运维审计系统

产品白皮书

杭州融至兴科技有限公司

二〇二三年五月

目录

[【第1部分】 概述 1](#_Toc134718381)

[1.1 背景介绍 1](#_Toc134718382)

[1.2 发展现状 1](#_Toc134718383)

[1.2.1 账号共享 1](#_Toc134718384)

[1.2.2 授权不清 2](#_Toc134718385)

[1.2.3 缺乏审计 2](#_Toc134718386)

[1.2.4 代维人员 2](#_Toc134718387)

[1.2.5 法规遵从 2](#_Toc134718388)

[【第2部分】 堡垒机产品介绍 4](#_Toc134718389)

[2.1 产品介绍 4](#_Toc134718390)

[2.2 产品定位 4](#_Toc134718391)

[2.3 应用环境 4](#_Toc134718392)

[2.4 产品设计 4](#_Toc134718393)

[2.4.1 网络结构图 4](#_Toc134718394)

[2.4.2 系统结构图 5](#_Toc134718395)

[2.4.3 系统技术架构 5](#_Toc134718396)

[2.4.4 管控对象 6](#_Toc134718397)

[2.4.5 支持协议类型 6](#_Toc134718398)

[2.5 关键技术应用 6](#_Toc134718399)

[2.5.1 逻辑命名自动识别技术 6](#_Toc134718400)

[2.5.2 分布式处理技术 7](#_Toc134718401)

[2.5.3 图形协议代理 7](#_Toc134718402)

[2.5.4 数据加密技术 7](#_Toc134718403)

[2.5.5 操作还原技术 7](#_Toc134718404)

[2.5.6 动态口令技术 7](#_Toc134718405)

[2.6 产品功能 9](#_Toc134718406)

[2.6.1 集中账号管理 9](#_Toc134718407)

[2.6.2 身份认证 9](#_Toc134718408)

[2.6.3 资源授权 9](#_Toc134718409)

[2.6.4 访问控制 10](#_Toc134718410)

[2.6.5 操作审计 10](#_Toc134718411)

[2.6.6 web终端可视化文件操作 10](#_Toc134718412)

[2.7 产品优势 10](#_Toc134718413)

[2.7.1 审计信息“零管理” 10](#_Toc134718414)

[2.7.2 强大丰富的管理能力 11](#_Toc134718415)

[2.7.3 方便灵活的可扩展性 11](#_Toc134718416)

[2.7.4 高可靠的自身安全性 11](#_Toc134718417)

[2.7.5 部署方式灵活性 11](#_Toc134718418)

[2.7.6 操作使用便捷性 11](#_Toc134718419)

[2.8 产品效益 11](#_Toc134718420)

[2.8.1 登录完善内控内审，满足合规要求 11](#_Toc134718421)

[2.8.2 简化运维管理，提高运维效率 12](#_Toc134718422)

[2.8.3 控制运维风险，防止数据泄露 12](#_Toc134718423)

[2.9 运维实施 13](#_Toc134718424)

[2.9.1 部署方式 13](#_Toc134718425)

# 

# 概述

## 背景介绍

我国经济的高速发展为信息化建设带来了源源不断的动力，现阶段各行各业无不在信息资产方面增加投入，以确保基础网络、业务系统、数据资产和信息安全方面的需要。高效的信息系统提升了企业的管理水平，提高了工作效率，同时也带来了经济效益。但与此同时，如何维护数量众多的信息资产，让它们健康有序运行，正在引起企业信息部门的关注。信息化建设的重点已经由原来的基础建设向深化应用、安全运维方面发生转变。

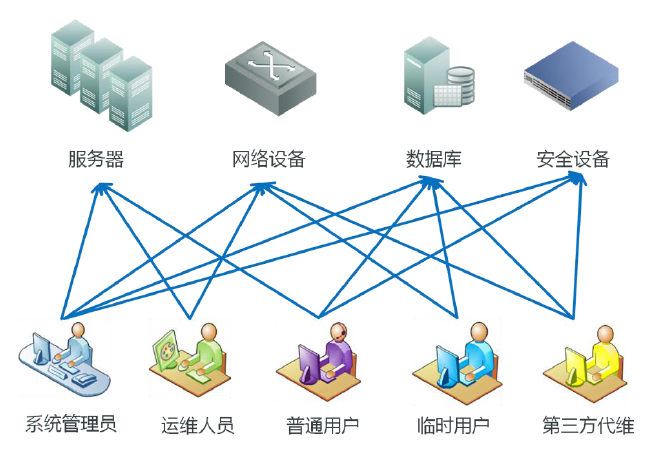
随着防火墙、入侵防御系统（IPS）等安全产品的广泛使用，网络已经具备了抵抗外部入侵的能力，但堡垒往往是在内部被攻破的

由于设备和服务器众多，账号管理混乱，授权不清、各种越权访问、误操作、滥用、恶意破坏等情况时有发生。据资料统计，在对网络造成严重损害的案例中，有70％是组织里的内部人员所为。如何提高系统运维管理水平，满足IT内控法规遵循的要求，提供控制和审计依据，降低人为安全风险，满足企业要求，是当下所面临的迫切需求。

## 发展现状

### 账号共享

为了方便登录，经常出现多人共用账号的情况。多人共享账号在带来方便的同时，导致用户身份的唯一性无法确定。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。更改密码需要通知到每一个需要使用此账号的人员，带来了密码管理的复杂性。

如下图所示，账号共享或一人使用多个账号会导致整个运维管理过程的复杂混乱。由于整个运维过程的不定因素太多，使得整个运维过程不可控。不仅仅给运维人员带来了巨大的麻烦，而且让管理人员也无法准确的定位责任人，如果长期在这种传统的模式下运维，将会给企业带来巨大的损失，甚至还无法追究责任。所以我们要建立新的运维模式和运维理念。 

### 授权不清

在传统的运维模式中，授权是不清晰的，例如：运维人员登录某台服务器或者某个核心交换机等关键设备的时候，他将拥有很大的权限，同时他也可以做一些越权的操作，比如是重启或是其他的敏感操作。也许他的操作是无意的，但都将引发不可估量或者无法挽回的后果。

### 缺乏审计

在传统运维模式下，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。

### 代维人员

目前，越来越多的企业选择将非核心业务外包给设备商或代维公司，企业在享受便利的同时，同时也带来了更多的问题：代维人员流动性大、缺少操作行为监控、第三方代维人员的权限过大等等，这些问题带来的风险日益凸现。

### 法规遵从

为加强信息系统风险管理，政府、金融、运营商等陆续发布信息系统管理规范和要求，如“信息系统等级保护”、“商业银行信息科技风险管理指引”、“企业内部控制基本规范”等均要求采取信息系统风险内控与审计，但很多企业并没有明确有效的技术手段来达到或满足这些要求。

# 堡垒机产品介绍

## 产品介绍

为满足用户对加强内部运维安全日益迫切的需要，融至兴依托自身强大的研发能力，丰富的行业经验，自主研发的新一代安全运维系统，能够对运维人员维护过程进行全面跟踪、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。对运维过程三个阶段进行严格管控：事前预防：建立“自然人-资源-资源账号”关系，实现统一认证和授权；

事中控制：建立“自然人-操作-资源”关系，实现操作审计和控制；

事后审计：建立“自然人-资源-审计日志”关系，实现事后溯源和责任界定。

## 产品定位

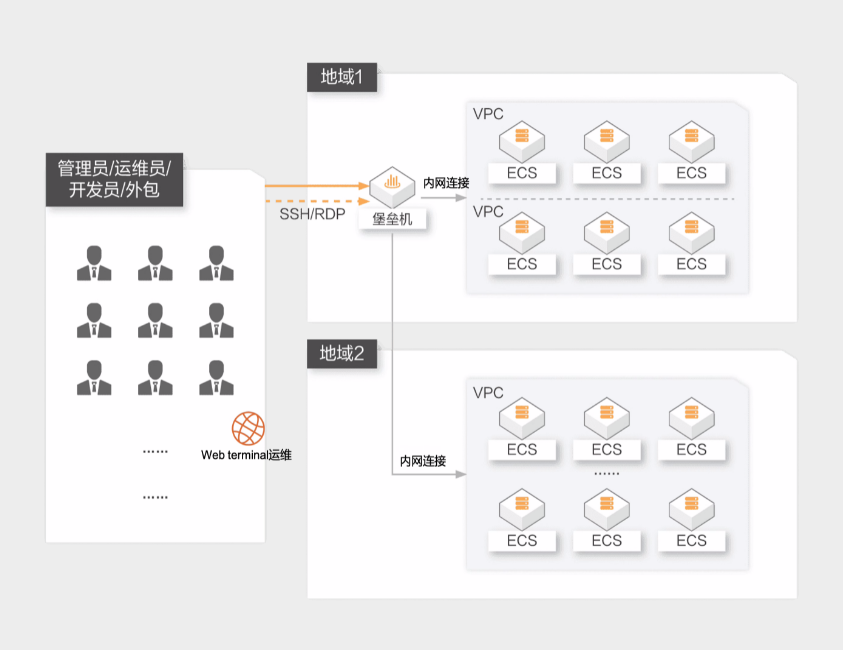
1. 融至兴堡垒机为企业IT资产提供运维审计服务，为客户构建一套完善的事前预防、事中监控、事后审计安全管理体系，助力企业顺利通过等保测评。
2. 适用对象：可广泛应用于金融、政府、电信、证券、邮政、税务、海关、交通等安全需求较高的行业。

## 应用环境

支持Telnet、FTP、SSH、SFTP、RDP ( Windows Terminal )、HTTP、HTTPS等多种通信协议，支持通过应用发布方式实现对B/S、C/S运维管理工具统一管理；支持常用浏览器，360浏览器/Chrome/Firefox/ie10。

## 产品设计

### 网络结构图



### 系统结构图



### 系统技术架构

统一安全运维平台通过“物理旁路，逻辑串联”的方式完成部署（也可以采用直通模式），建立集中的运维操作监控平台，建立基于唯一身份标识的实名制管理，统一账号管理策略。通过集中访问控制与授权，实现单点登录（SS0）和细粒度的命令集访问授权。基于用户的审计将直接审计到人，实现从登录到退出的全过程操作行为审计，满足合规管理和审计要求。

### 管控对象

|  |  |
| --- | --- |
| 用户 | 管理人员、运维人员、代维人员（第三方） |
| 资产 | 服务器（Unix/Linux/Windows）、网络设备、安全设备 |

### 支持协议类型

|  |  |
| --- | --- |
| 字符型协议 | SSH、Telnet |
| 图形协议 | RDP |
| 文件传输协议 | FTP、SFTP、SCP |
| 其他协议 | http、https |

## 关键技术应用

### 逻辑命名自动识别技术

自动识别当前操作终端，对当前终端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。该技术能自动识别命令状态和编辑状态以及私有工作状态，准确捕获逻辑命令。

### 分布式处理技术

采用分布式处理架构进行处理，启用命令捕获引擎机制，通过策略服务器完成策略审计，通过日志服务器存储操作审计日志，并通过实时监视中心，实时察看用户在服务器上的行为。

这种分布式设计有利于策略的正确执行和操作记录日志的安全。同时，各组件之间采用安全连接进行通信，防止策略和日志被篡改。各组件可以独立工作，也可以分布于不同的服务器上，亦可将所有组件安装于一台服务器上。

### 图形协议代理

为了对图形终端操作行为进行审计和监控，对图形终端使用的协议进行代理，实现多平台的多种图形终端操作的审计，例如 Windows 平台的RDP方式图形终端操作，Linux/Unix平台的 XWindow方式图形终端操作。

### 数据加密技术

在处理用户数据时采用相应的数据加密技术来保护用户通信的安全性和数据的完整性，防止恶意用户截获和篡改数据，充分保护用户在操作过程中不被恶意破坏。

### 操作还原技术

操作还原技术是指将用户在系统中的操作行为在真实的环境中模拟显现出来，审计管理员可以根据操作还原技术还原出真实的操作，以判定问题出在哪里。采用操作还原技术能够将用户的操作流程自动地展现出来，能够监控用户的每一次行为，判定用户的行为是否对企业内部网络安全造成危害。

### 动态口令技术

运维审计系统往往具有SSO功能，这意味着只要取得了用户运维审计系统主账号，就可以登录到这个用户拥有权限的所有主机，因此，运维审计系统往往会成为一个安全的薄弱点。

与其它厂商运维审计产品不同，系统内置了具有自主产品的动态口令产品，而其它厂商都需要购买第三方厂商的动态口令产品才能实现对主账号的密码保护，相比之下，具有内置的动态口令系统可以有效的降低用户采购和管理成本，在一个系统中对所有用户和令牌进行管理，而不需要分别在一套系统中管理用户，另一套系统中管理用户和令牌。

## 产品功能

### 集中账号管理

集中账号管理包含对所有服务器、网络设备账号的集中管理。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，而且还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。

### 身份认证

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的管理，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。

### 用户分权管理

支持多种用户角色：超级管理员、部门管理员、配置管理员、审计管理员、运维员、审计员、系统管理员、密码管理员，每种用户角色的权限都不同，为用户设立不同的角色提供了选择，提供灵活的角色自定义能力。

### 统一运维管控

提供资产运维统一入口，实现所有运维行为的管控及审计，同时对跨账号、异构云、线下IDC混合场景下的LINUX/WINDOWS资产的运维行为实现一站式安全管控。

### 资源授权

提供统一的界面，对用户、角色及行为和资源进行授权，以达到对权限的细粒度控制，最大限度保护用户资源的安全。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。

### 访问控制

可以细粒度的给用户分组分权，如限制文件上传、下载、创建等，在最小化权限的基础上，实现最灵活配置控制。

### 操作审计

操作审计管理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。

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日志。

### web终端可视化文件操作

WEB终端链接已授权服务器后，支持可视化的对服务器内的文件进行增删改查下载等操作。

### 高危行为自动阻断

在恶意访问行为上，可以对敏感的高危命令，如删除数据（rm -rf /\*）、格式化等高度敏感操作进行实时自动阻断，防止重大误删事件发生。

## 产品优势

### 全面的资产管理

支持多云、线下资产的统一管理，支持主流的 Linux 操作系统、Windows 操作系统和 MySQL 数据库版本，有效辅助管理员进行安全运维

### 细粒度权限控制

支持基于用户、资产、账号、操作权限等维度进行细粒度授权，确保用户所拥有的权限是其访问资产、完成工作任务的最小化权限。

### 良好的运维体验

支持多种主流运维操作客户端工具，并且完美适配 Windows 和 MacOS 终端，运维过程当中，不改变运维人员原有的操作习惯。

### 统一运维入口

堡垒机作为统一的入口进行内部资产的管理和维护，用户无需记忆多个地址和多套账号密码。

### 强大丰富的管理能力

支持B/S管理方式，Web管理灵活方便，适合在任何IP可达地点远程管理。系统提供带外管理功能，解决远程应急管理的需求，减少用户运营成本、提高运营效率、减少宕机时间、提高服务质量。

### 操作使用便捷性

提供多种运维方式、C/S运维客户端、资源批量登录、命令批量执行、设备自动改密等多种功能以保证运维过程的自动和快捷性。

## 产品效益

### 登录完善内控内审，满足合规要求

目前，越来越多的单位面临一种或者几种合规性要求。堡垒机提供的完备审计方案，可以完善组织的IT内控与审计体系，从而满足各种合规性要求，并且使组织能够顺利通过IT审计。

### 简化运维管理，提高运维效率

堡垒机对账号和资产进行统一管理，规范简化运维流程。提供多种运维操作方式以满足各种不同使用习惯。自动便捷的使用体验提供整体运维效率。

### 控制运维风险，防止数据泄露

堡垒机基于统一认证、集中管理、规范运维操作行为，对运维操作和数据流转过程做到严格的控制和记录，最大程度控制运维风险。

## 运维实施

### 部署方式

将堡垒机连接到交换机，保证其IP可达。通过配置交换机或被管理设备的访问控制策略，仅使堡垒机的IP可以访问需要管理的设备。

