**操作审计**

全面记录运维人员的操作行为，作为事件追溯的保障和事故分析的依据。

* **运维操作记录**：操作失误、恶意操作、越权操作详细记录。
* **Linux命令审计**：可提取命令符审计，支持命令定点回放。
* **Windows操作录像**：远程桌面的操作，支持全程录像，包括键盘操作、鼠标操作、打开窗口等。
* **文件传输审计**：支持远程桌面文件传输、SFTP的文件审计。

**权限控制**

通过账号管控和权限管理，实现人员和资产的权限管理。

* **账号管控**：使用唯一运维账号，解决共享账号、临时账号、滥用权限等问题。
* **权限管理**：按照人员、部门组织、资源组，建立人员职责与资源分配的授权管理体系。

**安全认证**

引入**双因子认证**机制，通过短信认证、动态令牌等技术，降低账号密码泄露风险，防止运维人员账号泄露被反复利用。对接**AD认证**和**LDAP认证**服务，一键同步认证用户，您可以保持原有的用户部署方式。

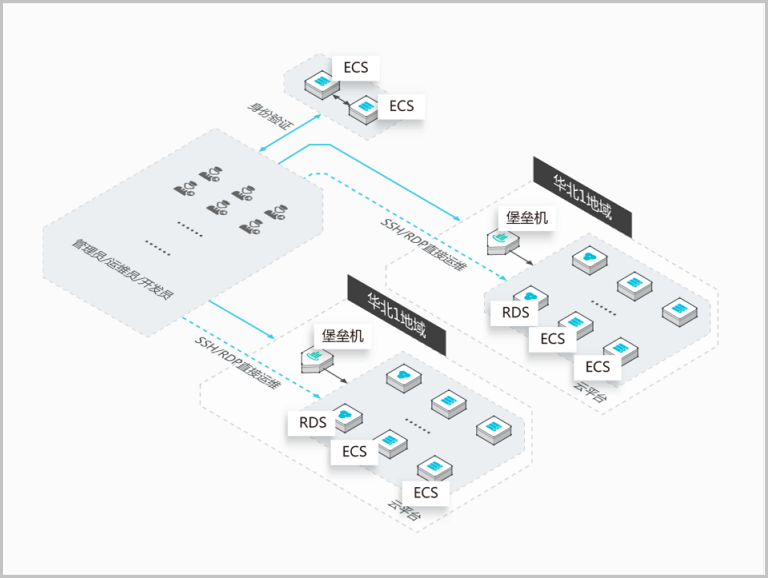
**高效运维**

从架构、工具、ECS接入、RDS接入等多方面提升运维效率。

* **C/S架构运维接入**：支持SSH、RDP、SFTP协议。
* **多运维工具**：支持PuTTY、SecureCRT、Xshell、WinSCP、mstsc等工具。
* **ECS高效接入**：支持一键同步并导入ECS实例。
* **RDS高效接入**：支持一键同步并导入RDS专有主机组。

堡垒机具备操作审计、权限控制、安全认证、高效运维等功能，能满足企业多方面进行运维管理的需求。本文介绍堡垒机的典型应用场景。

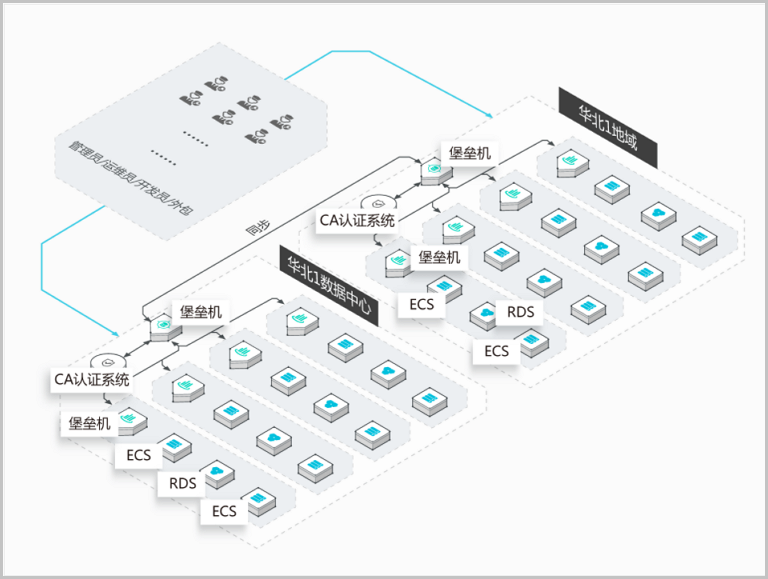
**审计合规要求严格**

例如金融保险行业企业，面临行业高规格的安全监管要求，需要建立完善的审计机制。[](https://static-aliyun-doc.oss-cn-hangzhou.aliyuncs.com/assets/img/zh-CN/4888478851/p3721.png)

通过在云平台部署堡垒机服务，能够实现以下功能：

* **部门权限隔离**： 基于部门隔离功能，实现各部门有效管理和审计。
* **统一运维入口**： 为操作人员提供统一的运维入口，解决分散登录难于管理的问题。
* **满足合规审核**： 建立健全的云上运维审核机制，满足行业监管要求。

**高效稳定的运维管理**

随着互联网行业地快速发展，更多互联网企业的人员与服务器数量增长迅速，需要高效、稳定的操作审计系统。堡垒机服务能很好地满足这些企业的运维需求。[](https://static-aliyun-doc.oss-cn-hangzhou.aliyuncs.com/assets/img/zh-CN/4888478851/p3722.png)

通过在云平台部署堡垒机服务，能够实现以下功能：

* **高并发会话**： 支撑千人级别的并发会话。
* **稳定运行**： 有高稳定性的SLA保障。
* **运维故障Review**： 运维人员在操作过程中难免发生误操作，通过审查操作内容，建立运维红线。