



[12] 发明专利说明书

专利号 ZL 200610139612.4

[45] 授权公告日 2009 年 3 月 25 日

[11] 授权公告号 CN 100472530C

[22] 申请日 2006.9.26

[21] 申请号 200610139612.4

[30] 优先权

[32] 2005.9.26 [33] EP [31] 05108882.1

[73] 专利权人 捷讯研究有限公司

地址 加拿大安大略省沃特卢市

[72] 发明人 奎因·斯潘塞

[56] 参考文献

US2003/0191757A1 2003.10.9

US6085188A 2000.7.4

US6356892B1 2002.3.12

US6347312B1 2002.2.12

An Enterprise Directory Solution With DB2.

S. S. B. Shi, E. Stokes, D. Byrne, C. F. Corn, D. Bachmann, T. Jones. IBM SYSTEM JOURNAL, Vol. 39 No. 2. 2000

审查员 李福永

[74] 专利代理机构 中科专利商标代理有限责任公司

代理人 王 玮

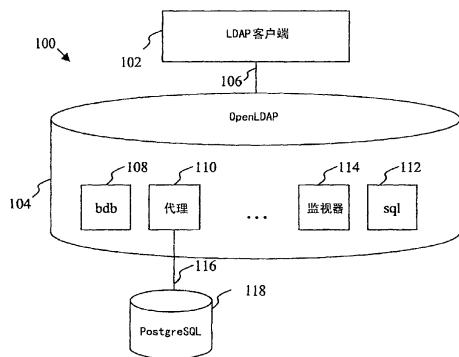
权利要求书 2 页 说明书 10 页 附图 4 页

[54] 发明名称

LDAP 到 SQL 的数据库代理系统和方法

[57] 摘要

提出了一种用于针对 LDAP 客户端的使关系数据库适于目录服务的 LDAP 到 SQL 代理。可以根据数据库模式来定义数据库，所述数据库模式在服务 LDAP 客户端的 LDAP 服务器外部。代理包括优选地针对一组缩减 LDAP 操作的 LDAP 到 SQL 查询和响应映射。代理可以包括维护多个永久数据库连接的机制以减少查询处理开销。代理还可以适于维护到用于执行查询的至少两个可选数据库中的每个的多个永久连接，以提供增强的安全保险操作。可以配置多个 LDAP 到 SQL 代理的数据库，用于均分查询负载以增强可扩展性和性能。



1. 一种根据轻量数据访问协议LDAP向LDAP客户端提供目录服务的方法，包括：

提供用于根据LDAP接收和响应目录服务请求的至少一个LDAP服务器，每个LDAP服务器包括LDAP到结构化查询语言SQL代理模块，定义所述LDAP到SQL代理模块以将接收到的LDAP服务请求映射到SQL查询、针对SQL数据库执行SQL查询以获得SQL查询结果、以及将SQL查询结果映射到LDAP响应；其中操作在LDAP服务器外部维护并且与LDAP服务器相分离的数据库模式来定义SQL数据库，且操作LDAP服务器来使用该外部维护的数据库模式。

2. 如权利要求1所述的方法，其中，配置每个所述代理模块，以仅映射一组缩减类型的LDAP服务请求。

3. 如权利要求2所述的方法，其中，LDAP到SQL代理模块映射LDAP服务请求，所述LDAP服务请求足以仅促进从数据库的信息检索。

4. 如权利要求1至3任一项所述的方法，其中，将LDAP服务器配置为OpenLDAP服务器。

5. 如权利要求1至3任一项所述的方法，其中，每组LDAP服务器、代理模块以及数据库定义了单元，所述方法还包括提供对于每个单元是可访问的主数据库。

6. 如权利要求1至3任一项所述的方法，其中，LDAP到SQL代理模块维护到至少一个数据库的永久连接池，所述永久连接池中的连接提供访问以执行所述SQL查询。

7. 如权利要求5所述的方法，还包括提供用于在单元中均分目录服务请求的重定向服务器。

8. 如权利要求5所述的方法，其中，对于每个单元，配置该单元中的每个代理模块，以在该单元的数据库不可用时来针对主数据库执行目录服务请求。

9. 一种计算机系统，包括：

至少一个轻量数据访问协议LDAP服务器，用于向LDAP客户端提供

目录服务；所述至少一个服务器中每一个包括：

LDAP到结构化查询语言SQL代理，用于使LDAP服务器适于将由SQL可访问的数据库与LDAP客户端相连，安排代理以将LDAP访问请求映射到SQL查询以及将SQL响应映射为LDAP响应；以及

使用SQL可访问的数据库，由在LDAP服务器外部维护且与LDAP服务器分离的数据库模式定义，每个LDAP服务器可操作地来使用该外部维护的数据库模式。

10. 如权利要求9所述的计算机系统，其中，安排代理以转换一组缩减类型的LDAP访问请求。

11. 如权利要求9或10所述的系统，其中，LDAP服务器是OpenLDAP服务器。

12. 如权利要求9或10所述的计算机系统，其中每组LDAP服务器、LDAP到SQL代理和数据库定义了单元，并且所述计算机系统还包括由每个单元可访问的主数据库。

13. 如权利要求12所述的计算机系统，还包括用于在单元中均分目录服务请求的重定向服务器。

14. 如权利要求12所述的计算机系统，其中，对于每个单元，配置该单元中的每个代理，以在该单元的数据库不可用时针对主数据库执行目录服务请求。

15. 如权利要求12所述的计算机系统，其中，安排每个代理以维护到该代理的单元的数据库和主数据库中每个的多个永久连接，所述连接提供访问以执行所述SQL查询来增强故障保险的操作。

LDAP到SQL的数据库代理系统和方法

技术领域

本发明一般涉及计算机系统集成，以及具体地，涉及促进在其他情况下不兼容的计算机系统组件之间的数据库活动。

背景技术

配置计算机系统以执行特定的功能（例如电子商务、网络服务、商业交易处理、电子数据通信等）经常包括对来自不同源的完全不同的硬件和软件的集成。可以配置针对此类系统的特定组件用于根据第一协议与一个或多个其他组件一起操作。然而，系统集成可能希望让该特定组件与并不支持第一协议的特定的其他组件一起操作。

例如，经常希望将包括目录或其他数据库的数据存储库（data store）组件与系统的另一个组件集成在一起。典型地，根据在数据存储库中针对访问信息的特定的模式和协议来定义数据存储库。此类协议中的一种是结构化查询语言（SQL），用于访问关系数据库管理系统（RDBMS）数据库，以及另一种是轻量目录访问协议（LDAP），用于提供到目录服务的访问，特别地针对读取、搜索、以及浏览信息优化的、基于X.500的目录服务。每一种具有特别的优点或其他特征，可以使其在计算机系统中得到值得期待的利用。例如，LDAP适于作为用于访问目录中的信息的网络协议，并且能够易于在用于访问远程存储的信息的客户端组件中实现。电子邮件客户端经常将LDAP用于访问目录信息（例如地址簿）。基于SQL的数据库对于不同的卖主是普遍可用的，并且提供复杂功能，包括利用LDAP目录通常不能发现的交易支持以及回滚（roll-back）方案。

有时，由针对不同协议配置的多个组件来共享计算机系统中的数据存储库。因此，存在组件与数据存储库不兼容的时候，例如，由于

针对SQL操作配置的数据存储库与针对LDAP操作配置的组件不兼容。

LDAP的一个实现是OpenLDAP，由OpenLDAP基金协调的、开放源码团体开发的软件数据存储库。该软件的一个组件是LDAP服务器，用于提供到存储在一个或多个后端中的数据的LDAP访问。OpenLDAP通过特定的模块提供到不同的后端或存储类型（即数据库的类型）的访问。配置OpenLDAP以提供三种一般类别的后端，也就是：1) 存储数据；2) 代理以其他方式存储的数据；以及3) 作业中（on the fly）产生数据。一个代理后端是用于将基于SQL的RDBMS映射到目录服务代理（DSA）的back-sql。支持RDBMS的示例是来自IBM的DB2、来自MySQL AB的MySQL以及来自PostgreSQL全球开发组的PostgreSQL。

然而，因为back-sql代理适合于多重目的的SQL数据库，并且根据OpenLDAP的需要预定义了模式，其执行比可能是必须的工作更多的工作，并且引起多于所期待的开销（存储装置和其他资源），使得其性能特性是不合适的。配置back-sql以使用其自己的专有数据库模式而不是外部数据库模式，即使根据其各自的数据库模式定义了现有的SQL数据库。

因此，存在对简单的LDAP到SQL数据库代理的需要。

IBM Systems Journal, Vol 39, no2, “An enterprise directory solution with DB2”, Shi et al, 公开了一种系统，通过该系统，由其所插入到的LDAP服务器通过数据库模式定义SQL数据库。类似地，美国专利US2003/0191757公开了一种系统，所述系统将LDAP请求映射到DA数据库响应，并且将DA响应传递到LDAP兼容的响应。

发明内容

优选地，提出了一种LDAP到SQL代理，以使关系数据适于针对典型地由LDAP服务器所服务的一个或多个客户端的目录服务。代理包括LDAP到SQL的查询和响应映射，优选地但是不必要地针对一组缩减LDAP操作。代理可以包括一种机制，维护多个永久数据库连接以减少查询处理开销。代理还可以适合于维护到用于执行查询的至少两个可选数据库中每个的多个永久连接，以提供改进的故障保险运作。可以配置

多个LDAP到SQL代理的数据库，用于均分查询负载以增强可扩展性和性能。可以将代理配置为用于向LDAP服务器提供后端关系数据库的模块。有利地，可以根据LDAP服务器外部的数据库模式来定义数据库，以促进现有的数据库向LDAP环境的集成并且避免复制。

根据第一方面，优选地，提出了一种根据轻量数据访问协议（LDAP）向LDAP客户端提供目录服务的方法包括：提供用于根据LDAP接收和响应目录服务请求的LDAP服务器，所述LDAP服务器包括LDAP到SQL代理模块，定义所述LDAP到SQL代理模块以将LDAP服务请求映射到SQL查询、针对数据库执行SQL查询以获得SQL查询结果并且将SQL查询结果映射到LDAP响应；以及其中根据LDAP服务器外部的数据库模式定义所述数据库。可以配置代理模块来映射一组缩减类型的LDAP服务请求，以最小化LDAP服务器资源消耗，例如，仅足以促进从数据库的信息检索的那些LDAP服务请求。优选地，将LDAP服务器配置为OpenLDAP服务器。可以定义LDAP到SQL代理模块以维护与至少一个数据库的永久连接池，以致于使得该连接提供访问以执行SQL查询。

根据另一个方面，优选地，提出了一种包括指令的计算机可读媒质，当由计算设备执行所述指令时，使用于提供目录服务的LDAP服务器适于将针对SQL操作而配置的数据库与针对LDAP操作而配置的客户端相连。所述指令包括映射以将LDAP服务请求转换到SQL查询以及将SQL响应转换到LDAP响应，并且根据LDAP服务器外部的数据库模式定义数据库。

根据又一方面，优选地，提出了一种计算机系统包括：LDAP服务器，用于向LDAP客户端提供目录服务；LDAP到SQL代理，使LDAP服务器适于将由SQL将可访问的数据库与LDAP客户端相连，代理将LDAP访问请求转换为SQL查询并且将SQL响应转换为LDAP响应；以及使用SQL可访问的数据库，根据LDAP服务器外部的数据库模式来定义所述数据库。

在一个实施例中，优选地，计算机系统包括：多个LDAP服务器、LDAP到SQL代理、以及数据库，每个的数目相类似；服务器、代理、以及数据库的之一是相关联的以定义一个单元；并且所述计算机系统还包括由每个单元可访问的主数据库。计算机系统还可以包括重定向服

务器以在单元中均分目录服务请求。优选地，配置特定单元中的每个代理，以在该特定单元的数据库不可用时针对主数据库执行目录服务请求。

附图说明

现在将参考下面的附图来描述仅作为示例的实施例，其中：

图1是根据实施例的具有LDAP到SQL代理模块的LDAP服务器的方框图；

图2是根据实施例的消息处理的方框图；

图3是根据实施例的经由LDAP到SQL代理向LDAP客户端提供多个SQL数据库的计算机系统体系统结构的方框图；以及

图4是根据图3的实施例的操作流程图。

为方便起见，描述中相同的数字代表图中相同的结构。

具体实施方式

图1说明了代表性的计算机系统100，其中第一组件102包括LDAP客户端，用于通过通信连接106访问由LDAP服务器104提供的目录服务。然而，后端数据存储库（第二组件）是经由SQL可访问的RDBMS 118。在本实施例中，将LDAP服务器配置为针对LINUX操作系统环境的OpenLDAP服务器（*slapd daemon*），所述LINUX操作系统环境具有针对诸如但不限于bdb 108、sql 112、以及监视器114的不同后端的多个标准模块。所述LDAP服务器104具有后端代理模块110，该后端代理模块110用于经由通信连接116向数据库118传递SQL查询，在该实施例中所述数据库118是根据在LDAP服务器104外部维护的数据库模式而定义的典型PostgreSQL数据库。连接106和116可以是公共网或专用网、局域网或广域网、或其他通信信道等。除了那些已示出或已描述的，还可以使用其他的基于SQL的数据库或LDAP服务器。如果不必要则不需要提供一些OpenLDAP模块，例如back-sql、back-bdb等。

根据DLAP协议来向LDAP服务器104传递来自LDAP客户端102的针对目录服务的请求（典型地，用于获得存储到后端118的信息的查询）。

服务器104调用代理110，代理110将LDAP查询转换到SQL用于传送到数据库118。根据SQL协议接收来自数据库118的响应，并且由代理模块110将其转换为LDAP协议响应来经由服务器104发送回LDAP客户端102。

图2说明了在服务器104、代理模块110以及数据库118之间的“消息”操作的示例。应该理解的是，这里的“消息”意味着从一个组件传送或以其他方式传递给另一个组件的信息，并且不必限制于以已定义的消息格式经由通信网络传送的数据。消息1包括一批针对服务器104和客户端102的证书。代理模块110转换消息以向数据库118提供客户端证书（消息2），并且本地地认证服务器证书、提供结果（消息3）。在收到认证请求（消息4）的SQL结果时，代理模块110向服务器104提供已转换的LDAP结果（消息5）。消息5因而取决于两次认证的结果。消息6包括LDAP查询，所述查询已被转换并且作为SQL查询（消息7）发送。接收SQL响应（消息8）（例如来自外部数据库的一组记录）以及将其转换为LDAP响应（消息9）。

可以根据LDAP客户端的需求以及将要向其提供的特定的目录服务来配置代理模块110。因此，可以确定和执行一组特定的LDAP到SQL的转换以及相反的转换，以提供减少的LDAP目录服务和操作。代理模块110因而将进来的消息格式有效地映射到外发的格式，而不必执行针对所有类型的LDAP服务请求、SQL查询和响应的映射。例如，如果LDAP客户端102受限于从目录检索（即，搜索和读取）信息，不必配置LDAP到SQL的代理模块110来促进LDAP请求以修改或存储信息。同样地，代理模块将消耗比诸如back-sql的完全SQL代理实现中更少的资源。另外并且重要地，代理准许现有的数据库的使用或集成，尤其当希望不改变现有数据库（即，定义新的模式）的时候。因此具有其现有模式的SQL数据库可以被有效地与配置用于使用LDAP的组件集成在一起。使用针对相同数据的第二模式的结果是不必创建复制表等。

在优选实现中，在针对OpenLDAP以C程序语言来配置代理模块110（back-prox），如表1中所述的：

表1

文件名称	用途
back-prox.h	定义由模块中的所有文件所要求的结构和常数。该结构被用于在函数之间传递信息。
connectionpool.h	这是针对连接池的头文件。
connectionpool.c	该文件包含用于初始化、维护、以及清除连接池的函数。
external.h	该头文件定义了针对关于其余OpenLDAP的外部接口的函数。该文件由每个模块来要求。
init.h	用于初始化模块的头文件。
init.c	
search.h	针对搜索功能的头文件。也定义了用于将LDAP属性名称转换为SQL列名称的结构。
search.c	当执行搜索时，在该文件中定义的函数被用于翻译进来的查询、将其发送到Postgres后端、以及然后将结果打包到LDAP响应中。
bind.c	该文件包含当用户试图绑定OpenLDAP中的节点时使用的函数。这也是针对服务器和用户证书的认证发生的地方。

为减少用于处理查询的交易开销，维护久连接池用于重复使用地连接到外部数据库。可以循环或者以本领域技术普通技术人员所知的共享方式来共享连接。下面将参考图4在这里描述另外的操作，其中优选的代理维护针对两个可选的数据库（本地拷贝和远程主数据库）中每个的连接池以查询。

下面的函数将来自OpenLDAP 102的函数指针映射到代理模块110（即，在优选实施例中的back-prox）中的实际实现。设置为0的函数没有实现，并且0是指示成功的缺省返回值。

```

bi->bi_open=0;
bi->bi_config=0;
bi->bi_close=0;
bi->bi_destroy=0;
bi->bi_db_init=backprox_db_init;
bi->bi_db_config=backprox_db_config;
bi->bi_db_open=backprox_db_open;

```

```

bi->bi_db_close=backprox_db_close;
bi->bi_db_destroy=backprox_db_destroy;
bi->bi_op_abandon=0;
bi->bi_op_compare=0;
bi->bi_op_bind=backprox_bind;
bi->bi_op_unbind=backprox_unbind;
bi->bi_op_search=backprox_search;
bi->bi_op_modify=0;
bi->bi_op_modrdn=0;
bi->bi_op_add=0;
bi->bi_op_delete=0;
bi->bi_op_referrals=0;
bi->bi_operational=0;
bi->bi_connection_init=0;
bi->bi_connection_destroy=0;

```

没有实现的函数是不必要的或是多余的，并且是没有被使用的，因为在不同的函数中进行实现。贯穿其余的模块能够找到对应的函数。由变量bi所参考的BackendInfo结构在slap.h中定义，并且被用于在模块中的不同函数之间传递信息、函数指针、以及信号量（semaphore）。模块中的函数实现的简要描述如下表2。每个*_db_*的描述来自slap.h文件。

表2

函数	描述
bi_db_init	调用以初始化每个数据库，在读取“数据库<类型>”时调用，仅从backend_db_init()调用
bi_db_config	调用以配置每个数据库，调用每个数据库以处理每个数据库选项，仅从read_config()调用
bi_db_open	调用以打开每个数据库，在bi_open()调用之后立即但是在daemon启动之前对每个数据库调用一次。仅由backend-startup()调用
bi_db_close	调用以关闭每个数据库，在关闭期间但是在任意

	bi_close调用之前对每个数据库调用一次。仅由backend_shutdown()调用
bi_db_destroy	调用以破坏每个数据库，在所有bi_close调用之后但是在bi_destroy调用之前的关闭期间对每个数据库调用一次。仅由backend_destroy()调用
bi_op_bind	调用绑定操作
bi_op_unbind	调用非绑定操作
bi_op_search	调用搜索操作

针对OpenLDAP的标准配置文件称作slapd.conf文件，并且能够经常在用于标准安装的Linux机器上的/etc/openldap中找到所述标准配置文件。back-prox模块包括附加参数，在从init.c文件中的backprox_db_config()函数启动时读取所述附加参数。表3列出了新的参数及其任务。

表3

参数	描述
cell_dbuser	单元数据库（cell database）用户的登录名称
cell_dbpasswd	单元数据库用户的密码
cell_dbname	将要登录进去的数据库实例的名称
cell_dbhost	单元数据库的主机机器
primary_dbuser	主数据库用户的登录名称
primary_dbpasswd	主数据库用户的密码
primary_dbname	将要登录进去的数据库实例的名称
primary_dbhost	主数据库的主机机器
connection_pool_size	在每个连接池中的永久连接的数目。存在用于本地复制的一个池以及用于主数据库的一个池
reconnect_interval	当数据库失败时，这是重连线程（thread）将使用的轮询频率

本领域的普通技术人员应该理解的是，LDAP属性到SQL的映射以及相反的映射可以以查表等不同方式来执行。

图3说明了用于向LDAP客户端提供可扩展的并且冗余的目录服务

的计算机系统300的方框图。在系统300中有主数据库324，所述主数据库被复制成多个单元306、308、以及310，每个单元包括之前具有各自的LDAP到SQL代理组件(312、314、以及316)的单元数据库(318、320、以及322)，用于向LDAP客户端302提供目录服务。重定向组件304(典型地是配置用于均分负荷的服务器)将来自LDAP客户端302的查询指引到n个单元306、308、以及310中的特定一个，以在单元中均分负荷并且提供可扩展和冗余服务。LDAP到SQL代理组件312、314、以及316可以包括具有如之前描述以及将在下边另外描述的LDAP到SQL代理模块的OpenLDAP服务器。

针对向特定单元的目录服务的请求可以根据以下部分进行服务：根据单元的数据库、根据主数据的本地拷贝、或本地拷贝数据库是不可用的时根据主数据库。图4说明了针对单元的连接池的操作400(例如LDAP到SQL代理)的流程图，以确定是单元数据库还是主数据库来指引已转换的LDAP到SQL的查询。为了减少处理，可以设置标记来向代理指示不要试图使用在单元连接池中的任意连接。可以执行后台线程以当其变得可用时重新建立到单元数据库的连接，必要时周期性重试直到成功。线程重建连接并且在终止前对标记复位。

操作400在接收到对服务的查询之后，在开始步骤402中开始。在步骤404中检查单元是否失败(down)。如果其没有失败，经由“否”分支转到步骤406，测试单元连接并且确定结果(步骤408)。如果单元连接是好的，经由“是”分支转到步骤410，针对单元的本地数据库执行已转换的LDAP到SQL的查询。将连接返回到池(步骤411)，并且针对该查询的操作结束(步骤412)。如果在步骤408中连接没有测试为“好”，或在步骤404中设置了单元标记，经由各自的分支转到步骤414，产生了单元重新连接并且操作试图查询主数据库。

相对于主数据库执行步骤416至423，并且与相对于单元数据库执行的步骤404至410相类似。如果没有针对单元数据库或主数据库来完成查询，在步骤424中返回错误并且结束操作(步骤412)。

在优选的实现中，系统300可以包括一部分电子邮件系统。LDAP客户端302可以包括电子邮件服务器，用于经由网络访问向电子邮件服

务的用户提供电子邮件，例如可从Mirapoint, Inc. 获得。可以将该服务器与其他用户供应服务等集成在一起，并且要求访问存储此类用户信息等的外部数据库。

尽管一些实施例、有时是优选实施例在这里已被描述，本领域的技术人员应该理解，在不脱离所附权利要求所限定的本发明范围情况下，可以对这些实施例进行改变。

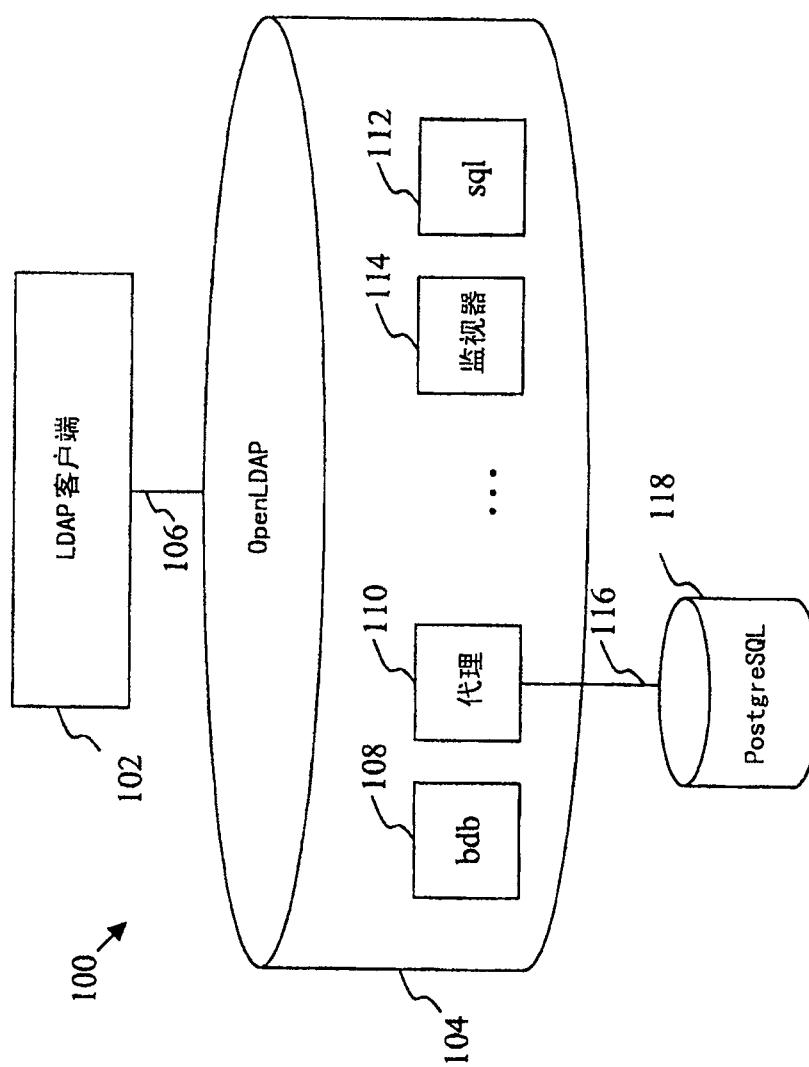


图 1

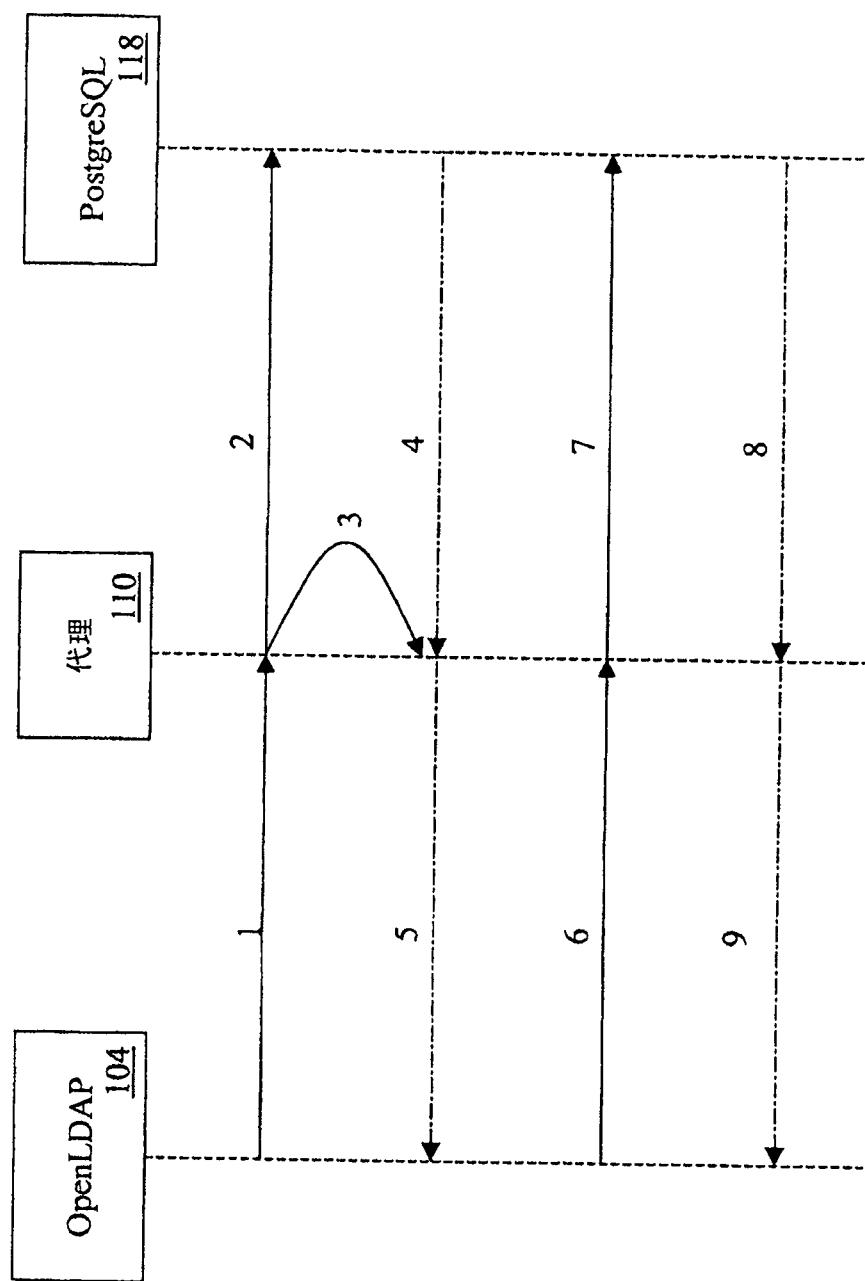


图 2

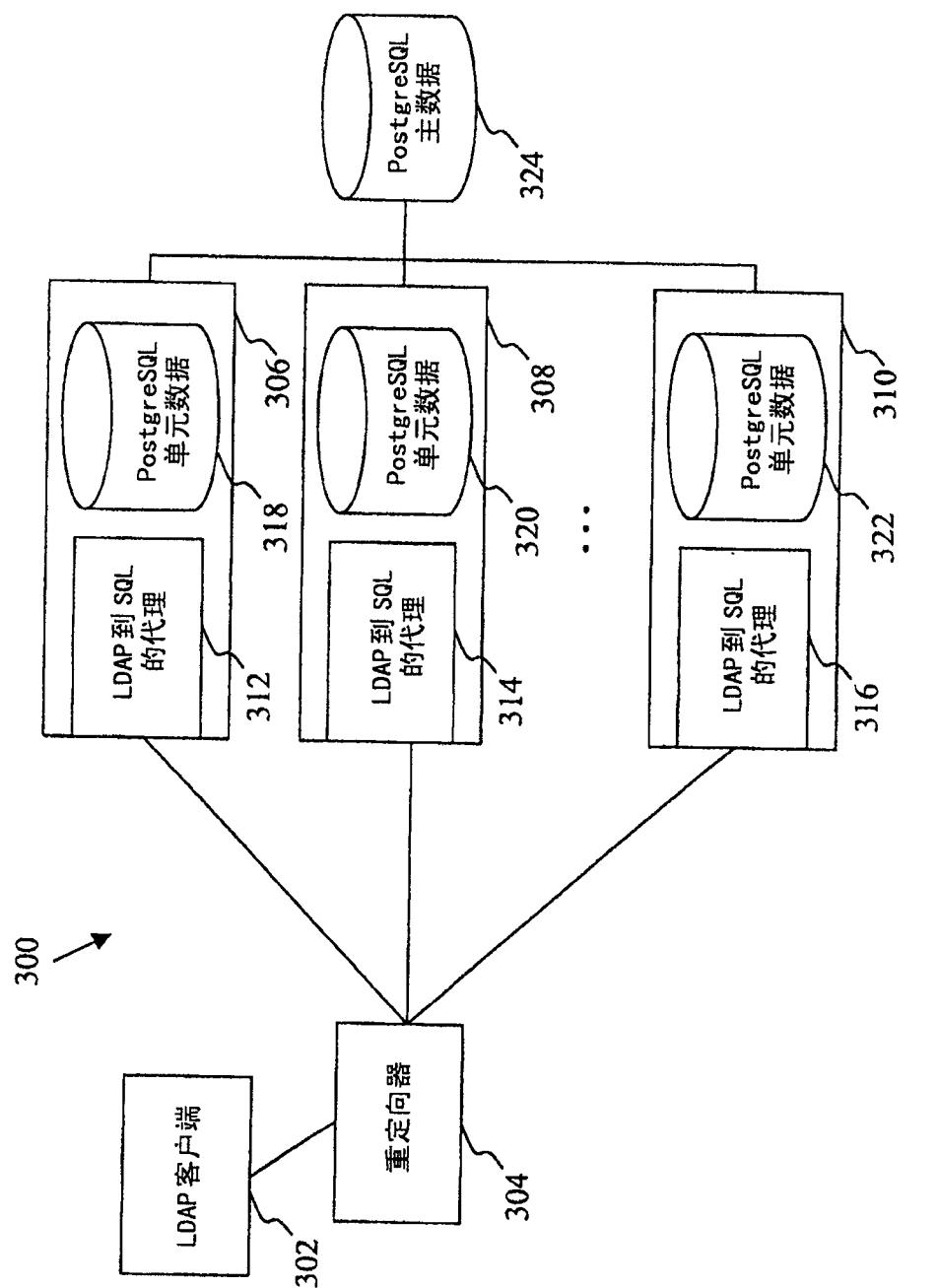


图 3

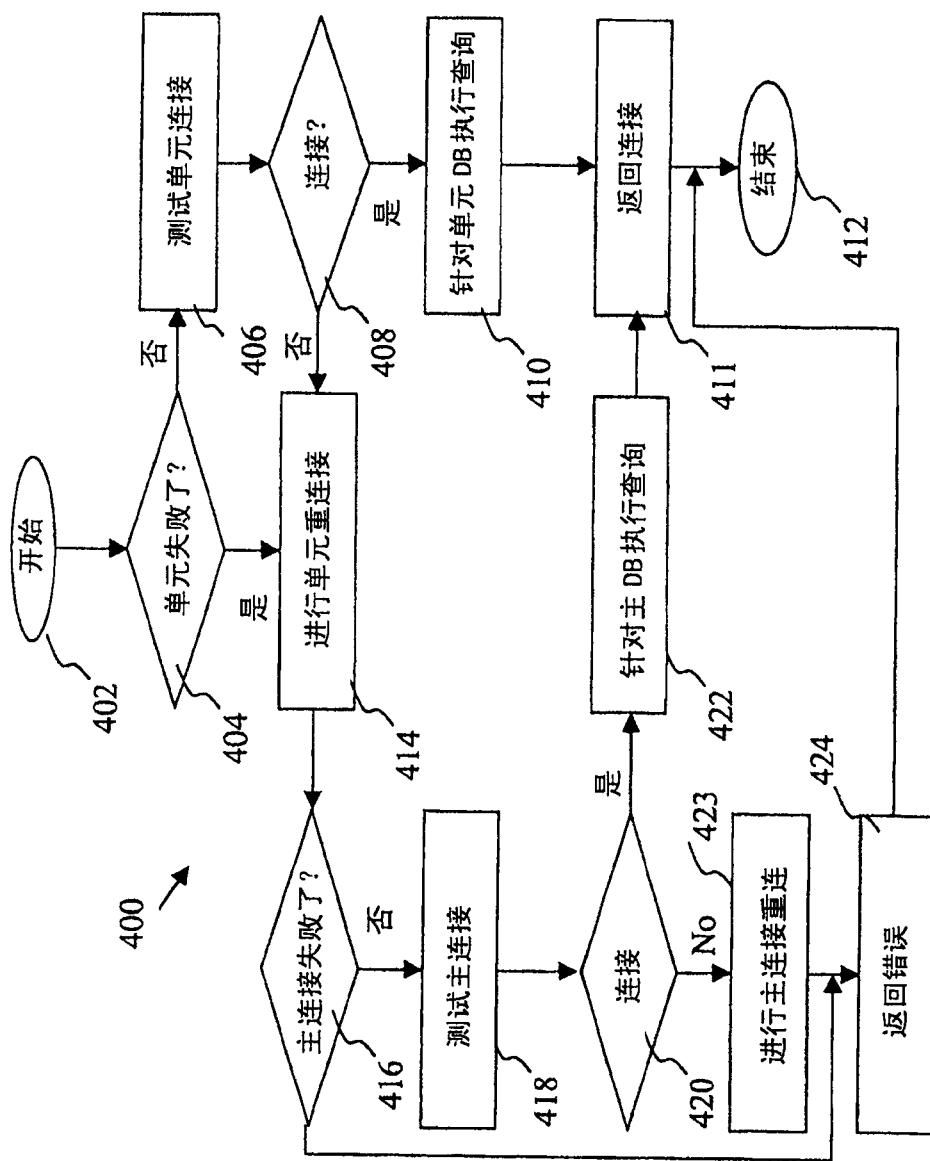


图 4