ALIBABA CLOUD

阿里云

堡垒机

产品简介

文档版本：20200911

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	**单击设置> 网络> 设置网络类型。**
粗体	表示按键、菜单、页面名称等UI元素。	**在结果确认页面，单击确定。**
`Courier字体`	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.什么是堡垒机

堡垒机是云盾提供的一个核心系统运维和安全审计管控平台。

云盾堡垒机集中了运维身份鉴别、账号管控、系统操作审计等多种功能。基于协议正向代理实现，通过正向代理的方式实现对SSH 、Windows远程桌面、及SFTP等常见运维协议的数据流进行全程记录，并通过协议数据流重组的方式进行录像回放，达到运维审计的目的。

堡垒机为您实现以下价值：

- 技术层三个统一
  - 统一运维入口。
  - 统一自然人与主机账号间的权限关系。
  - 统一运维操作审计管控点。
- 满足法规要求
  - 政府： 满足《等级保护》系列文件中的技术审计要求。
  - 金融： 满足金融监管部门系列文件中的技术审计要求。
  - 企业： 满足《ISO27000》系列文件中的技术审计要求。

2.产品优势

堡垒机具备审计合规、高效易用、多协议支持和追溯回放等优势。

审计合规

满足《萨班斯法案》、金融监管、《等级保护》的审计要求。

高效易用

管理界面简洁易用，支持一键同步当前阿里云帐号中的ECS云服务器和RDS专有主机组列表。

多协议支持

支持SSH、Windows远程桌面、SFTP等常见运维协议。

追溯回放

追溯运维操作的故障环节，支持在线回放操作记录。

3.功能特性

堡垒机具备操作审计、权限控制、安全认证、高效运维等功能。

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。

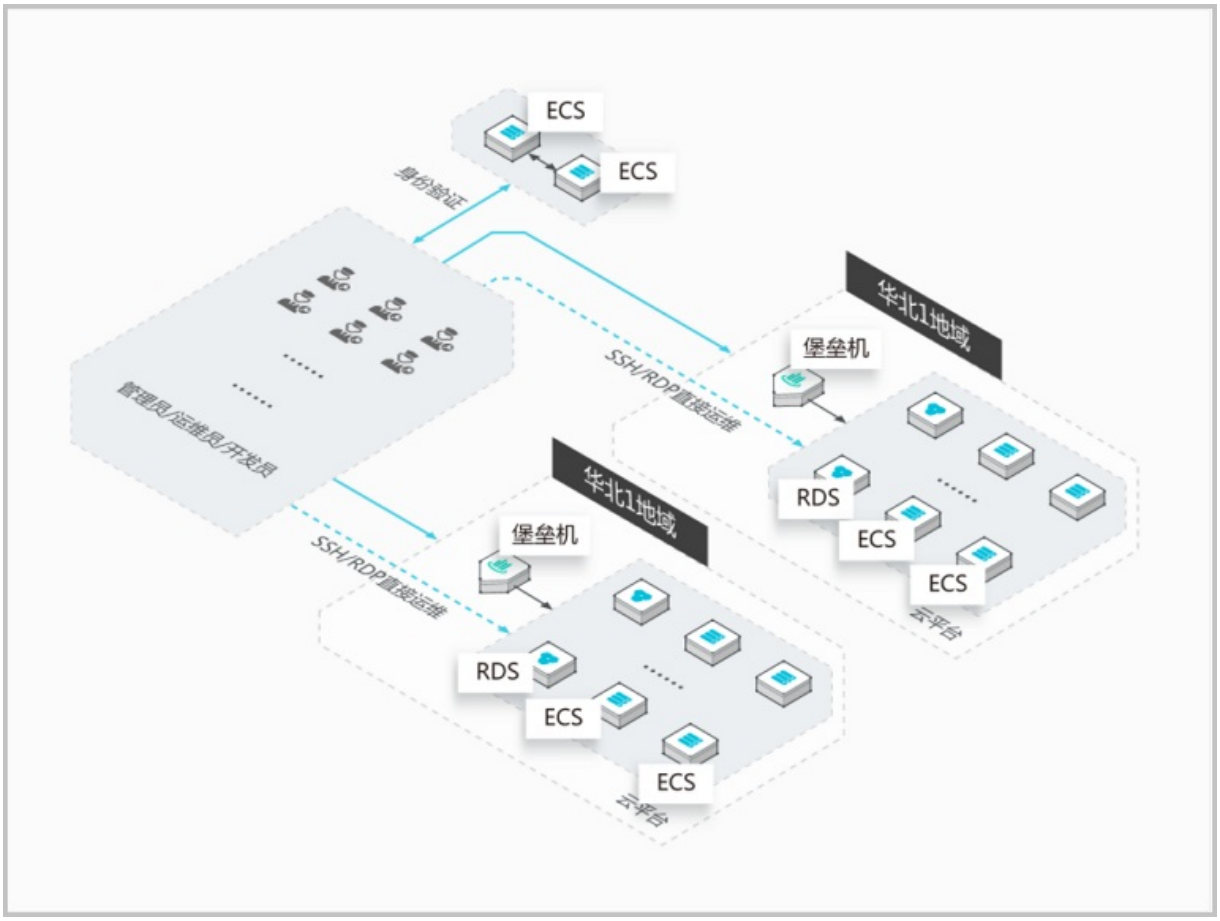
- **C/S架构运维接入**：支持SSH、RDP、SFTP协议。
- **多运维工具**：支持PuTTY、SecureCRT、Xshell、WinSCP、mstsc等工具。
- **ECS高效接入**：支持一键同步并导入ECS实例。
- **RDS高效接入**：支持一键同步并导入RDS专有主机组。

4.应用场景

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。

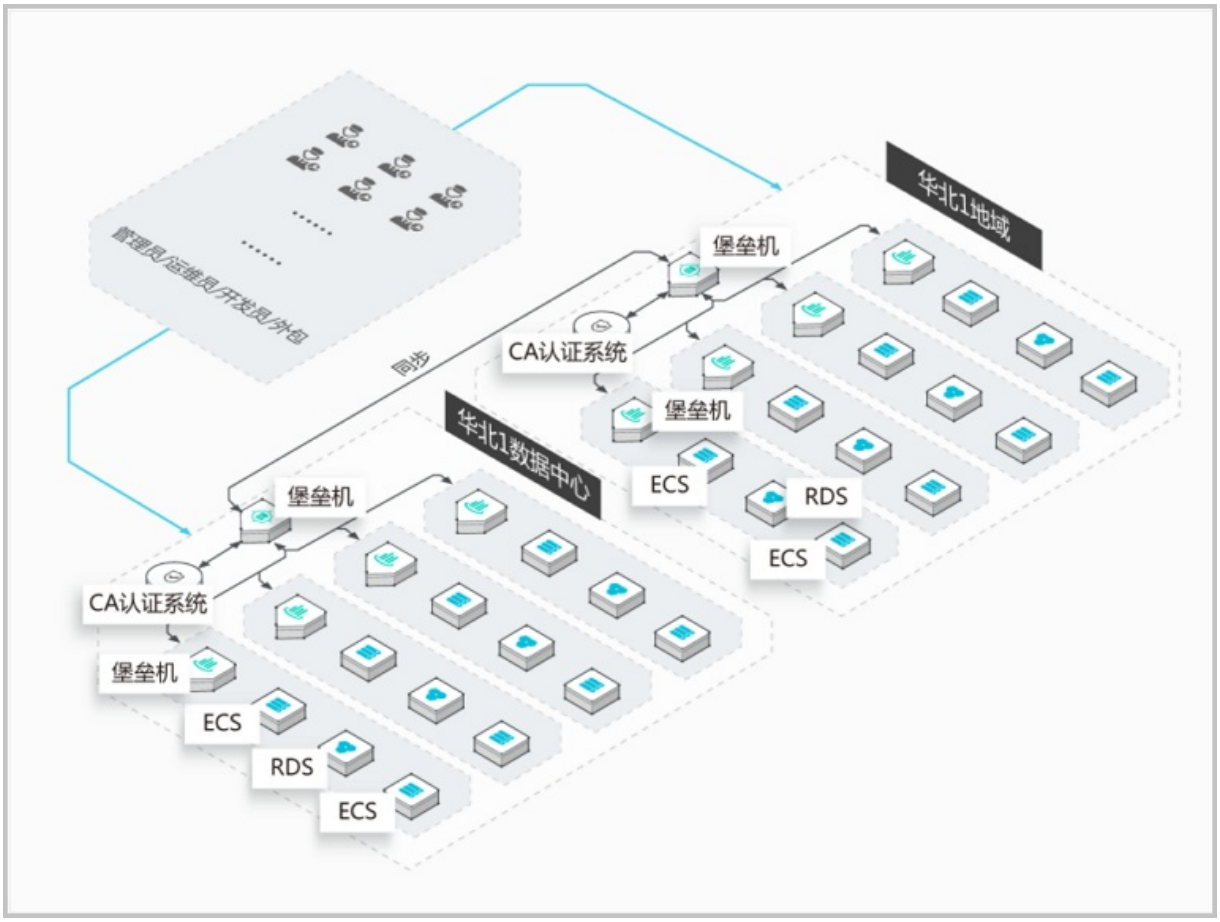


通过在云平台部署堡垒机服务，能够实现以下功能：

- **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。



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。

5.版本更新

5.1. V2版本更新说明

堡垒机V2版本镜像功能更新日志。

更新日期	新增特性

2018年5月10日	• 支持视频日志导出功能。
	• 新增自动续费功能。在购买堡垒机实例时可以勾选**自动续费**，所购买的实例将自动续费。
	  ○ 按月购买则自动续费时长为1月。
	  ○ 按年购买则自动续费时长为1年。
	• 开通**华北二阿里云政务云1**地域。
	  说明 仅供阿里云政务云用户购买使用。

2018年4月19日	堡垒机正式接入操作审计（Action Trail）服务。通过登录ActionTrail管理控制台，您可以查看最近七天内您的云账户中与创建、修改和删除堡垒机资源相关的操作记录。
2018年3月29日	• 堡垒机实例支持自定义实例名称。 • 开通中国香港、亚太东北1（东京）、亚太东南1（新加坡）、亚太东南2（悉尼）、亚太东南3（吉隆坡）、亚太东南5（雅加达）、亚太南部1（孟买）、美国东部1（硅谷）、中东东部1（迪拜）、欧洲中部1（法兰）共11个区域。
2018年1月22日	• 支持套餐规格升级。 • 优化实例释放后的展示体验。 • 优化RDP使用的文案内容。 • 修复子账号在堡垒机内无法正确禁用的问题。
2017年12月25日	• 支持配置堡垒机系统的备份与还原。 • 支持云子账号进行B/S运维- 密钥支持口令。 • 同步阿里云ECS功能位置调整。 • C/S模式的运维中，资产列表展示字段优化。
2017年11月20日	• 手动刷新ECS时超过并发限制的文案优化。 • 审计搜索文案修改。 • C/S运维服务器列表按服务器名称排序。 • 修复控制策略的访问时间段控制在特定时间段无法保存的问题。 • 修复公钥登录使用短信二次验证时会发送两次短信验证码的问题。 • 修复某些客户端公钥认证时双因子被绕过的问题。

6.版本说明

堡垒机通过不断地进行版本升级来提供更多的功能和更好的用户体验。堡垒机实例不同版本之间存在功能差异。本文介绍堡垒机实例版本与文档的对应关系。

背景信息

如果您开通了多个堡垒机实例，这些实例由于购买时间不同等原因可能会存在多个版本。您可以在云盾堡垒机控制台的实例页面查看堡垒机实例的版本。版本和文档的对应关系请参见版本及文档的对应关系。

版本及文档的对应关系

版本	快速入门	用户指南
• V3.2.10 • V3.2.11	快速入门（V3.2版本）	用户指南（V3.2版本）
• V3.1.3 • V3.1.2 • V3.0.3	快速入门（V3.1版本）	用户指南（V3.1版本）
• V2.1.7 • V2.1.6	快速入门（V2版本）	用户指南（V2版本）