xx-xxx /mountdir，同时配置第 5 步</p> <p>4.1 输入命令后无报错，则进入挂载路径/mountdir，创建文件验证挂载成功</p> <p>4.2 输入命令后有报错，请提示信息进行问题修改</p> <p>5.1 弹性云服务器如需重启自动挂载文件存储，则修改 /etc/fstab，增加 mount 命令开机自动挂载。</p> <p>5.2 步骤 1-5.2，可以用本步骤实现，在 OS 中安装好文件服务自动挂载 agent，在 SFS 用户页面上，选择文件</p>	<p>文件服务通过配置存储 OceanStor 9000 InfoEqualizer 特性的配置（动态域名）结合租户 DNS 配置的方式进行挂载访问文件存储。</p> <p>使用自动挂载功能，需要在操作系统中安装自动挂载 agent。</p>

功能点	功能点描述	功能实现约束（含组约束）
	共享的挂载标签，选择对应虚拟机 agent 会自动挂载文件共享。	
使用文件存储（自动挂载）	<p>1.用户的 ECS 虚拟机已经安装弹性文件服务自动挂载 agent。</p> <p>2.用户在弹性文件服务管理页面，点击弹性文件资源的挂载，选择需要挂载的 CS 虚拟机。</p> <p>3.用户也可以取消挂载弹性文件资源的挂载配置。</p>	<p>1、只支持 ECS 部分操作系统的虚拟机。</p> <p>2、不支持裸金属服务 BMS。</p> <p>3、自动挂载完成挂载的时间最长会有 3 分钟延迟。</p>
支持 NFS 协议	支持 NFS V3 协议	不支持 NFS v4 协议
支持 CIFS 协议	支撑 SMB2,SMB3 协议	
支持文件服务注册	支持定义无审批和有审批文件服务产品	-
租户 DNS	提供租户访问 SFS 的域名解析能力	-
SFS 云服务支持 UI3.0	参考 UI3.0 规范	
支持操作日志上报	日志包括（资源申请，变更，软删除，彻底删除，还原等）需要记录到 MangeOne, 云服务控制台操作也需要记录 MangeOne	
支持文件服务卸载	在安装时界面支持选择“取消注册到产品管理”	-
支持计量，计费	SFS 按照话单格式生成话单文件，上传到 ManageOne 提供的 SFTP 服务器上	-
支持添加 OceanStor 9000 存储	支持接入存储设备（型号、IP、用户名、密码等）	-
文件存储设备删除	支持移除存储设备	-
创建/删除/修改文件存储服务等级	创建/删除/修改文件存储服务等级	-

功能点	功能点描述	功能实现约束（含组合约束）
支撑 IPv6&IPv4 双栈	支持 IPv6 的主机挂载共享，也支持 IPv4 的主机挂载共享。	双栈是租户可见的地方为双栈，后台管理面是单栈，业务面是双栈。
HCS Deploy 部署	HCS Deploy 自动化安装部署 SFS 服务需要的组件，目前支持 SFS-Console, SFS-manila 的 HCS Deploy 部署, 不支持 OceanStor 9000 存储设备的 HCS Deploy 部署。	9000 产品不支持 HCS Deploy 部署，与 9000 相关的安装、配置、对接等操作，需要使用存储的 smartkit 工具操作。

4、服务约束条件

支持文件存储 OceanStor 9000 V5 7.0.1 版本，节点类型包括 P12X/P25X/P36X/C36X

客户端兼容性列表：支持文件系统挂载的操作系统版本范围

类型	版本范围
CentOS	CentOS 5,6,7 for x86
Debian	Debian GNU/Linux 6,7,8 for x86
Oracle	Oracle Enterprise Linux 5,6,7 for x86
Red Hat	Red Hat Enterprise Linux 5,6,7 for x86
SUSE	SUSE Linux Enterprise Server 10,11,12 for x86
Ubuntu	Ubuntu 10,11,12,13,14,15 LTS for x86

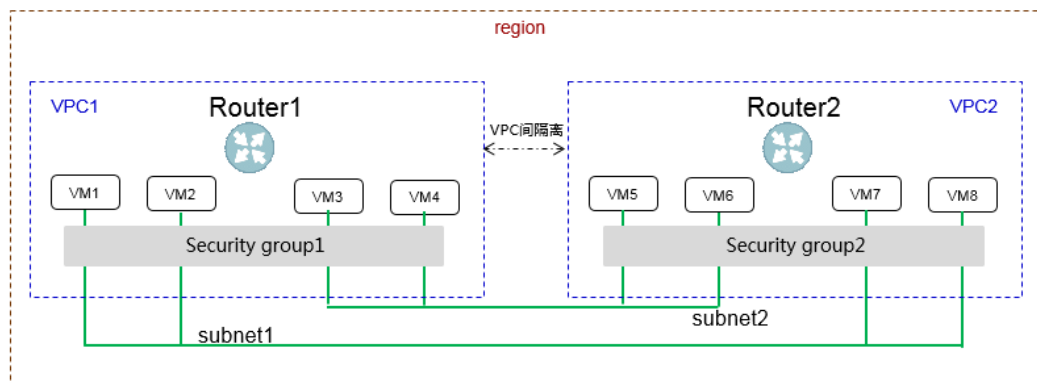
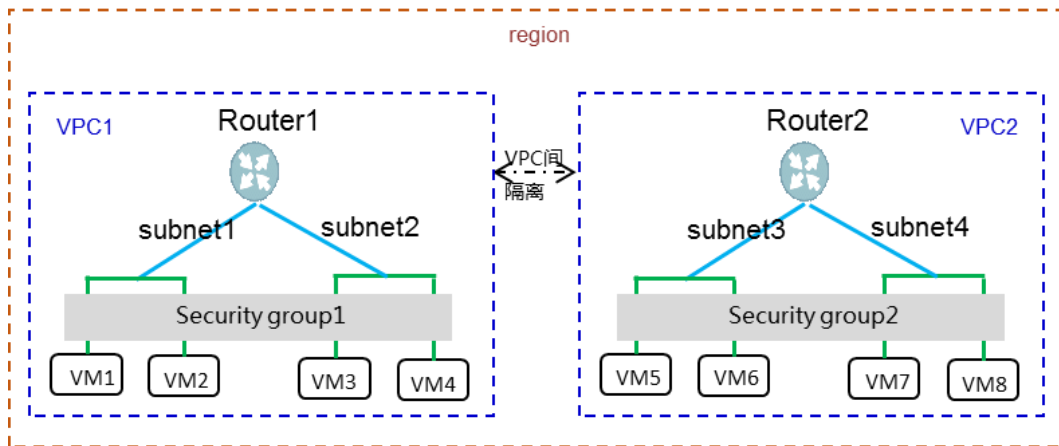
1.7 VPC 网络服务

1、服务应用场景

VPC 即虚拟私有云，是通过逻辑方式进行网络隔离，提供安全、隔离的网络环境，提供与传统网络无差别的虚拟网络。

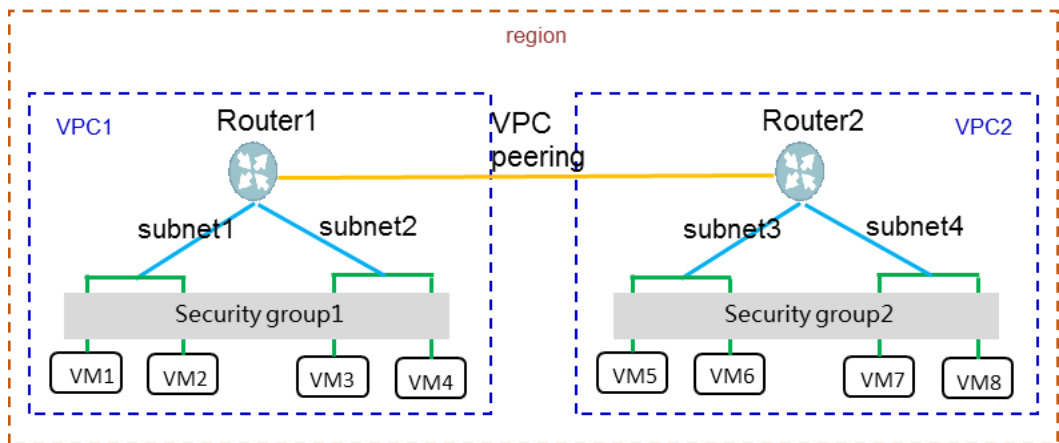
场景 1 多个子网的 VPC

首先按照网络规划创建 VPC 和 subnet, 并在虚拟私有云中创建云主机使用；VPC 间隔离。



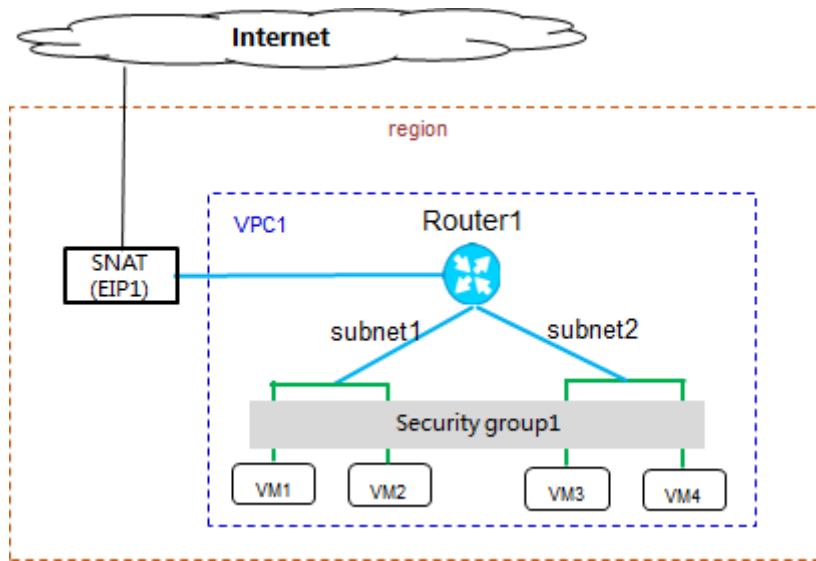
— 场景 2 VPC 互通

首先规划创建两个 VPC，互通 VPC 的子网地址不能重叠。



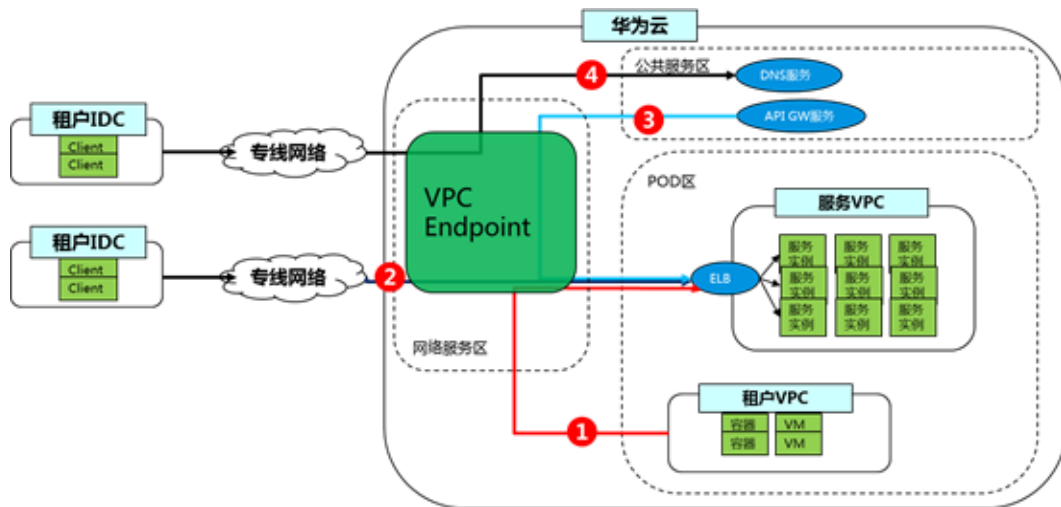
场景 3 VPC 通过 SNAT 访问公网

多个子网的虚拟机通过 SNAT 共享 EIP 访问 Internet 网络。如下图，VPC1 内 subnet1、subnet2 子网内的所有 VM 都共享 EIP1 访问外网。



场景 4 VPC 通过 VPC Endpoint 访问 其他租户的 VPC

VPC Endpoint 提供了不同租户 VPC 虚拟机间的内部互访，而不需要依赖公网 IP 资源。VPC Endpoint 没有源 VPC 和目的 VPC 子网不能重叠的限制。目前仅支持租户 VPC 虚拟机和 PaaS 服务提供商 VPC 虚拟机间的内部互访。



2、服务架构

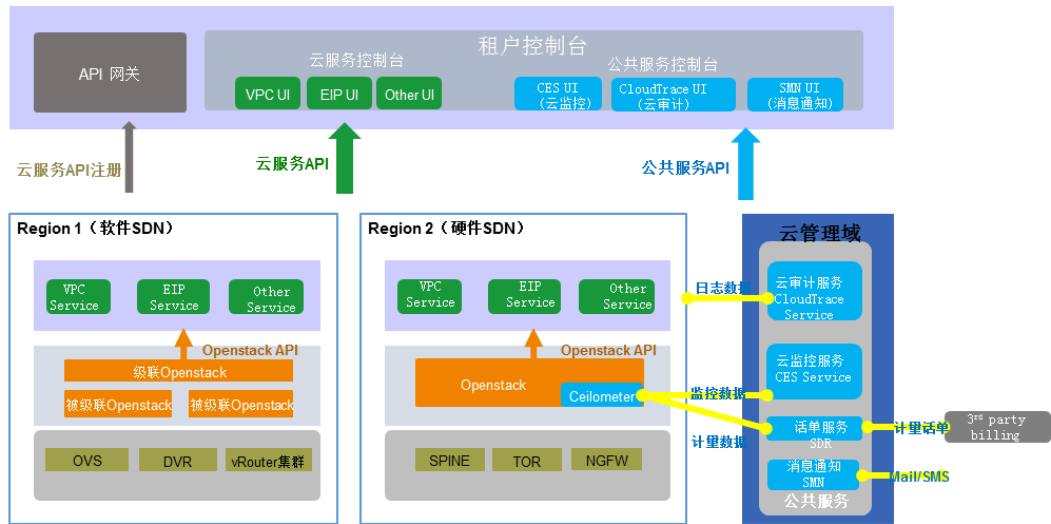


图 VPC 网络服务架构图

服务架构分为云服务层、资源池层、基础设施层和云管理域。

云服务层

云服务层提供统一的云服务申请和自助操作服务控制台。

VPC 服务提供 VPC 服务实例申请和自助操作维护控制台。VPC 服务分为 VPC UI 和 VPC Service 两部分，VPC UI 提供面向用户的控制台 VPC Service 提供服务管理功能。

公共管理服务控制台包括 CES UI, CTS UI, SMN UI。CTS 提供审计服务，可查看 VPC 实例的操作日志；SMN 提供消息通知功能，支持发送短信或邮件。

资源池层

资源池层为 VPC 服务提供计算、存储、网络资源。资源池分为软件 SDN 和硬件 SDN 两类 Region 类型。其中软件 SDN 使用计算节点的 OVS、DVR 和 vRouter 集群完成 VxLan 的封装/解封装；硬件 SDN Region 使用硬件交换机完成 VxLan 的封装/解封装。

基础设施层

服务器、存储、网络等物理基础设施，构成数据中心资源池的基础架构。

云管理域

云管理域提供公共管理服务，包括云审计服务、云监控服务、计量数据、消息通知服务。

3、服务能力

VPC 服务通过 web 管理控制台，让用户自主的完成服务的开通与关闭，让用户灵活使用 VPC 服务，达到即开即用，用完归还的目标。

VPC 服务具有以下功能：

支持子网管理

可以创建多个子网，指定子网申请虚拟 IP，以及修改私有 IP 地址。

支持 IPv4，IPv6 双栈场景。

路由管理

配置 VPC 的默认路由，把指定目的网段的报文发给指定下一跳。

支持 IPv4，IPv6 双栈场景。

支持 SNAT

SNAT 为虚拟私有云内的弹性云服务器提供网络地址转换服务，使多个弹性云服务器可以共享使用弹性 IP 访问 Internet，节省客户公网 IP 资源。

VPC Peering

支持租户使用私有业务 IP 地址在安全隔离的 VPC 之间实现三层路由互通。

支持 IPv4，IPv6 双栈场景。

专线

租户创建 VPC 的时候可以给 VPC 创建专线，允许 VPC 的 VM 直接与 DC 外的节点通信。

VPC Endpoint（Taishan 场景不支持）

支持租户 VPC 通过访问资源租户 VPC。

支持专线/VPN 通过 endpoint 访问资源租户 VPC

1.8 网络安全组

1、服务应用场景

安全组是一组对实例的访问规则的集合，为同一个 VPC 内具有相同安全保护需求并相互信任的实例提供访问策略。

2、服务架构

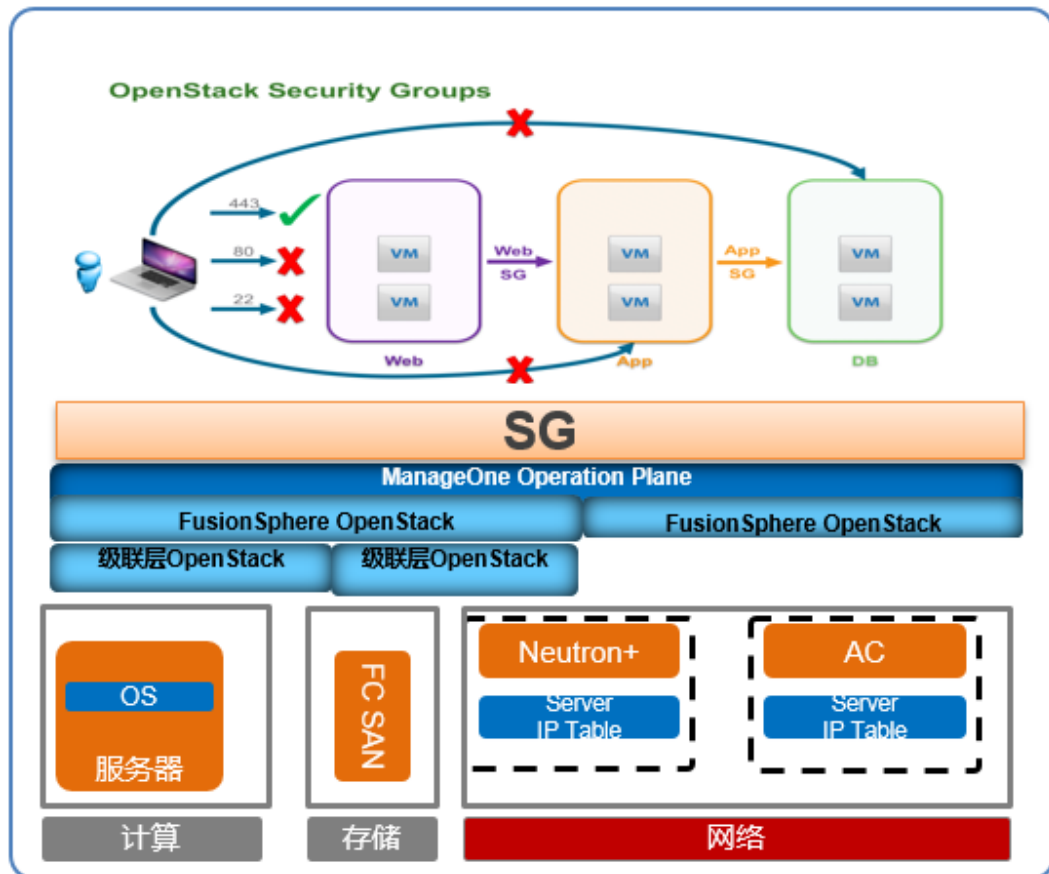


图 网络安全服务架构图

服务架构分为云服务层、资源池层、基础设施层和云管理域。

云服务层

云服务层提供统一的云服务申请和自助操作服务控制台。

安全组服务提供安全组服务实例申请和自助操作维护控制台。安全组服务分为 SG UI 和 SG Service 两部分，SG UI 提供面向用户的控制台 SG Service 提供服务管理功能。

公共管理服务控制台包括 CES UI，CTS UI，SMN UI。CTS 提供审计服务，可查看 VPC 实例的操作日志；SMN 提供消息通知功能，支持发送短信或邮件。

资源池层

资源池层为安全组服务提供计算、存储、网络资源。资源池分为软件 SDN 和硬件 SDN 两类 Region 类型。软件 SDN Region 和硬件 SDN Region 都使用 iptables 提供服务。

基础设施层

服务器、存储、网络等物理基础设施，构成数据中心资源池的基础架构。

云管理域

云管理域提供公共管理服务，包括云审计服务、云监控服务、计量数据、消息通知服务。

3、服务能力

安全组服务通过 web 管理控制台，让用户自主的完成服务的开通与关闭，让用户灵活使用安全组服务，达到即开即用，用完归还的目标。

安全组服务具有以下功能：

默认出方向放行。

同一个安全组的云主机默认可相互访问。

可以灵活配置出方向和入方向规格

管理

管理方便，用户可以通过 web 页面或者开放 API，同时管理一个、数十个、甚至上百个安全组实例。

安全

完全控制，用户可以完全控制自己创建的安全组实例。

支持 IPv4，IPv6 双栈场景。

1.9 VFW 服务

1、服务应用场景

VFW（Virtual Firewall）即虚拟防火墙，用于子网级别的安全防护，防火墙是一个或多个子网的访问控制策略，根据与子网关联的入方向/出方向规则，判断数据包是否允许流入/流出关联子网。

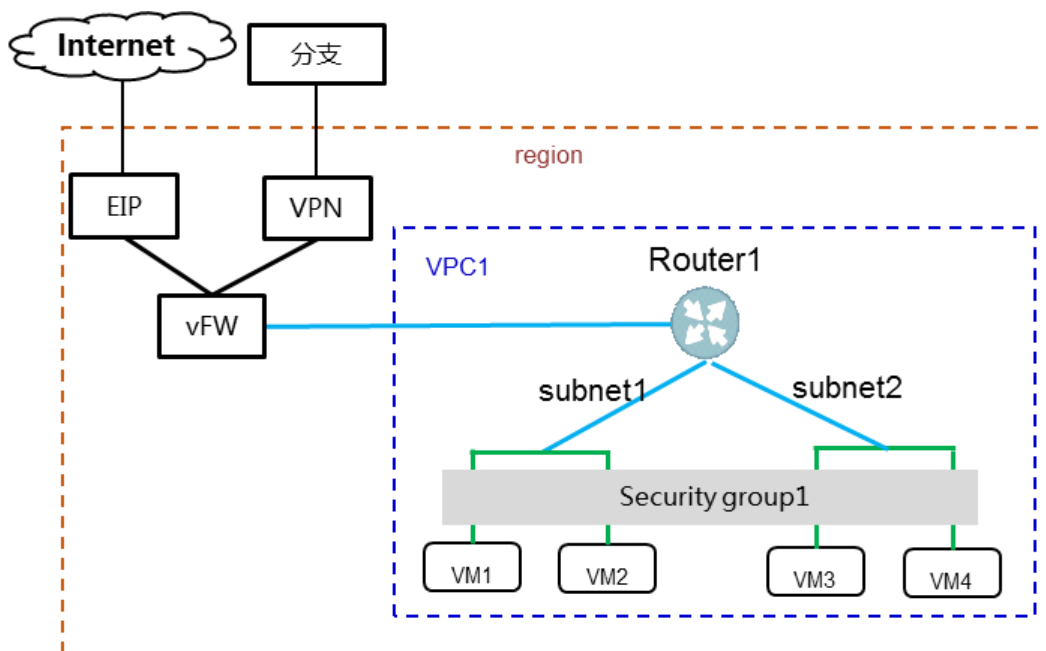


图 VFW 服务应用场景

2、服务架构

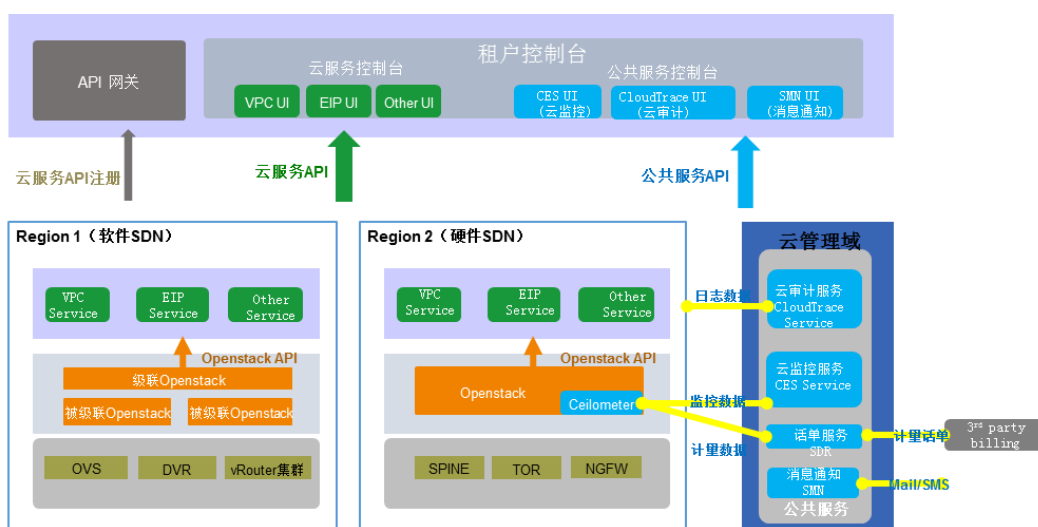


图 服务架构

服务架构分为云服务层、资源池层、基础设施层和云管理域。

云服务层

云服务层提供统一的云服务申请和自助操作服务控制台。

VFW 服务提供 VFW 服务实例申请和自助操作维护控制台。VFW 服务分为 VFW UI 和 VFW Service 两部分，VFW UI 提供面向用户的控制台 VFW Service 提供服务管理功能。

公共管理服务控制台包括 CES UI, CTS UI, SMN UI。CTS 提供审计服务, 可查看 VFW 实例的操作日志; SMN 提供消息通知功能, 支持发送短信或邮件。

资源池层

资源池层为 VPN 服务提供计算、存储、网络资源。资源池分为软件 SDN 和硬件 SDN 两类 Region 类型。其中软件 SDN 使用计算节点的 iptables 完成访问控制; 硬件 SDN Region 使用 NGFW 完成访问控制。

基础设施层

服务器、存储、网络等物理基础设施, 构成数据中心资源池的基础架构。

云管理域

云管理域提供公共管理服务, 包括云审计服务、云监控服务、计量数据、消息通知服务。

3、服务能力

VFW (Virtual Firewall) 即虚拟防火墙, 用于子网级别的安全防护, 防火墙是一个或多个子网的访问控制策略, 根据与子网关联的入站/出站规则, 判断数据包是否允许流入/流出关联子网。

VFW 服务具有以下功能:

支持配置 5 元组: 源端口, 源 IP 地址, 目的端口, 目的 IP 地址, 协议。

支持配置允许和丢弃。

支持与子网绑定, 一个 VFW 支持和多个子网绑定, 一个子网不能同时加入两个 VFW。

支持 IPv4, IPv6 双栈场景。

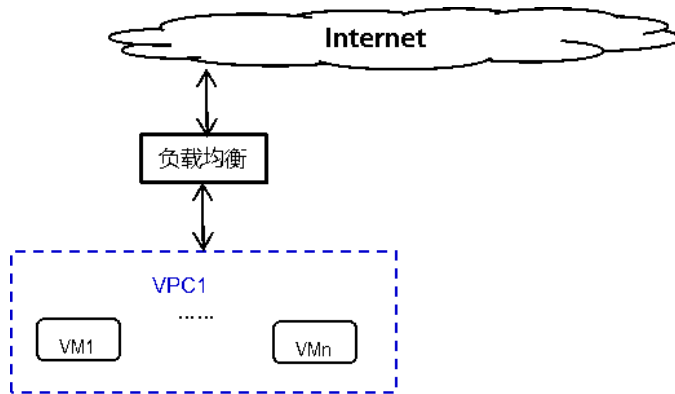
1.10 ELB 负载均衡服务

1、服务应用场景

ELB (Elastic Load Balance), 即弹性负载均衡, 是将访问流量根据转发策略分发到后端多台弹性云服务器的流量分发控制服务。弹性负载均衡可以通过流量分发扩展应用系统对外的服务能力, 实现更高水平的应用程序容错性能。弹性负载均衡可以消除单点故障, 提高整个系统的可用性。

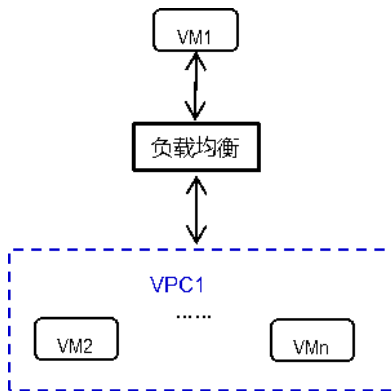
(1) 场景 1 南北向 ELB

通过 ELB 提供外网用户通过 internet 访问云服务。



(2) 场景 2 东西向 ELB

通过 ELB 提供内网租户在云网络内部访问云服务。



2、服务架构

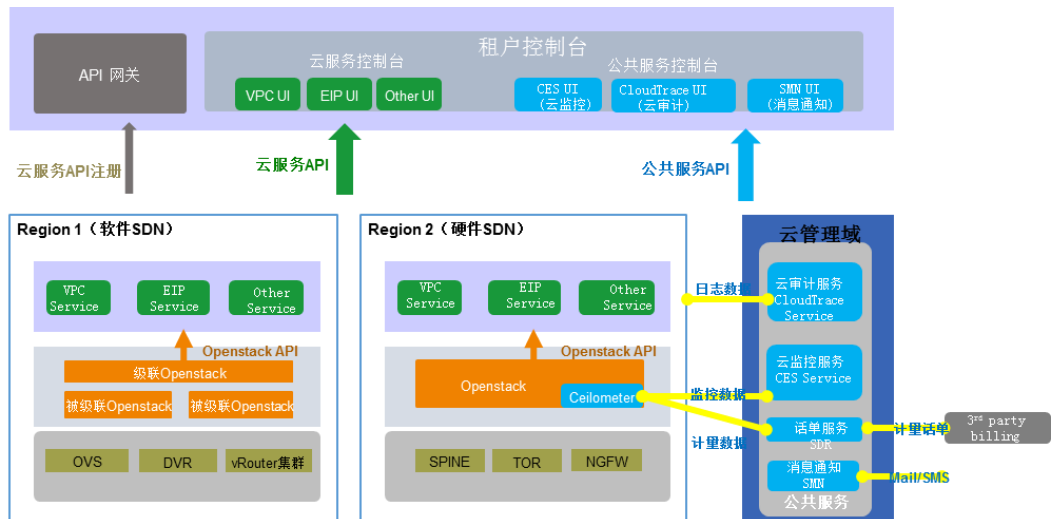


图 ELB 服务架构图

服务架构分为云服务层、资源池层、基础设施层和云管理域。

云服务层

云服务层提供统一的云服务申请和自助操作服务控制台。

LB 服务提供 LB 服务实例申请和自助操作维护控制台。LB 服务分为 LB UI 和 LB Service 两部分，LB UI 提供面向用户的控制台 LB Service 提供服务管理功能。

公共管理服务控制台包括 CES UI, CTS UI, SMN UI。CTS 提供审计服务，可查看 ELB 服务的操作日志；SMN 提供消息通知功能，支持发送短信或邮件。

资源池层

资源池层为 LB 服务提供计算、存储、网络资源。资源池分为软件 SDN 和硬件 SDN 两类 Region 类型。其中软件 SDN 使用融合 ELB 完成 LB 服务；硬件 SDN Region 使用深信服或融合 ELB 完成 LB 服务。

基础设施层

服务器、存储、网络等物理基础设施，构成数据中心资源池的基础架构。

云管理域

云管理域提供公共管理服务，包括云审计服务、云监控服务、计量数据、消息通知服务。

3、服务能力

LB 服务通过 web 管理控制台，让用户自主的完成服务的开通与关闭，让用户灵活使用 LB 服务，达到即开即用，用完归还的目标。

LB 服务具有以下功能：

支持多监听器能力，提供不同业务申请不同的监听器提供服务访问；

支持 TCP、UDP、HTTP、HTTPS 的负载均衡。

支持 HTTPS SSL 证书卸载。

支持证书管理。

支持 RR、源 IP、最小连接的负载均衡算法。

支持源 IP、HTTP_Cookie、APP_Cookie 的会话保持。

支持 TCP、HTTP 的健康检查。

支持访问白名单控制。

支持按域名、URL、内容转发。

支持 IPv4, IPv6 双栈场景。

1.11 AS 弹性伸缩服务

1、服务应用场景

弹性伸缩服务是根据用户的业务需求和策略，自动调整其弹性计算资源的管理服务。用户定义定时，周期及监控策略及伸缩组健康容量，来让弹性伸缩服务动态的调整 ECS 实例，保证业务平稳健康运行。

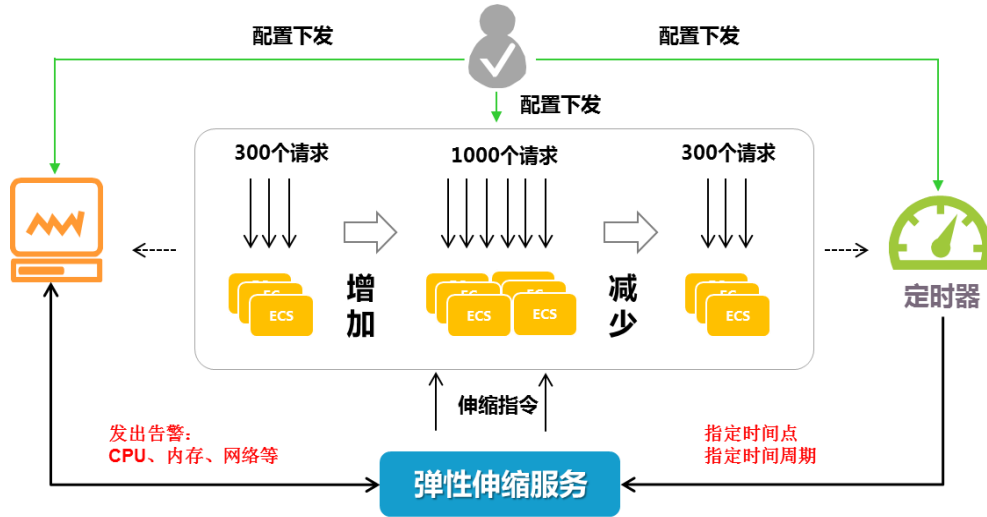


图 AS 应用场景示意图

2、服务架构

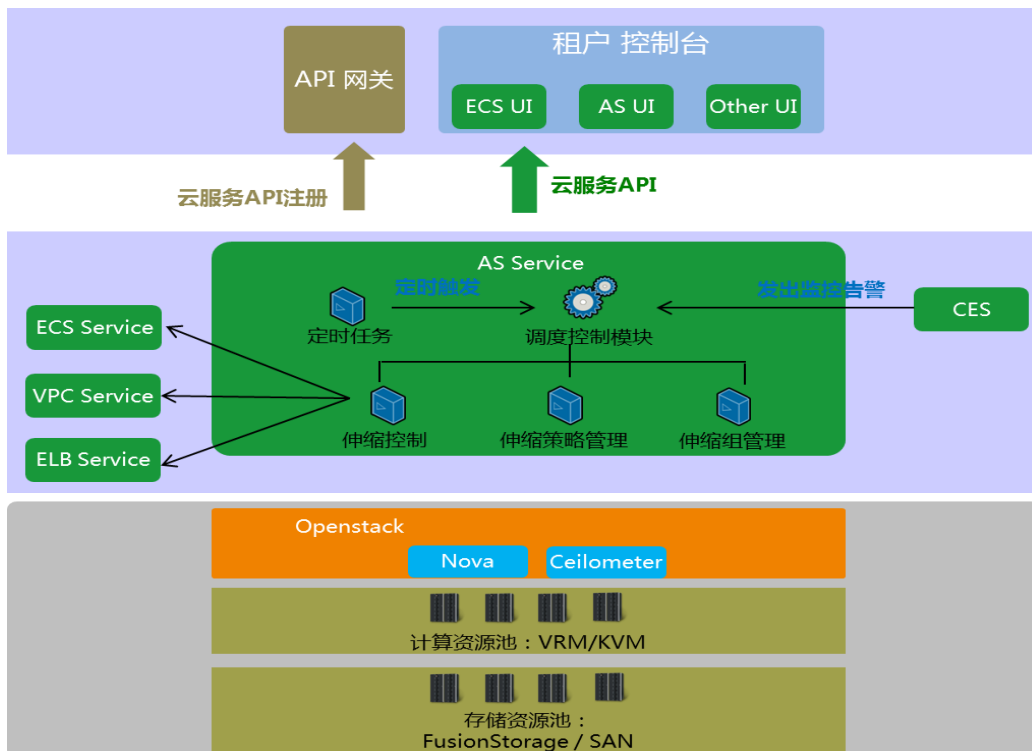


图 AS 服务架构图

AS 服务可以根据 ECS 实例的监控数据或定时任务触发弹性伸缩的调度。

基于监控告警触发：周期性（例如 5 分钟）获取伸缩组内各虚拟机的监控数据；伸缩组内各虚拟机监控数据的平均值若达到告警门限值，则 ECS 发送告警给 AS 调度控制模块。

基于定时或周期触发：定时任务触发后，定时任务发送调度任务到 AS 调度控制模块。

当满足伸缩条件时，AS 调度控制模块向 ECS 发送创建或删除虚拟机的请求；然后发送绑定后端云主机的请求给 ELB 完成伸缩活动。

3、服务能力

支持三种伸缩触发模式

基于监控告警的动态触发模式：

基于云监控性能指标（如 CPU 利用率、内存利用率、网络流入速率、网络流出速率），自动增加或减少 ECS 实例。

定时触发模式

配置一次性定时任务，定时地增加或减少 ECS 实例。

周期触发模式

配置周期性任务，周期性地增加或减少 ECS 实例，当周期性需求有所波动时，可同时配置告警触发模式以应付不可预期的变化。

实例数范围控制

支持期望实例数，最小实例数，最大实例数的管理；通过实例数范围控制，可以让您始终保持健康运行的 ECS 实例数量，自动替换不健康实例，以保证日常场景实时可用。

ELB 服务联动

支持与 ELB 服务结合，自动为伸缩组虚拟机实例绑定负载均衡器。在增加或减少 ECS 实例时，自动向 ELB 实例添加或移除相应的 ECS 实例。

支持 ECS 实例健康检查

支持对伸缩组内的虚拟机进行健康检查，包括“云主机健康检查”、“负载均衡健康检查”，可以对不健康节点自动处理。

1.12 vAPP 服务

1、服务应用场景

vApp 服务有如下表所示多个场景应用：

场景	诉求描述
从基础设施到应用统一编排	客户希望能够一键式完成基础设施到应用的部署，提升应用上云的效率。
弹性伸缩保证业务平稳运行	客户希望在业务访问压力大的情况下，系统能够自动扩容资源，保证业务正常可以，业务负荷低时，系统可以自动化回收资源，保证系统资源可以得到充分的利用。
多资源池编排	客户环境同时存在多种虚拟化资源池，希望能够统一编排部署应用环境. 提升部署效率.
快速的复制相同或相似配置的应用环境	客户希望能够快速的创建多套相同或相似配置的应用环境，不必要每个应用环境重新搭建。
频繁的部署和删除应用环境	客户的开发和测试环境需要频繁的搭建和删除应用环境，希望能够有快速便捷的手段。

2、服务架构

vApp 服务可以帮助企业实现 IT 资源和能力复用，通过图形化的模板编排能力和一站式的部署能力，快速实现应用部署，从而能够使客户专注于核心业务和创新，同时可以加快产品开发，缩短上市时间，提升应用弹性和可用性，升级产品的竞争力。

vApp 服务部署在 Global 区，可以和多个 Region 的云服务通过插件适配对接，具备多 Region，多资源池，多云，单 Region 跨资源池的编排能力，在 6.5 版本支持 OpenStack 资源池和 VMware 资源池的资源编排。同时，支持编排 AutoOps（自动化运维平台）服务，可以通过 AutoOps 部署应用软件。

注：方案中，兼容对接的资源池版本信息如下：

VMware: vSphere 5.0/5.1/5.5/6.0/6.5

Openstack: Mitaka、Queens

vApp 提供图形化资源模板编排、一键式应用部署、弹性伸缩的应用自动化部署服务。vAPP 服务通过可视化编排界面任意拖拽图元，快速完成云主机，块存储，VPC、VLB（依赖 SDN），弹性伸缩组、亲和性组、密钥对、应用等资源的自动化部署，并作为一个整体为用户提供服务，支撑业务快速上线，并且可以

自定义自动伸缩策略以达到自动扩容和减容的弹性云服务器，以实现负载均衡，资源充分利用。

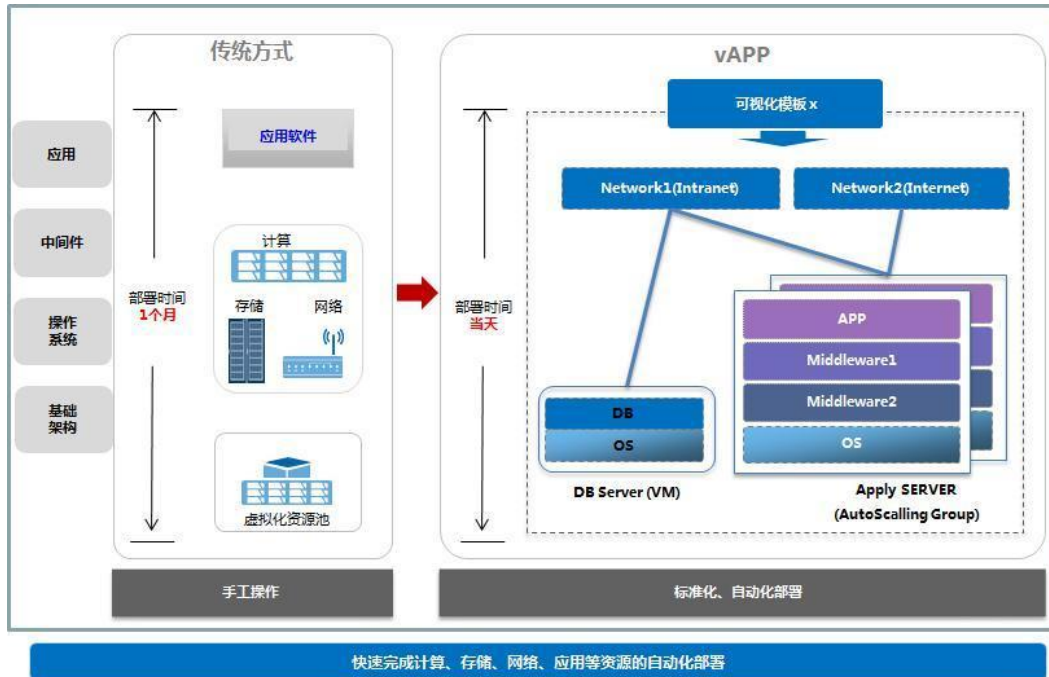


图 vAPP 服务架构

3、服务能力

(1) 应用编排

如下图所示，vApp 提供了专业的图形化设计器，帮助用户更好的编写和设计模板，用户可以通过图形化拖拽的方式快速编排资源和应用，定义资源和应用之间的关联关系，为资源和应用指定参数属性。同时图形化设计器还支持模板嵌套能力。用户在图形化设计器中设计好模板后，vApp 会自动根据设计的内容转换成模板代码。

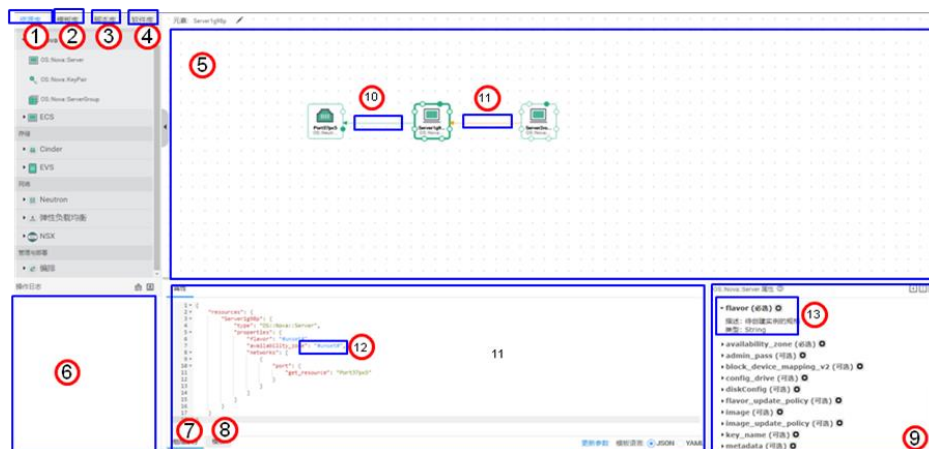


图 图形化界面设计器

-
1. 资源库：可被编排的单个基础设施资源列表。
 2. 模板库：可被编排的子模板列表。
 3. 脚本库：可被编排的系统配置或软件配置脚本。 来源于脚本管理中的脚本。
 4. 软件库：可被编排的软件资源， 来源于软件管理中的软件。
 5. 画布区：定义编排资源以及资源之间的依赖关系。
 6. 操作日志：记录本次编排做的所有操作。
 7. 组成部分：单个资源对应的模板代码片段。
 8. 模板：整个模块的完整代码。
 9. 属性列表区：资源的所有属性介绍。
 10. 绿色连线：资源属性应用。
 11. 黄色连线：资源间的部署依赖。
 12. 属性参数输入：属性入参设置。
 13. 单个属性的详细说明：包括参数属性的描述和类型等。

(2) 应用自动部署

vApp 支持两种部署应用的方式， 一种是通过 OpenStack 原生的 cloudinit 机制， 另外一种是通过 AutoOps 的机制实现应用的安装部署。

Cloudinit 机制依赖 OpenStack 平台， 且只能在虚拟机初始化阶段完成应用部署， 不支持部署后的变更， 属于 OpenStack 原生的能力。

AutoOps 机制不依赖 OpenStack 平台， 通过 AutoOps 自身的能力， 在目标虚拟机中安装 Agent， 通过 Agent 完成应用程序的部署。 且支持部署后的应用的变更。具体原理如下图所示。

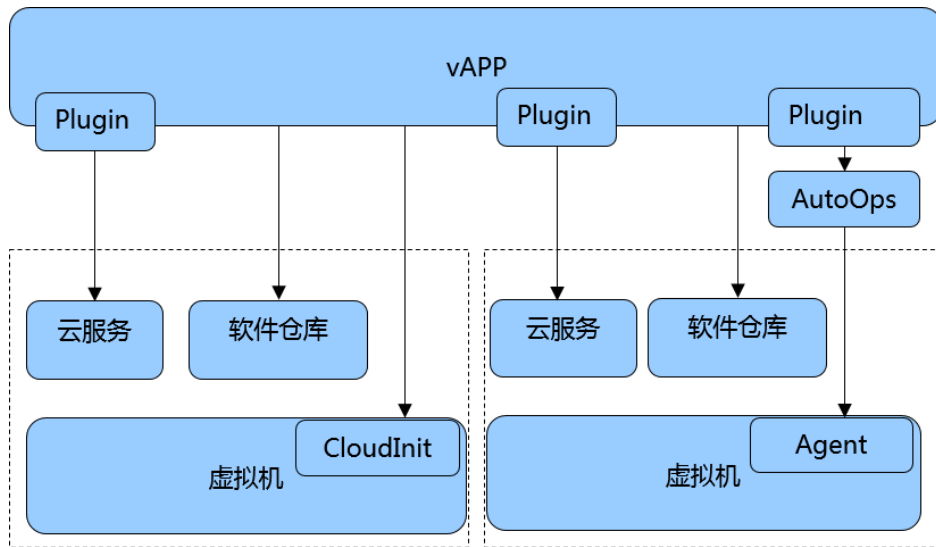


图 应用自动部署原理图

(3) 应用弹性伸缩

通过 vApp 部署应用时，可以为 vApp 部署应用的虚拟机定义弹性伸缩组和弹性伸缩策略，在 vApp 实例发放完成后，vApp 会根据弹性伸缩策略的定义在 CES 中设置阈值告警，CES 会定期采集 vApp 中的虚拟机的相关性能指标，检测是否超出阈值，如果超出阈值，则会发送通知告警给 vApp，vApp 收到后，根据策略定制执行相关的虚拟机扩缩的动作，具体的原理如下图所示。

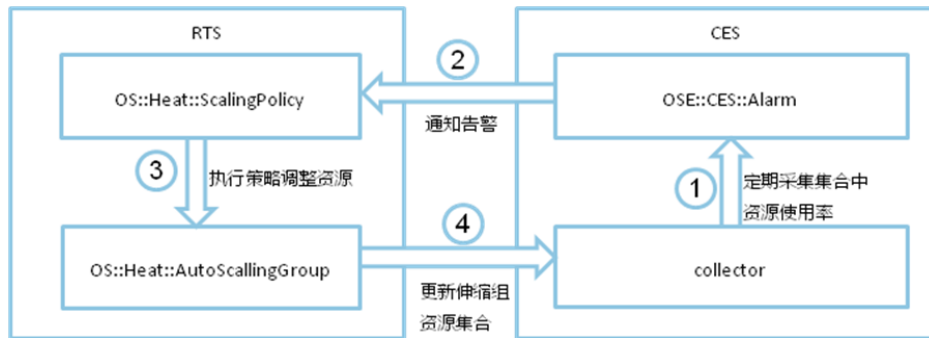


图 弹性伸缩原理

(4) 应用模板管理

vApp 提供的模板管理，具体支持的功能列表如下表所示：

表 vAPP 模板管理

功能分类	功能	功能描述
我的模板	自定义模板管理	支持模板的创建，删除，修改，查询，复制，导入，导出，创建服务产品等功能。
样例模板	样例模板管理	内置 32+样例模板，支持样例模板的复

功能分类	功能	功能描述
		制，导出，查询，创建服务产品等功能。
图形化设计器	图形化设计器	支持图形化拖拽方式设计模板，可以定义模板之间的属性依赖和资源依赖关系，支持设计的资源包括：基础设施资源，应用，脚本，子模板等。

模板样例

提供开箱即用的常见模板，用户可以直接使用这些模板，部署场景的基础设施资源和数据库，中间件以及应用。vApp 内置的模板列表如下表所示：

表 内置模板列表

模板分类	模板名称
弹性云服务器	VPC 下的弹性云服务器模板
	带弹性 IP 的弹性云服务器模板
	典型 Web 三层架构网站模板
	简单高可靠的基础设施模板
网络资源	小型 VPC 网络架构模板
	中型 VPC 网络架构模板
	微型 VPC 网络架构模板
数据库	安装 MySQL 数据库模板
	安装 SQLServer 数据库的模板
	安装 Oracle11g 数据库的模板
	安装 Oracle12c 数据库的模板
	安装 MongoDB 数据库的模板
	安装 MongoDB 数据库集群的模板
	安装 Redis 服务模板
	安装 Redis 集群模板
中间件	安装 Apache 服务模板
	安装 JDK 环境模板
	安装 Tomcat 服务模板
	安装 WordPress 平台模板

模板分类	模板名称
	安装 WebLogic 服务模板
	安装 WAS 集群的模板
	安装 Kafka 服务模板
	安装 Kafka 集群模板
	安装 Nginx 服务模板
	安装 Jboss 应用服务器的模板
	安装 RabbitMQ 服务模板
	安装 Jboss 集群的模板
	安装 RabbitMQ 集群服务模板
	安装 WebLogic 集群的模板
	安装 Apache 服务模板
	安装 JDK 环境模板

备注：以上方案中，vAPP 只是提供了默认的部署脚本和模板，不包含软件包本身，安装部署脚本支持的软件兼容版本信息如下：

软件名称	兼容版本	操作系统版本
Apache	apache2-2.2.12-1.38.2.x86_64.tar.gz	SUSE Linux Enterprise Server 11 SP3 (x86_64)
JDK	Java Development Kit 8u131(jdk-8u131-linux-i586.tar.gz)	SUSE Linux Enterprise Server 11 SP3 (x86_64)
Tomcat	jdk-7u17-linux-x64.tar.gz apache-tomcat-8.5.16.tar.gz	SUSE Linux Enterprise Server 11 SP3 (x86_64)
MySQL	mysql-5.5.31-0.7.10.x86_64.tar.gz	SUSE Linux Enterprise Server 11 SP3 (x86_64)
WordPress	apache22_php53_mysql55_wordpress49.tar.gz	SUSE Linux Enterprise Server 11 SP3 (x86_64)
WebLogic	jdk-8u131-linux-i586.tar.gz weblogic_12.2.1.0.0	SUSE Linux Enterprise Server 11 SP3 (x86_64)
SQLServer	linux.x64_11gR2_database_1of2.zip linux.x64_11gR2_database_2of2.zip	SUSE Linux Enterprise Server 11 SP3 (x86_64)

软件名称	兼容版本	操作系统版本
Oracle12c	linuxamd64_12102_database_se2_1of2.zip linuxamd64_12102_database_se2_2of2.zip	SUSE Linux Enterprise Server 11 SP3 (x86_64)
WAS	IBM Installation Manager 1.6.2 x86 Linux IBM WebSphere Application Server Network Deployment V8.5.5 IBM Installation Manager 1.6.2 x86 Linux IBM WebSphere Application Server Network Deployment V8.5.5	SUSE Linux Enterprise Server 11 SP3 (x86_64)
MongoDB	jdk-8u131-linux-i586.tar.gz kafka_2.11-2.1.0.tgz	SUSE Linux Enterprise Server 11 SP3 (x86_64)
Nginx	openssl-1.0.2p.tar.gz、 pcre-8.42.tar.gz、zlib-1.2.11.tar.gz、 nginx-1.14.2.tar.gz	SUSE Linux Enterprise Server 11 SP3 (x86_64)
JBoss	Java Development Kit 7u17(jdk-7u17-linux-x64.tar.gz)、 JBoss(jboss-as-7.1.1.Final.zip)、 Apache2(apache2-2.2.10-2.24.5.x86_64.tar)	SUSE Linux Enterprise Server 11 SP3 (x86_64)
RabbitMQ	otp_src_R16B03.tar.gz、 rabbitmq-server-generic-unix-3.6.12.tar.xz、 libopenssl-devel-1.0.2j-32.1.x86_64.rpm	SUSE Linux Enterprise Server 11 SP3 (x86_64)
MongoDB	mongodb-linux-x86_64-suse11-3.6.0.tgz	SUSE Linux Enterprise Server 11 SP3 (x86_64)
Redis	redis-5.0.3.tar.gz	SUSE Linux Enterprise Server 11 SP3 (x86_64)
WebLogic	Java Development Kit 8u131(jdk-8u131-linux-i586.tar.gz)、 WebLogic Server(weblogic_12.2.1.0.0)	SUSE Linux Enterprise Server 11 SP3 (x86_64)
OracleRAC	linuxamd64_12102_grid_1of2.zip 、 linuxamd64_12102_grid_2of2.zip 、 linuxamd64_12102_database_1of2.zip、	SUSE Linux Enterprise Server 11 SP3 (x86_64)

软件名称	兼容版本	操作系统版本
	linuxamd64_12102_database_2of2.zip、 compat-libstdc++-33-3.2.3-72.el7.x86_64.rpm、 cvuqdisk-1.0.9-1.rpm	

(5) 脚本管理

vApp 提供脚本管理功能， 用户可以将系统配置相关的脚本放到 vApp 脚本管理中， 脚本管理中的脚本可以在图形化设计器中编排， 最终通过 vApp 推送到对应的虚拟机中执行。脚本管理提供的功能如下表所示：

表 脚本管理

功能分类	功能	功能描述
我的脚本	自定义脚本管理	支持脚本的创建， 删除， 修改， 查询， 功能。
样例脚本	样例脚本管理	内置 19+样例脚本， 支持样例脚本的查看功能。

(6) 软件管理

软件管理是通过 vApp 模板部署 vApp 实例时， 运行在 vApp 实例中弹性服务或裸金属服务器中的应用软件。软件管理管理应用软件的基本信息包括： 软件名称， 描述， 版本， 安装， 卸载， 配置脚本等。软件管理中的软件可以在图形化设计器中编排， 最终通过 vApp 推送执行相关的安装部署脚本完成应用软件的部署。

表 软件管理

功能分类	功能	功能描述
软件管理	自定义软件管理	支持软件的创建， 删除， 修改， 查询， 功能。

(7) vAPP 实例

vApp 实例是提供某种业务的一组弹性云服务器和软件集合。由一个或多个弹性云服务器组成， 通过弹性云服务器的网络、软件、EIP、安全组、ELB 等相互配合， 对外提供某种服务。用户可以管理 vApp 实例， 具体的管理功能如下表所示。

表 实例管理

功能分类	功能	功能描述
------	----	------

功能分类	功能	功能描述
实例管理	实例管理	支持申请，变更，删除，修改，延期，查看实例。
实例概览	实例概览	支持查看实例的概要信息，包括实例的创建时间，输出参数等。
资源关系	资源关系	支持显示实例拓扑，并显示实例下资源的详情和基本操作，并支持跳转到对应资源的 console 做更详细的操作。
资源列表	资源列表	支持查看 vApp 下所有资源的信息
事件列表	事件列表	支持查看 vApp 的事件列表，显示资源的部署，变更，删除等操作的记录。

2. PaaS 层服务能力

2.1 RDS 数据库服务

1、服务应用场景

随着大数据时代的到来，数据采集手段越来越丰富，企业的存量数据和增量数据越来越多，数据库系统运维管理的难度越来越大，成本越来越高。企业自建数据库需要综合考虑高可用方案、数据备份方案、业务峰值及数据增长趋势等因素，技术实施难度较大，所以虽然企业客户在数据库系统建设上投入了大量的人力与物力，但是效果却难以达到预期。

关系型数据库服务（Relational Database Service, RDS）以及 Oracle 数据库服务，是一种基于云计算平台的可即开即用、稳定可靠、按需扩展、便捷管理的在线关系型数据库服务。

数据库服务提供丰富的自助管理功能，以及完善的性能监控体系和多重安全防护措施，并提供专业的数据库管理平台，让企业用户能够在云中轻松设置、操作和扩展关系型数据库，简化运营流程，减少日常运维工作量，从而能够专注于应用开发和业务发展。

目前关系型数据库服务支持 MySQL、SQLServer、PostgreSQL、Oracle 多种类型和版本的常用关系数据库。

具体而言，数据库服务具有如下优点：

易用性

RDS 提供了基于 Web 的自助管理控制台，用户可以方便的进行实例快速发放和自助管理。

安全性

RDS 提供了全面灵活的访问控制，包括基于 VPC 发放实例、设置安全组，并对 RDS 的实例数据库和 OS 进行了安全加固，保证系统安全健壮。

高可靠性

RDS 以多种方式保证用户数据库实例的数据可靠以及服务可用，包括支持主备实例发放、支持数据库备份恢复。

2、服务架构

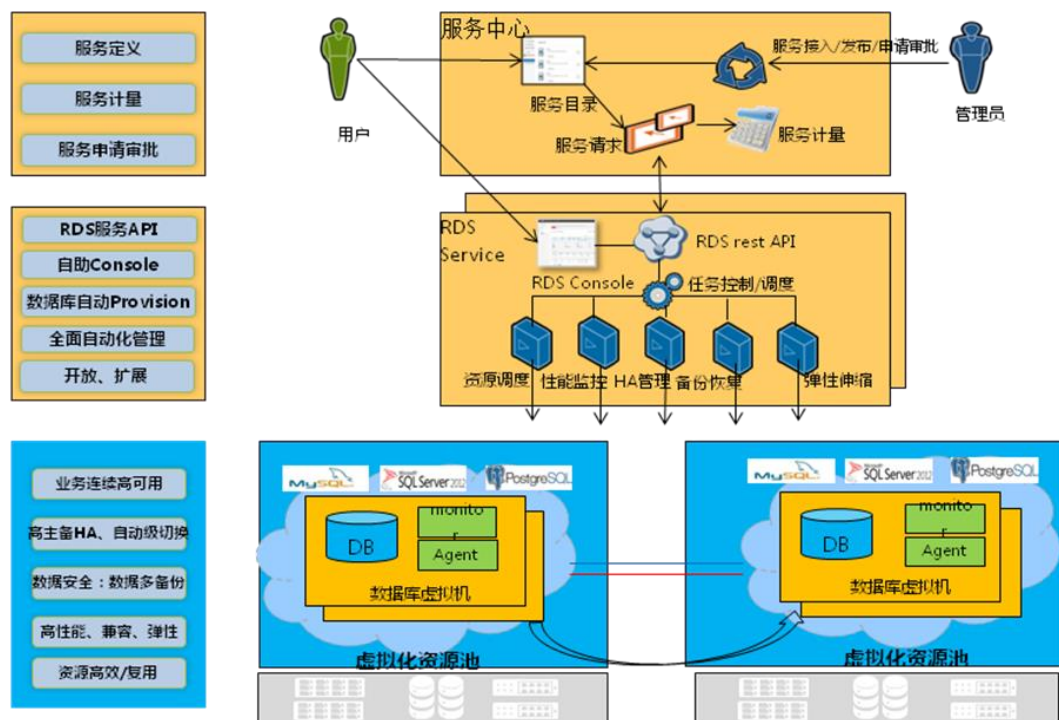


图 RDS 服务架构图

RDS 核心部件

RDS Console: 提供 RDS 服务自助申请和管理界面。

RDS Service: RDS 核心服务组件，实现自动化发放调度和自助管理能力，由 12 个微服务组件构成。

表 RDS 周边依赖组件

云主机 (ECS)	为 RDS 提供虚拟机，用来部署数据库实例
-----------	-----------------------

云硬盘 (EVS)	为 RDS 服务提供云硬盘，包括系统盘和数据盘
虚拟私有云 (VPC)	为 RDS 提供网络服务
镜像管理服务 (IMS)	为 RDS 的安装部署提供镜像
对象存储服务 (OBS)	为 RDS 提供备份存储
ManageOne 运营/运维	可以查看 RDS 实例的监控信息。
	提供 RDS 服务实例的操作记录，供用户查询、审计和回溯使用

3、RDS 服务能力

目前关系型数据库服务支持 MySQL、SQLServer、PostgreSQL、Oracle 多种类型和版本的常用关系数据库。

(1) RDS for MySQL 服务能力

服务申请管理

- 服务创建：支持创建 MySQL 实例；支持版本 MySQL 5.6 和 5.7；
- 服务状态查询：租户能从页面查看实例当前创建、删除的状态；
- 服务实例删除：支持租户删除服务实例；

服务实例管理

- 实例类型支持：支持部署 MySQL 单例、主备实例、只读副本；
- 实例规格修改：支持 MySQL 实例进行存储扩容；支持 MySQL 实例进行 CPU/内存的扩容、缩减；
- 实例重启：租户根据业务需要，在交互页面上操作，重启数据库实例；
- 实例列表显示：支持租户查看实例列表；
- 实例详情查询：支持租户查看实例详情，如数据库连接地址、规格等；
- 实例基本管理：包括实例端口修改、密码重置、存储使用率查看、数据库参数组设置、错误日志查看、慢日志查看；

- 支持为实例绑定 EIP，提供外网访问能力；

备份恢复

- 支持设置备份策略、自动备份、手动备份；
- 支持指定时间恢复数据库实例；
- 支持恢复到当前实例或恢复到新实例；

服务高可靠性管理

- 管控系统均通过双机主备部署保证可靠性，消除单点故障；
- 实例面支持高可靠主备数据库实例发放，支持数据备份和恢复；

服务监控管理

- 支持查看系统监控指标数据（CPU、内存、IOPS、数据连接数、QPS、TPS、InnoDB 指标等）；

数据库参数管理

- 支持查看数据库启动及运行时参数；
- 支持基于参数模板修改数据库参数；

日志管理

- 支持租户查询慢日志与错误日志，定位系统错误与性能问题；

(2) RDS for SQLServer 服务能力

服务申请管理

- 服务实例创建：用户创建 SQLServer 实例；支持版本 SQLServer 2014 SP2 SE、SQLServer 2014 SP2 EE；
- 服务状态查询：租户能从页面查看实例当前创建、删除的状态服务审批；
- 服务实例删除：支持租户删除 SQLServer 实例；

服务实例管理

- 实例类型支持：支持部署 SQLServer 单例；
- 实例规格修改：支持 SQLServer 实例的 CPU/内存的扩容、缩减；
- 实例重启：租户根据业务需要，在交互页面上操作，重启数据库实例；
- 实例列表显示：支持租户查看实例列表；
- 实例详情查询：支持租户查看实例详情；
- 实例基本管理：包括实例端口修改、密码重置、存储使用率查看、数据库参数组设置、日志查看；

- 支持为实例绑定 EIP，提供外网访问能力；

备份恢复

- 支持设置备份策略、自动备份、手动备份；
- 支持指定时间恢复数据库实例；

服务监控管理

- 支持查看操作系统和部分 SQLServer 实例监控指标数据；

数据库参数管理

- 支持查看数据库启动及运行时参数；
- 支持基于参数模板修改数据库参数；

日志管理

- 支持查询 SQLServer 运行日志，定位系统问题；

(3) RDS for PostgreSQL 服务能力

服务申请管理

- 服务实例创建：支持创建 PostgreSQL 实例；支持版本 PostgreSQL 9.5、9.6；支持 KVM 虚拟机；

- 服务状态查询：租户能从页面查看实例当前创建、删除的状态；
- 服务实例删除：支持租户删除 RDS 实例；

服务实例管理

- 实例类型支持：支持部署 RDS 单例、主备实例、只读副本；
- 实例规格修改：支持 RDS 实例进行存储扩容；支持 RDS 实例进行 CPU/内存的扩容、缩减；
- 实例重启：租户根据业务需要，在交互页面上操作，重启数据库实例；
- 实例列表显示：支持租户查看实例列表；
- 实例详情查询：支持租户查看实例详情，如数据库连接地址、规格等；
- 实例基本管理：包括实例端口修改、密码重置、存储使用率查看、数据库参数组设置、错误日志查看、慢日志查看；

- 支持为实例绑定 EIP，提供外网访问能力；

备份恢复

- 支持设置备份策略、自动备份、手动备份；
- 支持指定时间恢复数据库实例；

服务高可靠性管理

- 管控系统均通过双机主备部署保证可靠性，消除单点故障；
- 实例面支持高可靠主备数据库实例发放，支持数据备份和恢复；

服务监控管理

- 支持查看系统监控指标数据（CPU、内存、IOPS、数据连接数、QPS、TPS 指标等）；

数据库参数管理：

- 支持查看数据库启动及运行时参数
- 支持基于参数模板修改数据库参数；

日志管理：

- 支持租户查询错误日志，定位系统错误；

（4）Oracle 服务

资源池管理

- 支持资源池定义功能，将不同版本或地域的集群放到不同资源池。

主机/集群管理

- 提供 Oracle RAC 集群和物理主机添加和管理功能，包括查看集群进程、资源等信息。

- 支持管理 Oracle 12.1 和 12.2 版本。

CDB 实例管理

- 提供 CDB 实例创建和管理功能，包括查看配置参数、性能等信息。

PDB 实例管理

- 支持 PDB 实例发放和自助管理。
- 支持启停数据库、修改密码等操作。
- 支持查看数据库 Alert 日志。

备份恢复管理

- 支持 CDB 级别的备份策略设置和自动备份。
- 支持 PDB 级别的数据库恢复功能。
- 支持指定时间恢复。

性能监控

- 支持数据库实例常见数据库监控指标的查看。

表空间管理

- 支持租户为 PDB 数据库创建表空间。

- 支持为表空间添加数据文件。
- 用户管理
- 支持 PDB 数据库创建用户。
- 支持管理数据库用户权限。

2.2 DRS 数据迁移服务

1、服务应用场景

在云上创建数据库后,用户经常面临云下数据库迁移上云的场景。通过 DRS,用户能够简单、便捷地完成数据库迁移上云。

在迁移过程中, DRS 能够最大限度地缩短业务系统中断时间,降低对业务影响。

2、服务架构

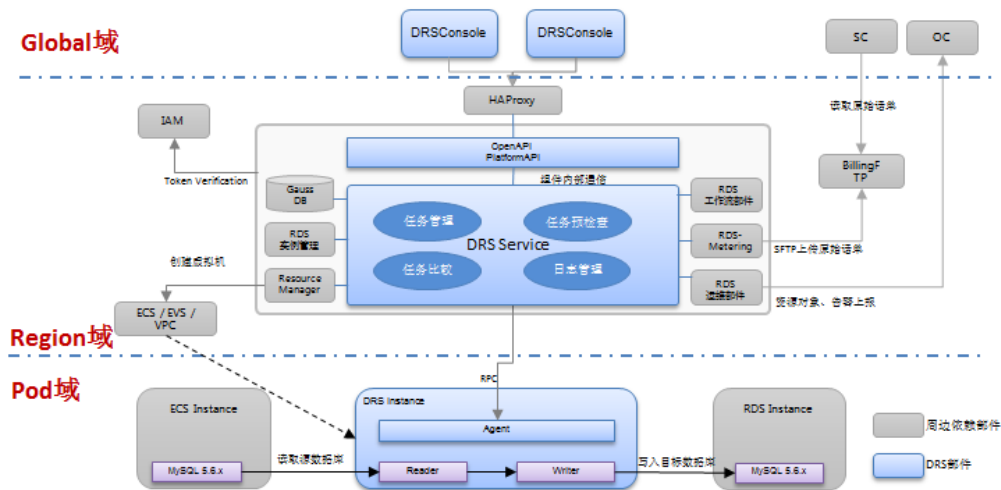


图 DRS 服务架构图

关键部件包括：

DRS Console: DRS 的 Web 用户自助管理控制台，用户在此输入需要迁移的场景类型、源数据库的连接信息、目标数据库的连接信息和迁移类型等信息。

OpenAPI、PlatformAPI: DRS 的 API 服务，负责处理 DRS console 的所有请求，通过调用 DRS Service 等组件对请求进行处理后，返回 DRS console 需要的信息，并将用户的主要操作记录到云审计系统。

DRS Service: DRS 后台服务，负责创建迁移任务、迁移前的预校验、迁移数据对比、创建迁移引擎、迁移日志处理等。

DRS Instance: 负责将源数据库的数据库迁移到目标数据库，并记录迁移过程中的状态变化和日志信息，上报给 DRS Service。

Resource Manager: DBS 提供的资源管理组件，用于封装 IaaS 各种资源的 API 接口，为 DBS 各系统提供统一的资源服务。

ECS/EVS/VPC: DRS 依赖的 IaaS+云服务，为用户提供可弹性申请的计算、存储和网络资源，RDS 需要从这些服务申请资源作为数据库实例的运行环境。

源数据库: 用户的源数据库，可以是用户在 ECS 上的自建数据库或者是用户在自己本地数据中心的数据库。

目标 RDS 实例: 作为迁移目标的 RDS instance。

3、服务能力

DRS 服务支持的功能特性如下：

支持 MySQL 数据库迁移

- 支持 ECS 自建 MySQL 数据库和本地数据中心的 MySQL 数据库迁移至 RDS。

支持 MySQL 数据库全量迁移

- 全量迁移将非系统数据库的全部数据库对象和数据，一次性迁移至目标端数据库，包括：表、视图、存储过程和触发器等。适用于可中断业务的数据库迁移场景。

支持 MySQL 数据库增量迁移

- 增量迁移将默认包含全量迁移，全量迁移完成目标端数据库的初始化后，增量迁移通过捕抓日志和应用日志等技术，保持源数据库和目标数据库数据持续一致。适用于对业务中断敏感的场景。

支持迁移任务预校验

- 支持迁移执行前进行自动迁移校验，并界面显示迁移满足和不满足项校验结果

支持查看迁移进度：

- 可查看到源数据库迁移表单的个数，和目标数据库已完成的表单数

支持迁移失败重试

- 迁移失败的任务，可单击“重试”，重新提交迁移任务

查看迁移任务中产生的迁移日志

- 支持查看迁移任务中产生的迁移日志

支持对比源数据库和目标数据库的迁移项

- 可查看到源数据库和目标数据库，对比项的对比结果和详情

2.3 API 网关服务

1、服务应用场景

API 网关是大型分布式系统中为了保护内部服务而设计的安全服务，可以提供高性能、高可用的 API 托管服务，从而帮助服务的开发者便捷地对外提供服务，而不用考虑安全控制、流量控制等问题，统一在网关层将安全认证，流量控制，黑白名单等实现。客户端的所有请求都首先经过 API 网关，然后由它将请求路由到合适的后端服务。API 网关负责服务请求路由、组合及协议转换。API 网关可以通过调用多个后端服务并合并结果来处理一个请求。它可以在 Web 协议（如 HTTP 与 WebSocket）与内部使用的非 Web 友好协议之间转换。服务开发者重点在开发和关注具体业务相关的实现。

2、服务架构

API 网关面向公司内外部的 API 开发者，提供简单、高效、安全、稳定的业务接入平台，并提供基本的管理功能，使之能对使用 API 的应用进行管理和统计。系统架构图如下：

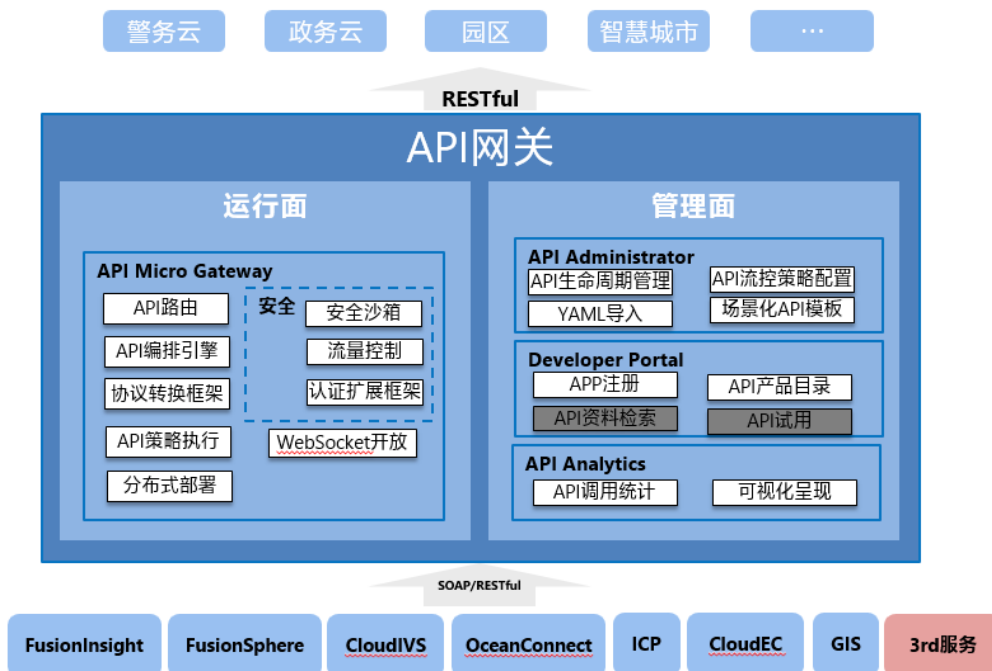


图 API 网关架构图

API Micro Gateway: 为企业应用访问 API 提供统一入口，提供 API 转发、API 流控、API 访问鉴权等功能。

API Administrator: 提供给 API 开发人员自助创建、测试、发布 API 的能力。

Developer Portal: 提供应用开发者获取和访问 API 目录的入口。

API Analytics: 提供 API 管理员了解和分析 API 使用情况及数字资产的应用情况。

注：上图中深灰色模块目前处于规划状态。

3、API 网关服务能力

支持高性能可扩展的 API 调用转发

支持 API 级联转发

支持 RESTful、SOAP 协议对外开放 API

支持后端服务以 RESTful、SOAP 或自定义协议（基于 TCP/IP）协议接入

支持后端服务与 API 之间透传、编排的路由和转发

支持多种访问 API 的认证方式（不认证、APPKey 认证、APPToken 认证、Basic 认证、APIKey 认证或自定义认证）

支持后端服务多种认证接入（不认证、Basic 认证、PublicKey 认证）

支持系统级和 API 级的黑白名单

支持通过安全沙箱运行第三方编排代码

支持 API 访问流量控制（共享配额、独占配额）

支持基于应用的 API 访问配额控制

支持应用访问配额控制

支持导入 OpenAPI 2.0 规范的 Yaml 文件创建 API

支持 API 配置的导入与导出

支持基础编排能力，将 Backend 的多个 API 在编排引擎中完成接口间的逻辑聚合，对外呈现为一个接口

支持增加自定义脚本节点或 Mediator 对消息内容进行复杂加工

支持 API 生命周期管理，支持 API 的发布、废弃、下线、删除、版本另存为、替换等管理

支持微网关的节点发现、状态监控、节点维护、API 产品部署情况展示等功能

支持后端服务管理，配置多个服务实例地址，并采用加权轮询算法进行分配

提供 API 产品、API、流控配置的管理面 API 开放

支持应用生命周期管理

支持应用订阅 API 产品

支持应用权限管理

提供 API 目录，可检索 API，API 文档在线查看，API 全访问路径 (URL)

支持 API 调测

支持 API 产品、API、API 操作粒度的 API 调用情况统计

支持 AppToken 参数配置 (密钥更新、AccessToken 和 RefreshToken 的有效时长)，系统最大可管理的应用、API 数量配置

支持对系统日志级别进行动态配置

2.4 分布式消息中间件

消息中间件用于应用间的消息高可靠传输及交换，基于高可用分布式集群技术，支持高可靠机制和死信处理机制，支持 RESTful 消息访问 API，支持集群节点弹性伸缩。适应云化场景，在租户使用 Topic 数量增加时可动态扩展。

消息中间件功能如下：

HTTP 协议的支持：支持 HTTP RESTful 开放接口，HTTP RESTful 接口支持多语言访问接入。提供 AK/SK、Token 安全认证机制；

支持发布订阅模型；支持多种队列类型，包括普通队列、顺序队列；

提供 WEB 管理界面，可以创建和管理各种类型的消息队列，并同时提供管理 API 接口；

RESTful 接口提供消费长轮询机制，保证消费消息时的实时性；RESTful 接口提供消费重置功能，用户可以自定义消费位置；RESTful 接口支持死信开关，将多次消费失败的消息放进死信队列，不阻塞消息正常消费，同时消息不丢失；

提供完善的多用户隔离机制，保障用户数据的私密性；

提供队列访问认证和授权机制，防止非法访问；

消息队列数据采用 3 份副本机制和冗余可靠存储，允许任一个副本故障不影响业务，数据可靠性不低于 99.9999%；

支持大规模分布式集群架构，无单点故障，服务可用性不低于 99.9%；

支持可扩展能力，支持扩容满足业务增长要求。

2.5 分布式缓存中间件

缓存中间件提供云化的缓存服务，在 Redis 基础上做了优化和扩展，增强运维及安全特性，并且在部署，监控，安全防护，管理维护提供关键能力,缓存中间件提供以下功能：

主备透明 HA 能力:利用数据持久化和数据复制机制实现主备 HA 模式，并支持故障自动迁移，对应用透明；

Cloud-Native 服务:完全云化的原生云服务，有别于传统的组件化使用，按需发放和使用；

数据备份恢复:对接外部 SFTP 存储服务（需要客户自己提供 SFTP 服务器），可自动或手动进行数据的备份，不担心出现故障时数据全部丢失问题；

云监控和告警:无缝集成 Paas APM 系统，面向租户第一时间呈现多种系统级、实例级的指标，随时查看 Redis 的运行情况；

即开即用:用户直接操作 Web 控制台即可申请 DCS 服务，快速部署无需亲自部署相关的硬件及软件；

支持管理 API:提供开放的基于 HTTPs 的管理 API，比如：用户可以通过远程 API 调用启动/停止缓存服务实例,详细 API 接口请参考华为云 Stack 6.5.1 API 参考；

丰富的缓存规格:支持 2GB 到 64G 的单机/主备实例，64G 到 512GB 的集群实例等容量大小，灵活满足应用的多样化需求；

数据持久化:主备、集群模式下开启数据持久化功能，在提供高性能数据读写的同时，保证数据的可靠性；

易维护:功能完整的监控、告警机制，提供丰富的服务监控指标(比如，key 的数据，客户端连接个数，处理过的命令数据等)，以及系统监控指标(比如内存，CPU，网络的使用率)；

集群在线水平扩容:集群模式下支持在线不影响业务的情况下，水平扩容；

2.6 分布式事务中间件

华为 FusionStage 分布式事务中间件(Distributed Transaction Middleware, 简称 DTM), 是一款用于解决分布式环境下事务一致性问题的中间件产品。

DTM 当前支持 TCC(Try-Confirm-Cancel)事务模型, 提供了以注解的方式定义事务信息, 实现高效且便捷接入。同时, DTM 提供处理高并发事务处理能力, 支持自动部署、高可用等全生命周期运维管控能力。包括以下主要功能:

提供 TCC 分布式事务管理能力。

提供 SDK 供用户二次开发使用, 客户端通过注解的方式声明事务信息, 支持动态配置, 服务发现, 连接注册, 负载均衡等能力

支持二阶段推进时同步异步可配置, 延时回调, 推进时 failover (仅应用离线) 等。

支持正常提交, 异常回滚, 超时回滚, 超时回查, 永不超时等场景, 支持事务超时上报事件, 永不超时场景长时间未推进上报告警等。

提供服务端集群模式, 支持集群间相互接管客户端请求能力, 服务端优雅退出。

控制台页面提供活跃事务, 历史事务, 事件告警, 配置修改等功能。

支持客户端配置查询及修改功能。

提供数据库连接异常告警, 数据库同步异常告警, etcd 连接异常告警等

2.7 CPE 服务

CPE (Cloud Pipeline Engine) 为基于 PaaS 平台的开发流水线引擎, 基于一组开源/商用的工具提供从源码管理, 构建到部署等各个研发环节的自动化工具链, 从而提供端到端的 DevOps 的能力, 功能如下:

流水线编排调度

多种部署方式

Jenkins 能力增强

端到端工具链最佳实践

2.8 容器管理

1、容器基础设施

PaaS 容器基础设施作为 PaaS 平台中的底座，为应用开发者提供一个简单易用、高效稳定的资源调度管理平台。

PaaS 容器基础设施主要管理用于托管应用的资源池，支持虚拟机不同类型计算资源，支持不同网络环境，支持静态资源纳管与动态资源创建等。

(1) 主机资源管理

PaaS 平台以应用为中心，进行统一资源管理和调度，支持虚拟机等计算资源，提供统一的网络、存储等服务；

PaaS 平台可以根据 IP 地址手动添加虚拟机资源节点；也可以批量导入虚拟机资源节点；

PaaS 平台可以与 IaaS 对接，通过选择虚拟机节点规格（包括 CPU、内存等）和数量，自动添加虚拟机节点资源。

PaaS 平台提供对主机节点的完善管理功能，可以方便直观的获取主机监控信息以及容器信息等。

为避免单一租户过量占用资源，提高资源利用率，PaaS 平台在租户层级，可以对每个租户设置资源配额，比如可供使用的节点数量、CPU、内存等资源。

PaaS 平台主机支持打标签功能，定义和分类主机，配合后续调度选择。

(2) 容器网络管理

随着容器集群规模不断增大，容器数量不断增长，这就要求容器网络能提供高性能的跨节点通信能力、更大规模的容器网络以及更快的单容器发放性能。

PaaS 平台容器网络为应用提供各种网络平面、组网模式和节点间的容器网络互通和隔离。具体包括：

支持 overlay 组网；

支持容器和虚拟机网络互通；

支持 ClusterIP、NodeIP、LoadBalance 等多种应用访问方式。

(3) 容器存储管理

容器支持本地存储，提供 hostPath、emptyDir、secret、configMap 四种类型本地存储。

面向大量有状态应用容器化改造诉求，需要支持容器持久卷存储和共享存储，PaaS 平台支持对接容器存储，具体内容如下：

应用依赖持久数据卷，需要容器支持持久化卷存储；

支持自动化分配存储资源池资源；

支持对接 NFS 存储（用户的 NFS Server），允许多容器共享；

支持存储生命周期基本操作（创建、修改、删除、挂载、卸载等）。

2、应用编排建模

PaaS 平台能够为各种类型的应用（有状态、无状态等）选取合适的资源进行安装部署，并支持运行时管理操作如配置、更新、升级、卸载等。

提供多种编排模型：TOSCA 模型、Helm 模型；

支持容器应用编排；

支持资源编排，包括虚 IP、VM、Port、Volume 等；

提供图形化设计器，方便用户以拖拉拽的方式进行应用组、应用、服务、资源的图形化编排；

支持无状态应用、有状态应用、短任务的编排部署；

支持堆栈的启动、部署、升级、弹缩、卸载等生命周期管理。

3、应用管理

支持无状态应用、有状态应用、短任务创建部署；

支持手工式和向导式创建发布应用；

支持应用的创建、升级、删除等生命周期管理；

支持应用配置的添加、删除、修改等统一配置管理。

4、应用调度管理

（1）应用调度策略

在 PaaS 平台中，用户通过使用容器的调度策略，可以为容器运行选择最优节点。PaaS 平台提供与应用相关的多种调度策略：

应用间的亲和/反亲和性调度：将不同的应用调度部署在相同或不同节点中。

应用与节点的亲和/反亲和性调度：将应用调度部署到指定标签的或与指定不同标签的节点中。

（2）应用升级与发布

无论是传统的单体应用还是基于互联网架构的新应用，都无可避免的面临升级问题。而臃肿的单体应用架构，由于代码基线大，依赖错综复杂，导致升级过程要投入大量人力与时间，升级过程中甚至会中断服务。

PaaS 平台应支持对传统应用进行改造，对改造后的应用和新应用支持替换升级、原地滚动升级、滚动升级，并提供完善的应用滚动升级支持：

- 按比例进行滚动升级；
- 按实例个数进行滚动升级；
- 按步长进行滚动升级；
- 支持有状态容器应用的升级。

PaaS 平台同时应支持应用的灰度发布，支持应用的优雅缩容，保证业务不中断。

（3）应用弹性伸缩

在实际应用中，我们可能会遇到某个服务需要扩容或缩容的场景，PaaS 平台应提供多种弹性伸缩的策略：

自动弹性伸缩模式：组件负载满足预先配置的平台组件自动伸缩策略，根据应用负载程度以及用户配置的伸缩策略，实现应用实例的自动扩缩容，并自动完成负载均衡的调整，过程中需确保业务会话不中断。弹性伸缩的规则包括：

- 策略指标应包含 CPU、内存、磁盘、网络等指标；
- 策略指标应包含基于时间的规则，包括周期弹缩和定时弹缩；
- 策略指标应包括用户自定义 KPI 指标。

手动弹性伸缩模式：用户手动确认弹性伸缩的实例数并执行。

（4）健康检查与异常恢复

PaaS 提供周期性监控检查和异常恢复机制，具体如下：

PaaS 平台在应用运行过程中，根据用户需要定时检查容器健康状况或是容器中应用的健康状况，支持容器自定义监控检查；

根据健康检查结果决定启动/删除对应实例。如果检查失败，平台将删除该应用实例，然后根据应用的重启策略来决定是否重启容器。

（5）D 卡类应用调度

支持容器调度使用升腾 310 加速资源，包括：

支持 1 个 GPU 对应的一个容器；

支持多个 GPU 对应 1 个容器；

(6) GPU 类应用调度

支持容器调度使用 P4,P40,P100,V100 四种类型的 GPU 资源(GPU、驱动和工具包需由客户自行提供)，包括：

支持 1 个 GPU 对应 1 个容器；

支持多个 GPU 对应 1 个容器；

支持多个容器按百分比共享 1 个 GPU。

5、多租户与项目管理

PaaS 平台需建立完善的多租管理模型和租户的资源配额管理，严格实现多租户资源/服务的安全隔离。通过用户组、用户和权限对各个租户集群的安全性进行隔离和控制。

PaaS 平台提供用户的统一身份认证管理，建立支持基于角色和基于属性的分布式授权检查，建立了最终租户与服务租户的信任授权，并基于配额管理实现应用/服务部署的准入控制。具体如下：

支持用户、组、角色的管理：支持租户下用户的注册和审批，激活或驳回用户；支持用户组的管理；支持角色的创建和管理；支持域/项目，用户组和角色的绑定；

支持多租户管理：支持租户的注册和审批，激活或驳回租户的注册申请；支持租户下的项目的创建；支持租户下的用户管理；

支持资源隔离：支持基于项目空间的资源隔离机制；支持项目空间的节点、实例、CPU 和内存的配额管理；

支持子系统基于操作的权限管理和配置：支持基于角色的对资源访问的细粒度授权控制；支持基于租户和角色的资源访问控制策略的配置；

6、软件仓库

(1) 多类型软件仓库

PaaS 平台的软件仓库提供两种类型软件的上传下载，分别是：容器镜像仓库和软件包仓库。

(2) 仓库权限控制

PaaS 平台的仓库分为公有仓库和私有仓库两种形式：

私有仓库：提供私有镜像或软件包管理功能，其中镜像或软件包只能被有权限用户看到和访问；

公有仓库：提供公有镜像或软件包管理功能，其中镜像或软件包可被系统所有用户都可看到和访问。

（3）镜像仓库管理

PaaS 平台能够提供对应用镜像进行统一管理，内容包括镜像文件路径、镜像名称、版本、类型等信息。并提供应用镜像规范的参考模型和流程指导。主要功能要求应包括：

支持私有、公有镜像仓库的创建、更新、查询、删除等；

支持镜像包签名管理；

支持镜像仓库私有和公有属性变更。

（4）软件仓库管理

PaaS 平台针对软件仓库提供以下功能：

私有、公有软件仓库的创建、更新、查询、删除等（二进制软件包、Blueprints 包、Helm charts 包等）；

支持软件包签名，支持软件仓库私有和公共属性变更；

支持上传时解压存储，支持存储目录管理。

7、镜像自动构建

原生镜像构建，需要在命令行下执行容器构建命令进行，操作不变。容器平台提供了 S2I 和 B2I 工具，通过界面化的镜像构建，简化打包操作：

S2I（Source2Image）工具：用户可通过基于 `dockerfile` 标准描述，完成从源码到容器镜像的自动构建。使用者通过把源代码仓库(SVN)的账户信息托管给容器平台，实现 S2I 工具可自动拉取源码和构建镜像。

B2I（Binary2Image）工具：用户可通过基于 `dockerfile` 标准描述，完成从二进制到容器镜像的自动构建。

2.9 微服务云管理

微服务架构是一种旨在通过将功能分解到各个离散的服务中以实现解决方案的解耦。不同于传统架构模式，微服务化就是以一系列小的服务来开发支撑一个应用的方法论，服务独立在自己的进程中，通过轻量级通信机制交互。这些服务是围绕着业务上的组织结构来构建的，全自动的、独立部署，几乎看不到中

心化的服务管理基础设施，可以使用不同的编程语言和数据存储技术来实现不同的服务。

华为 PaaS 平台 FusionStage 的微服务运行与治理框架提供完备的微服务运行与治理能力，并秉承开放的原则，兼容业界主流的其他微服务框架。

1、微服务开发

(1) 微服务开发框架

支持微服务的 War 包、jar 包等多种打成方式。

支持采用 SpringMVC、JAX-RS、透明 RPC 风格的注解方式开发微服务。

支持对微服务进行初始化配置，包括支持的配置项和配置方式。

支持一键自动生成微服务开发框架，帮助客户实现契约文件、接口定义、框架代码等生成。

(2) 多语言与多框架支持

不同的微服务应采用最合适的编程语言和开发框架开发，在一个微服务应用中可能会存在多种不同语言开发的微服务。平台本身提供多语言开发微服务的能力：

提供开发 SDK，根据提供的 SDK 进行微服务开发；

支持 Java、Go 等多种语言开发微服务，支持跨语言微服务之间相互调用；

提供 Spring Cloud 开源微服务接入工具，可以实现简单配置快速接入。

(3) 多运行容器支持

支持基于 JVM 独立运行（将服务打包成 jar 直接在 JVM 运行）。

支持 Tomcat、Jboss 等多种应用服务器运行。

支持虚拟机、容器多种资源类型运行微服务。

(4) 微服务间调用访问

由于微服务的“微”，一个完整的业务调用需要大量的微服务协同才能完成，存在较多的网络通信。PaaS 平台提供多种服务通信协议。

支持 Restful 通信协议；

支持 RPC 通信协议；

支持客户以插件方式接入自研或特定领域通信协议。

(5) 分布式事务

支持对接分布式事务组件 DTM，实现微服务间的最终一致性。

2、Mesher 接入

微服务运行与治理框架兼容 Spring Cloud 开源应用生态，基于 Spring Cloud 构建的应用只需少量改造即可接入微服务开发与运行框架。

存量服务通过 Mesher 快速接入微服务，只需完成应用和 Mesher 的部署，应用即可通过 Mesher 自动接入到微服务治理框架。应用代码“零”侵入，天级改造接入。可实现 NodeJS、.NET 等其他语言应用快速接入 CSE 微服务框架，实现微服务化。

3、微服务部署

(1) 与容器平台结合

微服务要能够和主流 Kubernetes 容器平台结合，基于 Kubernetes 部署云原生微服务应用，具体要求包括：

天然与 Kubernetes 容器平台融合，微服务可部署到 K8S 上进行生命周期管理；

支持通过图形化编排对复杂微服务进行建模；

支持一个应用不同微服务对象部署到容器或者虚机的混合环境；

(2) 生命周期管理

微服务生命周期管理具体要求包括：

支持微服务的启用、升级、停止、下线、删除等生命周期管理。

支持按照弹性伸缩策略增加或减少微服务实例。

支持权重比例、特定业务字段等配置灰度发布规则，对新老版本的微服务进行分流。

支持通过界面查看微服务列表及概要信息，支持进行微服务分组管理。

支持服务契约的在线查看，对于隐式服务契约的微服务支持服务契约的自动生成。

4、微服务治理

(1) 微服务基础治理

1) 微服务注册发现

微服务注册发现是实现分布式服务自动注册与发现的功能，即允许所有应用在本平台中自动注册自己作为服务，并可通过网络名称彼此发现的能力。

具体要求如下：

支持容器在本平台中自动注册自己作为服务，并可通过网络名称彼此发现的能力；

支持设置心跳监测监控微服务状态；

支持服务消费方按照服务名进行订阅推送；

支持微服务消费者可以自动发现微服务提供者；

2) 负载均衡

支持基于客户端的负载均衡机制访问多个微服务实例。

3) 边缘网关

通过边缘微服务或适配器对外开放微服务，使外部客户端可以访问内部微服务。用于路由分发、流量控制、认证鉴权（需用户扩展实现）等。

4) 依赖管理

支持通过列表式或者拓扑关系图展现微服务之间的依赖关系。

5) 微服务安全管理

支持微服务按照租户、项目进行访问认证管理和隔离机制。

针对静态服务信息进行屏蔽，只允许某些特定的服务查询实例信息（白名单），或只屏蔽某些特定服务查询服务实例（黑名单）。

支持 **Https** 协议的 **SSL** 安全链路加密访问方式。

(2) 微服务高可用治理

1) 支持服务降级

每一个应用会调用许多外部服务。对于这些服务，可以配置降级规则，实现对劣质服务的精准屏蔽，确保应用自身能够稳定运行，避免由于依赖的服务质量劣化，影响了应用自身的服务能力。

支持按服务粒度降级；

支持按接口粒度降级；

支持手工降级；

支持自动降级。

2) 支持服务限流

每一个应用都会提供很多服务。对于这些服务，可以配置限流规则以实现对服务的流控，确保服务能够稳定运行，拒绝超出服务能力的流量。

支持按服务提供端限流；

支持按服务消费端限流。

3) 支持服务熔断

熔断是一种异常反应机制，通常基于错误率来实现。当超过一定错误率阈值可自动屏蔽请求，若恢复正常可解除熔断状态。

支持按服务粒度熔断；

支持按接口粒度熔断；

支持按错误率策略自动熔断。

4) 支持服务容错

容错是一种异常处理机制，“容错”依赖于“熔断”。熔断以后，会调用“容错”的方法。支持多种服务容错策略。

failover: 当容错策略配置为 **failover** 时，失败后自动切换其他服务器，支持配置重试次数；

failfast: 当容错策略配置为 **failfast** 时，失败立即报错，不再重试；

failresend: 容错策略配置为 **failresend** 时，将失败消息放入缓存队列。

5) 支持故障隔离

支持对故障微服务实例的检测和隔离。错误率超过阈值时，系统自动隔离实例，不再向故障实例发起新的调用。

5、微服务运维

(1) 微服务监控告警

支持对具体微服务的运行状态进行监控，支持通过微服务仪表盘对进行整体监控管理。

支持查看具体微服务的运行日志信息。

支持通过监控指标自定义告警阈值规则，当超过阈值自动触发告警。

支持微服务之间的依赖关系及拓扑呈现。

(2) 服务调用链跟踪

支持 Web 界面展示分布式系统调用链路各个阶段的时延信息；

支持按照调用链要求埋点，系统根据这些埋点信息进行 KPI 统计。

2.10 云服务市场

1、多种服务集成

支持客户存量服务、合作伙伴等第三方服务集成 PaaS 平台；

支持业务应用、中间件、数据库服务集成 PaaS 平台；

支持托管方式服务集成，服务通过容器平台部署、实例发放、弹性伸缩等生命周期管理；

支持非托管方式服务集成，服务部署在云平台之外，由服务提供者自行进行服务管理；

2、服务集成发布

对服务提供者：提供服务的发布审批、服务生命周期管理（更新、下架、删除）；

服务发布：支持页面向导式、YML 脚本方式发布服务，支持服务与应用的绑定与解绑定，支持指定服务依赖关系、自定义参数等服务发布管理；

3、服务目录管控

支持通过服务市场进行服务目录展示、分类、管理；

支持服务实例详细信息的展示；

4、服务订阅消费

对服务使用者：提供服务实例的订购审批、服务实例生命周期管理（更新、删除）；

服务消费：全自助式服务申请、发放和释放；

多租方式：支持物理多租和逻辑多租方式的服务实例订购；

2.11 SaaS 服务能力

按照定义，此部分内容由 ISV 合作伙伴开发。

3. FusionInsight HD 大数据服务能力

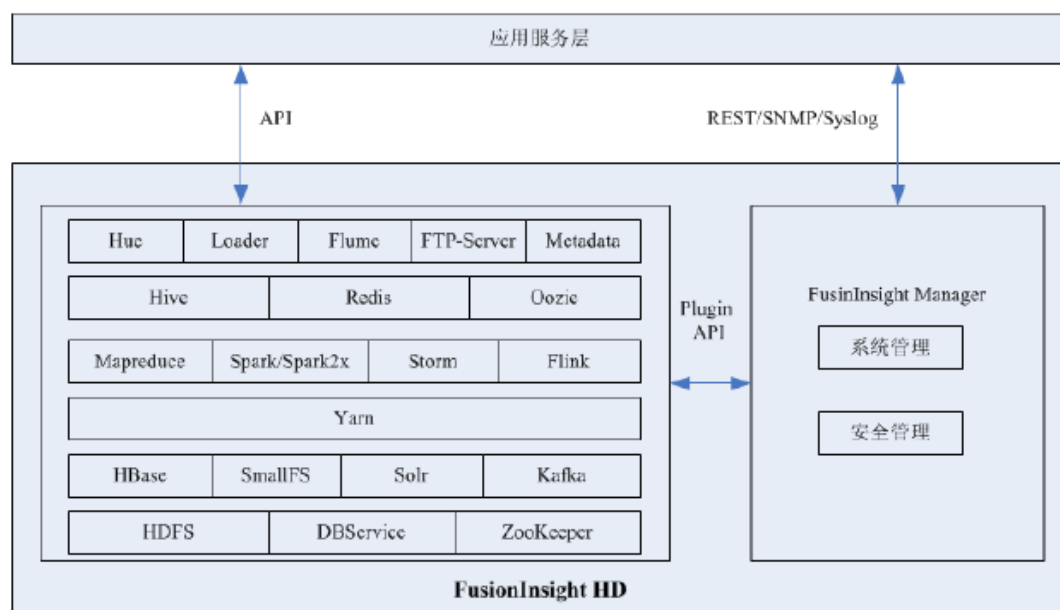


图 逻辑架构图

FusionInsight HD 对开源组件进行封装和增强，包含 Manager 和众多组件，分别提供功能如下：

Manager

作为运维系统，为 FusionInsight HD 提供高可靠、安全、容错、易用的集群管理能力，支持大规模集群的安装部署、监控、告警、用户管理、权限管理、审计、服务管理、健康检查、问题定位、升级和补丁等。

Hue

提供了 FusionInsight HD 应用的图形化用户 Web 界面。Hue 支持展示多种组件，目前支持 HDFS、Hive、YARN/MapReduce、Oozie、Solr、ZooKeeper 和 Spark。

Loader

实现 FusionInsight HD 与关系型数据库、文件系统之间交换数据和文件的数据加载工具；同时提供 REST API 接口，供第三方调度平台调用。

Flume

一个分布式、可靠和高可用的海量日志聚合系统，支持在系统中定制各类数据发送方，用于收集数据；同时，Flume 提供对数据进行简单处理，并写入各种数据接受方（可定制）的能力。

FTP-Server

通过通用的 FTP 客户端、传输协议提供对 HDFS 文件系统进行基本的操作，例如：文件上传、文件下载、目录查看、目录创建、目录删除、文件权限修改等。

Hive

建立在 Hadoop 基础上的开源的数据仓库，提供类似 SQL 的 Hive Query Language 语言操作结构化数据存储服务和基本的数据分析服务。

Mapreduce

提供快速并行处理大量数据的能力，是一种分布式数据处理模式和执行环境。

Storm

提供分布式、高性能、高可靠、容错的实时计算平台，可以对海量数据进行实时处理。CQL（Continuous Query Language）提供的类 SQL 流处理语言，可以快速进行业务开发，缩短业务上线时间。

Spark

基于内存进行计算的分布式计算框架。

Solr

一个高性能，基于 Lucene 的全文检索服务器。Solr 对 Lucene 进行了扩展，提供了比 Lucene 更为丰富的查询语言，同时实现了可配置、可扩展，并对查询性能进行了优化，并且提供了一个完善的功能管理界面，是一款非常优秀的全文检索引擎。

Oozie

提供了对开源 Hadoop 组件的任务编排、执行的功能。以 Java Web 应用程序的形式运行在 Java servlet 容器（如：Tomcat）中，并使用数据库来存储 workflow 定义、当前运行的 workflow 实例（含实例的状态和变量）。

Redis

一个开源的、高性能的 key-value 分布式存储数据库，支持丰富的数据类型，弥补了 memcached 这类 key-value 存储的不足，满足实时的高并发需求。

Kafka

一个分布式的、分区的、多副本的实时消息发布和订阅系统。提供可扩展、高吞吐、低延迟、高可靠的消息分发服务。

Yarn

资源管理系统，它是一个通用的资源模块，可以为各类应用程序进行资源管理和调度。

HDFS

Hadoop 分布式文件系统 (Hadoop Distributed File System), 提供高吞吐量的数据访问, 适合大规模数据集方面的应用。

SmallFS

提供小文件后台合并功能, 能够自动发现系统中的小文件(通过文件大小阈值判断), 在闲时进行合并, 并把元数据存储到本地的 LevelDB 中, 来降低 NameNode 压力, 同时提供新的 FileSystem 接口, 让用户能够透明的对这些小文件进行访问。

DBService

一个具备高可靠性的传统关系型数据库, 为 Hive、Hue、Spark 组件提供元数据存储服务。

HBase

提供海量数据存储功能, 是一种构建在 HDFS 之上的分布式、面向列的存储系统。

ZooKeeper

提供分布式、高可用性的协调服务能力。帮助系统避免单点故障, 从而建立可靠的应用程序。

Metadata

为数据仓库类型的组件 (Hive 和 HBase) 提供元数据的抽取能力, 并且可以人工为每个元数据进行标签设定, 用于后向的数据分析、搜索等扩展功能。

Flink

一个批处理和流处理结合的统一计算框架, 提供数据分发以及并行化计算的流数据处理引擎。

Spark2x

基于内存进行计算的分布式计算框架。

3.1 交互式查询

交互查询, 通常是指对数据进行交互式的分析和查询, 查询响应要求较高, 能够实现人机之间交互, 查询通常比较复杂。交互查询的数据通常已经被预处理过, 按照适合交互查询的数据模型进行组织。交互查询数据量巨大, 对 CPU 和内存要求很高, 对于存储要求也很高。交互查询, 以复杂 SQL 查询最为常见, 多维 Cube 分析也比较常见。

典型特点：

查询相应时间要求较高，3 秒内

处理数据量巨大，百 TB 级

SQL 支持度要求高，达到数据库水平

支持数据更新和插入

多种查询并发，容易产生资源抢占

支持第三方展现和报表工具

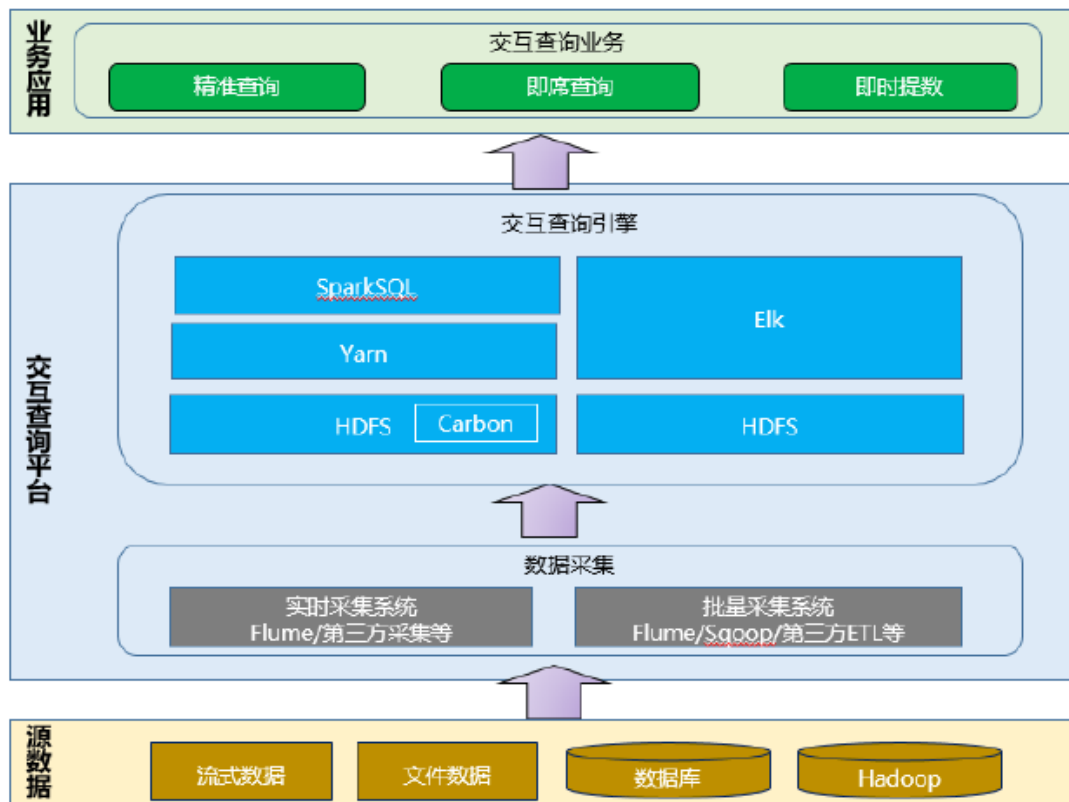


图 业务流程图

3.2 离线处理

离线处理，通常是指对海量数据进分析和处理，形成结果数据，供下一步数据应用使用。离线处理对处理时间要求不高，但是所处理数据量较大，占用计算存储资源较多，通常通过 MR 或者 Spark 作业或者 SQL 作业实现。

典型特点：

处理时间要求不高

处理数据量巨大，PB 级

处理数据格式多样

- 多个作业调度复杂
- 占用计算存储资源多
- 支持 SQL 类作业和自定义作业
- 容易产生资源抢占

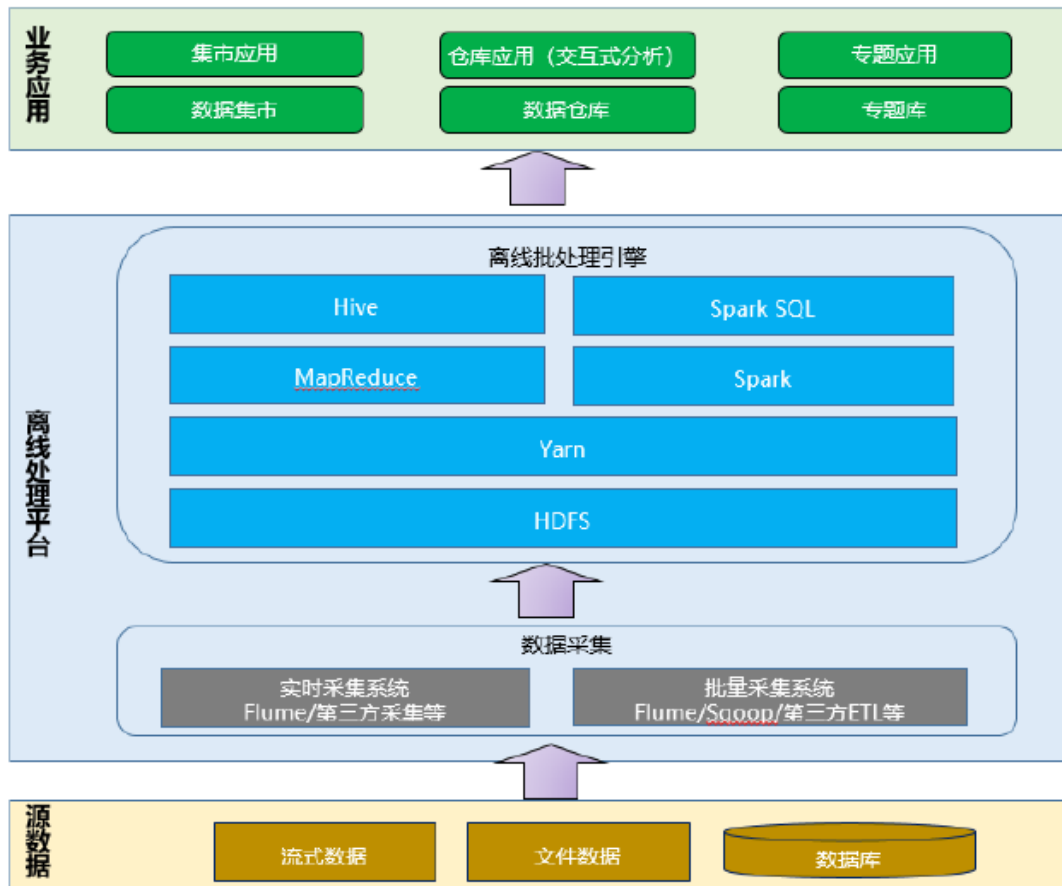


图 离线处理数据流图

3.3 实时流处理

实时流处理，通常是指对实时数据源进行快速分析，迅速触发下一步动作的场景。实时数据对分析处理速度要求极高，数据处理规模巨大，对 CPU 和内存要求很高，但是通常数据不落地，对存储量要求不高。实时处理，通常通过 Spark Streaming 或者 Flink 任务实现。

典型特点：

- 处理时间要求极高，毫秒级
- 处理数据量巨大，每秒数百兆

- 占用计算资源多
- 容易产生计算资源抢占
- 数据格式以各种网络协议格式为主
- 任务相对简单
- 数据不落地、存储量不大

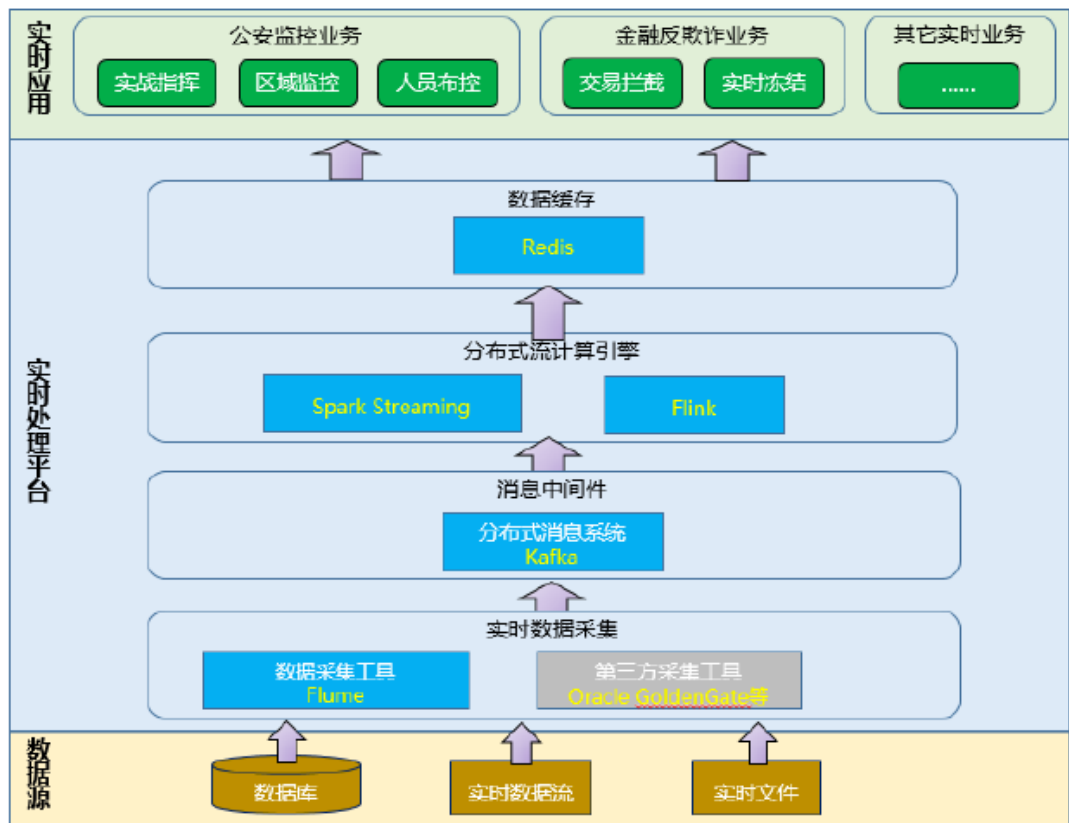


图 数据流图

3.4 融合数仓

融合数仓，是指用分布式数据仓库，完成数据的预处理、离线分析、主题查询等全流程的数据分析业务。融合数仓通常以 SQL 语言为基本数据操作手段，同时支持用户自定义的数据处理函数，既能支持海量数据离线处理，又能支持在线交互查询。融合数仓是一种跟 Hadoop 完全独立的数据分析工具，可以承担的业务也有很多重叠。相比 Hadoop，融合数仓在成本、数据规模上限、复杂数据挖掘、实时流处理方面有劣势，在 SQL 支持度、数据库兼容性、性能方面有优势。

典型特点：

SQL 支持度要求高，支持存储过程和自定义函数，兼容主流数据库和数据仓库

查询响应时间要求较高，查询时间 3 秒内

处理数据量巨大，可以达到百 TB 级、支持性能接近线性的水平扩展

支持数据更新和插入，支持事务

离线作业和在线查询并存，容易产生资源抢占

支持对接第三方展现和报表工具

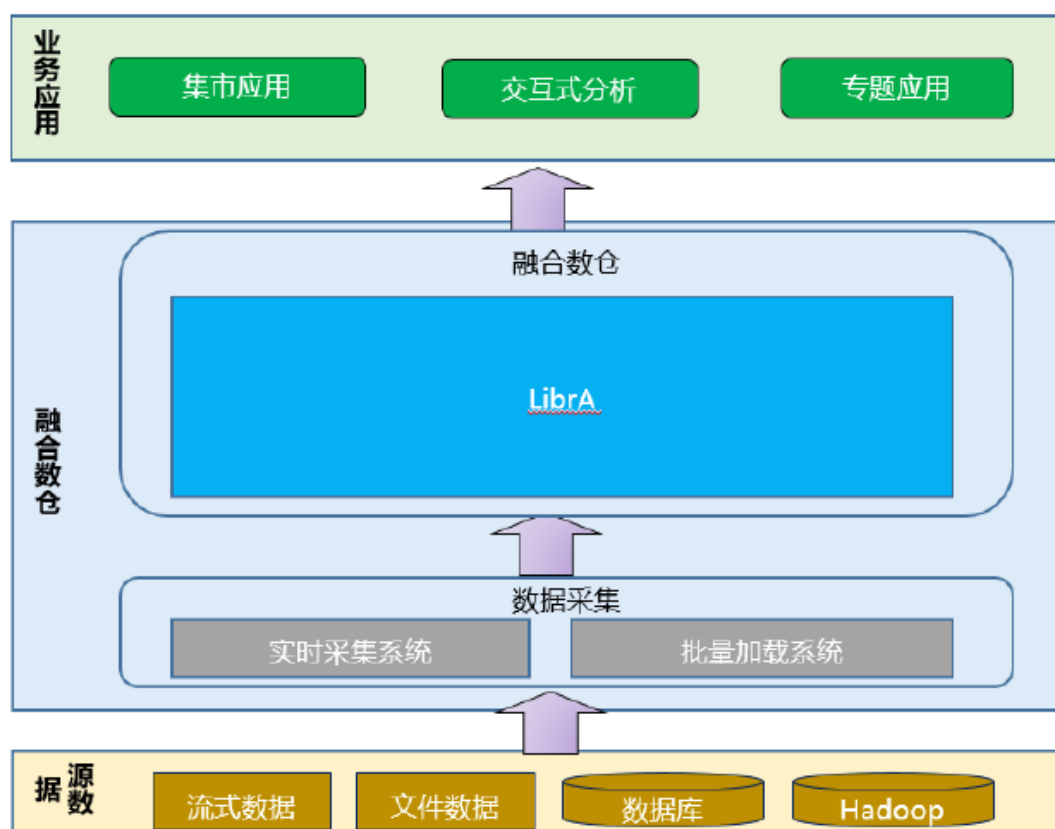


图 数据流图

3.5 实时检索

实时检索，通常是指数据实时写入，对海量数据基于索引主键实时查询，查询响应要求较高，查询条件相对比较简单。查询条件复杂的可以根据关键词在全域数据中通过索引搜索主键后，通过主键查询。全域数据既包含了结构化数据又包含了文本数据。例如：按照卡口和时间为主键快速查询过车数据，按照车辆为主键查询车辆轨迹数据。

典型特点：

查询响应时间要求较高，1 秒内

高并发

处理数据量巨大，PB 级

能够同时处理结构化和非结构化的数据

全文检索功能

近实时索引

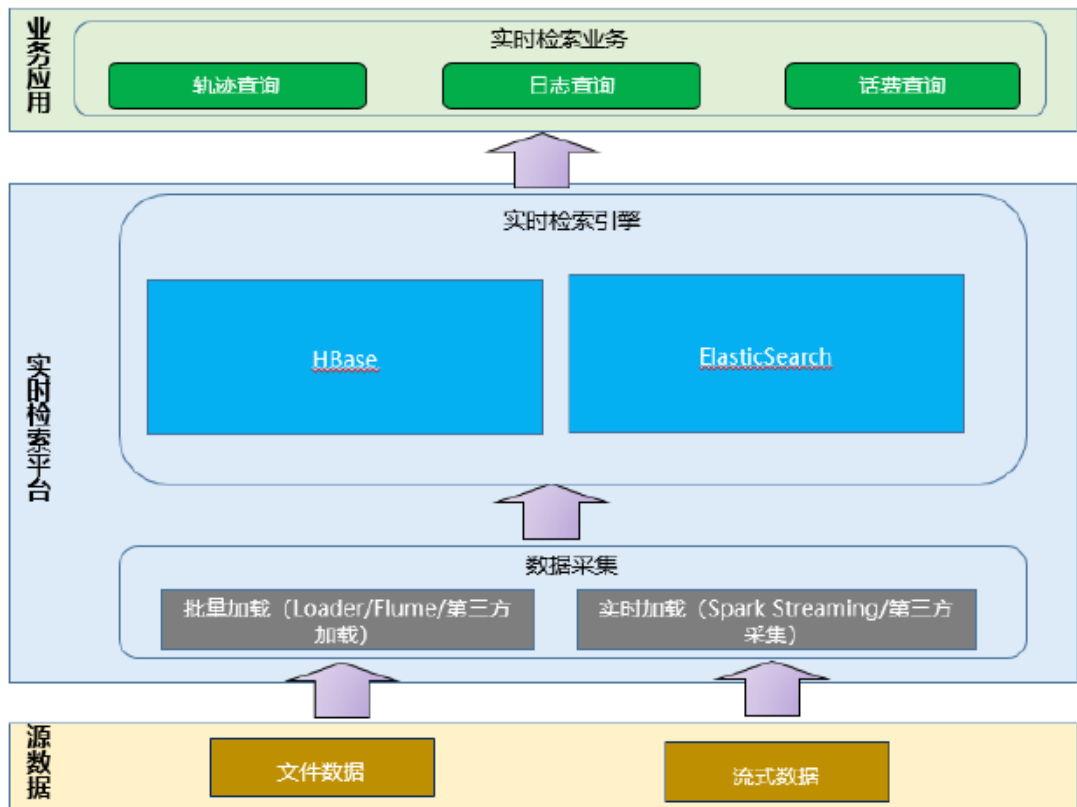


图 数据流图

4. FusionInsight ModelArts AI 服务能力

4.1 Miner workflow 可视化建模

1、业务场景

workflow 可视化建模，通常是指从预制的工作流算子，从，这种方式可以方便的查看数据分析结果和模型构建结果，并且可以直观的展示模型构建流程，适合对算法和接口无深入了解的数据分析业务人员。

银行金融交易业务中金融反欺诈模型构建和客户分群模型构建过程中，对于那些对业务很了解，但是不懂任何数据分析编程语言的数据分析人员，应用 workflow 可视化建模就是一个典型的应用场景。应用 workflow 可视化建模可以快速的帮助他们进行异常交易金融业务建模，客户分群建模，通过对以上业务的建模，可以方便后续进行反金融欺诈业务，对潜在客户拓展金融业务提供模型应用服务。

对于只熟悉金融交易业务不懂编程语言的业务员进行建模的需求特点是：

简单，易用

不需要任何编程语言基础

建模过程可视化

数据，模型结果可视化

算子种类多样丰富多样，方便构建各类模型

提供一站式机器学习应用算子，包括读取数据源、特征工程、算法、建模、模型应用模型评估等建模各阶段算子

提供建模项目管理能力

提供模型管理能力

2、方案概述

workflow 可视化建模，通常是指从预制的工作流算子，通过拖拽式工作流算子的方式构建模型生成工作流，这种方式可以方便的查看数据分析结果和模型构建结果，并且可以直观的展示模型构建流程，适合对算法和接口无深入了解的数据分析业务人员。

workflow 可视化建模的典型特点和核心诉求是：

1. workflow 建模流程可管理性——方便查看历史 workflow 建模过程，导入导出 workflow

2. workflow 可拖拉拽界面——提供简单易用的可拖拉拽图形界面，建模门槛低，无需任何编程需求

3. 数据可视化——方便的可视化数据预览界面，方便查看数据分布，基本的数据统计能力

4. 特征提取功能——具备数据特征提取功能，且提取操作简单，快捷，多角度提取，算法多样

5. 丰富的算子算法库——提供丰富的机器学习建模算法，种类齐全，包括分类、聚类、回归等算法

6. 模型评估功能——对模型训练结果方便的进行模型应用和模型性能评估，并且具备评估效果可视化

7. 模型构建结果可管理性——对训练结果可保存性，保存结果通用性，方便后续的模型应用

3、整体架构



图 整体架构图

各模块说明及相关组件在方案中的作用如下：

项目管理：项目管理主要用于管理工作流项目文件，其中包括新建工作流，删除工作流，修改工作流名字，导入工作流功能，通过工作流项目管理，用户可以方便的管理自己的工作流。

数据探索：提供 Web 化的自由探索界面，用户可以方便的查看数据，并将探索结果通过可视化的图形展示出来，大大提高数据分析师的探索效率。

特征工程：提供了大量提取特征的算子接口，满足绝大部分特征工程的需要，尤其适合高维稀疏大数据的特征处理。

建模分析：建模分析模块集成常用分类、聚类、回归算法接口，可以支持个性化推荐、异常检测、客户分群等典型场景的模型构建应用。

并行化算法库：并行化算法库主要为 workflow 算子提供可选择算法库，算法库提供了可操作算子达到 108，机器学习算法库达到 70+。

模型管理：主要用于管理构建后的模型，通过模型管理，用户可以方便的保存模型、查看模型和发布模型，模型的保存支持保存为 PMML 通用的模型文件，模型可以发布成 Jar 包，方便 java 应用程序调用。

4.2 Miner 交互式笔记本建模

1、业务场景

交互式笔记本建模，通常是指在在线 web 编辑器上，应用某类机器学习语言进行模型开发，交互式笔记本能够灵活编写代码，交互性强，适用于具备编程能力，了解数据分析、算法的数据科学家。

银行金融交易业务中金融反欺诈模型构建和客户分群模型构建过程中，对于那些了解数据分析、算法以及具备某类语言的数据科学家，应用交互式笔记本建模就是一个典型的应用场景。交互式笔记本建模可以帮助他们灵活的进行异常金融业务建模，目标客户分群建模，更有助于建立更强大更满足他们业务需求的模型。

对于了解数据分析、算法的数据科学家进行建模的需求特点是：

应用灵活，多样

支持典型数据挖掘语言

可以连接多种数据源

支持并行计算，计算性能优良

建模过程交互性好，可以边写边调试，查看结果

过程数据可视化

建模结果可保存，性能评估可视化

2、方案概述

交互式笔记本建模，通常是指在在线 web 编辑器上，应用某类机器学习语言进行模型开发，交互式笔记本能够灵活编写代码，交互性强，适用于具备编程能力，了解数据分析、算法以及具备某类语言的数据科学家。

交互式笔记本建模的典型特点和核心诉求是：

1. 打开方便——交互式笔记本不用安装专门的客户端，可以随时随地方便访问
2. 运行方便，交互性能优越——交互式笔记本运行方便，结果即时呈现，交互性优越
3. 代码调测方便——代码有问题可以反复修改，运行。
4. 支持多种语言——可以支持应用多种典型的机器学习语言进行模型训练代码编写，这样方便掌握不同语言的数据科学家使用
5. 支持多数据源访问——同时支持访问多种类型数据库 Elk, Hive, 还支持访问 HDFS。
6. 支持并行计算，高效率——支持调用 spark ml lib 进行并行机器学习训练
7. 运行结果呈现即时性高，可视化效果好

3、整体架构

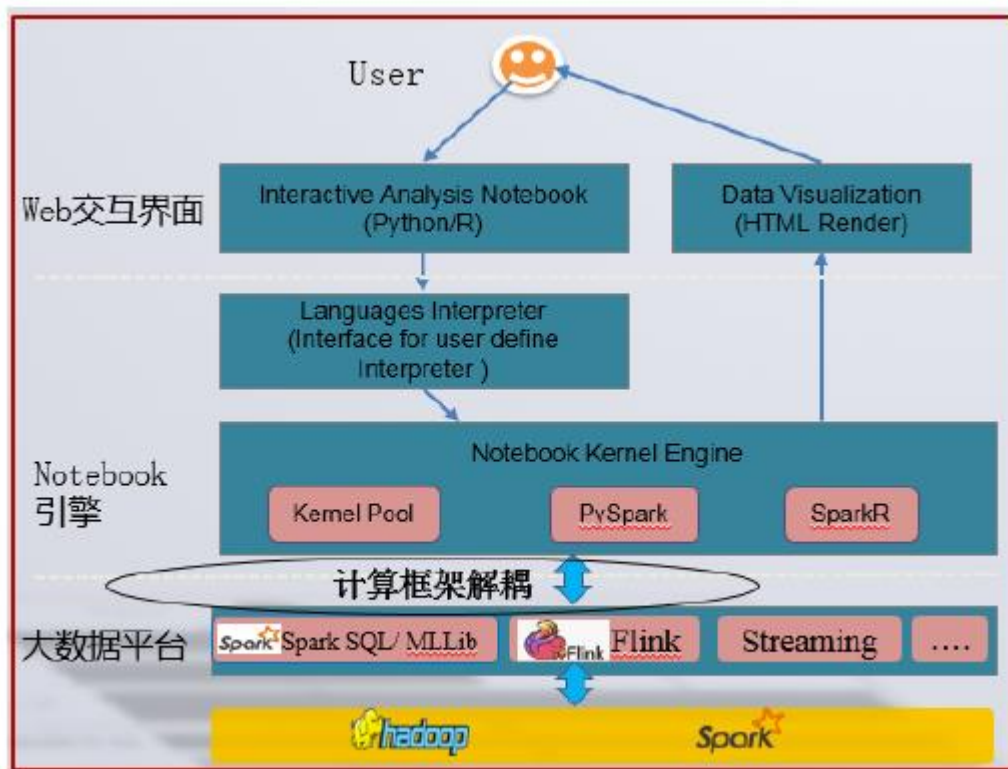


图 整体架构图

各模块说明及相关组件在方案中的作用如下：

Notebook web 交互界面：在交互式界面上，用户可以进行机器学习训练过程代码编写，在该平台上，可以编写数据读取及预处理、特征提取、特征建模、模型评估等机器学习各阶段代码。

语言解析器：后端预制 python2、python3、R 三种 notebook 语言解析器
Notebook kernel

引擎：kernel 引擎中管理者 kernel pool,该 kernel pool 维护两种类型的 kernel:

– **Pyspark：**用于 python 语言对接 spark，其中支持 python2 和 Python3 对接 spark 调用 spark ml lib 进行并行机器学习训练。

– **sparkR：**用于 R 语言对接 spark 调用 spark ml lib 进行并行计算。

数据可视化：数据运行结果即时呈现，即时性、可视化性能优越。

4.3 DLS 大规模训练平台

1、业务场景

近年来，深度学习技术在许多 AI 应用上获得了巨大的成功。拥有大量的数据之后，深度神经网络可以很好地学习特征表示。但是，深度神经网络以及大规模的数据，对计算资源的需求也是极大的。大规模训练处理，通常是指对深度学习中大数据训练场景。深度学习大规模训练会涉及到海量参数计算，大规模数据处理，超参数调优，传统的 CPU 资源已经很难满足需求，幸运的是，一些硬件加速器，包括 GPU、FPGA 和英特尔至强处理器都能用于减少模型的训练时间。

大规模训练平台整合当前主流的深度学习框架，Tensorflow, Pytorch, Mxnet, Caffe，集成分布式调度系统，实现资源隔离和分布式调用。满足客户海量数据大规模训练场景。

大规模训练平台是一站式深度学习平台，打通 AI 业务全流程，完成数据标注，模型开发，模型训练，模型发布：

标注工具：离线标注工具，用户原始数据预处理。

模型实时训练和调优：支撑建模人员在线编写代码实时训练，模型调优。

推理服务，模型训练完毕，在线发布，评估模型训练效果，在线发布服务，支撑业务服务无缝对接。

大规模训练平台的典型特点是：

多资源统一调度。

集成主流的深度学习框架。模型训练实时监控。

在线推理服务发布，模型评估。

一站式深度学习平台，模型开发，模型训练，模型发布实现完善 workflow。

2、方案概述

大规模训练，通常是指神经网络层数深，数据规模大，训练时间长的深度学习训练。大规模训练缩短用户训练时间，集成分布式调度系统，自动完成用户任务发布，模型训练。

大规模训练场景的典型特点和核心诉求是：

1. 数据预处理
2. 多训练框架集成
3. 分布式任务调度
4. 训练超参数调优
5. 训练模型导出
6. 训练模型在线推理

3、整体架构

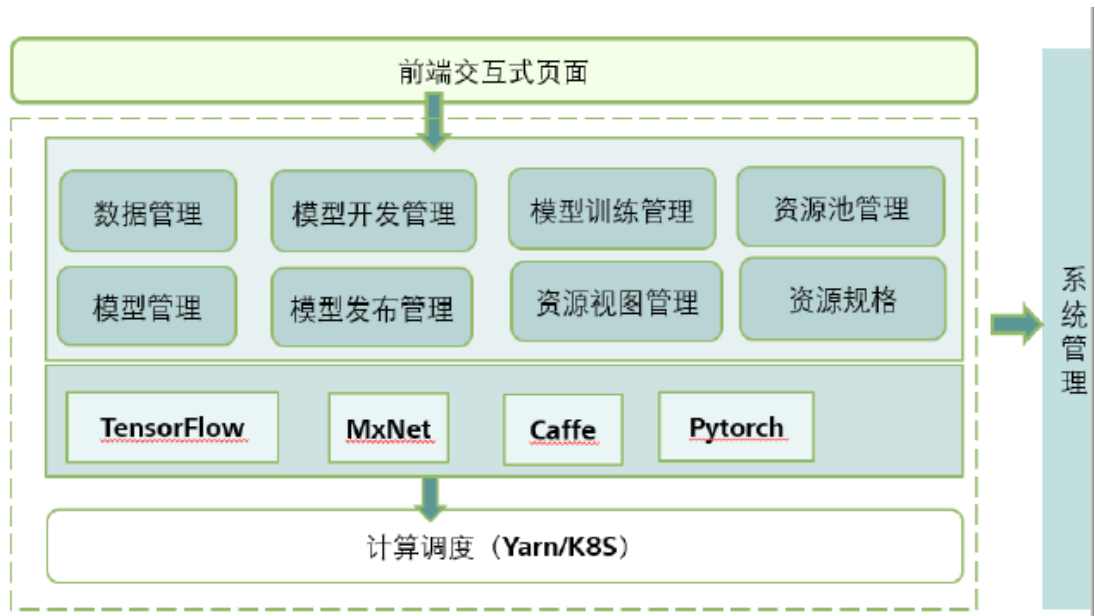


图 整体架构图

各模块说明及相关组件在方案中的作用如下：

前端交互页面：可视化操作页面，提供用户创建训练任务向导和任务资源的实时展示，模型开发-模型训练-模型发布，打通 AI 业务全流程。

数据管理：用户上传和下载数据集，作为用户训练的数据选择，与训练作业的无缝对接。

模型开发：创建开发环境，进行代码的开发与调测，支持使用 Jupyter Notebook 进行交互式的模型开发环境：为建模专家量身打造。

模型训练：创建训练作业进行模型训练，训练后的模型可创建可视化作业，帮用户理解、调试、优化深度学习代码和执行过程。训练参数可以保存在训练参数管理中，下次训练直接使用，支持主流的深度学习框架。

模型管理：将用户训练成熟的代码保存，进行管理。

模型发布管理：使用已训练好的模型创建推理作业，部署推理服务，用户可以基于推理服务进行简单的推理测试。

资源池管理：资源用户隔离，实现资源最大化利用。

资源规格：作业资源的精细化控制，支持全局规格和资源池规格。

4.4 DLS 预置算法训练平台

1、业务场景

用户训练模型创建中，用户对算法和深度学习框架的属性不多，需要借助深度学习，快速发布模型，上线应用服务。

深度学习平台集成常用的预制模型，用户不需要编写代码，不需要了解深度学习的专业知识，用户只需要准备数据集，上传到平台，就可以实现训练，支持用户模型快速发布，业务快速上线。

预置算法训练的典型特点是：

简化用户训练流程

支持一键式训练

模型实时更新二次训练

2、方案概述

预置模型训练。深度学习平台预置了用户常用的训练算法，用户上传代码数据实现模型的二次训练，模型训练实时查看，训练模型实时导出，模型训练完毕平台和在线预测。

交互查询的典型特点和核心诉求是：

1. 预置模型可视。
 2. 预置模型快速训练
 3. 模型超参数调优，训练过程可视化
 4. 模型实时导出，模型在线发布
- 3、整体架构

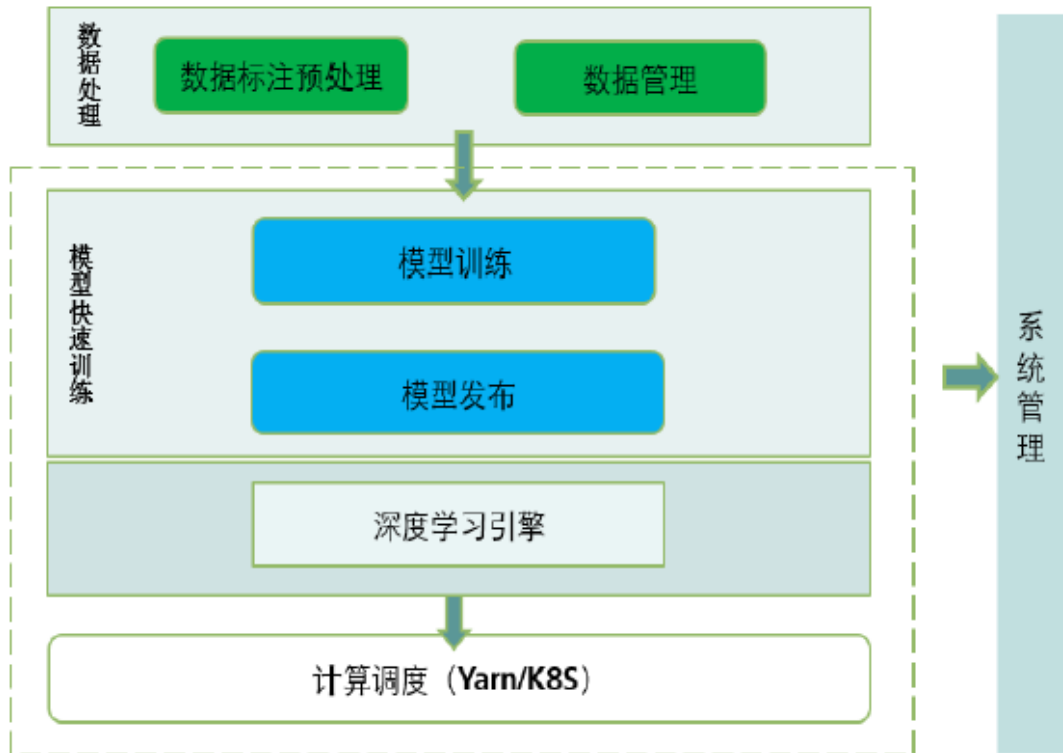


图 整体架构图

各模块说明及相关组件在方案中的作用如下：

数据处理：用户数据管理，数据预标注，与训练作业的无缝对接。

模型训练：预置算法快速训练，降低 AI 训练门槛，助力企业快速训练模型上线业务。

模型发布：使用已训练好的模型创建推理作业，部署推理服务，用户可以基于推理服务进行简单的推理测试。

4.5 在线推理平台

1、业务场景

在线推理，通常是指将推理发布成一个 web 服务，并提供接口，供上层应用实时调用，上层应用按规定格式输入数据，由推理服务完成推理处理，并将推

理结果返回给上层应用。在线推理服务对于稳定性要求高，如果推理服务故障，则对应的应用也可能无法提供服务。

安平智慧交通的信号优化就是一个典型的实时推理场景，服务于平安智慧交通业务。主要用来对实时的交通路口视频进行分析处理。将原始的路口车辆通行视频，推理成车流状况数据，以生成实时的交通控制信号，提高通行效率。

在线推理的典型特点是：

处理时间要求高

系统可靠性要求高

处理并发量有高低起伏，偏差量大

2、方案概述

在线推理，通常是指将推理发布 web 服务，并提供接口供应用调用。在线推理对处理时间要求高，且对系统可靠性要求高，且业务并发量有高低起伏。通常使用在线作业实现。

在线推理场景的典型特点和核心诉求是：

1. 处理时间要求高，要求推理服务响应不超过**毫秒。
2. 系统可靠性要求高，要求提供 7*24 小时在线服务，提供多实例负载均衡和异常服务的监控告警功能。
3. 处理并发量起伏大，需要根据不同的并发业务量，弹性增减推理服务实例数，确保推理服务容器响应时间满足要求。
4. 统一接口需求，支持一个算法的多实例统一接口访问。
5. 支持不同厂商的不用版本的推理镜像、模型运行在 ModelArts 推理平台。
6. 支持推理镜像模型分离，
7. 支持标准模型一键式发布成在线推理服务，无需用户手工制作镜像。
8. 支持指定节点调度作业，满足推理服务对特殊资源的需求。
9. 支持异构资源——支持 CPU、内存和 GPU 异构资源调度。

3、整体架构

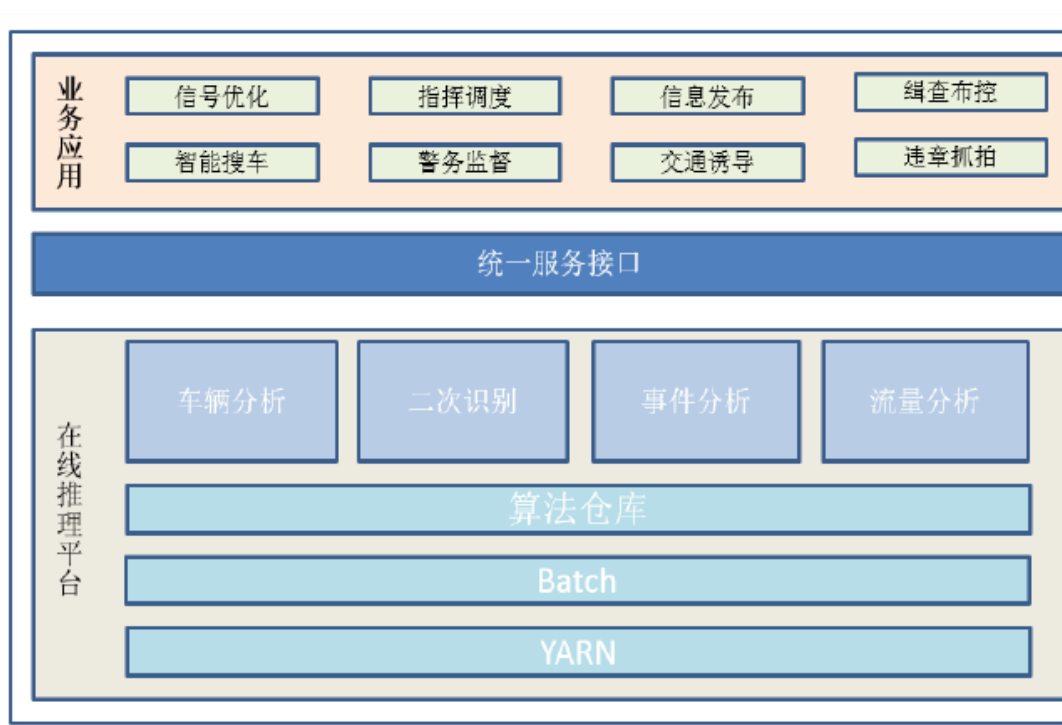


图 整体架构图

各模块说明及相关组件在方案中的作用如下：

统一服务接口：用于代理在线推理服务多实例和负载均衡，为一个算法的推理服务提供统一的服务接口。

在线推理平台：用于实现高性能高可靠的在线推理服务管理。

– **算法仓：**提供多厂商多版本的镜像模型管理功能；提供 TensorFlow Serving 预置框架，用于一键式将 TensorFlow 训练模型发布成在线推理服务，无需用户手工制作 Docker 镜像。

– **Batch：**作业任务调度管理引擎，支持基于 Docker 容器的作业和任务调度和生命周期管理。支持先进先出、优先级等高级调度策略。支持指定节点的亲和调度，满足作业任务运行的特殊资源需求。

– **Yarn：**资源调度引擎，为各种批处理引擎提供资源调度能力，支持 CPU、内存和 GPU 等多种异构资源的统一调度。

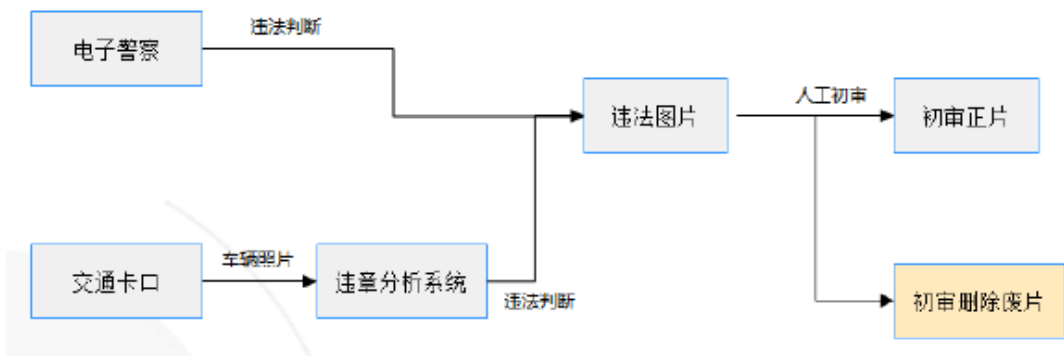
业务应用：实时调用在线推理服务提供的接口，并根据接口返回结果完成业务应用，一般由 ISV 开发。

4.6 批量推理平台

1、业务场景

批量推理，通常是指对批量离线数据进行分析和处理，形成结构化数据，共下一步业务使用的场景。批量推理对于时间要求比在线推理略低，对于可靠性的要求，也比在线推理要低，批量推理失败可以对作业或者任务进行重试，批量推理最终成功后，并不影响结果。但是所处理的数据量大，占用计算存储资源较多。通常批量推理通过队列作业或者非队列作业启动。

安平智慧交通的废品回滚就是一个典型的批量推理场景。服务于车辆违章的识别业务。主要用于对已经过人工筛选的“不可知法的废片”的进行二次筛检，有效提高车辆违章的识别率。



违章二次识别等批量推理任务，其典型特点体现在以下三个方面：

处理时间要求不高，如白天拍摄的图片，可以晚上进行批量处理。

数据格式多：数据文件/视频/图片等。

数据量大：每天需处理 30000+张废弃图片。

资源占用多：容易产生资源抢占。

2、方案概述

批量推理，通常是指对批量离线数据进行分析和处理，形成结构化数据，共下一步业务使用的场景。批量推理对于时间要求比在线推理略低，对于可靠性的要求，也比在线推理要低，批量推理失败可以对作业或者任务进行重试，批量推理最终成功后，并不影响结果。但是所处理的数据量大，占用计算存储资源较多。通常批量推理通过队列作业或者非队列作业启动。

批量推理场景的典型特点和核心诉求是：

1. 处理数据量大，单批次处理需要可达**万张图片，**G 视频。
2. 资源隔离：多个批量推理运行时，需要不同的资源，应进行资源隔离，避免抢占资源。

3. 优先级需求：大量批量推理运行时，由于系统资源不足，需要排队等待，需支持高优先级作业优先调度运行。
4. 推理失败重试：批量推理中途失败后，需要支持自动重试，确保能输出最终结果。
5. 支持异构资源——支持 CPU、内存和 GPU 异构资源调度。
6. 支持指定节点调度作业，满足推理服务的资源亲和需求。
7. 支持不同厂商的不用版本的推理镜像、模型运行在 ModelArts 推理平台。
8. 支持推理镜像模型分离。

3、整体架构

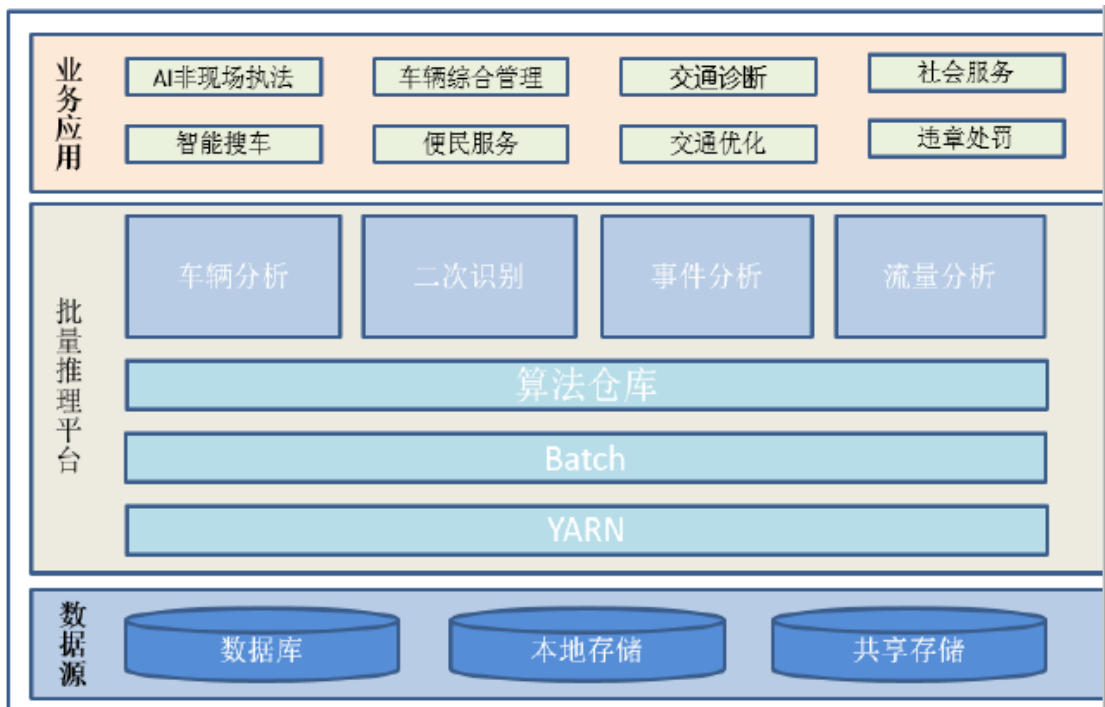


图 整体架构图

各模块说明及相关组件在方案中的作用如下：

数据源： 主要包含原始的业务数据和推理结果数据存储载体，一般包括数据库、本地存储和共享存储等。

批量推理平台： 用于实现高性能高并发的批量推理服务管理。

— **算法仓：** 提供多厂商多版本的镜像模型管理功能。镜像和模型分离，独立管理，创建作业动态加载模型，支持各种业务场景的批量推理。

– **Batch**: 作业任务调度管理引擎，支持基于 **Docker** 容器的作业和任务调度和生命周期管理。支持先进先出、优先级等高级调度策略。支持指定节点的亲和调度，满足作业任务运行的特殊资源需求。

– **Yarn**

: 资源调度引擎，为各种批处理引擎提供资源调度能力，支持 **CPU**、内存和 **GPU** 等多种异构资源的统一调度。

业务应用：使用批量推理结果完成的具体业务应用，一般由 **ISV** 开发。