运维安全中心（堡垒机）

常见问题

腾讯云

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

常见问题
使用相关

最近更新时间：2024-12-13 11:09:03

BHLoader 是必须要安装的吗?

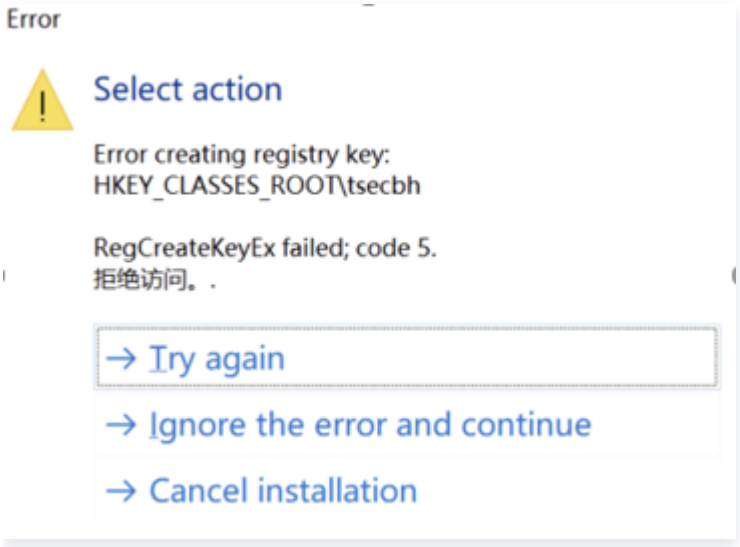
BHLoader 的主要功能是拉起本地应用程序，并通过本地应用程序创建连接，访问连接相关的目标资源，因此 BHLoader 是运维人员必须要安装的。

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，所以需要在本地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. 在运维安全中心（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），运维安全中心（堡垒机）服务本身不会对 CVM 进行创建用户操作。

登录运维安全中心（堡垒机）运维页面之后，在一段时间内没有进行操作将自动断开，是否支持自定义超时时间?

支持，管理员可自己设置 Web 闲置超时时间，详情请参见 登录安全设置 。

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。

双因子认证是否可以关闭?

运维安全中心（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），连接运维安全中心（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运维安全中心（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。

如何了解运维安全中心（堡垒机）带宽使用情况?

可在腾讯云可观测平台的 Dashboard 监控带宽使用情况。

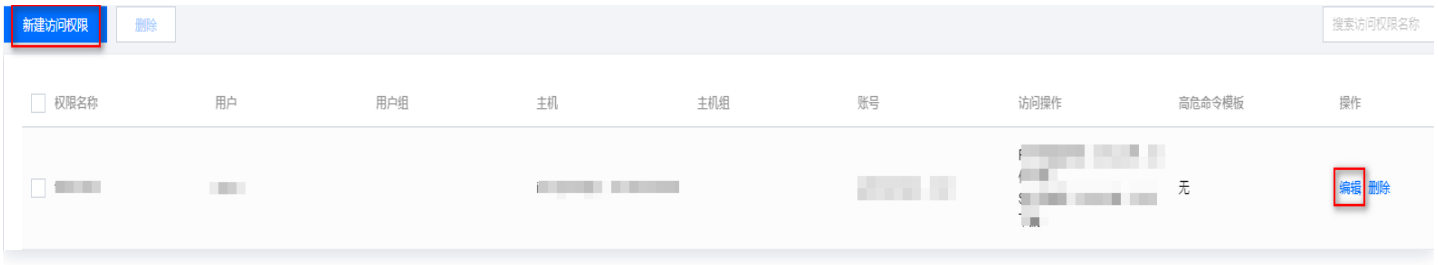
运维安全中心（堡垒机）是否可以阻止 Linux 执行相关命令?

可以阻止 Linux 执行需要禁止的命令，具体操作如下：

1. 在 权限管理 > 高危命令 页面，单击**新建模板**，添加需要禁止的命令。
2. 在 权限管理 > 访问权限 页面，单击**编辑**，为相关权限添加该模板就可实现。

当企业运维人员，登录运维页面后发现主机列表为空?

使用管理员登录到运维安全中心（堡垒机）管理界面，在 权限管理 > 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。



运维安全中心（堡垒机）的日志可以存储多久?

目前由于上线不久，用户可以免费存储180天的审计数据，后续可能会按照存储量收费。

WinSCP 创建相同文件名，提示被运维安全中心（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。而如果运维安全中心（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。

从客户端到堡垒机，需要开放哪些端口?

从客户端到堡垒机，可能会遇到客户网络限制，需要根据实际情况开放以下端口：

端口号	说明	协议	是否必开
443	HTTPS 端口	TCP	是
8322	SSH 代理端口	TCP	访问 SSH 服务器必开
8389	RDP 代理端口	TCP	访问 RDP 服务器必开
8306	MySQL 代理端口（版本低于8.0）	TCP	访问 MySQL 7.x 版本数据库必开
8307	MySQL 代理端口（版本高于或等于8.0）	TCP	访问 MySQL 8.x 版本数据库必开
8433	SQL Server 代理端口	TCP	访问 SQL Server 数据库必开
8432	PostgreSQL 代理端口	TCP	访问 PostgreSQL 数据库必开
8379	Redis 代理端口	TCP	访问 Redis 数据库必开
8321	命令行运维 SSH 代理端口	TCP	命令行运维 SSH 服务器必开
2000X	MongoDB 代理端口	TCP	访问 MongoDB 数据库必开，根据 MongoDB 的节点数量，X 动态变化，以访问串页面为准

咨询相关

最近更新时间：2025-08-14 17:51:22

运维安全中心（堡垒机）提供了标准版和专业版，应如何选择?

- 专业版：适用于有数据库资产纳管需求，或关注运维效率提升的企业。
- 标准版：适用于对云服务器有基本运维、审计需求的中小型企业。
- 详细区别请参见 运维安全中心（堡垒机）标准版与专业版区别 。

购买运维安全中心（堡垒机）之后，是否仍然能够直接连接 CVM 实例的 IP?

运维安全中心（堡垒机）服务本身不会对您 CVM 的安全组进行修改，如果您没有配置其他安全组，则您仍然可以通过 CVM 实例的 IP 进行连接。为了保障运维的合规性和审计的完整性，建议您配置相关的安全组策略，仅允许通过运维安全中心（堡垒机）服务登录 CVM 并进行相关运维操作。

运维安全中心（堡垒机）是否支持内网访问运维页面?

支持。如果您有内网运维需求，请 联系我们 开通此功能。

运维安全中心（堡垒机）是否支持纳管非腾讯云和云下服务器?

支持，前提是网络互通。

运维安全中心（堡垒机）适配哪些远程工具?

- Windows 系统客户端：Mstsc、SecureCRT、Xshell、Xftp、WinSCP、FileZilla、weterm。
- Mac 系统客户端：MRD、iTerm 、Mac Terminal、SecureCRT 、FileZilla、Transmit、weterm。

运维安全中心（堡垒机）支持哪些系统资源?

目前支持 Windows 和 Linux 系统资源，具体版本如下：

资源类型	支持版本
Windows	Windows Server 2012
	Windows Server 2016
	Windows Server 2019
Linux	CentOS 6 及以上
	Tencent Linux release 2.4 及以上

	Debian 7 及以上
	Ubuntu Server 14 及以上
	SUSE Linux Enterprise Server 12 SP3 及以上
	openSUSE 42.3 及以上
	openSUSE Leap 15.1 及以上

运维安全中心（堡垒机）支持哪些文件传输访问?

在权限允许范围内，可通过 SFTP、rz/sz、磁盘映射、剪切板等方式传输文件。

如何获取到 运维安全中心（堡垒机）的内外网 IP?

在 开通服务 页面，可以查看到 运维安全中心（堡垒机）的内外网 IP 地址。

运维安全中心（堡垒机）开通服务之后，是否支持修改 VPC 和子网?

不支持。

运维安全中心（堡垒机）是否支持纳管多个子网的资产?

支持，前提是网络互通。

运维安全中心（堡垒机）如何纳管不同 VPC 的资源?

根据实际情况，可选择如下一种方案：

- 方案1：在所需要纳管的 VPC 中再次 开通 运维安全中心（堡垒机）服务，即重新在不同 VPC 中购买一台 运维安全中心（堡垒机）。
- 方案2：将 VPC 之间的网络打通，网络打通之后不同 VPC 下的资源可以导入纳管，同时可以使用安全组策略，限制只让运维安全中心（堡垒机） IP 访问资源。如何打通不同 VPC 网络可参考： 连接其它 VPC 。

如何使用 运维安全中心（堡垒机）的高危命令管控?

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，编辑高危命令模板名称和禁止执行的命令，单击**确认**保存设置。

> **说明：**

- 每行对应一个正则表达式，表示一个或多个命令；如需要禁用“rm”和“reboot”两个命令，则需要将这两个命令分成两行进行输入。
- 支持正则输入，例如需要禁用“ rm”及"rm"后需要携带的参数命令可以写为“rm.*”或“^rm”，这条命令运维用户在执行命令时匹配中了"rm"的命令都禁止执行。
- 当需要精确匹配某条命令禁止执行，例如“ shutdown”命令，不匹配其余包含“shutdown”关键字的命令，则正则表达式可以写为“^shutdown$”。