云堡垒机（原生版）

用户操作指南

天翼云科技有限公司

目录

1 产品概述

1.1 产品定义

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

产品功能

- 账号管理：账号管理包括运维用户账号管理和资产账号管理。资产帐密在堡垒机内部均使用国密算法加密存储保护。
- 安全认证：支持双因子身份认证，运维人员认证登录后访问服务器、数据库等资产无需输入资产账号密码登录，降低帐密泄漏风险。
- 权限控制：支持集中对用户进行授权管理，支持对用户、用户组进行资产授权、操作授权，可基于授权实现细颗粒度访问控制。
- 运维工具集成：用户除了使用 web 网页运维外，用户还可使用 PuTTY、SecureCRT、Xshell、WinSCP、Mstsc 等专业运维工具完成运维。
- 操作审计：审计用户登录、系统管理、运维指令、文件传输等行为，发现运维风险，提供录像及回放功能，满足等保测评合规要求。
- 高危命令管控：运维管理员可对运维场景中的高风险行为设置管控规则，一旦运维用户操作行为触发高危命令，系统实时告警或阻断。

为什么选择云堡垒机

- **开通和使用非常便捷：**

您只需选择产品版本、实例规格、资产规格，为云堡垒机实例指定实例开通地域、配置相关网络参数即可开通。

开通完成后，您可以在控制台上快捷登入云堡垒机，管理运维您的服务器、数据库等 IT 资产。

- **满足合规性规范审查要求：**

满足《萨班斯法案》和《等级保护》系列文件中的技术审计要求。

满足等级保护、ISO/IEC27001 等对运维审计的要求。

- **云原生堡垒机更安全：**

云原生堡垒机运行操作系统及网络安全防护策略统一实现安全加固，缩小攻击面。

租户之间严格网络隔离、实例和数据隔离，各堡垒机实例环境独立，保障系统运行安全。

1.2 产品优势

- **运维高效快捷**

云堡垒机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、SQL Server、DB2、Sybase、PostgreSQL 等

WEB 访问协议：HTTP/HTTP

- **精细化权限管理**

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

降低越权操作风险

- **管控方式严格**

对于高危命令实现实时告警或阻断，对于特别重要的命令实现多人审核，避免用户进行不安全的运维操作。

支持运维账号登录 IP 地址绑定，限制登录地址，避免非授权用户登录进行重要运维操作。

- **快速开通使用**

用户根据自身业务需求，选择对应规格一键开通堡垒机实例，方便快捷。

- **安全合规**

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

1.3 产品特性

产品提供标准版和企业版三种不同版本堡垒机，下面表格为不同版本支持的功能及差异。

功能			标准版	企业版
资产管理	主机管理	支持 Windows、Linux 操作系统的服务器资产管理	√	√
	数据库管理	支持 Mysql、SqlServer、Oracle 等类型数据库资产管理及运维	×	√
	资产组管理	支持资产分组管理，按组管理资产，统一授权	√	√

	资产帐密管理	支持资产特权账号、密码集中加密存储和托管，运维整个过程不暴露资产帐密。	√	√
用户管理	双因子认证	支持帐密+手机 App 动态口令认证方式登录堡垒机。	√	√
	用户管理	统一管理运维访问用户、管理员、审计员，支持定义用户账号安全策略。	√	√
	用户组管理	支持用户分组管理，统一为分组内用户授权。	√	√
	账号安全策略	支持设置全局账号安全策略、密码策略。	√	√
授权管理	资产访问授权	支持设置用户、资产、资产账号的访问授权及管控。	√	√
	字符命令授权	支持对用户、用户组敏感命令的授权及管控。	√	√
	文件操作授权	支持对用户操作文件命令授权及管控。	√	√
资产运维	资产运维（SSH、Telnet、RDP、VNC）	支持 Mstsc、Xshell、SecureCRT、Putty 等客户端工具登录堡垒机以图形或字符方式运维资产。	√	√
	资产运维（SFTP、FTP）	支持使用本地 WinSCP、Xftp、SecureFX 等 SFTP 客户端工具登录堡垒机进行运维。	√	√

	Web 直接运维服务器	支持通过浏览器直接运维服务器、数据库资产。	√	√
	资产访问运维免帐密登录	支持通过堡垒机帐密单点登录到运维资产，运维人员无需掌握服务器、数据库等资产的帐密。	√	√
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。	√	√
金库管理	运维访问审批	运维用户运维高敏感资产可配置金库审批模式，一人操作一人监督审核。	×	√
	运维命令审批	运维用户运维资产的高危命令可配置金库模式，一人操作一人监督审核。	×	√
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。	√	√

	审计录像及回放	支持对字符、图形运维操作全程审计录像及回放。	√	√

1.4 产品应用场景

（一） 中小企业资产运维

场景说明

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

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

产品优势

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

（二）多人运维管理场景

场景说明

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

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

产品优势

- 运维高效便捷：支持 PuTTY、SecureCRT、Xshell、WinSCP、mstsc 等专业运维工具集成，提升运维效率。
- 精细化权限管理：以 4A 为核心实现用户按角色、资产授权及访问控制，最小化运维授权，降低越权操作风险。
- 安全合规：对所有运维操作集中记录，支持审计、录像及回放，满足等保测评要求，助力企业运维安全治理。

1.5 使用限制

网络访问限制

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

支持纳管的服务器限制

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

支持的数据库类型及版本限制

数据库引擎	引擎版本
Mysql	5.5,5.6,5.7,8.0
PostgreSQL	10,11,12,13
Oracle	10g,11g,12c

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
	Chrome	52.0 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
	Filezila	3 及以上版本

1.6 术语解释

资产数

资源数是同一个设备对应的需要运维的协议和应用总数。

云堡垒机实例

一个云堡垒机实例代表了一个独立运行的云堡垒机系统。

主备实例

在单机实例基础上增强高可用性。主备实例具有以下特征：

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

区域

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

可用区域

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

单点登录

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

2 计费说明

2.1 计费说明

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、购买时长计费。
实例购买时长	提供包月和包年的购买模式

计费模式

云堡垒机实例的计费模式为包月和包年计费。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 年享受 5 折优惠。

版本	资产规格	并发数	标准资费（元/个/月）	推荐云主机规格
高 级 版	20 资产	20 并发上限	999	CPU：2 核 内存：8GB 系统盘：50GB 数据盘：400GB
高 级 版	50 资产	50 并发上限	1888	CPU：4 核 内存：16GB 系统盘：50GB 数据盘：600GB
高 级 版	100 资产	100 并发上限	2999	CPU：8 核 内存：32GB 系统盘：50GB 数据盘：1000GB
高 级 版	200 资产	200 并发上限	4350	CPU：16 核 内存：32GB 系统盘：50GB 数据盘：1300GB
高 级	500 资产	500 并发上限	6230	CPU：12 核

版本	资产规格	并发数	标准资费（元/个/月）	推荐云主机规格
版				内存：64GB 系统盘：100GB 数据盘：2548GB
高 级 版	1000 资产	1000 并发上限	11100	CPU：16 核 内存：64GB 系统盘：2548GB
高 级 版	2000 资产	2000 并发上限	14000	CPU：16 核 内存：128GB 系统盘：100GB 数据盘：2548GB
高 级 版	5000 资产	2000 并发上限	20000	CPU：24 核 内存：192GB 系统盘：100GB 数据盘：4596GB
高 级 版	10000 资产	2000 并发上限	29550	CPU：32 核 内存：128GB 系统盘：100GB 数据盘：4596GB

2.2 购买云堡垒机

前提条件

- 已获取管理控制台的登录帐号与密码。
- 已购买至少一个弹性公网 IP（Elastic IP，EIP）。

注意： 一个弹性公网 IP 只能绑定一个云资源使用，云堡垒机绑定的弹性 IP 不能与其他云资源共用。

操作步骤

1. 登录管理控制台。
2. 选择“安全 > 云堡垒机（原生版）”，进入云堡垒机实例管理页面。
3. 单击右上角的“购买堡垒机”，进入产品订购页。
4. 选择“云堡垒机实例”相关参数，参数相关说明请参考下表。

参数	说明
计费模式	选择实例计费模式，仅支持“包年/包月”模式。 包年/包月是预付费模式，按订单的购买周期计费，适用于可预估资源使用周期的场景。
当前区域 可用分区	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分区。 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

参数	说明
	低网络时延、提高访问速度。
实例名称	自定义实例名称。
版本	选择标准版、企业版，各版本支持的功能清单请到产品介绍-功能特性查看。
实例规格	选择单机规格，目前标准版和企业版仅支持单机规格。
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。
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。
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。
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	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。
购买时长	选择实例使用时长。 可按月或按年购买云堡垒机。

1. 配置完成后，单击“立即购买”。

2. 进入“订单详情”页面，确认订单无误并阅读《天翼云云堡垒机服务协议》后，勾选“我已阅读并同意《天翼云云堡垒机服务协议》”，单击“提交订单”。
3. 在支付页面完成付款，返回云堡垒机控制台页面，在“云堡垒机实例”列表下查看新购买的实例。

2.3 变更资产规格

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。

注意

变更规格过程约需要 10min，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

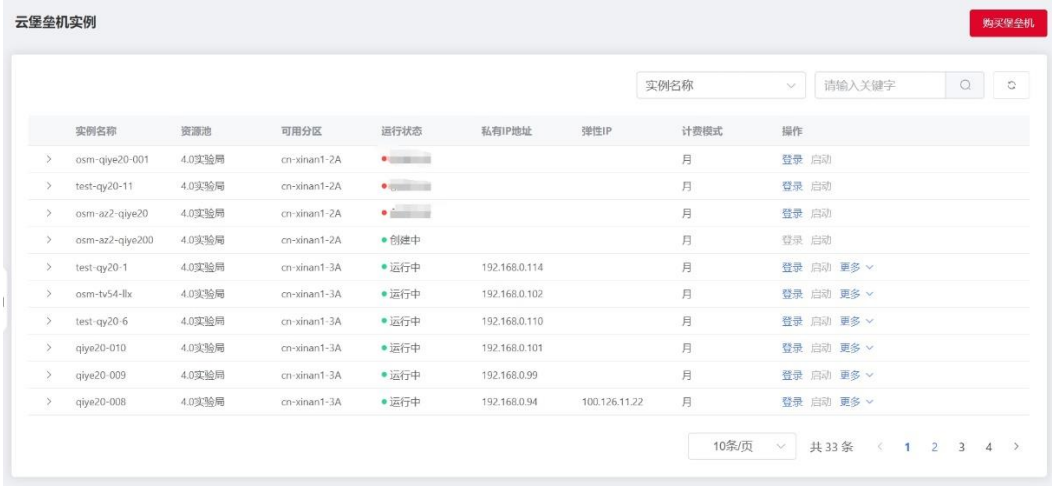
- 当前仅支持同版本、同实例规格内变更资产规格，不支持跨版本或跨实例规格变更。

前提条件

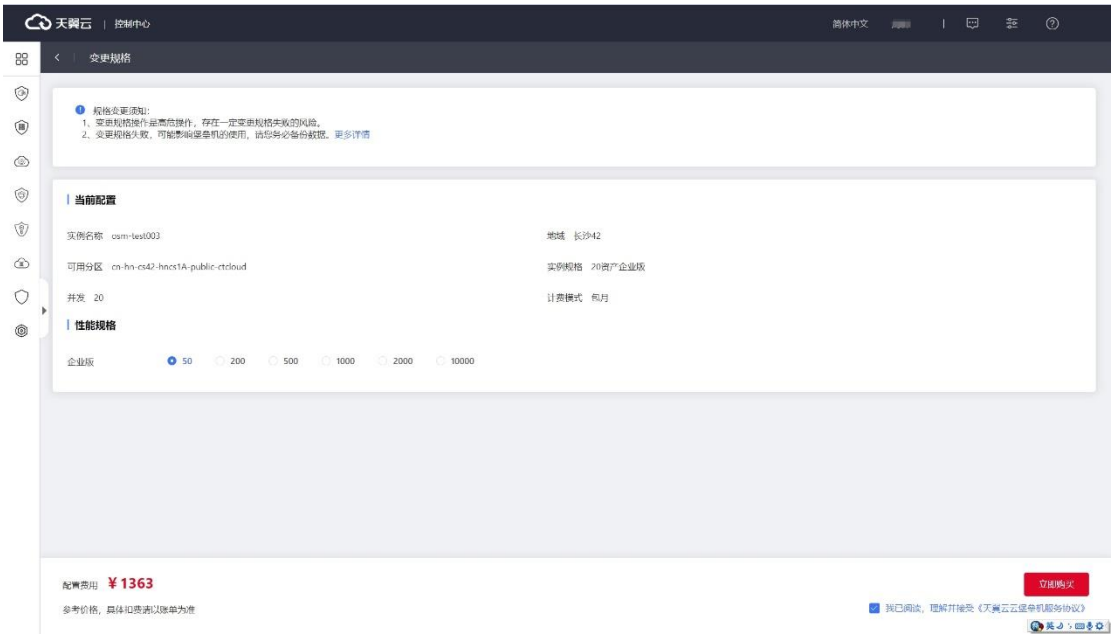
- 已获取管理控制台的登录帐号与密码。
- 已绑定 EIP，且 EIP 可用。

操作步骤

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

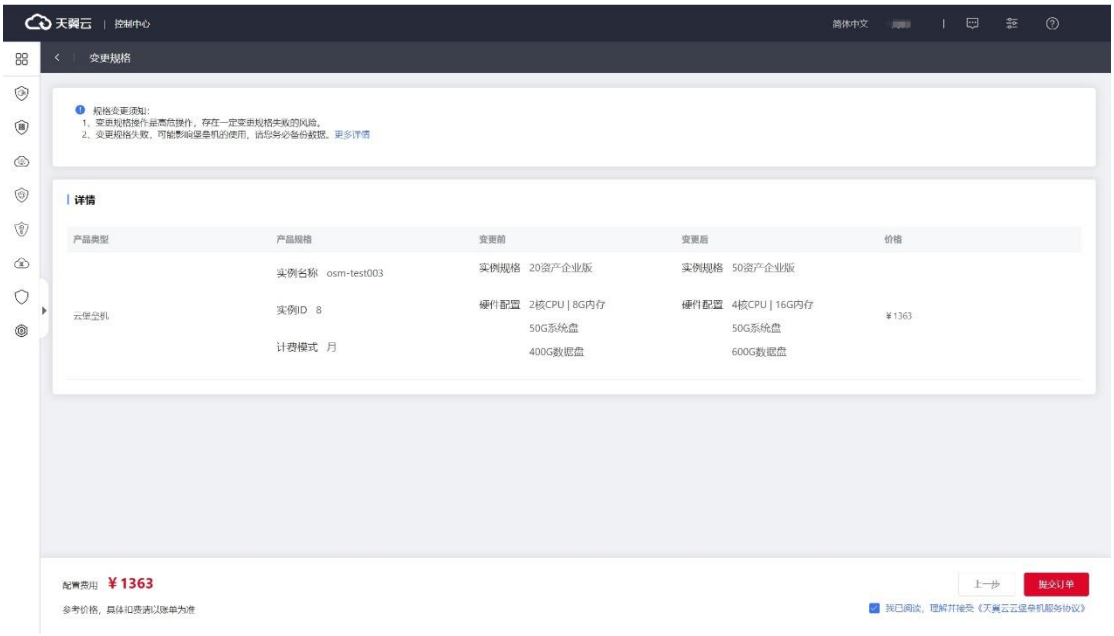


3. 选择需变更规格的实例，单击所在行“操作”列中“更多 > 变更规格”，跳转到“变更规格”页面。



4. 选择需变更的“资产规格”，单击“立即购买”。

5. 进入“订单详情”页面，确认订单无误后，单击“提交订单”。



6. 在支付页面完成付款。

7. 后台自动进行变更规格操作，整个变更规格过程需 10min 左右。

8. 实例运行状态变为“运行”，即可正常使用云堡垒机。

2.4 续费与退订

续费

- 为保证用户正常使用云堡垒机服务，在云堡垒机许可证到期前或使用许可到期后 15 天内，用户可通过“续费”操作增加授权使用期限。

- 在云堡垒机到期前，可以通过“续费”操作延长到期时间。

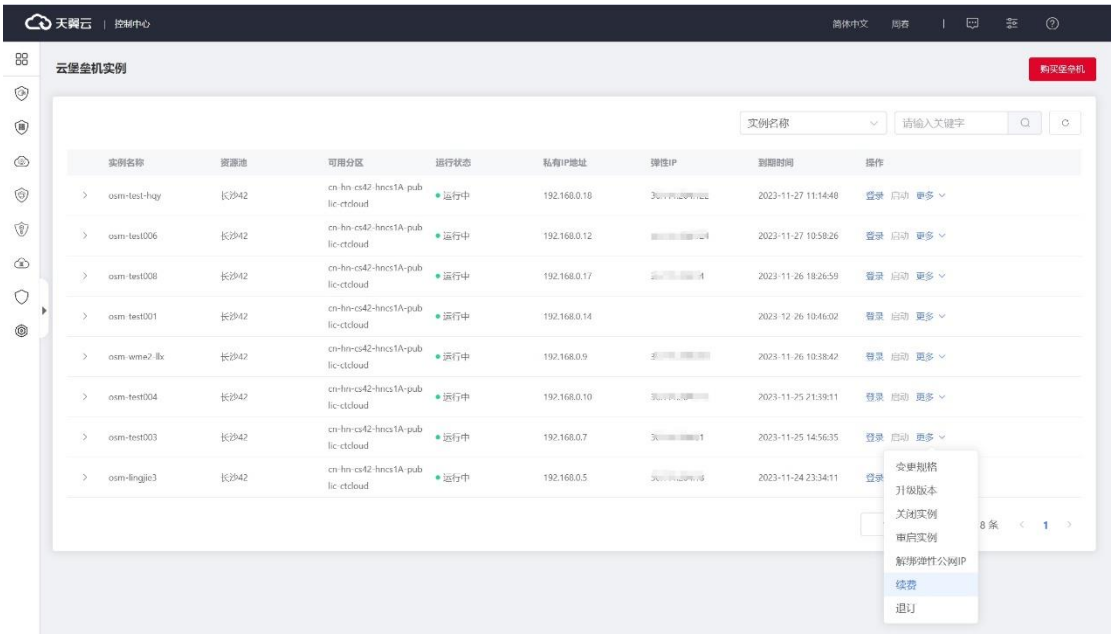
- 在云堡垒机到期后，若未及时续费，则进入“保留期”，不能登录云堡垒机系统。“保留期”为 15 天，到期仍未续订或充值，存储在云堡垒机中的数据将被删除、资源将被释放。

前提条件

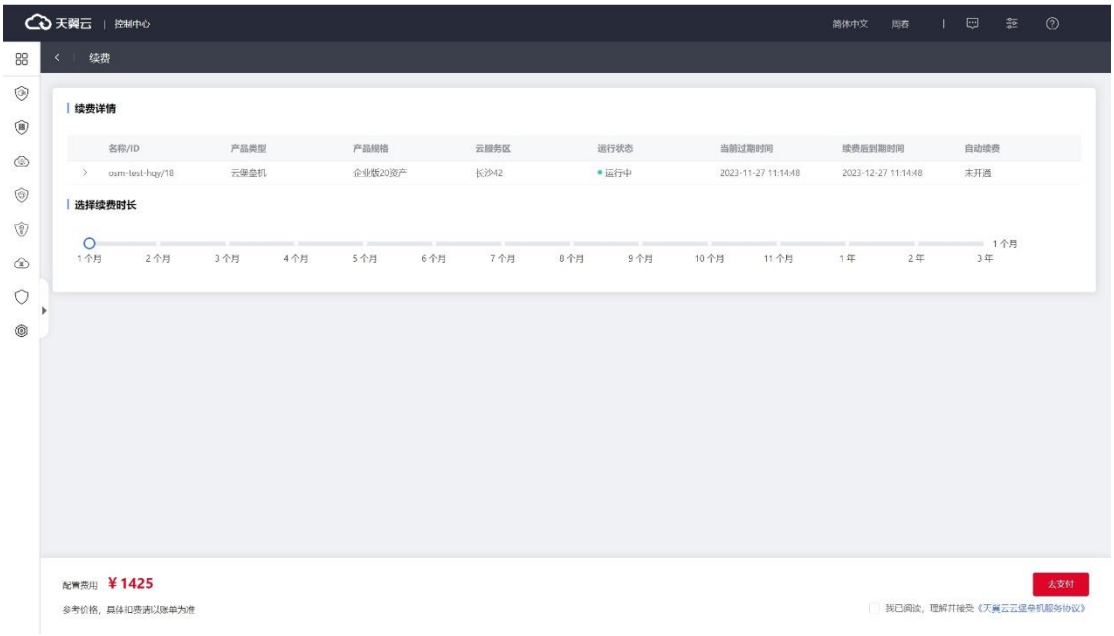
已获取控制台的登录帐号与密码。

操作步骤

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



4. 根据需要选择续费时长。



5. 单击“去支付”，在支付页面完成付款。

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

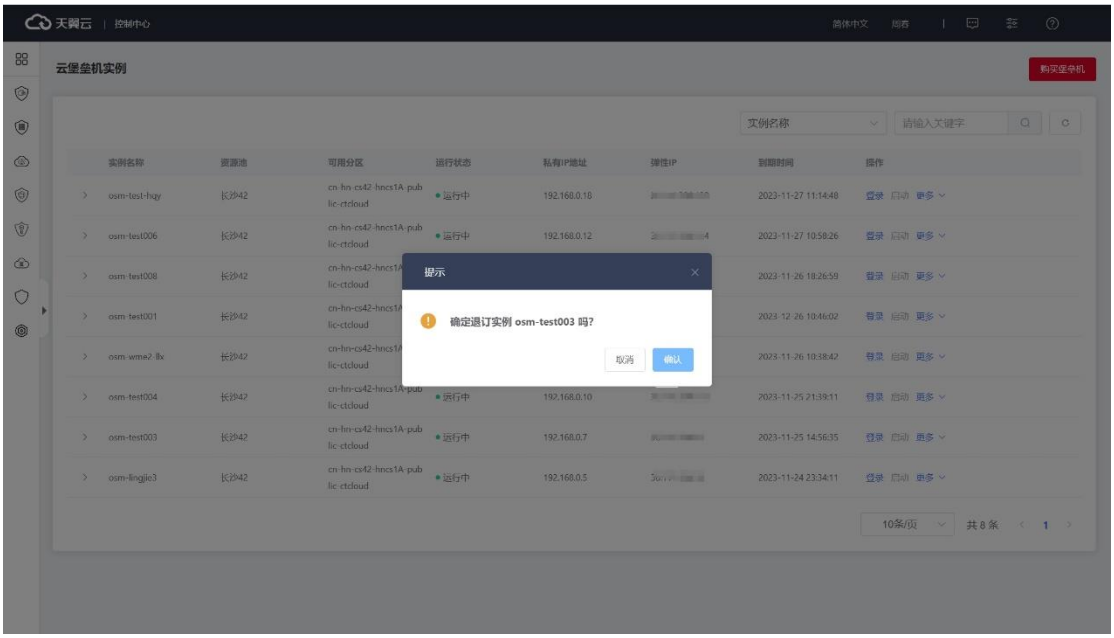
退订

前提条件

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

操作步骤

1. 登录管理控制台。
2. 选择“安全 > 云堡垒机（原生版）”，进入云堡垒机实例管理页面。
3. 选择待退订的实例，单击所在行“操作”列的“更多 > 退订”，弹出的退订实例对话框。



4. 确认实例信息无误后，单击“确定”。

5. 在退订资源页面完成退订。

到期与欠费

- 包周期资源开通成功后，如果没有按时续费，云平台会提供一定的保留期。

- 保留期 ：指宽限期到期后客户的包年/包月资源仍未续订或按需资源仍未缴清欠款，将进入保留期。保留期内客户不能访问及使用云服务，但对客户存储在云服务中的数据仍予以保留。

- 云服务进入保留期后，天翼云将会通过邮件、短信等方式向您发送提醒，提醒您续订或充值。保留期到期仍未续订或充值，存储在云服务中的数据将被删除、云服务资源将被释放。

- 欠费后，可以查看欠费详情。为防止相关资源不被停止或者释放，请及时进行充值，账号将进入欠费状态，需要在约定时间内支付欠款。

3 快速入门

3.1 步骤一：安全组策略设置

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

说明

- 安全组是一个逻辑上的分组，为同一个虚拟私有云内具有相同安全保护需求，并相互信

任的弹性云服务器和堡垒机 CBH 实例提供访问策略。

- 为了保障堡垒机的安全性和稳定性，在使用堡垒机实例之前，您需要设置安全组，开通需访问堡垒机的 IP 地址和端口。
- 设置堡垒机安全组规则：为堡垒机所在安全组配置相应的入方向规则。

堡垒机端口开放说明

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

端口	用途	说明
18443	门户端口，及 H5 运维端口	访问堡垒机门户页面时需开放该端口的入方向规则，（并可支持 H5 方式运维资产）
18000	字符资产访问端口	需通过堡垒机维护字符类协议资产时，需开放该端口的入方向规则
19000	图形资产访问端口	需通过堡垒机使用 mstsc 客户端维护图形类协议资产时，需开放该端口的入方向规则
20000	图形资产访问端口	需通过堡垒机使用 vncview 客户端维护图形类协议资产时，需开放该端口的入方向规则
6003	数据库资产访问端口	需通过堡垒机维护数据库协议资产时，需开放该端口的入方向规则
8765	数据库资产访问端口	需通过堡垒机维护数据库协议资产时，需开放该端口的入方向规则

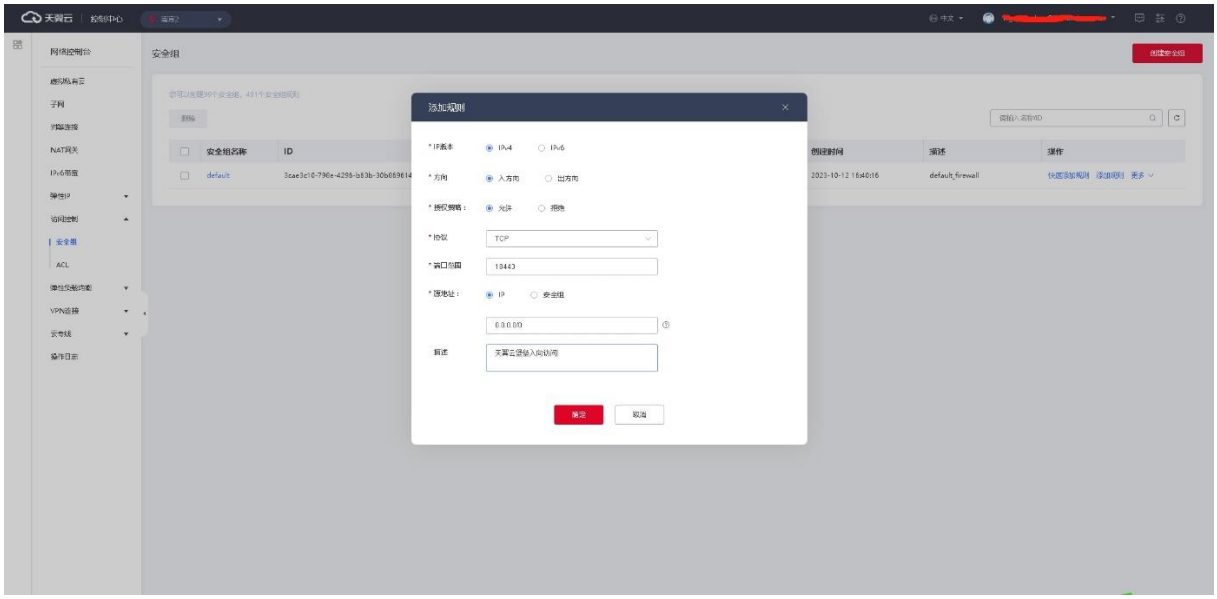
安全组规则设置

注意

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

堡垒机弹性 IP 安全组访问规则设置：

1. 登录管理控制台。
2. 在系统首页，单击“网络 > 弹性 ip”。
3. 在左侧导航树选择“访问控制 > 安全组”。
4. 在安全组界面，单击操作列的“配置规则”，进入安全组详情界面。
5. 在安全组详情界面，单击“添加规则”，弹出添加规则窗口。
6. 根据界面提示配置安全组规则。



3.2 步骤二：登录云堡垒机实例

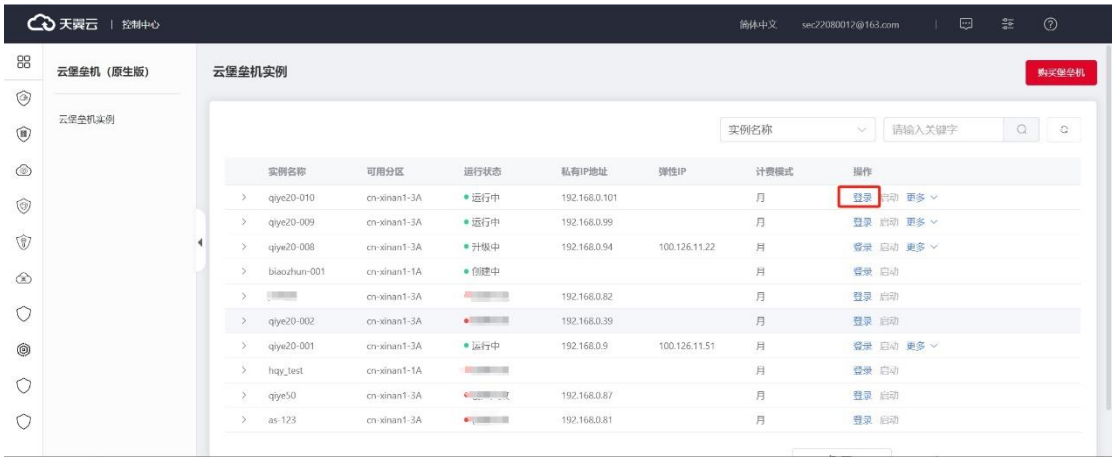
云堡垒机系统管理员 admin 拥有系统最高操作权限，登录 admin 可对系统进行管理和审计。开通堡垒机（原生版）后，用户在控制台 “云堡垒机实例”页面，在操作列点击“登录”链接单点登录进入云堡垒机，通过控制台登录进入默认用户为 admin 用户。

首次登入

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【云堡垒实例】列表条目录中选择要管理的实例,点击【登录】。
2. 登入堡垒机后，通过个人信息进行初始密码设置。



非首次登入

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

前置条件

已登录过云堡垒机并完成密码初始化。

操作步骤

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

3.3 步骤三：新增账号和资产

新增用户账号

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

操作步骤

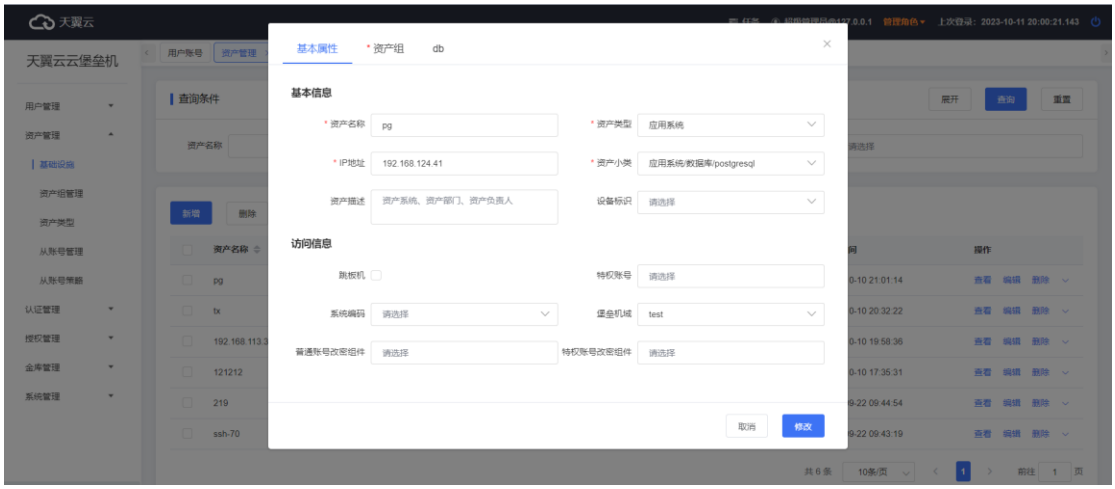
1. 管理员 admin 登录云堡垒机系统。
2. 角色身份切换到“管理角色”。
3. 在左侧导航栏，选择用户管理>账号管理>新增。
4. 填写账号基本信息，并选择角色身份，单击保存提交。

新增资产和资产账号

在使用云堡垒机进行运维前，管理员需要将主机资产和主机账号新增到云堡垒机系统中。

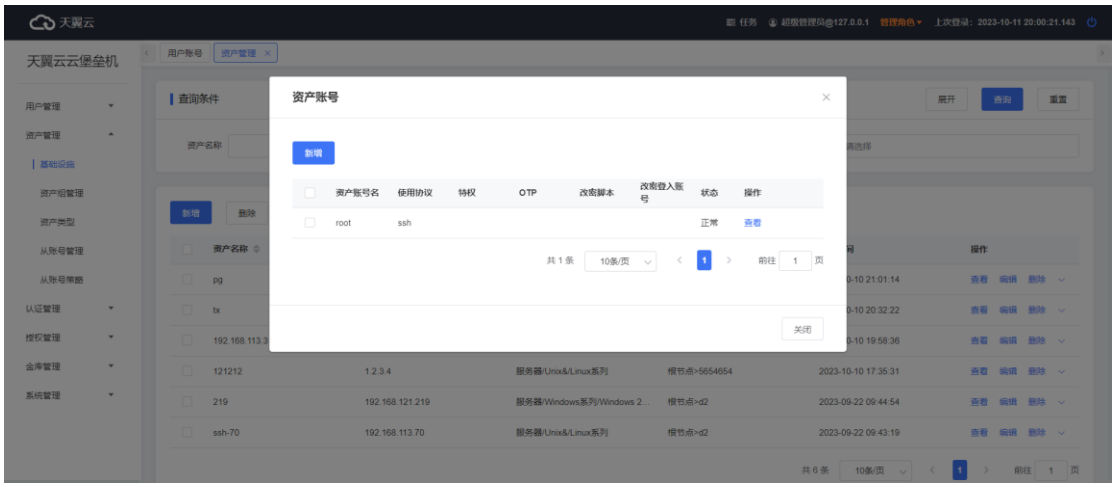
操作步骤

1. 管理员 admin 登录云堡垒机系统，角色身份切换到“管理角色”。
2. 在左侧导航栏，点击 资产管理>基础设施>新增。
3. 填写资产信息，单击保存提。



4. 选择资产，单击向下箭头。

5. 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。



6. 单击提交。

3.4 步骤四：配置运维权限

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

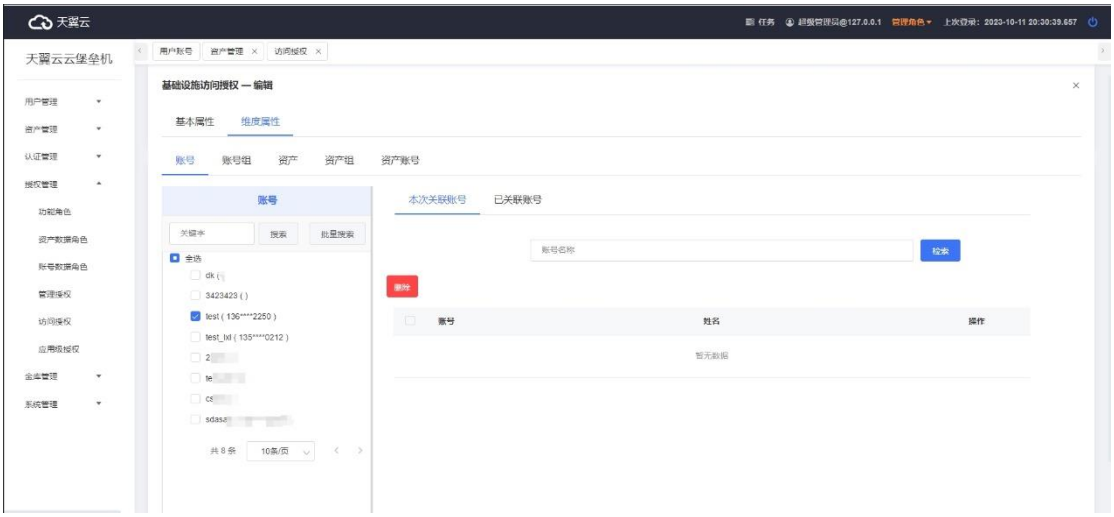
操作步骤

1. 管理员 admin 登录云堡垒机系统。

2. 角色身份切换到“管理角色”。

3. 在左侧导航栏，点击授权管理>访问授权>新增。

4. 填写授权基本属性并通过维度属性关联账号以及资产和资产账号。



3.5 步骤五：资产运维

堡垒机运维员可以通过客户端运维和网页运维方式对已授权的资产进行运维。

客户端运维

前置条件：

- 堡垒机成功纳管资产，且堡垒机与资产的网络可连通
- 运维账号已开通且分配了运维角色，同时对账号进行了资产访问授权
- 本地终端已安装访问控件并且正确对访问控件进行设置。

操作步骤

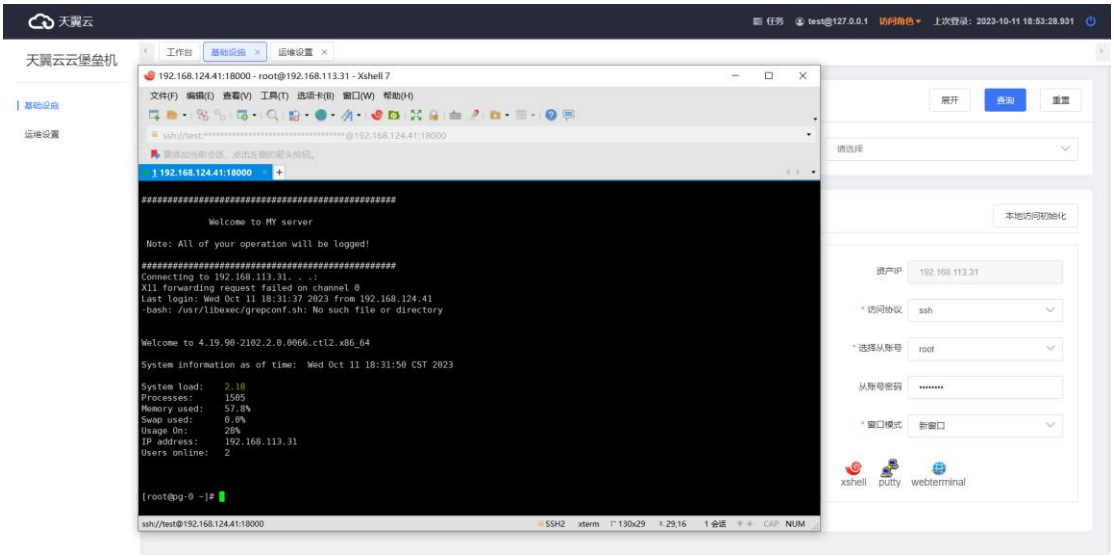
1. 用户账号登录云堡垒机系统。

2. 角色身份切换到“访问角色”。

3. 在左侧导航栏，选择基础设施。

4. 单击目标运维主机，在右下方访问图标选择访问方式

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

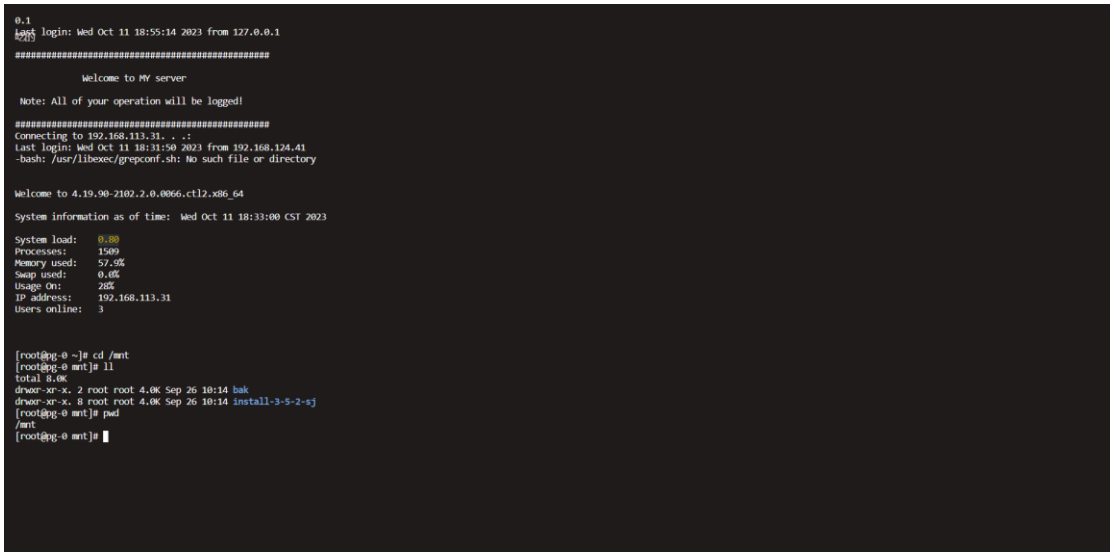


网页运维

用户可通过网页直接访问资产，无需安装运维客户端即可完成运维。

操作步骤

1. 用户账号登录云堡垒机系统。
2. 角色身份切换到“访问角色”。
3. 在左侧导航栏，选择基础设施。
4. 单击目标运维主机，在右下方访问图标选择 webterminal 方式访问。



3.6 步骤六：审计运维

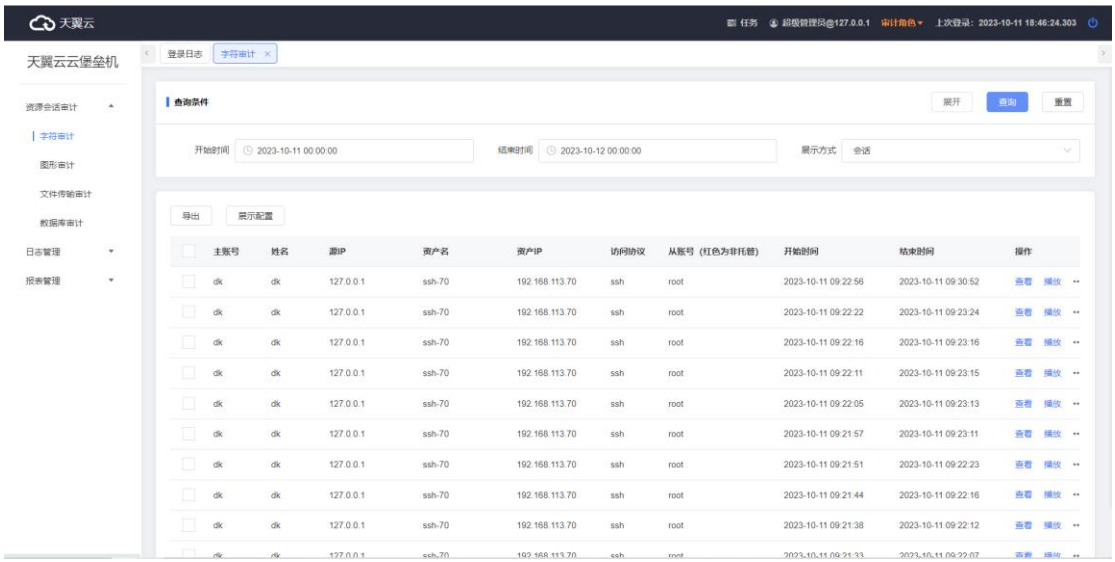
系统用户登录堡垒机并对已授权资产进行运维操作，管理员在堡垒机上可以查看到会话详情并播放运维录屏，实时监控运维会话并且可以中断高危风险会话。

前置条件

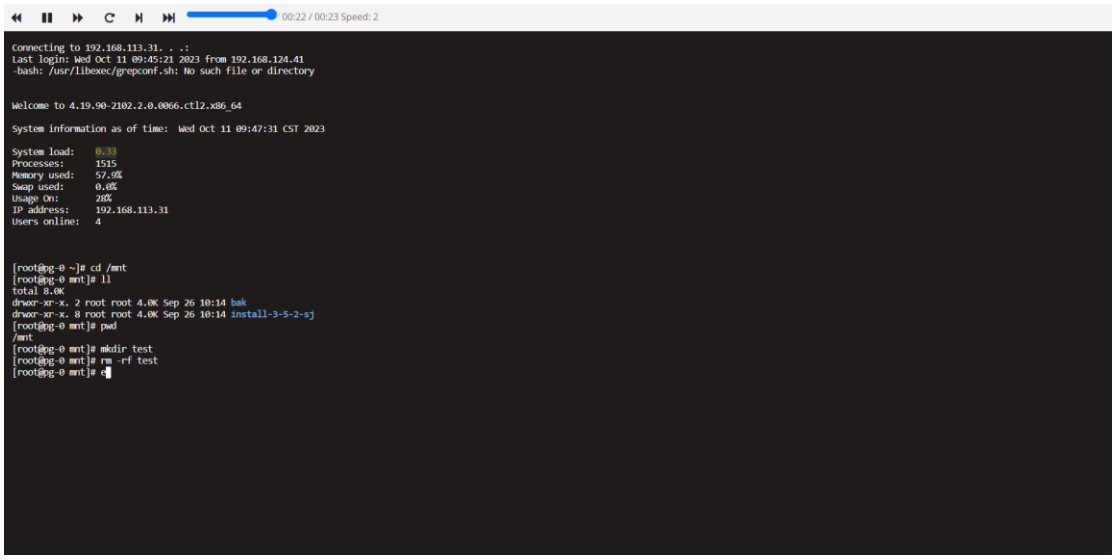
- 用户完成资产运维
- 登录授权的审计管理员账号

操作步骤

1. 管理员 admin 或审计管理员登录云堡垒机系统。
2. 角色身份切换到“审计角色”。
3. 在左侧导航栏，选择资源会话>字符审计。
4. 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。
5. 通过查看按钮，查看用户的详细操作记录
6. 通过播放按钮，可在线实时审计或回放用户的操作行为



回放操作历史



4 实例

4.1 购买实例

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。

您需首先购买云堡垒机实例，创建一个云堡垒机账户，再登录云堡垒机系统并配置运维管理环境，才能实现云堡垒机实时远程高效运维管理。

购买步骤

1.登录管理控制台。

2.选择“安全 > 云堡垒机（原生版）”，进入云堡垒机实例管理页面。

3.单击右上角的“购买堡垒机”，进入产品订购页。

4.选择“云堡垒机实例”相关参数，参数相关说明请参考下表。

购买参数	参数解释
计费模式	选择实例计费模式，仅支持“包年/包月”模式。 包年/包月是预付费模式，按订单的购买周期计费，适用于可预估资源使用周期的场景。
当前区域/可用区	选择云堡垒机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分区。 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	自定义云堡垒机实例名称。 长度为 2-15 字符，以字母或中文开头，可包含数字、“.” 、“_”、“-”。
实例规格	选择单机规格，目前仅单机版。
版本	目前支持“标准版”和“企业版”，具体版本支持的功能可参考功能特性章节。
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。 目前“标准版”和“企业版”都支持 10/20/50/100/200/500/1000/2000/5000/10000 资产规格。

购买参数	参数解释
企业项目	选择堡垒机所属的企业项目。
虚拟私有云	选择当前区域下虚拟私有云（Virtual Private Cloud，VPC）网络。 若当前区域无可选 VPC，可单击“查看虚拟私有云”创建新的 VPC。 注意 • 默认情况下，不同区域的 VPC 之间内网不互通，同区域的不同 VPC 内网不互通，同一个 VPC 下的不同可用区之间内网互通。 • 云堡垒机支持直接管理同一区域同一 VPC 网络下 ECS 等资源，同一区域同一 VPC 网络下 ECS 等资源可以直接访问
安全组	选择当前区域下安全组，若无合适安全组可选择，可单击“管理安全组”创建或配置新的安全组。 说明 • 一个安全组为同一个 VPC 网络内具有相同安全保护需求，并相互信任的 CBH 与资源提供访问策略。当云堡垒机加入安全组后，即受到该安全组中访问规则的保护。 • 云堡垒机可与资源主机 ECS 等共用安全组，各自调用安全组规则互不影响。 • 如需修改安全组，请参见更改安全组章节

购买参数	参数解释
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。
购买时长	选择实例使用时长。 可按月或按年购买云堡垒机。

5.配置完成后，单击“立即购买”。

6.进入“订单详情”页面，确认订单无误并阅读《天翼云云堡垒机服务协议》后，勾选“我已阅读并同意《天翼云云堡垒机服务协议》”，单击“提交订单”。

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。

4.2 登录实例

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

登录的时候可选“外网地址登录”或“内网地址登录”。

说明

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

首次登录

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

1.在“云堡垒机实例”列表条目录中选择要管理的实例，单击“管理”。

2.根据您自身的网络环境选择“内网地址登录”或“外网地址登录”。

3.登入堡垒机后，通过个人信息进行初始密码设置。

4.3 变更实例规格

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

注意

- 当前仅支持同版本、同实例规格内变更资产规格，不支持跨版本变更或跨实例规格变更。
- 仅支持云堡垒机资产规格升级，暂不支持资产规格降级，若需要降级，请先备份相关数据，退订堡垒机实例后重新订购新实例。
- 变更规格过程约需要 10min，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。

前提条件

已获取管理控制台的登录账号与密码。

已绑定 EIP，且 EIP 可用。

操作步骤

1.登录管理控制台。

2.选择“安全 > 云堡垒机（原生版）”，进入云堡垒机实例管理页面。

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

4.选择需变更的“资产规格”，单击“立即购买”。

5.在支付页面完成付款。

6.后台自动进行变更规格操作，整个变更规格过程需 10min 左右。

7 实例运行状态变为“运行”，即可正常使用云堡垒机。

4.4 升级实例

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。

前提条件

已获取管理控制台的登录账号与密码。

已绑定 EIP，且 EIP 可用。

操作步骤

1.登录管理控制台。

2.选择“安全 > 云堡垒机（原生版）”，进入云堡垒机实例管理页面。

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

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

5.待堡垒机状态变为“运行中”即表示升级已经结束，可正常使用堡垒机。

4.5 更改实例安全组

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

为了保障云堡垒机的安全性和稳定性，在使用云堡垒机之前，您需要设置安全组，开通需访问资源的 IP 地址和端口。但是若您在购买堡垒机的时候选择了不适用的安全组，也无法通过修改相应的安全组规则来放通这些 IP 地址和端口，这时候您可以通过更改堡垒机绑定的安全组来满足您的运维需求。

操作步骤

1.登录管理控制台。

2.选择“安全 > 云堡垒机（原生版）”，进入云堡垒机实例管理页面。

3.选择需要更改安全组的堡垒机实例，在实例详情页单击齿轮按钮。

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

5 运维用户指南

5.1 登录堡垒机

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

登录的时候可选“外网地址登录”或“内网地址登录”。

说明

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

首次登录

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

操作步骤

1.在“云堡垒机实例”列表条目录中选择要管理的实例，单击“管理”。

2.根据您自身的网络环境选择“内网地址登录”或“外网地址登录”。

3.登入堡垒机后，通过个人信息进行初始密码设置。

非首次登录

非首次登入云堡垒机可通过云堡垒机控制台单点登入跳转登入堡垒机，或通过云堡垒机登录地址使用静态认证或令牌认证等方式登录。以下介绍使用静态认证和令牌认证两种方式登录云堡垒机实例。

前置条件

已登录过云堡垒机并完成密码初始化。

静态认证登录操作步骤

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

2.选择认证方式为静态认证。

3.输入系统用户账号和密码，输入图形验证码。

4.单击“登录”，成功登录到堡垒机系统。

注意

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

短信认证登录操作步骤

说明

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

置章节。

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

2.选择认证方式为短信认证。

3.输入系统用户账号和密码，输入图形验证码。

4.单击“登录”，成功登录到堡垒机系统。

令牌认证登录操作步骤

说明

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

手机令牌章节。

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

2.选择认证方式为令牌认证。

3.输入系统用户账号和密码，输入手机动态口令。

4.单击“登录”，成功登录到堡垒机系统。

注意

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

5.2 运维环境设置

在使用堡垒机之前，您需要先设置运维工具及配置运维工具路径。

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

下载访问插件

1.使用访问用户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“运维设置”，进入“运维设置”页面。

3.单击页面右上角的“访问插件”按钮，根据实际操作环境选择插件下载。

配置运维工具

说明

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

1.在“运维设置”页面勾选需要使用的客户端工具，并单击“保存”。

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

3.在弹出的对话框中选择需要配置客户端，选择客户端路径。

5.3 资产运维

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

访问字符资产

1.使用访问用户登录云堡垒机（原生版）。

2.在左侧导航栏选择“资产访问”，在“资产访问”页面选择“字符”页签。

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

说明

资产账号可在管理员添加资产时同步添加。

访问图形资产

1.使用访问用户登录云堡垒机（原生版）。

2.在左侧导航栏选择“资产访问”，在“资产访问”页面选择“图形”页签。

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

使用文件传输

1.使用访问用户登录云堡垒机（原生版）。

2.在左侧导航栏选择“资产访问”，在“资产访问”页面选择“文字传输”页签。

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

访问数据库资产

1.使用访问用户登录云堡垒机（原生版）。

2.在左侧导航栏选择“资产访问”，在“资产访问”页面选择“数据库”页签。

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

说明

支持纳管的数据库请参考：使用限制章节。

5.4 工单管理

5.4.1 工单申请

当运维用户不具备某些资源访问控制权限时，可主动提交工单，申请相应资源访问控制权限。

约束限制

已被纳入审批规则的用户名单内。

创建工单

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

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，目前仅支持“资产访问授权”和“命令授权”
资产	选择您需要访问的资产或者命令，可多选。
资产账号	选择您需要授权的资产账号。
提示符正则式	（仅工单类型选择“命令授权”时可填写）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“命令授权”时可填写）输入待授权命令的正则式。
生/失效日期	填写权限生效的起始日期。
生/失效时间	填写权限每日生效的时间段。
描述	填写申请工单的相关描述

5.4.2 工单审批

前提条件

相关账号拥有工单审批的权限，若需要配置相关权限请参考规则配置章节。

工单审批

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

6 管理用户指南

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

6.1 用户管理

6.1.1 用户

云堡垒机系统具备集中管理用户功能，创建一个用户即创建一个云堡垒机系统的登录账号。系统管理员 **admin** 是系统默认用户，为系统第一个可登录用户，拥有系统最高操作权限，

且无法删除和更改权限配置。

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

用户相关操作

约束限制

仅有“管理角色”权限的用户可以新建、编辑和删除用户。

新增单个用户操作步骤

1.使用“管理角色”账号登录云堡垒机。

2.在左侧导航栏选择“用户管理 > 用户”，进入“用户”模块。

3.单击“新增”，在弹出的“新增用户”对话框中，填写用户信息。

参数	参数说明
用户	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
用户名	填写该账户的使用者的姓名（非登录账号）。
手机号	填写手机号，请确保手机号真实有效，否则会影响短信的接收。
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。

参数	参数说明
用户密码	输入该账户的密码。密码请根据管理员设置的密码规则填写，具体可参见：安全设置章节
确认密码	二次确认账户密码。
角色	选择该账户所属的角色，可选“管理角色”、“审计角色”和“访问角色”。
用户组	选择该账户所属的用户组，用户组操作请参见：用户组章节。
认证方式	选择认证方式，可选“静态认证”和“令牌认证”。
生效时间	选择该账户可登录的时间段。
准入 IP	选择可登录的 IP 地址。

4.填写完成后，单击“确定”完成用户新增。

后续操作

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

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

说明

您可以根据自身需求自定义密码规则，具体修改密码规则请参考安全设置章节。

批量导入用户

云堡垒机（原生版）支持批量导入用户信息。

1.使用“管理角色”账号登录云堡垒机。

2.在左侧导航栏选择“用户管理 > 用户”，进入“用户”模块。

3.单击“导入”按钮，弹出“账号导入”对话框。

4.单击“下载导入文件模板”，在线下文件模板中填写内容。

参数	参数说明
用户名	（必填）填写该账户的使用者的姓名（非登录账号）。
用户	（必填）填写该账户的用户名称（登录账号）。 只能为数字、大小写字母、“.”和“_”组成，首位只能数字或者字母，且不超过 25 个字符；
手机号	（必填）填写手机号，请确保手机号真实有效，否则会影响短信的接收。
邮箱	填写邮箱地址，请确保邮箱地址真实有效，否则会影响告警信息的接收。
密码	（必填）输入该账户的密码，密码请根据管理员设置的密码规则填写，具体可参见：安全设置章节。
角色	（必填）选择该账户所属的角色，可填写“管理角色”、“审计角色”和“访问角色”，需要选择多个角色请使用英文“,”分隔。
用户组	填写该账户所属的用户组，用户组操作请参见：用户组章节。若填写多个用

参数	参数说明
	户组请使用英文“,”分隔。
认证方式	（必填）选择认证方式，可选“静态认证”，“令牌认证”和“短信认证”，多个认证方式请使用英文“,”分隔。
授权生效日期	填写该用户生效的日期，日期格式支持：YYYY-MM-DD 或 YYYY/MM/DD。
授权失效日期	填写该用户失效的日期，日期格式支持：YYYY-MM-DD 或 YYYY/MM/DD。
授权生效日期	填写生效日期的具体时间点，填写范围：0-23，例如需要早上 10 点生效，就填写：10。
授权失效日期	填写失效日期的具体时间点，填写范围：0-23，例如需要晚上 10 点失效，就填写：22。
准入 IP	选择可登录的 IP 地址。

说明

若不填写生失效日期，则新建的账号默认永久生效。

4.填写完成后，上传模板文件后单击“提交”即可生成新的用户。

用户导出

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

说明

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

1.使用“管理角色”账号登录云堡垒机。

2.在左侧导航栏选择“用户管理 > 用户”，进入“用户”模块。

3.勾选需要导出的用户信息，单击“导出”即可生成用户信息表格导出。

用户加锁/解锁

云堡垒机支持对用户进行加锁操作，在锁定期间该用户无法登录云堡垒机。

1.使用“管理角色”账号登录云堡垒机。

2.在左侧导航栏选择“用户管理 > 用户”，进入“用户”模块。

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

用户删除

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

注意

用户删除后信息无法恢复，请谨慎操作！

1.使用“管理角色”账号登录云堡垒机。

2.在左侧导航栏选择“用户管理 > 用户”，进入“用户”模块。

3.勾选需要删除的用户信息，单击“删除”。

4.在弹出的对话框中单击“确定”即可删除用户。

6.1.2 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。

仅“管理角色”，可管理用户组，包括新建用户组、编辑用户组、删除用户组等。

用户组新增

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 > 用户组”，进入“用户组”模块。

3.单击“新增”，在弹出的“新增用户组”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。
用户	选择用户，新增用户操作请参见：用户章节。
描述	自定义用户组的描述。

后续操作

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

说明

同级间用户组名称不能重名。

删除用户组：选择需要删除的用户组，单击“操作”列的“删除”，在弹出的对话框中单击“确认”完成删除。

说明

- 关联用户的组不允许删除
- 非叶子节点不可删除

6.1.3 手机令牌

前提条件

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

1.进入云堡垒机（原生版）实例登录页。

2.选择“令牌验证”。

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

4.下载天翼云 APP，若已下载则单击“下一步”。

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

6.完成绑定后，即可使用令牌登录。

6.2 资产管理

6.2.1 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。

新增单个资产

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“资产管理 > 资产”，进入“资产”页面。

3.单击“新增”按钮，弹出“新增资产”对话框，并填写相关内容。

参数	参数说明	取值样例
资产名称	自定义新增的资产名称。	Test
资产类型	选择新增的资产类型，可选 Windows 服务器、Unix/Linux 服务器或数据库。	Windows 服务器

参数	参数说明	取值样例
	具体支持的资产类型可参考：使用限制章节。	
IP 地址	填写待纳管资产的 IP 地址，仅支持填写 IPv4 地址。	0.0.0.0
资产组	选择新增资产所在的资产组，资产组相关操作请参照：资产组章节。	-
资产描述	填写资产的描述。	-
协议	选择资产的协议类型： - 当**资产类型**选择 **Windows 服务器**或 **Unix/Linux 服务器**时支持选择：SSH、TELNET、SFTP、FTP、X11、RDP。 - 当**资产类型**选择**数据库**时支持选择：Oracle、DB2、MySQL、PostgreSQL。 协议选择完成后，需填写“端口”，若您选择的是**数据库**资产，还需再填写“服务器名称”。	SSH、80
账号	（可选）添加可访问资产的账号： - 账号名：填写可正常访问资产的账号名。 - 密码：输入账户名对应的密码。	-

参数	参数说明	取值样例
	- 私钥：若选择该项，需要上传有效的 RSA 证书。 - 使用协议：选择账户对应的协议。 - 状态：选择账号状态。 您也可以在资产账号模块添加。	
访 问 信息	选择资产系统编码，可选“UTF-8”或“GBK”。	GBK

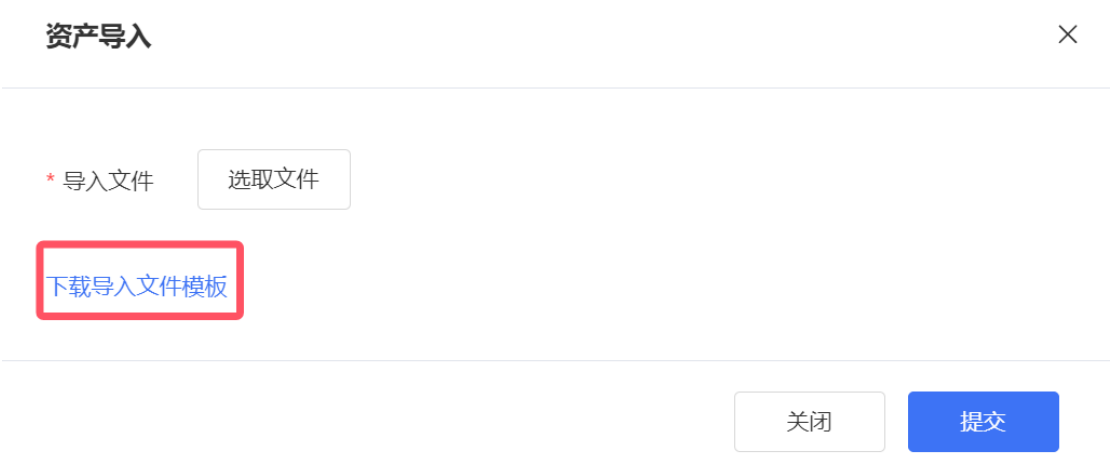
4.填写完成后，单击“提交”完成资产新增。

批量导入资产

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“资产管理 > 资产”，进入“资产”页面。

3.单击“导入”按钮，在弹出的对话框中下载导入模板。



4.在导入模板文件中填写内容，填写完成后保存。

说明

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

参数	参数说明	取值样例
资产名称	自定义新增的资产名称。	Test
资产类型	填写新增的资产类型：可填 **Windows 服务器**、**Unix/Linux 服务器**或**数据库**。	Windows 服务器
IP 地址	填写纳管资产的 IP 地址，仅支持 IPv4 地址。	0.0.0.0
资产组	填写新增资产所属的资产组。	-
资产描述	填写资产的描述。	-

参数	参数说明	取值样例
协议	填写协议的端口： - 资产类型为 **Windows 服务器**或 **Unix/Linux 服务器**时只会判断录入**黑色标题**的端口协议； - 资产类型为**数据库**时只会判断录入**蓝色标题**的端口协议且协议有填写时对应的服务名必填。	-
访问信息	填写资产的访问编码，仅支持填写“UTF-8”或“GBK”。	GBK

5.上传已经填写完成后的导入模板，单击“提交”完成资产导入。

后续操作

导出资产：在“资产”页面勾选需要导出的资产，单击“导出”即可导出。

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

注意

删除后的资产无法恢复，请谨慎删除！

6.2.2 资产组

您可以建立一个资产组来管理多个资产，方便您在授权的时候可以一键选择。

前提条件

仅“管理角色”支持资产相关的操作。

新增资产组

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“资产管理 > 资产组”，进入“资产组”页面。

3.单击“新增”，在弹出的对话框中填写内容。

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

4.填写完成后，单击“提交”完成资产组的创建。

6.2.3 资产账号

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

前提条件

仅“管理角色”支持资产相关的操作。

新增资产账号

资产账号有两种添加方式：

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

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“资产管理 > 资产账号”，进入“资产账号”页面。

3.单击“新增”按钮，在弹出的“新增资产账号”对话框中添加资产信息。

参数	参数说明	取值样例
资产名	选择需要添加资产账号的资产，请确保待添加的账号可以正常登录该资产。	-
账号名	填写可登录资产的账号名，例如：Administrator。	Administrator
密码	（可选）输入正确的账号密码。若不输入密码，则在登录资产时需要填写正确的密码才可登录。	-
私钥	（可选）若账户登录需要使用私钥验证，请开启此选项并且上传 RSA 私钥证书。	

参数	参数说明	取值样例
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

4.填写完成后单击“提交”即成功新增资产账号。

导入资产账号

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“资产管理 > 资产账号”，进入“资产账号”页面。

3.单击“导入”按钮，在弹出的对话框中下载导入模板。

4.在导入模板文件中填写内容，填写完成后保存。

说明

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

参数	参数说明	取值样例
资 产	填写需添加资产账号的资产名 (资产名需和堡垒机控制台上显示的一致)，请确保待添加的账号可以正常登录该资产。	Test

参数	参数说明	取值样例
账号名	填写可登录资产的账号名，例如：Administrator。	Administrator
密码	（可选）输入正确的账号密码。若不输入密码，则在登录资产时需要填写正确的密码才可登录。	-
协议	（可填多项）请选择资产的协议，支持填写：SSH、TELNET、SFTP、FTP、X11、RDP 和数据库。	
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

编辑资产账号

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

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“资产管理 > 资产账号”，进入“资产账号”页面。

3.选择需要修改账号信息的资产账号，单击“操作”列的“编辑”按钮。

4.在弹出的对话框中修改相关参数，单击“提交”完成修改。

冻结/解冻资产账号

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

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“资产管理 > 资产账号”，进入“资产账号”页面。

3.勾选需要冻结/解冻的账号，单击“冻结”/“解冻”按钮。

4.在弹出的对话框中单击“确定”完成操作。

6.3 授权管理

6.3.1 资源访问授权

资产访问授权用于控制用户访问资产的权限。

云堡垒机支持对运维用户限制登录时间段和协议限制。

前提条件

仅“管理角色”支持资产相关的操作。

新增访问资产授权

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

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

3.单击“新增”按钮，在弹出的“新增资产访问授权”对话框中配置信息。

参数	参数说明	取值样例
授权规则名称	自定义资产访问授权的规则名称。	Test
启用状态	选择该授权规则的启用状态，默认启用。	
用户	（可选）选择需要配置访问授权的用户。	-
用户组	（可选）选择需要配置访问授权的用户组。 若您选择的用户和用户组存在重合，默认取最大的合集。	-
资产	（可选）选择需要配置访问授权的资产。	-
资产组	（可选）选择需要配置访问授权的资产组。 若您选择的资产和资产组存在重合，默认取最大的合集。	-
资产账号	（可选）选择资产授权规则中允许使用的资产账号，添加资产账号请参见：资产账号章节。	-
协议	选择该授权规则支持访问的协议。	SSH
授权时间	选择该规则生效的时间段。	-

4.单击“提交”完成访问授权规则的创建。

批量导入访问授权

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

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

3.单击“导入”，在弹出的对话框中下载导入模板。

4.打开模板，配置相关内容。

参数	参数说明	取值样例
授权规则名称	自定义资产访问授权的规则名称。	Test
启用状态	选择授权规则创建完成后的启用状态，可选择“启用”或“禁用”。	启用
用户	（可选）填写需要配置访问授权的用户名，用户名请保持和系统中添加用户名保持一致。	-
用户组	（可选）填写需要配置访问授权的用户组，用户组请保持和系统中添加用户组名保持一致。 若您填写的用户和用户组存在重合部分，取两者最大的合集。	-
资产	（可选）填写需要配置访问授权的资产，资产名称请保持和系统中添加的资产名保持一致。	-

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

5.填写完成后，保存文件并上传。

6.3.2 字符命令授权

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

针对 SSH 和 Telnet 字符协议主机，根据管理员配置的策略限制，云堡垒机对用户运维过程中执行的命令进行审计和过滤，并返回审计的命令、过滤结果和命令返回的内容，用于会话操作记录、拒绝使用等动作。

命令控制策略支持以下功能项：

- 支持按策略列表页策略排序区分优先级，排序越靠前优先级越高（优先级可选 1-100）。
- 支持控制允许执行、拒绝执行、断开连接、动态授权四种命令动作。
    - 允许：触发该策略规则后，放行命令操作。默认允许执行所有操作。
    - 拒绝：触发该策略规则后，拒绝执行该命令，界面会提示您在执行命令时会得到该命令不能执行的提示。
    - 警告：触发该策略规则后，警告运维用户谨慎执行该命令。

新增命令组

您在新增字符命令授权前需要进行新增命令组的操作。

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“授权管理 > 字符命令授权”，进入“命令授权”页面。

3.在页面上面选择“命令组”页签，单击“新增”，开始新增命令组。

参数	参数说明	取值样例
名称	自定义命令组的名称。	Test
提示符正则式	填写命令提示符的正则表达式。	grep "su root" filename.txt
命令正	填写命令规则的正则表达式。	en\w*

参数	参数说明	取值样例
则式		
风险等级	选择该命令组的风险等级，共可选 5 个等级。	普通
动作	选择该命令组中的命令触发时产生的动作： - 允许：触发该策略规则后，放行命令操作。默认允许执行所有操作。 - 拒绝：触发该策略规则后，拒绝执行该命令，界面会提示您在执行命令时会得到该命令不能执行的提示。 - 警告：触发该策略规则后，警告运维用户谨慎执行该命令。	拒绝

说明

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

命令组后续操作

修改命令组：选择需要修改的命令组，单击“操作”列中“编辑”，按照需求进行命令组数据的修改，单击“提交”完成命令组数据更新。

删除命令组：选择需要删除的命令组，单击“操作”列中“删除”，在弹出的对话框中单击

“确定”即可删除命令组。

注意

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

新增命令授权规则

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

2.在左侧导航栏选择“授权管理 > 字符命令授权”，进入“命令授权”页面。

3.单击“新增”，开始新增字符命令授权。

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

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

说明

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

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

后续操作

启用/禁用授权规则：可单个或批量启用/禁用授权规则，禁用的授权规则状态将更新为“无效”，启用的授权规则状态更新为“有效”，只有状态为“有效”的规则授权会生效。

编辑授权规则：选择需要修改的规则，单击“操作”列的“编辑”，按照需求进行命令授权数据的修改，单击“提交”完成命令授权数据更新。

删除授权规则：在需要删除的授权数据的“操作”列单击“删除”，在弹出的对话框中单击“确定”完成删除。

6.3.3 文件操作授权

文件操作授权用于控制用户访问资源时对资源内的文件操作的权限。

文件操作权限的可选范围是：

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

新增文件操作授权

1.使用“管理角色”账户登录云堡垒机（原生版）控制台。

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

3.单击“新增”，配置文件操作授权相关内容。

参数	参数说明	取值样例
授权规则名称	自定义资产访问授权的规则名称。	Test

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

参数	参数说明	取值样例
源 IP	填写用户登录的源 IP 地址。	0.0.0.0
风险等级	选择此授权规则的风险等级，共有 5 个等级可选择。	普通

说明

- 策略匹配顺序为：允许 > 阻断；

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

后续操作

启用/禁用授权规则：可单个或批量启用/禁用授权规则，禁用的授权规则状态将更新为“无效”，启用的授权规则状态更新为“有效”，只有状态为“有效”的规则授权会生效。

编辑授权规则：选择需要修改的规则，单击“操作”列的“编辑”，按照需求进行文件操作授权数据的修改，单击“提交”完成文件操作授权数据更新。

删除授权规则：选择需要删除的规则，单击“操作”列的“删除”，在弹出的对话框中单击“确定”完成删除。

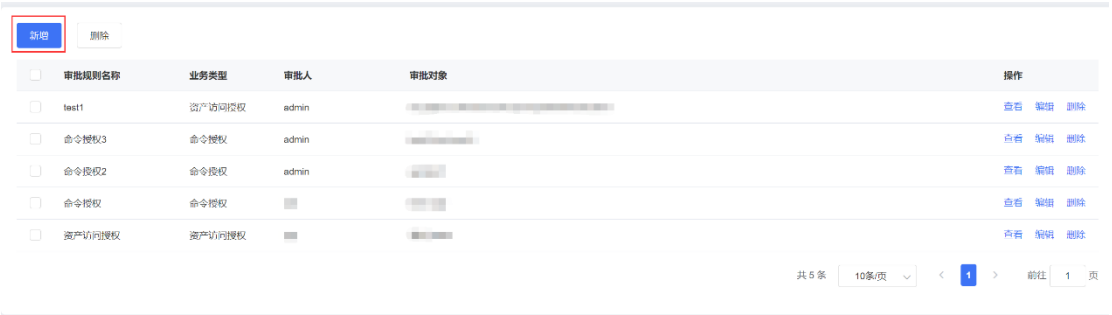
6.4 工单管理

6.4.1 审批规则

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

新增工单审批方式

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



4. 在弹出的对话框中配置相关内容，具体见下表，配置完成后单击“提交”。

规则名称	输入您的审批规则名称。
审批类型	目前仅支持选择“资产访问授权”和“命令授权”两种审批授权方式。 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。

审批人	选择该审批规则的具体审批人员，可多选。
用户（可选）	选择该条审批规则可以提交的相关用户，可多选。
用户组（可选）	选择该条审批规则可以提交的相关用户组，可多选。

6.4.2 工单审批

1. 登录云堡垒机系统。
2. 在左侧导航栏单击“工单管理”>“工单审批”，进入工单审批页面。
3. 查找需要待审批的工单，单击“操作”列的“**审批**”按钮。

6.5 **系统管理**

6.5.1 邮件服务器

邮件服务器，为改密提示和消息告警等通知提供邮件发送服务。

根据需求设置私有邮箱服务器或是公共邮箱服务器，并可测试所填写服务器信息是否有效。

邮件服务器配置

1.使用“管理角色”账号登录云堡垒机。

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

3.单击“编辑”按钮配置邮件服务器。

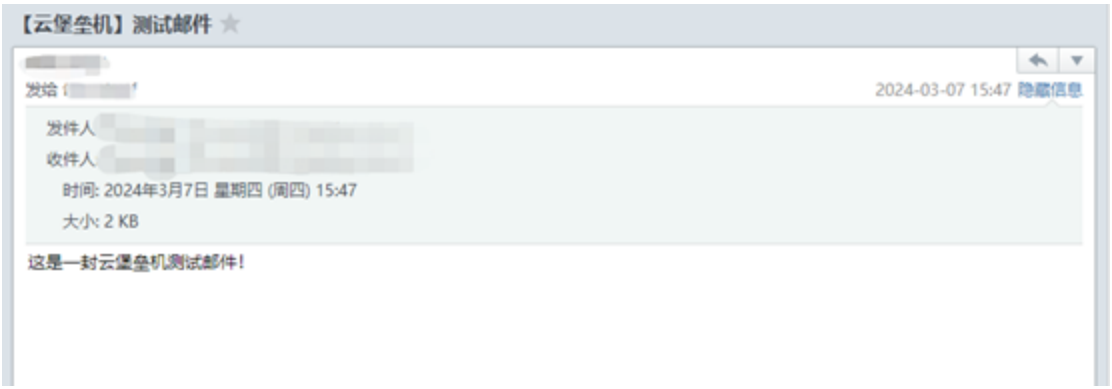
参数	参数说明
服务器地址	填写您的邮件服务器地址。
服务端口	填写您的邮件服务器端口
安全通信	选择是否开启安全通信。 安全通信支持 TLS/SSL 协议。
发送人账号	填写发送邮件的邮箱账号。
发送人密码	填写发送邮件的邮箱密码。

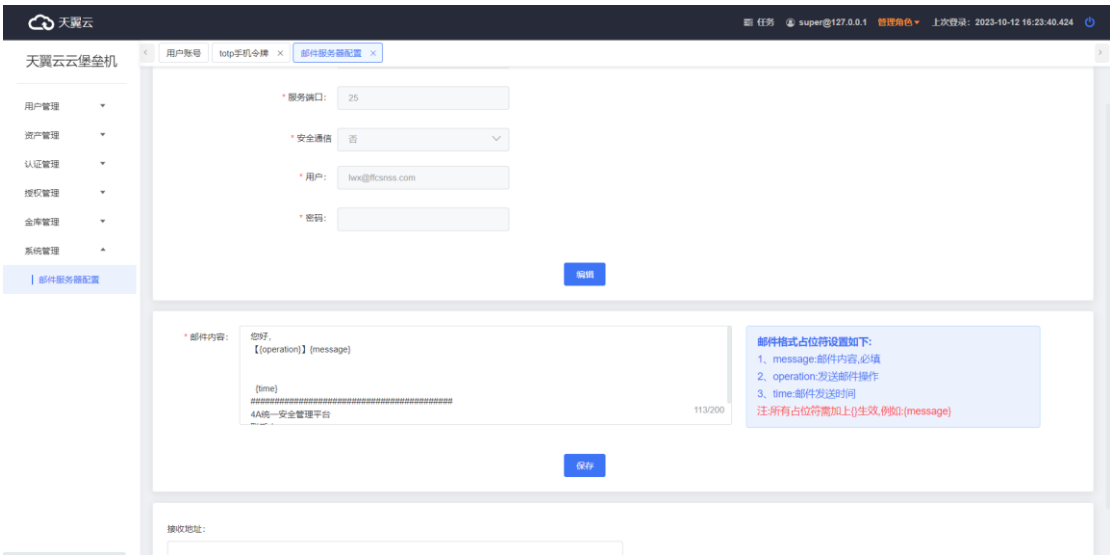
4.单击“保存”完成邮件服务器配置

后续操作

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

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





6.5.2 安全设置

云堡垒机安全设置模块支持您自定义密码强度、账户保护规则。

密码组成：配置用户密码策略，包括配置密码安全强度，密码字符组成。

密码事件：可设置安全登录事件、强制改密时间和首次登录改密。

账号策略：可设置账号空闲事件。

设置密码组成

1.使用“管理角色”账号登录云堡垒机。

2.在左侧导航栏选择“系统设置 > 安全管理”，进入“安全管理”模块。

3.选择密码组成模块，配置密码规则。

设置密码事件

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

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

强制用户改密后登录。

设置账号事件

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

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

醒邮件。

账号登录事件：根据配置的唯 N 性值，限制同一账号同时登录数。

6.5.3 认证设置

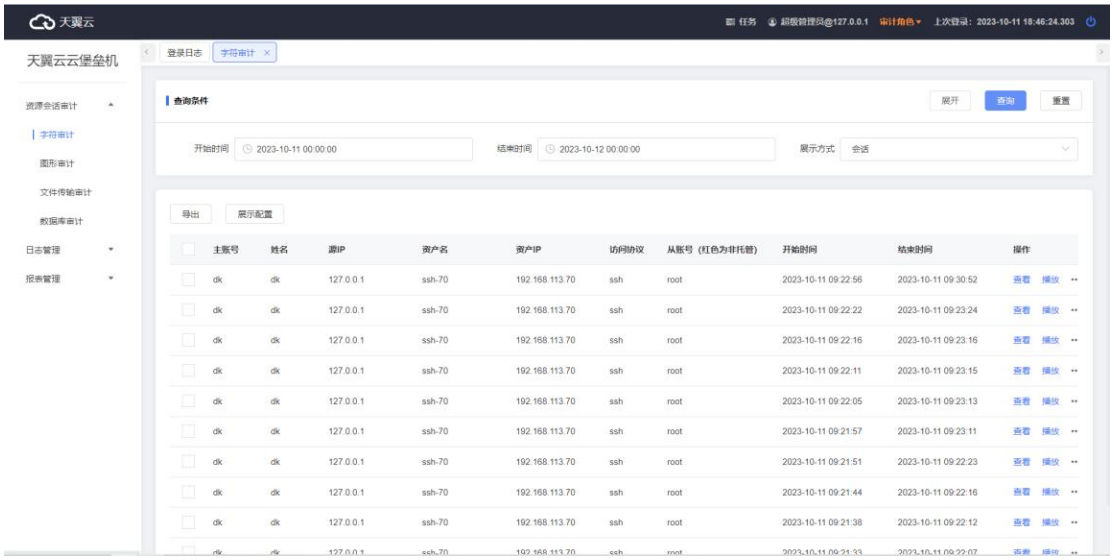
管理员登录并切换管理角色，打开系统管理>认证设置，该配置为全局认证策略，默认配置“静态认证” “令牌认证”，应用于所有账号，为空的情况下默认为静态认证方式。

6.6 资源会话审计

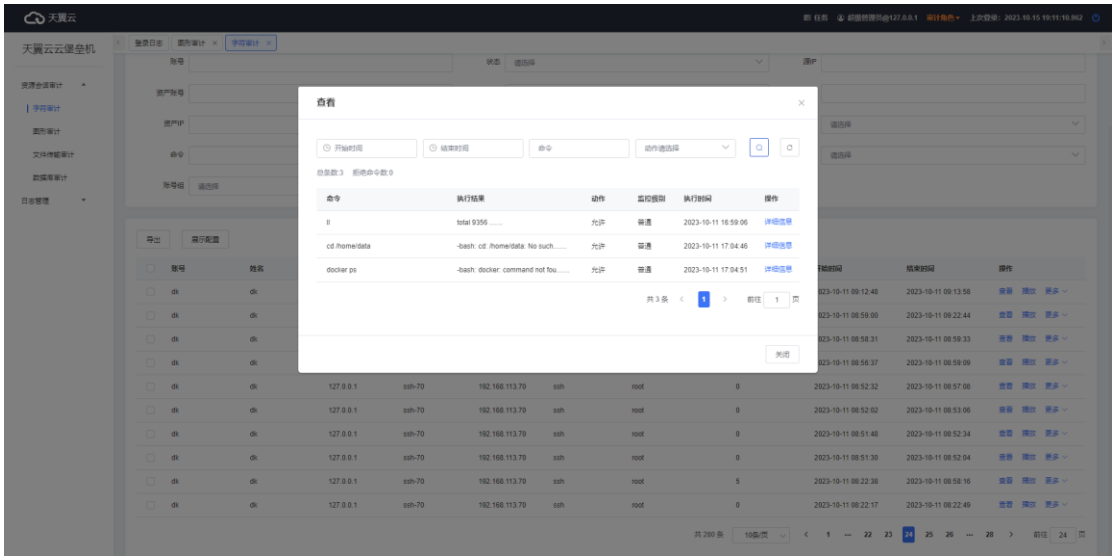
6.6.1 字符审计

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

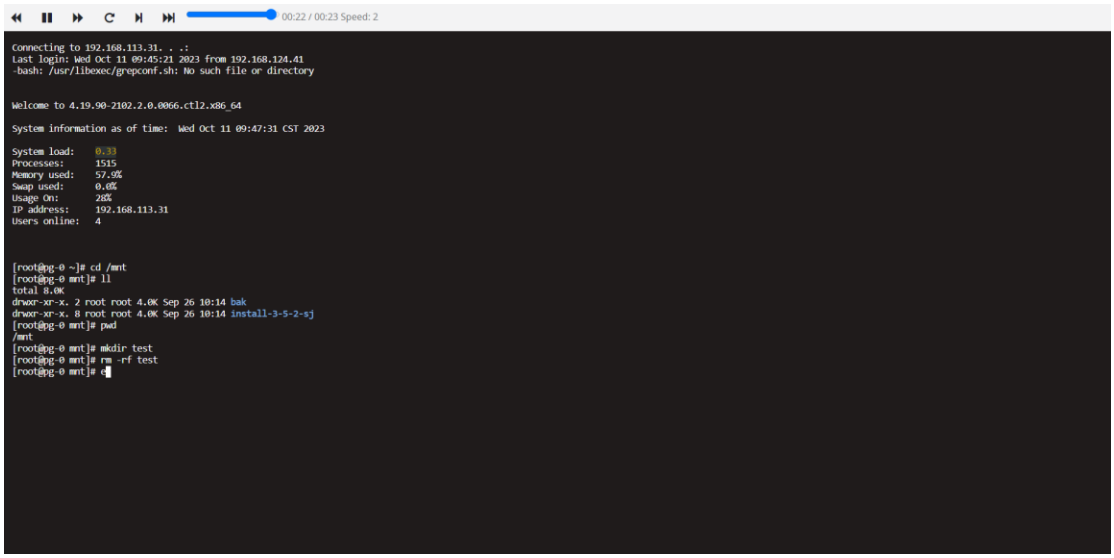
管理员登录并切换至 审计角色，管理员登录并切换至 管理角色，打开 审计管理>资源会话审计>字符审计



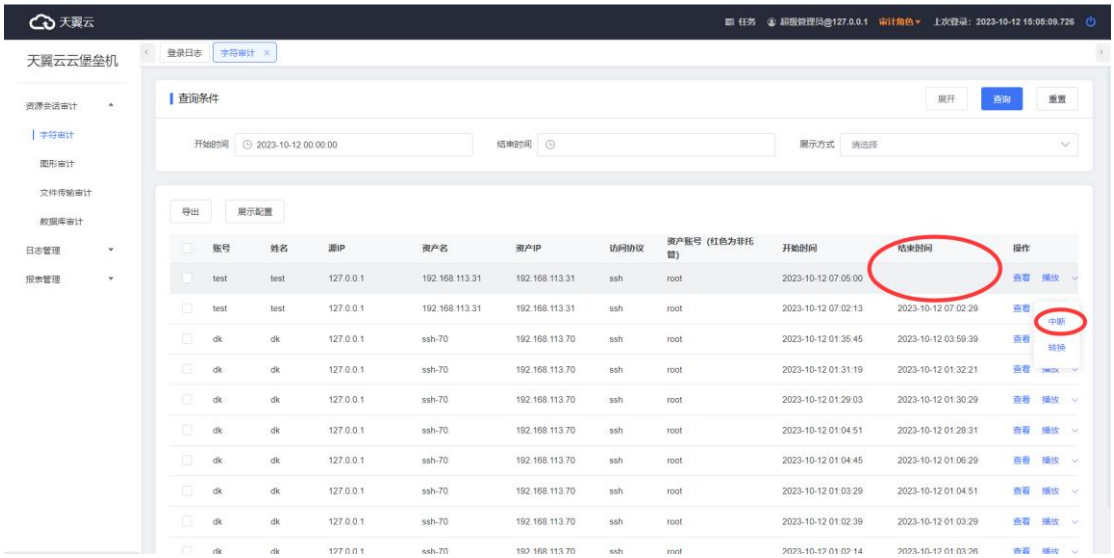
点击**查看**打开详细命令列表



点击**播放**可浏览器在线播放会话



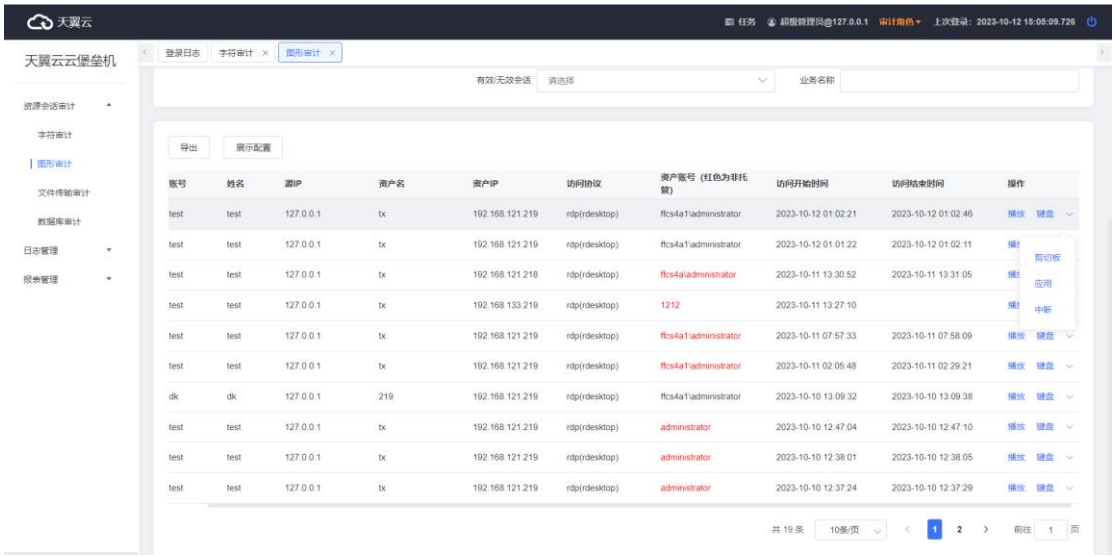
结束时间为空说明是活动会话，点击**播放**可实时观看会话，点击**中断**可中断该会话。



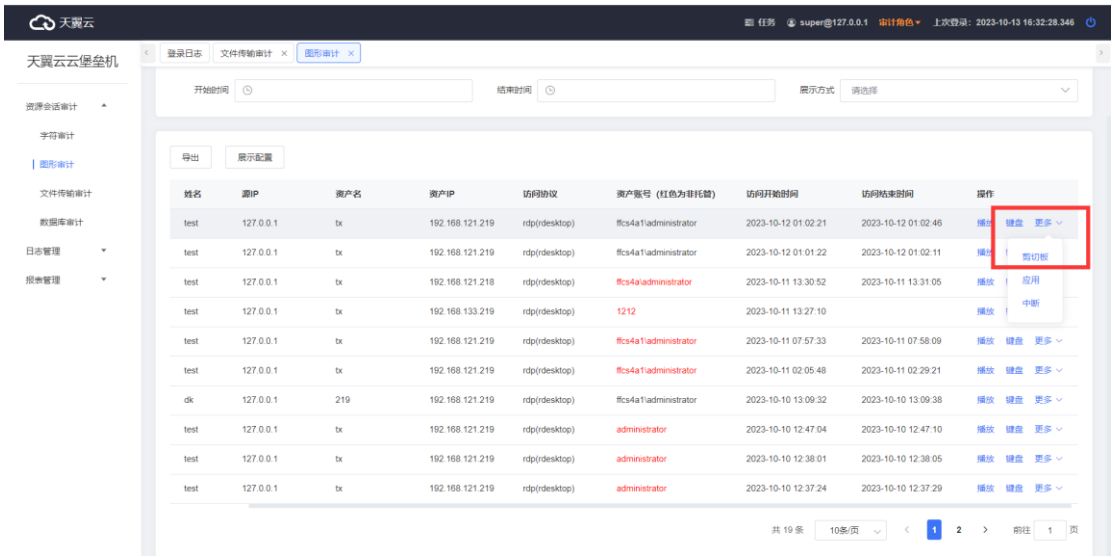
6.6.2 图形审计

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

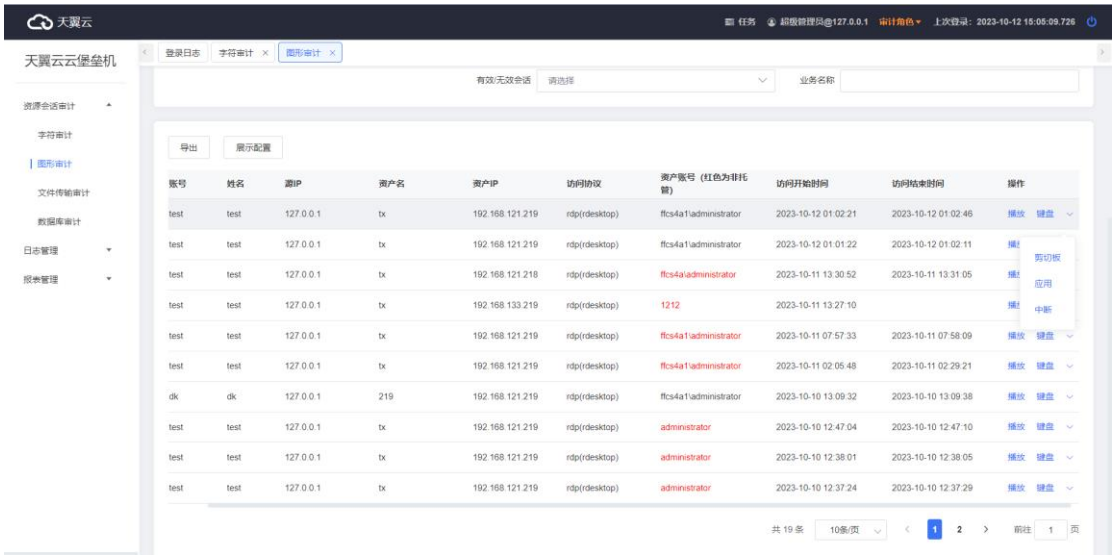
管理员登录并切换至 审计角色，打开 审计管理 > 资源会话审计 > 图形审计



点击键盘或剪切板可查看记录



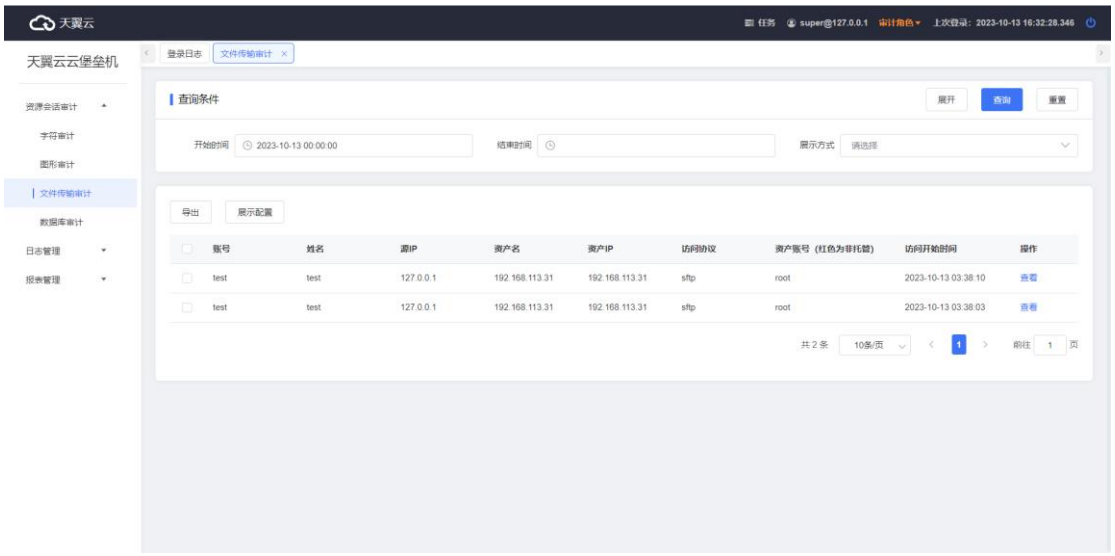
结束时间为空说明是活动会话，点击**播放**可实时观看会话，点击**中断**可中断该会话。



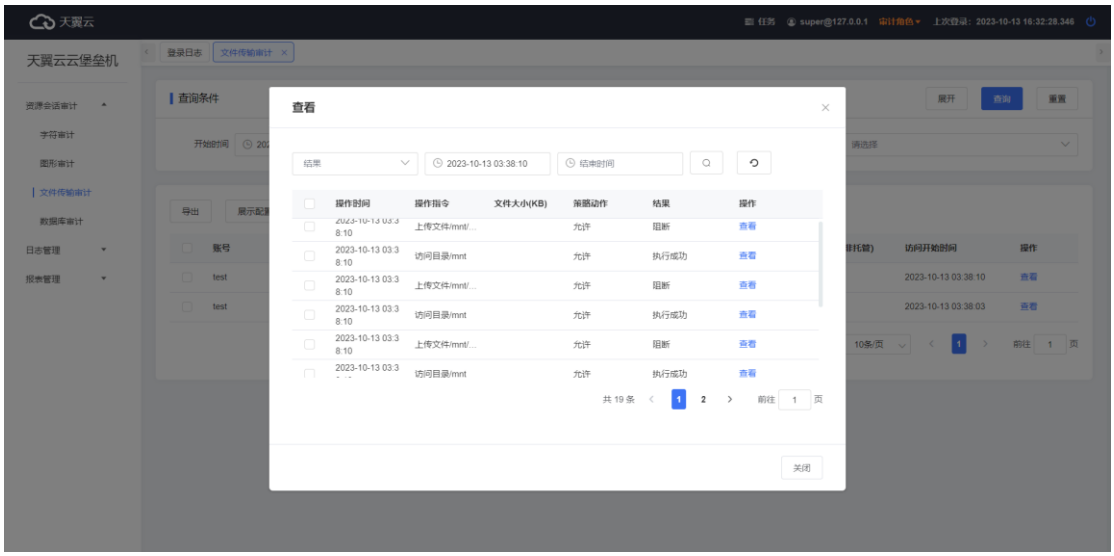
6.6.3 文件传输审计

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

管理员登录并切换至 审计角色，打开 审计管理>资源会话审计>文件传输审计



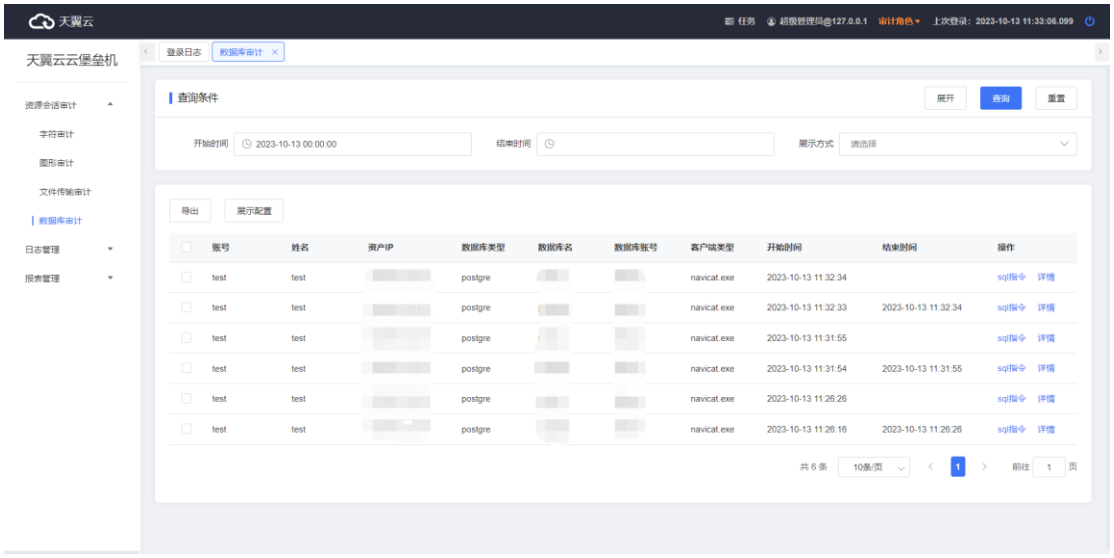
点击查看文件操作审计列表



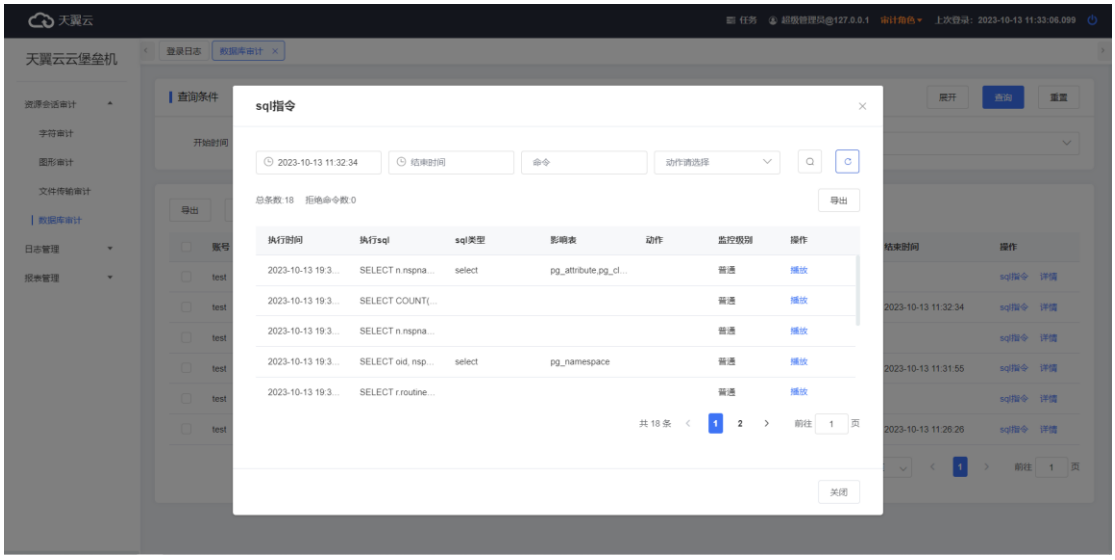
6.6.4 数据库审计

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

管理员登录并切换至 审计角色，打开 审计管理>资源会话审计>数据库审计：



点击 sql 指令可查看具体执行的 sql 语句。

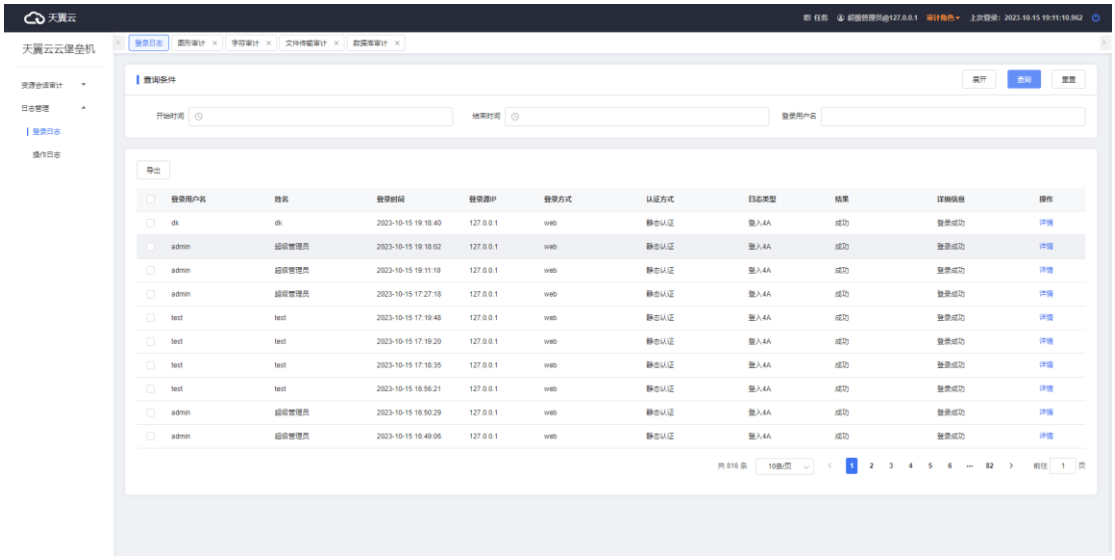


6.7 日志管理

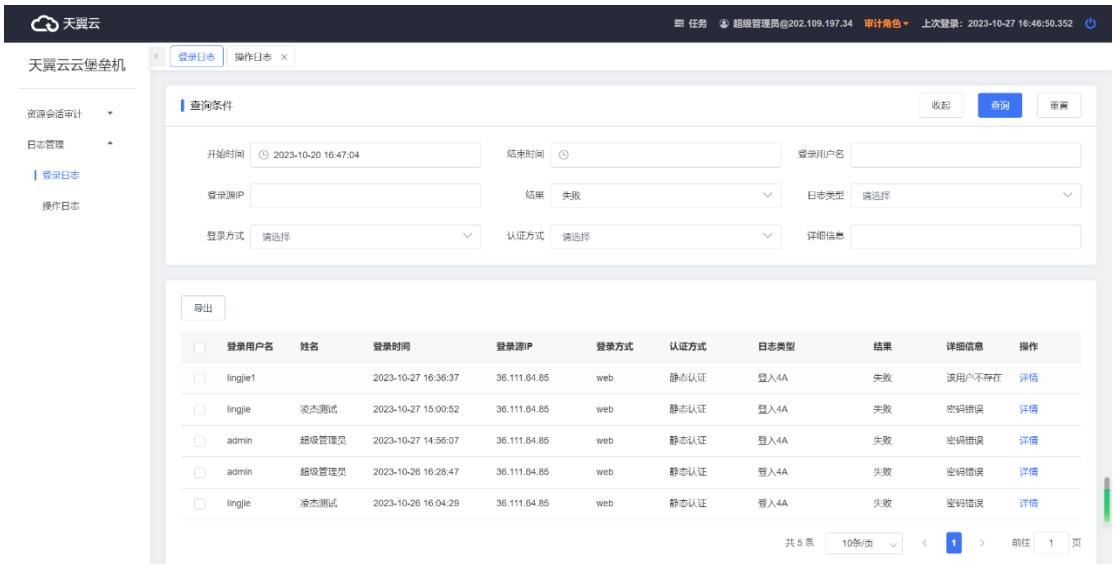
6.7.1 登录日志

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。

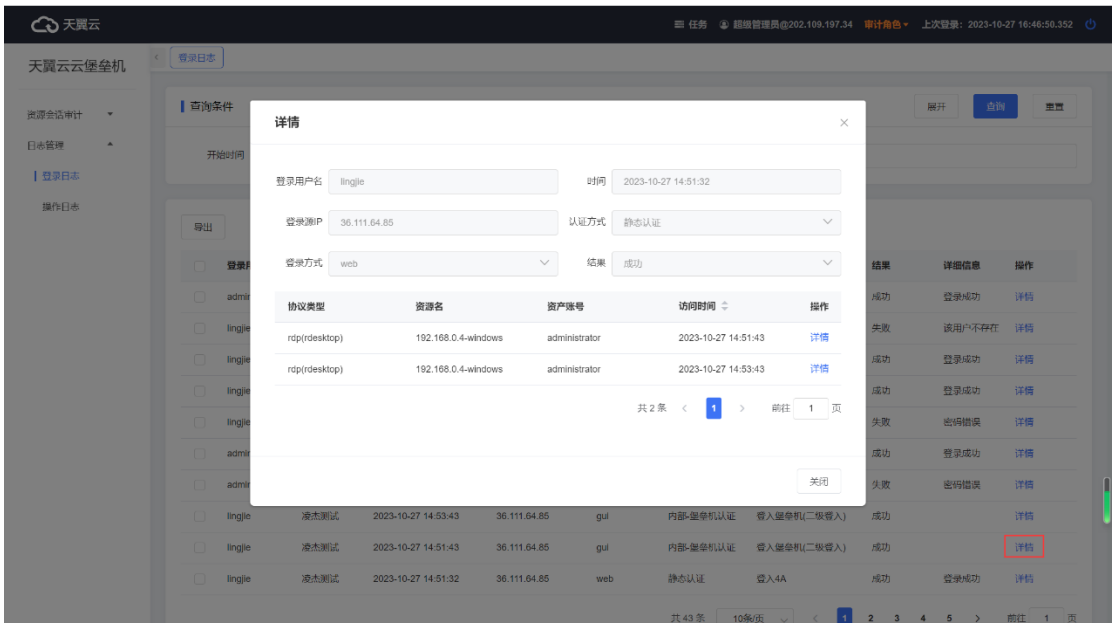
管理员登录并切换至 审计角色，打开 审计管理>日志管理>登录日志：



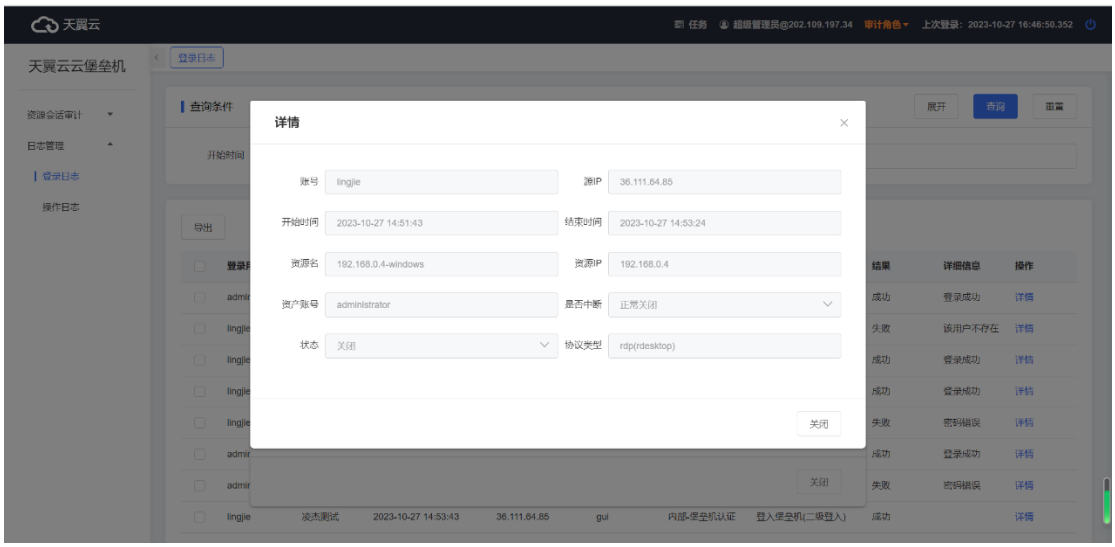
审计范围包括登录成功与登录失败（密码错误、账号不存在等）的情况。



点击详情，可查看用户登录系统后访问资产的信息。



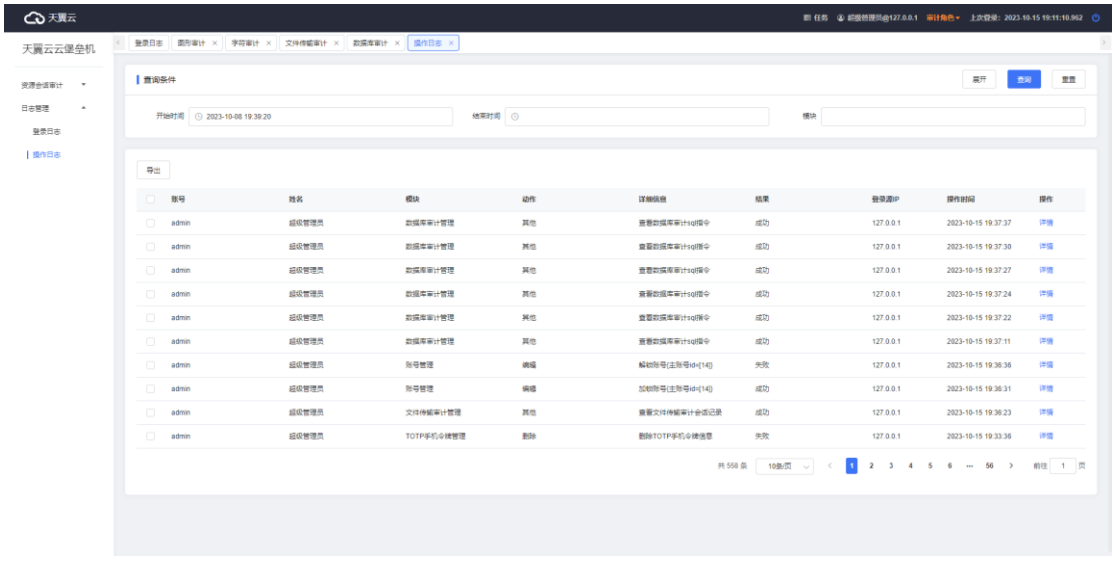
单击某条资产访问的详情，从更多维度展示该次访问会话的信息。



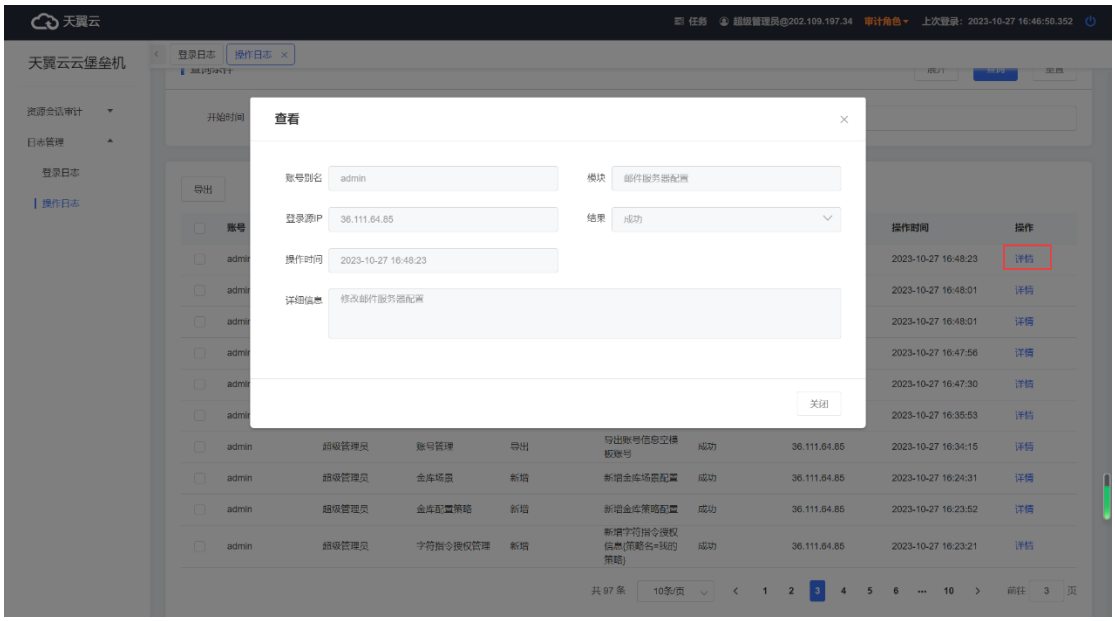
6.7.2 操作日志

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。

管理员登录并切换至 审计角色，打开 审计管理>日志管理>操作日志：



点击详情可查看该条记录的详细信息。



7 最佳实践

7.1 数据库运维实名审计

背景

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

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

同用户使用需求。

数据库运维流程

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

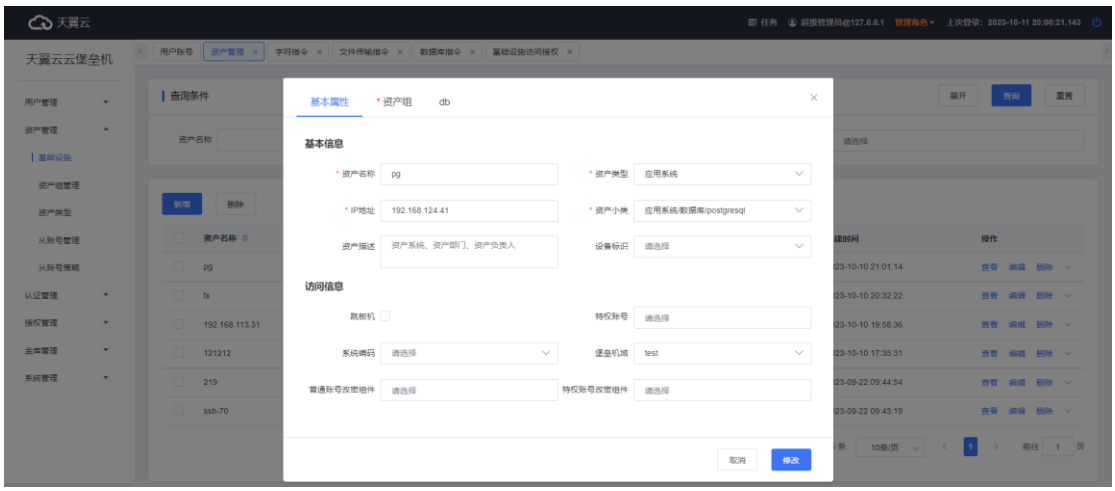
前提条件

- 已在本地安装数据库访问客户端，如 Navicat、DBeaver 等。
- 已将数据库资产纳入堡垒机进行管理。
- 已获取相关资产访问权限。

操作步骤

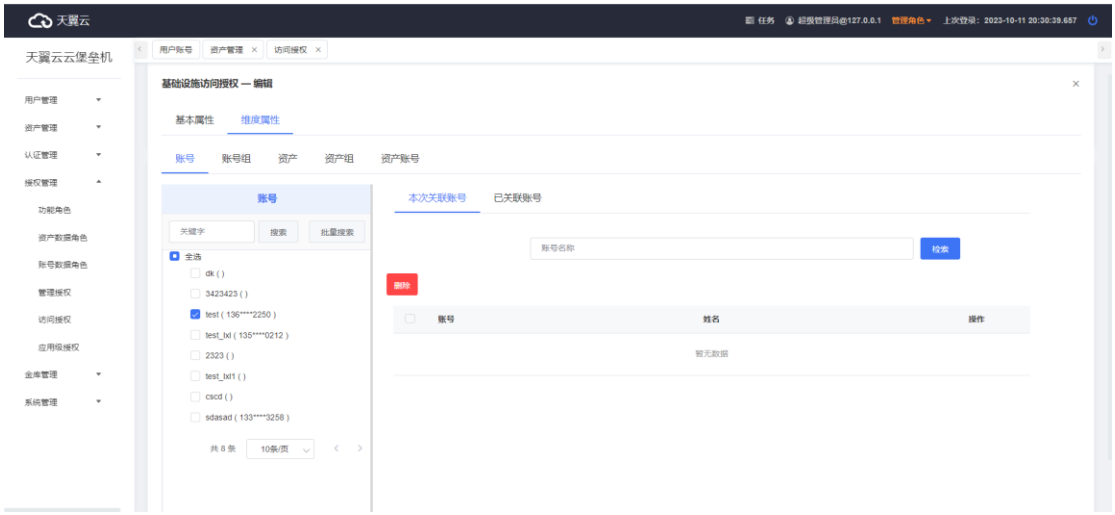
管理员将数据库资产纳入堡垒机进行管理

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



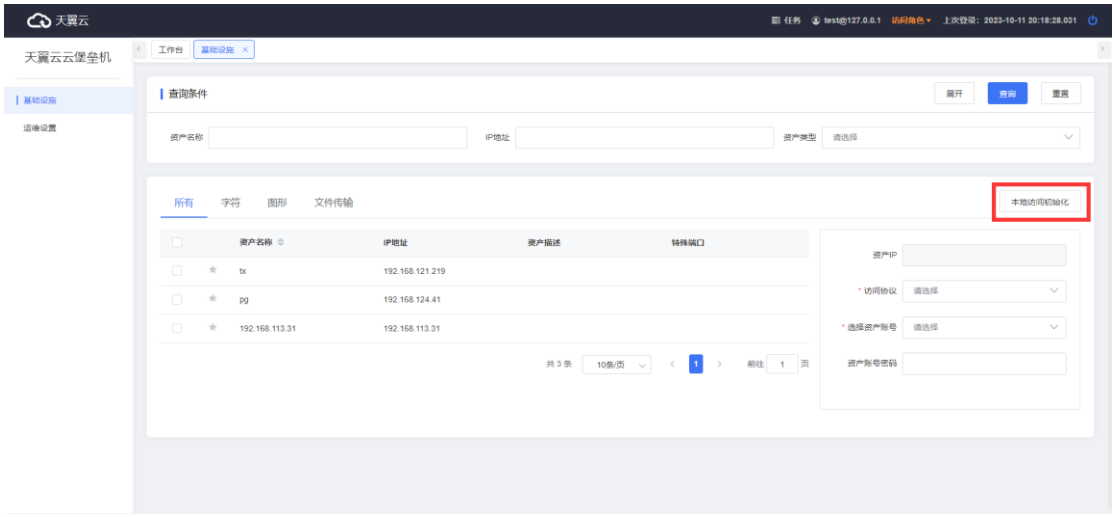
管理员对数据库资产进行授权

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



运维人员触发“本地访问初始化”进行运维

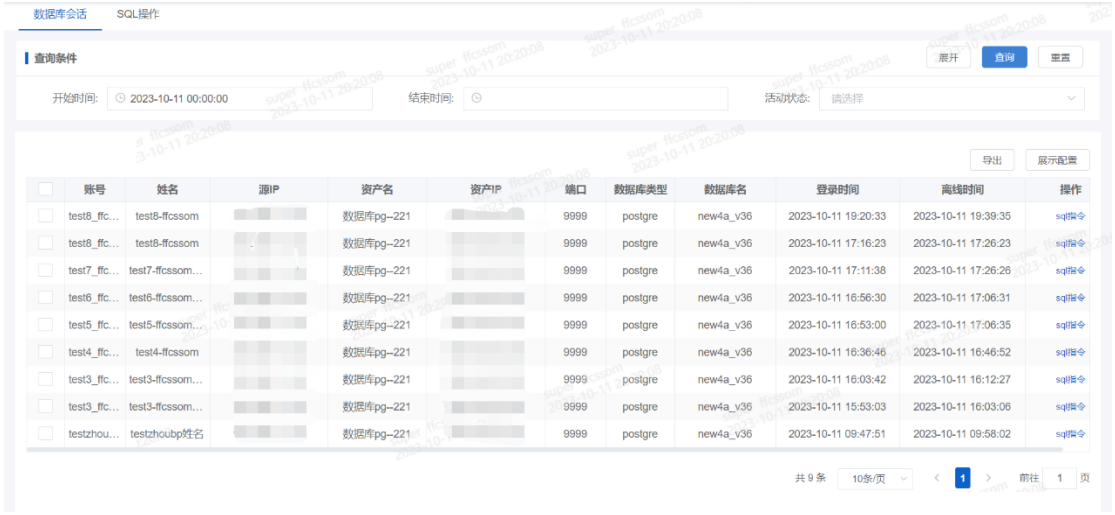
1. 运维人员登录堡垒机。
2. 左侧菜单选择“资产访问”。
3. 在资产访问页面，点击“本地访问初始化”后，系统后台将策略下发到本地，下发成功后将弹出提示。



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

数据库运维审计

1. 审计管理员登录堡垒机。
2. 左侧菜单选择“资源会话审计>数据库审计”。
3. 在数据库审计页面查看运维会话记录。



7.2 收敛资产运维暴露面

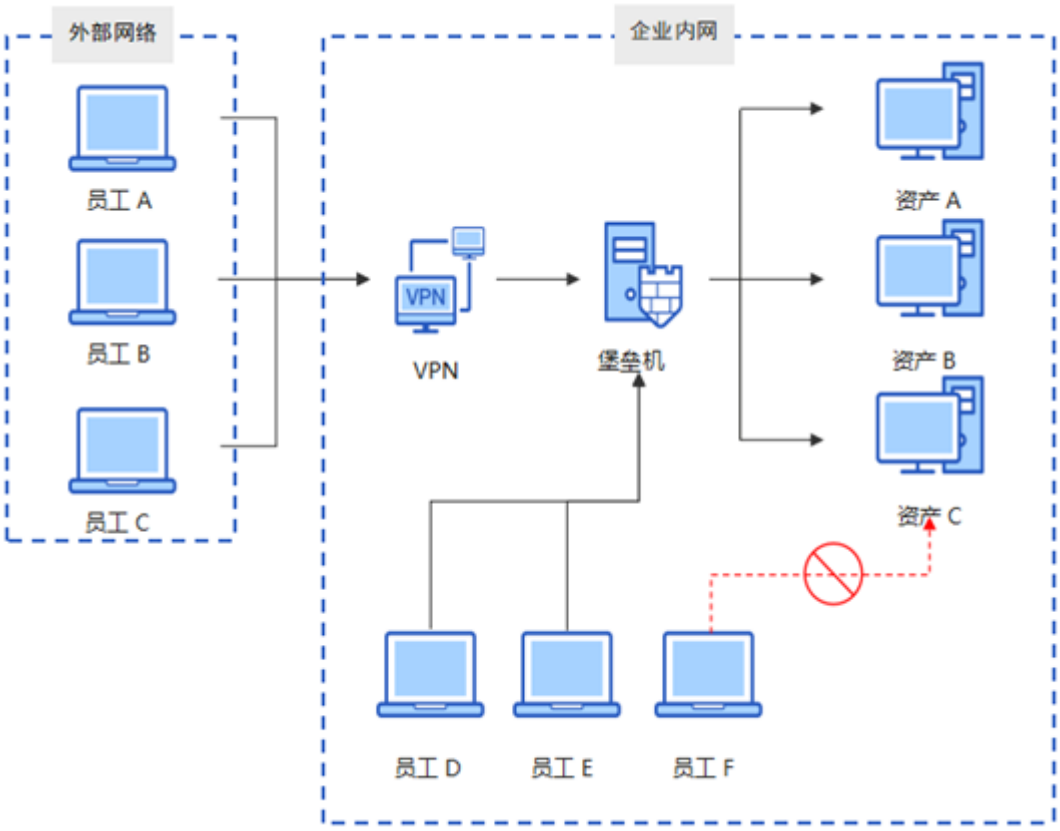
背景

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

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

解决方案

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



说明

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

7.3 资产运维细粒度权限管控

背景

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

天翼云堡垒机提供完善的用户访问授权和精细的操作权限管控，非授权用户无法访问指定资

产，授权用户访问资产后无法执行未授权的指定敏感操作。

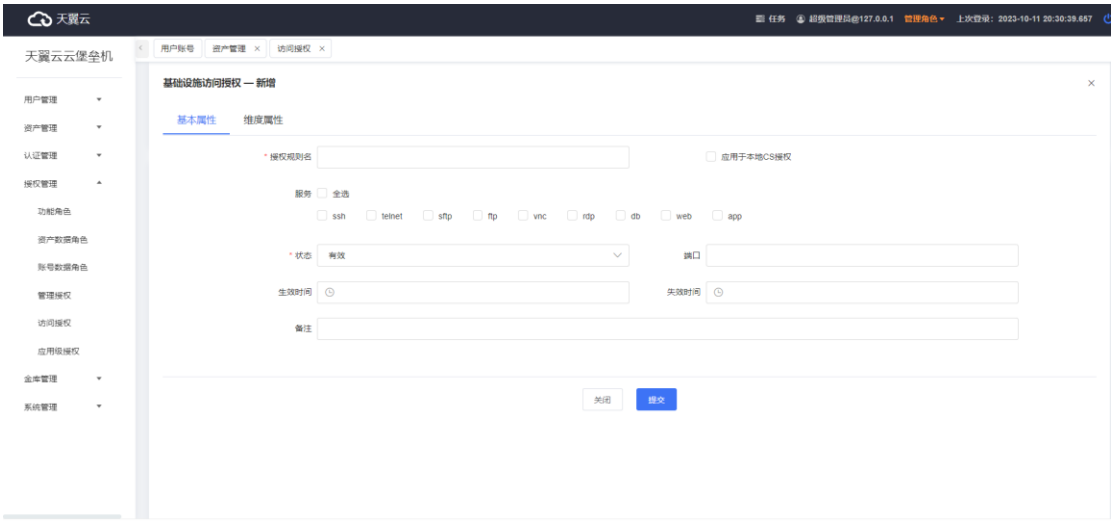
解决方案

一、访问授权

1、管理员登录堡垒机。

2、左侧菜单选择“授权管理>访问授权”。

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



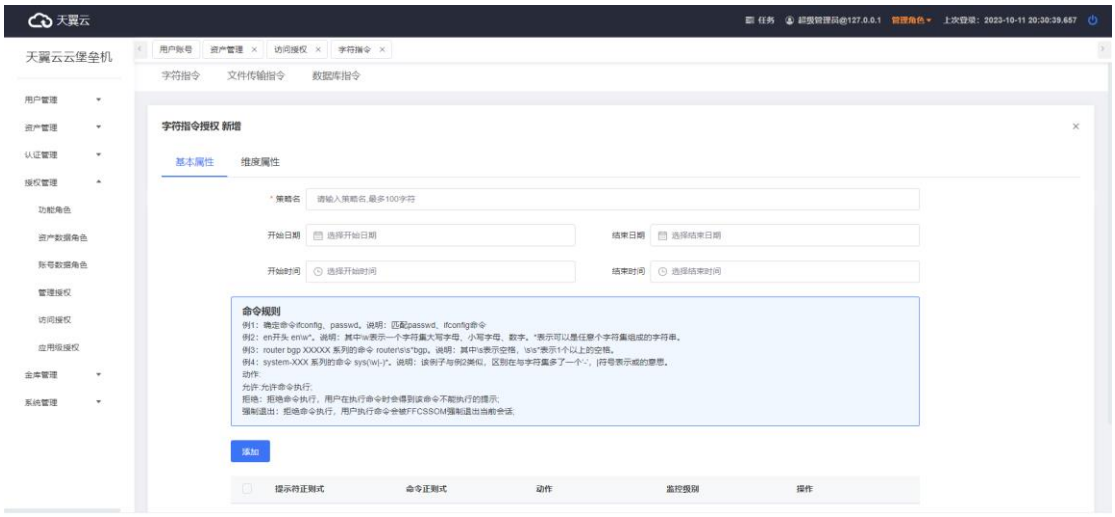
4、配置完成后，表示主账号(人员账号)可以在指定有效期内，使用指定的资产账户访问指定的资产。

二、应用级操作授权

1、左侧菜单选择“授权管理>应用级授权”。

2、支持字符命令、文件传输操作和数据库指令的操作配置。

3、在“字符指令”标签页点击“新增”，切换至字符指令授权页。在基本属性模块可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。



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

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

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

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

8 常见问题

8.1 常见问题

8.1.1 产品类

- **天翼云堡垒机支持纳管所有 region 上服务器吗?**

取决于云堡垒机到服务器的网络是否可达。

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

- **使用云堡垒机时需要配置哪些端口?**

为了能正常使用云堡垒机，推荐开放 18443,18000 端口的入方向安全组策略规则，其他端口根据运维场景需要按需进行配置。

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	需通过堡垒机使用 mstsc 客户端维护图形类协议资产时，

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

- **云堡垒机支持管理哪些数据库?**

数据库引擎	引擎版本
Mysql	5.5,5.6,5.7,8.0
PostgreSQL	10,11,12,13
Oracle	10g,11g,12c

- **如何配置云堡垒机的安全组?**

参考 3.1 步骤一：安全组策略设置。

- **云堡垒机是否支持纳管非天翼云服务器?**

支持。

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。

- **租户是否能进入云堡垒机的操作系统?**

不可进入。

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

- **资产数是什么?**

资产数表示云堡垒机管理的虚拟机等设备上运行的资源数，资产数不以设备的数量计算，而是以所管理设备上资源的数量计算，一个设备内可能有多种资源形式，包括不同协议的主机，不同类型的应用等。例如，目前有一台虚拟机，在云堡垒机中添加这台虚拟机的资源，分别添加了 2 个 RDP、1 个 TELNET 和 1 个 MySQL 协议的主机资源，以及 1 个 Chrome 浏览器的应用资源，那么当前管理的资产数即为 5，而不是 1。

8.1.2 订购类

- **同一账号可以购买多个云堡垒机吗?**

同一个账号在同一可用区内可购买多个云堡垒机，不同堡垒机之间数据完全独立。

- **云堡垒机到期后，还能继续使用吗?**

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

说明

- 天翼云在用户实例冻结前，以及资源销毁前将通过短信或邮件方式提醒用户。

- 为避免因未及时续费而导致云堡垒机正常运行，建议在购买云堡垒机时开启自动续费。

- **若当前版本云堡垒机支持的资产数不够时，是否可以升级?**

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

操作方式参见 2.3 变更资产规格。

注意

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

- **云堡垒机变更规格可以降低资产规格吗?**

不支持。

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

- **如果需要纳管的资产数小于标准的售卖资产规格该如何选择规格?**

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

例如，您现在有 15 资产，则您需要选购 20 资产套餐规格。

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

在购买云堡垒机实例时，为降低网络时延，建议配置云堡垒机实例与 ECS 等资源在同一区域同一 VPC 网络。堡垒机实例的 VPC 信息在购买时指定，后续不能修改。

- **如何选择云堡垒机实例区域和可用区?**

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

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

8.1.3 操作类

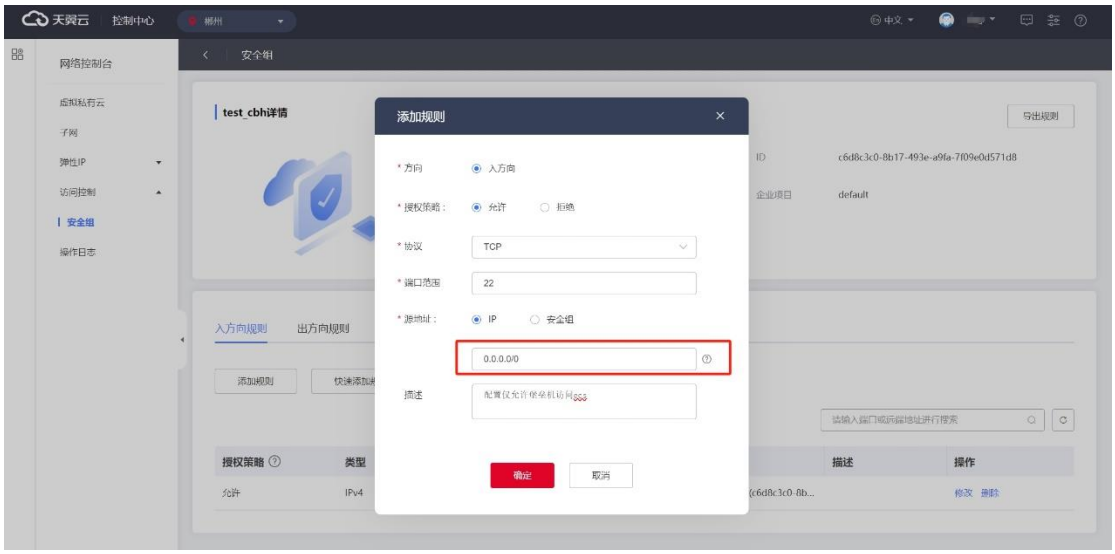
- **如何防止云堡垒机运维的服务器被绕过?**

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

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

操作步骤

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



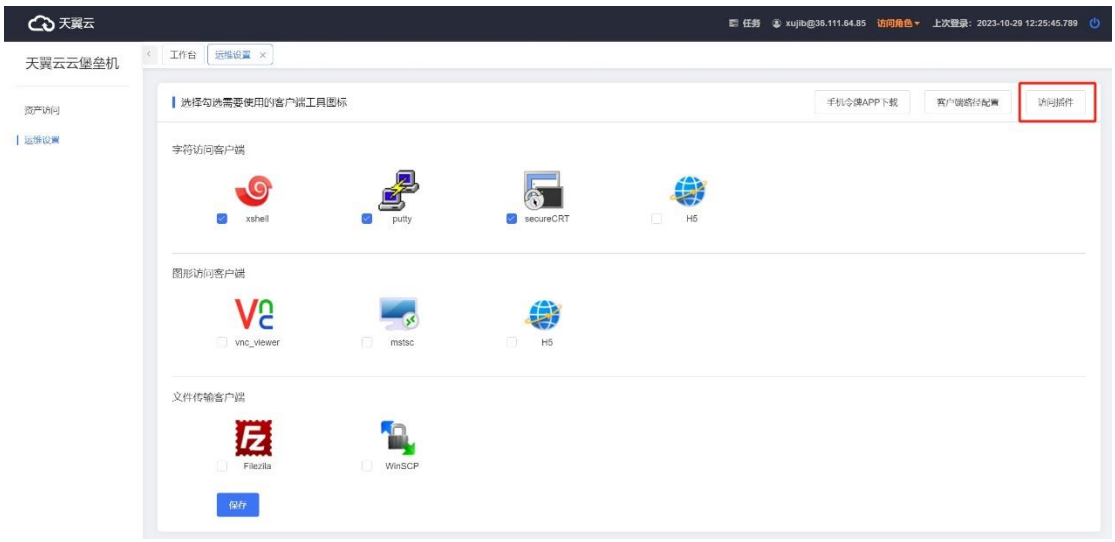
- **访问时页面提示“请确认是否安装访问插件”如何处理?**

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

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

操作步骤

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



3. 下载完成后，安装客户端插件。
4. 设置运维客户端本地安装路径，点击运维-客户端路径配置，配置您的运维工具本地路径。

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

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

账号密码被锁定主要有以下几种情况:

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

忘记密码

在云堡垒机实例登录页面点击忘记密码，通过注册邮箱重置密码，解锁账号。

注意

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

操作步骤

1. 进入云堡垒机登录页，点击忘记密码。

2. 输入用户名、邮箱等信息，验证用户身份。

3. 输入新登录密码，点击确定后，密码重置成功。

密码过期锁定

在云堡垒机实例登录页面点击自助解锁，通过注册邮箱解锁账号。

注意

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

操作步骤

1. 进入云堡垒机登录页，点击自助解锁链接。

2. 进入自助解锁功能后，输入用户名、邮箱和动态验证码，验证用户身份。
3. 输入更新后的密码，注意输入密码需要符合密码安全策略，点击确认。
4. 解锁成功。

其他原因账号被锁定

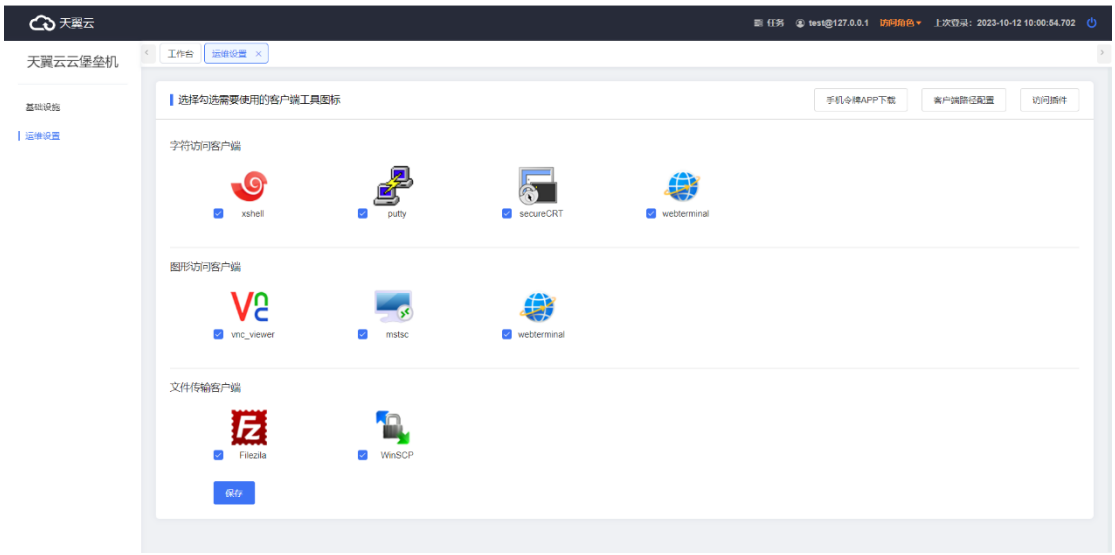
联系管理员解锁。管理员登入云堡垒机管理后台，在账号管理中可解锁用户账号、更改密码。

- **无法正常启用客户端运维工具运维资产**

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

1、确认是否配置需要使用的客户端工具

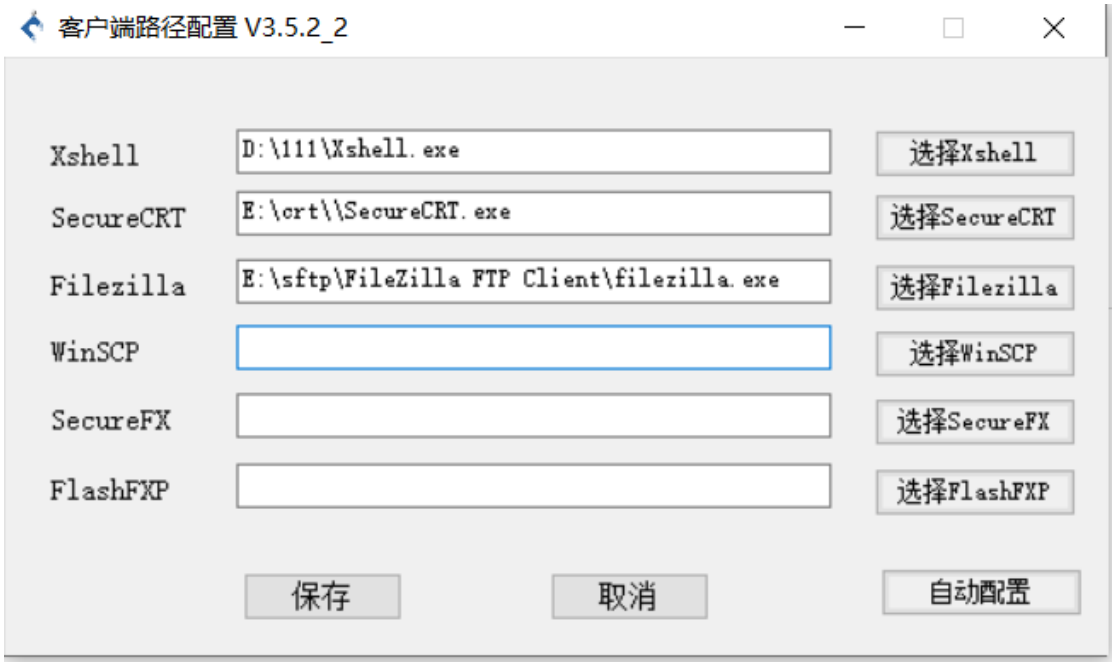
打开运维设置，勾选要调用的客户端，保存配置。



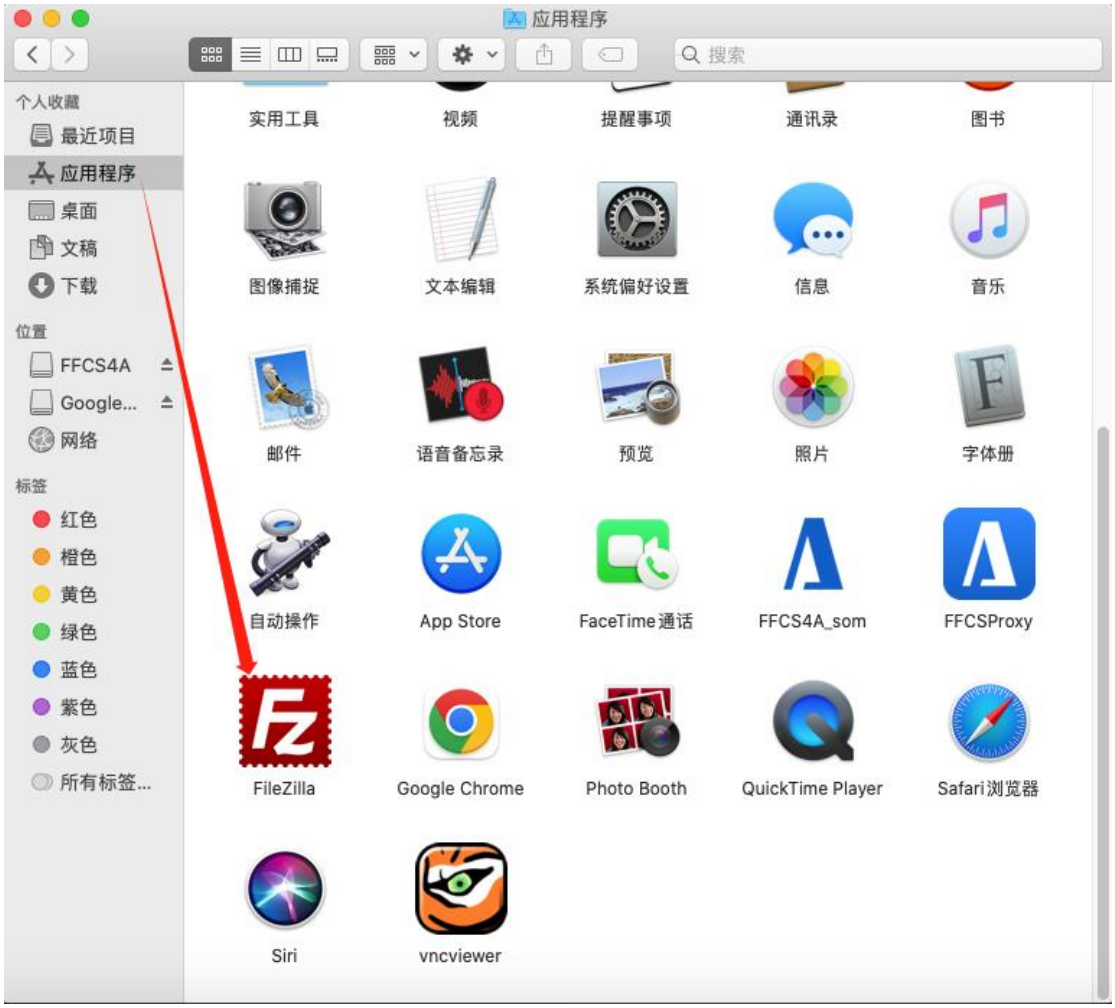
2、确认是否已正确安装并配置客户端工具。

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

Windows 的客户端路径配置，需要将软件启动程序文件路径严格配置到运维设置-客户端路径配置中。例如：Xshell 默认安装路径 C:\Program Files (x86)\NetSarang\Xshell 7\Xshell.exe，其他的软件或者安装到了其他的路径，根据自己的实际情况配置即可。



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



- **访问资产提示“登录设备失败，设备账号或密码错误”，怎么解决?**

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

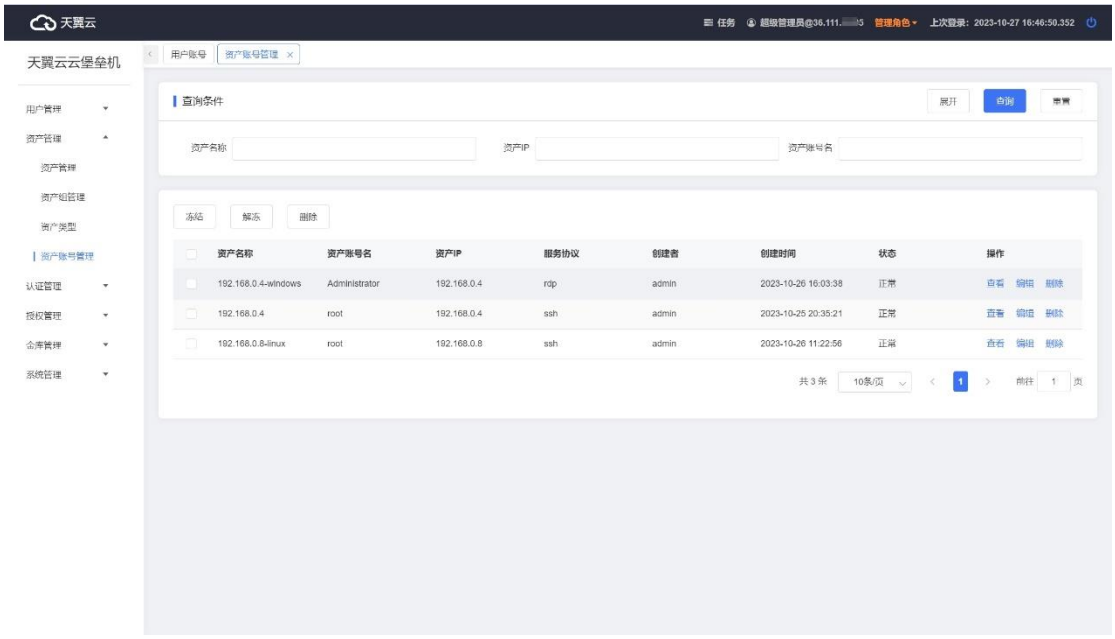
操作步骤

1. 管理员登录云堡垒机实例控制台，访问角色切换为管理角色。

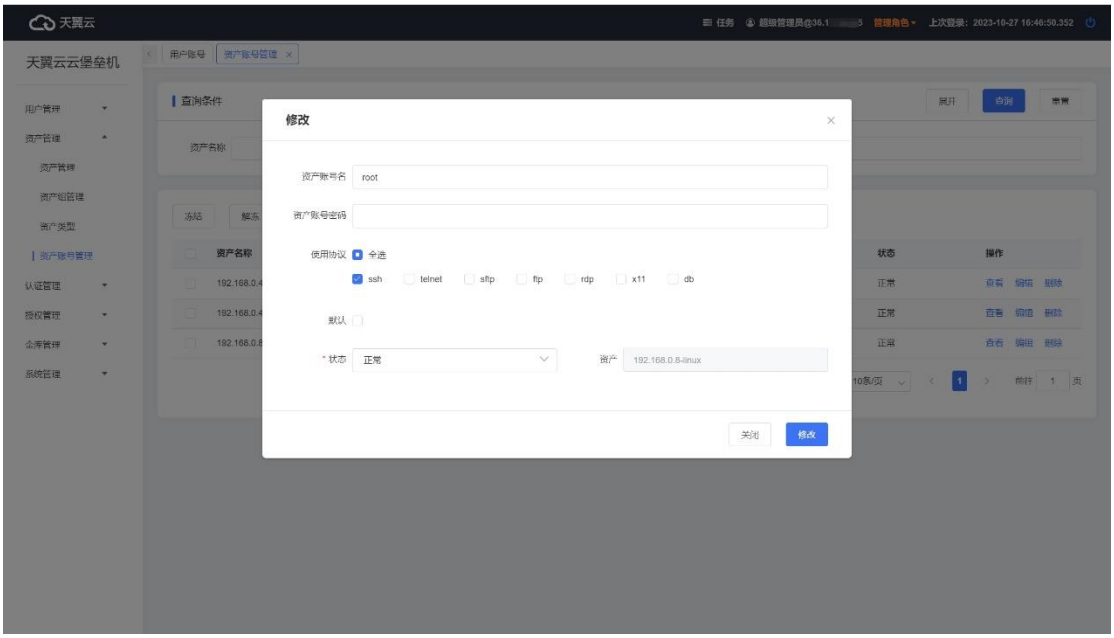
2. 进入资产管理-资产账号管理。

3. 按资产 IP 或资产名称搜索需要修改账号或密码的资产。

4. 点击资产操作栏编辑链接，编辑资产账号。



5. 更新资产账号、密码及应用的协议。



- **运维用户客户端无法访问用户资产如何处理?**

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

注意

请先确认以下配置均已正确配置：

1. 运维终端已正确安装访问插件，并配置访问路径。

2. 用户拥有访问及运维资产的授权。

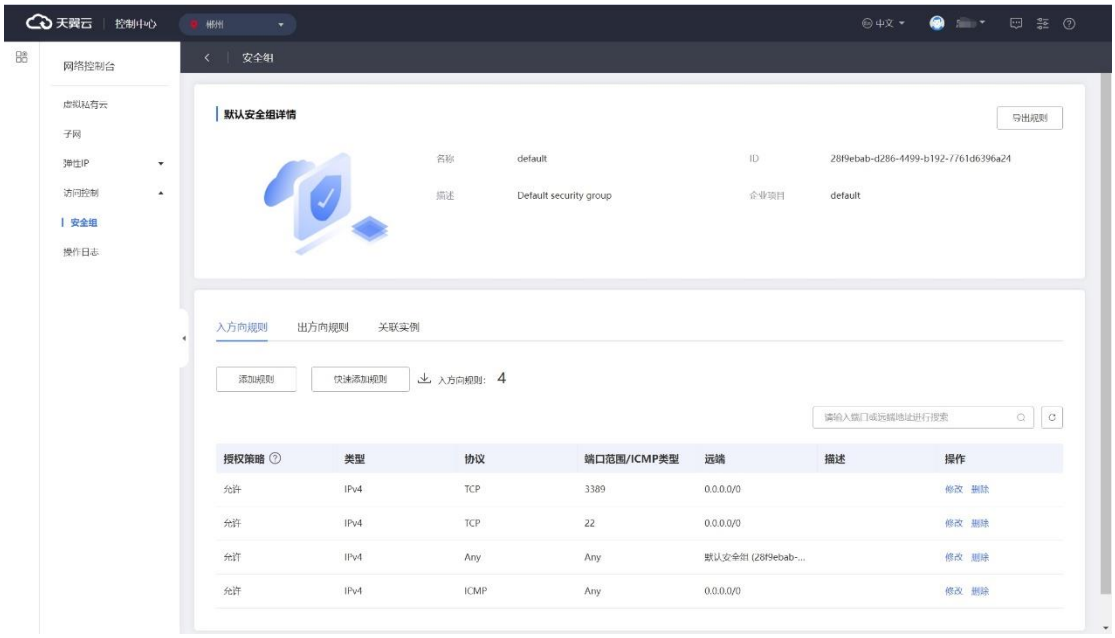
排查步骤

1、检查客户端到云堡垒机网络是否能连通。

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

2、检查堡垒机到运维资产网络是否能连通。

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


天翼云
控制中心
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
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