(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 107204995 A
(43)申请公布日 2017.09.26

(21)申请号 201710631030.6

(22)申请日 2017.07.28

(71)申请人 郑州云海信息技术有限公司
地址 450018 河南省郑州市郑东新区心怡路278号16层1601室

(72)发明人 许陆丹

(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
代理人 李红爽 李丹

(51)Int.Cl.
*H04L 29/06*(2006.01)

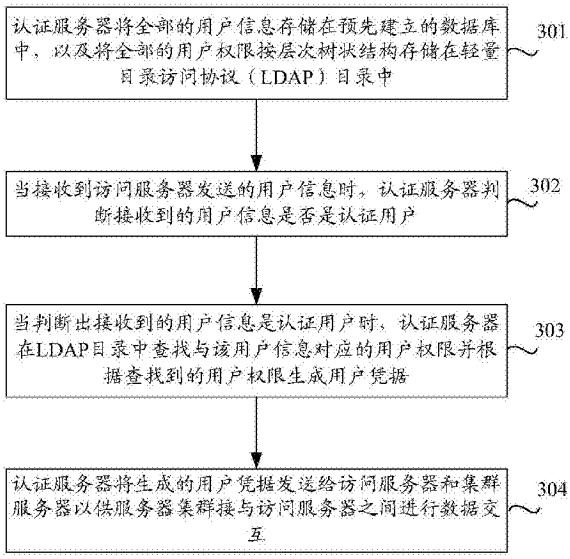
权利要求书3页 说明书9页 附图2页

(54)发明名称

一种控制访问权限的系统、认证服务器和方法

(57)摘要

本文公布一种控制访问权限的系统、认证服务器和方法，该方法包括：认证服务器将全部的用户信息存储在预先建立的数据库中，以及将全部的用户权限按层次树状结构存储在轻量目录访问协议(LDAP)目录中；当接收到访问服务器发送的用户信息时，认证服务器判断接收到的用户信息是否是认证用户；当判断出接收到的用户信息是认证用户时，认证服务器在LDAP目录中查找与该用户信息对应的用户权限并根据查找到的用户权限生成用户凭据；认证服务器将生成的用户凭据发送给访问服务器和集群服务器以供服务器集群接与访问服务器之间进行数据交互。本发明实施例实现了密码的统一管理以及权限的集中管理。




CN 107204995 A

1.一种控制访问权限的系统，其特征在于，包括：认证服务器、访问服务器和服务器集群；其中，

认证服务器，用于将全部的用户信息存储在预先建立的数据库中；将全部的用户权限按层次树状结构存储在轻量目录访问协议LDAP目录中；当接收到访问服务器发送的用户信息时，判断接收到的用户信息是否是认证用户；当判断出接收到的用户信息是认证用户时，在LDAP目录中查找与该用户信息对应的用户权限并根据查找到的用户权限生成用户凭据；将生成的用户凭据发送给访问服务器与服务器集群；

访问服务器，用于将用户输入的用户信息发送给认证服务器；接收认证服务器发送的用户凭据；根据接收到的用户凭据与服务器集群进行数据交互；

服务器集群，用于接收到来自认证服务器发送的用户凭据，对该用户开放与该用户凭据对应的用户权限以与访问服务器进行数据交互。

2.根据权利要求1所述的系统，其特征在于，所述用户信息包括：用户名和口令；

所述认证服务器中用于将全部的用户信息存储在预先建立的数据库中包括：

采用预先部署的网络认证协议Kerberos服务Service分别对每个用户的用户名和口令进行加密；

将加密后的每个用户的用户名和口令对应存储在所述预先建立的数据库中。

3.根据权利要求2所述的系统，其特征在于，所述认证服务器中用于判断接收到的用户信息是否是认证用户包括：

采用所述预先部署的Kerberos Service对接收到的用户名和口令进行加密；

将对接收到的加密后的用户名和口令与已存储在所述预先建立的数据库中的加密后的用户名和口令进行比较；

当所述对接收到的加密后的用户名和口令与所述已存储在所述预先建立的数据库中的加密后的用户名和口令中的某一加密后的用户名和口令一致时，判断出接收到的用户信息是认证用户；

当所述对接收到的加密后的用户名和口令与所述已存储在所述预先建立的数据库中的加密后的用户名和口令中的任一加密后的用户名和口令均不一致时，验证出接收到的用户信息不是认证用户。

4.根据权利要求1所述的系统，其特征在于，所述认证服务器通过预先部署的LDAP服务Service将所述全部的用户权限按层次树状结构存储在LDAP目录中。

5.一种认证服务器，其特征在于，包括：密码管理单元、权限管理单元、收发单元、认证单元和处理单元；其中，

密码管理单元，用于将全部的用户信息存储在预先建立的数据库中；

权限管理单元，用于将全部的用户权限按层次树状结构存储在轻量目录访问协议LDAP目录中；

收发单元，用于当接收到访问服务器发送的用户信息时，将接收到的用户信息发送给认证单元；将生成的用户凭据发送给访问服务器和集群服务器；

认证单元，用于判断接收到的用户信息是否是认证用户；当判断出接收到的用户信息是认证用户时，通知处理单元；

处理单元，用于接收到来自匹配单元发送的通知，在LDAP目录中查找与该用户信息对

应的用户权限并根据查找到的用户权限生成用户凭据。

6.根据权利要求5所述的认证服务器，其特征在于，所述用户信息包括：用户名和口令；

所述密码管理单元，具体用于：

采用预先部署的网络认证协议Kerberos服务Service分别对每个用户的用户名和口令进行加密；

将加密后的每个用户的用户名和口令对应存储在所述预先建立的数据库中。

7.根据权利要求6所述的认证服务器，其特征在于，所述认证单元中用于判断接收到的用户信息是否是认证用户包括：

采用所述预先部署的Kerberos Service对接收到的用户名和口令进行加密；

将对接收到的加密后的用户名和口令与已存储在所述预先建立的数据库中的加密后的用户名和口令进行比较；

当所述对接收到的加密后的用户名和口令与所述已存储在所述预先建立的数据库中的加密后的用户名和口令中的某一加密后的用户名和口令一致时，判断出接收到的用户信息是认证用户；

当所述对接收到的加密后的用户名和口令与所述已存储在所述预先建立的数据库中的加密后的用户名和口令中的任一加密后的用户名和口令均不一致时，验证出接收到的用户信息不是认证用户。

8.一种控制访问权限的方法，其特征在于，包括：

认证服务器将全部的用户信息存储在预先建立的数据库中，以及将全部的用户权限按层次树状结构存储在轻量目录访问协议LDAP目录中；

当接收到访问服务器发送的用户信息时，认证服务器判断接收到的用户信息是否是认证用户；

当判断出接收到的用户信息是认证用户时，认证服务器在LDAP目录中查找与该用户信息对应的用户权限并根据查找到的用户权限生成用户凭据；

认证服务器将生成的用户凭据发送给访问服务器和集群服务器以供服务器集群接与访问服务器之间进行数据交互。

9.根据权利要求8所述的方法，其特征在于，所述用户信息包括：用户名和口令；

所述认证服务器将全部的用户信息存储在预先建立的数据库中的步骤包括：

采用预先部署的网络认证协议Kerberos服务Service分别对每个用户的用户名和口令进行加密；

将加密后的每个用户的用户名和口令对应存储在所述预先建立的数据库中。

10.根据权利要求9所述的方法，其特征在于，所述认证服务器判断接收到的用户信息是否是认证用户的步骤包括：

采用所述预先部署的Kerberos Service对接收到的用户名和口令进行加密；

将对接收到的加密后的用户名和口令与已存储在所述预先建立的数据库中的加密后的用户名和口令进行比较；

当所述对接收到的加密后的用户名和口令与所述已存储在所述预先建立的数据库中的加密后的用户名和口令中的某一加密后的用户名和口令一致时，判断出接收到的用户信息是认证用户；

当所述对接收到的加密后的用户名和口令与所述已存储在所述预先建立的数据库中的加密后的用户名和口令中的任一加密后的用户名和口令均不一致时，验证出接收到的用户信息不是认证用户。

# 一种控制访问权限的系统、认证服务器和方法

## 技术领域

[0001] 本发明实施例涉及但不限于云计算技术，尤指一种控制访问权限的系统、认证服务器和方法。

## 背景技术

[0002] 随着云计算应用的普及，服务器数量越来越多，服务器上的虚拟机数量和关联关系也日渐复杂，安全问题伴随着虚拟机存在的整个生命周期中，涵盖的内容贯穿产品设计、开发、测试、运维、基础设施(如，互联网数据中心(IDC，Internet Data Center)、内网、外网办公网)等各个方面。

[0003] 用户登录某一个IDC线上服务器以进行与服务器集群之间的数据交互。其中，对IDC线上服务器的用户权限需要进行合理、规范、统一的用户权限验证和管理。其中，常见的认证方式是按照机器的，即用户每次修改用户信息(用户信息包括用户名和口令)中的口令(密码)后，都需要对所有相关机器一一进行该用户的口令的修改以及根据修改后的用户信息调整用户信息与用户权限，密码权限管理混乱，并且容易遗漏。

## 发明内容

[0004] 本申请提供了一种控制访问权限的系统、认证服务器和方法，能够实现密码的统一管理以及权限的集中管理。

[0005] 为了达到本申请目的，本申请提供了一种控制访问权限的系统，包括：认证服务器、访问服务器和服务器集群；其中，

[0006] 认证服务器，用于将全部的用户信息存储在预先建立的数据库中；将全部的用户权限按层次树状结构存储在轻量目录访问协议LDAP目录中；当接收到访问服务器发送的用户信息时，判断接收到的用户信息是否是认证用户；当判断出接收到的用户信息是认证用户时，在LDAP目录中查找与该用户信息对应的用户权限并根据查找到的用户权限生成用户凭据；将生成的用户凭据发送给访问服务器与服务器集群；

[0007] 访问服务器，用于将用户输入的用户信息发送给认证服务器；接收认证服务器发送的用户凭据；根据接收到的用户凭据与服务器集群进行数据交互；

[0008] 服务器集群，用于接收到来自认证服务器发送的用户凭据，对该用户开放与该用户凭据对应的用户权限以与访问服务器进行数据交互。

[0009] 可选地，所述用户信息包括：用户名和口令；

[0010] 所述认证服务器中用于将全部的用户信息存储在预先建立的数据库中包括：

[0011] 采用预先部署的网络认证协议Kerberos服务Service分别对每个用户的用户名和口令进行加密；

[0012] 将加密后的每个用户的用户名和口令对应存储在所述预先建立的数据库中。

[0013] 可选地，所述认证服务器中用于判断接收到的用户信息是否是认证用户包括：

[0014] 采用所述预先部署的Kerberos Service对接收到的用户名和口令进行加密；

[0015] 将对接收到的加密后的用户名和口令与已存储在所述预先建立的数据库中的加密后的用户名和口令进行比较；

[0016] 当所述对接收到的加密后的用户名和口令与所述已存储在所述预先建立的数据库中的加密后的用户名和口令中的某一加密后的用户名和口令一致时，判断出接收到的用户信息是认证用户；

[0017] 当所述对接收到的加密后的用户名和口令与所述已存储在所述预先建立的数据库中的加密后的用户名和口令中的任一加密后的用户名和口令均不一致时，验证出接收到的用户信息不是认证用户。

[0018] 可选地，所述认证服务器通过预先部署的LDAP服务Service将所述全部的用户权限按层次树状结构存储在LDAP目录中。

[0019] 本申请还提供了一种认证服务器，包括：密码管理单元、权限管理单元、收发单元、认证单元和处理单元；其中，

[0020] 密码管理单元，用于将全部的用户信息存储在预先建立的数据库中；

[0021] 权限管理单元，用于将全部的用户权限按层次树状结构存储在轻量目录访问协议LDAP目录中；

[0022] 收发单元，用于当接收到访问服务器发送的用户信息时，将接收到的用户信息发送给认证单元；将生成的用户凭据发送给访问服务器和集群服务器；

[0023] 认证单元，用于判断接收到的用户信息是否是认证用户；当判断出接收到的用户信息是认证用户时，通知处理单元；

[0024] 处理单元，用于接收到来自匹配单元发送的通知，在LDAP目录中查找与该用户信息对应的用户权限并根据查找到的用户权限生成用户凭据。

[0025] 可选地，所述用户信息包括：用户名和口令；

[0026] 所述密码管理单元，具体用于：

[0027] 采用预先部署的网络认证协议Kerberos服务Service分别对每个用户的用户名和口令进行加密；

[0028] 将加密后的每个用户的用户名和口令对应存储在所述预先建立的数据库中。

[0029] 可选地，所述认证单元中用于判断接收到的用户信息是否是认证用户包括：

[0030] 采用所述预先部署的Kerberos Service对接收到的用户名和口令进行加密；

[0031] 将对接收到的加密后的用户名和口令与已存储在所述预先建立的数据库中的加密后的用户名和口令进行比较；

[0032] 当所述对接收到的加密后的用户名和口令与所述已存储在所述预先建立的数据库中的加密后的用户名和口令中的某一加密后的用户名和口令一致时，判断出接收到的用户信息是认证用户；

[0033] 当所述对接收到的加密后的用户名和口令与所述已存储在所述预先建立的数据库中的加密后的用户名和口令中的任一加密后的用户名和口令均不一致时，验证出接收到的用户信息不是认证用户。

[0034] 本申请还提供了一种控制访问权限的方法，包括：

[0035] 认证服务器将全部的用户信息存储在预先建立的数据库中，以及将全部的用户权限按层次树状结构存储在轻量目录访问协议LDAP目录中；

[0036] 当接收到访问服务器发送的用户信息时，认证服务器判断接收到的用户信息是否是认证用户；

[0037] 当判断出接收到的用户信息是认证用户时，认证服务器在LDAP目录中查找与该用户信息对应的用户权限并根据查找到的用户权限生成用户凭据；

[0038] 认证服务器将生成的用户凭据发送给访问服务器和集群服务器以供服务器集群接与访问服务器之间进行数据交互。

[0039] 可选地，所述用户信息包括：用户名和口令；

[0040] 所述认证服务器将全部的用户信息存储在预先建立的数据库中的步骤包括：

[0041] 采用预先部署的网络认证协议Kerberos服务Service分别对每个用户的用户名和口令进行加密；

[0042] 将加密后的每个用户的用户名和口令对应存储在所述预先建立的数据库中。

[0043] 可选地，所述认证服务器判断接收到的用户信息是否是认证用户的步骤包括：

[0044] 采用所述预先部署的Kerberos Service对接收到的用户名和口令进行加密；

[0045] 将对接收到的加密后的用户名和口令与已存储在所述预先建立的数据库中的加密后的用户名和口令进行比较；

[0046] 当所述对接收到的加密后的用户名和口令与所述已存储在所述预先建立的数据库中的加密后的用户名和口令中的某一加密后的用户名和口令一致时，判断出接收到的用户信息是认证用户；

[0047] 当所述对接收到的加密后的用户名和口令与所述已存储在所述预先建立的数据库中的加密后的用户名和口令中的任一加密后的用户名和口令均不一致时，验证出接收到的用户信息不是认证用户。

[0048] 本发明实施例包括：认证服务器将全部的用户信息存储在预先建立的数据库中，以及将全部的用户权限按层次树状结构存储在轻量目录访问协议(LDAP)目录中；当接收到访问服务器发送的用户信息时，认证服务器判断接收到的用户信息是否是认证用户；当判断出接收到的用户信息是认证用户时，认证服务器在LDAP目录中查找与该用户信息对应的用户权限并根据查找到的用户权限生成用户凭据；认证服务器将生成的用户凭据发送给访问服务器和集群服务器以供服务器集群接与访问服务器之间进行数据交互。本发明实施例中，通过认证服务器将全部的用户信息存储在预先建立的数据库中，以及将全部的用户权限按层次树状结构存储在LDAP目录中，实现了密码的统一管理以及权限的集中管理。

## 附图说明

[0049] 此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0050] 图1为本发明实施例控制访问权限的系统的架构图；

[0051] 图2为本发明实施例认证服务器的结构示意图；

[0052] 图3为本发明实施例控制访问权限的方法的流程图。

## 具体实施方式

[0053] 为使本发明的目的、技术方案和优点更加清楚明白，下文中将结合附图对本发明

的实施例进行详细说明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互任意组合。

[0054] 图1为本发明实施例控制访问权限的系统的架构图，如图1所示，包括：认证服务器、访问服务器和服务器集群。其中，

[0055] 认证服务器，用于将全部的用户信息存储在预先建立的数据库中；将全部的用户权限按层次树状结构存储在轻量目录访问协议(LDAP)目录中；当接收到访问服务器发送的用户信息时，判断接收到的用户信息是否是认证用户；当判断出接收到的用户信息是认证用户时，在LDAP目录中查找与该用户信息对应的用户权限并根据查找到的用户权限生成用户凭据；将生成的用户凭据发送给访问服务器与服务器集群。

[0056] 其中，本发明实施例用户信息包括：用户名和口令。

[0057] 其中，本发明实施例认证服务器中用于将全部的用户信息存储在预先建立的数据库中包括：

[0058] 采用预先部署的网络认证协议(Kerberos)服务(Service)分别对每个用户的用户名和口令进行加密；

[0059] 将加密后的每个用户的用户名和口令对应存储在预先建立的数据库中。

[0060] 需要说明的是，可以在认证服务器中预先部署Kerberos Service，Kerberos Service实现了用户信息的验证，关于如何部署Kerberos Service属于本领域技术人员所熟知的惯用技术手段，此处不再赘述，并不用来限制本申请。

[0061] 可选地，本发明实施例认证服务器通过预先部署的LDAP Service将全部的用户权限按层次树状结构存储在LDAP目录中。

[0062] 其中，本发明实施例LDAP Service可以预先部署在认证服务器中，LDAP Service实现了用户权限的管理与认证(验证)。需要说明的是，如何将LDAP Service部署在认证服务器中，属于本领域技术人员所熟知的惯用技术手段，此处不再赘述，并不用来限制本申请。

[0063] 例如，本发明实施例认证服务器可以按照域/组织/角色/人员这样的层级建立结构进行权限划分管理，所有的用户权限按层次树状结构存储在认证服务器上的LDAP目录中，实现了权限集中管理。

[0064] 其中，本发明实施例认证服务器中用于判断接收到的用户信息是否是认证用户包括：

[0065] 采用预先部署的Kerberos Service对接收到的用户名和口令进行加密；

[0066] 将对接收到的加密后的用户名和口令与已存储在预先建立的数据库中的加密后的用户名和口令进行比较；

[0067] 当对接收到的加密后的用户名和口令与已存储在预先建立的数据库中的加密后的用户名和口令中的某一加密后的用户名和口令一致时，判断出接收到的用户信息是认证用户；

[0068] 当对接收到的加密后的用户名和口令与已存储在预先建立的数据库中的加密后的用户名和口令中的任一加密后的用户名和口令均不一致时，验证出接收到的用户信息不是认证用户。

[0069] 其中，本发明实施例对接收到的加密后的用户名和口令是指对接收到的用户名和

口令分别采用预先部署的Kerberos Service加密后的用户名和口令。

[0070] 其中，本发明实施例认证用户是合格用户，即拥有一定用户权限的合格用户。

[0071] 可选地，本发明实施例认证服务器，还用于当监测到某一用户信息更改时，通过预先部署的Kerberos Service将已存储的该用户信息更新为更改后的用户信息。

[0072] 其中，本发明实施例用户信息更改包括口令的更改。

[0073] 其中，本发明实施例认证服务器中用于通过预先部署的Kerberos Service将已存储的该用户信息更新为更改后的用户信息：

[0074] 通过预先部署的Kerberos Service对更改的用户信息的用户名和已更改的口令进行加密；

[0075] 在预先建立的数据库中查找与对加密后的更改的用户信息的用户名对应已存储的加密后的口令；

[0076] 将查找到的加密后的口令替换为加密后的已更改的口令。

[0077] 其中，本发明实施例系统包括一个或两个认证服务器。

[0078] 其中，当本发明实施例系统包括一个认证服务器时，Kerberos Service和LDAP Service均部署在该认证服务器中；当本发明实施例系统包括两个认证服务器时，Kerberos Service和LDAP Service分别部署在不同的认证服务器中，且两个认证服务器通过LVS+Keepalived(一种实现LINUX虚拟机负责均衡的方式。其中，LVS是一个开源的软件，可以实现LINUX平台下的简单负载均衡，LVS是Linux Virtual Server的缩写，意思是Linux虚拟服务器；Keepalived是运行在LVS之上，它的主要功能是实现真实机的故障隔离及负载均衡器间的失败切换，提高系统的可用性)的方案实现高可用性，同时保证Kerberos Service和LDAP Service的高可用性。

[0079] 例如，两个认证服务器分别为第一认证服务器和第二认证服务器，可以在第一认证服务器上预先部署Kerberos Service，在第二认证服务器上预先部署LDAP Service；也可以在第一认证服务器上预先部署LDAP Service，在第二认证服务器上预先部署Kerberos Service。

[0080] 需要说明的是，如何通过LVS+Keepalived的的方案实现高可用性属于本领域技术人员所熟知的惯用技术手段，此处不再赘述，并不用来限制本申请。

[0081] 访问服务器，用于将用户输入的用户信息发送给认证服务器；接收认证服务器发送的用户凭据；根据接收到的用户凭据与服务器集群进行数据交互。

[0082] 需要说明的是，如何根据用户权限生成用户凭据属于本领域技术人员所熟知的惯用技术手段，此处不再赘述，并不用来限制本申请。例如，用户凭据可以是包含用户信息和用户权限的令牌(token)字符码等。

[0083] 服务器集群，用于接收到来自认证服务器发送的用户凭据，对该用户开放与该用户凭据对应的用户权限以与访问服务器进行数据交互。

[0084] 其中，本发明实施例服务器集群可以理解为是各种资源池，其可以提供各种业务功能。

[0085] 图2为本发明实施例认证服务器的结构示意图，如图2所示，包括：密码管理单元、权限管理单元、收发单元、认证单元和处理单元。其中，

[0086] 密码管理单元，用于将全部的用户信息存储在预先建立的数据库中。

[0087] 其中，本发明实施例用户信息包括：用户名和口令。

[0088] 其中，本发明实施例密码管理单元，具体用于：

[0089] 采用预先部署的网络认证协议(Kerberos)服务(Service)分别对每个用户的用户名和口令进行加密；

[0090] 将加密后的每个用户的用户名和口令对应存储在预先建立的数据库中。

[0091] 其中，本发明实施例Kerberos Service可以预先部署在认证服务器中。需要说的是，关于如何部署Kerberos Service属于本领域技术人员所熟知的惯用技术手段，此处不再赘述，并不用来限制本申请。

[0092] 可选地，本发明实施例密码管理单元，还用于：

[0093] 当监测到某一用户信息更改时，通过预先部署的Kerberos Service将已存储的该用户信息更新为更改后的用户信息。

[0094] 其中，本发明实施例用户信息更改包括口令的更改。

[0095] 其中，本发明实施例密码管理单元中用于通过预先部署的Kerberos Service将已存储的该用户信息更新为更改后的用户信息：

[0096] 通过预先部署的Kerberos Service对更改的用户信息的用户名和已更改的口令进行加密；

[0097] 在预先建立的数据库中查找与对加密后的更改的用户信息的用户名对应已存储的加密后的口令；

[0098] 将查找到的加密后的口令替换为加密后的已更改的口令。

[0099] 权限管理单元，用于将全部的用户权限按层次树状结构存储在轻量目录访问协议(LDAP)目录中。

[0100] 可选地，本发明实施例权限管理单元可以通过预先部署的LDAP Service将全部的用户权限按层次树状结构存储在LDAP目录中。

[0101] 例如，本发明实施例认证服务器可以按照域/组织/角色/人员这样的层级建立结构进行权限划分管理，所有的用户权限按层次树状结构存储在认证服务器上的LDAP目录中，实现了权限集中管理。

[0102] 收发单元，用于当接收到访问服务器发送的用户信息时，将接收到的用户信息发送给认证单元；将生成的用户凭据发送给访问服务器和集群服务器。

[0103] 其中，本发明实施例访问服务器是用户登录互联网数据中心(IDC，Internet Data Center)的某一个线上服务器，用户通过登录(通过在该线上服务器输入用户信息)该线上服务器可以与服务器集群进行数据交互。

[0104] 其中，本发明实施例服务器集群可以理解为是各种资源池，其可以提供各种业务功能。

[0105] 认证单元，用于判断接收到的用户信息是否是认证用户；当判断出接收到的用户信息是认证用户时，通知处理单元。

[0106] 其中，认证单元中用于判断接收到的用户信息是否是认证用户包括：

[0107] 采用预先部署的Kerberos Service对接收到的用户名和口令进行加密；

[0108] 将对接收到的加密后的用户名和口令与已存储在预先建立的数据库中的加密后的用户名和口令进行比较；

[0109] 当对接收到的加密后的用户名和口令与已存储在预先建立的数据库中的加密后的用户名和口令中的某一加密后的用户名和口令一致时，判断出接收到的用户信息是认证用户；

[0110] 当对接收到的加密后的用户名和口令与已存储在预先建立的数据库中的加密后的用户名和口令中的任一加密后的用户名和口令均不一致时，验证出接收到的用户信息不是认证用户。

[0111] 其中，本发明实施例认证用户是合格用户，即拥有一定用户权限的合格用户。

[0112] 其中，本发明实施例对接收到的加密后的用户名和口令是指对接收到的用户名和口令分别采用预先部署的Kerberos Service加密后的用户名和口令。

[0113] 处理单元，用于接收到来自匹配单元发送的通知，在LDAP目录中查找与该用户信息对应的用户权限并根据查找到的用户权限生成用户凭据。

[0114] 图3为本发明实施例控制访问权限的方法的流程图，如图3所示，包括：

[0115] 步骤301：认证服务器将全部的用户信息存储在预先建立的数据库中，以及将全部的用户权限按层次树状结构存储在轻量目录访问协议(LDAP)目录中。

[0116] 其中，本发明实施例用户信息包括：用户名和口令。

[0117] 其中，本发明实施例认证服务器将全部的用户信息存储在预先建立的数据库中的步骤包括：

[0118] 采用预先部署的网络认证协议(Kerberos)服务(Service)分别对每个用户的用户名和口令进行加密；

[0119] 将加密后的每个用户的用户名和口令对应存储在预先建立的数据库中。

[0120] 其中，本发明实施例Kerberos Service可以预先部署在认证服务器中，Kerberos Service实现了密码的统一管理。需要说明的是，如何将Kerberos Service部署在认证服务器中，属于本领域技术人员所熟知的惯用技术手段，此处不再赘述，并不用来限制本申请。

[0121] 可选地，本发明实施例认证服务器可以通过预先部署的LDAP Service将全部的用户权限按层次树状结构存储在LDAP目录中。

[0122] 其中，本发明实施例LDAP Service可以预先部署在认证服务器中，LDAP Service实现了用户权限的管理与认证(验证)。需要说明的是，如何将LDAP Service部署在认证服务器中，属于本领域技术人员所熟知的惯用技术手段，此处不再赘述，并不用来限制本申请。

[0123] 例如，本发明实施例认证服务器可以按照域/组织/角色/人员这样的层级建立结构进行权限划分管理，所有的用户权限按层次树状结构存储在认证服务器上的LDAP目录中，实现了权限集中管理。

[0124] 其中，本发明实施例系统包括一个或两个认证服务器。

[0125] 其中，当本发明实施例系统包括一个认证服务器时，Kerberos Service和LDAP Service均部署在该认证服务器中；当本发明实施例系统包括两个认证服务器时，Kerberos Service和LDAP Service分别部署在不同的认证服务器中，且两个认证服务器通过LVS+Keepalived(一种实现LINUX虚拟机负责均衡的方式。其中，LVS是一个开源的软件，可以实现LINUX平台下的简单负载均衡，LVS是Linux Virtual Server的缩写，意思是Linux虚拟服务器；Keepalived是运行在LVS之上，它的主要功能是实现真实机的故障隔离及负载均衡器

间的失败切换，提高系统的可用性)的方案实现高可用性，同时保证Kerberos Service和LDAP Service的高可用性。

[0126] 例如，两个认证服务器分别为第一认证服务器和第二认证服务器，可以在第一认证服务器上预先部署Kerberos Service，在第二认证服务器上预先部署LDAP Service；也可以在第一认证服务器上预先部署LDAP Service，在第二认证服务器上预先部署Kerberos Service。

[0127] 需要说明的是，如何通过LVS+Keepalived的的方案实现高可用性属于本领域技术人员所熟知的惯用技术手段，此处不再赘述，并不用来限制本申请。

[0128] 步骤302：当接收到访问服务器发送的用户信息时，认证服务器判断接收到的用户信息是否是认证用户。

[0129] 其中，本发明实施例认证服务器判断接收到的用户信息是否是认证用户的步骤包括：

[0130] 采用预先部署的Kerberos Service对接收到的用户名和口令进行加密；

[0131] 将对接收到的加密后的用户名和口令与已存储在预先建立的数据库中的加密后的用户名和口令进行比较；

[0132] 当对接收到的加密后的用户名和口令与已存储在预先建立的数据库中的加密后的用户名和口令中的某一加密后的用户名和口令一致时，判断出接收到的用户信息是认证用户；

[0133] 当对接收到的加密后的用户名和口令与已存储在预先建立的数据库中的加密后的用户名和口令中的任一加密后的用户名和口令均不一致时，验证出接收到的用户信息不是认证用户。

[0134] 其中，本发明实施例认证用户是合格用户，即拥有一定用户权限的合格用户。

[0135] 其中，本发明实施例对接收到的加密后的用户名和口令是指对接收到的用户名和口令分别采用预先部署的Kerberos Service加密后的用户名和口令。

[0136] 可选地，在步骤301之后，在步骤302之前，本发明实施例方法还包括：

[0137] 访问服务器接收到用户输入的用户信息，并将用户输入的用户信息发送给认证服务器。

[0138] 其中，本发明实施例访问服务器是用户登录互联网数据中心(IDC，Internet Data Center)的某一个线上服务器，用户通过登录(通过在该线上服务器输入用户信息)该线上服务器可以与服务器集群进行数据交互。

[0139] 步骤303：当判断出接收到的用户信息是认证用户时，认证服务器在LDAP目录中查找与该用户信息对应的用户权限并根据查找到的用户权限生成用户凭据。

[0140] 步骤304：认证服务器将生成的用户凭据发送给访问服务器和集群服务器以供服务器集群接与访问服务器之间进行数据交互。

[0141] 其中，本发明实施例服务器集群可以理解为是各种资源池，其可以提供各种业务功能。

[0142] 其中，本发明实施例步骤304包括：

[0143] 认证服务器将生成的用户凭据发送给访问服务器和集群服务器；

[0144] 服务器集群接收到来自认证服务器发送的用户凭据，对该用户开放与该用户凭据

对应的用户权限以与访问服务器进行数据交互。

[0145] 需要说明的是，如何根据用户权限生成用户凭据属于本领域技术人员所熟知的惯用技术手段，此处不再赘述，并不用来限制本申请。例如，用户凭据可以是包含用户信息和用户权限的token字符码等。

[0146] 可选地，当认证服务器监测到某一用户信息更改时，本发明实施例方法还包括：

[0147] 认证服务器通过预先部署的Kerberos Service将已存储的该用户信息更新为更改后的用户信息。

[0148] 其中，本发明实施例用户信息更改包括口令的更改。

[0149] 其中，本发明实施例认证服务器通过预先部署的Kerberos Service将已存储的该用户信息更新为更改后的用户信息的步骤包括：

[0150] 通过预先部署的Kerberos Service对更改的用户信息的用户名和已更改的口令进行加密；

[0151] 在预先建立的数据库中查找与对加密后的更改的用户信息的用户名对应已存储的加密后的口令；

[0152] 将查找到的加密后的口令替换为加密后的已更改的口令。

[0153] 本发明实施方式中，通过认证服务器将全部的用户信息存储在预先建立的数据库中，以及将全部的用户权限按层次树状结构存储在轻量目录访问协议LDAP目录中，实现了密码的统一管理以及权限的集中管理。

[0154] 需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者装置不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者装置所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。

[0155] 上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0156] 本领域普通技术人员可以理解上述方法中的全部或部分步骤可通过程序来指令相关硬件(例如处理器)完成，所述程序可以存储于计算机可读存储介质中，如只读存储器、磁盘或光盘等。可选地，上述实施例的全部或部分步骤也可以使用一个或多个集成电路来实现。相应地，上述实施例中的各模块/单元可以采用硬件的形式实现，例如通过集成电路来实现其相应功能，也可以采用软件功能模块的形式实现，例如通过处理器执行存储于存储器中的程序/指令来实现其相应功能。本发明不限制于任何特定形式的硬件和软件的结合。

[0157] 以上仅为本申请的优选实施例，并非因此限制本申请的专利范围，凡是利用本申请说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本申请的专利保护范围内。

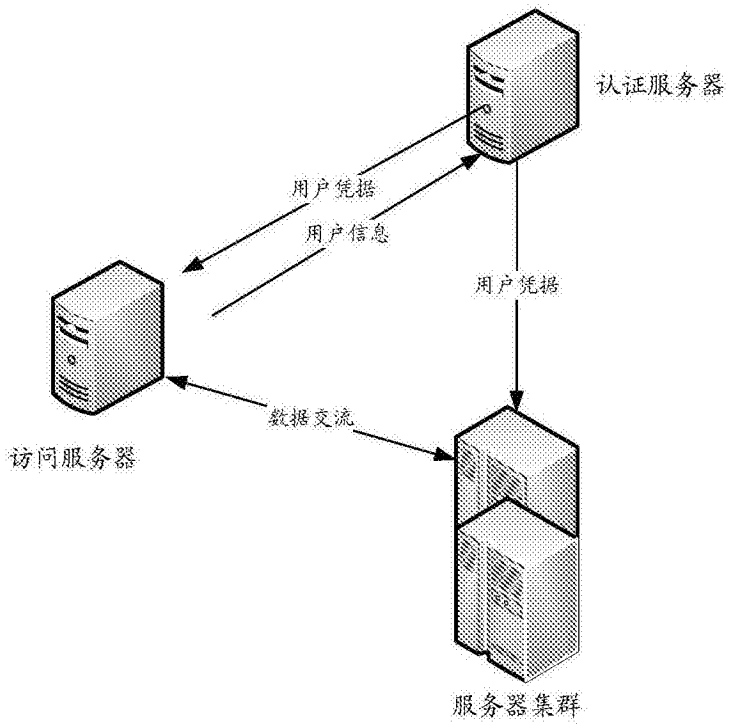

认证服务器
用户凭据
用户信息
用户凭据
数据交流
访问服务器
服务器集群

图1

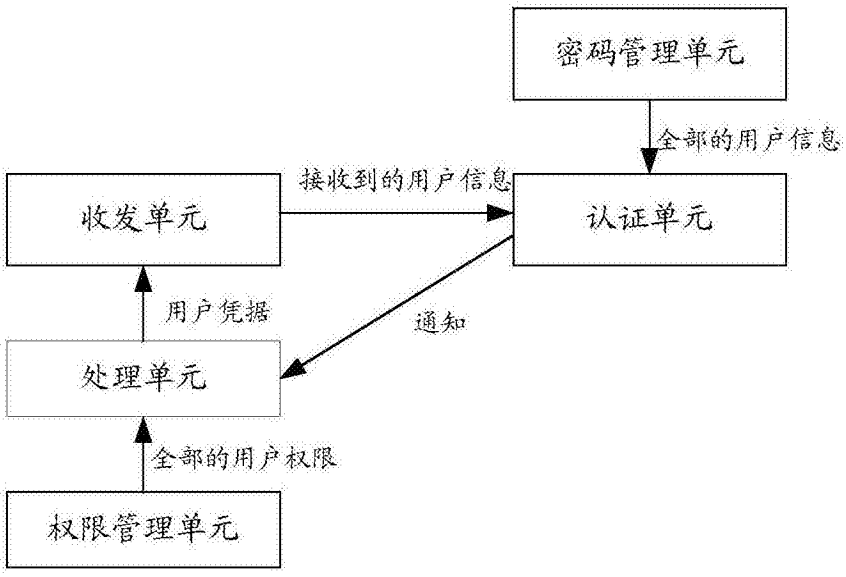

密码管理单元
全部的用户信息
接收到的用户信息
收发单元
认证单元
用户凭据
通知
处理单元
全部的用户权限
权限管理单元

图2

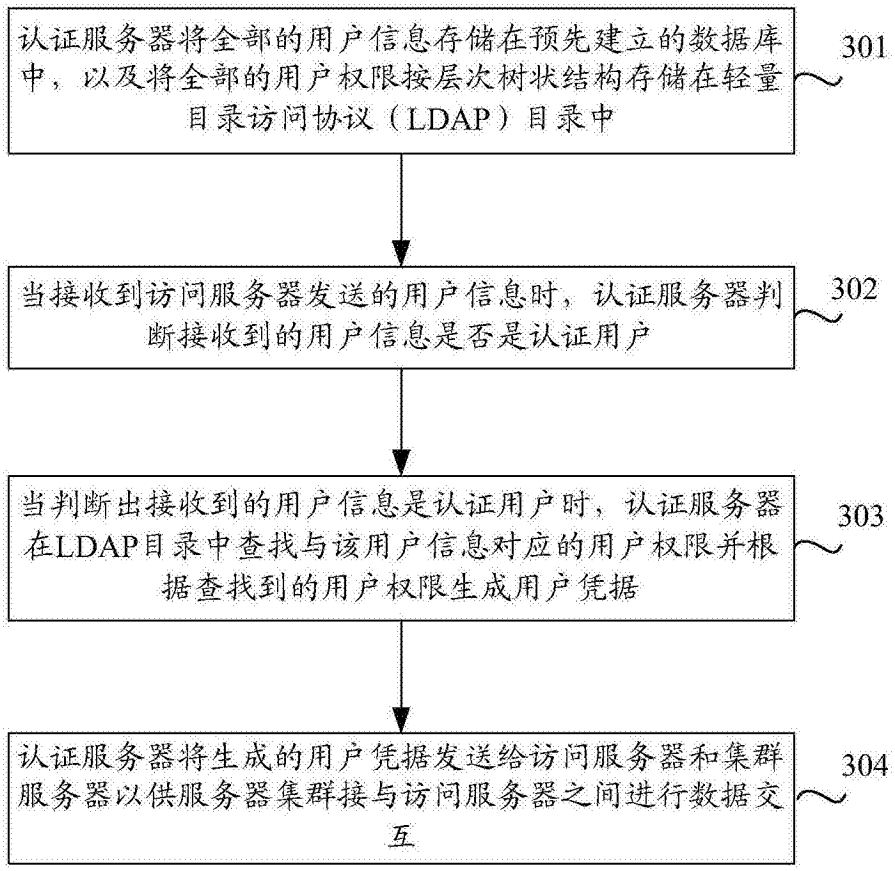

认证服务器将全部的用户信息存储在预先建立的数据库中，以及将全部的用户权限按层次树状结构存储在轻量目录访问协议（LDAP）目录中
301
当接收到访问服务器发送的用户信息时，认证服务器判断接收到的用户信息是否是认证用户
302
当判断出接收到的用户信息是认证用户时，认证服务器在LDAP目录中查找与该用户信息对应的用户权限并根据查找到的用户权限生成用户凭据
303
认证服务器将生成的用户凭据发送给访问服务器和集群服务器以供服务器集群接与访问服务器之间进行数据交互
304

图3