KYLINSOFT
麒麟软件

麒麟天御安全域管平台 V4.1.0
产品白皮书

麒麟软件有限公司

2024 年 8 月

商标声明

KYLINSOFT 麒麟软件和其他麒麟商标均为麒麟软件有限公司的商标。本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受麒麟软件有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，麒麟软件有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容有可能变更，麒麟软件有限公司保留在没有任何通知或提示的情况下对内容进行修改的权利。除非另有约定，本文档仅作为使用指导，并不确保手册内容完全没有错误。本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目录

1 关于麒麟

麒麟软件有限公司（简称“麒麟软件”）是中国电子信息产业集团有限公司（CEC）旗下科技企业，2019 年 12 月由天津麒麟信息技术有限公司和中标软件有限公司强强整合而成。

麒麟软件以安全可信操作系统技术为核心，面向通用和专用领域打造安全创新操作系统产品，现已形成桌面操作系统、服务器操作系统、万物智联操作系统、工业操作系统、智算操作系统产品等为代表的产品线，达到国内最高的安全等级，全面支持飞腾、鲲鹏、龙芯等国产主流 CPU，在系统安全、稳定可靠、好用易用和整体性能等方面具有领先优势，并为党政、行业信息化及国家重大工程建设提供安全可信的操作系统支撑。根据赛迪顾问统计，麒麟软件旗下操作系统产品连续 12 年位列中国 Linux 市场占有率第一名。

麒麟软件注重核心技术创新，2018 年荣获“国家科技进步一等奖”，2020 年发布的银河麒麟操作系统 V10 被国资委评为“2020 年度央企十大国之重器”，相关新闻入选中央广播电视总台“2020 年度国内十大科技新闻”，2021 年麒麟操作系统入选央视《信物百年》纪录片，2022 年入选工信部“2022 年国家技术创新示范企业”，2023 年发布的“开放麒麟 1.0”被国资委评为“2023 年度央企十大国之重器”，麒麟软件有限公司技术中心被多部委共同认定为“国家企业技术中心分中心”，入选国资委“创建世界一流专精特新示范企业”，2024 年麒麟操作系统被中国国家博物馆收藏，这是中国国家博物馆收藏的第一款国产操作系统。麒麟软件荣获“中国电力科学技术进步奖一等奖”、“水力发电科学技术奖一等奖”、“中国版权金奖·推广运用奖”等国家级、省部级和行业奖项 600 余个，并被授予“国家规划布局内重点软件企业”、“国家高技术产业化示范工程”、“科改示范行动企业”、“国有重点企业管理标杆创建行动标杆企业”等称号。通过 CMMI 5 级评估，现有博士后工作站、省部级企业技术中心、省部级基础软件工程中心等，先后申请专利 891 项，其中授权专利 408 项，登记软件著作权 647 项，主持和参与起草国家、行业、联盟技术标准 70 余项，被国家知识产权局成功认定为“国家知识产权优势企业”。

麒麟软件在北京、天津、上海、长沙、广州、深圳、太原、郑州、武汉、南京、南昌、济南、南宁、成都、沈阳、厦门等地设有分支机构，服务网点遍布全国 31 个省会城市和 2 个计划单列市。

麒麟软件高度重视生态体系建设，与众多软硬件厂商、集成商建立长期合作伙伴关系，建设完整的自主创新生态链，为国家网信领域安全创新提供有力支撑。截至 2024 年 4 月 30 日，麒麟软件已与 23100 多家厂商建立合作，硬件适配数超 71 万项，软件适配数超 378 万项，总量超过 449 万项，生态适配官网累计注册用户数超 6.6 万人。

麒麟软件积极贯彻人才是第一资源的理念，以麒麟软件教育发展中心为组织平台，联合政产学研各方力量，探索中国特色的网信人才培养模式，目前已形成了源自麒麟操作系统的“5 序”课程体系、教材体系、认证体系、师资体系、平台体系，并与工信部教育与考试中心联合推出“百城百万”操作系统培训专项行动，持续为我国培养各类操作系统专业人才。

在开源建设方面，成立桌面操作系统根社区 openKylin，旨在以“共创”为核心、以“开源聚力、共创未来”为社区理念，在开源、自愿、平等、协作的基础上，通过开源、开放的方式与企业构建合作伙伴生态体系，共同打造桌面操作系统顶级社区，推动 Linux 开源技术及其软硬件生态繁荣发展。截至 2024 年 4 月 30 日，openKylin 社区用户数量超过 110 万，社区会员突破 450 家，开发者数量超 6200 人，创建 103 个 SIG 组。从 2022 年开始，openKylin 连续两年获评中国信通院“先进级可信开源社区”。此外，麒麟软件正式成为开放原子开源基金会白金捐赠人；作为 openEuler 开源社区发起者，以 Maintainer 身份承担 80 个项目，除华为公司外贡献第一；在 OpenStack 社区贡献位列国内第一、全球第三。

2 问题与挑战

随着国家对信息化建设战略加码，国产操作系统在关键行业如党政、企业与金融领域获得了广泛部署。在此背景之下，作为网络安全与信息化管理核心的国产化域控产品的重要性日益凸显。然而，推进国产化替换过程中，业务信息的统一管理面临着前所未有的挑战，具体表现在以下八个方面：

- 组织管理：组织架构复杂多样，难以掌握全貌，维护工作量大。
- 人员管理：群体庞大、频繁变动、权限分散。
- 终端管理：终端形态多样、数量众多、分布广泛，难以统一纳管。
- 任务管理：缺少统一管理手段，执行步调不一致。
- 策略管理：策略执行不足，覆盖不全面，缺乏细致粒度。
- 安全管控：数据泄露、恶意软件攻击、非法访问和开发漏洞的利用等安全威胁日益严峻。
- 数据同步：在平滑替换 AD 过程中，同步复杂外部数据并确保数据一致性是一项挑战。
- 日志报表：关键信息监控不全面，难以及时发现威胁。

3 产品介绍

3.1 产品简介

麒麟天御安全域管平台（简称“麒麟天御”）是专为提升企业安全管理和操作效率而设计的企业级安全管理平台，旨在平滑替换 Windows AD。该平台致力于提高企业数据防护能力和管理效率，聚焦身份认证、终端安全、用户权限、软件管理、策略管控、高可用等场景，实现了对组织下的用户、主机、外设、软件、管控策略等全流程的统一管理。

3.2 产品架构

麒麟天御采用 B/S 与 C/S 混合架构，由服务端和客户端两大核心部分构成。这种架构设计不仅提升了系统的灵活性与扩展性，也确保了用户界面的友好性和操作的便捷性。服务端基于银河麒麟容器云平台设计，提供一体化 WEB 管理控制台，实现对组织、用户、终端等的全方位安全管理，支持多种单双园区高可用部署方案，确保业务系统运行的效率和连续性。客户端集成入域退域、数据同步、策略执行、策略取消、日志同步以及消息提醒等关键功能，并与麒麟通用桌面操作系统深度融合，有效应对系统统一认证、策略控制及维护升级等挑战，为业务信息系统管理提供坚实的保障。

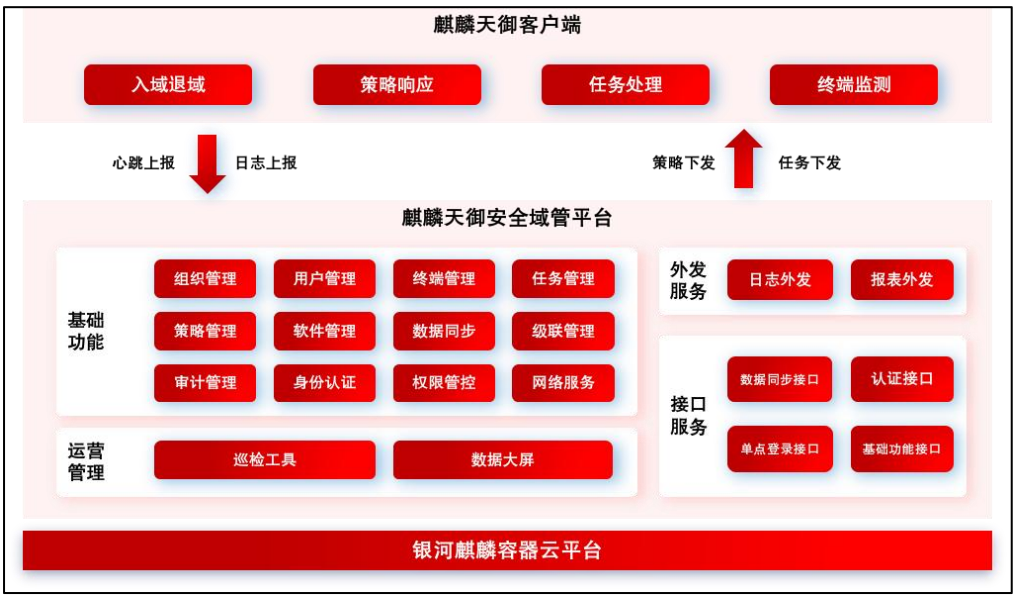

图 3-1 麒麟天御产品架构图

4 核心功能及特点

4.1 组织管理

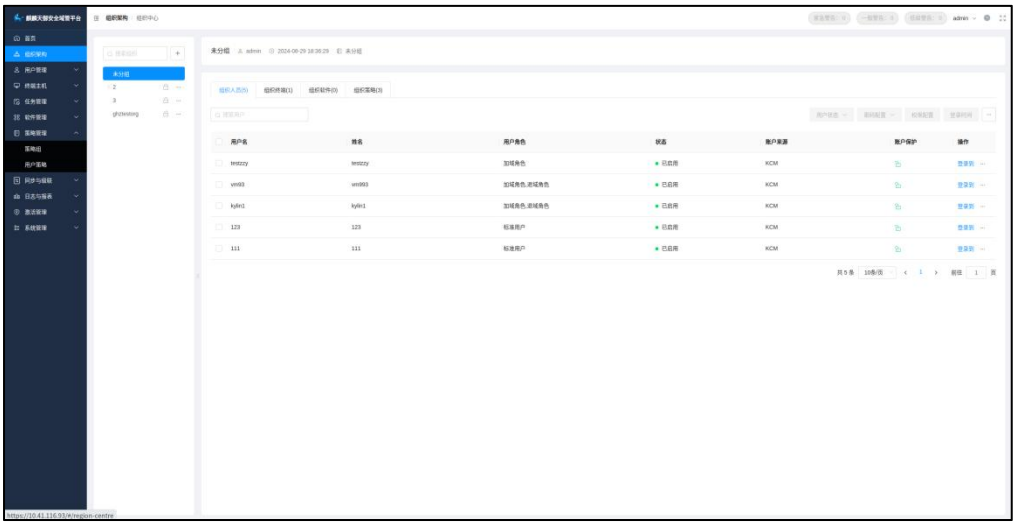

图 4-1 组织架构界面

组织创建

- 支持手动录入和数据自动同步二种方式。

组织展示

- 采用树状结构展示，管理员能够快速把握组织架构全貌。

管理维度

- 支持对组织内的人员、终端、软件和策略进行统一维护。

4.2 人员管理

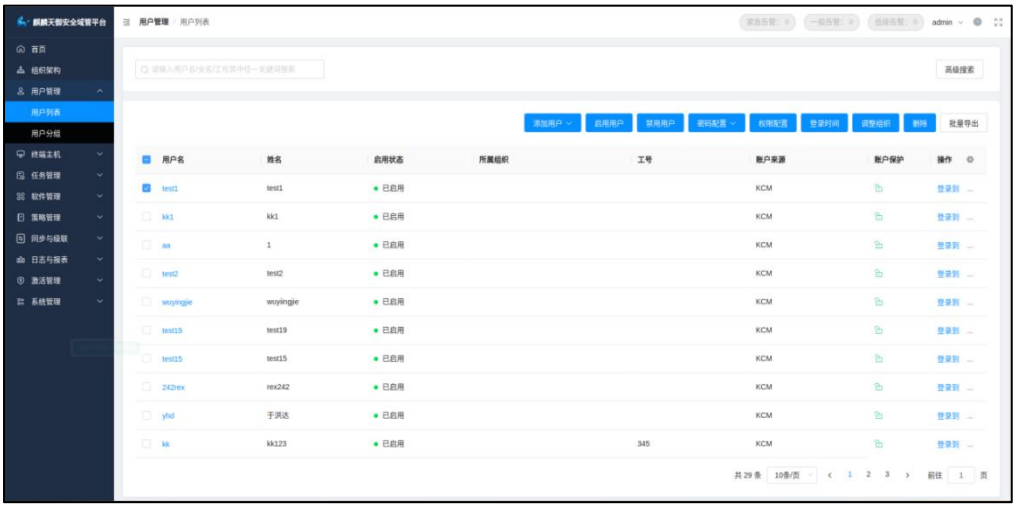

图 4-2 用户管理界面

平台用户管理

- 超级管理员：负责创建普通管理员，并分配相应的操作范围和权限。
- 普通管理员：负责管理指定的组织层级和功能模块。

终端域用户管理

- 用户创建：支持手动录入和数据自动同步二种方式，支持用户按照规则自动分组。
- 用户配置：支持配置用户的启用、禁用、密码重置、可登录终端和允许登录时间。
- 权限配置：支持配置用户的加域、退域、sudo 权限、软件安装、设备管理、网络管理和自定义命令执行等操作权限。

终端本地用户管理

- 用户配置：支持配置用户的启用、禁用和密码重置。

4.3 终端管理

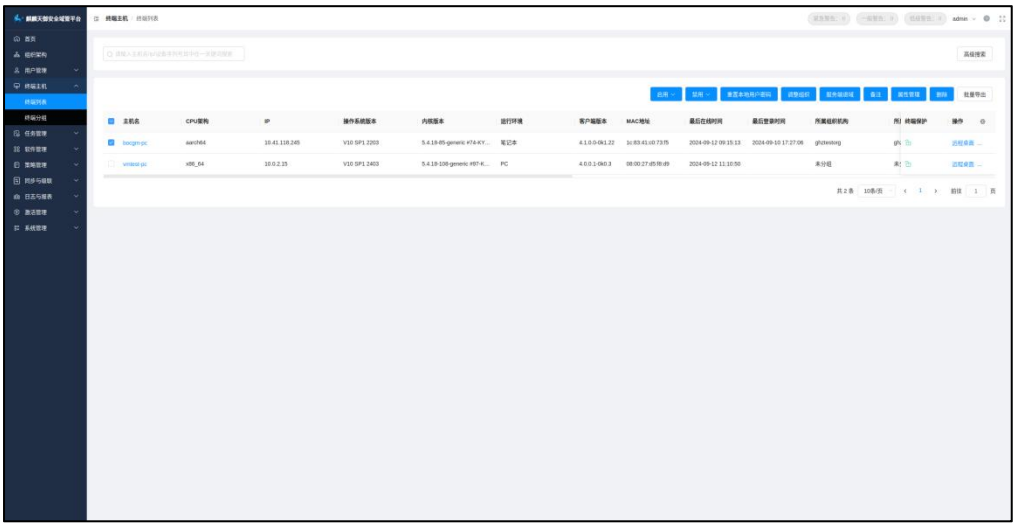

图 4-3 终端管理界面

终端统计维护

- 终端加域：支持重装系统的终端可重复加域，操作更简便。
- 统计信息：硬件信息、资源监控、进程信息、策略详情、登录日志和已安装软件。

- 远程维护：支持远程桌面连接、终端关机和重启。

终端应用场景

- 纳管兼容：支持纳管麒麟桌面及服务器操作系统。
- 终端属性：个人机专为指定用户登录，公共机允许组织内用户登录。

4.4 任务管理

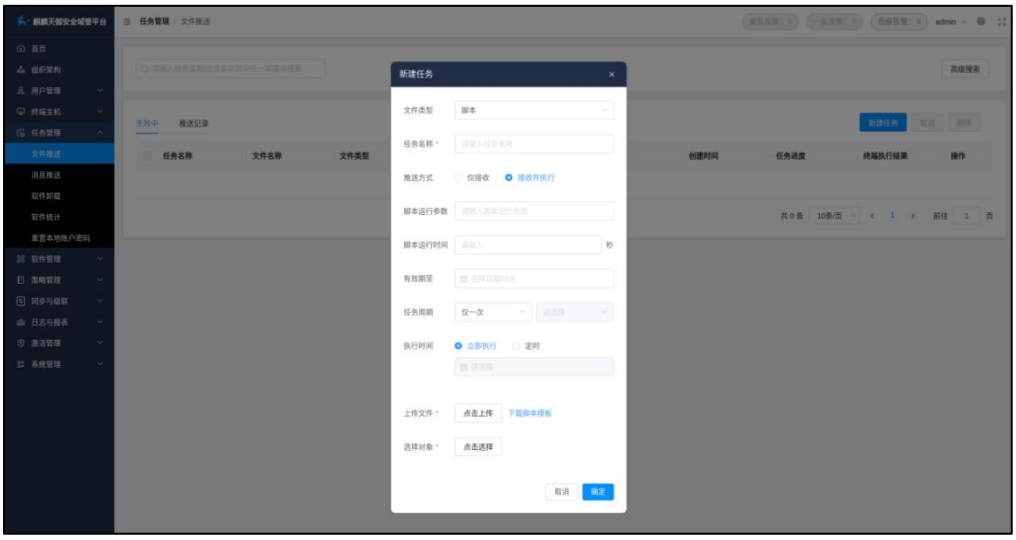

图 4-4 任务管理界面

任务创建

- 任务类型：文件推送、脚本执行、浏览器证书推送、消息推送、软件统计、软件卸载、重置本地账户密码。
- 任务时间：支持立即、定时、周期执行选择。
- 任务期限：支持设置任务有效期，到期后自动取消。
- 任务范围：支持面向特定的终端或人员推送。
- 任务复制：支持任务复制，便于快速创建新任务。

任务追溯

- 执行详情：支持查看任务的执行进度和历史执行结果。
- 失败重试：支持对失败任务进行重试，简化操作流程。

4.5 软件管理

图 4-5 软件管理界面

软件管理对接麒麟私有化软件商店统一进行软件全生命周期管理。

软件统计

- 支持对接麒麟私有化软件商店，统计软件使用情况。

软件分配

- 支持面向终端组织、分组分配可下载软件。

软件卸载

- 支持一键批量卸载软件。

软件行为审计

- 支持记录人员对软件的安装、升级、卸载等行为。

4.6 策略管理

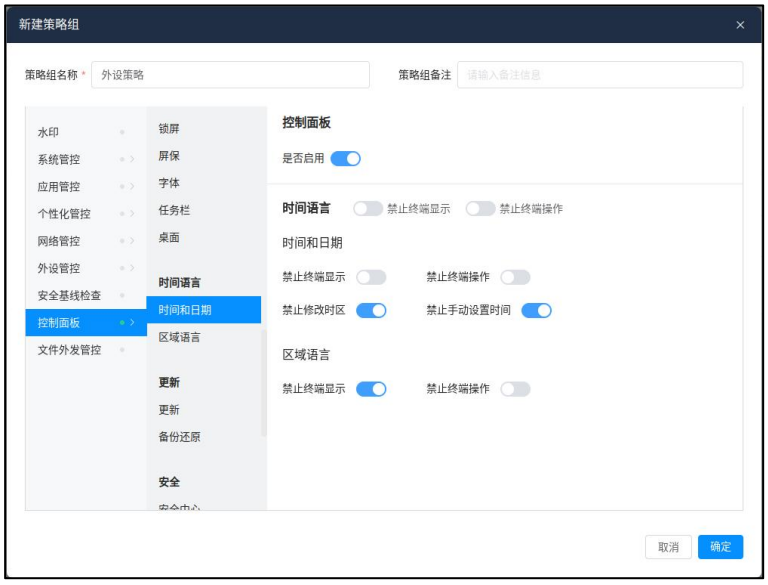

图 4-6 策略创建界面

策略创建

- 策略模板：内置 9 大类 150+项策略模板，覆盖系统、应用、网络、个性化、安全等管控内容。
- 策略场景：支持设置在线/离线场景策略。
- 策略范围：支持面向终端组织、终端和终端分组下发策略，其中终端组织可设置例外。
- 用户策略：支持面向全局用户下发密码策略。

策略维护

- 策略调整：支持策略优先级手动调整，策略冲突时按优先级生效。
- 策略操作：支持策略启停、临时取消、删除、备份、还原和导出功能。

4.7 安全管控

应用管控

- 软件运行管控、联网管控、防卸载管控。

数据安全

- 支持文件管理器管控、支持文件外发审批、支持水印设置。

外设管控

- 支持 usb、打印机、光驱、手机管控以及外设黑白名单管控。

网络管控

- 支持防火墙管控、内外网隔离管控、无线网卡管控、网络代理。
- 支持热点管控、热点黑白名单、Wi-Fi 管控。
- 支持流量管控。

SDK 安全

- 支持 SDK 门禁与审计。

4.8 数据同步

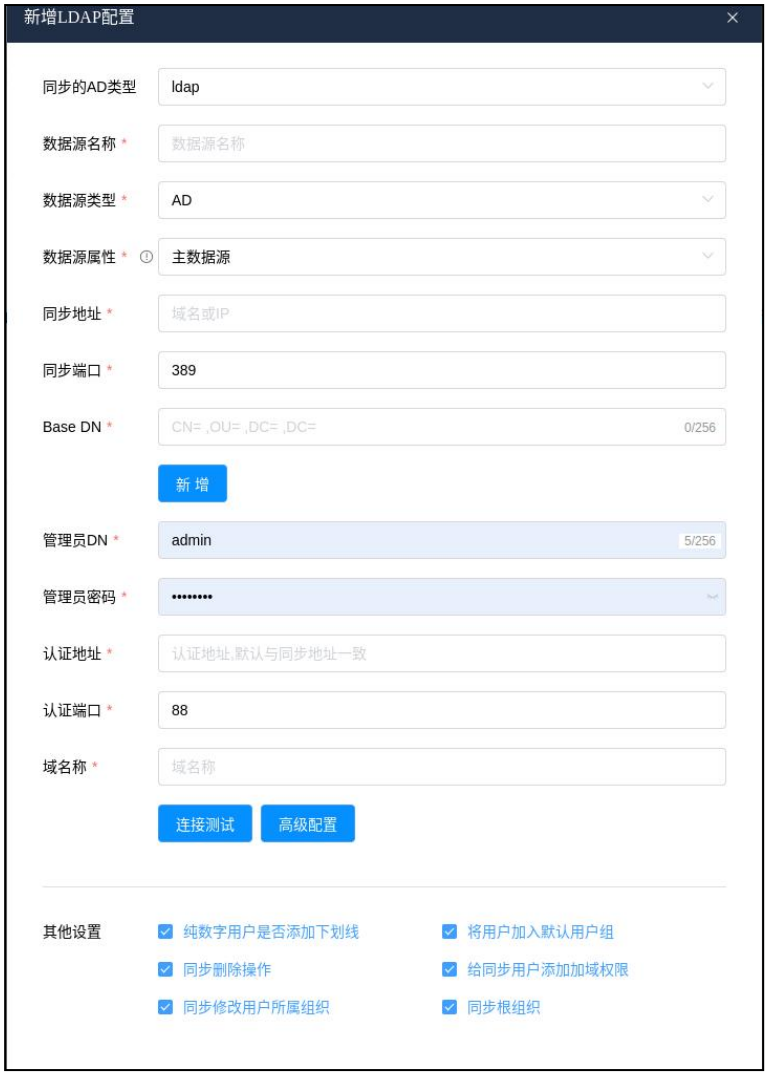

图 4-7 数据同步界面

认证对接

- 支持对统一身份认证系统和 Windows AD 数据平台进行数据同步和身份认证转发。

同步范围

- 支持组织、用户和用户组的多数据源自动同步。

冲突处理

- 支持设置主从数据源，避免数据冲突。

4.9 日志报表

平台日志

- 支持平台管理员操作日志、数据同步及日志外发审计。

终端日志

- 日志收集：支持终端用户登录、终端行为、外设使用、软件更新、关键进程监控、告警事件审计，以及自定义采集的终端日志。
- 日志报表：支持用户、终端在线时长统计报表。
- 日志外发：支持日志外发、报表周期外发，可推送至指定邮箱。

4.10 系统管理

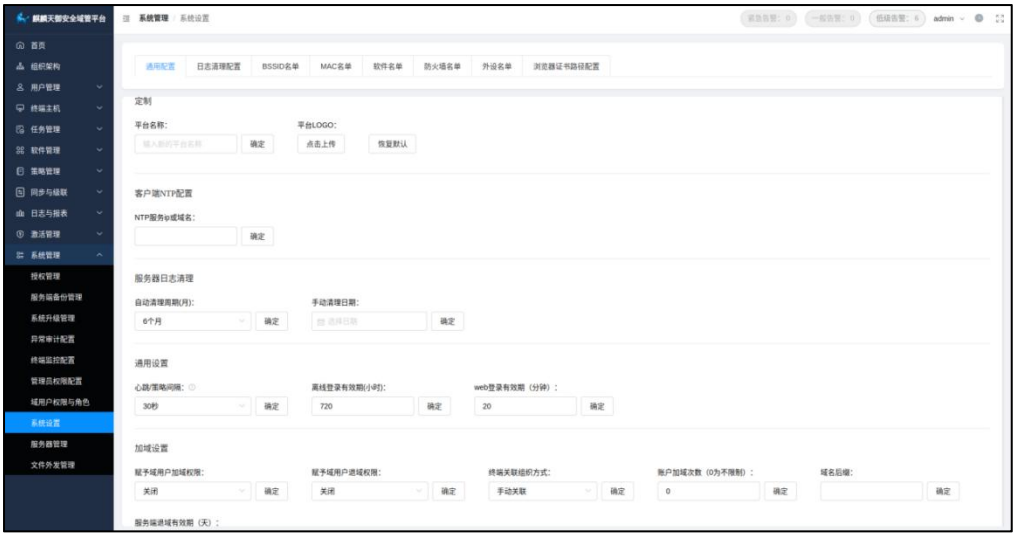

图 4-8 系统管理界面

平台备份升级

- 平台备份：支持手动与自动备份，可灵活调整备份文件数。
- 平台升级：支持一键升级与回滚，记录全流程升级日志。

集中配置入口

- 提供终端告警规则配置入口。
- 提供终端进程监控、进程保护配置入口。
- 提供域用户与平台管理员的权限配置入口。
- 提供 BSSID、MAC、软件、防火墙、外设名单配置入口。
- 提供浏览器证书路径配置入口。
- 提供文件外发管理配置入口。
- 提供平台基础设置入口。
- 提供 NTP\DNS\DHCP 服务配置入口。

5 部署模式

5.1 部署方式

- 支持在互联网环境部署
- 支持在隔离网环境部署
- 支持单节点部署
- 支持高可用部署
- 支持单节点级联部署
- 支持高可用级联部署

5.2 级联管理

在当今企业的信息化管理中，确保总部与分支机构之间的信息安全与高效协同工作是至关重要的。麒麟天御创新性提出级联管理概念，为企业提供了一个全面、灵活的解决方案。该方案采用根域-子域的架构模式，在用户网络中部署多套系统，通过级联管理实现平台间的统一管理。

- 子域向根域同步上报用户、终端、运营数据等关键信息。
- 级联管理能够实现根域对子域的安全策略下发、集中管理。
- 通过创建信任关系，形成级联受信网，实现跨域认证、数据同步等关键业务支撑。

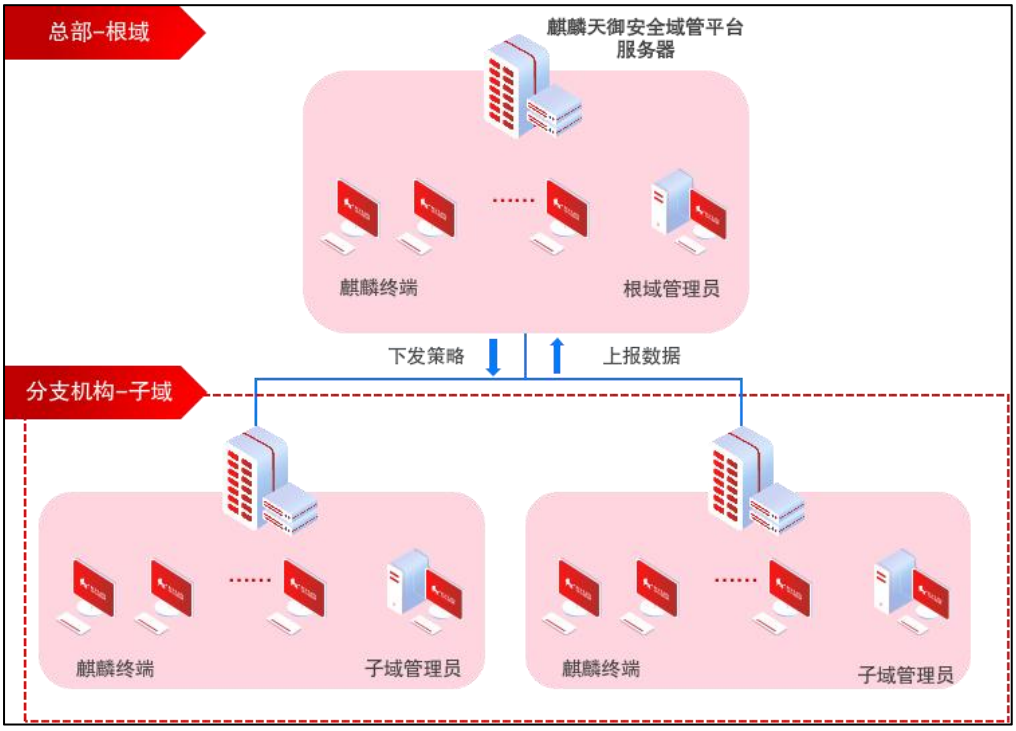

图 5-1 级联部署架构图

6 产品指标与参数

6.1 版本支持

麒麟天御服务端支持在麒麟服务器操作系统上部署，客户端需要在麒麟桌面操作系统上部署，以下为支持的麒麟操作系统版本：

表 6-1 麒麟天御支持纳管麒麟操作系统版本目录

部署平台	版本	架构
服务器版本	Kylin-Server-10-SP1-Release-Build20-20210518	arm64、x86_64
	Kylin-Server-10-SP2-Release-Build09-20210524	arm64、x86_64
	Kylin-Server-V10-SP3-General-Release-2303	ARM64、x86_64
桌面版本	Kylin-Desktop-V10-SP1-RC6-Build08-210610-2	x86_64
	Kylin-Desktop-V10-SP1-RC6-Build09-210610-2	arm64
	Kylin-Desktop-V10-SP1-Release-2107	arm64、x86_64
	Kylin-Desktop-V10-SP1-beta-Build1-20211020-kirin990	arm64
	Kylin-Desktop-V10-SP1-General-Release-2203	x86_64

	Kylin-Desktop-V10-SP1-HWE-Release-2203	X86_64
	Kylin-Desktop-V10-SP1-kirin990-Release-2203	ARM64
	Kylin-Desktop-V10-SP1-kirin9006c-Release-2203	ARM64
	Kylin-Desktop-V10-SP1-HWE-RC3-Build06-20220622	x86_64
	Kylin-Desktop-V10-SP1-General-RC8-Build01-2203	arm64、x86_64
	Kylin-Desktop-V10-SP1-HWE-Release-2303	x86_64
	Kylin-Desktop-V10-SP1-2303-update2-Release-20231023	ARM64、x86_64
	Kylin-Desktop-V10-SP1-2303-update1-Wayland-Release-Retail-HW-kirin990-20240326	arm64
	Kylin-Desktop-V10-SP1-2303-update1-Wayland-Release-Retail-HW-kirin9006c-20240326	arm64
	Kylin-Desktop-V10-SP1-2403-Release-20240430	ARM64、x86_64

6.2 推荐配置

表 6-2 麒麟天御部署推荐配置目录

管理规模	部署模式	配置建议	节点数量 （N 表示计算节点）	备注
1W	单节点	CPU：32 Core 内存：32G 硬盘:1TB 网络:千兆	1	物理机或虚拟机或微服务
3W	高可用	CPU：32 Core 内存：64G 硬盘:1TB 网络:千兆	3	物理机或虚拟机或微服务
5W	高可用	CPU：32 Core 内存：64G 硬盘:1TB 网络:千兆	3+N	物理机或虚拟机或微服务
10W	高可用	CPU：32 Core 内存：64G 硬盘:1TB 网络:千兆	3+N+3	物理机或虚拟机或微服务
20W	双园区高可用	CPU：32 Core	(3+N+3)+(3+N+3)	物理机或虚拟机

		内存：64G 硬盘:1TB 网络:千兆		或微服务

7 客户案例

7.1 某政府单位政务办公自主创新项目

项目概况：

麒麟天域安全管控平台应对某政府单位总部-多分支机构的管理模式，人员、终端数量众多，且政务办公地理分散的特点，实施级联部署，构建根域-子域架构，确保系统高效稳定、数据安全，破解分散单位统一管理、系统升级及跨域登录难题。

解决方案：

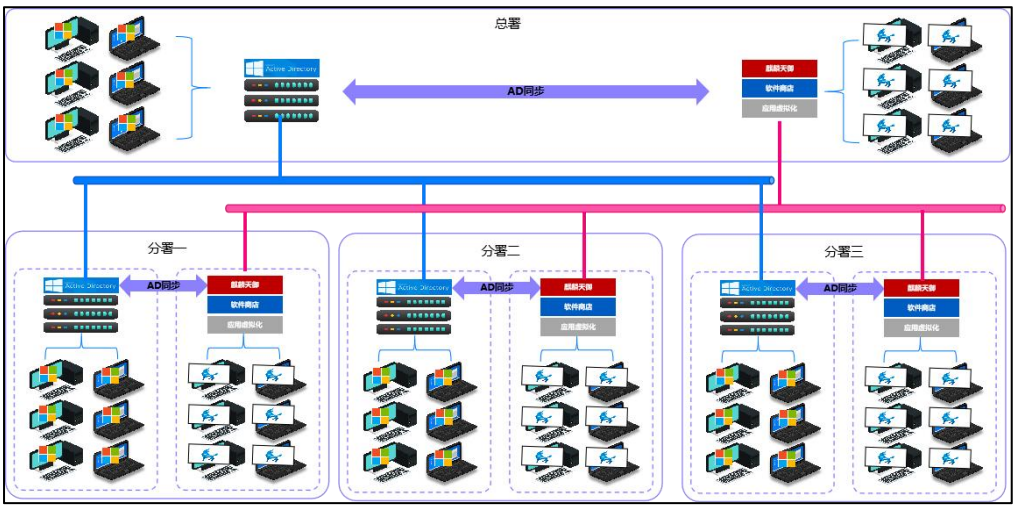

图 7-1 麒麟与某政府单位在政务办公场景下的解决方案

项目特色：

- **级联部署策略**

根域平台可对子域下发管理策略，子域平台向根域上报数据，双向保证信息同步和策略一致。

- **分级管理与权限控制**

平台支持分级分权的管理模式，根域管理员可对子域平台进行统一管理，确保不同权限级别的操作在适当的监管下进行。

- **跨域登录功能**

根域-子域网络环境互建信任机制，实现不同平台间账户的跨域登录，无需重复登录。

- **灵活的部署模式**

支持单节点/高可用以及单节点级联/高可用级联多种部署模式，便于未来灵活扩展和升级。

7.2 某国有银行终端系统联合创新项目

项目概况：

麒麟公司与某国有银行联合创新，聚焦金融办公、开发运维、柜面服务等场景，无缝对接行内运维管理体系，解决金融行业的安全、运维管理痛点，为全行规模化应用推广奠定了基础。

解决方案：

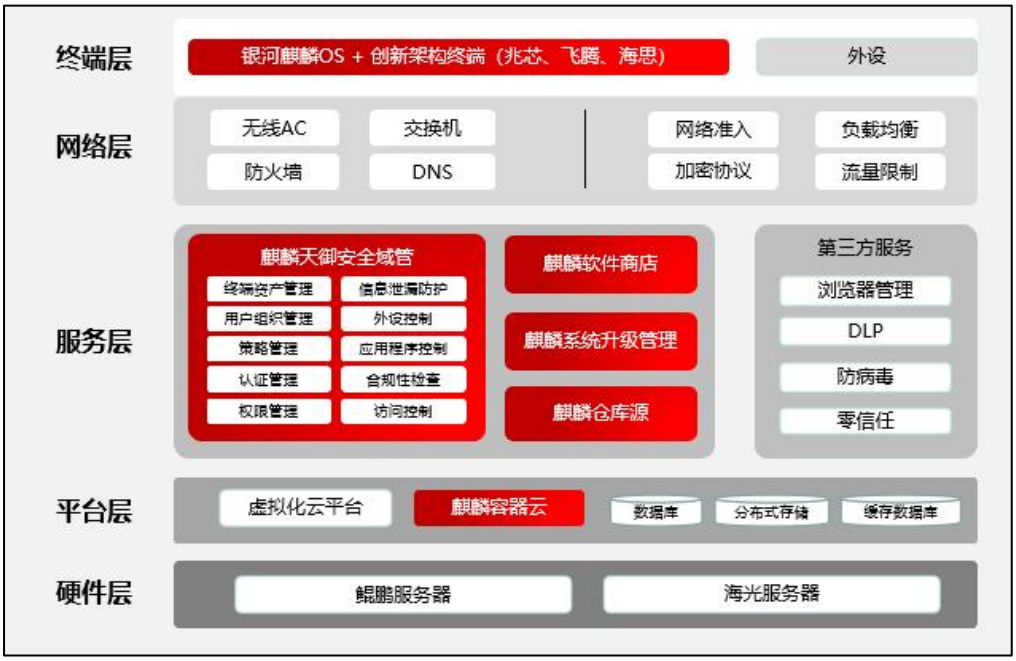

图 7-2 麒麟与某国有银行联合创新解决方案

项目特色：

- **统一网络身份认证**

打通行内统一认证平台，构建统一鉴权的身份认证体系，实现集中化网络身份认证管理。

- **分级运维管理策略**

分级分项精细化管理策略，结合一体化策略管控，完成快速批量部署。

- **终端运营审计管理**

支持规模化终端接入与软件行为管理，达到可信化终端准入、分钟级软件发布能力。

- **构建双园双活方案**

部署双园区双活高性能方案并支持动态扩容，可支持数十万级终端并发，请求响应成功率≥99.9%。

7.3 某头部保险公司信创终端系统创新项目

项目概况：

麒麟天御协助某头部保险公司全面实现云桌面生态转型，未来将管理超过千台信创物理机和 10 万套云桌面系统，确保从 Windows 到国产操作系统的平稳迁移与数据安全，加速其数字化转型目标的实现。

解决方案：

图 7-3 麒麟与某头部保险公司在云桌面场景下的创新解决方案

项目特色：

- **高效纳管云桌面**

通过个人专属与池化云桌面场景下的自动加域解决方案，实现云桌面的无感知纳管。

- **多元化认证体系**

实施一体化登录解决方案，融合密码、扫码等认证方式，提供安全又便捷的访问体验。

- **定制化数据漫游**

结合分布式存储，提供量身定制的数据漫游解决方案，确保个人数据一致性和访问连续性。

- **高性能稳定架构**

对接阿里的 ACK 云平台、Redis 中间件和 OceanBase 数据库，联合打造高效稳健的解决方案。

8 技术服务体系

麒麟软件有限公司拥有完善的技术服务体系和一流的服务团队。服务遵循 ISO27001、ISO20000、ITSS 等体系标准要求，为客户提供专业的厂商级服务。对于由于客观条件确实无法解决的问题，将给出明确计划及解决方案，主要提供远程服务以及现场服务。麒麟软件可提供多种服务模式，包括基础服务、高级服务、定制服务等，服务产品目录如下：

服务类型	服务产品名称	服务产品描述
基础服务	标准支持服务 5x8	标准服务，5X8 远程支持服务。工作时间：国家工作日，周一至周五 8:30-17:30（法定节假日除外）。
	优先支持服务 7X24	优先服务，7X24 远程支持服务，服务响应时间优于标准支持服务，详见服务说明书。工作时间：7X24X365 ；此项服务 7X24 全天候提供；包含法定节假日。
高级服务	问题解决服务	问题解决服务，7X24 远程支持服务（不含现场服务）。提供专属工程师快速响应与问题处理，熟悉客户环境，快速做出判断，优先的问题跟踪升级渠道；由客户服务经理定期服务沟通，支持相关需求并提供内部协调。工作时间：7X24X365，此项服务 24X7 全天候提供；包含法定节假日。

	主动服务	主动服务，提供高级工程师现场服务，专属客户服务经理定期与客户进行需求沟通和服务回顾，以及服务计划制定和资源调配，并分配高级工程师现场服务，可执行排故、健康检查、安全保障、知识传递、调优等服务。
	驻场服务	驻场服务：专属高级工程师，结合用户需求进行人员选派，在用户管理范畴内，提供全天现场驻场，例行维护和支持服务。工作时间：每天 8 小时（同用户工作时间，特殊时间段支持可视情况调整），参考：周一至周五 9：00-18:00 节假日除外
定制服务	定制服务	定制服务：针对客户的项目需求，由专属客户服务经理执行需求沟通，进行需求分析和工作量评估，编制工作说明书，签署服务并按照约定进行资源调配，管理和审核服务执行结果。此服务根据客户的情况按需分配高级工程师，服务形式不限可包括远程和现场服务。项目内容可包括例如：部署实施、数据迁移、产品升级、兼容性测试等。

为了满足不同用户、不同场景的需求，公司建立了完整的技术服务网络。麒麟软件在天津、北京、上海、长沙、广州、太原、郑州、成都、西安、沈阳等地设有分支机构，服务网点遍布全国 31 个省会城市和两个计划单列市。

服务联系方式：

服务热线：400-089-1870

公司网站：www.kylinos.cn

技术服务电子邮件：support@kylinos.cn