中科网威堡垒机技术白皮书

总机电话-- 0755-83658009　技术支持-- 0755-83658229　24 小时技术值班热线-----135-1069-3536
http://www.anysec.com　深圳市龙华区观澜街道观光路 1301-80 号电子科技大学(深圳)高等研究院 3 号楼 1401

声明

本公司对本手册的内容在不通知用户的情况下有更改的权利。

NOTICES

Shenzhen Anysec-Tech Company Limited reserves the right to make any changes in specifications and other information contained in this publication without prior notice and without obligation to notify any person or entity of such revisions or changes.

目录

1、运维管理风险分析

随着云计算的发展和市场推进，大量的企业、政府都将应用系统迁移至云环境中。云计算的发展使得云主机的运维方式发生了一定程度的变化，比如批量运维、自动化运维等等。然而，传统运维过程中存在的安全问题并未因为应用了云平台而减少，甚至比传统方式更加严峻，主要表现在：

（1）云主机和云数据库的运维端口直接暴露在公有云中，增加了被攻击的风险；

（2）大量的云主机带来的账号和密码管理难题，比如账号公用问题、密码修改问题、密码强度问题等等；

（3）特权账号的活动管理，操作系统自身难以实现权限最小化，从而导致过度授权、数据泄露等一系列安全风险；

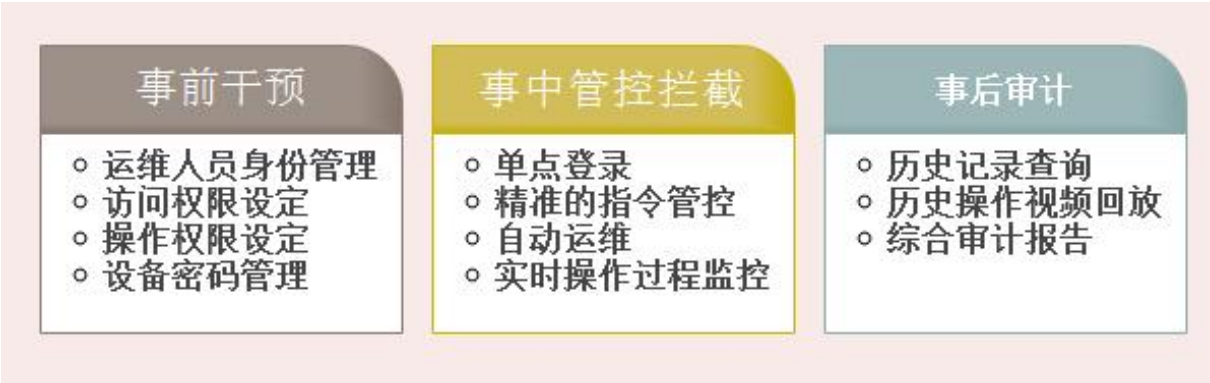
（4）运维过程引入第三方服务已是常态，运维人员的误操作、恶意操作行为时有发生；

（5）缺乏有效的审计和控制手段，系统无法满足等级保护需求。

传统的 IT 环境边界非常明确，可以利用堡垒机、防火墙对服务器、应用系统的访问进行严格的访问控制，在业务迁入云环境后，硬件的堡垒机、防火墙已经不再适用，业务的边界页不如传统边界清晰，因此云环境下，运维安全问题更加严峻。

堡垒机系统是深圳市中科网威科技有限公司基于多年的科研及实践经验，并充分研究云环境下的运维需求后推出的新一代云运维安全管理系统，系统具有易部署、易使用的特点，支持指令级细粒度授权、运维全过程控制和视频回放，能够对运维人员和运维过程进行有效控制，避免运维安全风险，满足等级保护等合规审计需求。

2、产品特性



2.1 身份鉴别与管理

云服务器账号和密码共享是一种普遍存在的现象，账号共享会导致安全事件无法清晰地定位责任人。堡垒机提供了一套完整的身份鉴别和管理功能，为每一个运维人员创建唯一的运维账号（主账号），并与云虚拟机账号（从账号）均进行关联，确保所有运维行为审计记录均可定位至自然人，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。

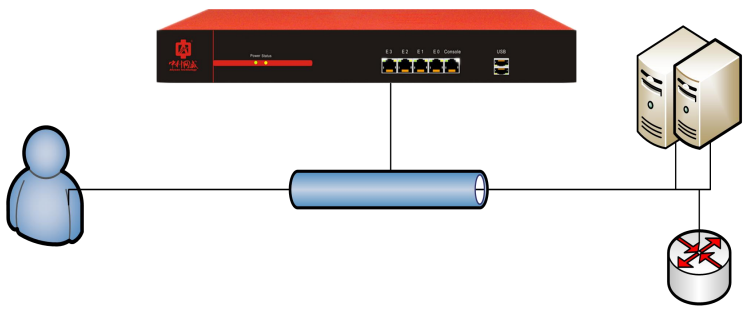


图 2-1 基于唯一身份标识的审计

- ✓ 支持多种认证类型，包括：本地、RADIUS、AD 域。
- ✓ 支持多因子身份认证，包括：动态令牌、短信认证。
- ✓ 支持密码强度、修改密码周期、尝试密码强度、无操作超时时间等安全管理功能。
- ✓ 支持用户分组管理。
- ✓ 支持用户导入导出管理，方便批量处理。

2.2 细粒度权限划分

堡垒机系统支持基于角色的访问控制（RBAC，Role-Based Access Control），将云平台与服务器的权限进行细粒度权限划分，可对不同的角色设置不同的权限，用户不能使用权限以外的功能。通过设置角色的模块权限、通用权限、业务权限和数据权限，确保用户拥有的权限是完成任务所需的最小权限。

图 2-2 角色权限控制

2.3 设备密码管理

堡垒机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 云虚拟机操作系统的账号密码。

- ✓ 设定改密计划的自动改密周期和起始时间。
- ✓ 支持随机生成不同密码、随机生成相同密码、手动指定相同密码等新密码设定策略。
- ✓ 改密结果自动发送至相关管理员邮箱。
- ✓ 可进行批量操作。

2.4 单点登录

堡垒机部署后，运维人员可以通过 B/S、C/S 两种方式登陆堡垒机系统并进行云虚拟机的安全管理工作。堡垒机支持单点登录功能，运维人员登录堡垒机时，只需输入一次堡垒机的主帐号，无需输入云主机的操作系统帐号密码即可访问所有授权范围内的云主机等资源。

2.5 精准的指令管控

用户在通过堡垒机系统使用资源时，所有的指令都将被堡垒机系统管控。系统管理员通过新建命令集和命令授权策略来管理用户的操作行为，并可以对其中的敏感指令进行精准匹配拦截。

- ✓ 管理员可根据用户、用户组、部门、角色、资源、自定义 IP 段设置细粒度访问策略。
- ✓ 支持自定义命令。
- ✓ 对命令集的管控动作有：拒绝执行、允许执行、告警、动态授权、断开。
- ✓ 动态授权的命令集需要管理员授权后才能被执行。
- ✓ 支持基于时间的访问控制。

2.6 批量执行

堡垒机支持对当前打开的命令窗口执行批量操作，当运维人员登录多台 SSH 服务器时，只需在任何一个窗口开启群发键输入，通过批量执行功能，运维人员在一个窗口的输入能够同步到其他的窗口，方便实现对多台主机的升级、备份等工作任务。

图 2-3 群发操作

2.7 自动运维

堡垒机支持对托管服务器、虚拟机、网络设备执行批量命令、脚本，或者是命令和脚本的组合。通过将运维任务与执行计划关联，可以设定运维任务定时执行或者是周期执行。当有批量任务的时候，它既可以让运维工作更加高效快捷，又可以让企业的运维安全、合法。同时也支持对 python、bash 脚本的管理。

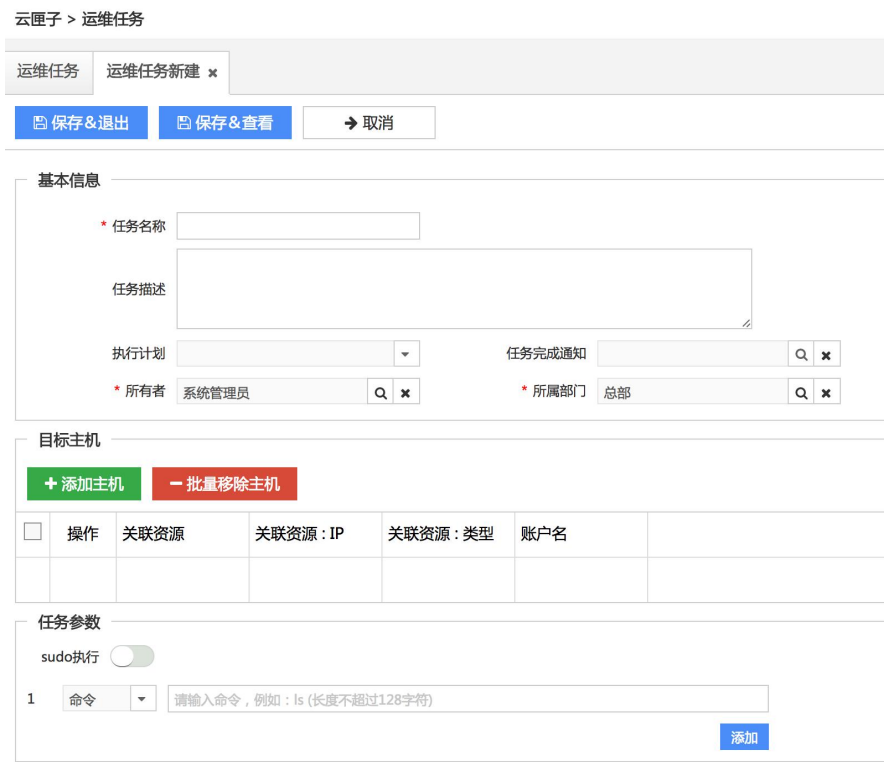


图 2-4 自动运维任务

2.8 账户收集

堡垒机能够对托管服务器、虚拟机、网络设备进行账号巡检，快速搜索主机内的僵尸账号、已遗忘的登录秘钥等。解决服务器运维人员对于服务器、虚拟机的口令管理难题，避免因外包人员工作后而保留服务器、虚拟机登录后门而带来的安全风险。

主机账户情况

快速查询： 账户名, 主机：名称, 主机：IP

操作	账户名	主机	主机：IP	状态	创建时间
编辑 删除	root	192.168.114.164	192.168.114.164	已同步	2017-07-19 11:40:54

主机SSHKey情况

快速查询： 账户名, 主机：名称, 主机：IP

操作	账户名	主机	主机：IP	SSHKey状态	创建时间
查看公钥 删除	root	192.168.114.164	192.168.114.164	非法key	2017-07-19 11:40:54
查看公钥 删除	root	192.168.114.164	192.168.114.164	非法key	2017-07-19 11:40:54

图 2-5 账户扫描结果

2.9 资源监控

堡垒机对托管服务器、虚拟机、网络设备等资源进行监控，预判设备的性能瓶颈。目前支持的性能参数包括：CPU、内存、磁盘使用率、上下行流量等。通过预置安全报警阈值，一旦达到安全警戒值，管理员便可通过堡垒机快速登录报警的服务器、虚拟机，快速解决问题，实现监控告警与运维审计一体化联动。

主机名称	192.168.114.10	设备类型及名称	Windows — WIN-OJMP4EF5OHB.surfilter.com
IP地址	192.168.114.10	持续运行时间	37 天, 6 小时, 39 分钟, 29 秒.
MAC地址	00:50:56:8f:40:d5 00:00:00:00:00:00:00:e0		
CPU核数(个)	4	内存(MB)	4095
磁盘(GB)	40		
CPU使用率(%)	5.50	内存使用率(%)	66.00
描述信息	Hardware: Intel64 Family 6 Model 44 Stepping 2 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 9600 Multiprocessor Free)		

告警列表

快速查询： 告警内容

操作	告警次数	告警内容	告警级别	首次告警时间
处理告警 确认告警	120	Windows服务器:192.168.114.10 内存使用率(66.0%),超过阈值(60.0%),告警级别(低)	低	2017-07-20 23:34:00

图 2-6 资源监控信息和告警

2.10 移动运维

堡垒机手机 APP，帮助用户实时运维。运维人员通过 APP 一键登录目标主机，不会再出现外出办公难，通宵留守机房等情况；审计管理员通过 APP 随时随地审计系统运维；管理员快速实时对运维工单申请相应，提高工作效率。

2.11 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。

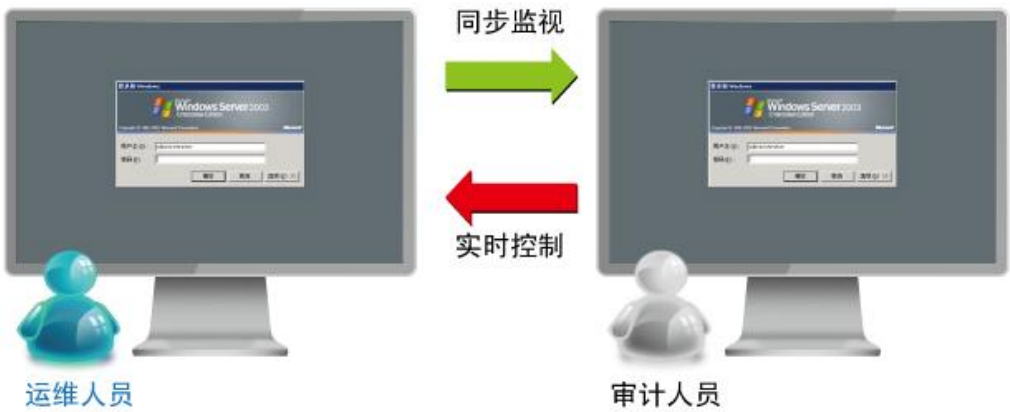


图 2-7 运维操作实时监控

2.12 历史记录查询

堡垒机支持两种记录查询功能，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。

2.13 历史操作视频回放

堡垒机能够以视频回放的方式，完整地展示运维人员的所有操作，并且对运维人员的操作命令进行记录。同时，可根据操作记录定位回放或完整重现运维、外包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。

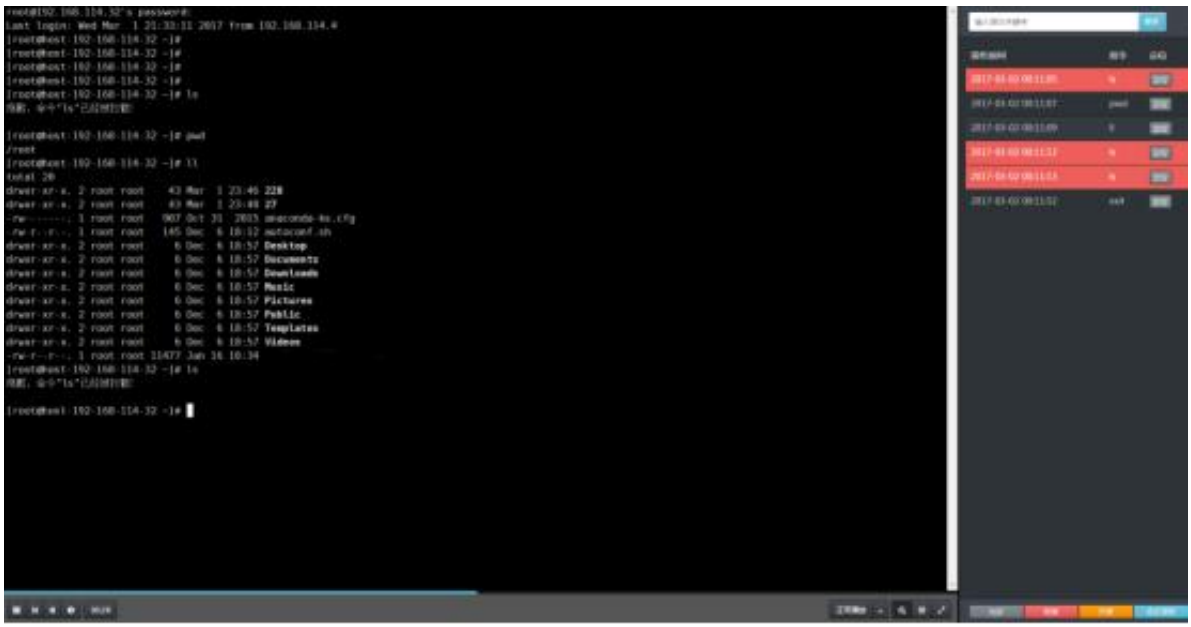


图 2-8 运维操作回放和定位

2.14 综合审计报告

堡垒机内置强大的报表功能，可提供满足不用客户审计需求的安全审计报表模板，能够生成基于时间、操作、用户和资源等条件的综合报表，并且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，降低维护费用与管理员的工作强度。

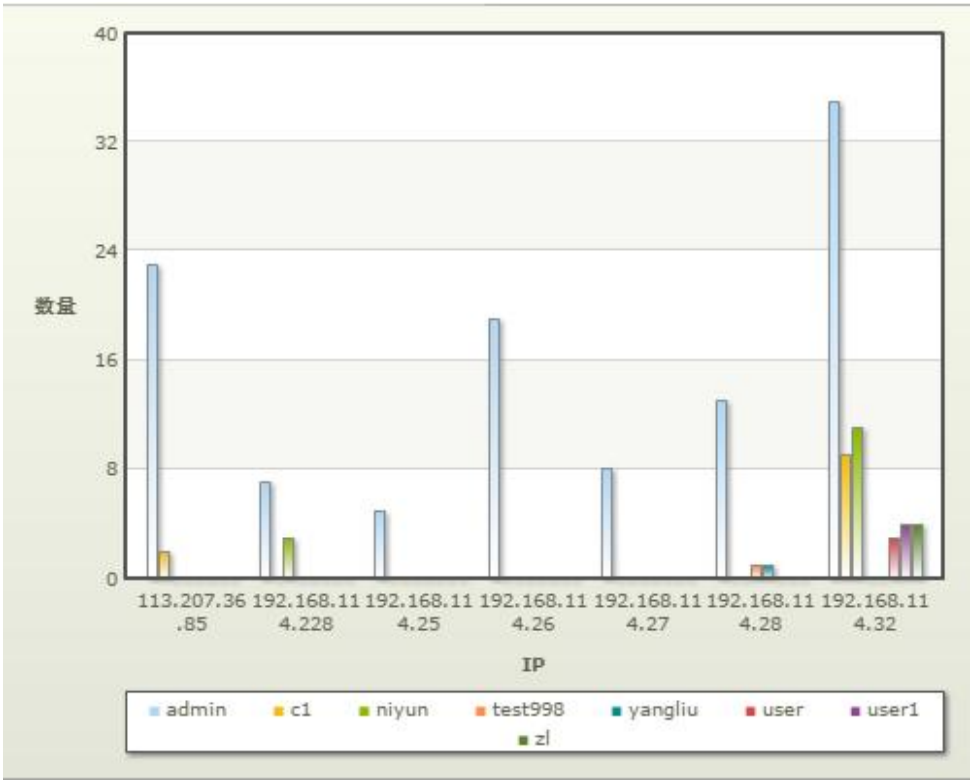


图 2-9 运维报表

3、部署

堡垒机支持多种部署方式，部署简单，并且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。部署单臂模式即可。

堡垒机部署单臂模式，配一个接口 IP 和网关，只要堡垒机能访问到下面所有要做运维的设备即可。

堡垒机部署示意图：

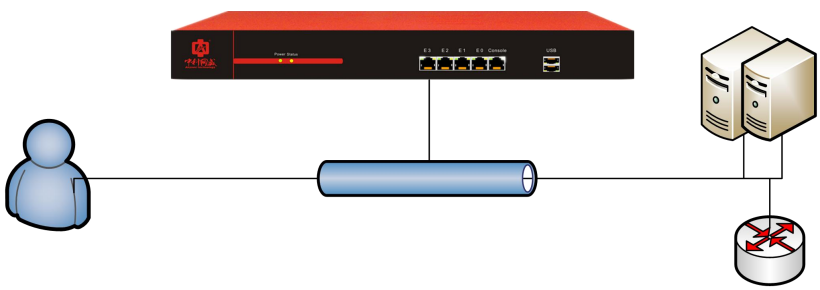


图 3-1 堡垒机部署

4、应用效果

通过部署堡垒机产品，可以帮助企业建立面向用户的运维安全管控平台，通过基于唯一身份标识的账户和访问控制策略，与企业的资源，包括服务器、网络设备等无缝连接，实现集中安全策略管理，提升主机的安全性和运维效率，降低人为的安全风险，避免安全损失，满足合规要求，保障企业的安全和效益。