



(12)发明专利申请

(10)申请公布号 CN 105933379 A

(43)申请公布日 2016. 09. 07

(21)申请号 201610203775.8

(22)申请日 2016.04.01

(71)申请人 浪潮电子信息产业股份有限公司
地址 250100 山东省济南市高新区浪潮路
1036号

(72)发明人 邸双朋

(74)专利代理机构 济南信达专利事务所有限公
司 37100

代理人 李世喆

(51)Int.Cl.

H04L 29/08(2006.01)

H04L 12/24(2006.01)

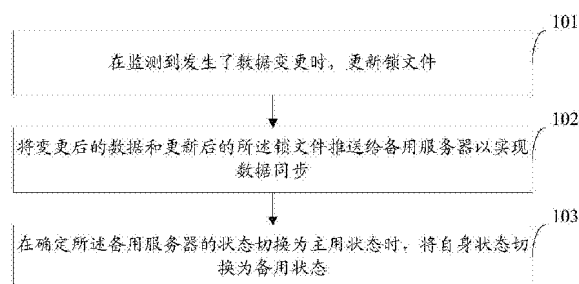
权利要求书2页 说明书8页 附图4页

(54)发明名称

一种业务处理方法、设备及系统

(57)摘要

本发明提供了一种业务处理方法、设备及系统,其中方法包括:在监测到发生了数据变更时,更新锁文件;将变更后的数据和更新后的所述锁文件推送给备用服务器以实现数据同步;在确定所述备用服务器的状态切换为主用状态时,将自身状态切换为备用状态。根据本方案,在主用服务器中发生了数据变更后,直接将变更后的数据推送给备用服务器以实现数据同步,为了保证业务处理的正常运行,可以利用锁文件确定主用服务器的故障与否,并在主用服务器发生故障时,备用服务器将自身状态切换为主用状态,主用服务器将自身状态切换为备用状态,从而保证了主用服务器和备用服务器的正常工作。



1. 一种业务处理方法,其特征在于,应用于主用服务器,所述方法包括:

在监测到发生了数据变更时,更新锁文件;

将变更后的数据和更新后的所述锁文件推送给备用服务器以实现数据同步;

在确定所述备用服务器的状态切换为主用状态时,将自身状态切换为备用状态。

2. 根据权利要求1所述的方法,其特征在于,

进一步包括:配置同步目录和同步密钥;

进一步包括:监控所述同步目录中每一个目录项所对应的数据,并在监测到目标目录项发生了数据变更时,则确定监测到发生了数据变更;

所述将变更后的数据推送给备用服务器,包括:将所述目标目录项以及对应的变更后的数据、所述同步密钥推送给所述备用服务器,以使所述备用服务器在验证所述同步密钥正确时,根据所述变更后的数据对所述目标目录项的数据进行同步更新。

3. 一种业务处理方法,其特征在于,应用于备用服务器,预先设定目标时间段,所述方法包括:

接收主用服务器推送的变更后的数据和锁文件;

同步更新主用服务器推送的变更后的数据,并存储当前接收到的锁文件;

将当前接收到的锁文件与距离当前的所述目标时间段内接收到的所有锁文件进行比较,在比较结果包括当前接收到的锁文件与该所有锁文件均相同时,则确定所述主用服务器发生故障;

将自身状态切换为主用状态,并将该切换信息通知给所述主用服务器,以使所述主用服务器将其状态切换为备用状态。

4. 根据权利要求3所述的方法,其特征在于,

进一步包括:配置同步目录和同步密钥;

所述同步更新主用服务器推送的变更后的数据,包括:根据所述同步密钥对所述主用服务器推送的数据中携带的密钥进行验证,并在验证通过时,根据所述主用服务器推送的目标目录项以及该目标目录项对应的变更后的数据,将该变更后的数据更新到所述同步目录中的所述目标目录项中。

5. 一种主用服务器,其特征在于,包括:

监测单元,用于监测是否发生了数据变更,并在监测到发生了数据变更时触发更新单元执行相应操作;

所述更新单元,用于更新锁文件;

推送单元,用于将变更后的数据和更新后的所述锁文件推送给备用服务器以实现数据同步;

切换单元,用于在确定所述备用服务器的状态切换为主用状态时,将自身状态切换为备用状态。

6. 根据权利要求5所述的主用服务器,其特征在于,

进一步包括:配置单元,用于配置同步目录和同步密钥;

所述监测单元,具体用于监控所述同步目录中每一个目录项所对应的数据,并在监测到目标目录项发生了数据变更时,则确定监测到发生了数据变更;

所述推送单元,具体用于将所述目标目录项以及对应的变更后的数据、所述同步密钥

推送给所述备用服务器,以使所述备用服务器在验证所述同步密钥正确时,根据所述变更后的数据对所述目标目录项的数据进行同步更新。

7.一种备用服务器,其特征在于,包括:

设定单元,用于设定目标时间段;

接收单元,用于接收主用服务器推送的变更后的数据和锁文件;

同步更新单元,用于同步更新主用服务器推送的变更后的数据;

存储单元,用于存储当前接收到的锁文件;

比较单元,用于将当前接收到的锁文件与距离当前的所述目标时间段内接收到的所有锁文件进行比较,在比较结果包括当前接收到的锁文件与该所有锁文件均相同时,则确定所述主用服务器发生故障;

处理单元,用于将自身状态切换为主用状态,并将该切换信息通知给所述主用服务器,以使所述主用服务器将其状态切换为备用状态。

8.根据权利要求7所述的备用服务器,其特征在于,

进一步包括:配置单元,用于配置同步目录和同步密钥;

所述同步更新单元,具体用于根据所述同步密钥对所述主用服务器推送的数据中携带的密钥进行验证,并在验证通过时,根据所述主用服务器推送的目标目录项以及该目标目录项对应的变更后的数据,将该变更后的数据更新到所述同步目录中的所述目标目录项中。

9.一种业务处理系统,其特征在于,包括上述权利要求5或6所述的主用服务器和上述权利要求7或8所述的备用服务器。

一种业务处理方法、设备及系统

技术领域

[0001] 本发明涉及通信技术领域,特别涉及一种业务处理方法、设备及系统。

背景技术

[0002] 在HPC(High Performance Computing,高性能计算)集群中,作业调度服务是一个关键服务,一般情况下,利用两个服务器与HPC集群相连,使用其中一个服务器对HPC集群进行作业调度,在当前该服务器出现故障时,切换到另一个服务器继续对HPC集群进行作业调度,在这种情况下,需要保证两个服务器中数据的一致性。

[0003] 目前,主用服务器和备用服务器将NFS(Network File System,网络文件系统)共享存储挂载在本地目录中,在主用服务器中发生数据更新时,将该数据更新到该NFS共享存储中,从而实现备用服务器中数据的更新,以达到主用服务器和备用服务器之间数据的一致性。

[0004] 然而,在NFS共享存储出现故障时,会导致主用服务器和备用服务器都无法正常工作,从而影响整个集群的业务。

发明内容

[0005] 本发明实施例提供了一种业务处理方法、设备及系统,以保证主用服务器和备用服务器的正常工作。

[0006] 第一方面,本发明实施例提供了一种业务处理方法,应用于主用服务器,所述方法包括:

[0007] 在监测到发生了数据变更时,更新锁文件;

[0008] 将变更后的数据和更新后的所述锁文件推送给备用服务器以实现数据同步;

[0009] 在确定所述备用服务器的状态切换为主用状态时,将自身状态切换为备用状态。

[0010] 优选地,进一步包括:配置同步目录和同步密钥;

[0011] 进一步包括:监控所述同步目录中每一个目录项所对应的数据,并在监测到目标目录项发生了数据变更时,则确定监测到发生了数据变更;

[0012] 所述将变更后的数据推送给备用服务器,包括:将所述目标目录项以及对应的变更后的数据、所述同步密钥推送给所述备用服务器,以使所述备用服务器在验证所述同步密钥正确时,根据所述变更后的数据对所述目标目录项的数据进行同步更新。

[0013] 第二方面,本发明实施例还提供了一种业务处理方法,应用于备用服务器,预先设定目标时间段,所述方法包括:

[0014] 接收主用服务器推送的变更后的数据和锁文件;

[0015] 同步更新主用服务器推送的变更后的数据,并存储当前接收到的锁文件;

[0016] 将当前接收到的锁文件与距离当前的所述目标时间段内接收到的所有锁文件进行比较,在比较结果包括当前接收到的锁文件与该所有锁文件均相同时,则确定所述主用服务器发生故障;

[0017] 将自身状态切换为主用状态,并将该切换信息通知给所述主用服务器,以使所述主用服务器将其状态切换为备用状态。

[0018] 优选地,进一步包括:配置同步目录和同步密钥;

[0019] 所述同步更新主用服务器推送的变更后的数据,包括:根据所述同步密钥对所述主用服务器推送的数据中携带的密钥进行验证,并在验证通过时,根据所述主用服务器推送的目标目录项以及该目标目录项对应的变更后的数据,将该变更后的数据更新到所述同步目录中的所述目标目录项中。

[0020] 第三方面,本发明实施例还提供了一种主用服务器,包括:

[0021] 监测单元,用于监测是否发生了数据变更,并在监测到发生了数据变更时触发更新单元执行相应操作;

[0022] 所述更新单元,用于更新锁文件;

[0023] 推送单元,用于将变更后的数据和更新后的所述锁文件推送给备用服务器以实现数据同步;

[0024] 切换单元,用于在确定所述备用服务器的状态切换为主用状态时,将自身状态切换为备用状态。

[0025] 优选地,进一步包括:配置单元,用于配置同步目录和同步密钥;

[0026] 所述监测单元,具体用于监控所述同步目录中每一个目录项所对应的数据,并在监测到目标目录项发生了数据变更时,则确定监测到发生了数据变更;

[0027] 所述推送单元,具体用于将所述目标目录项以及对应的变更后的数据、所述同步密钥推送给所述备用服务器,以使所述备用服务器在验证所述同步密钥正确时,根据所述变更后的数据对所述目标目录项的数据进行同步更新。

[0028] 第四方面,本发明实施例还提供了一种备用服务器,包括:

[0029] 设定单元,用于设定目标时间段;

[0030] 接收单元,用于接收主用服务器推送的变更后的数据和锁文件;

[0031] 同步更新单元,用于同步更新主用服务器推送的变更后的数据;

[0032] 存储单元,用于存储当前接收到的锁文件;

[0033] 比较单元,用于将当前接收到的锁文件与距离当前的所述目标时间段内接收到的所有锁文件进行比较,在比较结果包括当前接收到的锁文件与该所有锁文件均相同时,则确定所述主用服务器发生故障;

[0034] 处理单元,用于将自身状态切换为主用状态,并将该切换信息通知给所述主用服务器,以使所述主用服务器将其状态切换为备用状态。

[0035] 优选地,进一步包括:配置单元,用于配置同步目录和同步密钥;

[0036] 所述同步更新单元,具体用于根据所述同步密钥对所述主用服务器推送的数据中携带的密钥进行验证,并在验证通过时,根据所述主用服务器推送的目标目录项以及该目标目录项对应的变更后的数据,将该变更后的数据更新到所述同步目录中的所述目标目录项中。

[0037] 第五方面,本发明实施例还提供了一种业务处理系统,包括上述的主用服务器和上述的备用服务器。

[0038] 本发明实施例提供了一种业务处理方法、设备及系统,在主用服务器中发生了数

据变更后,直接将变更后的数据推送给备用服务器以实现数据同步,为了保证业务处理的正常运行,可以利用锁文件确定主用服务器的故障与否,并在主用服务器发生故障时,备用服务器将自身状态切换为主用状态,主用服务器将自身状态切换为备用状态,从而保证了主用服务器和备用服务器的正常工作。

附图说明

[0039] 为了更清楚地说明本发明实施例或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图是本发明的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

[0040] 图1是本发明一个实施例提供的一种方法流程图;

[0041] 图2是本发明一个实施例提供的另一种方法流程图;

[0042] 图3是本发明一个实施例提供的又一种方法流程图;

[0043] 图4是本发明一个实施例提供的一种主用服务器的结构示意图;

[0044] 图5是本发明一个实施例提供的另一种主用服务器的结构示意图;

[0045] 图6是本发明一个实施例提供的一种备用服务器的结构示意图;

[0046] 图7是本发明一个实施例提供的另一种备用服务器的结构示意图;

[0047] 图8是本发明一个实施例提供的业务处理系统结构示意图。

具体实施方式

[0048] 为使本发明实施例的目的、技术方案和优点更加清楚,下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例是本发明一部分实施例,而不是全部的实施例,基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动的前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0049] 请参考图1,本发明实施例提供了一种业务处理方法,应用于主用服务器,该方法可以包括以下步骤:

[0050] 步骤101:在监测到发生了数据变更时,更新锁文件。

[0051] 步骤102:将变更后的数据和更新后的所述锁文件推送给备用服务器以实现数据同步。

[0052] 步骤103:在确定所述备用服务器的状态切换为主用状态时,将自身状态切换为备用状态。

[0053] 根据本发明实施例提供的方案,在主用服务器中发生了数据变更后,直接将变更后的数据推送给备用服务器以实现数据同步,为了保证业务处理的正常运行,可以利用锁文件确定主用服务器的故障与否,并在主用服务器发生故障时,备用服务器将自身状态切换为主用状态,主用服务器将自身状态切换为备用状态,从而保证了主用服务器和备用服务器的正常工作。

[0054] 在本发明一个实施例中,为了降低主用服务器和备用服务器之间数据传输的数据量,以及提高数据同步的安全性,可以进一步包括:配置同步目录和同步密钥;

[0055] 进一步包括:监控所述同步目录中每一个目录项所对应的数据,并在监测到目标

目录项发生了数据变更时,则确定监测到发生了数据变更;

[0056] 所述将变更后的数据推送给备用服务器,包括:将所述目标目录项以及对应的变更后的数据、所述同步密钥推送给所述备用服务器,以使所述备用服务器在验证所述同步密钥正确时,根据所述变更后的数据对所述目标目录项的数据进行同步更新。

[0057] 根据本发明实施例提供的方案,可以利用同步密钥对数据推送方进行验证,以提高数据同步的安全性,防止恶意程序对备用服务器进行攻击。以通过配置同步目录,在同步目录中某几项发生数据变更的,可以只将发生数据变更的那几项同步给备用服务器即可,无需每次都把所有数据同步一遍,从而可以提高数据的传输效率。

[0058] 请参考图2,本发明实施例提供了一种业务处理方法,应用于备用服务器,该方法可以包括以下步骤:

[0059] 步骤201:设定目标时间段;

[0060] 步骤202:接收主用服务器推送的变更后的数据和锁文件;

[0061] 步骤203:同步更新主用服务器推送的变更后的数据,并存储当前接收到的锁文件;

[0062] 步骤204:将当前接收到的锁文件与距离当前的所述目标时间段内接收到的所有锁文件进行比较,在比较结果包括当前接收到的锁文件与该所有锁文件均相同时,则确定所述主用服务器发生故障;

[0063] 步骤205:将自身状态切换为主用状态,并将该切换信息通知给所述主用服务器,以使所述主用服务器将其状态切换为备用状态。

[0064] 根据本发明实施例提供的方案,通过接收主用服务器推送的变更后的数据以实现数据同步,从而无需考虑共享存储的故障问题,可以进一步提高了数据同步的安全性,为了保证业务处理的正常运行,可以利用锁文件确定主用服务器的故障与否,并在主用服务器发生故障时,备用服务器将自身状态切换为主用状态,主用服务器将自身状态切换为备用状态,从而保证了主用服务器和备用服务器的正常工作。

[0065] 在本发明一个实施例中,为了降低主用服务器和备用服务器之间数据传输的数据量,以及提高数据同步的安全性,进一步包括:配置同步目录和同步密钥;

[0066] 所述同步更新主用服务器推送的变更后的数据,包括:根据所述同步密钥对所述主用服务器推送的数据中携带的密钥进行验证,并在验证通过时,根据所述主用服务器推送的目标目录项以及该目标目录项对应的变更后的数据,将该变更后的数据更新到所述同步目录中的所述目标目录项中。

[0067] 根据本发明实施例提供的方案,可以利用同步密钥对数据推送方进行验证,以提高数据同步的安全性,防止恶意程序对备用服务器进行攻击。以通过配置同步目录,在同步目录中某几项发生数据变更的,可以只将发生数据变更的那几项同步给备用服务器即可,无需每次都把所有数据同步一遍,从而可以提高数据的传输效率。

[0068] 为使本发明的目的、技术方案和优点更加清楚,下面结合附图及具体实施例对本发明作进一步地详细描述。

[0069] 如图3所示,本发明实施例提供了一种业务处理方法,该方法可以包括以下步骤:

[0070] 步骤301:针对服务器mu01和服务器mu02进行主备状态的配置。

[0071] 为了保证业务处理的正常运行,尤其是在HPC集群中,可以采用两个服务器对HPC

集群进行作业调度,以保证其中一个服务器发生故障时,另一个服务器可以替代该故障的服务器进行工作。

[0072] 在初始状态下,对于服务器mu01和服务器mu02,可以为服务器mu01配置为主用状态以作为主用服务器,为服务器mu02配置为备用状态以作为备用服务器。

[0073] 步骤302:对主用服务器mu01进行配置文件的配置。

[0074] 在本发明一个实施例中,可以对主用服务器mu01可以进行如下配置:配置同步目录和同步密钥。

[0075] 其中,该同步目录可以包括多个目录项,用于表征主用服务器需要对该同步目录中所包括的各个目录项进行监控。

[0076] 其中,同步密钥是用来在主用服务器和备用服务器之间实现数据同步时对主用服务器的身份进行验证的。由于服务器之间在进行数据交互时,若经过身份验证,容易遭受到恶意程度或者恶意设备的攻击,给服务器的数据安全造成威胁。

[0077] 在本发明一个实施例中,可以利用如下一种配置文件实现对主用服务器的配置:

[0078] `<localpath watch="/opt/tsce/server_priv"> <!--同步目录-->`

[0079] `<remote ip="mu02"name="scheduler"/> <!--远程服务器-->`

[0080] `</localpath>`

[0081] `<rsync>`

[0082] `<commonParams params="-artuz"/>`

[0083] `<auth start="true"users="root"passwordfile="/etc/rsync.pas"/>`

[0084] `<userDefinedPort start="false"port="874"/><!--port=874-->`

[0085] `<timeout start="false"time="100"/><!--timeout=100-->`

[0086] `<ssh start="false"/>`

[0087] `</rsync>`

[0088] 在本发明一个实施例中,由于在后续过程中涉及到两台服务器的状态切换,因此还需要根据上述配置文件实现对服务器mu02的配置。

[0089] 步骤303:对备用服务器mu02进行配置文件的配置。

[0090] 在本发明一个实施例中,可以对备用服务器mu02可以进行如下配置:配置同步目录和同步密钥。

[0091] 其中,该同步目录可以包括多个目录项,用于表征备用服务器需要实现与主用服务器对该同步目录中所包括的各个目录项的数据同步。

[0092] 其中,同步密钥是用来在主用服务器和备用服务器之间实现数据同步时对主用服务器的身份进行验证的。由于服务器之间在进行数据交互时,若经过身份验证,容易遭受到恶意程度或者恶意设备的攻击,给服务器的数据安全造成威胁。

[0093] 在本发明一个实施例中,可以利用如下一种脚配置文件实现对备用服务器的配置:

```
uid = root
gid = root
use chroot = no
[0094] max connections = 100
pid file = /var/run/rsyncd.pid
auth users = root
secrets file = /etc/rsync.pas #密码文件

[scheduler]
[0095] path = /opt/tsce/server_priv #同步数据路径
comment = scheduler
read only = no #允许写操作
```

[0096] 在本发明一个实施例中,由于在后续过程中涉及到两台服务器的状态切换,因此还需要根据上述配置文件实现对服务器mu01的配置。

[0097] 步骤304:服务器mu01在监测到发生了数据变更时,更新锁文件。

[0098] 在本发明一个实施例中,服务器mu01需要根据预先配置的同步目录中所包括的各个目录项对数据进行监测,在监测到发生了数据变更时,需要将数据变更的属性信息更新到锁文件中。

[0099] 其中,该锁文件可以包括但不限于如下信息:作业属性、作业ID号、该作业所属的用户名、作业节点所使用的资源和作业提交时间等。

[0100] 步骤305:将发生了数据变更的目标目录项以及对应的变更后的数据、和同步密钥推送给服务器mu02。

[0101] 在本发明一个实施例中,为了保证当服务器mu01发生故障后,服务器mu02可以根据服务器mu01中数据正常运行,需要两个服务器之间进行数据同步。为了减少两个服务器之间数据传输的数据量,服务器mu01只需将发生了变更的数据推送给服务器mu02。

[0102] 步骤306:服务器mu02根据自身配置的同步密钥对服务器mu01发送的同步密钥进行验证,在验证通过时,继续执行下一步骤。

[0103] 在本发明一个实施例中,若同步密钥不通过,则拒绝与该服务器mu01进行数据同步更新。

[0104] 步骤307:服务器mu02根据接收到的变更后的数据进行本地同步更新操作。

[0105] 在本发明一个实施例中,服务器mu02可以根据服务器mu01推送的信息中的各个目标目录项确定发生了数据变更的目录项,并将变更后的数据更新到相应的目录项中,从而实现本地数据的同步更新。

[0106] 步骤308:服务器mu02对当前接收到的锁文件进行存储。

[0107] 步骤309:将当前接收到的锁文件与距离当前的目标时间段内接收到的所有锁文

件进行比较,在比较结果包括当前接收到的锁文件与该所有锁文件均相同时,则确定服务器mu01发生故障。

[0108] 其中,该目标时间段可以预先设置好,例如,10s。

[0109] 假设在距离当前接收到的锁文件10s内共接收到锁文件1、锁文件2和锁文件3,服务器mu02需要对这四个锁文件进行逐个扫描,并比较当前接收到的锁文件是否与锁文件1、锁文件2和锁文件3均相同,若是,则确定服务器mu01发生了故障。

[0110] 步骤310:服务器mu02将自身状态切换为主用状态,接管服务器mu01的工作,并向服务器mu02发送状态切换的通知。

[0111] 步骤311:服务器mu01根据该通知,将自身状态切换为备用状态。

[0112] 请参考图4,本发明实施例提供了一种主用服务器,包括:

[0113] 监测单元401,用于监测是否发生了数据变更,并在监测到发生了数据变更时触发更新单元执行相应操作;

[0114] 所述更新单元402,用于更新锁文件;

[0115] 推送单元403,用于将变更后的数据和更新后的所述锁文件推送给备用服务器以实现数据同步;

[0116] 切换单元404,用于在确定所述备用服务器的状态切换为主用状态时,将自身状态切换为备用状态。

[0117] 在本发明一个实施例中,请参考图5,该主用服务器可以进一步包括:

[0118] 配置单元501,用于配置同步目录和同步密钥;

[0119] 所述监测单元401,具体用于监控所述同步目录中每一个目录项所对应的数据,并在监测到目标目录项发生了数据变更时,则确定监测到发生了数据变更;

[0120] 所述推送单元403,具体用于将所述目标目录项以及对应的变更后的数据、所述同步密钥推送给所述备用服务器,以使所述备用服务器在验证所述同步密钥正确时,根据所述变更后的数据对所述目标目录项的数据进行同步更新。

[0121] 如图6所示,本发明实施例提供了一种备用服务器,包括:

[0122] 设定单元601,用于设定目标时间段;

[0123] 接收单元602,用于接收主用服务器推送的变更后的数据和锁文件;

[0124] 同步更新单元603,用于同步更新主用服务器推送的变更后的数据;

[0125] 存储单元604,用于存储当前接收到的锁文件;

[0126] 比较单元605,用于将当前接收到的锁文件与距离当前的所述目标时间段内接收到的所有锁文件进行比较,在比较结果包括当前接收到的锁文件与该所有锁文件均相同时,则确定所述主用服务器发生故障;

[0127] 处理单元606,用于将自身状态切换为主用状态,并将该切换信息通知给所述主用服务器,以使所述主用服务器将其状态切换为备用状态。

[0128] 在本发明一个实施例中,请参考图7,该备用服务器可以进一步包括:

[0129] 配置单元701,用于配置同步目录和同步密钥;

[0130] 所述同步更新单元603,具体用于根据所述同步密钥对所述主用服务器推送的数据中携带的密钥进行验证,并在验证通过时,根据所述主用服务器推送的目标目录项以及该目标目录项对应的变更后的数据,将该变更后的数据更新到所述同步目录中的所述目标

目录项中。

[0131] 请参考图8,本发明实施例还提供了一种业务处理系统,包括上述主用服务器801和上述备用服务器802。

[0132] 综上,本发明实施例至少可以实现如下有益效果:

[0133] 1、在本发明实施例中,在主用服务器中发生了数据变更后,直接将变更后的数据推送给备用服务器以实现数据同步,为了保证业务处理的正常运行,可以利用锁文件确定主用服务器的故障与否,并在主用服务器发生故障时,备用服务器将自身状态切换为主用状态,主用服务器将自身状态切换为备用状态,从而保证了主用服务器和备用服务器的正常工作。

[0134] 2、在本发明实施例中,通过在主用服务器和备用服务器之中配置同步目录,以使主备服务器之间在进行变更数据的更新时,只需将发生了变更的目录项发送备用服务器即可,无需将所有目录项当前的数据进行传输,从而可以降低主备服务器之间的数据传输量。

[0135] 3、在本发明实施例中,通过在主用服务器和备用服务器之中均配置同步密钥,以使主用服务器向备用服务器推送数据时,备用服务器可以根据该同步密钥对主用服务器进行身份验证,从而可以避免恶意程序对自身造成的攻击,提高了自身数据的安全性。

[0136] 上述装置内的各单元之间的信息交互、执行过程等内容,由于与本发明方法实施例基于同一构思,具体内容可参见本发明方法实施例中的叙述,此处不再赘述。

[0137] 需要说明的是,在本文中,诸如第一和第二之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来,而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且,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、物品或者设备不仅包括那些要素,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、物品或者设备所固有的要素。在没有更多限制的情况下,由语句“包括一个”限定的要素,并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同因素。

[0138] 本领域普通技术人员可以理解:实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成,前述的程序可以存储在计算机可读取的存储介质中,该程序在执行时,执行包括上述方法实施例的步骤;而前述的存储介质包括:ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质中。

[0139] 最后需要说明的是:以上所述仅为本发明的较佳实施例,仅用于说明本发明的技术方案,并非用于限定本发明的保护范围。凡在本发明的精神和原则之内所做的任何修改、等同替换、改进等,均包含在本发明的保护范围内。

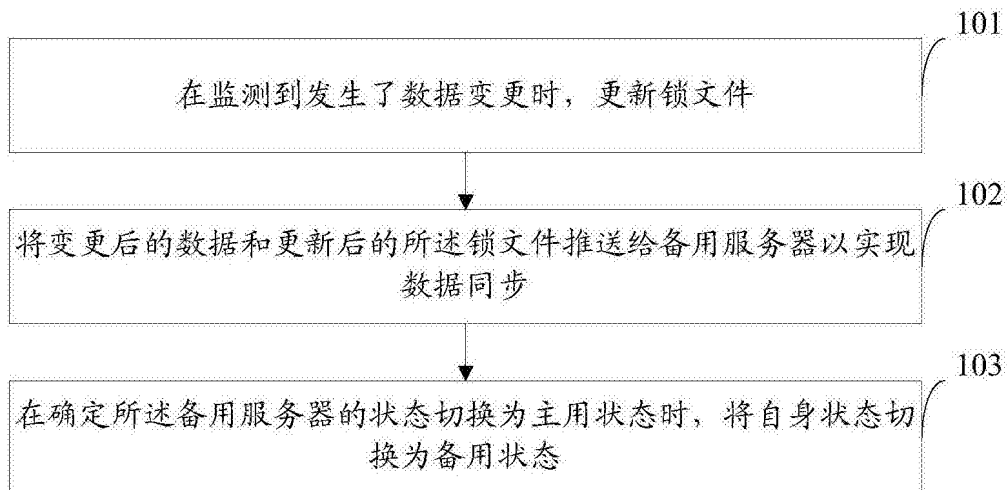


图1

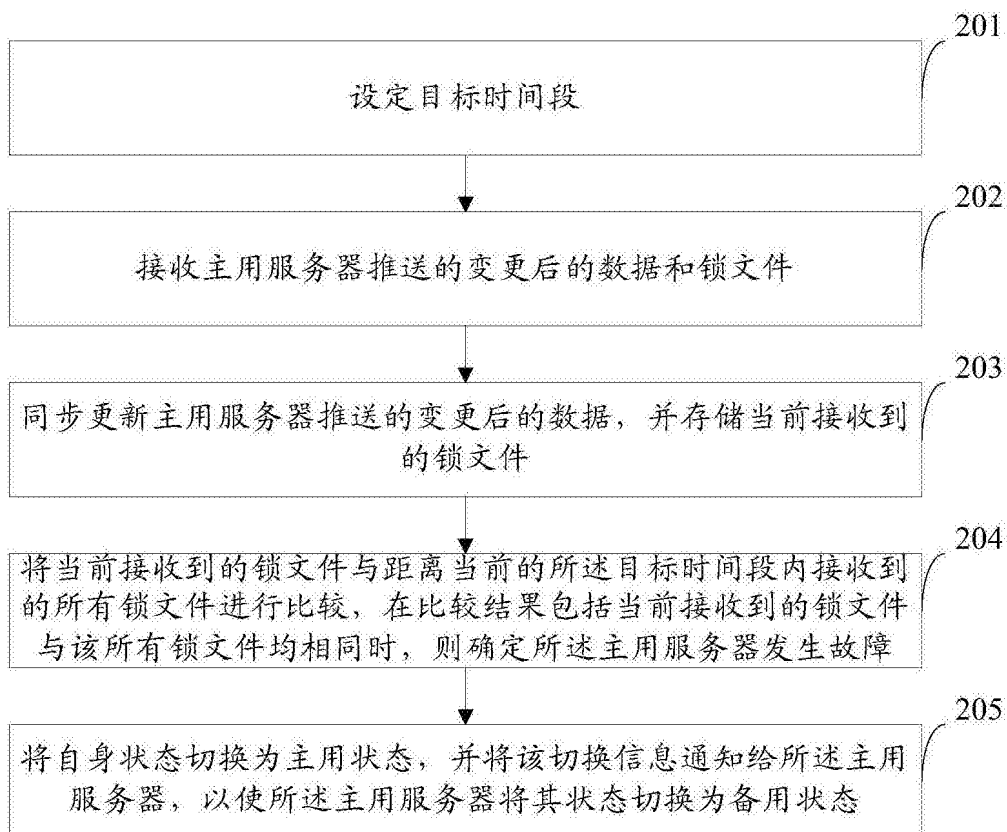


图2



图3

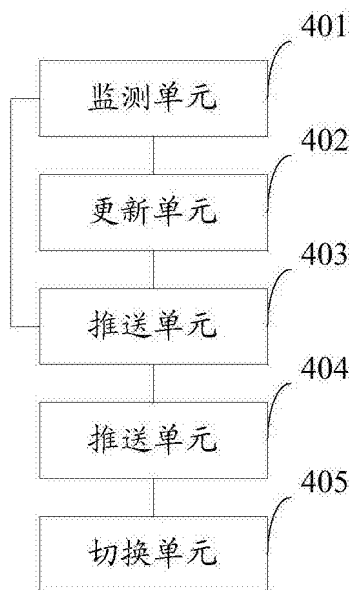


图4

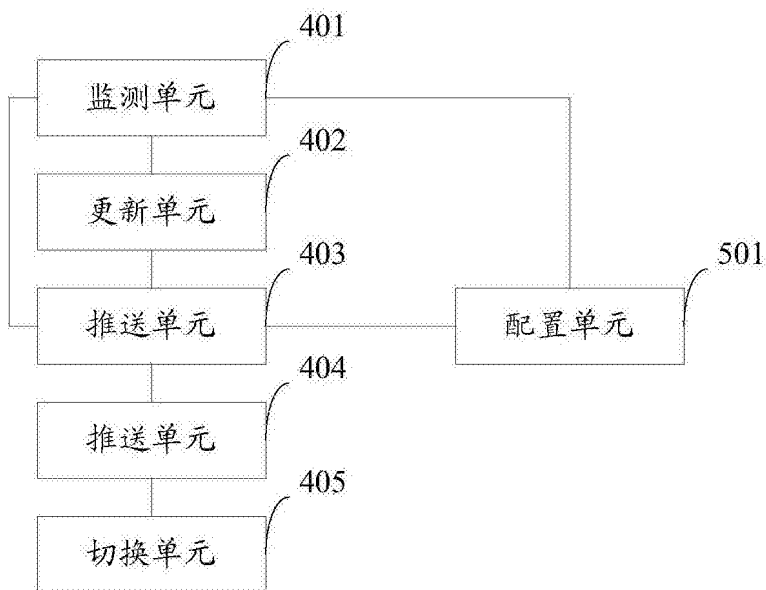


图5

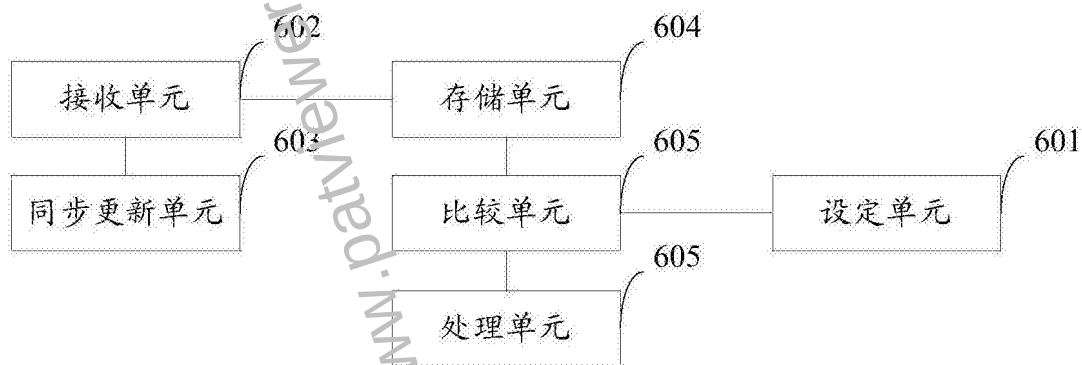


图6

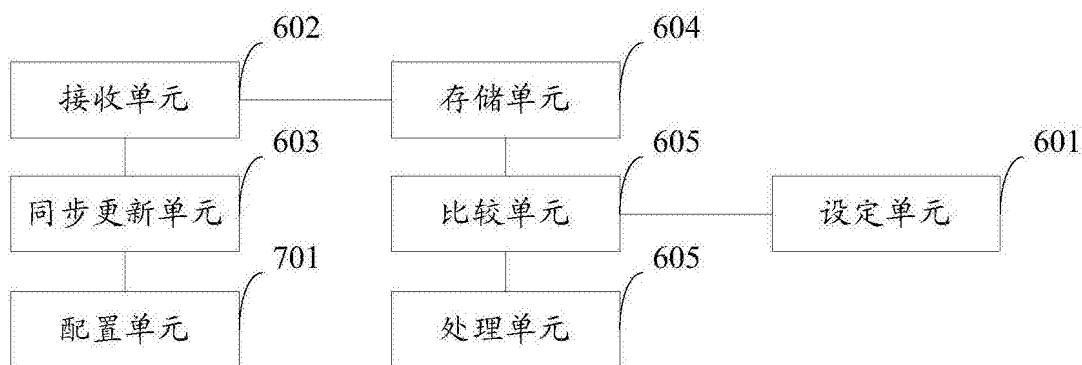


图7

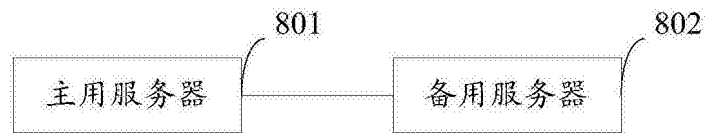


图8