Scientific Research Publishing

Journal of Information Security, 2023, 14, 16-24
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Research and Practice on High Availability Scheme of Unified Identity Authentication System Based on CAS in Colleges and Universities

Man Liu, Lei Yu*

Information Network Center, China University of Geosciences (Beijing), Beijing, China
Email: liuman@cugb.edu.cn, *yul@cugb.edu.cn

How to cite this paper: Liu, M. and Yu, L. (2023) Research and Practice on High Availability Scheme of Unified Identity Authentication System Based on CAS in Colleges and Universities. *Journal of Information Security*, **14**, 16-24.
https://doi.org/10.4236/jis.2023.141002

Received: October 24, 2022
Accepted: December 26, 2022
Published: December 29, 2022

Copyright © 2023 by author(s) and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/

Open Access

Abstract

Unified identity authentication has become the basic information service provided by colleges and universities for teachers and students. Security, stability, high concurrency and easy maintenance are our requirements for a unified identity authentication system. Based on the practical work experience of China University of Geosciences (Beijing), this paper proposes a high availability scheme of unified identity authentication system based on CAS, which is composed of multiple CAS Servers, Nginx for load balancing, and Redis as a cache database. The scheme has been practiced in China University of Geosciences (Beijing), and the application effect is good, which has practical reference significance for other universities.

Keywords

Unified Identity Authentication, CAS, Redis, High Availability, Colleges and Universities

1. Introduction

With the development of information technology in colleges and universities, many application systems have been built to provide relevant information services for teachers and students. At first, the same user needs to input different user name and password when accessing different system, which is extremely inconvenient to use and manage the application systems. Later, the unified identity authentication system came into being. The unified identity authentication system uniformly takes over the functions of the identity authentication modules

scattered in application systems, and the unique user information database located in the unified identity authentication system uniformly verifies the authenticity of the user identity. The security issues related to the storage and exchange of user identity information are all guaranteed by the security protocols and policies provided by the unified identity authentication center. All information systems are integrated with the unified identity authentication system for authentication. Teachers and students only need to remember the user name and password in the unified identity authentication system to log on to all information systems. Based on the unified identity authentication system, the SSO (Single Sign-on) is realized, which provides great convenience for teachers and students. Unified identity authentication has become one of the essential basic information services in the digital campus of colleges and universities [1].

Unified identity authentication mainly has three kinds of solutions: password-based, service-based and protocol-based. S/Key authentication is based on password. Microsoft Passport is a typical application of service-based unified identity authentication. The unified identity authentication based on the protocol is divided into many types according to different protocols, such as Kerberos protocol, shibboleth protocol, SAML protocol, liberty alliance protocol, OAuth protocol and CAS protocol, etc. [2] [3].

The SSO based on password is simple to implement, but its security is relatively low and it is vulnerable to malicious attacks resulting in the leakage of account information. Although the SSO based on service is easy to use, it is not strong in expansibility and is not convenient for personalized customization. Moreover, it is charged for use, which increases the cost. So now the more popular solution of SSO is based on protocol.

CAS is an enterprise SSO solution. It is open source, security, light weight, strong extensibility, and easy to deploy. Therefore, the unified identity authentication system based on CAS is used to achieve SSO in most universities in China.

The unified identity authentication system provides great convenience for teachers and students to access the information services in colleges and universities. However, due to the large number of users in colleges and universities and the concentration of some business, it is necessary to solve the problems of heavy load and high concurrency at the same time. The biggest bottleneck is the high concurrent access to the database. Most universities alleviate the pressure of database access by using LDAP (Lightweight Directory Access Protocol). LDAP service has poor writing performance but much higher reading performance than relational database, which is more suitable for business scenarios with a large number of data reading operations and less writing operations. Querying user information for identity authentication is precisely such business scenarios [4]. However, the operation and maintenance of LDAP is slightly complicated, because the source data that generate user information of teachers and students are stored in the relational database, which involves the synchronization between relational data and LDAP database. With more and more application sys-

tems integrated into unified identity authentication system, security, stability, efficient access and convenient operation and maintenance have become the challenges faced by unified identity authentication system.

2. CAS Overview

CAS is an enterprise multilingual single sign-on solution and identity provider for the web and attempts to be a comprehensive platform for our authentication and authorization needs.

2.1. Main Features

The following items include the important features presented by the CAS [5]:

1) Pluggable authentication support (LDAP, Database, X.509, SPNEGO, JAAS, JWT, RADIUS, MongoDb, etc.).

2) Support for multiple protocols (CAS, SAML v1, SAML v2, WS-Federation, OAuth2, OpenID, OpenID Connect, REST).

3) Support for delegated authentication to external identity providers such as ADFS, Facebook, Twitter, SAML2 IdPs, OIDC OPs, etc.

4) Cross-platform client support (Java, NET, PHP, Perl, Python, Ruby, Apache, etc.).

5) Manage and register client applications and services with specific authentication policies.

2.2. CAS Architecture and Authentication Process

The CAS server and CAS clients comprise the two physical components of the CAS system architecture that communicate by means of various protocols. The CAS architecture is shown in **Figure 1**.

CAS server needs to be deployed independently and is mainly responsible for user authentication. The CAS clients are responsible for processing the access request to the protected resources of the client. When it needs to log in, it will be redirected to the CAS server. The CAS authentication process is shown in **Figure 2**, which is mainly divided into the following 6 steps:

1) The browser sends a login request to the CAS client; 2) The CAS client redirects the request to the CAS server; 3) The CAS server authenticates the request; 4) After the authentication is passed, a ticket will be generated and returned to the CAS client; 5) Then the CAS client accesses the CAS server again with the ticket, and the CAS server verifies the ticket; 6) The CAS Server returns the user information after the verification of Ticket, and the user can login after receiving the information.

3. Design of High Availability Scheme for Unified Authentication System Base on CAS

There are many users and information systems in colleges and universities and there are some high concurrency business scenarios. The conventional unified

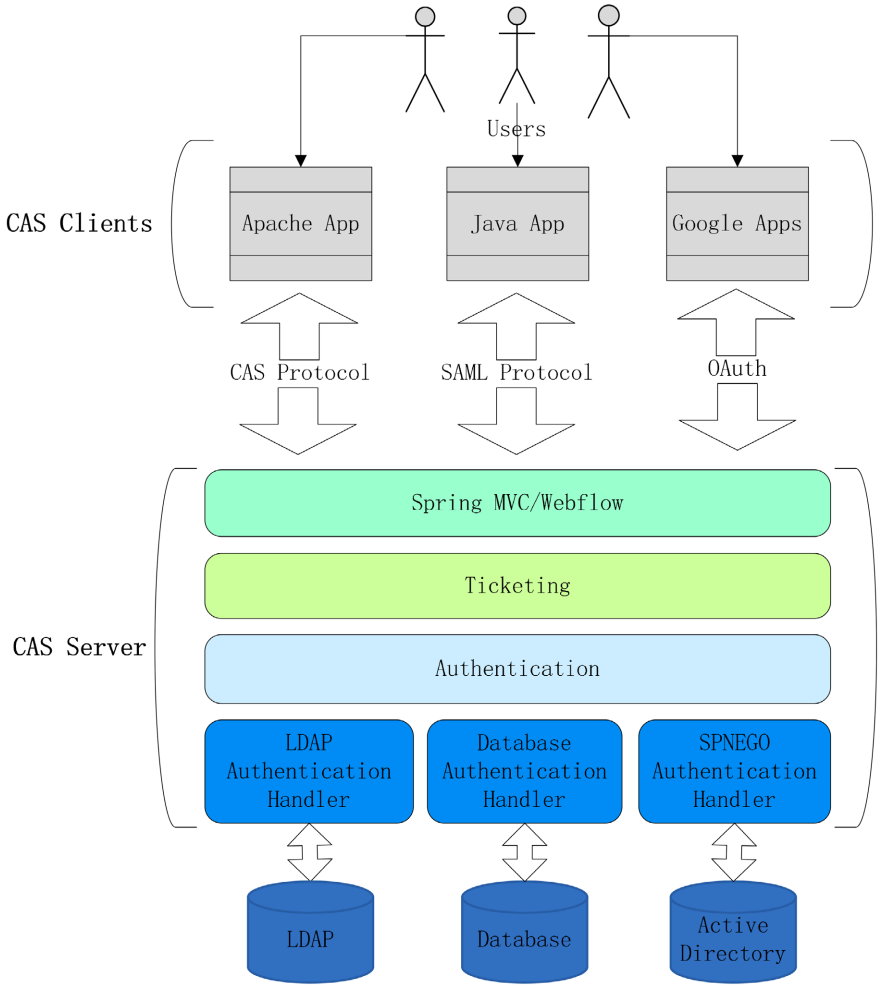

Figure 1. CAS Architecture.

identity authentication system based on CAS cannot meet the needs of large concurrency and heavy load well. After exploration and practice, the high availability scheme for unified identity authentication system is designed as shown in **Figure 3**. The high availability design has two key points. First, we deploy the CAS servers as a cluster. Second, the Redis is used as the cache database and the cluster deployment mode is used.

Multiple CAS server nodes are deployed as a cluster, and the Nginx performs load balancing at the front end. The number of Cas Server nodes can be comprehensively evaluated by the number of users, business concurrency, and the number of information systems integrated with Cas Client. Of course, the performance of the hardware server should also be considered. In general, 4 CAS server nodes can meet the concurrent needs for 20,000 users and 30 application systems.

Nginx is a lightweight and high-performance HTTP and reverse proxy server with high concurrency and fast response speed. Nginx can configure scheduling rules to realize the separation of static and dynamic resources. On the one hand, it acts as a reverse proxy at the front end to handle static resources such as

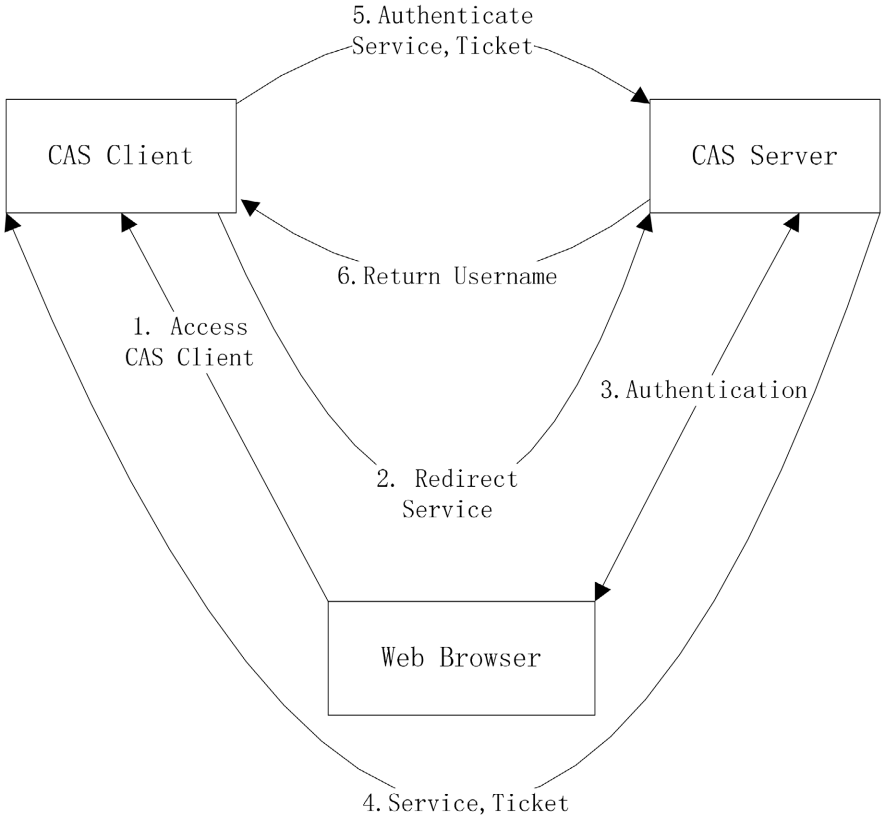

Figure 2. CAS authentication process.

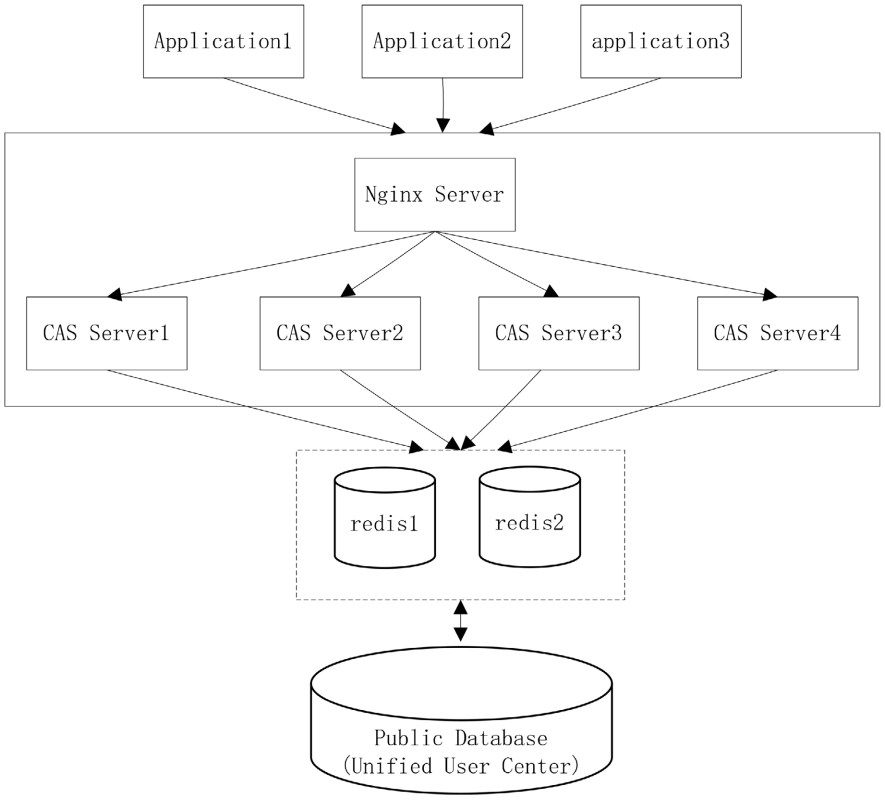

Figure 3. Architecture of high availability unified authentication system based on CAS.

HTML, CSS, JS, pictures, files, and on the other hand, it can use weight, ip_hash, url_hash and other load balancing strategies to shunt dynamic requests to the CAS server nodes on the back end.

During CAS authentication, if the client successfully logs on, the CAS Server randomly generates a fairly long, unique, unforgeable ticket and caches it for future verification. If the ticket is not persisted to the database or other middleware but only saved to the local cache, when the client requests to verify with CAS Server through the ticket, it will be randomly assigned to one of the nodes, resulting in matching failure. Here we choose to save the ticket to Redis. Redis is a high-performance key-value in-memory database that supports various data structures such as string, list, set, and hash. It caches data in memory and has a persistence mechanism, with excellent data reading and writing capabilities [6] [7].

In this scheme, Redis is used as the cache database of the relational database of the unified user center, and the user information is stored and accessed in the way of cooperation between Redis and the relational database. The CAS server accesses Redis first. If the current access user does not exist in Redis, the CAS Server accesses the relational database and updates the Redis at the same time.

To ensure stability and high availability and prevent the database from becoming a bottleneck of high concurrency, Redis is also deployed in cluster mode.

4. Implementation of High Availability Scheme for Unified Authentication System Base on CAS

The implementation of the high availability scheme for the unified identity authentication system based on CAS focuses on: the cluster deployment of CAS server; Redis acts as a cache database to uniformly store session, ticket and recent commonly used user information; improve the security of user authentication.

4.1. The Cluster Deployment of CAS Server

Two hardware servers are used and two CAS Server nodes are deployed on each hardware server. We select Tomcat as the middleware to run the CAS Server, occupying ports 8083 and 8084 respectively. Nginx is deployed on a single hardware server. The load balancing and reverse proxy configurations for Nginx are mainly reflected in the file of nginx.conf.

First, we add an upstream node as shown below:

```
upstream    cas_server {
   ip_hash;
   server      192.168.90.1:8083;
   server      192.168.90.1:8084;
   server      192.168.90.2:8083;
   server      192.168.90.2:8084;
   }
```

Second, we configure the proxy_pass parameter in the location node under the server node, referencing the name of upstream node as follows:

```
location / {
    proxy_pass http://cas_server/;
    proxy_http_version 1.1;
    proxy_set_header Connection "";
    proxy_buffering on;
    proxy_buffer_size          128k;
    proxy_buffers              2256k;
    proxy_busy_buffers_size 256k;
    proxy_connect_timeout      300;
    proxy_send_timeout         300;
    proxy_read_timeout         300;
    proxy_temp_file_write_size 256k;
}
```

4.2. Redis Database Stores Sessions, Tickets and User Information

The official CAS project takes into account the problems we encounter in the actual business scenario, and it supports Redis as a cache database to store sessions, tickets and user information.

1. Import dependent packages which support Redis to store and access sessions and tickets

```
<dependency>
    <groupId>org.apereo.cas</groupId>
    <artifactId>cas-server-webapp-session-redis</artifactId>
    <version>${cas.version}</version>
</dependency>
<dependency>
    <groupId>org.apereo.cas</groupId>
    <artifactId>cas-server-support-redis-ticket-registry</artifactId>
    <version>${cas.version}</version>
</dependency>
```

2. Configure sessions stored by Redis in application.properties

```
spring.session.store-type=redis
spring.redis.host=192.168.90.5:6379, 192.168.90.6:6379,
spring.redis.password=Ab@China86
```

3. Configure tickets stored by Redis in application.properties

```
cas.ticket.registry.redis.host=192.168.90.5:6379, 192.168.90.6:6379
cas.ticket.registry.redis.password=Ab@China86
cas.ticket.registry.redis.pool.max-active=20
cas.ticket.registry.redis.pool.maxIdle=8
cas.ticket.registry.redis.pool.minIdle=0
cas.ticket.registry.redis.pool.maxWait=1
```

4.3. Improve the Security of User Authentication

We have improved the identity authentication information security mechanism

based on CAS protocol and adopted some measures to ensure the security of identity authentication.

1) Improve the strength of the user's password, including the length and complexity. If the password does not meet the strength requirements during user authentication, the user will be forced to modify the password.

2) Enable two-factor authentication，using SMS verification code for secondary verification.

3) The hash function is used to calculate the user password to ensure the security of user information storage and prevent the password from being stolen or tampered in the transmission process.

4) The random number and timestamp are introduced to enhance the system's ability to resist network attacks such as dictionary attacks.

5. Summaries

In this paper, the high availability scheme of unified identity authentication system based on CAS has been practiced in China University of Geosciences (Beijing). The main business systems are integrated with the unified identity authentication system, realizing single sign-on, and the system runs securely and stably. It has the ability to support high concurrent access, and can meet the needs of large-scale information service access for teachers and students. The scheme in this paper can be used for reference by colleges and universities with large scale of teachers and students.

There are more and more user information authentication methods. It is the direction of future research and practice to unify traditional account password methods and biometrics (face, fingerprint), WeChat, NFC devices, campus cards and other authentication and recognition methods into one user ID and one identity authentication platform.

Acknowledgements

The author thanks the information network center of China University of Geosciences (Beijing) for providing a good working environment and all colleagues who provide help.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Ni, Y.Q. (2019) Design and Implementation of Unified Authentication for Highly Available LDAP Campus Network. *Value Engineering*, **35**, 284-286. (In Chinese) https://doi.org/10.14018/j.cnki.cn13-1085/n.2019.35.114

[2] Feng, K. (2018) Research on Uniform Identity Authentication Technology Optimization in Multi-application System Integration. Master Thesis, North China University of Technology, Beijing.

[3] Wang, Q. and Li, F.J. (2020) Laboratory Unified Authentication Scheme Based on Single Sign-On. *Experimental Technology and Management*, **5**, 219-223. (In Chinese) https://doi.org/10.16791/j.cnki.sjg.2020.05.049

[4] He, Y.M., Li, J.H. and Tang, H. (2011) Application of LDAP in Uniform Identity Authentication of Digital Compus. *Computer Technology and Development*, **5**, 139-142. (In Chinese) https://doi.org/10.3969/j.issn.1673-629X.2011.05.037

[5] Apereo Foundation. https://apereo.github.io/cas/6.5.x/index.html

[6] Li, J.L. (2014) Research on Unified Authentication Platform within High Concurrent Environment. Master Thesis, Nanchang University, Nanchang.

[7] Lin, P.R., Chen, Z.R. and Shi, X.Q. (2020) Highly Concurrent Multi-Threaded Competitive Shared Resource Architecture. *Computer Engineering and Design*, **11**, 3282-3288. (In Chinese) https://doi.org/10.16208/j.issn1000-7024.2020.11.045