(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 110737906 A
(43)申请公布日 2020.01.31

(21)申请号 201910901173.3

(22)申请日 2019.09.23

(71)申请人 广州海颐信息安全技术有限公司
地址 510000 广东省广州市天河区中山大道西89号办公楼(部位:B栋101)

(72)发明人 陈明朗 邓祯恒 刘博

(74)专利代理机构 北京联瑞联丰知识产权代理事务所(普通合伙) 11411
代理人 刘自丽

(51)Int.Cl.
G06F 21/60(2013.01)

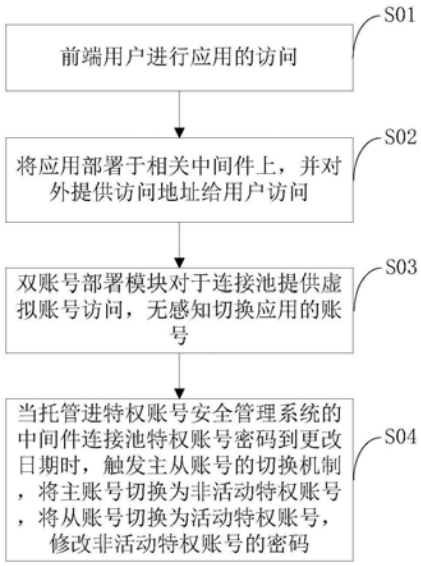
权利要求书2页 说明书6页 附图3页

(54)发明名称

无感切换中间件连接池特权账号的方法及装置

(57)摘要

本发明公开了一种无感切换中间件连接池特权账号的方法及装置,方法包括:前端用户进行应用的访问;将应用部署于相关中间件上,并对外提供访问地址给用户访问;双账号部署模块对于连接池提供虚拟账号访问,无感知切换应用的账号;当托管进特权账号安全管理系统的中间件连接池特权账号密码到更改日期时,触发主从账号的切换机制,将主账号切换为非活动特权账号,将从账号切换为活动特权账号,修改非活动特权账号的密码。本发明能够使得企业或组织的中间件连接池的特权账号密码可以得到定期的更改,也使得更改期间无缝切换,关键应用系统的稳定性得到保障,既加强了企业或者组织的中间件连接池的特权账号的安全,又更好保证业务系统的稳定性运行。



CN 110737906 A

1.一种无感切换中间件连接池特权账号的方法,其特征在于,包括如下步骤:

A)前端用户进行应用的访问;

B)将所述应用部署于相关中间件上,并对外提供访问地址给用户访问;

C)双账号部署模块对于连接池提供虚拟账号访问,无感知切换应用的账号;

D)当托管进特权账号安全管理系统的中间件连接池特权账号密码到更改日期时,触发主从账号的切换机制,将主账号切换为非活动特权账号,将从账号切换为活动特权账号,修改非活动特权账号的密码。

2.根据权利要求1所述的无感切换中间件连接池特权账号的方法,其特征在于,所述特权账号安全管理系统包括:

节点管理单元:用于构建符合企业组织架构的目录树,并允许赋权不同用户对各自目录的独立管理;

账号管理单元:用于特权账号的导入托管,并以特权账号本体为中心实现账号的生命周期管理工作;

访问控制单元:用于负责实现账号使用的权限细分,让不同用户对不同账号有不同的使用权限;

会话监控单元:用于为用户对账号的单点登录过程实现录像、监控、拦截及审计;

审计管理单元:用于为审计部门提供日志查询,所述日志查询至少包括账号的使用与管理和平台自身变更的日志查询;

审批管理单元:用于为用户提供一事一审的账号使用流程审批能力;

系统设置单元:用于为用户提供全平台的账号策略、连接策略、门户设置和自编属性参数;

所述节点管理单元、账号管理单元、访问控制单元、会话监控单元、审计管理单元、审批管理单元和系统设置单元相互连接。

3.根据权利要求2所述的无感切换中间件连接池特权账号的方法,其特征在于,所述账号管理单元进一步包括:

账号轮换模块:用于根据企业管理策略要求,对目标特权账号进行自动化的密码轮换管理;

内嵌依赖同步模块:用于把企业应用程序、脚本和运维工具中的硬编码密码部分取替为同步模块代码,不暴露密码,或者采取推送模式,定期推送新密码至硬编码配置上;

单点登录连接模块:用于为用户提供一键连接能力,且允许管理员为用户提供集中式发布的客户端工具,达到单点登录效果,最终让密码始终不落地用户端,实现持续性监控及审计能力;

细粒度分享模块:用于为用户提供基于账号级细粒度的分享能力;

所述账号轮换模块、内嵌依赖同步模块、单点登录连接模块和细粒度分享模块相互连接。

4.一种实现如权利要求1所述的无感切换中间件连接池特权账号的方法的装置,其特征在于,包括:

访问单元:用于前端用户进行应用的访问;

部署单元:用于将所述应用部署于相关中间件上,并对外提供访问地址给用户访问;

无感知切换单元:双账号部署模块对于连接池提供虚拟账号访问,无感知切换应用的账号;

密码修改单元:用于当托管进特权账号安全管理系统的中间件连接池特权账号密码到更改日期时,触发主从账号的切换机制,将主账号切换为非活动特权账号,将从账号切换为活动特权账号,修改非活动特权账号的密码。

5.根据权利要求4所述的装置,其特征在于,所述特权账号安全管理系统包括:

节点管理单元:用于构建符合企业组织架构的目录树,并允许赋权不同用户对各自目录的独立管理;

账号管理单元:用于特权账号的导入托管,并以特权账号本体为中心实现账号的生命周期管理工作;

访问控制单元:用于负责实现账号使用的权限细分,让不同用户对不同账号有不同的使用权限;

会话监控单元:用于为用户对账号的单点登录过程实现录像、监控、拦截及审计;

审计管理单元:用于为审计部门提供日志查询,所述日志查询至少包括账号的使用与管理和平台自身变更的日志查询;

审批管理单元:用于为用户提供一事一审的账号使用流程审批能力;

系统设置单元:用于为用户提供全平台的账号策略、连接策略、门户设置和自编属性参数;

所述节点管理单元、账号管理单元、访问控制单元、会话监控单元、审计管理单元、审批管理单元和系统设置单元相互连接。

6.根据权利要求5所述的装置,其特征在于,所述账号管理单元进一步包括:

账号轮换模块:用于根据企业管理策略要求,对目标特权账号进行自动化的密码轮换管理;

内嵌依赖同步模块:用于把企业应用程序、脚本和运维工具中的硬编码密码部分取替为同步模块代码,不暴露密码,或者采取推送模式,定期推送新密码至硬编码配置上;

单点登录连接模块:用于为用户提供一键连接能力,且允许管理员为用户提供集中式发布的客户端工具,达到单点登录效果,最终让密码始终不落地用户端,实现持续性监控及审计能力;

细粒度分享模块:用于为用户提供基于账号级细粒度的分享能力;

所述账号轮换模块、内嵌依赖同步模块、单点登录连接模块和细粒度分享模块相互连接。

无感切换中间件连接池特权账号的方法及装置

技术领域

[0001] 本发明涉及特权账号安全管理领域，特别涉及一种无感切换中间件连接池特权账号的方法及装置。

背景技术

[0002] 目前IT安全领域发展日新月异，不断变化。信息化安全防护手段越来越多，也越来越高级。但数据信息的最后一道防线，特权账号密码始终得不到有效保护与管理，攻击者依然能够通过合法的技术途径，进入企业内部网络，窃取有价值的数据。他们所用到的技巧，就是获知了被泄露的特权账号密码。这些高权限的账号，除了员工的个人账号之外，也包括企业或组织整个IT基础架构的底层系统账号以及应用内嵌账号。这些特权账号往往被人们所忽略，从而不受监控，最终成为了大多数攻击的突破口。但管理者也是无可奈何，因为没有很好的自动化、可扩展和高可靠技术平台，能让他们从万级数量的账号管理工作中解放出来。导致总有高权限的账号密码被泄露，最终发生数据泄露事件。

[0003] 特别针对像银行这种业务繁重且无法随时停机更新修改中间件连接池密码的应用程序，传统堡垒机无法提供应用不重启的解决方案，致使核心关键应用的中间件连接池密码无法定期修改，从而无法满足等保要求。

发明内容

[0004] 本发明要解决的技术问题在于，针对现有技术的上述缺陷，提供一种能够使得企业或组织的中间件连接池的特权账号密码可以得到定期的更改，也使得更改期间无缝切换，关键应用系统的稳定性得到保障，既加强了企业或者组织的中间件连接池的特权账号的安全，又更好保证业务系统的稳定性运行的无感切换中间件连接池特权账号的方法及装置。

[0005] 本发明解决其技术问题所采用的技术方案是：构造一种无感切换中间件连接池特权账号的方法，包括如下步骤：

[0006] A)前端用户进行应用的访问；

[0007] B)将所述应用部署于相关中间件上，并对外提供访问地址给用户访问；

[0008] C)双账号部署模块对于连接池提供虚拟账号访问，无感知切换应用的账号；

[0009] D)当托管进特权账号安全管理系统的中间件连接池特权账号密码到更改日期时，触发主从账号的切换机制，将主账号切换为非活动特权账号，将从账号切换为活动特权账号，修改非活动特权账号的密码。

[0010] 在本发明所述的无感切换中间件连接池特权账号的方法中，所述特权账号安全管理系统包括：

[0011] 节点管理单元：用于构建符合企业组织架构的目录树，并允许赋权不同用户对各自目录的独立管理；

[0012] 账号管理单元：用于特权账号的导入托管，并以特权账号本体为中心实现账号的

生命周期管理工作；

[0013] 访问控制单元：用于负责实现账号使用的权限细分，让不同用户对不同账号有不同的使用权限；

[0014] 会话监控单元：用于为用户对账号的单点登录过程实现录像、监控、拦截及审计；

[0015] 审计管理单元：用于为审计部门提供日志查询，所述日志查询至少包括账号的使用与管理和平台自身变更的日志查询；

[0016] 审批管理单元：用于为用户提供一事一审的账号使用流程审批能力；

[0017] 系统设置单元：用于为用户提供全平台的账号策略、连接策略、门户设置和自编属性参数；

[0018] 所述节点管理单元、账号管理单元、访问控制单元、会话监控单元、审计管理单元、审批管理单元和系统设置单元相互连接。

[0019] 在本发明所述的无感切换中间件连接池特权账号的方法中，所述账号管理单元进一步包括：

[0020] 账号轮换模块：用于根据企业管理策略要求，对目标特权账号进行自动化的密码轮换管理；

[0021] 内嵌依赖同步模块：用于把企业应用程序、脚本和运维工具中的硬编码密码部分取替为同步模块代码，不暴露密码，或者采取推送模式，定期推送新密码至硬编码配置上；

[0022] 单点登录连接模块：用于为用户提供一键连接能力，且允许管理员为用户提供集中式发布的客户端工具，达到单点登录效果，最终让密码始终不落地用户端，实现持续性监控及审计能力；

[0023] 细粒度分享模块：用于为用户提供基于账号级细粒度的分享能力；

[0024] 所述账号轮换模块、内嵌依赖同步模块、单点登录连接模块和细粒度分享模块相互连接。

[0025] 本发明还涉及一种实现上述无感切换中间件连接池特权账号的方法的装置，包括：

[0026] 访问单元：用于前端用户进行应用的访问；

[0027] 部署单元：用于将所述应用部署于相关中间件上，并对外提供访问地址给用户访问；

[0028] 无感知切换单元：双账号部署模块对于连接池提供虚拟账号访问，无感知切换应用的账号；

[0029] 密码修改单元：用于当托管进特权账号安全管理系统的中间件连接池特权账号密码到更改日期时，触发主从账号的切换机制，将主账号切换为非活动特权账号，将从账号切换为活动特权账号，修改非活动特权账号的密码。

[0030] 在本发明所述的装置中，所述特权账号安全管理系统包括：

[0031] 节点管理单元：用于构建符合企业组织架构的目录树，并允许赋权不同用户对各自目录的独立管理；

[0032] 账号管理单元：用于特权账号的导入托管，并以特权账号本体为中心实现账号的生命周期管理工作；

[0033] 访问控制单元：用于负责实现账号使用的权限细分，让不同用户对不同账号有不

同的使用权限；

[0034] 会话监控单元：用于为用户对账号的单点登录过程实现录像、监控、拦截及审计；

[0035] 审计管理单元：用于为审计部门提供日志查询，所述日志查询至少包括账号的使用与管理和平台自身变更的日志查询；

[0036] 审批管理单元：用于为用户提供一事一审的账号使用流程审批能力；

[0037] 系统设置单元：用于为用户提供全平台的账号策略、连接策略、门户设置和自编属性参数；

[0038] 所述节点管理单元、账号管理单元、访问控制单元、会话监控单元、审计管理单元、审批管理单元和系统设置单元相互连接。

[0039] 在本发明所述的装置中，所述账号管理单元进一步包括：

[0040] 账号轮换模块：用于根据企业管理策略要求，对目标特权账号进行自动化的密码轮换管理；

[0041] 内嵌依赖同步模块：用于把企业应用程序、脚本和运维工具中的硬编码密码部分取替为同步模块代码，不暴露密码，或者采取推送模式，定期推送新密码至硬编码配置上；

[0042] 单点登录连接模块：用于为用户提供一键连接能力，且允许管理员为用户提供集中式发布的客户端工具，达到单点登录效果，最终让密码始终不落地用户端，实现持续性监控及审计能力；

[0043] 细粒度分享模块：用于为用户提供基于账号级细粒度的分享能力；

[0044] 所述账号轮换模块、内嵌依赖同步模块、单点登录连接模块和细粒度分享模块相互连接。

[0045] 实施本发明的无感切换中间件连接池特权账号的方法及装置，具有以下有益效果：由于每当托管进特权账号安全管理系统的中间件连接池特权账号密码已到修改日期时，就触双账号的切换机制，并自动切换活动账号和非活动账号，然后修改非活动特权账号的密码，采用了这套机制后，本发明能够使得企业或组织的中间件连接池的特权账号密码可以得到定期的更改，也使得更改期间无缝切换，关键应用系统的稳定性得到保障，既加强了企业或者组织的中间件连接池的特权账号的安全，又更好保证业务系统的稳定性运行。

附图说明

[0046] 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，下面描述中的附图仅仅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。

[0047] 图1为本发明无感切换中间件连接池特权账号的方法及装置一个实施例中方法的流程图；

[0048] 图2为所述实施例中无感切换中间件连接池特权账号的方法的流程框图；

[0049] 图3为所述实施例中特权账号安全管理系统的结构示意图；

[0050] 图4为所述实施例中账号管理单元的结构示意图；

[0051] 图5为所述实施例中装置的结构示意图。

具体实施方式

[0052] 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，所描述的实施例仅仅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。

[0053] 在本发明无感切换中间件连接池特权账号的方法及装置实施例中，其无感切换中间件连接池特权账号的方法的流程图如图1所示。图2为本实施例中无感切换中间件连接池特权账号的方法的流程框图。图1中，该无感切换中间件连接池特权账号的方法包括如下步骤：

[0054] 步骤S01前端用户进行应用的访问：本步骤中，前端用户进行应用的访问。

[0055] 步骤S02将应用部署于相关中间件上，并对外提供访问地址给用户访问：本步骤中，将应用部署于相关中间件上，该应用对外提供访问地址给用户进行访问。

[0056] 步骤S03双账号部署模块对于连接池提供虚拟账号访问，无感知切换应用的账号：本步骤中，双账号(双账号指的是主账号和从账号)部署模块对于连接池提供虚拟账号访问，进行无感知切换应用账号。

[0057] 步骤S04当托管进特权账号安全管理系统的中间件连接池特权账号密码到更改日期时，触发主从账号的切换机制，将主账号切换为非活动特权账号，将从账号切换为活动特权账号，修改非活动特权账号的密码：本步骤中，当托管进特权账号安全管理系统的中间件连接池特权账号密码到更改日期时，触发主从账号的切换机制，具体是将主账号切换为非活动特权账号，将从账号切换为活动特权账号，修改非活动特权账号的密码，即自动轮换原本的主账号，因为应用访问的虚拟账号调用的实质为原本的从账号，这确保了业务连续性，没有延迟。

[0058] 图3为本实施例中特权账号安全管理系统的结构示意图；图3中，该特权账号安全管理系统包括相互连接的节点管理单元1、账号管理单元2、访问控制单元3、会话监控单元4、审计管理单元5、审批管理单元6和系统设置单元7；其中，节点管理单元1用于构建符合企业组织架构的目录树，并允许赋权不同用户对各自目录的独立管理。

[0059] 账号管理单元2用于特权账号的导入托管，并以特权账号本体为中心实现账号的生命周期管理工作。具体而言，针对需要进行密码自动化校验、改密甚至重置(找回密码)的特权账号类型繁多、内嵌至DevOps工具、代码、程序常见同时难以管理的问题。例如，持续集成工具Jenkins工具会内嵌云平台的开发访问密钥，意味着密钥容易暴露于工具配置中，且难以被审计使用情况，也不利于定期轮换密钥的维护工作。那么账号管理单元2都能很好地解决以上问题。另外，用户即人类需要对这些新型账号凭证使用时，通过账号管理单元2的单点登录连接模块即可实施凭证不落地的安全使用。

[0060] 访问控制单元3用于负责实现账号使用的权限细分，让不同用户对不同账号有不同的使用权限。访问控制单元3的账号密码箱提供了新增、修改与管理账号密码箱能力，为账号存储提供逻辑独立空间，密码箱。同时提供基于密码箱集合对用户、进行的访问使用授权。

[0061] 会话监控单元4用于方便为用户对账号的单点登录过程实现录像、监控、拦截及审计。能提供快速查询会话、定位操作记录、实现会话干预、操作拦截等功能。

[0062] 审计管理单元5用于为审计部门提供日志查询，该日志查询至少包括账号的使用与管理和平台自身变更的日志查询。换言之，审计管理单元5为审计部门提供账号使用与管理、平台自身变更等维度的日志查询。其日志内容满足账号操作轨迹回溯、用户行为分析之用。

[0063] 审批管理单元6用于为用户提供一事一审的账号使用流程审批能力。审批流程可以指定审批人、操作内容、时间窗口、原因等因素。且审批管理单元具备插件化扩展能力，满足对接外部工单系统平台需求。

[0064] 系统设置单元7用于为用户提供全平台的账号策略、连接策略、门户设置和自编属性参数等能力。该系统设置单元7主要与账号管理单元2进行互相连接。

[0065] 本发明通过设置节点管理单元1、账号管理单元2、访问控制单元3、会话监控单元4、审计管理单元5、审批管理单元6和系统设置单元7，能够自动化管理企业的特权账号，且能让用户在不接触密码的前提下进行单点登录使用，同时还能针对云、DevOps、容器化等环境下的特权账号做灵活的、插件式的账号管理。

[0066] 图4为本实施例中账号管理单元的结构示意图；图4中，该该账号管理单元2进一步包括相互连接的账号轮换模块21、内嵌依赖同步模块22、单点登录连接模块23和细粒度分享模块24；另外，账号轮换模块21、内嵌依赖同步模块22、单点登录连接模块23与系统设置单元7、节点管理单元1、审批管理单元6和审计管理单元5相互连接。

[0067] 其中，账号轮换模块21用于根据企业管理策略要求，对目标特权账号进行自动化的密码轮换管理，如周期校验、改密，遇错自动重置等。账号轮换模块21根据定义的账号策略，实施对目标特权账号的账号密码自动轮换，且不限目标账号类型。目前支持账号类型已包含且不限于操作系统账号、数据库账号、网络安全设备账号、虚拟化控制台账号、云平台控制台账号、容器化管理员账号、DevOps工具控制台账号、应用中间件控制台账号(非操作系统账号)、开发接口程序访问密钥账号等等。

[0068] 内嵌依赖同步模块22用于把企业应用程序、脚本和运维工具中的硬编码密码部分取替为同步模块代码，不暴露密码，或者采取推送模式，定期推送新密码至硬编码配置上。内嵌依赖同步模块22与账号轮换模块21互联，负责把账号轮换模块21中的账号主体实施同步推送至所需的内嵌依赖位置，如系统服务、配置文件、工具设置、数据库表项等中。同时，内嵌依赖同步模块22也能为程序代码中的内嵌密码代码提供相关开发语言包，取替代码中的明文密码，实现程序取密无需硬编码，且能审计、限制、隔离取密程序的身份合法性与安全性。

[0069] 单点登录连接模块23用于为用户提供一键连接能力，且允许管理员为用户提供集中式发布的客户端工具，达到单点登录效果，最终让密码始终不落地用户端，提高安全性，而且，能实现持续性监控及审计能力。单点登录连接模块23为用户提供账号的一键单点登录服务，并能实现自定义登录工具的登录逻辑，具备文件上下传控制、文本复制粘贴控制、快速克隆连接等能力。

[0070] 细粒度分享模块24用于为用户提供基于账号级细粒度的分享能力，灵活满足临时授权使用的需要。

[0071] 对比目前企业或者组织长期不更换关键业务中中间件连接池的特权账号密码，本发明的无感切换中间件连接池特权账号的方法采用了一种无感切换中间件连接池的特权

账号密码的机制，每当托管进特权账号安全管理系统的中间件连接池特权账号密码已到修改日期时，就触发此双账号的机制，并自动切换活动账号和非活动账号，然后修改非活动特权账号的密码。采用了这套机制后，能够使得企业或组织的中间件连接池的特权账号密码可以得到定期的更改，也使得更改期间无缝切换，关键应用系统的稳定性得到保障，既加强了企业或者组织的中间件连接池的特权账号的安全，又更好保证业务系统的稳定性运行。

[0072] 本实施例还涉及一种实现上述无感切换中间件连接池特权账号的方法的装置，该装置的结构示意图如图5所示。图5中，该装置包括访问单元100、部署单元200、无感知切换单元300和密码修改单元400；其中，访问单元100用于前端用户进行应用的访问；部署单元200用于将应用部署于相关中间件上，并对外提供访问地址给用户访问；无感知切换单元300双账号部署模块对于连接池提供虚拟账号访问，无感知切换应用的账号；密码修改单元400用于当托管进特权账号安全管理系统的中间件连接池特权账号密码到更改日期时，触发主从账号的切换机制，将主账号切换为非活动特权账号，将从账号切换为活动特权账号，修改非活动特权账号的密码。

[0073] 对比目前企业或者组织长期不更换关键业务中中间件连接池的特权账号密码，本发明的装置采用了一种无感切换中间件连接池的特权账号密码的机制，每当托管进特权账号安全管理系统的中间件连接池特权账号密码已到修改日期时，就触发此双账号的机制，并自动切换活动账号和非活动账号，然后修改非活动特权账号的密码。采用了这套机制后，能够使得企业或组织的中间件连接池的特权账号密码可以得到定期的更改，也使得更改期间无缝切换，关键应用系统的稳定性得到保障，既加强了企业或者组织的中间件连接池的特权账号的安全，又更好保证业务系统的稳定性运行。

[0074] 总之，本发明提供一种无感切换中间件连接池特权账号，基于双账号部署，采用中间件连接池双账号部署与无缝切换的机制，解决了无法定期修改连接池特权账号的密码，并且消除定期轮换密码时因延迟而导致密码不正确从而锁库的问题，应用于特权账号安全管理系统。

[0075] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

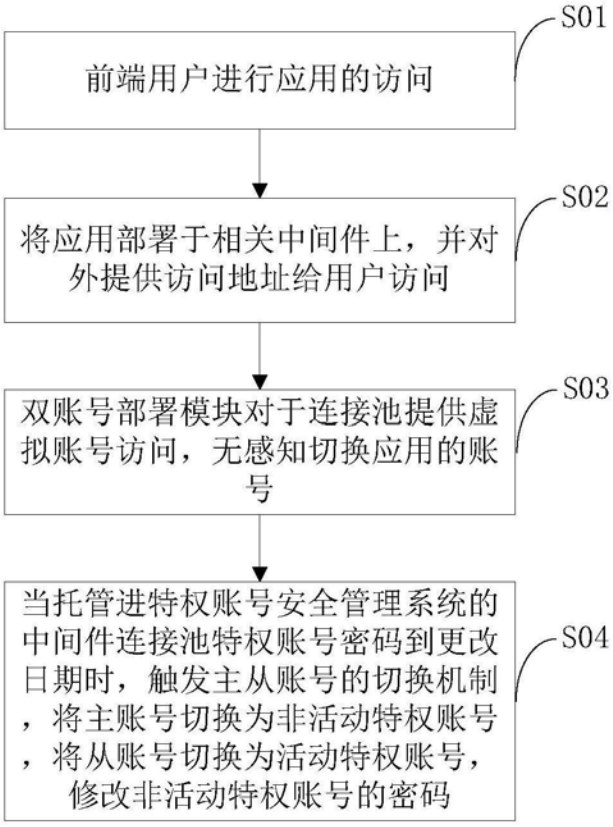

S01
前端用户进行应用的访问
S02
将应用部署于相关中间件上，并对外提供访问地址给用户访问
S03
双账号部署模块对于连接池提供虚拟账号访问，无感知切换应用的账号
S04
当托管进特权账号安全管理系统的中间件连接池特权账号密码到更改日期时，触发主从账号的切换机制，将主账号切换为非活动特权账号，将从账号切换为活动特权账号，修改非活动特权账号的密码

图1

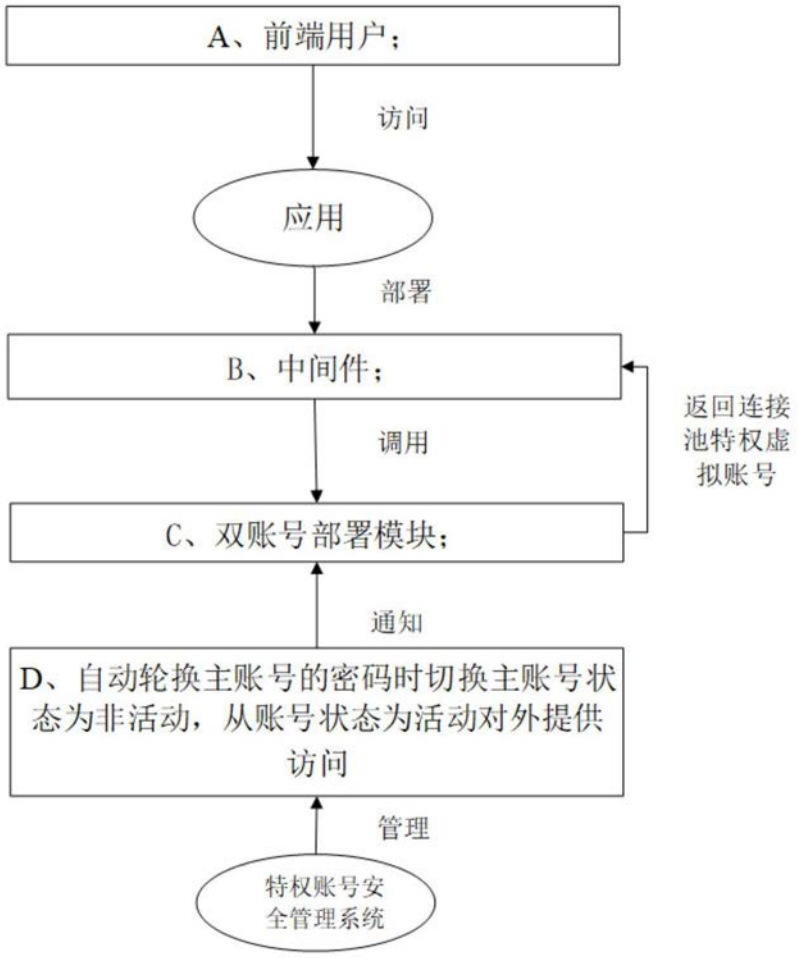

A、前端用户；
访问
应用
部署
B、中间件；
调用
返回连接池特权虚拟账号
C、双账号部署模块；
通知
D、自动轮换主账号的密码时切换主账号状态为非活动，从账号状态为活动对外提供访问
管理
特权账号安全管理系统

图2

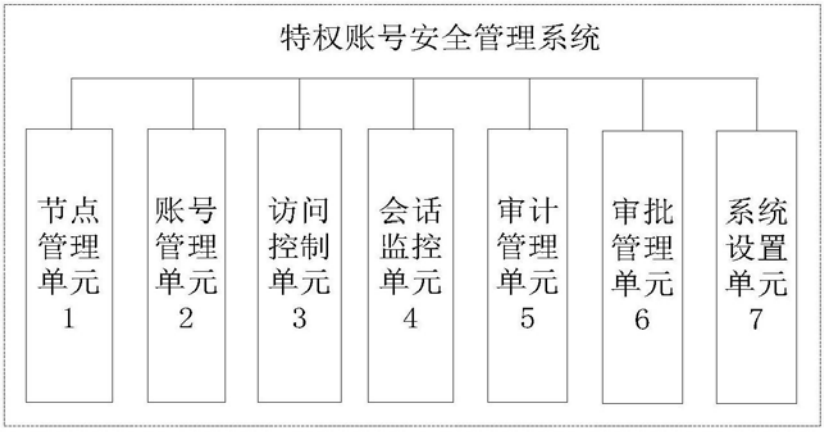

特权账号安全管理系统
节点管理单元1
账号管理单元2
访问控制单元3
会话监控单元4
审计管理单元5
审批管理单元6
系统设置单元7

图3

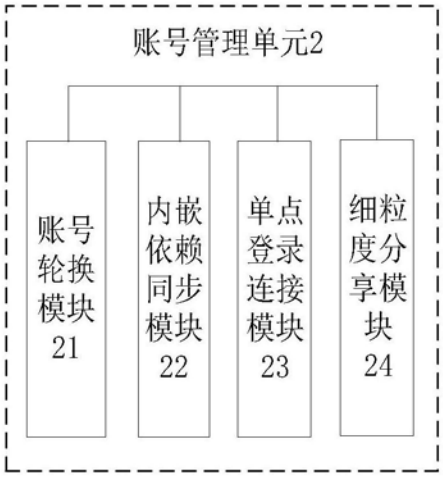

账号管理单元2
账号轮换模块21
内嵌依赖同步模块22
单点登录连接模块23
细粒度分享模块24

图4

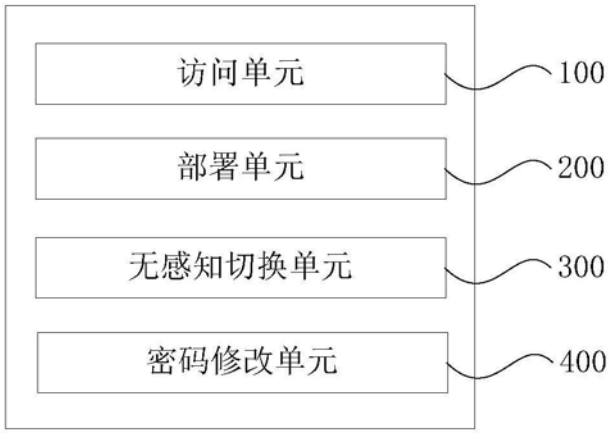

访问单元
100
部署单元
200
无感知切换单元
300
密码修改单元
400

图5