基于目录服务实现 JAVA 应用的统一认证

Unified Certification of Implementing Java Application Based on Directory Service

胡宏涛 张少应 (西安石油大学计算机学院 陕西 西安 710065)

摘要:为简化网络资源的访问和管理,目录服务已成为企业一个有效的网络管理工具。本文提出了一种使用目录服务实现 Java 应用统一认证的方法,并以微软活动目录为例详细说明了该方法的具体实现过程。基于目录服务实现企业应用系统的统一认证,使得用户管理更方便、系统更安全。

关键词:LDAP JNDI 目录服务

1 引言

在企业信息化建设过程中,由于总体规划、技术方案、企业各部门基于自身需求考虑等方面原因,企业中存在着各种独立的应用系统,分别给同一用户建立了帐号,而且各应用都采用各自独立的认证管理模式,这就要求用户记忆很多用户名和密码,给网络维护、系统升级以及统一授权带来不便;另一方面,随着企业网络信息和规模日益庞大,以各种格式存储的网络信息又源于不同开发平台,给用户信息查询和管理带来不便。如何给企业提供安全可靠的统一认证服务,减少网络维护以及用户管理方面投资,成为应用开发人员急需解决的问题。采用目录服务来进行网络管理成为目前解决该问题的好方法,目录服务已成为企业在网络管理中必不可少的管理工具。

基于 X.500 标准的 LDAP(Lightweight Directory Access Protocol,轻量级目录访问协议)目录服务是一种支持 TCP/IP 协议、允许客户机访问目录信息并完成认证服务的跨平台标准协议;Sun 公司组织开发的 JNDI(Java Naming and Directory Interface ,Java 的命名和目录接口)是一套开放的、标准的基于 Java 规范的接口,JNDI 提供的 API 独立于任何具体目录服务实现,使应用能够通过统一的方式访问多种名字和目录服务,通过绑定将对象和名称实现无缝连接。由于 JNDI 提供了支持 LDAP 目录服务接口,这使得在多种异构系统集成中,基于 Java 平台开发的应用通过目录服务实现用户认证统一管理成为现实。

2 基于目录服务实现 Java 应用统一认证的方法

2.1 LADP 的基本结构

LDAP 目录中可以存放各种类型数据:电子邮件地址、人力资源数据、联系人列表、公用密匙等。严格意义上说,LDAP 不是一个数据库,而是一个用来访问存储在信息目录中的协议,同数据库用来保存实时改变的数据不同,LDAP 目录服务主要用来优化集中式读操作(LDAP 服务器主要进行读操作和少量写操作)的性能,LDAP 定义了一套标准方法访问和更新目录中的信息。

LDAP 的基本结构(如图 1 所示)是以树型结构来存储的目录信息树(简称为 DIT),每个叶结点是个条目(Entry),每个条目包含一个唯一标识的 DN(Distinguished Name)和许多属性/值。而目录树的根结点称为目录树的基准,或者基准 DN(base DN)。理论上基准的选择可以是任意的,但这往往会产生混乱,也给终端用户带来记忆的麻烦,因而推荐使用将 DNS 编码作为基准 DN,在图 1 中可以看出 DNS 域名为:pisoftware. com。

其中:

dc: domain component

ou:Organizational Unit

©《计算机系统应用》编辑部 http://www.c-s-a.org.cn

uid:User ID

cn:Common Name

2.2 LDAP 认证管理的工作机制

Java 的 JNDI 提供了与 LDAP 服务器交互的 API，

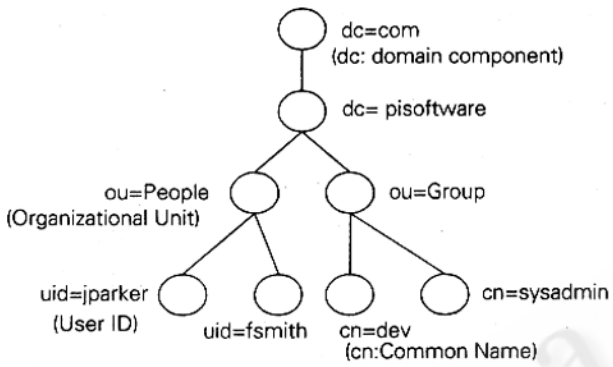

图 1　LDAP 存储模型的目录树结构

而 LDAP 为目录服务提供了开发的标准化协议，这就为使用 JNDI 对 LDAP 目录服务访问成为现实，整个工作机制如图 2 所示。

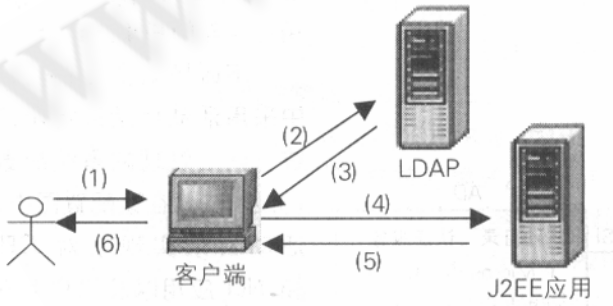

图 2　LDAP 进行认证的工作机制

2.3 实现方法

标准的 LDAP 访问操作主要包括：(1)连接 LDAP 服务器；(2)绑定 LDAP 服务器；(3)执行修改、删除、查询等 LDAP 操作；(4)断开连接。在实际操作中，针对 LDAP 的访问主要是查询操作。

2.3.1 JNDI 类的导入

要连接 LDAP 服务器，需要引用一个执行 DirContext 接口的对象，在应用程序中，通常选用 InitialDirContext 对象，该对象通过调用类型为 Hashtable 的变量来设置连接的环境变量、定义入口等操作。JNDI 中最重要的概念是上下文 context，即定位从哪个入口开始操作，其他操作都是该上下文操作的调用。所以需要导入 JNDI 的下列类包。

```
import javax. naming. Context;
import javax. naming. NamingException;
import javax. naming. directory. DirContext;
import javax. naming. directory. InitialDirContext;
```

2.3.2 连接 LDAP 服务器

定义连接 LDAP 的函数为：

public Hashtable Htable(String ProviderUrl,String Domain,String User,String Pwd)

由于 LDAP 提供了 RFC822 的命名格式(标准格式：object_name@ domain_name)，该形式类似电子邮件地址，许多企业使用该名字作为邮箱名和登录系统的帐户名，所以登陆入口 DN 也可以选用邮箱名。

```
//服务程序提供工厂，选用 sun 公司提供的缺省的服务提供者
public static final String Factory = "com. sun. jndi. ldap. LdapCtxFactory";
//构造 Hashtable 初始化连接 LDAP 数据库的环境变量
Hashtable env = new Hashtable(); //创建存储 JNDI 环境变量的表
env. put(Context. INITIAL_CONTEXT_FACTORY, Factory);
env. put(Context. PROVIDER_URL, ProviderUrl);
```

2.3.3 绑定 LDAP 服务器

一旦连接 LDAP，客户端本身就需要验证，该过程称为“绑定”服务器。在 LDAP v2 中，所有客户端都需要验证；而 LDAP v3 默认为匿名，即使默认值已使用，所有连接都使用匿名验证。LDAP 支持 simple、ssl 和 sasl 三种认证方法。

```
env. put(Context. SECURITY_AUTHENTICATION, "simple"); //定义认证方法为"simple"
if(Domain. equals(""))
  //根据用户名定义入口的 DN
  {env. put(Context. SECURITY_PRINCIPAL, User);}
else
  //根据邮件地址定义入口的 DN 和口令
  {env. put(Context. SECURITY_PRINCIPAL, User + "@" + Domain);}
env. put(Context. SECURITY_CREDENTIALS, Pwd);
```


©《计算机系统应用》编辑部 http://www.c-s-a.org.cn

2.3.4 对 LDAP 进行查询操作

```
//以 Hashtable 作为认证参数,如果认证成功返回 true,否则返回 false
public boolean connectladp(Hashtable env){
boolean result = false;
DirContext ctx = null;
//所有的目录操作都可能抛出异常
try{
  ctx = new InitialDirContext(env);
  result = true;
}catch(javax.naming.AuthenticationException e)
{
result = false;
}catch (Exception e) {
  e.printStackTrace();
}
```

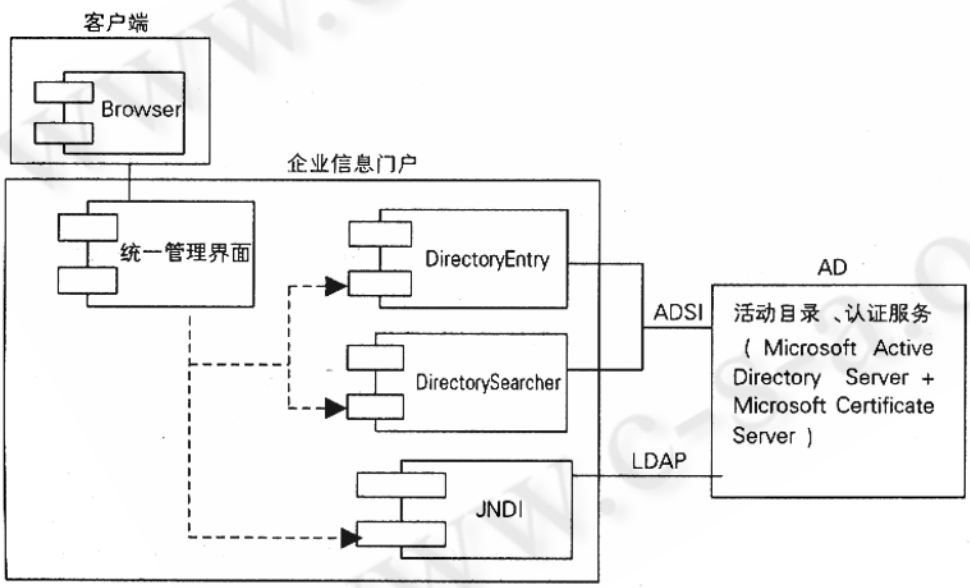

图 3　单点登录系统配置

```
if(ctx != null)
{
try{
  ctx.close();
  }catch (NamingException e)
}
return result;
}
```

3 使用微软活动目录实现 Java 应用统一认证的实例

活动目录是 Windows 平台的一个核心的部件,用来存储与网络资源有关的信息,它能够让企业有效地管理网络资源和用户信息,并允许操作系统方便地验证用户身份并控制其对网络资源的访问。活动目录为企业信息门户(简称 EIP)在实现个性化和安全性的单点登录 WEB 页面方面提供技术支持,而企业信息门户为企业现有各种同构或异构的应用集成提供了统一的系统平台,因而,活动目录与 WEB 技术的结合,将会有效地管理企业信息门户实现统一认证和单点登录,减少企业在网络管理方面的开销。

活动目录是基于标准目录访问协议的,许多应用界面(API)都允许开发者访问这些协议,而 LDAP 已经成为目录服务的标准,微软的活动目录服务对它提供了全面的支持。通过 JNDI 对活动目录的 LDAP 服务的访问实现 Java 应用的统一认证,使所有 Java 应用可以与门户集成认证。

下面是某企业在门户中采用活动目录进行用户统一认证管理的系统配置(如图 3)。在该配置图中,活动目录实现了对 J2EE 和. NET 应用以及门户本身的认证管理,而对于不同平台的应用,选用不同的组件来实现对活动目录的访问。

活动目录为用户提供了用户主名(由用户的"速记"名和用户对象归属域树的 DNS 名构成的)的命名方法,而对于 Java 应用在与活动目录连接中,选用邮件地址做为入口的 DN。对连接 LDAP 函数的调用可选用下面两种方式。

方式 1:Htable("ldap://epc.petro.com.cn:389","petro.com.cn","user","user");

方式 2:Htable("ldap://epc.petro.com.cn:389","","user@petro.com.cn","user");

(下转第 84 页)

©《计算机系统应用》编辑部 http://www.c-s-a.org.cn

(上接第 72 页)

4 结束语

目录服务在企业网络管理中,将分散用户信息整合到目录服务平台下,并提供统一操作管理界面,方便了网络管理人员进行管理与维护。作为网络的基础设施,目录服务不仅是一个终端用户工具,也是一个管理工具,被广泛应用于各类企业的信息管理系统中,在网络管理中扮演越来越重要的角色。WEB 技术的发展为企业现有各种同构、异构应用的集成提供了方法。通过 JNDI 对 LDAP 目录服务访问实现 Java 应用的用户统一认证,使实现企业信息门户的单点登录成为可能,减少了应用开发者在用户管理方面的工作量,给网络管理者在用户权限控制、网络资源管理、网络安全服务等方面带来很大便利。

参考文献

1 Sameer Tyagi . LDAP and JNDI:Together forever . http://www. javaworld. com/javaworld/jw – 03 – 2000/jw –0324 – ldap. html

2 Brad Marshall . Introduction to LDAP . http://quark. humbug. org. au/publications/ldap/ldap_tut. html

3 Java Naming and Directory InterfaceTM . http://java. sun. com/j2se/1. 5. 0/docs/guide/jndi/index. html

4 活动目录技术摘要. http://www. microsoft. com/china/

5 岳洋、张杰明等, 用 JNDI 访问 LDAP 服务,计算机时代 2003(6).

©《计算机系统应用》编辑部 http://www.c-s-a.org.cn