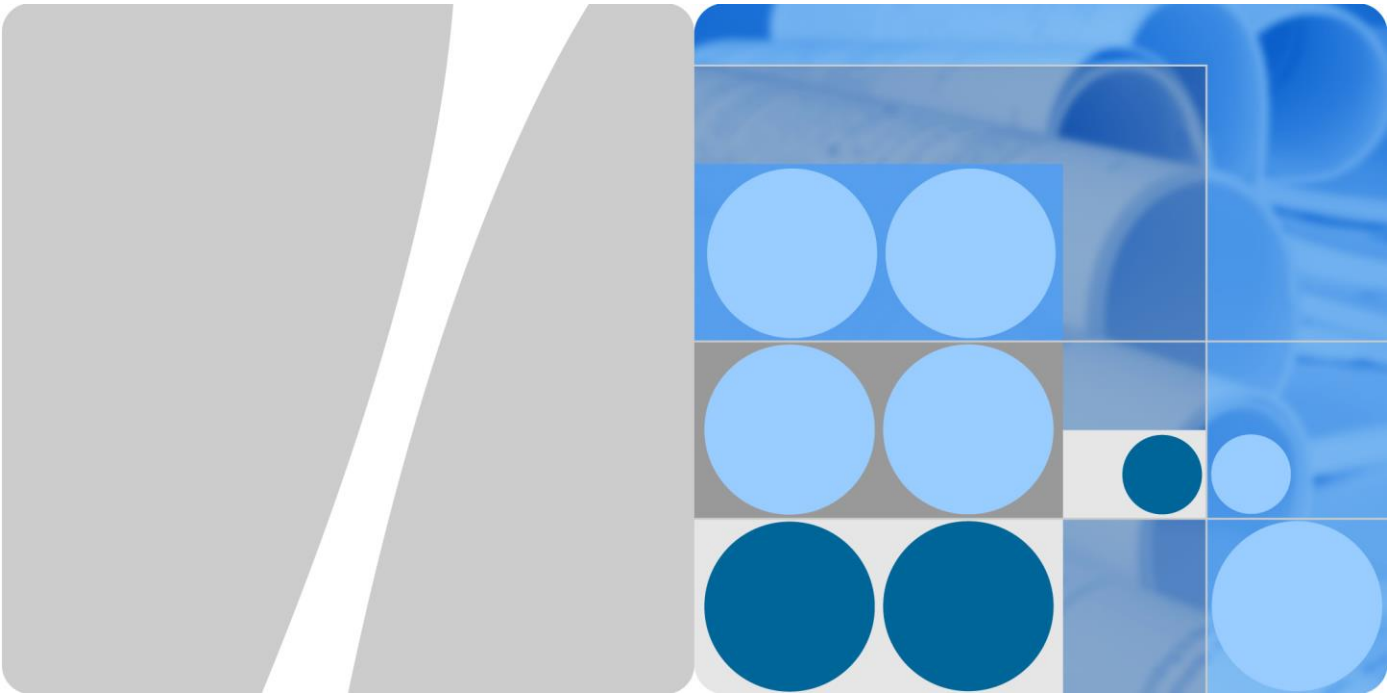


云堡垒机(CBH)
3.3.54.0
用户指南

发布日期 2024-05-20

目 录

1 产品介绍

1.1 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 功能特性

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。
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。 – 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

功能特性	功能说明
	– 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

功能特性	功能说明
	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以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。
资源运	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

功能特性	功能详情
维审计	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、剪切板拷贝等。 – 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	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。

功能特性	功能说明
运维	• 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。

1.3 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。

1.4 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涨。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。

1.5 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，标准版版本配备 10、20、50、100、200、500、1000、5000、10000 资产规格，专业版配备 10、20、50、100、200、500、1000、5000、10000 资产规格。

规格差异

云堡垒机支持 10、20、50、100、200、500、1000、5000、10000 资产规格配置，不同规格云堡垒机配置差异，请参见表 1-5。

表1-5 不同规格配置说明

资产数	最大并发数	CPU	内存	系统盘	数据盘
10	10	4 核	8GB	100GB	200GB
20	20	4 核	8GB	100GB	200GB
50	50	4 核	8GB	100GB	500GB
100	100	4 核	8GB	100GB	1000GB
200	200	4 核	8GB	100GB	1000GB
500	500	8 核	16GB	100GB	2000GB
1000	1000	8 核	16GB	100GB	2000GB
5000	2000	16 核	32GB	100GB	3000GB
10000	2000	16 核	32GB	100GB	4000GB

须知

表 1-5 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）的并发数只有该值的 1/3。

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 1-6。

表1-6 不同版本功能说明

功能项	功能说明	标准版	专业版
身份认证	用户账号双因子认证 支持手机令牌、手机短信、USBKey、动态令牌等多因子认证形式。	√	√
	用户账号远程认证 支持 AD 域、RADIUS、LDAP、Azure AD、SAML 远程认证。	√	√
权限控制	系统访问权限 通过划分组织部分结构、分配用户角色、设置用户登录限制，控制用户登录和访问系统权限。	√	√
	资源访问权限 按照用户、用户组、资源账户、账户组，建立用户对资源的访问控制授权，通过配置访问控制策略、双人授权、命令控制策略，实现对资源不同维度的控制。	√	√
	双人授权 通过配置“双人授权”实现双人或多人权限审核，保障核心资源安全。	√	√
	字符命令拦截 通过配置命令控制策略，对字符协议资源关键操作，进行动态授权。	√	√
	数据库命令拦截 通过配置数据库控制策略，对数据库资源敏感、危险等操作，进行精确限制、二次复核。 **说明** **数据库命令拦截功能不区分云数据库还是自建的数据库。**	×	√
账户管理	用户账号全生命周期管理 • 用户账号单个创建、批量导入、批量管理，以及划分用户组管理。	√	√
	资源账户全生命周期管理 • 资源和资源账户的单个添加、批量导入、批量管理，以及资源账户的划分账户组管理。	√	√

功能项	功能说明	标准版	专业版
	纳管主机资源 • 支持纳管 SSH、RDP、VNC、TELNET、FTP、SFTP、DB2、MySQL、SQL Server、Oracle、SCP、Rlogin 协议类型的 Linux 和 Windows 资源。	√	√
	纳管应用资源 • “服务器类型”选择“Windows”时： 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 • “服务器类型”选择“Linux”时： 支持类型：DM Tool、KingbaseES Tool、Firefox-Linux、GBaseDataStudio for GBase8a。	√	√
	纳管数据库资源 • 支持纳管 DB2、MySQL、SQL Server 和 Oracle 引擎类型数据库。	×	√
	资源账户自动改密 • 通过配置改密策略，定期修改资源账户密码，管控资源账户及登录密码。	√	√
	资源账户自动同步 • 通过配置账户同步策略，及时发现僵尸账户或未被管控账户。	×	√
操作审计	系统登录和操作全程记录 • 支持导出系统日志、生成系统报表，以及配置告警通知。	√	√
	资源运维操作全程审计 • 支持多种审计技术和审计形式，会话实时监控，历史会话可生成视频、导出文本报表的双重审计，并支持日志远程备份。	√	√
	数据库行为审计 • 基于操作命令审计数据库运维全程。	×	√
高效运维	Web 浏览器一站式运维 • 远程登录资源，无需安装客户端，一键登录运维资源，并集成批量登录、协同会话、文件传输、命令群发等功能。	√	√

功能项	功能说明	标准版	专业版
	第三方客户端运维 • 一键接入多种运维工具，支持多种运维形式，包括 SSH 客户端运维、FTP/SFTP 客户端运维等。	√	√
	数据库运维 • 通过 SSO 单点登录工具调用客户端，一键登录目标数据库。	×	√
	自动化运维 • 在线管理脚本，以及定时执行预置运维任务。	×	√
工单申请	访问授权工单、命令授权工单申请 • 系统用户为获取资源控制权限，通过手动或自动方式触发系统工单，提交工单给系统管理人员审批，获取权限的全程。	√	√
	数据库授权工单申请 • 系统用户可触发数据库敏感操作，自动生成授权工单，系统用户需提交工单申请，由管理人员审批通过才能获取继续操作权限。	×	√

1.6 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。

1.7 使用限制

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 22333 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。

  具体端口限制详见表 1-7。
- 只允许通过 IP 地址和端口访问 CBH 系统。

表1-7 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 浏览器登录云堡垒机（HTTP、HTTPS）	入方向	TCP	22333
通过 MSTSC 客户端登录云堡垒机	入方向	TCP	53389
通过 SSH 客户端登录云堡垒机	入方向	TCP	2222
通过 FTP 客户端登录云堡垒机	入方向	TCP	20~21
通过云堡垒机的 SSH 协议远程访问 Linux	出方向	TCP	22

场景描述	方向	协议/应用	端口
云服务器			
通过云堡垒机的 RDP 协议远程访问 Windows 云服务器	出方向	TCP	3389
通过云堡垒机访问 Oracle 数据库	入方向	TCP	1521
通过云堡垒机访问 Oracle 数据库	出方向	TCP	1521
通过云堡垒机访问 MySQL 数据库	入方向	TCP	33306
通过云堡垒机访问 MySQL 数据库	出方向	TCP	3306
通过云堡垒机访问 SQL Server 数据库	入方向	TCP	1433
通过云堡垒机访问 SQL Server 数据库	出方向	TCP	1433
通过云堡垒机访问 DB 数据库	入方向	TCP	50000
通过云堡垒机访问 DB 数据库	出方向	TCP	50000
通过云堡垒机访问 GaussDB 数据库	入方向	TCP	18000
通过云堡垒机访问 GaussDB 数据库	出方向	TCP	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 客户端登录云堡垒机	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
通过云堡垒机访问 PGSQL 数据库	入方向	TCP	15432
通过云堡垒机访问 PGSQL 数据库	出方向	TCP	5432

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1-8 支持的数据库引擎及版本

数据库引擎	引擎版本
MySQL	5.5，5.6，5.7，8.0
Microsoft SQL Server	2014、2016、2017、2019、2022
Oracle	10g、11g、12c、19c、21c
DB2	DB2 Express-C
PostgreSQL	11、12、13、14、15
GaussDB	2、3

- **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 1-9。

表1-9 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1-10 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

登录方式	支持使用的客户端	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1-11 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）	MySQL	Navicat 11、12、15、16 MySQL Administrator 1.2.17 MySQL CMD DBeaver22、23
	SQL Server	Navicat 11、12、15、16 SSMS 17
	Oracle	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
	DB2	DB2 CMD 命令行 11.1.0
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

运维方式	资源协议类型/应用类型	支持调用的客户端
	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。

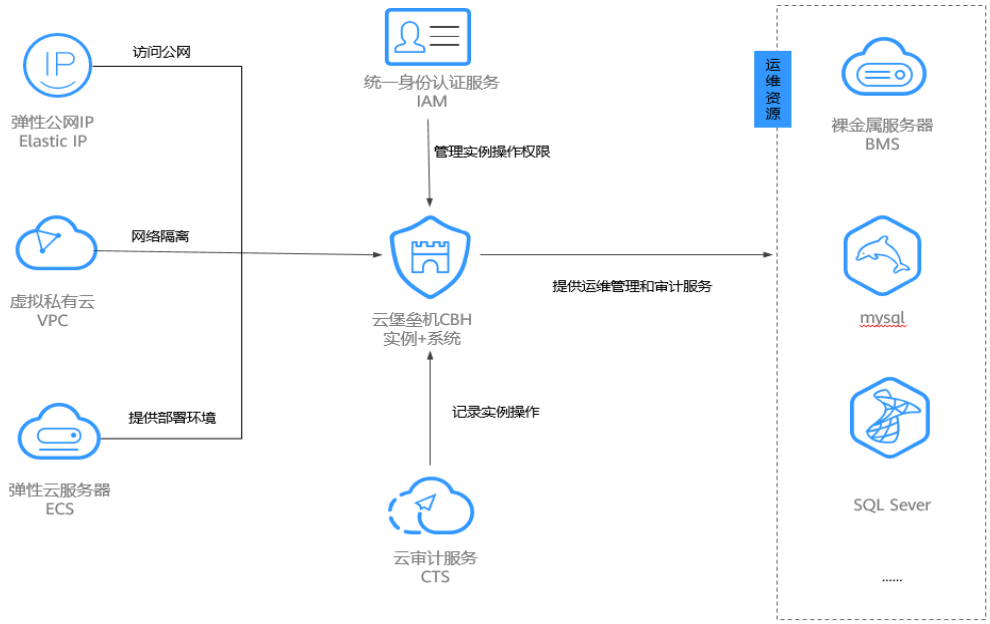
并发数是云堡垒机同一时刻连接运维协议的连接数。

详细说明请参见 1.6 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 EulerOS 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 IP 的关系

弹性 IP（Elastic IP，EIP）为 CBH 提供独立的 IP 资源，包括 IP 地址与出口带宽服务。一个弹性 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。

2 实例

2.1 购买云堡垒机

背景信息

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。用户需首先购买云堡垒机实例，创建一个云堡垒机账户，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。

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。
- 已购买至少一个弹性公网 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。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在页面左上角单击  ，选择区域，选择“安全 > 云堡垒机”，进入云堡垒机实例管理页面。

步骤 3 单击“购买云堡垒机”，进入云堡垒机的购买页面。

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 购买云堡垒机实例参数说明

参数	说明

参数	说明
计费模式	选择实例计费模式，仅支持“包年/包月”模式。 包年/包月是预付费模式，按订单的购买周期计费，适用于可预估资源使用周期的场景。
当前区域 当前项目 实例类型 可用分区	选择实例应用区域、企业项目、实例类型和可用区，即提供云堡垒机服务的区域和可用分区。 实例类型根据您的自身业务的需求选择单击实例或者主备实例。 说明 • 实例类型选择主备的时候需要选择主机和备机的可用区。 • 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。 建议根据待管理 ECS、RDS 等服务器上资源的区域和可用区选择，可以降低网络时延、提高访问速度。
实例名称	自定义实例名称。
性能规格	选择实例版本规格。 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 等打通两个 VPC 间的网络；不建议跨区域管理 ECS 等资源。
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“管理安全组”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 2.9 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。 • 堡垒机时创建时会自动开放 80、8080、443、2222 共四个端口，创建完成后若

参数	说明
	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。
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。
弹性 IP	选择当前区域下 EIP。 若当前区域无可选 EIP，可单击“购买弹性 IP”创建弹性 IP。 说明 • 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 2.10 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	选择此次购买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。 • 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

参数	说明
	置手机号码，否则无法进入云堡垒机系统。 • 完成实例购买后，若忘记 **admin** 用户密码，可重置密码。
购买时长	选择实例使用时长。 可按月或按年购买云堡垒机。
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，查看“当前配置”确认信息，单击“立即购买”。

说明

当收到网络限制提示时，请先“一键放通”网络限制，确保购买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 进入“订单详情”页面，确认订单无误并阅读《隐私政策声明》后，勾选“我已阅读并同意《隐私政策声明》”，单击“提交订单”。

步骤 7 在支付页面完成付款，返回云堡垒机控制台页面，在“云堡垒机实例”列表下查看新购买的实例。

购买实例成功后，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

2.2 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 在页面左上角单击  ，选择区域，选择“安全 > 云堡垒机”，进入云堡垒机实例管理页面。

步骤 3 单击实例名称，查看实例详情信息。

表2-2 实例的信息参数说明

参数	说明
实例名称	您自定义实例的名称，创建后不可编辑修改。
计费模式	当前实例的计费模式。
虚拟私有云	用户选择的实例 VPC 网络环境。
服务器 ID	当前实例的服务器 ID，包含备机的 ID。
安全组	用户配置的虚拟网络环境安全规则。
实例类型	您选择的实例类型。
子网	用户配置的 VPC 网络环境的子网。
备机状态	备机的运行状态。
Vip	当前实例的浮动 IP.
实例规格	用户选择的实例使用资产规格。
到期处理策略	到期后进入宽限期，可查看宽限规则。
私有 IP	实例的私有 IP 地址，包括备机的 IP 地址。
实例版本	当前实例的版本。
企业项目	实例所属的企业项目。

----结束

2.3 变更版本规格

当云堡垒机的规格不能满足需求时，可对云堡垒机实例进行规格升级，购买更高规格的**标准版**或**专业版**，扩大系统数据盘容量、最大并发数、最大资产数、CPU、内存等配置。云堡垒机系统盘默认为 100G，变更规格不影响系统盘规格和系统软件版本。

变更规格前后注意事项：

- 变更规格前

  用户必须在变更规格前备份数据，因变更规格有失败风险，以防因变更规格失败而影响使用。
- 变更规格中

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

- 变更规格后

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

约束限制

- 云堡垒机提供**标准版**和**专业版**两个功能版本，每个版本配备 **10 种**资产规格。
- 当前仅支持版本规格变更规格，不支持版本规格缩容。

前提条件

- 已备份系统数据。

  变更规格有失败的风险，因此在变更规格前必须备份数据，以防因变更规格失败而影响数据的使用。

- 已升级当前版本。

  变更规格到**专业版**，需确保云堡垒机软件版本在 3.2.16.0 及以上。

- 已绑定 EIP，且 EIP 可用。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在页面左上角单击  ，选择区域，选择“安全 > 云堡垒机”，进入云堡垒机实例管理页面。

步骤 3 单击左上角的  ，选择区域或项目。

步骤 4 在左侧导航树中，单击  ，选择“安全与合规 > 云堡垒机”，进入云堡垒机实例界面。

步骤 5 选择需变更规格的实例，单击所在行“操作”列中“更多 > 扩容 > 变更规格”，跳转到“变更规格”页面。

步骤 6 选择需变更的“性能规格”，单击“立即购买”。

步骤 7 进入“订单详情”页面，确认订单无误后，单击“提交订单”。

说明

当收到网络限制提示时，请先“一键放通”网络限制，确保变更规格激活成功。

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 8 在支付页面完成付款。

步骤 9 后台自动进行变更规格操作，整个变更规格过程需 30min 左右，且实例的运行状态将会由“变更中”到“正在重启”。

步骤 10 实例运行状态变为“运行”，即可正常使用云堡垒机。

----结束

2.4 升级版本

新版本的云堡垒机对系统进行了功能优化或添加了新功能，请及时升级版本。

升级前后注意事项：

- 升级前
  - 为防止因升级失败而影响使用，建议升级前备份数据。
- 升级中

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

  版本升级完成后会自动“重启”云堡垒机，重启完成后，即可使用云堡垒机。

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

  版本升级完成或者跨版本升级过程中，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”。

  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。

前提条件

- 已绑定 EIP，且 EIP 可用。
- 已备份系统数据。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在页面左上角单击，选择区域，选择“安全 > 云堡垒机”，进入云堡垒机实例管理页面。

步骤 3 单击左上角的，选择区域或项目。

步骤 4 在左侧导航树中，单击，选择“安全与合规 > 云堡垒机”，进入云堡垒机实例界面。

步骤 5 在需要升级服务版本的实例所在行，单击“操作”列中的“更多 > 升级 > 版本升级”。

步骤 6 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“UPGRADE”。若您已经预约过该堡垒机的升级时间，可以修改预约升级时间或者在对话框中输入“CANCEL”取消此次升级任务。

说明

升级类型说明：

- 小版本升级，升级过程中当前堡垒机业务将会中断，中断时长约为 15min~30min。
- 跨版本升级，升级过程中将会创建一台新的堡垒机实例，数据备份过程中当前云堡垒机业务将会中断，中断时长约为 30min~2h。(跨版本的升级状态为：“升级中” -> “数据迁移中” -> “配置 HA” -> “运行”)。

步骤 7 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 8 实例状态变为“运行”，即可正常使用云堡垒机。

说明

升级完成后请单击“实例名称”查看堡垒机版本号，若实例版本号未变动则表示升级失败，请联系技术支持人员。

----结束

2.5 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 在页面左上角单击，选择区域，选择“安全 > 云堡垒机”，进入云堡垒机实例管理页面。

步骤 3 单击左上角的，选择区域或项目。

步骤 4 在左侧导航树中，单击，选择“安全与合规 > 云堡垒机”，进入云堡垒机实例界面。

步骤 5 在需要启动的实例所在行，单击“操作”列中的“启动”。

步骤 6 在弹出的开启实例对话框中，单击“确定”。

实例启动成功后，实例的“运行状态”变为“运行”。

----结束

2.6 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。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在页面左上角单击，选择区域，选择“安全 > 云堡垒机”，进入云堡垒机实例管理页面。

步骤 3 单击左上角的，选择区域或项目。

步骤 4 在左侧导航树中，单击，选择“安全与合规 > 云堡垒机”，进入云堡垒机实例界面。

步骤 5 在需要关闭的实例所在行，单击“操作”列中的“更多 > 关闭”。

步骤 6 在弹出的关闭实例对话框中，单击“确定”。实例成功关闭后，实例的“运行状态”变为“关闭”。

说明

在关闭实例对话框，可选择“强制关机”，强制关闭实例可能会造成数据丢失，请确保数据文件已全部保存。

----结束

2.7 重启实例

出于维护目的，当 CBH 系统的运行异常，用户可以尝试重启实例，使其恢复到可用状态。

- 当 CBH 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”；
- 重启过程中，CBH 系统将不可用。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在页面左上角单击，选择区域，选择“安全 > 云堡垒机”，进入云堡垒机实例管理页面。

步骤 3 单击左上角的，选择区域或项目。

步骤 4 在左侧导航树中，单击，选择“安全与合规 > 云堡垒机”，进入云堡垒机实例界面。

步骤 5 在需要重启的实例所在行，单击“操作”列中的“更多 > 重启”。

步骤 6 在弹出的重启实例对话框中，单击“确定”。

步骤 7 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 8 实例状态变为“运行”，即可正常使用云堡垒机。

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。

----结束

2.8 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“运行中”的实例才可以更改 VPC。

- 在切换 VPC 前要确保待切换的 VPC 子网下的 IP 数≥3。
- 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 单击左上角的，选择区域或项目。

步骤 3 在左侧导航树中，单击，选择“安全与合规 > 云堡垒机”，进入云堡垒机实例界面。

步骤 4 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 5 在弹出的对话框中勾选需要切换的“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。

----结束

2.9 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。但是若您在购买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“运行中”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 单击左上角的，选择区域或项目。

步骤 3 在左侧导航树中，单击，选择“安全与合规 > 云堡垒机”，进入云堡垒机实例界面。

步骤 4 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 5 在弹出的对话框中勾选需要绑定的安全组。

步骤 6 单击“确定”，完成安全组的修改

----结束

2.10 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 CBH 使用需求，建议配置 EIP 带宽为 5M 以上。

- 使用 Web 浏览器登录云堡垒机系统。登录地址：https://*云堡垒机实例 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。
- V3.3.2.0 及以下版本，如果云堡垒机实例未绑定弹性公网 IP 的话，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

- 已购买至少一个弹性公网 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购买的。**

操作步骤

步骤 1 登录管理控制台。

步骤 2 在页面左上角单击  ，选择区域，选择“安全 > 云堡垒机”，进入云堡垒机实例管理页面。

步骤 3 单击左上角的  ，选择区域或项目。

步骤 4 在左侧导航树中，单击 ，选择“安全与合规 > 云堡垒机”，进入云堡垒机实例界面。

步骤 5 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 6 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，“登录”按钮变为可操作，且可在“弹性 IP”列查看已绑定弹性 IP。

----结束

2.11 解绑弹性公网 IP

当 CBH 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 在页面左上角单击 ，选择区域，选择“安全 > 云堡垒机”，进入云堡垒机实例管理页面。

步骤 3 单击左上角的 ，选择区域或项目。

步骤 4 在左侧导航树中，单击 ，选择“安全与合规 > 云堡垒机”，进入云堡垒机实例界面。

步骤 5 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”，弹出的解绑弹性 IP 对话框。

步骤 6 在弹出的解绑弹性 IP 对话框中，单击“确定”。

解绑成功后，“弹性 IP”列无 IP 信息，且“登录”按钮变为不可操作。

----结束

2.12 续费

为保证用户正常使用云堡垒机服务，在云堡垒机许可证到期前或使用许可到期后，用户可通过“续费”操作增加授权使用期限。

- 在云堡垒机到期前，可以通过“续费”操作延长到期时间。
- 在云堡垒机到期后，可以通过“续费”操作继续使用云堡垒机。若未及时续费，则进入“保留期”，将冻结云堡垒机，不能登录云堡垒机系统。“保留期”到期仍未续订或充值，存储在云堡垒机中的数据将被删除、资源将被释放。
- 可根据需求选择一次性续费和自动续费。

前提条件

已“一键放通”云堡垒机网络限制。

说明

当收到网络限制提示时，请先“一键放通”网络限制，确保续费更新授权成功。

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。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在页面左上角单击  ，选择区域，选择“安全 > 云堡垒机”，进入云堡垒机实例管理页面。

步骤 3 单击左上角的  ，选择区域或项目。

步骤 4 在左侧导航树中，单击  ，选择“安全与合规 > 云堡垒机”，进入云堡垒机实例界面。

步骤 5 单击待续费的实例，选择“操作”列的“更多”，根据需求选择目标续费模式，进入“续费”页面。

- 一次续费：选择一个固定周期进行续费，同时可设置固定的到期日期，确认无误后单击“去支付”，在支付页面完成付款。
- 开通自动续费：选择续费时长，可勾选“自动续费次数”选项，对续费的次数进行自定义设置，到期后自动结束自动续费，确认无误后单击“开通”，完成设置。

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

说明

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

----结束

2.13 退订

若用户不再有使用云堡垒机实例需求，可执行退订操作。

前提条件

- 已使用的云堡垒机，需停止系统所有操作，解绑 EIP。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在页面左上角单击  ，选择区域，选择“安全 > 云堡垒机”，进入云堡垒机实例管理页面。

步骤 3 单击左上角的  ，选择区域或项目。

步骤 4 在左侧导航树中，单击  ，选择“安全与合规 > 云堡垒机”，进入云堡垒机实例界面。

步骤 5 选择待退订的实例，单击所在行“操作”列的“更多 > 退订”，弹出的退订实例对话框。

步骤 6 确认实例信息无误后，单击“确定”。

步骤 7 在退订资源页面完成退订。

----结束

3 系统登录

3.1 登录系统概述

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 配置是否允许访问云堡垒机，并参考表 3-1 配置实例安全组。

表3-1 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 浏览器登录云堡垒机（HTTP、HTTPS）	入方向	TCP	22333
通过 MSTSC 客户端登录云堡垒机	入方向	TCP	53389
通过 SSH 客户端登录云堡垒机	入方向	TCP	2222
通过 FTP 客户端登录云堡垒机	入方向	TCP	20~21
通过云堡垒机的 SSH 协议远程访问 Linux 云服务器	出方向	TCP	22
通过云堡垒机的 RDP 协议远程访问 Windows 云服务器	出方向	TCP	3389
通过云堡垒机访问 Oracle 数据库	入方向	TCP	1521
通过云堡垒机访问 Oracle 数据库	出方向	TCP	1521
通过云堡垒机访问 MySQL 数据库	入方向	TCP	33306
通过云堡垒机访问 MySQL 数据库	出方向	TCP	3306
通过云堡垒机访问 SQL Server 数据库	入方向	TCP	1433
通过云堡垒机访问 SQL Server 数据库	出方向	TCP	1433
通过云堡垒机访问 DB 数据库	入方向	TCP	50000

场景描述	方向	协议/应用	端口
通过云堡垒机访问 DB 数据库	出方向	TCP	50000
通过云堡垒机访问 GaussDB 数据库	入方向	TCP	18000
通过云堡垒机访问 GaussDB 数据库	出方向	TCP	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 客户端登录云堡垒机	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
通过云堡垒机访问 PGSQL 数据库	入方向	TCP	15432
通过云堡垒机访问 PGSQL 数据库	出方向	TCP	5432

认证类型

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

表3-2 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。

认证类型	认证说明
	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。

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3-3 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）。
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）

3.2 使用 Web 浏览器登录云堡垒机

云堡垒机基于 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。

支持的登录方式包括静态密码、手机短信、手机令牌、USBKey、动态令牌等。

说明

- 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。

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://*云堡垒机实例 EIP*。例如，https://10.10.10.10。

说明

步骤 2 选择登录方式。

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。

详情请分别参见如下说明。

----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。

----结束

图3-1 静态密码登录

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。

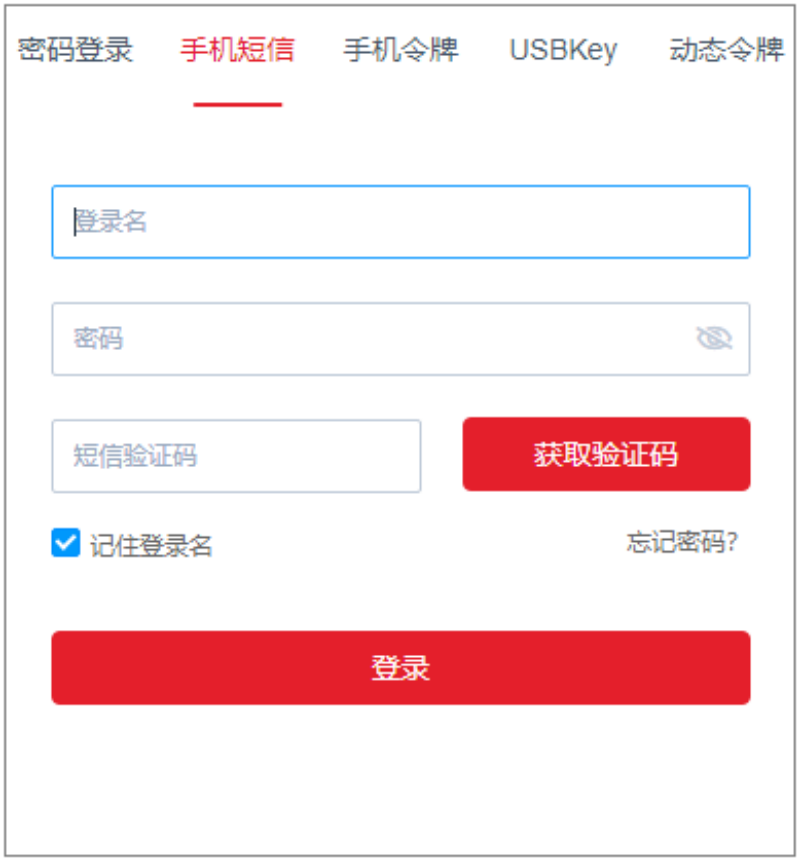
步骤 2 依次输入用户登录名、账户登录密码。

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。

----结束

图3-2 手机短信登录



使用手机令牌登录

手机时间必须与云堡垒机系统时间一致，精确到秒。

须知

云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，万一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。

----结束

图3-3 手机令牌登录

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。

----结束

图3-4 USBKey 登录

使用动态令牌登录

步骤 1 选择“动态令牌”方式。

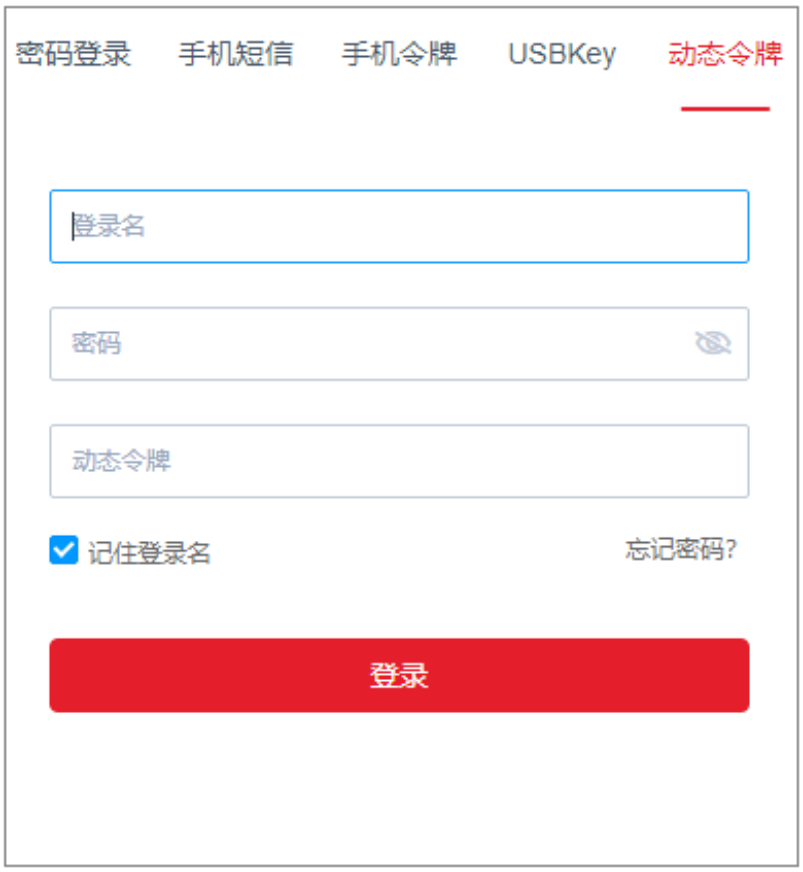
步骤 2 依次输入用户登录名、账户登录密码。

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。

----结束

图3-5 动态令牌登录



3.3 使用客户端登录云堡垒机

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 客户端登录云堡垒机

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。

- 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 -p 端口***，例如执行 ssh admin@10.10.10.10 -p 2222。

说明

系统登录 IP 地址指云堡垒机的 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。

表3-4 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	输入云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。
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，并在云堡垒机系统内的“个人中心”处将 SSH 公钥添加到云堡垒机系统中。
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	“密码登录”或“公钥登录”验证成功后，选择“手机令牌 OTP”方	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

登录方式	登录说明	登录方式配置说明
令牌	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。	登录系统。
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。

步骤 4 登录到云堡垒机系统，可查看系统简要信息，并运维已授权的资源。

说明

除了使用云堡垒机用户密码直接登录外，还支持使用 API 方式登录云堡垒机指定的资源账户。

在登录的用户窗口， 输入**用户登录名@资源账户名@主机 IP 地址:主机端口**，例如 admin@root@192.0.0.0:22。

----结束

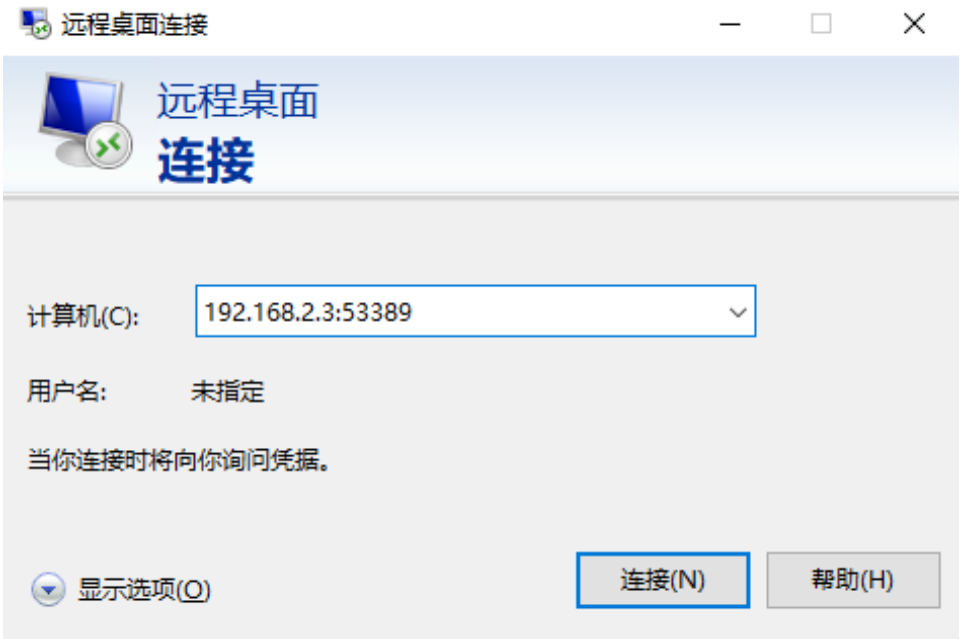
通过 MSTSC 客户端登录云堡垒机

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3-6 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。

- password：输入当前堡垒机的用户密码。

----结束

3.4 配置多因子认证

3.4.1 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，云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 。

约束限制

- 一个登录账号仅能绑定一个可用手机号码。
- 云堡垒机实例安全组必须已放开短信网关 IP 和 10743、22333 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云堡垒机系统。

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。

图3-7 绑定个人手机号码

步骤 4 在“手机”列框，输入有效手机号码。

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 管理员登录云堡垒机系统。

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

3.4.2 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，云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。

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。

目前云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：微信小程序手机令牌。
- RADIUS 手机令牌：APP 版手机令牌 Microsoft Authenticator、Google Authenticator 和 FreeOTP。

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：用户绑定手机令牌

步骤 1 用户通过静态密码方式登录云堡垒机系统。

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3-8 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

步骤二：管理员配置手机令牌认证

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”，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

3.4.3 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。

约束限制

- 目前平台堡垒机可识别飞天诚信的 USBKey，不同的厂商 USBKey 不能相互识别登录认证。需根据申购的 USBKey3.5.6 配置 USB Key 厂商厂商。
- 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 管理员登录云堡垒机系统。

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 管理员登录云堡垒机系统。

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3-5 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。

关联用户登录云堡垒机系统时，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

3.4.4 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。

约束限制

- 目前云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

已申购硬件令牌。

步骤一：配置动态令牌认证

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”，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 管理员登录云堡垒机系统。

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3-6 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。

关联用户登录云堡垒机系统时，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

3.5 登录安全管理

3.5.1 配置用户登录安全锁

为保障云堡垒机系统用户登录安全，在用户登录云堡垒机时，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”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“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。

表3-7 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，可选择“用户”或“来源 IP”。 • 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。
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。
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。

图3-9 系统用户安全锁

----结束

3.5.2 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“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3-8 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。
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。

图3-10 系统用户密码策略

----结束

3.5.3 配置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 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3-9 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 1～43200，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 15～3600，单位为秒。 • 若设置为 0，表示短信验证不过期。
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。

参数	说明
	• 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。

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。

图3-11 系统 Web 登录配置

----结束

客户端登录配置

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“客户端登录配置”区域，单击“编辑”，弹出客户端登录配置窗口。

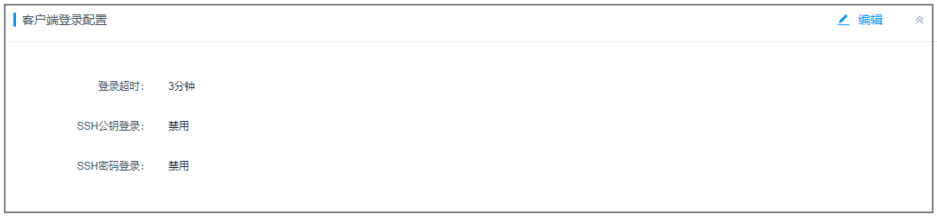
根据界面提示配置系统客户端登录参数。

表3-10 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。

图3-12 系统客户端登录配置



----结束

3.5.4 更新系统 Web 证书

云堡垒机 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。

云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云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

- 目前云堡垒机系统只适配 Tomcat 的 Java Keystore 格式证书文件，即后缀为 jks 的证书文件。
- 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 证书信息更新后，为了使证书生效，需要重启堡垒机系统。

重启堡垒机系统的有以下两种方式，您可以根据具体情况进行选择：

- 控制台重启实例，具体操作请参见 2.7 重启实例。
- 堡垒机系统工具重启系统，具体操作请参见管理系统工具。

图3-13 系统 Web 证书信息

----结束

3.5.5 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。云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，才能登录云堡垒机系统。

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：微信小程序手机令牌。
  - RADIUS 手机令牌：APP 版手机令牌，包括 Google Authenticator 和 FreeOTP。
- 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“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。

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。

图3-14 查看系统手机令牌类型

----结束

3.5.6 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

- 目前仅支持龙脉科技厂商的 USB Key。
- 更改 USBKey 厂商配置后，已签发的其他厂商 USB Key 将不能被识别。

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 > 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。

图3-15 查看系统 USB Key 厂商

----结束

3.5.7 配置僵尸用户禁用策略（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，至到管理员解除禁用。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“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 6.2.2 启停用户章节。

步骤 4 单击“确定”。

----结束

3.5.8 配置 RDP 资源客户端代理（3.3.26.0 及以上版本）

本小节主要介绍如何配置 RDP 资源客户端代理。

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 > 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

3.5.9 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 调用方式使用云堡垒机。

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“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”，使配置生效。

----结束

3.5.10 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“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”。

----结束

3.5.11 资源账户配置

开启资源账户可自动添加 Empty 的账户。

操作步骤

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”，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

3.5.12 客户端登录配置

可通过客户端登录配置登录后无操作的时间范围，超时后自动退出。

操作步骤

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”，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 填写登录后长久不操作空闲的超时时间，及选择 SSH 登录方式，如表 3-11 所示。

表3-11 客户端登录配置

参数名称	参数说明	取值样例
登录超时	设置登录成功后无操作的时间。 有效值区间为 1-43200。当超过设定时长无操作时，再次操作需要重新登录，默认值为 30。	30
SSH 公钥登录	超时后是否使用 SSH 公钥登录，默认开启。	
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

3.5.13 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“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状态  。

步骤 5 单击“确定”，完成配置。

----结束

3.5.14 会话限制配置

配置会话在开启后，当 CPU 和内存使用率超过服务器配置时，将自动禁止新增会话。

操作步骤

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”，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，当达到设置的使用率，将停止新增会话。

步骤 5 单击“确定”，完成配置。

----结束

4 系统桌面

4.1 桌面看板

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，呈现云堡垒机系统状态、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 登录云堡垒机系统。

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。

图4-1 活动用户

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。

图4-2 待审批工单

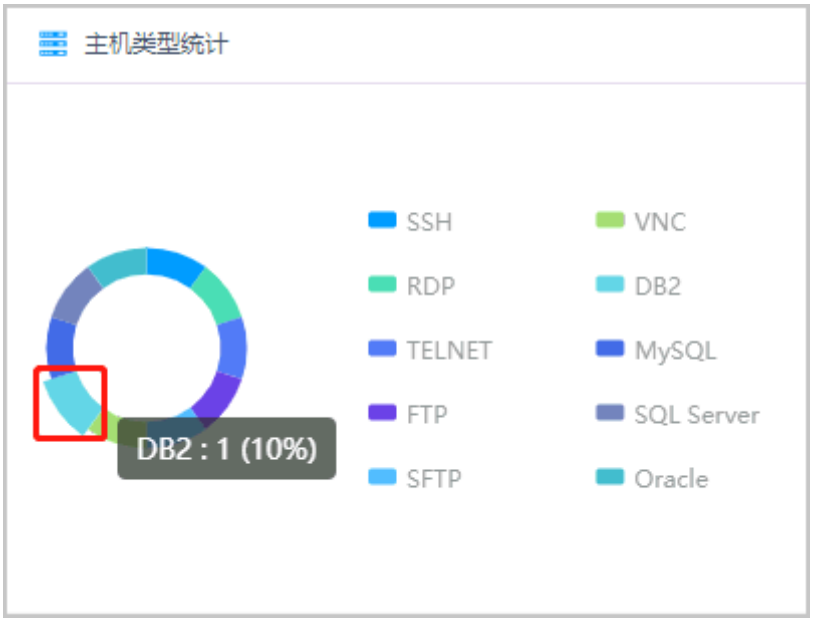
主机类型统计

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。

图4-3 主机类型统计



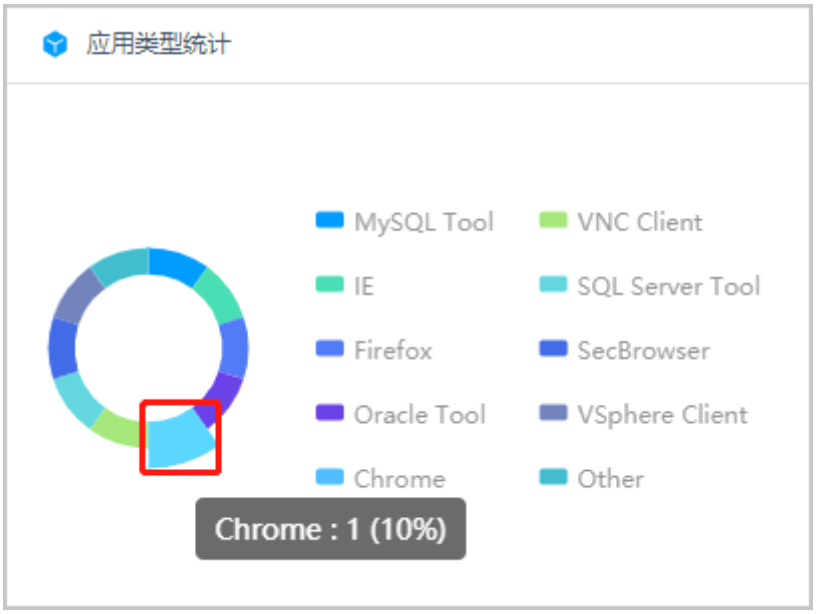
应用类型统计

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。

图4-4 应用类型统计



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。

图4-5 当前活动会话

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。

图4-6 今日新增会话

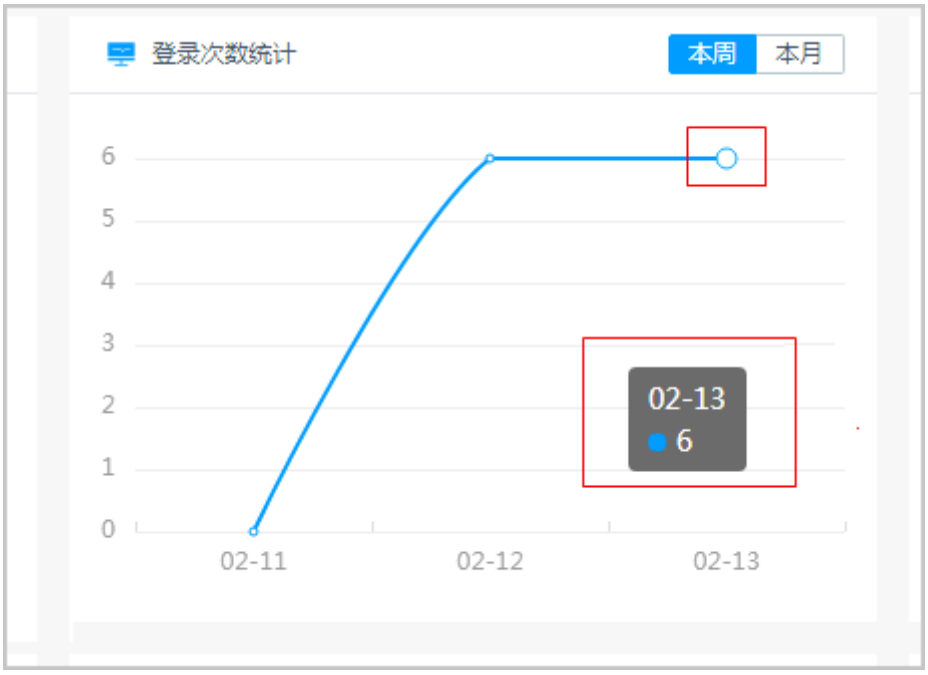
登录次数统计

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。

图4-7 用户登录系统次数统计



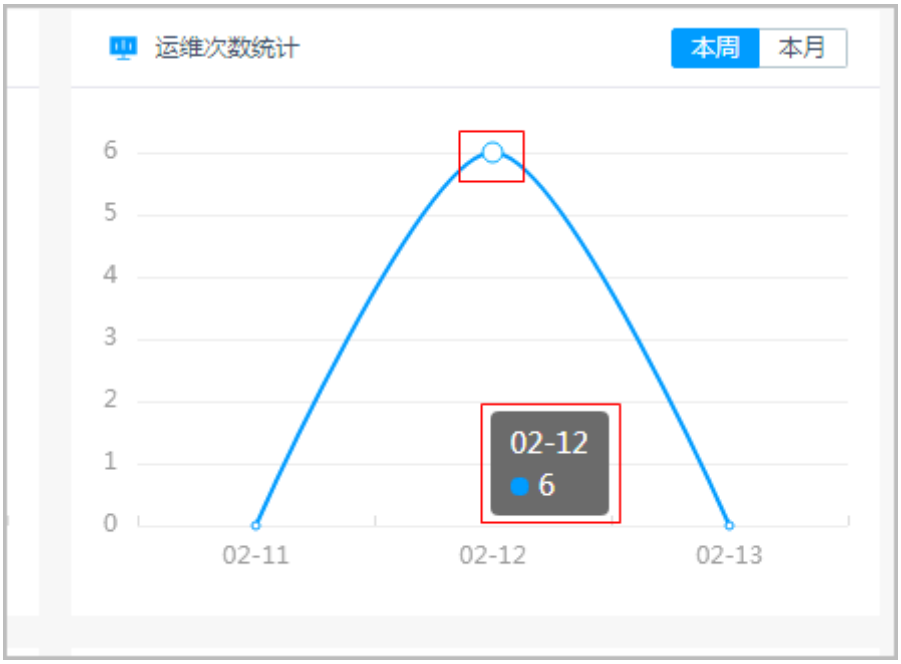
运维次数统计

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。

图4-8 运维次数统计



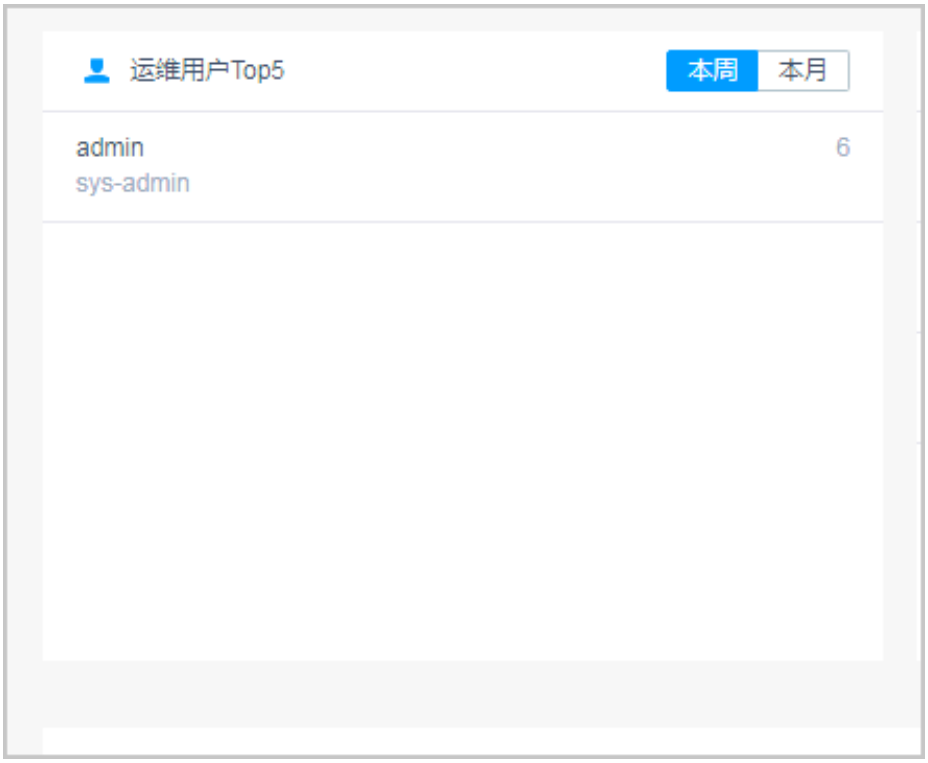
运维用户 Top5

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。

图4-9 运维用户 Top5



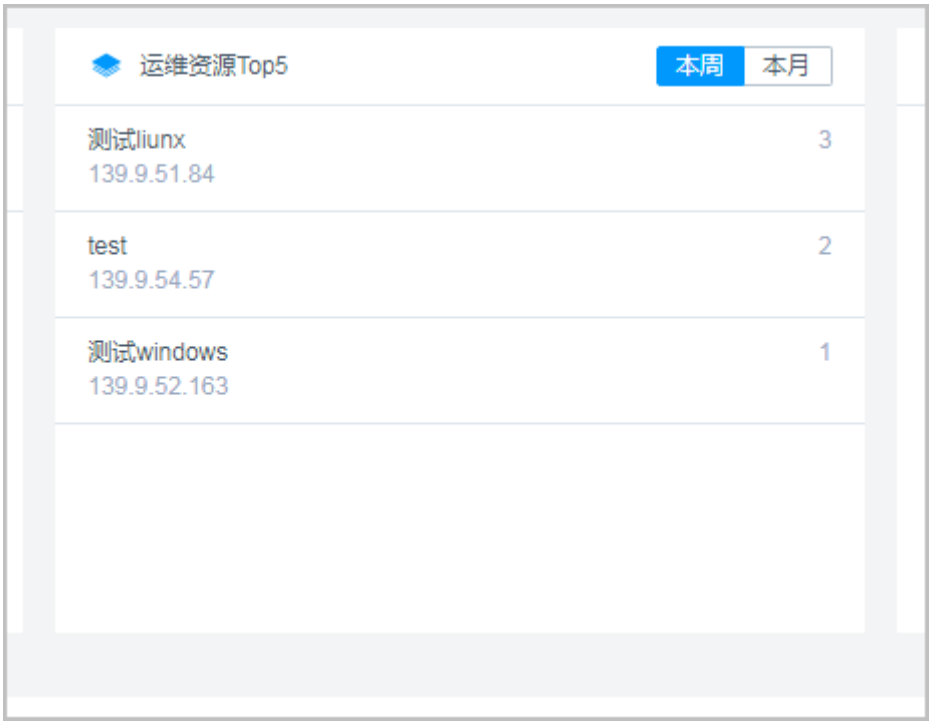
运维资源 Top5

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。

图4-10 运维资源 Top5



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。

图4-11 系统状态

系统信息

呈现当前系统的基本信息，以及授权系统版本规格。

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。

图4-12 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。

图4-13 最近登录主机

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。

图4-14 最近登录应用

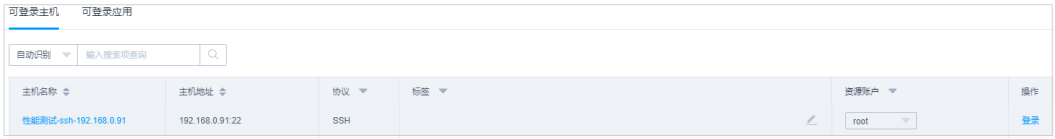
可登录主机

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。

图4-15 可登录主机



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。

图4-16 可登录应用

4.2 个人中心

4.2.1 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。

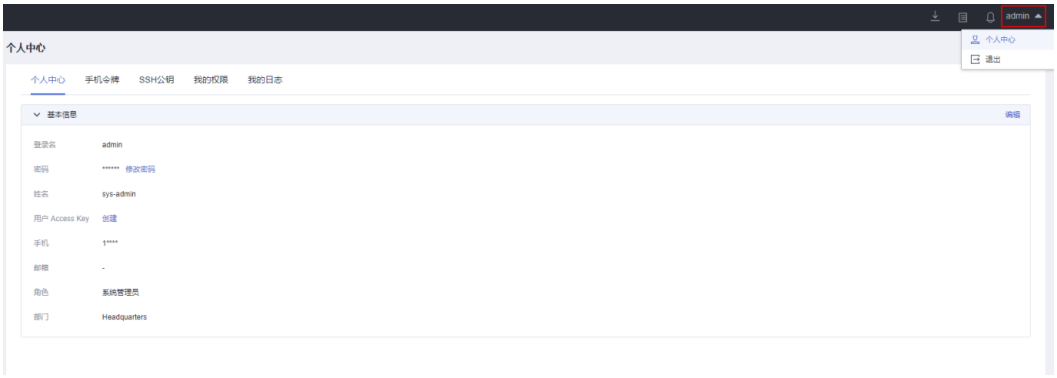
本小节主要介绍如何查看个人信息。

操作步骤

步骤 1 登录云堡垒机系统。

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4-17 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，请参见如下描述。

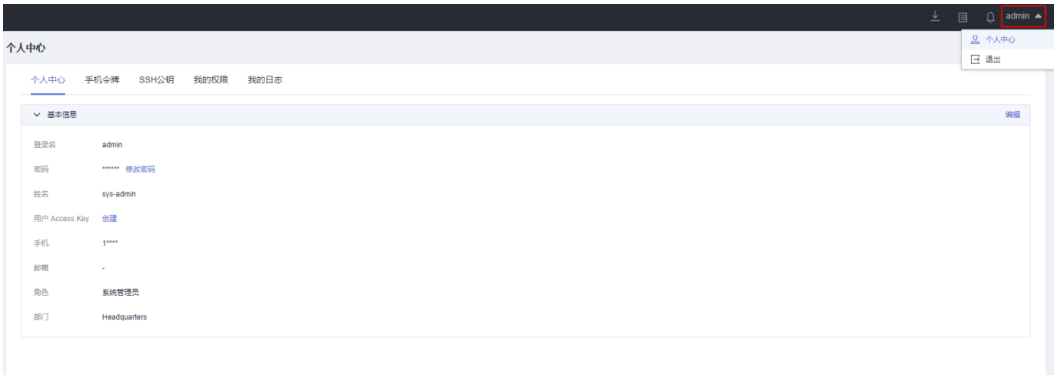
----结束

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。

更多修改手机号码、修改邮箱地址、修改密码等说明，请参见 4.2.2 修改个人基本信息。

图4-18 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。

更多绑定和解绑手机令牌说明，请参见 4.2.3 管理登录手机令牌。

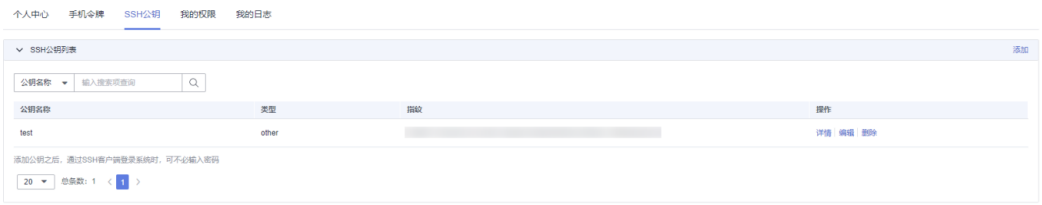
图4-19 手机令牌

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。

更多添加公钥、修改公钥、删除公钥等说明，请参见 4.2.4 管理个人 SSH 公钥。

图4-20 个人 SSH 公钥

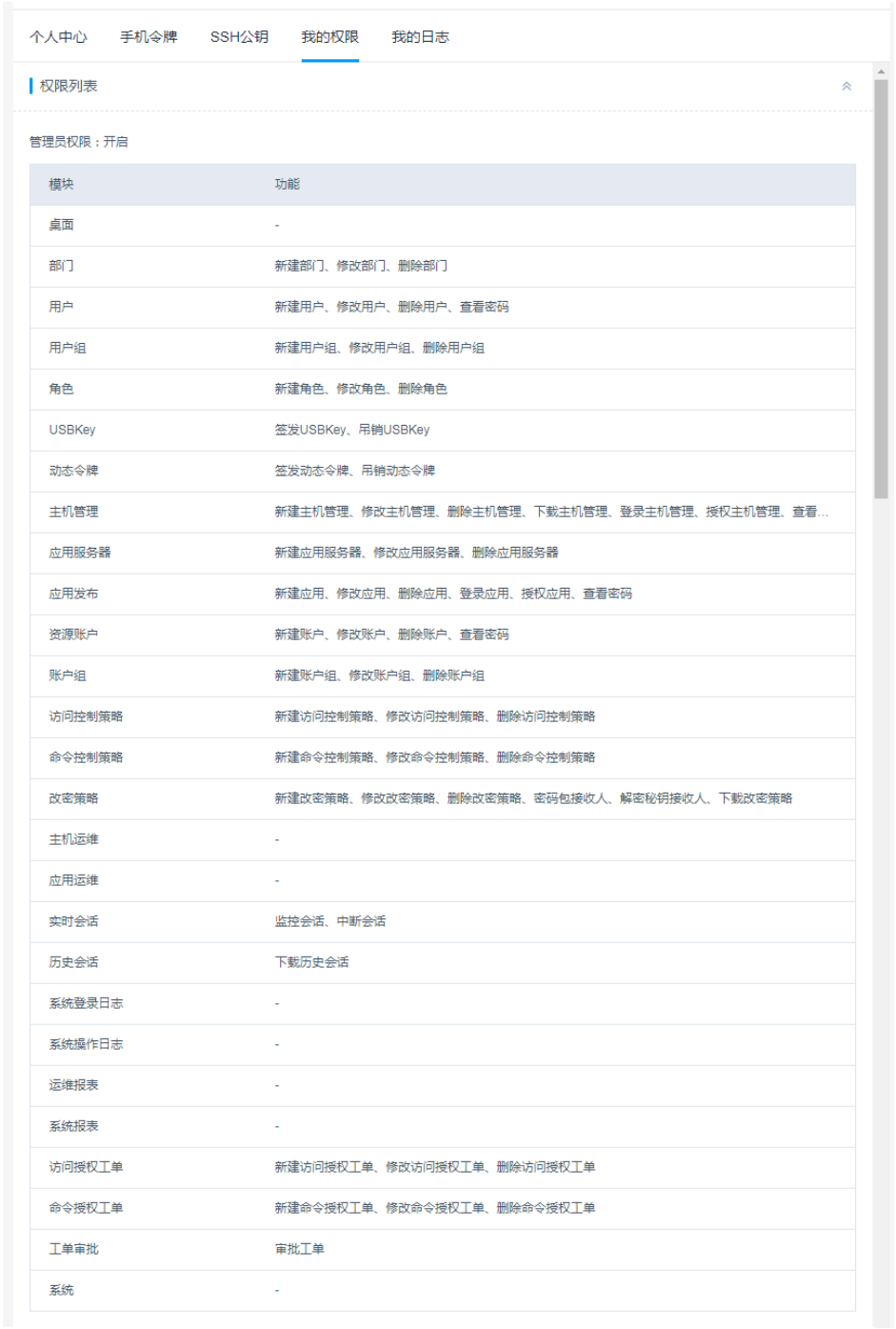


我的权限

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** 拥有云堡垒机系统最高权限。

图4-21 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 12.2 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4-22 我的日志列表

4.2.2 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 6.2.5 查询和修改用户信息。

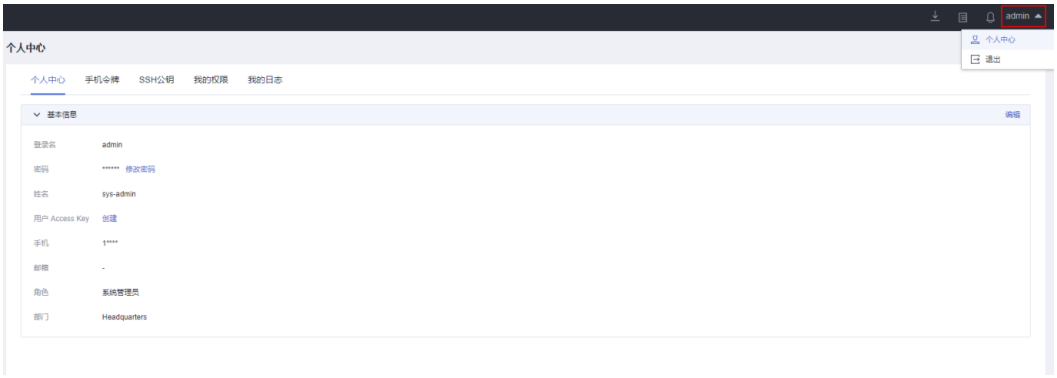
本小节主要介绍如何在个人中心修改个人密码和修改个人基本信息。

修改个人密码

步骤 1 登录云堡垒机系统。

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4-23 个人中心页面



步骤 3 在“基本信息”页签，单击“修改密码”，弹出修改密码窗口。

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，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。

步骤 5 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。

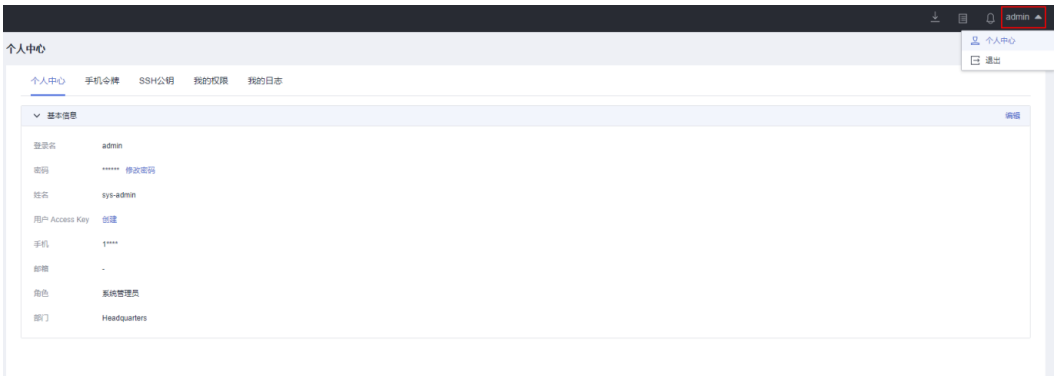
----结束

修改基本信息

步骤 1 登录云堡垒机系统。

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4-24 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

4.2.3 管理登录手机令牌

手机令牌可用来生成动态口令的手机客户端软件。云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，才能登录云堡垒机系统。更多详细说明，请参见 3.5.5 配置手机令牌类型。

目前云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：微信小程序手机令牌；
- RADIUS 手机令牌：APP 版手机令牌 Google Authenticator 和 FreeOTP。

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。

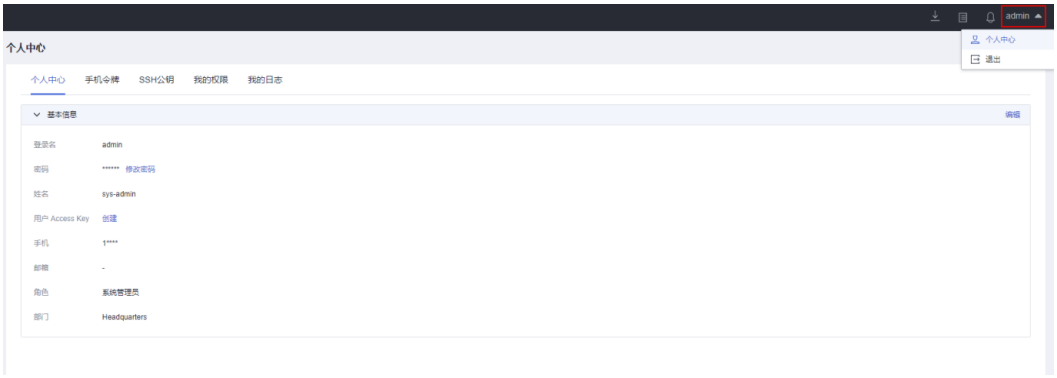
本小节主要介绍如何绑定和解绑手机令牌。

绑定手机令牌

步骤 1 登录云堡垒机系统。

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4-25 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。

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

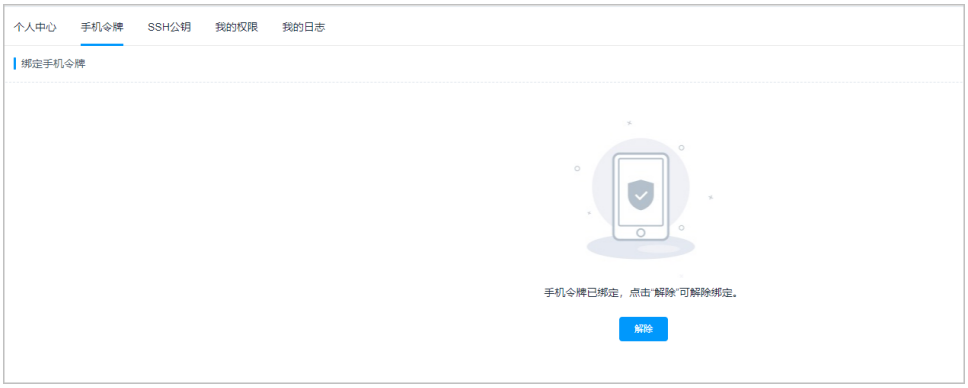
----结束

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。

图4-26 解除手机绑定



4.2.4 管理个人 SSH 公钥

用户个人 SSH 公钥是用在 SSH 客户端免密登录系统。

本小节主要介绍如何添加、修改、删除个人 SSH 公钥。

约束限制

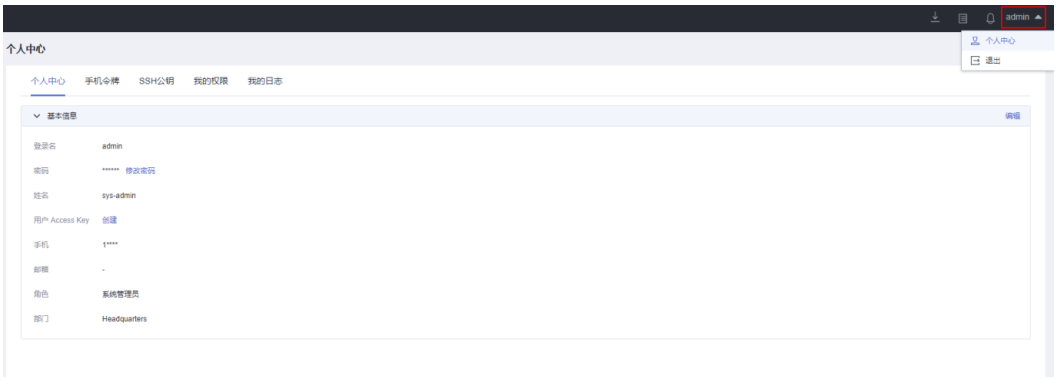
仅支持 OpenSSH 公钥。

添加 SSH 公钥

步骤 1 登录云堡垒机系统。

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4-27 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4-28 个人 SSH 公钥

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。

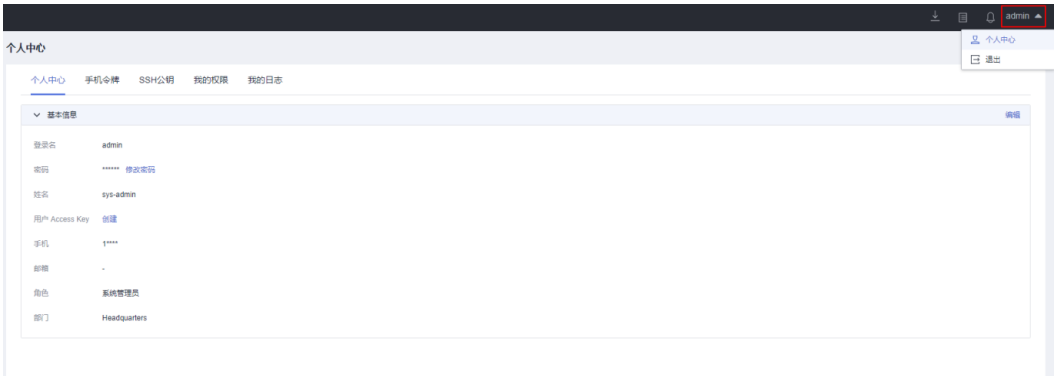
----结束

删除 SSH 公钥

步骤 1 登录云堡垒机系统。

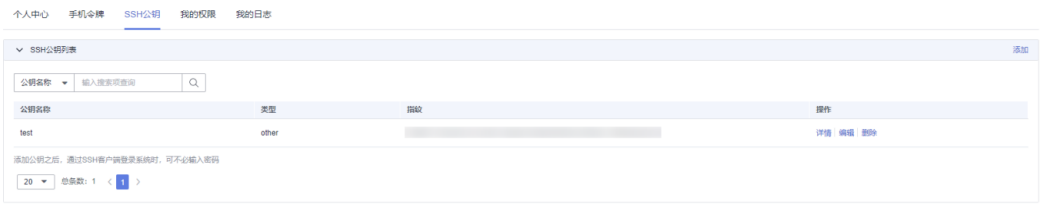
步骤 2 选择右上角用户名，单击“个人中心”，进入个人中心管理页面。

图4-29 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4-30 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。

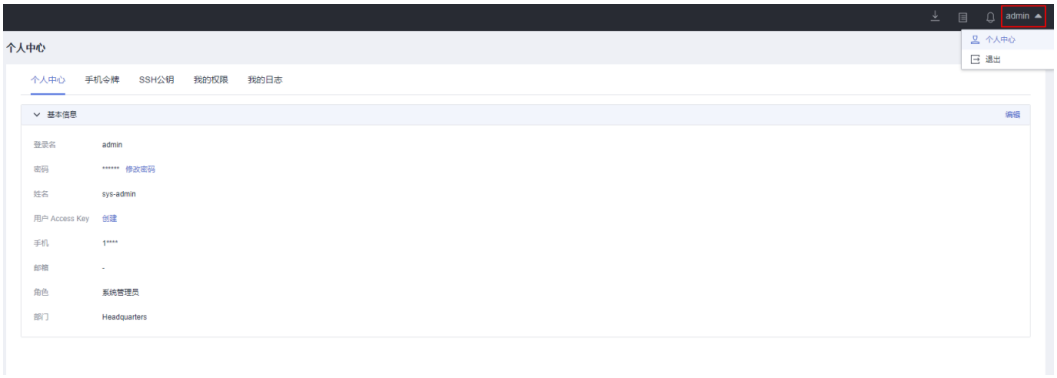
----结束

修改 SSH 公钥

步骤 1 登录云堡垒机系统。

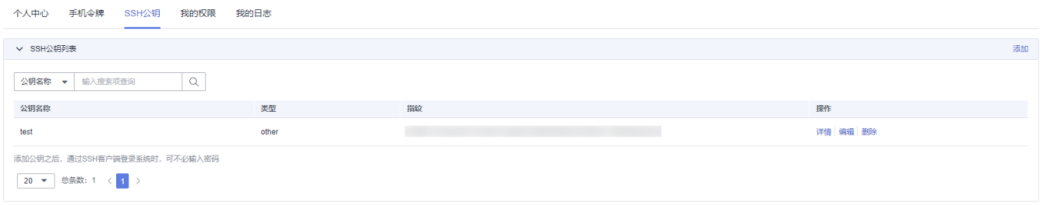
步骤 2 选择右上角用户名，单击“个人中心”，进入个人中心管理页面。

图4-31 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4-32 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

4.3 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”。

本小节主要介绍如何在任务中心查看任务内容。

操作步骤

步骤 1 登录云堡垒机系统。

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。

步骤 3 单击“查看更多”，进入任务中心列表页面。

图4-33 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。

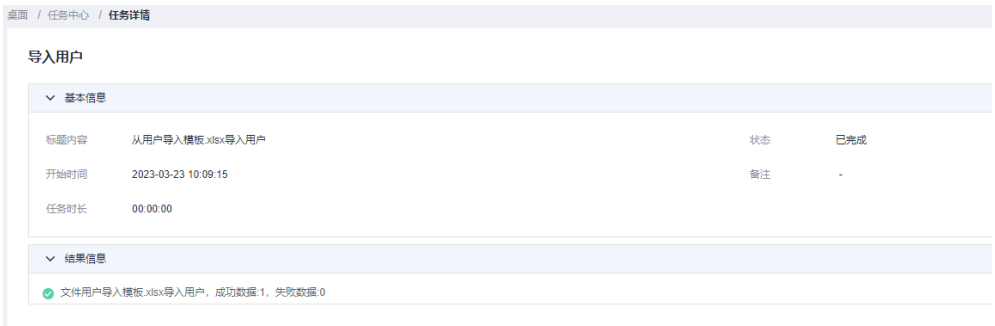
步骤 5 查看任务列表。

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4-34 查看任务详情。



----结束

4.4 消息中心

4.4.1 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。

本小节主要介绍如何在消息中心查看、删除、标记消息。

查看消息提醒

步骤 1 登录云堡垒机系统。

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4-35 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。

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。

----结束

删除消息提醒

步骤 1 登录云堡垒机系统。

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4-36 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。

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 登录云堡垒机系统。

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4-37 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。

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

4.4.2 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。

本小节主要介绍如何在消息中心创建系统公告。

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 登录云堡垒机系统。

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4-38 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。

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。

----结束

4.5 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。

本小节主要介绍如何进入下载中心。

操作步骤

步骤 1 登录云堡垒机系统。

步骤 2 单击右上角，进入下载中心工具列表页面。

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。

----结束

5 系统部门

5.1 部门概述

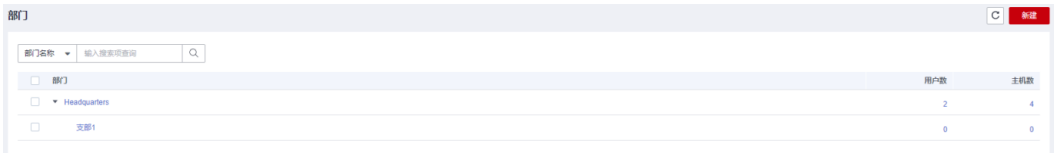
“部门”是用于划分组织结构，标识用户和资源的组织。系统默认有一个部门“总部”，仅可在“总部”基础上创建部门分支，且“总部”不可删除。

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5-1 部门管理



5.2 新建部门

云堡垒机默认“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 登录云堡垒机系统。

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。

图5-2 新建部门示例

----结束

快速创建

步骤 1 登录云堡垒机系统。

步骤 2 选择“部门”，进入部门管理页面。

步骤 3 在相应上级部门列，单击 + 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

5.3 删除部门

云堡垒机默认“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 登录云堡垒机系统。

步骤 2 选择“部门”，进入部门管理页面。

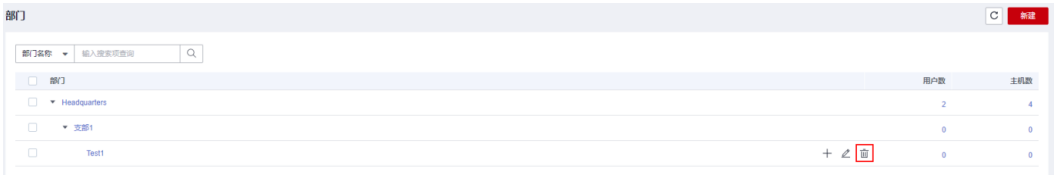
步骤 3 单个删除。

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。

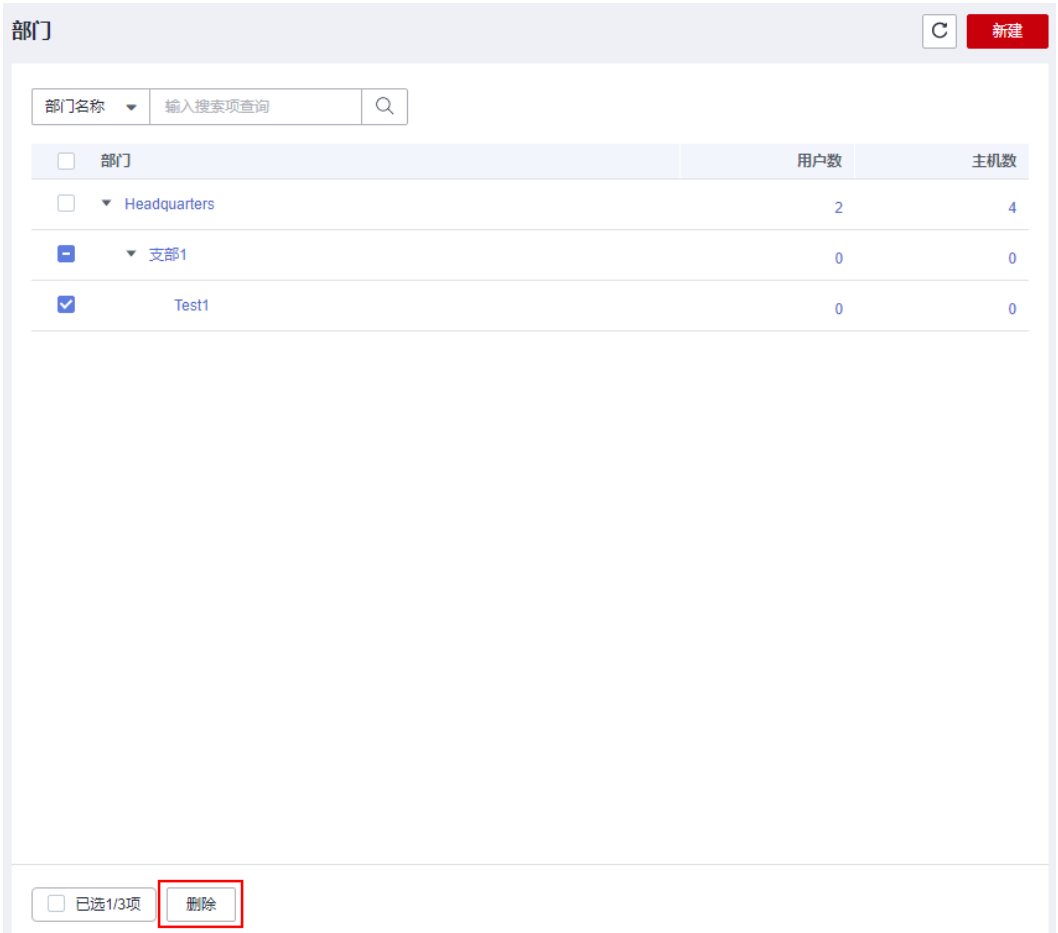
图5-3 单个删除部门



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5-4 批量删除部门



----结束

5.4 查看和修改部门信息

云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。

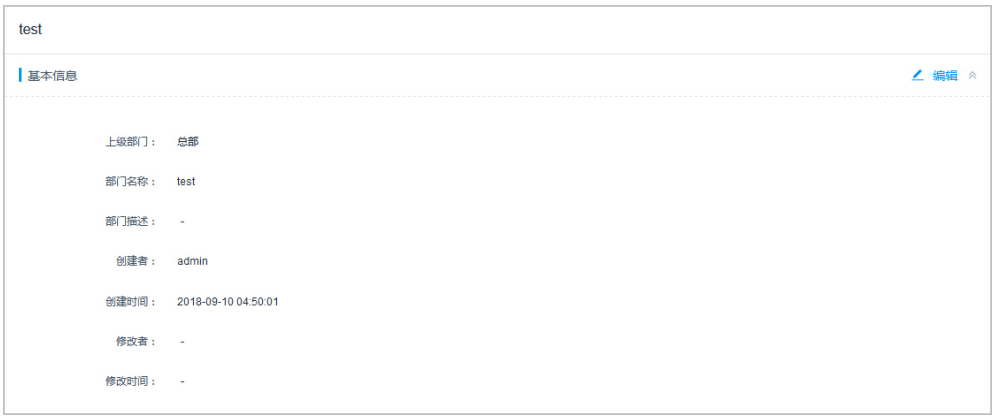
操作步骤

步骤 1 登录云堡垒机系统。

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。

图5-5 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

5.5 查询部门配置

云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 登录云堡垒机系统。

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

6 系统用户

6.1 用户概述

云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云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。

6.2 用户管理

6.2.1 新建用户并授权用户角色

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。

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 6.3.4 查询和修改角色信息。

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 登录云堡垒机系统。

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6-1 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。
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 6.5 远程认证管理。**
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

参数	说明
	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，详细介绍请见 6.3 用户角色管理。
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 5.2 新建部门。
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 登录云堡垒机系统。

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6-2 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。

参数	说明
	• 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	（必填）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 6.3.4 查询和修改角色信息。
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分。 • 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 5.5 查询部门配置。
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 6.4.4 查询和修改用户组信息。

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

云堡垒机通过配置 AD 认证“同步模式”，可一键同步 AD 域服务器上已有用户信息，无须手动创建用户。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 登录云堡垒机系统。

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。

图6-1 配置远程认证

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6-3 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。
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”。

参数	说明
	• 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。

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 域用户到云堡垒机，返回用户列表，即可查看同步的用户信息。

----结束

6.2.2 启停用户

云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

6.2.3 删除用户

云堡垒机系统用户支持一键删除和批量删除。

用户账号被删除后，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。

系统管理员 **admin** 不允许被删除。

前提条件

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 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

6.2.4 配置用户登录限制

背景介绍

为加强用户账号登录管理，云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 12.1.5.2 配置短信外发。
- 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 3.4.2 配置手机令牌登录，否则用户账号将无法登录。

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 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6-4 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 4.2.3 管理登录手机令牌后，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 6.6 USBKey 管理。 • 动态令牌：为生效动态令牌多因子认证，用户账号需再关联 6.7 动态令牌管理。
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

参数	说明
	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 地址登录云堡垒机。
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 地址登录云堡垒机。

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

批量修改用户登录配置

步骤 1 登录云堡垒机系统。

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 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 批量修改或取消多因子认证配置。

1. 单击“修改多因子认证”，弹出多因子认证修改窗口。
2. 勾选或去掉目标多因子认证方式。
3. 单击“确定”，即完成配置修改。

步骤 5 批量修改或取消有效期配置。

1. 单击“修改有效期”，弹出有效期修改窗口。
2. 勾选账号生效期或失效期，并选择目标日期和时间。去掉勾选，则取消有效期配置。
3. 单击“确定”，即完成配置修改。

步骤 6 批量修改登录时段限制配置。

1. 单击“登录时段限制”，弹出登录时段配置窗口。
2. 选择允许或禁止账号登录的目标星期和时刻。
3. 单击“确定”，即完成配置修改。

步骤 7 批量修改或取消登录 IP 地址限制配置。

1. 单击“登录 IP 地址限制”，弹出登录 IP 配置窗口。
2. 选择黑白名单限制方式，并输入或删除目标 IP 地址或地址段。
3. 单击“确定”，即完成配置修改。

步骤 8 批量修改或取消登录 MAC 地址限制配置。

1. 单击“MAC 地址限制”，弹出登录 MAC 配置窗口。
2. 选择黑白名单限制方式，并输入或删除目标 MAC 地址。
3. 单击“确定”，即完成配置修改。

----结束

6.2.5 查询和修改用户信息

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。

查询用户账号

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 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。

步骤 4 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。

----结束

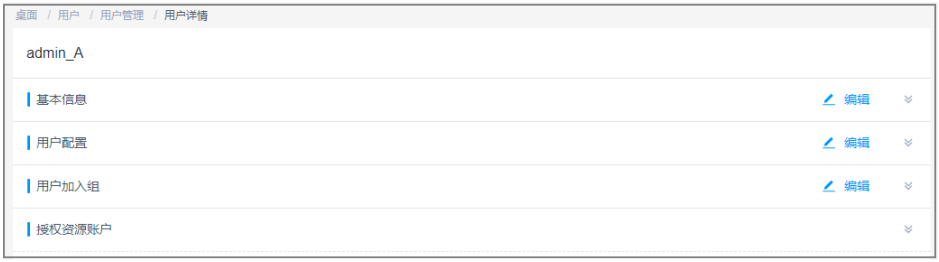
查看和修改用户信息

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 在查询的用户列表中，单击目标用户登录名，或者单击“管理”，进入用户信息详情页面。

图6-2 用户详情页面



步骤 4 查看和修改用户基本信息。

在“基本信息”区域，单击“编辑”，弹出基本信息编辑窗口，即可修改用户的基本信息。

- 可修改信息包括“认证类型”、“姓名”、“手机”、“邮箱”、“角色”、“所属部门”和“用户描述”。
- “登录名”不支持修改。

图6-3 用户基本信息

步骤 5 查看和修改用户登录配置信息。

在“用户配置”区域，单击“编辑”，弹出登录配置编辑窗口，即可修改用户的登录配置。

步骤 6 查看和移动用户组。

- 在“用户加入组”区域，可获取用户所属的用户组。
- 单击“编辑”，弹出用户组编辑窗口，即可移动所属用户组。

- 单击“操作”列“移出该组”，即可解除与该组关系。

步骤 7 查看用户已授权控制的资源。

展开“授权资源账户”区域，即可查看授权给该用户的资源账户信息。

图6-4 授权资源账户

----结束

批量修改用户信息

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 在查询的用户列表中，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 批量移动部门。

1. 单击“移动部门”，弹出部门修改窗口。
2. 选择目标部门。
3. 单击“确定”，即完成配置修改。

步骤 5 批量更改用户角色。

1. 单击“更改角色”，弹出角色修改窗口。
2. 选择目标角色。
3. 单击“确定”，即完成配置修改。

----结束

6.2.6 修改用户登录密码

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，云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 登录云堡垒机系统。

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 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“重置密码”，弹出重置密码窗口。

步骤 5 配置密码。

步骤 6 单击“确认”，完成密码重置。

建议及时将新配置的密码分发给被重置密码的用户。

----结束

6.2.7 导出用户信息

云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 登录云堡垒机系统。

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 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 单击“导出”，弹出导出用户账号确认窗口。

- 输入当前用户的密码，确保导出数据安全。
- （可选）设置加密密码，将导出文件加密。

步骤 5 单击“确认”，保存用户信息文件到本地。

步骤 6 打开本地文件，即可查看导出的用户基本信息。

----结束

6.2.8 加入用户组

本章节指导您如何将用户加入到用户组，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 登录云堡垒机系统。

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“确认”，返回用户详情页面，即可查看用户已加入的组。

----结束

多个用户批量加入组

步骤 1 登录云堡垒机系统。

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 在目标用户组“操作”列，单击“编辑组成员”，弹出用户组成员编辑窗口。

步骤 4 勾选多个用户账号，将用户加入用户组。

步骤 5 单击“确认”，返回用户组列表，即可查看用户组成员数增加。

----结束

6.3 用户角色管理

6.3.1 角色概述

用户所关联的角色，赋予用户不同系统操作访问权限。

云堡垒机系统仅 **admin** 拥有自定义角色和修改角色的权限。

缺省情况下，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。默认角色不可删除，但可修改默认角色的权限范围。

表6-5 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，主要负责云堡垒机系统的管理。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	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、资源组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的权限。

6.3.2 自定义角色

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 登录云堡垒机系统。

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“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。 • 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。

- 勾选系统模块和操作选项，即具备该模块和选项的权限。
- 仅勾选系统模块，则仅具备相应模块查看权限。

步骤 5 单击“确定”，返回角色列表，即可查看已创建角色。

----结束

6.3.3 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 登录云堡垒机系统。

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

6.3.4 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 登录云堡垒机系统。

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6-5 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

6.4 用户组管理

6.4.1 用户组概述

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 8.1.1 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。

6.4.2 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 登录云堡垒机系统。

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 6.2.8 加入用户组。

----结束

6.4.3 删除用户组

云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。

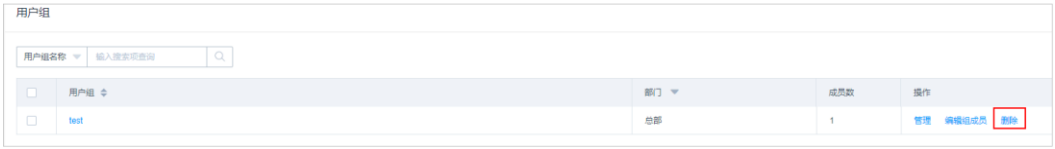
操作步骤

步骤 1 登录云堡垒机系统。

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。

图6-6 删除单个用户组



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

6.4.4 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 登录云堡垒机系统。

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。

图6-7 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 远程认证管理

6.5.1 配置 AD 域远程认证

云堡垒机与 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，云堡垒机不会同步 AD 域服务器上的用户信息，需要管理员手工创建用户。当用户登录云堡垒机时，将由 AD 域服务器提供认证服务。
- 同步模式

  在此模式下，云堡垒机可以同步 AD 域服务器的用户信息，无需管理员新建用户。当用户登录云堡垒机时，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。

本小节主要介绍如何配置 AD 域认证模式。

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 登录云堡垒机系统。

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。

图6-8 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 6-8。

表6-8 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。

6.5.2 配置 LDAP 远程认证

云堡垒机与 LDAP 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 LDAP 域认证模式。

约束限制

- 不支持一键同步 LDAP 服务器用户。
- 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。

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 登录云堡垒机系统。

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。

图6-9 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：

- “认证模式”选择“认证”时，参照表 6-9 配置相关参数。

图6-10 配置 LDAP 认证

表6-9 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

参数	说明
	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”。 • 认证模式：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。 • 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。

- “认证模式”选择“查询”时，参照表 6-10 配置相关参数。

表6-10 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。
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。

参数	说明
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 LADP 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，可在单击“删除”，删除认证信息。删除后认证信息不能找回，请谨慎操作。

6.5.3 配置 RADIUS 远程认证

云堡垒机与 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 登录云堡垒机系统。

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。

图6-11 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6-11 RADIUS 域认证模式参数说明

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”。
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。

6.5.4 配置 Azure AD 远程认证

云堡垒机与 Azure AD 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 Azure AD 认证模式。

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。

操作步骤

步骤 1 登录云堡垒机系统。

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。

图6-12 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6-12 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。
回复 URL	自动填写，默认为返回当前云堡垒机的跳转链接。 当云堡垒机 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 控制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 6.2.1 新建用户并授权用户角色。

6.5.5 配置 SAML 远程认证

云堡垒机与 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 登录云堡垒机系统。

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。

图6-13 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。

图6-14 配置 SAML 认证

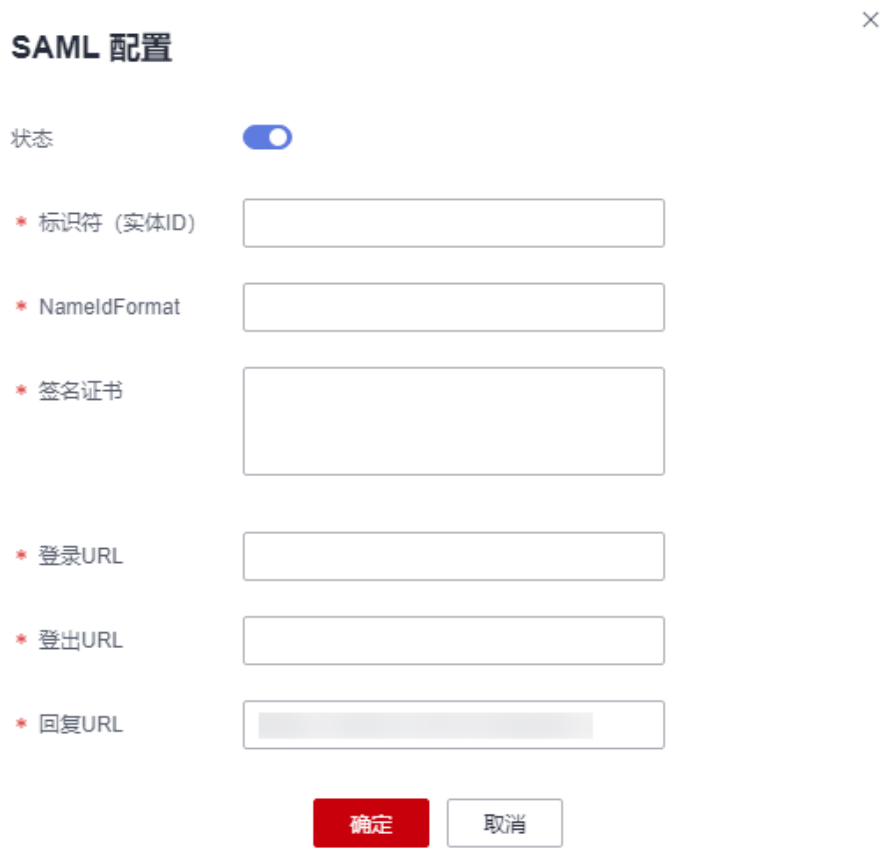


表6-13 SAML 域认证参数说明

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。
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。

参数	说明
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 SingleSLogoutService 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

6.6 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 USBKey6.6 USBKey 管理厂商。

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 登录云堡垒机系统。

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。

图6-15 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6-14 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。

关联用户登录云堡垒机系统时，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 登录云堡垒机系统。

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

6.7 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。目前云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 登录云堡垒机系统。

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6-16 新建签发动态令牌

步骤 4 配置令牌标识信息。

表6-15 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。

关联用户登录云堡垒机系统时，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 登录云堡垒机系统。

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 登录云堡垒机系统。

步骤 2 选择“用户 > 动态令牌”，进入动态令牌列表页面。

步骤 3 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 4 单击“导出”，保存文件到本地。

----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 登录云堡垒机系统。

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

7 系统资源

7.1 资源概述

云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，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、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。
  - 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。

7.2 通过云堡垒机纳管主机资源

云堡垒机支持添加 SSH、RDP、VNC、TELNET、FTP、SFTP、DB2、MySQL、SQL Server、Oracle、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、从文件导入主机资源、导入云主机资源、自动发现主机资源、克隆主机资源等方式，将主机资源纳入云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 6.3.4 查询和修改角色信息。

前提条件

已获取“主机管理”模块操作权限。

添加单个主机资源

步骤 1 登录云堡垒机系统。

步骤 2 选择“资源 > 主机管理”，进入主机管理列表页面。

步骤 3 单击“新建”，弹出新建主机编辑窗口。

配置主机资源的网络参数和基础信息。

表7-1 主机资源网络参数说明

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。
主机地址	输入主机与云堡垒机网络通畅的 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** 因云堡垒机管理同一 VPC 网络下的主机资源，根据网络稳定性与就近优势。私有 IP 对外访问的端口不受网络安全（安全组和 ACL）的限制。EIP 为独立的弹性 IP，对外访问的端口受网络安全限制，可能导致无法通过云堡垒机登录到主机。 故建议“主机地址”优先考虑配置同 VPC 网络下私有 IP 地址。
端口	输入主机的端口号。
系统类型	（可选）选择主机的操作系统类型或者设备系统类型。 • 默认不设置，后台根据资源系统类型匹配。 • 支持 14 种系统类型。 • 同时支持系统管理员 **admin** 自定义系统类型。 • 详情请参见 7.8 自定义系统类型说明。

参数	说明
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”协议类型主机时，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”协议类型主机可选择运维终端类型。 可选择 Linux、Xterm。
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7-2 纳管主机账户信息说明

参数	说明
添加账户	选择立即添加账户，或以后再添加账户。 • 选择“立即添加”，需要继续配置下面的各项内容。 • 选择“以后添加”，将结束本页配置，后续您可以在资源列表或资源详情中添加账户。
登录方式	选择登录方式，可选择自动登录、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。
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

参数	说明
	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。 • 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

从文件导入主机资源

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 单击界面右上角的“导入”，弹出配置界面。

步骤 4 “导入方式”选择“从文件导入”。

步骤 5 单击“单击下载”，下载模板文件到本地。

步骤 6 按照模板文件中的配置项说明，填写要导入的主机配置信息。

表7-3 主机导入模板参数说明

参数	说明

参数	说明
名称	（必填）填入自定义主机资源名。
IP 地址/域名	（必填）填入主机的 IP 地址或域名。
协议类型	（必填）选择主机资源的协议类型，仅能填写一种类型。
端口	（必填）填入主机端口。
系统类型	填入主机的系统类型。
所属部门	（必填）填入资源所归属的部门，需完整填写部门结构。 • 仅可填入一组部门层级，一个资源只能分属一个部门。 • 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 5.5 查询部门配置。
标签	填入主机资源标签。 • 可填入多个标签，标签之间用“，”隔开。
主机描述	填入对主机资源的简要描述。
主机账户	填入主机资源账户名称。 • 不填写，也不会生成 Empty 账户。
登录方式	选择主机资源登录方式。 • 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。
passphrase	填入 SSH Key 对应私钥序列。 若您已生成私钥密码，每次登录主机需手动输入私钥密码。
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。

参数	说明
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	针对 SSH 协议类型主机，填入 SSH 主机资源账户名称，将该账户提权为特权账户。
切换命令	填入切换账户的执行命令。
账户描述	填入对资源账户的简要描述。
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 7.6 账户组。

步骤 7 单击“单击上传”，选择要导入的文件。

步骤 8 （可选）勾选“覆盖已有主机”，默认不勾选。

- 勾选，表示当**协议类型@主机地址:端口**信息重复时，覆盖原有主机信息。
- 不勾选，表示当**协议类型@主机地址:端口**信息重复时，跳过重复的主机信息。

步骤 9 单击“确定”，返回主机列表查看新增的主机。

说明

- 文件方式导入主机时，需严格按照 Excel 配置要求填写主机信息。
- SSH 协议类型主机支持配置 SSH Key 私钥登录方式。在填写 SSH Key 和 Passphrase 时，需填写正确的私钥和密码，不要引入其他字符和空格。配置 SSH Key 公钥和 Passphrase 密码后，优先 SSH Key 私钥方式验证登录资源。
- SSH Key 私钥和 Passphrase 密码为选填项，建议批量导入的资源仅纳管主机账户和密码登录。

----结束

导入云主机资源

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 单击界面右上角的“导入”，弹出配置界面。

步骤 4 “导入方式”选择“导入云主机”，跳转到导入云主机配置窗口。

表7-4 导入云主机参数配置说明

参数	说明
云平台	选择云平台， 目前支持导入云主机资源。
Access Key ID	单击输入框后面的帮助按钮，获取相关信息。
Access Key Secret	单击“Access Key ID”输入框后面的帮助按钮，获取相关信息。
优先导入 IP	可选择“公网”或“内网”。
更多选项	（可选）勾选“覆盖已有主机”，默认不勾选。 • 勾选，表示当**协议类型@主机地址:端口**信息重复时，覆盖原有主机信息。 • 不勾选，表示当**协议类型@主机地址:端口**信息重复时，跳过重复的主机信息。
所属部门	为导入主机配置部门。
标签	为导入主机配置标签。
导入区域	选择导入区域，各个云平台支持导入主机区域不同。
运行环境	导入主机的运行环境。

步骤 5 单击“确定”，返回主机列表查看新增的主机。

----结束

自动发现主机资源

“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

主机与云堡垒机在同一 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 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

7.3 通过云堡垒机纳管应用服务器

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云堡垒机管理的功能。

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。

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

本章节主要介绍通过添加单个应用服务器、从文件导入应用服务器、添加单个应用发布、从文件导入应用发布，将应用资源纳入云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。
- 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 服务器仅支持调用 Firefox 浏览器应用和达梦管理工具 V8。

- 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。
- Linux 服务器的密码请联系技术支持获取。
- 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。

前提条件

- 已另行购买 Windows 类型主机或者 Linux 服务器、镜像、企业授权码、客户端 License 等资源，用于部署应用发布服务器。
- 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 登录云堡垒机系统。

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。

表7-5 应用服务器参数说明

参数	说明
服务器类型	• Windows • 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。 • “服务器类型”选择“Windows”时： 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 • “服务器类型”选择“Linux”时： 支持类型：DM Tool、KingbaseES Tool、Firefox-Linux、GBaseDataStudio for GBase8a。 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，Linux 服务器固定为 2376。
服务器账户	“服务器类型”选择“Windows”时，需要配置此参数。 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*

参数	说明
	户名，例如 *ad\administrator*。
密码	• “服务器类型”选择“Windows”时，输入访问应用的服务器账户的密码。 • “服务器类型”选择“Linux”时，密码联系技术支持获取。
所属部门	选择应用服务器的归属部门。
程序启动路径	“服务器类型”选择“Windows”时，需要配置此参数。 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。

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 登录云堡垒机系统。

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

添加单个应用发布

步骤 1 登录云堡垒机系统。

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7-6 新建应用发布参数说明

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。
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。
更多选项	（可选）选择文件管理、上行剪切板、下行剪切板、键盘审计。
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7-7 添加应用资源账户

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。

参数	说明
	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）。
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

从文件导入应用发布

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 登录云堡垒机系统。

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

7.4 将纳管的主机或应用添加到资源账户

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。

本小节主要介绍纳管资源后，如何添加资源账户。

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“新建”，弹出资源账户编辑窗口，配置资源账户的属性。

表7-8 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。
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”。 • 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。 • 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。

参数	说明
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7-9 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。

参数	说明
	• 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。
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。
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 、SCP、PostgreSQL、GaussDB。 • 应用资源应用类型：IE、Firefox-Windows、Chrome、VNC Client、

参数	说明
	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 7.6.2 新建账户组。

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 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 7-10 所示。

表7-10 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

参数名称	参数说明
	• 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

7.5 资源管理

7.5.1 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。

表7-11 资源账户状态说明

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，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。

约束限制

应用资源的账户不支持在线验证。

前提条件

已获取“资源账户”模块操作权限。

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（4.4.1 管理消息列表），不会生成任务。

实时验证

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 勾选指定账户，单击列表下方的“验证”，弹出验证配置框。

步骤 4 设置“连接超时”时间，以及“任务完成通知”。

- 默认“链接超时”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 4.3 任务中心查看验证结果详情。

步骤 5 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。

----结束

批量验证

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 登录云堡垒机系统。

步骤 2 选择“资源 > 账户组”，进入账户组列表页面。

步骤 3 勾选指定账户组，单击列表下方的“验证”，弹出验证配置框。

步骤 4 设置“连接超时”时间，以及“任务完成通知”。

- 默认“链接超时”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 4.3 任务中心查看验证结果详情。

步骤 5 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

7.5.2 删除资源

云堡垒机可删除已纳管的资源，包括主机资源、应用服务器、应用资源、资源账户等。

- 删除了主机资源或应用资源，相应关联的资源账户也会自动删除。
- 删除了应用服务器，相应关联的应用也会自动删除。

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。

删除资源账户

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 单击指定账户“操作”列的“删除”，可以删除该账户。

步骤 4 同时勾选多个账户，然后单击列表下方的“删除”，可以批量删除多个账户。

----结束

删除主机资源

步骤 1 登录云堡垒机系统。

步骤 2 选择“资源 > 主机管理”，进入主机列表页面。

步骤 3 单击指定主机“操作”列的“更多 > 删除”，可以删除该主机资源。

步骤 4 同时勾选多个主机，单击列表下方的“删除”，批量删除多个主机资源。

----结束

删除应用服务器

步骤 1 登录云堡垒机系统。

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 单击指定应用服务器“操作”列的“删除”，可以删除该应用服务器。

步骤 4 同时勾选多个应用服务器，单击列表下方的“删除”，批量删除多个应用服务器。

----结束

删除应用发布

步骤 1 登录云堡垒机系统。

步骤 2 选择“资源 > 应用发布 > 应用列表”，进入应用列表页面。

步骤 3 单击指定应用“操作”列的“更多 > 删除”，可以删除该应用资源。

步骤 4 同时勾选多个应用，单击列表下方的“删除”，批量删除多个应用资源。

----结束

7.5.3 查询和修改资源配置

云堡垒机可查看和修改纳管的资源配置，包括主机资源、应用服务器、应用资源、资源账户等。

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。

查看和修改主机配置

步骤 1 登录云堡垒机系统。

步骤 2 选择“资源 > 主机管理”，进入主机列表页面。

步骤 3 查询主机资源。

- 快速查询
  在搜索框中输入关键字，根据主机名称、主机地址、端口等快速查询主机资源。
- 高级搜索
  在相应属性搜索框中分别关键字，精确查询主机资源。

图7-1 高级搜索

步骤 4 单击目标主机名称，或者单击“管理”，进入主机详情页面。

步骤 5 查看和修改主机基本信息。

在“基本信息”区域，单击“编辑”，弹出基本信息编辑窗口，即可修改主机资源的基本信息。

- 可修改信息包括“主机名称”、“主机地址”、“端口”、“系统类型”、“所属部门”和“主机描述”等。
- “协议类型”不支持修改。

步骤 6 查看和修改主机资源账户。

- 在“资源账户”区域，单击“添加”，弹出添加账户窗口，可立即添加主机资源账户。
- 在相应资源账户行，单击“移除”，可立即删除该资源账户。

步骤 7 查看主机资源授权用户。

展开“授权用户”区域，可查看该主机已授权的用户。

图7-2 查看授权用户

----结束

批量修改主机资源配置

- 支持批量移动主机所属部门。
- 支持批量修改主机的文件管理、上行剪切板、下行剪切板、X11 转发、键盘审计功能。
- 支持批量修改主机编码格式。
- 支持批量修改主机系统类型。

步骤 1 登录云堡垒机系统。

步骤 2 选择“资源 > 主机管理”，进入主机列表页面。

步骤 3 在查询的主机列表中，勾选待修改配置的主机，单击左下角“更多”，展开批量操作项。

步骤 4 批量移动部门。

1. 单击“移动部门”，弹出部门修改窗口。
2. 选择目标部门。
3. 单击“确定”，即完成配置修改。

步骤 5 批量修改更多选项。

- 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。

1. 单击“更多选项”，弹出更多选项修改窗口。
2. 勾选目标功能选项，可选择文件管理、上行剪切板、下行剪切板、X11 转发、键盘审计。
3. 单击“确定”，即完成配置修改。

步骤 6 批量修改主机编码，仅 SSH、TELNET 协议类型主机可修改。

1. 单击“修改主机编码”，弹出主机编码修改窗口。
2. 选择目标主机编码，可选择 UTF-8、Big5、GB 18030。
3. 单击“确定”，即完成配置修改。

步骤 7 批量修改系统类型。

1. 单击“修改系统类型”，弹出系统类型修改窗口。
2. 选择目标系统类型。
3. 单击“确定”，即完成配置修改。

----结束

查看和修改应用服务器配置

步骤 1 登录云堡垒机系统。

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 查询应用服务器。

- 快速查询

  在搜索框中输入关键字，根据服务器名称、服务器地址、应用服务器账户等快速查询。
- 高级搜索

  在相应属性搜索框中分别关键字，精确查询应用服务器。

图7-3 高级搜索

步骤 4 单击目标服务器名称，或者单击“管理”，进入服务器详情页面。

步骤 5 查看和修改应用服务器基本信息。

在“基本信息”区域，单击“编辑”，弹出基本信息编辑窗口，即可修改应用服务器的基本信息。

- 可修改信息包括“服务器名称”、“服务器地址”、“端口”、“服务器账户”、“密码”、“所属部门”、“程序启动路径”和“服务器描述”等。
- “类型”不支持修改。

----结束

批量修改应用服务器配置

支持批量移动应用服务器所属部门。

步骤 1 登录云堡垒机系统。

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 在查询的应用服务器列表中，勾选待修改配置的应用服务器，单击左下角“更多”，展开批量操作项。

步骤 4 批量移动部门。

1. 单击“移动部门”，弹出部门修改窗口。
2. 选择目标部门。
3. 单击“确定”，即完成配置修改。

----结束

查看和修改应用发布配置

步骤 1 登录云堡垒机系统。

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 查询应用发布服务。

- 快速查询

  在搜索框中输入关键字，根据应用名称、应用地址等快速查询。
- 高级搜索

  在相应属性搜索框中分别关键字，精确查询应用发布。

步骤 4 单击目标应用名称，或者单击“管理”，进入应用详情页面。

步骤 5 查看和修改应用发布基本信息。

在“基本信息”区域，单击“编辑”，弹出基本信息编辑窗口，即可修改应用资源的基本信息。

- 可修改信息包括“应用名称”、“应用服务器”、“应用端口”、“应用地址”、“所属部门”和“应用描述”等。

步骤 6 查看和修改应用资源账户。

- 在“资源账户”区域，单击“添加”，弹出添加账户窗口，可立即添加应用资源账户。
- 在相应资源账户行，单击“移除”，可立即删除该资源账户。

步骤 7 查看应用资源授权用户。

展开“授权用户”区域，可查看该应用已授权的用户。

----结束

批量修改应用发布配置

- 支持批量移动应用发布所属部门。
- 支持批量修改应用发布的文件管理、剪切板、X11 转发、键盘审计功能。

步骤 1 登录云堡垒机系统。

步骤 2 选择“资源 > 应用发布 > 应用列表”，进入应用列表页面。

步骤 3 在查询的应用列表中，勾选待修改配置的应用，单击左下角“更多”，展开批量操作项。

步骤 4 批量移动部门。

1. 单击“移动部门”，弹出部门修改窗口。
2. 选择目标部门。
3. 单击“确定”，即完成配置修改。

步骤 5 批量修改更多选项。

1. 单击“更多选项”，弹出更多选项修改窗口。
2. 勾选目标功能选项，可选择文件管理和剪切板。
3. 单击“确定”，即完成配置修改。

----结束

查看和修改资源账户配置

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 查询应用发布服务。

- 快速查询

  在搜索框中输入关键字，根据资源账户、关联资源、主机地址、是否特权账户等快速查询。
- 高级搜索

  在相应属性搜索框中分别关键字，精确查询资源账户。

步骤 4 单击目标资源账户名称，或者单击“管理”，进入账户详情页面。

步骤 5 查看和修改资源账户基本信息。

在“基本信息”区域，单击“编辑”，弹出基本信息编辑窗口，即可修改资源账户的基本信息。

- 可修改信息包括“特权账户”、“密码”、“账户描述”等。
- “关联资源”、“登录方式”、“资源账户”、“SSH Key”、“Passphrase”不支持修改。

步骤 6 查看和修改账户加入的组。

- 在“账户加入的组”区域，单击“编辑”，弹出编辑账户组窗口，可立即移动账户的组。
- 在相应账户组行，单击“移出该组”，可立即解除与该组关系。

步骤 7 查看资源账户授权用户。

展开“授权用户”区域，可查看该账户已授权的用户。

图7-4 查看授权用户

----结束

7.5.4 导出资源信息

云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。

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。

批量导出主机资源信息

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 勾选需要导出的主机。

若不勾选，默认导出全部主机。

步骤 4 单击“导出”，弹出导出主机资源确认窗口。

步骤 5 导出确认。

1. （可选）设置加密密码：可选择设置。不设置，下载的主机资源文件为未加密的 CSV 格式；设置密码，下载的主机资源文件为加密的 ZIP 格式。
2. （必选）用户密码：输入当前用户的登录密码，验证通过才允许导出主机资源信息，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

批量导出应用服务器信息

步骤 1 登录云堡垒机系统。

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 勾选需要导出的应用服务器。

若不勾选，默认导出全部应用服务器。

步骤 4 单击“导出”，弹出导出应用服务器确认窗口。

步骤 5 导出确认。

1. （可选）设置加密密码：可选择设置。不设置，下载的应用服务器文件为未加密的 CSV 格式；设置密码，下载的应用服务器文件为加密的 ZIP 格式。
2. （必选）用户密码：输入当前用户的登录密码，验证通过才允许导出应用服务器信息，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

批量导出应用资源信息

步骤 1 登录云堡垒机系统。

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 勾选需要导出的应用。

若不勾选，默认导出全部应用。

步骤 4 单击“导出”，弹出导出应用发布确认窗口。

步骤 5 导出确认。

1. （可选）设置加密密码：可选择设置。不设置，下载的应用发布文件为未加密的CSV 格式；设置密码，下载的应用发布文件为加密的 ZIP 格式。
2. （必选）用户密码：输入当前用户的登录密码，验证通过才允许导出应用发布信息，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

批量导出资源账户

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 勾选需要导出的账户。

若不勾选，默认导出全部账户。

步骤 4 单击“导出”，弹出导出资源账户确认窗口。

步骤 5 导出确认。

1. （可选）设置加密密码：可选择设置。不设置，下载的资源账户文件为未加密的CSV 格式；设置密码，下载的资源账户文件为加密的 ZIP 格式。
2. （必选）用户密码：输入当前用户的账号登录密码，验证通过才允许导出资源账户，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

7.5.5 加入账户组

本章节指导您如何将资源账户加入到账户组。一个资源账户可加入多个账户组。

约束限制

- 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

已获取“资源账户”模块操作权限。

单个资源账户加入组

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 在目标资源账户“操作”列，单击“加入组”，弹出编辑账户窗口。

步骤 4 勾选一个或多个账户组，将资源账户加入账户组。

步骤 5 单击“确认”，返回资源账户详情页面，即可查看资源账户已加入的组。

----结束

多个资源账户批量加入组

步骤 1 登录云堡垒机系统。

步骤 2 选择“资源 > 账户组”，进入账户组列表页面。

步骤 3 在目标账户组“操作”列，单击“添加成员”，弹出添加资源账户窗口。

步骤 4 勾选多个资源账户，将资源账户加入账户组。

步骤 5 单击“确认”，返回账户组列表，即可查看账户组成员数增加。

----结束

7.6 账户组

7.6.1 账户组概述

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。

7.6.2 新建账户组

本章节指导您如何创建账户组。

前提条件

已获取“资源账户”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“资源 > 账户组”，进入账户组列表页面。

步骤 3 单击“新建”，弹出新建账户组窗口，配置账户组基本信息。

表7-12 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 4 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 7.5.5 加入账户组。

----结束

7.6.3 删除账户组

云堡垒机新建账户组后，支持删除账户组。删除账户组后，通过账户组授权的资源权限将失效。

前提条件

已获取“资源账户”模块操作权限。

删除账户组

步骤 1 登录云堡垒机系统。

步骤 2 选择“资源 > 账户组”，进入账户组列表页面。

步骤 3 单击账户组“操作”列的“删除”，即可删除该账户组。

步骤 4 同时勾选多个账户组，单击列表下方的“删除”，可批量删除多个账户组。

----结束

7.6.4 查询和修改账户组信息

若账户组信息有变更需求，可查看和修改账户组信息，包括查看账户组基本信息、查看账户组成员、修改账户组基本信息、添加成员、移除组成员等。

约束限制

- 下级部门拥有“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。

操作步骤

步骤 1 登录云堡垒机系统。

步骤 2 选择“资源 > 账户组”，进入账户组列表页面。

步骤 3 查询账户组。

在搜索框中输入关键字，根据账户组名称快速查询。

步骤 4 单击账户组名称，或者单击“管理”，进入账户组详情页面。

步骤 5 在“基本信息”区域，可查看账户组基本信息。

单击“编辑”，弹出基本信息配置窗口，即可修改账户组名称和简要描述。

步骤 6 在“账户组成员”区域，可查看账户组所有成员信息。

- 单击“添加”，弹出资源账户添加窗口，可添加或移除资源账户。
- 单击资源账户行的“移除出组”，可立即将资源账户移除出组。

----结束

7.7 资源标签

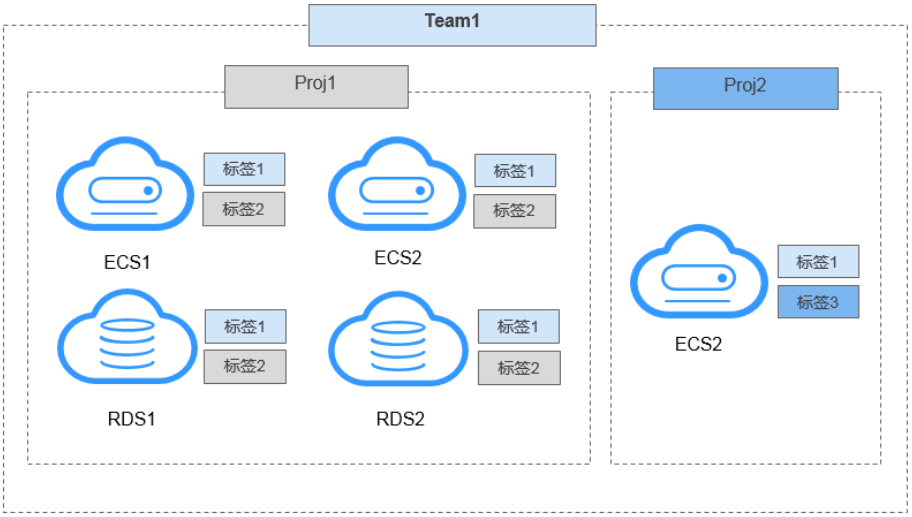
7.7.1 资源标签概述

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。

图 7-5 说明了标签的工作方式。在此示例中，以标识云主机 ECS 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7-5 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 7-13。

表7-13 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

7.7.2 新建资源标签

云堡垒机系统每个用户可自定义资源标签，资源标签仅能个人账户使用，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。

7.2 通过云堡垒机纳管主机资源或 7.3 通过云堡垒机纳管应用服务器可直接配置“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。

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

7.7.3 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。

操作步骤

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

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

7.8 自定义系统类型

云堡垒机能管理资源系统类型，并可自定义系统类型。

默认支持 14 种系统类型。

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 登录云堡垒机系统。

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7-14 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 管理系自定义统类型。

----结束

其他管理操作

步骤 1 登录云堡垒机系统。

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 系统策略

8.1 访问控制策略

8.1.1 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。
- 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：指该策略限制指定来源 IP 地址的用户访问资源。
  - 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。

操作步骤

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8-1 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。 • 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。
更多选项	在运维过程中管理文件或文件夹权限，RDP 剪切板、键盘审计和会话窗口显示水印功能。 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。
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。

若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

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。
- 若需线下管理策略，可单击“导出”，以 CSV 格式导出全量访问控制策略详情。

8.1.2 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。

8.1.3 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关键字，精确查询策略。

  图8-1 高级搜索

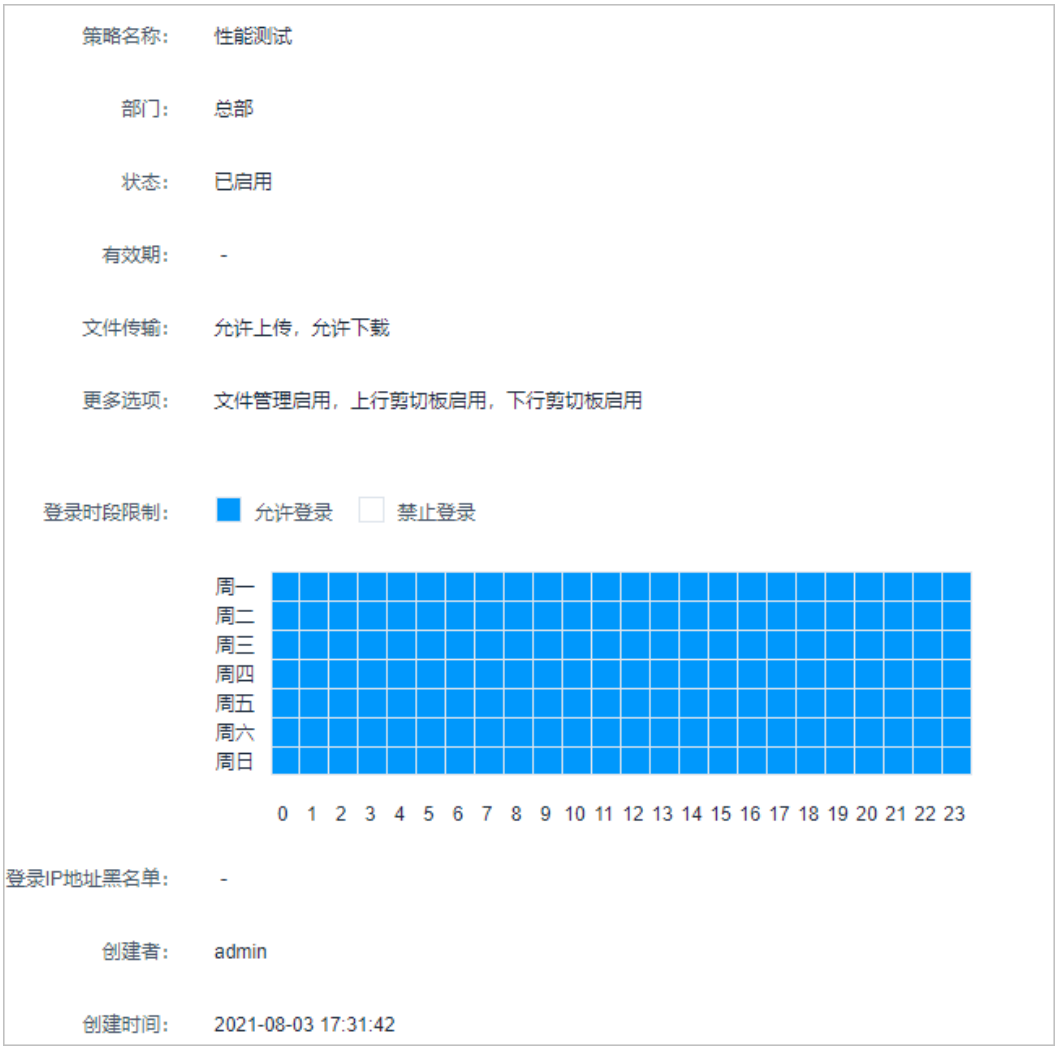
步骤 4 单击目标策略名称，或者单击“管理”，进入策略详情页面。

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”、“文件管理”、“上行剪切板”、“下行剪切板”、“登录时段限制”、“键盘审计”和“IP 限制”等。

图8-2 查看策略基本信息



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

8.2 命令控制策略

8.2.1 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

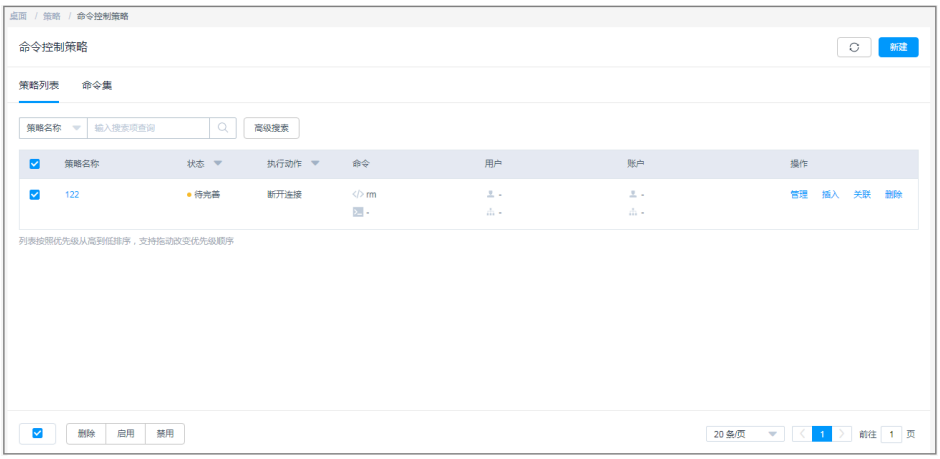
已获取“命令控制策略”模块操作权限。

新建命令控制策略

步骤 1 登录云堡垒机系统。

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。

图8-3 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。

图8-4 配置策略基本信息

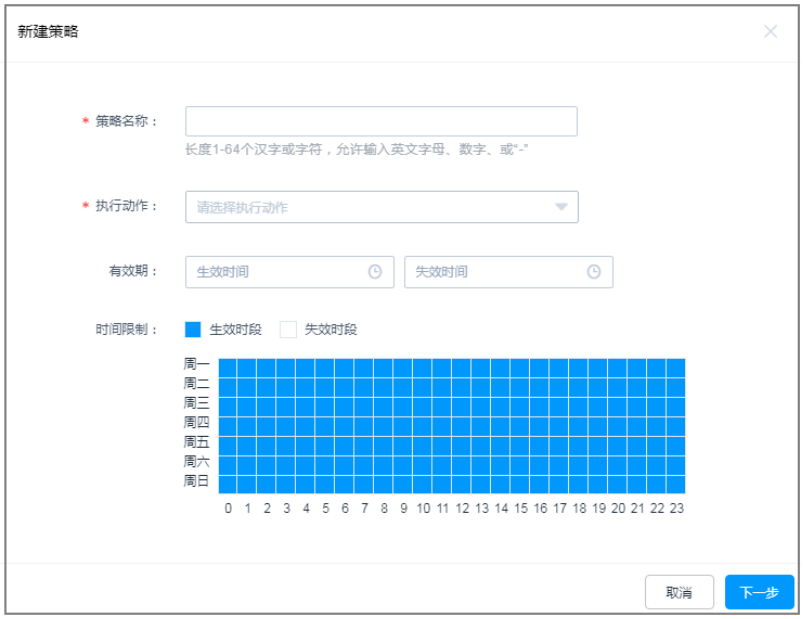


表8-2 策略基本信息参数说明

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 8.2.4 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 8.2.3 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。

8.2.2 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 登录云堡垒机系统。

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

8.2.3 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 登录云堡垒机系统。

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。
   目前系统预置了“Linux 系统”和“网络设备”常见命令和参数。
3. 单击“确定”，命令添加完成。

----结束

查询和修改命令集

步骤 1 登录云堡垒机系统。

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 登录云堡垒机系统。

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

8.2.4 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。

8.3 数据库控制策略

8.3.1 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**专业版**云堡垒机支持数据库运维操作审计。
- 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 登录云堡垒机系统。

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8-3 策略基本信息参数说明

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 8.3.3 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。

8.3.2 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 登录云堡垒机系统。

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

8.3.3 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。

云堡垒机预置 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、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 登录云堡垒机系统。

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。
   - 目前仅支持选择 MySQL、Oracle、Postgresql、Gaussdb 两种数据库协议类型，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8-4 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 登录云堡垒机系统。

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 登录云堡垒机系统。

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

8.4 改密策略

8.4.1 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。
- 关联 Windows 10 资源账户前，需先参照配置 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。

新建改密策略

步骤 1 登录云堡垒机系统。

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8-5 改密策略参数说明

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。
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，需输入改密周期。 • 单位为天。 • 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。 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。

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，可以批量导出主机资源信息，获取新的资源账户密码。

----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。

8.4.2 查询和修改改密策略

若改密策略有变更，例如需改密方式有变化等。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 登录云堡垒机系统。

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

8.4.3 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 登录云堡垒机系统。

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8-5 查看改密日志详情

----结束

下载改密日志

步骤 1 登录云堡垒机系统。

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 登录云堡垒机系统。

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

8.5 账户同步策略

8.5.1 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**云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 登录云堡垒机系统。

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8-6 新建账户同步策略

步骤 4 配置策略基本信息。

表8-6 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。

参数	说明
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。
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。

8.5.2 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 登录云堡垒机系统。

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

8.5.3 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 登录云堡垒机系统。

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。

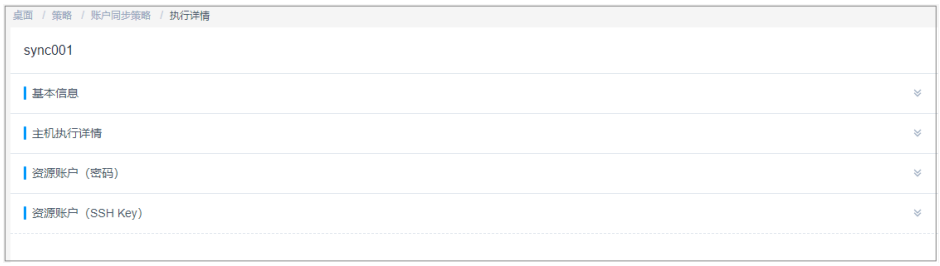
步骤 3 查询执行日志。

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8-7 查看日志基本信息



----结束

下载执行日志

步骤 1 登录云堡垒机系统。

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 登录云堡垒机系统。

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 系统工单

9.1 工单配置管理

9.1.1 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。

本小节主要介绍工单模式的配置指导。

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 登录云堡垒机系统。

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9-1 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。 • 默认为本部门。 • 本部门：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。 • 默认为手动提交。 • 手动提交：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。

步骤 4 单击“确认”，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 登录云堡垒机系统。

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 ，可在单击“删除”。删除后认证信息不能找回，请谨慎操作。

9.1.2 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 登录云堡垒机系统。

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9-2 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。 • 默认为分级流程方式。 • 分级流程：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。

参数	说明
	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 12.1.5.1 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 12.1.6.2 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

9.2 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。

本小节主要介绍如何创建和管理访问授权工单。

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 登录云堡垒机系统。

步骤 2 选择“工单 > 访问授权工单”，进入访问控制工单列表页面。

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9-3 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。
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

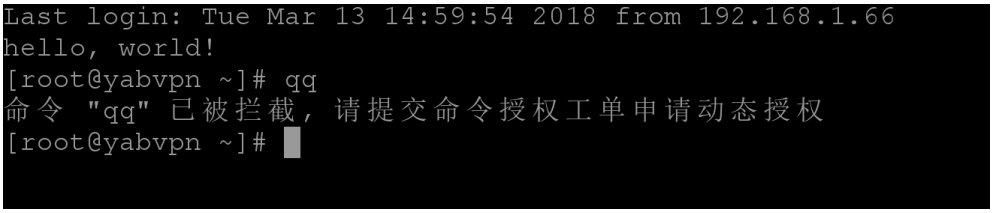
删除后工单信息不能找回，请谨慎操作。

9.3 命令授权工单

云堡垒机支持对 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9-1 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。
- 命令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“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 登录云堡垒机系统。

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9-2 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。

图9-3 已提交工单状态

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。

9.4 数据库授权工单

云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 登录云堡垒机系统。

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9-4 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。

9.5 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

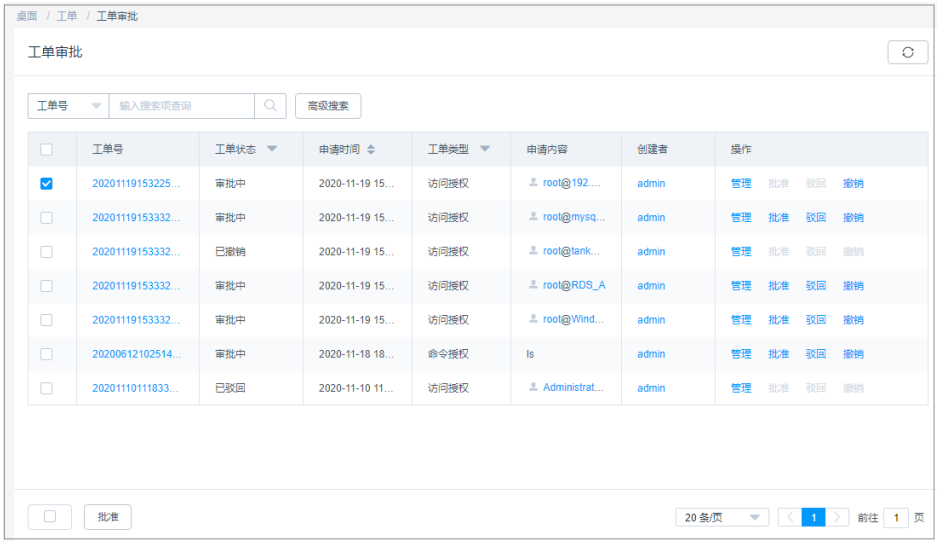
已获取“工单审批”模块管理权限。

操作步骤

步骤 1 登录云堡垒机系统。

步骤 2 选择“工单 > 工单审批”，进入审批工单列表页面。

图9-5 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9-6 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

9.6 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 5.1 部门概述，用户和角色设置请参考 6.1 用户概述，资源设置请参考 7.1 资源概述。
- 工单审批流程设置如表 9-4 所示，具体操作请参考 9.1.2 配置工单审批流程。

表9-4 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 5.1 部门概述，用户和角色设置请参考 6.1 用户概述，资源设置请参考 7.1 资源概述。
- 工单审批流程设置如表 9-5 所示，具体操作请参考 9.1.2 配置工单审批流程。

表9-5 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 5.1 部门概述，用户和角色设置请参考 6.1 用户概述，资源设置请参考 7.1 资源概述。
- 工单审批流程设置如表 9-6 所示，具体操作请参考 9.1.2 配置工单审批流程。

表9-6 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。

10 运维管理

10.1 主机运维

10.1.1 查看主机运维列表并设置资源标签

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。
- “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。

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 查询主机资源。

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”，返回主机运维列表，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”，返回主机运维列表，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”，返回主机运维列表，标签已删除。

----结束

10.1.2 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，被云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，在右侧控制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。

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。
  - 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“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 10.1.8 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。
- 拥有该云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，发送给拥有云堡垒机账户权限的用户，登录云堡垒机，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。

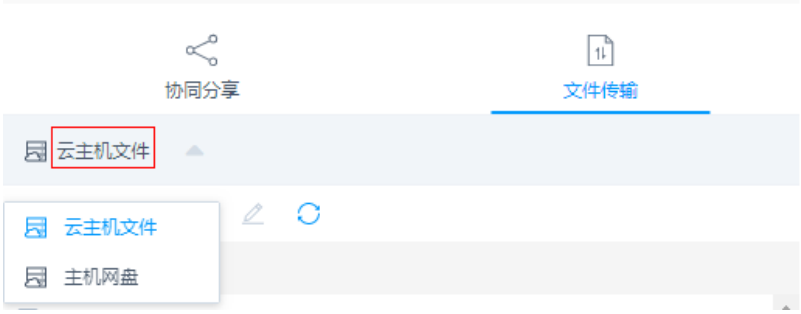
表10-1 会话操作参数说明

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 10.1.7 文件传输。

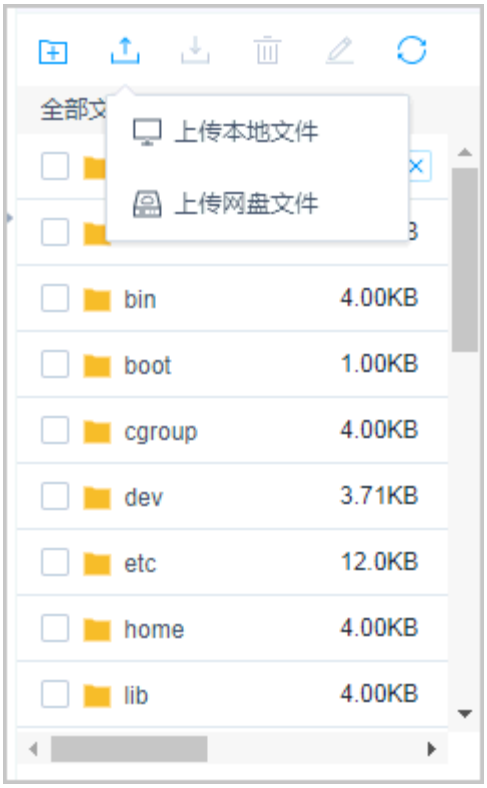
1. 单击“文件传输”，展开文件传输界面。
2. 默认为“云主机文件”，单击“云主机文件”可切换目标地址到“主机网盘”。

图10-1 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10-2 上传文件



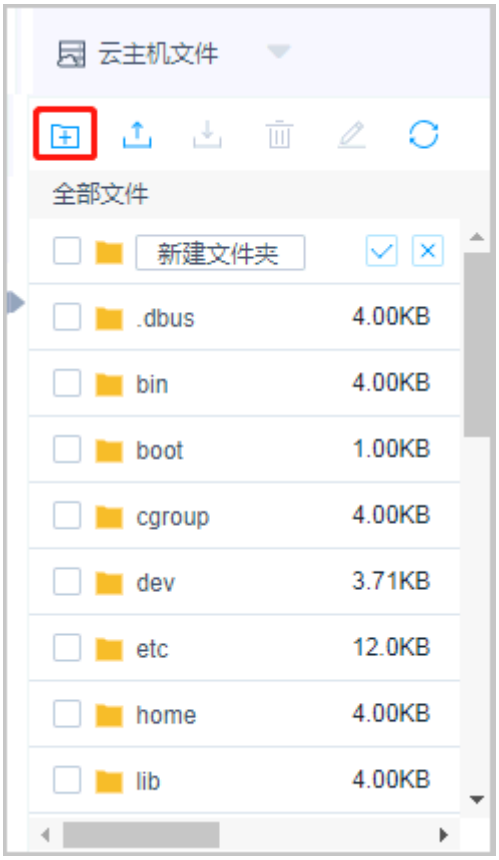
说明

- “主机网盘”属于云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10-3 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10-2 Linux 运维操作说明

参数	说明
中文编码	字符协议支持多种中文编码。
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。
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。

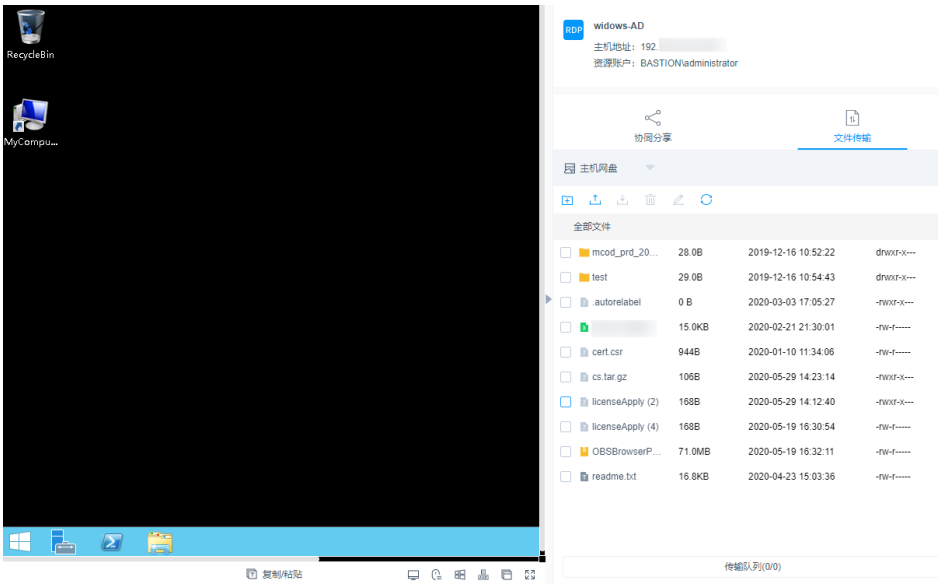
RDP/VNC 协议类型主机会话

表10-3 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	可复制当前会话窗口。

参数	说明
口	
全屏	可开启窗口全屏。

图10-4 RDP 主机会话窗口



10.1.3 通过 SSH 客户端登录资源进行运维

通过 SSH 客户端登录云堡垒机纳管资源，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。

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。

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。

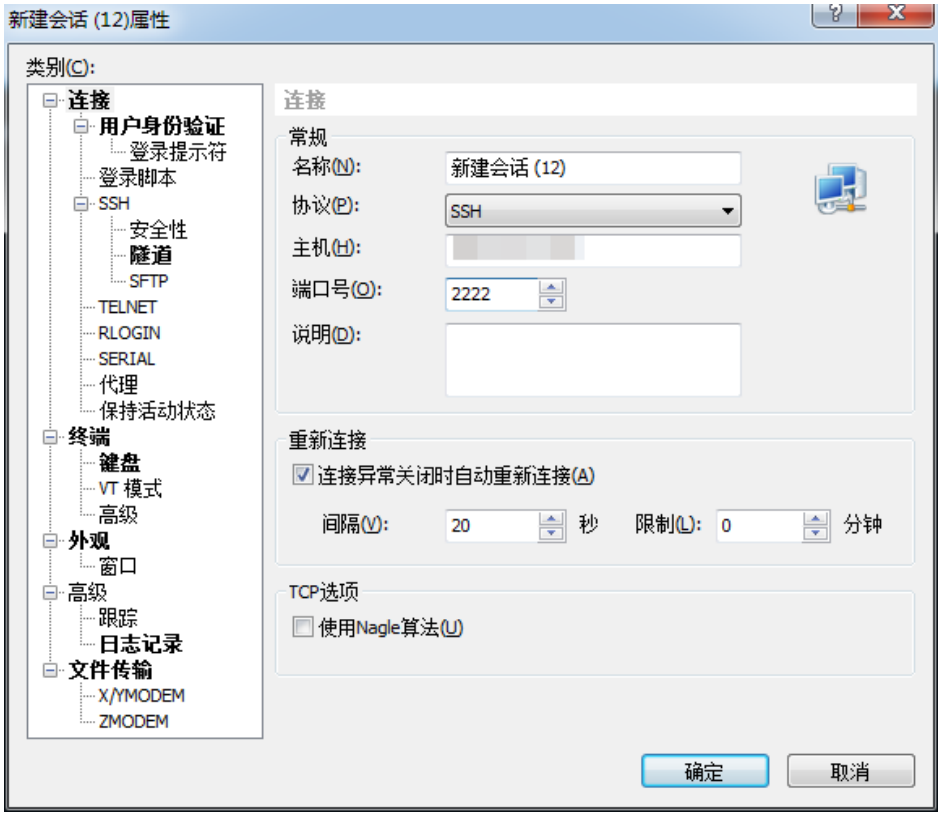
操作步骤

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。

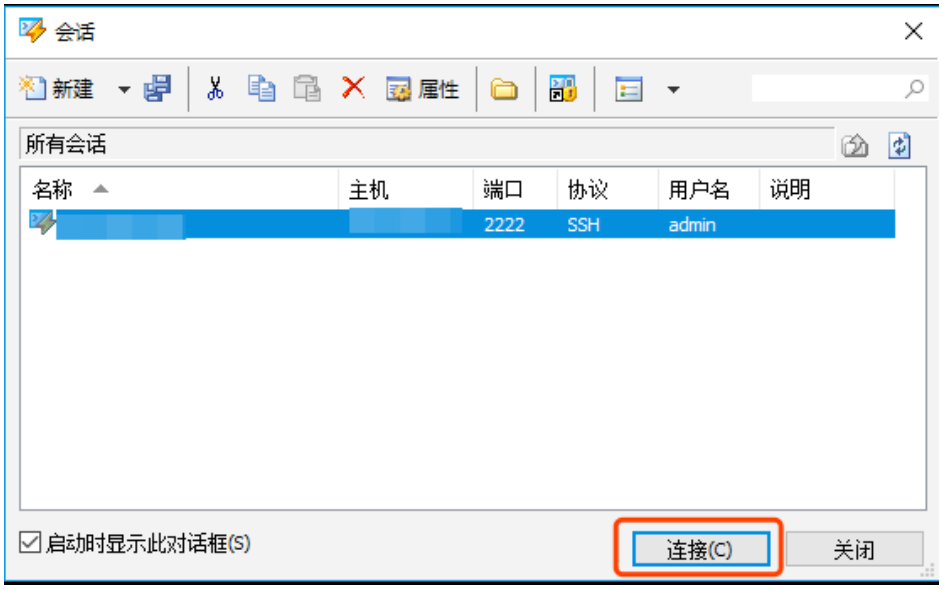
- 方式一
  a. 选择协议类型 SSH，输入云堡垒机实例弹性 IP 地址，端口号配置为 2222，单击“确认”。

图10-5 配置会话属性



b. 连接到会话，输入云堡垒机用户名，单击“连接”。

图10-6 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 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 地址指云堡垒机的 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 云堡垒机用户身份验证。

- 选择密码登录，输入云堡垒机用户密码，单击“确定”。
- 选择公钥登录，在“浏览”中选择用户密钥，输入密码，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。

图10-7 云堡垒机用户身份验证

步骤 4 登录到云堡垒机系统。

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 3.4 配置多因子认证。

- 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 批量导入云堡垒机资源账户。

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“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

10.1.4 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云堡垒机纳管资源，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，被云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

仅 FTP、SFTP、SCP 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：

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
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

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 12.1.4.1 配置系统运维端口。

操作步骤

步骤 1 获取登录信息。

1. 登录云堡垒机系统
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10-4 登录参数说明

参数	说明
登录 IP	配置信息的服务器地址，即云堡垒机登录 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

10.1.5 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。

说明

SSO 单点登录工具客户端目前有四种选择:

- Mysql cmd
- Mysql Adminstrator
- Navicat
- DBeaver（堡垒机 V3.3.48.0 及以上版本支持）

约束限制

- 仅**专业版**实例支持数据库运维操作审计。
- 仅支持 MySQL、SQL Server、Oracle、DB2、PostgreSQL、GaussDB 类型数据库的运维管理。
- 仅支持通过 SsoDBSettings 单点登录工具调用客户端。
- 仅支持调用部分数据库客户端，详情请参见下表。

表10-5 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、	Navicat 11、12、15、16

数据库类型	版本	支持调用客户端
	8.0	MySQL Administrator 1.2.17 MySQL CMD
Microsoft SQL Server	2014、2016、2017、2019、2022	Navicat 11、12、15、16 SSMS 17.6
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
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

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。

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 选择数据库协议类型的主机，单击“登录”，弹出客户端工具选择窗口。

步骤 4 选择本地已安装客户端工具，单击“确定”。

自动调用本地数据库客户端工具。

步骤 5 登录数据库资源进行操作。

----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。

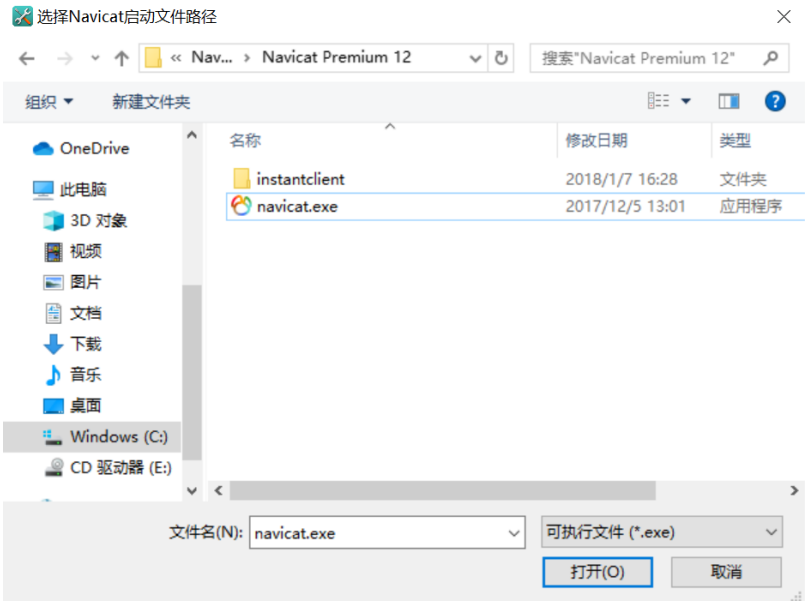
步骤 1 打开本地 SsoDBSettings 单点登录工具。

图10-8 单点登录工具界面

步骤 2 在“Navicat 路径”栏后，单击路径配置。

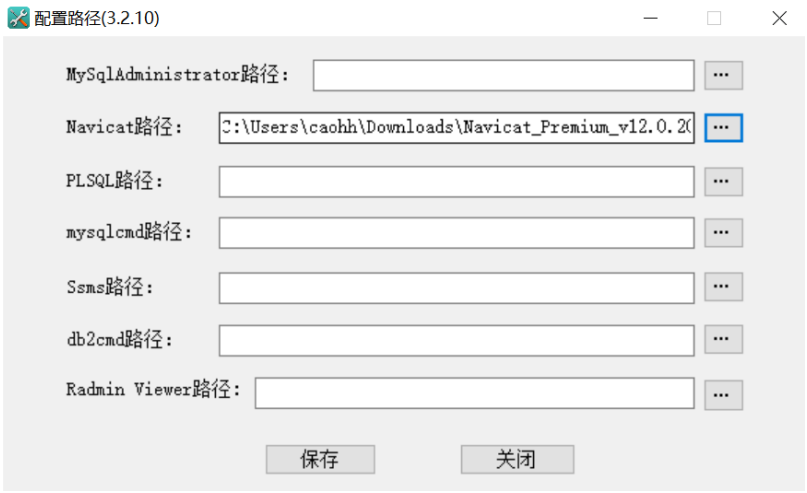
步骤 3 根据本地 Navicat 客户端安装的绝对路径，选中 Navicat 工具的 exe 文件后，单击“打开”。

图10-9 查找本地工具绝对路径



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。

图10-10 确认配置路径



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

----结束

10.1.6 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，被云堡垒机记录并生成审计数据。

本小节主要介绍如何通过 Web 浏览器批量登录主机。

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。

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。

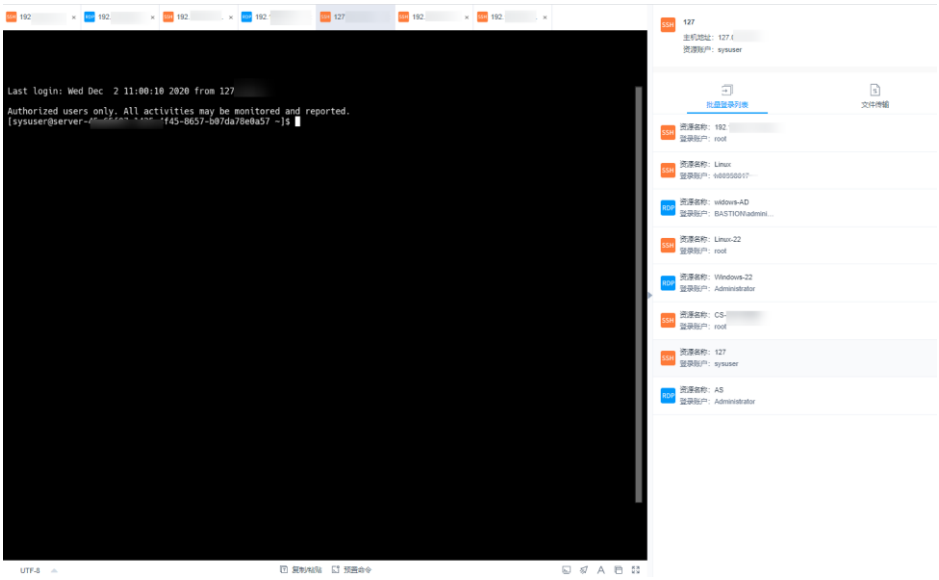
操作步骤

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 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10-11 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 10.1.7 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 10.1.2 通过 Web 浏览器登录资源进行运维。

----结束

10.1.7 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 10.1.4 通过 FTP/SFTP 客户端登录文件传输类资源。

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。

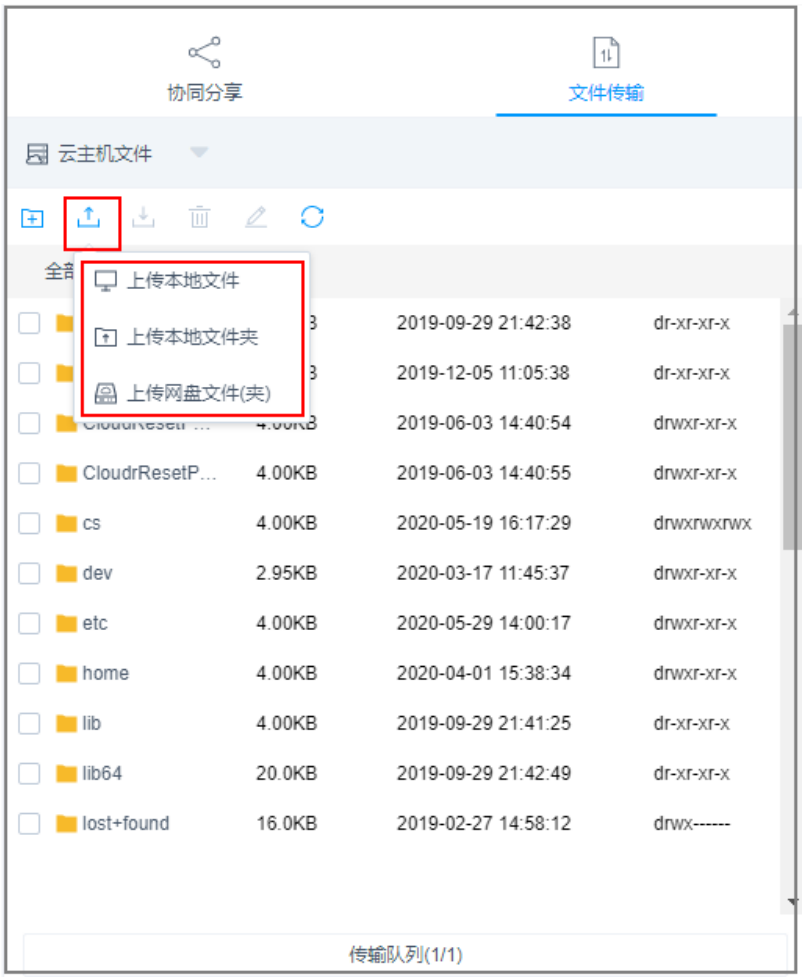
步骤 3 单击“登录”，跳转到 Linux 主机资源运维界面。

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）。

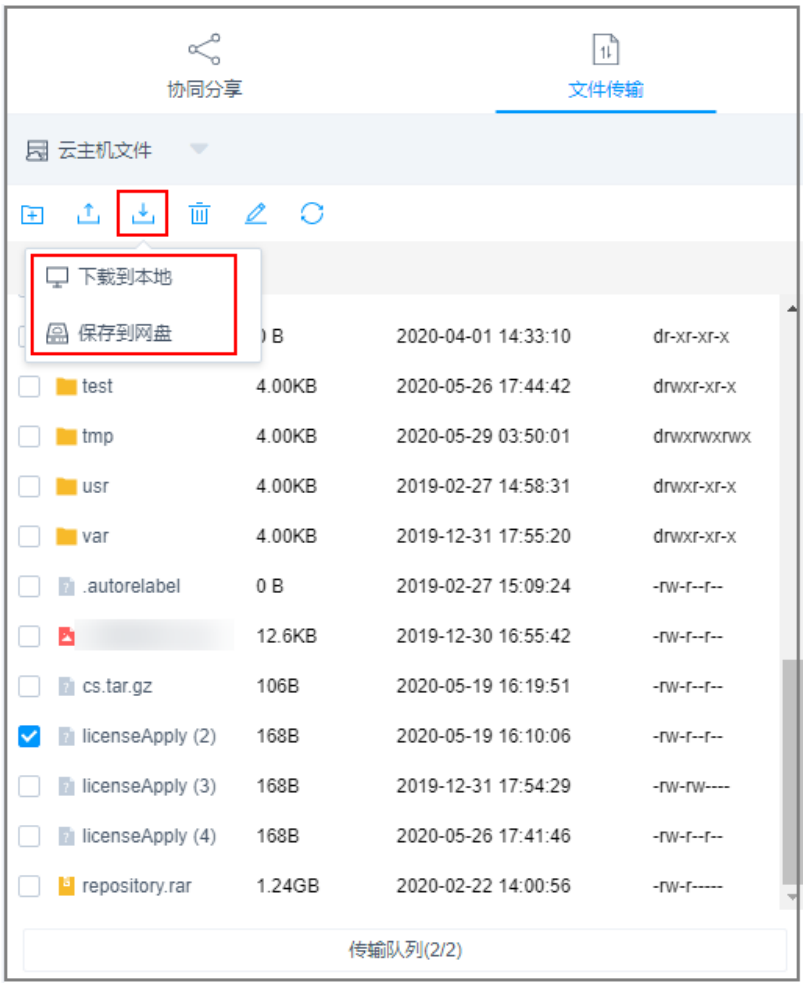
图10-12 上传文件到 Linux 主机



步骤 6 下载 Linux 主机中文件。

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

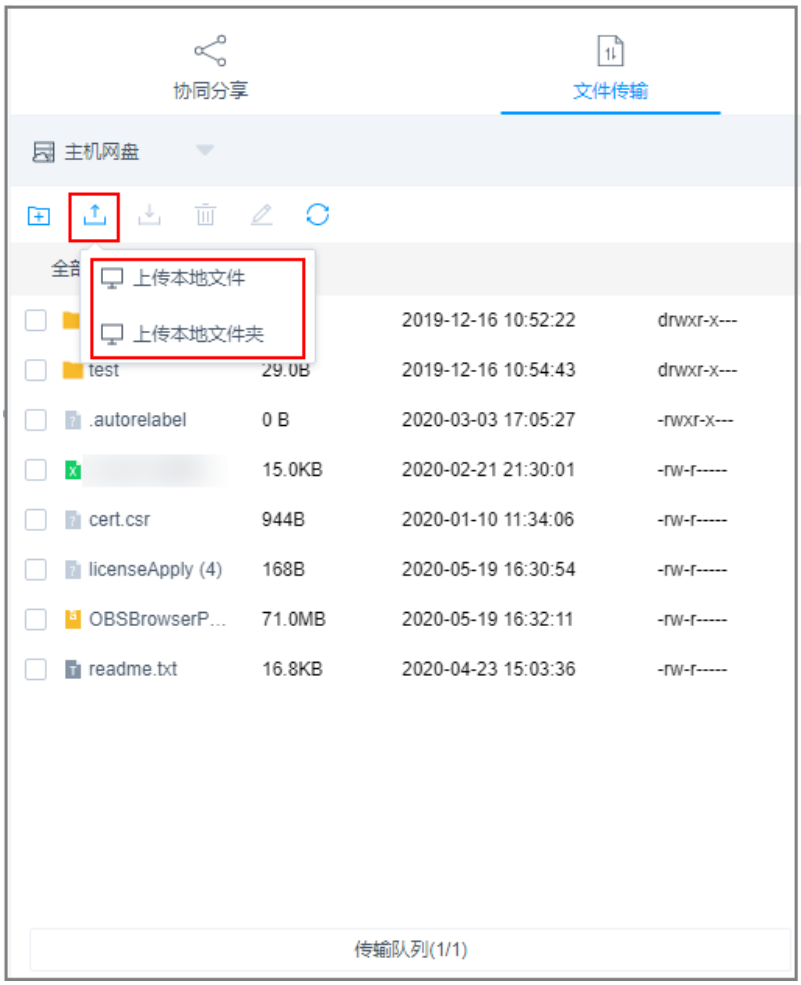
图10-13 下载 Linux 主机中文件



步骤 7 上传文件到个人网盘。

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

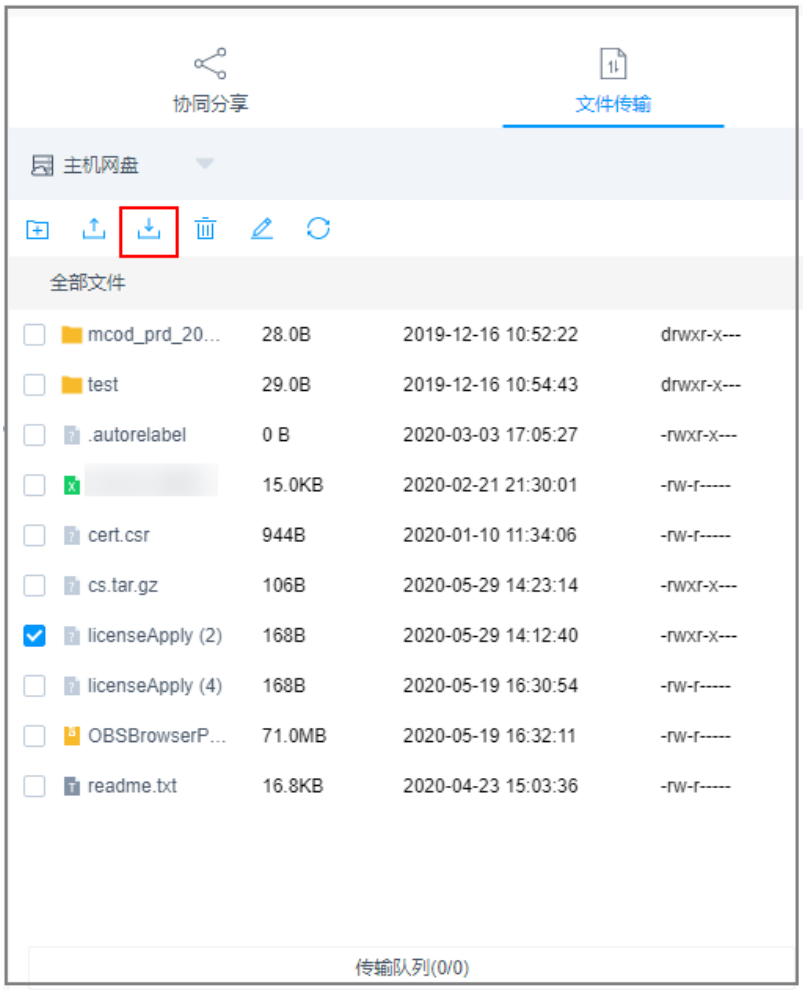
图10-14 上传文件到个人网盘



步骤 8 下载个人网盘中文件。

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

图10-15 下载个人网盘中文件



----结束

Windows 主机中文件的上传/下载

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

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

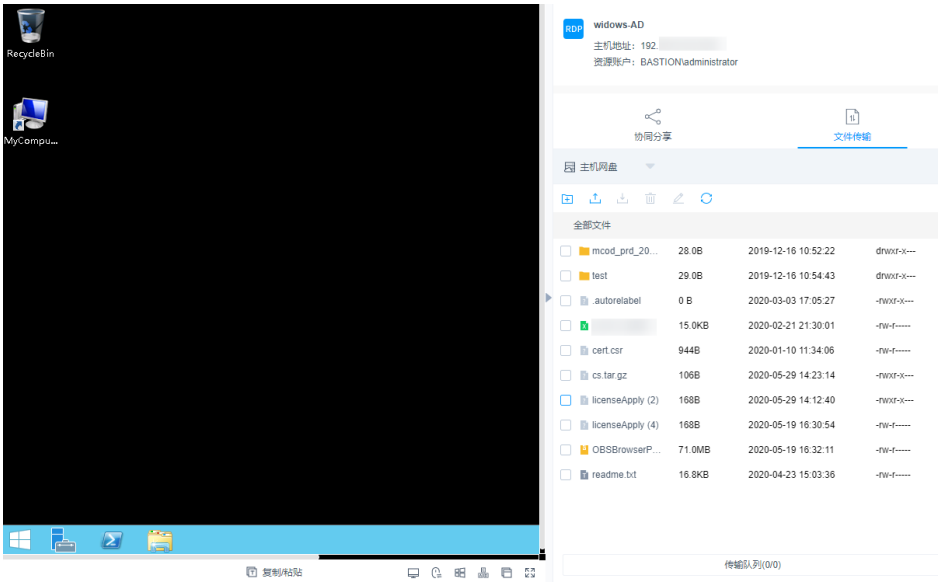
步骤 1 登录云堡垒机系统。

步骤 2 选择“运维 > 主机运维”，选择目标 Windows 主机资源。

步骤 3 单击“登录”，跳转到 Windows 主机资源运维界面。

步骤 4 单击“文件传输”，默认进入个人网盘文件列表。

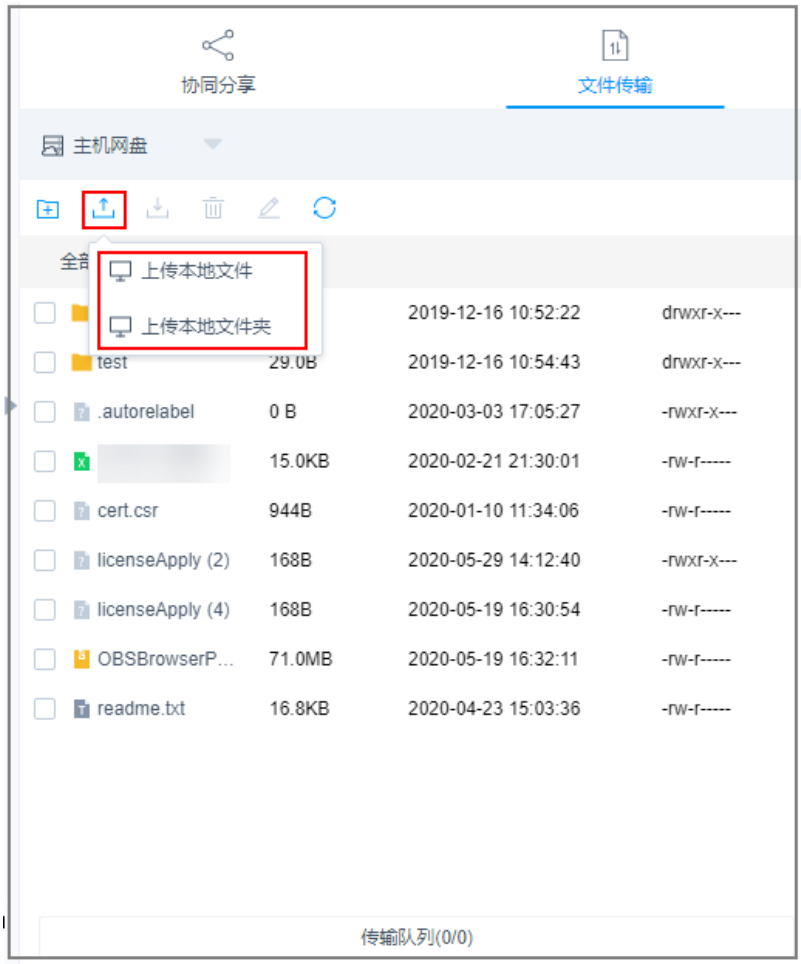
图10-16 Windows 主机文件传输



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10-17 上传文件到个人网盘



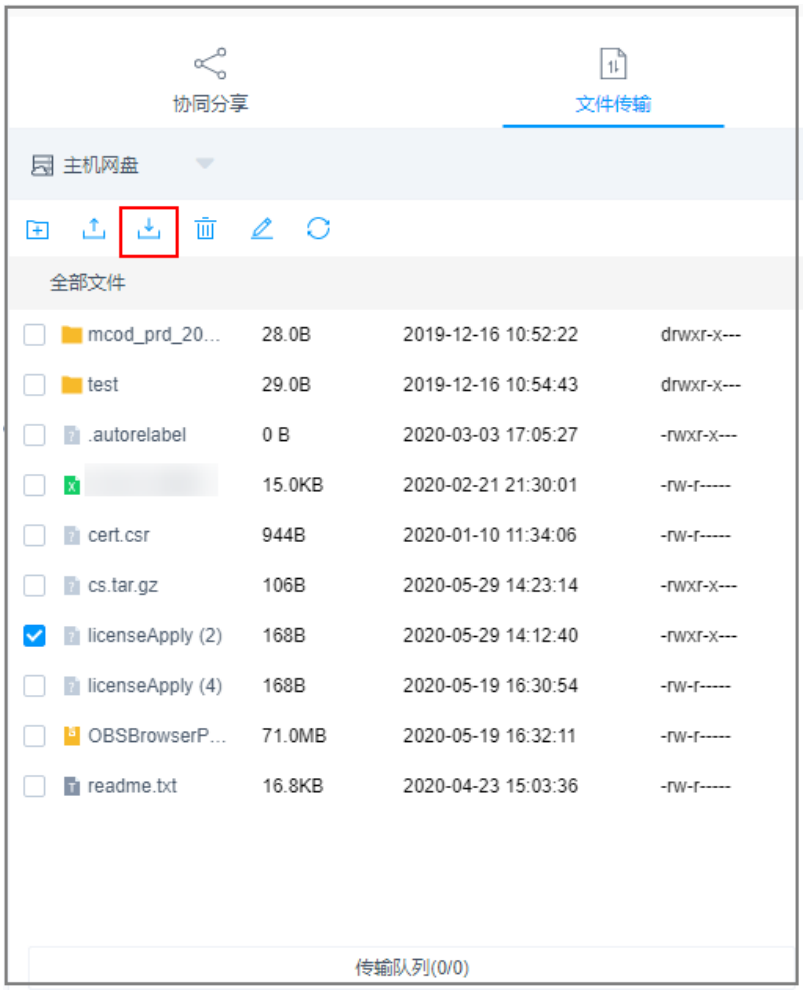
步骤 6 下载 Windows 主机中文件。

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10-18 下载个人网盘中文件



----结束

10.1.8 协同分享

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。

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

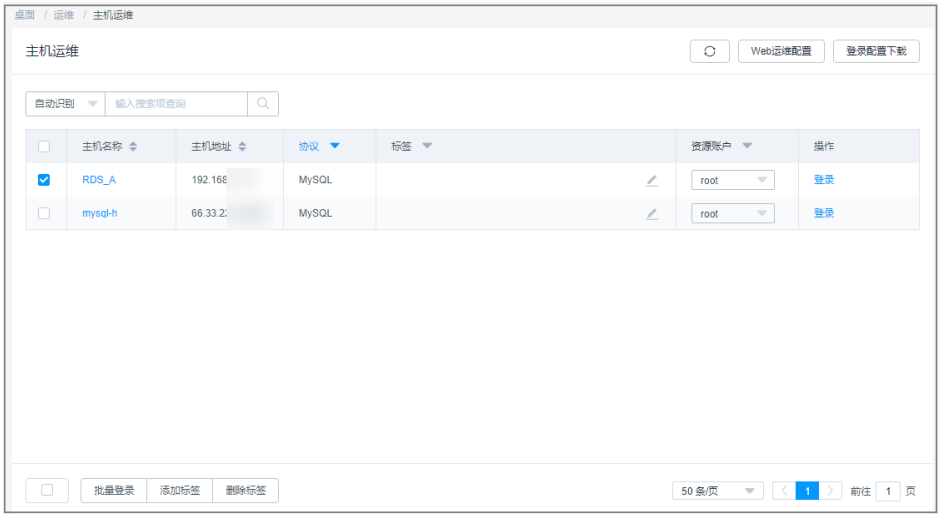
- 已获取主机资源运维的权限。
- 已通过 Web 浏览器正常登录。

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。

图10-19 主机运维列表



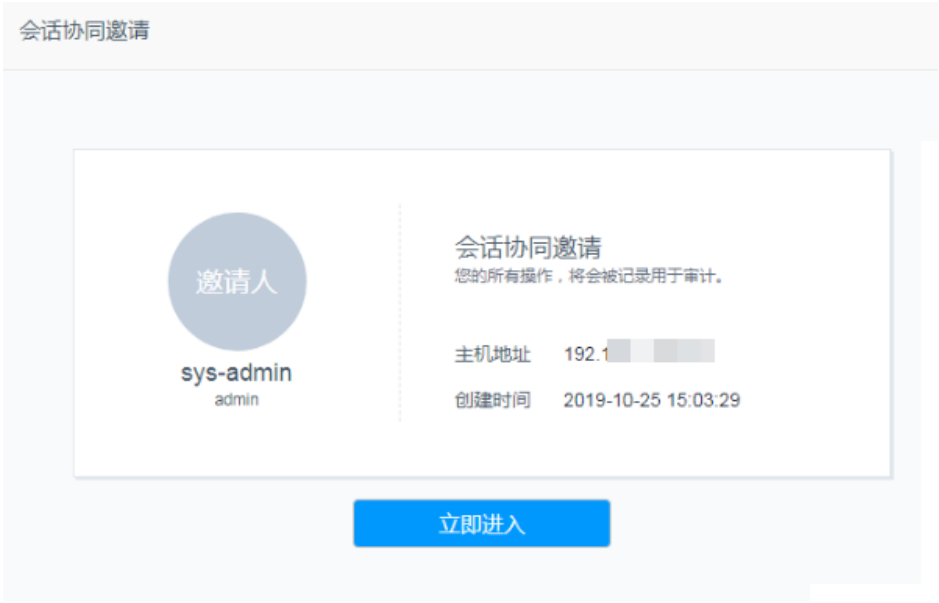
步骤 3 选择待运维主机资源，单击“登录”，登录会话进行操作。

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。

图10-20 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

10.1.9 开启 RDP 强制登录

当 Windows 远程桌面连接数超过最大限值时，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。

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 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值，会挤掉已登录用户，强制登录。

----结束

10.2 应用运维

10.2.1 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 登录云堡垒机系统

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

10.2.2 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，被云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。

约束限制

- 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。
- 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。
  - 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 登录云堡垒机系统。

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10-6 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。
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。

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 10.1.8 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”，弹出邀请链接窗口。

图10-21 邀请协同会话

说明

此链接可复制发送给多人。

3. 复制链接，发送给拥有云堡垒机账户权限的用户。
4. 受邀用户登录云堡垒机，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10-7 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。
退出会话	退出此会话。

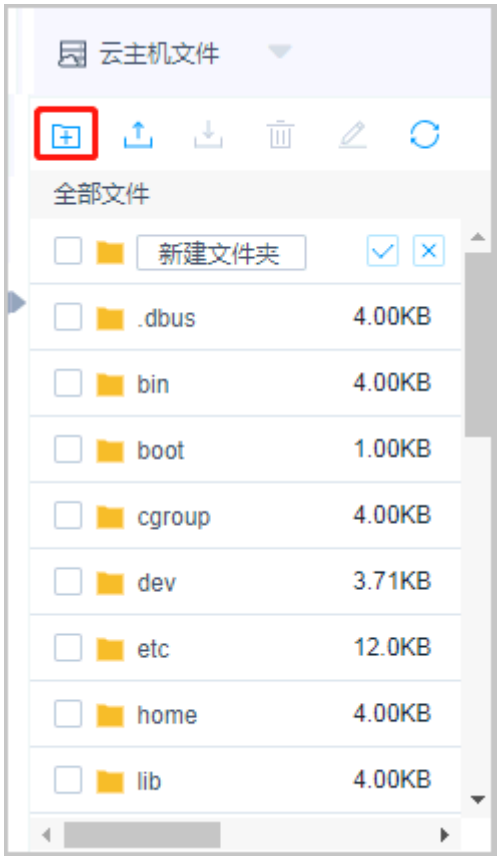
步骤 5 通过文件传输，可对主机网盘中文件进行上传或下载，详细说明请参见 10.1.7 文件传输。

单击“文件传输”，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. 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10-22 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

10.3 脚本管理

10.3.1 新建脚本

云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。云堡垒机支持在线编辑脚本和以文件方式导入脚本。

本小节主要介绍如何新建脚本。

说明

云堡垒机已内置 HSS-Agent 自动下载及安装脚本。

约束限制

- 仅**专业版**云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 登录云堡垒机系统。

步骤 2 选择“运维 > 脚本管理 ”，进入脚本列表页面。

步骤 3 单击“新建”，弹出“新建脚本”窗口。

步骤 4 配置脚本基本信息。

表10-8 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，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。

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 10.3.2 查看和修改脚本信息。

10.3.2 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 10.3.3 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 登录云堡垒机系统。

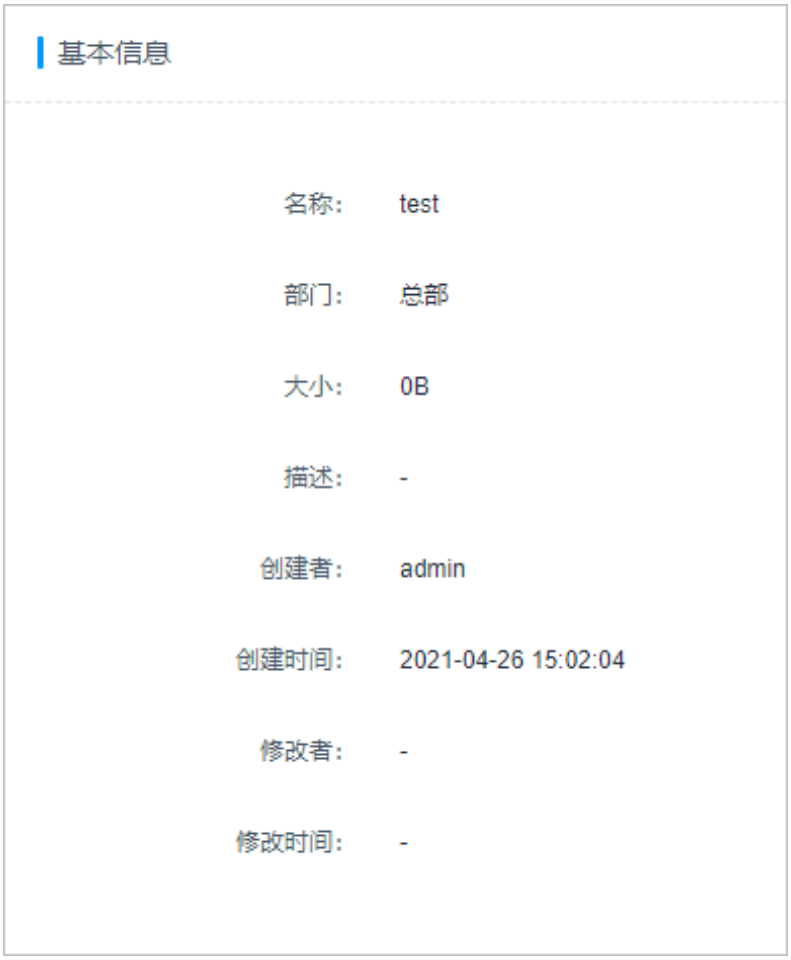
步骤 2 选择“运维 > 脚本管理 ”，进入脚本列表页面。

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10-23 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

10.3.3 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 登录云堡垒机系统。

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

10.3.4 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 登录云堡垒机系统。

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

10.4 快速运维

10.4.1 管理命令任务

云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**云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 登录云堡垒机系统。

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10-24 命令控制台

步骤 3 配置快速命令运维信息。

表10-9 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	• “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）用户对资源账户执行任务权限不够时，需勾选上“提权执

参数	说明
	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 10.4.4 管理快速任务执行日志。

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，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10-25 命令任务结果

----结束

10.4.2 管理脚本任务

云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**云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 登录云堡垒机系统。

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10-26 脚本控制台

步骤 3 配置快速脚本运维信息。

表10-10 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。
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。

参数	说明
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 10.4.4 管理快速任务执行日志。

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，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

10.4.3 管理文件传输任务

云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**云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 登录云堡垒机系统。

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10-27 文件传输控制台

步骤 3 配置快速文件传输信息。

表10-11 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 10.4.4 管理快速任务执行日志。

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，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10-28 文件传输任务结果

----结束

10.4.4 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 登录云堡垒机系统。

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。

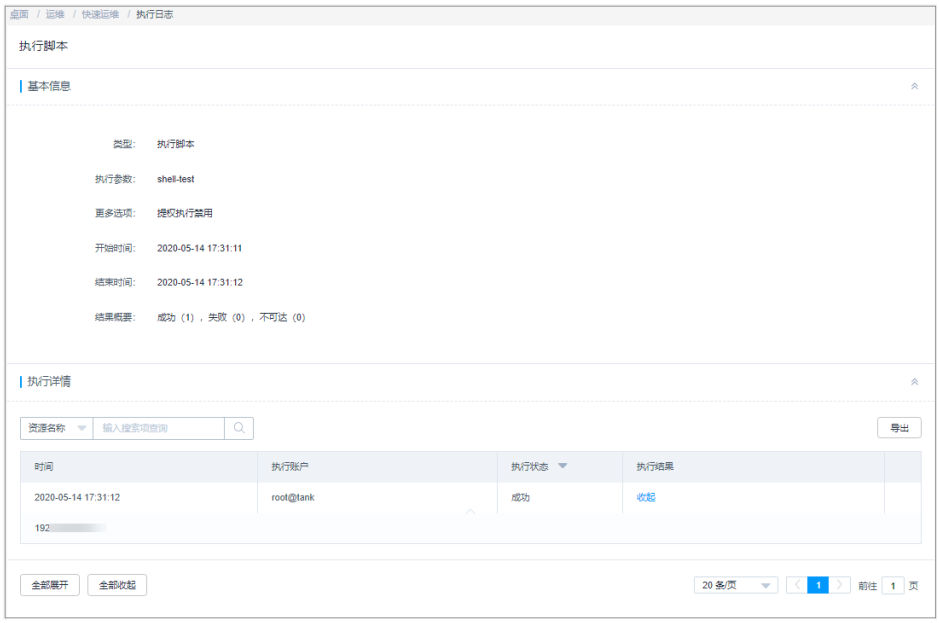
步骤 3 查询日志。

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10-29 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

10.5 运维任务

10.5.1 新建运维任务

云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**云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 登录云堡垒机系统。

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10-12 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。

10.5.2 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 登录云堡垒机系统。

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

10.5.3 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 登录云堡垒机系统。

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 登录云堡垒机系统。

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 登录云堡垒机系统。

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

11 运维审计

11.1 实时会话

11.1.1 查看实时会话

运维人员通过云堡垒机登录资源后，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。

本小节主要介绍如何查询和查看实时会话。

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 登录云堡垒机系统。

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

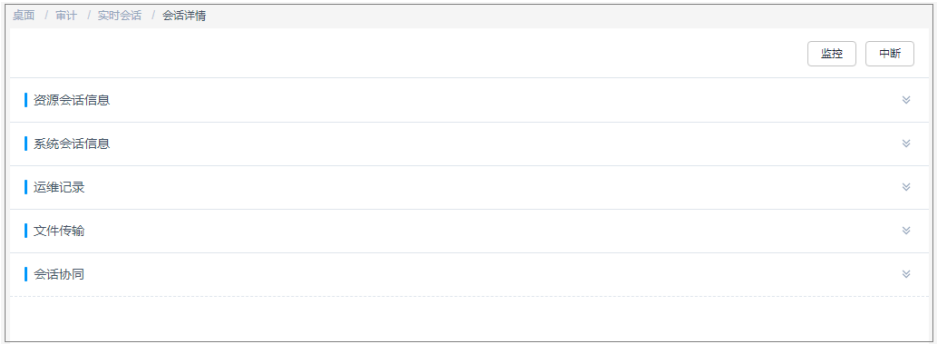
  在搜索框中输入关键字，根据资源名称、资源账户、用户、来源 IP 等快速查询实时会话。

- 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

运维人员通过云堡垒机登录资源后，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。

本小节主要介绍如何通过实时会话监控运维操作。

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 登录云堡垒机系统。

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

运维人员通过云堡垒机登录资源后，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。

本小节主要介绍如何中断实时会话。

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 登录云堡垒机系统。

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

运维人员通过云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。

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 7.5.1 验证资源账户的登录资源数据。
- 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 登录云堡垒机系统。

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

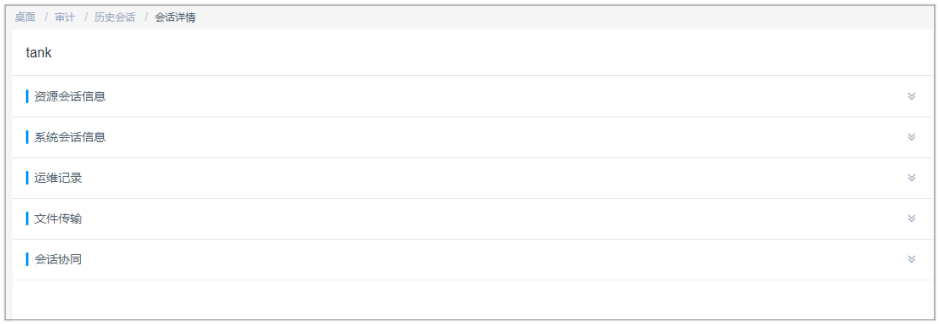
  在搜索框中输入关键字，根据资源名称、资源账户、用户、来源 IP 等快速查询历史会话。

- 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

说明

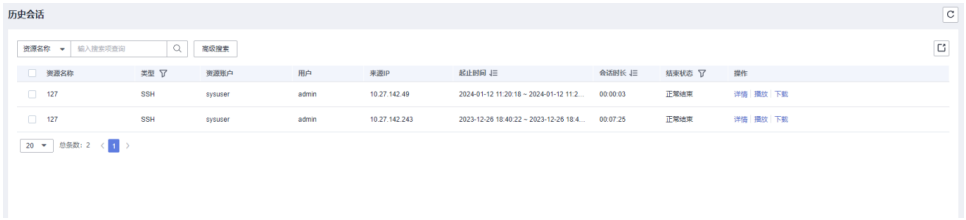
因登出时间和最后操作时间不同，视频文件的总时长与回放可播放时长可能不一致。

- “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 登录云堡垒机系统。

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。

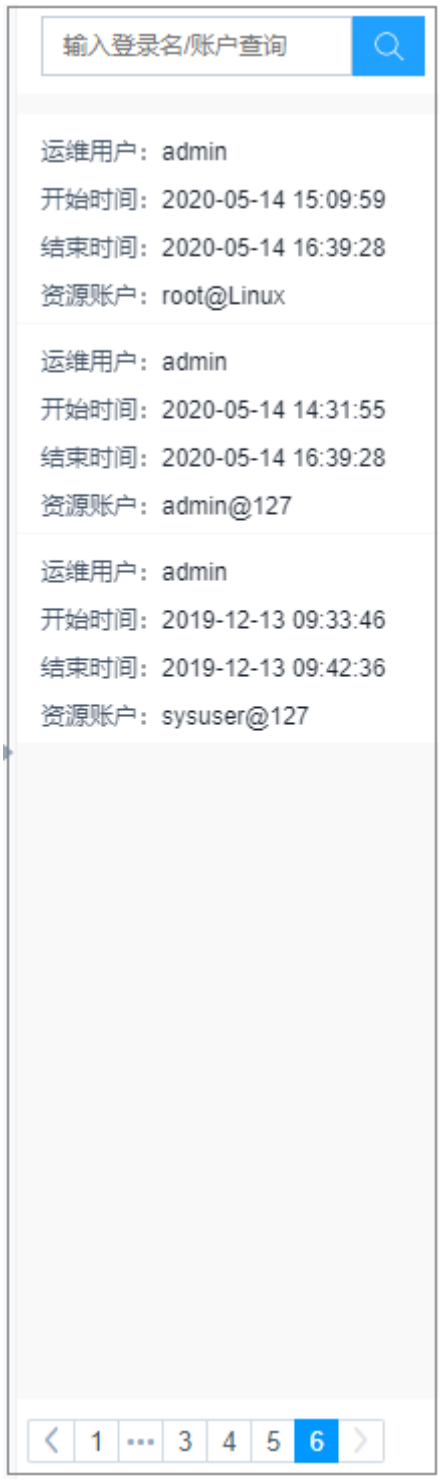
步骤 7 会话截屏。

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

运维人员通过云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。

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 登录云堡垒机系统。

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 单击右上角“导出”，即可立即下载的 CSV 格式的文件到本地。

----结束

11.2.3 管理会话视频

运维人员通过云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。

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

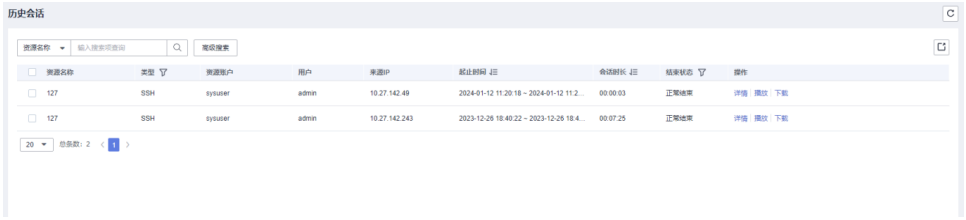
- 已获取“历史会话”模块管理权限。
- 已结束运维会话。

生成会话视频

步骤 1 登录云堡垒机系统。

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。
- 会话视频可备份至 OBS 桶，具体操作请参考 12.2.7 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 登录云堡垒机系统。

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 4.5 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

运维人员登录云堡垒机系统，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。

查看系统登录日志

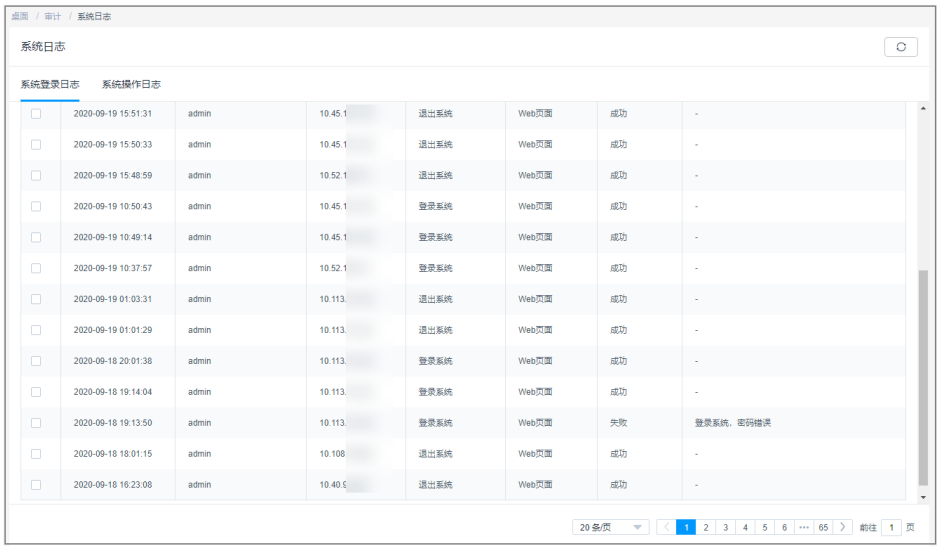
步骤 1 登录云堡垒机系统。

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。

图11-9 系统登录日志



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 登录云堡垒机系统。

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。

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

运维人员登录云堡垒机系统，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。

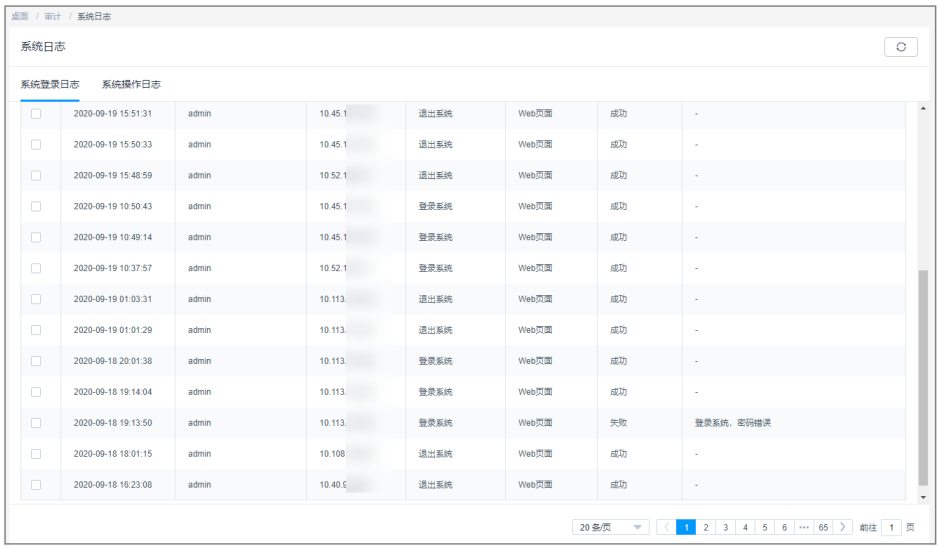
导出系统登录日志

步骤 1 登录云堡垒机系统。

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 单击右上角“导出”，即可立即下载 CSV 格式的文件到本地。

----结束

导出系统操作日志

步骤 1 登录云堡垒机系统。

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。

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 单击右上角“导出”，即可立即下载的 CSV 格式的文件到本地。

----结束

11.4 运维报表

11.4.1 查看运维报表

运维用户通过云堡垒机登录资源，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

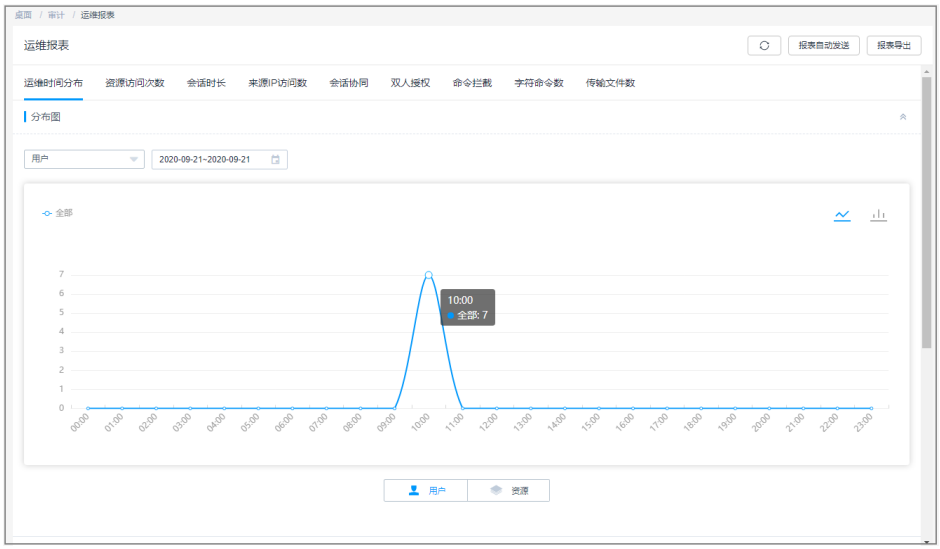
已获取“运维报表”模块管理权限。

操作步骤

步骤 1 登录云堡垒机系统。

步骤 2 选择“审计 > 运维报表”，进入系统报表查看页面。

图11-11 运维报表



步骤 3 单击各运维统计数据页签，查看各运维统计数及趋势如何详细信息。

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。

图11-12 运维时间分布图

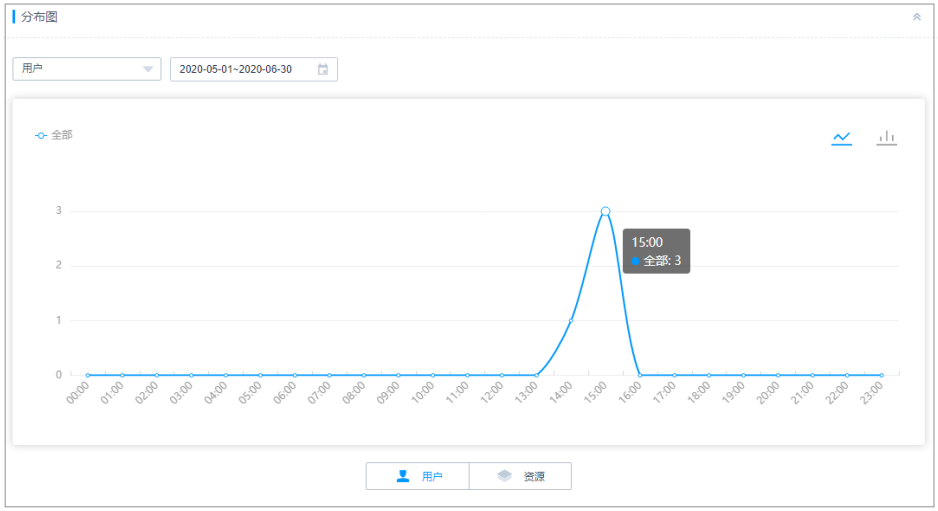


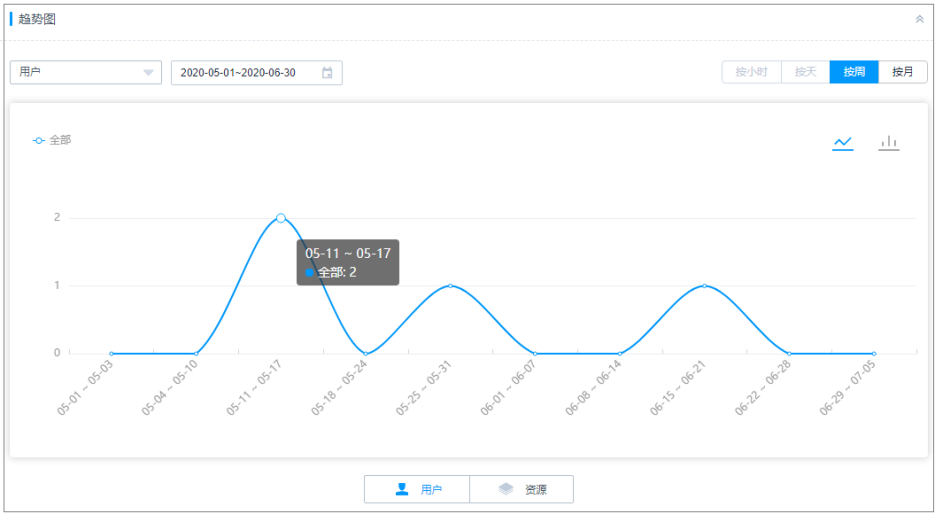
图11-13 运维时间分布详细数据

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。

图11-14 资源访问次数趋势图



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

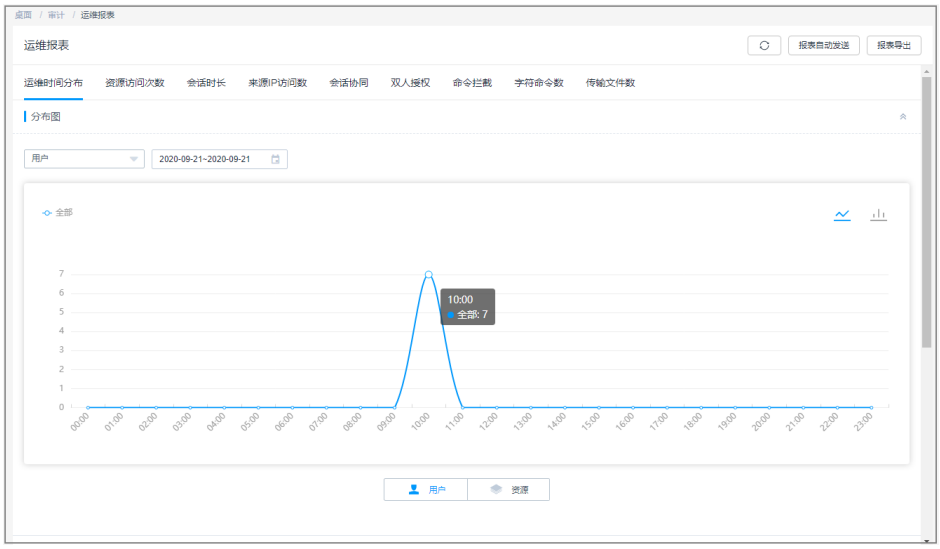
- 已获取“运维报表”模块管理权限。
- 已完成 12.1.5.1 配置邮件外发配置。

手动导出

步骤 1 登录云堡垒机系统。

步骤 2 选择“审计 > 运维报表”，进入系统报表查看页面。

图11-15 运维报表



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。

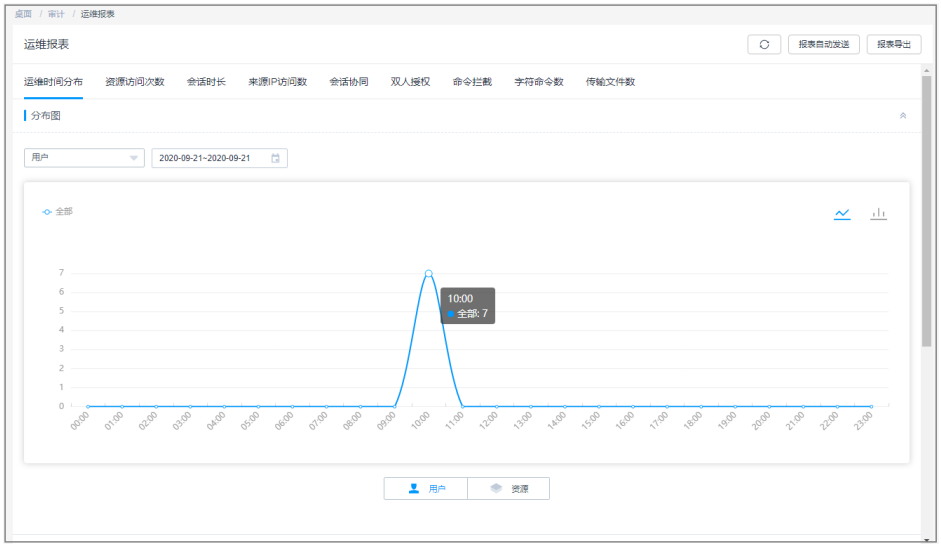
----结束

自动发送

步骤 1 登录云堡垒机系统。

步骤 2 选择“审计 > 运维报表”，进入系统报表查看页面。

图11-16 运维报表



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。
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。

参数	说明
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

运维用户登录云堡垒机系统，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 登录云堡垒机系统。

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如何详细信息。

----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。

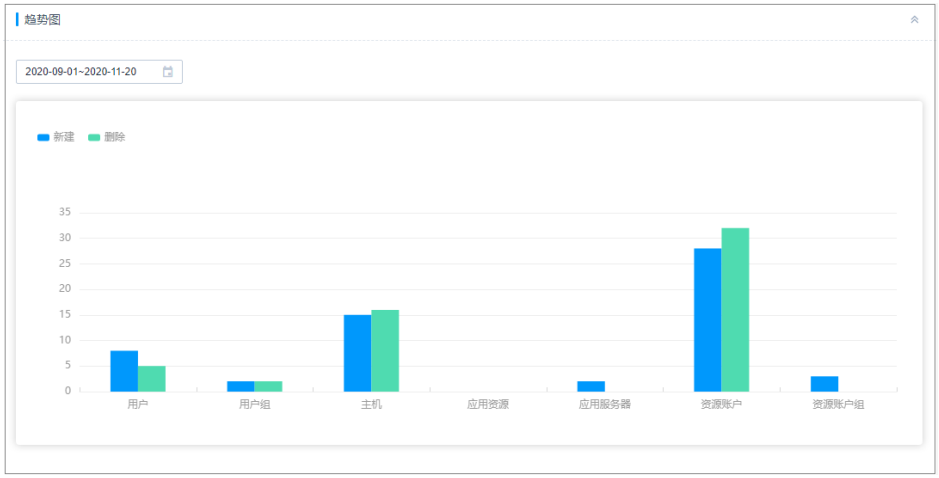
在“详细数据”区域，可查看操作时间、操作用户登录名、来源 IP、操作、操作结果等信息。

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11-17 用户与资源操作趋势图



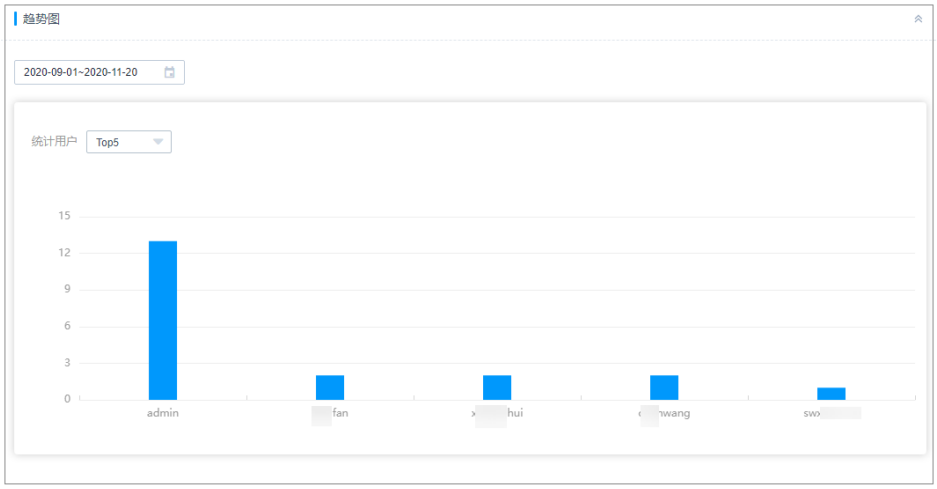
用户源 IP 数

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11-18 用户源 IP 数趋势图



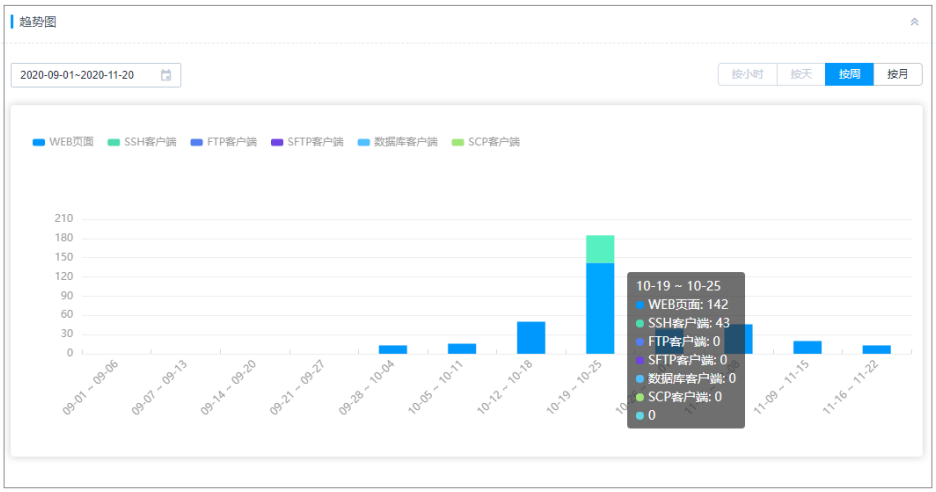
用户登录方式

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11-19 用户登录方式趋势图



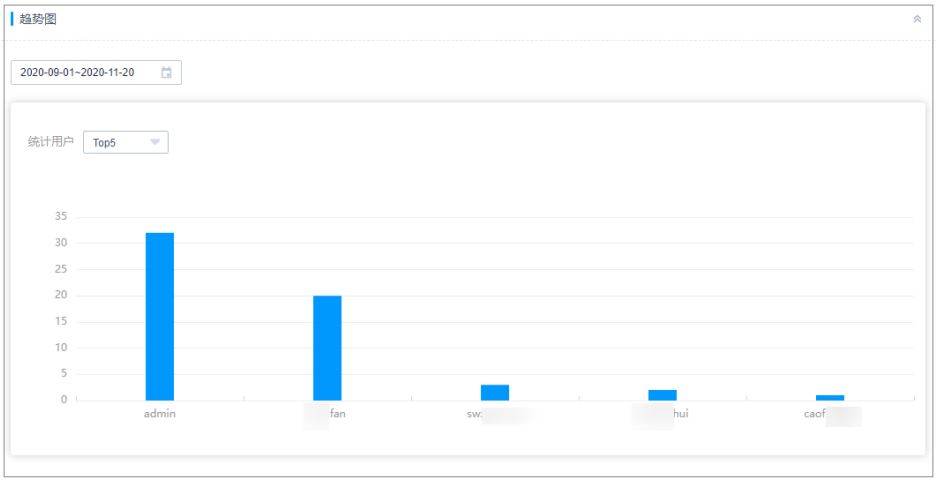
异常登录

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11-20 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 登录云堡垒机系统。

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 登录云堡垒机系统。

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 系统管理

12.1 系统配置

12.1.1 系统配置概述

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 3.5 登录安全管理。
- 网络配置，详情请参见 12.1.2 网络配置。
- 端口配置，详情请参见 12.1.4 端口配置。
- 外发配置，详情请参见 12.1.5 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 6.5 远程认证管理。
- 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 9.1 工单配置管理。
- 告警配置，详情请参见 12.1.6 告警配置。
- 系统风格，详情请参见 12.1.7 系统风格。

12.1.2 网络配置

12.1.2.1 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 登录云堡垒机系统。

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，可以查看当前云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，可以查看当前云堡垒机系统的首选 DNS 和备用 DNS 地址。

默认不支持修改系统 DNS 地址。

图12-1 系统 DNS 地址

步骤 5 在“默认网关”区域，可查看当前云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12-2 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

12.1.2.2 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。

本小节主要介绍如何为系统添加静态路由。

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 登录云堡垒机系统。

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。

12.1.3 HA 配置

12.1.3.1 启用 HA

云堡垒机支持双机 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。

本小节主要介绍如何启用双机 HA 备份。

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。
- 已准备两台云堡垒机，且两台云堡垒机授权同一个许可文件。

操作步骤

步骤 1 登录云堡垒机系统。

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。

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。

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12-1 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云堡垒机。
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，输入作为备节点的云堡垒机 IP 地址。
主节点 IP 地址	配置备节点 HA 参数时，输入作为主节点的云堡垒机 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 地址即为两个云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云堡垒机上，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，重启两台云堡垒机系统，重启完成后双机 HA 备状态即为关闭状态。

12.1.4 端口配置

12.1.4.1 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 客户端登录云堡垒机的端口，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 登录云堡垒机系统。

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

12.1.4.2 配置 Web 控制台端口

Web 控制台端口是通过 Web 浏览器登录云堡垒机的访问端口，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 登录云堡垒机系统。

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

12.1.4.3 配置 SSH 控制台端口

SSH 控制台端口是通过 SSH 客户端登录云堡垒机的访问端口，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 登录云堡垒机系统。

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

12.1.5 外发配置

12.1.5.1 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。

本小节主要介绍如何配置系统邮件外发。

前提条件

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 > 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。

分别选择 SMTP 和 Exchange 发送方式，并根据界面提示配置邮件发送方式。

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

12.1.5.2 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 12.1.6 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。
- 若您已购买“消息&短信服务”，请参考自定义消息&短信服务进行短信网关配置。

说明

- “消息&短信服务”不支持推送系统告警。
- “消息&短信服务”失效后，将自动切换为系统“内置”短信网关。

本小节主要介绍如何配置系统短信外发。

前提条件

已获取“系统”模块管理权限。

内置短信网关

步骤 1 登录云堡垒机系统。

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。
- 内置短信网关不支持外发中国大陆以外的手机号码，若有非中国大陆手机号的短信接收需求，请自定义配置海外短信网关。

----结束

自定义通用短信网关

步骤 1 登录云堡垒机系统。

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12-2 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。
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

自定义消息&短信服务

步骤 1 登录云堡垒机系统。

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 单击“确认”，返回外发配置页面，即可查看短信网关信息。

表12-3 云短信网关参数说明

参数	说明
APP_Key	申请短信应用后，输入短信应用的 APP_Key。
APP_Secret	申请短信应用后，输入短信应用的 APP_Secret。
APP 接入地址	申请短信应用后，输入短信应用的 APP 接入地址。
通道号	申请短信签名后，输入短信前面通道号。
模板 ID	申请短信模板后，输入短信模板的 ID。
测试手机号	输入可用手机号码，验证短信内容。

----结束

12.1.6 告警配置

12.1.6.1 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 登录云堡垒机系统。

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。

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

12.1.6.2 配置告警等级

本小节主要介绍如何配置系统各类消息告警等级。

前提条件

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 > 系统配置 > 告警配置”，进入系统告警配置管理页面。

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”，返回告警配置页面，即可查看已配置的告警信息。

----结束

12.1.7 系统风格

12.1.7.1 变更系统风格

本小节主要介绍如何切换系统语言和自定义图标。

前提条件

已获取“系统”模块管理权限。

系统风格

步骤 1 登录云堡垒机系统。

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，重启系统，即可查看自定义的系统图标和公司图标。

----结束

12.2 数据维护

12.2.1 查看系统内存

云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。

本小节主要介绍如何查看系统内存使用状况。

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 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12-3 存储空间概览

----结束

12.2.2 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 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12-4 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

参数	说明
	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

12.2.3 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。

危险

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 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12-5 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。
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。 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。
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。

图12-4 自动删除配置信息

----结束

手动删除

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 在“手动删除”区域，选择一个日期。

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

12.2.4 创建数据本地备份

为加强对系统数据的容灾管理，云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 登录云堡垒机系统。

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12-6 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。

图12-5 本地备份

----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。

12.2.5 配置远程备份至 Syslog 服务器

为加强对系统数据的容灾管理，云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 Syslog 服务器参数，将日志远程备份至 Syslog 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 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 登录云堡垒机系统。

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12-7 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	自定义云堡垒机到 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云堡垒机。
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 • 资源登录日志

参数	说明
	• 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 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。

12.2.6 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，云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 登录云堡垒机系统。

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12-8 配置 FTP 或 SFTP 服务器远程备份

参数	说明

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。
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。 • 只检测云堡垒机到 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。

12.2.7 配置远程备份至 OBS 桶

为加强对系统数据的容灾管理，云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 登录云堡垒机系统。

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12-9 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。

参数	说明
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/.../...
测试连通性	用于测试配置的 OBS 桶的网络是否通畅。 只检测云堡垒机到 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。

12.3 系统维护

12.3.1 查看系统状态

为了确认云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、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 登录云堡垒机系统。

步骤 2 选择“系统 > 系统维护 > 系统状态”，进入系统状态页面。

图12-6 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 登录云堡垒机系统。

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 登录云堡垒机系统。

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

12.3.2 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、更新系统版本，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

步骤 1 登录云堡垒机系统。

步骤 2 选择“系统 > 系统维护 > 系统管理”，进入系统管理页面。

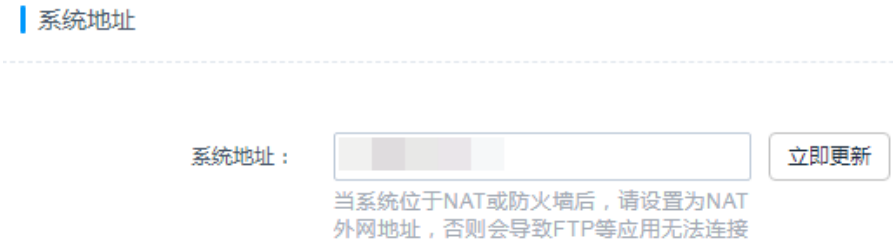
图12-7 系统管理

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12-8 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 登录云堡垒机系统。

步骤 2 选择“系统 > 系统维护 > 系统管理”，进入系统管理页面。

图12-9 系统管理

步骤 3 展开“系统时间”区域，可管理系统时间。

图12-10 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

管理系统工具

步骤 1 登录云堡垒机系统。

步骤 2 选择“系统 > 系统维护 > 系统管理”，进入系统管理页面。

图12-11 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。

图12-12 系统工具

- 重启系统。
  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。
- 关闭系统。
  a. 单击“关机”，弹出关机确认窗口。
  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”，验证通过后即可关闭系统。
- 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。

危险

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

12.3.3 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。

约束限制

- 系统备份文件仅限于本云堡垒机系统使用，不能用于其他云堡垒机系统。
- 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 12.2 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 登录云堡垒机系统。

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 登录云堡垒机系统。

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 登录云堡垒机系统。

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

12.3.4 系统授权许可

本小节主要介绍如何查看系统授权信息。

前提条件

已获取“系统”模块管理权限。

操作步骤

步骤 1 登录云堡垒机系统。

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12-10 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”。
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。

参数	说明
	• 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，对应需调整云堡垒机 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

12.3.5 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云堡垒机系统与主机网络是否可达。

- 对主机地址进行 ping 诊断，判断云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，判断云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，判断云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

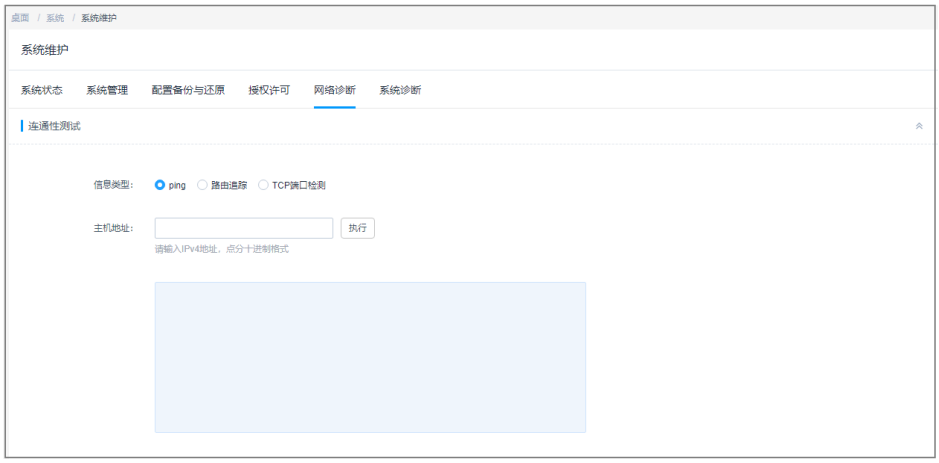
已获取“系统”模块管理权限。

操作步骤

步骤 1 登录云堡垒机系统。

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。

图12-13 网络诊断



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

12.3.6 系统诊断

通过系统诊断可获取当前系统相关信息，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。

本小节主要介绍如何进行系统诊断，获取系统后台信息。

前提条件

已获取“系统”模块管理权限。

操作步骤

步骤 1 登录云堡垒机系统

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12-11 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12-14 系统诊断信息

----结束

12.4 查看系统信息

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 登录云堡垒机系统。

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12-12 关于系统参数说明

参数	说明
产品名称	云堡垒机
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	当前系统版本。
设备系统	当前系统软件版本。
发行日期	当前系统版本发行日期。

----结束

13 安装应用发布服务器

13.1 安装 Windows Server 2019 应用服务器

13.1.1 安装服务器角色和功能

前提条件

已获取服务器管理员账号与密码。

操作步骤

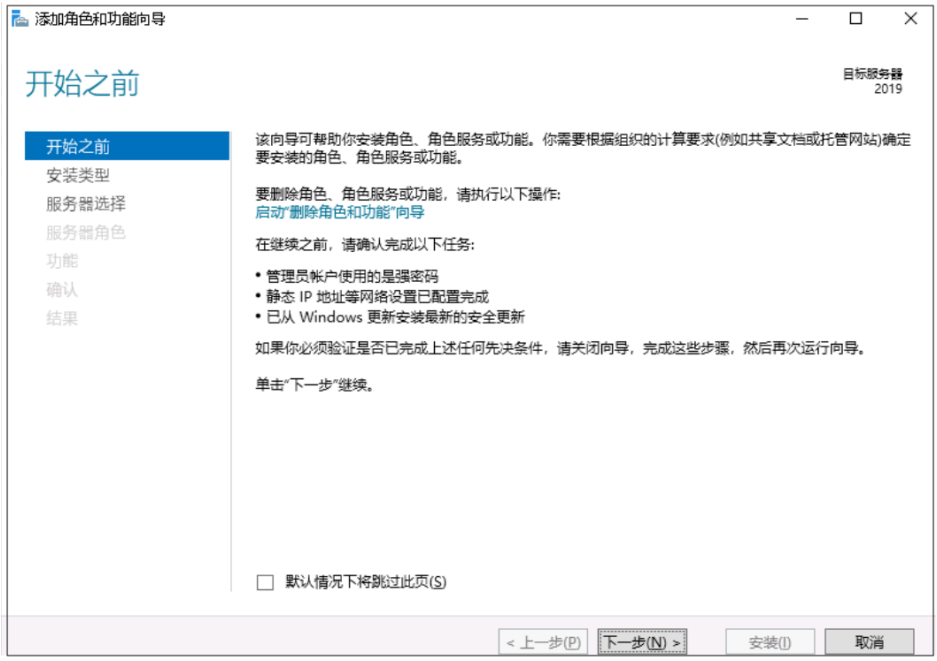
步骤 1 使用管理员账号登录服务器。

步骤 2 打开“服务器管理器”，选择“仪表板”，进入仪表板界面。

图13-1 仪表板页面

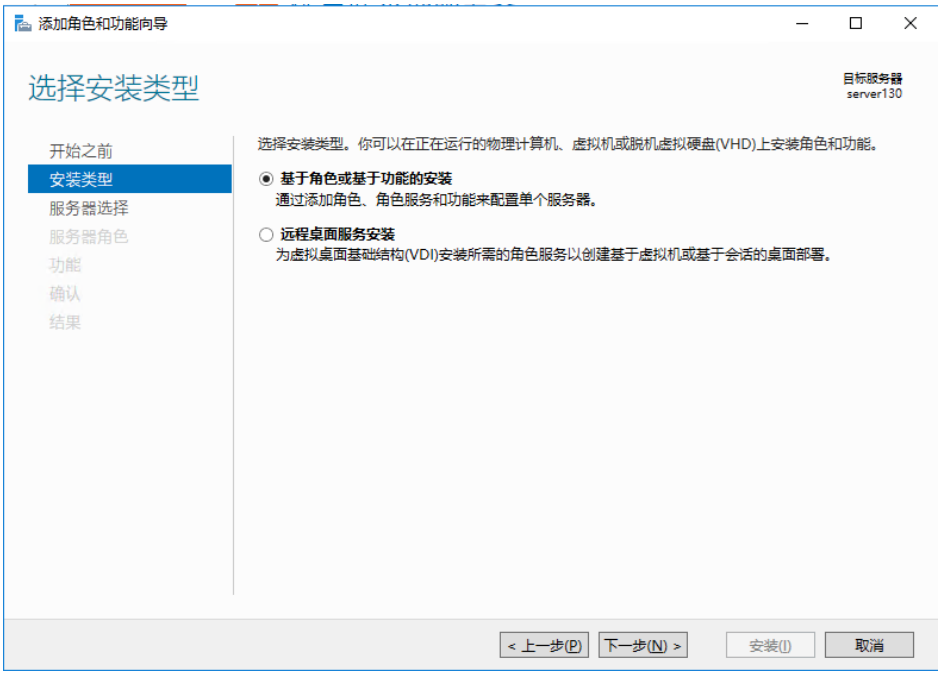
步骤 3 单击“添加角色和功能”，打开“添加角色和功能向导”窗口，根据向导指示，逐步单击“下一步”操作。

图13-2 开始之前



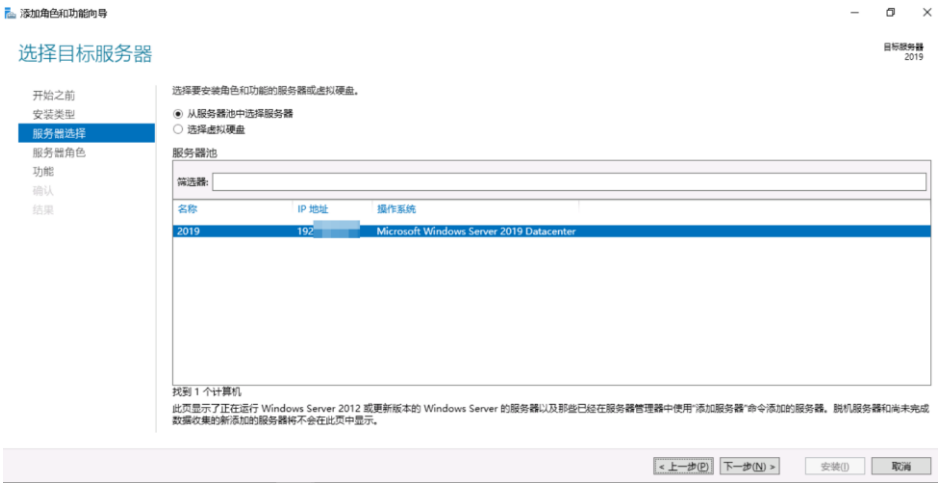
步骤 4 选择基于角色或基于功能的安装。

图13-3 选择安装类型



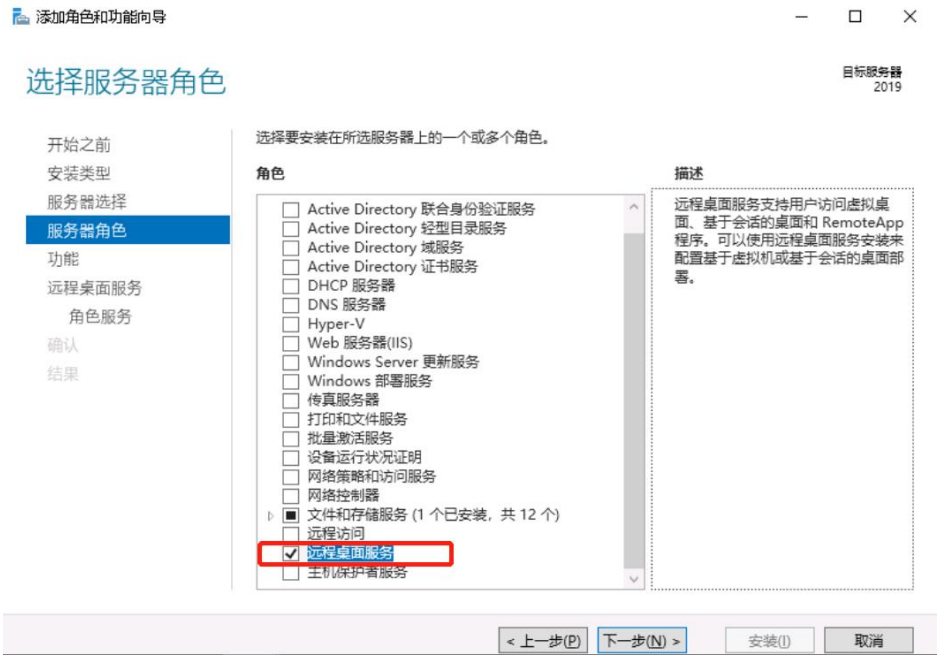
步骤 5 在服务器池中选择目标服务器。

图13-4 选择服务器



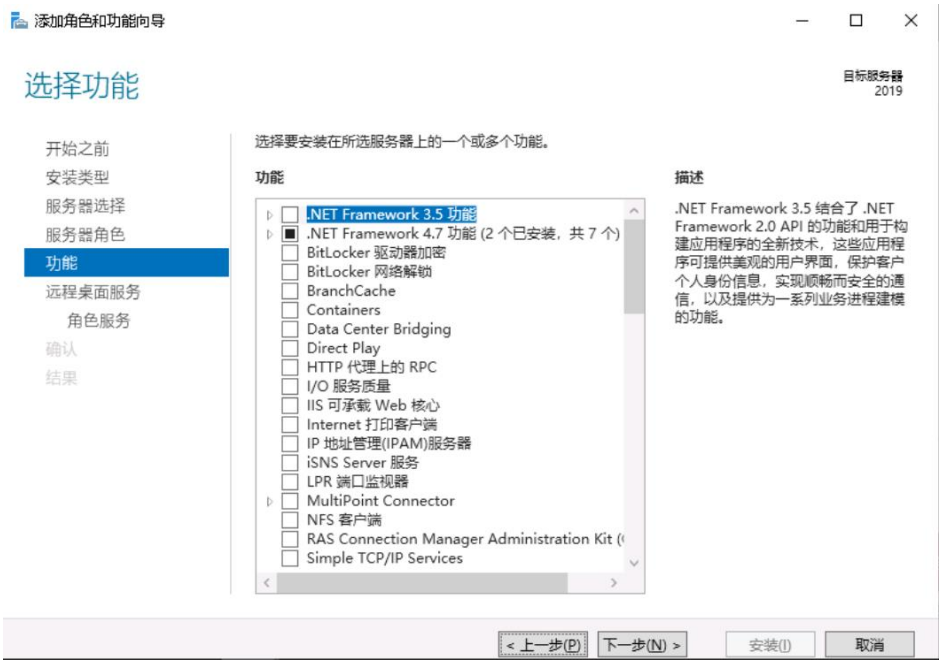
步骤 6 在服务器角色窗口中，勾选“Active Directory 域服务”、“DNS 服务器”、“远程桌面服务”三个角色项。

图13-5 选择服务器角色



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。

图13-6 选择其他功能



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。

图13-7 选择 IIS 服务角色

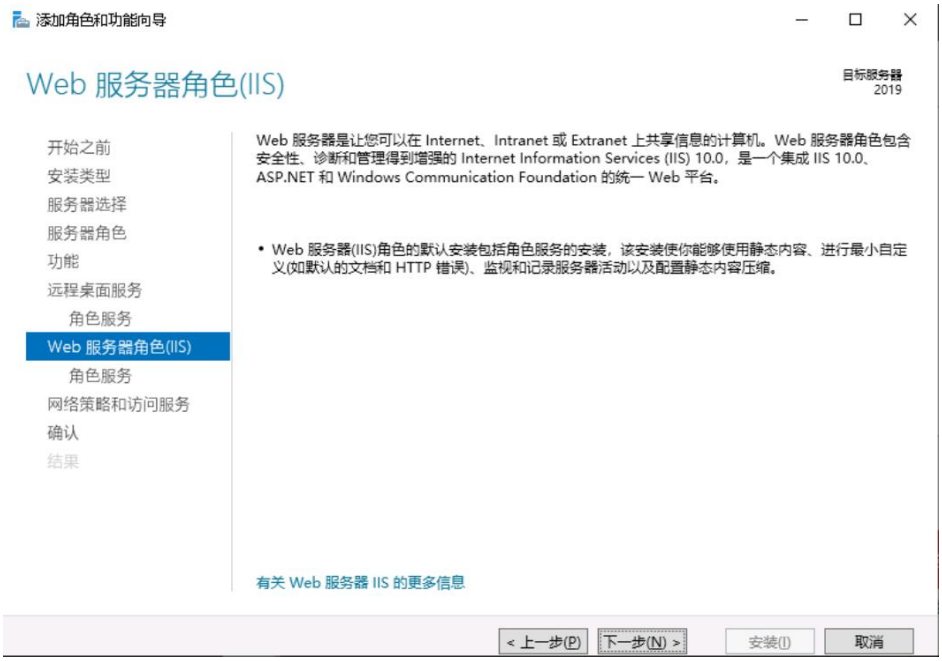
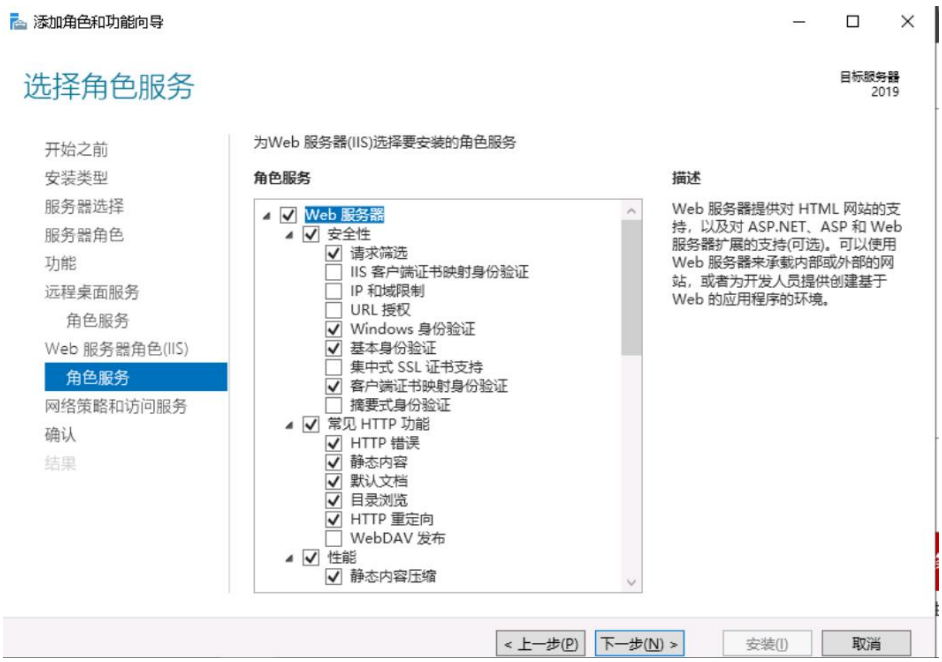


图13-8 选择服务角色

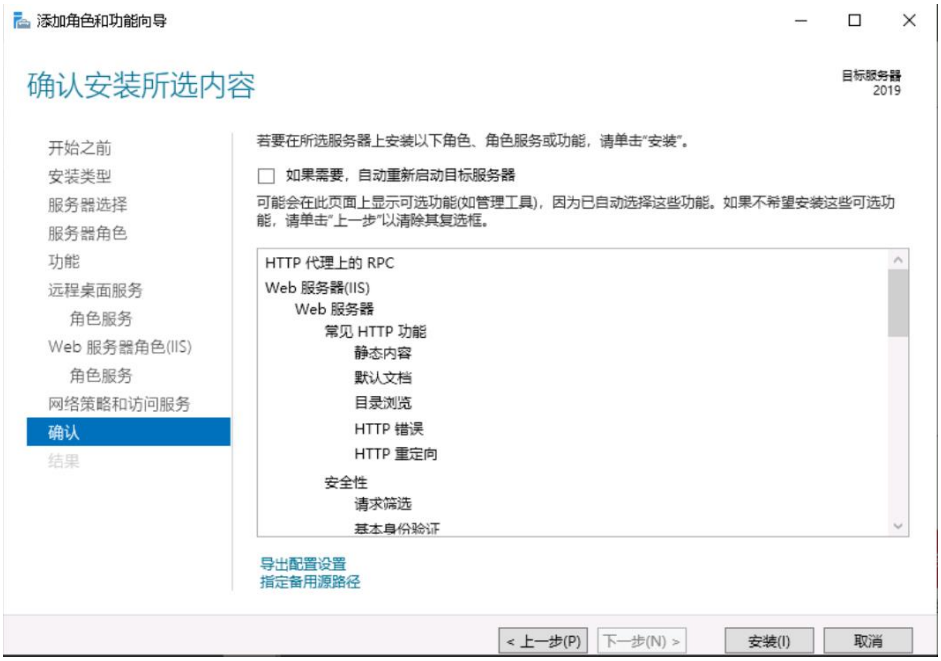


步骤 10 （可选）选择“网络策略和访问服务 ”，进入选择网络策略和访问服务窗口，默认勾选“网络策略服务器”选项。

图13-9 选择网络策略和访问服务

步骤 11 确认配置选择，单击“安装”，请耐心等待安装进度完成。

图13-10 安装服务器角色



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

13.1.2 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”。

图13-11 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。

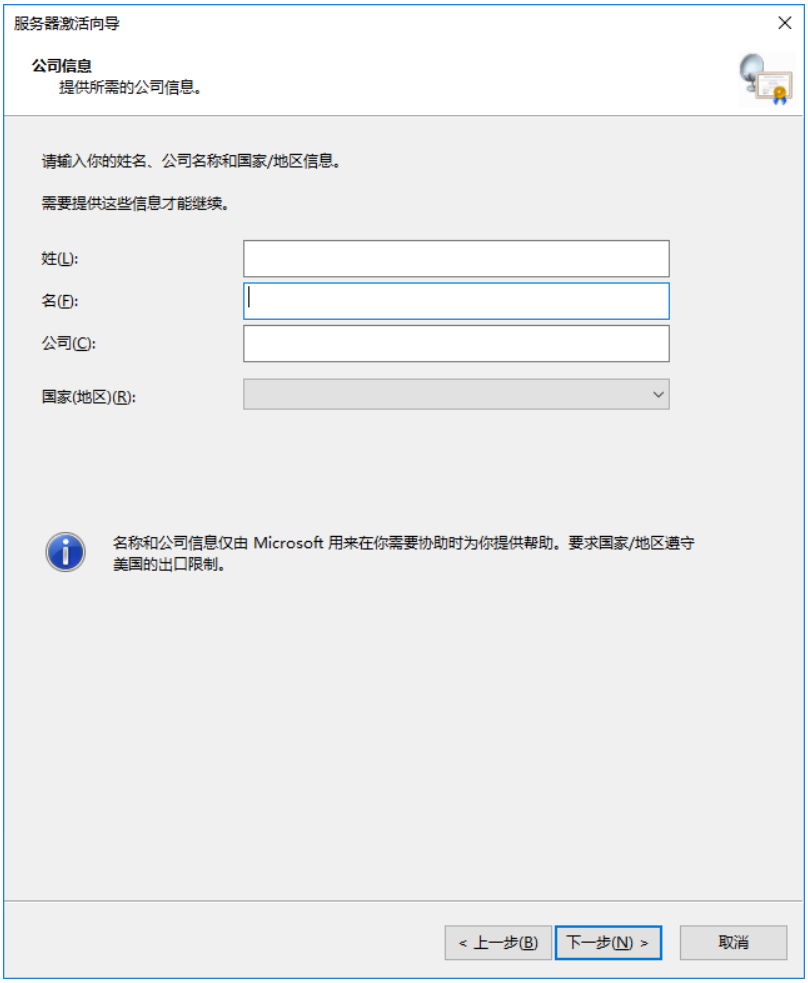
图13-12 打开服务器激活向导

步骤 5 选择自动连接方式。

图13-13 选择自动连接

步骤 6 输入公司名称和用户姓名。

图13-14 输入相关信息



步骤 7 （可选）输入公司详细通讯信息。

图13-15 输入公司详细信息

步骤 8 确认安装启动许可证安装向导。

图13-16 确认许可证安装向导

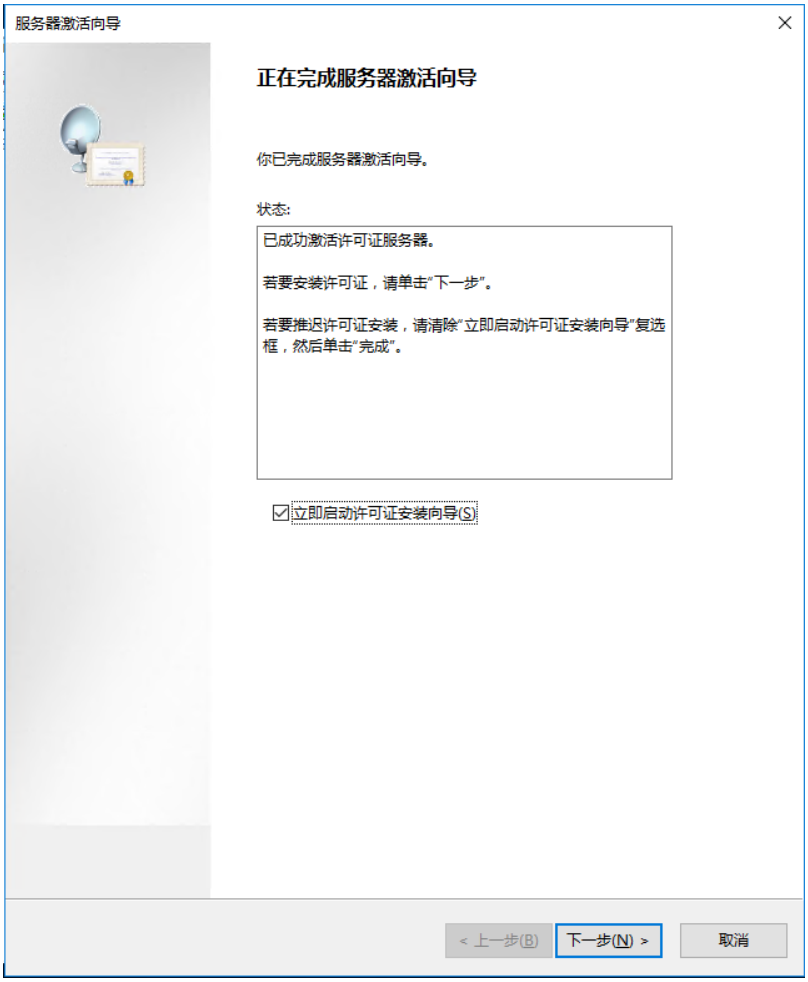


图13-17 启用许可证安装向导

步骤 9 许可证计划选择“企业协议”。

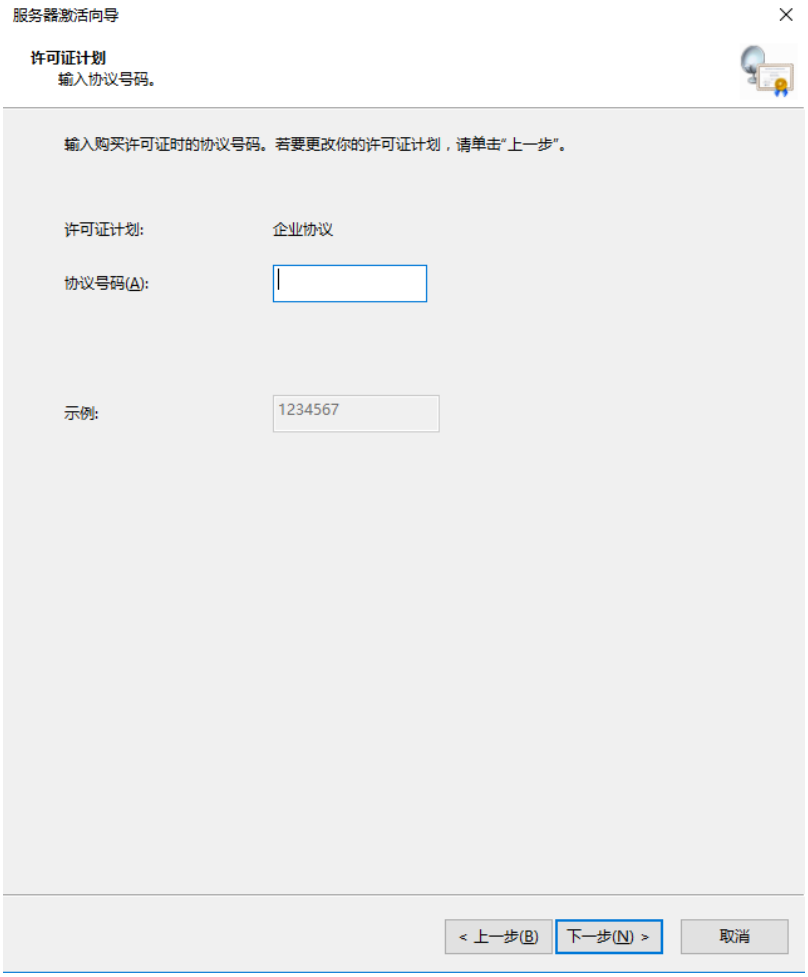
图13-18 选择许可证计划

步骤 10 输入企业协议号码。

说明

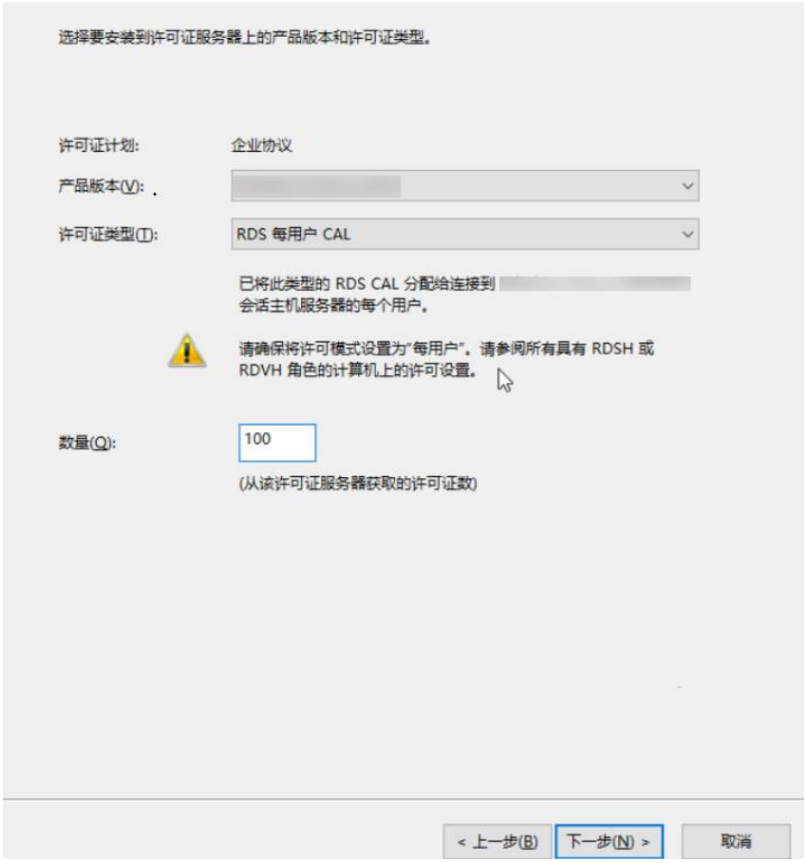
企业协议号码需提前向第三方平台申购获取官方远程桌面授权许可。

图13-19 输入协议号码



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。

图13-20 选择服务器版本



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。

图13-21 成功安装许可证

----结束

13.1.3 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。

图13-22 打开组策略

选择指定的远程桌面许可证服务器

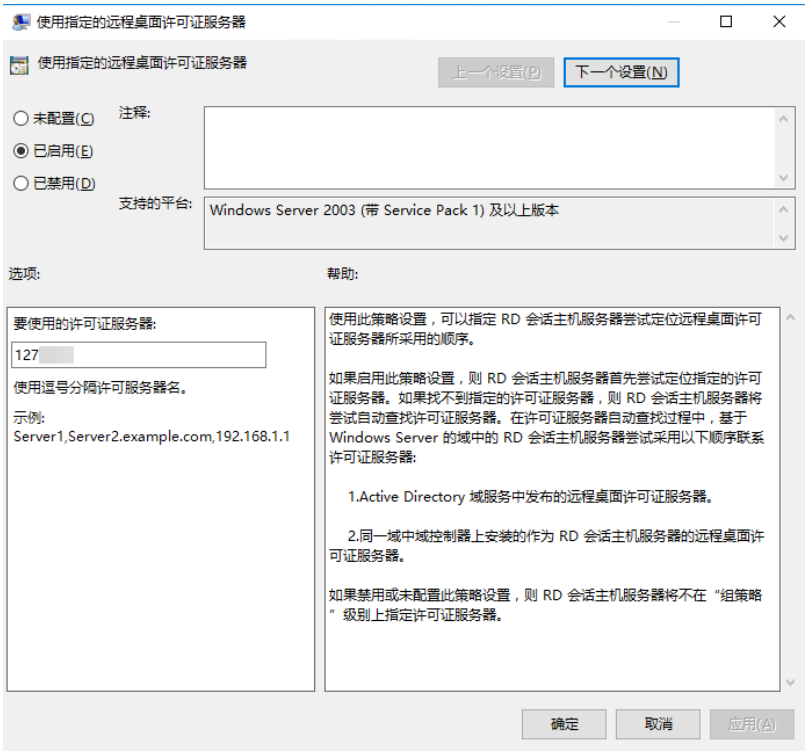
步骤 1 选择“计算机配置 > 管理模板 > Windows 组件 > 远程桌面服务 > 远程桌面会话主机 > 授权”，进入服务器授权许可设置页面。

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。

图13-23 使用指定许可证服务器



----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

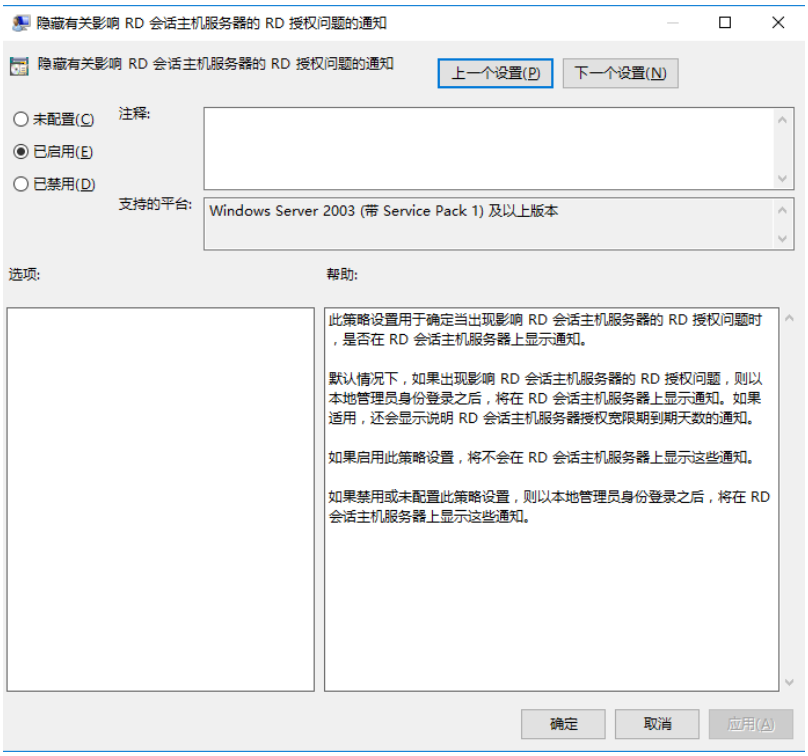
步骤 1 选择“计算机配置 > 管理模板 > Windows 组件 > 远程桌面服务 > 远程桌面会话主机 > 授权”，进入服务器授权许可设置页面。

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。

图13-24 隐藏 RD 授权问题的通知



----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。

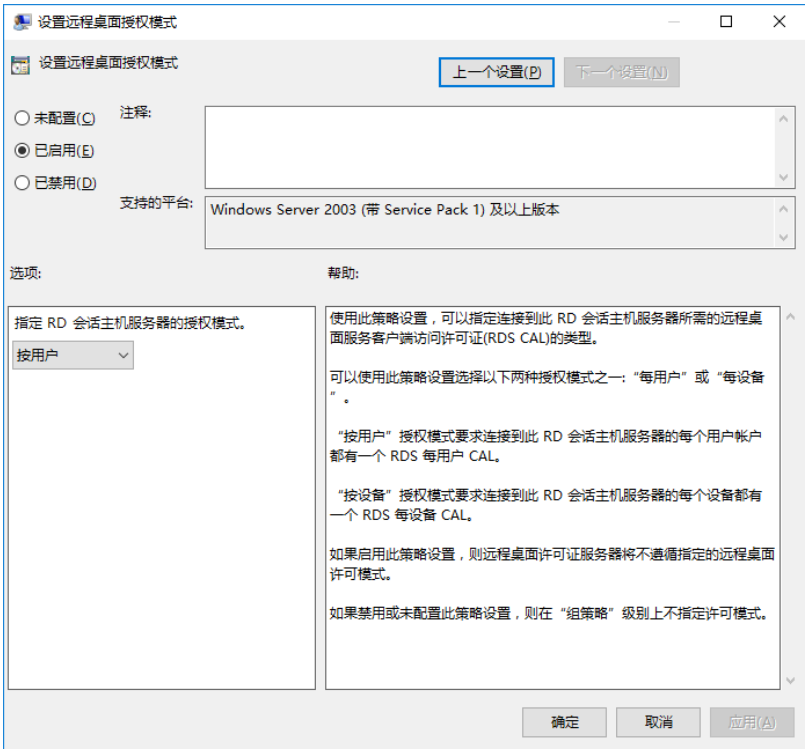
步骤 2 双击“设置远程桌面授权模式”，打开设置窗口。

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。

图13-25 设置远程桌面授权模式



----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。

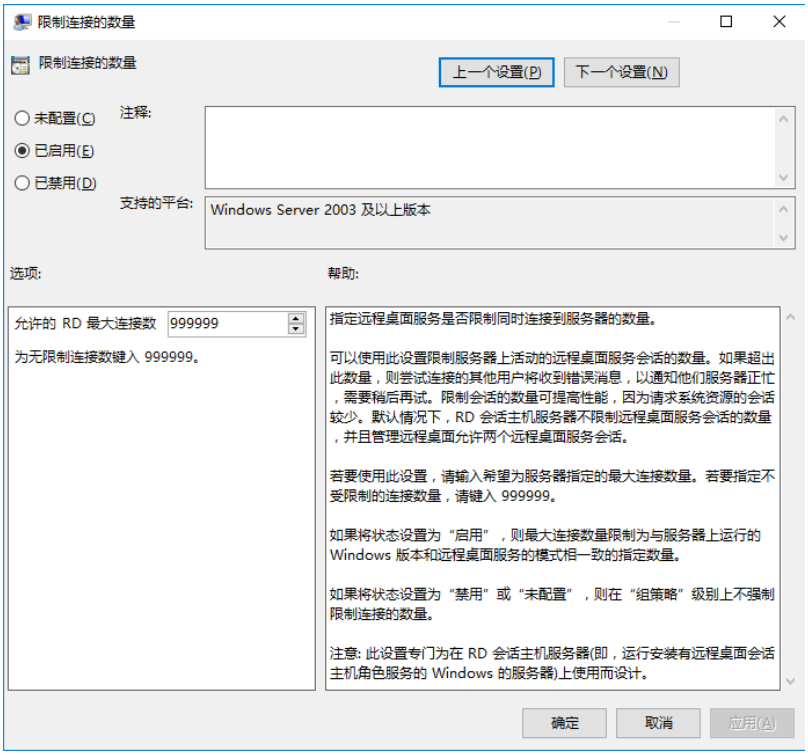
步骤 2 双击“限制连接的数量”，打开设置窗口。

步骤 3 勾选“已启用”，开启连接数量限制。

设置允许 RD 最大连接数位 999999。

步骤 4 单击“确定”，完成设置。

图13-26 限制连接的数量



----结束

允许远程启动未列出的程序

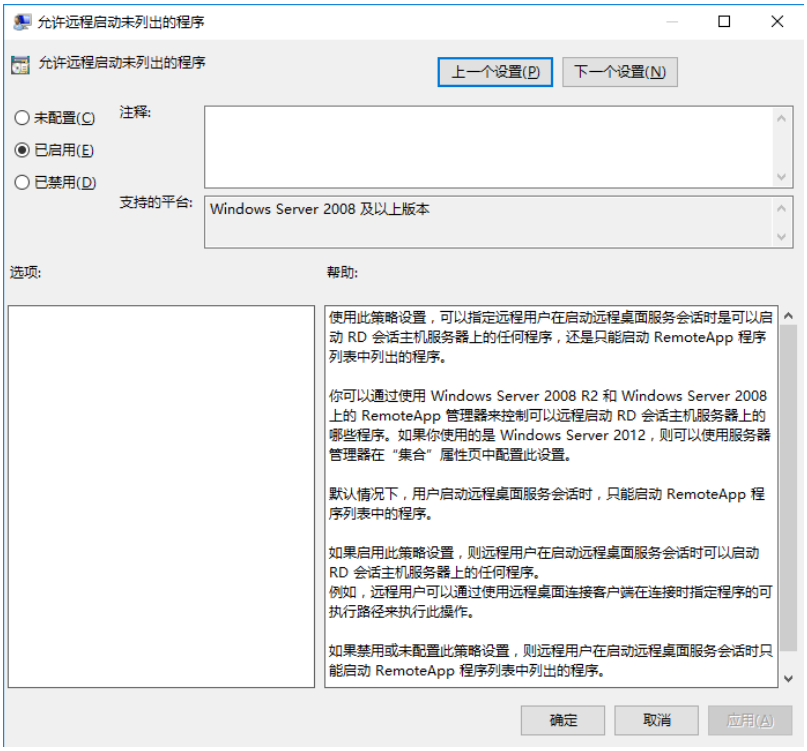
步骤 1 选择“计算机配置 > 管理模板 > Windows 组件 > 远程桌面服务 > 远程桌面会话主机 > 连接”，进入服务器连接配置页面。

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呈现。

步骤 4 单击“确定”，完成设置。

图13-27 允许远程启动未列出的程序



----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

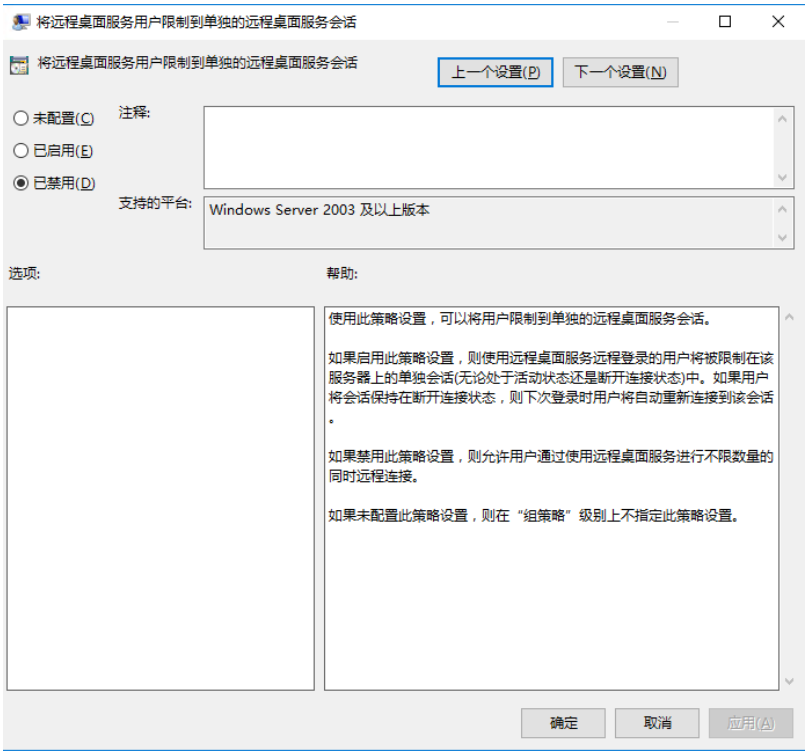
步骤 1 选择“计算机配置 > 管理模板 > Windows 组件 > 远程桌面服务 > 远程桌面会话主机 > 连接”，进入服务器连接配置页面。

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。

图13-28 将远程桌面服务用户限制到单独的远程桌面服务会话



----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。

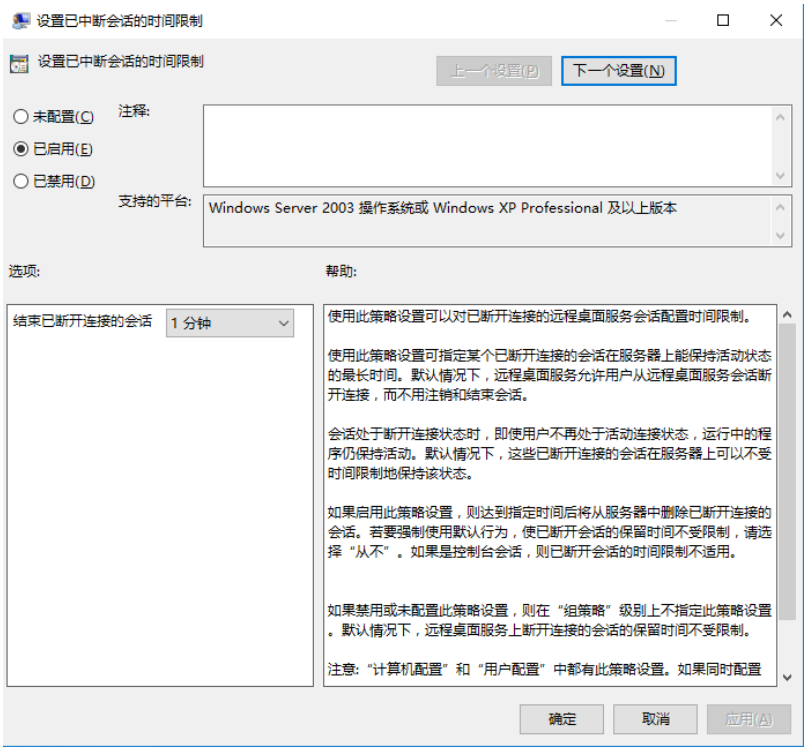
步骤 2 双击“设置已中断会话的时间限制”，打开设置窗口。

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。

图13-29 设置已中断会话的时间限制



----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。

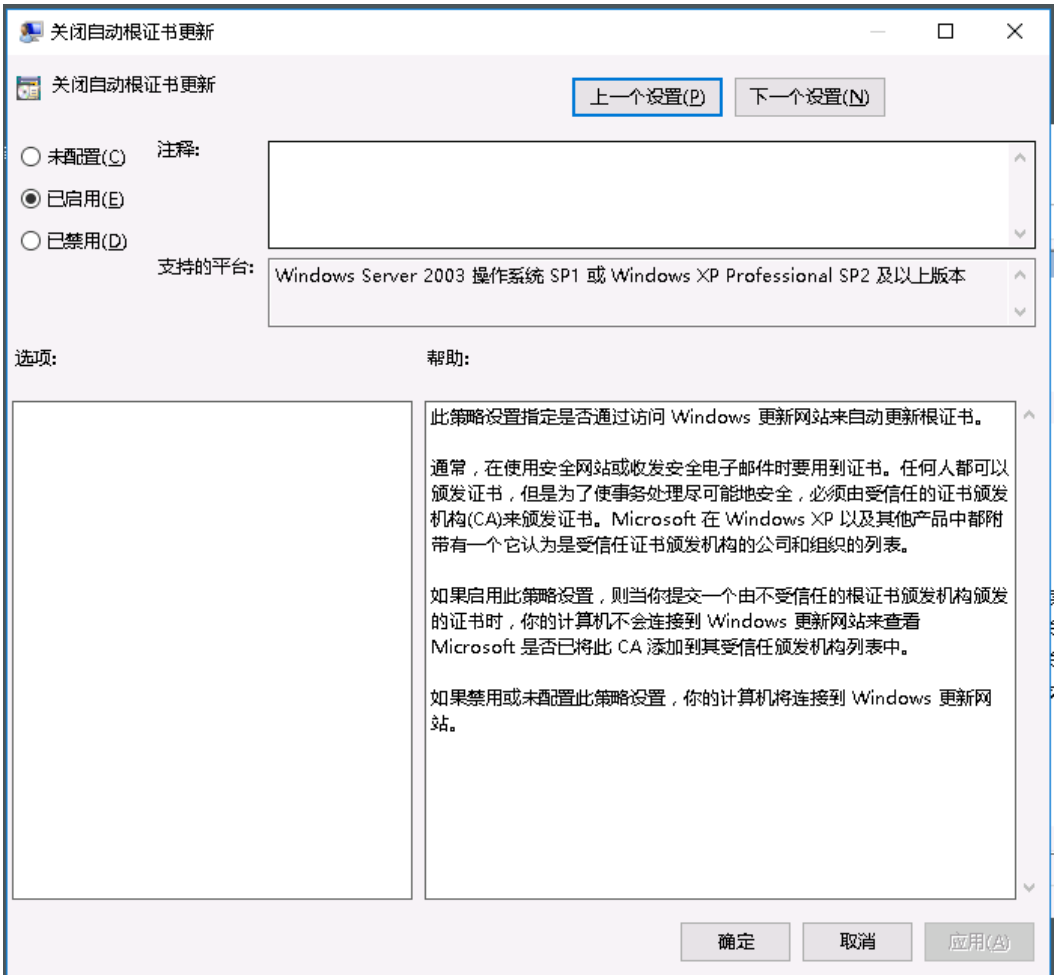
步骤 1 选择“管理模板 > 系统 > Internet 通信管理”，进入“Internet 通信管理”页面。

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。

图13-30 关闭自动根证书更新



----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。

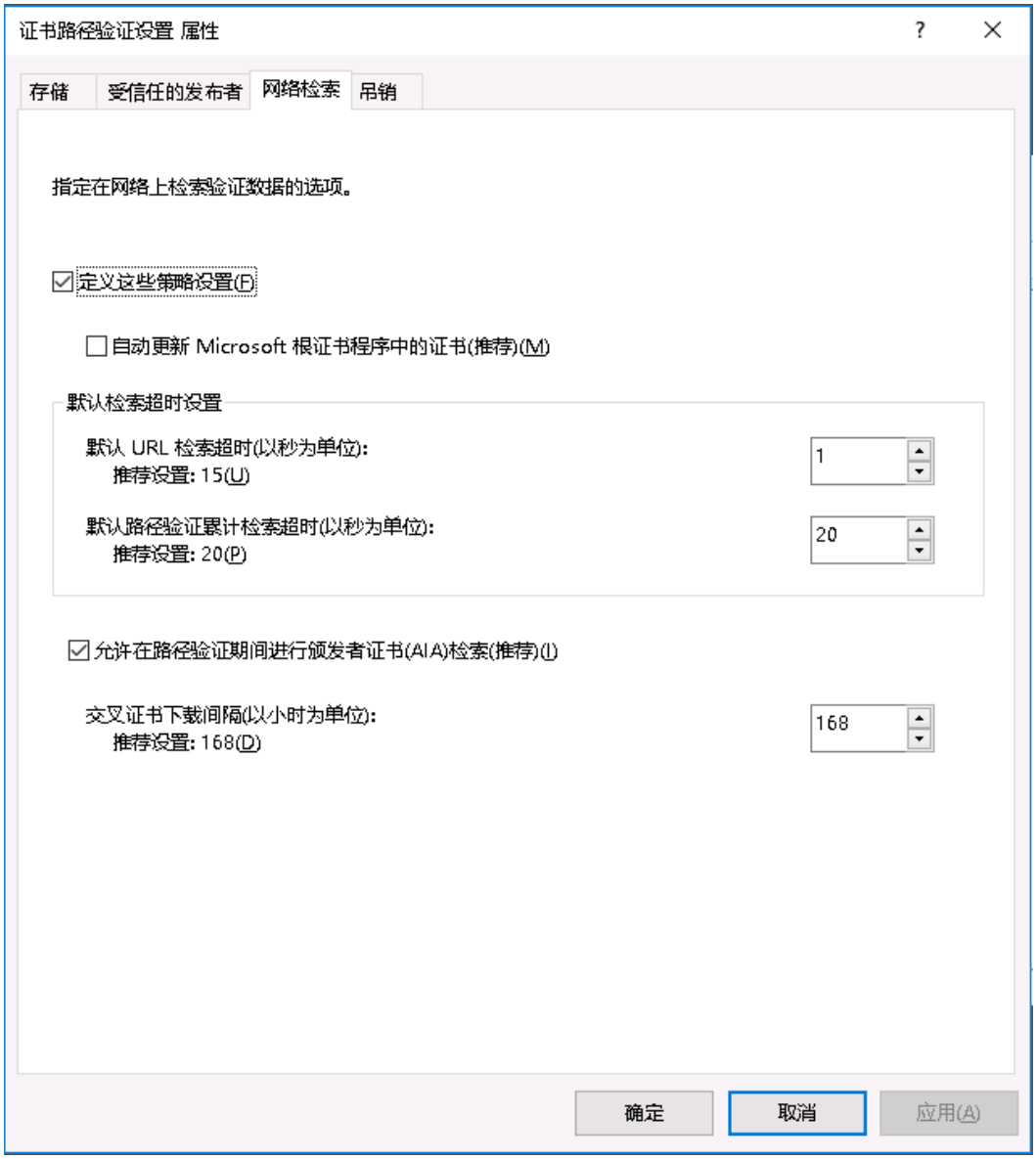
步骤 3 选择“网络检索”页签。

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。

图13-31 证书路径验证设置



----结束

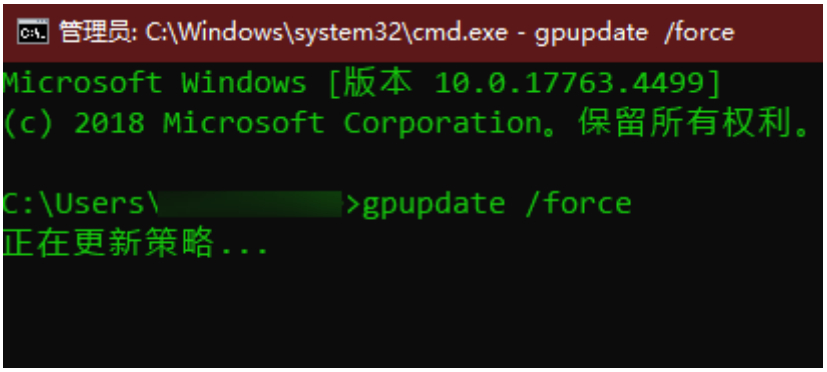
刷新本地组策略

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云堡垒机。

图13-32 刷新本地组策略



----结束

13.2 安装 Windows Server 2016 应用服务器

13.2.1 安装服务器角色和功能

前提条件

已获取服务器管理员账号与密码。

操作步骤

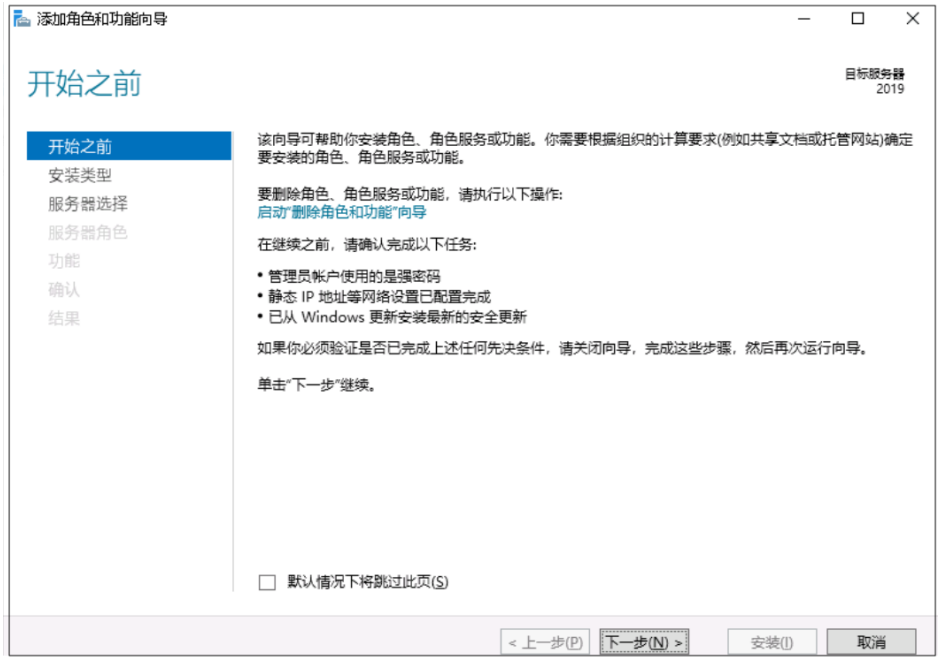
步骤 1 使用管理员账号登录服务器。

步骤 2 打开“服务器管理器”，选择“仪表板”，进入仪表板界面。

图13-33 仪表板页面

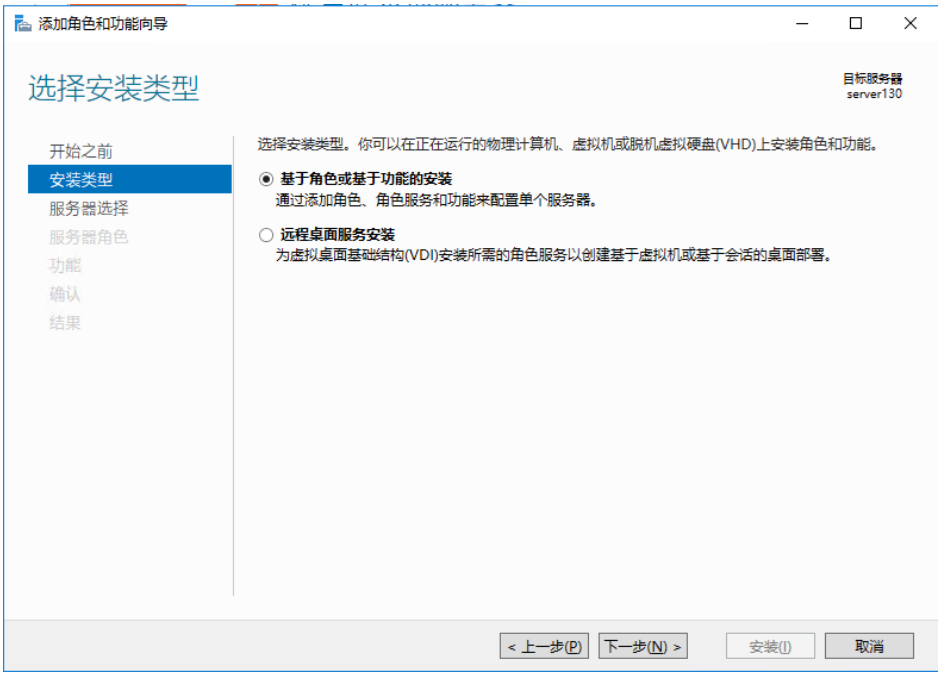
步骤 3 单击“添加角色和功能”，打开“添加角色和功能向导”窗口，根据向导指示，逐步单击“下一步”操作。

图13-34 开始之前



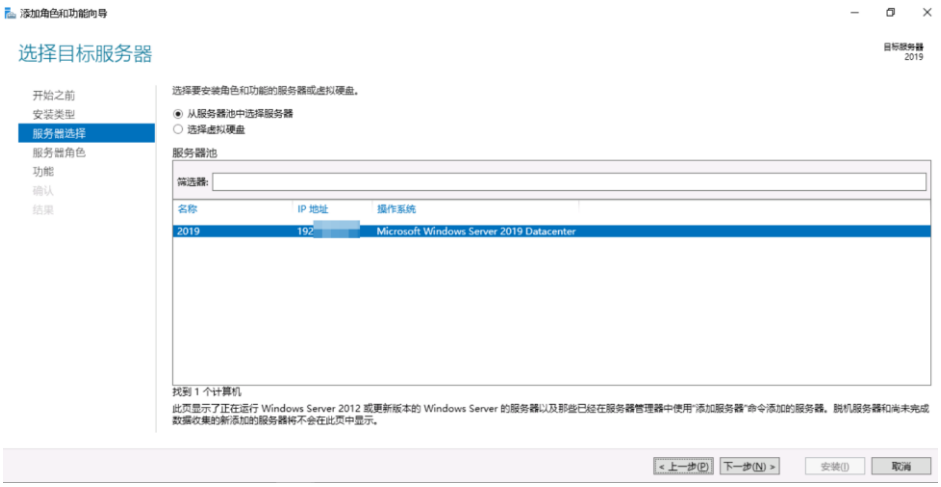
步骤 4 选择基于角色或基于功能的安装。

图13-35 选择安装类型



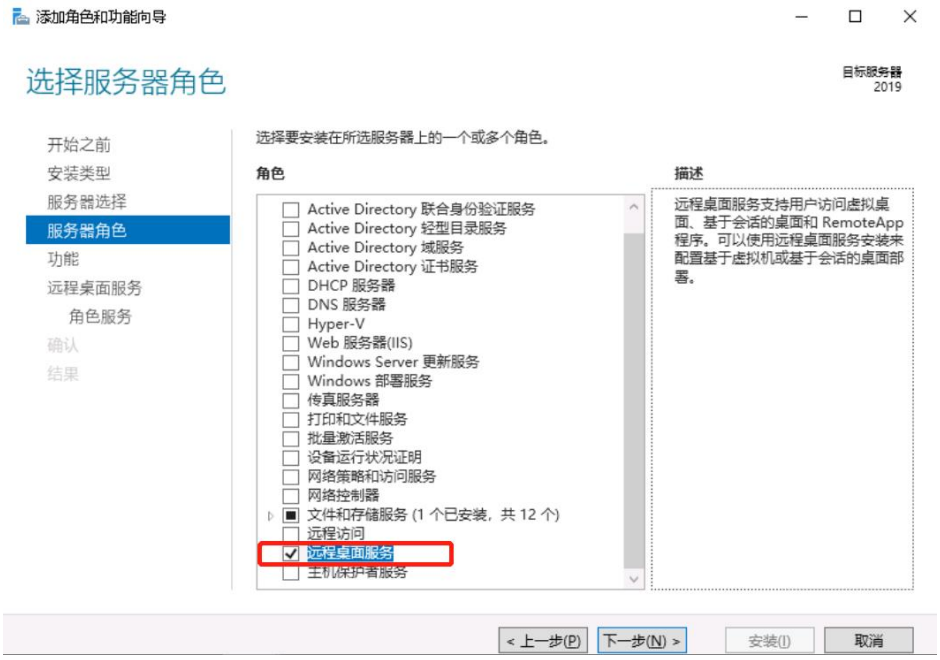
步骤 5 在服务器池中选择目标服务器。

图13-36 选择服务器



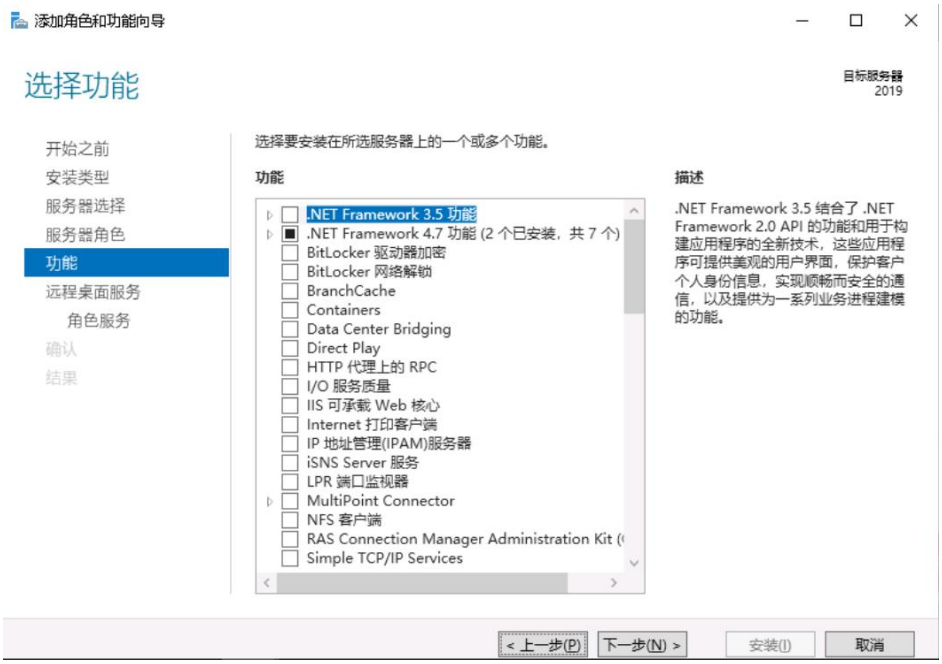
步骤 6 在服务器角色窗口中，勾选“Active Directory 域服务”、“DNS 服务器”、“远程桌面服务”三个角色项。

图13-37 选择服务器角色



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。

图13-38 选择其他功能



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。

图13-39 选择 IIS 服务角色

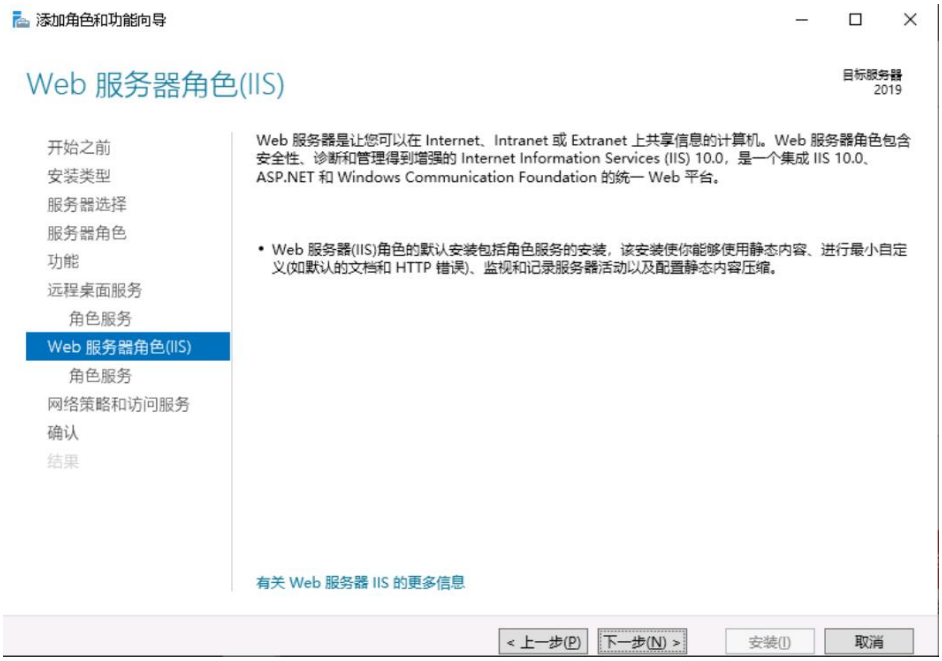
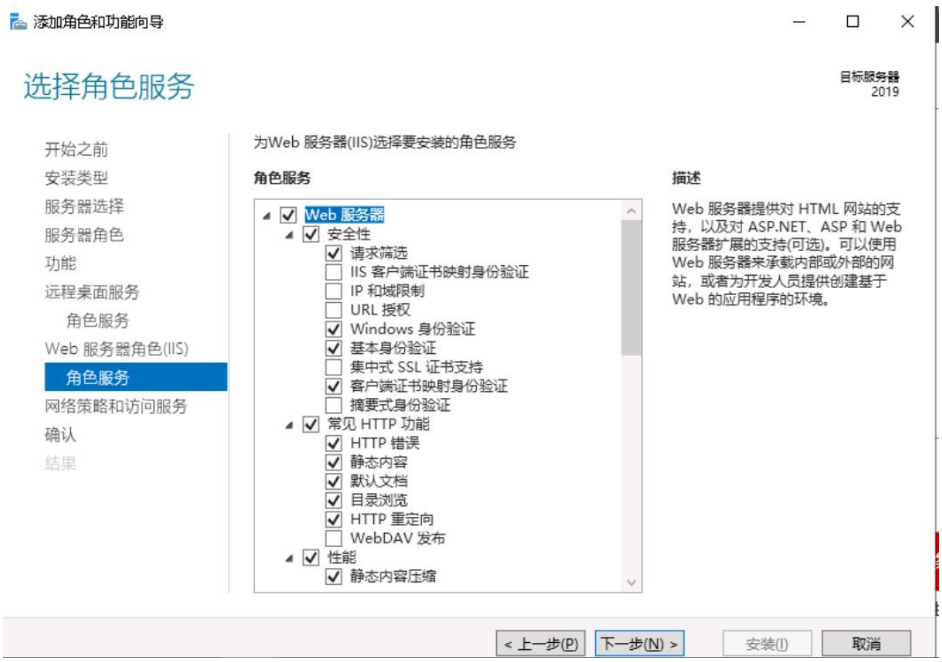


图13-40 选择服务角色

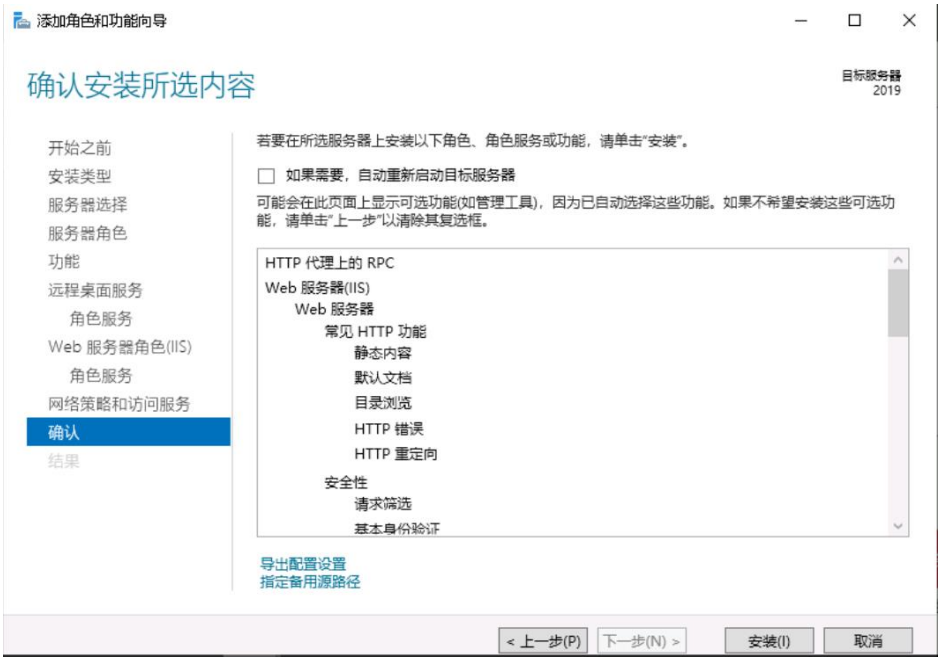


步骤 10 （可选）选择“网络策略和访问服务 ”，进入选择网络策略和访问服务窗口，默认勾选“网络策略服务器”选项。

图13-41 选择网络策略和访问服务

步骤 11 确认配置选择，单击“安装”，请耐心等待安装进度完成。

图13-42 安装服务器角色



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

13.2.2 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”。

图13-43 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。

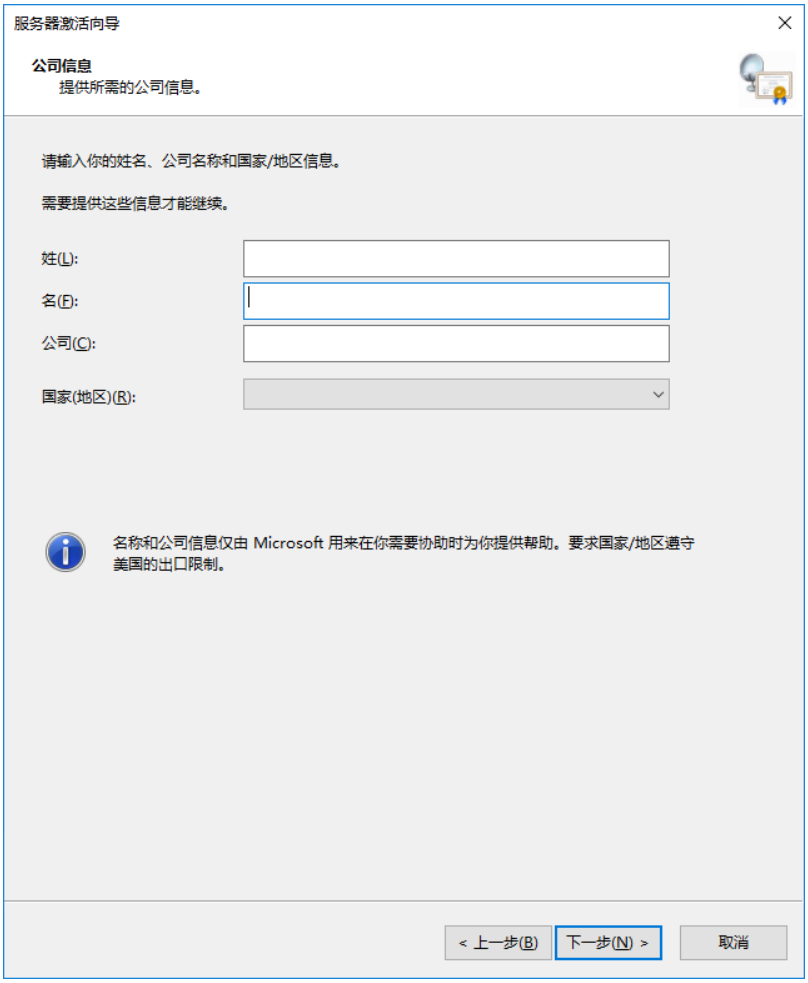
图13-44 打开服务器激活向导

步骤 5 选择自动连接方式。

图13-45 选择自动连接

步骤 6 输入公司名称和用户姓名。

图13-46 输入相关信息



步骤 7 （可选）输入公司详细通讯信息。

图13-47 输入公司详细信息

步骤 8 确认安装启动许可证安装向导。

图13-48 确认许可证安装向导

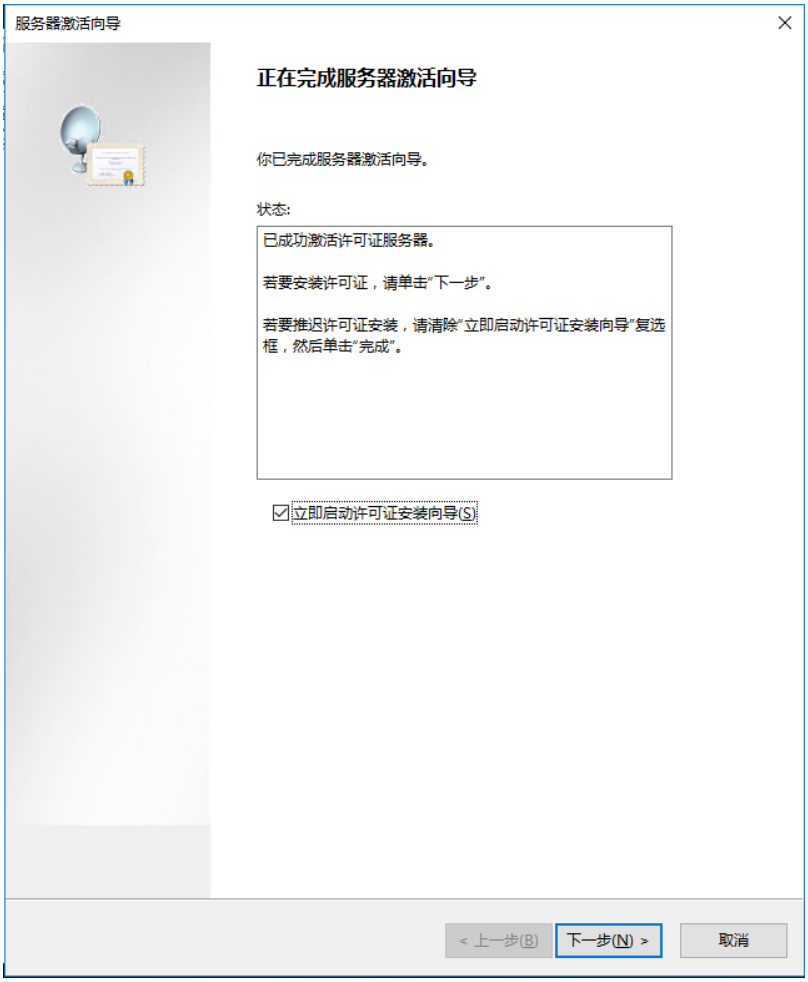


图13-49 启用许可证安装向导

步骤 9 许可证计划选择“企业协议”。

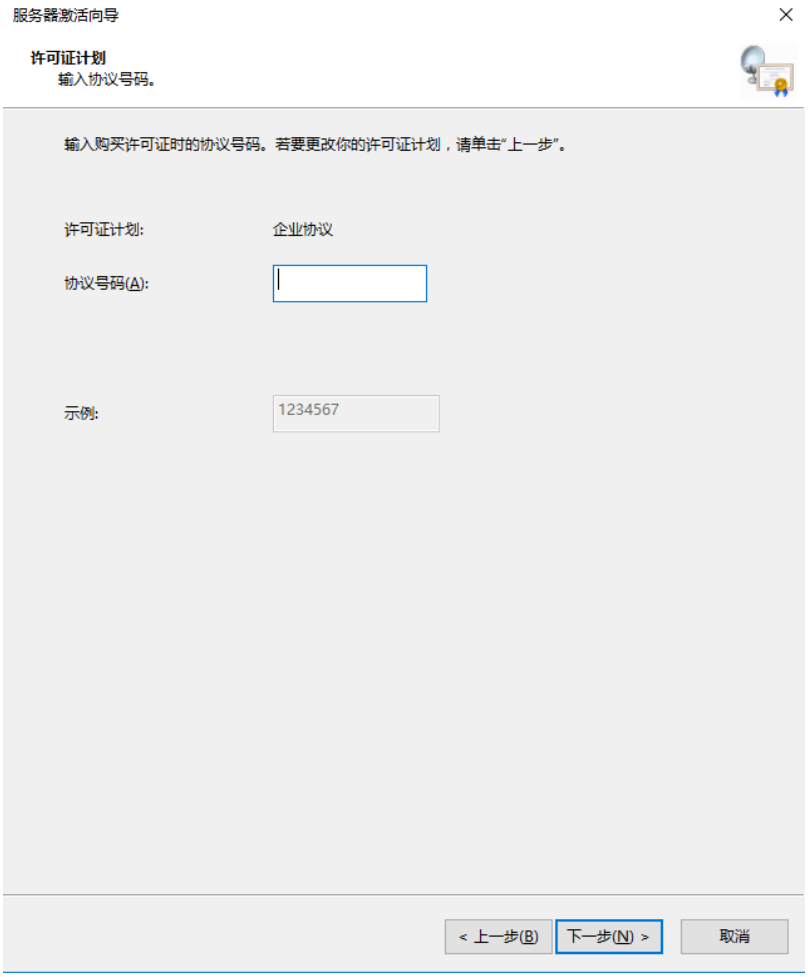
图13-50 选择许可证计划

步骤 10 输入企业协议号码。

说明

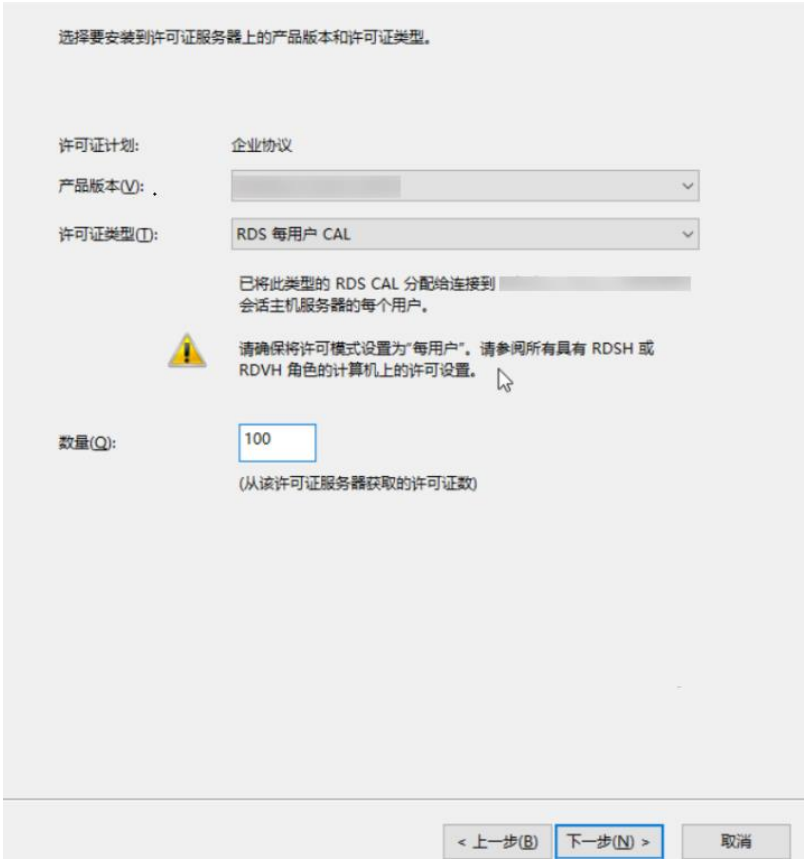
企业协议号码需提前向第三方平台申购获取官方远程桌面授权许可。

图13-51 输入协议号码



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。

图13-52 选择服务器版本



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。

图13-53 成功安装许可证

----结束

13.2.3 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。

图13-54 打开组策略

选择指定的远程桌面许可证服务器

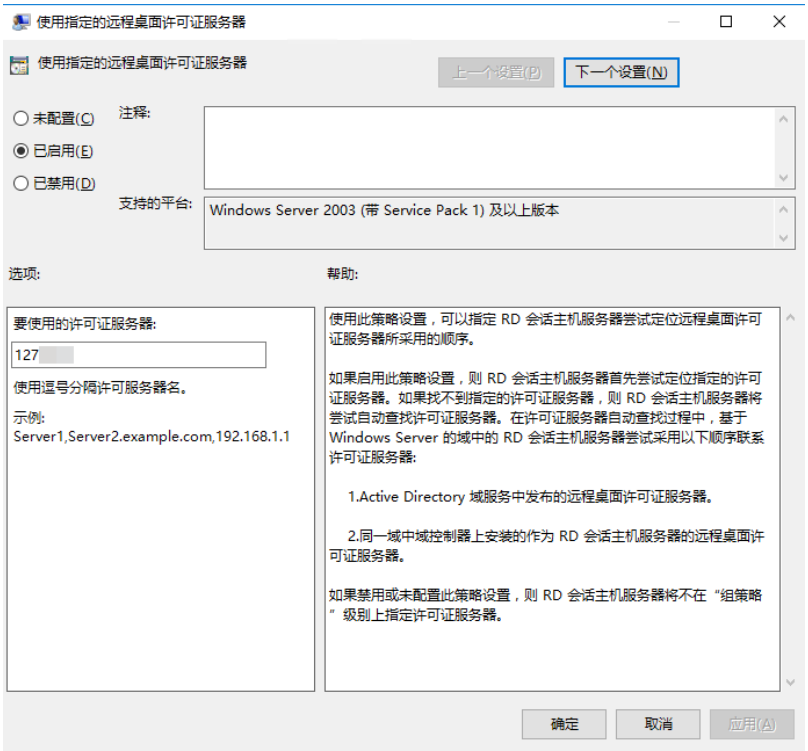
步骤 1 选择“计算机配置 > 管理模板 > Windows 组件 > 远程桌面服务 > 远程桌面会话主机 > 授权”，进入服务器授权许可设置页面。

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。

图13-55 使用指定许可证服务器



----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

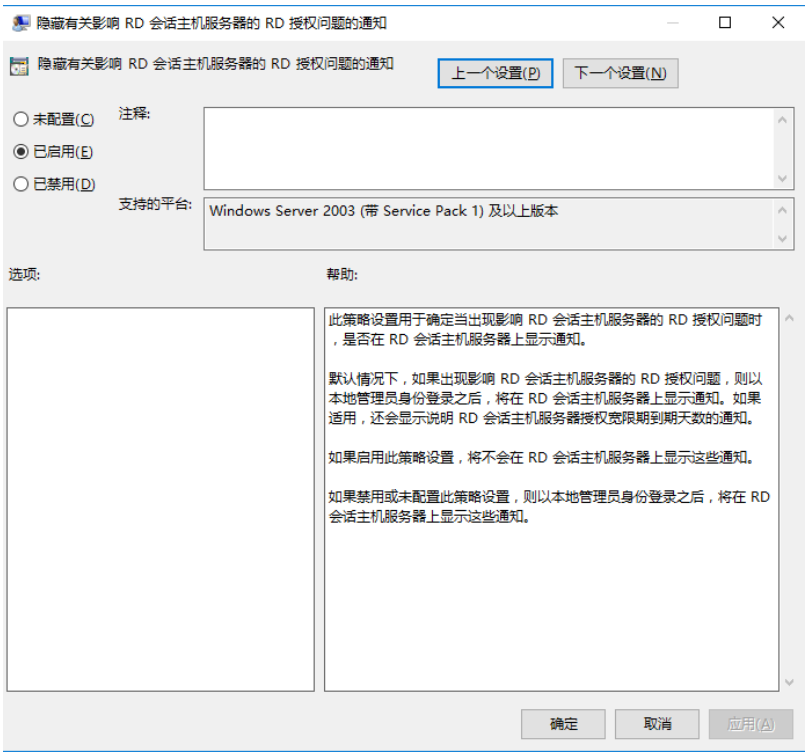
步骤 1 选择“计算机配置 > 管理模板 > Windows 组件 > 远程桌面服务 > 远程桌面会话主机 > 授权”，进入服务器授权许可设置页面。

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。

图13-56 隐藏 RD 授权问题的通知



----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。

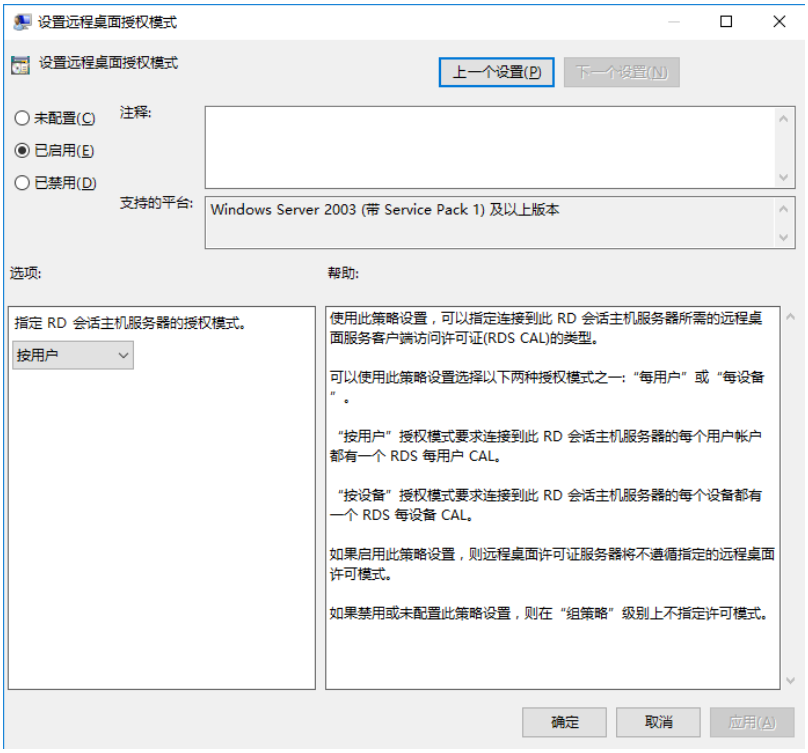
步骤 2 双击“设置远程桌面授权模式”，打开设置窗口。

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。

图13-57 设置远程桌面授权模式



----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。

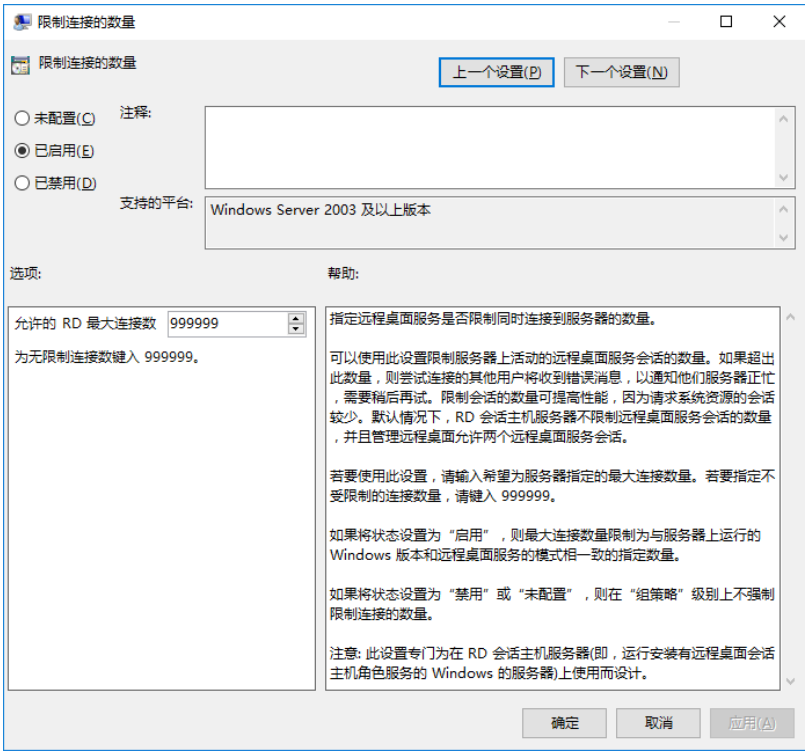
步骤 2 双击“限制连接的数量”，打开设置窗口。

步骤 3 勾选“已启用”，开启连接数量限制。

设置允许 RD 最大连接数位 999999。

步骤 4 单击“确定”，完成设置。

图13-58 限制连接的数量



----结束

允许远程启动未列出的程序

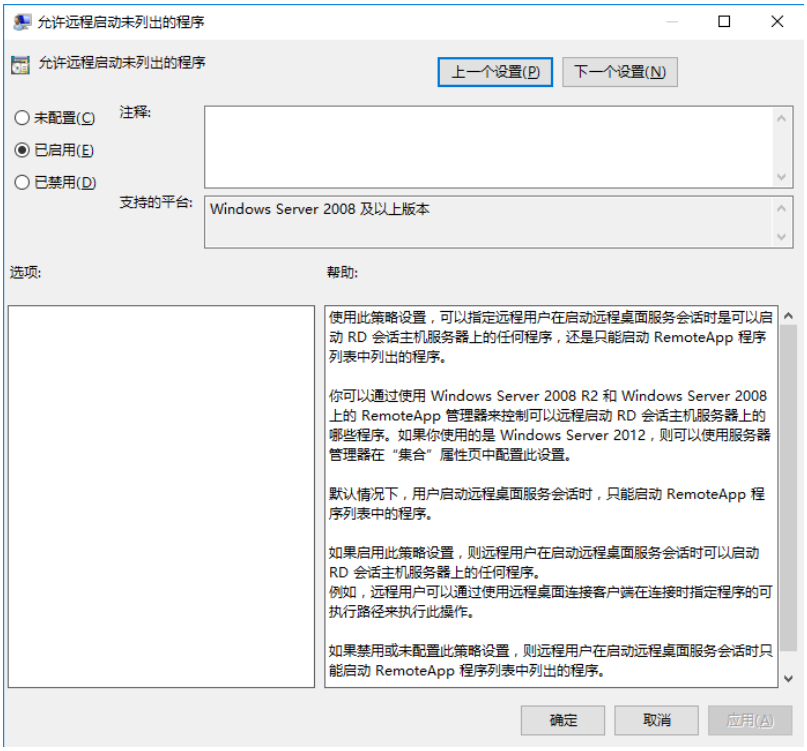
步骤 1 选择“计算机配置 > 管理模板 > Windows 组件 > 远程桌面服务 > 远程桌面会话主机 > 连接”，进入服务器连接配置页面。

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呈现。

步骤 4 单击“确定”，完成设置。

图13-59 允许远程启动未列出的程序



----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

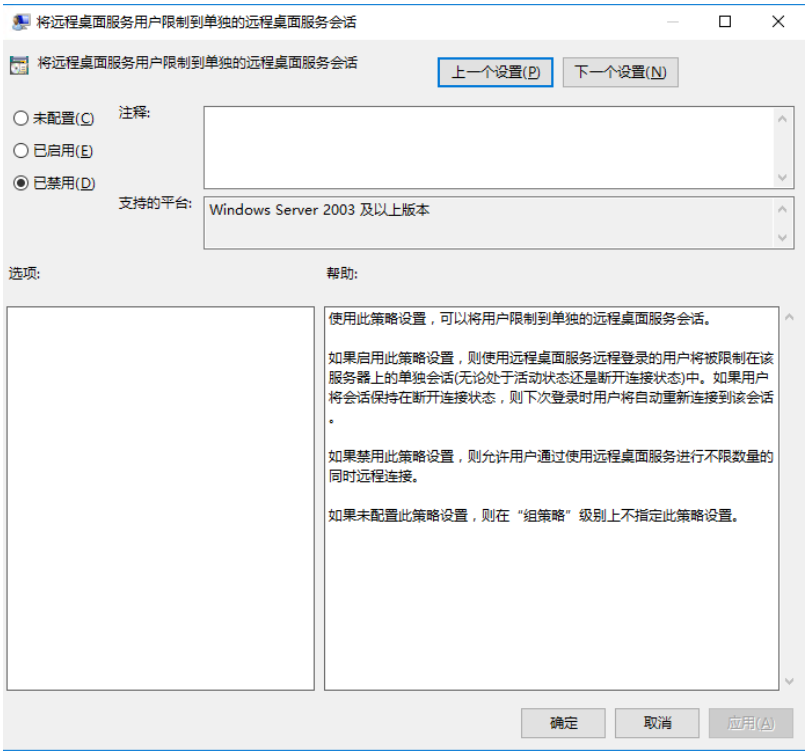
步骤 1 选择“计算机配置 > 管理模板 > Windows 组件 > 远程桌面服务 > 远程桌面会话主机 > 连接”，进入服务器连接配置页面。

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。

图13-60 将远程桌面服务用户限制到单独的远程桌面服务会话



----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。

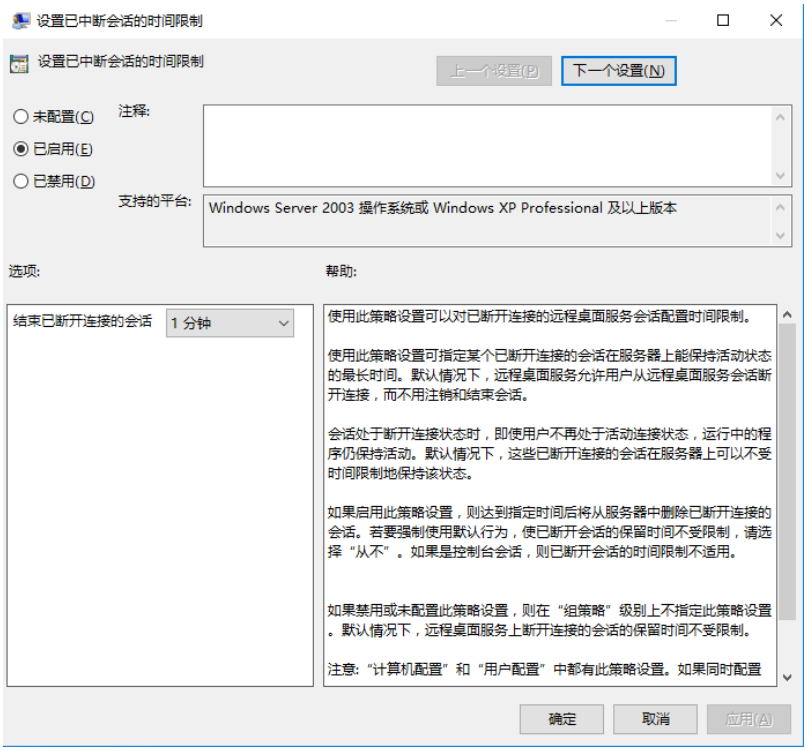
步骤 2 双击“设置已中断会话的时间限制”，打开设置窗口。

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。

图13-61 设置已中断会话的时间限制



----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。

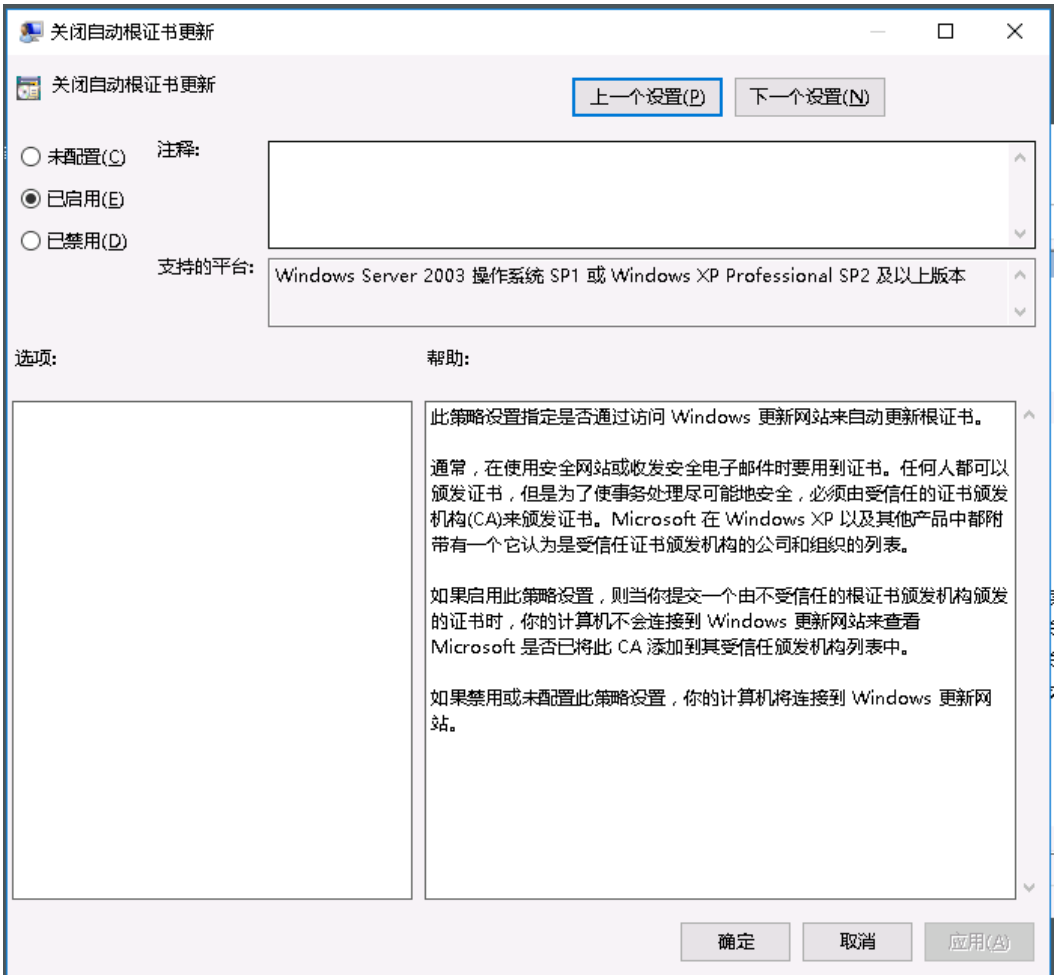
步骤 1 选择“管理模板 > 系统 > Internet 通信管理”，进入“Internet 通信管理”页面。

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。

图13-62 关闭自动根证书更新



----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。

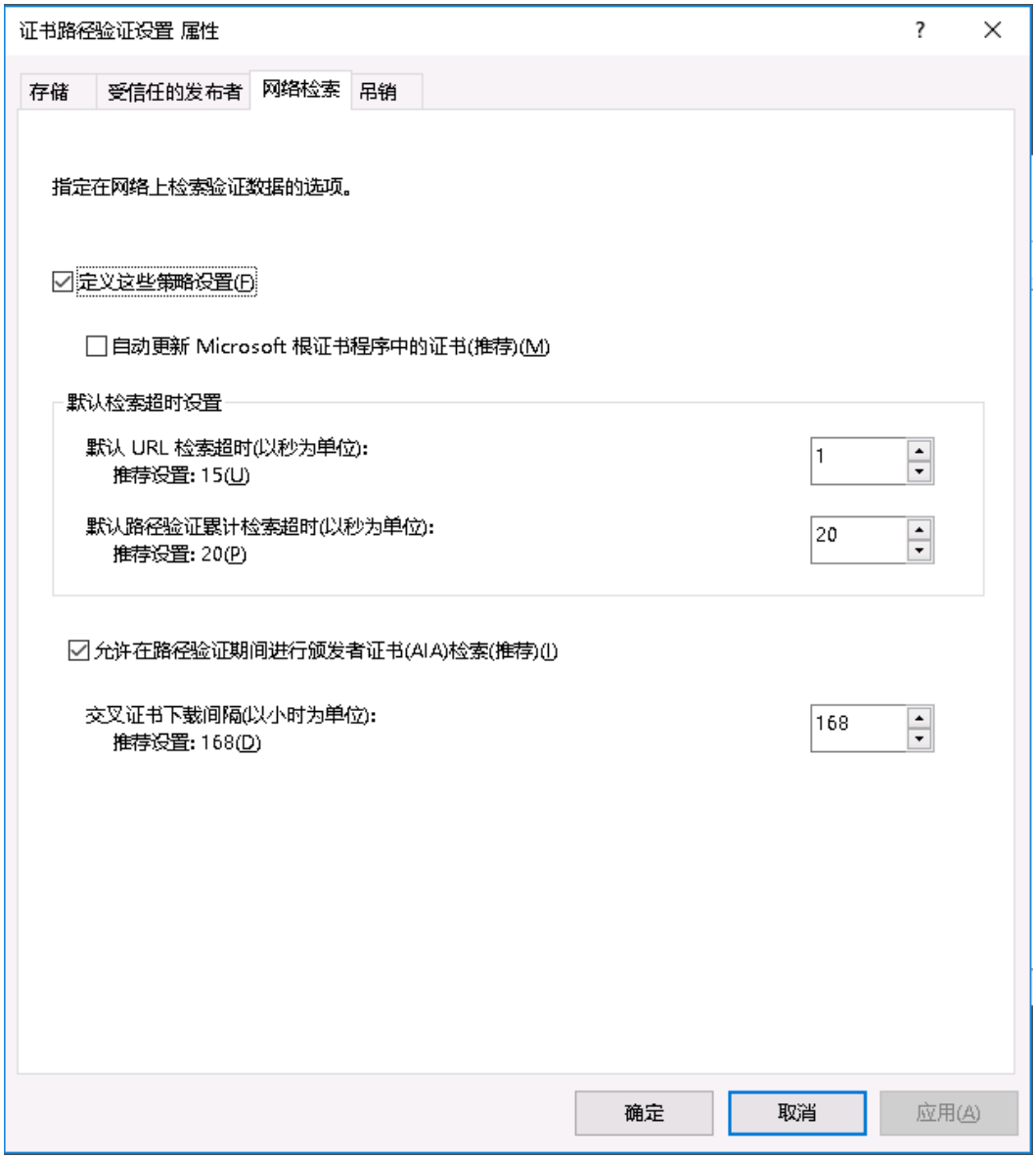
步骤 3 选择“网络检索”页签。

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。

图13-63 证书路径验证设置



----结束

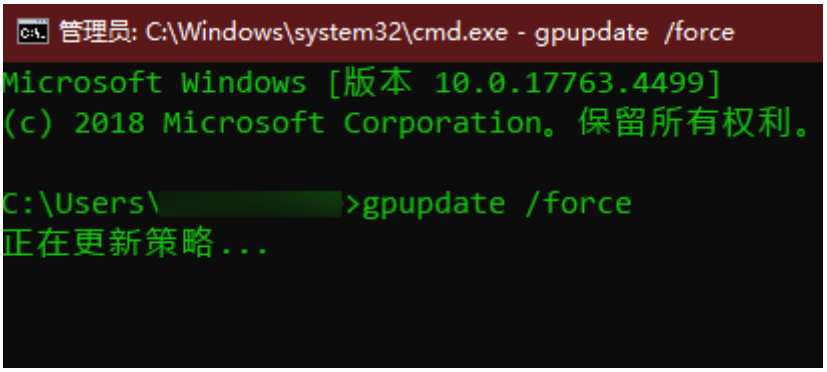
刷新本地组策略

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云堡垒机。

图13-64 刷新本地组策略



----结束

13.3 安装 Windows Server 2012 R2 应用服务器

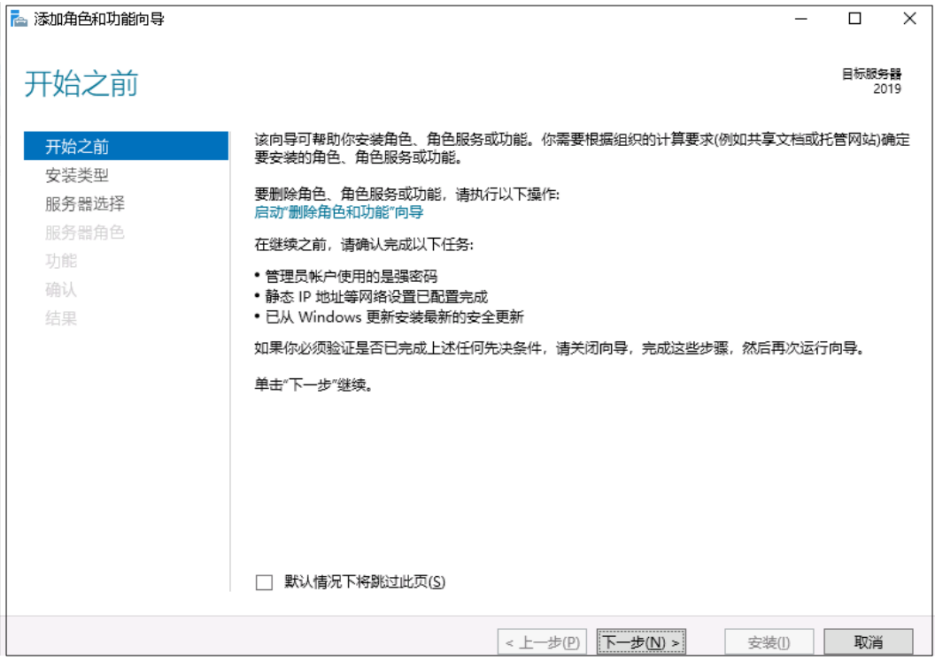
13.3.1 安装服务器角色和功能

步骤 1 打开“服务器管理器”，选择“仪表板”，进入仪表板界面。

图13-65 仪表板页面

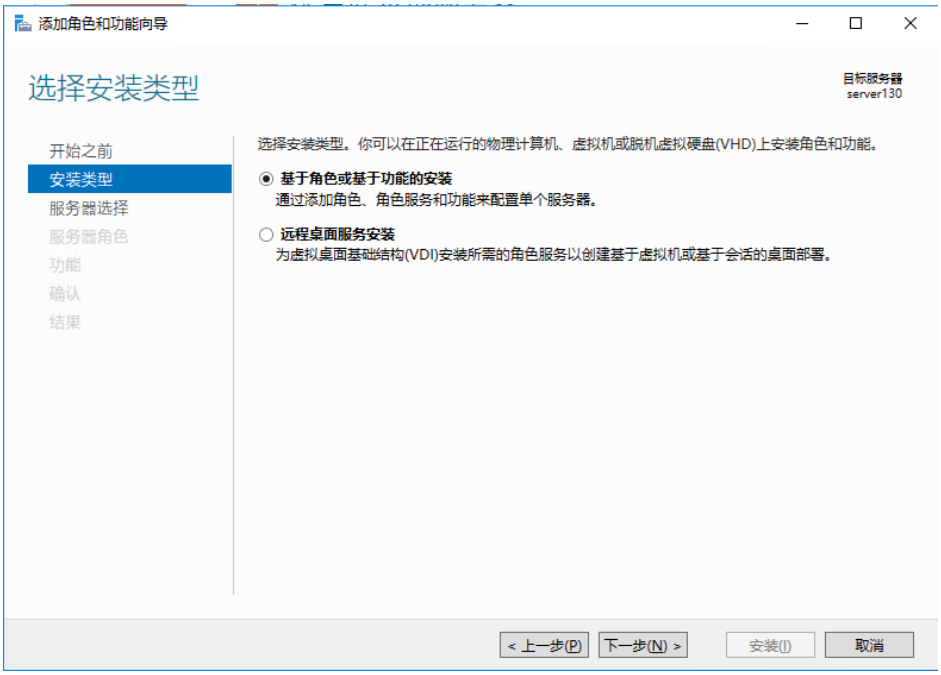
步骤 2 单击“添加角色和功能”，打开“添加角色和功能向导”窗口，根据向导指示，逐步单击“下一步”操作。

图13-66 开始之前



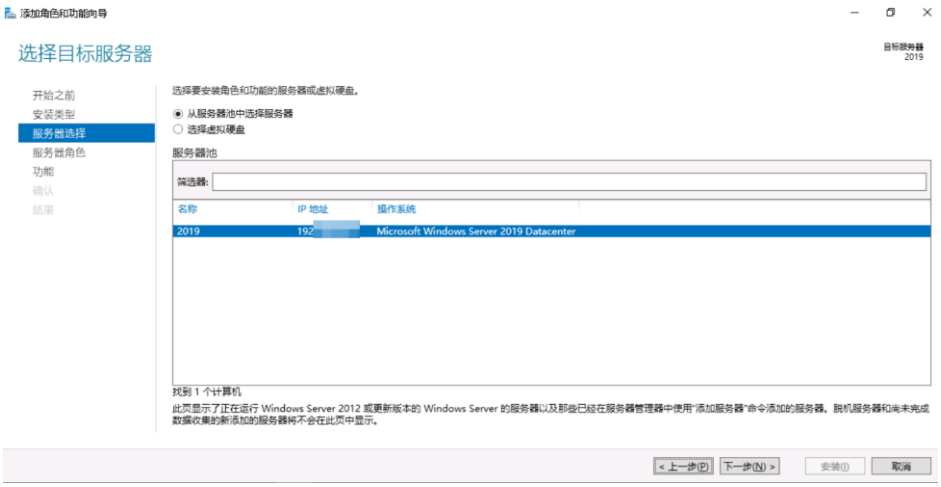
步骤 3 选择基于角色或基于功能的安装。

图13-67 选择安装类型



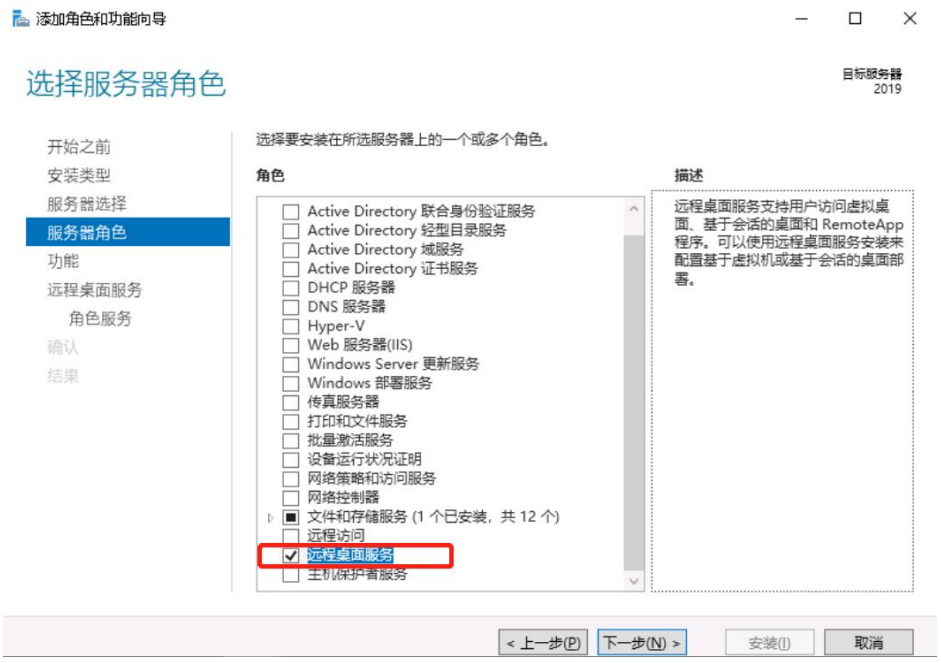
步骤 4 在服务器池中选择目标服务器。

图13-68 选择服务器



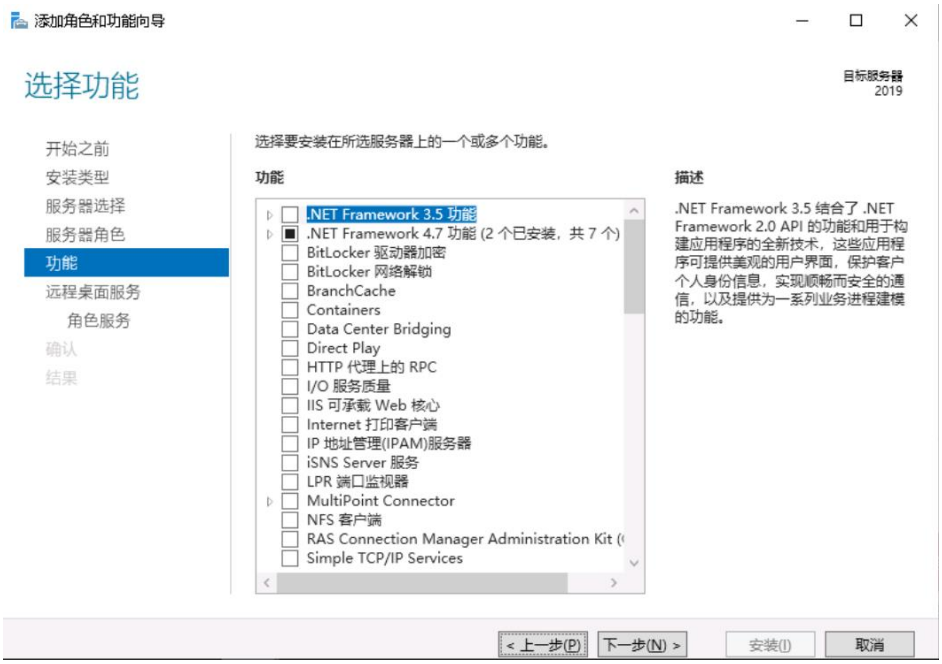
步骤 5 在服务器角色窗口中，勾选“Active Directory 域服务”、“DNS 服务器”、“远程桌面服务”三个角色项。

图13-69 选择服务器角色



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。

图13-70 选择其他功能



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。

图13-71 选择 IIS 服务角色

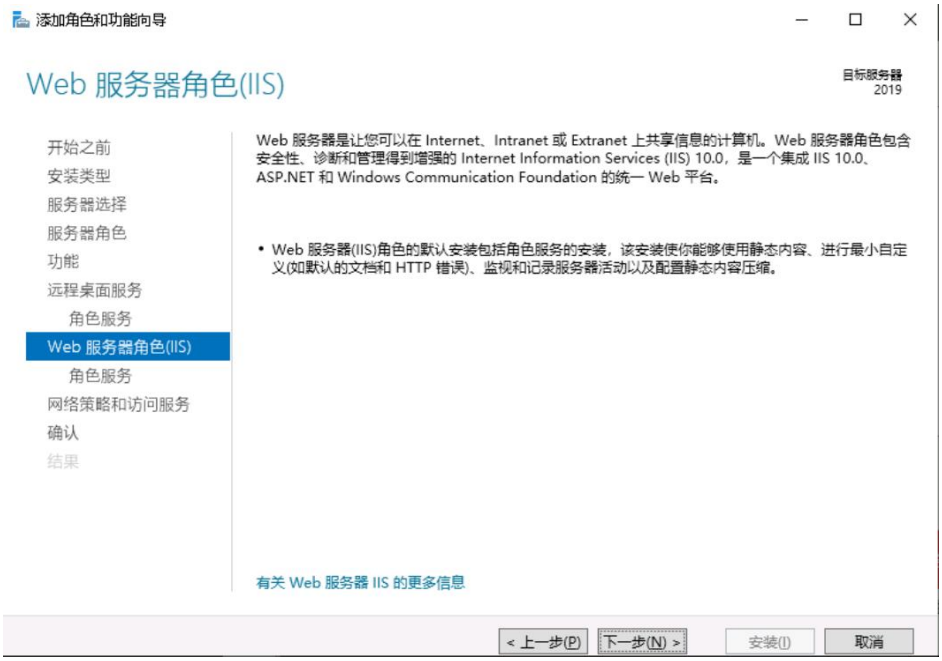
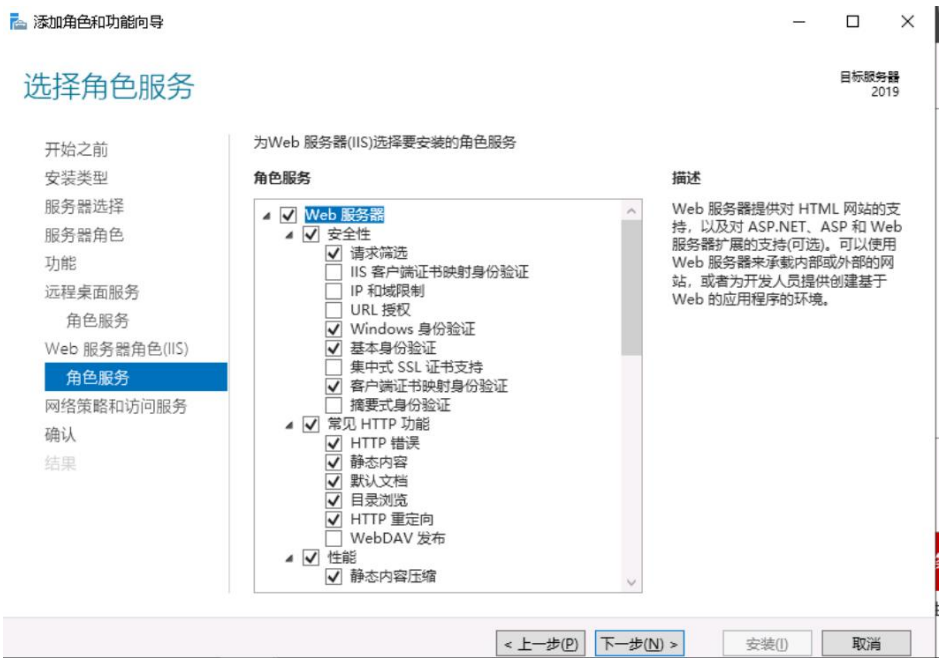


图13-72 选择服务角色

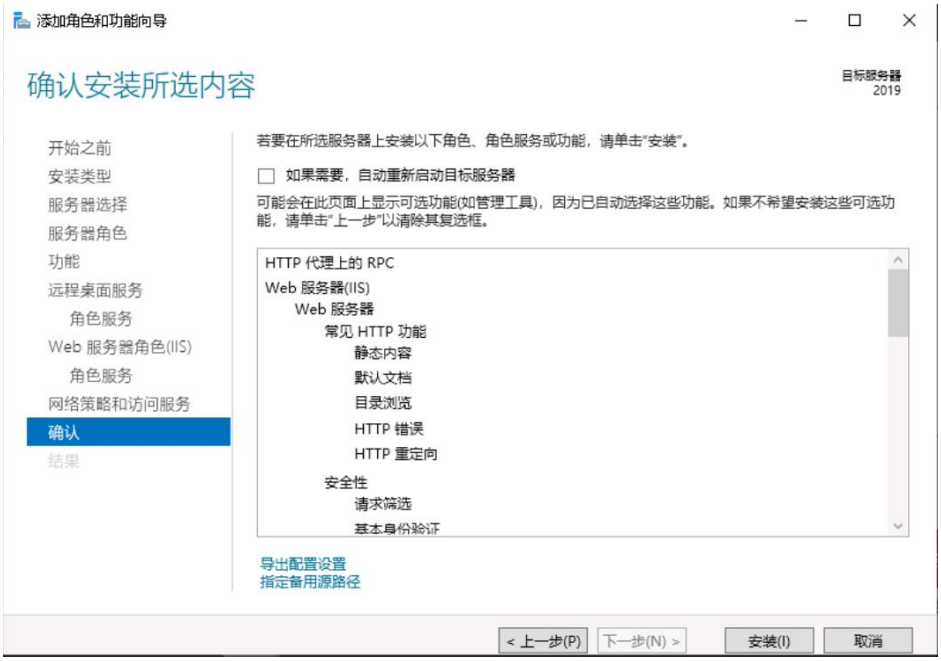


步骤 9 （可选）选择“网络策略和访问服务 ”，进入选择网络策略和访问服务窗口，默认勾选“网络策略服务器”选项。

图13-73 选择网络策略和访问服务

步骤 10 确认配置选择，单击“安装”，请耐心等待安装进度完成。

图13-74 安装服务器角色



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

13.3.2 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 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”。

图13-75 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。

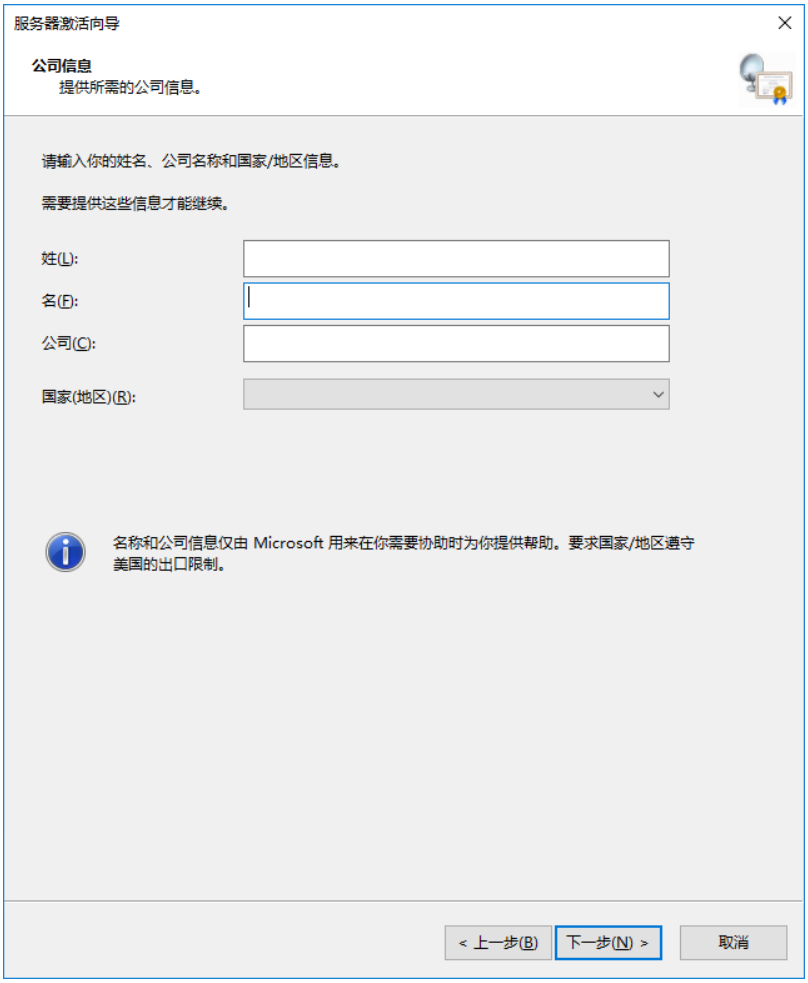
图13-76 打开服务器激活向导

步骤 4 选择自动连接方式。

图13-77 选择自动连接

步骤 5 输入公司名称和用户姓名。

图13-78 输入相关信息



步骤 6 （可选）输入公司详细通讯信息。

图13-79 输入公司详细信息

步骤 7 确认安装启动许可证安装向导。

图13-80 确认许可证安装向导

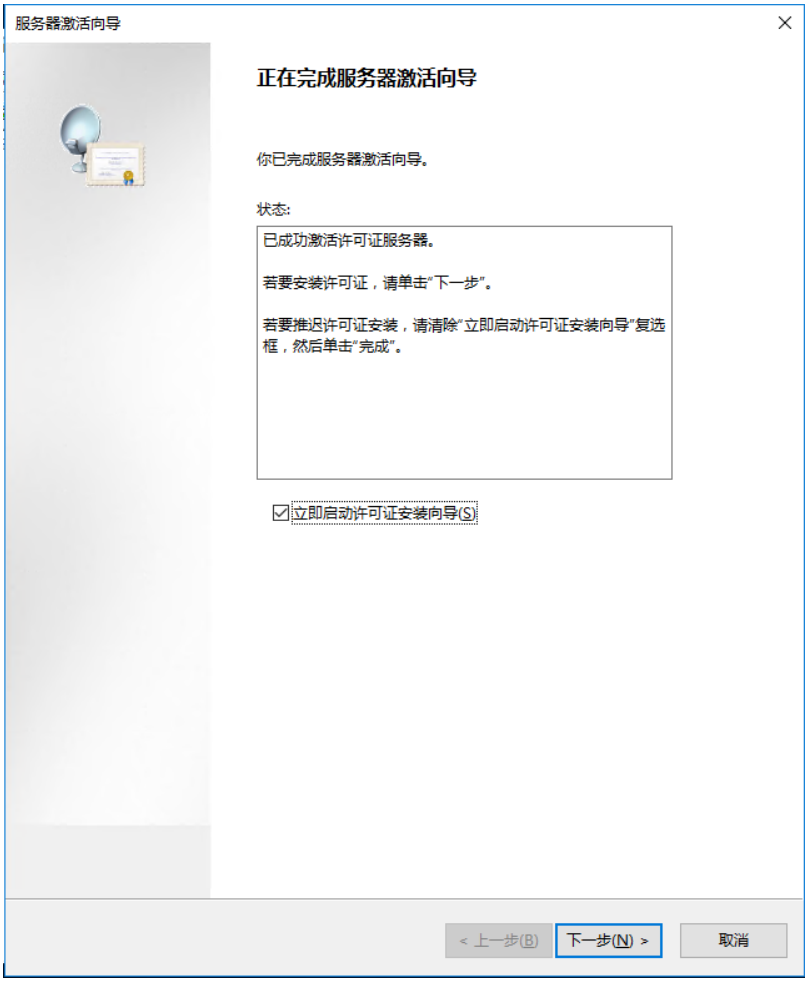


图13-81 启用许可证安装向导

步骤 8 许可证计划选择“企业协议”。

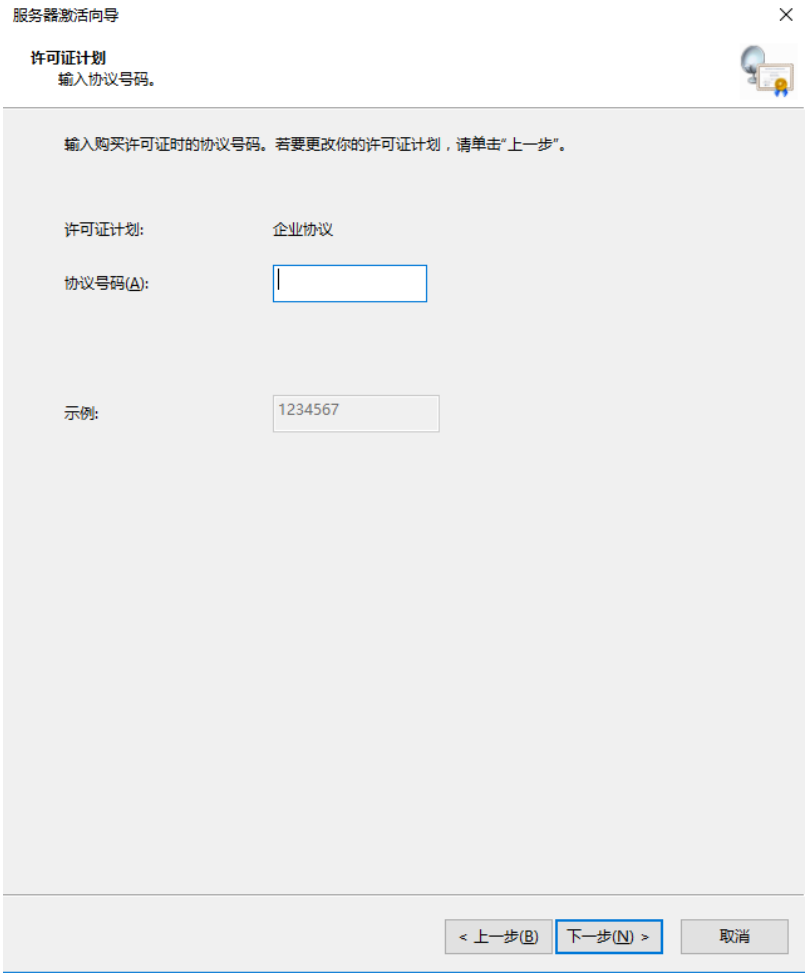
图13-82 选择许可证计划

步骤 9 输入企业协议号码。

说明

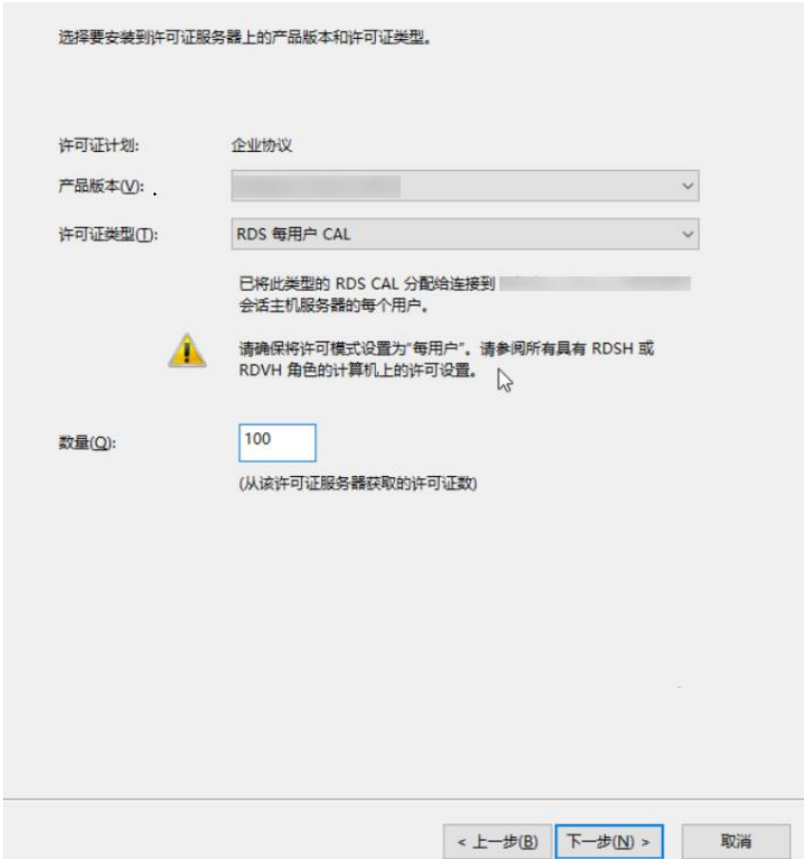
企业协议号码需提前向第三方平台申购获取官方远程桌面授权许可。

图13-83 输入协议号码



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。

图13-84 选择服务器版本



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。

图13-85 成功安装许可证

----结束

13.3.3 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。

图13-86 打开组策略

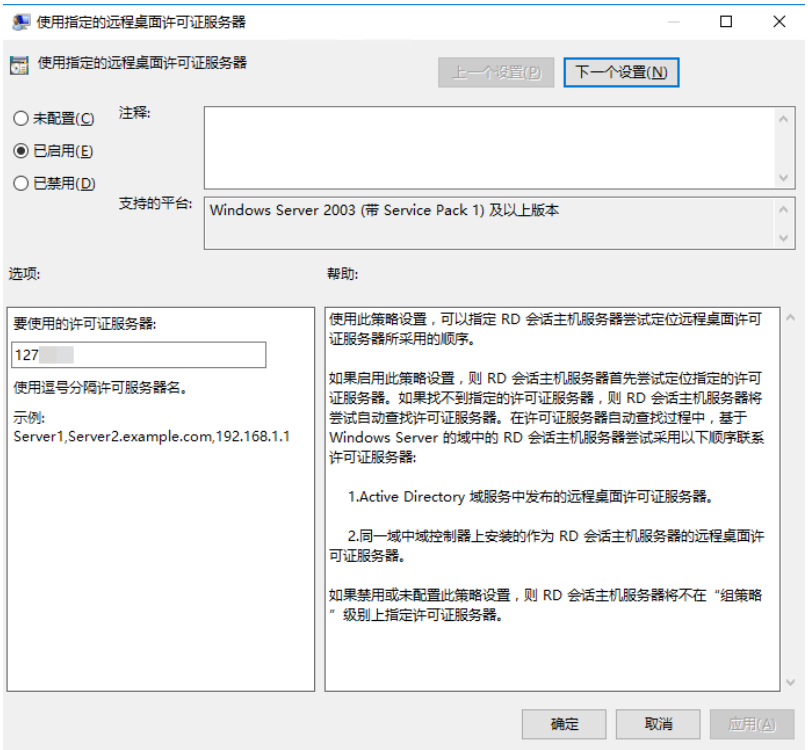
使用指定的远程桌面许可证服务器

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。

图13-87 使用指定许可证服务器



----结束

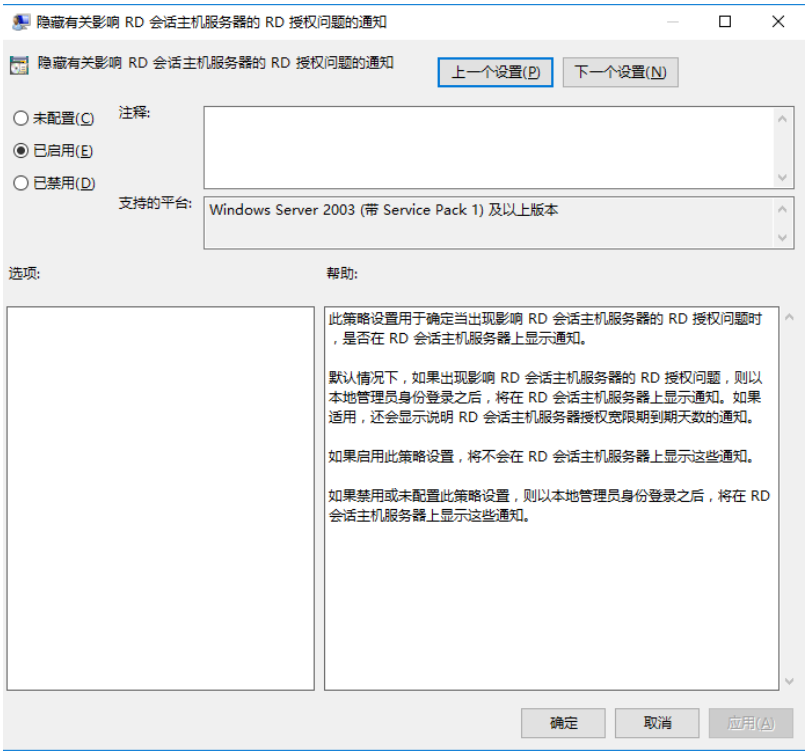
隐藏有关影响 RD 会话主机服务器的 RD 授权问题的通知

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。

图13-88 隐藏 RD 授权问题的通知



----结束

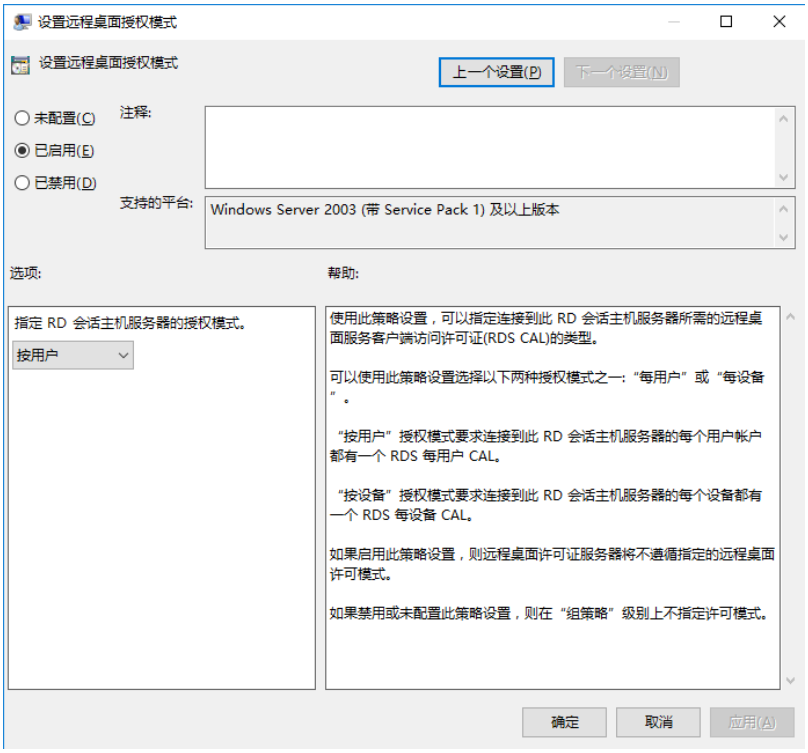
设置远程桌面授权模式

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。

图13-89 设置远程桌面授权模式



----结束

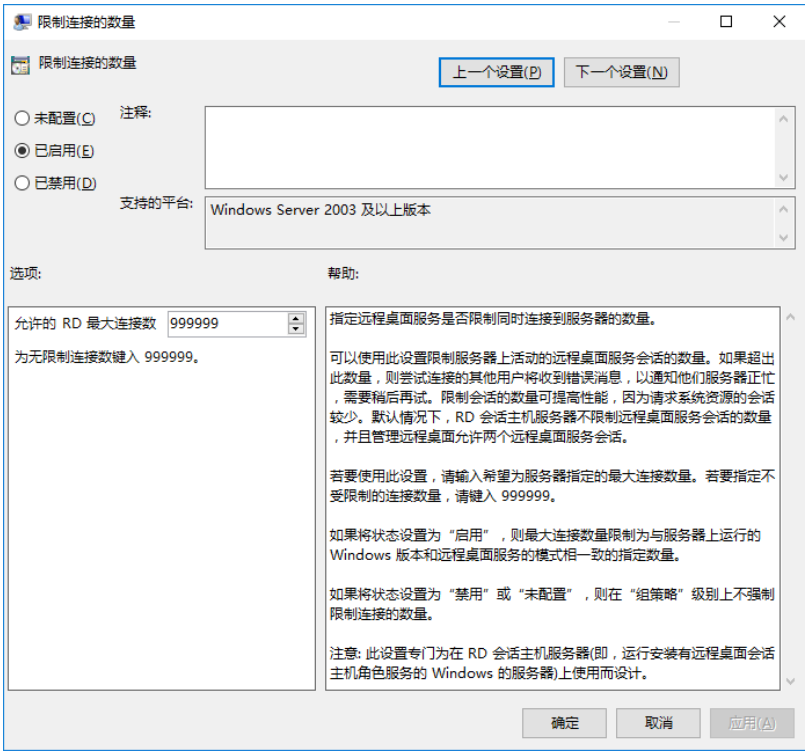
限制连接的数量

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 最大连接数位 999999。

步骤 3 单击“确定”，完成设置。

图13-90 限制连接的数量



----结束

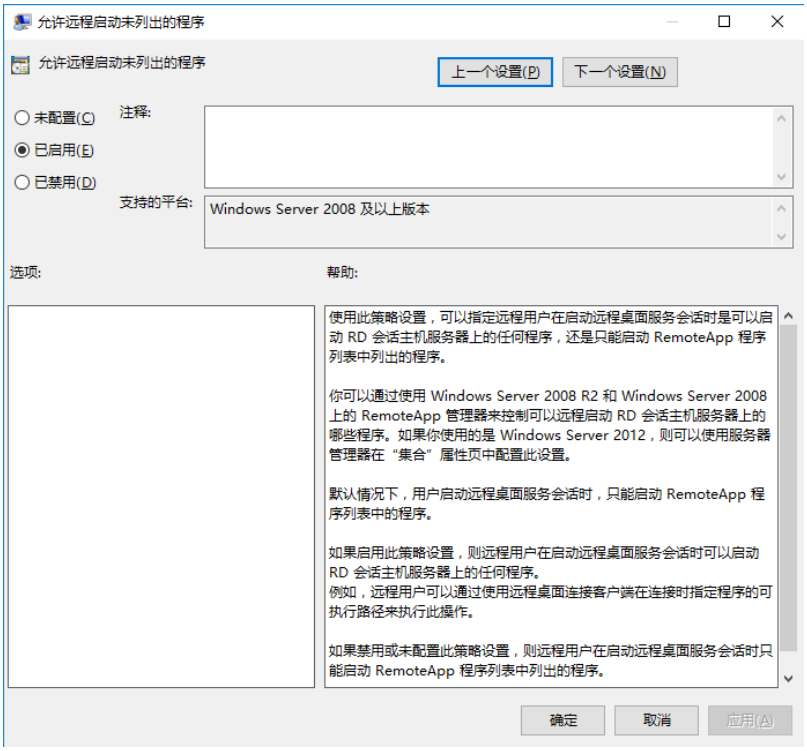
允许远程启动未列出的程序

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。

图13-91 允许远程启动未列出的程序



----结束

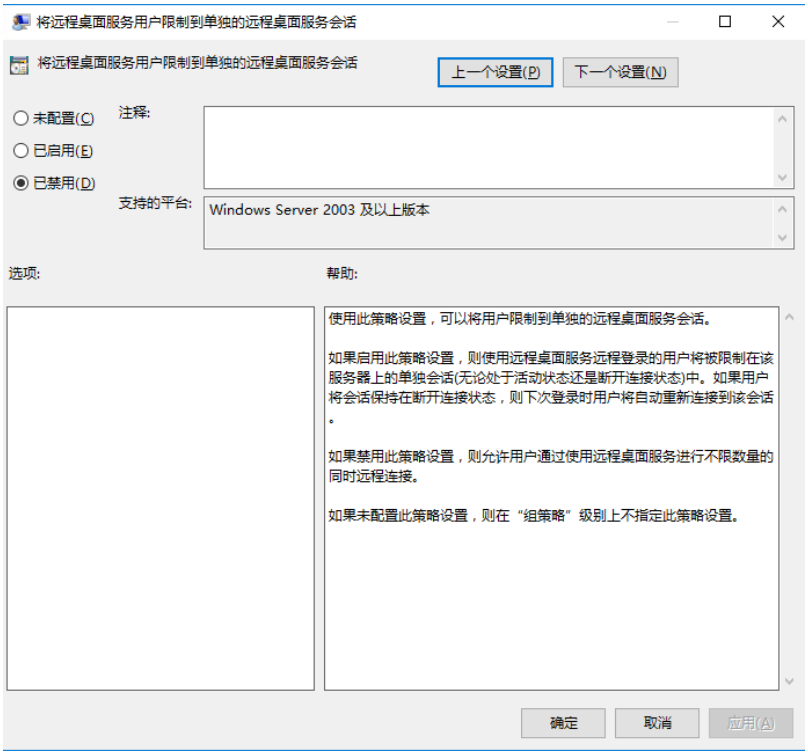
将远程桌面服务用户限制到单独的远程桌面服务会话

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。

图13-92 将远程桌面服务用户限制到单独的远程桌面服务会话



----结束

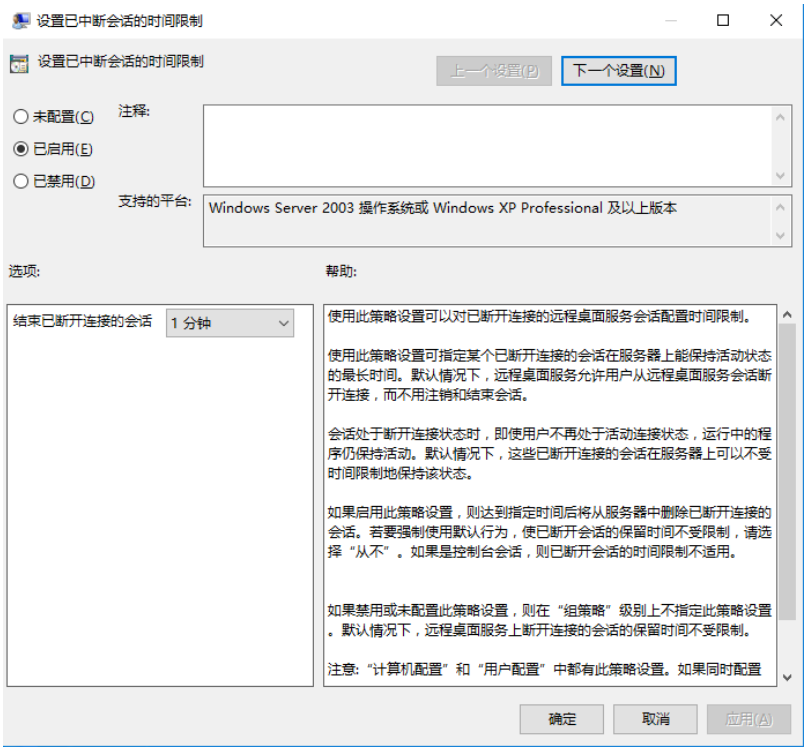
设置已中断会话的时间限制

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。

图13-93 设置已中断会话的时间限制



----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。

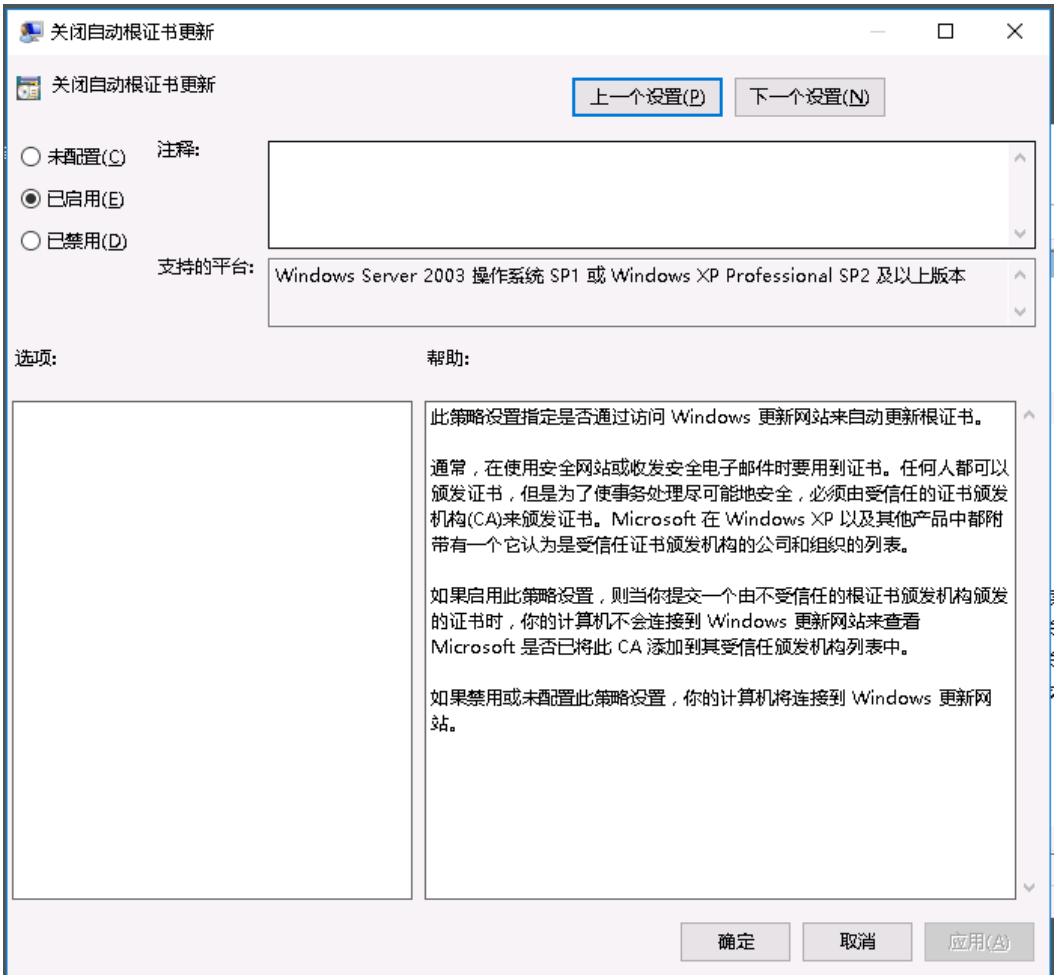
步骤 1 选择“管理模板 > 系统 > Internet 通信管理”，进入“Internet 通信管理”页面。

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。

图13-94 关闭自动根证书更新



----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。

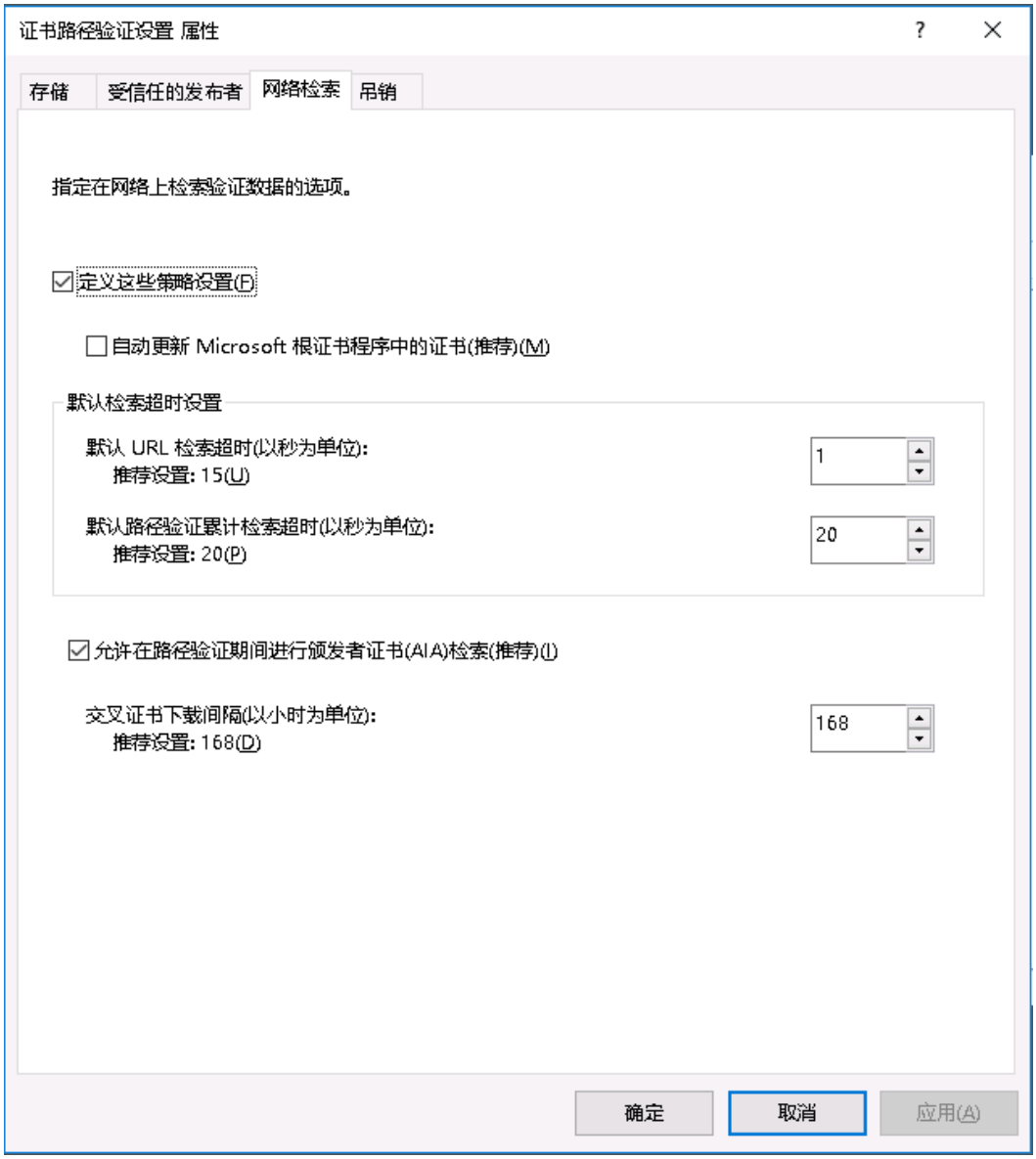
步骤 3 选择“网络检索”页签。

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。

图13-95 证书路径验证设置



----结束

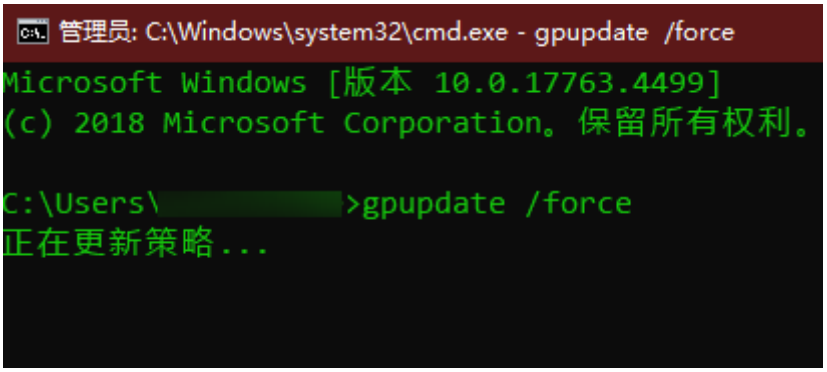
刷新本地组策略

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云堡垒机。

图13-96 刷新本地组策略



----结束

13.4 安装 Windows Server 2008 R2 应用服务器

13.4.1 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

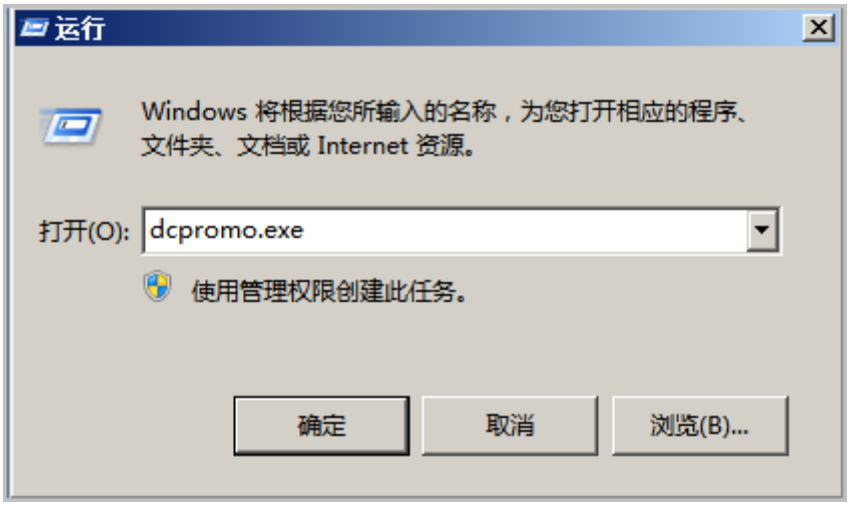
13.4.2 安装 AD 域

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。

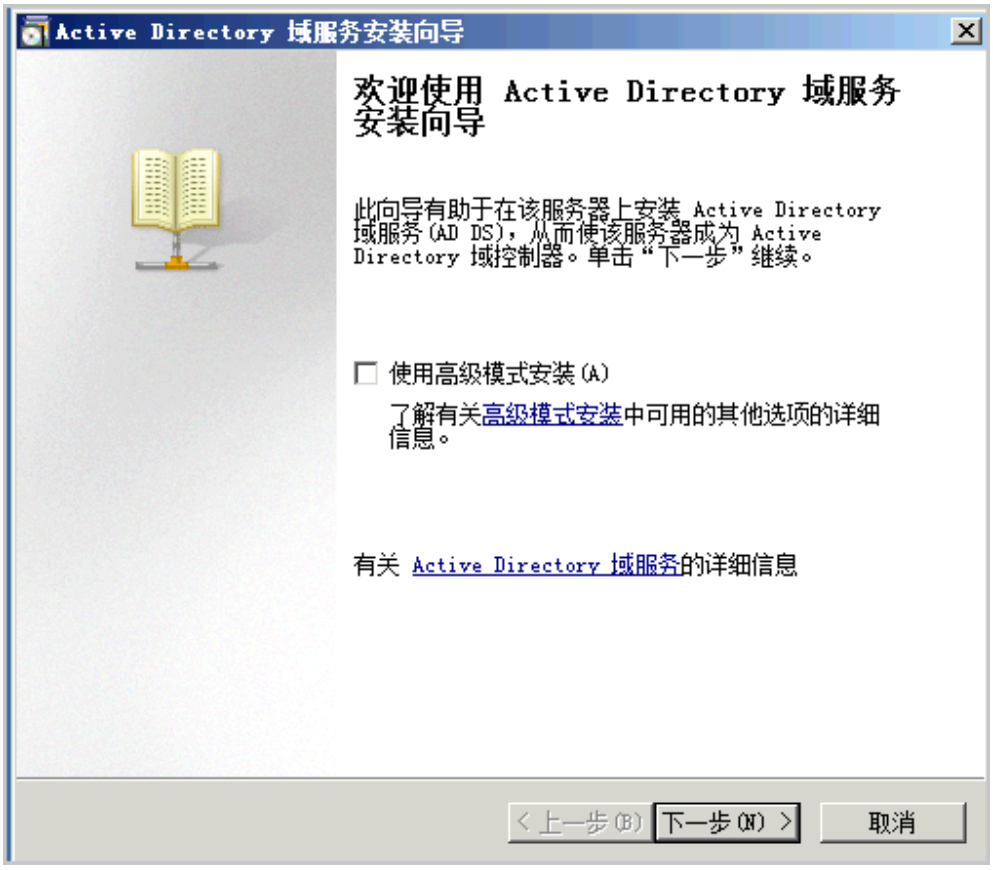
安装 AD 域

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。

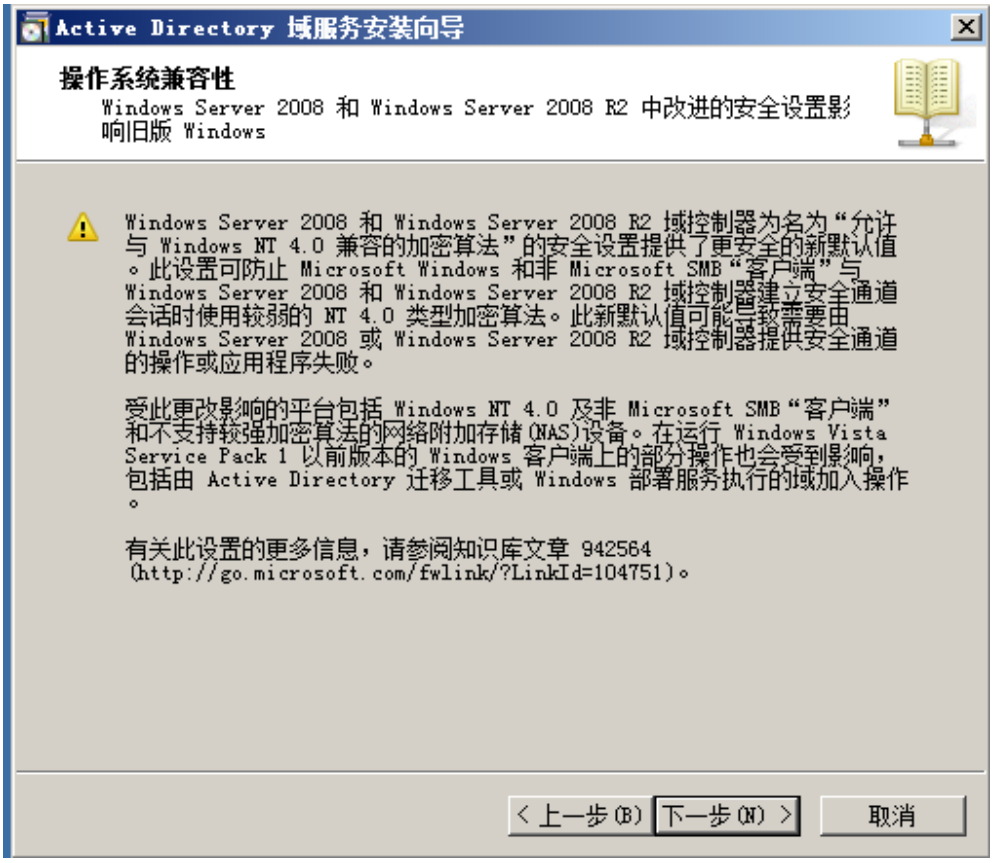


AD 域服务安装向导

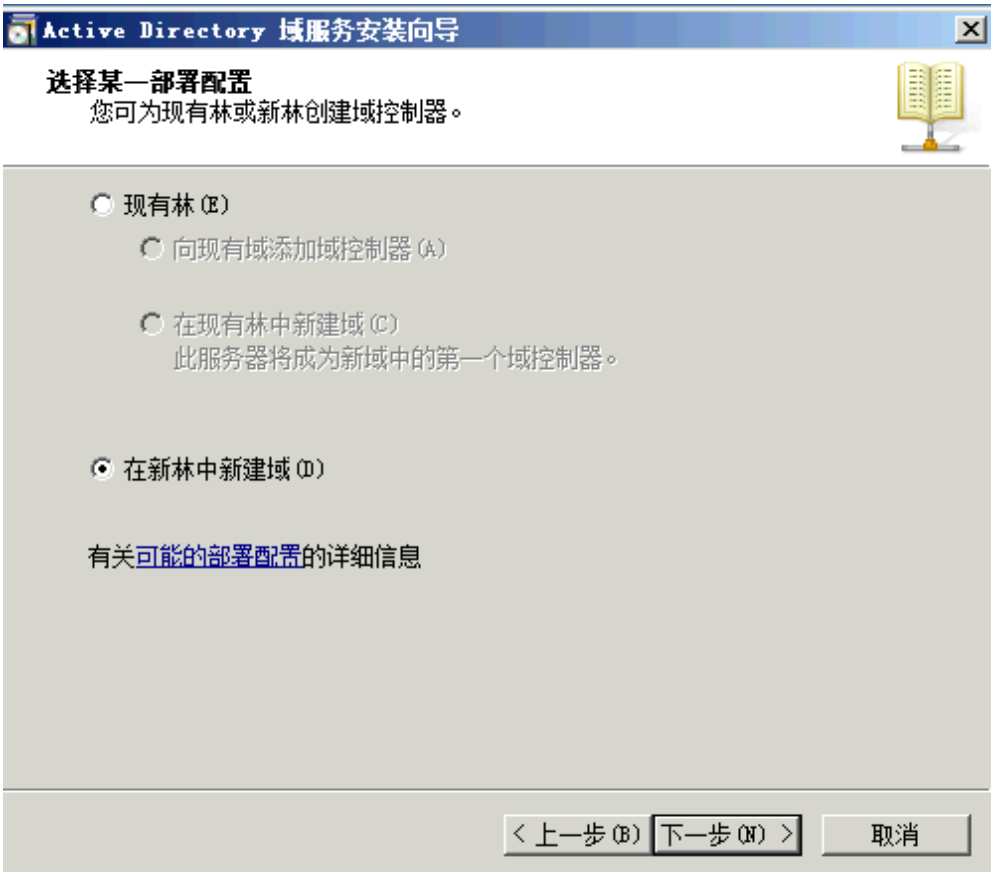
步骤 1 安装 AD 域，单击“下一步”。


Active Directory 域服务安装向导
欢迎使用 Active Directory 域服务安装向导
此向导有助于在该服务器上安装 Active Directory 域服务(AD DS)，从而使该服务器成为 Active Directory 域控制器。单击“下一步”继续。
使用高级模式安装(A)
了解有关高级模式安装中可用的其他选项的详细信息。
有关 Active Directory 域服务的详细信息
< 上一步(B)
下一步(N) >
取消

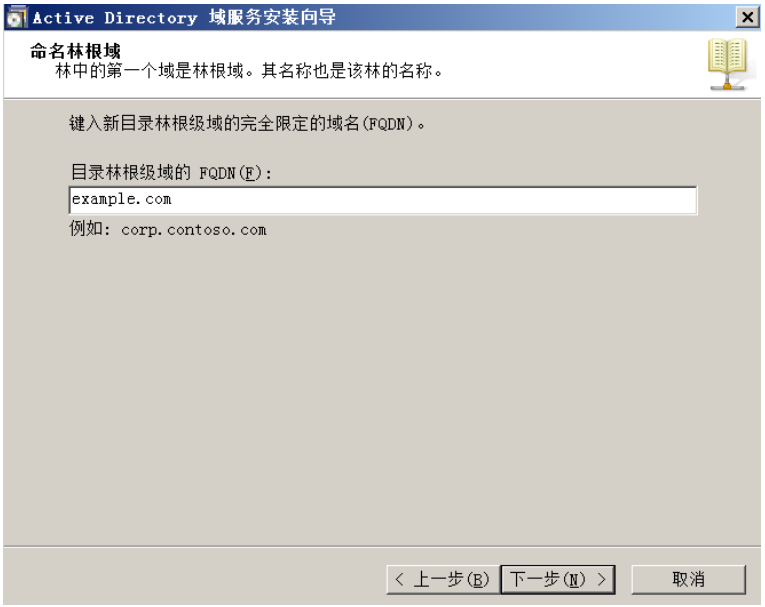
步骤 2 单击“下一步”。


Active Directory 域服务安装向导
操作系统兼容性
Windows Server 2008 和 Windows Server 2008 R2 中改进的安全设置影响旧版 Windows
Windows Server 2008 和 Windows Server 2008 R2 域控制器为名为“允许与 Windows NT 4.0 兼容的加密算法”的安全设置提供了更安全的新默认值。此设置可防止 Microsoft Windows 和非 Microsoft SMB“客户端”与 Windows Server 2008 和 Windows Server 2008 R2 域控制器建立安全通道会话时使用较弱的 NT 4.0 类型加密算法。此新默认值可能导致需要由 Windows Server 2008 或 Windows Server 2008 R2 域控制器提供安全通道的操作或应用程序失败。
受此更改影响的平台包括 Windows NT 4.0 及非 Microsoft SMB“客户端”和不支持较强加密算法的网络附加存储(NAS)设备。在运行 Windows Vista Service Pack 1 以前版本的 Windows 客户端上的部分操作也会受到影响，包括由 Active Directory 迁移工具或 Windows 部署服务执行的域加入操作。
有关此设置的更多信息，请参阅知识库文章 942564 (http://go.microsoft.com/fwlink/?LinkId=104751)。
< 上一步(B)
下一步(N) >
取消

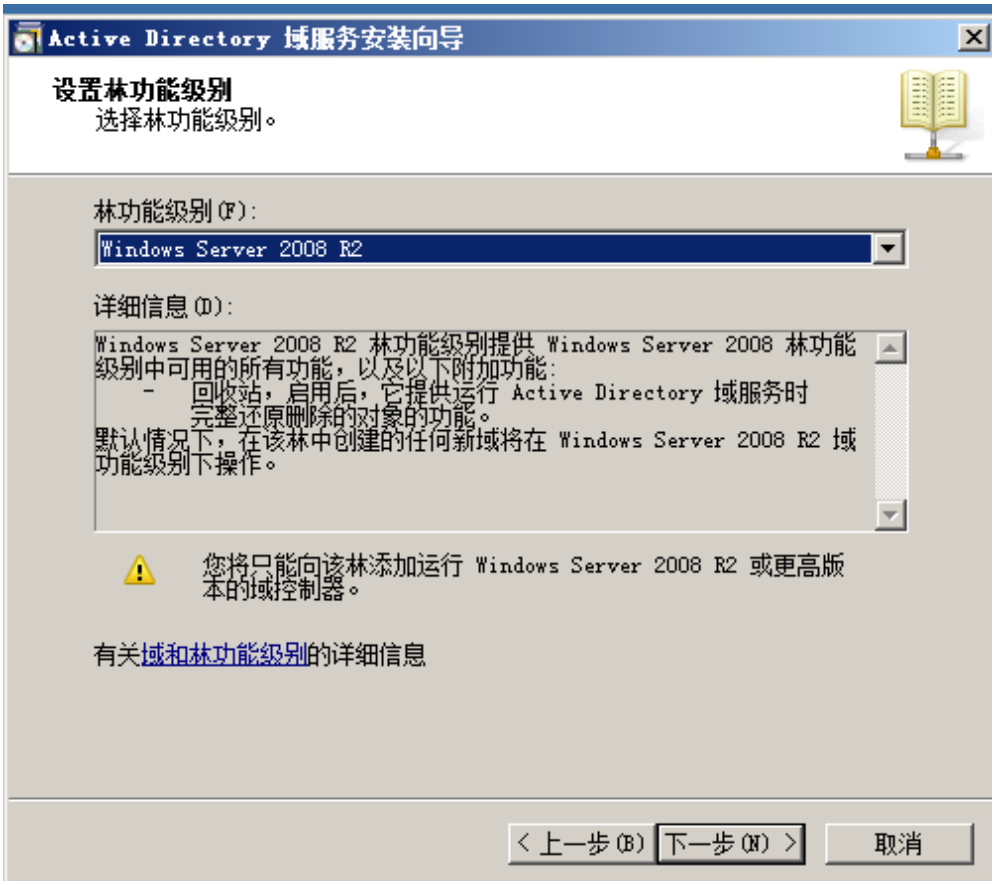
步骤 3 选择“在新林中新建域”，单击“下一步”。



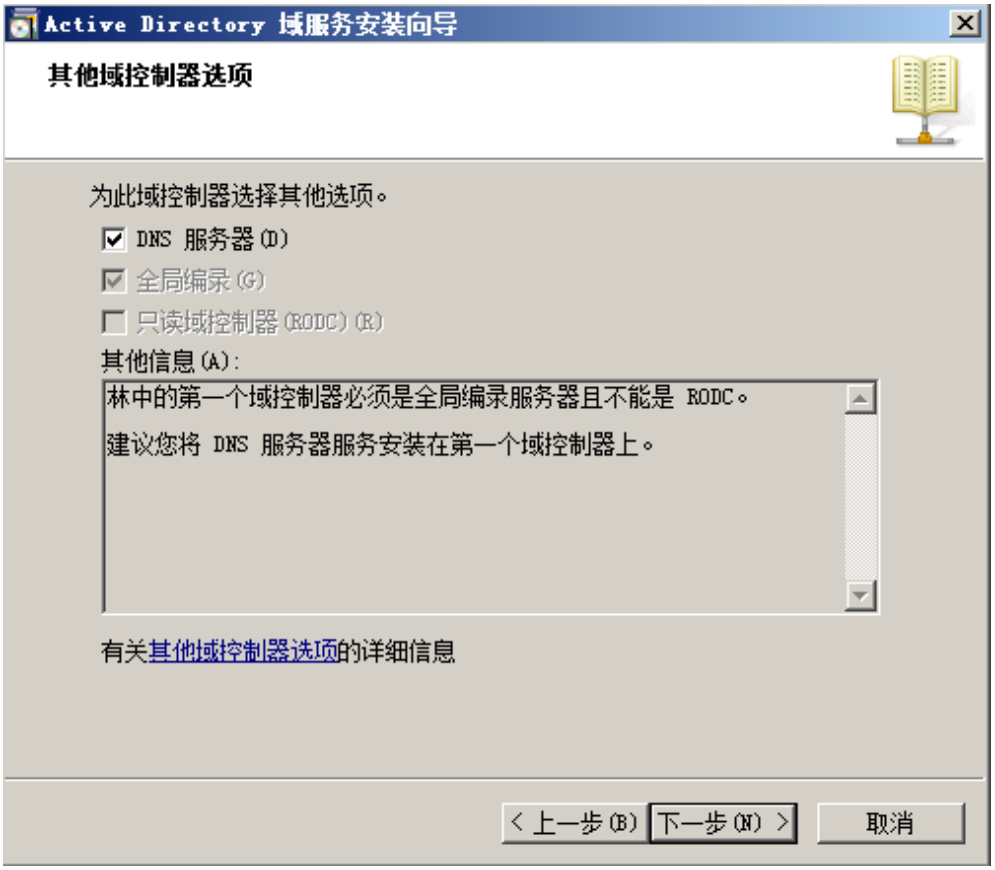
步骤 4 单击“下一步”。



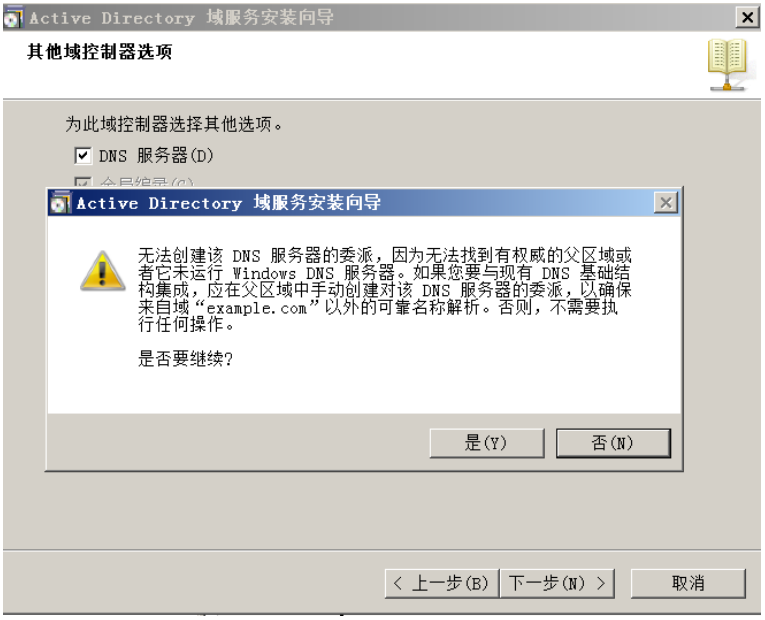
步骤 5 设置林功能级别，在下拉菜单中选择“Windows Server 2008 R2”，单击“下一步”。



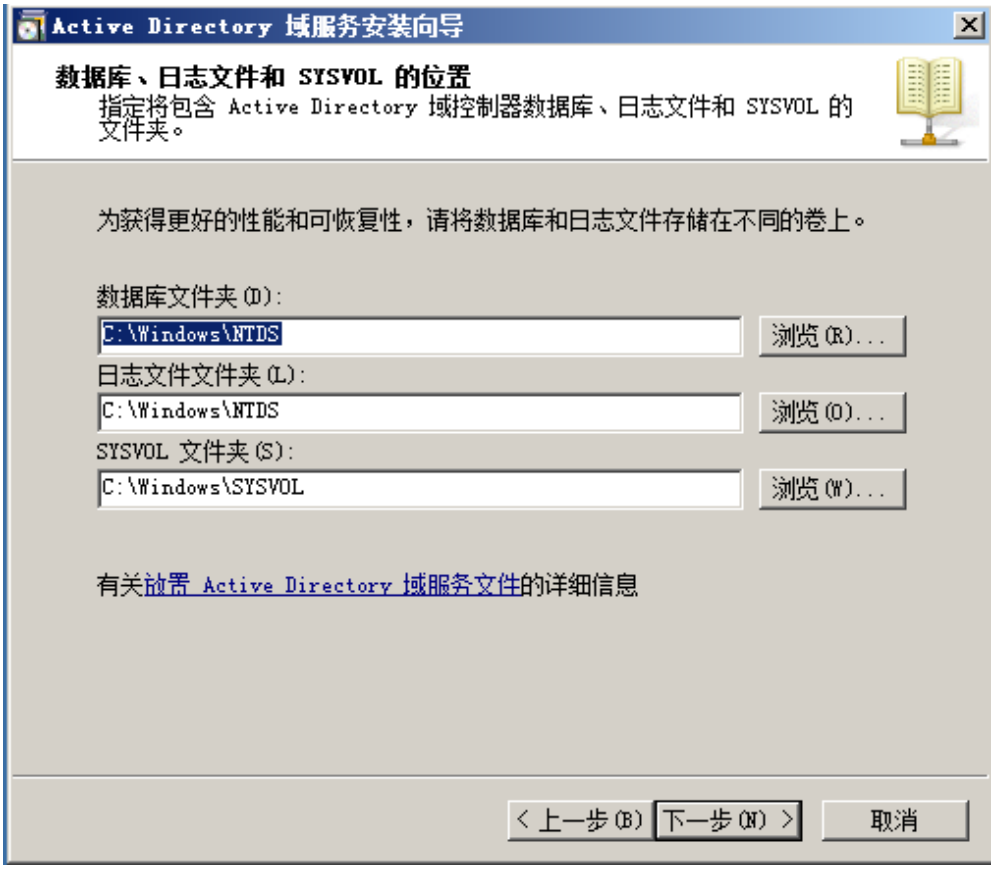
步骤 6 勾选“DNS 服务器”，单击“下一步”。



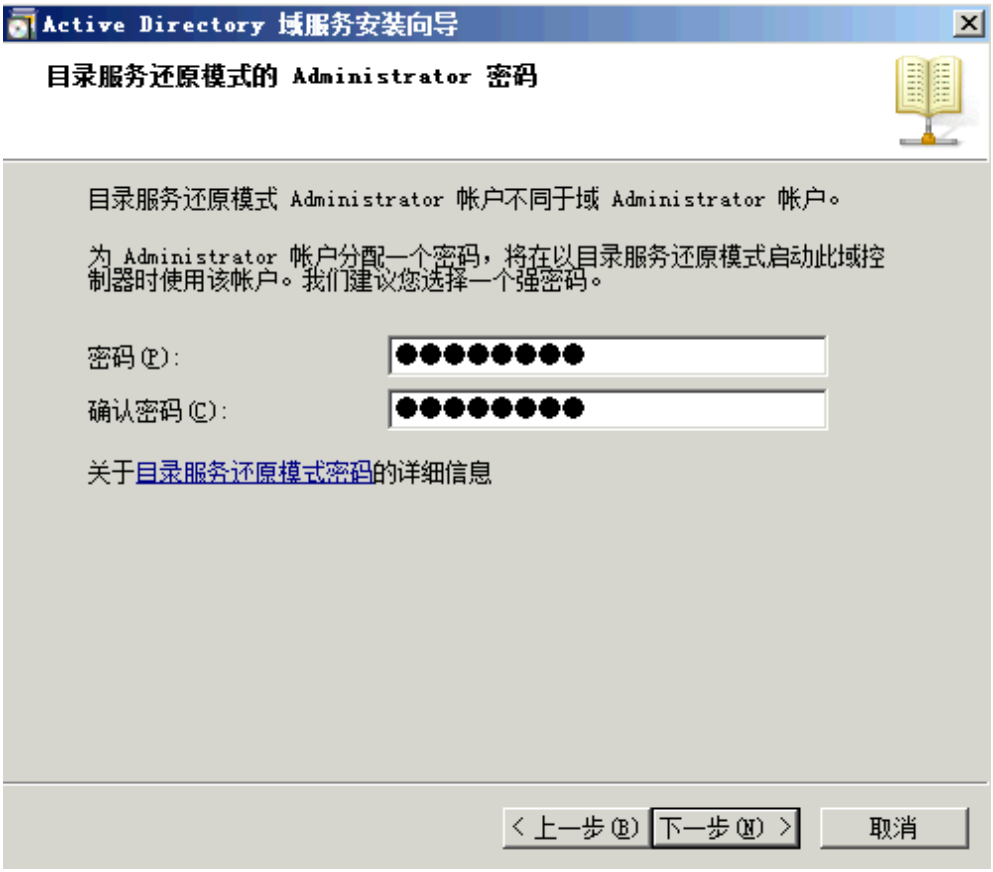
步骤 7 界面显示“无法创建 DNS 委派”，单击“是”，然后继续。



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”。



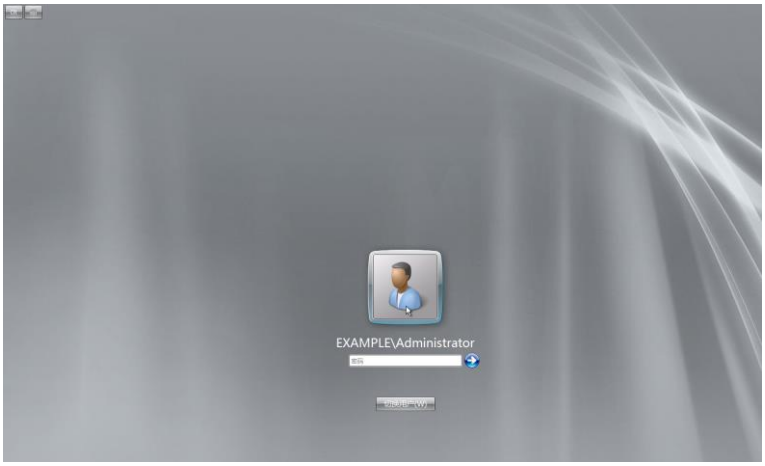
步骤 9 设置目录还原模式的密码，还原模式的 **Administrator** 密码不等于系统密码，单击“下一步”。



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，用域用户登录。



步骤 13 AD 域环境安装完成。

----结束

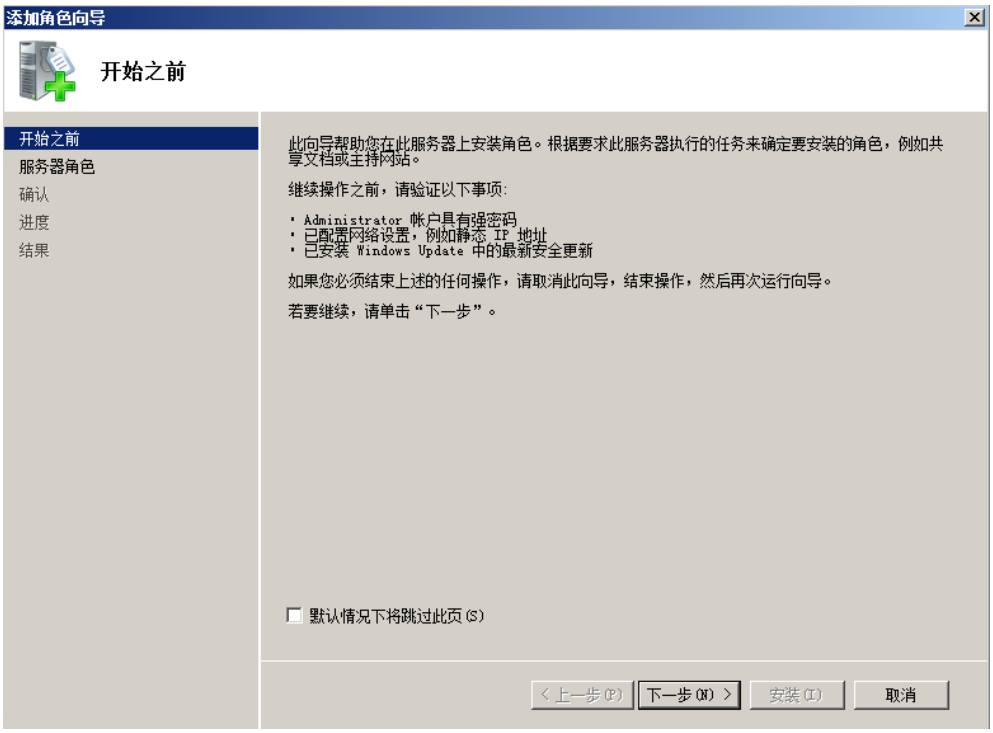
13.4.3 安装远程桌面服务和 RD 授权

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”。

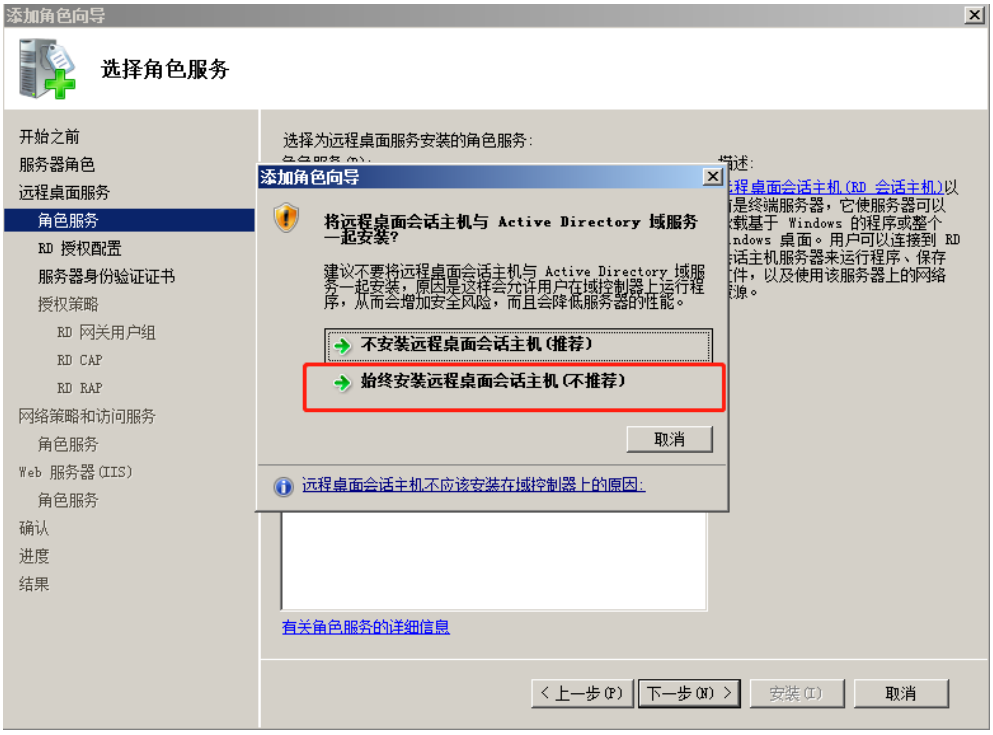
步骤 2 勾选“远程桌面服务”，单击“下一步”。

步骤 3 单击“下一步”。

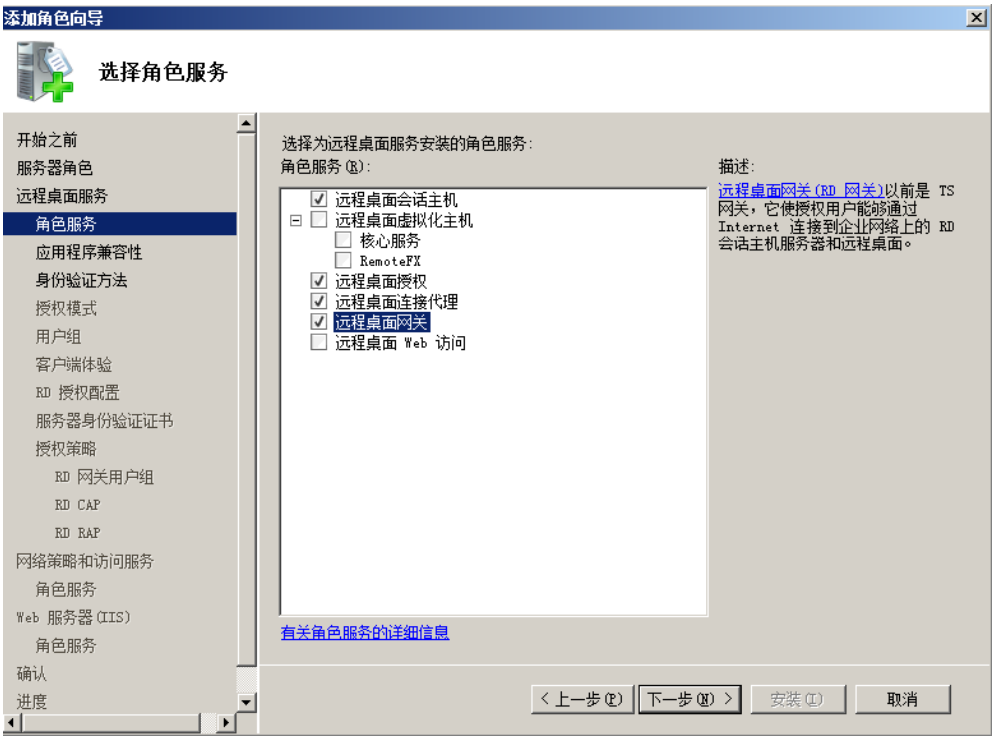


步骤 4 单击“下一步”。

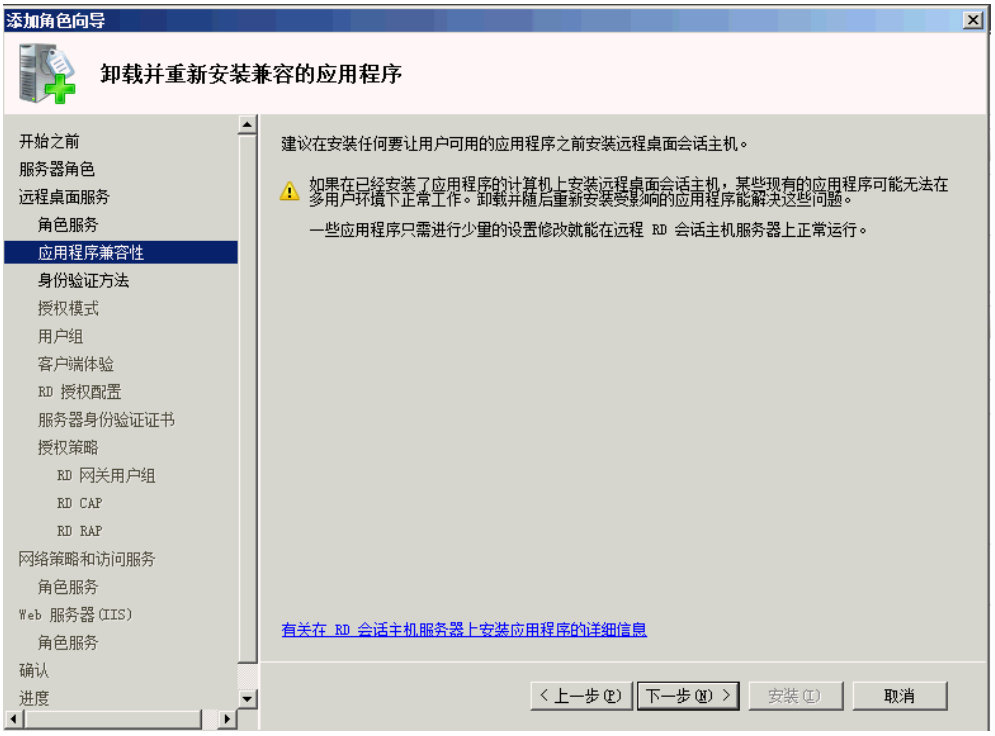
步骤 5 选择“始终安装远程桌面会话主机”，单击“下一步”。



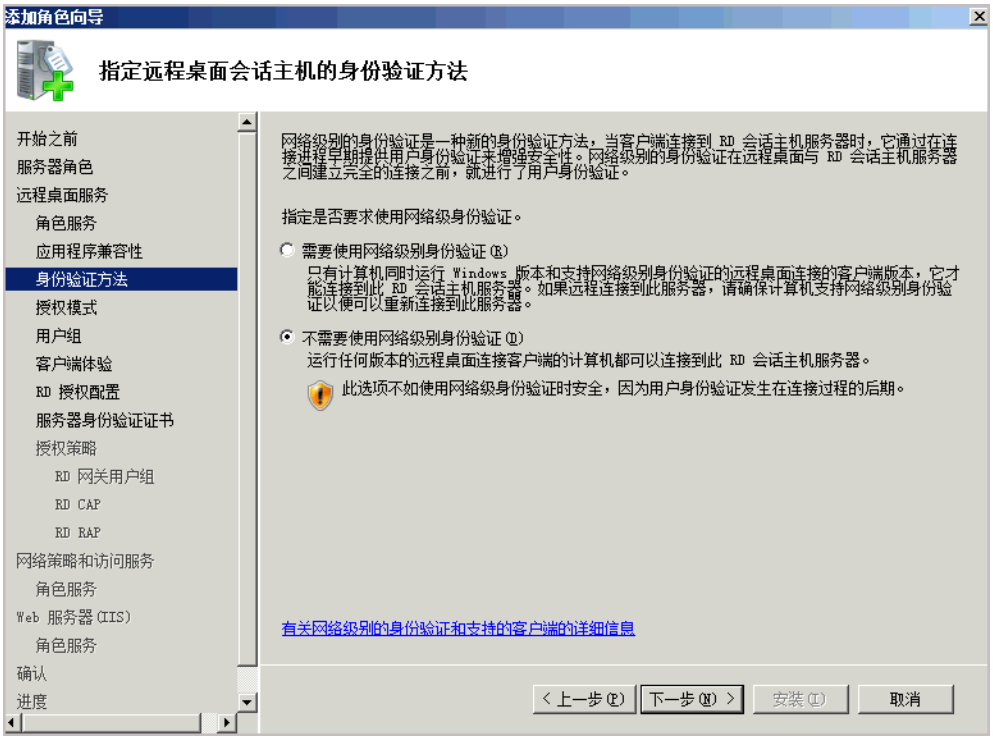
步骤 6 选择“角色服务”，勾选“远程桌面会话主机”和“远程桌面授权”，单击“下一步”。



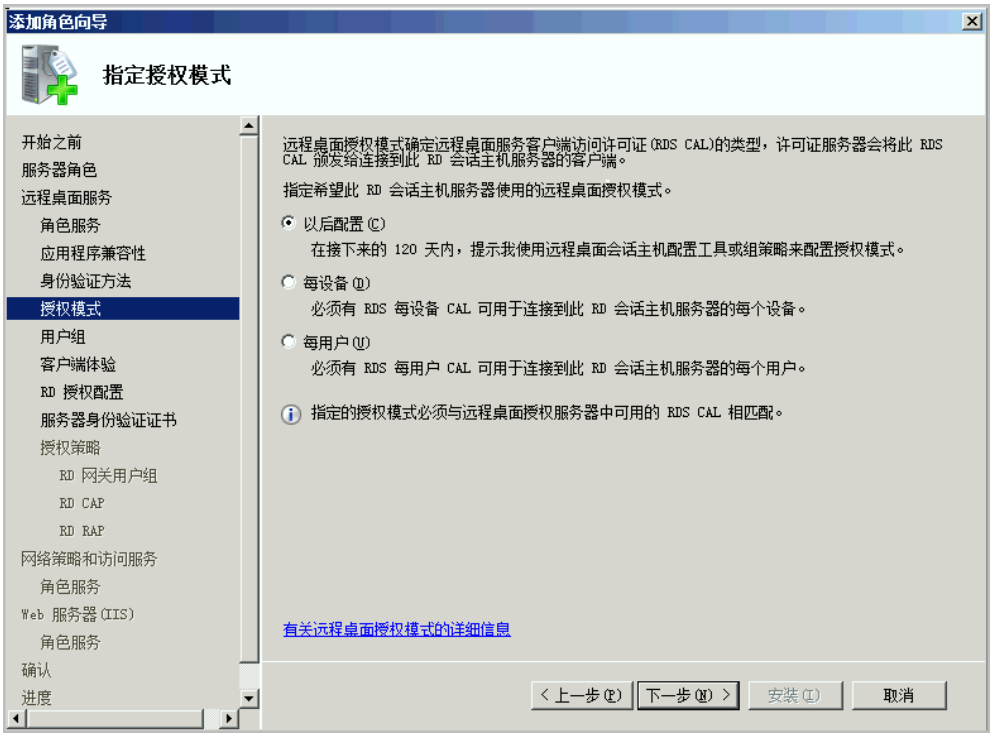
步骤 7 单击“下一步”。



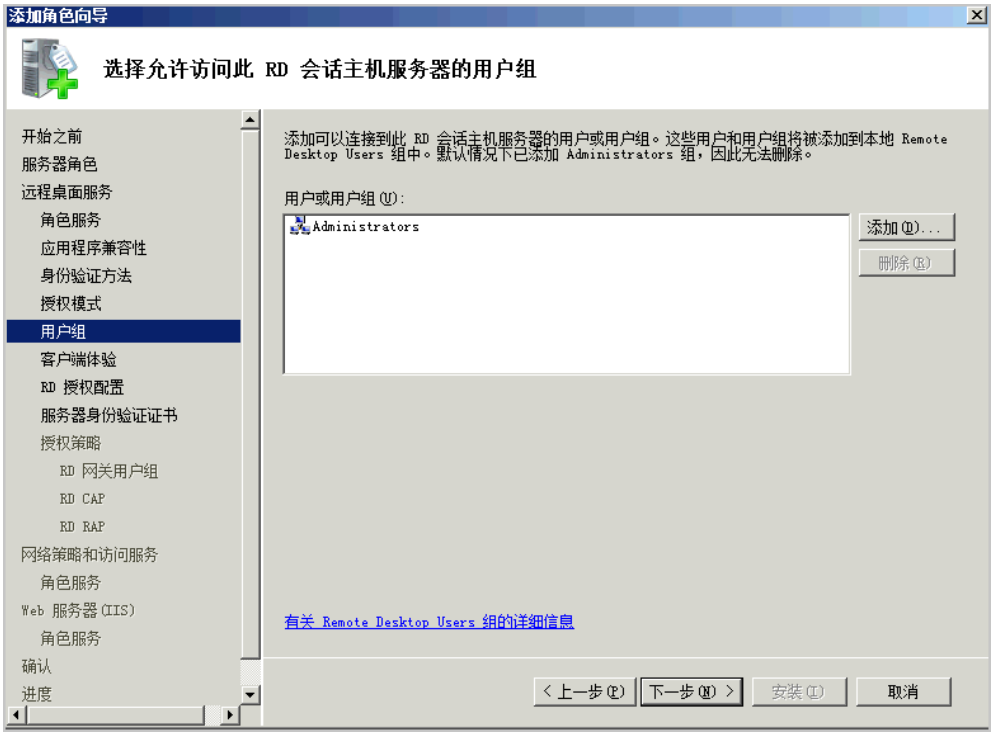
步骤 8 选择“不需要使用网络级别身份认证”，单击“下一步”。



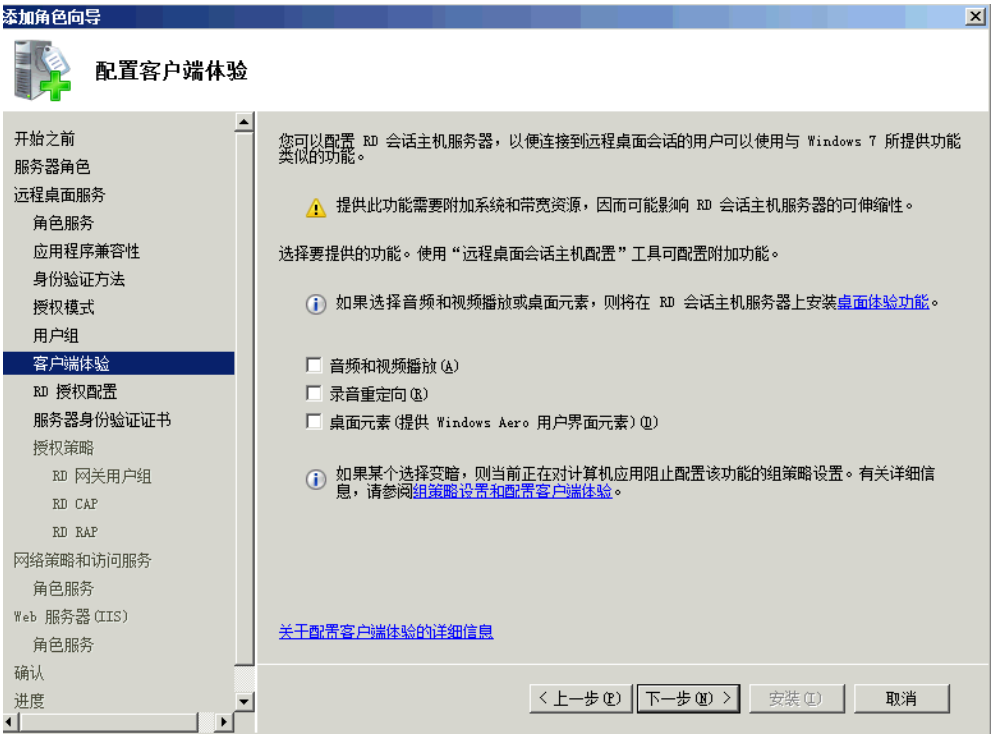
步骤 9 选择“以后配置”，单击“下一步”。



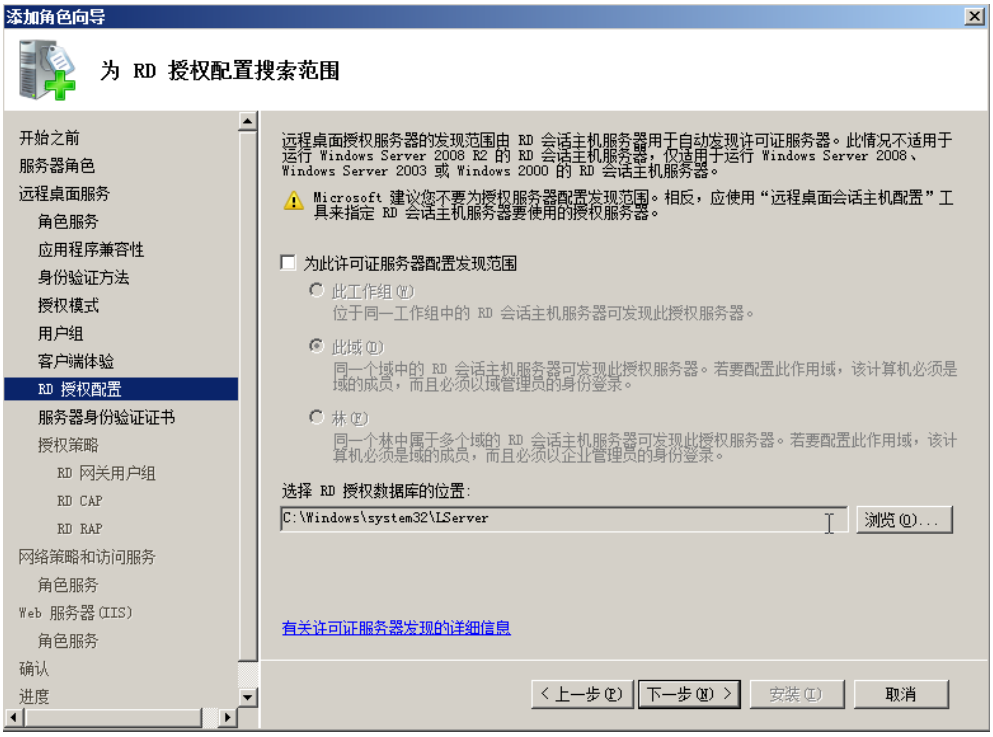
步骤 10 界面默认显示的“Administrators”能够连接到 RD 会话主机服务器（如果有特别需要，请添加需要的用户或组），单击“下一步”。



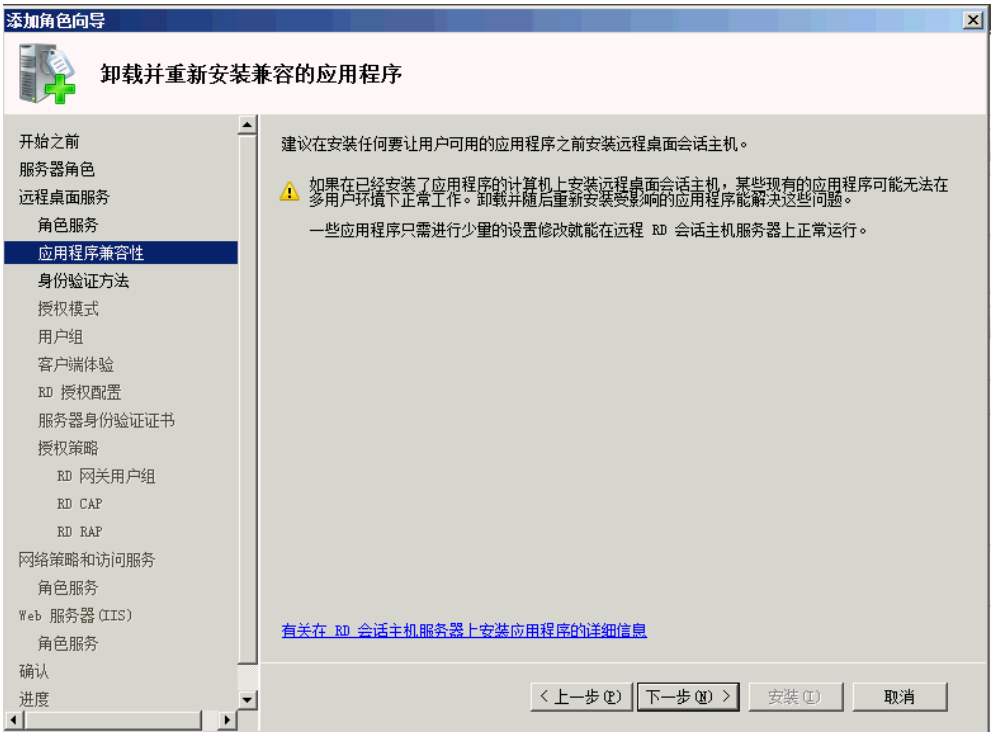
步骤 11 单击“下一步”。



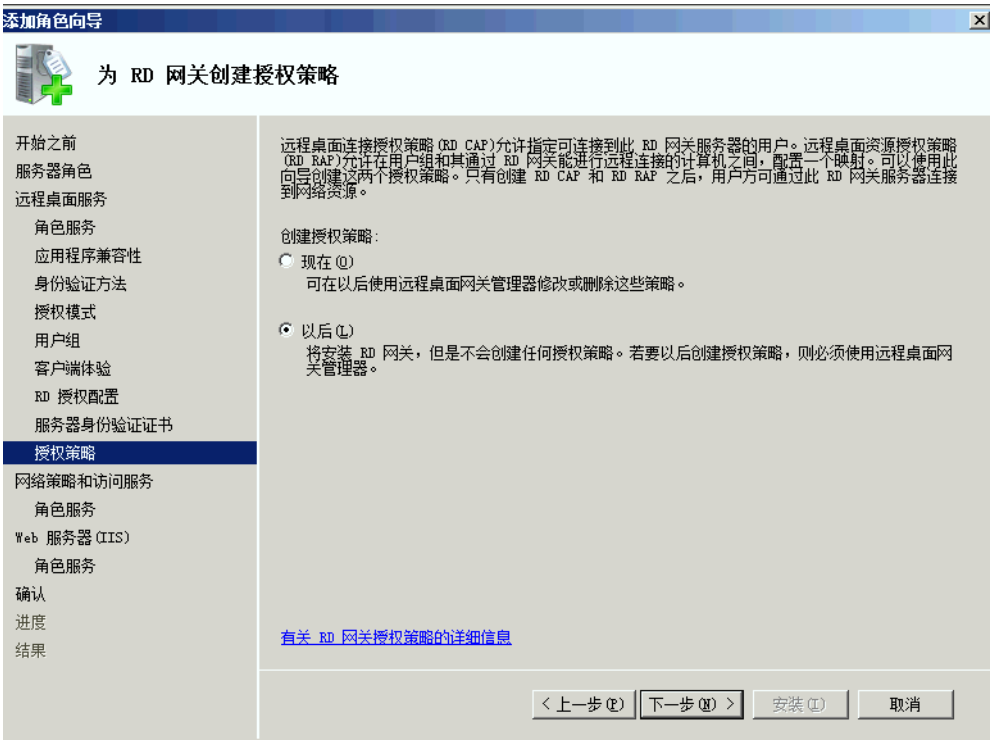
步骤 12 单击“下一步”。



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”。

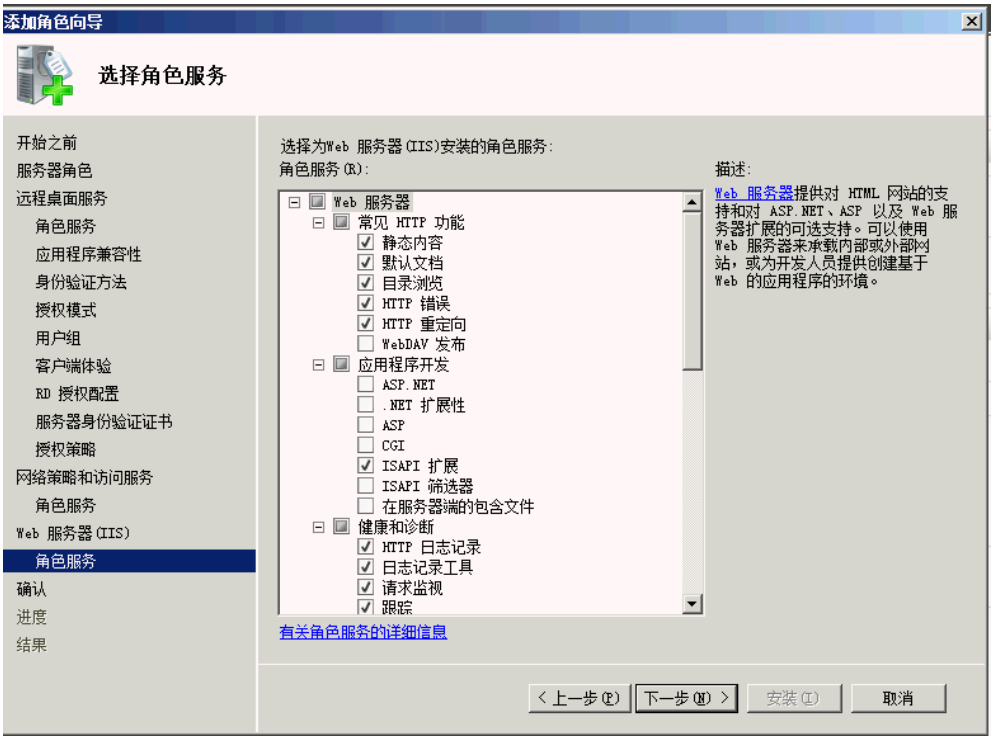


步骤 15 默认，单击“下一步”。

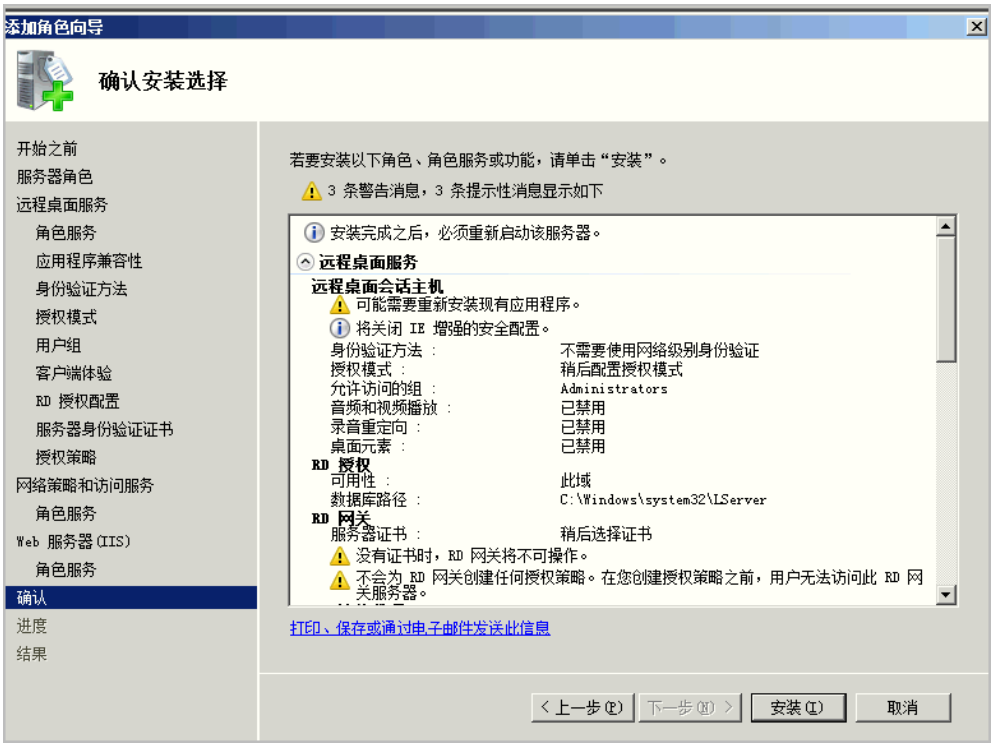
步骤 16 选择“角色服务”，勾选“网络策略服务器”，单击“下一步”。

步骤 17 安装 IIS，单击“下一步”。

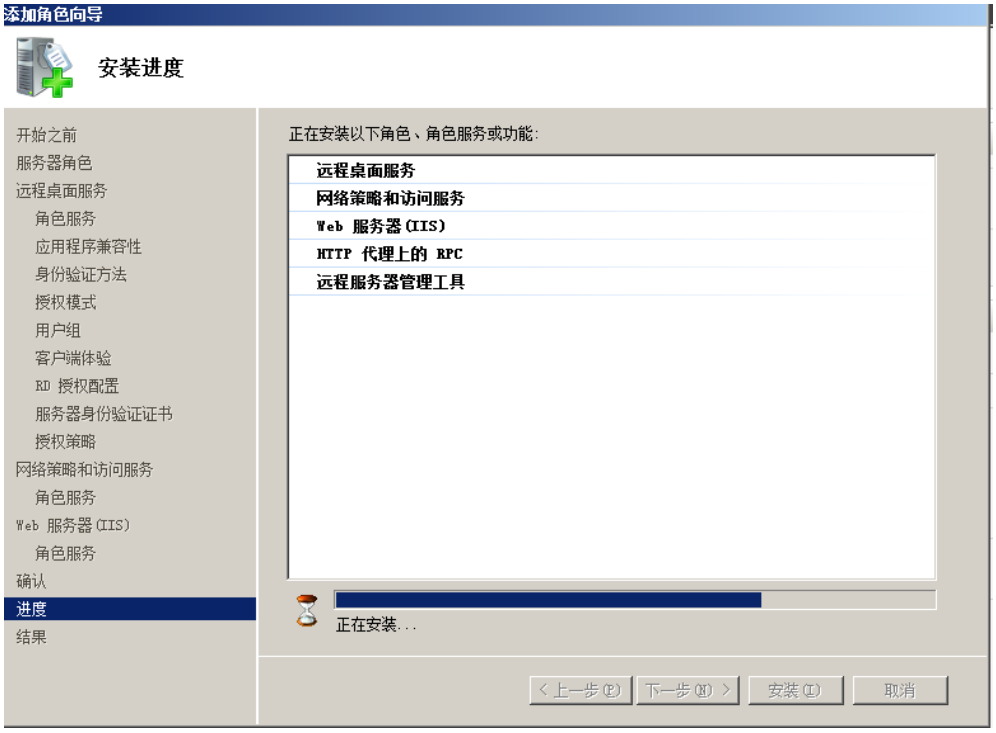
步骤 18 默认，单击“下一步”。



步骤 19 默认，单击“安装”。



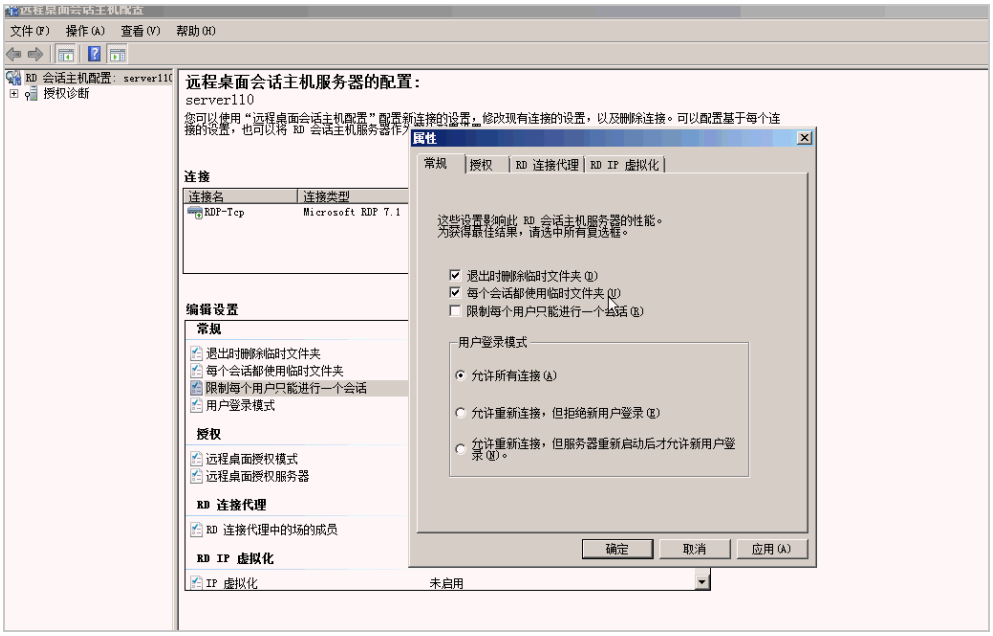
步骤 20 界面显示安装过程，请等待。



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

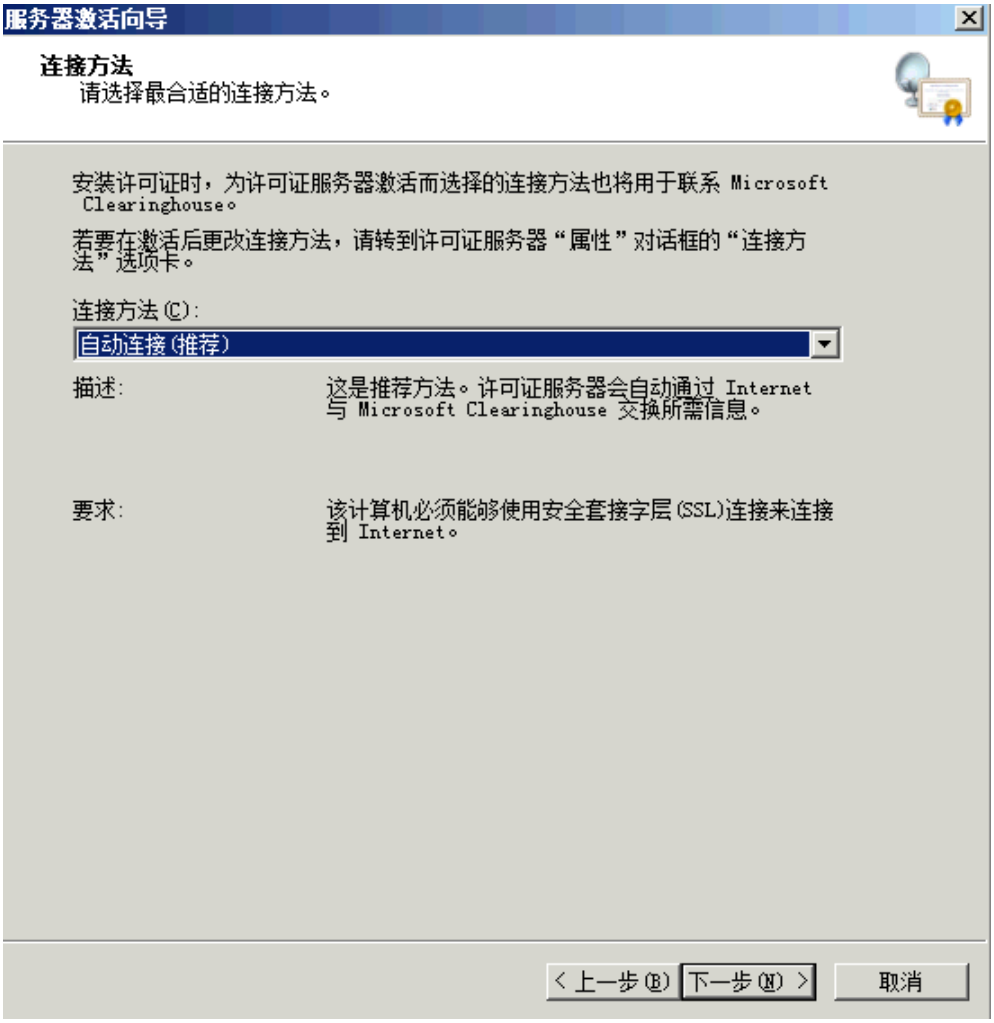
远程桌面授权激活

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”。

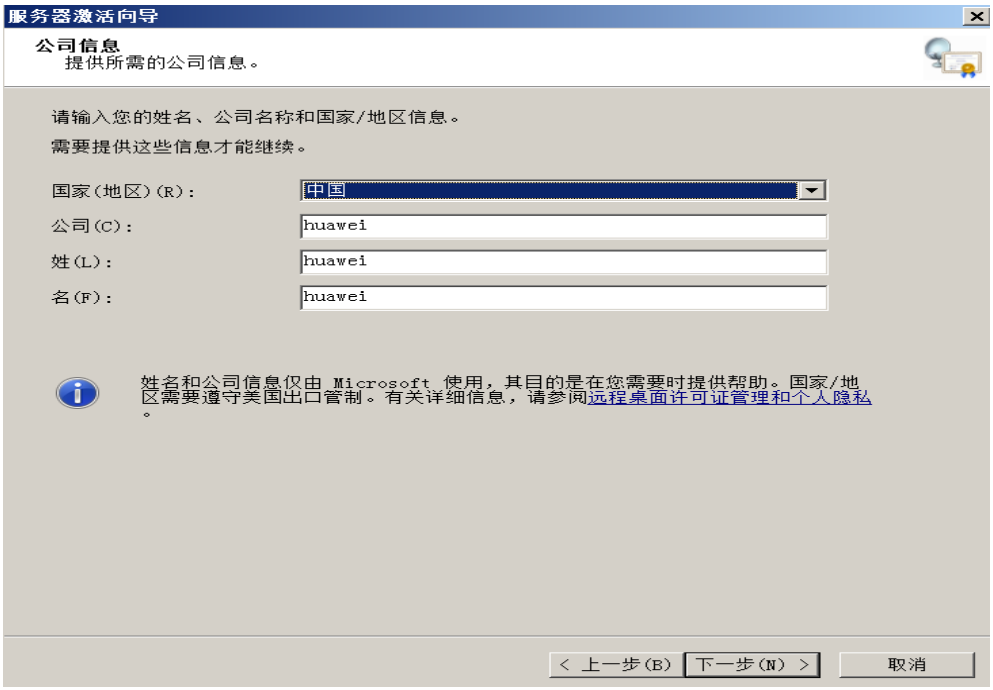
步骤 2 单击“下一步”。


服务器激活向导
欢迎使用服务器激活向导
若要安全地安装许可证，远程桌面授权服务器必须先被 Microsoft 激活。
许可证服务器成功完成激活之后，您将可以安装和颁发许可证。
如果在宽限时间到期之前 RD 会话主机或 RD 虚拟化主机服务器(如果适用)找不到已安装有相应许可证的已激活的许可证服务器，RD 会话主机或 RD 虚拟化主机服务器将停止接受未经授权客户端的连接。
有关激活远程桌面授权服务器的详细信息。
< 上一步(B)
下一步(N) >
取消

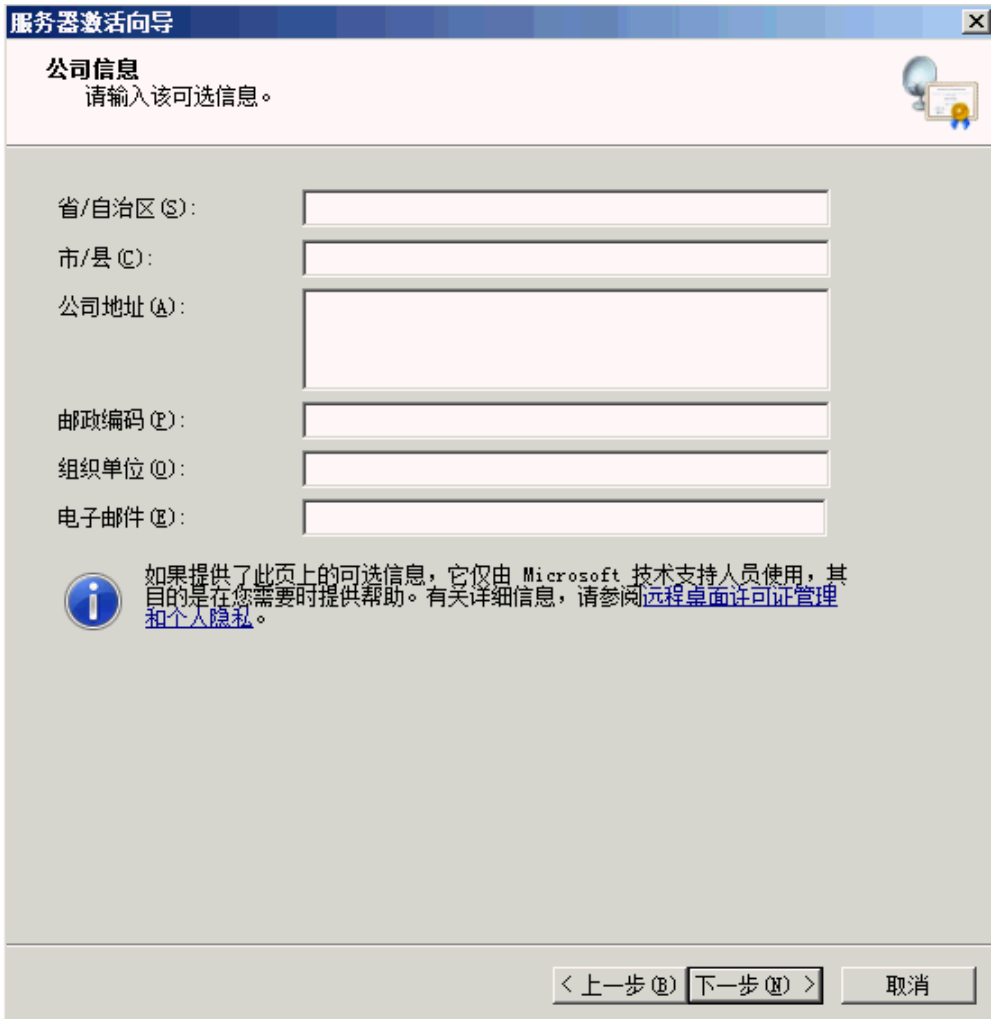
步骤 3 单击“下一步”。



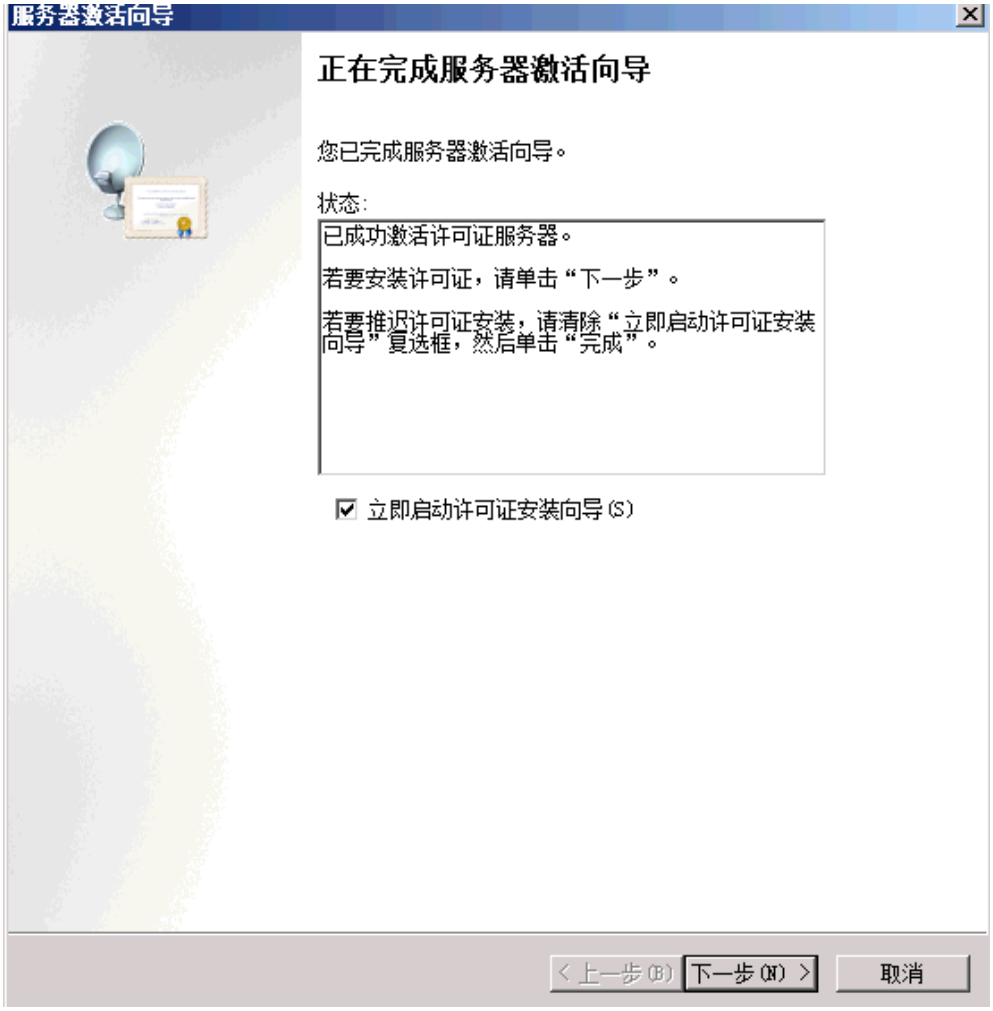
步骤 4 输入注册信息（必填选项），单击“下一步”。



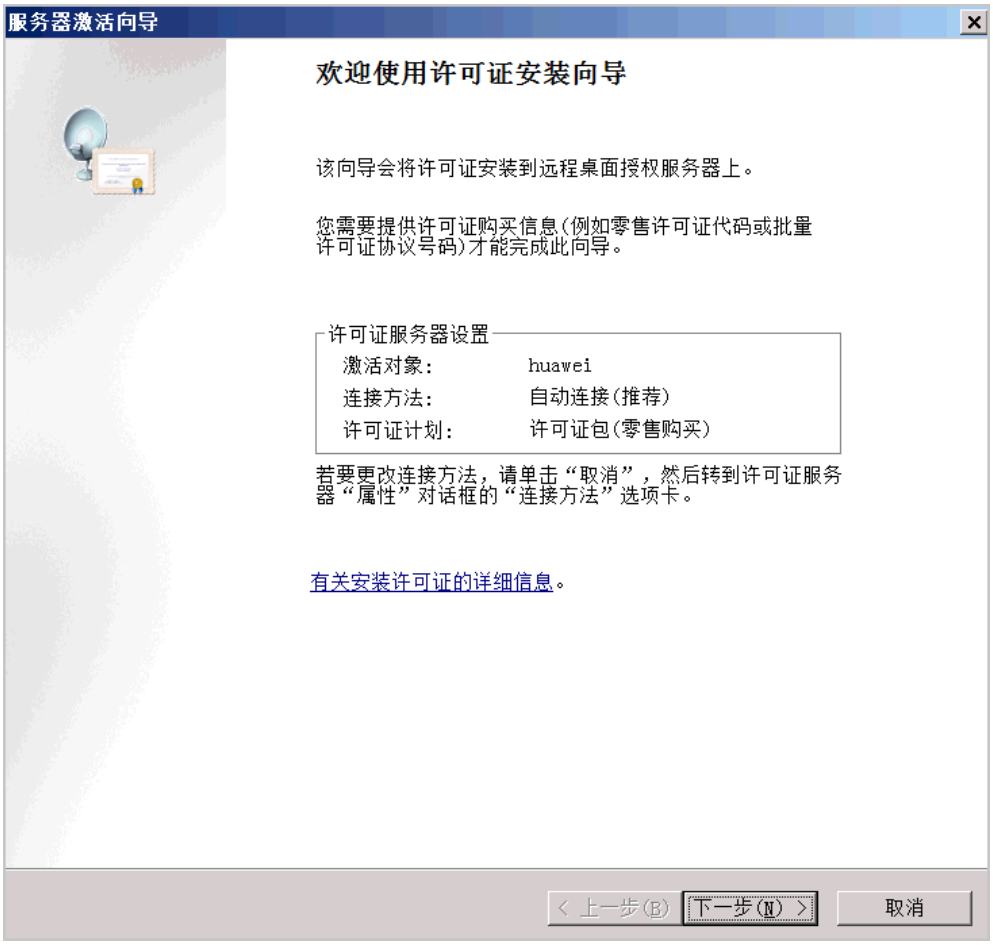
步骤 5 默认，单击“下一步”。



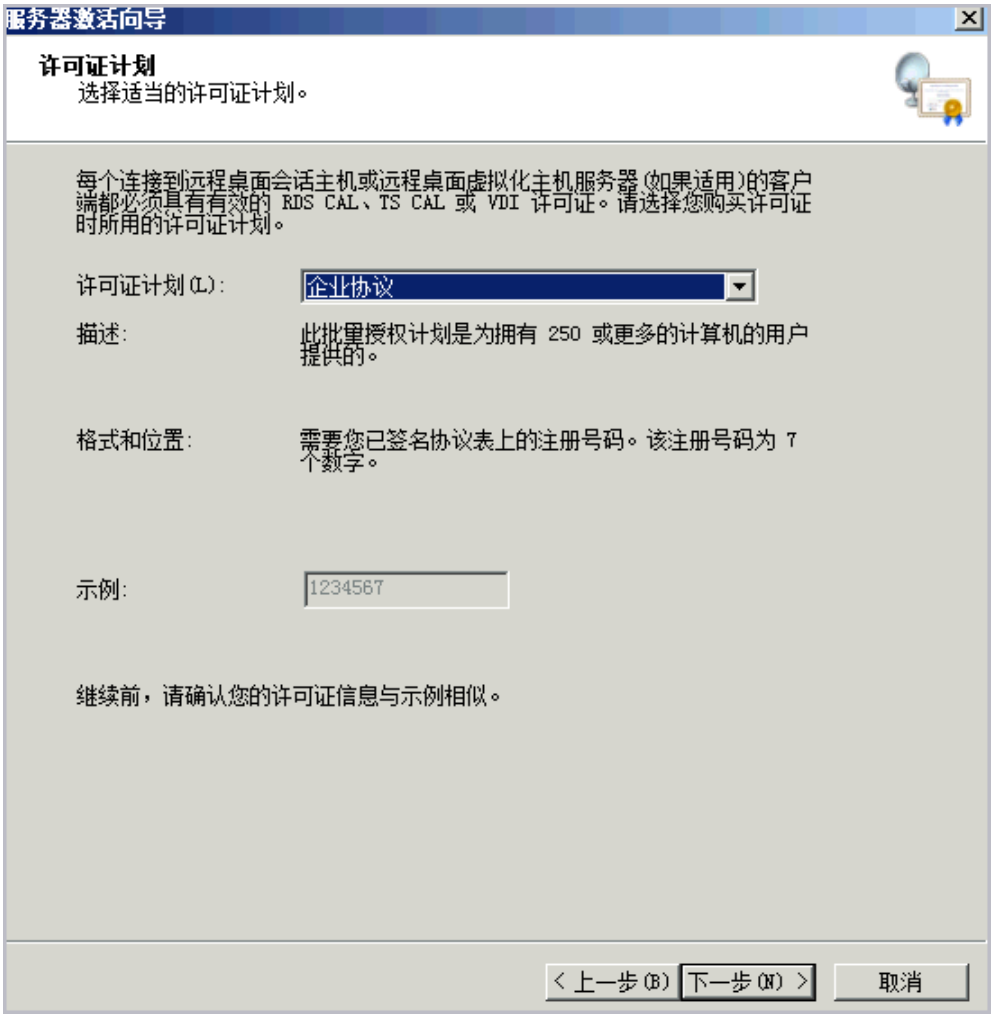
步骤 6 默认勾选“立即启动许可证安装向导”，单击“下一步”。


服务器激活向导
正在完成服务器激活向导
您已完成服务器激活向导。
状态:
已成功激活许可证服务器。
若要安装许可证，请单击“下一步”。
若要推迟许可证安装，请清除“立即启动许可证安装向导”复选框，然后单击“完成”。
立即启动许可证安装向导(S)
< 上一步(B)
下一步(N) >
取消

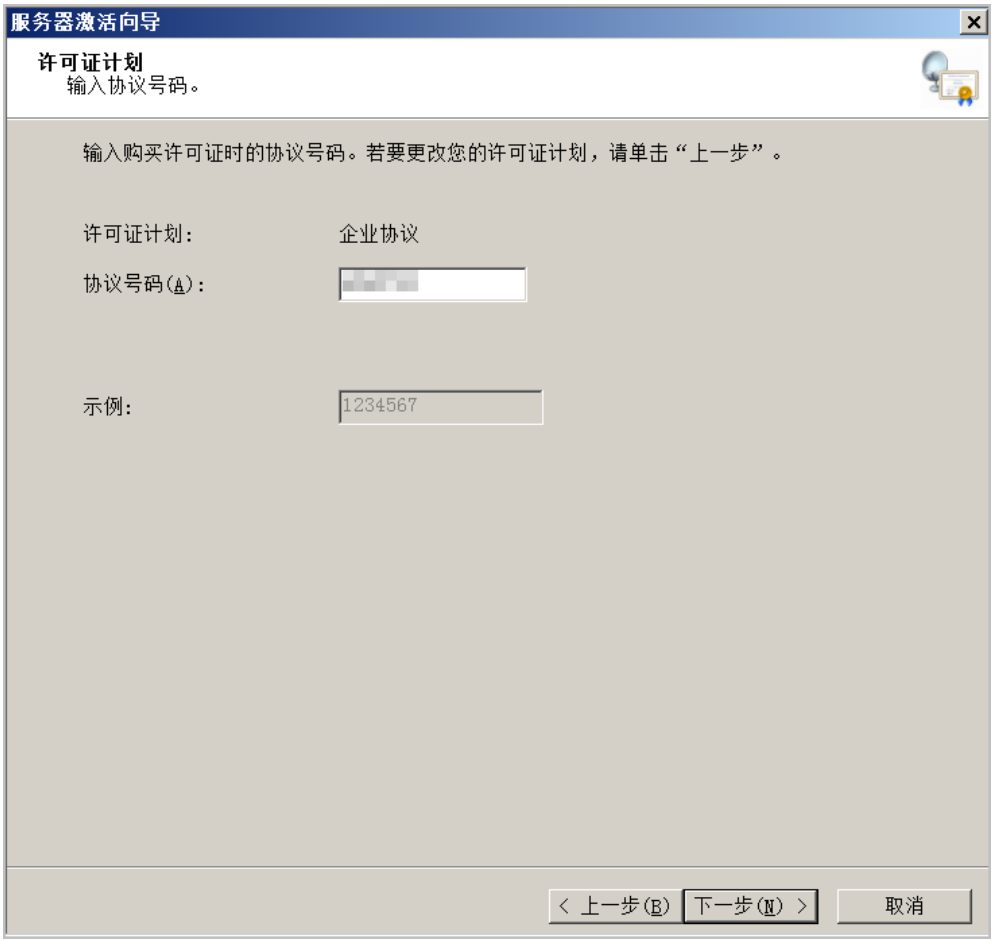
步骤 7 单击“下一步”。



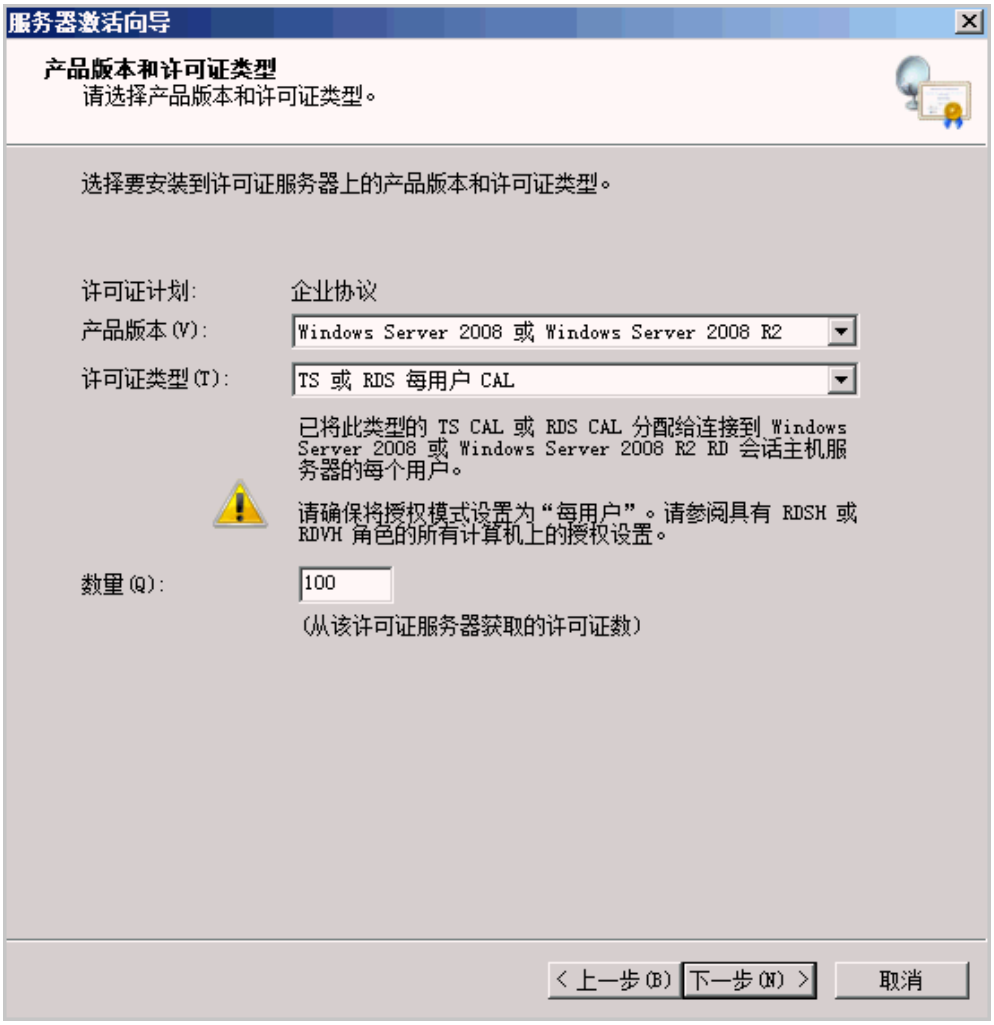
步骤 8 许可证计划项选择“企业协议”，单击“下一步”。



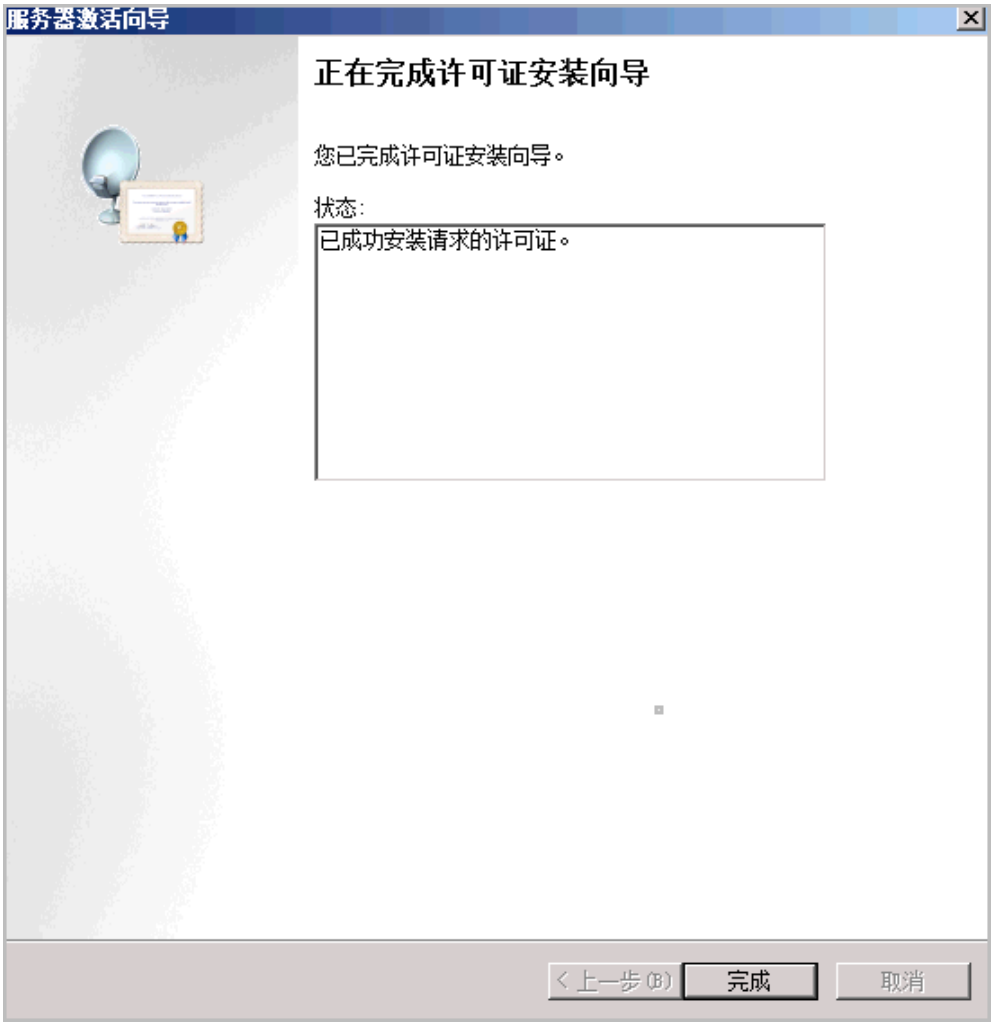
步骤 9 输入协议号码，单击“下一步”。



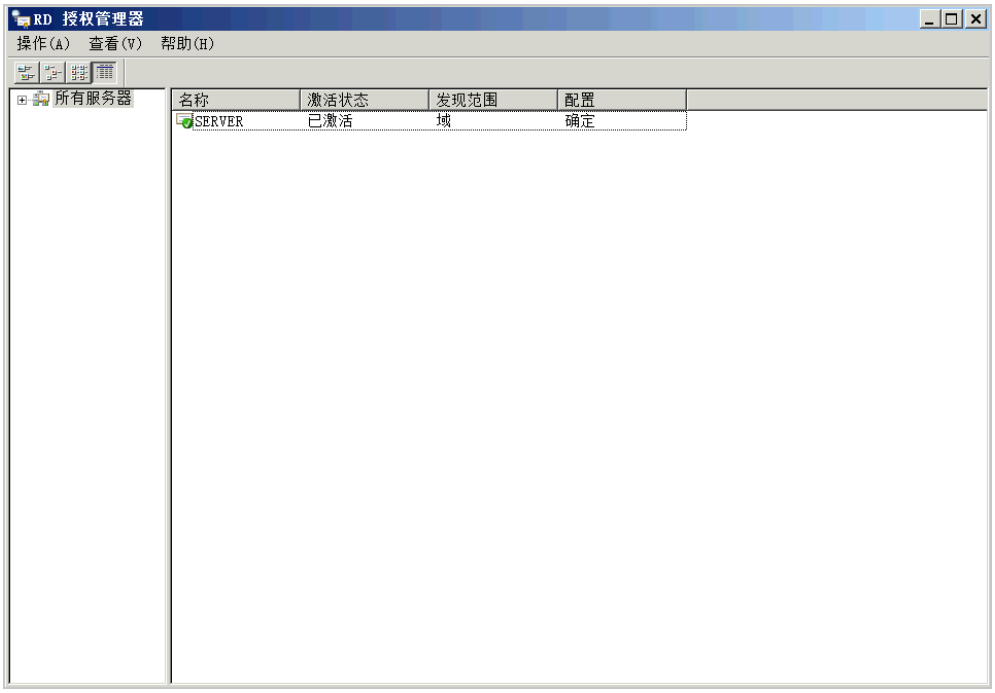
步骤 10 选择产品版本：“Windows Server 2008 或 Windows Server 2008 R2”，选择许可证类型：“TS 或 RDS 每用户 CAL”，输入允许的最大远程连接数量。


服务器激活向导
产品版本和许可证类型
请选择产品版本和许可证类型。
选择要安装到许可证服务器上的产品版本和许可证类型。
许可证计划:
企业协议
产品版本(V):
Windows Server 2008 或 Windows Server 2008 R2
许可证类型(T):
TS 或 RDS 每用户 CAL
已将此类型的 TS CAL 或 RDS CAL 分配给连接到 Windows Server 2008 或 Windows Server 2008 R2 RD 会话主机服务器的每个用户。
请确保将授权模式设置为“每用户”。请参阅具有 RDSH 或 RDVH 角色的所有计算机上的授权设置。
数量(Q):
100
(从该许可证服务器获取的许可证数)
< 上一步(B)
下一步(N) >
取消

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。

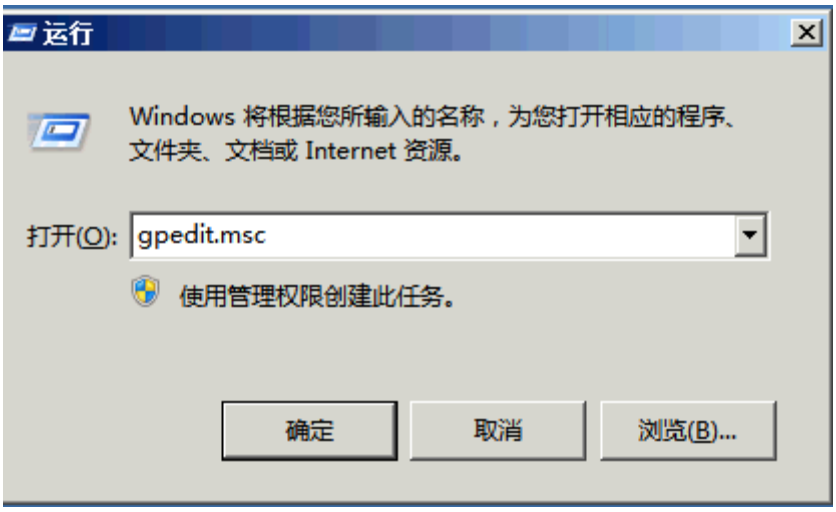


----结束

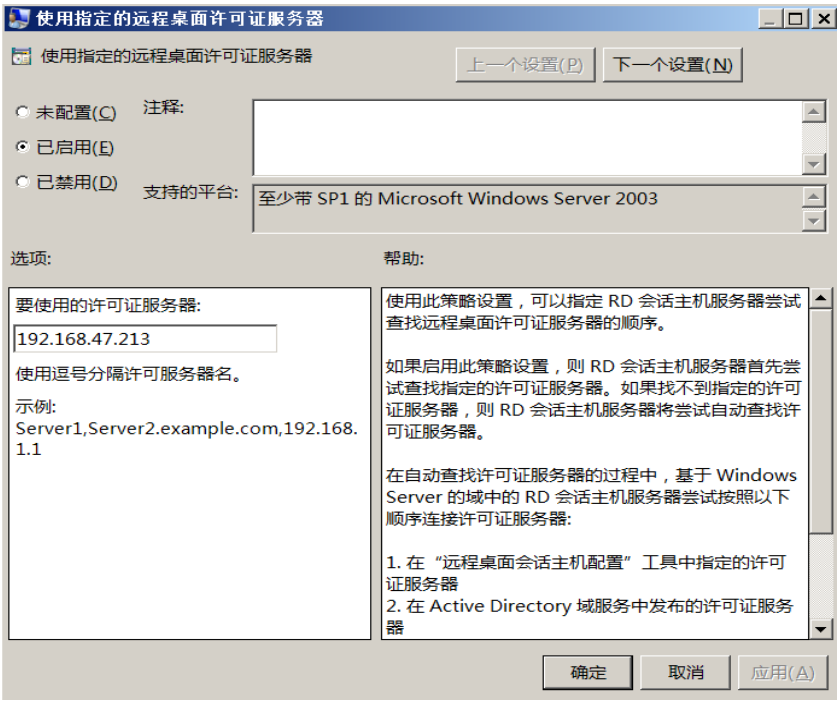
13.4.4 修改组策略

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。



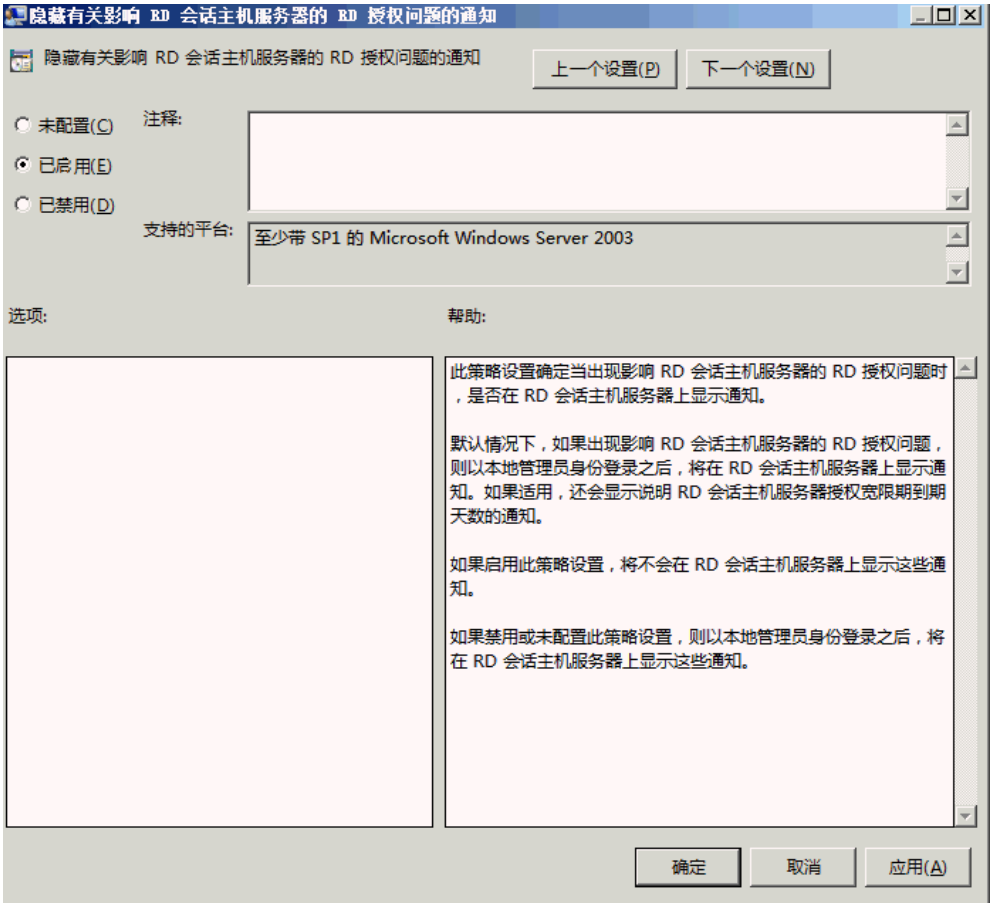
步骤 2 选择“计算机配置 > 管理模板 > Windows 组件 > 远程桌面服务 > 远程桌面会话主机 > 授权”，双击右侧的“使用指定的远程桌面许可证服务器”。



----结束

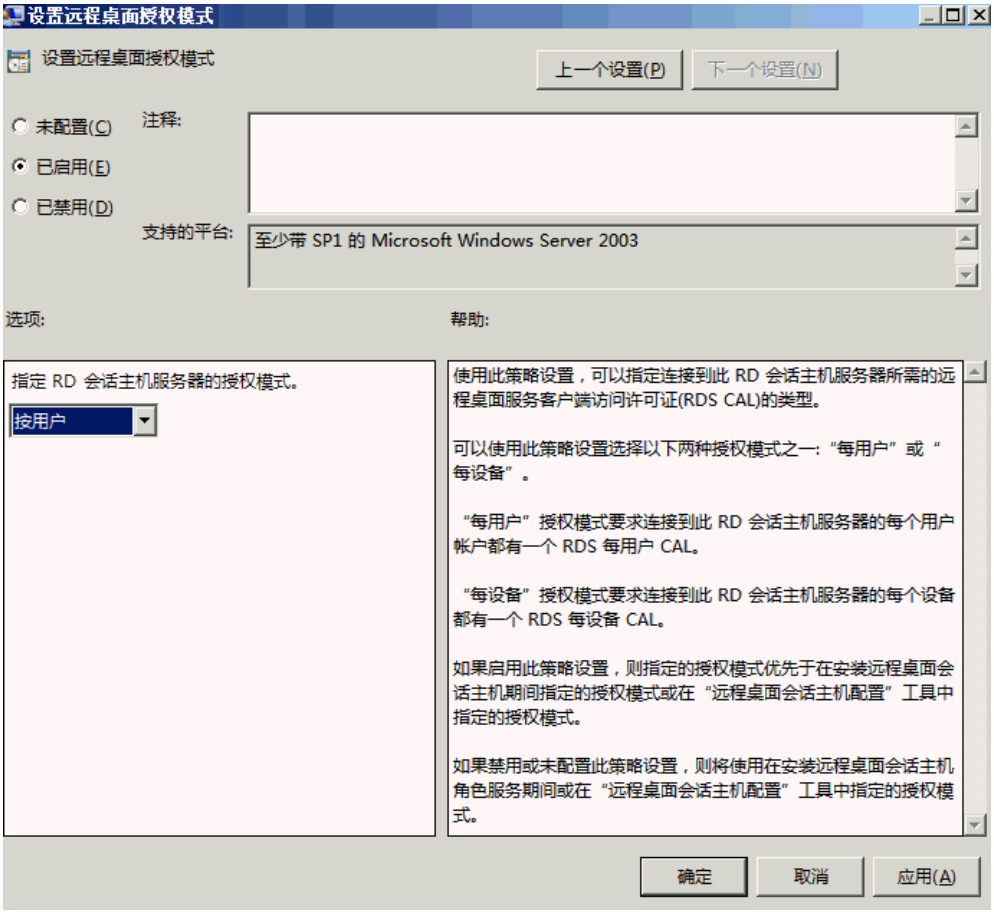
隐藏有关影响 RD 会话主机服务器的 RD 授权问题的通知

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”。



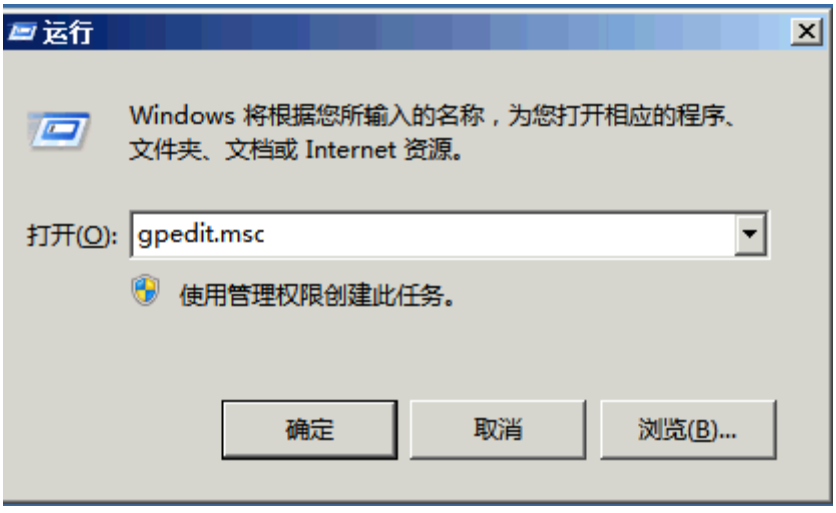
设置远程桌面授权模式

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。



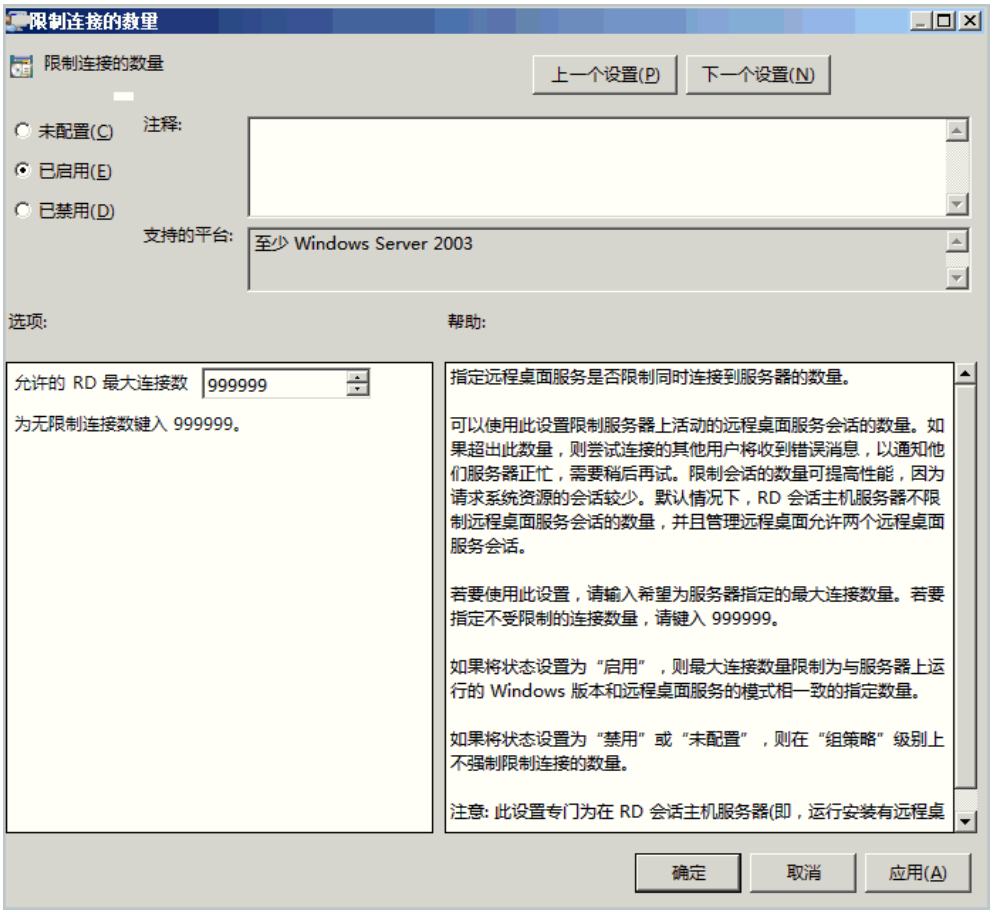
配置终端服务多用户

步骤 1 选择“开始 > 运行”，输入 **gpedit.msc** 打开组策略。

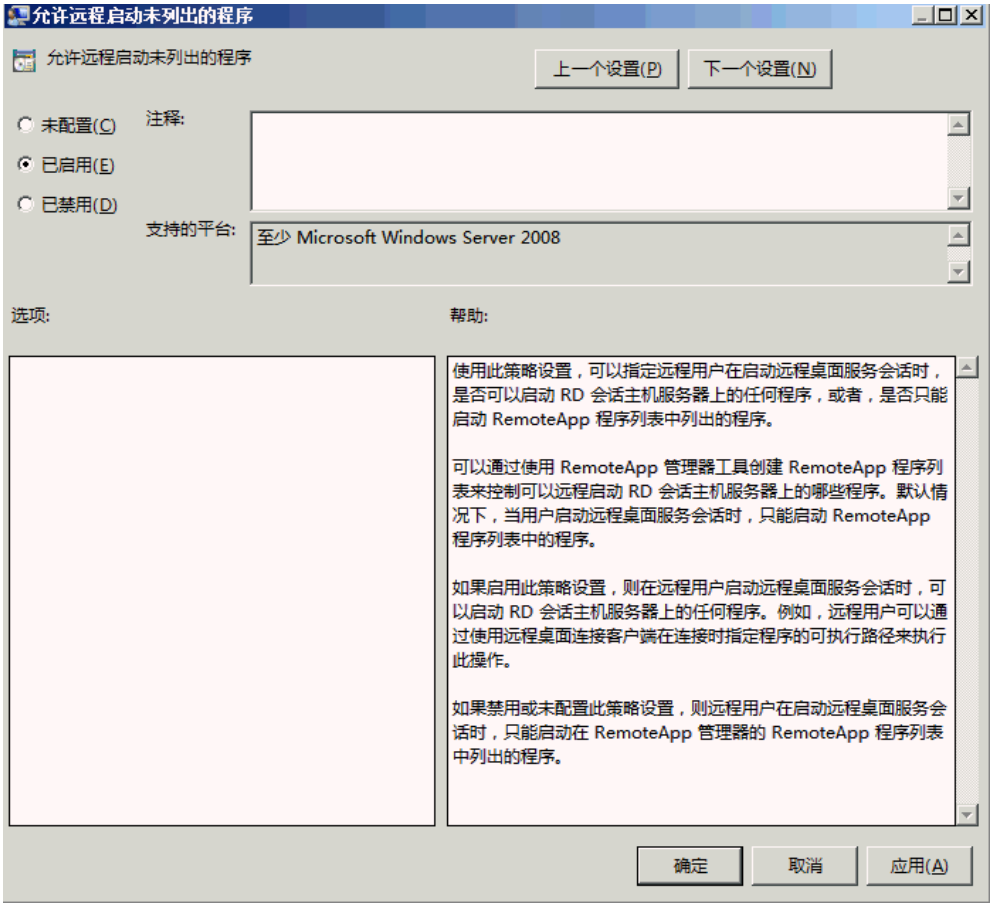


步骤 2 选择“计算机配置 > 管理模板 > windows 组件 > 远程桌面服务 > 远程桌面会话主机 > 连接”。

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。



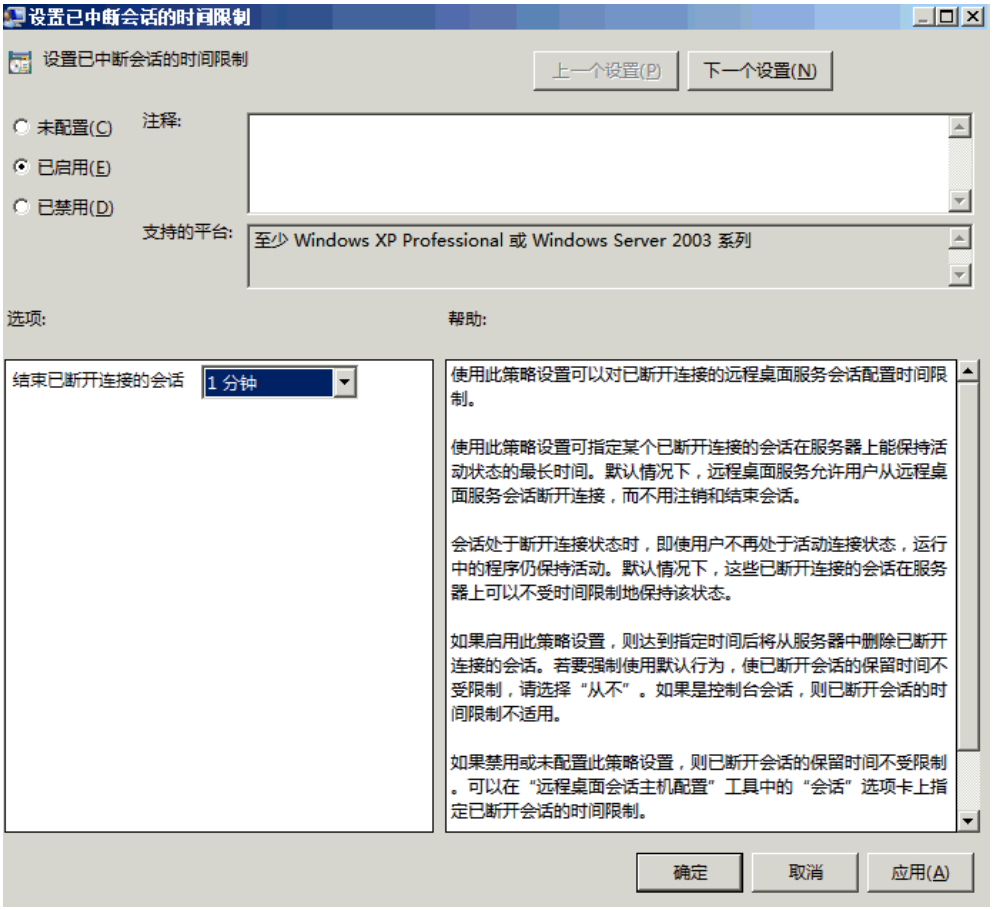
步骤 4 修改“允许远程启动未列出的程序” 为已启用。



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。

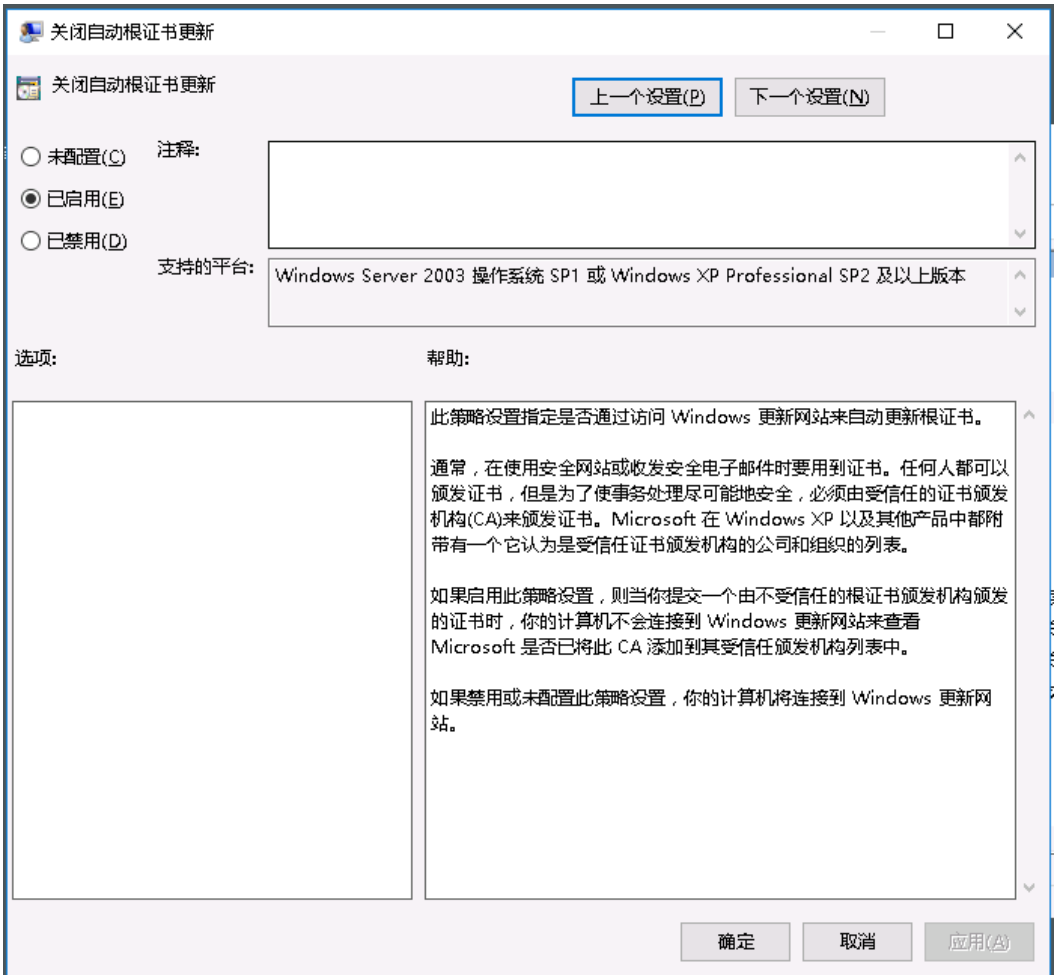
步骤 1 选择“管理模板 > 系统 > Internet 通信管理”，进入“Internet 通信管理”页面。

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。

图13-97 关闭自动根证书更新



----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。

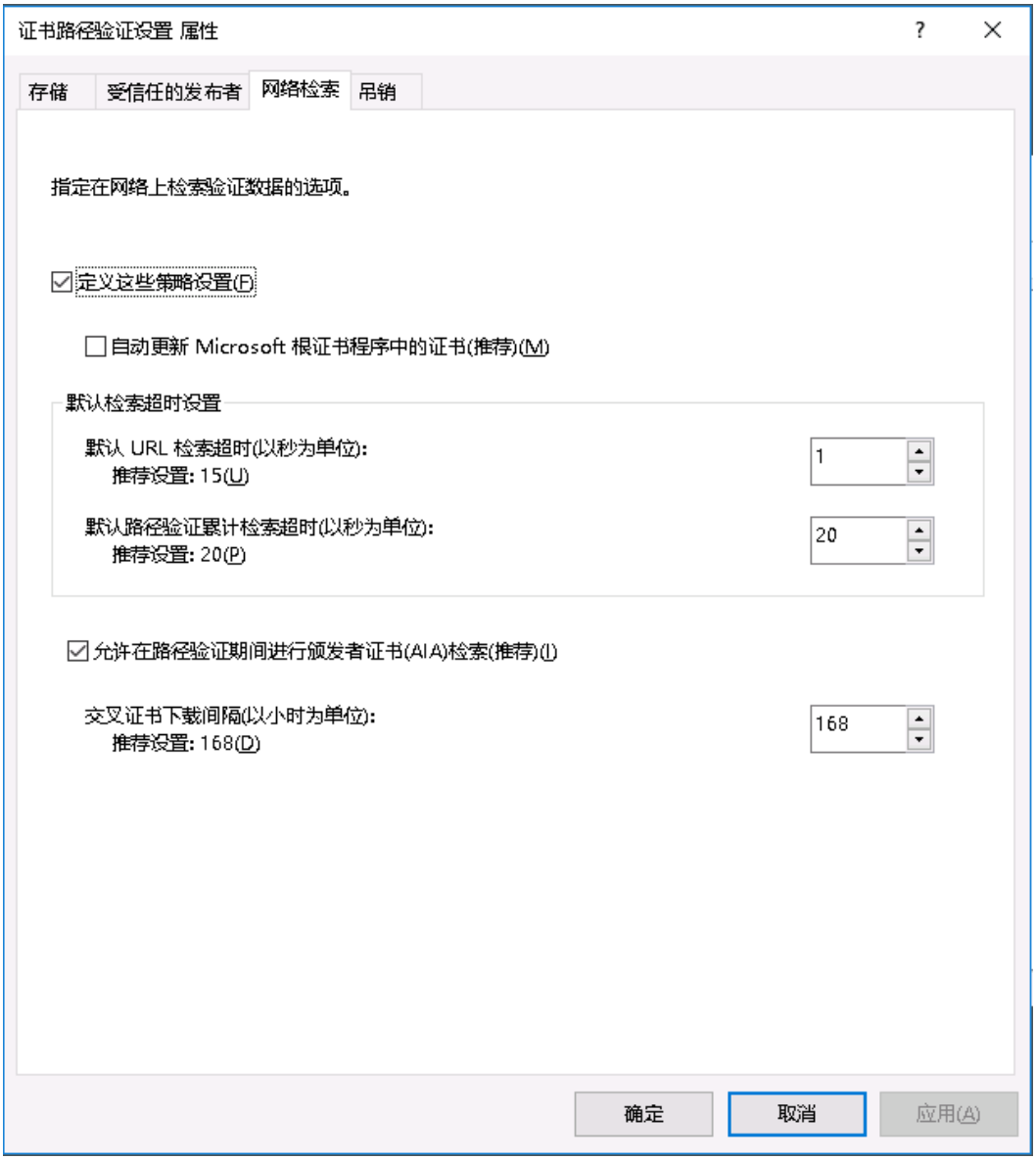
步骤 3 选择“网络检索”页签。

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。

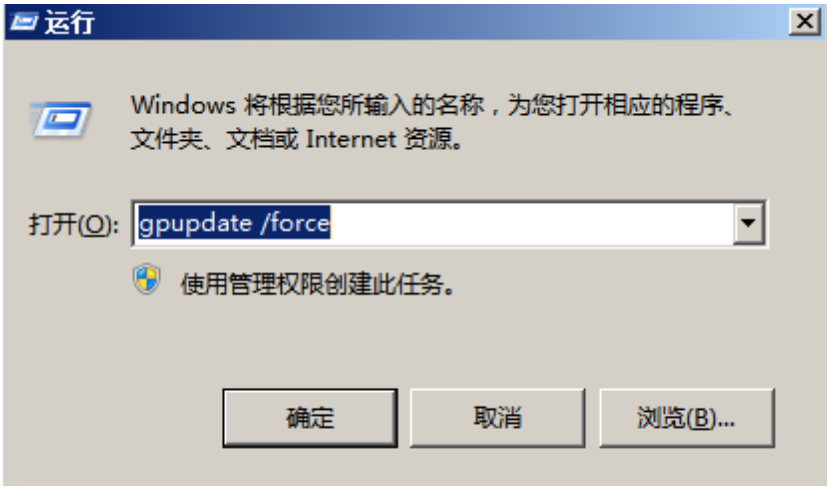
图13-98 证书路径验证设置



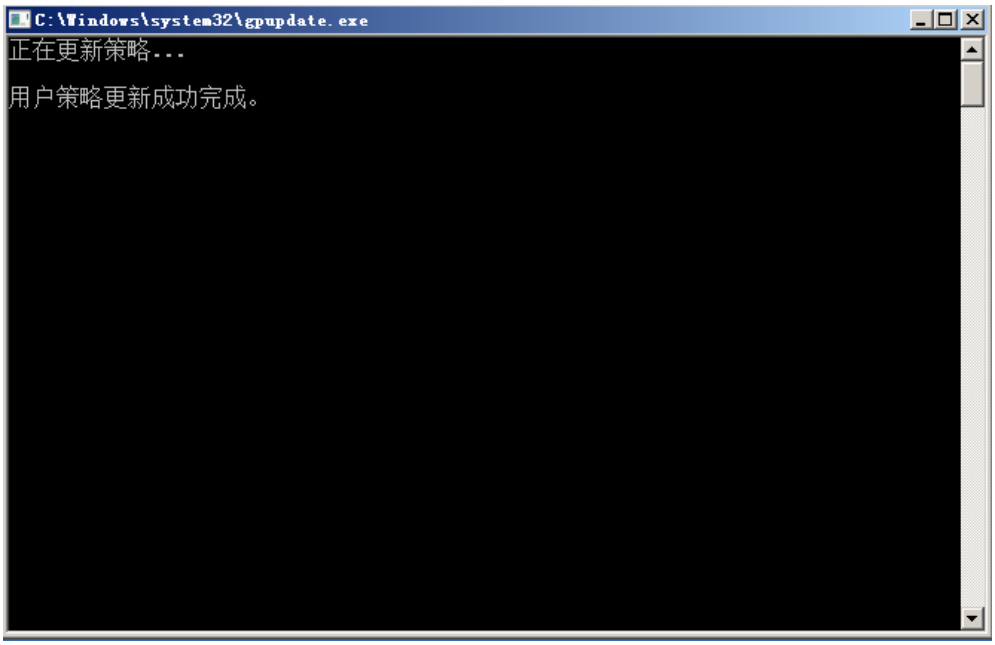
----结束

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云堡垒机。

----结束

13.4.5 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 RemoteaProxyInstaller_xxx.zip（xxx 为版本号）压缩包。

下载链接：

- RemoteaProxyInstaller_v3.3.26.0~v3.3.37.0 及以上版本下载链接
- RemoteaProxyInstaller_v3.3.38.0 及以上版本下载链接
- RemoteaProxy1.1.19.0 版本下载链接（适配所有堡垒机版本）

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 RemoteaProxyInstaller_xxx.zip（xxx 为版本号）压缩包进行解压。

步骤 4 双击“RemoteaProxyInstaller_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

14 常见问题

14.1 产品咨询

14.1.1 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。

用户可以登录管理控制台，选择“安全与合规 > 云堡垒机”，然后在云堡垒机管理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 EulerOS 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。

14.1.2 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。

14.1.3 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。

14.1.4 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。

14.1.5 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 实例的购买、升级、变更规格等关键操作进行细粒度授权。

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

14.1.6 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。

14.1.7 自动化运维包括哪些内容？

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

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

14.1.8 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。

14.1.9 使用云堡垒机时需要配置哪些端口？

为了能正常使用云堡垒机，实例和资源安全组端口配置可参考表 14-1。

表14-1 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 浏览器登录云堡垒机（HTTP、HTTPS）	入方向	TCP	22333
通过 MSTSC 客户端登录云堡垒机	入方向	TCP	53389
通过 SSH 客户端登录云堡垒机	入方向	TCP	2222
通过 FTP 客户端登录云堡垒机	入方向	TCP	20~21
通过云堡垒机的 SSH 协议远程访问 Linux 云服务器	出方向	TCP	22
通过云堡垒机的 RDP 协议远程访问 Windows 云服务器	出方向	TCP	3389
通过云堡垒机访问 Oracle 数据库	入方向	TCP	1521
通过云堡垒机访问 Oracle 数据库	出方向	TCP	1521

场景描述	方向	协议/应用	端口
通过云堡垒机访问 MySQL 数据库	入方向	TCP	33306
通过云堡垒机访问 MySQL 数据库	出方向	TCP	3306
通过云堡垒机访问 SQL Server 数据库	入方向	TCP	1433
通过云堡垒机访问 SQL Server 数据库	出方向	TCP	1433
通过云堡垒机访问 DB 数据库	入方向	TCP	50000
通过云堡垒机访问 DB 数据库	出方向	TCP	50000
通过云堡垒机访问 GaussDB 数据库	入方向	TCP	18000
通过云堡垒机访问 GaussDB 数据库	出方向	TCP	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 客户端登录云堡垒机	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
通过云堡垒机访问 PGSQL 数据库	入方向	TCP	15432
通过云堡垒机访问 PGSQL 数据库	出方向	TCP	5432

14.1.10 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。跨 VPC 的子网默认不能通信，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。

14.1.11 云堡垒机支持管理哪些数据库？

云堡垒机支持通过主机运维或应用运维两种方式管理数据库，可管理多种协议类型的云上数据库。主机运维方式提供增删改查操作命令审计。应用运维方式提供操作会话视频审计。

说明

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

主机运维方式

目前云堡垒机主机运维，支持管理以下协议类型的云上数据库，包括 MySQL、SQL Server、Oracle、DB2、PostgreSQL、GaussDB 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 14-2。

表14-2 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
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

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 14-3 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14-3 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 14-4 所示。

表14-4 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

14.1.12 云堡垒机是否支持纳管云下服务器？

您购买云下服务器，只要与云堡垒机网络互通并且协议互相支持，就可以通过云堡垒机纳管相应服务器。

14.2 区域和可用区

14.2.1 云堡垒机可以跨账号管理资源吗？

不建议。

云堡垒机仅支持直接管理同一 VPC 内资源，即可直接访问同一 VPC 内资源。

14.2.2 云堡垒机可以跨区域或跨 VPC 网络管理主机吗？

不建议。

云堡垒机仅支持直接管理同一 VPC 内资源，即可直接访问同一 VPC 内资源。

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

14.2.3 云堡垒机支持在专属云上使用吗？

支持。

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

14.3 如何配置安全组

如何选择云堡垒机实例区域和可用区？

区域是一个地理区域的概念。我国地域面积广大，由于带宽的原因，不可能只建设一个数据中心为全国客户提供服务。因此，根据地理区域的不同将全国划分成不同的区域。选择区域时通常根据就近原则进行选择。例如您或者您的客户在北京，那么您可以选择华北服务区，这样可以减少访问服务的网络时延，提高访问速度。

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

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

云堡垒机创建成功后，可以修改安全组吗？

云堡垒机创建成功后，安全组不可更改。如需修改 ，

云堡垒机创建成功后，可以修改 VPC 和子网吗？

云堡垒机创建成功后，VPC 和子网不可更改。如需修改 ，

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 14.6.3.1 如何设置云堡垒机登录安全锁？。

14.3.2 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。**
- 为确保云堡垒机正常连接资源，ECS 主机、RDS 数据库等资源需配置合理安全组规则，放开相应网关 IP 和端口，并允许云堡垒机“私有 IP 地址”访问，资源安全组配置可参考 ECS 安全组配置。
- 云堡垒机正常使用，实例和资源安全组端口配置可参考 14.1.9 使用云堡垒机时需要配置哪些端口？。

配置云堡垒机安全组

步骤 1 登录云堡垒机实例管理控制台。

步骤 2 单击“购买云堡垒机”，进入“购买云堡垒机实例”页面。

步骤 3 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 4 单击“创建安全组”，创建一个新的安全组。

步骤 5 单击“操作”列中的“配置规则”，为安全组添加安全组规则。

步骤 6 选择“入方向”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 14-1 配置。

步骤 7 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“Lincense 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 22333 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 22333 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。

14.4 License 相关

14.4.1 云堡垒机是否提供第三方 License？

不提供。

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

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

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

现象

现象一：堡垒机实例即将到期

现象二：堡垒机实例已到期

前提条件

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

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择“安全与合规 > 云堡垒机”，进入云堡垒机控制台页面。

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

步骤 4 根据需要选择续费时长。

图14-1 续费配置

步骤 5 单击“去支付”，在支付页面完成付款。

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

说明

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

----结束

14.5 文件传输类

14.5.1 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：

- 14.5.3 通过 Web 浏览器运维，如何上传/下载文件？
- 14.5.2 SSH 协议主机，如何使用 FTP/SFTP 传输文件？

14.5.2 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

14.5.3 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

14.5.4 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。

14.5.5 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

- 14.7.4.2 如何设置个人网盘空间大小？
- 14.5.4 云堡垒机的“主机网盘”是什么？

14.5.6 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

14.5.7 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。

14.6 CBH 系统登录

14.6.1 登录方式及密码类

14.6.1.1 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。

14.6.1.2 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。

14.6.1.3 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，签权绑定，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，签权绑定，再使用动态令牌进行身份认证。

AD 域认证

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

基本原理：通过 AD 域系统终端代理使用第三方库执行认证业务。

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

RADIUS 认证

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

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

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

LDAP 认证

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

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

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

Azure AD 认证

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

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

14.6.1.4 登录系统的初始密码是什么？

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

14.6.1.5 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 14-2 示例，单击“修改密码”，弹出“修改密码”对话框。

图14-2 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

14.6.2 多因子认证类

14.6.2.1 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。

14.6.2.2 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。

步骤 1 登录云堡垒机系统。

步骤 2 选择“系统 > 系统维护 > 系统管理 > 系统时间”，查看系统时间配置。

步骤 3 在“系统时间”区域，可以手动修改当前系统的时间，或者使用时间服务器同步当前系统的时间。

使用时间服务器同步系统时间时，可以选择系统默认自带的时间服务器，也可以手工输入时间服务器。

步骤 4 单击“同步时间”，完成时间同步。

步骤 5 选择“个人中心 > 手机令牌”，重新绑定手机令牌。

步骤 6 删除原来绑定的手机令牌，重新扫描二维码并绑定。

----结束

14.6.2.3 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。
- 云堡垒机实例安全组必须已放开短信网关 IP 和 10743、22333 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。

14.6.2.4 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

14.6.2.5 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。

14.6.2.6 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。

14.6.3 登录安全类

14.6.3.1 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 14-5。

表14-5 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

参数	说明
	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

14.6.3.2 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。

14.7 系统用户、资源及策略配置

14.7.1 系统用户类

14.7.1.1 在新建用户/资源时，为什么无法选择上级部门？

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

14.7.1.2 如何修改用户手机号码？

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

- CBH 不支持绑定海外的手机号码。
- **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

14.7.1.3 云堡垒机可新建多少个用户？

没有限制。

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

系统管理员 **admin** 是系统最高权限用户，也是系统第一个可登录用户。

14.7.2 资源添加类

14.7.2.1 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。

14.7.2.2 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14-6 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

14.7.2.3 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

14.7.2.4 如何批量导入/导出主机资源？

批量导入

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

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

说明

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

批量导出

云堡垒机还支持批量导出主机资源信息。验证用户后，一键导出全量已纳管的主机资源信息，可在导出的文件中查看主机资源账户最新的配置信息，以及设置改密策略修改后的账户密码。

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

14.7.2.5 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。

14.7.2.6 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 14-7。

表14-7 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

状态	说明
	“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”。

14.7.2.7 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。

14.7.2.8 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

14.7.2.9 为什么不能识别批量导入的云主机？

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

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

14.7.2.10 如何通过云堡垒机来访问内网提供的服务？

如果您需要通过云堡垒机来访问内网提供的服务，请参考以下步骤进行操作。

操作步骤

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

步骤 2 安装应用服务器

步骤 3 添加应用资源

----结束

14.7.2.11 如何在云堡垒机上添加 IPV6 地址的服务器？

堡垒机要支持添加 IPV6 地址的服务器 ，必须在购买堡垒机实例时，选择开启 IPV6 的子网。

14.7.2.12 Empty 账户是什么账户？

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。

14.7.3 系统策略类

14.7.3.1 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

14.7.4 系统配置类

14.7.4.1 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，拷贝公钥内容到 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 拷贝生成的私钥 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

14.7.4.2 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

14.7.4.3 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。

14.8 运维资源

14.8.1 运维管理

14.8.1.1 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”。

14.8.1.2 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

14.8.1.3 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

14.8.1.4 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。

14.8.1.5 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 14-8 所示。

表14-8 SSH 运维支持的算法

算法类型	H5 运维	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	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	aes128-ctr aes192-ctr aes256-ctr aes128-cbc aes192-cbc aes256-cbc 3des-cbc blowfish-cbc arcfour128 arcfour256

算法类型	H5 运维	客户端运维
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	ssh-rsa ssh-dss ecdsa-sha2-nistp256 ecdsa-sha2-nistp384

14.8.2 运维操作

14.8.2.1 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。

14.8.2.2 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

14.8.2.3 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 14-9。

表14-9 CBH 标签使用说明

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

示例-检索资源

以“主机管理”主机列表筛选“Proj1”的主机资源为操作示例。

步骤 1 登录云堡垒机系统。

步骤 2 选择“资源 > 主机管理”，进入主机管理列表页面。

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

步骤 4 主机列表查看通过标签筛选出的“Proj1”主机资源。

说明

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

----结束

14.8.2.4 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

14.8.2.5 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

14.8.2.6 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”适用相同的 Web 运维会话操作界面，快捷键操作方式相同。
- 数据库运维，因通过 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，因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。

14.9 审计运维日志

14.9.1 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 14-10。

表14-10 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。
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”。

14.9.2 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

14.9.3 可以删除某一天的云堡垒机运维数据吗？

不可以。

云堡垒机系统支持“自动删除”和“手动删除”系统中运维数据。

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

说明

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

14.9.4 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。

14.9.5 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。

14.9.6 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。

14.9.7 如果用户登录服务器 A 后，再登录到服务器 B，是否能够实现审计？

可以通过录像方式监控在服务器 A 上执行的所有操作，包括登录服务器 B 后的操作。如果是 Linux 服务器，还可以记录在服务器 B 上执行的命令。

14.9.8 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。

14.9.9 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。

14.10 故障排除

14.10.1 登录系统故障

14.10.1.1 登录云堡垒机系统异常怎么办？

问题现象

- IP 地址无法连接，网页打不开，不能通过互联网页面正常登录。

- 登录系统后界面异常无法显示。
- 登录系统提示授权未生效。
- AD 域认证的用户登录失败。
- 堡垒机不能正常登录，公网地址也不能访问。

可能原因

原因一：系统磁盘空间满了，磁盘空间使用率过高。

原因二：系统软件版本未更新，存在磁盘空间被占用，未被释放可能。

原因三：用户登录使用浏览器或浏览器版本，与系统不兼容。

原因四：实例配置安全组不合理。

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

原因六：配置 AD 域认证时，未禁用 SSL 加密认证。

原因七：堡垒机版本较低。

解决办法

原因一：

- 定期“手动删除”指定日期前的日志、视频等历史数据。设置磁盘空间满时日志“自动删除”，保证磁盘有足够空间。
- 对云堡垒机实例进行规格变更，满足大容量磁盘需求。
- 建议配置系统性能的磁盘空间使用率告警通知，当磁盘空间使用率超过设定阈值时，提示系统消息告警。

原因二：

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

原因三：

- 更换浏览器或升级浏览器版本，Web 登录推荐使用浏览器及版本。

原因四：

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

原因五：

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

说明

浏览器登录云堡垒机需放开入方向 TCP 协议 22333 端口，SSH 客户端登录云堡垒机需放开入方向 TCP 协议 2222 端口。

原因六：

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

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。

14.10.1.2 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。

14.10.1.3 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。

14.10.1.4 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。

14.10.1.5 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。

14.10.1.6 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值。
  - 主机运维 Windows 资源时，登录堡垒机用户不是 admin。

14.10.1.7 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14-3 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

将云堡垒机系统版本升级到 3.3.26.0 版本。

14.10.2 登录资源故障

14.10.2.1 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

- 14.10.2.2 通过 Web 浏览器登录资源，报 Code：T_514 错误怎么办？
- 14.10.2.4 通过 Web 浏览器登录资源，报 Code：C_515 错误怎么办？
- 14.10.2.5 通过 Web 浏览器登录资源，报 Code：C_519 错误怎么办？
- 14.10.2.6 通过 Web 浏览器登录主机资源，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。

14.10.2.2 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）”。

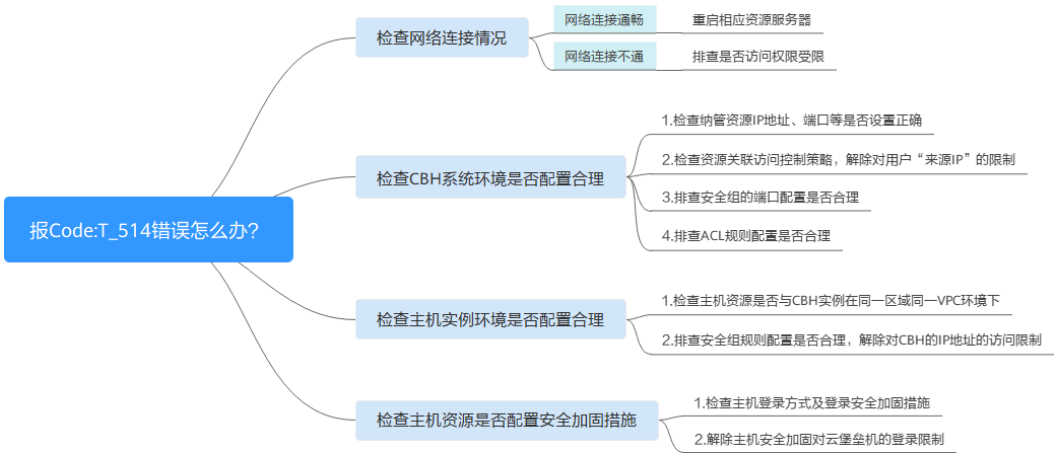
可能原因

- 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14-4 排查思路



检查网络连接情况

登录云堡垒机系统，，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。

- 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 22333 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。

14.10.2.3 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，，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 14.10.2.2 通过 Web 浏览器登录资源，报 Code：T_514 错误怎么办？依次排查。
- 网络连接通畅，则网络不稳定导致连接无响应。

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

  a. 排查云堡垒机和主机资源带宽是否超过限制请。

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。

14.10.2.4 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 主机资源，报登录错误，提示“运维资源过程中遇到一个错误，请重试或联系管理员（Code：C_515）”。

可能原因

- 原因一：密码输入错误次数超过 Linux 主机登录安全防护次数上限，导 CBH 的 IP 被加入“/etc/hosts.deny”文件名单。
- 原因二：Linux 主机开启了企业主机安全服务（Host Security Service，HSS），多次输入错误密码尝试登录，CBH 内网 IP 被 HSS 加入“/etc/sshd.deny.hostguard”文件名单。
- 原因三：堡垒机不支持操作系统的 SSH 算法。（仅针对 V3.3.38 版本以下堡垒机）

解除“/etc/hosts.deny”文件限制

步骤 1 管理员。

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。
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 管理控制台，解除 IP 限制。

1. 登录 HSS 管理控制台。

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 管理控制台，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。
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 修改算法：在 HostKeyAlgorithms 行后添加如下指令：

ssh-rsa,ssh-dss

说明

若您的默认配置文件中找不到 HostKeyAlgorithms 行，该步骤指令需要修改为：
HostKeyAlgorithms ssh-rsa,ssh-dss

步骤 3 使用如下命令，重启 SSH 服务：

systemctl restart sshd

----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。

14.10.2.5 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。

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。
- 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

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。，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。

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 22333 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 管理员直接登录主机资源。

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

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。

14.10.2.6 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 管理控制台，通过 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。请后，重新配置 CBH 资源账户密码，并是否正确。

----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 主机远程登录方式连接登录报错的 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。”

图14-5 没有远程桌面授权服务器可以提供许可证

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。

开启 RDP 强制登录

当 Windows 远程桌面连接数超过最大限值时，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 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值，会挤掉已登录用户，强制登录。

----结束

14.10.2.7 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。

14.10.2.8 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14-11 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14-6 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。

14.10.2.9 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”。

14.10.2.10 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。

14.10.2.11 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

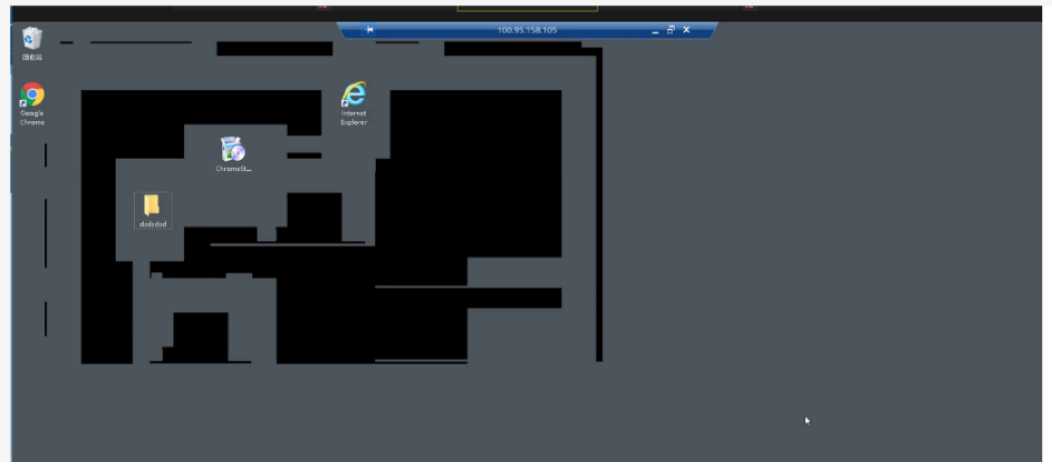
云堡垒机支持 50、100、200、500、1000、2000、5000、10000 资产规格配置，不同规格云堡垒机的并发数配置有差异。

建议您以提高并发数。

14.10.2.12 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。

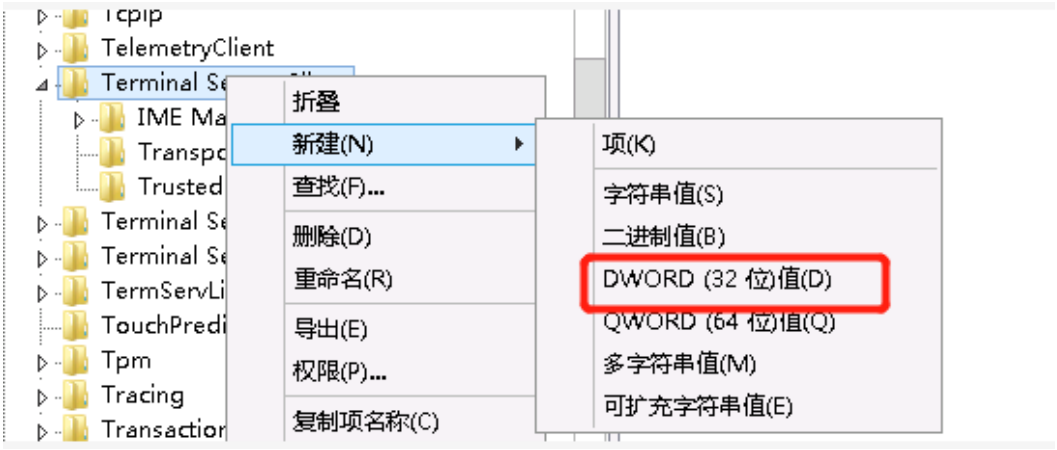


解决办法

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。

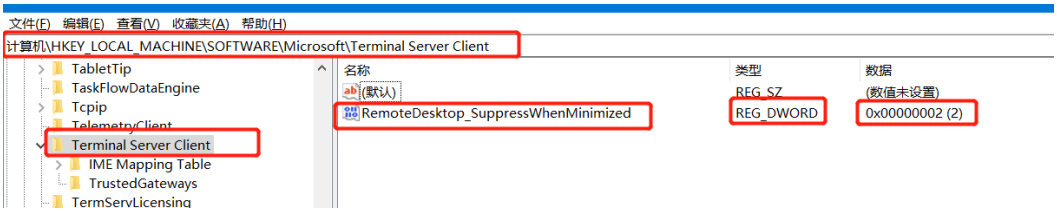
步骤 2 右键单击“Terminal Server Client”，单击“新建 > DWORD(32 位)值(D)”，新建 DWORD。

图14-7 新建 DWORD



步骤 3 将其 DWORD 命名为：RemoteDesktop_SuppressWhenMinimized，值设置为 2。

图14-8 设置值大小



----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”，如图 14-9 所示。则需要做如下调整。

图14-9 无法连接

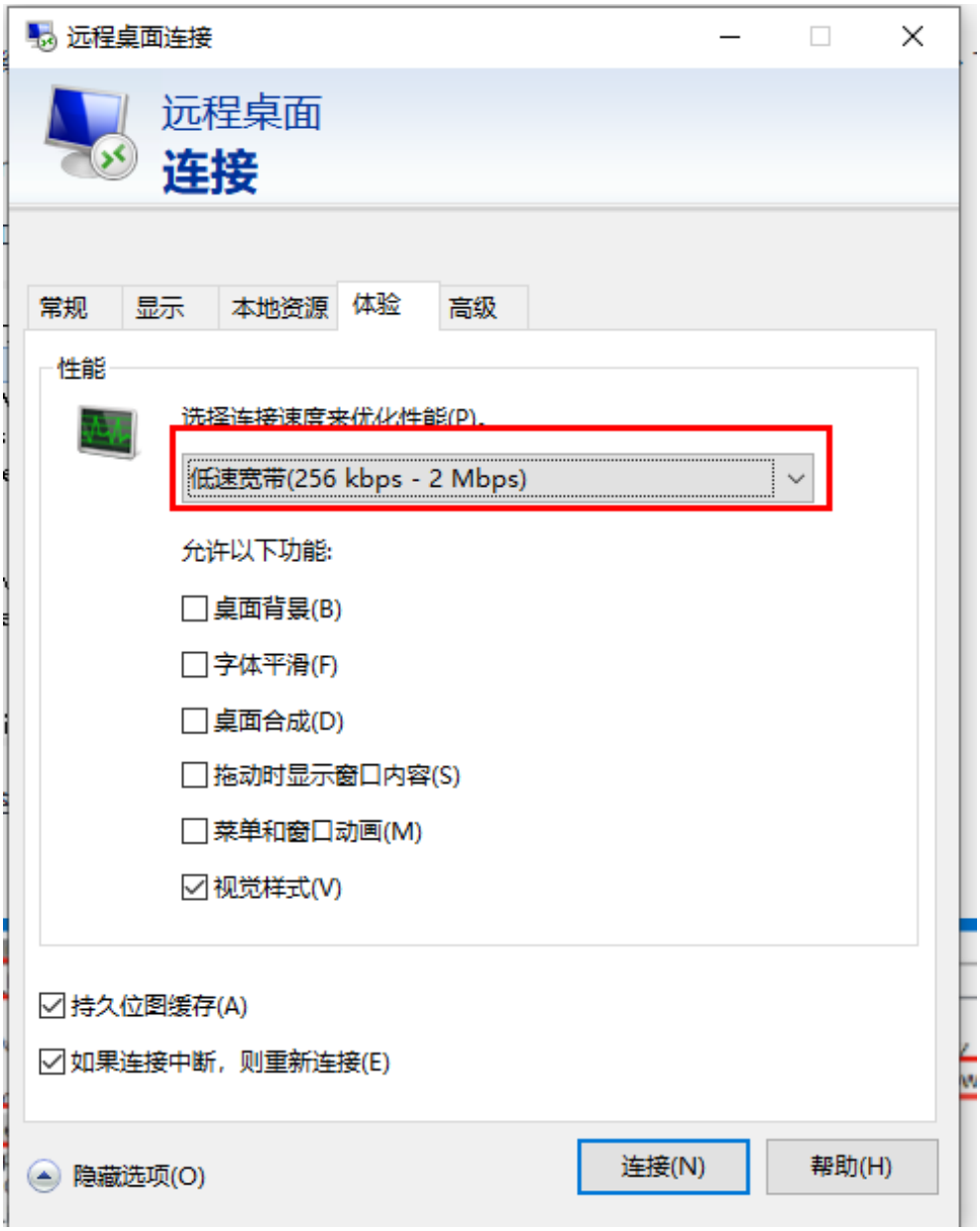
步骤 1 打开远程桌面连接程序，单击“显示选项”，选择“显示”。

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）”。如图 14-10 所示

图14-10 远程桌面显示设置

步骤 3 选择“体验”，修改连接速度为“低速宽带（256 kbps - 2 Mbps）”，如图 14-11 所示。

图14-11 修改性能选项



----结束

14.10.2.13 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”。

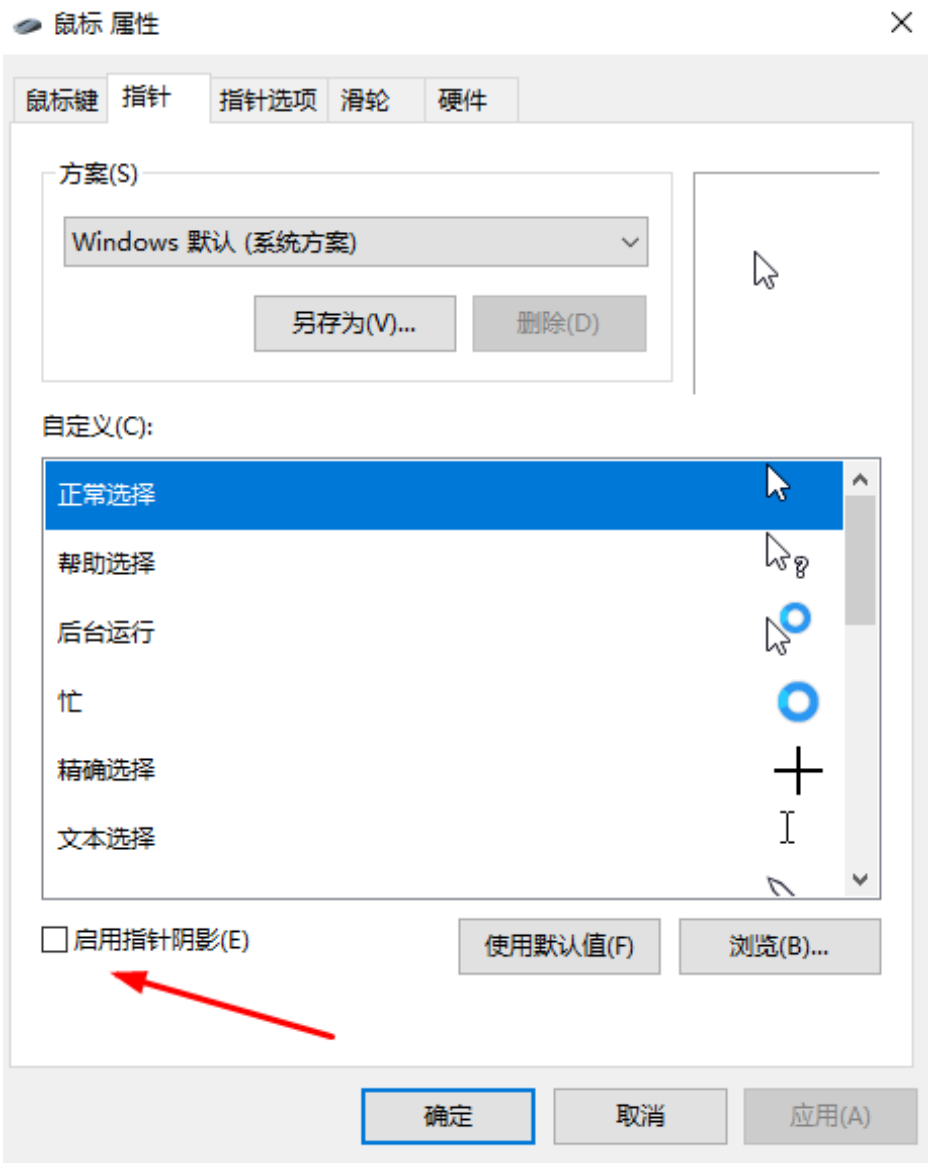
图14-12 控制面板

步骤 3 在左侧导航树中，单击“鼠标”，进入鼠标的配置页面。

图14-13 鼠标页面

步骤 4 单击“其他鼠标选项”，选择“指针”页签。

图14-14 指针



步骤 5 去掉勾选“启用指针阴影”的选项，单击“确定”。

----结束

14.10.3 运维故障

14.10.3.1 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 14-12。

表14-12 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。

14.10.3.2 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。

14.10.3.3 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。

14.10.3.4 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：
  - 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。

14.10.3.5 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，检索中文内容验证。

----结束

14.10.3.6 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

14.10.3.7 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。

14.10.3.8 通过 Web 浏览器运维，不能拷贝文本怎么办？

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。

无法拷贝超长文本到 Windows 主机

问题现象

从用户本地拷贝文本到 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

14.10.3.9 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 14-13。

表14-13 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	1. 检查 CBH 系统与 FTP 服务的网络，是否存在传输丢包现象；

错误码	错误提示	排查方法
	过长，请重试或联系系统管理员	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 14.10.2.4 通过 Web 浏览器登录资源，报 Code：C_515 错误怎么办？； 3. 检查 CBH 系统与故障主机的网络层，是否有服务协议拦截 CBH 系统 IP； 4. 请填写工单反馈问题现象，联系技术支持。
ERROR_CLIENT_519	Code：C_519 由于资源连接失败或不可达，当前无法访问。如果持续出现该问题，请通知系统管理员或检查系统日志	1. 检查 CBH 系统与主机资源的网络是否互通； 2. 本地登录主机资源，输入命令 **route -n**，检查目标主机的路由表，是否存在丢失 CBH 路由现象； 3. 请填写工单反馈问题现象，联系技术支持。 详细解决办法请参见 14.10.2.5 通过 Web 浏览器登录资源，报 Code：C_519 错误怎么办？。
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_	Code：C_523 由于连接被管理员	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；

错误码	错误提示	排查方法
523	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	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 14.10.2.6 通过 Web 浏览器登录主机资源，报 Code：C_769 错误怎么办？。
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	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 14.10.2.2 通过 Web 浏览

错误码	错误提示	排查方法
	络并重试	器登录资源，报 Code：T_514 错误怎么办？。
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。

14.10.3.10 如何解决“运维 Windows 服务器时使用 WPS 软件输入中文异常”的问题？

运维 Windows 服务器时，使用 WPS 软件输入文字出现重复现象，例如：输入“云堡垒机”会出现“云云云云”。

解决办法

步骤 1 将本地电脑的输入法设置为英文。

步骤 2 将被运维的 Windows 服务器的输入法设置为中文。

----结束

A 修订记录

发布日期	修改说明
2024-05-20	第三次正式发布。 新增： • 2.8 更改 VPC 章节。 • 2.9 更改安全组章节。 • 3.5.11 资源账户配置章节。 • 3.5.12 客户端登录配置章节。 • 3.5.13 用户有效期倒计时配置章节。 • 3.5.14 会话限制配置章节。 • 6.5.5 配置 SAML 远程认证章节。 修改： 改密策略自动生成密码的说明。
2023-04-21	第二次正式发布。 修改如下章节堡垒机需要开放的端口号，需要放开 22333 端口。 • 1.7 使用限制 • 14.1.9 使用云堡垒机时需要配置哪些端口？ • 14.3.2 如何配置云堡垒机的安全组？
2022-10-30	第一次正式发布