Computer Science and Application 计算机科学与应用, 2020, 10(10), 1870-1878
Published Online October 2020 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2020.1010197

Hans汉斯

基于动态口令获取技术的运维账号管理方法

郑宝铭[1]，苗刚中[2,3]，王理冬[4]，刘冬梅[2]

[1]国家开发银行信息科技局，北京
[2]合肥工业大学电气与自动化工程学院，安徽 合肥
[3]工业自动化安徽省工程技术研究中心，安徽 合肥
[4]安徽省电子产品监督检验所，安徽 合肥
Email: miaogzh@126.com

收稿日期：2020年10月7日；录用日期：2020年10月22日；发布日期：2020年10月29日

摘 要

针对部署于企业内部的网络软件系统应用群，基于动态口令获取技术研究构建了一套运维账号统一管理平台。首先分析了企业内部网络软件系统运维账号管理的现实困难，然后给出了运维账号统一管理的业务需求和整体架构，在此基础上介绍了平台的使用流程。最后，对平台的特点进行了总结。

关键词

运维账号，动态口令获取，统一管理

Unified Privileged Account Management Method Based on Dynamic Password Access

Baoming Zheng[1], Gangzhong Miao[2,3], Lidong Wang[4], Dongmei Liu[2]

[1]Council of Information Science and Technology, China Development Bank, Beijing
[2]School of Electrical Engineering and Automation, Hefei University of Technology, Hefei Anhui
[3]Industrial Automation Engineering and Technology Research Center of Anhui Province, Hefei Anhui
[4]Anhui Institute of Electron Production Supervision and Inspection, Hefei Anhui
Email: miaogzh@126.com

Received: Oct. 7th, 2020; accepted: Oct. 22nd, 2020; published: Oct. 29th, 2020

Abstract

Aiming at the practical difficulties of privileged account management in software systems based on intranet server cluster, a unified privileged account management platform is constructed based

文章引用: 郑宝铭, 苗刚中, 王理冬, 刘冬梅. 基于动态口令获取技术的运维账号管理方法[J]. 计算机科学与应用, 2020, 10(10): 1870-1878. DOI: 10.12677/csa.2020.1010197

on dynamic password access. Firstly, this paper discusses the shortcomings of the management for the internal network software system, and then gives the privileged account unified management platform with the need for integration and the overall architecture. On this basis, this paper introduces the overall use process of the platform. Finally, the innovation points of the platform are summarized.

Keywords

Privileged Account, Dynamic Password Access, Unified Management

1. 引言

随着国内企业 IT 系统的数据和业务的不断集中，IT 系统规模逐渐增大，关联关系日益复杂[1]，各系统所产生的运维账号(也称特权账号)的种类和数量逐渐增多，由于此类账号所独有的特殊作用和超强效应，在管理和使用过程中，诸多现实问题与安全要求之间的矛盾日渐突出，风险隐患日益明显。因此，建设一套先进、高效、可持续发展的运维账号全生命周期管理体系迫在眉睫。

事实上，超过 90%的网络攻击都与网络内部运维账号的口令泄露有关，前段时间发生的微盟删库事件、某交通银行员工盗取贷款密码违规发放 1900 余万贷款事件以及之前的斯诺登事件都与没有科学管理好运维账号有关[2]。从这个意义上说，可以认为网络安全的基础就是对运维账号的有效管理。目前，对于运维账号的管理，国内并没有特别好的手段，不少单位对运维账号还处于手工管理阶段，也有不少单位借助堡垒机兼顾做了一些运维账号的管理工作[3]，例如要求管理员手工记录，定期修改口令，离职时签署保密协议等等。这些方式既不利于工作效率的提高，也难以降低运维账号泄露的风险。

本文探讨和设计了一种运维账号统一管理平台，该平台可用于加强运维账号管理，并强制推行口令安全策略，通过构建访问控制一体化，达到对生产系统各平台用户的自动化管理和访问控制，以及运维账号完整生命周期管理。

1.1. 运维账号及管理中存在的问题

运维账号是指数据中心管理人员、软件开发人员，外包人员在进行 IT 系统生产运维、排错、支持过程中登录生产计算资源(也称为“被管理系统”)所使用的账号。其中，生产计算资源涵盖：操作系统、数据库、中间件、虚拟化设施、网络设备、防火墙、安全设备、业务应用系统、管理系统以及其他任务数据中心使用的账号。从使用的实体角度，运维账号分为管理员使用的账号和应用使用的账号。管理员使用的账号又称交互账号，是指 IT 管理员以命令行或者 GUI 交互操作的登录账号。例如：root，UNIX/Linux 普通用户，Windows Administrator，DBA 等。这类账号有些是特权账号，可以部署应用系统、起停服务，获取数据，有些则相对权限较小，只具有只读权限，用于排故障，健康检查之用。应用使用的账号又称应用内嵌账号，其是应用在程序或者配置文件中的账号，该账号用于连接数据库，在应用与应用之间交互认证的账号。该类账号通常对业务数据具有直接访问权限，即使在系统层面不是一个特权账号，而在数据层面却拥有敏感信息的访问权限[4]。

运维账号的管理存在的突出问题：其一，运维账号管理松散，账号口令由不同的运维人员持有。对

于业内账号口令定期修改的要求，在执行的时效上显的不足，且账号口令依赖人工修改，工作量大、且重复，其口令复杂度也无法保证，账号口令存于个人纸质、电子文件中或直接记于脑中，其安全及可靠性无法保障；其二，运维账号虽然通过 ITIL 系统建立了严格的审批制度，却没有便捷的口令发放及回收手段；其三，对于运维人员的整个账号操作过程缺乏有效的监管措施，事中的监控和事后审计无法完整复原，一旦出现事故无法通过有力的证据判断责任划分。

1.2. 网络安全等级保护中对于运维账号相关的评测要求

2017 年 6 月 1 日实施的《中华人民共和国网络安全法》第二十一条[5]规定了国家实行网络安全等级保护制度，网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。第三十一条规定国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。网络安全等级保护 2.0 相关标准于 2019 年 12 月 1 日正式实施，其中《信息安全技术 网络安全等级保护测评要求》(GB/T 28448-2019) [6]中描述了对运维账号管理的初级测评要求。其具体内容读者可以参考相关等级保护标准，在此就不累述了，国家自 2020 年 11 月 01 日起将启用新的网络安全等级评定程序。

针对国家测评要求及面临的挑战，如果没有一套功能完善的系统来专注于管理运维账号，今后的管理成本会越来越高，且因为运维账号泄露或遗失、误操作等事故所导致的损失将是不可预估的。

2. 系统架构

本节介绍了运维账号统一管理平台应实现的业务功能，在此基础上设计出平台整体架构，讲述了平台的使用流程，并就其核心关键技术(运维账号动态口令获取)进行探讨。

2.1. 平台功能及整体架构

如图 1 所示为平台整体工作流程图。

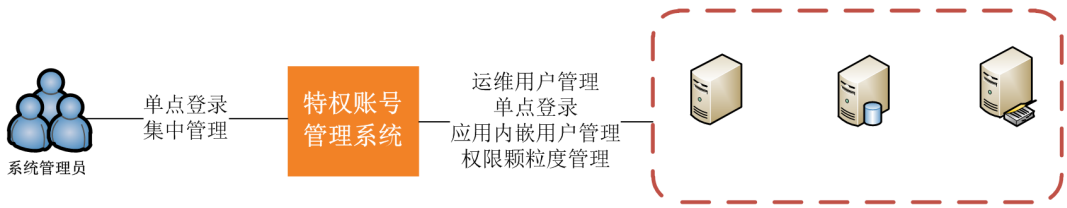

Figure 1. Platform overall workflow flow chart
图 1. 平台整体工作流程图

根据平台特点及业务需求，本系统核心功能包括以下七点：

1) 能够实现口令的集中管理。能够集中存储和自动化管理各系统平台(ZOS/AIX/UNIX/LINUX/WIN/ESX/数据库/中间件/网络设备/安全设备/WEB 应用维护用户/应用内嵌用户的 ID 口令，应根据实际需求配置自动化口令管理策略。

2) 能够实现单点登录和监控。为了进一步保证口令的安全性，软件需提供集中用户单点登录与监控。具体包括口令代填和实时监控两个要点。其中口令代填指的是在使用口令时不将口令的明文暴露给任何人员，通过口令代填的形式帮助管理人员打开客户端和填写口令。实时监控指的是在用户使用者在使用用户时，另一方人员可以同步登录系统查看用户使用情况与具体操作命令。

3) 登录主机时实现双因素认证。

4) 实现用户 ID 审批管理流程的整合。提供各平台系统用户口令的全生命周期管理，并与中心现有的系统用户申请流程整合，实现“一事一申请”的安全管理要求。

5) 实现系统系统用户的自动发现。对中心生产环境(ZOS/AIX/UNIX/LINUX/WIN/ESX/数据库/中间件/网络设备/安全设备/WEB 应用维护用户)的系统用户能够自动探测、收集并纳入一体化访问控制平台进行集中管理，一体化访问控制平台能够针对用户的添加、删除进行差异化对比，统计出每天中心平台用户变化情况，规避和杜绝“幽灵用户”的出现。

6) 提供应用运行类用户管理。对内嵌在中间件数据库连接、应用程序代码、脚本以及配置文件中的应用运行类用户口令可以实现自动化修改，满足内外审计监管要求，真正保护敏感数据。

7) 提供精细化权限管理。针对开放平台操作系统中的运维账号进行精细化的权限管理以“最小权限分配”原则实现访问控制中的用户授权环节。

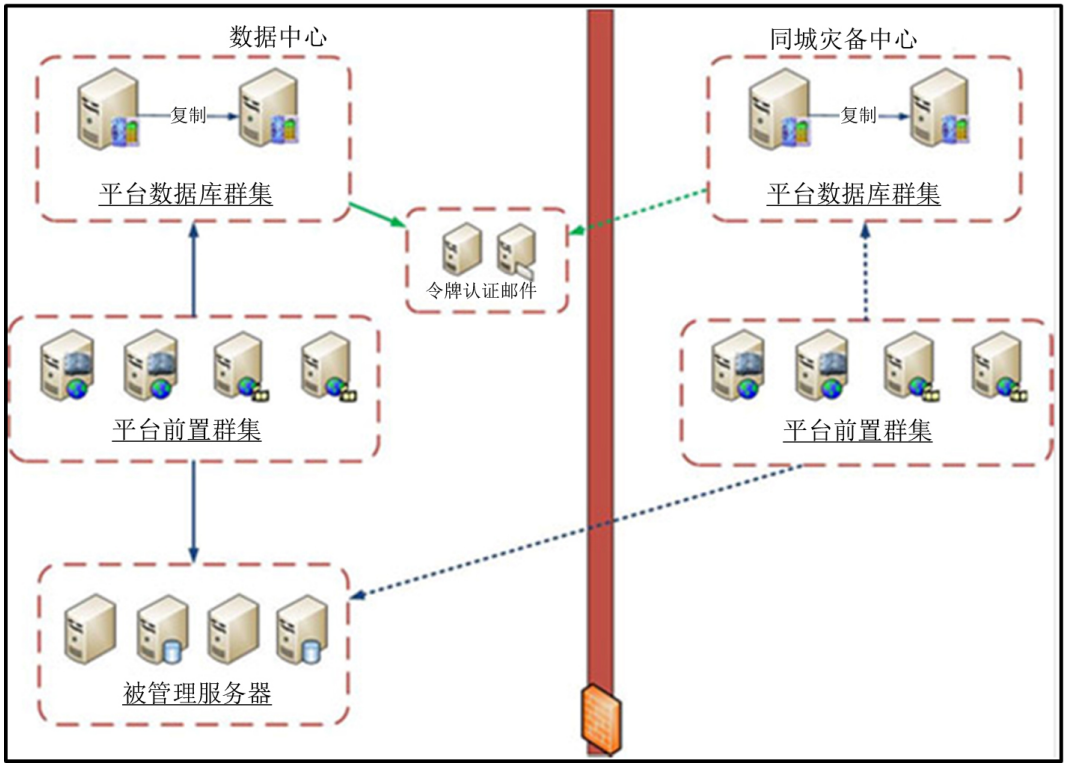

Figure 2. Operation and maintenance account management tool platform overall architecture diagram
图 2. 运维账号管理工具平台整体架构图

基于以上分析，以业内拥有数据中心和同城灾备中心结构[7]的模式为例，设计平台整体架构如图 2 所示。由图 2 可见，本系统运行于局域网内部，包括数据中心和同城灾备中心两部分，每一部分又包括平台数据库群集和平台前置群集。其中，平台前置群集和被管理的服务器之间直接通信，平台数据库群集用以保存运维账号管理平台中的动态用户口令。数据中心和同城灾备中心之间通过防火墙安全隔离，并通过令牌认证邮件的方式进行通信。

2.2. 平台整体使用流程

根据以上分析，设计平台工作架构如图 3 所示。具体描述如下。

步骤 1，IT 管理员登录管理平台，可以利用 AD/LDAP，附加 RSA 进行双因素认证。

步骤 2，IT 管理员通过浏览器访问 PVWA 进行口令获取，口令管理，单点登录及审计等功能。

步骤 3，单点登录时，浏览器打开至 PSM 服务器的 RDP 连接，由 PSM 自动代填口令，为管理员打开至目标服务器的会话，包括 SSH，RDP，XWindows，Oracle，DB2，FTP 等。

步骤 4，审计人员通过 PVWA 查询在线会话后，亦可登录 PSM 进行同步监控在线会话。

步骤 5，会话结束后 PSM 服务器将相关录像及操作文本上传至口令保险库中。

步骤 6，如果存在口令被查询后，CPM 会在一段时间后对目标服务器上的用户进行口令重置。

步骤 7，EPV Replicator 作为 EPV 套件自带软件，将 Vault 数据以加口令形式定期导出，后续企业备份软件可以保存并导入磁带用于未来恢复。

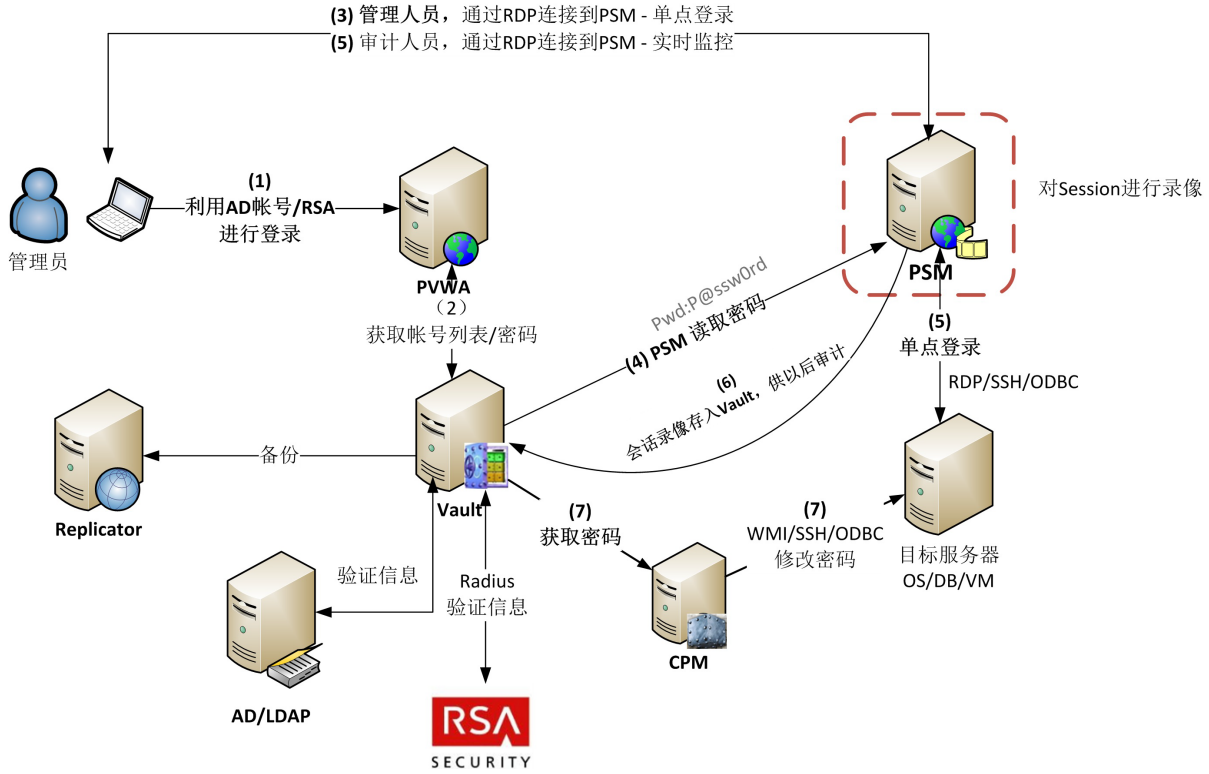

Figure 3. System architecture
图 3. 系统工作架构

2.3. 技术原理

平台通过如下手段实现运维账号全生命周期管理：

1) 口令管理插件框架：在内部形成状态机(StateMachine)的机制，形成<行动，状态，下一步行动>的模型。

```
……
StartSessionSSH,        Login,              CheckInitAction
StartSessionSSH,        PlinkStoreKey,      StoreKeyInCache
StartSessionTelnet,     UnableToConnect,    FailUnableToConnect
… …
LoginExtraUser,         Password,           LoginExtraPass
```

```
LoginExtraPass,     InvalidLogin,          FAILInvalidExtraPassword
LoginExtraPass,     Password,              FAILInvalidExtraPassword
LoginExtraPass,     AccountDisabled,       FAILAccountDisabled2
LoginExtraPass,     NotAllowedLogin,       FailNotAllowedLogin2
LoginExtraPass,     PasswordExpired,       FAILExpiredExtraPassword
LoginExtraPass,     StandardPrompt,        SwitchUser
SwitchUser,         PasswordMustChangedRootEnforced,FailTARGETInvalidUsernameOrPassword
SwitchUser,         Password,              SwitchPass
SwitchUser,         StandardPrompt,        CheckAction4
#SwitchPass,        SuWrongPassword,       FAILInvalidCurrPassword3
SwitchPass,         SuWrongPassword,       FailTARGETInvalidUsernameOrPassword
SwitchPass,         AccountDisabled,       FAILAccountDisabled2
SwitchPass,         NotAllowedLogin,       FailNotAllowedLogin2
SwitchPass,         PasswordExpired,       CheckAction2
……
```

上述例子中是针对 UNIX/Linux 的部分登陆过程，其中 LoginExtraUser 是由普通用户登录 UNIX/Linux，switchPass 是切换至 root 用户(或者其他用户)的状态，此处有 Password，InvalidLogin，AccountDisabled，NotAllowedLogin 等多种状态。此处不再由代码直接固定写死每种设备类型的执行步骤，而是由状态机的配置规定了管理模式，这样内部人员今后通过修改配置文件就可以集成各种内部设备，而且这个模式下还可以调用外部程序来实现口令更改，形成通用的管理模式。

2) 应用内嵌用户管理：应用程序内嵌用户管理就是通过 SDK 来获取动态口令，但是为了能在不重启应用的情况下面，使得应用能够更新使用到的相关口令，那么如何保持数据一致性成为管理思想的核心(见图 4)。笔者的技术思路如下：

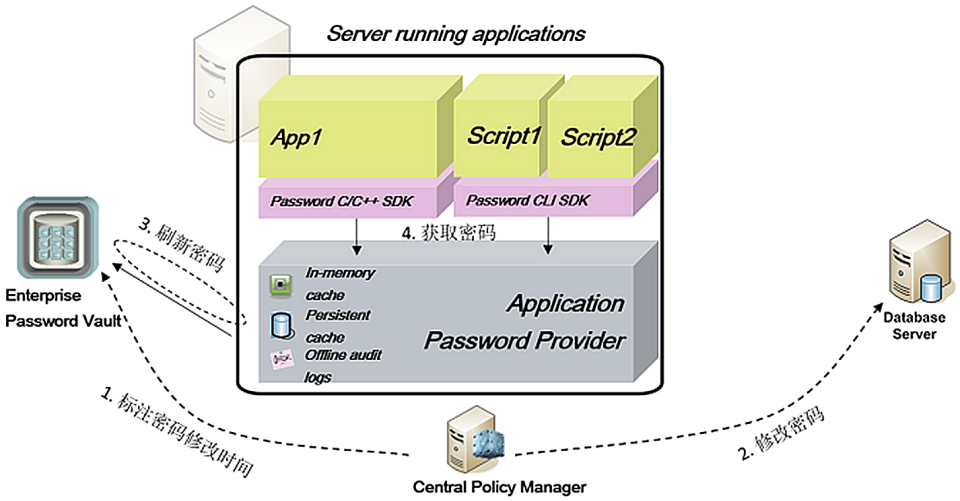

Figure 4. Password management consistency diagram
图 4. 口令管理一致性示意图

a) 口令变更模块(Central Policy Manager)在处理修改之前 3T 分钟时向 Vault 发起口令更改请求，并作标签(ChangeNotBefore)，该标签中记录了之后口令更改的时间戳。

b) 位于应用服务器本地的代理程序(Provider)具有本地缓存，并且会周期性(T 分钟)扫描 Vault 中的用户对象并刷新缓存，如果发现 ChangeNotBefore 标签时(如果里面为 10:00 am)，即知晓本地缓存在 10:00 am

时可能有新的数据变更。Provider 自然就不会在此时读取缓存。由于是周期性 T 分钟扫描，那么总能在 Central Policy Manager 修改之前刷新到 ChangeNotBefore 的标签。

c) 当 10:00 am 时，Central Policy Manager 触发口令修改，此时 Provider 又向 Vault 发送查询口令时，Vault 会锁住用户对象，不响应 Provider 的请求，一直等到 Central Policy Manager 完成口令更改请求，Vault 再向 Provider 响应最新的口令值。

d) 在口令修改期间，应用仅仅有短暂的停顿。但是由于数据库口令修改时间仅为 5~10 毫秒，因此对数据库连接影响非常之小。

上述这个方法最大程度保障了口令在应用和数据库之间的一致性，同时也满足了口令动态修改的要求。

3) 权限管理：在传统的权限管理中，UNIX/Linux 平台会依赖于 SELINUX 和普通的文件权限，windows 平台中通过组策略或者权限组来设定，但是管理粒度仍旧很粗，而且存在管理难度高、实现复杂、排查不易的特点。因此笔者利用口令集中存储的优势，在 IT 人员接触操作系统时，为他进行临时提权，提权的机制是通过输入特权口令实现，但是执行的命令又受到“权限控制器”中的规则制约(见图 5)。

上述为白名单模式，但是笔者在实践中，新建一个普通用户(UID 不等于 0)，授权其可以进行 root 提权，但是会将这样高危命令放入黑名单，如此，IT 人员虽然用这个普通用户，仍旧可以执行大量 root 的特权命令，只是 reboot 命令不能执行。这样有效防范误操作和攻击，而且也无法像堡垒机那样，可以将命令放入 shell 来绕开现有管理机制。即使放入 shell 脚本中，也受到权限控制器的管理。并且口令提供器会将提权命令上传至 Vault 中，便于集中审计。

4) 特权威胁分析：除了访问控制之外，笔者认为还需要对被管理的设备上的日志与平台日志进行关联分析，以发现内网异常行为。

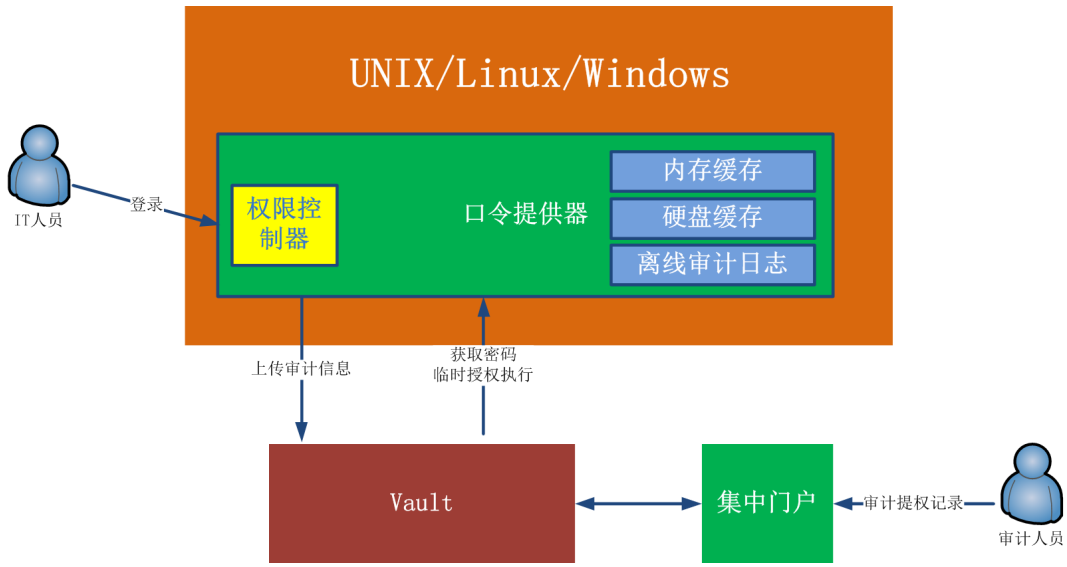

Figure 5. Schematic Diagram of Authority Management
图 5. 权限管理示意图

另外平台可以实现以下典型安全保护：

- 哈希传递是系统用户登录的时候使用口令的哈希值代替口令来完成认证，很多 Windows 的协议都是需要用户口令哈希值，并不一定非得需要用户口令，黑客可以通过 Windows 上残留的用户的哈希值来代替口令进行认证、操作。解决方案：使用平台监控 Windows AD 域控的网络数据包，从抓包中

获取到符合规则定义的可疑 Over Pass Hash 攻击操作，并结合 Central Policy Manager 组件，发现此类攻击后立即触发问题用户的口令修改，中断黑客手中 Hash 值的有效性以阻止攻击蔓延。

- 由于企业例行事务往往以月为单位，因此可以将过去 2 个月的历史数据作为基线，通过大数据分析 IT 管理员的使用习惯，对以下情况予以告警：
  - 当其访问口令频率超出正常水平
  - 当管理员在非正常时间段访问
  - 从非正常源 IP 地址访问
  - 未通过特权用户平台访问
- 另外，对非纳入管理的用户，如果在被管理设备上存在访问日志，则主动将该用户重新纳入平台自动托管，形成管理闭环。
- 禁止未通过特权平台获取口令，直接访问目标主机。
- 禁止未纳管特权用户登陆目标主机。
- 禁止特权会话中有可疑的高风险操作，比如修改底层配置文件。
- 禁止可疑的口令修改操作。正常情况下所有口令由特权用户管理平台统一管理，如果被管理设备上存在口令管理操作，而特权管理平台不存在，则一定是有黑客入侵或者其他非正常渠道修改了口令。因此需要将特权用户口令再修改一次。

3. 平台实际应用效果

目前，本平台已经在国家开发银行等单位开始使用，实现了全面的自动化管理，工作效率方面，相比传统模式有了很大的提升，实现了运维账号的全生命周期管理：

- 用户口令集中存放，定期修改、验证、重置。实现“一次性口令”的管理模式。
- 将管理模式拓展到应用内嵌用户管理，实现了应用内嵌用户动态口令的管理方案。
- 将运维账号的权限进行细分，严格实现“最小权限”原则，在加强内控管理的同时，减少各个团队之间对于权限依赖，提高了运维工作效率。
- 结合大数据分析和用户习惯，结合被管理设备的日志，发现系统用户的异常行为，以及自动化纳管未登记的用户。

下面给出了数据基线 1000 台管理设备的功效对照表(见表 1)。

Table 1. Efficiency Comparison Table for 1000 sets of management equipment
表 1. 1000 台管理设备的功效对照表

项目	传统模式 - 管理频率	传统模式 - 耗费人力(人小时)	运维账号管理系统 - 管理频率	运维账号管理系统 - 耗费人力(人小时)
口令更改	3 月	48/次	1 天	0.3/月
口令验证	无验证	N/A	1 天	0.2/月
账号梳理	6 月	120/次	1 天	0.2/月
应用内嵌账号管理	6 月	120/次	7 天	0.2/月

在运维账号管理系统模式下的管理成本仅仅限于一些管理平台的整体消耗，管理效率提高了 80 倍【计算公式：=(48/3 + 120/6 + 120/6)/(0.2 + 0.2 + 0.1 + 0.2)】，大大节省了人力成本。而且整个管理的框架更适合未来全面自动化的管理模式，可以与更多的专业系统集进行集成。更重要的是，运维账号管理形成了一个安全、集中的电子化平台，是一个该领域全面自动化的开端。

4. 平台具有的特点

1) 全流程自动化用户申请及发放，同时与移动审批结合，最大限度减少时间成本。
2) 通过用户行为分析构建用户画像，多维度用户分层定义，精细化用户操作控制。
3) 实现业内领先的应用系统用户推送，解决应用系统特定用户口令修改难题。
4) 建立操作命令黑白名单，对于高危命令执行采用实时升级审批，有效降低操作失误。
5) 多活架构部署，可以根据需要进行多中心多活部署，解决多中心远程访问缓慢问题。

参考文献

[1] 李晗. 大数据时代网上银行的安全保障义务研究[J]. 当代法学, 2016, 30(4): 24-28.
[2] 李敏, 李为民, 赖志君. 单点登录在电子商务中的应用[J]. 软科学, 2008, 22(9): 54-56.
[3] 马强, 丰树谦, 李体红. 基于网络银行发展谈计算机系统安全防范措施[J]. 新金融, 2007(5): 61-63.
[4] 王大威. 构建银行业信息安全屏障——商业银行信息科技风险防范与管理论坛综述[J]. 银行家, 2009(8): 69-69.
[5] 《中华人民共和国网络安全法》第二十一条和三十一条[S].
[6] 《信息安全技术 网络安全等级保护测评要求》(GB/T 28448-2019) [S].
[7] 吴溥峰. 网上银行信息安全体系框架的构建[J]. 西北大学学报(哲学社会科学版), 2010, 40(2): 34-38.