CLOUDBILITY
行云管家

行云管家堡垒机产品介绍

深圳市行云绽放科技有限公司

www.cloudbility.com

目录

一、 产品基本介绍

1.1 背景

随着企业信息化建设步伐的不断加速，IT 对企业业务起到的支撑作用也越来越明显，毫不夸张的说，在相当一部分企业中，IT 已经发展成为企业的生命线。相应的，在现如今信息安全事故频发的背景下，企业对内部信息安全的管控要求也越为严苛。

传统模式下，企业会考虑通过部署堡垒机的方式来提高企业内部信息安全管理水平，提供控制和审计依据，并满足相关法规要求。这些措施在传统运维方式下并无大碍，但在已经到来的云计算时代，企业已经开始逐步采用并充分利用云计算的低成本、按需配置等核心优势来满足企业的弹性化 IT 需求。云计算的发展将会对企业的信息安全带来新的挑战，主要体现在：传统的运维模式与管理思维是否能够适应云的变化？如何确保混合云模式下的统一管理与安全运维？是否能够充分发挥云计算好的优势？

通过行云绽放行云管家堡垒机，可对私有云、公有云和本地 IT 设备等资源进行运维、监管与审计，并实现账号集中管理、双因子认证、访问授权控制等功能，让企业内部人员、第三方代维人员的操作处于可见、可管、可控、可审的状态，规范运维的操作流程，避免误操作和非法授权带来的安全隐患，降低安全风险，满足合规性要求，并最终保障企业 IT 的安全、可持续运行。

1.2 主要功能

行云绽放行云管家堡垒机标准版是以 4A 管理理念为设计基础，满足国家相关堡垒机产品法规的要求，为用户提供合规的账号体系、严格的认证机制、完善的授权模型、精准的运维审计的一款堡垒机产品；在满足 4A 管理理念的同时，为了降低堡垒机对运维工作的影响，行云管家堡垒机将用户与 IT 资产进行分离，将自身定位为“运维中枢”、“会诊平台”、“黑匣子”三位一体的堡垒机平台，以保障运维工作的高效、提升故障处理水平、满足运维审计的要求。

- **IT 资产管理：**

行云管家堡垒机支持对多种类型的设备进行管理，不论是服务器、数据库、应用、网络设备、存储设备或其它网元设备，只要具备 IP 即可导入。

- **运维中枢：**

作为运维中枢，行云管家从管理协议、管理工具、文件传输等各层面为用户提供了强有力的支撑，在不改变运维人员习惯的前提下，帮助用户高效的完成运维工作。

- **会诊平台**：

在行云管家堡垒机中，任何一个远程桌面都可开启会话分享功能并形成一个分享链接，只需将此链接发送给您的好友，即可邀请好友进入同一个远程桌面。多人之间面对同一个工作场景，并自由切换操作控制权；协同过程中，用户免装软件、免交密码、全程审计。

- **黑匣子**：

针对运维过程不同阶段的要求，行云管家堡垒机提供了事前授权、事中监察、事后审计的能力，实现运维操作全生命周期的管控与审计。

1.3 产品特点

- **多云异构环境下的混合式管理**：

无论是企业内部局域网环境、IDC 托管设备、公有云资源以及私有云资源，行云管家堡垒机均可提供统一的运维管理与运维审计功能。

- **支持主流管理协议**：

行云管家堡垒机支持 RDP、SSH、VNC、Telnet、FTP/SFTP 等多种主要的服务器管理协议。

- **精细化授权模型**：

行云管家堡垒机采用基于角色和用户的访问控制模型来实现权限控制，具体来说，是将授权模型划分为功能授权和资源授权两个维度，角色承担功能授权，而用户/用户组/部门是资源权限的载体。

- **事中监管能力**：

行云管家堡垒机提供实时监控远程会话能力，一旦发现操作者有不当或违规的行为，可立即剥夺操作者的控制权，阻断风险；同时提供敏感指令拦截功能，管理者可预先定义好高危指令黑名单，一旦操作者在目标设备上执行的命令被黑名单规则命中，将自动触发拦截机制，阻止危险指令的执行。

- **事后审计回溯能力**：

整个运维过程将会被以录像的方式进行记录，录像存储在云端（服务器端），可避免数据被篡改。可根据操作记录定位回放或完整重现运维人员对目标设备的整个操作过程，从而真正实现对操作内容的完全审计，整个录像过程可：根据关键词进行全文检索及定位，并对关键搜索词进行圈红标记、支持倍速播放、拖动、暂停等播放控制功能、下载录像文件进行离线播放。

- **丰富多维度的安全运维策略：**

支持针对不同用户、不同的目标设备，定义不同的运维策略，用户可根据运维要求，定制多种场景的运维策略，满足各种个性化的应用场景，如：文件传输策略、会话水印限制、运维时段控制等。

二、 配置环境准备

2.1 硬件要求

1. CPU 内存：建议至少 8 核 16G；磁盘空间最低建议：500GB；
2. 依据纳管设备数和最大并发会话数适当提高硬件配置，依据后续审计日志存储要求，适当增加存储空间；

2.2 网络要求

1. 服务器开放 80 端口（http）、443 端口（https）访问；
2. 如果需要使用本地工具、跳板机功能，则需按需对外开放 8021（FTP）、8022（SSH）、8389(RDP)、8900（VNC）等端口的访问；
3. 为了方便后续对堡垒机系统的运维，建议在确保安全的前提下开放服务器的 SSH 端口（默认为 22，可修改为其它端口）；
4. 如需管理公有云主机、发送短信、邮件服务等，那么服务器需具备公网访问能力。

2.3 操作系统要求

1. 操作系统：行云堡垒基于容器化部署，支持业界常见的一些 Linux 发行版操作

系统；

注：目前 CPU 支持 x86_64 和 AMD64 架构，CPU 需支持 AVX 指令集；

可通过命令"lscpu"查看 CPU 是否符合系统需求。

2. 行云堡垒的安装必须由 root 用户执行。

三、 正式使用指引

初始化完成后，请使用 Edge、谷歌、火狐等对 HTML5 支持较好的浏览器来正式访问行云堡垒。

3.1 行云堡垒正式使用指引

所有用户在使用行云堡垒时，都将在门户网站中进行操作。

门户网址：http://行云堡垒 IP/

使用指引：http://行云堡垒 IP/help

3.2 管理控制台使用指引

管理控制台是针对于系统的全局管理平台。其中包括业务管理、系统管理、控制台管理等模块：

（1）业务管理：行云堡垒是一个多租户（团队）的管理模型，因此需要在管理控制台中管理不同团队、团队用户和设置用户登录的认证设置等功能。

（2）系统管理：用于对整个系统的全局设置（访问配置、系统参数、门户双因子认证、短信网关、邮件服务器配置等功能、中转服务设置、数据备份等重要功能）。

（3）控制台管理：用于管理后台的用户和角色并记录后台的相关日志。

管理控制台地址：http://行云堡垒 IP/console

3.3 默认账号密码

默认账号为：admin

默认密码：Admin@123

3.