Design and Achievement of the Single Sign-on Base on the CGSP Security Management

Xuxiu  
Dept. of computer and science, mining university of science and technology, XuZhou china.  
(xuxiu@cumt.edu.cn)

MA Jun  
School of Mechanical and Electrical Engineering, Xuzhou Normal University, Xuzhou China

Abstract—An ideal grid system through the use of grid middleware platform,Shielding bottom hardware and software information,Completely transparent to the users computing environment.It is based on the CERNET network CGSP provided a complete set of grid services to support platform.It is integration the education and scientific research systems of the various resources,Shielding grid resources isomerization unit and dynamic.To ensure the security of the platform CGSP,through a single point of entry that would enable operational implementation process transparent to users, without reducing the security of identity authentication techniques.

Keywords- SSO; CGSP; Grid

I. INTRODUCTION

Grid is accompanied by computer,information and network technology arising from the rapid development of an advanced information infrastructure. Not only is it one of the informatics major development directions. And multidisciplinary and cross-frontier hot areas. With the demand for high-performance computing and the rapid development of information services. A high-performance computer has not competent to resolve some of the super-large-scale applications. We need to be geographically distributed and isomerization unit of high-performance computers, data services, access to large storage systems and through a variety of specialized equipment such as high-speed Internet connectivity and integrated together. This large-scale application of common solutions. This is a wide area of high-performance computing technology (Metacomputing). We now also known as grid.

Grid application to change people's research methods, education, lifestyles and ways of production activities. Institutions of higher education as the driving force of scientific research is also being actively engaged in the rapid development of it. With the enormous computing resources, storage resources, information resources needs. ChinaGrid will be used CERNET dispersion, and local self-government integration of the enormous resources by grid, through concerted and orderly management of the calculation, resources for the realization of the broad sharing of information and effective clustering, full release, thus providing a highly efficient computing services, data services and information services.

CGSP is the grid core middleware of the ChinaGrid. It provides a development environment for grid application, and effective shielding of the bottom grid resources with the dynamic nature of isomerization unit, for various scientific and engineering research with high-performance computing, highly reliable, safe and convenient transparent grid services, form a grid-oriented public service system CERNET.CGSP is a group of software components with, ChinaGrid application support the development; debugging; deployment; management and operational control systems such links.

CGSP is system of the ChinaGrid grid, based on the threat of a tiered structure where a management model, all domain node internal structure of logic is the same. And provide a group-oriented application programming interface grid application developers and programming model, independent of the software subsystems. Network Portal respectively, grid development environment, information services, domain management devices, operational management devices; services; packaging; information management systems, data management systems, grid security. The figure shows the functional software modules:

II. SINGLE SIGN-ON

That the presence of large numbers of users Chinagrid. Services and resources, to ensure the security of the platform CGSP. Chinagrid first need to ensure the legitimacy of each entity, determine the identity of each entity, only allows the user to register with a legal identity, user and deployment of services and resources. To enhance the user-friendly nature chinagrid, the implementation process should not only make operations transparent to the user, but can not reduce safety. Therefore, establish a relationship of trust users trust chain to achieve single-point user posted a very good way to address security issues. On the basis of this demand, Chinagrid security
management in achieving single point of entry from the following areas to achieve its corresponding functional.

A. Authentication

To develop their own CA Authentication Center, CA customers - user operating software documentation and the certificate request documents generated key of the body. Stored in the users local folder. Then use browser download site certificate issued. Certificate will be issued a certificate request upload to the website, awaiting certification bodies CA issued. Website will be issued a certificate request documents stored in the database, CA issued for the core software. CA core software applications from electronic databases track certificate request documents, after the adoption of a new audit, generate X.509 certificates documents. Stored in the electronic database applications; Users to download the certificate issued websites, download paper certificates, stored in the local folder. Completion certificate and receive applications. After center the Chingrid entity from the CA certificate, between entities in the world to use their own certificate to the mutual certification.

B. Acting certificate management

CGSP users to submit requests for operations, CGSP may use more modular implementation of user services operations. These modules also exist between the interchange. Individual service module access control mechanisms are not necessarily identical, the service module a possible mistrust service module B but only trust the users. If users need to inform the service module on the A, B service module request is submitted in order to complete the user operations and issued. Therefore users will be provided a certificate to show their identity. If this situation recurring, users will continue to use their own certificate repeatedly certification, it will not only increase the use of the complexity, but also make frequent user certificate information exposed. Increased the risk of leakage of information users. Acting mechanism through certificates, but only users of a time-bound agent signing certificate stored in CGSP. Acting certificate management devices, Chingrid entities in the implementation of the service users operations, management devices directly from the agent to obtain user certificates Acting certificates, acting certificate requests, avoid recertification process, simplified operational procedures, the user will not be repeated in the implementation process of accreditation operations to achieve single-point entry.

C. Acting certificate management through a single point of entry

Acting certificate management tool for the preservation of user agent certificate information, CGSP entities to use the certificate to a user agent acting on the certificate management enquiries, acting certificate if users exist and allowing its visit, the direct use, or transfer agent services-certificate to the client-agency certificate signed by the Acting certificate request.

Users through the CA for identity authentication, will lead web browser certificate, and then through the Portal Https connect CGSP Web site will connect users successfully registered, the user ID and password to the domain of information management devices. Domain management device based on user ID information and shine upon rules will

D. Acting certificate management module

Acting certificate management module client side certificates by the acting clients, acting certificate management and certificate services by the three-part composition. Acting certificate management devices which use MyProxy achievement, the Acting certificate clients - module main conclusion of the signing user agents operating certificate request, the acting servers completion certificate services-main request made to the corresponding certificate signed users.

III. SINGLE SIGN-ON OF ENTRY

A. Acting client-certificates

- The Acting certificate clients - interface, complete service management agent signing certificate

Public boolean checkcert

Public string getcertId
Private void jbInit() throws Exception
Void JButtonOpenFile_actionPerformed
Void JButtonscankey_actionperformed
Void JButtonscantrusted_actionperformed
Private void saveconfig
Void JButtonstart_actionperformed
Void JButtonstop_actionperformed

Public void run
Public passDialog
Private void jbInit() throws Exception
Void JButtonok_actionperformed
JButtoncancel_actionperformed
• The Acting Acting certificate and the certificate customer-service-network connectivity

Public client
Public void run
Public passDialog
Private void jbInit() throws Exception
Void JButtonok_actionperformed
JButtoncancel_actionperformed
• Signed management-customer-completion certificate
  Acting certificate signed task

Private void jbInit() throws Exception
Void JButtonsign_actionperformed
Void JButtonreject_actionperformed
Public userCA
Public GSSCContext getsecureContext()
Public static privatekey loaduserkey
Public void stopserversocket
Public string getIP
Public int getPort
Public int getLifetime()
Public void setMyProxy
Public synchronized GSSCrednial getGSSCredential() throws myproxyException
• Acting in-service operating certificate services-operation, access to the user certificates signed by the Acting Information

B. Acting certificate services
• Acting in-service operating certificate, certificate of completion generated Acting preparations
  Public byte[] initDelegation
  Public byte[] acceptedDelegation
  Public void setDelegationType(int type)
  • Acting on the certificate services-operation, securing the two categories
  Public ProxyCertificateDealer(user user, string userCA_ip)
  Public ProxyCertificateDealer
  Public ProxyCertificateDealer
  Public static void checkCertificates
  Public synchronized GSSCrednial getGSSCredential
  Public void howToUse()
  • Acting certificate services-operation in the completion of the building work, the Acting certificate request, and transmitted to the corresponding agency -client certificates
  Public ExtendedGSSContext getsecureContext()
  Public GSSCrednial getGSSCredential()
  • Acting in-service operating certificate from the MyProxy visit Acting certificate
  Public proxyCertificateRetriver
  Public MyProxy getMyProxy()
  Public int getLifetime()
  Public void setLifetime
  Public void setMyProxy
  Public synchronized GSSCrednial getGSSCredential() throws myproxyException
  • Acting on the certificate services-operation, access to the user certificates signed by the Acting Information
  Public user(string user, string pass)
  Public void setPass(string newpass)

SUMMARY

Grid computing environment requires not affect the nodes local management and autonomy, not to change the original operating system, network and service agreements to ensure that users and remote nodes security, allowing remote nodes choose to join or withdraw from the system to make use of existing technology standards for the compatibility of existing applications and to provide reliable disk mechanisms.

An ideal grid system through the use of grid middleware platform, shield bottom hardware and software information to users with complete transparency computing environment.
Single point recorded (SSO, Single Sign-on) can visit user-friendly network. Network structure and network applications regardless of how complex, users need only to download a registration can obtain the necessary authorization to access the system and application software. Overall management of user identity and user information simultaneously to a single point of entry solution to the problem laid the foundation. Single point of entry for the user identification, and then visited network users through proxy servers, greatly increasing system security.

REFERENCES