网格门户平台权限模型的设计与实现①

Design and Implementation of Authority Management in Grid Portal Platform

段伟希 张宏海 迟学斌 (中国科学院 计算机网络信息中心 北京 100190)

摘 要： 根据网格门户平台功能模块多、业务流程多变、资源种类繁多、数据安全性要求高的特点，提出了一种综合访问控制模型。该模型以 RBAC、TBAC 模型为基础，同时有机地结合了工作流业务处理和网格环境资源访问的权限控制。利用该模型，设计了权限管理子系统，给出了系统中权限管理模块的具体设计和实现，解决了网格门户平台的访问控制问题。

关键词： 网格 权限管理 工作流 RBAC TBAC

1 引言

网格作为国家级高性能计算和信息服务的战略性基础设施，其目的是将分布异构的各种资源通过高速互联网络连接并集成起来，以实现统一的运维管理与资源调度，统一为用户提供服务，方便用户使用。用户可使用 Web 门户或者命令行等方式，访问网格环境内的所有资源，以符合不同层次、不同需求的用户的要求和使用习惯。目前，访问超级计算资源的方式还是以命令行为主，这样的访问方式存在对客户专业要求较高、对访问客户端限制严格、登录高性能计算机场所有限等缺点。一种相对更方便更快捷的方式是通过 web 门户的方式，提供一个访问资源的统一入口。这样不仅提供了更人性化更易操作的界面，降低了对用户的要求；也使得用户访问网格资源更加方便，只需要具备上网的条件即可；同时还可通过一个统一的入口来集中实施安全机制。使用 web 门户方式访问网格资源的一个关键问题就是权限控制。如何保证用户只能操作个人相关的任务、文件信息等？如何保证用户只能访问权限允许范围内的资源？如何在通过 web 服务器访问网格资源时进行身份验证？这些都是必须要解决的问题。

本文以实际开发的网格门户平台(ScGate)为背景，以 RBAC、TRBAC 等模型为基础，结合网格环境的安全机制，提出了一个综合的权限控制模型，很好地解决了 web 方式访问网格资源的安全需求。

2 系统介绍

网格门户平台的运行环境如图 1 所示。普通用户和管理员以 web 的方式通过门户 portal 访问本系统，系统通过网格系统中间件，以 CA 认证作为身份验证机制，与后台网格服务器进行交互。

图 1 平台应用环境

网格门户平台基于 B/S 模式，采用经典的 J2EE 多层架构实现。从高到低依次为用户接口层、应用服务层、对象关系映射层、公共类库层和数据库层。其中应用服务层是系统的核心，实现了系统所需的全部业务。该层总共可分为 10 个子系统，每个子系统下面又有 5-8 个功能模块。超算中心客户将使用本系统来进行网格账号申请、作业提交、问题提交、信息查

① 基金项目:中国科学院计算机网络信息中心青年基金(CNIC)(O814091103)
收稿时间:2008-11-27

询等；超算中心员工则将使用本系统来审批客户账号申请、解决技术问题以及日常办公等。超算中心内部各组织机构有着严格的职责和分工。不同部门有着不同的权力，同一部门内部不同职位的人员也有着不同的权力，同一职位的人员在不同的任务上下文中也对应着不同的权力。

本系统除了需考虑 URL、菜单、按钮等一般资源的访问控制外，还需要额外注意网格资源和工作流子系统的访问控制。因此，在设计权限管理子系统时，除了要满足对各种不同资源进行访问控制的要求外，还应该能够有效地将不同资源的权限控制整合起来，便于管理员进行统一的权限管理。为此，设计了一种综合的访问控制模型，用以解决系统中复杂的权限管理问题。

3　综合访问控制模型

由上文可知，系统中共有以下 3 类客体需要进行访问控制：(1)网格环境的资源实例；(2)工作流中的任务实例；(3)菜单、模块、文件等。为了有效控制用户对这 3 类客体进行访问，本系统以基于角色的访问控制模型以及基于任务实例的访问控制模型为基础，结合网格安全认证机制，形成了新的访问控制模型。

3.1 网格资源的权限控制

在本系统中，网格环境采用的安全机制为目前应用比较广泛的 CA 认证机制，其结构图可见上一节图 X。网格前端机服务器作为网格节点的代理与 CA 服务器进行交互，为用户生成证书以及验证证书的有效性。任何对网格资源的访问都以证书作为唯一的身份标识。

网格节点上的每一用户通过证书服务器生成对应的 CA 证书，以后每次访问网格节点时需要先提交此 CA 证书进行身份校验，然后根据 CA 证书的权限信息，访问自身的作业信息及权限许可内的其它网格资源。

本系统作为用户访问网格资源的统一入口，必须对访问网格资源的用户进行身份验证，并与后台网格环境的认证机制集成起来，提供用户透明的且安全可靠的权限控制机制。根据前面描述的网格环境的认证机制，后台访问网格资源时需要用户唯一对应的证书，这一证书是在创建网格用户时生成的。因此，可以将 CA 证书服务器为用户生成的证书保留至 web 系统服务器，并记录于数据库中。同时保存的还有前台用户和网格用户之间的对应关系。当用户需要访问网格资源时，系统根据对应关系获取到对应的网格用户，进而获取到该网格用户的 CA 证书。服务器自动将此证书随同访问请求一起发送至网格服务器。这样不仅保证了访问网格资源的安全性，同时也实现了对用户的透明性。一个典型的交互全过程的流程图，如图 2 所示：

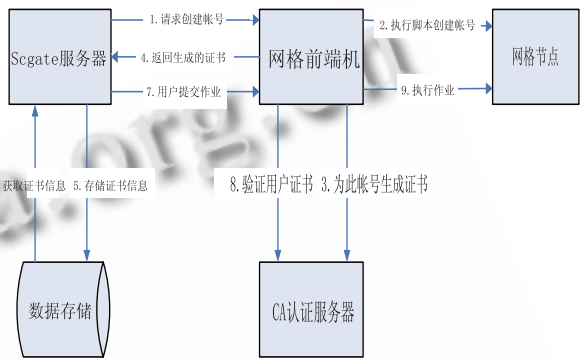

图 2　CA 认证流程

通过这种实现方案，有机地结合了网格环境和 web 系统之间的安全机制。

3.2 工作流中任务的权限控制

一个工作流的业务流程是由多个任务节点构成的，一个节点代表业务流转过程中的某种状态，一个节点上有多种可执行的动作，不同的动作转向不同的节点。工作流中不同节点对应不同的授权方案，权限是随着业务流程所处的上下文而相应变化的。节点的授权方案有两种方式，一种是基于模板的静态授权；另一种基于实例的动态授权。前一种方式是先定义好业务流程模板，然后将角色、部门或者用户的授权信息直接绑定到模板的每一个节点上。在实例化一个流程后，则可以根据模板定义的规则以及每一步所绑定的授权信息，直接在用户之间进行传递。这种授权方式对于流转过程比较简单以及业务处理人员相对比较固定的流程能够很好的工作；基于实例的动态授权方式则提供更加细粒度的控制，它用于对业务流程的不同实例需要进行不同的权限控制，以及在实例的流转过程中后面步骤的处理人员需要依赖前面步骤的处理结果的情况。下面以本系统中一个典型的技术支持流程为例来说明下基于实例的动态授权方式。一个典型的技术支持流程图，如图 3 所示：

图 3 技术支持流程

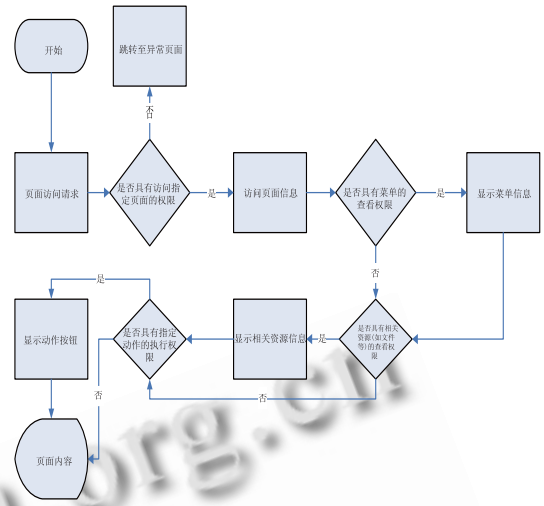

图 4 权限控制流程

在这个流程中，case 负责人的确立是在前一节点提交 case 时动态确定的；case 解决人的确立也是由分配 case 节点动态确定的。并且 case 解决人确立以后，在这个 case 流程中具有持续性，以后 case 流转到这一节点时都是由同一用户或者角色来进行处理，并不需要重新指定。

本系统采用了将两种授权方案相结合的方案。对于相对较简单且固定的业务流程，如公文发布、作业提交等，以静态授权为主、动态授权为辅；而对于流程复杂、周转时间较长、涉及人员较多、安全需求较高的业务，如账号审批、技术支持等，则以动态授权为主，静态授权为辅。因此，某用户在业务流程实例中所具有的权限即为：流程实例所属流程模板中静态定义的权限和在流程实例所有节点中动态分配的权限的并集。

3.3 菜单、模块的权限控制

本系统中，根据用户的类别、角色和所处的岗位不同而设置了不同的功能权限。任一用户只能够访问到他权限集合内的资源。这些资源在系统中表示出来包括菜单、按钮、文件、模块等。用户在访问系统任一页面时，首先会判断用户是否有访问此模块(也即 URL)的权限；在加载页面内容时，根据用户的菜单权限信息生成其特有的菜单选项以及用户的按钮权限信息来显示所能进行的操作；如果访问的是文件信息的话，则根据文件权限信息显示用户所能够下载和编辑的文件。整个权限控制的流程图如图 4 所示：

本系统以基于角色的权限管理为基础，结合超级计算中心的组织机构设置，实现了这一类型客体的权限控制。系统中引入了用户(包括客户和员工)、用户组(包括部门和专家组两种类型)、角色、权限单元、资源、操作的概念，以权限单元为基本，角色为核心来进行权限的设置和分配。资源表示的是上述提到的菜单、模块、文件等客体，而操作则是能够在客体上执行的动作，一个权限单元是资源以及在其上的操作的组合。权限单元是一个扁平结构，任何两个权限单元处于平行结构。角色是一系列权限单元的组合，角色本身是一个等级结构，可以是一系列下层角色的组合。用户组是一系列在某方面具有相同功能职责的用户的组合，这一概念是征对超级计算中心的组织方式和业务需求扩展而来的。超算中心内部有两种平行的组织结构，一种是按照实际的部门划分，每一个部门有一个经理，一个用户只属于一个部门，一个部门负责管理某一方面的业务，如客服部负责用户申请的处理等；另一种方式是按照虚拟的专家组划分，每一个专家组有一个组长，一个用户可以属于多个专家组，一个专家组负责指定领域的技术支持服务。因此，添加一个用户组到角色的对应关系，作为本组的基本角色，任何一个加入到本组中的用户都自动拥有了组角色，如给图像处理组添加文件服务器下对图像处理文件进行操作的角色等。又因为一个用户可能属于多个专家组，通过设立用户组，很大程度上减少了为单个用户分配权限的复杂性。用户即系统的使

用人员，每个用户可以拥有多个角色，通过分配不同角色进行权限控制。一个用户所拥有的所有权限为：用户本身所有的最底层角色对应的权限信息与用户所在用户组所有的最底层角色对应的权限信息的并集。

4　系统设计与实现

本文使用上一节描述的对 3 种资源进行权限控制的机制，并有机地将这些机制结合起来，形成了系统的权限控制模型。

4.1 权限子系统实体关系

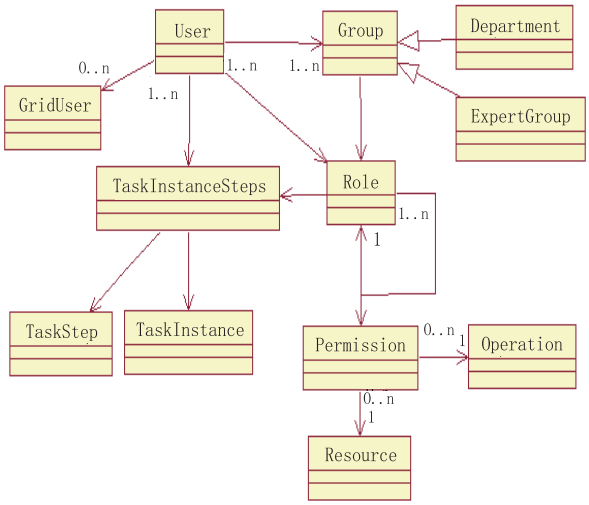

图 5　权限子系统实体关系

如图 5 所示，User 实体、Group 实体、Role 实体、Permission 实体、Operation 实体和 Resource 实体是整个权限控制模型的主体。User 实体和 GridUser 实体用于网格资源的权限控制。GridUser 实体表示网格账号信息，通过与 User 实体进行关联实现系统账号和网格账号之间的映射。User 实体、TaskInstanceSteps 实体、TaskStep 实体和 TaskInstance 实体用于工作流子系统的权限控制。TaskInstanceSteps 实体表示具体业务流程实例中的一个处理步骤，它和 User 实体以及 Role 实体相关联，用于指定 User 和 Role 拥有处理权限的所有步骤，进而实现基于实例的动态权限控制。

4.2 权限子系统实体关系

为了实现上一节描述的权限管理模块，创建了如下的数据库表：

表 1　数据库表

表名	列信息
用户表 User	用户 ID、密码、用户状态
用户组表 Group	组 ID、组名称、组描述、角色 ID
用户组和用户关系表 GroupUsers	用户 ID、组 ID
角色表 Role	角色 ID、角色名称、角色状态、角色等级
用户角色分配表 UserRoles	角色 ID、用户 ID
权限表 Permissions	权限 ID、权限名称、权限状态、资源 ID、操作 ID
角色权限分配表 RolePermissions	角色 ID、权限 ID
资源信息表 Resource	资源 ID、资源名称、资源类型、资源实例、资源状态
资源操作表 Operation	操作 ID、操作名称、操作状态
网格用户信息表 GridUser	网格用户 ID、网格用户证书、状态
用户映射表 UserMapping	用户 ID、网格用户 ID
任务实例步骤表 TaskInstanceStep	实例步骤 ID、步骤 ID、任务实例 ID
任务实例步骤用户分配表 UserSteps	实例步骤 ID、用户 ID
任务实例步骤角色分配表 RoleSteps	实例步骤 ID、角色 ID

4.3 功能模块设计

整个权限控制子系统包括了如下几个子模块：用户管理、用户组管理、权限单元管理、角色权限分配、用户角色分配、用户组角色分配、工作流权限管理。各模块的功能如下：

(1) 用户管理：该模块提供增删查改用户信息的功能。管理员能够对所有用户信息进行管理，普通用户则只能够管理自己的信息。

(2) 用户组管理：该模块提供了对部门和专家组信息的增删查改，以及用户组中用户信息的分配。

(3) 权限单元管理：该模块提供了管理基本权限单元的功能，同时包括了对权限单元所需的“资源+操作”进行管理的功能。本系统中，资源分成了按钮、菜单、文件、模块等；操作分成了添加、查看、编辑、访问等。

(4) 角色权限分配：该模块的功能是管理角色信息，为角色分配其所拥有的权限信息。角色和权限之间是多对多的关系。同时角色是有等级结构的，可以为角色分配其下层角色信息。上层角色所拥有的权限信息为所有底层角色权限信息的并集。

(下转第 46 页)

(上接第 22 页)

(5) 用户角色分配：该模块的功能为用户分配其所拥有的角色信息。用户和角色之间是多对多的关系。

(6) 用户组角色分配：该模块的功能为用户组分配其所拥有的角色信息。一个用户组最多只能够对应于一个角色信息。用户组中的用户自动获取用户组的角色信息。

(7) 工作流权限管理：该模块提供了定义工作流模板并将静态权限绑定到流程步骤上的功能；同时也能够根据需要征对工作流任务实例动态分配权限。工作流程被实例化(即新建任务)后，会根据定义好的流程模板自动进行流转。

5 结束语

本文提出的权限管理模型很好地解决了网格门户系统中多样的权限管理问题。该系统具有良好的安全性、灵活性和扩展性，在实际应用中达到了应有的效果，可供其他系统权限管理模块参考。

参考文献

1 王子仁,陆亿红.RBAC 在信息系统中的应用研究.计算机应用, 2007,27(6):240－241.

2 龚富强.基于角色的用户权限管理系统开发与应用[硕士学位论文].西安:西北工业大学, 2007.

3 Sandhu R, Coyne E, Feinstein H, Youman C. Role-Based Access Control Models. IEEE Computer, 1996, 29(2):38－47.

4 Thomas RK, Sandhu RS. Task-based Authorization Controls. Proceddings of the IFIP WG11.3 Workshop on Database Security, Lake Tahoe, California, August 1997:11－13.

5 Wu SL, Sheth A, Miller J, Luo ZW. Authorization and Access Control of Application Data in Workflow Systems. Journal of Intelligent Information Systems, Kluwer Academic Publicshers, January 2002,18(1):71－94.