★完全公开

奇安信
新一代网络安全领军者

奇安信网神运维安全管理系统产品白皮书

地址：北京市西城区西直门外南路26号院1号

邮编：100044

● 版权声明

● 免责声明

本免责声明（**“本声明”**）适用于奇安信集团（包括但不限于奇安信科技集团股份有限公司、奇安信网神信息技术（北京）股份有限公司、北京网康科技有限公司，以及前述主体直接或者间接控制的法律实体）旗下推出的全部产品和/或服务（以下统称**“本产品”**）。**如您使用前述产品，即表示您同意接受本声明的一切内容。如果您不同意接受，请立即停止使用相关产品。**

奇安信集团有权随时自行决定修改、添加或删除本声明的全部或部分内容。**您有责任定期检查免责声明部分的内容**，以了解是否发生了变更。**如您在我们发布变更后继续使用本产品，即表示您接受并同意这些变更。**

1. 您明确理解并同意，**本产品按“现状”提供**，不存在任何形式的明示或暗示保证，并且在适用法律允许的最大范围内，奇安信集团不提供任何明示或暗示的陈述或保证，包括但不限于有关适销性、适用于特定目的以及不侵犯第三方权利的保证。奇安信集团不保证产品中所含的功能将满足您的全部要求，也不保证您对本产品的使用不会中断或出错。**选择本产品来达到预期结果，以及安装、使用本产品并获取结果所带来的所有责任和风险由您承担。**

2. 奇安信集团承诺致力于不断提升产品的质量，本产品是在现有技术水平基础上提供的，但奇安信集团无法保证您使用本产品将完全符合您的期望，包括但不限于不能保证您【通过使用产品能够发现所有的安全漏洞以及能检测到所有的入侵威胁，检测到的入侵威胁不保证完全正确】，**您理解并同意，出现前述不符合您对产品期望的情形不视为奇安信集团违约。**

3. 您明确理解并同意，**您在使用本产品过程中可能发生不可抗力或不可预见的情形，包括但不限于：1)被某些未经许可的个人、团体或机构通过某种渠道获得或篡改；2)因通信繁忙出现延迟，或因其他原因出现中断、停顿或数据不完全、数据错误等情况，从而使交易出现错误、延迟、中断或停顿；3)因地震、火灾、台风及其他各种不可抗力因素引起的停电、网络系统故障、电脑故障等；4)计算机系统可能因存在性能缺陷、质量问题、计算机病毒、硬件故障及其他原因；黑客攻击、计算机病毒侵入或发作等非可归责于奇安信集团的原因；5）政府管制、网络故障、国家政策变化、法律法规之变化等。如发生不可抗力或不可预见的情形，奇安信集团将尽最大努力予以补救，但奇安信集团对于因不可抗力和不可预见的情形造成的各类直接或间接损失，均不承担任何责任。**

4. **对于任何本产品的使用行为，包括但不限于您自身和/或任何第三方的行为，奇安信集团均不承担任何责任。**

5. 对于从**非奇安信集团指定途径以及从非奇安信集团发行的介质上获得的本产品**，奇安信集团无法保证其是否感染计算机病毒、是否隐藏有伪装的特洛伊木马程序或者黑客软件。**使用此类产品，将可能导致不可预测的风险，建议用户不要轻易下载、安装、使用，奇安信集团不承担任何由此产生的一切法律责任。**

6. **上述免责声明适用于因任何性能故障、错误、遗漏、中断、删除、缺陷、操作或传输延迟、电脑病毒、通信线路故障、失窃、毁坏、未经授权的访问、篡改或使用（无论是出于违约、侵权、疏忽或任何其他诉因）而导致的任何损害、责任或伤害。**

7. 奇安信集团保留在**不发布通知**的情况下随时采取以下行动的权利：**在执行常规或非常规维护、错误纠正或其他更改所必需时，中断或修改本产品的任何组成部分的运行或功能。**

8. 本声明受中华人民共和国法律的约束并依据其解释。

9. 在法律允许的最大范围内，本声明最终解释权归奇安信集团享有。

修订记录

版本	状态	修订理由和内容摘要	修订人	批准人	修订日期
V1.0	C	新建	曾友钱	许瑞强	2021/7/12
V1.1	M	更新到 3.4.36.0 版本	孙一迪		2022/9/26
V1.2	M	更新新标准型号	孙一迪		2022/11/9
V1.3	M	更新到 3.4.38.0 版本	孙一迪		2022/12/1
V1.4	M	更新 logo，更新型号	吴凡		2024/12/27

状态：C-创建，A-增加，M-修改，D-删除

数据安全分级标注说明

■ 数据分级	公开数据（Y）	内部数据（）	普通商秘（）	核心商秘（）

*数据分级标注及说明：

1、文档编写前，应标注数据安全级别，默认为内部；

2、请根据文档内容评估数据安全级别，在对应数据级别（）中填写（Y）；

3、分级 TIPS：

【核心商秘】：限于个别人、小范围共享和使用的信息，例如薪酬数据、未公开的产生严重危害的样本等。如泄露将导致法律风险或者影响到社会公众利益或者严重的恶意竞争等；

【普通商秘】：限于特定人群、特定范围内共享和使用的信息，例如公司组织架构、产品样本集等。如泄露存在合规风险或者可能影响社会公众个人利益或者存在一般恶意竞争的风险等；

【内部数据】：限于在公司范围内按需使用，除去公开数据、核心商秘、普通商秘，都为内部数据。如泄露不存在法律合规风险或不存在影响社会公众个人利益的风险，但会产生轻微的恶意竞争风险等；

【公开数据】：对任何方面都无危害的、不会被任何方面进行利用的信息，例如官网上的产品简介等。如泄露对任何方面都无影响。

更多分级 Tips 参考链接: https://sec.qianxin-inc.cn/data-security/data-classification-tips

目录

1 产品概述

1.1 产品简介

奇安信网神运维安全管理系统（以下简称“本产品”或“堡垒机”）是具备全方位的运维安全风险控制能力的安全管理与审计产品。本产品支持对网络设备、数据库、安全设备、主机系统等资源的运维与审计，通过集中化运维管控、运维过程实时监管、运维访问合规性控制、运维过程图形化审计等功能，为客户的数据中心运维构建一套完善的事前预防、事中监控、事后审计安全管理体系，广泛满足政府、金融、能源、电力、教育、医疗、央企等行业客户的运维审计规范要求。

奇安信网神运维安全管理系统产品系列丰富齐全，包含标准产品（C6100 系列）、软件部署（C6100-BH-C、C6000-BH-Cloud）、信创产品（BH3300 系列）、涉密分保产品（C3200 系列）等，可根据客户实际需求进行配置。

1.2 产品定位

奇安信网神运维安全管理系统是采用新一代智能运维技术框架，集认证管理（Authentication）、授权管理（Authorization）、账户管理（Account）、操作审计（Audit）的于一体，具备全方位的运维安全风险控制能力的安全管理与审计产品。

1.3 产品形态及构架

1.3.1 产品构成

堡垒机主要由以下四大功能构成：

- 认证管理

堡垒机可以协助客户建立基于唯一身份标识的全局实名制管理制度。根据用户场景的实际需要，为不同用户提供不同类型的认证方式，既支持基本的静态口令方式，又能够提供双因子认证方式，例如 OTP 口令、USBKey、短信验证码。同

时，堡垒机还能够集成现有认证方式，例如 AD 域、LDAP、Radius，实现用户认证的统一管理。

- 授权管理

堡垒机能够集中管控用户角色权限细粒度划分，既可以添加删除部门、添加删除资源、添加删除人员、修改授权、系统配置等，也可以实现对操作命令、文件传输权限、剪切板操作权限、数据库SQL 语句的控制。堡垒机基于最小权限原则设置统一的访问控制策略和细粒度的命令级授权策略。

- 账户管理

堡垒机提供统一集中的资源账户管理方案，支持管理的资源包括主流的操作系统、网络设备、安全设备和数据库等资源，不仅能够实现被管理资源账户的创建、删除和同步等账户管理生命周期所包含的基本功能，而且也可以通过堡垒机进行资源账户改密策略的设定，定期修改资源账户的密码。

- 操作审计

堡垒机能够基于唯一身份标识，通过对用户从登录到退出堡垒机的全程操作行为进行审计，监控用户对目标设备的所有操作，聚焦关键事件，实现对安全事件的实时发现与预警。同时，通过对用户所有的操作日志集中记录管理和分析，不仅可以对用户行为进行监控，并且可以通过集中的审计数据进行数据挖掘，以便于事后的安全事故责任的认定。

1.3.2 产品架构

堡垒机产品由系统管理控制台、功能业务模块和基础服务模块构成，总体架构如下图所示：

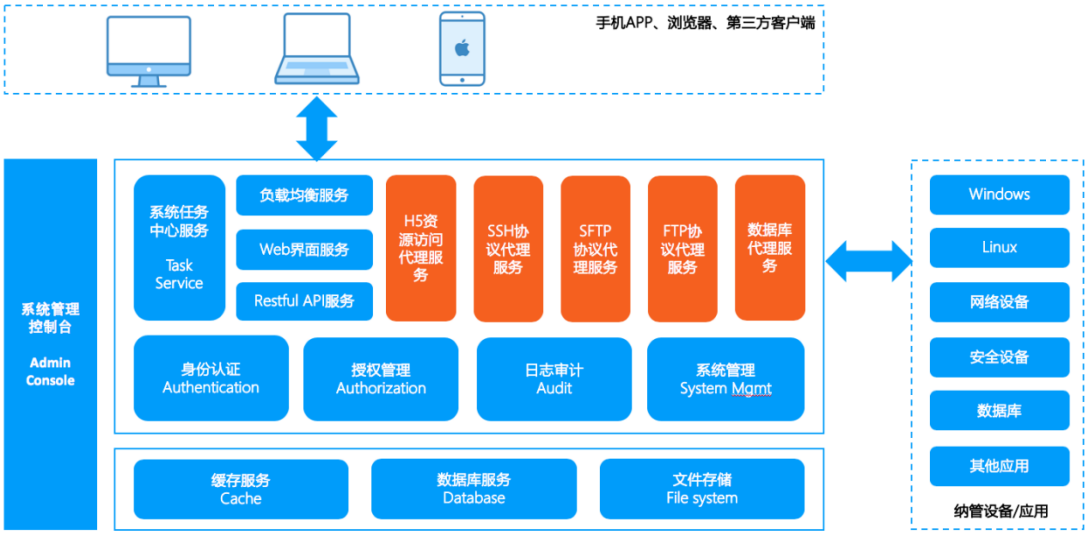


图 1 系统架构

- 系统管理控制台

提供系统的基本配置功能，包括网络配置、时间配置（NTP服务器同步时间）、重启、关机等，并提供系统服务的状态查询。

- 功能业务模块

提供身份认证、授权管理、日志审计、系统管理等功能，提供任务中心、Web 界面、Restful API 等服务，提供 H5 资源访问、SSH 协议、FTP/SFTP 协议、数据库协议等代理服务。

- 基础服务模块

提供缓存、数据库和文件存储等基础服务模块。

2 产品功能

堡垒机提供了丰富、全面的管控功能，帮助企业解决运维过程不透明、责任认定难、管理不规范、权限混乱、控制力度不足、审计不全面等难题，同时统一管理企业信息系统资源。

2.1 身份管理

堡垒机主账号通过本地认证、AD 认证、RADIUS 认证等多种认证方式，将主账户与实际用户身份一一对应，确保行为审计的一致性，从而准确定位事故责任

人，弥补传统网络安全审计产品无法准确定位用户身份的缺陷。

堡垒机数字身份认证，依据 GB/T39786-2021 等相关技术规范，支持使用国密算法（SM2/SM3/SM4）实现基于数字证书的身份认证、SSL 加密协议，并支持使用国密密钥对运维日志进行加密保存。并且能通过对接客户方国产化服务器，满足密评中关于“身份鉴别”、“安全通道”和“数据安全”的测评要求。

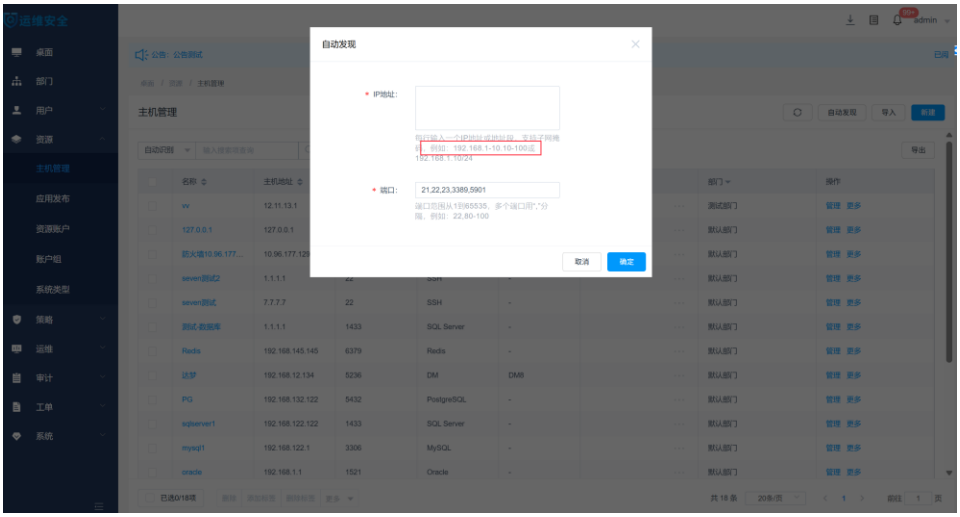

数据安全配置
* 用户密码:
数据安全配置:
开启后，会对数据完整性进行校验，请确认是否开启
数据完整性校验方式:
加密卡
加密机
请选择一种方式进行数据完整性校验，配置成功后无法更改，请谨慎操作!
取消
确定
数据安全配置
* 用户密码:
数据安全配置:
开启后，会对数据完整性进行校验，请确认是否开启
数据完整性校验方式:
加密卡
加密机
请选择一种方式进行数据完整性校验，配置成功后无法更改，请谨慎操作!
* 设备厂商:
奇安信
* 服务器地址:
请输入认证服务器的IP地址和端口，格式：IP地址：端口，例如：ndsec://192.168.1.100:24
* 密钥:
请输入认证服务器密钥!
上传授权文件:
上传
请上传认证服务器的授权文件!
取消
确定

2.2 角色分权

堡垒机预置多种用户角色：系统管理员、部门管理员、安全管理员、审计管理员、运维员。每种用户角色的权限都各不相同、相互制约。部门管理员负责本部门的用户和资源的管理，并制定访问控制策略，授权用户去访问资源的权限；审计管理员进行本部门用户的运维操作审计；运维员负责访问资源进行日常的运维、升级等工作。除了预置的角色之外，堡垒机支持自定义角色，如下图所示，通过角色的自定义，满足企业单位的复杂运维场景，为设立不同的角色提供了选择。

堡垒机在用户管理方面具备用户信息的批量修改，包括但不限于重置密码、更改所属部门、更改角色、修改多因子配置、修改用户有效期、修改登录时间段限制、修改 IP 限制、修改 MAC 限制等。可批量按照人员、人员组及运维资源、运维资源组进行权限划分。

堡垒机支持增加批量添加运维资源和用户，添加时能按需授权。



2.3 集中管控

通过集中的访问控制策略定制，帮助企业单位梳理用户与资源的关系，并且提供一对一、一对多、多对一、多对多的灵活授权模式。堡垒机提供的访问控制策略，实现的不仅仅是将资源授权给用户，更实现了功能权限的精细化控制，最大程度地降低越权操作的可能。

2.4 资源改密

在传统的运维模式下，管理员需要定期手动修改资源账户的密码，同时维护起来也比较繁琐。通过堡垒机提供的改密策略，实现自动化的改密，并且以日志形式记录改密执行结果，让管理员掌握资源的改密动态和历史密码。支持密码强度校验功能，支持设置固定密码强度或自定义密码强度，可以设置 8 到 32 位密码长度，支持密码相同校验且设定次数，支持密码修改周期设定。支持用户登录失败超过设定次数后锁定 IP 和账号，锁定时间可自定义，管理员可解除锁定，锁定时长可自定义；产品支持用户的登录时间、来源 IP 地址和来源 MAC 地址限制（黑名单和白名单）。

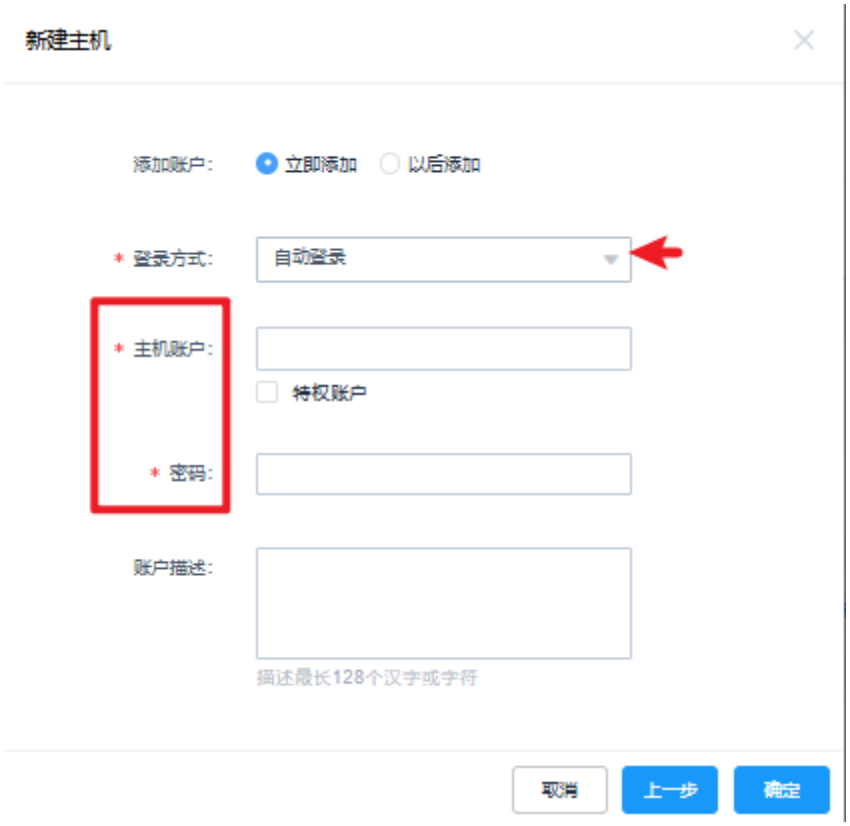
堡垒机支持以 IP 地址、目标运维资源账户、账户组、时间、改密周期、改密方式生成详细的改密计划，到期自动执行；支持改密计划立即执行，但是执行前需要输入用户密码以确认身份，保障安全性；系统支持随机生成不同、相同密码或者手动指定密码，可设置改密密码复杂度。

堡垒机支持生成改密日志，内容应包括改密后 IP、账号信息、改密结果的详细信息；支持批量导出改密操作中尝试修改的密码。

堡垒机支持改密日志的下载，且下载时需要输入用户密码以保障安全。

2.5 资源访问

堡垒机支持托管主机、网络设备、安全设备、数据库和应用发布的账户和密码，运维人员可单点登录到目标资源进行运维操作，无需输入账户和密码。同时，堡垒机支持 SSH、RDP、Telnet、VNC、FTP、SFTP、SCP、DB2、MySQL、SQL Server、Oracle、Rlogin、DM、Redis、PostgreSQL 等协议资源账户密码自动登录，无需用户手动输入账号或密码，避免重要资产账号及密码泄露。

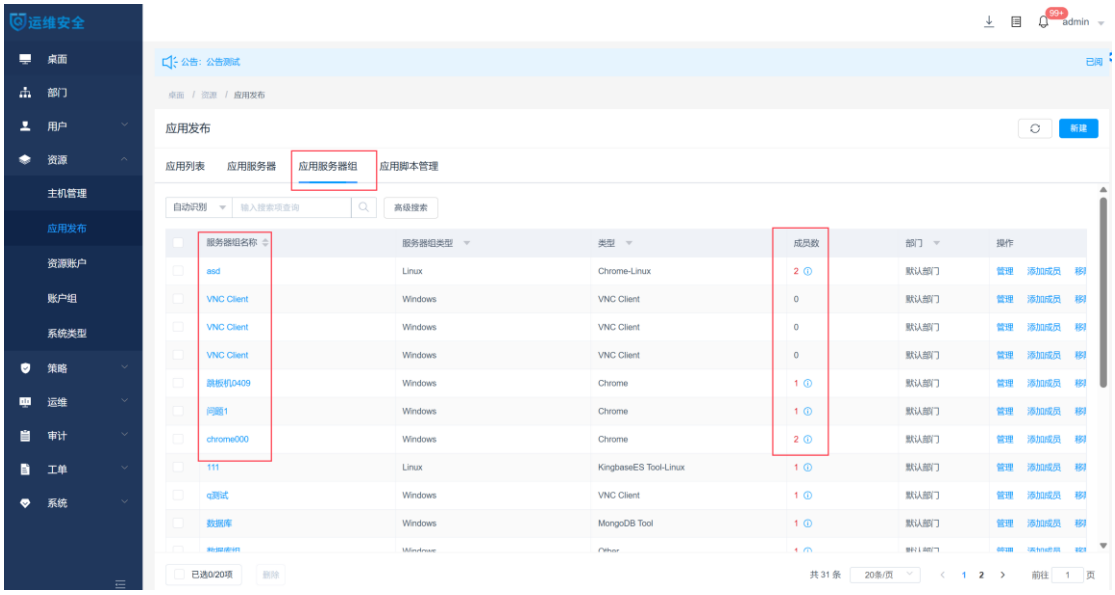



Web运维配置
RDP
SSH
FTP/SFTP
连接模式:
admin console
* 运维方式:
H5页面
取消
确定


Web运维配置
RDP
SSH
FTP/SFTP
* 运维方式:
H5页面
取消
确定

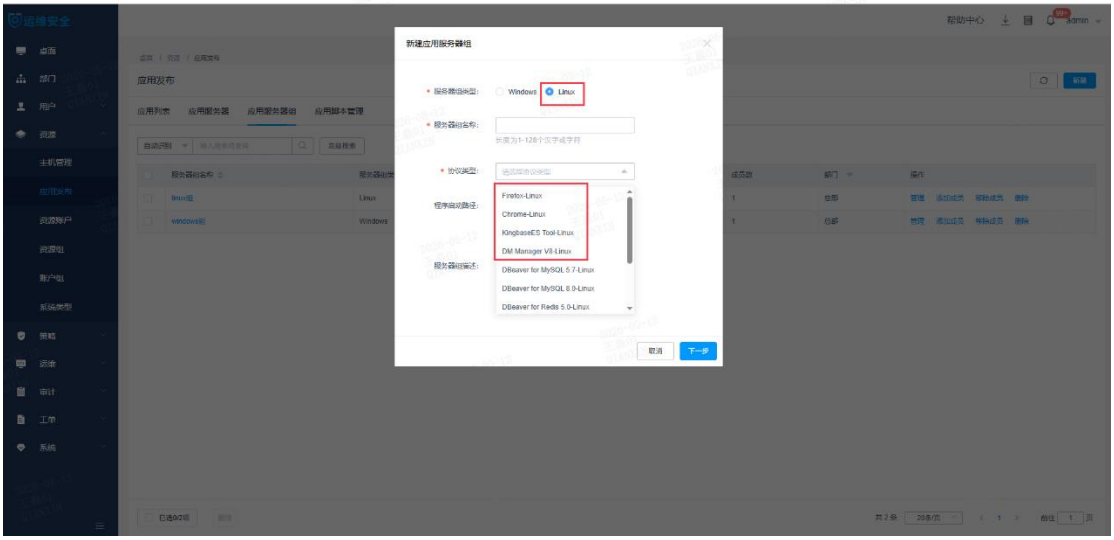

Web运维配置
RDP
SSH
FTP/SFTP
* 运维方式:
H5页面
取消
确定

支持对于 web 资源提供密码代填，无论被接入的应用资源如何设计登录动作，通过应用发布密码代填功能都可以实现单点登陆。应用发布服务器支持集群功能。



另外，如果用户本身更习惯客户端的方式进行运维，堡垒机也支持使用 XShell、Putty、SecureCRT、MSTSC、Navicat、PLSQL 等客户端访问资源。免客户端运维，仅需浏览器即可直接运维 SSH、RDP、Telnet、VNC、SFTP 资源。同时以用户、用户组、账户、账户组为核心要素，来设置多对多的资源访问授权，用户组和账户组内的新增成员可自动继承授权关系。

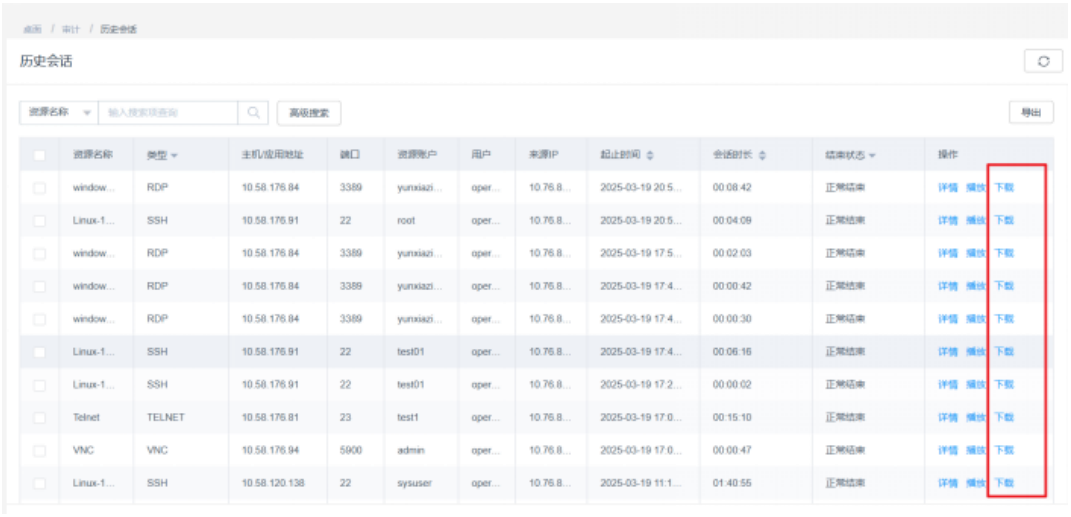
在资源管理方面可通过 Linux 应用发布（麒麟 V10）的方式实现对火狐浏览器、Chrome 浏览器、达梦数据库、人大金仓数据库等的扩展。

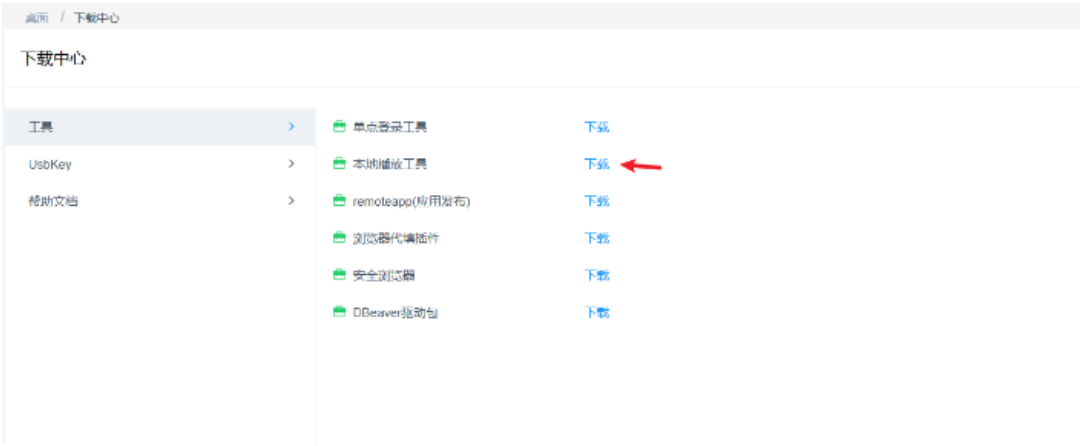


支持资源账户提权登录。当字符协议资源的特权账号禁止直接登录时，支持使用普通账户登录，并自动提权到特权账号，且支持切换自账号和提权命令。

2.6 全程审计

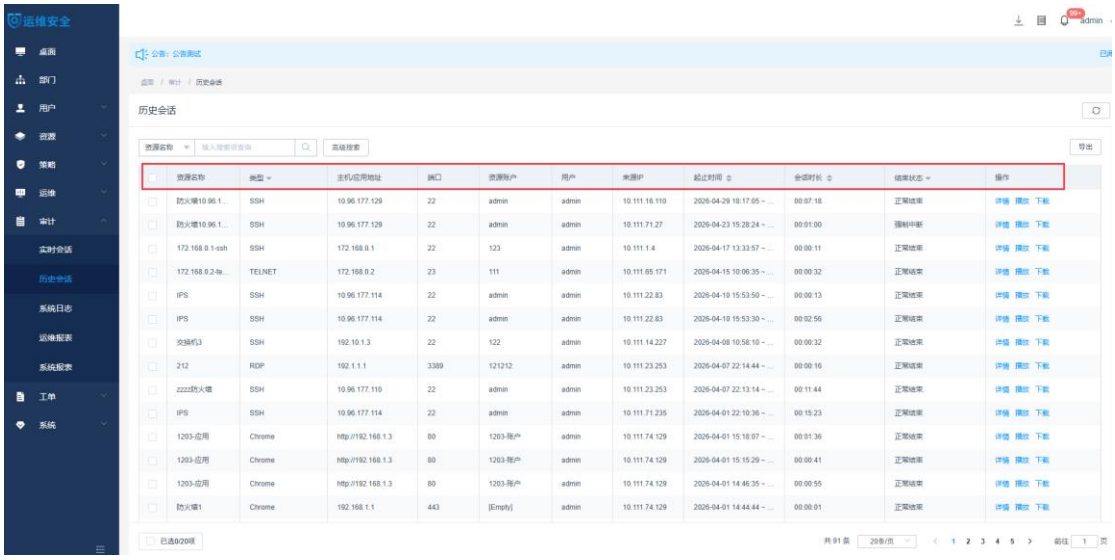
运维人员登录到堡垒机之后，所有的操作就都在堡垒机的管控之下，并且对所有的操作都进行了详细记录。针对会话的审计日志，还可以支持在线查看、在线播放和下载后离线播放。离线回放运维人员对资源的操作过程，回放文件可下载到本地，使用专用的播放器进行播放，专用播放器需要在堡垒机 web 界面可供下载.

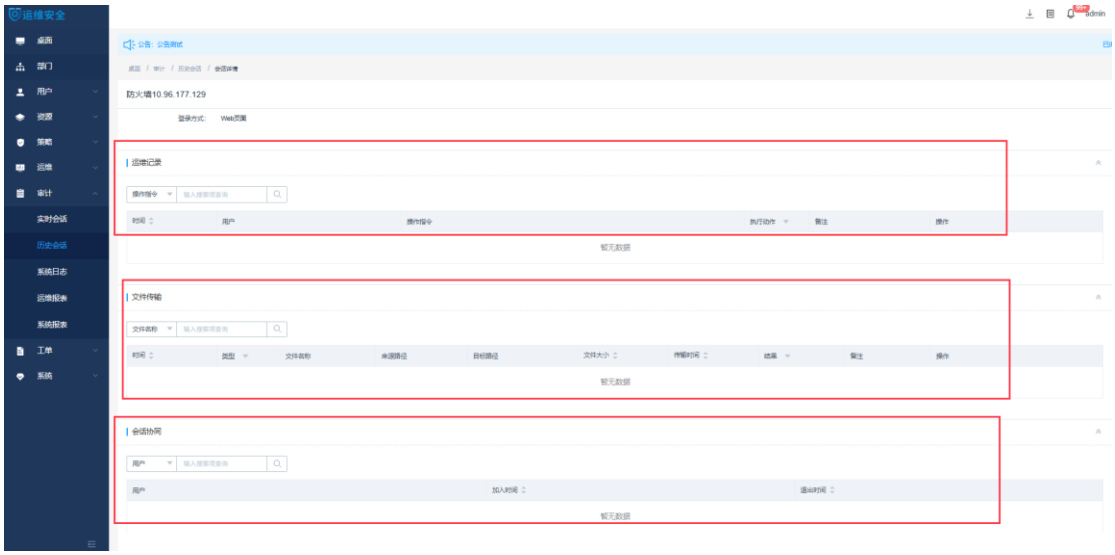




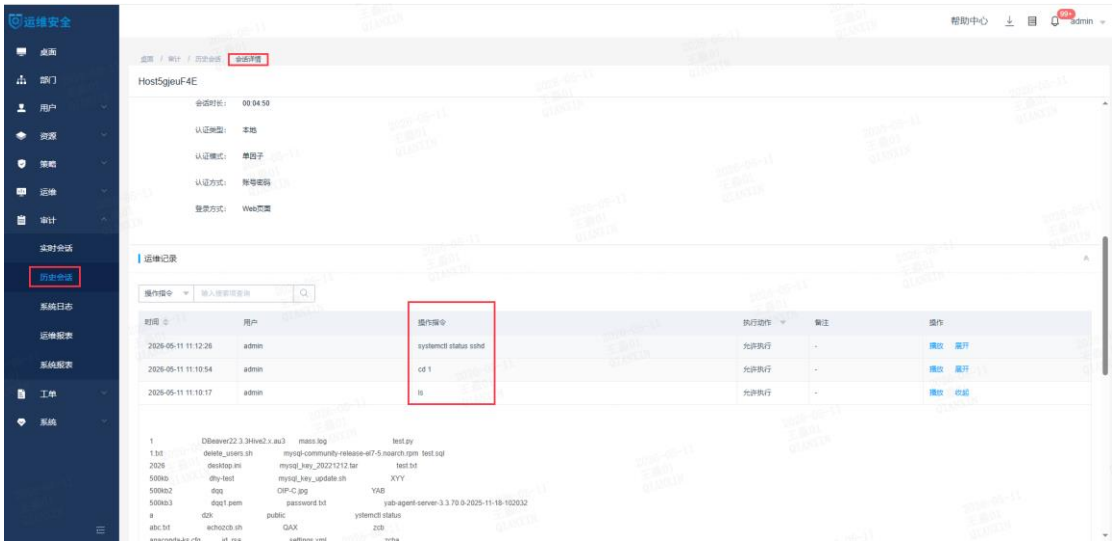
堡垒机目前支持字符协议（SSH、TELNET）、图形协议（RDP、VNC）、文件传输协议（FTP、FTP、SFTP）、数据库协议（DB2、MySQL、Oracle、SQL Server、达梦）和应用发布的操作审计。其中，字符协议和数据库协议能够进行操作指令解析，100%还原操作指令；图形协议和应用发布可以通过 OCR 进行文字识别；文件传输能够详细记录文件传输的操作、名称和目标路径。

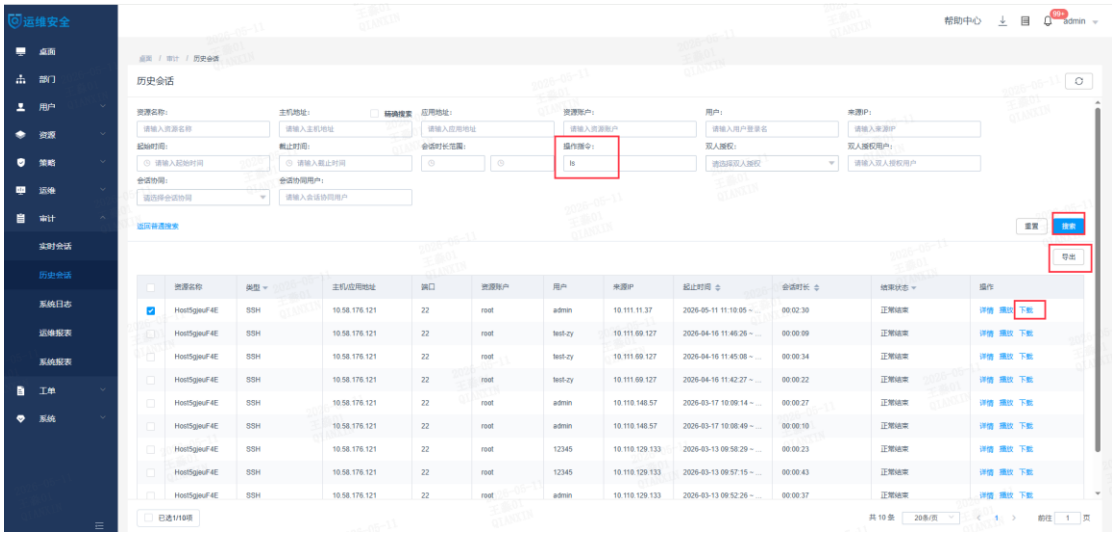
堡垒机支持记录用户登录资源的操作行为，包含：资源名称、协议类型、主机或应用地址、资源账户、起止时间、会话时长、操作用户、来源 IP、操作记录、文件传输记录、会话协同记录、以及会话结束状态的审计。





堡垒机支持对字符操作命令进行精准识别、查询和导出。





2.7 命令控制

堡垒机提供了集中的命令控制策略功能，不仅支持 SSH、TELNET 等字符协议，还支持 MySQL、Oracle、PostgreSQL 和达梦数据库的访问控制，实现基于不同的资源账户、不同的用户设置不同的命令控制策略。策略提供断开连接、拒绝执行、动态授权和允许执行等四种执行动作，如下表所示，根据命令的危险程度和资源的重要程度去设置命令的执行动作。同时，堡垒机预置了近千条 Linux/Unix、主流网络设备的操作命令，以及常用的数据库操作指令，让管理人员可以直接从命令库进行调取，简化命令控制策略的配置过程。

表 1 执行动作推荐

资源重要性 / 命令危险程度	核心资源	重要资源	普通资源
危险	断开连接	拒绝执行	动态授权
一般	动态授权	动态授权	允许执行

2.8 工单申请

运维人员向管理员申请需要访问的设备，以工单方式向管理员进行申请。当需要使用的功能权限（例如文件管理、RDP 剪切板等）由于策略的限制无法使用时，运维人员也可以通过工单申请相应的功能权限。管理员对工单进行审核和批准后，运维人员就拥有了临时的访问权限。

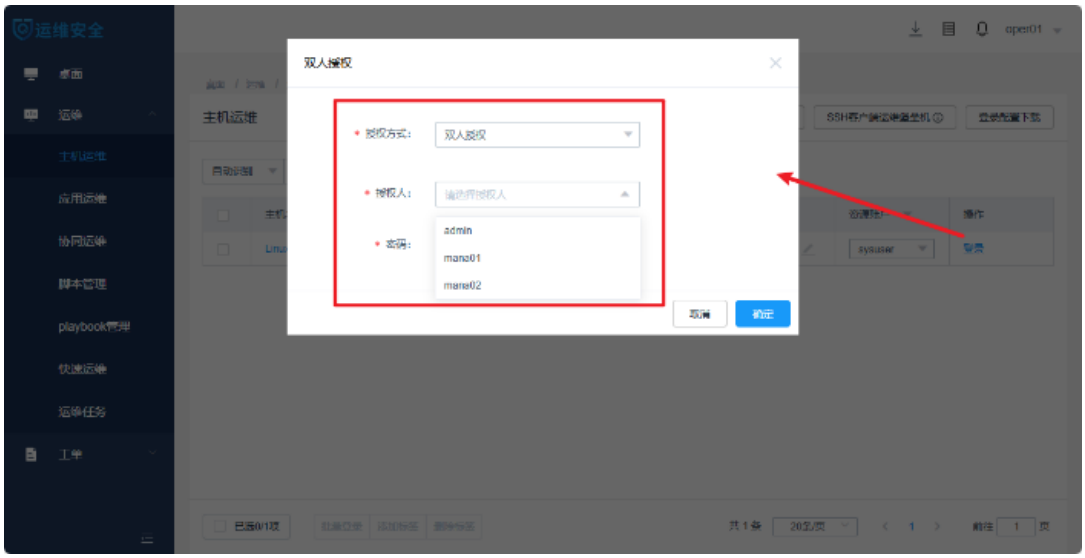
工单的审批流程可以由系统管理员进行自定义，并且可以设置多人审批或者是会签审批模式，规范资源运维操作流程。

2.9 会话协同

通过堡垒机，运维人员可以邀请其他用户加入自己的会话，进行协同操作。当新人操作不熟练时，通过会话协同监控功能，能够邀请其他的用户协助自己进行操作，操作控制权可在不同的用户之间能够进行灵活的切换。

2.10 双人授权

为降低高权限账号被滥用引起违规操作的风险，借鉴银行金库管理中开关库房必须由两名管库员在场共同进行的方式，以多人制衡的手段对高权限的使用进行监督和控制。堡垒机通过双人授权，让运维人员在访问核心资源时，必须要通过管理员的现场审批，通过双人授权有效遏制权限滥用的情况，降低安全事件发生的风险。在没有人员进行监控的情况下，运维员可以进入到运维界面，但是无法进行任何操作。



2.11 报表分析

堡垒机支持展示最近登录主机及应用，以便运维员快速跟进近期的运维工作。

并且预置了多种分析报表，如下图所示，通过报表能够全方位地分析系统操作、资源运维的情况，让管理员迅速了解系统的现状，快速分析系统操作和资源运维的情况，及时阻止安全事件的发生。报表支持自动发送，支持以天、周、月为粒度发送报表，并且以 HTML、PDF、WORD、EXCEL 等多种格式导出，让管理员随时掌握系统情况。

3 特点与优势

3.1 微信小程序多因子认证

堡垒机主账户是获取目标资源访问权限的唯一账户，为了提高来源身份的可靠性，防止身份冒用，堡垒机具有多种身份认证方式，包括但不限于本地静态密码认证、手机令牌、手机短信、动态令牌、国密 USBKey、等多因子认证方式，将主账户与实际用户身份一一对应，确保行为审计的一致性，从而准确定为事故责任人，弥补传统网络安全审计产品无法准确定位用户身份的缺陷。堡垒机可在不同 HA、集群、设备之间的认证方式配置同步。

手机令牌通过小程序实现，如图所示。无需安装 APP，通过微信就能使用，方便快捷。

3.2 一键同步和发现资源

堡垒机能够支持一键同步阿里云、百度云、华为云、腾讯云、AWS、Azure 和 UCloud 等云平台的主机资源。当企业有云上的资源时，只需管理员到对应的云平台获取相应的 Key，堡垒机就可以通过导入云主机功能，将企业的云上资源一键同步到堡垒机当中。并且无需任何定制开发，在零附加成本的基础之上，轻松将云上的资源同步到堡垒机当中。

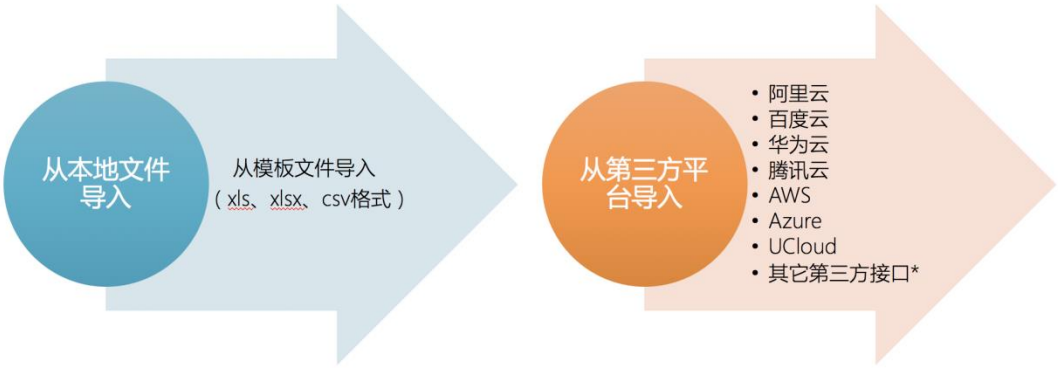


图 7 多种资源导入方式

除了同步云上的资源之外，堡垒机还支持通过自动发现的方式，自动获取企业网络中的资源，并且支持一键添加到堡垒机当中。

3.3 HTML5 运维

堡垒机提供 HTML5 运维访问方式，无需安装任何客户端，脱离运维工具和操

作系统束缚，用户在 Windows、Mac、Linux 等操作系统上只要通过一款主流的浏览器，就能实现对资源的访问和操作，让运维人员脱离运维工具和操作系统束缚，是真正意义上的云堡垒机。

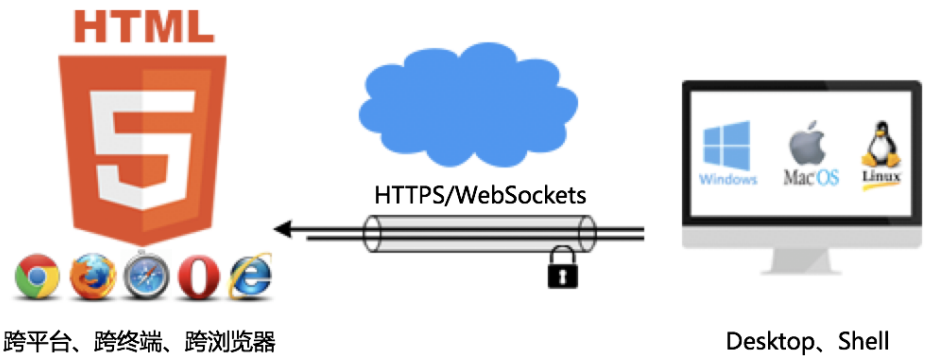
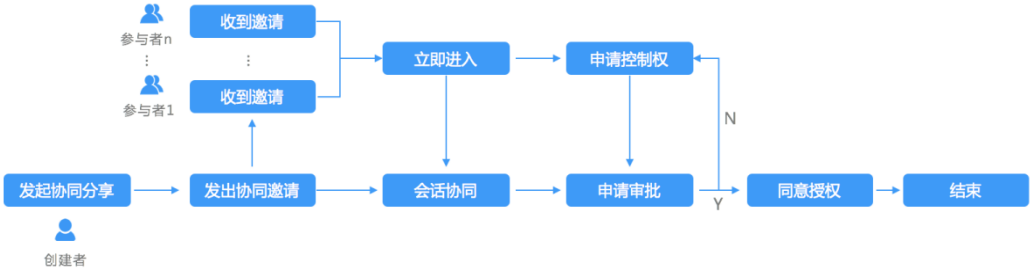


图 8 HTML5 运维

3.4 多人协同合作

堡垒机提供了一个协同合作、协同会诊、会话协同监控平台，用户只需将协同链接分享给其他协同者，协同者无需下载任何软件，只需要通过浏览器就能够面对同一个工作场景。并且，控制权能够在创建者和协同者之间自由切换，创建者能够随时中断协同者的违规操作，所有操作将被全程审计。



3.5 自动化运维

当资产数达到一定规模，运维往往需要向自动化方向发展，因此，很多企业都会引入各种各样的自动化运维工具。但是，使用运维工具往往又会带来其他的问题。首先，自动化运维工具的专业化程度较高，普通的运维人员想要熟练掌握需要花费大量的时间和精力，学习成本较高；其次，类似 ansible 的自动化运维

工具往往需要录入资源的账户和密码，而单位部署堡垒机就是不希望运维人员再接触到密码，这点和堡垒机的使用是相悖的；并且，密码的修改会影响自动化运维任务，遇到这种问题，很多单位的做法是不修改资源的密码。堡垒机支持提前预置频繁使用的命令，在运维时提高效率；支持群发命令，实现同时运维多台资源设备。

由此可见，为了自动化的引入，反而会增加单位的运维成本，并且还把密码暴露给运维人员，甚至之后单位的服务器都不会去修改密码，这无疑是本末倒置。但是，使用堡垒机的自动化运维，就不会产生这些问题，在提高运维效率的同时，也能够保障内部资源的运维安全。

堡垒机具备网络设备配置自动备份功能，如下图所示，管理员通过在堡垒机上配置相应策略，让堡垒机在指定的时间，自动备份指定的网络设备上的配置文件。

堡垒机具备执行 Linux 系统命令、执行脚本和批量分发文件的功能。如下图所示，运维人员通过在堡垒机编排任务，让任务在指定的时间自动到指定的 Linux 服务器上执行，并将执行的结果记录到堡垒机当中。

图 11 自动运维任务编排

堡垒机的自动化运维方案，可以帮助运维人员从重复的体力劳动中解放出来，提高运维效率。

3.6 多维度访问控制

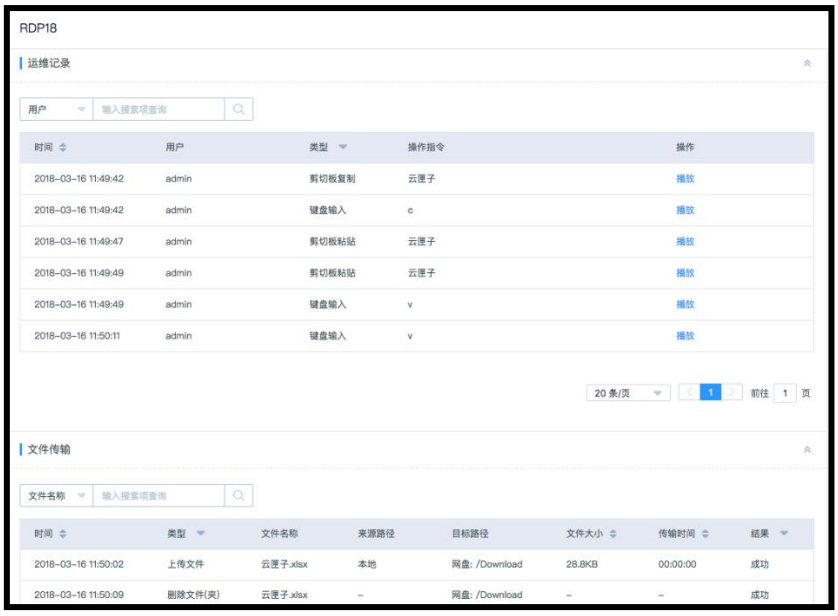
通过集中统一的访问控制策略和细粒度的命令控制策略，确保用户拥有的权限是完成任务所需的最小权限。堡垒机支持创建基于时间、IP、用户/用户组、账户/账户组、运维权限、操作命令、执行动作等元素作为组合条件，授权用户可访问的目标资源、定义危险操作管控策略。当用户越权执行特定命令的时候，实时进行阻断、告警，确保信息系统安全、稳定运行。

堡垒机通过 IPMI 协议（SNMP）或 restful 协议的方式，对运维操作审计系统硬件基础信息进行上报监控，要求包括但不限于 SNMP v2c 和 SNMP v3。

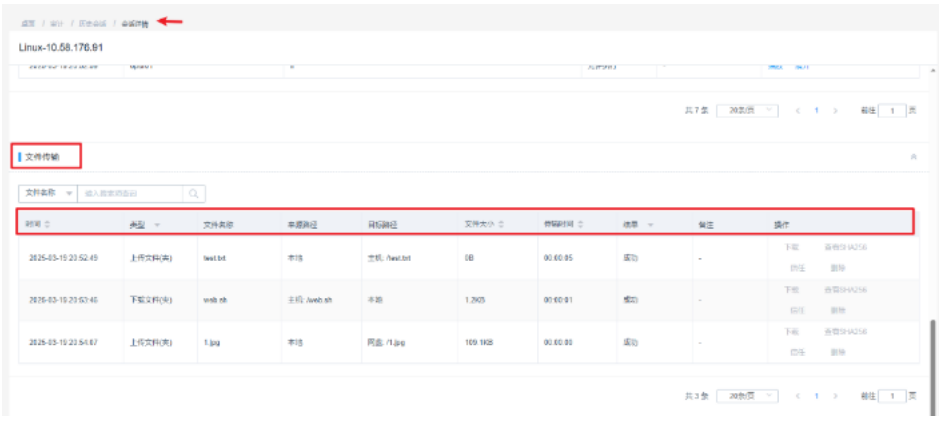
3.7 文件传输和剪切板审计

堡垒机不仅实现了对操作会话的实时监控、实时阻断、会话在线回放，和对会话的起止时间、来源用户、来源 IP、目标资源、协议/应用类型、运维操作等行为记录，还实现了对文件传输、剪切板操作的完整审计，为上传恶意文件、窃取数据等危险行为提供了查询依据，在进行大文件传输时，传输无需开通网络长连接。如下图所示：如文件传输通过网盘的方式，支持可调整网盘大小限制，支持管理员进行网盘清理，可以对单个用户网盘空间进行清理，也可以批量进行用户网盘清理。

堡垒机支持通过关键字搜索定位回放历史会话，并在线回放运维人员对资源的操作过程，并可以对播放速度进行调整，播放速度支持最快2X\4X\8X\16X 快进，支持拖动、暂停、停止、跳过空闲、重新播放、截屏、切换会话等操作，支持运维记录按照允许执行、动态授权、拒绝执行、断开连接等进行筛选，支持文件传输按照上传文件（夹）、下载文件（夹）、重命名文件（夹）、删除文件（夹）、创建文件夹进行筛选，支持审计协同用户。

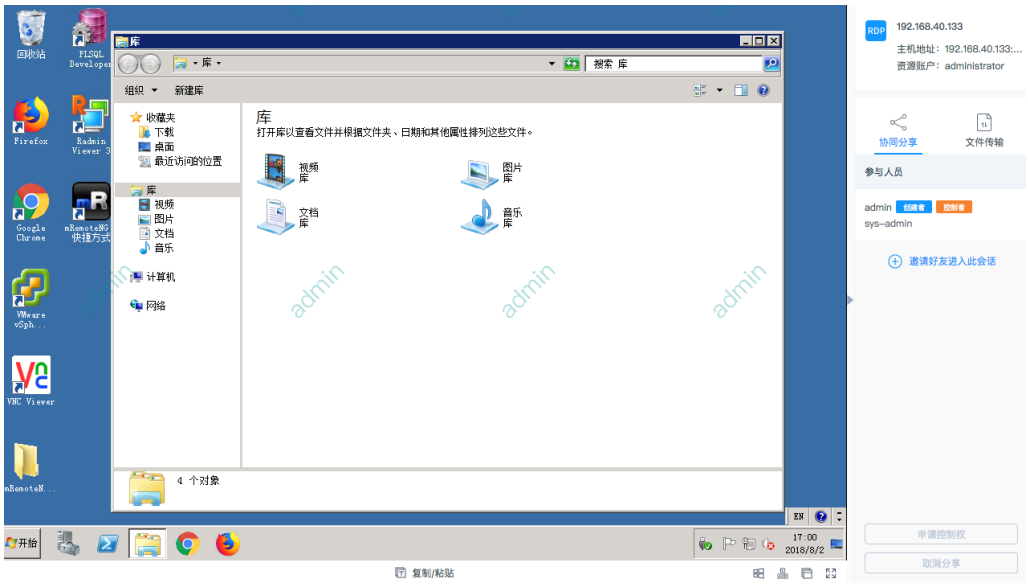


堡垒机文件传输审计针对 SSH、RDP、FTP、SFTP、SCP 协议资源，产品支持对用户通过堡垒机传输的原始文件进行审计留存，包括从本地上传、下载到主机的文件，以及从堡垒机网盘上传、下载到主机的文件，可灵活设置保存文件的大小（支持单文件或会话级别限制）；同时支持自动计算文件的 SHA256 值。



3.8 运维水印防泄密

如果重要资料外泄，将对企业造成不可估量的损失。而传统的运维模式下，用户采用拍照的方式造成的数据泄露，将很难定位和追随责任人。因此，运维水印添加功能就有了用武之地。试想，如果打开的运维操作页面能自动添加当前操作用户的登录名作为水印背景，一旦外泄，即可快速追溯相关人员，并迅速寻找到传播的源头，还有几个敢铤而走险？当用户想要传播时，心里必定有杆秤，好好掂量一下到底能不传播。



3.9 命令二次审批

堡垒机支持根据需求对特殊访问命令操作进行二次审批功能，该功能可以进一步加强对运维人员访问关键设备时运维操作的控制力度，确保所有访问操作都

在被管控的过程中进行。

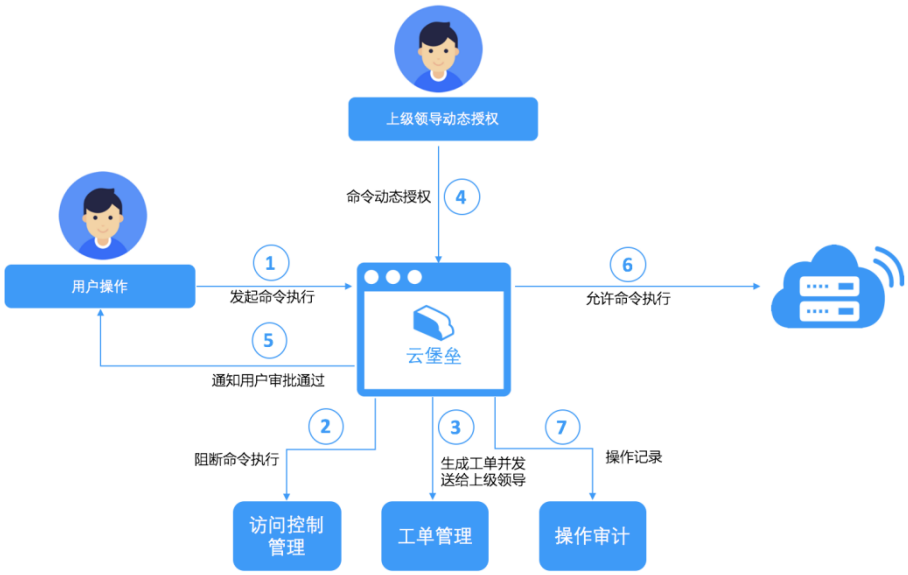


图 15 命令二次审批

3.10 IPv4/IPv6 双栈支持

随着互联网设备不断增多，IPv4 地址即将枯竭，全球可用的 IPv4 地址只有不到 43 亿个，远远无法满足互联网、物联网的快速发展。 IPv6 采用 128 位地址长度，可提供 3.4*1038 个 IP 地址，近似无限。

堡垒机支持 IPv4 和 IPv6 双栈网络，无论源地址（请求）或目的地址（发送）处于 IPv4 还是 IPv6 网络，双栈网络都能轻松驾驭，两种协议互不影响，运维 IPv6 地址的资源，包含 SSH、RDP、TELNET、FTP、SFTP 等协议类型。

3.11 改密结果分段发送

堡垒机支持对资源账户自动改密，同时改密结果支持通过邮件附件的方式发送到密码管理员的邮箱。针对改密附件，可以设置两个接收人，并且两个接收人分别收到资源账户的前半段和后半段密码，两段密码合并之后才能够得到完整的密码。

3.12 在线升级

在堡垒机可连接外网的情况下，堡垒机可自动检查并下载堡垒机的最新版本，用户在了解版本更新内容之后，可以自主选择是否升级到最新版本。通过在线升级，可以节省用户下载、上传升级包的时间，简化对堡垒机系统的管理和维护工作。

3.13 移动 App 运维管理

1. 远程审批运维工单

当运维人员需要访问敏感设备和执行高危命令时，需要发起访问授权工单和命令授权工单，经过管理员审批后方可执行操作，传统方式需要管理员在堡垒机 web 页面查看和审批授权，值守在电脑前，奇安信堡垒机支持在 App 上直接处理工单审批，极大提升了管理员审批权限的便捷性。

图 16 工单审批

2. 远程监控实时会话

堡垒机具备对会话进行实时监控和告警，对运维操作审计系统自身安全进行监控，包括异常进程监测、异常网络连接监测等，支持自动封停或终止此类异常行为并进行告警。

App 支持管理员监控并中断实时会话，当有敏感任务需要管理员实时监控时，监控操作可在手机上完成，并且支持历史会话记录的查看。

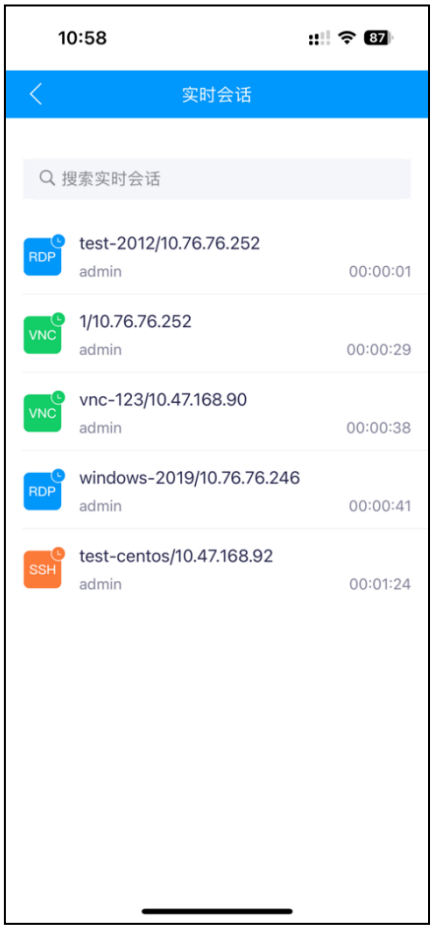
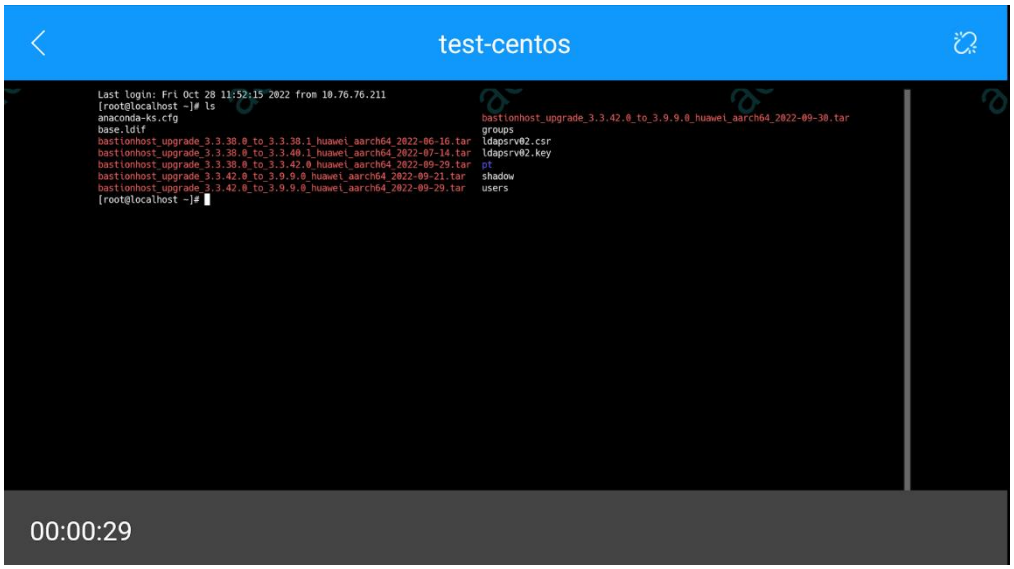

10:58
87
实时会话
搜索实时会话
RDP
test-2012/10.76.76.252
admin
00:00:01
VNC
1/10.76.76.252
admin
00:00:29
VNC
vnc-123/10.47.168.90
admin
00:00:38
RDP
windows-2019/10.76.76.246
admin
00:00:41
SSH
test-centos/10.47.168.92
admin
00:01:24

图 17 实时会话列表


test-centos
Last login: Fri Oct 28 11:52:15 2022 from 10.76.76.211
[root@localhost ~]# ls
anaconda-ks.cfg
base.ldif
bastionhost_upgrade_3.3.38.0_to_3.3.38.1_huawei_aarch64_2022-06-16.tar
bastionhost_upgrade_3.3.38.0_to_3.3.40.1_huawei_aarch64_2022-07-14.tar
bastionhost_upgrade_3.3.38.0_to_3.3.42.0_huawei_aarch64_2022-09-29.tar
bastionhost_upgrade_3.3.42.0_to_3.9.9.0_huawei_aarch64_2022-09-21.tar
bastionhost_upgrade_3.3.42.0_to_3.9.9.0_huawei_aarch64_2022-09-29.tar
bastionhost_upgrade_3.3.42.0_to_3.9.9.0_huawei_aarch64_2022-09-30.tar
groups
ldapsrv02.csr
ldapsrv02.key
pt
shadow
users
[root@localhost ~]#
00:00:29

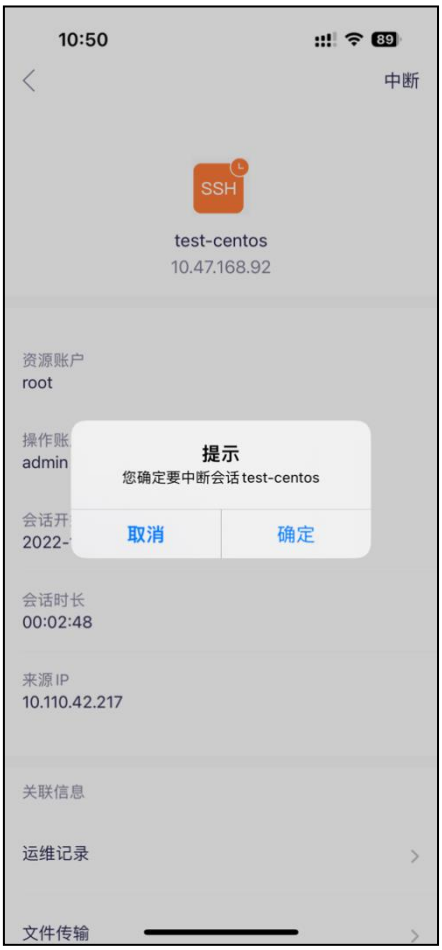


图 19 实时会话中断

3. 远程获取告警信息

在堡垒机 App 上可直接查看设备告警信息、系统消息、业务消息、任务消息等内容，方便管理员随时随地了解系统运行状态。

图 20 App 查看告警信息

4. 远程管理用户和资产

在堡垒机 App 上还可直接查看管理用户和资产信息。

图 21 查看管理用户和资产信息

iOS 手机可直接在 App Store 搜索“奇安信堡垒机”获取。

安卓手机可在堡垒机下载中心获取。

3.14 运维文件病毒扫描

堡垒机具备文件病毒扫描能力，可以扫描本地上传到网盘文件、主机上传到网盘文件的文件是否含有病毒，支持对带毒文件的隔离、信任、删除，并留下审计记录，防止运维场景下传播病毒文件到 IT 系统中，提升系统安全性。

4 产品价值

堡垒机为企业带来的价值主要体现在：

4.1 管理效益

- 所有主账号和从账户在一个平台上进行管理，账号管理更加简单有序；
- 通过建立用户与主账号的唯一对应关系，确保用户拥有的权限是完成任务所需的最小权限；
- 可视化运维行为监控，及时预警发现违规操作；
- 可对运维操作的故障进行追溯，支持通过文本方式和在线回放进行运维操作审计。

4.2 用户效益

- 运维人员只需记忆一个账号和密码，一次登录，便可实现对其所维护的多台资源的访问；
- 无需频发地输入 IP 地址和账户密码，提高工作效率，降低工作复杂度；
- 操作界面简单易用；
- 资源运维批量处理、批量操作。

4.3 企业效益

- 降低人为安全风险，避免安全损失；
- 满足合规要求，保障企业效益。

5 应用场景

堡垒机提供一套先进的运维安全管控与审计解决方案，目标是帮助企业转变传统安全运维被动响应的模式，建立面向用户的智能化运维安全管控模式，降低人为安全风险，满足合规要求，提高人员效率，助推企业核心业务发展。

5.1 数据中心运维管控与审计场景

场景 1：针对企业内部员工密码人传人横向泄露，设备很容易被没有权限的内部员工利用账户密码正常登录上之后出现安全风险。

方案：堡垒机将企业所有设备资源进行统一纳管，纳管后可对资源进行单点登录以及定期改密操作，从未实现环境中资源设备的密码定期修改，从未减少因密码被泄露导致的安全风险。

场景 2：员工离职后，账号权限回收不及时导致离职员工利用原有职务权限之便进行非法运维操作。

方案：堡垒机作为所有运维操作的唯一入口，所有运维操作均需要通过登录堡垒机后进行，所以针对所有运维行为，只要在员工离职后关闭赋予其堡垒机的账户权限，便可有效离职后非法运维现象。

场景 3：针对网络中资产数较多，对运维操作的审计均需从被运维的各个资产上逐一查看导出，缺少统一的运维审计方式，审计均需要从企业各个资产设备日志中逐一查看，效率低下。

方案：堡垒机提供对纳管 IT 资产的统一审计功能，通过堡垒机可快速查看对纳管资产的所有运维操作。通过实时会话审计功能，可对正在运维会话进行实时监控，发现违规操作可一键中断会话，还可对已运维结束的历史会话进行录像回放审计功能，通过视频回放精准还原每一步运维操作。

场景 4：针对运维过程中，难免出现拍照泄露、手机录像发生的数据泄露的安全风险，但针对此种现象发生的数据泄露，无法定位事故发生的责任人、

方案：堡垒机支持 H5 水印功能，针对当前的运维会话，会将运维者的用户名作为水印显示在运维屏幕上，一旦发生拍照泄露等现象，可根据水印用户名快速定位责任人。

5.2 云平台租户运维场景

云厂商需要在云平台上提供堡垒机服务给租户，帮助租户进行安全运维，满足等保合规要求。堡垒机与授权服务器和云管平台对接，当租户需要堡垒机时，云管平台自动按需分配堡垒机资源给租户，满足租户需求的同时降低云平台管理和维护成本。

5.3 信创改造场景

堡垒机具有国产化平台版本，可满足客户部署信创硬件堡垒机的需求。同时针对信创云环境，可在信创堡垒机软件基础上制作部署信创云镜像满足客户需求（信创云环境实施需要产品经理评估）。

5.4 电力运维调度场景

堡垒机成功入围电力行业 “调度自动化系统运维堡垒机” 名录，堡垒机与运维调度系统深度对接，实现工单申请、工单审批、工单派发、运维管控、运维审计追溯一体化，同时堡垒机与电网安管平台对接，实现运维日志可视化呈现，实时监测运维动态。

6 安装部署

6.1 产品部署外部环境约束条件

硬件型号列表——标准化型号

型号 指标		C6100-BH-TF8P	C6100-BH-TF8M	C6100-BH-TF10P	C6100-BH-TF10M	C6100-BH-TF20P	C6100-BH-TF20M
选型建议	最大授权许可	300	300	300	300	500	500
	最大图形并发	150	150	150	150	300	300
	最大字符并发	500	500	400	400	800	800
硬件配置	CPU	C3558	C3558	G4400	G4400	I3-6100	I3-6100
	内存	8G	8G	8G	8G	8G	8G
	硬盘	4T	4T	4T	4T	4T	4T
	RAID 方案	不支持	不支持	不支持	不支持	不支持	不支持
接口配置	LED 液晶屏	支持	支持	支持	支持	支持	支持
	其他接口	2USB+1Console	2USB+1Console	2USB+1Console	2USB+1Console	2USB+1Console	2USB+1Console
	板载网络接口	千兆电口*6 万兆光口*2	千兆电口*6 万兆光口*2	千兆电口*6	千兆电口*6	千兆电口*6	千兆电口*6
	接口扩展槽数	2	2	2	2	2	2
	接口板卡型号	C6100-BH-TF8-2X-QY C6100-BH-TF8-4GE-QY C6100-BH-TF8-4SFP-	C6100-BH-TF8-2X-QY C6100-BH-TF8-4GE-QY C6100-BH-TF8-4SFP-	C6100-BH-4GE-LY1U C6100-BH-4SFP-LY1U C6100-BH-4X-LY1U C6100-BH-2X-LY1U	C6100-BH-4GE-LY1U C6100-BH-4SFP-LY1U C6100-BH-4X-LY1U C6100-BH-2X-LY1U	C6100-BH-4GE-LY C6100-BH-4SFP-LY C6100-BH-8GE-LY C6100-BH-4X-LY C6100-BH-2X-LY	C6100-BH-4GE-LY C6100-BH-4SFP-LY C6100-BH-8GE-LY C6100-BH-4X-LY C6100-BH-2X-LY

		QY	QY				
其他	电源规格	单电源	冗余电源	单电源	冗余电源	单电源	冗余电源
	硬件 Bypass	不支持	不支持	不支持	不支持	不支持	不支持
	机箱规格	1U	1U	1U	1U	2U	2U
	尺寸(深*宽*高)	深 560mm*宽 440mm*高 45mm	深 560m*宽 440mm*高 45mm	深 580mm*宽 440mm*高 45mm	深 580mm*宽 440mm*高 45mm	深 560mm*宽 440mm*高 89mm	深 560mm*宽 440mm*高 89mm
	电源功率	150W	150W	250W	300W	250W	300w
	重量	约 15kg	约 15kg	约 15kg	约 15kg	约 18kg	约 18kg

型号 / 指标		C6100-BH-TF30M	C6100-BH-TF40M	C6100-BH-TF50M	C6100-BH-TF70M
选型建议	最大授权许可	1000	1000A（无限许可）	1000A（无限许可）	1000A（无限许可）
	最大图形并发	500	600	800	1200
	最大字符并发	1000	1500	3000	3000
硬件配置	CPU	E3-1225 v5(支持 ECC 功能)	E3-1225 v5(支持 ECC 功能)	E3-1225 v5(支持 ECC 功能)	Intel 4314（2 颗）
	内存	16G	16G	32G	64G
	硬盘	4T	6T	4T*3	8T*3
	RAID 方案	不支持	不支持	支持 RAID5	支持 RAID5
接口配置	LED 液晶屏	支持	支持	支持	不支持
	其他接口	2USB+1Console	2USB+1Console	2USB+1Console	4USB+2VGA+1BMC+1Console+1typeC
	板载网络接口	千兆电口*4、MGT*1、HA*1	千兆电口*4、MGT*1、HA*1	千兆电口*4、MGT*1、HA*1	千兆电口*4、万兆光口*6
	接口扩展槽数	2	3	3	3

	接口板卡型号	C6100-BH-4GE-QY C6100-BH-4SFP-QY C6100-BH-8GE-QY C6100-BH-4X-QY C6100-BH-2X-QY	C6100-BH-4GE-QY C6100-BH-4SFP-QY C6100-BH-8GE-QY C6100-BH-4X-QY C6100-BH-2X-QY	C6100-BH-4GE-QY C6100-BH-4SFP-QY C6100-BH-8GE-QY C6100-BH-4X-QY C6100-BH-2X-QY	不支持
其他	电源规格	冗余电源	冗余电源	冗余电源	冗余电源
	硬件 Bypass	不支持	不支持	不支持	不支持
	机箱规格	2U	2U	2U	2U
	尺寸(深*宽*高)	深 560mm*宽 440mm*高 89mm	深 560mm*宽 440mm*高 89mm	深 560mm*宽 440 mm*高 88mm	深 748mm*宽 447mm*高 87mm
	电源功率	300w	300w	300w	900W
	重量	约 18kg	约 18kg	约 18kg	约 25kg

硬件型号列表——国产化型号

型号 / 指标		BH3300-G-1000Z	BH3300-G-2000Z	BH3300-G-1000Z-GM
选型建议	最大授权许可	500	1000	500
	最大图形并发	50	100	50
	最大字符并发	200	500	200
硬件配置	CPU	兆芯 ZX-C4600(2.0GHz, 4 核)	兆芯 ZX-C4600(2.0GHz, 4 核)	兆芯 ZX-C4600(2.0GHz, 4 核)
	操作系统	中标麒麟 V7.0（桌面版）	中标麒麟 V7.0（桌面版）	中标麒麟 V7.0（服务器版）
	内存	16G	16G	16G
	硬盘	4T	4T	4T
	密码卡	不支持	不支持	内置密码卡
	RAID 方案	不支持	不支持	不支持
接口配置	LED 液晶屏	支持	支持	支持
	其他接口	2USB+1Console	2USB+1Console	2USB+1Console
	板载网络接口	千兆电口*6（含 MGT*1、HA*1）、千兆光	千兆电口*10（含 MGT*1、HA*1）、千兆光	千兆电口*6（含 MGT*1、HA*1）、千兆光

		口*4	口*4、万兆光口*2	口*4
	接口扩展槽	2	不支持	1
	扩展卡型号	BH3300-G-4SFP BH3300-G-8C BH3300-G-4X BH3300-G-2X BH3300-G-4C4F BH3300-G-4C	/	BH3300-G-4SFP BH3300-G-8C BH3300-G-4X BH3300-G-2X BH3300-G-4C4F BH3300-G-4C
其他	电源规格	冗余电源	冗余电源	冗余电源
	硬件 Bypass	不支持	不支持	不支持
	机箱规格	2U	2U	2U
	尺寸(深*宽*高)	深 560mm*宽 440mm*高 89mm	深 560mm*宽 440mm*高 89mm	深 560mm*宽 440mm*高 89mm
	电源功率	120W	120W	120W
	重量	约 15kg	约 15kg	约 15kg

型号 指标		BH3300-G-3000Z	BH3300-G-3000Z-GM	BH3300-G-5000Z	BH3300-G-5000Z-GM
选型建议	最大授权许可	1000	1000	1000A	1000A
	最大图形并发	400	400	800	800
	最大字符并发	2000	2000	3000	3000
硬件配置	CPU	海光 C86 3250	海光 C86 3250	海光 C86 3250	海光 C86 3250
	操作系统	银河麒麟 V10	银河麒麟 V10	银河麒麟 V10	银河麒麟 V10
	内存	16G	16G	32G	32G
	硬盘	6T	6T	12T	12T
	密码卡	不支持	内置密码卡	不支持	内置密码卡
	RAID 方案	不支持	不支持	不支持	不支持
接口配置	LED 液晶屏	支持	支持	支持	支持
	其他接口	2USB+1Console	2USB+1Console	2USB+1Console	2USB+1Console
	板载网络接口	千兆电口*6（含 MGT*1、HA*1）、千	千兆电口*6（含 MGT*1、HA*1）、千兆光口*4	千兆电口*6（含 MGT*1、HA*1）、千兆光口*4、万兆光口*2	千兆电口*6（含 MGT*1、HA*1）、千兆光口*4、万兆光口*2

		兆光口*4			
	接口扩展槽	2	1	1	/
	扩展卡型号	BH3300-G-2X-QY BH3300-G-4GE-QY BH3300-G-4SFP-QY	BH3300-G-2X-QY BH3300-G-4GE-QY BH3300-G-4SFP-QY	BH3300-G-2X-QY BH3300-G-4GE-QY BH3300-G-4SFP-QY	/
其他	电源规格	冗余电源	冗余电源	冗余电源	冗余电源
	硬件 Bypass	不支持	不支持	不支持	不支持
	机箱规格	2U	2U	2U	2U
	尺寸(深*宽*高)	深 560mm*宽 440mm*高 89mm	深 560mm*宽 440mm*高 89mm	深 560mm*宽 440mm*高 89mm	深 560mm*宽 440mm*高 89mm
	电源功率	350W	350W	350W	350W
	重量	约 18kg	约 18kg	约 18kg	约 18kg

硬件型号列表——涉密分保型号

型号 / 指标		C3200-BH-TF20M	BH3300-G-1000Z-SM
选型建议	最大授权许可	500	500
	最大图形并发	300	50
	最大字符并发	800	500
硬件配置	CPU	I3-6100	兆芯 ZX-C4600(2.0GHz，4 核)
	内存	8G	16G
	硬盘	4T	4T
	RAID 方案	不支持	不支持
接口配置	LED 液晶屏	支持	支持
	其他接口	2USB+1Console	2USB+1Console
	板载网络接口	千兆电口*6	千兆电口*6（含 MGT*1、

			HA*1）、千兆光口*4
	接口扩展槽数	2	2
	接口板卡型号	C6100-BH-4GE-LY C6100-BH-4SFP-LY C6100-BH-8GE-LY C6100-BH-4X-LY C6100-BH-2X-LY	BH3300-G-4SFP BH3300-G-8C BH3300-G-4X BH3300-G-2X BH3300-G-4C4F BH3300-G-4C
其他	电源规格	冗余电源	冗余电源
	硬件 Bypass	不支持	不支持
	机箱规格	2U	2U
	尺寸(深*宽*高)	深 560mm*宽 440mm*高 89mm	深 560mm*宽 440mm*高 89mm
	电源功率	300w	120W
	重量	约 18kg	约 15kg

硬件型号列表——央采型号

型号 指标		Y6150-C011	Y6150-C021	Y6150-C031
硬件配置	CPU	G4400	E3-1225 v5(支持 ECC 功能)	E3-1225 v5(支持 ECC 功能)
	内存	8G	16G	32G
	硬盘	4T	4T	4T*3
	RAID 方案	不支持	不支持	支持 RAID5
其他	电源规格	冗余电源	冗余电源	冗余电源
	硬件 Bypass	不支持	不支持	不支持
	机箱规格	1U	2U	2U
	尺寸(深*宽*高)	深 580mm*宽 440mm*高 45mm	深 560mm*宽 440mm*高 89mm	深 560mm*宽 440 mm*高 88mm
	电源功率	300W	300w	300w
	重量	约 15kg	约 18kg	约 18kg

6.2 部署方式

6.2.1 旁路部署

堡垒机无需改造现有网络结构，物理上以旁路的方式部署在运维终端与被管

理设备之间的交换机上，逻辑上以串行的方式部署在运维终端与被管理设备之间。用户在访问被管理设备时，要先登录到堡垒机，通过堡垒机以协议代理或应用发布的方式访问被管理设备。堡垒机根据登录用户的角色和权限，在堡垒机界面上显示用户可以访问的被管理设备列表，再通过单点登录功能登录到用户要访问的设备，用户的操作行为受到堡垒机的访问控制和审计。

6.2.2 HA 双机部署

堡垒机对外提供一个虚拟的 IP，当主机出现故障之后，备机自动接管服务，保证业务连续性，同时主备之前数据自动同步，切换主备之后，不影响用户使用。

堡垒机典型的 HA 双机部署应用场景如下图所示。

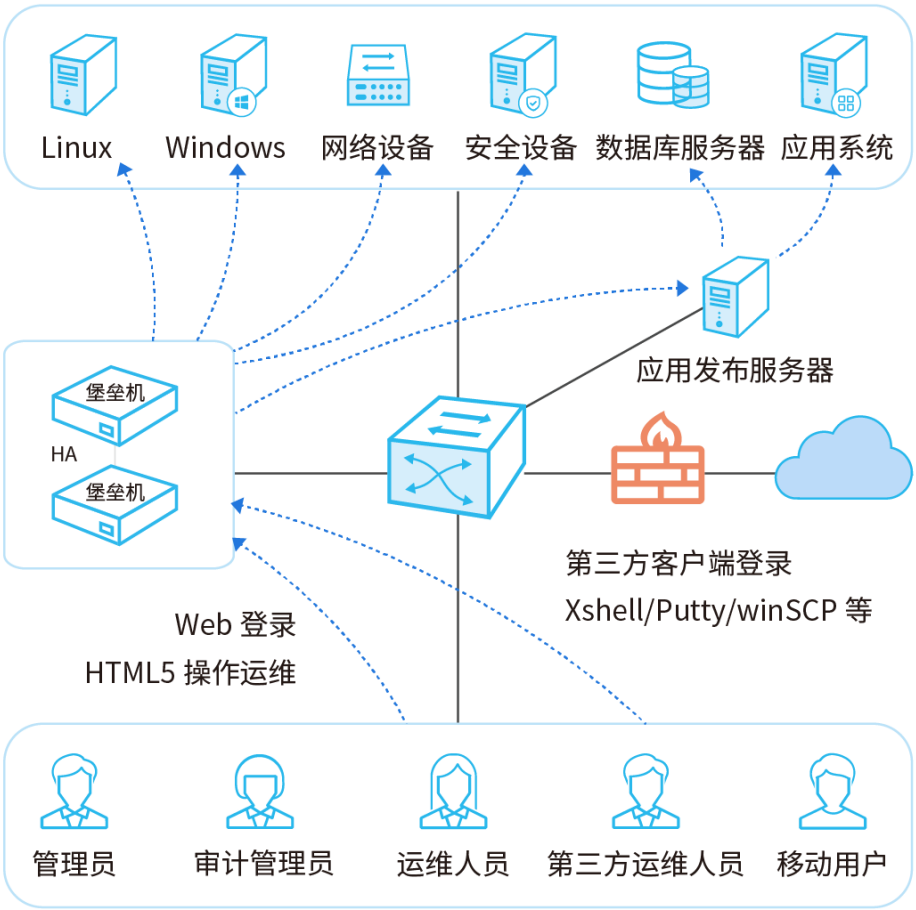


图 17 HA 双机部署

6.2.3 多租户部署

在云计算的场景下，堡垒机能够与云平台紧密联动，实现云租户购买、使用、续费、退订等全生命周期的自动化管理，无需人工介入。租户购买堡垒机之后能够一键启动，自动下发授权并激活。同时，能够提高云平台的管理及资源利用效率，云平台只需在云上存储一个堡垒机系统镜像，以及部署一台 LCC 授权服务器，即可进行多种规格的产品发布，授权按需下发、退订自动回收。

多租户场景的 License 授权流程如下图所示。

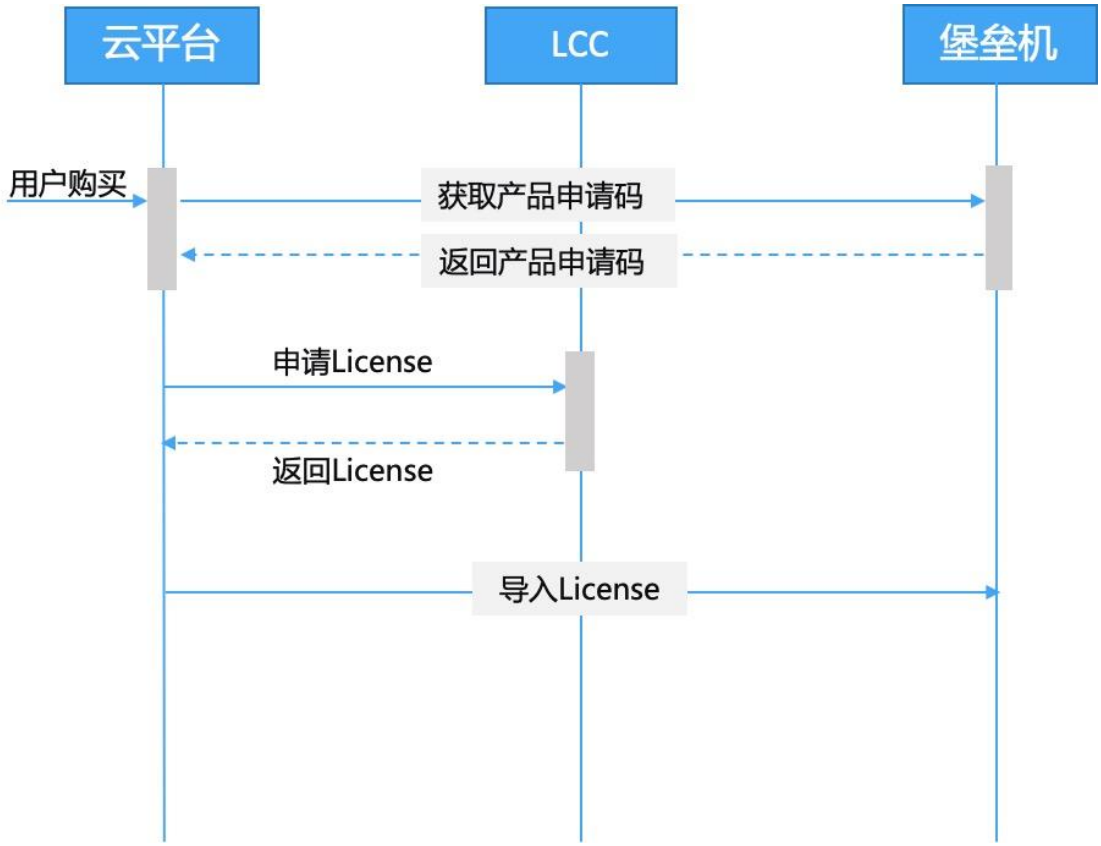
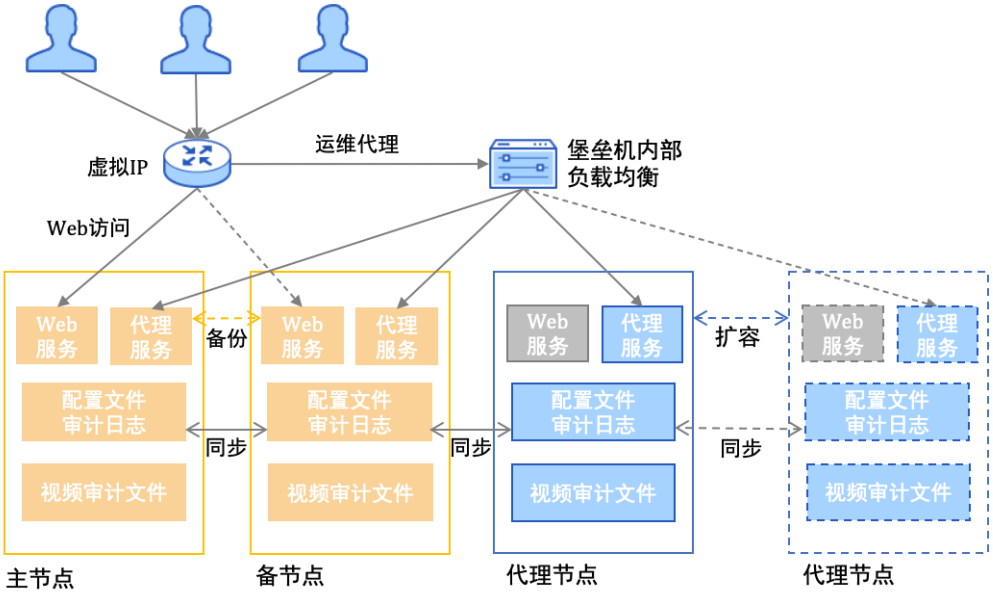


图 2 多租户 License 授权流程

6.2.4 集群部署

大型互联网/IT 公司、泛政府、银行、金融、电力、能源、卫生、环境等行业头部客户，具有资产规模大、可用性要求高、多数据中心的场景属性，传统单机或 HA 部署模式可能出现设备性能瓶颈，需要集群方案满足大规模资产运维管理需求。

堡垒机支持添加多台堡垒机作为协议代理服务器，分担主堡垒机性能压力，扩展运维能力，客户可以根据业务需求变化对集群节点进行弹性扩展，灵活满足客户不断增长的业务需求 。多协议代理服务器节点可访问相同资源时实现自动负载均衡，以便合理利用 CPU 和内存资源、提高集群的整体性能 。主堡垒机集中管理配置和日志信息。



堡垒机以任何部署模式下，自动切换时间小于 1min；任何部署模式均支持配置和审计日志的自动同步。