中数国科堡垒机系统
技术白皮书

（中数国科集团）

【中数国科】

■ 文档编号	■ 密　　级
■ 版本编号	■ 日　　期
■ 撰 写 人	■ 批 准 人

■ 版权声明

变更记录

序号	版本	变更记录	修改人/日期	检查人/日期	审批人/日期
1	V22.2		lzf		

目录

一、产品概述

当前IT技术正在成为诸多企业的神经中枢，越来越多的企业希望借助IT技术这一关键的战略资源提升公司的竞争优势，进而实现公司的战略目标。然而，随着网络建设和系统部署越来越深入，大多数企业面临着如何确保业务系统的稳定运行的难题。复杂的网络结构、人员结构和管理结构使得IT运维管理和企业生产运作间的矛盾日益凸显。日益发展变化的生产业务结构对基础IT运维操作的管理、审计等诸多方面提出了严峻的挑战。

庞大的运维结构，复杂的运维管理流程都对整体企业业务运行管理增加了很大的难度从而使得运维过程中的风险不易控制。同时国家也出台了相关的法律法规，如《安全等级保护》、《ISO27001》、《金融行业风险指引》等，要求在访问控制、操作审计等诸多方面做的更加全面有效的管理。故此需要通过有效的技术手段来降低运维风险、规范运维操作符和相关法律法规要求。

中数国科堡垒机系统，以下简称“运维审计系统”是集单点登录、账号管理、身份认证、资源授权、访问控制和操作审计于一体的新一代运维审计产品，它能够对操作系统、网络设备、安全设备、数据库等操作过程进行有效的运维操作审计，使运维审计由事件审计提升为操作内容审计，通过系统平台的事前预防、事中控制和事后溯源来全面解决企业的运维安全问题，提供了稳定、安全、便捷、快速接入式的解决方案，从而在现有的业务环境下完善了运维管理模式，消除固有弊端，使运维操作管理进入一个真正安全与便利相结合的阶段，帮助客户使运维操作管理变得更加简单、安全有效，进而提高企业的IT运维管理水平。

二、产品功能

2.1. 功能介绍

2.1.1. 单点登录

信息系统中有大量网络设备、主机设备和应用系统，分别属于不同的部门和不同的业务系统。运维人员通过不同的入口去维护信息系统，导致无法统一管理、设置统一安全策略，维护过程中，存在许多不可控的因素，从而容易引起各种安全隐患。还包括外部第三方运维人员进行信息系统运维时，管理员无法从技术上确保，第三方人员的所有操作行为是否合规。

单点登录功能是所有运维人员统一运维的入口，运维人员通过管理员认证和授权后，运维审计系统根据策略实现后台的自动登录。此功能提供了运维人员到后台账号的一种可控对应，同时实现了对后台账号的口令统一保护。

系统采取加密方式保存用户资源的账号和口令，使用户无需记忆多种登录用户 ID 和口令,同时由于系统自身是采用强认证的系统，从而提高了用户认证环节的安全性。

当运维人员需同时运维多个资源，系统支持多资产多协议的批量运维，运维人员可通过策略创建的方式勾选对应资产与协议生成批量运维策略，实现一键批量快捷登录。

2.1.2. 用户管理

先简单描述一下系统中存在的两种账号，分别为系统账号和资产账号，系统账号为登录系统时所使用的账号，每个账号都具有自己的角色岗位，每个角色拥有自己的权限。资产账号为单点登录资产时所使用的账号，该账号主要负责单点登录和资产改密功能。

为了明确用户单位的岗位职责，系统支持多种用户角色：超级管理员、安全保密员、安全审计员、系统管理员、运维管理员、运维操作员，每种角色的权限都不同，为用户设

立不同的角色提供了选择，防止用户越权，查看并操作不允许的信息和功能，保证系统自身的安全性，满足合规对三权分立的要求，并提供灵活的角色自定义能力。

用户支持设置双因素模式登录，外设认证包括（Google 动态令牌、飞天 Ukey、短信、动态令牌等），认证服务器包括（radius、AD 域、LDAP、证书等）。通过配置双因素认证，进一步加强了系统自身的安全性。

当第三方人员来现场进行运维操作时，为了限制第三方人员使用系统时长，管理员可建立临时用户，设置用户到期时间，设定时间到达，系统将自动收回用户所有权限并锁定用户。

用户以实名制的方式建立，需填写信息包括（姓名、邮箱、手机、身份证号码），方便审计信息直接查询用户登录登出信息和操作信息，假如未来系统通过人为操作出现故障，对溯源和追责起到了一定的作用。

2.1.3. 授权管理

由于大量使用特权账号维护，并且没有一种技术手段来监控、控制特权账户的操作，所以出现越权和违规操作的现象较多。从而导致安全事件发生。

通过运维审计系统的集中授权，帮助客户梳理用户与主机之间的关系，限制运维人员使用指定账号去运维可以操作访问的资源，并且提供部门对部门灵活授权模式。

运维审计系统为用户提供了一套临时授权功能，当运维人员在运维过程中，需要操作没有权限的服务器时，运维人员可向管理员申请临时授权，通过选择资产、协议、账号、时间范围来申请临时授权。根据审批策略，审批模式支持并行审批、串行审批等多种模式，审批流程可设置三级负责人审批，每级可为多个负责人。

2.1.4. 运维策略

在以往运维过程中，防止运维人员在操作过程中执行高危指令，例如删除，对用户的资源数据造成了一定的影响，运维过程通常需要管理人员的陪同下进行运维。运维审计系

统支持运维策略功能，提供多种基于用户和资产的运维策略，可以限制登录 IP 地址和时间策略下发可以限制运维人员访问会话，操作指令是否可以执行，是否允许复制粘贴文本内容，以及是否允许运维人员上传下载文件，根据这些操作对象，系统可对其采取阻断、发送告警信息或向管理员审批等处理动作。

此功能方便用户通过策略限制运维人员的一系列操作，提高了资源的安全性，运维人员无需管理员的陪同即可工作，管理员也可以进行其它工作，大大减少了人力的占用。

2.1.5. 操作审计

在运维人员操作时，当管理员想看运维人员在做什么的时候，管理员可通过实时会话在线查看运维人员的操作界面，若发现运维人员有违规操作可立即执行阻断操作。在这个过程中审计人员可同时监控多名操作人员操作，整体的监查过程对于操作人员均为无感监控。

当运维结束，系统将整个运维过程的信息保存，可以在历史会话中查看运维审计信息精确记录用户名称、IP、资产名称、资产 IP、资产账号、协议、开始时间、会话时长等审计信息。审计结果可录像回放，回放视频可调节播放速度，并且回放过程中支持进度条前后拖拽，针对本次运维所输入的指令或键盘信息可快速定位，通过选择指令可回放执行指令过程视频。系统中所记录的每条审计均可下载并且支持离线播放。审计查询也提供了多路同时查看的设计，方便管理员同时多窗口查看审计记录，方便用户对比操作，满足多人多设备协同运维操作时同时查看的需要。历史会话为用户提供查询功能，可按照系统中全量的审计信息进行模糊查询。

运维审计系统除了整体操作的录像回放外还提供了针对指令字符的单独审计功能，在运维过程操作的所有指令，系统会逐个详细记录下来，并具备类似于审计回放式在线视频播放。指令审计同样也具备查询功能，可按照全量审计信息进行模糊查询。

运维审计系统为了保证自身系统操作的合规性，针对系统本身的操作也具备一定的审计能力，可将各权限人员在系统所做的业务配置、系统配置、登录认证等操作行为进行详

细的记录。

2.1.6. 告警信息

运维审计系统针对重点运维操作或系统运行状态异常等情况提供在线或离线的告警，告警方式具备多种多样的模式，用户可选择页面告警或者邮箱、短信等方式的外发告警，用户需要查询告警信息时，可通过告警信息查询页面对告警内容具体信息进行查阅，告警信息页面会展示一定周期内未处理的告警行为，用户可对告警事件进行确认处理操作。可用户想要查询以外处理过的告警信息时，系统提供历史告警查询功能，可通过历史告警查询处理后的告警事件，历史告警与告警信息均具备事件搜索功能，可按照各类事件的信息模糊搜索。

2.1.7. 统计报表

运维审计系统本身具备强大的运维数据统计与整理能力，系统为用户提供统计报表功能可帮助用户统计现有运维趋势，在与上层管理汇报业务情况时，可作为设备维护量的有利依据，报表功能可对运维人员的操作行为与操作内容进行统计，系统本身内置大量报表模板并且可按照用户需要自定义报表，用户可根据自身需要创建系统全量数据的报表模板。如具备定期数据整理需求时，系统为用户提供了定时报表功能，可按照各类时间周期生成统计报表，并支持外发到对应的邮箱地址。报表内具备柱状图、饼状图、点线图等形式的统计数据图表，直观立体的为用户展示了现有运维环境与运维整体状态。

2.1.8. 会话协同

运维审计系统具备完善的会话协同功能，可实现多个具备相应权限的运维人员对同一远程会话的实时协作与管理。会话协同功能可帮助用户在复杂运维任务、应急故障处理及培训指导等场景下提高处理效率与协作能力，保障业务连续性与运维安全。系统支持多种协同模式，包括实时旁观、会话接管及多方互动等，如实时旁观：协同用户可同步查看当

前操作者的全部操作过程，包括命令输入、界面变化等，便于监督、审计与指导；会话接管：在操作者出现异常、断线或存在误操作风险时，具备权限的用户可立即接管当前会话，避免业务中断或风险扩大；多方互动：支持多名运维人员同时在同一会话中进行输入与操作，实现多人协作完成复杂任务。系统在会话协同过程中，会对所有操作进行完整记录，包括参与人员身份、操作时间、输入命令、界面录像等，确保可追溯、可审计。会话协同功能不仅提高了运维效率，还在培训、监督与应急接管等场景中发挥了重要作用

2.2. 关键技术

2.2.1. 网盘传输

运维审计系统具有网盘传输功能，在运维人员进行运维时，当需要对资源进行上传文件时，系统采用安全转存机制进行实现，用户需要将文件上传至运维审计系统特定安全存储中，系统对文件进行安全扫描，后以摆渡的形式将文件上传至资产中，这一过程大大降低了上传文件带有木马或病毒，感染全网资产的情况发生，进一步保障用户网络和资源的安全。

2.2.2. H5 运维

运维审计系统单点登录采用 HTML5 运维代理技术，无需安装 Agent 和插件，即可实现跨平台、多协议（RDP、TELNET、SSH、SFTP、FTP 等）的运维代理和安全审计功能。在线 H5 运维代理技术完美解决了异构运维终端环境下部分系统不支持安装或应用 AGENT 程序的情况，提高了本身系统的兼容性，也为用户网内对系统的应用提供了较好支撑。

2.2.3. 多因素认证

运维审计系统为保证系统自身安全，具备多因素认证方式，兼容多种外设认证方式和认证服务器方式，外设认证包括（Google 动态令牌、飞天 UKey、短信认证、动态令牌等），认证服务器包括（Radius、AD 域、LDAP、证书等），通过配置这一系列认证方式，

有效提高了运维人员访问系统和资源的安全性，同时提供访问控制功能，有效解决人员的操作风险问题，降低相关 IT 系统的安全风险。

三、产品优势

3.1.1. 跨平台兼容

运维审计系统凭借 HTML5 运维代理技术，无论运维人员身处何种设备环境，无需要安全任何插件、程序和工具，只要具备网络连接和浏览器，就能通过运维审计系统对所有 UNIX 类服务器、LINUX 类服务器、Windows 类服务器、国产操作系统、网络设备和安全设备等不同平台的设备统一、便捷管理。

得益于其跨平台兼容的特性，消除了设备间的操作差异，运维环境的灵活性和一致性得以显著提升。并且其直观的用户界面和直观的操作设计，确保了无论是经验丰富的技术人员还是新手运维都能迅速适应，显著降低了学习成本。打造了一个无边界、易用的运维平台。

3.1.2. 自动化运维

运维审计系统通过自动化运维方式，将例行的、冗余的、耗时的运维任务转化为预先设定的流程或自动化脚本，实现了对运维资产的自动化管理。这一流程涵盖了权限分配、登录验证、密码更新、任务调度和性能监控等多个运维环节。通过自动化，运维人员能够设定高效规则，如定时执行批量的密码更新或设备管理，从而提高了运维效率。并且针对 Web、VNC、X11 和数据库等应用程序的运维，系统通过应用发布机制，提供口令自动填充、完整操作记录等功能，且内置的应用发布服务器作为核心承载，消除了用户网络中额外设备的需要。同时，自动化运维产生的详细审计记录有助于追踪操作历史和符合合规性要求。总之，自动化运维提升运维效率、降低成本和强化服务质量，推动了企业的数字化转型进程。

3.1.3. 精确的分析功能

运维安全审计系统通过资产和用户运维记录形成用户和资产的追溯统计图，能够让客户方便、快捷进行审计溯源。针对用户和资产在一定时间范围内，用户分别运维了哪些资产，资产被用户进行了多少次运维，可查看审计，具有回放视频，指令操作等详细信息方便用户可快速查看追溯资产和用户信息。

由于大量资源，我们查看整个资源授权信息时，必须挨个查看每个资产的授权信息。系统具有授权图谱功能，以用户或者用户组为中心，呈现出用户和资源、协议之间的详细信息，方便用户可快速了解系统资源和用户之间的授权信息。

系统会自动统计一定时间范围内的数据信息（包括会话、指令、告警等），呈现出的信息有柱形统计图、圆形统计图，可得出在一定时间范围内的排名、分布，并可查看逐个次数。

3.1.4. 逻辑命令自动识别技术

运维安全审计系统自动识别当前操作页面，对当前页面的输入输出进行控制，组合输入输出流，自动识别逻辑语义命令。系统会根据输入输出上下文，确定逻辑命令编辑过程，进而自动捕获出用户使用的逻辑命令。该项技术解决了逻辑命令自动捕获功能，在传统键盘捕获与控制领域取得新的突破，可以更加准确的控制用户意图。

3.1.5. 静态转动态展示

系统采用最前沿界面架构，整体展示界面友好和操作过程便捷且舒适，展示界面中所包含的图表、数据、查询等功能具备良好的视觉感官。为了避免资源、用户、授权等在处理大量数据时浏览器出现的卡顿、崩溃等问题，系统采用了大数据的架构对数据进行存储与分析处理，主要数据采用 ES 压缩架构进行归档化存储。运维安管理系统支持谷歌、火狐、edge、IE 等主流浏览器，其中在实际业务运行中谷歌浏览器所展示效果最优。

3.1.6. SAAS 化多租户模式

运维审计系统支持 SAAS 化多租户模式提供资源利用，多个租户共享基础设施资源，减少闲置浪费。其成本低，开发、部署和运维成本都得以削减，提供商集中开发维护、租户无需搭建环境且无需专门运维人员。可扩展性强，能轻松添加租户，单个租户也可便捷扩展资源和功能。安全性高，提供商采用专业安全措施且租户数据相互隔离。功能更新及时，新功能推出时所有租户可立即使用。

四、部署建议

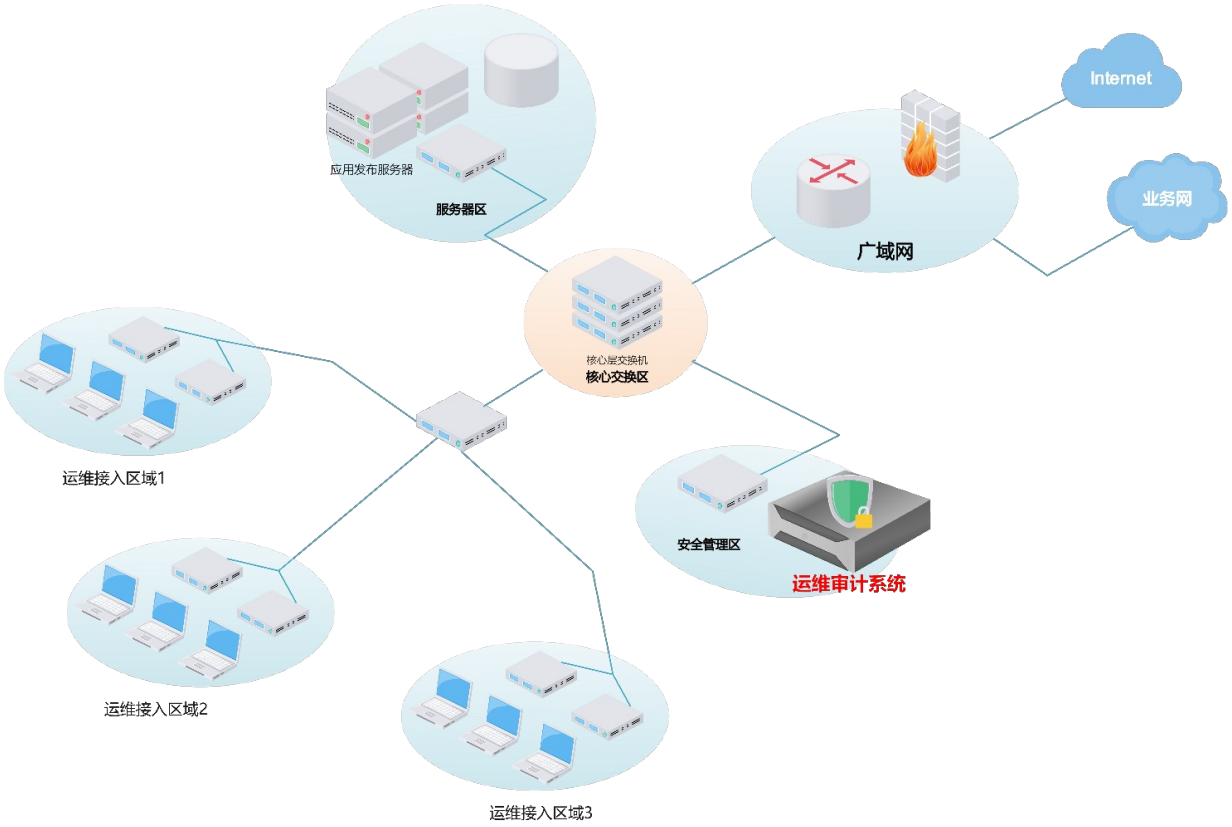

图 1：物理部署拓扑图

如图所示，运维审计系统采用物理旁路，逻辑串联方式进行部署。旁路模式部署起来比较灵活方便，只需接入交换机与全部网络达成通信状态，不会影响用户现有的网络结构。

五、用户收益

5.1. 统一操作管理门户

运维审计系统为用户提供了横跨所有 UNIX 类服务器、LINUX 类服务器、Windows 类服务器、网络/安全等重要设备的统一操作管理入口，并对用户操作管理等网络访问行为进行控制，避免用户直接接触目标服务器重要资源，构建安全规范的服务器操作管理唯一通道。

运维审计系统不改变用户原有使用习惯，提供了字符终端平台、图形终端平台、文件传输平台、应用中心操作等多种平台，实现虚拟应用集中发布操作统一管理。

5.2. 提高设备可用性，网络安全性

通过部署运维审计系统，可以减少设备运维的风险性，降低 IT 运维管理的复杂度，帮助企业提高 IT 设备的可用性；减少网络中原来所有服务器都需要对外开放维护端口的暴露，做到由单一的运维审计系统提供对外维护端口，提高网络安全性。

5.3. 完善责任认定体系

通过部署运维审计系统，所有系统管理人员、第三方系统维护人员，都将通过运维审计系统来实施网络管理和服务器维护，对所有的操作行为，都做到可记录、可控制，审计人员通过定期对维护人员的操作审计，可以规范运维人员的操作，真正做到“事前可知，事中可控，事后可查”。

审计人员通过定期对维护人员的操作审计，可以提高维护人员的操作规范性。对于第三方代维厂商，通过运维审计系统保证让他们所有的操作行为变得可视，可控，可管，可追踪，实现对第三方代维厂商的有效监管。

通过运维审计系统对网内资产上的命令行以及图形界面操作，均会被真实完整地记录

在系统中，当发生任何安全问题或对代维方的操作产生争议时，都可通过录像的回放再现真实运维过程，帮助管理者快速定位故障点及责任人。审计排查过程中提供了命令、时间、账号等多种关键字快速检索，并可按照具体范围生成统计报表及视频下载，作为故障排查与运维汇总的有利依据。

5.4. 规范操作管理

通过运维审计系统，可以实现操作透明化，对于用户的任意操作，可以通过 web 界面实时监控，无论是内部运维人员以及外包运维商所做的所有操作都会被真实完整地记录下来。

对于操作实现可控，对于存在风险的操作可以实现事前以及事中的控制。通过权限控制，可以主动切断用户的高危操作，也可以对于用户的违规操作，可以实时切断。

运维审计系统将用户从繁琐的监督管理工作中解放出来，投入到其他工作上，对第三方代维厂商的维护操作也不再需要专门陪同，从而有效提高了操作管理效率。

5.5. 兼容国产化操作系统

运维审计系统支持目前主要国产化操作系统的运维，在国产化运维中不仅提供了上述诸多优势，而且用户在进行国产化转型时无需更换现有设备，即可实现无缝对接和升级。这种灵活性和兼容性显著降低了因国产化要求而可能产生的额外成本和复杂性，确保用户在享受国产化带来的安全和自主可控优势的同时，也能保持现有 IT 基础设施的稳定性和连续性。通过这种方式，运维审计系统不仅提升了运维的效率和安全性，还为用户节省了大量的时间和经济成本，进一步增强了其在国产化进程中的竞争力和适应性。

5.6. 便捷高效的云化方案

为中小规模企业的理想之选，资金和技术资源有限的它们提供低成本、高性价比的运维审计服务。对大型企业部门级应用也有优势，可满足不同部门个性化需求并统一管理监

控。用户能灵活适应业务变化，按需调整使用方式和资源配置。数据安全与合规性得到保障，满足法律法规要求。还能使用户专注核心业务，不必在运维审计系统上耗费过多精力。

5.7. 满足法律法规要求

运维审计系统强大的权限控制和安全审计功能，可以用户充分符合以下要求：

- 国家标准 GB/T 22239–2019，《信息安全技术网络安全等级保护基本要求》
- 国家标准 GB/T18336.2–2024，《网络安全技术 信息技术安全评估准则 第 2 部分：安全功能组件》
- ISO27001/ISO17799:2005/BS7799,《信息安全管理技术规范》
- 国内外相关运维审计准则与办法