文档名称:	**橘云多租户管理功能说明书**
文档版本:	1.0
文档类型:	**产品功能说明书**
作者:	**王栋**
最近更新时间:	2017 年 5 月 24 日

注意事项:

亚信数据

产品功能说明

橘云多租户管理产品功能说明书

作者	王栋
审阅人	马松，王庚，夏建东，金文浩，郭茜，王琛，虞里杉，赵一鸣
密级	机密，此文档用于亚信内部人员使用
项目名称	橘云多租户管理产品功能说明书
项目描述	橘云多租户管理产品

文档更新历史:

版本	时间	作者	备注
1.0	2017/5/24	王栋	初稿

目录

1. 简介

1.1 目的

此产品规格说明书用于橘云多租户管理产品功能的说明。此文档应该详尽描述产品的规格，功能和设计，以便能够依据此文档生成测试用例以及客户文档。此文档的目标用户应该是产品经理，开发，测试，支持以及现场人员。

1.2 名词解释

OCDP	橘云大数据平台，是亚信数据发布的企业级 Hadoop 大数据平台
OCDF	橘云云计算，服务托管平台
租户	集群中各种服务，和对这些服务的使用容量的集合。
用户	租户资源使用的具体人员。
角色	用户在集群中的权限集合
服务	将底层平台提供的各种资源，都包装成服务，以服务的形式提供的租户来使用。

2. 规格说明

2.1 需求说明

2.1.1 概要

橘云多租户管理平台，通过使用统一的多租户模型，将企业级生产环境中的各种大数据，云计算服务，组织起来，形成不同级别的资源集合，然后把租户提供给相应的资源使用者。租户资源的使用者会牵涉到多种用户，包括租户的管理员，和租户的普通用户，租户的普通用户又可以有多种具体角色。

。

2.1.2 背景

1) 企业级大数据，和各种服务组件要统一管理，以消除资源孤岛和信息孤岛运维模式，集中化管理，平台化，虚拟化各种服务资源的使用，以利于整体的资源把控，提高资源和服务的使用效率。
2) 目前大数据平台和云计算平台缺乏一个统一的租户管理模型，也缺乏一个统一的租户管理入口，租户，用户和权限的概念在各个层面都存在理解上的差异性，导致产品开发和运维逻辑混乱。企业急需一个完整的租户管理模型和租户管理入口。

2.1.3 范围

In-Scope

1．功能需求

- 建立一个完整的企业级大数据，云计算租户管理模型，将企业的各种计算资源统一管理，授权使用。

- 提供一个 Web 访问界面，让企业的 IT 资源管理员可以通过界面看到企业的整个大数据，云计算平台资源的概览，使用情况，服务，资源配置信息等。

- 企业的 IT 资产管理员可以把大数据，和云计算平台上的各种服务能力，通过租户的方式整合在一起，满足一个租户对各种 IT 基础服务的要求。

- 租户在租户管理平台上，可以被创建，删除，查看，和更改。

- 租户上会创建一个默认的用户角色，用来讲租户中的各种服务的权限组合在一起。

-租户上的用户角色权限，可以授权给具体的用户，这样就让用户拥有了对租户上的服务资源的使用能力。

-当租户上的服务，或者服务的资源不够用时，租户可以提出扩容的申请。

-租户的扩容申请可以包含要求添加新服务，也可以要求对现有服务的容量进行提升。

- 租户的扩容，需要满足企业的服务和服务资源扩容审批流程，所以在橘云多租户管理的过程中，要把租户的扩容跟审批流程集成在一起，扩容请求会逐级通知到相关的人员，审批进度和决定也会逐级下发给相关的操作人员。

- 每一级租户，都可以对本租户上的 IT 服务和服务资源的使用情况进行查看，分配用户角色等。

- 上一层租户的管理员，可以对下一层租户的服务种类，服务的资源配置进行调整。

- 平台管理员，可以对要纳入多租户管理平台的服务进行配置，只有纳入到了多租户管理平台的 IT 基础服务，才能在创建租户时被分配给租户。

2．扩展性需求

- 支持跟信云智系统的集成，实现在租户创建，租户扩容时的审批流程。

- 支持跟云用户中心的集成，实现用户登陆时的认证工作，和租户授权时可以从云用户中心中获取用户信息。

- 支持跟 DACP 系统的集成，在租户创建，扩容时，能够通知 DACP 相关租户信息的变成情况。

Out of Scope

1. 租户的删除和缩容，在本次项目中暂不考虑。

2.1.4 平台描述

支持以下 64 位 Linux 操作系统:

- Red Hat Enterprise Linux (RHEL) v6.x v7.x
- CentOS v6.x 7.x

Kibana 界面支持的浏览器：

- IE 11 及以上版本
- FireFox
- Chrome

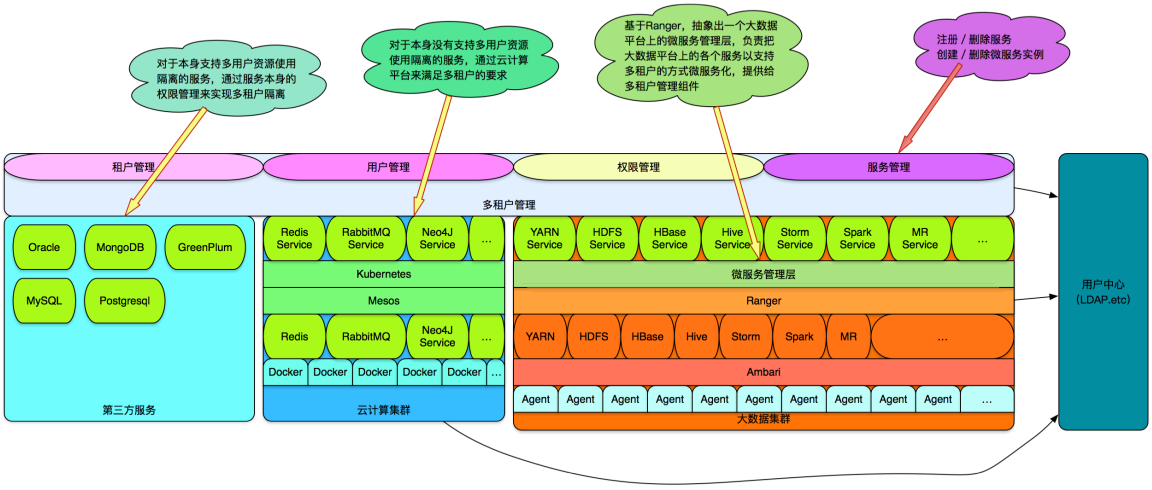
2.1.5 依赖关系

- 依赖于 OCDP4.1 集群环境
- 依赖云 OCDFxx 集成环境
- 依赖于第三方的 Oracle，GreenPlum，MongoDB 和 MySQL 的环境。

2.1.6 功能描述

2.1.6.1 架构设计

整个橘云的多租户管理，基于以下模型：



所有租户的管理，都由以上图中的四个实体来体现，这四个实体是服务，租户，用户和权限。其中：

服务是对底层大数据平台，云计算平台和第三方平台能提供的 IT 服务能力的一种抽象。底层的每一种 IT 基础服务，在橘云多租户管理平台上都是一个服务，服务会作为资源分配的最小单位。为了满足多租户的要求，服务的提供者，提供的服务要满足资源隔离和共享的要求。对于大数据平台，

租户是资源的组织形式，一个租户是一个服务的集合。租户里定义了一个租户里面包含什么服务，租户对每一个服务，可以使用的容量是多少。

用户是租户资源的使用者。可以使用租户中的各种服务上的资源。

权限是对租户上的各种服务资源使用能力的细力度定义。例如对 HDFS 服务上的一个文件的读能力，就是一个权限。

在橘云多租户管理平台上，多个权限会被打包在一起，形成一个角色，然后把角色授权给一个用户，这样用户就具有了多个权限。橘云多租户管理平台目前默认会提供平台管理员，租户管理员，租户用户三种角色。这三种角色分别代表的含义是：

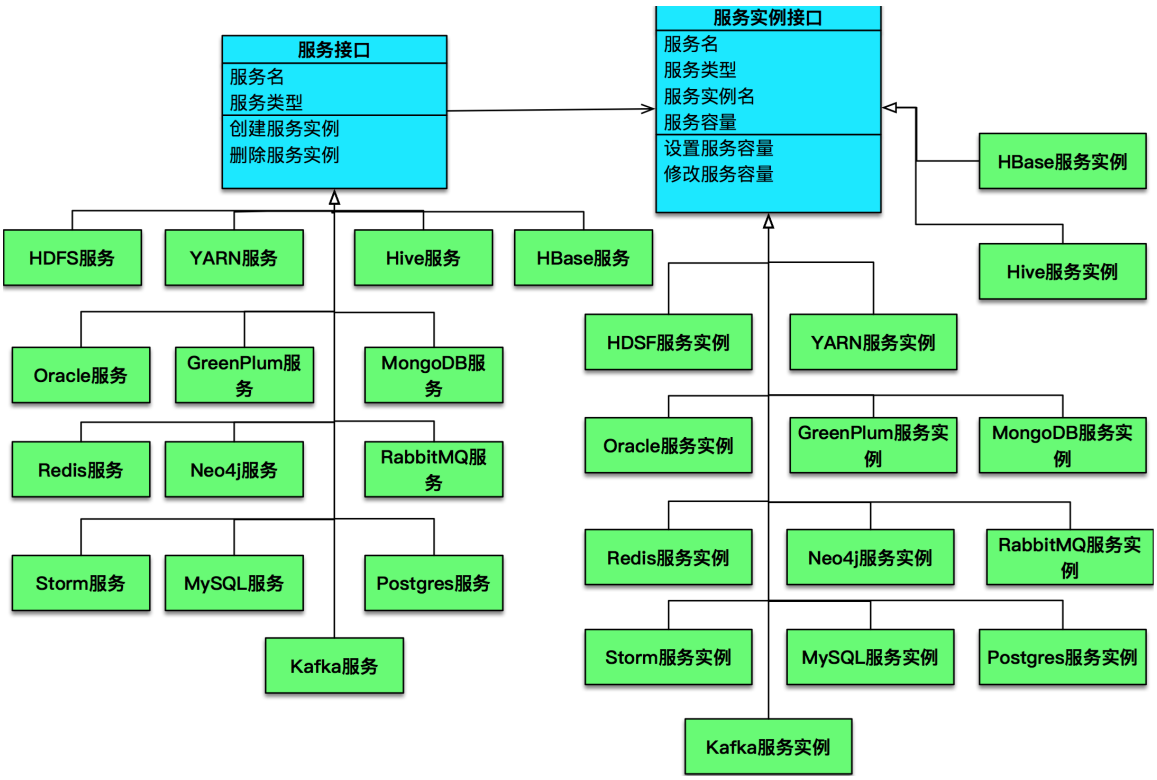
平台管理员：整个橘云多租户平台的管理员，拥有对企业所有大数据，云计算和其他 IT 基础服务资源的查看，管理和配置能力。

租户管理员：对应到一个具体的租户上，拥有对一个租户上的所有资源的管理能力，如：查看租户的信息；修改租户的信息；创建租户的子租户，并将租户资源分配给子租户；调整子租户的资源配置；为租户添加用户，并且给用户授权一个或者多个角色；对租户资源提出扩容申请，其中扩容包括扩大服务的种类，和扩大现有服务的容量。

租户用户：对应到一个租户上，可以对租户的所有信息进行查看，但是没有其他的操作权限。

企业中的所有 IT 基础服务，都会通过租户的方式来进行组织，租户会按照资源的使用和归属情况，将所有租户组织成一个树的形状。其中的树根节点代表一个企业的所有 IT 基础服务。第一级的租户可以由平台管理员来创建，它可以把服务和相应的服务容量分配给第一级的子租户。第一级的子租户，可以再创建第二级的子租户，并把它所具有的服务和相应容量，再分配给它的子租户。以此类推，形成一个租户的树形结构。

服务的抽象满足以下接口的要求：



其中的每一种服务，都要通过大数据平台，云计算平台或者服务本身的多用户隔离能力，抽象出在多租户条件下的资源隔离能力，具体如下：

HDFS 服务的多租户能力定义：

HDFS 本身可以支持多用户隔离访问不同的存储空间，HDFS 服务提供的多租户能力也是基于 HDFS 本身的这种能力，我们在给一个租户创建 HDFS 资源时，需要指定一个 HDFS 上的目录路径，租户在这个目录下的磁盘空间配额，和可以创建的文件个数这三种信息。HDFS 上提供的这种能力在橘云大数据平台上，是通过 Ranger＋HDFS 本身联合提供的，Ranger 可以用给租户指定一个具体的 HDFS 路径，配额和文件数配置，都是通过 HDFS 本身的命令来实现的。

租户在给 HDFS 在扩容时，可以设置指定目录的存储配额大小和文件个数，而文件路径一旦创建完成，则不可以修改，除非删除租户的 HDFS 服务能力。

在删除租户的 HDFS 的服务能力时，直接将 HDFS 的文件路径，磁盘配额和文件个数配置信息全部删除，同时将租户在 HDFS 目录下的所有数据文件也会全部删除。所以删除租户的 HDFS 服务是一个非常危险的操作，只有在明确了影响后才能执行这个操作。删除完后，租户原来占用的 HDFS 服务容量，会被返回给租户的上一层租户的 HDFS 服务容量中，作为其空闲容量保留。

YARN 服务的多租户能力定义：

YARN 服务的多租户能力依赖 YANR 本身的队列管理能力，每一个租户在分配 YARN 的服务能力时，会分配一个对应的 YANR 队列，在这个队列上，可

以指定租户使用的资源的容量信息，最大容量信息，和其中的 AM（Application Master）所占用的资源的比例信息。
在给租户扩容时，可以根据实际需要，更改租户队列的资源容量，最大资源容量，AM 资源占比信息，但是相应的队列名字不可以更改。
删除租户的 YARN 服务能力时，直接删除分配给租户的队列，队列删除后，相应的计算能力就会返回给上一级租户，作为上一级租户的空闲资源保留。

Hive 服务的多租户能力定义：
Hive 的多租户服务能力通过在 Hive 上创建数据库来实现，针对每一个租户，需要为其创建一个相应的 Hive 数据库，并分配合适的存储空间大小供其使用。
当要对租户的 Hive 数据库扩容时，只需要增加租户的 Hive 数据库存储空间大小即可，租户的数据库一旦创建，就无法更改名字，除非删除租户的 Hive 服务能力时，会删除租户相关的 Hive 数据库。
删除租户的 Hive 服务能力，其对应的 Hive 数据库也会被同时删除，Hive 数据库被删除时，里面存储的数据也会被同时删除，所以执行这个操作时，情务必明确其会造成的影响。

HBase 服务的多租户能力定义：
HBase

Kafka 服务的多租户能力定义：
Kafka 服务的多租户能力，结合 Kafka，kerberos 和 Ranger 来共同提供，通过 Ranger，Kafka 可以将 Topic 隔离开来，分配给一个租户来使用，实现租户间的隔离。每一个租户可以创建一个 Kafka 的 Topic，Topic 中可以指定消息的生命周期。
Kafka 的扩容包含对 Topic 中消息声明周期的延长，
删除租户的 Kafka 服务能力，会将给租户创建的 Kafka topic 整个删除，其中保存的消息也会一并被删除。

Oracle 服务的多租户能力定义：
Oracle 服务的多租户能力，通过为租户创建 Oracle 的 DBSchema 来实现，一个租户会创建一个 Oracle 的 DBSchema，这个 Schema 可以指定表空间的大小，表空间策略采用固定空间大小。
Oracle 服务的扩容通过增加表空间来实现。DBSchema 一旦创建，则不能修改，除非删除租户的 Oracle 服务能力。
删除租户的 Oracle 服务能力，会将为租户创建的 Oracle DBSchema 整个删除掉，同时其中保存的数据也会被删除掉。

GreenPlum 服务的多租户能力定义：
GreenPlum

MongoDB 服务的多租户能力定义：
MongoDB

RabbitMQ 服务的多租户能力定义：
RabbitMQ 的多租户能力，通过云计算平台提供，云计算平台需要把 RabbitMQ 包装成独立的服务提供给租户使用，租户可以配置 RabbitMQ 的 XXX
扩容租户的 RabbitMQ 时，通过调用云计算平台的接口来实现。
删除租户的 RabbitMQ 服务能力，通过调用云计算平台的接口来实现。

Neo4j 服务的多租户能力定义：
Neo4j 的多租户能力，通过云计算平台提供，云计算平台需要把 Neo4j 包装成独立的服务提供给租户使用，租户可以配置 Neo4j 的 XXX
扩容租户的 Neo4j 时，通过调用云计算平台的接口来实现。
删除租户的 Neo4j 服务能力，通过调用云计算平台的接口来实现

Storm 服务的多租户能力定义：
Storm

MySQL 服务的多租户能力定义：
MySQL 的多租户能力，通过为租户创建对应的 MySQL 数据库来实现，为一个租户创建一个对应的 MySQL 数据库，指定数据库的存储容量大小来给租户使用。
扩容租户的 MySQL 数据库服务能力，通过调整租户的 MySQL 数据库存储容量大小来实现，数据库本身一旦创建，则不能更改，除非删除租户的 MySQL 数据库服务能力。
删除租户的 MySQL 数据库服务能力，会把租户的对应 MySQL 删除，其中的表和表中的数据也会被删除。

Redis 服务的多租户能力定义：
Redis 的多租户能力，通过云计算平台提供，云计算平台需要把 Redis 包装成独立的服务提供给租户使用，租户可以配置 Redis 的 XXX
扩容租户的 Redis 时，通过调用云计算平台的接口来实现。
删除租户的 Redis 服务能力，通过调用云计算平台的接口来实现

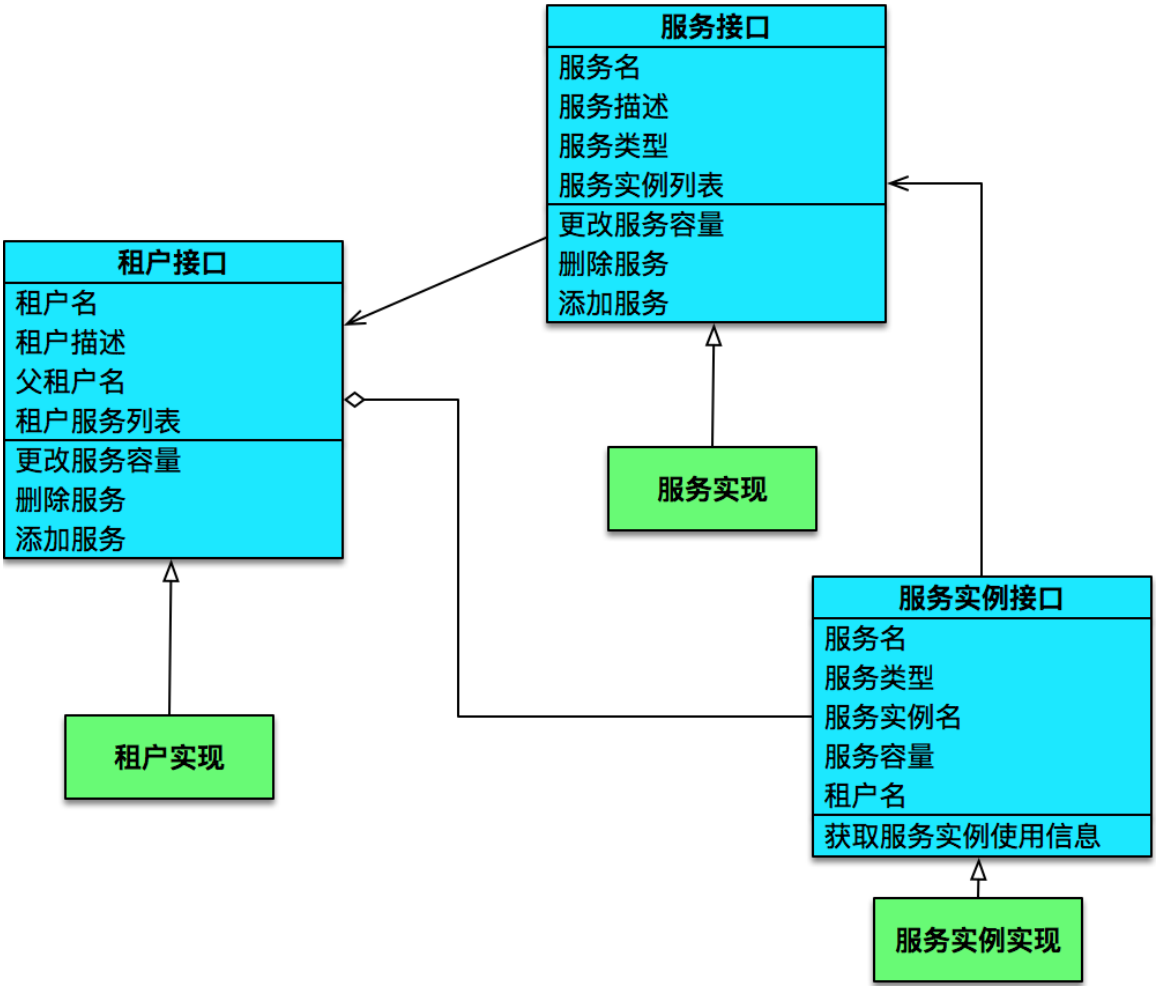
Postgres 服务的多租户能力定义：
Postgres 的多租户能力，通过云计算平台提供，云计算平台需要把 Postgres 包装成独立的服务提供给租户使用，租户可以配置 Postgres 的 XXX
扩容租户的 Postgres 时，通过调用云计算平台的接口来实现。
删除租户的 Postgres 服务能力，通过调用云计算平台的接口来实现

2.1.6.2 详细设计

详细设计使用多个章节对橘云多租户管理整个基础架构每一个部分的实现细节进行了详细的描述。

2.1.6.2.1 IT 基础服务能力的设计和实现

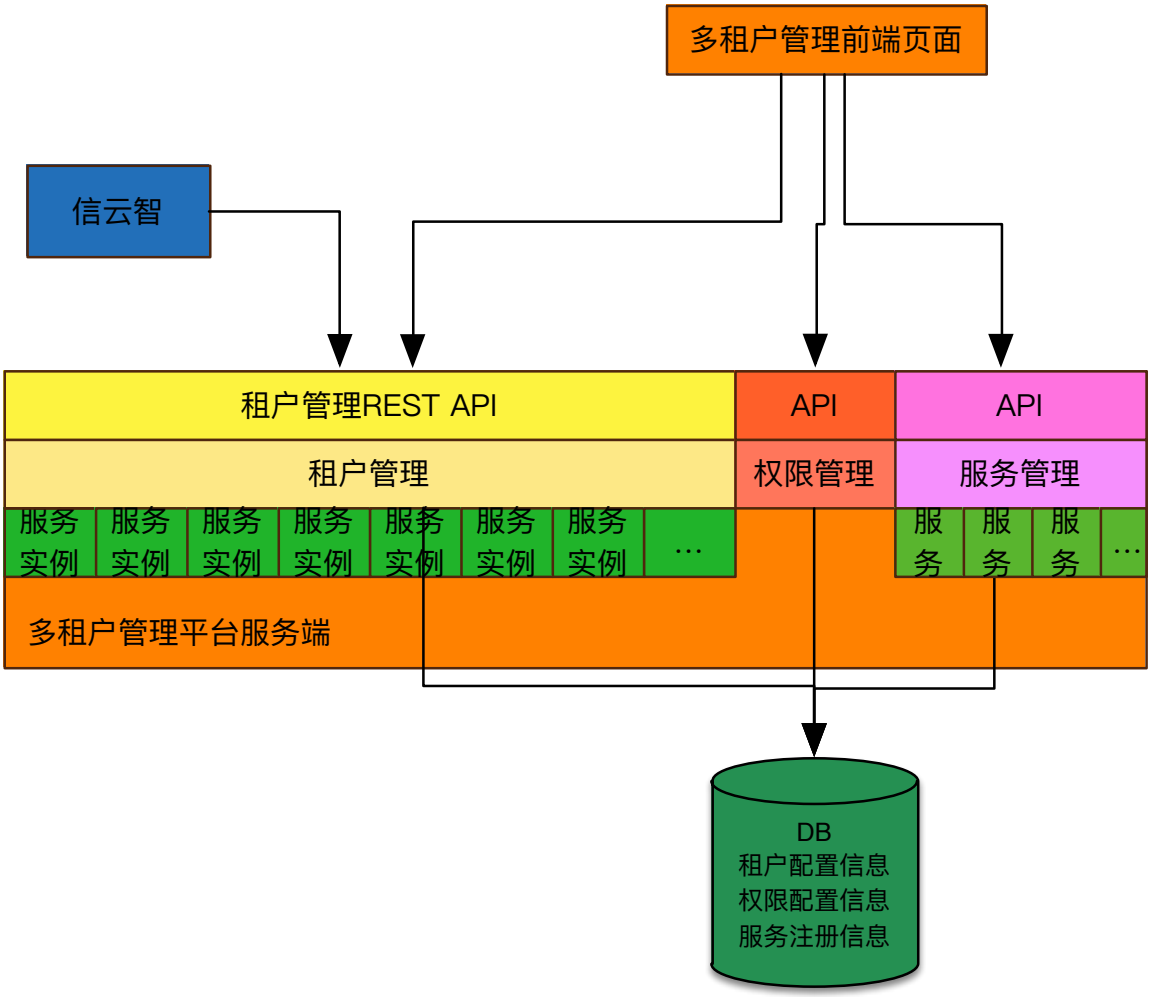
每一种 IT 基础服务能力，都会被包装成服务来给租户使用，为了满足租户的要求。需要为每一个服务开发相对应的适配程序，通过适配程序，可以把底层服务包装成多租户平台需要的服务格式，供租户管理平台灵活配置使用。以下类图是对这种关系的总结：



其中租户接口，服务接口和实例接口由橘云多租户平台来定义，每一个服务的适配程序要实自己的服务接口和服务实例接口。

2.1.6.2.2 橘云多租户管理服务端的设计和实现

请参考下图：



服务端包括了租户管理，权限管理和服务管理功能。租户的配置信息，权限的配置信息和服务的注册信息都会通过数据库来存储。

其中租户管理会将所有的服务实例，通过租户的方式来进行组织和管理。上层提供 REST API，外部用户可以使用 REST API 来创建一个租户，对租户的服务实例进行扩容，包括扩大容量或者给租户添加新的服务实例。

权限管理用来管理租户和用户之间的授权管理，根据目前的设计，多租户管理平台定义了三种角色，通过权限管理平台，只能给用户授权三种角色中的一种。这三种角色包括：系统管理员，项目管理员和团队成员：

系统管理员是一个超级用户，拥有对多租户管理平台上的所有租户，权限和服务的增删改查权限，并且可以给多租户管理平台上的所有租户，授权项目管理员和团队成员角色。

项目管理员对一个具体的租户，在多租户管理平台上，可以读取特定租户的所有信息，并且可以给一个用户授权团队成员角色。但是项目管理员在租户中所有创建的服务实例中，都有管理员权限。

团队成员角色在多租户管理平台上，只能读取特定租户的所有信息，无法做出任何修改操作。但是团队成员在租户中所有创建的服务实例中，都有只读权限。

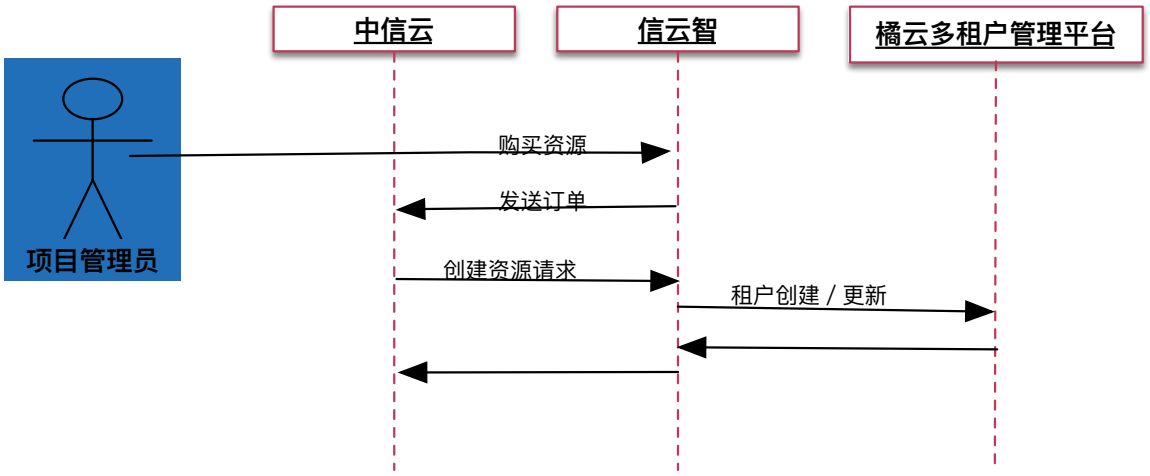
对于多租户管理平台，系统管理员是一个超级用户，会在系统中创建一个固定的账号，用户可以修改其密码，同时它也是多租户管理平台刚创建时的唯一一个账号，其他的账号，都是通过系统管理员来授权后，才可以在多租户管理平台上登录使用的。

橘云多租户管理平台的服务端，根据上图，会有如下几个模块：

1. 租户管理

   租户管理模块主要用来对租户进行增删改查操作。以下分别就租户的这四种操作进行介绍。

   首先，是租户的创建。创建租户的过程，会涉及多个外部系统，具体的交互过程如下图所示：



   项目管理员会通过信云智来发起资源购买的请求，

   - ✓ 信云智会有对项目管理员权限的检查，计费相关的检查，然后生成订单。
   - ✓ 订单会发送给中信云，由中信云来根据订单创建相应的资源购买请求，购买请求中会包含租户（可以理解为部门级租户，根租户）的相关信息，和项目的应用基线（可以理解为项目级别的租户，叶子租户）。
   - ✓ 购买请求会发送回信云智。
   - ✓ 信云智通过调用橘云多租户管理平台的 REST API，来实现真正的购买操作。
   - ✓ 橘云多租户管理平台，创建完租户后，会把租户的相关信息记录在自己的配置数据库中。

   整个交互过程中，涉及橘云多租户管理平台的部分主要是执行租户的创建和更新操作，多租户管理平台通过提供 REST API 调用来接收资源创建的要求，所有的操作都是通过信云智平台来发起。

   创建租户的 REST API 请求应该包含如下信息：

   - ✓ 租户 ID：租户的 ID 号码，如何通过 ID 获取租户的名字，租户的名字应该是部门级别的，体现在租户关系上，就是租户树上的根节点。
   - ✓ 应用基线：具体的项目，如何获取项目的名字，项目是具体使用资源的，体现在租户关系上，就是租户树上的叶子节点。
   - ✓ 服务类型：服务的类型名字，由多租户管理平台接入一个服务时，会指定一个服务名字，比如 HDFS，YARN，Hive，HBase 等。

- ✓ 服务容量：针对每一种服务，需要有一个对购买的服务的定量指标，因为服务类型不同，服务容量的具体指标也不一样，比如 HDFS，其服务容量包含：文件路径，空间配额，文件数；YARN 的服务容量包含：计算资源容量比例，最大容量比例，AM 资源占比等。每一种服务的容量信息定义，请参考上文。

2. 权限管理

权限管理在现阶段，主要体现在对三个角色的定义和对用户的授权上。如上文介绍，多租户管理平台目前指定了三种角色：系统管理员，项目管理员和团队成员。其中系统管理员是一个超级账号，~~在创建一个租户时，默认会给这个租户包含的每一个服务，授权一个超级管理员的权限，这个权限就会授予给系统管理员，所以系统管理员必须对应一个真实存在的用户账号 admin，这个 admin 账号名字是固定的，而且在每一种服务上，都应该存在这个账号，并且可以给其授权。多租户管理平台上不能再给其他用户授权系统管理员权限，但是系统管理员，可以给其他用户授权某个租户（这个租户包含租户树上的根节点和叶子节点）上的项目管理员或者团队管理员权限。其他用户只有在获得了相应的授权后，才能登录多租户管理平台并查看这执行自己权限相对应的操作，否则无法登录多租户管理平台。~~

默认多租户管理平台上会有一个系统管理员 admin，这个账号无法删除，但是可以更改密码。admin 这个账号登录后，主要用来给各级租户添加用户，并且授权角色。

项目管理员和团队成员，在多租户管理平台上，包含两类权限：

- ✓ 查看对应租户的所有信息。
- ✓ 给对应的租户添加团队成员。

多租户管理平台上所有角色的权限范围定义，参见下表：

权限	系统管理员	项目管理员	团队成员
给用户授权系统管理员	Y	N	N
给用户授权项目管理员	Y	N	N
给用户授权团队成员	Y	Y	N
查看租户基本信息	Y	Y	Y
查看租户服务列表	Y	Y	Y
查看租户资源报告	Y	Y	Y
查看租户用户列表	Y	Y	Y

所有角色，在其租户对应的服务上，具体的权限范围见下表：

服务	系统管理员权限	项目管理员权限	团队成员权限
HDFS		文件／文件夹的增删改查，文件的执行	文件／文件夹的浏览
YARN		作业的提交，查看，操作	作业的查看

Hive		数据库表的增删改查，表记录的增删改查	数据库表的查看，表记录的查看。
HBase			
Kafka			
Oracle			
GreenPlum			
MongoDB			
RabbitMQ			
Neo4j			
Redis			
Storm			
MySQL			
Postgres			

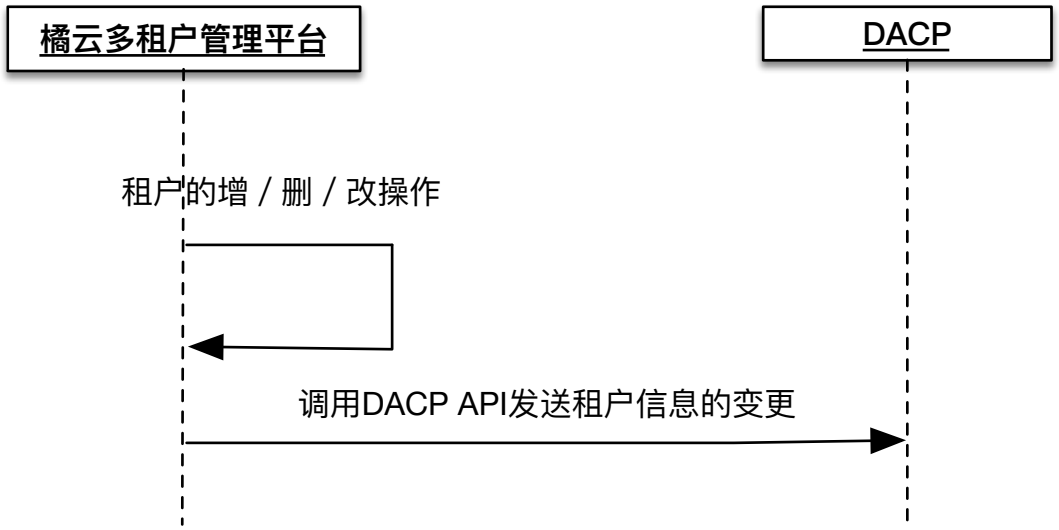
3. 服务管理

2.1.6.2.3 橘云多租户管理前端的设计与实现

2.1.6.2.5 橘云多租户管理与信云智交互流程的设计与实现

2.1.6.2.6 橘云多租户管理与 DACP 交互的设计与实现

橘云多租户管理平台与 DACP 之间的交互，由多租户平台调用 DACP 提供的 REST API 来实现。当橘云上的租户管理相关 API 被调用时，当发生租户的创建，扩容，删除操作时，橘云会调用 DACP 的 API 来通知 DACP 相关的租户信息变更结果。交互过程如下图所示：



具体的 API 由 DACP 来提供，详细要求如下：

1. DACP 提供 REST API，给出具体的 API 接口格式。
2. REST API 之间的数据传输采用 JSON 格式。
3. 橘云调用 DACP 的 REST API。
4. 橘云每次都将增量的租户信息传给 DACP
5. 橘云传递的租户信息包含：租户信息，用户信息，租户资源配置信息。
6. 橘云还要传递给 DACP，租户的各种资源的连接信息。

2.1.6.2.7 告警

2.1.7 接口需求

2.1.7.1 命令行接口描述

橘云多租户管理不支持命令行接口。

2.1.7.2 配置文件描述

2.2 用例

2.2.1 用例 1: 用户通过橘云多租户平台创建一个租户

用例描述：
前提条件：
使用步骤：
结果：

2.2.2 用例 2: 用户通过橘云多租户平台给一个租户添加用户，并分配权限。

用例描述：
前提条件：
使用步骤：
结果：

2.2.3 用例 3: 用户通过橘云多租户平台查看租户的资源使用情况。

用例描述：
前提条件：
使用步骤：
结果：

2.2.4 用例 3: 用户通过橘云多租户接入一种新的服务。

用例描述：
前提条件：
使用步骤：
结果：

2.3 非功能需求

2.3.1 性能

N/A

2.3.2 可扩展性

2.3.3 健壮性

2.3.4 安全性

Kerberos

2.3.5 可调试性

N/A

2.3.6 兼容性

- 只支持 OCDP4.0

2.4 附件