

堡垒机

实践教程

产品文档



Tencent Cloud

【版权声明】

©2013-2025 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【商标声明】



及其他腾讯云服务相关的商标均为腾讯集团下的相关公司主体所有。另外，本文档涉及的第三方主体的商标，依法由权利人所有。

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

文档目录

实践教程

- 高危命令阻断
- 文件传输控制
- 安全事故追溯
- 跨 VPC 资产管理
- 使用内网域名访问堡垒机运维页面

实践教程

高危命令阻断

最近更新时间：2025-04-18 11:17:40

操作场景

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堡垒机配置高危命令阻断策略。

说明：

该功能仅支持 Linux 服务器。

步骤1：创建高危命令模板

1. 登录 [堡垒机控制台](#)。
2. 在左侧导航栏中，选择权限管理 > 高危命令。
3. 在高危命令页面，单击新建模板。



模板名称	类型	禁止执行的命令	操作
高危命令模板	普通区	rm -rf /	编辑 删除

4. 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

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

5. 单击确定，即可创建高危命令模板。

步骤2：访问权限关联高危命令模板

1. 登录 [堡垒机控制台](#)。
2. 在左侧导航栏中，选择权限管理 > 访问权限。
3. 在访问权限页面，单击对应访问权限右侧的编辑。

4. 在编辑访问权限页面，跳转到第5步，设置访问权限的主机高危命令。

5. 单击下一步：完成，确认访问权限配置信息。
6. 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，将被堡垒机拦截。

文件传输控制

最近更新时间：2025-04-18 11:17:40

操作场景

文件传输控制可以防止运维人员通过下载文件的方式造成数据泄露，本文为您详细介绍如何在堡垒机配置文件传输权限。

操作步骤

1. 登录 [堡垒机控制台](#)。
2. 在左侧导航栏中，选择权限管理 > 访问权限。
3. 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。
4. 在新建访问权限页面，按照步骤分别配置基本信息、用户、资产、账号，在第5步时，设置仅允许上传文件、禁止下载文件。



主机访问控制 主机高危命令 数据库访问控制

已选主机： 1

RDP磁盘映射 上传文件 下载文件

RDP剪切板 上传文件 下载文件 上行文本 下行文本

RZSZ 上传文件 下载文件

SFTP选项 上传文件 下载文件 删除文件

[上一步：选择账号](#) [下一步：完成](#)

5. 访问操作设置完成之后，单击下一步：完成，继续设置高危命令。
6. 权限配置完成之后，单击确定提交，即可创建访问权限；此时通过该访问权限授权的用户，在访问主机时就无法进行下载文件操作。

设置基本信息 > 选择用户 > 选择资产 > 选择账号 > 设置访问控制 > 6 完成

配置项	配置详情
权限名称	...
有效期	长期有效
用户	...
用户组	未选择
资产	可用 (1)
资产组	未选择
账号	未选择
允许手动填写账号	禁止
允许使用访问串	禁止
RDP磁盘映射	允许文件上传
RDP剪贴板	允许文件上传, 允许上行文本
RZSZ	允许文件上传
SFTP选项	允许文件上传
高危命令	未选择
数据库访问控制	未选择

[上一步：设置访问控制](#)[确定提交](#)[返回权限列表](#)

7. 如果权限已经存在，您也可以通过编辑权限的方式对文件传输操作进行控制。

新建访问权限	删除	<input type="text" value="搜索权限名称"/>					
权限名称	状态	用户	用户组	资产	资产组	账号	操作
...	已生效	...					编辑 删除
...	已生效	...					编辑 删除

安全事故追溯

最近更新时间: 2025-04-18 11:17:40

操作场景

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详细介绍如何审计用户运维操作。

操作步骤

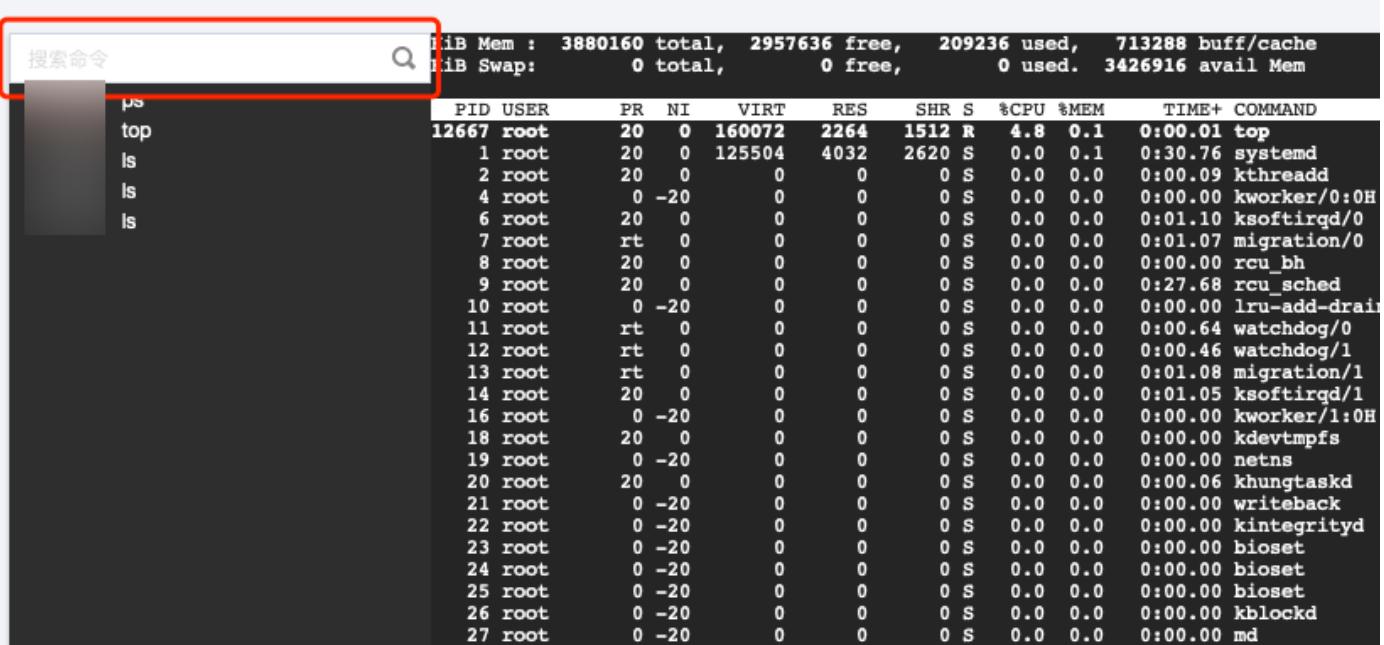
1. 登录 [堡垒机控制台](#)。
 2. 在左侧导航栏中, 选择[操作审计](#) > [会话记录](#) > [字符会话](#)。
 3. 在字符会话页面, 单击[搜索框](#), 可通过“用户名、姓名、资产名称”等关键字对会话进行过滤。

4. 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。

近7天	近14天	近30天	2023-10-13 ~ 2023-10-19	选择会话属性进行过滤	搜索				
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...	操作命令/阻...	状态	操作
192.168.1.1 (外) (内)	192.168.1.2	192.168.1.3	2023-10-13 09:20 2023-10-13 09:35	product1	user1	15秒 0.96KB	1 0	结束	详情 回放
192.168.1.1 (外) (内)	192.168.1.2	192.168.1.3	2023-10-13 10:16 2023-10-13 10:40	product1	user1	24秒 1.51KB	1 0	结束	详情 回放

5. 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。

会话回放



会话回放													
搜索命令		搜索结果											
		命令		状态		CPU 使用		内存 使用		时间			
ps		PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
top	12667	root	20	0	160072	2264	1512	R	4.8	0.1	0:00.01	top	
ls	1	root	20	0	125504	4032	2620	S	0.0	0.1	0:30.76	systemd	
ls	2	root	20	0	0	0	0	S	0.0	0.0	0:00.09	kthreadd	
ls	4	root	0	-20	0	0	0	S	0.0	0.0	0:00.00	kworker/0:0H	
ls	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	

跨 VPC 资产管理

最近更新时间: 2025-04-18 11:17:40

操作场景

当资产（例如 CVM）分布在多个 VPC 时，需要通过堡垒机统一进行管理，本文为您详细介绍如何实现跨 VPC 的资产管理。

操作步骤

1. 登录 [堡垒机控制台](#)。
2. 在左侧导航栏中，选择开通服务。
3. 在开通服务页面，单击购买，进入购买页面，选择合适的规格进行购买。

4. 购买完成之后，返回开通服务页面，找到新购买的堡垒机服务，单击开通。

5. 在开通服务弹窗中，配置地域、VPC 和子网信息后，单击确定，完成开通服务。
 - 地域：请选择堡垒机纳管的资产的所属地域。
 - VPC：请选择需要堡垒机纳管的资产的所属 VPC，选择之后 VPC 无法修改。
 - 子网：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。

开通堡垒机服务

X

资源ID *

b

资产授权数 50 到期

地域 *

中国香港

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, 选择之后VPC无法修改

子网 *

请选择

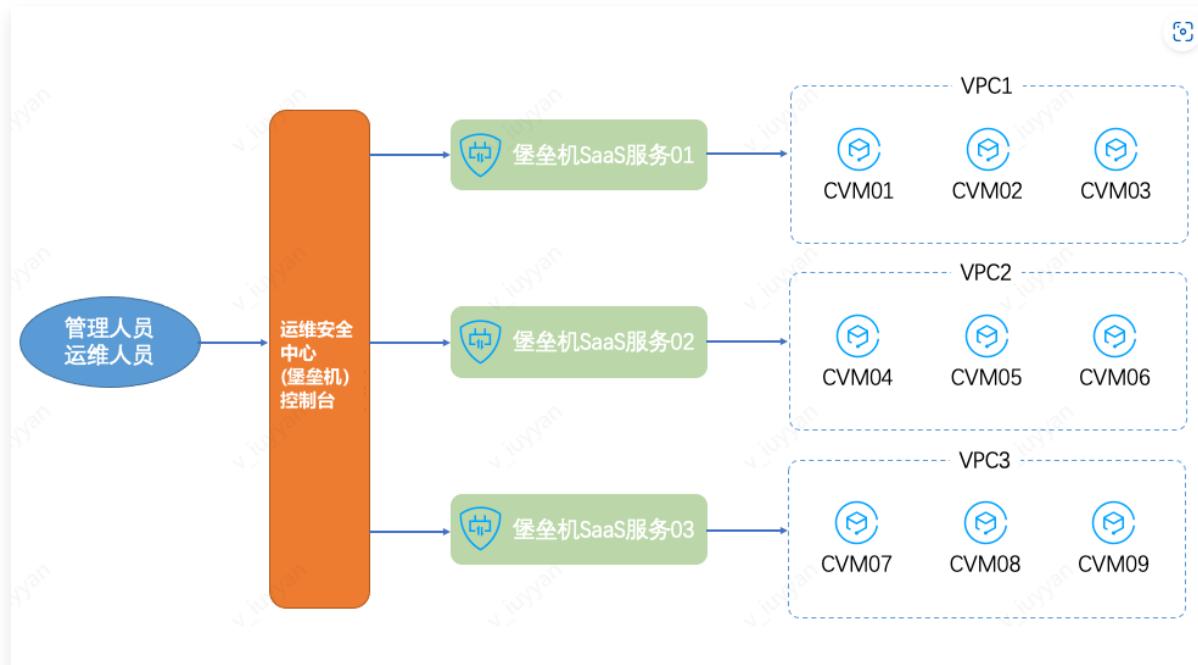
选择任意子网均可, 但完成初始化操作后, 该子网不能被销毁。

建议: 选择资产数量较多的子网。

确定

取消

6. 开通多个服务之后, 不同 VPC 的资产可由对应 VPC 内的堡垒机进行管理, 网络连接链路最短, 并且可通过统一的管理入口和运维入口进行管理和维护工作。



说明

- 管理和维护工作操作详情请参见 堡垒机的 快速入门。

- 除开通堡垒机服务外，还可以通过 [网络域](#)、[对等连接](#)、[云联网](#) 等方式来打通堡垒机与 CVM 之间的网络。

使用内网域名访问堡垒机运维页面

最近更新时间: 2025-08-28 17:26:34

操作场景

内网运维是指通过内部网络访问堡垒机，对主机、数据库、应用等资源进行运维管理，避免通过公网（互联网）访问。堡垒机支持内网运维模式，适用于高安全要求的场景，能有效降低公网暴露风险。

步骤一：开通内网运维

1. 登录 [堡垒机控制台](#)。
2. 在左侧导航栏中，选择开通服务 > 服务列表。
3. 在服务列表页面，单击对应服务操作栏的更多 > 调整运维网络。

4. 在调整运维网络窗口中，选择内网作为运维方式，然后选择 VPC 和子网，单击确定。

说明:

需确保运维人员终端网络和所选的VPC/子网网络能够连通。

步骤二：关联内网域名

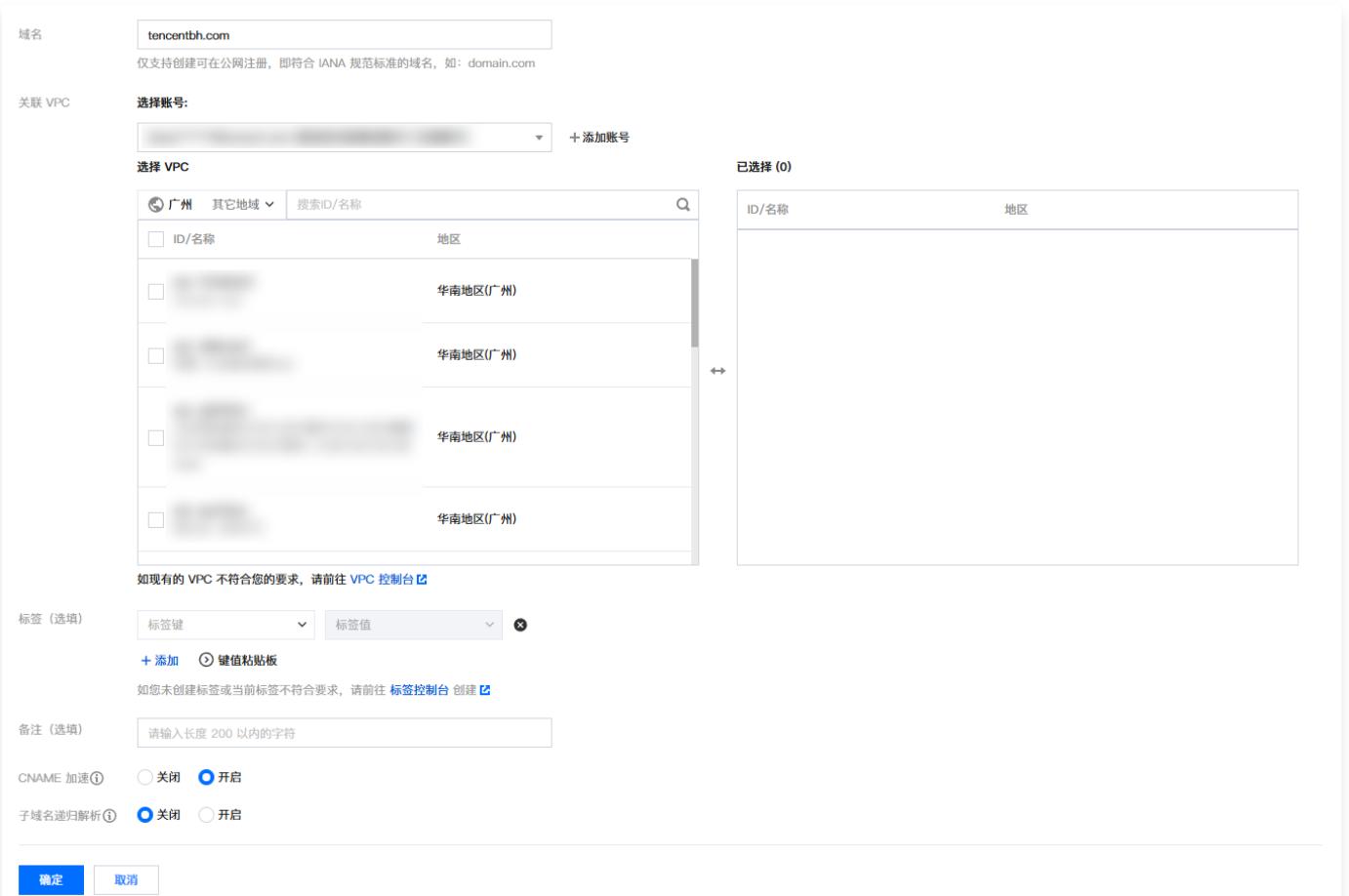
1. 登录 [私有域解析 Private DNS 控制台](#)。
2. 在左侧导航栏中，选择内网解析 > 域名列表。
3. 在域名列表中，单击新建私有域。



私有域/ID	状态	关联 VPC ①	记录	标签	更新时间	备注	操作
1	已关联VPC	██████████	1	0	2025-07-17 16:40:23		解析 关联 VPC 更多 ▾
2	已关联VPC	██████████	2	0	2025-07-16 19:00:40		解析 关联 VPC 更多 ▾

4. 在新建私有域页面，填写私有域相关信息，单击确定。

- 域名：tencentbh.com。
- 关联 VPC：开通内网访问的 VPC。
- 子域名递归解析：关闭。



域名 仅支持创建可在公网注册，即符合 IANA 规范标准的域名，如：domain.com

关联 VPC 选择账号：

选择 VPC 广州 其它地域

ID/名称	地区
██████████	华南地区(广州)

已选择 (0)

如现有的 VPC 不符合您的要求，请前往 [VPC 控制台](#)

标签 (选填)

+ 添加 键值粘贴板

如您未创建标签或当前标签不符合要求，请前往 [标签控制台](#) 创建

备注 (选填)

CNAME 加速 关闭 开启

子域名递归解析 关闭 开启

5. 创建完成后，返回域名列表页面，选择您刚创建的私有域，单击操作列中的解析。

新建私有域		更多操作		输入关键字过滤域名				
私有域/ID	状态	关联 VPC	记录	标签	更新时间	备注	操作	
<input type="checkbox"/> [REDACTED]	已关联VPC	[REDACTED]	1	0	2025-07-17 16:40:23		解析 关联 VPC 更多	
<input type="checkbox"/> [REDACTED]	已关联VPC	[REDACTED]	2	0	2025-07-16 19:00:40		解析 关联 VPC 更多	

6. 在解析记录页面，单击添加记录，添加主机记录和记录值，完成后单击保存即可。

解析记录 - 私有域设置

- 私有域解析 Private DNS 开启子域名谐归解析后，未配置记录将转至公共 DNS 查询。如未开启该功能，并无法正常解析未配置的子域名。请谨慎操作。[了解更多](#)

添加记录		更多操作		权限搜索						请输入要设置的记录	
记录ID	主机记录	记录类型	记录值	权重	权重优先级	TTI (秒)	状态	最后操作时间	备注	操作	操作
<input type="checkbox"/> xxxxxx-124debs9	<input type="text" value="A"/>	<input type="button" value="按如下设置选择"/>	<input type="button" value="按如下设置选择"/>	<input type="button" value="按如下设置选择"/>	-	300	启用	-	<input type="text" value="请输入备注"/>	<input type="button" value="保存"/>	<input type="button" value="取消"/>

提示
填写您服务器 IPv4 地址（如：8.8.8.8），如果您不知道，请咨询您的空间商

共 0 条 20 + 每 / 页 1 / 1 页

说明：

- 主机记录：建议格式为 {resource-id}-{vpc-id}。
- 例如：resource-id="bh-saas-xxxxx", vpc-id="vpc-124debs9"，则主机记录应填写为 xxxxxx-124debs9。
- 记录值：填写需要内网访问的 IP 地址，即 [堡垒机-概览](#) 中显示的内网运维页面的地址 IP。



步骤三：使用内网域名访问运维页面

内网域名关联成功后，即可通过配置的访问域名访问运维页面。

说明：

访问域名：主机记录.tencentbh.com。