360 运维安全管理与审计系统

产品白皮书

2017 年 2 月

目 录

1. 产品概述

随着企业信息系统规模的不断扩大，业务范围的快速扩张，运维工作量也随之增多。在运维过程中存在事前身份不确定、授权不清晰，事中操作不透明、过程不可控，事后结果无法审计、责任不明确导致客户业务及运维服务面临安全风险。

360 运维安全管理与审计系统是针对政府、金融、医疗、电力、教育、能源、企业、军队、海关等重点行业客户推出的，主要解决事企业 IT 运维部门账号难管理，身份难识别，权限难控制，操作过程难监控，事件责任难定位等问题。360 运维安全管理与审计系统基于软硬件一体化设计，集账号、认证、授权、审计为一体的设计理念，实现对事企业 IT 中心的网络设备、数据库、安全设备、主机系统、中间件等资源统一运维管理和审计。对运维人员整个操作过程处于可管、可控、可见、可审的状态，为事企业 IT 中心运维构建一套事前预防、事中监控、事后审计完善的运维管理体系。

2. 产品特点

健全的账号生命周期管理

通过主从账号分离的方式来将账号与具体的自然人相关联。通过这种关联，可以实现多级的用户管理和细粒度的用户授权，并针对自然人的行为审计。

密码强度策略对主从账号密码强度进行监测，强制对密码强度进行修改至符合强度要求才可进行修改或登录。

360 运维安全管理与审计系统提供账号密码到期提醒功能，强制对密码到期的用户进行密码修改，结合密码强度实现定期对密码按照密码强度强制修改。

360 运维安全管理与审计系统可对用户帐号密码、资源帐号密码按照密码策略要求进行定期、定时自动变更密码，防止口令因为过于简单易于猜测而被破解

的隐患，从而提高企业内部管理的安全性，降低资源损失风险。

丰富多样的安全认证机制

为了方便运维人员维护管理范围内的所有系统，360 运维安全管理与审计系统为运维人员提供了运维账号（主账号）。由于运维账号下关联了运维人员权限范围内的所有系统账号密码，因此需要对该运维账号采取高强度的认证措施。360 运维安全管理与审计系统支持静态密码认证，在此基础上，通过 LADP 认证、AD 域认证、USBKEY 认证、Radius 认证、证书认证、短信认证、指纹认证、动态口令认证等双因素认证来提高认证的安全性和可靠性。

细粒度的访问授权与控制

360 运维安全管理与审计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。管理员可根据运维用户的实际权限，对其访问主机、使用的协议、目标系统账号设置细粒度的访问策略。支持指令（黑白名单）的访问控制，支持基于时间的访问控制，支持基于访问者 IP 的访问控制。对于敏感资产的访问和操作，可实现登录审批和高危指令审批。

监控与敏感过程回放

原有的运维操作是客户机直接通过 RDP、SSH/Telnet 协议直接访问目标服务器，360 运维安全管理与审计系统采用代理模式将原有 RDP、SSH/Telnet 协议进行中转，将原有的 RDP、SSH/Telnet 访问分解为客户机到堡垒机、堡垒机到目标服务器的两次访问，堡垒机从中进行代理中转。中转过程中会记录所有 RDP、SSH 协议全部数据流，作为监控和审计的原始记录。

这些原始记录以友好合理的回放方式进行展现。堡垒机将 RDP、SSH/Telnet 等协议进行解析，SSH/Telnet 协议解析出输入命令行和输出文本并可进行逐屏展示；RDP 协议进行解析后形成逐帧的操作画面、并将这些画面组成操作视频供进行展现。

性能资源弹性调度

360 运维安全管理与审计系统底层程序通过自动伸缩(AutoScaling)和定时器(Scheduler)自动化运维工具的合理配合，自动伸缩功能，通过监控告警服务做支撑，可以对多活集群、负载均衡、多条互联链路等功能设计为后面扩充更多的主机、调高带宽；当然也可以做下调，就是在访问量长期处于低谷的时候，可以自动减少资源使用，调低带宽。

成熟的高可用性机制

360 运维安全管理与审计系统采用双调度引擎，分别为访问服务调度引擎和会话服务调度引擎。

通过双调度引擎模块完美实现对所有页面、会话访问服务进行全方位智能负载均衡

为保证 360 运维安全管理与审计系统连接持续可用，包含了多活集群的概念。多活集群是指所有堡垒机系统都是激活状态的，因此它们能够在其他节点出现故障时快速接管它的负载。使用多活集群可以保证集群中使用多个活跃节点。同时根据企业用户被管理设备逐渐增长的情况，360 运维安全管理与审计系统多活集群软件可进行无限扩容，保障被管设备随服务器的递增，360 运维安全管理与审计系统随时进行线性提升。

3. 主要功能

SSO 单点登录

360 运维安全管理与审计系统提供了基于 B/S 和 C/S 的应用系统(可实现不同行业用户 C/S 架构系统的定制开发)。单点登录为具有多账号的用户提供了方便快捷的访问途经，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。

集中账号管理

360 运维安全管理与审计系统对所有服务器、网络设备账号的集中管理。可

以完成对账号整个生命周期的监控和管理，且降低了管理大量用户账号的难度和工作量。同时，通过统一的管理还能够发现账号中存在的安全隐患，并且制定统一的、标准的用户账号安全策略。单位可以实现将账号与具体的自然人相关联。

集中身份认证

360 运维安全管理与审计系统为用户提供统一的认证接口，支持多种认证方式。采用统一的认证接口不但便于对用户认证的管理，且系统具有灵活的定制接口，可以方便的与第三方 LDAP 认证服务器对接。能够采用更加安全的认证模式，提高认证的安全性和可靠性。

统一资源授权

360 运维安全管理与审计系统提供统一的界面，对相应用户、角色及行为和资源进行授权，系统不但能够授权用户可以通过什么角色访问资源这样基于应用边界的粗粒度授权，对某些应用还可以限制用户的操作，以及在什么时间进行操作等的细粒度授权，最大限度保护用户资源的安全。

集中访问控制

360 运维安全管理与审计系统能够提供细粒度的访问控制，最大限度保护用户资源的安全。细粒度的命令策略是命令的集合，用来分配给具体的用户限制其系统行为，管理员根据其自身的角色为其指定相应的控制策略来限定用户，真正做到 who、where、when、what。然而更好的提高系统的安全性。

集中操作审计

操作审计管理分为内部审计和行为审计，内部审计针对堡垒机自身的操作情况的审计。行为审计主要针对操作人员的账号使用（登录、资源访问）情况、资源使用情况等。在各服务器主机、网络设备的访问日志记录都采用统一的账号、资源进行标识后，操作审计能更好地对账号的完整使用过程进行追踪。生成的日志支持丰富的查询和操作方式。

4. 核心功能列表

功能项	描述（特点）
单点登录	支持全局和局部的单点超时和登录超时设置；支持 ssh 实现公钥认证单点登录功能；
一键单点	对 ssh 协议可进行所有该协议的一键单点和勾选一键单点，实现在运维过程中进行批量的设备运维，方便使用
离线登录	支持 RDP 访问通过本地 mstsc 实现菜单模式的单点；支持 ssh、telnet 的直连模式和菜单模式的单点；支持 ftp 的菜单模式的单点；支持 sftp 的直连模式单点；
快速管理与添加用户	支持快速添加用户。支持将用户进行组的划分。支持用户的批量导入导出为.xls 格式的功能。
角色授权按部门管理	支持按照各部门管理各自资源自定义编辑和创建相对应的角色。
快速管理与添加资源	支持资源按时间、ip 列表排序。支持资源的分组管理。支持资源的批量导入导出为.xls 格式功能。
资产扫描	支持根据 ip 和网段进行目标资产的自动发现及所开放的端口，并且可以实现一键导入。
密码信封安全管理	支持将密码信封以加密方式导出.zip、.xls 格式的功能，支持每日定期自动备份密码信封功能。也可通过邮件以 txt、zip、xls 格式发送，也可通过 ftp 自动加密外发密码信封。
方便快捷的授权管理	支持细粒度授权，可以按照用户/组与资源/组进行关联。
临时授权的申请和审批	可以申请和审批临时授权信息，限制用户对资源的操作行为，操作时间。支持该功能在界面的开启和关闭。支持通过邮件、短信方式进行授权和审批。
二次申请和审批	支持对重要资源的二次申请功能。支持该功能在 web 界面的开启和关闭。
行为审计及指令搜索	可以对各种资源设备的访问进行回放审计，及键盘鼠标指令，内容的记录。支持实时监控和自动阻断。支持指令搜索标红显示。
多格式，多样式的组态报表显示	支持按照用户需求自定义报表格式。支持定时报表。支持报表统计以扇形、折现、柱形等多种形式展示，可导出 pdf、xls、csv、doc、txt、html 等多种格式的报表。

自动执行脚本	支持对于经常操作的指令集，通过上传脚本由运维审计系统定期代替自动执行。
定期自动改密和账号同步	支持对资源账号的定期自动同步和密码的更改，windows 改密支持通过 ssh、telnet、agent、AD 域数字证书方式进行。
磁盘使用告警	支持磁盘临界点告警。可启用审计日志将数据外置，可以以 ftp/sftp 方式选择性或者全部导出审计日志，界面可以直观查看导出的数量及进度等详情。
应用发布服务器的更新	支持对 netterm 软件、CRT 软件、TN5250、DB2 软件的调用。
FTP\SFTP 文件上传防病毒处理	对 FTP、SFTP 对重要服务器进行上传文件时，进行防病毒处理，避免因上传文件造成风险
多种单一和组合的认证方式	支持数字证书、key、动态令牌、AD、RADIUS、静态口令，自身证书认证功能等多种认证方式，可与认证服务器进行联动，实现双因素及多因素认证。

5.产品价值

规范运维管理

规范运维账号授权管理流程，统一访问入口的途径，让账号管理更加简单有序。

降低资源风险

有效阻止误操作，滥操作，以及越权访问造成系统破坏，保障企业效益。

提高管理效益

简化运维人员对账号、密码记忆难度及操作过程，有效提升企业 IT 管理效益。

过程透明可控

操作过程同步监控，对异常、高风险动作实时阻断，保障企业安全性。

完善责任认定

提供详细的运维审计分析报告，能精准的责任鉴定和事件追溯。

满足各组织合规要求

完善各行业组织的内控和审计体系，提供合规审计报告，使组织能顺利通过 IT 内审。