Research of Unified Authentication System Based on LDAP

Jing-wei Ming
Department of Computer Science and Technology
ChengDong College Of Northeast Agricultural University
Harbin,150025, China
mjw19971979@126.com

Abstract—**With the development of Internet technology, the increasing of the application service makes the enterprise network management and security more and more complex. Based on it, the enterprise portal needs a system with high performance for identity authentication management. In this, implements the research of unified identify authentication system through LDAP, designs a rational structure of the directory tree. Thus, All the application servers use the user information in the same directory. By the manner, the problem of disagreement and larger maintenance burden can be solved and the system security can be improved.**

Keywords-Identity authentication; Directory tree

I. Introduction

In order to reduce the times of user logging in the independent application system, academic researchers have paid more attention to the unified authentication system since long ago. Such as IBM's Tivoli Access Manager, Microsoft's 550 integration system in the windows 2000, and so on. Some of the representative are Kerberos Protocol, Liberty Protocol, Sun's Identity Server and Microsoft's NET Passport, which support the unified authentication system.[1]

With the continuous development of information construction, many domestic organizations and institutions start to consider the problem of integration of application system. Unified and authentication have the focus of the study. Now, our domestic technology of the unified identity authentication is mainly including two parts: one is the digital signature authentication based on certificate[2].But most of them maintain in solving the individual demand level. They does not form perfect, unified holistic solution or standard. Another is based on username and password like UNIX, Which is vulnerable to attack and low security.

This thesis research the authentication system based on LDAP, according to application requirement of portal system of Heilongjiang electric power company. The system concentrate service information on directory service, which allows different place and system client to access easily. By rational use of directory service, the system can effectively reduce data repeatability and the burden of the management work.

II. Relevent Work

A. Related Problems

LDAP server is the core of database of the unified identify authentication system based on directory service. The system storing user identify, role and access control information, establishes corresponding strategy service system. In addition, it manages portal application system as a whole and executes authorization service of policy made by administrator[3]. So, needing to solve the following several key problems:

1). Build Directory Information Base

Directory Information Base(DIB) is the foundation of the whole unified user authentication platform. A user or organization information is collected and stored with hierarchical structure way for unified management, which assure consistency and integrity of the data, and, server all kinds of application system of the enterprise including enterprise portal, ERP system, yellow pages, network billing system, and so on.

First, the DIB can store the information of all kinds of the object in the enterprise net system, including network devices, all kinds of server, sector organization, user and so on. The storage of the information is not only concentrated but also distributed in different geographic position. (or different network environment)

Secondly, The DIB adapts to all kinds of new needs, makes appropriate adjustments, flexible changes or expands the information in the database if it is necessary, but, does not produce great influence for the existing data , as a result of its good expansibility and applicability.

Thirdly, The DIB provides standard directory access to all kinds of application based on LDAP caused of general LDAP interface[4].

2). Provide Information Service

The application program used for viewing or modifying the information in the directory information database was achieved. The application program must have the following some function: access based on Web, queried and modified information through Web, providing the ability of distribution access and management, offering different levels of information and safely be transferred information between the LDAP client and be severed with the authentication and authorization.

3). Unified Identity Authentication

The application program authenticating with the directory server was achieved, which was used for unifying the authentication function of the different application servers. User's identify and access management in the whole portal system were done through building an independent, high safety and reliability identify authentication and user permission management system.

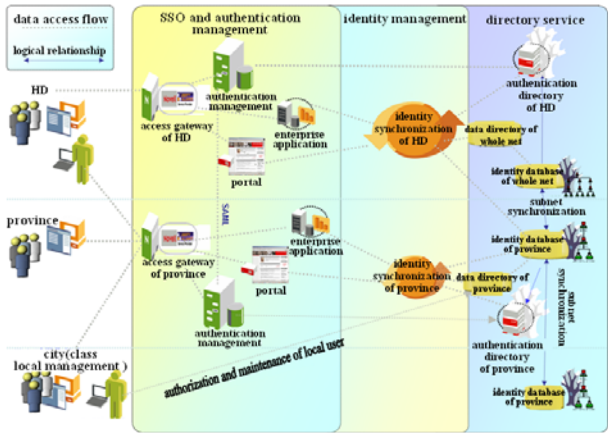
Published by Atlantis Press, Paris, France.

Than it changes the tradition and isolation of the identify authentication of each application system, and offers a possibility to realize a higher level of service in the intranet[5].

B. the System Architecture

State Grid Corporation of China Headquarters(HD) and all province companies composed the different security domain through the authentication systems which are independent of one another. After the user authenticated successfully in his security domain, the users can access all parts of the portal and the different application systems with Single Sign On(SSO). In addition, the user of HD can access the specified portal and application system of all province companies with cross-domain SSO, which must have the aid of the cascading authentication among the identity servers.

The chart of the structure shown as follows:


data access flow
logical relationship
SSO and authentication management
identity management
directory service
HD
access gateway of HD
authentication management
enterprise application
portal
identity synchronization of HD
data directory of whole net
authentication directory of HD
identity database of whole net
subnet synchronization
province
SAML
access gateway of province
enterprise application
portal
authentication management
identity synchronization of province
data directory of province
identity database of province
authentication directory of province
sub net synchronization
identity database of province
city(class local management)
authorization and maintenance of local user

FigureI. SYTEM ARCHITECTURE

The structure includes three parts.

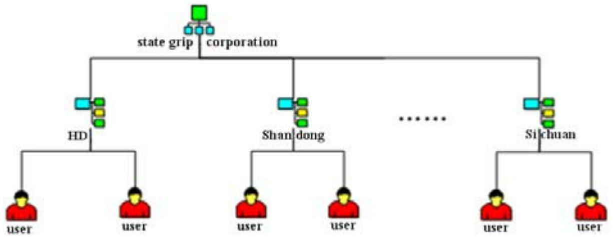
1). Directory Server

The directory system of HD was made up of 2-tier architecture, which were the HD directory and each province directory. According to the condition of network infrastructure, the requirement of personnel management and the requirement of application system deployment, each province company selectively established the city level of directory (That is third-tier deployment of the directory).

In order to promote the construction of directory system and implement the concatenation of levels of directory systems in the whole net, various directories of HD, province and city must be designed in strict accordance with the unified directory tree and the directory schema.

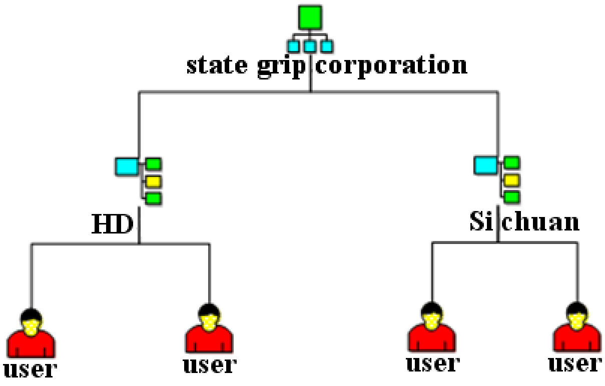
This 2-tier directory adapt to the geographical distribution of the HD and the province, reduce network bandwidth use, increase query efficiency of the directory, and conform to design standard of the super large enterprise distributed directory system at present.

In logic, identity directory in the whole net has the most completely user identity information and server user identity authentication and storage inside of state grid corporation of China. According to the organization structure, the design of directory tree can select a flat structure, showed as follows:



FigureII. DIRECTORY TREE OF WHOLE NET

Identity directory of province has the most completely user identity information and server the user identity authentication and storage inside of province. From the perspective of directory synchronization, the design of identity directory tree selected a flat structure, showed as follows:



FigureIII. DIRECTORY TREE OF PROVINCE

2). Identity Management

Identity management synchronized user information in the authoritative data source (such as human resource system) to identity directory is through identity synchronization tool. And, it can sent user information to each application system, according to a pre-specified strategy. That achieved Account to automatically creating, changing, canceling, replaced the existing manual account management. Novell Identity Manager (IDM) synchronized identity directory with database, directory and standard application. And, it stored the log information of key events in the database for later audit[].

3). Authentication System

Authentication system made up by access gateway and identity authentication management server, is the entry of unified access of portal in the HD or province and most application system, provides centralized authentication of user identity and security access of portal and application system. Using the mechanism of identity injection, access gateway based on reverse proxy realizes the SSO of portal and application system[6].

III. EXPERIMENTAL ANALYSIS AND RESULTS

C. Server Installation Requirements

Directory of state grid corporation, authentication and identity management need three computers at least. Considering of high availability reasons, computers

Published by Atlantis Press, Paris, France.

increased to eight HA or cluster architecture at least to avoid abnormal authentication of application system when single point of failure of wrong.

Installation of 3 computers is shown as follows:

TABLE I. AUTEHNTICATION SERVER REQUIREMENTS

CPU	Two 3Ghz CPU or higher
RAM	4.0 GB 533Mhz ECC DDR2
Hard Disk	100GB
Network	One integrated controller of 1000Mb/s Ethernet
Operator System	SUSE Linux Enterprise Server 9

TABLE II. GATEWAY SERVER REQUIREMENTS

CPU	Two 3Ghz CPU or higher
RAM	4.0 GB 533Mhz ECC DDR2
Hard Disk	100GB
Network	Two integrated controller of 1000Mb/s Ethernet
Operator System	SUSE Linux Enterprise Server 9

TABLE III. IDM SERVER REQUIREMENTS

CPU	Two 3Ghz CPU or higher
RAM	4.0GB 533Mhz ECC DDR2
Hard Disk	200GB
RAID	RAID10
Network	One integrated controller of 1000Mb/s Ethernet
Operator System	SUSE Linux Enterprise Server 9

D. Information Import

1). User Information Format

User information format using LDIF, is shown as follows[7]:

```
dn: cn=test1,ou=testou1,o=sgcc
ou=testou1,o=sgcc
changetype: add
objectClass: Top
objectClass: inetorgperson
```

2). Method of User Information Import

For importing and exporting user information, we use Novell ICE or JXplorer open source tools.

ICE is a Novell tool kit of data import and export. Command format is shown as follows:

ice –S LDIF –f export0904.ldif –D LDAP –s host IP –p port –d cn=admin4,o=sgcc –w novell –F

Jxplorer LDAP Browser, an open source graphical interface tool, is convenient to import and export full and partial data using LIDF.

We must modify the type of import entry in the import LIDF files. The detail is shown as follows:

changetype:modify （change user information）

or changetype:delete （delete user information）

User is modified and deleted by running the import script.

Example of command lines: ldapmodify –h 82.0.98.50:59151 –D cn=admin5,o=sgcc –w admin –f schema0607.ldif

3). Organization Information Import

Organization Information Format is shown as follows:

```
dn: ou=testou1,o=sgcc
ou=testou1,o=sgcc
changetype: add
objectClass: Top
objectClass: OU
```

4). Method of Organization Information Import

For importing and exporting user information, we use Novell ICE or JXplorer open source tools.

ICE is a Novell tool kit of data import and export. Command format is shown as follows:

ice –S LDIF –f export0904.ldif –D LDAP –s host IP –p port –d cn=admin4,o=sgcc –w novell -F

Jxplorer LDAP Browser, an open source graphical interface tool, is convenient to import and export full and partial data using LIDF.

We must modify the type of import entry in the import LIDF files. The detail is shown as follows:

changetype:modify （change organization information）

or changetype:delete （delete organization information）

Organization is modified and deleted by running the import script.

Example of command lines: ldapmodify –h 82.0.98.50:59151 –D cn=admin5,o=sgcc –w admin –f schema0607.ldif

E. Test Results and Performance Analysis

1). Test Results

When user access the enterprise portal, username and password will be submitted to directory service system. Directory server will compare them with data in the directory database , legal user can pass the authenticated of LDAP. If user is illegal, he can not log in the system successfully.

2). Performance Analysis

System design implemented centralized management and authorization of user. At the same time, through service of interface provided by user information management module, system served user centralized management of different user management systems. And system simplified integration process through registration function of application system. New application system without its own user system used unified identity authentication system to realize user's authentication and authorization.

By way of unified authentication, user's account and password are transferred only in the first login and transmitted encrypted. During user periodic authentication, asking message and authentication identifier for each authentication are different, so replay attack could be prevented effectively[8]. System bound user account with IP to timing authenticate to make sure user on line. That prevent certifier IP attack.

IV. CONCLUSION

In the thesis, system use directory tree structure and single sign on application system to solve the problem of user authentication of HD and authorization of accessing portal of province. Using TOKEN of mutual trust between HD and portal of province to realize unified identity authentication, user convenient and shortcut access all authorized application services, at the same time, system security is protected.

REFERENCES

[1] Hong Yan, “JAVA and model”,Beijing: Electronic Industry University Press,2002

[2] BruceSchneier, “Applied Cryptography”, Beijing: Machinery Industry Press,2005:361-367

[3] Xiang Li; Ai-nong Chao, “Research and application of LDAP in uniform identity authentication”, Journal of Computer Application,2008-S1,pp.28-32

[4] Cheng-long Zhang, Dong Wang, “Exploration and Practice of Directory Service Based on LDAP”, Financial Computerizing, No144,Apr.2012,pp.81-83

[5] W. Yeong, T.Howes, S.Kille. Lightweiht Directory Access Protocol.RFC1777, Mar.1995

[6] Jie Lan, “Research on Single sign-on System”, Technological Development of Enterprise,Vol.31 No.5,Feb.2012,pp.73-74

[7] Mohammad Salim; M Sana Akhtar; Mohammed A Qadeer,“Data Retrieval and Security using Lightweight Directory Access Protocol”, Proceedings of 2009 Second International Workshop on Knowledge Discovery and Data Mining,Jan.2009

[8] Wikipedia, “Replay Attack”, http://en.wikipedia.org/wiki/Replay_attack, Feb.2012