Computer Science and Application 计算机科学与应用, 2019, 9(7), 1434-1440
Published Online July 2019 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2019.97161

Hans汉斯

Design and Analysis of Single Sign on System Based on CAS Mode

Xiaowei Xu, Jinlei Wang, Wenfei Jiang, Fengjuan Cui

North China Sea Data and Information Service, SOA, Qingdao Shandong
Email: xuxiaowei@ncs.mnr.gov.cn, 407177515@qq.com

Received: Jul. 9th, 2019; accepted: Jul. 22nd, 2019; published: Jul. 29th, 2019

Abstract

In order to solve the problem of the integration of the existing business application system of NCS, this paper makes a deep research on the principle of CAS integrated authentication, and designs a single sign on system based on CAS mode. Based on the actual situation of various software systems of NCS, this paper analyzes the problems faced by various systems to achieve single sign-on, proposes different solutions to these problems, and provides technical route for the integration of business application systems of NCS, so as to realize the construction of single sign-on system of NCS.

Keywords

CAS Authentication, SSO, System Integration

基于CAS模式的单点登录系统设计与分析

徐晓玮，王金磊，姜雯斐，崔凤娟

国家海洋局北海信息中心，山东 青岛
Email: xuxiaowei@ncs.mnr.gov.cn, 407177515@qq.com

收稿日期：2019年7月9日；录用日期：2019年7月22日；发布日期：2019年7月29日

摘　要

针对自然资源部北海局现有业务应用系统整合问题，对CAS集成认证原理进行深入研究，设计搭建了基于CAS模式的单点登录系统。结合北海局各类软件系统的实际情况，分析各类系统实现单点登录所面临的问题，针对这些问题提出不同的解决方案，为北海局业务应用系统的整合集成提供技术路线，以实现北海局单点登录系统的建设。

文章引用: 徐晓玮, 王金磊, 姜雯斐, 崔凤娟. 基于 CAS 模式的单点登录系统设计与分析[J]. 计算机科学与应用, 2019, 9(7): 1434-1440. DOI: 10.12677/csa.2019.97161

关键词

CAS认证，单点登录，系统集成

1. 引言

随着海洋信息化的不断发展，自然资源部北海局内部逐步建立了为海洋管理业务服务的各类信息系统。这些系统建设技术选型各异，每个系统都有独立的认证体系和用户管理模块。用户在使用各个系统时，需要清楚记住每个系统的账户信息并逐一登录认证，这样不仅增大了用户管理的难度，而且不利于系统的安全管理。

基于 CAS 模式的单点登录系统，在实现一点登录、多点应用的同时，提供统一简便的用户管理，只有通过安全认证且获得使用权限的用户才能访问信息系统，不仅方便用户登录及管理，而且有效提高系统安全性能，保证系统资源的高效实用。

2. 系统设计方案

目前自然资源部北海局信息化软件系统主要包括 3 大类系统：基于 Java 平台的 B/S 结构应用系统、基于.NET 平台的 B/S 结构应用系统和基于.NET 平台的 C/S 结构应用系统。第一类系统在设计开发时就已充分考虑单点登录的问题，通过在系统配置文件中增加过滤器及监听器等代码，实现 CAS 单点登录；第二类系统在集成 CAS 单点登录时是结合表单认证方式完成的，这种方式在用户访问系统资源时会出现循环重定向问题，需要通过配置系统会话状态实现会话数据的保存，避免因用户票据数据丢失造成单点登录失败；第三类系统受系统开发框架限制，无法通过 Cookie 存储用户验证信息，针对这种情况考虑采取集成基于 REST (Representational State Transfer，表现层状态转化)架构的 RESTful API 接口，实现客户端与服务器端的用户信息交互，以此完成系统登录工作[1]。整个系统结构如图 1 所示。

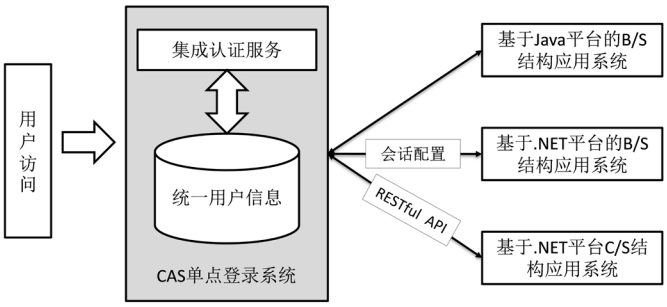

Figure 1. System structure diagram
图 1. 系统结构图

3. CAS 单点登录

3.1. CAS 认证原理

CAS (Central Authentication Service，中央认证服务)是 Yale 大学发起的一个旨在提供企业级单点登录

解决方案的开源项目，CAS 协议经过 3 个版本的不断提升，成为目前比较流行的针对 Web 应用的开源单点登录框架，它具有易用、跨平台、可扩展等特点。CAS 框架包括 CAS 客户端和 CAS 服务端两部分，CAS 服务端是需要对应部署的 Web 应用，负责对用户进行认证并颁发证书；CAS 客户端需要部署在 Web 应用中，可支持 Java、Php、.Net 等多种语言编写的 Web 应用，负责处理对 Web 应用中受保护资源的访问请求。

CAS 协议是基于票据(Ticket)的方式实现安全认证的，Ticket 是 CAS 客户与 CAS 服务端通信的重要凭证，CAS 服务端通过验证 Ticket 信息来判断用户是首次请求认证还是已通过认证，认证原理如图 2 所示[2]。用户通过浏览器访问应用系统时，部署在应用系统中的 CAS 客户端接收到访问请求后，会分析请求中是否含有 ST (Server Ticket，服务票据)，如果有说明用户已登录，将跳到图 2 的 Step4；如果没有，浏览器将重定向到 CAS 服务端。CAS 服务端的 TGS (Ticket Granting Service，票据授权服务)将对用户 Cookie 中的 TGT (Ticket Granting Ticket，票据授权票据)进行验证，验证通过则返回 ST 到 CAS 客户端，跳到图 2 的 Step4；验证不通过，则向浏览器返回登录页面。用户在登录页面中输入用户名和密码，提交到 CAS 服务端由 AS (Authentication Service，认证服务)进行验证，验证成功后 CAS 服务端会在用户浏览器设置一个 TGC (Ticket Granting Cookie，票据验证凭证)，用于存放包含用户身份信息的 TGT，以便后期验证用户是否已登录，同时生成唯一的 ST 返回给用户。用户携带 ST 通过 CAS 客户端重定向到 CAS 服务端，对 ST 的合法性进行核实，验证成功后返回用户名，验证失败则返回错误信息[3] [4] [5]。

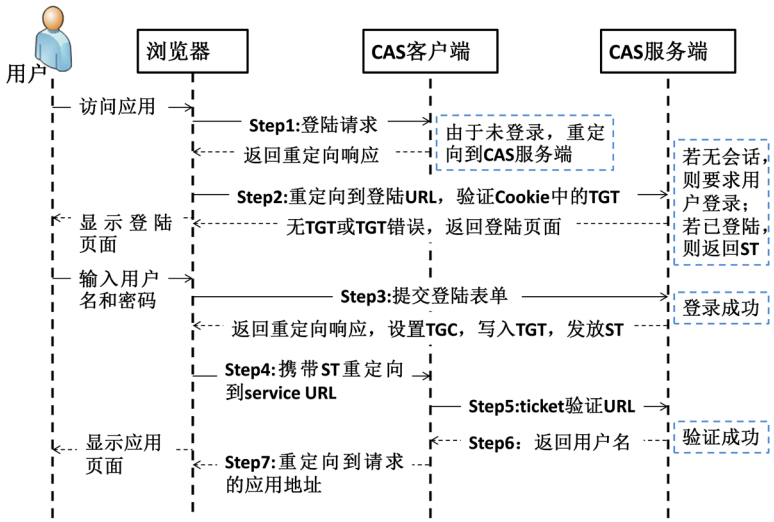

Figure 2. CAS certification schematic diagram
图 2. CAS 认证原理图

3.2. 单点登录平台搭建

单点登录(Single Sign-On，简称 SSO)，通过统一认证平台同时为多个应用系统提供登录认证服务，能够实现在多个应用系统中，用户只需要登录认证一次就直接访问已授权的系统，而不需要在访问每个系统时进行身份认证。基于 CAS 模式实现的单点登录平台认证流程如图 3 所示[6]。

CAS 单点登录认证平台包括服务端和客户端，CAS 服务端是基于 Https 协议与 CAS 客户端进行交互完成对用户的安全认证，搭建一套完整的认证体系主要包括三个步骤：安全设置、服务器定制和客户端配置[7]。

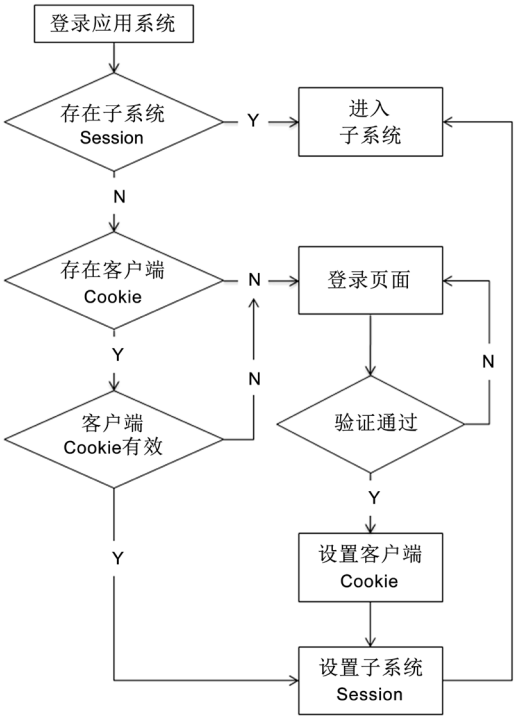

Figure 3. Single sign-on authentication flow chart
图 3. 单点登录认证流程图

安全配置：首先需要修改 CAS 服务端所在中心认证服务器的 Tomcat 环境配置，在 conf/server.xml 文件中启用 SSL (Secure Sockets Layer，安全套接层)功能，然后利用 JDK (Java Development Kit，Java 开发工具包)自带的 keytool 工具生成证书，将证书以文件的方式导入到 CAS 服务端和 CAS 客户端，使双方具有 Https 通信能力。这个证书是 CAS 客户端与 CAS 服务端安全交互的重要保证，通信双方以此证明自己的合法性。

服务器定制：将 CAS-Server 源代码安装部署到中心认证服务器的 Tomcat 中即可完成 CAS 服务端的初步配置。在实际应用中，需要 CAS 服务端能够读取指定数据库中的用户信息进行安全验证，可以通过修改 CAS-Server 目录下的 WEB-INF/deployerConfigContext.xml 文件，配置认证数据源和验证选项来实现。CAS 认证数据源支持单数据库、多数据库及域账户等多种方式，用户可以根据系统实际应用需求进行自定义配置。

客户端配置：下载 CAS-Client 源代码，根据项目实际应用需要将相应的 jar 包导入应用系统的 WEB-INF/lib 下，同时在应用系统的 web.xml 文件中增加 CAS 认证过滤器，将用户访问请求定向到 CAS 认证平台中进行安全认证。

4. 应用系统集成

4.1. 基于 Java 平台的 B/S 系统集成

这类系统与 CAS 单点登录系统结构嵌合度较高，集成难度相对较低，按照 CAS 客户端配置方法对系统配置文件进行修改后即可完成系统单点登录的集成，登录流程如图 4 所示。用户首次访问系统，由于未通过认证，系统将跳转至配置文件中指定的 casServerLoginUrl 地址(即 CAS 服务端登录认证中心)，在 CAS 服务端认证完成后，CAS 服务器将在系统访问地址(需要配置文件中指定 serverName)后添加 ticket 并返回 CAS 客户端，CAS 客户端接收后会再次向 CAS 服务端发起 ticket 验证，CAS 服务端验证通过返回成功信息后，CAS 客户端将打开受保护页面，登录完成。

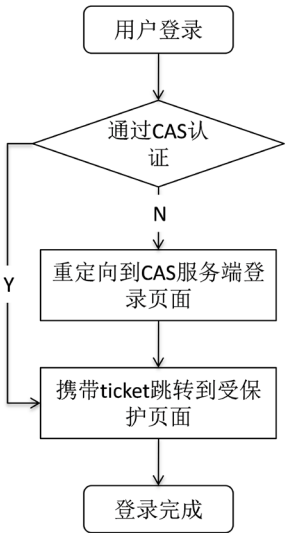

Figure 4. System login flowchart based on Java platform
图 4. 基于 Java 平台的系统登录流程图

4.2. 基于.NET 平台的 B/S 系统集成

此类系统在集成到 CAS 单点登录系统中时，会因用户票据失效而发生循环重定向问题，导致用户验证后依然无法正常访问系统资源，考虑通过会话配置保证用户票据的有效性，进而实现用户单点登录，登录流程如图 5 所示。用户登录系统时，首先重定向到 CAS 认证中心进行用户验证，验证通过后将用户重定向到系统页面，在此过程系统通过对用户 ST 进行验证来过滤每一次访问请求，进而实现对系统功能页面的控制。通过对系统 SessionState 的配置，启用系统会话状态，开始.NET 平台的状态服务，保证会话状态持久，从而在系统进行用户 ST 验证时提供有效的用户票据，实现用户的单点登录。

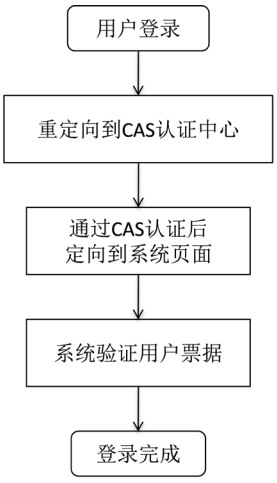

Figure 5. System login flow chart based on .NET platform
图 5. 基于.NET 平台的系统登录流程图

4.3. 基于.NET 平台的 C/S 系统集成

CAS 验证是基于浏览器 Cookie 存储验证信息进行用户认证，此类系统受设计框架限制，不具备 Cookie 容器，针对此类系统考虑利用 RESTful API 接口实现系统的 CAS 登录，登录流程如图 6 所示。用

户通过客户端登录时，首先提交用户名、密码和 Service 参数至 CAS 认证中心，验证成功后返回用户 TGT 至客户端，客户端根据 TGT 获取用户 ST 进行验证登录，此种方式与传统 CAS 认证方式的区别在于 TGT 存储方式的不同，客户端利用 RESTful API 接口解决了 C/S 系统因不具有 Cookie 容器无法存储用户验证信息的问题，实现了用户在客户端和浏览器之间的登录状态的传输。

Figure 6. System login flowchart based on RESTful
图 6. 基于 RESTful 的系统登录流程图

4.4. 基于 CAS 模式的北海局单点登录平台

利用 CAS 单点登录技术完成上述自然资源部北海局现有的 3 类信息系统的集成，形成基于 CAS 模式的北海局单点登录平台，实现北海局信息系统的一点登录，多点应用。登录平台如图 7 所示，账户信息验证如图 8 所示。

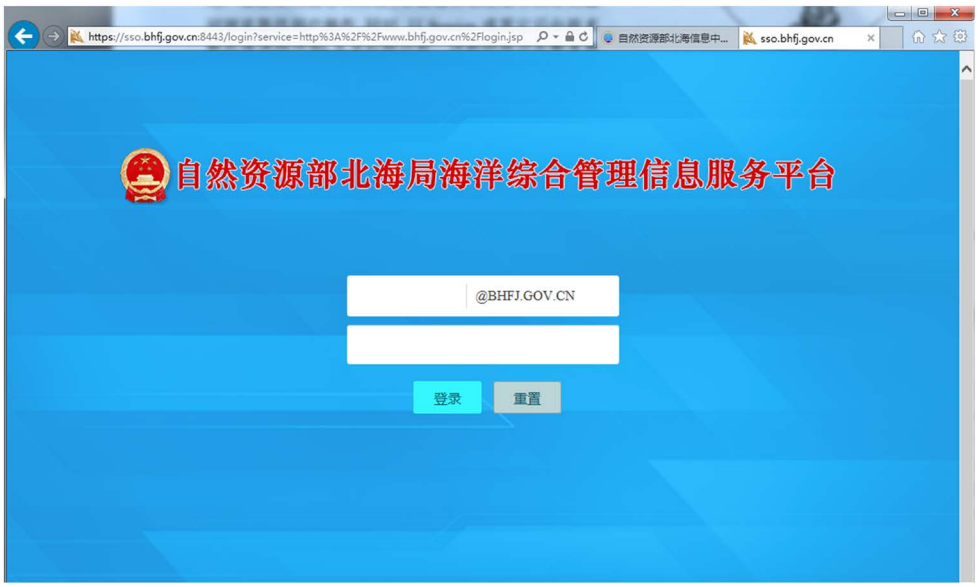

Figure 7. Schematic diagram of login platform
图 7. 登录平台示意图

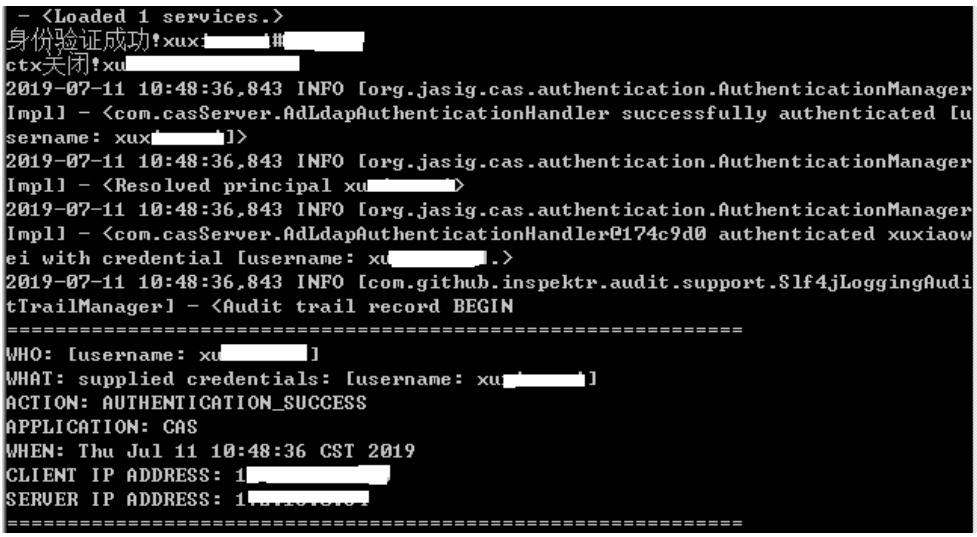

Figure 8. Schematic diagram of account information verification
图 8. 账户信息验证示意图

5. 总结

本文阐述了基于 CAS 模式的单点登录系统的设计与分析。在对 CAS 认证服务进行充分研究的基础上完成单点登录平台的搭建，结合自然资源部北海局业务应用系统现状，就现有异构业务应用系统如何实现单点登录的问题进行分析研究，归纳总结出系统配置、参数登录和 RESTful API 集成三种单点登录平台集成方式，以此逐步整合已有应用系统的用户认证登录，规范新开发应用系统，提高用户登录效率。此外，通过域账户与单点登录平台的集成，也可以实现多系统的集成登录，基于域账户的 CAS 认证方式将有助于进一步规范系统用户的管理，进一步提高系统集成度。

参考文献

[1] 赵艳芳. 基于 CAS 的统一认证平台的设计与实现[J]. 云南大学学报, 2013, 35(S2): 165-168.

[2] 鲁学, 汪丽华. 运用 CAS 模型实现数字校园统一认证[J]. 中国教育信息化, 2014(6): 58-59.

[3] 张齐, 钟观宝. 基于用户映射的 CAS 单点登录系统设计与实现[J]. 信息通信技术, 2009, 3(4): 6-11.

[4] 黄经赢. 基于 CAS 协议的单点登录系统在数字化校园中的应用与设计[D]: [硕士学位论文]. 广州: 华南理工大学.

[5] 张平, 郑津, 汪立欣. 一种基于 CAS 的校园网统一平台单点登录方法[J]. 电脑编程技巧与维护, 2013(16): 146-155.

[6] 秦怡, 马自卫. 基于 CAS 模式的统一认证与门户管理的研究与实现[J]. 数字图书馆, 2008, 24(12): 1-7.

[7] 裴华艳, 王焕民. 基于 CAS 的单点登录平台的研究与实现[J]. 电脑知识与技术, 2014(3): 534-536.

知网检索的两种方式：

1. 打开知网首页：http://cnki.net/，点击页面中“外文资源总库 CNKI SCHOLAR”，跳转至：http://scholar.cnki.net/new，搜索框内直接输入文章标题，即可查询；
   或点击“高级检索”，下拉列表框选择：[ISSN]，输入期刊 ISSN：2161-8801，即可查询。
2. 通过知网首页 http://cnki.net/顶部“旧版入口”进入知网旧版：http://www.cnki.net/old/，左侧选择“国际文献总库”进入，搜索框直接输入文章标题，即可查询。

投稿请点击：http://www.hanspub.org/Submission.aspx
期刊邮箱：csa@hanspub.org