

绿盟运维安全管理系统 产品白皮书

【绿盟科技】



■ 版权声明

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属绿盟科技所有，受到有关产权及版权法保护。任何个人、机构未经绿盟科技的书面授权许可，不得以任何方式复制或引用本文的任何片断。

目录

一. 背景	1
1.1 运维账号混用， 粗放式权限管理	1
1.2 审计日志粒度粗， 易丢失， 难定位	2
1.3 面临法规遵从的压力.....	2
1.4 运维工作繁重枯燥.....	2
1.5 虚拟云技术蓬勃发展.....	3
二. 产品概述.....	3
2.1 运维安全管理系统.....	3
2.2 目标.....	3
2.3 应用场景.....	4
2.3.1 管理员制定运维管理策略	5
2.3.2 普通运维用户访问目标设备	6
2.4 系统价值.....	8
三. 产品介绍.....	8
3.1 系统功能.....	8
3.2 系统架构.....	9
四. 产品特性.....	11
4.1 多维度、细粒度的认证与授权体系	11
4.1.1 灵活的用户认证方式	11
4.1.2 细粒度的运维访问控制	11
4.1.3 多维度的运维访问授权	12
4.2 高效率、智能化的资产管理体​​系	12
4.2.1 智能化巡检托管设备和设备账号	13
4.2.2 高效率管理设备和设备账号	13
4.3 提供丰富多样的运维通道.....	14
4.3.1 B/S 下网页访问.....	14
4.3.2 C/S 下客户端访问.....	14
4.3.3 跨平台无缝管理	15
4.3.4 强大的应用扩展能力	15
4.4 高保真、易理解、快定位的审计效果	16
4.4.1 数据库操作图形与命令行级双层审计.....	16
4.4.2 基于唯一身份标识的审计	16
4.4.3 全程运维行为审计	17
4.4.4 审计信息“零管理”.....	17
4.4.5 文字搜索定位录像播放	18
4.5 稳定可靠的系统安全性保障	19

4.5.1 系统安全保障	19
4.5.2 数据安全保障	19
4.6 快速部署，简单易用.....	19
4.6.1 物理旁路，逻辑串联	19
4.6.2 配置向导功能	21
五. 客户收益.....	22

插图索引

图 1.1 用户与运维账号的关系现状.....	1
图 2.1 核心思路.....	4
图 2.2 运维管理员制定策略.....	5
图 2.3 普通用户访问目标设备.....	7
图 3.1 系统功能.....	9
图 3.2 系统架构.....	10
前置机架构示意图.....	15
图 4.1 数据库操作图形与命令行级双层审计	16
图 4.2 文字搜索定位录像播放.....	18
图 4.3 产品部署.....	20

一. 背景

随着信息化的发展，企事业单位 IT 系统不断发展，网络规模迅速扩大、设备数量激增，建设重点逐步从网络平台建设，转向以深化应用、提升效益为特征的运行维护阶段，IT 系统运维与安全管理正逐渐走向融合。信息系统的安全运行直接关系企业效益，构建一个强健的 IT 运维安全管理体系对企业信息化的发展至关重要，对运维的安全性提出了更高要求。

1.1 运维账号混用，粗放式权限管理

目前，一个维护人员使用多个账号，记忆多套口令，同时多套主机系统、网络设备直接切换的场景是较为普遍的情况。在同一工作组中，多用户共享同一系统管理账号进行运维操作也是十分普遍。因此，在发生安全事故时难以定位账号的实际使用者和责任人，而且无法对运维账号的使用范围进行有效控制，设备和运维账号管理存在安全隐患，特别是在以数据为主要业务的客户群体中，问题更为凸显。

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，在享受便利的同时，由于代维人员流动性大、对操作行为缺少监控带来的风险日益凸显。因此，需要通过严格的权限控制和操作行为审计，加强对代维人员的行为管理，从而达到消隐患、避风险的目的。

大多数企事业单位的 IT 运维均采用设备、操作系统自身的授权系统，授权功能分散在各设备和系统中。管理人员的权限大多是粗放式管理，由于缺少统一的运维操作授权策略，授权粒度粗，无法基于最小权限分配原则管理用户权限，难以与业务管理要求相协调。因此，出现运维人员权限过大、内部操作权限滥用等诸多问题，如果不及时解决，信息系统的安全性难以充分保证。

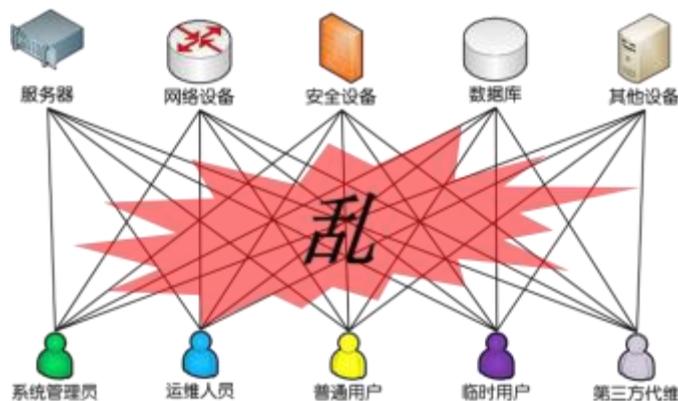


图 1.1 用户与运维账号的关系现状

1.2 审计日志粒度粗，易丢失，难定位

在运维工作中，大多是通过各网络设备、操作系统的系统日志进行监控审计，因此出现各系统自身审计日志分散、内容深浅不一，无法根据业务要求制定统一审计策略，容易被系统管理员权限用户删除，无法完整重现安全事件真实过程，最终导致难以通过系统自身审计及时发现违规操作行为和追查取证。

传统的旁路数据分析和主机探针审计方式，都存在着缺陷和不足。旁路数据分析审计无法对已加密的应用层数据（例如 SSH 和 SFTP 等）进行细粒度分析，无法对图形运维操作（例如 RDP，VNC 等）过程进行完整还原，特别是无法对图形内容的数据提取和分析；仅是记录运维 IP 地址信息是很难对安全事故进行定位和追责，为事后审计方式，无法做到实时管控；主机探针审计方式，在被托管主机上安装探针软件不仅占用宝贵的系统资源，并且对系统稳定性埋下隐患。不能对网络方式运维操作过程完整还原展示，能够做到实时管控，但事后审计能力不足。

1.3 面临法规遵从的压力

随着国家不断地投入信息化基础设施建设，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，但其自身却没有有效的技术手段。

1.4 运维工作繁重枯燥

一个运维管理员管理多台服务器的情况在运维工作中十分普遍，定期对服务器系统进行业务数据备份、补丁更新、设备账号改密等操作是日常工作内容，其中数据备份工作量大、设备账号改密量多等问题常常导致运维操作失误，效率低等现象，这严重影响企业的经济运行效能，并对企业声誉造成重大影响。

1.5 虚拟云技术蓬勃发展

自 SaaS 在 20 世纪 90 年代末出现以来，云计算服务经历了多年的发展历程，云环境下的信任问题日趋突出，多租户和用户下身份认证、权限控制，云主机系统运维和安全审计等种种问题都困扰着云服务厂商，也制约了云服务业务的发展。

二. 产品概述

2.1 运维安全管理系统

绿盟运维安全管理系统（简称堡垒机），是连接运维人员和目标设备系统之间安全可靠的“立交桥”，基于唯一身份标识的实名制管理机制，运维人员可以通过唯一身份标识“一卡通”对所有被托管的服务器进行访问运维，“立交桥”不但为运维人员提供便利的单点登录（SSO）通道，而且运维人员到堡垒机之间的访问数据均进行加密处理，保证“立交桥”上通行的数据安全，不会被窃听和篡改；

也是被托管设备服务器的安全守护神，智能可靠的设备托管平台，自动发现运维环境中的目标设备，智能管理被托管设备和设备账号，支持自动定期更新设备账号密码等操作，提高运维环境中目标设备管理效率，降低被托管设备非法访问风险；

更是 IT 运维管理的“天眼”，具备运维操作输入输出审计功能，不仅能够详细记录用户的每一条字符命令操作，而且还能够对图形终端操作进行记录和识别。在实时记录运维操作的过程中，还提供管理员用户对运维行为实时监管，包括但不限于智能阻断、实时告警、金库授权、主动切断会话等操作。

总的来说，绿盟运维安全管理系统为运维人员提供安全便利的通道，为管理人员提供专业合理的运维管理平台，助推企事业单位内控管理更上一层楼。

2.2 目标

绿盟运维安全管理系统（NSFOCUS Operation Security Management System，以下简称堡垒机或 OSMS）提供一套先进的运维安全管控与审计解决方案，目标是帮助企业转变传统 IT 安全运维被动响应的模式，建立面向用户的集中、主动的运维安全管控模式，降低人为风险，满足合规要求，保障企业效益。

绿盟堡垒机产品通过逻辑上将人与目标设备分离，建立“人->主账号（堡垒机用户账号）->授权->从账号（目标设备账号）->目标设备”的管理模式；在此模式下，通过基于唯一身份标识的集中账号与访问控制策略，与各服务器、网络设备、安全设备、数据库服务器等无缝连接，实现集中精细化运维操作管控与审计。

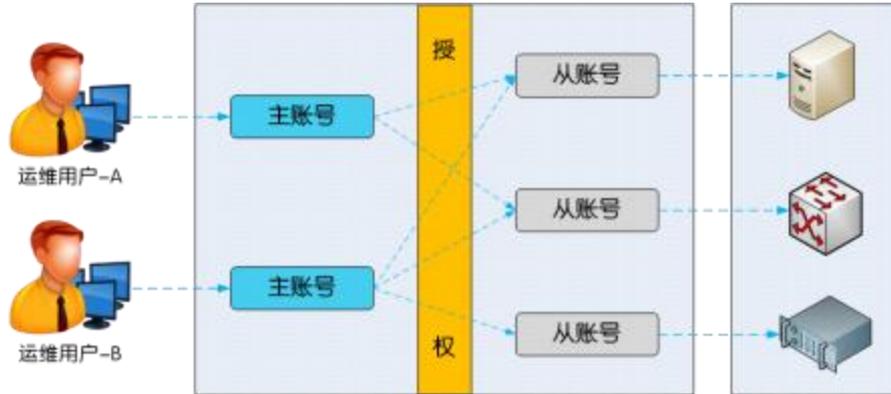


图 2.1 核心思路

2.3 应用场景

◆ 堡垒机产品主要应用于以下场景：

IT 运维的责任认定，远程接入办公/服务平台；

远程接入办公/服务平台；

第三方审计机构对运维行为审计；

企业整体应用交付；

数据库敏感数据防范；

运营商 4A 方案

◆ 管理对象

设备管理员、运维人员、第三方代维人员、审计员等。

服务器(Windows/Linux/UNIX)、网络设备、安全设备、数据库、WEB 服务器等。

◆ 管理范围

集中授权管控人员和设备，实时监控运维操作行为，事后审计管理操作。

◆ 可支持的协议/应用类型

SSH、Telnet、RDP、VNC、FTP、SFTP、HTTP、HTTPS、X11、KVM 等。

各类数据库客户端、浏览器、专有客户端工具等。

◆ 部署方式

堡垒机采用“物理旁路，逻辑串联”的部署思路，主要通过两步实现：

- 1) 通过配置交换机或目标设备的访问控制策略，只允许堡垒机的 IP 访问目标设备的运维、管理服务。
- 2) 将堡垒机连接到对应交换机，确保所有维护人员到堡垒机 IP 可达。

◆ 达成效果

- ✓ 建立智能可靠的设备托管平台，自动发现运维环境中的目标设备，智能管理被托管设备和设备账号，支持自动定期更新设备账号密码等操作，提高运维环境中目标设备管理效率，降低被托管设备非法访问风险；
- ✓ 建立基于唯一身份标识的实名制管理机制，灵活多样的身份管理策略，实现跨平台管理，消灭管理孤岛。
- ✓ 通过集中访问控制与授权，实现单点登录(SSO)和细粒度的命令级访问授权。
- ✓ 基于用户的审计，审计到人，实现从登录到退出的全程操作行为审计，满足合规管理和审计要求。

下面分别从堡垒机的运维管理员和普通用户的角度，介绍实现流程与效果：

2.3.1 管理员制定运维管理策略

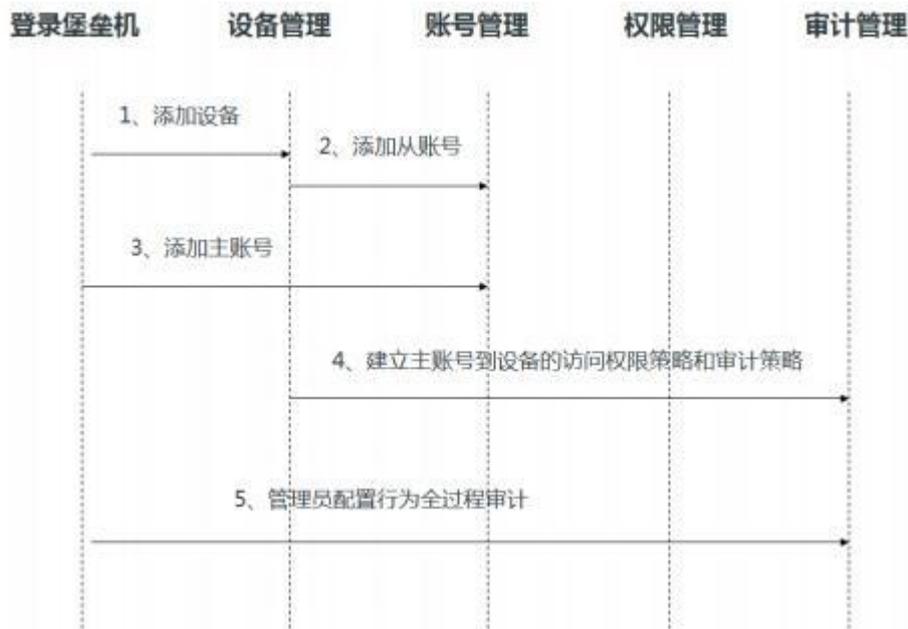


图 2.2 运维管理员制定策略

1. 添加设备

运维管理员添加需要管理的设备。设备包括服务器、网络设备、安全设备、前置机、数据库服务器等维护对象，支持编辑相关设备信息包括设备类型、所属部门、设备名称、IP地址、协议类型、应用程序等。

2. 添加从账号

管理员添加与设备对应的从账号（即设备的系统账号、数据库账号或WEB登录账号），包括账号名、口令等；其中口令可由堡垒机定期自动更新。

3. 添加主账号

管理员添加主账号（即普通运维用户账号）。主账号是登录堡垒机，获取目标设备访问权的唯一账号，与实际用户身份一一对应，每个用户一个主账号，每个主账号只属于一个用户。

4. 建立主账号到设备的访问控制与审计策略

基于访问权限策略，运维管理员建立基于“时间+主账号+目标设备+从账号+权限+审计”等要素的关联管理策略。

5. 管理员配置行为全程审计

堡垒机自动记录管理员的设备管理、账号管理和权限管理等所有行为日志，以便审计员监控。

2.3.2 普通运维用户访问目标设备

普通用户登录堡垒机后，可以实现下述功能：

- ④ 支持个性化参数配置和相关运维工具下载；
- ④ 多种交互方式、集中展示各类已授权设备资源，支持一键式快速登录目标设备运维；
- ④ 支持发起工单申请，申请更多的运维权限和资源。

具体实现流程如下：



图 2.3 普通用户访问目标设备

1. 登录请求

用户在终端通过 HTTPS 或第三方客户端工具登录堡垒机，输入主账号和口令，发起访问请求。

2. 登录认证

堡垒机的认证模块对用户的认证请求进行鉴别。

3. 检查主账号访问权限

认证成功之后，堡垒机的权限管理模块通过分析主账号属性（包括可访问的目标设备、访问权限、从账号、协议类型、应用程序等），确定主账号可访问的所有设备。

4. 显示可访问设备

直观地呈现出主账号可访问的所有目标设备。

5. 访问目标设备

用户选择需要访问的目标设备，进行操作维护。如果有违反访问控制策略的行为，堡垒机基于策略将自动记录、阻断及电邮通知管理员。

6. 返回访问结果

堡垒机将用户访问目标设备的所有操作执行结果，返回到用户终端。

7. 用户访问行为全程审计

堡垒机全程审计用户“登录堡垒机->目标设备访问操作->退出系统”的所有行为。

2.4 系统价值

绿盟运维安全管理系统为企业带来的价值主要体现在：

◆ 管理效益

- ✓ 所有运维账号在一个平台上进行管理，账号管理更加简单有序，并对其进行自动化运维，提高企业运行效率；
- ✓ 通过建立用户与账号的唯一对应关系，确保用户拥有的权限是完成任务所需的最小权限；
- ✓ 可视化运维行为监控，及时预警发现违规操作。

◆ 用户效益

运维人员只需记忆一个账号和口令，一次登录，便可实现对其所维护的多台设备的访问，提高工作效率，降低工作复杂度。

企业管理员轻松管理多台设备和运维人员，人员权限和设备资产信息清晰明了，提高管理效率而不失便利性。

◆ 企业效益

降低人为安全风险，提高托管设备和运维业务安全性，避免安全损失，满足合规要求，保障企业效益。

三. 产品介绍

3.1 系统功能

绿盟运维安全管理系统产品主要有三大功能：



图 3.1 系统功能

◆ 集中账号管理

建立基于唯一身份标识的全局实名制管理，支持统一账号管理策略，实现与各服务器、网络设备、安全设备、数据库服务器等无缝连接。

◆ 集中访问控制

通过集中访问控制和细粒度的命令级授权策略，基于最小权限原则，实现集中有序的运维操作管理，让正确的人做正确的事。

◆ 集中安全审计

基于唯一身份标识，通过对用户从登录到退出的全程操作行为进行审计，监控用户对目标设备的所有敏感操作，聚焦关键事件，实现对安全事件的实时发现与预警。

3.2 系统架构

绿盟运维安全管理系统系列由平台管理模块、功能管理模块和平台接口构成。总体架构如下图所示：

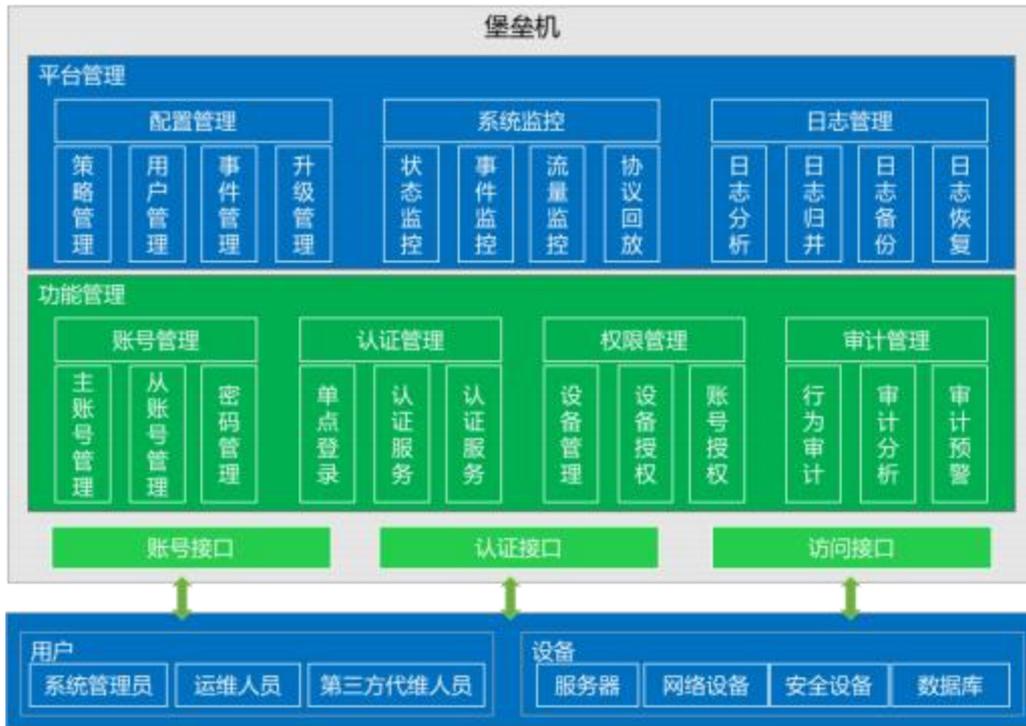


图 3.2 系统架构

1. 功能管理模块

提供账号管理功能、认证管理功能、权限管理功能和审计管理功能。

- 👉 账号管理：提供账号生命周期管理，包括账号创建、账号修改、状态调整、账号删除、账号查询等功能。
- 👉 认证管理：支持多种认证方式，包括本地认证、LDAP/RADIUS 认证。
- 👉 权限管理：提供基于时间、用户/用户组、设备/设备组、设备账号、命令关键字、危险级别等组合策略，授权用户可访问的目标设备及可使用的命令。
- 👉 审计管理：提供对用户通过堡垒机对目标设备的所有操作行为审计、事件查询分析和报表管理。

2. 平台管理

提供对堡垒机平台自身的管理，包括系统配置管理、系统监控及审计日志管理。

3. 平台接口

提供对用户（包括管理员、运维人员、代维人员等）、设备（包括服务器、网络设备、安全设备、数据库服务器等）的各种管理接口，包括设备导入接口、账号的同步和导入接口、认证接口、访问接口等。

3.3 系统性能

主要硬件标品参考性能参数

型号 主要参数	OSMSNX3- HD200	OSMSNX3- HD1000	OSMSNX3- HD2000	OSMSNX3- HD2200
外观规格	1U	1U	2U	2U
接口	标配：4*电口	标配：6*电口和4*光口		
	选配：4千兆电、8千兆电、4千兆光、8千兆光、4千兆电+4千兆光、2万兆光	选配：8千兆电、4千兆电+4千兆光、2万兆光、4万兆光		
SLOT插槽	1个	2个		
LED屏	N/A	N/A	支持	支持
缺省可设备管理数	25~200点	200~无限		
图形最大并发会话数	500	800	1000	1200
字符最大并发会话数	1000	1500	1800	2300
电源	交流单电源	交流冗余电源	交流冗余电源	交流冗余电源
额定功率	65W	300W	300W	300W

四. 产品特性

4.1 多维度、细粒度的认证与授权体系

4.1.1 灵活的用户认证方式

绿盟堡垒机产品对主账号的认证，支持本地认证、LDAP 认证、RADIUS 认证、USBkey 认证、短信认证等多种方式，能够根据用户实际需求，设置混合认证方式，即不同主账号采取不同的认证方式，实现按需设置认证方式。

堡垒机提供VPN 联动NAT 穿透等方案解决用户内外网隔离下的设备运维，用户拨通VPN 后可访问内网堡垒机，再单点登录托管的目标设备进行运维。

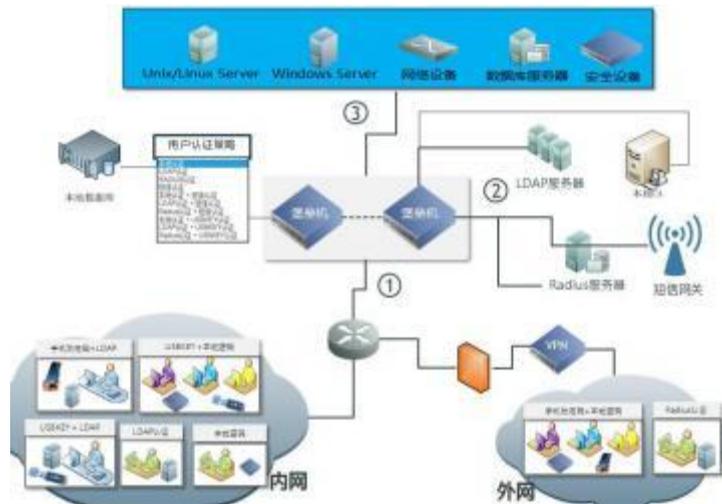


图 4.1 用户认证管理示意图

4.1.2 细粒度的运维访问控制

绿盟堡垒机产品支持基于角色的访问控制（RBAC ,Role-Based Access Control）。管理员可按照时间、部门、职责和安全策略等维度，设置细粒度权限策略，让正确的人做正确的事，简化授权管理。

通过集中统一的访问控制和细粒度的命令级授权策略，确保用户拥有的权限是完成任务所需的权限。系统支持创建基于时间、IP/IP 段、用户/用户组、设备/设备组、设备账号、命令关键字、危险级别（分为高、中、低）等元素的组合条件，授权用户可访问的目标设备、定

义高危操作监控策略。当用户越权执行特定命令的时候，实时进行告警、阻断，确保信息系统安全运行。

4.1.3 多维度的运维访问授权

绿盟堡垒机支持“向下”管控和“向上”申请的管理模式，支持 WEB 和 APP 通道对授权信息进行管理。

上级管理员角色通过策略方式设置运维人员能够登录哪些设备，能够执行哪些运维操作，甚至于对关键服务器或执行高危命令时，须有两人均认证通过方可执行，降低运维风险。支持登录双认证授权和高危命令双认证授权；

运维人员能够新建工单申请向管理员申请运维设备的权限。新建提前授权访问申请功能使得运维人员能够扩大对当前可运维设备的访问权限；新建临时访问申请功能能够获得当前无权限的目标设备访问权限。

以上管理模式不但支持 WEB 界面进行操作，并且为出差在外或请假不在电脑前无法审批的管理员提供了手机 APP 审批。

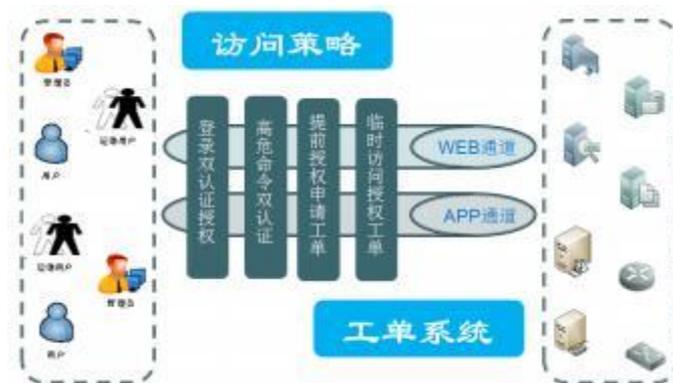


图 4.2 运维权限管理示意图

4.2 高效率、智能化的资产管理体系

绿盟堡垒机支持如下多种方式对用户托管设备进行智能化管理，有效提高用户资产管理能力，切实有效地保护托管在堡垒机中的设备和设备账号信息安全。

4.2.1 智能化巡检托管设备和设备账号

用户运维环境中常常存在大量的托管设备和设备账号信息，堡垒机能够智能化发现运维人员运维过程违规新建的设备账号（简称幽灵账号），幽灵账号常常会是系统的后门账号。同时由于运维人员离职，或职责切换等原因，出现已托管的设备账号长期不会被使用（简称为孤儿账号），因而导致托管设备上存在一定量的孤儿账号，长期以往必然会导致用户托管的设备存在严重的安全隐患，有效防范托管设备中设备账号管理漏洞带来的安全风险。

托管设备账号密码到堡垒机后能够有效防范弱口令问题，堡垒机提供完整细致的强密码安全策略，不但要求托管设备账号密码满足密码强度要求，并且要求托管的设备账号密码不应重复等更高强度的安全要求。

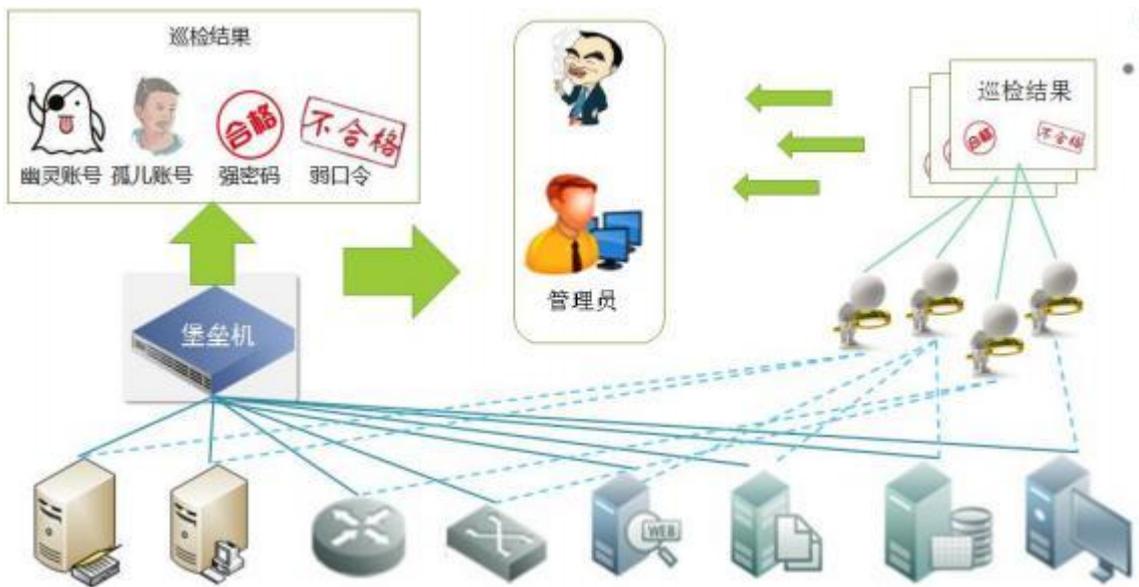


图 4.3 资产托管管理示意图

4.2.2 高效率管理设备和设备账号

运维环境中大量的设备和设备账号管理常常困扰运维管理员，绿盟堡垒机支持自动发现指定网络中的设备并自动将设备托管到堡垒机中，并支持定期自动发现设备中的设备账号，自动托管到堡垒机上，可大大提高运维管理员的运维管理效率。

多项法规合规要求中都有对设备账号管理有明确规定，要求定期对设备账号密码口令执行改密操作。堡垒机支持对托管设备账号执行周期改密，并支持用户自定义密码强度和密码内容，不仅提高运维管理员的运维效率，而且保障设备账号密码达到强密码要求。



图 4.4 设备自动发现示意图

4.3 提供丰富多样的运维通道

绿盟堡垒机支持以多种方式登录堡垒机及目标设备，灵活适应各种需求下的使用场景。

4.3.1 B/S 下网页访问

绿盟堡垒机支持 Internet Explorer、Firefox、Chrome 等多种内核的网页浏览器访问，支持一站式管理所有运维资源。网页界面展示方式丰富而多样，智能关联相关信息，充分体现了人性化用户界面设计原则和思路。

◆ 门户式管理

支持名片式、列表式和树形式的可访问设备信息展示，支持直接查询、编辑相关的访问策略，查询有权限访问的审计信息。

门户式管理极大地简化了管理员对设备、主账号、策略等的维护操作，优化管理员体验、提高管理员工作效率。

◆ 灵活的设备分组展示

绿盟堡垒机支持按照部门、设备类型、业务类型等不同的分组方式展示目标设备；不同的用户完全可以根据管理要求及使用习惯，选择不同的展示方式。

4.3.2 C/S 下客户端访问

绿盟堡垒机支持运维人员通过第三方客户端工具登录堡垒机，最大程度上保证运维人员的操作习惯不被改变。第三方客户端工具支持 RDP、VNC、Telnet、SSH、SFTP、HTTP/HTTPS 等协议的客户端工具软件，如 SecurCRT、putty、Xshell、Mstsc、VNC viewer、Winscp、

Xsftp 等。支持 RemoteApp 形式的应用发布程序访问，为数据库、WEB 服务器等系统运维提供最佳的运维体验。

结合 B/S 下丰富的资源展示效果，通过 WEB 上选择第三方客户端，直接调用客户端运维目标设备，将 B/S 和 C/S 的有机结合，使得用户在运维过程中能够获得更好的使用体验。

4.3.3 跨平台无缝管理

绿盟堡垒机产品具有跨平台的运维行为管控能力，可覆盖多种主流主机操作系统、网络设备、数据库和运维协议。

- ◆ 协议类型：SSH、RDP、VNC、SFTP、Telnet、FTP、HTTP、HTTPS、X11 等；
- ◆ 数据库类型：Oracle、MS SQL Server、IBM DB2、Sybase、IBM Informix Dynamic Server、PostgreSQL 等；
- ◆ 操作系统类型：FreeBSD、Solaris、RedHat Linux、Windows 等；
- ◆ 网络设备类型：Cisco、HUAWEI 等厂商的网络设备。

4.3.4 强大的应用扩展能力

绿盟堡垒机能够审计基于 Windows 平台下所有应用程序的运维操作。基于内置或外置前置机架构，当需要支持一款新的专有运维客户端程序时，只需管理员在前置机上安装、发布该客户端程序，而无须任何定制开发，堡垒机即可对通过该应用程序的运维操作进行审计。用户的投入产出比实现最大化，在零附加成本的基础之上，轻松支持所有通用及专有的运维客户端程序。



图 4.5 前置机架构示意图

运维设备时，运维人员只需登录堡垒机、选择目标设备以及应用程序，堡垒机将根据管理员事先配置好的参数自动启动前置机上相应的应用程序，并连接目标设备，前置机对运维人员完全透明。

4.4 高保真、易理解、快定位的审计效果

4.4.1 数据库操作图形与命令行级双层审计

绿盟堡垒机具备完善的数据库运维审计功能，能够同时支持数据库图形方式操作审计与 SQL 语句命令级操作审计；并支持 SQL 语句命令级审计日志与图形方式审计日志根据时间点进行关联查询，以方便用户进行日志查询。

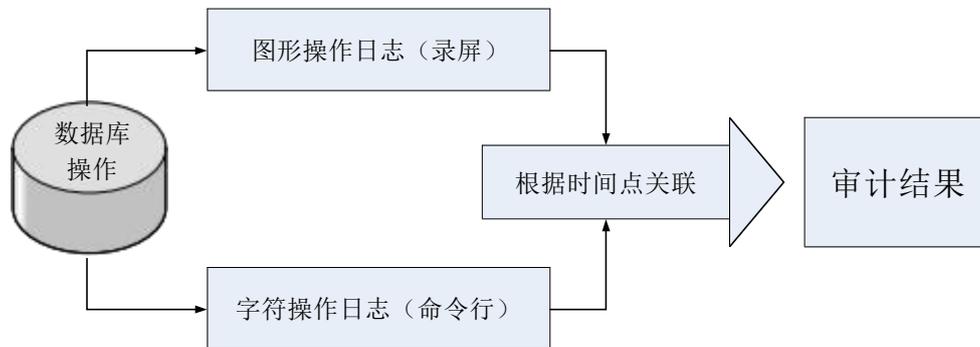


图 4.6 数据库操作图形与命令行级双层审计

4.4.2 基于唯一身份标识的审计

绿盟堡垒机产品主账号是获取目标设备访问权利的唯一账号，支持本地认证、LDAP 认证、RADIUS 认证、USBkey 认证、短信密码等多种认证方式，将主账号与实际用户身份一一对应，确保不同设备、系统间行为审计的一致性，从而准确确定为事故责任人，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。

4.4.3 全程运维行为审计

绿盟堡垒机可完整审计运维人员通过账号“在什么时间登录什么设备、做什么操作、返回什么结果、什么时间登出”等行为，全面记录“运维人员从登录到退出”的整个过程，帮助管理人员及时发现权限滥用、违规操作，准确定位身份，以便追查取证。

◆ 字符会话审计

系统支持审计通过 SSH、Telnet 等协议的操作行为，审计内容包括访问起始和终止时间、用户名、用户 IP、设备名称、设备 IP、协议类型、危险等级、操作命令等。可提供操作内容倍速回放、定位播放等功能。

◆ 图形操作审计

系统支持审计通过 RDP、VNC 等远程桌面以及 HTTP/HTTPS 协议的图形操作行为，审计内容包括访问起始和终止时间、用户名、用户 IP、设备名称、设备 IP、协议类型、危险等级、操作内容等。支持通过视频录像方式记录操作内容，可提供倍速回放、定位播放等功能。

◆ 数据库运维审计

系统支持审计 Oracle、MS SQL Server、IBM DB2、PostgreSQL 等各主流数据库的操作行为，审计内容包括访问起始和终止时间、用户名、用户 IP、设备名称、设备 IP、协议类型、危险等级、操作内容等。支持通过视频录像方式记录操作内容，可提供倍速回放、进度拖拉等功能。

◆ 文件传输审计

系统支持审计通过 SFTP、FTP 等协议的操作行为，审计内容包括访问起始和终止时间、用户名、用户 IP、设备名称、目标设备 IP、协议类型、文件名称、危险等级、操作命令等。可提供操作内容倍速回放功能。

◆ 合规审计

对上述各类运维审计日志，审计员能够单独或批量进行合规审计，方便地审核每一次运维行为及操作是否符合规章制度的要求，并填写具体的审核批注，最后统一输出合规审计结果。

4.4.4 审计信息“零管理”

绿盟堡垒机产品支持“日志零管理”技术

- ◆ 日志自动维护：根据日志自动维护计划的设置，系统在指定时间自动进行相应的日志数据备份。

- ◆ 日志查询：系统提供多种审计日志查询条件，包括时间、IP 地址、用户名、设备名、关键字、危险等级（高、中、低）等；
- ◆ 审计报表：系统提供详细的多种类别的报表模板，可提供基于操作时长、高危操作、阻断操作等类别的用户操作 TOP10。系统支持生成：日、周、月、年度综合报表，报表支持 Word、Excel 等格式导出，降低维护费用与管理员的工作强度。
- ◆ 自动报表：客户需要周期（比如每周、每月）进行运维审计，同时审计报表的范围都一致。此时客户可以自定义时间点和报表模板，堡垒机就可以周期生成统计报表，自动发送到客户邮箱中。

4.4.5 文字搜索定位录像播放

绿盟堡垒机产品支持指令输入和图形操作双审计技术

- ◆ 指令输入审计：运维过程中用户输入的键盘指令可以被审计记录
- ◆ 图形操作审计：运维过程中用户图形操作可以被审计记录
- ◆ 图形内容识别：运维过程中用户图形操作的窗口标题信息可以被审计记录
- ◆ 文字搜索定位录像播放：审计用户可以不用从头到尾查看运维录像，通过搜索键盘或窗口标题信息，直接跳转到当时运维的录像记录。节约审计操作成本。

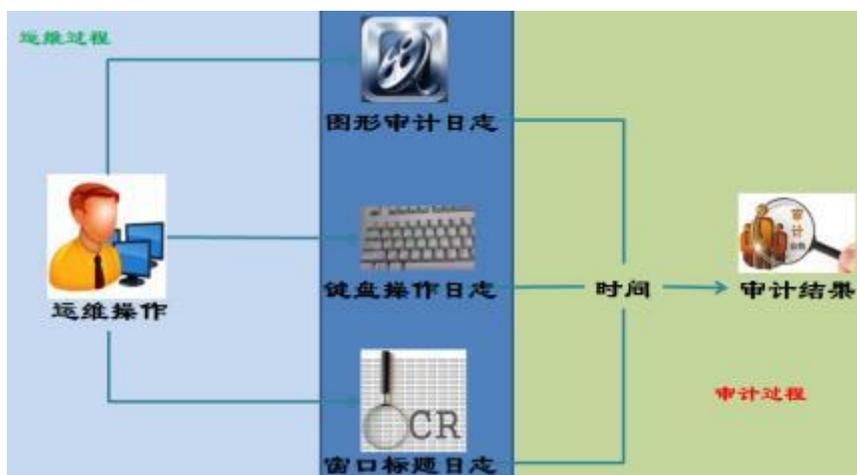


图 4.7 文字搜索定位录像播放

4.5 稳定可靠的系统安全性保障

4.5.1 系统安全保障

- ◆ 采用专门设计的安全、可靠、高效的硬件平台。该硬件平台采用严格的设计和工艺标准，保证高可靠性；
- ◆ 独特的硬件体系结构提升处理能力；
- ◆ 操作系统经过优化和安全性处理，保证系统的安全性；
- ◆ 支持热插拔的冗余双电源，避免电源硬件故障时设备宕机，具有可靠的高可用性；

4.5.2 数据安全保障

- ◆ 堡垒机与客户端通信均采用加密的 SSL 传输控制命令，完全避免可能存在的嗅探行为，确保数据传输安全。
- ◆ 审计日志信息采用专利特有的保存方法，支持关键特殊信息指纹签名，并可加密存储到外置存储设备。仅可在专用审计播放器下查看。
- ◆ 支持智能管理系统存储资源，系统存储达到瓶颈时自动告警或清理存储空间。
- ◆ 支持 RAID1 磁盘阵列实现数据冗余备份，提供高数据安全性和可用性。
- ◆ 用户配置信息采用加密存储，用户配置备份信息仅能通过系统解密获取，防止被不法用户盗取。

4.6 快速部署，简单易用

4.6.1 物理旁路，逻辑串联

绿盟堡垒机产品采用“物理旁路，逻辑串联”的模式，不改变网络拓扑结构，不需要在终端安装客户端软件，不改变管理员、运维人员的操作习惯，不影响正常业务运行。

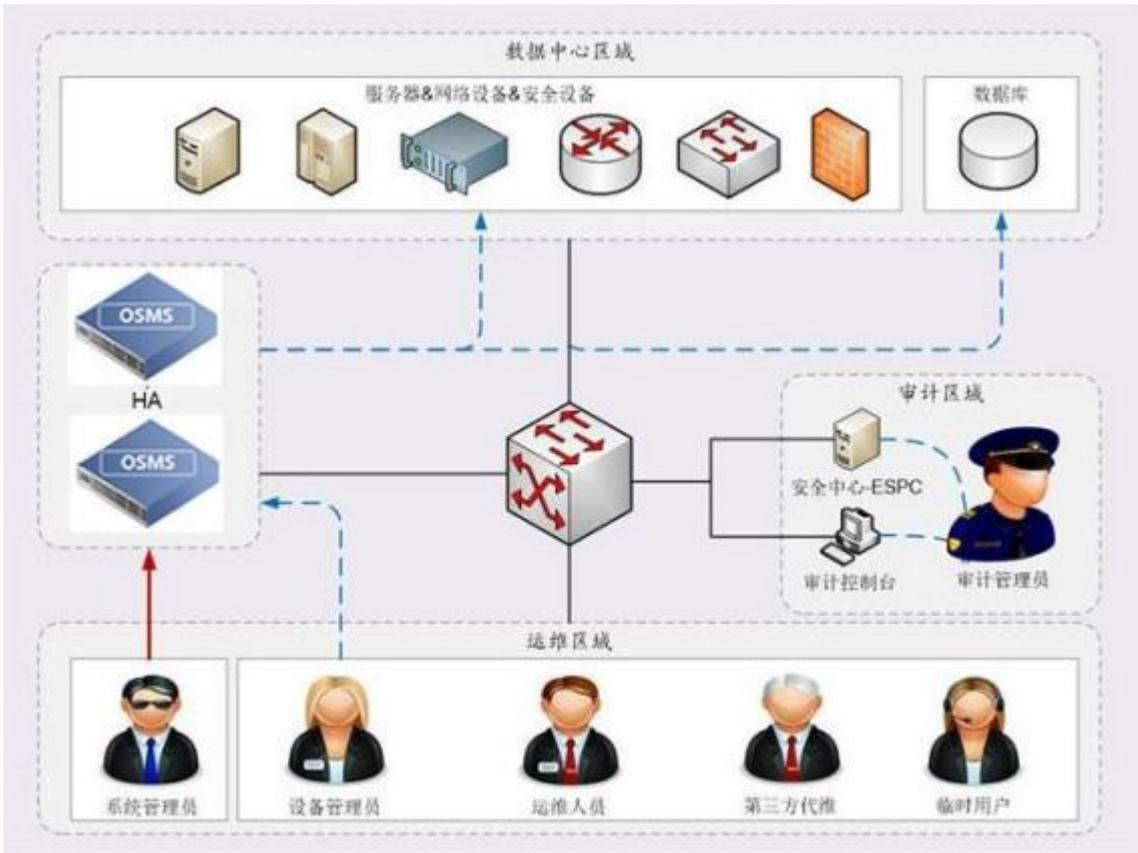


图 4.8 产品部署



图 4.9 支持 IPv4 和 IPv6 双栈网络

4.6.2 配置向导功能

提供对堡垒机管理配置向导、设备管理员策略配置向导、数据库运维配置向导；通过将配置操作分解成逻辑性更强的操作，在多个页面上进行向导，达到引导用户完成复杂配置的目的，提高产品易用性。



图 4.10 配置向导

4.6.3 在线帮助指南

提供完整详细的在线帮助指南，快速指引新用户使用，帮助解答老用户存在的疑问。



图 4.11 在线帮助指南

五. 客户收益

通过部署绿盟堡垒机产品，可帮助企业建立面向用户的集中、有序、主动的运维安全管控平台，通过基于唯一身份标识的集中账号与访问控制策略，与各服务器、网络设备等无缝连接，实现集中精细化运维操作管控与审计，降低人为安全风险，避免安全损失，满足合规要求，保障企业效益。