等级运维-技术设计方案

2020年06月

CONTENTS

目录

CONTENTS

目录

01 整体方案 – 建设等级运维平台，连通市县两级业务系统

平台定位

- 作为运维系统，提供对业务系统模块的版本更新，状态监控，日志查看等功能
- 作为跨网段调用服务，通过异步方式协助业务系统完成市级与区县级的功能交互

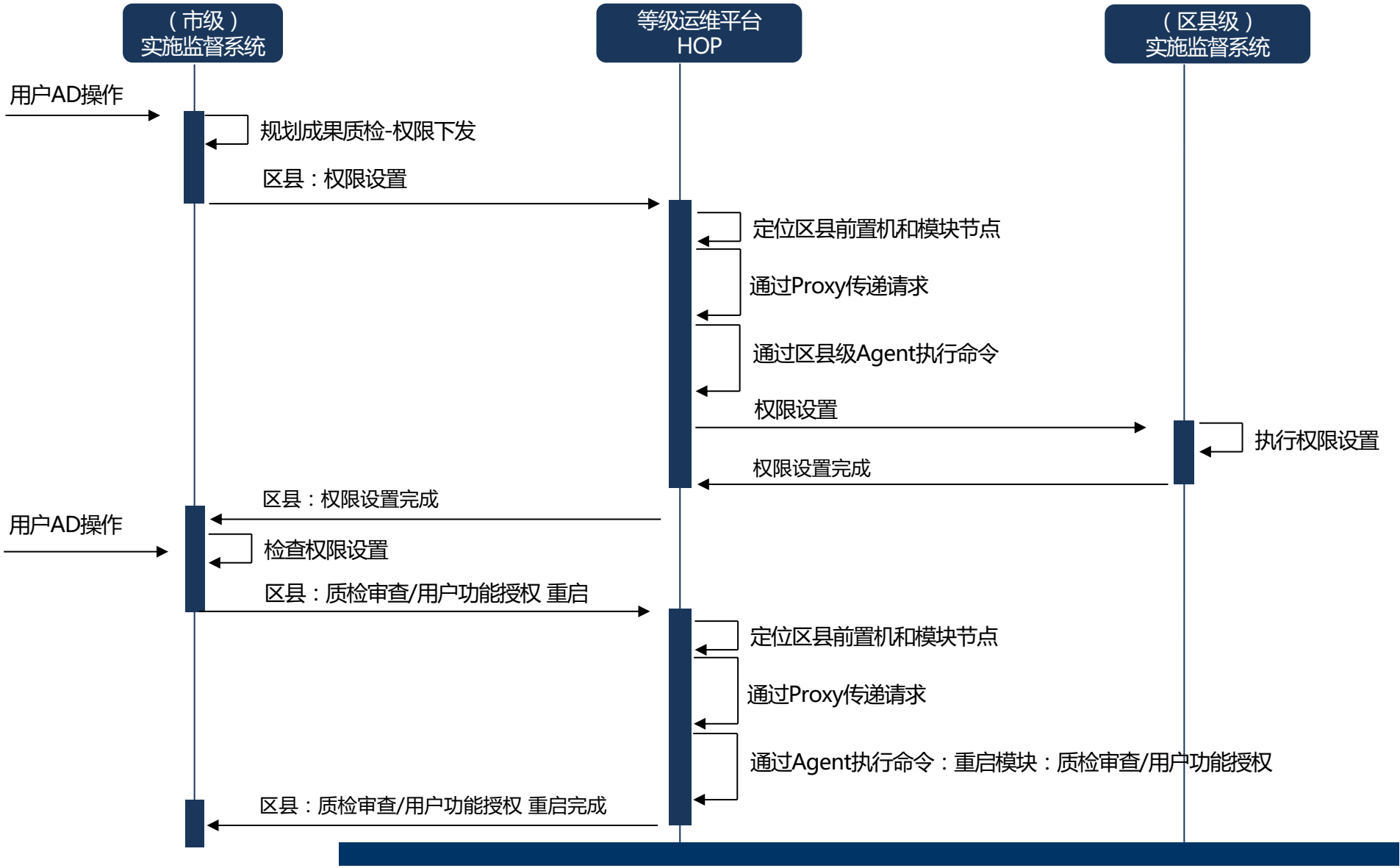
技术特点：

- 高扩展性：功能模块可扩充，充分满足业务需求
- 高稳定性：微服务架构，各模块独立部署，均可横向扩展
- 高安全性：业务系统与等级运维平台之间、等级运维平台内部通信均需验证各自签名，确保不被伪造调用

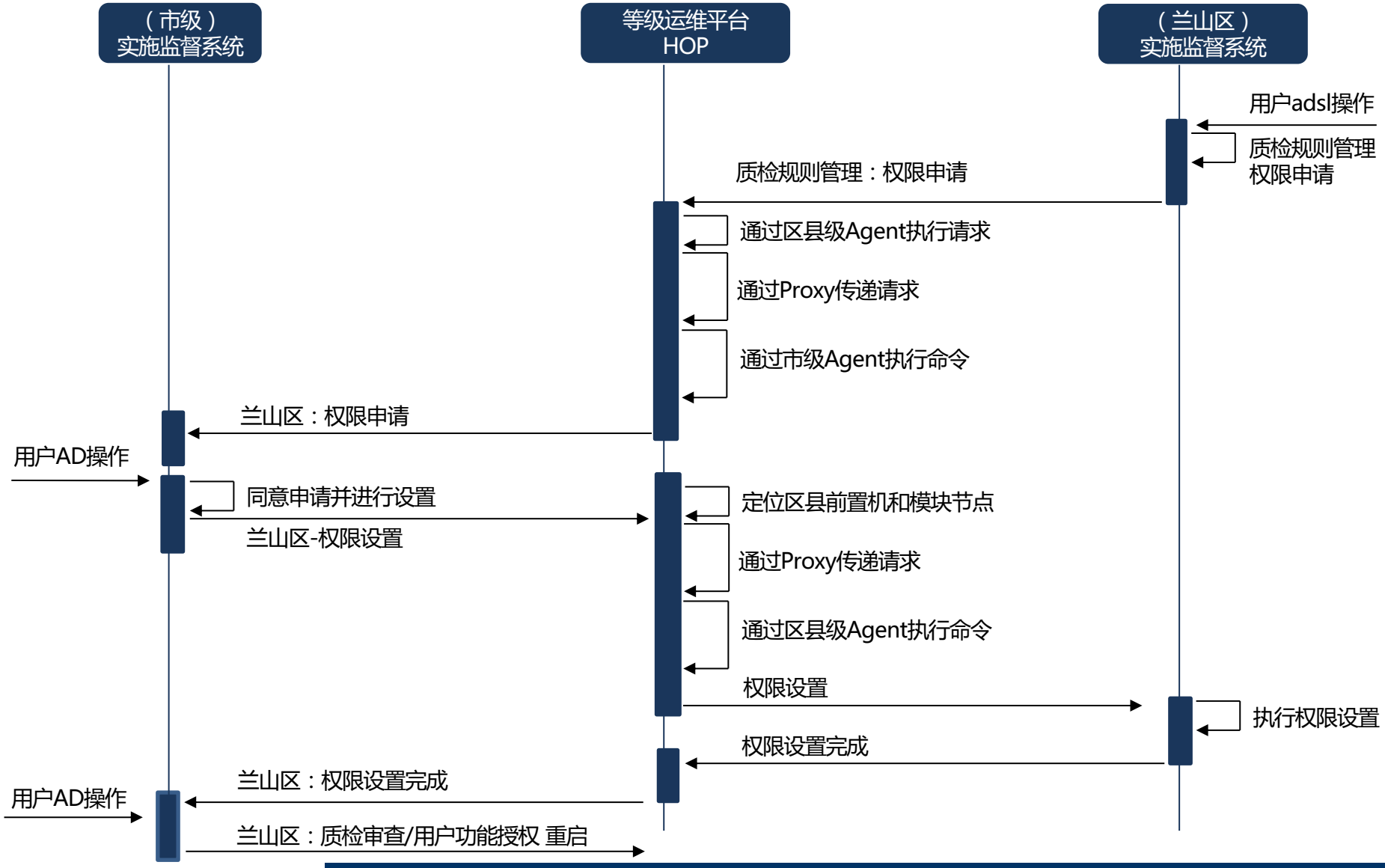
CONTENTS

目录

02 业务场景 – 市级对区县进行权限下发



02 业务场景 – 区县向市级进行权限申请



CONTENTS

目录

03 等级运维平台功能 – 系统运维

- 模块版本更新

市级业务系统可以上传模块打包文件到HOP上完成区县级业务系统的版本更新或回滚

- 模块重启

市级业务系统可以重启区县级业务系统模块

- 系统监控

HOP上可查看市级或区县级各系统模块的状态

03 等级运维平台功能 – 系统运维 – 协议

- 协议：模块版本更新

HID	HName	ModuleName	ModuleValue	ModuleVersion	NotifyUrl	SIG

- 协议：模块重启

HID	HName	ModuleName	NotifyUrl	SIG

- 协议：模块回滚

HID	HName	ModuleName	ModuleVersion	NotifyUrl	SIG

- 回调（回调时会同时附加原始请求协议作为参数）

Token	Result	Description

  - Token：业务系统对Hop发起请求时得到的票据凭证
  - Result：本次请求的结果，0：成功，1：失败
  - Description：原始返回的执行结果（由业务系统定义）
  - SIG：签名（HOP的签名，业务系统需要用HOP的公钥验证）

03 等级运维平台功能 – 系统运维 – 协议 – 版本更新

- 协议：模块版本更新

HID	HName	ModuleName	ModuleValue	ModuleVersion	NotifyUrl	SIG

- HID
  - 市区县ID，例：102
- HName
  - 市区县Name，例：兰山区
- ModuleName
  - 模块名称，例：AccessControl
- ModuleValue
  - 模块的部署tar包做base64编码后得到的字符串，等级运维平台会将此tar包按当前时间放到模块的部署路径下
  - 例：权限控制模块部署到：/var/data/accesscontrol/202006231700/
- ModuleVersion
  - 模块版本号，建议按时间命名，HOP会将此版本号与部署路径关联，以便进行回滚，例：202006231600
- NotifyUrl
  - 回调接口，由HOP发起Http请求（将协议的回调结果及原始请求协议作为参数，JSON格式），如：http://192.168.10.2/api/data/
- SIG
  - 签名（业务系统的签名，HOP需要用业务系统的公钥验证）

03 等级运维平台功能 – 权限运维

- 功能权限设置

市级业务系统设置区县级业务系统的功能权限

- 功能权限申请

区县级业务系统可以申请功能权限（审批后通过市级的“功能权限设置”进行下发）

- 数据权限设置

市级业务系统设置区县级业务系统的数据权限

- 数据权限申请

区县级业务系统可以申请数据权限（审批后通过市级的“数据权限设置”进行下发）

注：以上具体操作都需要业务系统落地执行，HOP只协助传递信息数据

03 等级运维平台功能 – 权限运维 – 协议

- 协议：功能权限设置

HID	HName	ModuleName	Function	AuthType	RoleID	UserID	ApproveUser	ApproveStatus	TargetUrl	NotifyUrl	SIG

- 协议：数据权限设置

HID	HName	ModuleName	Data	AuthType	RoleID	UserID	ApproveUser	ApproveStatus	TargetUrl	NotifyUrl	SIG

- 协议：功能权限申请

HID	HName	ModuleName	Function	AuthType	RoleID	UserID	ApplyUser	TargetUrl	NotifyUrl	SIG

- 协议：数据权限申请

HID	HName	ModuleName	Data	AuthType	RoleID	UserID	ApplyUser	TargetUrl	NotifyUrl	SIG

- 回调（回调时会同时附加原始请求协议作为参数）

Token	Result	Description

  - Token：业务系统对Hop发起请求时得到的票据凭证
  - Result：本次请求的结果，0：成功，1：失败
  - Description：原始返回的执行结果（由业务系统定义）
  - SIG：签名（HOP的签名，业务系统需要用HOP的公钥验证）

03 等级运维平台功能 – 权限运维 – 协议 – 功能权限设置

- 协议：功能权限设置

HID	HName	ModuleName	Function	AuthType	RoleID	UserID	ApproveUser	ApproveStatus	TargetUrl	NotifyUrl	SIG

- HID
  - 市区县ID，例：102
- HName
  - 市区县Name，例：兰山区
- ModuleName
  - 模块名称，例：AccessControl
- Function（*）
  - 由业务系统制定的功能权限设置，如：001（代表地图查看）
- AuthType（*）
  - 授权类型，如：0代表对角色授权，1代表对用户授权
- RoleID（*）
  - 角色ID
- UserID（*）
  - 用户ID
- ApproveUser（*）
  - 审核用户ID
- ApproveStatus（*）
  - 审核状态
- TargetUrl
  - 模块执行此操作的接口，由Agent发起Http请求（将协议作为参数，JSON格式），如：http://172.10.10.2/api/data/
- NotifyUrl
  - 回调接口，由HOP发起Http请求（将协议的回调结果及原始请求协议作为参数，JSON格式），如：http://192.168.10.2/api/data/
- SIG
  - 签名（业务系统的签名，HOP需要用业务系统的公钥验证）

03 等级运维平台功能 – 数据运维

- 数据更新

市级业务系统可以修改区县级业务系统的数据

- 数据库操作

市级业务系统可以在区县级数据库进行操作

注：数据更新操作需要业务系统落地执行，HOP只协助传递信息数据

03 等级运维平台功能 – 数据运维 – 协议

- 协议：数据更新

HID	HName	ModuleName	Data	OldValue	NewValue	Memo	TargetUrl	NotifyUrl	SIG

- 协议：数据库操作

HID	HName	ModuleName	DbName	SQL	NotifyUrl	SIG

- 回调（回调时会同时附加原始请求协议作为参数）

Token	Result	Description

  - Token：业务系统对Hop发起请求时得到的票据凭证
  - Result：本次请求的结果，0：成功，1：失败
  - Description：原始返回的执行结果（由业务系统定义）
  - SIG：签名（HOP的签名，业务系统需要用HOP的公钥验证）

03 等级运维平台功能 – 数据运维 – 协议 – 数据更新

- 协议：数据更新

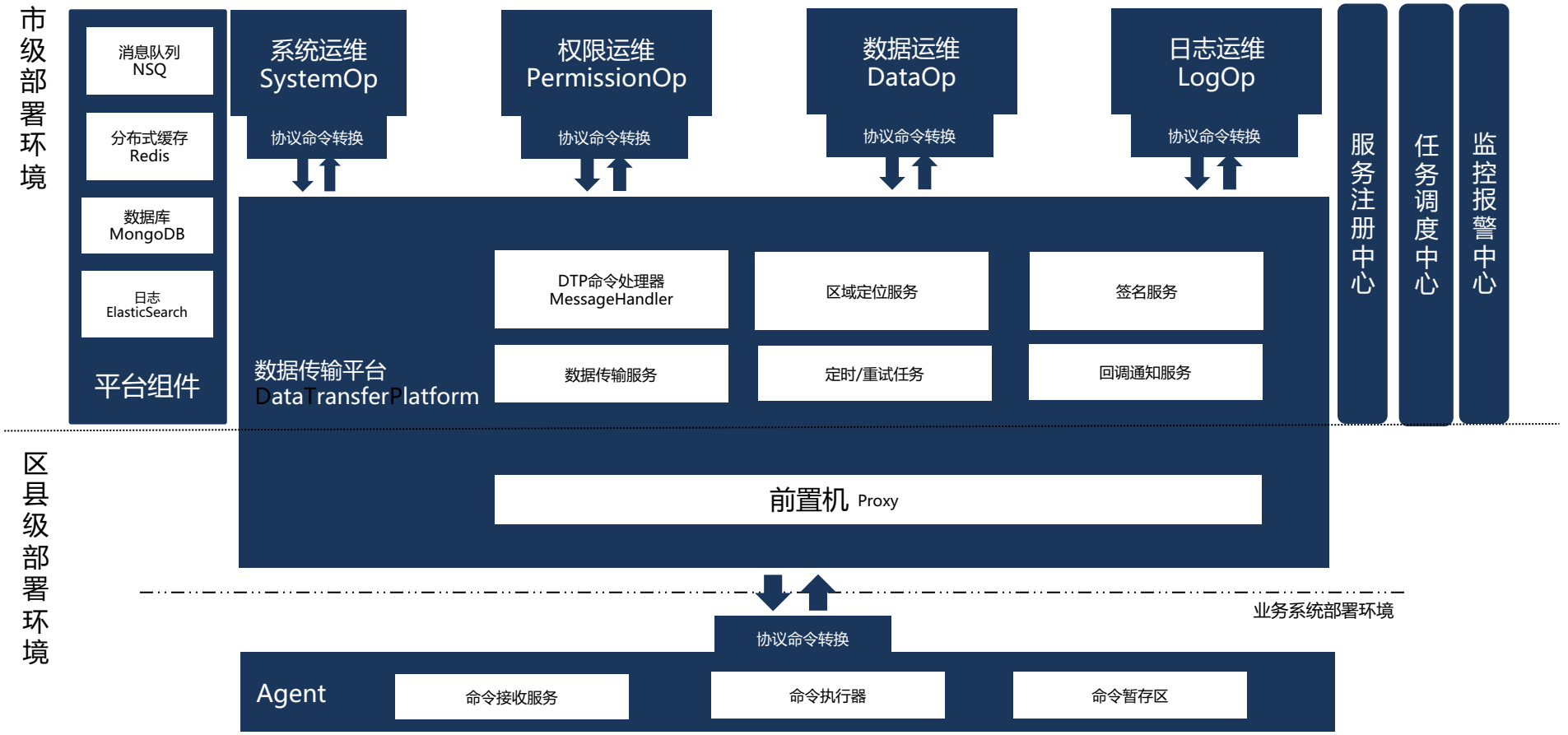
HID	HName	ModuleName	Data	OldValue	NewValue	Memo	TargetUrl	NotifyUrl	SIG

- HID
  - 市区县ID，例：102
- HName
  - 市区县Name，例：兰山区
- ModuleName
  - 模块名称，例：AccessControl
- Data（*）
  - 由业务系统制定的数据类型，如：001|123，类型是权限，ID是123
- OldValue（*）
  - 原始值
- NewValue（*）
  - 新值
- Memo（*）
  - 备注
- TargetUrl
  - 模块执行此操作的接口，由Agent发起Http请求（将协议作为参数，JSON格式），如：http://172.10.10.2/api/data/
- NotifyUrl
  - 回调接口，由HOP发起Http请求（将协议的回调结果及原始请求协议作为参数，JSON格式），如：http://192.168.10.2/api/data/
- SIG
  - 签名（业务系统的签名，HOP需要用业务系统的公钥验证）

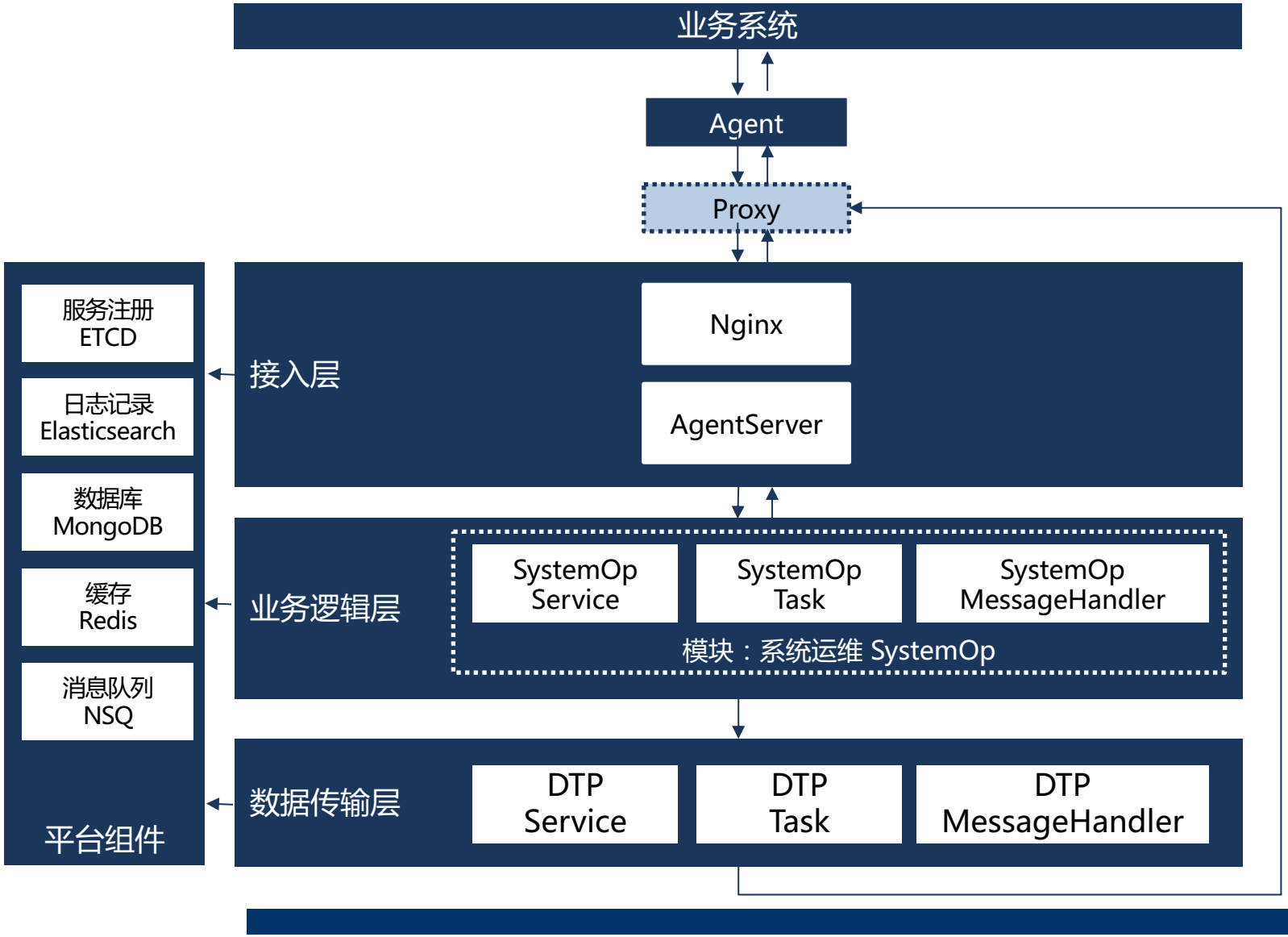
CONTENTS

目录

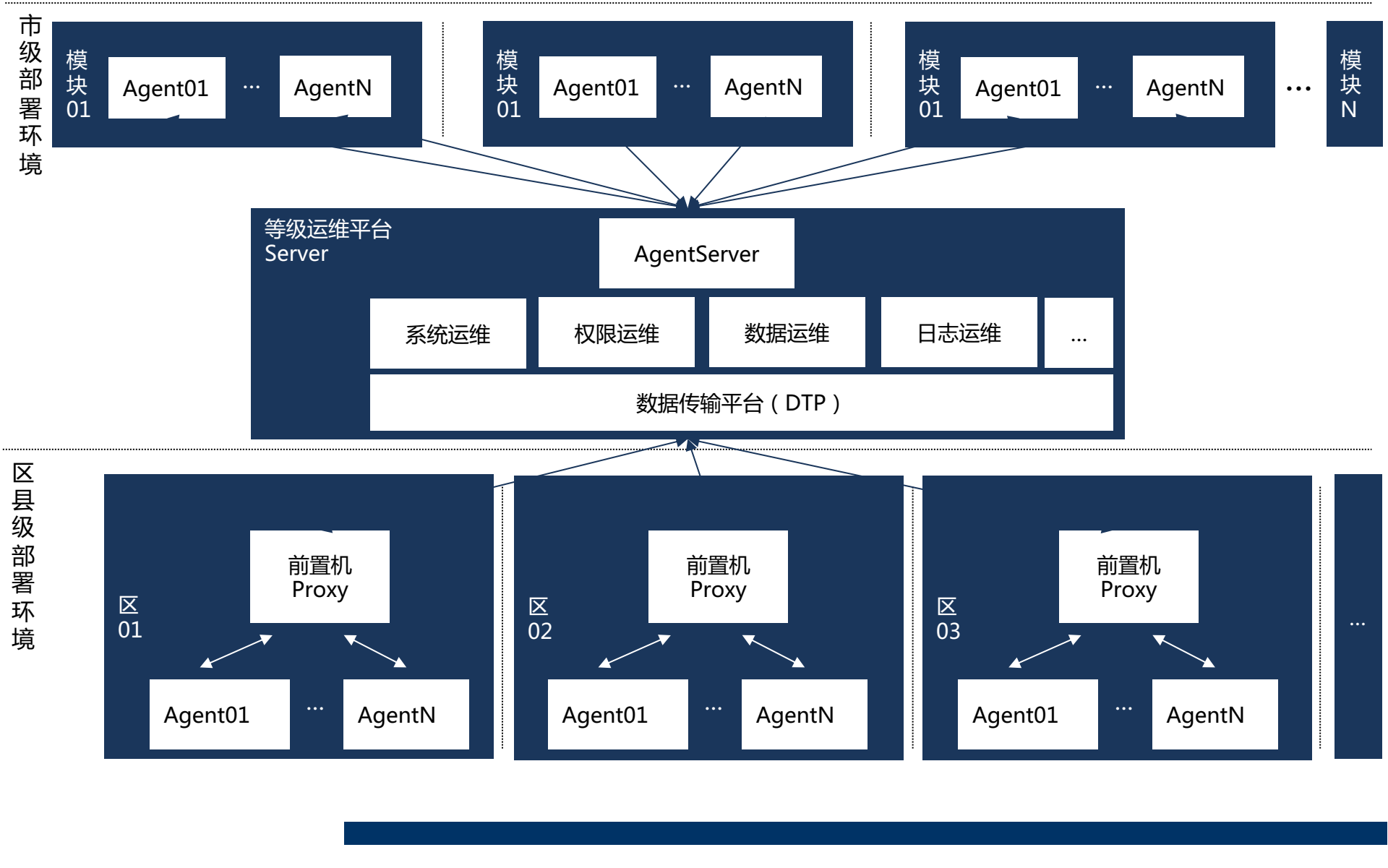
04 等级运维平台架构 – 应用架构



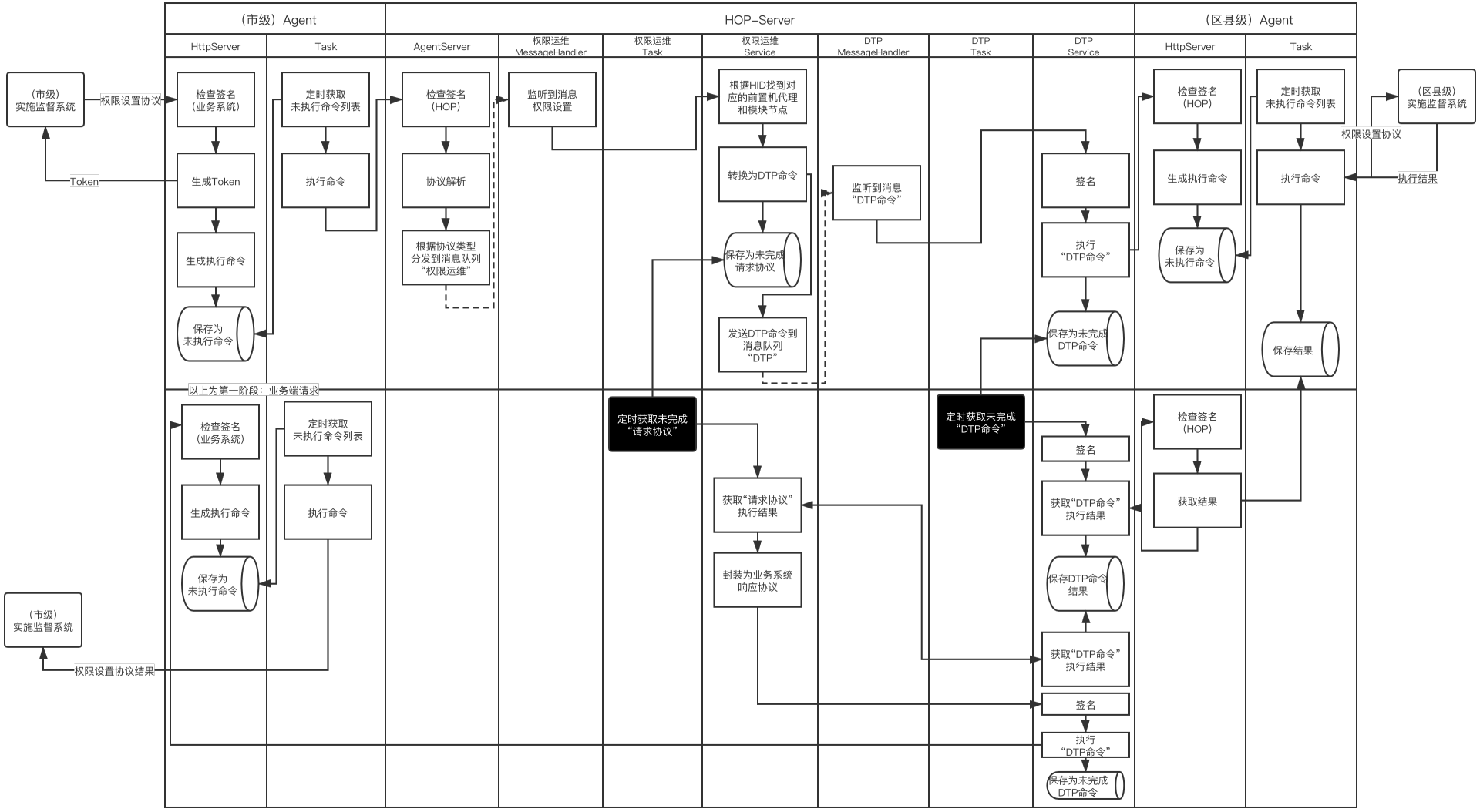
04 等级运维平台架构 – 系统架构



04 等级运维平台架构 – 部署架构



04 等级运维平台架构 – 核心流程



请求流程

1、业务系统按约定协议对本机的Agent发起Http请求
2、Agent接收请求并暂存
3、Agent的定时任务将此请求提交到Server
4、Server通过消息队列分发此请求到具体的模块进行处理（图中为权限运维模块）
5、权限运维模块将此请求转换为DTP命令并发送到DTP，同时将其保存为“**未完成的请求**”
6、DTP将此命令传输到对应的业务系统节点所在的Agent，同时将其保存为“**未完成的命令**”
7、Agent接收此请求并暂存
8、Agent的定时任务执行此请求并保存结果

回调流程

1、DTP定时获取“**未完成的命令**”并调用对应的Agent获取命令执行结果
2、权限运维模块定时获取“**未完成的请求**”并调用DTP获取请求执行结果
3、权限运维模块获取到请求执行的结果后按回调协议封装为DTP命令并发送给DTP
4、DTP将此命令传输到对应的业务系统节点所在的Agent
5、Agent接收此回调请求并暂存
6、Agent的定时任务执行此回调请求并保存结果

04 等级运维平台架构 – 部署说明

- 区县级-环境
  - 每个前置机上部署Proxy
- 市级-环境
  - 部署等级运维平台Server
- 市级和区县级-环境
  - 每个业务系统模块节点所在服务器部署Agent

04 等级运维平台架构 – 部署说明 – Proxy配置

- Proxy需设置用户名和密码，如：

```
<Auth>
    <User>user001</User>
    <Pwd>pwd001</Pwd>
</Auth>
```

- HOP中需配置每个Proxy的信息，如：

```
<Proxys>
    <Proxy>
        <ID>001</ID>
        <IP>172.10.10.2</IP>，Proxy的IP
        <Port>5001</Port>， Proxy的端口
        <User>user001</User>， Proxy的用户名
        <Pwd>pwd001</Pwd>， Proxy的密码
    </Proxy>
    ……
</Proxys>
```

04 等级运维平台架构 – 部署说明 – Server配置

- HOP中需配置每个业务模块的信息及部署路径，如：

```
<Modules>
    <Module>
        <Name>AccessControl</Name>
        <Title>权限控制</Title>
        <Nodes>
            <Node>
                <Proxy>001</Proxy>，前置机网络代理ID，市级系统无需配置
                <HID>1002</HID>，市区县ID
                <HType>1</HType>，0：市，1：区县
                <HName>兰山区</HName>
                <DeployPath>/var/data/accesscontrol/</DeployPath>，部署路径
                <AchivePath>/var/achive/accesscontrol/</DeployPath> ，归档路径，每次版本更新时保存
                <LogPath>/var/log/accesscontrol/</LogPath> ，日志路径
                <StartCMD>./app.sh –start</StartCMD>，启动命令
                <StopCMD>./app.sh –stop</StopCMD>，停止命令
                <HealthCheck>/health.api</HealthCheck>，健康检查，Agent通过http方式访问模块此接口，返回0代表正常
            </Node>
        </Nodes>
    </Module>
</Modules>
```

04 等级运维平台架构 – 部署说明 – Server配置

- HOP中需配置每个业务模块的数据库信息（*），如：

```
<Dbs>
    <Db>
        <Name>RightDb</Name>
        <Title>权限库</Title>
        <ConnectionUrl>jdbc:oracle:thin:@172.10.10...</ConnectionUrl>
        <Username>user</Username>
        <Password>pass</Password>
    </Db>
    ……
</Dbs>
```

04 等级运维平台架构 – 部署说明 – Agent配置

- 业务系统的每个模块所在服务器需部署Agent
- 每个Agent需保存该市或区县级业务系统颁发的公钥用于验签
- Agent中需配置Server端的信息，如：

```
<Servers>
    <Server>
        <ID>001</ID>
        <IP>172.10.10.2</IP>，Server的IP
        <Port>5002</Port>， Server的端口
    </Server>
    ……
</Servers>
```

- 区县级的Agent中需配置该区县前置机的Proxy信息，如：

```
<Proxys>
    <Proxy>
        <ID>001</ID>
        <IP>172.10.10.2</IP>，Proxy的IP
        <Port>5001</Port>， Proxy的端口
        <User>user001</User>， Proxy的用户名
        <Pwd>pwd001</Pwd>， Proxy的密码
    </Proxy>
    ……
</Proxys>
```

04 等级运维平台架构 – 部署说明 – DTP命令

- 等级运维平台中传输及执行的命令都为DTP命令，协议如下：
  - Token：请求凭证
  - Proxy：代理IP
  - ProxyUser：用户名
  - ProxyUser：密码
  - ModuleName：模块名称
  - ModuleConfig：模块配置
  - ExecuteNodeType：执行节点类型，如：0：所有节点都需执行，1：任意节点执行
  - CMDType：命令类型，如：0：bash指令，1：Http请求，2：数据库操作，3、自定义命令
  - CMD：命令内容，如：./app.sh –start，curl -d ‘参数‘ –X -POST http://172.10.10.2/data/
  - CMDParm：命令参数，如： –start
  - Result：执行原始结果
  - SIG：DTP签名
  - Protocol：原始协议

汇报完毕