**云堡垒帮助文档**

# 产品介绍

## 1.1产品定义

启明星辰云堡垒机是一款针对云主机、云数据库、网络设备等的运维权限、运维行为进行管理和审计的工具。主要解决云上IT运维过程中操作系统账号复用、数据泄露、运维权限混乱、运维过程不透明等难题。

云堡垒机对整个运维过程从事前预防、事中控制和事后审计进行全程参与。

事前预防：建立“自然人-资源-资源账号”关系，实现统一认证和授权。

事中控制：建立“自然人-操作-资源”关系，实现操作审计和控制。

事后审计：建立“自然人-资源-审计日志”关系，实现事后溯源和责任界定 。

## 1.3产品功能

（1）账号管理

账号管理包括云堡垒运维账号和运维资产账号。运维账号实名制、运维账号生命周期管理、运维资产账号集中管理和资产账号改密功能。

* 堡垒机账号的实名制：云堡垒为每个运维人员创建唯一的运维账号（主账号），所有资产账号（从账号）均与主账号进行关联，确保所有运维行为审计记录的一致性，有效解决账号共用问题便于定位问题责任人。
* 运维账号生命周期管理：账号的启用、禁用和有效时间，直接由管理员掌控。
* 运维资产账号的集中管理：账号密码掌握在管理员手中，避免了密码泄露风险。
* 资产账号改密：云堡垒支持人工或定期自动修改运维资产账号的密码。

（2）统一认证

登录认证是整个运维过程的首要环节也是最重要的环境，云堡垒提供双因素认证，大大保证了统一入口的登录安全。

云堡垒支持单点登录，运维人员认证登录后访问资产无需再次输入资产账号密码即可登录。

（3）集中授权

云堡垒通过集中统一的访问控制和细粒度的命令级授权策略，确保每个运维用户拥有的权限是完成任务所需的最合理权限。

* 访问策略（保证自然人和资产的授权最小化）；
* 命令策略（黑白名单）；
* 基于时间段和IP段进行限制；
* 协议功能分别控制（例如RDP剪贴板和磁盘映射功能等）。

（4）资源管理

资源管理包括：用户资产管理、服务管理、从账号管理、从账号密码管理。

* 资产管理：资产管理包括资产基础信息录入、资产导入导出、资产移动等功能；
* 服务管理：添加资产服务名、服务类型、端口、编码等信息；
* 从账号管理：按照服务添加账号及密码认证信息，和其他和服务相关的信息。
* 从账号密码管理：对常见资源进行从账号密码定期修改，可配置密码策略，定期对资产密码进行维护。

（5）行为审计

行为审计包括：实时操作过程监控、二次审批、告警与阻断、审计记录和回放、审计报表。

* 实时操作过程监控：对于所有远程访问目标主机的会话连接，均可实现操作过程同步监视，运维人员在远程主机上做的任何操作都会同步显示在审计人员的监控画面中，管理员可以随时手工中断违规操作会话。
* 二次审批：支持对特殊指令执行进行审批。运维人员操作过程中触发命令策略，需要得到管理员的审批后才能继续执行后续操作。
* 告警与阻断：支持根据已设定的访问控制策略，自动检测日常运维过程中发生的越权访问、违规操作等安全事件，系统能够根据安全事件的类型、等级等条件进行自动的告警或阻断处理。
* 审计与回放：审计过程的完整记录，根据操作记录定位回放或完整重现维护人员对远程主机的整个操作过程，从而真正实现对操作内容的完全审计。
* 审计报表：内置能够满足不同客户审计需求的安全审计报表模板，支持自动或手工方式生成运维审计报告，便于管理员全面分析运维的合规性。
* 审计存储：支持自动或手动配置备份和日志备份，管理员可以对备份数据导出保存。

（6）审计报表

审计报表功能，内置能够满足不用客户审计需求的安全审计报表模板，支持自动或手工方式生成运维审计报告，便于管理员全面分析运维的合规性。

* 系统内置多种运行维护报表模板。
* 支持以html、CSV方式生成并导出报表。
* 支持管理员自定义审计报表。
* 支持以日报、周报、月报的方式自动生成周期性报表

## 1.4产品优势

【运维协议全面】

云堡垒机支持多种运维访问协议，能够充分满足日常运维需要。

* 字符协议：SSHv1、SSHv2、TELNET。
* 图形协议：RDP、VNC。
* 文件传输协议：FTP、SFTP。
* 数据库访问：Oracle、SQL Server、DB2、Sybase、Informix、Teradata、MySQL、PostgreSQL。

【审计效果精细】

支持字符协议和文件传输协议的协议审计，审计详细的操作语句和操作语句的执行结果。

支持RDP、VNC图形操作过程中键盘输入操作记录、鼠标点击行为记录和窗口标题审计。

数据库协议深度解析、数据库返回行数记录。

【管控方式严格】

云堡垒机系统提供严格的管控方式以保证运维过程的规范性。

* 命令限制与复核：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。
* 运维账号IP、MAC限制：通过绑定运维账号IP、MAC地址，避免用户在不安全的工作岗位进行重要的运维操作。

【操作使用便捷】

云堡垒机系统提供多种功能以保证运维过程的自动和快捷性。

* 多种运维方式：浏览器调用运维工具访问、浏览器内嵌WEB控件访问、客户端（SSH、TELNET、RDP、VNC）直连菜单模式方式
* C/S运维客户端：安全性高、通用性强、效率更高，避免了安装和调试Active和JAVA控件的繁琐工作。
* 资源批量登录：支持TELNET、SSH协议使用SecureCRT工具批量登录目标资源，避免进行多次连接的重复工作量。
* 命令批量执行：在资源批量登录的基础上，通过SecureCRT实现命令的多资源批量执行功能，减少同类型设备上重复的操作工作。

# 购买指南

## 2.1购买流程



在云市场上通过”启明星辰云堡垒机镜像”商品进入，购买对应的资源**（在创建云主机时必须购买数据盘，才能保证云堡垒机首次启动时正常完成初始化）**，选择云堡垒机镜像生成云堡垒机系统，即可登录云堡垒机进行试用。



在云市场上通过”启明星辰云堡垒机许可”商品进入，购买对应档次许可授权。

云堡垒机许可购买成功后，请登录云堡垒机“系统管理 > 授权信息”界面下载授权申请文件，将授权申请文件提交给云堡垒机服务团队，会在1周内为你的云堡垒机系统提供正式许可授权文件。





登录云堡垒机“系统管理 > 授权信息”界面，导入正式许可授权文件后，即可进行正式的使用。

### 2.1.1登录云市场

登录腾讯云官网购买云商品，URL地址：[https://cloud.tencent.com](https://cloud.tencent.com/)。提前注册腾讯云账号或绑定QQ、微信，用于登录云市场购买商品。



在腾讯云市场，搜索“启明星辰云堡垒机”，结果显示包括：启明星辰云堡垒机镜像和启明星辰云堡垒机许可。  


### 2.1.2购买云堡垒机

在云市场选择进入“启明星辰云堡垒机镜像产品”界面，选择“立即购买”。



#### 2.1.2.1选择地域与机型

**地域与机型：**选择购买的云主机的地域与机型，重点关注：计费模式和实例机型。

计费模式：承载堡垒机系统的云主机的计费方式。实例：选择合适的CPU、内存等配置。



#### 2.1.2.2选择镜像

**镜像：**选择生成堡垒机系统的镜像，在镜像市场搜索“启明星辰云堡垒机镜像”。





#### 2.1.2.3选择存储和带宽

**存储：**堡垒机存储包括系统盘和数据盘。

系统盘大小默认50G；数据盘用于存储堡垒机的配置和审计数据，数据盘大小可参考推荐配置，空间尽可能大。

注意：在创建云主机时必须购买数据盘，才能保证云堡垒机首次启动时正常完成初始化。

**带宽：**根据实际需求选择合适的带宽和计费模式。选择分配免费公网IP访问。



#### 2.1.2.4设置安全组和主机

**安全组：**新建安全组放行堡垒机必须的端口或放通全部端口，需要使用的端口参考堡垒机帮助手册

**实例名称：**云主机的名称，用于区分不同的云主机。

**登录方式：**推荐自动生成密码。





#### 2.1.2.5确认配置并开通

确认配置，开通云堡垒机。开始计算云主机的硬件配置和网络带宽费用。



#### 2.1.2.6云堡垒机实例状态

在个人账户的“云服务器 > 实例”中可查看到购买的云堡垒机的相关信息。

实例状态：为运行中，即代表云堡垒机已经创建完成并运行正常。

实例IP地址：可通过公网地址访问堡垒机。



### 2.1.3云堡垒机登录

堡垒机登录：通过浏览器登录堡垒机，URL地址：https://堡垒机公网IP:8443

系统管理员账号：sysadmin，默认密码：password$123

默认试用授权情况：用户数2个，资产数5个，试用期1个月。



### 2.1.4购买云堡垒机许可

在云市场选择进入“启明星辰云堡垒机许可”界面，选择所需的规格和周期，选择“立即购买”进行费用支付。

用户购买“启明星辰云堡垒机许可”完成后，使用堡垒机系统管理员登录，在“系统管理 > 系统信息 > 授权信息”界面下载授权申请文件。将授权申请文件提交给安赛客服申请正式授权许可。



## 2.2配置推荐

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **云主机配置推荐** | | | | **授权控制** | |
| CPU、内存和带宽配置 | 系统盘  大小 | 数据盘  大小 | 并发会话数 | 最大资产数 | 最大用户数 |
| 1核CPU-2G内存-1M带宽 | 50G | 100G | 20 | 20 | 10 |
| 1核CPU-4G内存-2M带宽 | 50G | 200G | 50 | 50 | 25 |
| 2核CPU-4G内存-4M带宽 | 50G | 400G | 100 | 100 | 50 |
| 2核CPU-8G内存-6M带宽 | 50G | 800G | 200 | 200 | 100 |
| 4核CPU-8G内存-10M带宽 | 50G | 1000G | 400 | 400 | 200 |
| 4核CPU-16G内存-10M带宽 | 50G | 2000G | 1000 | 1000 | 500 |
| 注： 1、云堡垒机由系统盘和数据盘组成，系统盘运行堡垒机操作系统，数据盘用于存储堡垒机的配置和审计数据。 2、云堡垒机系统盘10G及以上即可，所有档次的都一样，由云平台统一分配。 3、资产数：指纳入云堡垒机管理的资产数量，以资产的IP地址个数进行计算。例如一个云主机有两个IP，算两个资产数。 4、并发数：指SSH、远程桌面的TCP连接会话数。 | | | | | |

# 操作指南

## 3.1开放端口

云堡垒机需要对用户开放的端口说明：

|  |  |  |
| --- | --- | --- |
| **端口号**  **TCP** | **协议** | **描述** |
| 8443 | HTTPS | 向外提供 Web 访问（支持更改默认端口） |
| 18080 | 运维通道协议 | WEB或专用运维客户端运维模式下必须开放, （支持更改默认端口） |
| 5106 | RDP | 客户端直连堡垒机菜单模式运维方式，支持访问RDP,VNC协议资源（支持更改默认端口） |
| 5107 | SSH | 客户端直连堡垒机菜单模式运维方式，支持访问TELNET,SSH协议资源（支持更改默认端口） |
| 5110 | 实时监控 | 用于管理员在管理界面使用实时监控功能（支持更改默认端口） |

## 3.2登录方式

通过浏览器中输入URL地址打开（https://启明星辰云堡垒机的管理IP:8443）。使用系统管理员sysadmin，默认密码password$123登录管理界面。

云堡垒机开通完成后，请您按照云堡垒机管理员手册中的账号、密码信息登录，修改密码为强密码（密码长度不低于8位，密码包含大小写、数字、特殊字符）。

## 3.3NAT访问规则

在云堡垒机环境下，用户用于登录、管理堡垒机的IP地址并非堡垒机实际IP，而是通过NAT映射后的公网地址。

在通过堡垒机运维操作之前，需要在堡垒机系统管理中设置“NAT访问规则”。

以下为一实例，配置信息仅供参考。表格中的映射关系需要先借助现场环境的网络设备来实现，然后在参考截图说明在堡垒机上做相应配置（应用发布服务器可以映射成和堡垒机一样的IP地址，也可映射成不一样的IP地址）：

|  |  |  |
| --- | --- | --- |
| 设备类型 | 实际IP和端口 | 映射后IP和端口 |
| 堡垒机（协议代理通道） | 172.16.68.250:18080 | 151.101.1.147:18080 |

1. 管理员登录在【系统管理】-【系统选项】-【NAT访问规则】中，“添加”规则，访问地址设置为映射后的堡垒机的管理IP地址，优先级任意设置（在有多条访问规则时，优先级才体现作用）；

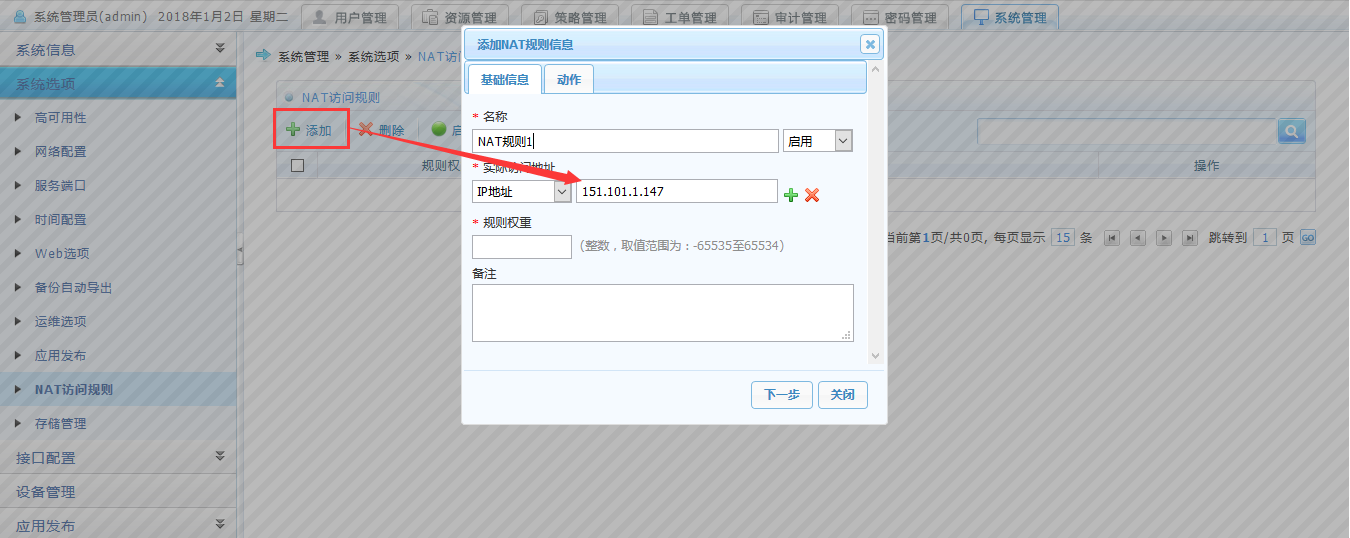


图1 添加NAT规则

1. 在NAT规则信息的“动作”中，建立映射关系，主要是堡垒机协议代理通道端口8080和应用发布服务器的远程桌面端口，选择设备“[SERVER]-172.16.68.250:8080（协议代理服务器）”，设置映射地址为：151.101.1.147，映射端口：18080；

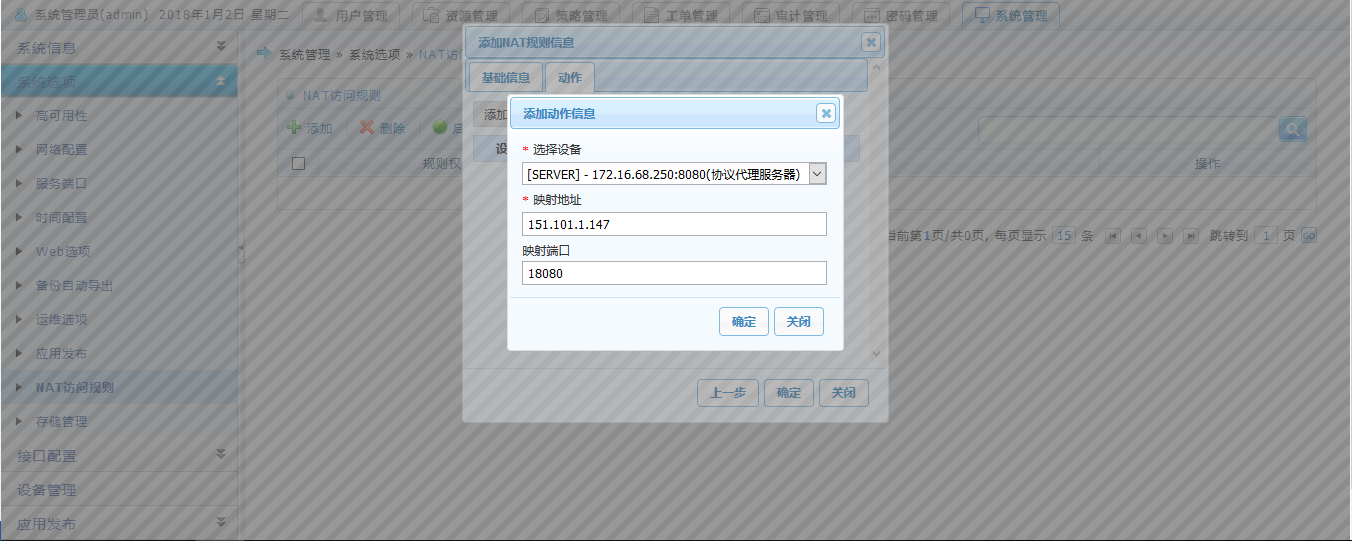


图2 添加NAT动作信息

设置完成后，即可通过映射地址https:// 151.101.1.147:10443访问堡垒机进行运维操作。

## 3.4授权申请

购买了“启明星辰云堡垒机许可”，请及时联系客服申请正式授权许可文件，同时提交授权申请文件。通过以下方法获取授权申请文件和导入正式授权许可文件。

1. 下载授权申请文件

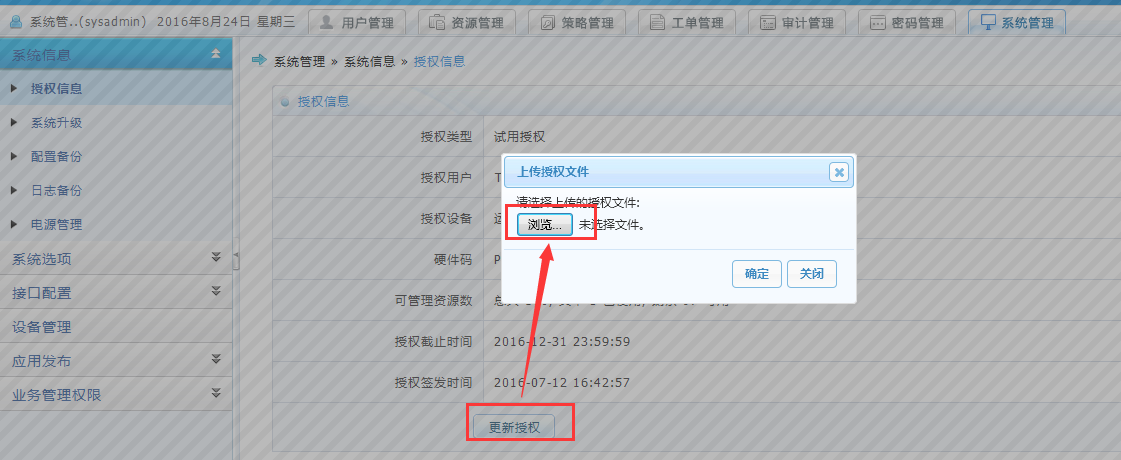
通过浏览器中输入URL地址打开（https://启明星辰云堡垒机的管理IP）。使用系统管理员sysadmin密码password$123登录。

在云堡垒机“系统管理 > 系统信息 > 授权信息”界面，下载授权申请文件。



1. 导入授权许可文件

在“系统管理”选项的“授权信息”中，“更新授权”选项用于导入已经申请到的正式授权许可文件。



# 常见问题

云堡垒机系统支持通过 SSH、SFTP、及 Windows 远程桌面等协议的方式代理接入授权的服务器，并实现全程录像。同时，支持使用标准客户端（如 Xshell、SecureCRT、PuTTY 等工具）对授权的服务器直接进行运维连接。

**问题1：**云堡垒所有节点都支持吗？

**回答：**云堡垒使用只需与您所要管理的服务器网络可达即可，所有接入堡垒机的云服务器，需要正常开机并保持运行中状态，云堡垒机需要与接入的云服务器属于一个相同的网络环境，且可以网络可达。不同资源池的服务器，如果网络不可达，需要分别部署云堡垒机。

**问题2：**云堡垒的操作系统是什么，能否更换为其他操作系统？

**回答：**云堡垒的操作系统是基于centos 6.9的专用系统，无法更改为其他操作系统。

**问题3：**用户是否可以登录云堡垒的操作系统？

回答：不可以，为了保障审计日志数据的合规性，要避免人为破坏，所以不开放登录堡垒机的操作系统的权利。

**问题4：**使用云堡垒机之后，服务器登录还可不通过堡垒机直接登录，是怎么回事？

**回答：**云堡垒机无防绕过的功能，服务器的登录限制有两种方式：

（1）网络上做访问控制，只允许用户访问堡垒机，堡垒机可访问服务器，禁止用户能直接访问服务器。

（2）在服务器端做访问限制，例如：linux 服务器通过设置 /etc/hosts.allow 和 /etc/hosts.deny这个两个文件，将所有的ip都禁止登录，只放行云堡垒的ip来达到只通过堡垒机才能登录的目的。