# 知道创宇

## 知道创宇运维审计堡垒机系统

## 产品技术白皮书


北京知道创宇信息技术股份有限公司

# 目录

# 版权说明



# 适用对象

本文档适合于各行业信息部门相关技术人员、服务人员、信息系统审计人员等。

# 名词释义

RDP：Windows 远程桌面的缩写；

SSO：单点登录系统的简称

主账号：堡垒机运维账号

从账号：服务器系统账号

# 1. 前言

随着信息化的快速发展与普及，业务运行已于信息化系统密不可分，由于业务需求的不断拓展，信息化系统的建设也在不断深入与增长，企事业单位的业务系统变得日益复杂，信息化系统俨然已经成为了业务运行保障的重中之重，信息化系统的瘫痪会对业务带来的损失和影响不可估量，为防止信息化系统事故的发生，加强信息化系统的安全建设与管理已迫在眉睫。然而根据各种权威的网络安全调查结果均表明，在可统计的安全事件中，85%以上均与内部人员有关，这其中既包括恶意行为（越权访问、恶意破坏、数据窃取），也包括各种非主观故意引起的非恶意行为（误操作、权限滥用）。由此可见，规范内部人员的访问行为，特别是核心系统（主机、网络设备、安全设备、数据等）的维护行为势在必行。

传统的信息安全建设，往往侧重于对外部黑客攻击的防范，以及网络边界的访问控制，对信息系统安全威胁最大的内部人员行为却缺乏有效的管理。企事业单位内部人员，特别是拥有信息系统较高访问权限的运维人员（如网管员、临时聘用人员、第三方代维人员、厂商工程师等），比外部入侵者更容易接触到信息系统的核心设备和敏感数据、内部人员恶意或非恶意的破坏行为更容易造成较大的破坏。然而，由于现有管理手段的不完善，账号共享情况普遍存在，以及加密、图形协议的广泛应用，使得这些运维审计人员的日常操作，存在操作身份不明确、操作过程不透明、操作内容不可知、操作行为不可控、操作事故无法定位等安全风险。内部人员的操作行为几乎处于完全失控的状态，一旦发生事故，其后果的严重性将是无法预估的。因此，放任内部风险的存在决不可行。

此外，随着《中华人民共和国计算机信息系统安全保护条例》的推广实施，对 IT 系统内部控制的要求越来越明确。从遵守国家及本行业各项法律法规的角度考虑，如等保基本要求中明确提出，要对“内部维护人员登录主机、数据库所进行的所有操作行为”、“第三方人员的维护行为”进行审计和控制。为满足用户对加强内部运维安全审计日益迫切的需要，杭州知道创宇信息技术股份有限公司依托自身强大的研发能力，丰富的行业经验，自主研发了新一代软硬件一体化运维安全专用审计系统——知道创宇运维审计堡垒机系统。该系统支持对企事业单位内部人员的维护行为进行全面的管理、审计，消除了传统审计系统中的盲点，

使企事业单位对运维人员的操作过程，能做到事前防范、事中控制、事后审计的能力，是企事业单位 IT 内控最有效的运维审计平台。

# 2. 需求背景

## 2.1.IT 内控运维安全管理需求

### 2.1.1. 缺乏人员身份认证和统一管理

目前随着企事业单位信息系统的发展和建设，信息系统的维护人员也在日益增多，介于企事业单位战略定位和人力资源等诸多问题，很多企事业单位会将信息系统和业务系统的开发与运维交予第三方系统开发商和运维公司，加之企事业单位内部人员流动和各类其他第三方厂商，人员繁多且关系复杂。出于信息化系统建设的便利性和内控管理制度的欠缺，对运维人员访问信息系统缺乏严格的身份认证和权限划分，权限关系混乱，账号公用滥用，当出现安全事故时相互推诿，缺乏客观、可信的依据来确定事故责任人。

### 2.1.2. 缺乏设备资产账号信息安全管理

随着信息化建设的深入，设备数量也是随之激增，大量的服务器账号密码成了一个重大管理难题。出于便利性考虑，一般服务器资产账号密码会统一设置和管理，但在信息化系统建设中各类人员需要不断登录和维护设备，由于密码基本相同，所有系统账号信息基本人尽皆知，存在着巨大的安全隐患。如果出于安全性考虑，管理人员各司其职管理各自的设备账号信息，则每个用户需要记忆多个不同的账号密码信息，导致管理工作量与复杂度大幅增加，使得运维效率下降，且还容易导致账号密码信息丢失和遗忘。所以设备账号密码信息管理已进退维谷。

### 2.1.3. 缺乏有效的访问控制和高危操作预防

一般企事业单位内部的网络访问控制管理都较为粗犷，一旦接入到网内即可访问到各类核心的业务服务器，需要非常完善和严谨的访问控制管理制度，但完善的管理制度又催生了极大的人力和时间成本，加之交换机和防火墙中访问控制的便利性和实效性较差，频繁的变更和过多臃肿的访问控制策略使管理非常的繁琐和不便。且运维操作管理制度难落实和操作权限控制的缺乏，加之各类高权限

账号滥用（如 administrator 和 root 账号），各类恶意操作和误操作频发，导致各类核心业务数据被窃取和业务中断，对企事业单位造成不可挽回的名誉及经济损失，而事后追查也只能是亡羊补牢而已。

### 2.1.4. 缺乏完整的运维操作审计记录

为保障系统的安全性，日常运维中都以加密协议为主（如 RDP 和 SSH 协议），由于系统自身操作日志的缺乏，加密协议无法在网络中审计抓取，给操作审计带来了严峻的挑战，当出现运维事故时无法准确定位故障原因，导致故障排查周期过长带来更多的损失，以及缺乏事故客观、有利的证据。

# 2.2.政策法规的合规性需求

## 2.2.1. 国际信息安全标准

★ **信息安全管理实施指南（ISO17799/BS7799-1）**

2000 年 12 月，国际标准化组织 ISO 正式发布了有关信息安全的国际标准 ISO17799，这个标准包括信息系统安全管理和安全认证两大部分。ISO17799 提供了一套综合的、由信息安全最佳措施组成的实施规则和管理要求，它广泛地涵盖了几乎所有的安全议题，非常适合于作为大、中、小组织的信息系统在大多数情况下所需的控制范围确定的参考基准。建立信息安全管理体系，能够提高组织自身的安全管理水平，将企事业单位的安全风险控制在可接受的程度，减小信息安全遭到破坏带来的损失，保证业务的可持续运作。

**ISO17799 关于安全审计的内容包括：**

- **10.10 监视**
  - ✓ 10.10.1 审计日志
  - ✓ 10.10.2 监视系统的使用
  - ✓ 10.10.3 保护日志信息
  - ✓ 10.10.4 管理员和操作者日志
  - ✓ 10.10.5 错误日志
- **15.3 信息系统审计考虑因素**
  - ✓ 15.3.1 信息系统审核控制
  - ✓ 15.3.2 信息系统审核工具的保护

## 2.2.2. 国内信息安全标准

★ **计算机信息系统安全保护等级划分准则（GB17859）**

计算机信息系统安全保护等级划分准则是我国计算机信息系统安全等级保护系列标准的核心，是我国实行计算机信息系统安全保护的重要基础，它将计算机信息系统安全性从低到高划分了五个等级：第一级用户自主保护级、第二级系统审计保护级、第三级安全标记保护级、第四级结构化保护级、第五级访问验证

保护级；二级以上系统安全保护中增加了对安全审计的要求，从主机安全、网络安全、应用安全三个层面提出了安全审计的具体要求及应有措施，并逐级增强。（详见信息系统安全等级保护基本要求之 6.1.2.3、6.1.3.3、6.1.4.3…）

## 2.2.3. 国内重点行业信息安全法规

★ **商业银行信息科技风险管理指引**

- **第二十五条：**

（三） 制定最高权限系统账户的审批、验证和监控流程，并确保最高权限用户的操作日志被记录和监察。

（五） 在系统日志中记录不成功的登录、重要系统文件的访问、对用户账户的修改等有关重要事项，手动或自动监控系统出现的任何异常事件，定期汇报监控情况。

- **第二十六条：**

（七） 以书面或电子格式保存审计痕迹。

（八） 要求用户管理员监控和审查未成功的登录和用户账户的修改。

★ **证券期货业信息系统安全等级保护基本要求**

其中对网络、主机和应用的安全审计有明确的要求

第二级中针对主机安全审计要求 “审计范围应覆盖到服务器上的每个操作系统用户和数据库用户。系统不支持该要求的，应以系统运行安全和效率为前提，采用第三方安全审计产品实现审计要求。审计记录应至少保存 6 个月”。

第二级中针对应用安全审计要求“对应用系统重要安全事件进行审计，审计记录至少保存 6 个月”。

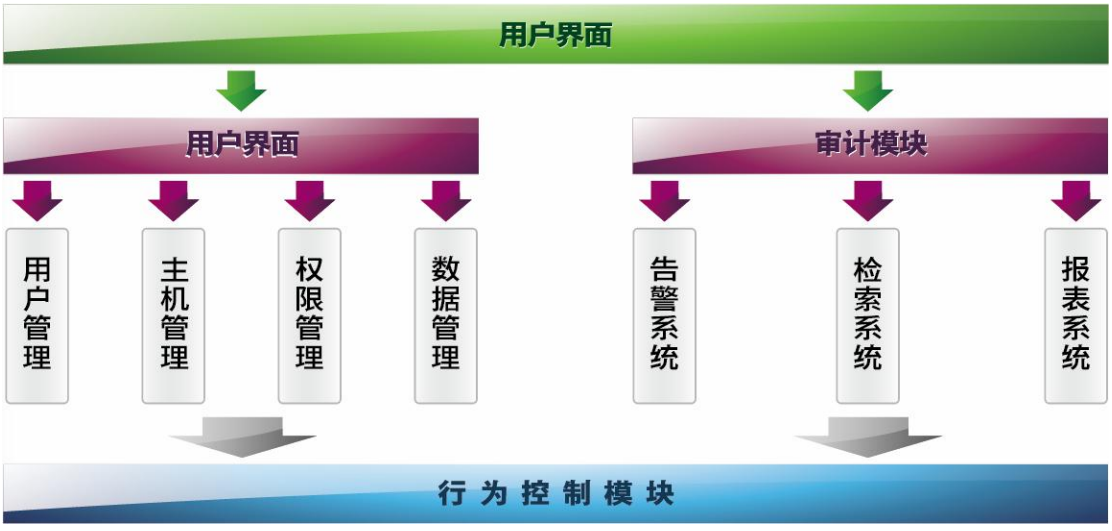
第二级系统运维管理中要求“至少每季度对运行日志和审计数据进行分析，以便及时发现异常行为”。

# 3. 产品概述

知道创宇运维审计堡垒机系统（简称知道创宇运维审计堡垒机系统）是新一代操作行为管理安全审计系统，它采用软硬件一体化设计，通过 B/S 方式（https）进行管理，其主要功能为实现对运维人员远程访问操作服务器、网络设备、数据库过程的认证、授权、监控与审计，实现对 IT 运维过程的全面监管，做到有效的事前预防、事中控制及事后审计，满足用户的安全管理需求。该产品采用先进的设计理念，支持对多种远程维护方式的支持，如字符终端方式（SSH、Telnet、Rlogin）、图形方式（RDP、X11、VNC、Radmin、PCAnywhere）、文件传输（FTP、SFTP）以及多种主流数据库的访问操作。

## 3.1. 系统架构

知道创宇运维审计堡垒机系统采用模块化设计，主要由以下模块组成：行为控制模块、审计模块、管理模块、存储模块、用户管理接口模块，各模块间关系如下图所示：




**行为控制模块**

实现对网络、数据库、服务器维护过程的网络数据包代理转发、行为还原及记录、违规行为阻断功能；

**管理模块**

实现维护用户管理、主机资产管理、用户授权与访问权限管理，以及对审计记录的数据存储控制；

**审计模块**

实现行为安全审计功能，包括实时违规行为告警系统、历史记录检索系统以及报表系统；

**用户界面**

提供运维人员审计管理接口，以及运维用户的远程工具使用界面。

## 3.2. 部署方式

**单臂部署：**


单臂部署示意图

如图所示，堡垒机系统在部署时只需要为其分配一个独立 IP 地址即可，无需对网络拓扑结构进行任何调整。一般而言，知道创宇运维审计堡垒机系统部署在服务器所在网段，同时堡垒机的 IP 地址通过网络设备发布到外部网络中供运维人员访问。

部署知道创宇运维审计堡垒机系统后，内部服务器的维护端口只需开放给运维安全管理系统，无需再让运维人员直接访问。对运维人员，只需开放知道创宇运维审计堡垒机系统的访问端口，从而进一步加强内部服务器的安全性。

**双臂模式部署：**


双臂部署示意图

在双臂模式下，知道创宇运维审计堡垒机系统拥有内外两个 IP 地址，内部 IP 地址与服务器网段相通，外部服务器用于运维用户访问。该部署方案适用于服务器网段与客户端网段划分清晰的情况，此外采用该方案有利于实施网络控制 ACL。

# 3.3. 支持的运维协议与对象

| 支持访问协议列表 | 支持访问对象列表 |
| --- | --- |
| 字符型访问协议 | 操作系统 |
| SSH | windows |
| Telnet | linux |
| rlogin | bsd |
| | AIX |
| 图形访问协议 | 网络设备 |
| RDP | CISCO |
| X11 | HUAWEI |
| VNC | 其他 |
| Radmin | |
| Pcanywhere | |
| 文件传输协议 | 安全设备 |
| FTP | 防火墙 |
| SFTP | 负载均衡 |
| | 其他 |
| 数据库访问协议 | 数据库 |
| Oracle | Oracle |
| MsSQL | Mssql |
| Mysql | Sybase |
| DB2 | DB2 |
| Sybase | Sybase |
| Informix | Informix |
| 其他访问协议 | 其他应用系统 |
| HTTP(s) | KVM |
| ... | 第三方应用程序 |

# 4.产品功能

## 4.1.统一身份认证与 SSO

在信息系统的运维操作过程中，经常会出现多名维护人员共用设备（系统）账号进行远程访问的情况，从而导致出现安全事件无法清晰地定位责任人。知道创宇运维审计堡垒机系统为每一个运维人员创建唯一的运维账号（主账号），运维账号是获取目标设备访问权利的唯一账号，进行运维操作时，所有设备账号（从账号）均与主账号进行关联，确保所有运维行为审计记录的一致性，从而准确定位事故责任人，弥补传统网络安全审计产品无法准确定位用户身份的缺陷，有效解决账号共用问题。

**知道创宇运维审计堡垒机系统支持多种身份认证方式：**

- ✓ 本地认证
- ✓ Radius 认证
- ✓ 动态令牌（安盟、RSA）
- ✓ LDAP 认证
- ✓ AD 域认证等
- ✓ 短信认证

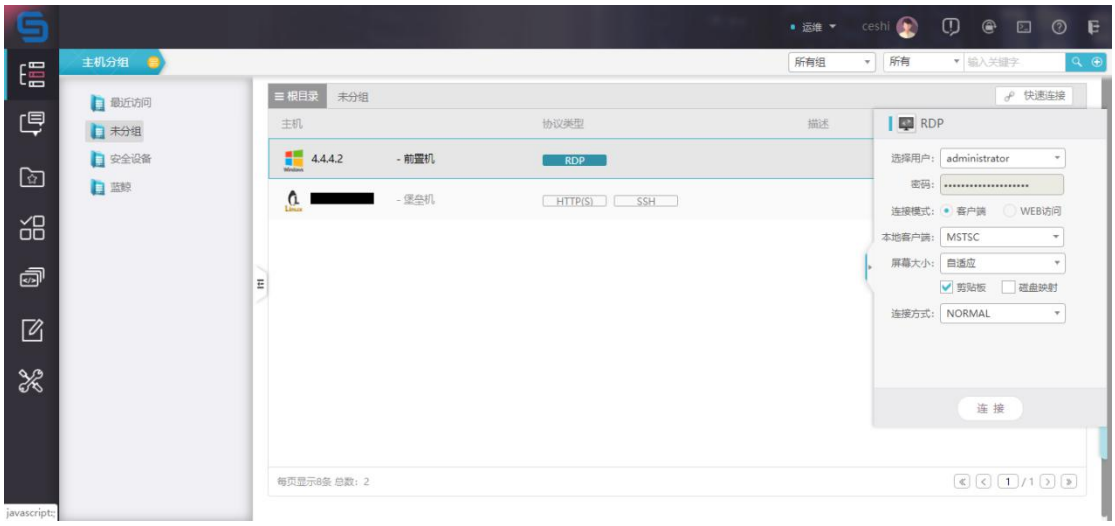
知道创宇运维审计堡垒机系统系统还支持 SSO 功能，运维人员一次登陆，即可访问所有目标资源，无需二次输入用户名、口令信息。

## 4.2.统一维护访问通道功能

知道创宇运维审计堡垒机系统部署后，运维人员可以通过不同的方式对目标对象进行访问、维护：

- ✓ WEB 控件方式访问，所有协议均可通过 WEB 空间方式从 WEB 直接发起访问，访问过程支持 IE、Firefox、chrome 等多种浏览器；
- ✓ 支持通过 WEB 直接调用本地客户端方式进行访问；
- ✓ 支持本地直接使用 CS 客户端直接访问，兼容管理员原有使用习惯

运维人员登录知道创宇运维审计堡垒机系统时，系统会根据访问授权列表自动展示授权范围的主机，避免用户访问未经授权主机。




用户访问界面展示

此外，知道创宇运维审计堡垒机系统还支持在运维过程中要求其他运维人员进行协同操作的功能，在协同操作模式下，2 名运维人员可以共同操作同一个访问会话界面；

## 4.3.运维工作流管理

知道创宇运维审计堡垒机系统系统内置了多个运维工作流程管理功能，IT 部门能够通过运维工作流功能规范 IT 运维过程，工作流功能包含以下具体流程：

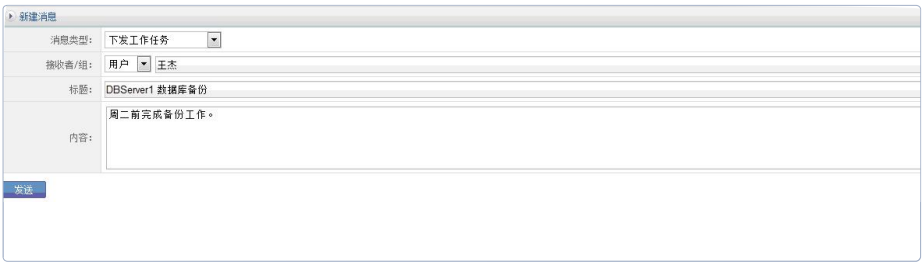
a）工作任务管理流程：

1. 任务发起人通过系统下发工作任务；
2. 任务接收人在个人消息中心实时接收工作任务信息；

3. 任务接收人完成工作，在 WEB 界面中进行任务回复；
4. 任务发起人接收到回复信息后，对任务执行情况进行确认，结束工作任务流程；

b）审计流程：

审计流程包含异常事件处理流程及报表审计流程两部分，审计人员可以查看相关异常事件及报表并添加相应的审计意见，否则该事件会一直处于未处理状态，以提醒审计人员对重点事件进行关注并审计。


消息中心功能展示

## 4.4. 设备密码管理功能

知道创宇运维审计堡垒机系统支持主机系统账号的密码维护托管功能，系统支持自动定期修改 windows、Linux、Unix、cisco、huawei 等设备的账号密码。自动密码管理支持以下功能：

- ✓ 设定密码复杂度策略；
- ✓ 针对不同设备制定不同改密计划；
- ✓ 设定改密计划的自动改密周期；
- ✓ 支持随机不同密码、随机相同密码、手工指定密码等新密码设定策略；
- ✓ 改密结果自动发送至指定密码管理员邮箱；
- ✓ 设定指定的改密对象，支持 AD 域账号改密；
- ✓ 手工下载部分或全部密码列表；
- ✓ 自动改密结果确认功能，密码管理员必须人工确认已经下载或收到密码文件；

否则改密计划自动停止执行，确保改密过程可靠性；

✓ 改密结果高强度保护功能，必须经过专用密码查看器加密码以及设备序列号才能访问


密码策略配置界面展示


自动改密计划界面展示

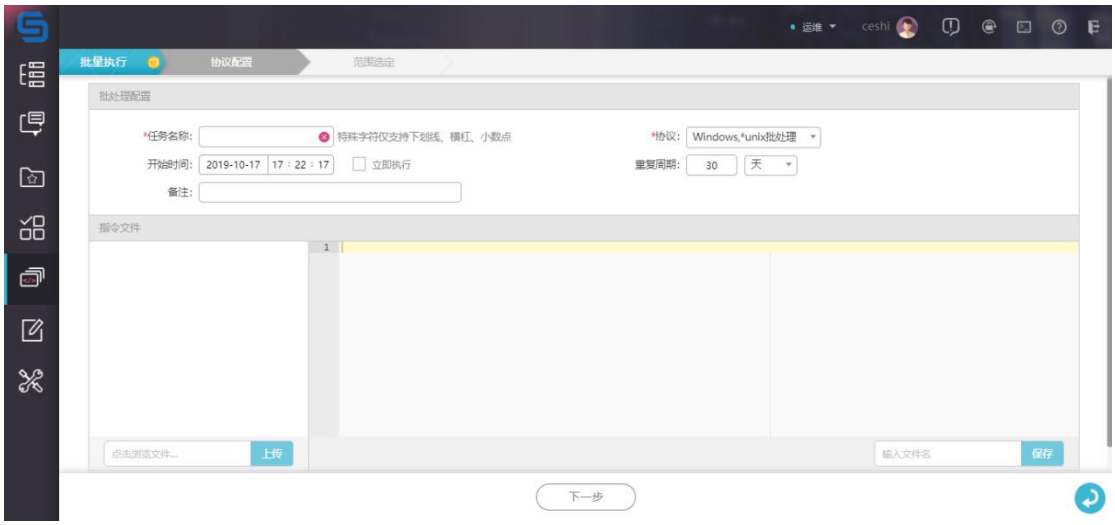
## 4.5.批量执行功能

知道创宇运维审计堡垒机系统系统支持自动化在多台机器上批量执行指令。通过批量执行功能，管理员可以方便实现对多台主机的升级、备份等工作任务。

✓ 支持通过 SSH、Telnet、Rlogin 执行系统命令；

✓ 支持 MySQL 批量指令执行；

- ✓ 支持 MySQL over SSH 模式；
- ✓ 可设定任务执行开始时间；
- ✓ 可设定执行的目标主机与系统账号；
- ✓ 执行过程与结果审核；




批处理管理界面展示

## 4.6.便利及细粒度访问授权

知道创宇运维审计堡垒机系统系统通过集中统一的访问控制和细粒度的命令级授权策略，确保每个运维用户拥有的权限是完成任务所需的最合理权限。

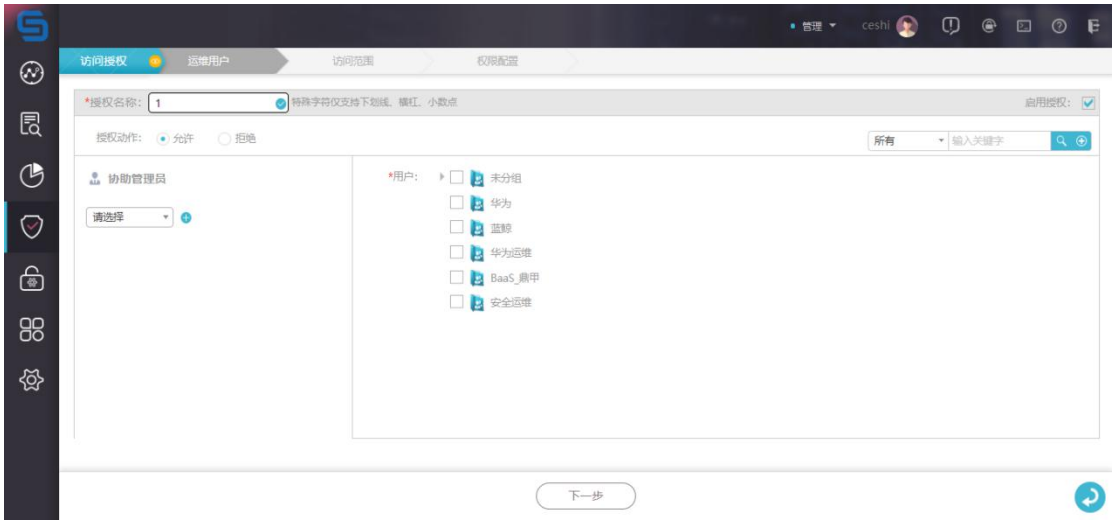

- ✓ 基于向导式的配置过程；
- ✓ 支持基于用户角色的访问控制（RBAC ,Role-Based Access Control）。管理

员可根据用户、用户组、访问主机、目标系统账号、访问方式设置细粒度访问策略；

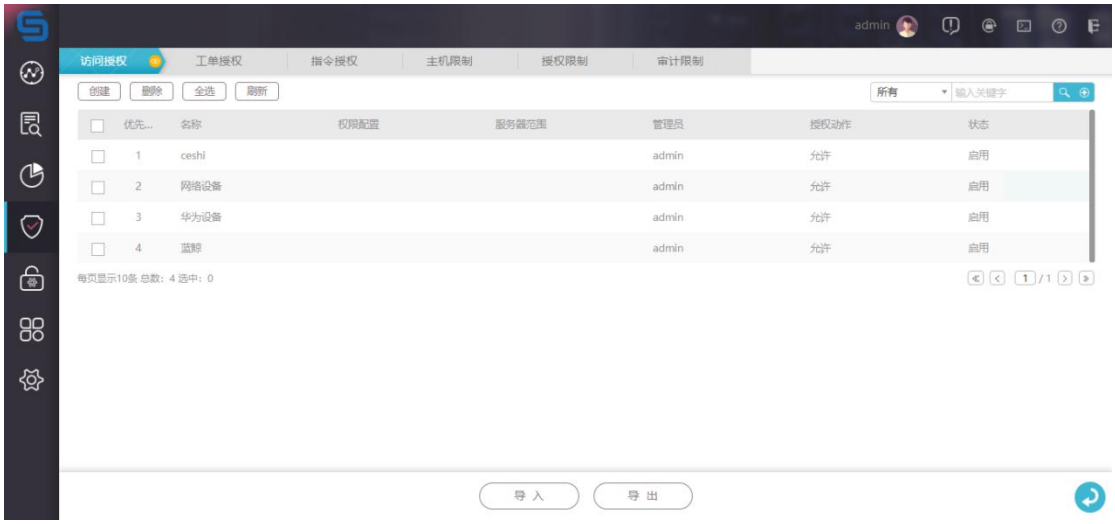
- ✓ 支持基于时间的访问控制；
- ✓ 支持基于访问者 IP 的访问控制；
- ✓ 基于指令（黑白名单）的访问控制；

除访问授权之外，堡垒机系统还支持针对访问协议进行深层控制，比如：

- ✓ 限制 SSH 协议使用 SFTP
- ✓ 限制 RDP 访问使用剪贴板功能
- ✓ 限制 RDP 访问使用磁盘映射功能
- ✓ 是否启用强制审批功能（访问和操作前必须经过管理员审批）
- ✓ 是否启用备注功能（访问前必须先填写维护内容）




向导式策略配置界面展示



访问策略界面展示

## 4.7.关键访问操作二次审批

堡垒机系统支持根据需求对特殊访问与操作进行二次审批功能，该功能可以进一步加强对第三方人员访问或关键设备访问操作的控制力度，确保所有访问操作都在实时监控过程中进行。

二次审批功能支持以下两种方式：

- ✓ 对新建远程访问会话进行审批
- ✓ 对特殊指令执行进行审批

由于每次访问操作都需要管理员进行审批确认，该功能也可以代替部分客户使用的双人密码管理方式。

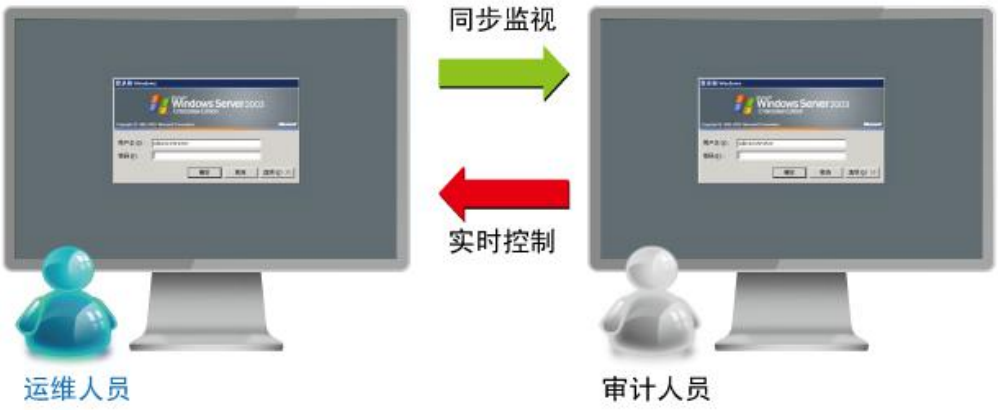
## 4.8.违规访问告警与阻断

知道创宇运维审计堡垒机系统系统支持根据已设定的访问控制策略，自动检测日常运维过程中发生的越权访问、违规操作等安全事件，系统能够根据安全事件的类型、等级等条件进行自动的告警或阻断处理。


- ✓ 阻断未经授权用户访问主机；
- ✓ 阻断从异常客户端、异常时间段发起的访问行为；
- ✓ 阻断指令黑名单的操作行为；
- ✓ 阻断方式支持：断开会话、忽略指令；
- ✓ 告警方式支持：WEB 界面告警、短信告警、邮件告警等。


违规处理配置界面展示

## 4.9. 实时操作过程监控




对于所有远程访问目标主机的会话连接，堡垒机系统均可实现操作过程同步监视，运维人员在远程主机上做的任何操作都会同步显示在审计人员的监控画面中，管理员可以随时手工中断违规操作会话。

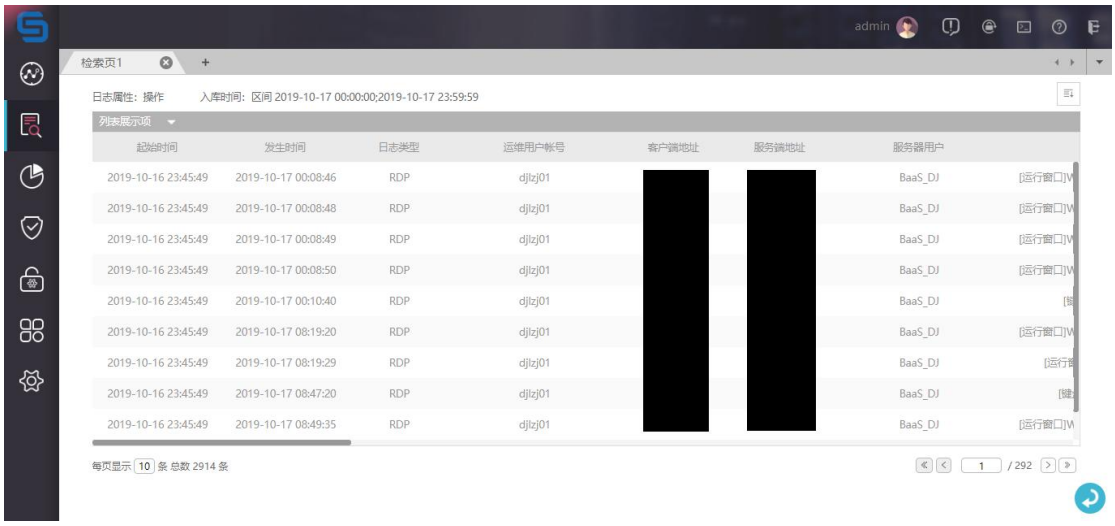
- ✓ 实时同步显示操作画面；
- ✓ 支持 vi、smit、setup 等字符菜单操作同步显示；
- ✓ 随时手工阻断违规操作过程。

## 4.10. 历史记录查询

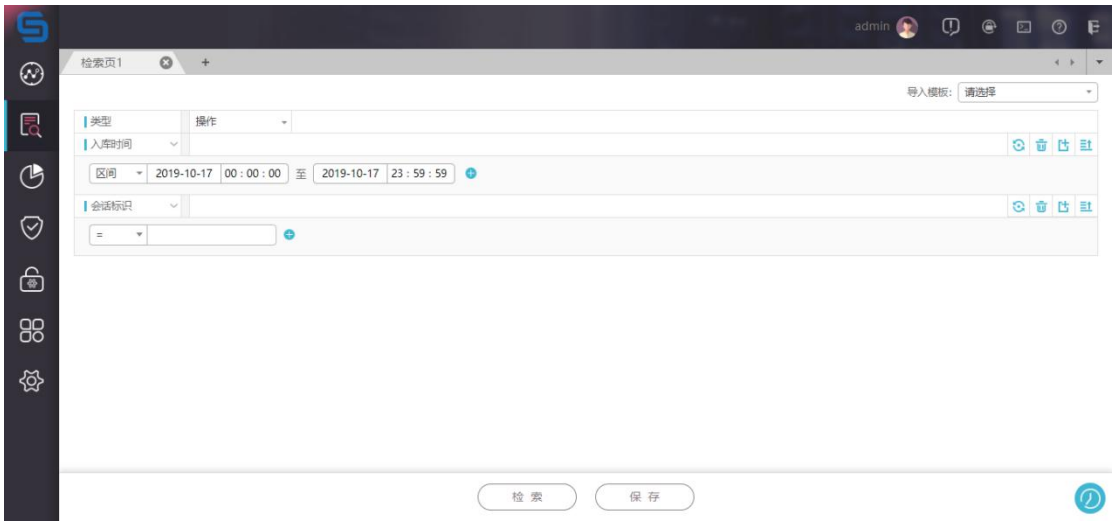
知道创宇运维审计堡垒机系统支持两种查询功能，快速查询（单一条件）和

高级查询（多重组合条件），审计人员可以根据操作时间、源、目标 IP 地址、用户名（运维、主机）、操作指令等条件对历史数据进行查询，快速定位历史事件。

- ✓ 快速审计查询支持在结果集中继续深入查询；
- ✓ 高级查询支持对将任意字段设为查询条件；
- ✓ 支持大于、小于、等于、字符包含、不包含、时间区间、IP 区间等多种逻辑判断符；
- ✓ 支持任意多重条件组合查询；
- ✓ 海量数据高速检索能力，检索结果即搜即得；




快速检索界面展示

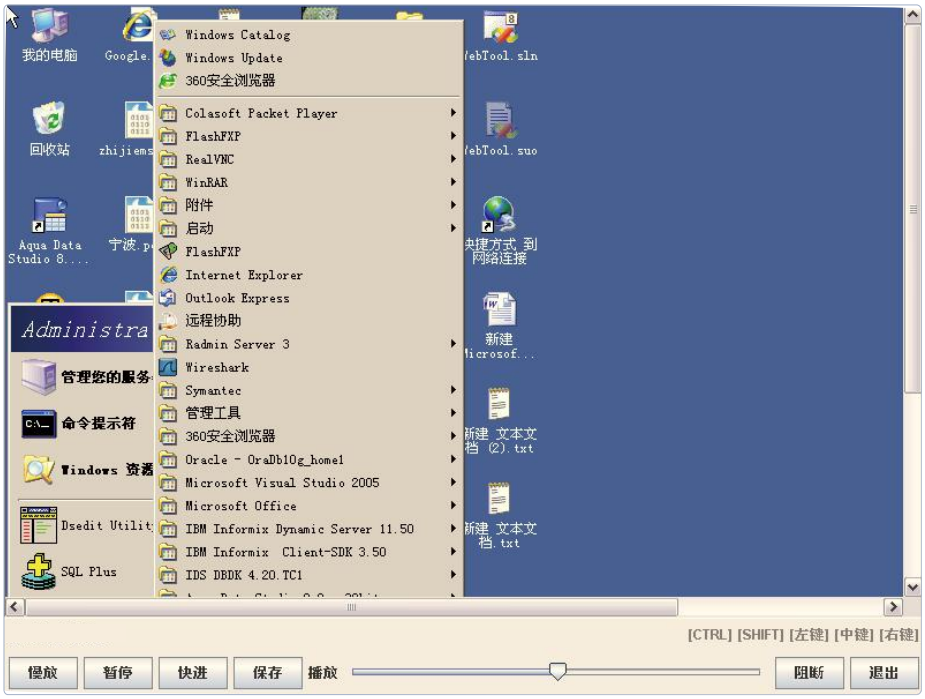



高级查询界面展示

## 4.11. 历史操作图形回放

知道创宇运维审计堡垒机系统能够以视频回放方式，可根据操作记录定位回放或完整重现维护人员对远程主机的整个操作过程，从而真正实现对操作内容的完全审计。

- ✓ 完整回放整个操作过程；
- ✓ 根据特定操作进行定位回放；
- ✓ 支持快速播放、拖动、暂停、重放等播放控制功能；
- ✓ 可下载记录文件进行离线播放；

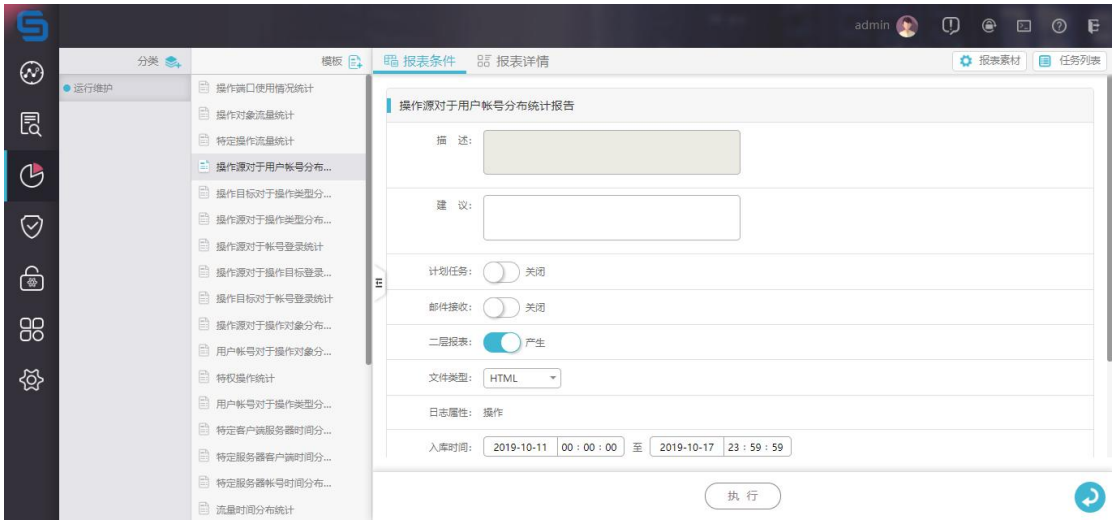



## 4.12. 综合审计报告

知道创宇运维审计堡垒机系统系统拥有强大的报表功能，内置能够满足不用客户审计需求的安全审计报表模板，支持自动或手工方式生成运维审计报告，便于管理员全面分析运维的合规性。

- ✓ 支持报表自定义扩展；
- ✓ 支持柱状图、饼图、折线图等多种方式对统计数据进行展示；
- ✓ 支持按天、周、月自动周期性生成报表；

✓ 支持报表自动发送功能；




报表配置界面展示


# 4.13. 审计数据存储管理

知道创宇运维审计堡垒机系统系统支持自动化审计数据存储管理，管理员可以对审计数据进行手工备份、导出，也可以设定自动归档策略进行自动归档。

✓ 手工归档、到处审计数据；

✓ 存储空间不足时自动归档并删除最早数据；

✓ 支持通过 FTP、SFTP 自动上传归档文件；

✓ 周期性自动归档功能；


自动归档策略展示

# 5. 产品特性

## 5.1. 协议覆盖全、易扩展

知道创宇运维审计堡垒机系统支持各种主流操作协议包括字符型操作（Telnet、SSH、Rlogin）、图形化操作（RDP、VNC、X11）、文件传输（FTP/SFTP）、数据库访问操作等。通过配置应用扩展中心（ACC），还可以灵活扩展其他操作协议及工具。

## 5.2. 灵活的访问方式

知道创宇运维审计堡垒机系统系统是兼容管理员使用习惯最好的运维审计产品，是唯一一款同时支持页面访问方式、菜单访问方式、客户端工具访问方式，WEB 使用界面友好，能够最大程度适应不同用户的使用习惯。

同时，堡垒机还支持多种协议的网络协同操作功能。

## 5.3. 协议深度支持

知道创宇运维审计堡垒机系统不仅能够对运维协议进行指令与图形操作记录，还能对多种协议进行深度支持，如：

- ✓ SSH CLONE SESSION 支持，管理员可方便复制当前会话；
- ✓ SSH 客户端中可直接创建文件传输会话；
- ✓ 支持 MySQL over SSH 功能
- ✓ RDP 磁盘映射支持；
- ✓ RDP 键盘输入与窗口标题识别
- ✓ RDP 剪贴板支持等。

## 5.4.细粒度访问授权与控制

- ✓ 知道创宇运维审计堡垒机系统是业界唯一同时具备指令黑白名单、时间黑白名单、IP 黑白名单的运维审计产品
- ✓ 无论字符还是图形操作均可进行同步监控、阻断；
- ✓ 重要会话与操作二次审批机制，大大增强了临时账号的安全性，阻断和忽略指令功能大大降低了误操作的风险。

## 5.5.支持批量执行功能

针对游戏运营商、云架构提供商等拥有大量服务器数量的客户，知道创宇运维审计堡垒机系统系统支持批量执行功能，能够对大批量服务器自动执行批量指令或脚本，并能够对脚本的执行过程及结果进行跟踪及审计。

## 5.6.大并发量处理能力

- ✓ 高并发会话处理能力，能够满足不同容量用户运维审计需求；
- ✓ 采用专利存储和检索技术，轻松处理海量审计数据；

## 5.7.流程化管理能力

知道创宇运维审计堡垒机系统系统支持工单模式与消息中心功能。

在启用工单模式下，每次会话访问前都必须先输入本次访问的内容与目的，便于后期审计。

知道创宇运维审计堡垒机系统系统内置消息中心功能，管理员员可以通过消息中心发布维护任务，或者接收系统关键事件提醒，方便管理人员对信息系统运维状态进行。

## 5.8.高度安全保障能力

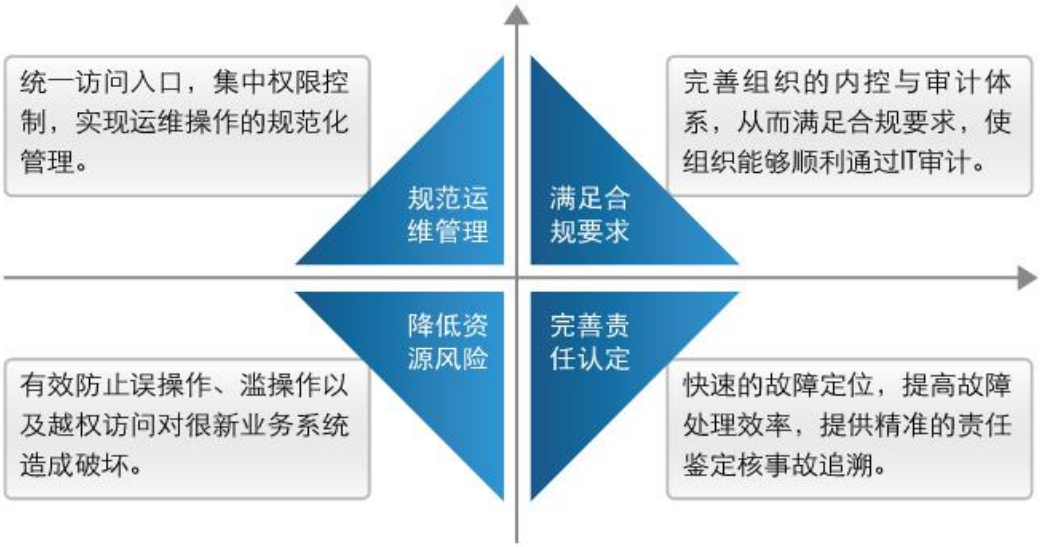
知道创宇运维审计堡垒机系统系统通过多种技术手段来保障自身与审计数据的安全性。如：

- ✓ 存储空间采用 RAID 磁盘阵列，有效保护数据安全；
- ✓ Linux 安全优化内核，有效提升系统稳定性和可用性；
- ✓ 系统模块独立设计，互相不影响安全性；
- ✓ chroot 运行环境，确保系统不受模块影响；
- ✓ 数据防篡改、防删除设计；
- ✓ 严格的访问权限、审计权限控制体系；
- ✓ 运维用户虚拟化，不在运维系统中建立实际系统账号。

## 5.9.部署简单，使用方便

无需在服务器、网络设备上安装代理程序，不需要改变原有网络架构，只需知道创宇运维审计堡垒机系统系统与被管目标网络可达即可，保证了业务系统原有的安全性和整体架构，不会影响业务系统的性能和稳定。

# 6. 应用效果


统一访问入口，集中权限控制，实现运维操作的规范化管理。
规范运维管理
满足合规要求
完善组织的内控与审计体系，从而满足合规要求，使组织能够顺利通过IT审计。
降低资源风险
完善责任认定
有效防止误操作、滥操作以及越权访问对很新业务系统造成破坏。
快速的故障定位，提高故障处理效率，提供精准的责任鉴定核事故追溯。

# 7.总结

知道创宇运维审计堡垒机系统，能够对运维人员维护过程的全面跟踪、控制、记录、回放；支持细粒度配置运维人员的访问权限，实时阻断违规、越权的访问行为，同时提供维护人员操作的全过程的记录与报告；系统支持对加密与图形协议进行审计，消除了传统行为审计系统中的审计盲点，是 IT 系统内部控制最有力的支撑平台之一。