云堡垒机

常见问题

文档版本 08

发布日期 2025-09-29

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 产品咨询 1
1.1 云堡垒机实例与云堡垒机系统的区别是什么? 1
1.2 云堡垒机系统有哪些安全加固措施? 1
1.3 资产数是什么? 2
1.4 并发数是什么? 2
1.5 云堡垒机支持 IAM 细粒度管理吗? 2
1.6 云堡垒机支持统一管理企业 ERP 上云、SAP 上云等业务吗? 2
1.7 自动化运维包括哪些内容? 3
1.8 如何获取企业协议号码? 3
1.9 使用堡垒机时需要配置哪些端口? 3
1.10 云堡垒机可以管理多个子网的资源吗? 5
1.11 云堡垒机支持管理哪些数据库? 5
2 区域和可用区 8
2.1 什么是区域和可用区? 8
2.2 云堡垒机可以跨账号管理资源吗? 9
2.3 云堡垒机可以跨区域或跨 VPC 网络管理主机吗? 9
2.4 云堡垒机支持在专属云上使用吗? 10
3 购买 11
3.1 购买部署相关 11
3.2 云堡垒机实例有哪些规格? 11
3.3 如何配置云堡垒机的安全组? 13
4 License 相关 15
4.1 云堡垒机是否提供第三方 License? 15
4.2 如何处理“授权 License 快到期或者已到期，需及时更新 License 许可证”的问题? 15
5 备份/变更规格/升级 18
5.1 云堡垒机支持备份哪些系统数据? 18
5.2 版本升级前，如何备份云堡垒机系统中数据? 20
5.3 堡垒机变更规格和升级是否会造成审计数据丢失 21
5.4 FTP/SFTP 远程备份失败怎么办? 22
5.5 云堡垒机如何将备份数据导入到主备实例中? 23
6 文件传输类 24

6.1 云堡垒机有哪些文件传输方式? 24
6.2 SSH 协议主机，如何使用 FTP/SFTP 传输文件? 25
6.3 通过 Web 浏览器运维，如何上传/下载文件? 26
6.4 云堡垒机的“主机网盘”是什么? 33
6.5 上传/下载文件失败怎么办? 34
6.6 如何清理个人网盘空间? 36
6.7 通过 Web 浏览器运维，提示不支持文件传输怎么办? 38
6.8 通过 Web 浏览器运维，单击“文件传输”加载不出文件列表怎么办? 38
6.9 如何配置文件管理权限? 39
6.10 云堡垒机能对上传文件进行安全检测吗? 40
7 计费、到期续费与退订 41
7.1 云堡垒机如何续费，更新授权? 41
7.2 云堡垒机支持哪些计费方式? 42
7.3 云堡垒机实例可以退订吗? 42
7.4 云堡垒机变更规格的费用如何计算? 43
7.5 云堡垒机升级版本是否收费? 43
7.6 如何增加云堡垒机实例配额? 43
7.7 提示资源售罄，如何购买云堡垒机实例? 44
8 CBH 系统登录 46
8.1 登录方式及密码类 46
8.1.1 云堡垒机可以域名登录吗? 46
8.1.2 云堡垒机系统支持哪些登录方式? 46
8.1.3 云堡垒机系统有哪些登录认证方式? 46
8.1.4 登录系统的初始密码是什么? 48
8.1.5 如何重置云堡垒机用户登录密码 48
8.2 多因子认证类 51
8.2.1 如何绑定手机令牌? 51
8.2.2 绑定手机令牌失败怎么办? 51
8.2.3 如何使用手机短信认证方式登录系统? 52
8.2.4 如何取消手机短信方式登录认证? 53
8.2.5 配置了手机令牌登录，但未绑定手机令牌怎么办? 53
8.2.6 绑定了手机令牌，却不能登录怎么办? 53
8.3 登录安全类 54
8.3.1 如何设置云堡垒机登录安全锁? 54
8.3.2 如何解锁登录云堡垒机时被锁定的用户/IP? 55
9 系统用户、资源及策略配置 56
9.1 系统用户类 56
9.1.1 在新建用户/资源时，为什么无法选择上级部门? 56
9.1.2 如何修改用户手机号码? 56
9.1.3 云堡垒机可新建多少个用户? 57
9.2 资源添加类 57

9.2.1 如何创建云堡垒机数据库运维? 58
9.2.2 如何通过云堡垒机纳管 RDS 数据库? 59
9.2.3 如何修改系统资源账户密码? 62
9.2.4 如何设置提权登录资源账户? 63
9.2.5 如何设置云堡垒机资源标签? 63
9.2.6 如何批量导入/导出主机资源? 64
9.2.7 导入云主机的访问密钥 AK/SK 是什么? 如何获取? 65
9.2.8 系统资源账户有哪些状态? 65
9.2.9 系统资源标签可以共用吗? 65
9.2.10 是否支持手动输入密码的方式登录资源? 66
9.2.11 为什么不能识别批量导入的云主机? 66
9.2.12 如何通过云堡垒机来访问内网提供的服务? 66
9.3 系统策略类 66
9.3.1 动态授权的作用及操作流程是什么? 66
9.4 系统配置类 67
9.4.1 如何配置 SSH Key 登录主机资源? 67
9.4.2 如何设置个人网盘空间大小? 69
9.4.3 如何解决短信限制问题? 70
9.4.4 CBH 如何对接三方邮箱服务器? 70
10 运维资源 71
10.1 运维管理 71
10.1.1 云堡垒机支持图形化运维 Linux 主机吗? 71
10.1.2 云堡垒机支持手机 APP 运维吗? 71
10.1.3 如何配置 SSO 单点登录工具? 71
10.1.4 云堡垒机允许多用户同时登录同一资源吗? 72
10.1.5 云堡垒机 SSH 运维支持哪些算法? 72
10.2 运维操作 74
10.2.1 云堡垒机支持哪些登录资源方式? 74
10.2.2 如何创建运维协同会话? 75
10.2.3 如何使用系统资源标签? 75
10.2.4 通过 Web 浏览器运维，如何设置会话窗口的分辨率? 76
10.2.5 通过 Web 浏览器运维，如何使用快捷键复制/粘贴文本? 77
10.2.6 云堡垒机运维，操作快捷键有哪些? 78
10.2.7 通过 Web 浏览器运维，文件列表获取失败怎么办? 79
11 审计运维日志 80
11.1 云堡垒机可提供哪些审计日志? 80
11.2 操作回放视频支持下载吗? 81
11.3 可以删除某一天的云堡垒机运维数据吗? 82
11.4 系统审计日志支持备份到 OBS 桶吗? 82
11.5 系统审计日志能保存多久? 82
11.6 系统审计日志处理机制是什么? 82
11.7 为什么视频可播放时长比总会话时长短? 83

11.8 为什么收到登录资源提示，但历史会话无登录记录？ 83
12 故障排除 84
12.1 登录系统故障 84
12.1.1 登录云堡垒机系统异常怎么办？ 84
12.1.2 登录系统，报 IP/MAC 地址不在登录范围怎么办？ 85
12.1.3 登录系统，系统提示“404：服务错误”怎么办？ 86
12.1.4 登录系统，系统提示“499：服务错误”怎么办？ 86
12.1.5 内网用户登录云堡垒机系统，可能会遇到哪些故障？ 86
12.1.6 通过堡垒机登录主机，无法正常登录怎么办？ 87
12.1.7 通过 VPN 或者 VPC Peering 打通 VPC 后，新 VPC 下的 VM 登录失败怎么办？ 87
12.2 登录资源故障 88
12.2.1 通过云堡垒机登录资源异常怎么办？ 88
12.2.2 通过 Web 浏览器登录资源，报 Code：T_514 错误怎么办？ 89
12.2.3 通过 Web 浏览器登录资源，报 Code：T_1006 错误怎么办？ 91
12.2.4 通过 Web 浏览器登录资源，报 Code：C_515 错误怎么办？ 92
12.2.5 通过 Web 浏览器登录资源，报 Code：C_519 错误怎么办？ 94
12.2.6 通过 Web 浏览器登录主机资源，报 Code：C_769 错误怎么办？ 96
12.2.7 运维资源列表可登录资源不可见怎么办？ 98
12.2.8 通过 Web 浏览器登录资源，不弹出会话界面怎么办？ 99
12.2.9 应用运维异常，调用程序失败怎么办？ 100
12.2.10 SSO 工具异常，不能登录数据库资源怎么办？ 101
12.2.11 通过堡垒机登录服务器资源，报“并发会话超出许可限制”怎么办？ 102
12.2.12 如何解决“mstsc 客户端访问服务器资源时鼠标出现黑块”的问题？ 102
12.2.13 访问 Windows 应用发布服务器，提示“创建用户失败”怎么办？ 102
12.3 运维故障 103
12.3.1 登录云堡垒机实例时，收不到短信验证码怎么办？ 103
12.3.2 无法添加资源，提示“资源超出许可限制”怎么办？ 104
12.3.3 主机资源账户验证不通过怎么办？ 104
12.3.4 打开系统数据文件显示乱码怎么办？ 105
12.3.5 运维会话经常提示登录超时，断开连接怎么办？ 105
12.3.6 应用运维调用 PL/SQL 客户端，文本乱码了怎么办？ 106
12.3.7 登录主机资源后，提示“拒绝请求的会话访问”怎么办？ 106
12.3.8 云堡垒机带宽超限了怎么办？ 107
12.3.9 通过 Web 浏览器运维，不能复制文本怎么办？ 107
12.3.10 资源运维过程有哪些常见报错？ 108
12.3.11 堡垒机 IP 绑定域名，再将域名添加到 WAF 中进行防护，添加完成后访问不成功怎么处理？ 111
12.3.12 应用运维登录后显示本次链接已断开怎么处理？ 111
12.3.13 跨版本升级之后证书状态异常怎么处理？ 111
12.4 SSO 运维故障 112
12.4.1 DBeaver 配置自定义驱动连接 GaussDB 数据库 112
12.4.2 配置 DBeaver 连接 GaussDB 数据库 113

12.4.3 mysql 协议访问数据库，执行备份数据库表提示 1251-lost connection to mysql server during query 114
12.4.4 mysql 主机运维失败，提示：1251-Client does not support authentication protocol requested by server..... 114
12.4.5 访问 mysql 协议主机失败，提示：“2013-Lost connection to MySQL server at ‘waiting for initial communicationpacket system error0”..... 115
12.4.6 Oracle 协议访问数据库提示：ORA-12537_TNS_连接关闭..... 115
12.4.7 Oracle 协议访问数据提示：ORA-12637_包接收失败..... 115
12.4.8 主机运维 Oracle 失败，提示：ora 12170 TNS 连接超时..... 117
12.4.9 主机运维调用 DBeaver 连接 Postgres 数据库失败..... 118
12.4.10 SSO 拉起客户端失败，主机运维后提示：运行环境缺少 jre..... 118

1 产品咨询

1.1 云堡垒机实例与云堡垒机系统的区别是什么?

一个云堡垒机实例代表了一个独立运行的云堡垒机系统。

用户可以登录CBH服务控制台，然后在控制台申请和管理实例。

云堡垒机系统是云堡垒机实际运维功能核心，后台采用华为云欧拉操作系统，包含用户管理、资源管理、策略、审计和工单等功能模块，支持对Windows或Linux等操作系统的主机提供安全管控保护。

1.2 云堡垒机系统有哪些安全加固措施?

云堡垒机有完整的安全生命周期管理，从系统开发过程的安全编码规范，到经过严格安全漏洞扫描、渗透测试等安全性测试，并通过了公安部门的安全检测，符合“网络安全法”等法律法规，满足合规性规范审查要求，达到信息安全等级评定Ⅲ级标准。

系统数据安全

- 登录安全：镜像加密，SSH远程登录安全加固，内核参数安全加固，系统账户口令使用强密码并且默认登录失败超过3次将锁定登录。
- 数据安全：敏感信息加密存储，系统根密钥独立动态生成。
- 应用安全：防SQL注入攻击、防CSV注入攻击、防XSS恶意攻击、API接口认证机制。

系统安全

- 系统全自动化安装，LUKS加密用户系统数据盘。
- 系统自带防火墙功能，防止常规网络攻击，例如暴力破解等。
- 统一HTML5方式访问入口，仅开放一个系统Web访问端口，减少攻击面。
- 针对SSH登录参数配置加固，提高SSH登录系统的安全性。

1.3 资产数是什么?

资产数表示云堡垒机管理的虚拟机等设备上运行的资源数，资源数是同一个虚拟机对应的需要运维的协议和应用总数，可在**桌面看板**查看不同类型资产数。

受CBH资产版本规格限制，CBH系统管理的资源总数，不能超过当前版本规格的**资产数**。

资产数不以CBH系统所管理虚拟机等设备的数量计算，而是以所管理虚拟机上资源的数量计算，一个虚拟机内可能有多种资源形式，包括不同协议的主机，不同类型的应用等。

例如，目前有一台虚拟机，在云堡垒机中添加这台虚拟机的资源，分别添加了2个RDP、1个TELNET和1个MySQL协议的主机资源，以及1个Chrome浏览器的应用资源，那么当前管理的资产数即为5，而不是1。

1.4 并发数是什么?

并发数是指云堡垒机上同一时刻连接的运维协议连接数。

云堡垒机系统对登录用户数没有限制，可无限创建用户。但是同时刻不同用户连接协议总数，不能超过当前版本规格的**并发数**。

例如，10个运维人员同时通过云堡垒机运维设备，假设平均每个人产生5条协议连接（例如通过SSH客户端、MySQL客户端进行远程连接），则并发数等于50。

1.5 云堡垒机支持 IAM 细粒度管理吗?

支持。

统一身份认证（Identity and Access Management，IAM）是华为云提供权限管理的基础服务。默认情况下，新建的IAM用户没有任何权限，您需要授权IAM用户后，IAM用户才可以基于已有权限对云服务进行操作。CBH服务已开通IAM细粒度权限管理功能，通过IAM权限管理，可对CBH实例的购买、升级、变更规格等关键操作进行细粒度授权。

此外，CBH系统管理和运维资源，在云堡垒机系统内配置“用户登录限制”、“访问控制策略”等，细粒度管理用户访问、操作资源的权限。但该功能是CBH系统本身的权限管理功能，IAM不为CBH系统提供权限管理功能。

1.6 云堡垒机支持统一管理企业 ERP 上云、SAP 上云等业务吗?

支持。

云堡垒机与云上业务网络通畅情况下，可通过安装应用发布服务器，依赖Windows系统的远程桌面服务，接入ERP生产系统、ERP容灾系统、SAP生产系统、SAP开发/测试系统、SAP Router、SAP Hybris等典型场景的应用、数据库或网页，将ERP和SAP上云业务作为一个网页或应用来审计和录屏操作，实现对企业上云业务的统一管理。

1.7 自动化运维包括哪些内容?

云堡垒机“专业版”支持自动化运维功能，可将复杂运维精准化和效率化。自动化运维主要包括资源账户同步、脚本线上管理、多资源快速运维，以及多步骤自动运维。

- 资源账户同步：通过账户同步功能，可以实现对主机上资源账户的有效监管，及时发现僵尸账户或未纳管账户，加强对资产的管控。

  详细操作请参见**账户同步策略**。
- 脚本线上管理：支持管理Python和Shell两种脚本格式，通过导入脚本文件或在线编辑脚本，在云堡垒机系统一体化管理和运行脚本。

  详细操作请参见**脚本管理**。
- 多资源快速运维：支持快速将命令或脚本在多个SSH协议资源上执行，并根据发起的命令和脚本，返回相应执行结果；此外，还支持将一个或多个文件上传到多个资源上，并返回文件上传结果。

  详细操作请参见**快速运维**。
- 多步骤自动运维：支持分步骤同时对多个SSH协议资源批量执行多种运维操作，可同时运维操作包括执行命令、执行脚本、传输文件。运维任务执行后，按照步骤顺序依次自动执行操作，并返回执行结果。

  详细操作请参见**运维任务**。

1.8 如何获取企业协议号码?

用户在配置云堡垒机安装远程桌面服务，创建一个应用发布服务器时，需要输入企业协议号码授权，企业协议号非免费提供套件。

云堡垒机不提供企业协议号，应用发布服务器为第三方管理插件，企业协议号需要客户自行申购。类似于客户申购了Windows系统，但Office套件并非免费提供，需要客户单独申购。

1.9 使用堡垒机时需要配置哪些端口?

为了能正常使用堡垒机，实例和资源安全组端口配置可参考**表1-1**。

⚠ 注意

- 堡垒机跨版本升级会自动开放80、8080、443、2222共四个端口，升级完成后若不需要使用请第一时间关闭。
- 堡垒机主备实例跨版本升级还会自动开放22、31036、31679、31873共四个端口，升级完成后保持31679开放即可，其余端口若不需要使用请第一时间关闭。

表 1-1 入/出方向规则配置参考

场景描述	方向	协议/应用	端口
通过Web浏览器登录堡垒机（HTTP、HTTPS） **说明** ● 若使用HTTPS协议，只需配置443端口。 ● 因HTTP会自动跳转到HTTPS，若使用HTTP协议，则需同时配置80和443端口，否则自动跳转不会生效。	入方向	TCP	80、443
通过MSTSC客户端登录堡垒机	入方向	TCP	53389
通过SSH客户端登录堡垒机	入方向	TCP	2222
通过FTP客户端登录堡垒机	入方向	TCP	2121、20000-21000
通过SFTP客户端登录堡垒机	入方向	TCP	2222
通过堡垒机的SSH协议远程访问Linux云服务器	出方向	TCP	22
通过堡垒机的RDP协议远程访问Windows云服务器	出方向	TCP	3389
通过堡垒机访问Oracle数据库	入方向	TCP	1521
	出方向	TCP	1521
通过堡垒机访问MySQL数据库	入方向	TCP	33306
	出方向	TCP	3306
通过堡垒机访问SQL Server数据库	入方向	TCP	1433
	出方向	TCP	1433
通过堡垒机访问DB数据库	入方向	TCP	50000
	出方向	TCP	50000
通过堡垒机访问GaussDB数据库	入方向	TCP	18000
	出方向	TCP	8000、18000
License注册许可服务器	出方向	TCP	9443
华为云服务	出方向	TCP	443
同一安全组内通过SSH客户端登录堡垒机	出方向	TCP	2222
短信服务	出方向	TCP	10743、443
DNS域名解析	出方向	UDP	53

场景描述	方向	协议/应用	端口
通过堡垒机访问PGSQL数据库	入方向	TCP	15432
	出方向	TCP	5432
通过堡垒机访问DM数据库	入方向	TCP	15236
	出方向	TCP	5236
通过堡垒机访问Redis数据库	入方向	TCP	16379
	出方向	TCP	6379
通过SSH隧道运维数据库	入方向	TCP	62222

1.10 云堡垒机可以管理多个子网的资源吗?

可以。

子网是属于VPC的资源，同一VPC内的子网可以进行通信，即云堡垒机可以直接管理同一VPC多个子网内的资源，且同一VPC不同子网下的云堡垒机可以通信。

堡垒机和主机必须要在同一个区域，同一个VPC下，具体的限制请参考**网络使用限制**。跨VPC的子网默认不能通信，虽可通过创建**对等连接**使不同VPC的子网通信，但受限于跨VPC场景下网络的复杂性和网段冲突的可能性，不建议跨VPC使用云堡垒机管理资源。

1.11 云堡垒机支持管理哪些数据库?

云堡垒机支持通过**主机运维**或**应用运维**两种方式管理数据库，可管理多种协议类型的云上数据库。主机运维方式提供增删改查操作命令审计。应用运维方式提供操作会话视频审计。

说明

- **标准版**仅支持应用运维方式，不支持直接运维数据库，需要建立应用发布服务器才可以运维数据库。
- **专业版**支持主机运维和应用运维两种方式，支持直接运维数据库。

主机运维方式

目前云堡垒机主机运维，支持管理以下协议类型的云上数据库，包括MySQL、SQL Server、Oracle、DB2、PostgreSQL、GaussDB、DM、Redis协议类型。云堡垒机支持数据库协议类型、版本，以及支持调用的数据库客户端软件版本，请参见**表1-2**。

表 1-2 支持数据库协议类型、版本和数据库客户端

数据库类型	版本	支持调用客户端
MySQL	5.5，5.6，5.7，8.0	Navicat 11、12、15、16 MySQL Administrator 1.2.17 MySQL CMD DBeaver22、23（堡垒机V3.3.48.0及以上版本支持）
Microsoft SQL Server	2014、2016、2017、2019、2022	Navicat 11、12、15、16 SSMS 17.6、18、19
Oracle	10g、11g、12c、19c、21c	Toad for Oracle 11.0、12.1、12.8、13.2 Navicat 11、12、15、16 PL/SQL Developer 11.0.5.1790 DBeaver22、23（堡垒机V3.3.48.0及以上版本支持）
DB2	DB2 Express-C	DB2 CMD命令行 11.1.0
PostgreSQL	11、12、13、14、15	DBeaver22、23
GaussDB	2、3	DBeaver22、23
DM	DM8	DM管理工具V8（Build 2023.12.14版本支持）
Redis	5.0、6.0	redis-cli x64 5.0.9 (git:9414ab9b)

应用运维方式

云堡垒机通过应用运维方式管理数据库，支持对以下系统版本的应用进行管理：

- 支持对Windows Server2008 R2及以上的Windows系统版本的应用进行管理。

  此时，需通过在一台支持远程桌面的Windows系统上部署数据库客户端。通过Web浏览器远程登录Windows桌面并调用数据库客户端，实现云堡垒机对数据库类型应用的运维。

  云堡垒机支持直接配置并调用的Windows系统的数据库客户端如表1-3所示。Windows主机上的其他类型数据库应用，都可通过配置应用服务器类型为“Other”，实现应用运维。

  表 1-3 支持直接调用的 Windows 系统上部署的数据库客户端

应用类型	支持调用的客户端
MySQL Tool	MySQL Administrator
Oracle Tool	PL/SQL Developer

应用类型	支持调用的客户端
SQL Server Tool	SSMS
dbisql	dbisql
PostgreSQL	Navicat for PostgreSQL

- 支持对Centos7.9系统的Linux服务器的数据库应用进行管理。

⚠ 注意

Linux服务器仅支持调用达梦数据库V8的应用。

云堡垒机支持直接配置并调用的Linux服务器的数据库客户端如表1-4所示。

表 1-4 支持直接调用的 Linux 服务器的数据库客户端

应用类型	支持调用的客户端
达梦数据库	达梦管理工具V8

2 区域和可用区

2.1 什么是区域和可用区?

什么是区域、可用区?

通过区域和可用区来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- 区域（Region）：从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。
- 可用区（AZ，Availability Zone）：一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

图2-1阐明了区域和可用区之间的关系。

图 2-1 区域和可用区

如何选择区域?

选择区域时，您需要考虑以下几个因素：

- 地理位置

  一般情况下，建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。不过，在基础设施、BGP网络品质、资源的操作与配置等方面，中国大陆各个区域间区别不大，如果您或者您的目标用户在中国大陆，可以不用考虑不同区域造成的网络时延问题。

  中国香港、泰国曼谷等其他地区和国家提供国际带宽，主要面向非中国大陆地区的用户。如果您或者您的目标用户在中国大陆，使用这些区域会有较长的访问时延，不建议使用。

  - 在除中国大陆以外的亚太地区有业务的用户，可以选择“中国-香港”、“亚太-曼谷”或“亚太-新加坡”区域。
  - 在非洲地区有业务的用户，可以选择“南非-约翰内斯堡”区域。
  - 在欧洲地区有业务的用户，可以选择“欧洲-巴黎”区域。

如何选择可用区?

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

区域和终端节点

当您通过API使用资源时，您必须指定其区域终端节点。有关华为云的区域和终端节点的更多信息，请参阅**地区和终端节点**。

2.2 云堡垒机可以跨账号管理资源吗?

可以。

云堡垒机支持直接管理同一VPC内资源，即可直接访问同一VPC内资源。跨账号情况下，可通过**对等连接**，打通不同账户下两个VPC之间网络。

但受限于跨VPC场景下网络的复杂性和网段冲突的可能性，不建议跨账号使用云堡垒机纳管资源。

2.3 云堡垒机可以跨区域或跨 VPC 网络管理主机吗?

支持。

云堡垒机仅支持直接管理同一VPC内资源，即可直接访问同一VPC内资源。

虽跨区域或跨VPC可通过云服务构建网络连接，但受限于网络的不稳定性，不建议跨区域或跨VPC使用云堡垒机纳管资源。

- 跨VPC情况下，可通过**对等连接**打通两个VPC之间网络。
- 跨区域情况下，可通过**云连接（Cloud Connect，CC）**、**虚拟专用网（Virtual Private Network，VPN）**等构建跨区域网络。
- 云专线场景不支持双栈网络，vip无法连通。

2.4 云堡垒机支持在专属云上使用吗?

支持。

专属云（Dedicated Cloud）是面向企业、政府、金融等客户，提供计算、存储资源池以及网络、管控多级隔离的综合解决方案。用户独享专属资源池，与公有云资源物理隔离，满足特定性能、应用及安全合规等要求。

3 购买

3.1 购买部署相关

云堡垒机规格支持降级购买吗?

云堡垒机实例仅支持版本规格升级，不支持版本规格的回退或降级。

变更规格详细说明，请参见**变更云堡垒机规格**。

如何选择云堡垒机实例区域和可用区?

区域是一个地理区域的概念。有些国家地域面积广大，由于带宽的原因，不可能只建设一个数据中心为全国客户提供服务。因此，根据地理区域的不同将全国划分成不同的区域。选择区域时通常根据就近原则进行选择。

云堡垒机支持直接管理同一区域同一VPC下资源，同一区域同一VPC下资源可以直接访问。

因不同区域的VPC和同一区域不同VPC之间内网不互通，在购买云堡垒机实例时，建议配置云堡垒机实例与ECS等资源在同一区域同一VPC网络。此外，为降低网络时延，建议在配置实例区域的可用区时，选择与所选VPC同一区域和可用区。

若购买云堡垒机时，某个可用区无法选择（如“中国-香港”的**可用区1**），可以选择同一区域的其它可用区（如选择“中国-香港”区域的**可用区2**）。

云堡垒机创建成功后，可以删除 admin 账号吗?

系统管理员账号admin拥有系统最高操作权限，该账号是不允许删除的。

- 但是admin账号支持锁定，具体的操作方法请参见**如何设置云堡垒机登录安全锁?** 。

3.2 云堡垒机实例有哪些规格?

目前云堡垒机提供**标准版**和**专业版**两个功能版本，本文介绍各版本的功能和规格等差异，您可以根据业务需求选择相应的版本。

说明

- 云堡垒机暂不支持自定义规格，只能选择默认的版本规格。
- 华为云新用户仅能购买当前版本规格实例，已使用云堡垒机的用户可继续使用历史版本规格的实例。

实例版本规格

表 3-1 实例版本规格

版本	功能说明	版本规格
标准版	基础功能：身份认证、权限控制、账号管理、操作审计	• 10 • 20 • 50 • 100 • 200 • 500 • 1000 • 2000 • 5000 • 10000
专业版	基础功能：身份认证、权限控制、账号管理、操作审计 增强功能：云服务运维、自动化运维、数据库运维审计	• 10 • 20 • 50 • 100 • 200 • 500 • 1000 • 2000 • 5000 • 10000

表 3-2 不同规格配置说明

资产数	最大并发数	CPU	内存	系统盘	数据盘
10	10	4核	8GB	100GB	200GB
20	20	4核	8GB	100GB	200GB
50	50	4核	8GB	100GB	500GB
100	100	4核	8GB	100GB	1000GB

资产数	最大并发数	CPU	内存	系统盘	数据盘
200	200	4核	8GB	100GB	1000GB
500	500	8核	16GB	100GB	2000GB
1000	1000	8核	16GB	100GB	2000GB
2000	1500	8核	16GB	100GB	2000GB
5000	2000	16核	32GB	100GB	3000GB
10000	2000	16核	32GB	100GB	4000GB

须知

表 不同规格配置说明中的“并发数”是基于字符协议客户端运维（如SSH客户端、MySQL客户端）的并发数，基于图形协议运维（如H5 Web运维、RDP客户端运维）的并发数与分辨率、色彩度、画面动态程度强相关，基于实验室测试结果纯图形并发数只有纯字符协议并发数的1/10 ~ 1/3。

3.3 如何配置云堡垒机的安全组?

背景介绍

安全组是一个逻辑上的分组，为同一个虚拟私有云内具有相同安全保护需求并相互信任的弹性云服务器、云堡垒机等提供访问策略。

为了保障云堡垒机的安全性和稳定性，在使用云堡垒机之前，您需要设置安全组，开通需访问资源的IP地址和端口。

- 云堡垒机实例可与纳管的资源共用一个安全组，各自取用安全组规则，互不影响。
- 每个用户有一个默认安全组**Sys-default**，用户可选择**Sys-default**安全组，根据需要添加相应安全组规则。用户也可选择自定义安全组，新建安全组并添加合理安全组规则。
- **云堡垒机实例创建成功后，您可以随时修改堡垒机绑定的安全组，一台堡垒机实例最多接入5个安全组，详见更改安全组。**
- 为确保云堡垒机正常连接资源，ECS主机、RDS数据库等资源需配置合理安全组规则，放开相应网关IP和端口，并允许云堡垒机“私有IP地址”访问，资源安全组配置可参考**ECS安全组配置**。
- 云堡垒机正常使用，实例和资源安全组端口配置可参考**使用堡垒机时需要配置哪些端口?** 。

配置云堡垒机安全组

步骤1 **登录CBH服务控制台**。

步骤2 单击控制台左上角的，选择区域。

步骤3 单击“购买云堡垒机”，进入“购买云堡垒机实例”页面。

步骤4 在“安全组”参数选项框右侧，单击“管理安全组”，跳转至安全组配置页面，创建安全组和添加安全组规则。

说明

也可在“安全组”选项框内选择合理配置的安全组。

步骤5 单击“创建安全组”，创建一个新的安全组，详细指导请参见**创建安全组**。

步骤6 单击“操作”列中的“配置规则”，为安全组添加安全组规则，详细指导请参见**添加安全组规则**。

步骤7 选择“入方向规则”页签，单击“添加规则”。同理，可以添加出方向规则。

根据云堡垒机使用组网场景配置安全规则，参考**表1-1**配置。

步骤8 完成安全组规则配置，返回“购买云堡垒机服务”页面，选择指定安全组，合理配置其他参数后创建实例。

----结束

配置安全组不合理，运维故障场景

安全组配置不合理，在使用云堡垒机时可能会出现以下故障：

1. 实例许可证认证错误
   - 实例创建失败，提示“License激活失败”，可能未配置出方向TCP协议9443端口，导致网络不通获取不到许可证认证
   - 登录云堡垒机提示License过期，未配置出方向TCP协议9443端口，导致网络不通获取不到许可证认证。
2. 登录云堡垒机系统错误
   - 云堡垒机系统登录页面载入失败，提示“服务器响应时间过长”，可能未配置入方向TCP协议443端口；
   - 云堡垒机系统页面无法正常显示，可能未配置入方向TCP协议443端口，导致Web浏览器不能正常登录系统。
3. 主机资源验证错误
   - 在资源中添加主机时，提示“主机不可达”，可能未配置入方向TCP协议3389端口，导致不能远程连接云服务器；
   - 添加主机时验证账户密码，提示“主机不可达”，可能未配置入方向ICMP协议，导致外网ping不通主机资源。
4. 云堡垒机访问资源错误
   - 在登录云资源时，提示“连接错误”，可能未配置入方向TCP协议3389端口，导致不能远程连接云服务器；
   - 使用云堡垒机登录云主机黑屏，无法正常显示，可能未配置入方向TCP协议3389端口，导致不能远程连接云服务器；
   - 云堡垒机使用过程中上报514错误，提示“由于服务器长时间无响应，连接已断开，请检查您的网络并重试（Code：T_514）”，可能未配置入方向TCP协议2222端口。

4 License 相关

4.1 云堡垒机是否提供第三方 License?

不提供。

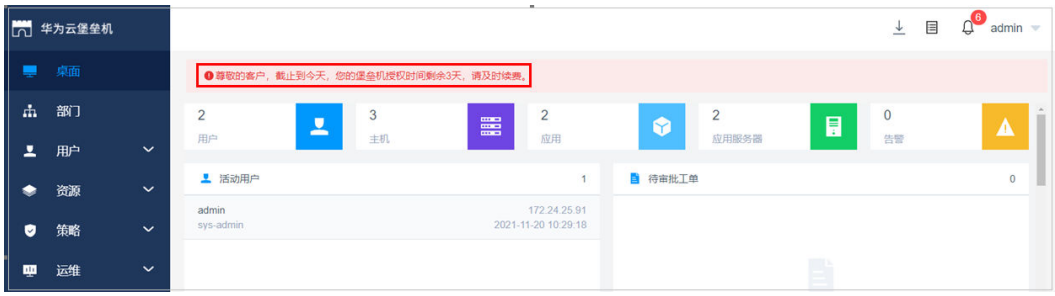
云堡垒机有Navicat等第三方插件相关的功能，若用户通过Navicat等第三方插件进行数据库等资产管理，由于Navicat属第三方应用，云堡垒机不提供相应License认证，需要单独联系Navicat申请License。

4.2 如何处理“授权 License 快到期或者已到期，需及时更新 License 许可证”的问题?

当堡垒机即将过期提示更新授权或者堡垒机已过期提示更新授权时，需要通过控制台为堡垒机实例续费获取新的授权许可证文件，更新许可证。

现象

现象一：堡垒机实例即将到期



现象二：堡垒机实例已到期

前提条件

- 拥有CBH操作权限。
- 已放通安全组和防火墙ACL出方向9443端口，解除网络限制，否则可能导致续费更新授权失败。
- 如果您的堡垒机版本是V3.3.2.0及以下版本，需要为堡垒机实例**绑定弹性公网IP**，否则可能导致续费更新授权失败。

操作步骤

步骤1 **登录CBH服务控制台**。

步骤2 单击控制台左上角的，选择区域。

步骤3 单击待续费的实例“操作”列的“更多 > 续费”，进入“续费”配置页面。

步骤4 根据需要选择续费时长。

图 4-1 续费配置

步骤5 单击“去支付”，在支付页面完成付款。

步骤6 返回云堡垒机实例列表页面，在“计费模式”列查看授权后最新到期时间。大约5分钟后可正常登录云堡垒机系统。

说明

续费后，新的License许可证大约需5分钟自动下发授权并部署，请耐心等待。

----结束

5 备份/变更规格/升级

5.1 云堡垒机支持备份哪些系统数据?

为加强对数据的容灾管理，云堡垒机支持**手动备份**和**自动备份**，提高审计数据安全性和系统可扩展性。

版本升级前，如何备份云堡垒机系统中的数据，请参考**版本升级前，如何备份云堡垒机系统中数据?** 。

手动备份

通过手动导出/下载各功能模块数据文件保存在本地，可手动备份日志请参见**表5-1**。

说明

系统内导出的csv文件，用Excel打开可能会乱码。若出现乱码情况，请先修改文件编码格式再打开文件，详细说明请参考**为什么打开CBH系统数据文件显示乱码?**

表 5-1 支持导出或下载的数据

数据信息	导出	下载	格式	说明
用户	支持	-	CSV	不支持导出“用户密码”、“手机号码”和“邮箱”信息。
动态令牌	支持	-	CSV	-
主机	支持	-	CSV	-
应用发布服务器	支持	-	CSV	-
应用发布	支持	-	CSV	-
资源账户	支持	-	CSV	-
访问控制策略	支持	-	CSV	-

数据信息	导出	下载	格式	说明
改密策略	-	支持	CSV	支持密码验证后，下载单个“改密策略”执行日志。
账户同步策略	-	支持	CSV	“专业版”支持下载单个“账户同步策略”执行日志。
快速运维	支持	-	CSV	“专业版”支持导出单个“快速运维”执行日志。
运维任务	支持	-	CSV	“专业版”支持导出单个“运维任务”执行日志。
历史会话	支持	支持	CSV，MP4	支持导出多条历史会话，同时支持生成并下载单个会话视频。
系统日志	支持	-	CSV	-
运维报表	支持	-	PDF、DOC、XLS、HTML	“运维报表”支持文本格式导出。
系统报表	支持	-	PDF、DOC、XLS、HTML	“系统报表”支持文本格式导出。 不支持导出系统权限配置报表。
系统配置	-	支持	bak	• 支持备份并还原当前“系统配置”信息，下载的备份文件仅能用于还原当前系统配置。 • 不支持导出系统权限配置数据。 • 支持设置“自动备份”，每天零点备份前一天系统配置。

自动备份

通过配置日志备份，用户可将登录日志、关键操作日志等压缩成tar文件后，分别远程备份到本地/Syslog/FTP/SFTP服务器，以及远程备份存储到OBS桶中。

表 5-2 支持配置备份的数据

备份方式	数据信息	说明
本地下载备份	系统登录日志、资源登录日志、命令操作日志、文件操作日志、双人授权日志	可选择时间范围备份日志，并下载保存到本地。
远程备份至Syslog服务器	系统登录日志、资源登录日志、命令操作日志、文件操作日志、双人授权日志	Syslog服务器配置成功后，历史日志记录全量远程备份。当有新日志记录时，实时启动备份。

备份方式	数据信息	说明
远程备份至FTP/SFTP服务器	系统配置、会话回放日志	• FTP/SFTP服务器配置成功后，每天零点备份前一天日志数据。 • 此外可选择需备份日期，立即将数据备份至服务器。
远程备份至OBS服务器	系统配置、会话回放日志	• 远程备份至OBS桶配置成功后，每天零点备份前一天日志数据。 • 此外可选择需备份日期，立即将数据备份至OBS桶。

5.2 版本升级前，如何备份云堡垒机系统中数据?

当云堡垒机系统有新版本时，用户为使用优化或新增的系统功能，用户需对系统进行**版本升级**。

需备份数据

版本升级前，为实现新云堡垒机系统中复用数据信息，用户需在系统升级前手动备份系统数据，系统升级完成后再导入备份数据。

针对不同的数据信息，用户需分别进行导出/导入操作，才能完成所有数据的备份。

表 5-3 版本升级需备份数据

数据信息	导出	导入	说明
用户	√	√	无法导出“用户密码”。升级完成后，可选择重置用户密码。
资源账户	√	√	为防止资源账户信息丢失，建议单独备份和还原资源账户文件。
审计数据	√	×	审计数据无法重新导入到系统，需全量备份审计数据，主要包括历史会话、会话视频、系统登录日志、系统操作日志、运维报表和系统报表。 • “运维报表”和“系统报表”支持文本格式导出。 • “历史会话”支持导出MP4格式会话视频。
系统配置	√	√	“系统配置”信息包含全量系统配置数据。

备份操作示例

以备份“资源账户”数据信息为例，介绍如何导出和导入系统数据。

步骤1 登录需要备份的云堡垒机系统。

步骤2 导出升级前系统数据信息。

在“资源账户”页面，单击“导出”，导出全部用户信息Excel表。

说明

- 若勾选特定信息，再单击“导出”，即导出指定数据信息。若不勾选，则导出全部数据信息。
- 导出“主机”信息，会将“主机”下所有的“资源账户”一同导出。
- 导出“应用发布”信息，会将“应用发布”下所有的“资源账户”信息一同导出。

步骤3 升级版本。

步骤4 对比Excel表模板。

重新登录云堡垒机新版本系统，在“资源账户”页面，单击“导入”，在导入页面单击“单击下载”，下载新系统Excel表模板。

对比版本升级前后系统Excel表，查看两个Excel表中格式是否一致。若不一致，修改升级前系统Excel表格式。

步骤5 导入修改后Excel表。

在“资源账户”页面，单击“导入”，在导入页面单击“单击上传”，将修改后Excel表导入到新系统。

说明

- 若升级前系统配置了“部门”信息，需首先在新系统中配置相应部门结构，再导入数据信息。
- **系统配置**文件无需修改操作，直接上传原系统备份文件，即可恢复系统配置。

步骤6 刷新“资源账户”信息列表，查看已成功导入的数据信息。

----结束

5.3 堡垒机变更规格和升级是否会造成审计数据丢失

堡垒机变更规格和升级软件版本，正常情况下，都不会造成审计数据丢失。

但是变更规格和升级有失败的风险，因此，在变更规格前必须备份数据，以防因变更规格/升级失败而影响数据的使用。

变更规格前后的注意事项

- 变更规格前

  用户必须在变更规格前备份数据，因变更规格有失败风险，以防因变更规格失败而影响使用，备份说明请参见**版本升级，如何备份云堡垒机系统中数据？**。

  若需变更规格到**专业版**，变更规格前请确保当前软件版本在3.2.16.0及以上，否则变更规格后的增强功能不生效。若软件版本在3.2.16.0以下，请先**升级软件版本**，再变更规格升级云堡垒机规格。查看云堡垒机当前版本，请参见**关于系统**的设备系统。

- 变更规格中

  变更规格过程约需要30min，变更规格期间云堡垒机系统不可用，业务中断，但不影响主机资源运行。建议用户不要登录云堡垒机系统进行操作，以免重要数据丢失影响使用。

- 变更规格后

  变更规格只对数据盘进行变更规格，不会影响系统盘。变更规格到新版本后，后台为用户变更规格CPU、内存、带宽等，不影响原有EIP的使用。

升级前后的注意事项

- 升级前

  为防止因升级失败而影响使用，建议升级前备份数据。

- 升级中

  版本升级过程约需要30min，版本升级期间云堡垒机系统不可用，但不影响主机资源运行。但在升级期间，建议用户不要登录云堡垒机系统进行操作，以免重要数据丢失。

- 升级后

  版本升级完成后会自动“重启”云堡垒机，重启完成后，即可使用云堡垒机。

  版本升级后用户可正常继续使用原有配置和存储数据，升级不影响系统原有配置和存储数据。

相关问题

- **云堡垒机支持备份哪些系统数据?**
- **版本升级前，如何备份云堡垒机系统中数据?**

5.4 FTP/SFTP 远程备份失败怎么办?

问题现象

- 云堡垒机配置了FTP/SFTP远程备份，报“请检查服务器密码或网络连接情况”错误，不能启动远程备份。
- 选择备份具体某一天日志，提示“备份正在执行”，但远程服务器未接收到该备份文件。

可能原因

原因一：云堡垒机配置的FTP/SFTP服务器账户或密码错误，导致远程备份失败。

原因二：云堡垒机与FTP/SFTP服务器的网络连接不通，导致远程备份失败。

原因三：FTP/SFTP服务器用户目录限制文件上传，导致远程备份失败。

原因四：被选择日期当天的运维日志量大，备份传输速率慢，长时间未备份完成，导致在远程服务器不能及时查看备份文件。

解决办法

原因一：

- 登录ECS管理控制台，VNC方式登录一台Linux主机，通过Linux主机登录FTP/SFTP服务器，验证服务器账户和密码。验证成功后，重新配置FTP/SFTP服务器远程备份账户和密码，尝试备份。

原因二：

- 登录云堡垒机系统，通过网络诊断，检查与FTP/SFTP服务器之间网络连接情况。
  - 网络连接正常，请排查其他可能原因。
  - 网络连接异常，请参考CBH安全组规则，检查云堡垒机和FTP/SFTP服务器主机安全组是否放开22端口；检查FTP/SFTP服务器主机的ACL是否放开22端口，并添加云堡垒机公网IP（即弹性IP）为允许。

原因三：

- 开启用户目录上传权限。
- 登录云堡垒机系统，选择“系统 > 数据维护 > 日志备份”，重新正确配置FTP/SFTP服务器的“存储路径”。

  说明

  “存储路径”置空表示备份内容存放到FTP/SFTP服务器用户的主目录下，例如绝对路径/**home/*用户名***；配置的路径需以英文句号开头，例如配置路径为 **./*test*/*abc***，则其绝对路径为/**home/*用户名*/*test*/*abc***。

原因四：

- 请您耐心等待，建议备份启动后的第二天再查看服务器上备份文件。

如果通过上述排查，仍然无法使用FTP/SFTP远程备份，请联系技术支持处理。

5.5 云堡垒机如何将备份数据导入到主备实例中?

CBH暂不支持将备份数据导入到主备实例。

请关注后续功能迭代刷新。

6 文件传输类

6.1 云堡垒机有哪些文件传输方式?

云堡垒机支持文件传输功能，以及审计传输的文件。Linux主机和Windows主机的文件传输方式有所区别。

Linux 主机

Linux主机上传/下载文件，可选择Web运维和FTP/SFTP客户端运维两种方式，具体的操作方法请参见**Linux主机中文件的上传/下载**。

- Web运维

  需先将Linux主机配置为SSH协议主机资源。

  通过Web运维登录目标Linux主机，可在会话窗口“文件传输”页面，执行上传/下载操作，实现本地与目标主机间文件的直接传输。也可经个人网盘“中转”，实现目标主机与其他主机间文件的间接传输。

  说明

  Web运维不支持执行**rz**/**sz**命令上传/下载文件。

- FTP/SFTP客户端运维

  需先将Linux主机配置为FTP、SFTP协议主机资源。

  通过客户端工具登录目标Linux主机，可在会话窗口执行**rz**/**sz**命令传输文件。

Windows 主机

Windows主机上传/下载文件，仅可选择Web运维方式。

需先将Windows主机配置为RDP协议主机资源。

通过Web浏览器登录目标Windows主机，可在会话窗口“文件传输”页面，执行上传/下载操作，经个人网盘“中转”，打开Windows服务器磁盘目录，对G盘上文件进行上传下载操作，即可实现Windows主机的文件传输。

说明

个人网盘在Windows主机上的默认路径为NetDisk G盘。

更多文件传输说明，请参见如下文档：

- **通过Web运维，如何上传/下载文件?**
- **SSH协议主机，如何使用FTP/SFTP传输文件?**

6.2 SSH 协议主机，如何使用 FTP/SFTP 传输文件?

运维员**admin_A**需要利用FTP/SFTP客户端，向云堡垒机已纳管的SSH协议主机**HOST_A**传输文件。

前提条件

- 系统要求：目标设备支持SFTP/FTP协议。
- 防火墙要求：开放2222(堡垒机SFTP协议)端口、2121(堡垒机FTP协议)端口。

配置 HOST_B 资源

云堡垒机管理员用户为运维员**admin_A**配置主机**HOST_B**运维的权限。

步骤1 选择“资源 > 主机管理”。

步骤2 单击“新建”，新建一个FTP/SFTP协议主机**HOST_B**。

- “协议类型”选择FTP或SFTP。为了提高安全性，建议采用SFTP。
- “主机地址”配置为**HOST_A**的主机地址。
- 其他参数值均参考**HOST_A**进行设置。即**HOST_A**和**HOST_B**实际指向同一台主机，只是协议类型不同。

步骤3 选择“策略> 访问控制策略”，将新创建的主机**HOST_B**授权给运维员**admin_A**。

----结束

SFTP/FTP 传输文件

运维员**admin_A**登录云堡垒机，通过**HOST_B**资源传输文件。

步骤1 选择“运维 > 主机运维”。

步骤2 单击主机**HOST_B**对应的“登录”。

步骤3 打开本地FTP/SFTP客户端，参考弹出窗口填写登录信息。

步骤4 成功登录主机**HOST_B**，即可进行文件传输。

说明

- FTP/SFTP登录密码即为运维员**admin_A**登录云堡垒机的密码。
- 登录云堡垒机的注意事项请参考**通过FTP/SFTP/SCP客户端登录**。

----结束

6.3 通过 Web 浏览器运维，如何上传/下载文件?

通过Web运维支持“文件传输”功能，在Web浏览器会话窗口上传/下载文件。不仅可实现本地与主机之间文件的传输，同时可实现不同主机资源之间文件的相互传输。CBH系统详细记录传输文件的全过程，可实现对文件上传/下载的审计。

“主机网盘”是为CBH用户定义的系统个人网盘，可作为不同主机资源间文件的“中转站”，暂存用户上传/下载的文件，且个人网盘中文件内容对其他用户不可见。

“主机网盘”与系统用户直接匹配，删除用户后，个人网盘中文件将被清空，个人网盘空间将被释放。

约束限制

- Linux系统目前仅支持SSH协议主机通过Web运维上传/下载文件。
- Windows系统目前仅支持RDP协议主机通过Web运维上传/下载文件。
- Web运维不能通过执行**rz**/**sz**命令等方式上传/下载文件，仅能通过“文件传输”操作上传/下载文件。

  说明

  Linux主机资源支持在客户端执行命令方式传输文件，例如在SSH客户端执行**rz**/**sz**命令上传/下载文件。但该方式不能被CBH系统记录上传/下载的具体文件，不能达到对全程安全审计的目的。
- 支持下载一个或多个文件，不支持下载文件夹。
- 不支持断点续传，文件上传或下载过程请勿终止或暂停。
- 不支持传输超大文件，建议分批次上传/下载文件，传输的文件大小不超过1G。

前提条件

- 已获取主机资源文件上传/下载权限。
- 已获取主机资源运维的权限，能通过Web浏览器正常登录。

Linux 主机中文件的上传/下载

Linux主机资源上传/下载文件不依赖个人网盘，可直接实现与本地的文件传输。个人网盘可“中转”来自其他主机资源的文件。

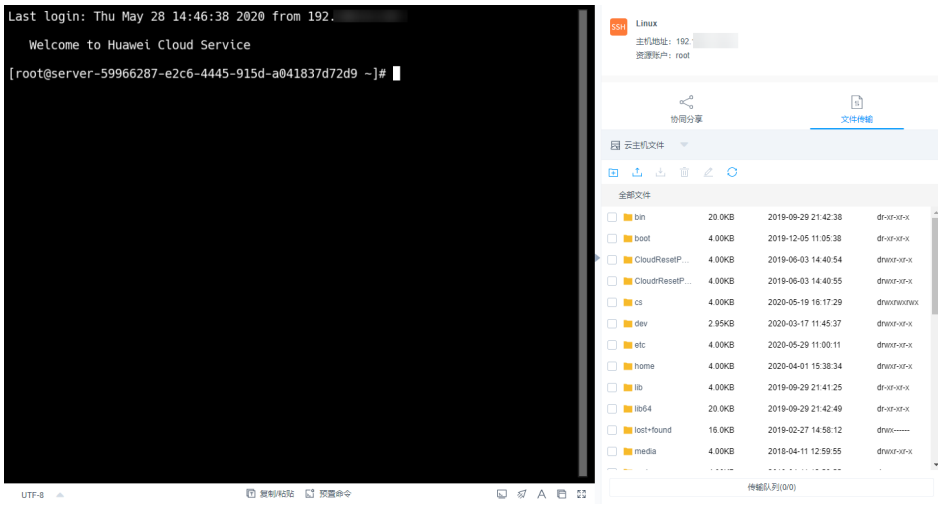
步骤1 登录云堡垒机系统。

步骤2 选择“运维 > 主机运维”，选择目标Linux主机资源。

步骤3 单击“登录”，跳转到Linux主机资源运维界面。

步骤4 单击“文件传输”，默认进入Linux主机文件列表。

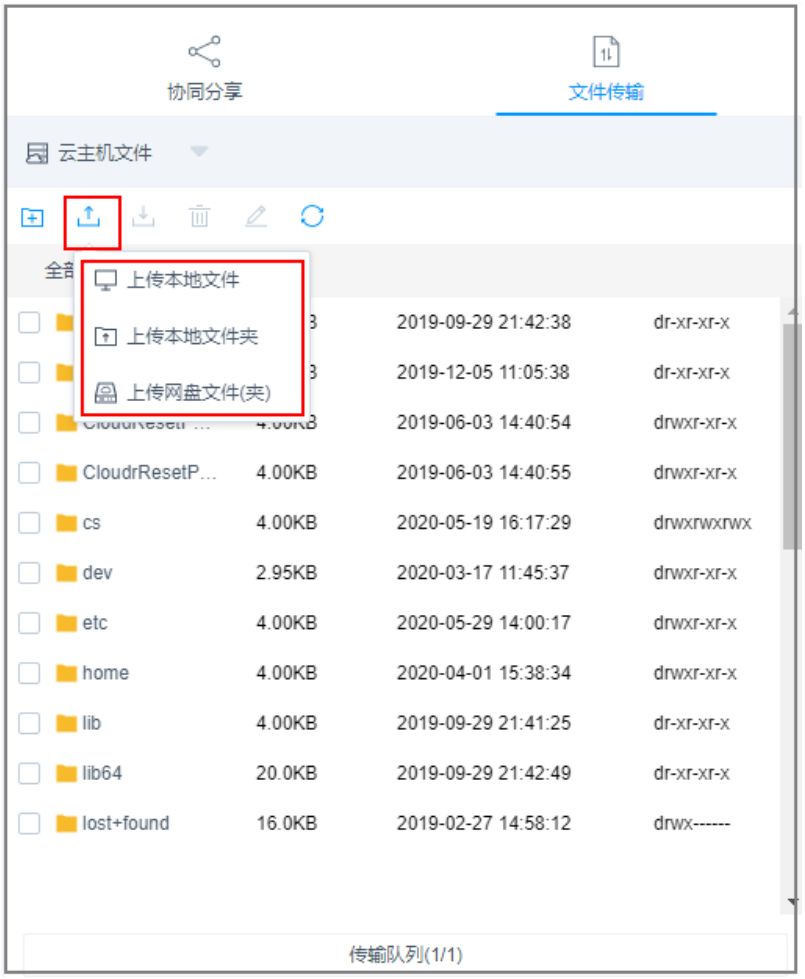
图 6-1 Linux 主机文件传输页面



步骤5 上传文件到Linux主机。

单击上传图标，可选择“上传本地文件”、“上传本地文件夹”、“上传网盘文件（夹）”，可分别上传一个或多个来自本地或个人网盘的文件（夹）。

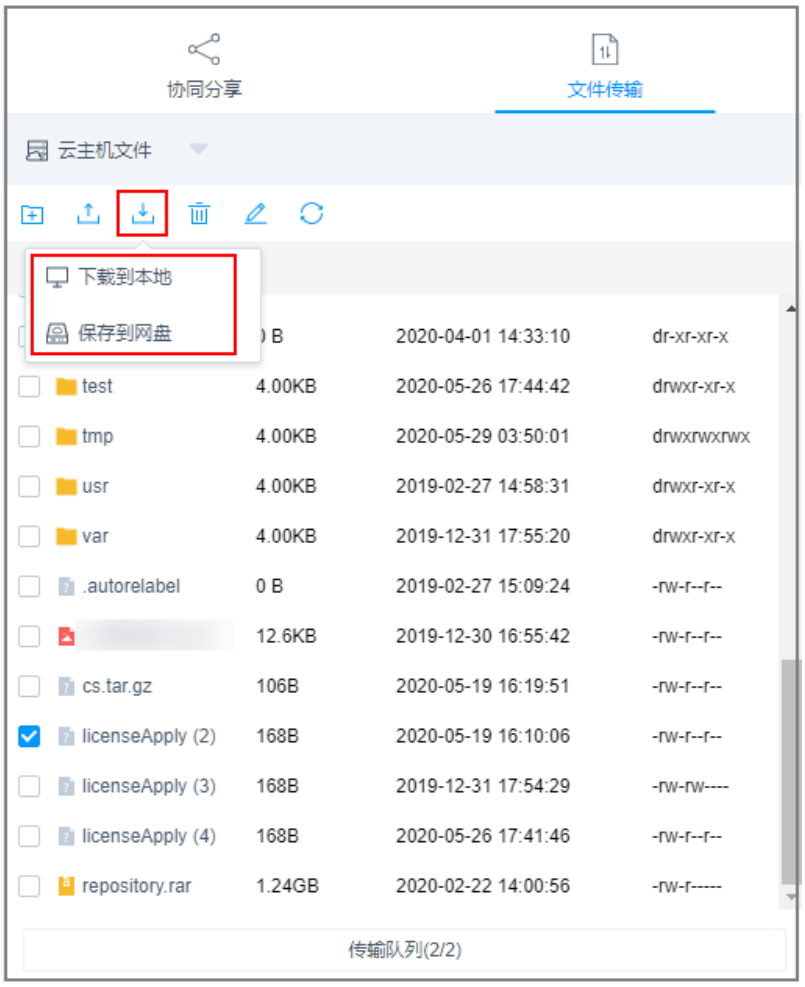
图 6-2 上传文件到 Linux 主机



步骤6 下载Linux主机中文件。

1. 选中一个或多个待下载文件。
2. 单击下载图标，可选择“下载到本地”、“保存到网盘”，可分别下载一个或多个文件到本地或个人网盘。

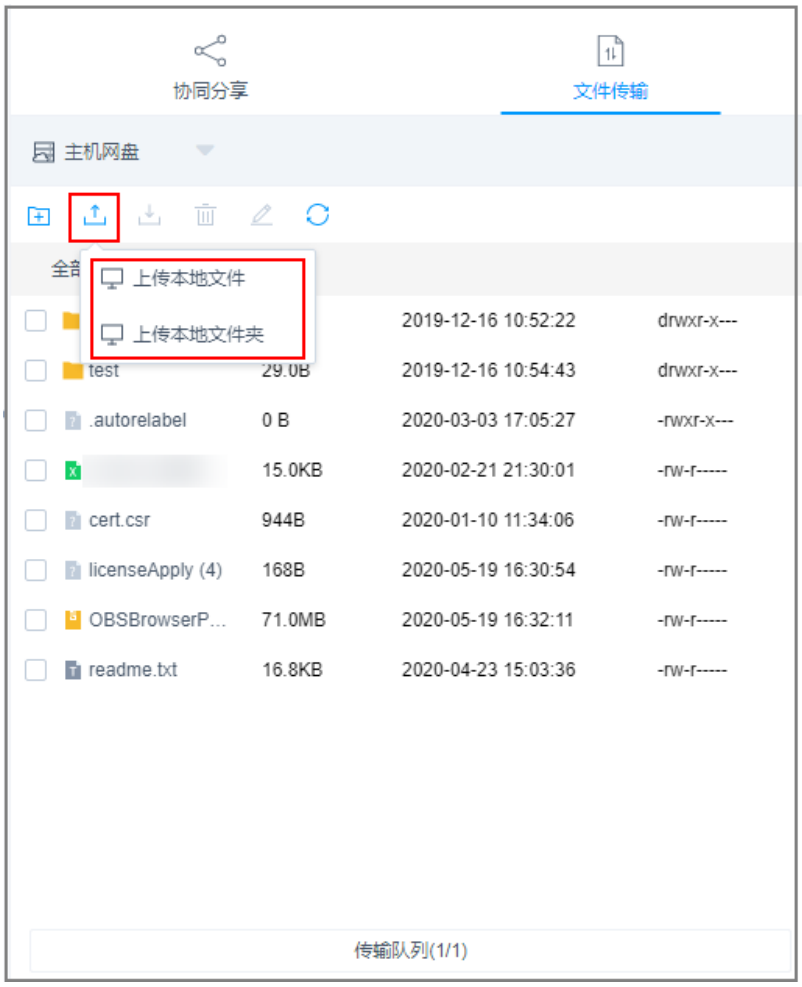
图 6-3 下载 Linux 主机中文件



步骤7 上传文件到个人网盘。

1. 单击“云主机文件”，选择“主机网盘”，切换到个人网盘文件列表。
2. 单击上传图标，可选择“上传本地文件”、“上传本地文件夹”，可上传一个或多个来自本地的文件或文件夹。

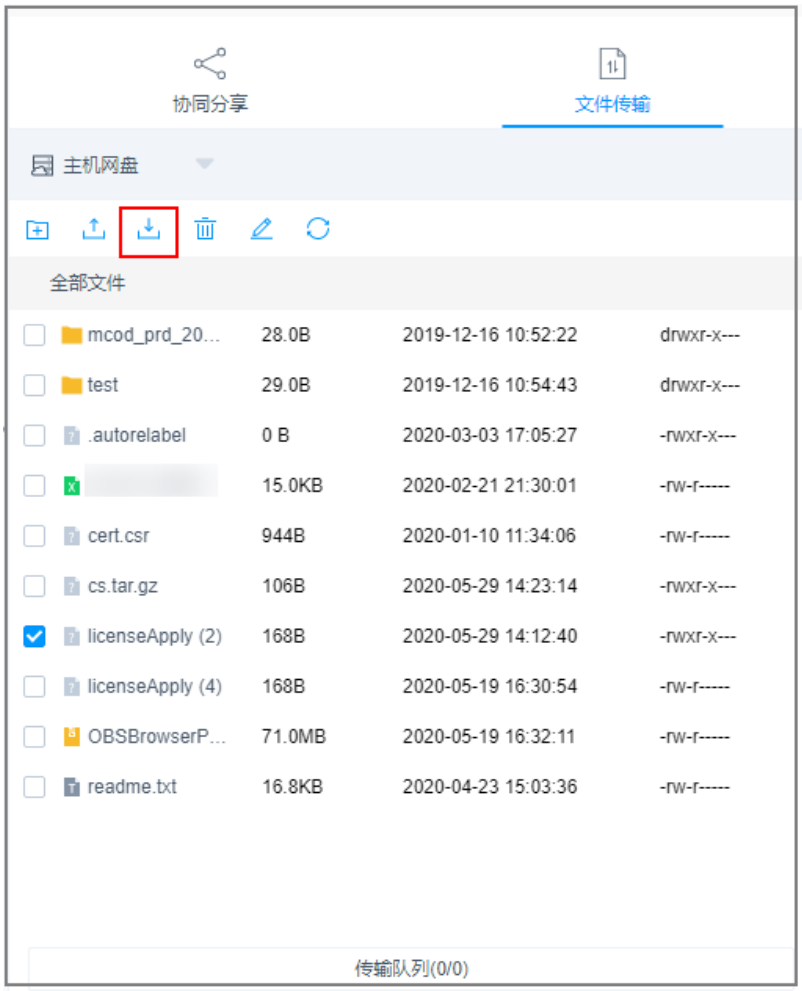
图 6-4 上传文件到个人网盘



步骤8 下载个人网盘中文件。

1. 选中一个或多个待下载文件。
2. 单击下载图标，直接下载一个或多个文件到本地。

图 6-5 下载个人网盘中文件



----结束

Windows 主机中文件的上传/下载

通过CBH运维Windows主机资源，个人网盘在Windows主机上的默认路径为NetDisk G盘，该磁盘即为当前用户的个人网盘。

Windows主机资源不能直接与本地进行文件传输，必须依赖于个人网盘的“中转”才能实现文件的传输。

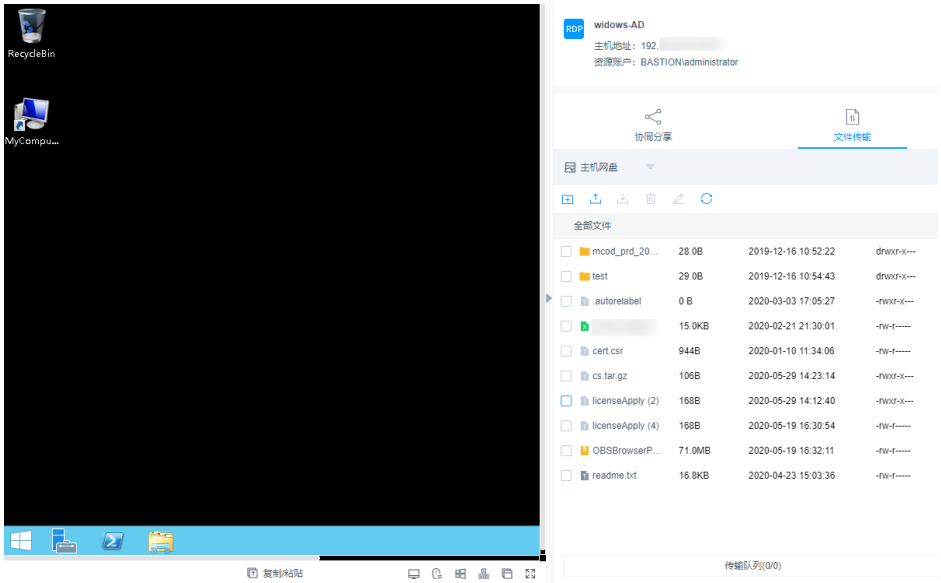
步骤1 登录云堡垒机系统。

步骤2 选择“运维 > 主机运维”，选择目标Windows主机资源。

步骤3 单击“登录”，跳转到Windows主机资源运维界面。

步骤4 单击“文件传输”，默认进入个人网盘文件列表。

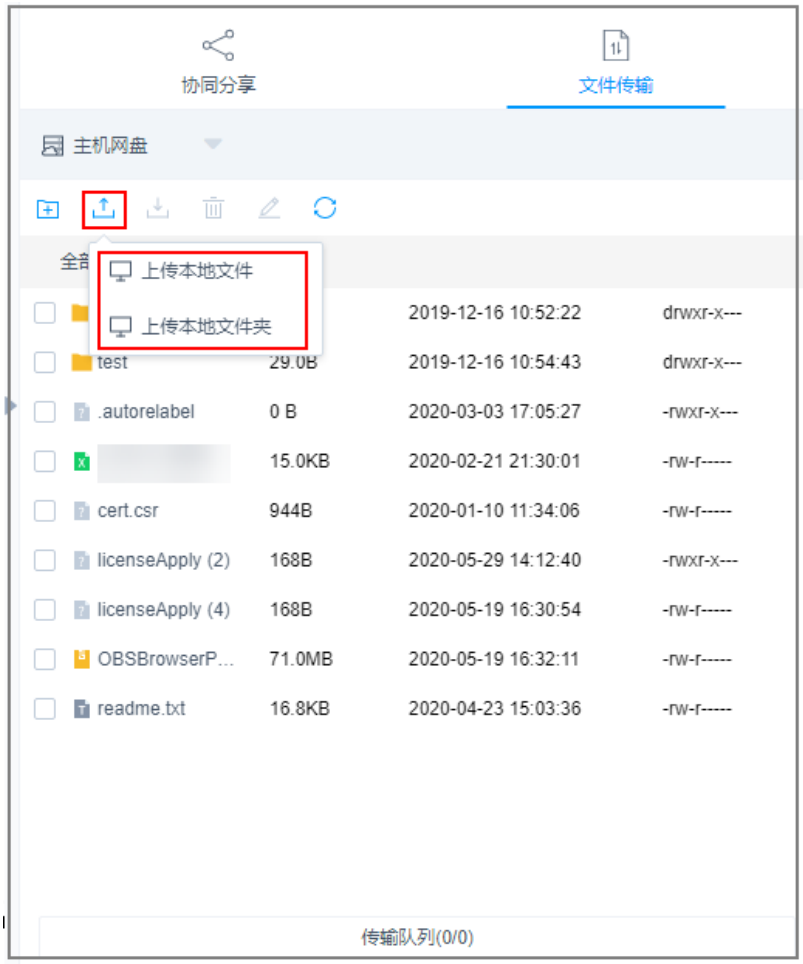
图 6-6 Windows 主机文件传输页面



步骤5 上传文件到Windows主机。

1. 单击上传图标，可选择“上传本地文件”、“上传本地文件夹”，可上传一个或多个来自本地的文件或文件夹。
2. 打开Windows主机的磁盘目录，查找G盘NetDisk。
3. 打开NetDisk磁盘目录，鼠标右键复制目标文件（夹），并将其粘贴到Windows主机目标目录下，实现将文件上传到Windows主机。

图 6-7 上传文件到个人网盘



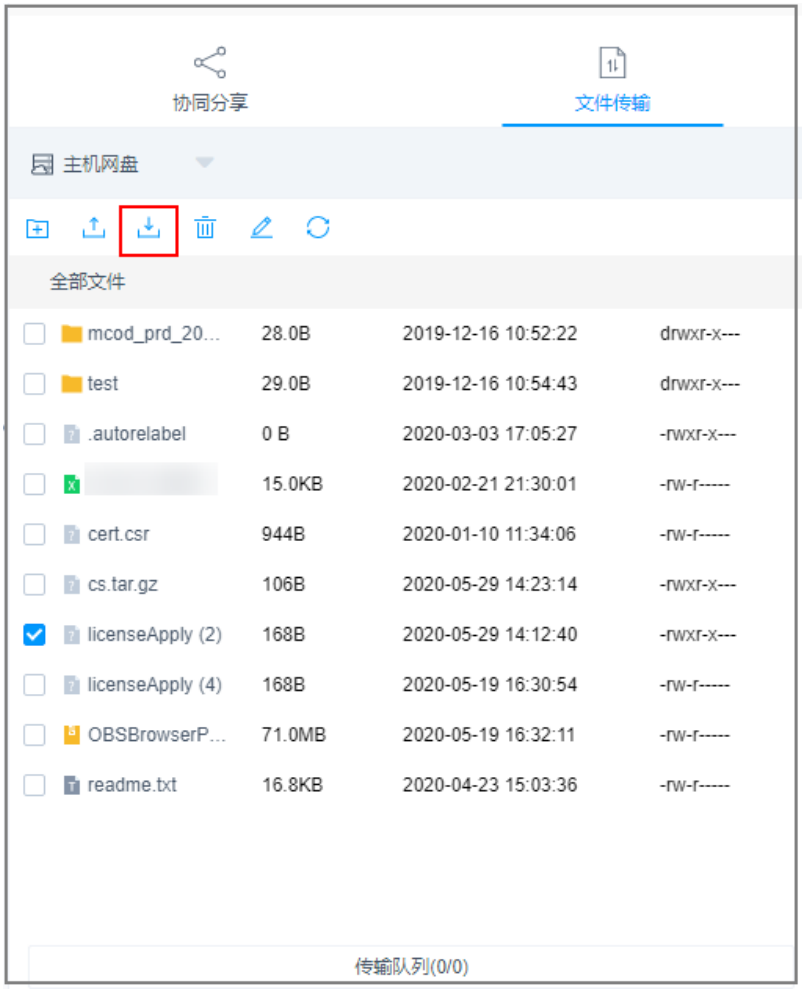
步骤6 下载Windows主机中文件。

1. 打开Windows主机的磁盘目录，鼠标右键复制目标文件（夹）。
2. 打开NetDisk磁盘目录，鼠标右键粘贴文件（夹）目录下，实现将Windows主机文件下载到个人网盘。

步骤7 下载个人网盘中文件。

1. 选中一个或多个待下载文件。
2. 单击下载图标，直接下载一个或多个文件到本地。

图 6-8 下载个人网盘中文件



----结束

上传/下载失败的处理办法

参见**上传/下载文件失败怎么办?** 进行排查解决。

6.4 云堡垒机的“主机网盘”是什么?

云堡垒机“主机网盘”是系统用户的个人网盘，可作为用户传输文件的“中转站”，暂存用户上传/下载的文件。

- 系统用户私有个人网盘空间。网盘中内容仅用户自己可见，对系统其他用户不可见。
- 与系统用户直接关联。用户被删除后，个人网盘中数据将被清空，个人网盘内存将被释放。
- 可用内存大小为系统配置的“个人网盘空间”大小。

  系统所有用户的已使用个人网盘空间，不能超过系统配置的“网盘总空间”大小。

使用限制

- 不支持用户自定义个人网盘空间大小，仅能由系统管理员设置“个人网盘空间”，为系统用户分配相同大小的个人网盘空间。
  详情请参见**如何设置个人网盘空间大小?**
- 不支持查询个人网盘已使用内存大小。
- 不支持设置定期清理，用户仅能通过手动删除文件来清理空间。

更多关于“主机网盘”的使用说明，请参见**通过Web运维，如何上传/下载文件?**

6.5 上传/下载文件失败怎么办?

通过 Web 运维上传下载失败

问题现象

- 下载“云主机文件”到“主机网盘”，即下载文件到用户个人主机网盘时，提示下载失败错误。
- 上传文件失败，提示“/3.0/h5FileService/upload-403：服务错误，请稍后重试”。
- 从本地上传文件到“主机网盘”，即上传到用户个人主机网盘时，提示“个人网盘空间不足，请清理网盘或联系管理员增加网盘空间”或“网盘存储空间不足”。
- 上传/下载大文件失败。
- 客户使用debian+rdp协议上传文件失败。
- 客户使用zoc客户端工具上传文件失败。

排查思路及解决办法

图 6-9 排查思路图

表 6-1 解决办法

排查步骤	可能的原因	解决办法
排查堡垒机的版本是否是最新的版本	堡垒机版本太低	对堡垒机进行升级，具体操作请参见**升级版本**。
排查待上传/下载的文件是否打包成压缩文件	堡垒机不支持下载文件夹， 需要把文件夹打包成压缩文件才可以上传/下载。	把文件夹打包成压缩文件，再进行上传/下载。
排查是否配置了上传/下载权限	未开启资源“文件管理权限”，也未授权用户“文件管理”的上传/下载权限。	1. **开启资源“文件管理”权限**。 2. **授权用户“文件管理”的上传/下载权限**。
排查浏览器的缓存空间	浏览器的缓存空间不足	用户手动清理浏览器缓存空间后，再次上传。
排查“个人网盘空间”是否还有可存储容量	“个人网盘空间”即磁盘，不支持自动定期清理，“个人网盘空间”容量小，个人网盘空间不足，系统剩余可用磁盘存储空间不足。	• 用户手动清理用户个人主机网盘文件，释放出可用空间。 • 管理员用户重新**设置个人网盘空间**。 • 受限于云堡垒机“数据分区”空间大小，当上传/下载的文件大小大于剩余“数据分区”空间时，请管理员用户先**清理系统空间**或**变更版本规格**。
排查上传/下载的文件是否太大	上传/下载的文件太大	• 用户将大文件切割成1G左右的小文件，分批次上传/下载。 • 受限于云堡垒机“数据分区”空间大小，当上传/下载的文件大小大于剩余“数据分区”空间时，请管理员用户先**清理系统空间**或**变更版本规格**。
排查Web登录超时时间配置是否不合理	上传/下载大文件耗时较长，且Web登录连接超时，导致上传/下载超大文件失败。	• 用户上传/下载过程中不定时返回上传/下载界面，保持云堡垒机在操作状态。 • 管理员用户修改Web登录超时时间。 • 管理员用户重新**设置个人网盘空间**。

排查步骤	可能的原因	解决办法
排查客户端使用的协议和上传工具是否与云堡垒机兼容	云堡垒机暂不支持debian+rdp协议和zoc工具上传/下载文件。	使用云堡垒机支持的协议以及对应的客户端工具上传/下载文件： • **SFTP协议**：Xftp 6及以上、WinSCP 5.14.4及以上、FlashFXP 5.4及以上 • **FTP协议**：Xftp 6及以上、WinSCP 5.14.4及以上、FlashFXP 5.4及以上、FileZilla 3.46.3及以上
排查主机SCP命令是否正常可用	未安装SCP	需要在ECS的服务器配置中安装SCP。

通过 SSH 客户端运维上传/下载失败

问题现象

在Xshell客户端上，登录云堡垒机运维SSH协议主机资源，不能正常调用Xftp客户端传输文件。

可能原因

云堡垒机SSH客户端运维限制调用工具进行文件传输，即SSH客户端运维不支持文件传输功能和审计传输的文件。

解决办法

- 重新配置一个同“主机地址”的FTP/SFTP协议主机资源，通过FTP/SFTP客户端运维进行文件传输。

  例如，配置SFTP协议主机资源并授权访问控制权限后，直接在Xftp客户端上，登录云堡垒机运维配置的主机资源，即可实现上传/下载文件。
- 通过Web运维SSH协议主机资源，实现上传/下载文件操作。

更多Web运维文件传输说明，请参见**通过Web运维，如何上传/下载文件？**。

更多SSH协议主机资源文件传输说明，请参见**SSH协议主机如何使用FTP/SFTP传输文件?**

如果通过上述排查，仍然无法上传/下载文件，请单击控制台右上方的“工单”，填写工单反馈问题现象，联系技术支持。

6.6 如何清理个人网盘空间?

云堡垒机“主机网盘”是系统用户的个人网盘，暂不支持设置定期清理。

管理员可通过手动删除过期或废弃的文件，来清理个人网盘空间。

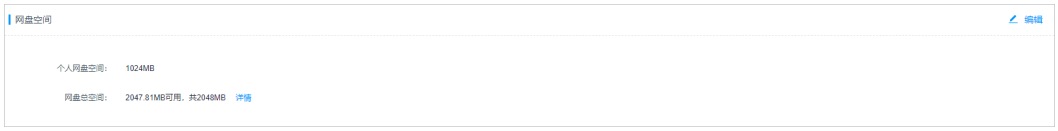
删除某个用户所有的网盘空间

步骤1 登录云堡垒机系统。

步骤2 选择“系统 > 数据维护 > 存储配置”，进入系统存储配置管理页面。

步骤3 展开网盘空间，即可查看设置的“个人网盘空间”和“网盘总空间”。

图 6-10 网盘空间



步骤4 单击“详情”，进入网盘详情页面。

步骤5 在目标网盘所在行的“操作”列，单击“删除网盘数据”，可以清理个人网盘空间。

说明

勾选多个需要删除的网盘数据，单击“删除网盘数据”，可批量清理个人网盘数据。

----结束

删除部分网盘空间

Linux主机

步骤1 登录云堡垒机系统。

步骤2 选择“运维 > 主机运维”，选择目标Linux主机资源。

步骤3 单击“登录”，跳转到Linux主机资源运维界面。

步骤4 单击“文件传输”，默认进入Linux主机文件列表。

步骤5 单击“云主机文件”，选择“主机网盘”，切换到个人网盘文件列表。

步骤6 勾选一个或多个文件或文件夹，单击删除图标，可删除文件或文件夹。

----结束

Windows主机

步骤1 登录云堡垒机系统。

步骤2 选择“运维 > 主机运维”，选择目标Windows主机资源。

步骤3 单击“登录”，跳转到Windows主机资源运维界面。

步骤4 单击“文件传输”，默认进入个人网盘文件列表。

步骤5 勾选一个或多个文件或文件夹，单击删除图标，可删除文件或文件夹。

----结束

相关操作

- 如何修改网盘空间大小?
- 云堡垒机的“主机网盘”是什么?

6.7 通过 Web 浏览器运维，提示不支持文件传输怎么办?

问题现象

通过Web浏览器登录Linux主机资源，选择“文件传输”页签，提示“当前主机不支持文件传输功能”，无法查看文件目录。

可能原因

Linux主机systemd-logind服务异常，影响SSH服务正常使用，导致文件传输功能不能被识别。

解决办法

步骤1 检查SSH服务是否正常。

在运维会话窗口，执行**systemctl status sshd.service**命令，查看服务状态。

- 若回显信息如下，则为systemd-logind服务异常，请执行**2**。
  ```
  pam_systemd sshd:session:Failed to create session :Activation of org.....
  ```
- 若回显其他信息，请联系技术支持。

步骤2 重启Linux主机systemd-logind服务。

在运维会话窗口，执行**systemctl restart systemd-logind.service**命令，重启登录服务。

步骤3 重启Linux主机SSH服务。

在运维会话窗口，执行如下命令，重启SSH服务。

- CentOS 6

  service sshd restart
- CentOS 7

  systemctl restart sshd

步骤4 退出登录，重新通过云堡垒机登录Linux主机资源，打开运维会话窗口。

----结束

如果通过上述解决办法，若仍不能使用文件传输功能，请单击控制台右上方的“工单”，填写工单信息反馈问题现象，联系技术支持。

6.8 通过 Web 浏览器运维，单击“文件传输”加载不出文件列表怎么办?

问题现象

Web页面登录云堡垒机实例并纳管Linux服务器后 ，单击“文件传输”，加载不出文件列表（一直转圈）。

可能的原因

Linux服务器的目录下，有特殊字符（乱码）的文件或者文件夹导致的。

解决办法

检查Linux服务器目录下是否有乱码文件或者文件夹。建议将有乱码的文件名或者文件夹名进行重命名，否则无法加载出目录列表。

6.9 如何配置文件管理权限?

云堡垒机支持“文件管理”，可对纳管资源中文件或文件夹进行管理。

- 通过开启资源和访问控制策略的“文件管理”权限，用户即可对资源文件进行增删改查操作。
- 若用户需要上传或下载文件，则需要堡垒机管理员（Admin）或者堡垒机策略管理员为该用户开启访问控制策略的“上传”或“下载”权限，实现文件上传和下载功能。

约束限制

目前仅SSH、RDP和VNC协议主机资源和应用资源支持“文件管理”。

前提条件

拥有资源和访问控制策略管理权限的用户，才能配置文件管理权限。

步骤一：开启资源“文件管理”权限

主机资源和应用资源都支持“文件管理”功能，以添加主机资源**ECS1**的“文件管理”权限为例。

步骤1 登录云堡垒机系统。

步骤2 选择“主机 > 主机管理”，单击**ECS1**的名称或“管理”，进入**ECS1**详情页面。

步骤3 单击“基本信息”区域“编辑”，进入“编辑主机基本信息”窗口。

步骤4 在“更多选项”行勾选“文件管理”，单击“确认”完成设置。

----结束

步骤二：授权用户“文件管理”

通过配置访问控制策略，将资源的运维操作权限授予用户，以运维用户**User1**获取**ECS1**文件管理权限为例。

步骤1 选择“策略 > 访问控制策略”，单击“新建”，进入“新建访问控制策略”窗口。

步骤2 配置“基本信息”，开启策略“文件管理”权限。

- （可选）在“文件传输”行勾选“上传”或“下载”。
- （必选）在“更多选项”行勾选“文件管理”。

步骤3 单击“下一步”，依次关联用户**User1**和资源**ECS1**。

步骤4 单击“确认”完成配置。

----结束

权限验证

以**User1**通过云堡垒机系统登录**ECS1**，进行Web运维为例。

步骤1 **User1**登录云堡垒机系统。

步骤2 选择“运维 > 主机运维”，在**ECS1**行单击“登录”，跳转到**ECS1**运维窗口。

步骤3 单击“文件传输”，即可查看到**主机网盘**或**云主机**上文件。

说明

- **云主机**是CBH纳管的资源，用户可管理资源中文件或文件夹。
- **主机网盘**是一个系统用户的个人网盘，用户可将个人网盘作为不同主机资源间的文件“中转站”，实现纳管资源间文件的传输。

步骤4 授权了“上传”或“下载”权限的资源，单击 或 标识，可对文件进行上传或下载操作。

----结束

更多**文件管理**操作介绍请参见**Web浏览器运维**。

6.10 云堡垒机能对上传文件进行安全检测吗?

不能。

云堡垒机是运维安全管理与审计平台，不支持对上传文件进行检测。

如果上传文件失败请参见**上传/下载文件失败怎么办?** 进行排查解决。

7 计费、到期续费与退订

7.1 云堡垒机如何续费，更新授权?

为保证用户正常使用云堡垒机服务，在云堡垒机到期前或保留期期间，用户可通过手动“续费”增加授权使用期限。

- 在云堡垒机到期前，可以通过“续费”操作延长到期时间。
- 在云堡垒机到期后，通过“续费”继续使用云堡垒机。若未及时续费，则进入“保留期”将冻结云堡垒机，不能访问或使用云堡垒机。“保留期”到期仍未续订或充值，存储在云堡垒机中的数据将被删除、资源将被释放。

适用场景

- 云堡垒机实例已到期或即将到期。
- 云堡垒机系统“消息中心”提示，授权License快到期，需及时更新License许可证。
- 云堡垒机系统无法正常登录，提示需更新授权，更新License许可证。

前提条件

- 拥有CBH操作权限。
- 已放通安全组和防火墙ACL出方向9443端口，解除网络限制，否则可能导致续费更新授权失败。
- 如果您的堡垒机版本是V3.3.2.0及以下版本，需要为堡垒机实例**绑定弹性公网IP**，否则可能导致续费更新授权失败。

手动续费

步骤1 **登录CBH服务控制台**。

步骤2 单击待续费的实例，“操作”列的“更多 > 续费”，进入“续费”配置页面。

步骤3 根据需要选择续费时长。

图 7-1 续费配置

步骤4 单击“去支付”，在支付页面完成付款。

步骤5 返回云堡垒机实例列表页面，在“计费模式”列查看授权后最新到期时间。大约5分钟后可正常登录云堡垒机系统。

说明

续费后，新的License许可证大约需5分钟自动下发授权并部署，请耐心等待。

----结束

7.2 云堡垒机支持哪些计费方式?

云堡垒机服务提供包月/包年的计费方式。

在购买云堡垒机实例时，需要使用弹性云服务器的弹性IP，弹性IP需单独计费。

7.3 云堡垒机实例可以退订吗?

若用户不再有使用云堡垒机实例需求，或配置的实例VPC或安全组等信息有误，可执行退订操作。

详细退订规则请参见**云服务退订规则**。

前提条件

- 拥有CBH操作权限。
- 已使用的云堡垒机，需停止系统所有操作，解绑EIP。

退订流程

为了防止退订后，数据丢失，建议您按如下流程进行操作：

1. **退订前**，参考**维护系统配置**备份系统配置。

2. **退订**。参照**操作步骤**进行操作。
3. **还原系统配置**（可选，适用于退订后想继续使用云堡垒机，且需要还原原版本系统配置的用户）。购买同版本的云堡垒机，再参考**还原系统配置**章节还原系统配置。

说明

退订堡垒机资源后，次日凌晨3点才会自动清理残留资源，如需删除安全组需等残留资源清理后才可进行安全组的删除操作。

操作步骤

步骤1 **登录CBH服务控制台**。

步骤2 单击待退订的实例所在行，“操作”列的“更多 > 退订”。

步骤3 在弹出的“退订实例”对话框中，单击“确定”。

步骤4 在退订资源页面完成退订。

说明

弹性公网IP只解绑不释放，释放需要到弹性公网IP管理页面手动释放。

----结束

7.4 云堡垒机变更规格的费用如何计算?

云堡垒机支持在原版本上直接变更规格。

变更规格时，后台会根据**实例当前规格剩余费用**和**实例变更规格规格所需费用**之间的差值，计算为变更规格“配置费用”。

云堡垒机实例授权开放变更规格功能，并备份数据后。登录云堡垒机管理控制台，在对应实例的“操作”列单击“更多 > 变更规格”，根据需要选择目标“性能规格”，并支付变更规格“配置费用”，即可变更云堡垒机实例到新规格版本，详细操作请参见**变更版本规格**。

7.5 云堡垒机升级版本是否收费?

不收费。

云堡垒机软件版本升级免费，但规格升级（即变更规格）需要收取“变更规格配置费用”。

登录云堡垒机控制台，在对应实例的“操作”列单击“更多 > 升级”，确认“升级实例”提示后，即可升级软件版本。升级版本详细操作请参见**升级版本**。

升级软件版本后，用户需重启实例，并可根据实际需求变更规格。变更规格详细操作请参见**变更版本规格**。

7.6 如何增加云堡垒机实例配额?

目前一个华为云账户默认实例配额数为5个。

当您在购买云堡垒机实例时，界面提示配额不足，请您提交工单申请配额。

工单反馈

步骤1 登录CBH服务控制台。

步骤2 在界面右上方，选择“工单 > 新建工单”，进入“工单管理”界面。

步骤3 在“产品类”区域，单击“更多工单产品分类”，选择“安全与合规 > 云堡垒机”。

步骤4 选择问题类型后，单击“新建工单”，根据您的需求，填写相关参数。

其中，“问题描述”请填写相关内容和申请原因，提供对应区域的“项目ID”和需要增加的CBH实例配额数。

说明

“项目ID”获取方法请参考**我的凭证**。

步骤5 填写完毕后，勾选协议并单击“提交”。

----结束

7.7 提示资源售罄，如何购买云堡垒机实例?

当您在购买云堡垒机实例时，界面提示资源售罄。

- 请您单击管理控制台左上角的，选择其他区域或未售罄可用区购买。
- 您也可选择提工单反馈。

工单反馈

步骤1 登录CBH服务控制台。

步骤2 在界面右上方，选择“工单 > 新建工单”，进入“工单管理”界面。

步骤3 在“产品类”区域，单击“更多工单产品分类”，选择“安全与合规 > 云堡垒机”。

步骤4 选择问题类型后，单击“新建工单”，根据您的需求，填写相关参数。

其中，“问题描述”请填写相关内容和申请原因。

步骤5 填写完毕后，勾选协议并单击“提交”。

----结束

8 CBH 系统登录

8.1 登录方式及密码类

8.1.1 云堡垒机可以域名登录吗?

可以。

一般情况下，云堡垒机通过绑定的EIP地址登录。当企业用户有统一登录域名管理需求时，可先通过云解析服务（Domain Name Service，DNS）将域名解析为EIP，再创建云堡垒机实例绑定解析的EIP。用户可直接在浏览器中输入域名，登录云堡垒机系统。

8.1.2 云堡垒机系统支持哪些登录方式?

云堡垒机系统支持Web浏览器方式直接登录，同时支持SSH客户端方式登录。

Web浏览器方式登录，为用户提供全量云堡垒机系统配置和管理功能。SSH客户端方式登录在不改变用户原来使用SSH客户端习惯的前提下，对授权云主机资源进行运维管理，并支持多种快捷操作命令。建议管理员优先在Web浏览器为运维员完成授权配置后，运维员再在SSH客户端登录系统进行运维操作。

详细Web浏览器方式登录指导，请参考**Web方式登录云堡垒机**。

详细SSH客户端方式登录指导，请参考**SSH客户端运维**。

8.1.3 云堡垒机系统有哪些登录认证方式?

云堡垒机的认证方式是系统全局可选择设置，即系统**所有用户**都可选择认证方式，包括本地认证、多因子认证（手机令牌、手机短信、USBKey、动态令牌）、远程认证（AD域、RADIUS、LDAP、Azure AD）。

说明

- 用户账号配置多因子认证后，仅可通过多因子认证方式登录。通过登录名和密码不能登录，本地认证方式验证失效。
- 配置了多种双因子认证时，可任意选择其中一种方式登录云堡垒机系统。

本地认证

系统默认，即通过“密码登录”方式验证系统用户**登录名**和**密码**，认证登录用户身份。

手机令牌

通过“手机令牌”方式同时验证**登录名**、**密码**和**手机动态码**，认证登录用户身份。

在使用手机令牌登录前，用户需通过密码登录系统，配置手机令牌绑定方式，并绑定手机令牌。再由管理员配置用户登录认证方式，选择“手机令牌”多因子认证。

手机短信

通过“手机短信”方式同时验证**登录名**、**密码**和**短信验证码**，认证登录用户身份。

用户账号需先配置可使用手机号码，再由管理员配置用户登录认证方式，选择“手机短信”多因子认证。

USBKey

通过“USBKey”方式验证插入的USBKey和**PIN码**，认证登录用户身份。

需先申购USBKey，授权绑定，再使用USBKey进行身份认证。

动态令牌

通过“动态令牌”方式同时验证**登录名**、**密码**和**动态令牌**，认证登录用户身份。

需先申购动态令牌，授权绑定，再使用动态令牌进行身份认证。

AD 域认证

管理员配置AD系统认证方式，创建AD域认证用户或同步AD域服务器用户。使用“密码登录”方式验证AD域用户账户和密码时，通过Windows AD域服务器对系统用户进行身份认证。

基本原理：通过AD域系统终端代理使用第三方库执行认证业务。

- IP：AD域服务器的IP地址。
- 端口：根据实际情选择，默认选择389端口。
- 域：AD域的域名。

RADIUS 认证

管理员配置RADIUS系统认证方式，并创建RADIUS认证用户。使用“密码登录”验证RADIUS用户账户和密码时，通过RADIUS协议，由第三方认证服务器对系统用户进行身份认证。

基本原理：通过远程网络接入设备的**用户**，与包含用户认证和配置信息的**服务器**之间，采用**用户/服务器模式**交换信息标准，执行认证业务。

- IP：RADIUS服务器的IP地址。
- 端口：根据实际情选择，默认选择1812端口。
- 认证共享密钥：RADIUS的认证密码。

- 测试：用RADIUS的账号密码做测试。

LDAP 认证

管理员配置LDAP认证方式，并创建LDAP认证用户。使用“密码登录”验证LDAP用户账户和密码时，通过轻量级目录访问协议，由第三方认证服务器对系统用户进行身份认证。

基本原理：LDAP基于TCP/IP协议的目录访问协议，是Internet上目录服务的通用访问协议，形式一个树状目录类的数据库。

- IP：LDAP服务器的IP地址。
- 端口：根据实际情况选择，默认选择389端口。
- 用户OU：LDAP中树状形式的组织信息，DN是分支节点到根目录的路径，Base_DN则是基准DN，即LDAP搜索的起始DN为用户的组织单元ou。例如：如果开始搜索的DN的组织单元为ou1，则Base_DN为ou=ou1，o=O。

Azure AD 认证

管理员需先在Azure平台创建企业应用程序，并将平台用户加入企业应用程序；再在云堡垒机系统配置Azure AD认证，并添加Azure平台已加入应用程序的用户。使用Azure认证入口验证用户身份时，跳转到Azure登录窗口，输入用户账号和密码，由第三方认证平台验证通过后，跳转登录云堡垒机系统。

基本原理：Azure AD认证基于SAML协议，通过在Azure平台配置企业应用程序，将Azure AD用作企业使用的应用程序的标识，认证登录用户身份。

8.1.4 登录系统的初始密码是什么?

- 系统管理员**admin**用户首次登录云堡垒机的默认密码为购买实例时配置的密码。
- 其他用户首次登录的默认密码是管理员创建用户时配置的密码。

8.1.5 如何重置云堡垒机用户登录密码

所有用户首次登录云堡垒机系统时，请务必根据提示绑定手机号，以便忘记密码后重置密码。

- admin账号忘记密码，请参见**admin账号重置密码**。
- 已登录过云堡垒机且配置了手机号码的账号忘记了密码，请参见**登录页面重置密码**。
- 普通用户忘记了密码，且不记得配置的手机号码，可通过系统管理员**admin**或拥有“用户”管理权限的用户重置普通用户密码。具体的操作方法请参见**批量重置普通用户密码**。
- 已登录的用户定期修改密码，请参见**修改密码**。

约束限制

- 云堡垒机用户账号被锁定期间不支持重置密码。用户可待锁定时间到期后，再进行重置密码操作。
- 配置了AD域认证或RADIUS认证的云堡垒机用户，需在AD域或RADIUS服务器上重置密码或修改密码，不能通过云堡垒机系统重置密码、设置密码期限等用户密码管理操作。

admin 账号重置密码

仅适用于admin账号重置密码，具体的操作方法请参见**重置admin账号密码**。

登录页面重置密码

已登录过云堡垒机且配置了手机号码的账号忘记了密码可参考本章节进行重置密码。

步骤1 在云堡垒机系统登录页面，单击“忘记密码？”，进入“重置密码”页面。

步骤2 根据“重置密码”引导。确认账号信息，输入“登录名”、“手机号码”和“短信验证码”，输入的手机号码需与用户账号绑定的手机号码一致。

步骤3 确认重置密码身份。

根据提示信息，输入用户绑定的手机号码，并通过短信验证码验证身份。

若忘记手机号码，可单击“无法获取短信？”，填写系统信息尽量找回密码。

步骤4 根据密码设置要求重置和确认密码。

说明

密码设置要求：长度范围8~32个字符；需同时包含英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符，不支持空格。

步骤5 新密码设置成功后，返回登录页面输入“登录名”和“密码”，登录云堡垒机系统。

----结束

修改密码

若用户已登录云堡垒机系统，可根据需要定期修改登录密码。

步骤1 如**图8-1**示例，单击“修改密码”，弹出“修改密码”对话框。

图 8-1 云堡垒机系统修改密码

步骤2 输入“当前密码”验证，根据要求输入“新密码”，并确认新密码。

步骤3 新密码设置成功后，需退出系统，返回登录页面重新登录云堡垒机系统。

----结束

批量重置普通用户密码

系统管理员**admin**或拥有“用户”管理权限的用户，可批量为其他用户重置密码。

步骤1 登录云堡垒机系统。

步骤2 选择“用户 > 用户管理 ”，进入用户列表页面。

步骤3 选择待重置密码用户，单击“更多 > 重置密码”，弹出“重置密码”窗口。

步骤4 配置密码。

步骤5 单击“确认”，将新配置的密码分发给被重置密码的用户。

说明

- 因批量重置的用户密码相同，建议被重置密码的用户登录系统后及时修改个人密码。
- 其他任何用户都不能重置系统管理员**admin**的密码。
- 批量重置密码仅能修改其他用户密码，不能修改个人密码。
- 用户密码重置后不能明文查看和导出。

----结束

8.2 多因子认证类

8.2.1 如何绑定手机令牌?

针对某个用户配置手机令牌认证登录功能前，必须先为此用户绑定手机令牌，再由管理员配置用户手机令牌多因子认证，才能实现用户手机令牌登录验证。

说明

- 若**admin**用户已配置手机令牌登录认证，但未绑定手机令牌，请单击控制台右上方的“工单”，填写工单信息反馈问题现象，联系技术支持重置登录方式。
- 若其他用户未绑定手机令牌，无法登录系统，请先联系部门管理员取消“手机令牌”多因子登录认证。

8.2.2 绑定手机令牌失败怎么办?

问题现象

绑定手机令牌登录时，扫描二维码获取验证码，并正确输入验证码绑定到设备后，提示“绑定手机令牌失败”。

可能原因

可能因为系统时间和手机时间不一致造成。手机令牌登录方式，系统时间与必须一致，精确到秒。

解决办法

绑定失败后，请先修改系统时间与手机时间一致，刷新页面重新生成二维码绑定。具体步骤如下：

步骤1 登录堡垒机系统。

步骤2 同步时间，使系统时间与手机时间一致。

1. 左侧导航栏，选择“系统 > 系统维护”，进入系统维护页面。
2. 切换到“系统管理”页签，在“系统时间”区域查看系统时间配置。

3. 修改系统时间。
   - 手动修改：单击当前时区或当前时间后的“修改”，设置时区或时间后，单击“确定”。
   - 服务器同步：选择时间服务器后，单击“同步时间”，单击“确定”。

步骤3 重新绑定手机令牌。

1. 在堡垒机系统右上角，单击已登录用户名，选择“个人中心”，进入个人中心页面。
2. 切换到“手机令牌”页签，解除原来绑定的手机令牌后，并根据界面提示重新绑定手机令牌。

----结束

8.2.3 如何使用手机短信认证方式登录系统?

前提条件

- 已为用户账号配置手机号码，且用户手机号码可用。
- 堡垒机实例安全组必须已放开短信网关IP和10743、443端口，系统才能够访问短信网关。
- 发送短信验证码的频率未超过要求限制。

  说明

  系统短信网关配置为“内置”时，手机短信验证码针对单个账号发送频率有以下限制：
  - 1分钟内发送短信不超过1条；
  - 1小时内发送短信不超过5条；
  - 1天内发送短信不超过15条。

配置手机短信认证

步骤1 管理员登录云堡垒机系统。

步骤2 选择“用户 > 用户管理”。

步骤3 单击待修改的用户登录名，或者单击相应“管理”，进入“用户详情”页面。

步骤4 单击“用户配置”区域的“编辑”，修改用户的登录配置。

步骤5 配置“多因子认证”为“手机短信”。

步骤6 单击“确认”，完成用户“手机短信”双因子认证配置。

----结束

手机短信方式登录

修改认证配置后，用户进入云堡垒机系统登录Web页面或SSH客户端登录界面，选择“手机短信”认证方式，输入登录名和用户账号绑定手机号，获取短信验证码登录。

详细登录说明请参见**Web方式登录云堡垒机**和**SSH客户端登录**。

8.2.4 如何取消手机短信方式登录认证?

当用户短信网关故障，无法通过手机短信方式登录，可由管理员取消“手机短信”多因子认证配置。

说明

若**admin**用户配置了“手机短信”多因子认证，无法登录系统取消多因子认证配置，请联系技术支持。

前提条件

管理员已获取“用户”模块操作权限。

操作步骤

步骤1 登录云堡垒机系统。

步骤2 选择“用户 > 用户管理”，进入用户列表页面。

步骤3 勾选待修改配置的用户账号，单击左下角“更多”，展开批量操作项。

步骤4 单击“修改多因子认证”，弹出多因子认证修改窗口。

步骤5 去掉勾选“手机短信”多因子认证方式。

步骤6 单击“确定”，即关闭了目标用户“手机短信”认证方式。

----结束

8.2.5 配置了手机令牌登录，但未绑定手机令牌怎么办?

- 当系统管理员**admin**设置了开启手机令牌登录，但是没有绑定手机令牌时，可提工单反馈，技术支持人员收到反馈后，重置**admin**登录验证为初始状态，而不改变系统其它配置。
- 当系统非**admin**用户未绑定手机令牌时，系统管理员**admin**可为目标用户修改登录“多因子认证”方式。

8.2.6 绑定了手机令牌，却不能登录怎么办?

问题现象

绑定手机令牌后，登录提示您“无法用手机令牌登录，请尝试其他登录方式”。

可能原因

可能因目标用户账户“多因子认证”配置中，没有勾选“手机令牌”。

解决办法

目标用户在“个人中心”绑定手机令牌后，管理员用户登录系统，为目标用户重新配置手机令牌多因子认证。

步骤1 管理员用户登录系统。

步骤2 选择“用户 > 用户管理”，单击“管理”进入用户详情页面。

步骤3 单击“用户配置”区域内的“编辑”，弹出“编辑用户配置”页签。

步骤4 在“多因子认证”栏，勾选“手机令牌”。

步骤5 单击“确认”，完成配置。

----结束

目标用户返回系统登录页面，即选择“手机令牌”方式验证登录。

8.3 登录安全类

8.3.1 如何设置云堡垒机登录安全锁?

背景

- CBH同一账户可以在同一台PC上的不同浏览器登录。
- 云堡垒机不支持同时登录同一用户账号。当同时登录同一用户账号时，“来源IP”将被锁定。
- CBH目标是限制多人使用同一账号，同一账号专人使用，应该做到一个账号一人使用。

现象

为保障云堡垒机系统登录安全，在登录云堡垒机输入密码超过系统设置的次数限制后，用户“来源IP”或“用户”账号将被锁定。

配置步骤

步骤1 登录云堡垒机系统。

步骤2 选择“系统 > 系统配置 > 安全配置 > 用户锁定配置”，查看当前配置信息。

步骤3 单击“用户锁定配置”区域的“编辑”，进入“用户锁定配置”参数配置页面。

步骤4 用户根据需要配置参数，详细参数说明请参考表8-1。

表 8-1 锁定配置参数说明

参数	说明
锁定方式	可选择“用户”和“来源IP”两种方式。 • 选择“用户”指密码错误超过输入限制次数后，用户账号将被锁定。 • 选择“来源IP”指密码错误超过输入限制次数后，用户本地来源IP将被锁定，且局域网内同一网段IP都将被锁定。
尝试密码次数	用户通过最多能尝试登录云堡垒机的次数。

参数	说明
锁定时长	密码错误超过输入限制次数后，锁定的时间长度，单位为分钟。 ● 默认值为30分钟。 ● 设置为0分钟表示需管理员解除锁定。
重置计数器时长	密码错误超过输入限制次数后，从设定时间提示的剩余被锁定时间。

步骤5 单击“确定”，完成用户登录输入密码限制设置。

----结束

8.3.2 如何解锁登录云堡垒机时被锁定的用户/IP?

云堡垒机登录锁定方式有“用户”、“来源IP”和**“用户+来源IP”**，用户可在云堡垒机系统“安全配置 > 用户锁定配置”中，修改锁定方式。

解锁 IP

当登录云堡垒机系统时，提示“IP已被锁定！请30分钟后重试”，表明用户“来源IP”已被云堡垒机后台锁定，该用户IP地址在限定时间内无法再登录云堡垒机系统。

解决办法如下：

- 等待锁定时间到期后，再操作。
- 当IP被锁定时，请提交工单并提供被锁定的IP，联系技术支持协助解除IP锁定。

解锁用户

当登录云堡垒机系统时，提示“当前用户已被锁定，请30分钟后重试！”，表明“用户”账号已被云堡垒机后台锁定，该用户登录名在限定时间内无法再登录云堡垒机系统。解决办法如下：

- 等待锁定时间到期后，再操作。
- 当非**admin**用户账号被锁定时，可登录系统管理员admin账号，选择“用户 > 用户管理”，进入“用户管理”页面。选择被锁定用户，单击“启用”，即可解除该用户账号的锁定。

  说明

  系统管理员**admin**账号拥有最高操作权限，当**admin**账号被锁定后，只能等待锁定时间到期后，再操作。

9 系统用户、资源及策略配置

9.1 系统用户类

9.1.1 在新建用户/资源时，为什么无法选择上级部门?

因为用户所属“角色”未配置“管理权限”，用户在新建用户或资源时，不能配置新用户或资源的“所属部门”为当前用户的上级部门。

更多部门管理和角色管理说明，请分别参见**部门**和**角色**。

9.1.2 如何修改用户手机号码?

云堡垒机“手机号码”为用户登录验证、找回密码、获取系统动态信息的账户重要信息。

- **admin**用户的手机号码，为首次登录时自行绑定的手机号码。
- 其他用户的手机号码，为管理员创建用户时或用户首次登录系统时，绑定的手机号码。

用户账号手机号码，支持个人修改，管理员修改，以及管理员批量修改。

用户个人修改

步骤1 登录云堡垒机系统。

步骤2 在界面右上角，单击“个人中心 ”，进入个人中心管理页面。

步骤3 在基本信息页签，单击右上角“编辑”，进入个人信息管理窗口。

步骤4 配置新手机号码。

步骤5 单击“确认”，即完成修改个人手机号码。

----结束

管理员逐个修改

系统管理员**admin**或拥有“用户”模块管理权限的用户，可逐个为其他用户重置手机号码。

步骤1 登录云堡垒机系统。

步骤2 选择“用户 > 用户管理 ”，进入用户列表管理页面。

步骤3 选择待修改手机号的用户，单击用户名或“管理”，进入用户详情页面。

步骤4 在“基本信息”区域，单击“编辑”，管理用户基本信息。

步骤5 配置新手机号码。

步骤6 单击“确认”，即完成修改单个用户手机号码。

----结束

管理员批量修改

系统管理员**admin**或拥有“用户”模块管理权限的用户，可批量为多个用户重置手机号码。

步骤1 登录云堡垒机系统。

步骤2 选择“用户 > 用户管理 ”，进入用户列表管理页面。

步骤3 导出用户信息。

选择待修改手机号的用户，单击“导出”，导出用户信息文件到本地。

步骤4 修改用户手机号。

将用户信息文件保存到本地，手动修改“用户手机号码”，并保存。

步骤5 导入用户信息。

1. 返回用户列表管理页面，单击“导入”，进入导入用户窗口。
2. 单击“单击上传”，选择修改后的用户信息文件并上传。
3. 上传完成后，先选择“更多选项”中的“覆盖已有用户”。
4. 单击“确定”，即完成批量修改用户手机号码。

----结束

9.1.3 云堡垒机可新建多少个用户?

没有限制。

云堡垒机系统的一个用户代表一个可登录自然人，支持新建本地用户，批量导入用户，以及同步AD域用户。

系统管理员**admin**是系统最高权限用户，也是系统第一个可登录用户。

如何新建用户，详细操作可参考**新建用户**章节。

9.2 资源添加类

9.2.1 如何创建云堡垒机数据库运维?

云堡垒机支持通过**主机运维**和**应用运维**两种方式管理数据库，可管理多种协议类型的云上数据库，具体请参考**云堡垒机支持管理哪些数据库?** 。主机运维方式提供增删改查操作命令审计。应用运维方式提供操作会话视频审计。

说明

- **标准版**仅支持应用运维方式，不支持直接运维数据库，需要建立应用发布服务器才可以运维数据库。
- **专业版**支持主机运维和应用运维两种方式，支持直接运维数据库。

前提条件

- 已购买云堡垒机实例，且能正常登录云堡垒机系统。若需通过命令运维数据库，即通过主机运维方式管理数据库，请购买**专业版**云堡垒机实例。
- 数据库资源与云堡垒机之间网络连接畅通。云堡垒机实例安全组已放开入方向33306端口，且数据库安全组允许云堡垒机IP访问。

主机运维方式

主机运维支持SSO单点登录方式运维MySQL、SQL Server、Oracle、DB2四种协议类型数据库。

步骤1 管理员创建数据库主机资源。

选择“资源 > 主机管理”，配置“协议类型”为DB2、MySQL、SQL Server或Oracle数据库协议，生成相应数据库资源账户。

步骤2 管理员授权用户访问控制权限。

- 选择“策略 > 访问控制策略”，授权用户访问数据库资源权限，并关联已创建的数据库资源账户。
- 选择“策略 > 数据库控制策略”，针对MySQL和Oracle类型数据库，可配置数据库关键操作控制策略，通过命令拦截运维会话。详细操作请参见**数据库控制策略**。

步骤3 运维用户登录数据库资源。

选择“运维 > 主机运维”，授权用户登录数据库资源。登录方式请参见**SSO单点客户端运维**。

运维用户可对数据库资源执行增删改查运维命令，并可在**实时会话**查看正在执行的操作命令，在**历史会话**查看历史操作命令记录。

运维用户在操作关键命令时，触发“动态授权”操作命令，系统自动拦截操作命令，生成**数据库授权工单**。运维用户需提交工单申请，待管理员审批工单后，才能继续操作。

说明

主机运维方式不支持生成和下载数据库运维历史会话视频。

----结束

应用运维方式

只要数据库与应用发布服务器网络连接通畅，且应用发布服务器与云堡垒机网络连接通畅，应用运维方式可以Web运维所有类型数据库，支持代填数据库的账户和密码。

步骤1 管理员创建数据库应用资源。

选择“资源 > 应用发布”，配置数据库类型应用，生成相应数据库资源账户。其他参数配置说明请参见**新建应用发布服务**。

步骤2 管理员授权用户访问控制权限。

选择“策略 > 访问控制策略”，授权用户访问数据库资源权限，并关联已创建的数据库资源账户。

步骤3 运维用户登录数据库资源。

选择“运维 > 应用运维”，授权用户登录数据库资源。登录后会话操作说明请参见**应用运维**。

运维用户可对数据库资源运维会话视频记录，并可在**历史会话**下载会话视频。

说明

应用运维方式不支持在会话过程使用命令运维。

----结束

9.2.2 如何通过云堡垒机纳管 RDS 数据库?

CBH支持通过云堡垒机纳管同一VPC下的RDS数据库，达到通过云堡垒机管理数据库资源的目的。

约束限制

仅**专业版**云堡垒机实例支持直接纳管DB2、MySQL、SQL Server和Oracle引擎类型数据库。

前提条件

- 已购买云堡垒机实例，且能正常登录云堡垒机系统。若需通过命令运维数据库，即通过主机运维方式管理数据库，请购买**专业版**云堡垒机实例。
- RDS实例与云堡垒机之间网络连接畅通。云堡垒机实例安全组已放开入方向33306端口，且数据库安全组允许云堡垒机IP访问。

获取 RDS 实例的数据库版本、内网地址、数据库端口和管理员账户名

步骤1 **登录RDS服务控制台**。

步骤2 单击目标实例名称，进入实例详情页面，记录该实例的“数据库引擎版本”、“内网地址”、“数据库端口”和“管理员账户名”。

图 9-1 RDS 实例详情页面

----结束

通过云堡垒机纳管 RDS 数据库

步骤1 登录云堡垒机系统。

步骤2 选择“资源 > 主机管理”，进入主机管理列表页面。

步骤3 单击“新建”，弹出新建主机编辑窗口，参数的配置如**表9-1**所示。

表 9-1 纳管 RDS 实例参数配置说明

参数	说明
主机名称	自定义的主机资源名称，系统内“主机名称”不能重复。
协议类型	选择MySQL或者SQL Server。 纳管的RDS实例的数据库类型请参考**获取RDS实例的数据库版本、内网地址、数据库端口和管理员账户名**获取。
主机地址	输入主机与云堡垒机网络通畅的IP地址。 纳管RDS数据库时，“主机地址”对应RDS实例的“内网地址”，具体的获取步骤请参见**获取RDS实例的数据库版本、内网地址、数据库端口和管理员账户名**。 **说明** 因云堡垒机管理同一VPC网络下的主机资源，根据网络稳定性与就近优势。私有IP对外访问的端口不受网络安全（安全组和ACL）的限制。EIP为独立的弹性IP，对外访问的端口受网络安全限制，可能导致无法通过云堡垒机登录到主机。 故建议“主机地址”优先考虑配置同VPC网络下私有IP地址。
端口	输入主机的端口号，纳管的RDS实例的数据库端口请参考**获取RDS实例的数据库版本、内网地址、数据库端口和管理员账户名**获取。
系统类型	（可选）选择主机的操作系统类型或者设备系统类型。 默认不设置，后台根据资源系统类型匹配。

参数	说明
更多选项	（可选）选择配置“文件管理”、“X11转发”、“上行剪切板”、“下行剪切板”。 ● 文件管理：仅SSH、RDP、VNC协议类型主机可配置。 ● 剪切板：仅RDP协议类型主机可配置。 ● X11转发：仅SSH协议类型主机可配置。
所属部门	选择主机所属部门。
标签	（可选）自定义标签或选择已有标签。
主机描述	（可选）对主机的简要描述。

步骤4 单击“下一步”，纳管主机资源的账号信息。

表 9-2 纳管主机账户信息说明

参数	说明
添加账户	选择立即添加账户，或以后再添加账户。 ● 选择“立即添加”，需要继续配置下面的各项内容。 ● 选择“以后添加”，将结束本页配置，后续您可以在资源列表或资源详情中添加账户。
登录方式	选择登录方式，可选择自动登录或手动登录。 ● 选择“自动登录”时，“主机账户”和“密码”为必填项。 ● 选择“手动登录”时，“主机账户”和“密码”为可选项。
主机账户	输入主机中的账户名，即RDS实例的“管理员账户名”，具体的获取方法请参见**获取RDS实例的数据库版本、内网地址、数据库端口和管理员账户名**。 **说明** 若主机安装了AD域服务，添加的主机账户为*域名\主机账户名*，例如ad\administrator。
密码	输入主机账户对应的密码，即RDS实例的登录密码。 默认勾选“验证”，配置完成确定后，自动验证资源账户的状态。 **说明** ● 验证账户通过后，直接保存资源主机相关信息。 ● 验证账户不通过 – 提示验证账户超时，请返回配置窗口，确认并修改资源信息。 – 提示账户密码错误，请返回配置窗口，确认并修改资源账户密码。
账户描述	对资源账户的简要描述。

说明

未配置主机账户和密码时，默认创建“[Empty]”空账户，登录资源时需手动输入主机账户和相应密码。

步骤5 单击“确定”，且资源账户验证通过后，返回主机列表查看新建的RDS数据库资源。

步骤6 在左侧导航树中，选择“策略 > 访问控制策略”，配置纳管的RDS数据库的访问控制策略。

步骤7 在左侧导航树中，选择“运维 > 主机运维”，进入主机运维列表，在新建的RDS数据库实例主机所在行的“操作”列，单击“登录”。

步骤8 （可选）在弹出的对话框中，单击“下载单点登录工具”，并按默认方式安装。

说明

如果已安装单点登录工具，则不需要执行该步骤。

步骤9 配置**SSO单点登录工具**，具体的操作请参见**如何配置SSO单点登录工具?**。

步骤10 执行完**步骤8**~**步骤9**后，再次单击“操作”列的“登录”。

说明

如果出现“数据库客户端工具配置路径配置有误，请重新配置！”的错误提示，请重新执行**步骤9**。

----结束

9.2.3 如何修改系统资源账户密码?

资源账户修改密码

当主机或应用服务器上账户的密码修改后，需同步修改云堡垒机纳管的资源账户密码。

步骤1 登录云堡垒机系统。

步骤2 选择“资源 > 资源账户”，进入资源账户列表页面。

步骤3 单击待修改密码的资源账户，或单击“管理”，进入资源账户详情页面。

步骤4 在“基本信息”区域单击“编辑”，弹出“编辑资源账户信息”窗口。

步骤5 输入新密码，勾选“验证”。单击“确认”纳管资源账户新密码。

步骤6 返回资源账户列表页面，查看“任务中心”消息，验证新密码是否正确。

说明

也可在返回资源账户列表页面后，选择已修改密码的资源账户，单击“验证”，验证资源账户新密码。

----结束

改密策略修改密码

通过云堡垒机“改密策略”，可修改主机或应用资源服务器上的账户密码，并将新密码纳管到云堡垒机中。

此外，您可以下载改密日志或导出资源账户列表，查看修改后的资源账户密码。

说明

“改密策略”修改密码仅对密码登录的资源账户生效，对SSH Key登录验证的主机资源不生效。

9.2.4 如何设置提权登录资源账户?

云堡垒机仅支持对SSH、Telnet协议主机增加提权账户。

运维员admin_A可以使用test账户登录主机，但是test账户的权限较小，因此需要云堡垒机管理员为其提权。管理员成功为其提权后，运维员admin_A使用test账户登录主机时，将自动切换到提权后的账户登录界面。管理员配置提权登录操作如下：

步骤1 选择“资源 > 主机管理”。

步骤2 单击目标主机对应“操作”的“更多 > 添加账户”。

步骤3 添加提权登录账户，完成后单击“确定”。

表 9-3 设置提权账户参数说明

参数	设置说明
登录方式	选择“提权登录”。
密码	输入目标主机上权限更高账户的登录密码。 例如，**root**是资源主机上权限最高的账户，则输入**root**账户的登录密码。
切换自	选择提权前的资源账户。
切换命令	此项无需修改，默认为**su**。

步骤4 选择“资源 > 资源账户”，可以查看新增的提权账户。

步骤5 选择“策略 > 访问控制策略”，将提权账户[root->su]授权给运维员admin_A。

----结束

9.2.5 如何设置云堡垒机资源标签?

前提条件

已拥有“主机管理”、“应用发布”、“主机运维”或“应用运维”功能模块权限。

添加标签

步骤1 登录云堡垒机系统。

步骤2 选择“资源 > 主机管理”，进入主机管理列表页面。

步骤3 选择需添加标签主机资源，单击“添加标签”，弹出“添加标签”窗口。

步骤4 输入需自定义标签内容，并按“Enter”创建标签，或在“标签”下拉框选择已创建标签。

步骤5 单击“确定”，返回主机资源管理页面或主机运维管理页面，可查看该主机资源的新建标签。

步骤6 标签添加成功后，可在资源管理列表页的“标签”列，单击下拉框，通过选择设定的标签来检索资源。

----结束

删除标签

已添加标签的资源，可对标签进行删除操作，以“主机管理”为操作示例。

步骤1 登录云堡垒机系统。

步骤2 选择“资源 > 主机管理”，进入主机管理列表页面。

步骤3 选择需删除标签主机资源，单击“删除标签”，确认删除提示信息，将删除该主机资源所有标签。

步骤4 返回主机资源管理页面或主机运维管理页面，查看该主机资源标签已被删除。

说明

- “删除标签”将去除所选资源上的所有标签。
- 当创建标签不被任何资源使用时，将会自动被删除。
- 主机或应用标签的单个删除，可单击主机或应用资源列表的“管理”，在资源基本信息编辑页面，对已有标签单个删除。

----结束

9.2.6 如何批量导入/导出主机资源?

批量导入

云堡垒机不支持批量创建主机资源，但可以通过主机“导入”的方式批量导入主机资源，包括通过Excel文件导入资源和通过云平台导入资源。

“从文件导入”的Excel文件需配置内容，包括名称、IP地址/域名、协议类型、端口、系统类型、所属部门、标签、主机描述、主机账户、登录方式、特权账户等。

说明

- “从文件导入”方式的Excel文件，需严格按照表格配置要求填写主机信息，且上传的Excel文件可打开，不能加密。否则会导入资源失败。
- 通过Excel批量导入方式，配置“自动登录”，录入主机资源信息，可避免生成“Empty”账户。

批量导出

云堡垒机还支持批量导出主机资源信息。验证用户后，一键导出全量已纳管的主机资源信息，可在导出的文件中查看主机资源账户最新的配置信息。

导出的Excel文件内容包括资源名称、资源地址、资源协议、资源端口、系统类型、部门、资源标签、资源描述、账户名称、登录方式、特权账户等。

9.2.7 导入云主机的访问密钥 AK/SK 是什么？如何获取?

访问密钥即AK/SK（Access Key ID/Secret Access Key），是用户通过开发工具访问云资源时的身份凭证。系统通过AK识别访问用户的身份，通过SK进行签名验证，通过加密签名验证可以确保请求的机密性、完整性和请求者身份的正确性。

- 若用户选择导入到云平台时，可在“我的凭证”中管理自己的访问密钥。获取方法如下：

  登录管理控制台，在右上角用户账号名内，单击“我的凭证 > 管理访问密钥”，进入访问密钥管理页面。
- 用户若选择导入到其他云平台，可单击“如何获取”，跳转到相应云平台，根据指导说明获取访问密钥AK/SK。

9.2.8 系统资源账户有哪些状态?

云堡垒机系统被纳管资源的账户**状态**，用于标识资源账户的密码是否被验证，且验证是否通过，不能手动修改，可通过实时验证和自动巡检更新。

资源账户共有“正常”、“异常”和“未知”三种状态，各状态详细说明请参见**表 9-4**。

表 9-4 资源账户状态说明

状态	说明
正常	经过“验证”，账号及密码正确，且能正常登录的资源账户，显示为“正常”状态。
异常	经过“验证”，账户或密码不正确，可能不能正常登录的资源账户，显示为“异常”状态。
未知	添加完资源账户后，未经过“验证”的资源账户，显示为“未知”状态。

说明

云堡垒机自动巡检：

在每月的5号、15号和25号凌晨一点，对纳管的资源账户进行账号巡检，通过检测资源账户的连通性，标记资源账户状态。

- 连通性良好，能正常登录的账户显示为“正常”。
- 不能连接，无法正常登录的账户显示为“异常”。

9.2.9 系统资源标签可以共用吗?

不可以。

因云堡垒机系统用户间隔离，每个用户自定义的资源标签仅能个人账户使用，不能被CBH系统内用户共用。

例如系统管理员**admin**添加的资源标签，其他管理员或运维人员登录系统后，不能看到**admin**为资源添加的标签，反之亦然。

9.2.10 是否支持手动输入密码的方式登录资源?

用户在不希望云堡垒机托管密码时，可将登录方式设置为手动输入密码的登录方式，具体操作如下：

步骤1 登录云堡垒机系统。

步骤2 选择“策略 > 访问控制策略”，进入访问控制策略列表管理页面。

步骤3 单击“新建”或“关联”。

步骤4 在配置关联资源账户时，选择**Empty**账户。

步骤5 在“运维 > 主机运维”页面登录该主机，需要手动输入资源账户名和相应密码。

----结束

9.2.11 为什么不能识别批量导入的云主机?

受云堡垒机版本限制，当用户云堡垒机“设备系统”版本低于V3.3.0.0时，导入的云主机可能会识别失败，不能获取主机信息。

您可以先选择升级系统到最新版本后，再次导入云主机。也可以将云主机信息转入Excel表格。

9.2.12 如何通过云堡垒机来访问内网提供的服务?

如果您需要通过云堡垒机来访问内网提供的服务，请参考以下步骤进行操作。

操作步骤

步骤1 购买Windows类型主机或者Linux服务器、镜像、企业授权码、客户端License等资源，用于部署应用发布服务器。

步骤2 安装应用服务器，详细操作指导请参见**安装应用发布服务器**。

步骤3 添加应用资源，详细操作指导请参见**添加应用资源**。

----结束

9.3 系统策略类

9.3.1 动态授权的作用及操作流程是什么?

动态授权是授权用户运维操作触发规则集，系统对字符命令或数据库会话操作进行拦截，自动生成授权工单。授权用户若需继续执行操作，需管理员批准工单。

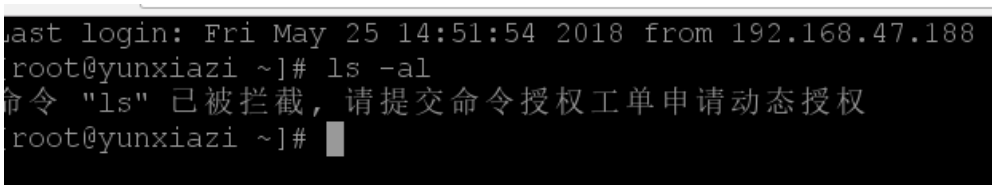
以命令控制策略的动态授权为例。

步骤1 管理员用户登录云堡垒机，选择“策略 > 命令控制策略”，新建字符（SSH或Telnet）命令集和命令控制策略。

命令控制策略“执行动作”需选择“动态授权”。

步骤2 命令控制策略设置成功后，授权用户登录云堡垒机，登录目标主机，执行相关命令触发命令拦截，生成命令授权工单。

图 9-2 动态拦截

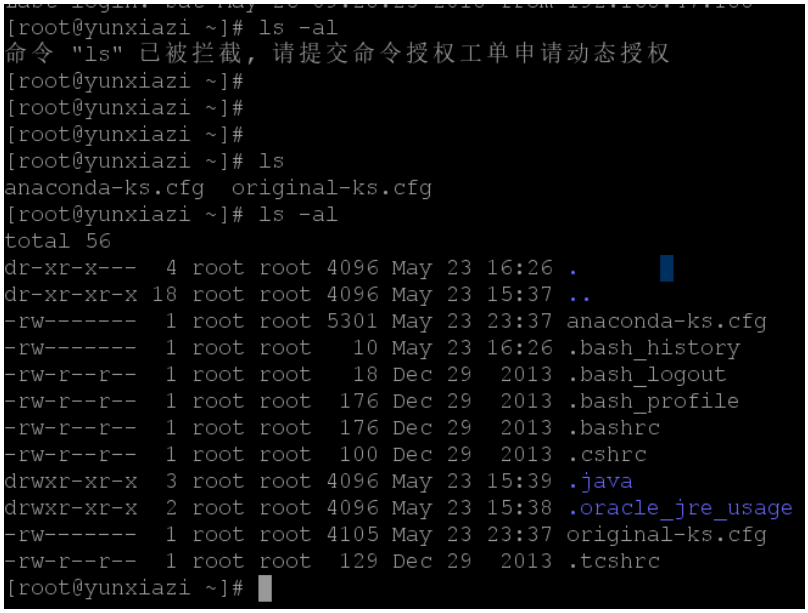


步骤3 授权用户选择“工单 > 命令授权工单”，查看并提交工单。

步骤4 管理员或上级部门领导可以在“工单 > 工单审批”，查看工单并批准工单。

步骤5 获得批准后，授权用户即可成功运行相关命令。

图 9-3 获取授权



----结束

9.4 系统配置类

9.4.1 如何配置 SSH Key 登录主机资源?

云堡垒机支持配置SSH Key登录主机资源，主机资源配置SSH Key后优先验证SSH Key登录资源。

生成 SSH Key

步骤1 生成认证Key。

登录主机，执行以下命令，生成SSH Key。

ssh-keygen -t rsa

回显信息如下：


```
[root@Server ~]# ssh-keygen -t rsa
Generating public/private rsa key pair.
```

可根据需要配置SSH Key的文件名和密码，回显信息示例如下：

```
Enter file in which to save the key (/root/.ssh/id_rsa):置空或输入将生成的文件名，文件保存目录为/root/.ssh。
Enter passphrase (empty for no passphrase):置空或根据需要输入密码
Enter same passphrase again:确认输入密码
Your identification has been saved in /home/fdipzone/.ssh/id_rsa.
Your public key has been saved in /home/fdipzone/.ssh/id_rsa.pub.
The key fingerprint is: f2:76:c3:6b:26:10:14:fc:43:e0:0c:4d:51:c9:a4:b2 root@Server
The key's randomart image is:
+--[ RSA 2048]----+
|    .+=*         |
|  .  +=  +       |
|   o   +         |
|  E . . o        |
|    .S.          |
|      .o .       |
|       . +       |
|       ..        |
|       . +.      |
+-----------------+
```

说明

参数**-t rsa**表示使用rsa算法进行加密，也可以使用dsa加密算法加密，命令如下：

ssh-keygen -t dsa

步骤2 执行以下命令，查看SSH Key文件。

cd /root/.ssh*（文件保存目录）*/

在当前用户SSH Key文件保存目录下，查看已生成私钥id_rsa和公钥id_rsa.pub文件，配置密码后还可查看到私钥密码key和公钥密码key.pub。

回显信息示例如下：

```
[root@Server ~]# cd /root/.ssh/
[root@Server ~]# ll
total 16
-rw------- 1 root root    0 Oct 14 15:47 authorized_keys
-rw------- 1 root root 1679 Nov 15 09:45 id_rsa
-rw------- 1 root root  430 Nov 15 09:45 id_rsa.pub
-rw------- 1 root root 1766 Nov 15 09:48 key
-rw------- 1 root root  430 Nov 15 09:48 key.pub
```

步骤3 在当前用户/.ssh目录下，执行以下命令，复制公钥内容到authorized_keys文件中。

cat id_rsa.pub >>authorized_keys

步骤4 打开主机SSH Key登录验证方式。

1. 执行以下命令，修改sshd_config配置文件参数，生效“RSAAuthentication”和“PubkeyAuthentication”，授权SSH Key验证。

   vim /etc/ssh/sshd_config

2. 修改完后按“Esc”，输入**:wq!**命令并按“Enter”，保存修改并退出。
3. 执行以下命令，重启sshd服务。

   service sshd restart

   回显如下信息表示sshd服务重启成功。

   ```
   Redirecting to /bin/systemctl restart sshd.service
   ```

----结束

配置 SSH Key 信息

步骤1 登录云堡垒机系统。

步骤2 选择“资源 > 主机管理”，新建已生成SSH Key的主机资源。

说明

已被纳管的目标主机，可单击“管理”，在主机信息详情页“添加”资源账户。

步骤3 单击“新建”配置SSH主机资源，配置“主机账户”和“密码”。

步骤4 复制生成的私钥id_rsa文件内容和私钥密码，配置“SSH Key”和“passphrase”。

说明

云堡垒机系统可选择性配置“passphrase”，当未配置“passphrase”时：

- 未生成私钥密码情况下，登录主机无需输入密码。
- 已生成私钥密码情况下，每次登录主机需手动输入私钥密码。

步骤5 单击“确定”，新增拥有SSH Key的主机资源账户。

说明

- “批量导入”主机资源请正确输入SSH Key私钥和Passphrase密码，不要引入其他字符或空格。
- 建议批量导入的资源先仅配置主机账户和密码登录，主机导入云堡垒机系统后，再修改“资源账户”添加私钥和密码。

步骤6 配置访问控制策略。

将配置了SSH Key的主机资源账户授权给用户。

步骤7 授权用户登录资源主机。

----结束

9.4.2 如何设置个人网盘空间大小?

云堡垒机“主机网盘”属于用户系统个人空间，即系统个人网盘。当用户个人网盘空间内存不足时，可由管理员配置“个人网盘空间”，来解决个人网盘内存空间不足的问题。

- 设置“个人网盘空间”后，默认为系统每个用户预置相同大小的个人网盘空间。
- 设置“个人网盘空间”和“网盘总空间”为零，表示在系统数据盘内存充足情况下，不限制用户使用个人网盘，个人网盘空间可无限使用。

前提条件

用户已获取“系统”模块管理权限。

操作步骤

步骤1 登录云堡垒机系统。

步骤2 选择“系统 > 数据维护 > 存储配置”，进入系统存储配置管理页面。

步骤3 查询“网盘空间”区域“个人网盘空间”和“网盘总空间”配置项。

“个人网盘空间”和“网盘总空间”默认值分别为100MB和5120MB。

步骤4 单击“网盘空间”区域“编辑”，弹出“编辑网盘空间”窗口。

步骤5 修改“个人网盘空间”为目标数值。

步骤6 单击“确定”，返回查看“个人网盘空间”设置成功。

----结束

9.4.3 如何解决短信限制问题?

堡垒机赠送的短信服务有以下限制：

- 1分钟内发送短信不超过1条。
- 1小时内发送短信不超过5条 。
- 1天内发送短信不超过15条。

如果不够使用的话，建议修改短信网关配置，设置为“自定义”短信网关。

9.4.4 CBH 如何对接三方邮箱服务器?

CBH支持对接开放在公网的三方邮箱服务器。

操作步骤

以下以163邮箱为例。

步骤1 登录163或邮箱，进入“设置”选择“POP3/SMTP/IMAP”，开启IMAP/SMTP服务或POP3/SMTP服务。

步骤2 开启时弹出账户安全提示框，单击“继续开启”。

步骤3 手机扫描二维码发送短信，发送成功后单击“我已发送”。

步骤4 保存生成的授权密码，单击“确定”。

步骤5 登录堡垒机web界面，进入“系统 > 系统配置 > 外发配置 > 邮件配置”。

步骤6 输入smtp邮件服务器地址，发送人密码输入**步骤4**生成的授权密码，发送测试邮件成功则对接成功。

----结束

10 运维资源

10.1 运维管理

10.1.1 云堡垒机支持图形化运维 Linux 主机吗?

支持。

说明

请在本地**测试VNC**连接正常之后再使用云堡垒机纳管，云堡垒机不负责第三方VNC软件的兼容性问题。

云堡垒机支持纳管VNC协议类型的资源，并通过Web浏览器登录资源，实现Linux主机的图形化运维。

您需要在添加主机资源时，将“协议类型”选择为“VNC”。

10.1.2 云堡垒机支持手机 APP 运维吗?

云堡垒机暂时不支持手机APP运维，但可以通过手机浏览器访问云堡垒机系统。

步骤1 打开手机浏览器，输入https://*EIP地址*，进入云堡垒机系统登录页面。

步骤2 输入用户登录名和密码，完成用户登录验证。

登录成功后，可管理部门、用户、资源、策略、系统配置等系统数据，以及审批工单和下载日志。

说明

不支持“主机运维”和“应用运维”登录。

----结束

10.1.3 如何配置 SSO 单点登录工具?

云堡垒机数据库运维使用单点登录（Single Sign On，SSO）工具，登录主机运维方式的数据库资源。

云堡垒机默认使用SsoDBSettings单点登录工具，用户登录数据库资源前，需在本地安装好SSO单点登录工具和数据库客户端工具，并配置正确数据库客户端的路径到SSO单点登录工具上。

说明

登录数据库资源前，需参照**如何配置云堡垒机的安全组?** 放通对应场景的端口。

以Navicat客户端为例，示例正确的配置客户端路径操作。

步骤1 打开本地SsoDBSettings单点登录工具。

步骤2 在“Navicat路径”栏后，单击路径配置。

步骤3 根据本地Navicat客户端安装的绝对路径，选中Navicat工具的exe文件后，单击“打开”。

步骤4 返回SsoDBSettings单点登录工具配置界面，可查看已选择的Navicat客户端路径。

步骤5 单击“保存”，返回云堡垒机“主机运维”列表页面，即可登录数据库资源。

----结束

10.1.4 云堡垒机允许多用户同时登录同一资源吗?

云堡垒机本身允许多用户同时登录同一资源，即不限制登录资源的用户数量。但受限于资源的多用户登录配置，多个云堡垒机用户不能同时登录同一资源账户。

例如，受限于Windows资源的多用户同时登录配置，同时登录Windows资源的用户数量有最大限额。Windows 2008和Windows 2012服务器默认仅支持两个用户同时登录，即被CBH系统纳管的Windows服务器默认最多允许两个用户同时登录。

为解除资源多用户同时登录限制，您可以选择如下方式解决：

- 配置资源服务器允许多用户登录。例如，在Windows服务器配置远程桌面会话主机和远程桌面授权。
- 在资源服务器创建多个账号，并纳管为云堡垒机资源账户后，再分别授权给用户。

10.1.5 云堡垒机 SSH 运维支持哪些算法?

云堡垒机3.3.26.0及以上版本SSH运维支持的算法如**表10-1**所示。

表 10-1 SSH 运维支持服务器情况

算法类型	H5页面运维	SSH客户端运维
Key exchange	• diffie-hellman-group-exchange-sha256 • diffie-hellman-group-exchange-sha1 • diffie-hellman-group14-sha1 • diffie-hellman-group1-sha1 • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521 • curve25519-sha256 • curve25519-sha256@libssh.org • diffie-hellman-group14-sha256	• diffie-hellman-group-exchange-sha256 • diffie-hellman-group-exchange-sha1 • diffie-hellman-group14-sha1 • diffie-hellman-group1-sha1 • ecdh-sha2-nistp521 • ecdh-sha2-nistp384 • ecdh-sha2-nistp256
Encryption	• aes128-ctr • aes192-ctr • aes256-ctr • aes128-cbc • aes192-cbc • aes256-cbc • 3des-cbc • blowfish-cbc • arcfour128 • arcfour • cast128-cbc • 3des-cbc • rijndael-cbc@lysator.liu.se	• aes128-ctr • aes192-ctr • aes256-ctr • aes128-cbc • aes192-cbc • aes256-cbc • 3des-cbc • blowfish-cbc • arcfour128 • arcfour256
HMAC	• hmac-md5 • hmac-md5-96 • hmac-sha1 • hmac-sha1-96 • hmac-sha2-256 • hmac-sha2-512 • hmac-ripemd160 • hmac-ripemd160@openssh.com	• hmac-md5 • hmac-md5-96 • hmac-sha1 • hmac-sha1-96 • hmac-sha2-256 • hmac-sha2-512

算法类型	H5页面运维	SSH客户端运维
Host Key	• ssh-rsa • ssh-dss • ecdsa-sha2-nistp256 • ecdsa-sha2-nistp384 • ecdsa-sha2-nistp521 • ssh-ed25519	• ssh-rsa • ssh-dss • rsa-sha2-256 • rsa-sha2-512 • ecdsa-sha2-nistp256 • ecdsa-sha2-nistp384 • ecdsa-sha2-nistp521

10.2 运维操作

10.2.1 云堡垒机支持哪些登录资源方式?

云堡垒机支持设置“自动登录”、“手动登录”或“提权登录”三种登录方式访问目标资源，此外还支持批量登录资源功能。

自动登录

在新建资源时选择“自动登录”方式，并配置资源账户名和密码，托管主机或应用资源的账户和密码。

运维人员访问资源时，无需输入资源的账户和密码，在“主机运维”或“应用运维”页面单击“登录”，即可成功自动登录到目标资源实现运维。

说明

- Edge类型应用资源不支持配置“自动登录”。
- SSH协议类型主机资源配置SSH Key后，需优先使用SSH Key登录。

手动登录

在新建资源时选择“手动登录”方式或选择“以后添加”账户，生成“[Empty]”资源账户，即未配置主机或应用账户名和密码。

运维人员访问资源时，需要输入主机或应用的账户名和相应密码登录资源。

提权登录

纳管资源创建了“特权账户”，普通资源账户可设置提权登录。

运维人员访问资源时，通过普通资源账户登录，将自动切换到提权的资源账户，此时普通资源账户可拥有提权后账户的访问操作权限。

批量登录

在“主机运维”页面，运维人员可以选择多个主机资源，单击左下方“批量登录”，在一个运维页面登录多个不同协议类型主机资源，并可以在一个运维页面切换资源，方便运维人员运维操作，提高运维效率。

说明

“批量登录”不支持登录FTP、SFTP、SCP、DB2、MySQL、Oracle、SQL Server协议类型主机资源，以及配置了“手动登录”或“双人授权账户”的主机资源。

10.2.2 如何创建运维协同会话?

云堡垒机系统Web运维“协同分享”功能，支持通过分享URL，邀请系统其他用户共同查看同一会话，并且参与者在会话控制者批准的前提下可对会话进行操作，可应用于远程演示、对运维疑难问题“会诊”等场景。

说明

- 创建协同分享前，需确保云堡垒机与资源主机网络连接正常，否则受邀用户无法加入会话，且邀请人会话界面上报连接错误，提示“由于服务器长时间无响应，连接已断开，请检查您的网络并重试（Code：T_514）”。
- 邀请URL链接可复制发送给多个用户，拥有该资源账户策略权限的用户才能正常打开链接。
- 受邀用户需在链接有效期前或会话结束前才能有效加入会话。

操作步骤

步骤1 登录云堡垒机系统。

步骤2 选择“运维 > 主机运维”，进入主机运维列表页面。

步骤3 选择待运维主机资源，单击“登录”，登录会话进行操作。

步骤4 单击会话框右侧“协同分享”，邀请用户参与会话，一同进行操作。

步骤5 单击“邀请好友进入此会话”，获取邀请链接。复制链接，发送给拥有云堡垒机资源账户权限的用户。

步骤6 受邀用户登录云堡垒机，打开邀请链接，查看邀请信息。

步骤7 受邀用户单击“立即进入”，加入会话操作。

- 单击“申请控制权”，向当前控制者发送控制申请，申请控制会话的权限。
- 单击“释放权限”或“退出会话”，会话权限将返给邀请人控制。
- 单击“退出会话”，用户退出当前会话。当邀请链接未过期且邀请人未结束会话时，用户可再次加入会话。

步骤8 邀请人或当前控制者可对会话进行管理操作。

- 邀请人单击“取消分享”或退出会话，将结束协同分享会话，受邀用户将被强制退出会话，且不能通过链接再次进入。
- 当受邀用户申请会话控制权限时，会话控制者可单击“同意”或“拒绝”，转交会话控制权限。

----结束

10.2.3 如何使用系统资源标签?

云堡垒机标签用于标识CBH中被纳管的资源，达到对CBH系统中主机、应用资源进行分类的目的，并可以与运维资源进行关联识别。当为主机或应用添加标签后，该资源所有关联的运维资源都会带上标签，从而可以对运维资源分类检索。一个主机或应用资源最多拥有10个标签。

在此示例中，以标识云主机ECS和云数据库RDS资源为例，为每个运维资源分配了两个标签，“标签1”按照团队标识，“标签2”和“标签3”按照项目标识，用户可根据不同标签筛选所标识的资源。

用户添加标签后，可在CBH系统通过标签检索资源，并管理资源标签，参见表10-2。

表 10-2 CBH 标签使用说明

界面入口	可执行操作
桌面 > 最近登录主机	检索资源
桌面 > 最近登录应用	检索资源
桌面 > 可登录主机	检索资源
桌面 > 可登录应用	检索资源
资源 > 主机管理	添加标签、删除标签、编辑标签、检索资源
资源 > 应用发布	添加标签、删除标签、编辑标签、检索资源
运维 > 主机运维	添加标签、删除标签、检索资源
运维 > 应用运维	添加标签、删除标签、检索资源

示例-检索资源

以“主机管理”主机列表筛选“Proj1”的主机资源为操作示例。

步骤1 登录云堡垒机系统。

步骤2 选择“资源 > 主机管理”，进入主机管理列表页面。

步骤3 单击列表“标签”，展开并选择标签“Proj1”。也可通过搜索框搜索并选择标签。

步骤4 主机列表查看通过标签筛选出的“Proj1”主机资源。

说明

支持多个不同标签的组合搜索，并取各个标签的合集筛选出资源。例如同时选择“Team1”和“Proj1”标签，会筛选出带有“Team1”和“Proj1”标签的主机资源。

----结束

10.2.4 通过 Web 浏览器运维，如何设置会话窗口的分辨率?

通过Web运维支持调整运维会话窗口的分辨率，提升运维体验。

约束限制

- Windows系统的会话窗口支持调整分辨率，包括Windows系统主机资源和应用资源。
- vnc协议类型主机资源的会话窗口暂不支持调整分辨率。

前提条件

- 用户已获取“主机运维”或“应用运维”模块管理权限。
- 用户账号已获取资源访问控制权限，即管理员已授权访问控制策略或用户提交权限申请工单已审批通过。
- 资源网络连接正常，且资源账户登录账号和密码无误。

操作步骤

以调整Windows系统主机资源的会话窗口分辨率为例。

步骤1 登录云堡垒机系统

步骤2 选择“运维 > 主机运维”，进入主机运维列表页面。

步骤3 选择目标Windows系统主机资源，单击“登录”，进入运维会话窗口。

步骤4 单击运维会话窗口右下角分辨率图标，弹出分辨率选项。

步骤5 选择预置分辨率选项或设置为“自适应”。

- 默认为“自适应”。
- 可选择1920*1080、1024*768、800*600预置分辨率。

图 10-1 设置会话窗口分辨率

步骤6 选择自定义分辨率。

1. 单击“自定义”，弹出分辨率设置窗口。
2. 配置分辨率“宽度”和“高度”。
3. 单击“确认”。

步骤7 重新选择或自定义分辨率设置后，将重新连接运维会话窗口。

连接成功后，将呈现设置的分辨率会话窗口。

----结束

10.2.5 通过 Web 浏览器运维，如何使用快捷键复制/粘贴文本?

Web运维捷键操作使用Windows快捷键，“复制/粘贴”文本快捷键“Ctrl+C”和“Ctrl+V”，因Linux或Windows主机系统不同，操作方式有所差异。

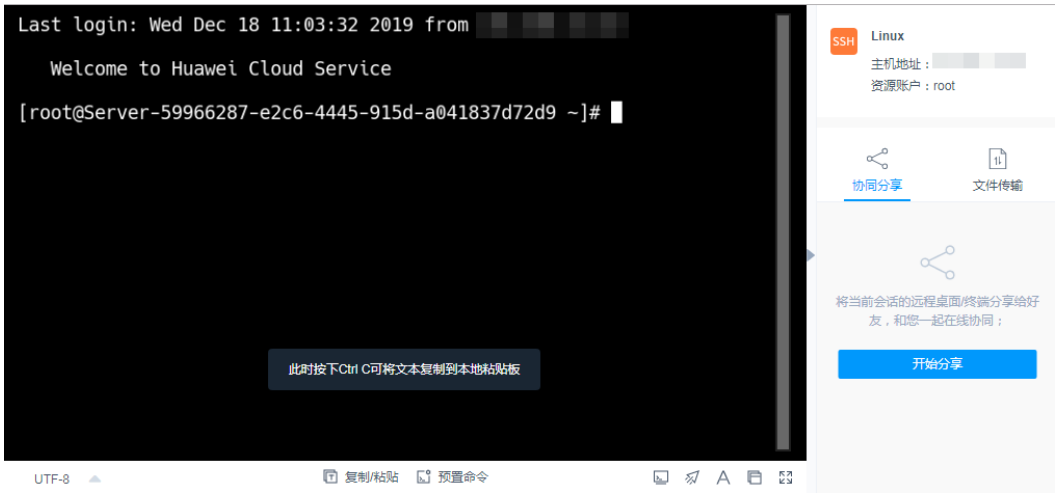
说明

- VNC协议主机资源，不支持文本的复制/粘贴。
- 仅SSH、RDP、TELNET协议主机资源，支持“Ctrl+C”和“Ctrl+V”复制/粘贴文本。
- 云堡垒机“复制/粘贴”有字符数限制，本地到源端限制不超过8万个字符的文本，源端到本地限制不超过100万个字符。
- 若您在复制的时候出现了输入一个单“C”字符的情况，请升级您的堡垒机版本至V3.3.40.0版本及以上来规避该问题。

Linux 主机“复制/粘贴”

登录Linux主机资源，进入运维会话窗口。选中文本内容，“Ctrl+C”复制文本，“Ctrl+V”粘贴文本。

图 10-2 Linux 主机复制文本



Windows 主机“复制/粘贴”

登录Windows主机资源，进入运维会话窗口。选中文本内容，需操作两次“Ctrl+C”复制文本，“Ctrl+V”粘贴文本。

说明

Windows主机内文件“复制/粘贴”快捷键：“Ctrl+B”复制，“Ctrl+G”粘贴

10.2.6 云堡垒机运维，操作快捷键有哪些?

- Web运维快捷键操作与Windows系统快捷键通用，常用“Ctrl+C”复制文本，“Ctrl+V”粘贴文本，“Ctrl+X”剪切文本等。

  当Web运维快捷键与浏览器快捷键有冲突时，优先执行浏览器快捷键。建议用户修改浏览器快捷键，以免冲突。

  “应用运维”与“主机运维”使用相同的Web运维会话操作界面，快捷键操作方式相同。
- 数据库运维，由于通过SSOTool调用本地数据库客户端，Windows快捷键仍适用。
- SSH客户端运维和FTP/SFTP客户端运维，由于直接通过客户端工具登录CBH系统连接主机，快捷键与客户端工具快捷键通用。

10.2.7 通过 Web 浏览器运维，文件列表获取失败怎么办?

问题现象

使用Web浏览器运维时，文件传输处一些目录下显示文件列表获取失败。其他目录打开均正常。

解决方法

原因是部分文件名称中带有“\”字符，导致堡垒机无法正确识别相关文件，只要重新命名文件或者文件夹，取消“\”字符即可正常。

11 审计运维日志

11.1 云堡垒机可提供哪些审计日志?

云堡垒机分别提供实例和系统审计日志。

实例审计

云堡垒机实例审计，需开启云审计服务（Cloud Trace Service，简称CTS），实现对CBH实例的操作的记录，CTS管理控制台将保存最近7天的操作记录。

实例审计日志操作和说明，请参见**CBH云审计**。

系统审计

云堡垒机系统能集中管理用户登录系统，提供系统日志和系统报表。此外，CBH系统授权用户登录被纳管的资源，并进行运维操作，云堡垒机提供用户对系统和资源的运维记录，包括历史会话和运维报表。系统审计日志详细内容，请参见**表2 CBH系统审计日志说明**。

表 11-1 CBH 系统审计日志说明

日志类型	日志内容
历史会话	• 运维会话视频：无需设置，全程录屏记录运维会话操作，可在线播放或下载操作视频。 • 运维会话详情：用户运维会话详情，可在线查看或导出Excel文件。详情内容包括**资源会话信息**、**系统会话信息**、**运维记录**、**文件传输**、**协同会话**的详细操作记录。
系统日志	以折线图的形式，从多方面呈现用户运维资源随时间变化的趋势，并可生成运维资源综合分析报告。 主要涵盖内容有“运维时间分布”、“资源访问次数”、“会话时长”、“来源IP访问数”、“会话协同”、“双人授权”、“命令拦截”、“字符命令数”和“传输文件数”。

日志类型	日志内容
运维报表	• 系统登录日志：用户登录系统的详细记录，可在线查看或导出Excel文件。 • 系统操作日志：用户系统操作的详细记录，可在线查看或导出Excel文件。
系统报表	以柱状图的形式，从多方面统计用户登录系统和系统操作次数，并可生成系统管理综合分析报告。 主要涵盖内容有“用户控制”、“用户与资源操作”、“用户源IP数”、“用户登录方式”、“异常登录”、“会话控制”和“用户状态”。

11.2 操作回放视频支持下载吗?

支持下载mp4格式视频文件，并可在多种播放器上播放。

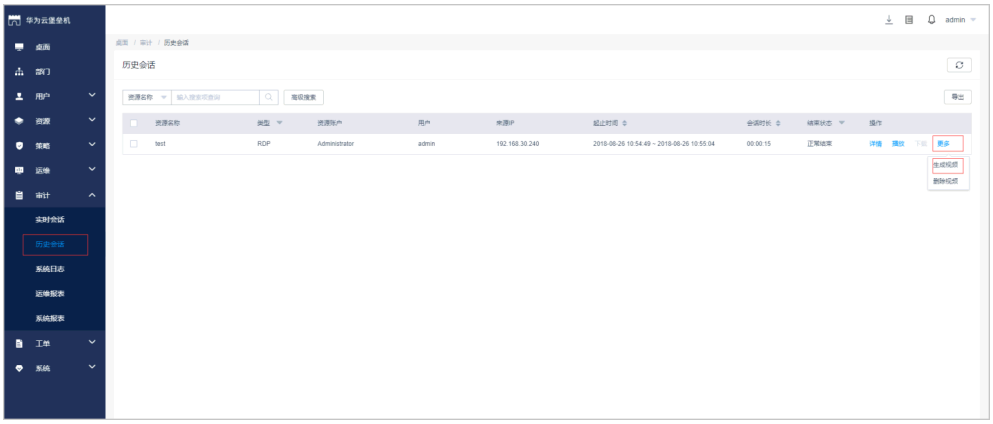
默认情况下，不生成可下载视频文件，需手动“生成视频”。下载视频后请及时删除，以免占用过多存储空间。

步骤1 登录云堡垒机系统。

步骤2 选择“审计 > 历史会话”。

步骤3 单击“操作”列中的“更多 > 生成视频”。

图 11-1 生成视频



步骤4 生成视频后，单击“操作”列的“下载”，将视频保存到本地。

步骤5 下载视频后，可将系统缓存的视频文件删除，可以单击“操作”列中的“更多 > 删除视频”，或选中多条记录单击左下角批量“删除视频”。

说明

因登出时间和操作时间不同，下载后的视频文件的总时长与可播放时长可能不一致。“总时长”是指从登录资源到登出资源的时间段，“可播放时长”是指从登录资源到最后一次会话操作的时间段。

----结束

11.3 可以删除某一天的云堡垒机运维数据吗?

不可以。

云堡垒机系统支持“自动删除”和“手动删除”系统中运维数据。

- “自动删除”：当云堡垒机系统空间使用率达到90%时，或数据在云堡垒机系统存储超过180天（默认180天），系统自动清理数据。
- “手动删除”：手动选择日期，删除选择日期之前的数据。不能删除具体某一天的数据。

说明

没有备份的数据删除后不能恢复，建议您对重要的数据进行备份，具体的操作请参见**备份系统配置**。

11.4 系统审计日志支持备份到 OBS 桶吗?

支持。

目前不仅支持通过FTP/SFTP备份到同一个VPC网络内的服务器中，还支持将数据备份到同一个VPC网络内的OBS桶中。

系统数据备份详情，请参见**云堡垒机日志备份方式**。

11.5 系统审计日志能保存多久?

在云堡垒机系统数据盘空间使用率低于90%情况下，系统审计日志默认可保存180天。

因云堡垒机系统默认开启了“自动删除”功能，将根据日志存储历史和系统存储空间使用率，触发自动删除历史日志。

您也可以修改自动删除设置，修改“自动删除”中日志保存时间，在系统数据盘空间充裕情况下，可延长系统审计日志存储时间，甚至可一直保存系统审计日志。

更多云堡垒机系统数据备份说明，请参见**如何备份系统数据?**

11.6 系统审计日志处理机制是什么?

云堡垒机系统审计日志存储在系统数据盘。系统默认开启“自动删除”功能，根据日志存储时间和系统存储空间使用率，触发自动删除历史日志。

日志自动删除机制说明如下：

- 默认逐日删除180天前历史日志。
- 当系统存储空间使用率高于90%时，将自动清理存放时间最久的日志（每次删除一天的数据），直到空间使用率在90%以下为止。
- 当天审计日志不会被删除。

说明

- 您也可以选择“手动删除”，删除某一天及之前历史日志。
- 当系统存储空间使用率高于95%后，系统可能会故障无法使用，建议不要关闭“自动删除”功能。

11.7 为什么视频可播放时长比总会话时长短?

因云堡垒机视频审计仅记录有效运维时间，即仅记录到最后执行命令操作的时间，不会记录操作空白期到会话关闭的时间。若登出时间和最后操作时间不同，则视频文件的总时长与可播放时长可能不一致。

例如：某次Web浏览器运维会话，总会话时长为30分钟，最后一次执行命令操作时间在第5分钟，后25分钟到退出会话这段时间，无任何操作为操作空白期。视频总时长仍为30分钟，但仅可播放前5分钟，因为后25分钟操作空白期不会被记录。

说明

- “总时长”是指从登录资源到登出资源的时间段。
- “可播放时长”是指从登录资源到最后一次会话操作的时间段。

11.8 为什么收到登录资源提示，但历史会话无登录记录?

因每月5号、15号、25号的凌晨一点，后台启动“自动巡检”，通过登录所有纳管的主机验证资源账户的连通性。验证完成后，系统管理员**admin**将收到登录资源的验证结果消息。

但“自动巡检”登录资源过程不生成任务，故历史会话无登录记录。

12 故障排除

12.1 登录系统故障

12.1.1 登录云堡垒机系统异常怎么办?

问题现象

- IP地址无法连接，网页打不开，不能通过互联网页面正常登录。
- 登录系统后界面异常无法显示。
- 登录系统提示授权未生效。
- AD域认证的用户登录失败。
- 堡垒机不能正常登录，公网地址也不能访问。

可能原因

原因一：系统磁盘空间满了，磁盘空间使用率过高。

原因二：系统软件版本未更新，存在磁盘空间被占用，未被释放可能。

原因三：用户登录使用浏览器或浏览器版本，与系统不兼容。

原因四：实例配置安全组不合理。

原因五：实例配置VPC内，网络ACL规则配置不合理，或登录IP被网络ACL限制。

原因六：配置AD域认证时，未禁用SSL加密认证。

原因七：堡垒机版本较低。

解决办法

原因一：

- 定期“手动删除”指定日期前的日志、视频等历史数据。设置磁盘空间满时日志“自动删除”，保证磁盘有足够空间。详细配置说明请参见**存储配置**。
- 对云堡垒机实例进行规格**变更**，满足大容量磁盘需求。

- 建议配置系统性能的磁盘空间使用率告警通知，当磁盘空间使用率超过设定阈值时，提示系统消息告警。详细配置说明请参考**告警配置**。

原因二：

- 在云堡垒机管理控制台“重启”云堡垒机实例，检查故障是否解决。若不能解决，需“升级”云堡垒机到最新版本，并根据实际需求进行规格变更。

原因三：

- 更换浏览器或升级浏览器版本，Web登录推荐使用浏览器及版本，请参见**登录云堡垒机系统**。

原因四：

- 若因安全组配置不合理导致异常，请先**排查安全组规则**，并根据CBH建议安全组规则，**配置安全组**规则，再重新登录云堡垒机系统。

原因五：

- 若因网络ACL配置不合理导致异常，请先**排查网络ACL规则**，并参考**CBH安全组规则**放开出/入方向端口，再重新登录云堡垒机系统。
- 若因云堡垒机登录IP被网络ACL限制，请先**排查网络ACL规则**，并重新配置ACL规则，添加云堡垒机公网IP（即弹性IP）为允许。

  说明

  浏览器登录云堡垒机需放开入方向TCP协议443端口，SSH客户端登录云堡垒机需放开入方向TCP协议2222端口。

原因六：

- 系统管理员**admin**登录云堡垒机系统，重新**配置AD域认证**，取消SSL加密认证。
- 检查用户登录IP地址和MAC地址是否被加入用户访问限制，请参见**用户登录限制**。
- 检查访问控制策略是否限制了用户IP地址，请参见**访问控制限制**。

原因七：

参照**升级版本**章节，对堡垒机进行升级。

如果通过上述排查，仍然无法登录云堡垒机系统，请单击管理控制台右上方的“工单”，填写工单反馈问题现象，联系技术支持。

12.1.2 登录系统，报 IP/MAC 地址不在登录范围怎么办?

问题现象

- 通过Web浏览器登录云堡垒机系统，上报“您的IP地址不在允许登录的范围内！”错误。
- 通过Web浏览器登录云堡垒机系统，上报“您的MAC地址不在允许登录的范围内！”错误。

可能原因

云堡垒机系统限制了用户IP地址或MAC地址登录，用户登录IP地址或MAC地址被设置了登录黑名单，不能登录云堡垒机系统。

解决办法

请管理员排查用户登录限制配置，查看是否配置“登录IP地址限制”和“登录MAC地址限制”白名单或黑名单。

- 若配置了白名单，请根据配置的IP/MAC地址，使用配置范围内的服务器登录。
- 若配置了黑名单，请根据配置的IP/MAC地址，使用未被限制的服务器登录。

12.1.3 登录系统，系统提示“404：服务错误”怎么办?

问题现象

通过Web浏览器登录云堡垒机系统，弹出系统提示框，提示“/3.0/AUTHSERVICE/CONFIG-404：服务错误”。

可能原因

云堡垒机系统网盘空间满了，可使用数据盘空间不足。

解决办法

- 单独挂载系统数据盘，并重启云堡垒机即可恢复。
- 变更云堡垒机规格，提高系统整体规格性能。

说明

不允许对原有的系统盘或数据盘进行扩充，只能单独挂载数据盘，重启云堡垒机自动挂载。

12.1.4 登录系统，系统提示“499：服务错误”怎么办?

问题现象

通过Web浏览器登录云堡垒机系统，弹出系统提示框，提示“/3.0/profileService/freshProfile 499：服务错误，请稍后重试”。

可能原因

云堡垒机系统还处于“正在重启”状态中，当前系统还不可用。

解决办法

5分钟后再登录CBH系统，待系统重启完成。

12.1.5 内网用户登录云堡垒机系统，可能会遇到哪些故障?

常见场景

- 用户在公司内网，登录云堡垒机系统后，屏幕黑屏，且图标加载显示不全；
- 用户在公司内网，登录云堡垒机系统后，有时网络会突然断开或网络不稳定；
- 用户在公司内网，登录云堡垒机系统时，跳转到其他链接；
- 云堡垒机无法登录，提示“网络异常，请检查网络配置”。

可能原因

用户公司设置了代理服务器拦截，云堡垒机无法正常连接。

解决办法

确认设置了代理服务器拦截后，申请对云堡垒机的登录IP开启白名单。

12.1.6 通过堡垒机登录主机，无法正常登录怎么办?

问题现象

- **现象一**：使用云堡垒机远程登录，无法使用主账号administrator进行远程登录。
- **现象二**：使用云堡垒机普通账号，无法登录Windows虚拟机，管理员账号可以登录。

可能原因

- **现象一的原因**：用户主机为非RDP协议类型的，但开启了RDP强制登录（admin console配置）。
- **现象二的原因**：
  - 用户使用了RDP协议类型的主机，Windows远程桌面连接数超过最大限制。
  - 主机运维Windows资源时，登录堡垒机用户不是admin。

解决办法

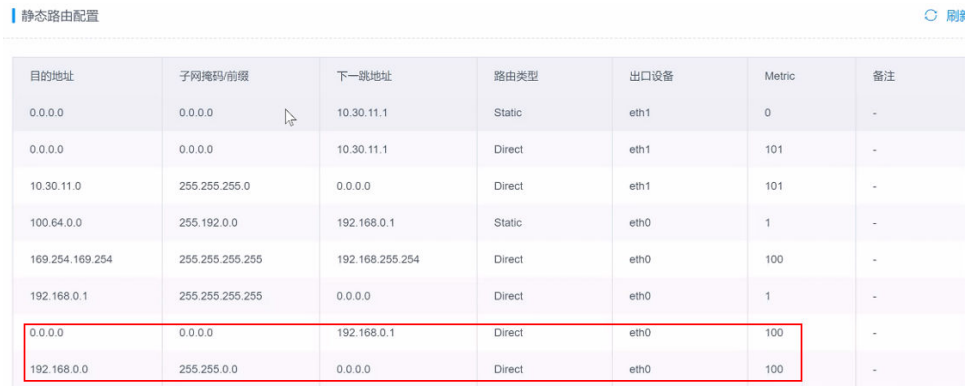
- **现象一的解决办法**：参考开启RDP强制登录章节，去掉勾选“admin console”连接模式。
- **现象二的解决办法：**参考开启RDP强制登录章节，勾选“admin console”连接模式。

12.1.7 通过 VPN 或者 VPC Peering 打通 VPC 后，新 VPC 下的 VM 登录失败怎么办?

问题现象

1. 客户创建堡垒机时，选择了网段为10的VPC。
2. 客户通过VPN或者VPC Peering将另外一个192网段的VPC与10的VPC打通。
3. 客户可以通过10或者192的VPC下的VM正常访问堡垒机。
4. 客户在使用过程中，低概率出现无法通过192网段的VM访问堡垒机。
5. 登录堡垒机检查网络配置，发现出现红框中的路由。

图 12-1 检查网络配置



问题原因

客户的堡垒机未升级，使用的是3.3.26.0之前的版本，堡垒机3.3.26.0之前的版本存在缺陷。在堡垒机业务压力大的情况下，当进行系统状态检查时，线程异常退出导致路由刷新失败，将客户的请求流量错误地转发到ETH0后丢弃，致使登录堡垒机失败。

解决办法

将云堡垒机实例版本升级到3.3.26.0版本。

12.2 登录资源故障

12.2.1 通过云堡垒机登录资源异常怎么办?

问题现象

- 通过云堡垒机登录资源，云主机黑屏无法正常显示。
- 通过云堡垒机登录资源，登录不上或出现网络断连。
- 通过云堡垒机纳管资源后，登录不了资源。

可能原因

原因一：资源主机服务器卡顿，网络连接不稳定。

原因二：云堡垒机共享带宽不满足使用需求。

原因三：资源相关主机服务授权到期，例如Windows授权到期，RDP远程服务120天授权到期等。

原因四：堡垒机实例与纳管的主机不在同一VPC。

解决办法

原因一：

- 重启相应主机资源，重新开机后网络恢复正常。登录云堡垒机系统，**网络诊断**验证云堡垒机与主机资源之间的网络连接情况。

- 若重启主机不能解决，建议再排查**云服务器故障/卡顿**。

原因二：

- 重新配置CBH实例绑定EIP的带宽，建议配置5M以上带宽，详细带宽超限说明，请参见**如何排查EIP带宽是否超限?**
- 排查并修改配置完成后，重启CBH系统。

原因三：

重新购买资源相关主机服务，获取授权后，再使用云堡垒机登录资源。

原因四：

云堡垒机仅支持直接管理同一VPC内资源，即可直接访问同一VPC内资源。

虽跨区域或跨VPC可通过云服务构建网络连接，但受限于网络的不稳定性，不建议跨区域或跨VPC使用云堡垒机纳管资源。

- 跨VPC情况下，可通过**对等连接**打通两个VPC之间网络。
- 跨区域情况下，可通过**云连接（Cloud Connect，CC）**、**虚拟专用网（Virtual Private Network，VPN）**等构建跨区域网络。

其他异常问题处理办法

- **云堡垒机登录资源，报Code：T_514错误怎么办?**
- **云堡垒机登录主机资源，报Code：C_515错误怎么办?**
- **云堡垒机登录主机资源，报Code：C_519错误怎么办?**
- **云堡垒机登录Linux主机，报Code：C_769错误怎么办?**

如果通过上述排查，仍然无法登录主机资源，请单击管理控制台右上方的“工单”，填写工单信息反馈问题现象，联系技术支持。

12.2.2 通过 Web 浏览器登录资源，报 Code：T_514 错误怎么办?

问题现象

通过Web浏览器登录资源，会话页面载入失败，提示“由于服务器长时间无响应，连接已断开，请检查您的网络并重试（Code：T_514）”。

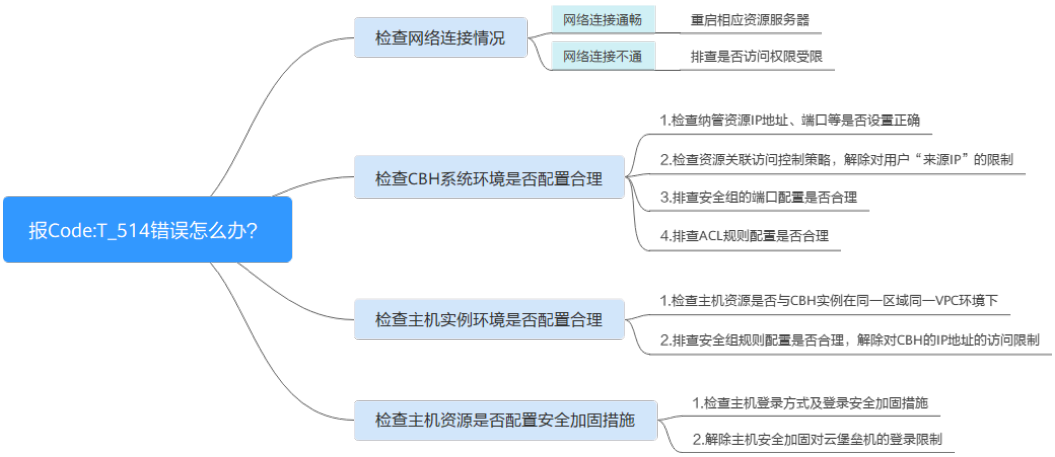
可能原因

- 云堡垒机系统与资源服务器之间网络连接不稳定，导致连接断开。
- 云堡垒机系统到资源服务器的网络被设置拦截，导致网络不通畅。
- 资源服务器异常无响应，导致连接断开。

排查思路

以下排查思路按照“Code：T_514”问题的状态进行逐层细化，您可以根据实际情况选择对应的分支进行排查。

图 12-2 排查思路



检查网络连接情况

登录云堡垒机系统，**网络诊断ping连通性测试**，验证云堡垒机与资源服务器之间的网络连接是否正常。

- 网络连接通畅，则网络不稳定导致连接无响应。

  重启相应资源服务器，重新开机后网络恢复正常。若重启主机不能解决，建议再排查**云服务器故障/卡顿**。
- 网络连接不通，则CBH系统到资源服务器有网络限制，请参考下述方案依次排查。

  a. 请先确认当前用户网络环境，是否为内网用户，以及用户访问权限是否受限。

  例如因华为云内网用户，无法访问公网资源，即未授权的内网用户不能登录运维资源，需先申请外网访问权限或申请Websocket权限。

  b. **检查CBH系统环境是否配置合理**

  c. **检查主机实例环境是否合理配置**

  d. **检查主机资源是否配置安全加固措施**

检查 CBH 系统环境是否配置合理

步骤1 登录云堡垒机系统，检查纳管资源IP地址、端口等是否设置正确。

步骤2 检查资源关联访问控制策略，是否设置IP限制。修改访问控制策略，解除对用户“来源IP”的限制。

步骤3 检查云堡垒机实例关联的安全组，排查安全组的端口配置是否合理。建议按照CBH推荐端口，重新配置CBH安全组。

用户若通过Web浏览器方式登录资源，请手动添加安全组规则TCP协议443入方向。

步骤4 检查云堡垒机所在内网关联的网络ACL ，排查ACL规则配置是否合理。

解除云堡垒机IP地址的访问限制，以及在“目的地址”中添加资源IP地址，允许云堡垒机访问资源。

步骤5 重新设置后，尝试重新通过CBH系统登录资源。

----结束

检查主机实例环境是否合理配置

步骤1 管理员登录主机实例管理控制台。

步骤2 检查主机资源是否与CBH实例在同一区域同一VPC环境下，CBH仅支持直接访问同一区域同一VPC下资源。

步骤3 检查主机实例关联的安全组规则，排查安全组规则配置是否合理。

解除对CBH的IP地址的访问限制，在源地址中添加CBH的IP地址，允许CBH访问资源。

步骤4 重新设置后，尝试重新通过CBH系统登录资源。

----结束

检查主机资源是否配置安全加固措施

步骤1 管理员直接登录主机资源。

步骤2 检查主机登录方式及登录安全加固措施，建议从以下几个方面排查：

- **Linux云服务器SSH登录的安全加固**
- **Windows弹性云服务器登录方式概述**
- **Linux弹性云服务器登录方式概述**

步骤3 从以下几个方面分别排查，解除主机安全加固对云堡垒机的登录限制。

- **无法登录到Linux云服务器怎么办?**
- **无法登录到Windows云服务器怎么办?**

步骤4 解除安全加固的限制后，尝试重新通过CBH系统登录资源。

----结束

如果通过上述排查，仍然无法解决问题，请单击管理控制台右上方的“工单”，填写工单信息反馈问题现象，联系技术支持。

12.2.3 通过 Web 浏览器登录资源，报 Code：T_1006 错误怎么办?

问题现象

通过Web浏览器登录资源，会话连接断开，提示“网络连接异常，连接已断开，请重试（Code：T_1006）”。

可能原因

- 云堡垒机系统与资源服务器之间网络连接不稳定，导致连接断开。
- 云堡垒机或资源服务器的带宽超限，导致连接断开。
- 资源服务器卡顿，导致连接断开。

解决办法

登录云堡垒机系统，**网络诊断ping连通性测试**，验证云堡垒机与资源服务器之间的网络连接是否正常。

- 网络连接不通，则CBH系统到资源服务器有网络限制，请参考**Code：T_514错误方案**依次排查。

- 网络连接通畅，则网络不稳定导致连接无响应。

  重启相应资源服务器，重新登录网络恢复正常。若重启主机不能解决，请参考下述方案依次排查。

  a. 排查云堡垒机和主机资源带宽是否超过限制请。
  b. 排查主机资源是否卡顿，请参考**Linux云服务器卡顿怎么办？**或**Windows云服务器卡顿怎么办？**

如果通过上述排查，仍然无法解决问题，请单击管理控制台右上方的“工单”，填写工单信息反馈问题现象，联系技术支持。

12.2.4 通过 Web 浏览器登录资源，报 Code：C_515 错误怎么办？

问题现象

通过Web浏览器登录Linux或Windows主机资源，报登录错误，提示“运维资源过程中遇到一个错误，请重试或联系管理员（Code：C_515）”。

可能原因

- 原因一：密码输入错误次数超过Linux主机登录安全防护次数上限，导CBH的IP被加入“/etc/hosts.deny”文件名单。
- 原因二：Linux主机开启了企业主机安全服务（Host Security Service，HSS），多次输入错误密码尝试登录，CBH内网IP被HSS加入“/etc/sshd.deny.hostguard”文件名单。
- 原因三：堡垒机不支持操作系统的SSH算法。（仅针对V3.3.38.0版本以下堡垒机）。
- 原因四：Windows主机开启了防火墙，导致堡垒机与主机网络无法正常连接。

解除“/etc/hosts.deny”文件限制

步骤1 管理员登录Linux主机。

步骤2 执行以下命令，查看“/var/log/secure”日志，确认主机拒绝云堡垒机IP记录。

cat /var/log/secure

步骤3 执行以下命令，编辑“/etc/hosts.deny”文件，删除云堡垒机的IP。

vim /etc/hosts.deny

步骤4 （可选）将CBH的IP加入白名单。

执行以下命令，编辑Linux主机的“/etc/hosts.allow”文件，允许所有IP地址登录，避免影响云堡垒机正常使用。

vim /etc/hosts.allow

----结束

解除 HSS 登录 IP 限制

步骤1 查看“/etc/sshd.deny.hostguard”文件。

1. 管理员登录Linux主机。

2. 执行以下命令，查询“/etc/sshd.deny.hostguard”文件。
   cat /etc/sshd.deny.hostguard
3. 执行以下命令，打开“/etc/sshd.deny.hostguard”文件。
   vim /etc/sshd.deny.hostguard
4. 确认“/etc/sshd.deny.hostguard”文件中是否有CBH内网IP记录。

步骤2 在HSS服务控制台，解除IP限制。

1. **登录HSS服务控制台**。
2. 选择“入侵检测 > 事件管理”，进入事件管理页面。
3. 在“安全告警统计”模块，单击“已拦截IP”，展开已拦截IP列表。
4. 找到并勾选CBH内网IP所在行，单击列表左上角“解除拦截”。

步骤3 （可选）将CBH加入IP白名单。

在HSS服务控制台，将CBH的IP添加“SSH登录IP白名单”，允许CBH登录到Linux主机。

----结束

说明

此外，建议使用云堡垒机**纳管主机账户密码**，并定期进行**账户同步**，避免手动输入账户密码错误或未同步僵尸账户，而导致云堡垒机IP被加入黑名单。

解除 SSH 算法限制

步骤1 检查服务器配置文件“/etc/ssh/sshd_config”。

1. 管理员登录Linux主机。
2. 执行以下命令，查询“/etc/ssh/sshd_config”文件。
   ```
   cat /etc/ssh/sshd_config
   ```
3. 执行以下命令，打开“/etc/ssh/sshd_config”文件。
   ```
   vim /etc/ssh/sshd_config
   ```

步骤2 在**HostKeyAlgorithms**行后添加以下算法参数：

rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp256,ssh-ed25519,ssh-rsa,ssh-dss

如果在查询的文件中找不到**HostKeyAlgorithms**行，可能是该参数缺失，需在**Ciphers and keying**行下面添加以下参数及算法。

HostKeyAlgorithms rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp256,ssh-ed25519,ssh-rsa,ssh-dss

如果有其他算法的添加需求，可参照**通过SSH客户端登录资源进行运维**进行添加。

步骤3 新增完成后，执行以下命令查看所有支持的算法，确定修改或添加的算法已存在。
```
sshd -T | grep pubkey
```

- 如果服务器安装了nmap，也可执行以下命令进行查询。
  ```
  nmap --script ssh2-enum-algos -sV -p 22 服务器ip
  ```
  如果使用nmap方式查询确认是**key exchange**算法不匹配时，需临时修改服务器配置。
  a. 执行以下命令打开“/etc/ssh/sshd_config”文件。
     ```
     vim /etc/ssh/sshd_config
     ```


b. 执行以下命令添加参数及算法。

KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha1,diffie-hellman-group-exchange-sha256

如果参数**KexAlgorithms**已存在，添加算法即可。

c. 配置后执行以下命令重启服务器sshd服务。

```
systemctl restart sshd
```

步骤4 执行以下命令重启SSH服务。

```
systemctl restart sshd
```

----结束

添加堡垒机 IP 为白名单

Windows服务器如果是由于开启防火墙导致堡垒机无法正常登录，可在Windows防火墙内添加堡垒机IP为白名单，即可正常登录。

12.2.5 通过 Web 浏览器登录资源，报 Code：C_519 错误怎么办?

问题现象

通过Web浏览器无法登录资源，提示“由于资源连接失败或不可达，当前无法访问。如果持续出现该问题，请通知系统管理员或检查系统日志（Code：C_519）”。

可能原因

- CBH系统与资源服务器之间网络连接不稳定，导致连接失败。
- CBH系统到资源服务器的网络被设置拦截，导致网络不通畅连接失败。
- 资源服务器异常无响应，导致连接不可达。
- 纳管的主机IP未配置在堡垒机eth1网卡所在子网中，当CBH在连接主机时，找不到目标主机的路由，导致连接不可达。

检查网络连接情况

登录云堡垒机系统，**ping连通性测试和TCP端口检测**，验证云堡垒机与资源服务器之间的网络连接是否正常。

- 网络连接通畅，则网络不稳定导致连接无响应。

  重启相应资源服务器，重新开机后网络恢复正常。若重启主机不能解决，建议再排查**云服务器故障/卡顿**。

- 网络连接不通，则CBH系统到资源服务器有网络限制，请参考下述方案依次排查。

  a. 请先确认当前用户网络环境，是否为内网用户，以及用户访问权限是否受限。

  b. **检查CBH系统环境是否配置合理**

  c. **检查主机实例环境是否合理配置**

  d. **检查主机资源是否能接受CBH访问**

e. **检查纳管的主机IP是否在堡垒机eth1网卡所在子网中**

检查 CBH 系统环境是否配置合理

步骤1 登录云堡垒机系统，检查纳管资源IP地址、端口等是否设置正确。

步骤2 检查资源关联访问控制策略，是否设置IP限制。**修改访问控制策略**，解除对用户“来源IP”的限制。

步骤3 检查云堡垒机实例关联的安全组，排查安全组的端口配置是否合理。建议按照CBH推荐端口，重新**配置CBH安全组**。

用户若通过Web浏览器方式登录资源，请手动添加安全组规则TCP协议443入方向。

步骤4 检查云堡垒机所在内网关联的网络ACL ，排查ACL规则配置是否合理。

解除云堡垒机IP地址的访问限制，以及在“目的地址”中添加资源IP地址，允许云堡垒机访问资源。

步骤5 重新设置后，尝试重新通过CBH系统登录资源。

----结束

检查主机实例环境是否合理配置

步骤1 管理员登录主机实例管理控制台。

步骤2 检查主机资源是否与CBH实例在同一区域同一VPC环境下，CBH仅支持直接访问同一区域同一VPC下资源。

步骤3 检查主机实例关联的安全组规则，排查安全组规则配置是否合理。

解除对CBH的IP地址的访问限制，在源地址中添加CBH的IP地址，允许CBH访问资源。

步骤4 重新设置后，尝试重新通过CBH系统登录资源。

----结束

检查主机资源是否能接受 CBH 访问

步骤1 管理员登录主机资源。

步骤2 输入命令**route -n**，检查主机的路由表，是否存在丢失CBH路由现象。

步骤3 检查主机登录方式及登录安全加固措施，建议从以下几个方面排查：

- **Linux云服务器SSH登录的安全加固**
- **Windows弹性云服务器登录方式概述**
- **Linux弹性云服务器登录方式概述**

步骤4 从以下几个方面分别排查，解除主机安全加固对云堡垒机的登录限制。

- **无法登录到Linux云服务器怎么办?**
- **无法登录到Windows云服务器怎么办?**

步骤5 解除安全加固的限制后，尝试重新通过CBH系统登录资源。

----结束

检查纳管的主机 IP 是否在堡垒机 eth1 网卡所在子网中

步骤1 检查纳管的主机IP是否在堡垒机eth1网卡所在子网中。

1. 登录堡垒机系统。
2. 选择“系统 > 系统配置 > 网络配置”，进入系统网络配置管理页面。
3. 在“网络接口列表”区域，查看纳管的主机IP是否在eth1网卡所在子网中。
   - 否，参考**步骤2**。
   - 是，联系技术支持。

步骤2 添加静态路由，将纳管的主机IP配置到eth1网卡所在子网中。

1. 在“网络配置”页面的“静态路由配置”区域，单击“添加”，弹出静态路由添加窗口。

   按如下说明配置参数：
   - 目的地址：填写纳管的主机IP或纳管的主机IP所在子网网段。
   - 子网掩码：如果目的地址为IP，则掩码填写255.255.255.255；如果目的地址为网段，则掩码填写对应网段的掩码。
   - 下一跳地址：填写eth1的下一跳地址。
   - 出口设备：选择“eth1”。
   - 备注：可自定义填写或不填。
   - 同步到备机：可根据实际情况进行打开或者关闭。
2. 单击“确定”。

----结束

如果通过上述排查，仍然无法解决问题，请单击管理控制台右上方的“工单”，填写工单信息反馈问题现象，联系技术支持。

12.2.6 通过 Web 浏览器登录主机资源，报 Code：C_769 错误怎么办?

问题现象

通过Web浏览器登录主机资源，报资源账户密码错误，提示“登录失败，有可能是账户名、密码或密钥错误，请尝试重新连接（Code：C_769）”。

检查云堡垒机资源账户密码是否正确

步骤1 登录云堡垒机系统，选择目标Linux主机，**导出资源账户**，获取主机账户名和密码。

步骤2 **登录ECS服务控制台**，通过**VNC方式登录**Linux主机，验证主机账户和密码。

- 若不能登录，则主机账户密码错误。请**修改Linux主机账户密码**后，重新配置CBH资源账户密码，并**验证账户**是否正确。
- 若能够登录，请分别**检查Linux主机是否开启双因子认证**和**检查Linux主机是否拒绝root账户登录**。

----结束

检查 Linux 主机是否开启双因子认证

当登录Linux主机需输入动态密码时，即Linux主机开启了企业主机安全服务（Host Security Service，HSS）的双因子认证功能。

因云堡垒机不能登录已开通双因子认证的Linux主机，请参考**HSS双因子认证**，关闭Linux主机的双因子认证。

关闭Linux主机双因子认证后，请重新尝试在云堡垒机上登录Linux主机。

检查 Linux 主机是否拒绝 root 账户登录

由于sshd服务配置文件“/etc/ssh/sshd_config”中，“PermitRootLogin”参数值为“no”时，Linux主机不允许root账户登录。

步骤1 登录Linux主机，查看sshd服务的配置文件。

步骤2 在“/etc/ssh/sshd_config”文件中，查找“PermitRootLogin”参数，确认参数值是否为“no”。

步骤3 修改“/etc/ssh/sshd_config”文件。

查找“PermitRootLogin”参数，修改参数值为“yes”或注释掉参数所在行。

```
#PermitRootLogin no
```

步骤4 执行以下命令，重启sshd服务。

systemctl restart sshd

----结束

完成上述操作后，请重新尝试在云堡垒机上登录Linux主机。

检查 Windows 服务器是否 120 天授权到期

检查方法：通过内网的一台Windows主机以远程登录方式连接报错的Windows云服务器时，如果出现如下错误：“由于没有远程桌面授权服务器可以提供许可证，远程会话被中断，请跟服务器管理员联系。”

则说明该Windows服务器120天授权到期。Windows操作系统的云服务器默认支持免费使用120天，到期后需要付费，如未付费会则造成远程连接失败。

解决办法：请参照**激活服务器**重新激活并授权。

如果通过上述排查，仍然无法解决问题，请单击管理控制台右上方的“工单”，填写工单信息反馈问题现象，联系技术支持。

开启 RDP 强制登录

当Windows远程桌面连接数超过最大限制时，用户将无法登录。云堡垒机通过开启“admin console”，在远程桌面连接用户超限时，用户可挤掉已登录的用户，强制登录。

步骤1 登录堡垒机系统。

步骤2 选择“运维 > 主机运维”，进入主机运维列表页面。

步骤3 单击“Web运维配置”，弹出Web运维配置窗口。

步骤4 勾选“admin console”连接模式。

步骤5 单击“确认”，返回主机运维列表。

配置成功后，用户登录RDP协议类型主机时，若连接数已超过最大限制，会挤掉已登录用户，强制登录。

----结束

检查堡垒机镜像版本

检查方法：登录堡垒机后在“系统 > 关于系统”中查看“设备系统”的版本是否为3.3.54.0。

如果是，可能是服务器启用了keyboard。

解决办法：

- centos系统：将服务器配置文件/etc/ssh/sshd_config的ChallengeResponseAuthentication值设为no。
- Ubuntu系统：将服务器配置文件/etc/ssh/sshd_config的KbdInteractiveAuthentication值设为no。

检查资源操作系统是否为 sles

步骤1 执行以下命令检查资源系统是否为sles系统。

```
cat /etc/os-release
```

返回如下信息表示该资源系统为sles操作系统。

```
NAME="SLES"
VERSION="12-SP3"
ID="sles"
ID_LIKE="suse opensuse"
```

步骤2 确定为sles系统，执行以下命令将PasswordAuthentication值修改为yes，将ChallengeResponseAuthentication修改为no保存后退出。

```
/etc/ssh/sshd_config
```

----结束

12.2.7 运维资源列表可登录资源不可见怎么办?

问题现象

云堡垒机“主机运维”或“应用运维”列表页面，用户原可登录资源突然不可见了。

可能原因

- 资源授权的“访问控制策略”设置了“有效期”，用户访问资源权限失效。
- 资源授权的“访问控制策略”设置了“登录时段限制”，用户在“禁止登录”时间段不能查看登录资源。
- “访问控制策略”关联的用户或资源被移除，用户访问资源权限被取消。
- 资源授权的“访问控制策略”被禁用，用户失去该资源访问控制权限。
- 资源授权的“访问控制策略”被删除，用户失去该资源访问控制权限。

解决办法

查看资源授权的“访问控制策略”详情，根据实际情况重新配置或新建访问控制策略。

- 修改“访问控制策略”基本信息，重新配置“有效期”或“登录时段限制”。
- 启用被禁用的“访问控制策略”。
- 修改“访问控制策略”的详情，重新关联用户或资源。
- 若“访问控制策略”被删除，请新建策略关联用户和资源。

12.2.8 通过 Web 浏览器登录资源，不弹出会话界面怎么办?

问题现象

正常登录系统，在主机运维或应用运维列表，单击“登录”，不能正常跳转到运维会话页面。

可能原因

浏览器拦截限制或系统SSL证书过期。

解除浏览器拦截

1. 确认使用浏览器及版本，确认是否在推荐范围内。

   表 12-1 推荐浏览器及版本

浏览器	版本
Edge	44及以上版本
Chrome	52.0及以上版本
Safari	10及以上版本
Firefox	50.0及以上版本

2. 打开浏览器检查右上角地址栏，确认是否被浏览器拦截。
3. 根据不同操作系统，解除浏览器拦截。
   - 在Windows系统下，以Chrome浏览器为例，选择“始终允许显示弹出窗口”后即可登录资源。
   - 在macOS系统下，需要先设置Safari浏览器的偏好设置，将“阻止弹出式窗口”去掉勾选框。

图 12-3 Safari 浏览器限制

更新系统 SSL 证书

系统默认配置安全的自签发证书，受限于自签发证书的认证保护范围和认证保护时间限制，用户可替换证书。但当证书过期或安全扫描不通过时，用户需更新证书才能确保系统安全。

12.2.9 应用运维异常，调用程序失败怎么办?

应用发布程序启动路径配置错误

问题现象

用户配置完成应用发布资源后，通过云堡垒机首次访问应用发布资源，不能正常访问。

可能原因

- 原因一：应用程序启动路径配置错误。
- 原因二：配置应用程序非云堡垒机默认支持的应用程序，不支持调用。

解决办法

- 修改“程序启动路径”配置
  a. 登录云堡垒机系统，在应用服务器详情页面，查看配置的应用“程序启动路径”。
  b. 登录Windows应用服务器，查询应用安装路径，获取程序exe启动路径。
  c. 对比路径是否一致。若不一致，则需修改配置的“程序启动路径”。
- 重新安装支持的应用程序
  a. 登录Windows应用服务器，安装云堡垒机支持调用的应用，详情请参见**使用限制**。
  b. 登录云堡垒机系统，重新配置应用服务器“程序启动路径”。

Windows 主机重启后，无法调用应用程序

问题现象

Windows应用服务器系统升级前，可以正常访问应用发布资源。系统升级重启后，访问应用发布资源被拒绝，无法调用配置的应用程序，提示“无法启用此初始程序”错误。

可能原因

Windows病毒和威胁防护更新后，对执行程序进行病毒检查时，Windows Defender会禁止启用所有名称中含有“administrator”字样的exe程序，例如默认支持的数据库应用程序“mysqladministrator.exe”。

解决办法

- 修改程序名称

  在Windows应用服务器修改应用的启动程序名称，并在云堡垒机配置中修改应用的“程序启动路径”。

- 关闭Windows Defender

  在Windows应用服务器控制面板，选择“设置 > 更新和安全 >Windows Defender”，关闭Windows Defender的“实时保护”。

12.2.10 SSO 工具异常，不能登录数据库资源怎么办?

版本升级后无法登录数据库

问题现象

版本升级前可以正常登录数据库资源，版本升级后不能登录数据库资源，提示“已安装单点登录工具，仍无法登录，请重试或安装最新版工具”。

可能原因

云堡垒机版本升级后，SsoTools单点登录工具未升级，不能正常匹配连接。

解决办法

每次云堡垒机版本升级后，都需卸载本地SsoDBSettings单点登录工具，重新下载安装单点登录工具，并正确配置数据库客户端路径。

数据库客户端路径配置错误

问题现象

用户首次登录数据库资源，提示“数据库客户端工具路径配置有误，请重新配置！”，不能正常登录。

可能原因

在SsoTools单点登录工具上，配置的数据库客户端路径不正确，或未配置路径。

解决办法

打开SsoTools单点登录工具，检查数据库客户端路径是否正确，配置正确的客户端路径。

12.2.11 通过堡垒机登录服务器资源，报“并发会话超出许可限制”怎么办?

问题现象

多个用户同时通过SSH连接方式登录云堡垒机纳管的服务器时，堡垒机允许同时登录的账号数有上限，当登录的账号数超出上限值时，必须退出一个账号才能再登录一个账号。

问题原因

该问题是由于并发数限制导致的。

解决办法

云堡垒机支持多种资产规格配置，不同规格云堡垒机的并发数配置有差异。

建议您**变更版本规格**以提高并发数。

12.2.12 如何解决“mstsc 客户端访问服务器资源时鼠标出现黑块”的问题?

当通过mstsc客户端访问服务器资源时，如果鼠标出现黑块时，按如下方法解决处理。

操作步骤

步骤1 登录目标服务器。

步骤2 打开控制面板，单击“设备”。

步骤3 在左侧导航树中，单击“鼠标”，进入鼠标的配置页面。

步骤4 单击“其他鼠标选项”，选择“指针”页签。

步骤5 去掉勾选“启用指针阴影”的选项，单击“确定”。

----结束

12.2.13 访问 Windows 应用发布服务器，提示“创建用户失败”怎么办?

问题现象

发布Windows应用之后，应用运维单击登录，报错信息：访问Windows应用发布失败，提示“创建用户失败”。

可能原因

- 原因一：应用发布服务器中安装的RemoteAppProxy跳板工具版本过低，需要升级。
- 原因二：创建影子账户用户名最大长度和服务器账户最大长度冲突。

解决办法

- 解决办法一：将应用发布服务器安装的RemoteAppProxy组件升级至最新版本，具体操作请参见**升级RemoteApp或app_publisher程序**。
- 解决办法二：登录应用发布服务器，修改“C:\DevOpsTools\RemoteAPPProxy\Application.ini”文件，修改参数影子账户用户名最大长度**max_user_length=20**将值改为服务器支持的创建用户长度，例如15。

  说明

  若您不想通过升级RemoteAppProxy跳板工具的临时处理方法，可登录应用发布服务器修改“C:\DevOpsTools\RemoteAPPProxy\Application.ini”文件，修改参数，关闭影子账户：use_shadow_user=0

  是否使用影子账户模式的参数说明：

  - 1：开启
  - 0：关闭

12.3 运维故障

12.3.1 登录云堡垒机实例时，收不到短信验证码怎么办?

问题现象

- 配置“手机短信”方式多因子登录后，通过手机短信方式登录，不能获取手机验证码，提示“发送短信失败！”。
- 重置登录密码，收不到短信验证码。

可能原因

- 原因一：受浏览器兼容性限制，当浏览器版本与云堡垒机系统不匹配时，会导致不能获取到短信验证码，甚至登录后页面显示异常和无法操作。
- 原因二：安全组限制了短信网关IP，或未放开10743、443端口。
- 原因三：用户手机号码配置错误。
- 原因四：用户手机短信业务有异常。
- 原因五：堡垒机实例未绑定弹性公网IP（Elastic IP，EIP）。

解决办法

- 原因一：

  更换浏览器或升级浏览器版本，通过Web登录推荐使用浏览器及版本请参见**表12-2**。

  表 12-2 推荐浏览器及版本

浏览器	版本
Edge	44及以上版本
Chrome	52.0及以上版本

浏览器	版本
Safari	10及以上版本
Firefox	50.0及以上版本

- 原因二：
  云堡垒机实例绑定的安全组放开短信网关IP和10743、443端口。
- 原因三：
  普通用户请联系管理员，修改绑定的手机号码。

  说明

  若**admin**用户配置了手机短信登录，但手机号码配置错误，请直接联系技术支持。
- 原因四：
  用户确认绑定手机的短信业务状态，请从以下几个方面分别确认：
  - 确认手机是否欠费停机。
  - 确认验证短信是否被拦截归为垃圾短信。
  - 确认手机网络通讯是否正常。
- 原因五：
  用户若需登录云堡垒机系统，必须首先为实例绑定弹性IP。为满足CBH使用需求，建议配置EIP带宽为5M以上。

12.3.2 无法添加资源，提示“资源超出许可限制”怎么办?

问题现象

登录云堡垒机系统，在主机管理或应用发布中添加资源，提示“资源超出许可限制”，不能继续添加资源。

可能原因

添加资源总数已达到实例规格“资产数”上限，继续添加资源超出许可资产数限制。

解决办法

1. 升级实例规格，详细操作指导请参见**变更版本规格**。
2. 删除闲置或僵尸资源账户，详细操作指导请参见**删除资源**。
   为加强资源管控，可**设置账户同步策略**，自动发现并删除僵尸账户等。

12.3.3 主机资源账户验证不通过怎么办?

问题现象

- 添加主机资源账户时验证账户，提示“验证账户超时”。
- 添加主机资源账户时验证账户，提示“输入错误的账户密码”。
- 添加主机资源账户后验证账户，任务中心验证结果显示失败，提示“主机不可达”。

- 添加主机资源账户后验证账户，任务中心验证结果显示失败，提示“密码错误”

可能原因

原因一：主机信息配置错误，例如主机IP或端口配置错误。

原因二：主机资源账户密码配置错误。

原因三：主机网络延时，网络状况差。

解决办法

原因一：

- 返回主机信息配置页面，或进入主机详情页面，修改主机IP地址、端口等基本信息。

原因二：

- 返回主机资源账户配置页面，或进入资源账户详情页面，修改主机资源账户密码。

原因三：

- 重启相应主机资源，检查主机资源网络状况。

12.3.4 打开系统数据文件显示乱码怎么办?

问题现象

用户将CBH系统数据导出为csv文件，并以Excel工具打开文件，文件内数据信息乱码。

可能原因

云堡垒机系统导出的csv文件使用了UTF-8编码格式，而Excel工具以ANSI编码格式打开文件，编码方式不一致而导致数据信息识别错误，出现乱码。

解决办法

使用记事本等文本编辑器打开csv文件，另存文件时选择编码为ANSI格式。

文件另存成功后，重新用Excel工具打开文件，文件信息即可显示正常。

12.3.5 运维会话经常提示登录超时，断开连接怎么办?

问题现象

- 在Web运维会话界面，登录超时连接断开，提示“由于您长时间未操作，此会话已结束”。
- 云堡垒机系统未退出登录，但运维会话界面主机资源断开连接。

可能原因

- 原因一：用户使用默认“登录超时”30分钟，在云堡垒机运维会话超过30分钟无操作，云堡垒机系统退出登录，登录的资源断开连接。

- 原因二：ECS主机资源系统空闲等待时间或锁屏超时时间设置不合理，配置时间太短，ECS主机系统超时退出。

解决办法

- 原因一：
  - 重新设置“登录超时”时间，延长登录超时时间，详细配置说明请参见**Web登录安全配置**。
  - 保持云堡垒机运维会话界面在线状态。
- 原因二：
  - 设置Linux主机的空闲等待时间TMOUT，即设置TMOUT=目标时间。
  - 设置Windows主机的锁屏超时时间，即在Windows主机系统设置中，重新选择目标超时锁屏时间。

12.3.6 应用运维调用 PL/SQL 客户端，文本乱码了怎么办?

问题现象

应用发布纳管Oracle Tool应用客户端PL/SQL Developer，通过Web浏览器登录应用资源，PL/SQL客户端乱码。

可能原因

PL/SQL客户端为英文编码，Oracle数据库的编码格式与PL/SQL客户端的编码格式不统一，使得PL/SQL客户端不兼容，导致乱码。

解决办法

步骤1 查看Oracle数据库字符集。

在PL/SQL客户端中，执行以下命令，查看Oracle数据库的编码格式。

select userenv('language') from dual;

获取编码默认值“SIMPLIFIED CHINESE_CHINA.ZHS16GBK”

步骤2 修改PL/SQL客户端的编码格式。

在应用发布的服务器上，创建一个“NLS_LANG”的系统环境变量，设置其值为“SIMPLIFIED CHINESE_CHINA.ZHS16GBK”。

步骤3 重新启动PL/SQL客户端，检索内容验证。

----结束

12.3.7 登录主机资源后，提示“拒绝请求的会话访问”怎么办?

问题现象

用户Web浏览器登录主机资源后，提示“拒绝请求的会话访问”，不能正常运维会话。

可能原因

云堡垒机系统配置了“admin console”连接模式，当主机远程桌面登录用户数上限后，新登录用户可强制登录RDP协议类型主机，已登录的用户将被强制下线，不能继续运维会话。

解决办法

步骤1 登录云堡垒机系统。

步骤2 选择“运维 > 主机运维”，进入“主机运维”列表页面。

步骤3 单击“Web运维配置”，弹出配置窗口。

步骤4 不勾选“admin console”连接模式选项。

步骤5 单击“确认”，返回主机运维列表页面，重新登录主机资源。

----结束

12.3.8 云堡垒机带宽超限了怎么办?

问题现象

云堡垒机使用过程中，报“流量超出带宽”错误，不能正常使用云堡垒机系统和登录资源。

可能原因

云堡垒机使用过程中的流量带宽，超过绑定的EIP的共享带宽或独享带宽的最大限制。

解决办法

步骤1 登录管理控制台，排查EIP带宽受限原因，详情请参见如何排查带宽超过限制?

步骤2 重新配置云堡垒机绑定EIP的带宽，建议配置5Mbit/s以上带宽，详细带宽说明请参见VPC共享带宽。

----结束

12.3.9 通过 Web 浏览器运维，不能复制文本怎么办?

无法复制/粘贴文本

问题现象

用户在主机运维会话界面，不能使用复制/粘贴功能。

可能原因

- 原因一：授权用户或主机资源未开启“剪切板”功能权限。
- 原因二：Windows主机中剪切板程序故障或假死。

解决办法

- 原因一

用户获取主机资源“剪切板”权限，分别需要开启主机“剪切板”功能和授权用户“剪切板”使用权限。

- 主机资源开启“剪切板”功能，请参见**修改主机配置**。
- 授权用户“剪切板”权限，请参见**修改访问控制策略**或**申请访问授权工单**。

- 原因二

  重载或重启Windows主机中rdpclip.exe剪切板程序。

无法复制超长文本到 Windows 主机

问题现象

从用户本地复制文本到Windows主机资源，提示“粘贴文本超长，建议使用文件管理功能”。

可能原因

云堡垒机“复制/粘贴”有字符数限制，不支持从用户本地“复制/粘贴”超过8万字符的文本。

解决办法

步骤1 用户获取主机资源“文件管理”权限，分别需要开启主机“文件管理”功能和授权用户“文件管理”权限。

1. 主机资源开启“文件管理”功能，请参见**修改主机配置**。
2. 授权用户“文件管理”权限，请参见**修改访问控制策略**或**申请访问授权工单**。

步骤2 用户将文本先复制到文本文件中，再将文件从本地上传到“主机网盘”。打开Windows主机的G盘目录，获取文件中超长文本内容。

----结束

更多复制/粘贴使用说明，请参见**通过Web运维，如何使用快捷键复制/粘贴文本？**。

12.3.10 资源运维过程有哪些常见报错?

通过云堡垒机登录资源，运维过程系统发出请求后，若遇到错误，会在响应中包含响应的错误码，以及描述错误信息。

CBH系统的常见错误码，以及错误排查方法，请参见**表12-3**。

表 12-3 常见运维错误码

错误码	错误提示	排查方法
ERROR_CLIENT_514	Code：C_514 文件传输响应时间过长，请重试或联系系统管理员	1. 检查CBH系统与FTP服务的网络，是否存在传输丢包现象； 2. 本地登录FTP服务器，检查是否能正常上传文件； 3. 检查本地网络，是否限制上传文件的大小； 4. 请填写工单反馈问题现象，联系技术支持。

错误码	错误提示	排查方法
ERROR_CLIENT_515	Code：C_515 运维资源过程中遇到一个错误，请重试或联系系统管理员	1. 尝试本地登录故障主机资源，或者登录同网段的其他资源进行测试； 2. 检查主机**/etc/hosts.deny**文件配置，是否将CBH系统IP加入了黑名单，详细解决办法请参见**Code：C_515错误**； 3. 检查CBH系统与故障主机的网络层，是否有服务协议拦截CBH系统IP； 4. 请填写工单反馈问题现象，联系技术支持。
ERROR_CLIENT_519	Code：C_519 由于资源连接失败或不可达，当前无法访问。如果持续出现该问题，请通知系统管理员或检查系统日志	1. 检查CBH系统与主机资源的网络是否互通； 2. 本地登录主机资源，输入命令**route -n**，检查目标主机的路由表，是否存在丢失CBH路由现象； 3. 请填写工单反馈问题现象，联系技术支持。详细解决办法请参见**Code：C_519错误**。
ERROR_CLIENT_520	Code：C_520 由于RDP拒绝了此次连接或等待数据出错，资源无法访问。如果持续出现该问题，请通知系统管理员或检查系统日志	1. 检查Windows主机资源的远程配置，是否开启远程桌面； 2. 本地MSTSC方式登录主机资源，检查是否可以正常登录； 3. 请填写工单反馈问题现象，联系技术支持。
ERROR_CLIENT_521	Code：C_521 由于其他用户登录导致连接发生冲突，请稍后重试	1. 本地登录Windows主机资源，输入命令**gpedit.msc**，设置“限制链接的数量”，修改已启用的最大链接数；或关闭“限制每个用户只能进行一个会话”选项。 2. 请填写工单反馈问题现象，联系技术支持。
ERROR_CLIENT_522	Code：C_522 于RDP闲置时间超时，连接已断开，如果不是本人意愿，请通知系统管理员或检查系统设置	1. 本地登录Windows主机资源，输入命令**gpedit.msc**，修改“为断开的会话设置时间”选项； 2. 本地MSTSC方式登录主机资源，检查是否出现RDP超时错误； 3. 请填写工单反馈问题现象，联系技术支持。
ERROR_CLIENT_523	Code：C_523 由于连接被管理员断开、账户被注销或登录资源时长达到上限，连接已断开，如果不是本人意愿，请通知系统管理员或检查系统日志	1. 检查RDP连接是否被管理员强制断开； 2. 检查系统用户是否被服务器管理员注销； 3. 检查系统用户登录时长是否超过限制。

错误码	错误提示	排查方法
ERROR_CLIENT_769	Code：C_769 登录失败，有可能是账户名、密码或密钥错误，请尝试重新连接	1. 本地登录故障主机资源，检查资源账户和密码是否正确； 2. 检查主机资源是否开启双因子认证； 3. 检查主机资源是否拒绝root账户登录； 4. 请填写工单反馈问题现象，联系技术支持。详细解决办法请参见**Code：C_769错误**。
ERROR_CLIENT_771	Code：C_771 请联系管理员授予从账户访问权限，或检查您的系统设置	检查主机资源是否开启目标账户远程登录权限。
ERROR_CLIENT_776	Code：C_776 • 由于浏览器长时间无响应，连接已断开，请检查您的网络并重试。 • 由于浏览器长时间无响应，连接已断开，请检查应用发布服务器安全组的出方向访问策略，需要放通访问堡垒机IP 443端口。	检查本地浏览器运行状态，推荐使用Chrome浏览器。
ERROR_CLIENT_797	Code：C_797 连接数超过使用限制，请关闭一个或多个连接后重试	本地登录Windows主机资源，输入命令**gpedit.msc**，设置“限制链接的数量”，修改已启用的最大链接数。
ERROR_TUNNEL_514	Code：T_514 由于服务器长时间无响应，连接已断开，请检查您的网络并重试	1. 检查CBH系统与主机资源间网络是否稳定； 2. 检查CBH系统与主机资源的网络是否互通； 3. 请填写工单反馈问题现象，联系技术支持。详细解决办法请参见**Code：T_514错误**。
ERROR_TUNNEL_520	Code：T_520 由于H5服务器H5代理服务器拒绝了此次连接，请检查您的网络并重试	1. 检查主机资源IP地址或端口等配置是否正确； 2. 检查主机资源是否开启guacd服务； 3. 检查主机资源guacd服务是否接受CBH系统IP的连接； 4. 请填写工单反馈问题现象，联系技术支持。

12.3.11 堡垒机 IP 绑定域名，再将域名添加到 WAF 中进行防护，添加完成后访问不成功怎么处理?

堡垒机IP绑定域名，再将域名添加到WAF中进行防护，添加完成后访问不成功 ，报错重定向过多。

解决办法

步骤1 关闭堡垒机来源IP检测功能，详情请参见**Web登录配置**。

步骤2 进入“系统 > 系统维护 > 系统管理”，在“系统地址”下添加系统地址并单击“立即更新”即可正常登录。

----结束

12.3.12 应用运维登录后显示本次链接已断开怎么处理?

问题现象

应用运维登录后页面直接弹窗提示本次链接已断开，无法继续正常操作。

问题分析

在登录前可能重启过应用发布服务器，导致原有配置文件RemoteAPPProxy.conf丢失。

解决办法

重新添加RemoteAPPProxy.conf配置文件。

步骤1 登录服务器进入C:\DevOpsTools\RemoteAPPProxy\目录。

步骤2 在路径下创建名称为RemoteAPPProxy.conf的文本文件。

步骤3 创建后打开文本文件配置如下信息。

ServiceAddress = https://ip:port

说明

ip为目标堡垒机内网地址，port为443。

步骤4 确认无误，保存退出，重新登录即可。

----结束

12.3.13 跨版本升级之后证书状态异常怎么处理?

如果在升级CBH时有跨版本升级的情况，升级后需要重新上传证书，也可以按照迭代版本依次升级。

原因分析

- 可能存在原有证书过期之类的情况。

- 证书状态异常之前做过跨版本升级堡垒机的操作，升级之后证书和手动添加的路由都会受影响，需要重新同步证书。

解决办法

原有证书过期

需要您自行重新购买商业证书后在CBH进行替换，替换操作详情请参见**证书替换**。

跨版本升级导致

步骤1 登录云堡垒机系统。

步骤2 选择“系统 > 系统配置 > 安全配置”，进入系统“安全配置”管理页面。

步骤3 在“Web证书配置”区域，单击“编辑”，弹出Web证书更新窗口。

步骤4 上传下载到本地的证书文件。

步骤5 证书文件上传成功之后，输入keystore密码，证书密码验证文件。

步骤6 单击“确定”，返回安全配置管理页面，查看当前系统Web证书信息。

说明

证书信息更新之后，为了使证书有效，通过管理控制台或者堡垒机系统工具重启堡垒机系统。

步骤7 查看证书信息无误，更新完成。

----结束

12.4 SSO 运维故障

12.4.1 DBeaver 配置自定义驱动连接 GaussDB 数据库

支持通过DBeaver自定义配置驱动连接Gaussdb数据库。

版本要求

3.3.52.0及以上版本。

网络要求

- PC端到堡垒机：18000
- 堡垒机到GaussDB数据库：对应的数据库端口，默认8000

堡垒机侧配置

步骤1 登录堡垒机web界面，单击右上角下载中心，进入“下载中心”，下载“单点登录工具Windows”。

步骤2 选择“资源 > 主机管理”，新建GaussDB协议主机。

步骤3 新建后，通过“策略 > 访问控制策略”给用户关联GaussDB协议主机的访问权限。

----结束

DBeaver 客户端配置

步骤1 打开DBeaver客户端，进入“数据库 > 驱动管理器”单击“新建”。

表 12-4 新建参数说明

参数名称	参数说明
驱动名称	命名为便于识别的名称，例如GaussDB
驱动类型	选择Generic
类名	org.postgresql.Driver
URL模板	jdbc:postgresql://{host}[:{port}]/[{database}]
默认端口	需要连接的数据库端口。默认8000

步骤2 选择“库”页签，单击“添加文件”，添加gsjdbc4.jar，驱动包文件需与数据库版本一致。

- 下载对应版本的驱动包：**获取驱动包**
- 下载解压后进入解压目录GaussDB_driver\GaussDB_driver\Centralized\Euler2.5_X86_64，并解压Jdbc压缩包。

步骤3 添加完成后，单击“确定”，重新编辑对应驱动，单击“找到类”。

步骤4 打开DBeaver客户端，直连目标GaussDB数据库，数据库选择**步骤一**新建的驱动文件。

步骤5 单击“完成”，连接成功后，打开文件：C:\sso\SsoTool\DBeaver\General\.DBeaver\data-sources.json，确认生成了对应连接，并打开文件C:\sso\SsoTool\ssotool.conf

将C:\sso\SsoTool\DBeaver\General\.DBeaver\data-sources.json参数填入C:\sso\SsoTool\ssotool.conf，填入后ssotool.conf对应行取消注释保存文件。

步骤6 进入“运维 > 主机运维”，访问对应协议主机。

----结束

12.4.2 配置 DBeaver 连接 GaussDB 数据库

版本要求

3.3.50.0及以上版本。

网络要求

- PC端到堡垒机：18000
- 堡垒机到GaussDB数据库：对应的数据库端口，默认8000

DBeaver 客户端配置

步骤1 通过DBeaver直连GaussDB数据库，数据库选择PostgreSQL，连接时会提示下载驱动，下载驱动后进行连接。

步骤2 DBeaver配置驱动，获取云数据库GaussDB驱动包，驱动包版本需与GaussDB数据库版本一致。

- 下载对应版本的驱动包：**获取驱动包**
- 解压后进入解压目录GaussDB_driver\GaussDB_driver\Centralized\Euler2.5_X86_64，并解压Jdbc压缩包。

步骤3 打开DBeaver客户端，选择“数据库 > 驱动管理器 > PostgreSQL”单击“编辑”选择“库”，删除库中原始的驱动后，导入gsjdbc4.jar。

步骤4 导入后单击“确定”，重新编辑postgres驱动，单击“找到类”。

步骤5 Gaussdb开启ssl配置，在DBeaver中配置ssl禁用。

打开DBeaver客户端，选择“数据库 > 驱动管理器 > PostgreSQL”单击“编辑”选择“连接属性”，添加属性sslmode，参数值为disable。

步骤6 配置工作空间。

“文件 > 切换工作空间”设置为C:\sso\SsoTool\DBeaver。

----结束

12.4.3 mysql 协议访问数据库，执行备份数据库表提示 1251-lost connection to mysql server during query

问题现象

mysql协议访问数据库，执行备份数据库表提示lost connection to mysql server during query

后台查看proxy日志，提示内存溢出。

解决办法

该问题在3.3.34镜像版本修复，升级至该版本即可。

12.4.4 mysql 主机运维失败，提示：1251-Client does not support authentication protocol requested by server

问题现象

mysql主机运维失败，提示：1251-Client does not support authentication protocol requested by server

可能原因

堡垒机IP可能被限制。

解决办法

登录数据库，执行以下命令，查看对应用户的Host值是否限制了堡垒机ip，如果被限制，需要解除。

```
select * from user
```

说明

堡垒机ip在“系统 > 系统配置 > 网络配置”中查看，或者在云控制台对应堡垒机实例查看。

12.4.5 访问 mysql 协议主机失败，提示：“2013-Lost connection to MySQL server at ‘waiting for initial communicationpacket system error0”

问题现象

访问mysql协议主机失败，提示：“2013-Lost connection to MySQL server at ‘waiting for initial communicationpacket’,system error:0”

可能原因

- 33306或3306端口可能未放通。
- 域名解析的网卡为多个。

解决办法

- 将本地pc到堡垒机的33306端口，堡垒机到数据库服务器的3306端口放通。
- 域名访问堡垒机web界面，域名解析的是多个网卡。
  登录堡垒机后台，执行以下命令，添加域名：域名=堡垒机ip。
  ```
  vim /usr/local/yunanbao/apache-tomcat-7.0.82/webapps/ROOT/WEB-INF/classes/domain.properties
  ```

12.4.6 Oracle 协议访问数据库提示：ORA-12537_TNS_连接关闭

问题现象

Oracle协议访问19c数据库提示：ORA-12537:TNS:连接关闭

可能原因

1521端口可能未放通。

解决办法

将本地pc到堡垒机的1521，堡垒机到数据库服务器的1521端口放行。

12.4.7 Oracle 协议访问数据提示：ORA-12637_包接收失败

问题现象

堡垒机升级到 3.3.26.0 后，Oracle协议调用PL/SQL客户端访问数据库报错：ORA-12637:包接收失败处理

可能原因

配置文件oci.dll缺失

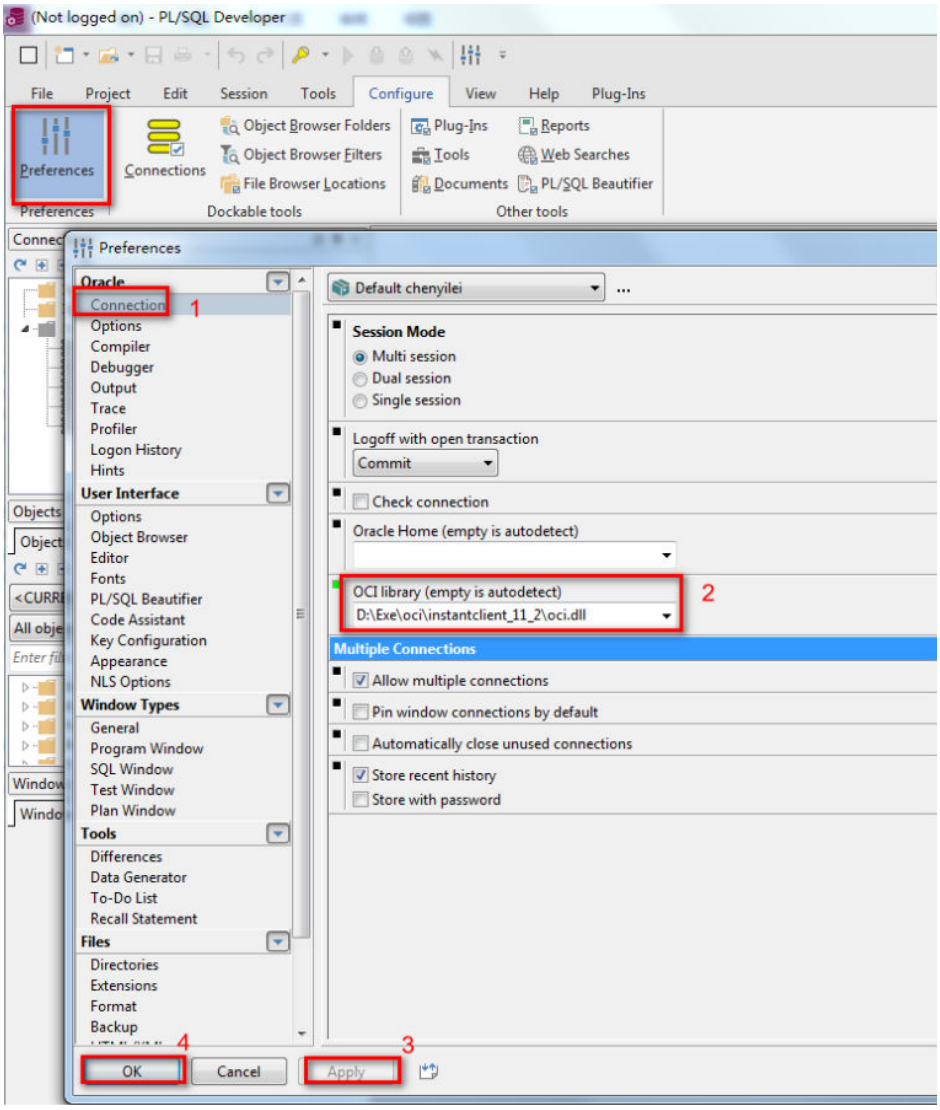
解决办法

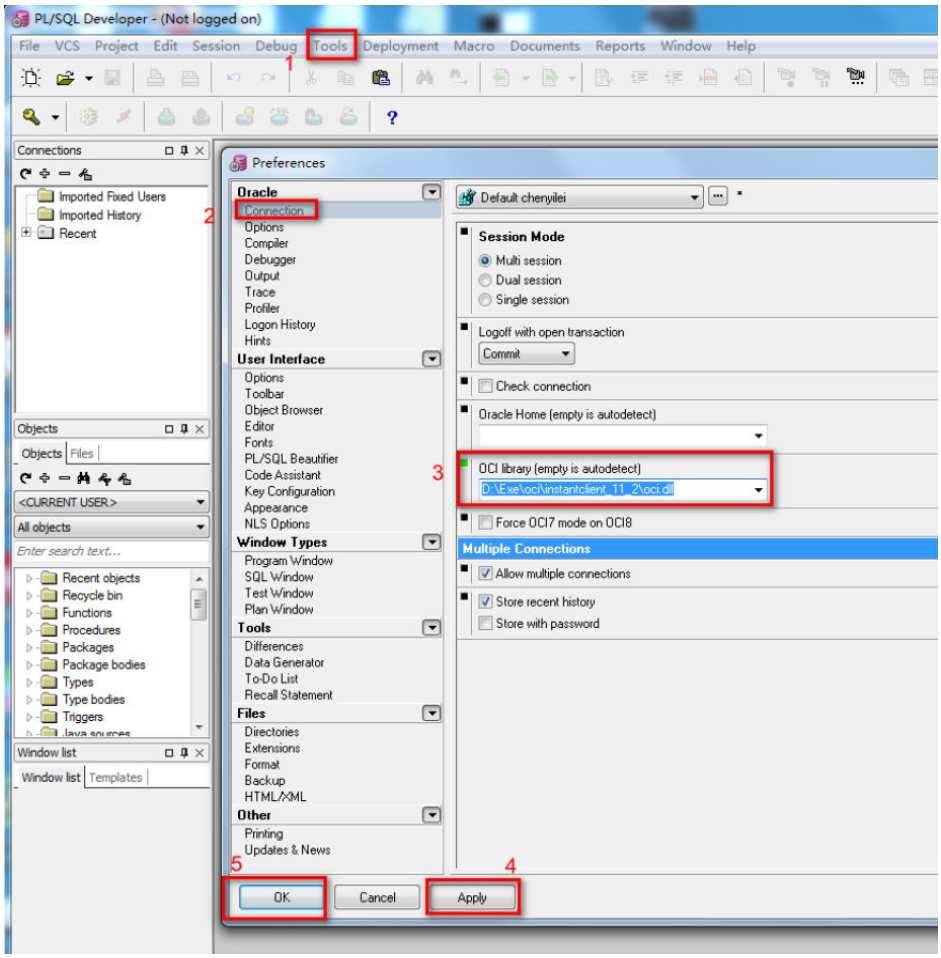
步骤1 下载oci.dll文件，oci位数根据PL/SQL位数下载。

步骤2 下载后进行解压，确认oci.dll文件在解压的目录中。

步骤3 在PL/SQL配置oci.dll，配置后需要关闭程序才生效。

图 12-4 配置文件





----结束

12.4.8 主机运维 Oracle 失败，提示：ora 12170 TNS 连接超时

问题现象

主机运维Oracle失败，提示：ora:12170 tns 连接超时

可能原因

客户端和虚拟IP之间网络不通。

解决办法

步骤1 确认网络通信正常。

- PC端到堡垒机：1521
- 堡垒机到数据库：Oracle数据库默认1521端口

步骤2 如果网络通信正常，在堡垒机后台抓包，确认纳管在堡垒机上的数据库ip是否是数据库节点真实ip，而不是Oracle数据库的虚拟ip。

----结束

12.4.9 主机运维调用 DBeaver 连接 Postgres 数据库失败

问题现象

主机运维调用DBeaver连接postgres数据库失败。

可能原因

网络不通

解决办法

步骤1 确认网络是否通信正常。

- PC端到堡垒机：15432
- 堡垒机到数据库：PGSQL数据库的端口

步骤2 如果通信正常，确认PGSQL启用ssl，在DBeaver中禁用ssl。

打开DBeaver客户端，进入“数据库 > 驱动管理器”单击“编辑”选择“连接属性”添加属性：sslmode，参数值为disable。

----结束

12.4.10 SSO 拉起客户端失败，主机运维后提示：运行环境缺少 jre

问题现象

SSO客户端拉起数据库客户端失败，主机运维后提示：运行环境缺少jre。

可能原因

进程或监听端口对应镜像版本不正确。

解决办法

- 主机运维数据库主机后，确认存在YabLocalAgent.exe进程，3.3.56.0及以上版本为LocalAgent.exe进程。
- 确认存在LocalAgent主进程端口监听，3.3.56.0以下版本7001端口，3.3.56.0及以上版本为9010端口。且运维pc不存在冲突端口。

  netstat -ano |findstr 7001

  netstat -ano |findstr 9010

