 DOI: https://doi.org/10.12345/gcjsygl.v5i23.9677

Discussion on the Application Management of Single Sign-on Technology in Enterprise System Engineering

Yongsheng Sun

Sinosoft Co., Ltd., Beijing, 100089, China

Abstract

Due to the rapid development of the national economy, the scale of the enterprise has gradually expanded, enterprises in order to respond to the call of the state, speed up the information construction, the construction of various information systems. This paper proves through practice that the introduction of single sign-on technology can solve the problem of inconsistent enterprise customer information management and multiple login of each system, and has good social and economic value.

Keywords

single sign-on unified; identity authentication enterprise; information technology

浅谈单点登录技术在企业系统工程中的应用管理

孙永升

中科软科技股份有限公司，中国·北京 100089

摘　要

由于国民经济的高速发展，企业规模逐渐壮大，企业为了响应国家号召，加快信息化建设，投建各种信息系统。论文通过实践证明，引入单点登录技术能够解决企业客户信息管理不统一、各个系统分别多次登录的问题，具有良好的社会和经济价值。

关键词

单点登录；统一身份认证；企业信息化

1 引言

单点登录技术是一个用户认证的过程，允许用户一次性进行认证之后，访问系统中不同的应用；而不需要访问每个应用时都重新输入密码。利用单点登录，可以将企业的各种信息系统，实现无缝切换登陆。

2 需求分析

根据单点登录技术的特点，分为服务端和客户端。服务端需单独部署为单点登录系统，客户端集成到企业的各个信息系统。这就要求这些系统需要采用集群、分布式的方式部署到多台物理机、云服务器上面，以满足企业的需求；物理机选用华为系统服务器，云端服务器采用的阿里云服务器；不同类型企业有不同类型信息系统。

单点登录主要功能：能够缓存登录者的信息，实现各个系统之间的自如跳转，在各个功能之间共享基础数据和登录数据。

【作者简介】孙永升（1985–），男，中国河南周口人，本科，工程师，从事软件工程研究。

3 概要设计

3.1 网络结构设计

某企业采用 B/S 架构模式进行系统部署，用户可以通过客户端访问单点登录，可以自由切换到账户管理系统、资金管理系统、融资管理系统、用户管理系统。这些系统通过对数据库的访问实现对流程数据、业务数据和基础数据的存储。远程客户通过 VPN 方式访问该企业的信息系统，局域网用户则通过 LAN 方式访问系统。

单点登录系统 CAS 设计，采用的是 Cookie 机制，优点很多。例如，设计理念先进、体系结构合理、配置简单、客户端支持广泛、技术成熟等。

CAS 的实现原理：单点登录分为“服务端”和“客户端”。某个应用程序第一要发起第 1 次认证，用户在单点登录服务器的登录页面中，输入用户名和密码。第二单点登录服务器会对用户名和密码进行认证，如 LDAP 或者数据库等。认证通过之后，单点登录服务器会和应用程序进行某种授权，授权完成后，CAS 把页面重定向，回到 Web 应用。单点登录服务器会在客户端创建一个 Cookie 保存用户登录的信息，如果用户此时希望进入其他 Web 应用程序，自动寻

找 Cookie，根据 Cookie 中保存的信息，进行登录，登录之后，CAS 重定向回到用户的应用程序 [1]。

3.2 部署架构设计

系统部署的各个服务器使用物理机和云服务器两种，物理机硬件设备采用华为 FusionServer 2488H V5 机架服务器，安装虚拟机，虚拟机使用红帽 Linux 操作系统，根据不同的信息系统，分配不同的内存和磁盘空间。例如，账户管理系统需要磁盘空间 200G、运行内存 40G；云服务器使用的阿里云服务器，同样使用红帽 Linux 操作系统，根据不同的信息系统，分配不同的内存和磁盘空间。例如，资金管理系统需要磁盘空间 150G、运行内存 30G。

4 实现与部署

4.1 单点登录系统详细设计实现

以某企业的账户管理系统客户端为例，描述主要单点登录过程的详细设计与实现，单点登录过程，需要众多类的支持才能完成登录认证操作，下面针对客户端、服务端对 CAS 底层 JAR 包重点类的调用配置进行说明。

客户端：在 web.xml 中加载单点登录 SSO 的 CAS 配置文件 security-cas.xml，该文件主要用于配置单点登录地址、登录成功后返回的地址。

服务端：在 web.xml 中加载单点登录 SSO 的 CAS 配置文件 SafeDispatcherServlet、deployerConfigContext.xml、warnCookieGenerator.xml、ticketGrantingTicketCookieGenerator.xml。

deployerConfigContext.xml 主要用于配置去除 https 认证，增加参数 p:requireSecure=“false”，是否需要安全验证，即 https，false 为不采用。

ticketGrantingTicketCookieGenerator.xml 在该文件中配置参数 p:cookieSecure=“true”，改参数与 https 验证相关，当 cookieSecure 的值为 true 则采用 https 验证；当 cookieSecure 的值为 false 则禁用 https 验证。

warnCookieGenerator.xml 在该文件中配置参数 p:cookieSecure=“true”，改参数与 https 验证相关，当 cookieSecure 的值为 true 则采用 https 验证；当 cookieSecure 的值为 false 则禁用 https 验证。

输入任意系统登录地址，跳转到单点登录 login 登录页面，输入用户名和密码点击登录调用 Authen ticationViaFormAction 的 submit 进行登录，AuthenticationViaFormAction 调用 CASjar 包的底层类 [2]。

用户访问账户管理系统的受保护资源，账户管理系统发现用户未登录，跳转至单点登录模块系统，并将自己的地址作为参数。单点登录系统发现用户未登录，将用户引导至登录页面，用户输入用户名密码提交登录申请。单点登录系统校验用户信息，创建用户与单点登录系统之间的会话，称为全局会话，同时创建授权令牌。

单点登录系统带着令牌跳转至最初的请求地址（账户管理系统）。账户管理系统拿到令牌，去单点登录系统校验令牌是否有效，单点登录系统校验令牌，返回有效，注册账户管理系统。账户管理系统使用该令牌创建与用户的会话，称为局部会话，返回受保护资源，用户访问资金管理系统的受保护资源。

资金管理系统发现用户未登录，跳转至单点登录系统，并将自己的地址作为参数。

单点登录系统发现用户已登录，跳转回资金管理系统地址，并附上令牌。

资金管理系统拿到令牌，去单点登录系统校验令牌是否有效，单点登录模块系统校验令牌，返回有效，注册资金管理系统。

资金管理系统使用该令牌创建与用户的局部会话，返回受保护资源用户登录成功之后，会与单点登录系统及各信息系统建立会话，用户与单点登录系统建立的会话称为全局会话，用户与各信息系统建立的会话称为局部会话，局部会话建立之后，用户访问个信息系统受保护资源将不再通过单点登录系统，全局会话与局部会话有如下约束关系局部会话存在，全局会话一定存在；全局会话存在，局部会话不一定存在；全局会话销毁，局部会话必须销毁。

4.2 实施系统部署

某企业的不同系统可以部署到物理机或云服务器不同类型的服务器上，下面以部署到物理上的虚拟机器上的服务为例来进行说明。

首先物理机器上安装虚拟机，并安装红帽 Linux 操作系统，部署选择 200G 的硬盘空间，详细可划分为根目录、home、boot、root 等分区，分配 40G 运行内存，并配置网络；虚机和网络准备完毕后；下一步安装中间件 tomcat，其次通过选择合适方式将信息系统的应用部署到中间件 tomcat；最后启动 tomcat。以同样的方式其他信息系统 [3]。待所有的信息部署启动完成以后，可以选择任意系统登录，然后无缝切换到其他信息系统。

5 结语

第一，论文论述了企业信息系统运营面临的现状；第二，提出了单点登录技术在企业引入的必要性；第三，结合单点登录技术的特点和某企业各个信息系统的情况进行详细的需求分析；第四，从网络结构、部署架构两个方面进行概要设计；第五，从单点登录服务系统代码实现层面和实施部署两个层面进行实现。

参考文献

[1] 陈圣楠.基于CAS-LDAP的统一身份认证管理系统[J].信息与电脑,2019(12):3.

[2] 王群,李馥娟.一种基于单点登录的实验室统一身份认证方案[J].实验技术与管理,2020,37(5):5.

[3] 倪叶青.高可用LDAP校园网统一身份认证设计与实现[J].价值工程,2019,38(35):3.