第32卷 第20期 计 算 机 工 程 2006年10月
Vol.32 № 20 Computer Engineering October 2006
·网络与通信· 文章编号：1000—3428(2006)20—0132—03 文献标识码：A 中图分类号：TP311.52

DACS:网格数据服务访问控制的设计与实现

吴 勇，张 武
(上海大学计算机工程与科学学院，上海 200072)

摘 要：网格中大量用户共享不同组织提供的资源。传统的网格授权控制方式已无法适应具有大量用户的模式。该文在实际需求下建立了一个轻量级访问控制服务DACS。DACS将VO用户划分为不同的等级，资源只需对VO用户按级别进行整体授权。
关键词：网格安全；授权；数据访问控制服务

DACS: Design and Implementation of Access Control for Grid Data Service

WU Yong, ZHANG Wu
(School of Computer Engineering and Science, Shanghai University, Shanghai 200072)

【Abstract】 Grid is composed of several thousands of users from different organizations sharing their resources. Controlling access to these resources is a difficult problem and traditional access authorization is not applicable to a large scale environment. This paper describes a lightweight authorization service developed to solve this problem in the project requirements: data access control service (DACS). DACS divide VO users into different levels and resources only maintain access control policies to all users in same level as a whole.
【Key words】 Grid security; Authorization; Data access control service (DACS)

在任何网络环境中，安全性都是一个非常重要的问题。在网格环境中，客户机可以位于不同的地理空间和组织中，因此，在网格应用系统中，身份鉴别和授权在获取资源访问的过程中起着关键作用。然而设计网格应用程序时经常会碰到这样一个问题，随着网格中机器数目的增长，在高度动态的分布式环境中，管理安全性与访问控制列表变得越来越困难。本文主要描述采用网格技术和OGSA-DAI[1]实现“基于网格的多系统公共信息数据交换平台”(简称“数据交换平台”)时开发的一个数据访问控制服务(DACS)的架构与设计。DACS采用对用户进行分级管理的方法来控制对DAI数据服务的授权。

1 GSI

GSI是Globus Tookit（GT）提供的标准的网格安全基础设施。GSI所有的功能都是基于公钥加密体系。GSI使用了X.509证书[2]来建立持久性的实体身份，例如用户和资源。它引入了代理证书[2]的概念，可以支持委托，并为临时和短期存在的实体建立身份。DACS的实现完全基于GSI，代理证书和委托是DACS实现的主要技术基础。

1.1 代理证书

代理证书类似于标准的X.509证书。与X.509证书的长期性不同，代理证书是由用户签发的，用来在短期内委托授权给其他实体。用户首先生成一对新的临时公私密钥，然后生成一个用自己的用户证书的私钥签署的新证书，以此将用户的身份和新生成的密钥对建立起一个短期的绑定。在使用代理证书进行身份认证时，使用者要同时出示代理证书和本身的用户证书。验证方先验证使用者的用户证书的有效性(用户证书的私钥用来签署代理证书)，使用者证明自己拥有代理证书的私钥。所有这些条件符合则身份认证通过，使用者被认为是用户证书的那个身份。

1.2 委托

在分布式应用中，一个用户程序能够在用户不参与的情况下代表用户身份进行操作也是非常重要的。GSI是通过创建用户代理证书来实现委托授权的。GSI允许使用者委托一个代理证书给远程主机上的进程，授予一个进程代表自己身份的权利，以便该进程能够访问用户被授权的资源。另外，如果需要的话，该程序也可以进一步委托另一个程序。

1.3 GSI授权机制

GSI支持本地策略本地控制的概念。鉴别了使用者的身份后，通过本地配置文件(grid-mapfile)将用户身份映射到一个本地身份（如Unix用户、数据库用户）。这个配置文件同时起着访问控制的作用：如果用户没有在本地配置文件的用户列表中，那么他将被拒绝访问资源。一旦用户被映射到一个本地身份，GT将完全依赖于本地操作系统或者应用系统的策略管理机制，并确保用户的行为是本地策略所允许的。

2 实际需求及相关工作

OGSA-DAI是DAIS（数据存取和集成标准）规范的一个参考实现，它在OGSA的框架上提供了一个数据集成的解决方案。OGSA-DAI的目的就是通过网格环境来提供统一的数据集成和存取的服务接口。

OGSA-DAI的安全机制基于GSI，通过角色映射文件(RoleMap，类似于GT中的gridmap-file)将网格用户凭证的身份映射至一个本地数据库用户实现对数据库的访问授权。这

作者简介：吴 勇(1978－)，男，硕士生，主研方向：网格计算，网格安全；张 武，博士、教授、博导
收稿日期：2006-01-09 **E-mail：**wuyong@graduate.shu.edu.cn

种授权方式对于参与组织少、用户数小的小规模应用是可以满足需要的。然而，在实际的网格应用中，比如采用OGSA-DAI正在建设的数据交换平台，系统中共享的DAI数据服务由跨多个管理域的不同部门、不同系统提供，而数据服务的使用者又极其众多且具有极强的动态性。在这种环境下，目前这种由DAI数据服务提供者不断地修改更新RoleMap文件的方式来对每个网格用户进行服务授权控制的方法是一个及其繁琐和低效率的解决方案。

目前，在解决网格的授权控制问题方面较为著名的项目有Globus组织的社区授权服务(Community Authorization Service,CAS)[3,4]和欧洲的虚拟组织成员服务(Virtual Organization Member Service,VOMS)[5]项目。这两种解决方案都是通过虚拟组织(VO)内的CAS或VOMS服务在用户的代理证书中插入一些额外的策略声明，并由服务提供者解析这些策略并决定是否允许用户访问资源。它们的主要不同在于操作的授权级别不同，CAS的策略声明直接包含了权限，并不需要由资源提供者来解释权限；而VOMS的策略声明包含一个角色或组成员的列表，用户将这个组关系策略声明发送给资源提供者，由资源提供者基于本地的组策略来授予用户权限。从效果上看，VOMS用户的成员属性是集中在VOMS Server控制，但是对于这些成员具体的权限的策略则是分布在不同节点。而CAS策略由VO的CAS Server直接提供用户权限，而不要资源进行任何解释。

CAS和VOMS这两种授权机制都提供了细粒度的访问控制解决方案。然而这两种方案具体实施时都需要服务提供者能够解析它们提供的策略声明，对于不能解析其策略声明的服务将采用默认的GSI的身份映射机制。也就是说，要使用这两种解决方案，服务提供者必须对其服务的授权控制方面进行修改以便能够解析它们提供的策略声明。这对于很多已经部署的网格服务或使用第三方系统集成的网格应用来说显然是一个不可能的任务。

3 DACS系统及其实现

基于数据交换平台对数据服务访问控制的需求以及现有中间件系统(CAS,VOMS)的相对局限性，我们设计并实现了一个轻量级的访问控制服务——DACS，通过DACS服务将整个VO内部/外部的所有用户按照一定的策略划分为不同等级。DAI数据服务按照DACS提供的VO用户等级信息对该级别的用户进行整体授权，而不是以每个用户自身的身份来控制用户对数据库的访问。DACS没有采用在用户证书中添加策略的方式,而是通过证书委托的方式实现同一级别的VO用户在访问DAI数据服务时使用一个相同的身份证书（称之为DACS证书)。DACS证书采用标准的GSI代理证书格式，因此DAI服务只需将一个VO中不同级别的DACS证书映射到具体的本地数据库用户即可控制该类VO用户对其资源的访问。对于DAI服务提供者来说，原先一个VO中成千上万的用户一下子变成了仅有的拥有DACS证书的几个用户，大大简化身份映射的管理和维护。从效果上看DACS更像VOMS，而从设计实现上则类似于CAS的Alpha 1版本（一个VO所有用户使用同一个VO身份)。当然，DACS系统并不排斥用户采用自己的用户证书直接访问DAI数据服务。也就是说，如果DAI服务给予了某个用户一定的访问权限，那么这用户可以不需要通过DACS，而是使用自己的身份证书直接去访问服务。而对于那些没有被DAI服务直接赋予访问权限的用户，则需要先通过DACS获取一个DACS证书。由于DACS服务使用了标准的GSI代理证书，因此除了结合DAI使用外，也很容易推广到其他的网格应用中。

3.1 DACS系统组成

DACS系统共由5个功能模块组成(见图1)。

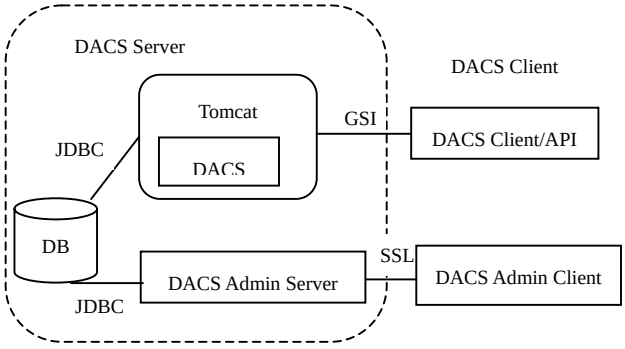

图1 DACS 系统组成

(1)DACS服务：DACS服务对外提供一个标准的GT3.2兼容的网格服务界面。它接受客户端的请求，从中提取出用户的身份证书，然后以用户证书的公钥生成一份与用户所属级别相符的DACS证书的代理，并将此返回给客户端。由于返回的代理证书是由DACS证书签署的，其密钥对使用了用户证书的密钥对，从而实现了用户证书和DACS证书的一个绑定关系，达到了将DACS身份委托给用户的作用。

(2)客户端工具：DACS系统提供一套命令行工具以及一套JAVA API供客户端同DACS交互。客户端提供用户的身份证书给DACS服务并取回相应的DACS证书，并设置该证书为访问DAI数据服务的临时身份。所有客户端同DACS服务间的交互都是基于GSI身份认证和安全通信机制。

(3)DACS管理客户端：数据交换平台/VO管理员用来进行一些日常的管理，如：添加/删除用户，添加/删除用户级别，修改用户级别，查询DACS相关信息等。

(4)DACS系统管理服务：接受管理客户端的请求并进行相应的数据库操作。

(5) DACS系统数据库：系统后台采用MySQL数据库存储用户、VO级别划分以及其他的一些数据信息。

3.2 DACS系统流程

3.2.1 DACS服务交互过程

在同用户交互部分，核心在于用户通过DACS服务取得DACS身份证书的交互过程。这个过程如下（见图2)。

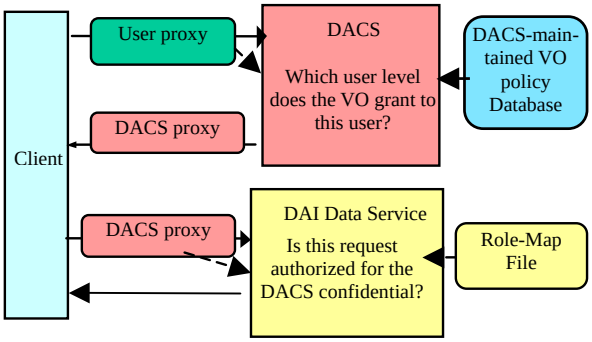

图2 DACS 系统交互过程

(1)用户和DACS服务使用他们的证书进行双方的身份认证；
(2)用户发送获取DACS证书的请求；
(3)DACS服务查询数据库系统，获取用户所属相应的级别的

DACS 证书；

(4)DACS 用取得的 DACS 证书生成一个代理证书，并将其委托给用户；

(5)用户以 DACS 证书的身份访问 DAI 数据服务；

(6)DAI 数据服务根据其 RoleMap 的配置对用户操作授权并提供服务。

3.2.2 用户接口

为了方便客户端操作和编程，我们提供了一套完整的客户端工具和 API。用户如果需要使用 DACS 提供 VO 级别角色来访问 DAI 数据服务，那么他应该遵循以下步骤。下面以命令行方式为例：

(1)grid-proxy-init
(2)get-dacs-cert
(3)……
(4)destory-dacs-cert
(5)……

首先如步骤(1)，用户在使用 DACS 服务之前首先要生成自己的代理证书。接着需要按步骤(2)取得一个 DACS 证书并将 DACS 证书作为临时的缺省用户身份证书，然后按照标准 OGSA-DAI 应用方式访问 DAI 服务；当不再使用 DACS 证书时按步骤(4)销毁 DACS 证书。

同样对于采用编程方式来实现访问 DAI 服务，我们也提供了标准的编程接口。下面的伪码表现了这个过程：

```
URL GSH=new URL(args);
GridProxyCertificate dacsCert=null;
        DACSServiceLocator Locator=
                    new DACSServiceLocator();
        DACSPortType dacs =
Locator.getDACSService(GSH);
        DACSHelper      dacsHelper =
new DACSHelper(dacs);
        dacsCert = dacsHelper.getDACSCert();
        ... (Normal OGSA-DAI operations)...
        dacsHelper.destroryDACSCert(dacsCert);
```

3.2.3 DACS 系统管理

系统管理模块主要负责 DACS 系统的数据库维护。该部分目前是一个基于 C/S 模式的数据库应用程序。DACS 系统管理服务监听一个服务端口并接受客户端的请求，然后根据请求进行相应的数据库操作。客户端同服务器之间也是采用 GSI 的身份认证机制进行身份验证，并且服务器还需要根据配置文件验证使用者是否拥有管理员权限，只有被许可的使用者才可进行相应的管理操作。目前系统支持以下几类操作：

(1)查询信息：查询 VO 所有级别信息，查询用户信息；

(2)修改信息：增加/删除 VO 级别，增加/删除用户，增加/删除/修改用户级别；

(3)数据备份：备份系统数据。

4 总结

作为“基于网格的多系统公共信息数据交换平台”的授权访问控制模块，DACS 系统采用了将 VO 的访问授权策略和 OGSA-DAI 数据服务的授权策略分开来考虑的方式。一个 VO 通过 DACS 服务按照内部策略对该组织中用户实现分级，而 OGSA-DAI 数据服务将一个 VO 中的某个等级的所有用户当作一个整体对其进行授权。由于 DACS 服务使用了标准的 GSI 代理证书，因此具有良好的扩展性并较容易推广到其他的网格应用中。然而作为一个轻量级的授权控制服务，DACS 尽管满足了一定的需求，但在很多方面考虑还不是很成熟，使其更具有扩展性和实用性是下一步工作的主要研究方向。

参考文献

1 Antonioletti M, Atkinson M, Baxter R, et al. The Design and Implementation of Grid Database Services in OGSA-DAI[J]. Concurrency and Computation: Practice and Experience, 2005, 17(2): 357-376.

2 Welch V, Foster I, Kesselman C, et al. X.509 Proxy Certificates for Dynamic Delegation[C]. Proc. of the 3rd Annual PKI R&D Workshop, 2004.

3 Pearlman L, Welch V, Forster I, et al. A Community Authorization Service for Group Collaboration[C]. Proceedings of the IEEE 3rd International Workshop on Policies for Distributed Systems and Networks, 2002.

4 Pearlman L, Kesselman C, Welch V, et al. The Community Authorization Service: Status and Future[C]. Proceedings of Computing in High Energy Physics'03, 2003.

5 Alfieri R, Cecchini R, Ciaschini V, et al. From Gridmap-file to VOMS: Managing Authorization in a Grid Environment[J]. Future Generation Computer System, 2005, 21(4).

(上接第 122 页)

生命周期管理中的大量软硬件设计将被逐步完成。将来，信息生命周期管理也可能会成为一种存储行业标准的名称，用以规范存储产品的设计、制造、测试、验收和运用。

6 结束语

本文概略地讨论和评价了网络存储领域 5 个新技术。这些新技术已经对网络存储产生了较大的推动力，但是它们还都不十分成熟，仍处于发展之中。鉴于其应用价值大，IT 业界人士应当进一步深入研究这些新技术。

参考文献

1 李佳师. 2005 年中国存储趋势大盘点[EB/OL]. 中国电子报, http://www.cena.com.cn/htm/Article_detail.asp?id=10534,2005-03-22.

2 Maitland J. EMC Limits Invista to Big Shops, [EB/OL], Search Storage.com, http://searchstorage.techtarget.com/originalContent/0,289142,sid5_gci1089063,00.html, 2005-05.

3 SearchStorage.com Staff. Storage Clips: NetApp Unveils Virtualization Appliance[EB/OL]. http://searchstorage.techtarget.com/original Content/2005-03-29.

4 RDDP Protocol [EB/OL]. http://www.ietf.org/internet-drafts/drafts-ietf-rddp-rdma-01.txt.

5 Brustoloni J. Interoperation of Copy Avoidance in Network and File I/O[C]. Proceedings of IEEE Infocom, 1999: 534–542.

6 Chase J S, Gallatin A J. End System Optimizations for High-speed TCP[J]. IEEE Communications, 2001, 39(4): 68-74.

7 李国杰. 国家智能计算机研究开发中心回顾[EB/OL]. http://www.ncic.ac.cn/road/road3_1.htm, 2002-09.

8 Derrington S. 为什么 SAN 和 NAS 将融为一体[EB/OL]. http://www.zdnet.com.cn/biztech, 2003-06.