

Enabling remote access to projects in a large collaborative environment

V.F. Pais^{a,*}, S. Balme^b, H.S. Akpangny^b, F. Iannone^c, P. Strand^d

^a Laser Department, National Institute for Laser, Plasma and Radiation Physics, P.O. Box MG-36, Bucharest 077125, Association EURATOM/MEDC, Romania

^b Association EURATOM CEA/IRFM CEA-Cadarache, France

^c Associazione EURATOM-ENEA sulla Fusione, C.R. ENEA Frascati, via E. Fermi 45, 00044 Frascati, Rome, Italy

^d Department of Radio and Space Science, Chalmers University of Technology, SE-412 96 Goteborg, Sweden

ARTICLE INFO

Article history:

Available online 11 March 2010

Keywords:

Portal

Project management

Authentication

Remote data access

ABSTRACT

In the context of the Integrated Tokamak Modelling Task Force, a large number of software projects are made available to the task force members, including developers and end-users. This has been achieved through a combination of tools and technologies.

The front-end is represented by a Java based portal system exposing a PHP project management system, GForge. These two applications are linked by a single sign-on mechanism, Shibboleth [1], and through secure HTTP [2] request rewriting, where appropriate. Furthermore, the underlying storage facility is an OpenAFS [3] distributed file system and the user base comes from both a network information server and an LDAP [4] directory. Security mechanisms are those of a distributed system, with multiple access points and protocols used for reading and writing data.

The present paper presents the challenges of integrating these different technologies and programming languages into a single, working, application presented to its users as a web portal. Chaining of the tools is explored through the user perspective, with an in-depth overview of the background transitions between the various systems involved with regard to security requirements for the front-end nodes and the policies as seen by the users.

© 2010 Elsevier B.V. All rights reserved.

1. Introduction

Portal systems provide an easy way to access applications running in remote locations through a web browser. Users can share data and collaborate on projects without the need to install any local applications, thus making it possible to do their work on any operating system equipped with a web browser. Furthermore, the applications used through the Portal can run on powerful servers, allowing users to harness their resources.

To serve the needs of the Integrated Tokamak Modelling Task Force, a portal system has been developed. It offers access to dedicated areas for each ITM project and tools like wiki, content management, software project management and administration tools.

After a careful consideration of various portal systems, like Glassfish [5], oPortal [6] and OpenPortal [7], it has been decided to use the JBoss Portal [8] in combination with the JBoss Application Server. The decision was based on standards compliance, application speed, availability of servlets for the chosen platform and the possibility of integration with other technologies, discussed below.

Since there are no software management systems available as servlets and offering acceptable performance on the existing platforms, a PHP-based system was selected: GForge Advanced Server [9]. GForge AS is a modern, extensible platform with an intuitive interface that ties together a huge toolset, from Source Code Management (SCM) to extremely customizable trackers, task managers, document managers, forums and mailing lists. All of these are controlled by a centralized permission system and maintained automatically by the system.

Because the two systems, the ITM Portal and GForge AS, are written in different languages and are running on separate machines it was necessary to deploy a single sign-on (SSO) mechanism that becomes a central node for all authentication requests, dispatching this information to all applications. The SSO application used for the ITM Portal is Shibboleth. It was selected based on standards compliance, configuration requirements, security and the easiness of integrating it in different programming languages and servers.

2. System architecture and implementation

The overall system architecture is based on several applications, each executing inside a container, interacting through the network.

After selecting the appropriate technologies for each required function of the Portal, it was necessary to integrate them in a

* Corresponding author. Tel.: +40 721678357.

E-mail address: pvf2005@gmail.com (V.F. Pais).

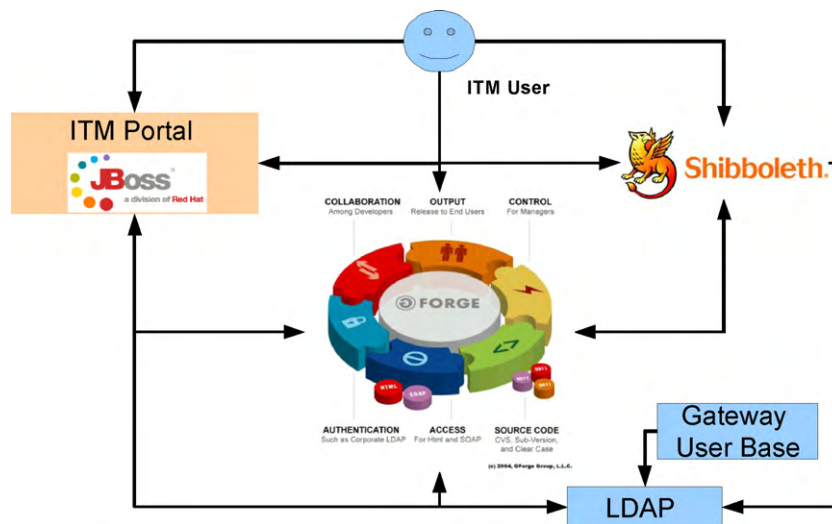


Fig. 1. General system architecture with connections between the various elements.

single, working, environment. Several “glue” mechanisms were needed.

Each application is running inside a specialized container: JBoss Portal inside JBoss Application Server, Shibboleth Identity Provider inside Apache Tomcat, GForge AS inside Apache HTTPD [10]. A “super server” in the form of an Apache HTTPD server was placed as the front-end of this system. All user requests first arrive at this HTTPD server and then are routed to the appropriate application. Because of this implementation, some address spaces became overlapping and requests needed to be modified, using “mod_rewrite”, part of Apache HTTPD.

Furthermore, for certain parts of the portal, the identity of the user must be passed in custom headers inside the request. This was achieved using “mod_rewrite” as well, but with the added problem of disallowing such headers to arrive from the Internet. Therefore, filtering of inbound requests was also integrated in the front-end server.

In order to access the same user base as the ITM Gateway system, an LDAP server, based on OpenLDAP, was placed between the portal and the Gateway. This directory server is synchronized periodically with the Gateway, in regard to authentication information and basic group membership. Nevertheless, more advanced group membership information was needed for the Portal operation. This is stored in LDAP on top of regular Gateway data.

Authentication is performed by the Shibboleth Identity Provider and all other systems rely on this information. However, authorization is a local issue, because there are different requirements for each application. For example, the main portal needs information on who has access to various pages, the content management system needs to know who can edit documents and GForge must have access rights for the various projects and files hosted inside its system.

A diagram describing the various interactions between the ITM Portal components is presented in Fig. 1.

3. Security considerations

Users interact with the ITM Portal through its web interface. Therefore, the primary concern was to restrict access to the HTTP related ports. Nevertheless this is not enough to ensure a secure system.

All HTTP requests must be inspected to make sure they do not contain unwanted or potentially malicious data. This is achieved through the Apache HTTPD front server.

Furthermore, policies must be correctly defined for the various parts of the system. The policy setting task is delegated to ITM project leaders and software project administrators.

Software project management is a very sensitive component of the system. Each project can have various options activated, like source code management, bug reporting, wiki and document management. A special ITM policy has been defined describing what rights various users should have, in close relation with their ITM involvement. When a new software project is submitted for approval by the ITM leadership, a default policy is applied. Afterwards, the project administrator must make sure the policy is updated and enforced when needed.

Since the official launch of the ITM Portal, several attacks by web worms were registered and there is always the possibility of facing denial of service (DoS) attacks. In order to resist to such incidents, the exposed pages without authentication are kept to a minimum.

All components use the Gateway distributed file system (AFS) for storage. This required special access control lists to be put in place in order to prevent unauthorized access from other machines in the Gateway cluster.

4. User interaction with GForge system

GForge is a management system for the collaborative development of projects. It provides a unified interface to a set of server software and integrates several open-source applications. It is used by thousands of firms and government agencies around the world.

The version used for the ITM project is GForge Advanced Server (GForge AS). GForge assists in the management of the entire development life of projects and offers via a unique access point from a web browser, the three main types of functions necessary for the collaborative development:

1. Communication tools: web forums, mailing lists, publishing of news, wiki, etc. to ensure better traceability of actions. With these tools, any member of a project is always informed of any relevant event that takes place on the platform via a notification by mail and can respond to a solicitation.
2. Issue tracking system: bug tracking, support, task and project managers.
3. Tools for sharing information: source code management (SCM) to create and control access to files in repositories, documentation manager, file manager.

Download English Version:

<https://daneshyari.com/en/article/272385>

Download Persian Version:

<https://daneshyari.com/article/272385>

[Daneshyari.com](https://daneshyari.com)