

北京师范大学组织工作管理与服务一体化平台

系统概要设计文档



2015-11-2

北京骥贤科技有限公司

2015-11-2

目录

[1 项目背景 2](#_Toc434484137)

[2 项目目标及意义 2](#_Toc434484138)

[3 系统总体设计 2](#_Toc434484139)

[3.1 基于SOA的系统架构 2](#_Toc434484140)

[3.2 系统设计原则 4](#_Toc434484141)

[3.3 系统的技术选型 5](#_Toc434484142)

[3.4 系统接口设计 7](#_Toc434484143)

[4 系统结构描述 7](#_Toc434484144)

[4.1 系统总体结构图 7](#_Toc434484145)

[4.2 网络拓扑图 8](#_Toc434484146)

[5 系统安全设计 9](#_Toc434484147)

[5.1 系统防火墙 9](#_Toc434484148)

[5.2 XSS攻击和SQL注入 10](#_Toc434484149)

[5.3 接口签名技术 10](#_Toc434484150)

[5.4 权限控制 11](#_Toc434484151)

[6 系统功能 12](#_Toc434484152)

[6.1 需求概述 12](#_Toc434484153)

[6.2 用户及权限管理 12](#_Toc434484154)

[6.3 党员业务办理 12](#_Toc434484155)

[6.4 各级管理员权限 12](#_Toc434484156)

[6.5 管理员（组织部）权限 13](#_Toc434484157)

[6.6 老数据迁移 13](#_Toc434484158)

# 项目背景

新组工系统将倚重组织部工作人员多年系统操作经验和日常工作累计，以提高用户体验为目标，优化现有的流程，提供更加完善和可靠的服务。新系统将集成北师大门户系统的用户体系，将线下党员的日常工作和审批流程移植到线上，在方便党员用户日常工作的前提下，提供多维度的报表统计。

# 项目目标及意义

本系统平台建设主要包括以下建设内容：

* 党组织信息管理；
* 党员信息管理
* 党建管理
* 干部信息管理
* 单位信息管理
* 发文管理
* 干部考核

# 系统总体设计

## 基于SOA的系统架构

面向服务架构（Service Oriented Architecture, SOA）具备松散耦合、可复用的特点，并可采取可定制的服务编排，因而很大程度上减少了系统之间的技术依赖性，增加了企业基础架构的灵活性和透明性。基于SOA体系架构能够实现客户端和服务器之间的松散耦合，主要优势有：

* 每种服务类型可以有多个相互独立的实例
* 在运行时能够根据服务类型、服务内容、服务质量来查找相应的服务实例
* 可以根据发现的元数据来调用相应的服务
* 允许组织、协调及序列化相关的服务

我们设计了一个4层架构的信息管理平台，包含客户端、Web Service层、服务层以及资源数据支持层。



针对系统的整个业务模式和IT环境，在充分考虑到系统扩展性的要求基础上，系统架构设计多层的体系结构模型。按服务功能粒度大小顺序将系统分解成若干层次，每一层次包含若干功能以及实现这些功能的软件和硬件。某个层次上的任意一个服务，只能使用更低层次的服务或本层次的其它服务，不能使用更高层次的服务。按照这种架构来组织整个系统，可以降低内各个系统间的依赖关系，使系统以更松散的方式耦合，从而更易于建设、维护和演进。

## 系统设计原则

* 实用性原则

充分考虑系统和基础环境，根据管理的模式和特点，胜任力测评系统基于开放的标准与规范，达到系统操作简单直观，配置方便，减少需要配置的选项以提供更好的支持和服务。

* 扩展性与先进性原则

考虑到系统能够随着未来信息技术的发展而不断平滑升级，系统基于Java EE 平台,采用Java语言进行开发，目的是为了系统具有良好的平台移植性，可以移植到AIX、HP－UNIX、Solaris、Windows、Linux等不同操作系统中。

* 安全性原则

系统的建设具备完善的安全体系结构。在系统设计中，充分考虑信息资源的灵活配置，同时注意信息资源的保护和隔离，保证用户的信息安全性以及数据和系统运行的安全性。在安全审计层面提供非法登录次数的校验、非法登录账户锁定、密码复杂度校验、用户IP地址的绑定、登录日志管理等；在数据安全保障层面提供机密数据的传输加密和存储加密。

对各种数据、报表的权限控制达到页面元素级，提供基于用户及用户组级别的访问权限分配。

* 稳定性与可靠性原则

从系统平台搭建，以及硬件实施部署方面着手，确保系统运行的可靠性和稳定性。采用中间件集群技术对系统进行多线程并发设置并采用数据缓存机制，提高系统高可用性；采用系统容灾恢复机制对提高系统稳定性。

* 可管理性和可维护性原则

伴随系统功能强大、使用者的增加，系统的可管理和可维护性就显得尤为重要，针对应用、服务体系、接口、权限、安全、数据审计进行管理，形成完善的管理体系。同时通过系统的监控模块，通过SNMP、syslog、trap等方式，能够对系统中各种对外服务进程、网络流量、硬件I/O读写速度、数据库实例等进行监控，及时发现系统故障和性能瓶颈，并将产生的告警信息及时发送给运维人员，以确保系统的稳定运行。

* 易用性原则

系统的易用性体现诸多方面，系统采用门户技术对外提供综合服务，管理员可以根据实际需求灵活自定义相关服务，并且提供功能导航、协作工具等帮助使用者快速定位服务和使用服务。

* 开放性与标准化原则

系统的建设采用具备开放架构、开放标准且符合业界主流技术标准的系统开放平台，便于自行进行二次开发；与系统相关的基础软件和工具软件均为国际主流软件，在系统技术层面采用相关标准技术XML、Webservice、Ladp、PortLet、ETL、Jquery等。

测评工具的信效度应该获得国内相关部门的鉴定或认可；测评系统必须可以移植，确保测评数据的独立性和安全性。

## 系统的技术选型

本系统采用浏览器+中间件+数据库 （Browser/Server三层结构） B/S结构，即Browser/Server(浏览器/服务器)结构，B/S 建立在浏览器上, 有更加丰富和生动的表现方式与用户交流。 并且大部分难度减低,减低开发成本。

系统软件平台遵守J2EE规范，采用Java编程语言和服务器端Java技术进行开发，包括Servlet、Portlet、JNDI、JDBC和RMI等技术。应用程序的开发和运行结构：应用系统平台的开发及运行结构基于后台数据库的三层架构，即Web服务器、应用服务器和数据库服务器。应用软件采用主流应用程序开发工具，并最有效地支持按J2EE规范的Java程序语言开发应用程序。系统将支持JAVA 6 等更高版本。支持Unix、Linux、Windows多种平台，完全支持跨平台的部署。



* JAVA

Java是一个纯的面向对象的程序设计语言，它继 承了 C++ 语言面向对象技术的核心，舍弃了C ++语言中容易引起错误的指针（以引用取代）、运算符重载（operator overloading）、多重继承（以接口取代）等特性，增加了垃圾回收器功能用于回收不再被引用的对象所占据的内存空间，使得程序员不用再为内存管理而担忧。Java 不同于一般的编译执行计算机语言和解释执行计算机语言。它首先将源代码编译成二进制字节码(bytecode)，然后依赖各种不同平台上的虚拟机来解释执行字节码，从而实现了“一次编译、到处执行”的跨平台特性。Sun 公司对 Java 编程语言的解释是：Java 编程语言是个简单、面向对象、分布式、解释性、健壮、安全与系统无关、可移植、高性能、多线程和动态的语言。

* MySQL

MySQL是一种开放源代码的RDBMS (Relational Database Management System，关系数据库管理系统)，MySQL数据库系统使用最常用的数据库管理语言--结构化查询语言（SQL）进行数据库管理。在 WEB 应用方面 MySQL是最好的 应用软件之一。MySQL 是一种关联数据库管理系统，关联数据库将数据保存在不同的表中，而不是将所有数据放在一个大仓库内，这样就增加了速度并提高了灵活性。MySQL 所使用的 SQL 语言是用于访问数据库的最常用标准化语言。

## 系统接口设计

本系统采用REST技术进行接口开发。REST即表述性状态传递（英文：Representational State Transfer，简称REST），REST是Web开发中的一种主流接口风格，

REST定义了应该如何正确地使用Web标准，例如HTTP和URI 。REST的优点：

* 可以利用缓存Cache来提高响应速度
* 通讯本身的无状态性可以让不同的服务器的处理一系列请求中的不同请求，提高服务器的扩展性
* 浏览器即可作为客户端，简化软件需求
* 相对与其他叠加在HTTP协议之上的机制，REST的软件依赖性更小
* 不需要额外的资源发现机制
* 在软件技术演进中的长期的兼容性更好

# 系统结构描述

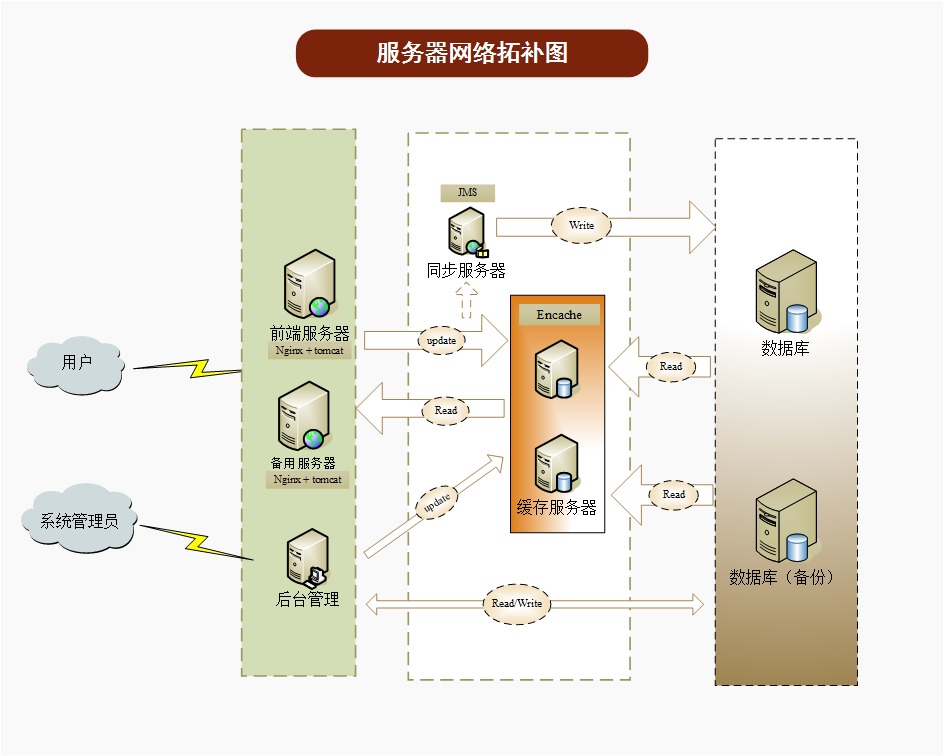
## 系统总体结构图

系统采用MVC三层架构模式，使用SpringMVC+Mybatis，数据库采用MySql+Redis内存数据库和缓存相结合，视图层采用JSP+Freemaker。外部接口主要有人事系统基本信息接口、学生管理系统基本信息接口等。



## 网络拓扑图

在服务器配置方面，系统采用应用服务器与数据库分离的手段，为数据安全性和可靠性打下基础。采用数据库缓存和异步更新机制，保证数据库服务的可用性和稳定性。服务器网络拓扑图如下：



# 系统安全设计

## 系统防火墙

防火墙的安全策略有两种：允许和禁止。

* 允许访问

　　允许访问是指在防火墙的安全策略中没有被列为允许访问的服务都是被禁止的。这意味着需要确定所有可以被提供的服务以及他们的安全特性，开放这些服务，并将所有其他未列入的服务排斥在外，禁止访问。

* 禁止访问

　　禁止访问是指在防火墙的安全策略中没有被列为禁止访问的服务都是被允许的。这意味着首先确定那些被禁止的、不安全的服务，以禁止他们被访问，而其他服务则被认为是安全的，允许访问。

## XSS攻击和SQL注入

XSS又称CSS，全称Cross SiteScript，跨站脚本攻击，是Web程序中常见的漏洞，XSS属于被动式且用于客户端的攻击方式，所以容易被忽略其危害性。其原理是攻击者向有XSS漏洞的网站中输入(传入)恶意的HTML代码，当其它用户浏览该网站时，这段HTML代码会自动执行，从而达到攻击的目的。如，盗取用户Cookie、破坏页面结构、重定向到其它网站等。本系统针对XSS攻击采取的措施有：

* HttpOnly防止劫取Cookie

HttpOnly最早由微软提出，至今已经成为一个标准。浏览器将禁止页面的Javascript访问带有HttpOnly属性的Cookie。目前主流浏览器都支持，HttpOnly解决是XSS后的Cookie支持攻击。

* 输入检查

输入检查一般是检查用户输入的数据中是否包含一些特殊字符，如<、>、'、"等，如果发现存在特殊字符，则将这些字符过滤或者编码。

* 输出检测

使用各种过滤和编码手段，对html、script、css和url中的输出变量就行处理。

所谓SQL注入，就是通过把SQL命令插入到Web表单提交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令。本系统采用高规格的编码方案，从根本上杜绝了SQL注入。

## 接口签名技术

接口开发是各系统之间对接的重要方式，其数据是通过开放的互联网传输，对数据的安全性要有一定要求。为了提高传输过程参数的防篡改性，签名sign的方式是目前比较常用的方式。签名大致步骤如下：

第1步: 将所有参数（注意是所有参数），除去sign本身，以及值是空的参数，按参数名字母升序排序。

第2步: 然后把排序后的参数按参数1值1参数2值2…参数n值n（这里的参数和值必须是传输参数的原始值，不能是经过处理的，如不能将&quot;转成”后再拼接）的方式拼接成一个字符串。

第3步: 把分配给接入方的验证密钥key拼接在第2步得到的字符串前面。

第2步: 在上一步得到的字符串前面加上验证密钥key(这里的密钥key是接口提供方分配给接口接入方的)，然后计算md5值，得到32位字符串，然后转成大写.

第4步: 计算第3步字符串的md5值(32位)，然后转成大写,得到的字符串作为sign的值。

根据前面描述的签名参数sign生成的方法规则，计算得到参数的签名值，和参数中通知过来的sign对应的参数值进行对比，如果是一致的，那么就校验通过，如果不一致，说明参数被修改过。

## 权限控制

本系统采用Apache Shiro进行身份验证和授权。shiro是apache提供的强大而灵活的开源安全框架，它主要用来处理身份认证，授权，企业会话管理和加密。

Shiro主要功能有，用户验证、用户执行访问权限控制、在任何环境下使用session API，如cs程序。可以使用多数据源如同时使用oracle、mysql。单点登录(sso)支持。remember me服务。

Apache Shiro具有以下特点：

* **易于使用** - 易用性是这个项目的最终目标。提供易于理解的 Java Security API。
* **广泛性** - 没有其他安全框架可以达到Apache Shiro宣称的广度，它可以为你的安全需求提供“一站式”服务。
* **灵活性** - Apache Shiro可以工作在任何应用环境中。虽然它工作在Web、EJB和IoC环境中，但它并不依赖这些环境。Shiro既不强加任何规范，也无需过多依赖。
* **Web能力** - Apache Shiro对Web应用的支持很神奇，允许你基于应用URL和Web协议（如REST）创建灵活的安全策略，同时还提供了一套控制页面输出的JSP标签库。
* **可插拔** - Shiro干净的API和设计模式使它可以方便地与许多的其他框架和应用进行集成。你将看到Shiro可以与诸如Spring、Grails、Wicket、Tapestry、Mule、Apache Camel、Vaadin这类第三方框架无缝集成。
* **支持** -Apache Shiro是[Apache软件基金会](http://www.apache.org/)成员，这是一个公认为了社区利益最大化而行动的组织。项目开发和用户组都有随时愿意提供帮助的友善成员。像[Katasoft](http://www.katasoft.com/)这类商业公司，还可以给你提供需要的专业支持和服务。

# 系统功能

# 需求概述

新的组工系统，为党员和党组织管理员提供相应的信息查询以及资料变更服务，在线受理党员的出党，转入/转出请求，实现党员用户在学校期间的全部党员日常操作的闭环操作；借助平台，提供组织部日常工作的多维度报表统计。系统分为23个核心功能点。

# 用户及权限管理

* 用户单点登录
* 用户的权限管理及配置，主要角色如下：管理员，党总支/委员会/党支部的三级管理员，党员，积极分子
* 用户的数据权限及菜单权限的配置
* 组织机构树的维护

# 党员业务办理

* 积极分子申请入党
* 党员转入申请
* 党员转出申请
* 党员校内组织关系转接
* 党费缴纳

# 各级管理员权限

* 党员信息查询
* 转入申请审批
* 转出申请审批
* 校内组织关系转接审批
* 党员出党操作
* 党支部信息的管理（添加/修改/删除）
* 党员批量迁移
* 统计报表

# 管理员（组织部）权限

* 年度报表统计及视图
* 党员信息导出
* 党员年龄分布图
* 党员转入/转出表单打印
* 转入/转出申请统计图
* 发布系统通知

# 老数据迁移

* 党员信息
* 党员转入转出申请
* 组织机构迁移
* 用户权限迁移