云堡垒机(CBH)

用户指南

文档版本 01

发布日期 2025-12-10

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 产品介绍

1.1 什么是云堡垒机

云堡垒机（Cloud Bastion Host，CBH）是一款统一安全管控平台，为企业提供集中的账号（Account）、授权（Authorization）、认证（Authentication）和审计（Audit）管理服务。

云堡垒机提供云计算安全管控的系统和组件，包含部门、用户、资源、策略、运维、审计等功能模块，集单点登录、统一资产管理、多终端访问协议、文件传输、会话协同等功能于一体。通过统一运维登录入口，基于协议正向代理技术和远程访问隔离技术，实现对服务器、云主机、数据库、应用系统等云上资源的集中管理和运维审计。

服务特点

- 一个实例对应一个独立运行的系统，通过配置实例部署系统后台运行基本环境。系统环境独立管理，保障系统运行安全。
- 一个单点登录系统，提供统一的单点登录入口，轻松地集中管理大规模云上资源，避免资源账户泄露危险，保障资源信息安全。
- 符合“网络安全法”等法律法规，满足合规性规范审查要求。
  - 满足《萨班斯法案》和《等级保护》系列文件中的技术审计要求；
  - 满足金融监管部门的技术审计要求；
  - 满足各类法令法规（如SOX、PCI、企业内控管理、等级保护、ISO/IEC27001等）对运维审计的要求。

1.2 产品优势

HTML5 一站式管理

无需安装特定客户端，无需安装任何插件，任意终端的主流浏览器，包括移动端APP浏览器登录，用户随时随地打开即可进行运维。

系统HTML5管理界面简洁易用，集中管理用户、资源和权限，支持批量创建用户、批量导入资源、批量授权运维、批量登录资源等高效运维管理方式。

操作指令准确拦截

针对资源敏感操作进行二次复核，系统预置标准Linux字符命令库或自定义命令，对运维操作指令和脚本的准确拦截，并可通过异步“动态授权”，实现对敏感操作的动态管控，防止误操作或恶意操作的发生。

核心资源二次授权

借鉴银行金库授权机制，针对重要资源的运维权限设置多人授权，若需登录此类资源，需多位授权候选人进行“二次授权”，加强对核心资源数据的保护，提升数据安全防护能力和管理能力，保障核心资产数据的安全。

应用发布扩展

针对数据库类、Web应用类、客户端程序类等不同应用资源，提供统一访问入口，并可提高对应用操作的图形化审计。

数据库运维审计

针对DB2、MySQL、SQL Server和Oracle等云数据库，支持统一资源运维管理，以及SSO单点登录工具一键登录数据库，提供对数据库操作的全程记录，实现对云数据库的操作指令进行解析，100%还原操作指令。

自动化运维

自动化运维是将系统运维管理中复杂的、重复的、数量基数大的操作，通过统一的策略、任务将复杂运维精准化和效率化，帮助运维人员从重复的体力劳动中解放出来，提高运维效率。

1.3 应用场景

任何企业都需要安全运维管理和审计，故任何企业都需要云堡垒机。云堡垒机能适用于各种企业运维场景，特别针对企业员工数量复杂、企业资产数量繁杂、人员运维权限交叉、企业运维方式多样等场景。

严格要求的审计合规场景

例如保险和金融行业，具有大量个人信息数据和金融资金操作行为，以及大量第三方机构代为运作，可能存在巨大违规操作、滥用职权等非法运作风险。

通过在云上部署云堡垒机系统，单点登录入口，集中管理账户和资源，部门权限隔离，核心资产多人审核授权，敏感操作二次复核授权，健全的运维审计机制，能够为高风险行业提供严要求审计功能，满足行业监管要求。

高效稳定的运维场景

例如极速发展的互联网企业，大量经营数据等敏感信息，暴露在公网，且由于服务高度公开，存在高度数据泄露风险。

云堡垒机在远程运维过程中，隐藏资产真实地址，解决远程运维资产信息暴露问题。同时提供全面的运维日志，为审计运维和代运维人员的操作行为，提供有效监控，减少网上安全事故，助力企业长久稳定发展。

大量资产和人员管理场景

随着民生政务和传统企业集团的上云管理，云上人员账户数量不断增加，以及云上服务器、网络设备等资产数量也成倍增长。同时很多企业为解决人力不足的问题选择把系统运维转交给系统供应商或第三方代维商进行，由于涉及提供商、代维商过多，人员复杂流动性又大，对操作行为缺少监控带来的风险日益凸显。

云堡垒机针对大量用户和大量资产，可海量容纳庞大人员和资源数据，运维人员单点登录，解决运维人员维护多台资产效率低，易出错的问题。同时通过制定细粒度权限控制，资源操作全程记录，可审计全量用户操作行为，并对事故问题进行有效追溯，确保有效定责。此外，系统桌面实时呈现运维全景，并可接收异常行为告警通知，确保人员无法越权操作。

1.4 产品功能

云堡垒机不仅拥有传统4A安全管控的基本功能特性，包括身份认证、账户管理、权限控制、操作审计四大功能。还拥有高效运维、工单申请等特色功能。

身份认证

采用多因子认证和远程认证技术，加强用户身份认证管理。

- 引用多因子认证技术，包括手机短信、手机令牌、USBKey、动态令牌等方式，安全认证登录用户身份，降低用户账号密码风险。
- 对接第三方认证服务或平台，包括AD域、RADIUS、LDAP、Azure AD远程认证，支持远程认证用户身份，防止身份泄露。并支持一键同步AD域服务器用户，复用原有用户部署结构。

账户管理

集中管理系统用户和资源账号信息，对账号全生命周期建立可视、可控、可管运维体系。

表 1-1 账号管理功能说明

功能特性	功能说明
用户账号管理	系统用户账号全生命周期管理，用户使用唯一账号登录系统，解决共享账号、临时账号、滥用权限等问题。 • 批量导入 通过同步第三方服务器用户，以及批量导入用户，支持一键同步并导入已有用户信息，无需重复创建用户。 • 用户组 用户账号按属性分组管理，可实现对同类型用户按用户组赋予权限。 • 批量管理 支持批量管理用户账号，包括删除、启用、禁用、重置密码、修改用户基本配置等。

功能特性	功能说明
资源账户管理	集中资源账户管理，资源账户全生命周期管理，实现单点登录资源，管理或运维无缝切换。 ● 资源类型 纳管资源类型丰富，包括Windows、Linux等主机资源，MySQL、Oracle等数据库资源，以及Windows应用程序资源。 – 支持C/S架构运维接入，包括SSH、RDP、VNC、TELNET、FTP、SFTP、DB2、MySQL、SQL Server、Oracle、SCP、Rlogin协议类型主机资源。 – 支持B/S、C/S架构应用系统资源接入，可直接配置12+种Edge、Chrome、Oracle Tool等浏览器或客户端Windows服务器应用资源。 ● 资源管理 – 批量导入 通过自动发现、同步云上资源，以及批量导入资源，支持一键同步并导入云上ECS、RDS等服务器上资源。 – 账户组管理 资源账户按属性分组管理，可实现对同类型资源账户按账户组给用户赋权 – 密码自动代填 采用AES256加密方式存储资源账户，通过密码自动代填技术加密共享账户，避免账户泄露风险。 – 账户自动改密 通过设置改密策略，可定时定期修改账户密码，确保资源的账户安全。 – 账户自动同步 通过设置账户同步策略，可定时定期核查和同步主机资源账户，包括拉取主机账户统计异常系统资源账户，以及推送系统新建、删除、修改的资源账户到主机，确保资源账户健康生存周期。 – 批量管理 支持批量管理资源信息和资源账户，包括删除资源、添加资源标签、修改资源信息、验证资源账户、删除资源账户等。

权限控制

集中管控用户访问系统和资源的权限，对系统和资源的访问权限进行细粒度设置，保障了系统管理安全和资源运维安全。

表 1-2 权限控制功能说明

功能特性	功能说明
系统访问权限	从单个用户账号属性出发，控制用户登录和访问系统权限。 ● 用户角色 通过为每个用户账号分配不同的角色，赋予用户访问系统不同模块的权限，对系统用户身份进行分权。 系统支持自定义角色，自定义角色中可以自选添加系统模块，实现角色多样化模式。 ● 组织部门 通过为每个用户划分部门，采用部门组织树形结构，不限制部门层级，可将用户按部门分层级管理。 ● 登录限制 通过设置用户登录配置，从登录有效期、登录时间、多因子认证、登录IP限制、登录MAC限制等维度，赋予用户登录系统的权限。
资源访问权限	按照用户、用户组与资源账户、账户组之间的关联关系，建立用户对资源的控制权限。 ● 访问控制 通过设置访问控制权限，从访问有效期、登录时间、IP限制、上传/下载、文件传输、剪切板、显示水印等维度，赋予用户访问资源的权限。 ● 双人授权 通过设置双人或多人授权审核，需要授权人实时授权才能访问资源，保障敏感核心资源安全。 ● 命令拦截 通过设置命令控制策略或数据库控制策略，对服务器或数据库中敏感、高危操作，强制阻断、告警及二次复核，加强对关键操作的管控。 ● 批量授权 通过用户组和账户组形式，支持同时授权多个用户对多个资源的控制权限。

操作审计

基于用户身份系统唯一标识，从用户登录系统开始，全程记录用户在系统的操作行为，监控和审计用户对目标资源的所有操作，实现对安全事件的实时发现与预警。

表 1-3 操作审计功能说明

功能特性	功能详情
系统行为审计	系统操作行为全纪录，针对操作失误、恶意操作、越权操作等行为告警通知。 ● 系统登录日志 详细记录登录系统的方式、登录用户、用户来源IP、登录时间等信息。支持一键导出全部系统登录日志。 ● 系统操作日志 系统操作行为全程记录，覆盖所有系统操作事件。支持一键导出全部系统操作日志。 ● 系统报表 集中可视化呈现用户在系统的操作统计信息，包括用户启用状态、用户与资源创建、用户登录方式、异常登录、会话控制等信息。 支持一键导出系统报表，并可定周期以邮件方式自动推送系统报表。 ● 告警通知 通过配置系统告警，针对系统操作和系统环境制定不同告警方式和告警级别，以邮件方式和系统消息方式推送告警通知，以便及时发现系统异常和用户异常操作。

功能特性	功能详情
资源运维审计	全程记录用户的运维操作，支持多种运维审计技术和审计形式，可随时审计用户操作行为，识别运维风险，为安全事件追溯和分析提供依据。 ● 运维审计技术 – Linux命令审计 基于字符协议（SSH、TELNET）的命令操作审计，记录命令运维全程，支持解析字符操作命令，还原操作指令，根据输入、输出结果关键字搜索快速定位回放。 – Windows操作审计 基于图形协议（RDP、VNC）终端和应用发布的行为操作审计，远程桌面的操作全纪录，包括键盘操作、功能键操作、鼠标操作、窗口指令、窗口切换、剪切板复制等。 – 数据库命令审计 基于数据库协议（DB2、MySQL、Oracle、SQL Server）的命令操作审计，记录从SSO单点登录数据库到数据库命令操作全程，支持解析数据库操作指令，100%还原操作指令。 – 文件传输审计 基于远程桌面的文件传输操作审计，以及基于文件传输协议（FTP、SFTP、SCP）的传输操作审计，对Web浏览器或客户端文件传输全程审计，记录传输的文件名称和目标路径。 ● 运维审计形式 – 实时监控 实时查看正在进行的运维会话，支持监控和中断实时会话。 – 历史日志 运维操作全程记录，详细记录历史运维会话信息，支持一键导出历史会话日志。 – 会话视频 支持对Linux命令审计、Windows操作审计全程录像记录，回放录像视频。 支持生成视频文件，一键下载会话视频。 – 运维报表 集中可视化呈现运维统计信息，包括运维时间分布、资源访问次数、会话时长、双人授权、命令拦截、字符数命令、传输文件数等信息。 支持一键导出运维报表，并可定周期以邮件方式自动推送系统报表。 – 日志备份 通过配置日志备份，可将历史会话日志远程备份至Syslog服务器、FTP/SFTP服务器、OBS桶，实现系统日志容灾备份。

高效运维

通过多种架构运维、多种运维资源、多种运维工具、多种运维形式的接入，全面提升运维效率。

表 1-4 高效运维功能说明

功能特性	功能说明
Web浏览器运维	HTML5远程登录资源，无需安装客户端，一键登录运维资源，实现操作实时监控、文件上传下载等运维管理。 ● 一站式登录运维 在Windows、Linux、Android、iOS等操作系统上，支持任意主流浏览器无插件化运维，包括Edge、Chrome、Firefox等主流浏览器，让运维人员脱离运维工具和操作系统束缚，随时随地远程运维。 ● 批量登录 支持一键登录多个授权资源，多个资源可同时在一个浏览器页签运维。 ● 协同会话 支持多人参与“协同分享”，邀请其他运维人员或专家进行协同运维，对同一会话进行协同操作或问题定位，提高多人运维效率。 ● 文件传输 基于WSS的文件管理技术，支持文件上传/下载，以及文件在线管理，实现多主机文件共享功能 。 ● 命令群发 针对多个Linux资源，开启群发键。在一个会话窗口执行命令后，其他会话窗口将同步执行相同操作。
第三方客户端运维	在不改变用户使用原来客户端习惯的前提下，支持一键接入多种运维工具，提升运维效率。 ● 多种运维工具 支持接入SecureCRT、Xshell、Xftp、WinSCP、Navicat 、Toad for Oracle等工具。 ● SSH客户端运维 针对字符协议类主机资源，可通过运维客户端登录资源，实现运维平台多种选择。 ● 数据库客户端运维 针对数据库主机资源，通过配置SSO单点登录工具，调用数据库客户端，实现一键登录目标数据库资源，数据库运维操作。 ● 文件传输客户端运维 针对文件传输协议类主机资源，通过调用FTP/SFTP客户端登录资源，实现客户端运维。
自动化运维	线上多步骤复杂操作自动化执行，告别枯燥的重复工作，提高工作效率。 ● 脚本管理 线下脚本上线管理，支持Shell和Python类型脚本的管理。 ● 运维任务 通过配置命令执行、脚本执行、文件传输的运维任务，可定期、批量、自动执行预置的运维任务。

工单申请

系统运维用户在运维过程中，遇到需运维资源而无权限情况，可提交系统工单申请资源控制权限，寻求管理人员授权审批。

- 系统运维人员
  - 通过手动或自动触发工单系统，提交访问授权工单、命令授权工单、数据库授权工单申请权限。
  - 支持提交工单、查询工单、撤销工单、删除工单等功能。
- 系统管理人员
  - 通过自定义审批流程，支持多级审批。
  - 支持批准单个工单、批量批准工单、驳回工单、撤销工单、查询工单、删除工单等功能。

1.5 服务版本差异

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。

实例版本规格

表 1-5 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	• 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	• 50 • 100 • 200 • 500 • 1000 • 2000 • 5000 • 10000

规格配置说明

不同规格云堡垒机配置差异，请参见**表1 不同规格配置说明**。

表 1-6 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
50	50	4核	8GB	100GB	500GB
100	100	4核	8GB	100GB	1000GB
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1 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。

功能详情及版本差异

标准版和**专业版**的基础功能均支持身份认证、权限控制、账户管理、操作审计，主要功能差异为自动化运维、数据库运维审计两个增强功能。

详细版本功能差异，请参见**表2 不同版本功能差异说明**。

表 1-7 功能详情及版本差异

功能模块	功能项	功能描述	标准版	专业版
个人中心	账户基本信息	查看当前登录用户的详细信息，同时支持对姓名、手机、邮箱以及密码的修改操作。	√	√
	手机令牌	提供手机令牌绑定和生成动态密码的指导。	√	√
	SSH公钥管理	查看所有公钥信息，可添加并管理SSH公钥。	√	√
	权限管理	查看当前用户所拥有的权限。	√	√

功能模块	功能项	功能描述	标准版	专业版
	操作日志	当前登录用户的登录、操作以及资源登录的所有操作记录。	√	√
系统基本信息	系统桌面	按照不同维度呈现了堡垒机的运行情况，包括会话、工单、登录情况、运维情况、主机类型、应用类型、系统状态等多维度的数据图表统计。	√	√
	下载中心	提供部分远端登录工具和本地播放工具的下载。	√	√
	消息中心	配置告警后，触发告警后会生成告警信息。	√	√
	系统基本信息	呈现系统的ID、凭证、版本、发行日期等信息，支持凭证、HA Key的更新，服务码的获取。	√	√
认证管理	账户多因子登录认证	登录堡垒机支持账户密码、手机令牌、手机短信、USBKey、动态令牌的方式。 ● 账户密码：申请堡垒机时生成的账户和密码，首次登录堡垒机只能使用该方式登录。 ● 手机令牌：在堡垒机配置手机号码后，在移动端或小程序注册后使用生成的动态密码进行登录。 ● 手机短信：在堡垒机配置手机号码后，登录时可使用随机验证码进行登录。 ● USBKey：需提前获取到正确的USBKey及密令，在堡垒机配置关联账户后可使用该方式登录。 ● 动态令牌：需提前获取到正确的令牌和密钥，在堡垒机配置关联账户后可使用该方式登录。	√	√
	账户远程认证配置	可通过远程认证，将局域的账户与堡垒机进行对接，在堡垒机实现对局域账户的统一管理。 支持AD域、RADIUS、LDAP、Azure AD、SAML远程认证。	√	√
系统账户	用户管理	对登录堡垒机的账户进行管理，包括账户的创建、导入、导出、删除、用户组配置以及对账户登录限制的管理。	√	√
	用户组管理	将用户进行分组管理，通过对用户组授权实现对用户的批量授权，支持新建、删除、修改编辑用户组信息。	√	√

功能模块	功能项	功能描述	标准版	专业版
	角色管理	将用户关联角色，赋予用户对应角色的操作访问权限，包含部门管理员、策略管理员、审计管理员、运维员，但仅admin账户可自定义新增角色和修改角色所属权限。	√	√
	资源账户管理	资源账户在堡垒机实例中用来登录资源进行运维，一个资源可以创建多个资源账户，资源账户的账户和密码须与资源的原账户密码保持一致，否则可能登录资源失败，无法在堡垒机运维。	√	√
	资源账户组管理	将资源账户进行分组管理，通过对账户组授权实现对资源账户的批量授权、批量验证，支持新建、删除、维护账户组资源以及账户组信息管理。	√	√
系统资源	主机资源管理	通过新建、自动发现、导入或克隆实现对主机资源的纳管，纳管后可对主机资源所有信息进行查看，实现对资源的运维。	√	√
	应用资源管理	先创建应用服务器后，再通过文件导入、新建实现对应用资源的纳管，纳管后可对应用资源所有信息进行查看，以实现对资源的运维。	√	√
	云服务资源管理	先创建Kubernetes服务器后，再通过新建实现对容器节点资源的纳管，纳管后可对容器资源所有信息进行查看，以实现对资源的运维。	×	√
	资源系统类型管理	系统类型可通过标签形式区分被纳管的资源，实现对资源的管理，同时可用于服务器改密，存放改密参数，执行改密策略时，会以系统类型执行脚本。	√	√
系统策略	访问控制策略	用于控制用户或用户组访问资源的权限，将用户或用户组与策略绑定，用户或用户组就受限于策略的约束限制，包括传输、文件管理、登录时间段限制等，同时也可绑定资源账户。	√	√
	命令控制策略	• 用于控制用户或用户组执行命令或命令集的机制，将指定命令或命令集按照预设的执行机制绑定用户或用户组，用户在执行策略内的命令时将直接触发绑定的策略机制，同时也可绑定资源账户。 • 支持自定义命令集。	√	√

功能模块	功能项	功能描述	标准版	专业版
	数据库控制策略	● 用于控制用户或用户组执行规则或规则集的机制，将指定规则或规则集按照预设的执行机制绑定用户或用户组，用户在执行策略内的规则或规则集时将直接触发绑定的策略机制，同时也可绑定资源账户。 ● 支持自定义规则集。	×	√
	改密策略	用于为服务器资源的改密预设改密机制，通过将资源账户与策略绑定，在执行改密时，将为资源账户绑定的所有资源执行改密策略机制。	√	√
	账户同步策略	用于相对于主机资源账户信息的拉取或推送预设执行机制，通过将资源账户与策略绑定，在执行资源账户同步时，将为资源账户绑定的所有资源执行策略的机制。	×	√
资源运维	主机资源运维	可通过浏览器、客户端登录主机资源，进行协同分享、文件传输、文件管理和预置命令的运维操作。	√	√
	应用资源维护	仅支持通过浏览器登录应用资源，进行协同分享、文件传输和文件管理的运维操作。	√	√
	云服务资源运维	仅支持通过浏览器登录容器资源，进行协同分享的运维操作。	×	√
	运维脚本管理	在堡垒机导入和编辑需要执行的脚本，完成一些复杂或重复性的任务，提升运维效率。	×	√
	快速运维	在堡垒机直接执行预设的命令、脚本以及文件传输、执行日志操作可实现对资源快速运维。	×	√
	运维任务管理	可按照手动、定时、定期的执行方式自定义命令、脚本、文件传输的运维任务，同时可对所有操作进行记录。	×	√
系统审计	实时会话审计	针对当前正在运行中的所有会话进行记录，可查看目标会话所对应的资源、类型、账户、来源IP等信息。	√	√
	历史会话审计	针对已关闭的所有历史会话进行记录，可查看目标会话所对应的资源、类型、账户、来源IP等信息。	√	√
	系统日志审计	对堡垒机系统的登录和操作进行详细记录，包括时间、账户、来源IP、涉及模块及操作详情。	√	√

功能模块	功能项	功能描述	标准版	专业版
	运维报表审计	对运维操作的时间、资源访问次数、会话时长、来源IP访问情况、会话协同、双人授权、命令拦截、字符命令数、传输文件数按照时间、用户、资源的维度进行全量统计。	√	√
	系统报表审计	对用户的系统操作控制、资源操作、源IP、登录方式、异常登录、会话、状态维度分别进行数据统计。	√	√
系统工单	访问授权工单管理	无权限访问目标资源时，可通过工单申请绑定资源账户在固定运维时间周期内对目标资源进行文件传输、管理、键盘审计等操作权限。	√	√
	命令控制工单管理	无权限执行命令运维资源时，可通过工单申请绑定资源账户在固定运维时间周期内执行预设的命令。	√	√
	数据库授权工单管理	无权限执行数据库资源操作时，可通过工单申请绑定资源账户在固定运维时间周期内对目标数据库执行预设的指定命令。	×	√
	工单审批管理	呈现所有发起的工单信息，并在该页面执行工单的审批操作。	√	√
	工单配置	可对工单的申请范围、提交方式、生效时间以及审批流程进行自定义设置。	√	√
系统配置	安全配置	对密码错误次数、僵尸用户、密码修改周期、登录超时、证书、代理安全层、手机令牌信息、USBKey信息、巡检、到期提醒、会话限制等进行配置。	√	√
	网络配置	可查看堡垒机的网络接口列表、DNS以及默认网关详情，可对静态路由进行配置操作。	√	√
	HA配置	如果堡垒机为主备实例，可通过HA设置启用或禁用的状态。	√	√
	端口配置	呈现运维和控制台的端口默认信息，如有自定义需求可进行修改，通常不建议修改。	√	√
	外发配置	可配置不同的外发方式，包括邮件、短信和LTS方式，邮件和短信配置后可推送告警信息，LTS在安装Agent后可将堡垒机日志发送至服务器。	√	√
	告警配置	支持对不同维度的消息类型的告警方式、告警等级的配置，包括登录情况、用户的操作、资源操作事件、运维操作等。	√	√
	系统风格管理	支持对堡垒机默认的图标和logo进行自定义修改。	√	√

功能模块	功能项	功能描述	标准版	专业版
堡垒机维护	数据存储维护	可查看系统和数据磁盘的使用情况，可对网盘空间进行修改，可自定义日志的保存周期，进行自动或手动删除。	√	√
	日志备份维护	可自定义配置将日志备份至本地、syslog服务器、FTP/SFTP服务器或OBS服务器。	√	√
	系统维护	可查看系统当前的运行状态，对系统地址、时间等信息进行自定义设置，可操作系统备份及还原，查看授权许可信息，以及网络和系统的诊断操作。	√	√

1.6 CBH 实例权限管理

如果您需要对云上创建的云堡垒机（Cloud Bastion Host，CBH）实例资源进行管理，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全地控制云资源的访问。

通过IAM，您可以在账号中给员工创建IAM用户，并使用策略来控制对资源的访问范围。例如您的员工中有负责软件开发的人员，您希望员工拥有云堡垒机（Cloud Bastion Host，CBH）实例的使用权限，但是不希望员工拥有创建、变更规格、升级CBH实例等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用CBH实例，但是不允许创建、变更规格、升级CBH实例的权限策略，控制员工对CBH实例资源的使用范围。

如果账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用CBH的其它功能。

IAM是提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。关于IAM的详细介绍，请参见《IAM产品介绍》。

CBH 实例权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

CBH实例部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问CBH实例时，需要先切换至授权区域。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。

- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对CBH实例，管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。

如表1-8所示，包括了CBH实例的部分系统权限。

表 1-8 CBH 实例系统权限

系统角色/策略名称	描述	类别
CBH FullAccess	云堡垒机实例的所有权限（支付权限除外）。	系统策略
CBH ReadOnlyAccess	云堡垒机实例只读权限，拥有该权限的用户仅能查看云堡垒机服务，不具备服务配置和操作权限。	系统策略

说明

您在赋予账号企业项目级的CBH FullAccess权限时，还需要授予账号IAM项目级别的CBH ReadOnlyAccess权限，这样才可以在Console控制台正常使用CBH服务的各项功能。

如表1-9列出了CBH实例常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 1-9 常用操作与系统权限的关系

操作	CBH FullAccess	CBH ReadOnlyAccess
创建云堡垒机	√	x
变更云堡垒机规格（变更规格）	√	x
查询云堡垒机列表	√	√
升级云堡垒机软件版本	√	x
查询ECS配额	√	x
绑定或解绑EIP	√	x
重启云堡垒机	√	x
启动云堡垒机	√	x
关闭云堡垒机	√	x

CBH 控制台功能依赖的角色或策略

表 1-10 CBH 控制台依赖服务的角色或策略

控制台功能	依赖服务
创建堡垒机	弹性云服务器 ECS 虚拟私有云 VPC
绑定/解绑EIP	弹性公网IP EIP
云资产委托	密码安全中心 DEW 弹性云服务器 ECS 云数据库 RDS 统一身份认证服务 IAM

CBH FullAccess 策略内容

```
{
   "Version": "1.1",
   "Statement": [
      {
                "Effect": "Allow",
                "Action": [
                    "cbh:*:*",
                    "vpc:subnets:get",
                    "vpc:publicIps:list",
                    "vpc:vpcs:list",
                    "vpc:securityGroups:get",
                    "vpc:firewallGroups:get",
                    "vpc:firewallPolicies:get",
                    "vpc:firewallRules:get",
                    "vpc:ports:get",
                    "vpc:publicips:update",
                    "vpc:securityGroups:create",
                    "vpc:firewallRules:create",
                    "vpc:firewallPolicies:addRule"
                    "ecs:cloudServerFlavors:get",
                    "evs:types:get"
         ]
      }
   ]
}
```

CBH ReadOnlyAccess 策略内容

```
{
   "Version": "1.1",
   "Statement": [
      {
                "Effect": "Allow",
                "Action": [
                    "cbh:*:list*",
                    "vpc:publicIps:list",
                    "vpc:vpcs:list",
                    "vpc:securityGroups:get",
                    "vpc:subnets:get"
         ]
      }
   ]
}
```

1.7 约束与限制

为提高云堡垒机安全管理系统的稳定性和安全性，在CBH实例和系统的使用上有固定一些限制。

网络访问限制

- 不支持跨区域（Region）直接使用。

  云堡垒机实例与系统资源（系统内管理的弹性云服务器、云数据库等）必须在同一区域内。

  虽跨区域跨VPC可通过云连接（Cloud Connect，CC）、虚拟专用网络（Virtual Private Network，VPN）等构建跨区域网络，但受限于网络的不稳定性，不建议跨区域使用云堡垒机纳管资源。

- 不支持跨VPC直接使用。

  云堡垒机实例与系统资源必须在同一个VPC的子网内，才能直接连接访问。

  跨VPC情况下，可通过对等连接打通两个VPC之间网络。

- 云堡垒机实例与系统资源的安全组，必须允许相互访问。

  系统资源必须处于实例所属安全组允许访问的范围内，且资源所属安全组必须允许实例私有IP访问。

  如果实例与系统资源处于不同的安全组，系统默认不能访问。需要在实例的安全组添加“入”的访问规则。

  实例的安全组默认端口有443和2222，默认支持Web浏览器和SSH客户端访问。若需其他访问方式，需用户手动添加目标端口。

- 只允许通过IP地址和端口访问CBH系统。

表 1-11 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

场景描述	方向	协议/应用	端口
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
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
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

支持管理的资源

- **支持的主机类型**

  支持SSH、RDP、VNC、TELNET、FTP、SFTP、SCP、Rlogin协议类型的Windows或Linux主机。
- **支持的数据库类别**
  - 关系型数据库（Relational Database Service，RDS）。
  - 弹性云服务器（Elastic Cloud Server ， ECS）的自建数据库。
- **支持的数据库类型及版本**

表 1-12 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）

- **支持应用管理的服务器类型及版本**

  仅支持对Windows服务器和Linux上的应用进行管理 ，且支持的服务器系统版本如**表1-13**。

表 1-13 支持的应用服务器类型及版本

系统类型	系统版本
Windows	Windows Server 2008 R2及以上版本
Linux	CentOS7.9

说明

目前仅x86版本云堡垒机支持应用运维，Arm版本云堡垒机不支持应用运维。

支持使用的第三方客户端

云堡垒机需通过第三方客户端登录CBH系统，以及调用第三方客户端，实现安全运维管理。

表 1-14 登录 CBH 支持的客户端及版本

登录方式	支持使用的客户端	版本
Web浏览器登录	Edge	44及以上版本 **说明** Edge浏览器上传大文件限制：文件上传到主机，支持单个文件最大4G。
	Chrome	52.0及以上版本
	Safari	10及以上版本
	Firefox	50.0及以上版本
SSH客户端登录	SecureCRT	8.0及以上版本
	Xshell	5及以上版本
	Mac Terminal	2.0及以上版本

表 1-15 运维过程支持调用的客户端

运维方式	资源协议类型/应用类型	支持调用的客户端
数据库运维（主机运维方式）	参见表1-12	
文件传输运维	SFTP	Xftp、WinSCP、FlashFXP
	FTP	Xftp、WinSCP、FlashFXP、FileZilla
应用发布运维	MySQL Tool	MySQL Administrator
	Oracle Tool	PL/SQL Developer
	SQL Server Tool	SSMS
	dbisql	dbisql
	Chrome	Chrome
	Edge	Edge
	Firefox	Firefox
	VNC Client	VNC Viewer
	SecBrowser	SecBrowser
	VSphere Client	VSphere Client
	Radmin	Radmin

其他约束与限制

- 云堡垒机能纳管资源的最大数量不能超过实例规格的总资产数。
- 云堡垒机能同时登录运维资源的最大数量不能超过实例规格的总并发数。

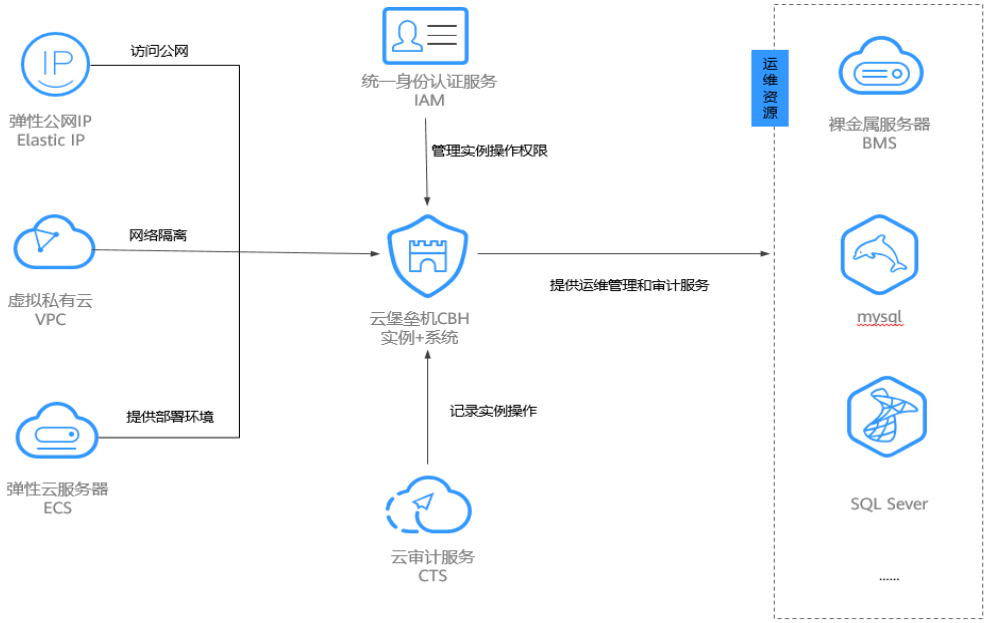
说明

资产数是云堡垒机管理的云服务器上运行的资源数，同一个云服务器上对应有多个需要运维的协议、应用等资源。并发数是云堡垒机同一时刻连接运维协议的连接数。详细说明请参见**基本概念**。

1.8 与其他云服务的关系

云堡垒机需要与其他云服务协同工作，与其他云服务的依赖关系如**图1-1**。

图 1-1 与其他云服务之间关系



与虚拟私有云的关系

虚拟私有云（Virtual Private Cloud，VPC）为CBH提供虚拟网络环境，用户通过配置安全组、子网、EIP等子服务，方便地管理、配置内部网络。以及通过自定义安全组内访问规则，加强安全保护。

与弹性云服务器的关系

弹性云服务器（Elastic Cloud Server，ECS）为CBH提供部署环境，同时CBH为ECS上资源提供安全管理服务。

- ECS为CBH系统后台提供部署环境，后台采用欧拉操作系统。
- 用户通过CBH登录ECS上资源，为弹性云上面的服务器、数据库等资源，提供资产管理、登录身份管理、运维会话审计等功能，加强主机资源运维安全。

与弹性公网 IP 的关系

弹性公网IP（Elastic IP，EIP）为CBH提供独立的公网IP资源，包括公网IP地址与公网出口带宽服务。一个弹性公网IP只能绑定一个云资源使用。EIP与CBH灵活绑定连接Internet，并支持灵活调整带宽，应对访问流量业务的变化。

与云审计服务的关系

云审计服务（Cloud Trace Service，CTS）为CBH实例提供云服务资源的操作记录，记录内容包括访问管理控制台发起的云服务资源操作请求以及每次请求的结果，供您查询、审计和回溯使用。

CTS记录CBH实例相关操作事件，方便用户日后的查询、审计和回溯，更多说明请参见云审计支持的CBH操作。

与统一身份认证服务的关系

统一身份认证服务（Identity and Access Management，IAM）为CBH实例提供用户身份鉴权、IAM用户权限设置等权限管理服务，更多详细说明请参见CBH权限管理。

1.9 基本概念

云堡垒机实例

一个云堡垒机实例对应一个独立运行的云堡垒机系统，用户登录云堡垒机控制台管理实例。只有创建了云堡垒机实例后，才能登录云堡垒机系统，实现安全运维管理与审计。

单点登录

单点登录（Single Sign On，SSO）是指在多个独立应用系统环境下，各个应用系统相互信任，在一个应用系统中将用户认证信息映射到其他系统中，多个系统共享用户认证数据。简言之，即用户通过登录一个应用系统，就可以访问其他所有相互信任的应用系统，实现用户单点多系统登录。

资产数

资产数是指云堡垒机管理的云服务器上运行的资源数，同一台云服务器上对应有多个需要运维的协议、应用等资源。

例如，目前有一台云服务器，在云堡垒机中添加这台云服务器的资源，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，则当前管理的资产数即为5，而不是1。

并发数

并发数是指云堡垒机上同一时刻连接的运维协议连接数。

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。

OTP

OTP（One-Time Password）是一种独特的密码，仅对单次登录会话或交易有效。

在堡垒机中使用手机短信、手机令牌、动态令牌方式登录堡垒机时需要使用到验证口令（OTP）。

1.10 个人数据保护机制

云堡垒机实例不直接采集用户个人数据。实例创建成功后，登录云堡垒机系统需创建用户账号，创建登录系统用户账号涉及个人数据采集。

为了确保您的个人数据（例如云堡垒机系统登录名、密码、手机号码等）不被未经过认证、授权的实体或者个人获取，云堡垒机通过加密存储个人数据、控制个人数据访问权限以及记录操作日志等方法防止个人数据泄露，保证您的个人数据安全。

收集范围

云堡垒机收集及产生的个人数据如**表1-16**所示：

表 1-16 个人数据范围列表

服务	类型	收集方式	是否可修改	是否必须
云堡垒机实例	登录名	在创建用户账号时由系统管理员配置登录名	否	是 登录名是用户的身份标识信息
	密码	• 在管理员创建用户、重置用户密码时配置密码 • 在用户登录系统前重置密码、登录系统后修改密码时输入密码	是	是 用户登录云堡垒机系统时使用
	邮箱	• 在管理员创建用户时配置邮箱 • 在用户登录系统后修改邮箱时输入邮箱	是	是 接收系统邮件通知
	手机	• 在管理员创建用户时配置手机号 • 在用户登录系统后修改手机号时输入手机号	是	是 • 接收系统手机短信通知 • 在忘记密码时通过手机验证码重置密码

存储方式

云堡垒机通过加密算法对用户个人敏感数据加密后进行存储。

- 登录名：不属于敏感数据，明文存储
- 密码、邮箱、手机：加密存储

访问权限控制

云堡垒机系统用户个人数据通过加密存储，系统管理员及上级管理员需通过安全码才能查看用户的手机、邮箱。但用户密码对所有人（包括本人）都不明文可见。

二次认证

云堡垒机系统用户账号配置用户登录限制“多因子认证”后，用户在登录系统时开启登录验证功能，需要二次认证（二次认证方式支持“手机短信”、“手机令牌”、“USBKey”、“动态令牌”），有效保护用户敏感信息。

日志记录

云堡垒机系统用户个人数据的所有操作，包括增加、修改、查询和删除，云堡垒机系统都会记录审计日志，并可备份到远程服务器或本地电脑。拥有审计权限用户可以查看并管理下级管理部门用户账号的日志，系统管理员**admin**拥有系统最高权限，可查看并管理登录系统全部用户账号操作记录。

1.11 安全声明

在操作CBH前请仔细阅读，避免出现网络安全事件。

账户管理

云堡垒机系统的系统管理员默认账号为**admin**，登录密码为申请实例时自定义设置的密码。

在首次登录云堡垒机系统后，请按照系统提示修改密码，否则无法进入系统运行页面。

密码管理

为充分保证安全，建议您设置的各类密码满足以下要求：

- 在首次登录云堡垒机系统后，请按照系统提示修改密码和配置手机号码，否则无法进入云堡垒机系统。
- 密码必须满足密码安全策略：
  - 长度范围：8~32个字符，不能低于8个字符，且不能超过32 个字符。
  - 规则要求：可设置英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符，且需同时包含其中三种。
  - 不能设置为用户名或倒序的用户名。
- 建议定期修改密码，以提高登录账户的安全性。

特性声明

- 您创建的产品、服务或特性等应受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创建或使用范围之内。

- 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。
- 云堡垒机支持HTTPS访问协议，不支持HTTP访问协议。
- 请在法律法规允许的目的和范围内使用。

第三方软件

云堡垒机使用了以下第三方软件：

- 第三方浏览器

  云堡垒机系统Web浏览器登录方式，建议使用浏览器和版本请参见**表1-17**。

  表 1-17 建议使用浏览器及版本

浏览器	版本	说明
Edge	44及以上版本	上传大文件限制：H5运维界面，文件上传到主机，支持单个文件最大4G。
Chrome	52.0及以上版本	-
Safari	10及以上版本	-
Firefox	50.0及以上版本	-

- Nmap工具

  保留原因：Nmap是行业领先的资产扫描工具，CBH服务借用此工具批量发现主机，方便用户批量纳管资产。

  使用场景：CBH的自动发现主机和数据库资源功能通过Nmap工具扫描获取指定网段内的资产，将其添加到堡垒机中进行运维。

  风险：通过该工具，用户可以对指定网段进行资产发现、漏洞扫描操作。相关功能只有管理员角色能够使用，已按照最小权限原则安装使用，整体风险较小。

第三方软件下载方式推荐：

CBH使用中需要用到的部分第三方软件，请按如下方式下载。

- 管理员用户账号成功登录云堡垒机系统后，单击桌面右上角“下载中心”， 单击相应软件下载。
- 运维用户账号成功登录云堡垒机系统后，单击桌面右上角“下载中心”， 单击相应软件下载。

2 创建云堡垒机

背景信息

一个云堡垒机实例对应一个独立运行的云堡垒机运维管理系统环境。首先用户需创建云堡垒机实例，获得一个云堡垒机账户，再登录云堡垒机系统并配置运维管理环境，才能实现云堡垒机实时远程高效运维管理。

操作场景

购买堡垒机时，根据堡垒机“单机”和“主备”实例类型的不同，可用区选择也有所区别。

- 单机：创建后只创建一台堡垒机，可以选择任意可用区。
- 主备：创建后会创建两台堡垒机，需要分别选择主可用区和备可用区，可根据容灾或网络时延需求进行选择。
  - 场景一：如果有容灾能力的需求，建议主实例和备实例部署在不同的可用区。

    示例：“主可用区”选择“可用区1”，“备可用区”选择“可用区2”。

    图 2-1 满足容灾能力的可用区选择

  - 场景二：如果对网络时延有较高要求，建议主实例和备实例部署在同一可用区，此时网络时延较小。

    示例：“主可用区”和“备可用区”都选择“可用区1”。

图 2-2 满足网络低时延的可用区选择

前提条件

- 已获取待纳管资源信息，且待纳管资源在CBH支持使用的区域内。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击 ☰，在服务列表选择“安全 > 云堡垒机”。

步骤3 单击“创建云堡垒机”，进入云堡垒机的申请页面。

步骤4 选择“云堡垒机实例”服务类型，根据设置实例的相关参数，相关说明请参考表2-1。

表 2-1 云堡垒机实例参数说明

参数	说明
计费模式	选择实例计费模式，仅支持“按需”模式。 按需计费：以小时计费。 **说明** 按需计费开启后，只有删除目标实例才会停止计费，与实例运行状态无关。
当前区域	选择堡垒机的区域，请就近选择靠近您业务的区域，可减少网络时延，提高访问速度。
实例类型	根据您的自身业务需求选择单机或者主备实例类型。 • 单机：购买后只有一台堡垒机。 • 主备：购买后会下发两台堡垒机，组成双机设备，主设备不可正常使用时可继续使用备用堡垒机。 **说明** 如您购买的是主备实例，切勿禁用HA，否则会导致对应堡垒机无法登录。
可用区	可用区是创建的堡垒机部署的位置。
实例名称	自定义实例名称。

参数	说明
性能规格	选择实例版本规格。 云堡垒机提供“标准版”和“专业版”两个功能版本，配备50/100/200/500/1000/2000/5000资产规格。 资产量表示当前创建的云堡垒机支持的最大可纳管的资源数和最大并发数，同时不同资产量对应的处理器、数据盘、系统盘大小都将会不同。 示例：选择100资产量表示可纳管资源数和最大并发数都为100个。 **说明** 当前主备实例暂不支持通过弹性公网EIP纳管公网资源。
虚拟私有云	选择当前区域下虚拟私有云（Virtual Private Cloud，VPC）网络。 若当前区域无可选VPC，可单击“查看虚拟私有云”创建新的VPC。 **说明** • 默认情况下，不同区域的VPC之间内网不互通，同区域的不同VPC内网不互通，同一个VPC下的不同可用区之间内网互通。 • 云堡垒机支持直接管理同一区域同一VPC网络下ECS等资源，同一区域同一VPC网络下ECS等资源可以直接访问。若需管理同一区域不同VPC网络下ECS等资源，要通过对接连接、VPN或其他方式打通两个VPC间的网络；不建议跨区域管理ECS等资源。
子网	选择当前VPC内子网。 **说明** 子网选择必须在VPC的网段内。
分配IPv4地址	选择“自动分配IP地址”或者“手动分配IP地址”。 选择“手动分配IP地址”后，可查看已使用的IP地址。
安全组	选择当前区域下安全组，系统默认安全组**Sys-default**。 若无合适安全组可选择，可单击“新建安全组”创建或配置新的安全组。 **说明** • 一个安全组为同一个VPC网络内具有相同安全保护需求，并相互信任的CBH与资源提供访问策略。当云堡垒机加入安全组后，即受到该安全组中访问规则的保护。 • 云堡垒机可与资源主机ECS等共用安全组，各自调用安全组规则互不影响。 • 如需修改安全组，请参见**更改安全组**章节。 • 在创建HA实例前，需要安全组在入方向中放通22、31036、31679、31873这四个端口。 • 堡垒机创建时会自动开放80、8080、443、2222共四个端口，创建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。

参数	说明
弹性IP	（可选参数）选择当前区域下EIP。 若当前区域无可选EIP，可单击“创建弹性IP”。 **说明** • 若创建时选择了弹性IP之后，在实例状态变为运行后，EIP未绑定成功，可能是创建过程中此EIP已经绑定其他服务器，需要参考**绑定弹性公网IP**章节重新绑定弹性公网IP。 • 一个弹性公网IP只能绑定一个云资源使用，云堡垒机绑定的弹性IP不能与其他云资源共用。实例创建成功后，弹性IP作为云堡垒机系统登录IP使用。所以为了正常使用云堡垒机，用户账号至少需要创建一个弹性IP。此处若未绑定EIP，后期可参考**绑定弹性公网IP**章节绑定弹性公网IP。 • 为满足CBH系统使用需求，建议配置EIP带宽为5M以上。 • 实例创建成功后，可根据需要“解绑弹性公网IP”和“绑定弹性公网IP”操作，更换云堡垒机系统登录EIP地址。
企业项目	选择此次创建的堡垒机所属的企业项目。 默认选择为“default”。
用户名	默认用户名“admin”。 系统管理员账号**admin**拥有系统最高操作权限，请妥善保管账号信息。
登录密码	自定义**admin**用户密码信息。 **说明** • 密码设置要求 – 长度范围：8~32个字符，不能低于8个字符，且不能超过32 个字符。 – 规则要求：可设置英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（!@$%^-_=+[{}]:,./?~#*），且需同时至少包含其中三种。 – 不能包含用户名或倒序的用户名。 – 不能包含超过2个连续的相同字符。 • 需设置和确认输入两次密码信息，两次输入信息需一致才能成功设置密码。 • 云堡垒机系统无法获取系统管理员**admin**用户密码，请务必保存好登录账号信息。 • 系统管理员**admin**在首次登录云堡垒机系统时，请按照系统提示修改密码和配置手机号码，否则无法进入云堡垒机系统。 • 完成实例创建后，若忘记**admin**用户密码，可参考**重置密码**解决。
标签	标签：如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下选择同一标签，建议在TMS中创建预定义标签。 如您的组织已经设定云堡垒机的相关标签策略，则需按照标签策略规则为云堡垒机实例添加标签。标签如果不符合标签策略的规则，则可能会导致云堡垒机创建失败，请联系组织管理员了解标签策略详情。

步骤5 配置完成后，确认当前配置信息无误后，单击“立即创建”。

说明

当收到网络限制提示时，请先“一键放通”网络限制，确保创建实例后授权下发成功。

您可以在安全组和防火墙ACL中查看相应规则。

- 云堡垒机所在安全组允许访问出方向9443端口。
- 云堡垒机所在子网未关联防火墙ACL，或关联的防火墙ACL为“开启”状态且允许访问出方向9443端口。

步骤6 在订单详情页面，确认订单信息无误后，单击“提交订单”。

步骤7 返回云堡垒机控制台页面，在“云堡垒机实例”列表下查看新创建的实例。

创建实例成功后，后台自动创建CBH系统，大约需要10分钟。

说明

后台创建CBH系统完成前，即实例的“状态”未变为“运行”前，请勿解绑EIP，否则可能导致CBH系统创建失败。

----结束

后续操作

- 当实例的“运行状态”为“运行”时，说明CBH系统创建成功，此时您才能登录CBH系统。
- 当实例的“运行状态”为“创建失败”时，在弹出的“创建失败实例”对话框中查看失败原因。
- 实例发放完成后，建议您及时配置、更换堡垒机实例的证书。

3 云资产委托授权

云堡垒机已统一对接云凭据管理服务 CSMS、密钥管理 KMS、弹性云服务器 ECS、关系型数据库 RDS，方便您在堡垒机上使用纳管的凭据。

使用说明

- 开启各资产模块的授权后，CBH将获取的各服务的权限如下：
  - CSMS：CBH将有权限查询您的CSMS凭据列表，您可以在CBH实例上选择凭据作为资源账户。

    须知

    通过堡垒机调用的凭据，账户及密码命名需要在“键”中规范，否则无法获取到正确的账号密码。

    例如：

    username:root

    password:*****
  - KMS：CBH将有权限使用KMS接口获取CSMS凭据值，您可以在CBH实例上使用该凭据值登录纳管的主机。
  - ECS：CBH将有权限查询您的ECS实例列表，您可以在CBH实例上一键同步您的ECS实例至云堡垒机的主机列表中。
  - RDS：CBH将有权限查询您的RDS实例列表，您可以在CBH实例上一键同步您的RDS实例至云堡垒机的主机列表中。
- 开启CSMS凭据、KMS密钥、ECS、RDS委托授权后，需要等待10分钟左右，云堡垒机才可以获取有委托权限的Token。

操作步骤

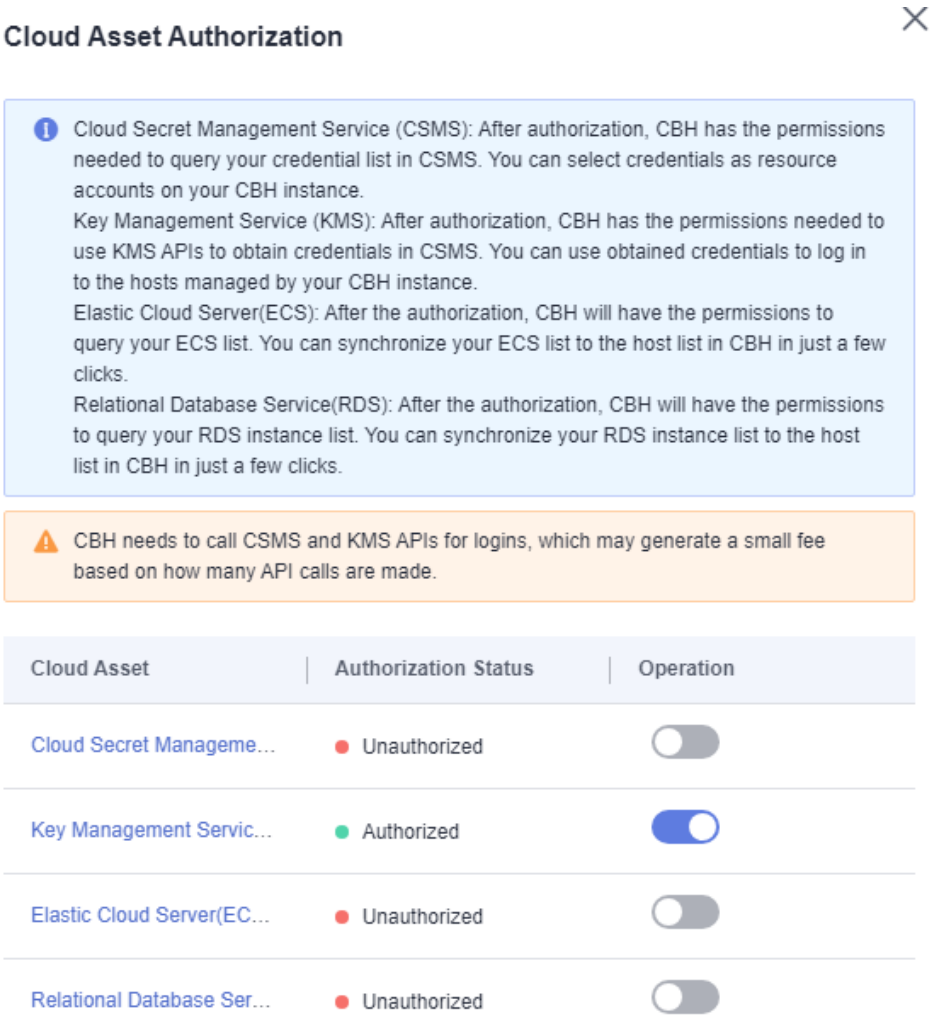
步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击 ☰，在服务列表选择“安全 > 云堡垒机”。

步骤3 单击右上角的“云资产委托授权”。

步骤4 在弹出的对话框中，切换“操作”列的开关至  ，打开资产模块的授权。

图 3-1 云资产委托授权



步骤5 后续添加资源账户请参照**创建资源账户并绑定资源**章节。

----结束

4 实例管理

4.1 查看实例详情

一个云堡垒机实例对应一个独立运行的云堡垒机系统。

用户可以在获取有CBH操作权限的账号和密码后，对云堡垒机实例进行管理操作。

查看实例信息

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击 ☰，在服务列表选择“安全 > 云堡垒机”。

步骤3 单击实例名称，进入实例详情页面，查看实例详情信息，包含实例信息、服务器信息、交易信息和标签信息。

表 4-1 实例的信息参数说明

参数	说明
实例名称	当前实例自定义的名称，创建后不可编辑修改。
服务器ID	当前实例的服务器ID，包含备机的ID。
实例类型	当前实例的类型。
备机状态	当前实例的备机运行状态。 **说明** 仅“实例类型”为“主备”才可查看此项。
实例规格	当前实例的资产规格，支持变更。 **说明** • 变更规格操作是高危操作，受已运行业务的影响，存在失败的风险，不建议直接进行规格变更。 • 变更规格失败，可能影响堡垒机的使用，请您务必备份数据。
实例版本	当前实例的版本。

参数	说明
企业项目	当前实例绑定的企业项目名称。
计费模式	当前实例的计费模式。
创建时间	当前实例的创建时间。
虚拟私有云	当前实例绑定的VPC网络环境，可执行切换VPC。 **说明** • 切换虚拟私有云会导致云服务器网络中断，同时更改云服务器子网、IP地址、MAC地址，如有业务正在运行，务必谨慎操作。 • 切换虚拟私有云过程中，请勿操作云服务器的弹性公网IP，或对云服务器做其它操作。
子网	当期实例配置的VPC网络环境的子网。
Vip	当前实例的浮动IP。
私有IP	当前实例的私有IP地址，包括备机的IP地址。
安全组	用户配置的虚拟网络环境安全规则。

步骤4 在“标签”区域，可以查看和编辑该实例的标签信息。

----结束

4.2 重置 admin 登录方式

当您因多因子认证登录手段的缺失而导致无法使用admin账号登录至堡垒机，可参考本章节的方法重新设置admin账号的登录方式。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击 ☰，在服务列表选择“安全 > 云堡垒机”。

步骤3 在目标实例所在行，单击“操作”列中的“更多 > 重置 > 重置Admin登录方式”。

步骤4 在弹出的对话框中单击“确定”，完成重置admin用户登录方式。

说明

重置登录方式完成后，admin用户需以用户名和密码的方式登录，如需配置多因子认证方式登录，详细步骤请参见**多因子认证配置**。

----结束

4.3 重置 admin 密码

当忘记admin账号密码时，可参考本章节的方法重新设置admin账号的密码。

其他账号忘记密码时，请参考**如何重置云堡垒机用户登录密码**解决。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击 ☰，在服务列表选择“安全 > 云堡垒机”。

步骤3 在目标实例所在行，单击“操作”列中的“更多 > 重置 > 重置Admin密码”。

步骤4 在弹出的对话框中重新配置admin账号的密码。

步骤5 配置后确认无误，单击“确认”，完成配置。

----结束

4.4 升级实例版本

CBH服务会定期升级云堡垒机实例版本，进行功能优化或新增功能特性，建议您及时升级云堡垒机实例版本。

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，备份说明请参见**云堡垒机支持备份哪些系统数据？**。
  - 预约升级，升级时间需要比当前时间至少晚一天（24h），建议您在无业务使用时升级，预约升级任务后，不能关机，重启，变更，扩容操作，升级任务开始前可以取消，重新设置升级时间。
- 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。
  - 版本升级完成，您可以在堡垒机实例详情页面选择“版本回退”，版本回退开始后堡垒机“运行状态”会变为“版本回滚中”。
- 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。
  - 升级后的扩容操作不可回退，在升级完成后，如您需要进行扩容操作请等待5分钟后再进行，且务必在验证数据无误后再进行扩容或变更操作。
- 版本回退

  版本回退后版本会变为升级前的版本状态，升级后修改或新增的数据会丢失，并且因为数据回滚会导致当前堡垒机业务中断，请您谨慎操作。

约束限制

- 由于新版本的云堡垒机对应用发布功能进行了优化，故版本升级后，需要在应用发布服务器上安装相应的插件，才能正常使用应用运维功能。
- 3.3.40.0和3.3.41.0版本升级时间存在问题，需要先同步OBS桶的时间再进行升级。

- 当前版本升级所有实例暂不支持无损变更，升级期间业务需要暂停使用。

前提条件

已备份系统数据。

升级版本有失败的风险，因此在升级前必须备份数据，以防因升级失败而影响使用。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击 ☰，在服务列表选择“安全 > 云堡垒机”。

步骤3 在需要升级服务版本的实例所在行，单击“操作”列中的“更多 > 预约升级 > 预约升级时间”。

步骤4 在弹出的升级实例对话框中，选择预约升级时间，确定完后在对话框中输入“YES”。

步骤5 后台自动启动升级，版本升级过程约需要15min至2h（实际升级时间视堡垒机升级的类型而定），且实例的运行状态将会变为“升级中”。

步骤6 实例状态变为“运行”，即可正常使用云堡垒机。

升级完成后，可单击实例名称进入详情页查看实例的版本号。

说明

- 若升级完成后，实例版本号未变动则表示升级失败，请联系技术支持人员处理。

----结束

4.5 启动实例

以下场景需要启动实例：

- 当实例关闭后，实例的“运行状态”为“关闭”时，如果需重新登录使用云堡垒机系统，则需执行启动实例操作。
- 当实例异常时，实例的“运行状态”为“异常”时，为重新登录使用云堡垒机系统，可尝试执行启动实例操作。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击 ☰，在服务列表选择“安全 > 云堡垒机”。

步骤3 在需要启动的实例所在行，单击“操作”列中的“启动”。

步骤4 在弹出的启动实例对话框中，单击“确定”。

实例启动成功后，实例的“运行状态”变为“运行”。

----结束

4.6 关闭实例

当实例的“运行状态”为“运行”时，可以关闭实例。关闭实例后，将不能登录云堡垒机系统。

说明

执行关闭前，请确保目标堡垒机实例没有正在进行中的操作或运维任务，执行关闭后，正在执行的操作或运维会立即被强制退出，请谨慎操作。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击 ，在服务列表选择“安全 > 云堡垒机”。

步骤3 在需要关闭的实例所在行，单击“操作”列中的“更多 > 关闭”。

步骤4 在弹出的关闭实例对话框中确认关闭信息，确认无误，单击“确定”。

实例成功关闭后，实例的“运行状态”变为“关闭”。

实例关闭后，堡垒机仍会计费，如后续不再使用该堡垒机实例，建议将该堡垒机执行删除操作。

----结束

4.7 重启实例

出于维护目的，当堡垒机系统运行异常，用户可以尝试重启实例，使其恢复到可用状态。

说明

- 执行重启前，请确保目标堡垒机实例没有正在进行中的操作或运维任务，执行重启后，正在执行的操作或运维会立即被强制退出，请谨慎操作。
- 堡垒机实例的“运行状态”为“运行”时，可执行重启操作。
- 重启云堡垒机实例将导致系统业务中断约5min，在此期间实例“运行状态”将显示为“正在重启”，且重启过程中，堡垒机系统不可用。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击 ，在服务列表选择“安全 > 云堡垒机”。

步骤3 在需要重启的实例所在行，单击“操作”列中的“更多 > 重启”。

步骤4 在弹出的重启实例对话框中，单击“确定”。

说明

在重启实例对话框，可选择“强制重启”，强制重启实例可能会造成数据丢失，请确保数据文件已全部保存，且云堡垒机系统无操作。

步骤5 重启过程一般需要5分钟左右，且实例的运行状态将会变为“正在重启”。

若是升级版本和变更规格后，重启所需时间可能会更久。

说明

若重启过程中出现“堡垒机实例异常，请联系工程师解决”的提示，为正常现象。

步骤6 实例的运行状态变为“运行”，即可正常使用堡垒机。

----结束

4.8 更改 VPC

为方便您的堡垒机和云上其他项目处于同一VPC下，您可以在堡垒机控制台更改VPC。

约束条件

- 控制台中“运行状态”为“运行”的实例才可以更改VPC。
- 在切换VPC前需要确保切换的目标VPC子网下“可用IP数”满足对应数量要求，查看可用IP数可通过虚拟私有云服务控制台选择子网，进入目标子网查看。
  - 单机实例：可用IP数至少有1个。
  - 主备实例：可用IP数至少有3个。
- 堡垒机实例版本在V3.3.52.0及以上版本才支持更换VPC操作。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击 ☰，在服务列表选择“安全 > 云堡垒机”。

步骤3 在需要修改VPC的实例所在行，单击“操作”列中的“更多 > 网络设置 > 切换VPC”。

步骤4 在“虚拟私有云”和“子网”的下拉框中选择目标VPC和子网。

说明

堡垒机实例切换VPC后，旧子网会依旧处于占用状态，需要您手动去子网下删除。

步骤5 单击“确认”。

----结束

4.9 更改安全组

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。但是若您在创建堡垒机的时候选择了不适用的安全组，也无法通过修改相应的安全组规则来放通这些IP地址和端口，这时候您可以通过更改堡垒机绑定的安全组来满足您的运维需求。

约束条件

- 堡垒机最多可以接入5个安全组。
- 控制台中“运行状态”为“运行”的实例才可以更改安全组。
- 堡垒机绑定多个安全组时，安全组的规则生效方式为并集。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击 ☰，在服务列表选择“安全 > 云堡垒机”。

步骤3 在需要修改安全组的实例所在行，单击“操作”列中的“更多 > 网络设置 > 更改安全组”。

步骤4 在弹出的对话框中勾选需要绑定的安全组。

步骤5 单击“确认”，完成安全组的修改。

----结束

4.10 绑定弹性公网 IP

以下操作必须为堡垒机实例绑定弹性公网IP，且为了满足堡垒机的使用需求，建议配置EIP带宽为5M以上。

- 使用Web浏览器登录堡垒机系统。登录地址：https://*堡垒机实例EIP*。例如，https://10.10.10.10。
- 配置了手机短信登录，需要通过手机获取验证码等操作，不配置EIP，会导致不能接收短信。
- 对接LTS外发日志，具体的操作请参见**配置LTS日志外发服务**。
- V3.3.2.0及以下版本，如果堡垒机实例未绑定弹性公网IP，会导致变更版本规格、升级版本、启动/重启实例等操作失败。

约束限制

为云堡垒机绑定弹性公网IP时，必须在云堡垒机控制台进行操作绑定，否则会导致无法使用IAM进行登录。

前提条件

已创建至少一个弹性公网IP（Elastic IP，EIP）。

⚠ 注意

- 一个弹性公网IP只能绑定一个云资源使用，云堡垒机绑定的弹性IP不能与其他云资源共用。
- 该弹性公网IP和要绑定的云堡垒机实例必须是同一个账号同一个区域下创建的。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击 ，在服务列表选择“安全 > 云堡垒机”。

步骤3 在需要绑定弹性IP的实例所在行，单击“操作”列中的“更多 > 网络设置 > 绑定弹性公网IP”。

步骤4 在弹出的绑定弹性IP对话框中，选择已有“未绑定”状态的弹性IP，单击“确定”。

绑定成功后，在实例列表的“弹性IP”列可查看已绑定的弹性IP；操作列的“登录”按钮变为可操作。

----结束

4.11 解绑弹性公网 IP

当堡垒机实例需要重新绑定EIP或释放EIP时，需要为该实例解绑EIP。当实例成功解绑EIP后，则无法再通过该EIP登录云堡垒机系统。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击 ，在服务列表选择“安全 > 云堡垒机”。

步骤3 选择需要解绑弹性IP的实例，单击所在行“操作”列中的“更多 > 网络配置 > 解绑弹性公网IP”。

步骤4 在弹出的解绑弹性IP对话框中，单击“确定”。

解绑成功后，实例列表的“弹性IP”列无IP信息；操作列的“登录”按钮变为不可操作。

----结束

4.12 标签管理

您可通过标签对资源进行批量管理，针对分层管理的资源可采用键和值的模式，普通资源只用键即可满足。

添加标签

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击 ，在服务列表选择“安全 > 云堡垒机”。

步骤3 单击目标实例名称，进入实例详情页面。

步骤4 在“标签”区域单击“添加标签”，在弹窗中填写标签键和值。

说明

- 标签的键不能以_sys_开始，不能以空格开始或结束，只能包含UTF-8格式表示的字母、数字和空格，以及：_.:=+-@符号。
- 标签的值只能包含UTF-8格式表示的字母、数字和空格，以及：_.:=+-@符号。
- 如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下拉选择同一标签，建议在TMS中创建预定义标签。

步骤5 确认无误，单击“确定”，标签添加完成。

----结束

编辑标签

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击 ☰，在服务列表选择“安全 > 云堡垒机”。

步骤3 单击目标实例名称，进入实例详情页面。

步骤4 单击目标标签“操作”列的“编辑”，可对标签的值内容进行编辑。

步骤5 确认无误，单击“确定”，标签修改完成。

----结束

删除标签

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击 ☰，在服务列表选择“安全 > 云堡垒机”。

步骤3 单击目标实例名称，进入实例详情页面。

步骤4 单击目标标签“操作”列的“删除”，可对当前标签进行删除。

步骤5 确认无误，单击“确定”，标签删除完成。

----结束

4.13 资源管理

云堡垒机目前已对接LTS，可在“我的资源”查看CBH的资源情况。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击 ☰，在服务列表选择“安全 > 云堡垒机”。

步骤3 单击右上角的登录账号名称，选择“My Resources”，进入资源总览页面。

步骤4 在“Service”中单击“Cloud Bastion Host”可筛选云堡垒机所有资源进行查看。

步骤5 同时在列表处通过筛选名称、资源ID、企业项目可筛选资源类别。

步骤6 单击列表处的“导出资源列表”可导出资源详情。

----结束

4.14 版本回退

堡垒机支持回退到历史版本。

前提条件

- 回退的堡垒机实例须为由历史版本升级至新版本的实例。
- 回退前请确保没有正在运行的操作。

约束与限制

- 仅处于“运行”状态的堡垒机支持回退。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击 ，在服务列表选择“安全 > 云堡垒机”。

步骤3 在需要回退版本的实例所在行，单击“操作”列中的“更多 > 预约升级 > 版本回退”。

步骤4 将自动启动回退操作，完成后可单击实例名称进入详情页查看实例的当前版本。

----结束

4.15 审计实例关键操作

4.15.1 云审计支持的 CBH 实例操作

云审计服务（Cloud Trace Service，简称CTS），是云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

开启了云审计服务后，系统开始记录云堡垒机实例的相关操作，云审计服务管理控制台将保存最近7天的操作记录。云审计服务支持的CBH实例操作参考**表4-2**。

表 4-2 支持 CBH 实例操作列表

操作名称	资源类型	事件名称
启动堡垒机实例	cbh	StartInstance
关闭堡垒机实例	cbh	StopInstance
重启堡垒机实例	cbh	RebootInstance
升级堡垒机实例	cbh	UpgradeInstance

操作名称	资源类型	事件名称
回退升级的堡垒机实例	cbh	RollbackInstance
重置堡垒机实例admin密码	cbh	ResetInstancePassword
重置堡垒机实例admin登录方式	cbh	ResetInstanceLoginMethod
删除故障云堡垒机实例	cbh	DeleteInstance
变更堡垒机实例	cbh	ResizeInstance
创建堡垒机实例	cbh	CreateInstance
堡垒机实例绑定弹性公网IP	cbh	InstallInstanceEip
堡垒机实例解绑弹性公网IP	cbh	UninstallInstanceEip
修改堡垒机实例安全组	cbh	UpdateInstanceSecurityGroup
切换堡垒机虚拟私有云	cbh	SwitchInstanceVpc

4.15.2 查看云审计日志

开启了云审计服务后，系统开始记录CBH实例的操作。云审计服务管理控制台保存最近7天的操作记录。

操作步骤

步骤1 登录管理控制台。

步骤2 在左侧导航树中，单击 ☰，选择“管理与监管 > 云审计服务”，进入云审计服务信息页面。

步骤3 单击左侧导航树的“事件列表”，进入事件列表信息页面。

步骤4 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询，详细信息如下：

- “事件来源”、“资源类型”和“筛选类型”。
  - 在下拉框中选择查询条件，例如：依次选择“CBH”>“cbh”>“按事件名称”>“createInstance”，单击“查询”，查询所有创建CBH实例的操作。
  - 事件名称：选择具体的事件名称，例如createInstance。
  - 资源ID：选择或者手动输入需要查看审计日志的CBH实例ID。
  - 资源名称：选择或手动输入需要查看审计日志的CBH实例名称。
- “操作用户”：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。

- “事件级别”：可选项为“所有事件级别”、“normal”、“warning”、“incident”，只可选择其中一项。
- “起始时间”、“结束时间”：可通过选择时间段查询操作事件。

步骤5 在需要查看的记录左侧，单击 展开该记录的详细信息。

步骤6 在需要查看的记录右侧，单击“查看事件”，查看该操作事件结构的详细信息。

----结束

5 登录堡垒机实例

5.1 登录实例概述

如果当前浏览器已通过任意方式登录，在登录其他账号时，需要将已登录的账号退出才可正常登录。

开放端口要求

为避免网络故障或网络配置问题影响登录系统，请管理员优先检查网络ACL配置是否允许访问堡垒机，并参考**表5-1**配置实例安全组。

表 5-1 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

场景描述	方向	协议/应用	端口
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
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
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

登录方式

用户账号配置多因子认证后，静态密码登录方式失效。

表 5-2 登录方式说明

登录方式	登录说明
静态密码	输入用户登录名和密码。
手机短信	输入用户登录名和密码，单击“获取验证码”，并输入短信验证码。
手机令牌	输入用户登录名和密码，并输入手机令牌的动态验证码（每隔一段时间就会变化）。

登录方式	登录说明
USBKey	接入并选择已签发的USBKey，并输入对应的PIN码。
动态令牌	输入用户登录名和密码，并输入动态令牌的动态口令（每隔一段时间就会变化）。

认证类型

AD域、RADIUS、LDAP、Azure AD、SAML远程认证使用远程服务上的已有用户密码。

表 5-3 认证类型说明

认证类型	认证说明
本地认证	用户登录密码为系统配置静态密码。 ● 可选择多因子认证方式登录。 ● 可重置用户密码、个人找回密码、个人修改密码。
AD域认证	用户登录密码为AD域用户密码。 ● 可选择多因子认证方式登录。 ● 不能通过系统修改用户密码。
RADIUS认证	用户登录密码为RADIUS服务器用户密码。 ● 可选择多因子认证方式登录。 ● 不能通过系统修改用户密码。
LDAP认证	用户登录密码为LDAP服务器用户密码。 ● 可选择多因子认证方式登录。 ● 不能通过系统修改用户密码。
Azure AD认证	用户登录密码为Microsoft用户账号密码。 需跳转到Microsoft登录页面，输入用户账户信息登录。 ● 不能选择多因子认证方式登录。 ● 不能通过系统修改用户密码。
SAML认证	用户登录密码为SAML服务器用户密码。 ● 可选择多因子认证方式登录。 ● 不能通过系统修改用户密码。

5.2 使用控制台登录堡垒机

如果当前浏览器已通过任意方式登录，在登录其他账号时，需要将已登录的账号退出才可正常登录。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击 ☰，在服务列表选择“安全 > 云堡垒机”。

步骤3 在目标实例“操作”列单击“远程登录”，在弹窗页面选择登录实例的方式。

说明

- 登录的堡垒机如果未绑定弹性公网IP，若使用私网IP登录，需确保当前本地网络环境与堡垒机私网能正常连接，否则会出现登录失败。

步骤4 在堡垒机登录页面，选择验证方式，并按提示输入相应的登录名、静态密码、动态验证码等信息后，单击“登录”。

支持的验证方式及具体操作，请参见**使用Web浏览器登录堡垒机**。

----结束

5.3 使用 Web 浏览器登录堡垒机

堡垒机基于Web浏览器登录系统的方式，可通过各大主流浏览器登录，并可使用系统管理和资源运维功能。建议系统管理员**admin**或管理员使用Web浏览器登录进行系统管理和授权审计。

说明

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

前提条件

已绑定弹性公网IP。

操作步骤

步骤1 启动浏览器，在Web地址栏中输入系统登录地址，进入系统登录页面。

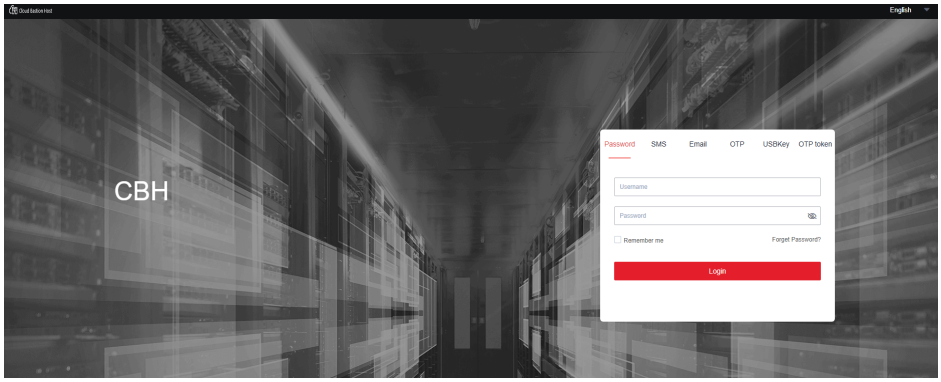
登录地址：https://*堡垒机实例EIP*。例如，https://10.10.10.10。

说明

受浏览器兼容性限制，当浏览器版本与堡垒机系统不匹配时，可能导致登录时获取不到验证信息，或登录后页面显示异常，建议使用推荐的浏览器及版本。

步骤2 在登录页面选择登录方式。

图 5-1 系统登录界面



步骤3 按选择的登录方式，依次填入登录名、静态密码、动态验证码等信息。

- **使用静态密码登录**
- **使用手机短信登录**
- **使用邮箱认证登录**
- **使用手机令牌登录**
- **使用USBKey登录**
- **使用动态令牌登录**
- **Azure AD用户登录**

----结束

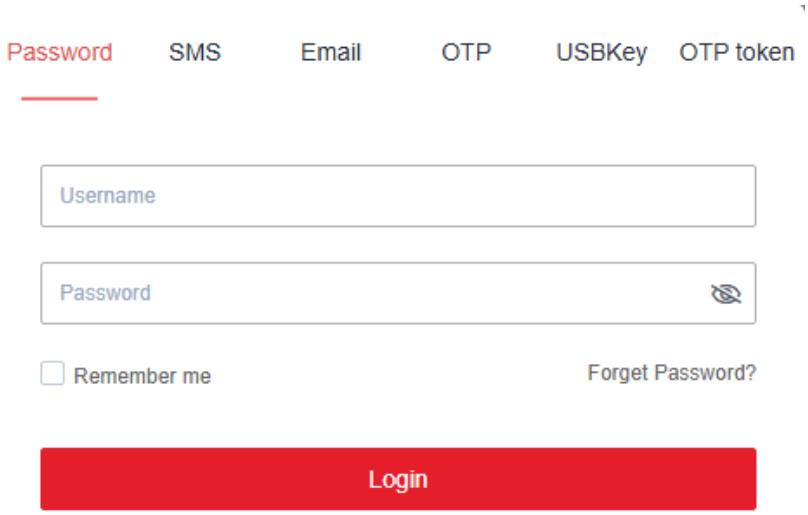
使用静态密码登录

步骤1 选择“密码登录”方式。

步骤2 依次输入用户登录名、账户登录密码。

步骤3 单击“登录”，验证通过后即可登录系统。

图 5-2 静态密码登录



----结束

使用手机短信登录

手机号码需能正常接收短信。

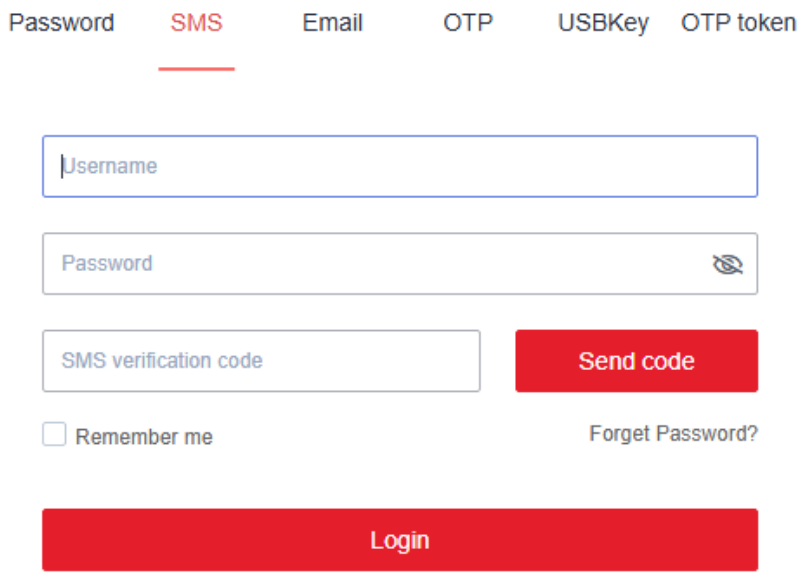
步骤1 选择“手机短信”方式。

步骤2 依次输入用户登录名、账户登录密码。

步骤3 单击“获取验证码”，收到短信消息后，输入6位OTP口令。

步骤4 单击“登录”，验证通过后即可登录系统。

图 5-3 手机短信登录



----结束

使用邮箱认证登录

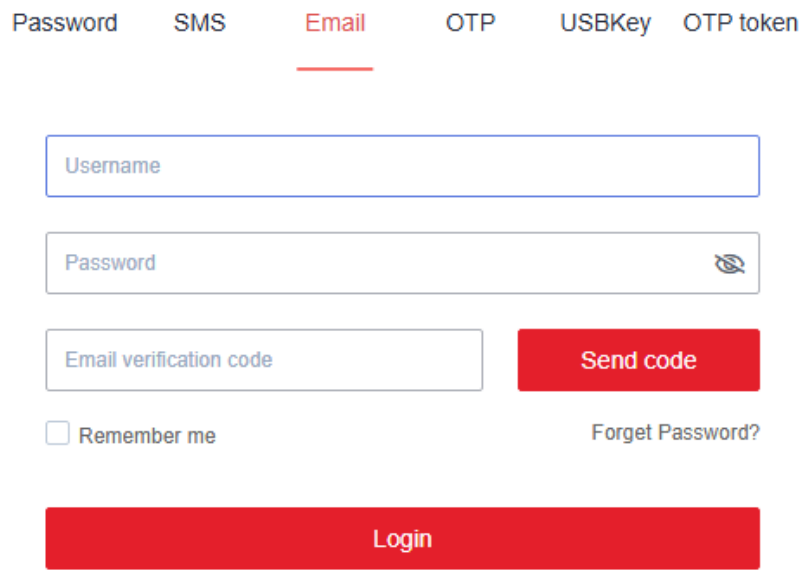
步骤1 选择“邮箱认证”方式。

步骤2 依次输入用户登录名、账户登录密码。

步骤3 获取邮箱验证码，输入验证码。

步骤4 单击“登录”，验证通过后即可登录系统。

图 5-4 邮箱认证登录



----结束

使用手机令牌登录

手机时间必须与堡垒机系统时间一致，精确到秒。

须知

堡垒机的手机令牌小程序是存储在小程序的缓存之中，手机后台可能会误清除小程序缓存，导致用户手机令牌消失。

建议您保存申请手机令牌时的二维码图片，如果出现上述情况再次扫描即可。

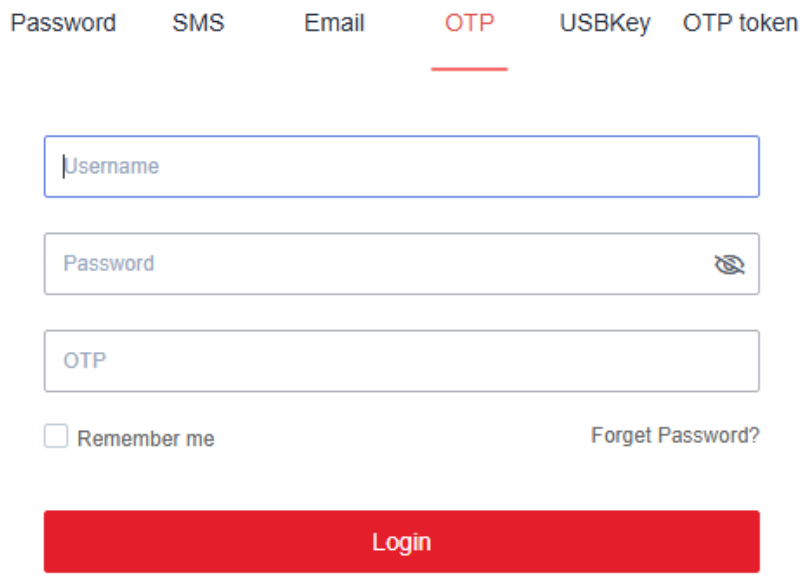
步骤1 选择“手机令牌”方式。

步骤2 依次输入用户登录名、账户登录密码。

步骤3 打开手机令牌客户端，获取动态口令，输入6位OTP口令。

步骤4 单击“登录”，验证通过后即可登录系统。

图 5-5 手机令牌登录



----结束

使用 USBKey 登录

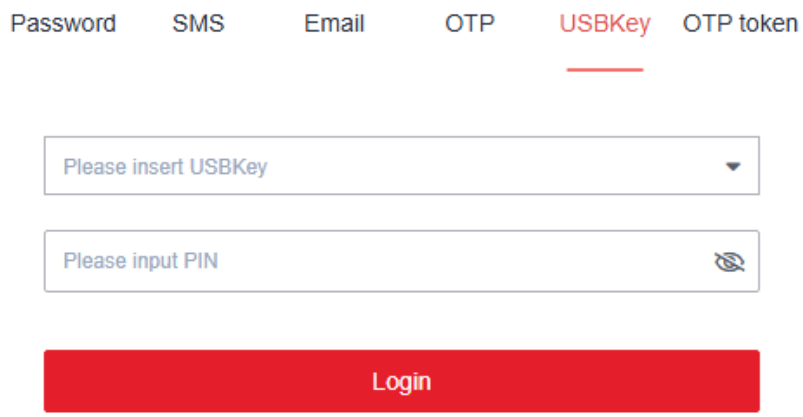
步骤1 选择“USBKey”方式。

步骤2 接入USBKey，自动识别已签发USBKey。

步骤3 输入PIN码。

步骤4 单击“登录”，验证通过后即可登录系统。

图 5-6 USBKey 登录



----结束

使用动态令牌登录

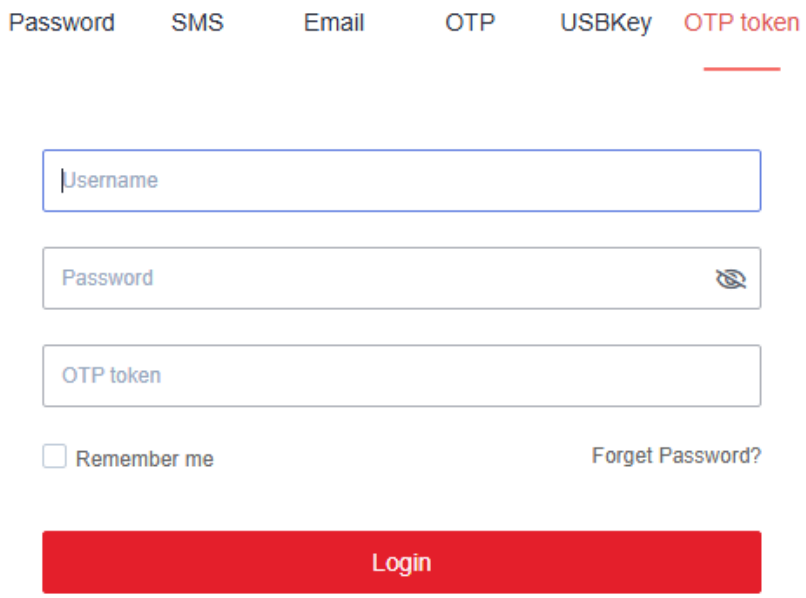
步骤1 选择“动态令牌”方式。

步骤2 依次输入用户登录名、账户登录密码。

步骤3 在已签发硬件令牌上获取动态口令，输入6位OTP口令。

步骤4 单击“登录”，验证通过后即可登录系统。

图 5-7 动态令牌登录



----结束

Azure AD 用户登录

步骤1 单击“使用Azure AD登录”，跳转到Microsoft登录页面。

步骤2 按步骤依次输入用户登录名和密码。

说明

用户登录名需加邮箱后缀，例如zhang@example.com。

步骤3 单击“登录”，验证通过后即可登录系统。

----结束

5.4 使用客户端登录堡垒机

客户端登录是在不改变用户原使用客户端习惯的条件下，可对授权资源进行运维管理。运维人员可选择使用SSH客户端和MSTSC客户端直接登录运维资源。

- 通过SSH客户端登录支持的登录方式包括静态密码、公钥登录、手机短信、手机令牌、动态令牌等。

- 通过MSTSC客户端登录仅支持静态密码的登录方式。
- 推荐使用客户端SecureCRT 8.0及以上版本、Xshell 5及以上版本。

通过 SSH 客户端登录堡垒机

用户获取资源运维权限后，可通过SSH客户端直接登录进行运维操作。

- 支持使用SSH客户端运维的资源，包括SSH、TELNET和Rlogin协议类型主机资源。
- 推荐使用客户端SecureCRT 8.0及以上版本、Xshell 5及以上版本。

步骤1 打开本地SSH客户端工具，选择“文件 > 新建”，新建用户会话。

步骤2 配置会话用户连接。

- 方式一

  在新建会话弹出框，选择协议类型，输入系统登录IP地址、端口号（2222），单击“确认”。再输入系统用户登录名，单击“连接”，连接会话。

- 方式二
  - 在新的空白会话窗口，执行登录命令：***协议类型 用户登录名@系统登录IP 端口***，例如执行ssh admin@10.10.10.10 2222，登录后选择目标服务器。
  - 在新的空白会话窗口，执行登录命令：***协议类型 堡垒机用户登录名@主机账户名@Linux主机IP@堡垒机IP 端口***，例如执行ssh admin@10.10.10.10@10.10.10.101 2222，可直接登录目标服务器。
- 方式三
  - 在新的空白会话窗口，执行登录命令：***协议类型 用户登录名@系统登录IP -p 端口***，例如执行ssh admin@10.10.10.10 -p 2222，登录后选择目标服务器。
  - 在新的空白会话窗口，执行登录命令：***协议类型 堡垒机用户登录名@主机账户名@Linux主机IP@堡垒机IP -p 端口***，例如执行ssh admin@10.10.10.10@10.10.10.101 -p 2222，可直接登录目标服务器。

说明

系统登录IP地址指堡垒机的IP地址（私有IP地址或弹性IP地址），且本地PC与该IP地址的网络连接正常。

步骤3 用户身份验证。

根据命令提示，在新建会话窗口，输入用户身份验证信息。

- SSH客户端登录认证支持“密码登录”、“公钥登录”、“手机短信”、“手机令牌”和“动态令牌”方式。其中“手机短信”、“手机令牌”和“动态令牌”方式，需配置用户多因子认证，详情请参见**多因子认证配置**。
- 如需配置登录SSH客户端后，无操作超时后自动退出的时间，详情请参见**客户端登录配置**。

表 5-4 SSH 客户端登录验证说明

登录方式	登录说明	登录方式配置说明
密码登录	输入堡垒机系统的用户密码。	默认登录方式。 “AD域认证”、“RADIUS认证”、“LDAP认证”或“Azure AD认证”用户登录密码为远程服务器用户密码，详情请参见**远程认证管理**。
公钥登录	输入用于验证登录的私钥和私钥密码，登录验证成功后，再次登录时，该用户在SSH客户端可以免密登录。	用户需要先生成用于验证登录的公私钥对，并在堡垒机系统内的“个人中心”处将SSH公钥添加到堡垒机系统中，具体操作请参见**添加SSH公钥**。
手机短信	“密码登录”或“公钥登录”验证成功后，选择“短信验证码”方式，输入手机短信验证码。	需已为用户账号配置可用手机号码。
手机令牌	“密码登录”或“公钥登录”验证成功后，选择“手机令牌OTP”方式，输入手机令牌验证码。 **说明** 需确保用户登录系统时间与手机时间一致，精确到秒，否则会提示验证码错误。	需用户先绑定手机令牌，再由管理员配置多因子认证，否则用户无法登录系统，详情请参考**配置手机令牌登录**。
动态令牌	“密码登录”或“公钥登录”验证成功后，选择“动态令牌OTP”方式，输入动态令牌验证码。	需已为用户签发动态令牌，详情请参考**动态令牌管理**。

步骤4 登录到堡垒机系统，可查看系统简要信息，并运维已授权的资源。

说明

除了使用堡垒机用户密码直接登录外，还支持使用API方式登录堡垒机指定的资源账户，在获取URL地址后通过URL地址直接登录即可。

----结束

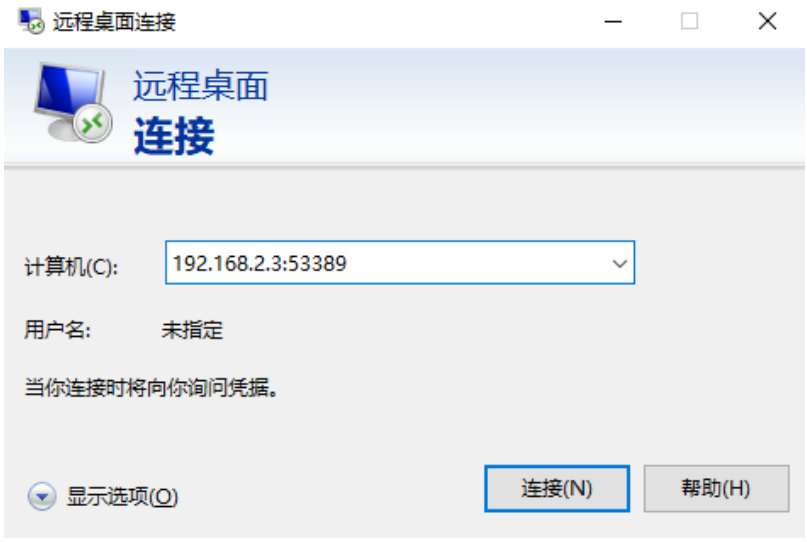
通过 MSTSC 客户端登录堡垒机

用户获取资源运维权限后，可通过MSTSC客户端直接登录进行运维操作。

步骤1 打开本地远程桌面连接（MSTSC）工具。

步骤2 在弹出的对话框中，“计算机”列，输入“堡垒机IP:53389”。

图 5-8 配置计算机



步骤3 单击“连接”，在登录页面完成登录。

- username：***堡垒机用户登录名@Windows主机资源账户名@Windows主机资源IP:Windows远程端口（默认3389）***，例如admin@Administrator@192.168.1.1:3389。

  说明

  “Windows主机资源账户名”必须是已添加到堡垒机中的资源账户，且登录方式是”自动登录“，否则无法识别Windows主机资源账户，且无法生成运维审计文件。不支持实时会话运维。如何添加主机资源账户，请参考**创建资源账户并绑定资源**。

- password：输入当前堡垒机的用户密码。

----结束

6 用户及资源账户管理

6.1 登录用户、角色及资源账户概述

在堡垒机实例管理过程中，按照不同场景采用了登录用户、角色、资源账户类型的区分。

登录用户

堡垒机系统具备集中管理用户功能，创建一个用户即创建一个堡垒机系统的登录账号。

系统管理员**admin**是系统默认用户，为系统第一个可登录用户，拥有系统最高操作权限，且无法删除和更改权限配置。

- 根据用户角色的不同，用户拥有不同的系统操作权限。
- 根据用户组的划分，可批量为同组用户授予资源运维的权限。

仅系统管理员**admin**或拥有“用户”模块权限的用户，可管理系统用户，包括新建用户、批量导入用户、批量导出用户、重置用户账号密码、移动用户部门、更改用户角色、加入用户组、配置用户登录权限、启用、禁用、批量管理用户等操作。

用户组

多个用户加入一个“用户组”形成用户群组，通过对用户组授权可对用户进行批量授权，具体的操作请参见**新建访问控制策略并关联用户和资源账户**。

仅系统管理员**admin**或拥有“用户”模块权限用户，可管理用户组，包括新建用户组、维护用户组成员，管理用户组信息、删除用户组等。

用户组与部门挂钩，不属于个人，当前登录用户新建的用户组默认放在登录用户部门下，不支持修改部门，上级部门有用户组权限的用户可以查看下级部门的所有用户组信息，反之不能，同级之间的用户组都能查看。

说明

- 上级部门管理员向下级部门用户组添加用户时，可将上级部门的用户添加到下级部门用户组。
- 下级部门拥有“用户”模块管理权限的用户，查看用户组详情时，只能查看到用户组内上级部门用户成员列表，不能查看上级部门用户的详情信息。
- 下级部门拥有“用户”模块管理权限的用户，将当前用户组中的上级部门成员移除后，不能再添加移除的上级部门用户。
- 一个用户可加入多个用户组。

用户角色

堡垒机实例预设有角色类型，通过角色来授权不同模块的查看、操作的权限。

堡垒机系统仅**admin**拥有自定义角色和修改角色的权限。

在创建用户后，可为不同用户绑定目标角色，实现权限的控制，一个用户仅能配置一个角色。

实例角色默认包括部门管理员、策略管理员、审计管理员和运维员，默认角色不可删除，但可修改默认角色的权限范围。

同时也支持自定义角色配置权限范围，但仅**admin**可自定义新角色或编辑默认角色的权限范围。各角色的具体权限，可通过“用户 > 角色”，单击角色名称进入角色详情页面查看。

表 6-1 系统默认角色说明

参数	说明
部门管理员	部门的运维管理员，主要负责堡垒机系统的管理。拥有用户管理、资源管理、策略管理等权限。
策略管理员	用户权限策略管理员，负责主机运维的权限策略管理。主要负责策略权限的配置，拥有用户组管理、资源管理和访问策略管理等模块的配置权限。
审计管理员	运维结果审计管理员，查询管理系统审计数据。主要负责查阅和管理系统的审计数据，拥有实时会话、历史会话和系统日志等模块的配置权限。
运维员	访问系统的普通用户和操作人员。主要负责资源的运维，拥有主机运维、应用运维和工单授权管理等权限。

资源账户

资源账户是用来在堡垒机实例中登录资源的账户，登录至资源后可进行运维操作。

一个主机或应用可能有多个登录主机或应用资源的账户，每个被纳管的主机账户或应用账户对应一个资源账户。登录被纳管资源账户时，自动登录无需输入账号和密码。

当添加主机或应用未纳管账户和密码时，默认生成一个“Empty”账户，登录“Empty”资源账户时需手动输入账户名和相应密码。

资源账户组

多个资源账户加入一个“账户组”形成账户群组，通过对账户组授权可对资源账户进行批量授权、批量账户验证。

仅系统管理员**admin**或拥有“账户组”管理权限用户，可管理账户组，包括新建账户组、维护账户组资源，管理账户组信息、删除账户组等。

账户组与部门挂钩，不属于个人。当前登录用户新建的账户组默认放在登录用户部门下，不支持修改部门。

上级部门拥有“账户组”管理权限用户可查看下级部门的所有账户组信息，反之不能，同级之间的账户组可相互查看。

说明

- 上级部门管理员为下级部门账户组添加资源账户时，可将上级部门的资源账户添加到下级部门的账户组，但是下级部门拥有“账户组”管理权限用户操作账户组时，只能查看资源账户列表，不能查看上级部门资源账户的详情信息。
- 下级部门拥有“账户组”管理权限用户将当前账户组中的上级部门资源账户移除后，将不能添加移除的上级部门资源账户。
- 一个资源账户可加入多个账户组。

6.2 新建登录用户并绑定角色

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。

约束限制

为用户配置“所属部门”为上级部门时，当前用户的角色需拥有管理权限，否则会配置失败。修改用户角色管理权限，请参见**修改角色信息**。

前提条件

- 新建单个用户和批量导入用户，需已获取“用户”模块操作权限。
- 同步AD域用户，需已获取“系统”模块操作权限。

新建单个用户

步骤1 登录堡垒机系统。

步骤2 在左侧导航树中，选择“用户 > 用户管理”，进入用户列表页面。

步骤3 在界面的右上角，单击“新建”，弹出用户信息配置窗口。

表 6-2 新建用户参数说明

参数	说明
登录名	自定义登录系统的用户名。 创建后不可修改，且系统内“登录名”唯一不能重复。

参数	说明
认证类型	选择登录系统的认证方式。 • 本地：系统默认方式，即通过系统自身的账号管理系统进行身份认证。 • AD域：通过Windows AD域服务器对用户进行身份认证。 • LDAP：通过LDAP协议，由第三方认证服务器对用户进行身份认证。 • RADIUS：通过RADIUS协议，由第三方认证服务器对用户进行身份认证。 • Azure AD：基于SAML配置，由Azure平台对登录用户进行身份认证。 **说明** 若需启用AD域、LDAP、RADIUS、Azure AD远程认证方式的用户，需先在系统配置远程认证服务器信息，详细操作请参见**认证配置**。
域名	“认证类型”选择“Azure AD”时，需要配置此项。 需输入在Azure平台用户注册时的后缀。
密码/确认密码	仅“认证类型”选择“本地”时，需要配置用户登录系统的密码。
认证服务器	仅“认证类型”选择“AD域”和“LDAP”时，需要选择服务器名称。
姓名	自定义用户姓名。 用户账号使用人员的姓名，便于区分不同的用户。
手机	输入手机号码。 用户账号系统预留手机号码，用于手机短信登录或找回密码。
邮箱	输入邮箱地址。 用户账号系统预留邮箱地址，用于通过邮箱接收系统消息通知。
角色	选择用户的角色，一个用户仅能配置一个角色。 缺省情况下，系统角色包括部门管理员、策略管理员、审计管理员和运维员。 • 部门管理员：负责部门管理，除“用户管理”和“角色管理”模块之外，部门管理员拥有其他全部模块的配置权限。 • 策略管理员：负责策略权限的配置，拥有“用户组管理”、“资源组管理”和“访问策略管理”等模块的配置权限。 • 审计管理员：负责系统和运维数据的审计，拥有“实时会话”、“历史会话”和“系统日志”等模块的配置权限。 • 运维员：系统普通用户和资源操作人员，拥有“主机运维”、“应用运维”和“授权工单”模块的操作访问权限。 • 自定义的角色：仅**admin**可自定义新角色或编辑默认角色的权限范围。
所属部门	选择用户所属部门组织。如何创建系统部门，请参见**新建部门**。

参数	说明
用户描述	（可选）对用户情况的简要描述。

步骤4 单击“确定”，返回用户列表，即可查看和管理新建的用户。

----结束

批量导入用户

步骤1 登录堡垒机系统。

步骤2 在左侧导航树中，选择“用户 > 用户管理”，进入用户列表页面。

步骤3 单击界面右上角的  ，弹出导入用户操作窗口。

步骤4 单击“单击下载”，下载模板文件到本地。

步骤5 按照模板文件中的配置项说明，填写用户信息。

表 6-3 用户导入模板参数说明

参数	说明
登录名	（必填）填入自定义登录系统的用户名。
认证类型	（必填）填入认证方式，仅能填写一种类型。 可选择填入字样：本地，RADIUS，AD域，LDAP，Azure AD、IAM。
密码	（必填）选择认证类型为“本地”时，填入自定义的用户登录密码。
认证服务器/域名	（必填）选择认证类型为“AD域”、“LDAP”或“Azure AD”时，按填写格式要求，填入认证服务器。 • AD域认证填写格式为***IP:PORT***，例如10.10.10.10:389。 • LDAP认证填写格式为**IP:'PORT/ou=test,dc=test,dc=com'**，例如10.10.10.10:'389/ou=test,dc=com'。 • Azure AD认证时填写域名。
姓名	填入使用人员的姓名。
手机	填入使用人员的手机号码。
邮箱	填入使用人员的邮箱地址。
角色	（必填）填入用户的系统角色。 • 仅能填入一个角色类型， • 默认可选角色包括部门管理员、策略管理员、审计管理员和运维员。 • 请务必确保填入系统内已创建的**角色**。

参数	说明
所属部门	（必填）填入用户所归属的部门，需完整填写部门结构。 ● 仅可填入一组部门层级，一个用户只能分属一个部门。 ● 默认可填入部门为总部，部门上下级之间用“,”隔开。 ● 请务必确保填入系统内已创建的**部门**。
用户描述	填入对用户账号的简要描述。
用户组	填入用户账号所属的用户组。 ● 用户账号可同时存在于同部门多个用户组，不同用户组之间用“,”隔开。 ● 请务必确保填入系统内已创建的**用户组**。

步骤6 单击“单击上传”，选择已填入用户信息的模板文件。

步骤7 （可选）勾选“覆盖已有用户”。

- 勾选，表示覆盖同“登录名”的用户账号，刷新用户信息。
- 不勾选，表示跳过同“登录名”的用户账号。

步骤8 单击“确定”，返回用户列表中，即可查看和管理新增的用户。

----结束

同步 AD 域用户

堡垒机通过配置AD认证“同步模式”，可一键同步AD域服务器上已有用户信息，无需手动创建用户。在用户账号登录系统时，由AD域服务器提供身份认证服务。

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统配置 > 认证配置”，进入远程认证配置管理页面。

步骤3 单击“AD认证配置”区域的“添加”，弹出AD认证配置窗口。

步骤4 选择AD域认证“模式”为“同步模式”，展开同步模式参数配置信息。

表 6-4 AD 域同步用户参数说明

参数	说明
服务器地址	输入AD域服务器地址。
状态	选择开启或关闭AD域远程认证，默认开启。 ● 开启，表示开启AD域认证。在配置信息有效情况下，登录系统时启动AD域认证，或同步AD域用户。 ● 关闭，表示关闭AD域认证。

参数	说明
SSL	选择开启或关闭SSL加密认证，默认关闭。 ● 关闭，表示禁用SSL加密认证。 ● 开启，表示启用SSL加密认证，将加密同步用户或认证用户所传输的数据。
模式	选择“同步模式”。
端口	AD域远程服务器的接入端口，默认389端口。
登录名	输入AD域服务器的账户的登录名。
密码	输入AD域服务器的账户的密码。
域	输入AD域的域名。
Base DN	输入AD域远程服务器上的基准DN。
部门过滤	输入AD域远程服务器上待过滤的部门。
用户过滤	输入AD域远程服务器上待过滤的用户。
登录名过滤	输入待过滤的用户登录名，过滤多个登录名用“|”隔开。
姓名	输入AD域远程服务器上代表用户姓名的属性名，例如name。
邮箱	输入AD域远程服务器上代表用户邮箱的属性名，例如mail。
手机	输入AD域远程服务器上代表用户手机的属性名，例如mobile。
同步方式	选择同步AD域用户的方式，包括“手动同步”和“自动同步”。 ● 手动同步：信息配置完成后，手动执行用户同步操作。 ● 自动同步：信息配置完成后，按照配置自动执行用户同步。需同时配置“同步时间”、“同步周期”、“结束时间”。
目标部门	选择将用户账号的所归属的系统部门。
更多	● 勾选“覆盖已有用户”。 – 勾选，表示覆盖同“登录名”的用户账号，刷新用户信息。 – 不勾选，表示跳过同“登录名”的用户账号。 ● 勾选“同步用户状态”，可将用户当前状态同步至堡垒机，建议勾选。

步骤5 （可选）如需选择同步AD域服务器中的用户，单击“下一步”，获取AD域服务器用户源部门结构。

- 默认开启“同步全部用户”。
- 勾选用户源上级部门，即该部门下级部门所有用户都将纳入导入源范畴。
- 开启“创建新部门”，根据AD域的部门结构，同步新建系统部门并同步部门中用户。

步骤6 单击“确认”，返回AD域认证服务器表中，即可查看和管理的AD认证配置信息。

步骤7 单击“立即同步”，立即启动同步AD域用户到堡垒机，返回用户列表，即可查看同步的用户信息。

----结束

6.3 用户管理

6.3.1 管理用户基本信息

当系统用户数量庞大，可通过快速查询和高级搜索方式查询用户。

若用户信息有变更需求，可通过用户管理功能查看和修改，包括查看用户基本信息、查看用户登录配置、查看授权资源账户、修改用户组基本信息、修改用户登录限制、关闭或开启多因子认证、设置用户账号使用有效期等。

前提条件

已获取“用户”模块操作权限。

查看和修改用户信息

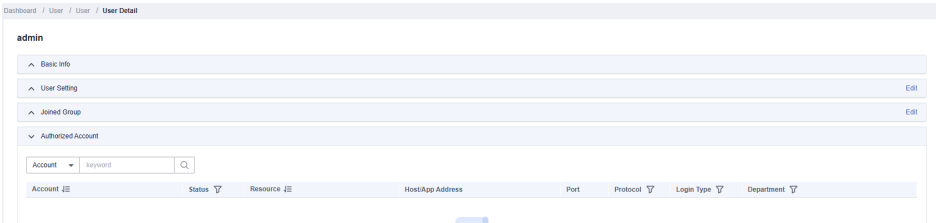
步骤1 登录堡垒机。

步骤2 选择“用户 > 用户管理”，进入用户列表页面，可通过快速查询或高级搜索查询目标用户。

- 快速查询：在搜索框中输入关键字，根据登录名、姓名等快速查询用户。
- 高级搜索：单击“高级搜索”，在相应属性搜索框中分别输入关键字，精确查询用户。

步骤3 在查询的用户列表中，单击目标用户登录名，或者单击“管理”，进入用户详情页面，在“基本信息”区域查看用户基本信息，在“授权资源账户”区域查看用户的资源授权信息。

图 6-1 用户详情页面



步骤4 单击“用户配置”或“用户加入组”区域右侧的“编辑”，可修改相关用户配置信息及用户组成员。

----结束

批量修改用户信息

步骤1 登录堡垒机。

步骤2 选择“用户 > 用户管理”，进入用户列表页面，可通过快速查询或高级搜索查询目标用户。

- 快速查询：在搜索框中输入关键字，根据登录名、姓名等快速查询用户。
- 高级搜索：单击“高级搜索”，在相应属性搜索框中分别输入关键字，精确查询用户。

步骤3 在查询的用户列表中，勾选需要修改的登录用户。

- 在左下角选择“更多 > 删除网盘数据”，在弹窗中确认删除信息，单击“确定”，完成批量删除。
- 在左下角选择“更多 > 移动部门”，在弹窗中选择目标部门，单击“确定”，完成部门的批量修改。
- 在左下角选择“更多 > 更改角色”，在弹窗中选择目标角色，单击“确定”，完成角色的批量修改。

----结束

6.3.2 加入用户组

多个用户加入一个“用户组”形成用户群组，通过对用户组授权可对用户进行批量授权，一个用户可加入多个用户组。

约束限制

- 上级部门管理员向下级部门用户组添加用户时，可将上级部门的用户添加到下级部门用户组。
- 下级部门拥有“用户”模块管理权限的用户，将当前用户组中的上级部门成员移除后，不能再添加移除的上级部门用户。

前提条件

已获取“用户”模块操作权限。

单个用户加入组

步骤1 登录堡垒机。

步骤2 选择“用户 > 用户管理”，进入用户列表页面，可通过快速查询或高级搜索查询目标用户。

- 快速查询：在搜索框中输入关键字，根据登录名、姓名等快速查询用户。
- 高级搜索：单击“高级搜索”，在相应属性搜索框中分别输入关键字，精确查询用户。

步骤3 在目标用户“操作”列，单击“加入组”，弹出用户加入组编辑窗口。

步骤4 勾选一个或多个用户组，将用户加入用户组。

步骤5 单击“确定”，返回用户详情页面，单击目标用户登录名进入用户详情页面，在“用户加入组”区域即可查看已加入的用户组。

说明

如需将批量用户添加至用户组，操作详情请参见**编辑用户组成员**。

----结束

6.3.3 启停用户

堡垒机系统用户快速管理，支持一键批量“启用”或“禁用”其他用户，修改用户账号使用状态。

系统管理员**admin**默认保持“已启用”状态，不支持禁用**admin**用户。

- 启用

  默认为启用，用户状态为“已启用”，用户在权限范围内可正常使用。

- 禁用

  用户状态为“已禁用”。用户账号被禁用后，将被禁止登录系统，失去系统所有操作权限；已登录的用户将被强制退出。

前提条件

已获取“用户”模块操作权限。

操作步骤

步骤1 登录堡垒机。

步骤2 选择“用户 > 用户管理”，进入用户列表页面，可通过快速查询或高级搜索查询目标用户。

- 快速查询：在搜索框中输入关键字，根据登录名、姓名等快速查询用户。
- 高级搜索：单击“高级搜索”，在相应属性搜索框中分别输入关键字，精确查询用户。

步骤3 勾选待改变状态用户，单击左下角“启用”或“禁用”，操作立即生效，即刻可查看用户状态变化。

----结束

6.3.4 删除用户

堡垒机系统用户支持一键删除和批量删除。

系统管理员**admin**不允许被删除。

说明

- 如果删除的目标用户正在使用堡垒机实例，被删除后会被立即强制退出，请谨慎操作。
- 删除后，用户账号所有关联的权限将失效，用户个人网盘中文件将被清空，且无法恢复，因此在删除前请确保已经完成相关数据的备份。

前提条件

已获取“用户”模块操作权限。

操作步骤

步骤1 登录堡垒机。

步骤2 选择“用户 > 用户管理”，进入用户列表页面，可通过快速查询或高级搜索查询目标用户。

- 快速查询：在搜索框中输入关键字，根据登录名、姓名等快速查询用户。
- 高级搜索：单击“高级搜索”，在相应属性搜索框中分别输入关键字，精确查询用户。

步骤3 单击“操作”列的“删除”，即可立即删除该用户。

步骤4 同时勾选多个用户，单击左下角“删除”，可批量删除多个用户。

----结束

6.3.5 配置用户登录限制

背景介绍

为加强用户账号登录管理，堡垒机支持通过配置登录开启或关闭多因子认证、设置账号使用有效期、设置登录时段限制、设置登录IP地址限制、设置登录MAC地址限制，管理用户账号登录权限，有效降低用户账号泄露等导致的安全风险。

- 多因子认证：指开启多因子认证后，用户登录时通过发送短信口令、动态令牌、USBKey等二次认证用户身份。
- 有效期：指用户账号的使用有效期，仅在限定时间内可登录。
- 登录时段限制：指用户账号限定登录星期和时刻。
- 登录IP地址限制：指限制指定来源IP地址的用户登录。
- 登录MAC地址限制：指在局域网内限制指定MAC地址的用户登录。

约束限制

- 为正常使用“手机令牌”多因子认证，需确保系统时间与绑定手机时间一致，精确到秒。否则使用手机令牌登录时，口令将验证失败。
- 系统默认内置短信网关有短信发送频率和条数限制，为避免对“手机短信”多因子认证登录造成影响，可设置“自定义”短信网关，详情请参见**短信网关配置**。
- 由于MAC地址属于数据链路层，用于局域网寻址。MAC地址在传输过程中经过路由或主机，地址会发生变化，因此“登录MAC地址限制”仅在局域网生效。
- 若**admin**用户配置了多因子认证，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

- 已获取“用户”模块操作权限。
- 若需开启“手机令牌”多因子认证，用户需已在个人中心**绑定手机令牌**，否则用户账号将无法登录。

单用户配置登录限制

步骤1 登录堡垒机。

步骤2 选择“用户 > 用户管理”，进入用户列表页面，可通过快速查询或高级搜索查询目标用户。

- 快速查询：在搜索框中输入关键字，根据登录名、姓名等快速查询用户。
- 高级搜索：单击“高级搜索”，在相应属性搜索框中分别输入关键字，精确查询用户。

步骤3 单击需修改的用户登录名，或者单击“管理”，进入“用户详情”页面。

步骤4 单击“用户配置”区域的“编辑”，弹出用户登录限制配置窗口。

表 6-5 用户登录限制参数说明

参数	说明
多因子认证	勾选认证方式，可选择“手机短信”、“手机令牌”、“USBKey”、“动态令牌”。 ● 默认都不勾选，即关闭多因子认证，仅通过本地密码验证身份。 ● 手机短信：用户账号需先绑定可接收短信的手机号码后，再配置手机短信多因子认证。 ● 手机令牌：先由用户在个人中心**绑定手机令牌**后，再配置手机令牌多因子认证。 ● USBKey：为生效USBKey多因子认证，用户账号需再关联**签发USBKey**。 ● 动态令牌：为生效动态令牌多因子认证，用户账号需再关联**签发动态令牌**。
IAM登录	启用后，允许直接从IAM登录到堡垒机。
有效期	设置用户账号使用有效期，包括生效时间和失效时间。
登录时段限制	设置允许或禁止用户账号登录的星期和时刻。
登录IP地址限制	选择黑白名单方式，设置IP地址或地址段。 ● 选择“黑名单”，并配置IP地址或地址段，限制该IP地址或地址段的用户登录。 ● 选择“白名单”，并配置IP地址或地址段，仅允许该IP地址或地址段的用户登录。 ● 选择“黑名单-名单内多因子登录”，并配置IP地址或地址段。该IP地址或地址段名单内的用户，仅允许通过多因子认证方式登录。 ● 选择“白名单-名单外多因子登录”，并配置IP地址或地址段。该IP地址或地址段名单外的用户，仅允许通过多因子认证方式登录。 ● IP地址缺省状态下，即不限制IP地址登录堡垒机。
登录MAC地址限制	选择黑白名单方式，设置MAC地址。 ● 选择“黑名单”，并配置相应MAC地址，限制该MAC地址用户登录。 ● 选择“白名单”，并配置相应MAC地址，仅允许该MAC地址用户登录。 ● MAC地址缺省状态下，不限制MAC地址登录堡垒机。

步骤5 单击“确定”，返回用户详情页面，即可查看用户登录配置信息。

----结束

批量配置用户登录限制

步骤1 登录堡垒机。

步骤2 选择“用户 > 用户管理”，进入用户列表页面，可通过快速查询或高级搜索查询目标用户。

- 快速查询：在搜索框中输入关键字，根据登录名、姓名等快速查询用户。
- 高级搜索：单击“高级搜索”，在相应属性搜索框中分别输入关键字，精确查询用户。

步骤3 勾选待修改配置的登录用户账号。

- 修改多因子认证
  a. 在左下角选择“更多 > 修改多因子认证”，在弹窗中勾选目标账号需要修改的多因子认证方式。
     - 可同时勾选多个不同的认证方式。
     - 勾选“修改全部”后，将会修改当前账号所属部门以及下级部门全部用户的多因子信息。
  b. 确认无误，单击“确定”，完成修改。
- 修改有效期
  a. 在左下角选择“更多 > 修改有效期”，在弹窗中选择目标账号的生效或失效时间。
     - 设置后目标账号在生效时间前不可登录，超过失效时间后也无法登录。
     - 可只设置生效时间和失效时间其中一个，也可同时设置生效和失效时间。
  b. 确认无误，单击“确定”，完成修改。
- 修改登录时段限制
  a. 在左下角选择“更多 > 登录时段限制”，在弹窗中选择登录时段的时间。
     - 按照小时选择目标账号可登录的时间。
     - 在图示中按照“允许登录”和“禁止登录”的标识选择时间。
  b. 确认无误，单击“确定”，完成修改。
- 修改登录IP地址限制
  a. 在左下角选择“更多 > 登录IP地址限制”，在弹窗中选择登录IP地址限制的类型。
     地址限制类型可选择如下：
     - 黑名单：禁止填写的地址进行登录。
     - 白名单：只允许填写的地址进行登录。
     - 黑名单-名单内多因子登录：该IP地址或地址段名单内的用户，仅允许通过多因子认证方式登录。
     - 白名单-名单外多因子登录：该IP地址或地址段名单外的用户，仅允许通过多因子认证方式登录。

b. 在文本框填写IP地址。

多个地址需要换行输入，保证每行只有一个地址或地址段，支持子网掩码，例如：192.168.1.10-192.168.1.100或192.168.1.10/24。

c. 确认无误，单击“确定”，完成修改。

- 修改MAC地址限制

a. 在左下角选择“更多 > MAC地址限制”，在弹窗中选择MAC地址限制的类型。

地址限制类型可选择“黑名单”或“白名单”。

b. 在文本框填写MAC地址。

多个地址需要换行输入，保证每行只有一个地址。

c. 确认无误，单击“确定”，完成修改。

----结束

6.3.6 重置用户登录密码

当用户人员变动较大，用户忘记密码、密码丢失、密码过期等，可能造成登录安全事故。为降低用户登录密码风险，加强系统登录安全，堡垒机支持批量修改用户登录密码。

约束限制

- 系统管理员**admin**的密码不能被其他任何用户重置，可在**admin**的个人中心修改。
- 批量重置仅能生成相同用户密码，建议被批量重置密码的用户登录系统后及时修改个人密码。
- 批量重置密码仅能修改其他用户密码，不能修改个人密码。
- 用户密码不支持明文查看和导出。
- 远程认证用户不支持在系统修改密码，仅能在远程服务器上修改密码。

前提条件

已获取“用户”模块操作权限。

操作步骤

步骤1 登录堡垒机。

步骤2 选择“用户 > 用户管理”，进入用户列表页面，可通过快速查询或高级搜索查询目标用户。

- 快速查询：在搜索框中输入关键字，根据登录名、姓名等快速查询用户。
- 高级搜索：单击“高级搜索”，在相应属性搜索框中分别输入关键字，精确查询用户。

步骤3 勾选需重置密码的登录用户账号，选择左下角“更多 > 重置密码”。

步骤4 弹出重置密码窗口，填写新的密码。

步骤5 确认无误，单击“确定”，完成用户的密码重置。

建议及时将新配置的密码分发给被重置密码的用户。

----结束

6.3.7 导出用户信息

堡垒机支持批量导出用户信息，用于本地备份用户配置，以及便于快速修改用户基本信息。

约束限制

- 支持导出用户登录名、认证类型、认证服务器、用户姓名、手机号码、邮箱、角色、所属部门、用户组等基本信息。
- 为保障用户账号安全，账号登录密码不支持导出。

前提条件

已获取“用户”模块操作权限。

操作步骤

步骤1 登录堡垒机。

步骤2 选择“用户 > 用户管理”，进入用户列表页面，可通过快速查询或高级搜索查询目标用户。

- 快速查询：在搜索框中输入关键字，根据登录名、姓名等快速查询用户。
- 高级搜索：单击“高级搜索”，在相应属性搜索框中分别输入关键字，精确查询用户。

步骤3 勾选需要导出的用户账户，如果不勾选，默认导出全部用户。

步骤4 右上角单击  ，弹出导出确认窗口。

- 设置加密密码，将导出文件加密。
- 输入当前用户的密码，确保导出数据安全。
- 可选择csv或Excel导出格式。

步骤5 单击“确定”，任务创建成功，单击“去下载中心”查看打包进度为100%时，单击“操作”列的“下载”，下载文件到本地，打开本地文件，即可查看导出的用户基本信息。

----结束

6.4 用户角色管理

6.4.1 创建用户角色

系统中的默认角色包括部门管理员、策略管理员、审计管理员和运维员。本章节指导您如何自定义创建角色。

约束限制

- 仅系统管理员**admin**可新建系统角色。
- 系统用户组和账户组模块权限无需单独配置，通过配置用户和资源账户模块即可获取权限。

新建角色

步骤1 登录堡垒机。

步骤2 在左侧导航树中，选择“用户 > 角色”，进入角色列表页面。

步骤3 单击“新建”，弹出角色配置窗口。

表 6-6 新建角色参数说明

参数	说明
角色	自定义角色名称。 创建后不可修改，且系统内“角色”唯一不能重复。
管理权限	选择开启或关闭，默认关闭。 具备管理权限的用户在新建用户或资源时，能够选择当前用户的上级部门。 **说明** 如需赋予角色工单审批权限，则必须开启管理权限，否则即使在**步骤4**中启用工单审批模块的权限，工单审批权限也不生效。 • 开启：代表该角色具备管理权限，能够查看本部门及下级部门的数据。 • 关闭：代表该角色不具备管理权限。
角色描述	（可选）对角色情况的简要描述。

步骤4 单击“下一步”，切换到角色的系统模块权限配置窗口。

在左侧打开或关闭各系统模块权限，打开后，在对应系统模块右侧可以勾选各功能子项。配置后，该角色将具备已勾选功能项的权限。

步骤5 单击“确定”，返回角色列表，即可查看已创建角色。

----结束

6.4.2 删除角色

本章节指导您如何删除角色。

约束限制

- 仅系统管理员**admin**可删除系统角色。
- 系统默认角色不支持删除。

操作步骤

步骤1 登录堡垒机系统。

步骤2 在左侧导航树中，选择“用户 > 角色”，进入角色列表页面。

步骤3 单击目标角色“操作”列的“删除”，即可删除该角色。

步骤4 同时勾选多个角色，单击左下方的“删除”，可批量删除多个角色。

----结束

6.4.3 查询和修改角色信息

若用户角色信息有变更需求，可由**admin**统一查看确认角色信息和修改角色信息，包括查看角色基本信息、查看角色权限范围、修改角色基本信息、修改角色权限范围、移除权限模块等。

约束限制

- 仅系统管理员**admin**可查看和修改系统角色。
- 系统默认角色不支持修改角色的管理权限。
- 系统默认角色支持一键恢复默认权限范围。

操作步骤

步骤1 登录堡垒机系统。

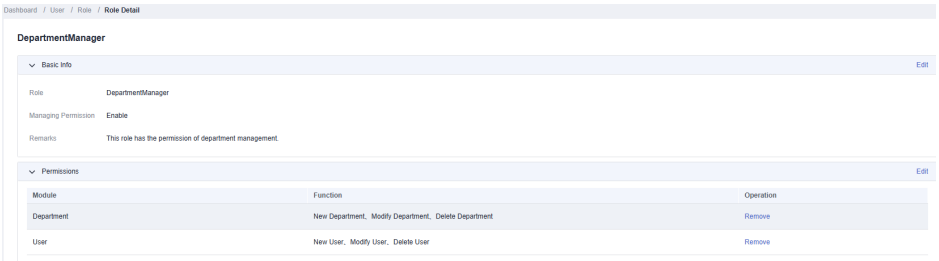
步骤2 在左侧导航树中，选择“用户 > 角色”，进入角色列表页面。

步骤3 查询角色。

在搜索框中输入关键字，根据角色名称快速查询。

步骤4 单击角色名称，或者单击“管理”，进入角色详情页面。

图 6-2 角色详情页面



步骤5 在“基本信息”区域，可查看角色基本信息配置

单击“编辑”，弹出基本信息窗口，即可修改基本信息。

步骤6 在“角色权限”区域，可查看角色系统操作权限范围。

- 单击“编辑”，弹出角色权限配置窗口，即可修改角色系统操作权限。
- 单击任意模块的“移除”，即可立即移除该模块权限。

----结束

6.5 用户组管理

6.5.1 新建用户组

本章节指导您如何新建用户组。

前提条件

已获取“用户”模块操作权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 在左侧导航树中，选择“用户 > 用户组”，进入用户组列表页面。

步骤3 单击“新建”，弹出新建用户组窗口，配置账户组基本信息。

表 6-7 新建用户组

参数	说明
用户组	自定义组名称，系统唯一。
用户组描述	（可选）自定义对用户组的简要描述。

步骤4 配置“用户组”名称和“用户组描述”，系统内自定义的“用户组”名称不能重复。

步骤5 单击“确定”，返回用户组列表页面，查看新建的用户组，并可将用户**加入用户组**。

----结束

6.5.2 删除用户组

堡垒机新建用户组后，支持删除用户组。删除用户组后，通过用户组授权的资源权限将失效。

前提条件

已获取“用户”模块操作权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“用户 > 用户组”，进入用户组列表页面。

步骤3 单击用户组“操作”列的“删除”，即可删除该用户组。

步骤4 同时勾选多个用户组，单击列表下方的“删除”，可批量删除多个用户组。

----结束

6.5.3 查询和修改用户组信息

若用户组信息有变更需求，可查看和修改用户组信息，包括查看用户组基本信息、查看用户组成员、修改用户组基本信息、添加成员、移除组成员等。

约束限制

- 下级部门拥有“用户”模块管理权限的用户，查看用户组详情时，只能查看到用户组内上级部门用户成员列表，不能查看上级部门用户的详情信息。
- 下级部门拥有“用户”模块管理权限的用户，将当前用户组中的上级部门成员移除后，不能再添加移除的上级部门用户。

前提条件

已获取“用户”模块操作权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“用户 > 用户组”，进入用户组列表页面。

步骤3 查询用户组。

在搜索框中输入关键字，根据用户组名称快速查询。

步骤4 单击用户组名称，或者单击“管理”，进入用户组详情页面。

步骤5 在“基本信息”区域，可查看用户组基本信息。

单击“编辑”，弹出基本信息配置窗口，即可修改用户组名称和简要描述。

步骤6 在“用户组成员”区域，可查看用户组所有成员信息。

- 单击“查看”，跳转到用户详情页面。
- 单击用户成员行的“移除出组”，可立即将用户移除出组。

----结束

6.5.4 编辑用户组成员

若您需要在用户组中添加或删除成员，可以参照此章节进行操作。

约束限制

- 下级部门拥有“用户”模块管理权限的用户，查看用户组详情时，只能查看到用户组内上级部门用户成员列表，不能查看上级部门用户的详情信息。
- 下级部门拥有“用户”模块管理权限的用户，将当前用户组中的上级部门成员移除后，不能再添加移除的上级部门用户。

前提条件

已获取“用户”模块操作权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“用户 > 用户组”，进入用户组列表页面。

步骤3 单击用户组“操作”列的“编辑组成员”，即可编辑用户组成员。

步骤4 在弹出的对话框中进行添加用户，添加方式可选择“按用户添加”和“按部门添加”。

步骤5 选择完用户或者部门后，单击“确定”完成组成员的添加。

----结束

6.6 创建资源账户并绑定资源

一个主机或应用可能有多个登录主机或应用的账户，每个被纳管的主机账户或应用账户对应一个资源账户。登录被纳管资源账户时，自动登录无需输入账号和密码。

当添加主机或应用未纳管账户和密码时，默认生成一个“Empty”账户，登录“Empty”资源账户时需手动输入账户名和相应密码。

约束限制

- Edge浏览器应用资源不支持配置自动登录资源账户。
- 若资源安装了AD域服务，添加的资源账户为*域名\资源账户名*，例如ad\administrator。

前提条件

- 已获取“资源账户”模块操作权限。
- 已添加主机或应用资源。

新建单个资源账户

步骤1 登录堡垒机。

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“新建”，弹出资源账户编辑窗口，配置资源账户的属性。

表 6-8 新建资源账户参数说明

参数	说明
关联资源	选择已添加的主机或应用资源。

参数	说明
登录方式	选择登录方式，可选择手动登录、自动登录、提权登录、CSMS凭据登录。 ● 选择“自动登录”，“资源账户”和“密码”为必填项。 ● 选择“手动登录”，可选配置“资源账户”。 ● 选择“CSMS凭证登录”，可选配置仅为“CSMS凭证”和“账户描述”。 ● 选择“提权登录”，必须输入“密码”。 ● 仅针对SSH协议类型主机，可选择“提权登录”。选择后，“切换自”和“切换命令”为必填项，可将原资源账户提权为特权账户。
资源账户	输入资源的账户名称。创建后不可修改，且系统内“资源账户”名唯一，不能重复。 勾选“特权账户”，即该账户可标识为管理资源的特权账户，拥有改密权限。
密码	资源账户对应的密码。 默认勾选“验证”，配置完成确定后，自动验证资源账户的状态。 ● 验证账户通过后，直接保存资源相关信息。 ● 验证账户不通过，根据提示修改配置。 提示验证账户超时，请修改资源的相关配置信息。 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。
SSH Key	针对SSH协议类型主机，可配置登录SSH Key验证。 配置后优先使用SSH Key登录SSH主机资源。
Passphrase	针对SSH协议类型主机，SSH Key对应私钥序列。
CSMS凭证	（仅登录方式选择CSMS凭证登录时可见）选择需要纳管的CSMS凭证。
切换自	针对SSH协议类型主机，选择已配置SSH主机资源账户，将该账户提权为特权账户。
切换命令	针对SSH协议类型主机，配置相应切换命令，例如**su root**。
账户描述	对资源账户的简要描述。

步骤4 单击“确定”，返回资源账户列表页面，看到新建的账户。

----结束

批量导入资源账户

文件导入方式上传的文件类型需为csv、xls或xlsx格式的表格文件。

步骤1 登录堡垒机系统。

步骤2 选择“资源 > 资源账户”，进入资源账户列表页面。

步骤3 单击界面右上角的“导入”，弹出配置界面。

步骤4 如果本地没有可编辑的模板，可以单击“单击下载”，下载模板文件到本地。

步骤5 按照模板文件中的配置项说明，填写要导入的账户配置信息。

表 6-9 资源账户导入模板参数说明

参数	说明
账户	（必填）填入资源账户名称。
登录方式	选择资源登录方式。 ● 可选择自动登录、手动登录、提权登录。
特权账户	选择是否设置资源账户为特权账户。 ● 可选择是或否。
密码	填入资源账户的登录密码。
SSH Key	针对SSH协议类型主机，可填入登录SSH Key验证。 配置后优先使用SSH Key登录资源。 **说明** 导入的目标资源账户仅使用密码登录时，该项不需要输入内容，保留为空即可。
Passphrase	填入SSH Key对应私钥序列。
Oracle参数	针对Oracle协议类型主机，必须填入参数。 ● 可选择SERVICE_NAME或SID ● 可填入多个参数，参数之间用“,”隔开。
SERVICE_NAME或SID	针对Oracle协议类型主机，必须填入参数值。 ● 可填入多个参数值，参数值之间用“,”隔开。
登录角色	针对Oracle协议类型主机，必须填入参数。 ● 可选择normal、sysdba、sysoper ● 可填入多个参数，参数之间用“,”隔开。
数据库名	针对DB2数据库，必须填入参数。 ● 可选择数据库名、实例名。 ● 可填入多个参数，参数之间用“,”隔开。
实例名	针对DB2数据库，必须填入参数。 ● 可选择数据库名、实例名。 ● 可填入多个参数，参数之间用“,”隔开。
切换自	填入一级账户名称。
切换命令	填入切换账户的执行命令。
AD域	针对Radmin类型应用资源，必须填入AD域地址。

参数	说明
账户描述	填入对资源账户的简要描述。
关联资源名称	填入已添加到主机列表或应用列表的资源名称。
IP地址/域名	针对关联主机资源，必须填入主机资源的IP地址或域名。
类型	（必填）填入主机资源的协议类型或应用资源的应用类型。 • 主机资源协议类型：SSH、RDP、TELNET、FTP、SFTP、VNC 、DB2、MySQL、SQL Server、Oracle、SCP、PostgreSQL、GaussDB。 • 应用资源应用类型：IE、Firefox-Windows、Chrome、VNC Client、SecBrowser、VSphere Client、Radmin、dbisql、Other、Mysql Tool、Sql Server Tool、Oracle Tool、Rlogin、Firefox-Linux、DM Tool、KingbaseES Tool、GBaseDataStudio for GBase8a、X11。
端口	针对关联主机资源，必须填入主机端口号。
账户组	填入资源账户所属的账户组。 • 资源账户可同时存在于同部门多个账户组，不同账户组之间用“，”隔开。 • 请务必确保填入系统内已创建的**账户组**。

步骤6 单击“单击上传”，选择要导入的文件。

步骤7 （可选）勾选“覆盖已有账户”，默认不勾选。

- 勾选，表示当账户名称重复时，覆盖原有账户信息。
- 不勾选，表示当账户名称重复时，跳过重复的账户信息。

步骤8 （可选）勾选“验证账户”，默认勾选。

- 勾选，表示当导入账户信息时，同时验证账户状态。
- 不勾选，表示当导入账户信息时，不验证账户状态。

步骤9 单击“确定”，返回资源账户列表页面，查看新增的账户。

----结束

批量创建资源账户

可同时为多台主机创建资源账户。

步骤1 登录堡垒机系统。

步骤2 选择“资源 > 主机管理”，进入主机管理列表页面。

步骤3 勾选需要创建账户的多台主机，单击下方的“更多 > 添加账户”。

说明

只支持协议类型相同的主机。

步骤4 填写添加的账户信息，如表6-10所示。

表 6-10 批量添加资源账户参数

参数名称	参数说明
登录方式	选择创建的账户的登录方式。 • 自动登录 • 手动登录 • CSMS凭证登录 • 提权登录
主机账户	添加账户的名称，可自定义。 如果登录方式选择自动登录，则该项为必选项。
密码	添加账户的密码。
SSH Key	如果当前账户需要SSH Key方式登录，则需要填写该项。 支持PEM或RFC4716格式的RSA私钥，填写之后将优先通过SSH Key登录。
passphrase	SSH Key对应的口令、密码，需先填写SSH Key，如果SSH Key为免密，则该项不需要填写。
CSMS凭证	仅支持登录方式选择CSMS凭证时需要选择填写。
账户描述	当前账户的描述。 描述最长128个汉字或字符。
更多选项	自主选择勾选项。 • 覆盖已有账户：如果账户名重复，是否覆盖已有的账户信息。 • 验证账户：验证添加的账户是否可正常登录，仅支持登录方式为自动登录。

步骤5 确认无误，单击“确认”，完成创建。

----结束

6.7 资源账户管理

通过对资源账户的管理可实现基本信息编辑、验证、加入资源账户组、用户绑定、删除、导出等操作。

约束限制

- 应用资源的账户不支持在线验证。
- 上级部门管理员向下级部门账户组添加资源账户时，可将上级部门的资源账户添加到下级部门账户组。
- 下级部门拥有“资源账户”模块管理权限的用户，将当前账户组中的上级部门资源账户移除后，不能再添加移除的上级部门资源账户。

- 一个资源账户可加入多个账户组。

前提条件

已分别获取“主机管理”、“应用服务器”、“应用发布”、“资源账户”模块操作权限。

查看资源账户列表

步骤1 登录堡垒机。

步骤2 选择“资源 > 资源账户”，进入资源账户列表页面，可通过快速查询或高级搜索查询目标资源账户。

- 快速查询：选择对应搜索字段，在搜索框中输入关键字进行搜索，可选择资源账户、关联资源、主机地址、是否特权账户、是否SSH Key账户、是否使用passphrase。
- 高级搜索：单击“高级搜索”，在相应属性搜索框中分别输入关键字，精确查询资源账户。

----结束

查看和编辑资源账户基本信息

步骤1 在资源账户列表单击目标资源账户名称或“操作”列的“管理”，进入资源账户详情页面。

步骤2 在“基本信息”区域查看资源账户信息，单击“基本信息”区域右侧的“编辑”。

步骤3 在弹窗中可对资源账户的部分信息进行修改，参数详情请参见**表6-8**。

步骤4 确认无误，单击“确定”，完成修改。

----结束

加入资源账户组

将资源账户加入组后，可实现对资源账户的批量管理。

方式一

步骤1 在资源账户列表单击目标资源账户名称或“操作”列的“管理”，进入资源账户详情页面。

步骤2 在“账户加入的组”区域查看已加入的资源账户组信息。

步骤3 单击“账户加入的组”区域右侧的“编辑”，在弹窗中可对资源账户加入的组进行加入或移除。

- 单击已加入的目标账户组名称或“操作”列的“查看”，可查看该资源账户组的全部信息。
- 单击已加入的目标账户组“操作”列的“移除该组”，可将目标资源账户组与当前资源账户取消关联关系。

----结束

方式二

步骤1 在资源账户列表单击目标资源账户“操作”列的“加入组”。

步骤2 在弹窗中可对资源账户加入的组进行加入或移除。

----结束

编辑资源账户绑定的授权用户

用户和资源账户关联后，使用资源账户绑定登录用户进行登录后才可以查看对应的资源。

步骤1 在资源账户列表单击目标资源账户名称或“操作”列的“管理”，进入资源账户详情页面。

步骤2 在“授权用户”区域查看已关联的登录用户信息。

步骤3 单击用户名称可查看用户的详细信息。

----结束

验证资源账户

资源账户**状态**用于标识纳管资源的账户密码是否正确，不能手动修改，只能通过验证账户更新。

资源账户支持“实时验证”和“自动巡检”验证功能。

说明

资源账户验证是后台通过登录资源验证连通性，历史会话不记录该过程。

自动巡检

“自动巡检”在每月5号、15号、25号的凌晨一点，启动验证所有纳管的主机资源账户。验证完成后，系统管理员**admin**会收到验证结果消息（**消息中心**），不会生成任务。

实时验证

步骤1 在资源账户列表页面，勾选指定账户，单击列表下方的“验证”，弹出验证配置框。

步骤2 设置“连接超时”时间，以及“任务完成通知”。

- 默认“连接超时”时长为10秒。网络条件不佳时，可增加“连接超时”时长。
- 默认情况下，不发送任务完成通知。
- 可勾选“邮件通知”，验证完成后在**任务中心**查看验证结果详情。

步骤3 单击“确定”，刷新“资源账户”列表页面，即可查看资源“状态”栏结果。

如需对某一资源账户组的所有资源账户进行批量验证，操作详情请参见**资源账户组管理**。

表 6-11 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。

状态	说明
异常	经过“验证”，账户或密码不正确，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。

----结束

导出资源账户信息

堡垒机支持批量导出资源信息，用于本地备份资源配置，以及便于快速管理资源基本信息。

- 为加强资源信息安全管理，支持加密导出资源信息。
- 导出的主机资源文件中包含主机基本信息、主机下所有资源账户信息、主机资源账户明文密码等。
- 导出的应用服务器文件中包含应用服务器基本信息、应用服务器账户信息、应用路径信息、服务器账户明文密码等。
- 导出的应用发布文件中包含应用发布基本信息、应用资源账户信息、应用资源账户明文密码等。
- 导出的资源账户文件中包含资源账户基本信息、关联资源信息、资源地址信息、资源账户明文密码等。

操作步骤

步骤1 在资源账户列表页面，勾选需要导出的账户。

若不勾选，默认导出全部账户。

步骤2 右上角单击  ，弹出导出资源账户确认窗口。

- 设置加密密码，将导出文件加密。
- 输入当前用户的密码，确保导出数据安全。
- 可选择csv或Excel导出格式。

步骤3 单击“确认”，任务创建成功，单击“去下载中心”查看打包进度为100%时，单击“操作”列的“下载”，下载文件到本地，打开本地文件，即可查看导出的资源账户信息。

----结束

删除资源账户

步骤1 在资源账户列表页面，单击目标资源账户“操作”列的“删除”。

步骤2 在弹窗中确认删除信息，确认无误单击“确认”，完成删除。

如需批量删除，勾选多个资源账户，单击列表查下方的删除进行操作。

说明

- 如果删除的资源账户为某一资源的唯一资源账户，删除后将无法登录目标资源进行运维，请谨慎操作。
- 删除目标资源账户前，请确保目标资源没有正在执行或操作中的任务，删除后会立即生效，正在执行的操作或会话会立即中断，请谨慎操作。

----结束

6.8 资源账户组管理

多个资源账户加入一个“账户组”形成账户群组，通过对账户组授权可对资源账户进行批量授权、批量账户验证。

仅系统管理员**admin**或拥有“账户组”管理权限用户，可管理账户组，包括新建账户组、维护账户组资源，管理账户组信息、删除账户组等。

账户组与部门挂钩，不属于个人。当前登录用户新建的账户组默认放在登录用户部门下，不支持修改部门。上级部门拥有“账户组”管理权限用户可查看下级部门的所有账户组信息，反之不能，同级之间的账户组可相互查看。

说明

- 上级部门管理员为下级部门账户组添加资源账户时，可将上级部门的资源账户添加到下级部门的账户组，但是下级部门拥有“账户组”管理权限用户操作账户组时，只能查看资源账户列表，不能查看上级部门资源账户的详情信息。
- 下级部门拥有“账户组”管理权限用户将当前账户组中的上级部门资源账户移除后，将不能添加移除的上级部门资源账户。
- 一个资源账户可加入多个账户组。

约束限制

- 下级部门拥有“资源账户”模块管理权限的用户，查看账户组详情时，只能查看到账户组内上级部门资源账户列表，不能查看上级部门资源账户的详情信息。
- 下级部门拥有“资源账户”模块管理权限的用户，将当前账户组中的上级部门资源账户移除后，不能再添加移除的上级部门资源账户。

前提条件

已获取“资源账户”模块操作权限。

查看资源账户组列表

步骤1 登录堡垒机。

步骤2 选择“资源 > 账户组”，进入资源账户组列表页面，可通过快速查询搜索目标资源账户组。

快速查询：选择对应搜索字段，在搜索框中输入关键字进行搜索。

----结束

新建资源账户组

步骤1 在账户组页面单击右侧的“新建”，弹出新建账户组窗口，配置账户组基本信息。

表 6-12 新建账户组

参数	说明
账户组	自定义组名称，系统唯一。
账户组描述	（可选）自定义对账户组的简要描述。

步骤2 单击“确定”，返回账户组列表页面，查看新建的账户组，并可将资源账户**加入账户组**。

----结束

编辑资源账户组基本信息

步骤1 在账户组页面单击账户组名称或“操作”列的“管理”进入账户组详情页面。

步骤2 在基本信息区域右侧单击“编辑”，在弹窗中可编辑账户组名称和账户组描述。

步骤3 确认无误，单击“确定”，完成修改。

----结束

编辑资源账户组成员

方式一

步骤1 在账户组页面单击账户组名称或“操作”列的“管理”进入账户组详情页面。

步骤2 在账户组成员区域右侧单击“添加”，在弹窗中勾选需要加入组的资源账户。

可根据资源账户、关联资源、主机地址、应用地址搜索目标资源账户。

步骤3 确认无误，单击“确定”，完成修改。

步骤4 单击目标资源账户的名称或“操作”列的“查看”，可查看资源账户详细信息。

步骤5 单击关联的资源名称可查看资源的详细信息。

步骤6 单击目标资源账户“操作”列的“移除出组”，可将目标资源账户移除出当前账户组。

----结束

方式二：仅添加资源账户至账户组

步骤1 在账户组列表页面单击目标账户组“操作”列的“添加成员”。

步骤2 在弹窗中勾选需要加入组的资源账户。

可根据资源账户、关联资源、主机地址、应用地址搜索目标资源账户。

步骤3 确认无误，单击“确定”，完成修改。

----结束

移除资源账户组成员

方式一：可参照**编辑资源账户组成员**中方式一进行移除。

方式二

步骤1 在账户组列表页面单击目标账户组“操作”列的“移除成员”。

步骤2 在弹窗中勾选需要移除当前组的资源账户。

可根据资源账户、关联资源、主机地址、应用地址搜索目标资源账户。

步骤3 确认无误，单击“确定”，完成移除。

----结束

批量验证账户组的资源账户

对已加入账户组的资源账户，可一键批量验证账户组内资源账户状态。

步骤1 在账户组列表页面勾选需要验证的账户组，单击列表下方的“验证”，弹出验证配置框。

步骤2 设置“连接超时”时间，以及“任务完成通知”。

- 默认“连接超时”时长为10秒。网络条件不佳时，可增加“连接超时”时长。
- 默认情况下，不发送任务完成通知。
- 可勾选“邮件通知”，验证完成后在**任务中心**查看验证结果详情。

步骤3 单击“确定”，返回资源账户列表页面，即可查看资源“状态”栏结果。

----结束

删除资源账户组

步骤1 在账户组列表页面单击目标账户组“操作”列的“删除”。

步骤2 在弹窗确认删除信息，确认无误，单击“确定”，完成删除。

说明

账户组被删除后，账户组所关联的资源账户将批量移除该组，资源账户原有配置不受影响。

----结束

7 纳管资源

7.1 资源纳管概述

堡垒机具备集中资源管理功能，将已有资源和资源账户添加到系统，可实现对资源账户全生命周期管理，单点登录资源，管理或运维无缝切换。

资源纳管场景

堡垒机可纳管主机资源、应用资源、云服务器（容器资源）以及数据库资源。

说明

- 主机资源、数据库资源和应用资源纳管时支持批量导入和批量导出。
- 纳管应用资源、容器资源时需要先在堡垒机实例新建服务器与堡垒机实现连接，建立连接后再将连接的资源添加至堡垒机实例。

表 7-1 堡垒机不同资源纳管说明

支持纳管的资源类型	纳管方式
主机资源	• 公网资源：在堡垒机实例通过新建、导入、自动发现进行连接纳管。 • 不同网络环境或专有网络环境资源：通过在堡垒机实例创建代理服务器实现纳管，目前仅支持SOCKS5代理。
应用资源	通过在堡垒机实例新建应用服务器，实现应用客户端与堡垒机实例的对接，随后在堡垒机实例新建应用资源实现纳管。
数据库资源	在堡垒机实例通过新建、导入、自动发现进行连接纳管。
容器资源	通过在堡垒机实例新建Kubernetes服务器，实现k8s的pod节点与堡垒机实例的对接，随后在堡垒机实例新建容器资源实现纳管。

资源纳管类型

纳管资源类型丰富，包括Windows、Linux等主机资源，Kubernetes服务器以及Windows应用程序资源。

- 支持C/S架构运维接入，包括SSH、RDP、VNC、TELNET、FTP、SFTP、SCP、Rlogin协议类型主机资源。
- 支持B/S、C/S架构应用系统资源接入，可直接配置12+种Edge、Chrome、Oracle Tool等浏览器或客户端Windows服务器应用资源。

表 7-2 堡垒机支持纳管的资源类型

支持纳管的资源类型	支持纳管的资源系统及协议类型
主机资源	支持的协议类型：SSH、RDP、VNC、TELNET、FTP、SFTP、SCP、Rlogin。
应用资源	• Windows支持类型：MySQL Tool、Edge、Firefox-Windows、Oracle Tool、Chrome、VNC Client、SQL Server Tool、SecBrowser、VSphere Client、Radmin、dbisql、Navicat for MySQL、Navicat for PgSQL、Other、IE。 • Linux支持类型：DM Tool、KingbaseES Tool、Firefox-Linux、GBaseDataStudio for GBase8a。
数据库资源	支持的协议类型：Gaussdb、DM。
容器资源	目前仅支持Kubernetes服务器。

7.2 纳管主机或数据库资源

7.2.1 通过堡垒机纳管主机或数据库资源

堡垒机支持添加SSH、RDP、VNC、TELNET、FTP、SFTP、SCP、Rlogin等协议类型的资源，包括Linux主机、Windows主机和数据库等。

本章节主要介绍通过添加单个主机资源、自动发现主机资源、克隆主机资源等方式，将主机资源纳入堡垒机进行集中管理。

约束限制

- 添加的主机和应用资源数量总和不能超过资产数。
- 系统内**协议类型@主机地址:端口**需唯一，不能重复，即被纳管的主机资源需唯一。否则再次创建相同配置的主机时，会报“主机已存在”错误。
- 为主机资源配置“所属部门”为上级部门时，当前用户的角色需拥有管理权限，否则会配置失败。修改用户角色管理权限，请参见**修改角色信息**。

前提条件

已获取“主机管理”模块操作权限。

添加单个主机或数据库资源

步骤1 登录堡垒机系统。

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。

配置主机资源的网络参数和基础信息。

表 7-3 添加资源参数说明

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	选择主机的协议类型。 支持协议类型有SSH、RDP、VNC、TELNET、FTP、SFTP、SCP、Rlogin。
主机地址	输入主机与堡垒机网络通畅的IP地址 ● 选择主机的EIP地址或私有IP地址，建议优先选择可用私有IP地址。 ● 系统默认要求网络接口为主机的IPv4地址。主机开启IPv6地址后，可配置主机的IPv4或IPv6地址。 **说明** 因堡垒机管理同一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。
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。 ● 默认为空，需要根据添加的资源系统类型选择对应的系统类型。 ● 提供多种默认系统类型，并支持系统管理员**admin**自定义系统类型，详情请参见**系统类型**。
终端速度	“协议类型”选择“Rlogin”协议类型主机时，可选择不同终端速率。
编码	“协议类型”选择“SSH”、“TELNET”时，可选择运维界面中文编码。 可选择UTF-8、Big5、GB18030。
终端类型	“协议类型”选择“SSH”、“TELNET”时，可选择运维终端类型。 可选择Linux、Xterm。

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、键盘审计。 ● 文件管理：仅SSH、RDP、VNC协议类型主机可配置。 ● 剪切板：仅SSH、RDP、TELNET协议类型主机可配置。 ● X11转发：仅SSH协议类型主机可配置。 ● 键盘审计：仅RDP、VNC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 7-4 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、手动登录、提权登录或CSMS凭证登录。 ● 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。 ● 选择“CSMS凭证登录”时，需要已有凭证供选择。 ● 选择“提权登录”，必须输入密码。 **说明** 如果选择了密钥对自动登录方式，在创建改密策略的时候需要勾选“允许修改SSH key”选项，否则手动执行改密可能会失败。
主机账户	输入主机中的账户名。 **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。 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；如果纳管的是root账号，请确认对应主机已开启允许root登录权限。 – 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。

参数	说明
SSH Key	针对SSH协议类型主机，可配置登录SSH Key验证。 配置后优先使用SSH Key登录资源。
Passphrase	SSH Key对应私钥序列，可选择配置。 ● 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。
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主机资源。

----结束

自动发现主机或数据库资源

“自动发现”功能可通过输入的IP地址或地址段，使用Nmap工具扫描并发现该IP网段下所有的主机资源。

说明

主机与堡垒机在同一VPC内，且网络连接通畅，才能“自动发现”主机。

步骤1 登录堡垒机系统。

步骤2 选择“资源 > 主机管理”，进入主机管理列表页面。

步骤3 单击界面右上角的“自动发现”，弹出配置界面。

步骤4 输入需导入的主机“IP地址”和主机的“端口”。

默认端口21，22，23，3389，5901，也可添加其它端口或端口范围。

步骤5 单击“确定”，自动开始扫描。

步骤6 扫描结束后，勾选需要导入的主机。

- 输入主机名称，如果不输入主机名称，默认名称为主机IP。
- 主机会根据端口默认选中相关协议类型，如果未匹配默认端口，则需要手动选取协议类型。

步骤7 选择自动发现的主机，单击“添加”。

单击“返回”或“关闭”，返回主机列表页面，查看新增的主机资源。

----结束

克隆主机或数据库资源

若主机服务器内有多种资源形式，可通过克隆已添加的主机资源配置，并修改一定配置参数，快速添加主机资源。

步骤1 登录堡垒机。

步骤2 选择“资源 > 主机管理”，进入主机管理列表页面。

步骤3 在已添加的主机资源的“操作”列，单击“更多 > 克隆”，弹出新建主机编辑窗口。

步骤4 修改已有主机信息，并添加资源账户。

“协议类型”、“主机地址”、“端口”三个参数中必须修改一个。

步骤5 单击“确认”，返回主机列表页面，查看新添加的主机资源。

----结束

7.2.2 代理服务器管理

堡垒机除了能纳管在公网环境的资源外，还可通过创建代理服务器的方式纳管不同网络环境或专有网络环境中的资源，通过代理服务器实现对这里资源的运维。

前提条件

- 已获取“主机管理”模块操作权限。
- 目前仅支持SSH、RDP协议的主机资源。

新建代理服务器

步骤1 登录堡垒机系统。

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“代理服务器”页签，单击“新建”，弹出新建代理服务器编辑窗口，编辑代理服务器信息。

表 7-5 新建代理服务器参数

参数名称	参数说明
服务器名称	自定义代理服务器的名称，长度为1-128个汉字或字符。
代理方式	选择代理方式，目前仅支持SOCKS5代理。
服务器地址	创建为代理服务器的服务器内网IP或公网IP。 IP地址需要能够与堡垒机正常连接。
端口	供代理服务器访问的端口。 SOCKS5代理默认端口为1080，如果有设置固定端口，请填写已设置的端口号。
所属部门	选择已有的所属部门，如果没有可新建。
服务器账户	创建为代理服务器的账户名称。

参数名称	参数说明
密码	创建为代理服务器账户对应的密码。
测试连通性	在创建时可对服务器的连通性进行测试。 建议勾选，如果不勾选，无法保证创建的代理服务器的连通性，可能无法正常管理或运维服务器。

步骤4 确认无误，单击“确认”，创建完成。

----结束

编辑代理服务器信息

步骤1 在堡垒机实例选择“资源 > 主机管理 > 代理服务器”，进入主机代理服务器列表页面。

步骤2 单击服务器名称或“操作”列的“管理”，进入代理服务器详情页面，单击“基本信息”区域右侧的“编辑”。

步骤3 在弹窗中可编辑代理服务器的基本信息，参数详情请参见表7-5。

步骤4 确认无误，单击“确定”，完成修改。

----结束

删除代理服务器

步骤1 在堡垒机实例选择“资源 > 主机管理 > 代理服务器”，进入主机代理服务器列表页面。

步骤2 单击目标代理服务器“操作”列的“删除”，在弹窗中确认删除信息，确认无误，单击“确定”，完成删除。

说明

如果有资源正在使用目标代理服务器，删除后资源将无法正常与堡垒机实例连接，目标资源将无法正常运维，请谨慎操作。

----结束

7.2.3 主机或数据库资源管理

纳管在堡垒机的主机资源可在堡垒机对基本信息、登录用户、资源账户以及运维任务进行查看和编辑，同时也可对代理服务器的基本信息进行查看和编辑。

查看主机或数据库资源列表

步骤1 登录堡垒机。

步骤2 选择“资源 > 主机管理”，进入主机管理页面。

步骤3 选择“主机列表”，在页面可通过快速查询或高级搜索查询目标资源。

- 快速查询：在搜索框中输入关键字，根据登录名、姓名等快速查询用户。

- 高级搜索：单击“高级搜索”，在相应属性搜索框中分别输入关键字，精确查询资源。

----结束

编辑单个资源基本信息

步骤1 单击目标资源名称或“操作”列的“管理”，进入资源详情页面。

步骤2 在“基本信息”区域可查看当前的资源所有信息。

步骤3 单击区域右侧的“编辑”，在弹窗中可对当前资源的基本信息进行修改，参数详情请参见**表7-3**。

步骤4 修改内容需要根据实际情况编辑，确认无误，单击“确定”，完成修改。

----结束

编辑或添加单个资源的资源账户

资源账户是在堡垒机中登录资源进行运维时验证的账户信息，一个资源可绑定多个资源账户。

方式一：可编辑和添加资源账户

步骤1 单击目标资源名称或“操作”列的“管理”，进入资源详情页面。

步骤2 在“资源账户”区域可查看当前资源已绑定的资源账户。

步骤3 单击区域右侧的“添加”，在弹窗中可新建资源账户，参数详情请参见**表6-8**。

步骤4 确认内容无误，单击“确定”，资源账户新建成功并完成与当前资源的关联，返回资源账户列表查看新增的资源账户，存在表示添加成功。

步骤5 单击目标资源账户操作列的“移除”，可取消目标资源账户与当前资源的关联状态，移除的资源账户不会被删除。

步骤6 单击资源账户名称或“操作”列的“查看”，进入资源账户详情页面，可对资源账户的基本信息、所属资源账户组和授权用户进行编辑。

----结束

方式二：只可添加资源账户

步骤1 单击目标资源“操作”列的“更多 > 添加账户”。

步骤2 在弹窗中可为当前资源新建资源账户，参数详情请参见**表6-8**。

步骤3 确认内容无误，单击“确定”，资源账户新建成功并完成与当前资源的关联。

----结束

编辑单个资源的授权登录用户

资源关联的登录用户在登录堡垒机实例后可查看该资源详情，无授权将无法查看。

步骤1 单击目标资源名称或“操作”列的“管理”，进入资源详情页面。

步骤2 在“授权用户”区域可查看当前资源已授权的登录用户。

步骤3 单击用户名称，可查看目标用户的详细信息，同时可编辑用户的登录限制、所属用户组等信息，操作详情请参见**用户管理**。

----结束

编辑单个资源的运维任务

步骤1 单击目标资源名称或“操作”列的“管理”，进入资源详情页面。

步骤2 在“运维任务”区域可查看当前资源的运维任务详情。

----结束

删除单个已纳管的资源

单击目标资源“操作”列的“更多 > 删除”，可删除已纳管的资源。

说明

删除后资源所有数据将被清空，资源关联的资源账户也会被清除，同时策略、工单中关联对应资源账户的数据也会被删除。

批量修改资源系统类型

资源的系统类型是以标签的形式标记于资源，旨在实现通过标签筛选同一系统类型的资源进行管理或编辑。

同时，通过系统类型可区分同一类型的系统资源，方便进行改密操作。

步骤1 在主机列表页面勾选需要修改系统类型的多个资源，在列表左下角选择“更多 > 修改系统类型”。

说明

勾选时请仔细确认勾选的资源是否为同一系统类型，一旦修改完成，所勾选资源的系统类型将统一修改为选择的系统类型。

步骤2 在弹窗中选择需要修改的系统类型。

步骤3 确认无误，单击“确定”，完成修改。

----结束

批量修改资源编码

通过堡垒机纳管的资源可在堡垒机进行编码格式的切换，以便多种编码格式的查看。

步骤1 在主机列表页面勾选需要修改系统类型的多个资源，在列表左下角选择“更多 > 修改主机编码”。

步骤2 在弹窗中选择需要修改的编码类型。

目前仅支持UTF-8、Big5、GB18030。

步骤3 确认无误，单击“确定”，完成修改。

----结束

批量修改运维选项

资源的运维选项是指在运维期间目标资源可执行对应选项的操作或审计。

步骤1 在主机列表页面勾选需要修改系统类型的多个资源，在列表左下角选择“更多 > 修改更多选项”。

说明

勾选时请仔细确认勾选的资源，一旦修改完成，所勾选资源支持的运维选项将进行统一修改。

步骤2 在弹窗中选择需要修改的运维选择。

目前支持文件管理、X11转发、上行剪切板、下行剪切板、键盘审计。

步骤3 确认无误，单击“确定”，完成修改。

----结束

批量修改连接方式

自定义批量修改主机资源的连接方式，选择对应方式后，堡垒机连接目标主机将通过修改的连接方式进行连接。

步骤1 在主机列表页面勾选需要修改系统类型的多个资源，在列表左下角选择“更多 > 修改主机连接方式”。

说明

勾选时请仔细确认勾选的资源，一旦修改完成，所勾选资源支持的连接方式都将进行统一修改。

步骤2 在弹窗中选择需要修改的主机连接选择。

说明

目前支持直连和代理模式，选择代理模式后需要选择代理服务器，如果没有代理服务器信息，需要参照**代理服务器管理**进行创建。

步骤3 确认无误，单击“确定”，完成修改。

----结束

批量移动资源所属部门

步骤1 在主机列表页面勾选需要修改系统类型的多个资源，在列表左下角选择“更多 > 移动部门”。

说明

勾选时请仔细确认勾选的资源，一旦修改完成，所勾选资源的所属部门将进行统一修改。

步骤2 在弹窗中选择需要修改的部门。

步骤3 确认无误，单击“确定”，完成修改。

----结束

批量添加资源账户

可通过批量添加账户为多个资源添加同样的资源账户，添加后该资源账户关联选择的所有资源。

步骤1 在主机列表页面勾选需要修改系统类型的多个资源，在列表左下角选择“更多 > 添加账户”。

说明

勾选时请仔细确认勾选的资源，一旦添加完成，所勾选资源将统一新增同一个账户。

步骤2 在弹窗中填写添加资源账户的相关信息，参数详情请参见**表6-8**中对应参数信息。

步骤3 确认无误，单击“确定”，完成修改。

----结束

批量导出主机资源

步骤1 在“主机管理”页面，勾选需要导出的主机资源。

说明

若不勾选，默认导出全部资源。

步骤2 右上角单击  ，弹出导出主机资源确认窗口。

- 设置加密密码，将导出文件加密。
- 输入当前用户的密码，确保导出数据安全。
- 可选择csv或Excel导出格式。

步骤3 单击“确认”，任务创建成功，单击“去下载中心”查看打包进度为100%时，单击“操作”列的“下载”，下载文件到本地，打开本地文件，即可查看导出的主机资源信息。

----结束

7.3 纳管应用资源

7.3.1 通过堡垒机纳管应用资源

通过在一台支持远程桌面的Windows系统或者Linux操作系统服务器上，部署客户端软件和浏览器，应用发布是将服务器和应用账户纳入堡垒机管理的功能。

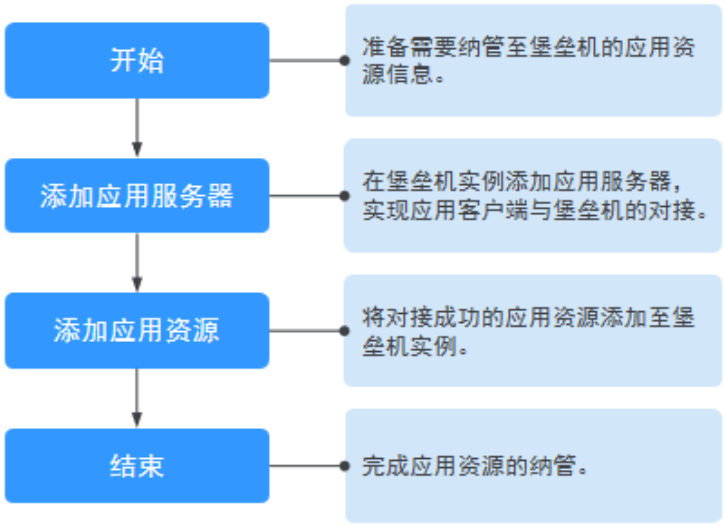
用户获取应用发布访问权限后，通过应用账户的密码自动代填，访问客户端应用和Web应用，并以视频方式全程记录用户运维操作，实现对远程应用账户的安全管理和用户远程访问应用的操作审计。

堡垒机支持添加Chrome、Edge、Firefox、SecBrowser、Oracle Tool 、MySQL、SQL Server Tool、dbisql、VNC Client、VSphere Client、Radmin等应用。

纳管应用资源流程

通过在堡垒机实例新建应用服务器，实现应用客户端与堡垒机实例的对接，随后在堡垒机实例新建应用资源实现纳管。

图 7-1 纳管应用资源流程



约束限制

- 添加的主机和应用资源数量总和不能超过资产数。
- 支持对Windows Server2008 R2及以上的Windows系统版本的应用进行管理。
- 支持对Centos7.9系统的Linux服务器的应用进行管理。
- Linux服务器和堡垒机之间需要开通的端口号：2376和35000~40000，且端口号不可修改。
- 添加应用发布前，需已添加应用服务器。
- Edge浏览器应用不支持配置自动登录账户。
- 当多个堡垒机实例共用一个应用服务器时，堡垒机实例版本需保持一致，否则可能会出现低版本实例无法正常使用应用服务器的问题。

前提条件

- 已有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。
- 已成功安装应用服务器，详细操作指导请参见**安装应用发布服务器**。
- 已获取“应用服务器”和“应用发布”模块管理权限。

添加单个应用服务器

步骤1 登录堡垒机系统。

步骤2 选择“资源 > 应用发布 > 应用服务器”，进入应用服务器列表页面。

步骤3 单击“新建”，进入应用服务器配置窗口。

- 新建Windows应用服务器

表 7-6 Windows 应用服务器参数说明

参数	说明
服务器类型	Windows
服务器名称	自定义的访问应用服务器名称，系统内“服务器名称”不能重复。
服务器地址	输入访问应用的服务器IP地址或域名。
类型	选择访问应用的浏览器或客户端工具类型。 默认支持14种类型，包括MySQL Tool、Edge、Firefox-Windows、Oracle Tool、Chrome、VNC Client、SQL Server Tool、SecBrowser、VSphere Client、Radmin、dbisql、Navicat for MySQL、Navicat for PgSQL、Other。 每一类应用类型默认一种应用程序，可在默认“程序启动路径”中获取应用程序名称。
端口	输入访问应用发布服务器的端口，Windows服务器默认为3389。
服务器账户	输入访问应用的服务器账户。 因应用服务器通过AD域安装，“服务器账号”输入格式为*域名\账户名*，例如*ad|administrator*。
密码	输入访问应用的服务器账户的密码。
所属部门	选择应用服务器的归属部门。
程序启动路径	输入限制应用资源访问应用服务器上的具体应用的程序路径。 – 每种程序类型有一个默认启动路径，也可自定义启动路径。例如：限制只能访问应用设备的Chrome浏览器，默认启动路径为“C:\DevOpsTools\Chrome\chrome.exe”。 – 选择“Other”类型，必须手动配置相应程序路径。
服务器描述	（可选）对应用服务器的简要描述。

- 新建Linux应用服务器

表 7-7 Linux 应用服务器参数说明

参数	说明
服务器类型	Linux
服务器名称	自定义的访问应用服务器名称，系统内“服务器名称”不能重复。
服务器地址	输入访问应用的服务器IP地址或域名。
类型	选择访问应用的浏览器或客户端工具类型。 支持类型：DM Tool、KingbaseES Tool、Firefox-Linux、GBaseDataStudio for GBase8a。

参数	说明
端口	输入访问应用发布服务器的端口，Linux服务器固定为2376。
密码	密码请联系技术支持获取。
所属部门	选择应用服务器的归属部门。
服务器描述	（可选）对应用服务器的简要描述。

步骤4 单击“确定”，返回应用服务器列表中查看新增的服务器。

----结束

从文件导入应用服务器

文件导入方式上传的文件类型需为csv、xls或xlsx格式的表格文件。

步骤1 登录堡垒机系统。

步骤2 选择“资源 > 应用发布 > 应用服务器”，进入应用服务器列表页面。

步骤3 单击界面右上角的“导入”，弹出配置界面。

步骤4 如果本地没有可编辑的模板，可以单击“单击下载”，下载模板文件到本地。

步骤5 按照模板文件中的配置项说明，填写要导入的应用服务器配置信息。

步骤6 单击“单击上传”，选择要导入的文件。

步骤7 （可选）勾选“覆盖已有应用服务器”，默认不勾选。

- 勾选，表示当应用服务器名称重复时，覆盖原有应用服务器信息。
- 不勾选，表示当应用服务器名称重复时，跳过重复的应用服务器信息。

步骤8 单击“确定”，可以在列表中看到新增的应用服务器。

----结束

添加单个应用资源

步骤1 登录堡垒机系统。

步骤2 选择“资源 > 应用发布 > 应用列表”，进入应用发布列表页面。

步骤3 单击“新建”，进入应用发布资源配置窗口。

表 7-8 添加应用资源参数说明

参数	说明
应用名称	自定义的应用发布名称，系统内“应用名称”不能重复。 **说明** 应用名称全系统唯一，不能重复，也不能与主机名称重复。
应用服务器	选择已创建的应用发布服务器。

参数	说明
所属部门	选择应用所属部门。
应用地址	（可选）输入有效IP或域名。 ● 应用发布为浏览器时，输入网页地址。若地址有对应的端口，则地址为URL:端口号。 ● 应用发布为数据库或客户端时，输入数据库服务器的地址。
应用端口	（可选）输入应用访问端口。 ● 应用发布为数据库时，输入对应数据库访问的端口。 ● 应用发布为除数据库外其他应用时，无需填写。
应用参数	（可选）输入应用相关参数。 ● 应用发布为数据库时，输入实例名。 ● 应用发布为除数据库外其他应用时，无需填写。
自定义参数	（可选）输入应用的自定义参数。 ● 代填节点：填写被代填输入框的Selector路径。例如：**#accountNamed > input** 如何获取Selector路径，请参见**获取Selector路径**。 ● 代填内容：填写代填的文本，可使用**{account}**或者**{password}**替代应用账户和密码。
更多选项	（可选）设置在运维过程中，会话窗口功能选项。 ● 文件管理：管理文件或文件夹的权限，即查看、删除、编辑文件和文件夹的权限。 ● 上行剪切板：运维会话RDP剪切板的功能，复制文本的权限。 ● 下行剪切板：运维会话RDP剪切板的功能，粘贴文本的权限。 ● 键盘审计：对键盘输入的信息进行记录。
标签	（可选）自定义标签或选择已有标签。
应用描述	（可选）对应用发布的简要描述。

步骤4 单击“下一步”，进入资源账户配置页面。

表 7-9 添加应用资源账户参数说明

参数	说明
添加账户	● 选择“立即添加”，需要继续配置依次配置“登录方式”、“应用账户”等信息。 ● 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。 单击“确定”，自动创建一个“[Empty]”资源账户（一个应用仅包含一个“[Empty]”账户）。

参数	说明
登录方式	• 登录方式为“自动登录”时，“应用账户”和“密码”为必填项。 • 登录方式为“手动登录”时，可选设置“应用账户”。 未设置“应用账户”时，自动创建一个“[Empty]”资源账户。
应用账户	访问应用使用的账户名。
密码	应用账户对应的密码。
AD域	针对Radmin类型应用，可填入AD域地址。
账户描述	对资源账户的简要描述。

说明

登录“[Empty]”账户时，需在运维会话窗口手动输入应用账户名和密码。

步骤5 单击“确认”，返回应用发布列表页面，查看新建的应用发布服务。

----结束

从文件导入应用资源

文件导入方式上传的文件类型需为csv、xls或xlsx格式的表格文件。

步骤1 登录堡垒机系统。

步骤2 选择“资源 > 应用发布 > 应用列表”，进入应用发布列表页面。

步骤3 单击界面右上角的“导入”，弹出配置界面。

步骤4 单击“单击下载”，下载模板文件到本地。

步骤5 按照模板文件中的配置项说明，填写要导入的应用发布服务配置信息。

步骤6 单击“单击上传”，选择要导入的文件。

步骤7 （可选）勾选“覆盖已有应用”，默认不勾选。

- 勾选，表示当应用名称重复时，覆盖原有应用信息。
- 不勾选，表示当应用名称重复时，跳过重复的应用信息。

步骤8 单击“确定”，可以在应用发布服务列表中看到新增的应用发布。

----结束

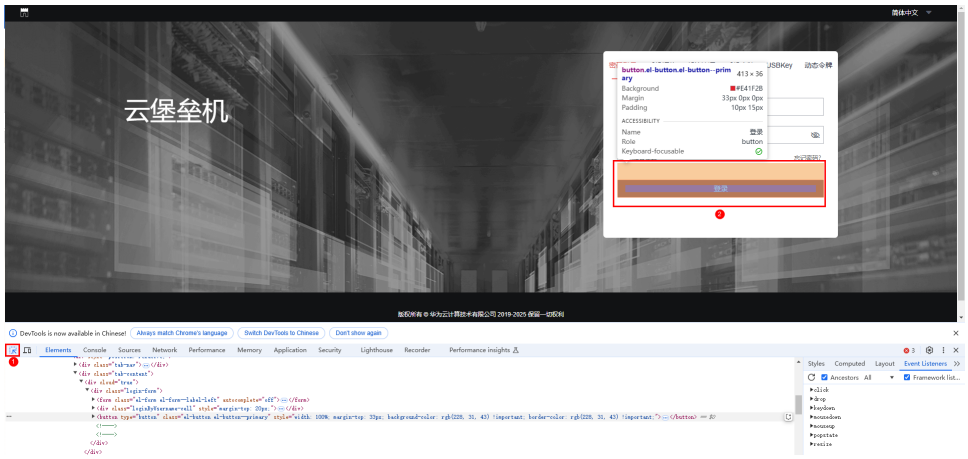
获取 Selector 路径

此处以获取堡垒机登录页面的登录按钮的Selector路径为例进行说明。

步骤1 在堡垒机登录页面，按F12打开浏览器的开发者工具。

步骤2 单击  后，再单击“登录”。

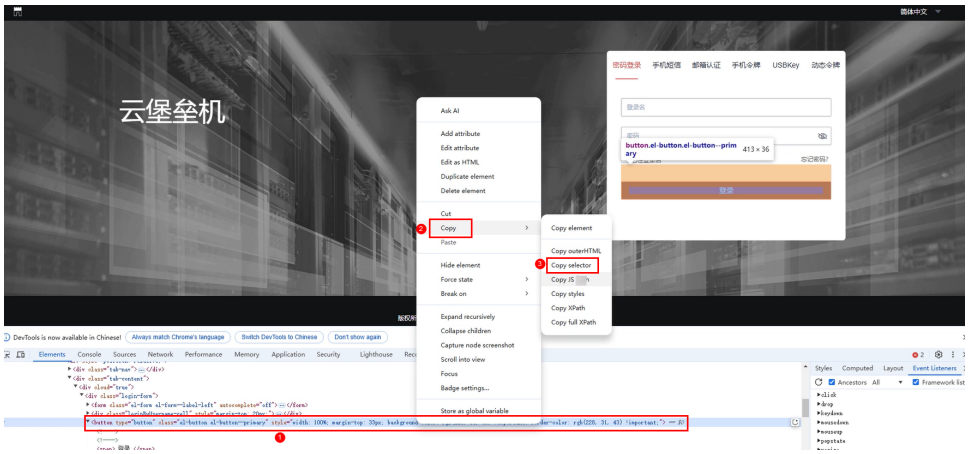
图 7-2 捕获登录按钮元素



步骤3 在Elements面板的button所在行，单击鼠标右键，然后选择“Copy > Copy selector”。

复制所得的值，即为登录按钮的Selector路径。

图 7-3 获取 Selector 路径



----结束

7.3.2 应用服务器管理

通过堡垒机实例可对应用服务器进行修改、删除、导出操作，确保应用服务器信息保持及时更新。

编辑应用服务器信息

步骤1 登录堡垒机。

步骤2 选择“资源 > 应用发布 > 应用服务器”，进入应用服务器列表页面。

步骤3 单击目标应用服务器名称或“操作”列的“管理”，进入应用服务器详情页面。

步骤4 在基本信息区域查看应用服务器详细信息，单击区域右侧的“编辑”。

步骤5 在弹窗中编辑应用服务器的基本信息，参数详情请参见**表7-6**。

说明

编辑应用服务器信息时服务器系统类型不可修改。

步骤6 确认无误，单击“确定”，完成修改。

----结束

删除应用服务器

步骤1 登录堡垒机。

步骤2 选择“资源 > 应用发布 > 应用服务器”，进入应用服务器列表页面。

步骤3 单击目标应用服务器名称或“操作”列的“删除”，在弹窗中确认删除信息，确认无误，单击“确定”，完成删除。

说明

如果有资源正在使用目标应用服务器，删除后资源将无法正常与堡垒机实例连接，目标资源将无法正常运维，请谨慎操作。

----结束

批量导出应用服务器列表

步骤1 在“应用发布 > 应用服务器”页面，勾选需要导出的应用服务器资源。

若不勾选，默认导出全部应用服务器资源。

步骤2 右上角单击  ，弹出导出应用服务器资源确认窗口。

- 设置加密密码，将导出文件加密。
- 输入当前用户的密码，确保导出数据安全。
- 可选择csv或Excel导出格式。

步骤3 单击“确认”，任务创建成功，单击“去下载中心”查看打包进度为100%时，单击“操作”列的“下载”，下载文件到本地，打开本地文件，即可查看导出的应用服务器资源信息。

----结束

修改应用服务器所属部门

步骤1 登录堡垒机。

步骤2 选择“资源 > 应用发布 > 应用服务器”，进入应用服务器列表页面。

步骤3 勾选目标应用服务器，选择列表左下方的“更多 > 移动部门”，在弹窗中选择需要移动的部门，确认无误，单击“确定”，完成修改。

说明

如果勾选了多台应用服务器，部门信息将进行批量修改，批量操作无法撤回，请谨慎修改。

----结束

7.3.3 应用资源管理

在堡垒机实例可对已添加的应用资源的信息进行编辑，包括基本信息、资源关联的资源账户、授权的登录用户，同时可为应用资源添加资源账户、添加标签等操作。

查看应用资源列表

步骤1 登录堡垒机系统。

步骤2 选择“资源 > 应用发布 > 应用列表”，进入应用列表页面，可查看所有已纳管的应用资源。

----结束

编辑应用资源基本信息

步骤1 单击目标应用资源的名称或“操作”列的“管理”，进入应用资源详情页面。

步骤2 在“基本信息”区域查看基本信息，单击右侧“编辑”，在弹窗中可对应用资源的基本信息进行编辑修改，参数详情请参见**表7-8**。

步骤3 确认无误，单击“确定”，完成修改。

----结束

管理应用资源的资源账户

步骤1 单击目标应用资源的名称或“操作”列的“管理”，进入应用资源详情页面。

步骤2 在“资源账户”区域查看应用资源已关联的资源账户。

- 单击资源账户名称或“操作”列的“查看”，可查看目标资源账户的详细信息。
- 单击目标资源账户“操作”列的“移除”，可取消资源账户与当前应用资源的关联关系。

步骤3 单击右侧“添加”，在弹窗中填写账户信息，为当前应用资源添加资源账户，参数详情请参见**表7-9**。

步骤4 确认无误，单击“确定”，完成添加。

----结束

管理应用资源的授权用户

步骤1 单击目标应用资源的名称或“操作”列的“管理”，进入应用资源详情页面。

步骤2 在“授权用户”区域查看应用资源已关联的登录账户。

----结束

批量修改应用资源运维选项

步骤1 在应用列表中勾选需要修改运维选项的应用资源，在列表左下方选择“更多 > 修改更多选项”。

步骤2 在弹窗中勾选需要修改的选项。

说明

如果是为应用资源进行批量修改，执行成功后，不可回退，请谨慎操作。

步骤3 确认无误，单击“确定”，完成修改。

----结束

修改应用资源的部门

步骤1 在应用列表中勾选需要修改运维选项的应用资源，在列表左下方选择“更多 > 移动部门”。

步骤2 在弹窗中选择需要修改的部门。

说明

如果是为应用资源进行批量修改，执行成功后，不可回退，请谨慎操作。

步骤3 确认无误，单击“确定”，完成修改。

----结束

批量添加应用资源的资源账户

步骤1 在应用列表中勾选需要修改运维选项的应用资源，在列表左下方选择“更多 > 添加账户”。

步骤2 在弹窗中输入账户信息，参数详情请参见**表7-9**。

步骤3 确认无误，单击“确定”，完成添加。

----结束

删除应用资源

步骤1 在应用列表中单击目标应用资源“操作”列的“更多 > 删除”。

步骤2 在弹窗中确认删除信息，确认无误，单击“确定”，完成删除。

说明

删除后将无法执行目标资源的运维，请谨慎操作。

----结束

导出应用资源列表

步骤1 在“应用列表”页面，勾选需要导出的应用资源。

说明

若不勾选，默认导出全部资源。

步骤2 右上角单击  ，弹出导出应用资源确认窗口。

- 设置加密密码，将导出文件加密。

- 输入当前用户的密码，确保导出数据安全。
- 可选择csv或Excel导出格式。

步骤3 单击“确认”，任务创建成功，单击“去下载中心”查看打包进度为100%时，单击“操作”列的“下载”，下载文件到本地，打开本地文件，即可查看导出的应用资源信息。

----结束

7.4 云服务器管理（通过堡垒机纳管容器资源）

7.4.1 新建 Kubernetes 服务器

堡垒机支持您将Kubernetes服务器添加至堡垒机上进行管理。本小节介绍如何将Kubernetes服务器添加至堡垒机上。

约束限制

- 纳管的Kubernetes服务器数量受堡垒机的License限制。
- 新建Kubernetes服务器需要“Kubernetes服务器”模块操作权限。
- 仅专业版堡垒机支持纳管Kubernetes服务。
- 使用此功能需要V3.3.48.0及以上版本堡垒机。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“资源 > 云服务器管理”，进入云服务器管理页面。

步骤3 单击“Kubernetes服务器”，进入Kubernetes服务器页面。

步骤4 单击右上角的“新建”，在弹出的对话框中填写参数。

表 7-10 新建 Kubernetes 服务器参数说明

参数	说明
服务器名称	自定义服务名称。
服务器地址	填入您的Kubernetes服务器地址。
端口	填入您的Kubernetes服务器端口。
类型	V3.3.54.0版本堡垒机只可选择“Kubernetes”。
所属部门	选择Kubernetes服务器归属的部门，默认为“总部”。
client-cert	获取调试信息中的“client-certificate-data”参数值，并将“client-certificate-data”参数值base64解码后填入。
client-key	获取调试信息中的“client-key-data”参数值，并将“client-key-data”参数值base64解码后填入。

参数	说明
ca-cert	获取调试信息中的“certificate-authority-data”参数值，并将“certificate-authority-data”参数值base64解码后填入。
服务器描述	（可选）输入对该服务器的描述。

步骤5 单击“确定”，完成Kubernetes服务器的创建。

----结束

7.4.2 Kubernetes 服务器相关操作

Kubernetes服务器纳入堡垒机管理后，您可以随时将纳入管理的服务器删除或者修改信息切换服务器。

约束限制

- 纳管的Kubernetes服务器数量受堡垒机的License限制。
- 对Kubernetes服务器操作需要“Kubernetes服务器”模块操作权限。
- 使用此功能需要V3.3.48.0及以上版本堡垒机。

修改 Kubernetes 服务器信息

步骤1 登录堡垒机系统。

步骤2 选择“资源 > 云服务器管理”，进入云服务器管理页面。

步骤3 单击“Kubernetes服务器”，进入Kubernetes服务器页面。

步骤4 在待修改信息服务器所在的“操作”列，单击“管理”，进入管理页面。

步骤5 单击左上角的编辑，修改Kubernetes服务器相关信息，具体参数请参考**表7-10**。

步骤6 单击“确定”，完成Kubernetes服务器的信息修改。

----结束

删除 Kubernetes 服务器

步骤1 登录堡垒机系统。

步骤2 选择“资源 > 云服务器管理”，进入云服务器管理页面。

步骤3 单击“Kubernetes服务器”，进入Kubernetes服务器页面。

步骤4 在待删除服务器所在的“操作”列，单击“删除”。

步骤5 在弹出的对话框中单击“确定”，完成删除Kubernetes服务器。

----结束

7.4.3 新建容器

堡垒机支持您将容器添加至堡垒机上进行管理。本小节介绍如何将容器添加至堡垒机上。

约束限制

- 对容器的操作需要“容器列表”模块操作权限。
- 已将容器所在的Kubernetes服务器添加至堡垒机进行管理，详情操作请参见**新建Kubernetes服务器**。
- 使用此功能需要V3.3.48.0及以上版本堡垒机。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“资源 > 云服务器管理”，进入云服务器管理页面。

步骤3 单击左上角的“新建”，在弹出的对话框中填写相关参数。

表 7-11 新建容器参数说明

参数	说明
容器名称	自定义您需要纳管的容器（Container）名称。
Kubernetes服务器	选择您在**新建Kubernetes服务器**中添加的Kubernetes服务器。
Namespace	选择待纳管容器所在的Namespace。
Pod	（可选）选择待纳管容器所在的Pod。 若该Pod下只有您待纳管的Container，则可以不选择。
Container	（可选）选择您需要纳管的Container。 若Pod下存在多个容器您未选择，系统默认会自动连接Pod下的第一个Container。
exec-command	（可选）请输入您需要在Container内的预运行命令。 如果您不填此项，则不会运行任何命令，并且输入/输出将附加到容器的主进程。 **说明** 如果您填写了此行参数，连接行为类似于**kubectl exec** 若您未填写此行参数，连接行为类似于**kubectl attach**
所属部门	选择纳管容器所属的部门。
标签	添加纳管容器的标签。
容器描述	添加该容器的描述。

步骤4 单击“确定”，完成容器的纳管。

----结束

7.4.4 容器资源管理

容器纳入堡垒机管理后，您可以随时将纳入管理的容器删除或者修改容器信息。

约束限制

- 容器的操作需要“容器列表”模块操作权限。
- 使用此功能需要V3.3.48.0及以上版本堡垒机。

编辑容器

步骤1 登录堡垒机系统。

步骤2 选择“资源 > 云服务器管理”，进入云服务器管理页面。

步骤3 在待修改信息容器所在的操作列单击“管理”，进入“容器详情”页面。

步骤4 在“基本信息”行的右侧单击“编辑”，在弹出的对话框中修改容器的相关信息，具体参数规则详见**表7-11**。

步骤5 修改完参数信息后，单击“确定”，完成容器的信息修改。

----结束

删除容器

步骤1 登录堡垒机系统。

步骤2 选择“资源 > 云服务器管理”，进入云服务器管理页面。

步骤3 在待删除容器所在的操作列单击“删除”。

步骤4 在弹出的对话框中单击“确定”，完成删除容器。

----结束

7.5 资源标签管理

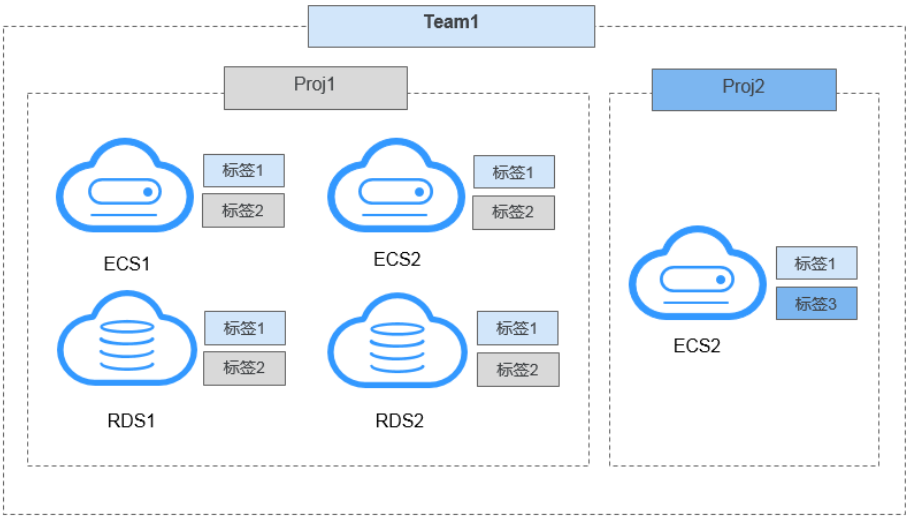
7.5.1 资源标签概述

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。

图 7-4 标签示例



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7-12。

表 7-12 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

7.5.2 添加资源标签

堡垒机系统每个用户可自定义资源标签，资源标签仅个人账户使用，不能被CBH系统内用户共用。

您可以在创建主机或应用资源时添加标签，也可以在资源创建完成后，在资源或运维列表的详情页添加标签。一个主机或应用默认最大拥有10个标签。

添加主机或添加应用可直接配置“标签”参数。本小节主要介绍资源创建完成后，在资源或运维管理页面添加标签，以“主机管理”为操作示例。

前提条件

已获取“主机管理”、“应用发布”、“主机运维”或“应用运维”功能模块权限。

为主机资源添加标签

步骤1 登录堡垒机。

步骤2 选择“资源 > 主机管理”，进入主机管理列表页面。

步骤3 勾选需要添加标签主机资源，单击列表下方的“添加标签”，弹出“添加标签”窗口。

步骤4 输入自定义标签内容，确认无误，单击“确定”，完成标签添加，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5 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

为应用资源添加标签

步骤1 登录堡垒机。

步骤2 选择“资源 > 应用发布”，进入应用发布列表页面。

步骤3 勾选需要添加标签应用资源，单击列表下方的“添加标签”，弹出“添加标签”窗口。

步骤4 输入自定义标签内容，确认无误，单击“确定”，完成标签添加，返回应用资源管理页面，可查看该应用资源的标签。

----结束

为容器资源添加标签

步骤1 登录堡垒机。

步骤2 选择“资源 > 云服务管理”，进入云服务器列表页面。

步骤3 勾选需要添加标签容器资源，单击列表下方的“添加标签”，弹出“添加标签”窗口。

步骤4 输入自定义标签内容，确认无误，单击“确定”，完成标签添加，返回容器资源管理页面，可查看该容器资源的标签。

----结束

7.5.3 删除资源标签

本章节指导您如何删除资源标签。

约束限制

- “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。

前提条件

已获取“主机管理”、“应用发布”、“主机运维”或“应用运维”功能模块权限。

删除主机资源标签

已添加标签的资源，可对标签进行删除操作。

步骤1 登录堡垒机。

步骤2 选择“资源 > 主机管理”，进入主机管理列表页面。

步骤3 勾选需要删除标签的主机资源，单击列表下方的“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

主机或应用资源标签的单个删除，还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

删除应用资源标签

步骤1 登录堡垒机。

步骤2 选择“资源 > 应用发布”，进入应用发布列表页面。

步骤3 勾选需要删除标签的应用资源，单击列表下方的“删除标签”。

步骤4 在弹窗中确认删除信息，确认无误，单击“确定”，完成删除。

----结束

删除容器资源标签

步骤1 登录堡垒机。

步骤2 选择“资源 > 云服务管理”，进入云服务器列表页面。

步骤3 勾选需要删除标签的容器资源，单击列表下方的“删除标签”。

步骤4 在弹窗中确认删除信息，确认无误，单击“确定”，完成删除。

----结束

7.6 资源系统类型管理

堡垒机能管理资源系统类型，并可自定义系统类型。

系统类型作为标签标识对应服务器，同时用于服务器改密，存放改密参数，执行改密策略时，会按照资源的同一系统类型执行脚本。

默认支持14种系统类型，包括Linux、Windows、Cisco、Huawei、H3C、DPtech、Ruijie、Sugon、Digital China sm-s-g 10-600、Digital China sm-d-d 10-600、ZTE、ZTE5950-52tm、Surfilter、ChangAn。

约束限制

- 仅系统管理员**admin**用户可修改系统类型配置。
- 默认系统类型不可删除和修改，仅可删除和修改自定义系统类型。

自定义系统类型

步骤1 登录堡垒机系统。

步骤2 选择“资源 > 系统类型”，进入系统类型列表页面。

步骤3 单击“新建”，弹出“新建系统类型”窗口，配置系统类型参数。

表 7-13 新建系统类型参数说明

参数	说明
系统类型	自定义系统类型名称。
改密参数	修改账户密码的执行命令和成功返回值。最多添加16条。 ● password表示旧密码； ● new_password表示新密码； ● change_user表示需要改密的资源账户； ● 不支持的字符（）。
提权账户改密参数	获取账户修改密码权限的执行命令和成功返回值。最多添加16条。 ● password表示旧密码； ● new_password表示新密码； ● 不支持的字符（）。
描述	系统类型简要介绍。

步骤4 单击“确定”，返回系统类型列表查看新建系统类型。

步骤5 管理自定义系统类型。

----结束

其他管理操作

步骤1 登录堡垒机系统。

步骤2 选择“资源 > 系统类型”，进入系统类型列表页面。

步骤3 删除自定义资源系统类型。

- 单击指定系统类型“操作”列的“删除”，可删除该系统类型。
- 同时勾选多个系统类型，单击列表下方的“删除”，可以批量删除多个系统类型。

步骤4 查看和修改自定义系统类型配置。

1. 单击系统类型名称，或者单击“管理”，进入“系统类型详情”界面。

2. 在“基本信息”区域，单击“编辑”，可修改系统类型参数信息。

----结束

8 策略管理

8.1 策略概述

堡垒机实例提供了控制策略的功能，可在堡垒机实例中提前配置部分策略，实现快速运维。

堡垒机支持访问控制、命令控制、数据库控制、改密和账户同步策略的预设。

表 8-1 堡垒机支持预设的策略说明

支持预设的策略类型	策略说明
访问控制策略	访问控制策略用于控制用户访问资源的权限。
命令控制策略	命令控制策略用于控制用户访问资源的关键操作权限，实现Linux主机运维操作的细粒度控制。
数据库控制策略	数据库控制策略是用于拦截数据库会话敏感操作，实现数据库运维操作的细粒度控制。授权用户登录策略关联的数据库资源，当数据库运维会话触发规则，将会拦截数据库会话操作。
改密策略	改密策略用于对主机资源账户自动改密，并可针对多个主机资源账户同时定期改密，提高资源账户安全性。 改密策略支持以下功能项： ● 支持通过策略手动、定时、周期修改资源账户密码。 ● 支持生成不同密码、相同密码，以及生成自定义相同密码。
账户同步策略	账户同步策略用于对主机资源账户自动同步，管理主机上资源账户，及时发现僵尸账户或未纳管账户，加强对资源的管控。

8.2 访问控制策略

8.2.1 新建访问控制策略并关联用户和资源账户

访问控制策略用于控制用户访问资源的权限。

访问控制策略支持以下功能项：

- 支持策略的批量导入和导出。
- 支持按策略列表页策略排序区分优先级，排序越靠前优先级越高。
- 策略基本限制和授权功能，包括使用有效期、登录时段限制、用户IP限制、文件传输权限、文件管理权限、RDP剪切板功能、键盘审计、运维水印显示功能等维度。同时可通过关联用户组或账户组，批量授权访问控制权限。
  - 有效期：指该策略的使用有效期，仅在限定时间内有效。
  - 登录时段限制：指该策略的限定使用时间范围。
  - IP限制：指该策略允许或禁止指定来源IP地址的用户访问资源，可选择白名单或黑名单进行配置。
    - 白名单：该策略只允许已填写的IP地址访问资源。
    - 黑名单：该策略不允许已填写的IP地址访问资源。
  - 文件传输：指该策略允许或禁止使用文件传输，即上传或下载资源文件的权限。
  - 文件管理：指该策略允许或禁止使用文件管理，即查看、删除、编辑文件的权限。
  - RDP剪切板：指该策略允许或禁止使用RDP剪切板功能，即复制/粘贴文本的权限。
  - 键盘审计：指该策略允许或禁止使用键盘审计功能，针对键盘输入的信息进行记录。
  - 显示水印：指该策略开启或关闭Web运维背景水印显示，水印显示内容为执行运维的用户登录名。

约束限制

- 授权文件上传/下载权限，需同时开启“文件传输”和“文件管理”。
- 键盘审计仅支持RDP和VNC协议。

前提条件

已获取“访问控制策略”模块操作权限。

访问控制策略说明

不同运维方式或不同的资源类型在执行部分运维操作时目前还存在不支持的情况。

Linux应用运维从3.3.40.0版本开始支持文件上传、下载，上、下行剪切板功能。

特性名称	有效期	文件传输	更多选项	登录时段限制	IP限制	双人授权候选人

	生效时间/失效时间	上传/下载	文件管理	上行剪切板/下行剪切板	显示水印	允许登录	禁止登录	黑名单	白名单	
SSH-H5运维	√	√	√	√	√	√	√	√	√	√
SSH-客户端运维	√	×	×	×	×	√	√	√	√	×
RDP-H5运维	√	√	√	√	√	√	√	√	√	√
RDP-客户端运维	√	×	×	×	×	√	√	√	√	×
TELNET-H5运维	√	√	√	√	√	√	√	√	√	√
TELNET-客户端运维	√	×	×	×	×	√	√	√	√	×
VNC	√	×	×	×	√	√	√	√	√	√
FTP	√	√	√	×	×	√	√	√	√	√
SFTP	√	√	√	×	×	√	√	√	√	√
SCP	√	×	×	×	×	√	√	√	√	√
Postgresql	√	×	×	×	×	√	√	√	√	√
Gaussdb	√	×	×	×	×	√	√	√	√	√
DB2	√	×	×	×	×	√	√	√	√	√
MYSQL	√	×	×	×	×	√	√	√	√	√
SQL Server	√	×	×	×	×	√	√	√	√	√
Oracle	√	×	×	×	×	√	√	√	√	√

Rlogin-H5运维	√	√	√	√	√	√	√	√	√	√
Rlogin-客户端运维	√	×	×	×	×	√	√	√	√	×
Windows应用运维	√	√	√	√	√	√	√	√	√	√
Linux应用运维	√	√	√	√	√	√	√	√	√	√

创建访问控制策略

步骤1 登录堡垒机系统。

步骤2 选择“策略 > 访问控制策略”，进入策略列表页面。

步骤3 单击“新建”，弹出策略基本属性配置窗口。

说明

选择一个策略，单击“更多 > 插入”，亦可新建访问控制策略。配置完成后，在已创建的策略前新建一个策略。

步骤4 配置策略基本信息。

表 8-2 访问控制策略基本信息参数说明

参数	说明
策略名称	自定义的访问控制策略名称，系统内“策略名称”不能重复。
有效期	选择策略生效时间和策略的失效时间。
文件传输	在运维过程中上传和下载文件权限，如果勾选了“上传”或“下载”，在“更多选项”需勾选“文件管理”才会生效。 ● 勾选代表允许对文件上传或下载。 ● 不勾选代表禁止对文件上传或下载。

参数	说明
更多选项	在运维过程中，会话窗口功能选项。此处勾选功能项后，对应关联资源的更多选项也需勾选相同功能项，对应功能才会生效。 ● 文件管理：管理文件或文件夹的权限，即查看、删除、编辑文件和文件夹的权限。 **说明** – SSH和RDP协议主机支持文件管理。 – VNC协议主机不能直接文件管理，但可通过应用发布方式实现文件管理。 – Telnet协议主机不支持文件管理。 ● 上行剪切板：运维会话RDP剪切板的功能，复制文本的权限。 ● 下行剪切板：运维会话RDP剪切板的功能，粘贴文本的权限。 ● 显示水印：运维会话窗口显示用户登录名水印。 ● 键盘审计：对键盘输入的信息进行记录。
登录时段限制	选择登录资源的时间段权限。
IP限制	限制/允许用户“来源IP”访问资源。 ● 选择“黑名单”，配置相应IP或IP网段，即限制该IP或IP网段用户登录资源。 ● 选择“白名单”，配置相应IP或IP网段，即仅允许该IP或IP网段用户登录资源。 ● IP地址缺省状态下，即不限制用户IP登录资源。

步骤5 单击“下一步”，关联用户或用户组。

- 可同时配置关联多个用户或用户组。
- 当用户组关联策略后，新用户加入到用户组中会自动继承用户组的策略权限。

步骤6 单击“下一步”，关联资源账户或账户组。

- 可同时配置关联多个资源账户或资源账户组。
- 当资源账户组关联策略后，新资源账户加入到账户组中会自动继承账户组的策略权限。

步骤7 单击“确定”，返回策略列表页面查看新建策略。

授权用户即可在“主机运维”或“应用运维”列表页面，查看和登录资源。

说明

“关联用户”和“关联用户组”中用户需拥有资源运维的权限，即“角色”已配置**主机运维**或**应用运维**。否则用户登录系统后无法查看资源运维模块，不能进行运维登录操作。

----结束

批量导入访问控制策略

支持批量导入访问控制策略。

步骤1 单击右上角  下载批量导入模板，填写访问控制策略信息。

步骤2 单击弹窗中的“点击上传”，将填写好的访问控制策略表格进行上传。

如果需要覆盖已有策略，可勾选“覆盖已有策略”。

说明

格式只能上传xls/xlsx/csv文件。

步骤3 单击“确认”，完成上传。

----结束

批量导出访问控制策略

在列表右上角单击  ，可一键导出当前列表所有数据。

后续管理

访问控制策略创建完成后，可在策略列表页面，管理已创建策略，包括管理关联用户或资源、删除策略、启停策略、策略排序等。

- 若需补充关联用户或资源，可单击“关联”，快速关联用户、用户组、资源账户、账户组。
- 若需删除策略，可选择目标策略，单击“删除”，立即删除策略。
- 若需禁用策略授权，可勾选一个或多个“已启用”状态的策略，单击“禁用”，策略状态变更为“已禁用”，策略授权立即失效。
- 若需排序策略优先等级，可选中策略行上下拖动策略，改变策略排序。

8.2.2 设置双人授权

双人授权即金库授权模式。配置双人授权后，运维人员若需访问核心资源，要求管理员现场授权认证，通过认证后才能访问核心资源。即使运维人员账号丢失，也不会泄露核心资源信息，降低运维风险，保障核心资产安全。

约束限制

授权候选人仅可选择本部门及上级部门的部门管理员，包括系统管理员**admin**。

前提条件

- 已获取“访问控制策略”模块操作权限。
- 已创建访问控制策略，并已关联用户和资源账户。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“策略 > 访问控制策略”，进入访问控制策略列表页面。

步骤3 选择目标策略，在“操作”列单击“更多 > 双人授权候选人”，弹出授权候选人名单窗口。

步骤4 选择一个或多个部门管理员，设为双人授权候选人。

步骤5 单击“确认”，双人授权候选人设置完成。

----结束

后续管理

双人授权配置成功后，该策略授权用户再次登录资源时，则会弹出双人授权确认窗口。

需选择一位授权人，并输入授权人账号密码。验证通过后，才能登录资源。

8.2.3 查询和修改访问控制策略

若运维人员有变动，或授权资源权限有变化，可查看和修改已创建的策略配置，包括修改基本权限、修改关联用户或用户组、修改关联资源账户或账户组、修改双人授权配置等。

- 修改策略配置，且策略状态为“已启用”时，策略规则才生效。
- 修改策略配置后，若关联用户已登录资源，需退出登录重新连接，相关策略规则在下一次运维操作时才会生效。

前提条件

已获取“访问控制策略”模块操作权限。

查看和修改策略配置

步骤1 登录堡垒机系统。

步骤2 选择“策略 > 访问控制策略”，进入访问控制策略列表页面。

步骤3 查询访问控制策略。

- 快速查询

  在搜索框中输入关键字，根据策略名称、用户、资源名称、主机地址、资源账户、时间限制、IP限制等快速查询策略。

- 高级搜索

  在相应属性搜索框中分别输入关键字，精确查询策略。

步骤4 单击目标策略名称，或者单击“管理”，进入策略详情页面。

步骤5 查看和修改策略基本信息。

在“基本信息”区域，单击“编辑”，弹出基本信息编辑窗口，即可修改策略的基本信息。

可修改信息包括“策略名称”、“有效期”、“文件传输”、“更多选项”、“登录时段限制”和“IP限制”等。

步骤6 查看和修改策略关联的用户。

- 在“用户”区域，单击“编辑”，弹出关联用户窗口，可立即添加或移除关联的用户。
- 在相应用户行，单击“移除”，可立即删除该关联用户，取消授权。

步骤7 查看和修改策略关联的用户组。

- 在“用户组”区域，单击“编辑”，弹出关联用户组窗口，可立即添加或移除关联的用户组。
- 在相应用户组行，单击“移除”，可立即删除该关联用户组，取消授权。

步骤8 查看和修改策略关联的资源账户。

- 在“资源账户”区域，单击“编辑”，弹出关联资源账户窗口，可立即添加或移除关联的资源账户。
- 在相应资源账户行，单击“移除”，可立即删除该资源账户，取消授权。

步骤9 查看和修改策略关联的账户组。

- 在“账户组”区域，单击“编辑”，弹出关联账户组窗口，可立即添加或移除关联的账户组。
- 在相应账户组行，单击“移除”，可立即删除该账户组，取消授权。

步骤10 查看和修改双人授权。

- 在“双人授权候选人”区域，单击“编辑”，弹出多人授权候选人窗口，可立即添加或移除关联的授权候选人。
- 在相应候选人行，单击“移除”，可立即删除该授权候选人，取消该候选人。

----结束

导出访问控制策略

步骤1 登录堡垒机系统。

步骤2 选择“策略 > 访问控制策略”，进入访问控制策略列表页面，勾选需要导出的策略。

若不勾选，默认导出全部策略。

步骤3 右上角单击  ，任务创建成功，单击“去下载中心”查看打包进度为100%时，单击“操作”列的“下载”，下载文件到本地，打开本地文件，即可查看导出的访问控制策略信息。

----结束

8.3 命令控制策略

8.3.1 新建命令控制策略

命令控制策略用于控制用户访问资源的关键操作权限，实现Linux主机运维操作的细粒度控制。

针对SSH和Telnet字符协议主机，根据管理员配置的策略限制，Guacd代理对用户运维过程中执行的命令进行审计和过滤，并返回审计的命令、过滤结果和命令返回的内容，用于会话操作记录、动态授权、断开连接等动作。

命令控制策略支持以下功能项：

- 支持按策略列表页策略排序区分优先级，排序越靠前优先级越高。

- 支持控制允许执行、拒绝执行、断开连接、动态授权四种命令动作。
  - 允许执行：触发该策略规则后，放行命令操作。默认允许执行所有操作。
  - 拒绝执行：触发该策略规则后，拒绝执行该命令，界面提示“命令“xxx”已被拦截”。
  - 断开连接：触发该策略规则后，拒绝执行该命令，断开会话连接，界面提示“本次连接已被管理员强制断开！”
  - 动态授权：触发该策略规则后，拒绝执行该命令，界面提示“命令“xxx”已被拦截，请提交命令授权工单申请动态授权”，同时生成命令授权工单。用户需提交工单，并审核通过后，才能继续执行该命令。

约束限制

仅SSH和Telnet协议类型的Linux主机，支持命令控制策略设置操作细粒度控制。

前提条件

已获取“命令控制策略”模块操作权限。

新建命令控制策略

步骤1 登录堡垒机系统。

步骤2 选择“策略 > 命令控制策略 > 策略列表”，进入命令控制策略列表页面。

步骤3 单击“新建”，弹出新建策略窗口。

说明

选择一个策略，单击“更多 > 插入”，亦可新建命令控制策略。配置完成后，在已创建的策略前新建一个策略。

步骤4 配置策略基本信息。

表 8-3 策略基本信息参数说明

参数	说明
策略名称	自定义的命令控制策略名称，系统内“策略名称”不能重复。
执行动作	选择策略控制用户的执行动作。 包括“断开连接”、“拒绝执行”、“动态授权”、“允许执行”。 ● 断开连接：当会话执行策略生效的命令时，直接断开会话。 ● 拒绝执行：当会话执行策略生效的命令时，直接拒绝命令的执行。 ● 动态授权：当会话执行策略生效的命令时，直接拒绝命令的执行，需要向管理员提交审批，管理员通过之后才能执行。 ● 允许执行：当会话执行策略生效的命令时，允许执行。
有效期	策略生效时间和策略的失效时间。
时段限制	限制策略的生效时间段。

步骤5 单击“下一步”，关联命令或命令集。

- 关联命令：可设置多个命令，每行输入一条命令。详细设置说明请参见**自定义关联命令**。
- 关联命令集：关联已创建的命令集。详细命令集说明请参见**管理命令集**。

步骤6 单击“下一步”，关联用户或用户组。

- 当用户组关联策略后，新用户加入到用户组中会自动继承用户组的策略权限。

步骤7 关联资源账户或账户组，选择已创建资源账户或账户组。

- 当账户组关联策略后，新账户加入到账户组中会自动赋予账户组的策略权限。

步骤8 单击“确定”，返回策略列表页面，查看新建的命令控制策略。

用户在运维过程中，触发策略规则，即会被限制相关操作。

说明

“关联用户”和“关联用户组”中用户需提交命令授权工单权限，即已配置拥有**命令授权工单**权限的“角色”。否则用户登录系统后无法查看命令授权工单模块，不能提交工单获取权限。

----结束

后续管理

命令控制策略创建完成后，可在策略列表页面，管理已创建策略，包括管理关联用户或资源、删除策略、启停策略、策略排序等。

- 若需补充关联用户或资源，可单击“关联”，快速关联用户、用户组、资源账户、账户组。
- 若需删除策略，可选择目标策略，单击“删除”，立即删除策略。
- 若需禁用策略授权，可勾选一个或多个“已启用”状态的策略，单击“禁用”，策略状态变更为“已禁用”，策略授权立即失效。
- 若需排序策略优先等级，可选中策略行上下拖动策略，改变策略排序。

8.3.2 查询和修改命令控制策略

若命令控制策略有变更，例如运维人员有变动，授权资源权限有变化等。可查看和修改已创建的策略配置，包括修改策略基本信息、修改关联密码或命令集。修改关联用户或用户组、修改关联资源账户或账户组等。

- 修改策略配置，且策略状态为“已启用”时，策略规则才生效。
- 修改策略配置后，若关联用户已登录资源，需退出登录重新连接，相关策略规则在下一次运维操作时才会生效。

前提条件

已获取“命令控制策略”模块操作权限。

查看和修改策略配置

步骤1 登录堡垒机系统。

步骤2 选择“策略 > 命令控制策略”，进入命令控制策略列表页面。

步骤3 查询命令控制策略。

- 快速查询

  在搜索框中输入关键字，根据策略名称、用户、资源名称、主机地址、资源账户、命令集、命令/参数等快速查询策略。

- 高级搜索

  在相应属性搜索框中分别输入关键字，精确查询策略。

步骤4 单击目标策略名称，或者单击“管理”，进入策略详情页面。

步骤5 查看和修改策略基本信息。

在“基本信息”区域，单击“编辑”，弹出基本信息编辑窗口，即可修改策略的基本信息。

可修改信息包括“策略名称”、“有效期”、“执行动作”、“时间限制”等。

步骤6 查看和修改策略关联的命令。

- 在“命令”区域，单击“编辑”，弹出关联命令窗口，可立即修改命令参数。
- 单击“移除”，可立即删除该关联命令。

步骤7 查看和修改策略关联的命令集。

- 在“命令集”区域，单击“编辑”，弹出关联命令集窗口，可立即添加或移除关联的命令集。
- 在相应命令集行，单击“移除”，可立即删除该关联命令集。

步骤8 查看和修改策略关联的用户。

- 在“用户”区域，单击“编辑”，弹出关联用户窗口，可立即添加或移除关联的用户。
- 在相应用户行，单击“移除”，可立即删除该关联用户，取消授权。

步骤9 查看和修改策略关联的用户组。

- 在“用户组”区域，单击“编辑”，弹出关联用户组窗口，可立即添加或移除关联的用户组。
- 在相应用户组行，单击“移除”，可立即删除该关联用户组，取消授权。

步骤10 查看和修改策略关联的资源账户。

- 在“资源账户”区域，单击“编辑”，弹出关联资源账户窗口，可立即添加或移除关联的资源账户。
- 在相应资源账户行，单击“移除”，可立即删除该资源账户，取消授权。

步骤11 查看和修改策略关联的账户组。

- 在“账户组”区域，单击“编辑”，弹出关联账户组窗口，可立即添加或移除关联的账户组。
- 在相应账户组行，单击“移除”，可立即删除该账户组，取消授权。

----结束

8.3.3 管理命令集

为简化添加大量命令的繁琐操作，可查询并添加常见命令参数，包括Linux主机和网络设备常见命令参数。

本小节主要介绍如何新建关联命令集、查看命令集、修改命令集、删除命令集、批量导入命令集。

前提条件

已获取“命令控制策略”模块操作权限。

新建命令集

步骤1 登录堡垒机系统。

步骤2 选择“策略 > 命令控制策略 > 命令集”，进入命令集列表页面。

步骤3 创建命令集。

1. 单击“新建”，弹出新建命令集窗口。
2. 配置命令集名称。

   系统内“命令集名称”不能重复
3. 单击“确定”，返回规则集列表页面，查看新建的命令集。

步骤4 添加命令集规则。

1. 在目标命令集行，单击“操作”列的“添加命令”，弹出添加命令窗口。
2. 选择命令集合或者单条命令。
3. 单击“确定”，命令添加完成。

----结束

查询和修改命令集

步骤1 登录堡垒机系统。

步骤2 选择“策略 > 命令控制策略 > 命令集”，进入命令集列表页面。

步骤3 查询命令集。

快速查询：在搜索框中输入关键字，根据命令集名称、命令/参数等快速查询策略。

步骤4 单击命令集名称，或者单击“管理”，进入命令集详情页面。

步骤5 查看和修改命令集基本信息。

在“基本信息”区域，单击“编辑”，弹出基本信息编辑窗口，即可修改命令集的基本信息。

可修改信息包括“命令集名称”，“部门”不可修改。

步骤6 查看和修改命令参数。

- 在“命令”区域，单击“添加”，弹出添加命令窗口，可立即添加预置的命令参数。
- 单击“移除”，可立即删除该命令参数。

----结束

删除命令集

步骤1 登录堡垒机系统。

步骤2 选择“策略 > 命令控制策略 > 命令集”，进入命令集列表页面。

步骤3 单击指定命令集“操作”列的“删除”，可删除该命令集。

步骤4 同时勾选多个命令集，单击列表下方的“删除”，可以批量删除多个命令集。

----结束

批量导入命令集

步骤1 登录堡垒机系统。

步骤2 选择“策略 > 命令控制策略 > 命令集”，进入命令集列表页面。

步骤3 单击右上角  ，在弹窗中下载模板。

步骤4 下载后按照模板填写完成单击“点击上传”，将填写的命令集信息导入到堡垒机。

在更多选项可选择是否覆盖已有的命令集。

说明

只能上传xls/xlsx/csv文件。

步骤5 确认无误，单击“确定”，导入完成。

----结束

8.3.4 自定义关联命令

命令控制策略关联的自定义的命令，关联命令后，在执行相关命令或参数时，触发拦截和允许操作。

自定义关联命令大小写敏感，严格按照设置的关联命令进行审核和过滤，若执行命令与设置命令不一致，则不能触发策略规则。详细设置说明和示例，请参考如下说明：

- 支持单命令格式。

  如设置拒绝执行查询命令，即设置关联命令为**ls**，执行单命令操作时触发策略规则。

- 支持命令路径格式。

  如设置动态授权查询日志，即设置关联命令为**ls /var/log/**，执行命令参数操作时触发策略规则。此时若执行**ls /var/log**，则无法触发策略拦截规则。

- 支持命令带“*”通配符，“*”表示任意多个字符。

  如设置拒绝执行所有删除命令，即设置关联命令为**rm ***，执行命令加任意参数触发策略拦截，如执行**rm -rf**。此时若执行**rm**命令本身，则不会触发策略拦截规则。

- 支持命令带“?”通配符，“?”表示任意单个字符，输入几个“?”就代表几个未知字符。

  如设置拒绝执行删除两个字符名称的文件或目录，即设置关联命令为**rm -rf ??**，执行命令加任意两个字符触发策略拦截，如执行**rm -rf ts**。此时若执行**rm -rf test**，则不会触发策略拦截规则。

- 支持命令带“[]”通配符，“[]”表示框内的任意字符、范围、取反（使用“|”或“^”取反）。

  如设置动态授权删除带abcd名称的文件或目录，即设置关联命令为**rm -rf [abcd]**，执行命令加任意abcd字符触发策略拦截，如执行**rm -rf cloud**。此时若执行**rm -rf test**或**rm -rf ABCD**，则不会触发策略拦截规则。

8.4 数据库控制策略

8.4.1 新建数据库控制策略

数据库控制策略是用于拦截数据库会话敏感操作，实现数据库运维操作的细粒度控制。授权用户登录策略关联的数据库资源，当数据库运维会话触发规则，将会拦截数据库会话操作。

数据库控制策略支持以下功能项：

- 支持按策略列表页策略排序区分优先级，排序越靠前优先级越高。
- 支持控制允许执行、拒绝执行、断开连接、动态授权四种命令动作。
  - 允许执行：默认允许执行所有操作。当触发策略规则后，放行规则集中操作。
  - 拒绝执行：触发该策略规则后，拒绝执行该操作，界面提示“操作“xxx”已被拦截”。
  - 断开连接：触发该策略规则后，拒绝执行该操作，断开会话连接，界面提示“本次连接已被管理员强制断开！”。
  - 动态授权：触发该策略规则后，拒绝执行该操作，界面提示“操作“xxx”已被拦截，请提交数据库授权工单申请动态授权”，同时生成数据库授权工单。用户需提交工单，并审核通过后，才能继续执行该命令。

约束限制

仅针对MySQL、Oracle、Postgresql、Gaussdb类型数据库，支持通过数据库控制策略设置操作细粒度控制。

前提条件

已获取“数据库控制策略”模块操作权限。

新建数据库控制策略

步骤1 登录堡垒机系统。

步骤2 选择“策略 > 数据库控制策略 >策略列表”，进入策略列表页面。

步骤3 单击“新建”，弹出策略基本信息配置窗口。

说明

选择一个策略，单击“更多 > 插入”，亦可新建数据库控制策略。配置完成后，在已创建的策略前新建一个策略。

步骤4 配置策略基本信息。

表 8-4 策略基本信息参数说明

参数	说明
策略名称	自定义的数据库控制策略名称，系统内“策略名称”不能重复。
执行动作	策略控制用户在数据库的执行动作。 包括“断开连接”、“拒绝执行”、“动态授权”、“允许执行”。 • 断开连接：当数据库运维会话执行策略生效的命令时，直接断开会话。 • 拒绝执行：当数据库运维会话执行策略生效的命令时，直接拒绝命令的执行。 • 动态授权：当数据库运维会话执行策略生效的命令时，直接拒绝命令的执行，需要向管理员提交审批，管理员通过之后才能执行。 • 允许执行：当数据库运维会话执行策略生效的命令时，允许执行。
有效期	策略生效时间和策略的失效时间。
时间限制	限制策略的生效时间段。

步骤5 单击“下一步”，关联规则集。

选择规则集。详细规则集说明请参见**管理规则集**。

步骤6 单击“下一步”，关联用户或用户组，选择用户或用户组。

当用户组关联策略后，新用户加入到用户组中会自动继承用户组的策略权限。

步骤7 单击“下一步”，关联资源账户或账户组，选择数据库资源账户或账户组。

当账户组关联策略后，新账户加入到账户组中会自动继承账户组的策略权限。

步骤8 单击“确定”，返回策略列表页面，查看新建的数据库控制策略。

用户在运维过程中，触发策略规则，即会被限制相关操作。

说明

“关联用户”和“关联用户组”中用户需提交数据库授权工单权限，即已配置拥有**数据库授权工单**权限的“角色”。否则用户登录系统后无法查看数据库授权工单模块，不能提交工单获取权限。

----结束

后续管理

数据库控制策略创建完成后，可在策略列表页面，管理已创建策略，包括管理关联用户或资源、删除策略、启停策略、策略排序等。

- 若需补充关联用户或资源，可单击“关联”，快速关联用户、用户组、资源账户、账户组。
- 若需删除策略，可选择目标策略，单击“删除”，立即删除策略。
- 若需禁用策略授权，可勾选一个或多个“已启用”状态的策略，单击“禁用”，策略状态变更为“已禁用”，策略授权立即失效。

- 若需排序策略优先等级，可选中策略行上下拖动策略，改变策略排序。

8.4.2 查询和修改数据库控制策略

若数据库控制策略有变更，例如运维人员有变动，授权资源权限有变化等。可查看和修改已创建的策略配置，包括修改策略基本信息、修改关联规则集、修改关联用户或用户组、修改关联资源账户或账户组等。

- 修改策略配置，且策略状态为“已启用”时，策略规则才生效。
- 修改策略配置后，若关联用户已登录资源，需退出登录重新连接，相关策略规则在下一次运维操作时才会生效。

前提条件

已获取“数据库控制策略”模块操作权限。

查看和修改策略配置

步骤1 登录堡垒机系统。

步骤2 选择“策略 > 数据库控制策略”，进入数据库控制策略列表页面。

步骤3 查询数据库控制策略。

- 快速查询

  在搜索框中输入关键字，根据策略名称、用户、资源名称、主机地址、资源账户、规则集名称等快速查询策略。

- 高级搜索

  在相应属性搜索框中分别输入关键字，精确查询策略。

步骤4 单击目标策略名称，或者单击“管理”，进入策略详情页面。

步骤5 查看和修改策略基本信息。

在“基本信息”区域，单击“编辑”，弹出基本信息编辑窗口，即可修改策略的基本信息。

可修改信息包括“策略名称”、“有效期”、“执行动作”、“时间限制”等。

步骤6 查看和修改策略关联的规则集。

- 在“规则集”区域，单击“编辑”，弹出关联规则集窗口，可立即添加或移除关联的规则集。
- 在相应规则集行，单击“移除”，可立即删除该关联规则集。

步骤7 查看和修改策略关联的用户。

- 在“用户”区域，单击“编辑”，弹出关联用户窗口，可立即添加或移除关联的用户。
- 在相应用户行，单击“移除”，可立即删除该关联用户，取消授权。

步骤8 查看和修改策略关联的用户组。

- 在“用户组”区域，单击“编辑”，弹出关联用户组窗口，可立即添加或移除关联的用户组。
- 在相应用户组行，单击“移除”，可立即删除该关联用户组，取消授权。

步骤9 查看和修改策略关联的资源账户。

- 在“资源账户”区域，单击“编辑”，弹出关联资源账户窗口，可立即添加或移除关联的资源账户。
- 在相应资源账户行，单击“移除”，可立即删除该资源账户，取消授权。

步骤10 查看和修改策略关联的账户组。

- 在“账户组”区域，单击“编辑”，弹出关联账户组窗口，可立即添加或移除关联的账户组。
- 在相应账户组行，单击“移除”，可立即删除该账户组，取消授权。

----结束

8.4.3 管理规则集

为简化添加大量数据库规则的繁琐操作，可通过创建规则集并添加规则。

堡垒机预置29种常见数据库操作命令，包括ALTER、TRUNCATE、EXECUTE、INSERT、DELETE、UPDATE、SELECT、GRANT、REVOKE、HANDLER、DEALLOCATE、SET、COMMIT、ROLLBACK、PREPARE、CREATEINDEX、DROPINDEX、CREATEFUNCTION、DROPFUNCTION、CREATEVIEW、DROPVIEW、CREATEDATABASE、DROPDATABASE、CREATEPROCEDURE、DROPPROCEDURE、CREATETABLE、DROPTABLE、CALL、ACCESS。

本小节主要介绍如何新建关联规则集、查看规则集、修改规则集、删除复制集。

前提条件

已获取“数据库控制策略”模块操作权限。

新建规则集

步骤1 登录堡垒机系统。

步骤2 选择“策略 > 数据库控制策略 > 规则集”，进入规则集列表页面。

步骤3 创建规则集。

1. 单击“新建”，弹出规则集基本信息配置窗口。
2. 配置规则集名称和选择协议。
   - 系统内“规则集名称”不能重复。
   - 目前支持选择MySQL、Oracle、Postgresql、Gaussdb、DM数据库协议类型，且选定后不可修改。
3. 单击“确定”，返回规则集列表页面，查看新建的规则集。

步骤4 添加规则。

1. 在目标规则集行，单击“操作”列的“添加规则”，弹出添加规则窗口。
2. 添加规则集的库、表和命令规则。

表 8-5 添加规则参数说明

参数	说明
库	可选项，支持正则表达式匹配库名。 缺省状态下表示将会拦截所有使用该命令的sql语句。
表	可选项，支持正则表达式匹配表名。 缺省状态下表示将会拦截所有使用该命令的sql语句。
命令	必选项，必须选择一条预置命令。 目前支持选择29种命令，同时可选择多条命令。

3. 单击“确定”，规则添加完成。

----结束

查询和修改规则集

步骤1 登录堡垒机系统。

步骤2 选择“策略 > 数据库控制策略 > 规则集”，进入规则集列表页面。

步骤3 查询规则集。

快速查询：在搜索框中输入关键字，根据规则集名称快速查询策略。

步骤4 单击规则集名称，或者单击“管理”，进入规则集详情页面。

步骤5 查看和修改规则集基本信息。

在“基本信息”区域，单击“编辑”，弹出基本信息编辑窗口，即可修改规则集的基本信息。

可修改信息包括“规则集名称”，“协议”、“部门”不可修改。

步骤6 查看和修改规则。

- 在“规则”区域，单击“添加”，弹出添加规则窗口，可立即添加库、表、命令规则。
- 单击“移除”，可立即删除该规则。

----结束

删除规则集

步骤1 登录堡垒机系统。

步骤2 选择“策略 > 数据库控制策略 > 规则集”，进入规则集列表页面。

步骤3 单击指定规则集“操作”列的“删除”，可删除该规则集。

步骤4 同时勾选多个规则集，单击列表下方的“删除”，可以批量删除多个规则集。

----结束

8.5 改密策略

8.5.1 新建改密策略

改密策略用于对主机资源账户自动改密，并可针对多个主机资源账户同时定期改密，提高资源账户安全性。

改密策略支持以下功能项：

- 支持通过策略手动、定时、周期修改资源账户密码。
- 支持生成不同密码、相同密码，以及生成自定义相同密码。

约束限制

- 仅SSH，RDP和Telnet协议类型的主机，支持通过改密策略修改资源账户密码。
- Windows主机资源需启用SMB服务，并放开主机安全组445端口，才能通过改密策略修改资源账户密码。
- Windows 10不能使用SMB方式改密，关联Windows 10资源账户前，需配置winRM后进行改密策略的创建，可参照**配置Windows 10服务器相关参数**进行服务器相关参数的配置。

前提条件

- 已获取“改密策略”模块操作权限。
- 待改密资源的“系统类型”需与资源实际系统类型完全匹配。
- 创建改密策略绑定的资源账户的登录方式必须为自动登录或提权登录，否则创建策略时无法选中对应账户。

新建改密策略

步骤1 登录堡垒机系统。

步骤2 选择“策略 > 改密策略 > 策略列表”，进入改密策略列表页面。

步骤3 单击“新建”，弹出改密策略配置窗口。

步骤4 配置改密策略基本配置。

表 8-6 改密策略参数说明

参数	说明
策略名称	自定义的改密策略名称，系统内“策略名称”不能重复。

参数	说明
执行方式	选择改密执行方式，可选择“手动执行”、“定时执行”、“周期执行”。 ● 手动执行：手动触发改密策略，修改资源账户密码。 ● 定时执行：定期自动触发改密策略，修改资源账户密码。仅执行一次。 ● 周期执行：周期自动触发改密策略，修改资源账户密码。可按周期执行多次。
执行时间	执行改密策略的日期。默认执行时刻为日期的凌晨零点。
执行周期	执行周期改密，需输入改密的执行周期，输入后在“执行时间预览”可预览最近5次的执行时间。 **说明** ● 单位为天，当输入超过8位的正整数时，不支持执行时间预览。 ● 需同时选择“结束时间”，否则将无限期执行周期改密。
改密方式	选择改密方式。可选择“生成不同密码”、“生成相同密码”、“指定相同密码”。 ● 生成不同密码：根据主机对账户的密码要求，随机生成不同资源账户密码。 ● 生成相同密码：根据主机对账户的密码要求，随机生成相同资源账户密码。 ● 指定相同密码：需手动输入预置密码，请根据界面提示输入符合要求的密码。 **说明** 堡垒机随机生成的密码长度为20位，其中包含大小写字母数字和特殊字符“%”、“-”、“_”和“？”，大小写字符及特殊字符至少在随机密码中包含1位。
更多选项	支持以下几种方式： ● “允许修改特权账户密码”，表示可修改特权账户的密码，否则特权账户密码不能被修改。默认不选中。 ● “使用特权账户改密”，表示系统自动寻找资源账户对应的特权账户，通过特权账户修改资源账户密码。无特权账户时，资源账户自行修改密码。默认选中。 ● “允许修改SSH Key”，表示系统可以自动修改SSH的公钥。 **说明** ● 仅V3.3.36.0及以上版本才支持“允许修改SSH Key”。 ● 如果在纳管主机资源时选择了密钥对自动登录方式，必须勾选“允许修改SSH key”选项，否则手动执行改密可能会失败。

步骤5 单击“下一步”，关联资源账户或账户组。

- 当账户组关联策略后，新资源账户加入到账户组中会自动继承账户组的策略权限。
- 关联多个资源账户时，可批量修改资源账户密码。

步骤6 单击“确定”，返回改密策略列表，查看新建的改密策略。

改密策略执行后，可以参考**批量导出主机资源**，获取新的资源账户密码。

步骤7 单击“操作”列的“立即执行”，在弹窗确认执行后，策略立即刷新。

----结束

配置 Windows 10 服务器相关参数

步骤1 登录Windows 10服务器。

步骤2 启动winRM服务。

1. 搜索“组件服务”，进入“组件服务”页面。
2. 在左侧导航树中，选择“服务（本地）”，在右侧弹框中，找到“Windows Remote Management(WS-Management)”。
3. 右键单击“Windows Remote Management(WS-Management)”，在弹窗中单击“启动”。

步骤3 配置winRM。

1. 以管理员身份运行cmd，执行以下命令：
   ```
   winrm qc
   ```
2. （执行两次）回显后，根据提示输入y。
3. 执行以下命令：
   ```
   winrm set winrm/config/service '@{AllowUnencrypted="true"}'
   ```
4. 执行以下命令：
   ```
   winrm set winrm/config/service/auth '@{Basic="true"}'
   ```

步骤4 （如果已是管理员，可不执行该步骤）执行以下命令，添加用户到用户组。

例如，用户名为“appuser01”。

```
net localgroup "Remote Management Users"  appuser01  /add
```

步骤5 在power shell会话框中执行以下命令，添加防火墙命令。

```
New-NetFirewallRule -DisplayName "WinRM-5985" -Direction Inbound -LocalPort 5985 -Protocol TCP -Action Allow
```

----结束

后续管理

改密策略创建完成后，可在策略列表页面，管理已创建策略，包括管理关联资源、删除策略、启停策略、立即执行策略等。

- 若需补充关联资源，可单击“关联”，快速关联资源账户、账户组。
- 若需删除策略，可选择目标策略，单击“删除”，立即删除策略。
- 若需禁用策略改密，可勾选一个或多个“已启用”状态的策略，单击“禁用”，策略状态变更为“已禁用”，策略立即失效。
- 若需立即修改资源账户密码，可单击“立即执行”，立即执行改密任务。

8.5.2 查询和修改改密策略

若改密策略有变更，例如改密方式有变化等。可查看和修改已创建的策略配置，包括修改策略基本信息、修改改密执行方式、修改改密日期、修改改密周期、修改关联资源账户或账户组等。

修改策略配置，且策略状态为“已启用”时，策略规则才生效。

前提条件

已获取“改密策略”模块操作权限。

查看和修改策略配置

步骤1 登录堡垒机系统。

步骤2 选择“策略 > 改密策略 > 策略列表”，进入改密策略列表页面。

步骤3 查询改密策略。

- 快速查询

  在搜索框中输入关键字，根据策略名称、资源名称、资源账户等快速查询策略。
- 高级搜索

  在相应属性搜索框中分别输入关键字，精确查询策略。

步骤4 单击目标策略名称，或者单击“管理”，进入策略详情页面。

步骤5 查看和修改策略基本信息。

在“基本信息”区域，单击“编辑”，弹出基本信息编辑窗口，即可修改策略的基本信息。

- 可修改信息包括“策略名称”、“执行方式”、“改密方式”、“更多选项”等。
- “部门”不可修改。

步骤6 查看和修改策略关联的资源账户。

- 在“资源账户”区域，单击“编辑”，弹出关联资源账户窗口，可立即添加或移除关联的资源账户。
- 在相应资源账户行，单击“移除”，可立即取消对该资源账户的改密。

步骤7 查看和修改策略关联的账户组。

- 在“账户组”区域，单击“编辑”，弹出关联账户组窗口，可立即添加或移除关联的账户组。
- 在相应账户组行，单击“移除”，可立即取消对该组中资源账户的改密。

----结束

8.5.3 管理改密日志

改密策略执行后产生的改密日志。改密日志中可查看改密详情。

前提条件

已获取“改密策略”模块操作权限。

查看日志详情

步骤1 登录堡垒机系统。

步骤2 选择“策略 > 改密策略 > 改密日志”，查看和管理改密日志记录。

步骤3 查询改密日志。

快速查询：在搜索框中输入关键字，根据策略名称快速查询改密日志。

步骤4 选择目标执行日志，单击“详情”，进入日志详情页面。

可查看日志内容包括基本信息、改密结果等信息。

图 8-1 查看改密日志详情

----结束

下载改密日志

步骤1 登录堡垒机系统。

步骤2 选择“策略 > 改密策略 > 改密日志”，查看和管理改密日志记录。

步骤3 单击“下载”，进入下载改密日志文件窗口。

步骤4 下载确认。

1. （可选）设置加密密码：可选择设置。不设置，下载的改密日志为未加密的CSV格式文件；设置密码，下载的改密日志为加密的ZIP格式文件。
2. （必选）用户密码：输入当前用户的账号登录密码，验证通过才允许下载改密日志，确保资源账户密码安全。
3. 单击“确定”，即可下载CSV格式文件或加密的ZIP格式文件保存到本地。

----结束

删除日志

步骤1 登录堡垒机系统。

步骤2 选择“策略 > 改密策略 > 改密日志”，进入改密日志列表页面。

步骤3 单击“删除”，可删除该执行日志。

步骤4 同时勾选多条执行日志，单击列表下方的“删除”，可以批量删除多个执行日志。

----结束

8.6 账户同步策略

8.6.1 新建账户同步策略

账户同步策略用于对主机资源账户自动同步，管理主机上资源账户，及时发现僵尸账户或未纳管账户，加强对资源的管控。

账户同步策略支持以下功能项：

- 支持通过策略手动、定时、周期同步主机上资源账户。
- 支持拉取目标主机上账户，判断账户的可用情况，并更新系统资源账户状态。
- 支持将系统资源账户信息同步到主机，更新主机上账户密码、新建主机账户、删除主机非法账户。

约束限制

- 仅**专业版**堡垒机支持执行账户自动同步。
- 仅SSH协议类型的主机，支持通过策略进行资源账户同步。
- 每个目标资源主机仅限一个资源账户登录并执行拉取账户任务。

前提条件

已获取“账户同步策略”模块操作权限。

新建账户同步策略

步骤1 登录堡垒机系统。

步骤2 选择“策略 > 账户同步策略 > 策略列表”，进入策略列表页面。

步骤3 单击“新建”，弹出新建账户同步策略窗口。

图 8-2 新建账户同步策略

步骤4 配置策略基本信息。

表 8-7 账户同步策略基本信息参数说明

参数	说明
策略名称	自定义的账户同步策略名称，系统内“策略名称”不能重复。
执行方式	选择账户同步执行方式，可选择“手动执行”、“定时执行”、“周期执行”。 “定时执行”和“周期执行”需同时配置动作执行时间或周期。 • 手动执行：手动触发策略，修改资源账户密码。 • 定时执行：定期自动触发策略，修改资源账户密码。仅执行一次。 • 周期执行：周期自动触发策略，修改资源账户密码。可按周期执行多次。
执行时间	定期执行策略的日期。默认执行时刻为日期的凌晨零点。

参数	说明
执行周期	执行周期同步，需输入同步周期。 ● 可选择每分钟、每小时、每天、每周、每月。 ● 需同时选择“结束时间”，否则将无限期执行周期改密。
同步动作	选择同步方式，默认选择“拉取账户”。 ● 拉取账户：扫描目标主机的所有账户，并统计所有正常、 异常账户信息。 ● 推送账户：将资源账户同步到目标主机，更新主机密码、 或新建主机账户、或删除主机非法账户。 **说明** 同步方式选择推送账户时可选下列三个选择功能 – 账密不一致时，允许更新该账户密码。 – 账户不存在于主机，允许创建该账户。 – 主机存在非纳管账户，允许删除该账户。
连接超时	自定义连接目标主机的超时时间，连接超时断开连接，中断账户同步任务。 默认为10秒。

步骤5 单击“下一步”，配置执行账户或账户组，选择已创建资源账户或账户组。

每个目标主机仅限配置一个账户执行同步任务。

步骤6 单击“确定”，返回策略列表页面，查看新建的同步账户策略。

账户同步策略执行后，可以**下载执行日志**，获取同步的资源账户信息。

----结束

后续管理

账户同步策略创建完成后，可在策略列表页面，管理已创建策略，包括管理关联资源、删除策略、启停策略、立即执行策略等。

- 若需补充关联资源，可单击“关联”，快速关联资源账户、账户组。
- 若需删除策略，可选择目标策略，单击“删除”，立即删除策略。
- 若需禁用策略同步账户，可勾选一个或多个“已启用”状态的策略，单击“禁用”，策略状态变更为“已禁用”，策略立即失效。
- 若需立即同步主机账户，可单击“立即执行”，立即执行账户同步任务。

8.6.2 查询和修改账户同步策略

若账户同步策略有变更，例如需同步方式变化等。可查看和修改已创建的策略配置，包括修改策略基本信息、修改同步方式、修改同步日期、修改同步周期、修改关联资源账户或账户组等。

修改策略配置，且策略状态为“已启用”时，策略规则才生效。

前提条件

已获取“账户同步策略”模块操作权限。

查看和修改策略配置

步骤1 登录堡垒机系统。

步骤2 选择“策略 > 账户同步策略 > 策略列表”，进入账户同步策略列表页面。

步骤3 查询账户同步策略。

- 快速查询
  在搜索框中输入关键字，根据策略名称、资源名称、执行账户等快速查询策略。
- 高级搜索
  在相应属性搜索框中分别输入关键字，精确查询策略。

步骤4 单击目标策略名称，或者单击“管理”，进入策略详情页面。

步骤5 查看和修改策略基本信息。

在“基本信息”区域，单击“编辑”，弹出基本信息编辑窗口，即可修改策略的基本信息。

- 可修改信息包括“策略名称”、“执行方式”、“同步动作”等。
- “部门”不可修改。

步骤6 查看和修改策略关联的资源账户。

- 在“执行账户”区域，单击“编辑”，弹出关联资源账户窗口，可立即添加或移除关联的资源账户。
- 在相应资源账户行，单击“移除”，可立即取消对该资源账户的同步。

步骤7 查看和修改策略关联的账户组。

- 在“执行账户组”区域，单击“编辑”，弹出关联账户组窗口，可立即添加或移除关联的账户组。
- 在相应账户组行，单击“移除”，可立即取消对该组中资源账户的同步。

----结束

8.6.3 管理执行日志

账户同步策略执行后产生的执行日志。执行日志中可查看账户同步结果，包括同步的账户信息、新建的账户信息、删除的账户信息等。

前提条件

已获取“账户同步策略”模块操作权限。

查看日志详情

步骤1 登录堡垒机系统。

步骤2 选择“策略 > 账户同步策略 > 执行日志”，查看和管理日志记录。

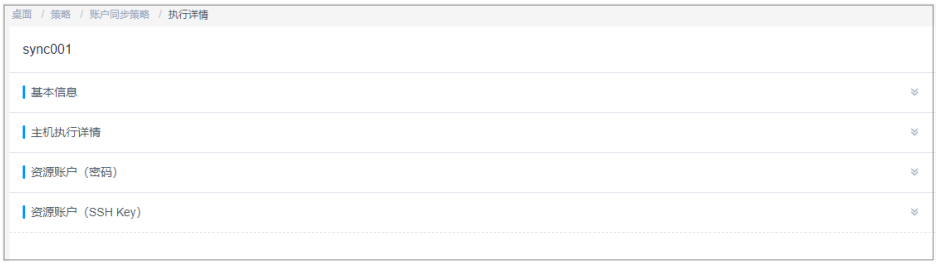
步骤3 查询执行日志。

快速查询：在搜索框中输入关键字，根据策略名称快速查询执行日志。

步骤4 单击目标执行日志，或者单击“详情”，进入日志详情页面。

可查看基本信息、主机执行详情结果、同步密码的资源账户列表、同步SSH Key的资源账户列表等信息。

图 8-3 查看日志基本信息



----结束

下载执行日志

步骤1 登录堡垒机系统。

步骤2 选择“策略 > 账户同步策略 >执行日志”，查看和管理执行日志记录。

步骤3 选择目标执行日志，单击“下载”，立即下载执行日志CSV格式文件保存到本地。

----结束

删除日志

步骤1 登录堡垒机系统。

步骤2 选择“策略 > 账户同步策略 > 执行日志”，进入日志列表页面。

步骤3 选择目标日志，单击“删除”，即可删除该执行日志。

步骤4 同时勾选多条执行日志，单击列表下方的“删除”，可以批量删除多个执行日志。

----结束

9 资源运维

9.1 主机资源运维

9.1.1 主机资源运维设置

运维用户获取主机资源访问操作权限后，即可在主机运维列表查看已授权资源，并可设置资源标签、运维方式。

运维方式包含H5页面、客户端、主从账号，不同协议支持的运维方式也不一样。

- H5页面运维：通过浏览器页面进行资源运维。
- 客户端运维：通过堡垒机自动启用安装的客户端进行资源的运维。
- 主从账号运维：通过堡垒机获取目标资源的账号密码，手动启动客户端进行登录后对资源实现运维。

约束限制

- 每个用户可自定义资源标签，资源标签仅能个人账号使用，不能与系统内用户共用。
- “登录配置下载”仅支持SSH运维的资源。

前提条件

- 已获取“主机运维”模块管理权限。
- 已获取资源访问控制权限，即已被关联访问控制策略或访问授权工单已审批通过。

查看主机资源列表

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。

快速查询：可选择自动识别、主机名称、主机地址后在搜索框进行搜索目标资源。

----结束

资源标签设置

通过给主机资源自定义标签可实现资源的分类，达到快速运维的目的。

步骤1 进入主机资源列表后选择目标资源，在相应“标签”列单击，弹出标签编辑窗口。

如需批量添加，勾选多个目标资源后，单击列表左下角“添加标签”。

步骤2 输入标签类型回车选定标签，或选择已有标签类型。

步骤3 单击“确认”，添加完成，返回主机运维列表，即可查看资源已添加的标签。

如需删除资源标签，选择一个或多个目标资源，单击列表左下角“删除标签”，弹出删除标签确认窗口，确认信息无误后，单击“确认”，完成标签的删除。

----结束

Web 运维配置

在主机资源运维页面可设置RDP、SSH、FTP/SFTP协议的运维方式。

步骤1 进入主机运维页面后，单击右上角的“Web运维配置”。

步骤2 在弹窗中选择需要设置的资源协议后再选择运维方式。

- 当前支持的协议有RDP、SSH、FTP/SFTP。
  - RDP、SSH：支持H5页面和客户端运维方式。
  - FTP/SFTP：支持主从账号和客户端运维方式。
- 运维方式包含H5页面、客户端、主从账号，不同协议支持的运维方式也不一样。
  - H5页面运维：通过浏览器页面进行资源运维。
  - 客户端运维：通过堡垒机自动启用安装的客户端进行资源的运维。
  - 主从账号运维：通过堡垒机获取目标资源的账号密码，手动启动客户端进行登录后对资源实现运维。
- 设置RDP协议时，支持“连接模式”的设置，详情可参见**开启RDP强制登录**。

步骤3 运维方式选择后，确认无误单击“确定”，完成设置。

----结束

下载登录配置文件

如果有使用SecureCRT或者XShell客户端运维SSH协议的资源时，可通过该章节指导下载配置文件。

步骤1 进入主机运维页面后，单击右上角的“登录配置下载”。

步骤2 在弹窗中勾选登录配置下载项和对应的编码格式。

- 登录配置下载：仅支持选择SecureCRT和XShell客户端。
- 文件编码格式：选择下载文件的编码格式，建议与本地客户端编码格式保持一致。

步骤3 确认无误，单击“确定”，开始下载。

----结束

9.1.2 通过 Web 浏览器登录资源进行运维

通过Web浏览器登录主机，提供“协同分享”、“文件传输”、“文件管理”和“预置命令”等功能。用户在主机上执行的所有操作，被堡垒机记录并生成审计数据。

- “协同分享”指会话创建者将当前会话链接发送给协助者，协助者通过链接登录创建者的会话中参与运维，实现运维协同操作。
- “文件管理”指参与会话的用户获取操作权限后，在右侧管理面板可对云主机和主机网盘中文件或文件夹进行管理。
  - 支持新建文件夹。
  - 支持修改文件或文件夹名称。
  - 支持批量删除。
- “文件传输”指参与会话的用户获取操作权限后，可对云主机和主机网盘中文件进行上传或下载。
  - 支持上传/下载文件。
  - 支持上传文件夹。
  - 目标地址为“云主机文件”，支持上传多个本地或网盘文件到云主机，支持从云主机下载多个文件到本地或网盘保存。
  - 目标地址为“主机网盘”，支持上传多个文件或一个文件夹到主机网盘，支持从主机网盘下载文件到本地保存。

本小节主要介绍如何通过Web浏览器登录主机，以及字符协议类型和图像类协议类型主机会话界面操作说明。

注意事项

在运维过程中，堡垒机会自动录制视频进行保存审计，为了防止敏感信息泄露，请避免在运维过程中输入明文回显的敏感信息。

约束限制

- 仅字符协议类型（SSH、TELNET）和图像类协议类型（RDP、VNC）主机支持通过Web浏览器登录。
- TELNET协议类型主机不支持“文件传输”和“文件管理”功能。
- 支持复制/粘贴大量字符不乱码，本地到远端最多8万字符，远端到本地最多100万字节。
- 主机运维Windows资源时，如果登录堡垒机用户不是admin，需在“运维 > 主机运维”页面中右上角“Web运维配置”中取消勾选“admin console”选项。
- 文件管理

  不支持批量编辑文件或文件夹。
- 文件传输
  - 系统默认支持上传最大100G的单个文件，但实际上传单个文件大小，受“个人网盘空间”大小和使用浏览器限制。

    说明

    空间不足会导致上传失败，需清理磁盘或扩充磁盘容量。
  - 不支持下载文件夹。

- RDP协议类型主机的目标地址只有“主机网盘”。

前提条件

- 已获取“主机运维”模块管理权限。
- 已获取资源访问控制权限，即已被关联访问控制策略或访问授权工单已审批通过。
- 资源主机网络连接正常，且资源账户登录账号和密码无误。

操作步骤

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“登录”，登录会话进行操作。

- **RDP/VNC协议类型主机会话窗口**
- **SSH/TELNET协议类型主机会话窗口**

步骤4 通过协同分享，可邀请同事参与此会话，一同参与操作，详细说明请参见**协同分享**。

1. 单击“协同分享”，展开协同会话界面。
2. 邀请同事参与会话，单击“邀请好友进入此会话”。

   说明

   - 链接可复制发送给多人。
   - 拥有该堡垒机账户访问权限的用户，才能正常打开连接，否则将会上报连接错误，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）”。
3. 复制链接，发送给拥有堡垒机账户权限的用户，登录堡垒机，打开新的浏览器窗口，粘贴链接。
4. 单击“立即进入”参与会话操作。

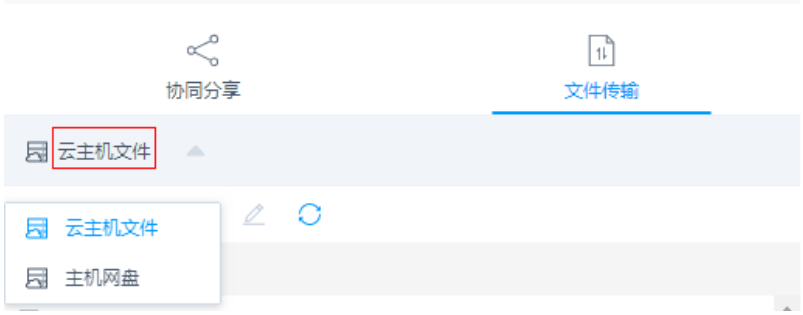
表 9-1 会话操作参数说明

参数	说明
申请控制权	向会话邀请者发申请控制权，邀请者同意后，可以操作此会话。
退出会话	退出此会话。

步骤5 通过文件传输，可对云主机或主机网盘中文件进行上传或下载，详细说明请参见**文件传输**。

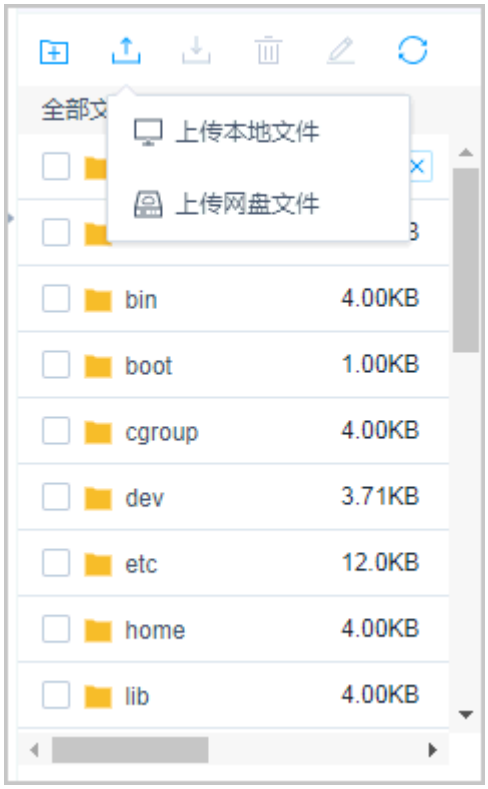
1. 单击“文件传输”，展开文件传输界面。
2. 默认为“云主机文件”，单击“云主机文件”可切换目标地址到“主机网盘”。

图 9-1 切换目标地址



3. 单击 上传图标，上传文件。
4. 选择文件，单击下载图标，下载文件。

图 9-2 上传文件



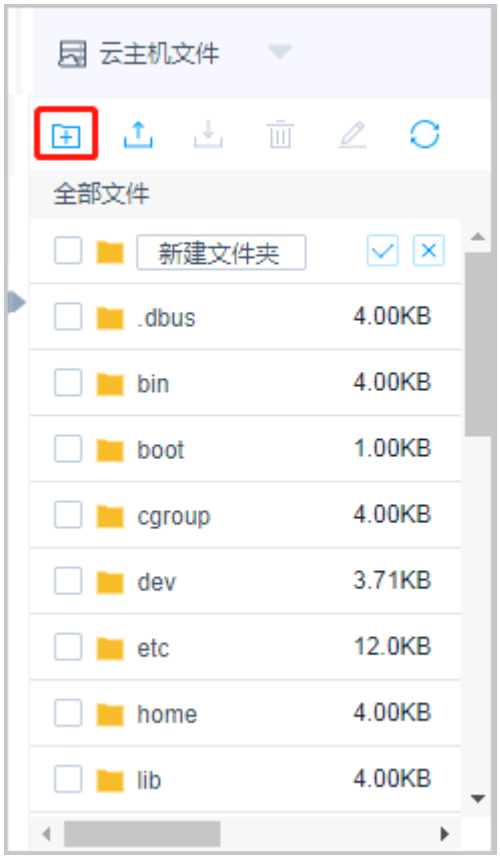
说明

- “主机网盘”属于堡垒机用户个人空间，其他用户不可见，用户可以将“主机网盘”文件上传到多个主机。
- Windows服务器文件存放的默认路径在G盘，Linux服务器文件存放的默认路径在根目录。
- Windows服务器上传下载文件，需打开服务器的磁盘目录，对NetDisk的G盘上文件复制/粘贴，实现对文件的上传/下载。

步骤6 通过文件管理，可对云主机或主机网盘中文件或文件夹进行管理。

1. 单击“文件传输”，展开文件传输界面。
2. 单击可以新建文件夹。

图 9-3 新建文件夹



3. 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。
4. 勾选一个文件或文件夹，单击编辑图标，可修改文件或文件夹名称。
5. 单击刷新图标，可刷新全部文件目录。

----结束

SSH/TELNET 协议类型主机会话

表 9-2 Linux 运维操作说明

参数	说明
编码	字符协议支持多种编码格式。
复制/粘贴	选中字符，按“Ctrl+C”进行复制，按“Ctrl+V”进行粘贴。
预置命令	对于字符较长，且经常输入的命令，可以提前预置。

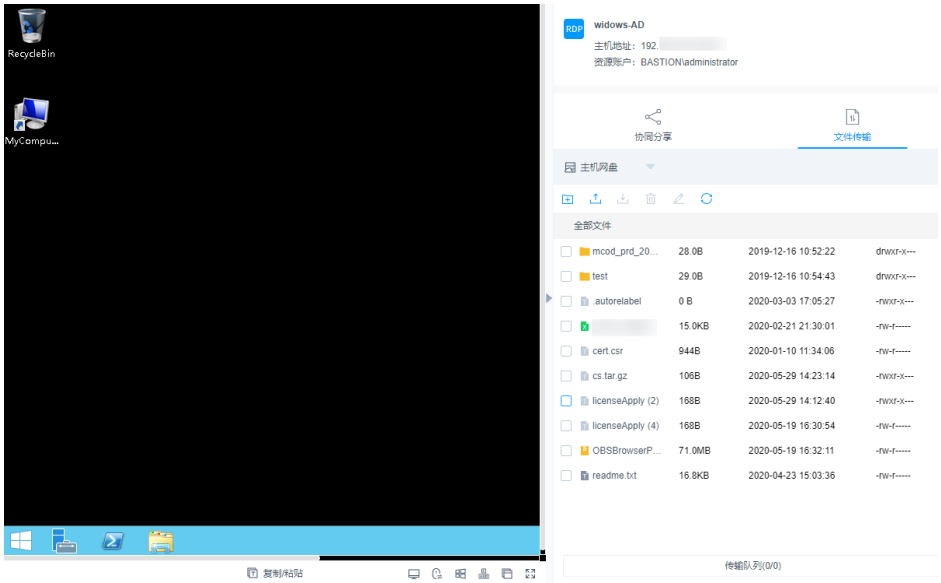
参数	说明
终端类型	字符协议支持切换终端类型，包括Linux和Xterm两种类型。
群发键	开启群发可同时对多个会话进行命令输入。
字体大小	设置字体大小：大、中、小。
复制窗口	可复制当前会话窗口。
全屏	可开启窗口全屏。

RDP/VNC 协议类型主机会话

表 9-3 Windows 主机运维操作说明

参数	说明
复制/粘贴	远程文本：选中字符， 需按两次“Ctrl+C”复制，按“Ctrl+V”粘贴。 远程机器文件：选中文本或图像，“Ctrl+B”复制，“Ctrl+G”粘贴。 **说明** Web浏览器运维支持复制/粘贴大量字符不乱码，本地到远端最多8万字符，远端到本地最多100万字节。
分辨率	可切换当前操作界面分辨率，切换途中会重新创建连接。
切换鼠标	可分别切换为本地鼠标和远程鼠标。
Windows键	适用于Win快捷键操作。
锁屏键	“Ctrl+Alt+Delete”。
复制窗口	可复制当前会话窗口。
全屏	可开启窗口全屏。

图 9-4 RDP 主机会话窗口



9.1.3 通过 SSH 客户端登录资源进行运维

通过SSH客户端登录堡垒机纳管资源，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，并且支持系统的命令拦截策略和运维审计功能。

本小节以Xshell登录SSH协议类型资源为例，介绍如何通过SSH客户端登录资源进行运维，以及如何下载登录资源的配置文件。

注意事项

在运维过程中，堡垒机会自动录制视频进行保存审计，为了防止敏感信息泄露，请避免在运维过程中输入明文回显的敏感信息。

约束限制

- 仅SSH、TELNET和Rlogin协议主机支持通过SSH客户端登录，其中Rlogin协议主机仅支持SSH客户端登录。
- 支持SSH协议客户端工具：SecureCRT 8.0及以上版本、Xshell 5及以上版本、PuTTY、MAC Terminal 2.0及以上版本。
- 不同算法类型不同场景支持的服务器情况如下：

表 9-4 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

前提条件

- 已获取“主机运维”模块管理权限。
- 已获取资源访问控制权限，即已被关联访问控制策略或访问授权工单已审批通过。
- 已在本地安装客户端工具。
- 资源主机网络连接正常，且资源账户登录账号和密码无误。

操作步骤

步骤1 打开本地Xshell客户端工具，选择“文件 > 新建”，新建用户会话。

步骤2 配置会话用户连接。

- 方式一
  a. 选择协议类型SSH，输入堡垒机实例弹性IP地址，端口号配置为2222，单击“确认”。
  b. 连接到会话，输入堡垒机用户名，单击“连接”。
- 方式二
  在新的空白会话窗口，执行登录命令：***协议类型 用户登录名@系统登录IP地址 端口***，例如执行*ssh admin@10.10.10.10 2222*。
- 方式三
  在正在运行的Linux主机会话窗口，执行登录命令：***协议类型 用户登录名@系统登录IP地址 -p 端口***，例如执行*ssh admin@10.10.10.10 -p 2222*。

  说明

  系统登录IP地址指堡垒机的IP地址（私有IP地址或弹性IP地址），且本地PC与该IP地址的网络连接正常。

步骤3 堡垒机用户身份验证。

- 选择密码登录，输入堡垒机用户密码，单击“确定”。
- 选择公钥登录，在“用户密钥”中上传与添加到堡垒机**SSH公钥**中相匹配的私钥文件后，选中目标私钥，单击“确定”。
  登录验证成功后，再次登录时该用户在SSH客户端可以免密登录。

步骤4 登录到堡垒机系统。

SSH客户端登录认证支持密码登录、手机短信、手机令牌和动态令牌方式。其中手机短信、手机令牌和动态令牌方式，需配置用户多因子认证，详情请参考**用户登录配置**。

- 手机短信：本地密码方式登录后，选择“短信验证码”，输入手机短信验证码。
- 手机令牌：本地密码方式登录后，选择“手机令牌OTP”，输入手机令牌验证码。
- 动态令牌：本地密码方式登录后，选择“动态令牌OTP”，输入动态令牌验证码。

步骤5 批量导入堡垒机资源账户。

解压配置文件压缩包（文件压缩包下载方式请参考**下载登录配置**），打开“readme.txt”文件，并参考指导导入资源账户。

步骤6 登录资源账户。

选择需登录的资源账户，输入系统用户密码，登录资源账户进行运维操作。

----结束

下载登录配置

为在SSH客户端批量导入运维资源，用户需下载资源配置文件。

步骤1 通过Web浏览器登录堡垒机系统。

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“登录配置下载”，弹出配置下载窗口。

步骤4 勾选相应客户端的配置文件，单击“确定”下载配置文件到本地。

----结束

9.1.4 通过 FTP/SFTP 客户端登录文件传输类资源

通过文件传输客户端登录堡垒机纳管资源，在不改变用户原来使用客户端习惯的前提下，对授权云主机资源进行远程文件传输管理。用户在主机上执行的所有操作，被堡垒机记录并生成审计数据。

本小节主要介绍如何获取客户端登录信息，并登录文件传输类资源。

约束限制

- FTP/SFTP协议的运维方式选择主从账号时，该协议资源的登录账户只能选择“登录方式”为“自动登录”的资源账户，且不能是Empty资源账户。
- 通过**多因子认证**方式登录的主机资源不支持通过SFTP协议进行文件传输。
- 仅FTP、SFTP协议主机支持通过Web浏览器登录，且登录资源的客户端工具的版本要求如下：

表 9-5 工具支持情况

协议主机	登录资源的客户端工具的版本要求
SFTP协议	Xftp 6及以上、WinSCP 5.14.4及以上、FlashFXP 5.4及以上

协议主机	登录资源的客户端工具的版本要求
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

表 9-6 客户端运维支持服务器情况

算法类型	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-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 • arcfour256
HMAC	• hmac-md5 • hmac-md5-96 • hmac-sha1 • hmac-sha1-96 • hmac-sha2-256 • hmac-sha2-512
Host Key	• ssh-rsa • ssh-dss • rsa-sha2-256 • rsa-sha2-512 • ecdsa-sha2-nistp256 • ecdsa-sha2-nistp384 • ecdsa-sha2-nistp521

前提条件

- 已获取“主机运维”模块管理权限。
- 已获取资源访问控制权限，即已被关联访问控制策略或访问授权工单已审批通过。
- 已在本地安装客户端工具。
- 资源主机网络连接正常，且资源账户登录账号和密码无误。
- 已在端口配置中打开FTP开关，开放2222（SFTP协议端口）、2121（FTP协议端口），具体操作详见**配置系统运维端口**。
- FTP/SFTP协议的运维方式选择客户端时，已在本地完成**配置SSO单点客户端**。
- 如需通过FTP协议传输文件，则需先开启系统的FTP代理服务配置，具体操作请参见**配置系统运维端口**。

操作步骤

步骤1 获取登录信息。

1. 登录堡垒机系统。
2. 选择“运维 > 主机运维”，进入主机运维列表页面。
3. 选择FTP/SFTP协议类型的主机，单击“登录”，弹出登录配置信息窗口。

步骤2 通过客户端工具登录。

1. 打开本地SFTP、FTP客户端工具。
2. 填写服务器地址、端口、用户名，输入登录密码。

说明

支持使用API的登录方式登录FTP、SFTP协议类型的主机。

表 9-7 登录参数说明

参数	说明
登录IP	配置信息的服务器地址，即堡垒机登录IP地址。
登录端口	配置信息的端口，默认端口号2222。
登录用户名	配置信息的用户名，即“用户登录名@资源账号名@主机地址”，例如admin@root@192.168.1.1。
登录密码	用户登录系统密码。

----结束

9.1.5 通过 SSO 单点客户端登录和运维数据库资源

通过SSO单点客户端调用本地数据库工具，登录和运维数据库资源，实现对数据库的运维审计。用户需先在本地安装SSO单点登录工具和数据库客户端工具，然后配置数据库客户端工具路径。

本小节主要介绍如何配置SSO单点客户端，以及如何通过SSO单点客户端登录数据库资源。

注意事项

在运维过程中，堡垒机会自动录制视频进行保存审计，为了防止敏感信息泄露，请避免在运维过程中输入明文回显的敏感信息。

约束限制

- 仅**专业版**实例支持数据库运维操作审计。
- 仅支持通过SsoDBSettings单点登录工具调用客户端。
- 仅支持调用SecureCRT和XShell主机资源运维客户端。
- 支持运维的数据库协议类型，及对应的客户端请参见下表。

表 9-8 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）

说明

- 堡垒机支持的数据库及版本，需您自行前往产品官网搜索相关版本下载。
- 当您需要使用单点登录工具运维PostgreSQL和GaussDB时，需要在“数据库 - > 驱动管理器”中的“连接属性”中添加“sslmode”属性，并且将“值”保存为：“disable”。
- SsoTool.msi 远程工具安装只能选择默认的路径：C:\sso\SsoTool，若自定义安装路径可能会导致该工具无法启动。
- 由于堡垒机无法校验启用了ssl的数据库，连接GaussDB时，需要在DBeaver禁用ssl，将sslmode设置成disable。

前提条件

- 已获取“主机运维”模块管理权限。
- 已获取资源访问控制权限，即已被关联访问控制策略或访问授权工单已审批通过。
- 已在本地安装客户端工具。
- 资源主机网络连接正常，且资源账户登录账号和密码无误。

操作步骤

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 选择数据库协议类型的主机，单击“登录”。

系统弹出客户端工具选择窗口。

说明

- 首次登录数据库资源，弹出SsoDBSettings下载窗口，可下载SsoDBSettings工具。
- 不同堡垒机版本选择的下载工具会有差别，具体以实际堡垒机界面显示为准。
  以V.3.3.44.0版本为例：下拉框可选择单点登录工具Windows和单点登录工具UOS(arm)。

步骤4 选择本地已安装的客户端工具后，单击“确定”。

系统将自动调用本地数据库客户端工具登录数据库。

----结束

配置 SSO 单点客户端

以Navicat客户端为例，示例配置客户端路径。

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”，返回堡垒机“主机运维”列表页面，即可登录数据库资源。

----结束

9.1.6 批量登录主机进行运维

通过Web浏览器支持批量登录主机，提供“文件传输”、“文件管理”和“预置命令”等功能。用户在主机上执行的所有操作，被堡垒机记录并生成审计数据。

约束限制

- FTP、SFTP、SCP协议类型资源，不支持批量登录。
- 手动登录账户和双人授权账户，不支持批量登录。
- 批量登录的多运维会话窗口，不支持“协同分享”功能。

说明

如果批量登录的资源中存在账号和密码不正确的资源，在会话窗口中将无法正常显示，同时也不会报错，需单独登录该资源查看报错信息。

前提条件

- 已获取“主机运维”模块管理权限。
- 已获取资源访问控制权限，即已被关联访问控制策略或访问授权工单已审批通过。

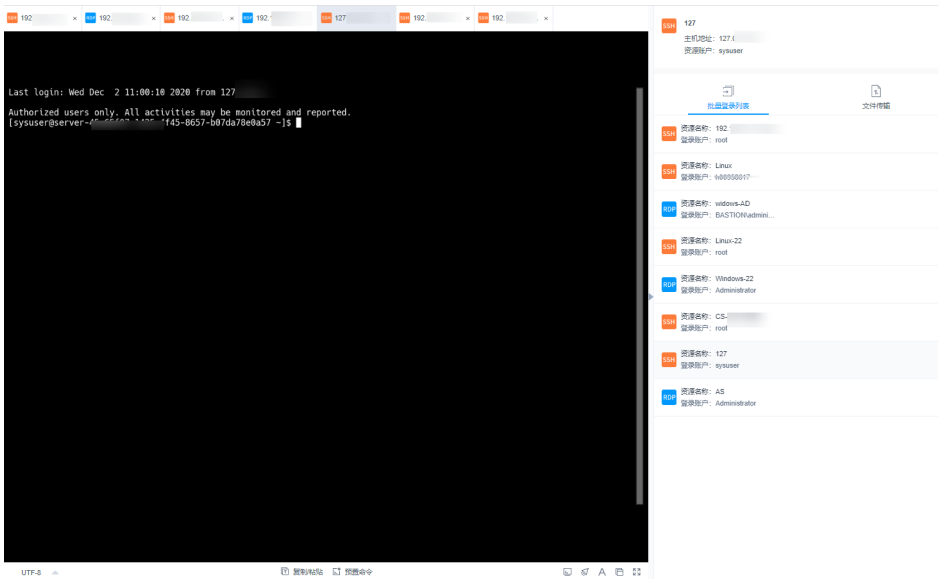
操作步骤

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 勾选多个目标运维资源，单击“批量登录”，跳转到运维会话窗口。

图 9-5 批量登录会话窗口



步骤4 切换资源会话窗口。

单击批量登录列表中资源名称，可将切换到目标会话窗口。

步骤5 会话窗口操作说明，请分别参见如下说明。

- **RDP/VNC协议类型主机会话窗口**
- **SSH/TELNET协议类型主机会话窗口**

步骤6 通过文件传输，可对云主机或主机网盘中文件进行上传或下载，详细说明请参见**文件传输**。

步骤7 通过文件管理，可对云主机或主机网盘中文件或文件夹进行管理，详细说明请参见**通过Web浏览器登录**。

----结束

9.1.7 文件传输

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

- 目前仅SSH、RDP协议主机，支持通过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。
- 不支持传输大小超过1G的超大文件，建议分批次上传/下载文件，或**通过FTP客户端传输文件**。

  说明

  空间不足会导致上传失败，需清理磁盘或扩充磁盘容量。

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。

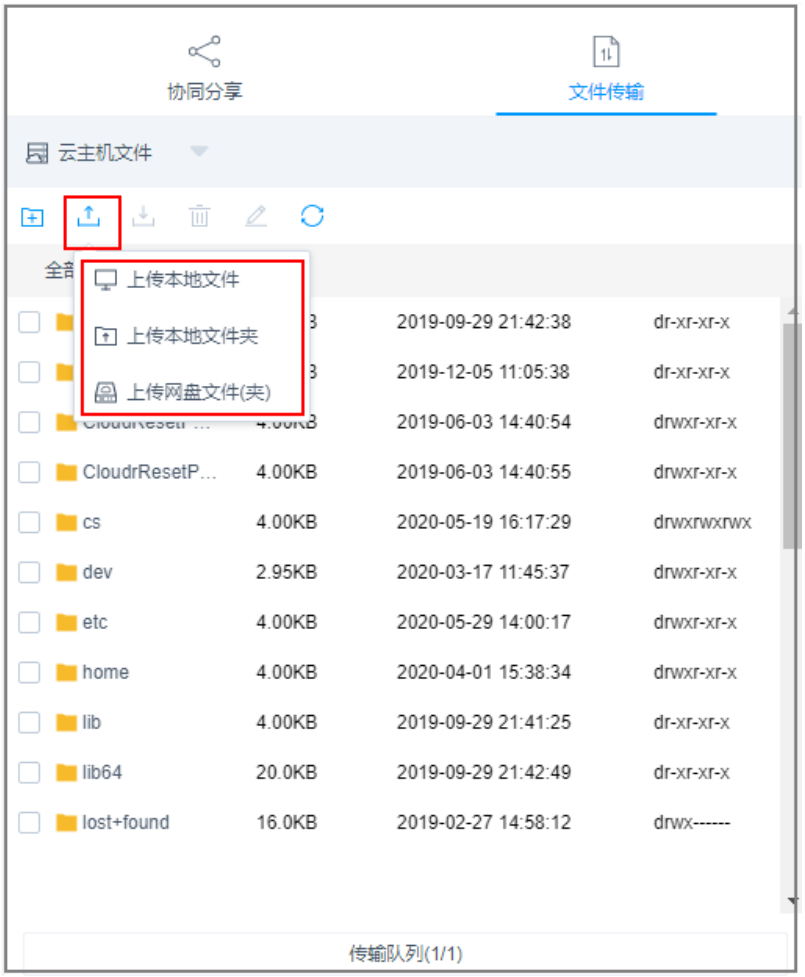
步骤2 选择“运维 > 主机运维”，选择目标Linux主机资源，单击“登录”，跳转到Linux主机资源运维界面。

步骤3 在运维页面右侧选择“文件传输”，查看Linux主机文件列表。

步骤4 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）。

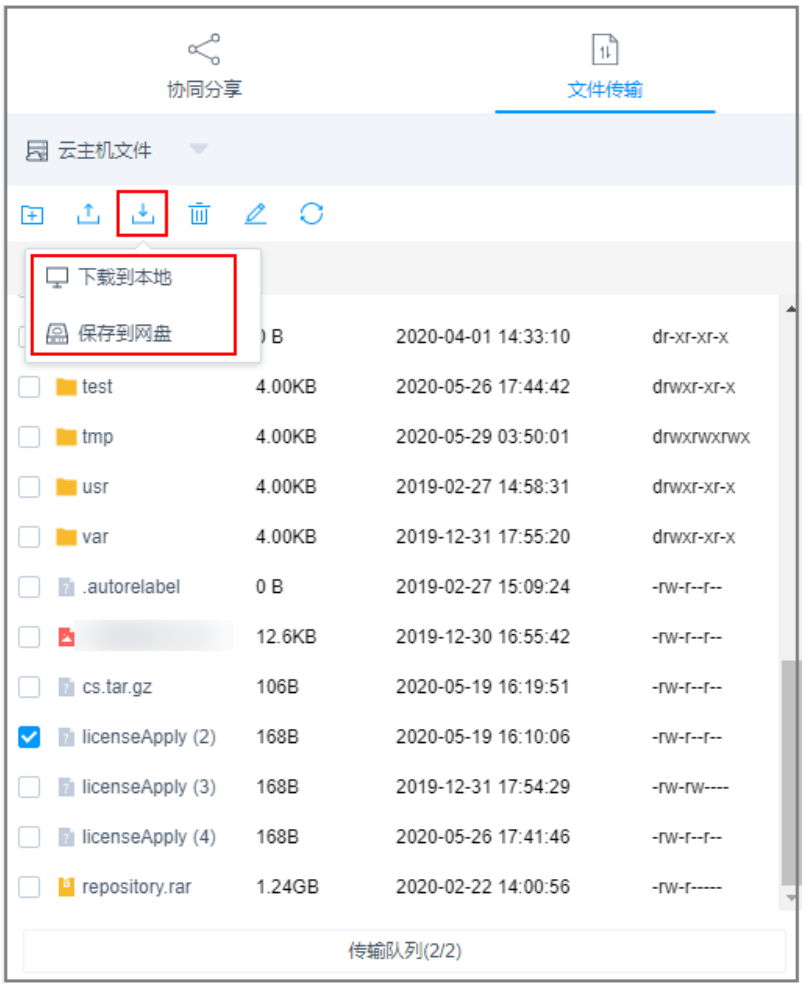
图 9-6 上传文件到 Linux 主机



步骤5 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。

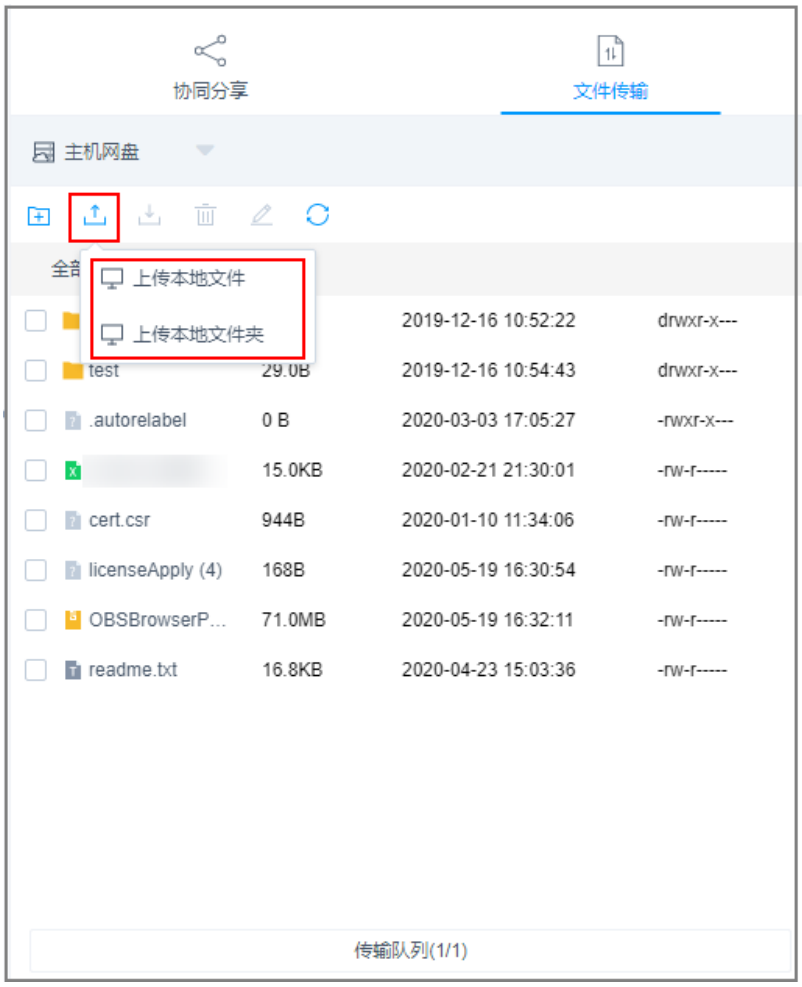
图 9-7 下载 Linux 主机中文件



步骤6 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。

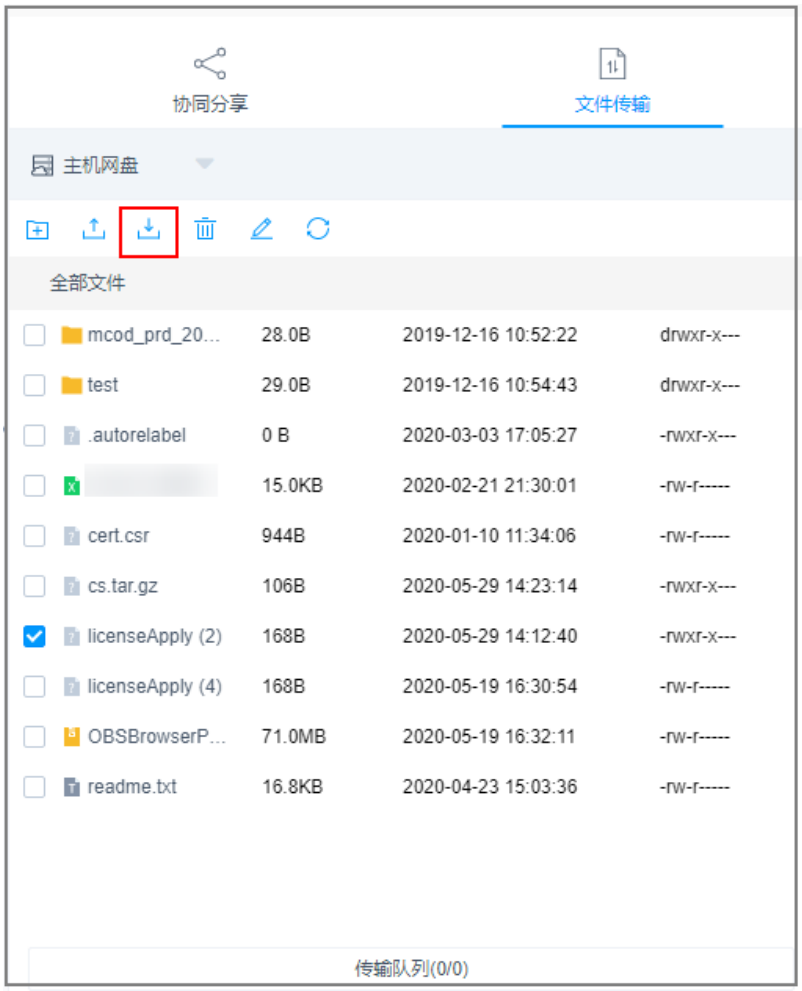
图 9-8 上传文件到个人网盘



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 9-9 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。

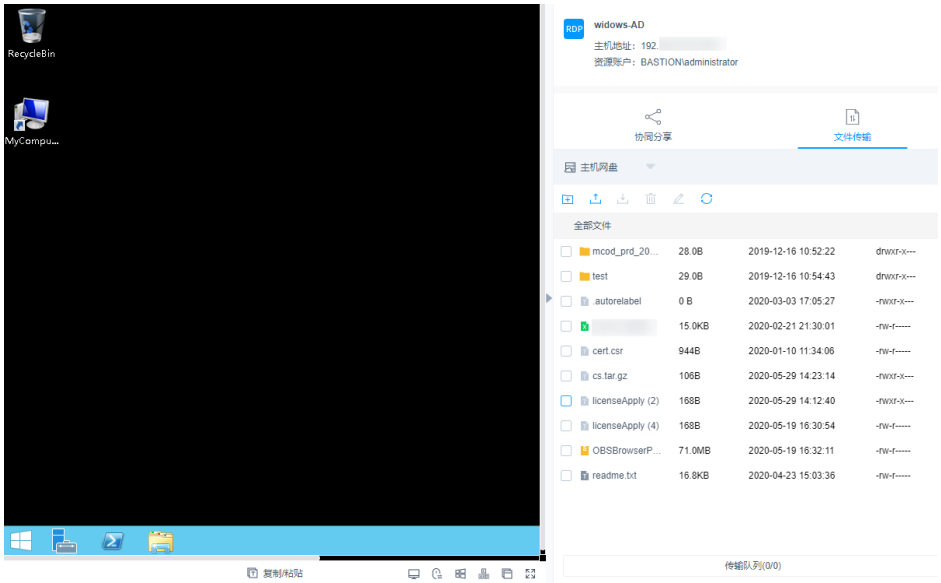
步骤1 登录堡垒机系统。

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。

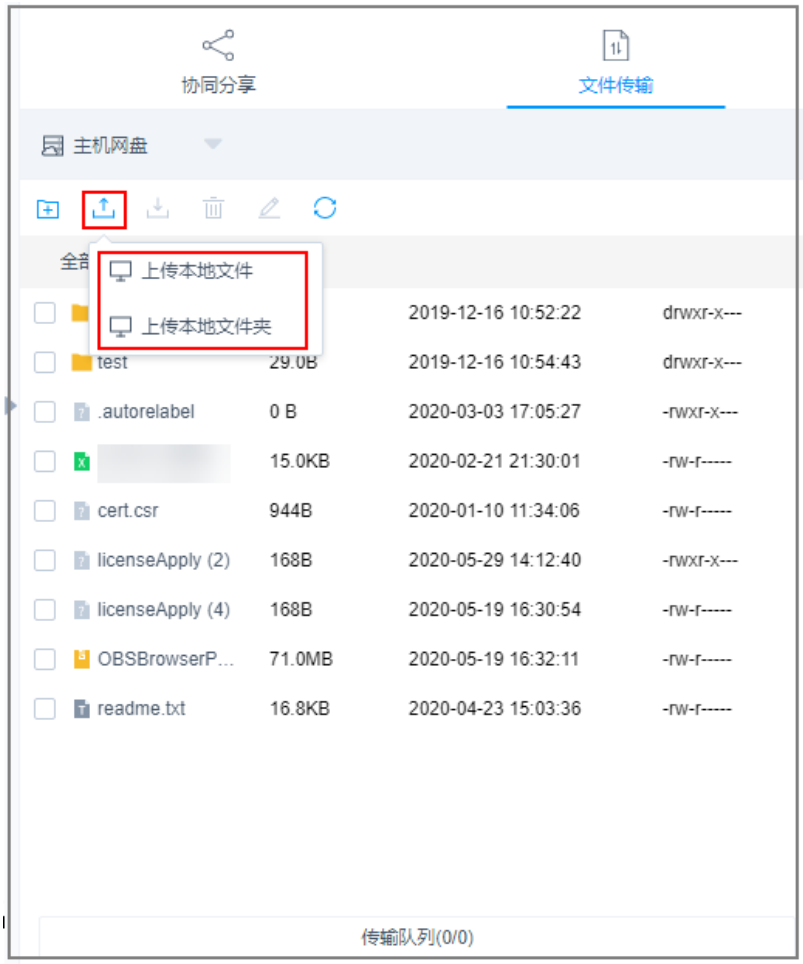
图 9-10 Windows 主机文件传输



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 9-11 上传文件到个人网盘



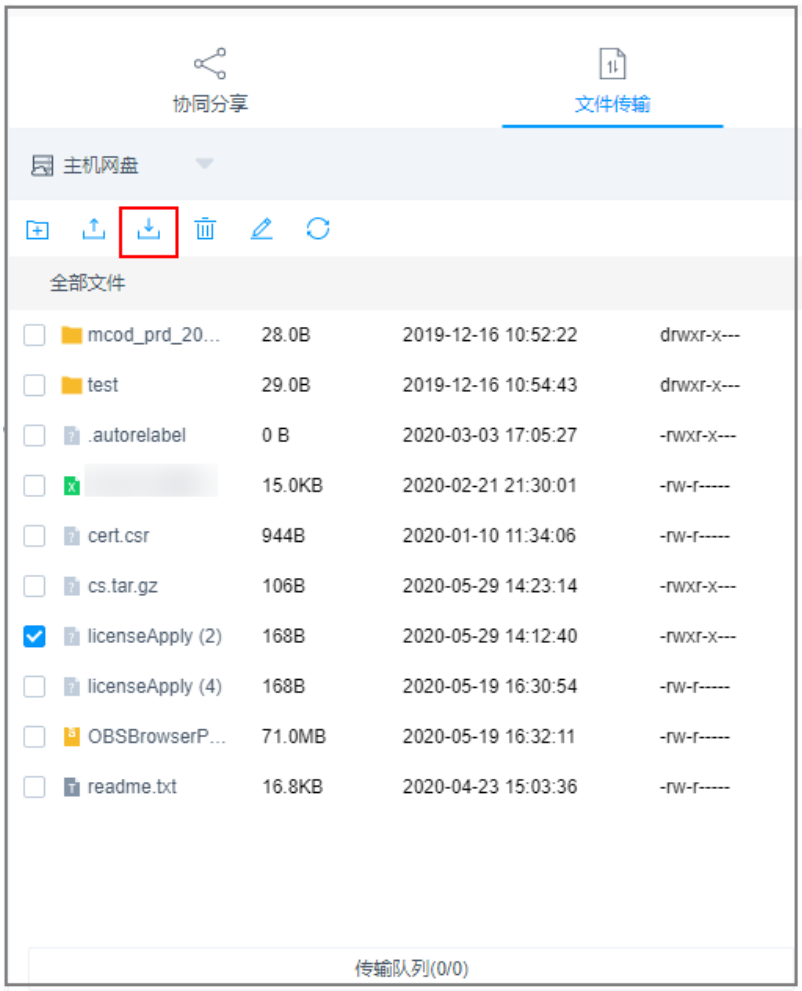
步骤6 下载Windows主机中文件。

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 9-12 下载个人网盘中文件



----结束

9.1.8 协同分享

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。

约束限制

- 创建协同分享前，需确保系统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。

前提条件

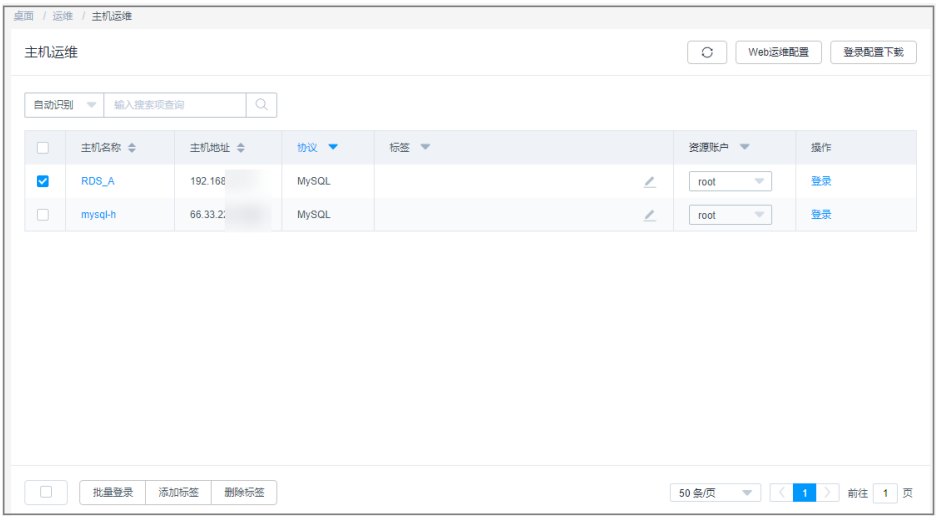
- 已获取主机资源运维的权限。
- 已通过Web浏览器正常登录。

操作步骤

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。

图 9-13 主机运维列表



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，发送给拥有堡垒机资源账户权限的用户。

步骤6 受邀用户登录堡垒机，打开邀请链接，查看邀请信息。

图 9-14 受邀用户查看会话协同邀请信息

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

9.1.9 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。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。

本小节主要介绍如何开启admin console配置。

约束限制

- 仅对RDP协议类型主机生效。
- 登录时需使用admin账户登录。

前提条件

已获取“主机运维”模块管理权限。

操作步骤

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

9.2 应用资源运维

9.2.1 查看应用运维列表并设置资源标签

运维用户获取应用发布资源访问操作权限后，即可在应用运维列表查看已授权资源，并设置资源标签。

本小节主要介绍如何查看已授权资源，以及如何设置资源标签。

约束限制

每个用户可自定义资源标签，资源标签仅能个人账号使用，不能与系统内用户共用。

前提条件

- 已获取“应用运维”模块管理权限。
- 已获取资源访问控制权限，即已被关联访问控制策略或访问授权工单已审批通过。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“运维 > 应用运维”，进入应用运维列表页面。

步骤3 查询应用资源。

快速查询：在搜索框中输入关键字，根据自动识别、应用名称、应用地址等快速查询资源。

步骤4 添加标签。

1. 选择目标资源，在相应“标签”列单击，弹出标签编辑窗口。
2. 输入标签类型回车选定标签，或选择已有标签类型。
3. 单击“确认”，返回运维列表，即可查看已添加的标签。

步骤5 批量添加标签。

1. 选择多个目标资源，单击列表左下角“添加标签”，弹出标签编辑窗口。
2. 输入标签类型回车选定标签，或选择已有标签类型。
3. 单击“确认”，返回运维列表，即可查看已添加的标签。

步骤6 删除标签。

1. 选择一个或多个目标资源，单击列表左下角“删除标签”，弹出删除标签确认窗口。
2. 确认信息无误后，单击“确认”，返回运维列表，标签已删除。

----结束

9.2.2 通过 Web 浏览器登录应用资源进行运维

通过Web浏览器登录应用资源，提供“协同分享”、“文件传输”、“文件管理”等功能。用户在应用上执行的所有操作，被堡垒机记录并生成审计数据。

- “协同分享”指会话创建者将当前会话链接发送给协助者，协助者通过链接登录创建者的会话中参与运维，实现运维协同操作。
- “文件管理”指参与会话的用户获取操作权限后，可对云主机和主机网盘中文件或文件夹进行管理。
  - 支持新建文件夹。
  - 支持修改文件或文件夹名称。

  - 支持批量删除。
- “文件传输”指参与会话的用户获取操作权限后，可对云主机和主机网盘中文件进行上传或下载。
  - 支持上传/下载文件。
  - 支持上传文件夹。
  - 目标地址为“主机网盘”，支持上传多个文件或一个文件夹到主机网盘，支持从主机网盘下载文件到本地保存。

本小节主要介绍如何通过Web浏览器登录应用资源，以及应用运维会话窗口操作说明。

注意事项

在运维过程中，堡垒机会自动录制视频进行保存审计，为了防止敏感信息泄露，请避免在运维过程中输入明文回显的敏感信息。

约束限制

- 应用运维仅支持通过Web浏览器方式登录进行运维。
- 支持复制/粘贴大量字符不乱码，本地到远端最多8万字符，远端到本地最多100万字节。
- 文件管理

  不支持批量编辑文件或文件夹。
- 文件传输
  - 系统默认支持上传最大100G的单个文件，但实际上传单个文件大小，受“个人网盘空间”大小和使用浏览器限制。

    说明

    空间不足会导致上传失败，需清理磁盘或扩充磁盘容量。
  - 不支持下载文件夹。
  - 应用运维的目标地址只有“主机网盘”。

前提条件

- 已获取“应用运维”模块管理权限。
- 已获取资源控制权限，即已被关联访问控制策略或提交的访问授权工单已审批通过。
- 应用发布服务器网络连接正常，且资源账户登录账号和密码无误。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“运维 > 应用运维”，进入应用运维列表页面。

步骤3 单击“登录”，登录会话进行操作。

表 9-9 会话操作说明

参数	说明
复制/粘贴	• 远程文本：选中字符， 需按两次“Ctrl+C”复制按“Ctrl+V”粘贴。 • 远程机器文件：选中文本或图像，“Ctrl+B”复制，“Ctrl+G”粘贴。 **说明** Web浏览器运维支持复制/粘贴大量字符不乱码，本地到远端最多8万字符，远端到本地最多100万字节。
切换鼠标	可分别切换为本地鼠标和远程鼠标。
复制窗口	可复制当前会话窗口。
全屏	可开启窗口全屏。

步骤4 协同分享，可邀请同事参与此会话，一同进行操作，详细说明请参见**协同分享**。

1. 在“协同分享”页签，单击“开始分享”，展开协同会话界面。
2. 邀请同事参与会话，单击“邀请好友进入此会话”，弹出邀请链接窗口。

图 9-15 邀请协同会话

说明

此链接可复制发送给多人。

3. 复制链接，发送给拥有堡垒机账户权限的用户。
4. 受邀用户登录堡垒机，打开新的浏览器窗口，粘贴链接。
5. 单击“立即进入”参与会话操作。

表 9-10 会话操作管理说明

参数	说明
申请控制权	可以向会话邀请者发申请控制权，邀请者同意后，可以操作此会话。

参数	说明
退出会话	退出此会话。

步骤5 通过文件传输，可对主机网盘中文件进行上传或下载，详细说明请参见**文件传输**。

在运维窗口的“文件传输”页签，可以对系统个人网盘文件或文件夹进行管理。

步骤6 通过文件管理，可对主机网盘中文件或文件夹进行管理。

1. 在运维窗口的“文件传输”页签，单击可以新建文件夹。

图 9-16 新建文件夹

2. 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。
3. 勾选一个文件或文件夹，单击编辑图标，可修改文件或文件夹名称。
4. 单击刷新图标，可刷新全部文件目录。

----结束

9.3 云服务运维

9.3.1 查看云服务运维列表并设置资源标签

运维用户获取云服务资源访问操作权限后，即可在云服务运维列表查看已授权资源，并设置资源标签。

本小节主要介绍如何查看已授权资源，以及如何设置资源标签。

约束限制

每个用户可自定义资源标签，资源标签仅能个人账号使用，不能与系统内用户共用。

前提条件

- 已获取“云服务运维”模块管理权限。
- 已获取资源访问控制权限，即已被关联访问控制策略或访问授权工单已审批通过。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“运维 > 云服务运维”，进入云服务器运维列表页面。

步骤3 查询容器资源。

快速查询：在搜索框中输入关键字，根据自动识别、主机名称、主机地址等快速查询主机资源。

步骤4 添加标签。

1. 选择目标资源，在相应“标签”列单击，弹出标签编辑窗口。
2. 输入标签类型回车选定标签，或选择已有标签类型。
3. 单击“确认”，返回云服务运维列表，即可查看已添加的标签。

步骤5 批量添加标签。

1. 选择多个目标资源，单击列表左下角“添加标签”，弹出标签编辑窗口。
2. 输入标签类型回车选定标签，或选择已有标签类型。
3. 单击“确认”，返回云服务运维列表，即可查看已添加的标签。

步骤6 删除标签。

1. 选择一个或多个目标资源，单击列表左下角“删除标签”，弹出删除标签确认窗口。
2. 确认信息无误后，单击“确认”，返回云服务运维列表，标签已删除。

----结束

9.3.2 通过 Web 浏览器登录资源运维容器

通过Web浏览器登录容器，提供“协同分享”功能。用户在主机上执行的所有操作，被堡垒机记录并生成审计数据。

说明

使用Web浏览器运维容器暂不支持“文件传输”功能。

“协同分享”指会话创建者将当前会话链接发送给协助者，协助者通过链接登录创建者的会话中参与运维，实现运维协同操作。

本小节主要介绍如何通过Web浏览器登录容器。

注意事项

在运维过程中，堡垒机会自动录制视频进行保存审计，为了防止敏感信息泄露，请避免在运维过程中输入明文回显的敏感信息。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“运维 > 云服务运维”，进入云服务器运维列表页面。

步骤3 单击目标容器“操作”列的“登录”，登录会话进行操作。

步骤4 通过协同分享，可邀请同事参与此会话，一同参与操作，详细说明请参见**协同分享**。

1. 单击“协同分享”，展开协同会话界面。
2. 邀请同事参与会话，单击“邀请好友进入此会话”。

   说明

   - 链接可复制发送给多人。
   - 拥有该堡垒机账户访问权限的用户，才能正常打开连接，否则将会上报连接错误，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）”。
3. 复制链接，发送给拥有堡垒机账户权限的用户，登录堡垒机，打开新的浏览器窗口，粘贴链接。
4. 单击“立即进入”参与会话操作。

表 9-11 会话操作参数说明

参数	说明
申请控制权	向会话邀请者发申请控制权，邀请者同意后，可以操作此会话。
退出会话	退出此会话。

----结束

9.4 运维脚本管理

9.4.1 新建脚本

堡垒机支持脚本管理功能。通过执行脚本，完成复杂或重复的运维任务，提升运维效率。堡垒机支持在线编辑脚本和以文件方式导入脚本。

说明

堡垒机已内置HSS-Agent.sh自动下载及安装脚本。

约束限制

- 仅**专业版**堡垒机支持脚本管理功能。

- 仅支持管理Python和Shell两种脚本语言。
- 脚本仅能由个人账户，管理员，部门管理员管理，不能被系统内其他用户管理。

前提条件

已获取“脚本管理”模块管理权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“运维 > 脚本管理 ”，进入脚本列表页面。

步骤3 单击右上角“新建”，弹出“新建脚本”窗口。

步骤4 配置脚本基本信息。

表 9-12 新建脚本信息参数说明

参数	说明
来源	脚本内容来源。 • “在线编辑”手动编辑脚本信息。 • “文件导入”导入线下脚本文件，只能上传shell/python脚本文件，文件大小不能超过5M。
所属部门	选择脚本所属部门。
名称	自定义的脚本策略名称，系统内脚本“名称”不能重复。 **说明** “文件导入”方式上传的脚本，名称会根据导入文件名自动填充。
描述	脚本简要描述，最长128个汉字或字符。

步骤5 单击“确定”，返回脚本列表页面，查看新建的脚本信息。

----结束

后续管理

新建在线编辑脚本后，可在脚本详情页面，在线编辑脚本，详情请参见**查看和修改脚本信息**。

9.4.2 查看和修改脚本信息

本小节主要介绍如何在线查看和修改脚本信息。

约束限制

- 当脚本大小超过128KB，将不能在线查看脚本内容，可下载脚本文件到本地查看，详情请参见**下载脚本**。

前提条件

已获取“脚本管理”模块管理权限。

操作步骤

步骤1 登录堡垒机系统。

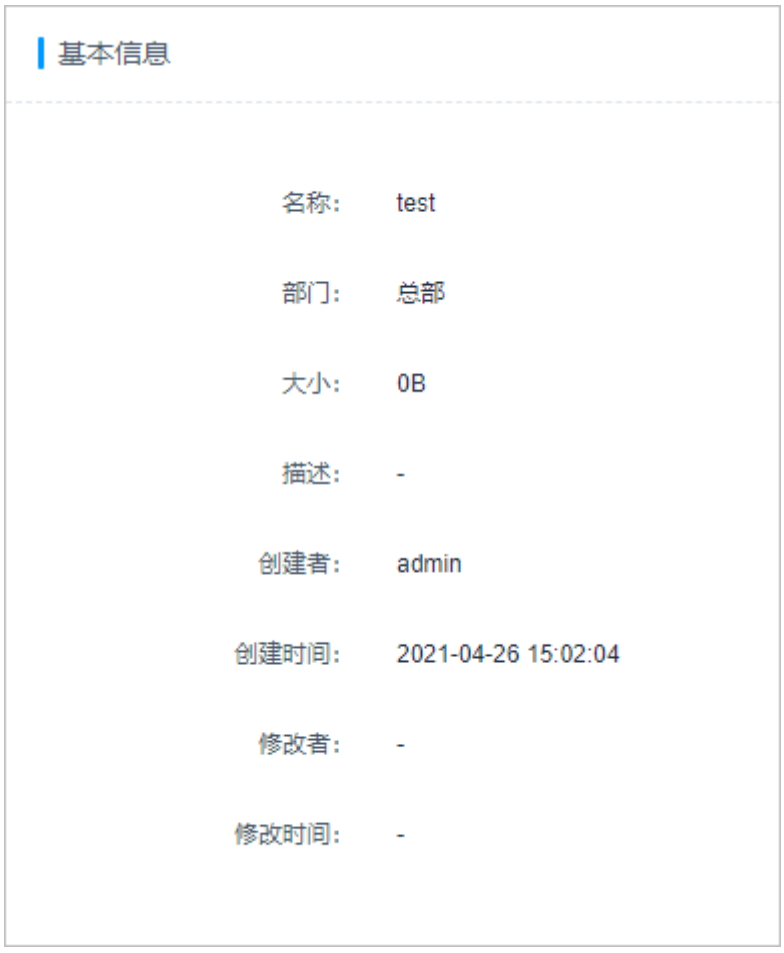
步骤2 选择“运维 > 脚本管理 ”，进入脚本列表页面。

步骤3 查询脚本。

- 快速查询
  在搜索框中输入关键字，根据脚本略名称等快速查询脚本。
- 高级搜索
  在相应属性搜索框中分别输入关键字，精确查询脚本。

步骤4 单击脚本名称，或者单击“管理”，进入“脚本详情”页面。

图 9-17 脚本详情页面



步骤5 查看和修改脚本基本信息。

在“基本信息”区域，单击“编辑”，弹出基本信息编辑窗口，即可修改脚本的基本信息。

可修改信息包括“脚本名称”、“描述”等。

步骤6 查看和修改脚本内容。

在“脚本内容”区域，单击“编辑”，弹出脚本编辑窗口，即可修改或移除脚本命令。

----结束

9.4.3 下载脚本

本小节主要介绍如何下载脚本，以便本地查看和管理脚本。

前提条件

已获取“脚本管理”模块管理权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“运维 > 脚本管理 ”，进入脚本列表页面。

步骤3 选择目标脚本，在相应“操作”列单击“下载”，即可下载脚本文件保存到本地。

----结束

9.4.4 删除脚本

本小节主要介绍如何删除线上脚本，管理脚本列表。

前提条件

已获取“脚本管理”模块管理权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“运维 > 脚本管理 ”，进入脚本列表页面。

步骤3 单个删除。

1. 选择目标脚本，在相应“操作”列单击“删除”，弹出删除确认窗口。
2. 单击“确认”，即可删除目标脚本。

步骤4 批量删除。

同时勾选多个脚本，单击列表下方的“删除”，即可批量删除多个脚本。

----结束

9.5 快速运维

9.5.1 管理命令任务

堡垒机支持快速运维功能，用户可通过命令方式快速运维多个目标资源。通过将命令在多个SSH协议主机资源上执行，并根据发起的命令，返回相应执行结果。

本小节主要介绍如何管理命令任务，包括创建命令任务、执行命令任务、中断命令任务、查看任务执行结果等。

约束限制

- 仅**专业版**堡垒机支持快速运维功能。
- 仅支持快速运维Linux主机（SSH协议类型）资源的任务。
- 暂不支持快速运维Windows主机资源、数据库资源和应用资源的任务。

前提条件

- 已获取“快速运维”模块管理权限。
- 已获取资源访问控制权限，即已配置访问控制策略或访问授权工单已审批通过。
- 资源主机网络连接正常。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“运维 > 快速运维 > 命令控制台”，进入快速命令运维页面。

图 9-18 命令控制台

步骤3 配置快速命令运维信息。

表 9-13 快速命令运维参数说明

参数	说明
执行命令	输入针对主机资源需执行的命令。
执行账户	• 单击“选择”在弹窗选择您已创建的SSH协议类型资源账户或账户组。 • 单击“重置”对已选择的资源账户或账户组进行重置。 **说明** 每个资源的执行账户最多一个。
更多选项	（可选）用户对资源账户执行任务权限不够时，需勾选上“提权执行”，用户需在该主机资源的Sudoers文件下执行任务。

步骤4 立即执行命令任务。

单击“立即执行”，即可针对目标资源，执行当前命令任务。

步骤5 中断命令任务。

任务正在执行时，单击“中断执行”，可中断命令任务。

说明

“中断执行”会将当前执行账户完成后才停止任务，再立即终止未执行的账户。

步骤6 查看执行结果。

命令任务执行完成后，查看当前命令任务执行结果。查看更多历史任务执行结果，请参见**查看执行日志**。

1. 在执行结果区域，在搜索框中输入关键字，根据资源名称、执行结果、执行账户、主机地址，快速查询任务执行结果。
2. 单击“展开”，即可查看目标任务执行结果。
3. 单击“导出”，即可下载当前命令任务执行结果的CSV格式文件保存到本地。

图 9-19 命令任务结果

----结束

9.5.2 管理脚本任务

堡垒机支持快速运维功能，用户可通过脚本方式快速运维多个目标资源。通过将脚本在多个SSH协议主机资源上执行，并根据发起的脚本，返回相应执行结果。

本小节主要介绍如何管理脚本任务，包括创建脚本任务、执行脚本任务、中断脚本任务、查看任务执行结果等。

约束限制

- 仅**专业版**堡垒机支持快速运维功能。
- 仅支持快速运维Linux主机（SSH协议类型）资源的任务。
- 暂不支持快速运维Windows主机资源、数据库资源和应用资源的任务。

前提条件

- 已获取“快速运维”模块管理权限。
- 已获取资源访问控制权限，即已配置访问控制策略或访问授权工单已审批通过。
- 资源主机网络连接正常。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“运维 > 快速运维 > 脚本控制台”，进入快速脚本运维页面。

图 9-20 脚本控制台

步骤3 配置快速脚本运维信息。

表 9-14 快速脚本运维参数说明

参数	说明
执行脚本	输入针对主机资源需执行的脚本。 ● 可选择“脚本管理”中脚本内容，也可新上传本地脚本文件。
脚本参数	（可选）自定义脚本参数。

参数	说明
执行账户	• 单击“选择”在弹窗选择您已创建的SSH协议类型资源账户或账户组。 • 单击“重置”对已选择的资源账户或账户组进行重置。 **说明** 每个资源的执行账户最多一个。
更多选项	（可选）用户对资源账户执行任务权限不够时，需勾选上“提权执行”，用户需在该主机资源的Sudoers文件下执行任务。

步骤4 立即执行脚本任务。

单击“立即执行”，即可针对目标资源，执行当前脚本任务。

步骤5 中断脚本任务。

任务正在执行时，单击“中断执行”，可中断脚本任务。

说明

“中断执行”会将当前执行账户完成后才停止任务，再立即终止未执行的账户。

步骤6 查看执行结果。

脚本任务执行完成后，查看当前脚本任务执行结果。查看更多历史任务执行结果，请参见**查看执行日志**。

1. 在执行结果区域，在搜索框中输入关键字，根据资源名称、执行结果、执行账户、主机地址，快速查询任务执行结果。
2. 单击“展开”，即可查看目标任务执行结果。
3. 单击“导出”，即可下载当前脚本任务执行结果的CSV格式文件保存到本地。

----结束

9.5.3 管理文件传输任务

堡垒机支持快速运维功能，用户可将系统磁盘文件或本地文件快速上传到多个目标主机路径。通过将一个或多个文件上传到多个主机资源上，并返回文件上传结果。

本小节主要介绍如何管理文件传输任务，包括创建文件传输任务、执行文件传输任务、中断文件传输任务、查看任务执行结果等。

约束限制

- 仅**专业版**堡垒机支持快速运维功能。
- 仅支持快速运维Linux主机（SSH协议类型）资源的任务。
- 暂不支持快速运维Windows主机资源、数据库资源和应用资源的任务。

前提条件

- 已获取“快速运维”模块管理权限。
- 已获取资源访问控制权限，即已配置访问控制策略或访问授权工单已审批通过。

- 资源主机网络连接正常。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“运维 > 快速运维 > 文件传输控制台”，进入快速文件传输页面。

图 9-21 文件传输控制台

步骤3 配置快速文件传输信息。

表 9-15 快速文件传输参数说明

参数	说明
源文件	默认选择系统个人磁盘文件，也可先将个人本地文件上传到个人网盘再选择。 最多选择10个文件。
目标路径	文件传输到目标主机资源的绝对路径。
执行账户	• “选择”已创建的SSH协议类型资源账户或账户组。 • “重置”已选择的资源账户或账户组。 **说明** 每个资源的执行账户最多一个。
更多选项	（可选） • 提权执行：用户对资源账户执行任务权限不够时，需勾选上“提权执行”，用户需在该主机资源的Sudoers文件下执行任务。 • 覆盖重名文件：若上传主机路径下有同名文件，将覆盖原有文件，保留新上传文件。

步骤4 立即执行文件传输任务。

单击“立即执行”，即可针对目标资源，执行当前文件传输任务。

步骤5 中断文件传输任务。

任务正在执行时，单击“中断执行”，可中断文件传输。

说明

“中断执行”会将当前执行账户完成后才停止任务，再立即终止未执行的账户。

步骤6 查看执行结果。

文件传输任务执行完成后，查看当前文件传输任务执行结果。查看更多历史任务执行结果，请参见**查看执行日志**。

1. 在执行结果区域，在搜索框中输入关键字，根据资源名称、执行结果、执行账户、主机地址，快速查询任务执行结果。
2. 单击“展开”，即可查看目标任务执行结果。
3. 单击“导出”，即可下载当前文件传输任务执行结果的CSV格式文件保存到本地。

图 9-22 文件传输任务结果

----结束

9.5.4 管理快速任务执行日志

本小节主要介绍快速运维任务执行完成后，如何管理任务执行日志，包括查看任务详情、导出执行日志、删除执行日志等。

前提条件

- 已获取“快速运维”模块管理权限。
- 快速运维任务（快速命令任务、快速脚本任务、快速文件传输任务）已执行完成。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“运维 > 快速运维 > 执行日志”，进入快速运维执行日志列表页面。

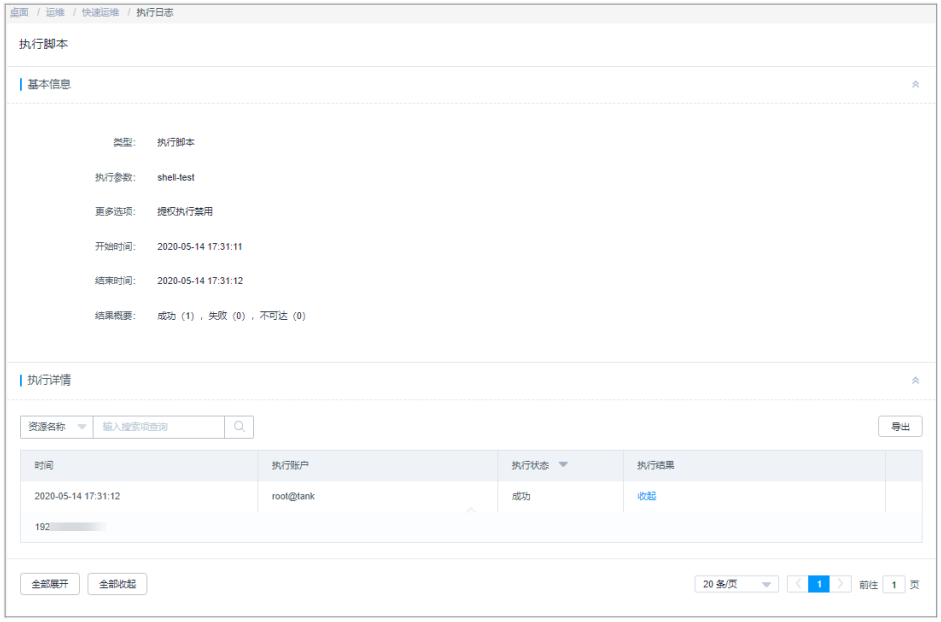
步骤3 查询日志。

在搜索框中输入关键字，根据执行参数，快速查询目标执行日志。

步骤4 查看执行日志详情。

1. 选择目标执行日志，单击“管理”，进入“执行日志详情”页面。

图 9-23 执行日志详情页面



2. 在“基本信息”区域，可查看运维任务执行基本信息和简要结果。
3. 在“执行详情”区域，可查看运维任务执行详细结果。
4. 在“执行详情”区域，单击“导出”，可下载当前运维任务执行详细结果。

步骤5 下载执行日志。

选择目标执行日志，在相应“操作”列单击“导出”，可立即下载当前执行日志CSV格式文件保存到本地。

步骤6 删除执行日志。

- 选择目标执行日志，在相应“操作”列单击“删除”，可删除该执行日志。
- 同时勾选多条日志记录，单击列表下方的“删除”，可以批量删除多个执行日志。

----结束

9.6 运维任务

9.6.1 新建运维任务

堡垒机支持自动运维任务功能，用户可按步骤自动执行命令和脚本方式运维多个目标资源，并可设置自动执行步骤将系统磁盘文件或本地文件快速上传到多个目标主机路径。此外，可设置执行周期和时间定期执行任务，并可同时执行多种任务步骤类型，实现多台资源设备自动化运维，提高运维效率。

- 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。

约束限制

- 仅**专业版**堡垒机支持快速运维功能。
- 仅支持对Linux主机（SSH协议类型）资源执行自动运维任务。
- 暂不支持对Windows主机资源、数据库资源和应用资源执行自动运维任务。
- 运维任务仅能由个人账户管理，不能被系统内其他用户管理。

前提条件

- 已获取“运维任务”模块管理权限。
- 已获取资源访问控制权限，即已配置访问控制策略或访问授权工单已审批通过。
- 资源主机网络连接正常。

新建自动运维任务

步骤1 登录堡垒机系统。

步骤2 选择“运维 > 运维任务 > 任务列表”，进入运维任务列表页面。

步骤3 单击“新建”，弹出新建运维任务窗口。

步骤4 配置任务基本信息。

表 9-16 运维任务基本信息参数说明

参数	说明
任务名称	自定义的运维任务名称，系统内“任务名称”不能重复。
执行方式	选择运维任务执行的方式，包括“手动执行”、“定时执行”、“周期执行”。 “定时执行”和“周期执行”需同时配置动作执行时间或周期。 ● 手动执行：手动触发执行任务。 ● 定时执行：定期自动触发执行任务。仅执行一次。 ● 周期执行：周期自动触发执行任务。可按周期执行多次。
执行时间	定期执行任务的日期。默认执行时刻为日期的凌晨零点。
执行周期	执行周期同步，需输入任务执行周期。 ● 可选择每分钟、每小时、每天、每周、每月。 ● 需同时选择“结束时间”，否则将无限期按周期执行任务。
更多选项	（可选）用户对资源账户执行任务权限不够时，需勾选上“提权执行”，用户需在该主机资源的Sudoers文件下执行任务。
任务描述	简要描述运维任务信息。

步骤5 单击“下一步”，配置执行账户或账户组，选择已创建的SSH协议类型资源账户或账户组。

步骤6 单击“下一步”，配置任务步骤。

1. 单击“添加任务步骤”，选择添加任务类型“执行命令”、“执行脚本”或“传输文件”。
2. 选择一个或多个任务类型，并配置任务参数。

   说明

   运维任务步骤数不限制，一个任务可添加多个执行步骤。

步骤7 单击“确定”，返回任务列表页面，查看新建的运维任务。

任务执行完成后，可以**下载执行日志**，获取任务执行结果。

----结束

后续管理

运维任务创建完成后，可在任务列表页面，管理已创建任务，包括管理关联执行账户、删除任务 、启停任务、立即执行任务等。

- 若需补充关联执行账户，可单击“关联”，快速关联执行账户、账户组。
- 若需删除任务，可一个或多个选择目标任务，单击“删除”，立即删除任务。
- 若需禁用任务的周期执行，可勾选一个或多个“已启用”状态的任务，单击“禁用”，任务状态变更为“已禁用”，任务立即失效。
- 若需立即执行任务，可单击“立即执行”，立即执行运维任务。

  说明

  任务执行过程中，按照任务步骤依次执行。当一个任务步骤被中断或所选资源不可达时，后续任务步骤将被终止不再执行。

9.6.2 查询和修改运维任务

若运维任务有变更，例如需运维步骤变化等。可查看和修改已创建的任务配置，包括修改任务基本信息、修改任务步骤、修改执行日期、修改执行周期、修改执行账户或账户组等。

前提条件

- 已获取“运维任务”模块管理权限。
- 已获取资源访问控制权限，即已配置访问控制策略或访问授权工单已审批通过。

查看和修改任务配置

步骤1 登录堡垒机系统。

步骤2 选择“运维 > 运维任务 > 任务列表”，进入运维任务列表页面。

步骤3 查询运维任务。

- 快速查询

  在搜索框中输入关键字，根据任务名称、资源名称、执行账户等快速查询任务。
- 高级搜索

  在相应属性搜索框中分别输入关键字，精确查询任务。

步骤4 单击目标任务名称，或者单击“管理”，进入任务详情页面。

步骤5 查看和修改任务基本信息。

在“基本信息”区域，单击“编辑”，弹出基本信息编辑窗口，即可修改任务的基本信息。

- 可修改信息包括“任务名称”、“执行方式”等。

步骤6 查看和修改任务执行账户。

- 在“执行账户”区域，单击“编辑”，弹出执行账户编辑窗口，可立即添加或移除执行账户。
- 在相应资源账户行，单击“移除”，可立即取消对该资源账户的执行。

步骤7 查看和修改执行账户组。

- 在“执行账户组”区域，单击“编辑”，弹出执行账户组编辑窗口，可立即添加或移除执行账户组。
- 在相应账户组行，单击“移除”，可立即取消对该组中资源账户的执行。

步骤8 查看和修改任务步骤。

- 在“任务步骤”区域，单击“添加”，弹出任务步骤添加窗口，可立即添加任务步骤。
- 在相应步骤行，单击“编辑”，弹出任务步骤编辑窗口，可修改任务步骤内容。
- 在相应步骤行，单击“移除”，可立即取消对该步骤的执行。

步骤9 查看执行历史记录。

- 在相应历史记录行，单击“查看”，弹出执行结果窗口，可查看详细任务步骤执行结果。
- 在相应历史记录行，单击“导出”，可立即下载当前执行结果记录。

----结束

9.6.3 管理运维任务执行日志

运维任务执行完成后生成执行日志，执行日志中可查看任务执行结果，包括执行结果信息、执行详情等。

本小节主要介绍如何管理执行日志，包括查看执行日志、下载执行日志、删除日志等。

前提条件

已获取“运维任务”模块管理权限。

查看日志详情

步骤1 登录堡垒机系统。

步骤2 选择“运维 > 运维任务 > 执行日志”，进入任务日志列表页面。

步骤3 查询执行日志。

快速查询：在搜索框中输入关键字，根据运维任务名称快速查询任务。

步骤4 选择目标任务，在相应“操作”列单击“详情”，进入日志详情页面。

- 在“基本信息”区域，可查看运维任务执行基本信息和简要结果。
- 在“执行详情”区域，可查看和导出运维任务执行详细结果。

----结束

下载执行日志

步骤1 登录堡垒机系统。

步骤2 选择“运维 > 运维任务 > 执行日志”，进入任务日志列表页面。

步骤3 选择目标任务，在相应“操作”列单击“导出”，立即下载执行日志CSV格式文件保存到本地。

步骤4 单击“查看”，进入“任务详情”页面。

可查看运维任务执行基本信息和简要结果，并可在“执行详情”区域，查看和导出运维任务执行详细结果。

步骤5 单击“导出”，可下载当前执行日志CSV格式文件保存到本地。

步骤6 单击“删除”，可删除该执行日志。

同时勾选多条日志记录，单击列表下方的“删除”，可以批量删除多个执行日志。

----结束

删除执行日志

步骤1 登录堡垒机系统。

步骤2 选择“运维 > 运维任务 > 执行日志”，进入任务日志列表页面。

步骤3 选择目标任务，在相应“操作”列单击“删除”，即可删除该执行日志。

步骤4 同时勾选多条执行日志，单击列表下方的“删除”，可以批量删除多个执行日志。

----结束

10 系统工单

10.1 工单配置管理

10.1.1 配置工单模式

系统工单模式是指用户在申请资源访问权限时，可通过工单申请资源的范围，以及提交工单的方式。

- “基本模式”通过选择资源范围，简单限定访问控制工单申请范围；同时通过选择工单提交方式，可指定命令控制工单的提交方式。
- “高级模式”针对访问授权工单，从用户部门、用户角色、资源部门多维度限定用户可访问资源的范围。
  - 配置用户部门后，该部门内的用户即形成用户池，只有用户池的用户才能申请资源池中的资源。
  - 如果未配置用户角色，则用户池内所有角色的用户均可申请资源池中的资源。
  - 如果配置了用户角色，则用户池中只有相应角色的用户才能申请资源池中的资源。
- 用户池指根据用户部门、用户角色限制的用户范围。关联部门或角色后，该部门或角色的用户能够申请资源池内资源。
- 资源池指根据资源部门限定的资源范围。关联的部门之后，该部门的资源能够被用户池内的用户申请。

前提条件

已获取“系统”模块管理权限。

配置基本工单模式

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统配置 > 工单配置”，进入系统工单配置管理页面。

步骤3 在“基本模式”区域，单击“编辑”，弹出基本工单模式配置窗口。

设置用户可以查看的资源范围，以及命令授权工单的提交方式。

表 10-1 基本模式参数说明

参数	说明
访问授权工单申请范围	选择访问控制工单可申请资源范围。 ● 本部门（默认）：申请访问控制工单时，运维人员可申请本部门资源的访问控制权限，不包括下级部门的资源。 ● 本部门及下级部门：申请访问控制工单时，运维人员可申请本部门及下级部门资源的访问控制权限。 ● 全部：运维人员可申请系统全部资源的访问控制权限。
命令授权工单提交方式	选择命令授权工单提交方式，可选择手动提交或自动提交。 ● 手动提交（默认）：触发生成命令控制工单后，需运维人员提交工单至管理员处审批。 ● 自动提交：触发生成命令控制工单后，自动提交至管理员处审批。
命令授权工单生效时间	设置命令授权工单的生效时间，有效值1-10080，单位：分钟。

步骤4 单击“确定”，返回工单配置管理页面，可查看已配置的基本工单模式配置。

----结束

配置高级工单模式

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统配置 > 工单配置”，进入系统工单配置管理页面。

步骤3 在“高级模式”区域，单击“添加”，弹出高级工单模式配置窗口。

步骤4 配置用户池。

选择用户部门或用户角色。

步骤5 单击“下一步”，配置资源池。

步骤6 单击“确定”，返回系统工单配置管理页面，查看高级模式配置。

----结束

后续管理

- 若需修改高级模式资源池和用户池，可单击“编辑”，在弹出的高级模式编辑窗口重新选择用户或资源范围。
- 若不再需要该高级模式限制 ，可单击“删除”。删除后认证信息不能找回，请谨慎操作。

10.1.2 配置工单审批流程

系统工单审批流程是指用户提交工单后，工单审批通过的策略。可从审批流程方式、审批形式、审批节点、审批级数、终审节点等维度，自定义系统工单审批流程，加强对工单审批流程的管理。

- 审批流程

  包括分级流程和固定流程。分级流程适用于部门内部审批的场景，固定流程适用于跨部门审批的场景。

- 审批形式

  审批环节中多名审批人时，审批通过方式包括多人审批和会签审批。多人审批是任意一名审批人同意，即审批通过；会签审批是需所有审批人同意，审批才通过。

- 审批节点

  审批环节中审批人的属性，包括部门和角色属性，符合部门和角色要求的部门管理员拥有审批权限。

- 审批级数

  审批环节的数量，选择分级流程后必须确定审批级数。

- 终审节点

  各级审批环节后，由系统管理员**admin**进行最终审批的一个环节。

本小节主要介绍如何配置系统工单审批流程。

前提条件

已获取“系统”模块管理权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统配置 > 工单配置”，进入系统工单配置管理页面。

步骤3 在“审批流程”区域，单击“编辑”，弹出审批流程配置窗口。

配置审批流程的各项参数。

表 10-2 工单审批流程参数说明

参数	说明
审批流程	选择审批流程方式，可选择“分级流程”和“固定流程”。 配置工单审批流程后，工单将由各级审批人进行逐级审批。若其中一级审批环节没有符合要求的审批人，则默认此环节已批准，工单流转至下一审批环节。 ● 分级流程（默认）：按照审批级数逐级进行审批。 ● 固定流程：按照固定审批节点进行审批。 **说明** 若您想通过邮件通知到审批人工单的提交情况需进行以下两个操作： – 参考**配置邮件外发**章节设置一个外发邮箱，并确保邮件可以正常发送。 – 参考**配置告警等级**章节，在“工单”页签将需要通知的操作设置为“高”告警等级。
审批形式	选择审批形式，可选择“多人审批”和“会签审批”。 ● 默认为多人审批形式。 ● 多人审批：同级节点仅需一个审批人进行批准，即可通过审批。审批通过后，同级其他审批人也不会看到该工单。如果同级的任意一个审批人驳回，则审批不通过。 ● 会签审批：同级节点所有审批人都审批通过，工单才进入下一级审批。任意一个审批人驳回，则审批不通过。 ● 审批过程中admin账户可在任意节点审批所有工单，且审批结果为最终结果。
审批节点	设置节点审批人属性，需同时设置部门属性和角色属性。 设置完成后，符合部门和角色要求的用户自动成为节点审批人。如果没有符合部门和角色要求的用户，则自动向上级部门内寻找，直到找到“总部”为止。 ● 部门属性：“用户所属部门”为工单申请人所属部门的管理员；“资源所属部门”为工单申请资源所属部门的管理员。 ● 角色属性：需要拥有管理员和工单审批权限的角色，默认为部门管理员。
审批级数	设置审批环节数量，选择“分级流程”后必须配置工单通过审批所需的最大级数。 ● 最多可设置5层审批节点。 ● 默认为1，则需要一个审批环节进行审批。
终审节点	选择开启或关闭系统管理员**admin**终审，默认  。 ● ，表示关闭**admin**终审环节。 ●  ，表示启用**admin**终审环节，所有环节审批人通过审批后，还需**admin**进行最终审批。 **说明** 极端情况下，所有审批环节都没有符合要求的审批人，那么无论是否开启终审，都需**admin**审批工单。

步骤4 单击“确定”，返回系统工单配置管理，可查看已配置的审批流程。

----结束

10.2 新建访问授权工单

当运维用户不具备某些资源访问控制权限时，可主动提交工单，申请相应资源访问控制权限。

前提条件

已获取“访问授权工单”模块管理权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“工单 > 访问授权工单”，进入访问授权工单列表页面。

步骤3 单击“新建”，弹出新建访问授权工单窗口。

配置访问授权工单基本信息。

表 10-3 访问授权工单基本信息说明

参数	说明
运维时间	选择访问资源的时间段，生效时间和失效时间均必须配置。
文件传输	在运维过程中文件传输权限，包括上传和下载文件权限。
更多选项	在Web浏览器运维过程中，会话窗口功能选项。 ● 文件管理：管理文件或文件夹的权限。若需文件上传下载权限，必须同时配置文件管理权限。 ● 上行/下行剪切板：运维会话RDP剪切板的功能。 ● 显示水印：运维会话窗口显示用户登录名水印的功能。 ● 键盘审计：对键盘输入的信息进行记录。
工单备注	（可选）简要描述申请资源访问控制权限的原因或其他信息。

步骤4 单击“下一步”，选择待访问资源账户。

步骤5 单击“确定”，提交工单申请，返回工单列表页面。

管理员审批工单后，即可拥有资源的访问控制权限。

----结束

后续管理

- 提交工单申请后，相关管理员即可在“消息中心”收到提醒，查看详细工单内容。并可在工单审批页面收到工单，可对工单进行批准或驳回操作。

- 提交工单申请后，若需修改已提交的工单，可单击“撤回”，取消已提交的工单申请，工单状态变为“已撤回”。
- 创建工单后，若需查看工单和修改工单信息，可单击“管理”，进入工单详情页面查看和修改工单信息。

  说明

  “审批中”状态的工单仅能查看工单详情信息，不能修改工单内容。“已撤回”和“待提交”状态的工单才能被修改。
- 若已提交的工单已过期，可单击“删除”，管理工单列表。亦可勾选多条工单，单击列表左下角删除，批量删除工单。

注意

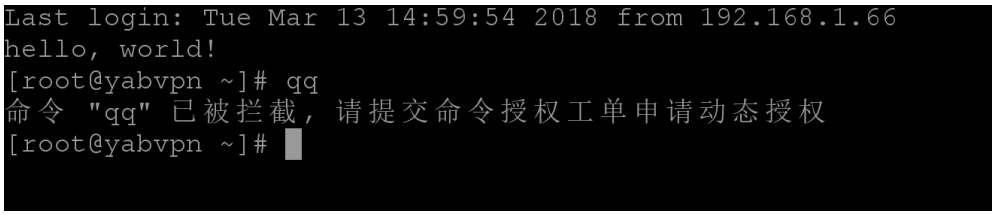
删除后工单信息不能找回，请谨慎操作。

10.3 命令授权工单管理

堡垒机支持对Linux主机操作进行“动态授权”管理，加强对敏感操作的限制管理。

当运维用户登录Linux主机进行运维操作时，触发“动态授权”命令控制策略的操作命令，系统会自动拦截操作命令，生成命令授权工单。管理员将会收到工单审批申请。当管理员用户批准工单后，运维用户才有执行该Linux“动态授权”操作命令的权限。

图 10-1 命令被拦截示例



本小节主要介绍如何管理命令控制工单。

约束限制

仅SSH和Telnet协议类型的Linux主机，支持拦截敏感操作生成工单。

前提条件

- 已获取“命令授权工单”模块管理权限。
- 已触发命令拦截，生成命令授权工单。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“工单 > 命令授权工单”，进入命令授权工单列表页面。

图 10-2 命令授权工单

步骤3 提交工单。

命令授权工单可通过“自动提交”和“手动提交”。工单提交方式说明请参见**配置工单基本模式**。

- 若为自动提交方式，则由系统自动提交工单给管理员审批。
- 若为手动提交方式，则需运维用户在工单列表页面，单击指定工单“操作”列的“提交”，手动提交工单给管理员审批。
- 若工单被管理员驳回，可修改工单信息后再次提交工单。

步骤4 撤回工单。

单击指定工单“操作”列的“撤回”，即可取消已提交的工单申请，工单状态变为“已撤回”。

步骤5 修改工单信息。

- 单击“管理”，进入工单详情页面，即可查看工单基本信息。
- 单击工单详情页面编辑，即可修改工单授权运维时间。

说明

“审批中”状态的工单仅能查看工单详情信息，不能修改工单内容。“已撤回”和“待提交”状态的工单才能被修改。

步骤6 删除工单。

- 单击指定工单“操作”列的“删除”，可以删除该工单。
- 同时勾选多个工单，单击列表下方的“删除”，批量删除多个工单。

注意

删除后工单信息不能找回，请谨慎操作。

----结束

后续管理

- 运维用户提交工单后，相关管理员即可在“消息中心”收到提醒，查看详细工单内容。并可在工单审批页面收到工单，可对工单进行批准或驳回操作。
- 相关管理员审批工单通过后，运维用户权限立刻生效，即可在授权范围和时间段拥有命令操作权限。
- 相关管理员撤销工单权限后，运维用户权限立刻失效，操作命令会再次被拦截。

10.4 数据库授权工单管理

堡垒机支持对数据库操作进行“动态授权”管理，加强对数据库关键操作的限制管理。

当运维用户登录数据库进行运维操作时，触发“动态授权”数据库控制策略的操作命令，系统会自动拦截操作命令，生成数据库授权工单。管理员将会收到工单审批申请。当管理员用户批准工单后，运维用户才有执行该数据库“动态授权”操作命令的权限。

本小节主要介绍如何管理数据库授权工单。

约束限制

- 仅**专业版**实例支持数据库运维操作审计。
- 仅针对MySQL和Oracle类型数据库，支持拦截敏感操作生成工单。
- 数据库授权工单由运维用户触发命令策略，自动创建，不能手动创建。

前提条件

- 已获取“数据库授权工单”模块管理权限。
- 已触发操作拦截，生成数据库授权工单。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“工单 > 数据库授权工单”，进入数据库授权工单页面。

图 10-3 数据库授权工单列表

步骤3 提交工单。

- 单击指定工单“操作”列的“提交”，手动提交工单给管理员审批。
- 若工单被管理员驳回，可修改工单信息后再次提交工单。

步骤4 撤回工单。

单击指定工单“操作”列的“撤回”，即可取消已提交的工单申请，工单状态变为“已撤回”。

步骤5 修改工单信息。

- 单击“管理”，进入工单详情页面，即可查看工单基本信息。

- 单击工单详情页面编辑，即可修改工单授权运维时间。

说明

“审批中”状态的工单仅能查看工单详情信息，不能修改工单内容。“已撤回”和“待提交”状态的工单才能被修改。

步骤6 删除工单。

- 单击指定工单“操作”列的“删除”，可以删除该工单。
- 同时勾选多个工单，单击列表下方的“删除”，批量删除多个工单。

注意

删除后工单信息不能找回，请谨慎操作。

----结束

后续管理

- 运维用户提交工单后，相关管理员即可在“消息中心”收到提醒，查看详细工单内容。并可在工单审批页面收到工单，可对工单进行批准或驳回操作。
- 相关管理员审批工单通过后，运维用户权限立刻生效，即可在授权范围和时间段拥有操作权限。
- 相关管理员撤销工单权限后，运维用户权限立刻失效，操作命令会再次被拦截。

10.5 审批系统工单

运维用户提交工单申请或者触发命令工单后，工单流转到系统指定的审批人处。审批人可在“消息中心”收到工单审批提醒，此时可在工单审批列表中查看到待审批的工单。

本小节主要介绍如何管理已提交审批工单，包括查看工单详情、审批工单、驳回工单、撤销工单授权等。

前提条件

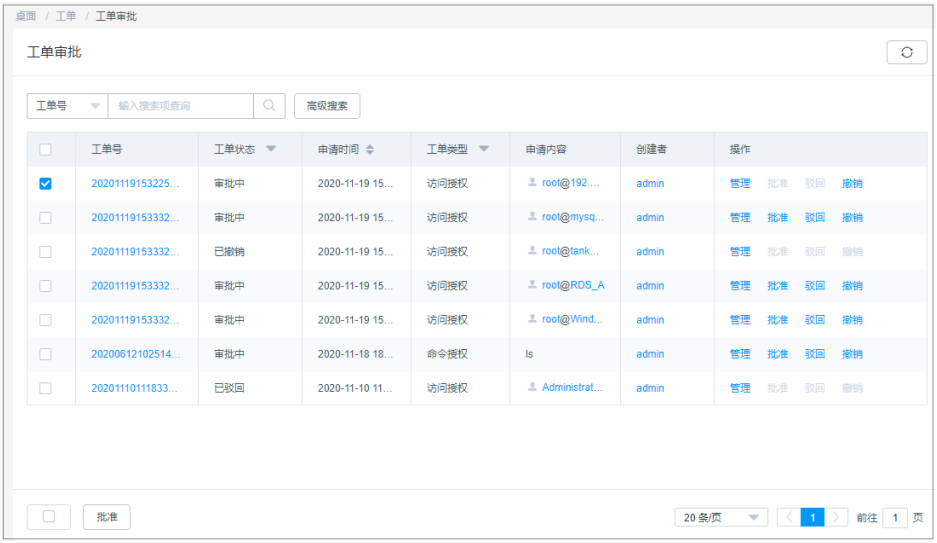
已获取“工单审批”模块管理权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“工单 > 工单审批”，进入审批工单列表页面。

图 10-4 审批工单列表



步骤3 查看工单详情。

单击目标工单“操作”列的“管理”，进入工单详情页面，即可查看工单详细信息，包括工单基本信息、资源账户列表、审批人列表。

图 10-5 查看工单详细信息

步骤4 批准工单。

- 单击目标工单“操作”列的“批准”，即可通过该工单审批。
- 勾选多个工单，单击列表左下角批准，即可批量通过。

步骤5 驳回工单。

单击目标工单“操作”列的“驳回”，即可取消申请的工单。

步骤6 撤销工单。

工单被批准后，单击目标工单“操作”列的“撤销”，即可收回资源的授权。

----结束

10.6 系统工单应用示例

示例一：按用户所属部门申请资源，建立分级流程工单

前提条件

- 已完成部门、用户、角色和资源等项的规划和设置。部门设置请参考**部门**，用户和角色设置请参考**用户**，资源设置请参考**资源**。
- 工单审批流程设置如**表10-4**所示，具体操作请参考**工单配置**。

表 10-4 工单配置参数说明

参数	值
审批流程	分级流程
审批形式	多人审批
审批节点	用户所属部门-部门管理员
审批级数	3

审批流程

用户提起工单电子流，按用户所属部门申请访问资源。

大队管理员User A和User B均拥有审批权，只要任意一人批准，则该环节审批通过，任意一人驳回，则该环节审批不通过。大队管理员审批通过后，下一环节将由村管理员User C进行审批。以此类推，直到镇管理员User D审批通过后，用户即可获得相应的权限。审批过程中任意一个环节驳回，则该工单审批不通过，用户不能获得相应的权限。

说明

拥有admin管理员权限的账号可在任意节点审批或驳回任意工单，且结果为最终结果。

示例二：按资源所属部门申请资源，建立分级流程工单

前提条件

- 已完成部门、用户、角色和资源等项的规划和设置。部门设置请参考**部门**，用户和角色设置请参考**用户**，资源设置请参考**资源**。
- 工单审批流程设置如**表10-5**所示，具体操作请参考**工单配置**。

表 10-5 工单配置参数说明

参数	值
审批流程	分级流程
审批形式	多人审批
审批节点	用户所属部门-部门管理员
审批级数	3

审批流程

用户提起工单电子流，按资源所属部门申请访问资源。

镇管理员User D进行审批，审批通过则由县管理员User E进行下一环节的审批，审批不通过则工单被驳回。以此类推，直到市管理员User F审批通过后，用户即可获得相

应的权限。审批的过程中任意一个环节驳回，则该工单审批不通过，用户不能获取相应的权限。

说明

拥有admin管理员权限的账号可在任意节点审批或驳回任意工单，且结果为最终结果。

示例三：建立固定流程的会签审批工单

前提条件

- 已完成部门、用户、角色和资源等项的规划和设置。部门设置请参考**部门**，用户和角色设置请参考**用户**，资源设置请参考**资源**。
- 工单审批流程设置如**表10-6**所示，具体操作请参考**工单配置**。

表 10-6 工单配置参数说明

参数	内容
审批流程	固定流程
审批形式	会签审批
审批节点	3

签核流程

用户提起工单电子流，申请访问非用户所属部门的资源。

工程部管理员User B和User C均拥有审批权，两者都批准则该环节审批通过，任意一人驳回则该环节审批不通过。工程部管理员审批通过后，下一环节将由财务部管理员User D进行审批，以此类推，直到财务部管理员User E审批通过后，用户即可获得相应的权限。审批过程中任意一个环节驳回，则该工单审批不通过，用户不能获取相应的权限。

说明

拥有admin管理员权限的账号可在任意节点审批或驳回任意工单，且结果为最终结果。

11 运维审计

11.1 实时会话

11.1.1 查看实时会话

运维人员通过堡垒机登录资源后，审计管理员将会实时收到会话记录，通过实时会话查看正在进行的运维会话，以免运维违规操作造成损失。

前提条件

- 已获取“实时会话”模块管理权限。
- 有正在进行中运维会话。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“审计 > 实时会话”，进入实时会话列表页面。

步骤3 查询实时会话。

- 快速查询

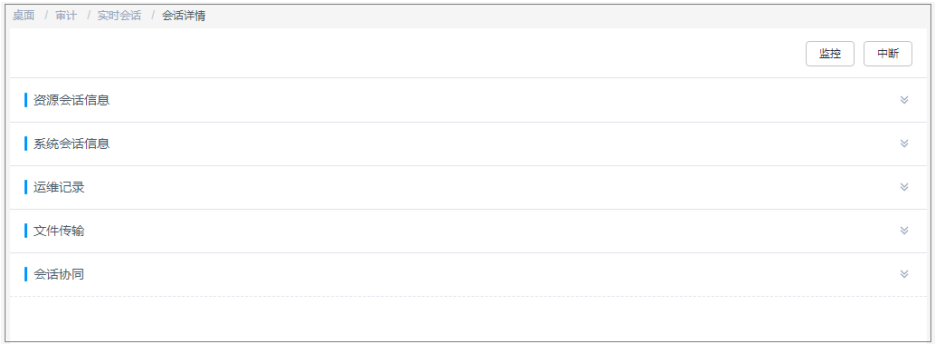
  在搜索框中输入关键字，根据资源名称、资源账户、用户、来源IP等快速查询实时会话。

- 高级搜索

  在相应属性搜索框中分别输入关键字，精确查询实时会话。

步骤4 单击目标实时会话“操作”列的“详情”，进入实时会话详情页面。

图 11-1 查看实时会话



步骤5 可分别查看资源会话信息、系统会话信息、运维操作记录、文件传输记录、会话协同记录等。

----结束

11.1.2 监控实时会话

运维人员通过堡垒机登录资源后，审计管理员将会实时收到会话记录。通过实时会话，可监控正在进行的运维会话，实时监督用户正在进行的操作。

前提条件

- 已获取“实时会话”模块管理权限。
- 有正在进行中运维会话。
- 目前仅支持H5运维会话和SSH客户端的会话，其它会话暂不支持 。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“审计 > 实时会话”，进入实时会话列表页面。

步骤3 单击目标实时会话“操作”列的“监控”，跳转到运维人员运维会话窗口。

步骤4 可查看运维人员实时运维操作，并可分别在会话窗口栏查看历史运维记录、文件传输记录和协同会话参与用户记录。

----结束

11.1.3 中断实时会话

运维人员通过堡垒机登录资源后，审计管理员将会实时收到会话记录。当监控到有违规或高危运维操作时，可通过实时会话阻断会话，阻止运维人员的进一步操作。

前提条件

- 已获取“实时会话”模块管理权限。
- 有正在进行中运维会话。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“审计 > 实时会话”，进入实时会话列表页面。

步骤3 单击目标实时会话“操作”列的“中断”，强制断开会话连接。

中断会话后，运维人员会话页面将被立即断开，并收到会话断开连接提示。

----结束

11.2 历史会话

11.2.1 查看历史会话

运维人员通过堡垒机登录资源运维结束后，审计管理员将会收到历史会话记录。通过历史会话记录，可查询详细的操作记录，在线审计历史会话。

⚠ 注意

审计的视频文件中可能存在敏感数据信息，查看时请注意信息泄露风险。

约束限制

- 通过Web运维支持文本和视频审计。
- 通过SSH客户端运维、客户端文件传输和数据库运维仅支持文本审计，不支持视频审计。
- 不支持记录资源账户自动巡检的登录资源数据。
- 视频仅可回放有效会话记录，即登录资源到最后一次会话操作的这一段记录。

前提条件

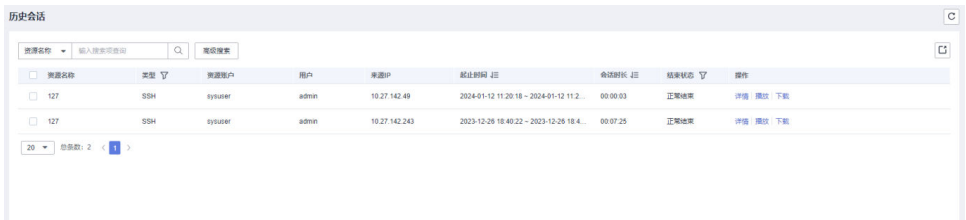
- 已获取“历史会话”模块管理权限。
- 已结束运维会话。

查看历史会话记录

步骤1 登录堡垒机系统。

步骤2 选择“审计 > 历史会话”，进入历史会话列表页面。

图 11-2 历史会话列表



说明

V3.3.42.0及以上版本堡垒机取消了“详情”列的“更多”操作。

步骤3 查询历史会话。

- 快速查询

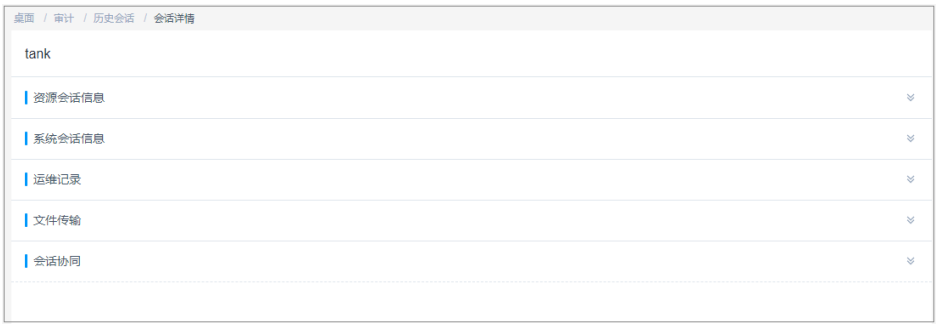
  在搜索框中输入关键字，根据资源名称、资源账户、用户、来源IP等快速查询历史会话。

- 高级搜索

  在相应属性搜索框中分别输入关键字，精确查询历史会话。

步骤4 单击目标历史会话“操作”列的“详情”，进入历史会话详情页面。

图 11-3 查看历史会话



步骤5 可分别查看资源会话信息、系统会话信息、运维操作记录、文件传输记录、会话协同记录等。

主要包含资源名称、类型、主机IP、资源账户、起止时间、会话时长、会话大小、操作用户、操作用户来源IP、操作用户来源MAC、登录方式、运维记录、文件传输记录、会话协同记录等信息。

----结束

在线会话回放

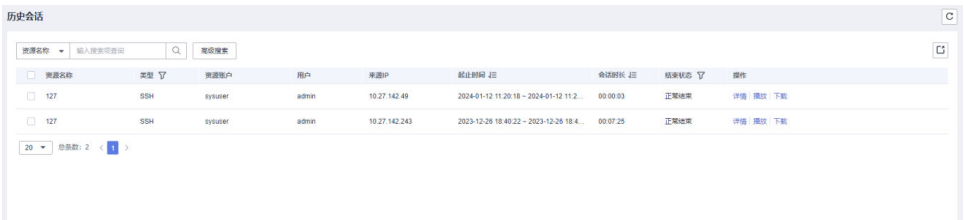
因登出时间和最后操作时间不同，视频文件的总时长与回放可播放时长可能不一致。

- “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。

步骤1 登录堡垒机系统。

步骤2 选择“审计 > 历史会话”，进入历史会话列表页面。

图 11-4 历史会话列表



说明

V3.3.42.0及以上版本堡垒机取消了“详情”列的“更多”操作。

步骤3 单击目标历史会话“操作”列的“播放”，跳转到历史会话窗口。

步骤4 回放会话操作全过程。

- 在会话窗口可查看运维操作的总会话时长，并可拖动播放进度。
- 在会话窗口右侧，可查看运维操作指令记录、传输文件记录、会话协同参与用户、加入实时会话监控用户等信息。

步骤5 跳过空闲播放。

- 开启“跳过空闲”，表示播放历史会话时，将跳过无运维操作的会话回放。
- 默认为关闭。

步骤6 多倍速率播放。

单击“正常速度”，可配置会话多倍速率播放。可分别选择正常速度、2X速度、4X速度、8X速度、16X速度。

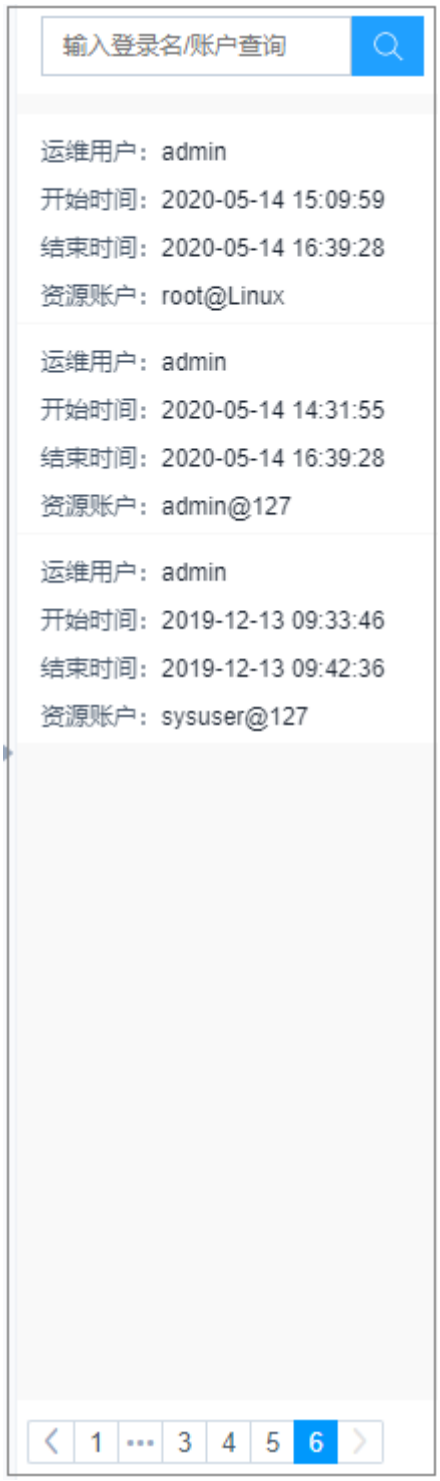
步骤7 会话截屏。

单击，可立即截取播放的会话窗口，生成本地PNG格式快照。

步骤8 会话播放列表。

1. 单击，展开会话窗口右侧的播放列表，可选择播放历史会话。
2. 在搜索框输入登录名或资源账户名，搜索目标历史会话。
3. 单击目标会话，即可立即播放。

图 11-5 历史会话播放列表



----结束

11.2.2 导出历史会话

运维人员通过堡垒机登录资源运维结束后，审计管理员将会收到历史会话记录，并可导出全部历史会话记录，离线审计历史会话。

注意

审计的视频文件中可能存在敏感数据信息，导出时请注意信息泄露风险。

前提条件

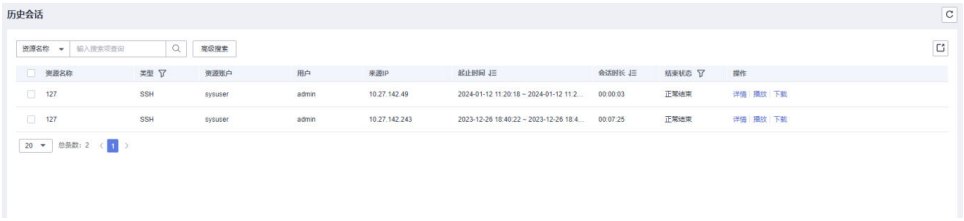
- 已获取“历史会话”模块管理权限。
- 已结束运维会话。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“审计 > 历史会话”，进入历史会话列表页面。

图 11-6 历史会话列表



说明

V3.3.42.0及以上版本堡垒机取消了“详情”列的“更多”操作。

步骤3 （可选）勾选一个或多个历史会话。

若未勾选日志，默认导出全量历史会话。

步骤4 右上角单击  ，任务创建成功，单击“去下载中心”查看打包进度为100%时，单击“操作”列的“下载”，下载文件到本地，打开本地文件，即可查看导出的历史会话信息。

说明

历史会话导出最多同时并行2个任务。

----结束

11.2.3 管理会话视频

运维人员通过堡垒机登录资源运维结束后，审计管理员将会收到历史会话记录。针对Linux命令审计、Windows操作审计全程录像记录，支持生成运维视频，并支持一键下载和删除视频管理。

注意

审计的视频文件中可能存在敏感数据信息，下载时请注意信息泄露风险。

约束限制

- 通过Web运维支持文本和视频审计。
- 通过SSH客户端运维、客户端文件传输和数据库运维仅支持文本审计，不支持视频审计。
- 视频仅可回放有效会话记录，即登录资源到最后一次会话操作的这一段记录。
- 生成视频后，视频将缓存在系统空间，占用系统存储空间，建议及时将视频保存在本地并清理磁盘空间。

前提条件

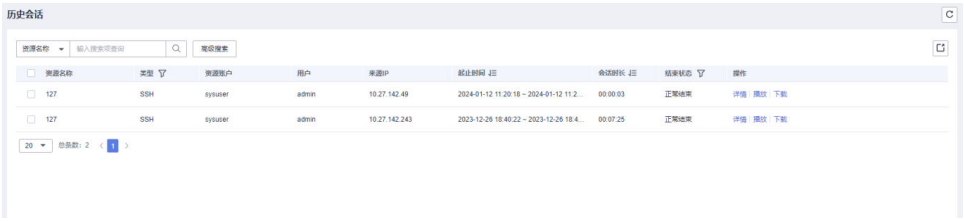
- 已获取“历史会话”模块管理权限。
- 已结束运维会话。

生成会话视频

步骤1 登录堡垒机系统。

步骤2 选择“审计 > 历史会话”，进入历史会话列表页面。

图 11-7 历史会话列表



说明

V3.3.42.0及以上版本堡垒机取消了“详情”列的“更多”操作。

步骤3 在目标历史会话“操作”列，单击“更多 > 生成视频”，系统后台立即启动生成历史会话视频。

“任务中心”提醒有正在执行的任务。当“任务中心”任务执行完成，“消息中心”收到生成会话视频提醒后，会话视频生成完成。

说明

- 在系统存储空间充足条件下，不限制生成视频的时长和大小。
- 当系统存储空间不足时，生成视频可能失败，建议您及时扩大系统盘空间。
- 会话视频可备份至OBS桶，具体操作请参考**配置远程备份至OBS桶**章节。

----结束

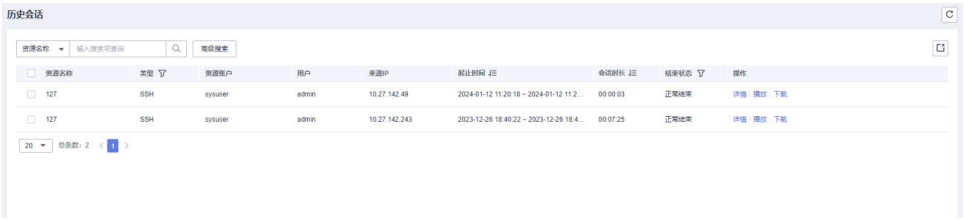
下载会话视频

生成视频后，视频将缓存在系统空间，占用系统存储空间。为节约系统存储空间，可下载视频到本地保存。

步骤1 登录堡垒机系统。

步骤2 选择“审计 > 历史会话”，进入历史会话列表页面。

图 11-8 历史会话列表



说明

V3.3.42.0及以上版本堡垒机取消了“详情”列的“更多”操作。

步骤3 在目标历史会话“操作”列，单击“下载”，即可下载压缩包的文件到本地。

“消息中心”收到下载会话视频完成提醒。

说明

若您需要播放压缩包中会话视频，请按照以下步骤操作：

1. 进入**下载中心**下载“本地播放工具”。
2. 打开本地播放工具，将下载的压缩包拖入播放窗口即可查看。

----结束

11.3 系统日志

11.3.1 查看系统日志

系统日志包括系统登录日志和系统操作日志两部分。系统登录日志指登录堡垒机的所有日志记录，系统操作日志指登录后在堡垒机控制台所有操作的日志记录，包括但不限于对资源账户或用户的新增、删除、修改以及登录行为记录等。

例如运维人员登录堡垒机系统，执行配置权限、审计管理等操作后，审计管理员将会收到系统日志记录。通过系统日志记录，可查询详细的系统登录和操作记录，在线审计系统日志。

前提条件

已获取“系统登录日志”或“系统操作日志”模块管理权限。

查看系统登录日志

步骤1 登录堡垒机系统。

步骤2 选择“审计 > 系统日志”，选择“系统登录日志”页签，进入系统日志列表页面。

说明

在系统操作日志中，运维任务的结果记录的是运维任务是否执行完成，与运维任务内具体命令、脚本等执行结果无关。

步骤3 查询系统登录日志。

- 快速查询

  在搜索框中输入关键字，根据用户、来源IP、日志内容、起止时间等快速查询系统登录日志。

- 高级搜索

  在相应属性搜索框中分别输入关键字，精确查询系统登录日志。

步骤4 根据筛选条件，即可查看到目标登录日志。

----结束

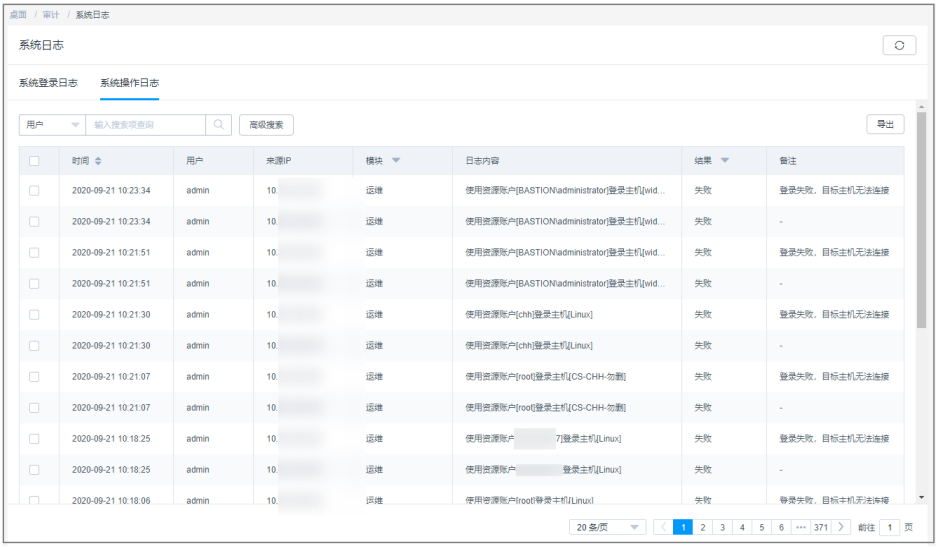
查看系统操作日志

步骤1 登录堡垒机系统。

步骤2 选择“审计 > 系统日志”，进入系统日志列表页面。

步骤3 选择“系统操作日志”页签，进入系统操作日志列表页面。

图 11-9 系统操作日志



步骤4 查询系统操作日志。

- 快速查询

  在搜索框中输入关键字，根据用户、来源IP、日志内容、起止时间等快速查询系统操作日志。

- 高级搜索

  在相应属性搜索框中分别输入关键字，精确查询系统操作日志。

步骤5 根据筛选条件，即可查看到目标操作日志。

----结束

11.3.2 导出系统日志

运维人员登录堡垒机系统，执行配置权限、审计管理等操作后，审计管理员将会收到系统日志记录。通过系统日志记录，可查询详细的系统登录和操作记录，在线审计系统日志。系统日志包括系统登录日志和系统操作日志两部分。

前提条件

已获取“系统登录日志”或“系统操作日志”模块管理权限。

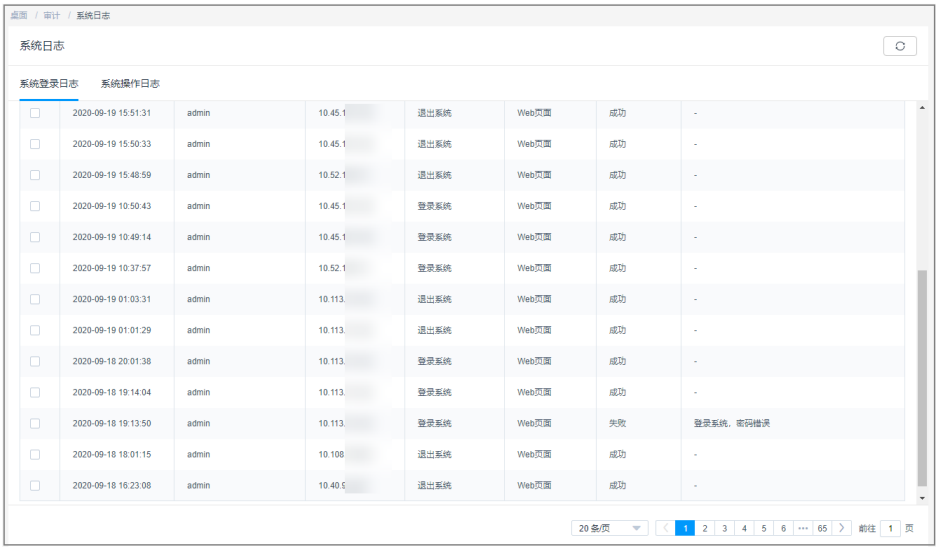
导出系统登录日志

步骤1 登录堡垒机系统。

步骤2 选择“审计 > 系统日志”，进入系统日志列表页面。

步骤3 选择“系统登录日志”页签，单击页面右上角的“导出”，可以导出系统登录日志。

图 11-10 系统登录日志



步骤4 （可选）勾选一个或多个系统登录日志。

若未勾选日志，默认导出全量历史登录日志。

步骤5 右上角单击  ，任务创建成功，单击“去下载中心”查看打包进度为100%时，单击“操作”列的“下载”，下载文件到本地，打开本地文件，即可查看导出的系统登录日志信息。

----结束

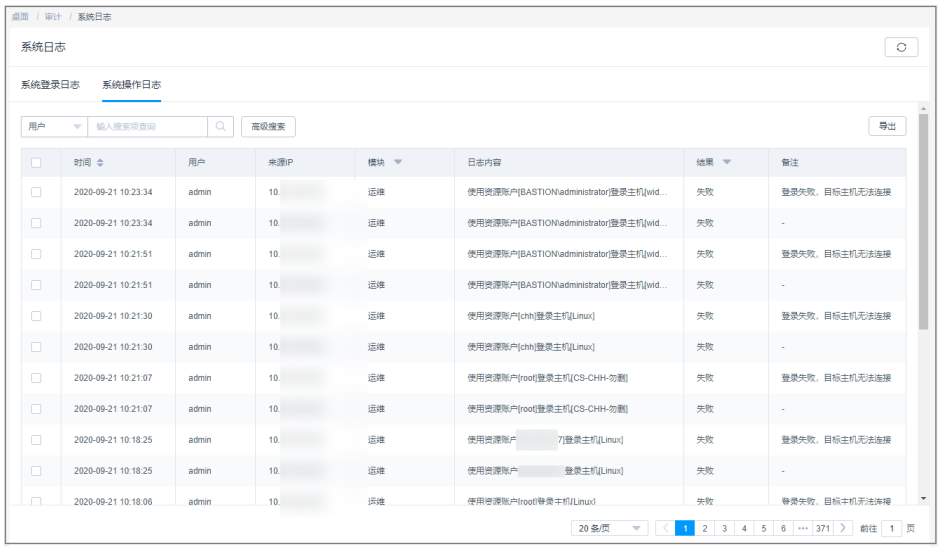
导出系统操作日志

步骤1 登录堡垒机系统。

步骤2 选择“审计 > 系统日志”，进入系统日志列表页面。

步骤3 选择“系统操作日志”页签，进入系统操作日志列表页面。

图 11-11 系统操作日志



步骤4 （可选）勾选一个或多个系统操作日志。

若未勾选日志，默认导出全量历史操作日志。

步骤5 右上角单击  ，任务创建成功，单击“去下载中心”查看打包进度为100%时，单击“操作”列的“下载”，下载文件到本地，打开本地文件，即可查看导出的系统操作日志信息。

说明

操作日志系统生成两条数据，一条为单击导出时触发的创建任务，一条为执行打包的任务，记录打包成功和失败。

----结束

11.4 运维报表

11.4.1 查看运维报表

运维用户通过堡垒机登录资源，以及进行运维操作后，审计管理员可查看运维详细报表，主要涵盖“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”等趋势图和详细数据。

约束限制

- 趋势图最多呈现连续180天的运维数据变化趋势。
  - 默认按小时呈现当天运维数据变化趋势。
  - 筛选周期时间在同一月且在同一周时，仅可选择按天呈现趋势图。
  - 筛选周期时间跨月且在同一周时，可选择按天和按月呈现趋势图。
  - 筛选周期时间在同一月且跨周时，仅可选择按天和按周呈现趋势图。
  - 筛选周期时间跨月且跨周时，仅可选择按天、按周和按月呈现趋势图。

- 趋势图可选择线状图、柱状图、饼状图形式。
  -  表示线状图形式。
  -  表示柱状图形式。
  - 仅命令拦截动作趋势图可呈现饼状图形式。
- 默认呈现运维时间段内总的趋势图。
  - 支持按目标用户呈现运维统计趋势图，最多可选择5个目标用户。
  - 支持按目标资源呈现运维统计趋势图，最多可选择5个目标资源。

前提条件

已获取“运维报表”模块管理权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“审计 > 运维报表”，进入系统报表查看页面。

步骤3 单击各运维统计数据页签，查看各运维统计数据及趋势的详细信息。

详细介绍请参见如下说明。

----结束

运维时间分布

呈现用户登录资源情况分布或资源被登录分布情况，默认按小时呈现当天运维数据变化趋势。

在“详细数据”区域，可查看会话起止时间、用户登录名、资源名称、协议类型、资源账户等信息。

资源访问次数

呈现用户或资源所属历史会话的数量，默认按小时呈现当天运维数据变化趋势。

在“详细数据”区域，可查看会话起止时间、用户登录名、资源名称、协议类型、资源账户等信息。

会话时长

呈现用户或资源所属历史会话的会话时长，默认按小时呈现当天运维数据变化趋势。

在“详细数据”区域，可查看会话起止时间、用户登录名、资源名称、协议类型、资源账户、会话时长等信息。

来源 IP 访问数

呈现用户或资源所属会话的不同来源IP数量，默认按小时呈现当天运维数据变化趋势。

在“详细数据”区域，可查看会话起止时间、用户登录名、资源名称、协议类型、资源账户、来源IP等信息。

会话协同

呈现用户或资源所属会话的协同参与运维用户的数量，默认按小时呈现当天运维数据变化趋势。

在“详细数据”区域，可查看会话起止时间、用户登录名、资源名称、协议类型、资源账户、协同用户登录名等信息。

双人授权

呈现用户或资源所属会话通过双人授权的数量，默认按小时呈现当天运维数据变化趋势。

在“详细数据”区域，可查看授权时间、用户登录名、资源名称、协议类型、资源账户、双人授权用户登录名等信息。

命令拦截

呈现用户或资源所属会话触发的拦截的命令数量，默认按小时呈现当天运维数据变化趋势。

拦截命令类型包括断开连接、拒绝执行、动态授权。

在“详细数据”区域，可查看操作执行时间、用户登录名、资源名称、协议类型、资源账户、操作指令、执行动作等信息。

字符命令数

呈现用户或资源所属会话执行的字符命令数量，默认按小时呈现当天运维数据变化趋势。

在“详细数据”区域，可查看操作执行时间、用户登录名、资源名称、协议类型、资源账户、操作指令等信息。

传输文件数

呈现用户或资源所属会话上传、下载文件的数量，默认按小时呈现当天运维数据变化趋势。

在“详细数据”区域，可查看文件操作时间、用户登录名、资源名称、协议类型、资源账户、操作类型、文件名称等信息。

11.4.2 推送运维报表

为方便审计管理员及时获取运维统计信息，可通过邮件发送运维报表。

- 自发送周期可选择每日、每周、每月。
- 报表格式可选择PDF、DOC、XLS、HTML。
- 每次推送最多可呈现连续180天的运维统计数据。

前提条件

- 已获取“运维报表”模块管理权限。
- 已完成**配置邮件外发**配置。

手动导出

步骤1 登录堡垒机系统。

步骤2 选择“审计 > 运维报表”，进入系统报表查看页面。

步骤3 单击右上角的“报表导出”，弹出运维报表导出配置窗口。

步骤4 配置运维报表推送方式、时间和文件格式。

表 11-1 导出运维报表参数说明

参数	说明
展示粒度	选择运维报表趋势图呈现粒度。 可以选择“按小时”、“按天”、“按周”、“按月”。
时间	选择运维报表统计数据时间范围。 • 需同时选择起始时间和结束时间。 • 最长可选择连续的180天。
报表类型	选择运维报表需呈现统计数据类型。
文件格式	选择报表的文件格式，仅可选择一种格式。 • 默认导出DOC文件格式。 • 可选择PDF、DOC、XLS、HTML格式。

步骤5 单击“确定”，立即导出运维报表。

----结束

自动发送

步骤1 登录堡垒机系统。

步骤2 选择“审计 > 运维报表”，进入系统报表查看页面。

步骤3 单击右上角的“报表自动发送”，弹出报表推送配置窗口。

步骤4 配置报表推送方式、时间和文件格式。

表 11-2 自动发送运维报表参数说明

参数	说明
状态	选择开启或关闭自动推送上一周期报表，默认。 • ，表示关闭自动推送报表。 •  ，表示开启以邮件方式发送上一周期的报表至当前用户邮箱。

参数	说明
发送周期	选择报表发送周期。 ● 默认为目标日期的零点发送报表。 ● 可以按每日、每周、每月周期进行发送。 ● 每日发送的报表中展示粒度为按小时。 ● 每周发送的报表中展示粒度为按天。 ● 每月发送的报表中展示粒度为按周。
文件格式	选择报表格式，仅可选择一种格式类型。 ● 默认选DOC格式。 ● 可选择PDF、DOC、XLS、HTML格式。

步骤5 单击“确定”，返回运维报表页面，按期接收到运维报表邮件。

----结束

11.5 系统报表

11.5.1 查看系统报表

运维用户登录堡垒机系统，以及在系统内进行操作后，审计管理员可查看系统详细报表，主要涵盖“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”、“用户状态”等趋势图和详细数据。

约束限制

- 趋势图最多呈现连续180天系统统计数据变化趋势。
  - 默认按小时呈现当天运维数据变化趋势。
  - 运维数据大于30天时，仅可选择按周或按月呈现趋势图。
  - 运维数据小于30天时，可选择按天、按周、按月呈现趋势图。
- 趋势图仅可选择柱状图形式。

前提条件

已获取“系统报表”模块管理权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“审计 > 系统报表”，进入系统报表查看页面。

步骤3 单击各系统统计数据页签，查看各系统统计数及趋势详细信息。

----结束

用户控制

呈现启用和禁用用户操作的数量，默认按小时呈现当天系统数据变化趋势。

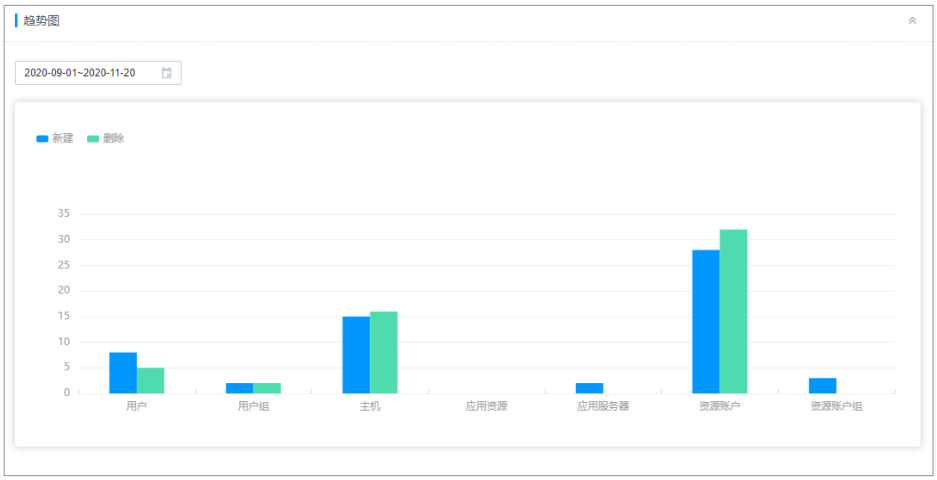
在“详细数据”区域，可查看操作时间、操作用户登录名、来源IP、操作、操作结果等信息。

用户与资源操作

呈现用户、用户组、主机、应用、应用服务器、资源账户、账户组的新建和删除操作的数量，默认呈现当天系统数据变化趋势。

在“详细数据”区域，可查看操作时间、操作用户登录名、来源IP、操作、操作结果等信息。

图 11-12 用户与资源操作趋势图



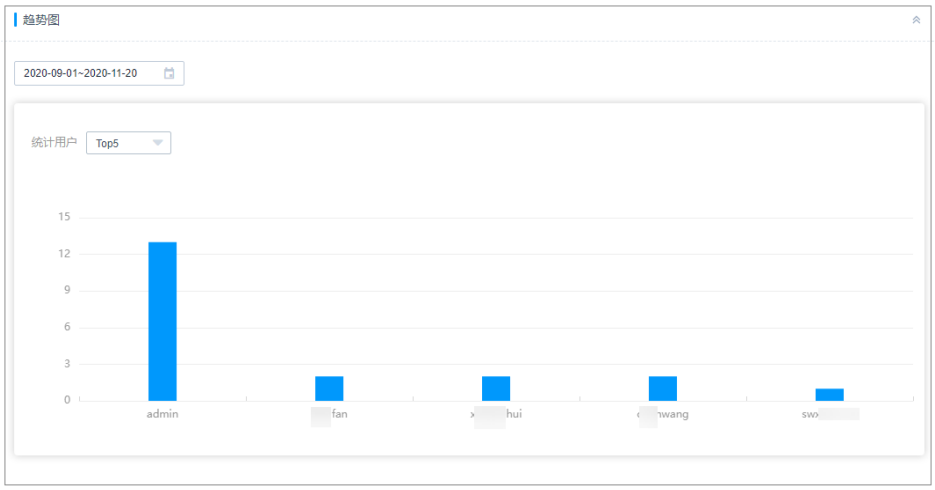
用户源 IP 数

呈现用户登录系统的不同来源IP的数量，默认呈现当天系统数据变化趋势。

可选择查看TOP5、TOP10、TOP20来源IP的用户数据。

在“详细数据”区域，可查看用户登录时间、用户登录名、来源IP、操作、操作结果等信息。

图 11-13 用户源 IP 数趋势图



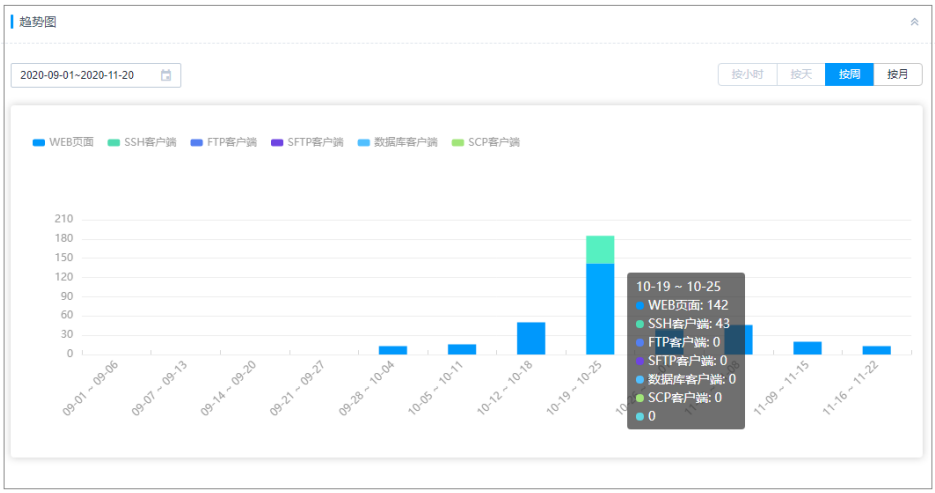
用户登录方式

呈现用户登录系统的不同登录方式的数量，默认呈现当天系统数据变化趋势。

登录方式包括Web页面、SSH客户端、FTP客户端、SFTP客户端。

在“详细数据”区域，可查看用户登录时间、用户登录名、来源IP、操作、操作结果等信息。

图 11-14 用户登录方式趋势图



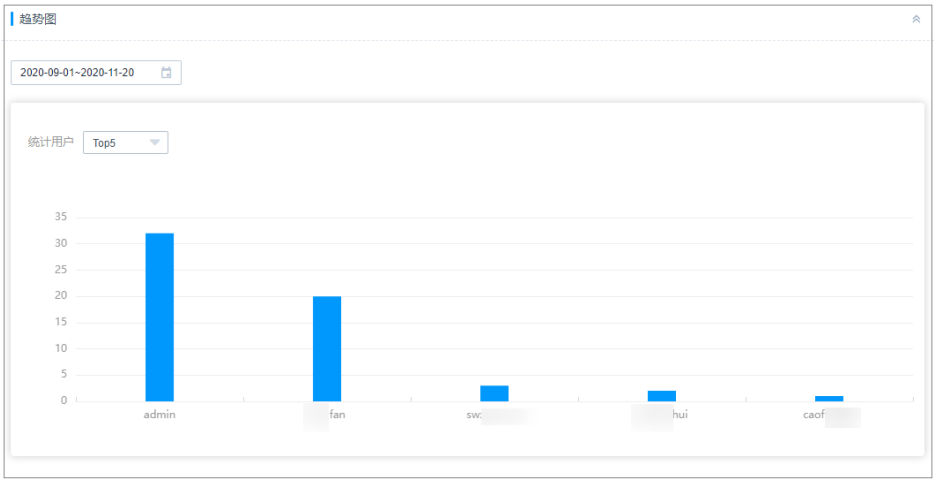
异常登录

呈现用户异常登录次数，默认呈现当天系统数据变化趋势。

可选择查看TOP5、TOP10、TOP20异常登录的用户数据。

在“详细数据”区域，可查看用户登录时间、用户登录名、来源IP、操作、操作结果等信息。

图 11-15 异常登录趋势图



会话控制

呈现用户中断和监控会话的次数，默认按小时呈现当天系统数据变化趋势。

在“详细数据”区域，可查看用户登录时间、用户登录名、来源IP、操作、操作结果等信息。

用户状态

呈现僵尸账户和密码强度的用户账号数量。

- 僵尸账户是当前未登录时间超过14天的已生效用户，按未登录天数统计。

  默认呈现TOP5僵尸账户信息。可选择查看TOP5、TOP10、TOP20的僵尸账户。

  在“详细数据”区域，可查看上一次成功登录的时间、用户登录名、来源IP、操作、操作结果等信息。
- 密码强度则是对系统内用户密码强度的划分，分为高、中、低三个等级。

  在“详细数据”区域，可查看上一次改密的用户登录名、密码强度、上次改密时间，以密码强度由低至高排列。

  说明

  密码强度的划分具体按照以下规则：

  高：8位及以上，包含大写字母、小写字母、数字、特殊字符。

  中：8位及以上，包含大写字母、小写字母、数字、特殊字符中的两种或三种。

  低：8位及以上，包含大写字母、小写字母、数字、特殊字符中的一种，或8位以下。

11.5.2 推送系统报表

为方便审计管理员及时获取运维统计信息，通过邮件发送系统报表。

- 自动发送周期可选择每日、每周、每月。
- 报表格式可选择PDF、DOC、XLS、HTML。
- 每次推送最多可呈现连续180天的系统统计数据。

前提条件

- 已获取“系统报表”模块管理权限。
- 已配置有效邮箱地址。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“审计 > 系统报表”，进入系统报表查看页面。

步骤3 单击右上角的“报表导出”，弹出系统报表导出配置窗口。

步骤4 配置系统报表推送方式、时间和文件格式。

表 11-3 系统报表导出参数说明

参数	说明
展示粒度	选择系统报表趋势图呈现粒度。 可以选择“按小时”、“按天”、“按周”、“按月”。
时间	选择报表统计数据时间范围。 ● 需同时选择起始时间和结束时间。 ● 最长可选择连续的180天。
报表类型	选择报表需呈现统计数据类型。
文件格式	选择报表的文件格式，仅可选择一种格式。 ● 默认导出DOC文件格式。 ● 可选择PDF、DOC、XLS、HTML格式。

步骤5 单击“确定”，立即导出系统报表。

步骤6 “消息中心”收到导出系统报表完成提醒，即可在邮箱收到系统报表文件。

----结束

自动发送

步骤1 登录堡垒机系统。

步骤2 选择“审计 > 系统报表”，进入系统报表查看页面。

步骤3 单击右上角的“报表自动发送”，弹出系统报表自动推送配置窗口。

步骤4 配置报表推送方式、时间和文件格式。

表 11-4 自动发送系统报表参数说明

参数	说明
状态	选择开启或关闭自动推送上一周期报表，默认 。 ● ，表示关闭自动推送报表。 ● ，表示开启以邮件方式发送上一周期的报表至当前用户邮箱。
发送周期	选择报表发送周期。 ● 默认为目标日期的零点发送报表。 ● 可以按每日、每周、每月周期进行发送。 ● 每日发送的报表中展示粒度为按小时。 ● 每周发送的报表中展示粒度为按天。 ● 每月发送的报表中展示粒度为按周。
文件格式	选择报表格式，仅可选择一种格式类型。 ● 默认选DOC格式。 ● 可选择PDF、DOC、XLS、HTML格式。

步骤5 单击“确定”，返回系统报表页面，按期接收到系统报表邮件。

----结束

12 认证配置

12.1 多因子认证管理

12.1.1 USBKey 管理

用户账号需配置了“USBKey”多因子认证，才能为用户账号签发USBKey。

签发授权USBkey前，需提前申购USBKey，并在本地安装对应的USBKey驱动。

不同的厂商USBKey不能相互识别登录认证，用户根据申购的USBKey**配置USBKey厂商**，在云堡垒机中一次仅支持配置一个厂商，不支持同时配置多个厂商。

前提条件

- 已申购USBKey。
- 已获取“用户”模块管理权限。
- 已获取“USBKey”模块管理权限。

签发 USBKey

一个USBKey只能签发给一个用户使用。

步骤1 登录堡垒机系统。

步骤2 选择“用户 > USBKey”，进入USBKey列表页面。

步骤3 单击“签发”，新建签发USBKey。

步骤4 配置“关联用户”，选择已经开启USBKey多因子认证的用户。

表 12-1 签发 USBKey 参数说明

参数	说明
USBKey	USBKey商品标识码。
关联用户	选择已配置“USBKey”多因子认证的用户账号。

参数	说明
PIN码	USBKey厂商提供，与“USBKey”一一对应的唯一识别码。

步骤5 单击“确定”，在USBKey列表查看已签发USBKey信息。

关联用户登录堡垒机系统时，插入签发的USBKey到本地主机，登录界面会自动识别USBKey，选择对应的USBKey，并输入对应的PIN码，即可完成USBKey认证方式登录。

----结束

吊销 USBKey

步骤1 登录堡垒机系统。

步骤2 选择“用户 > USBKey”，进入USBKey列表页面。

步骤3 单击“操作”列的“吊销”，可吊销该USBKey。

步骤4 勾选多个USBKey，单击列表下方的“吊销”，可批量吊销USBKey。

----结束

12.1.2 动态令牌管理

用户账号需配置了“动态令牌”多因子认证，才能为用户账号签发动态令牌。

动态令牌需要提前申购，目前堡垒机支持坚石诚信ETZ201/203型号。

前提条件

- 已申购硬件令牌。
- 已获取“用户”模块管理权限。
- 已获取“动态令牌”模块管理权限。

签发动态令牌

一个动态令牌只能签发给一个用户使用。

步骤1 登录堡垒机系统。

步骤2 选择“用户 > 动态令牌”，进入动态令牌列表页面。

步骤3 单击“签发”，新建签发令牌标识。

图 12-1 新建签发动态令牌

步骤4 配置令牌标识信息。

表 12-2 签发动态令牌参数说明

参数	说明
令牌标识	动态令牌条形码。
密钥	动态令牌的厂商提供，与“令牌标识”一一对应的唯一“密钥”。
关联用户	选择已配置“动态令牌”多因子认证的用户账号。

步骤5 单击“确定”，返回动态令牌列表，即可查看已签发令牌标识。

关联用户登录堡垒机系统时，在登录界面输入用户登录名、用户密码，以及动态令牌上动态口令，即可完成动态令牌方式登录。

----结束

导入动态令牌

步骤1 登录堡垒机系统。

步骤2 选择“用户 > 动态令牌”，进入动态令牌列表页面。

步骤3 单击“导入”，弹出批量导入动态令牌窗口。

步骤4 单击“单击下载”，下载模板文件到本地。

步骤5 按照模板文件中的配置项说明，填写需导入的动态令牌配置信息。

步骤6 单击“单击上传”，选择已配置的模板文件。

- 支持上传的文件类型包括CSV、xls、xlsx。
- 勾选“覆盖已有令牌”。
  - 勾选：当密钥、关联用户重复时，将覆盖令牌标识并更新现有令牌的标识信息，但不会删除令牌重新创建。
  - 未勾选：当密钥、关联用户重复时，直接跳过密钥、关联用户重复的令牌。

步骤7 单击“确定”，返回动态令牌列表，接口查看导入的动态令牌。

----结束

导出动态令牌

步骤1 登录堡垒机系统。

步骤2 选择“用户 > 动态令牌”，进入动态令牌列表页面，勾选需要导出的动态令牌。

若不勾选，默认导出全部动态令牌。

步骤3 右上角单击  ，弹出导出动态令牌确认窗口。

- 设置加密密码，将导出文件加密。
- 输入当前用户的密码，确保导出数据安全。

- 可选择csv或Excel导出格式

步骤4 单击“确认”，任务创建成功，单击“去下载中心”查看打包进度为100%时，单击“操作”列的“下载”，下载文件到本地，打开本地文件，即可查看导出的动态令牌信息。

----结束

吊销动态令牌

动态令牌删除后，关联用户账号将暂时不能通过动态令牌方式登录。

步骤1 登录堡垒机系统。

步骤2 选择“用户 > 动态令牌”，进入动态令牌列表页面。

步骤3 单击“操作”列的“吊销”，即可吊销该动态令牌。

步骤4 在动态令牌列表中，同时选中多个动态令牌，单击列表下方的“吊销”按钮，可批量吊销动态令牌。

----结束

12.1.3 登录手机令牌管理

手机令牌可用来生成动态口令的手机客户端软件。堡垒机系统支持通过绑定手机令牌对用户登录进行多因子身份认证，用户配置“手机令牌”多因子认证后，需同时输入用户密码和6位手机令牌验证码，才能登录堡垒机系统。更多详细说明，请参见**配置手机令牌登录**。

目前堡垒机系统可选择两种手机令牌绑定方式“内置手机令牌”和“RADIUS手机令牌”。

- 内置手机令牌：支持TOTP算法，需要到堡垒机的个人中心绑定手机令牌，可通过支持TOTP算法的微信小程序或APP（例如Google Authenticator、FreeOTP Authenticator等）绑定手机令牌。
- RADIUS手机令牌：支持TOTP算法，需对接用户自建的RADIUS服务器并在RADIUS服务器上绑定手机令牌，可通过支持TOTP算法的微信小程序或APP（例如Google Authenticator、FreeOTP Authenticator等）绑定手机令牌。

须知

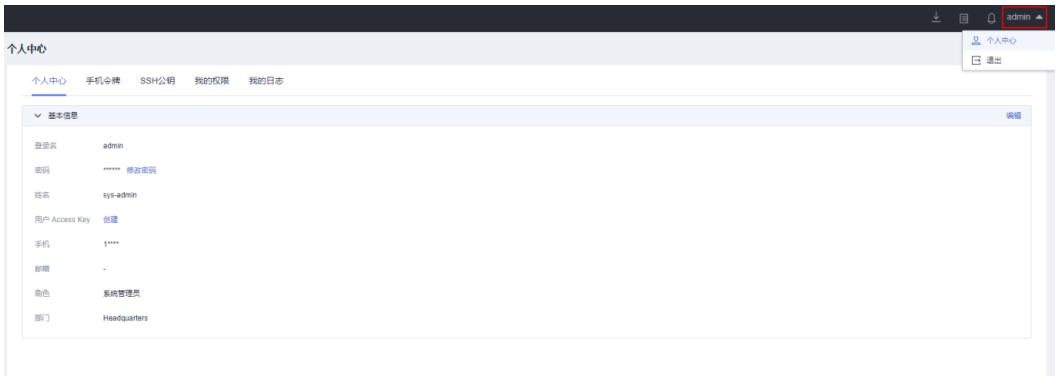
- 需确保系统时间与手机时间一致，精确到秒，否则可能提示绑定失败。
- 绑定失败后，修改系统时间与手机时间一致，刷新页面重新生成二维码，重新绑定手机令牌。

绑定手机令牌

步骤1 登录堡垒机系统。

步骤2 选择右上角用户名，单击“个人中心”，进入个人中心管理页面。

图 12-2 个人中心页面



步骤3 选择“手机令牌”页签，进入个人手机令牌管理页面。

步骤4 按照界面提示和实际令牌类型，执行绑定操作。

说明

绑定前务必将堡垒机时间和手机时间保持一致。

1. 微信小程序手机令牌

   打开手机微信，依次按照操作指导，获取绑定动态口令，输入6位“动态密码”，验证通过绑定手机令牌。

2. APP版手机令牌

   打开已安装好的手机令牌APP，扫描页面操作指导步骤2的二维码，获取绑定动态口令，输入6位“动态密码”，验证通过绑定手机令牌。

步骤5 “手机令牌”页签更新为已绑定手机令牌页面。

----结束

解绑手机令牌

手机令牌绑定完成后，在“手机令牌”页签，单击“解绑”，即可立即解除绑定的手机令牌。

解绑后，在“手机令牌”页签更新为操作指导步骤页面。

12.1.4 个人 SSH 公钥管理

用户个人SSH公钥用于**SSH客户端免密登录**。

用户在本地自行生成SSH密钥（包括公钥和私钥），将公钥添加到堡垒机系统中，将私钥导出到本地并导入到SSH客户端工具中，可实现通过SSH客户端免密登录堡垒机系统。

约束限制

仅支持OpenSSH公钥。

前提条件

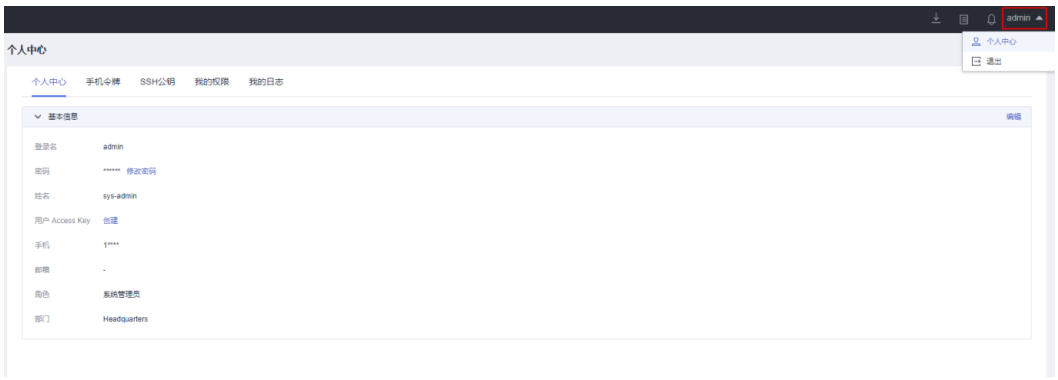
已在本地自行生成SSH密钥对。

添加 SSH 公钥

步骤1 登录堡垒机系统。

步骤2 选择右上角用户名，单击“个人中心”，进入个人中心管理页面。

图 12-3 个人中心页面



步骤3 选择“SSH公钥”页签，进入个人SSH公钥管理页面。

步骤4 单击“添加”，弹出添加个人SSH公钥窗口。

步骤5 自定义公钥名称，并输入SSH公钥。

步骤6 单击“确定”，返回SSH公钥列表，即可查看已添加的SSH公钥。

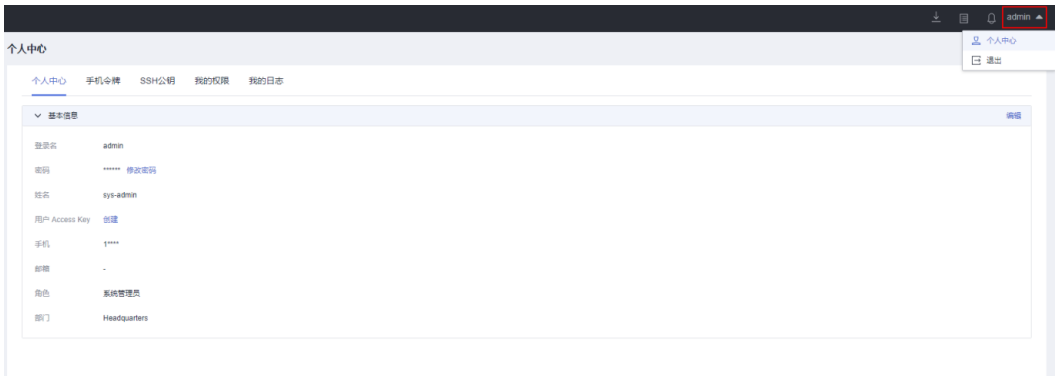
----结束

删除 SSH 公钥

步骤1 登录堡垒机系统。

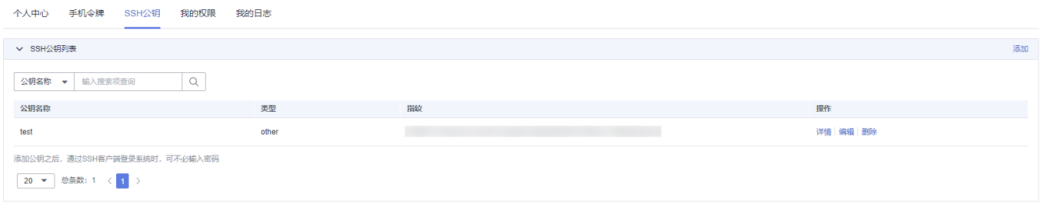
步骤2 选择右上角用户名，单击“个人中心”，进入个人中心管理页面。

图 12-4 个人中心页面



步骤3 选择“SSH公钥”页签，进入个人SSH公钥管理页面。

图 12-5 个人 SSH 公钥



步骤4 在目标SSH公钥“操作”列，单击“删除”，弹出删除个人SSH公钥确认窗口。

步骤5 确认信息无误后，单击“确定”，返回SSH公钥列表，即可删除SSH公钥。

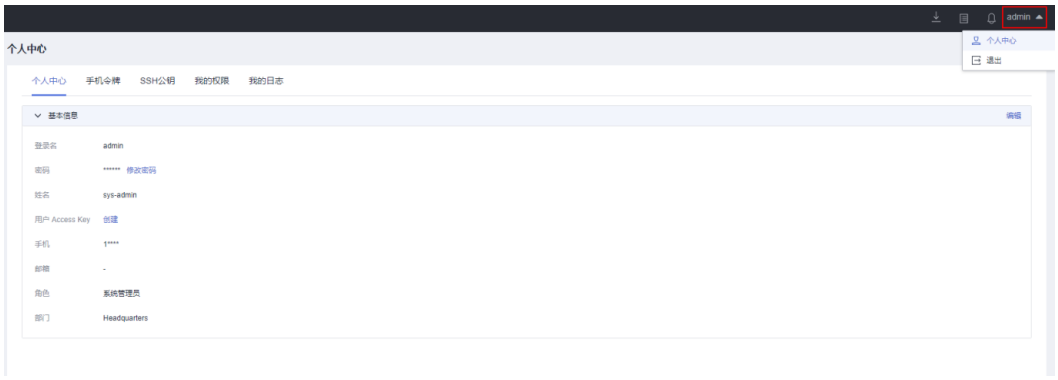
----结束

修改 SSH 公钥

步骤1 登录堡垒机系统。

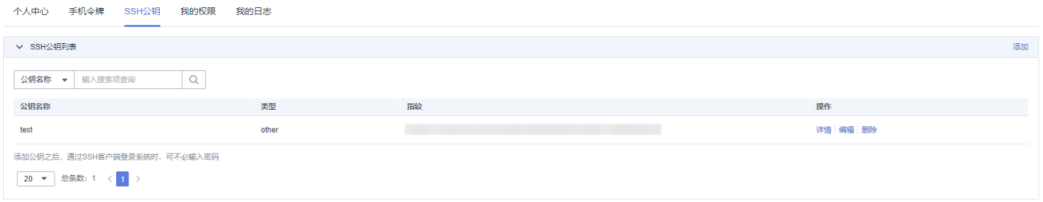
步骤2 选择右上角用户名，单击“个人中心”，进入个人中心管理页面。

图 12-6 个人中心页面



步骤3 选择“SSH公钥”页签，进入个人SSH公钥管理页面。

图 12-7 个人 SSH 公钥



步骤4 在目标SSH公钥“操作”列，单击“编辑”，弹出编辑个人SSH公钥窗口。

步骤5 可修改公钥名称和SSH公钥。

步骤6 单击“确定”，返回SSH公钥列表，即可查看已修改的SSH公钥。

----结束

12.2 多因子认证配置

12.2.1 配置手机短信登录

手机短信是以手机短信形式发送的6位随机数的动态密码，堡垒机系统支持通过手机短信动态密码对用户登录身份进行认证。配置手机短信认证后，登录系统需同时输入静态密码和6位手机短信动态密码，才能通过身份认证，从而确保系统身份认证的安全性 。

您绑定的手机号码必须有效，若绑定后因个人原因导致号码变更无法登录，需重置admin登录方式，请参见**重置admin登录方式**。

约束限制

- 一个登录账号仅能绑定一个可用手机号码。
- 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。

步骤一：绑定手机号码

用户账号绑定的手机号码必须有效，可正常接收短信。

方式一：用户绑定个人手机号码

步骤1 用户通过静态密码方式登录堡垒机系统。

步骤2 选择右上角用户名，单击“个人中心”，进入个人中心基本信息管理页面。

步骤3 单击“编辑”，弹出个人信息编辑窗口。

说明

手机填写规则如下：+国家区号+手机号码。

步骤4 在“手机”列框，输入有效手机号码。

说明

若是国际号码，须在前缀加上国际代码：+国家代码 手机号码，示例：+86 1xxxxxxxxx。

步骤5 单击“确定”，绑定手机号码。

----结束

方式二：管理员修改用户手机号码

步骤1 管理员登录堡垒机系统。

步骤2 选择“用户 > 用户管理 ”，进入用户列表管理页面。

步骤3 选择目标用户，单击登录名，进入用户详情页面。

步骤4 在“基本信息”区域，单击“编辑”，弹出用户基本信息管理窗口。

步骤5 在“手机”列框，输入新手机号码。

步骤6 单击“确定”，即修改用户手机号码。

----结束

步骤二：管理员配置手机短信认证

步骤1 管理员登录堡垒机系统。

步骤2 选择“用户 > 用户管理”，进入用户管理页面。

步骤3 找到目标用户，单击用户登录名，进入用户详情页面。

步骤4 在“用户配置”区域，单击“编辑”，弹出用户的登录配置窗口。

步骤5 勾选“手机短信”多因子认证项。

步骤6 单击“确定”，完成用户配置。

用户再次登录系统时，手机短信登录认证生效。

----结束

12.2.2 配置手机令牌登录

手机令牌是可用来生成动态口令的手机客户端软件，堡垒机系统支持通过手机令牌动态密码对用户登录身份进行认证。

配置手机令牌认证后，登录系统需同时输入静态密码和6位手机令牌动态密码，才能通过身份认证。

手机令牌认证后，只要堡垒机时间与手机时间完全保持一致，堡垒机在非公网环境也可以正常使用。

须知

admin账户若要使用多因子认证方式登录，需先配置手机令牌，否则**admin账户**将无法使用多因子认证方式登录系统。

若手机令牌失效无法登录，可选择重置admin登录方式，详情请参见**重置admin登录方式**。

目前堡垒机系统可选择两种手机令牌绑定方式，包括“内置手机令牌”和“RADIUS手机令牌”。

- 内置手机令牌：支持TOTP算法，需要到堡垒机的个人中心绑定手机令牌，可通过支持TOTP算法的微信小程序或APP（例如Google Authenticator、FreeOTP Authenticator等）绑定手机令牌。
- RADIUS手机令牌：支持TOTP算法，需对接用户自建的RADIUS服务器并在RADIUS服务器上绑定手机令牌，可通过支持TOTP算法的微信小程序或APP（例如Google Authenticator、FreeOTP Authenticator等）绑定手机令牌。

约束限制

系统时间与手机时间必须一致，精确到秒，否则可能提示绑定失败。

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。

步骤一：配置系统手机令牌类型

步骤1 登录堡垒机系统。

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“手机令牌配置”区域，单击“编辑”，弹出手机令牌类型配置窗口。

步骤4 选择系统手机令牌类型。

支持“内置手机令牌”和“RADIUS手机令牌”，设置为“RADIUS手机令牌”时，各参数说明如下：

表 12-3 RADIUS 手机令牌参数说明

参数名称	参数说明
服务器地址	填写RADIUS服务器的地址。
端口	填写RADIUS服务器的端口。
认证协议	支持“PAP”和“CHAP”。
认证共享密钥	填写RADIUS服务器的认证共享密钥。
认证超时	设置认证超时时间，取值：5~30，单位：秒。 认证最多尝试3次，每次尝试的时间为认证超时配置时间。

步骤5 单击“确定”，返回安全配置管理页面，查看当前系统手机令牌类型。

----结束

步骤二：用户绑定手机令牌

内置手机令牌方式

步骤1 用户通过静态密码方式登录堡垒机系统。

步骤2 选择右上角用户名，单击“个人中心”，进入个人中心管理页面。

步骤3 选择“手机令牌”页签，进入个人手机令牌配置页面。

按照界面提示信息依次执行操作。

图 12-8 手机令牌配置页面

说明

若您没有微信APP，请直接使用谷歌验证码程序扫描第二个二维码。

步骤4 后续若需要解除手机令牌绑定，可在“手机令牌”页签，单击“解除”。

----结束

RADIUS手机令牌方式

步骤1 在RADIUS服务器上创建用户，并根据提示为该用户完成手机令牌绑定。

----结束

步骤三：管理员配置手机令牌认证

内置手机令牌方式

步骤1 管理员登录堡垒机系统。

步骤2 选择“用户 > 用户管理”，进入用户管理页面。

步骤3 找到已绑定手机令牌的用户，单击用户登录名，进入用户详情页面。

步骤4 在“用户配置”区域，单击“编辑”，弹出用户的登录配置窗口。

步骤5 勾选“手机令牌”多因子认证项。

步骤6 单击“确定”，完成用户配置。

用户再次登录系统时，手机令牌登录认证生效。

----结束

RADIUS手机令牌方式

步骤1 在堡垒机系统中创建用户，该用户的登录名须与**步骤1**中RADIUS服务器上创建的用户同名。

1. 管理员登录堡垒机系统。
2. 选择“用户 > 用户管理”，进入用户管理页面。
3. 单击“新建”，弹出用户信息配置窗口。

表 12-4 新建用户参数说明

参数	说明
登录名	须与RADIUS服务器上创建的用户同名。 创建后不可修改，且系统内“登录名”唯一不能重复。
认证类型	选择“本地”认证类型。 本地：系统默认方式，即通过系统自身的账号管理系统进行身份认证。
密码/确认密码	需要配置用户登录系统的密码，可自定义。
姓名	自定义用户姓名。 用户账号使用人员的姓名，便于区分不同的用户。
手机	输入手机号码。 用户账号系统预留手机号码，用于手机短信登录或找回密码。
邮箱	输入邮箱地址。 用户账号系统预留邮箱地址，用于通过邮箱接收系统消息通知。

参数	说明
角色	选择用户的角色，一个用户仅能配置一个角色。 缺省情况下，系统角色包括部门管理员、策略管理员、审计管理员和运维员。 – 部门管理员：负责部门管理，除“用户管理”和“角色管理”模块之外，部门管理员拥有其他全部模块的配置权限。 – 策略管理员：负责策略权限的配置，拥有“用户组管理”、“资源组管理”和“访问策略管理”等模块的配置权限。 – 审计管理员：负责系统和运维数据的审计，拥有“实时会话”、“历史会话”和“系统日志”等模块的配置权限。 – 运维员：系统普通用户和资源操作人员，拥有“主机运维”、“应用运维”和“授权工单”模块的操作访问权限。 – 自定义的角色：仅**admin**可自定义新角色或编辑默认角色的权限范围。
所属部门	选择用户所属部门组织。如何创建系统部门，请参见**新建部门**。
用户描述	对用户情况的简要描述。

4. 单击“确定”。
   在用户管理页面，可以查看已创建的用户。

步骤2 在堡垒机系统中为该同名用户配置手机令牌认证。

1. 在用户管理页面。
2. 找到该同名用户，单击用户登录名，进入用户详情页面。
3. 在“用户配置”区域，单击“编辑”，弹出用户的登录配置窗口。
4. 勾选“手机令牌”多因子认证项。
5. 单击“确定”，完成用户配置。
   使用该同名用户登录系统时，手机令牌登录认证生效。

----结束

12.2.3 配置 USBKey 登录

uToken是基于USBKey实现的OTP动态密码技术。配置USBKey认证后，登录系统时需接入USBKey，登录页面自动识别唯一关联USBKey，输入相应PIN码，才能通过身份认证。

若您不慎卸载USBkey驱动导致无法登录，可选择重置admin登录方式，详情请参见**重置admin登录方式**。

约束限制

- 不同的厂商USBKey不能相互识别登录认证。需根据申购的USBKey**配置USBKey厂商**，在云堡垒机中一次仅支持配置一个厂商，不支持同时配置多个厂商。
- 一个USBKey仅能签发给一个用户使用。

前提条件

已申购USBKey，并在本地安装对应的USBKey驱动。

步骤一：配置 USBKey 认证

步骤1 管理员登录堡垒机系统。

步骤2 选择“用户 > 用户管理”，进入用户管理页面。

步骤3 找到目标用户，单击用户登录名，进入用户详情页面。

步骤4 在“用户配置”区域，单击“编辑”，弹出用户的登录配置窗口。

步骤5 勾选“USBKey”多因子认证项。

步骤6 单击“确定”，完成用户多因子认证配置。

----结束

步骤二：签发 USBKey

步骤1 管理员登录堡垒机系统。

步骤2 选择“用户 > USBKey”，进入USBKey列表页面。

步骤3 单击“签发”，新建签发USBKey。

步骤4 配置“关联用户”，选择已经开启USBKey多因子认证的用户。

表 12-5 签发 USBKey 参数说明

参数	说明
USBKey	USBKey商品标识码。
关联用户	选择已配置“USBKey”多因子认证的用户账号。
PIN码	USBKey厂商提供，与“USBKey”一一对应的唯一识别码。

步骤5 单击“确定”，在USBKey列表查看已签发USBKey信息。

关联用户登录堡垒机系统时，连接签发的USBKey到本地主机，登录界面会自动识别USBKey，选择对应的USBKey，并输入PIN码，即可完成USBKey登录认证。

----结束

12.2.4 配置动态令牌登录

动态口令是基于事件同步的令牌实现的OTP动态密码技术。配置动态令牌认证后，登录系统时需输入静态密码和6位硬件令牌动态密码，才能通过身份认证。

若您不慎遗失硬件令牌导致无法登录，可选择重置admin登录方式，详情请参见**重置admin登录方式**。

约束限制

- 目前堡垒机可识别坚石诚信ETZ201/ETZ203型号硬件令牌。
- 一个硬件令牌仅能签发给一个用户使用。

前提条件

已自行购买坚石诚信ETZ201/ETZ203型号的硬件令牌。

步骤一：配置动态令牌认证

步骤1 管理员登录堡垒机系统。

步骤2 选择“用户 > 用户管理”，进入用户管理页面。

步骤3 找到目标用户，单击用户登录名，进入用户详情页面。

步骤4 在“用户配置”区域，单击“编辑”，弹出用户的登录配置窗口。

步骤5 勾选“动态令牌”多因子认证项。

步骤6 单击“确定”，完成用户多因子认证配置。

----结束

步骤二：签发动态令牌

步骤1 管理员登录堡垒机系统。

步骤2 选择“用户 > 动态令牌”，进入动态令牌列表页面。

步骤3 单击“签发”，新建签发令牌标识。

步骤4 配置令牌标识信息。

表 12-6 签发动态令牌参数说明

参数	说明
令牌标识	动态令牌条形码。
密钥	动态令牌的厂商提供，与“令牌标识”一一对应的唯一“密钥”。
关联用户	选择已配置“动态令牌”多因子认证的用户。

步骤5 单击“确定”，返回动态令牌列表，即可查看已签发令牌标识。

关联用户登录堡垒机系统时，在登录界面输入用户登录名、静态密码，以及硬件令牌上动态密码，即可完成动态令牌方式登录。

----结束

12.2.5 配置邮箱认证登录

邮箱认证是为用户添加邮箱验证码认证，在登录时输入密码后还需要邮箱验证码验证，验证成功后才能登录至实例，同时邮箱认证支持SSH客户端登录。

前提条件

- 已完成**邮件配置**，且测试成功。
- 已完成**用户添加**。

约束限制

- 首次登录堡垒机不能使用此方式登录，需配置后才可使用。
- 堡垒机版本须在3.3.62.0及以上版本。

为账户添加邮箱地址

步骤1 以“Admin登录”方式登录堡垒机实例，选择“用户 > 用户管理”，进入用户管理页面。

步骤2 在用户列表勾选单个或多个需要添加邮箱的账户，在列表下方选择“更多 > 修改多因子认证”。

步骤3 在弹窗中勾选邮箱认证为目标账户登录堡垒机实例的认证方式。

说明

- 如果目标账户已有其他登录认证方式需继续使用，则需要一并勾选。
- 如果需要对目标账户所属部门的所有账户或下属部门所有账户一并添加邮箱认证，勾选“修改全部”即可。

步骤4 单击“确定”，完成添加，添加后可在“用户 > 用户管理”页面单击目标账户名称查看账户添加的邮箱和多因子认证方式。

----结束

12.3 远程认证管理

12.3.1 配置 AD 域远程认证

堡垒机与AD服务器对接，认证登录系统的用户身份，AD认证的模式包括认证模式和同步模式两种。

- 认证模式

  在此模式下，堡垒机不会同步AD域服务器上的用户信息，需要管理员手工创建用户。当用户登录堡垒机时，将由AD域服务器提供认证服务。

- 同步模式

  在此模式下，堡垒机可以同步AD域服务器的用户信息，无需管理员新建用户。当用户登录堡垒机时，由AD域服务器提供认证服务，详细配置操作请参见**同步AD域用户**。

前提条件

- 用户已获取“系统”模块管理权限。
- 已获取AD服务器相关信息。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统配置 > 认证配置”，进入认证配置页面。

图 12-9 配置远程认证

步骤3 在“AD认证配置”区域，单击“添加”，弹出AD认证配置窗口。

步骤4 选择AD域认证“模式”为“认证模式”，其他参数的配置如**表12-7**。

表 12-7 AD 域认证模式参数说明

参数	说明
服务器地址	输入AD域服务器地址。
状态	选择开启或关闭AD域远程认证，默认 。 • ，表示开启AD域认证。在配置信息有效情况下，登录系统时启动AD域认证，或同步AD域用户。 • ，表示关闭AD域认证。
SSL	选择开启或关闭SSL加密认证，默认 。 • ，表示禁用SSL加密认证。 • ，表示启用SSL加密认证，将加密同步用户或认证用户所传输的数据。
模式	选择“认证模式”。
端口	AD域远程服务器的接入端口，默认389端口。
域	输入AD域的域名。

步骤5 单击“确认”，返回AD域认证服务器表中，即可查看和管理的AD认证配置信息。

----结束

后续管理

- 若需查看配置的AD域认证信息，可单击“详情”，在弹出的AD域详情窗口查看。
- 若需修改认证信息、关闭认证、更换认证模式等，可单击“编辑”，在弹出的AD认证配置窗口重新配置。
- 若不再需要该AD认证，可单击“删除”，删除认证信息。删除后认证信息不能找回，请谨慎操作。

12.3.2 配置 LDAP 远程认证

堡垒机与LDAP服务器对接，认证登录系统的用户身份。

约束限制

- 不能添加两个相同的LDAP配置，即“服务器IP地址+端口+用户OU”不能相同。
- 仅V3.3.36.0及以上版本支持“查询”认证模式，如需使用此模式，请参照**升级实例版本**章节将实例版本升级至最新版本。

前提条件

- 用户已获取“系统”模块管理权限。
- 已获取LDAP服务器相关信息。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统配置 > 认证配置”，进入认证配置页面。

图 12-10 配置远程认证

步骤3 在“LDAP认证配置”区域，单击“添加”，弹出LDAP认证配置窗口。

LDAP支持两种认证模式：

- “认证方式”选择“认证”时，参照**表12-8**配置相关参数。

表 12-8 LDAP 域认证模式参数说明

参数	说明
服务器地址	输入LDAP服务器地址。
状态	选择开启或关闭LDAP远程认证，默认  。 –  ，表示开启LDAP认证。在配置信息有效情况下，登录系统时启动LDAP认证。 – ，表示关闭LDAP认证。
SSL	选择开启或关闭SSL加密认证，默认 。 – ，表示禁用SSL加密认证。 –  ，表示启用SSL加密认证，将加密同步用户或认证用户所传输的数据。

参数	说明
端口	输入LDAP远程服务器的接入端口，默认389端口。
模式	选择“认证模式”或“同步模式”。 – 认证模式：堡垒机和LDAP服务器做对接，域用户的添加需要手动在用户管理处选择LDAP认证添加。 – 同步模式：堡垒机和AD服务器对接好之后，可以在“系统配置 > 认证配置”处，把对应OU下的用户同步到堡垒机上。
用户OU	输入LDAP服务器上用户OU。
用户过滤器	输入LDAP服务器上待过滤的用户。

- “认证方式”选择“查询”时，参照**表12-9**配置相关参数。

  说明

  仅V3.3.36.0及以上版本支持“查询”认证模式，如需使用此模式，请参照**升级实例版本**章节将系统版本升级至最新版本。

图 12-11 查询模式

表 12-9 LDAP 域查询模式参数说明

参数	说明
服务器地址	输入LDAP服务器地址。

参数	说明
状态	选择开启或关闭LDAP远程认证，默认 。 – ，表示开启LDAP认证。在配置信息有效情况下，登录系统时启动LDAP认证。 – ，表示关闭LDAP认证。
SSL	选择开启或关闭SSL加密认证，默认 。 – ，表示禁用SSL加密认证。 – ，表示启用SSL加密认证，将加密同步用户或认证用户所传输的数据。
端口	输入LDAP远程服务器的接入端口，默认389端口。
模式	选择认证模式或同步模式。 – 堡垒机和AD服务器做对接，域用户的添加需要手动在用户管理处选择LDAP认证添加。 – 堡垒机和AD服务器对接好之后，可以在“系统配置 > 认证配置”处，把对应OU下的用户同步到堡垒机上。
Base DN	LDAP服务器的根唯一标识名称。
管理员DN	管理员唯一标识名称。
管理员密码	管理员的密码。
用户OU	输入LDAP服务器上用户OU。
用户过滤器	输入LDAP服务器上待过滤的用户。

步骤4 单击“确定”，返回LDAP认证服务器表中，即可查看和管理的LDAP认证配置信息。

----结束

后续管理

- 若需查看配置的LDAP认证信息，可单击“详情”，在弹出的LDAP详情窗口查看。
- 若需修改认证信息、关闭认证等，可单击“编辑”，在弹出的LDAP配置窗口重新配置。
- 若不再需要该LDAP认证，可单击“删除”，删除认证信息。删除后认证信息不能找回，请谨慎操作。

12.3.3 配置 RADIUS 远程认证

堡垒机与RADIUS服务器对接，认证登录系统的用户身份。

本小节主要介绍如何配置RADIUS域认证模式，并可对配置的RADIUS认证进行用户有效性测试。

前提条件

- 用户已获取“系统”模块管理权限。
- 已获取RADIUS服务器相关信息。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统配置 > 认证配置”，进入认证配置页面。

图 12-12 配置远程认证

步骤3 在“RADIUS认证配置”区域，单击“编辑”，弹出RADIUS认证配置窗口。

表 12-10 RADIUS 域认证模式参数说明

参数	说明
服务器地址	输入RADIUS服务器地址。
状态	选择开启或关闭RADIUS远程认证，默认 。 • ，表示开启RADIUS认证。在配置信息有效情况下，登录系统时启动RADIUS认证。 • ，表示关闭RADIUS认证。
端口	输入RADIUS远程服务器的接入端口，默认1812端口。
认证协议	选择远程认证协议，可选择“PAP”和“CHAP”。 **说明** 需要与认证的资源协议保持一致。
认证共享密钥	输入RADIUS远程服务器的认证密钥。
认证超时	输入RADIUS远程认证超时时间。
用户名	输入RADIUS服务器上用户名，用于测试配置的RADIUS服务器信息是否正确。
密码	输入RADIUS服务器上用户密码，用于测试配置的RADIUS服务器信息是否正确。
测试	单击测试，用于测试配置的RADIUS服务器信息是否正确。

步骤4 单击“确认”，返回RADIUS认证服务器表中，即可查看和管理的RADIUS认证配置信息。

----结束

后续管理

若需修改认证信息、关闭认证等，可单击“编辑”，在弹出的RADIUS配置窗口重新配置。

12.3.4 配置 Azure AD 远程认证

堡垒机与Azure AD平台对接，认证登录系统的用户身份。

前提条件

- 用户已获取“系统”模块管理权限。
- 已在Azure AD创建用户和添加企业应用程序，并获取Azure AD平台配置的相关信息。

  说明

  Azure AD相关操作及配置需在Azure页面进行，请参考Azure官网相关指导文档或咨询Azure工程师。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统配置 > 认证配置”，进入认证配置页面。

图 12-13 配置远程认证

步骤3 在“Azure AD认证配置”区域，单击“编辑”，弹出Azure AD认证配置窗口。

表 12-11 Azure AD 域认证参数说明

参数	说明
状态	选择开启或关闭Azure AD远程认证，默认 。 • ，表示开启Azure AD认证。在配置信息有效情况下，登录系统时呈现Azure AD认证入口。 • ，表示关闭Azure AD认证。
标识符（实体ID）	输入企业名称或URL。

参数	说明
回复URL	自动填写，默认为返回当前堡垒机的跳转链接。 当堡垒机IP或域名变更，需同时修改此链接中IP或域名。
应用联合元数据URL	输入在Microsoft Azure中配置SAML签名证书后生成的应用联合元数据URL。
登录URL	输入在Microsoft Azure中配置SAML单一登录后生成的登录URL。
Azure AD标识符	输入在Microsoft Azure中配置SAML单一登录后生成的Azure AD标识符。

步骤4 单击“确认”，提交配置数据验证可达后，返回Azure AD认证服务器表中，即可查看和管理的Azure AD认证配置信息。

须知

若更新了Azure AD的证书，需要在Azure AD管理面删除旧证书才可正常登录。

----结束

后续管理

- 若需修改认证信息、关闭认证等，可单击“编辑”，在弹出的Azure AD配置窗口重新配置。
- 成功配置Azure AD认证后，您还需在系统创建已加入到企业应用程序或已在Azure平台创建的用户，更多配置说明请参见**新建用户**。

12.3.5 配置 SAML 远程认证

堡垒机与SAML平台对接，认证登录系统的用户身份。

本小节主要介绍如何配置SAML认证模式。

前提条件

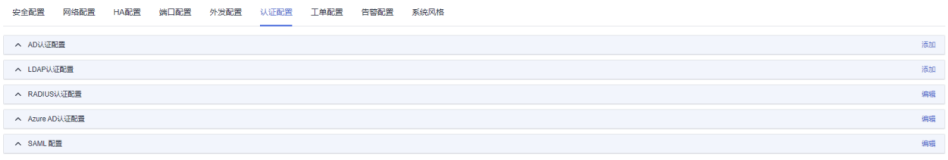
- 用户已获取“系统”模块管理权限。
- 已在SAML创建用户，并获取SAML平台配置的相关信息。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统配置 > 认证配置”，进入认证配置页面。

图 12-14 配置远程认证



步骤3 在“SAML认证配置”区域，单击“编辑”，弹出SAML认证配置窗口。

表 12-12 SAML 域认证参数说明

参数	说明
状态	选择开启或关闭SAML远程认证，默认 。 • ，表示开启SAML认证。在配置信息有效情况下，登录系统时呈现SAML认证入口。 • ，表示关闭SAML认证。
覆盖已有用户	选择开启或关闭SAML覆盖功能，默认 。 • ，表示开启覆盖，如果已存在同名账户，开启后将会覆盖已有账户。 • ，表示不启用覆盖，如果已存在同名账户，SAML用户创建会失败。
标识符（实体ID）	获取idp上的元数据（Shibboleth IDP，默认配置在C:\Program Files (x86)\Shibboleth\IdP\metadata目录） 标识符：填写entityID后续的部分。
NameIdFormat	获取idp上的元数据（Shibboleth IDP，默认配置在C:\Program Files (x86)\Shibboleth\IdP\metadata目录） NameIdFormat：建议取urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified。
签名证书	证书请填写idp中对应的FrontChannel的sigining证书。
登录URL	登录URL请填写协议HTTP-Redirect中对应的SingleSignOnService的Location地址。
登出URL	登录URL请填写协议HTTP-Redirect中对应的SingleLogoutService的Location地址。
回复URL	默认Host为Localhost的IP，请您按照实际部署的情况去填写（如域名地址）。

步骤4 单击“确认”，提交配置数据验证可达后，返回SAML配置项中，即可查看和管理SAML认证配置信息。

----结束

13 登录安全配置

13.1 配置用户登录安全锁

为保障堡垒机系统用户登录安全，在用户登录堡垒机时，输入密码错误次数超过系统设置的次数限制后，用户“来源IP”、“用户+来源IP”或“用户”账号将被锁定。

本小节主要介绍如何配置用户登录安全锁，包括修改锁定方式、锁定时长、可尝试密码次数等。

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“用户锁定配置”区域，单击“编辑”，弹出用户锁定配置窗口。

根据界面提示配置系统用户登录安全锁。

图 13-1 配置用户安全锁

表 13-1 用户锁定配置参数说明

参数	说明
锁定方式	选择用户锁定方式。 • 用户：输入密码错误次数超过次数限制后，禁止使用该登录名的用户登录。 • 来源IP：输入密码错误次数超过次数限制后，禁止该来源IP的用户登录。 • 用户+来源IP：输入密码错误次数超过次数限制后，禁止该登录名和来源IP的用户登录。
尝试密码次数	连续输入密码错误的最大次数。 • 默认为5次。 • 取值范围为0～999。 • 设置为0，表示密码错误后不锁定用户登录。
锁定时长	因密码错误锁定用户登录的时长。 • 默认为30分钟。 • 取值范围为0～10080，单位为分钟。 • 设置为0，表示除非管理员解除锁定，用户登录账号或来源IP将一直被锁定。

参数	说明
重置计数器时长	用户登录失败后，登录失败次数计数器重置为0的时长。 ● 默认值为5分钟。 ● 取值范围为1～10080，单位为分钟。

步骤4 单击“确定”，返回安全配置管理页面，查看当前系统用户锁定配置。

----结束

13.2 配置登录密码策略

本小节主要介绍如何配置用户密码策略，包括配置密码安全强度、密码验证次数、密码修改周期等。

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“密码策略配置”区域，单击“编辑”，弹出密码策略配置窗口。

根据界面提示配置系统用户密码策略。

表 13-2 密码策略配置参数说明

参数	说明
密码强度校验	选择开启或关闭强制系统用户强密码验证，默认  。 ● ，表示关闭强密码校验。 ●  ，长度为8-32个字符，密码只能包含大写字母、小写字母、数字和特殊字符(!@$%^-_=+[{}]:,./?~#*)且至少包含四种字符中的三种。
新用户强制改密	选择开启或关闭强制系统新用户首次登录修改密码，默认  。 ● ，表示系统新用户首次登录无需修改密码。 ●  ，表示强制系统新用户首次登录必须修改密码。
密码相同校验	校验修改后新密码与前N次设置的密码重复性。 ● 系统用户首次登录的密码不计算在内。 ● 默认次数为5。 ● 取值范围为1～30。

参数	说明
密码修改周期	校验系统用户密码的修改周期，密码超过修改周期后强制修改密码。 ● 默认周期为30天。 ● 取值范围为0～90，单位为天。 ● 若设置为0，表示密码永不过期。

步骤4 单击“确定”，返回安全配置管理页面，查看当前系统用户密码策略配置。

----结束

13.3 配置 Web 登录超时和登录验证

本小节主要介绍如何配置通过Web页面和客户端的登录系统，包括配置登录超时时间、短信验证码过期时间、图形验证码启用、SSH公钥登录、SSH密码登录等。

前提条件

用户已获取“系统”模块管理权限。

Web 登录配置

步骤1 登录堡垒机系统。

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登录配置”区域，单击“编辑”，弹出Web登录配置窗口。

根据界面提示配置系统Web登录参数。

表 13-3 Web 登录配置参数说明

参数	说明
登录超时	用户在系统管理界面或运维会话界面，无操作退出登录的限定时间。 即用户通过Web浏览器登录系统后，在系统管理界面或运维会话界面，无操作时长超过设定的值，将退出登录，运维会话断开连接。 ● 默认超时时间为30分钟。 ● 取值范围为1～1440，单位为分钟。
短信验证码过期时间	登录系统短信验证码的过期时间。 ● 默认过期时间为60秒。 ● 取值范围为60～3600，单位为秒。 ● 若设置为0，表示短信验证不过期。

参数	说明
图形验证码	选择启用、禁用或自动启用登录系统图形验证码。 ● 选择“启用”，登录系统时必须图形验证码验证。 ● 选择“禁用”，登录系统时无需图形验证码验证。 ● 选择“自动”，登录系统时，根据密码错误次数，自动启用图形验证码。
登录尝试次数	登录密码错误次数超过限制，将自动启用图形验证码。 ● “图形验证码”配置为“自动”时，必须配置登录尝试次数。 ● 默认尝试次数为3。 ● 取值范围为1～30。
图形验证码过期时长	图形验证码的过期时间。 ● 默认过期时间为60秒。 ● 取值范围为15～3600，单位为秒。 ● 若设置为0，表示图形验证码不过期。
域控校验	选择开启或禁用域控校验，默认。 ●  ，表示当系统配置“域控校验”，且用户选择AD域认证时，该用户需下载SSO登录工具，并在登录名相同的域服务器中才能成功登录系统。 ● ，表示禁用域控校验。
来源IP检测	选择开启或禁用来源IP检测，默认。 ●  ，表示当前系统开启“来源IP检测”。开启后，堡垒机会从tcp连接信息中获取访问堡垒机的源IP，当系统识别到源IP变化时，当前的会话会被断开，堡垒机需要重新登录。 ● ，表示关闭“来源IP检测”，关闭后源IP变化时会话不会被断开。 **说明** – 无论是否开启“来源IP检测”，堡垒机都会对来源IP进行记录。 – 如果开启后因IP不固定导致被频繁退出，可将“来源IP检测”进行关闭，关闭后不会对业务产生影响。 – V3.3.44.0-S及之后版本才支持该功能。
不允许多点登录	开启后同一堡垒机不允许多地址或多端登录。
保留客户端会话	需要开启“不允许多点登录”功能才能对该功能进行开启或关闭。 ● 关闭：当通过Web页面访问堡垒机时，会将已登录的客户端会话强制断开，如果同属客户端登录，已登录的无法被强制断开。 ● 开启：开启后通过Web页面访问堡垒机时，不会将已登录的客户端会话强制断开，会保留客户端会话，Web页面无法登录。
强制多因子登录	开启后，系统将强制使用多因子认证登录，如果账户未配置多因子认证，需要联系管理员进行配置，否则需关闭此项。

步骤4 单击“确定”，返回安全配置管理页面，查看当前系统Web登录配置。

----结束

客户端登录配置

步骤1 登录堡垒机系统。

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“客户端登录配置”区域，单击“编辑”，弹出客户端登录配置窗口。

根据界面提示配置系统客户端登录参数。

表 13-4 客户端登录配置参数说明

参数	说明
登录超时	用户登录SSH客户端后，无操作退出登录的限定时间。 • 默认超时时间为30分钟。 • 取值范围为1～43200，单位为分钟。
SSH公钥登录	选择开启或关闭SSH公钥登录，默认 。 • ，表示用户使用客户端登录系统时，且添加了SSH公钥，可免密验证登录。 • ，表示关闭SSH公钥登录。
SSH密码登录	选择开启或关闭SSH密码登录，默认 。 • ，表示用户使用客户端登录系统时，需输入用户密码验证登录。 • ，表示关闭SSH密码登录。 • 若同时开启了“公钥登录”和“密码登录”，优先验证公钥登录方式。

步骤4 单击“确定”，返回安全配置管理页面，查看当前系统客户端登录配置。

----结束

13.4 更新系统 Web 证书

堡垒机Web证书是验证系统网站身份和安全的SSL（Secure Sockets Layer）证书，遵守SSL协议的服务器数字证书，并由受信任的根证书颁发机构颁发。

堡垒机系统默认配置安全的自签发证书，但受限于自签发证书的认证保护范围和认证保护时间，用户可替换证书。

本小节主要介绍在证书过期或安全扫描不通过时，用户如何更新证书，确保CBH系统安全。

前提条件

- 已获取证书，并下载签发证书。
- 上传证书绑定的域名已解析到绑定堡垒机实例的弹性公网IP。
- 用户已获取“系统”模块管理权限。

约束限制

- 目前堡垒机系统只适配Tomcat的Java Keystore格式证书文件，即后缀为jks的证书文件。
- 目前堡垒机系统支持的证书加密算法类型如下：RSA、ECDSA。
- 上传的证书文件大小不超过20KB，且证书文件包含证书密码。无证书密码将不能验证上传证书，SSL证书文件无法上传到系统。

操作步骤

步骤1 登录堡垒机系统。

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证书上传窗口。

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。

步骤7 如果是主备类型的堡垒机，在主堡垒机中更新Web证书后，还需要切换到备堡垒机，参考**步骤1**到**步骤6**将Web证书同步更新到备堡垒机中。如果是单机类型的堡垒机，可忽略此步骤。

1. 在主堡垒机中，选择“系统 > 系统维护 > 系统管理”。
2. 在“系统工具”区域，单击“重启”右侧的“重启”。

   重启后，将切换到备堡垒机。

----结束

13.5 配置手机令牌类型

手机令牌可用来生成动态口令的手机客户端软件。堡垒机系统支持通过绑定手机令牌，对用户登录进行多因子身份认证，用户配置“手机令牌”多因子认证后，需同时输入用户密码和6位手机令牌验证码，才能登录堡垒机系统。

本小节主要介绍如何设置系统手机令牌类型。

约束限制

- 目前仅支持两种手机令牌类型：
  - 内置手机令牌：支持TOTP算法，需要到堡垒机的个人中心绑定手机令牌，可通过支持TOTP算法的微信小程序或APP（例如Google Authenticator、FreeOTP Authenticator等）绑定手机令牌。

  - RADIUS手机令牌：支持TOTP算法，需对接用户自建的RADIUS服务器并在RADIUS服务器上绑定手机令牌，可通过支持TOTP算法的微信小程序或APP（例如Google Authenticator、FreeOTP Authenticator等）绑定手机令牌。
- 系统手机令牌类型，需与实际绑定手机令牌类型一致。

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“手机令牌配置”区域，单击“编辑”，弹出手机令牌类型配置窗口。

步骤4 选择系统手机令牌类型。

支持“内置手机令牌”和“RADIUS手机令牌”，设置为“RADIUS手机令牌”时，各参数说明如下：

表 13-5 RADIUS 手机令牌参数说明

参数名称	参数说明
服务器地址	填写RADIUS服务器的地址。
端口	填写RADIUS服务器的端口。
认证协议	支持“PAP”和“CHAP”。
认证共享密钥	填写RADIUS服务器的认证共享密钥。
认证超时	设置认证超时时间，取值：5~30，单位：秒。 认证最多尝试3次，每次尝试的时间为认证超时配置时间。

步骤5 单击“确定”，返回安全配置管理页面，查看当前系统手机令牌类型。

----结束

13.6 配置 USB Key 厂商

本小节主要介绍如何配置系统USB Key厂商。

约束限制

- 更改USBKey厂商配置后，已签发的其他厂商USB Key将不能被识别。
- USB Key厂商配置详情请参见**配置USBKey登录**。

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“USB Key配置”区域，单击“编辑”，弹出系统USB Key厂商配置窗口。

步骤4 选择USBKey厂商。

步骤5 单击“确定”，返回安全配置管理页面，查看当前系统USB Key厂商。

----结束

13.7 配置用户禁用策略（V3.3.30.0 及以上版本）

僵尸用户策略功能，支持对僵尸用户进行判定并自定义设置判定时间，即超过判定时间未登录的用户会被判定为僵尸用户，系统将自动禁用这些用户，直到管理员解除禁用。默认判定时间为30天，如果时间设置为0，则所有用户会立即被禁用。

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“用户禁用配置”模块的右侧，单击“编辑”，进入“用户禁用配置”页面。

- 禁用僵尸用户：默认为关闭状态，打开后的状态为  。
- 僵尸用户判定时间：有效值0~10080，默认为30天，如果设置为0，则所有用户会立即被禁用，直到管理员解除禁用。解除禁用的相关操作请参考**启停用户**章节。

步骤4 单击“确定”，完成配置。

----结束

13.8 配置 RDP 资源客户端代理（3.3.26.0 及以上版本）

使用了RDP协议的服务器在通过堡垒机使用RDP连接服务器时，会使用安全层的校验，可自行选择不同的安全层校验模式。

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“RDP资源客户端代理配置”模块的右侧，单击“编辑”，进入“RDP资源客户端代理配置”页面。

步骤4 在“安全层”下拉框中，选择客户端代理，然后单击“确定”。

支持选择的安全层：RDP、TLS、协商。

----结束

13.9 开启 API 配置（V3.3.34.0 及以上版本支持）

开启API配置后，将支持通过API调用方式使用堡垒机。

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“API配置”模块的右侧，单击“编辑”，进入“API配置”页面。

步骤4 单击，开启API配置。

步骤5 单击“确定”，配置生效。

----结束

13.10 配置自动巡检（V3.3.36.0 以及上版本支持）

开启自动巡检后，系统将在每月5日、15日、25日凌晨01:00时自动对资源账户进行验证。

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“自动巡检配置”模块的右侧，单击“编辑”，进入“自动巡检配置”页面。

步骤4 自动巡检的状态默认为开启状态  ，可单击图标，关闭或开启自动巡检功能。

步骤5 单击“确定”，配置完成。

----结束

13.11 资源账户配置

开启后资源账户可自动添加账户名为Empty的账户，可进行修改，关闭后创建资源账户时必须自定义账户名称。

操作步骤

步骤1 登录堡垒机系统。

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“资源账户配置”模块的右侧，单击“编辑”，进入“资源账户配置”页面。

步骤4 自动添加Empty账户的状态默认为开启状态  ，可单击图标，关闭或开启资源账户功能。

步骤5 单击“确定”，完成配置。

----结束

13.12 客户端登录配置

可配置登录客户端后无操作的超时时间，超时后自动退出。

操作步骤

步骤1 登录堡垒机系统。

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“客户端登录配置”模块的右侧，单击“编辑”，进入“客户端登录配置”页面。

步骤4 设置客户端登录配置参数，如表13-6所示。

表 13-6 客户端登录配置

参数名称	参数说明	取值样例
登录超时	成功登录后，当用户超过设定时长无操作时将自动退出登录，再次操作需要重新登录。 有效值区间为1-43200，默认值为30，单位：分钟。	30
SSH公钥登录	超时后是否使用SSH公钥登录，默认开启。	

参数名称	参数说明	取值样例
SSH密码登录	超时后是否使用SSH密码登录，默认开启。	

步骤5 单击“确定”，完成配置。

----结束

13.13 用户有效期倒计时配置

配置有效期后，在到期前5天，每天会自动发送一次邮件提醒。

操作步骤

步骤1 登录堡垒机系统。

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“用户有效期倒计时配置”模块的右侧，单击“编辑”，进入“用户有效期倒计时配置”页面。

步骤4 输入用户密码，开启用户有效期倒计时开关  。

步骤5 单击“确定”，完成配置。

----结束

13.14 会话限制配置

配置会话在开启后，当CPU、内存使用率、磁盘空间保护任意一个超过配置的限制时，将禁止新增会话，超过运维会话超时设置的限制时，主动断开会话。

操作步骤

步骤1 登录堡垒机系统。

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“会话限制配置”模块的右侧，单击“编辑”，进入“会话限制配置”页面。

步骤4 开启会话限制的开关状态为  ，并设置CPU和内存的使用率，以及磁盘保护大小和会话超时时间，当达到任意一个设置的限制值时，将停止新增会话，超过运维会话超时设置的限制时，主动断开会话。

说明

超时运维会话设置后，在运维会话窗口右侧有会话时长倒计时，如有延长会话时间的需要请联系管理员在会话限制增大会话超时配置，剩余15分钟的时候，倒计时变红色字体进行提示。

步骤5 单击“确定”，完成配置。

----结束

13.15 不安全协议配置

堡垒机支持对不安全协议的禁用配置。

操作步骤

步骤1 登录堡垒机系统。

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“协议配置”模块的右侧，单击“编辑”，在弹窗可开启不安全协议的开关。

启用后，将允许使用FTP，Telnet，Rlogin协议，使用不安全协议，您的数据可能面临风险。请避免输入敏感信息。

步骤4 确认无误，单击确认，完成配置。

----结束

13.16 不安全算法配置

堡垒机支持对不安全算法的禁用配置。

操作步骤

步骤1 登录堡垒机系统。

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“算法配置”模块的右侧，单击“编辑”，在弹窗可开启不安全算法的开关。

启用后，SSH将允许使用不安全算法与第三方对接或向下兼容等场景。使用不安全算法，您的数据可能面临风险。请避免输入敏感信息。

步骤4 确认无误，单击确认，完成配置。

----结束

14 实例配置

14.1 实例配置概述

系统配置包括安全、网络、端口、外发、认证、工单、告警、审计、HA备份等配置。为确保系统安全运行，默认仅系统管理员**admin**可修改系统配置，整体管理系统运行状况。

- 安全配置，详情请参见**登录安全管理**。
- 网络配置，详情请参见**系统网络配置**。
- HA配置，详情请参见**HA配置**。
- 端口配置，详情请参见**系统端口配置**。
- 外发配置，详情请参见**系统外发配置**。

  说明

  用户有效期倒计时邮件：配置完成后在到期前5天才会发送邮件。
- 认证配置，详情请参见**远程认证配置**。
- 工单配置，主要介绍工单配置的基本模式、高级模式、审批流程等，详情请参考**工单配置管理**。
- 告警配置，详情请参见**系统告警配置**。
- 系统风格，详情请参见**系统风格变更**。

14.2 网络配置

14.2.1 查看系统网络配置

本小节主要介绍如何查看系统网络接口、DNS地址、默认网关地址、静态路由等信息。

前提条件

已获取“系统”模块管理权限。

操作步骤

步骤1 登录堡垒机系统。

步骤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。

步骤3 在“网络接口列表”区域，可以查看当前堡垒机系统的相关网络接口信息。

默认不支持修改系统网络接口。

步骤4 在“DNS配置”区域，可以查看当前堡垒机系统的首选DNS和备用DNS地址。

默认不支持修改系统DNS地址。

图 14-1 系统 DNS 地址

步骤5 在“默认网关”区域，可查看当前堡垒机系统的默认网关。

默认识别DHCP网关地址，且不支持修改默认网关。

图 14-2 系统默认网关

步骤6 在“静态路由配置”区域，可查看当前系统可以访问其他网段的服务器。

----结束

14.2.2 添加系统静态路由

为系统添加静态路由，避免重启系统后路由丢失而影响到网络可用性。

前提条件

已获取“系统”模块管理权限。

⚠ 注意

静态路由信息需填写准确，若信息填写不当会导致堡垒机无法登录。

操作步骤

步骤1 登录堡垒机系统。

步骤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。

步骤3 在“静态路由配置”区域，单击“添加”，弹出静态路由添加窗口。

根据界面提示，配置静态路由。

步骤4 单击“确认”，返回网络配置页面，查看已配置的静态路由。

----结束

后续管理

若解除某个静态路由，可单击“删除”，删除相关路由配置。

14.3 HA 配置

14.3.1 启用 HA

堡垒机支持双机HA热备功能。启用HA备份后，用户登录系统，使用HA热备机功能，此时主节点断开，备节点也可提供服务。

约束限制

- 必须先配置主节点。主节点配置生效后，再配置备节点，并需确保主备节点使用内网进行HA同步配置。
- 备节点HA配置生效后，无论备节点上是否已有配置数据，历史数据都会被清空，并同步主节点的配置数据。

前提条件

- 已获取“系统”模块管理权限。
- 已准备两台堡垒机，且两台堡垒机授权同一个许可文件。

操作步骤

步骤1 登录堡垒机系统。

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

图 14-3 HA 配置

步骤3 在“双机热备配置”区域，可查看当前HA状态，默认为“禁用”。

⚠ 注意

如您创建的是主备实例，切勿禁用HA，否则会导致对应堡垒机无法登录。

步骤4 单击“HA状态”后的“启用”，弹出HA备份配置窗口。

配置主备节点HA备份信息。

表 14-1 启用 HA 配置参数说明

参数	说明
热备初始角色	选择主节点或备节点。 必须先配置主节点的堡垒机。
HA群组验证密钥	系统自动生成，用于双机互相验证。 ● 配置主节点HA参数时，需记录HA群组验证密钥，并配置到备节点。 ● 取值范围是8～20位的数字或字母。
备节点IP地址	配置主节点HA参数时，输入作为备节点的堡垒机IP地址。
主节点IP地址	配置备节点HA参数时，输入作为主节点的堡垒机IP地址。
HA Key	配置主节点HA参数时，输入双机互相验证的密钥Key。
浮动IP地址	输入与当前堡垒机固定IP在同一网段且未被使用的IP地址。浮动IP地址后需要加掩码。 浮动IP地址即为两个堡垒机对外体现的逻辑IP地址。用户访问此IP地址时，自动登录到双机中的一台堡垒机上，一般是主节点。
浮动IP网口	选择堡垒机固定IP所在的网口。
HA心跳接口	与浮动IP网口一致。

步骤5 单击“确定”，返回HA配置页面，重启系统生效配置。

----结束

生效条件

重启生效主备节点HA配置。

- 未重启时，“当前运行状态”显示为“单机”，即配置未生效。
- 重启完毕，在主节点检测到备节点登录IP，“当前运行状态”显示为“在线状态”，即配置生效。

后续管理

若需关闭双机HA备份，需分别单击“HA状态”后的“禁用”，即可关闭双机热备。

保存设置后，重启两台堡垒机系统，重启完成后双机HA备状态即为关闭状态。

14.4 端口配置

14.4.1 配置系统运维端口

系统运维端口是登录SSH、SFTP、FTP类型资源的端口，包括通过SSH客户端登录堡垒机的端口，默认端口号2222。

默认端口修改后，需同时修改实例安全组配置。

本小节主要介绍如何管理系统运维端口。

前提条件

已获取“系统”模块管理权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统配置 > 端口配置”，进入系统端口配置页面。

步骤3 在“运维端口配置”区域，单击“编辑”，弹出运维端口配置窗口。

- 配置SSH/SFTP端口号，默认端口号2222。
- FTP代理服务，默认为关闭。开启FTP代理服务，默认端口号2121。

步骤4 单击“确定”，返回端口配置页面，重启系统生效配置。

----结束

14.4.2 配置 Web 控制台端口

Web控制台端口是通过Web浏览器登录堡垒机的访问端口，默认端口号443。

默认端口修改后，需同时修改实例安全组配置的端口。

本小节主要介绍如何管理系统Web控制台端口。

前提条件

已获取“系统”模块管理权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统配置 > 端口配置”，进入系统端口配置页面。

步骤3 在“Web控制台端口配置”区域，单击“编辑”，弹出Web控制台端口配置窗口。

配置Web浏览器访问端口号，默认端口号443。

步骤4 单击“确定”，返回端口配置页面，重启系统生效配置。

----结束

14.4.3 配置 SSH 控制台端口

SSH控制台端口是通过SSH客户端登录堡垒机的访问端口，默认端口号22。

默认端口修改后，需同时修改实例安全组配置的端口。

本小节主要介绍如何管理系统SSH控制台端口。

前提条件

已获取“系统”模块管理权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统配置 > 端口配置”，进入系统端口配置页面。

步骤3 在“SSH控制台端口配置”区域，单击“编辑”，弹出SSH控制台端口配置窗口。

配置SSH客户端访问端口号，默认端口号22。

步骤4 单击“确定”，返回端口配置页面，重启系统生效配置。

----结束

14.5 外发配置

14.5.1 配置邮件外发

邮件服务器，为改密提示和消息告警等通知提供邮件发送服务。

- 根据需求设置私有邮箱服务器或是公共邮箱服务器，并可测试所填写服务器信息是否有效。
- 目前支持两种发送方式，分别为SMTP和Exchange，其中Exchange仅支持Exchange2010版本。

前提条件

已获取“系统”模块管理权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统配置 > 外发配置”，进入系统外发配置管理页面。

步骤3 在“邮件配置”区域，单击“编辑”，弹出邮件配置窗口，并根据界面提示配置邮件发送方式。

表 14-2 邮件外发配置参数说明

参数名称	参数描述
发送方式	支持选择SMTP和Exchange的方式。 ● SMTP：使用SMTP为邮件传输协议的邮件类型。 ● Exchange：使用Exchange为邮件处理组件的邮件类型。
服务器地址	当前正在添加的邮箱所在的服务器地址，需通过邮箱所属企业的官网或者邮箱所属企业的统一管理员获取。
加密方式	选择SMTP方式时，填写此项。 选择原始邮箱的加密方式，可选择SSL或TLS，未加密选择无，可通过邮箱所属企业的官网或者邮箱所属企业的统一管理员获取。
端口	选择SMTP方式时，填写此项。 填写原始邮箱在服务器开放的端口，可通过邮箱所属企业的官网或者邮箱所属企业的统一管理员获取。
版本	选择Exchange方式时，填写此项。 选择Exchange方式支持的版本，目前仅支持Exchange2010版本。
域	选择Exchange方式时，填写此项。 填写原始邮箱的所属域，可通过邮箱所属企业的官网或者邮箱所属企业的统一管理员获取。
发送人账号	填写发送邮件的账号。 该账号为邮箱服务器中已存在且可正常使用的账号。
发送人密码	填写发送邮件账号的密码。 该账号为邮箱服务器中已存在且可正常使用账号的密码。
收件人	邮件的接收人。

配置完成后，单击下方的“发送测试邮件”，可测试是否能正常发送。

步骤4 单击“确认”，返回外发配置页面，即可查看已配置信息。

----结束

14.5.2 配置短信外发

系统短信外发主要功能如下：

- 通过手机验证码方式登录堡垒机。
- 重置密码。
- 告警消息发送，告警消息范围可参考**告警配置**。

目前可选择配置“内置”和“自定义”两种类型，其中“自定义”类型还可选择通用“短信网关”和“消息&短信服务”。

- 若您没有系统告警推送及短信收发的需求，可参考**内置短信网关**进行短信网关配置。

- 若您有系统告警接收或短信收发的需求，请参考自定义通用短信网关进行短信网关配置。

前提条件

已获取“系统”模块管理权限。

内置短信网关

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统配置 > 外发配置”，进入系统外发配置管理页面。

步骤3 在“短信网关配置”区域，单击“编辑”，弹出短信网关配置窗口。

步骤4 选择“内置”类型，并可输入手机号码验证内置短信网关的连通性。

步骤5 单击“确认”，返回外发配置页面，即可查看短信网关信息。

⚠ 注意

- “内置”短信网关不支持推送系统告警。
- 若有短信接收需求，请在个人信息页面按照要求填写手机号。

----结束

自定义通用短信网关

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统配置 > 外发配置”，进入系统外发配置管理页面。

步骤3 在“短信网关配置”区域，单击“编辑”，弹出短信网关配置窗口。

步骤4 选择“自定义”类型，并选择“短信网关”配置，展开通用短信网关配置窗口。

根据提示配置参数信息。

步骤5 单击“确认”，返回外发配置页面，即可查看短信网关信息。

表 14-3 通用短信网关参数说明

参数	说明
发送方式	选择请求方法，可选择POST或GET。
URL地址	输入通用URL地址或带有参数的URL地址。 不支持md5加密方式的网关地址。
HTTP头部	HTTP请求头部名称与值用英文冒号“:”隔开。 只支持HTTP和HTTPS协议网关。
API参数	输入短信网关API参数，关键字$MOBILE和$TEXT将被替换成手机号码和短信内容。

参数	说明
编码	选择UTF-8、Big5、GB18030。
测试手机号	输入可用手机号码，验证短信内容。

----结束

14.5.3 配置 LTS 日志外发服务

LTS采集日志为堡垒机系统的操作日志。

前提条件

- 已获取“系统”模块管理权限。
- 已开通云日志服务（LTS）。
- 已绑定弹性公网IP。

限制条件

- 堡垒机安装Agent时必须绑定弹性公网IP。
- 必须先开通云日志服务（LTS）才可在堡垒机中进行配置。

操作步骤

步骤1 在LTS中获取安装ICAgent的命令。

参考《云日志服务用户指南》中的“安装ICAgent（区域内主机）”章节，获取安装ICAgent的命令结构如下：

```
set +o history;curl https://icagent-{region}.{obsdomain}/ICAgent_linux/apm_agent_install.sh > apm_agent_install.sh && REGION=[region] bash apm_agent_install.sh -ak {input_your_ak} -sk {input_your_sk} -region [region] -projectid [projectid] -accessip [accessip] -obsdomain [obsdomain] -aomvpcepurl [aomvpcepurl] -ltsvpcepurl [ltsvpcepurl];set -o history;
```

步骤2 将**步骤1**中获取到的命令按如下规则处理：

- 将命令中的**{input_your_ak}**和**{input_your_sk}**替换为您实际的AK和SK。
- 删除命令首尾的**set +o history;** 字段。
- 删除命令后半段的**-aomvpcepurl [aomvpcepurl] -ltsvpcepurl [ltsvpcepurl];** 字段。
- 堡垒机从V3.3.54.0版本开始支持对接https域名，因此，如果堡垒机是V3.3.54.0以前的版本，则需将https修改为http。

经过处理的命令格式如下：

- V3.3.54.0以前版本

```
curl http://icagent-{region}.{obsdomain}/ICAgent_linux/apm_agent_install.sh > apm_agent_install.sh && REGION=[region] bash apm_agent_install.sh -ak {input_your_ak} -sk {input_your_sk} -region [region] -projectid [projectid] -accessip [accessip] -obsdomain [obsdomain]
```

- V3.3.54.0及以后版本

```
curl https://icagent-{region}.{obsdomain}/ICAgent_linux/apm_agent_install.sh > apm_agent_install.sh && REGION=[region] bash apm_agent_install.sh -ak {input_your_ak} -sk {input_your_sk} -region [region] -projectid [projectid] -accessip [accessip] -obsdomain [obsdomain]
```

步骤3 在堡垒机系统中安装ICAgent。

1. 登录堡垒机系统。
2. 选择“系统 > 系统配置 > 外发配置”，进入系统外发配置管理页面。
3. 在“LTS配置”区域，单击“编辑”，弹出LTS配置窗口。
4. 单击 ，开启LTS服务，在“安装agent”框中输入步骤2中处理后的命令。

图 14-4 V3.3.54.0 及以后版本配置示例

5. 单击“确定”。
   可在弹窗中单击“去任务中心”，在任务中心查看任务进度及任务状态。

----结束

14.6 告警配置

14.6.1 配置告警方式

针对系统消息、业务消息、任务消息、命令告警、工单消息五大类告警类型，支持不同告警类型各级别消息是否告警和告警方式。

- 告警方式包括消息中心、邮件通知、短信通知。
- 根据告警等级划分各类消息是否告警，以及告警方式。
  - 默认低等级消息不告警。
  - 默认中等级消息告警，通过消息中心告警提醒。
  - 默认高等级消息告警，通过消息中心和邮件通知。

本小节主要介绍如何配置系统告警方式。

约束限制

配置了自定义通用短信网关后，才支持“短信通知”，通过手机短信推送系统告警。

前提条件

已获取“系统”模块管理权限。

告警配置

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统配置 > 告警配置”，进入系统告警配置管理页面。

图 14-5 告警配置

步骤3 在“告警方式配置”区域，单击“编辑”，弹出告警方式配置窗口。

配置不同消息类型的告警方式。

步骤4 单击“确认”，返回告警配置页面，即可查看已配置的告警信息。

----结束

14.6.2 配置告警等级

通过配置告警可对告警等级、告警方式和告警发送范围进行设置。

前提条件

已获取“系统”模块管理权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统配置 > 告警配置”，进入系统告警配置管理页面。

图 14-6 告警配置

步骤3 在“告警等级配置”区域，单击“编辑”，弹出告警等级配置窗口。

- 根据各模块事件，配置不同消息类型的告警等级。
- “告警等级”支持选择高、中、低。

步骤4 单击“确定”，返回告警配置页面，即可查看已配置的告警信息。

----结束

14.6.3 配置告警发送

本小节主要介绍如何配置系统告警的发送范围。

前提条件

已获取“系统”模块管理权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统配置 > 告警配置”，进入系统告警配置管理页面。

图 14-7 告警配置

步骤3 在“告警发送配置”区域，单击“编辑”，弹出告警发送配置窗口。

- 根据告警通知发送范围，选择发送给“本部门”或者“本部门及所有上级部门”。
- 告警发送通知范围支持发送给系统管理员，请根据自身情况选择是否发送。

图 14-8 告警发送配置

步骤4 单击“确认”，返回告警配置页面，即可查看已配置的告警发送信息。

图 14-9 查看告警发送配置

----结束

14.7 系统风格

14.7.1 变更系统风格

通过风格页面可自定义堡垒机的页面语言和堡垒机呈现的图标。

前提条件

已获取“系统”模块管理权限。

系统风格

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统配置 > 系统风格”，进入系统风格页面。

步骤3 切换系统语言。

1. 在“语言配置”区域，单击“编辑”，弹出语言配置窗口。
2. 选择语言类型，可选择简体中文和英文。
3. 单击“确认”，返回系统风格页面。
   切换语言后，需退出登录并清除Cookie，再重新登录系统，切换的语言才生效。

   说明

   建议在系统登录页面右上角直接切换语言，立即生效。

步骤4 变更系统图标。

1. 在“图标配置”区域，单击“编辑”，弹出图标配置窗口。
2. 分别单击系统图标和公司图标，打开本地路径，根据图标要求选择目标图标。
3. 单击“确认”，返回系统风格页面，即可查看自定义的系统图标和公司图标。

----结束

15 实例基本信息管理

15.1 实例桌面

系统桌面看板分为关注资源、活动用户、待审批工单、主机类型统计、应用类型统计、当前活动会话、今日新增会话、登录次数统计、运维次数统计、运维用户Top5、运维资源Top5、系统状态、系统信息、最近登录主机、最近登录应用、可登录主机、可登录应用共17个信息模块，呈现堡垒机系统状态、用户活动统计、主机/应用运维统计等信息。

不同用户角色拥有不同模块查看权限，本小节以系统管理员**admin**为例，介绍系统桌面看板的含义。

操作步骤

步骤1 登录堡垒机系统。

步骤2 在左侧导航树中，选择“桌面”，进入系统桌面看板页面。

步骤3 各个模块详细功能介绍和使用方法，请分别参见下述内容。

----结束

关注资源

呈现当前用户可管理用户、主机、应用、应用服务器的统计数据，以及未处理告警消息的数量。

用户角色需分别获取“用户管理”、“主机管理”、“应用发布”、“应用服务器”模块管理权限，以及开启角色管理权限，即可查看系统控制板统计信息。当角色权限只有其中一个时，默认不显示统计控制板。

- 用户

  呈现当前用户可管理用户数。单击用户模块，跳转到用户列表页面，可管理当前用户列表。

- 主机

  呈现当前用户可管理主机资源数。单击主机模块，跳转到主机列表页面，可管理当前主机资源列表。

- 应用

  呈现当前用户可管理应用发布资源数。单击应用模块，跳转到应用列表页面，可管理当前应用资源列表。

- 应用服务器

  呈现当前用户可管理应用服务器数。单击应用服务器模块，跳转到应用服务器列表页面，可管理当前应用服务器列表。

- 告警

  呈现当前用户未处理告警消息数。单击告警模块，跳转到消息中心页面，可管理当前消息列表。

活动用户

呈现当前用户管理范围内的在线用户和历史登录用户。

用户角色需获取“用户管理”模块管理权限，以及开启角色管理权限，即可查看活动用户统计信息。

单击列表中用户名，跳转到用户详情页面，可查看和管理用户信息。

待审批工单

呈现当前用户管理范围内的待审批工单。

用户角色需获取“工单审批”模块管理权限，以及开启角色管理权限，即可查看待审批工单统计信息。

单击列表中工单号，跳转到工单详情页面，可查看工单信息，并可立即审批工单。

主机类型统计

呈现当前用户管理范围内的主机类型统计数据。

用户角色需获取“主机管理”模块管理权限，以及开启角色管理权限，即可查看主机类型统计信息。

- 将鼠标放在圆环不同类型颜色模块上，呈现相应的主机类型统计数量。
- 单击不同类型颜色模块，跳转到相应类型主机列表页面。

应用类型统计

呈现当前用户管理范围内的应用发布类型统计数据。

用户角色需获取“应用发布”模块管理权限，以及开启角色管理权限，即可查看应用发布统计信息。

- 将鼠标放在圆环不同类型颜色模块上，呈现相应的应用发布类型统计数量。
- 单击不同类型颜色模块，跳转到相应类型应用发布列表页面。

当前活动会话

呈现当前用户管理范围内的实时会话统计数据。

用户角色需获取“实时会话”模块管理权限，以及开启角色管理权限，即可查看当前活动会话统计信息。

单击不同类型实时会话，跳转到实时会话列表页面，可实时监控相应会话。

今日新增会话

呈现当前用户管理范围内的历史会话统计数据。

用户角色需获取“历史会话”模块管理权限，以及开启角色管理权限，即可查看今日新增会话统计信息。

单击不同类型历史会话，跳转到历史会话列表页面，可查看相应类型历史会话。

登录次数统计

呈现当前用户管理范围内的用户登录系统次数趋势图，可分别查看本周和本月的趋势图。

用户角色需获取“用户管理”模块管理权限，以及开启角色管理权限，即可查看用户登录系统次数统计信息。

- 将鼠标放置在某个日期上，可查看当天的用户登录系统次数。

运维次数统计

呈现当前用户管理范围内的用户登录资源次数趋势图，可分别查看本周和本月的趋势图。

用户角色需获取“历史会话”模块管理权限，以及开启角色管理权限，即可查看用户登录资源次数统计信息。

将鼠标放置在某个日期上，可查看当天的用户登录资源次数。

运维用户 Top5

呈现当前用户管理范围内的登录资源次数最多的Top5用户，可分别查看本周和本月的统计数据。

用户角色需获取“历史会话”模块管理权限，以及开启角色管理权限，即可查看用户登录次数统计信息。

单击列表中用户，跳转到用户详情页面，可快速查看和管理用户信息。

运维资源 Top5

呈现当前用户管理范围内的运维次数最多的Top5资源，可分别查看本周和本月的统计数据。

用户角色需获取“历史会话”模块管理权限，以及开启角色管理权限，即可查看运维资源统计信息。

单击列表中资源，跳转到资源详情页面，可快速查看和管理资源信息。

系统状态

呈现当前系统的CPU、内存、磁盘的使用情况。

用户角色需获取“系统”模块管理权限，以及开启角色管理权限，即可查看系统状态统计信息。

系统信息

呈现当前系统的基本信息，以及授权实例版本规格。

用户角色需获取“系统”模块管理权限，以及开启角色管理权限，即可查看系统信息。

最近登录主机

呈现当前用户最近登录过的主机资源统计列表。

用户角色需获取“主机运维”模块管理权限，即可查看最近登录过的主机资源。

- 单击列表主机名称，跳转到主机详情页面，可查看主机详情信息。
- 单击列表中“登录”，可快速登录主机资源。

最近登录应用

呈现当前用户最近登录过的应用资源统计列表。

用户角色需获取“应用运维”模块管理权限，即可查看最近登录过的应用资源。

- 单击列表应用名称，跳转到应用发布详情页面，可查看应用发布详情信息。
- 单击列表中“登录”，可快速登录应用资源。

可登录主机

呈现当前用户被授权登录的主机资源。

用户角色需获取“主机运维”模块管理权限，即可查看有权限访问的主机资源。

- 单击列表主机名称，跳转到主机详情页面，可查看主机详情信息。
- 单击列表中“登录”，可快速登录主机资源。

可登录应用

呈现当前用户被授权登录的应用资源。

用户角色需获取“应用运维”模块管理权限，即可查看有权限访问的应用资源。

- 单击列表应用名称，跳转到应用发布详情页面，可查看应用发布详情信息。
- 单击列表中“登录”，可快速登录应用资源。

15.2 查看实例信息

本小节主要介绍如何查看当前系统基本信息。

前提条件

已获取“系统”模块管理权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“系统管理 > 关于系统”，进入系统信息页面。

步骤3 查看系统基本信息。

表 15-1 关于系统参数说明

参数	说明
产品名称	堡垒机
产品ID	用户产品ID唯一认证码。
服务码	单击“查看”获取，主要用于技术人员登录系统后台，技术人员根据内部系统提供的解密功能进行后台管理。 获取服务码之后请妥善保存，切勿外发至公共信息平台。 **说明** 技术人员使用服务码登录系统后台时，堡垒机登录日志中会增加一条root账户登录信息。
API凭证	主要用于统一管理平台添加节点认证使用。 ● 单击“查看”时需要输入系统管理员**admin**密码、Access Key Secret、Access Key ID。 ● “更新”、“清除”API凭证需要输入系统管理员**admin**密码，并且更新后，统一管理平台管理的该节点将会失效。
HA Key	主要用于配置HA时使用。 当用户通过Web界面配置HA的备节点时，备节点上的程序需要连接到指定的主节点上，再获取相关配置信息进行有效性校验，并在校验通过后才能修改主节点上的配置。
版本号	当前实例版本。
设备系统	当前系统软件版本。
发行日期	当前实例版本发行日期。

----结束

15.3 个人中心

15.3.1 查看个人信息

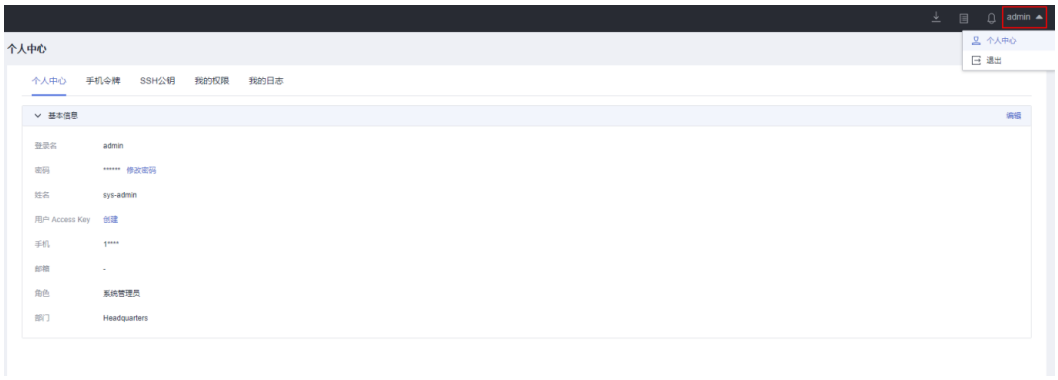
“个人中心”涵盖当前用户账号基本信息、权限范围、系统使用日志等信息，以及手机令牌和SSH公钥配置信息等。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择右上角用户名，单击“个人中心”，进入个人中心管理页面。

图 15-1 个人中心页面



步骤3 分别单击各页签，即可查看相应用户信息。

个人信息、手机令牌、个人SSH公钥、个人权限、个人日志等详细内容。

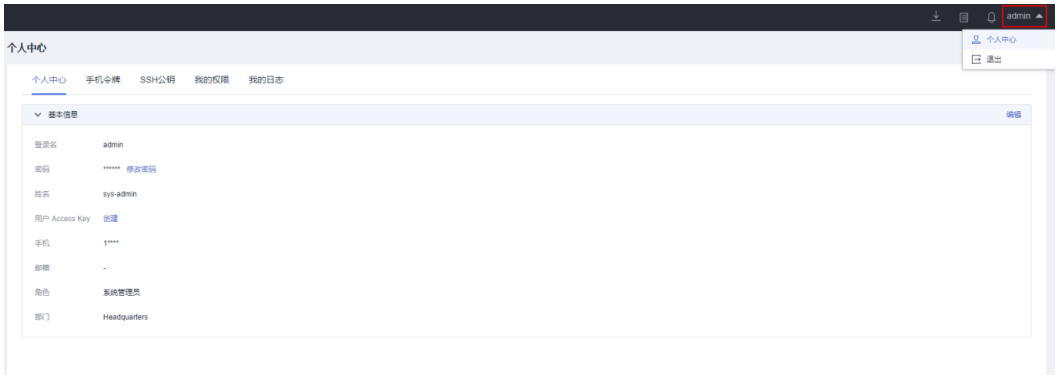
----结束

基本信息

选择“个人中心”页签，可查看用户基本信息，包括登录名、密文密码、姓名、手机号码、邮箱地址、角色、部门等信息。

修改手机号码、修改邮箱地址、修改密码详情请参见**修改个人基本信息**。

图 15-2 个人中心页面



手机令牌

选择“手机令牌”页签，可查看用户绑定手机令牌情况。

绑定和解绑手机令牌详情请参见**管理手机令牌**。

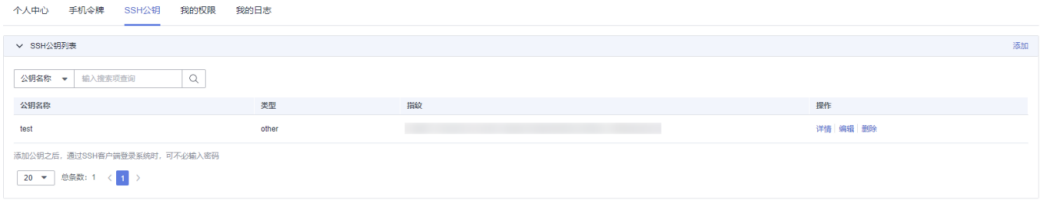
图 15-3 手机令牌

SSH 公钥

选择“SSH公钥”页签，可查看个人SSH公钥列表，并可查看公钥基本信息。

添加公钥、修改公钥、删除公钥详情请参见**管理个人SSH公钥**。

图 15-4 个人 SSH 公钥

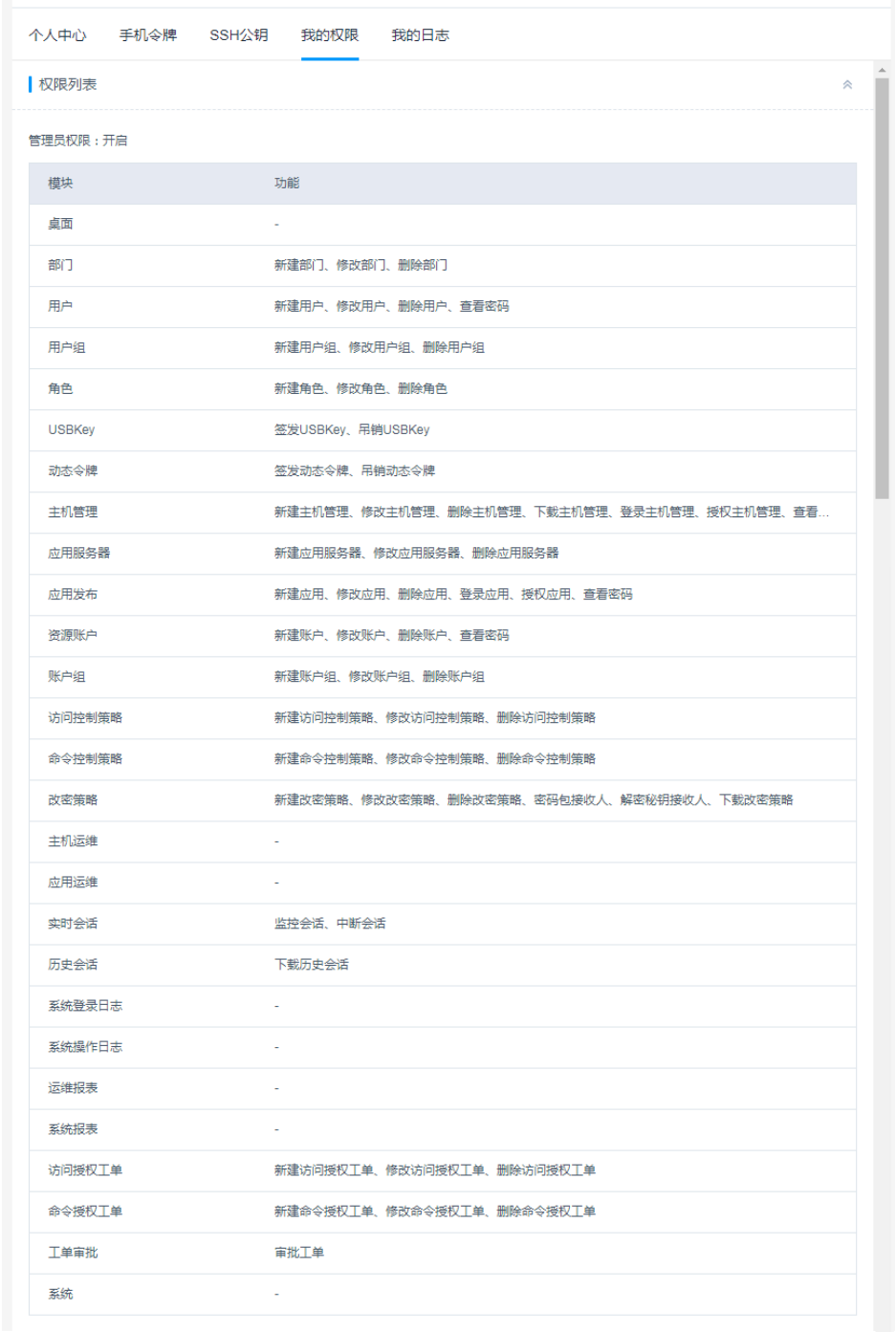


我的权限

选择“我的权限”页签，可查看个人系统权限范围，以及是否开启管理员权限。

系统管理员**admin**拥有堡垒机系统最高权限。

图 15-5 admin 用户权限



模块	功能
桌面	-
部门	新建部门、修改部门、删除部门
用户	新建用户、修改用户、删除用户、查看密码
用户组	新建用户组、修改用户组、删除用户组
角色	新建角色、修改角色、删除角色
USBKey	签发USBKey、吊销USBKey
动态令牌	签发动态令牌、吊销动态令牌
主机管理	新建主机管理、修改主机管理、删除主机管理、下载主机管理、登录主机管理、授权主机管理、查看...
应用服务器	新建应用服务器、修改应用服务器、删除应用服务器
应用发布	新建应用、修改应用、删除应用、登录应用、授权应用、查看密码
资源账户	新建账户、修改账户、删除账户、查看密码
账户组	新建账户组、修改账户组、删除账户组
访问控制策略	新建访问控制策略、修改访问控制策略、删除访问控制策略
命令控制策略	新建命令控制策略、修改命令控制策略、删除命令控制策略
改密策略	新建改密策略、修改改密策略、删除改密策略、密码包接收人、解密秘钥接收人、下载改密策略
主机运维	-
应用运维	-
实时会话	监控会话、中断会话
历史会话	下载历史会话
系统登录日志	-
系统操作日志	-
运维报表	-
系统报表	-
访问授权工单	新建访问授权工单、修改访问授权工单、删除访问授权工单
命令授权工单	新建命令授权工单、修改命令授权工单、删除命令授权工单
工单审批	审批工单
系统	-

我的日志

选择“我的日志”页签，可查看个人“系统登录日志列表”、“系统操作日志列表”和“资源登录日志列表”。

说明

个人用户不能清理个人日志，日志仅能由有系统管理权限的用户统一管理，详细说明请参见**数据维护**。

- 系统登录日志列表

  主要包括登录时间、登录用户来源IP、登录方式、登录结果等信息。
- 系统操作日志列表

  主要包括操作时间、操作用户来源IP、操作的模块、操作内容、操作结果等信息。
- 资源登录日志列表

  主要包括资源名称、资源协议类型、资源账户、登录资源用户来源IP、登录起止时间、会话时长等信息。

图 15-6 我的日志列表

15.3.2 修改个人基本信息

用户个人基本信息包括登录名、密文密码、姓名、手机号码、邮箱地址、角色、部门等信息。

- 在个人中心，用户个人可修改个人密码、修改姓名、手机号码、邮箱地址。
- “登录名”系统唯一，一旦创建，不能修改。
- “角色”、“部门”用户个人不能修改，仅能由有用户管理权限用户统一管理，详细说明请参见**查询和修改用户信息**。

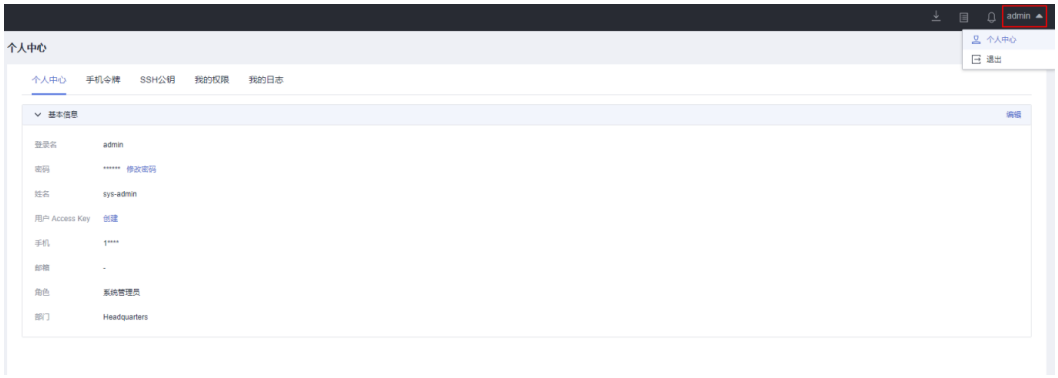
本小节主要介绍如何在个人中心修改个人密码和修改个人基本信息。

修改个人密码

步骤1 登录堡垒机系统。

步骤2 选择右上角用户名，单击“个人中心”，进入个人中心管理页面。

图 15-7 个人中心页面



步骤3 在“基本信息”页签，单击“修改密码”。

步骤4 输入当前密码，并自定义新密码。

新密码要求：

- 长度范围：8~32个字符。
- 规则要求：可设置英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（!@$%^-_=+[{}]:,./?~#*），且需同时至少包含其中三种。
- 不能包含用户名或倒序的用户名。

步骤5 确认无误，单击“确定”，返回个人基本信息页面。

退出登录，再次登录新密码即生效。

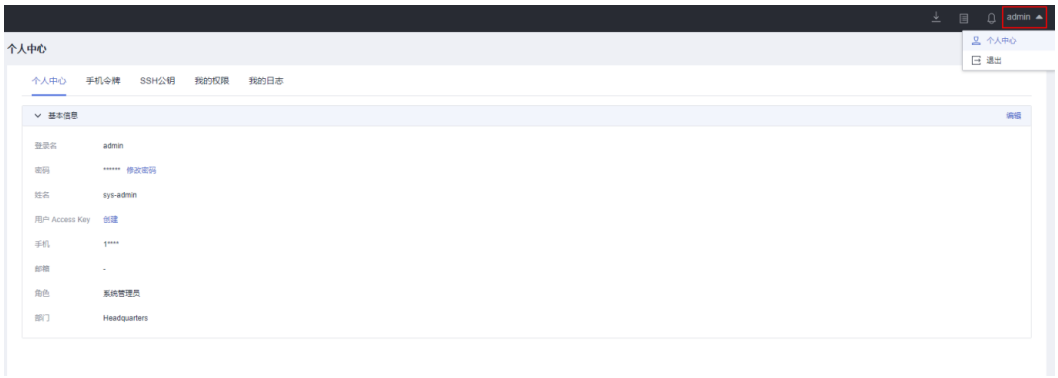
----结束

修改基本信息

步骤1 登录堡垒机系统。

步骤2 选择右上角用户名，单击“个人中心”，进入个人中心管理页面。

图 15-8 个人中心页面



步骤3 单击“编辑”，弹出基本信息修改窗口。

步骤4 输入用户“姓名”、“手机”或“邮箱”。

步骤5 单击“确定”，返回个人基本信息页面。

修改后用户姓名、手机号码、邮箱地址立即生效。

----结束

15.4 任务中心

任务中心是系统执行任务接收状态提示管理中心。

- 任务类型：导入用户、导入主机、导入云主机、导入应用、导入应用服务器、导入账户、账户改密、AD域同步、系统维护（升级和还原）、生成视频、账户同步、账户验证、配置备份、自动运维、导入动态令牌、安装Agent。
- 任务状态共有3种，分别包括“进行中”、“已完成”、“已停止”。

操作步骤

步骤1 登录堡垒机系统。

步骤2 单击右上角，展开任务中心小窗口。

可查看最新三条“执行中”任务。

图 15-9 任务中心小窗口

步骤3 单击“查看更多”，进入任务中心列表页面。

图 15-10 任务中心列表

步骤4 查询任务。

在搜索框中输入关键字，根据任务标题内容快速查询任务。

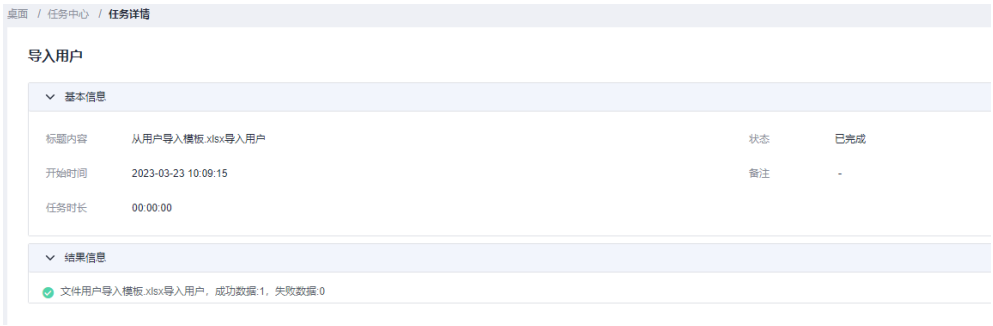
步骤5 查看任务列表。

在任务列表可以查看到正在进行的任务、已完成的任务和被停止的任务。

步骤6 查看任务详情。

1. 单击目标任务名称，进入任务详情页面。
2. 可查看任务基本信息和任务执行结果。

图 15-11 查看任务详情。



----结束

15.5 消息中心

15.5.1 管理消息列表

消息中心是系统内各类消息接收提示管理中心。消息中心小窗可呈现最新三条未读消息。任务执行完成后，则可在任务中心查看全部任务。

- 消息类型共有5种，分别包括系统消息、业务消息、任务消息、命令告警、工单消息。
- 消息级别共有3种，分别包括“高”、“中”、“低”，消息级别越高代表消息重要程度越高。

查看消息提醒

步骤1 登录堡垒机系统。

步骤2 单击右上角，展开消息中心小窗口。

可查看最新三条未读消息。

图 15-12 消息中心小窗口

步骤3 单击“查看更多”，进入消息中心列表页面。

图 15-13 消息中心列表

步骤4 查询消息。

在搜索框中输入关键字，根据消息标题内容快速查询消息。

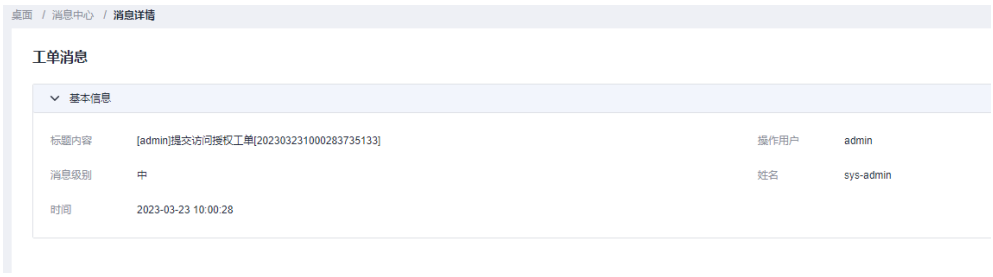
步骤5 查看消息列表。

消息按发生时间顺序倒序排列，可查看全部已读、未读的消息 。

步骤6 查看消息详情。

1. 单击目标消息名称，进入消息详情页面。
2. 可查看消息基本信息。

图 15-14 查看消息详情



----结束

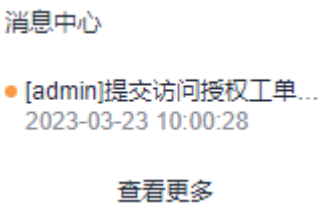
删除消息提醒

步骤1 登录堡垒机系统。

步骤2 单击右上角，展开消息中心小窗口。

可查看最新三条未读消息。

图 15-15 消息中心小窗口



步骤3 单击“查看更多”，进入消息中心列表页面。

图 15-16 消息中心列表

步骤4 勾选一条或多条消息，单击左下角“删除”，弹出删除消息确认窗口。

步骤5 单击“确定”，即可立即删除选中消息。

注意

消息删除后不可找回，请谨慎操作。

----结束

标记消息提醒

步骤1 登录堡垒机系统。

步骤2 单击右上角，展开消息中心小窗口。

可查看最新三条未读消息。

步骤3 单击“查看更多”，进入消息中心列表页面。

步骤4 标记一条或多条消息。

1. 选一条或多条消息，单击左下角“标为已读”，弹出标记消息确认窗口。
2. 单击“确定”，返回消息列表页面，目标消息状态更新为“已读”。

步骤5 标记全部消息。

1. 单击“全部已读”，弹出标记消息确认窗口。
2. 单击“确定”，返回消息列表页面，全部消息状态更新为“已读”。

----结束

15.5.2 新建系统公告

系统公告是对系统用户广播系统内重大变更的消息提醒。创建系统公告后，每个系统用户页面的顶部将会出现公告内容。

系统用户收到公告消息，单击“已阅”，可取消公告提醒。

约束限制

- 仅系统管理员admin可创建系统公告。

- 公告面向对象为全系统用户，不可指定用户。
- 一次仅能呈现一条系统公告。

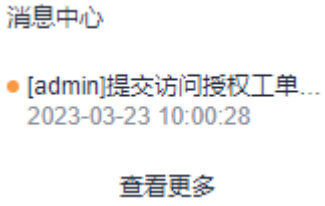
操作步骤

步骤1 登录堡垒机系统。

步骤2 单击右上角，展开消息中心小窗口。

可查看最新三条未读消息。

图 15-17 消息中心小窗口



步骤3 单击“查看更多”，进入消息中心列表页面。

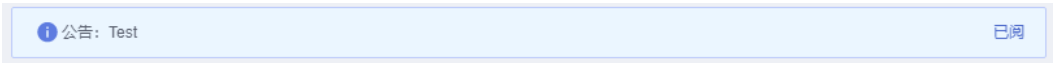
图 15-18 消息中心列表

步骤4 单击“新建公告”弹出公告编辑窗口。

步骤5 输入公告内容。

步骤6 单击“确定”，返回消息列表页面，即可查看到未读的系统公告内容。

图 15-19 消息公告



----结束

15.6 下载中心

下载中心提供客户端工具下载链接，包括数据库客户端等工具包，同时提供下载或导出任务的查看。

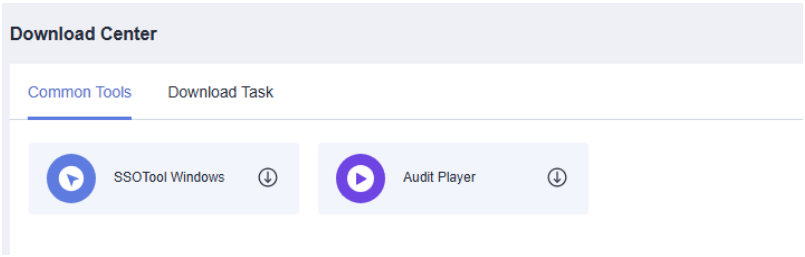
下载中心仅自己可见，生成的文件也仅自己可以下载。

操作步骤

步骤1 登录堡垒机系统。

步骤2 单击右上角，进入“下载中心”选择“常用工具”页签。

图 15-20 系统下载中心



步骤3 单击，即可跳转到第三方工具页面，根据实际需求下载工具。

步骤4 单击“下载任务”页签，查看下载详情。

- 同时下载任务数量超过15个后，将不能继续新增下载任务，需等待其他任务完成后方可继续。
- 历史会话的下载任务最多并行2个。
- 下载任务不可手动删除，到下载截止时间后自动删除。

----结束

16 实例部门管理

16.1 部门概述

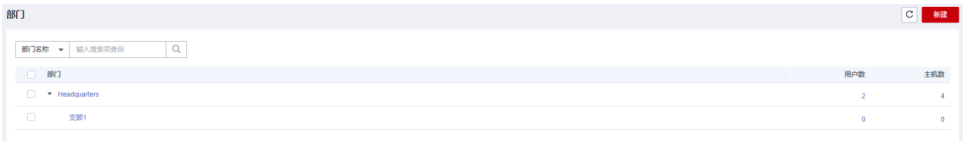
“部门”是用于划分组织结构，标识用户和资源的组织。系统默认有一个部门“总部”，仅可在“总部”基础上创建部门分支，且“总部”不可删除。

根据部门划分用户组织结构后，下级部门用户不能查看上级部门信息，包括上级部门组织结构、用户、主机资源、应用资源、应用发布服务器、资源账户，以及上级部门配置的策略信息和运维审计数据。

不同部门的用户，仅同部门和上级部门管理员可管理用户。

仅系统管理员**admin**或拥有“部门”模块权限的用户，可管理系统部门组织结构，包括新建部门、编辑部门、删除部门、查询部门用户和查询部门资源等。

图 16-1 部门管理



16.2 新建部门

堡垒机默认“总部”为系统最上级部门，仅可在“总部”基础上创建部门分支。

前提条件

已获取“部门”模块操作权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 在左侧导航树中，选择“部门”，进入部门管理页面。

步骤3 单击页面右上角的“新建”，弹出“新建部门”窗口。

步骤4 选择“上级部门”，输入待新建的“部门名称”，并根据需要输入简要“部门描述”。

说明

- 系统内自定义的“部门名称”不能重复。
- 上级部门仅能在已有部门目录树中选择。

步骤5 单击“确定”，返回部门管理页面，查看新建的部门。

----结束

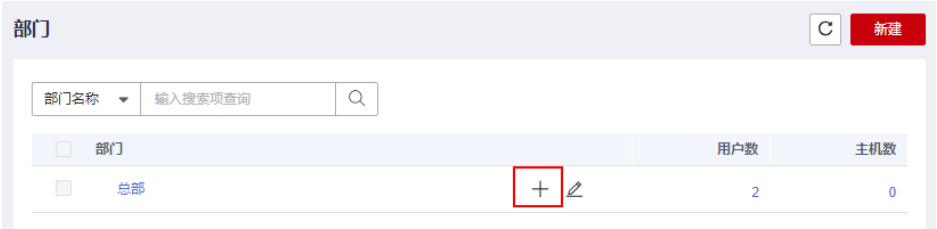
快速创建

步骤1 登录堡垒机系统。

步骤2 选择“部门”，进入部门管理页面。

步骤3 鼠标悬停到目标上级部门列，单击 + 快速创建下级部门。

图 16-2 快速创建下级部门



步骤4 修改部门名称，即完成快速创建下级部门。

----结束

16.3 删除部门

堡垒机默认“总部”为系统最上级部门，不可删除。删除上级部门，默认删除下级部门。

前提条件

已获取“部门”模块操作权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“部门”，进入部门管理页面。

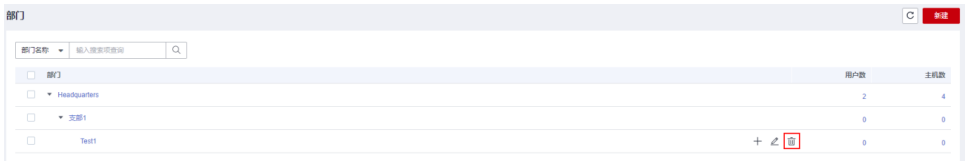
步骤3 单个删除。

鼠标悬停到要删除的部门所在行，显示快捷删除，单击快捷键删除该部门。

说明

删除部门时，其下级部门和所有部门下的用户和资源会被同时删除。

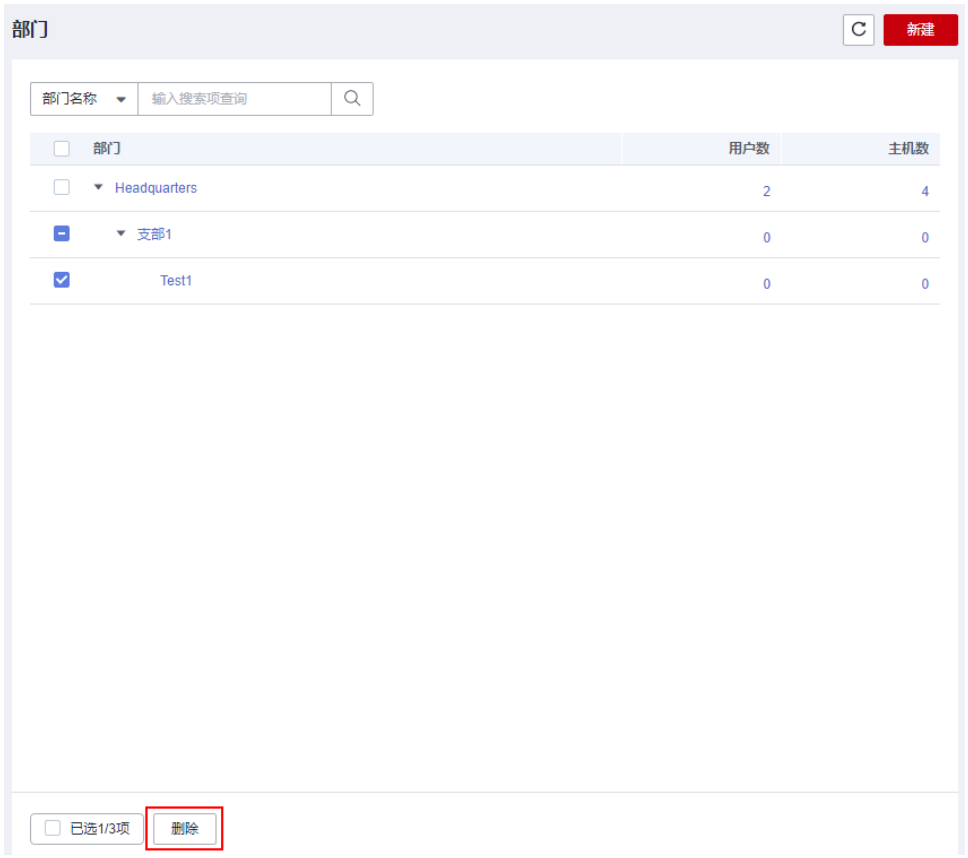
图 16-3 单个删除部门



步骤4 批量删除。

同时勾选多个部门，然后单击列表下方的“删除”，可以批量删除多个部门。

图 16-4 批量删除部门



----结束

16.4 查看和修改部门信息

堡垒机支持修改部门名称、移动部门所属上级部门。

移动部门后，部门下资源和用户自动移动上级部门归属。

前提条件

已获取“部门”模块操作权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“部门”，进入部门管理页面。

步骤3 单击要修改的部门的名称，进入部门详情页面。

步骤4 在“基本信息”区域，可查看部门基本信息。

单击“编辑”，弹出部门信息配置窗口，即可修改部门的基本信息。

----结束

16.5 查询部门配置

堡垒机支持分别统计各部门的用户数和主机数，通过在部门管理页面，可查询部门的用户和主机资产配置。应用资源和应用发布服务器不纳入统计。

前提条件

已获取“部门”模块操作权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“部门”，进入部门管理页面。

步骤3 在搜索框内输入部门名称，即可查询到部门所归属的上级部门树结构。

步骤4 查看部门“用户数”或“主机数”。

步骤5 单击相应数值，跳转到筛选后的用户管理或主机管理页面，即可查看部门配置。

----结束

17 维护管理

17.1 数据维护

17.1.1 查看系统内存

堡垒机存储空间分为系统分区和数据分区。当数据分区可用内存不足时，建议您及时删除历史系统数据。

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 在“存储概览”区域，即可查看系统分区和数据分区的空间使用情况。

图 17-1 存储空间概览

----结束

配置下载任务

步骤1 在存储配置页面，单击“下载任务”栏右侧的“编辑”。

步骤2 在弹窗中可对单个下载任务的大小进行配置。

说明

默认值是4，配置后不允许从堡垒机对超过该数值的文件进行打包下载，有效值为1-1024。

----结束

17.1.2 配置网盘空间

Web运维会话中，通过“主机网盘”可暂时存储来自主机或本地的文件，实现文件中转暂存。“主机网盘”即系统个人网盘，属于系统个人存储空间。

本小节主要介绍如何设置网盘空间大小，确保主机网盘的正常使用。

约束限制

- 网盘空间最大可使用空间为系统数据盘可使用空间大小。
- 设置“个人网盘空间”后，默认为系统用户预置相同大小的网盘空间，不支持按需配置。
- “主机网盘”中文件仅能由运维用户手动删除，不支持设置定期清理个人网盘空间。

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 在“网盘空间”区域，单击“编辑”，弹出网盘空间编辑窗口，设置网盘空间大小。

表 17-1 设置网盘空间

参数	说明
个人网盘空间	系统用户可使用的个人网盘空间大小。 ● 默认值为100MB。 ● 设置为0，表示在数据盘空间充足条件下，不限制用户使用个人网盘，个人网盘空间可无限使用。
网盘总空间	系统总可用网盘空间大小。 ● 默认值为5120MB。 ● 设置为0，表示在数据盘空间充足条件下，总网盘空间可无限使用。

步骤4 单击“确定”，返回存储配置管理页面，即可查看设置的“个人网盘空间”和“网盘总空间”。

步骤5 单击“详情”，进入网盘详情页面，可查看网盘的详细信息。

步骤6 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

17.1.3 删除系统数据

当系统数据盘使用率高于95%后，可能导致系统故障无法使用。为确保系统数据盘的正常使用，您可参考本小节配置自动删除或定期手动删除系统数据。

通过自动或手动删除的系统数据，主要为数据盘暂存的文件，包括历史会话视频大文件、本地备份的日志文件、本地备份的系统配置文件等。

须知

系统数据被删除后，默认不可找回，请谨慎操作。

约束限制

“手动删除”不能删除具体某一天的数据。手动删除选择日期，即删除该日期之前的全部数据。

前提条件

用户已获取“系统”模块管理权限。

配置自动删除

步骤1 登录堡垒机系统。

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 在“自动删除”区域，单击“编辑”，弹出自动删除配置窗口，配置相关参数。

表 17-2 配置自动删除

参数	说明
自动删除	选择开启或关闭自动删除功能，默认  。 •  ，表示开启自动删除功能。根据数据存储时间和数据盘空间使用率，触发自动清除。 • ，表示关闭自动删除功能。

参数	说明
自动删除（天）前数据	数据存储天数超过设定时长，将会被自动清除。 ● 默认为180天。 ● 取值范围为1～10000，单位为天。
空间满时覆盖之前数据	数据盘使用率超过90%时，将自动删除数据，建议开启。 选择开启或关闭，默认 。 ● ，表示关闭该功能。 ● ，表示开启该功能。 ● 自动删除规则： – 系统每隔30min检查一次数据盘使用率。当使用率低于90%时，则停止删除。 – 优先删除存储时间更久远的数据，默认先删除180天之前的数据。 – 若删除180天之前数据后，数据盘使用率仍高于90%，则逐日依次删除数据。 – 当天数据不能被自动删除。
下载任务有效时间	任务执行的有效时间，超过该值后待下载的文件将自动删除，默认值为60，有效值1-10000。
删除内容	删除内容可选择项如下： ● 系统日志 ● 会话日志

步骤4 单击“确认”，返回存储配置管理页面，查看配置的自动删除信息。

----结束

手动删除

步骤1 登录堡垒机系统。

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 在“手动删除”区域，选择一个日期。

说明

最近30天的数据暂不允许删除，30天内的日期不能选中。

步骤4 单击“删除”，则可立即删除该日期之前的全部数据。

----结束

17.1.4 创建数据本地备份

为加强对系统数据的容灾管理，堡垒机支持配置日志备份，提高审计数据安全性和系统可扩展性。

本小节主要介绍如何创建系统本地备份。

注意事项

- 支持系统本地备份的日志包括系统登录日志、资源登录日志、命令操作日志、文件操作日志、双人授权日志。
- 系统本地备份创建成功后，会在系统数据盘生成一个日志文件。

前提条件

用户已获取“系统”模块管理权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 数据维护 > 日志备份”，进入系统日志备份配置管理页面。

步骤3 在“本地备份”区域，单击“新建”，弹出日志本地备份窗口，配置需备份日志和备份日期范围。

表 17-3 创建本地备份

参数	说明
日志内容	选择需备份的日志类型。 ● 可勾选系统登录日志、资源登录日志、命令操作日志、文件操作日志、双人授权日志。 ● 至少需勾选一个类型。
时间范围	设置需备份的日志时间范围。 ● 至少需选择一天。
备注	简要描述该备份信息。 ● 最长128个汉字或字符。

步骤4 单击“确认”，返回日志备份管理页面，查看创建的系统本地备份信息。

----结束

后续管理

- 若需下载系统本地备份日志，单击“下载”，可立即将备份日志下载到用户本地服务器。
- 若需删除系统本地备份日志，单击“删除”，可删除在系统数据盘中备份的日志文件。

17.1.5 配置远程备份至 Syslog 服务器

为加强对系统数据的容灾管理，堡垒机支持配置日志备份，提高审计数据安全性和系统可扩展性。

注意事项

- 开启远程备份后，系统默认实时备份系统数据。
- 以天为单位自动备份，生成日志文件，并上传到Syslog服务器相应路径。
- 支持备份至Syslog服务器的日志包括系统登录日志、资源登录日志、命令操作日志、文件操作日志、双人授权日志。

前提条件

用户已获取“系统”模块管理权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 数据维护 > 日志备份”，进入系统日志备份配置管理页面。

步骤3 在“远程备份至Syslog服务器”区域，单击“编辑”，弹出备份至Syslog服务器配置窗口，配置服务器相关参数。

表 17-4 配置 Syslog 服务器远程备份

参数	说明
状态	选择开启或关闭备份至Syslog服务器，默认 。 • ，表示开启备份日志至Syslog服务器。每天零点自动启动备份。 • ，表示关闭备份日志至Syslog服务器。
发送者标识符	自定义堡垒机到Syslog服务器的标识符。用于在Syslog日志服务器，区分所接收的日志来自于相应的堡垒机。
服务器IP	输入Syslog服务器的IP地址。
端口	输入Syslog服务器的端口。
协议	选择Syslog服务器协议类型。 • 可选择TCP或UDP。 • 若选择TCP，可以单击“测试连通性”确认服务器是否可达。
备份内容	选择需备份的日志类型，至少需勾选一个类型。 • 系统登录日志：所有登录实例的操作记录日志。 • 资源登录日志：在当前实例登录已纳管资源的所有操作记录日志。 • 命令操作日志：在当前实例中执行的所有命令记录日志。 • 文件操作日志：对实例中文件的操作日志，包括上传、下载等。 • 双人授权日志：实例中执行双人授权操作的所有日志。

步骤4 单击“确定”，返回日志备份管理页面，查看创建的系统备份信息。

配置完成后，系统会每天零点定时将前一日的数据备份，并上传至远程Syslog服务器。

----结束

后续管理

- 若需关闭Syslog服务器备份，单击“编辑”，将状态置为关闭即可。
- 若需查看或下载备份到Syslog服务器的日志，请登录Syslog服务器操作。

17.1.6 配置远程备份至 FTP/SFTP 服务器

为加强对系统数据的容灾管理，堡垒机支持配置日志备份，提高审计数据安全性和系统可扩展性。

本小节主要介绍如何在系统配置FTP/SFTP服务器参数，将日志远程备份至FTP/SFTP服务器。

注意事项

- 开启远程备份后，系统默认在每天零点备份前一天的系统数据。
- 以天为单位自动备份，生成日志文件，并上传到FTP/SFTP服务器相应路径。
- 服务器同一路径下，不能重复备份同一天日志。
- 支持备份至FTP/SFTP服务器的日志包括系统配置、会话回放日志。

前提条件

用户已获取“系统”模块管理权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 数据维护 > 日志备份”，进入系统日志备份配置管理页面。

步骤3 在“远程备份至FTP/SFTP服务器”区域，单击“编辑”，弹出备份至FTP/SFTP服务器配置窗口，配置服务器相关参数。

表 17-5 配置 FTP 或 SFTP 服务器远程备份

参数	说明
状态	选择开启或关闭备份至FTP或SFTP服务器，默认 。 • ，表示开启备份日志至FTP或SFTP服务器。每天零点自动启动备份。 • ，表示关闭备份日志至FTP或SFTP服务器。 **说明** 启用后系统每天定时在凌晨00:30进行前一日的数据备份（改密日志为实时备份），会将数据备份至远程FTP/SFTP服务器。

参数	说明
传输模式	选择日志传输模式。 ● 可选择FTP或SFTP模式。
服务器IP	输入FTP或SFTP服务器的IP地址。
端口	输入FTP或SFTP服务器的端口。
用户名	输入FTP或SFTP服务器上用户名，用于测试配置的FTP或SFTP服务器是否可达。
密码	输入FTP或SFTP服务器上用户密码，用于测试配置的FTP或SFTP服务器是否可达。
存储路径	输入日志的存放路径。 ● 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***。 ● 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***。
测试连通性	用于测试配置的FTP或SFTP服务器是否可达。 ● 只检测堡垒机到FTP/SFTP服务器的网络状况，不验证服务器的用户账号。
备份内容	选择需备份的日志类型，至少需勾选一个类型。 ● 系统配置 ● 会话回放日志 ● 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

步骤4 单击“确定”，返回日志备份管理页面，查看创建的系统备份信息。

配置完成后，系统会每天零点定时将前一日的数据备份，并上传至远程FTP/SFTP服务器。

----结束

后续管理

- 若需立即备份某一天日志，可立即启动远程备份。

  在“远程备份至FTP/SFTP服务器”区域，选择需备份日志的日期，单击“备份”即可。
- 若需关闭FTP或SFTP服务器备份，单击“编辑”，将状态置为关闭即可。
- 若需查看或下载备份到FTP或SFTP服务器的日志，请登录FTP或SFTP服务器操作。

17.1.7 配置远程备份至 OBS 桶

为加强对系统数据的容灾管理，堡垒机支持配置日志备份，提高审计数据安全性和系统可扩展性。

本小节主要介绍如何在系统配置OBS桶参数，将日志远程备份至OBS桶。

注意事项

- 开启远程备份后，系统默认在每天零点备份前一天的系统数据。
- 以天为单位自动备份，生成日志文件，并上传到OBS桶相应文件夹。
- 服务器同一路径下，不能重复备份同一天日志。
- 支持备份至OBS桶的日志包括系统配置、会话回放日志。

前提条件

- 用户已获取“系统”模块管理权限。
- 已创建OBS桶，且创建的OBS桶与CBH系统网络通畅。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 数据维护 > 日志备份”，进入系统日志备份配置管理页面。

步骤3 在“远程备份至OBS服务器”区域，单击“编辑”，弹出备份至OBS桶配置窗口，配置桶相关参数。

表 17-6 配置桶参数说明

参数	说明
状态	选择开启或关闭备份至OBS桶，默认 。 • ，表示开启备份日志至OBS桶。每天零点自动启动备份。 • ，表示关闭备份日志至OBS桶。
Access Key ID	输入访问密钥ID，用于验证访问OBS桶请求发送者的身份。 与私有访问密钥关联的唯一标识符；访问密钥ID和私有访问密钥一起使用，对请求进行加密签名。
Secret Access Key	输入与访问密钥ID结合使用的私有访问密钥。 对请求进行加密签名，可标识发送方，并防止请求被修改。
EndPoint	输入桶所在区域的终端节点。
桶	输入桶名称。
存储路径	输入桶的路径或桶文件夹的路径，输入的文件夹路径不能包含两个以上相邻的斜杠（/）。 若OBS桶中无相应路径，将在桶中自动生成一个文件夹。 例如：cbh/bastion/.../...

参数	说明
测试连通性	用于测试配置的OBS桶的网络是否通畅。 只检测堡垒机到OBS桶的网络状况。
备份内容	选择需备份的日志类型，至少需勾选一个类型。 ● 系统配置 ● 会话回放日志 ● 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

步骤4 单击“确定”，返回日志备份管理页面，查看创建的系统备份信息。

配置完成后，系统会每天零点定时将前一日的数据备份，并上传至远程OBS桶。

----结束

后续管理

- 若需立即备份某一天日志，可立即启动远程备份。
  在“远程备份至OBS服务器”区域，选择需备份日志的日期，单击“备份”即可。
- 若需关闭OBS桶备份，单击“编辑”，将状态置为关闭即可。
- 若需查看或下载备份到OBS桶的日志，请登录OBS管理控制台，在相应桶文件夹下操作。

17.2 系统维护

17.2.1 查看系统状态

为了确认堡垒机系统的健康运行，可监控系统CPU、内存、磁盘、网络使用状态，及时了解系统的运行状况。

本小节主要介绍如何查看系统CPU、内存、磁盘、网络使用状态。

前提条件

已获取“系统”模块管理权限。

查看系统使用率

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统维护 > 系统状态”，进入系统状态页面。

图 17-2 查看系统状态

步骤3 展开“CPU/内存使用率”区域，可查看系统CPU或内存使用情况。

- 分别选择5分钟、15分钟、1小时，可分别呈现近5分钟、15分钟、1小时的CPU或内存使用率变化趋势图。
- 将鼠标放置在时刻点上，可查看该时刻的CPU或内存使用率情况。

----结束

查看磁盘读写状态

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统维护 > 系统状态”，进入系统状态页面。

步骤3 展开“磁盘读写状态”区域，可查看系统磁盘读取或写入使用情况。

- 分别选择5分钟、15分钟、1小时，可分别呈现近5分钟、15分钟、1小时的磁盘读取或写入速率变化趋势图。
- 将鼠标放置在时刻点上，可查看该时刻的读取或写入速率。

----结束

查看网络收发状态

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统维护 > 系统状态”，进入系统状态页面。

步骤3 展开“网络收发状态”区域，可查看系统接收或发送情况。

- 分别选择5分钟、15分钟、1小时和24小时，可分别呈现近5分钟、15分钟、1小时和24小时的网络接收和发送速率变化趋势图。
- 可分别查看eth0和eth1网络接口的收发状态。
- 将鼠标放置在时刻点上，可查看该时刻的发送或接收速率。

----结束

17.2.2 维护系统信息

本小节主要介绍如何更新系统IP地址、更新系统时间、更新实例版本，以及如何重启系统、关闭系统、恢复出厂设置等，管理系统基本信息和状态。

前提条件

已获取“系统”模块管理权限。

管理系统地址

当系统位于NAT或防火墙后，请设置为NAT外网地址，否则会导致FTP等应用无法连接。

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统维护 > 系统管理”，进入系统管理页面。

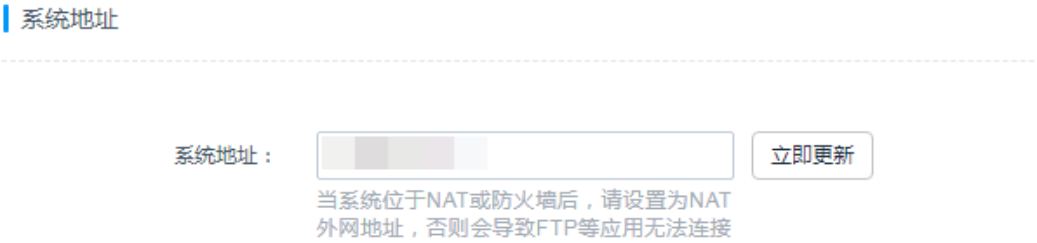
图 17-3 系统管理

步骤3 展开“系统地址”区域，可管理系统登录IP地址。

步骤4 更新IP地址。

- 当用户修改了实例绑定EIP后，输入新IP地址，更新系统IP地址。
- 系统地址需为NAT外网地址，否则会导致FTP等应用无法连接。

图 17-4 系统地址



----结束

管理系统时间

说明

当系统时间不正确时，将影响策略和工单的生效，也会导致“手机令牌”、“动态令牌”的绑定验证不通过。

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统维护 > 系统管理”，进入系统管理页面。

图 17-5 系统管理

步骤3 展开“系统时间”区域，可管理系统时间。

步骤4 手动更新系统时间。

1. 单击“修改”，弹出系统时间修改窗口。
2. 选择目标日期和时刻。
3. 单击确定，返回系统管理页面，系统时间更新完成。

步骤5 同步服务器时间。

默认同步当前系统的时间。

1. 选择系统自带时间服务器，或者输入时间服务器IP地址。
2. 单击“同步时间”，即可完成时间同步。

----结束

管理系统版本

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统维护 > 系统管理”，进入系统管理页面。

图 17-6 系统管理

步骤3 展开“系统升级”区域，可管理实例版本信息。

步骤4 升级实例版本。

说明

建议通过实例侧升级实例版本，详细操作请参见**升级版本**。

1. 升级操作前，需要您校验升级包sha256值。
2. 单击“升级”，打开本地目录，选择并上传升级包。
3. 升级包上传成功，显示升级包的版本号，单击“确定”即可开始实例版本升级。
4. 版本升级完成后，系统自动重启约5min，重启完毕后完成版本升级。
5. 重新登录系统，选择“系统 > 关于系统”可查看升级后“设备版本”。

----结束

管理系统工具

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统维护 > 系统管理”，进入系统管理页面。

图 17-7 系统管理

步骤3 展开“系统工具”区域，可管理系统工具，包括重启、升级、恢复出厂设置。

- 重启系统。

  说明

  建议通过实例侧重启系统，详细操作请参见**重启实例**。

  a. 单击“重启”，弹出重启确认窗口。
  b. 单击“确认”，弹出管理员确认窗口。
  c. 输入系统管理员**admin**登录密码。
  d. 单击“确认”，验证通过后即可重启系统。
- 重启运维服务

  a. 单击“重启”，弹出重启确认窗口。
  b. 单击“确认”，弹出管理员确认窗口。
  c. 输入系统管理员**admin**登录密码。
  d. 单击“确认”，验证通过后即可重启运维服务。
- 恢复出厂设置。

  a. 单击“恢复出厂设置”，弹出确认窗口。
  b. 单击“确认”，弹出管理员确认窗口。
  c. 输入系统管理员**admin**登录密码。
  d. 单击“确认”，验证通过后即可恢复到系统的初始设置，系统所有的数据将被清空。

警告

非紧急特殊情况，请不要恢复出厂设置，否则将导致系统数据丢失。

----结束

17.2.3 系统配置备份与还原

为确保系统配置数据不丢失，可开启系统配置自动备份，或定期备份系统配置，维护系统配置。

本小节主要介绍如何备份系统配置、还原系统配置，以及如何管理备份列表。

备份数据会备份在堡垒机本地，会占用一定的空间，具体可以在备份列表查看不同日期备份的文件大小。

约束限制

- 系统备份文件仅限于本堡垒机系统使用，不能用于其他堡垒机系统。
- 系统配置备份仅备份系统配置参数，不能备份运维产生的系统数据，更多系统数据备份说明，请参见**数据维护**。

前提条件

已获取“系统”模块管理权限。

备份系统配置

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统维护 > 配置备份与还原”，进入系统配置备份管理页面。

步骤3 启动自动备份。

在“备份列表”区域，开启“自动备份”，系统将在每天零点自动对系统配置备份。

步骤4 立即启动备份。

1. 在“备份列表”区域，单击“新建”，弹出新建备份弹窗。
2. 输入备注信息来区分备份文件。
3. 单击“确定”开始备份，备份成功后，可在备份列表查看已备份文件。

----结束

还原系统配置

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统维护 > 配置备份与还原”，进入系统配置备份管理页面。

步骤3 还原系统配置，可选择如下任意一种方式。

- 一键还原系统配置。
  在备份列表生成备份文件后，即可一键还原系统配置。

a. 在“备份列表”区域，选择目标备份文件。
b. 单击对应“操作”列“还原”，恢复备份系统配置。

- 本地文件还原系统配置。
  a. 在“配置还原”区域，单击“单击上传”，打开本地文件目录。
  b. 选择已下载到本地的备份配置文件。
  c. 备份文件上传完成后，单击“确认”，立即开始还原系统配置。

步骤4 刷新页面，系统还原完成后，将重新登录系统。

----结束

管理备份列表

在备份列表生成备份文件后，可对备份文件进行下载和删除管理。

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统维护 > 系统状态”，进入系统状态页面。

步骤3 下载备份文件。

1. 在“备份列表”区域，选择目标备份文件。
2. 单击对应“操作”列“下载”，立即将备份文件下载到本地保存。

步骤4 删除备份文件。

1. 在“备份列表”区域，选择目标备份文件。
2. 单击对应“操作”列“删除”，立即删除备份文件，可释放系统存储空间。

----结束

17.2.4 系统授权许可

暂不支持通过系统授权许可更新实例License授权。当实例到期后，请重新申请实例使用堡垒机。

从3.3.62.0版本开始支持在不拆解HA的情况下分别为主备实例授权。

前提条件

已获取“系统”模块管理权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统维护 > 授权许可”，查看系统当前授权信息。

表 17-7 系统授权参数说明

参数	说明
客户信息	当时系统使用区域和可用区。
授权类型	系统默认内置“正式版”。

参数	说明
状态	“已激活”状态为授权许可正常使用状态。 ● 单击“更新许可证”，根据系统提示，下载许可申请文件，并联系供应商申请授权许可。导入供应商已授权的许可文件，更新许可证。 ● 单击“备份许可证”，下载当前系统许可证到本地保存。 **说明** 当资产数、用户数、并发数需求扩大，可更新授权许可证升级系统规格，对应需调整堡垒机CPU、内存、带宽配置。
初始主机状态	实例类型为主备时呈现该项。 “已激活”状态为授权许可正常使用状态。 ● 单击“更新许可证”，根据系统提示，下载许可申请文件，并联系供应商申请授权许可。导入供应商已授权的许可文件，更新许可证。 ● 单击“备份许可证”，下载当前系统许可证到本地保存。 **说明** 当资产数、用户数、并发数需求扩大，可更新授权许可证升级系统规格，对应需调整堡垒机CPU、内存、带宽配置。
初始备机状态	实例类型为主备时呈现该项。 “已激活”状态为授权许可正常使用状态。 ● 单击“更新许可证”，根据系统提示，下载许可申请文件，并联系供应商申请授权许可。导入供应商已授权的许可文件，更新许可证。 ● 单击“备份许可证”，下载当前系统许可证到本地保存。 **说明** 当资产数、用户数、并发数需求扩大，可更新授权许可证升级系统规格，对应需调整堡垒机CPU、内存、带宽配置。
产品ID	当前系统产品ID。
授权模块	系统支持功能模块，分**标准版**和**专业版**。 ● **标准版**仅包含“基础模块”。 ● **专业版**包含“基础模块”、“自动化运维”、“数据库审计”。 – 自动化运维包括“账户同步策略”模块、“配置备份策略”模块、“脚本管理”模块、“快速运维”模块、“运维任务”模块。 – 数据库审计支持添加数据库，通过调用本地数据库工具的方式连接到数据库，审计数据库日志记录和操作命令。
授权资源数	系统最多可添加资源数（包含主机资源和应用发布资源总数）。
授权资源并发连接数	系统不同用户可同时登录资源的协议连接数（包含主机资源和应用发布资源），即连接协议用户数与登录资源数的乘积。

----结束

17.2.5 系统网络诊断

当用户登录主机失败时，可通过网络诊断来判断堡垒机系统与主机网络是否可达。

- 对主机地址进行ping诊断，判断堡垒机系统与主机的ICMP协议是否可通信。
- 对主机地址进行路由追踪，判断堡垒机系统与主机之间路由是否可达。
- 对主机地址进行TCP端口诊断，判断堡垒机系统与主机之间的TCP协议端口是否可达。

说明

- 如果网络不可达，需先解决主机网络连接问题；
- 如果网络连通性正常，则需判断系统添加的主机用户名、密码、端口是否输入正确。

本小节主要介绍如何测试系统网络连通性。

前提条件

已获取“系统”模块管理权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统维护 > 网络诊断”，进入系统网络诊断页面。

步骤3 通过ping主机地址，检测网络连通性。

1. 信息类型选择“ping”。
2. 输入主机地址，单击“执行”，查看连通性测试结果。
3. 判断系统与主机的ICMP协议是否可通信。

步骤4 通过路由追踪主机地址，检测网络连通性。

1. 信息类型选择“路由追踪”。
2. 输入主机地址，单击“执行”，查看连通性测试结果。
3. 判断系统与主机之间路由是否可达。

步骤5 通过TCP端口检测，检测网络连通性。

1. 信息类型选择“TCP端口检测”。
2. 输入主机地址和端口号，单击“执行”，查看连通性测试结果。
3. 判断系统与主机之间的TCP协议端口是否可达。

----结束

17.2.6 系统诊断

可通过系统诊断页面获取当前堡垒机系统相关信息，查看当前的运行情况，包括综合信息、系统负载、内核信息、内存信息、网卡信息、磁盘使用信息、路由信息、ARP信息。

前提条件

已获取“系统”模块管理权限。

操作步骤

步骤1 登录堡垒机系统。

步骤2 选择“系统 > 系统维护 > 系统诊断”，进入系统诊断页面。

步骤3 选择“信息类型”，单击“获取信息”在信息窗口查看结果。

表 17-8 系统诊断参数说明

参数	说明
综合信息	获取系统的综合信息，包含内存、IO、CPU等信息。
系统负载	获取系统的负载信息。
内核信息	获取系统的内核信息。
内存信息	获取系统的内存信息。
网卡信息	获取系统的网卡信息。
磁盘使用信息	获取系统的磁盘使用信息。
路由信息	获取系统的路由信息。
ARP信息	获取系统的ARP信息。

图 17-8 系统诊断信息

----结束

18 安装应用发布服务器

18.1 应用发布服务器简介

针对Windows系统和特殊的Linux系统，在堡垒机控制台无法直接进行资源运维，需创建应用发布服务器，通过应用发布服务器来实现对资源的运维。

规格选型

在申请发布Windows服务器时，建议根据需要运维的资源数量来选择发布服务器的内存规格，以确保能正常运维所有资源。

表 18-1 Windows 应用发布服务器建议规格与资产数

内存规格	空负载时系统占用内存	剩余可用内存	支持的资产并发数（个）
4GiB	约800MiB	约3.2GiB	约16
8GiB	约800MiB	约7.2GiB	约36
16GiB	约800MiB	约15.2GiB	约76
32GiB	约800MiB	约31.2GiB	约156
64GiB	约800MiB	约63.2GiB	约316
128GiB	约800MiB	约127.2GiB	约636

18.2 安装 Windows Server 2019 应用服务器

18.2.1 安装服务器

前提条件

已获取服务器管理员账号与密码。

操作步骤

步骤1 使用管理员账号登录服务器。

步骤2 打开“服务器管理器”，选择“仪表板”，进入仪表板界面。

步骤3 单击“添加角色和功能”，打开“添加角色和功能向导”窗口，根据向导指示，逐步单击“下一步”操作。

步骤4 选择基于角色或基于功能的安装。

步骤5 在服务器池中选择目标服务器。

步骤6 在服务器角色窗口中，勾选“Active Directory域服务”、“DNS服务器”、“远程桌面服务”三个角色项。

步骤7 （可选）选择服务器所需要的其它功能，默认下一步跳过。

步骤8 选择“远程桌面服务 > 角色服务”，进入选择远程桌面角色服务窗口。

勾选“Remote Desktop Session Host”、“远程桌面连接代理”、“远程桌面授权”、“远程桌面网关”、“远程桌面Web访问”角色服务项。

步骤9 （可选）选择“Web服务器角色（IIS）> 角色服务”，进入选择网络策略和访问角色服务窗口，按默认选项执行。

步骤10 （可选）选择“网络策略和访问服务 ”，进入选择网络策略和访问服务窗口，默认勾选“网络策略服务器”选项。

步骤11 确认配置选择，单击“安装”，请耐心等待安装进度完成。

步骤12 安装进度结束后，单击“关闭”并重启应用发布服务器，即服务器角色安装完成。

----结束

18.2.2 授权并激活远程桌面服务

前提条件

- 已提前申购企业许可号码，并获取相关信息。
- 已获取服务器管理员账号与密码。

操作步骤

步骤1 使用管理员账号登录服务器。

步骤2 选择“开始 > 管理工具 > 远程桌面服务 >RD授权管理器”，打开RD授权管理器界面。

步骤3 选择未激活的目标服务器，鼠标右键选择“激活服务器”。

步骤4 打开服务器激活向导界面，根据界面引导操作。

步骤5 选择自动连接方式。

步骤6 输入公司名称和用户姓名。

步骤7 （可选）输入公司详细通讯信息。

步骤8 确认安装启动许可证安装向导。

步骤9 许可证计划选择“企业协议”。

步骤10 输入企业协议号码。

说明

企业协议号码需提前向第三方平台申购获取官方远程桌面授权许可。

步骤11 选择服务器版本为“Windows server 2019”，选择许可证类型为“RDS每用户CAL”，选择许可证数为100。

步骤12 完成许可证安装，激活服务器，返回RD授权管理页面，查看服务器已激活。

----结束

18.2.3 修改组策略

前提条件

已获取服务器管理员账号与密码。

打开本地组策略编辑器

打开CMD运行窗口，输入**gpedit.msc**，打开本地组策略编辑器。

选择指定的远程桌面许可证服务器

步骤1 选择“计算机配置 > 管理模板 > Windows组件 > 远程桌面服务 > 远程桌面会话主机 > 授权”，进入服务器授权许可设置页面。

步骤2 双击“使用指定的远程桌面许可证服务器”，打开设置窗口。

步骤3 勾选“已启用”，启用远程桌面许可证服务器，并输入本服务器地址。

步骤4 单击“确认”，完成设置。

----结束

隐藏有关影响 RD 会话主机服务器的 RD 授权问题的通知

步骤1 选择“计算机配置 > 管理模板 > Windows组件 > 远程桌面服务 > 远程桌面会话主机 > 授权”，进入服务器授权许可设置页面。

步骤2 双击“隐藏有关影响RD会话主机服务器的RD授权问题的通知”，打开设置窗口。

步骤3 勾选“已启用”，启用隐藏通知，并配置本服务器地址。

步骤4 单击“确定”，完成设置。

----结束

设置远程桌面授权模式

步骤1 选择“计算机配置 > 管理模板 > Windows组件 > 远程桌面服务 > 远程桌面会话主机 > 授权”，进入服务器授权许可设置页面。

步骤2 双击“设置远程桌面授权模式”，打开设置窗口。

步骤3 勾选“已启用”，启用远程桌面授权模式。

在“指定RD会话主机服务器的授权模式”下拉列表中选择“按用户”。

步骤4 单击“确定”，完成设置。

----结束

限制连接的数量

步骤1 选择“计算机配置 > 管理模板 > Windows组件 > 远程桌面服务 > 远程桌面会话主机 > 连接”，进入服务器连接配置页面。

步骤2 双击“限制连接的数量”，打开设置窗口。

步骤3 勾选“已启用”，开启连接数量限制。

设置允许RD最大连接数为999999。

步骤4 单击“确定”，完成设置。

----结束

允许远程启动未列出的程序

步骤1 选择“计算机配置 > 管理模板 > Windows组件 > 远程桌面服务 > 远程桌面会话主机 > 连接”，进入服务器连接配置页面。

步骤2 双击“允许远程启动未列出的程序”，打开设置窗口。

步骤3 勾选“已启用”，启用远程启动未列出的程序。

步骤4 单击“确定”，完成设置。

----结束

将远程桌面服务用户限制到单独的远程桌面服务会话

步骤1 选择“计算机配置 > 管理模板 > Windows组件 > 远程桌面服务 > 远程桌面会话主机 > 连接”，进入服务器连接配置页面。

步骤2 双击“将远程桌面服务用户限制到单独的远程桌面服务会话”，打开设置窗口。

步骤3 勾选“已禁用”，禁止将用户限制到单独的远程桌面服务会话。

步骤4 单击“确定”，完成设置。

----结束

设置已中断会话的时间限制

步骤1 选择“计算机配置 > 管理模板 > Windows组件 > 远程桌面服务 > 远程桌面会话主机 > 会话时间限制”，进入服务器会话时间限制配置页面。

步骤2 双击“设置已中断会话的时间限制”，打开设置窗口。

步骤3 勾选“已启用”，启用已中断会话的时间限制。

设置结束已断开连接的会话为1分钟。

步骤4 单击“确定”，完成设置。

----结束

刷新本地组策略

步骤1 关闭本地组策略编辑器对话框。

步骤2 打开CMD运行窗口，执行**gpupdate /force**，刷新本地策略。

步骤3 应用发布服务器部署完成，需要测试功能请将此服务器和服务器应用添加到堡垒机。

----结束

18.2.4 安装 RemoteApp 程序

*V3.3.26.0*及以上版本需要在应用发布服务器中安装RemoteAppProxy跳板工具。

前提条件

已获取服务器管理员账号与密码。

操作步骤

步骤1 使用管理员账号登录服务器。

步骤2 在服务器中，下载RemoteAPPProxyInstaller_xxx.zip（xxx为版本号）压缩包。

下载RemoteAppProxy2.0.1版本，请提交工单获取（适配3.3.26.0及以上版本堡垒机）。

说明

服务器需要有公网访问权限（绑定弹性EIP）。

步骤3 在应用服务器中，将RemoteAPPProxyInstaller_xxx.zip（xxx为版本号）压缩包进行解压。

步骤4 双击“RemoteAPPProxyInstaller_xxx.msi”（xxx为版本号）启动安装。

安装时请选择默认的安装路径。

步骤5 安装完成后，单击“关闭”。

----结束

18.3 安装 Windows Server 2016 应用服务器

18.3.1 安装服务器

前提条件

已获取服务器管理员账号与密码。

操作步骤

步骤1 使用管理员账号登录服务器。

步骤2 打开“服务器管理器”，选择“仪表板”，进入仪表板界面。

步骤3 单击“添加角色和功能”，打开“添加角色和功能向导”窗口，根据向导指示，逐步单击“下一步”操作。

步骤4 选择基于角色或基于功能的安装。

步骤5 在服务器池中选择目标服务器。

步骤6 在服务器角色窗口中，勾选“Active Directory域服务”、“DNS服务器”、“远程桌面服务”三个角色项。

步骤7 （可选）选择服务器所需要的其它功能，默认下一步跳过。

步骤8 选择“远程桌面服务 > 角色服务”，进入选择远程桌面角色服务窗口。

勾选“Remote Desktop Session Host”、“远程桌面连接代理”、“远程桌面授权”、“远程桌面网关”、“远程桌面Web访问”角色服务项。

步骤9 （可选）选择“Web服务器角色（IIS）> 角色服务”，进入选择网络策略和访问角色服务窗口，按默认选项执行。

步骤10 （可选）选择“网络策略和访问服务 ”，进入选择网络策略和访问服务窗口，默认勾选“网络策略服务器”选项。

步骤11 确认配置选择，单击“安装”，请耐心等待安装进度完成。

步骤12 安装进度结束后，单击“关闭”并重启应用发布服务器，即服务器角色安装完成。

----结束

18.3.2 授权并激活远程桌面服务

前提条件

- 已提前申购企业许可号码，并获取相关信息。
- 已获取服务器管理员账号与密码。

操作步骤

步骤1 使用管理员账号登录服务器。

步骤2 选择“开始 > 管理工具 > 远程桌面服务 >RD授权管理器”，打开RD授权管理器界面。

步骤3 选择未激活的目标服务器，鼠标右键选择“激活服务器”。

步骤4 打开服务器激活向导界面，根据界面引导操作。

步骤5 选择自动连接方式。

步骤6 输入公司名称和用户姓名。

步骤7 （可选）输入公司详细通讯信息。

步骤8 确认安装启动许可证安装向导。

步骤9 许可证计划选择“企业协议”。

步骤10 输入企业协议号码。

说明

企业协议号码需提前向第三方平台申购获取官方远程桌面授权许可。

步骤11 选择服务器版本为“Windows server 2016”，选择许可证类型为“RDS每用户CAL”，选择许可证数为100。

步骤12 完成许可证安装，激活服务器，返回RD授权管理页面，查看服务器已激活。

----结束

18.3.3 修改组策略

前提条件

已获取服务器管理员账号与密码。

打开本地组策略编辑器

打开CMD运行窗口，输入**gpedit.msc**，打开本地组策略编辑器。

选择指定的远程桌面许可证服务器

步骤1 选择“计算机配置 > 管理模板 > Windows组件 > 远程桌面服务 > 远程桌面会话主机 > 授权”，进入服务器授权许可设置页面。

步骤2 双击“使用指定的远程桌面许可证服务器”，打开设置窗口。

步骤3 勾选“已启用”，启用远程桌面许可证服务器，并输入本服务器地址。

步骤4 单击“确认”，完成设置。

----结束

隐藏有关影响 RD 会话主机服务器的 RD 授权问题的通知

步骤1 选择“计算机配置 > 管理模板 > Windows组件 > 远程桌面服务 > 远程桌面会话主机 > 授权”，进入服务器授权许可设置页面。

步骤2 双击“隐藏有关影响RD会话主机服务器的RD授权问题的通知”，打开设置窗口。

步骤3 勾选“已启用”，启用隐藏通知，并配置本服务器地址。

步骤4 单击“确定”，完成设置。

----结束

设置远程桌面授权模式

步骤1 选择“计算机配置 > 管理模板 > Windows组件 > 远程桌面服务 > 远程桌面会话主机 > 授权”，进入服务器授权许可设置页面。

步骤2 双击“设置远程桌面授权模式”，打开设置窗口。

步骤3 勾选“已启用”，启用远程桌面授权模式。

在“指定RD会话主机服务器的授权模式”下拉列表中选择“按用户”。

步骤4 单击“确定”，完成设置。

----结束

限制连接的数量

步骤1 选择“计算机配置 > 管理模板 > Windows组件 > 远程桌面服务 > 远程桌面会话主机 > 连接”，进入服务器连接配置页面。

步骤2 双击“限制连接的数量”，打开设置窗口。

步骤3 勾选“已启用”，开启连接数量限制。

设置允许RD最大连接数为999999。

步骤4 单击“确定”，完成设置。

----结束

允许远程启动未列出的程序

步骤1 选择“计算机配置 > 管理模板 > Windows组件 > 远程桌面服务 > 远程桌面会话主机 > 连接”，进入服务器连接配置页面。

步骤2 双击“允许远程启动未列出的程序”，打开设置窗口。

步骤3 勾选“已启用”，启用远程启动未列出的程序。

步骤4 单击“确定”，完成设置。

----结束

将远程桌面服务用户限制到单独的远程桌面服务会话

步骤1 选择“计算机配置 > 管理模板 > Windows组件 > 远程桌面服务 > 远程桌面会话主机 > 连接”，进入服务器连接配置页面。

步骤2 双击“将远程桌面服务用户限制到单独的远程桌面服务会话”，打开设置窗口。

步骤3 勾选“已禁用”，禁止将用户限制到单独的远程桌面服务会话。

步骤4 单击“确定”，完成设置。

----结束

设置已中断会话的时间限制

步骤1 选择“计算机配置 > 管理模板 > Windows组件 > 远程桌面服务 > 远程桌面会话主机 > 会话时间限制”，进入服务器会话时间限制配置页面。

步骤2 双击“设置已中断会话的时间限制”，打开设置窗口。

步骤3 勾选“已启用”，启用已中断会话的时间限制。

设置结束已断开连接的会话为1分钟。

步骤4 单击“确定”，完成设置。

----结束

关闭自动根证书更新（V3.3.26.0）

升级到*V3.3.26.0*及以上的版本需要执行该操作，“V3.3.26.0”之前的版本不执行本章节的相关操作。

步骤1 选择“管理模板 > 系统 > Internet 通信管理”，进入“Internet 通信管理”页面。

步骤2 双击“关闭自动根证书更新”，打开设置窗口。

步骤3 勾选“已启用”，启用关闭自动根证书更新。

步骤4 单击“确定”，完成设置。

----结束

证书路径验证设置（V3.3.26.0）

升级到*V3.3.26.0*及以上的版本需要执行该操作，“V3.3.26.0”之前的版本不执行本章节的相关操作。

步骤1 选择“Windows设置 > 安全设置 > 公钥策略”，进入对象类型页面。

步骤2 双击“证书路径验证设置”，打开设置窗口。

步骤3 选择“网络检索”页签。

步骤4 取消勾选“自动更新Microsoft根证书程序中的证书(推荐)(M)”。

“默认URL检索超时(以秒为单位)”的值设置为“1”。

步骤5 单击“确定”，完成设置。

----结束

刷新本地组策略

步骤1 关闭本地组策略编辑器对话框。

步骤2 打开CMD运行窗口，执行**gpupdate /force**，刷新本地策略。

步骤3 应用发布服务器部署完成，需要测试功能请将此服务器和服务器应用添加到堡垒机。

----结束

18.3.4 安装 RemoteApp 程序

*V3.3.26.0*及以上版本需要在应用发布服务器中安装RemoteAppProxy跳板工具。

前提条件

已获取服务器管理员账号与密码。

操作步骤

步骤1 使用管理员账号登录服务器。

步骤2 在服务器中，下载RemoteAPPProxyInstaller_xxx.zip（xxx为版本号）压缩包。

下载RemoteAppProxy2.0.1版本，请提交工单获取（适配3.3.26.0及以上版本堡垒机）。

说明

服务器需要有公网访问权限（绑定弹性EIP）。

步骤3 在应用服务器中，将RemoteAPPProxyInstaller_xxx.zip（xxx为版本号）压缩包进行解压。

步骤4 双击“RemoteAPPProxyInstaller_xxx.msi”（xxx为版本号）启动安装。

安装时请选择默认的安装路径。

步骤5 安装完成后，单击“关闭”。

----结束

18.4 安装 Windows Server 2012 R2 应用服务器

18.4.1 安装服务器

步骤1 打开“服务器管理器”，选择“仪表板”，进入仪表板界面。

步骤2 单击“添加角色和功能”，打开“添加角色和功能向导”窗口，根据向导指示，逐步单击“下一步”操作。

步骤3 选择基于角色或基于功能的安装。

步骤4 在服务器池中选择目标服务器。

步骤5 在服务器角色窗口中，勾选“Active Directory域服务”、“DNS服务器”、“远程桌面服务”三个角色项。

步骤6 （可选）选择服务器所需要的其它功能，默认下一步跳过。

步骤7 选择“远程桌面服务 > 角色服务”，进入选择远程桌面角色服务窗口。

勾选“Remote Desktop Session Host”、“远程桌面连接代理”、“远程桌面授权”、“远程桌面网关”、“远程桌面Web访问”角色服务项。

步骤8 （可选）选择“Web服务器角色（IIS）> 角色服务”，进入选择网络策略和访问角色服务窗口，按默认选项执行。

步骤9 （可选）选择“网络策略和访问服务 ”，进入选择网络策略和访问服务窗口，默认勾选“网络策略服务器”选项。

步骤10 确认配置选择，单击“安装”，请耐心等待安装进度完成。

步骤11 安装进度结束后，单击“关闭”并重启应用发布服务器，即服务器角色安装完成。

----结束

18.4.2 授权并激活远程桌面服务

前提条件

- 已提前申购企业许可号码，并获取相关信息。
- 已获取服务器管理员账号与密码。

操作步骤

步骤1 打开服务器管理器，选择“所有服务器 >选择服务器名称”，鼠标右键选择“RD授权管理器”，打开RD授权管理器界面。

步骤2 选择未激活的目标服务器，鼠标右键选择“激活服务器”。

步骤3 打开服务器激活向导界面，根据界面引导操作。

步骤4 选择自动连接方式。

步骤5 输入公司名称和用户姓名。

步骤6 （可选）输入公司详细通讯信息。

步骤7 确认安装启动许可证安装向导。

步骤8 许可证计划选择“企业协议”。

步骤9 输入企业协议号码。

说明

企业协议号码需提前向第三方平台申购获取官方远程桌面授权许可。

步骤10 选择服务器版本为“Windows server 2012 R2”，选择许可证类型为“RDS每用户CAL”，选择许可证数为100。

步骤11 完成许可证安装，激活服务器，返回RD授权管理页面，查看服务器已激活。

----结束

18.4.3 修改组策略

本地组策略编辑器

打开运行窗口，输入**gpedit.msc**，打开本地组策略编辑器。

使用指定的远程桌面许可证服务器

步骤1 选择“计算机配置 > 管理模板 > Windows组件 > 远程桌面服务 > 远程桌面会话主机 > 授权”，双击“使用指定的远程桌面许可证服务器”，打开设置窗口。

步骤2 启用远程桌面许可证服务器，并输入许可证服务器地址。

步骤3 单击“确认”，完成设置。

----结束

隐藏有关影响 RD 会话主机服务器的 RD 授权问题的通知

步骤1 选择“计算机配置 > 管理模板 > Windows组件 > 远程桌面服务 > 远程桌面会话主机 > 授权”，双击“隐藏有关影响RD会话主机服务器的RD授权问题的通知”，打开对话框。

步骤2 启用隐藏通知。

步骤3 单击“确定”，完成设置。

----结束

设置远程桌面授权模式

步骤1 选择“计算机配置 > 管理模板 > Windows组件 > 远程桌面服务 > 远程桌面会话主机 > 授权”，双击“设置远程桌面授权模式”，打开对话框。

步骤2 启用远程桌面授权模式，在“指定RD会话主机服务器的授权模式”下拉列表中选择“按用户”。

步骤3 单击“确定”，完成设置。

----结束

限制连接的数量

步骤1 选择“计算机配置 > 管理模板 > Windows组件 > 远程桌面服务 > 远程桌面会话主机 > 连接”，双击“限制连接的数量”，打开对话框。

步骤2 开启连接数量限制，允许RD最大连接数为999999。

步骤3 单击“确定”，完成设置。

----结束

允许远程启动未列出的程序

步骤1 选择“计算机配置 > 管理模板 > Windows组件 > 远程桌面服务 > 远程桌面会话主机 > 连接”，双击“允许远程启动未列出的程序”，打开对话框。

步骤2 启用远程启动未列出的程序。

步骤3 单击“确定”，完成设置。

----结束

将远程桌面服务用户限制到单独的远程桌面服务会话

步骤1 选择“计算机配置 > 管理模板 > Windows组件 > 远程桌面服务 > 远程桌面会话主机 > 连接”，双击“将远程桌面服务用户限制到单独的远程桌面服务会话”，打开对话框。

步骤2 禁用将用户限制到单独的远程桌面服务会话。

步骤3 单击“确定”，完成设置。

----结束

设置已中断会话的时间限制

步骤1 选择“计算机配置 > 管理模板 > Windows组件 > 远程桌面服务 > 远程桌面会话主机 > 会话时间限制”，双击“设置已中断会话的时间限制”，打开对话框。

步骤2 启用已中断会话的时间限制，并设置结束已断开连接的会话为1分钟。

步骤3 单击“确定”，完成设置。

----结束

关闭自动根证书更新（V3.3.26.0）

升级到*V3.3.26.0*及以上的版本需要执行该操作，“V3.3.26.0”之前的版本不执行本章节的相关操作。

步骤1 选择“管理模板 > 系统 > Internet 通信管理”，进入“Internet 通信管理”页面。

步骤2 双击“关闭自动根证书更新”，打开设置窗口。

步骤3 勾选“已启用”，启用关闭自动根证书更新。

步骤4 单击“确定”，完成设置。

----结束

证书路径验证设置（V3.3.26.0）

升级到*V3.3.26.0*及以上的版本需要执行该操作，“V3.3.26.0”之前的版本不执行本章节的相关操作。

步骤1 选择“Windows设置 > 安全设置 > 公钥策略”，进入对象类型页面。

步骤2 双击“证书路径验证设置”，打开设置窗口。

步骤3 选择“网络检索”页签。

步骤4 取消勾选“自动更新Microsoft根证书程序中的证书(推荐)(M)”。

“默认URL检索超时(以秒为单位)”的值设置为“1”。

步骤5 单击“确定”，完成设置。

----结束

刷新本地组策略

步骤1 关闭本地组策略编辑器对话框。

步骤2 打开运行窗口，执行**gpupdate /force**，刷新本地策略。

步骤3 应用发布服务器部署完成，需要测试功能请将此服务器添加到堡垒机。

----结束

18.4.4 安装 RemoteApp 程序

*V3.3.26.0*及以上版本需要在应用发布服务器中安装RemoteAppProxy跳板工具。

前提条件

已获取服务器管理员账号与密码。

操作步骤

步骤1 使用管理员账号登录服务器。

步骤2 在服务器中，下载RemoteAPPProxyInstaller_xxx.zip（xxx为版本号）压缩包。

下载RemoteAppProxy2.0.1版本，请提交工单获取（适配3.3.26.0及以上版本堡垒机）。

说明

服务器需要有公网访问权限（绑定弹性EIP）。

步骤3 在应用服务器中，将RemoteAPPProxyInstaller_xxx.zip（xxx为版本号）压缩包进行解压。

步骤4 双击“RemoteAPPProxyInstaller_xxx.msi”（xxx为版本号）启动安装。

安装时请选择默认的安装路径。

步骤5 安装完成后，单击“关闭”。

----结束

18.5 安装 Windows Server 2008 R2 应用服务器

18.5.1 安装环境介绍

以下为安装AD域环境的服务器信息：

- Windows Server版本：Windows Server 2008 R2（所有软件包已经全部安装完成）
- IP：192.168.X.X/X
- 网关：192.168.X.X
- DNS：192.168.X.X
- 域名：example.com
- 计算机名：server

18.5.2 安装 AD 域

修改计算机名和服务器静态 IP

修改服务IP地址，并且将DNS地址指向本机，然后修改计算机名为server。安装AD域服务之后，机器名称会自动变成“主机名+域名”的形式。

安装 AD 域

在命令行下输入**dcpromo.exe** ，安装AD域和DNS服务器，不能使用添加角色向导的方式将AD域和DNS服务器安装在一起。

AD 域服务安装向导

步骤1 安装AD域，单击“下一步”。

步骤2 单击“下一步”。

步骤3 选择“在新林中新建域”，单击“下一步”。

步骤4 单击“下一步”。

步骤5 设置林功能级别，在下拉菜单中选择“Windows Server 2008 R2”，单击“下一步”。

步骤6 勾选“DNS服务器”，单击“下一步”。

步骤7 界面显示“无法创建DNS委派”，单击“是”，然后继续。

步骤8 选择数据库文件和日志文件的目录，采用默认配置即可，单击“下一步”。

步骤9 设置目录还原模式的密码，还原模式的**Administrator**密码不等于系统密码，单击“下一步”。

步骤10 界面显示信息概要，单击“下一步”。

步骤11 勾选“完成后重新启动”。

步骤12 重启后，使用域用户登录。

步骤13 AD域环境安装完成。

----结束

18.5.3 安装远程桌面服务和 RD 授权

远程桌面服务安装和配置

步骤1 选择“服务器管理器 > 角色 > 添加角色”。

步骤2 勾选“远程桌面服务”，单击“下一步”。

步骤3 单击“下一步”。

步骤4 单击“下一步”。

步骤5 选择“始终安装远程桌面会话主机”，单击“下一步”。

步骤6 选择“角色服务”，勾选“远程桌面会话主机”和“远程桌面授权”，单击“下一步”。

步骤7 单击“下一步”。

步骤8 选择“不需要使用网络级别身份认证”，单击“下一步”。

步骤9 选择“以后配置”，单击“下一步”。

步骤10 界面默认显示的“Administrators”能够连接到RD会话主机服务器（如果有特别需要，请添加需要的用户或组），单击“下一步”。

步骤11 单击“下一步”。

步骤12 单击“下一步”。

步骤13 选择“稍后为SSL加密选择证书”，单击“下一步”。

步骤14 选择“以后”，单击“下一步”。

步骤15 默认，单击“下一步”。

步骤16 选择“角色服务”，勾选“网络策略服务器”，单击“下一步”。

步骤17 安装IIS，单击“下一步”。

步骤18 默认，单击“下一步”。

步骤19 默认，单击“安装”。

步骤20 界面显示安装过程，请等待。

步骤21 安装完成后，单击“关闭”，弹出重启服务器提示框，选择“是”自动重启服务器，单击“下一步”。

步骤22 服务器重启后，登录会自动弹出角色服务配置窗口，自动配置完成后单击“关闭”。

步骤23 选择“开始 > 管理工具 > 远程桌面服务 > 远程桌面会话主机配置”，在右侧窗口中双击“限制每个用户只能进行一个会话”，在“属性”中取消勾选“限制每个用户只能进行一个会话”，单击“确定”。

----结束

远程桌面授权激活

步骤1 选择“开始 > 管理工具 > 远程桌面服务 > RD授权管理器”，由于RD授权服务器还未激活，所以授权服务器图标右下角显示红色×号，选中授权服务器 ，单击鼠标右键，选择“激活服务器”。

步骤2 单击“下一步”。

步骤3 单击“下一步”。

步骤4 输入注册信息（必填选项），单击“下一步”。

步骤5 默认，单击“下一步”。

步骤6 默认勾选“立即启动许可证安装向导”，单击“下一步”。

步骤7 单击“下一步”。

步骤8 许可证计划项选择“企业协议”，单击“下一步”。

步骤9 输入协议号码，单击“下一步”。

步骤10 选择产品版本：“Windows Server 2008或Windows Server 2008 R2”，选择许可证类型：“TS或RDS每用户CAL”，输入允许的最大远程连接数量。

步骤11 单击“完成”。

步骤12 RD授权服务器已经激活，图标也由红“×”变为绿“√”，远程桌面服务的配置和激活全部完成。

----结束

18.5.4 修改组策略

本地组策略编辑器

步骤1 选择“开始 > 运行”，输入**gpedit.msc**打开组策略。

步骤2 选择“计算机配置 > 管理模板 > Windows组件 > 远程桌面服务 > 远程桌面会话主机 > 授权”，双击右侧的“使用指定的远程桌面许可证服务器”。

----结束

隐藏有关影响 RD 会话主机服务器的 RD 授权问题的通知

打开“隐藏有关影响RD会话主机服务器的RD授权问题的通知”对话框，选择“已启用”，单击“下一个设置”。

设置远程桌面授权模式

在“设置远程桌面授权模式”对话框中，选择“已启用”，在“指定RD会话主机服务器的授权模式”下拉列表中选择“按用户”，之后单击“确定”，完成设置。

配置终端服务多用户

步骤1 选择“开始 > 运行”，输入**gpedit.msc**打开组策略。

步骤2 选择“计算机配置 > 管理模板 > windows组件 > 远程桌面服务 > 远程桌面会话主机 > 连接”。

步骤3 修改“限制连接的数量” 为已启用，允许的最大连接数改为999999。

步骤4 修改“允许远程启动未列出的程序” 为已启用。

步骤5 单击“确定”。

步骤6 选择“计算机配置 > 管理模板 > windows组件 > 远程桌面服务 > 远程桌面会话主机 > 会话时间限制”。

步骤7 修改“设置已中断会话的时间限制”为已启用，修改“结束已断开连接的会话”为1分钟。

步骤8 单击“确定”。

----结束

关闭自动根证书更新（V3.3.26.0）

升级到*V3.3.26.0*及以上的版本需要执行该操作，“V3.3.26.0”之前的版本不执行本章节的相关操作。

步骤1 选择“管理模板 > 系统 > Internet 通信管理”，进入“Internet 通信管理”页面。

步骤2 双击“关闭自动根证书更新”，打开设置窗口。

步骤3 勾选“已启用”，启用关闭自动根证书更新。

步骤4 单击“确定”，完成设置。

----结束

证书路径验证设置（V3.3.26.0）

升级到*V3.3.26.0*及以上的版本需要执行该操作，“V3.3.26.0”之前的版本不执行本章节的相关操作。

步骤1 选择“Windows设置 > 安全设置 > 公钥策略”，进入对象类型页面。

步骤2 双击“证书路径验证设置”，打开设置窗口。

步骤3 选择“网络检索”页签。

步骤4 取消勾选“自动更新Microsoft根证书程序中的证书(推荐)(M)”。

“默认URL检索超时(以秒为单位)”的值设置为“1”。

步骤5 单击“确定”，完成设置。

----结束

刷新策略

步骤1 关闭本地组策略编辑器，选择“开始 > 运行”，执行**gpupdate /force**。

步骤2 刷新本地策略。

步骤3 应用发布服务器部署完成，需要测试功能请将此服务器添加到堡垒机。

----结束

18.5.5 安装 RemoteApp 程序

*V3.3.26.0*及以上版本需要在应用发布服务器中安装RemoteAppProxy跳板工具。

前提条件

已获取服务器管理员账号与密码。

操作步骤

步骤1 使用管理员账号登录服务器。

步骤2 在服务器中，下载RemoteAPPProxyInstaller_xxx.zip（xxx为版本号）压缩包。

下载RemoteAppProxy2.0.1版本，请提交工单获取（适配3.3.26.0及以上版本堡垒机）。

说明

服务器需要有公网访问权限（绑定弹性EIP）。

步骤3 在应用服务器中，将RemoteAPPProxyInstaller_xxx.zip（xxx为版本号）压缩包进行解压。

步骤4 双击“RemoteAPPProxyInstaller_xxx.msi”（xxx为版本号）启动安装。

安装时请选择默认的安装路径。

步骤5 安装完成后，单击“关闭”。

----结束

18.6 安装 Linux 应用服务器

基础环境要求

- 系统要求：EulerOS 2.9.8系统版本。
- 网络要求：服务器需要有公网访问权限（绑定弹性EIP）。
- 防火墙要求：开放2376（docker服务）端口和35000-40000端口。
- 磁盘空间要求：安装目录/var/lib所在分区，建议大小在50G以上。

前提条件

已获取Linux服务器root账号密码。

操作步骤

步骤1 使用root账号登录Linux服务器。

步骤2 在Linux服务器中，下载Linux环境app_publisher_x86_64_xxx.tar.gz（xxx为版本号）压缩包。

表 18-2 app_publisher 组件版本说明

堡垒机版本	支持架构	app_publisher组件版本	下载地址
V3.3.60.0及以后版本	x86	1.7.1_CentOS7	请提交工单获取
V3.3.52.0及以后版本	x86	1.6.1_CentOS7	**软件包下载地址**

步骤3 在Linux服务器中，执行以下命令，将app_publisher_x86_64_xxx.tar.gz（xxx为版本号）压缩包进行解压。

 # tar -xvf app_publisher_*.tar.gz

 # cd app_publisher

步骤4 环境之前是否已安装过firefox应用发布服务器。

- 是，执行以下命令，把之前安装的firefox docker镜像删除。

  # docker rmi 127.0.0.1:5000/psm-firefox:0.2

  删除后，继续执行**步骤5**。
- 否，执行**步骤5**。

步骤5 执行以下命令，部署脚本。

 # /bin/bash install.sh

步骤6 执行以下命令，检查服务状态。

 # service docker status

```
[root@localhost firefox]# service docker status
Redirecting to /bin/systemctl status docker.service
● docker.service - Docker Application Container Engine
   Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; vendor preset: disabled)
  Drop-In: /usr/lib/systemd/system/docker.service.d
           └─docker.conf
   Active: active (running) since Fri 2021-02-26 14:30:25 CST; 3 weeks 6 days ago
     Docs: https://docs.docker.com
 Main PID: 995 (dockerd)
    Tasks: 19
   Memory: 161.3M
   CGroup: /system.slice/docker.service
           ├─  995 /usr/bin/dockerd
           └─29505 /usr/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 8908 -container-i
```

active (running)表示应用发布服务器安装成功。

步骤7 创建share目录（仅针对堡垒机V3.3.26.0版本）。

 # mkdir /opt/autorun/share

步骤8 （可选）重启应用发布服务器。

----结束

18.7 升级 RemoteApp 或 app_publisher 程序

升级堡垒机实例版本后，通常需要同步升级Windows应用服务器的RemoteApp或Linux应用服务器的app_publisher至新版本，否则对应的应用发布功能无法正常运行，本小节介绍如何升级RemoteApp和app_publisher。

RemoteApp和app_publisher的升级步骤可概括为：先卸载旧版本，再重新安装新版本。

前提条件

- 已获取目标应用服务器管理员账号与密码。
- 安装Linux安装包时需要确保/var/lib路径有足够的空间安装。
- 已获取新版本的RemoteApp或app_publisher安装包。
  - app_publisher

    表 18-3 app_publisher 组件版本说明

堡垒机版本	支持架构	app_publisher组件版本	下载地址
V3.3.60.0及以后版本	x86	1.7.1_CentOS7	请提交工单获取
V3.3.52.0及以后版本	x86	1.6.1_CentOS7	软件包下载地址

  - RemoteApp

    新版本始终向前兼容，当前最新版本：RemoteAppProxy2.0.1版本，请提交工单获取

升级 RemoteApp（Windows 应用服务器）

步骤1 登录Windows应用服务器，进入“控制面板 > 程序 > 程序和功能”中卸载老版本RemoteApp程序。

Windows应用服务器地址在堡垒机实例的“资源 > 应用发布 > 应用服务器”页面查看。

步骤2 卸载完成后，上传并解压新版本RemoteApp安装包。

步骤3 双击解压包中的setup.exe进行安装，直到安装完成。

----结束

升级 app_publisher（Linux 应用服务器）

步骤1 登录Linux应用服务器，上传新版本app_publisher安装包并解压。

tar -zxvf app_publisher_V1.xxxxxxxxxx.tar.gz

```
[root@localhost ~]# tar -zxvf app_publisher_V1.7.0_CentOS7_B1_x86_64_2024082216.tar.gz
app_publisher_V1.7.0_CentOS7_B1_x86_64/
app_publisher_V1.7.0_CentOS7_B1_x86_64/dockerinstall/
app_publisher_V1.7.0_CentOS7_B1_x86_64/dockerinstall/lib/
app_publisher_V1.7.0_CentOS7_B1_x86_64/dockerinstall/lib/audit-libs-python-2.8.5-4.el7.x86_64.rpm
```

Linux应用服务器地址在堡垒机实例的“资源 > 应用发布 > 应用服务器”页面查看。

步骤2 执行以下命令卸载老版本docker镜像。

```
docker rmi $(docker images -q)
```

注意

卸载镜像时如果出现提示：Error response from daemon: conflict: unable to delete 4852fb6f5512 (cannot be forced) - image is being used by running container xxxx

依次执行以下命令，删除container会话，并重新卸载镜像。

```
docker rm -f $(docker ps -aq)
docker rmi $(docker images -q)
```

```
[root@localhost ~]# docker rmi $(docker images -q)
Untagged: 127.0.0.1:5000/psm-kingbase:1.0
Deleted: sha256:e8112c7ae487cbae343ce6bee22166427d0a35e2bda60b184a28c5f39a77a70c
Deleted: sha256:f68b8fd1a003743c94573d22d6ecc19810df5dc7213e25266b4cb90048413e0b
Deleted: sha256:2b5bf875ff1941ce4ce182cbbb765d5b9a87e19b6869dc11a723427873bd60b1
Deleted: sha256:5bdf5a86ba627281e87f7c428d685e5402fa0fa8043ebe4678293d8bd642fd3d
Deleted: sha256:5c5e89dbaa3eeb500886162b375638adc447136f6427dda64b142318010231c5
Untagged: 127.0.0.1:5000/psm-gbase8a:1.0
Deleted: sha256:5fb9d3d7ac01f8f71f0a22a684633df5a1d9a144da5253ce4990f5fa37c0629d
Deleted: sha256:87037e4f775af66db0d6909d5d0419d97f953a97b3f74321554a8f9798a9b40c
Deleted: sha256:b6a6f6ca70437e96019b85eb3f0b4fade2107f8d87878f1f5006b3d75e5259f0
Deleted: sha256:a88bb1af2d34ed6f2aaed4ff958257f505701e4b723d8eaecb73dcb73ffa3e36
Deleted: sha256:f24018d51ae7af3b12d83073996e539d6f03c7372e71c67d227f34f983a70038
Deleted: sha256:e9aae227662fc9606c1cc8d167797cbfcc872d845b393f7b3be47fda78e84748
Deleted: sha256:4e7d1588ff7214ef7119f965aa9c2d5f4ae37469bb96f18ff8be948b9ee8d528
Untagged: 127.0.0.1:5000/psm-dameng:1.0
Deleted: sha256:5264b8e6c5b3ad443ee52f793343737770c7dd4893ac43696a848c868923eb20
Deleted: sha256:acd0947d789f9fae23767969330e22ffbb18bdd46fad6680822ef2ea18dcaa99
Deleted: sha256:3d9e909bbb1be6b31ed251a45bcce6f42e5ee0ac6ea36c47acf2ff6d77f9b424
Deleted: sha256:2f47ebba5d3106677c1852879202f79f2f69588d551679ec874d082d02272515
Deleted: sha256:fd4ca087a14304b5e4c3317a7a68c6a549e921e4e18db930d3f972cacb5d819a
Error response from daemon: conflict: unable to delete 4852fb6f5512 (cannot be forced) - image is being used by ru
nning container c51b357b93e3
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# docker rm -f $(docker ps -aq)
c51b357b93e3
[root@localhost ~]# docker rmi $(docker images -q)
Untagged: 127.0.0.1:5000/psm-firefox:1.0
Deleted: sha256:4852fb6f551228b24e6e6368609d667eb74500829a5a831a4e83c6b632f39061
Deleted: sha256:0300fc4b884418279f6a0899b96ae5619864ed34676d90d7175dc28a812b4b90
Deleted: sha256:13aba614a4786d021988b09999730a18e96f196eb3e58d50cb556830c38ef306
Deleted: sha256:84b23f153fed1e0eb3fc2c4eb454ee78288b8ea45d7da869e07e130b1672aff6
Deleted: sha256:54047a1de78d5bb2b2ec82dd8091b70a5ab5745b7b8f7502394d0bc5817d0ec5
```

步骤3 卸载完成后，执行以下命令安装新版本app_publisher目录下安装包和镜像。

```
cd app_publisher_V1.xxxxxxx
./install.sh
```

安装完成后，如果当前堡垒机版本为3.3.38.0及以下版本，且app_publisher为V1.2.0及以下版本时，更新app_publish到1.2.0以上版本后，需要依次执行以下命令手动更新docker证书时间。

```
docker swarm update --cert-expiry 867240h0m0s
docker swarm ca --rotate
```

----结束

19 权限管理

19.1 创建用户并授权使用 CBH 实例

如果您需要对您所拥有的云堡垒机（Cloud Bastion Host，CBH）服务进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用CBH服务资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将CBH服务资源委托给更专业、高效的其他账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用服务的其它功能。

本章节为您介绍对用户授权的方法，操作流程如**图19-1**所示。

前提条件

给用户组授权之前，请您了解用户组可以添加的CBH服务权限，并结合实际需求进行选择，CBH服务支持的系统权限，请参见**表1-8**。

示例流程

图 19-1 给用户授予 CBH 权限流程

1. 创建用户组并授权

   在IAM控制台创建用户组，并授予云堡垒机的只读权限“CBH ReadOnlyAccess”。

2. 创建用户组并加入用户组

   在IAM控制台创建用户，并将其加入1中创建的用户组。

3. 用户登录并验证权限

   新创建的用户登录控制台，切换至授权区域，验证权限：

   - 在“服务列表”中选择云堡垒机，进入CBH实例主界面，单击“创建云堡垒机”，尝试创建CBH实例，若提示权限不足，无法创建CBH实例（假设当前权限仅包含“CBH ReadOnlyAccess”），表示“CBH ReadOnlyAccess”生效。
   - 在“服务列表”中选择除云堡垒机外（假设当前策略仅包含“CBH ReadOnlyAccess”）的任一服务，若提示权限不足，表示“CBH ReadOnlyAccess”已生效。

19.2 CBH 实例自定义策略

如果系统预置的CBH服务权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参考**CBH实例权限及授权项**。

目前支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见：IAM用户指南-创建自定义策略。本章为您介绍常用的CBH实例自定义策略样例。

CBH 自定义策略样例

- 示例1：授权用户变更规格CBH实例规格、升级CBH实例版本

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cbh:instance:upgrade",
                "cbh:instance:alterSpec"
            ]
        }
    ]
}
```

- 示例2：拒绝用户重启CBH实例

  拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在Allow和Deny，则遵循**Deny优先原则**。

  如果您给用户授予“CBH FullAccess”的系统策略，但不希望用户拥有“CBH FullAccess”中定义的重启云堡垒机的权限，您可以创建一条拒绝重启云堡垒机的自定义策略，然后同时将“CBH FullAccess”和拒绝策略授予用户，根据Deny优先原则，则用户可以对CBH实例执行除了重启云堡垒机外的所有操作。拒绝策略示例如下：

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "cbh:instance:reboot"
            ]
        }
    ]
}
```

- 示例3：多个授权项策略

  一个自定义策略中可以包含多个授权项，且除了可以包含本服务的授权项外，还可以包含其他服务的授权项，可以包含的其他服务必须跟本服务同属性，即都是项目级服务或都是全局级服务。多个授权语句策略描述如下：

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cbh:instance:create"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "vpc:subnets:get"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecs:cloudServerFlavors:get"
            ]
        }
```



```
  ]
}
```

19.3 CBH 实例权限及授权项

如果您需要对您所拥有的云堡垒机（Cloud Bastion Host，CBH）服务进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，IAM），如果账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用CBH实例的其它功能。

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使用户组中的用户获得相应的权限，这一过程称为授权。授权后，用户就可以基于已有权限对云服务进行操作。

权限根据授权的精细程度，分为角色和策略。角色以服务为粒度，是IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。策略授权更加精细，可以精确到某个操作、资源和条件，能够满足企业对权限最小化的安全管控要求。

支持的授权项

策略包含系统策略和自定义策略，如果系统策略不满足授权要求，管理员可以创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制。

- 权限：允许或拒绝某项操作。
- 授权项：自定义策略中支持的Action，在自定义策略中的Action中写入授权项，可以实现授权项对应的权限功能。

表 19-1 IAM3.0 支持的授权项

权限	对应API接口	授权项（Action）	IAM项目(Project)	企业项目(Enterprise Project)
查询ECS配额	GET /v2/{project_id}/cbs/instance/ecs-quota	cbh:instance:getEcsQuota	√	×
查看云堡垒机可用区	GET /v2/{project_id}/cbs/available-zone	cbh:instance:getAvailableZones	√	×
登录云堡垒机	POST /v2/{project_id}/cbs/instance/login	cbh:instance:login	√	×
关闭云堡垒机	POST /v2/{project_id}/cbs/instance/stop	cbh:instance:stop	√	×

权限	对应API接口	授权项（Action）	IAM项目(Project)	企业项目(Enterprise Project)
重启云堡垒机	POST /v2/{project_id}/cbs/instance/reboot	cbh:instance:reboot	√	×
升级云堡垒机软件版本	POST /v2/{project_id}/cbs/instance/upgrade	cbh:instance:upgrade	√	×
修改堡垒机admin用户密码	PUT /v2/{project_id}/cbs/instance/password	cbh:instance:resetPassword	√	×
启动云堡垒机	POST /v2/{project_id}/cbs/instance/start	cbh:instance:start	√	×
扩容云堡垒机规格	PUT /v2/{project_id}/cbs/instance	cbh:instance:alterSpec	√	×
创建云堡垒机	POST /v2/{project_id}/cbs/instance	cbh:instance:create	√	√
绑定或解绑EIP	• POST /v2/{project_id}/cbs/instance/{server_id}/eip/bind • POST /v2/{project_id}/cbs/instance/{server_id}/eip/unbind	cbh:instance:eipOperate	√	×
委托授权给CBH	POST /v2/{project_id}/cbs/agency/authorization	cbh:agency:authorize	√	×
查询云堡垒机列表	GET /v2/{project_id}/cbs/instance/list	cbh:instance:list	√	×
切换堡垒机实例的虚拟私有云	PUT /v2/{project_id}/cbs/instance/vpc	cbh:instance:switchInstanceVpc	√	×

权限	对应API接口	授权项（Action）	IAM项目(Project)	企业项目(Enterprise Project)
登录堡垒机admin控制台	GET /v2/{project_id}/cbs/instances/{server_id}/admin-url	cbh:instance:loginInstanceAdmin	√	×
修改单机堡垒机实例类型	PUT /v2/{project_id}/cbs/instance/type	cbh:instance:changeInstanceType	√	×
获取堡垒机内资产运维链接	GET /v2/{project_id}/cbs/instance/get-om-url	cbh:instance:getOmUrl	√	×

20 监控

20.1 CBH 监控指标说明

功能说明

本节定义了堡垒机上报云监控服务的监控指标的命名空间和监控指标列表，用户可以通过云监控服务提供管理控制台来检索堡垒机产生的监控指标和告警信息。

须知

堡垒机实例在V3.3.30及以上版本才支持对接云监控服务(CES)。

命名空间

SYS.CBH

说明

命名空间是对一组资源和对象的抽象整合。在同一个集群内可创建不同的命名空间，不同命名空间中的数据彼此隔离。使得它们既可以共享同一个集群的服务，也能够互不干扰。

监控指标

表 20-1 堡垒机服务支持的监控指标

指标ID	指标名称	指标含义	取值范围	单位	进制	维度	监控周期（原始指标）
cpu_util	CPU利用率	该指标为从物理机层面采集的CPU使用率，数据准确性低于从弹性云服务器内部采集的数据	0%~100%	%	不涉及	server_id	300秒
mem_util	内存使用率	该指标用于统计测量对象的内存利用率	0%~100%	%	不涉及	server_id	300秒
disk_util	磁盘使用率	该指标用于统计测量对象的磁盘利用率	0%~100%	%	不涉及	server_id	300秒
session_count	会话连接数	该指标用于统计测量对象的实时会话连接数	≥0	不涉及	不涉及	server_id	300秒
resource_count	管理资源数	该指标用于统计测量对象的管理资源数	≥0	不涉及	不涉及	server_id	300秒

维度

Key	Value
server_id	CBH实例ID。 获取方法请参见查看实例详情。

20.2 设置监控告警规则

通过设置堡垒机告警规则，用户可自定义监控目标与通知策略，设置告警规则名称、监控对象、监控指标、告警阈值、监控周期和是否发送通知等参数，帮助您及时了解堡垒机运行状况，从而起到预警作用。

前提条件

已创建堡垒机实例。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“管理与监管 > 云监控服务 ”。

步骤3 在左侧导航树栏，选择“告警 > 告警规则”，进入“告警规则”页面。

步骤4 在页面右上方，单击“创建告警规则”，进入“创建告警规则”界面。

步骤5 填写告警规则信息，填写规则如表20-2所示。

表 20-2 设置 CBH 告警规则参数说明

参数名称	参数说明	取值样例
名称	系统会随机产生一个名称，您也可以进行修改。	alarm-lm45
描述	告警规则描述。	-
告警类型	选择“指标”。	指标
资源类型	选择资源的类型，选择堡垒机。	堡垒机
维度	选择CBH。	CBH
监控范围	告警规则适用的资源范围，可选择资源分组或指定资源。	全部资源
触发规则	选择关联模板、导入已有模板或者自定义创建。	关联模板

参数名称	参数说明	取值样例
模板	从下拉框中选择模板“例如CBH告警模板”	-
告警策略	编辑“告警策略”。	-
发送通知	配置是否发送邮件、短信、HTTP和HTTPS通知用户。	是
通知方式	可选择通知组或者主题订阅。	主题订阅
通知对象	需要发送告警通知的对象，可选择云账号联系人或主题。 • 云账号联系人为注册账号时的手机和邮箱。 • 主题是消息发布或客户端订阅通知的特定事件类型，若此处没有需要的主题则需先创建主题并订阅该主题，该功能会调用消息通知服务（SMN）。	-
生效时间	该告警规则仅在生效时间内发送通知消息。	00:00-8:00
触发条件	可以选择“出现告警”、“恢复正常”两种状态，作为触发告警通知的条件。	-

步骤6 单击“立即创建”，在弹出的提示框中，单击“确定”， 告警规则创建成功。

----结束

20.3 查看监控指标

您可以通过管理控制台，查看CBH的相关指标，及时了解堡垒机防护状况，并通过指标设置防护策略。

前提条件

CBH已对接云监控，即已在云监控页面设置监控告警规则。有关设置监控告警规则的详细操作，请参见**设置监控告警规则**。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ，选择“管理与监管 > 云监控服务 ”。

步骤3 在左侧导航树栏，选择“云服务监控 > 云堡垒机”，进入“云服务监控”页面。

步骤4 在目标CBH实例所在行的“操作”列中，单击“查看监控指标”，查看对象的指标详情。

----结束

21 常见问题

21.1 产品咨询

21.1.1 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。

21.1.2 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。

21.1.3 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。

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。

21.1.4 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。

21.1.5 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实例的创建、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。

21.1.6 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。

21.1.7 自动化运维包括哪些内容?

云堡垒机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。

- 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。
- 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。
- 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。

21.1.8 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。

21.1.9 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21-1**。

表 21-1 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

场景描述	方向	协议/应用	端口
	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
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
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

21.1.10 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**网络访问限制**。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。

21.1.11 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。

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21-2。

表 21-2 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）

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21-3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 21-3 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
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21-4**所示。

表 21-4 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

21.2 申请

21.2.1 申请部署相关

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?** 。

21.2.2 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。

实例版本规格

表 21-5 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	• 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	• 50 • 100 • 200 • 500 • 1000 • 2000 • 5000 • 10000

表 21-6 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
50	50	4核	8GB	100GB	500GB
100	100	4核	8GB	100GB	1000GB
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。

21.2.3 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**default**，用户可选择**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。
- 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 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击 ☰，在服务列表选择“安全 > 云堡垒机”。

步骤3 单击“创建云堡垒机”，进入“创建云堡垒机实例”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。

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。

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21-1**配置。

步骤8 完成安全组规则配置，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。

21.3 备份/变更规格/升级

21.3.1 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21-7**。

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 21-7 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	-
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 21-8 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。
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。

21.3.2 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，用户为了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，为了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 21-9 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。

数据信息	导出	导入	说明
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

21.3.3 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。

21.4 文件传输类

21.4.1 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。

- 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?**

21.4.2 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。

----结束

21.4.3 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。

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）。

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。

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。

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。

----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。

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。

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。

----结束

21.4.4 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。
- 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。

21.4.5 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 21-1 排查思路图

表 21-10 解决办法

排查步骤	可能的原因	解决办法
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**。

排查步骤	可能的原因	解决办法
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。
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

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。

21.4.6 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”。

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?

21.4.7 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

21.4.8 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。

21.4.9 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

21.4.10 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。

21.5 CBH 系统登录

21.5.1 登录方式及密码类

21.5.1.1 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。

21.5.1.2 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。

21.5.1.3 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，形似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。

21.5.1.4 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创建实例时配置的密码。
- 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。

21.5.1.5 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。

- 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。

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21-2示例，单击“修改密码”，弹出“修改密码”对话框。

图 21-2 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

21.5.2 多因子认证类

21.5.2.1 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。

21.5.2.2 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

21.5.2.3 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。

21.5.2.4 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

21.5.2.5 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。

21.5.2.6 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。

21.5.3 登录安全类

21.5.3.1 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21-11**。

表 21-11 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。
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

21.5.3.2 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。

21.6 系统用户、资源及策略配置

21.6.1 系统用户类

21.6.1.1 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

21.6.1.2 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。

21.6.2 资源添加类

21.6.2.1 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。

21.6.2.2 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 21-12 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

21.6.2.3 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

21.6.2.4 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。

21.6.2.5 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21-13**。

表 21-13 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”。

21.6.2.6 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。

21.6.2.7 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

21.6.2.8 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 创建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

步骤3 添加应用资源

----结束

21.6.3 系统策略类

21.6.3.1 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。

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。

----结束

21.6.4 系统配置类

21.6.4.1 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

21.6.4.2 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

21.6.4.3 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。

21.7 运维资源

21.7.1 运维管理

21.7.1.1 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”。

21.7.1.2 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

21.7.1.3 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。

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

21.7.1.4 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。

21.7.1.5 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21-14**所示。

表 21-14 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

算法类型	H5页面运维	SSH客户端运维
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
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

21.7.2 运维操作

21.7.2.1 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。

21.7.2.2 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

21.7.2.3 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21-15**。

表 21-15 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

界面入口	可执行操作
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

21.7.2.4 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。

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

21.7.2.5 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。

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

21.7.2.6 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。

21.7.2.7 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。

21.8 审计运维日志

21.8.1 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。

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 21-16 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”。
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。

日志类型	日志内容
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”。

21.8.2 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”。

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

21.8.3 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。

21.8.4 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。

21.8.5 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。

21.8.6 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。

21.8.7 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。

21.8.8 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。

21.9 故障排除

21.9.1 登录系统故障

21.9.1.1 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。

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。

21.9.1.2 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。

21.9.1.3 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。

21.9.1.4 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。

21.9.1.5 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。

21.9.1.6 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。

21.9.1.7 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 21-3 检查网络配置

静态路由配置

目的地址	子网掩码/前缀	下一跳地址	路由类型	出口设备	Metric	备注
0.0.0.0	0.0.0.0	10.30.11.1	Static	eth1	0	-
0.0.0.0	0.0.0.0	10.30.11.1	Direct	eth1	101	-
10.30.11.0	255.255.255.0	0.0.0.0	Direct	eth1	101	-
100.64.0.0	255.192.0.0	192.168.0.1	Static	eth0	1	-
169.254.169.254	255.255.255.255	192.168.255.254	Direct	eth0	100	-
192.168.0.1	255.255.255.255	0.0.0.0	Direct	eth0	1	-
0.0.0.0	0.0.0.0	192.168.0.1	Direct	eth0	100	-
192.168.0.0	255.255.0.0	0.0.0.0	Direct	eth0	100	-

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。

21.9.2 登录资源故障

21.9.2.1 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。

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。

21.9.2.2 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

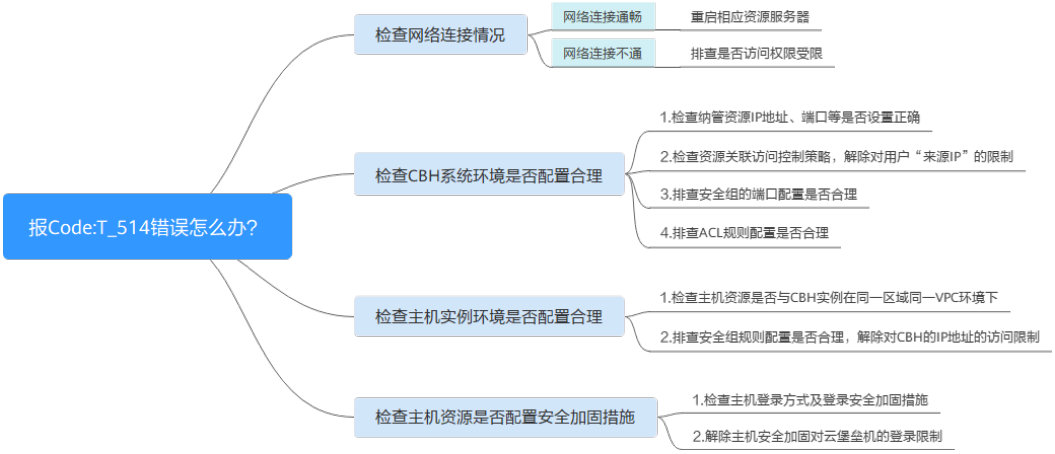
- 云堡垒机系统与资源服务器之间网络连接不稳定，导致连接断开。

- 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 21-4 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。
  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**

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

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。

21.9.2.3 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。

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。

21.9.2.4 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，导致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

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

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。

21.9.2.5 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 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。

21.9.2.6 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。

----结束

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。

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。

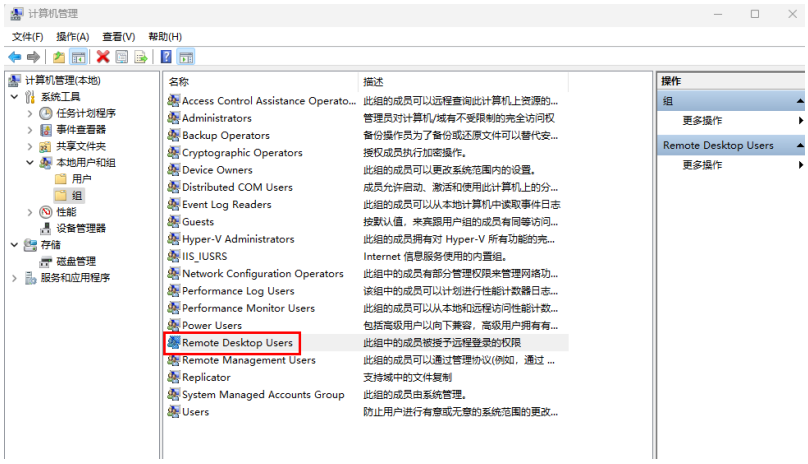
检查 Windows 主机登录用户是否已具备远程登录权限

如果您在Windows主机上使用新创建的用户通过远程登录方式登录堡垒机，请确保已先将该用户添加到远程登录组“Remote Desktop Users”中，使其具备远程登录权限。具体操作如下：

步骤1 在Windows主机上，使用快捷键“Win + X”，选择“计算机管理”。

步骤2 选择“系统工具 > 本地用户和组 > 组”，双击“Remote Desktop Users”，打开Remote Desktop Users属性窗口。

图 21-5 Remote Desktop Users 组



步骤3 查看用户是否已添加到“Remote Desktop Users”组的“成员”中。

若未添加，可单击“添加”，将目标用户添加到“Remote Desktop Users”组中。

图 21-6 添加组成员

----结束

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

21.9.2.7 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。

21.9.2.8 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 21-17 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 21-7 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。

21.9.2.9 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。
  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”。

21.9.2.10 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。

21.9.2.11 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。

21.9.2.12 如何解决“mstsc 客户端访问服务器资源时，移动界面应用有黑屏”的问题?

问题描述

通过mstsc客户端访问服务器资源时，移动界面应用有黑屏。

解决办法

步骤1 打开本地电脑的组策略，进入“计算机 > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Terminal Server Client”路径下。

步骤2 右键单击“Terminal Server Client”，单击“新建 > DWORD(32位)值(D)”，新建DWORD。

步骤3 将其DWORD命名为：RemoteDesktop_SuppressWhenMinimized，值设置为2。

----结束

修改注册表后提示错误

若您通过修改注册表后提示“无法连接至远程计算机”，则需要做如下调整。

步骤1 打开远程桌面连接程序，单击“显示选项”，选择“显示”。

步骤2 减小“显示配置”的分辨率，并且修改颜色为“增强色（16位）”。

步骤3 选择“体验”，修改连接速度为“低速宽带（256 kbps - 2 Mbps）”。

----结束

21.9.2.13 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

21.9.2.14 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

21.9.3 运维故障

21.9.3.1 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21-18**。

表 21-18 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

- 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。

21.9.3.2 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。

21.9.3.3 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。

21.9.3.4 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。

21.9.3.5 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。
  - 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。

21.9.3.6 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

21.9.3.7 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

21.9.3.8 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 排查EIP带宽受限原因。

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。

----结束

21.9.3.9 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。
  - 授权用户“剪切板”权限。
- 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。
2. 授权用户“文件管理”权限。

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

21.9.3.10 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21-19**。

表 21-19 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。
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。

错误码	错误提示	排查方法
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。
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**。

错误码	错误提示	排查方法
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。

21.9.3.11 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

21.9.3.12 应用运维登录后显示本次连接已断开怎么处理?

问题现象

应用运维登录后页面直接弹窗提示本次连接已断开，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

21.9.3.13 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

需要您自行重新创建商业证书后在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

