

解决方案实践

华为云区域教育云平台解决方案实践

文档版本 2.1
发布日期 2024-05-07



版权所有 © 华为技术有限公司 2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：

<https://www.huawei.com/cn/psirt/vul-response-process>

如企业客户须获取漏洞信息，请参见如下网址：

<https://securitybulletin.huawei.com/enterprise/cn/security-advisory>

目录

1 方案概述	1
2 资源和成本规划	8
3 操作流程	17
4 实施步骤	18
4.1 教育应用市场 RomaExchange 环境部署.....	18
4.1.1 购买部署基线 RomaExchange.....	18
4.1.2 配置 RomaExchange.....	22
4.1.3 切换教育环境.....	35
4.2 区级管理平台环境部署（含数据中心部署）.....	41
4.3 物联中心应用环境部署.....	50
4.4 数字基座客户端服务开通.....	54
5 集成对接	69
6 修订记录	73

1 方案概述

本文档重点描述区域教育云平台基线解决方案的交付策略、标准化交付的项目组织结构和角色、各组织和角色的职责、项目交付的标准人力基线，以及交付的流程和活动。旨在为负责区域教育云平台集成交付的内部组织和外部伙伴提供指导，按照规范流程进行实施，确保项目交付高质高效。

应用场景

- 教育应用市场**

按照教育应用管理要求，优化应用上架、审核、发布等流程，并针对待上架和已上架教育应用市场的应用，依据工信部、教育部和网信办等相关标准规范进行隐私合规和安全漏洞检测，并针对具体问题给出修复建议，确保教育应用符合监管合规要求。
- 学校数字基座-数据中心**

基于数据标准规范，提供教育数据从采集、存储、加工、分析、共享及可视化的全过程能力。为用户提供教育数据共享、数据标准管理查询和应用数据回流。通过可视化的呈现方式为管理平台提供基础数据、应用使用情况等数据的汇总概览。
- 学校数字基座-物联中心**

校园物联网是校园数字化的重要组成部分，当前物联网主要实现设备运行状态的监控和设备的控制，教育数字化转型要求按照“物联、数联、智联”原则，实现多个智能设备的连接与协同，支撑个性化教学、场景化教学。

方案架构

区域教育云平台是针对市/区/县教育局统筹建设的区域教育云平台，应用和能力区域集中建设，避免重复建设；建立统一应用标准和数据标准，实现优质教育资源多元供给和共享，为区域内学校构建数字教育资源服务体系。

图 1-1 方案架构



区域教育云平台打造以“五大中心”为核心的基座，赋能创智教育提质升级，全面支撑教育数字化转型。采用平台与数据分离架构，数据本地化部署，区级数据库/数仓和学校数据库/数仓通过API接口提供数据服务，做到数据可用而不可得，实现数据安全应用服务。

- 统一工作台**

统一门户面向用户提供统一入口，包括PC端、移动端等，供区校管理员、教职工、学生、家长等用户使用，基于角色的个性化资源、内容推荐，不同角色具有不同的权限、菜单、首页视图，实现千人千面，实现统一账号、统一组织、统一登录、统一授权。
- 开放应用生态**

建设开放的区域应用生态，面向第三方应用提供易接入的标准化接口，实现应用注册、上架、审核、运营及监控，支撑区域建设标准化+学校个性化的应用生态，校级管理员可浏览、查找应用，订阅到工作台进行使用。应用包括区级应用、校本应用和第三方应用，为促进区域教育的优质化、均衡化发展，充分整合区内外优质教育资源，形成优质教育资源共建共享、衔接融通机制，基本满足全区中小学教育信息化教与学需求。
- 基础能力开放层**

基础能力开放层包括API网关和低代码开发工具。API网关主要面向应用及开发者提供公共服务接口，如认证接口、标准数据接口、物联标准接口等，实现公共服务区域共享，减少重复建设。低代码开发工具提供了云上无码化、低码化的应用开发模式，屏蔽了技术的复杂性，无码工具协助教师托拉拽式创建问卷调查/活动报名等轻应用，自动生成统计结果，避免传统式文件收集方式，提效减负。低码

工具提供的界面、逻辑、对象等可视化编排工具，以“拖、拉、拽”的方式来快速构建应用，从而实现所见即所得的快速应用开发和构建。

- **学校数据基座“五大中心”**

学校数字基座是建设的核心和重点，包括数据中心、物联中心、应用中心、消息中心和组织中心等部分。

数据中心基于数据标准规范，提供教育数据从采集、存储、加工、分析、共享及可视化的全过程能力，并通过基座实现跨数据空间互联，实现教育数据在市、区、校之间的共享。物联中心解决所有物联网设备的无缝连接，实现对物联感知设备统筹管理。应用中心实现应用浏览、查找应用，并订阅应用到工作台进行使用，同时支持应用管理、应用分组、应用授权等功能。消息中心实现用户按需推送各类消息和通知，并向上层应用提供消息通知的统一接口。组织中心建立统一组织用户体系，组织内进行权限角色管理、权限设置、管理员管理、应用授权，实现不同角色的用户权限管理。

- **运营运维体系和安全体系**

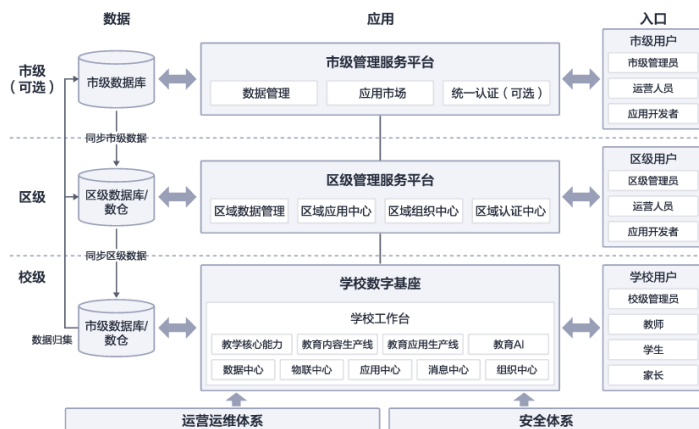
为保障教育数字基座基更好的服务区域和学校，需要成立专门的运营运维团队，建设运营运维保障机制，能及时响应区域和学校的日常运维需求和应急响应需求，同时通过运营，不断优化应用和服务，支撑区域教育数字化转型。

建设完备的安全体系，建立从应用、数据、网络、存储、管理等端到端的安全防护体系，保障业务安全可靠运行。

业务架构

区域教育云平台业务架构如下：

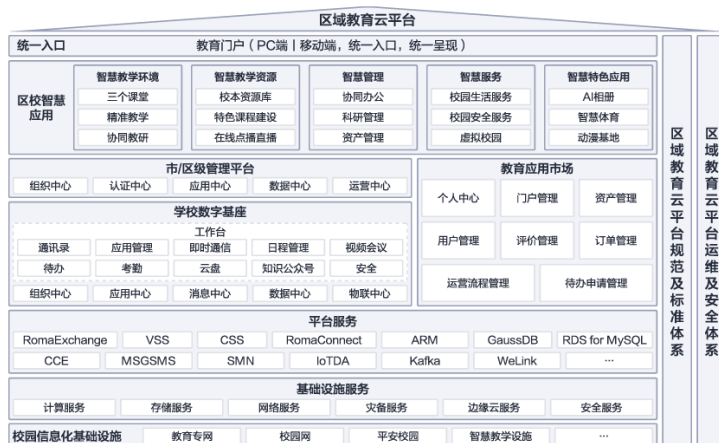
图 1-2 业务架构



技术架构

区域教育云平台是面向学校师生和教育管理者的统一应用入口，提供通过手机或是PC端登录区域教育云平台，查看即时消息、待办等信息，可根据业务需求访问数字基座提供的原生应用和预集成的第三方应用。

图 1-3 技术架构



- 区域教育云平台提供统一的教育应用市场，提供符合教育应用管理的完整教育应用管理流程，同时支持多个厂商的学校数字基座的对接，实现应用及开发者信息的同步，以及各个学校基座的基础信息的管理。
- 区域教育云平台提供市级/区级管理平台，对多个学校数字基座进行管理及数据服务，对外提供统一用户信息和认证对接服务；
- 区域教育云平台提供运行在Android/IOS/鸿蒙/Windows等操作系统端侧应用程序运行框架；
- 区域教育云平台-学校数字基座提供基础的办公应用：通讯录、应用管理、即时通信、日程管理、视频会议、待办、考勤、表单、云盘、知识、公众号等应用及服务；
- 区域教育云平台-学校数字基座提供组织中心、应用中心、消息中心、数据中心、物联中心；

组织中心提供统一身份管理能力：组织管理、权威的用户身份库管理及提供服务、身份管理审计，用户日志供查询；

应用中心提供统一认证与访问控制能力，实现单点登录和认证权限管理；

消息中心提供消息转发分发能力，支持多种消息发送，如：即时消息、短信、邮件等；

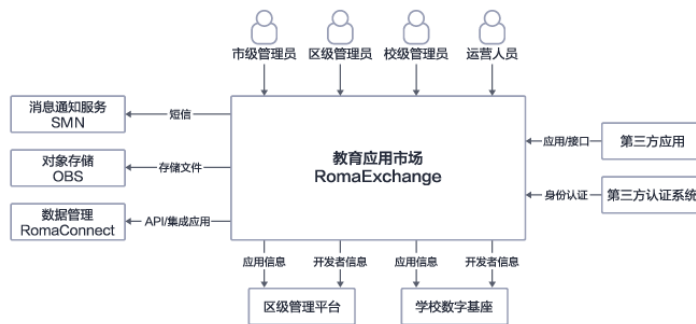
数据中心提供融合集成能力，包括API集成、数据集成、消息集成等，还提供教育业务模型管理、融合数仓服务、数据结构管理、数据回流管理、数据资产管理、数据标准管理等；

物联中心提供物联网设备接入支持多网络、多协议和多模式，提供接入设备的管理、双向设备通信、制定规则、监控运维、物联感知数据管理等。

区域教育云平台系统主要包括三部分：教育应用市场、市/区级管理平台和学校数字基座。

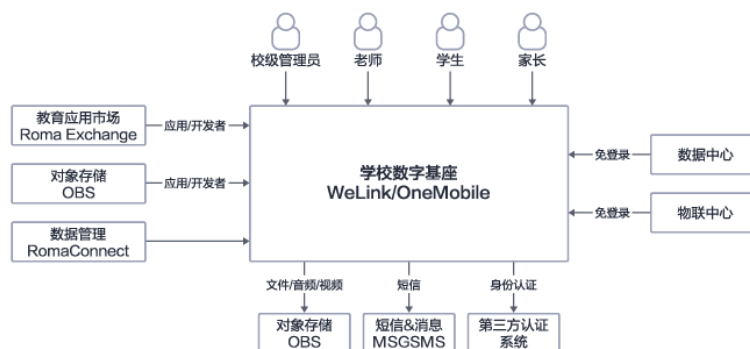
- 教育应用市场包括教育应用市场Web门户、教育应用市场管理后台，与周边的关系如下：

图 1-4 关系图 1



- a. 教育应用市场Web门户端面向市级管理员、运营人员、区校管理员和开发者，提供统一的应用访问门户，通过Web门户访问浏览上架的教育应用相关信息。
 - b. 教育应用市场Web管理后台面向市级管理员、运营人员、区校管理员和开发者，针对不同角色权限提供不同个人管理界面功能。支持面向逻辑统一的教育应用市场运营运维管理团队，支撑教育应用市场入口的系统配置、用户与组织的增删改管理等；
 - c. 教育应用市场与消息通知服务集成实现对系统内容发送订阅短息消息，与对象存储实现应用管理相关的音视频、word等文件的存储管理，与数据管理服务集成实现与数据接口的申请、审批的统一管理，应用注册信息的统一发放。
 - d. 教育应用市场与区级管理平台、学校数字基座集成实现应用的自上而下的分发、同步，和开发者信息的同步。
 - e. 教育应用市场为第三方应用开发者，提供教育应用的注册、上架、发布等功能；
 - f. 教育应用市场与第三方认证系统集成对接，实现用户的身份统一认证登录。
- 学校数字基座与周边的关系如下：

图 1-5 关系图 2



方案优势

- **统一工作台**
面向用户提供统一入口，包括PC端、移动端等，供区校管理员、教职工、学生、家长等用户使用，基于角色的个性化资源、内容推荐，不同角色具有不同的权限、菜单、首页视图，实现千人千面。

- **开放应用生态**
面向第三方应用提供易接入的标准化接口，实现应用注册、上架、审核、运营及监控，支撑区域建设标准化+学校个性化的应用生态，形成优质教育资源共建共享、衔接融通机制。
- **数字基座“五大中心”协同**
“五大中心”包括数据中心、物联中心、应用中心、消息中心和组织中心。数据中心基于数据标准实现应用数据回流、数据融通和共享；物联中心解决所有物联设备的无缝连接，实现教学场景下的多设备统一调度和协同。“五大中心”协同赋能教学业务场景。
- **教育应用市场**
人有我优，建设开放生态的教育应用市场生态，提供在线一站式低代码开发平台，实现对教育应用的在线快速开发、调试、上架、部署。

约束与限制

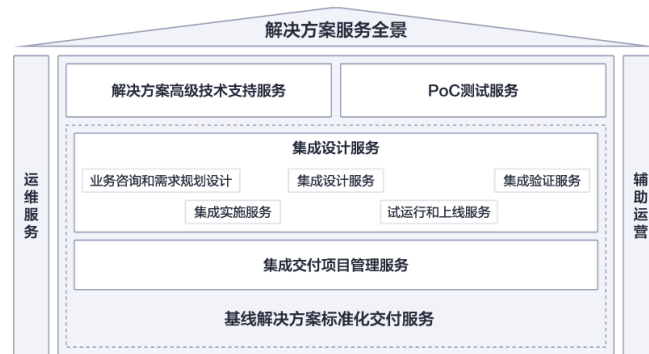
- **交付对象**
华为云生态解决方案的产品构成中，既包含华为基础云资源，也可能包含华为的服务、软件、硬件，以及伙伴的服务、软件、硬件，对于上述具体的产品的交付，参见对应的产品交付指导书或者类似的文档，不在本文档描述的范围。
本文档重点描述从解决方案整体的角度，如何组织、协调解决方案包含的各产品交付团队和人员，调用产品交付的能力，通过文档定义的交付流程和活动，完成整个解决方案的集成交付。
对于项目中出现的超出解决方案范围的华为或者第三方产品或服务，不在本解决方案集成服务范围内，建议由项目面向客户的总集负责集成交付。
解决方案集成交付和其中华为或伙伴的产品（服务、软件、硬件）的交付的关系参考下图。

图 1-6 交付对象



- **服务范围**
区域教育云平台基线解决方案配套的专业服务类别有交付、运维、辅助运营。其中交付部分，包含基线解决方案标准化交付、解决方案高级技术支持服务及PoC测试服务，本文档针对基线解决方案标准化交付进行描述，其中包含集成实施和项目管理两个领域。
区域教育云平台基线解决方案相关的服务全景和关系如下图所示。

图 1-7 服务范围



● 使用对象

本文档面向的对象为华为公司内部负责区域教育云平台解决方案项目交付的组织、外部承接区域教育云平台解决方案集成交付的服务伙伴，以及上述组织内参与到项目交付中的角色，包括：

- a. 交付项目经理
- b. PCM
- c. 生态合作经理
- d. TD（项目技术总体负责人）
- e. 测试经理、测试设计工程师、测试工程师
- f. 实施经理
- g. BA/SA
- h. SE
- i. 版本经理
- j. 其它参与项目交付的角色

2 资源和成本规划

整体集成架构图资源清单由教育应用市场RomaExchange、区级管理平台、学校数字基座WeLink、数据中心、物联中心以及周边集成云服务组成。

解决方案整体集成架构

- 集成架构图

图 2-1 市校两级集成

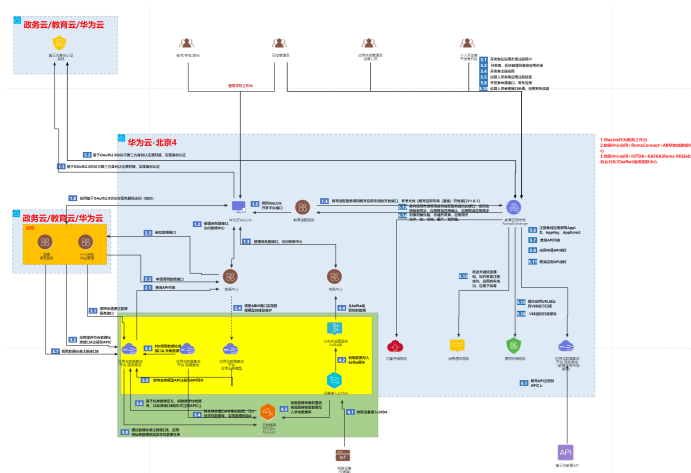


图 2-2 市校两级平台集成

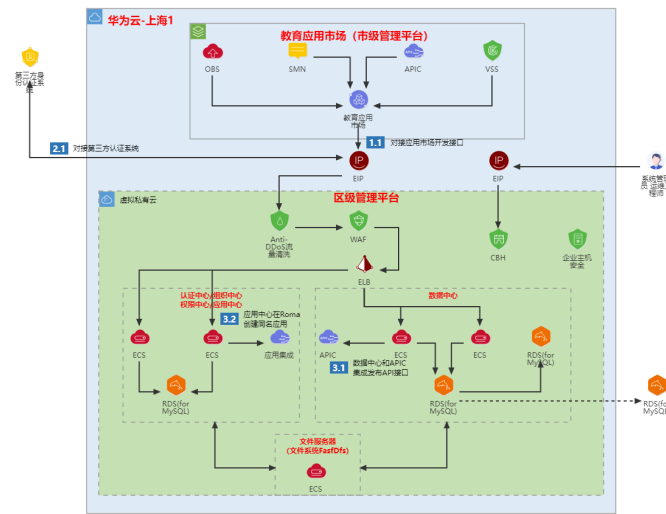


图 2-3 区校两级平台集成

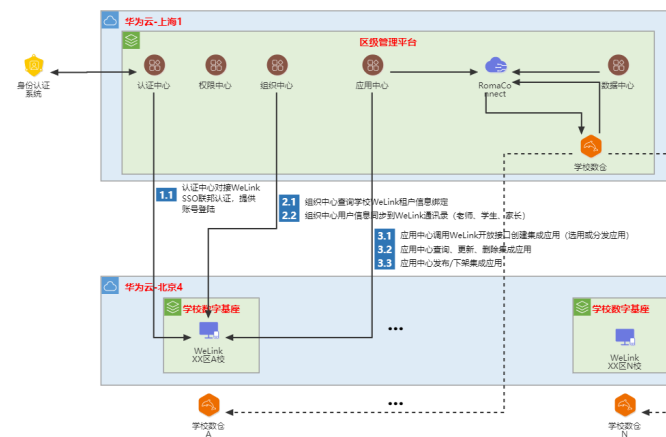


图 2-4 市校两级集成

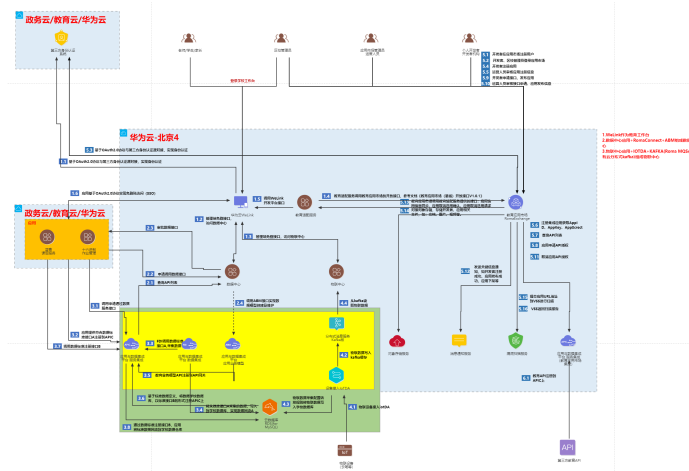


图 2-5 市校两级平台集成

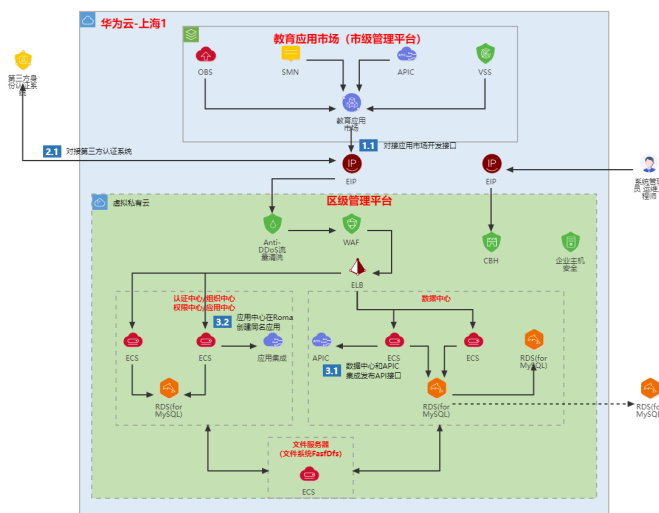
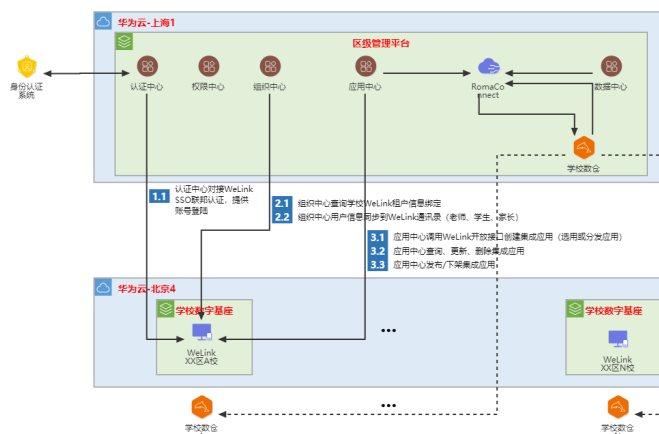


图 2-6 区校两级平台集成



解决方案版本的主要构成如下：

- 教育应用市场：**基于Roma Exchange构建的区域教育应用市场，建立开放教育应用生态，市区县统一上架应用，学校按需使用；
- 区级管理平台：**由伙伴开发基于华为云服务部署，集成RomaConnect、SMN、MSGSMS等服务，实现对多个学校数字基座的组织用户信息管理，提供组织管理、认证管理、权限管理、应用管理等，将用户信息、组织信息、应用信息、开发者信息同步给各个数字基座。
- 学校数字基座WeLink：**包括PC和移动端，承载五大中心能力，并提供应用中心、消息中心和组织中心三大能力；
- 数据中心：**基于数据标准规范，提供教育数据从采集、存储、加工、分析、共享及可视化的全过程能力。为用户提供实现跨数据空间互联，实现教育数据的跨级共享。通过可视化的呈现方式为管理平台提供基础数据、应用使用情况等数据的汇总概览；
- 物联中心：**校园物联网是校园数字化的重要组成部分，当前物联网主要实现设备运行状态的监控和设备的控制，教育数字化转型要求按照“物联、数联、智联”原则，实现实现多个智能设备的连接与协同，支撑个性化教学、场景化教学；

- **资源清单**

整体集成架构图资源清单由教育应用市场RomaExchange、区级管理平台、学校数字基座WeLink、数据中心、物联中心以及周边集成云服务组成。

表 2-1 资源清单

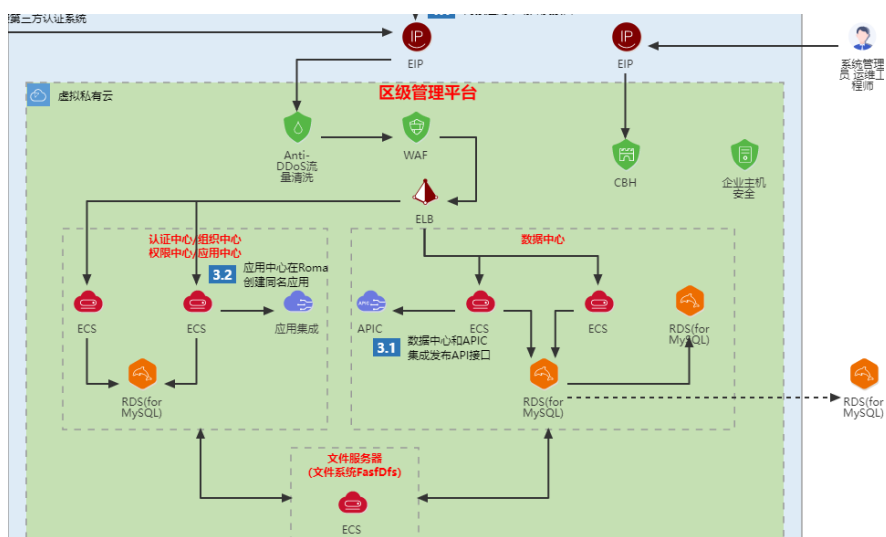
序号	云服务/伙伴产品	规格	数量	部署环境	说明
1	RomaExchange	专业版/旗舰版	1	公有云	教育应用市场基线，按项目规模配置，参考配置报价器选型
2	OBS	标准存储单AZ存储包	按需	公有云	/
3	VSS	漏洞扫描服务企业版	1	公有云	/
4	SMN	消息通知服务	按需	公有云	应用市场集成，按需求收费
5	RomaConnect	应用与数据集成平台，基础版/专业版/企业版，按项目规模配置，参考配置报价器选型	1	公有云	主要是使用APIC、应用集成与RomaExchange做服务集成（专属应用市场使用）
6	区级管理平台	参考区级管理平台配置	1	公有云	伙伴产品；基于ECS部署和云数据库RDS for MySQL部署
7	WeLink	学校数字基座（工作台）	1	公有云	/
8	数据中心	参考数据中心配置	1	公有云	伙伴产品；基于ECS部署和云数据库RDS for MySQL部署
9	RomaConnect	应用与数据集成平台（含ABM），基础版/专业版/企业版，按项目规模配置，参考配置报价器选型	1	公有云	主要是使用APIC、FDI、应用集成与数据中心集成
10	物联中心	参考物联中心配置	1	公有云	伙伴产品；基于ECS部署和云数据库RDS for PostgreSQL部署

序号	云服务/伙伴产品	规格	数量	部署环境	说明
11	IoTDA	IoTDA企业版	1	公有云	/
12	Kafka	kafka.4u8g.cluster 代理个数: 3; 超高IO 400GB;	1	公有云	/

区级管理平台集成架构

- 集成架构图

图 2-7 区级管理平台集成架构图



- 资源清单

表 2-2 区级管理平台资源清单

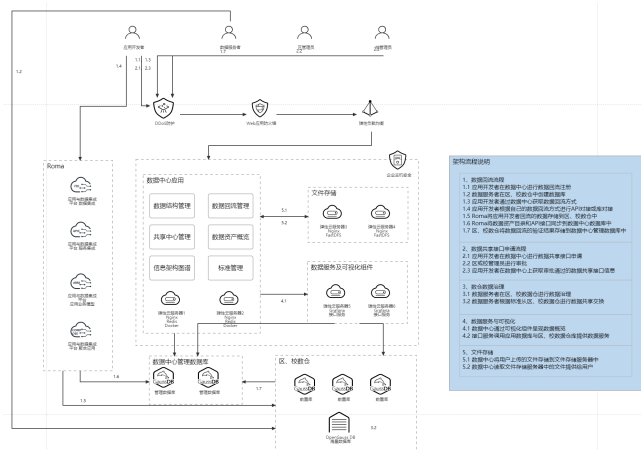
序号	云服务	规格	数量	部署环境	说明
1	数据中心应用	参考数据中心配置	1	公有云	参考数据中心配置
2	ECS	X86计算 通用计算增强型 c6.2xlarge.2 8核 16GB CentOS 7.9 通用型SSD 400GB;	4	公有云	数字基座其他中心-文件服务器

序号	云服务	规格	数量	部署环境	说明
3	RDS for MySQL	RDS S for MySQL 8.0 高可用只读 通用型 8核32GB; SSD云盘 1000GB;	2	公有云	区数仓前置数据库
4	SMN	消息通知服务,发送短信、邮件	按需	公有云	消息中心 PaaS服务
5	ELB	全动态BGP , 50Mbit/s带宽	1	公有云	/
6	企业主机安全	企业版;	1	公有云	/
7	Web应用防火墙	规格: 标准版; 独享型, 100小规格	1	公有云	/
8	Anti-DDoS流量清洗	DDoS原生基础防护	1	公有云	/
9	云堡垒机	规格: 50资产专业版	1	公有云	/
10	云备份	1000GB	1	公有云	/

数据中心应用集成架构

- 集成架构图

图 2-8 数据中心应用集成架构图



● 资源清单

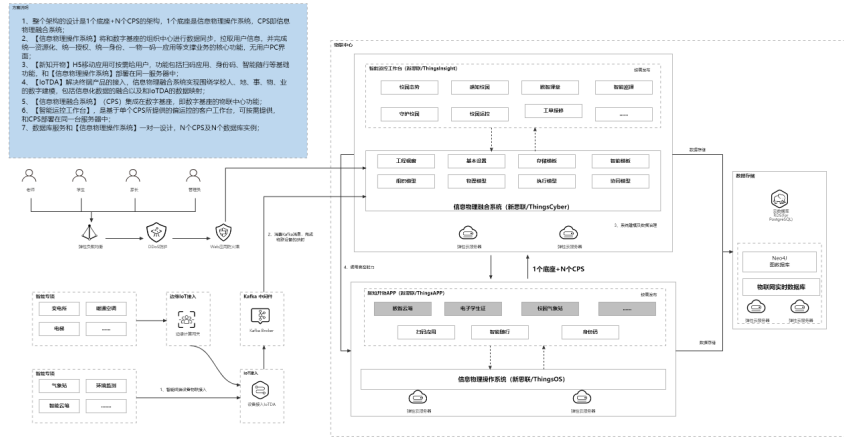
表 2-3 数据中心应用资源清单

序号	云服务	规格	数量	部署环境	说明
1	ECS	X86计算 通用计算增强型 c6.2xlarge.2 8核 16GB CentOS 7.9 系统盘通用型SSD 400GB;	2	公有云	数据中心管理服务
2	ECS	X86计算 通用计算增强型 c6.2xlarge.2 8核 32GB CentOS 7.9 系统盘通用型SSD 400GB;	2	公有云	数据接口与可视化组件服务
3	ECS	X86计算 通用计算增强型 c6.xlarge.2 4核 8GB CentOS 7.9 系统盘通用型SSD 400GB;	1	公有云	文件服务器
4	RDS for MySQL	RDS for MySQL 8.0 主备 通用型 8核16GB; SSD云盘 1000GB;	1	公有云	数据中心管理数据库
5	RDS for MySQL	S for MySQL 8.0 高可用只读 通用型 8核32GB; SSD云盘 1000GB;	2	公有云	区数仓前置数据库
6	Roma Coone ct	企业版	1	公有云	数据中心PaaS服务

物联中心应用集成架构

- 集成架构图

图 2-9 物联中心应用集成架构图



- 资源清单

表 2-4 物联中心应用资源和成本规划内容说明

序号	云服务	规格	数量	部署环境	说明
1	ECS	规格: X86计算 通用计算增强型 c7.xlarge.2 4核 8GB 镜像: Windows Windows Server 2019 数据中心版 64位简体中文 系统盘: 高IO 100GB 数据盘: 高IO 100GB	2	公有云	信息物理操作系统
2	ECS	规格: X86计算 通用计算增强型 c7.xlarge.2 4核 8GB 镜像: Windows Windows Server 2019 数据中心版 64位简体中文 系统盘: 高IO 100GB 数据盘: 通用型SSD 100GB	2	公有云	物联网实时数据库加 Neo4J
3	ECS	规格: X86计算 通用计算增强型 c7.xlarge.2 4核 8GB 镜像: Windows Windows Server 2019 数据中心版 64位简体中文 系统盘: 高IO 100GB	1	公有云	ThingsCyber
4	设备接入 IoTDA	实例版本: 标准版 中频单元S2 1	1	公有云	/

序号	云服务	规格	数量	部署环境	说明
5	分布式消息服务 Kafka版 云数据库 RDS(for PostgreSQL)	规格: kafka.2u4g.cluster 代理个数: 3 单个代理存储空间: 超高IO 200GB 规格 PostgreSQL 12 主备 通用型 4核8GB 存储空间 SSD云盘 100GB	1 1	公有云 公有云	/

3 操作流程

产品交付策略

解决方案内包含的各类软硬件产品，由对应的产品部负责交付或提供交付伙伴。伙伴的产品由伙伴负责交付。

解决方案交付策略

解决方案的集成交付策略如下：

0-1阶段：由解决方案构建部门华为云生态解决方案部主导交付。

1-3阶段：由华为云生态解决方案部牵头，联合外部的集成交付伙伴，共同参与完成项目的交付。

3-N阶段：由外部的集成交付伙伴独立完成交付，生态解决方案部作为解决方案交付能力中心，对负责交付的内部组织和外部伙伴提供技术支撑。

解决方案交付 KCP 点

所有解决方案项目需经过项目准入评审、SRB评审，在评审会议上明确项目具体交付模式，所有评审通过后方可进入项目交付阶段。

对于0-3阶段由华为主导交付的项目，需按照华为云交付项目流程开展DTRB评审、DRB评审，由项目组发起，评审部门为机关生态解决方案部PE及核心团队。

对于3-N阶段由伙伴主导交付的项目，原则上由伙伴在签合同前按照自身的交付流程进行交付可行性评估，华为不开展DTRB评审、DRB评审。在解决方案上市初期，对于一些重大的、高风险的项目，可以在SRB评审过程中具体明确是否由华为支撑伙伴开展DTRB和DRB评审。

4 实施步骤

- 4.1 教育应用市场RomaExchange环境部署
- 4.2 区级管理平台环境部署（含数据中心部署）
- 4.3 物联中心应用环境部署
- 4.4 数字基座客户端服务开通

4.1 教育应用市场 RomaExchange 环境部署

4.1.1 购买部署基线 RomaExchange

背景信息

ROMA Exchange是基于AppCube开发的应用，部署依赖AppCube Runtime运行环境。

ROMA Exchange上的用户总数受AppCube规格里显示的用户数限制，用户总数包括部署ROMA Exchange的租户、该租户下创建的用户以及自行在ROMA Exchange资产中心前台注册的用户、通过第三方接入ROMA Exchange的用户。

因此，购买ROMA Exchange时，会同步订购AppCube服务创建实例申请部署AppCube Runtime运行实例。

ROMA Exchange提供专业版规格，可以根据需要选择按月购买或按年购买。

- 按月：20万元/月，可以选择购买数个月。
- 按年：200万元/年，当前仅支持购买1年，一年的费用相比按月购买更优惠。

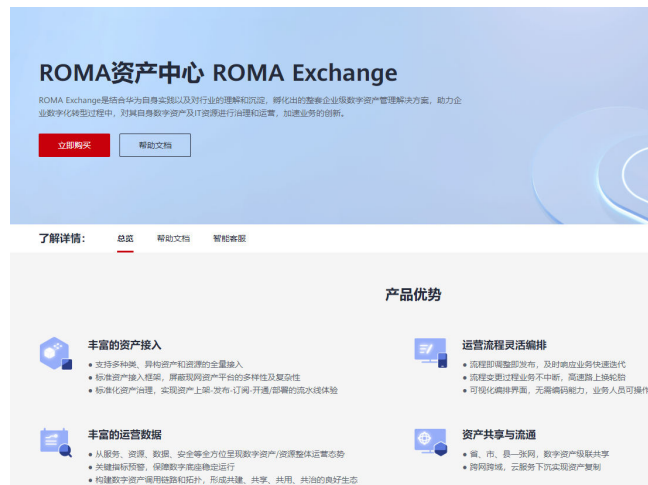
前提条件

资产提供方上传资产时，需要保存资产的相关文件，因此需要用到OBS桶。建议提前购买好OBS桶，可以参考[OBS的相关文档](#)。OBS的大小建议1T，因为ROMA Exchange是包年或包月的，因此建议您购买OBS时考虑好匹配的规格。

操作指导

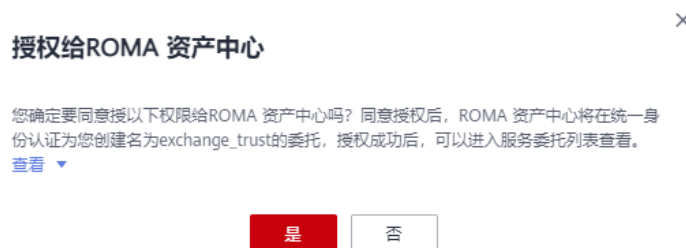
- 步骤1** 登录**华为云官网**。如果没有华为账号，请立即注册，相关操作请参见**用户注册**。注册后参考**个人帐号如何完成实名认证**或**企业帐号如何完成实名认证**完成个人或企业账号实名认证。选择“产品”，在菜单栏中选择“企业应用 应用平台”，单击“ROMA 资产中心 ROMAExchange”，进入ROMA Exchange官网页。申请购买ROMA Exchange。
- 步骤2** 用户申请购买后，系统会为用户部署一套ROMA Exchange实例，该套实例包括ROMA Exchange资产中心和运营管理平台。
- 步骤3** 单击“立即购买”。

图 4-1 立即购买



- 步骤4** 单击“查看”，了解授权信息，同意后，单击“是”。系统进入ROMA Exchange的控制台。
- 步骤5** 如果用户之前授权过，则没有该步骤，可以忽略该步骤。

图 4-2 授权



- 步骤6** 在ROMA Exchange的控制台页面上，单击“购买ROMA Exchange实例”。

图 4-3 单击购买实例



步骤7 在购买页面填入信息，勾选阅读并同意服务声明。用户还可以勾选到期后是否自动续费。

图 4-4 填写信息

购买 ROMA Exchange 实例

* 区域：华北-北京五

* 实例名称：romaexchange-3suu6

实例规格：专业版

* 购买时长：1, 2, 3, 4, 5, 6, 7, 8, 9个月, 1年

自动续费

我已阅读并同意《ROMA资产中心服务声明》

步骤8 单击“立即购买”，系统进入订单页面。用户查看订单情况，并选择支付方式。

图 4-5 查看订单情况

购买 ROMA Exchange 实例

云服务订单

订单号	商品名称	订单金额	应付金额
CS21118164894AP	ROMA资产中心	¥200,000.00	¥200,000.00

选择支付方式：在线支付

余额/在线支付

余额支付 使用账户余额支付 ¥0.00 (可用余额: ¥0.00)

在线支付 使用第三方支付 ¥199,999.02

余额支付 ¥0.98
在线支付 ¥199,999.02

在线支付

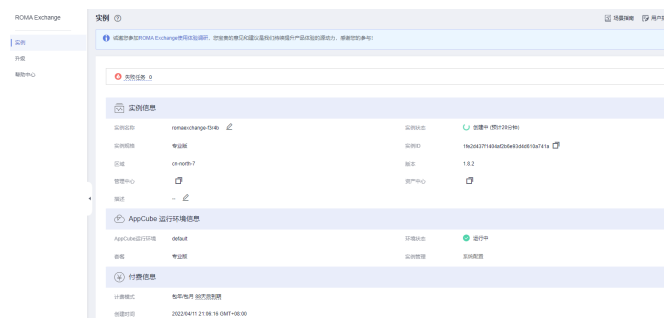
步骤9 根据付款方式，单击“确认付款”或“去在线支付”，系统弹出如下提示信息，表示订单支付成功。系统自动在后台安装 ROMA Exchange。

图 4-6 支付



步骤10 单击“返回ROMA资产中心控制台”，可以查看ROMA Exchange的安装状态。如下图所示，实例在“创建中”。

图 4-7 查看



步骤11 当“实例状态”变为“运行中”，说明实例已经安装好，可以使用。在正式使用ROMA Exchange前，请参考


- 单击页面右上角的“进入管理中心”，即可进入ROMA Exchange的运营管理后台。
- 单击页面右上角的“进入资产中心”，即可进入ROMA Exchange的前台资产中心。
- 单击页面上“资产中心”参数后面的，可以修改资产中心的域名，修改后单击“✓”提交。

图 4-8 使用前 1

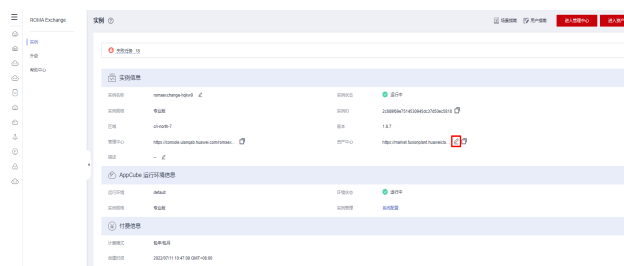
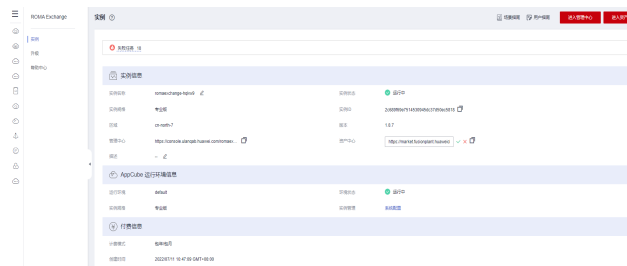


图 4-9 使用前 2



---结束

4.1.2 配置 RomaExchange

进入租户管理员配置界面

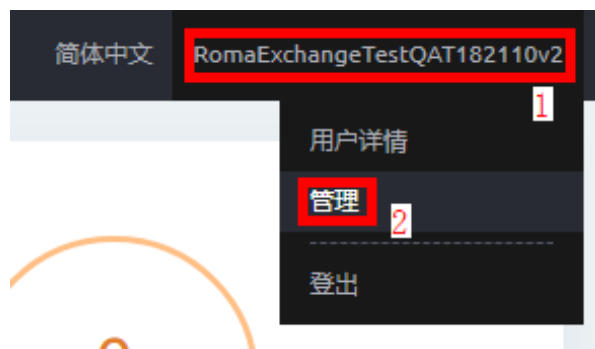
说明

实例的配置是在AppCube上配置，本文档仅是举例，不同的AppCube版本界面可能会有变化，请以实际为准。

部分非必要的参数配置，请结合业务实际需要和界面参数说明进行配置。

- 步骤1** 租户管理员配置都是在AppCube上完成，因此用户需要参考如下步骤进入AppCube的租户管理员配置界面。
- 步骤2** 在ROMA Exchange的运营管理员界面的右上角，单击账号名，然后单击“管理”，进入AppCube界面。

图 4-10 进入 AppCube 界面



- 步骤3** 在AppCube界面上单击“管理”，然后在左侧选择“应用管理 BO配置”菜单后，单击“Digital Store Service”，进入ROMA Exchange的配置界面。

图 4-11 配置界面



步骤4 在配置界面上，单击需要配置的项并根据本文档指导或界面提示进行配置。

图 4-12 配置 1

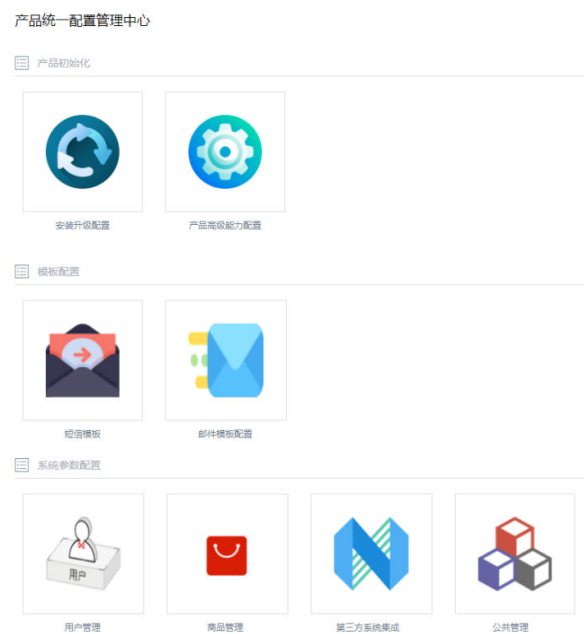
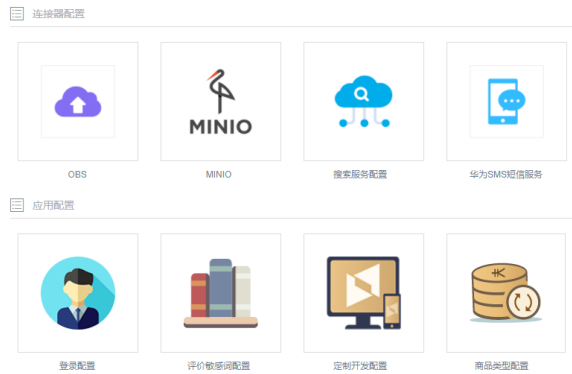


图 4-13 配置 2



----结束

配置 OBS 存储功能

步骤1 资产提供方上传资产时，需要保存资产的相关文件，因此需要用到存储。

步骤2 前提条件

- 使用OBS之前，您需要拥有一个华为账号或一个可用于访问OBS的IAM用户，本节将介绍如何注册华为云并实名认证、创建IAM用户、充值以及购买资源包，具体操作请参见[使用OBS前需要做的准备工作](#)。
- 参考[获取AK/SK](#)获取AK（Access Key ID）、SK（Secret Access Key），即访问密钥对。
- 在OBS上创建存储桶（例如“bing.testonly.1”），用于后续存储对象使用，具体操作请参见[如何创建桶](#)，并记录创建桶时选择的区域。具体创建方法请参见对象存储服务帮助中心里“控制台指南 管理桶 创建桶”的相关操作。
- 建议该桶单独给ROMA Exchange使用，以便后续万一需要，方便进行数据文件的操作。

步骤3 配置说明

步骤4 参考 [进入租户管理员配置界面](#)，在租户管理员界面上，单击“连接器配置”下的“OBS”，跳转到OBS列表页。

图 4-14 OBS 列表页



步骤5 单击“新建”

图 4-15 新建



步骤6 参考界面和下表配置必选参数。

表 4-1 OBS 存储配置参数说明

字段		说明	如何配置
基本信息	名称	OBS连接器的名称，用户自定义。	单击文本框，填入名称。
	账号地区	前提条件里创建桶时，选择的区域。	下拉框里选择，请根据实际情况配置。
	访问密钥	前提条件里获取的访问密钥ID（Access Key Id）。	单击文本框，填入访问密钥。
	密钥	前提条件里获取的秘密访问密钥（Secret Access Key）。	单击文本框，填入密钥。
桶（一个OBS连接器只支持配置一个桶。）	区域	前提条件里创建桶时，选择的区域。	下拉框里选择，请根据实际情况配置。
	桶名称	前提条件里创建桶时，配置的名称。	单击文本框，填入桶名称。
	文件类型	上传到桶里的文件类型。	必须填写文件类型，配置后在后台限制上传的类型，防止修改拦截报文绕过后台文件类型检测。 取值： pdf,png,jpg,jpeg,doc,docx,zip,mp4,ppt,pptx,bmp。
	文件大小	上传到桶里的文件大小。	必须填写文件大小，配置后在后台限制上传的大小，防止修改拦截报文绕过后台文件大小检测。 取值：209715200字节

步骤7 功能测试

测试对接是否成功。


单击桶操作列中的图标，选择一个文件上传，如图所示。

图 4-16 文件上传 1

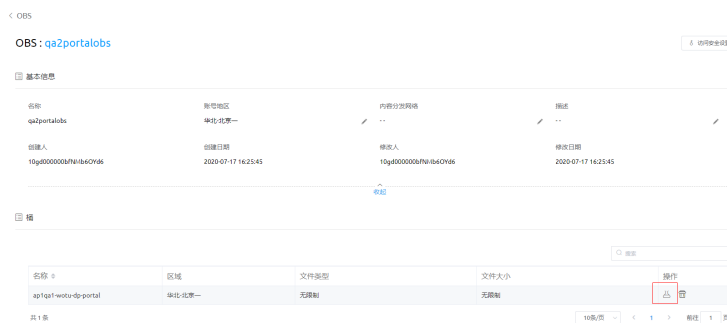


图 4-17 文件上传 2



上传成功后会出现上传成功字样，单击文件尝试下载，下载成功，并且文件内容正确，则说明OBS配置成功。

----结束

短信的配置

• 短信连接器配置

在产品初始化配置里开启发送短信功能，通过与华为云的消息通知服务SMN（Simple Message Notification）对接，实现短信发送功能。

步骤1 前提条件

已在华为云的消息通知服务SMN注册账号并获取关键信息。获取方法如下。

登录控制台[华为云官网](#)。如果没有华为账号，请立即注册，相关操作请参见[帐号注册](#)。注册后参考[企业帐号如何完成实名认证](#)完成企业帐号实名认证。

步骤2 说明

为防止个人用户发送垃圾短信，SMN服务暂只向通过认证的企业用户提供短信功能。单击右上角的“控制台”，进入“管理控制台”界面。鼠标移动至用户名处，在下拉列表中单击“我的凭证”，进入“我的凭证”页面。在“API凭证”页签下，请获取“IAM用户名”、“账号名”、所用SMN资源对应的“项目ID”、“项目”、“所属的区域”取值。

图 4-18 获取关键信息



获取AK (Access Key ID)、SK (Secret Access Key)，即访问密钥对。

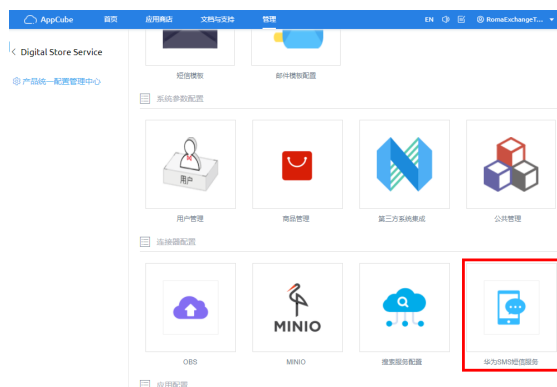
1. 在“我的凭证”页面选择“访问密钥”页签，单击“新增访问密钥”按钮。
2. 输入当前用户的登录密码。通过邮箱或者手机进行验证，输入对应的验证码。
3. 单击“确定”，在下载的文件中获取AK、SK，请妥善保管AK、SK信息。

从SMN获取短信签名的“签名ID”，用于在短信内容中携带签发内容。

步骤3 配置连接器

参考进入租户管理员配置界面进入配置界面，在界面上，单击“连接器配置”下的“华为SMS短信服务”，跳转到华为SMS短信服务连接器详情页面。

图 4-19 配置连接器



单击“新建”。

图 4-20 新建



有如下两种认证方式。不同的认证方式，连接器参数配置会有所不同。请参考该步骤中的图和表进行配置。

- 选择“密钥模式”，表示用“Access Key ID”和“Secret Access Key”验证。
- 选择“用户名密码模式”，表示用用户名、密码验证。

图 4-21 密钥模式新建连接器



图 4-22 用户名密码模式新建连接器

表 4-2 密钥模式新建连接器页面参数说明

参数	说明
名称	连接器的名称，用户自定义。
访问密钥	当认证方式为“密钥模式”时，需要配置用户的访问密钥ID（Access Key ID）。请与步骤 2 获取的“AK”取值保持一致。
密钥	当认证方式为“密钥模式”时，需要配置用户的秘密访问密钥（Secret Access Key）。请与步骤 2 中获取的“SK”取值保持一致。
项目ID	为项目的唯一标识。请与步骤 2 中获取的“项目ID”取值保持一致。
区域	所属的区域。请与步骤 2 中获取的“所属的区域”取值保持一致。
描述	可选，连接器的描述信息。

表2用户名密码模式新建连接器页面参数说明

参数	说明
名称	连接器的名称，用户自定义。
账号名	登录消息通知服务SMN的账号名。请与步骤 2 中获取的“账号名”取值保持一致。

参数	说明
项目名	该SMN用户所属的项目名。请与步骤 2中获取的“项目”取值保持一致。
用户名	使用消息通知服务SMN的用户名。请与步骤 2中获取的“IAM用户名”取值保持一致。
密码	使用消息通知服务SMN的用户名对应的密码。请与步骤 2中获取的“IAM用户名”的密码。
项目ID	项目的唯一标识。请与步骤 2中获取的“项目ID”取值保持一致。
用户类型	用户类型。 <ul style="list-style-type: none">个人用户：只测试可用。实际场景中只有企业用户才可以发短信。企业用户。
区域	所属的区域。请与步骤 2中获取的“所属的区域”取值保持一致。
描述	可选，连接器的描述信息。

配置完后，单击“保存”。

步骤4 功能测试

创建连接器后，您可进行简单的测试，测试是否能发送短信。

在连接器列表页单击连接器的名称，进入连接器的详情页。

在该连接器详情页面单击“发送测试”。

输入接收者号码和短信内容，单击“发送”。

接收者收到短信，表示测试成功。

----结束

• 短信模板配置

进入配置界面，在配置界面上，单击“模板配置”下的“短信模板”。单击需要编辑的短信类别对应的“编辑”。

图 4-23 编辑

短信模板管理

以下是所有短信模板的列表。您可以在列表单个模板时使用这些模板。

名称	类别	描述	最后修改人	最后修改时间	操作
VerifyCodeSMS	校验身份发送验证码	验证码校验	RomaExchangeTest@AT 182110x2	2020-11-02 09:46:12	编辑
IdentityApplicationApprove	发送通知	注册信息通知	RomaExchangeTest@AT 182110x2	2020-11-02 09:45:59	编辑
OrgRealnameApplicationReject	发送通知	企业实名认证失败通知	RomaExchangeTest@AT 182110x2	2020-11-02 09:46:12	编辑
PersonalRealnameApplicationReject	发送通知	个人实名认证失败通知	RomaExchangeTest@AT 182110x2	2020-11-02 09:46:23	编辑
TodoTaskReminder	发送通知	待办任务提醒	RomaExchangeTest@AT 182110x2	2020-11-02 09:47:25	编辑
OfflineSucceeded	发送通知	离线下载成功短信提醒	RomaExchangeTest@AT 182110x2	2021-04-09 16:21:58	编辑

参考界面修改短信模板的信息。

以校验身份发送验证码的短信为例，可以修改“描述”和“值”里的描述性语言，但类似下图红框的内容请不要修改，那些是系统变量参数。

图 4-24 修改短信模板信息

编辑

参数名称	VerifyCodeSMS
类别	<input type="text" value="校验身份发送验证码"/>
描述	<input type="text" value="验证码校验"/>
值	<input type="text" value="【ROMA Exchange】验证码: {VerifyCode} {DurationTime}分钟内输入有效。
(VerifyCode: {VerifyCode}, the input is valid within {DurationTime} minutes.)"/>
<input type="button" value="确认"/>	

产品初始化配置

租户部署ROMA Exchange后，需要进行一些初始化配置。

进入配置界面，在租户管理员配置界面上，单击“安装升级配置”。

单击每个参数后的🔗了解参数说明，并请参考下图和产品初始化配置说明表格进行配置。

图 4-25 安装升级配置

🔗 安装升级配置

登录配置

登录账号类型

公共配置

*主题风格 政务风 华为云

信任域名

门户网站访问域名

通知管理

是否发送邮件 是 否

是否发送短信 是 否

下载资产通知管理员

图 4-26 产品初始化配置说明

表 4-3 产品初始化配置说明

字段		说明	如何配置
登录配置	登录账号类型	登录ROMA Exchange的账号类型。	在下拉框里选择。
公共配置	主题风格	ROMA Exchange的界面风格。	选中需要的风格。
	信任域名	链接跳转时，信任域名不会有风险提示。	直接在文本框里输入，不同域名间用“;”隔离。
	门户网站访问域名	门户网站的访问域名。	直接在文本框里输入。
通知管理	是否发送邮件	是否在业务相关操作给用户发送邮件。	单选。 如果配置为“是”，需要参考邮件的配置配置。
	是否发送短信	是否在业务相关操作给用户发送短信。	单选。 如果配置为“是”，需要参考短信的配置配置。
存储服务	系统存储连接器类型	资产提供方上传资产时，需要保存资产的相关文件，因此需要用到存储。	直接在文本框里输入类型： <ul style="list-style-type: none"> ● OBS：OBS需要单独部署。推荐使用OBS。 ● MINIO：AppCube内置的存储服务。
	系统存储连接器名称	系统存储连接器的名称。	请参考配置OBS存储功能里配置。
	系统存储连接器桶名	系统存储连接器桶的名称。	请参考配置OBS存储功能里配置。

字段		说明	如何配置
云搜索服务配置	配置云搜索地址	操作日志、资产的文档，如果同步到ES，查询性能更高。也可以不配置，内容存在本地。	公有云场景下，ROMA Exchange使用的云搜索服务的地址不能与AppCube相同。 请参考AppCube指导配置后，在这里配置。 直接单击字段后的文本框，填入云搜索服务的地址。还需要参考搜索服务配置配置。
用户管理	是否需要实名认证	用户是否需要实名认证才能拥有更高权限的功能。 说明 该参数初始配置后，不建议中途修改，避免引发功能问题。	<ul style="list-style-type: none"> 是：如果用户想订阅资产，需要认证为个人实名认证用户；如果用户想发布资产，需要认证为企业实名认证用户。 否：不需要认证即可订阅或发布资产。

如果是初次安装后配置，则配置完后，单击“一键配置”；如果是升级后配置，则配置完后，单击“一键升级”，增量更新。

产品高级能力配置

📖 说明

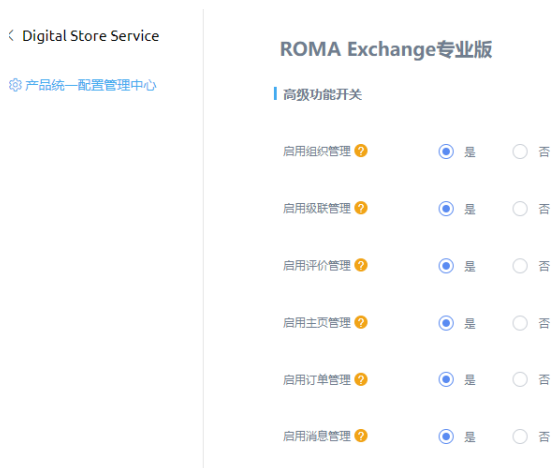
租户必须拥有System Administrator Profile权限，才可以修改“产品高级能力配置”。

运营管理员权限需设置为“Developer Profile”，共享管理员权限需设置为“SharedCenterOperation”权限。

具体权限的配置请参见“用户指南”的“在AppCube上创建用于运营管理的用户”章节和“在AppCube上创建共享中心的用户和授权”。

租户部署ROMA Exchange后，需要进行一些初始化配置。进入配置界面，在配置界面上，单击“产品高级能力配置”。单击每个参数后的🔗了解参数说明，并请参考界面图配置。

图 4-27 产品高级能力配置



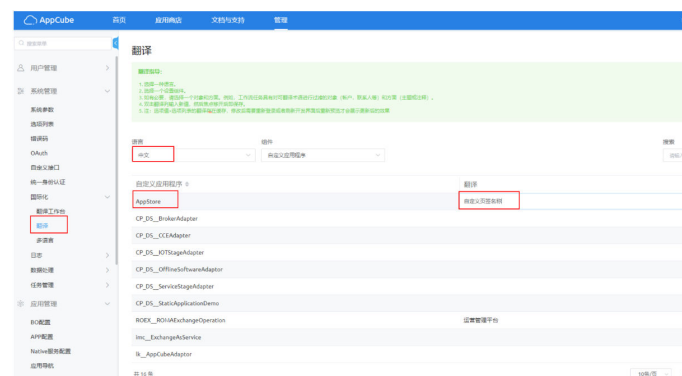
配置完成后，单击“确定”。配置完成后，对于值为“否”的功能，ROMA Exchange门户portal和运营管理台受控的功能会被隐藏。

门户页面页签名称配置

ROMA Exchange提供了门户页签名称的配置能力，用户可以根据业务需求自定义。配置方法如下：在APP Cube首页，单击“管理-系统管理-国际化-翻译”，找到对应语言下的AppStore应用程序，双击翻译列输入新的值，保存后可以在门户首页看到效果。

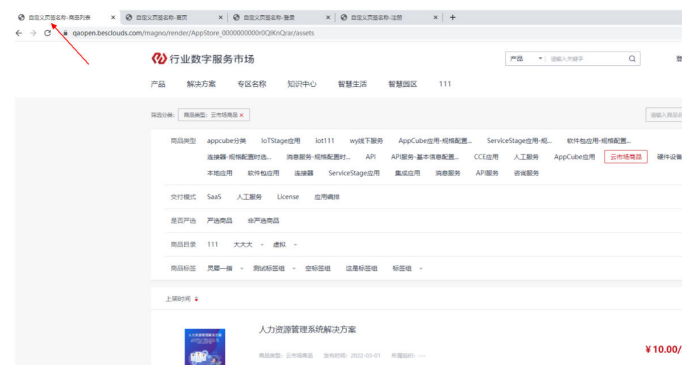
ROMA Exchange提供了默认的页签名称“数字资产运营管理平台”，用户可根据需要自定义。

图 4-28 门户页面页签名称配置 1



配置效果图:

图 4-29 门户页面页签名称配置 2

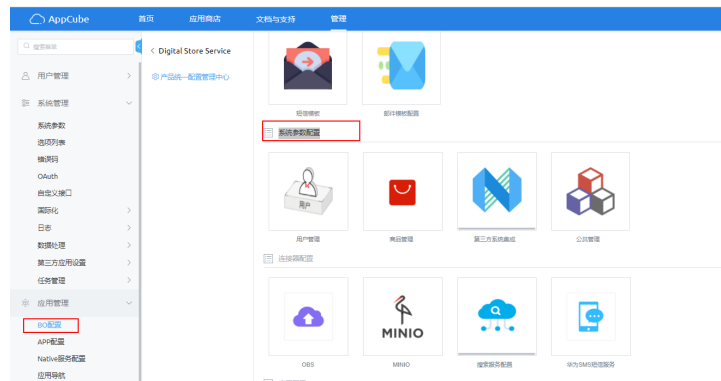


根据业务需要配置其它系统参数

ROMA Exchange提供了很多系统参数，可以根据不同的业务场景设置系统参数值。系统参数说明及配置如下：

在APP Cube首页，单击“管理-应用管理-BO配置”，找到“Digital Store Service”这个BO，单击“DigitalStoreService”，进入Digital Store Service的“产品统一配置管理中心”界面。有少量的参数在APP Cube首页，单击“管理 系统管理 系统参数”。系统参数包括用户管理、商品管理、第三方系统集成、公共管理四类，用户可以根据自己的需要找到相应的系统参数并结合界面上的参数说明进行修改。

图 4-30 根据业务需要配置其它系统参数



4.1.3 切换教育环境


获取教育相关软件包

请找华为工程师获取教育数据包“educationData.zip”。

运行教育切换脚本

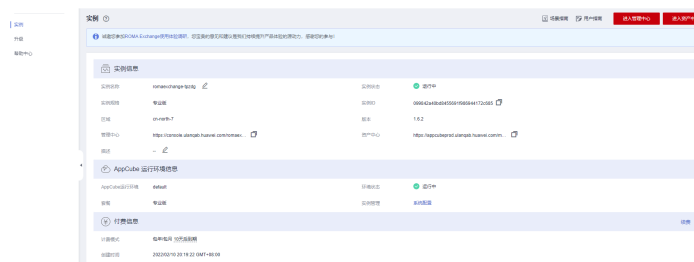
登录[华为云官网](#)。

单击界面右上角的“控制台”。

在“控制台”，选择左侧的 ，在出现的服务列表里选择“企业应用 ROMA 资产中心 ROMAExchange”，进入ROMA Exchange的控制台页面。

选择左侧的“实例”，然后再右侧页面单击“实例管理”后面的“系统配置”，进入AppCube首页。

图 4-31 进入 AppCube 首页



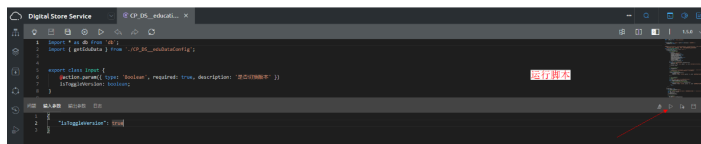
在首页的库菜单中，找到“Digital Store Service” BO文件，并单击进入。

图 4-32 进入 Digital Store Service



搜索脚本“CP_DS_educationDataMigration”并进入页面。

图 4-33 搜索脚本



在输入参数下的大括号里输入参数“isToggleVersion”: true”，然后单击头部右边的运行脚本。运行完成，查看系统输出，xx表示运行成功。

导入教育预制数据包

运行完教育切换脚本后，进行教育数据包“educationData.zip”的导入。

在AppCube的首页单击“管理”，选择菜单“系统管理 > 数据处理 > 数据导入”

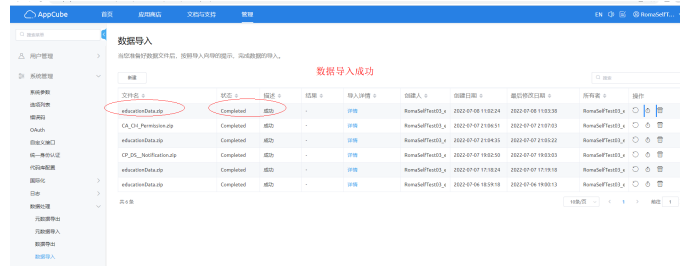
图 4-34 数据导入 1



基本信息里“导入类型”选“导入记录ID值不为空”，将教育数据包“educationData.zip”拖入“导入文件”下的框里。

单击“导入”。导入需要一会，导入后，在“数据导入”列表上可以看到导入成功的文件记录。

图 4-35 数据导入 2



Connect 来源配置

说明

如果切换教育版本之前有配置过ROMA Connect来源，则切换教育版本后之前的配置失效，用户需要重新配置。

获取connect来源相关配置参数。

下面以北京四环境为例

- 授权地址：<https://iam.cn-north-4.myhuaweicloud.com>
- 业务地址：<https://roma.cn-north-4.myhuaweicloud.com>
- 区域：cn-north-4
- 平台租户名：（华为云IAM账号）如下图所示。
- 平台用户名：如下图所示。
- 密码：如下图所示。

图 4-36 Connect 来源配置 1



获得connect来源相关配置参数后，在ROMA Exchange管理台的“系统管理 > 来源管理”对名称为“EduRomaConnectAuth”的来源进行配置。

图 4-37 Connect 来源配置 2



图 4-38 Connect 来源配置 3



相关系统参数配置

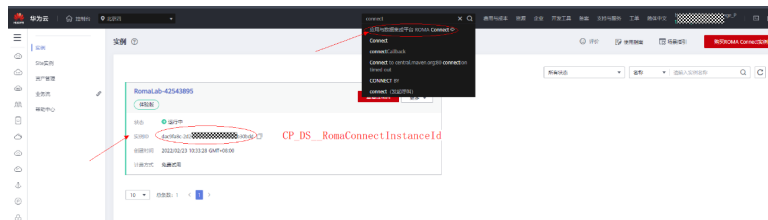
登录[华为云官网](#)。

单击界面右上角的“控制台”。

获取ROMA Connect实例ID、ROMA Connect的项目ID和服务ID，并做相关配置。

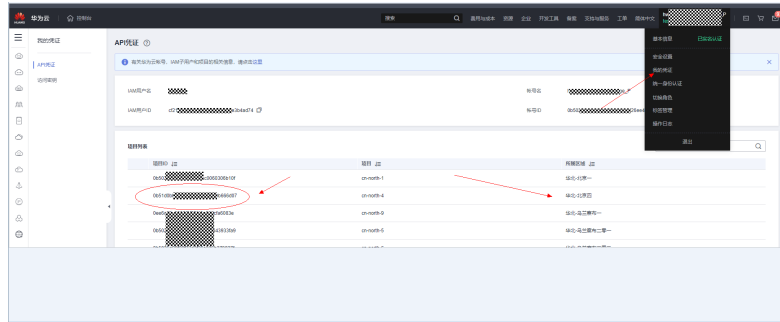
1. 在控制台的搜索框里模糊搜索ROMA Connect服务，并进入ROMA Connect服务的控制台。
2. 获取实例ID参数对应的值，该值就是CP_DS__RomaConnectInstanceId参数要配置的值。

图 4-39 Connect 来源配置 3



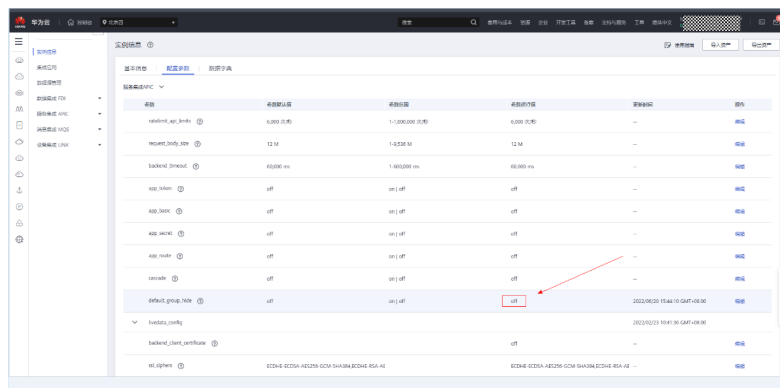
单击华为公有云页面右上角个人账号处，选择“我的凭证”。然后在页面左侧选择“API凭证”，找到并获取ROMA Connect的项目ID。该值就是CP_DS__RomaConnectProjectId参数要配置的值。

图 4-40 Connect 来源配置 4



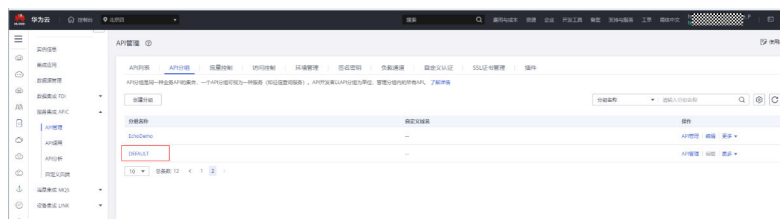
在ROMA Connect的“实例信息”里，单击“配置参数”页签，将“default_group_hide”参数运行值修改成off。

图 4-41 Connect 来源配置 5



在ROMA Connect的“服务集成APIC > API管理”里，单击“API分组”页签。

图 4-42 Connect 来源配置 6



单击“DEFAULT”分组，查看并获取服务ID的值，该值就是CP_DS_RomaGroupId参数要配置的值。

图 4-43 Connect 来源配置 7



配置CP_DS__RomaConnectInstancelId、CP_DS__RomaConnectProjectId和CP_DS__RomaGroupId参数。

进入ROMA Exchange控制台，选择左侧的“实例”，然后再右侧页面单击“实例管理”后面的“系统配置”，进入AppCube首页。

在首页上单击“管理”，然后选择“系统管理 > 系统参数”。

找到CP_DS__RomaConnectInstancelId，单击参数名称，修改参数值见下图中【值】参数。

图 4-44 Connect 来源配置 7



找到CP_DS__RomaConnectProjectId，单击参数名称，修改参数值见下图中【值】参数。

图 4-45 Connect 来源配置 8



找到CP_DS__RomaGroupId，单击参数名称，修改参数值见下图中【值】参数。

图 4-46 Connect 来源配置 8



升级版本注意事项

说明

如果基线版本升级，则用户必须参考[运行教育切换脚本](#)、[导入教育预制数据包](#)、[Connect来源配置](#)重新操作重新操作一遍。

4.2 区级管理平台环境部署（含数据中心部署）

区级管理平台环境部署

配置要求：

- 硬件配置要求
服务器标准16C/32G内存，磁盘空间要求300G以上的存储空间。
内部服务器需要互通，防火墙关闭，SELinux关闭。
- 网络设备配置要求
内部服务器之间所有端口要求互通,带宽百兆以上，接入服务器需要有ELB或VIP。
- 存储设备配置要求
磁盘空间要求300G以上的存储空间。根目录下40G以上，挂载盘300G以上。
- 服务器设备的配置要求
服务器时间要求一致，端口要求互通。
- 部署工具
远程ssh工具：xshell。
浏览器：Chrome 96.0.4664.110。

安装 docker、kubernetes（所有 k8s 节点）

安装前先卸载冲突的软件

```
yum remove docker docker-client docker-client-latest docker-common docker-latest docker-latest-logrotate  
docker-logrotate docker-engine
```

安装docker

```
cd docker && yum install -y *.rpm  
mkdir -pv /data/docker  
ln -s /data/docker/ /var/lib/docker
```

安装docker-compose

```
cd ../docker-compose && yum install -y *.rpm  
正常情况下docker和docker-compose就已经安装完成了
```

可通过查看docker确认是否安装成功

```
docker -v
```

系统初始化（所有服务器都要操作）

- 创建用户
系统运行需要创建uid和gid为2049的admin用户，先使用id admin查看是否有admin用户，有admin用户的话用户ID的组ID是多少
如果没有admin用户，则创建admin用户

```
groupadd -g 2049 admin  
useradd -g 2049 -G docker admin
```


如果已存在admin用户且UID和GID不为2049的话，需更改UID和GID

```
usermod -u 2049 admin && groupmod -g 2049 admin && gpasswd -a admin docker
```

创建admin用户后UID不为2049的情况，先使用下面命令更改下/home/admin目录的权限，

```
chown admin.admin /home/admin/ -R
```

再更改用户UID即可

```
usermod -u 2049 admin
```

查看admin用户是否创建成功

```
id admin
```

```
uid=2049(admin) gid=2049(admin) groups=2049(admin),946(docker)
```

图 4-47 查看

```
[admin@ecsningqiuyan-0001 ~]$ id admin
```

```
uid=2049(admin) gid=2049(admin) groups=2049(admin),994(docker)
```

- **系统调优**

- **关闭防火墙**

```
setenforce 0
```

```
sed -i 's/SELINUX=enforcing/SELINUX=disabled/g' /etc/selinux/config
```

```
systemctl disable --now firewalld
```

```
chmod a+x /etc/rc.d/rc.local
```

图 4-48 关闭防火墙

```
[admin@ecsningqiuyan-0001 ~]$ cat /etc/selinux/config
```

```
# This file controls the state of SELinux on the system.
```

```
# SELINUX= can take one of these three values:
```

```
#   enforcing - SELinux security policy is enforced.
```

```
#   permissive - SELinux prints warnings instead of enforcing.
```

```
#   disabled - No SELinux policy is loaded.
```

```
SELINUX=disabled
```

```
# SELINUXTYPE= can take one of three values:
```

```
#   targeted - Targeted processes are protected,
```

```
#   minimum - Modification of targeted policy. Only selected processes are protected.
```

```
#   mls - Multi Level Security protection.
```

```
SELINUXTYPE=targeted
```

- **配置iptables的ACCEPT规则**

```
iptables -F && iptables -t nat -F && iptables -t mangle -F && iptables -X
```

- **关闭swap分区**

```
swapoff -a
```

```
sed -ri 's/.*swap.*/#&/' /etc/fstab
```

- **创建docker服务相关目录**

```
mkdir -pv /data/{backup,cds,contacts,logs,tinyfs,webapps}
```

```
chown admin.admin /data/{backup,cds,contacts,logs,tinyfs,webapps}
```

- **修改docker服务配置文件**

```
mkdir -p /etc/docker
```

```
cat > /etc/docker/daemon.json <<EOF
```

```
{
```

```
  "exec-opts": ["native.cgroupdriver=systemd"],
```

```
  "log-driver": "json-file",
```

```
  "log-opts": {
```

```
    "max-size": "100m"
```

```
  }
```

```
}
```

```
EOF
```

使用Systemd管理的Cgroup来进行资源控制与管理，因为相对Cgroupfs而言，Systemd限制CPU、内存等资源更加简单和成熟稳定。

日志使用json-file格式类型存储，大小为100M，保存在/var/log/containers目录下，方便ELK等日志系统收集和管理日志。

```
systemctl daemon-reload
systemctl restart docker
systemctl enable --now docker
systemctl enable --now crond
```

设置定时清理日志任务

```
echo "0 0 */1 * * find /data/logs/ -name '*202*' -mtime +1 |xargs gzip &" >> /var/spool/cron/root
echo "0 0 */1 * * find /data/logs/ -name '*202*' -mtime +30 |xargs rm -fr &" >> /var/spool/cron/root
```

安装常用服务

```
yum install -y net-tools vim wget gdb lsof sysstat iotop wget lrzsz tree unzip nfs-utils tcpdump telnet
ntpdate yum-utils
```

调整内核参数

开启网桥模式，可将网桥的流量传递给iptables链

关闭IPv6协议

```
cat > /etc/sysctl.d/kubernetes.conf << EOF
net.bridge.bridge-nf-call-ip6tables=1
net.bridge.bridge-nf-call-iptables=1
net.IPv6.conf.all.disable_ipv6=1
net.IPv4.ip_forward=1
EOF
```

加载参数

```
sysctl --system
```

配置 k8s 镜像源（所有节点）

定义kubernetes源

```
cat > /etc/yum.repos.d/kubernetes.repo << EOF
[kubernetes]
name=Kubernetes
baseurl="镜像源地址"/kubernetes-el7-版本号
enabled=1
gpgcheck=0
repo_gpgcheck=0
gpgkey="镜像源地址"/yum-key.gpg
EOF
```

安装 kubeadm, kubelet 和 kubectl（所有节点）

```
yum install -y kubelet-1.21.3 kubeadm-1.21.3 kubectl-1.21.3
```

开机自启kubelet

```
systemctl enable kubelet.service
```

启动k8S通过kubeadm安装出来以后都是以Pod方式存在，即底层是以容器方式运行，所以kubelet必须设置开机自启

```
systemctl start kubelet.service
```

初始化 master 节点(master 节点)

```
kubeadm init \
--apiserver-advertise-address=IP地址 \
```

```
--image-repository "镜像源地址" /\n--kubernetes-version v版本号 \n--service-cidr= IP地址/12 \n--pod-network-cidr= IP地址/16
```

如果要重新初始化集群状态：kubeadm reset，然后再进行上述操作记得保存好最后的kubeadm join的信息node节点加入集群需要token!!!

也可以利用kubeadm token create --print-join-command 利用kubeadm命令重新生成token，node 节点加入集群需要token

使用 kubectl 管理工具 (master 节点)

```
mkdir -p $HOME/.kube\nsudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config\nsudo chown $(id -u):$(id -g) $HOME/.kube/config
```

查看是否成功，等待一会，同时可发现像etc，controller，scheduler等组件都以pod的方式安装成功

```
kubectl cluster-info
```

node 节点操作 (所有 node 节点)

在每个节点上执行，加入集群

```
kubeadm join 10.13.16.61:6443 --token q7glri.mjm2gperz347n99e --discovery-token-ca-cert-hash sha256:869fcc7584845d937a94f2a159a062565b64ac56b33207e2300d61fa2f98e2a7
```

安装 flannel 网络插件

下载flannel插件

```
wget https://gitcode.net/mirrors/flannel-io/flannel/-/blob/v0.20.2/Documentation/kube-flannel.yml
```

修改字段

```
net-conf.json: |\n{\n  "Network": "10.244.0.0/16", ###初始化master节点时设置一样就行 将ip段修改和上文初始化master节点一样即可\n  "Backend": {\n    "Type": "vxlan"\n  }\n}
```

发布网络

```
kubectl apply -f kube-flannel.yml
```

查看所有pod

```
kubectl get pods -A
```

如果出现Running则表示正常，如果出现Init:0/1执行以下命令，修改 flannel 插件文件，这个版本比较低，高版本 k8s 尽量选择一些高一些的版本 flannel

```
sed -i -r "s#quay.io/coreos/flannel:.*-amd64#lizhenliang/flannel:v0.12.0-amd64#g" kube-flannel.yml
```

检查各节点健康状态

查询master是否正常


```
kubectl get cs
```

如果状态为unhealthy

```
vim /etc/kubernetes/manifests/kube-scheduler.yaml  
vim /etc/kubernetes/manifests/kube-controller-manager.yaml
```

将- --port=0注释掉

部署 StorageClass

安装nfs

```
yum install -y nfs-utils rpcbind
```

手动加载 NFS 共享服务时，应该先启动 rpcbind，再启动 nfs

```
systemctl start rpcbind && systemctl enable rpcbind  
systemctl start nfs && systemctl enable nfs
```

查看 rpcbind 端口是否开启，rpcbind 服务默认使用 tcp 端口 111

```
netstat -anpt | grep rpcbind
```

创建共享目录，并授权

```
mkdir /root/data/nfs  
chmod 777 /root/data/nfs
```

编辑 exports 文件

```
vim /etc/exports  
/root/data/nfs *(rw,no_root_squash,sync)
```

保存退出

```
:wq
```

重新export一次

```
exportfs -rv
```

查看本机的共享目录

```
showmount -e  
cd /root  
kubectl apply -f storageClass.yaml
```

图 4-49 查看

```
mountPath: /persistentvolumes  
env:  
  - name: PROVISIONER_NAME  
    value: k8s-sigs.io/nfs-subdir-external-provisioner  
  - name: NFS_SERVER  
    value: 10.13.16.61 ## 指定自己nfs服务器地址  
  - name: NFS_PATH  
    value: /root/data/nfs ## nfs服务器共享的目录  
volumes:  
  - name: nfs-client-root  
    nfs:  
      server: 10.13.16.61  
      path: /root/data/nfs  
Version: v1
```

数据库连接工具(在 ops 服务器上部署)

- 配置数据库源

```
sudo rpm -Uvh https://dev.mysql.com/get/mysql80-community-release-el7-3.noarch.rpm
```

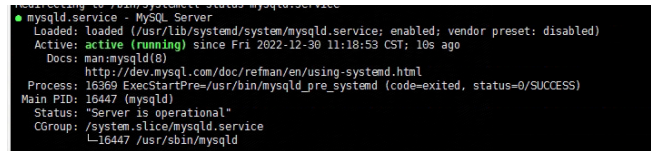
- **安装数据库连接工具**

```
sudo yum --enablerepo=mysql80-community install mysql-community-server --nogpgcheck
```

启动mysql服务

```
service mysqld start
```

图 4-50 启动



```
● mysqld.service - MySQL Server
   Loaded: loaded (/usr/lib/systemd/system/mysqld.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2022-12-30 11:18:53 CST; 10s ago
     Docs: man:mysqld(8)
           http://dev.mysql.com/doc/refman/en/using-systemd.html
   Process: 16369 ExecStartPre=/usr/bin/mysqld_pre_systemd (code=exited, status=0/SUCCESS)
   Main PID: 16447 (mysqld)
   Status: "Server is operational"
   CGroup: /system.slice/mysqld.service
           └─16447 /usr/sbin/mysqld
```

查看root临时密码

```
grep "A temporary password" /var/log/mysqld.log
```

登录数据库

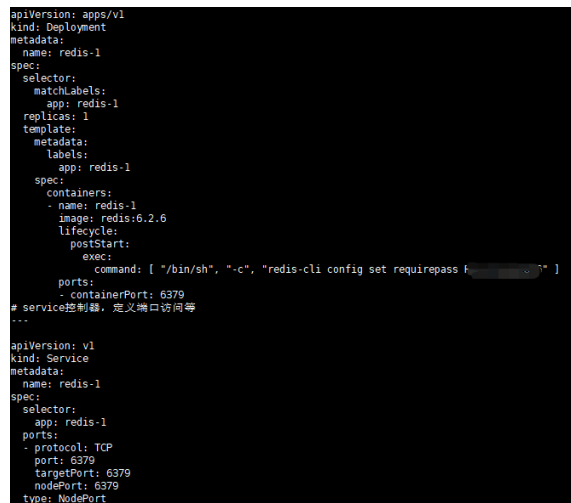
```
mysql -uroot -p"数据库密码"
```

修改数据库密码并授权

```
ALTER USER 'root'@'localhost' IDENTIFIED BY '数据库密码';
create user 'root'@'%' identified by '数据库密码' ;
grant all privileges on *.* to 'root'@'%' with grant option ;
flush privileges;
```

- **启动redis**

图 4-51 启动 redis



```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: redis-1
spec:
  selector:
    matchLabels:
      app: redis-1
  replicas: 1
  template:
    metadata:
      labels:
        app: redis-1
    spec:
      containers:
        - name: redis-1
          image: redis:6.2.6
          lifecycle:
            postStart:
              exec:
                command: [ "/bin/sh", "-c", "redis-cli config set requirepass h" ]
          ports:
            - containerPort: 6379
# service控制器, 定义端口访问等
---
apiVersion: v1
kind: Service
metadata:
  name: redis-1
spec:
  selector:
    app: redis-1
  ports:
    - protocol: TCP
      port: 6379
      targetPort: 6379
      nodePort: 6379
  type: NodePort
```

```
kubectl apply -f redis-1.yaml
```

进入容器检查redis

```
redis-cli -h redis哨兵服务器的地址 -p 6379 -a 'redis的密码' info Sentinel
```

部署 seata 服务

```
cd /root
```

```
kubectl apply -f seata-server.yaml
```

服务部署

- **修改配置文件**

将本地的 user-center-admin.jar复制到的/rhCloud/sjzx/java下

将本地的 developer-center-0.0.1-SNAPSHOT.jar复制到的/rhCloud/kfzzx/java下

将本地的 organization-center-0.0.1-SNAPSHOT.jar复制到的/rhCloud/zzzx/java下

将本地的 permissions-center-0.0.1-SNAPSHOT.jar复制到的/rhCloud/qxzx/java下

将本地的 authentication-center-0.0.1-SNAPSHOT.jar复制到的/rhCloud/rzzx/java下

修改/rhCloud/qxzx/java/java.yaml、Dockerfile配置文件

修改/rhCloud/zzzx/java/java.yaml、Dockerfile配置文件

修改/rhCloud/kfzzx/java/java.yaml、Dockerfile配置文件

修改/rhCloud/sjzx/java/java.yaml、Dockerfile配置文件

修改/rhCloud/rzzx/java/java.yaml、Dockerfile配置文件

- **Dockerfile**

图 4-52 包名称

```
[root@master java]# cat Dockerfile
FROM openjdk:8-jre
VOLUME /tmp
ADD ./developer-center-0.0.1-SNAPSHOT.jar app.jar
ENTRYPOINT ["java","-jar","/app.jar"]
EXPOSE 8080
```

java包名称

修改nginx配置

配置文件在/rhCloud/rzzx/nginx/nginx-configmap.yaml

配置文件在/rhCloud/qxzx/nginx/nginx-configmap.yaml

配置文件在/rhCloud/zzzx/nginx/nginx-configmap.yaml

配置文件在/rhCloud/kfzzx/nginx/nginx-configmap.yaml

配置文件在/rhCloud/sjzx/nginx/nginx-configmap.yaml

配置文件在/rhCloud/zhjy/nginx/nginx-configmap.yaml

图 4-53 修改 nginx 配置

```
gzip on;
include /etc/nginx/conf.d/*.conf;
# 新增service及个
server {
    listen 80;
    charset utf-8;
    client_max_body_size 600M;
    server_name 10.8.120.4;
    location / {
        root /usr/share/nginx/html/kaifazhezongxin;
        index index.html index.htm;
        try_files $uri $uri/ /index.html;
    }
    location /api-kfzz/ {
        proxy_pass http://10.8.120.4:8530;
        proxy_redirect default;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header Host $host;
        proxy_set_header Upgrade-Insecure-Requests 1;
        proxy_set_header X-Forwarded-Proto http;
    }
    location /api-rzzx/ {
        proxy_pass http://10.8.120.4:52270;
        proxy_redirect default;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header Host $host;
        proxy_set_header Upgrade-Insecure-Requests 1;
        proxy_set_header X-Forwarded-Proto http;
    }
    location /api-zzzx/ {
        proxy_pass http://10.8.120.4:61131;
        proxy_redirect default;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header Host $host;
        proxy_set_header Upgrade-Insecure-Requests 1;
        proxy_set_header X-Forwarded-Proto http;
    }
}
```

```
kubectl apply -f nginx-configmap.yaml
```

修改前端挂载目录

配置文件在/rhCloud/rzzx/nginx/nginx-pvc.yaml

配置文件在/rhCloud/qxzx/nginx/nginx-pvc.yaml

配置文件在/rhCloud/zzzx/nginx/nginx-pvc.yaml

配置文件在/rhCloud/kfzzx/nginx/nginx-pvc.yaml

配置文件在/rhCloud/sjzx/nginx/nginx-pvc.yaml

配置文件在/rhCloud/zhjy/nginx/nginx-pvc.yaml

图 4-54 修改前端挂载目录

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: nginx-web
  namespace: kfzzx
  annotations:
    volume.beta.kubernetes.io/storage-class: nfs-storage # 在 storageclass.yaml 中已 name == 0
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 20G
```

```
kubectl apply -f nginx-pvc.yaml
```

修改nginx.yaml项目配置文件

配置文件在/rhCloud/rzzx/nginx/nginx.yaml

配置文件在/rhCloud/qxzx/nginx/nginx.yaml

配置文件在/rhCloud/zzzx/nginx/nginx.yaml

配置文件在/rhCloud/kfzzx/nginx/nginx.yaml

配置文件在/rhCloud/sjzx/nginx/nginx.yaml

配置文件在/rhCloud/zhjy/nginx/nginx.yaml

图 4-55 修改 nginx.yaml 项目配置文件

```
metadata:
  labels:
    app: nginx
spec:
  nodeSelector:
    name: "node-1"
  containers:
    - name: nginx
      image: nginx:1.23.3
      ports:
        - containerPort: 80
      volumeMounts:
        - name: nginx-web
          mountPath: /usr/share/nginx/html
        - name: nginx-conf
          mountPath: /etc/nginx/nginx.conf
          subPath: nginx.conf
      volumes:
        - name: nginx-web
          persistentVolumeClaim:
            claimName: nginx-web
        - name: nginx-conf
          configMap:
            name: nginx-config
# service控制器，定义端口访问等
---
apiVersion: v1
kind: Service
metadata:
  name: nginx
  namespace: kfzxx
spec:
  selector:
    app: nginx
  ports:
    - protocol: TCP
      port: 80
      targetPort: 80
      nodePort: 558
      type: NodePort
```

```
kubectl apply -f nginx.yaml
```

- **启动服务**

以数据中心为例：

后端部署方式

```
cd /rhCloud/sjzx/java
bash restart.sh
```

前端部署方式

将项目打好的包dist包放在对应目录下

```
cd /root/data/nfs
kfzxx-nginx-web-pvc-8db0b2d4-bbe6-46c5-88a6-7e2363b1d033
qxzx-nginx-web-pvc-5d0ccd38-3f7d-4d45-90de-a85fcf78b955
rzzx-nginx-web-pvc-24131e74-ca7a-4634-81ec-47e3f71278a8
sjzx-nginx-web-pvc-69c8c590-8580-40e6-a70b-a8752c40f582
zhjy-nginx-web-pvc-7402ccbb-f828-4247-bc25-f07f9a1d5e5e
zzzx-nginx-web-pvc-58e3122b-cbfd-4822-8328-716bcc8f27b
```

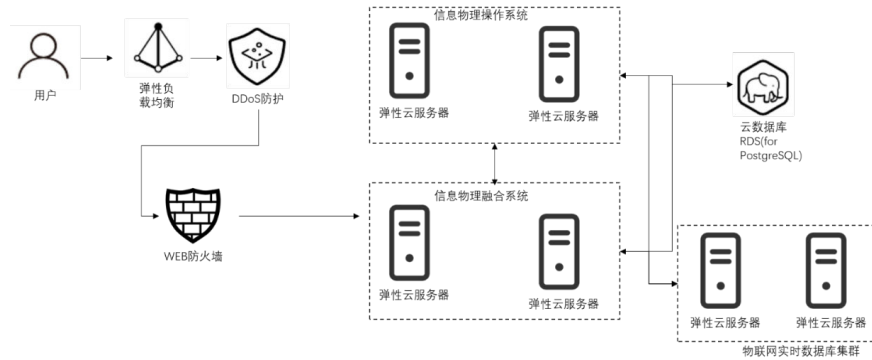
图 4-56 前端部署方式

```
[root@master nginx]# cd /root/data/nfs/
[root@master nfs]# ls
kfzxx-nginx-web-pvc-8db0b2d4-bbe6-46c5-88a6-7e2363b1d033
qxzx-nginx-web-pvc-5d0ccd38-3f7d-4d45-90de-a85fcf78b955
rzzx-nginx-web-pvc-24131e74-ca7a-4634-81ec-47e3f71278a8
sjzx-nginx-web-pvc-69c8c590-8580-40e6-a70b-a8752c40f582
zhjy-nginx-web-pvc-7402ccbb-f828-4247-bc25-f07f9a1d5e5e
zzzx-nginx-web-pvc-58e3122b-cbfd-4822-8328-716bcc8f27b
```

4.3 物联中心应用环境部署

部署组网

图 4-57 部署组网



配置要求

- **硬件配置要求**
 - 两台服务器标准16c64G内存，磁盘空间要求300G以上的存储空间，用于安装信息物理整合系统。
 - 两台服务器标准4c16G内存，磁盘空间要求300G以上的存储空间，用于安装信息物理操作系统。
 - 两台服务器标准16c64G内存，磁盘空间要求1T以上的存储空间，用于安装物联网实时数据库。
 - 云数据库标准规格PostgreSQL12，主备，4核8GB，SSD云盘500GBI以上的存储空间。
 - 内部服务器需要互通，防火墙关闭。
- **网络设备配置要求**

内部服务器之间所有端口要求互通，带宽百兆以上。
- **存储设备配置要求**

磁盘空间要求1T以上的存储空间。C盘系统盘60G以上，数据盘1T以上
- **服务器设备的配置要求**

服务器时间要求一致，端口要求互通
- **部署工具**

远程工具：远程桌面
浏览器：Chrome

云服务资源开通

- **ECS**

弹性云服务器（Elastic Cloud Server，ECS）是由CPU、内存、操作系统、云硬盘组成的基础的计算组件。弹性云服务器创建成功后，您就可以像使用自己的本地

PC或物理服务器一样，在云上使用弹性云服务器。详情参考[帮助文档](#)。本次使用ECS来安装部署物联中心，作为物联中心的信息物理整合系统服务器、信息物理操作系统服务器和物联网实时数据库服务器。

开通后的资源如下所示：

表 4-4 资源

系统	规格	内网地址	EIP
信息物理操作系统	规格: X86计算 通用型 c7.4xlarge.4 16vCPUs 64GiB 镜像: Windows Server 2019 Datacenter 64bit 系统盘: 高IO 300GB	192.168.0.152	124.70.24.119
		192.168.0.210	
信息物理融合系统	规格: X86计算 通用型 c7.xlarge.4 4vCPUs 16GiB 镜像: Windows Server 2019 Datacenter 64bit 系统盘: 高IO 300GB	192.168.0.152	/
		192.168.0.207	
物联网实时数据库	规格: X86计算 通用型 c7.4xlarge.4 16vCPUs 64GiB 镜像: Windows Server 2019 Datacenter 64bit 系统盘: 高IO 60GB 数据盘:1T	192.168.0.42	/
		192.168.0.43	

- **RDS**

一种基于云计算平台的可即开即用、稳定可靠、弹性伸缩、便捷管理的在线关系型数据库服务。RDS 具有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。详情参考[帮助文档](#)。本方案使用RDS-PostgreSQL实例作为物联中心的业务数据库。

开通后的资源如下所示：

表 4-5 资源

系统	规格	内网地址	EIP
DB	数据库类型: 云数据库RDS (PostgreSQL) 规格: 主备 4 vCPUs 16 GB 500GB	192.168.0.72	/

- **EIP**

弹性公网IP (Elastic IP, 简称EIP) 提供独立的公网IP资源，包括公网IP地址与公网出口带宽服务。可以与弹性云服务器、裸金属服务器、虚拟IP、弹性负载均衡、NAT网关等资源灵活地绑定及解绑。详情参考[帮助文档](#)。

a. 登录华为云 弹性公网IP

- b. 单击“弹性公网IP和带宽”->“弹性公网IP”，单击右上角的“创建弹性公网IP”

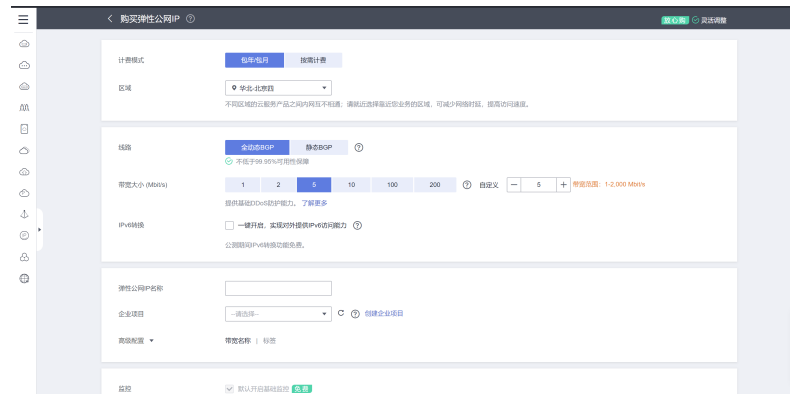
线路：全动态BGP

公网带宽：独享带宽

带宽大小：5

购买量：1

图 4-58 创建弹性公网 IP



云服务网络配置

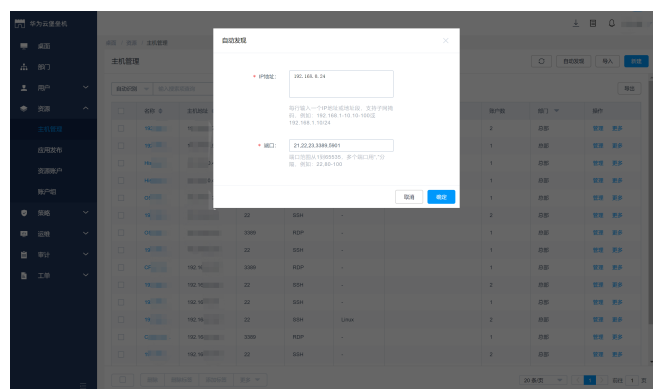
云堡垒机CBH配置

云堡垒机（Cloud Bastion Host, CBH）是华为云的一款4A统一安全管控平台，为企业提供集中的账号（Account）、授权（Authorization）、认证（Authentication）和审计（Audit）管理服务。

登录云堡垒机

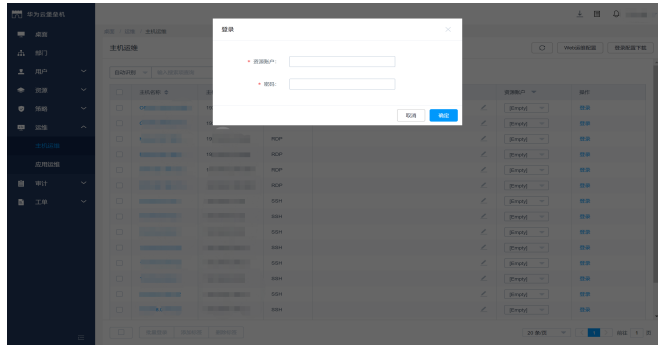
在主机管理中添加主机

图 4-59 登录云堡垒机 1



在主机运维菜单中可选择某个主机进行远程运维。

图 4-60 登录云堡垒机 2



应用安装

- 涉及软件及版本

表 4-6 软件及版本

序号	软件	软件名	软件版本
1	新思联信息物理操作系统	ThingsOS	V3.0
2	新思联信息物理融合系统	ThingsCyber	V3.0
3	物联网实时数据库	ThingsHistory	V3.0

- 安装包准备

由新思联提供软件包。

- 安装过程

新思联信息物理操作系统：

- 将安装包解压缩到C盘，ThingsOS目录；
- 打开解压后的目录C:/ThingsOS，执行“安装服务.bat”

新思联信息物理融合系统：

- 将安装包解压缩到C盘，ThingsCyber目录；
- 打开解压后的目录C:/ ThingsCyber，执行“安装服务.bat”

物联网实时数据库：

- 将安装包解压缩到C盘，ThingsHistory目录；
- 打开解压后的目录C:/ ThingsHistory，执行“安装服务.bat”

4.4 数字基座客户端服务开通

WeLink 开通服务

注册welink学校租户的流程如下：

- 步骤1** 您可以直接单击[免费注册学校套餐](#)，或者在[华为云WeLink首页](#)单击“免费注册”，申请免费试用。
- 步骤2** 输入手机号，填写验证码后，单击“下一步”。

图 4-61 注册



The screenshot shows the '注册WeLink企业' (Register WeLink Enterprise) page. It features a form with the following elements: a phone number input field with a dropdown for '+86' and a label '手机号'; a verification code input field with a '获取验证码' (Get Verification Code) button; a radio button for '我已阅读并同意《隐私政策声明》与《华为云WeLink服务使用声明》' (I have read and agree to the Privacy Policy Statement and the Huawei Cloud WeLink Service Usage Statement); a large blue '下一步' (Next Step) button; and a link at the bottom that says '已有账号? 立即登录' (Already have an account? Log in immediately).

- 步骤3** 填写您的学校名称、您的姓名、邮箱、行业，单击“创建”。

图 4-62 创建



步骤4 注册成功, 请到手机端WeLink设置登录密码: 输入您的手机号, 单击获取短信验证码并输入。选择您的学校后, 设置您的登录密码, 即可登录WeLink。

图 4-63 登录



----结束

WeLink 实名认证

学校账号实名认证步骤如下（举例使用华为账号实名认证）：

步骤1 单击管理后台首页的“立即认证”或者单击“设置 > 学校信息”，在学校中文名称后，单击“实名认证”。

图 4-64 实名认证 1



步骤2 此时分四种情况：

1. 没有华为账号

可使用WeLink免登华为云，直接进行实名认证。

进入实名认证界面，单击“没有华为云账号”，进入下一步。

图 4-65 实名认证 2



2. 已有华为账号但未确认绑定WeLink学校

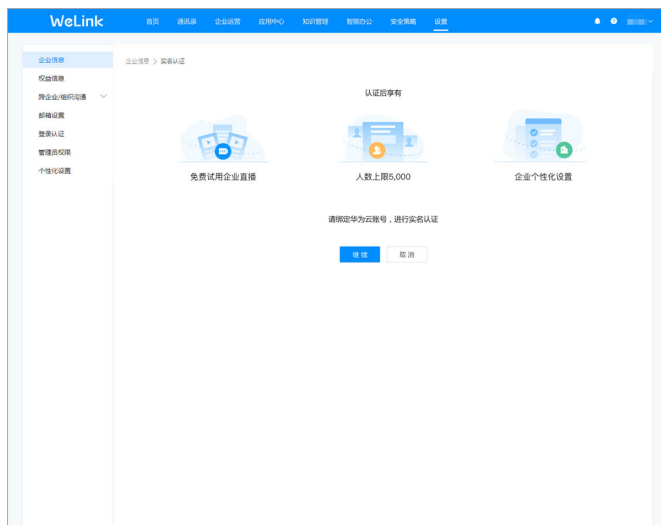
可登录华为账号绑定WeLink学校，再进行实名认证。

进入实名认证界面，单击“已有华为云账号”，进入下一步

3. 已有华为账号但未绑定WeLink学校

进入实名认证界面，单击“继续”。进入下一步

图 4-66 实名认证 3



4. 已有华为账号且已绑定WeLink学校
进入下一步

步骤3 登录华为账号。

图 4-67 登录华为云账号



步骤4 绑定WeLink学校。

单击“立即绑定”，即可绑定WeLink学校。

图 4-68 绑定 1



如后续需要更换绑定的华为账号，在管理后台，单击“设置 > 权益信息”，在下方的“已绑定华为云账号”，单击“更改”。即可更换绑定的华为账号。

图 4-69 绑定 2



步骤5 学校华为账号实名认证。

在学校华为账号实名认证界面，选择“企业账号”。

图 4-70 认证 1



学校账号实名认证分为银行对公账户认证和学校证件认证两种方式，总体流程如下：

图 4-71 认证 2



说明

welink实名认证其他方式：1.通过银行对公账户认证；2.通过学校证件认证

----结束

WeLink 与区级管理平台对接设置

初始化流程

1. 区级管理平台调用应用市场RomaExchange接口“区级管理平台查询学校基座编码”，获取各学校的基座编码和学校名称。
2. 校级管理员在WeLink开通租户。
3. 校级管理员在WeLink创建预集成应用，获取client_id, client_key并完成相应接口权限申请。
4. 校级管理员将client_id, client_key发送或同步给区级管理平台管理员补充学校对接信息完成注册。
5. 区级管理平台利用client_id, client_key调用学校WeLink租户查询企业信息接口查询学校信息。接口<https://open.welink.huaweicloud.com/docs/#/990hh0/whokyc/e3d0zi>，获取租户信息：唯一标识符、中文名称、标识等信息。
6. 区级管理平台利用client_id, client_key调用学校WeLink租户创建企业内部集成应用接口创建集成应用。

创建通讯录同步的微码应用

步骤1 WeLink管理员登录Welink后台管理页面，单击应用菜单，进入应用管理页面；在应用管理页面单击“到开放平台创建”，进入Welink开放平台。

图 4-72 进入 1



图 4-73 进入 2

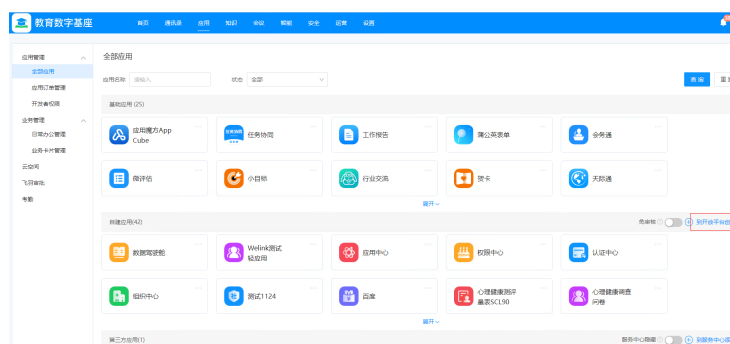


图 4-74 进入 3



步骤2 在应用开发页面选择企业内部应用->轻应用，单击“创建轻应用”，进入应用创建界面，填写应用信息，单击保存。

图 4-75 轻应用 1



图 4-76 轻应用 2



图 4-77 轻应用 3



步骤3 应用信息保存成功，进入应用【开发指引】界面；单击“申请权限”进入权限申请界面，将需要的接口权限申请授权，授权之后状态变成“已开通”

图 4-78 进入应用 1



图 4-79 进入应用 2



图 4-80 进入应用 3

WeLink日志			
身份与鉴权			
权限名称	权限描述	状态	操作
用户登录信息	获取用户的基本信息，用于登录系统和应用	已开通	取消授权
轻应用鉴权	轻应用鉴权，用于调用JS-API	已开通	取消授权
通讯录			
权限名称	权限描述	状态	操作
租户详细信息	获取租户详细信息，如租户名称、许可、规模等	已开通	取消授权
组织架构信息	获取通讯录组织架构信息，包括部门列表、人员列表、角色列表等	已开通	取消授权
用户简单信息	根据部门ID获取部门内所有用户简单信息，如用户ID、中英文名等	已开通	取消授权
用户详细信息	根据用户ID或者部门ID获取用户详细数据，如中英文名、手机号等	已开通	取消授权
通讯录同步	企业向WeLink同步通讯录信息，支持实时与异步操作，包含增删改等	已开通	取消授权
用户邮箱信息	获取用户信息，包括邮箱等敏感信息	已开通	取消授权
用户权限信息	获取用户权限信息，包括分城管理员所管理的部门范围等	已开通	取消授权

图 4-81 进入应用 4

消息推送			
权限名称	权限描述	状态	操作
公众号消息	通过公众号推送通知消息	已开通	取消授权
小助手推送	以小助手形式推送信息，提醒直达用户	已开通	取消授权
待办			
权限名称	权限描述	状态	操作
待办通知	将待办事项推送到WeLink	已开通	取消授权

步骤4 预置应用发布操作，在版本管理进行发布版本，免审核发布。（在WeLink管理后台设置免审核操作，开启免审核按钮）

图 4-82 预置应用免审核发布 1

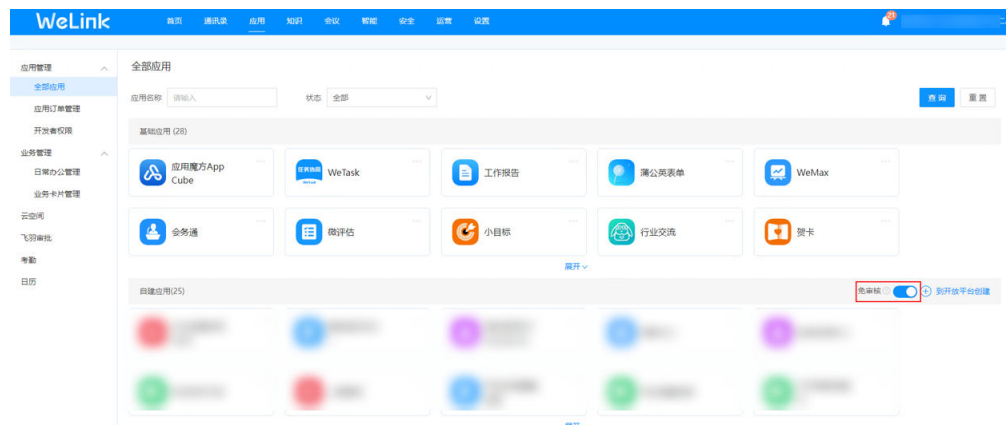


图 4-83 预置应用免审核发布 2



---结束

到区级管理平台注册学校

步骤1 校级管理员登录Welink开放平台，单击创建好的预集成应用，进入应用的基本信息页面，获取应用的client_id和client_secret

图 4-84 预集成应用基本信息 1



图 4-85 预集成应用基本信息 2



步骤2 校级管理员将预置应用的client_id和client_secret发送给区级管理平台管理员；区级管理平台管理员汇总进入区级管理平台组织中心->机构管理->机构信息页面，单击“新增”按钮，进入新增机构（学校）界面，填写完包括预置应用的client_id和client_secret的信息后单击保存，完成机构新增（学校注册）。

图 4-86 机构新增 1

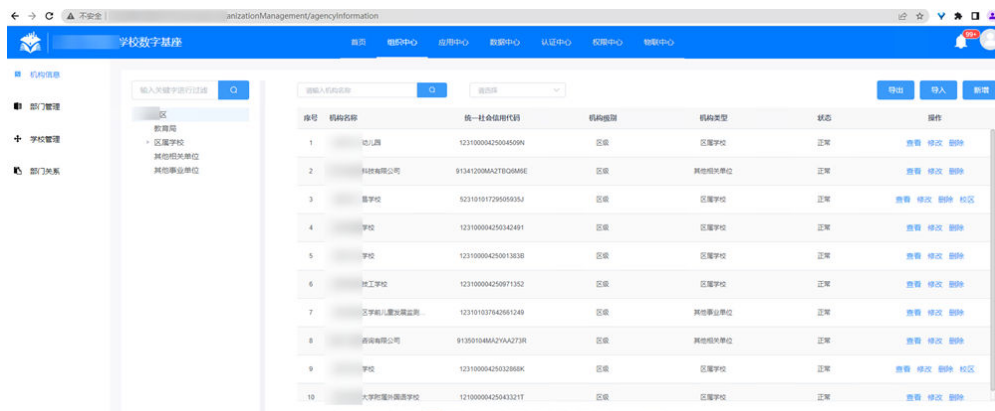
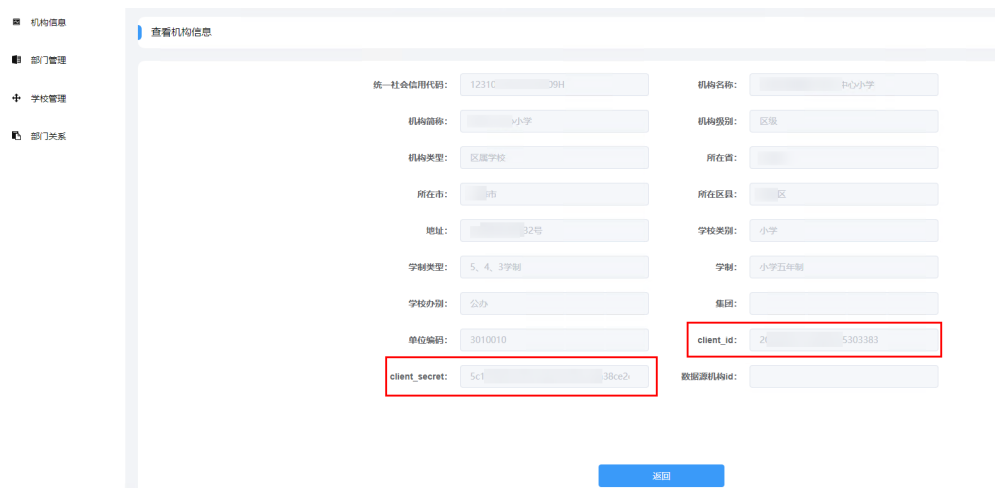


图 4-87 机构新增 2



----结束

同步数字基座默认应用

两个区统建应用：XX区教育数字基座和应用反馈中心，以【XX区教育数字基座】应用作为样例，进行分发到WeLink：

图 4-88 XX 区教育数字基座



图 4-89 应用反馈中心



步骤1 开发者登录区级管理平台->开发者平台，应用上架->应用管理创建区统建应用【XX区教育数字基座】，填写应用信息，单击提交。

图 4-90 开发者平台



图 4-91 应用信息 1



图 4-92 应用信息 2



步骤2 区级管理平台->应用中心完成应用审核流程【区管、运营人员角色】，相关角色审核处理

图 4-93 角色审核 1



图 4-94 角色审核 2

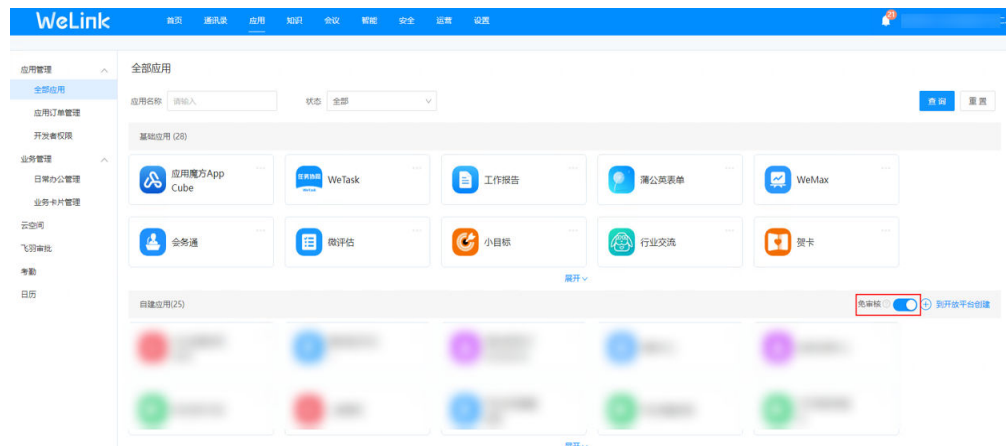


步骤3 应用上架中（应用中心），同时调WeLink的创建自建应用、提交审核接口（已选择分发机构范围 WeLink租户），WeLink租户管理后台开启免审核功能

图 4-95 应用上架



图 4-96 免审核

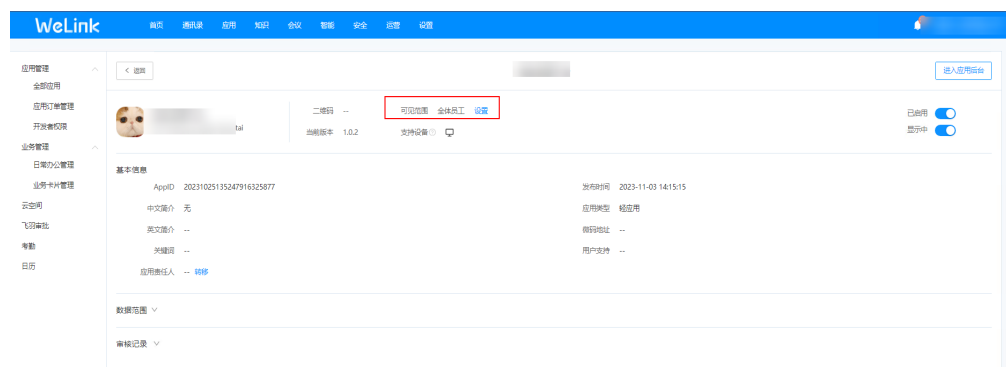


步骤4 在WeLink开放平台自动发布应用（前提条件：开启免审核），在管理后台设置应用可见范围

图 4-97 自动发布应用



图 4-98 设置应用可见范围



步骤5 发布成功的【XX区教育数字基座】，在WeLink端进行展示，单击免登跳转访问成功

图 4-99 XX 区教育数字基座发布成功

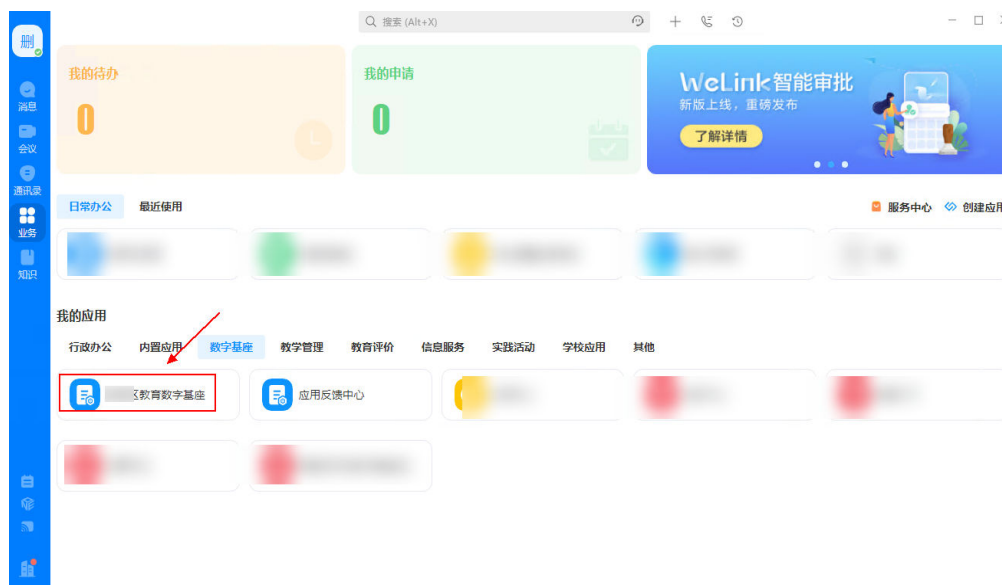


图 4-100 免登访问



----结束

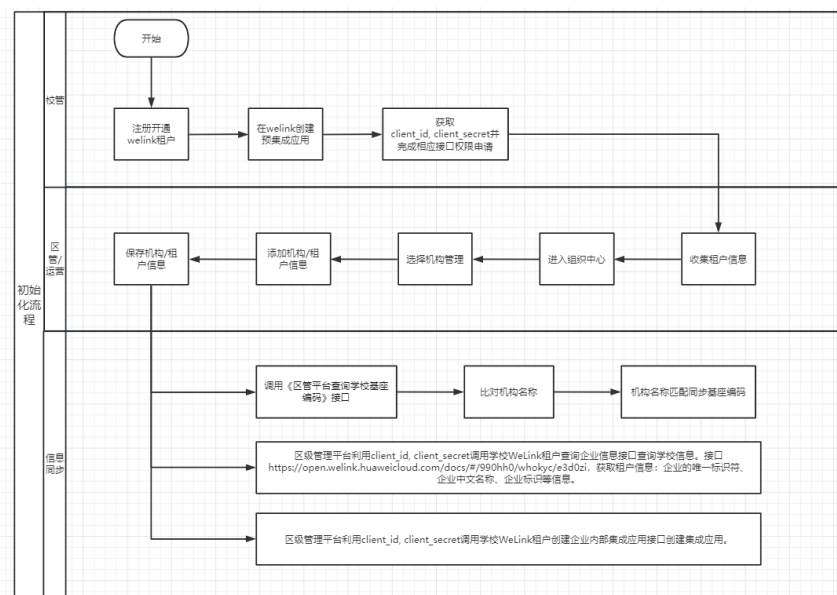
5 集成对接

区级管理平台与 WeLink 集成对接

前提条件：区级管理平台已按照WeLink接口规范完成接口开发。

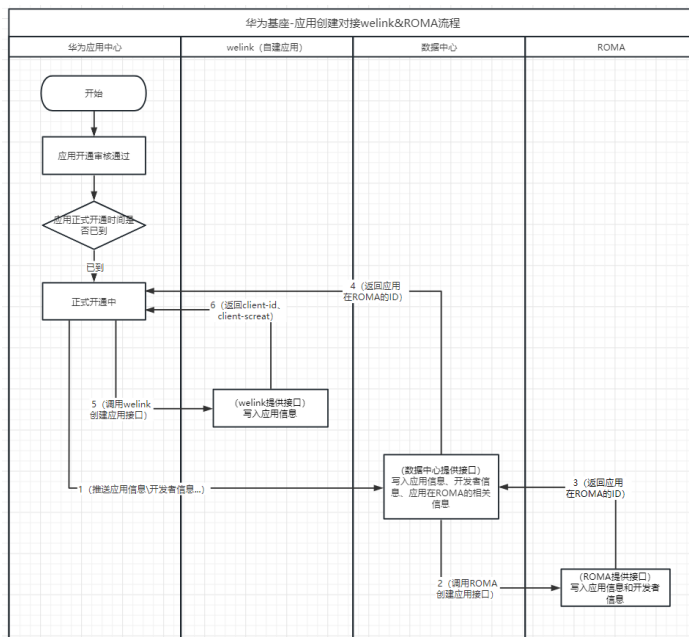
修改WeLink地址配置（联邦认证）

图 5-1 区级管理平台与 WeLink 集成对接



区级管理平台与 RomaExchange 集成对接

图 5-2 区级管理平台与 RomaExchange 集成对接



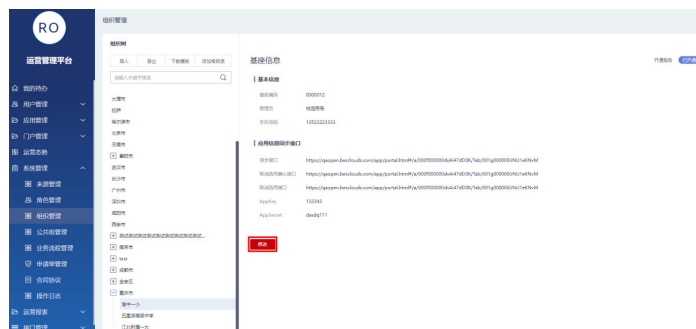
1. 华为区级基座-应用中心，应用创建完成首次正式开通后，调用数据中心提供的创建应用的接口将应用信息和开发者信息写入到数据中心；
2. 数据中心调用ROMA 创建应用的接口再将应用信息和开发者信息写入到ROMA，应用写入ROMA 区分为市应用和区校应用；
3. 数据中心在ROMA创建应用成功之后，将返回的应用在ROMA的ID再返回到应用中心。

配置指导：

进入RomaExchange的运营管理员界面。

选择“系统管理 > 组织管理”，找到并单击需要配置应用信息同步的组织。

图 5-3 配置指导



单击“修改”，然后在“应用信息同步接口”下的相应参数里，填入前提条件里收集的信息。

图 5-4 信息

基座信息

基本信息

- 基座编码: 0000012
- 管理员: 校选用号
- 手机号码: 13522223333

应用信息同步接口 由基座提供商提供

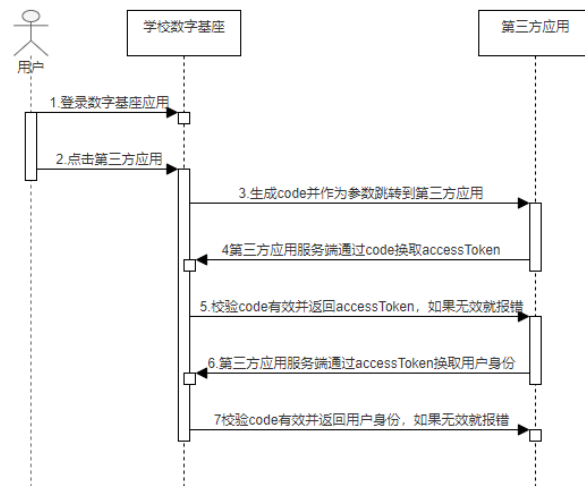
- 同步接口: https://qaopen.besclouds.com/app/portal.html#/a/000f00c
- 取消选用确认接口: https://qaopen.besclouds.com/app/portal.html#/a/000f00c
- 取消选用接口: https://qaopen.besclouds.com/app/portal.html#/a/000f00c
- AppKey: 132343
- AppSecret: dasdq111

提交 取消

区级管理平台与物联中心应用集成对接

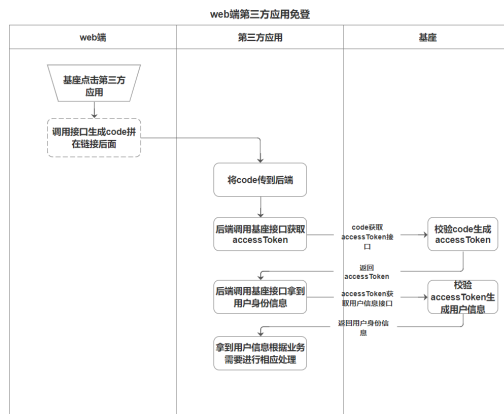
Web端（浏览器）应用跳转第三方应用采用OAuth2.0的授权码模式来实现免登。时序图如下：

图 5-5 时序



流程图如下：

图 5-6 流程



物联中心与区级管理平台，做按钮集成展示；再以独立应用上架到WeLink。

6 修订记录

表 6-1 修订记录

发布日期	修订记录
2024-05-07	规范词、敏感词专项处理，章节优化
2024-02-19	版本更新
2024-01-30	版本更新
2023-12-21	内容刷新
2023-03-30	内容刷新
2023-01-10	第一次正式发布。