

云堡垒机（原生版）

目录

产品介绍

产品定义.....	2
功能特性.....	3
产品优势.....	5
应用场景.....	5
使用限制.....	6
术语解释.....	8

计费说明

计费说明（一类节点）.....	10
计费说明（二类节点）.....	21

快速入门

安全组策略设置.....	30
登录云堡垒机实例.....	31
新增账号和资产.....	33
配置运维权限.....	37
资产运维.....	37
运维审计.....	39

用户指南

实例管理.....	42
管理员手册.....	58
运维使用手册.....	123

最佳实践

数据库运维实名审计.....	133
收敛资产运维暴露面.....	136
资产运维细粒度权限管控.....	137

常见问题

产品类.....	139
订购类.....	140
操作类.....	142

产品介绍

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。

产品介绍

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。

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	√	√	×
资产管理	主机管理	√	√	√
	数据库管理	×	√	√
	自动导入天翼云上ECS资产	√	√	×
	应用管理	×	√	√
	资产组管理	√	√	√
	资产账密管理	√	√	√
	账户改密	√	√	√
用户管理	双因子认证	√	√	√
	用户管理	√	√	√
	用户组管理	√	√	√
	账号安全策略	√	√	√
授权管理	资产访问授权	√	√	√
	字符命令授权	√	√	√

产品介绍

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）
	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、Filezilla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	×	√	√

产品介绍

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）
	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	√	√	√

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。

应用场景

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。

产品介绍

- 小规格成本更低：按设备数包年包月，最低支持20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。

中大型企业多人运维场景

场景说明

政务、金融及大型央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、资产账密管理、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。

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。

Windows服务器版本：Windows Server 2012、2016。

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
金仓(Kingbase)	V8、V9

产品介绍

数据库引擎	引擎版本
万里(GreatSQL)	8.4.4-4
SQL Server	2016企业版
天翼云分布式关系型数据库（DRDS）	1.0 说明 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	Edge	95及以上版本
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。	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	Winscp	5及以上版本
	Filezilla	3及以上版本
数据库运维	Navicat	11、12、15、16、17
	DBeaver	22、23、24
	HeidiSQL	10.0及以上版本
	说明 需要自行下载客户端并使用。	

产品介绍

登录方式	支持的客户端	版本
	PL/SQL Developer 说明 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

术语解释

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。

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。

产品介绍

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。

计费说明

计费说明（一类节点）

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。
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。

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

计费说明

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
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。

计费说明

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。

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。

- 主备版默认提供的EIP带宽如下表所示。如需解绑EIP，请提工单联系技术支持处理。

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)	EIP带宽	主机规格
10资产	10并发上限	1300	2040	5M	CPU: 2核, 内存: 4GB, 系统盘: 40GB, 数据盘: 300GB
20资产	20并发上限	1700	2560	5M	CPU: 2核, 内存: 8GB, 系统盘: 50GB, 数据盘: 300GB
50资产	50并发上限	3040	5200	10M	CPU: 4核, 内存: 16GB, 系统盘: 50GB, 数据盘: 500GB
100资产	100并发上限	5040	9200	10M	CPU: 8核, 内存: 32GB, 系统盘: 50GB, 数据盘: 800GB
200资产	200并发上限	7040	12400	10M	CPU: 8核, 内存: 32GB, 系统盘: 50GB, 数据盘: 800GB
500资产	500并发上限	10560	18400	20M	CPU: 12核, 内存: 48GB, 系统盘: 50GB, 数据盘: 2TB
1000资产	1000并发上限	21560	28340	20M	CPU: 16核, 内存: 64GB, 系统盘: 50GB, 数据盘: 2TB
2000资产	2000并发上限	27560	34340	20M	CPU: 16核, 内存: 128GB, 系统盘: 50GB, 数据盘: 2TB
5000资产	2000并发上限	36000	54000	20M	CPU: 24核, 内存: 192GB, 系统盘: 50GB, 数据盘: 4TB
10000资产	2000并发上限	48000	72000	20M	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。

计费说明

计费项	标准价格-主备版	计费单位
存储扩容	1000	元/月/TB

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。
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。 <ul style="list-style-type: none">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。

购买步骤

- 登录管理控制台。
- 选择“安全 > 云堡垒机（原生版）”，进入云堡垒机实例管理页面。
- 单击右上角的“购买堡垒机”，进入产品订购页。
- 配置“云堡垒机实例”相关参数，参数说明如下。

参数	说明
计费模式	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。
地域/可用区	选择云堡垒机实例应用区域，即提供云堡垒机服务的区域。建议根据待管理ECS、RDS等服务器上资源的区域选择，可以降低网络时延、提高访问速度。

计费说明

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 。
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 <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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	根据您的业务自身的需求选择需要扩容的数据盘大小。

计费说明

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。

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、增加数据盘容量（即版本、资产规格、存储扩容）。

支持跨版本变更实例的资产规格。例如，由标准版10资产升级到企业版20资产。

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。
- 仅支持云堡垒机升级，暂不支持降级。
- 不支持升级实例类型（不支持由单机版升级到主备版）。若需要升级实例类型，请先备份相关数据，退订单机版后重新订购主备版。

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“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：

计费说明

- 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： $(1280-650) \times 3 \times 0.85 = 1606.5$ 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“更多 > 关闭实例”，待实例状态变更为“已关机”后，单击“更多 > 变更规格”，跳转到“变更规格”页面。



计费说明

4. 选择需变更的规格，可以变更“版本”、“资产规格”、“存储扩容”。

说明

如果当前要升级版本/资产规格和存储扩容，但此前没有订购存储扩容，则执行：

- 升级版本/资产规格。
- 升级存储扩容。

当前配置

实例名称	osm-0ypr	地域/可用区	华东1/可用区1
实例规格	10资产企业版	并发	10
计费模式	包月		

性能规格

版本 企业版
适用于对数据库有运维、审计需求的企业。

资产规格 10资产 20资产 50资产 100资产 200资产
500资产 2000资产 5000资产

存储扩容 0TB 5TB 10TB 15TB 20TB 25TB

* 协议 我已阅读并同意 [《天翼云云堡垒机（原生版）服务协议》](#) [《隐私政策声明》](#)

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。

6. 变更完成后，实例状态恢复为“已关机”。单击“启动”，启动实例。

待实例运行状态变为“运行中”，即可正常使用云堡垒机。

续订实例

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。

计费说明

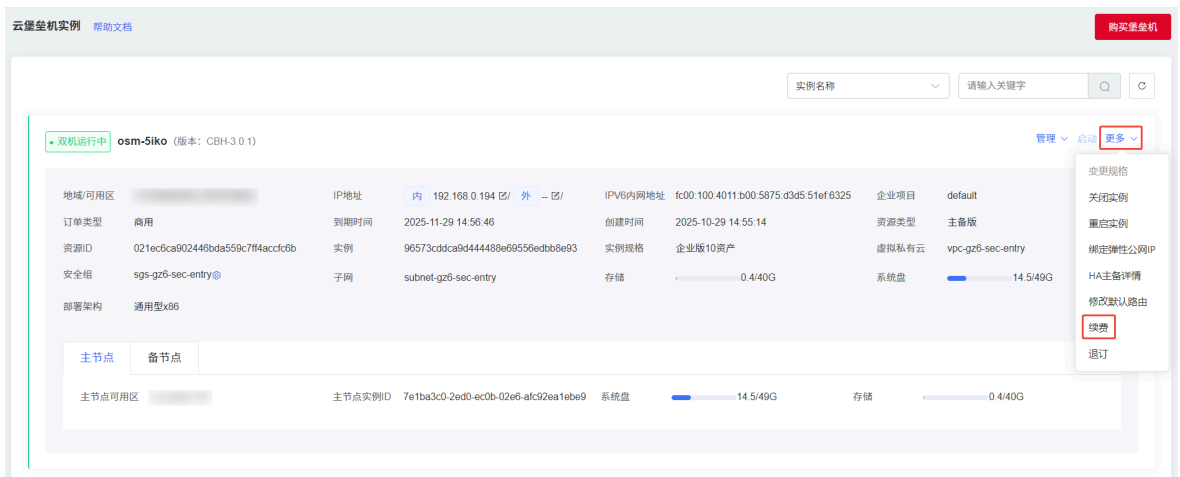
- 在云堡垒机到期后，若未及时续费，则进入“保留期”，不能登录云堡垒机系统。“保留期”为15天，到期仍未续订或充值，存储在云堡垒机中的数据将被删除、资源将被释放。

前提条件

已获取控制台的登录账号与密码。

操作步骤

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



- 根据需要选择续费时长。



配置费用 ¥

去支付

- 单击“去支付”，在支付页面完成付款。

计费说明

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。

管理中心续费

登录天翼云官网，进入管理中心，选择“订单管理 > 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。

续订管理

1. 支持自动续订的产品范围详见 [帮助文档](#)
2. 如果在自动续订前已完成人工续订，则同一周期内不会再自动续订。
3. 对于7天内到期的资源，或已到期的资源，不支持设置修改自动续订。
4. 对于设置了自动续订，且7天内到期的资源，如果用户手动修改自动续订周期，关闭自动续订、转按量计费，可能会因当期自动续订已完成导致当前资源未生效的情况。
5. 非续费订购但具有绑定续费关系的资源，需要分别开通自动续订，例如仅对云堡垒机设置自动续订，该堡垒机所挂载的云主机到期冻结后，可能导致整体服务不可用。
6. 若资源到期后续费，续费周期自资源续订解冻开始，计算新的服务有效期。

到期时间: 全部时间 | 7天内到期 | 15天内到期 | 30天内到期 | 未到期 | 已到期 | 自定义

筛选: 产品名称: 云堡垒机 (原生版) | 资源ID: 请输入资源ID或控制台资源ID | 订单号: 请输入订单号 | 搜索 | 导出

手动续订 (6) | 自动续订 | 到期转按需 | 到期不续订

批量续订 | 开通自动续订 | 到期转按需 | 统一到期日 | 到期不续订

产品名称	资源ID / 订单号	资源池	资源状态	资源名称	企业项目	倒计时	续订周期	订购方式	时间	操作
云堡垒机 (原生版)			有效	osm-rf4j	default	26 天	--	包周期	创建 2025-10-11 15:52: 到期 2025-11-11 15:52:	手动续订 开通自动续订 到期不续订
云堡垒机 (原生版)			有效	osm-00m4	default	8 天	--	包周期	创建 2025-09-25 09:48: 到期 2025-10-25 09:48:	手动续订 开通自动续订 到期不续订

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。

退订实例

前提条件

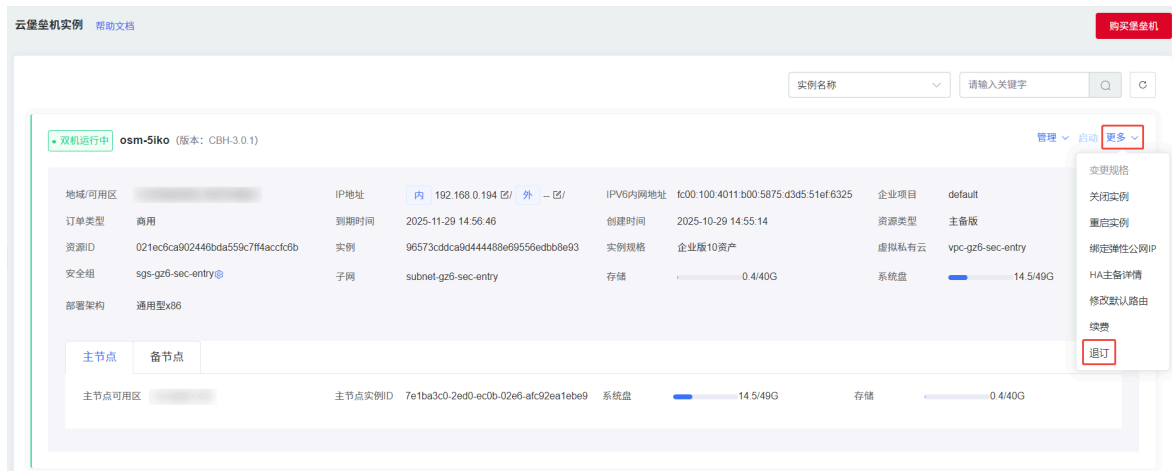
- 已获取管理控制台的登录账号与密码。
- 已使用的云堡垒机，需停止系统所有操作，解绑EIP。

操作步骤

- 登录管理控制台。
- 选择“安全 > 云堡垒机（原生版）”，进入云堡垒机实例管理页面。

计费说明

3. 选择待退订的实例，单击所在行“操作”列的“更多 > 退订”。



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。



计费说明

计费说明（二类节点）

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)	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	860	2核	8GB	40GB	300GB
高级版	20资产	20并发上限	999	2核	8GB	50GB	300GB
高级版	50资产	50并发上限	1888	4核	16GB	50GB	500GB
高级版	100资产	100并发上限	2999	8核	32GB	50GB	800GB
高级版	200资产	200并发上限	4350	8核	32GB	50GB	800GB
高级版	500资产	500并发上限	6230	12核	48GB	50GB	2048GB
高级版	1000资产	1000并发上限	11100	16核	64GB	50GB	2048GB
高级版	2000资产	2000并发上限	14000	16核	128GB	50GB	2048GB
高级版	5000资产	2000并发上限	20000	24核	192GB	50GB	4096GB
高级版	10000资产	2000并发上限	29550	32核	192GB	50GB	4096GB

计费说明

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
----	----

计费说明

虚拟私有云	<p>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。</p> <p>注意</p> <ul style="list-style-type: none"> 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	<p>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。</p> <p>说明</p> <ul style="list-style-type: none"> 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	<p>选择当前VPC内子网。</p> <p>说明</p> <p>子网需在VPC的网段内。</p>
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	300GB
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

计费说明

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	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。

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

- 只有2.0及以上版本的堡垒机支持提升规格。
- 仅支持云堡垒机升级，暂不支持降级。

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。



计费说明

4. 选择需变更的“资产规格”。

当前配置

实例名称	osm-c-1757350861641	地域/可用区	重庆/cn-cq1a
实例规格	10资产企业版	并发	10
计费模式	包月		

性能规格

版本 高级版
适用于对数据库有运维、审计需求的企业。

资产规格 10资产 20资产 50资产 100资产 200资产
500资产 1000资产 2000资产 5000资产

●当前资产所需的主机规格为 (CPU: 2核; 内存: 4G; 系统盘: 40G; 数据盘: 300G), 请同时修改所在机器的规格

* 协议 我已阅读并同意 [《天翼云云堡垒机（原生版）服务协议》](#) [《隐私政策声明》](#)

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](#)。

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。

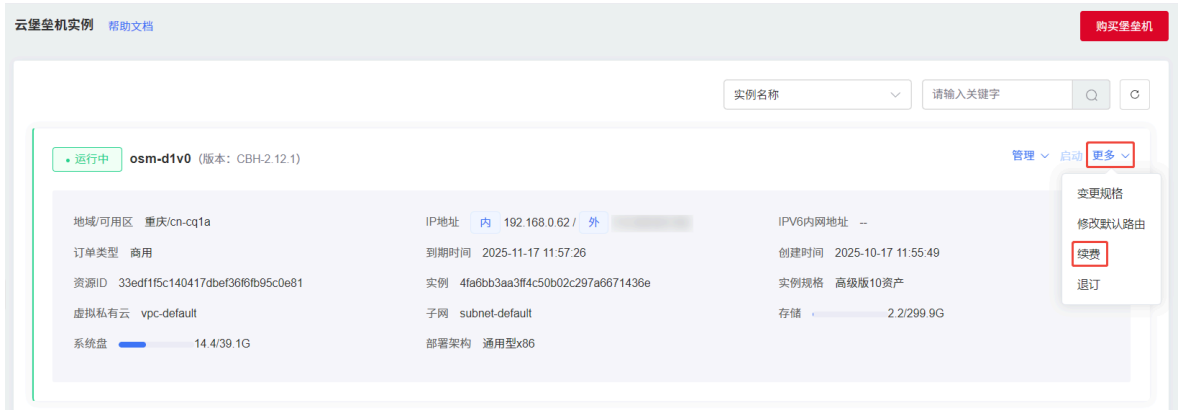
前提条件

已获取控制台的登录账号与密码。

计费说明

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。



配置费用 **¥** 去支付

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。

计费说明

费用中心

- 总览
- 订单管理
- 我的订单
- 待支付订单
- 续订管理**
- 退订管理
- 导出记录
- 账单管理
- 资金管理
- 账单管理
- 资源管理
- 发票管理
- 成本管理
- 合同管理

续订管理

1. 支持自动续订的产品范围详见 [帮助文档](#)。
2. 如果在自动续订前已完成人工续订，则同一周期内不会再自动续订。
3. 对于7天内到期的资源，或已到期的资源，不支持设置/修改自动续订。
4. 对于设置了自动续订，且10天内到期的资源，如果用户尝试修改自动续订周期、关闭自动续订、转按需计费，可能会因当期自动续订已完成导致当前变更未生效的情况。
5. 非成簇订购但具有绑定或挂载关系的资源，需要分别开通自动续订，例如仅对云硬盘设置自动续订，该硬盘所挂载的云主机到期冻结后，可能导致整体服务不可用。
6. 若资源到期后续费，续费周期自资源续订解冻开始，计算新的服务有效期。

到期时间：全部时间 | 7天内到期 | 15天内到期 | 30天内到期 | 未到期 | 已到期 | 自定义

筛选：产品名称 **云堡垒机（原生版）** | 资源ID | 请输入资源ID或控制台资源ID | 订单号 | 请输入订单号 | 搜索 | 导出

手动续订 (7) | 自动续订 | 到期转按需 | 到期不续订

批量续订 | 开通自动续订 | 到期转按需 | 统一到期日 | 到期不续订

<input type="checkbox"/>	产品名称	资源ID / 订单号	资源池	资源状态	资源名称	企业项目	倒计时	续订周期	订购方式	操作	
>	<input type="checkbox"/>	云堡垒机（原生版）	33edf1f5c140417dbef36f6b95c0e81 (20251017115517708329)	重庆	有效	osm-d1v0	default	31天	--	包周期	手动续订 开通自动续订 到期不续订

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

- 登录管理控制台。
- 选择“安全 > 云堡垒机（原生版）”，进入云堡垒机实例管理页面。
- 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。

云堡垒机实例

实例名称 请输入关键字

运行中 **osm-d1v0** (版本: CBH-2.12.1) 管理 启动 **更多**

地域/可用区	重庆/cn-cq1a	IP地址	内 192.168.0.62 / 外 <input type="text"/>	IPv6内网地址	--
订单类型	商用	到期时间	2025-11-17 11:57:26	创建时间	2025-10-17 11:55:49
资源ID	33edf1f5c140417dbef36f6b95c0e81	实例	4fa6bb3aa3ff4c50b02c297a0671436e	实例规格	高级版10资产
虚拟私有云	vpc-default	子网	subnet-default	存储	2.2/299.9G
系统盘	<input type="text"/> 14.4/39.1G	部署架构	通用型x86		

- 变更规格
- 修改默认路由
- 续费
- 退订**

计费说明

- 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。

提示



确定退订实例 osm-d1v0 吗?

如您需要同时退订相关云主机，请手动退订云主机

取消

确认

- 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。

退订管理 / 退订申请

满意度评价 资源被锁定

退订须知:

- 退订成功后资源不可恢复;
- 确定退订前建议完成数据备份或者数据迁移;
- 除特殊约定(云电脑、云间高速尊享版两款产品，退订后资源立即释放)以外，退订后的资源将以冻结形式保留15天后释放;
- 退订可能会导致其他存在的关联业务产生影响。

退订规则请查看: [退订规则说明](#)

产品名称	资源ID	资源池	资源状态	时间	产品金额	可退订金额
云堡垒机 (原生版)	33edf1f5c1404170bef36f6fb95c0e81	重庆	有效	创建 2025-10-17 11:57:31 到期 2025-11-17 11:57:26	元	元
云堡垒机 (原生版) _单机版 产品名称: 云堡垒机 (原生版) 版本: 高级版 最大资产数: 10 虚拟私有云名称: vpc-default						

* 请选择退订原因:

- 购买云服务时选错参数 (配置、时长、台数等)
- 云服务功能不完善, 不满足业务需求
- 其他云服务商的性价比更高
- 区域选择错误
- 云服务故障无法修复
- 其他

产品金额: 元

退订金额: 元

我已确认本次退订金额和相关费用

退订

取消

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。

计费说明

- 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。

安全组策略设置

若云堡垒机绑定了EIP，在用户通过EIP访问堡垒机之前需要配置安全组策略，编辑入方向策略，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，添加规则允许需访问堡垒机的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18443，18000，8765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
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	本地初始化获取配置端口	需通过客户端工具运维时，需开放该端口的入方向规则

快速入门

端口	用途	说明
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，需开放该端口的出方向规则 说明 仅“二类节点”区域的实例涉及该端口。

安全组规则设置

堡垒机弹性IP安全组访问规则设置请参见：[虚拟私有云-添加安全组规则](#)。

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。

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”。

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。

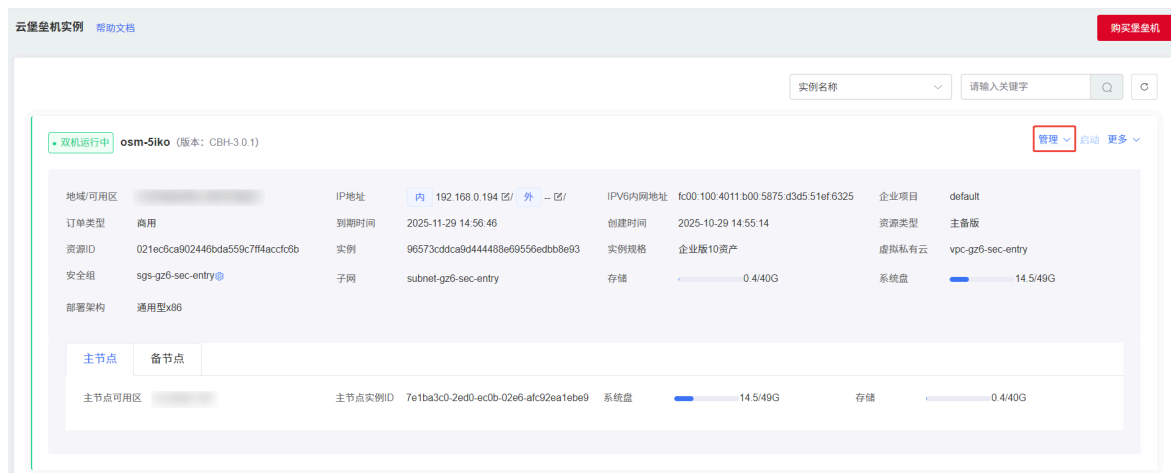
首次登录

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。

- 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”。
- 根据您的自身的网络环境选择“内网地址登录”或“外网地址登录”。

快速入门

3. 登录堡垒机后，通过个人信息进行初始密码设置。



非首次登录

非首次登录云堡垒机可通过云堡垒机控制台单点登录跳转登录堡垒机，或通过云堡垒机登录地址使用本地认证、AD认证等方式登录。

说明

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。

前置条件

已登录过云堡垒机并完成密码初始化。

本地认证登录操作步骤

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“本地认证”。
3. 输入系统用户账号和密码，输入图形验证码。
4. 在弹出的对话框中选择绑定的双因子认证方式，若未开启双因子认证则跳过该步骤。

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。
- 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。

5. 单击“确定”，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。

AD认证登录操作步骤

说明

使用AD认证登录，请确保该云堡垒机已开启AD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AD认证。
- 3.输入系统用户账号和密码，输入图形验证码。
- 4.在弹出的对话框中选择绑定的双因子认证方式。

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。
- 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。

- 5.单击“确定”，成功登录到堡垒机系统。

新增账号和资产

在使用云堡垒机进行系统管理和运维前，管理人员需要在云堡垒机系统中创建系统用户，为用户分配不同系统角色。

根据角色系统权限的不同，用户拥有不同的系统操作和访问权限，新创建的用户登录系统，即可访问角色权限内模块。

新增用户账号

在使用云堡垒机进行运维前，系统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。

操作步骤

- 1.管理员登录云堡垒机系统。
- 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 > 用户”，单击左上角的“新增”按钮。
- 4.填写账号基本信息，并选择角色身份，单击“确定”。

快速入门

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，用户组相关操作请参见 用户 章节。
认证方式	填写认证方式，可选“跟随系统”和“自定义”： <ul style="list-style-type: none">跟随系统：沿用系统认证方式的设置，并且动态更新同步。自定义：自定义选择认证源、双因子认证。
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。

操作步骤

- 1.管理员登录云堡垒机系统，角色身份切换到“管理角色”。
- 2.在左侧导航栏，选择“资产管理 > 资产”，单击左上角的“新增”按钮。
- 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。

快速入门

参数	参数说明
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”。

快速入门

基本信息

* 资产名称

* 资产类型

请选择



* IP地址

资产组

请选择



资产描述

协议

* 协议

新增

账号

账号列表

添加

账号名	协议	状态	操作
-----	----	----	----

暂无数据

访问信息

系统编码

UTF-8



取消

提交

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。

说明

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。

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。

配置说明

步骤	说明
步骤一：配置访问授权基本信息	可配置服务协议、状态、生效时间、失效时间等信息。
步骤二：关联账号或账号组	关联账号：赋权给单个系统用户。关联账号组：批量赋权给整个账号组成员。赋权后，新加入组的用户账号即刻拥有该访问控制权限。
步骤三：关联资产或资产组	关联资产：授权访问单个资产。关联资产组：授权访问整个账号组。授权后，新加入组的资产可立即被赋权用户访问。
步骤四：关联资产账号	授权访问可访问的资产账号、密码，授权后运维用户可使用该账号密码单点登录到该资产。

操作步骤

1. 使用管理员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“授权管理 > 资产访问授权”，单击左上角的“新增”按钮。
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	
基本信息	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。
登录名	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	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。
账号	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	服务	选择资产访问的协议类型，可多选。
授权时间	生/失效日期	设置该条授权规则的生效/失效日期。
	生/失效时间	将针对上述日期范围的每一天，设置该条授权规则的生效/失效时间段（限定为某固定时间段，例如 9:00~ 18:00），未填写表示全天有效。

5. 填写完成后，单击“提交”。

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“资产访问”。
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/Filezilla/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“资产访问”。
4. 单击目标运维主机，在右下方访问图标选择webterminal方式访问。

```
0.1
Last login: Wed Oct 11 18:55:14 2023 from 127.0.0.1
吃的

#####

Welcome to MY server

Note: All of your operation will be logged!

#####
Connecting to 192.168.113.31. . .:
Last login: Wed Oct 11 18:31:50 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.ct12.x86_64

System information as of time: Wed Oct 11 18:33:00 CST 2023

System load: 0.80
Processes: 1509
Memory used: 57.9%
Swap used: 0.0%
Usage On: 28%
IP address: 192.168.113.31
Users online: 3

[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]# █
```

运维审计

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

快速入门

- 登录授权的审计管理员账号或管理员账号。

操作步骤

1. 使用“管理员账号”或“审计管理员”登录云堡垒机系统。

说明

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“会话日志 > 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。

The screenshot displays the 'Character Audit' (字符审计) interface. A modal window titled '播放' (Playback) is open, showing a terminal session. The terminal output includes:

```
Authorized users only. All activities may be monitored and reported.
Last login: Wed May 7 10:52:31 2025 from 192.168.1.250

Welcome to 4.19.90-2102.2.0.0068.ct12.x86_64

System information as of time: Wed May 7 10:59:18 CST 2025

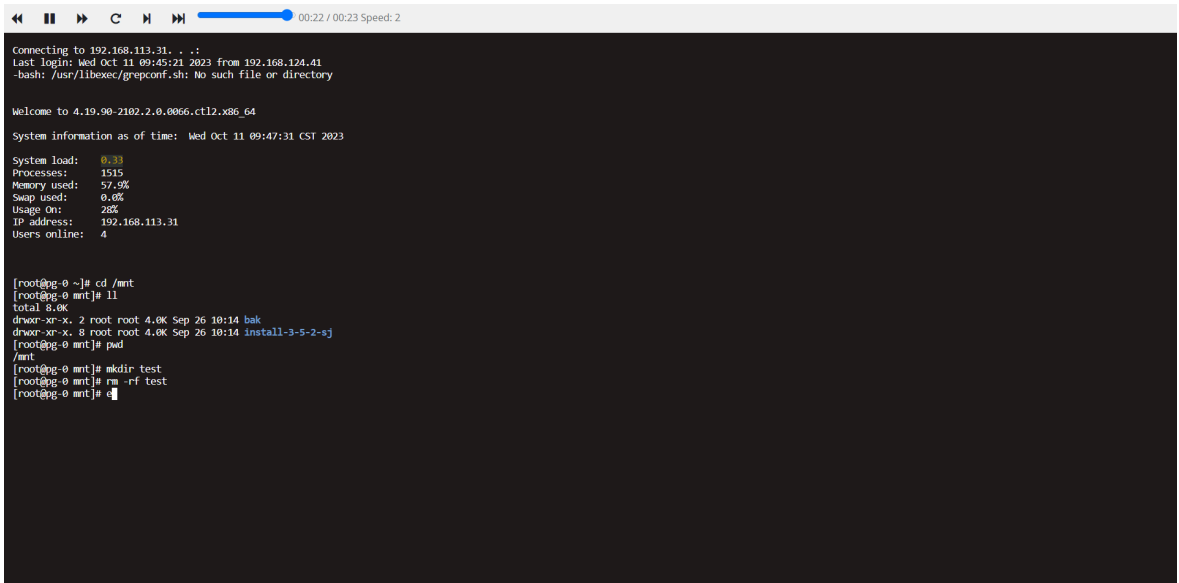
System load:  0.00
Processes:    227
Memory used: 57.5%
Swap used:    0.0%
Usage on /:  55%
IP address:   192.168.1.250
Users online: 4

[root@ctyun-osm-1730955431935 ~]#
```

The background interface shows a table of audit records with columns for '访问开始时间' (Access Start Time), '访问结束时间' (Access End Time), and '操作' (Action). The table contains several rows of data, including timestamps and actions like '查看', '播放', '录屏下载', and '中断'.

快速入门

5. 通过播放按钮，可在线实时审计或回放用户的操作行为。



The screenshot shows a terminal window with a playback control bar at the top. The terminal output includes connection details, system information, and a series of commands and their outputs:

```
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.ct12.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@q-0 ~]# cd /mnt
[root@q-0 mnt]# ll
total 8.0K
drwxr-xr-x. 2 root root 4.0K Sep 26 10:14 bak
drwxr-xr-x. 2 root root 4.0K Sep 26 10:14 install-3-5-2-sj
[root@q-0 mnt]# pwd
/mnt
[root@q-0 mnt]# mkdir test
[root@q-0 mnt]# rm -rf test
[root@q-0 mnt]# c
```

实例管理

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。	<ul style="list-style-type: none"> 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。 <p>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。</p>	<ul style="list-style-type: none"> 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。	<p>一般等待约15分钟后，会自动转为“运行中”状态。</p> <p>如果状态长时间未发生变化：</p> <ul style="list-style-type: none"> 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。	<p>一般等待约15分钟后，会自动转为“运行中”状态。</p> <p>如果状态长时间未发生变化：</p> <ul style="list-style-type: none"> 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。

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。

用户指南

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。

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本地认证、AD认证等方式登录。

前置条件

已登录过云堡垒机并完成密码初始化。

本地认证登录操作步骤

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“本地认证”。
3. 输入系统用户账号和密码，输入图形验证码。

用户指南

4. 在弹出的对话框中选择绑定的双因子认证方式，若未开启双因子认证则跳过该步骤。

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。
- 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。

5. 单击“确定”，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。

AD认证登录操作步骤

说明

使用AD认证登录，请确保该云堡垒机已开启AD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AD认证。
- 3.输入系统用户账号和密码，输入图形验证码。
- 4.在弹出的对话框中选择绑定的双因子认证方式。

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。
- 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。

5.单击“确定”，成功登录到堡垒机系统。

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。

用户指南

参数	说明
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。

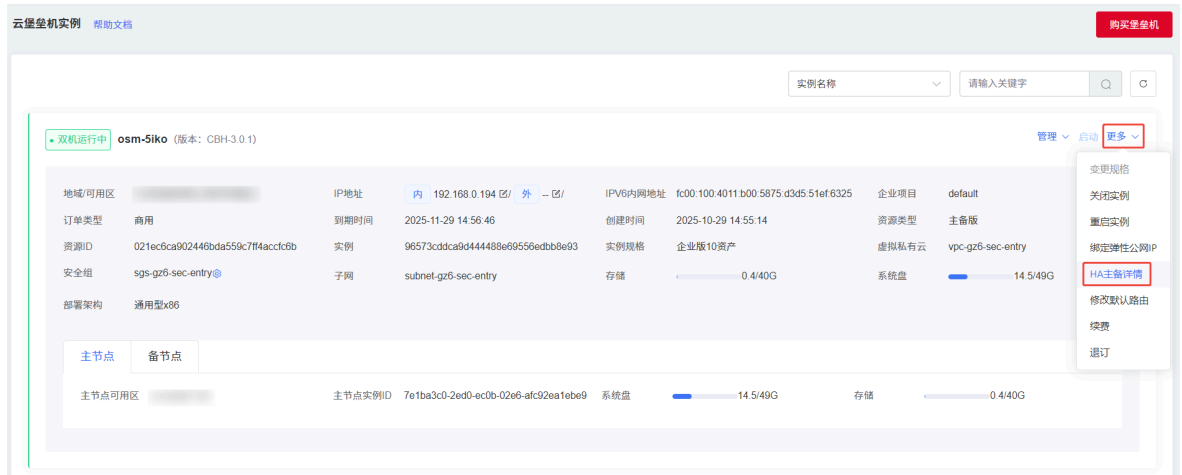
说明

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。

用户指南

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。

HA主备详情



HA状态 主：运行中 备：运行中

数据同步接口 主：192.168.0.190 备：192.168.0.193

本机接口IP 主：192.168.0.187 备：192.168.0.191

对端接口IP 主：192.168.0.188 备：192.168.0.192

VRRP_ID 99

关闭

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

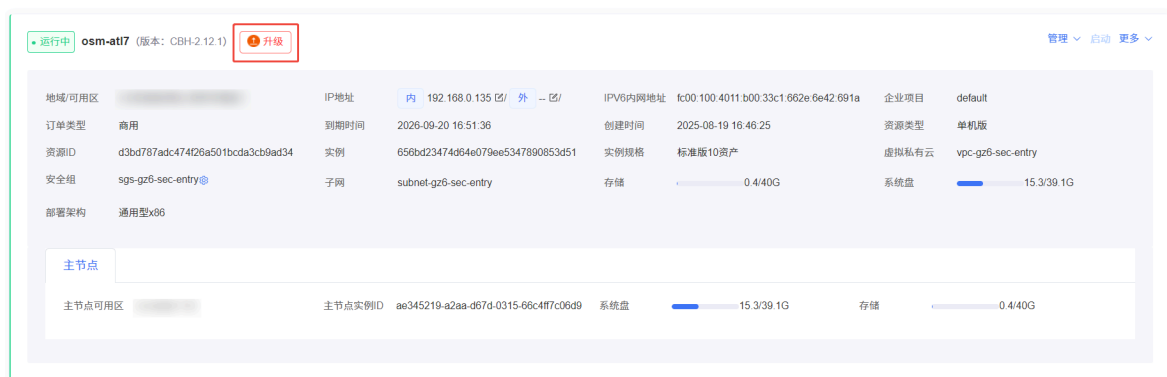
- 在堡垒机升级至1.3.0版本后，需要卸载旧的访问插件，在“运维设置 > 访问插件”中下载最新版本插件进行安装。
- 堡垒机在升级失败后会自动回退版本。

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

- 登录管理控制台。
- 选择“安全 > 云堡垒机（原生版）”，进入云堡垒机实例管理页面。
- 选择需变更升级的实例，单击实例名称旁的“升级”。



- 在弹出的对话框中单击“确认”，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”。
- 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。

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，详见[安全组策略设置](#)：

- 方式一：配置安全组规则，具体操作请参见[修改安全组规则](#)。
- 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。

用户指南

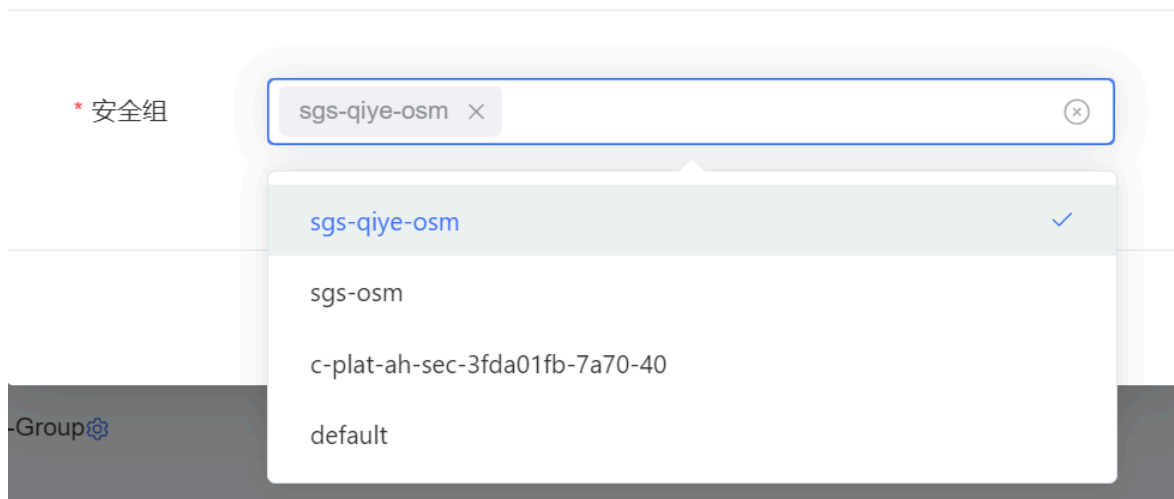
操作步骤

1. 登录天翼云控制中心。
2. 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。
3. 选择需要更改安全组的堡垒机实例，在实例详情页单击  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。

配置安全组



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。

用户指南

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”。

修改默认路由

×

类型	目标网络	下一跳网关（仅内网）	是否生效
IPv4	0.0.0.0/0	-- <input checked="" type="checkbox"/>	<input type="checkbox"/>
IPv6	:::/0	-- <input checked="" type="checkbox"/>	<input type="checkbox"/>

取消

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”。

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。

用户指南

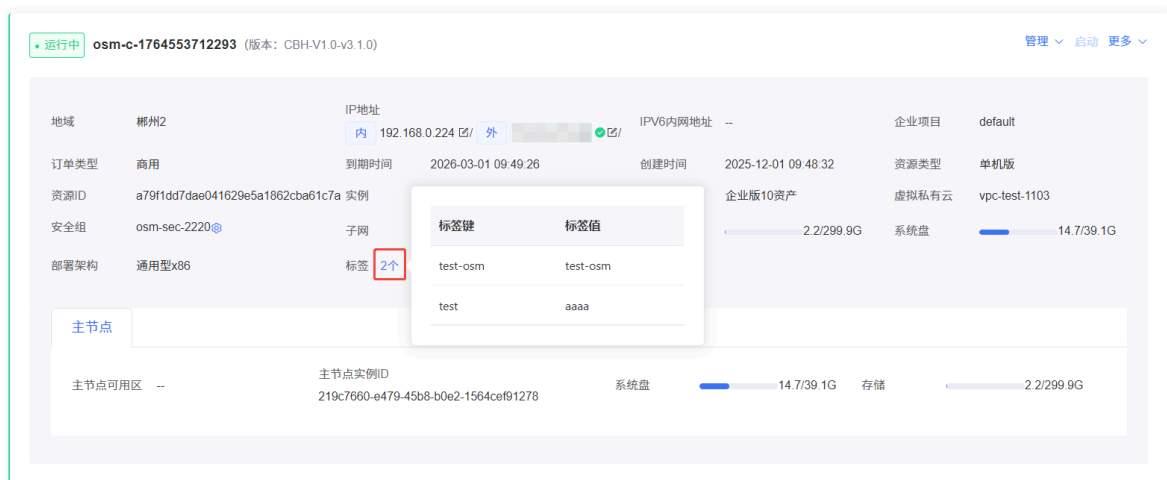
- 每个实例下的标签键是唯一的，不可绑定相同标签键。
- 不支持修改标签，可以解绑标签后，绑定新的标签。

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。



用户指南

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. 选择需要解绑标签的堡垒机实例，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”。

编辑标签



标签键	标签值	操作
test-osm	test-osm	删除

您还可以添加9个标签

取消

确定

6. 单击“确定”，解绑标签完成。

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（CBH）的全读写访问权限。	系统策略	全局级
ctcbh viewer	云堡垒机（CBH）的只读访问权限。	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	✓	×

用户指南

权限	授权项	权限类型（读/写）	ctcbh admin	ctcbh viewer
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](#)

使用云监控服务监控云堡垒机实例

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

用户指南

监控指标	指标说明	单位	是否支持告警	监控周期
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。



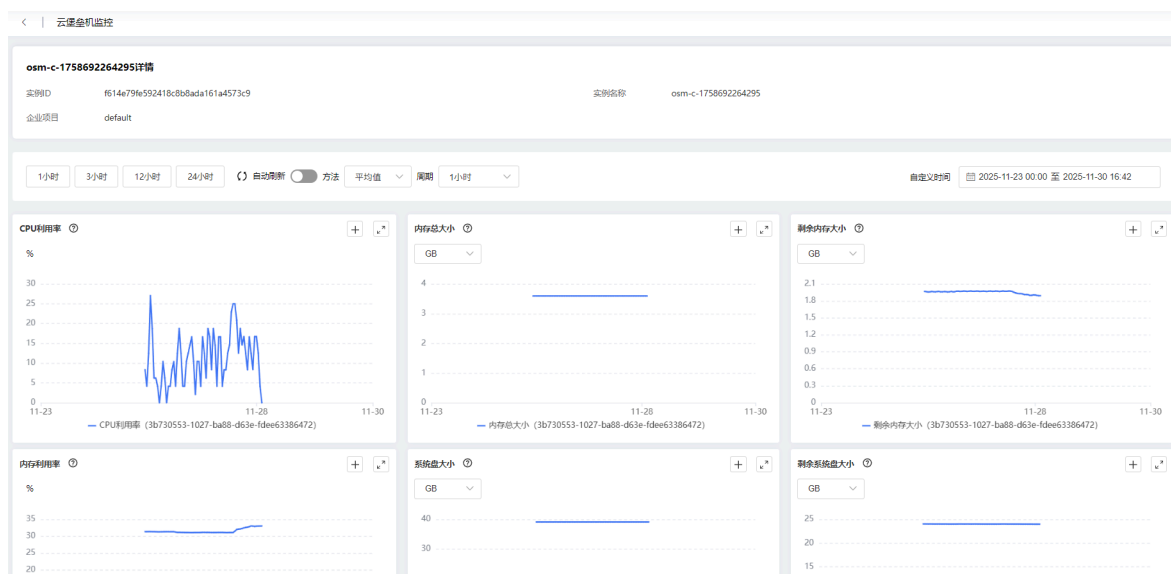
用户指南

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。



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为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。

用户指南

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

用户指南

模块	参数	参数说明	配置示例
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
	策略	支持选择 满足全部 或 任意策略 。 策略信息包括： <ul style="list-style-type: none"> • 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） <p>说明 同一告警规则，告警条件最多支持添加20条。</p>	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	

用户指南

模块	参数	参数说明	配置示例
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
	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。

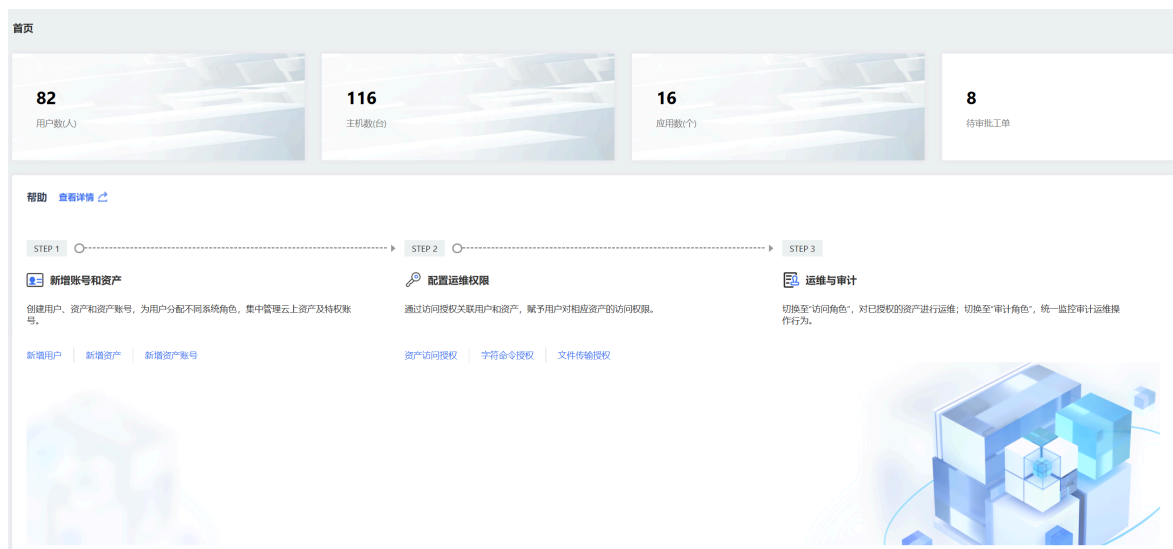
告警规则添加完成后，当监控指标触发设定的阈值时，云监控会在第一时间通过邮件实时告知您云上资源异常，以免因此造成业务损失。关于云监控的其他操作和更多信息，请参考《云监控服务》。

管理员手册

首页

管理角色首页

使用管理角色登录云堡垒机时可查看目前堡垒机下纳管的用户数、主机数、应用数及待审批的工单数量。



审计角色首页

使用审计角色登录云堡垒机时可查看目前堡垒机下纳管的用户数、主机数以及历史会话数。

会话统计：图表显示目前堡垒机正在连接的会话数。

剩余会话：目前堡垒机剩余可连接的会话总数。

活跃人数：目前登录堡垒机的总用户数。

活动主机：目前正在连接的主机总数。

用户指南



用户管理

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”权限的用户可以管理用户和用户组。

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。

用户指南

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

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	(选填)填写该账户的使用者的姓名。

用户指南

参数	参数说明
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，可选以下角色： <ul style="list-style-type: none">• 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） <p>说明 一个用户支持配置多个角色，但管理角色和工单管理角色只支持二选一。</p>
用户组	(选填) 选择该账户所属的用户组，用户组操作请参见 新增用户组 。若不配置，则默认在“未分组”列表。
认证方式	选择认证方式，可选“跟随系统”和“自定义”： <ul style="list-style-type: none">• 跟随系统：沿用系统认证方式的设置，并且动态更新同步。• 自定义：自定义选择认证源、双因子认证。
生效时间-失效时间	(选填) 选择该账户可登录的时间段。若不配置，默认永久生效。
准入IP	(选填) 选择可登录的IP地址。
准入MAC	(选填) 填写该用户允许登录的MAC地址。

4. 填写完成后，单击“确定”完成单个用户新增。

您可以根据需要对用户信息和密码进行修改：

- 修改用户信息：选择需要修改信息的用户，单击“操作”列中“编辑”，按照需求进行用户数据的修改，单击“确定”完成用户信息修改。

注意

不支持修改用户登录名。

- 修改用户密码：管理员可以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。

使用本地文件批量导入用户

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。

用户指南

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“用户导入”对话框。
4. 单击“下载导入文件模板”，下载导入模版。

用户导入 ×

从本地文件导入 AD认证用户导入

* 上传文件

重复用户导入策略 [?] 跳过 覆盖（重设新密码） 覆盖（保留原密码） 建立副本

[下载导入文件模板](#)

5. 在下载导入模板中填写用户信息。

参数	参数说明
姓名	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；
登录名	（必填）填写该账户的使用者的登录名。
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。
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。
状态	（必填）选择该账户的状态，“正常”或者“锁定”。
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，用户组相关操作请参见 用户组 章节。 <ul style="list-style-type: none">• 多级用户组格式为：用户组/用户组1/用户组1-1。• 若填写多个用户组请使用英文“,”分隔。

用户指南

参数	参数说明
认证方式	(必填)填写认证方式,可选“跟随系统”和“自定义”: <ul style="list-style-type: none">跟随系统:沿用系统认证方式的设置,并且动态更新同步。自定义:自定义选择认证源、双因子认证。
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。
授权生效时间	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。
授权失效时间	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	填写可登录的IP地址。
准入MAC	填写该用户允许登录的MAC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。

6. 填写完成后,上传模板文件;选择重复用户导入策略。

用户导入

×

从本地文件导入

AD认证用户导入

* 上传文件

选取文件

重复用户导入策略



跳过



覆盖 (重设新密码)



覆盖 (保留原密码)



建立副本

[下载导入文件模板](#)

关闭

提交

注意

导入后,用户登录名不可修改。

7. 完成后单击“提交”即可完成用户导入。

用户指南

AD认证用户导入

说明

需要开启AD认证并使用AD同步配置后才可使用此功能。

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“用户导入”对话框。
4. 在上方页签选择“AD认证用户导入”。

用户导入

从本地文件导入 **AD认证用户导入**

搜索用户名/姓名

<input type="checkbox"/>	登录名	姓名	手机号	邮箱	角色 <small>批量填充</small>	用户组 <small>批量填充</small>
暂无数据						

共 0 条 < >

重复用户导入策略 跳过 覆盖

5. 勾选需要导入的用户信息，并且选择导入策略。
6. 单击“导入”完成AD认证用户导入。

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。不勾选时，可导出所有用户信息。

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. 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。

用户指南

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。

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。

手机令牌

若您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

已给堡垒机开通“令牌认证”方式，即用户的认证方式支持“令牌认证”，具体配置方式请参见[认证设置](#)。

手机令牌绑定

1. 进入云堡垒机（原生版）实例登录页。
2. 选择“本地认证”或“AD认证”方式，输入账号密码登录。
3. 在弹出的双因子认证对话框中选择“令牌认证”，单击登录下方的“绑定令牌”按钮，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。

资产管理

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。

用户指南

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”，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。 当您选择Windows服务器或Unix/Linux服务器时，可填写SSH登录指令/目录和Telnet登录指令/目录。 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。	-
资产描述	填写资产的描述。	-
协议	选择资产的协议类型： <ul style="list-style-type: none">• 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。• 资产类型选择数据库时支持选择：Oracle、DB2、MySQL、PostgreSQL、达梦、金仓(Kingbase)、万里(GreatSQL)、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
	说明 金仓(Kingbase)配置方法参考PostgreSQL；万里(GreatSQL)配置方法参考MySQL。	

用户指南

参数	参数说明	取值样例
账号	<p>(可选) 添加可访问资产的账号:</p> <ul style="list-style-type: none">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。 <p>您也可以在资产账号模块添加。</p>	-
访问信息	选择资产系统编码, 可选“UTF-8”或“GBK”。	GBK

4. 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. 选择“导入 > 从本地文件导入”，在弹出的对话框中下载导入模板。

用户指南

4. 在导入模板文件中填写内容，填写完成后保存。

资产导入 ×

[从本地文件导入](#) [天翼云ESC实例导入](#) [资产发现](#)

* 上传文件

重复资产导入策略 [?] 跳过 覆盖 建立副本

[下载导入文件模板](#)

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，支持IPv4和IPv6。	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： <ul style="list-style-type: none">• 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。	-
访问信息	填写资产的访问编码，仅支持填写“UTF-8”或“GBK”。	GBK

用户指南

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）。

6. 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自动发现资产。

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. 选择“导入 > 资产发现”，填写需要扫描的目标网段和端口。

扫描地址

* 目标网段

地址段格式：192.168.1.1/24，单地址格式：192.168.1.1，多个地址（段）用“;”分隔

* 端口

端口范围从1到65535，多个端口用“;”分隔，例如:22,80-100

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。

相关操作

- 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。若不勾选，则默认导出所有资产。
- 批量编辑资产组：在“资产”页面勾选资产，单击“编辑”，可将资产关联到一个或者多个资产组。
- 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”，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！

- 批量测试连通性：在“资产”页面勾选资产，单击“测试连通性”，批量测试连通性。已检测的历史结果每隔4小时被清空，展示为“未检测”。

应用资产

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，无需登录应用服务器，即可便捷地访问Web应用。

约束限制

- 仅企业版支持使用应用运维功能。
- Windows应用服务器仅支持2016版本。

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。

用户指南

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。

新增应用服务器 ×

* 服务器名称

* 服务器类型

* 服务器IP地址

* 端口

服务器描述

* 服务器账户

* 密码

* app类型和路径

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。

用户指南

参数	填写说明
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”。

应用服务器导入



* 上传文件

选择文件

重复授权导入策略



跳过



覆盖



建立副本

[下载导入文件模板](#)

关闭

提交

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. 上传已经填写完成的导入文件，根据需求选择重复导入策略。

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。

用户指南

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。

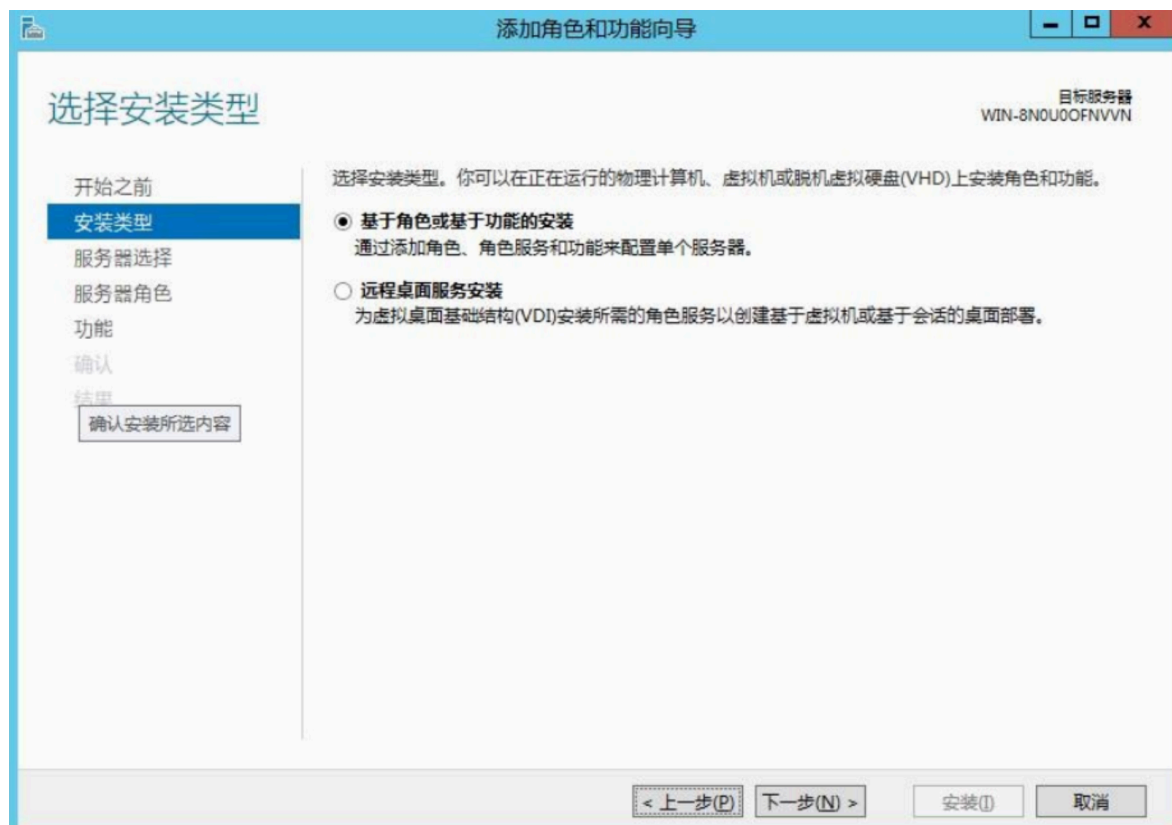
安装服务器

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“仪表盘”，进入仪表盘界面。
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。

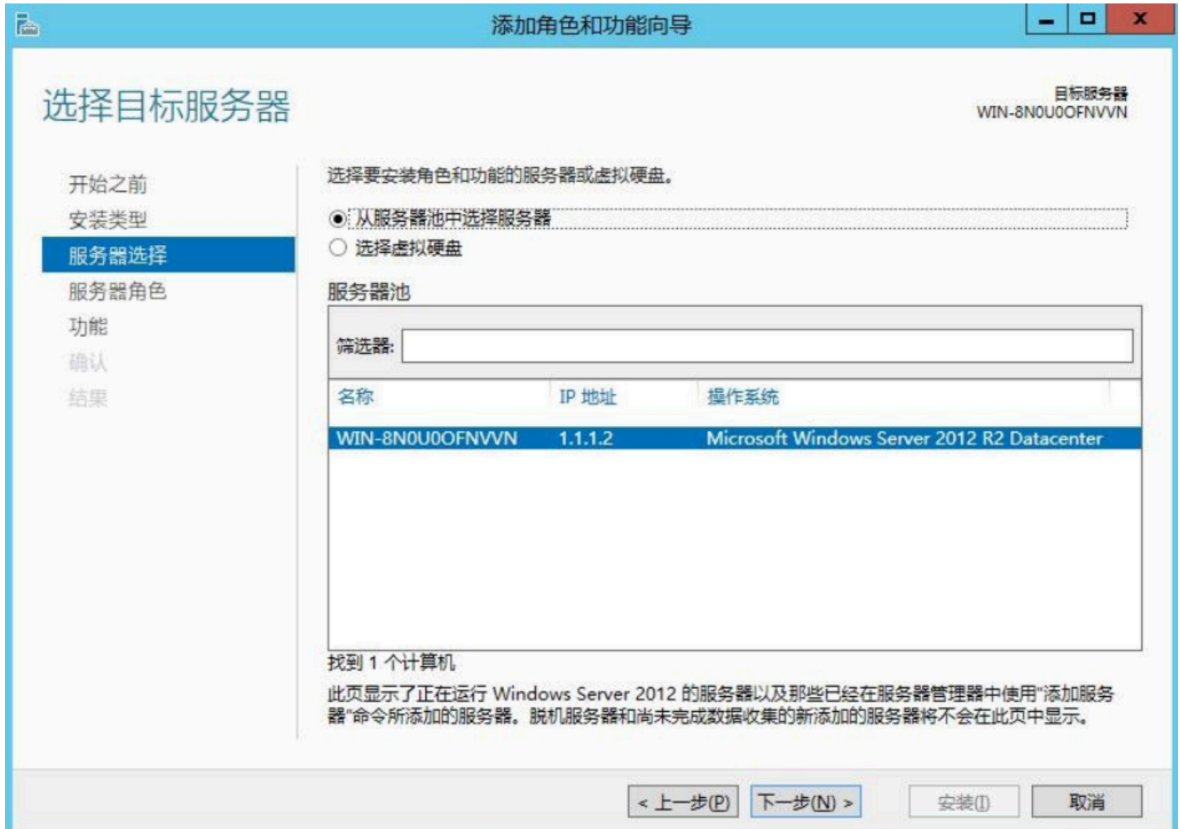


4. 选择“基于角色或基于功能的安装”。



用户指南

5. 在服务器池中选择目标服务器。



- 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。

选择服务器角色

开始之前

安装类型

服务器选择

服务器角色

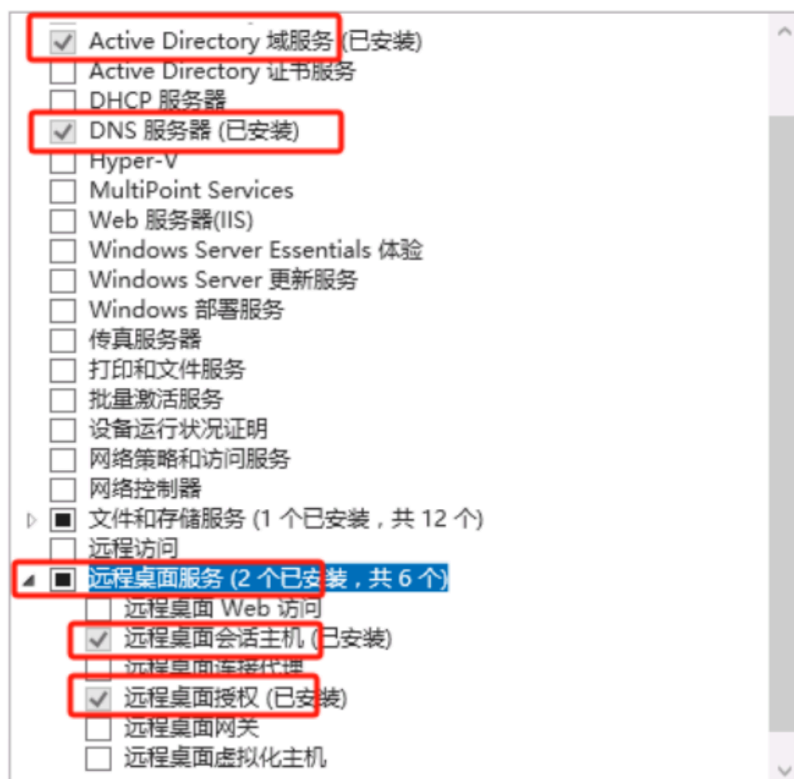
功能

确认

结果

选择要安装在所选服务器上的一个或多个角色。

角色



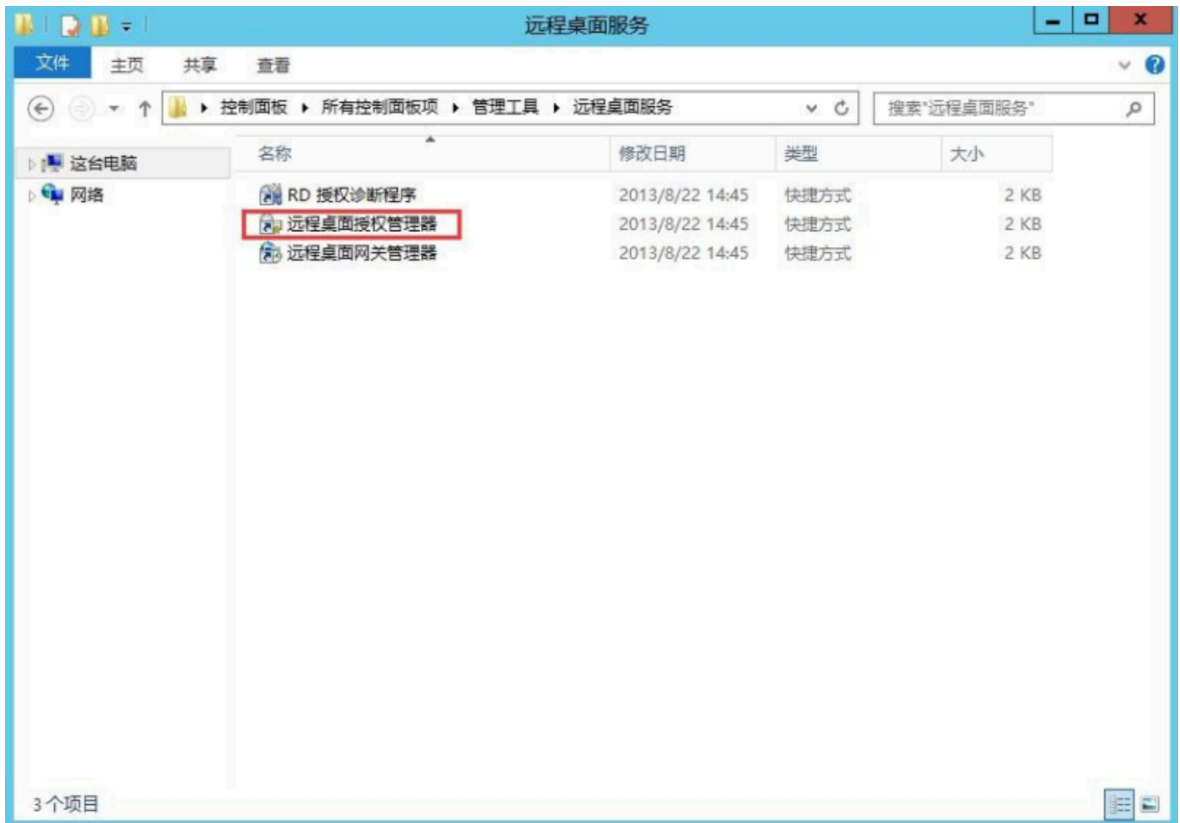
- (可选) 选择服务器所需要的其它功能，默认下一步跳过。
- 选择“远程桌面服务 > 角色服务”，进入选择远程桌面角色服务窗口，勾选“Remote Desktop Session Host”、“远程桌面连接代理”、“远程桌面授权”、“远程桌面网关”、“远程桌面Web访问”角色服务项。
- (可选) 选择“Web服务器角色 (IIS) > 角色服务”，进入选择网络策略和访问角色服务窗口，按默认选项执行。
- (可选) 选择“网络策略和访问服务”，进入选择网络策略和访问服务窗口，默认勾选“网络策略服务器”选项。
- 确认配置选择，单击“安装”，请耐心等待安装进度完成。
- 安装进度结束后，单击“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

- 使用管理员账号登录服务器。

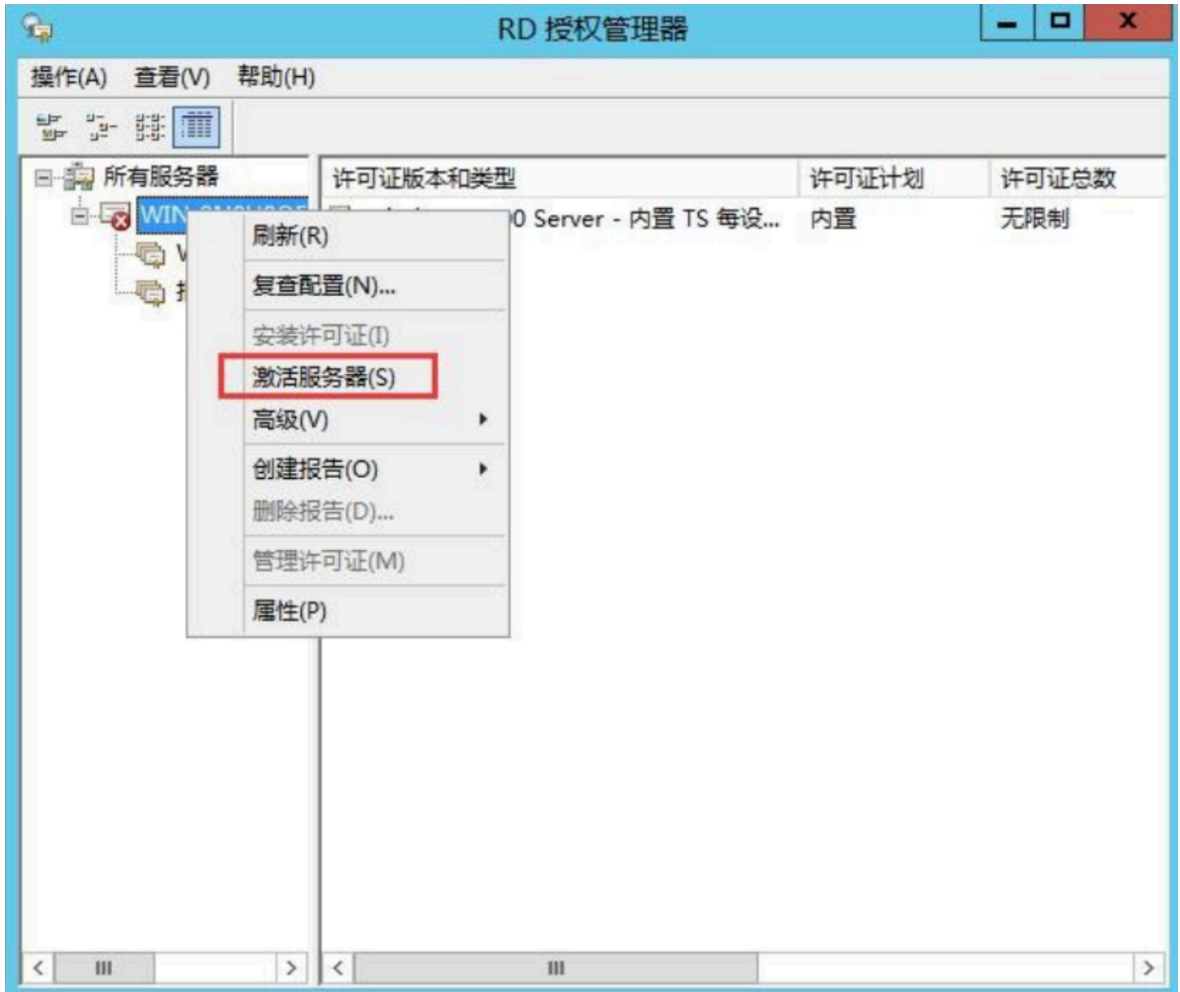
用户指南

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。



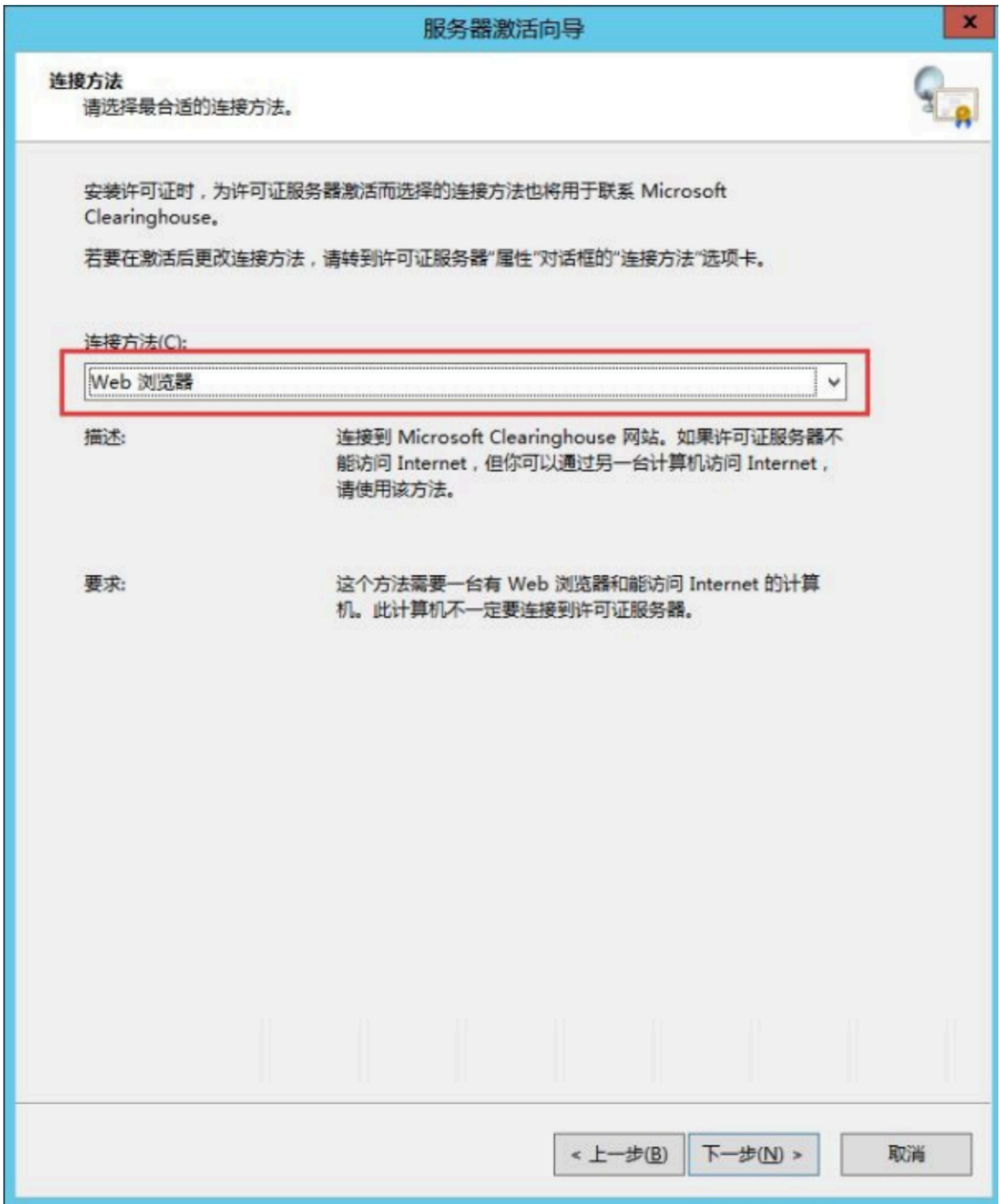
用户指南

3. 选择未激活的目标服务器，鼠标右键选择“激活服务器”。



用户指南

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。

用户指南

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。

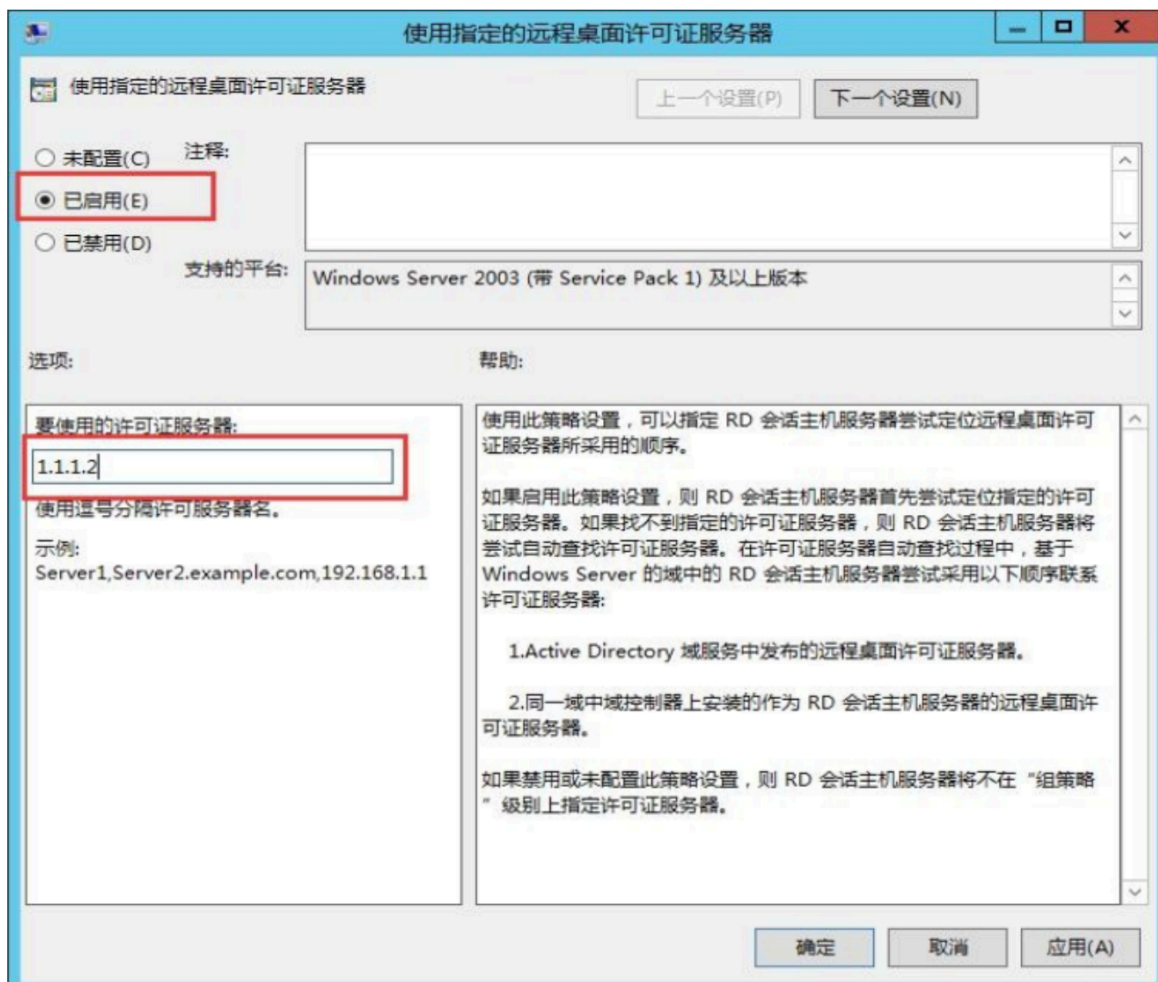
服务器策略配置

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。

用户指南

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。

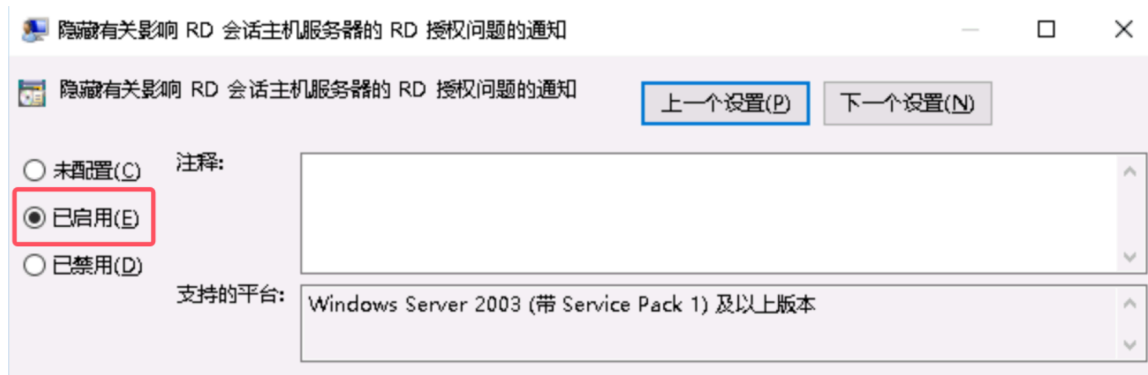


5. 单击“确定”完成配置。

(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”。



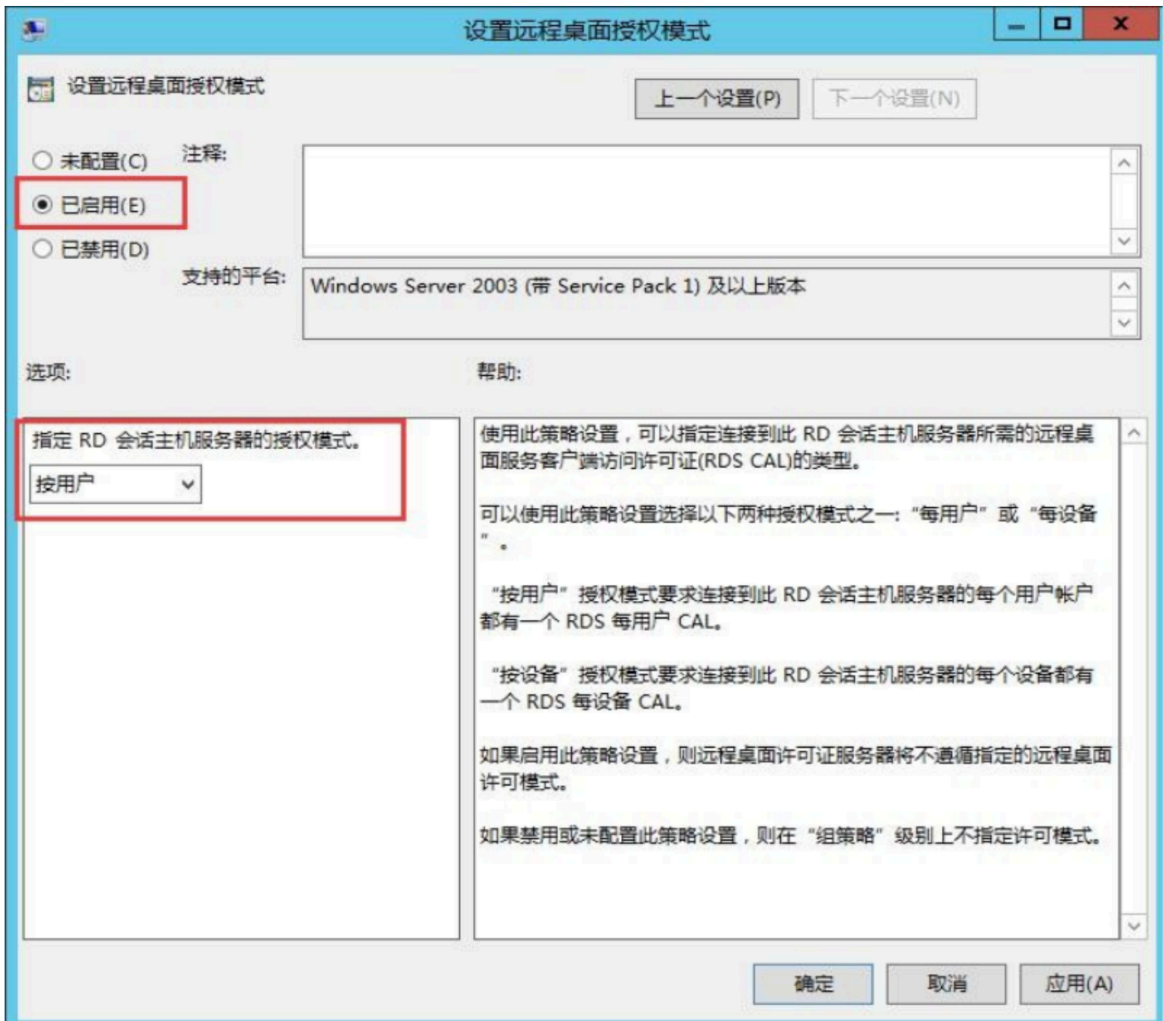
5. 单击“确定”完成配置。

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。

用户指南

4. 选择“已启用”，并且在“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”。



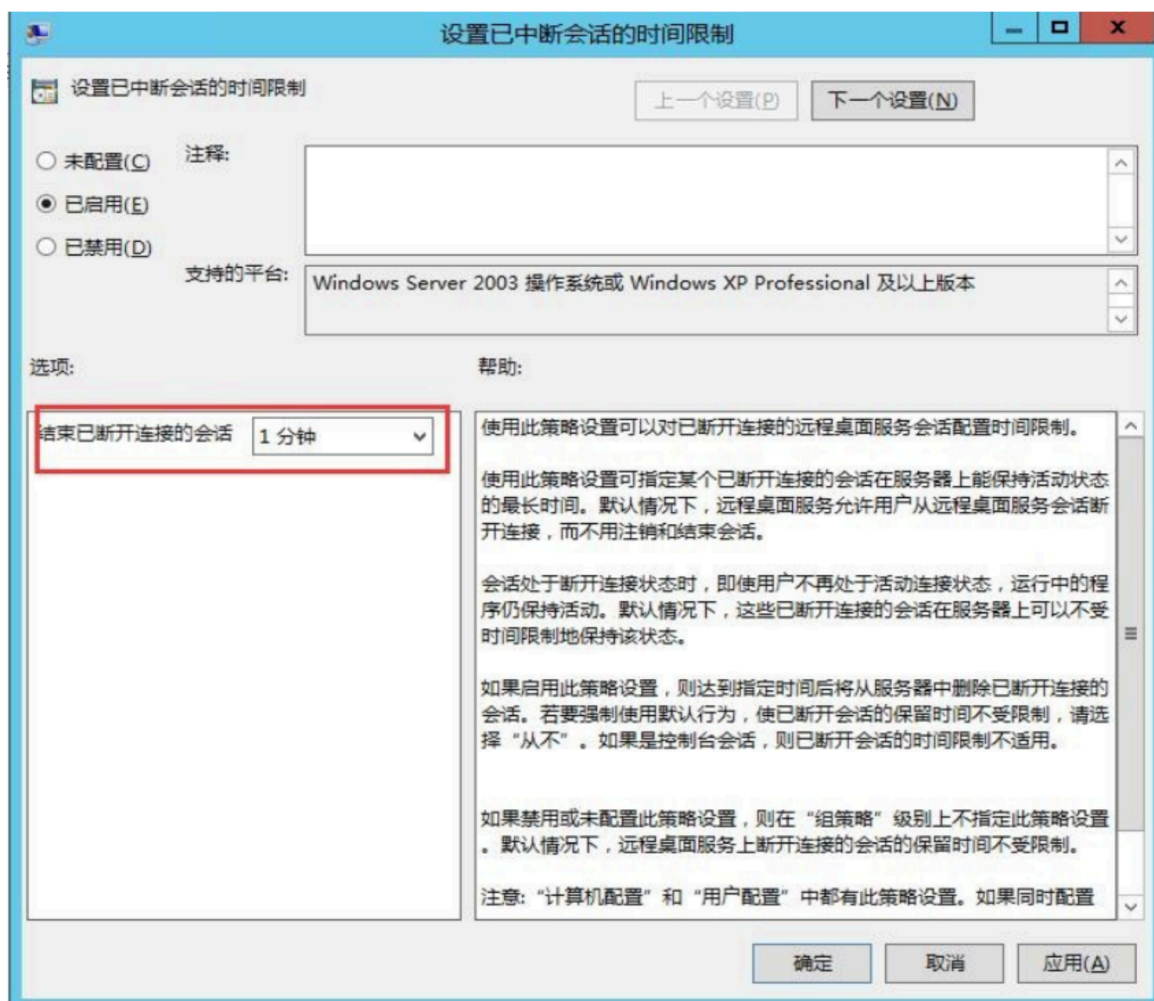
5. 单击“确定”完成配置。

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。

用户指南

- 勾选“已启用”，并且设置结束已断开连接的会话为1分钟。



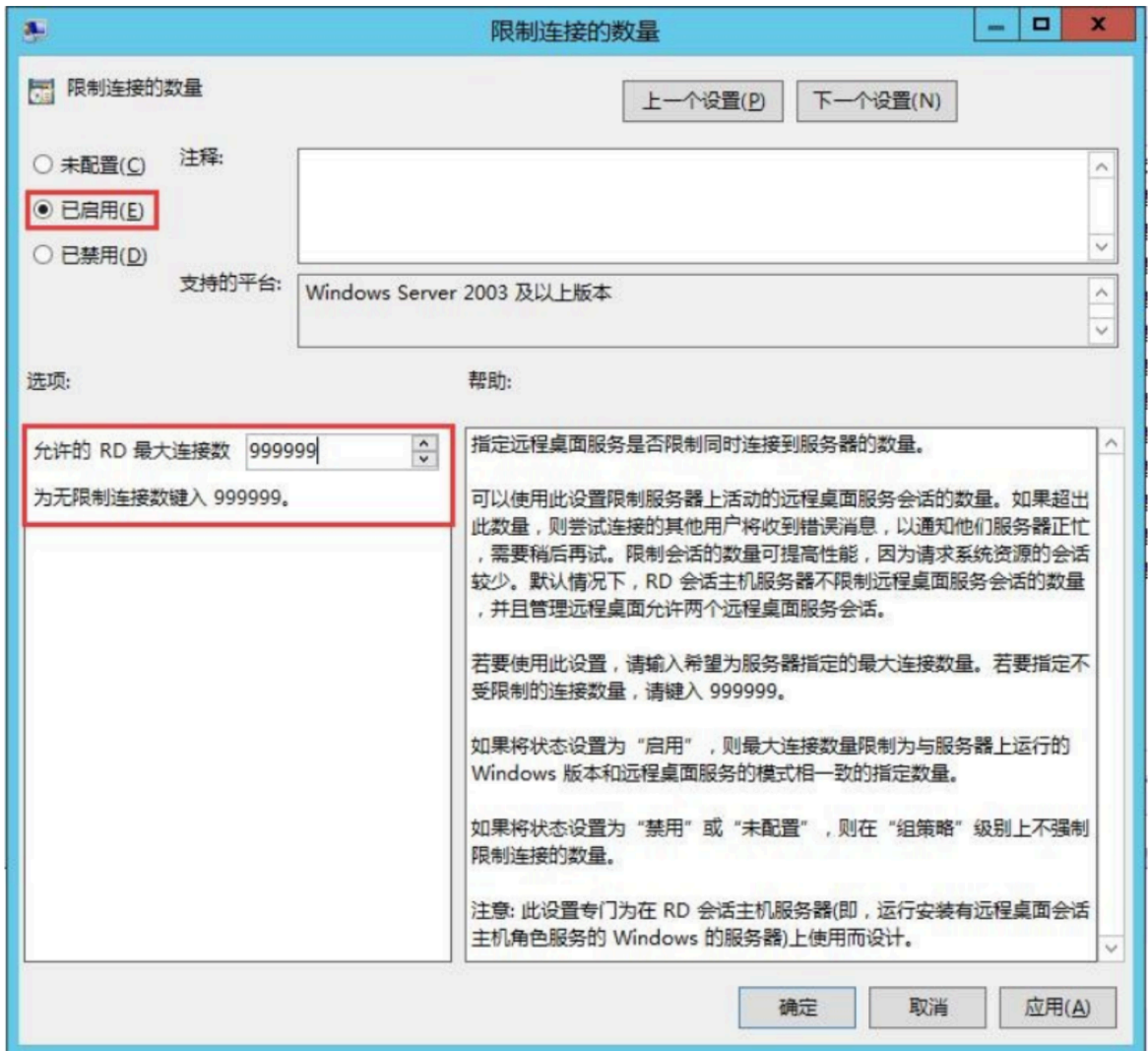
- 单击“确定”完成配置。

限制连接的数量

- 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”。
- 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。
- 选择“限制连接数量”，进入设置窗口。

用户指南

- 勾选“已启用”，并且填写“RD最大连接数”为999999。



- 单击“确定”完成配置。

允许远程启动未列出的程序

- 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”。
- 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。
- 选择“允许远程启动未列出的程序”，进入设置窗口。
- 勾选“已启用”。
- 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

- 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”。

用户指南

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。



```
管理员: Windows PowerShell
Windows PowerShell
版权所有 (C) 2014 Microsoft Corporation. 保留所有权利。
PS C:\Users\Administrator> gpupdate /force
正在更新策略...
计算机策略更新成功完成。
用户策略更新成功完成。
PS C:\Users\Administrator> _
```

远程设置

1. 选择“计算机”，右键选择“属性”。

用户指南

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”。

计算机名 硬件 高级 远程

远程协助

允许远程协助连接这台计算机(R)

高级(V)...

远程桌面

选择一个选项，然后指定谁可以连接。

不允许远程连接到此计算机(D)

允许远程连接到此计算机(L)

仅允许运行使用网络级别身份验证的远程桌面的计算机连接(建议)(N)

[帮助我选择](#)

选择用户(S)...

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。

用户指南

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。

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。

添加应用资产

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。

用户指南

参数	填写说明
应用服务器	先选择浏览器，然后再选择浏览器所属的应用服务器。 浏览器当前仅支持：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。

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。
- 使用“管理角色”账户登录云堡垒机系统。
 - 在左侧导航栏选择“资产管理 > 资产账号”，进入“资产账号”页面。
 - 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。

分类	参数	参数说明	取值样例
资产信息	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。	-
账号信息	账号名	填写可登录资产的账号名。	root
	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，并填写证书密码保存至堡垒机中。	
	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	

用户指南

分类	参数	参数说明	取值样例
多层登录配置	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”账户登录云堡垒机系统。
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文件模板。

资产账号导入



* 上传文件

选取文件

文件解密密码

如有，则必填

重复资产账户导入策略 [?]

跳过

覆盖

下载导入文件模板

取消

提交

用户指南

4. 在导入文件模板中填写内容，填写完成后保存文件。

模版参数说明：

分类	参数	参数说明	取值样例
资产信息	资产名称	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。 多个资产用英文逗号“,”隔开。	Test
账号信息	账号名	填写可登录资产的账号名，例如：Administrator。	root
	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	（可选）请选择资产的协议，支持填写：SSH、TELNET、SFTP、FTP、X11、RDP和数据库。 多个协议用英文逗号“,”隔开。	-
	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
多层登入配置	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。	是
	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

5. 单击“选取文件”，上传已填写完成的导入文件。若文件已加密，还需填写文件解密密码。

6. 单击“提交”，完成资产账号导入。

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”账户登录云堡垒机系统。
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”账户登录云堡垒机系统。
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。

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）。
- 不以“/”开头，不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”账户登录云堡垒机系统。
2. 在左侧导航栏选择“资产管理 > 账户改密”，进入“改密策略”页面。
3. 单击“新增”按钮，在弹出的窗口中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
改密账号	添加改密账号。 <ul style="list-style-type: none">• 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： <ul style="list-style-type: none">• 立即执行：保存后立即执行。• 定时执行：在选择时间后，仅在选择的时间执行一次。• 按周期执行：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： <ul style="list-style-type: none">• 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

用户指南

参数	参数说明	取值样例
指定密码	仅在“改密方式”选择“手动生成指定密码”时需要填写。	-
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	开启“改密完成通知”，还需要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.com
改密附件密码	开启“改密完成通知”，还需要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。

管理改密策略

- 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。

授权管理

资产访问授权

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。

新增资产访问授权

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“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
基本信息	授权规则名	自定义资产访问授权的规则名称。 Test

用户指南

参数		参数说明	取值样例
	启用状态	选择该授权规则的启用状态，默认启用。	
登录名	登录名	(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	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。	-
账号	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。	root
协议	服务	选择该授权规则支持访问的协议。	ssh
	RDP允许选项	仅 服务 选择为“RDP”时可勾选，可选是否可以通过RDP协议复制/粘贴内容或上传/下载文件。	全选
	vnc允许选项	仅 服务 选择为“VNC”时可勾选，可选是否可以通过VNC协议复制/粘贴内容。	全选
授权时间	生/失效日期	选择该规则生效的日期。	2025-12-01 - 2025-12-31
	生/失效时间	选择该规则生效的时间段。	9:00:00 - 18:00:00

4. 单击“提交”完成访问授权规则的创建。

批量导入资产访问授权规则

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 > 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
基本信息	授权规则名	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
登录名	登录名	(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。	-

用户指南

参数		参数说明	取值样例
	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	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。 若您填写的资产和资产组存在重合, 默认取最大的合集。	-
账号	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。	root
协议	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、VNC。	SSH
授权时间	授权生效日期	选择规则生效的日期, 日期填写格式为yyyy/mm/dd。	2023-10-01
	授权失效日期	选择规则失效的日期, 日期填写格式为yyyy/mm/dd。	2024-10-01
	授权生效时间	填写规则生效的时间段, 时间段填写格式为00:00:00。	9:00:00
	授权失效时间	填写规则失效的时间段, 时间段填写格式为00:00:00。	18:00:00

5. 填写完成后, 保存文件并上传。

后续操作

- 导出资产授权访问规则: 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/禁用资产访问授权规则: 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。

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, 排序数字越小优先级越高(优先级可选1~100)。
- 支持以下控制命令的动作。
 - 触发审批: 拦截该命令, 并自动创建为审批工单。支持审批超时配置, 超时xx分钟默认拒绝执行或默认允许执行。
 - 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。
 - 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, 界面会提示您在执行命令时会得到该命令不能执行的提示。

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。

用户指南

- 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。
- 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	当匹配方式选择“单命令匹配”时需要填写命令。	/rm
命令正则式	填写命令规则的正则表达式。	enlw*
风险等级	选择该命令组的风险等级，共可选5个等级：普通、重要、危险、警告、致命。	普通
动作	<p>选择该命令组中的命令触发时产生的动作：</p> <ul style="list-style-type: none">触发审批：拦截该命令，并自动创建为审批工单。支持审批超时配置，超时xx分钟默认拒绝执行或默认允许执行。 <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"><p>说明</p><p>对于包含“触发审批”动作的命令组，需要当前选择的用户（组）具有审批规则，否则无法配置“触发审批”动作，请先前往工单管理配置审核人。</p></div> <ul style="list-style-type: none">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。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。	拒绝执行
审批超时配置	设定审批时限，超时未处理则自动拒绝或通过。	5分钟内未审批，则默认拒绝执行。
授权有效期	填写该授权的有效期。审批通过后，在有效期内可多次执行符合该规则的命令。	2小时内有效。

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：触发审批 > 提示警告 > 允许执行 > 拒绝执行，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。

用户指南

注意

- 删除后的命令组不可恢复。
- 若命令组已绑定命令授权规则，删除命令组会导致绑定的命令授权规则失效，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
授权规则名称	自定义资产访问授权的规则名称。
启用状态	选择该授权规则的启用状态，默认启用。
登录名	（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。
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	填写该授权的有效期限。审批通过后，在有效期内可多次执行符合该规则的命令。

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。

命令授权规则后续操作

- 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。

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（优先级可选1~100）。

用户指南

- 支持以下控制命令的动作。
 - 触发审批：拦截该命令，并自动创建为审批工单。支持审批超时配置，超时xx分钟默认拒绝执行或默认允许执行。
 - 断开连接：触发该策略规则后，断开与数据库的连接。
 - 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。

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。

- 使用“管理角色”账户登录云堡垒机系统。
- 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。
- 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
名称	自定义命令组的名称。
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、SHOW、DESCRIBE、EXPLAIN、RENAME。
SQL库名	填写命令生效的SQL库名。
SQL表名	填写命令生效的SQL表名。
风险等级	选择该命令组的风险等级，共可选5个等级。
动作	选择该命令组中的命令触发时产生的动作： <ul style="list-style-type: none">触发审批：拦截该命令，并自动创建为审批工单。支持审批超时配置，超时xx分钟默认拒绝执行或默认允许执行。 <div style="background-color: #e6f2ff; padding: 5px; margin: 5px 0;"><p>说明 对于包含“触发审批”动作的命令组，需要当前选择的用户（组）具有审批规则，否则无法配置“触发审批”动作，请先前往工单管理配置审核人。</p></div> <ul style="list-style-type: none">断开连接：触发该策略规则后，断开与数据库的连接。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。
审批超时配置	设定审批时限，超时未处理则自动拒绝或通过。
授权有效期	填写该授权的有效期。审批通过后，在有效期内可多次执行符合该规则的命令。

说明

命令匹配上多条策略时，动作执行优先级：触发审批 > 断开连接 > 允许执行，若未匹配上任何策略则放行。

用户指南

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”账户登录云堡垒机系统。
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
基本信息	授权规则名称	自定义资产访问授权的规则名称。
	启用状态	选择该授权规则的启用状态，默认启用。
登录名	登录名	(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	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。
账号	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		填写该授权的有效期。审批通过后，在有效期内可多次执行符合该规则的命令。

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。

命令授权规则后续操作

- 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。

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”账户登录云堡垒机系统。
2. 在左侧导航栏选择“授权管理 > 文件传输授权”，进入“文件传输授权”页面。
3. 单击“新增”，配置文件传输授权相关内容。

参数	参数说明	
基本信息	授权规则名称	自定义资产访问授权的规则名称。
	动作	选择此授权规则的动作，可选“允许”或“拒绝”。
	启用状态	选择该授权规则的启用状态，默认启用。
登录名	登录名	(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	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。
账号	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	文件操作	选择需要做限制的文件操作动作。
	文件或目录	可填写具体的文件或文件目录，使用正则表示填写，若填写多个使用回车分行。若不填写文件范围，默认为全选所有文件。 配置示例： <ul style="list-style-type: none">• 只限制tmp文件夹下的同层目录使用，正则表达式可填写：<code>/tmp</code>• 限制tmp目录下所有文件及子目录的使用，正则表达式可填写：<code>/tmp/*</code>
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。
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。

说明

- 策略匹配顺序为：允许 > 拒绝。
- 配置时至少需要关联一个授权对象，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。

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”账户登录云堡垒机系统。
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。 <ul style="list-style-type: none">• 手动执行：保存运维策略后可手动执行该策略。• 定期执行：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。

用户指南

配置项	说明
执行方式	选择自动化运维的执行方式。 <ul style="list-style-type: none">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。

- 单击“确认”，弹出“验证用户身份”窗口。
- 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。

工单管理

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。

新增工单审批规则

- 使用管理员账号登录云堡垒机系统。
- 在左侧导航栏选择“工单管理 > 审批规则”，进入“审批规则”页面。
- 单击左上角的“新增”，弹出“规则新增”配置窗口。

<input type="checkbox"/>	审批规则名称	业务类型	审批人	审批对象	创建时间	操作
<input type="checkbox"/>	doctest	资产访问授权	admin	doc1/a/1	2025-09-09 11:30:34	查看 编辑 删除

- 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”。

参数	说明	
基本信息	规则名称	输入您的审批规则名称。

用户指南

参数	说明
工单类型	根据业务需求选择审批规则： <ul style="list-style-type: none">• 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。
审批对象	登录名（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。
申请范围配置	资产组选项 关闭后，访问角色工单申请页面将屏蔽“资产组”维度，仅能申请单个或多个资产，实现最小化授权。
	可申请资产范围 选择访问角色可申请的资产或资产组，实现可见性隔离。

相关操作

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

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。

工单号	工单名称	状态	申请时间	工单类型	申请人	操作
CW2025052810423276906330	888888	已批准	2025-05-28 10:42:32	数据导出授权	ld	查看 取消授权
CW2025052111390058714411	11111	已批准	2025-05-21 11:39:00	数据导出授权	ld	查看 取消授权
CW2025052108541890638010	55	已批准	2025-05-21 08:54:18	数据导出授权	ld	查看 取消授权
CW2025050714173399624641	0000000000000000	取消授权	2025-05-07 14:17:33	数据导出授权	ld	查看
CW2025050714170088838317	000	待审批	2025-05-07 14:17:00	数据导出授权	ld	审批 查看
CW2025050710195986702038	111	已批准	2025-05-07 10:19:59	数据导出授权	ld	查看 取消授权

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。

系统管理

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：

用户指南

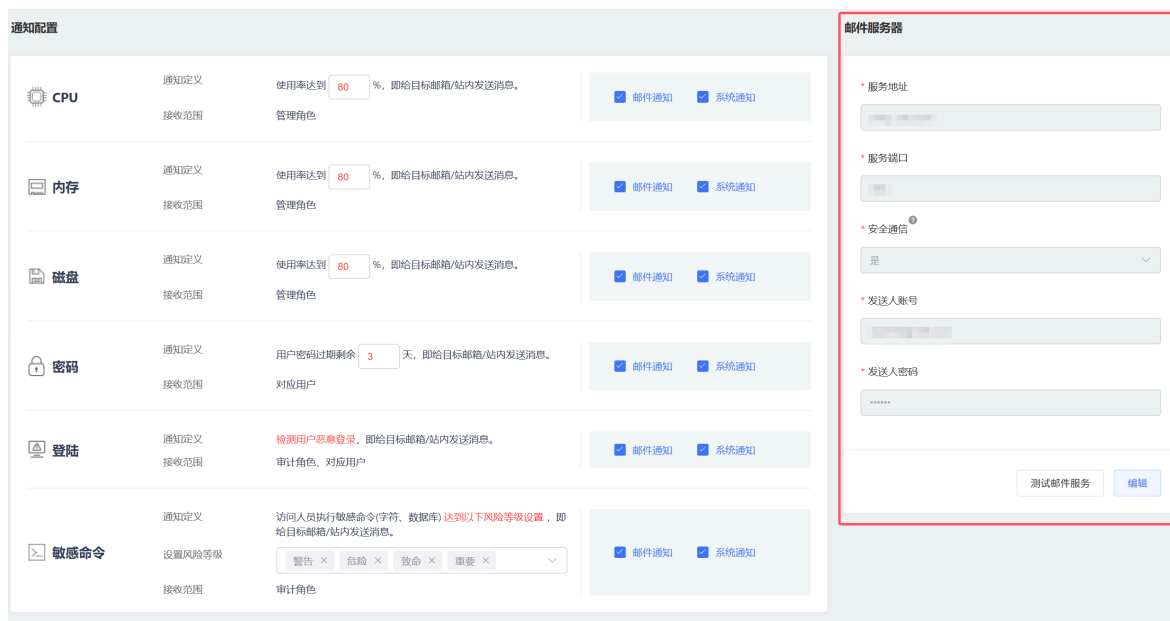
- CPU、内存、磁盘资源使用率超过80%
- 账号密码剩余3天过期
- 用户恶意登录情况告警
- 访问人员执行敏感命令(字符、数据库) 达到风险等级设置发送告警。

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。

设置邮件服务器

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“通知和告警”页面。



3. 在右侧邮件服务器模块，单击“编辑”按钮配置邮件服务器。

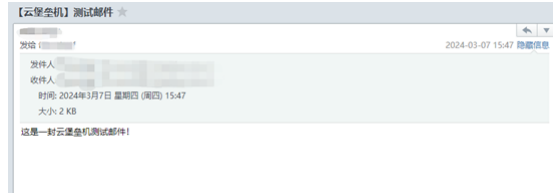
参数	参数说明
服务地址	填写您的邮件服务器地址。
服务端口	填写您的邮件服务器端口
安全通信	选择是否开启安全通信。安全通信支持TLS/SSL协议。
发送人账号	填写发送邮件的邮箱账号。
发送人密码	填写发送邮件的邮箱密码。

4. 单击“保存”完成邮件服务器配置。

用户指南

5. 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 > 通知和告警”，进入“通知和告警”页面。
3. 根据自身需求选择发送通知的项目。

注意

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。

通知配置

CPU	通知定义	使用率达到 <input type="text" value="80"/> %，即给目标邮箱/站内发送消息。	<input checked="" type="checkbox"/> 邮件通知 <input checked="" type="checkbox"/> 系统通知
	接收范围	管理角色	
内存	通知定义	使用率达到 <input type="text" value="80"/> %，即给目标邮箱/站内发送消息。	<input checked="" type="checkbox"/> 邮件通知 <input checked="" type="checkbox"/> 系统通知
	接收范围	管理角色	
磁盘	通知定义	使用率达到 <input type="text" value="80"/> %，即给目标邮箱/站内发送消息。	<input checked="" type="checkbox"/> 邮件通知 <input checked="" type="checkbox"/> 系统通知
	接收范围	管理角色	
密码	通知定义	用户密码过期剩余 <input type="text" value="3"/> 天，即给目标邮箱/站内发送消息。	<input checked="" type="checkbox"/> 邮件通知 <input checked="" type="checkbox"/> 系统通知
	接收范围	对应用户	
登陆	通知定义	检测用户恶意登录，即给目标邮箱/站内发送消息。	<input checked="" type="checkbox"/> 邮件通知 <input checked="" type="checkbox"/> 系统通知
	接收范围	审计角色、对应用户	
敏感命令	通知定义	访问人员执行敏感命令(字符、数据库) 达到以下风险等级设置，即给目标邮箱/站内发送消息。	<input checked="" type="checkbox"/> 邮件通知 <input checked="" type="checkbox"/> 系统通知
	设置风险等级	<input type="text" value="警告"/> <input type="text" value="危险"/> <input type="text" value="致命"/> <input type="text" value="重要"/> <input type="text" value=""/>	
	接收范围	审计角色	

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。

密码组成

密码最小长度	<input type="text" value="8"/>	密码最大长度	<input type="text" value="20"/>
禁止使用历史最近口令(次)	<input type="text" value="1"/>	禁止使用键盘连续字符个数(含以上)	<input type="text" value="0"/>
与账号连续重复不超过口令长度的(%)	<input type="text" value="0"/>	是否必须包含大写字母	<input checked="" type="checkbox"/>
是否必须包含小写字母	<input checked="" type="checkbox"/>	是否必须包含数字	<input checked="" type="checkbox"/>
是否必须包含特殊字符	<input checked="" type="checkbox"/>	<input type="checkbox"/> 禁止使用口令字典中的口令 查看 编辑	

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。
- 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。

密码事件

启用恶意登录事件

密码锁定 分钟内,连续错误 次

账号加锁

启用密码过期事件

密码有效期 天

账号加锁

首次登录, 强制改密

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。

账号事件

账号空闲事件

未使用天数

账号加锁

账号登录事件

唯N性

保存

- 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。
- 账号登录事件: 根据配置的唯一性值,限制同一账号同时登录数。

用户指南

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。

登录超时配置

用户登录超时 分钟

有效值10-1440, 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

资产访问超时 分钟

有效值10-1440, 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

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”。

运维水印配置

运维水印 开启后，访问角色单点登录H5页面会展示该用户信息，实时形成屏幕水印

内容包括 姓名 用户名 手机号 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。

用户指南

获取USBKey认证证书

说明

此操作步骤仅以三未信安产品为例。

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”。

The screenshot shows a web interface for managing USBKey devices. It contains several input fields and buttons. A red arrow points to the password field containing '12345678' with the text '输入口令'. Another red arrow points to the '导出证书' button with the text '导出证书'. Other visible elements include fields for device ID, user, container, and various export options like '导出公钥', '杂凑初始化', '单组数据杂凑', and '关闭杂凑对象'. A '断开设备' button is at the bottom left.

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”。

用户指南

4. 输入证书名称，并且在“证书”模块填入生成的证书。

绑定证书 ×

证书名

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 ，即可在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，证书校验通过后会显示下图提示。



国际证书绑定成功，刷新页面后生效

4. 绑定完成后，会在控制台显示证书相关信息。

资产账号配置

您可以根据合规要求，配置是否允许保存访问角色的密码。

将“访问角色记住密码”开关调整至 ，即可不允许保存访问角色的密码。

资产账号配置

访问角色记住密码



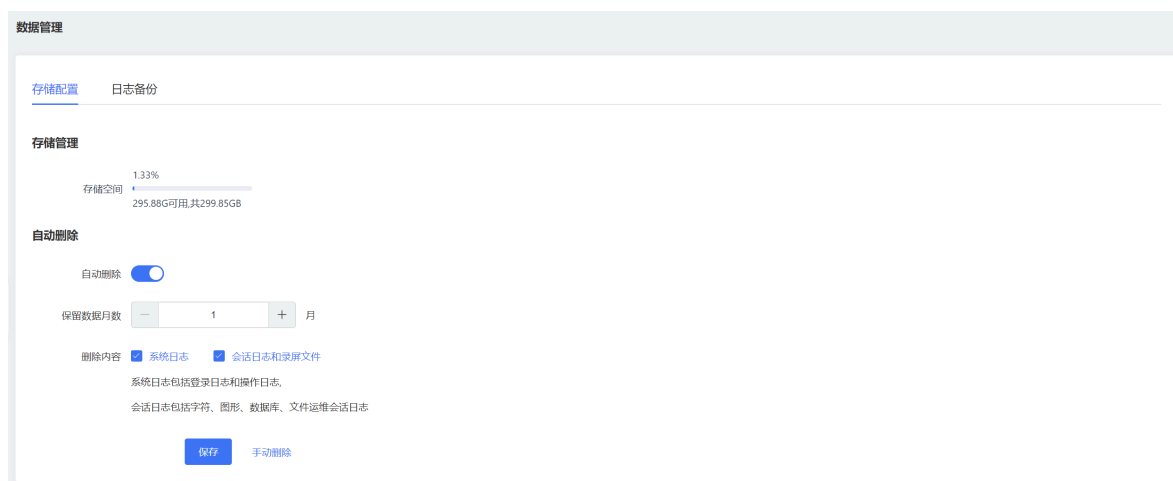
开启后，访问角色手动输入资产账密时，将允许保存账号和密码

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

用户指南

参数	参数说明	取值样例
协议	选择访问Syslog服务器的协议。	UDP

用户指南

参数	参数说明	取值样例
备份内容	选择您需要备份的堡垒机中的业务内容。	-

存储配置 [日志备份](#)

远程备份至syslog服务器

状态

syslog服务器配置

- * 发送名称 用于标识当前发送的日志
- * 服务器IP
- * 端口
- * 协议

备份内容

- 登录日志
- 操作日志
- 会话日志
 - 字符会话日志
 - 图形会话日志
 - 文件传输会话日志
 - 数据库会话日志

取消

保存

4. 填写完成后，单击“保存”即配置完成。

认证设置

认证策略

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“本地认证”、“令牌认证”。

认证策略

AD配置

系统认证方式

* 认证源 本地认证 AD认证

双因子认证 短信认证 令牌认证

全局生效 开启后,所有用户均使用系统认证方式

提交

参数	参数说明
认证源	<ul style="list-style-type: none">本地认证：不依赖外部网络或远程服务器的情况下，直接在设备或系统内部完成用户身份验证的过程。AD认证：用户登录时，系统将账号密码发送到AD认证服务器进行验证，而非在本地校验。AD认证让云堡垒机“借用”了企业现有的、成熟的身份管理目录来识别用户是谁，并决定他们能做什么。
双因子认证	<ul style="list-style-type: none">短信认证：使用手机短信验证码进行二次认证。令牌认证：使用手机令牌进行认证。需下载天翼云App，详情请参见手机令牌。

用户指南

参数	参数说明
全局生效	<ul style="list-style-type: none">• 开启：所有用户均使用系统认证方式。• 关闭：账号的“认证方式”配置为“跟随系统”的用户使用此处配置的“系统认证方式”，配置为“自定义”的用户使用自定义的认证方式。详情请参见新增用户账号。

AD配置

堡垒机支持与AD认证服务器对接，可将AD认证服务器用户同步到堡垒机作为堡垒机用户。

进入“认证策略”页面，勾选“AD认证”后，选择“AD配置”页签，开始AD配置。

AD认证配置

AD认证配置

启用AD认证 开启后，可通过远程AD服务器对用户进行认证

* 服务器地址

* 域名

* 端口 SSL [测试连通性](#)

* BaseDN

* 服务器账号名

账号密码 密码已设置

过滤器

参数	参数说明
服务器地址	输入AD认证服务器地址。
域名	输入AD认证服务器域名。
端口	端口默认两个选择： <ul style="list-style-type: none">• 关闭SSL，默认为389端口。• 开启SSL，默认为636端口。 支持自定义端口号。
BaseDN	填写AD认证服务器中设置的用户目录节点。

用户指南

参数	参数说明
服务器账号名	填写AD认证服务器账号名称，默认为administrator。
账号密码	填写AD认证服务器账号密码。
过滤器	符合过滤条件的用户将被同步至云堡垒机。 例如：(&(objectClass=person))

AD同步配置

AD同步配置

上次同步时间

[立即同步用户](#)

自动同步

自动同步周期 小时

同步内容

本地用户属性	认证源用户属性	是否启用
* 登录名	<input type="text" value="sAMAccountName"/>	<input checked="" type="checkbox"/>
姓名	<input type="text"/>	<input type="checkbox"/>
手机号	<input type="text"/>	<input type="checkbox"/>
邮箱	<input type="text"/>	<input type="checkbox"/>

同步策略 同步新建用户 覆盖已有用户 同步删除用户

默认角色

默认用户组

参数	参数说明
自动同步	开启后，将按“自动同步周期”将AD认证服务器上的用户自动同步到堡垒机用户列表中。 如果需要手动导入，详情请参见新增 单个用户 或 AD认证用户导入 。
自动同步周期	选择自动同步的时间周期，取值范围4~168小时。

用户指南

参数	参数说明
同步内容	支持同步 登录名、姓名、手机号、邮箱 ，登录名为必选同步项。
同步策略	同步策略内容： <ul style="list-style-type: none">• 同步新建用户：如果当次同步AD用户，发现有AD认证服务器上的用户不在堡垒机用户列表中，则在堡垒机新建这个用户，认证方式为“跟随系统”。• 覆盖已有用户：<ul style="list-style-type: none">- 如果登录名重复，则刷新用户信息，如已有本地认证，保持本地密码不变。- 如果登录名不重复，但手机号重复，则导入为新的用户、更新手机号等信息，同时将原来用户的手机号置为空。• 同步删除用户：如果当次同步AD用户，发现有堡垒机内的AD用户不在AD认证服务器中，则在堡垒机将这个用户事件记为“AD用户源已删除”、用户状态置为“锁定”。
默认角色	同步用户后，为同步至堡垒机的用户添加角色，默认为“访问角色”。
默认用户组	同步用户后，为同步至堡垒机的用户添加用户组，默认为空。

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

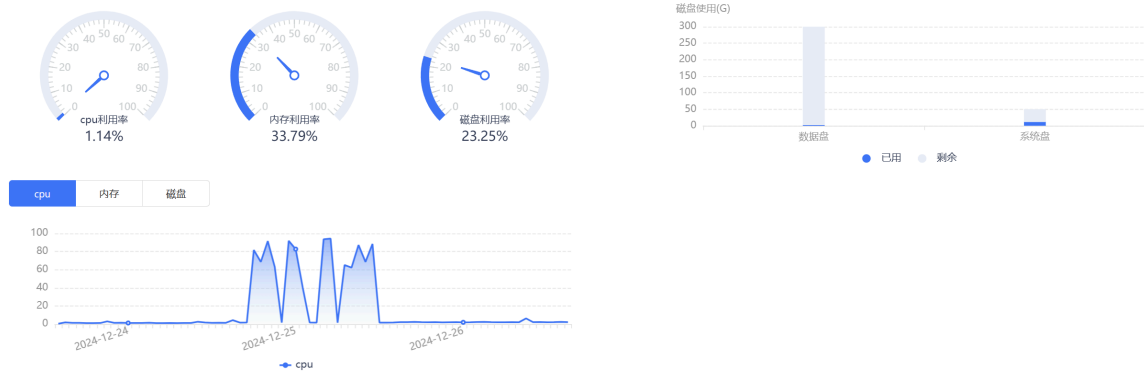
1. 使用管理角色账号登录云堡垒机。

用户指南

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。

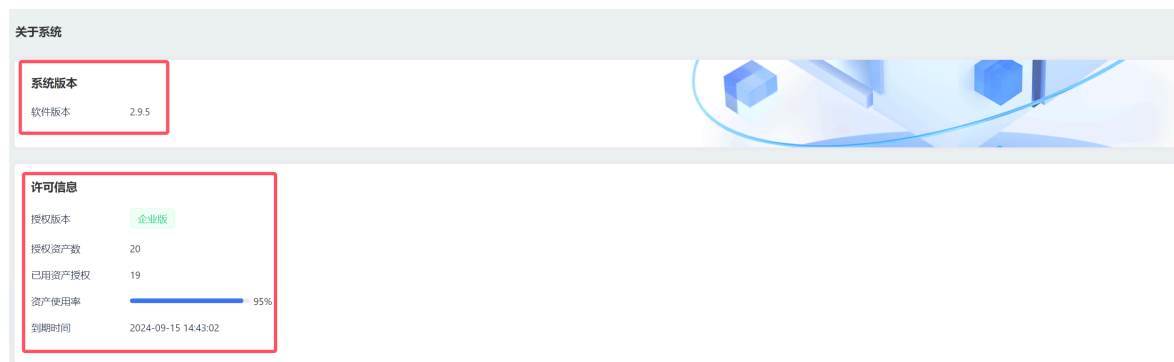
系统监控可查看堡垒机的“CPU利用率”、“内存利用率”和“磁盘利用率”的情况，每1个小时记录一次数值。

系统监控



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。



会话日志

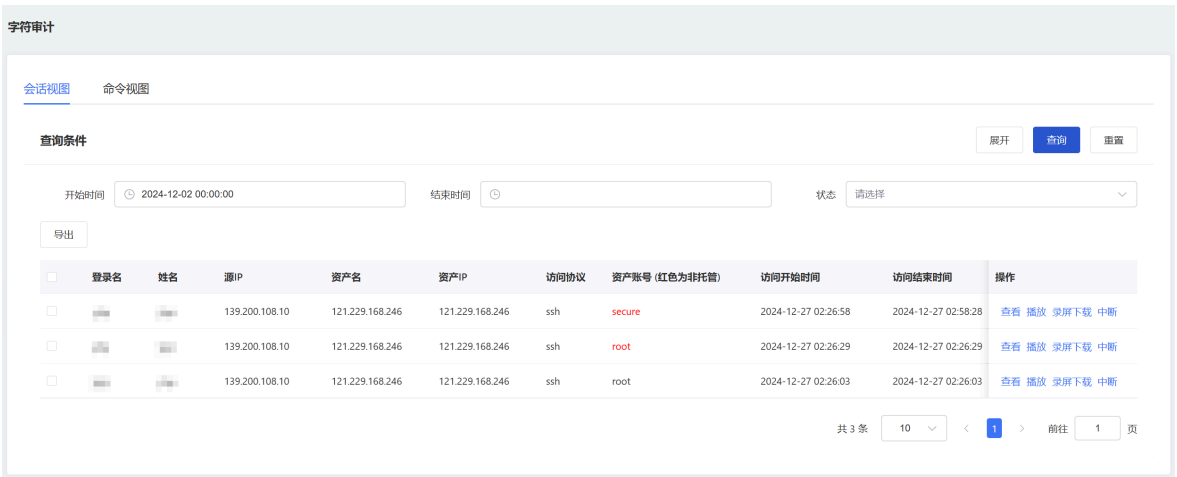
字符审计

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。

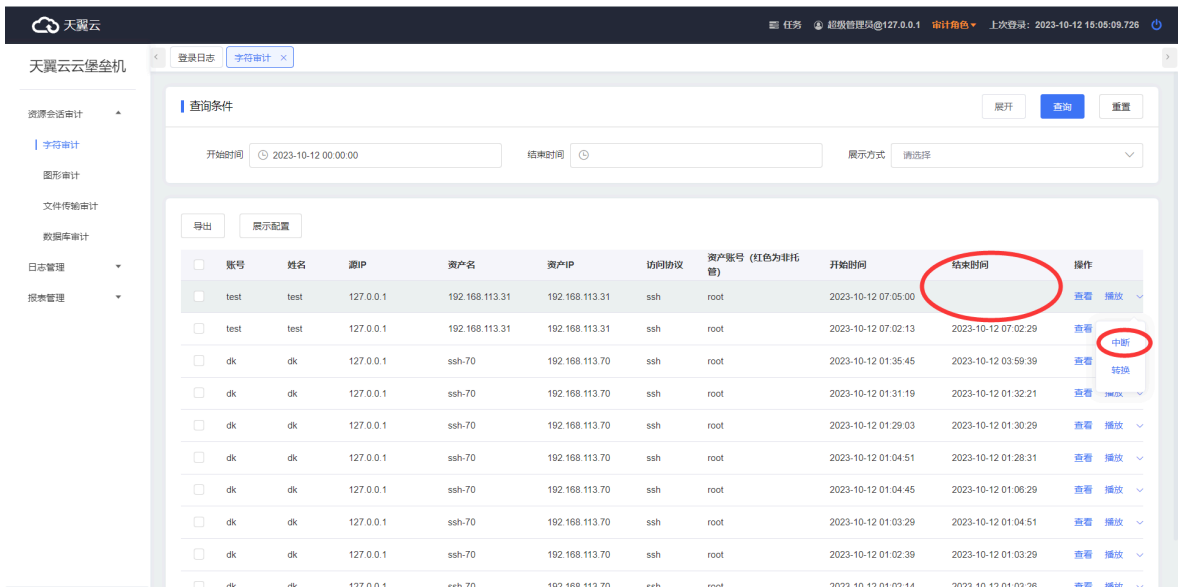
操作步骤

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。

用户指南



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。



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。

操作步骤

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。

用户指南

账号	姓名	源IP	资产名	资产IP	访问协议	资产账号 (红色为非托管)	访问开始时间	访问结束时间	操作
test	test	127.0.0.1	tx	192.168.121.219	rdp(desktop)	flc4a1administrator	2023-10-12 01:02:21	2023-10-12 01:02:46	播放 键盘
test	test	127.0.0.1	tx	192.168.121.219	rdp(desktop)	flc4a1administrator	2023-10-12 01:01:22	2023-10-12 01:02:11	播放 应用
test	test	127.0.0.1	tx	192.168.121.218	rdp(desktop)	flc4a1administrator	2023-10-11 13:30:52	2023-10-11 13:31:05	播放 应用
test	test	127.0.0.1	tx	192.168.133.219	rdp(desktop)	1212	2023-10-11 13:27:10		播放 中断
test	test	127.0.0.1	tx	192.168.121.219	rdp(desktop)	flc4a1administrator	2023-10-11 07:57:33	2023-10-11 07:58:09	播放 键盘
test	test	127.0.0.1	tx	192.168.121.219	rdp(desktop)	flc4a1administrator	2023-10-11 02:05:48	2023-10-11 02:29:21	播放 键盘
dk	dk	127.0.0.1	219	192.168.121.219	rdp(desktop)	flc4a1administrator	2023-10-10 13:09:32	2023-10-10 13:09:38	播放 键盘
test	test	127.0.0.1	tx	192.168.121.219	rdp(desktop)	administrator	2023-10-10 12:47:04	2023-10-10 12:47:10	播放 键盘
test	test	127.0.0.1	tx	192.168.121.219	rdp(desktop)	administrator	2023-10-10 12:38:01	2023-10-10 12:38:05	播放 键盘
test	test	127.0.0.1	tx	192.168.121.219	rdp(desktop)	administrator	2023-10-10 12:37:24	2023-10-10 12:37:29	播放 键盘

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。

操作内容

- 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。

用户指南

查看

×

结果

▼

🕒 2024-05-08 15:48:27

🕒 结束时间

🔍

🔄

<input type="checkbox"/>	操作时间	操作命令	文件大小(KB)	策略动作	结果	操作
<input type="checkbox"/>	2024-05-08 15:48:27	访问目录/root	0	允许	执行成功	查看
<input type="checkbox"/>	2024-05-08 15:48:36	访问目录/	0	允许	执行成功	查看
<input type="checkbox"/>	2024-05-08 15:48:40	访问目录/home	0	允许	执行成功	查看
<input type="checkbox"/>	2024-05-08 15:48:42	访问目录/home/install	0	允许	执行成功	查看
<input type="checkbox"/>	2024-05-08 15:51:34	访问目录/opt	0	允许	执行成功	查看

共 6 条 < **1** > 前往 页

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。

操作步骤

- 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。

数据库审计

[会话视图](#) 命令视图

查询条件 展开 查询 重置

开始时间 结束时间 状态

导出

<input type="checkbox"/>	登录名	姓名	资产 IP	数据库类型	数据库名	数据库用户 (红色为非托管)	客户端类型	开始时间	结束时间	操作
暂无数据										

共 0 条 < **1** > 前往 页

系统日志

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。

操作步骤

- 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。

详情



登录用户名	qgf	时间	2024-05-08 15:37:29
登录源IP	██████████	认证方式	静态认证
登录方式	web	结果	成功

协议类型	资源名	资产账号	访问时间	操作
------	-----	------	------	----

暂无数据

共 0 条 < 1 > 前往 1 页

关闭

- 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。

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。

操作步骤

- 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。

运维使用手册

登录堡垒机

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。

前提条件

管理员已添加该用户。

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。

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。

2. 选择认证方式为“本地认证”或“AD认证”。
3. 输入系统用户账号和密码，输入图形验证码。
4. 在弹出的对话框中选择绑定的双因子认证方式，若未开启双因子认证则跳过该步骤。

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。
- 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。

5. 单击“确定”，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。

运维环境设置

在使用堡垒机之前，您需要先下载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。

使用限制

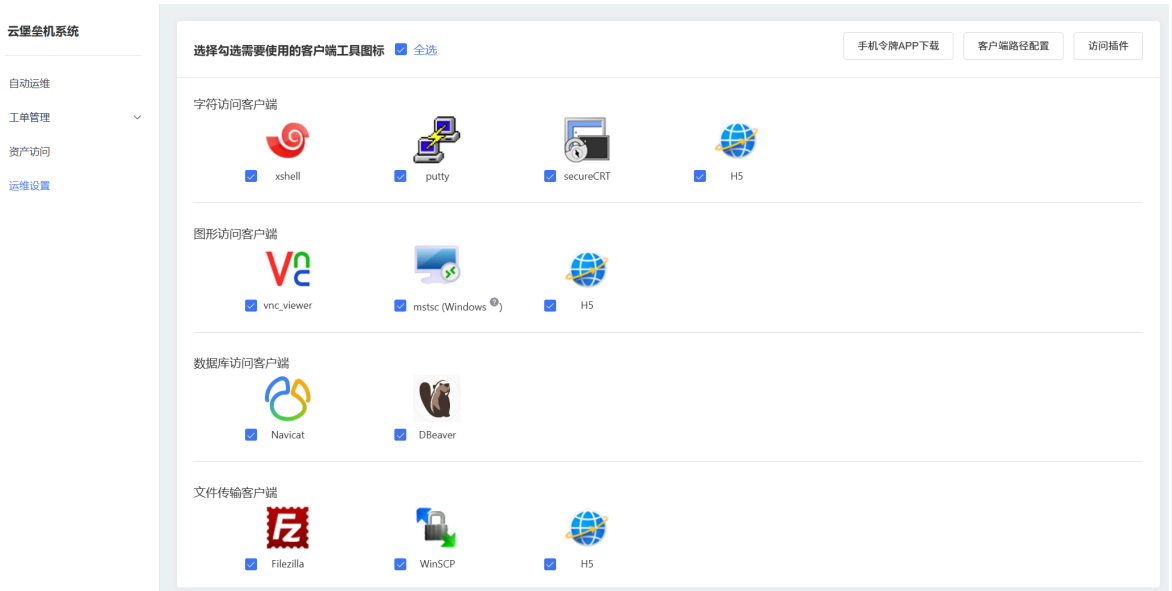
支持的运维终端操作系统、支持的运维客户端软件，请参见[使用限制](#)。

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。

用户指南

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

注意

- 仅Windows系统需要配置客户端路径，Mac系统无需配置。
- 仅Xshell、SecureCRT、DBeaver、Navicat、Filezilla、WinSCP需要配置路径后才可以使⽤，其他客户端工具无需配置。

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。



资产运维

在您配置好运维设置后，可在“资产访问”模块，运维已授权访问的资产。

前提条件

管理员已经成功[新增资产](#)，并通过[资产访问授权](#)或[工单审批](#)对运维人员授予访问权限。

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。

用户指南

- 选择需要访问的资产，单击“访问协议”，在右侧选择和填写相关内容后，单击需要使用的运维工具(如 xshell、putty等)，即可单点登录访问字符资产。

说明

- 仅企业版/高级版支持H5运维。标准版不支持H5运维。
- 做H5运维操作前请先放通18443端口，参见[安全组策略设置](#)。可使用telnet 堡垒机IP 18443命令验证端口是否放通。

所有 收藏夹 字符 图形 文件传输 数据库 应用 本地访问初始化

资产名称	IP 地址	资产组	资产描述	访问协议
★ osm-p8v2		test		ssh
★ osm-l8xy		test		ssh
★ KMS测试环境-KMS包周期-1.4_1		KMS		ssh
★ 堡垒机新主机镜像实例后台-2.143		堡垒机		ssh
★ 测试联通性提示				telnet ssh
★ 堡垒机测试环境代理机器--250		test,堡垒机		ssh
★ ipv6资产		堡垒机		ssh
★ linux-ssh/telnet/sftp/ftp-102		测试资产组lj		telnet ssh

用户首次使用或原堡垒机升级版本后，需前往“运维设置”，下载最新版本的访问插件

资产 IP

* 访问协议 ssh

* 选择资产账号

* 资产账号密码

窗口模式 新标签页

测试连通性

xshell putty secureCRT H5

访问图形资产

注意

MacOS系统目前仅支持使用VNC客户端或H5方式进行运维。

- 使用访问用户登录云堡垒机（原生版）。
- 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。

用户指南

3. 选择需要访问的资产，单击“访问协议”，在右侧选择和填写相关内容后，单击需要使用的运维工具(如mstsc、H5等)，即可单点登录访问图形资产。

说明

- 仅企业版/高级版支持H5运维。标准版不支持H5运维。
- 做H5运维操作前请先放通18443端口，参见[安全组策略设置](#)。可使用telnet 堡垒机IP 18443命令验证端口是否放通。

所有 收藏夹 字符 **图形** 文件传输 数据库 应用 本地访问初始化

资产名称	IP 地址	资产组	资产描述	访问协议
★ 堡垒机测试资产-rdp-153		test.堡垒机		rdp
★ 堡垒机测试资产-rdp-170		test.堡垒机		rdp
★ osm-win-test-web-server		堡垒机		rdp
★ windows-rdp-170		测试资产组lj		rdp
★ windows-rdp-170-IPV6		测试资产组lj		rdp
★ windwos-vnc-105		测试资产组lj		rdp vnc

共 6 条 10 < 1 > 前往 1 页

用户首次使用或原堡垒机升级版本后，需前往“运维设置”，下载最新版本的访问插件

资产 IP

* 访问协议 rdp

* 选择资产账号

* 资产账号密码

* 分辨率 全屏

* 显示桌面背景 否

测试连通性

vnc_viewer mstsc H5

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“文件传输”页签。

用户指南

- 选择需要访问的资产，单击“访问协议”，在右侧选择和填写相关内容后，单击需要使用的运维工具(如Filezilla、WinSCP等)，即可使用文件传输。

说明

- 仅企业版/高级版支持H5运维。标准版不支持H5运维。
- 做H5运维操作前请先放通18443端口，参见[安全组策略设置](#)。可使用telnet 堡垒机IP 18443命令验证端口是否放通。
- 不支持传输大小超过1G的超大文件，建议分批次上传/下载文件，或通过客户端工具传输文件。
- 请务必确认您传输的文件不包含任何敏感数据（如密码、密钥、身份证号等）、恶意代码（如病毒、木马、脚本后门等）或未授权的受控信息。如需对文件内容进行安全检查，建议提前使用本地杀毒软件或内容检测工具进行扫描。

所有 收藏夹 字符 图形 **文件传输** 数据库 应用 本地访问初始化

资产名称	IP地址/目标地址	资产组	资产描述	访问协议
★ KMS测试环境-KMS包周期-1.4_1		KMS		sftp
★ 堡垒机新主机镜像实例后台-2.143		堡垒机		sftp
★ 测试联通性提示				ftp sftp
★ 堡垒机测试环境代理机器--250		test.堡垒机		sftp
★ linux-ssh/telnet/sftp/ftp-102		测试资产组lj		ftp sftp
★ 3.16		测试资产组lj		sftp

共 6 条 10 < 1 > 前往 1 页

用户首次使用或原堡垒机升级版本后，需前往“运维设置”，下载最新版本的访问插件

资产 IP

* 访问协议 sftp

* 选择资产账号

* 资产账号密码

测试连通性

Filezilla WinSCP H5

访问数据库资产

方式一：堡垒机单点登录

说明

堡垒机单点登录运维数据库仅适用于Windows系统用户，对于Mac系统请使用[方式二：“本地访问初始化”登录](#)。

- 使用访问用户登录云堡垒机（原生版）。
- 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。

用户指南

- 选择需要访问的资产，单击“访问协议”，在右侧选择和填写相关内容后，单击需要使用的运维工具(如 Navicat、DBeaver等)，即可单点登录访问数据库资产。

说明

支持纳管的数据库请参考：[使用限制](#)章节。

所有 收藏夹 字符 图形 文件传输 数据库 应用 本地访问初始化

资产名称	IP 地址	资产组	资产描述	访问协议
★ 170达梦				db
★				db
★				db
★			sadf	db
★ db-mysql-102		测试资产组lj		db
★ db-oracle-102		测试资产组lj		db
★ cyj-drds				db
★ 数据库访问				db
★ 开发环境数据库-PG		堡垒机		db
★ ipv6-mysql				db

共 18 条 < 1 2 > 前往 页

用户首次使用或原堡垒机升级版本后，需前往“运维设置”，下载最新版本的访问插件

资产 IP

* 访问协议 db

* 选择资产账号

* 资产账号密码

* 数据库类型 dameng

* 数据库名 DMSERVER

* 端口 5236

测试连通性

Navicat DBeaver(Windows)

方式二：“本地访问初始化”登录

- 运维人员登录堡垒机。
- 左侧菜单选择“资产访问”。

用户指南

- 在资产访问页面，单击“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“本地访问初始化成功”。

“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。

说明

- 支持纳管的数据库请参考：[使用限制](#)章节。
- 做本地访问初始化操作前请先放通8765端口，参见[安全组策略设置](#)。可使用telnet 堡垒机IP 8765命令验证端口是否放通。



访问应用资产

- 使用访问用户登录云堡垒机（原生版）。
- 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。
- 选择需要访问资产，单击需要使用的访问协议，在右侧选择相关内容，单击需要使用的运维工具(如Chrome等)，即可单点登录访问应用资产。

工单管理

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。

约束条件

已被纳入[审批规则](#)的用户名单内。

创建工单

- 使用运维用户登录云堡垒机。
- 在左侧导航栏选择“工单管理 > 工单申请”，进入工单申请页面。
- 单击左上角的“新增”按钮，弹出“工单申请”对话框。
- 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”。

申请类型：

用户指南

申请命令授权

审批通过后，具备执行权限，在有效期内可重复执行。

参数		说明
基本信息	工单名称	输入您待提交工单的名称。
	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： <ul style="list-style-type: none">• 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	选择模式	取值范围： <ul style="list-style-type: none">• 全部资产• 选择资产（组）
	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。
	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。 *协议 [Ⓢ] 服务 <input type="radio"/> 默认全部 <input checked="" type="radio"/> 选择服务 <input type="checkbox"/> ssh <input type="checkbox"/> telnet <input type="checkbox"/> sftp <input type="checkbox"/> ftp <input type="checkbox"/> x11 <input checked="" type="checkbox"/> rdp <input type="checkbox"/> vnc <input type="checkbox"/> 应用 <input type="checkbox"/> 数据库 rdp允许选项 <input checked="" type="checkbox"/> 全选 <input checked="" type="checkbox"/> 剪贴板下载文字 <input checked="" type="checkbox"/> 剪贴板上传文字 <input checked="" type="checkbox"/> 剪贴板下载文件 <input checked="" type="checkbox"/> 剪贴板上传文件 <input checked="" type="checkbox"/> 磁盘映射
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。

用户指南

参数		说明
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。

申请自动执行

审批通过后，由系统自动立即执行，并在工单记录执行结果。

参数		说明
基本信息	工单名称	输入您待提交工单的名称。
	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类型： <ul style="list-style-type: none">• 字符命令授权• 数据库命令授权
资产账号	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。
敏感命令	待执行命令	单条可执行命令。审批通过后，由堡垒机系统 立即自动执行 ，授权为单次。
其他	描述	填写申请工单的相关描述。

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[审批规则](#)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。

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。

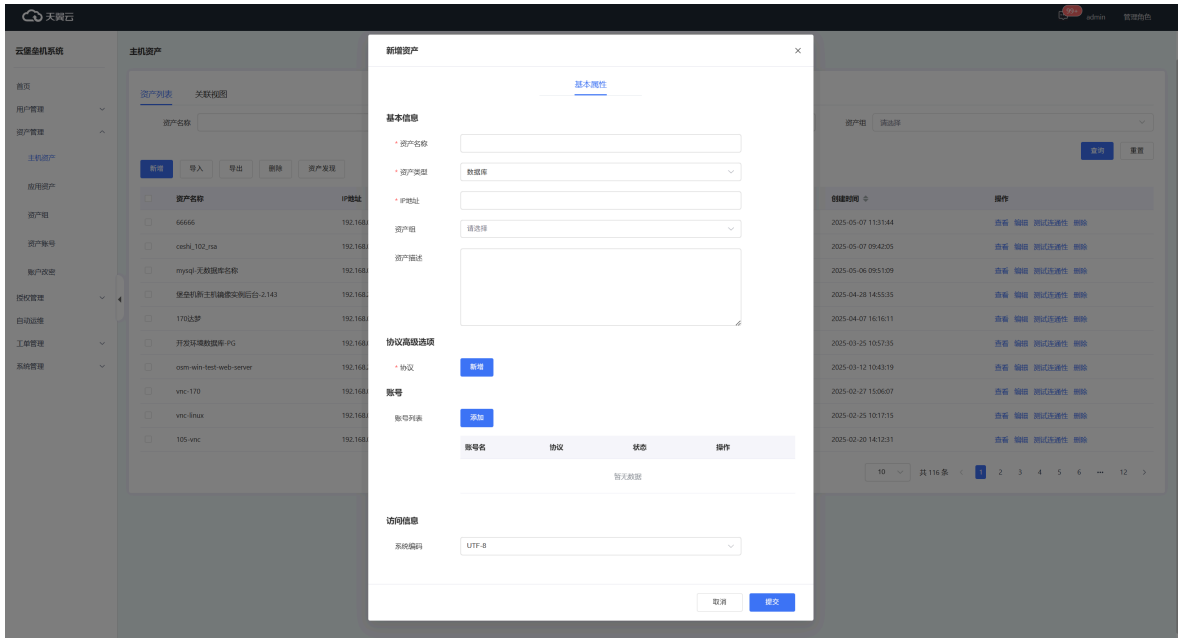
操作步骤

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”。

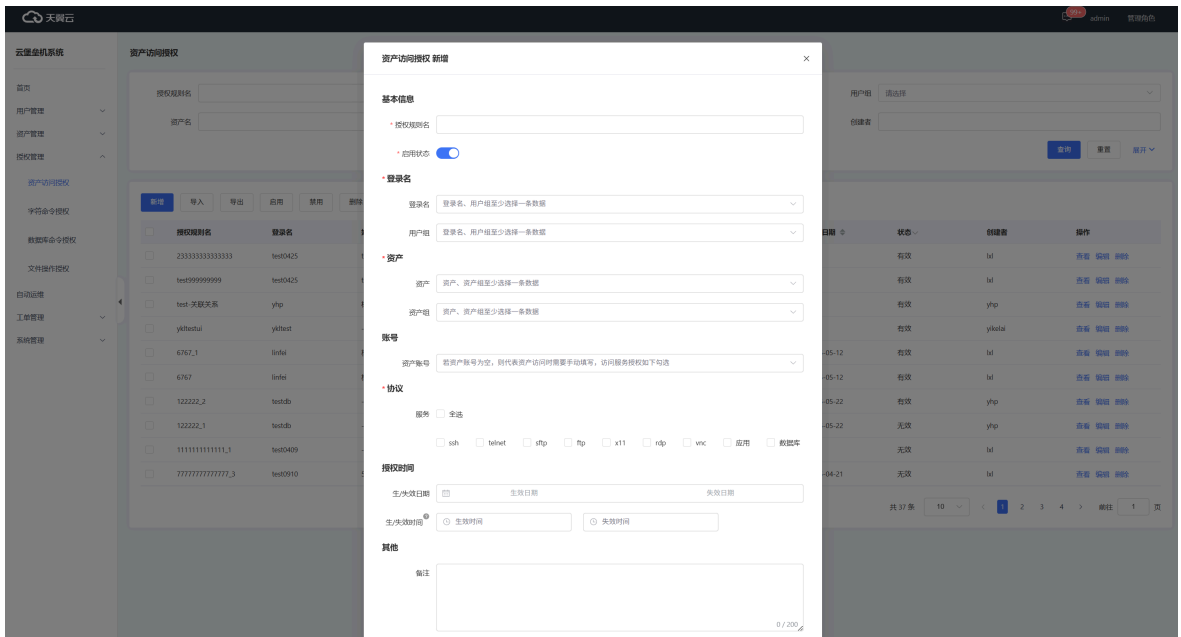
最佳实践

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>资产访问授权”，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。



最佳实践

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“本地访问初始化成功”。

说明

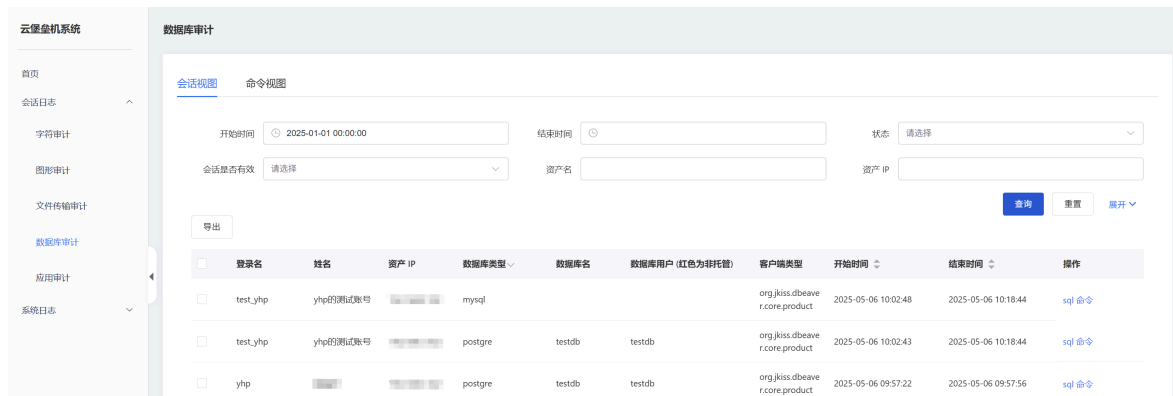
做本地访问初始化操作前请先放通8765端口，参见[安全组策略设置](#)。可使用telnet **堡垒机IP** 8765命令验证端口是否放通。



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。



收敛资产运维暴露面

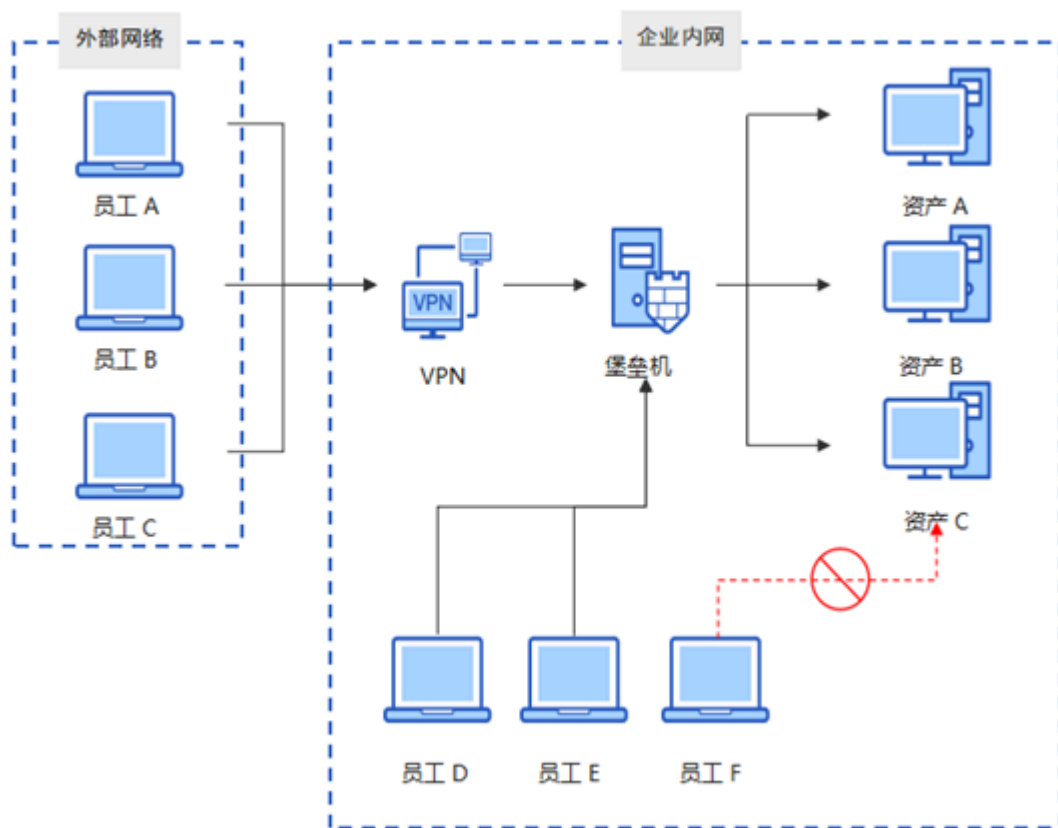
背景

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。

资产运维细粒度权限管控

背景

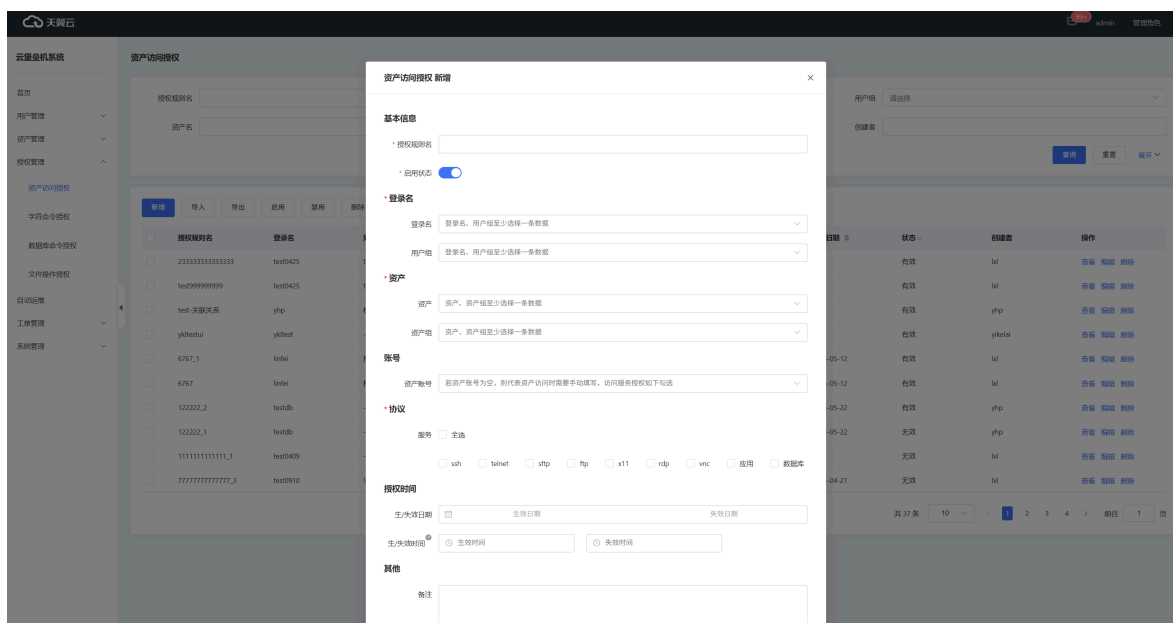
传统的权限网格比较粗放，围城内的大部分用户默认具有超范围的权限，外围用户通过VPN连接企业网络后，也默认具备“围城内用户”的身份和权限，越权访问、敏感操作比比皆是且无从管控，发生数据泄露等安全事故后也难以审计追溯具体详情。

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>资产访问授权”。
- 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。



最佳实践

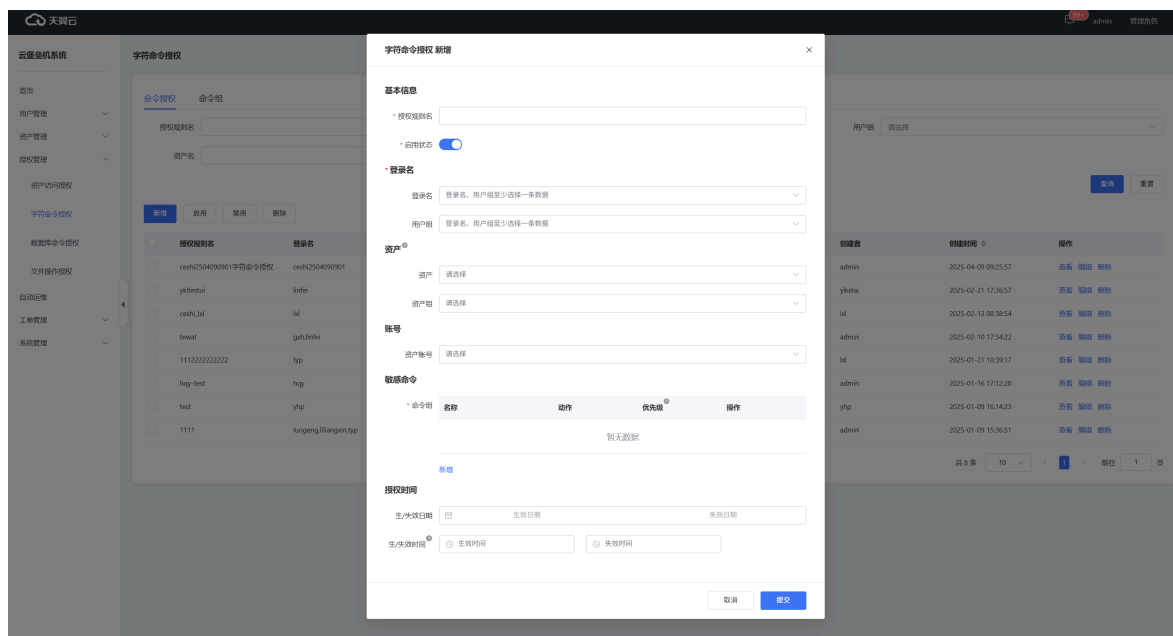
4、配置完成后，表示主账号(人员账号)可以在指定有效期内，使用指定的资产账户访问指定的资产。

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。

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
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	本地初始化获取配置端口	需通过客户端工具运维时，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

如何配置云堡垒机的安全组？

参考[安全组策略设置](#)。

常见问题

云堡垒机是否支持纳管非天翼云服务器？

支持。

只要与云堡垒机网络可达并且协议支持，且云服务器操作系统在云堡垒机支持的[操作系统清单](#)，就可以通过天翼云云堡垒机纳管。

云堡垒机是否支持内网访问运维页面？

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。

订购类

云堡垒机提供了标准版和企业版，应如何选择？

企业版：适用于有数据库资产纳管需求，有运营审批需求的企业。

标准版：适用于对云服务器有基本运维、审计需求的中小型企业。

详细区别请参见 [云堡垒机功能特性区别](#)。

云堡垒机适配哪些远程工具？

登录方式	支持的客户端	版本
Web浏览器登录	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	Winscp	5及以上版本

常见问题

登录方式	支持的客户端	版本
	Filezilla	3及以上版本
数据库运维	Navicat	11、12、15、16、17
	DBeaver	22、23、24
	HeidiSQL	10.0及以上版本
	说明 需要自行下载客户端并使用。	
	PL/SQL Developer	14.0.2
	说明 需要自行下载客户端并使用。	
图形运维	Vnc_viewer	堡垒机客户端自带
	MSTSC	6.0及以上版本

云堡垒机支持运维哪些资源？

支持数据库和服务器资源，具体限制如下：

- 数据库限制

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

- 服务器限制：支持SSH、TELNET、RDP、VNC、FTP、SFTP协议类型的Windows或Linux主机。

云堡垒机是否支持纳管多个子网的资产？

支持，前提是网络互通。

同一账号可以购买多个云堡垒机吗？

同一个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。

常见问题

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[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。

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

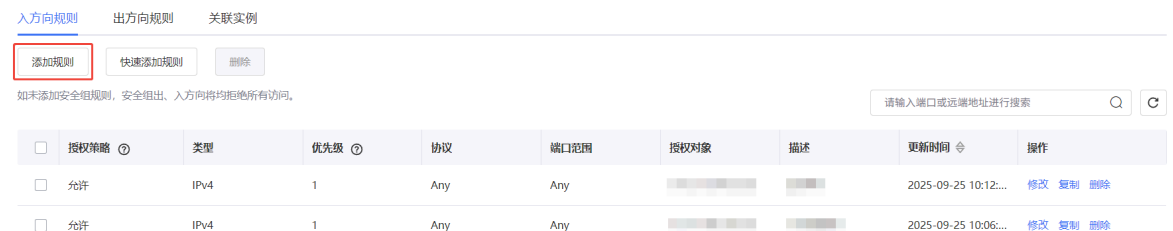
1. 登录管理控制台。
2. 在产品服务列表页，选择“网络 > 弹性IP”。
3. 在左侧导航树选择“访问控制 > 安全组”。

常见问题

4. 在安全组界面找到服务器的安全组，单击安全组操作列的“添加规则”，进入安全组详情界面。



5. 在安全组详情界面，选择“入方向规则”页签，单击“添加规则”，弹出添加规则窗口。



6. 授权对象（源地址）配置为云堡垒机的IP地址。



7. 配置完成后，单击“确定”。

访问时页面提示“请确认是否安装访问插件”如何处理？

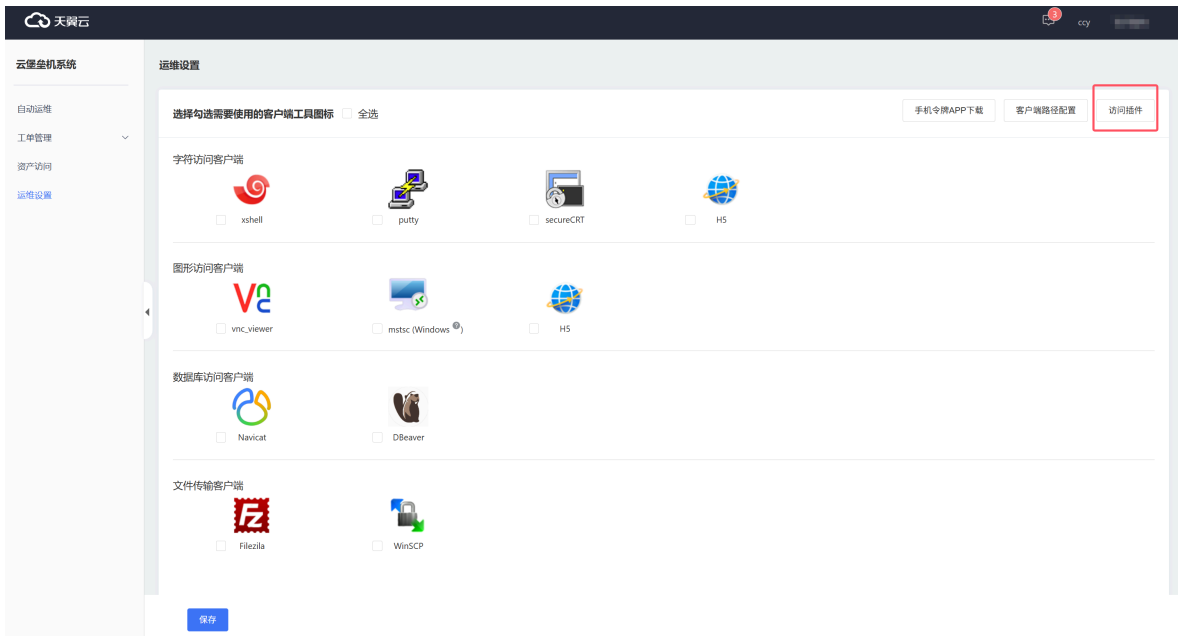
运维用户登录云堡垒机控制台后，窗口弹出“若访问失败，请确认是否安装访问插件”，这说明用户第一次在当前终端还未安装云堡垒机客户端插件，需要下载并安装。

常见问题

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、资源免密单点登录等重要功能。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。

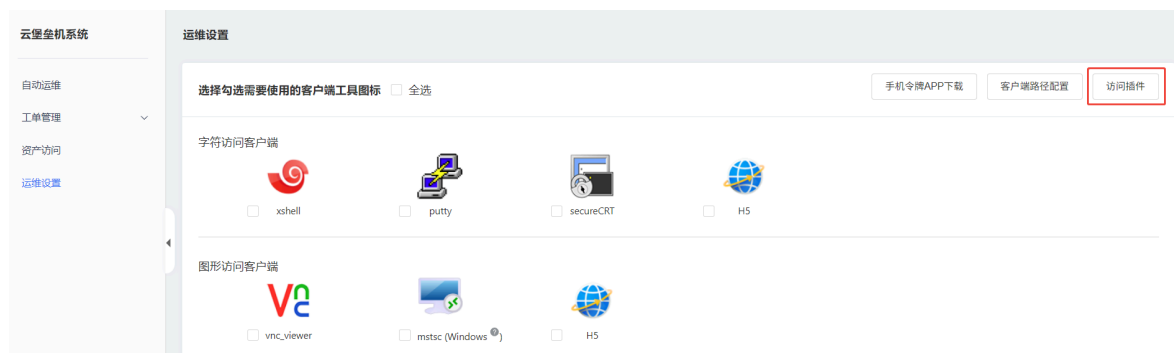
MacOS如何安装堡垒机访问插件

下载MacOS版控件

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。

常见问题

3. 单击页面右上角的“访问插件”按钮。



4. 在访问插件窗口，下载MacOS版控件到本地。

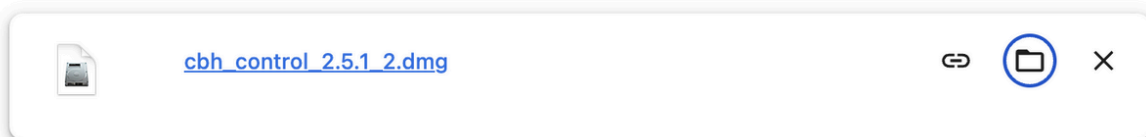


常见问题

5. 下载完成后，可以查看文件“cbh_control_xxx.dmg”。

示例：

2025年1月21日

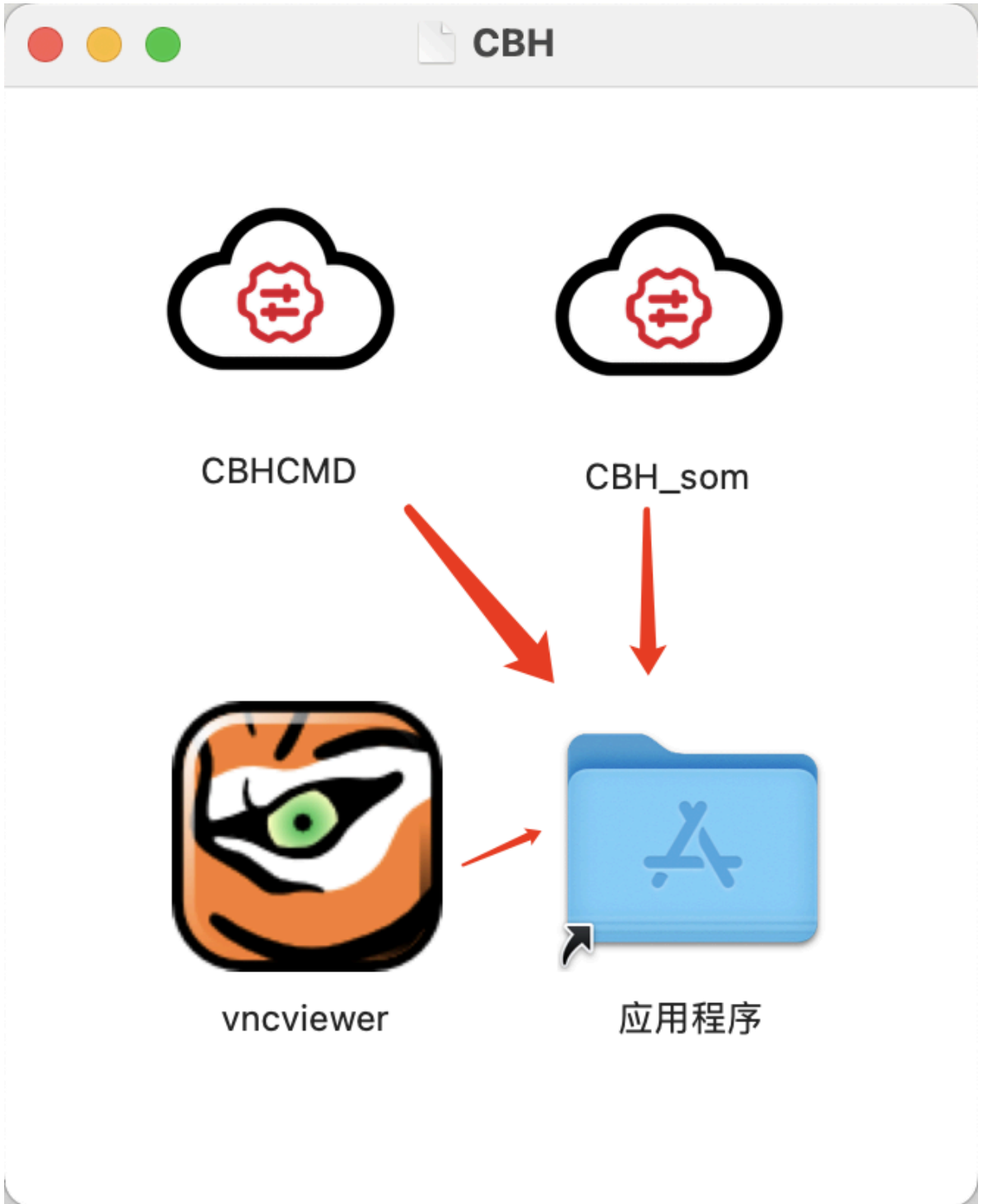


安装MacOS版控件

1. 双击下载的MacOS版控件。

常见问题

2. 在弹出的窗口中，将CBHCMD、CBH_som、vncviewer放入应用程序。



常见问题

3. 在安装过程中出现的权限申请，需要选择“允许”，如果点击其他地方或点击不允许，弹框消失后，只能卸载重装插件。

允许插件添加代理配置：在如下窗口中，单击“允许”。



允许系统扩展：在如下窗口中，单击“打开系统设置”。



系统扩展已被阻止

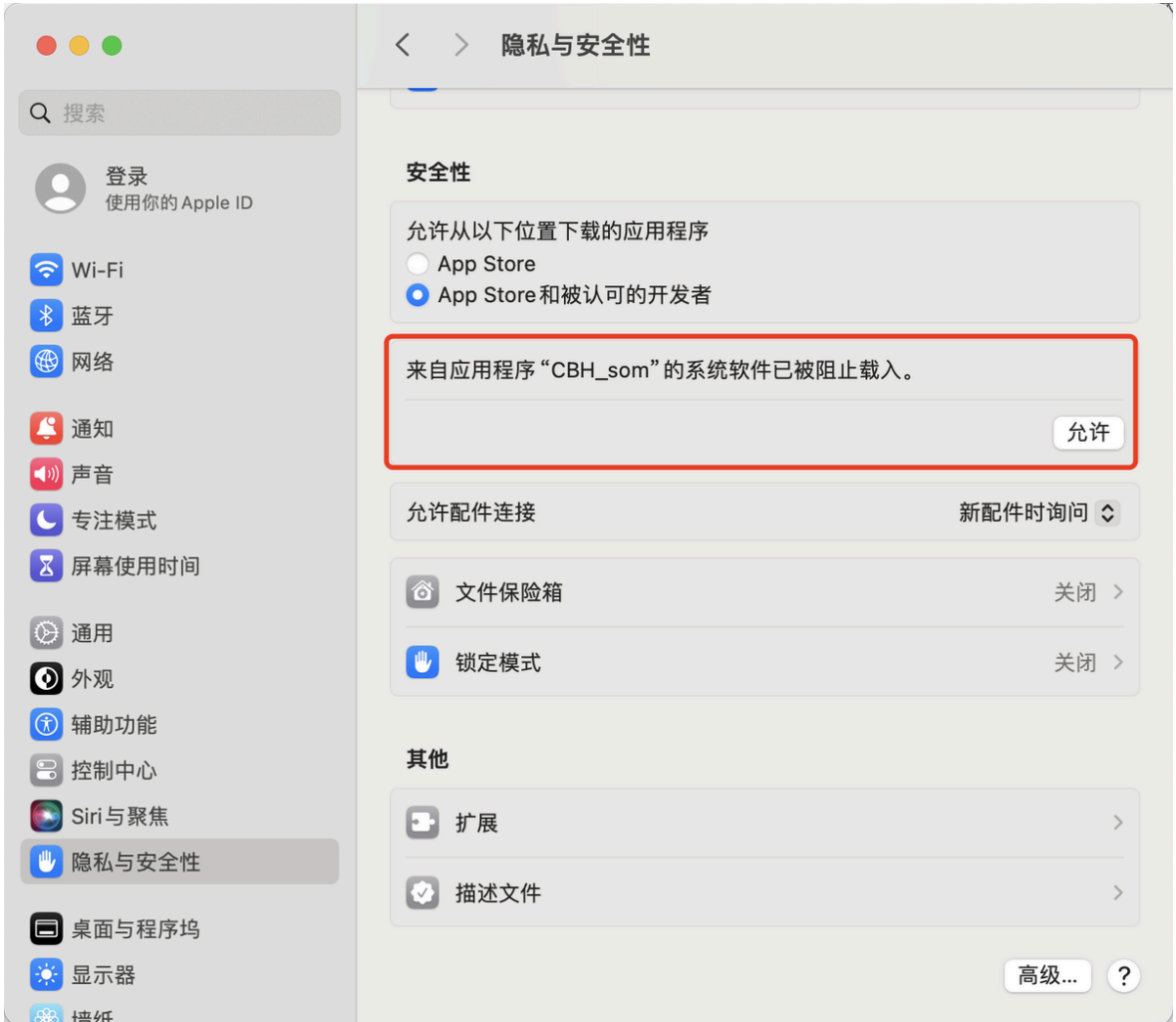
应用程序“CBH_som”尝试载入新的系统扩展。如果你想要启用这些扩展，请打开“系统设置”中的“隐私与安全性”。

打开系统设置

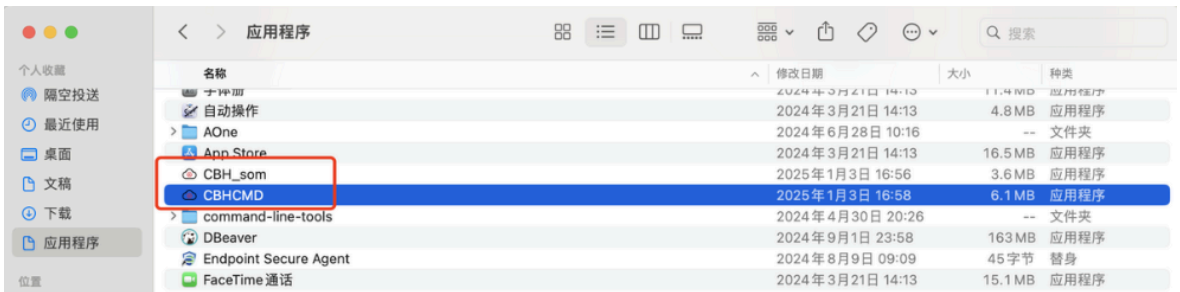
好

在如下页面，单击“允许”，允许应用程序“CBH_som”的系统软件载入。

常见问题



4. 安装完成后，能在应用程序里看到已安装的插件。



常见问题

5. 若使用了本地初始化功能，在“设置 > 网络 > 过滤条件”里能看到名为CBHAppProxy的透明代理状态为已启用。

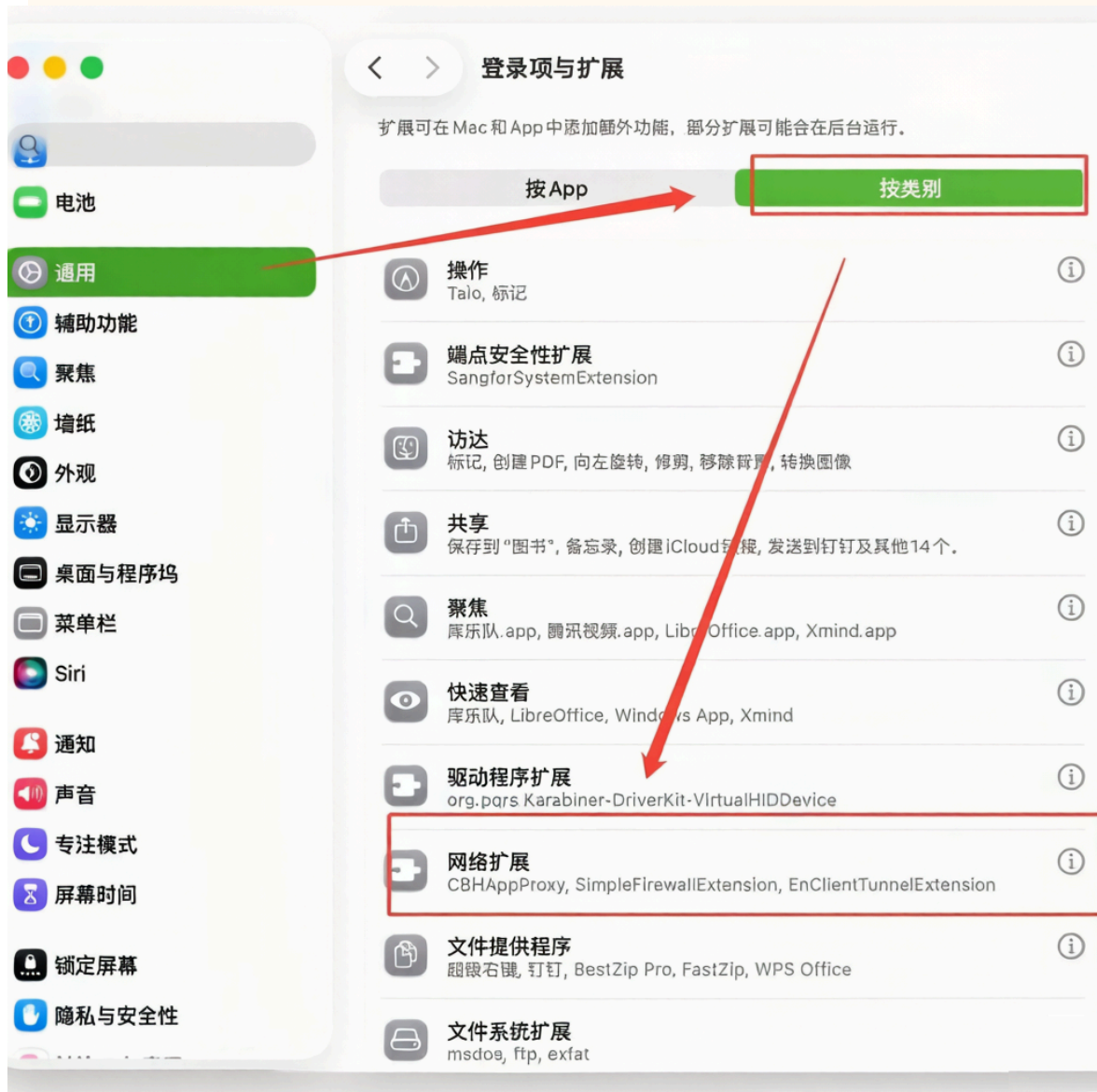


若无法拉起CBHAppProxy的透明代理，请在“通用 > 登录项与扩展 > 网络拓展”中启用CBH_som，需要卸载重装插件，并确保安装过程中权限申请均选择“允许”。

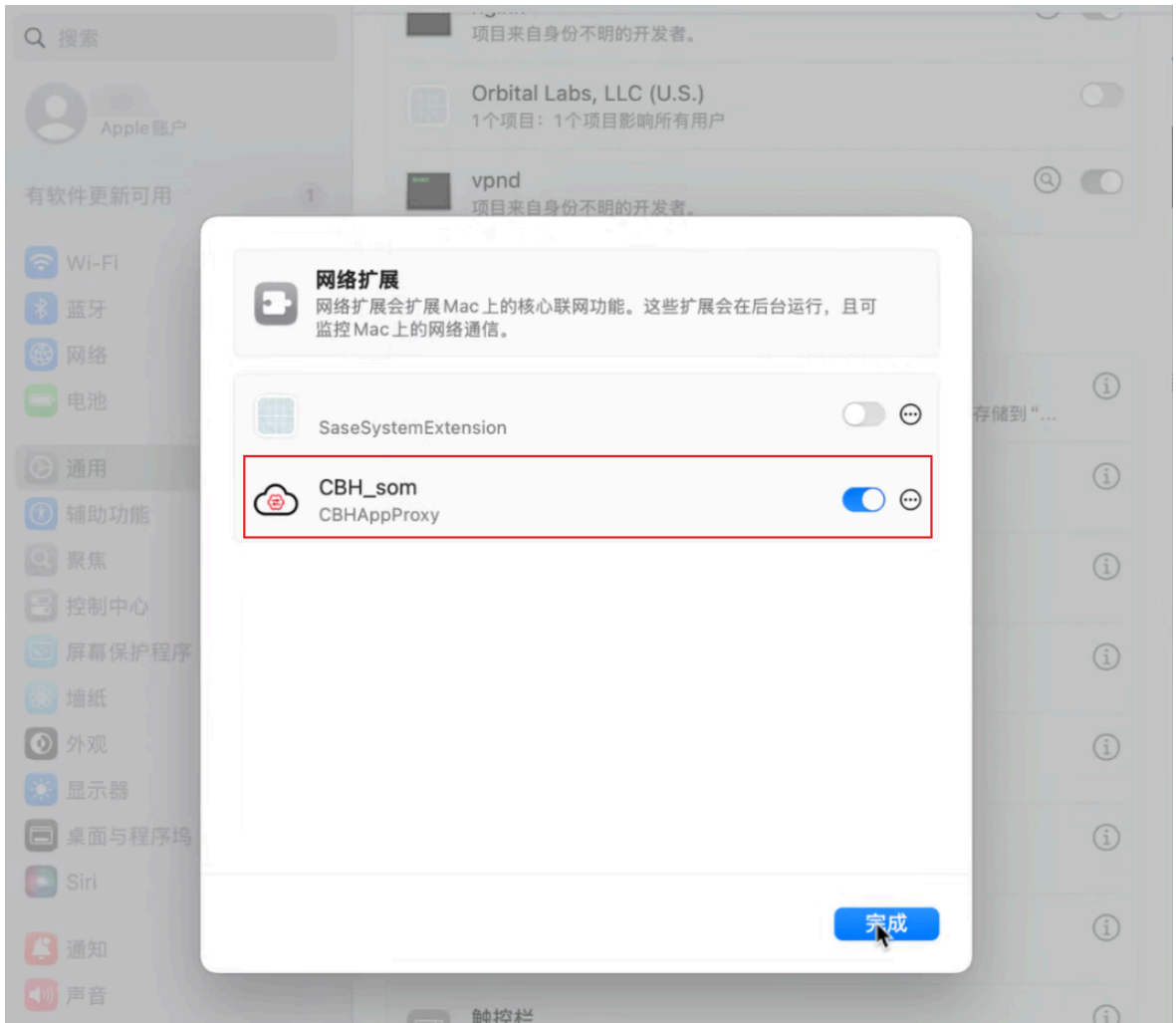
常见问题

注意

高版本的Mac需要手动打开网络拓展才能正常拉起代理，如下图所示。



常见问题



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：

- 忘记密码，连续输错N次密码后账号自动锁定。
- 账号、密码超过有效期，自动锁定。
- 账号空闲超过阈值未登录系统。
- 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。

常见问题

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。

重置密码

×



验证方式

短信 邮箱

* 登录名

手机号码

动态验证码

获取验证码

下一步

3. 输入新登录密码，点击确定后，密码重置成功。

常见问题

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。

自助解锁



自助解锁流程图，包含三个步骤：1. 验证身份，2. 密码过期锁定修改密码，3. 解锁成功。当前显示的是验证身份步骤，包含用户名、邮箱、图形验证码和动态验证码输入框，以及一个“下一步”按钮。

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。

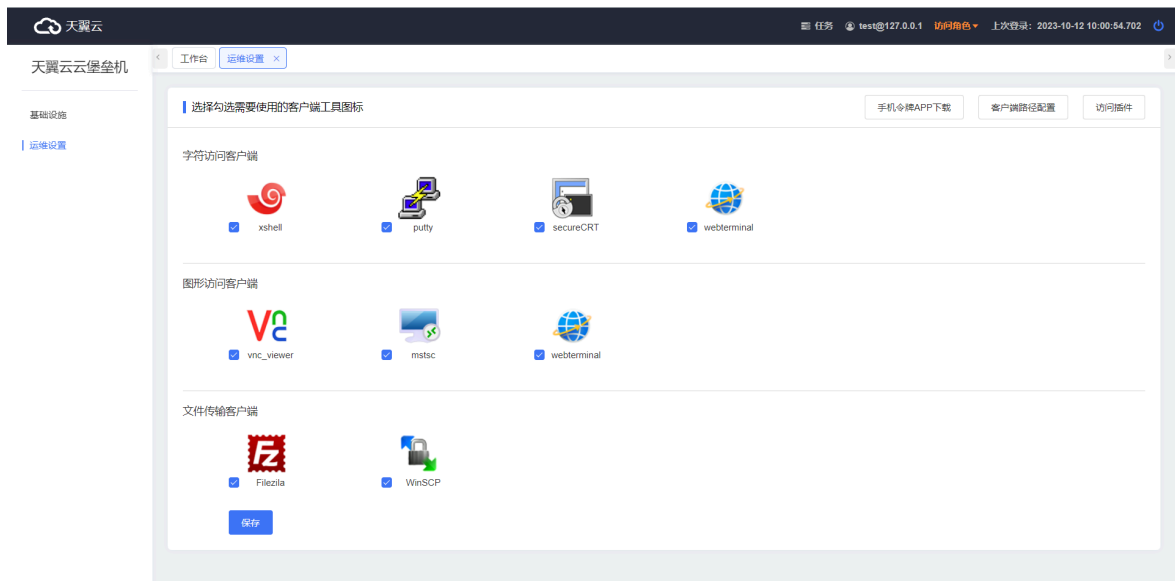
无法正常启用客户端运维工具运维资产

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。

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。

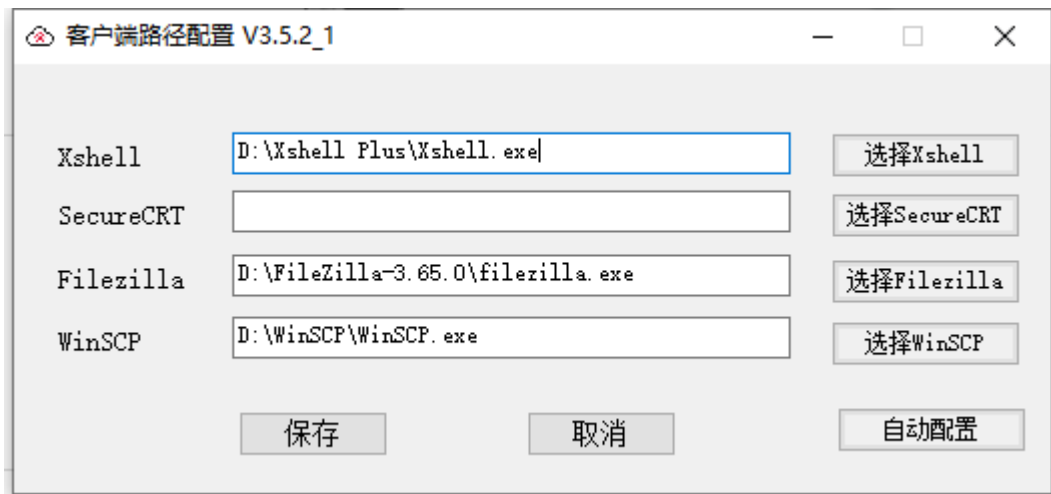
常见问题



确认是否已正确安装并配置客户端工具。

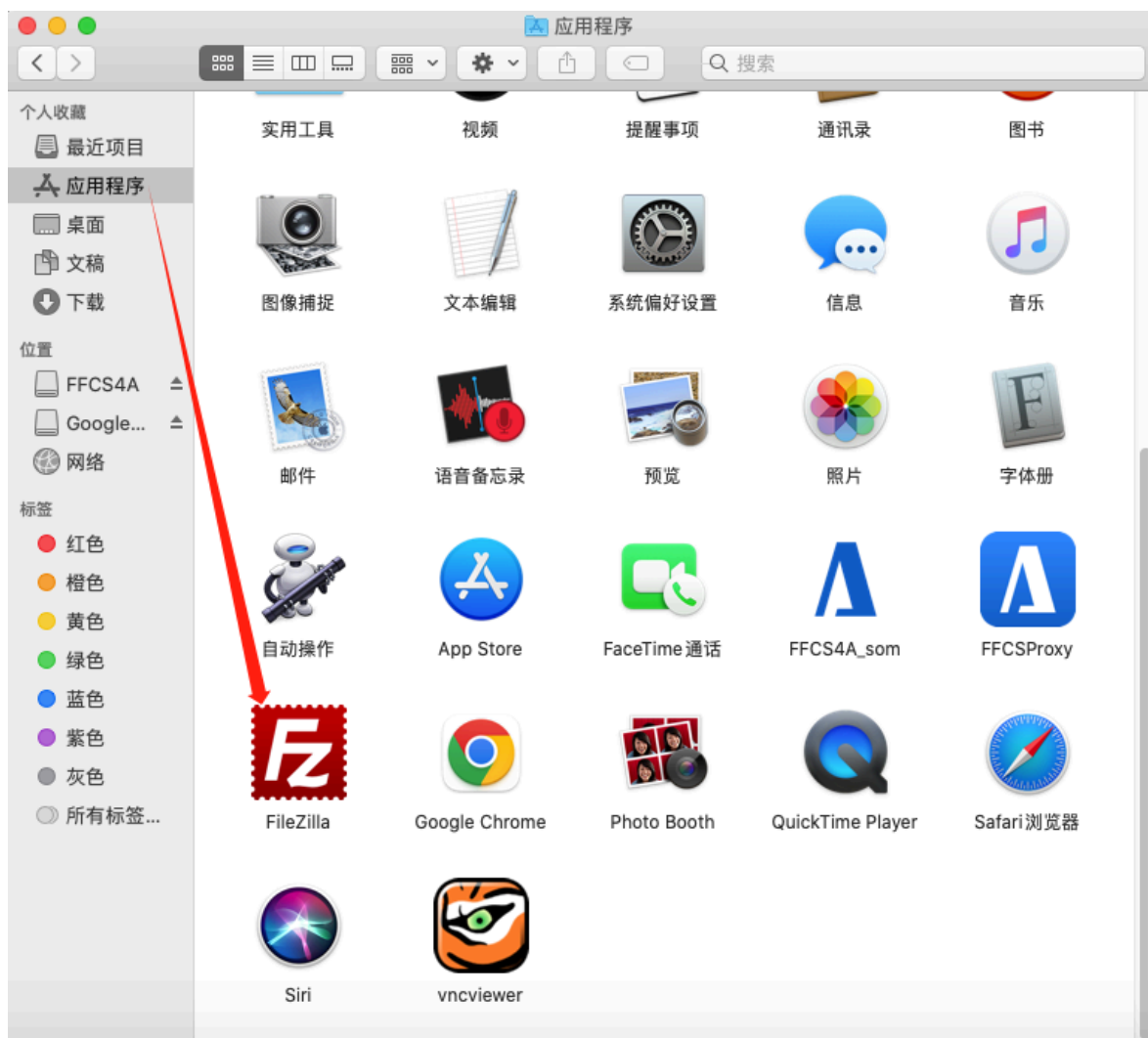
云堡垒机不提供Xshell、vnc等客户端运维工具下载，用户需要自行去官网下载安装需要使用的软件。

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。

常见问题



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？

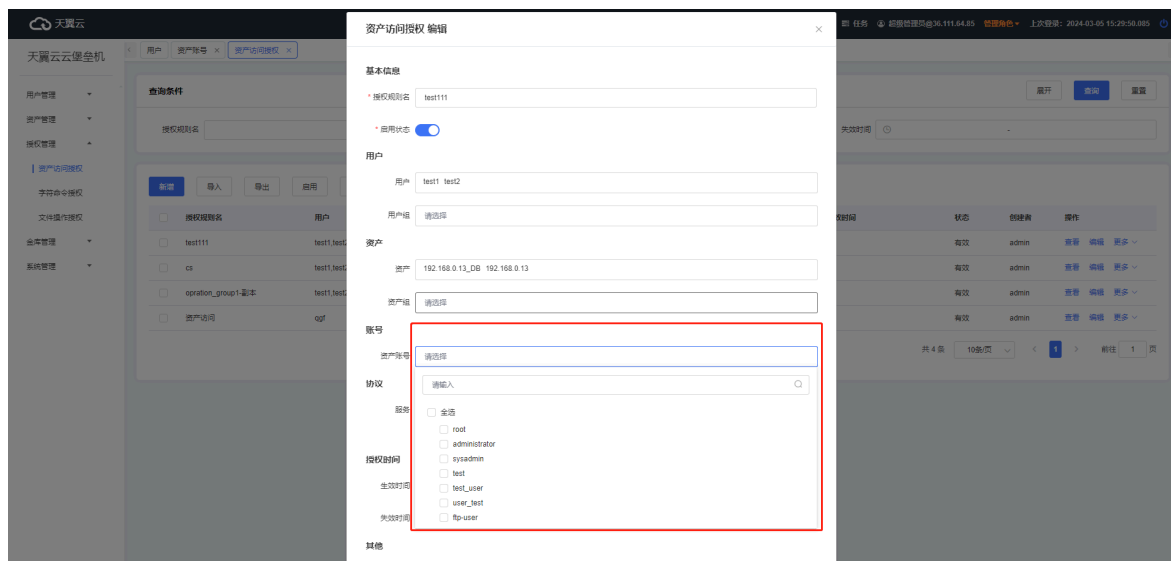
访问资产提示“登录设备失败，设备账号或密码错误”，如果使用托管的账号密码，则需联系资产管理员，确认托管的账号和密码是否正确。

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 页面，按资产IP或资产名搜索需要修改资产账号密码的资产。
- 3、点击资产数据操作栏【编辑】，在账号项选择需要修改的资产账号点击【编辑】。
- 4、进入 资产管理>资产账号 页面，选择需要修改的资产账号点击【编辑】。
- 5、更新资产账号、密码及应用的协议。

常见问题



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：

- 运维终端已正确安装访问插件，并配置访问路径；
- 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。

常见问题

天翼云 控制中心 郴州

网络控制台

- 虚拟私有云
- 子网
- 弹性IP
- 访问控制
- 安全组**
- 操作日志

安全组

默认安全组详情

导出规则

名称	default	ID	28f9ebab-d286-4499-b192-7761d6396a24
描述	Default security group	企业项目	default

入方向规则 出方向规则 关联实例

添加规则 快速添加规则 入方向规则: 4

请输入端口或远端地址进行搜索

授权策略	类型	协议	端口范围/ICMP类型	远端	描述	操作
允许	IPv4	TCP	3389	0.0.0.0/0		修改 删除
允许	IPv4	TCP	22	0.0.0.0/0		修改 删除
允许	IPv4	Any	Any	默认安全组 (28f9ebab-...		修改 删除
允许	IPv4	ICMP	Any	0.0.0.0/0		修改 删除