

# 堡垒机 (CBH)

## 产品文档



腾讯云TCE

# 文档目录

## 产品简介

- 产品简介

## 快速入门

- 管理员首次登录

- 管理员操作入门

- 运维员首次登录

- 运维员操作入门

## 操作指南

- 管理员操作指南

  - 开通服务

  - 资产管理

    - 同步主机

    - 添加主机

    - 编辑主机

    - 添加主机账号

  - 用户管理

    - 新建用户

    - 编辑用户

    - 重置用户

  - 用户组管理

    - 新建用户组

    - 编辑用户组

    - 将用户添加到用户组

  - 权限管理

    - 新建访问权限

    - 编辑访问权限

    - 新建高危命令模板

    - 编辑高危命令模板

  - 审计管理

    - 审计字符会话

    - 审计图形会话

    - 审计文件传输会话

    - 审计数据库会话

  - 系统设置

    - 访问白名单

登录安全设置

本地认证设置

双因子认证设置

自动同步资产设置

运维员操作指南

下载 BHLoader

访问主机

Web 页面调用客户端

H5 运维

SSH 或 SFTP 直连

访问串

访问数据库

访问串

最佳实践

高危命令阻断

安全事故追溯

常见问题

常见问题

# 产品简介

## 产品简介

最近更新时间: 2024-12-19 17:12:00

云堡垒机 ( Bastion Host , CBH ) 是集用户 ( Account ) 管理、授权 ( Authorization ) 管理、认证 ( Authentication ) 管理及综合审计 ( Audit ) 于一体的集中运维管理系统，提供 IT 资产访问代理以及智能操作审计服务，为用户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，实现异常行为告警，防止内部数据泄密，助力企业顺利通过等保测评。

云堡垒机主要特点：

- 为企业提供集中的管理平台，减少系统维护工作。
- 为企业提供全面的用户和资源管理，降低企业维护成本。
- 帮助企业制定严格的资源访问策略，并且采用强身份认证手段，全面保障系统资源安全。
- 详细记录用户对资源的访问及操作，达到对用户行为审计的需要。

## 产品功能

云堡垒机能够审计多种主流运维协议，对服务器、操作系统运维工作进行详尽记录，确保企业安全问题得到有效追溯。

## 认证管理

云堡垒机支持基本的静态口令方式，同时，为了提高安全性，云堡垒机支持用户使用双因子认证方式，实现用户认证的统一管理。

## 授权管理

云堡垒机能够集中管控用户访问资产的权限，不仅能够实现对资产的访问权限的控制，还能够实现对操作命令、剪切板、文件传输的细粒度控制。基于最小权限原则进行授权，确保用户拥有的权限是其访问资产、完成工作任务所需要的最小权限。

## 资产访问



云堡垒机支持托管 IT 资产的账号密码，运维人员可单点登录到目标资产进行运维操作，无需记忆全部资产的账号密码，仅需记住自己云堡垒机账号和密码即可。

## 操作审计

云堡垒机能够对用户所有的操作日志进行记录和分析，不仅可以对用户行为进行监控，还可以通过集中的审计数据进行数据挖掘，以便于事后进行安全事故责任的追溯和认定。

# 快速入门

## 管理员首次登录

最近更新时间: 2024-12-19 17:12:00

- 步骤1：进入云堡垒机服务之后，单击侧边栏的开通服务，可查看所有的云堡垒机服务。
- 步骤2：在开通服务页面中，单击对应云堡垒机右侧的开通服务，开启“开通云堡垒机服务”弹窗。
- 步骤3：在开通云堡垒机服务弹窗中，选择地域、VPC 和子网后，单击确定，即可完成云堡垒机服务的开通。

开通堡垒机服务

资源ID \*

资产授权数 100

地域 \*

— 华东地区 —

杭州一区

请选择需要堡垒机纳管的资产的所属地域

VPC \*

请选择

请选择需要堡垒机纳管的资产的所属VPC

子网 \*

请选择

选择任意子网均可，但完成初始化操作后，该子网不能被销毁。  
建议：选择资产数量较多的子网。

确定

取消

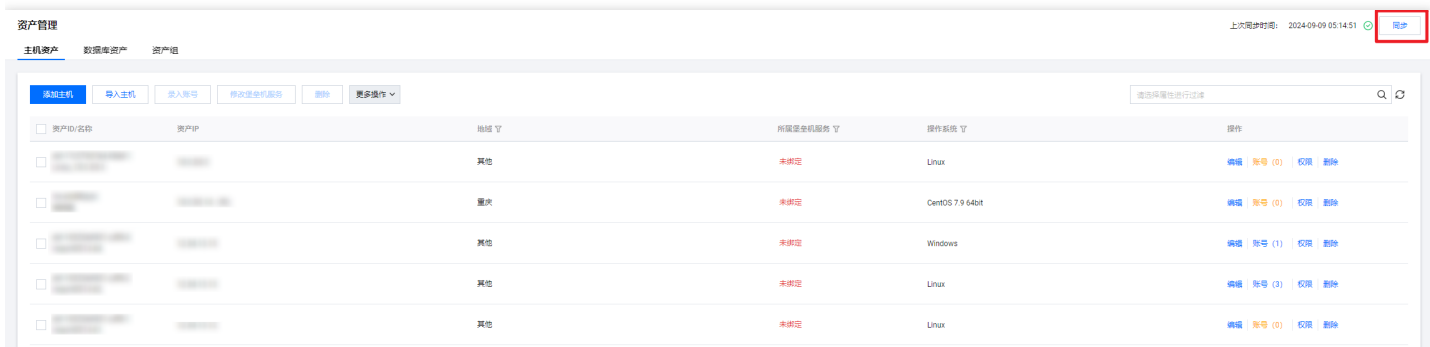
# 管理员操作入门

最近更新时间: 2024-12-19 17:12:00

## 添加纳管资产

步骤1：进入云堡垒机控制台之后，在左侧导航选择资产管理 > 主机资产，进入主机资产页面。

步骤2：在主机资产页面，单击同步。



步骤3：在弹出的对话框，单击确定。

步骤4：同步完成之后，在主机资产页面，选中主机之后，单击修改堡垒机服务给主机绑定云堡垒机服务。



步骤5：在修改云堡垒机服务窗口，选择要绑定的云堡垒机服务，单击确定完成绑定。

步骤6：在主机列表处选择一台主机，单击账号，弹出账号管理窗口。

资产管理

上次操作时间: 2024-09-09 05:14:51

操作

主机资产

数据库资产

资产组

添加主机

导入主机

导入账号

修改堡垒机服务

删除

更多操作

请按照属性进行过滤

Q

清除

资产ID/名称	资产IP	地域	所属堡垒机服务	操作系统	操作
<input checked="" type="checkbox"/>		其他	未绑定	Linux	编辑 账号 (0) 权限 删除
<input type="checkbox"/>		重庆	未绑定	CentOS 7 9 64bit	编辑 账号 (0) 权限 删除
<input type="checkbox"/>		其他	未绑定	Windows	编辑 账号 (1) 权限 删除
<input type="checkbox"/>		其他	未绑定	Linux	编辑 账号 (3) 权限 删除

步骤7：在账号管理窗口，单击添加资产账号，输入资产账户名称，单击确定完成添加资产账号。

步骤8：在账号管理窗口，单击未托管密码处的设置，输入密码后，单击确定完成添加托管密码。

## 添加运维用户

步骤1：进入云堡垒机控制台之后，在左侧导航选择用户管理 > 用户，进入用户页面。

步骤2：在用户页面，单击新建用户。

步骤3：在弹出的对话框，录入用户名、姓名、手机号等必填项，选择性录入邮箱、用户组、有效时间等非必填项，单击确认，完成运维用户添加操作。

新建用户

×

基本信息

高级选项

用户名 \*

请输入用户名

姓名 \*

请输入姓名

认证方式 \*

本地

手机号 \*

+86

请输入手机号

邮箱 \*

请输入邮箱

用户组

请选择用户组

确定

取消

## 授权运维用户访问资产权限

步骤1：进入云堡垒机控制台之后，在左侧导航选择权限管理 > 访问权限配置，进入访问权限页面。

步骤2：在访问权限页面，单击新建访问权限。

步骤3：跳转到新建访问权限页面后，按照流程指引进行操作。

1 设置基本信息

2 选择用户

3 选择资产

4 选择账号

5 设置访问控制

6 完成

权限名称 \*

有效期

台

下一步: 选择用户

步骤4：完成上述操作后，确认配置信息，单击确认提交，使授权配置生效。

## 告知运维用户运维页面登录地址

步骤1：进入云堡垒机控制台之后，在左侧导航选择概览，进入概览页面。

步骤2：在概览页面，复制右侧的帮助 > 运维页面链接，告知给已经授权的运维用户。



## 审计用户操作行为

步骤1：进入云堡垒机控制台之后，在左侧导航选择审计管理 > 运维审计。

步骤2：在运维审计页面，审计运维用户对纳管资产的操作行为。

# 运维员首次登录

最近更新时间: 2024-12-19 17:12:00

步骤1：运维页面登录地址不对外公开，由云堡垒机管理员负责告知运维人员。

步骤2：运维人员在浏览器中输入运维页面登录地址，打开主机运维页面。

步骤3：在主机运维页面，单击账号激活，跳转到账号激活页面。

步骤4：运维人员可以通过管理员授权的手机号码（登录账号），完成激活账号（登录密码初始化）操作。

步骤5：完成账号激活操作，单击登录，返回主机运维页面。

步骤6：在主机运维页面，输入账号（手机号码）、密码，单击登录按钮。

步骤7：如系统开通了 OTP 验证设置，登录过程会自动跳转到 OTP 验证页面。

步骤8：完成 OTP 小程序激活操作之后，将自动登录云堡垒机运维。

步骤9：首次登录云堡垒机运维页面，系统会引导您下载并安装运维辅助小工具（BHLoader）。

步骤10：您可以根据常用的运维客户端的操作系统类型，选择合适的运维辅助工具。

# 运维员操作入门

最近更新时间: 2024-12-19 17:12:00

步骤1：登录 运维页面（联系管理员获取），在主机列表页面，可查看已授权的主机信息。

步骤2：在主机列表页面，单击操作列的访问。

步骤3：在弹出的对话框，可选择访问方式（运维客户端）对主机进行访问，确定访问方式后，单击访问。

## 访问主机

访问方式

Mac Terminal

主机账号

root

主机密码

.....

访问

取消

步骤4：浏览器会弹窗提示，单击弹窗当中的打开 BHLoader。

步骤5：如果客户端安装路径不是默认路径，BHLoader 会提示用户选择对应的客户端，此时选择正确的客户端即可。

# 操作指南

## 管理员操作指南

### 开通服务

最近更新时间: 2024-12-19 17:12:00

步骤1：进入云堡垒机控制台之后，在云堡垒机系统左侧导航栏中，单击开通服务，进入开通服务页面。

步骤2：在开通服务页面，单击对应服务操作栏的开通，弹出开通堡垒机服务弹窗。

步骤3：在开通堡垒机服务弹窗，需配置地域、VPC 和子网。

开通堡垒机服务

资源ID \*

资产授权数 100

地域 \*

— 华东地区 —

杭州一区

请选择需要堡垒机纳管的资产的所属地域

VPC \*

请选择

请选择需要堡垒机纳管的资产的所属VPC

子网 \*

请选择

选择任意子网均可，但完成初始化操作后，该子网不能被销毁。  
建议：选择资产数量较多的子网。

确定

取消

参数名称	参数说明
地域	开通云堡垒机服务的地域。
VPC	开通云堡垒机服务的 VPC。
子网	开通云堡垒机服务的子网。



参数名称	参数说明
其他	页面标*的为必填项。

# 资产管理

## 同步主机

最近更新时间: 2024-12-19 17:12:00

步骤1：进入云堡垒机控制台之后，在左侧导航选择资产管理 > 主机资产，进入主机资产页面。

步骤2：在主机资产列表，单击同步，弹出同步主机窗口。



步骤3：单击确定，即可将主机同步到云堡垒机。

步骤4：主机同步完成之后，选择未绑定云堡垒机服务的主机，单击修改堡垒机服务。



步骤5：在修改堡垒机服务窗口中，选择要绑定的云堡垒机服务，单击确定即可完成绑定。

# 添加主机

最近更新时间: 2024-12-19 17:12:00

## 添加单台主机

步骤1：进入云堡垒机控制台之后，在左侧导航选择资产管理 > 主机资产，进入主机资产页面。

步骤2：在主机资产页面，单击添加主机，弹出添加主机窗口。



步骤3：在添加主机窗口中，需配置主机信息。

添加主机

资产IP \*

请输入资产IP

操作系统类型 \*

请选择操作系统类型

管理端口 \*

请输入管理端口

资产名称

请输入资产名称，不填将自动生成

确定

取消

步骤4：主机添加完成之后，选择未绑定云堡垒机服务的主机，单击修改堡垒机服务。



步骤5：在修改堡垒机服务窗口中，选择要绑定的云堡垒机服务，单击确定即可完成绑定。

## 批量添加主机

步骤1：进入云堡垒机控制台之后，在左侧导航选择资产管理 > 主机资产，进入主机资产页面。

步骤2：在主机页面，单击导入主机，弹出导入主机窗口。



步骤3：在导入主机窗口中，单击点击下载把模板下载到本地。



步骤4：在本地终端中，根据模板把需要导入的主机信息填写完整。

步骤5：在导入主机窗口中，单击点击上传把主机模板信息上传到云堡垒机，并单击下一步。

步骤6：对主机信息进行确认，如果有不符合要求的主机，请修改主机信息使其符合要求；确认主机信息都正确后，单击完成，即可导入主机。

导入主机

全部 (2)

符合要求 (2)

不符合要求 (0)

切换GBK编码

资产IP	操作系统类型	管理端口	资产名称
10.	Linux		Linux_10.
10.	Windows		Windows_10.

共 2 项

20 条 / 页

1

/ 1 页

上一步

完成

取消

步骤7：主机添加完成之后，选择未绑定云堡垒机服务的主机，单击修改堡垒机服务。

资产管理

主机资产

数据库资产

资产组

添加主机

导入主机

导入账号

修改堡垒机服务

删除

更多操作

资产ID/名称

资产IP

地址 IP

所属堡垒机服务 IP

操作系统 IP

操作

<input checked="" type="checkbox"/>			未绑定	Linux	编辑   账号 (0)   权限   删除
<input type="checkbox"/>		重庆	未绑定	CentOS 7 9 64bit	编辑   账号 (0)   权限   删除
<input type="checkbox"/>		其他	未绑定	Windows	编辑   账号 (1)   权限   删除

步骤8：在修改堡垒机服务窗口中，选择要绑定的云堡垒机服务，单击确定即可完成绑定。

# 编辑主机

最近更新时间: 2024-12-19 17:12:00

步骤1：进入云堡垒机控制台之后，在左侧导航选择资产管理 > 主机资产，进入主机资产页面。

步骤2：在主机资产页面，单击编辑，弹出编辑主机窗口。



步骤3：在编辑主机窗口，修改相应信息。

步骤4：修改完所需内容，单击确定，即可保存主机信息。

# 添加主机账号

最近更新时间: 2024-12-19 17:12:00

步骤1：进入云堡垒机控制台之后，在左侧导航选择资产管理 > 主机资产，进入主机资产页面。

步骤2：在主机资产页面，单击账号，弹出账号管理窗口。



步骤3：在账号管理窗口，单击添加资产账号，弹出添加主机账号窗口。



步骤4：在添加资产账号窗口，配置账号名后，单击确定，即可保存。



步骤5：单击对应账号的设置，弹出设置密码窗口。



步骤6：在设置密码窗口，填写密码信息。

步骤7：单击确定，即可保存密码信息。



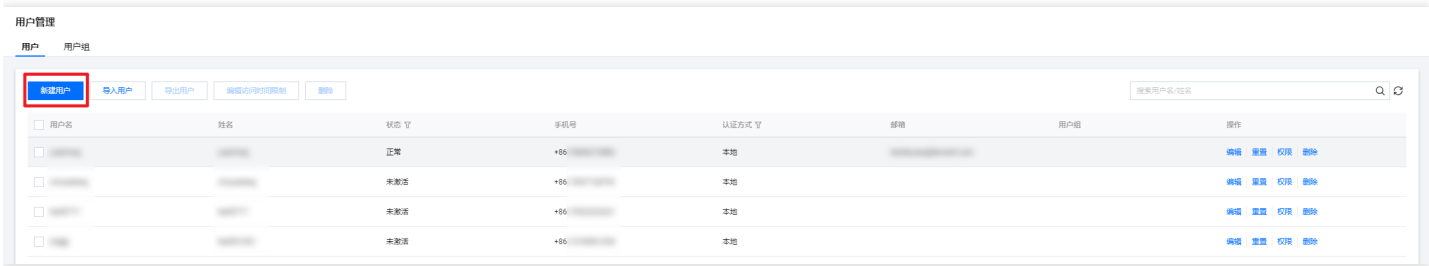
# 用户管理

## 新建用户

最近更新时间: 2024-12-19 17:12:00

步骤1：进入云堡垒机控制台之后，在左侧导航选择用户管理 > 用户，进入用户页面。

步骤2：在用户页面，单击新建用户，弹出新建用户弹窗。



步骤3：在新建用户弹窗，需配置用户信息。

新建用户

基本信息

高级选项

用户名 \*

请输入用户名

姓名 \*

请输入姓名

认证方式 \*

本地

手机号 \*

+86

请输入手机号

邮箱 \*

请输入邮箱

用户组

请选择用户组

确定

取消

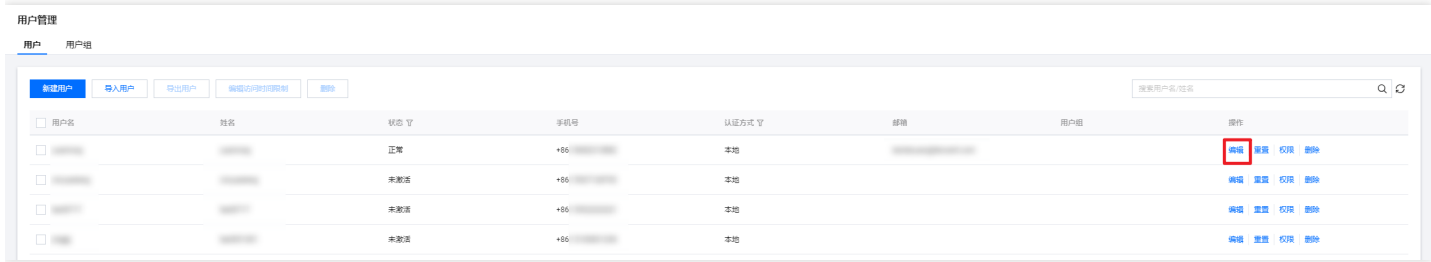
步骤4：用户信息配置完成之后，单击确定，即可创建用户。

# 编辑用户

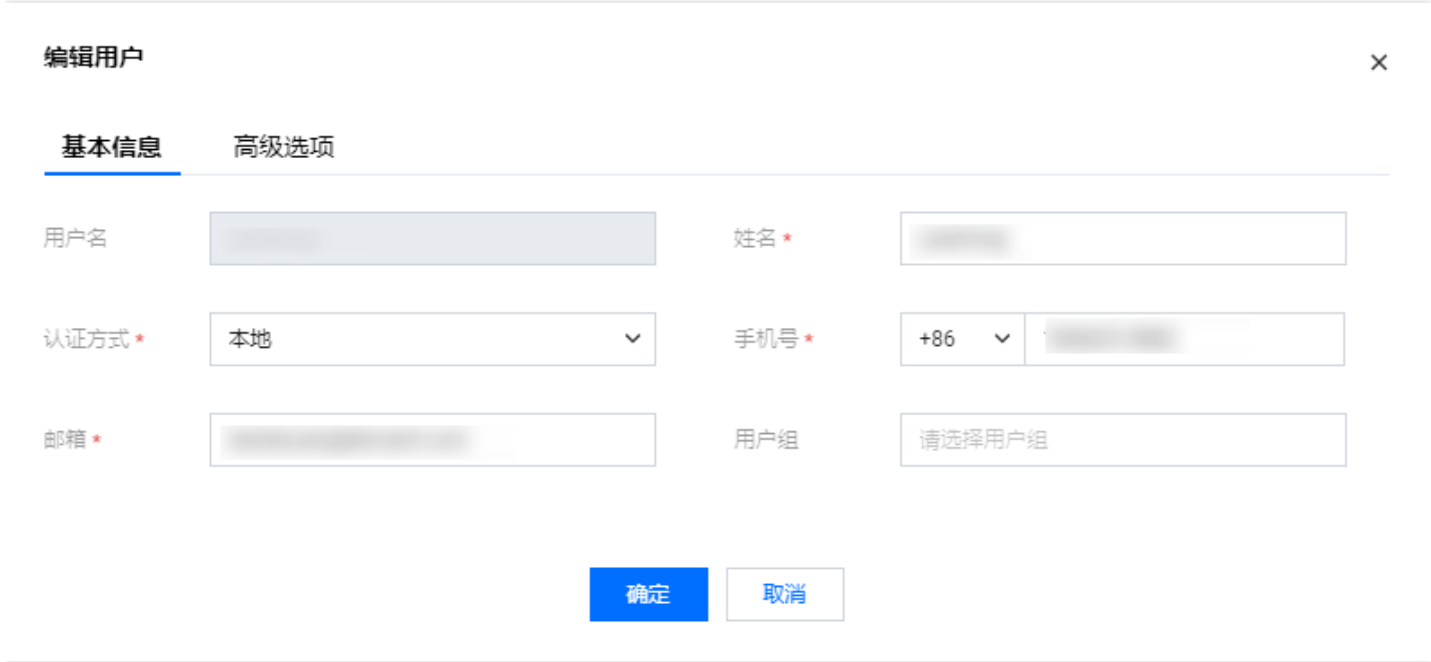
最近更新时间: 2024-12-19 17:12:00

步骤1：进入云堡垒机控制台之后，在左侧导航选择用户管理 > 用户，进入用户页面。

步骤2：在用户页面，单击编辑，弹出编辑用户弹窗。



步骤3：在编辑用户弹窗，修改需要变动的信息。



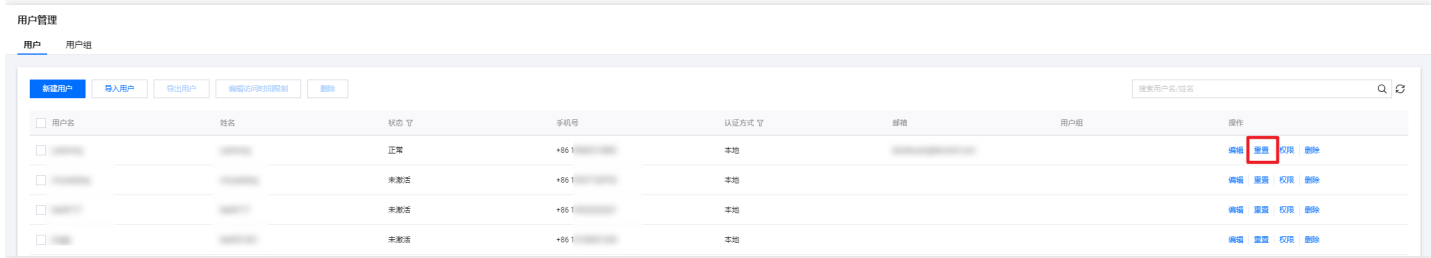
步骤4：单击确定，即可保存新的用户信息。

# 重置用户

最近更新时间: 2024-12-19 17:12:00

步骤1：进入云堡垒机控制台之后，在左侧导航选择用户管理 > 用户，进入用户页面。

步骤2：在用户页面，单击重置，弹出"二次确认"弹窗。



步骤3：在"二次确认"弹窗，单击确定，即可重置用户。

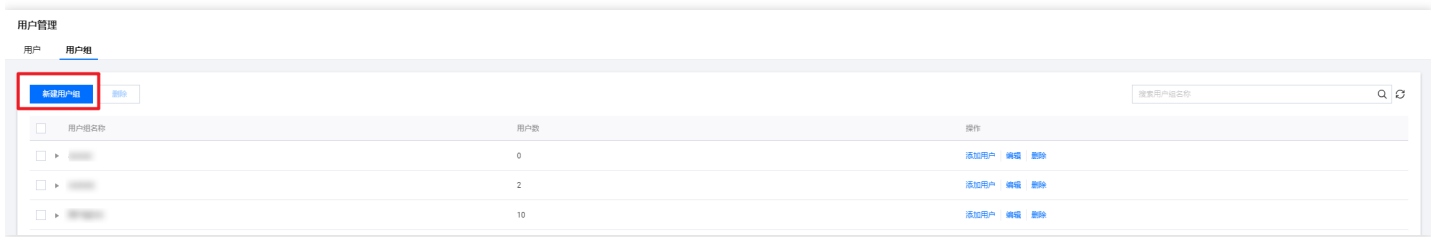
# 用户组管理

## 新建用户组

最近更新时间: 2024-12-19 17:12:00

步骤1：进入云堡垒机控制台之后，在左侧导航选择用户管理 > 用户组，进入用户组页面。

步骤2：在用户组页面，单击新建用户组，打开新建用户组弹窗。



步骤3：在新建用户组弹窗，输入用户组名后，单击确定即可创建用户组。

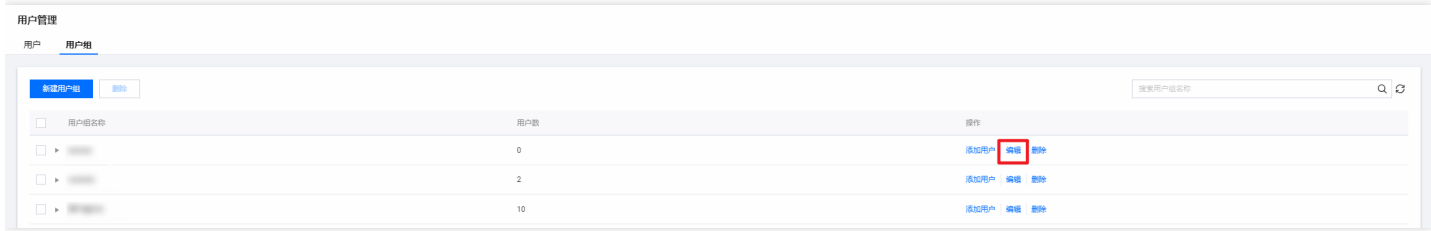


# 编辑用户组

最近更新时间: 2024-12-19 17:12:00

步骤1：进入云堡垒机控制台之后，在左侧导航选择用户管理 > 用户组，进入用户组页面。

步骤2：在用户组页面，单击编辑，可修改用户组的基本信息。



步骤3：在编辑用户组窗口，修改需要变动的信息后，单击确定，即可保存新的用户组信息。

# 将用户添加到用户组

最近更新时间: 2024-12-19 17:12:00

步骤1：进入云堡垒机控制台之后，在左侧导航选择用户管理 > 用户组，进入用户组页面。

步骤2：在用户组页面，单击添加用户，可往用户组添加用户。



步骤3：进入云堡垒机控制台之后，在左侧导航选择用户管理 > 用户组，进入用户组页面。

步骤4：在添加用户窗口，选中需要添加的用户后，单击确定，即可将选择的用户添加到用户组。

添加用户



选择用户

搜索用户名/姓名			
用户名	姓名	手机号	
<input checked="" type="checkbox"/>		+86	
<input checked="" type="checkbox"/>		+86	
<input checked="" type="checkbox"/>		+86	
<input checked="" type="checkbox"/>		+86	
<input type="checkbox"/>		+86	
<input type="checkbox"/>		+86	
<input type="checkbox"/>		+86	
<input type="checkbox"/>		+86	
<input type="checkbox"/>		+86	
<input type="checkbox"/>		+86	
共 17 条			
10 条 / 页			

已选择(4)

用户名	姓名	手机号	
		+86	
		+86	
		+86	
		+86	

取消全部选择

确定

取消

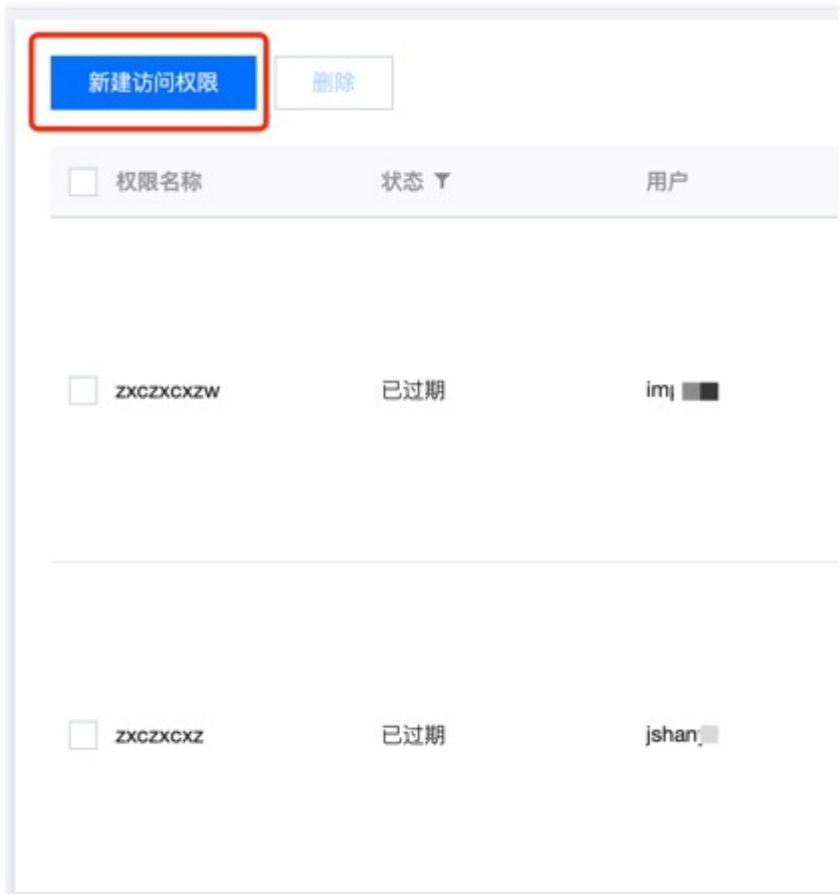
# 权限管理

## 新建访问权限

最近更新时间: 2024-12-19 17:12:00

步骤1：进入云堡垒机控制台之后，在左侧导航选择权限管理 > 访问权限配置，进入访问权限页面。

步骤2：在访问权限页面，单击新建访问权限，进入新建访问权限页面。



步骤3：在新建访问权限页面，按照步骤分别配置权限名称、用户、资产、账号、访问操作、高危命令，实现用户与资产的授权，并对用户操作权限进行控制。



新建访问权限

1

设置权限信息

>

2

选择用户

>

3

选择资产

>

4

选择资产账号

>

5

设置访问操作

>

6

选择高危命令模板

>

7

完成

权限名称 \*

请输入权限名称

有效期

请输入有效期 (默认长期有效)



下一步: 选择用户

步骤4：权限配置完成之后，单击确定提交，即可创建访问权限；此时，运维人员登录运维页面时，就能够看到可访问的主机。

# 编辑访问权限

最近更新时间: 2024-12-19 17:12:00

- 步骤1：进入云堡垒机控制台之后，在左侧导航选择权限管理 > 访问权限配置，进入访问权限页面。
- 步骤2：在访问权限页面，单击编辑，进入编辑访问权限页面。
- 步骤3：在编辑权限页面，可对权限信息、关联用户、关联资产、关联账号、关联访问操作、关联高危命令进行修改。

编辑访问权限

1 设置权限信息 > 2 选择用户 > 3 选择资产 > 4 选择资产账号 > 5 设置访问操作 > 6 选择高危命令模板 > 7 完成

权限名称 \*

有效期

请输入有效期（默认长期有效）

下一步：选择用户

步骤4：权限修改完成之后，单击确定提交，即可保存对访问权限的修改。

# 新建高危命令模板

最近更新时间: 2024-12-19 17:12:00

步骤1：进入云堡垒机控制台之后，在左侧导航选择权限管理 > 高危命令模板，进入高危命令模板页面。

步骤2：在高危命令模板页面，单击新建模板，弹出新建高危命令模板弹窗。

步骤3：在弹出新建高危命令模板弹窗，设置对应的模板名称和禁止执行的命令。

新建高危命令模板

模板名称

高危命令禁止执行

禁止执行的命令

9

确定

取消

步骤4：单击确定，即可创建高危命令模板。

# 编辑高危命令模板

最近更新时间: 2024-12-19 17:12:00

步骤1：进入云堡垒机控制台之后，在左侧导航选择权限管理 > 高危命令模板，进入高危命令模板页面。

步骤2：在高危命令模板页面，单击编辑，弹出编辑高危命令模板弹窗。

<div>新建模板</div>		<div>删除</div>		<div>搜索模板名称</div>	
<div><input type="checkbox"/></div>	模板名称	<div><input type="checkbox"/></div>	禁止执行的命令	操作	
<div><input type="checkbox"/></div>		<div><input type="checkbox"/></div>		<div>编辑</div>	
<div><input type="checkbox"/></div>		<div><input type="checkbox"/></div>		<div>编辑</div>	

步骤3：在编辑高危命令模板弹窗，可对模板名称、禁止执行命令进行修改。

编辑高危命令模板

模板名称

禁止执行的命令

41

确定

取消

步骤4：修改后，单击确定，即可保存模板。

# 审计管理

## 审计字符会话

最近更新时间: 2024-12-19 17:12:00

步骤1：进入云堡垒机控制台之后，在左侧导航选择审计管理 > 运维审计，默认进入字符会话页面。

步骤2：在字符会话页面，单击对应会话右侧的详情，可打开会话详情页面。

资产IP	来源IP	账号	开始时间/结束时间	资产名	用户名/姓名	会话时长/会话大小	操作命令/阻断命令	状态 ▾	操作
			2022-04-21 2022-04-21			23秒 0.70KB	3 0	结束	<a href="#">详情</a> <a href="#">回放</a>
			2022-04-21 2022-04-21			14秒 0.19KB	0 0	结束	<a href="#">详情</a> <a href="#">回放</a>

步骤3：在会话详情页面，可查看会话的基本信息、运维操作记录和文件操作记录。

会话详情

会话信息

运维操作

文件操作

资产IP

资产账号

资产名

跨

用户名称

来源IP

开始时间

2022-04-2

结束时间

2022-04-2

会话时长

23秒

执行命令数

3

会话大小

0.70KB

阻断命令数

0

步骤4：在字符会话页面，单击对应会话右侧的回放，可在新的页面回放历史会话，还原用户真实操作行为。

资产IP	来源IP	账号	开始时间/结束时间	资产名	用户名/姓名	会话时长/会话大小	操作命令/阻断命令	状态	操作
			2022-04-2 2022-04-2			23秒 0.70KB	3 0	结束	<a href="#">详情</a> <a href="#">回放</a>
			2022-04-2 2022-04-2			14秒 0.19KB	0 0	结束	<a href="#">详情</a> <a href="#">回放</a>

步骤5：在历史会话回放页面，可在搜索框对操作命令进行搜索，并定位用户的操作命令。

会话回放

搜索操作命令

14:24:48 浏览

14:24:54 ls

14:25:10 cd deta

14:25:31 cd /

14:25:33 ll

14:25:36 ls

14:25:44 cd data

14:25:46 ll

14:25:48 ls

14:25:57 ll

14:26:02 cd shell

14:26:47 exit

Last login: Tue Apr 26 11:30:33 CST 2022 from 192. on pts/0

Container Linux by CoreOS stable (1 5.5.0)

Update Strategy: No Reboots

Failed Units: 1

systemd-modules-load.service

VM-0-3-coreos ~ # 浏览

-bash: 浏览: command not found

VM-0-3-coreos ~ # ls

# 审计图形会话

最近更新时间: 2024-12-19 17:12:00

步骤1：进入云堡垒机控制台之后，在左侧导航选择审计管理 > 会话审计，进入会话审计页面。

步骤2：单击图形会话，切换到图形会话页面。

## 运维审计

字符会话

图形会话

文件传输

数据库

步骤3：在图形会话页面，单击对应会话右侧的详情，可打开会话详情页面。

近7天近14天近30天2022-04-22 ~ 2022-04-28选择会话属性进行过滤								
资产IP	来源IP	资产账号	开始时间/结束时间	资产名称	用户名/姓名	会话时长/会话大小	状态	操作
10.10.10.10	3.1	administrator	2022-04-25 15:30:24 2022-04-25 15:30:45	资产名称	用户名	21秒 308.58KB	结束	详情回放
42.119.192.192	113.113.113.113	administrator	2022-04-25 15:28:46 2022-04-25 15:28:51	资产名称	用户名	5秒 137.67KB	结束	详情回放
42.192.192.192	11.11.11.11	administrator	2022-04-25 15:28:12 2022-04-25 15:28:26	资产名称	用户名	13秒 47.59KB	结束	详情回放

步骤4：在会话详情页面，可查看会话的基本信息、运维操作记录和文件操作记录。

会话详情

ins- [redacted]



会话信息

运维操作

文件操作



主机IP

192. [redacted]



主机账号

administrator

主机名称

gord [redacted]

用户名称

test- [redacted]



来源IP

113. [redacted]

● 开始时间

2021-09-06 11:36:37

● 结束时间

2021-09-06 11:37:12

会话时长

34秒

会话大小

555.91KB

步骤5：在图形会话页面，单击对应会话右侧的回放，可在新的页面回放历史会话，还原用户真实操作行为。

资产IP	来源IP	资产账号	开始时间/结束时间	资产名称	用户名/姓名	会话时长/会话大小	状态 ▾	操作
10.19. [redacted]	[redacted]	[redacted]tor	2022-04-25 15:30:24 2022-04-25 15:30:45	司 [redacted]	[redacted]	21秒 308.58KB	结束	<a href="#">详情</a> <a href="#">回放</a>
[redacted]	[redacted]	[redacted]tor	2022-04-25 15:28:46 2022-04-25 15:28:51	司 [redacted]	[redacted]	5秒 137.67KB	结束	<a href="#">详情</a> <a href="#">回放</a>
4.1. [redacted]	[redacted]	[redacted]stor	2022-04-25 15:28:12 2022-04-25 15:28:26	司 [redacted]	[redacted]	13秒 47.59KB	结束	<a href="#">详情</a> <a href="#">回放</a>

步骤6：在历史会话回放页面，可查看用户对 Windows 主机的操作行为。



## 图形回放



# 审计文件传输会话

最近更新时间: 2024-12-19 17:12:00

步骤1：进入云堡垒机控制台之后，在左侧导航选择审计管理 > 会话审计，进入会话审计页面。

步骤2：单击文件传输，切换到文件传输会话审计页面。

运维审计

字符会话

图形会话

文件传输

数据库

步骤3：在文件传输页面，单击对应会话右侧的详情，可查看会话详情。

近7天近14天近30天2022-04-22 ~ 2022-04-28

选择会话属性进行过滤

资产IP	来源IP	资产账号	开始时间/结束时间	资产名称	用户名/姓名	会话时长	文件(夹)操作数	状态	操作
106.5.192.11	113.111.111.111	root	2022-04-28 14:20:58 2022-04-28 14:21:03	113.111.111.111	lrgn	4秒	0	结束	详情
114.111.111.111 (外)	113.111.111.111	root	2022-04-27 19:50:11 2022-04-27 19:50:14	113.111.111.111	lcldk	3秒	0	结束	详情
192.168.1.1	113.111.111.111	root	2022-04-26 15:30:35 2022-04-26 16:14:53	113.111.111.111	lcldk	44分17秒	2	结束	详情

步骤4：在会话详情页面，可查看用户的文件传输操作，包括操作类型、文件(夹)名称、文件大小、文件路径等信息。

会话详情

ins



会话信息

文件操作

请输入文件(夹)名称



操作时间	操作类型	文件(夹)名称	文件大小	来源路径/目标路径	状态
2021-09-01 16:53:11	下载文件	Dja	7.33MB	来源路径: /root/Dj	• 已执行
2021-09-01 16:53:03	删除文件	.ex	0B	来源路径: /root/.e	• 已执行
2021-09-01 16:53:03	删除文件	上传	0B	来源路径: /root/上	• 已执行
2021-09-01 16:53:03	删除文件	新建	0B	来源路径: /root/新	• 已执行
2021-09-01 16:50:56	上传文件	.ex	134.75MB	目标路径: /root/.e	• 已执行
2021-09-01 16:50:39	上传文件	上传	0.28KB	目标路径: /root/上	• 已执行
2021-09-01 16:50:39	上传文件	新建	0B	目标路径: /root/新	• 已执行

# 审计数据库会话

最近更新时间: 2024-12-19 17:12:00

步骤1：进入云堡垒机控制台之后，在左侧导航选择审计管理 > 会话审计，进入会话审计页面。

步骤2：单击数据库，切换到数据库会话列表。

## 运维审计

字符会话

图形会话

文件传输

数据库

步骤3：在数据库会话列表，单击对应会话右侧的详情，可查看会话详情。

近7天

近14天

近30天

2022-04-22 ~ 2022-04-28

选择会话属性进行过滤

资产IP	来源IP	资产账号	开始时间/结束时间	资产名称	用户名/姓名	语句数	状态	操作
192.1	11:	root	2022-04-25 16:49:57 2022-04-25 16:49:57	SQLSe	lc ld	10	结束	详情
192.	11:	root	2022-04-25 16:49:56 2022-04-25 16:53:55	SQLSe	lc ld	1	结束	详情
192	11:	root	2022-04-25 16:49:56 2022-04-25 16:53:55	SQLS	lc lc	8	结束	详情

步骤4：在会话详情页面，可查看用户的运维操作，包括操作时间、操作命令信息。

会话详情

cdb-

×

会话信息

运维操作

请输入操作语句

Q

↺

操作时间	操作命令	状态 ▾
2021-11-06 17:22:54	use	• 已执行
2021-11-06 17:22:55	use	• 已执行
2021-11-06 17:23:12	sho	• 已执行
2021-11-06 17:23:15	sele	• 已执行
2021-11-06 17:23:15	sho	• 已执行
2021-11-06 17:24:12	Cre prin	• 已执行
2021-11-06 17:24:13	sho	• 已执行

# 系统设置

## 访问白名单

最近更新時間: 2024-12-19 17:12:00

步骤1：进入云堡垒机控制台之后，在左侧导航选择系统管理>访问白名单，进入访问白名单页面。

步骤2：如果自动添加白名单功能为开启状态，则运维用户登录成功之后，将自动把运维用户的来源 IP 加到访问白名单；该功能用户可手动关闭。

步骤3：在访问白名单页面，单击添加，弹出添加访问白名单弹窗，配置白名单信息。

添加访问白名单

来源IP \*

请输入来源IP

备注

请输入备注

确定

取消

步骤4：单击确定，即可完成访问白名单添加。

# 登录安全设置

最近更新时间: 2024-12-19 17:12:00

步骤1：进入云堡垒机控制台之后，在左侧导航选择系统设置 > 安全设置，进入安全设置页面。

步骤2：进入登录安全设置页面，单击编辑可设置以下内容。

Web闲置超时	<input type="text" value="60"/>	分钟 ⓘ
密码错误锁定	<input type="text" value="5"/>	次 ⓘ
锁定时长	<input type="text" value="10"/>	分钟

确定取消

步骤3：单击确定，即可保存设置。

# 本地认证设置

最近更新时间: 2024-12-19 17:12:00

步骤1：进入云堡垒机控制台之后，在左侧导航选择系统设置 > 认证设置，进入认证设置页面。

步骤2：在本地认证页面，单击右上角的编辑，并设置以下内容：

密码最小长度	<input type="text" value="8"/>
密码复杂度	<input type="text" value="必须包括大写字母、小写字母、数字和特殊符号中的三类"/>
密码有效期	<input type="text" value="180天"/> ⓘ
历史密码相同检查	<input type="text" value="2"/> ⓘ
<div><input type="button" value="确定"/> <input type="button" value="取消"/></div>	

步骤3：设置所需内容后，单击确定，即可保存设置。



# 双因子认证设置

最近更新时间: 2024-12-19 17:12:00

步骤1：进入云堡垒机控制台之后，在左侧导航选择系统设置 > 认证设置，默认进入本地认证页面，单击双因子认证，可切换至双因子认证页面。

步骤2：在双因子认证页面，单击右上角的编辑，并设置双因子选择 OTP 或短信。

开启双因子认证

☒ OTP

☐ 短信

开启后，全部运维用户将强制采用OTP+密码双因子认证。

开启后，全部运维用户将强制采用短信+密码双因子认证。暂不支持国际/港澳台短信。

确定

取消


步骤3：设置所需内容后，单击确定，即可保存设置。

# 自动同步资产设置

最近更新时间: 2024-12-19 17:12:00

步骤1：进入云堡垒机控制台之后，在左侧导航选择系统设置 > 数据维护，进入资产自动同步页面。



步骤2：在资产自动同步页面，单击编辑，在编辑页面单击  开启自动同步开关。



步骤3：单击确定，即可保存设置。启用自动同步之后，每间隔大约8小时会自动同步对应资产到云堡垒机当中。

# 运维员操作指南

## 下载 BHLoader

最近更新时间: 2024-12-19 17:12:00

步骤1：在浏览器中输入运维页面登录地址，打开云堡垒机运维页面；输入手机号、密码登录云堡垒机；也可以单击账号密码切换到账号名、密码方式登录。

步骤2：进入云堡垒机之后，在左侧导航选择辅助工具，进入辅助工具页面。

步骤3：根据用户终端的操作系统类型，下载对应的工具、并安装。下载并安装 BHLoader 之后，用户还需要安装对应的运维工具（例如 XShell）才能访问主机。

# 访问主机

## Web 页面调用客户端

最近更新时间: 2024-12-19 17:12:00

- 步骤1：进入云堡垒机运维页面之后，在左侧导航选择主机资产，进入主机列表页面。
- 步骤2：在主机列表页面，单击对应主机右侧的访问，弹出访问主机弹窗。
- 步骤3：在访问主机弹窗，选择访问协议、访问方式和主机账号后，单击访问，即可调用对应的客户端工具访问主机。

访问主机

×

访问协议

☒ SSH

☐ SFTP

访问方式

SecureCRT

▼

主机账号

 root

▼

访问

取消

# H5 运维

最近更新时间: 2024-12-19 17:12:00

步骤1：进入云堡垒机运维页面之后，在左侧导航选择主机资产，进入主机列表页面。

步骤2：在主机列表页面，单击对应主机右侧的访问，弹出访问主机弹窗。

步骤3：在访问主机弹窗，选择访问协议和主机账号，并将访问方式选择为 Web 后，单击访问，即可通过 H5 的方式访问主机。

访问资产

访问协议

☒ SSH

☐ SFTP

访问方式

Web

资产账号

 root

访问

取消

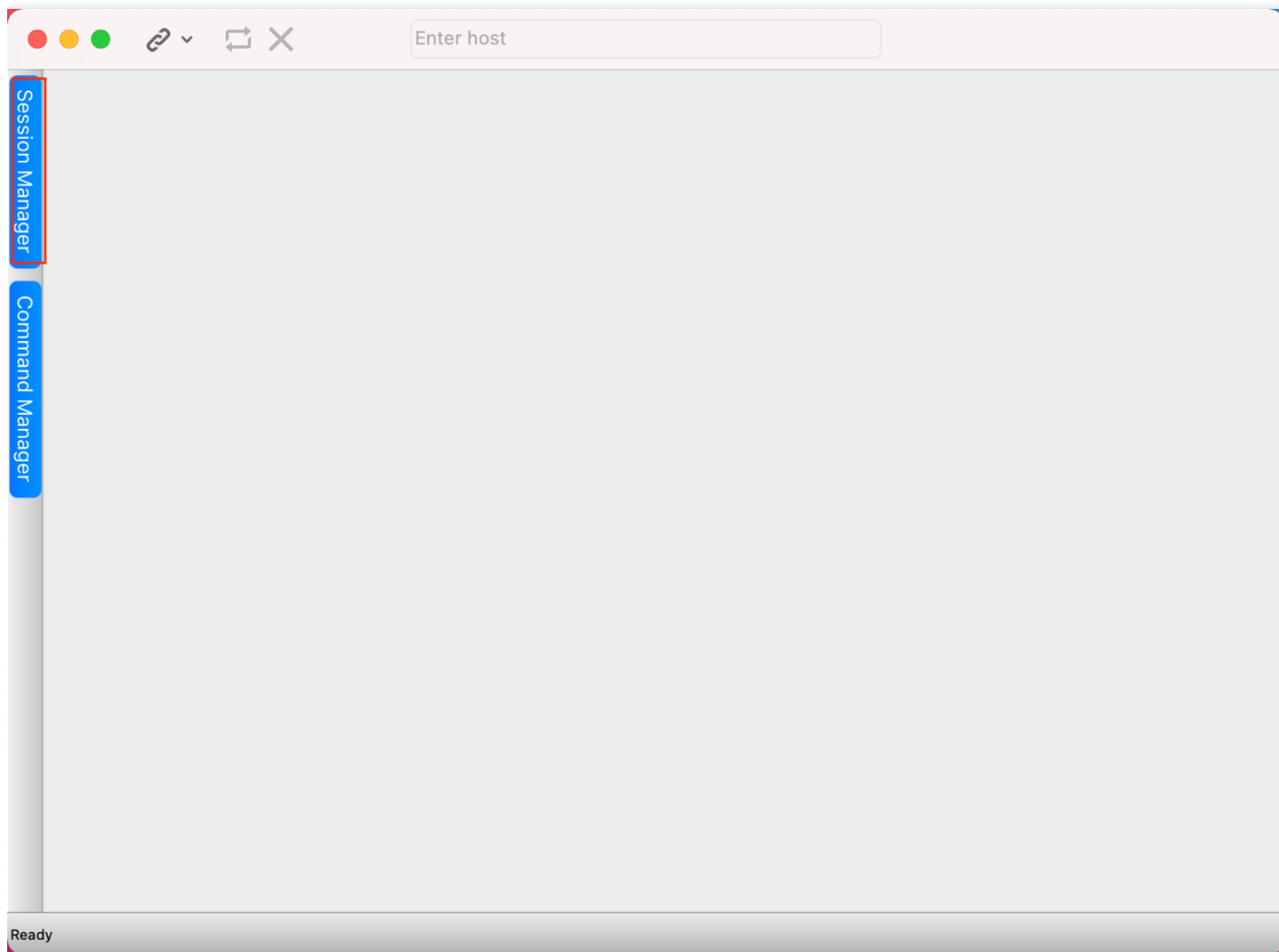
步骤4：在 H5 运维页面，用户可直接输入操作命令。

# SSH 或 SFTP 直连

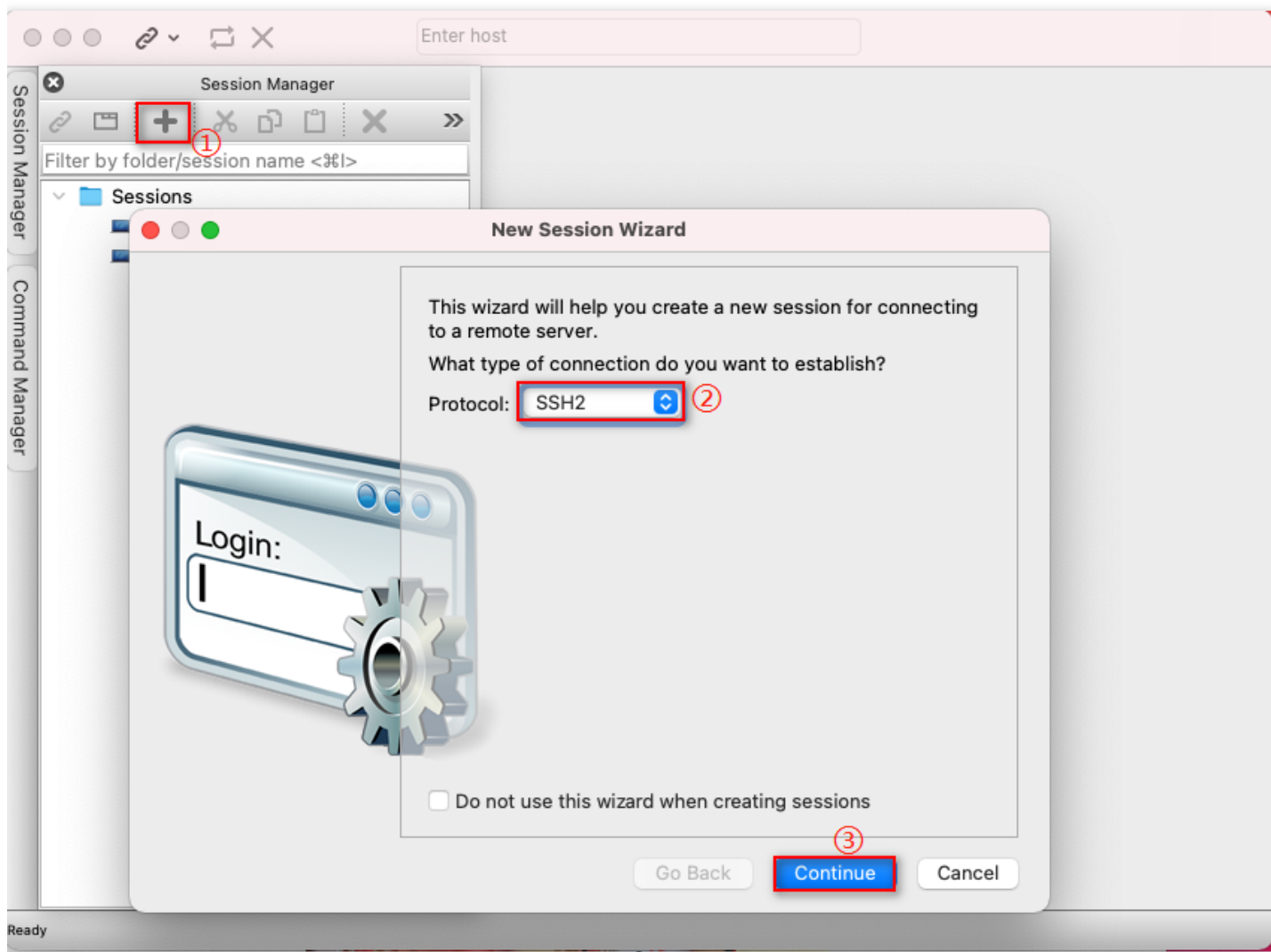
最近更新时间: 2024-12-19 17:12:00

以 macOS 系统下的SecureCRT 为例，介绍如何通过 SSH 客户端直连方式访问 Linux 主机，其他客户端（例如 XShell、Xftp、Transmit 等）请参考以下方式进行访问。

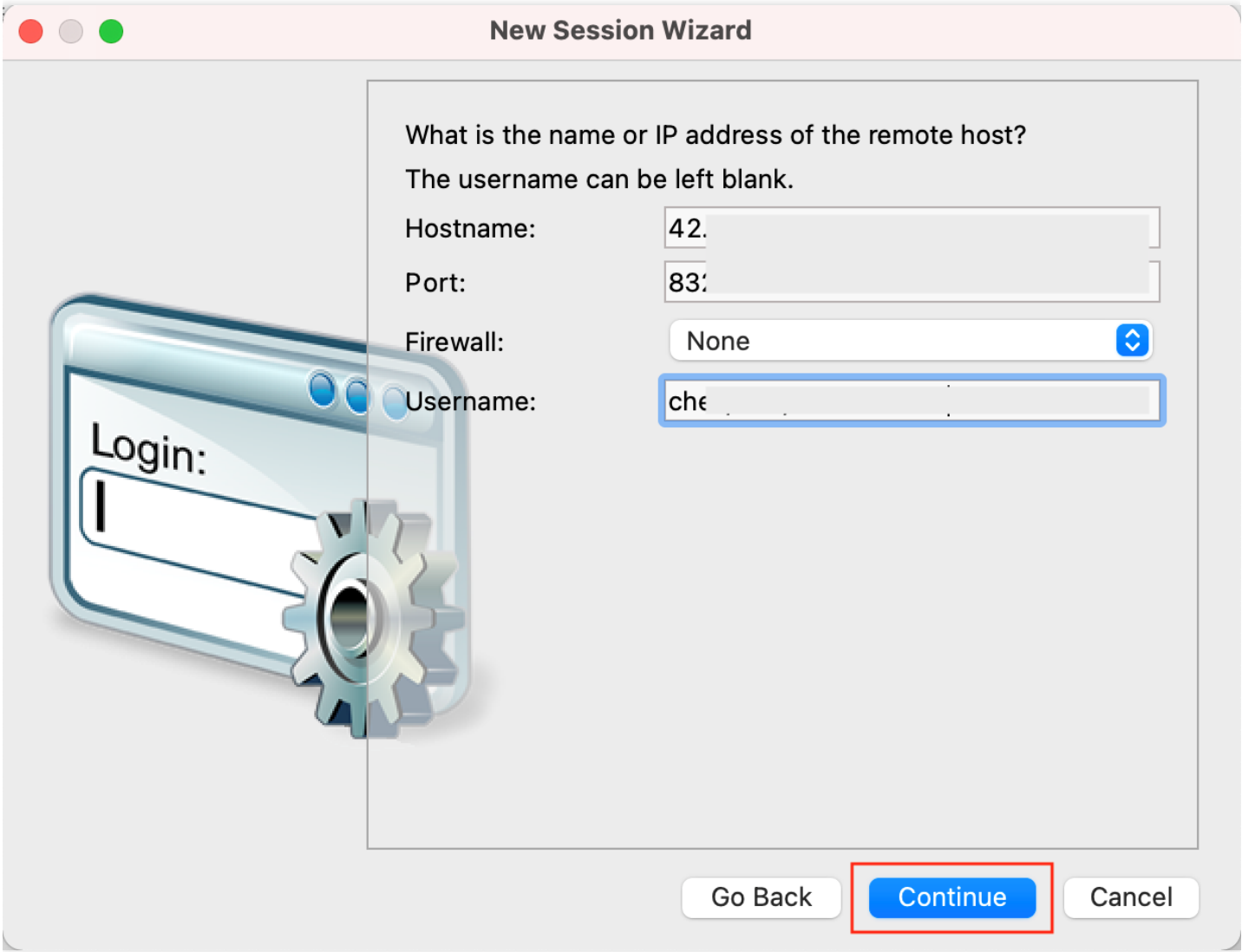
步骤1：打开 SecureCRT，单击左侧的 Session Manager。



步骤2：单击 New Session，打开 New Session Wizard 窗口，窗口当中 Protocol 设置为 SSH2，单击 Continue。



步骤3：输入登录信息，单击 Continue。

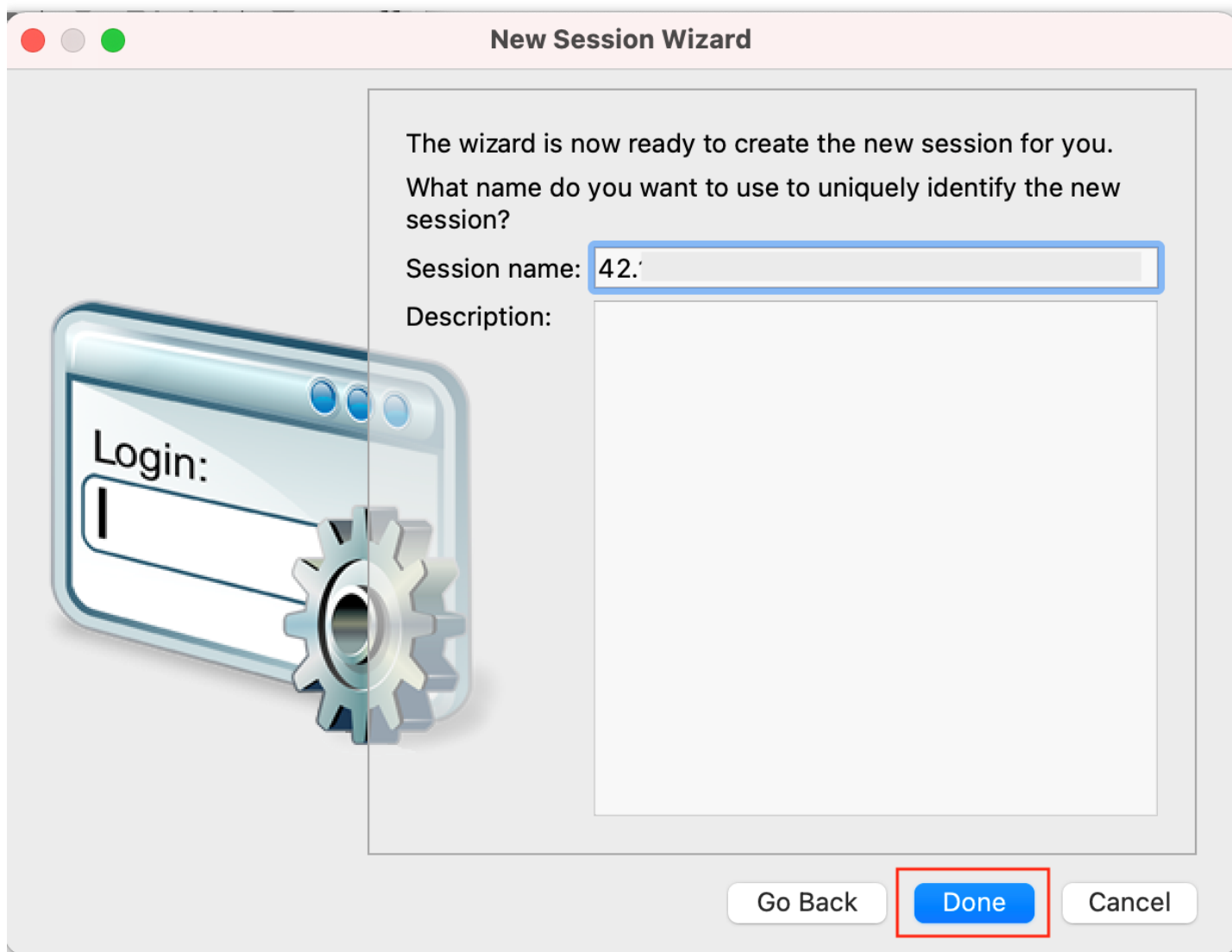


参数列表

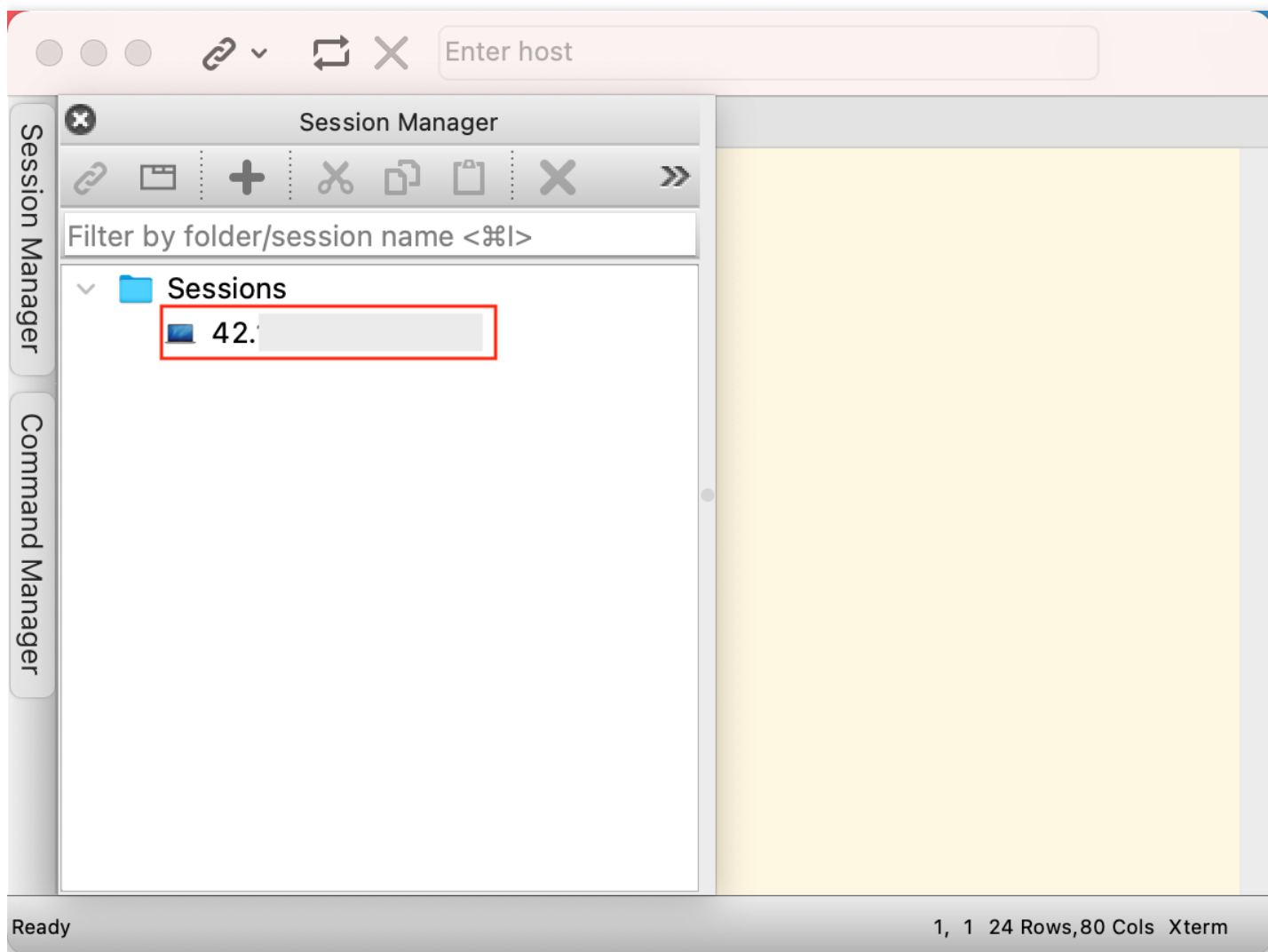
参数名称	参数说明
Hostname	云堡垒机的 IP 地址，联系管理员获取
Port	8322
Firewall	None
Username	云堡垒机的用户名/待访问主机的账号/待访问主机的 IP 地址，例如：test/root/192.168.10.20

步骤4：输入自定义的 Session name 之后，单击 Done。

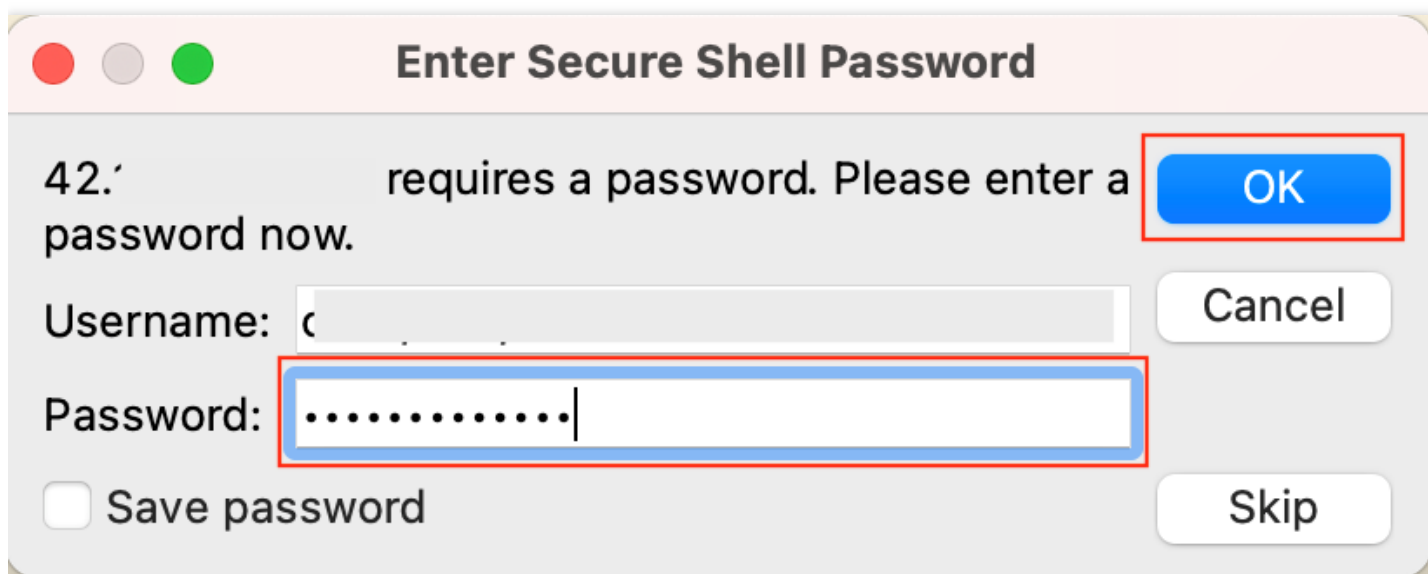




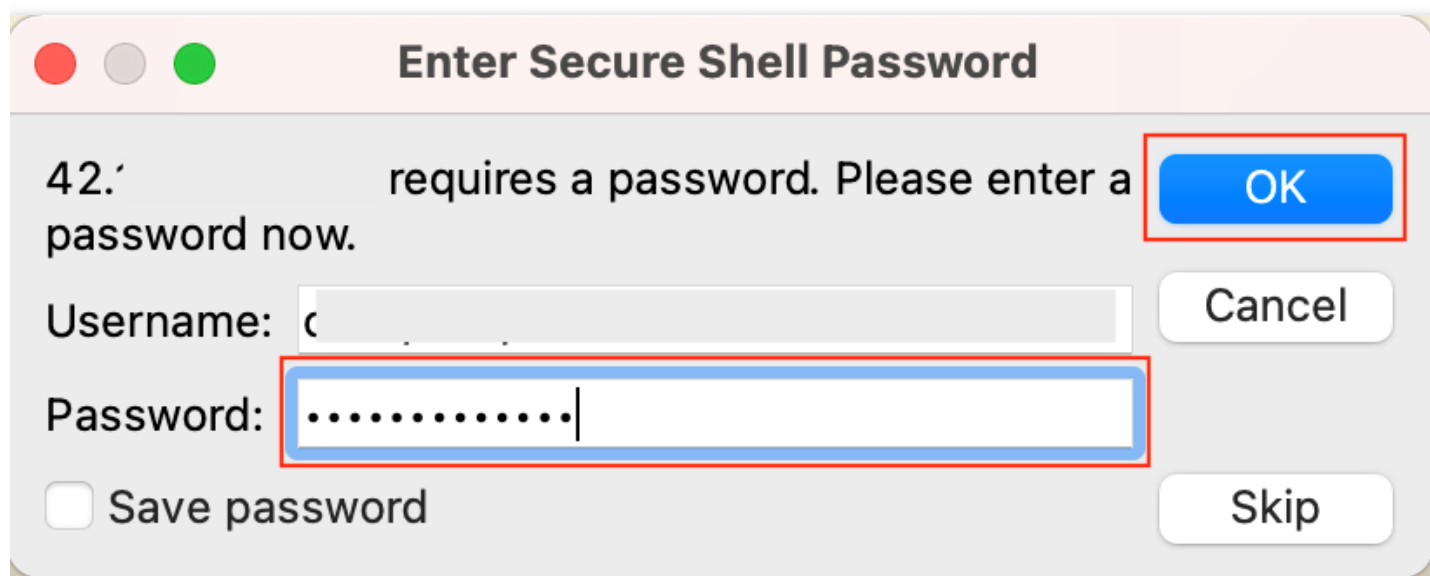
步骤5：返回 Session Manager 后，双击“待访问的会话”。



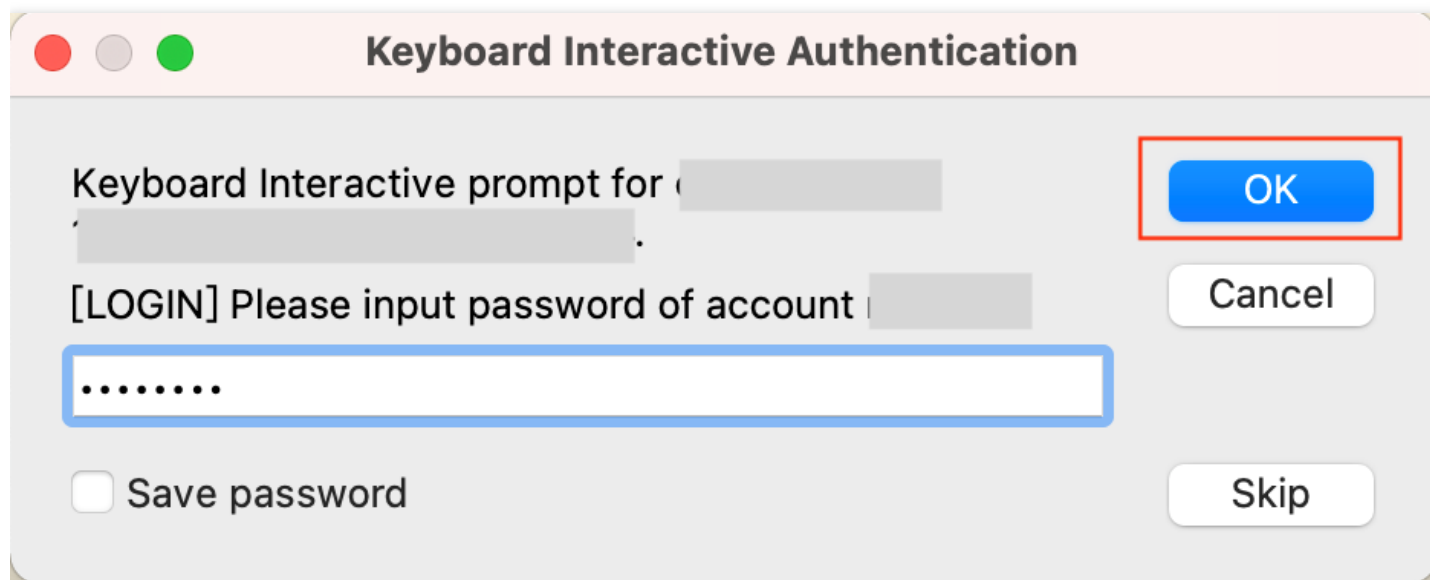
步骤6：在弹窗当中，输入当前云堡垒机用户的密码，单击 OK。



步骤7：在弹窗当中，输入双因子验证码，单击 OK。



步骤8：如果待访问的目标主机的账号未托管密码，则在弹窗当中输入主机账号的密码，然后单击 OK。如果已托管密码，则跳过此步骤。



步骤9：登录到目标主机，可进行运维操作。

# 访问串

最近更新时间: 2024-12-19 17:12:00

以 macOS 系统下的 SecureCRT为例，介绍如何通过访问串方式访问 Linux 主机，其他客户端（例如 XShell、Xftp、Transmit等）请参考以下方式进行访问。

步骤1：进入云堡垒机运维页面之后，在左侧导航选择主机资产，进入主机列表页面。

步骤2：在主机列表页面，单击对应主机右侧的访问串，弹出访问串对话框。

搜索资产名称/IP

Q

资产ID/名称	资产IP	操作系统	操作
ins yjs	4. 1	CentOS 8.2 64位	<a href="#">访问</a> <a href="#">访问串</a> <a href="#">收藏</a>
ext gor	8	Windows	<a href="#">访问</a>   已收藏
ex gc	8.	Linux	<a href="#">访问</a>   <a href="#">访问串</a>   <a href="#">收藏</a>

步骤3：在访问串对话框中，单击查看访问串。（如果访问串未创建，请先单击更新访问串）



步骤4：将访问串展示的 IP、端口、用户名、密码等信息，复制并粘贴到客户端进行访问。

Login:

New Session Wizard

What is the name or IP address of the remote host?  
The username can be left blank.

Hostname:

Port:

Firewall:

None

Username:

Go Back

Continue

Cancel

参数说明：

参数名称	参数说明
Hostname	访问串 IP
Port	访问串端口
Firewall	None
Username	访问串用户名

最近更新时间: 2024-12-19 17:12:00


步骤1：进入云堡垒机运维页面之后，在左侧导航选择数据库资产，进入数据库列表页面。

步骤2：在数据库资产列表页面，单击对应数据库右侧的访问串，弹出访问串窗口。

步骤3：在访问串对话框中，单击查看访问串。（如果访问串未创建，请先单击更新访问串）





访问串


资产账号

 t

[更新访问串](#) [删除访问串](#)

访问串信息

IP	42		端口	8433	
用户名	root@1dC		密码	BRtO3M	
过期时间	2022-10-25 15:53:28 <a href="#">续期</a>				

 请将访问串复制并粘贴到客户端进行访问。

关闭

步骤4：将访问串展示的 IP、端口、用户名、密码等信息，复制并粘贴到数据库客户端进行访问，下面以 MySQLWorkbench 和 Navicat 客户端为例介绍如何操作。

- MySQLWorkbench



Setup New Connection

Connection Name:

Type a name for the connection

Connection Method:

Standard (TCP/IP)

Method to use to connect to the RDBMS

Parameters

SSL

Advanced

Hostname:

Port:

Name or IP address of the server host - and TCP/IP port.

Username:

Name of the user to connect with.

Password:

Store in Keychain ...

Clear

The user's password. Will be requested later if it's not set.

Default Schema:

The schema to use as default schema. Leave blank to select it later.

Configure Server Management...

Test Connection

Cancel

OK

参数列表

参数名称	参数说明
Connection Name	自定义连接名称
Connection Method	默认选择 Standard ( TCP/IP )
Hostname	访问串 IP
Port	访问串端口
Username	访问串用户名
password	访问串密码
Default Schema	-

- Navicat

新建连接 — MySQL

常规

高级

数据库

SSL

SSH

HTTP

Navicat

服务器

连接名:

主机:

端口:

3306

用户名:

密码:

☒

保存密码

测试连接

取消

保存

参数列表

参数	参数说明
连接名	自定义连接名称
主机	访问串 IP
端口	访问串端口
用户名	访问串用户名

参数	参数说明
密码	访问串密码

步骤5：访问串设置并保持之后，在访问串的有效期内，均可以使用该访问串进行数据库访问。

# 最佳实践

## 高危命令阻断

最近更新时间: 2024-12-19 17:12:00

高危命令阻断可有效防止运维人员由于误操作，或者恶意操作导致的运维安全事故，本文为您详细介绍如何在云堡垒机配置高危命令阻断策略。

### 创建高危命令模板

- 步骤1：进入云堡垒机控制台之后，在左侧导航选择权限管理 > 高危命令模板，进入高危命令模板页面。
- 步骤2：在高危命令模板页面，单击新建模板，弹出新建高危命令模板弹窗。
- 步骤3：在新建高危命令模板弹窗中，设置对应的模板名称和禁止执行的命令。

新建高危命令模板

模板名称

请输入模板名称

禁止执行的命令

每行对应一个正则表达式，表示一个或多个命令。比如： "rm \*.\*"表示文件删除命令； "shutdown \*.\*" 表示关机命令

0

确定

取消

步骤4：单击确定，即可创建高危命令模板。

### 访问权限关联高危命令模板

- 步骤1：进入云堡垒机控制台之后，在左侧导航选择权限管理 > 访问权限设置，进入访问权限页面。
- 步骤2：在访问权限页面，单击对应访问权限右侧的编辑，进入编辑访问权限页面。

步骤3：在编辑访问权限页面，跳转到第6步，选择高危命令模板。

1 设置权限名称 > 2 选择用户 > 3 选择主机 > 4 选择账号 > 5 设置访问操作 > 6 选择高危命令模板 > 7 完成

选择账号

账号	主机数
<input checked="" type="checkbox"/> [redacted]	1
<input type="checkbox"/> [redacted]	1
<input type="checkbox"/> [redacted]	1

已选择 (1)

账号	主机数
[redacted]	1

上一步：选择主机

下一步：设置访问操作

步骤4：单击下一步：完成，确认访问权限配置信息。

步骤5：确认信息无误之后，单击确定提交，即可保存对访问权限的修改，此时通过该访问权限授权的用户，在访问。

Linux 主机时如果执行高危命令模板里面的命令，将被云堡垒机拦截。

# 安全事故追溯

最近更新时间: 2024-12-19 17:12:00

审计模块能够对用户的运维操作行为进行记录，并且展示运维操作日志，当发生安全事故时，可通过审计模块对安全事故进行追溯，本文以字符会话为例为您介绍如何审计用户运维操作。

步骤1：在左侧导航选择审计管理 > 会话审计，进入会话审计页面。

步骤2：在会话审计页面，单击搜索框，可通过“用户名、姓名、主机名”等关键字对会话进行过滤。



步骤3：查找到相关会话之后，可单击对应会话右侧的回放，通过会话回放方式真实还原用户操作行为。



步骤4：在会话回放页面，可搜索用户运维过程当中执行的命令，结合会话回放录像、检查是否存在违规操作。

```
搜索命令 11:04:28 ps
11:04:30 top
11:04:34 ls
11:04:35 ls
11:04:35 ls

MiB Mem : 3880160 total, 2957636 free, 209236 used, 713288 buff/cache
MiB Swap: 0 total, 0 free, 0 used. 3426916 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM    TIME+  COMMAND
 12667 root        20   0   160072    2264   1512 R   4.8   0.1   0:00.01 top
    1 root        20   0   125504    4032   2620 S    0.0   0.1   0:30.76 systemd
    2 root        20   0         0         0         0 S    0.0   0.0   0:00.09 kthreadd
    4 root         0 -20         0         0         0 S    0.0   0.0   0:00.00 kworker/0:0H
    6 root        20   0         0         0         0 S    0.0   0.0   0:01.10 ksoftirqd/0
    7 root        rt    0         0         0         0 S    0.0   0.0   0:01.07 migration/0
    8 root        20   0         0         0         0 S    0.0   0.0   0:00.00 rcu_bh
    9 root        20   0         0         0         0 S    0.0   0.0   0:27.68 rcu_sched
   10 root         0 -20         0         0         0 S    0.0   0.0   0:00.00 lru-add-drain
   11 root        rt    0         0         0         0 S    0.0   0.0   0:00.64 watchdog/0
   12 root        rt    0         0         0         0 S    0.0   0.0   0:00.46 watchdog/1
   13 root        rt    0         0         0         0 S    0.0   0.0   0:01.08 migration/1
   14 root        20   0         0         0         0 S    0.0   0.0   0:01.05 ksoftirqd/1
   16 root         0 -20         0         0         0 S    0.0   0.0   0:00.00 kworker/1:0H
   18 root        20   0         0         0         0 S    0.0   0.0   0:00.00 kdevtmpfs
   19 root         0 -20         0         0         0 S    0.0   0.0   0:00.00 netns
   20 root        20   0         0         0         0 S    0.0   0.0   0:00.06 khungtaskd
   21 root         0 -20         0         0         0 S    0.0   0.0   0:00.00 writeback
   22 root         0 -20         0         0         0 S    0.0   0.0   0:00.00 kintegrityd
   23 root        0 -20         0         0         0 S    0.0   0.0   0:00.00 bioset
   24 root         0 -20         0         0         0 S    0.0   0.0   0:00.00 bioset
   25 root         0 -20         0         0         0 S    0.0   0.0   0:00.00 bioset
   26 root         0 -20         0         0         0 S    0.0   0.0   0:00.00 kblockd
   27 root         0 -20         0         0         0 S    0.0   0.0   0:00.00 md
```

# 常见问题

## 常见问题

最近更新时间: 2024-12-19 17:12:00

## BHLoader 是必须要安装的吗？

BHLoader 的主要功能是拉起本地应用程序，并通过本地应用程序创建连接，访问连接相关的目标资源，因此 BHLoader 是运维人员必须要安装的。

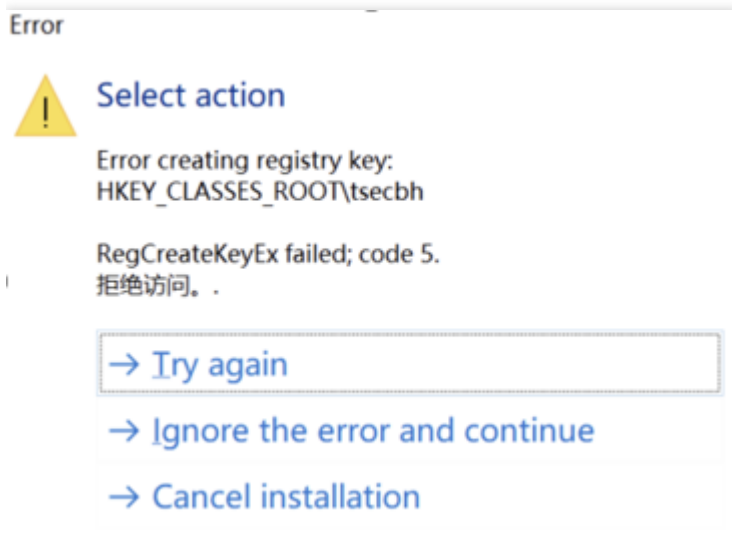
## 安装 BHLoader 后，是否还需要安装 SecureCRT，Xshell 等连接工具软件？

BHLoader 的主要功能是拉起本地应用程序，剩余的连接工作，以及从本地操作 CVM 都是需要在相关的 SecureCRT 或 Xshell 等软件操作的，所以需要在本机安装相关连接工具软件。

## 安装 BHLoader 时，操作系统账户是否需要管理员权限？

需要管理员权限，若没有管理员权限会报如下错误：





## BHLoader 程序出现闪退现象，如何处理？

场景一：检查 Mac 电脑版本，如果是13.0及以上，请按照如下步骤操作。

1. 在本地电脑上执行命令。

```
sudo vim /etc/ssh/ssh_config
```

2. 在文件最后追加一行命令。

```
HostKeyAlgorithms +ssh-rsa,ssh-dss
```

3. 在云堡垒机上重新访问资产。

场景二：如果是运维工具（例如PuTTY）安装路径配置错误，请按照如下步骤操作。

1. 找到 BHLoader 的安装目录。
2. 在安装目录下找到文件 config.toml。

3. 打开 config.toml 文件，检查运维工具安装路径是否正确，如果错误，可以直接删除，后续程序将引导客户重新选择运维工具，也可以修改为正确的运维工具路径。

## 资产账号是否必须是 CVM 上的真实用户？

资产账号中必须是目标 CVM 上已有的用户（如 root、administrator），云堡垒机服务本身不会对 CVM 进行创建用户操作。

## 目前登录 Linux 服务器的私钥带有密码，应如何录入？

设置私钥时，同时设置解密私钥口令，即可实现通过带密码的私钥登录 Linux 服务器。

设置私钥

×

① 您的密钥将加密存储

私钥 \*

请输入私钥

解密私钥口令

请输入解密私钥口令

🔑 ?

确定

取消

## 双因子认证是否可以关闭？

SaaS 型堡垒机必须使用双因子认证，目前阶段有两种选择：密码+OTP 或密码+短信，出于安全性考虑，不支持关闭双因子。

## 访问白名单是什么，没有添加为什么里面会有相关的IP 地址？

访问白名单是限制用户使用本地工具软件（SecureCRT，Xshell，mstsc等），连接云堡垒机的IP 名单，类似于CVM 的安全组。

当用户成功访问运维页面时，会自动把用户的公网IP 地址添加到白名单里面，也可以手动添加。

## 已登录运维页面了，在使用工具访问时，有时候无法连接成功？

造成这种问题可能是贵公司网络出口有多个公网IP 导致，登录运维页面添加的IP 地址，和使用本地工具连接云堡垒机的IP 地址不一致。可将贵公司出口IP 地址的相关IP 网段手动添加到白名单中。

## 云堡垒机是否可以阻止 Linux 执行相关命令？

可以。参考最佳实践《高危命令阻断》。

## 当企业运维人员，登录运维页面后发现主机列表为空？

使用管理员登录到堡垒机管理界面，在访问权限页面单击新建访问权限或编辑，在第3步选择对应主机或主机组，可新建或修改访问权限。



新建访问权限								
权限名称	用户	用户组	主机	主机组	账号	访问操作	高危命令模板	操作
							无	<a href="#">编辑</a> <a href="#">删除</a>

# WinSCP 创建相同文件名，提示被云堡垒机阻断，管理端审计记录为下载操作被阻断，这个是什么原因？

在 WinSCP 中创建文件时，如果服务器上已有同名文件，那么 WinSCP 会默认将这个文件下载下来并进入编辑模式。而如果云堡垒机限制了 SFTP 只能上传不能下载，那么就会出现上述情况。