派拉 IT 运维安全管理软件
ParaSecure OSC V4.6
技术白皮书

上海派拉软件股份有限公司

www.paraview.cn

1 产品背景 3

2 产品概述 5

3 产品功能 7

3.1 集中账号管理 8
3.2 统一认证管理 8
3.3 单点登录 8
3.4 统一授权管理 9
3.5 访问控制 9
3.6 操作会同管理 10
3.7 实时监控与阻断 10
3.8 集中审计管理 10

4 系统部署 11

5 系统特点 12

5.1 良好的扩展性 12
5.2 强大的审计功能 12
5.3 部署简单、使用快捷 12
5.4 安全成熟 13

1 产品背景

目前 IT 基础架构的运行维护中普遍存在交叉管理、多途径维护和外包等现象，这些势必增加了 IT 操作风险。具体表现在：服务器管理方面、用户操作方面、非法攻击等各个方面。

1）账号管理混乱

- 信息化的 IT 支撑系统中部署了大量的网络设备、主机系统和应用系统，分别属于不同的部门和不同的业务系统，各应用系统都有一套独立的账号体系，用户为了方便登陆，经常会出现多人共用账号的情况。
- 多人同时使用一个系统账号在带来方便性的同时，直接导致无法确定用户身份的唯一性。如果其中任何一个人离职或者将账号告诉其他无关人员，会使这个账号的安全无法保证。
- 由于共享账号是多人共同使用，发生问题后，无法准确定位恶意操作或误操作的责任人。而更改密码则必须通知到每一个需要使用此账号的人员，增加了密码管理的复杂性。
- 企业信息中心有大量的网络设备、主机系统和应用系统。通常情况下，一次运维操作需要在多个被管设备之间来回跳转，需要多次输入密码，这一方面造成运维管理效率低下，另一方面，容易让管理员为全部系统账号设置同样的密码或者低强度密码。为系统留下了严重的安全隐患

2）密码策略无法有效执行

为了保证密码的安全性，安全管理员制定了严格的密码策略，比如密码要定期修改，密码 要保证足够的长度和复杂度等，但是由于管理的机器数量和账号数量太多，且用户经常需要在各系统间切换，为不影响工作效率，往往导致密码策略的实施流于形式。或者多台设备设置相同的密码，或者干脆把所有密码以明文的形式记录在某个文档中，这都给密码的安全性带来了威胁。

3）身份鉴别机制不强

很多企业或组织为了保护重要系统的安全，实施了双人分段管理密码、操作系统与数据库管理人员的权限分离、禁止混岗等策略，但实际工作中难免有工作或账户使用交叉情况出现，存在着无法对自然人身份的强制识别和认证风险。

4）授权关系不清晰

各部门分别管理所属的系统资源，为本部门的用户分配权限，往往无法准确分配用户权限并且一般只授权到设备级。另外，随着用户数量的增加，资源及权限网络会日趋复杂，权限管理任务越来越繁重。当维护人员同时对多个系统进行维护时，工作复杂度会成倍增加，而安全性也无法得到充分保证。

5）访问控制不严格

- 目前的管理中，没有一个清晰的访问控制列表，无法一目了然的看到什么用户能够以何种身份访问哪些关键设备，同时缺少有效的技术手段来保证访问控制策略被有效执行。
- 由于生产的特殊性，常常需要用户具有 ROOT 账户权限。这就造成生产和管理的矛盾，临时 ROOT 权限分发可以解决 ROOT 权限生产问题，但是，这极大增大管理的复杂性和不安全性，稍有疏忽，就可能造成管理的混乱。不分发 ROOT 权限，可能导致生产不能正常进行，至少影响生产效率。

6）用户操作无法有效审计

- 各系统独立运行、维护和管理，所以各系统的审计也是相互独立的。每个网络设备，每个主机系统分别进行审计，安全事故发生后需要排查各系统的日志，但是往往日志找到了，也不能最终定位到行为人，只能定位到某个系统中的用户而不是运维人员即无法进行实名制审计。
- 随着越来越多的企业将非核心业务系统交给第三方厂商进行开发和运维，而代维厂商人员流动较大，如何对这部分人进行有效地监管，防患于未然显得日益重要。
- 无法记录操作人员、操作时间、操作结果等
- root 用户不仅仅可以修改自己的历史记录，还可以修改他人的历史记录，系统本身的历史记录文件已经变的不可信

另外各系统的日志记录能力各不相同，例如对于 Unix 系统来说，日志记录的命令数量有限制

7）法律法规压力

对于公司而言，越来越多的政策法规对安全提出了具体明确的要求。例如国外萨班斯法案（SOX）404条款，对信息内控提出明确要求，其中安全占据重要地位，特别是对安全日志、账号口令的流程管理和审计管理，给用户带来大量管理工作，需要自动化系统能够有效对这些控制和管理进行支撑。

我国公安部及相关行业也相继推出了数十部法律法规。如：

- 国家《计算机信息系统安全等级保护划分准则》
- 2007年公安部、国家保密局、国家密码管理局、国务院信息工作办公室颁布了《信息安全等级保护管理办法》
- **金融行业：**《商业银行内部控制指引》、《商业银行操作风险管理指引》、《电子银行业务管理办法》、《银行业金融机构信息系统风险管理指引》、《商业银行合规风险管理指引》、《中国银行业监督委员会办公厅文件银监办通313号》、《保险公司内部审计指引（试行）》、《保险公司风险管理指引（试行）》、《深圳证卷交易所上市公司内部控制指引》、《上海证卷交易所上市公司内部控制指引》等。
- **ISO27001标准：**

条款A10.10.1要求组织必须记录用户访问、意外和信息安全事件的日志，并保留一定期限，以便为安全事件的调查和取证

条款A10.10.4要求组织必须记录系统管理和维护人员的操作行为

条款A15.1.3明确要求必须保护组织的运行记录

- **CC标准信息技术通用评估准则**（Common Criteria for Information Technology Security Evaluation）中信息技术通用评估准则：安全审计是其安全功能要求中最重要的组成部分，同时也是信息系统安全体系中必备的一个措施，它是评判一个系统是否真正安全的重要尺码
- **政府：**《政府部门信息技术外包服务机构申请信息安全管理体系认证安全审查程序》（暂行），该文是《关于鼓励政府和企业发包促进我国服务外包产业发展的指导意见》和《关于境内企业承接服务外包业务信息保护的若干规定》等

这些法律法规明确提出了信息安全的重要性。

2 产品概述

IT运维安全管理系统构建了一个统一的安全管理平台，集中解决AIX、Unix、Linux、Windows、Solaris 、AS/400等操作系统，以及数据库(包含DB2、Oracle、Sybase、Informix、MySQL、MS SQL等)、网络设备(交换机、路由器等)的账号集中管理、集中授权、集中认证和集中审计。

主要目标如下：

- **账号集中管理：**主要实现对操作系统、数据库、网络设备等各种 IT 资源的账号、认证、授权和审计的集中控制和管理。有效地保障业务支撑系统安全可靠地运行。为业务支撑系统提供机制统一、多样化的认证与授权安全服务，实现平滑过渡并实现与其他统一安全管理平台之间的数据交互。

- **密码集中管理：**主要实现对操作系统、数据库、网络设备等各种 IT 资源的账号密码进行集中存储，设定特权账号密码自动修改时间、密码信函打印、密码导出、密码策略设置等。

- **细粒度权限分配：**主要实现集中化、基于角色的主从账号管理。自然人与其拥有的主账号关联，统一规划用户身份信息和角色，对不同系统中的账号进行创建、分配、同步，最终建立业务支撑系统中自然人的单一视图（主账号管理）、建立业务支撑系统中资源的单一视图（从账号管理）。
- **层级审批：**主要实现可视化、集中化的审批流程引擎。自然人通过申请资源设备账号，并得到领导的同意，方可使用特权账号，做到领导可放、可收。
- **单点登录和统一认证：**单点登录主要体现在用户只需要记住一个主账号，可自动实现单点登录访问有权限访问的资源，且客户端无需安装任何客户端工具，这样便统一了登录的入口。另外根据安全需要选择不同的身份认证方式，在不更改或只对应用进行有限更改的情况下，即可在原来只有弱身份认证手段的应用上，增加强身份认证手段。**认证方式主要包含：RSA、CA证书、PKI、Ukey、短消息、AD域等。**

- **访问控制：**基于集中资源访问策略、用户访问策略和角色的授权管理。对用户使用业务支撑系统中资源的具体情况进行合理分配，实现不同用户对不同部分实体资源的访问。最终建立完善的资源对自然人的授权管理。**主要包含有两种范围大小的限定，大的范围可通过设定全局控制，主要是对客户端 IP、限制命令、可访问周期、可访问协议进行限定；小范围可限定申请人使用特权账号的周期。当周期结束，系统将强制退出。**

- **集中审计：**主要实现集中安全审计管理，收集、记录用户对业务支撑系统关键重要资源的使用情况。**主要表现形式有：字符审计、图形化审计等；主要审计内容有：管理审计、操作行为审计、访问审计(字符审计、视频审计)、密码审计等；主要保存形式有：PDF、Excel、密码信封等。**

3 产品功能

系统功能图：

说明：

① 展现层：提供统一的 Web 访问入口，用户无需再安装客户端工具。

② 核心业务层：划分为身份管理、账号管理、密码管理、授权管理、流程管理、审计管理 6 大功能模块

③ 基础结构：提供国密标准 SM4 及国外 AES256 加解密算法。提供双因素动态口令强认证、Windows AD 域认证、静态口令等多种认证方式进行强认证。

④ 提供对外标准的 Webservice 接口

3.1集中账号管理

集中账号管理包含对所有服务器、数据库、网络设备、中间件账号的集中管理。账号和资源的集中管理是集中授权、认证和审计的基础。集中账号管理可以完成对账号整个生命周期的监控和管理，而且降低了设备管理员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。

通过建立集中账号管理，可实现账号与实际自然人相关联。通过这种关联，可实现多级的用户管理和细粒度的用户授权。而且，还可以实现针对自然人的实名行为审计，真正满足审计的需要。

IT 运维管理系统可以实现对企业内网原有设备实现账号权限发布、回收等功能，方便管理员集中管理和分配内网资源。

3.2统一认证管理

IT 运维安全管理系统平台为用户提供统一的认证接口。采用统一的认证接口不但便于对用户认证管理，而且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。

系统自身是经过加固的可防御进攻的安全设备，支持 Windows AD 域、RSA 双因素动态口令、一次性口令、CA 证书、KEY、数字证书认证、生物特征认证等多种组合认证方式；并且传输过程加密。

而且系统具有灵活的定制接口，可以方便的与第三方认证服务器对接。

3.3单点登录

系统提供了基于 B/S 的单点登录和本地字符工具，如 SecureCRT、putty 等 C/S 的单点登录，同时支持基于 SecureCRT 工具的 ssh 会话多开。运维人员通过一次登录，就可以访问被授权的多个主机系统或设备。单点登录为在整个 IT 系统中具有多账号的用户提供了方便快捷的访问途径，使用户无需记忆多个登录账号 ID 和口令，而且访问不同系统不用重复登录，提高了

运维的效率。同时，集中的单点登录便于全系统采用强认证，从而提高了用户认证环节的安全性。

单点登录可以实现与用户授权管理的无缝链接，可以通过对用户、角色、行为和资源的授权，增加对资源的保护和对用户行为的监控及审计。

3.4统一授权管理

系统提供统一的界面，对用户、角色与行为、资源进行关联授权，以达到对权限的细粒度分配，最大限度保护 IT 资源的安全。通过集中访问授权和访问控制可以对用户通过 B/S、C/S 对服务器主机、网络设备的访问进行审计和阻断。

在集中访问授权里强调的“集中”是逻辑上的集中，而不是物理上的集中。即在各网络设备、服务器主机系统中可能拥有各自的权限管理功能，管理员也由各自的归口管理部门委派，但是这些管理员在 IT 运维安全管理平台上，可以对各自的管理对象进行授权， 而不需要进入每一个被管理对象才能授权。 授权的对象包括用户、用户角色、资源和用户行为。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。

另外，在设备和账号上的管理方式采用分权分域模式进行管理，使得原有的运维管理分权制度保持不变，便于各类型或业务管理员进行设备和账号的管理，并减少对平台管理员的集中管理工作。

3.5访问控制

IT 运维安全管理系统平台系统能够提供细粒度的访问控制，最大限度保护 IT 资源的安全。细粒度的命令策略是命令的集合，提供基于黑白灰名单的命令清单配置，该命令策略可分配给运维自然人或后台设备，另外也可提供基于访问时间、访问地点、资源、系统账号、操作命令、自定义命令表达式、访问协议的强访问控制。通过对访问内容的监控和记录、对危险命令的过滤，实现内部访问的安全运作。

访问控制策略是保护系统安全性的重要环节，制定良好的访问控制策略能够有效提高系统的安全性。

3.6操作会同管理

IT 运维安全管理系统平台提供受管系统管理员 A 登录系统时必须由系统管理员 B 或其它有权限的用户审核会同登录。允许操作和复核在不同终端上进行，即变更操作人在 ECC-PC1 上进行操作，变更复核人可在 ECC-PC2 上观看操作过程。

3.7实时监控与阻断

IT 运维安全管理系统平台提供对运维人员实际操作的实时监控功能，审计员可以实时的监视运维人员的运维操作，如果发现运维人员存在不合规的操作，审计员有权限实现对当前会话的实时阻断。

另外，系统可提供与第三方监控平台进行对接，及时将告警信息进行短信或邮件发送。

3.8集中审计管理

操作审计功能主要审计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审计。

系统支持对如下协议进行审计：SSH1、SSH2、Telnet、FTP、SFTP、RDP 等。

系统通过系统自身的用户认证系统、用户授权系统，以及访问控制等详细记录整个会话过程中用户的全部行为，还可以将审计日志传送给第三方。

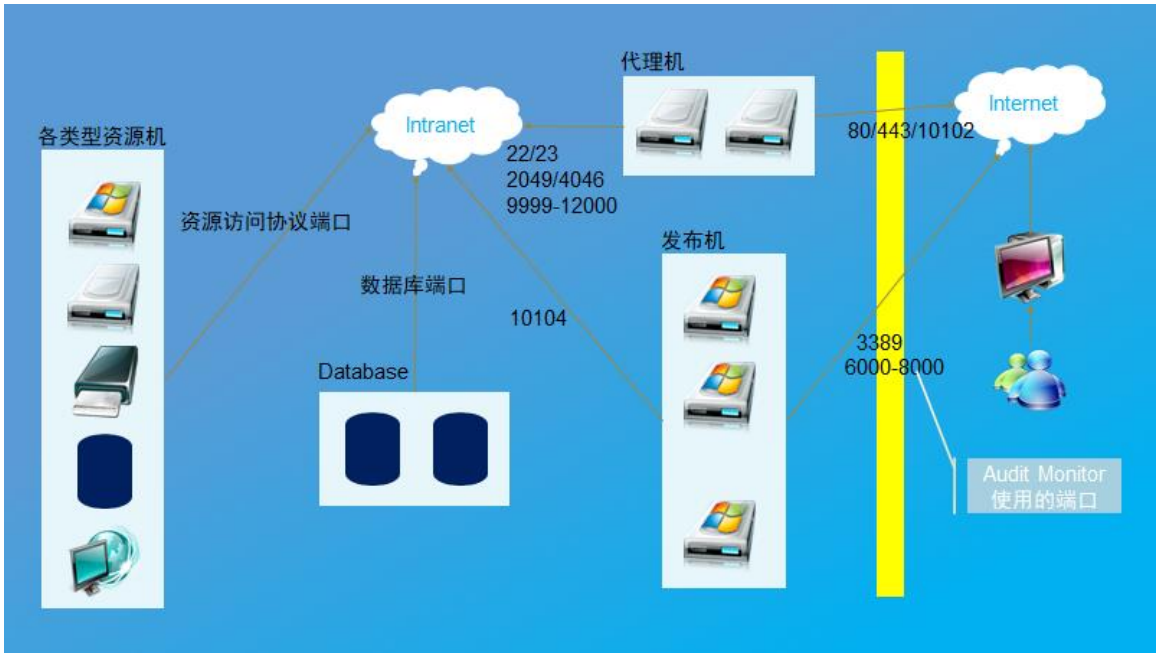
对于审计日志支持丰富的查询和操作，主要体现如下：

- 支持按设备或服务器方式进行查询：以 IP 地址为检索条件。
- 支持按用户名方式进行查询：以实际运维用户名为检索条件。
- 支持按登陆地址方式进行查询：以运维客户端 IP 地址为检索条件。
- 支持按照登陆时间进行查询：以登录时间为检索条件。
- 支持对命令发生时间进行查询：以运维具体时间为检索条件。
- 支持对命令名称进行查询：以特定命令为检索条件。

- 支持上述六个查询条件的任意组合查询：如：可以查询"谁（用户名）""什么时间登录（登录时间）"服务器并在"什么时间（命令发生时间）"在"服务器（目标服务器）"上执行过"什么操作（命令）"。
- 支持对日志的备份操作处理
- 提供图形审计、字符审计两种展现方式
- 系统具有灵活的日志检索方式，能够以时间、用户、操作命令、目标系统等字段检索日志和录像信息；能够以与、或、非等操作设置复杂的查询条件；相关查询结果能够以一定的格式批量导出
- 系统具有较高的视频检索和审计效率，针对字符界面的访问会话，能够通过字符快速定位和检索相应的视频录像

4 系统部署

鉴于企业网络及管理架构的复杂性，系统提供了灵活的部署方式，既可以采取纯内网部署模式，也可以采用内外网结合部署方式。部署时不改变网络拓扑，安装调试过程简单，可按照企业网络架构的实际情况灵活接入。



图：部署图

5 系统特点

5.1 良好的扩展性

系统从 4A 解决方案中抽象出来，提供最便捷的 4A 项目集成方案。在程序结构上充分考虑到 4A 项目和非 4A 项目的使用场景，以先进的体系结构，清晰合理的模块划分适用多种用户场景。在 4A 项目中，IT 运维安全管理系统继承 4A 方案中的账号、认证、授权的集中管理，本身提供执行单元，完成访问控制和操作审计功能；在非 4A 项目中则将 4A 的一些理念融合到产品中，除提供基础的访问控制和操作审计功能外，还提供精简的账号、认证、授权、特权、邮件、短信网关集中管理功能。

5.2强大的审计功能

精确记录用户操作时间。

审计结果对于用户的字符命令及键盘操作可以进行详细记录。

审计结果可以录像回放，支持调节播放速度，并且回放过程中支持前后拖拽，方便快速定位问题操作。

审计功能支持审计员对用户的操作行为进行实时监控，并可以对非法用户实现实时阻断。

方便的审计查询功能，支持按照多种组合条件查询，并能够一次查询多条指令。

审计表现形式多样化：字符、图形、定位回放、定位搜索等。

5.3部署简单、使用快捷

不需要在被管理设备上安装代理程序。

采用旁路部署方式，不需要改变网络的物理拓扑结构。

不影响被管理设备的运行。

管理员和操作员都使用 WEB 方式操作，操作简单直观。

5.4安全成熟

系统运用了先进的加密、过滤、备份、数字签名与身份认证、权限管理等安全手段，建立健全的系统安全机制，保证了用户的合法性和数据的安全性，从而保证产品的运维安全。

方案成熟，在大型公司有成熟应用案例。如：

零售行业代表：家乐福；

金融行业代表：中行银行；

制作行业代表：上海大众；

教育行业代表：上海电教馆；

电信行业代表：天翼视讯

政府行业代表：上海浦东软件园