增值税管理平台   
外购系统架构评估报告

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本/状态 | 作者 | 参与者 | 起止日期 | 备注 |
| 1A | Zrz |  | 2016-9-5 | 1A 完成 第一部分 ATA 质量属性效用树创建及第一轮架构方法分析 |
| 1.1A | Zrz |  | 2016-9-9 | 完成 第二部分 ATA 非功能场景分级及第二轮架构方法验算与评估 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## 1. 基本信息

|  |  |  |  |
| --- | --- | --- | --- |
| 待评审的外购软件产品 | |  | |
| 技术评审方式 | | ATAM | |
| 评审时间 | | 2016-09-02 | |
| 评审地点 | | 深圳航天信息 - 研发部 | |
| **参加技术评审的人员** | | | |
| **类别** | **名字** | **工作单位** | **职称、职务：** |
| 主持人 |  |  |  |
| 评审  小组  成员 |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| 记录员 |  |  |  |
| 作者 | **Zrz** | 深圳航天信息 | **系统架构师** |
|  |  |  |
|  |  |  |
| 其他  人员 |  |  |  |
|  |  |  |

## 2. 架构权衡分析（ATA）

### 第一部分：调查

#### 1）质量属性效用归集：

|  |  |
| --- | --- |
| 质量属性 | 优先级（1、2、3、5、8、13、21、34） \* 34为最高 |
| 性能 | 13 |
| 可用性（含可靠性） | 21 |
| 安全性 | 34 |
| 可修改性 | 8 |
| 可变性 | 5 |
| 功能性 | 21 |
| 互操作性 | 2 |

注：以上指标评级以标准平台系统为基准，未考虑定制系统的特型需求；涉及特性系统及各业务子系统时，请需求人员、客户代表、开发人员协商酌情修正之。

#### 2）架构方法分析

|  |  |  |
| --- | --- | --- |
| 质量属性 | 架构方法/现状 | 改进期望 |
| 性能 | memcache 缓存服务 | 期望memcache缓存可以支持停机恢复，并使该特性在对象级可配置。 |
| Redis key-value数据库 | 承包商其他项目中有使用Redis消息队列,但外购产品中尚未支持消息队列，望集成此特性，并支持缓存服务器集群环境。 |
| Nginx动静分离 | N/A |
| 服务采用Restful风格（传递JSON） | 框架中是否也有采用SOA或存在服务总线的实现？<待证实> |
|  |  |
|  |  |
| 可用性（含可靠性） | Nginx应用层负载均衡 | 此为单故障点，承包商之前将此方案部署到阿里云上；如此法不适用于我方，若有此类需求，实际部署中建议采用LVS方案，推荐ipvsadm辅以heartbeat做高可用，并采用DR模式做双向分流。 |
| mysql主从复制 |  |
| 数据库水平分片，未作垂直拆分 |  |
|  |  |
| 安全性 | 服务采用对称加密算法 | 建议采用非对称加密（数字签名）的方式，减小密钥管理的成本。 |
| 服务的客户端认证基于权限系统实现 | 建议在服务总线中划分领域，对于部分对外集成性质的服务接口采用数字签名的方式（推荐X.509证书），在提供消息非对称加密的同时亦能支持客户端认证（重要）和服务端认证。（外系统或异构系统大多不便使用权限系统，且往往对RPC有性能要求） |
|  |  |
|  |  |
|  |  |
| 可修改性 | memcache缓存方案 | 期望memcache缓存可以支持停机恢复，并使该特性在对象级可配置 |
| 消息队列方案 | 消息队列的可配置性 |
| 目前数据库方案为mysql | 期望相关中间件优化对主流关系型数据库（目前oracle、mssql）的支持方案 |
| Javascript脚本框架 | 期望按业务领域归档脚本，建议统一采用基于闭包和IIFE的模块模式等设计模式对作用域加以封装并实现框架搭建。 |
| Bootstrap前端框架 | 建议使用原生Bootstrap3，自行修改和扩展的部分望予以标注。 |
|  |  |
|  |  |
| 可变性 | 目前项目应对的是单企业的权限管理需求 | 期望承包商能够提供迁移到“企业角色（多企业）+运维角色”的云服务模式的可行性（仅就权限系统而言：可能涉及但不限于以下角度：  1）运维管理（模块管理、角色管理、权限管理、附加属性管理、企业签约管理……）  2）企业用户中心（升级、购买、支付）  3）企业管理（企业角色、部门角色、企业管理员、合约管理……）  4）数据库分片策略 |
|  |  |
|  |  |
|  |  |
| 功能性 | 基于角色的权限树生成策略 |  |
| 附加属性模块 |  |
| 按钮权限 |  |
| 菜单权限 |  |
| 数据权限 | 请承包商提供数据权限的实现方式 |
|  |  |
|  |  |
| 互操作性 | 目前编程语言采用java | 期望预留与其他编程语言（.NET平台C#）交互的通用接口并测试其互操作性，如：加密解密，SOAP消息解析等 |
|  |  |
|  |  |
|  |  |

### 第二部分：架构验算

#### 1）场景要求

关键场景：

|  |  |
| --- | --- |
| 场景一 | 若站点1断电，要求3秒内将用户请求重定向到其他站点。 |
| 场景二 | 开票业务在99.9%的时间内是安全的。 |
| 场景三 | 以小于2人周的工作量更改Web用户管理界面。 |
| 场景四 | 在集成方案确认的前提下，以小于1人周的工作量完成与第三方系统的集成。 |
| 场景五 | 大批量集中开票情形下，构建异步的、均匀的请求散列。 |
| 场景六 | 若反向代理主服务器断电，8秒内须将用户请求重定向到备用的反向代理服务器。 |
| 场景七 | 采用三次握手方式实现客户端认证；客户端认证未通过的请求，服务总线直接返回未授权，无需访问数据库。 |
| 场景八 | LAN内的传输协议支持TCP/UDP,WAN传输协议采用HTTP。 |
| 场景九 | 免密钥管理。 |
| 场景十 | 开发人员可以自行配置需要由消息队列管理的对象。 |
| 场景十一 | 缓存服务器重启过程中，系统操作员的操作不受影响；重启后，亦无需重新登录。 |
| 场景十二 | 静态资源统一存储到NFS共享文件服务器上。 |
| 场景十三 | 访问量较大的动态页面需要静态化。 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

评估小组内的需求分析人员请在表格中补充业务场景。

#### 2）场景分级

|  |  |  |
| --- | --- | --- |
| 场景一 | 若站点1断电，要求3秒内将用户请求重定向到其他站点。 | ★★★★☆ |
| 场景二 | 开票业务在99.9%的时间内是安全的。 | ★★★★★ |
| 场景三 | 以小于2人周的工作量更改Web用户管理界面。 | ★★★☆☆ |
| 场景四 | 在集成方案确认的前提下，以小于1人周的工作量完成与第三方系统的集成。 | ★★★☆☆ |
| 场景五 | 大批量集中开票情形下，构建异步的、均匀的请求散列。 | ★★★☆☆ |
| 场景六 | 若反向代理主服务器断电，8秒内须将用户请求重定向到备用的反向代理服务器。 | ★★★★☆ |
| 场景七 | 采用三次握手方式实现客户端认证；客户端认证未通过的请求，服务总线直接返回未授权，无需访问数据库。 | ★★☆☆☆ |
| 场景八 | LAN内的传输协议支持TCP/UDP,WAN传输协议采用HTTP。 | ★★☆☆☆ |
| 场景九 | 免密钥管理。 | ★★☆☆☆ |
| 场景十 | 开发人员可以自行配置需要由消息队列管理的对象。 | ★★★☆☆ |
| 场景十一 | 缓存服务器重启过程中，系统操作员的操作不受影响；重启后，亦无需重新登录。 | ★★★☆☆ |
| 场景十二 | 静态资源统一存储到NFS共享文件服务器上。 | ★☆☆☆☆ |
| 场景十三 | 访问量较大的动态页面需要静态化。 | ★☆☆☆☆ |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

评估小组内的需求分析人员请在表格中补充业务场景分级信息。

#### 3）场景-架构交叉验算

|  |  |  |  |
| --- | --- | --- | --- |
| 质量属性 | 架构方法/现状 | 验算场景 | 评估 |
| 性能 | memcache 缓存服务 |  |  |
| Redis key-value数据库与消息队列 | 场景五 | 未实现 |
| Nginx动静分离 | 场景十二 | 支持 |
| 场景十三 | 支持 |
| 服务采用Restful风格（传递JSON） | 场景八 | 未实现 |
|  |  |  |
|  |  |  |
| 可用性（含可靠性） | Nginx应用层负载均衡 | 场景一 | 支持 |
| 场景六 | 未实现 |
| mysql主从复制 |  |  |
| 数据库水平分片，未作垂直拆分 |  |  |
| memcache 缓存服务可用性 | 场景十一 | 未实现 |
| 安全性 | 服务采用对称加密算法 | 场景二 | 支持 |
| 场景七 | 未实现 |
| 场景九 | 未实现 |
|  |  |
| 服务的客户端认证基于权限系统实现 | 场景二 | 支持 |
| 场景七 | 未实现 |
|  |  |  |
|  |  |  |
|  |  |  |
| 可修改性 | memcache缓存方案 |  |  |
| 消息队列方案 | 场景十 | 未实现 |
| 目前数据库方案为mysql |  |  |
| Javascript脚本框架 | 场景三 | 待验证 |
| Bootstrap前端框架 | 场景三 | 待验证 |
| 中间件可扩展性 | 场景四 | 待验证 |
| 服务总线 | 场景四 | 未实现 |
| 可变性 | 目前项目应对的是单企业的权限管理需求 |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| 功能性 | 基于角色的权限树生成策略 |  |  |
| 附加属性模块 |  |  |
| 按钮权限 |  |  |
| 菜单权限 |  |  |
| 数据权限 |  |  |
|  |  |  |
|  |  |  |
| 互操作性 | 平台采用J2EE中间件 | 场景四 | 待验证 |
| 服务总线 | 场景四 | 未实现 |
|  |  |  |
|  |  |  |

评估小组内的需求分析人员请在表格中补充场景验算与评估结果。