云堡垒机（原生版）

用户指南

天翼云科技有限公司

目录

1 产品概述

1.1 产品定义

云堡垒机（原生版）是一款运维安全管理产品，提供云上安全运维通道，集中管理云上资产及特权账号，统一监控审计运维操作行为，帮助企业满足等保合规测评要求。

产品功能

资产账密管理

- 支持统一管理、授权资产特权账户，账户在堡垒机中统一存储管理；
- 特权账户由堡垒机统一代理单点登录， 运维人员登录堡垒机后，无需输入资产账密即可自动登录服务器等资产，降低账密泄漏风险。

资产运维

- 支持 WEB 运维，支持主流浏览器无插件化运维，让运维脱离工具和操作系统束缚，随时随地远程运维；
- 支持 PuTTY、SecureCRT、Xshell、WinSCP、Mstsc 等专业运维工具完成运维。

安全认证

支持账密+OTP+短信双因子身份认证，保证运维用户登录堡垒机及资产的认证安全。

运维安全管控

- 支持命令控制、文件操作控制，对服务器中敏感、高危操作进行管控。
- 支持工单管理审批模式，重要运维需要授权人审批授权才能执行运维指令，保障敏感核心资源安全。

资产访问授权

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。

安全审计

- 支持对用户登录日志、系统管理操作日志进行审计。
- 支持对字符操作、图形运维、文件操作及传输、数据库运维产生的会话日志统一审计，同时支持字符操作、图形运维操作全程审计录像及回放。

为什么选择云堡垒机

开通和使用非常便捷：

- 您只需选择产品版本、实例规格、资产规格，为云堡垒机实例指定实例开通地域、配置相关网络参数即可开通。
- 开通完成后，您可以在控制台上快捷登入云堡垒机，管理运维您的服务器、数据库等 IT 资产。

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。
- 满足等级保护、ISO/IEC27001 等对运维审计的要求。

云原生堡垒机更安全：

- 云原生堡垒机运行操作系统及网络安全防护策略统一实现安全加固，缩小攻击面。
- 租户之间严格网络隔离、实例和数据隔离，各堡垒机实例环境独立，保障系统运行安全。

1.2 功能特性

产品提供标准版、企业版、高级版，不同版本支持的功能及差异如下：

产品功能		描述	标准版 （一类节点）	企业版 （一类节点）	高级版 （二类节点）
部署方式	主备版	购买主备版后会创建两台堡垒机，通过双机热备机制，提升服务高可用性。	√	√	×
资产管理	主机管理	支持 Windows、Linux 操作系统的服务器资产管理	√	√	√
	数据库管理	支持 Mysql、PostgreSQL、Oracle 等类型数据库资产管理及运维	×	√	√
	自动导入天翼云上 ECS 资产	支持自动导入账号下所拥有的天翼云上 ECS 资产	√	√	×
	应用管理	支持纳管应用服务器，并且可以直接纳管 Chrome、IE、Firefox、SecBrowser 等应用	×	√	√
	资产组管理	支持资产分组管理，按组管理资产，统一授权	√	√	√
	资产账密管理	支持资产特权账号、密码集中加密存储和托管，运维整个过程不暴露资产账密	√	√	√
	账户改密	支持预设策略，对一个或多个主机资源账户的密码进行手动、定时或周期性的修改	√	√	√
用户管理	双因子认证	支持账密+手机令牌认证方式登录堡垒机	√	√	√
	用户管理	统一管理运维访问用户、管理员、审计员，支持定义用户账号安全策略	√	√	√
	用户组管理	支持用户分组管理，统一为分组内用户授权	√	√	√
	账号安全策略	支持设置全局账号安全策略、密码策略	√	√	√
授权管理	资产访问授权	支持设置用户、资产、资产账号的访问授权及管控	√	√	√
	字符命令授权	支持对用户、用户组敏感命令的授权及管控	√	√	√
	文件操作授权	支持对用户操作文件命令授权及管控	√	√	√
	数据库授权	支持设置用户访问数据库授权及管控	×	√	√
资产运维	字符运维 （SSH、Telnet）	支持 Xshell、SecureCRT、Putty 等客户端工具登录堡垒机运维资产	√	√	√
	图形运维 （RDP、VNC）	支持 MSTSC、VNC 等客户端工具登录堡垒机运维主机资产	√	√	√
	文件运维 （SFTP、FTP）	支持使用本地 WinSCP、Filezila 等 SFTP 客户端工具登录堡垒机进行文件运维	√	√	√
	数据库运维	支持 Navicat、DBeaver 等客户端工具登录	×	√	√

产品功能		描述	标准版 (一类节点)	企业版 (一类节点)	高级版 (二类节点)
		堡垒机进行数据库运维			
	Web 直接运维服务器	支持通过浏览器直接 SSH 运维字符资产和 RDP 图形资产	×	√	√
	资产访问运维免账密登录	支持通过堡垒机账密单点登录到主机资产，运维人员无需掌握服务器资产的账密	√	√	√
运维管控	资产访问控制	支持对用户访问资产、协议、资产账号的访问管控，用户仅可运维自己已授权资产	√	√	√
	运维命令管控	支持根据字符命令授权对用户允许和拒绝的操作命令进行管控，支持自定义常用命令组	√	√	√
	文件操作控制	支持根据文件授权对用户文件操作进行管控，超出授权范围无法操作文件	√	√	√
	自动运维	支持依照既定步骤自行执行命令和运维脚本，对多个目标进行自动化运维管理	×	√	√
工单管理	运维访问审批	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	√	√	√
	运维命令审批	运维用户在运维过程中，遇到命令使用无权限情况，可提交系统工单申请资源字符使用权限	√	√	√
审计	日志审计	支持对用户登录日志、系统管理操作日志进行审计	√	√	√
	会话审计	支持对字符操作、图形运维、文件操作及传输、数据库运维产生的会话日志统一审计	√	√	√
	文件传输审计	支持文件传输会话（ftp、sftp）、账号数据角色产生的文件管理操作、个人目录文件操作，支持文件操作记录查看	√	√	√
	数据库审计	支持查看 sql 指令，会话详情	×	√	√
	审计录像及回放	支持对字符、图形运维操作全程审计录像及回放	√	√	√

1.3 产品优势

运维高效快捷

云堡垒机（原生版）支持多种运维访问协议，满足用户统一对数据库、服务器、web 应用等系统或设备的日常运维需求。

- 字符协议：SSH、TELNET
- 图形协议：RDP、VNC
- 文件传输协议：FTP、SFTP
- 数据库协议：MySQL、Oracle、DB2、PostgreSQL 等
- WEB 访问协议：HTTP/HTTPS

灵活的授权模型

以 4A 为核心实现对用户进行功能授权、资产授权、操作授权，最小化用户运维授权管理，降低越权操作风险

管控方式严格

- 对于高危命令实现实时告警或阻断，对于特别重要的命令实现多人审核，避免用户进行不安全的运维操作。
- 支持运维账号登录 IP 地址绑定，限制登录地址，避免非授权用户登录进行重要运维操作。

快速开通使用

用户根据自身业务需求，选择对应规格一键开通堡垒机实例，方便快捷。

安全合规

对所有运维操作集中记录，支持审计、录像及回放，满足等保测评要求，助力企业安全合规建设。

1.4 应用场景

（一）中小企业资产运维

场景说明

中小企业运维投入资源相对较少，运维管理流程规范度较低，运维人员可能会因为无意操作造成数据丢失、业务故障等，黑客也可能远程进入主机之后进行有意的数据窃取、数据篡改等。

针对资产数量少，运维并发低及可靠性需求不高的小型企业，提供轻量级堡垒机实例，实现运维用户双因子认证、云上资产统一运维审计，满足等保合规测评要求。

产品优势

- 快速开通使用：一键开通，即开即用，方便快捷。
- 小规格成本更低：按设备数包年包月，最低支持 5 资产小规格，成本更低。
- 运维高效快捷：提供 web 及客户端运维两种方式，兼顾便捷性和专业性。
- 安全合规：满足等保测评要求，助力企业运维安全治理。

（二）多人运维管理场景

场景说明

政务、金融及大型央国企运维存在账户重复授权、交叉使用、授权范围过大等问题，面对大量主机资源、系统特权账户，如何做好运维安全治理，防止因账户管理不善导致数据泄漏是非常具有挑战性的问题。

针对资产数量大，运维用户多，可靠性要求高的中大型企业，提供企业版堡垒机，提供双因子认证、资产帐密管理、运维审计、高危命令阻断等能力，满足企业运维安全治理需求。

产品优势

- 运维高效便捷：支持 PuTTY、SecureCRT、Xshell、WinSCP、mstsc 等专业运维工具集成，提升运维效率。

- 精细化权限管理：以 4A 为核心实现用户按角色、资产授权及访问控制，最小化运维授权，降低越权操作风险。
- 安全合规：对所有运维操作集中记录，支持审计、录像及回放，满足等保测评要求，助力企业运维安全治理。

1.5 使用限制

网络访问限制

系统资源所属安全组必须允许实例私有 IP 访问，需要在实例的安全组添加“入方向”的访问规则。

注意：

云堡垒机 Docker0 的网卡地址为：172.17.0.1，请勿占用此网桥网卡地址，否则会导致云堡垒机无法正常使用。

支持纳管的服务器限制

支持 SSH、TELNET、RDP、VNC、FTP、SFTP 协议类型的 Windows 或 Linux 主机。

支持的数据库类型及版本限制

数据库引擎	引擎版本
MySQL	5.5、5.6、5.7、8.0
PostgreSQL	10、11、12、13
Oracle	10g、11g、12c
DB2	10.5、11.5、12
达梦	V8
SQL Server	2016 企业版
天翼云分布式关系型数据库（DRDS）	1.0 建议关联 MySQL5.7 和 8.0 版本

支持的运维终端操作系统限制

终端类型	系统版本	芯片
Windows	windows7 及以上版本	Intel 芯片
Mac	MacOS 10.15 及以上版本	Apple silicon 或 Intel 芯片

支持的运维客户端软件限制

登录方式	支持的客户端	版本
Web 浏览器登录 说明 Html5 运维方式为临时运维方式，若出现显示异常等问题建议使用 MSTSC、VNC 等更稳定的运维方式。	Edge	95 及以上版本
	Chrome	91.0 及以上版本
	Safari	13 及以上版本
	Firefox	50.0 及以上版本
SSH/Telnet 协议运维登录	SecureCRT	8.0 及以上版本
	Xshell	6 及以上版本
	Putty	堡垒机客户端自带
	Mac Terminal	2.0 及以上版本
Sftp/Ftp 协议运维登录 说明 Windows 上面的 FTP 服务不支持上传文件。	Winscp	5 及以上版本
	Filezila	3 及以上版本
数据库运维	Navicat	11、12、15、16、17
	DBeaver	22、23、24
	HeidiSQL 需要自行下载客户端并使用。	10.0 及以上版本
	PL/SQL Developer 需要自行下载客户端并使用。	14.0.2
图形运维	Vnc_viewer	堡垒机客户端自带
	MSTSC	6.0 及以上版本

使用 Navicat 运维达梦数据库时，驱动程序在不同操作系统下的兼容性有所差异，当前支持使用 win2016

运维达梦数据库，win11 系统下 Navicat 没有可用的驱动，如需使用可切换至 DBeaver 运维使用。

支持的区域

区域	一类节点	二类节点
华东地区	杭州 2/杭州 7/合肥 2/华东 1/九江/南 昌 5/南京 3/南京 4/南京 5/上海 15/上海 36/上海 7/芜湖 2/芜湖 4	杭州/南昌/上海 4/苏州/芜湖
华南地区	长沙 3/长沙 42/郴州 2/佛山 3/福州 25/福州 4/广州 6/海口 2/华 南 2/南宁 2/南宁 23/武汉 3/武汉 4/武汉 41/厦门 3/襄阳 2	长沙 2/福州 1/广州 4/海口/南宁/ 深圳/武汉 2
西北地区	兰州 2/庆阳 2/乌鲁木齐 27/乌鲁木齐 4/乌鲁木齐 7/西安 3/西安 4/西安 5/西安 7/西宁 2/中卫 2/中卫 5	兰州/乌鲁木齐/西安 2/西宁/中卫
西南地区	成都 4/重庆 2/贵州 3/昆明 2/拉萨 3/西南 1/西南 2-贵州	成都 3/重庆/贵州 1/昆明
北方地区	北京 5/华北 2/呼和浩特 3/晋中/辽阳 1/内蒙 6/青岛 20/沈阳 8/石 家庄 20/太原 4/郑州 5	北京 2/华北/内蒙 3/青岛/石 家庄/太原/天津/郑州

1.6 术语解释

资产数

资源数是同一个设备对应的需要运维的协议和应用总数。

云堡垒机实例

一个云堡垒机实例代表了一个独立运行的云堡垒机系统。

主备实例

在单机实例基础上增强高可用性。主备实例具有以下特征：

- 实例包含一个主节点和一个备节点，支持数据持久化。
- 主备节点通过数据同步的方式保持一致。
- 备节点对用户不可见，不支持客户端直接读写数据。
- 当主节点故障后，备节点自动升级为主节点，无需用户操作。

区域

区域（Region）：从地理位置和网络时延维度划分，同一个 Region 内共享弹性计算、块存储、对象存储、VPC 网络、弹性公网 IP、镜像等公共服务。Region 分为通用 Region 和专属 Region，通用 Region 指面向公共租户提供通用云服务的 Region；专属 Region 指只承载同一类业务或只面向特定租户提供业务服务的专用 Region。

可用区

可用区（AZ，Availability Zone）：一个 AZ 是一个或多个物理数据中心的集合，有独立的风火水电，AZ 内逻辑上再将计算、网络、存储等资源划分成多个集群。一个 Region 中的多个 AZ 间通过高速光纤相连，以满足用户跨 AZ 构建高可用性系统的需求。

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。

2 计费说明

2.1 计费说明（一类节点）

2.1.1 计费说明

计费模式

云堡垒机实例、存储扩容的计费模式为**包月和包年**计费。

计费项

云堡垒机实例按选购的产品规格和购买时长计费。

计费项目	计费说明	计费公式
云堡垒机实例	按购买实例类型、实例版本、资产规格、购买时长计费。 云堡垒机实例价格已包含配套的云主机。	实例规格单价 * 购买时长
存储扩容	根据您选择的扩容数据盘大小按时长计费。	存储扩容单价 * 购买时长

产品价格（单机版）

实例规格

堡垒机实例规格请参见下表。

说明

- 标准版和企业版的功能差异请参见功能特性。

  标准版和企业版均提供 10、20、50、100、200、500、1000、2000、5000、10000 的资产规格。

- 堡垒机实例享受如下优惠：购买 1 年，在包月总价基础上享受 85 折优惠，购买 2 年享受 7 折优惠，购买 3、4、5 年享受 5 折优惠。

- **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。

资产规格	并发数	标准版资费-单机版（元/个/月）	企业版资费-单机版（元/个/月）	主机规格
10 资产	10 并发上限	650	1020	CPU：2 核，内存：4GB，系统盘：40GB，数据盘：300GB
20 资产	20 并发上限	850	1280	CPU：2 核，内存：8GB，系统盘：50GB，数据盘：300GB
50 资产	50 并发上限	1520	2600	CPU：4 核，内存：16GB，系统盘： 50GB，数据盘：500GB
100 资产	100 并发上限	2520	4600	CPU：8 核，内存：32GB，系统盘： 50GB，数据盘：800GB
200 资产	200 并发上限	3520	6200	CPU：8 核，内存：32GB，系统盘： 50GB，数据盘：800GB
500 资产	500 并发上限	5280	9200	CPU：12 核，内存：48GB，系统盘： 50GB，数据盘：2TB
1000 资产	1000 并发上限	10780	14170	CPU：16 核，内存：64GB，系统盘： 50GB，数据盘：2TB
2000 资产	2000 并发上限	13780	17170	CPU：16 核，内存：128GB，系统盘： 50GB，数据盘：2TB
5000 资产	2000 并发上限	18000	27000	CPU：24 核，内存：192GB，系统盘： 50GB，数据盘：4TB
10000 资产	2000 并发上限	24000	36000	CPU：32 核，内存：192GB，系统盘： 50GB，数据盘：4TB

存储扩容

说明

存储扩容享受如下优惠：购买 1 年，在包月总价基础上享受 85 折优惠，购买 2 年享受 7 折优惠，购买 3、4、5 年享受 5 折优惠。

计费项	标准价格-单机版	计费单位
存储扩容	500	元/月/TB

产品价格（主备版）

实例规格

堡垒机实例规格请参见下表。

说明

- 标准版和企业版的功能差异请参见功能特性。

  标准版和企业版均提供 10、20、50、100、200、500、1000、2000、5000、10000 的资产规格。
- 堡垒机实例享受如下优惠：购买 1 年，在包月总价基础上享受 85 折优惠，购买 2 年享受 7 折优惠，购买 3、4、5 年享受 5 折优惠。
- **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。

资产规格	并发数	标准版资费-主备版（元/个/月）	企业版资费-主备版（元/个/月）	主机规格
10 资产	10 并发上限	1300	2040	CPU：2 核，内存：4GB，系统盘：40GB，数据盘：300GB
20 资产	20 并发上限	1700	2560	CPU：2 核，内存：8GB，系统盘：50GB，数据盘：300GB
50 资产	50 并发上限	3040	5200	CPU：4 核，内存：16GB，系统盘：50GB，数据盘：500GB
100 资产	100 并发上限	5040	9200	CPU：8 核，内存：32GB，系统盘：50GB，数据盘：800GB
200 资产	200 并发上限	7040	12400	CPU：8 核，内存：32GB，系统盘：50GB，数据盘：800GB
500 资产	500 并发上限	10560	18400	CPU：12 核，内存：48GB，系统盘： 50GB，数据盘：2TB

资产规格	并发数	标准版资费-主备版（元/个/月）	企业版资费-主备版（元/个/月）	主机规格
1000 资产	1000 并发上限	21560	28340	CPU：16 核，内存：64GB，系统盘： 50GB，数据盘：2TB
2000 资产	2000 并发上限	27560	34340	CPU：16 核，内存：128GB，系统盘： 50GB，数据盘：2TB
5000 资产	2000 并发上限	36000	54000	CPU：24 核，内存：192GB，系统盘： 50GB，数据盘：4TB
10000 资产	2000 并发上限	48000	72000	CPU：32 核，内存：192GB，系统盘： 50GB，数据盘：4TB

存储扩容

说明

存储扩容享受如下优惠：购买 1 年，在包月总价基础上享受 85 折优惠，购买 2 年享受 7 折优惠，购买 3、4、5 年享受 5 折优惠。

计费项	标准价格-主备版	计费单位
存储扩容	1000	元/月/TB

2.1.2 购买云堡垒机实例

云堡垒机每一个实例对应一个独立运行的云堡垒机运维管理系统环境。

用户首先需要购买一个云堡垒机实例，购买后，系统默认创建一个云堡垒机管理员账号（默认管理员用户 admin），可通过该账号单点登录云堡垒机系统；登录实例后，根据提示配置运维管理环境，实现云堡垒机实时远程高效运维管理。

如何选择实例类型

云堡垒机（原生版）支持“单机版”和“主备版”，可根据实际情况进行选择。

实例类型	单机版	主备版
节点数量	购买后只创建一台堡垒机。	购买后会创建两台堡垒机，形成主备关系。

实例类型	单机版	主备版
可用区选择	您可以根据业务部署需要，为这台堡垒机选择任意一个可用区。	需要分别选择主节点可用区和备节点可用区，可根据容灾或网络时延需求进行选择。 • 场景一：如果有容灾能力的需求，建议主备节点部署在不同的可用区，实现跨可用区容灾。 • 场景二：如果对网络时延有较高要求，建议主备节点部署在同一可用区，优先保证网络性能。
适用场景	适用于无需高可用性的业务场景。	适用于对服务高可用性和业务连续性有要求的场景。
优势	成本低	可靠性高

前提条件

- 已获取管理控制台的登录账号与密码。
- 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

1.登录管理控制台。

2.选择“安全 > 云堡垒机（原生版）”，进入云堡垒机实例管理页面。

3.单击右上角的“购买堡垒机”，进入产品订购页。

4.选择“云堡垒机实例”相关参数，参数相关说明请参考下表。

参数	说明
部署架构	选择新购堡垒机的部署架构，目前支持：通用性 x86、鲲鹏 ARM、海光 X86、飞腾 ARM。
实例类型	支持“单机版”和“主备版”。
可用区	实例类型选择“主备版”时，可以分别为主节点和备节点选择不同的可用区。
实例名称	自定义云堡垒机实例名称。 长度为 2-15 字符，以字母开头，可包含数字、“.”、“_”、“-”，不可包含中文。
版本	目前支持“标准版”和“企业版”，各版本支持的功能请参见功能特性。

参数	说明
资产规格	选择需要纳管的资产数，堡垒机在不同资源池版本支持的资产数略有不同，请根据实际需要选择。 支持 10/20/50/100/200/500/1000/2000/5000/10000 资产规格。
企业项目	选择堡垒机实例所属的企业项目。 说明 订购完成后，企业项目不支持修改。
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。 注意 • 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 网络下的 ECS 等资源，通过堡垒机纳管资源后，可直接访问并管理对应的资源。 • 订购完成后，虚拟私有云不支持修改。
安全组	选择当前区域下安全组，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、并相互信任的堡垒机资源提供访问策略。当云堡垒机加入安全组后，即受到该安全组中访问规则的保护。 • 云堡垒机可与资源主机 ECS 等共用安全组，各自调用安全组规则互不影响。 • 如需修改安全组，请参见更改安全组。
子网	选择当前 VPC 内子网。 说明 子网选择必须在 VPC 的网段内。
弹性 IP	（可选）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。
存储扩容	根据您业务自身的需求选择需要扩容的数据盘大小。

5. 选择“购买时长”，可按月或按年购买云堡垒机。

支持开启“到期自动续费”，当服务到期前，系统会自动按照默认的续订周期生成续费订单并进行续费，无须用户手动续费。

6. 确认参数配置无误后，阅读并同意相关协议，单击“立即购买”。

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。

2.1.3 变更实例规格

当云堡垒机的资产规格不能满足需求时，可对云堡垒机实例进行资产规格升级，扩大纳管的资产数上限。

系统影响

变更规格过程大约需要 10 分钟，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。

约束限制

- 只有 2.0 及以上版本的堡垒机支持提升规格。
- 当前仅支持同版本、同实例规格内变更资产规格，不支持跨版本变更或跨实例规格变更。
- 仅支持云堡垒机资产规格升级，暂不支持资产规格降级，若需要降级，请先备份相关数据，退订堡垒机实例后重新订购新实例。

前提条件

- 已获取管理控制台的登录账号与密码。
- 已绑定 EIP，且 EIP 可用。
- 实例的状态为“已关机”时支持变更规格。

计费样例

计费场景：

某用户于 2025/01/01 购买了一个云堡垒机实例，购买时长 1 年（在包月总价基础上享受 85 折优惠），规格如下：

- 实例类型：单机版
- 版本：标准版
- 资产规格：10 资产

使用一段时间后，用户发现当前规格无法满足业务需要，于 2025/10/01 进行升级（还剩 3 个月到期），需要升级的规格如下:

- 实例类型：单机版
- 版本：企业版
- 资产规格：20 资产计费分析:

新配置价格高于老配置价格，执行升级操作时，您需要支付新老配置的差价。计算公式:

升级费用=（新配置价格-旧配置价格）*剩余周期*优惠折扣

本示例中，相关参数如下:

- 旧配置价格：10 资产标准版，标准资费 650 元/个/月
- 新配置价格：20 资产企业版，标准资费 1280 元/个/月
- 剩余周期：3 个月
- 优惠折扣：享受 85 折优惠

> 说明
>
> 若实例升级时仍在原包年周期内，则升级差价可继续享受原有的包年折扣。

代入公式可得，执行升级时需要支付的费用为：（1280-650）×3×0.85= 1606.5 元

注意

本样例仅供参考，实际需支付的费用请以云堡垒机（原生版）控制台展示为准。

操作步骤

1.登录管理控制台。

2.选择“安全 > 云堡垒机（原生版）”，进入云堡垒机实例管理页面。

3.选择需变更规格的实例，单击所在行“操作”列中“更多 > 关闭实例”，待实例状态变更为“已关机”后，单击中“更多>变更规格”，跳转到“变更规格”页面。

4.选择需变更的“资产规格”，单击“立即购买”。

当您选择变更堡垒机的规格时，不支持扩容资产。

5. 在支付页面完成付款。

6.后台自动进行变更规格操作，整个变更规格过程需 10min 左右。

7.实例运行状态变为“运行”，即可正常使用云堡垒机。

2.1.4 续费与退订

控制台续费

- 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 15 天内，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，若未及时续费，则进入“保留期”，不能登录云堡垒机系统。“保留期”为 15 天，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。

前提条件

已获取控制台的登录账号与密码。

操作步骤

1.登录管理控制台。

2.选择“安全 > 云堡垒机（原生版）”，进入云堡垒机实例管理页面。

3.选择待续费的实例，单击“更多 > 续费”，进入“续费”配置页面。

4.根据需要选择续费时长。

5.单击“去支付”，在支付页面完成付款。

6.返回云堡垒机实例列表页面，在“云堡垒机实例”列表查看授权后最新到期时间。

管理中心续订

登录天翼云官网，进入管理中心，选择续订管理，点击“手动续订”或者“开通自动续订”按钮，即可完成实例的续订。

2.2 计费说明（二类节点）

2.2.1 计费说明

计费模式

云堡垒机实例的计费模式为包月和包年计费。

计费项

云堡垒机实例按选购的产品规格和购买时长计费。

计费项目	计费说明
云堡垒机实例	按购买实例的版本、实例规格、资产规格和购买时长计费。

产品价格

此处价格仅为云堡垒机（原生版）的价格，实际结算页面会根据您所选择的云主机规格有所变动，云主机规格价格可参考：云主机价格。

说明

- 购买 1 年，在包月总价基础上享受 85 折优惠，购买 2 年享受 7 折优惠，购买 3、4、5 年享受 5 折优惠。
- 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。

版本	资产规格	并发数	标准资费（元/个/月）
高级版	10 资产	10 并发上线	860
高级版	20 资产	20 并发上限	999
高级版	50 资产	50 并发上限	1888
高级版	100 资产	100 并发上限	2999
高级版	200 资产	200 并发上限	4350
高级版	500 资产	500 并发上限	6230

版本	资产规格	并发数	标准资费（元/个/月）
高级版	1000 资产	1000 并发上限	11100
高级版	2000 资产	2000 并发上限	14000
高级版	5000 资产	2000 并发上限	20000
高级版	10000 资产	2000 并发上限	29550

2.2.2 购买云堡垒机实例

云堡垒机每一个实例对应一个独立运行的云堡垒机运维管理系统环境。

用户首先需要购买一个云堡垒机实例，购买后，系统默认创建一个云堡垒机管理员账号（默认管理员用户admin），可通过该账号单点登录云堡垒机系统；登录实例后，根据提示配置运维管理环境，实现云堡垒机实时远程高效运维管理。

前提条件

- 已获取管理控制台的登录账号与密码。
- 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

1. 登录管理控制台。
2. 选择“安全 > 云堡垒机（原生版）”,进入云堡垒机实例管理页面。
3. 单击右上角的“购买堡垒机”，进入产品订购页。
4. 选择“云堡垒机实例”基础信息和资产规格。

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。
部署架构	选择新购堡垒机的部署架构，目前支持：通用性 x86、鲲鹏 ARM、海光 X86、飞腾 ARM。

地域/可用区	选择实例应用区域和可用区，即提供云堡垒机服务的区域和可用区。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。 长度为 2-15 字符，以字母开头，可包含数字、“.”、“_”、“-”，不可包含中文。
实例规格	选择实例规格，目前仅支持“单机版”。
版本	支持“高级版”，该版本支持的功能清单请到功能特性查看。
资产规格	选择需要纳管的资产数，堡垒机不同版本支持的资产数略有不同，请根据实际需要选择。

5. 配置云堡垒机实例的网络信息。

参数	说明
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。 注意 • 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 网络下的 ECS 等资源，通过堡垒机纳管资源后，可直接访问并管理对应的资源。 • 订购完成后，虚拟私有云不支持修改。
安全组	选择当前区域下安全组，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、并相互信任的堡垒机资源提供访问策略。当云堡垒机加入安全组后，即受到该安全组中访问规则的保护。 • 云堡垒机可与资源主机 ECS 等共用安全组，各自调用安全组规则互不影响。 • 如需修改安全组，请参见更改安全组。
子网	选择当前 VPC 内子网。 子网需在 VPC 的网段内。
弹性 IP	（可选）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。

6. 选择配套的弹性云主机规格，包括云主机规格、系统盘、数据盘。

- 云主机规格默认选择最低规格，您可在下拉框中选择主机规格或者输入规格名称进行搜索（支持模糊搜索）。
- 系统盘和数据盘默认选择最低规格，您可根据业务实际需求进行适量提升。

具体云主机规格需求如下：

版本	资产规格	并发数	推荐云主机规格			
			CPU	内存	系统盘	数据盘
高级版	10 资产	10 并发上线	2 核	8GB	40GB	200GB
高级版	20 资产	20 并发上限	2 核	8GB	50GB	300GB
高级版	50 资产	50 并发上限	4 核	16GB	50GB	500GB
高级版	100 资产	100 并发上限	8 核	32GB	50GB	800GB
高级版	200 资产	200 并发上限	8 核	32GB	50GB	800GB
高级版	500 资产	500 并发上限	12 核	48GB	50GB	2048GB
高级版	1000 资产	1000 并发上限	16 核	64GB	50GB	2048GB
高级版	2000 资产	2000 并发上限	16 核	128GB	50GB	2048GB
高级版	5000 资产	2000 并发上限	24 核	192GB	50GB	4096GB
高级版	10000 资产	2000 并发上限	32 核	192GB	50GB	4096GB

7. 选择“购买时长”，可按月或按年购买云堡垒机。

支持开启“到期自动续费”，当服务到期前，系统会自动按照默认的续订周期生成续费订单并进行续费，无须用户手动续费。

8. 确认参数配置无误后，阅读并同意相关协议，单击“立即购买”。

9. 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。

2.2.3 变更实例规格

当云堡垒机的资产规格不能满足需求时，可对云堡垒机实例进行资产规格升级，扩大纳管的资产数上限。

注意

- 当前仅支持同实例规格内变更资产规格，不支持跨实例规格变更。
- 仅支持云堡垒机资产规格升级，暂不支持资产规格降级，若需要降级，请先备份相关数据，退订堡垒机实例后重新订购新实例。
- 只有 2.0 及以上版本的堡垒机支持提升规格。

前提条件

- 已获取管理控制台的登录账号与密码。
- 实例已绑定 EIP，且 EIP 可用。
- 实例的状态为“运行中”时，支持变更规格。

步骤一：变更资产规格

1. 登录管理控制台。
2. 选择“安全 > 云堡垒机（原生版）”,进入云堡垒机实例管理页面。
3. 选择需变更规格的实例，单击“更多 > 变更规格”，跳转到“变更规格”页面。

4. 选择需变更的“资产规格”。

5. 阅读并同意相关协议后，单击“提交订单”。在订单详情页面根据提示完成支付。

后台自动进行变更规格操作，实例状态更新为“变配中”，整个变更规格过程需 10 分钟左右。

变更完成后，实例状态恢复为“运行中”。

步骤二：变更云主机规格

变更资产规格完成后，还需要再变更搭载堡垒机的云主机规格。

- 云主机对应规格详情请见云堡垒机（原生版）计费模式。
- 云主机升配规格请参见弹性云主机变更规格。

2.2.4 续订与退订

控制台续费

- 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 15 天内，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，若未及时续费，则进入“保留期”，不能登录云堡垒机系统。“保留期”为 15 天，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。
- 堡垒机续费不会自动续费云主机，请您手动续订对应云主机。

前提条件

已获取控制台的登录账号与密码。

操作步骤

1. 登录管理控制台。
2. 选择“安全 > 云堡垒机（原生版）”,进入云堡垒机实例管理页面。
3. 选择待续费的实例，单击“更多 > 续费”，进入“续费”配置页面。

4. 根据需要选择续费时长。

5. 单击“去支付”，在支付页面完成付款。

6. 返回云堡垒机实例列表页面，在“云堡垒机实例”列表查看授权后最新到期时间。

管理中心续订

登录天翼云官网，进入管理中心，选择续订管理，点击“手动续订”或者“开通自动续订”按钮，即可完成实例的续订。

退订

> 说明
>
> 退订堡垒机不会自动退订对应云主机，请您单独退订云主机。

前提条件

- 已获取管理控制台的登录账号与密码。
- 已使用的云堡垒机，需停止系统所有操作，解绑 EIP。

操作步骤

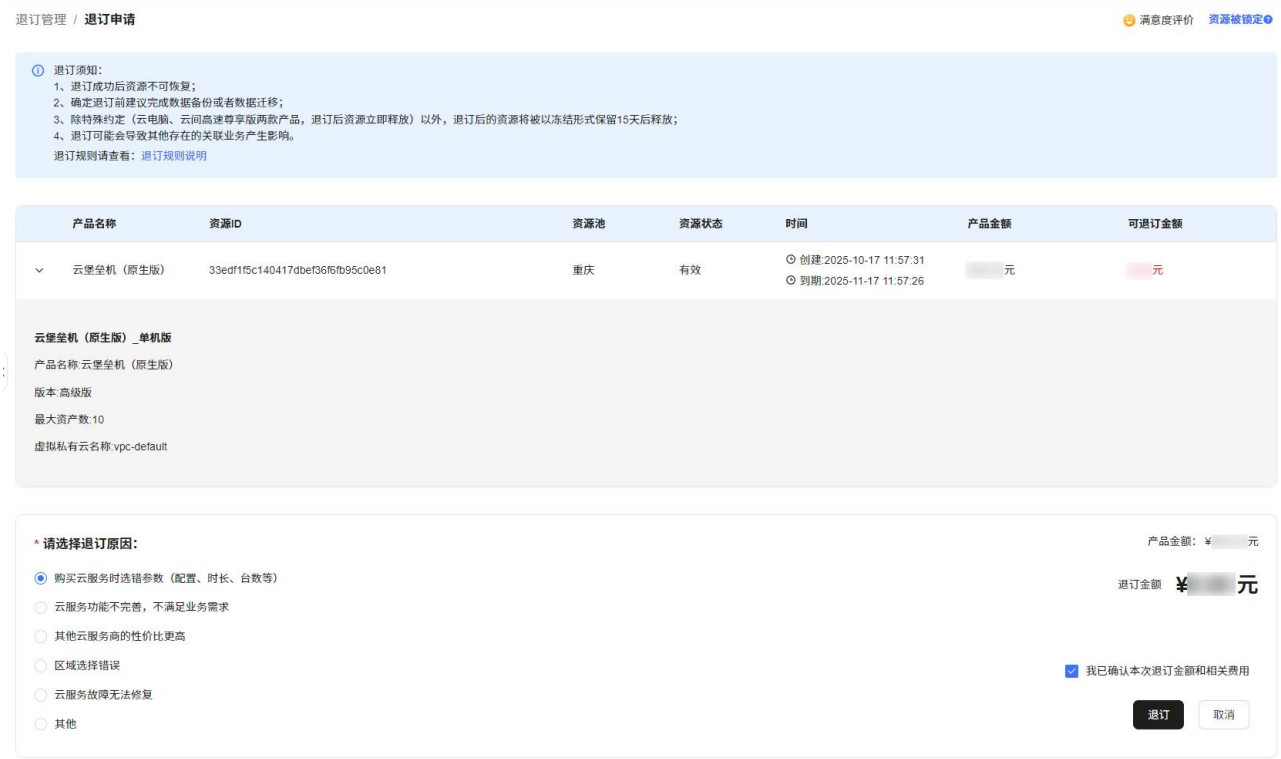
1. 登录管理控制台。

2. 选择“安全 > 云堡垒机（原生版）”,进入云堡垒机实例管理页面。

3. 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。

4. 在弹出的退订提示框中，确认实例信息无误后，单击“确认”，进入“费用中心 > 退订管理 > 退订申请”页面。

5. 在退订申请页面，确认退订信息，信息确认无误后选择退订原因，勾选“我已确认本次退订金额和相关费用”后，点击“退订”后即可进行退订。



到期与欠费

- 包周期资源开通成功后，如果没有按时续费，云平台会提供一定的保留期。

- 保留期：指宽限期到期后客户的包年/包月资源仍未续订或按需资源仍未缴清欠款，将进入保留期。保留期内客户不能访问及使用云服务，但对客户存储在云服务中的数据仍予以保留。
- 云服务进入保留期后，天翼云将会通过邮件、短信等方式向您发送提醒，提醒您续订或充值。保留期到期仍未续订或充值，存储在云服务中的数据将被删除、云服务资源将被释放。
- 欠费后，可以查看欠费详情。为防止相关资源被停止或者释放，请及时进行充值，账号将进入欠费状态，需要在约定时间内支付欠款。

3 快速入门

3.1 步骤一：安全组策略设置

开通云堡垒机需要绑定 EIP，在用户通过 EIP 访问堡垒机之前需要配置安全组策略，编辑入项策略，用户才可通过 EIP 直接访问云堡垒机。

说明

- 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和堡垒机 CBH 实例提供访问策略。
- 为了保障堡垒机的安全性和稳定性，在使用堡垒机实例之前，您需要设置安全组，开通需访问堡垒机的 IP 地址和端口。

堡垒机端口开放说明

注意：为确保系统安全，请合理配置堡垒机安全组策略，避免将高危端口（如 SSH、RDP 等）直接暴露在公网，建议通过白名单限制访问源 IP 或结合 VPN 专线访问

推荐开放 18443,18000 端口的入方向安全组策略规则，其他端口根据运维场景需要按需进行配置。

云堡垒机使用端口用途详见下表：

端口	用途	说明

端口	用途	说明
18443	门户端口，及 H5 运维端口	访问堡垒机门户页面时需开放该端口的入方向规则，（并可支持 H5 方式运维资产）
18000	字符资产访问端口	需通过堡垒机维护字符类协议资产时，需开放该端口的入方向规则
19000	图形资产访问端口	需通过堡垒机使用 mstsc 客户端维护图形类协议资产时，需开放该端口的入方向规则
20000	图形资产访问端口	需通过堡垒机使用 vncview 客户端维护图形类协议资产时，需开放该端口的入方向规则
6003	数据库资产访问端口	需通过堡垒机维护数据库协议资产时，需开放该端口的入方向规则
8765	数据库资产访问端口	需通过堡垒机维护数据库协议资产时，需开放该端口的入方向规则
5662	获取授权信息以及升级端口	堡垒机升级以及或者获取资源池信息，需开放该端口的入方向规则 说明 仅“二类节点”区域的实例涉及该端口。

安全组规则设置

注意

- 安全组的默认规则是在出方向上的数据报文全部放行，同一个安全组内的弹性云服务器和堡垒机实例可互相访问。安全组创建后，您可以在安全组中定义各种访问规则，当堡垒机实例加入该安全组后，即受到这些访问规则的保护。
- 默认情况下，一个租户可以创建 500 条安全组规则。
- 为一个安全组设置过多的安全组规则会增加首包延时，因此，建议一个安全组内的安全组规则不超过 50 条。
- 当需要从安全组外访问安全组内的堡垒机实例时，需要为安全组添加相应的入方向规则。
- 源地址默认的 IP 地址 0.0.0.0/0 是指允许所有 IP 地址访问安全组内的堡垒机实例。

堡垒机弹性 IP 安全组访问规则设置：

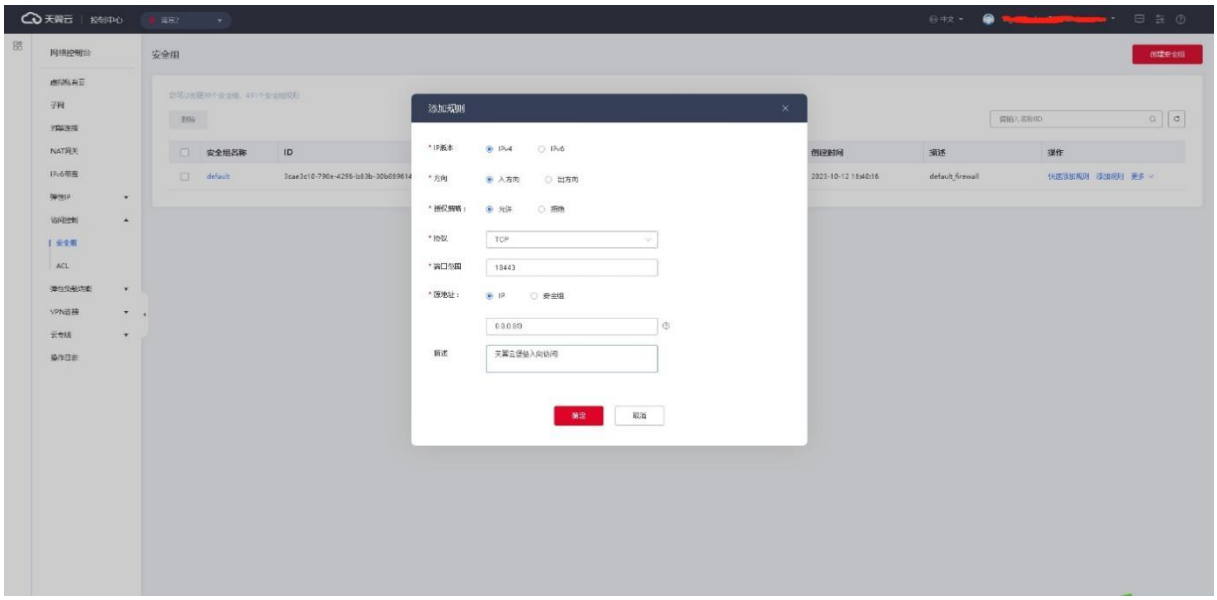
1. 登录管理控制台。
2. 在系统首页，单击“网络 > 弹性 ip”。

3. 在左侧导航树选择“访问控制 > 安全组”。

4. 在安全组界面，单击操作列的“配置规则”，进入安全组详情界面。

5. 在安全组详情界面，单击“添加规则”，弹出添加规则窗口。

6. 根据界面提示配置安全组规则。



3.2 步骤二：登录云堡垒机实例

开通堡垒机（原生版）后，用户在控制台 “云堡垒机实例”页面，在操作列点击“管理”操作，系统单点登录进入云堡垒机实例，通过控制台登录进入默认管理员用户。

登录的时候可选“外网地址登录”或“内网地址登录”。

- 内网地址登录需要确保网络环境互通。
- 外网地址登录需要绑定弹性 IP。

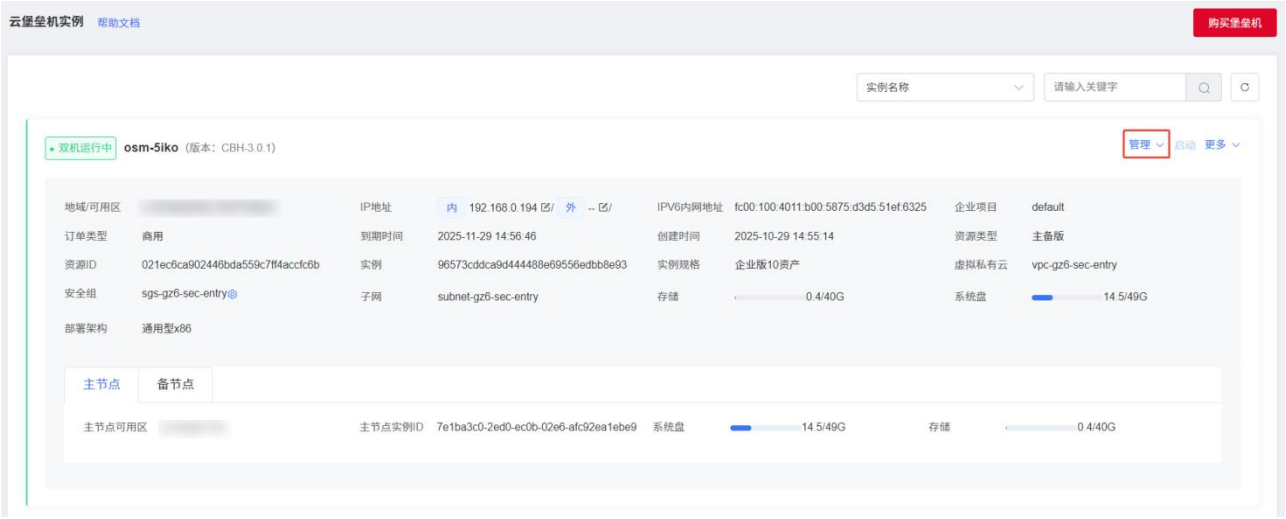
首次登录

在未设置初始密码时，需通过云堡垒机控制台单点登入跳转登入堡垒机，并进行初始化管理操作。

1. 在“云堡垒机实例”列表条目录中选择要管理的实例，单击“管理”。

2. 根据您自身的网络环境选择“内网地址登录”或“外网地址登录”。

3. 登入堡垒机后，通过个人信息进行初始密码设置。



非首次登入

非首次登入云堡垒机可通过云堡垒机控制台单点登入跳转登入堡垒机，或通过云堡垒机登录地址使用账号认证方式登录。

前置条件

已登录过云堡垒机并完成密码初始化。

操作步骤

1. 启动浏览器，在浏览器 Web 地址栏中输入系统登录地址，进入到系统登录页面。
2. 选择账号开通的认证方式。
3. 输入系统管理员 admin 的账号和密码，输入图形验证码。
4. 单击“登录”，成功登录到堡垒机系统。

3.3 步骤三：新增账号和资产

新增用户账号

在使用云堡垒机进行运维前，管理员需要先创建系统用户，并为系统用户分配角色身份。不同的角色身份，拥有不同的菜单权限和操作权限。

1. 管理员 admin 登录云堡垒机系统。

2. 角色身份切换到“管理角色”。

3. 在左侧导航栏，选择用户管理>账号管理>新增。

4. 填写账号基本信息，并选择角色身份，单击保存提交。

参数	参数说明
登录名	填写该账户的登录名称。 只能为数字、大小写字母、“.”和“_”组成，首位只能数字或者字母，且不超过 25 个字符；
姓名	填写该账户的使用者的姓名。
手机号	填写手机号，请确保手机号真实有效，否则会影响短信的接收。
邮箱	（选填）填写邮箱地址，请确保邮箱地址真实有效，否则会影响告警信息的接收。
用户密码	输入该账户的密码。密码请根据管理员设置的密码规则填写，具体可参见：安全设置章节。
确认密码	二次确认账户密码。
角色	选择该账户所属的角色，可选“管理角色”、“审计角色”和“访问角色”。
用户组	选择该账户所属的用户组，用户组操作请参见：用户组章节。
认证方式	选择认证方式，可选“静态认证”和“令牌认证”。
生效时间	选择该账户可登录的时间段。
准入 IP	选择可登录的 IP 地址。
准入 MAC	填写该用户允许登录的 MAC 地址。

新增资产和资产账号

云堡垒机系统集中管理云资源，主要包括管理资产账户和运维权限管理。为实现统一管理资源，需添加资产到系统。

一个主机或应用资产可能有多个登录主机或应用的账户。云堡垒机系统纳管主机或应用的账户（资产账户）后，无需反复输入账户和密码，通过登录资产账户，自动登录资源进行运维管控。

1. 管理员 admin 登录云堡垒机系统，角色身份切换到“管理角色”。

2. 在左侧导航栏，点击 资产管理>基础设施>新增。

3. 填写资产信息，单击保存提交。

参数	参数说明
资产名称	输入您需要纳管的资产名称。
资产类型	选择待纳管的资产类型。
IP 地址	填写待纳管资产的 IP 地址，请确保资产 IP 的正确。
资产组	选择待纳管资产所属的资产组。
资产描述	添加资产的描述。
协议	选择访问待纳管资产的访问协议，并添加协议的端口号。
账号	添加待纳管资产下的维护账号。
访问信息	选择访问资产的系统编码，可选“UTF-8”和“GBK”。

4. 选择资产账号，单击新增，填写资产账号信息并勾选相应的访问协议。

资产账号也可通过选择“资产管理 > 资产账号”，新增资产账号。

5. 单击提交，完成资产创建。

3.4 步骤四：配置运维权限

在使用云堡垒机进行运维前，管理员需要通过访问授权关联用户和资产，赋予用户对相应资产的访问权限。

操作步骤

1. 管理员 admin 登录云堡垒机系统。
2. 角色身份切换到“管理角色”。
3. 在左侧导航栏，点击授权管理>访问授权>新增。
4. 填写授权基本属性并通过维度属性关联账号以及资产和资产账号。

参数	参数说明
授权规则名	填写资产访问授权的规则名称。
启用状态	通过开关控制该条授权规则的启用状态，默认状态为开启。
用户	选择资产访问授权允许生效的用户，可多选。
用户组	选择资产访问授权允许生效的用户组，可多选。
资产	选择该条授权规则允许访问的资产，可多选。
资产组	选择该条授权规则允许访问的资产组，可多选。
资产账号	选择该条授权规则下允许使用的资产账号，可多选。
协议	选择资产访问的协议类型，可多选。
生效日期/失效日期	选择该条授权规则的生效/失效日期。
生效时间/失效时间	选择该条授权规则的生效/失效时间段。

5. 填写完成后，单击“提交”。

3.5 步骤五：资产运维

堡垒机运维员可以通过客户端运维和网页运维方式对已授权的资产进行运维。

客户端运维

前置条件：

- 堡垒机成功纳管资产，且堡垒机与资产的网络可连通

- 运维账号已开通且分配了运维角色，同时对账号进行了资产访问授权
- 本地终端已安装访问控件并且正确对访问控件进行设置。

操作步骤

1. 用户账号登录云堡垒机系统。

2. 角色身份切换到“访问角色”。

3. 在左侧导航栏，选择基础设施。

4. 单击目标运维主机，在右下方访问图标选择访问方式

（xshell/putty/secureCRT/vnc/mstsc/Filezila/WinSCP）访问。

网页运维

用户可通过网页直接访问资产，无需安装运维客户端即可完成运维。

说明：通过 Html5 登录堡垒机只支持进行简单的运维操作，复杂运维可能出现卡顿，显示异常等问题，建议您安装插件并且使用使用 mstsc，vnc 等方式进行运维。

操作步骤

1. 用户账号登录云堡垒机系统。

2. 角色身份切换到“访问角色”。

3. 在左侧导航栏，选择基础设施。

4. 单击目标运维主机，在右下方访问图标选择 webterminal 方式访问。

3.6 步骤六：审计运维

系统用户登录堡垒机并对已授权资产进行运维操作，管理员在堡垒机上可以查看到会话详情并播放运维录屏，实时监控运维会话并且可以中断高危风险会话。

前置条件

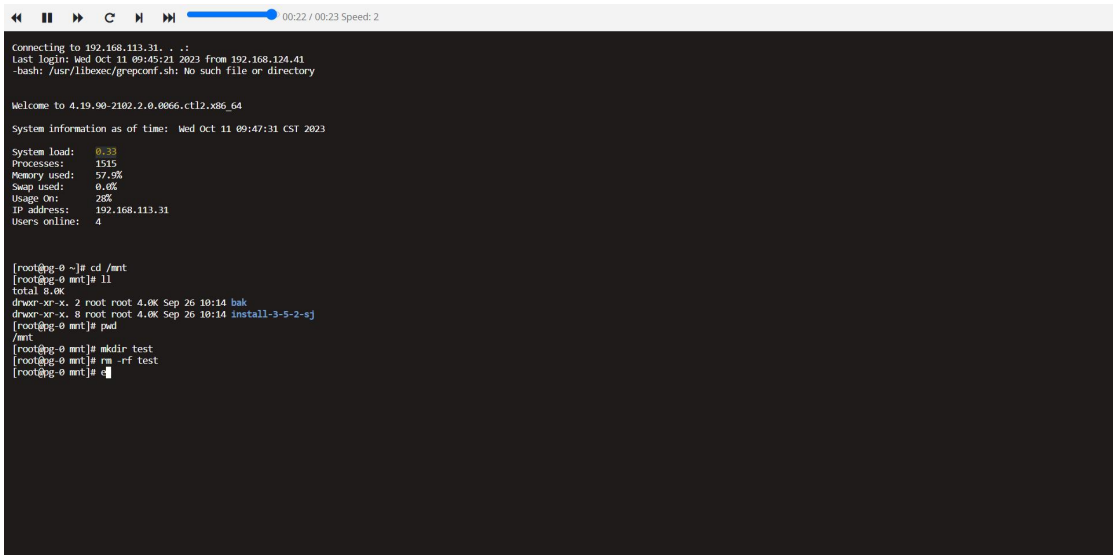
- 用户完成资产运维。
- 登录授权的审计管理员账号或管理员账号。

操作步骤

1. 管理员 admin 或审计管理员登录云堡垒机系统。

   若使用管理员账号登录，需在页面右上角将角色身份切换到“审计角色”。

2. 在左侧导航栏，选择资源会话>字符审计。
3. 设置搜索条件，单击查询，可快速检索到想要审计的会话记录。
4. 通过查看按钮，查看用户的详细操作记录。
5. 通过播放按钮，可在线实时审计或回放用户的操作行为。


00:22 / 00:23 Speed: 2
Connecting to 192.168.113.31. . .:
Last login: Wed Oct 11 09:45:21 2023 from 192.168.124.41
-bash: /usr/libexec/grepconf.sh: No such file or directory
Welcome to 4.19.90-2102.2.0.0066.ctl2.x86_64
System information as of time: Wed Oct 11 09:47:31 CST 2023
System load: 0.33
Processes: 1515
Memory used: 57.9%
Swap used: 0.0%
Usage On: 28%
IP address: 192.168.113.31
Users online: 4
[root@pg-0 ~]# cd /mnt
[root@pg-0 mnt]# ll
total 8.0K
drwxr-xr-x. 2 root root 4.0K Sep 26 10:14 bak
drwxr-xr-x. 8 root root 4.0K Sep 26 10:14 install-3-5-2-sj
[root@pg-0 mnt]# pwd
/mnt
[root@pg-0 mnt]# mkdir test
[root@pg-0 mnt]# rm -rf test
[root@pg-0 mnt]# e

4 实例管理

4.1 实例状态说明

云堡垒机实例常见状态说明如下:

状态	含义&造成原因	影响	解决措施
运行中	堡垒机正常开机运行	-	-
离线	堡垒机失去了到控制中心的连接，心跳信息没有成功发送到控制中心侧。 一般是与控制中心网络不通导致。	• 影响用户的升级和续订。 • 后台无法及时监控资源状态，导致资源占满堡垒机服务不可用时，无法及时监控告警。 说明 此状态属于监控告警，暂时不影响堡垒机本身业务，但建议及时排查处理。	• 实例在“一类节点”：请提交工单联系技术支持进行排查。 • 实例在“二类节点”：请检查网络，确保堡垒机网络可连通公网。
冻结中	堡垒机资源已过期冻结，但未销毁。	用户无法使用堡垒机，堡垒机处于关机状态。	在资源销毁前及时续费。
创建中	订购堡垒机后，正在初始化。	用户无法使用堡垒机，堡垒机处于初始化阶段。	一般等待约 15 分钟后，会自动转为“运行中”状态。 如果状态长时间未发生变化： • 实例在“一类节点”：请提交工单联系技术支持进行排查。 • 实例在“二类节点”：请检查网络，确保堡垒机网络可连通公网。

初始化失败	堡垒机创建失败	用户无法使用堡垒机。	请提交工单联系技术支持进行排查。
升级中	正在升级实例版本	用户无法使用堡垒机。	一般等待约 15 分钟后，会自动转为“运行中”状态。 如果状态长时间未发生变化： • 实例在“一类节点”：请提交工单联系技术支持进行排查。 • 实例在“二类节点”：请检查网络，确保堡垒机网络可连通公网。

4.2 登录实例

开通堡垒机（原生版）后，用户在控制台 “云堡垒机实例”页面，在操作列点击“管理”操作，系统单点登录进入云堡垒机实例，通过控制台登录进入默认管理员用户。

登录的时候可选“外网地址登录”或“内网地址登录”。

说明：

- 内网地址登录需要确保网络环境互通。
- 外网地址登录需要绑定弹性 IP。
- 通过 Html5 登录堡垒机只支持进行简单的运维操作，复杂运维可能出现卡顿，显示异常等问题，建议您安装插件并且使用使用 mstsc，vnc 等方式进行运维。

首次登录

在未设置初始密码时，需通过云堡垒机控制台单点登入跳转登入堡垒机，并进行初始化管理操作。

1.在“云堡垒机实例”列表条目录中选择要管理的实例，单击“管理”。

2.根据您自身的网络环境选择“内网地址登录”或“外网地址登录”。

3.登入堡垒机后，通过个人信息进行初始密码设置。

4.3 查看实例详情

购买云堡垒机实例后，可以查看实例的详细信息，包括实例状态、IP 地址等信息。

查看实例信息

1. 登录管理控制台。
2. 选择“安全 > 云堡垒机（原生版）”，进入云堡垒机实例管理页面。
3. 查看实例的基本信息、网络信息、节点信息。

参数	说明
实例状态	当前实例的运行状态，更多信息请参见实例状态说明。
实例名称	当前实例的名称，购买实例后不支持修改。
实例版本	当前实例的版本。 若实例不是最新版本，可单击“升级”升级到最新版本。详细操作请参见升级实例版本。
地域/可用区	当前实例的地域/可用区。
IP 地址	当前实例的内网地址和外网地址，支持修改。 单击地址旁边的编辑按钮，可修改 IP 地址。仅单机版支持修改内网地址。
IPV6 内网地址	当前实例的 IPV6 内网地址。
企业项目	当前实例绑定的企业项目名称。
到期时间	当前实例到期的时间。 若购买的实例即将到期或已经到期，可单击“更多 > 续费”，延长当前实例规格的使用时长，详细操作请参见续订实例。
创建时间	当前实例的创建时间。
资源类型	当前实例的类型，单机版或主备版。
资源 ID	当前实例的资源 ID。通过资源 ID 可以在订单管理页面查找相关订单。
实例	当前实例的实例 ID。
实例规格	当前实例的资产规格。 当云堡垒机的资产规格不能满足需求时，可对云堡垒机实例进行资产规格升级，扩大纳管的资产数上限、增加存储容量，变更规格详细操作请参见变更实例规格。
虚拟私有云	当前实例绑定的 VPC，购买实例后不支持切换 VPC。
安全组	用户配置的虚拟网络环境安全规则。
子网	当期实例配置的 VPC 网络的子网。
存储	当前实例系统盘的使用情况。
系统盘	当前实例系统盘的使用情况。
部署架构	当前实例的部署架构。

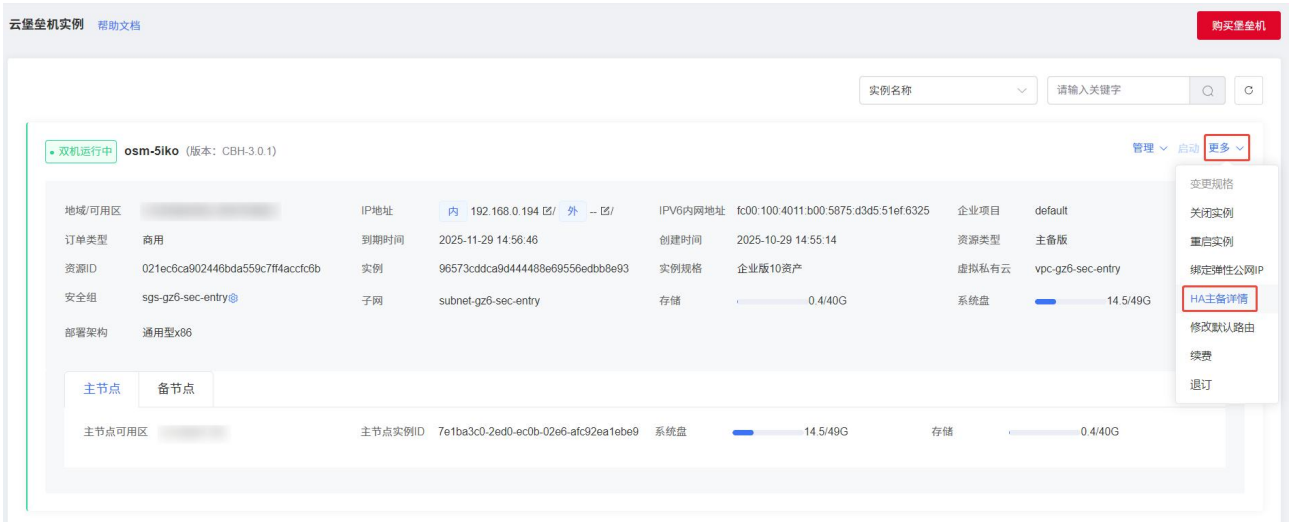
主节点	当前实例主节点的可用区、实例 ID、系统盘、存储信息。
备节点	当前实例备节点的可用区、实例 ID、系统盘、存储信息。 仅“资源类型”为“主备版”才可查看此项。

查看实例 HA 主备详情

购买云堡垒机主备版实例后，可以通过 HA 主备详情查看 HA 状态、IP 地址、接口等信息。

> 说明
>
> 仅“一类节点”区域的实例支持主备版。

1. 登录管理控制台。
2. 选择“安全 > 云堡垒机（原生版）”，进入云堡垒机实例管理页面。
3. 选择目标实例，单击“更多 > HA 主备详情”。



4. 查看 HA 主备详情，查看主备节点的运行状态、IP 地址等信息。

4.4 升级实例版本

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。

注意：

- 在堡垒机升级至 1.3.0 版本后，需要卸载旧的访问插件，在“运维设置 > 访问插件”中下载最新版本插件进行安装。
- 堡垒机在升级失败后会自动回退版本。

前提条件

- 已获取管理控制台的登录账号与密码。

- 已绑定 EIP，且 EIP 可用。

操作步骤

1.登录管理控制台。

2.选择“安全 > 云堡垒机（原生版）”，进入云堡垒机实例管理页面。

3.选择需变更升级的实例，单击所在行“操作”列中“更多 > 升级版本”，或单击实例名称旁的提示框中“升级”。

4.在弹出的对话框中单击“确定”，堡垒机开始进行自动升级并且堡垒机的状态会变为“升级中”。

5.待堡垒机状态变为“运行中”即表示升级已经结束，可正常使用堡垒机。

4.5 更改实例安全组

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。

使用云堡垒需要设置安全组：

- 方式一：配置安全组规则。
- 方式二：切换安全组，若因安全组限制无法修改安全组规则，可以选择更改安全组。

操作步骤

1.登录管理控制台。

2.选择“安全 > 云堡垒机（原生版）”，进入云堡垒机实例管理页面。

3.选择需要更改安全组的堡垒机实例，在实例详情页单击齿轮按钮。

4.在弹出的对话框中选择需要更改的安全组，选择完成后单击保存即可完成安全组的修改。

4.6 修改默认路由

云堡垒机（原生版）实例的默认路由指向用户 VPC 的默认网关，若用户需要临时修改默认路由，可参考本文进行操作。

注意

本操作仅用于临时修改实例的默认路由，重启实例后修改的默认路由会失效，恢复原有路由。

约束限制

仅 v2.12 及以上版本支持修改默认路由。若实例版本较低，请参见升级实例版本进行升级。

操作步骤

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > 云堡垒机（原生版）”，进入云堡垒机实例管理页面。
4. 选择需要修改默认路由的堡垒机实例，单击“更多 > 修改默认路由”。

5. 进入修改默认路由页面，单击“下一跳网关（仅内网）”列的按钮，在弹出的窗口中配置内网 IP 地址后，单击“确定”。

6. 单击“是否生效”列的开关，开关开启，修改的默认路由才生效。
7. 配置完成后，单击“确定”。

4.7 标签管理

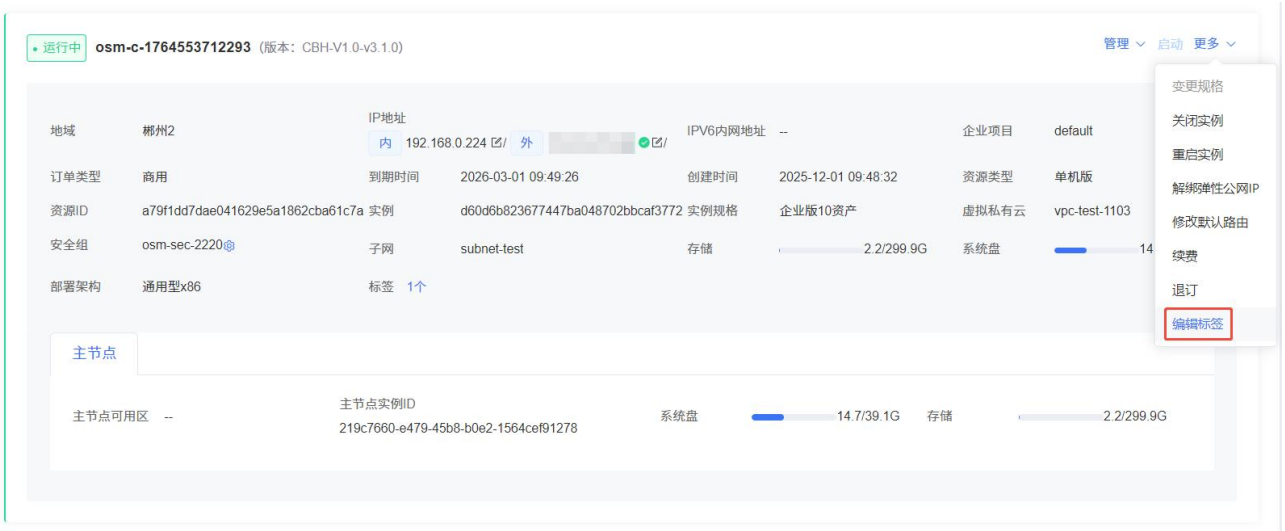
标签是对实例的标识。基于标签，您可以实现对实例的便捷搜索和整理。 标签由键值对（Key-Value）组成，您可以为实例绑定和解绑标签，在控制台中通过标签快速查找实例。

约束限制

- 每个实例最多可绑定 10 个标签。
- 每个实例下的标签键是唯一的，不可绑定相同标签键。
- 不支持修改标签，可以解绑标签后，绑定新的标签。

绑定标签

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > 云堡垒机（原生版）”,进入云堡垒机实例管理页面。
4. 选择需要添加标签的堡垒机实例，单击“更多 > 编辑标签”。

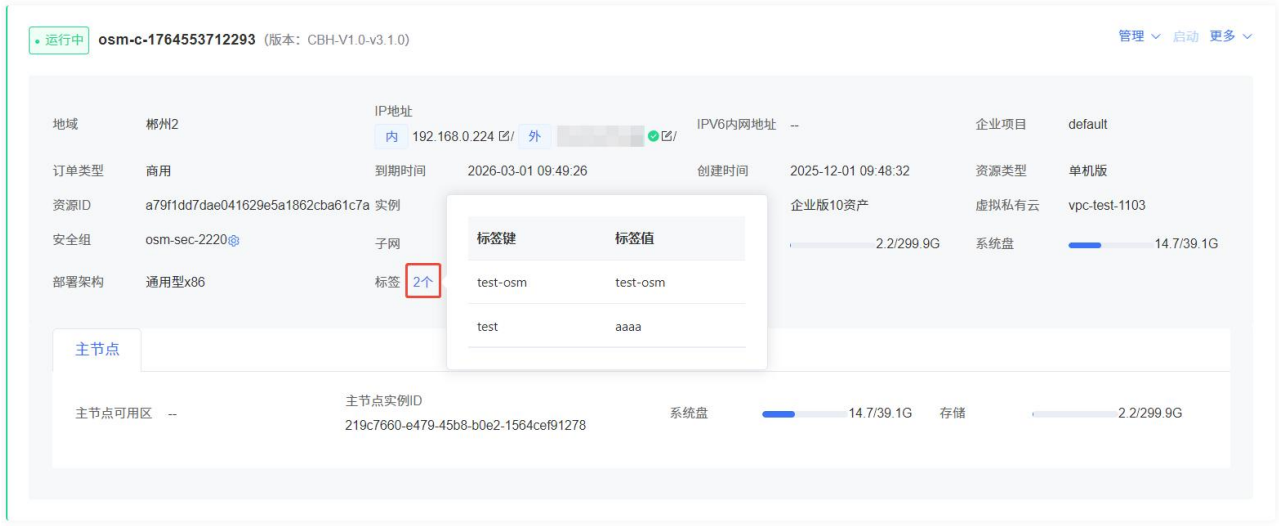


5. 在弹出的编辑标签窗口中，填写标签键和值。

   方式一：在输入框中输入新的标签键和值，新增标签。

   方式二：下拉选择已有标签。

6. 配置完成后，单击“确定”，绑定标签完成。
7. 标签绑定成功后，鼠标点击实例信息的“标签”数量，可查询标签绑定情况。



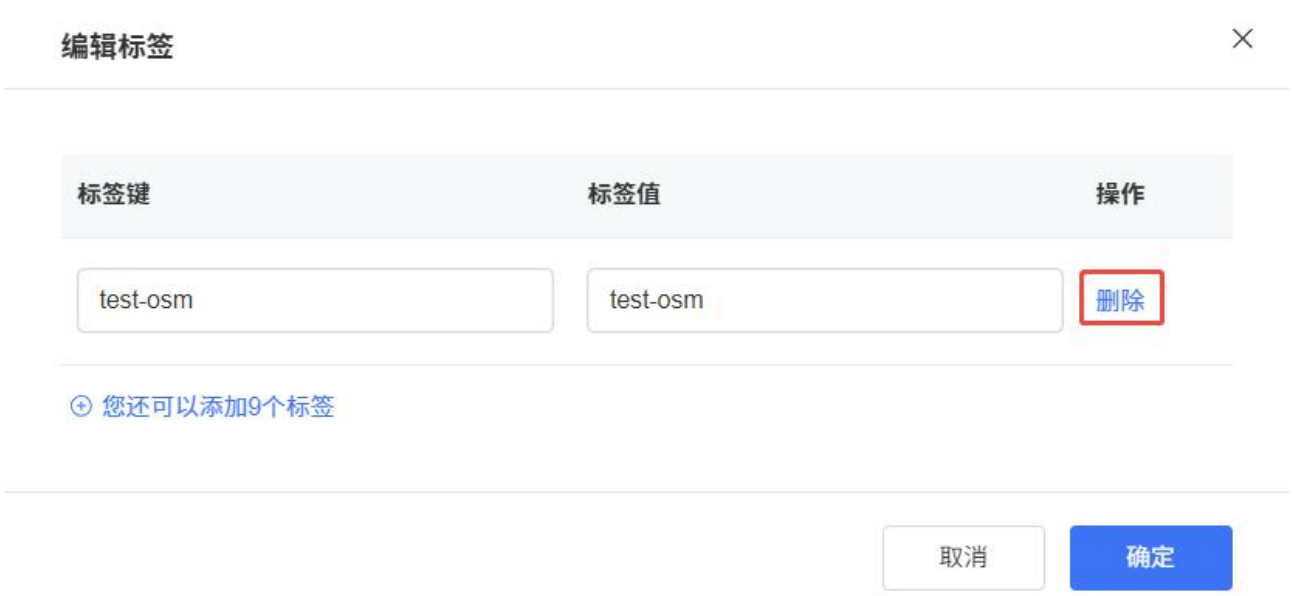
使用标签筛选实例

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > 云堡垒机（原生版）”，进入云堡垒机实例管理页面。
4. 单击“筛选标签”。

5. 在“标签筛选”弹窗中，下拉选择已有标签。
6. 单击确定，执行筛选标签操作，列表将展示标签筛选结果。筛选结果返回包含所选择的多项键值的实例。

解绑标签

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > 云堡垒机（原生版）”，进入云堡垒机实例管理页面。
4. 选择需要添加标签的堡垒机实例，单击“更多 > 编辑标签”。
5. 在弹出的编辑标签窗口中，单击目标标签操作列的“删除”。



6. 单击“确定”，解绑标签完成。

4.8 IAM 权限管理

云堡垒机（原生版）通过 IAM（统一身份认证服务，Identity and Access Management）对用户权限进行管理，IAM 可以帮助用户安全地控制云堡垒机（原生版）服务的访问及操作权限。

默认情况下，天翼云主账号拥有管理员权限，而主账号创建的 IAM 用户没有任何权限。IAM 用户需要加入用户组，并给用户组授权相应策略后，IAM 用户才能获得策略对应的权限，才可以基于被授予的权限对云服务进行操作。

IAM 应用场景

IAM 策略主要面向同一主账号下，对不同 IAM 用户授权的场景：

- 您可以为不同操作人员或应用程序创建不同 IAM 用户，并授予 IAM 用户刚好能完成工作所需的权限，比如查看权限，进行最小粒度授权管理。
- 新创建的 IAM 用户可以使用自己的登录名和密码登录控制台，实现多用户协同操作时无需分享账号密码的安全要求。

云堡垒机（原生版）IAM 策略说明

天翼云为云堡垒机（原生版）提供如下**系统策略**。如果系统策略不满足授权要求，可以创建**自定义策略**，自定义策略是对系统策略的扩展和补充，详情请参见创建自定义策略。

策略名称	策略描述	类别	授权范围
ctcbh admin	云堡垒机（原生版）管理员策略，拥有产品所有操作权限。	系统策略	全局级
ctcbh viewer	云堡垒机（原生版）查看策略，只具备查看权限。	系统策略	全局级

云堡垒机（原生版）权限及授权项

策略支持的操作与授权项相对应，授权项列表说明如下：

- 权限：允许或拒绝 IAM 用户某项操作。
- 授权项：授权操作对应的权限三元组，创建自定义策略时，支持可视化 JSON 视图写入权限三元组实现策略配置。
- 权限类型：授权操作对应的读写类型。

权限	授权项	权限类型（读/写）	ctcbh admin	ctcbh viewer
实例列表查询	osm:instance:list	读	✓	✓
云堡垒机管理员身份登录	osm:instance:loginAsAdmin	写	✓	×
实例开机	osm:instance:poweron	写	✓	×
实例关机	osm:instance:poweroff	写	✓	×
实例重启	osm:instance:restart	写	✓	×
实例升级	osm:instance:upgrade	写	✓	×
实例绑定弹性 IP	osm:instance:bindEip	写	✓	×
云堡垒机实例开通	osm:instance:create	写	✓	×

通过 IAM 授权使用云堡垒机（原生版）

详细操作请参考：

1. 创建用户组和授权
2. 创建 IAM 用户和登录

4.9 使用云监控服务监控云堡垒机实例

4.9.1 查看监控数据

为保证云堡垒机实例的可靠性、可用性和可观测性，对云堡垒机进行监控已经成为一种必要且重要的手段。天翼云控制平台提供的云堡垒机监控功能，可方便用户更快、更直观的了解云堡垒机的运行情况、使用情况及其他性能指标，同时可根据实时监控情况，执行告警通知等操作，帮助客户更好的管理云堡垒机实例。
当用户开通云堡垒机（原生版）服务后，即可通过云监控来查看监控指标。

> 说明
>
> **目前仅支持监控“一类节点”区域的实例。**云堡垒机（原生版）支持的区域请参见支持的区域。

实例支持的监控指标

监控指标	指标说明	单位	是否支持告警	监控周期
CPU 利用率	该指标用于统计云堡垒机实例的 CPU 利用率。	%	是	5 分钟
内存总大小	该指标用于统计云堡垒机实例的实际内存大小。	GB	是	5 分钟
剩余内存大小	该指标用于统计云堡垒机实例的空闲的内存大小。	GB	是	5 分钟
内存利用率	该指标用于统计云堡垒机实例的内存利用率。 内存利用率 = 100% -（剩余内存大小/内存总大小）	%	是	5 分钟
系统盘大小	该指标用于统计云堡垒机实例的实际系统盘大小。	GB	是	5 分钟
剩余系统盘大小	该指标用于统计云堡垒机实例的空闲的系统盘大小。	GB	是	5 分钟
系统盘利用率	该指标用于统计云堡垒机实例的系统盘利用率。 系统盘利用率 = 100% -（剩余系统盘大小/系统盘大小）	%	是	5 分钟
数据盘大小	该指标用于统计云堡垒机实例的实际数据盘大小。	GB	是	5 分钟
剩余数据盘大小	该指标用于统计云堡垒机实例的空闲的数据盘大小。	GB	是	5 分钟
数据盘利用率	该指标用于统计云堡垒机实例的数据盘利用率。 系统盘利用率 = 100% -（剩余数据盘大小/数据盘大小）	%	是	5 分钟
异常登陆事件累计数	该指标用于统计云堡垒机实例异常登录事件的数量。	个	是	5 分钟

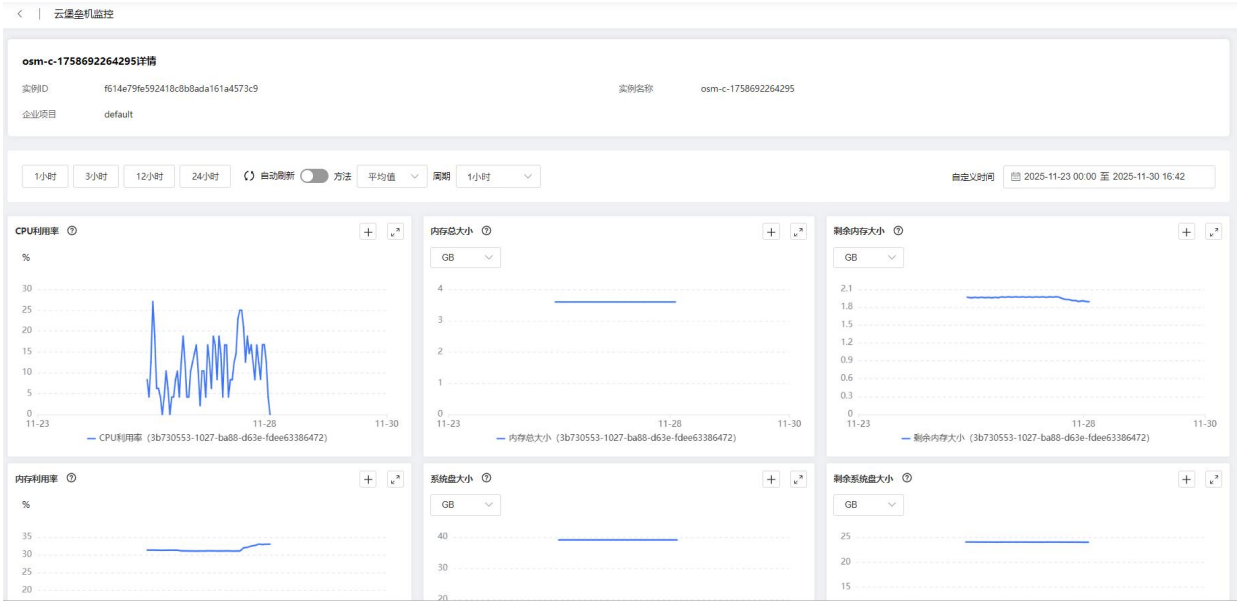
查看监控图表

1. 登录天翼云控制中心。
2. 在产品服务列表中“管理与部署 > 云监控服务”，进入云监控服务主页面。
3. 在左侧导航栏，选择“云服务监控”，单击“云堡垒机”产品。

4. 在云堡垒机监控列表中选择目标的实例，单击操作列的“查看监控图表”，进入监控详情页。

5. 在监控详情页，可以查看实例详情和监控图表。

   切换不同的时间周期，查看不同周期内监控指标的情况。



4.9.2 创建告警监控规则

云监控支持灵活的创建告警规则。您既可以根据实际需要对某个监控指标设置自定义告警规则，同时也能够使用告警模板为多个资源或者云服务批量创建告警规则。

> **说明**
>
> **目前仅支持监控“一类节点”区域的实例。**云堡垒机（原生版）支持的区域请参见支持的区域。

操作步骤

1. 登录天翼云控制中心。
2. 在产品服务列表中“管理与部署 > 云监控服务”，进入云监控服务主页面。
3. 在左侧导航栏，选择“云服务监控”，单击“云堡垒机”产品。

4. 在云堡垒机监控列表中选择目标的实例，单击操作列的“创建告警规则”。

5. 在“创建告警规则”页面，根据界面提示配置参数。

配置参数及相关含义说明如下：

模块	参数	参数说明	配置示例
选择监控对象	规则类型	选择规则的类型，主要包括指标监控、事件监控、站点监控、自定义监控、自定义事件五种。	指标监控
	服务	配置告警规则监控的云服务资源类型。	云堡垒机（原生版）
	维度	用于指定告警规则对应指标的维度名称。	云堡垒机实例
	监控对象类型	具体实例/资源分组/全部资源	具体实例
	监控对象	用来配置该告警规则针对的具体资源，可以是一个或多个。	实例名称
定义告警策略	选择类型	支持**自定义创建**、**从模板导入**。	自定义创建

模块	参数	参数说明	配置示例
	策略	支持选择**满足全部**或**任意**策略。 策略信息包括： • 监控指标，支持的监控指标请参见实例支持的监控指标。 • 数据类型（原始值） • 判断条件（>、≥、<、≤、=、环比上升、环比下降、环比变化） • 值 • 单位 • 发生次数 • 级别（普通、警示、紧急） 说明 同一告警规则，告警条件最多支持添加 20 条。	满足全部以下条件：若 CPU 利用率的原始值>=80%，连续发生 1 次，普通
	无数据处理	不做处理/视为告警/视为恢复。	不做处理
配置告警通知	发送通知	配置是否发送邮件通知用户，可以选择开启（推荐选择）或者关闭。	开启
	通知方式	仅支持“通知联系人组”。	通知联系人组
	告警联系组	选择发生告警通知时通知的用户组。支持选择联系组或者云账户默认联系人。	-
	触发场景	触发告警邮件的场景，可在出现告警和告警恢复时发送提醒信息。	出现告警
	通知渠道	配置告警通知的通知渠道，支持邮箱、短信、语音（语音需要单独订购）。	邮箱
	重复告警	指告警发生后如果未恢复正常，将重复发送告警通知次数。	不重复
	通知频率	指告警发生后如果未恢复正常，间隔多久重复发送一次告警通知。若**重复告警**选择“不重复”时，无需配置该参数。	每 24 小时通知一次
	通知周期	配置告警通知的周期时间。	星期天、星期一、星期二、星期三、星期四、星期五、星期六
	通知时段	配置告警通知的时间段。	00:00:00-23:59:59
	告警回调	配置告警通知 webhook 地址。	-
	通知模板	告警信息默认使用系统模板；也可以选择用户自定义创建的通知模板，自定义模板详细操作请参见创建自定义告警模板。	系统模板
规则信息	名称	该告警规则的自定义名称。	evs-alarm-note
	企业项目	选择告警规则适用的企业项目。	default

模块	参数	参数说明	配置示例
	描述	添加对该告警规则描述。	-

6. 配置完成后，单击“确定”完成操作。

告警规则添加完成后，当监控指标触发设定的阈值时，云监控会在第一时间通过邮件实时告知您云上资源异常，以免因此造成业务损失。关于云监控的其他操作和更多信息，请参考《云监控服务》。

5 运维用户指南

5.1 登录堡垒机

开通堡垒机（原生版）后，用户在控制台 “云堡垒机实例”页面，在操作列点击“管理”操作，系统单点登录进入云堡垒机实例，通过控制台登录进入默认管理员用户。

登录的时候可选“外网地址登录”或“内网地址登录”。

说明

- 内网地址登录需要确保网络环境互通。
- 外网地址登录需要绑定弹性 IP。

首次登录

在未设置初始密码时，需通过云堡垒机控制台单点登入跳转登入堡垒机，并进行初始化管理操作。

操作步骤

1.在“云堡垒机实例”列表条目录中选择要管理的实例，单击“管理”。

2.根据您自身的网络环境选择“内网地址登录”或“外网地址登录”。

3.登入堡垒机后，通过个人信息进行初始密码设置。

非首次登录

非首次登入云堡垒机可通过云堡垒机控制台单点登入跳转登入堡垒机，或通过云堡垒机登录地址使用静态

认证或令牌认证等方式登录。以下介绍使用静态认证和令牌认证两种方式登录云堡垒机实例。

前置条件

已登录过云堡垒机并完成密码初始化。

静态认证登录操作步骤

1.启动浏览器，在浏览器 Web 地址栏中输入系统登录地址，进入到系统登录页面。

2.选择认证方式为静态认证。

3.输入系统用户账号和密码，输入图形验证码。

4.单击“登录”，成功登录到堡垒机系统。

注意：

云堡垒机实例登录地址为 https://EIP:18443，EIP 为您绑定在堡垒机实例的弹性 IP 地址。若未绑定 EIP，则地址为 https://私网 IP:18443。您也可以从云堡垒机账号注册通知邮件中获取您购买的堡垒机实例登录链接。

短信认证登录操作步骤

说明：

使用短信认证登录，请确保该云堡垒机已开启短信认证方式，具体开启操作请参考：认证设置章节。

1.启动浏览器，在浏览器 Web 地址栏中输入系统登录地址，进入到系统登录页面。

2.选择认证方式为短信认证。

3.输入系统用户账号和密码，输入图形验证码。

4.单击“登录”，成功登录到堡垒机系统。

令牌认证登录操作步骤

说明：

使用手机令牌登录前，请先确保您已经为该账号绑定手机令牌，绑定手机令牌才做请参见：手机令牌章节。

1.启动浏览器，在浏览器 Web 地址栏中输入系统登录地址，进入到系统登录页面。

2.选择认证方式为令牌认证。

3.输入系统用户账号和密码，输入手机动态口令。

4.单击“登录”，成功登录到堡垒机系统。

注意：

- 动态口令的获取需要使用天翼云 app 虚拟 MFA 管理功能，若未安装天翼云 app，请进入手机应用商店搜索”天翼云“，下载安装天翼云手机 APP；
- 使用天翼云手机 app 首页扫描二维码功能扫描云堡垒机注册邮箱中系统发送的手机令牌二维码图片，绑定手机令牌。

5.2 运维环境设置

在使用堡垒机之前，您需要先设置运维工具及配置运维工具路径。

使用本地客户端方式运维资产，需要初始化本地终端环境设置，下载并设置访问插件。

下载访问插件

1.使用访问用户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“运维设置”，进入“运维设置”页面。

3.单击页面右上角的“访问插件”按钮，根据实际操作环境选择插件下载。

配置运维工具

说明：

- 目前版本 Xshell、SecureCRT、Filezilla、WinSCP、DBeaver 和 Navicat 需要使用客户端路径配置工具配置路径后才可以使用。
- 使用版本限制请参考：使用限制章节。

1.在“运维设置”页面勾选需要使用的客户端工具，并单击“保存”。

2.若您配置的工具需要配置客户端路径，则单击页面右上角的“客户端路径配置”。

3.在弹出的对话框中选择需要配置客户端，选择客户端路径。

5.3 资产运维

在您配置好运维设置后，并且已经成功新增资产和授予访问权限后。可在“资产访问”模块，运维已授权访问的资产。

访问字符资产

1.使用访问用户登录云堡垒机（原生版）。

2.在左侧导航栏选择“资产访问”，在“资产访问”页面选择“字符”页签。

3.选择需要访问资产，在右侧选择相关内容后，单击需要使用的访问协议即可登录。

说明：

资产账号可在管理员添加资产时同步添加。

访问图形资产

1.使用访问用户登录云堡垒机（原生版）。

2.在左侧导航栏选择“资产访问”，在“资产访问”页面选择“图形”页签。

3.选择需要访问资产，在右侧选择相关内容后，单击需要使用的访问协议即可登录。

使用文件传输

1.使用访问用户登录云堡垒机（原生版）。

2.在左侧导航栏选择“资产访问”，在“资产访问”页面选择“文字传输”页签。

3.选择需要访问资产，在右侧选择相关内容后，单击需要使用的访问协议即可登录。

访问数据库资产

1.使用访问用户登录云堡垒机（原生版）。

2.在左侧导航栏选择“资产访问”，在“资产访问”页面选择“数据库”页签。

3.选择需要访问资产，在右侧选择相关内容后，单击需要使用的访问协议即可登录。

说明

支持纳管的数据库请参考：使用限制章节。

访问应用资产

1.使用访问用户登录云堡垒机（原生版）。

2.在左侧导航栏选择“资产访问”，在“资产访问”页面选择“应用”页签。

3.选择需要访问资产，在右侧选择相关内容后，单击需要使用的访问协议即可登录。

5.4 工单管理

5.4.1 工单申请

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。

约束限制

已被纳入审批规则的用户名单内。

创建工单

1. 登录云堡垒机。
2. 在左侧导航栏选择“工单管理”>“工单申请”，进入工单申请页面。
3. 单击左上角的“新增”按钮，弹出“工单申请”对话框。
4. 在弹出的对话框中输入相关信息，具体填写参数可以参考下表，填写完成后单击“提交”。

参数		说明
基本信息	工单名称	输入您待提交工单的名称。

参数		说明
	工单类型	选择需要授权的工单类型，根据业务需求选择如下四种类型： • 资产访问授权 • 字符命令授权 • 文件传输授权 • 数据库命令授权
资产	资产	选择您需要访问的资产或者命令，可多选。
	资产组	选择您需要访问的资产组，可多选。
账号	资产账号	选择您需要授权的资产账号。 注意 若选择授权的资产账号为二次登录账号（例如 root），需同时授权二次登录的源账号（例如添加 root 资产账号时配置的二次登录源账号 testuser），否则将无法完成二次登录。
协议	服务	（仅工单类型选择“资产访问授权”时需要配置）默认全部服务，也支持选择单个服务。
敏感命令	提示符正则	（仅工单类型选择“字符命令授权”时需要配置）输入待授权命令的提示符正则式。
	命令正则式	（仅工单类型选择“字符命令授权”时需要配置）输入待授权命令的正则式。
	文件传输	（仅工单类型选择“文件传输授权”时需要配置）选择需要授权的文件传输操作，包括上传、下载、删除等。
	文件或目录	（仅工单类型选择“文件传输授权”时需要配置）配置策略生效的文件或目录的正则表达式，可配置多个，多个以回车进行分隔。
	sql 命令类型	（仅工单类型选择“数据库命令授权”时需要配置）选择需要授权的 SQL 命令类型。
授权时间	生/失效日期	配置权限生效的起始和截止日期。 支持选择 1 天、3 天、7 天、15 天、长期有效，或者自定义选择日期。
	生/失效时间	配置权限生效的具体时间点。 支持选择全天、闲时（0 点-6 点），或者自定义时间。
其他	描述	填写申请工单的相关描述。

5.4.2 工单审批

前提条件

相关账号拥有工单审批的权限，若需要配置相关权限请参考规则配置章节。

工单审批

1. 登录云堡垒机系统。
2. 在左侧导航栏单击“工单管理”>“工单审批”，进入工单审批页面。
3. 查找需要待审批的工单，单击“操作”列的“审批”按钮。
4. 在弹出的“工单审批”对话框中，查看待审批的工单内容，选择是否批准。

6 管理员用户指南

通过本章，我们可以了解管理员的基本功能，以及给用户创建账号并授权的基本流程。管理员的基础功能包括“管理账号”、“管理资产”、“管理授权”以及“查看审计”。

6.1 用户管理

6.1.1 用户

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。

约束限制

仅有“管理角色”权限的用户可以新建、编辑和删除用户。

新增用户组

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

1. 使用“管理角色”账号登录云堡垒机。
2. 在左侧导航栏选择“用户管理 > 用户”，进入“用户”模块。

3. 在用户列表左侧用户树中，单击用户组右侧的更多图标，选择“新增子节点”或“复制”。支持创建多级用户组，最多支持创建 10 级。

4. 在弹出的“新增用户组”或“用户组复制”对话框中，填写用户信息。

参数	参数说明
用户组名	自定义用户组名。同级间用户组名称不能重名。
用户	选择用户。
描述	自定义用户组的描述。

5. 填写完成后，单击“提交”完成用户组的创建。

创建完成后，您也可以根据需要对用户组进行修改或删除：

- **编辑用户组**：选择需要修改的用户组，单击用户组右侧的更多图标，选择“编辑”，按照需求对用户组进行修改，单击“确定”完成操作。
- **删除用户组**：选择需要删除的用户组，单击用户组右侧的更多图标，选择“删除”，在弹出的对话框中单击“确定”完成删除操作。

新增单个用户操作步骤

1.使用“管理角色”账号登录云堡垒机。

2.在左侧导航栏选择“用户管理 > 用户”，进入“用户”模块。

3.单击“新增”，在弹出的“新增用户”对话框中，填写用户信息。

参数	参数说明
登录名	填写该账户的用户名称（登录账号）。 只能为数字、大小写字母、“.”和“_”组成，首位只能数字或者字母，且不超过 25 个字符；
姓名	填写该账户的使用者的姓名（非登录账号）。
手机号	填写手机号，请确保手机号真实有效，否则会影响短信的接收。

参数	参数说明
邮箱	（选填）填写邮箱地址，请确保邮箱地址真实有效，否则会影响告警信息的接收。
用户密码	输入该账户的密码。密码请根据管理员设置的密码规则填写，具体可参见：安全设置章节。
确认密码	二次确认账户密码。
角色	选择该账户所属的角色，可选以下角色： ● 管理角色 ● 审计角色 ● 访问角色 ● 工单管理角色（提供工单管理模块的权限） 注意： 管理角色和工单管理角色只支持二选一配置。
用户组	选择该账户所属的用户组，用户组操作请参见：用户组章节。
认证方式	选择认证方式，可选“静态认证”和“令牌认证”。
生效时间	选择该账户可登录的时间段。
准入 IP	选择可登录的 IP 地址。

4.填写完成后，单击“确定”完成用户新增。

后续操作：

修改用户数据：选择需要修改的用户数据，单击“操作”列中“编辑”，按照需求进行用户数据的修改，单击“提交”完成用户数据更新。

修改用户密码：管理员可以修改修改对应账户的密码，选择需要修改的用户密码，单击“操作”列的“更多 > 改密”，在弹出的对话框中根据密码规则修改密码。

说明

您可以根据自身需求自定义密码规则，具体修改密码规则请参考安全设置章节。

批量导入用户

云堡垒机（原生版）支持批量导入用户信息。

1.使用“管理角色”账号登录云堡垒机。

2.在左侧导航栏选择“用户管理 > 用户”，进入“用户”模块。

3.单击“导入”按钮，弹出“账号导入”对话框。

4.单击“下载导入文件模板”，在线下文件模板中填写内容。

参数	参数说明
用户名	（必填）填写该账户的使用者的姓名（非登录账号）。
用户	（必填）填写该账户的用户名称（登录账号）。 只能为数字、大小写字母、“.”和“_”组成，首位只能数字或者字母，且不超过 25 个字符；
手机号	（必填）填写手机号，请确保手机号真实有效，否则会影响短信的接收。

参数	参数说明
邮箱	填写邮箱地址，请确保邮箱地址真实有效，否则会影响告警信息的接收。
密码	（必填）输入该账户的密码，密码请根据管理员设置的密码规则填写，具体可参见：安全设置章节。
角色	（必填）选择该账户所属的角色，可填写“管理角色”、“审计角色”和“访问角色”，需要选择多个角色请使用英文“,”分隔。
用户组	填写该账户所属的用户组，用户组操作请参见：用户组章节。若填写多个用户组请使用英文“,”分隔。
认证方式	（必填）选择认证方式，可选“静态认证”，“令牌认证”和“短信认证”，多个认证方式请使用英文“,”分隔。
授权生效日期	填写该用户生效的日期，日期格式支持：YYYY-MM-DD 或 YYYY/MM/DD。
授权失效日期	填写该用户失效的日期，日期格式支持：YYYY-MM-DD 或 YYYY/MM/DD。
授权生效日期	填写生效日期的具体时间点，填写范围：0-23，例如需要早上 10 点生效，就填写：10。
授权失效日期	填写失效日期的具体时间点，填写范围：0-23，例如需要晚上 10 点失效，就填写：22。
准入 IP	选择可登录的 IP 地址。

说明：

若不填写生失效日期，则新建的账号默认永久生效。

5.填写完成后，上传模板文件后选择重复用户导入策略。

6.单击“提交”即可生成新的用户。

导出用户

云堡垒机（原生版）支持批量导出已在控制台保管的账户信息，同时也支持导出 admin 账户信息。

说明：

若您需要导出 admin 账户信息，则默认不勾选用户，直接单击“导出”即可获取。

1.使用“管理角色”账号登录云堡垒机。

2.在左侧导航栏选择“用户管理 > 用户”，进入“用户”模块。

3.勾选需要导出的用户信息，单击“导出”即可生成用户信息表格导出。

锁定/解锁用户

云堡垒机支持对用户进行加锁操作，在锁定期间该用户无法登录云堡垒机。

1.使用“管理角色”账号登录云堡垒机。

2.在左侧导航栏选择“用户管理 > 用户”，进入“用户”模块。

3.勾选需要加锁/解锁的用户信息，单击“加锁”/“解锁”即可锁定或解锁用户。

用户删除

云堡垒机系统用户支持一键删除和批量删除，用户被删除后，用户账号所有关联的权限将失效。

注意：

用户删除后信息无法恢复，请谨慎操作！

1.使用“管理角色”账号登录云堡垒机。

2.在左侧导航栏选择“用户管理 > 用户”，进入“用户”模块。

3.勾选需要删除的用户信息，单击“删除”。

4.在弹出的对话框中单击“确定”即可删除用户。

6.1.2 手机令牌

若您的给用户开通了令牌验证权限，那么该用户可以绑定天翼云令牌验证，使用令牌登录，提高账户的安全性。

前提条件

已给用户开通“令牌认证”权限。

手机令牌绑定

1.进入云堡垒机（原生版）实例登录页。

2.选择“令牌验证”。

3.单击登录下方的“绑定令牌”按钮，输入需要绑定令牌的用户名及密码，开始绑定令牌。

4.下载天翼云 APP，若已下载则单击“下一步”。

5.在天翼云 APP 下方选择“我的 > 虚拟 MFA”进入“虚拟 MFA”界面，单击右上角的按钮，选择“扫码添加”，扫描页面上的二维码并输入 MFA 码。

6.完成绑定后，即可使用令牌登录。

6.2 资产管理

6.2.1 主机资产

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、Mac 等主机资源，MySQL、PostgreSQL、Oracle 等数据库资源以及 Windows 应用程序资源。

前提条件

仅“管理角色”支持资产相关的操作。

新增资产组

您可以通过主机资产组来管理多个资产，方便您在授权的时候可以一键选择。

1. 使用“管理角色”账户登录云堡垒机（原生版）控制台。
2. 在左侧导航栏选择“资产管理 > 主机资产”，进入主机资产页面。
3. 在主机资产列表左侧资产树中，单击资产组右侧的更多图标，选择“新增子节点”或“复制”。

   支持创建多级资产组，最多支持创建 10 级。
4. 在弹出的“新增资产组”或“资产组复制”对话框中，填写资产组信息。

参数	参数名称
资产组名称	自定义资产组的名称。
资产	在下拉框中选择需要添加至该资产组中的资产。
描述	自定义资产组的描述。

5. 填写完成后，单击“提交”完成资产组的创建。

   创建完成后，您也可以根据需要对资产组进行修改或删除：

   - **编辑资产组**：选择需要修改的资产组，单击资产组右侧的更多图标，选择“编辑”，按照需求对资产组进行修改，单击“确定”完成修改操作。
   - **删除资产组**：选择需要删除的资产组，单击资产组右侧的更多图标，选择“删除”，在弹出的对话框中单击“确定”完成删除操作。

新增单个资产

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“资产管理 > 资产”，进入“资产”页面。

3.单击“新增”按钮，弹出“新增资产”对话框，并填写相关内容。

参数	参数说明	取值样例
资产名称	自定义新增的资产名称。	Test
资产类型	选择新增的资产类型，可选 Windows 服务器、Unix/Linux 服务器或数据库。 具体支持的资产类型可参考：使用限制章节。	Windows 服务器
IP 地址	填写待纳管资产的 IP 地址，支持 IPv4 和 IPv6。	0.0.0.0
资产组	选择新增资产所在的资产组，资产组相关操作请参照：资产组章节。	-
资产描述	填写资产的描述。	-
协议	选择资产的协议类型： ● 当**资产类型**选择 **Windows 服务器**或 **Unix/Linux 服务器**时支持选择：SSH、TELNET、SFTP、FTP、X11、RDP、VNC。 ● 当**资产类型**选择**数据库**时支持选择：Oracle、DB2、MySQL、PostgreSQL、达梦、DRDS、SQL Server。 协议选择完成后，需填写“端口”，若您选择的是**数据库**资产，还需再填写“服务器名称”。	SSH、80
账号	（可选）添加可访问资产的账号： ● 账号名：填写可正常访问资产的账号名。 ● 密码：输入账户名对应的密码。 ● 私钥：若选择该项，需要上传有效的 RSA 证书。 ● 使用协议：选择账户对应的协议。 ● 状态：选择账号状态。 您也可以在资产账号模块添加。	-
访问信息	选择资产系统编码，可选“UTF-8”或“GBK”。	GBK

4.填写完成后，单击“提交”完成资产新增。

自动导入天翼云上 ECS 资产

说明

目前仅“一类节点”区域的实例支持自动导入天翼云上 ECS 资产。云堡垒机（原生版）支持的区域请参见支持的区域。

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“资产管理 > 资产”，进入“资产”页面。

3.选择“导入 > 天翼云 ECS 实例导入”，勾选需要导入的 ECS 资产。

4.根据需求选择导入策略。

说明：

- 跳过：若存在同名资产，则跳过该资产的导入。
- 覆盖：若存在同名资产，使用新资产覆盖旧资产。
- 建立副本：若存在同名资产，则为新资产增加后缀后导入（后缀新增为_1;_2.....以此类推）。

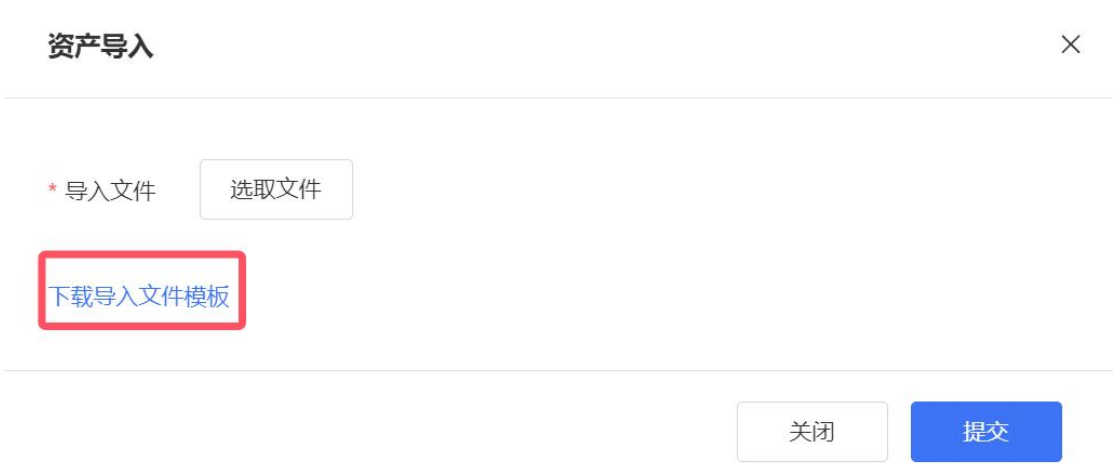
5.单击“导入”，完成天翼云 ECS 资产导入。

批量导入资产

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“资产管理 > 资产”，进入“资产”页面。

3.单击“导入”按钮，在弹出的对话框中下载导入模板。



4.在导入模板文件中填写内容，填写完成后保存。

说明：

- 模板中红色标题为必填项；
- 多个资产组用英文逗号“,”隔开；
- 资产类型为 Windows 服务器或 Unix/Linux 服务器时只会判断录入黑色标题的端口协议；
- 资产类型为数据库时只会判断录入蓝色标题的端口协议且协议有填写时对应的服务名必填。

参数	参数说明	取值样例
资产名称	自定义新增的资产名称。	Test
资产类型	填写新增的资产类型：可填 **Windows 服务器**、**Unix/Linux 服务器**或**数据库**。	Windows 服务器
IP 地址	填写纳管资产的 IP 地址。	0.0.0.0
资产组	填写新增资产所属的资产组。	-
资产描述	填写资产的描述。	-
协议	填写协议的端口： ● 资产类型为 **Windows 服务器**或 **Unix/Linux 服务器**时只会判断录入**黑色标题**的端口协议； ● 资产类型为**数据库**时只会判断录入**蓝色标题**的端口协议且协议有填写时对应的服务名必填。	-

参数	参数说明	取值样例
访问信息	填写资产的访问编码，仅支持填写“UTF-8”或“GBK”。	GBK

5.上传已经填写完成后的导入模板，单击“提交”完成资产导入。

资产发现

云堡垒机支持设置端口和网段扫描并发现资产。

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“资产管理 > 资产”，进入“资产”页面。

3.单击“资产发现”按钮，在弹出的对话框中填写需要扫描的目标网段和端口。

4.填写完成后，单击“立即扫描”开始扫描资产。

5.扫描完成后，根据您自身业务需求勾选需要导入至堡垒机的资产，分别填写“资产名称”、“资产类型”和“协议”。

6.选择“重复资产导入策略”，单击“添加至堡垒机资产列表”即可完成资产导入。

后续操作

- 导出资产：在“资产”页面勾选需要导出的资产，单击“导出”即可导出。

- 删除资产：在“资产”页面选择需要删除的资产，单击“操作”列的“删除”按钮，在弹出的对话框中单击“确定”即可删除。

注意：

删除后的资产无法恢复，请谨慎删除！

6.2.2 应用资产

6.2.2.1 新增应用服务器

在一台支持远程桌面的 Windows 系统服务器上部署浏览器应用（Web 应用），通过云堡垒机的应用发布功能，将浏览器应用纳入云堡垒机进行管理。

用户获取应用资产访问权限后，通过应用发布服务器访问 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。

约束限制

- 仅企业版支持使用应用运维功能。
- 添加的主机和应用资源数量总和不能超过资产数。
- Windows 应用服务器仅支持 2016 版本。
- 添加应用发布前，需已添加应用服务器。

添加应用服务器

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“资产管理 > 应用资产”，并且在左上方选择“应用服务器”，进入“应用服务器”页面。

3.单击“新增”按钮，弹出“新增应用服务器”对话框，并填写相关内容。

参数	填写说明

参数	填写说明
服务器名称	自定义服务器名称，在同一堡垒机内应用服务器名称不得重复。
服务器类型	选择服务器类型，当前版本仅支持 Windows。
服务器 IP 地址	填写访问应用的服务器真实 IP 地址或域名。
端口	填写访问应用发布服务器的端口，Windows 服务器默认为 5901。
服务器描述	填写应用服务器的简要描述。
服务器账户	填写访问应用的服务器账户。
密码	填写访问应用的服务器账户的密码。
app 类型和路径	填写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”。 注意：路径中请勿输入 Administrator，否则程序可能无法启动。

4.填写完成后，单击“提交”即可完成新增应用服务器。

导入应用服务器

云堡垒机提供线下模板，方便您批量导入应用服务器。

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“资产管理 > 应用资产”，并且在左上方选择“应用服务器”，进入“应用服务器”页面。

3.单击“导入”按钮，弹出“应用服务器导入”对话框，单击“下载导入文件模板”。

4.根据模板提供的配置项说明，填写要导入的应用服务器配置信息。

5.上传已经填写完成后的导入模板，根据需求选择导入策略。

说明：

- 跳过：若存在同名服务器，则跳过该服务器的导入。
- 覆盖：若存在同名服务器，使用新服务器覆盖旧服务器。
- 建立副本：若存在同名服务器，则为新服务器增加后缀后导入（后缀新增为_1;_2.....以此类推）。

6.单击“提交”完成应用服务器导入。

6.2.2.2 应用发布服务器配置

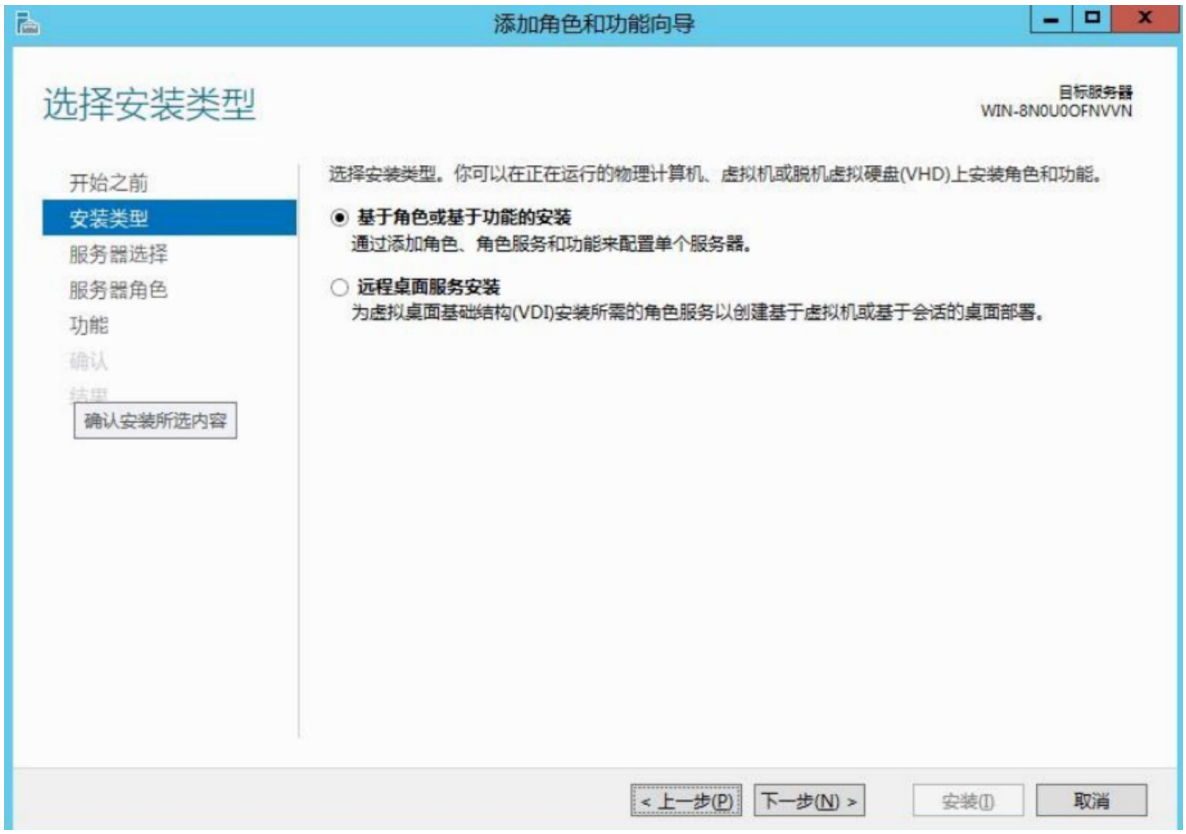
应用发布服务器的主要作用是将应用程序部署到生产环境，使其能够对外提供服务，同时通过版本管理、自动化测试等功能保障应用稳定运行。

安装服务器

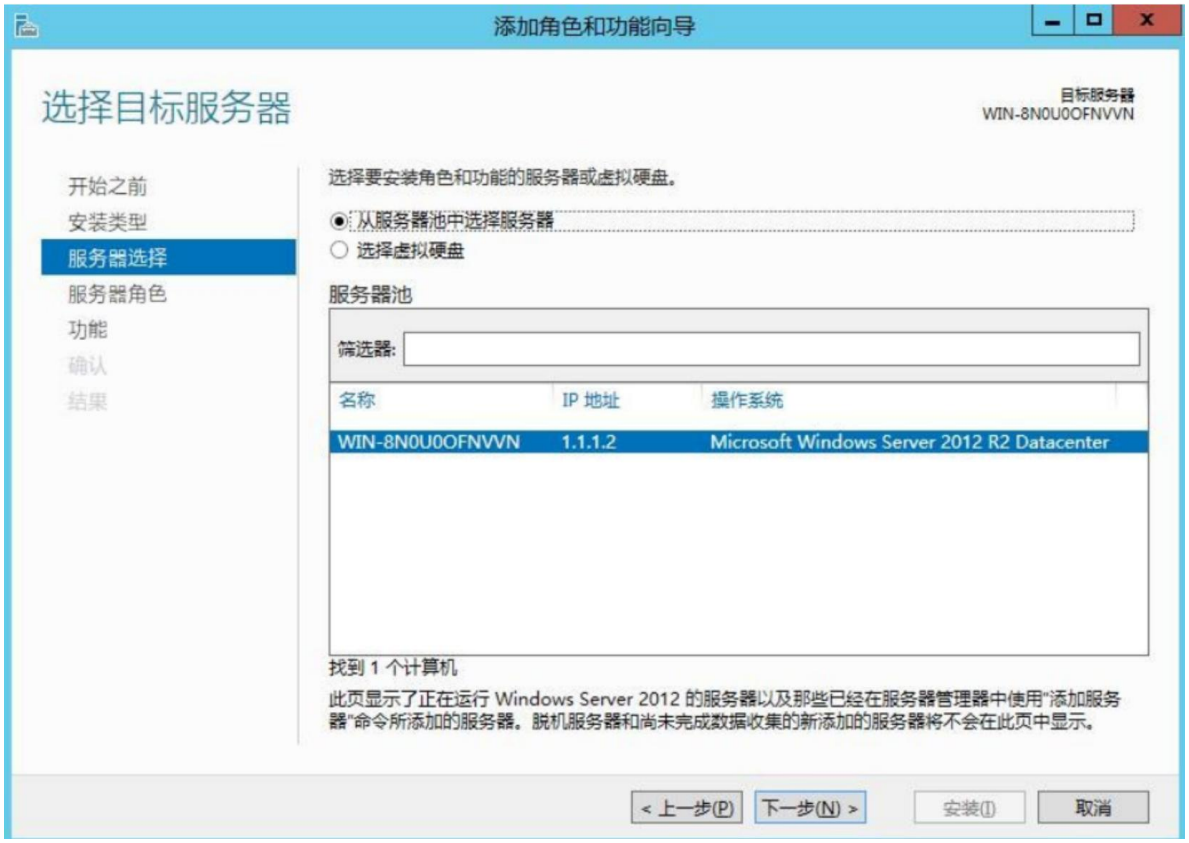
本文以 Windows 2016 版本为例。

1. 使用管理员账号登录服务器。
2. 打开“服务器管理器”，选择“仪表板”，进入仪表板界面。
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。

4. 选择“基于角色或基于功能的安装”。



5. 在服务器池中选择目标服务器。



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。

7. （可选）选择服务器所需要的其它功能，默认下一步跳过。

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。

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。

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。

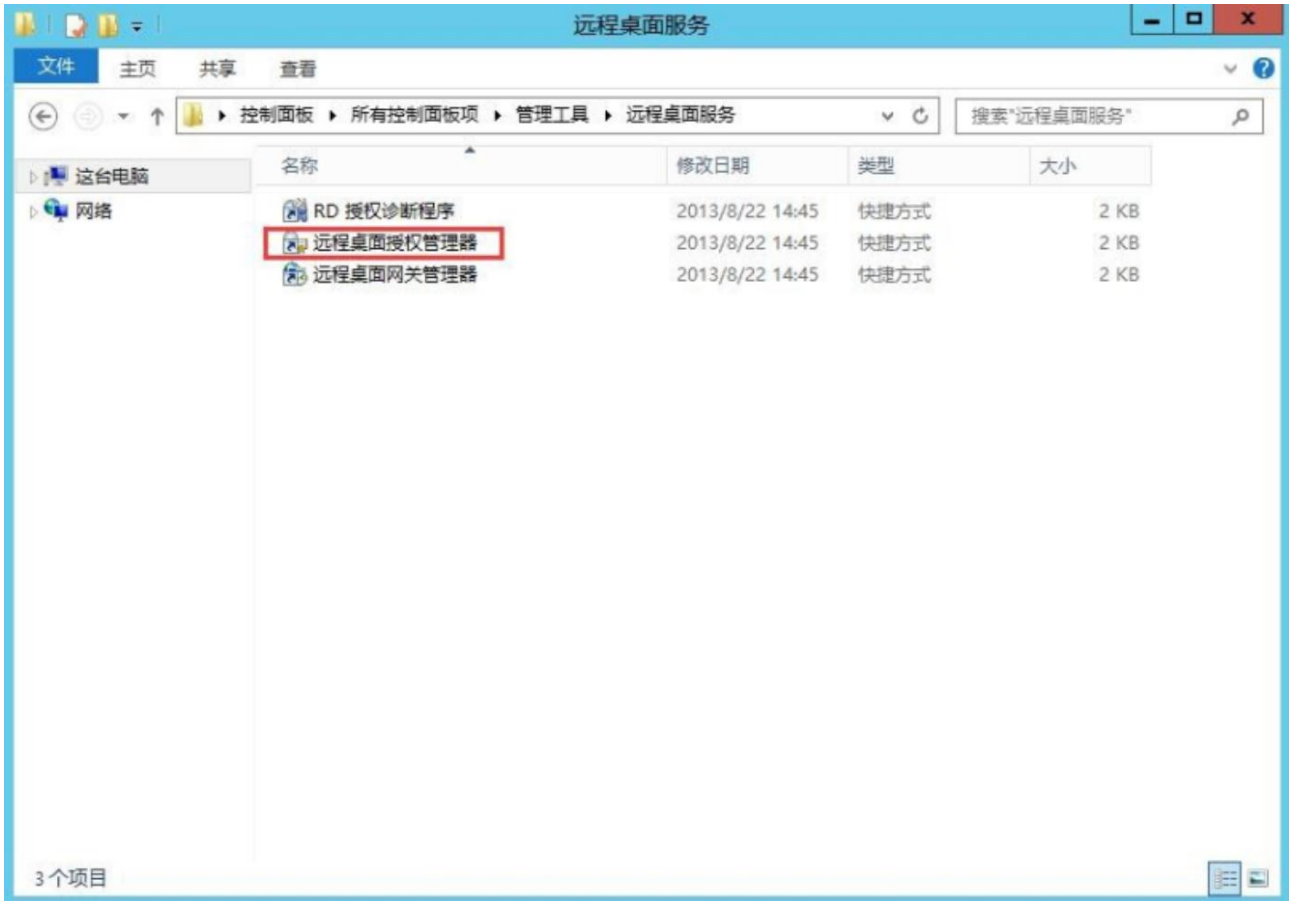
11. 确认配置选择，单击“安装”，请耐心等待安装进度完成。

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。

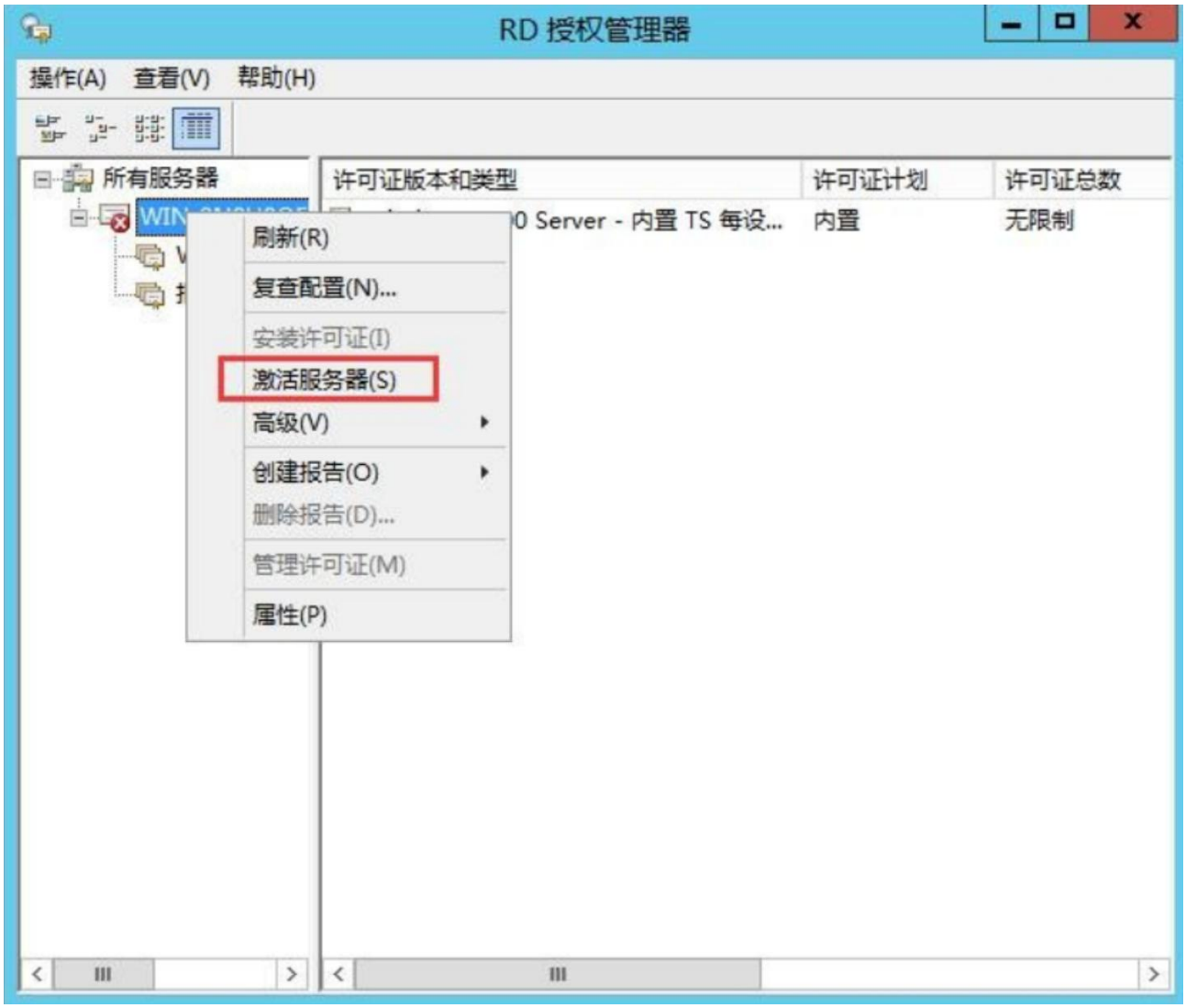
激活远程桌面服务

1. 使用管理员账号登录服务器。

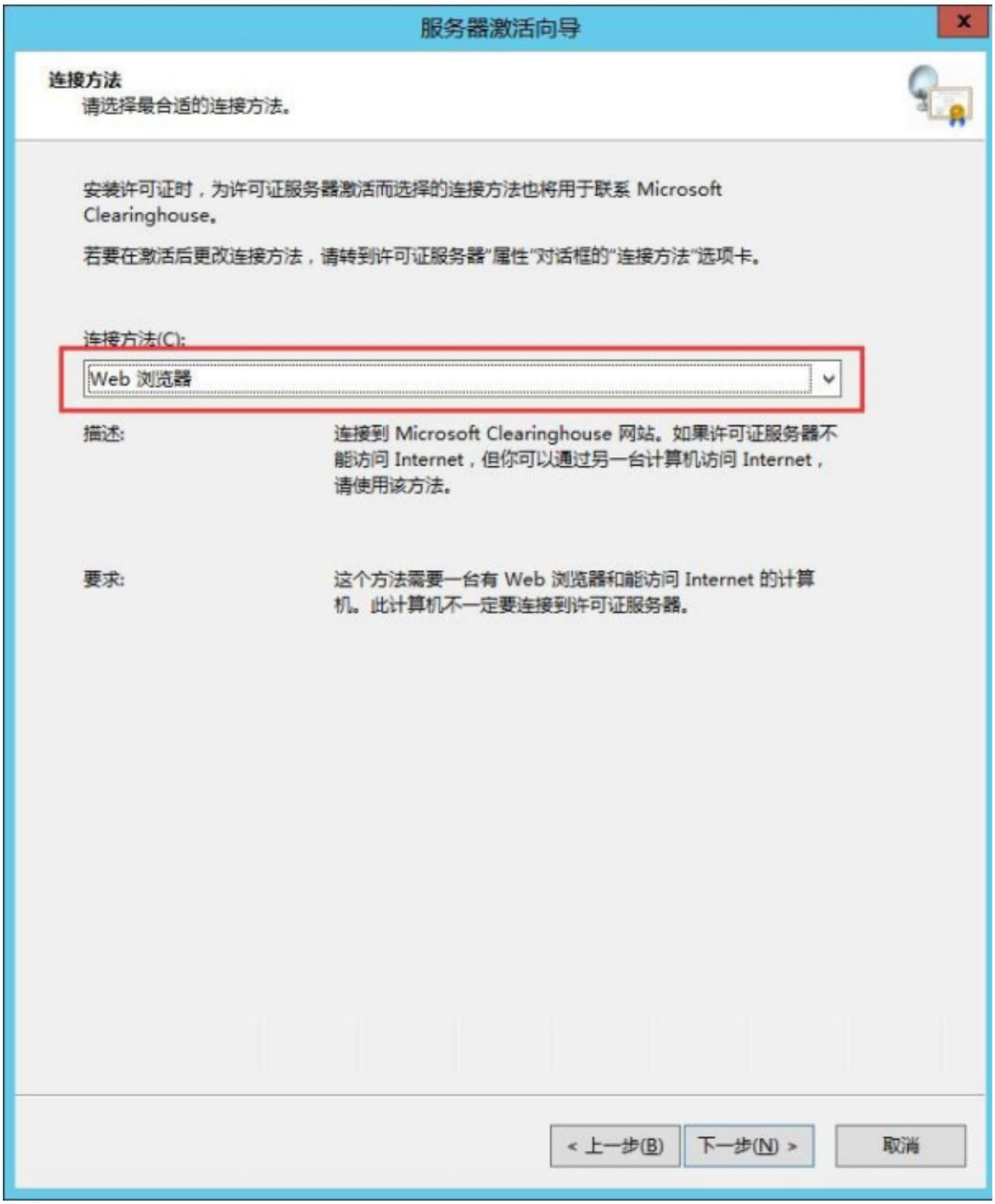
2. 选择“开始> 管理工具> 远程桌面服务> RD 授权管理器”，打开 RD 授权管理器界面。



3. 选择未激活的目标服务器，鼠标右键选择“激活服务器”。



4. 打开服务器激活向导界面，连接方法选择“Web 浏览器”。



5. 在激活向导页面选择复制产品 ID，并且进入微软官网进行激活操作。
6. 在网页中选择 Chinese(Simplified)简体中文，进入下一步。
7. 输入第五步中的产品 ID 和公司信息，进入下一步。
8. 获取许可证 ID，妥善保存此 ID 后，进入下一步。

9. 在授权信息处的许可证程序，选择“企业协议”，填写公司信息后，进入下一步。

10. 在产品类型处选择“Windows Server 2016远程桌面服务每用户客户端访问许可证”，数量选择“9999”，填入企业协议号（需购买后获取），点击下一步。

> 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。

11. 获取许可证密钥包 ID，回到第 5 步的页面，填入密钥包 ID，单击下一步。

12. 完成服务器激活。

服务器策略配置

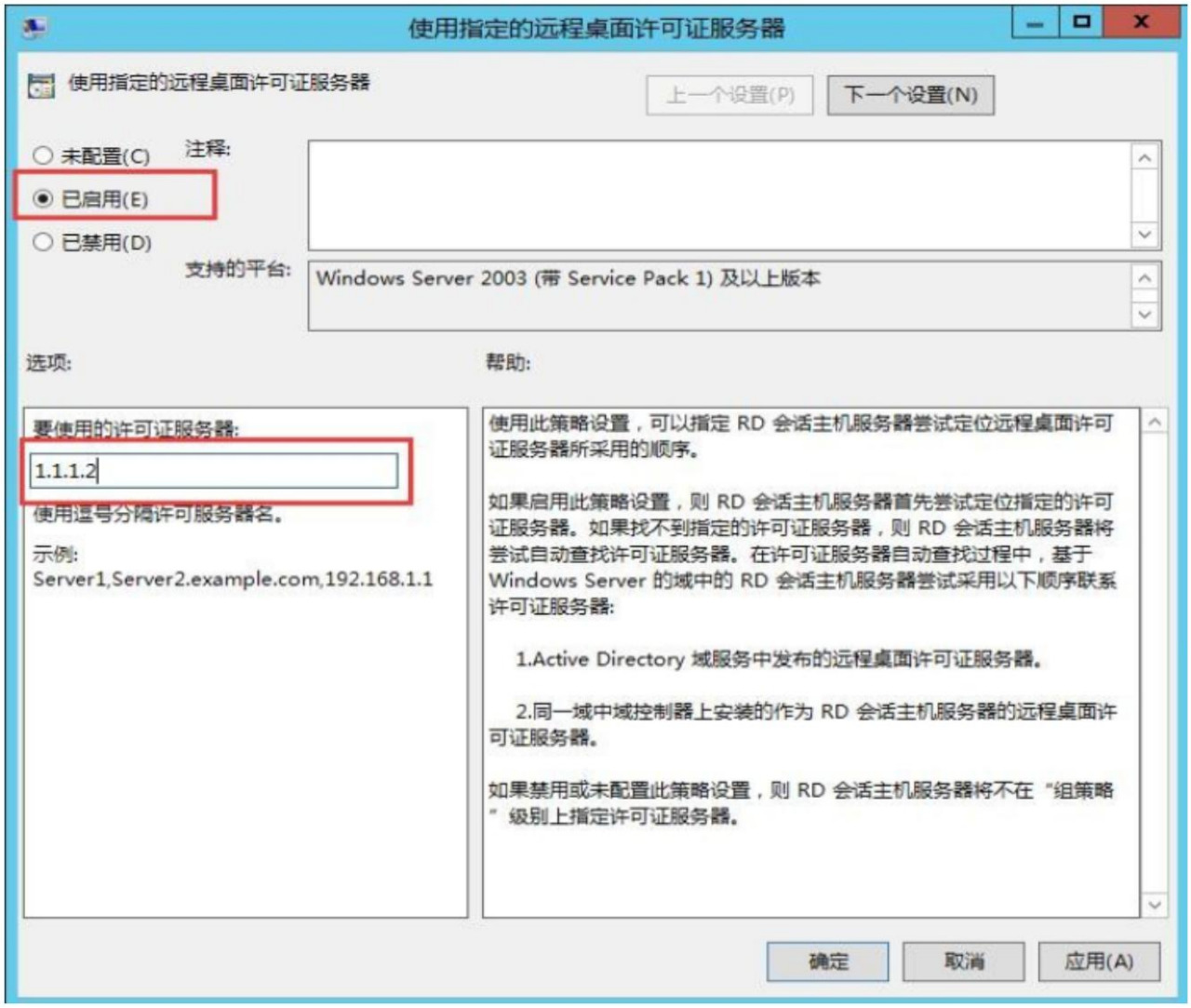
选择指定的远程桌面许可证服务器

1. 打开组策略编辑器：使用 Win+R 快捷键打开“运行”程序，输入“gpedit.msc”。

2. 在本地策略组选择“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。

3. 选择”使用指定的远程桌面许可证服务器“，进入设置窗口。

4. 在设置窗口勾选“已启用”，并且在“要使用的许可服务器”下填写本地服务器 IP。



5. 单击“确定”完成配置。

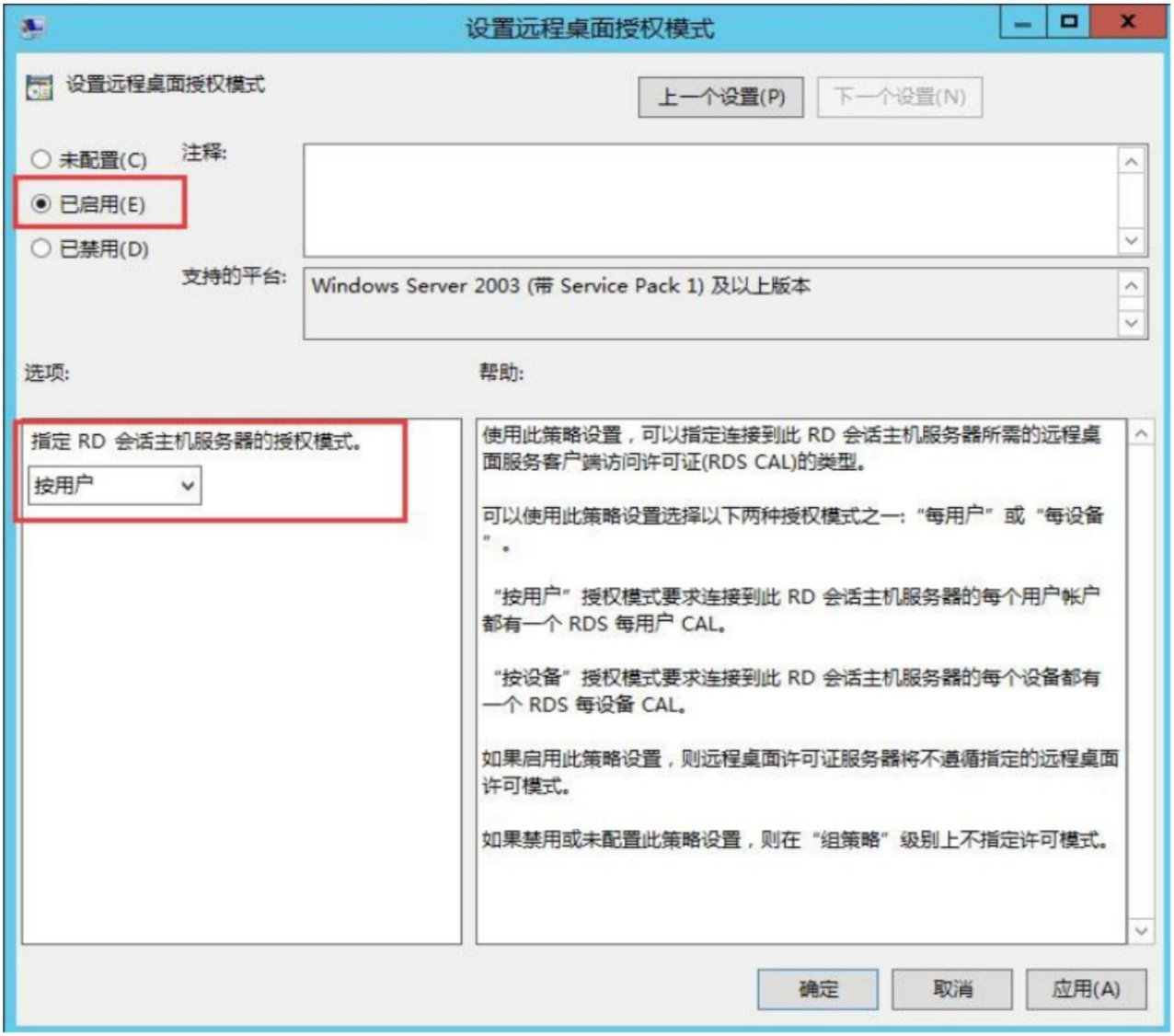
（可选）隐藏有关影响 RD 会话主机服务器的 RD 授权问题的通知

1. 打开组策略编辑器：使用 Win+R 快捷键打开“运行”程序，输入“gpedit.msc”。
2. 在本地策略组选择“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。
3. 选择“隐藏有关影响RD会话主机服务器的RD授权问题的通知”，进入设置窗口。
4. 选择“已启用”。

5. 单击“确定”完成配置。

设置远程桌面授权模式

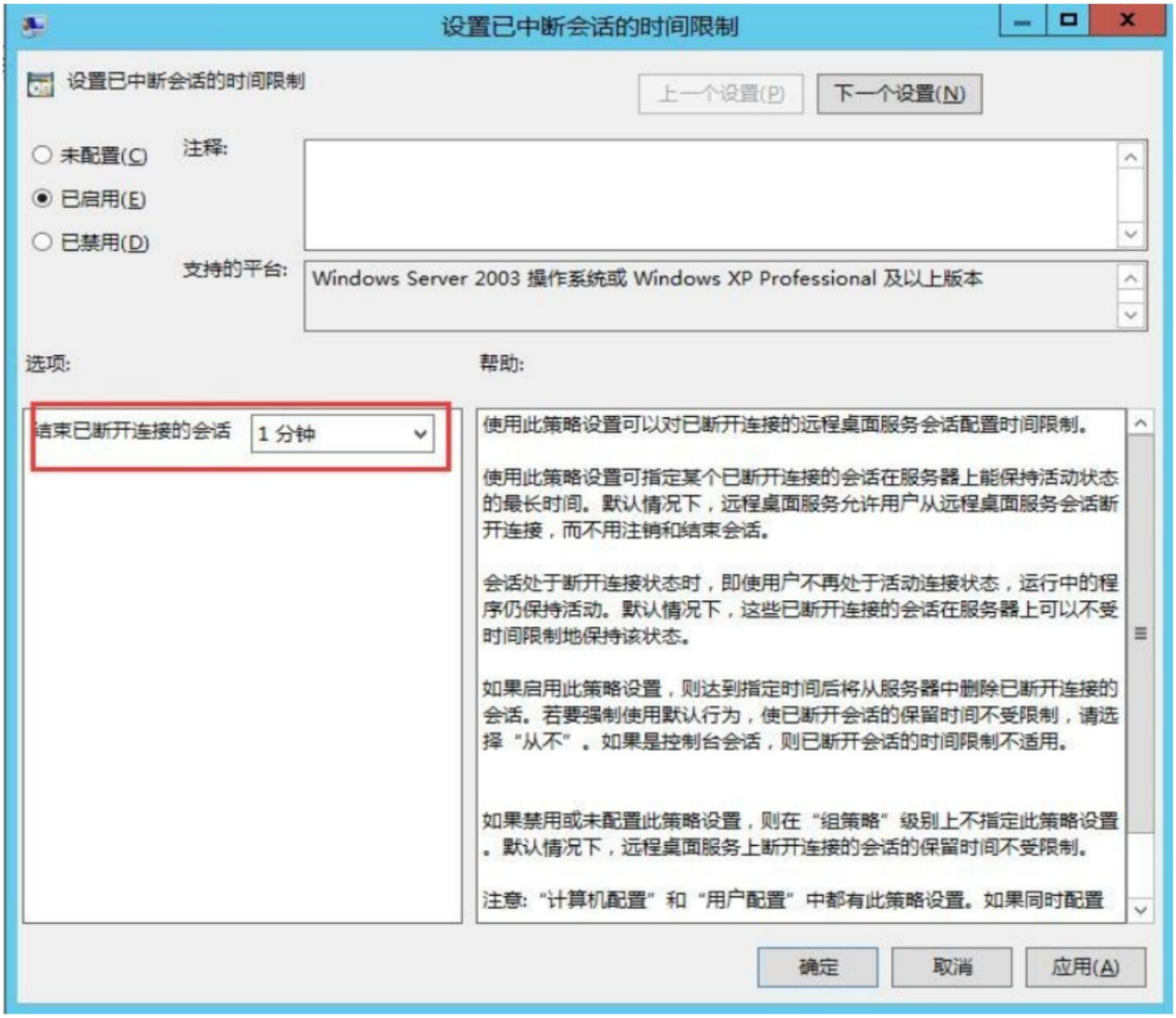
1. 打开组策略编辑器：使用 Win+R 快捷键打开“运行”程序，输入“gpedit.msc”。
2. 在本地策略组选择“计算机配置 > 管理模板 > Windows 组件 > 远程桌面服务 > 远程桌面会话主机 > 授权”，进入服务器授权许可设置页面。
3. 选择“设置远程桌面授权模式”，进入设置窗口。
4. 选择“已启用”，并且在在“指定 RD 会话主机服务器的授权模式”下拉列表中选择“按用户”。



5. 单击“确定”完成配置。

设置已中断的会话时间限制

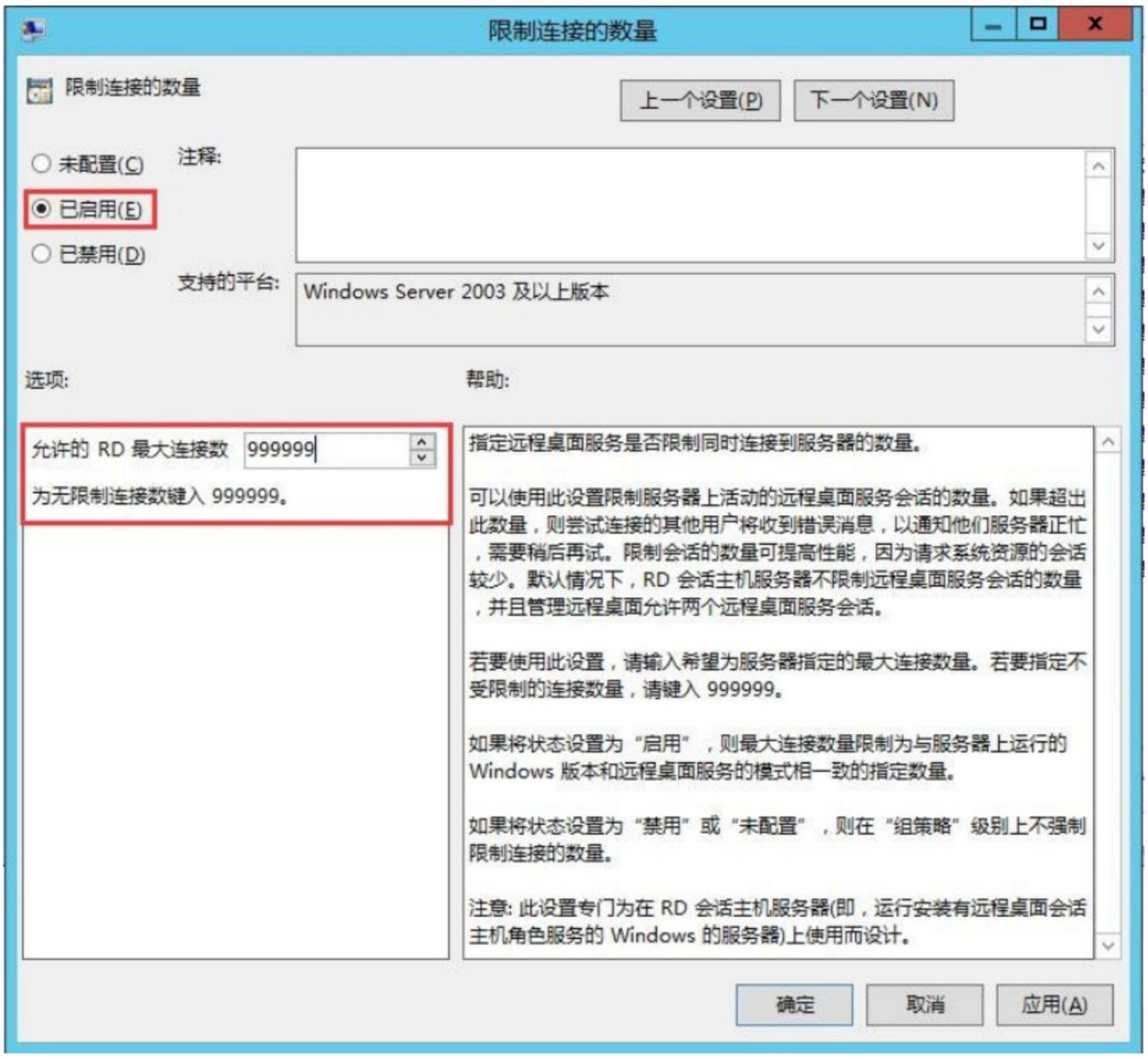
1. 打开组策略编辑器：使用 Win+R 快捷键打开“运行”程序，输入“gpedit.msc”。
2. 在本地策略组选择“计算机配置 > 管理模板 > Windows 组件 > 远程桌面服务 > 远程桌面会话主机 > 会话时间限制”，进入会话限制设置页面。
3. 选择“设置已中断会话的时间限制”，进入设置窗口。
4. 勾选“已启用”，并且设置结束已断开连接的会话为 1 分钟。



5. 单击“确定”完成配置。

限制连接的数量

1. 打开组策略编辑器：使用 Win+R 快捷键打开“运行”程序，输入“gpedit.msc”。
2. 在本地策略组选择“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。
3. 选择“限制连接数量”，进入设置窗口。
4. 勾选“已启用”，并且填写“RD 最大连接数”为 999999。



5. 单击“确定”完成配置。

允许远程启动未列出的程序

1. 打开组策略编辑器：使用 Win+R 快捷键打开“运行”程序，输入“gpedit.msc”。
2. 在本地策略组选择选择“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。
3. 选择“允许远程启动未列出的程序”，进入设置窗口。
4. 勾选“已启用”。
5. 单击“确定”完成配置。

禁用远程桌面服务用户限制到单独的远程桌面服务会话

1. 打开组策略编辑器：使用 Win+R 快捷键打开“运行”程序，输入“gpedit.msc”。

2. 在本地策略组选择选择“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。
3. 选择“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。
4. 勾选“已禁用”。
5. 单击“确定”完成配置。

更新组策略

1. 使用 Win+R 快捷键打开“运行”程序，输入“cmd”。
2. 在窗口中输入：”gpupdate /force“完成组策略更新。

远程设置

1. 选择“计算机”，右键选择“属性”。
2. 在“系统属性”窗口，选择“远程”，勾选“允许远程连接到此计算机”。

RemoteAPP 程序发布

您若要使用云堡垒机访问应用服务器，需要在应用发布服务器中安装 RemoteAppProxy 跳板工具。

- 2.8 及以上版本堡垒机请选择 open_app_mstsc.exe。
- 2.8 及以下版本堡垒机请选择 open_app_mstsc.exe。

堡垒机版本请参考：关于系统章节。

下载步骤：

1. 使用管理员账号登录服务器。
2. 在服务器中，将 RemoteAPP 程序拷贝到“C:\tool”目录中，若没有则手动创建该目录。
3. 将对应文件放到上述的目录中即可开始使用。

6.2.2.3 新增应用资产

用户获取应用资产访问权限后，通过应用发布服务器访问 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。

约束限制

- 仅企业版支持使用应用运维功能。
- 添加的主机和应用资源数量总和不能超过资产数。

前提条件

添加应用资产前，需已添加应用服务器，具体操作请参见应用服务器。

新增资产组

您可以通过应用资产组来管理多个应用资产，方便您在授权的时候可以一键选择。

1. 使用“管理角色”账户登录云堡垒机（原生版）控制台。
2. 在左侧导航栏选择“资产管理 > 应用资产”，进入应用资产页面。
3. 在应用资产列表左侧资产树中，单击资产组右侧的更多图标，选择“新增子节点”或“复制”。

   支持创建多级资产组，最多支持创建 10 级。
4. 在弹出的“新增资产组”或“资产组复制”对话框中，填写资产组信息。

参数	参数名称
资产组名称	自定义资产组的名称。
资产	在下拉框中选择需要添加至该资产组中的资产。
描述	自定义资产组的描述。

5. 填写完成后，单击“提交”完成资产组的创建。

   创建完成后，您也可以根据需要对资产组进行修改或删除：

   - **编辑资产组**：选择需要修改的资产组，单击资产组右侧的更多图标，选择“编辑”，按照需求对资产组进行修改，单击“确定”完成修改操作。
   - **删除资产组**：选择需要删除的资产组，单击资产组右侧的更多图标，选择“删除”，在弹出的对话框中单击“确定”完成删除操作。

添加应用资源

在完成应用服务器添加后，您可添加应用资源至云堡垒机中。

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“资产管理 > 应用资产”，进入“应用资产”页面。

3.单击“新增”按钮，弹出“新增应用资产”对话框，并填写相关内容。

参数	填写说明
应用名称	填写应用名称，在同一堡垒机内应用名称不得重复。
应用服务器	先选择客户端，然后再选择客户端所属的应用服务器。 客户端当前仅支持：Chrome、IE、Firefox、SecBrowser。
目标地址	填写正确的应用 IP 或域名。 说明： 若网页地址有对应的端口，则地址为 URL:端口号。
资产组	选择新增应用资源所属的资产组。
应用描述	填写应用服务器的简要描述。

4.填写完成后，单击“提交”即可完成新增应用资源。

6.2.3 资产组

您可以建立一个资产组来管理多个资产，方便您在授权的时候可以一键选择。

前提条件

仅“管理角色”支持资产相关的操作。

新增资产组

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“资产管理 > 资产组”，进入“资产组”页面。

3.单击“新增”，在弹出的对话框中填写内容。

参数	参数名称	取值样例
资产组名称	自定义资产组的名称。	Test
资产	在下拉框中选择需要添加至该资产组中的资产，如何新增资产请参见资产章节。	-
描述	自定义资产组的描述。	-

4.填写完成后，单击“提交”完成资产组的创建。

6.2.4 资产账号

每个被云堡垒机纳管的资产可能有一个或多个登录资产的账号。若您已配置了资产的相关账号，那么运维人员在登录纳管资产时，可以自动登录无需输入账号和密码。

前提条件

仅“管理角色”支持资产相关的操作。

新增资产账号

资产账号有两种添加方式：

- 在新增资产时添加，具体可参考资产章节。
- 在“资产账号”模块添加，本章节内容以此添加方式展开介绍。

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“资产管理 > 资产账号”，进入“资产账号”页面。

3.单击“新增”按钮，在弹出的“新增资产账号”对话框中添加资产信息。

参数	参数说明	取值样例
资产名	选择需要添加资产账号的资产，请确保待添加的账号可以正常登录该资产。	-
账号名	填写可登录资产的账号名，例如：Administrator。	Administrator
密码	（可选）输入正确的账号密码。若不输入密码，则在登录资产时需要填写正确的密码才可登录。	-
私钥	（可选）若账户登录需要使用私钥验证，请开启此选项并且上传 RSA 私钥证书。	
使用协议	（可多选）请选择资产的协议，支持选择：SSH、TELNET、SFTP、FTP、X11、RDP和数据库。	SSH
状态	（可选）选择新增账号目前的状态，可选“正常”或“冻结”。	正常
二次登录	该功能主要用于配置不允许直接登录的特权账号（例如root），实现免密提权。 开启二次登录，并配置源账号名、切换命令，可将源账号提权为特权账号。 说明 仅 ssh、telnet 协议支持配置二次登录。	
源账号名	选择已配置的资产账号作为源账号（例如 testuser），二次登录场景将由该源账号提权为特权账号。	testuser
切换命令	针对 CTyunOS、CentOS 系统，执行该切换命令，实现由源账号提权到特权账号，例如 su - root。 **说明** 资产系统上的源账号需要具有执行切换命令（例如 su -）的权限。若没有权限，可参考如下操作进行配置： # 将 testuser 加入 wheel 组 usermod -aG wheel testuser # 刷新组 newgrp wheel	su -

4.填写完成后单击“提交”即成功新增资产账号。

导入资产账号

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“资产管理 > 资产账号”，进入“资产账号”页面。

3.单击“导入”按钮，在弹出的对话框中下载导入模板。

4.在导入模板文件中填写内容，填写完成后保存。

说明

- 红色标题必填；
- 多个资产、协议用英文逗号“,”隔开；
- 协议可选：SSH、TELNET、SFTP、FTP、X11、RDP、数据库。

参数	参数说明	取值样例
资产	填写需添加资产账号的资产名（资产名需和堡垒机控制台上显示的一致），请确保待添加的账号可以正常登录该资产。	Test
账号名	填写可登录资产的账号名，例如：Administrator。	Administrator
密码	（可选）输入正确的账号密码。若不输入密码，则在登录资产时需要填写正确的密码才可登录。	-
协议	（可填多项）请选择资产的协议，支持填写：SSH、TELNET、SFTP、FTP、X11、RDP 和数据库。	

参数	参数说明	取值样例
状态	（可选）选择账号当前的状态，支持“正常”和“冻结”，导入模板时若不填写该项，默认为“冻结”状态	正常
私钥	（可选）若账户登录需要使用私钥验证，你上传的私钥认证优先级高于密码认证。	-
二次登录	该功能主要用于配置不允许直接登录的特权账号（例如 root），实现免密提权。 开启二次登录，并配置源账号名、切换命令，可将源账号提权为特权账号。 说明 仅 ssh、telnet 协议支持配置二次登录。	
源账号名	选择已配置的资产账号作为源账号（例如 testuser），二次登录场景将由该源账号提权为特权账号。	testuser

编辑资产账号

若您的资产账号密码保存在堡垒机内，并且近期发生了密码变更，那么您可以通过编辑资产账号来修改保存在堡垒机上的密码。

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“资产管理 > 资产账号”，进入“资产账号”页面。

3.选择需要修改账号信息的资产账号，单击“操作”列的“编辑”按钮。

4.在弹出的对话框中修改相关参数，单击“提交”完成修改。

冻结/解冻资产账号

您可以在云堡垒机控制台冻结已纳管的资产账号，处于“冻结”状态的资产账号无法登录资产。

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“资产管理 > 资产账号”，进入“资产账号”页面。

3.勾选需要冻结/解冻的账号，单击“冻结”/“解冻”按钮。

4.在弹出的对话框中单击“确定”完成操作。

6.2.5 账户改密

改密策略是一种自动化工具，旨在增强主机资源账户的安全性。它允许用户通过预设的策略，对一个或多个主机资源账户的密码进行手动、定时或周期性的修改。

以下是改密策略的主要功能：

- 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，以及生成指定相同密码。

说明：

随机生成的密码遵循以下设定：随机生成的密码长度为 8-30 个字符，同时包含三项（大小字母、数字、()`!@#$%^&_-+=|[]{}:;<>,.?/中的特殊符号），且不会以“/”开头，不会出现连续三个以上相同字符。

新建改密策略

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“资产管理 > 改密策略”，进入“改密策略”页面。

3.单击页面右上角的“新建”按钮，填写改密策略相关参数。

参数	参数说明	取值样例
名称	自定义改密策略名称。	定期改密
描述	自定义改密策略描述。	XX 主机定期改密策略

参数	参数说明	取值样例
改密账号	添加改密账号： ● 目前仅支持添加 SSH、Telnet 协议的主机账号。 ● 选择后改密账号格式为：协议[资产账号名@]资产名称。	SSH[admin@]Test01
执行策略	按需选择您的执行策略： ● 立即执行：保存后立即执行。 ● 定时执行：在选择时间后，仅在选择的事件执行一次。 ● 周期执行：选择执行起始时间和执行周期。	立即执行
改密方式	按需选择您的改密方式： ● 随机生成不同密码 ● 随机生成相同密码 ● 手动生成指定密码	手动生成指定密码
指定密码	仅在“改密方式”选择“手动生成指定密码”时可填写。	-
改密完成通知	通过开关按钮选择是否进行通知。	
收件人邮箱	填写接收改密内容的邮箱，仅支持填写一个邮箱。 改密结果会以加密附件的方式发送。	admin@chinatelecom.cn
改密附件密码	填写改密附件的密码。	-

4.填写完成后，单击“提交”即可完成新建改密策略。

后续操作

- 立即执行改密策略：选择需要执行改密的账号，在对应策略下单击“操作”列的“立即执行”即可执

行改密。

- 编辑改密策略：选择需要编辑的改密策略，单击“操作”列的“编辑”，在弹出的对话框中修改内容后单击“提交”即可完成修改。

查看改密记录

每条策略完成一次改密操作后会生成一条改密记录，您可以选择“操作”列的“改密记录”查看该条策略生成的改密记录。

6.3 授权管理

6.3.1 资源访问授权

资产访问授权用于控制用户访问资产的权限。

云堡垒机支持对运维用户限制登录时间段和协议限制。

前提条件

仅“管理角色”支持资产相关的操作。

新增访问资产授权

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“授权管理 > 资产访问授权”，进入“资产访问授权”页面。

3.单击“新增”按钮，在弹出的“新增资产访问授权”对话框中配置信息。

参数	参数说明	取值样例
授权规则名称	自定义资产访问授权的规则名称。	Test
启用状态	选择该授权规则的启用状态，默认启用。	

参数	参数说明	取值样例
用户	（可选）选择需要配置访问授权的用户。	-
用户组	（可选）选择需要配置访问授权的用户组。 若您选择的用户和用户组存在重合，默认取最大的合集。	-
资产	（可选）选择需要配置访问授权的资产。	-
资产组	（可选）选择需要配置访问授权的资产组。 若您选择的资产和资产组存在重合，默认取最大的合集。	-
资产账号	（可选）选择资产授权规则中允许使用的资产账号，添加资产账号请参见：资产账号章节。 注意： 若选择授权的资产账号为二次登录账号（例如 root），需同时授权二次登录的源账号（例如添加 root 资产账号时配置的二次登录源账号 testuser），否则将无法完成二次登录。	-
协议	选择该授权规则支持访问的协议。	SSH
授权时间	选择该规则生效的时间段。	-

4.单击“提交”完成访问授权规则的创建。

批量导入访问授权

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“授权管理 > 资产访问授权”，进入“资产访问授权”页面。

3.单击“导入”，在弹出的对话框中下载导入模板。

4.打开模板，配置相关内容。

参数	参数说明	取值样例
授权规则名称	自定义资产访问授权的规则名称。	Test
启用状态	选择授权规则创建完成后的启用状态，可选择“启用”或“禁用”。	启用

参数	参数说明	取值样例
用户	（可选）填写需要配置访问授权的用户名，用户名请保持和系统中添加用户名保持一致。	-
用户组	（可选）填写需要配置访问授权的用户组，用户组请保持和系统中添加用户组名保持一致。 若您填写的用户和用户组存在重合部分，取两者最大的合集。	-
资产	（可选）填写需要配置访问授权的资产，资产名称请保持和系统中添加的资产名保持一致。	-
资产组	（可选）填写需要配置访问授权的资产，资产组名称请保持和系统中添加的资产名保持一致。	-
资产账号	（可选）选择资产授权规则中允许使用的资产账号，添加资产账号请参见：资产账号章节。	-
协议	选择该授权规则支持访问的协议，协议可填写：SSH、TELNET、SFTP、FTP、X11、RDP、数据库。	SSH
生效时间	填写规则生效的日期，日期格式请使用 yyyy-mm-dd 或 yyyy/mm/dd。	2023-10-01
失效时间	填写规则失效的日期，日期格式请使用 yyyy-mm-dd 或 yyyy/mm/dd。	2024-10-01

5.填写完成后，保存文件并上传。

后续操作

- 导出授权访问规则：勾选需要导出的资产访问授权规则，单击“导出”即可导出授权访问规则。
- 启用/禁用授权访问规则：勾选需要启用/禁用的资产访问授权规则，单击“启用/禁用”即可导出授权访问规则。

6.3.2 字符命令授权

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，云堡垒机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、拒绝使用等动作。

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（优先级可选 1-100）。
- 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：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：触发该策略规则后，拒绝执行该命令，界面会提示您在执行命令时会得到该命令不能执行的提示。
  - 警告：触发该策略规则后，警告运维用户谨慎执行该命令。

新增命令组

您在新增字符命令授权前需要进行新增命令组的操作。

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“授权管理 > 字符命令授权”，进入“命令授权”页面。

3.在页面上面选择“命令组”页签，单击“新增”，开始新增命令组。

参数	参数说明	取值样例
名称	自定义命令组的名称。	Test
匹配方式	支持正则匹配和单命令匹配。	单命令匹配
命令	（仅选择单命令匹配填写）填写命令。	/rm
命令正则式	填写命令规则的正则表达式。	en\w*
风险等级	选择该命令组的风险等级，共可选 5 个等级。	普通
动作	选择该命令组中的命令触发时产生的动作： ● 允许：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：触发该策略规则后，拒绝执行该命令，界面会提示您在执行命令时会得到该命令不能执行的提示。 ● 警告：触发该策略规则后，警告运维用户谨慎执行该命令。	拒绝

说明：

- 提示符、命令采用正则表达式书写；
- 命令匹配上多条策略时，动作执行优先级“警告”>“允许”>“拒绝"，若未匹配上任何策略则放行。

命令组后续操作

- 修改命令组：选择需要修改的命令组，单击“操作”列中“编辑”，按照需求进行命令组数据的修改，单击“提交”完成命令组数据更新。
- 删除命令组：选择需要删除的命令组，单击“操作”列中“删除”，在弹出的对话框中单击“确定”即可删除命令组。

注意：

删除后的命令组不可恢复，并且若命令组已绑定命令授权规则会导致该命令规则失效，请谨慎操作。

新增命令授权规则

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“授权管理 > 字符命令授权”，进入“命令授权”页面。

3.单击“新增”，开始新增字符命令授权。

参数	参数说明	取值样例
授权规则名称	自定义资产访问授权的规则名称。	Test
启用状态	选择该授权规则的启用状态，默认启用。	
用户	（可选）选择需要配置访问授权的用户。	-
用户组	（可选）选择需要配置访问授权的用户组。 若您选择的用户和用户组存在重合，默认取最大的合集。	-

参数	参数说明	取值样例
资产	（可选）选择需要配置访问授权的资产。	-
资产组	（可选）选择需要配置访问授权的资产组。 若您选择的资产和资产组存在重合，默认取最大的合集。	-
资产账号	选择命令授权规则生效的资产账号，添加资产账号请参见：资产账号章节。	-
敏感命令	选择需要进行控制的命令组，并填写优先级，优先级范围：1-100，数字越小优先级越高。	-
授权时间	选择该规则生效的时间段。	-

说明：

配置时至少需要关联至少一个授权对象，否则这条命令策略不起作用，其余未关联的表示对所有生效；

以基础设施访问授权时，账号必须拥有该基础设施访问授权的访问权限策略才会生效。

后续操作

- 启用/禁用授权规则：可单个或批量启用/禁用授权规则，禁用的授权规则状态将更新为“无效”，启用的授权规则状态更新为“有效”，只有状态为“有效”的规则授权会生效。
- 编辑授权规则：选择需要修改的规则，单击“操作”列的“编辑”，按照需求进行命令授权数据的修改，单击“提交”完成命令授权数据更新。
- 删除授权规则：在需要删除的授权数据的“操作”列单击“删除”，在弹出的对话框中单击“确定”完成删除。

6.3.3 数据库命令授权

数据库命令授权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。

数据库命令授权支持以下功能项：

- 支持按命令组列表排序区分优先级，排序数字越小优先级越高。
- 支持控制允许、拒行两种命令动作。
  - 允许：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：触发该策略规则后，拒绝执行该操作。

约束限制

- 仅企业版堡垒机支持数据库运维操作审计。
- 仅针对 MySQL、Oracle、Postgresql 类型数据库，支持通过数据库命令授权设置操作细粒度控制。

新增命令组

您在新增数据库命令授权前需要进行新增命令组的操作。

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“授权管理 > 数据库命令授权”，进入“数据库命令授权”页面。

3.在页面上面选择“命令组”页签，单击“新增”，开始新增命令组。

参数	参数说明	取值样例
名称	自定义命令组的名称。	Test
动作	选择该命令组中的命令触发时产生的动作： ● 允许：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：触发该策略规则后，拒绝执行该命令，界面会提示您在执行命令时会得到该命令不能执行的提示。	拒绝
SQL 命令类型	根据您业务的需求，选择需要进行控制的命令，云堡垒机目前支持选择如下命令： SELECT、INSERT、UPDATE、DELETE、TRUNCATE、CREATE、DROP、ALTER、GRANT、REVOKE。	SELELCT
SQL 库名	填写命令生效的 SQL 库名。	Test
SQL 表名	填写命令生效的 SQL 表名。	Test

参数	参数说明	取值样例
风险等级	选择该命令组的风险等级，共可选 5 个等级。	普通

命令组后续操作

- 修改命令组：选择需要修改的命令组，单击“操作”列中“编辑”，按照需求进行命令组数据的修改，单击“提交”完成命令组数据更新。
- 删除命令组：选择需要删除的命令组，单击“操作”列中“删除”，在弹出的对话框中单击“确定”即可删除命令组。

注意：

删除后的命令组不可恢复，并且若命令组已绑定命令授权规则会导致该命令规则失效，请谨慎操作。

新增命令授权规则

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“授权管理 > 数据库命令授权”，进入“命令授权”页面。

3.单击“新增”，开始新增字符命令授权。

参数	参数说明	取值样例
授权规则名称	自定义资产访问授权的规则名称。	Test
启用状态	选择该授权规则的启用状态，默认启用。	
用户	（可选）选择需要配置访问授权的用户。	-
用户组	（可选）选择需要配置访问授权的用户组。 若您选择的用户和用户组存在重合，默认取最大的合集。	-
资产	（可选）选择需要配置访问授权的资产。	-
资产组	（可选）选择需要配置访问授权的资产组。	-

参数	参数说明	取值样例
	若您选择的资产和资产组存在重合，默认取最大的合集。	
资产账号	选择命令授权规则生效的资产账号，添加资产账号请参见：资产账号章节。	-
敏感命令	选择需要进行控制的命令组，并填写优先级，优先级范围：1-100，数字越小优先级越高。	-
授权时间	选择该规则生效的时间段。	-

说明：

- 配置时至少需要关联至少一个授权对象，否则这条命令策略不起作用，其余未关联的表示对所有生效；
- 以基础设施访问授权时，账号必须拥有该基础设施访问授权的访问权限策略才会生效。

后续操作

- 启用/禁用授权规则：可单个或批量启用/禁用授权规则，禁用的授权规则状态将更新为“无效”，启用的授权规则状态更新为“有效”，只有状态为“有效”的规则授权会生效。
- 编辑授权规则：选择需要修改的规则，单击“操作”列的“编辑”，按照需求进行命令授权数据的修改，单击“提交”完成命令授权数据更新。
- 删除授权规则：在需要删除的授权数据的“操作”列单击“删除”，在弹出的对话框中单击“确定”完成删除。

6.3.4 文件操作授权

文件操作授权用于控制用户访问资源时对资源内的文件操作的权限。

文件操作权限的可选范围是：

- 上传：允许/拒绝运维用户上传文件。
- 下载：允许/拒绝运维用户下载文件。

- 删除：允许/拒绝运维用户删除文件。
- 创建目录：允许/拒绝运维用户新建目录。
- 删除目录：允许/拒绝运维用户删除目录。
- 移动/重命名：允许/拒绝运维用户移动/重命名文件。

新增文件操作授权

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“授权管理 > 文件操作授权”，进入“文件操作授权”页面。

3.单击“新增”，配置文件操作授权相关内容。

参数	参数说明	取值样例
授权规则名称	自定义资产访问授权的规则名称。	Test
动作	选择此授权规则的动作，可选“允许”或“拒绝”。	允许
启用状态	选择该授权规则的启用状态，默认启用。	
用户	（可选）选择需要配置访问授权的用户。	-
用户组	（可选）选择需要配置访问授权的用户组。 若您选择的用户和用户组存在重合，默认取最大的合集。	-
资产	（可选）选择需要配置访问授权的资产。	-
资产组	（可选）选择需要配置访问授权的资产组。 若您选择的资产和资产组存在重合，默认取最大的合集。	-
资产账号	选择命令授权规则生效的资产账号，添加资产账号请参见：资产账号章节。	-
文件	选择需要做限制的文件操作动作。可填写具体的文件或文件目录，使用正则表示填写，若填写多个用英文的“,”分隔。	-
授权时间	选择该规则生效的时间段。	-
源 IP	填写用户登录的源 IP 地址。	0.0.0.0

参数	参数说明	取值样例
风险等级	选择此授权规则的风险等级，共有 5 个等级可选择。	普通

说明

- 策略匹配顺序为：允许 > 阻断；

  配置时至少需要关联至少一个授权对象，否则该条授权策略不会生效，其余未关联的表示对所有生效；
- 以基础设施访问授权时，账号必须拥有该基础设施访问授权的访问权限策略才会生效。

后续操作

- 启用/禁用授权规则：可单个或批量启用/禁用授权规则，禁用的授权规则状态将更新为“无效”，启用的授权规则状态更新为“有效”，只有状态为“有效”的规则授权会生效。
- 编辑授权规则：选择需要修改的规则，单击“操作”列的“编辑”，按照需求进行文件操作授权数据的修改，单击“提交”完成文件操作授权数据更新。
- 删除授权规则：选择需要删除的规则，单击“操作”列的“删除”，在弹出的对话框中单击“确定”完成删除。

6.4 自动运维

云堡垒机具备自动运维功能，允许用户依照既定步骤自行执行命令和运维脚本，对多个目标进行自动化运维管理。除此之外，系统支持设定任务执行的周期和时间，实现自动化定期执行。同时，它还能够并行处理多种类型的任务步骤，大大提高了效率。

约束限制

- 仅企业版云堡垒机支持自动运维功能。
- 仅支持对 Linux 主机（SSH、Telnet 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。
- 管理员和运维角色都支持自动化运维功能
- 用户自动化运维可执行的命令和脚本受到命令权限的限制

新建自动运维策略

1.使用“管理角色”或“运维角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“自动运维”，进入“自动运维”页面。

3.单击“新增”，开始新增自动运维策略。

4.在弹出的“新增自动运维策略”对话框中填写相关内容。

配置项	说明
任务名称	自定义运维策略名称。
描述	自定义运维策略的描述内容。
资产账号	单击“添加”选择需要自动化运维的设备及账号。
执行策略	选择运维策略。 ● 立即执行：保存运维策略后立即执行该策略。 ● 定时执行：选取执行时间，保存后在对应时间执行该策略。 ● 周期执行：选取首次执行时间和执行周期（天），保存后在对应时间执行该策略。
执行方式	选择自动化运维的执行方式。 ● 执行命令：在“执行命令”参数框中填写需要执行的运维的命令。 ● 执行脚本：上传可使用的.sh/.py 脚本命令，若有相关脚本参数在“脚本参数”对话框中填写，多个参数使用英文逗号","分隔。

5.单击“确认”，弹出“验证用户身份”窗口。

6.在“验证用户身份”窗口输入资产账号的密码，完成输入后单击“提交”即可完成自动运维策略建立。

后续操作

- 立即执行：单击“操作”列的“立即执行”即可马上执行对应的运维策略。
- 编辑自动运维策略：选择需要修改的运维策略，单击“操作”列的“编辑”即可编辑自动运维策略。
- 启用/禁用自动运维策略：选择需要启用/禁用的运维策略，单击“操作”列的“更多 > 启用/禁用”即可编辑启用/禁用运维策略。

6.5 工单管理

6.5.1 审批规则

工单功能是指运维用户在申请资源访问权限或命令使用权限时，可通过工单申请资源的范围，以及提交工单的方式。

新增工单审批方式

1. 登录云堡垒机系统。
2. 在左侧导航栏选择“工单管理”>“审批规则”，进入“审批规则”页面。
3. 单击左上角的【新增】按钮，弹出“规则审批”配置窗口。

4. 在弹出的对话框中配置相关内容，具体见下表，配置完成后单击“提交”。

规则名称	输入您的审批规则名称。
工单类型	根据业务需求选择审批规则： ● 资产访问授权 ● 字符命令授权 ● 文件操作授权 ● 数据库命令授权 ● 数据导出授权 注意：字符授权工单默认开通所有命令的使用权限，若您需要限制高危命令的使用 请在“字符命令授权”模块将对应用户纳管入相关授权规则当中。
审核人	选择该审批规则的具体审核人员，可多选。
用户（可选）	选择该条审批规则可以提交的相关用户，可多选。
用户组（可选）	选择该条审批规则可以提交的相关用户组，可多选。

后续管理

- 若需修改审批规则，可单击“操作”列的“编辑”按钮，在弹出的编辑窗口重新配置相关内容。
- 若不再需要某条审批规则 ，可在单击“操作”列的“删除”按钮。删除后的信息不能找回，请谨慎操作。

6.5.2 工单审批

1. 登录云堡垒机系统。
2. 在左侧导航栏单击“工单管理”>“工单审批”，进入工单审批页面。

3. 查找需要待审批的工单，单击“操作”列的“审批”按钮。

4. 在弹出的“工单审批”对话框中，查看待审批的工单内容，选择是否批准。

6.6 系统管理

6.6.1 通知和告警

云堡垒机支持发送以下通知内容至您设置的接收邮箱或者站内信：

- CPU、内存、磁盘资源使用率超过 80%
- 账号密码剩余 3 天过期
- 用户恶意登录情况告警
- 访问人员执行敏感命令(字符、数据库) 达到风险等级设置发送告警。

说明：

- 邮件通知需校验，如果没有配置邮件服务器，“邮件通知“选项为禁用状态。
- 对于系统状态的告警，触发后，下一次提醒间隔时长为 24 小时。
- 敏感命令告警，可展开自定义选择风险等级，默认为勾选：警告、危险、致命。

邮件服务器配置

1. 使用“管理角色”账号登录云堡垒机。

2. 在左侧导航栏选择“系统管理 > 通知和告警”，进入“邮件服务器配置”页面。

3. 在左侧邮件服务器模块，单击“编辑”按钮配置邮件服务器。

参数	参数说明
服务器地址	填写您的邮件服务器地址。
服务端口	填写您的邮件服务器端口
安全通信	选择是否开启安全通信。 安全通信支持 TLS/SSL 协议。
发送人账号	填写发送邮件的邮箱账号。
发送人密码	填写发送邮件的邮箱密码。

4. 单击“保存”完成邮件服务器配置。

后续操作

完成邮件服务配置后，单击“测试邮件服务”，在弹窗中填写发送测试邮件的邮件地址，单击“发送测试邮件”即可测试邮件是否可以正常发送。

- 邮件发送**成功**后在测试邮箱中会收到一封测试邮件，邮件服务配置正确；
- 若提示邮件发送**失败**，请检测配置的邮件服务信息，更正后再次测试。

配置通知

1. 使用“管理角色”账号登录云堡垒机。
2. 在左侧导航栏选择“系统管理 > 告警和通知”，进入“告警和通知”页面。
3. 在右侧根据自身需求选择发送通知的项目。

6.6.2 安全设置

云堡垒机安全设置模块支持您自定义密码强度、账户保护规则。

密码组成：配置用户密码策略，包括配置密码安全强度，密码字符组成。

密码事件：可设置安全登录事件、强制改密时间和首次登录改密。

账号策略：可设置账号空闲事件。

设置密码组成

1.使用“管理角色”账号登录云堡垒机。

2.在左侧导航栏选择“系统设置 > 安全管理”，进入“安全管理”模块。

3.选择密码组成模块，配置密码规则。

设置密码事件

密码事件包含恶意登录事件、密码过期事件、强制改密，用户可根据使用需求对事件进行设置开启或关闭，单击“保存”后生效。

- 恶意登录事件：根据设置的时间和密码错误次数生效，触发后账号锁定，状态变更为“锁定 F”，可联系管理员操作解锁。
- 密码过期事件：根据设置的有效时间生效，有效时间到期后，触发账号锁定，状态变更为“锁定 P”，可联系管理员操作解锁；密码过期提醒事件打开后，根据设置的提醒时间，到达提醒时间，发送一次提醒邮件，到达提醒时间最后一天，再发送一次提醒邮件。
- 强制改密：默认开启，开启强制改密后，用户首次登录堡垒机跳转强制改密界面，强制用户改密后登录。

设置账号事件

账号事件包含账号空闲事件、账号登录事件，您可根据使用需求对事件进行设置开启或关闭，单击“保存”后生效。

账号空闲事件：根据设置的空闲时间生效，距离上一次登录时间达到设置时间后，触发账号锁定，状态变更为“锁定 L”，可联系管理员操作解锁；账号空闲提醒事件打开后，根据设置的提醒时间，到达提醒时间，发送一次提醒邮件，到达提醒时间最后一天，再发送一次提醒邮件。

账号登录事件：根据配置的唯 N 性值，限制同一账号同时登录数。

登录超时配置

您可在“登录超时配置”模块，配置用户登录超时时间和资产访问超时。

用户登录超时：可选择 10-1440 分钟，当用户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 分钟。

资产访问超时：可选择 10-1440 分钟，当用户访问资产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 分钟。

运维水印配置

您可在“运维水印配置”模块开启运维水印，开启运维水印后，默认显示“姓名”、“用户名”，您可选择是否显示“手机号”和“源 IP”。

国密配置

国密配置默认关闭，若您需要开启国密配置，请在工单页面提交工单申请开通。

国密配置开启后，系统将开启 USBKey 认证，用户可以通过 USBKey 认证的方式登录堡垒机。

注意：

- 开启国密配置后，堡垒机中保存的账户密码、个人信息和配置信息等将会使用国密算法加密。
- 若您需要为用户开启 USBKey 认证登录，需要先为用户开启 USBKey 证书认证。
- 开启国密配置后无法关闭，请您酌情选择。

获取 USBKey 认证证书

1.登录 USBKey 产品官网下载对应 USBKey 产品驱动。

2.将 USBKey 设备与电脑连接，并且打开 UKEY.html 页面，将右侧的按钮从上至下生成数据后，单击“导出证书”。

3.妥善保管好 USBKey 证书。

为用户绑定 USBKey 认证方式

1.使用“管理角色”账号登录云堡垒机。

2.在左侧导航栏选择“用户管理 > 用户”，进入“用户”模块。

3.选择需要绑定 USBKey 认证方式的用户，单击“操作”列的“更多 > 绑定证书”。

4.输入证书名称，并且在“证书”模块填入生成的证书。

Web 证书配置

您可以自行上传证书至云堡垒机。

说明：目前仅支持上传国际标准证书，暂不支持国密标准。

1.将“证书绑定”开关调整至开启状态，即可右侧弹出的对话框中绑定证书。

2.根据提示完成证书相关内容输入。

3.填写完成后，单击“确认”即开始证书校验，证书校验通过后会出现下图提示。

4.绑定完成后，会在控制台显示证书相关信息。

6.6.3 数据管理

您可在堡垒机存储配置页查看已使用的存储空间。当存储空间可用内存不足时，建议您及时删除历史系统数据，或变更实例规格扩充数据盘大小。

查看存储空间

1.登录云堡垒机（原生版）实例。

2.在左侧导航栏选择“系统管理 > 数据管理”，进入“存储配置”页面。

3.您可在“存储配置”页面查看已用的存储空间和设置自动删除的内容。

开启自动删除功能

1.打开自动删除功能，将“自动删除”后的按钮切换至开启状态 。

2.填写需要保留数据月数，默认为 6 个月。

3.勾选需要删除的内容后，单击“保存”。

管理日志备份

1.登录云堡垒机（原生版）实例。

2.在左侧导航栏选择“系统管理 > 数据管理”，选择“日志备份”页签。

3.开启日志备份，并填写 Syslog 服务器地址。

参数	参数说明	取值样例
状态	决定是否开启备份至 Syslog 服务器功能	
发送名称	用于标识堡垒机发送至 Syslog 服务器的日志。	Test
服务器 IP	填写正确的 Syslog 服务器 IP 地址。	0.0.0.0
端口	填写 Syslog 服务器的端口地址。	80
协议	选择访问 Syslog 服务器的协议。	UDP
备份内容	选择您需要备份的堡垒机中的业务内容。	-

4.填写完成后，单击“保存”即配置完成。

6.6.4 认证设置

管理员登录并切换管理角色，打开系统管理>认证设置，该配置为全局认证策略，默认配置“静态认证”“令牌认证”，应用于所有账号，为空的情况下默认为静态认证方式。

全局避险

开启全局避险开关以后，所有账号都可以使用静态认证方式登录。

6.6.5 系统状态

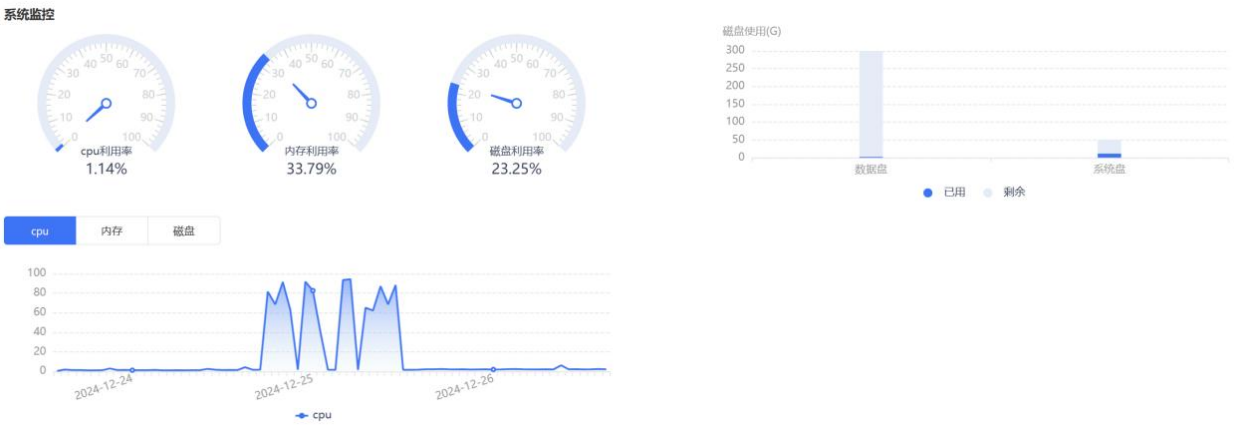
系统状态可以帮助您确认堡垒机系统的运行状况，可监控系统 CPU、内存、磁盘的使用状态，及时了解系统的运行状况。

查看系统状态

1.使用管理角色账号登录云堡垒机。

2.在左侧导航栏选择“系统管理 > 系统状态”，进入“系统状态”页面，即可查看系统状态。

系统监控可查看堡垒机的“CPU 利用率”、“内存利用率”和“磁盘利用率”的情况，每 1 个小时记录一次数值。

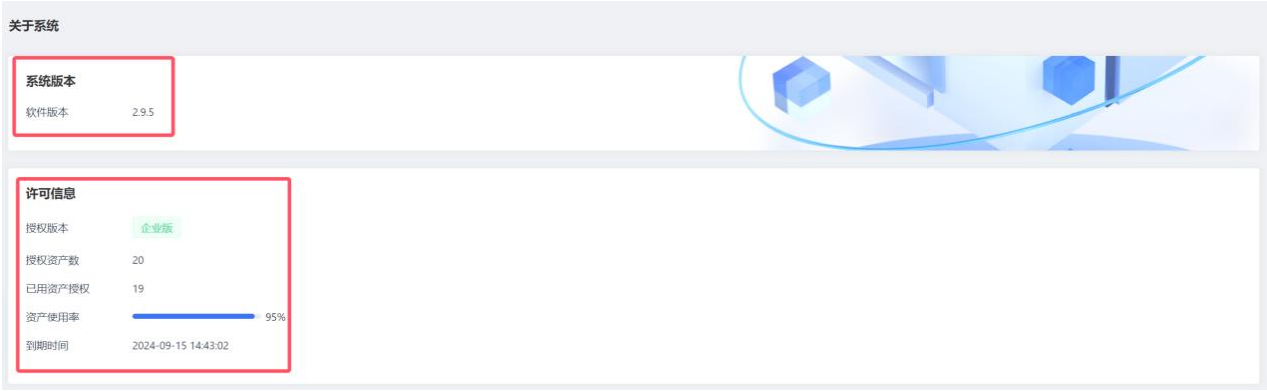


6.6.6 关于系统

1.登录云堡垒机（原生版）实例。

2.在左侧导航栏选择“系统管理 > 关于系统”，进入“关于系统”页面。

3.您可在“关于系统”页面查看堡垒机的系统版本及许可信息。



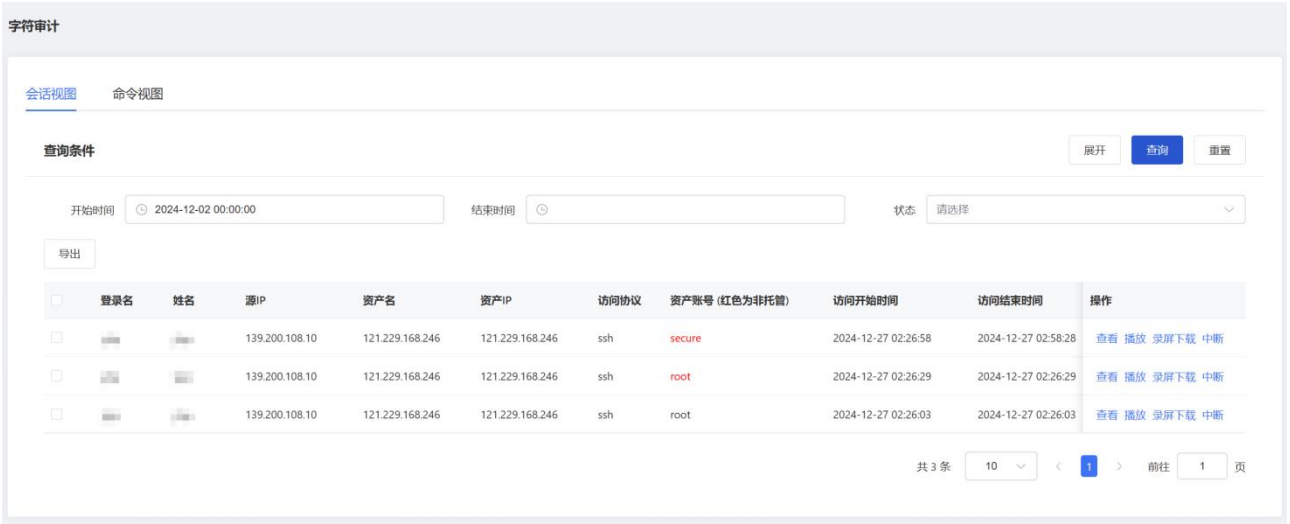
6.7 会话日志

6.7.1 字符审计

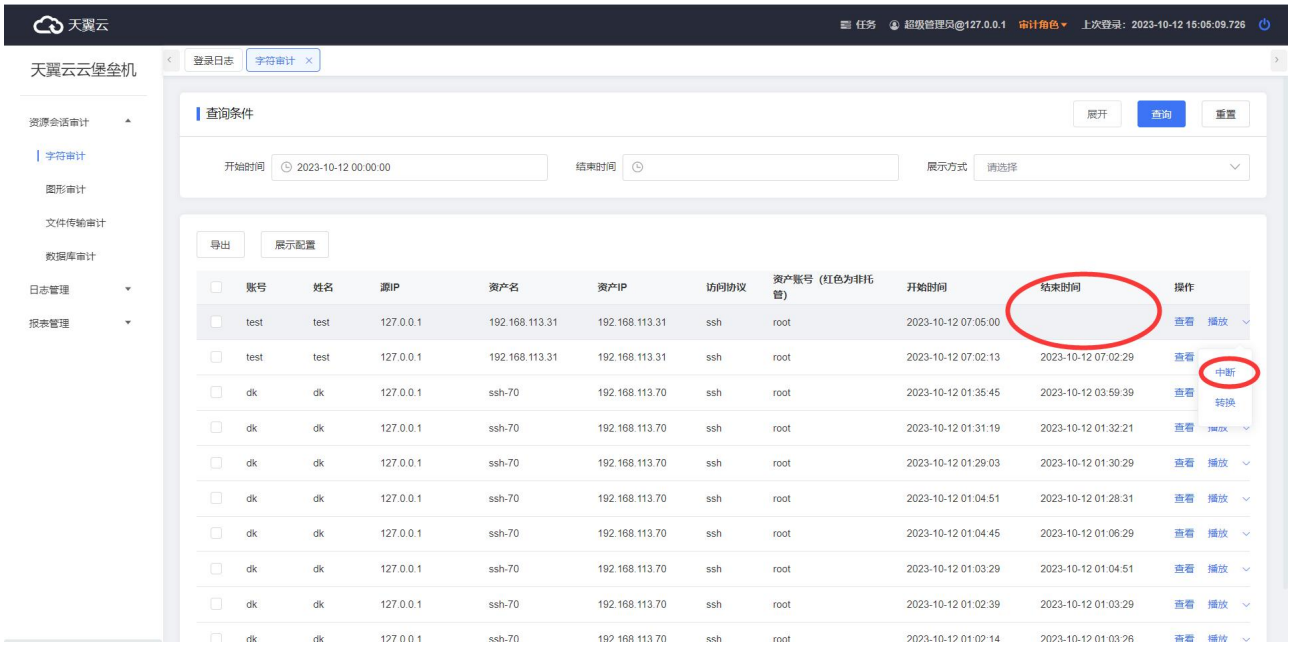
审计对象为授权的资产数据角色产生的字符访问会话（ssh、telnet），支持查看命令列表，回放访问录屏，中断活动会话，实时播放会话，下载会话审计文件。

1.管理员登录并切换至 审计角色，选择“会话日志 > 字符审计”。

2.单击“操作”列的“查看”可打开详细命令列表。



3.单击“操作”列的“播放”可使用浏览器在线播放会话。结束时间为空说明是活动会话，单击“播放”可实时观看会话，单击“中断”可中断该会话。

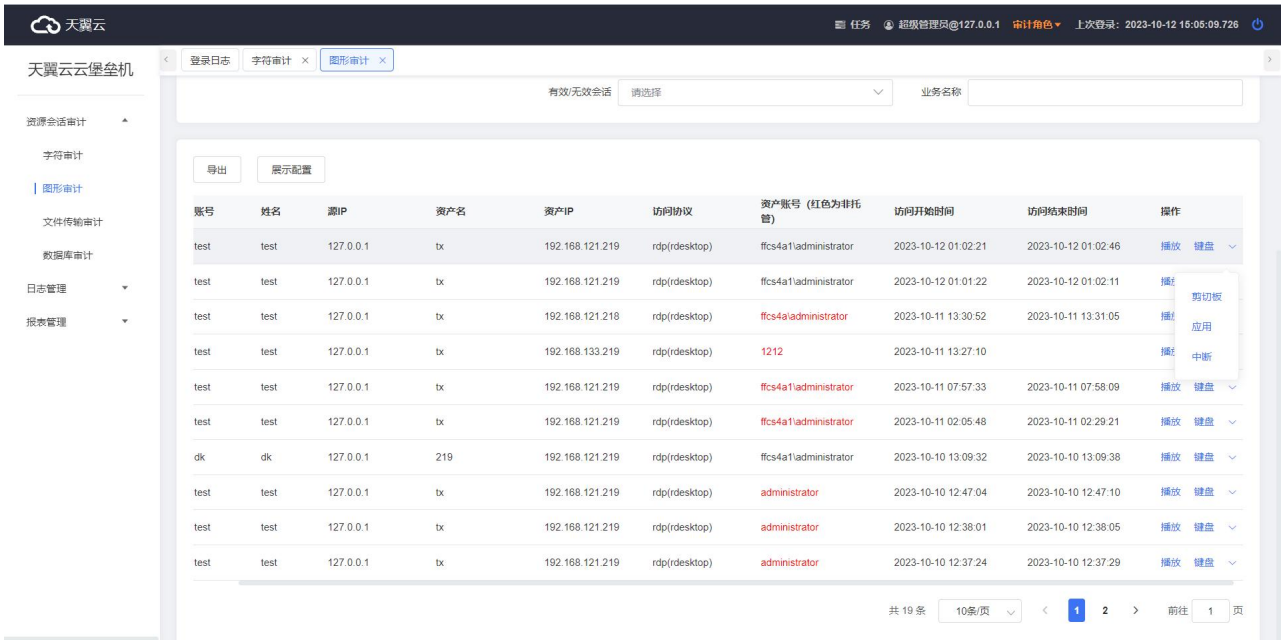


6.7.2 图形审计

可审计对象为授权的资产数据角色产生的图形访问会话，支持访问实时播放和回放、键盘记录、剪切板记录和中断会话。

1.管理员登录并切换至“审计角色”，选择“会话日志 > 图形审计”。

2.单击“操作”列的“键盘”或“更多 > 剪切板”可查看记录。结束时间为空说明是活动会话，单击“播放”可实时观看会话，单击“中断”可中断该会话。

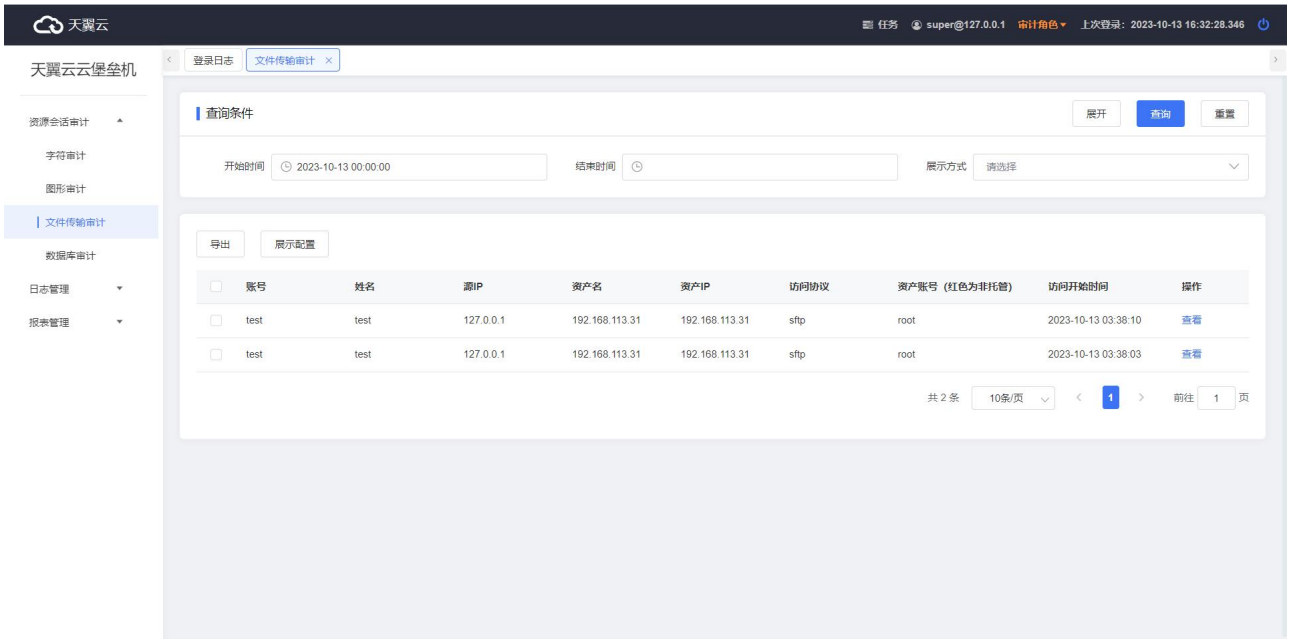


6.7.3 文件传输审计

可审计对象为授权的资产数据角色产生的文件传输会话（ftp、sftp）、账号数据角色产生的文件管理操作、个人目录文件操作，支持文件操作记录查看。

1.管理员登录并切换至“审计角色”，选择“会话日志 > 文件传输审计”。

2.单击“操作”列的“查看”可查看文件操作审计列表。

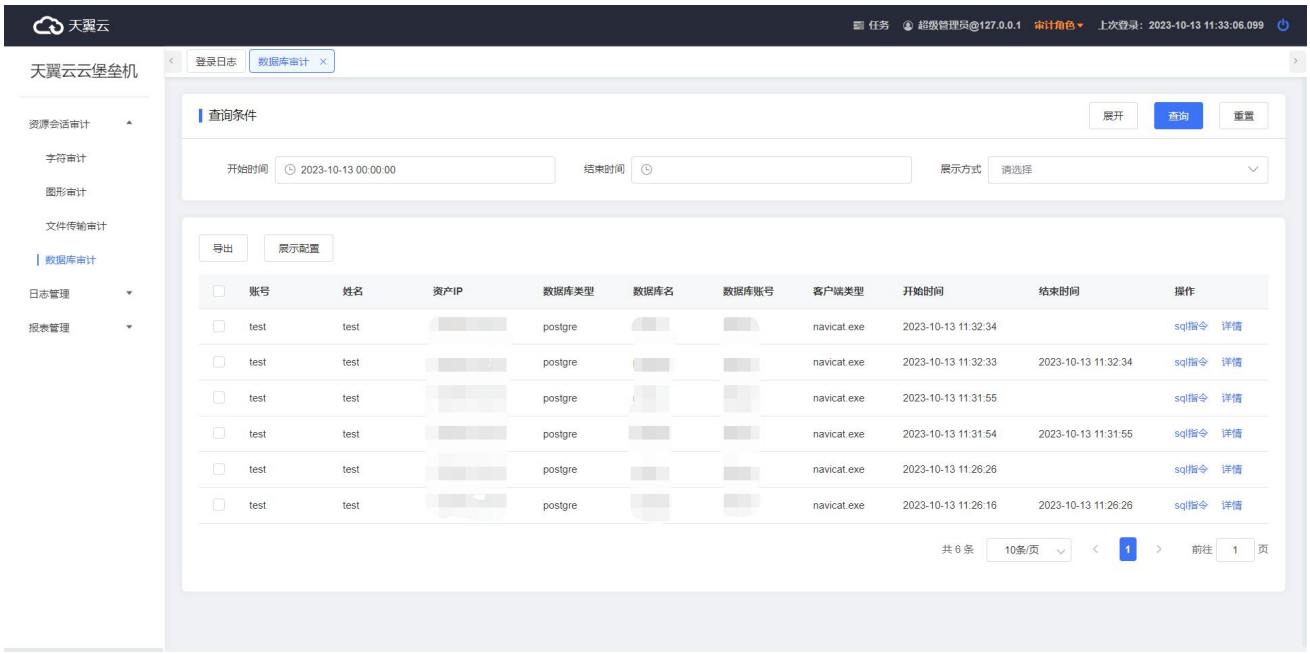


6.7.4 数据库审计

审计对象为授权的资产数据角色在本地初始化访问方式产生的数据库会话，支持查看 sql 指令，会话详情。

1.管理员登录并切换至“审计角色”，在左侧导航栏选择“会话日志 > 数据库审计”。

2.可直接查看数据库审计的相关内容。



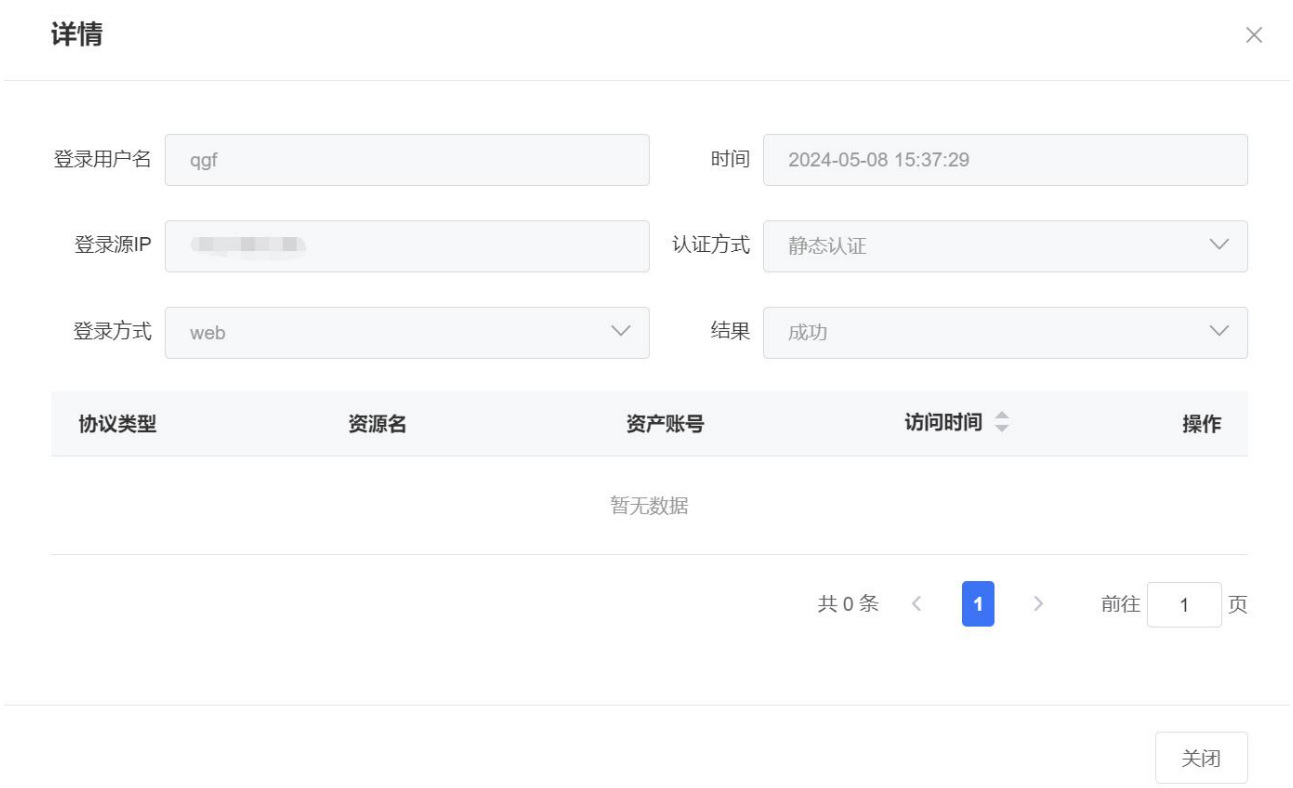
6.8 系统日志

6.8.1 登录日志审计

登录日志里 admin 可查看所有用户在登录堡垒机的详细记录，其他有授权用户可查看到授权的账号数据角色的操作记录。

1.管理员登录并切换至审计角色，在左侧导航栏选择“系统日志 > 登录日志审计”，审计范围包括登录成功与登录失败（密码错误、账号不存在等）的情况。

2.单击详情，可查看用户登录系统后访问资产的信息。



3.单击某条资产访问的详情，从更多维度展示该次访问会话的信息。

6.8.2 操作日志审计

操作日志里 admin 可查看所有用户在页面上的操作的详细记录，其他有授权用户可查看到授权的账号数据角色的操作记录。

1.管理员登录并切换至审计角色，在左侧导航栏选择“系统日志 > 操作日志审计”

2.单击“操作”列的“详情”可查看该条记录的详细信息。

7 最佳实践

7.1 数据库运维实名审计

背景

数据库资产作为企业各类经营业务数据的承载体，其重要性不言而喻。企业的核心业务数据往往是私密且敏感的，如何有效防护数据库资产安全，防止越权访问、违规操作以及进一步导致数据泄露等事件发生，成为企业在数据安全防护工程建设中重点关注的一项内容。传统数据库审计或数据库防火墙产品可审计及控制操作，但很难实名到自然人操作。

天翼云堡垒机支持数据库资产的运维管控，支持多种类型数据库运维，如 MySQL、PostgreSQL、Oracle 等协议类型数据库，支持自然人、数据库资源的操作关联，以满足不同用户使用需求。

数据库运维流程

管理员先将数据库纳入堡垒机进行管理，将资产访问权限分配给相关运维人员，运维人员登录系统，在资产访问页面触发“本地访问初始化”，系统会将运维访问策略下发到本地，初始化成功后，运维人员打开本地客户端连接资产进行访问运维。整个运维流程，从建立连接到资产中的操作详情，都将在堡垒机中实现管控审计。

前提条件

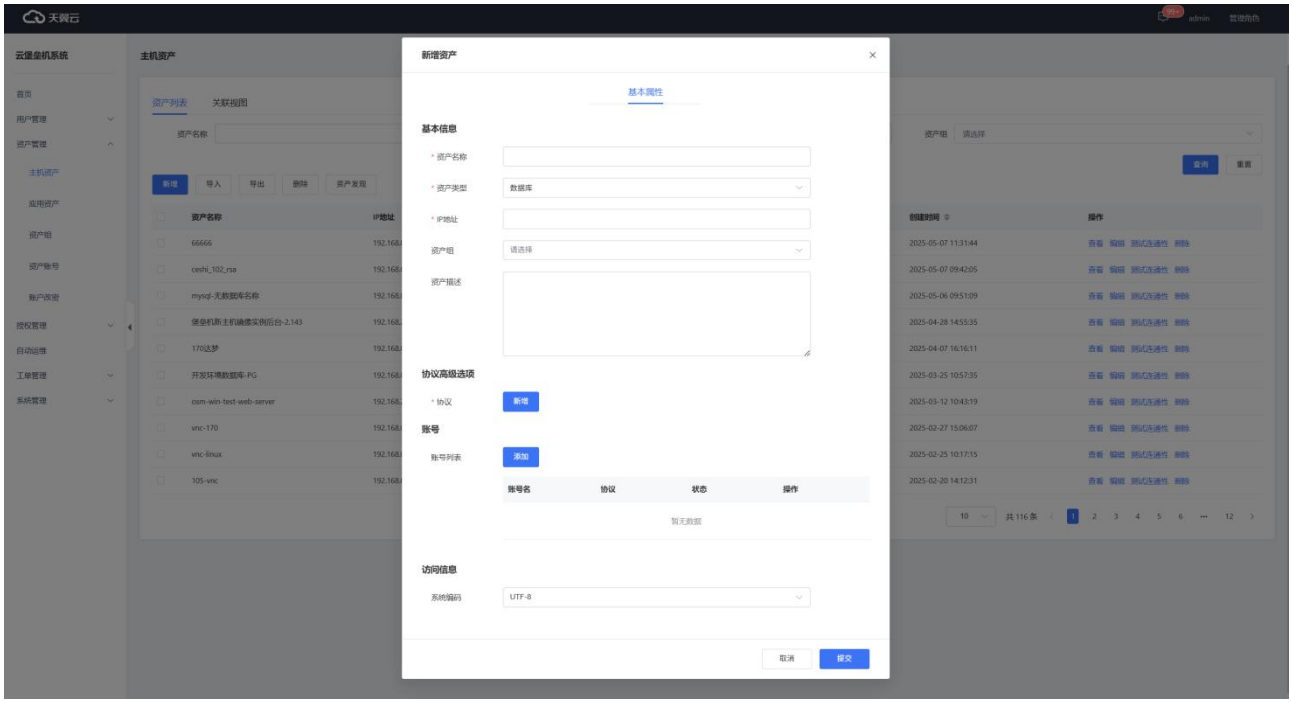
- 已在本地安装数据库访问客户端，如 Navicat、DBeaver 等。

- 已将数据库资产纳入堡垒机进行管理。
- 已获取相关资产访问权限。

操作步骤

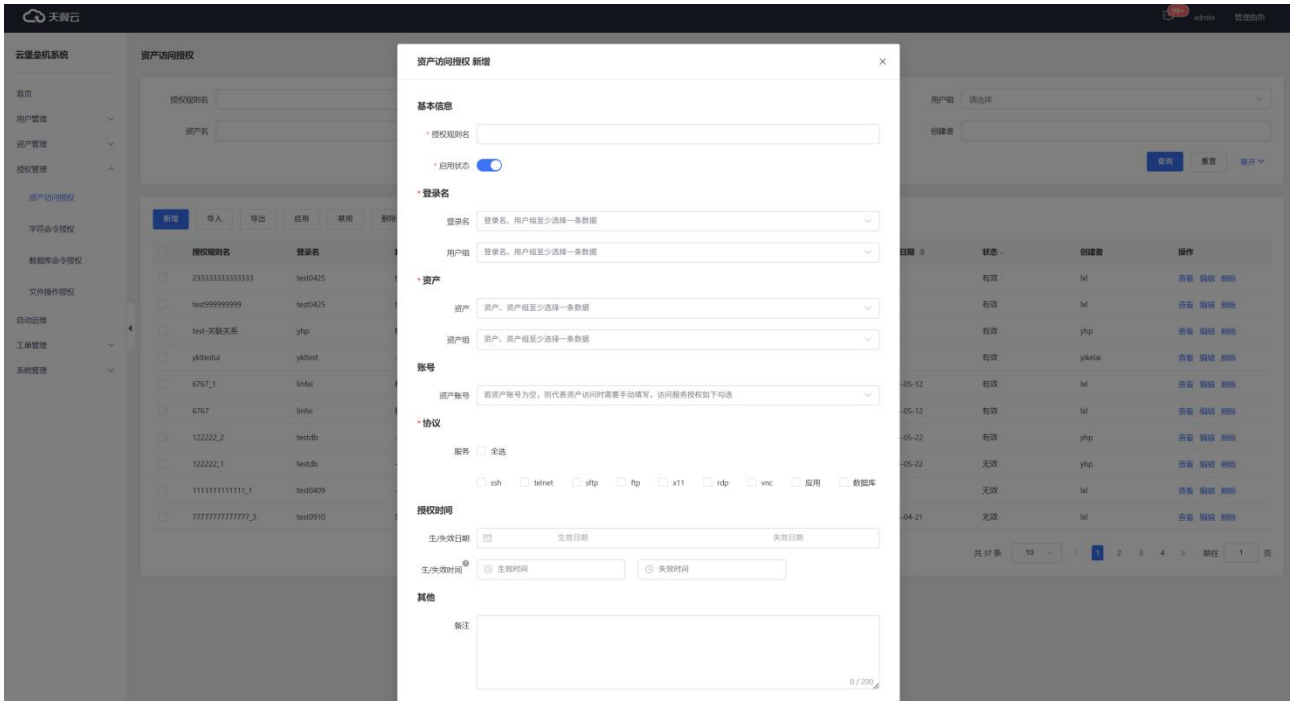
管理员将数据库资产纳入堡垒机进行管理

1. 管理员登录堡垒机。
2. 左侧菜单选择“资产管理>资产管理”。
3. 在资产管理界面点击“新增”，弹出资产信息输入窗口，按界面各项属性引导输入相关信息后提交即可。



管理员对数据库资产进行授权

1. 左侧菜单选择“授权管理》访问授权”，在基础设施访问授权标签页中点击“新增”后，切换至授权配置页。
2. 按授权引导属性配置运维人员（主账号）和数据库资产的关联关系，授权后，即表示配置中的运维人员有权限访问配置关联的资产。

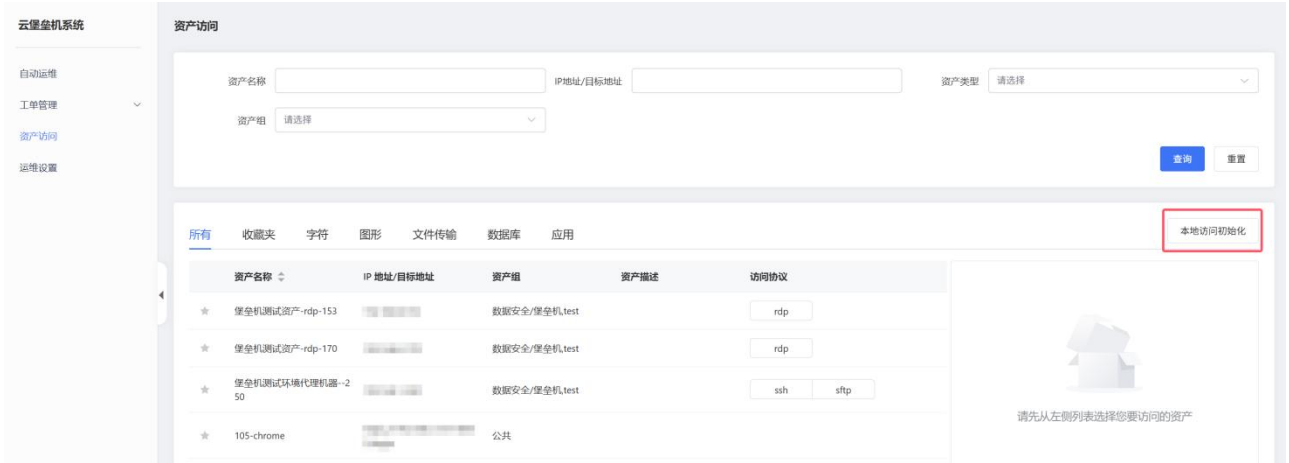


运维人员触发“本地访问初始化”进行运维

1. 运维人员登录堡垒机。

2. 左侧菜单选择“资产访问”。

3. 在资产访问页面，点击“本地访问初始化”后，系统后台将策略下发到本地，下发成功后将弹出提示。



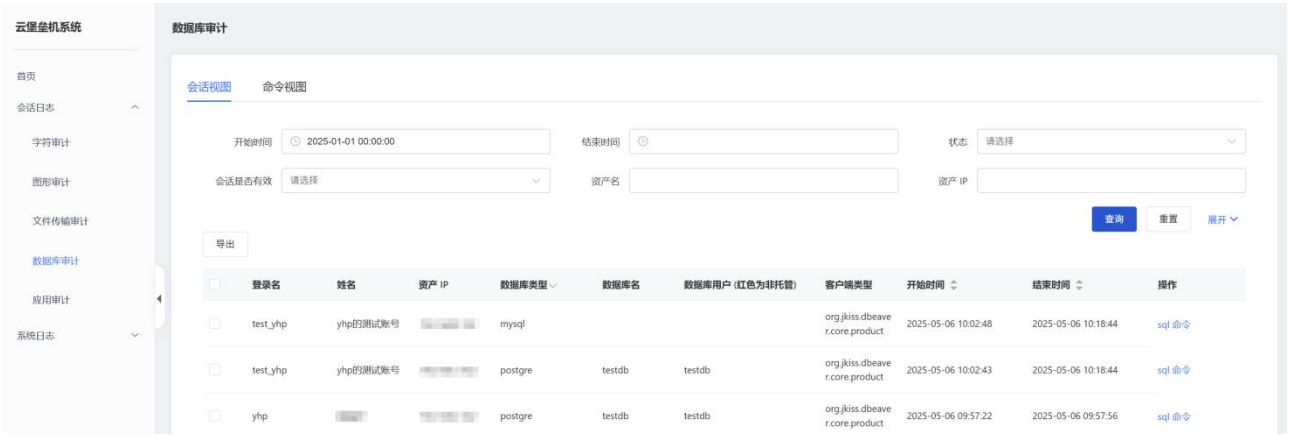
4. “本地访问初始化”成功后，运维人员即可按使用习惯打开本地客户端，输入资产地址、账户、密码连接资产进行运维。

数据库运维审计

1. 审计管理员登录堡垒机。

2. 左侧菜单选择“资源会话审计>数据库审计”。

3. 在数据库审计页面查看运维会话记录。



7.2 收敛资产运维暴露面

背景

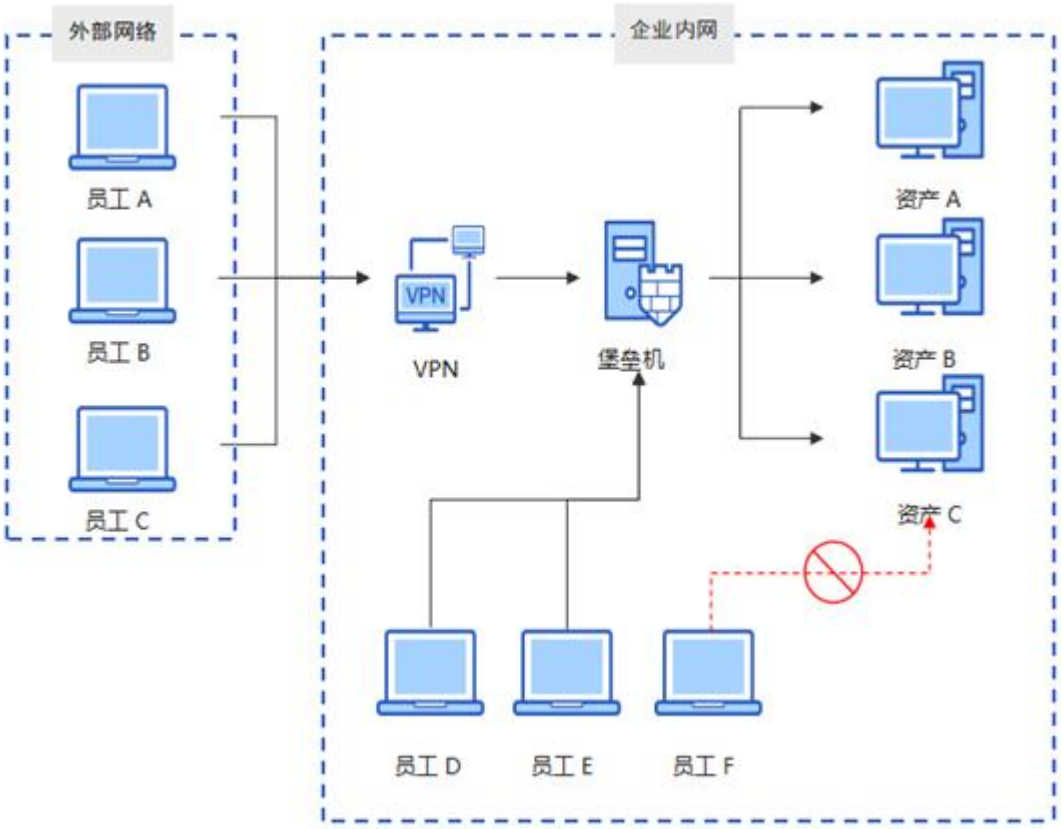
企业在经营过程中，随着业务的发展，资产规模也越来越大，各式各样的应用服务资源分布在不同的资产中，所有资源和应用都需要开放端口以提供不同的功能服务，随着时间的推移，资产的运维工作将变得越来越繁重，且难以梳理管控。近年来，网络攻击手段层出不穷，企业资产时刻面临各种网络攻击威胁，在这种安全形势下，收敛企业资产暴露面，从源头掐断各类探测连接的可能性，成为企业防护资产安全的有效手段之一。

天翼云支持纳管各种类型资产，如 Windows\Linux 等类型主机服务器、DB 协议类型数据库、安全设备、网络设备以及 WEB 应用类等资产。企业将各服务类型资产纳管至堡垒机，仅提供堡垒机访问入口，资产本身暴露面可实现隐藏，各类资产访问统一通过堡垒机进行单点登录，既实现将受攻击的范围从面缩小到点，也可实现资产及资产账户的统一管控，降低企业在资产运维管理工作中所需支付的成本。

解决方案

为解决企业资产暴露面过多的问题，堡垒机提供全网资产纳管能力，用户入网统一通过堡垒机入口，经过严密的身份认证以及权限验证后才允许用户进一步访问资产。在此基础上，为了解决用户登录资产问题，

堡垒机提供资产账户密码托管能力，可实现资源的快捷单点登录。



说明：

- 企业将资产纳入堡垒机进行管理维护
- 根据运维场景需求，企业可选择性的将资产账户托管至堡垒机，堡垒机提供定期修改资产账户密码功能，并在修改后发送相关消息告知管理员。
- 已纳入堡垒机的资产，企业陆续关闭其互联网访问入口，视情况关闭内网直连入口。

7.3 资产运维细粒度权限管控

背景

传统的权限网格比较粗放，围城内的大部分用户默认具有超范围的权限，外围用户通过 VPN 连接企业网络后，也默认具备“围城内用户”的身份和权限，越权访问、敏感操作比比皆是且无从管控，发生数据泄露等安全事故后也难以审计追溯具体详情。

天翼云堡垒机提供完善的用户访问授权和精细的操作权限管控，非授权用户无法访问指定资产，授权用户访问资产后无法执行未授权的指定敏感操作。

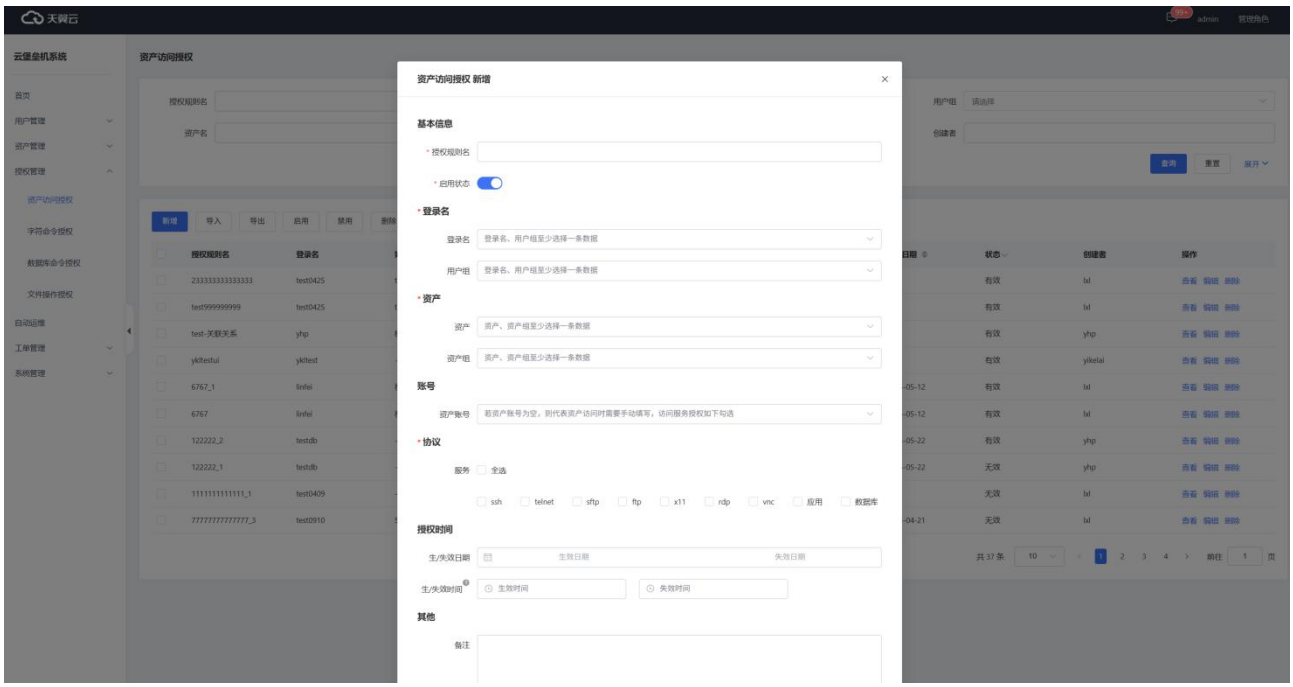
解决方案

一、访问授权

1、管理员登录堡垒机。

2、左侧菜单选择“授权管理>访问授权”。

3、选择“资产访问授权”标签页，点击“新增”切换至授权配置页，在基本属性模块支持配置访问的协议、访问的端口以及授权有效期；维度属性模块可配置主账号(组)和资产(组)以及资产从账号的关联关系。



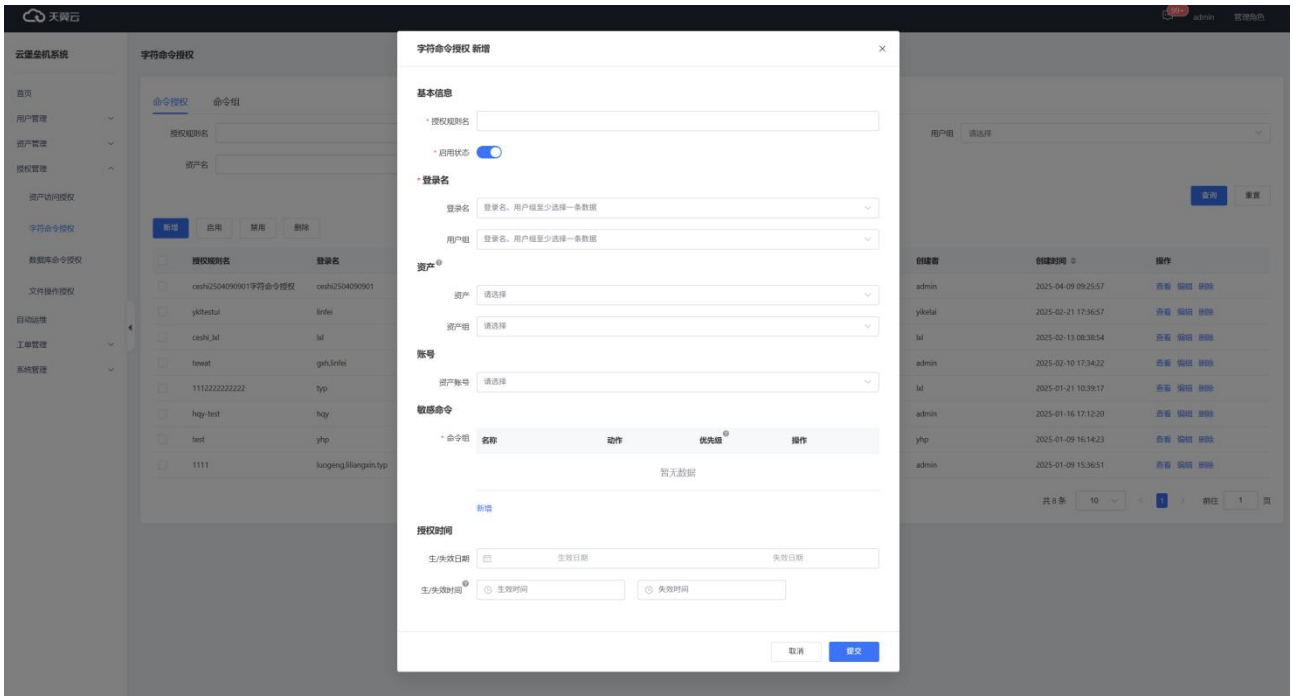
4、配置完成后，表示主账号(人员账号)可以在指定有效期内，使用指定的资产账户访问指定的资产。

二、命令授权

1、左侧菜单选择“授权管理>字符命令授权”。

2、在“命令组”标签页，点击【新增】，在属性中添加需要管控的命令集以及针对性的响应动作。支持以正则表达式的方式匹配相关命令。

3、在“命令授权”标签页，点击【新增】，填写指定用户和资产属性，选择创建的命令组提交。



在维度属性模块中，可配置命令管控策略需要关联生效的“用户--资产账户--资产”场景。

4、配置完成后，表示指定的用户使用指定的资产账户登录资产后，在资产上执行指定的命令时，将会触发策略中指定的响应动作。

5、文件传输配置原理同字符指令，可匹配具体的上传、下载等操作触发相关响应动作。

6、数据库指令配置原理同字符指令，可匹配 sql 类型、表名及条件去触发阻断或脱敏等动作。

8 常见问题

8.1 产品类

- **天翼云堡垒机支持纳管所有 region 上服务器吗?**

  取决于云堡垒机到服务器的网络是否可达。

  不同 region 的服务器，如果网络可达，云堡垒机可直接纳管。如果网络不可达，则需要分别开通天翼云堡垒机。

- **使用云堡垒机时需要配置哪些端口?**

  推荐开放 18443，18000，8765 端口的入方向规则，其他端口根据运维场景需要按需进行配置。云堡垒机使用端口用途详见下表：

端口	用途	说明
18443	门户端口，及 H5 运维端口	访问堡垒机门户页面时需开放该端口的入方向规则，（并可支持 H5 方式运维资产）
18000	字符资产访问端口	需通过堡垒机维护字符类协议资产时，需开放该端口的入方向规则

端口	用途	说明
19000	图形资产访问端口	需通过堡垒机使用 mstsc 客户端维护图形类协议资产时，需开放该端口的入方向规则
20000	图形资产访问端口	需通过堡垒机使用 vncview 客户端维护图形类协议资产时，需开放该端口的入方向规则
6003	数据库资产访问端口	需通过堡垒机维护数据库协议资产时，需开放该端口的入方向规则
8765	数据库资产访问端口	需通过堡垒机维护数据库协议资产时，需开放该端口的入方向规则

- **云堡垒机支持管理哪些数据库?**

数据库引擎	引擎版本
MySQL	5.5、5.6、5.7、8.0
PostgreSQL	10、11、12、13
Oracle	10g、11g、12c
DB2	10.5、11.5、12
达梦	V8
SQL Server	2016 企业版

数据库引擎	引擎版本
天翼云分布式关系型数据库（DRDS）	1.0 建议关联 MySQL5.7 和 8.0 版本

- **如何配置云堡垒机的安全组?**

  参考 3.1 步骤一：安全组策略设置。

- **云堡垒机是否支持纳管非天翼云服务器?**

  支持。

  云堡垒机提供绑定 EIP 功能，支持用户通过互联网远程直接运维资产。

  同时云堡垒机自身也提供私网接入地址，用户可以通过 vpn 远程拨入云堡垒机实例所在 vpc，然后使用云堡垒机实例私网地址接入运维内网资产。

- **租户是否能进入云堡垒机的操作系统?**

  不可进入。

  云堡垒机实例部署的服务器租户不可见，用户无法访问服务器操作系统，从而也避免进入操作系统破坏数据完整性，影响云堡垒机的安全合规。

- **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，资产数不以设备的数量计算，而是以所管理设备上资源的数量计算，一个设备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。

8.2 订购类

- **同一账号可以购买多个云堡垒机吗?**

  同一个账号在同一可用区内可购买多个云堡垒机，不同堡垒机之间数据完全独立。

- **云堡垒机到期后，还能继续使用吗?**

  云堡垒机到期后，系统处于冻结状态，无法继续登录堡垒机实例继续运维资源。云堡垒机到期超过 15 天，云堡垒机资源会自动销毁，数据无法恢复。

  说明

  - 天翼云在用户实例冻结前，以及资源销毁前将通过短信或邮件方式提醒用户。
  - 为避免因未及时续费而导致云堡垒机正常运行，建议在购买云堡垒机时开启自动续费。

- **若当前版本云堡垒机支持的资产数不够时，是否可以升级?**

  可以升级。若用户使用云堡垒机运维的资产数超过购买的云堡垒机资产规格时，您可以选择更高资产规格进行升级。

  操作方式参见 2.3 变更资产规格。

  注意

  - 仅支持同版本、同实例规格内变更资产规格，不支持跨版本变更或跨实例规格变更。
  - 标准版和企业版支持的最大资产规格数为 10000。

- **云堡垒机变更规格可以降低资产规格吗?**

  不支持。

  如需降低当前规格，你可以先备份相关数据后，退订当前云堡垒机，再重新购买降低规格的云堡垒机。

- **如果需要纳管的资产数小于标准的售卖资产规格该如何选择规格?**

  如果堡垒机购买页没有与您资产数量一致的套餐规格，您需要选择比现有资产数量更大的套餐规格以保证可以统一运维。

例如，您现在有 15 资产，则您需要选购 20 资产套餐规格。

- **订购时如何配置 VPC 信息，堡垒机实例 VPC 信息可以修改吗?**

  在购买云堡垒机实例时，为降低网络时延，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。堡垒机实例的 VPC 信息在购买时指定，后续不能修改。

- **如何选择云堡垒机实例区域和可用区?**

  选择堡垒机实例区域和可用区的选择通常根据所需要运维的服务器、数据库等资产的区域和可用区的距离来确定，一般根据就近原则进行选择。

  如您要运维的服务器或数据库资产在上海，那么您可以选择华东区域，这样可以减少访问服务的网络时延，提高访问速度。

8.3 操作类

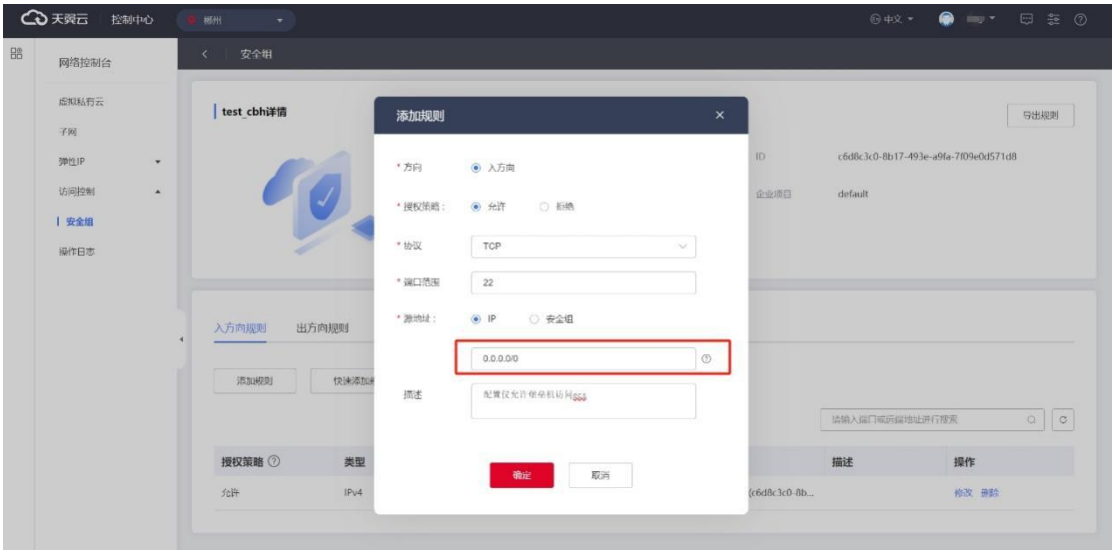
- **如何防止云堡垒机运维的服务器被绕过?**

  云堡垒机没有防绕过的功能，运维用户只要掌握服务器账号密码，即可直接登录服务器并运维。

  为避免云堡垒机被绕过，需要设置服务器安全组，配置入方向仅对云堡垒机 IP 地址开放，拒绝其他地址访问，实现只通过云堡垒机登录的目的。

  操作步骤

  1. 登录管理控制台。
  2. 在系统首页，单击“网络 > 弹性 ip”。
  3. 在左侧导航树选择“访问控制 > 安全组”。
  4. 在安全组界面，单击操作列的“配置规则”，进入安全组详情界面。
  5. 在安全组详情界面，单击“添加规则”，弹出添加规则窗口，规则配置中原地址配置云堡垒机的 IP 地址。



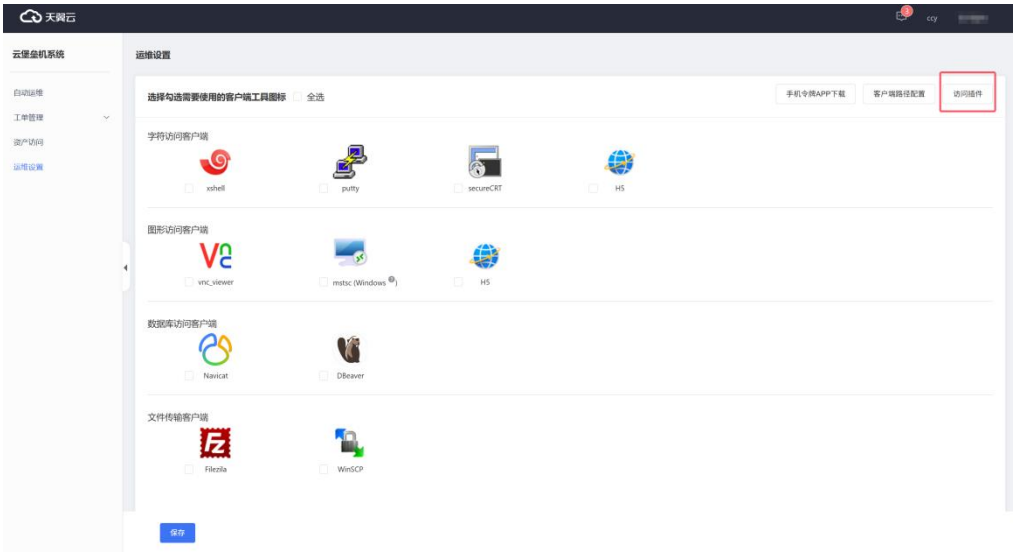
- **访问时页面提示“请确认是否安装访问插件”如何处理?**

运维用户登录云堡垒机控制台后，窗口弹出“若访问失败，请确认是否安装访问插件”，这说明用户第一次在当前终端还未安装云堡垒机客户端插件，需要下载并安装。

云堡垒机客户端插件是天翼云堡垒机产品重要组成部分之一，支撑客户端工具运维和 web 网页运维代理、资源免密单点登录登重要功能。用户需要点击运维设置-访问插件 按钮下载并安装插件。

操作步骤

1. 运维用户登录云堡垒机实例控制台。
2. 访问控制台运维设置-访问插件，点击访问插件按钮下载客户端插件。



3. 下载完成后，安装客户端插件。

4. 设置运维客户端本地安装路径，点击运维-客户端路径配置，配置您的运维工具本地路径。

   配置完成后，下次你登录云堡垒机后就可直接点击客户端工具图标，直接开始运维你权限内的资产。

- **登录提示“您的账户已经被锁定,请自助解锁或联系管理员”如何处理?**

账号密码被锁定主要有以下几种情况：

1. 忘记密码，连续输错 N 次密码后账号自动锁定。
2. 账号、密码超过有效期，自动锁定。
3. 账号空闲超过阈值未登录系统。
4. 管理员主动锁定。

忘记密码

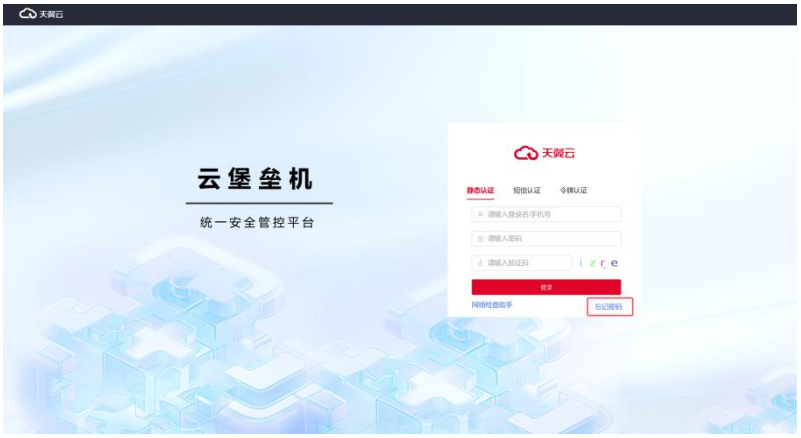
在云堡垒机实例登录页面点击忘记密码，通过注册邮箱重置密码，解锁账号。

注意

忘记密码自助解锁功能，需要用户在注册时有绑定邮箱地址，若未绑定邮箱地址，只能联系管理员解锁。

操作步骤

1. 进入云堡垒机登录页，点击忘记密码。



2. 输入用户名、邮箱等信息，验证用户身份。

3. 输入新登录密码，点击确定后，密码重置成功。

密码过期锁定

在云堡垒机实例登录页面点击自助解锁，通过注册邮箱解锁账号。

注意

密码过期自助解锁功能，需要用户在注册时有绑定邮箱地址，若未绑定邮箱地址，只能联系管理员解锁。

操作步骤

1. 进入云堡垒机登录页，点击自助解锁链接。

2. 进入自助解锁功能后，输入用户名、邮箱和动态验证码，验证用户身份。

3. 输入更新后的密码，注意输入密码需要符合密码安全策略，点击确认。

4. 解锁成功。

其他原因账号被锁定

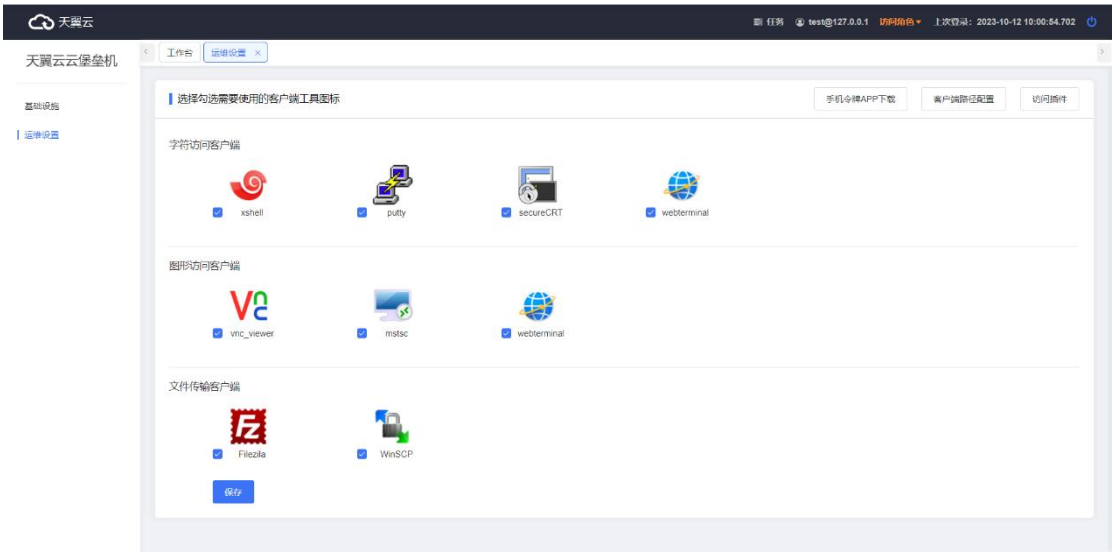
联系管理员解锁。管理员登入云堡垒机管理后台，在账号管理中可解锁用户账号、更改密码。

- **无法正常启用客户端运维工具运维资产**

无法正常启用客户端运维工具运维资产一般是因为未下载或未在云堡垒机系统中配置需要使用的客户端工具，用户可根据以下步骤排查。

1、确认是否配置需要使用的客户端工具

打开运维设置，勾选要调用的客户端，保存配置。



2、确认是否已正确安装并配置客户端工具。

云堡垒机不提供 Xshell、vnc 等客户端运维工具下载，用户需要自行去官网下载安装需要使用的软件。

Windows 的客户端路径配置，需要将软件启动程序文件路径严格配置到运维设置-客户端路径配置中。

例如：Xshell 默认安装路径 C:\Program Files (x86)\NetSarang\Xshell 7\Xshell.exe，其他的软件或者安装到了其他的路径，根据自己的实际情况配置即可。

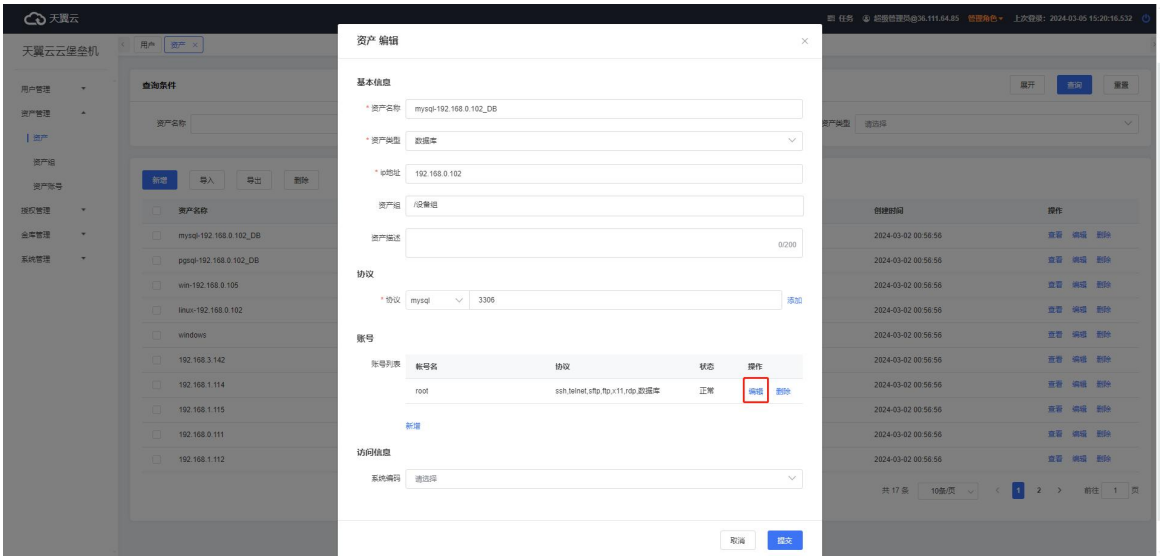
Mac OS 不需要客户都按照路径配置，使用的应用安装在应用程序（Application）路径中就可以，例如下图 FileZilla。

- **访问资产提示“登录设备失败，设备账号或密码错误”，怎么解决?**

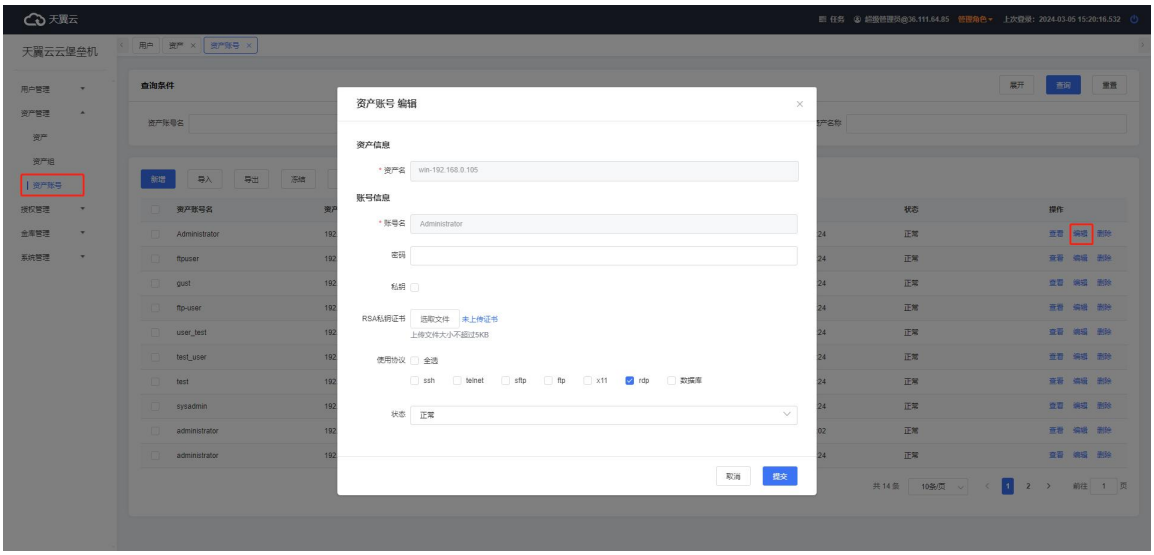
  访问资产提示“登录设备失败，设备账号或密码错误”，如果使用托管的账号密码，则需联系资产管理员，确认托管的账号和密码是否正确。资产管理员需要将正确的资产账号和密码重新添加到资产，运维用户才能正常登录设备运维。

  操作步骤

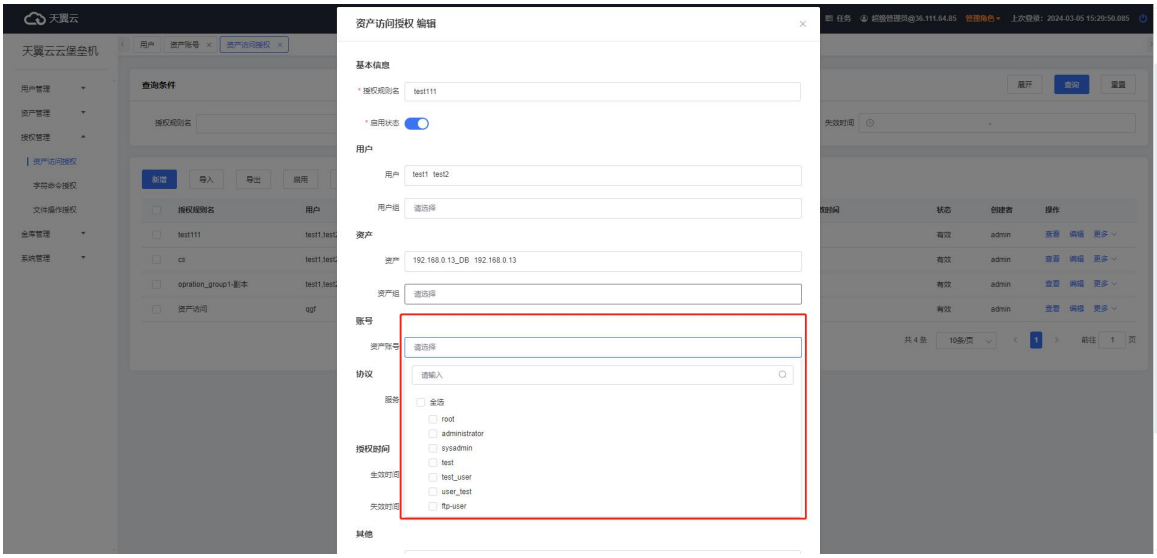
  1. 管理员登录云堡垒机实例控制台，访问角色切换为管理角色。
  2. 进入资产管理-资产账号管理，按资产 IP 或资产名称搜索需要修改账号或密码的资产。
  3. 点击资产操作栏编辑链接，编辑资产账号。



  4. 更新资产账号、密码及应用的协议。



5. 更新资产账号、密码及应用的协议。



- **运维用户客户端无法访问用户资产如何处理?**

运维用户客户端无法访问服务器、数据库等用户资产需要排查客户端到云堡垒机以及云堡垒机到运维资产的网络通路，重点排查安全组配置。

注意：

请先确认以下配置均已正确配置：

1. 运维终端已正确安装访问插件，并配置访问路径。
2. 用户拥有访问及运维资产的授权。

排查步骤

1. 检查客户端到云堡垒机网络是否能连通。

   在您的客户端使用 ping 命令测试客户端与堡垒机的网络是否连通，如果连接失败，请您登录堡垒机控制台，查看堡垒机 EIP 是否正常，检查云堡垒机实例安全组策略是否正确配置，确认 IP 和端口是否正确开放，具体请查阅 安全策略配置方法。

2. 检查堡垒机到运维资产网络是否能连通。

   检查云堡垒机实例到运维资产的网络和端口是否开放，需要检查运维资产所属安全组的安全端口访问策略限制，是否允许云堡垒机实例访问运维资产。