长江大保护时空大数据云平台建设方案研究

* 报告直接引用本报告样式，严禁使用或引用其他报告样式或模板
* 报告章节编号请严格遵照我院质量管理文件要求：



报告中单位统一用英文（m km m2 m3 hm2等），出现表、图的地方，正文中应写见表1.1-1、图1.1-1等



二零二零年九月

# 绪论（张钟海）

## 研究背景

## 研究意义

## 研究现状

### 长江流域信息化平台研究现状

#### 感知体系

##### xx

（1）xx

### 时空大数据云平台研究现状

### 研究现状总结

## 研究目标、内容及技术路线

### 研究目标

### 研究内容

### 技术路线

## 考核指标与完成情况

xx图

xx表

# 长江大保护时空大数据云平台建设需求分析

## 引言

## 长江流域管理涉及主要单位部门及其职责

## 长江流域信息化建设现状及存在的问题

## 长江大保护时空大数据云平台服务对象及范围

## 长江大保护时空大数据云平台业务需求

## 长江大保护时空大数据云平台功能需求

## 长江大保护时空大数据云平台数据需求

## 长江大保护时空大数据云平台安全需求

## 长江大保护时空大数据云平台性能需求

## 长江大保护时空大数据云平台非功能需求

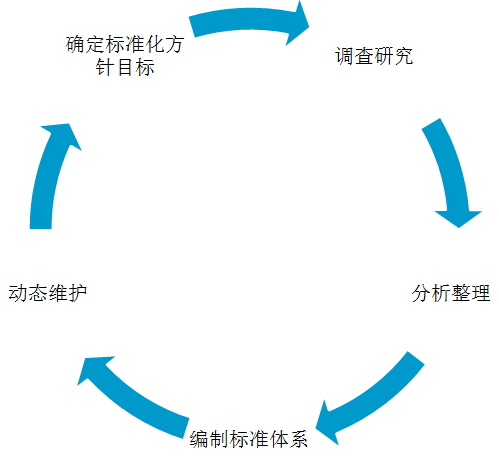
## 长江大保护时空大数据云平台建设目标及原则

# 长江大保护时空大数据云平台标准体系构建

## 时空大数据云平台标准体系（匡欢）

### 总体研究流程

构建标准体系是运用系统论指导标准化的一种方法。构建标准体系主要体现为编制标准体系结构图和标准明细表，提供标准统计表、编写标准体系编制说明，是开展标准体系建设的基础和前提工作，也是编制标准、修改规划和计划的依据。标准体系表是一定范围内包含现有、应有和预计制定标准的蓝图，是一种标准体系模型。如图3.1-1所示，总体研究流程包括确定标准化方针目标、调查研究、分析整理、编制标准体系、动态维护。详情如下：



研究流程

##### 确定标准化方针目标

（1）了解标准化所支撑的业务战略;

（2）明确标准体系建设的愿景、近期拟达到的目标;

（3）确定实现标准化目标的标准化方针或策略、指导思想、基本原则；

（4）确定标准体系的范围和边界。

##### 调查研究

进行标准体系的调查研究，包括：

（1）标准体系建设的国内外情况；

（2）现有的标准化基础，包括已制定的标准和已开展的相关标准化研究项目和工作项目；

（3）存在的标准化相关问题;

（4）对标准体系的建设需求。

##### 分析整理

根据标准体系建设的方针、目标以及具体的标准化需求，借鉴国内外现有的标准体系的结构框架，从标准的类型、专业领域、级别、功能、业务的生命周期等若干不同标准化对象的角度，对标准体系进行分析，从而确定标准体系的结构关系。

##### 编制标准体系表

编制标准体系表，通常报告：

（1）确定标准体系结构图

根据不同维度的标准分析的结果，选择恰当的维度作为标准体系框架的主要维度，编制标准体系结构图，编写标准体系结构的各级子体系、标准体系模块的内容说明。

（2）编制标准明细表

收集整理拟彩的国际标准、国家标准等外部标准和本领域已有的内部标准，提出近期和将来规划拟制定的标准列表，编制标准明细表。

（3）编写标准体系编制说明

标准体系表编制说明的内容一般包括：

a)标准体系建设的背景；

b)标准体系的建设目标、构建依据及实话原则；

c)国内外相关标准化情况综述；

d)各级子体系划分原则和依据；

e)各级子体系的说明，包括主要内容、适用范围等；

f)与其他体系交叉情况和处理意见；

g)需要其他体系协调配套的意见；

h)结合统计表，分析现有的标准与国际、国外的差距和薄弱环节，明确今后的主攻方向；

i)标准制修订规划建议；

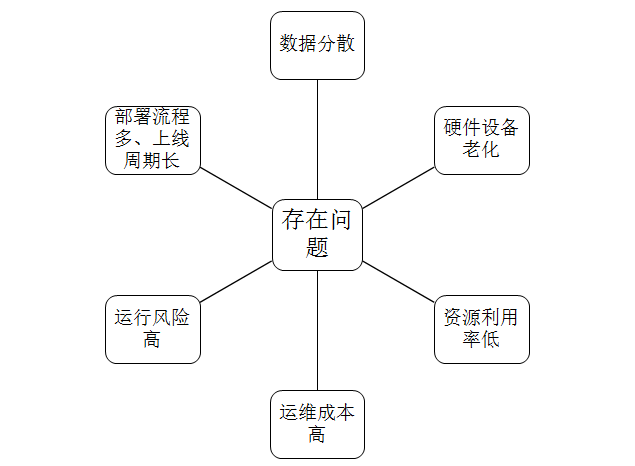
##### 动态维护更新

标准体系是一个动态的系统，在使用过程中应不断优化完善，并随着业务的需求、技术发展的不断变化进行维护更新。

### 初步分析

长江流域信息化的研究和建设取得了较大进展，沿长江流域的水利外网、水利专网、防汛骨干网、电子政务网已基本建成。各类雨量站、水位站、水情、旱情、水质站、取水口与排污口视频监测站也逐步完善，水情监测系统、防汛抗旱系统、水资源监控能力建设等核心业务应用日趋丰富。但各应用系统多局限于某个区域、部门或者业务，且存在信息资源共享困难、缺少业务协同、信息化管理机制体制不健全等问题。在长江大保护的背景下，长江流域已有信息化系统难以满足长江流域科学管理的需求，迫切需要一个统一管理平台来支撑长江大保护背景下的综合管理。

当前长江大保护时空大数据相关的系统，如图3.1-2所示，存在以下问题：



存在问题

##### 数据分散

当前长江大保护系统均采用物理硬件独立部署，增加了管理的复杂度，导致各系统成为信息孤岛，不能即时共享信息。同时由于历史原因，应用系统使用的数据库包括ORACLE、MYSQL、PROGRESQL、SQLSERVER等，并且相同的数据库使用的版本不同，数据无法集中管理，综合利用率不高，维护人员工作负担重。

##### 硬件设备老化

长江大保护应用系统设备投入使用年限过长，高比例的服务器存储设备在线运行超过5年，大部分已运行3年，设备老化的问题，越来越影响到业务系统的处理能力，无法满足现有的需求。

##### 资源利用率低

由于各应用系统独立部署，每个应用按照峰值进行硬件资源配置，导致大量的硬件资源并没有合理高效经济的利用。并且由于系统独立，分布在各单位，各部门，导致数据不能集中，与数据的挖掘设置了屏障。

##### 运维成本高

由于每个单位或部门建立了自己的应用系统，采用了专用的服务器、网络、操作系统、数据库、存储等软硬件系统，导致了场地投入、机柜投入、制冷设备投入、硬件投入、运维人员投入的重复投入，导致运维成本高。

##### 安全配置不足

当前的安全防御系统主要实现在物理服务器的场景，无法满足业务系统虚拟化的场景，无法实现应用层安全防御。

##### 运行风险高

为了满足政策法规、部门规章对于应用系统的安全性与合规性要求，运维人员进行了大量的工作以保证要求，但由于数量和业务众多，导致这一目标在实际当中难以实现。并由于运维人员的技术水平、工作效率上的差异，硬件条件的区别，导致实施结果存在很大的差异，从而带来各种风险。

##### 部署流程多、上线周期长

随着经济的发展，系统需求的不断演进，需要购置新的服务器，导致需要计划部门、采购部门、维护部门等参与，由于各部门的进度和流程不一致，经常导致部署流程多、上线周期长。

因此制定一套长江大保护时空大数据云平台标准体系很有必要性、迫切性、指导性、规范性作用。

结合需求、当前长江大保护信息化发展水平、未来发展需要，长江大保护时空大数据云平台标准体系包括政策法规、基础标准、专用标准大三模块。

### 编制方法

##### 工作计划制定

（1）任务分析与理解

理清编制目标和任务要求是做好标准制订的前提和基础。标准制订团队在负责人组织下共同参与学习讨论，对所要编制的标准总体目标和任务进行充分的讨论和深入理解，讨论过程都发表意见，统一了认识，形成了一个全面的共识。

（2）工作任务分解

对工作任务进行细化和拆分，分解到相对独立的子项任务。分解不能出现漏项，也不能包含不在任务范围之内的任何技术和要求。工作任务分解编制成了树形的电子文档。

（3）编制工作计划

工作计划内容包括：标准制度的总体目标和分项工作目标及阶段工作目标;任务的描述和质量要求;完成任务的支持条件;时间节点;责任人和配合人;形成了正式的文件。

##### 资料和信息的收集

（1）确定收集范围

依据标准编制的计划要求确定完成工作任务需要的相关资料和信息的范围、调研的对象、调研的方式、预设调研的题目，列出题纲。对调研的内容要依据编制原则的要求分裂出具体的调研点。

（2）调研方法

在调研阶段，为了标准制订的规范、全面、科学，收集信息采用现场调研、专家调研和文献查阅相结合的方式。

（3）信息处理

每一次的调研都编写了调研报告，完成调研后，将所有的资料和信息进行了汇总，分门别类的进行归纳总结，形成了最后的调研报告。

（4）信息分析

信息分析是为了全面的了解现状，包括国内外、行业内外的情况。在此过程中，一方面是找寻长处和不足，及存在的共性问题，另一方面通过对长江大保护时空大数据相关资料的学习，清楚明确对于时空、大数据、云平台三者相互之间的关系及相关技术的要求;再一方面对收集国内外、行业内外的相关标准特点进行分析，总结优劣，并与现状进行对比，确定需要改进的地方。对于信息分析过程中发现的潜在问题和不完善的地方，进行补充针对性的调研或信息的收集。

##### 标准的编写

标准编写采取分工编写共同讨论的方法。团队中每个人按各自熟悉的领域和专业特长，起草标准时充分发挥了组员的特长。共同讨论是为了多角度看问题，力争表述准确，用词规范，逻辑严谨。

标准编写的内容全面的遵守了标准编写的原则，充分体现行业特点。

对于长江大保护云平台现状存在的不足进行改善时，充分借鉴国内外、行业内外的先进经验，借鉴时十分清楚其规定的核心思想和要义。对相关内容完全适用的进行引用，与实际情况不同的不可直接引用，但借鉴他们的思想进行部分的吸收或转换表达方式。

##### 意见征询

标准起草后，为避免编写团队囿于经验、知识和能力方面的不足等客观存在的因素，造成标准编写存在缺陷、漏洞或错误，在行业内进行意见的征询。

（1）征询意见广泛

意见的征询做到较广泛，行业内相关单位，行业外信息化水平高的公司或单位，行业相关的高校，及相关领域的专家。

（2）反馈意见认真对待

反馈结束后，对反馈的意见进行了学习和讨论，采纳好的建议对标准进行改进和完善。

### 规范设计

##### 标准体系编码规则

依据编制原则和编制需求，结合长江大保护时空大数据云平台建设特点，制定长江大保护时空大数据云平台标准体系表编号规则，对列入技术标准体系中的每一项技术标准均赋予唯一的标准编号。编号规则采用结构编码+标准序列号的组合方式：

（1）结构编码分为：类别编号、子类别编号，每级结构编号由两位数字组成，当类别结构或专业结构需要扩充，可在已有结构编号基础上进行编号递增扩充，最多可扩充至99，当层级空缺时用“00”表示；

（2）标准序列号由三位数字组成，数字递增编码，当标准序列号需要递增，可在已有标准序列号基础上进行编号递增扩充，每级结构中的标准号最多可扩充至999。

##### 标准体系结构表及说明

|  |  |  |  |
| --- | --- | --- | --- |
| 编码 | 类别 | 子类别 | 说明 |
| 01 | 政策法规 |  |  |
| 01.01 |  | 国家法律法规 |  |
| 01.02 |  | 地方条例法规 |  |
| 02 | 基础标准 |  |  |
| 02.01 |  | 顶层设计 |  |
| 02.01 |  | 术语 |  |
| 03 | 专用标准 |  |  |
| 03.01 |  | 物联感知 |  |
| 03.02 |  | 网络传输 |  |
| 03.03 |  | 基础设施 |  |
| 03.04 |  | 数据资源 |  |
| 03.05 |  | 基础支撑 |  |
| 03.06 |  | 业务应用 |  |
| 03.07 |  | 信息化管理 |  |
| 03.08 |  | 信息安全 |  |
| 03.09 |  | 运维管理 |  |

长江大保护时空大数据云平台标准体系分类说明

### 成果内容

标准体系主要成果包括：标准体系结构图、标准明细表、标准统计表、标准体系编制说明。

#### 标准体系结构图

长江大保护标准体系结构图，如下图所示，分为:

##### 政策法规

包括：国家法律法规和地方条例法规，用于指导长江大保护云平台的工作的开展，确保系统建设在合规合法的前提下有序推进。

##### 基本标准

包括：顶层设计和术语，用于总体指导云平台工作开展。

##### 专用标准

包括物联感知、网络传输、基础设施、数据资源、基础支撑、业务应用、信息化管理、信息安全、运维管理。其中数据资源包括：数据分类与编码、数据存储模块、数据管理，用于规范统一相关模块的工作开展。

标准体系结构图

#### 标准明细表

#### 标准统计表

## 时空大数据云平台顶层设计

### 总体研究流程

### 初步分析

### 编制方法

### 规范设计

### 成果内容

## 时空大数据云平台术语

### 总体研究流程

### 初步分析

### 编制方法

### 规范设计

### 成果内容

## 时空大数据云平台共享交换数据服务目录

### 总体研究流程

### 初步分析

### 编制方法

### 规范设计

### 成果内容

# 长江大保护时空大数据云平台数据资源建设

## 资源汇聚

### 主要时空数据资源

#### 基础时空数据

#### 公共专题数据

#### 物联网实时感知数据

#### 互联网在线抓取数据

### 资源汇聚方式

### 数据库设计

#### 总体设计

#### 逻辑设计

#### 概念设计

#### 物理设计

## 空间数据处理

### 处理原则

### 处理流程

### 处理方法

## 数据引擎

### 引擎架构

研究矢量数据、影像数据在云平台中的组织和索引方式，提出一个私有云的地理数据存储体系，帮助用户在线调用现成的时空大数据中的数据

### 属性数据存储及索引

### 矢量数据存储及索引

### 影像数据存储及索引

### 数据安全设计

## 分布式管理系统开发

### 设计原则

### 系统架构

### 系统划分

### 模块设计

#### 动态数据获取

#### 数据管理

#### 分析量测

#### 模拟推演

#### 大数据挖掘

#### 大数据管理

### 接口设计

#### 外部接口

#### 内部接口

# 长江大保护时空大数据云平台运行环境保障

## 时空大数据运行服务设计

### 设计原则

### 总体设计

### 数据资源管理

### 资源可视化管理

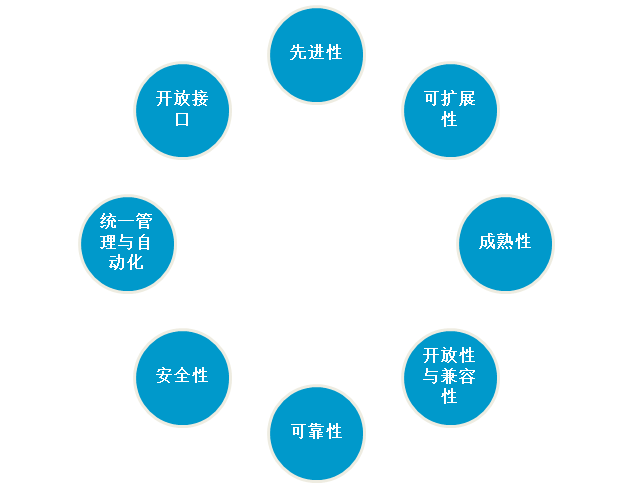
### 服务引擎设计

### 云端部署

## 云平台运行服务设计（匡欢）

### 设计原则

长江大保护云平台结合当前长江大保护信息化存在的问题和未来发展需要，在设计当中，遵守以下原则：



遵守原则

##### 先进性

广泛采用虚拟化、自动化调配等先进技术或模式，确保先进技术与应用模式的有效与适用。

##### 可扩展性

云平台支持资源，应能够根据业务应用运行的负荷需求进行伸缩，这样性能可以和服务水平的符合性保持适当。在系统进行容量扩展时，只需要增加相应数量的硬件设备，并在其上部署相应的资源调度管理软件和业务应用软件，即可实现系统扩展。

##### 成熟性

采用成熟的技术手段实现各种功能，满足相关部门的业务要求。

##### 开放性与兼容性

开放性是指源代码开放和标准开放。源代码开放，可以拥有完全的掌控，可以修改或增加新的功能满足自身的需求;标准开放意味着可以通过各种符合标准的产品构成自己的云平台方案。

采用业界通用的服务器，能够兼容主流的操作系统、虚拟化软件及应用程序，降低使用、管理、运维等成本。

##### 可靠性

充分考虑系统的高可用，系统在出现高并发达到瓶颈、出故障等问题时，能够较自动化进行伸缩、重启、切换、迁移，使得用户无感知，保证业务的稳定高效的运维，提高用户体验,资源的使用更合理。

##### 安全性

必须高度的防范网络入侵攻击、病毒感染，也需要对内部人员权限的管理，确保信息安全和私密性。

##### 统一管理与自动化

实现系统的按需运营，多种服务的开通，这依赖于对计算、存储、网络资源的调度和分配，同时提供用户管理、组织管理、工作流管理等。从IT资源的申请、审批到分配部署的智能化。管理系统不仅要实现对传统物理资源和新的虚拟资源进行管理，还要从全局而非割裂地管理资源。

##### 标准规范化原则

在云平台的建设、运维过程中，将依据国际、国内相关标准，避免采用私有的协议与标准，而导致互通困难。同时通过遵循统一的标准，实现资源共享、业务协同、安全可靠运转奠定坚实的基础。

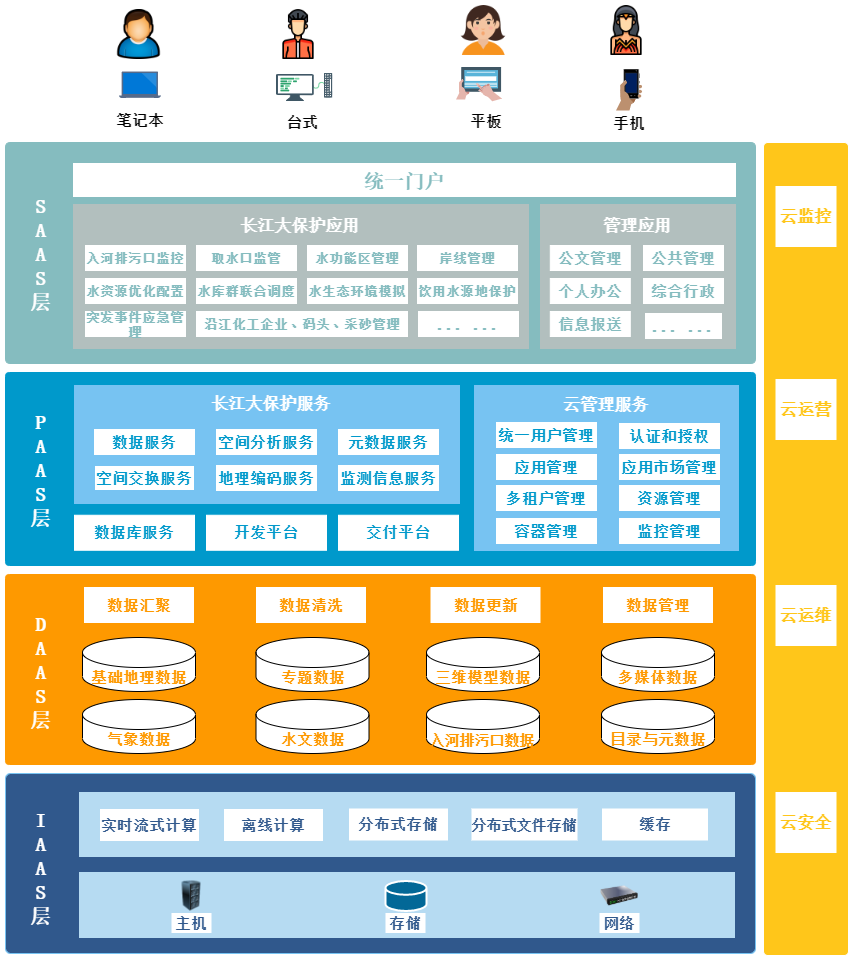
##### 开放接口

为保证服务器、存储、网络等资源能够被虚拟化运营平台良好的调度与管理，提供开放的API接口，能够通过API接口、命令行脚本实现对设备的配备与策略的下发联动。同时云平台提供开放的API接口，未来可以在这些接口的基础上进行再开发，实现面向虚拟化的数据中心管理平台。

### 总体设计

长江大保护时空大数据云平台使用四层架构设计，分别是SaaS应用层、DaaS数据层、PaaS平台层以及IaaS基础设施层。如图5.2-2所示。

IaaS层基于OpenStack、KVM虚拟化以及Ceph分布式存储技术，为业务系统提供基础承载平台。实现了存储资源、计算资源、网络资源的虚拟化。通过统一的接口，对这些虚拟资源进行集中的调度和管理。并在之上实现实时流计算、离线计算等分布式大数据计算技术，以及分布式存储、缓存等功能。



总体结构

DaaS层，提供基础地理数据、三维模型数据、多媒体数据等数据服务功能，并实现数据汇聚、数据清洗、数据更新、数据管理等功能。

PaaS层使用混合的PaaS架构，实现高可用架构的统一的云管理平台、运维体系、流程和工具、安全体系、数据存储、数据分析、文件存储等。

在安全方面，按物理安全、网络安全、主机安全、应用安全、数据安全进行设计。实现统一登录认证、认证和授权、单点登录的用户管理，在网络方面实现防火墙、流量统计、地址转换、VPN访问。应用和数据安全方面实现应用防火墙、流量监控、无代理病毒防护、敏感数据保护、全链接追踪、日志监控、性能监控等。运维管理方面，包括监控、交付、运维等功能。

SaaS应用层，用户通过统一门户可以使用公共管理、公文管理、个人办公、综合行政等管理办公应用，可以访问使用入河排污口监控、取水口监管、水功能区管理等长江大保护相关应用。

### IaaS层设计

基础架构即服务 (IaaS，Infrastructure as a Service) 提供托管的 IT 基础架构，供用户调配处理能力、存储、网络和其他基础计算资源。IaaS 提供运行并管理此基础架构，用户可以在此基础架构上运行选择的操作系统和应用程序软件。

#### laaS层结构

IaaS层基于OpenStack平台，结合KVM虚拟化技术以及Ceph分布式存储技术搭建云平台。实现虚拟计算服务、网络服务、对象存储服务、镜像管理服务、块存储服务及控制面板服务等服务。通过浏览器来对计算、存储和网络等资源的访问控制，如创建、启动、停止虚拟机实例、创建路由子网、设置安全组、虚拟机管理、认证管理、镜像管理以及计算资源、网络资源和存储资源的管理和调度等操作。

IaaS层建立了统一标准的信息化基础设施。通过资源池化技术和虚拟化技术。把硬件资源如服务器、存储设备和网络资源通过用户访问和需求动态计算的方式向辖区内各接入单位提供灵活多变的应用资源交付。用户不用担心服务器端硬件资源的维护和拓扑布局，可以实时自由访问所需要的资源。IaaS层提供了整个架构的物理基础稳定的同时，亦提供了可靠的可访问性和可维护性。

资源层将物理资源与PaaS应用业务解耦，屏蔽了节点之间的配置差异。资源层主要分为两部分：物理资源与虚拟资源。如图5.2-3所示。

物理资源层为平台提供了最基础的物理资源，包括主机、存储、网络及其他硬件在内的硬件设备，例如X86服务器集群、存储设备、交换机、路由器、物理资源负载均衡器以及防火墙等为云平台提供虚拟资源池的物理设备，是容器化云平台的基础和硬件条件。

虚拟资源层隐藏了物理资源的复杂性，实现了多种资源的虚拟化服务。通过对于多种资源的虚拟化整合技术，完成了集群资源的池化管理。虚拟资源层主要提供三种资源池：计算资源池、存储资源池和网络资源池。计算资源池中包括了各种不同配置的容器；存储资源池支持HostPath、NFS和Ceph这三种主流的持久化存储卷类型；网络资源池提供了相关的网络处理能力，如IP保持、网络限速及访问控制等。



IaaS结构图

#### 高可用设计

高可用是云平台必须考虑的重要问题，由于资源被整合在一起，一旦出现故障将影响整个平台的运行。云平台使用3+N的拓扑结构，即包含了3台控制节点， N台计算存储节点（N>=3）。该结构既可以为用户提供可靠的分布式存储，也能保证OpenStack服务的高可用性，也增强云平台的可扩展性。在集群服务方面，将OpenStack高可用集群化分为基础架构服务高可用（包括消息队列高可用、数据库高可用和缓存服务高可用）、控制服务高可用、网络服务高可用、存储服务高可用和计算服务高可用。实现高可用的方法使用Keepalived和HAProxy来实现。如图5.2-4所示。



OpenStack高可用节点部署图。

##### 控制服务、数据库和消息队列高可用

为了满足控制服务、数据库和消息队列高可用，设计部署三台服务器做控制节点。 OpenStack集群对外服务地址抽象层为一个虚拟IP地址，该IP的地址在Keepalived控制下实现控制节点之间的漂移，从而实现对外服务IP地址的高可用性。数据库以Galera实现高可用，采用MySQL和Galera组成三个Active节点，外部请求通过被Haproxy进行负载均衡后以轮询的方式进行，一个控制节点出现故障，则会在剩余的控制节点上轮询转发，从而实现高可用。消息队列以同步镜像的方式实现高可用，它的实现原理与数据库的原理一样。

##### 网络服务高可用

考虑到目前和未来很长一段时间内，集群规模都不是很大，L3高可用方案就可以满足网络高可用。在三个控制节点上同时部署L3Agent服务，当创建高可用L3Router时，同时运行L3Agent的多个网络节点上同步创建多个L3Agent实例，不同网络节点上的L3Agent完全相同，借助VRRP使得多个网络节点上的L3Router具有不同的运行状态，仅有一个L3Router是Master状态，而其它的都是Standby状态。由Master享虚拟机提供路由服务，当Master出现故障时，会重新从Standby中选举新的Master，从而实现L3高可用。由于使用Ceph分布式存储系统，后端的高可用就可以由Ceph集群通过三备份的方式解决。前端高可用由HAProxy实现，HAProxy进行负载均衡后转发，转发以轮询的方式进行，一个控制节点出现故障，则会在剩余的控制节点上轮询转发，从而实现高可用。

##### 计算服务高可用

计算服务是OpenStack私有云中最核心的服务，目前主流的计算服务高可用实现方案是Pacemaker\_remote。由于只能实现16个节点的高可用，对于虚拟机高可用来说，Pacemaker\_remote方案不能满足现实的要求。使用Docker容器化部署OpenStack，因为采用容器化部署，很容易发现计算节点故障。然后对计算节点进行周期性监测，发现故障后，通过Nova的EvacuateAPI进行虚拟机撤离，从而实现计算服务高可用。另外采用数据级的容灾方案，就能满足需求。由于使用Ceph分布式存储系统，可以使用Ceph的RBDMirroring异步备份技术，完成数据备份。

### DaaS层设计

数据即服务（DaaS，Data as a Service）是指与数据相关的任何服务都能够发生在一个集中化的位置，如数据的聚合、质量管理、清洗等，然后再将数据提供给不同的系统和用户，而不用再考虑这些数据从哪些数据源来的。DaaS层实现对基础地理数据、专题数据、三维模型数据及多媒体数据的集中管理，并开发服务及API供外部使用。

### PaaS层设计

平台即服务 (PaaS，Platform as a Service) 提供在集成式云环境中开发、测试、运行和管理 SaaS 应用程序所需的基础架构和计算资源。

PaaS 平台是基于底层不同云基础资源之上的一个开放、可运营、可动态扩展、易运维的云服务平台。实现对不同云基础资源统一化管理、第三方工具快速集成管理、应用产品快速部署管理、统一用户和应用管理、统一公告管理、平台运行状态实时监控等。为保证平台通用性，不受IaaS层限制，通过打造 PaaS 平台，实现对所有IaaS层基础服务统一封装和协议转换，适配不同云服务提供商的开发接口，为上下层平台提供一个标准化开发运行环境。

PaaS 平台层，把软件开发、测试和部署环境以服务方式对外进行提供。PaaS 平台层为各业务提供包括消息中间件、关系数据库、大数据框架、Window/Linux操作系统、开发环境(python、C、C++、Java、Go、nodejs)等在内的软件，允许进行应用远程开发、配置、部署。如图5.2-5所示。

PaaS服务层，采用混合型PaaS架构设计。其核心思路是基于统一的PaaS框架，提供适合不同业务需求的PaaS开发环境。针对无法改造的业务，提供VM模板和应用模板两种PaaS服务，让传统业务可以平滑迁移到云上。针对传统应用架构但可以优化改造的系统，采用CloudFoundry的PaaS服务。针对新开发的应用，采用基于Kubernetes的分布式容器服务PaaS服务，作为后续演进的统一的PaaS架构。

PaaS层主要分为两部分，云管理服务和长江大保护服务。

##### 云管理服务

Paas层云管理服务提供了应用管理、镜像管理、容器管理、应用市场管理、资源管理、审计管理、多租户管理和监控管理等多种管理和维护功能。如图5.2-6所示。



功能分解

* 1. 应用管理

应用管理为两类用户提供服务：PaaS运维管理人员和应用开发者。此模块为前者提供了必要的监控告警和日志管理等，提高了管理效率以及为应用的高稳定、高可靠性等提供了平台级的保障。应用管理为应用开发者提供了丰富类型的组件和应用运行环境，开发者可以更加专注于业务逻辑开发，进一步加快开发与发布应用的效率。

负载均衡管理：由于容器生命周期短暂，随时可能被删除和重建，是不稳定的对象，为了对外部提供更稳定的访问入口，让用户感知不到容器状态的变化，设计了负载均衡器模块。用户在访问容器服务的时候，访问的是负载均衡器的地址，由负载均衡器将流量转发到后端对应的一组容器当中去。

应用拓扑管理：为了让用户更好地了解应用内服务之间的依赖关系，每当应用发布后，会自动生成一个应用拓扑关系图。用户从应用拓扑管理中可以直观地查看应用中服务的关联关系。

服务和应用监控：PaaS平台需要随时了解应用和服务的实时健康状态，包括系统的性能指标以及应用指标。当应用异常时，会立即触发告警并帮助运维人员快速定位错误发生的位置及原因。

服务扩容：当服务在运行过程中需要增加容器实例时，服务扩容模块可以支持用户手动增加容器数量。容器关联的负载均衡器通过事件监听发现容器数量变化后，自动修改并重新加载配置，动态调整流量的分发策略。弹性伸缩：当业务需求变化后，弹性伸缩模块可以自动为用户调整物理计算资源量，在提高系统资源利用率的同时保证业务能够正常平稳地运行。

应用编排：应用编排是将一组关联应用组件自动整合为一个完整应用的过程，其目的就是将这些应用组件统一管理，统一监控。模板化的应用编排为应用开发者重用解决方案、快速发布应用提供了可靠的技术支持。

灰度升级：将正在运行的服务相关的容器逐个进行升级；针对不同的应用设置不同的滚动周期，逐一替换；升级过程中如果发生异常，可以对已升级的容器做回滚操作，确保服务的可用性。当需要对正在运行的应用进行升级时，为了保证服务不中断，需要进行灰度升级。

应用和服务的生命周期管理：提供了完整的应用和服务的生命周期管理机制，可监控应用和服务的创建、部署、启动、回滚，扩容缩容和停止下线等过程的状态。

（2）资源管理

PaaS平台的稳定运行离不开基础设施的支持，底层资源既可以是IaaS平台提供的虚拟化资源，也可以是数据中心直接提供的物理资源。资源管理模块的主要功能就是对底层资源进行整合，并建立其与容器的映射关系，解决运行容器应用所依赖的物理机计算、存储、网络等，简化了创建和维护容器化应用的难度。

主机管理：负责对接多种不同类型的主机，包括各种云平台的虚拟机、自有的物理机等。支持查询集群中管理的主机列表，每台主机的状态、操作系统、使用的Docker版本、主机上运行的容器列表等。

存储管理：支持为PaaS平台添加多种不同类型的存储池。容器需要使用共享存储卷持久化数据时，从存储池里创建存储卷，挂载给容器使用。同时还提供文件管理器，容器中的应用可以直接对存储卷中的数据做操作，比如上传文件、下载文件、编辑文件、移动文件等等。网络管理：支持为PaaS平台对接多种不同类型的网络插件，如Calico、Flannel以及作者设计的Xanet插件等，这些插件将在以后的章节详细介绍。

（3）镜像管理

镜像是容器技术的核心之一。镜像管理模块应用Docker容器技术把应用及其所依赖的软件包、操作系统文件等封装在镜像文件中，使应用在开发、测试和发布过程中具有相同的运行环境。管理镜像仓库和其中的镜像也是PaaS平台需要提供的功能。

镜像仓库：包含所有平台中提供的镜像。无论发布镜像，还是下载镜像，都要通过镜像仓库来完成。镜像仓库和租户体系相结合，可对仓库中的各种操作鉴权，使用角色限制用户对镜像的操作权限。

镜像构建：支持用户在PaaS平台利用DockerBuild命令在线构建新的镜像。把Dockerfile及其依赖的安装包、可执行文件等压缩成tar包，提交到Docker服务中构建镜像，最后把构建好的镜像上传到本地的镜像仓库中。

镜像管理：提供Docker镜像的管理功能，例如镜像权限管理，多租户间镜像隔离，镜像版本查询等。除此之外，还可以统计topN镜像、配置备份仓库中的镜像做定时同步、导入外部镜像到本地仓库中等。

镜像仓库管理：与镜像管理类似，不过管理的对象由单个镜像变为整个镜像仓库。系统默认为每个租户创建一个镜像仓库，镜像仓库中的镜像默认是私有权限，只对本租户下的用户可见。管理员可以修改镜像属性为公开，提供镜像给租户外部的用户使用。

（4）应用市场管理

PaaS平台提供了功能强大的应用市场支持，把常用的Mencache集群、MySql集群、Redis集群、Tomcat等封装成模板，普通用户可以自由选择这些独立的组件模板构建应用；同时也提供了大量经过验证的微服务集群应用，为用户获取和分享业务组件提供了技术手段。

应用市场管理包含大量经过验证的微服务集群应用软件，支持用户快速获取和分享业务组件。容器管理主要负责容器运行过程中的展示、监控、迁移以及容器中数据的持久化。多租户管理可有效隔离多个具有不同权限租户之间的应用状态和数据。监控管理对平台中容器、主机、应用的重要指标进行监控，并汇总监控结果生成报表，辅助系统快速找出故障原因及位置。

（5）容器管理

在PaaS平台当中，应用、运行环境软件、系统文件等被封装在容器的镜像中。启动镜像后，容器成为一个镜像的实体，业务就运行在其中。所有的容器都必须属于某一个服务，不允许对容器进行单独的申请和特殊操作。PaaS平台中的容器管理模块主要负责管理容器的运行情况，以及容器和服务之间的依赖关系。

容器控制台：在门户提供控制台功能，普通用户可以在控制台中执行命令，相当于用户直接登录到容器的操作系统中执行命令。容器控制台功能使用websocket实现，使用websocket建立门户和后台服务的双工通信，把用户的操作封装后发送到后台服务，把容器的响应封装后推送到门户中做展示。

容器监控：支持容器级别的性能监控，主要监控容器的CPU、内存、存储和网络信息。容器监控通过cAdvisor实现，进行原始的数据采集，监控服务在每个采集周期内调用cAdvisor接口查询原始数据，并对原始数据做处理和汇聚，处理后的数据提供给Grafana做展示。容器列表：支持多维度的容器列表展示，包括应用下的容器列表、服务下的容器列表和主机下的容器列表。

容器网络：容器网络使用Docker的none模式，容器创建时只创建一个空的网络命令空间，由网络插件设置容器的网络命令空间参数，对容器分配IP，保证容器到主机、容器到容器之间的网络通信。

容器迁移：容器迁移的目标是使容器在不停止业务运行的前提下，从一台主机迁移到另一台主机。由于容器本身不支持迁移操作，作者选择了一种折中的实现方案，当容器要迁移时，先在目标主机上创建一个相同的容器，然后等容器正常工作后更新负载均衡器，把新创建的容器接入到负载均衡器，把旧的容器从负载均衡器上删除。最后删除旧的容器。

容器持久化：容器持久化利用共享存储实现。容器启动时候挂载共享存储卷到容器中使用，需要持久化的数据写入共享存储卷，保证容器停掉或迁移后数据不会丢失。

（6）多租户管理

对于一个企业级的PaaS平台来说，多租户架构不仅能够降低服务的开发成本与运维成本，还可以让企业内不同部门的授权用户独立创建并管理自己的应用。当应用服务运行时，租户之间的状态和数据都是隔离开的，对于租户来说，自己是独享服务的，租户是可以持有资源的最大单位。

租户管理：负责创建新租户，将租户与机构绑定或解绑，访问查询租户信息等操作。管理的租户信息包括基本信息，成员信息，权限等级，所属机构等。

用户管理：负责创建新用户，将用户与机构绑定或解绑，设置用户角色，访问查询租户信息等操作。管理用户的基本信息，例如登录名，密码及其它个人信息等。用户和租户使用角色关联，每个用户登录后可以看到所属租户下的资源信息，可以对所属租户下的资源进行操作。

组织机构管理：分级管理全部租户的应用权限，包括普通用户、普通管理员、以及超级管理员。普通用户可以对所属租户下的资源进行操作。普通管理员除了管理当前租户的资源外，也同时管理本租户下的用户信息，修改用户的权限信息。超级管理员管理集群中的所有资源，同时管理所有的租户和用户信息。

用户权限管理：设置并管理租户，权限和角色的映射关系。根据用户和租户的权限内容授予其不同的资源操作权限。

（7）监控管理

监控管理主要负责PaaS平台中各种资源的监控管理，并支持查看资源和应用的各种指标，例如负载指标、服务指标等。同时可以自定义指标的汇总方式，设置相关告警，帮助运维人员快速定位故障及解决故障。容器监控：与容器管理中的容器监控相同。

服务器监控：定时从服务器拉取服务器的CPU、内存、存储、网络等指标数据。运行在主机上的node-exporter进行原始的数据采集，监控服务在每个采集周期调用接口获取指标数据，数据处理和汇聚后提供给Gafana做数据展示。

应用监控：使用特定的应用监控exporter实现。每种exporter采集特定应用的指标，如mysql-exporter负责采集MySql数据库的连接数、每秒事务量等；redis-exporter负责采集Redis的内存使用率、延迟时间等。部署应用时，如果用户选择需要采集应用指标，PaaS平台除了部署应用本身外，也会部署应用指标采集的exporter。监控服务通过定时调度，定时通过特定的exporter采集指标数据，数据处理和汇聚后提供给Grafana做展示。

指标管理：负责接收性能指标数据，如容器、服务器、节点、CPU和内存的利用率、硬盘存储量、磁盘读写和网络速率，系统IP数，吞吐量以及集群整体的各项指标，并提供查询和展示的功能。

监控汇总分析：支持用户在平台中自定义如何处理原始指标数据，比如采集周期的长短，多条应用指标以哪种方式汇聚，使用原始指标生成复杂的报表指标等。处理后的指标依然和原始指标一样可以被查询和使用。

监控告警：通过配置告警规则，当如存储、CPU使用量、网络、内存等超过告警规则临界值时，触发告警，通过webhook方式，通知相应工作人员。

（8）数据引擎管理

针对传统数据库和大数据两种数据类型的功能，提供Oralce、My SQL、Postgresql、MongoDB、Hadoop、Spark、Flink、Storm等技术。

大数据分析引擎作为 PaaS 平台基础服务能力，处于 PaaS 平台核心应用层，可与 PaaS 平台消息引擎、用户管理、基础服务能力管理、云管理中间件无缝结合，为 SaaS 层业务系统提供统一的数据处理能力，大幅提升SaaS层业务系统数据处理效率。利用OpenStack中的Sahara组件实现在OpenStack云环境中简单、快速地部署并管理Hadoop集群，集成Hadoop可以向上提供和扩展理高效的大数据存储、大数据安全备份、大数据处理分析等服务。

##### 长江大保护服务

PaaS层长江大保护服务，提供了数据服务、空间分析服务、元数据服务、空间交换服务、地理编码服务等服务。

### SaaS层设计

软件即服务 (SaaS，Software as a Service) 使用户可以通过 Internet 访问软件应用程序。用户不必购买并在自己的计算机或设备上安装、更新和管理这些资源，而可以通过Web 浏览器访问并使用它们。SaaS 提供商在云中为用户管理软件、处理能力和存储。大多数 SaaS 解决方案在公共云中运行，并以订阅或免费服务的形式提供

SaaS应用层包括两方面内容 ：一是应用服务产品体系 ，应用服务须支持多租户、可配置、可扩展、网络化 ；二是服务运营管理体系，服务须安全稳定，支持产品管理、终端管理、用户管理等功能。在 SaaS 应用层提供智能汇聚、融合生产、内容库管理、内容发布、全媒体业务协同指挥等模块。这一层是通过网络浏览器来接入 ，在远程服务器上的任一应用都可以通过网络来运行。通过这种模式 ，不需要顾虑类似安装等琐事 ，能够方便用户使用 ，并提供一定的可定制性以满足用户的特殊需求。

平台门户主要分为三个部分：运营门户、运维门户和开发者门户，分别对应PaaS平台不同的使用对象，为他们提供了更直观的系统信息内容整合。平台门户帮助使用者快速获取平台、集群资源和应用服务的使用情况和运行状况。

### 运行环境要求

#### 软硬件要求

云平台相关的软件、服务器CPU、内存、硬盘等的要求如下：

##### 部署服务器要求

CPU：支持基于Intel VT /AMD-V以上X86指令集架构的处理器；

内存：单条内存8G，16G，32G，选用DDR4接口标准为最佳；

机械硬盘：需要支持SATA，SAS硬盘接口；

SSD硬盘：对IO要求高的应用需要配置SSD盘，支持SATA或PCI-E接口；

网络：每台服务器至少三块网卡，网卡需要支持1GbE/10GbE/infiniband，根据不同需求选择不同网络。

##### 推荐配置

服务器：6台, CPU E5-2620V3\*2

内存：DDR4 16G\*16

万兆网卡：双口万兆网卡\*2

千兆网卡：双口千兆网卡\*1

系统硬盘：SAS 300G\*2

硬盘：SATA或SSD 4T\*12

交换机：管理网有带外管理口48口千兆交换机；计算网使用48口万兆交换机（支持堆叠）

##### 组件列表

云平台所需组件如下表5.2-1所示：

|  |  |
| --- | --- |
| 组件 | 说明 |
| OpenStack版本 | Victoria |
| 操作系统 | CentOS7.4及以上 |
| 虚拟软件 | KVM |
| 数据库 | MySQL |
| 消息队列 | RabbitMQ |
| 高可用 | HAProxy、Keepalive |
| 应用容器引擎 | Docker |
| 容器集群管理 | Kubernetes |
| 镜像仓库 | Harbor |
| 自动化运维工具 | Ansible |
| 日志监控 | Elasticsearch、Kibana、Logstash、Kafka |
| 性能监控 | Promethues、Grafana |
| 网络监控 | Skydive |
| 网络隔离 | VxLAN |
| 网络服务 | Neutron |
| 分布式存储 | Ceph |

组件列表

#### 机房环境要求

机房环境对于云平台的稳定、安全、可靠取着至关重要的作用，云平台机房要求有接地系统、电气系统、照明系统、应急系统、机房空调系统、送排风系统、设备集中监控系统、KVM管理系统、自动灭火系统、综合布线系统等配置。对于机房污染物、温度等的具体要求如下：

##### 污染物。

远离腐蚀气体、易燃易爆物；腐蚀气体随着新风吸入机房后会对计算机设备和人员健康造成危害，同时不洁净的空气也会对计算机设备的运行造成不利影晌，还会对机房内精密空调、新风机等的滤网等造成污染。

##### 温度、湿度。

温度和湿度必须被严格控制，以提供可连续运行的温度和湿度范围。干球温度计:20℃~25℃(68F~77F)。相对湿度:40%~50%。最大露点:2l℃(69.8℉)。最大变化速度:每小时5℃(9℉)。

##### 噪声。

计算机系统停机时，机房内的噪声在主机房中心处测试应小于6SdB(A)。

##### 照度。

计算机机房在距地0.8m处，照度不应低于3001x，辅助房间照度不低于2001x。

##### 其它

无线电干扰场强。在频率为0.15~1000MHz时不大于126dB。

磁场干扰场强不大于800A/m。在计算机系统停机条件下，主机房地板表面垂直及水平向的振动加速度值不应大于5OOmm/s。

主机房地面及工作台面的静电泄漏电阻，应符合现行国家标准GE6650一1986《计算机机房用活动地板技术条件》的规定。

主机房内绝缘体的静电电位不应大于lkV

### 安全保障要求

对于云平台的安全要求从虚拟安全、网络安全、应用安全、主机安全和数据安全五方面进行规范。

#### 虚拟安全

（1）虚拟机基础安全应符合以下要求：

a)应实现平台虚拟主机的访问控制和身份鉴别；

b)应在本地或外部设备上对虚拟机的日志记录进行输出、存储，并及时、定期审计；

c)应提供实时的虚拟机监控机制，可以通过带内或带外的技术手段对虚拟机的运行状态、资源占用、迁移等信息进行监控，并提供可视化的监控结果；

d)应确保虚拟机的镜像安全，并保证提供虚拟机镜像文件完整性校验功能，防止虚拟机镜像被恶意篡改，采取有关措施保证逻辑卷同一时刻只能被一个虚拟机挂载。

（2）虚拟机配置与加固应符合以下要求：

a)应通过及时更新虚拟化软件补丁，提供虚拟化主机的安全；应考虑对非工作状态的虚拟机镜像进行补丁操作或者对刚刚运行的虚拟机采取保护措施，直到它们被打上补丁；

b)应通过对平台的资源监控管理，控制虚拟机所消耗的服务器资源，保障受到攻击的虚拟机不会对在同一台物理主机运行的其他虚拟机造成影响；

c)应限制虚拟机到物理主机的通信，防止拒绝服务攻击。

（3）虚拟机安全防护应符合以下要求：

a)应实现常见针对虚拟机的恶意攻击的安全防护；

b)应避免虚拟机共同体之间通过共同访问资源进行恶意攻击；

c)应提供虚拟机跨物理机迁移过程中的保护措施；

d)应提供虚拟机镜像文件加密功能，防止虚拟机镜像文件数据被非授权访问；

e)应可以对虚拟机模版文件、配置文件等重要数据进行完整性检测。

（4）物理主机上的多个虚拟主机应隶属同一个安全区域，禁止跨安全域部署，应提供虚拟主机之间隔离服务。虚拟主机隔离应符合以下要求：

a)应根据安全等级，关闭或拆除主机的光盘驱动、USB接口、串口等接口；

b)应提供存储空间级安全隔离，租户应可以建立不同安全等级的安全存储空间；

c)应设置隔离措施实现虚拟机资源之间的安全隔离：应提供CPU调度隔离、内部网络隔离、不同虚拟机的内存隔离、不同虚拟机的存储隔离；

d)应只允许符合安全策略的虚拟机之间实现相互访问资源。

e)虚拟主机之间的信息交互应按其安全属性要求选择建立VPN安全通道、身份认证或访问控制；

（5）虚拟主机的远程管理应符合以下要求：

a)当对平台虚拟主机进行远程管理时，应采取必要措施，防止鉴别信息在网络中传输被窃听；

b)对虚拟主机的远程访问应采用安全协议。

#### 网络安全

网络访问控制应该符合以下要求：

（1）应根据业务需求在网络内划分不同的域，不同的域之间启用边界访问控制, 应设置统一的网络访问策略，按照安全域安全级别进行严格访问控制。

（2）应利用虚拟防火墙功能，实现虚拟环境下的逻辑分区边界防护和分段的集中管理与配置。

（3）应在创建客户虚拟机的同时，根据具体的拓扑和可能的通信模式，在虚拟网卡和虚拟交换机上配置防火墙，提高客户虚拟机的安全性。

（4）虚拟交换机应启用虚拟端口的限速功能，通过定义平均带宽、峰值带宽和流量突发大小，实现端口级别的流量控制，同时应禁止虚拟机端口使用混杂模式进行网络通信嗅探。

（5）外部用户通过互联网访问平台中设备时，应设置严格访问控制机制，且提供相对安全的访问通道，例如通过VPN方式。

#### 应用安全

（1）业务系统安全应符合以下要求：

a)业务系统试运行前应经过安全检查与安全扫描，通过后再接入平台。

b)业务系统应优先部署在虚拟机环境中。

c)业务应用迁移应事先做迁移方案，并对风险和资源做评估；

d)核心业务节点应在安全域内受控迁移，不能在安全域间迁移；

e)重要业务节点可在安全域内自由迁移，不能在安全域间迁移；

f)一般业务节点可在安全域内自由迁移，应在安全域间受控迁移；

g)不同安全级别的资源池之间禁止业务迁移；

h)关键平台支撑节点不可迁移。

i)应对业务系统运行过程进行监控，详细记录系统运行过程中网络通信，资源请求和使用等的信息，并进行审计。

（2）业务资源安全应符合以下要求：

a)应能够对业务应用系统的最大并发会话数进行限制；

b)应能够对单个账户的并发会话进行限制；

c)应提供服务优先级设定功能，可以根据安全策略设定访问账户或请求进程的优先级，进而根据优先级分配系统资源；

d)业务虚拟资源应安全可控，虚拟资源的接入应提供身份认证和访问控制措施。

（3）业务与数据隔离应满足以下要求：

a)应对虚拟机进行加固，保证不同主机之间的数据处理隔离；

b)应对新上线应用和已有应用提供数据层的数据隔离，并通过配置虚拟资源隔离系统实现；

c)应提供有效的虚拟机间内存隔离等机制，避免来自同一宿主机上的其他虚拟机破坏数据完整性；

d)不同用户数据应采用不同密钥进行加密隔离；

e)不同安全域及部门专属业务域之间应实现配置化的跨域认证与授权；

f)应对平台所部署的应用建立针对安全域之间、应用服务器之间通信的密钥服务管理系统；

（4）应提供统一身份认证服务，为业务应用用户分配不同的资源及操作权限访问云资源。该服务应满足以下条件：

a)应提供用户注册服务：用户在统一身份认证服务中注册帐号，这个帐号可以在所有使用统一身份认证服务的应用系统中使用。

b)应提供帐号关联服务：如果用户之前已经在相关的应用系统中拥有帐号，同时也已经设置了相应的权限，那么用户能够将这些应用系统的帐号与统一身份认证服务的帐号进行关联。

c)应提供用户认证服务，为应用系统提供用户身份认证。

（5）云平台应根据云资源的不同，提供不同的访问控制服务，包括自主访问控制，强制访问控制和基于角色的访问控制。访问控制服务应满足以下要求：

a)自主访问控制安全策略应实现对主体与客体间操作的控制。可以有多个自主访问控制安全策略，它们应独立命名，且不能相互冲突。常用的自主访问控制策略包括：访问控制表访问控制、目录表访问控制、权能表访问控制等。

b)强制访问控制策略应包括策略控制下的主体、客体，及主体与客体间的操作，按照多级安全模型策略进行访问控制授权管理。

c)基于角色的访问控制应实现按角色进行权限的分配和管理：通过对主体进行角色授予，使主体获得相应角色的权限；通过撤消主体的角色授予，取消主体所获得的相应角色权限。

（6）云平台应根据云资源的不同，提供不同的数据安全服务，包括数据完整性安全服务，数据机密性安全服务和数据备份回复服务。主要服务应满足以下要求:

a)应可以对存储在安全域内的用户数据进行完整性检测；

b)应可以对被传输的用户数据进行完整性检测，及时发现用户数据被篡改、删除、插入等情况发生。

c)应可以对存储在安全域内的用户数据进行保密性保护；

d)应可以对在安全域内传输的用户数据进行保密性保护。

e)应提供数据本地备份与恢复功能，完成数据备份至少每天一次，备份介质场外存放。

（7）系统安全服务应满足以下要求：

a)主机加固服务：针对不同目标系统根据主机所承载的应用进行专业的安全评估，并进行恰当的安全配置，通过打补丁、修改安全配置、增加安全机制等方法，合理进行主机安全性加强或者消除等的服务；

b)操作系统防病毒服务：针对指定操作系统安装多重病毒防护组件，组织多种类型病毒的入侵，增强操作系统自身的安全性的服务。

c)跨域认证服务：提供统一用户数据管理，并且提供统一用户认证服务入口；在区域网络畅通且无阻碍的情况下，支持多区域统一用户认证；

d)应用系统授权管理服务：对接入的应用系统，提供应用系统业务访问级权限管理；

#### 主机安全

主机安全应满足以下要求：

（1）身份鉴别

a) 应对登录操作系统和数据库系统的用户进行身份标识和鉴别；

b) 操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换；

c) 应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

d) 当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听；

e) 应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性。

f) 应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。

（2）访问控制

a) 应启用访问控制功能，依据安全策略控制用户对资源的访问；

b) 应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；

c) 应实现操作系统和数据库系统特权用户的权限分离；

d) 应严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令；

e) 应及时删除多余的、过期的帐户，避免共享帐户的存在。

f) 应对重要信息资源设置敏感标记；

g) 应依据安全策略严格控制用户对有敏感标记重要信息资源的操作；

（3）安全审计

a) 审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户；

b) 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；

c) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；

d) 应能够根据记录数据进行分析，并生成审计报表；

e) 应保护审计进程，避免受到未预期的中断；

f) 应保护审计记录，避免受到未预期的删除、修改或覆盖等。

（4）剩余信息保护

本项要求包括：

a) 应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

b) 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。

（5）入侵防范

a) 应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；

b) 应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施；

c) 操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。

（6）恶意代码防范

本项要求包括：

a) 应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；

b) 主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库；

c) 应支持防恶意代码的统一管理。

（7）资源控制

a) 应通过设定终端接入方式、网络地址范围等条件限制终端登录；

b) 应根据安全策略设置登录终端的操作超时锁定；

c) 应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况；

d) 应限制单个用户对系统资源的最大或最小使用限度；

e) 应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。

#### 数据安全

（1）数据安全应符合以下要求：

a) 应采用密码技术或其他措施保证数据的完整性。

b) 应采用加密技术对存储和传输中的敏感数据进行机密性保护。

c) 应能够提供手段清除因数据在不同物理服务器上迁移、业务终止、自然灾害、合同终止等遗留的数据；

d) 应提供不同平台间的数据迁移能力；

e) 数据迁移应制定迁移方案，并进行迁移方案可行性评估与风险评估，确定数据迁移风险控制措施，做好数据备份以及恢复相关工作，应保证数据迁移不影响业务应用的连续性；

f) 应避免敏感机密数据的复制和物理迁移

g) 应采用访问控制技术对数据进行分类保护。

h) 应提供数据备份与恢复功能。

（2）业务调度安全应符合以下要求：

a)应赋予不同的用户不同的服务优先级；

b)应根据用户的优先级高低安排服务，不可跨优先级服务；

c)应能对用户的优先级进行实时控制和管理。

# 长江大保护时空大数据云平台高效管理及智慧应用

## 长江大保护信息管理与服务支撑平台高效管理要求

### 数据资源建设要求

### 模型建设与管理要求

### 资源统一管理要求

## 长江大保护时空大数据云平台高效管理要求（匡欢）

### 信息共享与高效分发要求

信息共享与高效分发要求参照标准 GB/T 30850.4—2017。信息共享技术层面涉及网络、系统、安全、管理等方面的要求。

##### 网络要求

信息资源共享网络要求如下：

（1）非涉密的业务信息应通过国家电子政务外网传输；

（2）公开信息可通过互联网传输的信息共享；

##### 数据要求

（1）数据内容

信息资源共享应从语义层面对数据内容进行规范，要求如下：

1. 元数据：关于数据的数据，应规范数据的标识、内容、分发、数据质量、数据模式、图示表达、限制和维护信息。通用政务信息资源应遵循GB/T 21063.3—2007第5章的要求，特定领域如地理空间信息资源应遵循GB/T 19710—2005第6章的要求。
2. 标识符：对共享数据进行唯一标识，数据标识符不可重复，宜参照GB/T 18391.5—2009中的要求执行。
3. 分类：应根据信息内容的属性或特征，将信息按一定原则和方法进行区分和归档，并建立起一定的分类体系和排列顺序。宜参照GB/T 7027—2002第5章的原则并参照GB/T 21063.4—2007第5章确定。
4. 指标：用来描述某一类考察对象的特定属性的一个或多个名称及其量化数值，应科学合理、具有一定的稳定性。
5. 数据元：由一组属性规定其定义、标识、表示和允许值的数据单位，应明确、客观、同一数据元的描述不应相互冲突。
6. 代码：表示特定事物或概念的一个或一组字符，应全覆盖全部可能取值，代码值之间不应相互冲突或遗漏。

（2）数据编码

对数据进行编码应遵循唯一性、稳定性和简洁性的原则，编码方法应以预定的应用需求和编码对象的性质为基础，选择适当的代码结构。

（3）数据质量

应建立数据质量评价与保证体系，对数据和元数据进行质量评价，要求如下：

1. 规范性：数据内容的表达应符合国际、国内和行业中的标准术语（包括缩写），暂无标准的，应尽量按照行业习惯给出准确名称。
2. 准确性：数据收集范围在规定的地理空间和时间范围内；应反映真实的数据情况；数据的模型、数据元、代码、标识符、格式及分类均遵循相应标准。
3. 完整性：数据表述全面，无字段缺失、漏项；对于有时间跨度数据，尽可能不间断收集。
4. 时效性：对于具有时效性数据，应明确标注数据随时间变化的频度信息。

（4）数据表达

可通过二维或者三维图形图像进行数据表达，应描述各类数据的图示表达模式，也要描述各类数据的标准符号和注记的等级、规格和颜色标准，以及使用这些符号的基本原则、表示方法和使用要求等。

##### 系统要求

（1）目录系统

建立目录系统实现目录内容在提供者与管理者之间、管理者与使用者之间的传输，具体要求如下：

1. 管理者提的目录服务，宜采用通用的目录服务接口规范；特定领域的如地理信息共享与交换应符合GB/Z 25598—2010第4章和第5章的要求。
2. 提供者通过向目录服务注册元数据，共享数据目录，元数据遵循2）（1）a)。

（2）交换系统

建立交换系统实现信息在提供者与使用者之间交换，交换系统要求如下：

1. 提供者应建立数据共享服务，接受使用者的数据申请，用于给使用者提供数据；
2. 提供者建立的数据共享服务应遵循统一的数据交换接口和数据交换格式；

##### 安全要求

（1）信息安全管理

信息安全管理要求如下：

a）所有数据应进行分类存档；

b）保证数据完整性，不仅能够检测出数据受到破坏，并能进行恢复；

c）保证数据完整性，实现系统管理数据、鉴别信息和重要业务数据的传输和存储的保密性；

d）实现本地完全数据备份，逐步建立数据异地备份。

（2）信息安全技术

a）所有数据应进行分类存档；

b）保证数据完整性，不仅能够检测出数据受到破坏，并能进行恢复；

c）保证数据保密性，实现系统管理数据、鉴别信息和重要业务数据的传输和存储保密性；

d）实现本地完全数据备份，逐步建立数据异地备份。

##### 信息管理要求

信息管理要求如下：

a）数据目录管理：应建立统一的电子政务信息资源目录体系，统一管理电子政务信息资源；

b）数据字典管理：应借助数据字典统一管理信息分类、数据元、代码、标识符、元数据等；

c）数据日常维护管理：应建立数据备份、恢复及安全管理制度。建立信息共享考核绩效评价制度进行年度考核。

### 空间数据管理要求

空间数据管理要求如下：

##### 数据格式统一

对于空间矢量数据，不同的系统的数据格式可能不同，如MapInfo系统采用MapInfo格式，ARC/Info系统采用ARC/Info格式。为了实现后绪数据使用的共享，要求数据格式进行统一成一种格式。

##### 数据更新

由于地理数据会随着时间变迁而发生变化，为了保持GIS数据的时效性，应对GIS数据进行定期更新，即修改陈旧数据用新数据代替或补充。在更新前，应该进行全面的调查和分析，有哪些空间数据发生变化，变化程度多大，以确定更新的方法。

##### 保密性

按《测绘管理工作国家秘密范围的规定》中规定：凡不能向社会公开提供的数据，不能存储在Internet连接的环境下。1:50万、1:25万、1:1万国家基本比例尺地形图及其数字化成果被确定为秘密等级，不能在互联网进行公布。在云平台的空间数据管理中，严格按照国家空间数据管理规定进行管理。同时对于空间数据的权限进行严格的定义，不同的部门，不同岗位的相关人员查看数据的权限是不同的。数据的查看等操作进行详细的记录。同时对相关工作人员进行规范培训，减少数据泄露的风险。

##### 空间化

空间化包括地名谱特征提取、空间匹配与数据序列化的方式实现数据资源在统一时空基准中进行定位匹配。

##### 一致性处理

对于存放的矢量数据、影像数据和实体数据，将更新后的数据快速及时进行地图综合，利用综合的结果联动更新相应范围数据，原内容自动变成历史数据。

### 多层级访问要求

组织架构定义是云平台的基础，云管理平台需要支持多级组织嵌套，每级组织都会划分资源(CPU、内存、存储、网络等)和用户，并提供了多种用户的角色，各用户的功能视角也不同。根据数据云平台的业务划分需求，云管理平台将使用者分为三大类：云管理员、租户管理员、最终用户。

（1）云管理员负责云数据中心的运维与运营，一方面云管理员需要负责云数据中心基础设施的运维工作，另一方面要负担起租户管理、流程管理等运营工作。云管理员对私有云的所有虚拟主机资源进行管理，包括主机的创建、主机的启动、主机控制台的访问、主机的关闭、主机的重启、主机信息的修改、主机的销毁、主机列表的查看、主机详细信息的查看、主机规格的创建、主机规格列表的查看和主机规格详细信息的查看。主机创建需要提供主机的规格(CPU类型、内存大小、硬盘大小等参数)，需要提供镜像模板(依赖于镜像模板模块)，创建主机前需要创建网络(依赖于网络模块)。主机启动后可访问主机控制台。查看主机列表后给出查看各个主机详细信息的链接，查看主机规格列表后给出查看各个主机规格详细信息的链接。

（2）租户管理员负责维护租户云资源，租户管理员可以对组织内云主机、云防火墙、云硬盘、云防火墙、云负载均衡、云数据库等进行管理。对系统资源管理类模块的功能需求与云管理员大致相同，所不同的是管理范围。云管理员可管理云平台中所有虚拟化资源，组织管理员管理的是其所属组织和该组织的各下级组织的虚拟化资源。

（3）云平台用户作为云资源的使用者，通过自助服务申请、使用、管理云资源，最终用户存在于租户之内。管理其所拥有的虚拟主机，包括申请主机、启动主机、关闭主机、重启主机、修改主机、销毁主机、查看主机列表、查看主机详细信息等操作。

### 风险管控要求

##### 虚拟化安全要求

（1）服务器虚拟化安全，服务最小化原则、内核模块完整性、补丁管理机制等。虚拟机安全，要做到隔离、访问控制、恶意虚拟机防护（如防地址欺骗和VM端口扫描等）、虚拟机资源限制。

（2）网络虚拟化安全包括虚拟交换机和虚拟防火墙，其中虚拟交换机，采用VxLan划分虚拟机组，对端口限速，禁止混杂模式进行网络嗅探。虚拟防火墙设置安全访问控制策略，建立逻辑安全边界。

（3）存储安全，支持存储空间的负载均衡、空余保护。

（4）高可用要求，支持虚拟机的冷备、热备、备份恢复，实现故障虚拟机的重新启用或者快速的进行切换，保障高可用的容灾的能力。

（5）虚拟化安全管理，支持宿主机资源监控、虚拟机资源监控、安全迁移回退机制、负载均衡和资源预留等。

##### 基础设施安全要求

（1）基础网络，包括安全域划分、异常流量监测与攻击防范和承载网络应支持设备级和链路级的冗余备份。

（2）主机及管理终端安全要求，主机终端系统要进行补丁管理和安全配置管理；进行控制蠕虫、病毒在云平台内传播，非法入侵的监测防范。

（3）基础设施资源池化安全要求，采用安全云技术提升安全基础设施服务效能，构建安全服务资源池。

（4）应急响应，建立完善、高效、快速响应、迅速解决问题的应急响应机制，提高对异常情况和突发事件的处理能力。

##### 数据安全

（1）数据隔离，通过虚拟化层安全机制实现虚拟机之间存储访问的隔离。

（2）数据访问控制，设置虚拟环境下的逻辑边界安全访问控制策略，实现虚拟机、虚拟机组间的数据访问控制。

（3）数据存储安全，为用户提供可选的加密存储服务，在上传、存储前对重要的数据进行加密处理。

（4）数据传输安全，采用SSH、SSL的方式保障信息安全；支持数据加密、VPN等技术保障用户数据信息的网络传输安全。

（5）数据备份与恢复，支持文件级完整和增量备份，映像级恢复和单个文件恢复。

##### 运营管理安全要求

（1）用户管理，对用户帐户信息进行集中维护管理，为集中访问控制、集中授权、集中审计提供可靠的原始数据。

（2）访问认证，建立统一、集中的认证授权系统，提高访问的安全性。

（3）安全审计，建立安全审计系统，进行统一、完整的审计分析，通过对操作、维护等各类日志的安全审计，提高对违规溯源追踪的事后审查能力。

### 应急管理要求

为了保障长江大保护业务的安全、稳定运行，确保信息系统的实体安全、运行安全、数据安全，云平台基础设施及应用系统的日常运维及应急管理是至关重要。那么工作明确、岗位制度、流程规范、组织结构清晰是基础。

对于云平台的应急管理可以分为事前的准备、事中处理、事后完善改进三部分。事前，做好运维人员的岗位、工作内容的安排，按要求做好日常检查，系统监控日志监控系统的建设完善可靠自动化，相关工作人员能够熟练的使用，建立比较完善的突发事件应急处理手册、机制、流程。事中，能够按既定的手册处理的，按手册进行处理，少见的突发事件，按能够最好解决办法，降低损失的方式进行处理。事后，总结经验，对于薄弱环节进行整改。

云平台的应急管理要求，具体来讲如下：

##### 建立安全应急团队

建立强有力的运维团队，分为云平台维护组、应用维护组、技术值班组。对成员进行培训，提高运维管理、应急突发事故的处理能力。

按照谁主管理、谁运营、谁使用谁负责，以及条块结合、以条为主的原则，建立和完善安全责任制及联动工作机制。根据各组职能，各司其职，加强组间的协调与配合，形成合力，共同履行应急处置工作管理职责。

##### 建立应急操作手册

有效的安全应急处理需要有完善可操作的应急操作手册，从而全面、详细的指导如何应对安全事件。

（1）应急操作手册需要涵盖事前准备、检测、分析、限制、根除、重建和事件后处理。应急操作手册的关键在于需要足够详细，具体的岗位和流程都在手册中清晰明了地予以描述。

（2）应急操作手册也要一定程度的灵活性，因为没有人能预测网络安全事件的类型和严重程度，所以需要允许相关人员在条件允许的情况下临场发挥。

（3）安全应急部门还需要随着外界网络安全环境的变化以及政策文件要求，及时持续地进行安全应急手册修正。同样，在安全事件处置团队对威胁进行应急处置后，需要将新获取的经验做法融入到安全应急操作手册中。

##### 日常检查

日常检查分为人工的检查和系统的自动检查。人工检查是对云平台重要系统，重要组成部分的运行情况进行查看，是否有异常情况。系统自动检查，是通过监控系统、日志收集后的自动监控等进行预警。通过日常的例行检查及时的发现一些运行中的隐患，并进行排除，降低突发事故的发生可能性。根据云平台承载业务的重要性的不同，对运行的设备进行例行检查。一些设备厂商提供了检查软件，可以利用这些软件查看设备运行情况。查看网络运行情况、服务器应用服务是否正常、CPU内存利用率是否正常。如发现异常及时进行处理，必要时将重要业务切换到备用环境中，排除后再切回。

对云平台的机房环境也要进行日常检查，环境的温度、湿度、灰尘等是否合乎要求。空调、供电系统是否运行正常，设备运行是否温度不正常。地板、天窗、消防、监控都是检查不可缺的环境。如果发现问题及时整改。

##### 应急资源的储备

应储备核心交换机、服务器设备、光纤线缆、网线等，当发生由于硬件设备故障或者设备被攻击出现宕机等情况，运维人员可以使用储备的设备进行替换，确保最短时间恢复。

##### 监控系统建立

建立完善、稳定的性能监控系统，包括对于CPU、内存、存储、应用的性能等指标的收集，日志收集系统的建立，并根据对应的特点，建立预警规则。在日常的系统运维中，有助于较早的发现系统的漏洞问题解决隐患。在应急事故发生中，有利于故障的尽快排查。

##### 事故总结

分析故障原因，总结经验教训，明确责任，制定解决方案。并进行隐患排查，防患于未然，避免相似的故障再次发生。同时针对故障的原因、解决办法，对运维团队进行针对性的培训，提升运维的水平。

## 镜像长江建设

### 设计原则

### 系统架构

### 系统划分

### 模块设计

### 接口设计

## 智慧应用

### 供水监管

### 排水监管

### 岸线监管

### 防洪减灾管理

### 工程建设管理

### 水环境治理管理

### 应急处置管理

### 综合决策支持（匡欢）

# 关键技术

## 长江大保护时空大数据统一的描述方法

## 长江大保护背景下的时空大数据云平台建设方案

## 长江大保护数据、资源高效管理和平台性能保障

# 总结

## 结论

## 创新点

## 研究展望