

面向分布式系统集成的 Web 服务管理方案

吴 靖¹, 彭启瑞¹, 李 清¹, 刘永青²

(1 清华大学 自动化系, 北京 100084; 2 经纬纺织机械股份有限公司, 北京 100125)

摘 要: 针对我国企业目前普遍面临的分布式应用集成难题, 为解决 SOA 架构下 Web 服务资源共享管理和跨域访问安全控制的问题, 设计了一套完整的服务管理方案. 通过建立一种服务访问代理架构和全局认证授权机制, 以较低的成本确保了集成系统的安全性, 同时采用一种基于全局 ID 的服务注册发现和动态调用机制, 有效提高了 SOA 系统的敏捷性和松耦合性. 该方案在典型集团企业工程应用中展现了良好的适应性和实用价值.

关键词: 系统集成; 面向服务架构; 服务管理; 服务访问代理; 服务注册

中图分类号: TP315

文献标识码: A

文章编号: 1000-7180(2010)08-0004-05

Distributed System Integration-Oriented Web Service Management Method

WU Jing¹, PENG Qi-rui¹, LI Qing¹, LIU Yong-qing²

(1 Department of Automation, Tsinghua University, Beijing 100084, China;

2 Jingwei Textile Machinery Stock Co., Ltd, Beijing 100125, China)

Abstract: To overcome the universal challenge of distributed application integration for Chinese enterprise groups and solve the problem of shared management and cross-domain access control of the service resources under SOA, a whole web service management method is presented. By designing an infrastructure based on Service-Access-Agent and a global authentication and authorization mechanism, the security of the integrated system is ensured with low cost. Meanwhile, by using a registration service based on global unique ID and dynamic invocation mechanism, the agility and loose coupling of SOA are improved. The good adaptability and practical value of the method has been shown by engineering application in a typical group enterprise.

Key words: systems integration; SOA; service management; Service-Access-Agent; service registration

1 引言

基于 WS(Web Service)实现的 SOA, 具有松散耦合、互操作和开放性等特点, 为解决分布式异构系统集成提供了全新的模式和基础架构^[1].

目前我国企业的信息化现状大都呈现显著的分布式异构特征, 在 SOA 分布系统中, 所有具有业务能力的功能组件都以 WS 的形式部署和运行. 与传统的 WS 管理目标主要面向单个系统不同, 在分布

式环境中的应用集成, 跨系统的业务交互不可避免会通过互联网实现, 因此, 设计完善的安全控制策略以确保 WS 资源的安全可控也是服务管理功能的核心任务^[2-3].

基于此, 本文设计的 WS 管理方案(如图 1 所示), 采用了一种基于服务访问代理(SAA)的安全架构, 并围绕 SAA 设计了完整的服务注册发现、动态调用、认证授权机制和服务注册库结构, 实现了对分布式系统中的 WS 资源的共享管理和访问控制.

收稿日期: 2010-05-09; 修回日期: 2010-06-09

基金项目: 国家“八六三”计划项目(2007AA04Z1A6); 北京市自然科学基金项目(9072007); 清华大学亚洲研究中心 2010 年青年 C1 类资助项目

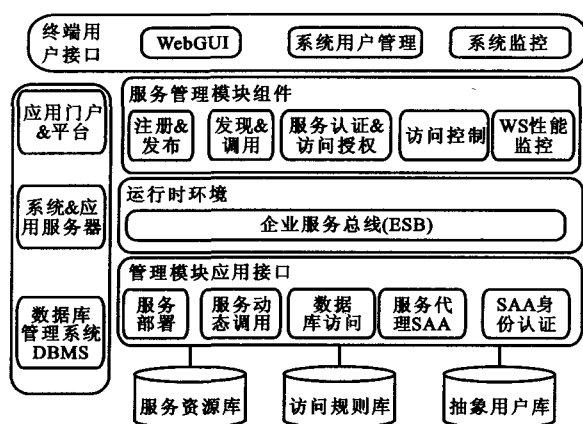


图1 WS管理方案总体设计

该方案针对的对象分为终端用户和WS资源两类。前者(包括系统管理员、服务开发者和服务用户等)主要是围绕中心数据库完成服务注册、信息维护、服务性能及质量监控等传统管理功能^[4],系统将为其提供相关的人机交互界面和应用接口。对于后者,控制策略会以约束规则的形式集成到其运行机制之中,当WS运行时会自动调用相关的功能组件而受到系统的保护。

2 基于代理机制的WS安全策略

2.1 基于代理的安全架构设计

分布系统间的应用集成安全性问题是企业关注的焦点,也是本方案要解决的核心问题。通常单个企业的信息系统结构上相对独立,安全功能完善,执行相同的WS策略,可视作一个“安全域”^[5]。但企业间的应用集成往往需要进行跨域交互,这一过程显然超出了原WS策略的控制范围,需要引入新的机制加以保护。目前业界对WS安全性的研究主要集中在两个方向:①利用新兴技术(如本体、语义技术等)在标准WS策略框架中引入控制因素,从规范制定的层面扩展安全控制功能^[6];②在消息层面实现服务保护,例如在SOAP消息中定义访问控制信号,基于XML的消息署名、加密技术等^[7]。前者目前尚处理论验证阶段,后者通常依赖具体的WS运行环境,解决方法容易就事论事,缺乏通用性。同时,由于WS资源数量众多,且随着企业业务需求的变化呈现极高的动态性,要实现对所有资源的一一控制也是极其困难的。

针对这一问题,本系统提出了一种服务访问代理架构和统一授权认证机制。整套方案根据WS资源的区域分布性,也采用了相应的分布式架构(如图2所示),由全局认证授权中心(GAAC)^[8]和各域的

服务访问代理(SAA)协同工作实现。GAAC包括服务信息模块、域间认证模块和访问授权模块。信息模块实现WS的注册信息维护;域间认证模块完成SAA间身份认证;访问授权模块用来对WS进行统一的访问授权控制。SAA对本域内的WS资源进行控制和管理。除了执行域内的WS身份认证功能外,作为域内WS资源对外的唯一通道,SAA还承担转发跨域交互(包括调用和被调用)请求和反馈WS运行结果的任务。

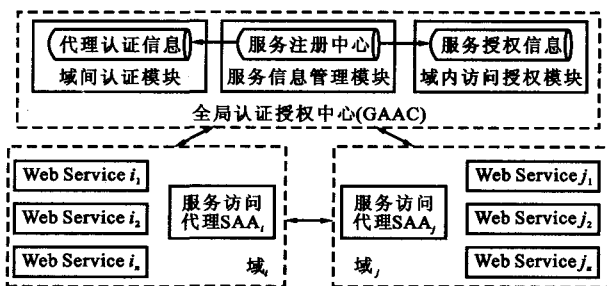


图2 基于SAA的服务访问控制原理

2.2 认证授权流程

由于SAA的引入,WS的跨域访问控制被分为三步实现,以图2中服务 i_k 跨域调用 j_l 为例。

(1) 域内认证:服务 i_k 首先将调用请求发送给SAA_i(该请求中应该包含 i_k 和 j_l 的身份信息),由SAA_i对该服务的身份进行认证,如果认证失败则调用过程终止,若成功则继续调用流程。

(2) 域间认证: SAA_i将访问GAAC对SAA_j的身份进行域间认证。域间认证采用双向认证,即源代理SAA_i和目标代理SAA_j同时被认证。认证失败则调用过程终止;若成功,则在代理间建立起一个安全信道支持数据加密传输,同时GAAC会继续进行访问授权验证等操作。

(3) 服务访问授权:当域内和域间认证成功之后,GAAC会查询服务授权列表判断 i_k 是否具有访问目标 j_l 的权限;如访问非法则终止调用;如合法则SAA_i通过(2)建立的安全信道将调用请求转发给SAA_j对目标 j_l 发起间接调用,最后 j_l 将响应原路反馈给 i_k 。

对于域内调用,由于源服务和目标服务处于同一个安全域,其调用过程控制更加容易。SAA能为域内调用提供简单身份认证,服务访问授权环节依然由SAA调用GAAC的授权模块实现。

2.3 安全策略的优点

本方案通过基于SAA的架构将众多WS跨域调用关系转换成几个SAA之间的交互关系,大大降

低了安全策略实现的复杂性.同时,基于 SAA 和 GAAC 实现的两级身份认证机制,将域内和域间认证独立开来,使得用户可以灵活地针对域内外两种不同的网络环境采用不同的身份认证策略,有利于简化配置工作、提高认证效率.当安全域内增加新 WS 资源时,只需在完成注册部署后进行简单的域内认证配置即可;而如果集成系统需要新增安全域,则只需要在新域内部署一套 SAA 并在 GAAC 中为完成相应的注册工作.因此,这套基于 SAA 的访问控制机制保证了系统的安全性,还具备较高的灵活性和可扩展性,能够适应企业应用动态集成的需求.

3 基于全局 ID 的服务注册机制

服务注册中心是任何一个 SOA 系统的核心架构,对 WS 资源的发现、调用,安全策略的实施等都是在此基础上实现的.在标准 WS 技术中,基于 UDDI 协议的服务注册机制受到普遍关注,应用广泛.但是,UDDI 作为主要面向公共领域的服务发现规范,不易与私有的安全管理策略集成,同时其复杂的结构和规则还会增加系统开发的负担,因此本文采用了私有架构来实现服务注册中心.如图 1 所示,注

册中心由三部分组成:①服务资源库存储 WS 资源信息,如服务描述、调用规范、WSDL 契约等;②访问规则库保存服务访问授权信息;③抽象用户库记录 SAA 注册信息及其与域内 WS 资源的映射关系.

基于上述注册库结构,本文设计了一套基于全局 ID 的服务注册机制:系统内每个 WS 资源与 SAA 都拥有全局唯一的 ID,对应其一组注册信息,服务调用过程中调用方只需掌握被调方的 ID 并动态地从注册中心获取其详细信息(如图 3 所示).与传统 UDDI 注册机制相比,本方案能够更好地支持服务动态调用过程,将调用双方有效地解耦,使系统表现出极大的松耦合性.例如由于 SAA 对其调用目标的不确定性,可以将每次调用目标服务的 ID 作为参数传递给它,由它自行获取调用参数完成调用过程,而不必在其实现代码中紧密绑定其所有可能的访问目标;又或者由于某服务器迁移导致其上的服务要更改部署信息,也只需要更新服务的注册信息(ID 不变),无需改动调用它的上级流程服务或 SAA.这种基于服务注册和动态调用机制既支持了系统安全策略的实现,又显著提高了系统的可维护性和 SOA 中流程编排功能的敏捷性.

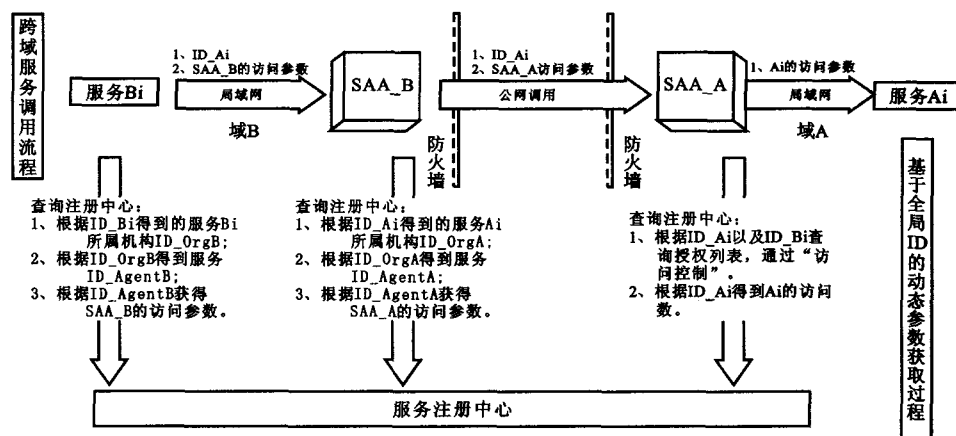


图3 基于全局 ID 的服务动态调用过程

4 关键技术研究实现

4.1 系统应用门户 Portal

Portal 为终端用户提供操作界面和应用接口.本系统中 Portal 采用了 B/S 的架构,服务器部署在分布式架构的中心节点处,用户直接通过浏览器访问 Portal 完成管理工作.

Portal 的实现采用了网站开发领域经典的三层架构.①表现层:采用 JSP、Servlet 等动态网页技术开发 Web 界面.②业务层:通过封装 JDBC 与数据

访问逻辑实现与数据层的操作接口,采用 JavaBean 和 JavaScript 等技术实现所需的业务逻辑处理并向表现层提交结果.③数据层:借助 DBMS 完成底层的数据存储与维护功能.

4.2 服务访问代理 SAA

SAA 是各安全域内所有 WS 资源运行的总代理,集成了域内身份认证、消息处理和服务调用的功能.其中,域内认证部分可以在开发阶段将约定的规则通过编程直接固化在其处理逻辑中;消息处理模块由 Module_I 和 Module_O 两部分组成:前者负

责接收来访的服务调用请求,并经认证后进行处理和转发;后者功能则与之相反。

在服务调用方面,由于调用发生前SAA对目标WS及其传递参数等都不确定,需要在调用进行时对其访问接口和数据包进行动态获取和解算,这与普通的WS调用方式有很大不同。J2EE为工程开发人员了提供各种用于构建WS的API,其中JAX-RPC利用SOAP进行远程方法调用,并定义了3种标准WS调用模型:静态存根(Static Stub)、动态代理(Dynamic Proxy)和动态调用接口(Dynamic Invocation Interface)。静态存根模型最简单常用,但需要在开发阶段就通过映射工具构建客户端,生成静态代理,才能利用客户端来调用远程服务。动态代理模型是最常见的动态连接方法,该方法需要针对特定的WS接口定义编写公共调用程序,主要适用于动态访问多个服务提供者提供的同类WS资源。显然这两种模型都很难满足SAA对服务动态调用的需求。

动态调用接口比动态代理模型更进一步,客户端使用 `javax.xml.rpc.Call` 接口实现远程动态调用,主要步骤为:①定义WS提供者的名称及端口名称,利用 `ServiceFactory.newInstance()` 方法创建服务工厂(ServiceFactory);②从工厂中创建一个WS实例;③从实例中创建调用对象,传递端口名称和要执行的操作名称;④在执行实际方法调用之前使用 `setProperty` 方法设置属性;⑤设置操作名称;⑥使用 `Call.invoke()` 方法调用服务,得到调用结果。此法不需在开发阶段生成客户端代理程序,而是在运行时动态读取WSDL、发现服务、配置远程调用并执行。本文即采用了此方法配合特殊的全局ID注册机制实现了SAA的服务动态调用功能(如图3所示)。

4.3 服务访问认证机制

基于SAA的身份认证机制是实现WS访问控制的核心策略,本方案采用了两级认证的方法。

(1) 域内认证

由于原安全策略有一定保护功能,域内认证可以使用相对简单的认证策略。本文通过在每个WS的SOAP调用请求中添加与所属域相关的标识符并在SAA域内认证模块中对其进行验证实现。

(2) 域间认证

跨域的访问要通过互联网实现,因此域间认证需要更复杂、可靠的策略支持,本文借用了“安全/代价比”都比较理想的Kerberos协议。Kerberos协议是由MIT提出的基于可信第三方密钥分发中心(KDC)使用对称密钥加密算法来实现认证服务的。

该协议部署简单,运行高效,能够实现双向认证。Client在访问Server的资源之前,可以要求对Server的身份执行认证,这也增强了系统的安全性。因此,在认证策略中集成Kerberos协议,可以将GAAC域间认证模块配置成KDC,将待认证的SAA配置成Client和Server从而实现二者的双向身份认证。另一方面,Kerberos协议除了提供域间认证功能外,还可以在SAA间建立起安全信道也间接确保了传输级安全,无需企业再建立专门的数据通道(如VPN、企业专网等),有效降低了成本。

目前,Kerberos协议已在企业界得到广泛应用,拥有良好的稳定性和兼容性,受到了Unix, Linux, Windows等多种主流操作系统的支持,可以方便地实现跨异构平台的部署和互操作。

5 应用实例

本文设计的WS管理方案作为核心模块被运用到国家“八六三”计划项目——“面向业务流程的异构系统集成平台”中,并在我国典型集团企业经纬纺织机械股份有限公司进行了工程应用。经纬纺机在企业信息化领域起步较早,但随着企业规模增大和业务领域拓展,目前该集团面临营销服务体系集成的迫切需求。

为实现集团营销数据集成自动化的目标,集成平台根据企业的分布式结构采用了相应的星型架构(如图4所示),在集团总部安装平台中央节点,其上部署了管理系统Portal、全局认证授权中心GAAC、总部子网SAA及封装遗留系统功能组件形成的WS资源;在榆次和常德分公司企业域内分别安装平台子节点并部署相应的SAA和WS等。于是总部中央节点部署的流程服务通过跨域调用两个子节点相关的WS资源实现下属企业营销数据自动采集和集成过程。

在上述工程应用中,管理方案确保了应用集成的可行性和安全性,其灵活的组织架构有效地应对了集团企业业务需求动态性变化的特点,同时该方案采用通用的实现技术对集团企业复杂的遗留环境有很强的适应性,保护了其前期的IT投资。

6 结束语

在SOA架构的基础上设计了一套完整的WS管理方案,通过建立一种灵活的服务访问代理架构和两级身份认证授权机制,充分实现了对分布式系统中WS资源的共享管理和访问控制并具有良好的

扩展性和可维护性;采用基于全局 ID 的服务注册和动态调用机制,增强了 SOA 系统的敏捷性和松耦合性.同时,该方案的实现采用了业界主流的 J2EE

技术和开源成熟的 Kerberos 协议,对企业异构且复杂的遗留环境具有较强的通用性和适应能力,在企业工程时间中展现了良好的经济和实用价值.

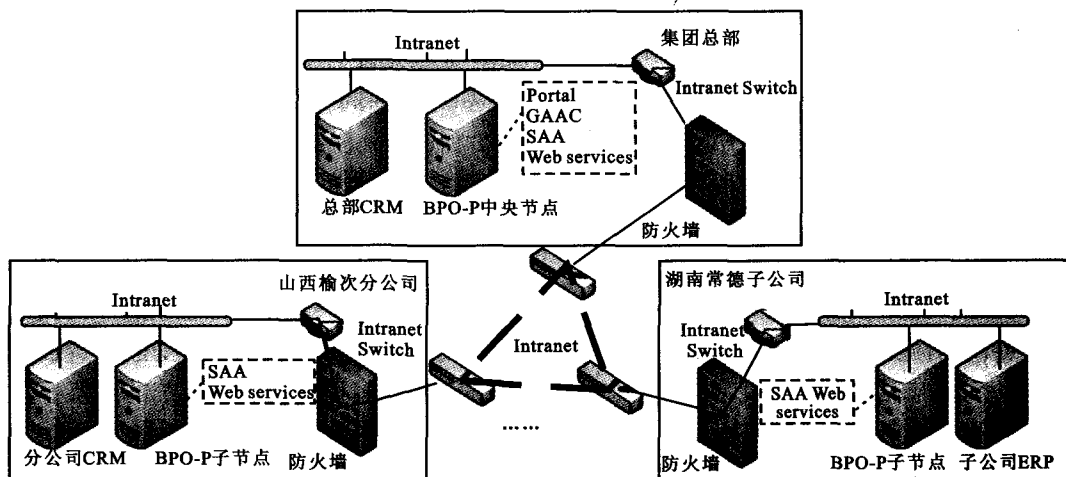


图 4 工程应用系统物理架构

参考文献:

- [1] Komoda N. Service oriented architecture (SOA) in industrial systems[C]// 2006 IEEE International Conference. Taiwan: Taipei, 2006: 1-5.
- [2] Kanneganti R, Chodavarapu P. SOA security[M]. Greenwich: Manning Publications Co, 2008.
- [3] 邵晓燕, 邵贝恩. 基于 SOA 的企业应用跨安全域访问控制[J]. 清华大学学报, 2009, 49(7): 1050-1053.
- [4] Bill Jones, Kevin Minder. Planning for service management within a service-oriented computing infrastructure [EB/OL]. [2009-11-19]. <http://java.sys-con.com/read/45783html>
- [5] 呼斯乐, 邵贝恩. 集团型企业异构系统的中间件集成方案[J]. 微计算机信息, 2009, 25(9): 3-5.
- [6] Sheth A, Verma K, Miller J, et al. Enhancing web service descriptions using WSDL-S[J]. Lecture Notes in Computer Science, 2005(3387): 55-68.
- [7] Li H, Du X, Tian X. A WSMO-based semantic web services discovery framework in heterogeneous ontologies environment[J]. Lecture Notes in Computer Science, 2007 (4798): 617-622.
- [8] 邵晓燕. 企业服务资源共享中跨安全域访问控制研究[D]. 北京: 清华大学自动化系, 2008.

作者简介:

吴靖 男, (1985-), 研究方向为系统集成、企业计算等。
 彭启瑞 男, (1986-), 研究方向为网络安全。
 李清 男, (1970-), 博士, 副教授. 研究方向为系统建模、系统评价体系、航空飞行器控制等。
 刘永青 男, (1979-), 工程师. 研究方向企业信息化应用。

(上接第 3 页)

参考文献:

- [1] Verma K, Sivashanmugam K, Sheth A. Meteor-S WSDI: a scalable infrastructure of registries for semantic publication and discovery of web services[J]. Journal of Information Technology and Management, 2005, 6(1): 17-39.
- [2] 许斌, 李涓子, 王克宏. Web 服务语义标注方法[J]. 清华大学学报: 自然科学版, 2006, 46(10): 1784-1787.
- [3] 张大陆, 吕韬. 基于概念频率的 Web 服务语义标注[J]. 同济大学学报: 自然科学版, 2008, 36(1): 1395-1400.
- [4] Paolucci M. Semantic matching of Web service capabilities [M]. Berlin: Springer Verlag, 2002.
- [5] 严蔚敏, 吴伟民. 数据结构[M]. 北京: 清华大学出版社, 2002.

作者简介:

曾诚 男, (1976-), 博士, 副教授. 研究方向为网络化软件工程。
 李兵 男, (1969-), 教授, 博士生导师. 研究方向为网络化软件工程。
 何克清 男, (1947-), 教授, 博士生导师. 研究方向为网络化软件工程。