瑞和云图
Safe in Cloud

云翼运维审计系统

技术白皮书

北京瑞和云图科技有限公司

www.rivercloud.com.cn

2020 年

目　　录

1 产品概述

用于对运维人员的操作权限进行控制和操作行为审计。

云翼运维审计系统综合了运维管理和安全性，切断了人员对网络和服务器资源的直接访问，而是采用协议代理的方式，接管了人员对网络和服务器的访问。形象的说，人员对云主机的访问需要经过云翼运维审计系统的翻译。

2 产品功能

2.1 云翼运维审计系统的作用主要体现在以下几个方面

1. 杜绝权限滥用
2. 发现违规操作
3. 降低人为安全风险
4. 降低工作复杂度

2.2 使用场景

1、共享账号难控制

公司员工数量多、部门多、主机数量多，公司不同部门间业务交接、人员更

换部门、人员离职等情况也时有发生，这些都导致操作权限分散难以管理。采用共享账号操作一旦出现问题，事后很难追责到具体个人。

Account（账号管理）可以提供员工账号+主机账户管理功能，轻松分部门、分组，权限分配、变更及注销轻松完成。

2、设备密码难管理

公司员工按照自己习惯，应用 SSH、VNC、Telnet 等多种协议，管理员难以设置统一认证、出现问题也很难定位。使用 SecureCRT、Xshell 等各类运维工具出现安全漏洞后，难以保证所有人都及时完成升级防御。

Authentication（认证管理）使用旗舰版云翼运维审计系统作为安全的统一认证入口，集中管理，员工依然可以保持自身操作习惯，应用各类常见协议，使用原有运维工具。

3、操作行为难约束

公司的外包人员，为工作方便需要开放一系列权限，但开放的权限无法实现限制和监管。

UHAS 的 Authorization（权限管理）分配给外包人员足够的运维权限，公司指派管理员和审计员，对外包开发人员权限做监管、行为做审计，轻松管理。

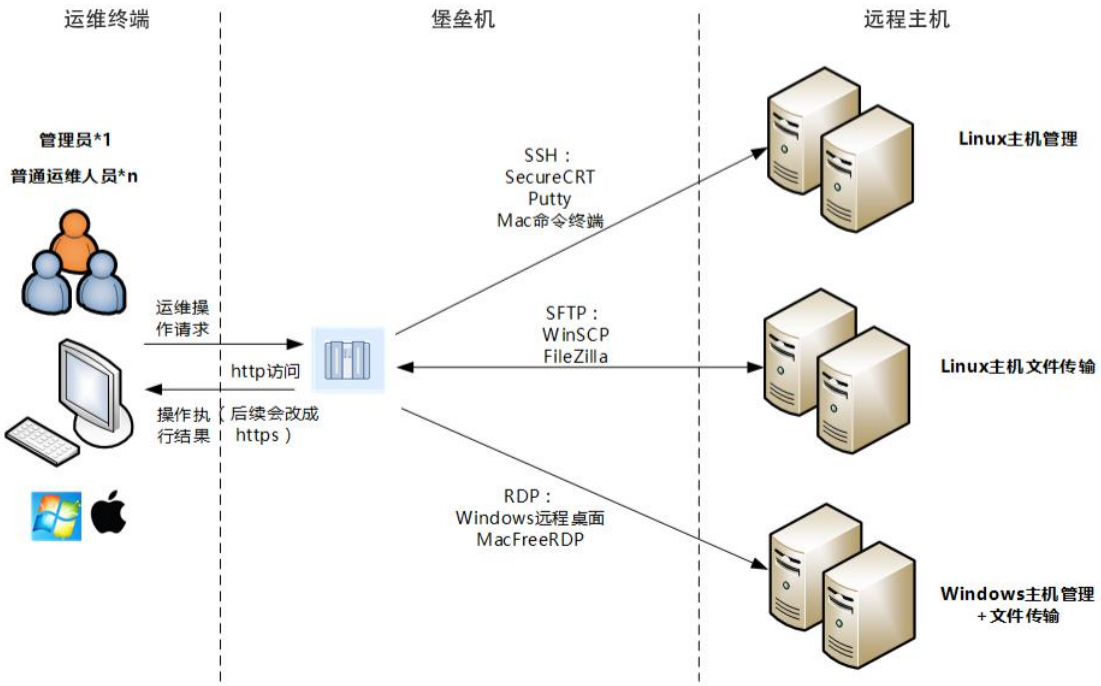
4、操作过程不透明

公司重要业务系统的登陆、操作和聘请的外包团队的操作过程不透明，对企

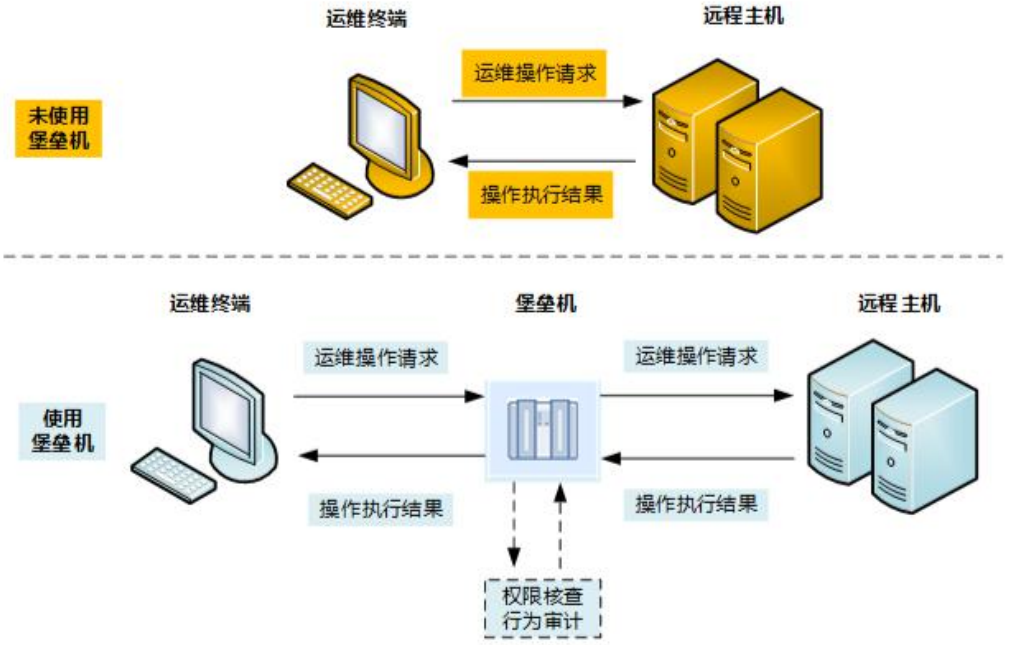
业来说高危操作无法进行监管，一旦系统被删除或者安装后门，将对企业造成致命打击；对运维人员来说，出现安全事故无法自证清白，也无法定位源头。

Audit（审计管理）管理员可以对运维人员的操作进行实时监控和及时中止，可以对所有经过云翼运维审计系统的操作进行审计，审计记录无法篡改。

2.3 原理

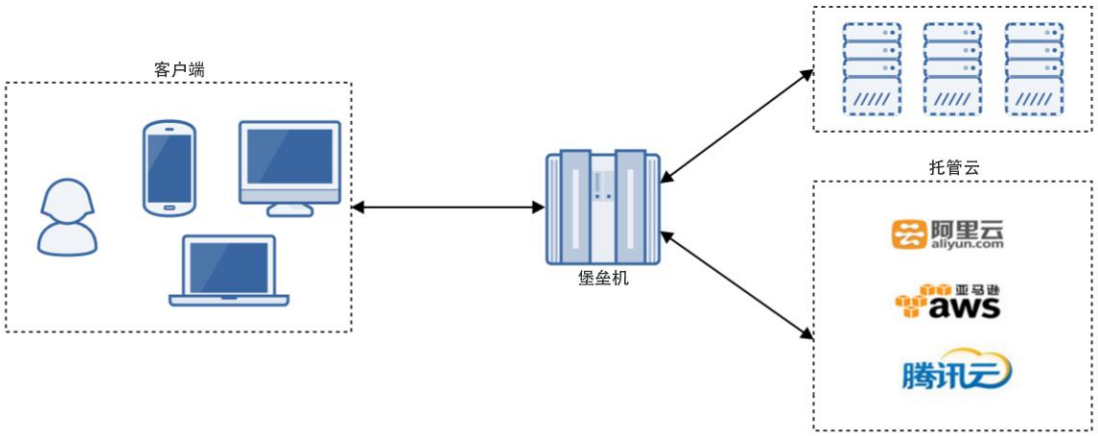


使用云翼运维审计系统之前，用户直接登录主机进行管理和控制。使用云翼运维审计系统之后，用户登录主机之前需要先登录云翼运维审计系统，云翼运维审计系统将记录用户对主机所有的操作，并将这些操作返回给管理员。管理员可以查看任何用户的操作历史，然后根据这些操作进行追责或者提出整改要求。

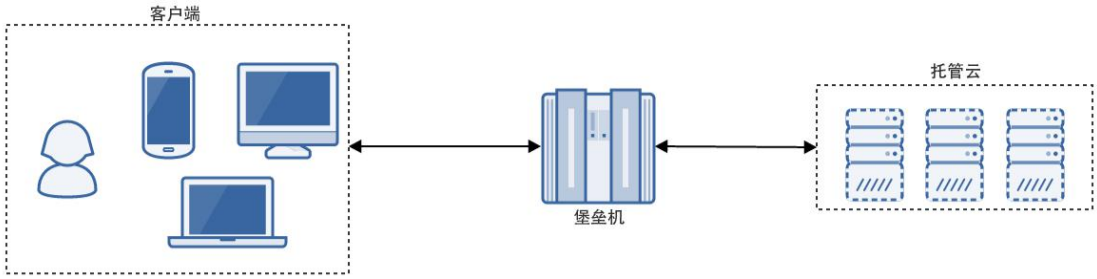


2.4 架构

2.4.1 公有云架构



2.4.2 托管云架构



2.5 主要功能

2.5.1 用户管理

新建与管理云翼运维审计系统管理账号，可对账户进行冻结/解冻操作；管理用户组，可将用户放入用户组统一管理。

2.5.2 资产管理

资产管理可对 Windows 和 Linux 主机以及网络设备进行管理。除了传统意义上的主机与网络资产外，管理用户、系统用户、标签等都属于资产管理范围。

2.5.3 应用管理

针对的是 MySQL 数据库管理。

2.5.4 授权管理

授权过程其实就是把各系统上建立的帐号分配给操作人员的过程，管理员要定义帐号的权限，然后做帐号分配，根据用户置位调整做相应的帐号权限修改。

2.5.5 操作审计

管理员要定期做服务器的巡检，分析各系统上的日志，查看是否有越权访问，查看是否有误操作，如果有事故还需要根据日志进行故障排查和事故追踪。

2.5.6 单点登录

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。

2.5.7 集中账号管理

通过建立集中账号管理，单位可以实现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。而且，还可以实现针对自然人的行为审计，以满足审计的需要。

2.5.8 集中身份认证

Windows AD 域、双因素多种认证方式，可以方便的与第三方 LDAP 认证服务器对接。

2.5.9 统一资源授权

云翼运维审计系统提供统一的界面，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。

2.5.10 命令过滤

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，是一组非可执行的命令，该命令集合用来分配给具体的用户，来限制其系统行为，管理员会根据其自身的角色为其指定相应的控制策略来限定用户。

2.5.11 运维审计

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。

系统支持对如下协议进行审计：Telnet、SSH、RDP（Windows Terminal）等。

2.5.12 批量命令执行

用户可以通过统一界面对其所管理的终端进行命令的批量下发。

2.5.13 管理多种运维操作方式

终端命令行操作：Telnet、SSH

图形终端操作：RDP、VNC

文件传输操作：FTP、RDP 磁盘通道、剪贴板等文件传输

数据库运维操作：MS SQL

2.5.14 审计功能

精确记录用户操作时间。

审计结果支持多种展现方式，让操作得以完整还原。

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。

方便的审计查询功能，能够一次查询多条指令。

2.5.15 加密协议审计

系统支持对 SSH 等加密类协议，以及 RDP 等图形协议进行全面审计。可以记录操作命令、操作过程中的键盘事件，同时可以对操作过程进行实时监控、录像、回放。