格尔特权账号管理系统

PAM/V3.0

技术白皮书

格尔软件股份有限公司

2026 年 3 月

格尔软件股份有限公司
上海市江场西路 299 弄 5 号（中铁中环时代广场 4 号楼）6 楼
http://www.koal.com/

版权所有© **格尔软件股份有限公司、上海格尔安全科技有限公司、北京格尔国信科技有限公司**保留一切权利。

本文档所涉及到的文字、图表等，版权归**格尔软件股份有限公司、上海格尔安全科技有限公司、北京格尔国信科技有限公司**（以下简称：**格尔公司**）所有，未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

信息更新

本文档仅用于为渠道代理商或最终用户提供信息，并且随时可由格尔公司更改或撤回。

信息反馈

格尔软件股份有限公司欢迎您通过尽可能多的渠道向我们提供尽可能多的信息，您的意见和问题都会得到我们的重视和妥善处理，请将反馈信息投递到地址：上海市静安区江场西路 299 弄中环时代广场 4 号楼 6 楼。

服务热线：400-021-8870

传 真：021-62327015

公司网址 http://www.koal.com

目录

1 产品背景 6

2 产品概述 7

2.1 产品简介 7

2.2 产品形态 8

2.3 产品架构 8

2.4 产品组件 9

2.4.1 平台服务 9

2.4.2 账号服务 9

2.4.3 会话代理服务 10

2.4.4 内嵌应用取密服务 10

2.4.5 密码保险箱服务 10

2.4.6 辅助服务 11

3 产品功能 11

3.1 资产组管理 11

3.2 资产管理 12

3.3 账号管理和发现 12

3.4 账号巡检及风险识别 13

3.5 账号改密 14

3.6 账号监控 14

格尔软件股份有限公司

上海市江场西路 299 弄 5 号（中铁中环时代广场 4 号楼）6 楼

http://www.koal.com/

3.7 访问授权 15
3.8 指令管控策略 15
3.9 SQL 管控策略 15
3.10 文件传输和剪贴板管控 16
3.11 特权会话 16
3.12 会话审计 16
3.13 工单审批 17
3.14 应用内嵌账号管理 17
3.15 用户身份管理 18
3.16 用户认证 18
3.17 系统配置和监控 19
3.18 资产视图 19
4 部署方式/运行环境 20
4.1 部署方式 20
4.2 软件化运行环境 21
5 产品技术特性 21
5.1 自动化生命周期管理 21
5.2 高效巡检机制 21
5.3 合规安全运维链路 21
5.4 覆盖应用内嵌场景 22
5.5 适应云场景 22

格尔软件股份有限公司
上海市江场西路 299 弄 5 号（中铁中环时代广场 4 号楼）6 楼
http://www.koal.com/

5.6 产品适合等保密评场景 22

6 产品优势 22

6.1 账号及风险数据可视化 22

6.2 灵活、可靠的自动改密 23

6.3 高安全用户身份认证 24

6.4 Web 方式运维覆盖各类型资产 24

6.5 丰富 SDK/插件，方便应用快速集成取密 25

7 典型应用 26

7.1 实施背景 26

7.2 解决方案 26

7.3 用户收益 28

7.4 适用场景 28

1 产品背景

特权账号是广泛存在于主机和网络设备操作系统、数据库服务、中间件控制台、物联网设备以及其他服务的身份凭据，具有访问数据、执行业务、操作文件、更改配置、变更账号权限等特殊权限，一旦控制了特权账号就掌握了 IT 系统的“生杀大权”。

随着企业数字化转型加速，IT 环境变得日益复杂，云计算、物联网等新技术的应用进一步扩大了特权账号的使用范围和管理难度。传统基于边界的防御策略已难以满足当前需求，如何在动态变化的环境中确保特权账号的安全成为了一项严峻挑战。加之内部人员的安全意识参差不齐，人为错误或违规行为屡见不鲜，这无疑增加了特权账号遭受攻击的可能性。

特权账号滥用造成数据泄露案例比比皆是，2020 年圆通速递公司回应称其内部员工与不法分子勾结，致 40 万条公民个人信息被泄露；微盟程序员删库跑路，公司市值蒸发超过 10 亿，300 万商铺瘐停业。2020 年 7 月，国内多家安全厂商检测数万台 MSSQL 服务器遭爆破入侵，沦为门罗币矿机，该挖矿木马主要针对 MSSQL 服务进行爆破弱口令攻击，爆破成功后会植入门罗币挖矿木马进行挖矿。发现在众多攻击手段中，利用弱口令攻击的占比高达 70%。另一方面，2019Microsoft Vulnerabilities Report 爆出的 189 重大微软漏洞中,81%能够通过删除用户解决。

从政策层面，网络安全已上升为国家战略，制定和颁布了一系列法规和标准，

格尔软件股份有限公司
上海市江场西路 299 弄 5 号（中铁中环时代广场 4 号楼）6 楼
http://www.koal.com/

如 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》、GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》包含对账号管理、身份鉴别、访问控制、安全审计、链路保障、敏感数据保护、日志完整性的合规要求。

因此，为了有效应对上述问题，组织必须采取更加全面和前瞻性的安全措施，强化对特权账号全生命周期的管理，构建起多层次、立体化的防护体系。这包括但不限于提升身份验证机制的安全性、加强权限管理和审计监督及建立健全应急响应机制等，从而为企业的数字资产提供坚实的安全保障。

2 产品概述

2.1 产品简介

格尔特权账号管理系统（Koal Privileged Account Management System，简称：PAM）是一款集中管理和保护操作系统、网络设备、数据库、应用系统、中间件等 IT 资产账号的运维安全审计产品。系统具备用户管理、资产管理、账号发现任务管理、账号巡检任务管理、改密计划管理、账号工单管理、日志记录等各项功能。支持消除应用内嵌密码硬编码风险，帮助企业减少账号安全隐患，抵御外部攻击风险，提高网络安全防护水平。

PAM 设计严格遵循网络安全专用产品-运维审计系统的规范标准，满足等级保护、密评等法律法规的合规要求。

PAM 适用于多个行业，包括但不限于政务、金融、运营商、电力能源、医

疗教育以及智能制造等领域，具有广泛的应用前景。无论是需要高度安全保障的金融机构，还是对数据隐私有严格要求的医疗教育机构，PAM 都能够提供必要的工具和支持，以实现对特权账号的有效管理和保护。此外，它还帮助企业提高应对安全威胁的能力，减少因特权账号管理不当所带来的风险，助力企业达成信息安全目标。

2.2 产品形态

特权账号管理系统由平台软件、平台运行环境（物理服务器、虚拟机、容器云等）和缓存、数据库、反向代理等基础服务组成。针对不同的业务场景对外提供特权账号管理维护、特权会话访问、应用内嵌账号取密服务。

2.3 产品架构

特权账号管理系统系统由平台服务、内置密码保险箱服务、会话代理服务、账号服务、内嵌应用取密服务、辅助服务、客户端组件、基础设置进行有机组合形成完整的特权账号管理系统。



格尔软件股份有限公司
上海市江场西路 299 弄 5 号（中铁中环时代广场 4 号楼）6 楼
http://www.koal.com/

2.4 产品组件

2.4.1 平台服务

平台服务采用 B/S（浏览器/服务器）架构设计，前后端分离，前端使用现代 Web 技术（如 HTML、CSS 和 JavaScript）进行开发，以实现用户友好的界面和良好的用户体验。后端采用 Java 开发，遵循标准化的 RESTful API 设计原则，确保系统的可扩展性和可维护性。平台组要完成系统的用户身份管理、资产账号数据维护、访问控制信息配置、账号安全审计、取密应用身份管理、系统配置等业务管理功能。平台作为管理中枢，为其他业务组件提供数据检索、交互支撑作用。

2.4.2 账号服务

账号服务通过 SSH/Tenlnet/WinRM/Jdbc 等远程管理技术实现远程资产账号管理，无须在资产侧安装 Agent，为平台提供资产账号巡检和改密服务。目前已适配近百种类型的资产，具备良好的扩展性，以便能快速适配新资产类型。

2.4.3 会话代理服务

为运维用户提供字符、图形、数据库、Web 会话协议代理服务，提供符合密评要求的安全运维链路和代填服务。会话过程全程记录和管控，满足等保要求的对身份鉴别、访问控制、安全审计要求。

2.4.4 内嵌应用取密服务

内嵌应用取密服务旨在消除内嵌程序中的密码硬编码问题，提供安全的密码获取服务。具体而言，应用程序的账号密码由特权账号管理系统（PAM）进行托管。在应用程序启动时，或者在内嵌账号更改密码后，应用程序会向 PAM 请求获取密码。通过这种方式，密码不再以明文形式写入本地配置文件，从而有效避免运维人员和开发人员接触到程序账号密码。这种做法不仅提高了密码管理的安全性，也显著增强了业务数据的安全性，降低了潜在的安全风险。

2.4.5 密码保险箱服务

系统内置密码保险箱服务采集多层级密钥保护机制，算法采用国密 SM4，确保资产账号密码的存储安全。系统初始化时，硬件密码模块产生高质量随机数作为系统主密钥。系统主密钥支持由密码卡或外部密码机/密码服务平台保护。资产账号密码采用一账号一密钥方式存储，其中密钥由系统主密钥保护。

2.4.6 辅助服务

辅助服务包括以下几个关键组件：

密码接口服务：该服务用于统一适配密码卡或外部接入的密码机，确保不同设备之间的兼容性和交互性，从而提供统一的密码管理解决方案。

设备配置服务：此服务主要为平台提供设备的网络配置、时钟服务及主机名等相关配置。

监控检测服务：此服务负责对系统资源状况、平台各组工作状态进行实时监

控。当系统检测到异常情况时，会及时产生告警，通知相关人员进行处理。这一机制能够帮助运维团队迅速响应潜在问题，确保系统的稳定性和可靠性。

这些辅助服务共同构成了一个全面、可靠的平台支持体系，提升了系统的安全性和可管理性。

3 产品功能

3.1 资产组管理

按照业务系统分组管理资产，可以有效提高资产管理的灵活性和安全性。每个资产组指定一名或多名管理员，负责该组内资产的管理，拥有相应的数据权限以维护资产账号、访问授权和进行安全审计。系统允许对敏感操作权限进行细致设置，如查看组内资产账号明文密码和重置资产账号密码。通过这种分组管理和权限控制机制，可以显著提升资产管理的安全性，降低潜在的安全风险。系统等价资产、账号管理，相关资产配置为等价资产或账号时，修改其中一台资产账号密码，所配置的等价账号密码自动更新。

3.2 资产管理

资产信息日常维护包括手动增加、修改、删除等操作，以及通过文件方式导入或按 B/C 网段端口扫描方式批量导入资产账号。资产基础信息包括资产类别、系统类型、远程访问协议、端口；也支持配置资产允许访问 IP 白名单、访问时段、文件是否允许下载等信息。

每个资产允许配置一个用于日常资产的账号发现和巡检的管理账号(链接账号)。系统支持以附属资产模式在主机类资产上创建附属资产，以便关联操作系统账号或使用操作系统账号进行改密或巡检，例如 VNC 服务、部分中间件控制台或网安设备 web 控制台。

系统可以自定义资产类型和属性，在原有资产分类基础上，可以新增编码、协议、端口、自定义分类等多种分类方式。可对云上主机、网络、数据库类资产账号进行统一管控，同时支持国内主流云厂商 AccessKey、AccessKey Secret 的安全管理。

3.3 账号管理和发现

资产账号日常维护包括手动增加、修改、删除、禁用、启用等操作，以及通过文件方式批量导入资产账号；在资产配置有管理账号情况下资产巡检和账号发现也能从资产上读取资产账号列表和账号信息，合并形成资产完整的账号清单。

账号基础信息包括账号类型[普通账号|管理账号|程序账号]、账号密码、账号安全级别信息。各类型账号管理上存在差异，例如：程序账号不允许托管密码；管理账号密码不允许为空等。资产账号密码支持预设保存到 PAM 平台上，也支持托管，即 PAM 系统立即重置改密密码，用户不再掌握该密码。账号安全级别主要用于特权会话访问时对高安全级别账号实施二次认证或会话流程审批管控措施。

账号发现支持自动采集账号关联属性信息，采集范围包含：

（1）银河麒麟等 UNIX/Linux 类主机：账号 ID、上次密码修改时间、所属用户组、最后登录时间、账号过期时间、家目录、Shell 类型、权限等级、是否允许修改密码；

（2）Windows 主机：上次密码修改时间、所属用户组、最后登录时间、账号过期时间、是否允许修改密码；

（3）Oracle 数据库：UID、账号状态（正常 / 锁定）、账号创建时间、默认表空间、密码过期时间、账号系统权限、所属角色（如 DBA）、上次登录时间；

（4）人大金仓、达梦、MSSQL、MySQL、PGSQL、HANA、MongoDB 等主流数据库：账号创建时间、密码是否过期、上次密码修改时间等信息。

3.4 账号巡检及风险识别

账号巡检目的是识别资产上存在的账号脆弱性和异常活动。系统通过创建或执行周期性巡检，使用管理账号远程登录上资产读取账号信息，通过与 PAM 系统记录的账号信息比对分析，产生账号数量、信息差异记录，并识别长期未登录、未改密、弱密码、访问绕行、密码失效等账号风险，内置账号评分模型对资产账号风险项进行评分，让管理员直观掌握资产账号总体安全状况和威胁变化趋势。支持资产与账号安全分析，可识别弱密码、僵尸账号、幽灵账号、权限变更、长期未改密等异常账号，通过不同颜色可视化标注业务风险等级；支持账号白名单配置，覆盖僵尸账号、幽灵账号、超时未改密账号、提权账号、空密码账号、非

法名称账号。具备异常账号风险治理能力，可展示僵尸账号、幽灵账号、弱密码账号、提权账号等风险账号待整改清单，并支持对完成整改的风险账号执行一键复核。

3.5 账号改密

账号密码安全是特权账号管理主要目标，除了将密码存储于内置密码保险箱中安全存储外，也需要按照相关法律法规要求周期性修改资产账号。PAM 改密已适配近百款各类型资产，改密触发方式分为自定义改密任务、托管改密、单账号重置密码等三种方式，其中改密任务需要改密账号范围、密码生成规则以及执行周期；而托管改密则按照资产密码策略定期修改托管账号密码，改密完成后输出改密结果报告，让管理员轻松完成账号密码维护工作。支持在申请相关资产、账号的密码时，可设置密码有效期。经过审批后的账号，过期自动修改密码。

3.6 账号监控

该功能主要为管理员提供可视化界面，直观查看资产账号密码等数量和分布，账号数量变化趋势、风险账号数量、各类型账号风险变化趋势、风险资产排名、风险账号明细以及账号增减变化明细，相关数据支持账号报表导出。

3.7 访问授权

PAM 系统提供了单用户、单资产账号、多对多模式团队授权、基于用户和资产账号的属性动态策略授权(ABAC)等长期授权功能。系统也提供权限工单方式增

加长期或短期访问权限，针对线下运维使用托管密码的运维场景也可以申请使用明文密码，工单结束后系统重置账号密码回收权限。

3.8 指令管控策略

系统支持对 ssh/telnet/rlogin 等协议会话过程中可能出现的高危命令进行管控。系统内置正则高危管控指令模板，支持配置适用的资产账号和运维用户；指令策略响应中包括放行、审批、阻断、终止会话，其中放行的指令需要运维用户做二次确认，审批的指令管理员审核通过才允许执行；指令集之间允许配置优先级。

3.9 SQL 管控策略

系统支持主流数据库进行高危 SQL 管控，系统支持定义以关键字匹配为主的 SQL 管控规则，支持配置适用的资产账号和运维用户；策略响应中包括放行、审批、阻断、终止会话等四种类型，需要审批的 SQL 需要管理员审批通过才允许执行；SQL 管控策略之间允许配置优先级。

3.10文件传输和剪贴板管控

文件传输主要涉及操作系统类资产访问和通过应用发布方式运维的文件上传下载。Linux 主机支持控制 Sftp/Ftp 文件下载或上传；Windows 主机(含应用发布)支持控制驱动器重定向、剪切板文件上下行、剪切板文本下行；以及 Web 方式访问 Windows 挂载的安全文件夹文件下载管控。在实际业务场景中也支持

基于用户源 IP 的控制文件传输。

3.11特权会话

系统提供统一的运维会话入口，支持运维 Linux 主机、Windows 主机、主流关系数据库、Web 应用等类型资产。为会话提供安全运维链路，确保会话过程中的机密性和完整性；会话建立实现单点登录和代填，确保资产账号密码安全，客户端工具已适配主流字符运维工具、远程桌面以及自研带水印图形客户端、数据库工具 Dbeaver、Navicat、Smss、Sqlyog、Plsqldev、达梦 Manager、人大金仓等 Manager 工具，Web 提供 DOM 级别精准代填服务。系统还提供会话协同能力，允许运维人员邀请其他用户加入会话协同运维。

3.12会话审计

运维会话访问过程系统全程记录，包括不限于字符指令和录像、图形录像和键盘鼠标操作、剪贴板操作、关键字、文件传输、SQL 操作日志、WebURL 日志等;字符和图形支持录像审计（含应用发布方式的运维录像）,SFTP/FTP/RZ/SZ 可开启文件内容审计；审计日志支持离线备份和导出，为安全事件溯源审计提供可信依据。

3.13工单审批

系统内置工单审批能力，账号新增、删除、变更等账号运维操作可通过工单发起；支持自定义审批流程模板，所有操作全程留痕、可追溯。申请资产、账号

密码时支持设置密码有效期；账号申请审批通过后，密码到期将自动执行改密操作。

3.14应用内嵌账号管理

针对应用内嵌账号的业务场景提供应用取密服务。系统内根据集成方式或服务类型定义不同的取密应用类型，配置订阅账号方式标识应用内嵌哪个账号，支持双账号轮换取密场景。同时，也考虑取密应用为集群场景，所有取密应用的身份均对应到具体的部署实例。取密过程中会对取密应用做严格身份鉴别，该身份鉴别利用应用运行态属性生成身份指纹，可以有效避免取密身份被冒用，系统也充分考虑取密程序升级业务，支持平滑更替身份指纹。

系统提供一系列集成 SDK 和插件，方便应用快速接入 PAM 取密，取密插件支持周期性检索新密码，动态更新密码能力。系统具备资产快速检索能力，通过对新增加的资产类型、属性等字段的快速筛选，搜索到相关资产。

系统也支持主动推送的方式同步最新资产账号密码到指定的应用。

3.15用户身份管理

系统用户身份维护支持手动添加、编辑、删除，也支持通过表格方式批量导入或外部业务系统同步，例如 LDAP 服务器、第三方 IAM 系统。用户身份主要信息包括账号、所属组织、姓名、账号有效期、邮件、手机号、允许访问白名单、允许登录的设备 MAC、证书 ID、用户标签、用户密码、用户状态等信息；用户账号过期自动锁定账号，用户标签主要用于动态策略授权。

组织机构也是支持手动维护或来自于第三方系统的同步。支持组织机构上配置管理员，开启按组织机构数据权限控制开关后，每个管理员仅能查看到本机构或下级机构的用户数据和资产数据。

3.16用户认证

系统提供完善的身份认证功能。包括本地账密认证、国密证书认证、LDAP认证、Radius 认证、钉钉扫码、企微扫码、飞书扫码等认证功能。其中非扫码模式支持组合短信、OTP、令牌等动态因子，实现强安全身份认证。系统也具备接入 4A 等身份平台实现标准 CAS 协议认证，以及网关设备代理认证、浏览器国密证书双向认证能力。

系统也具备完善的认证安全机制，IP 白名单控制、连续认证失败锁定用户、锁定 IP、长期未登录锁定账号、Web 空闲时长、用户密码策略等安全措施。

3.17系统配置和监控

系统具备完善的配置管理和监控能力，包括不限于告警模板、日志外发、数据备份、巡检参数、协议代理参数、双机热备、短信通道、推送设置、密钥保护、应急逃生、界面个性化设置等功能。提供设备状态和组件运行状态监控能力。系统提供工单审批能力，通过工单进行账号操作，如增加账号、删除账号、修改账号等，支持审批流程模版，支持相关操作留痕。系统提供密码查询、系统事件等 API 接口；支持账号密码备份、系统配置备份等备份功能；支持日志对外推送至第三方平台。

可以从格尔运维安全管理系统同步资产、账号数据。当运维安全管理系统中资产、账号数据发生更新时，特权账号管理系统相关数据可同步更新。

3.18资产视图

该功能可全面总览企业内部主机、网络设备、数据库等各类核心资产的账号分布状况，不仅能清晰呈现账号在不同资产类型中的数量占比、归属关系，还能精准统计出各类账号存在的风险等级及具体风险点，让管理者对整体账号安全态势一目了然。

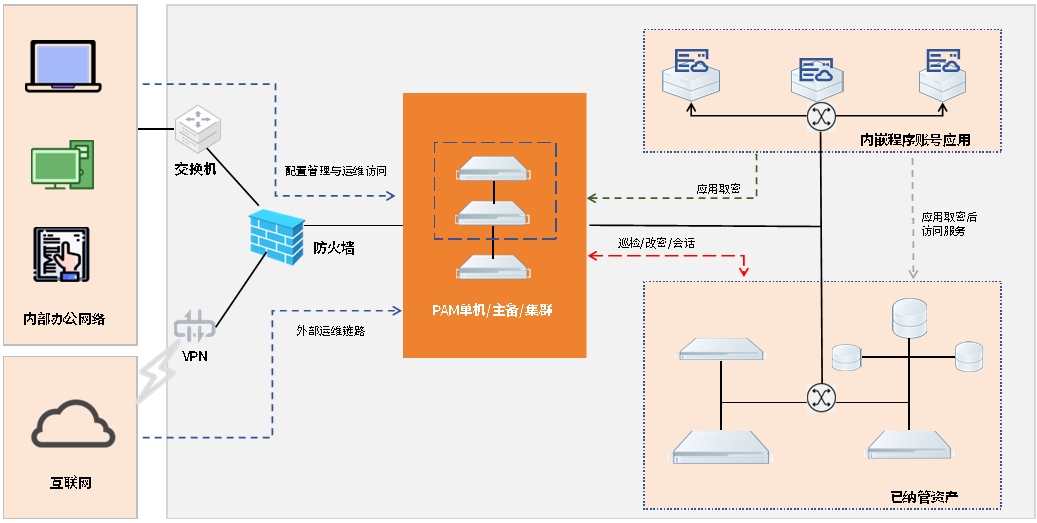
在异常账号管理方面，支持多维度统计与查看：既可以从全局视角掌握系统内所有异常账号的整体分布情况，也能按部门维度细分，了解各部门异常账号的数量、类型及占比，还能按主机、网络、数据库等分项进行精准统计，快速定位不同资产类型下的异常账号问题。

同时，该功能具备强大的趋势分析能力，能够直观展示异常账号在最近一年、半年以及一个月内的动态变化趋势，包括异常账号数量的增减波动、风险等级的变化走向等，通过清晰的趋势图表，帮助管理者及时发现账号安全管理中的潜在规律与隐患，为制定针对性的安全策略提供数据支撑。

格尔软件股份有限公司
上海市江场西路 299 弄 5 号（中铁中环时代广场 4 号楼）6 楼
http://www.koal.com/

4 部署方式/运行环境

4.1 部署方式



产品承载着包括资产账号密码等核心敏感数据，因此建议采用主备或集群的高可用方案部署，推荐使用物理机。由于需要面向运维用户提供运维代理服务，通常 PAM 部署在 DMZ 区，对用户侧仅暴露必要的业务端口，后端资产侧开通 PAM 到资产运维和账号管理端口策略，有应用取密的的业务，则需要向后端应用放开从 PAM 取密服务端口网络策略。

4.2 软件化运行环境

服务器规格： 8 核(X86/ARM)16G 硬盘 500G

操作系统： UOS V20/银河麒麟 V10/Centos7.9 /Ubuntu20.0.4

数据库： mysql8/Oceanbase4.3/达梦 V8/人大金仓 V8r6

格尔软件股份有限公司
上海市江场西路 299 弄 5 号（中铁中环时代广场 4 号楼）6 楼
http://www.koal.com/

5 产品技术特性

5.1 自动化生命周期管理

支持近百种 IT 资产账号的自动发现、改密、禁用、删除等全流程管理；支持快速扩展适配新资产类型。

5.2 高效巡检机制

巡检采用多线程并发机制，同时对多个资产进行巡检，遵循避免多次登录的原则设计思路，可以极大降低对资产的访问频率，不增加资产运行负荷，提升巡检效率。针对数据库使用了 24 万规模弱密码字典，单账号弱密码检测耗时控制在 2 秒以内。

5.3 合规安全运维链路

1) 特权会话全链路管控：支持会话录制、命令拦截、实时监控，会话审计。

2) 产品设计符合零信任理念，支持多因子身份认证，权限最小化及动态访问控制，支持临时权限任务工单。

3) 健全的协议代理服务能力，精准、安全的账号密码代填功能。

5.4 覆盖应用内嵌场景

产品主动推送或提供取密服务接口方式覆盖主流应用内嵌账号密码场景，例如多编程语言应用程序、Java 数据库应用、中间件数据源应用、Nacos 配置中

心、Apollo 配置中心、数据库 DB_link、Ansible、Jenkins Credentials、Windows 凭据管理器、脚本命令取密(CLI)、kubernetes secret 等场景。

5.5 适应云场景

支持主流共有云平台账号纳管和云内资产纳管；产品可在云信创环境中部署。

5.6 产品适合等保密评场景

1) 产品符合网络专用产品安全功能要求和运维安全管理产品安全技术要求，取得《网络安全专用产品安全检测证书》。

2) 产品在访问链路机密性和完整性、敏感数据保护、控制信息完整性、日志完整性保护等设计符合密评要求，产品取得二级商密资质。

6 产品优势

6.1 账号及风险数据可视化

资产账号集中管理后，利用账号发现和巡检功能，自动采集资产账号增减变化和资产信息变更数据，通过账号必读和风险识别后在账号监控页面可视化展示账号及风险数据，包括：

1) 资产、账号、密码数量、账号分布图标以及账号数量变化趋势。

2) 账号风险数量统计，总体风险评分、风险统计趋势、风险资产排名。

3) 资产数量变化明细和统计。

4) 各类型风险账号明细。

6.2 灵活、可靠的自动改密

资产账号密码是信息安全关键屏障,因此对 IT 资产管理员来说定期轮换和记住资产账号密码日常管理中最重要的工作，一旦发生密码遗失和泄露，带来的风险将无法估量。PAM 提供了完善的自动改密功能，可以实现：

5) 自动轮换修改主机、网络设备系统账号密码，无需安装 Agent;

6) 自动轮换 oracle、人大金仓、mysql、达梦、sqlserver 等主流数据库资产账号密码以及中间件 Web 控制账号密码。

7) 可以指定修改密码、自动生成随机密码、上传密码文件、密码复杂度等方式生成新密码；可以制定自动改密任务周期、手工执行、支持使用密码本轮换模式的任务改密。

8) 通过导出、邮件方式、异地备份数据库保存密码文件，做到改密前自动备份、改密后自动备份，防止密码丢失。

9) 提供密码手工验证、手动重置、密码回滚的容错机制，确保密码修改失败之后恢复到正确的密码。

10) 批量改密，通过创建改密计划方式，关联多个待改密的账号，实现批量改密能力。具备改密的安全保护机制，确保改密成功率，在批量修改密码时确保改密零失败。

11) 具备账号密码变更能力，支持配置自动改密策略，可自定义改密执行时间、改密周期及密码规则，实现系统账号定期自动改密。

6.3 高安全用户身份认证

为了提高用户身份的可靠性，防止身份冒用，特权账号支持以下认证机制实现：

1) 支持基于国密用户证书的浏览器双向认证，确保运维链路接入安全。

2) 国密证书+PIN+动态令牌组合认证，满足密评要求。

3) 支持 LDAP(AD 域)、RADIUS 认证。

4) 支持本地账密+OPT 因子组合认证，兼容谷歌身份验证器和通讯令牌。

5) 支持安全应用网关代理认证或通过 CAS 协议接入 IAM 统一认证。

6) 支持钉钉、企微、飞书扫码认证。

6.4 Web 方式运维覆盖各类型资产

基于 H5 技术实现浏览器客户端运维，无需安装本地工具，直接支持浏览器打开运维界面操作:

1) 支持 SSH、Telnet、Rlogin、RDP、VNC、Sftp、Ftp 协议的 Web 客户端运维；

2) 支持 SSH、Telnet、Rdp、Sftp、ftp 协议运维文件传输；

3) 支持 Mysql、Oracle、MS-SQL、达梦、人大金仓等数据库协议的 Web 客户端运维，实现 SQL 级别安全管控；

4) 无须应用发布实现 Web 应用类资产代理访问，实现会话审计和 URL 审计；

5) 支持主机类资产会话协同功能。

6.5 丰富 SDK/插件，方便应用快速集成取密

为方便应用快速集成接入 PAM 取密，缩短集成调试周期，PAM 提供一系列取密 SDK 和插件：

1) Java/C/GO/.Net 多语言版本 SDK。

2) JDBC 取密插件。

3) Weblogic/WAS 数据源动态改密服务。

4) Ansible/Jenkins Credentials 插件。

5) CLI 工具。

6) Kubernetes Secret Server 服务。

格尔软件股份有限公司
上海市江场西路 299 弄 5 号（中铁中环时代广场 4 号楼）6 楼
http://www.koal.com/

7 典型应用

为了深入探讨某省电信运营商项目的典型应用案例，我们将分析其实施背景、解决方案、用户收益、适用场景。

7.1 实施背景

日常客户和三方厂商的许多技术人员都需要访问 IT 资产进行运维、数据分析、安装部署、升级、迁移等操作，对 IT 资产的安全管理带来了很大的挑战，存在以下问题：

1) 大量的 IT 资产账号采用人工的方式进行管理难度大，效率低下；

2) 账号密码由运维人员掌握，存在泄露的风险；

3) 密码长期不修改，存在许多僵尸账号和弱密码账号，账号安全风险较大。

7.2 解决方案

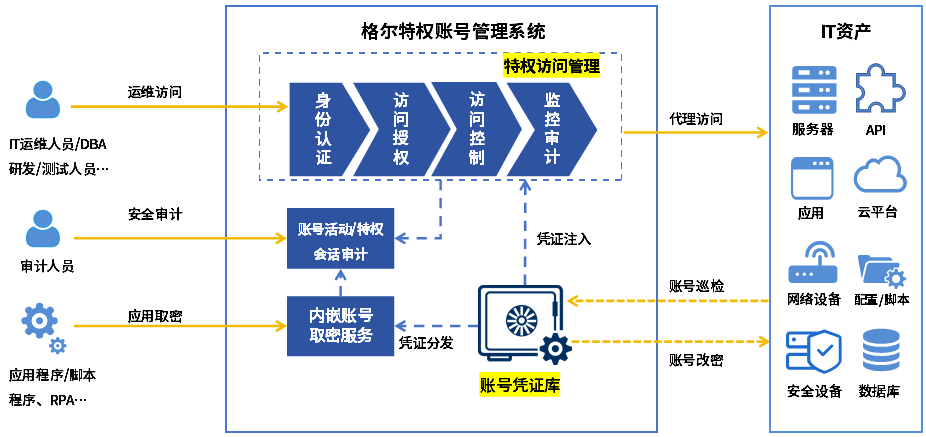
针对上述问题，省公司采购了格尔特权账号管理系统，通过项目实施实现资产账号凭证库，确保账号密码存储安全和轮换改密，解决运维、开发、管理人员直接掌握账号密码的问题，有助于降低密码泄露风险，减少未经许可的异常访问。

在项目实施期间，客户对旧堡垒机系统中导出的资产、账号及密码等数据进行了细致的比对和确认。随后利用 PAM 系统提供的批量导入功能，顺利完成了业务数据的初始化。

导入后按照规划对已纳入管理的操作系统和数据库类账号系统执行每季度

一次的自动密码，实现密码托管，符合集团要求的密码管理要求。

系统开启定期执行资产巡检检测资产账号潜在的风险。截至 2024 年底，累计识别并报告了 100 个使用弱密码的账号、超过 80 次的账号访问异常绕行以及 20 余个无归属的新账号，并通过账号监控模块实现资产账号总量、资产账号分布、账号增减变化、账号风险明细、资产风险排名等全方位可视化效果展示。



利用 PAM 提供的特权账号全生命周期管理功能，依据需求在目标资产上创建、禁用、启用或删除运维账号。利用特权会话协议代理组件，实现了身份鉴别、集中授权、访问控制、单点登录、会话监控审计等运维审计功能，有效避免了运维人员直接掌握账号密码带来的风险。

针对程序账号密码业务能力，项目建设期间客户安排 ITSM 系统集成了 PAM 提供的 JDBC 取密插件，集成过程只需要重新打包并修改配置后上线运行，ITSM 顺利从 PAM 侧获取到订阅账号的密码，系统本地不再存储密码解决了凭证硬编码的问题。

7.3 用户收益

1) 系统化梳理资产与账号信息，构建清晰的账号管理体系，使账号分布与状态一目了然，大幅提升管理效率；

2) 自动化改密功能显著提高了账号密码更新的效率与准确性，有效减少了人工操作可能带来的错误；同时，运维代填账号密码和应用内嵌账号取密的落地，大幅收敛了密码泄露的风险；

3) 通过定期巡检和智能分析，系统能够主动发现弱密码、无主账号及异常访问等潜在漏洞，并及时采取措施，将风险扼杀在萌芽状态，保障系统安全稳定运行。

4) 产品满足等保和密评的合规要求，具备优秀的信创替代能力，有效解决了信息安全、国产化替代等多个问题，节约预算投入。

7.4 适用场景

特权账号管理系统适用于各类需要严格控制和管理对关键信息系统访问权限企业。其主要适用场景包括但不限于以下几个方面：

1) **数据中心和云服务提供商**：管理和保护用于维护服务器、网络设备及云资源的特权账号。

2) **金融机构**：如银行、保险公司等，需严格管理对敏感客户信息和交易系统的访问。

3) **医疗保健行业**：确保患者数据的安全性，管理对电子健康记录系统和其他医

疗 IT 资源的访问。

4) **政府和公共部门**：保护政府数据库和公民个人信息，防止未经授权的访问。

5) **制造业**：管理对生产控制系统、设计软件及其他关键业务应用的访问。

6) **零售业**：保护顾客支付信息和销售数据，同时管理企业资源规划(ERP)系统中的特权访问。

7) **能源与公用事业**：保证对电力网、水处理设施等关键基础设施的安全访问。

8) **教育机构**：管理对学生信息系统、研究数据和校园网络的访问权限。

9) **媒体和娱乐公司**：保护知识产权和敏感内容，同时管理内部 IT 资源的访问。

总的来说，任何涉及敏感信息处理或关键业务流程的企业和组织都可以从特权账号管理系统中受益，以提高安全性，降低风险，并符合合规要求。PAM 解决方案帮助这些企业确保只有经过授权的人员才能访问特定的系统和数据，从而有效地保护了企业的核心资产。

格尔软件股份有限公司
上海市江场西路 299 弄 5 号（中铁中环时代广场 4 号楼）6 楼
http://www.koal.com/