ISSN 1673-9418 CODEN JKYTA8
Journal of Frontiers of Computer Science and Technology
1673-9418/2012/06(00)-0000-00
DOI: 10.3778/j.issn.1673-9418.2012.00.000

E-mail: fcst@vip.163.com
http://www.ceaj.org
Tel: +86-10-51616056

动态虚拟组织管理系统设计与实现*

蔡世霞[1], 曹军威[1,2+], 林筱[3]

1. 清华大学 信息技术研究院, 北京市 100084
2. 清华大学 清华信息科学与技术国家实验室,北京市 100084
3. 清华大学 自动化系,北京市 100084
+ 通信作者邮箱: jcao@tsinghua.edu.cn

Design and Implementation of a Dynamic Virtual Organization Management System*

CAI Shixia[1], CAO Junwei[1,2+], LIN Xiao[3]

1. Research Institute of Information Technology, Tsinghua University, Beijing 100084, China
2. Tsinghua National Laboratory for Information Science and Technology, Beijing 100084, China
3. Department of Automation, Tsinghua University, Beijing 100084, China
+ Corresponding author: E-mail: jcao@tsinghua.edu.cn

CAI Shixia, CAO Junwei, LIN Xiao. Design and implementation of a dynamic virtual organization management system. Journal of Frontiers of Computer Science and Technology, 2012, 6(0): 1–000.

Abstract: The innate coarse-grained management of grid computing leads to inflexible structure, which brings about much inconvenience and inhibits a broader application of grid computing. With the virtual organization concept, this paper proposes a dynamic virtual organization management scheme which provides fine-grained project management to solve this problem. This scheme manages grid projects as different virtual organizations and controls user access according to membership relations in virtual organizations. Above the Globus grid system, a dynamic virtual organization management system is developed. A case study is also given to demonstrate the effectiveness of this scheme for fine-grained dynamic management of multiple grid systems.

*The National 973 Basic Research Program under Grant No. 2011CB302805, (国家 973 重点基础研究发展计划); the National 863 High-tech R&D Program under Grant No. 2011AA040501 (国家 863 高技术研究发展计划).
Received 2012-2-21, Accepted 2012-2-21.

Key words: grid computing; virtual organization; dynamic management systems; Globus

摘 要: 网格计算粗粒度的管理方式导致的网格体系僵化也带来了诸多不便，成为了将网格计算在科研领域更深入应用的阻碍。采用虚拟组织的思想，本文提出了动态虚拟组织管理方案来针对网格计算项目进行细粒度管理。该方案按照虚拟组织的方式管理多个网格计算项目，以虚拟组织成员关系控制用户访问的权限，使得虚拟组织的构成更加灵活。针对 Globus 网格平台设计了动态虚拟组织管理系统，实际应用表明该系统实现了细粒度的多网格管理，证明了动态虚拟组织管理方案的有效性。

关键词: 网格计算；虚拟组织；动态管理系统；Globus

文献标识码：A 中图分类号：TP302

1 引言

网格计算能够以低廉的价格快速获取计算能力的优势使其尤其适用于科学计算[1]，为特定的大型科研应用提供专门的计算机，数据共享和管理平台，LIGO[1]（Laser Interferometer Gravitational-Wave Observatory，激光干涉引力波天文台）和 GIMPS[2] (Great Internet Mersenne Prime Search,寻找最大梅森素数)都是典型的网格计算项目。这些项目的实施都需要跨组织的合作，而网格计算可以从技术上使用虚拟组织（Virtual Organization，简称 VO）的运行和管理[2]。

在过去十多年中，许多网格被建立起来以满足某些重大专项科研项目，在美国网格类型的科研合作项目有几十个，典型的如美国的 OSG （Open Science Grid）[3]等。随着网格计算的应用日渐广泛，网格规模的逐渐扩大，网格计算粗粒度管理方式的弊端开始显现，虽然每个科研组织内部通过网格计算等技术实现了跨组织的资源共享，但是多个网格之间还是彼此无法互通[3]。主要体现在：网格是针对特定的项目构建的，每当应用变化时往往需要搭建新的网格平台，这会带来不小的开销；网格中的项目相互之间需要权限管理来区分，这对于资源较多以及人员变更频繁的网络来说是一个不小的负担；当网格中的项目增多时，用户想查找一个具体项目或某一个项目需要寻找一个合适的资源时也有着诸多不便，这些成为了将网格计算在科研领域更深入应用的阻碍。和过去相比，当前的科学研究方式要求提供更加广泛的集成和共享资源；跨越地理和组织的限制，动态的，按需的集成资源；安全，可扩展的管理资源；而这是传统网格技术不能解决或不擅长解决的。

在美国，国家科学基金委（NSF）为了解决上述问题提出了赛百平台（Cyberinfrastructure，简称 CI）[4]的构想。赛百平台是众多网格的集成，打破了网格之间的屏障，实现不同网格资源的重新调配和安全访问。如何将赛百平台上分布式的资源根据科研项目需求动态安全的集成为一个虚拟组织，实现虚拟组织内部的高度共享和虚拟组织之间便捷安全的合作成为亟待解决的问题。

目前有几种被广泛使用的 VO 管理相关机制和技术，如 VOMS[4]（Virtual Organization Membership Service，虚拟组织成员服务），但是其缺点是虚拟组织成员或权限发生变更时，网格应用并不能第一时间获知这一变更，对于管理一个成员频繁变动，

[1] LIGO, http://ligo.org.cn/
[2] GIMPS, http://www.mersenne.org/
[3] OSG,http:// www.opensciencegrid.org/
[4] VOMS,http://edg-wp2.web.cern.ch/edg-wp2/security/voms/voms.html

十分活跃的虚拟组织来说并不是很有利。GUMS[5]（Grid User Management System）提供了网格用户身份映射的服务，但是在网格计算的动态环境中，映射表的维护问题没能很好地解决。VO Services Project[6]是对 VOMS 和 GUMS 的一个综合，很好地对二者的优缺点进行了互补，形成了一套相对完善的细粒度虚拟组织管理系统。但 VO Services Project 依旧带有 VOMS 和 GUMS 的一部分缺点，如需要多次颁发证书等。

本文根据虚拟组织的思想，针对上述分析的问题提出了动态虚拟组织管理方案。基于虚拟组织的访问控制直观方便，更适合当前大规模的权限管理。该方案按照虚拟组织的方式管理网格计算项目，以虚拟组织成员关系控制用户访问的权限。根据实际项目需要动态创建、取消虚拟组织，使得虚拟组织的构成更有针对性，从而达到网格计算的细粒度管理。为了实现资源的共享，同时为用户提供权限的管理，针对 Globus[5]网格平台，本文给出了这个方案的具体实现——动态虚拟组织管理系统，并描述了系统关键模块的功能和实现技术。

本文第 2 章介绍动态虚拟组织管理解决方案的构成；第 3 章重点描述动态虚拟组织管理系统关键模块的功能和实现技术；第 4 章描述该系统在 Globus 网格平台上的测试过程；第 5 章总结全文。

2 动态虚拟组织管理解决方案

2.1 虚拟组织的概念与应用

虚拟组织是网格计算的关键概念，是由个人和自治域按照一定的资源共享规则形成的集合，自治域或个人通过虚拟组织共享资源和进行问题求解。通过动态管理虚拟组织的方式可以很方便地实现权限管理[6]。同一个虚拟组织内的成员之间可以相互访问资源，而虚拟组织外的用户不能访问虚拟组织内部的资源，在收到访问请求后，资源提供者只需要在虚拟组织登记表中查询用户与自己是否处于同一个 VO。用户加入或退出虚拟组织的时候，也只需要根据其请求来对应修改表格，而不是维护所有成员的访问权限映射表。对于一个节点众多的网格，这省去了可观的重复操作，动态虚拟组织的这个特点使其很适合于网格管理的工作。

动态创建与管理的虚拟组织能够实现细粒度的网格管理。对每一个具体的计算项目构建一个单独的虚拟组织，组织中的科学家可以访问组织中的资源。当科学家需要更多资源时，可以批准更多的资源加入虚拟组织，每个科学家并不需要直接与组织外的其他人建立信任关系，这正契合了计算项目自然的组织方式。Cyberinfrastructure 是用虚拟组织方式管理网格计算的一种应用。

2.2 带有评价系统的动态虚拟组织管理方式

动态虚拟组织通过动态地在网格内部创建、取消以及虚拟组织成员变更来方便地实现网格计算的权限管理。其核心是维护包含虚拟组织信息的数据库。这个数据库中有两类重要的表格：虚拟组织登记表和成员登记表。当一个用户或资源提供者加入一个虚拟组织时，他将可以访问虚拟组织中的所有其他成员提供的资源，而同时他也需要贡献出自己的资源（如果有）供虚拟组织中其他成员来使用。虚拟组织外部的用户或资源提供者不能够访问虚拟组织内部的资源。而虚拟组织的关系可以通过查询虚拟组织成员的方式从数据库中得到，因此权限管理变得十分方便，只要通过读取数据库中的信

[5] GUMS，https://www.racf.bnl.gov/Facility/GUMS/1.3/

[6] VO Services Project，http://computing.final.gov/docs/products/voprivilege

息，即可确定成员是否可以访问，以及应该如何被映射。

虚拟组织的创建和撤销可以通过在虚拟组织登记表中添加新项和删除对应项来完成。当一个新用户或新资源提供者进入网格后，通过在数据库中查找虚拟组织信息，寻找并加入与自己的目标或与自己的服务特性相吻合的虚拟组织，从而快速投入使用。如果要开始一个新的项目，则可以创建一个新的虚拟组织。在虚拟组织登记表中添加新的一项，并在成员登记表中添加本虚拟组织对应的新的成员，或者新开一张成员登记表。当项目结束需要关闭时，则只需要撤销当前的虚拟组织，在虚拟组织登记表中删除对应项，并删除成员登记表中对应的内容。

虚拟组织在批准用户或资源提供者的加入请求之前会进行审核。审核并批准加入的过程可以是手动的，但对于有很多用户和资源提供者的大环境来说，自动批准或拒绝申请可以节省很多工作量。审核的过程可以通过一个函数的形式完成，比如：如果审核不通过，则拒绝该用户或资源提供者的加入申请；如果审核通过，则自动将该用户或资源提供者加入成为虚拟组织的成员。另外，审核过程中也可以同时对用户打分，并根据打分情况决定用户能访问的资源或决定用户的角色，从而实现更细粒度的权限管理。

审批的过程也可以是有目的的，比如提高网格的 QoS（Quality of Service，服务质量），王震等提出了专门针对网格计算资源评价的算法[7]，相应的开发了虚拟组织成员评价系统[8]。这个算法首先选择一些有威望的节点形成一个 Committee，由 Committee 对资源进行打分，最后通过一个模糊决策方式得到资源的最终得分。该系统被证明能够有效地提升网格资源的质量。通过有目的性的审核机制，可以针对虚拟组织的目标优化组织内部的人员和资源配置，从而更好地完成预定的任务。

相比传统的网格计算管理方式，动态虚拟组织的管理方式有如下优点：

1.动态虚拟组织的管理方式提供了细粒度的计算项目管理。

2.不需要每个成员维护一个访问控制表,访问控制维护更加便捷。

3.通过虚拟组织的管理方式可以很清楚地追踪一个计算项目的发展，而且可以分清项目与其他计算项目之间的界限。

4.增加了对用户和资源管理者的评价机制，使得虚拟组织的成员加入审批有了一个有价值的参考标准，从而保证资源的共享和使用能够安全可信，建立可信安全的共享关系。这种细粒度的权限管理方式可以使得依据审批规则生成的 VO 对计算项目的目标更有针对性。

2.3 动态虚拟组织管理的架构

动态虚拟组织管理的方式提供了便捷的细粒度访问控制功能。通过这种方式管理的网格计算系统由三部分组成：客户端、CI 服务器与 VO 服务器三大部分组成，方案架构如图 1 所示。

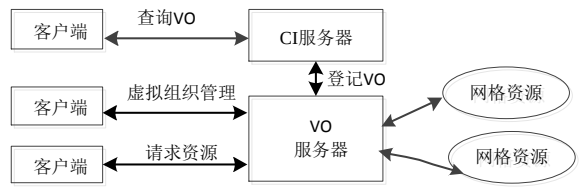

Fig.1 Dynamic virtual organization management system structure

图 1 动态虚拟组织管理系统架构

在该架构中，用户对资源的访问需要虚拟组织的认证来授权。因此当用户访问资源时，需要向 VO 服务器提交访问资源的请求，VO 服务器验证用户身份后授权用户访问虚拟组织中的资源。VO 服务

器还需要维护虚拟组织成员的表格以支持用户的加入、退出、成员查询等操作。为了更好地维护虚拟组织成员登记表 VO 服务器中还需要配备管理员的机制以及合理的管理员任免机制以便更好的维护虚拟组织成员登记表。

CI 服务器管理网格中所有用户和资源的身份信息，并登记所有 VO 的信息，方便用户和资源提供者查找并加入合适的 VO。CI 服务器还需要维护用户以及虚拟组织登记表，支持虚拟组织的登记、解散等操作。CI 应当配备一个证书中心，供新用户注册使用。

动态虚拟组织管理系统应该有一个便于操作的客户端，给用户提供查找 VO 及使用资源的良好界面，同时又要完成与 VO 服务器及 CI 服务器的通信。

该架构支持了用户从查找 VO 到使用资源的一整套流程，是动态虚拟组织管理的基本框架。

2.4 动态虚拟组织管理与 Globus 的连接

动态虚拟组织管理系统提供了网格中用户权限的信息管理，为了真正让用户能够利用分布式资源，实现资源共享，还需要其他组件例如 Globus，Condor 等工具的支持，我们采用 Globus Toolkit 搭建网格，通过动态虚拟组织管理系统与 Globus 连接来完整地实现用动态虚拟组织管理网格计算的理念。

Globus 通过证书机制和帐户映射的方式完成用户认证以及访问控制。其核心思路在于将远程来访者映射到本地的特定账户，使之拥有本地账户相应的权限。针对 Globus 通过配置 grid-mapfile 与制定 localname 权限实现访问控制的方式，动态虚拟组织管理框架可以通过修改 grid-mapfile 来完成对 Globus 构建的网格计算系统的访问控制。

Globus 修改 grid-mapfile 的命令主要有两条：

- 添加：grid-mapfile-add –dn distantname –ln localname
- 移除：grid-mapfile-delete –dn distantname –ln localname

在该方案中，动态虚拟组织管理架构与 Globus 连接方式的示意图如图 2 所示。

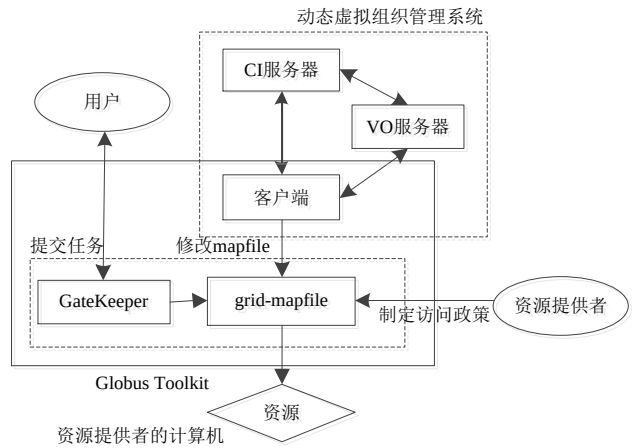

Fig.2 Connection between dynamic virtual organization management structure and Globus

图 2 动态虚拟组织管理与 Globus 的连接

当服务器端虚拟组织成员信息发生变化时，由服务器端向客户端报告，客户端通过变化成员的 Subject、加入还是退出和资源提供者的 localname 生成 grid-mapfile-add 或 grid-mapfile-delete 命令并执行，从而自动地修改 grid-mapfile。

资源提供者不在线时，服务器无法实时报告成员变化，需要将成员变化信息保存起来，待资源提供者上线之后进行对应 grid-mapfile 的修改。可以通过在 CI 服务器中建立一个消息表 Message，保存所有 VO 的成员变化信息及变化发生时间来解决。资源提供者上线后向 CI 服务器请求 Message 表，按照时间顺序执行 VO 成员变化的修改，就可以实现自动修改 grid-mapfile 的功能。

3 动态虚拟组织管理系统的设计与实现

为了实现用动态虚拟组织管理方式管理网格计算，基于前面提出的架构我们设计了一个动态虚拟组织管理系统。该系统应能够完成基本的虚拟组织管理操作，如建立、加入、退出、解散以及查询组织成员等功能；并且能够按照虚拟组织的信息向网格计算软件提供控制外来用户访问的信息，对于组织内部的成员则允许访问，对于组织外的成员则拒绝访问，实现网格的权限管理。该系统的模块结构如图 3 所示：

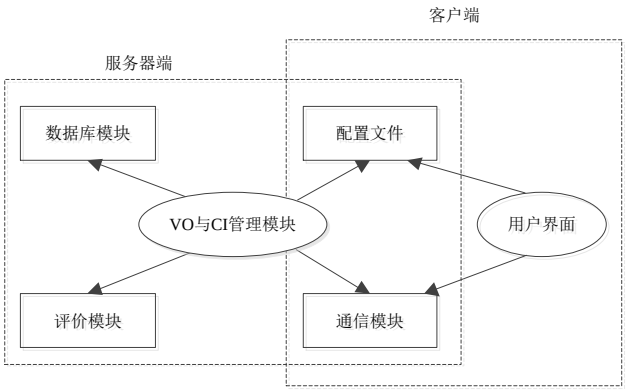

Fig.3 Module structure of dynamic virtual organization management system

图 3 动态虚拟组织管理系统的模块结构

系统分为服务器端和客户端两部分，服务器端由配置文件、通信、数据库、评价以及 VO 与 CI 管理模块构成。配置文件模块负责配置文件的读取与分析；通信模块负责通信规则与保证通信的安全；数据库模块负责管理数据库的访问操作；评价模块负责对用户或资源提供者给出评价；VO 与 CI 管理模块负责按照命令对 VO 服务器端与CI服务器端的数据库进行合理的操作，维护成员登记表和虚拟组织登记表，以完成权限管理。客户端由配置文件模块、通信模块和用户界面模块组成。配置文件模块负责读取与分析配置文件；通信模块负责客户端与服务器的通信规则与安全；用户界面模块负责用户与客户端的接口。下面详细描述一下系统的关键模块。

3.1 通信模块

为了保证用户与服务器交互的传输安全，并将 VO 与 CI 管理包装成 WEB 服务的形式，本系统的通信模块基于带 SSL（Secure Sockets Layer ，安全套接层）的 SOAP（Simple Object Access Protocol，简单对象获取协议）协议建立。SSL 的基础是 PKI（Public Key Infrastructure，公钥基础设施），通过提供加密和数字签名等密码服务及所必需的密钥和证书管理体系来保证信息传输的安全。

证书的签署：用户生成私钥和一个请求签发的 request 证书，将 request 证书发送至证书中心。证书中心用自己的私钥签署用户的 request 证书 ,生成用户的公钥，并发送回用户。

证书的使用：用户发送消息时用自己的私钥和对方的公钥对消息进行加密。解密时只能用公钥和对方的私钥解密。对于一个恶意用户，由于不知道二者中任何一人的私钥，既不能伪造成发送方，也不能伪造成接收方。

服务器端具体流程是 SOAP 通信的服务端绑定并侦听一个端口 ,每当端口接收到数据包时 ,SOAP 首先对对方进行身份认证,认证通过后调用回调函数 ns__hdl 进行处理，流程如图 4 所示。

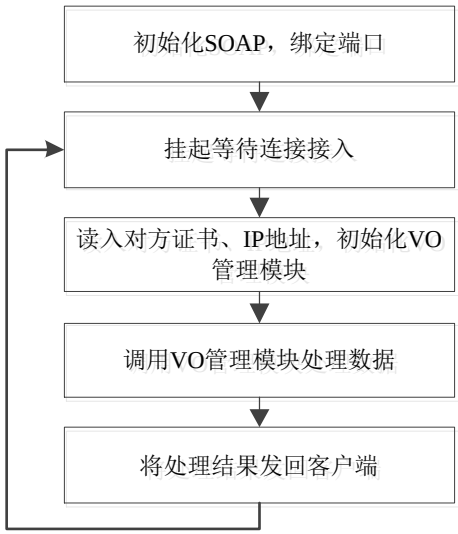

Fig.4 Sever communication module flowchart

图 4 服务器端通信模块流程图

客户端的通信模块 Sender 完成客户端与服务器进行通信的工作。该模块发送指定的一个 vector<string>对象到服务器，并读取服务器返回的 vector<string>，具体流程如图 5 所示。

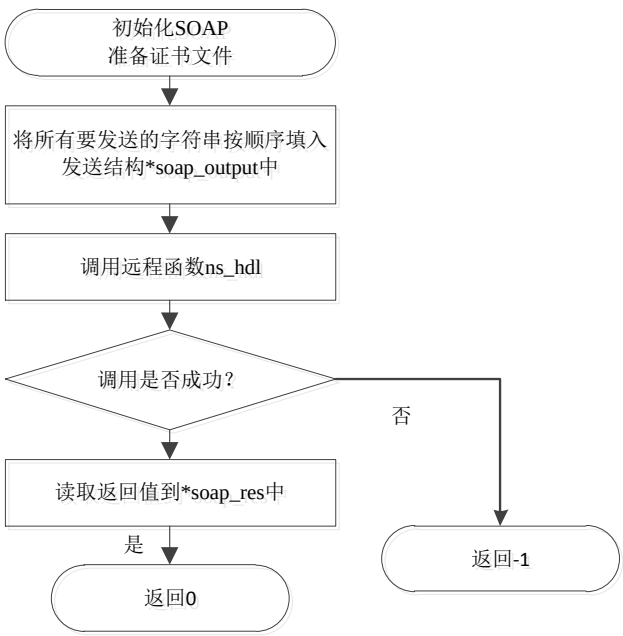

Fig.5 Client communication module flowchart

图 5 客户端通信模块流程

3.2 数据库模块

数据库模块负责管理数据库的访问操作。该模块以 ODBC（Open Database Connectivity，开放数据库互连）为核心，并通过配置文件的帮助，使数据库模块能够根据数据库信息和 VO 与 CI 管理模块给出的命令结合，动态生成 SQL 语句，从而实现服务模块与数据库信息的剥离，利于服务模块的组建以及今后对该系统的扩展。

数据库模块中只有三个操作：初始化、执行数据库命令、关闭 ODBC 连接，简化了服务器端的操作，这样大大减轻了虚拟组织管理模块的负担。

服务器端共有四个数据库表，UserInfo，保存 CI 中每个用户的信息；VOInfo，保存每个 VO 的信息，即 VO 登记表；Member，保存每个用户属于哪个 VO 的信息，即 VO 成员登记表；Message，保存消息信息。

3.3 VO 与 CI 管理模块

VO 与 CI 管理模块负责按照客户端发来的命令进行对应的 VO 和 CI 管理操作。VO 与 CI 管理模块从通信模块接收到用户发来的消息，服务器对内容进行分析后调用对应的函数进行处理。为了降低命令处理过程中客户端的负载，同时避免服务器端更新过程中也要更改客户端的麻烦，系统在命令处理过程中引入了表单机制。服务器端保存很多客户端可能用到的表单，客户端获取指定的表单后，用户根据表单上给出的规则生成一条命令，并将信息填入命令的对应位置发给服务器。

该系统在服务器端设定了严格的权限机制，每做一项数据库操作时，都需要检查用户是否具有相应的权限等级。各个角色所拥有的权限不能互通，权限设定如下：

- VO 创建者：解散 VO，批准成员，指定管理员、解职管理员、踢出成员（除自己）
- VO 管理员：批准成员、踢出成员（除创建者和管理员）、退出 VO
- VO 成员：退出 VO

在该模块中，我们提供了多个函数来完成用户加入 VO、退出 VO、查询 VO、查找 VO 中指定成员、创建取消虚拟组织等功能，具体函数设计这里不再一一陈述了。此外，本系统中为评价函数预留了一个评价接口，该接口作为 VO 管理模块中的一个私有函数存在，客户端不能直接访问该评价函数。评价接口具有访问数据库的权利，可以实现大多数的评价方法。

3.4 评价模块

该系统设计并实现了对用户和资源提供者进行评价的评价函数，客户端不能直接访问该函数。评价函数当用户或资源提供者提交加入请求的审批过程中调用，返回对指定用户或资源提供者的评价信息，具体函数的实现过程在本文中不再详细描述。

在该系统中为评价函数预留了一个评价接口。评价接口作为 VO 管理模块中的一个私有函数存在。该评价接口具有访问数据库的权力，可以实现大多数的评价方法。

3.5 客户端模块

系统中客户端由配置文件模块、通信模块和用户界面模块组成。客户端模块承担了与客户的交互工作，包括整理用户命令向通信模块发送命令，以及将服务器的信息显示出来。为了与 Globus 进行连接，客户端还需要负责根据服务器端报告的 VO 成员变动修改对应的 grid-mapfile。

本系统中提供了命令行版的简单客户端形式和网页版的复杂客户端形式。命令行版客户端循环接收并发送用户给出的命令，服务器端返回后，客户端对服务器端的信息进行解析，并以用户友好的方式显示出来，如图 6 所示。

```
grrr@grrr-desktop:~/www/Terminal$ ./terminal2 Bob wangz

>ShowRequest LIGO
Requests

commonName      Alice
Status          Submitted
AdditionalInfo  LIGO scientist

>Approve LIGO Alice
Your CommonName:Bob
Send?[Y/N]:y
Message
Confirmed

>
```

Fig.6 User interface of command-line client

图 6 命令行客户端的用户界面

网页版客户端通过 PHP 实现，命令转化为超链接的形式，在用户点击对应位置时向服务器发送命令，服务器返回的信息解析成 HTML 格式显示出来，网页版客户端使用界面如图 7 所示。

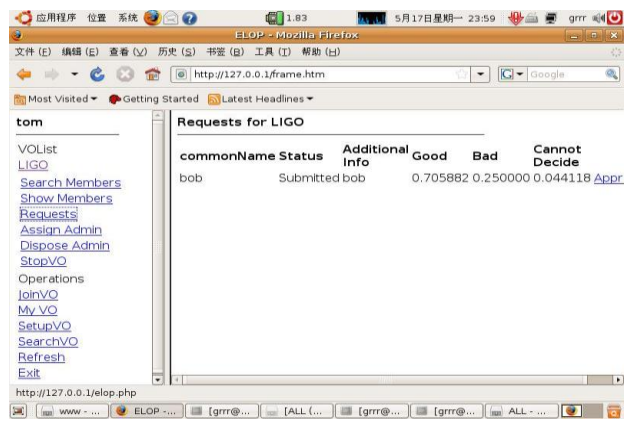

Fig.7 User interface of web-version client

图 7 网页版客户端使用界面

4 动态虚拟组织管理系统与 Globus 的协作

虚拟组织管理中，比较典型的组织管理应用可以分为 1. 查找虚拟组织；2. 建立虚拟组织；3. 加入/退出虚拟组织；4. 利用评价系统帮助虚拟组织管理员审核申请人；5. 踢出不安全的虚拟组织成员；6. 在实际应用结束后终止虚拟组织。

我们在安装并配置了动态虚拟组织管理系统

与 Globus 的计算机上，通过启用 grid-mapfile-add 和 grid-mapfile-delete 命令对 Globus 的 grid-mapfile 进行修改，实现该系统与 Globus 的连接，测试该系统在 Globus 平台上可以进行细粒度的访问控制。测试中我们使用四台计算机进行动态虚拟组织管理系统与 Globus 的协作测试。这四台计算机的 ip 地址分别是 166.111.137.17（grrr）、166.111.137.18（jinchun）、166.111.137.19（hanqiu）和 166.111.137.170（ligo）。其中 166.111.137.17 是 VO 与 CI 服务器，其余三台计算机上运行客户端。客户端计算机上的用户有各自的 Gloubs 证书用于 Globus 身份识别以及与服务器的安全通信与身份验证，证书分别为 bob、tom 和 alice，我们使用 SSH 工具连接到这四台计算机上并进行操作。

首先 tom 创建一个 VO，名为 LIGO。tom 在本地打开帐户 tom 供 VO 中的其它成员通过 Globus 进行访问。随后，bob 和 alice 加入 LIGO，并各自打开帐户 bob 和 alice 供虚拟组织成员进行访问。tom 根据评价系统给出的评价值批准二者的加入请求，如图 8 所示。在批准加入后，客户端根据收到服务器发送的 VO 成员变化信息执行 grid-mapfile-add 或 grid-mapfile-delete 命令，bob 和 alice 分别加入对方到自己本地的映射，二者之间可以互相访问。

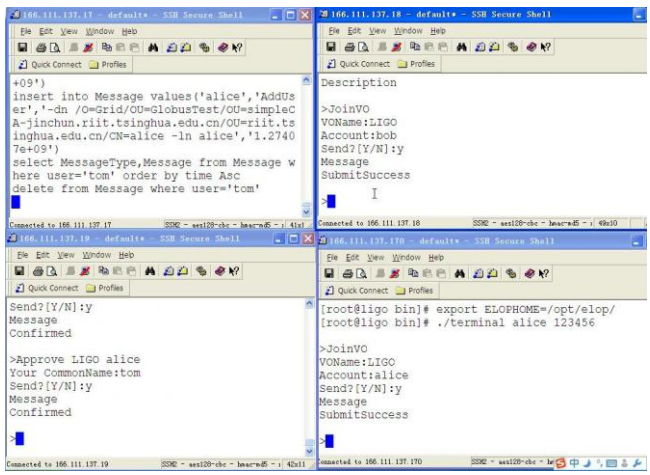

Fig.8 bob and alice join LIGO

图 8 bob 和 alice 加入 LIGO

alice 使用 Globus 执行 bob 计算机（jinchun）上的/bin/date 命令显示当前时间。命令成功返回正确的结果，如图 9 所示。说明该动态虚拟组织管理系统成功地修改了 grid-mapfile，实现了与 Globus 的对接。

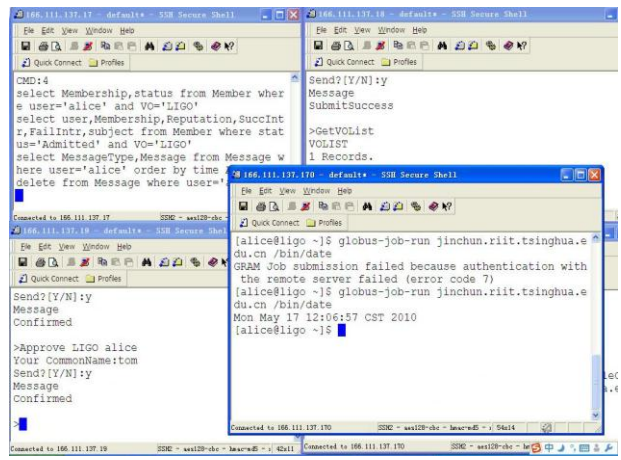

Fig.9 alice access the program of bob's computer

图 9 alice 访问 bob 计算机上的程序

接下来，VO 的创建者 tom 通过评价系统认为 alice 的评价值过低，而将 alice 踢出 VO。随后，alice 再通过 Globus 的 globus-job-run 命令执行 bob 计算机上的/bin/date 命令时，出现了错误 7，表示身份认证失败。这个错误当 grid-mapfile 中没有 alice 的映射条目时才会出现。这说明动态虚拟组织管理系统成功地使用 grid-mafile-delete 将 alice 从 bob 的访问映射表中移除。

之后 alice 再次加入虚拟组织 LIGO，随后项目结束，tom 通过 StopVO 命令解散了该虚拟组织。虚拟组织关闭后，alice 和 bob 之间都不能够通过 Globus 相互访问（错误 7），如图 10 所示。

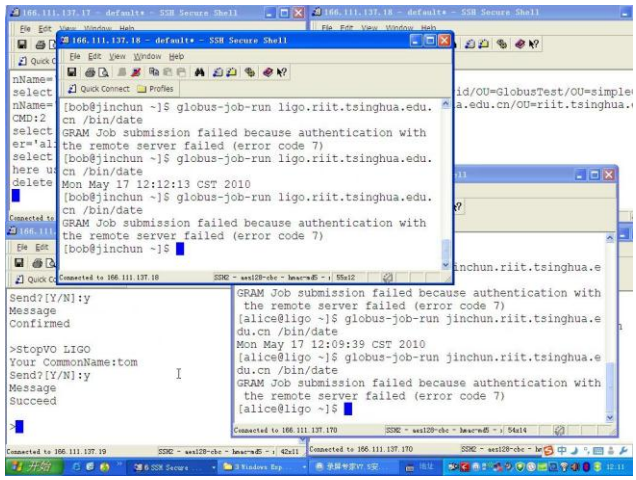

Fig.10 bob and alice can't access each other after tom closed the virtual organization

图 10 tom 关闭虚拟组织，bob 和 alice 不能相互访问

整个过程直观地说明了动态虚拟组织管理系统与 Globus 的协作流程。虚拟组织内部的成员能够访问虚拟组织内部的资源，而虚拟组织外的用户不能访问虚拟组织内的资源。通过对加入与退出虚拟组织的控制，该系统可以根据网格项目目标以及评价值调整用户和资源提供者的访问权限，达到了细粒度网格权限管理的目标。该动态虚拟组织管理系统成功地完成了 Globus 网格中访问控制与权限管理的相关功能，说明动态虚拟组织管理的方案是切实有效的。

4 总结

本文针对网格粗粒度管理僵化的问题，提出了解决该问题的动态虚拟组织管理方案。该方案按照虚拟组织的方式管理网格计算项目，按照虚拟组织成员关系控制用户访问的权限。对于该动态虚拟组织的管理方案，本文提出了一个能够实现该方案的客户端-VO 服务器-CI 服务器框架。基于该框架，设计并实现了动态虚拟组织管理系统。该系统是针对 Globus 网格平台进行设计的网格中间件，通过根据虚拟组织成员变化动态修改 grid-mapfile，控制用户的访问。该系统与 Globus 的结合实现了 Globus 平台上细粒度的访问控制，达到了用动态虚拟组织的管理方式管理网格计算的目的。实际应用表明该系统实现了细粒度的网格项目管理，证明了动态虚拟组织管理方案的有效性。

虚拟组织的研究虽然已经有很多年，但更大的范围内动态的创建、管理和运行多个虚拟组织，同时支持网格计算资源共享的功能，还是近年来才提出的需求。清华大学与美国 LIGO 和 Open Science Grid 项目都建立了长期的合作关系。未来会基于这些项目提供的全球的计算资源和合作伙伴，真正实现动态虚拟组织系统的实际运用。

References

[1] The Grid: A New Infrastructure For 21st Century Science. I. Foster. Physics Today, 55(2):42-47, 2002.

[2] I. Foster, C. Kesselman, S. Tuecke. The Anatomy Of The Grid: Enabling Scalable Virtual Organizations. International J. Supercomputer Applications, 15(3), 2001.

[3] Cao J. (Ed.), Cyberinfrastructure Technologies And Applications. Nova Science Publishers, 2009.

[4] 曹军威。赛百平台及其技术挑战[J].国际学术动态，2010,(2):38-42.
Cao Junwei..Platform And Technical Challenge Of Cyberinfrastructure[J]. International Academic Development, 2010,(2):38-42.

[5] Foster I. Globus Toolkit Version 4: Software For Service Oriented Systems[J]. Journal of Computer Science and Technology, 2006, 21(4):513-520.

[6] 孙为群,单保华,张程,等.一种基于角色代理的服务网格虚拟组织访问控制模型[J].计算机学报, 2006, 29(7): 1199-1208.
Sun Weiqun,Shan Baohua,Zhang cheng,et al.A Role-based Selegation Access Control Model For Virtual Organization In Service Grid[J].Chinese Journal Of Computers, 2006,29(7):1199-1208.

[7] Wang Zhen, Cao Junwei. Committee-based Evaluation And Selection Of Grid Resources For QoS Improvement[C]// Proceeding of the 10th IEEE/ACM International Conference on Grid Computing, Banff, Alberta, Canada, 2009: 138-144.

[8] Cao Junwei, Wang Zhen, VOMES: A Virtual Organization Membership Evaluation System[J]. International Journal on Networking and Virtual Organizations, 10(1): 88-108 (2012)

Cai Shixia was born in 1980. She received M.S. degree in computer software and theory from Nankai University in 2004. She is a research engineer of Research Institute of Information Technology, Tsinghua University, Beijing, China. Her research interests include database and cloud computing, etc.

蔡世霞(1980-)，女，河北吴桥人，2004 年于南开大学计算机软件与理论专业获得硕士学位，现为清华大学信息技术研究院工程师，主要研究领域为数据库，云计算等。

Cao Junwei was born in 1973. He received the Ph.D. degree in computer science from University of Warwick, UK in 2001.He is currently a Professor and Deputy Director of Research Institute of Information Technology, Tsinghua University, China. He is also Director of Common Platform & Technology Division, Tsinghua National Laboratory for Information Science and Technology. His research interests include distributed computing and applications. He has published over 130 academic papers and books.

曹军威(1973-)，男，河北乐亭人，2001 年于英国华威大学计算机科学系获得博士学位，现为清华大学信息技术研究院研究员，院务委员会副主任，清华信息科学与技术国家实验室公共平台与技术部主任，主要研究领域为分布式计算及应用，发表论文 130 余篇。

Lin Xiao was born in 1988. He is an undergraduate student at Department of Automation, Tsinghua University, Beijing, China. His research interests include virtual organization and grid computing.

林筱(1988-)，男，目前是清华大学自动化系本科生，主要研究领域为虚拟组织和网格计算。