格尔软件
KOALSOFTWARE

格尔特权账号管理系统

产品白皮书

格尔软件股份有限公司

2023 年 3 月

权利声明

免责声明

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 背景

近年来，随着“网络强国”、“信息技术应用创新”、“数字化转型”等国家战略思想的不断提出，各党政机关和企事业单位积极响应和贯彻落实国家战略，在国家电子政务外网和互联网的网络环境下，建设了大量的应用系统和安全保障系统。在国家提出的互联互通、安全共享、业务协同的指导方针下，实现了相关单位之间的网络互通、业务协同和数据共享，并通过建设统一身份管理等相关系统，实现了使用系统的用户身份安全、认证安全和审计安全等，为应用系统的安全访问、安全授权、安全审计提供了安全基础。

随着国家网络安全主管部门和密码主管部门对“等级保护”、“密码测评”等相关测评的进一步强化要求和重视，各单位也加深了对等级保护和密码测评要求的理解和落实。除对业务应用系统使用人员身份管理要求外，网络设备/安全设备/密码设备/应用系统等后台管理配置的人员管理也是等级保护和密码测评关注的重点，也是实行密码保护和安全防护的难点，特权账号管理的概念应运而生。

特权账号既包括操作系统中的 root 账号、数据库中的 DBA 账号，又包括这些系统中普通权限的账号，及网络设备、安全设备、集中管理控制平台（云管平台、自动化管理平台等）、Web 管理后台等的管理账号。特权账号可在运营过程中，给相关业务运营、系统管理、系统运维等人员赋予系统维护、权限增加、数据修改删除、导出等高级权限，这些账号及其持有人掌握着信息系统的生死大计，绝大部分时间这些账号都在为各项客户业务正常开展保驾护航。

根据国标 GBT22239-2019《信息安全技术网络安全等级保护基本要求》（等保 2.0）、国家保密局《涉及国家秘密的信息系统分级保护管理办法》和信安标委 GBT 39786-2021《信息系统密码应用基本要求》，要求对所有使用特权账号访问的用户进行身份鉴别、账号密码应有复杂度要求并定期更换、应授予完成任务所需的最小权限、应及时删除多余的、过期的帐户、对访问的活动进行安全审计。因此满足合规性、精细化管理需求的特权账号管理产品是信息安全必备安全基础设施之一。

格尔特权账号管理系统通过建立资产特权账号库，实现对特权账号全生命周

期的管理，集中保护和更改特权账号密码；采用多因素子用户身份认证机制与细粒度访问控制机制，防止滥用特权，确保特权会话安全可信，会话全程记录；为应用内嵌密码提供取密服务及快速集成 SDK/组件，消除应用内嵌特权凭证硬编码现象，降低凭证泄露风险，缩小特权攻击面。通过以上特权账号管理和防护措施，满足等保要求和密评要求，促进信息化管理的自动化、智能化和安全化，为信息化安全建设赋能、提质增效。

第三，建立国信新网安全运维体系。国信新网网络中开展业务的用户群体主要有两大类，一是使用业务应用系统的普通用户群体，二是各类服务器、操作系统、网络设备、数据库的后台管理者群体。普通用户群体的身份认证、访问控制和安全审计等由统一身份管控体系实现，后台管理者的身份认证、鉴权、指令控制和操作审计等，需要建立安全运维体系进行统一管理。在等保 2.0 和密评要求中，都对安全设备、网络设备、操作系统和数据库中的后台管理特权账号的管理和使用提出了明确的要求，因此建立对特权账号的集中发现与收集、托管与巡检等合规化、自动化管理的安全运维体系是国信新网通过等保和密评的必要条件。特权账号运维体系不仅应满足对“人”的管控和服务，还应满足对应用系统配置文件、中间件配置文件、自动化运维脚本等“非人”的使用对象中，明文存储的数据库密码等特权账号的管控和服务。通过提供特权账号的不落地服务，避免运维人员、研发人员、测试人员等接触到敏感的数据库密码等数据，也为“护网行动”提供特权账号的防护能力，保护好数据安全的最后一公里。

2 产品概述

2.1 产品简介

格尔特权账号管理系统（简称 PAM：Privilege Account Manager）是为网络中设备、操作系统和应用系统等提供特权账号管理的一款产品，它通过对特权账号的集中管理、自动发现、自动改密、会话管控等技术，对管理对象的操作特权账号、服务内嵌特权账号等提供自动化、智能化的管理；通过多因子认证和细粒度访问控制，对使用特权账号的人员进行身份认证和访问控制，保证特权管理会话安全并提供会话全程记录；通过国密算法对特权账号、敏感配置等数据进行加密存储，保证账号和配置基于国产密码技术的存储安全。

系统支持热备部署，支持以多租户模式为不同使用者提供完全隔离的、差异化的服务；提供统一的管理、监控、审计、授权，自身符合等级保护要求；支持独立部署和云上部署（支持私有云、公有云、混合云环境）。

以信息系统特权账号为核心，通过特权账号的发现和纳管、自动改密等技术，提供一套信息系统特权账号管理的自动化技术措施，加强对特权账号底账动态管理能力，及账号全生命周期管理能力，实现信息系统特权账号的统一管理和合规使用。

2.2 产品形态

可提供硬件一体化的整机产品形态，也可支持云环境下多租户的部署模式。

2.3 总体架构

系统设计基本思路：统一资产、账号、凭证、应用管理，构建符合等保和分保要求的特权账号管理体系；遵循“零信任，始终验证，强制执行最小特权”进行身份鉴别和访问授权；实现“事前预防、事中管控、事后审计”的会话监管体系，达到资产账号厘得清、身份认证可信任、访问权限最小化、风险识别实时化、事故责任可追溯的内网安全管控目标。

产品遵循最小权限设计，系统角色支持三员管理，通过角色划分功能权限。数据权限方面主要以资产组为维度的权限配置，按照组配置管理员模式管理资产、账号、改密、巡检、应用配置等功能。

系统总体架构下图所示：

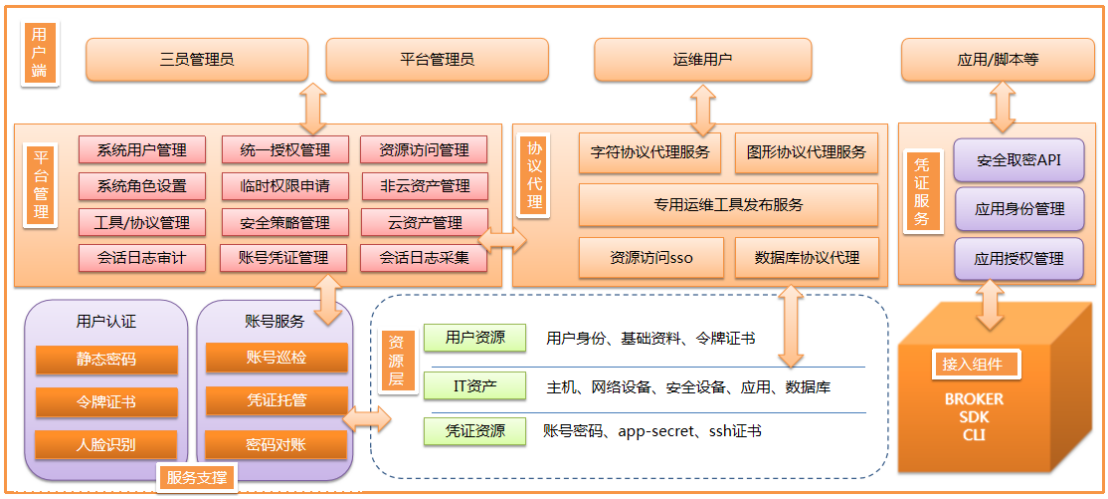

图 1　格尔 PAM 总体架构图

2.4 产品组成

格尔特权账号管理系统 WEB 平台采用前后端分离架构，基于三员分立设计理念，实现机构管理、人员管理、角色权限、资产账号管理、账号凭证管理、应用身份及应用特权管理、授权管理、监控审计、系统管理、特权会话等产品功能。

协议代理模块是会话管控核心支撑组件，由图形协议代理、字符命令协议代理、数据库协议代理等组件组成，实现单点登录、会话状态、审批或阻断指令执行、会话录像和日志记录等功能。该模块独立运行，对外提供安全访问通道。

账号服务模块是系统账号管理驱动组件。主要有资产的账号自动发现、账号凭证(密码)更换、密码定期对帐等功能。

认证模块实现对用户的身份鉴别功能，内置证书、密码认证、AD/LDAP 密码认证功能。实现基于静态密码+动态口令(短信验证码、邮件验证码、TOTP)双因子认证方式。

凭证服务模块是为第三方应用通过特权凭证分发和配置下发服务。支持 RESTful,soap 及 socket 方式接入。满足应用/脚本/自动化/容器等内嵌账号场景动态取密需求。

3 产品功能

模块	功能描述

用户认证	☆ 支持证书认证 ☆ 支持 PAM 用户密码认证+动态口令式认证 ☆ 支持 LDAP 密码认证+动态口令方式认证
用户管理	☆ 用户账号管理 ☆ 组织机构管理 ☆ 部门分权管理 ☆ 用户访问权限分配 ☆ 支持“三员分立” ☆ 用户账号信息 LDAP 导入 ☆ 用户账号信息模板文件导入 ☆ TOTP 验证码密钥管理 ☆ 文件下载权限设置
资产管理	☆ 资产组(业务系统)添加、移除。配置资产组管理员，支持按管理员的数据权限管理资产、维护账号、扫描巡检、账号改密、取密应用。 ☆ 批量导入方式导入资产，或通过端口扫描方式快速扫描主机、网络设备、安全设备端口方式批量添加资产，添加管理账号[用于设备巡检、重置密码、账号维护]; ☆ 支持手动或定时任务对目标设备/对象发起扫描，并输出扫描结果，形成资产账号底数。 ☆ 资产账号创建、禁用、启用、刷新、移除账号权生命周期管理(账号刷新主要从资产同步账号信息)。支持批量导入管理账号。 ☆ 手动或按纳管策略自动纳管账，设置资产账号密码托管、分级、配置跳转账号 ☆ 允许用户自定义资产账号密码策略，配置密码强度要求、账号有效期。 ☆ 资产账号采用符合密评要求的国密算法保护账号密码，使用根密钥->主密钥->数据密钥的三层级密钥保护机制,根密钥支持硬件密码卡内密钥和密码机内数据密钥，未不符合密评要求密码算法。 ☆ 内置资产巡检任务，分资产组分段多线程执行资产账号扫描，扫码仅短暂登录资产读取账号数据，不会过多消耗设备和应用服务计算资源;

	☆ 账号巡检识别资产账号存在安全风险，包括不限于长期未登录僵尸账号、新账号（幽灵账号）、长期未改密、弱密码、访问绕行、账号所属组变化、账号被删除、账号密码过期、管理账号登录失败、网络问题等。对资产账号风险扫描后按照内置风险评估模型进行打分，并输出巡检报告。 ☆ 资产扫描无须安装插件，采用主动发起扫描远程，故障时停止扫描，不会影响被扫系统的正常运行；部署实施时仅需要开通资产账号管理端口或远程访问端口策略，可以不改变应用系统的网络拓扑结果。 ☆ 账号监控集中展示资产数量、账号总量、凭证数量、托管密码数量，资产账号分布、资产类型分布；展示 IT 网络资产中存在的资产账号风险数量，风险资产和账号占比；风险资产 TOP100 排名。风险账号明细支持按系统名称、账号名、IP、类型、角色、账号创建时间、账号状态等导出。支持导出账号风险趋势报表，数据包括资产账号风险数量、账号增减变化情况。 ☆ 支持以 API 接口方式将扫描任务的结果推送或将资产信息导入至指定的信息化平台
访问授权	☆ 授权创建、移除、分配授权组 ☆ 支持批量授权资产账号和用户 ☆ 即时授权审批、历史记录查询 ☆ 字符命令金库审批 ☆ SQL 指令金库审批 ☆ 支持用户下载权限审批
应用特权管理	☆ 应用身份管理及应用身份标识，通过配置绑定方式关联特权账号信息 ☆ API 接口读取特权账号信息，实现应用特权审计
安全审计	☆ 在线会话记录、实时监控、会话中断和访问隔离 ☆ 历史会话记录、录像回放、命令集查询 ☆ 查询历史命令行操作记录 ☆ 查询历史 SQL 语句操作记录 ☆ 查询文件传输日志 ☆ 查询系统平台操作日志 ☆ 查询认证日志，用户认证和资产访问认证

	☆ 应用配置访问日志、第三发接口调用审计 ☆ 访问隔离管理，支持查看和移除隔离对象 ☆ 用户权限报表及导出
管理功能	☆ 系统会话参数设置、业务参数、日志备份设置、告警邮箱设置、短信发送设置、威胁风控策略设置 ☆ 资产账号密码策略和用户密码策略 ☆ 命令防火墙策略创建、设置、成员资产账号管理、成员用户管理 ☆ 资产账号密码备份设置，支持密-钥分离或密码分段备份。 ☆ 设备状态监控 ☆ 第三方调用方添加、移除，查看 AppSecret 值，访问权限、和 IP 白名单 ☆ 应用运维工具配置、支持协议、启动参数 ☆ 管理员查看 License 及更换
运维 portal **（特权会话）**	☆ 授权资源列表和访问入口、会话启动 ☆ 批量访问组创建、批量访问资产会话、移除访问批量组 ☆ 临时访问授权申请、访问 ☆ 个人最近访问记录
用户自服务	☆ 修改密码 ☆ 修改个人资料 ☆ 相关工具下载

4 产品特点

4.1 IPV6 支持

产品网站支持 IPv6 地址访问 ，支持纳管 IPv6 资产和设备。

4.2 特权账号全生命周期管理

格尔 PAM 提供"统一的、集中的、安全的"特权账号密码管理解决方案。完全满足客户对"特权账号生命周期管理" 需求，支持扫描目标设备/对象包括但不限于主机设备、网络设备、数据库、WEB 应用、终端应用、云主机等 IT 资产管理、其他主流操作系统，包括 Linux 系列操作系统、windows 系列操作系统、银河麒

麟系列操作系统、UOS 系列操作系统；数据库类型 Mysql 系列、Oracle 系列、SQL Server 系列、Gauss（DWS DBA）系列、达梦系列、Gbase 8a 及以上版本、Kingbase 系列数据库类型所有版本，支持通过二次开发支持其他系列数据库。中间件支持 Weblogic、Tomcat、宝兰德、东方通等中间件控制台账号管理。

通过账号发现感知设备资产账号变况，资产账号密码或证书通过国密算法加密安全存储于系统凭证库中，账号密码托管后按照密码策略定期更换，满足国密、等保等安全法规对资产账号密码强度和生命周期的管理要求。

4.3 完善的账号风险预警能力

产品具备完善的账号风险检测阈值管理和检测引擎，通过远程方式采集到资产上账号清单、账号详情、账号凭据等信息，利用内置的账号风险识别引擎相对资产线下方式对资产账号做风险检测，识别并输出检测结果报告，检查会主动推送至资产组管理员邮箱或页面下载，提示资产管理员能及时处置资产账号风险。

图 2 账号风险识别结果

4.4 消除应用内嵌账号硬编码

各种应用程序都需要频繁访问数据库和其他应用程序，一般通过在配置文件和脚本中明文嵌入应用程序账号凭证。这些凭证一般都会长期保持不变，一旦凭证泄露就会导致敏感系统受到未经授权的访问。

产品提供内嵌账号管理功能，通过对应用配置订阅账号、部署实例信息，提供高安全应用取密身份鉴别机制，保障取密应用身份真实性。提供集成的多语言 SDK 帮助应用快速接入取密服务，针对 JAVA 的 JDBC 数据库应用提供插件，集成数据库链接即可动态从特权账号获取密码，支持双账号轮换。采用高可用设计

支持多节点部署取密服务，取密集成组件具备取密服务端监控检测和自动切换机制，遭遇故障节点可以切换到其他节点取密。

支持面向 Nacos/Apollo/Windows 凭据管理等应用主动推送资产账号密码。

图 3 内嵌账号应用管理

4.5 会话访问方式多样

支持 Putty/Xshell/secureCRT/Filezilla/Winscp/plsqldev 等本地工具运维，可审计又不改变运维用户习惯运维通道，在不改变运维用户习惯前提下确保特权会话可管控和审计。WEB 终端会话通道，使用 HTML5 的浏览器进行 Windows RDP、SSH 和 Telnet 会话，无需额外插件或代理软件，支持终端使用国产化浏览器：360、奇安信、瀛达信等。

可扩展支持远程工具会话通道，实现非通用协议网络会话管控和录像审计。

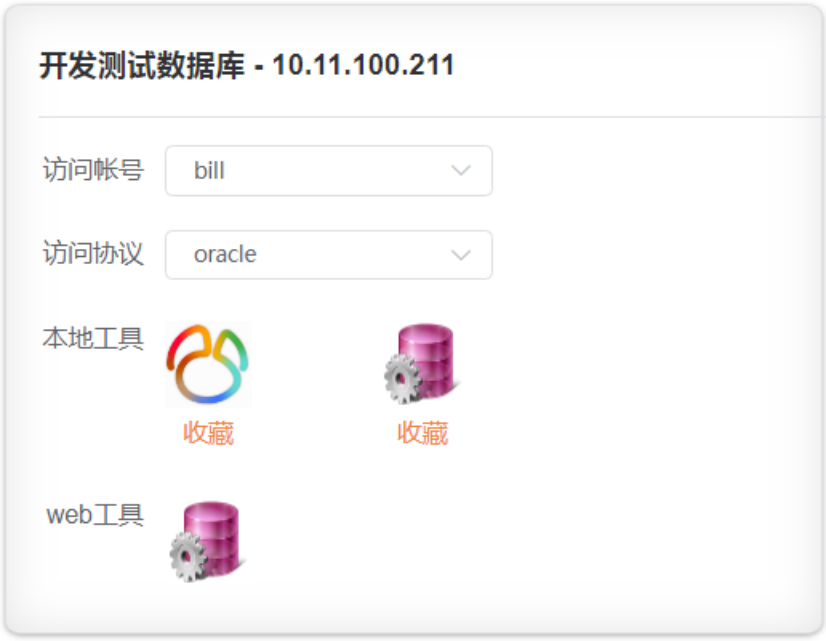

图 4 远程工具会话

4.6 符合零信任安全架构

特权账号管理系统可作为零信任 IT 体系中的运维安全网关使用，可无缝与格尔公司的 KIAM/SSL 网关/CA 集成。运维协议代理提供客户端到 PAM 端运维通道的功能，基于国密算法 TLS 安全通道，创建起安全的链接，防止交换数据时受到窃听及篡改，实践软件定义边界(SDP)会话级微隔离技术。

4.7 实时监控审计与追责

提供会话监控功能，管理员可对高危会话可采取中断和隔离措施。实现 ssh,telnet 及数据库 SQL 命令级审计,对历史会话可以进行溯源审计和责任认定，会话录像支持快进、定位回放等方式还原用户操作，以便对安全事件进行责任认定。

全面记录系统操作日志，并支持 syslog 外发。

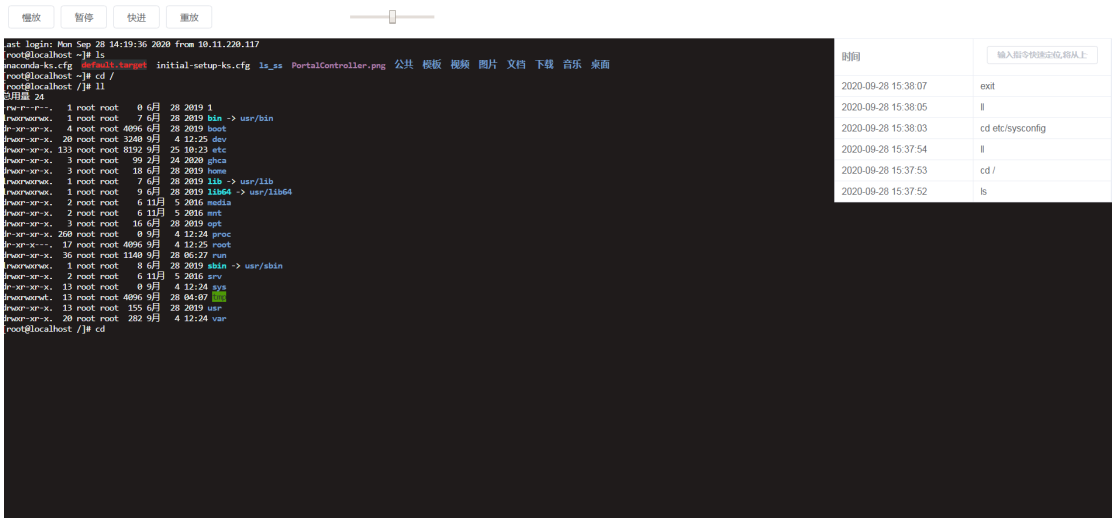

图 5 监控审计

5 典型部署

产品支持单机部署、双机热备、集群部署等三种模式，比较常见为双机热备模式。

5.1 双机热备部署方案

双机热备部署需要部署两台控制服务器，一台作为主机，一台作为从机，两

台机器同时与网络连接，两台设备之间使用“心跳线”连接，当主机发生故障时能够实现主机向从机的秒级切换。

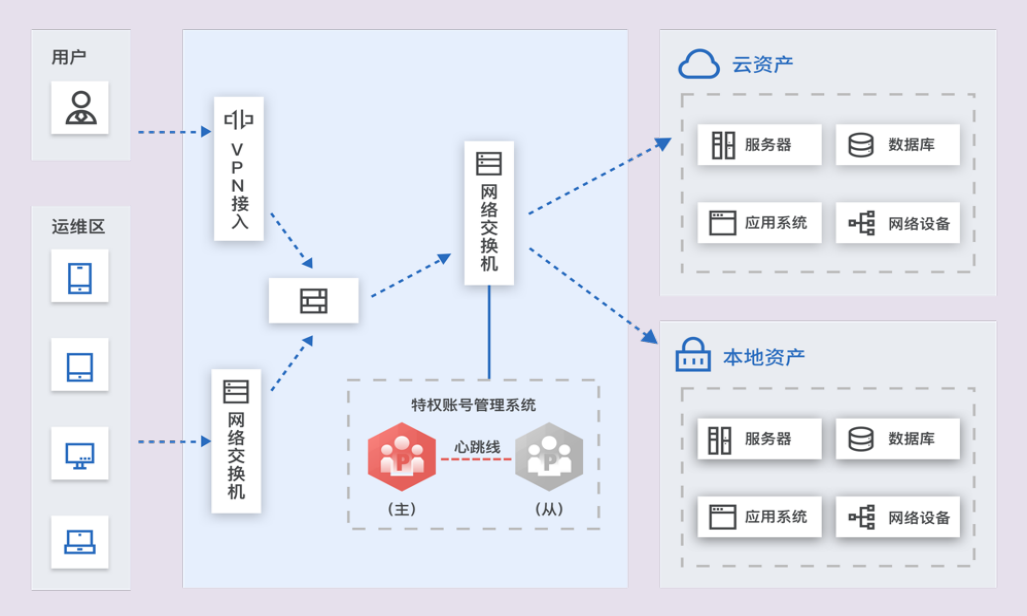

图 6　格尔 PAM 双机热备部署图

6 产品参数

外观规格	2U
网络接口	4 个 10/100/1000Mb 自适应接口 1 个千兆管理网口 支持扩展 2/4 个万兆光口
电源	双模块冗余电源，支持断电保护备份等机制
内存	≥64G，整机最大支持 128GB
硬盘	≥32T，支持存储空间扩展
授权资产数	≥5000 个
用户并发数	≥100 个
扫描线程	≥20 个
数据检索性能	≤15S(1 亿条数据规模)

7 产品带给客户收益

管的省心	管理员再不需手动改密，支持动态改密 分级分类管理大量系统/设备 不用担心运维人员掌握密码
用的舒心	不用担心过失泄密 不用担心误操作
心中有数	有多少设备/系统有数 设备/系统中有多少账号有数 这些特权账号谁管理有数 哪个账号做了哪些操作有数
心里有底	特权账号加密存储，有底 特权账号授权使用，有底 特权账号密取密用，有底

8 技术支持

格尔软件股份有限公司

电 话 ：021-62327010

传真： 021-62327015

地址：上海市江场西路 299 弄 5 号中铁时代广场 4 楼 6 楼

邮编： 200436