

运维安全中心（堡垒机）

实践教程



腾讯云

【版权声明】

©2013–2025 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【商标声明】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。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。

【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

实践教程

数据迁移

高危命令阻断

文件传输控制

安全事故追溯

跨 VPC 资产管理

等保实践教程

等保二级

等保三级

混合云管理实践教程

暴露面收敛实践教程

OrcaTerm 运维实践教程

使用内网域名访问堡垒机运维页面

iOA 零信任堡垒机集成实践教程

实践教程

数据迁移

最近更新时间：2025-08-29 09:44:31

传统型堡垒机于2024年09月30日正式 EOSS (End of Standard Support: 产品停止全面技术支持和续订)，于2024年12月31日正式 EOMS (End of Maintenance Support: 产品停止所有服务)，为了让您的系统服务更加安全，强烈建议您切换至 SaaS 型运维安全中心（堡垒机）。

传统型堡垒机数据迁移到 SaaS 型运维安全中心（堡垒机），目前可迁移的数据包含：用户、资产。迁移之后，用户需要自己完成激活，管理员需要重新为用户设置访问权限。

准备工作

开通 SaaS 型运维安全中心（堡垒机）服务，参考 [开通服务](#)。

数据迁移

用户数据

1. 登录传统型堡垒机控制台，单击用户管理。
2. 在用户管理页面，选中要导出的用户信息，单击操作 > 用户导出将用户信息进行导出。

The screenshot shows the user management interface of a traditional堡垒机. On the left, there's a sidebar with '数据中心' and a group named 'test11月'. The main area has tabs for '仪表盘', '用户管理' (which is active), '资源管理', '计划管理', '角色管理', and '策略管理'. Under '用户管理', there are buttons for '新建', '删除', '搜索', '用户类型管理', and '操作'. The '操作' dropdown menu includes options like '注销选中用户', '解禁选中用户', '锁定选中用户', '解锁选中用户', '修改选中用户组织结构', '修改选中用户策略', '用户导入', and '用户导出' (which is highlighted with a red box). The user list table shows two entries:

序号	用户ID	用户名
1	ct	ch
2	ji	jin

Total number of items: 2

3. 登录 [运维安全中心（堡垒机）控制台](#)，单击侧边栏用户管理。
4. 在用户页面，单击导入用户，在导入用户弹窗中，单击点击下载将模板下载到本地。

导入用户

下载模板

[点击下载](#)

导入用户时，用户数量需小于等于500

上传文件

[点击上传](#)

目前支持的文件类型为*.csv

[下一步](#)

5. 将从传统型堡垒机导出的用户信息复制，并粘贴到 SaaS 型运维安全中心（堡垒机）导入用户模板当中，需要注意将信息粘贴到对应的位置。模板字段对应关系如下：

SaaS 型运维安全中心 (堡垒机)	传统型堡垒机	备注
用户名	用户账号	传统型堡垒机资源类型 UNIX 对应 SaaS 型运维安全中心（堡垒机）的操作系统类型需修改为 Linux。
姓名	用户名称	—
认证方式	—	传统型堡垒机导出之后无认证方式信息，需手动填写。
手机区号	—	传统型堡垒机导出之后无手机区号信息，需手动填写。
手机号	手机	—
邮箱	邮箱	—

6. 单击[点击上传](#)，将模板上传到 SaaS 型运维安全中心（堡垒机），并完成导入操作。

导入用户

下载模板

点击下载

导入用户时，用户数量需小于等于500

上传文件

点击上传

目前支持的文件类型为*.csv

下一步

资产数据（腾讯云内）

腾讯云的云服务器、云数据库资产，可直接使用一键同步即可完成同步操作。

1. 登录 [运维安全中心（堡垒机）控制台](#)，单击侧边栏资产管理，进入资产管理页面。
2. 在资产管理页面，单击同步资产。即可将腾讯云的资产同步到 SaaS 型运维安全中心（堡垒机）。

The screenshot shows the 'Asset Management' page in the Tencent Cloud console. At the top, there are tabs for 'Asset Management' (selected), 'Cloud Audit' (disabled), 'Host Assets' (selected), 'Container Assets', 'Database Assets', 'Web Application Assets', and 'Asset Groups'. On the right, it says 'Last synchronization time: 2025-05-19 13:14:27'. Below the tabs, there's a search bar with placeholder text 'Please enter堡垒机 service name' and a filter button. There are buttons for 'Select Asset' (highlighted in blue), 'Add Asset', 'Batch Add', 'Delete', and 'More Actions'. A dropdown menu shows '更多操作' with options like 'Import', 'Export', 'Sync', and 'Delete'. The main area displays a table of assets with columns: Asset ID/Name, Asset IP, Managed Status, Associated堡垒机, Network Address, Operation System, and Action. Four asset entries are listed:

资产ID/名称	资产IP	托管状态	托管堡垒机	网络地址	操作系统	操作
...	...	未绑定	-	Linux	编辑 账号 (0) 权限 删除	
...	...	未绑定	-	TencentOS Server 2.4 for ARM64 (TKE4)	编辑 账号 (0) 权限 删除	
...	...	未绑定	-	Debian 9.0 64位	编辑 账号 (0) 权限 删除	

资产数据（腾讯云外）

腾讯云外的服务器，可通过导出/导入方式进行迁移。

1. 登录传统型堡垒机控制台，单击资源管理。
2. 在资源管理页面，选中要导出的资源信息，单击操作 > 资源导出将用户信息进行导出。

The screenshot shows the 'Resource Management' tab selected in the top navigation bar. On the left, there's a sidebar with 'Data Security Gateway' and a 'Cloud Data Center' section. The main area displays a table of hosts with columns for序号 (Index), 名称 (Name), IP, 所属组 (Group), and 类型 (Type). A context menu is open over the fifth host, listing options like 'Select Offline Resources', 'Modify Selected Resource Port', 'Modify Selected Resource Organization Structure', 'Modify Selected Resource Authorization Account Password', 'Resource Import', and 'Resource Export'. The 'Resource Export' option is highlighted with a red box.

3. 登录 [运维安全中心（堡垒机）控制台](#)，单击侧边栏资产管理，进入资产管理页面。
4. 在资产管理页面，单击导入主机，在导入主机弹窗中，单击点击下载将模板下载到本地。

This screenshot shows the 'Import Host' dialog. It contains two main sections: 'Download Template' (with a red box around the 'Click to Download' button) and 'Upload File' (with a 'Click to Upload' button and a note: 'Currently supported file types are *.csv. After asset import, please manually modify the asset's corresponding service in the堡垒机 service'). At the bottom is a large blue 'Next Step' button.

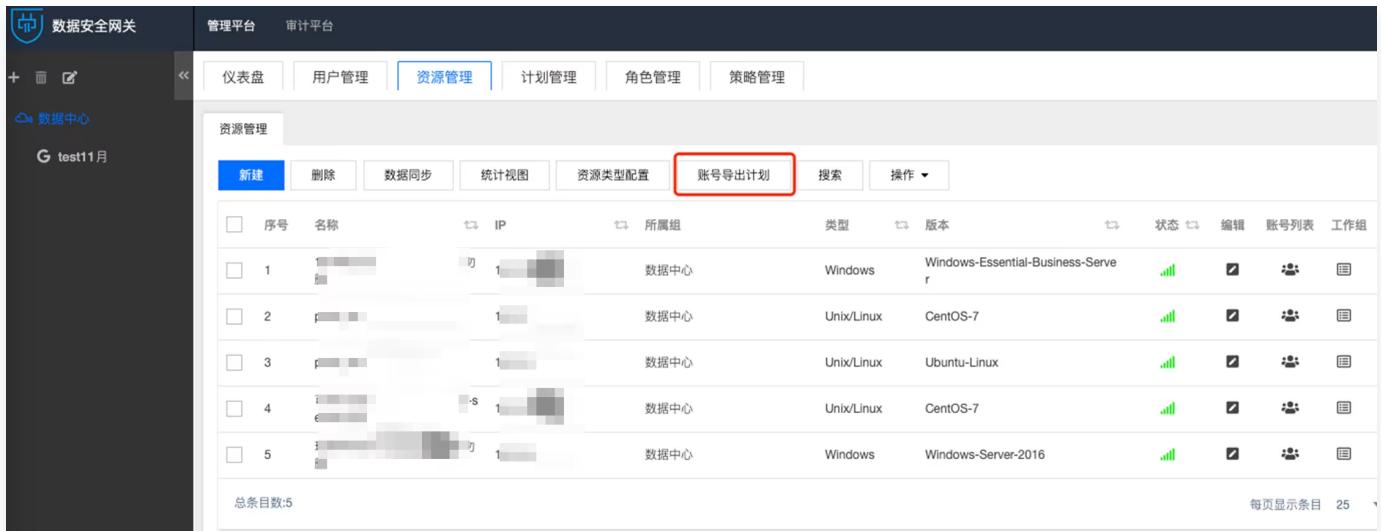
5. 将从传统型堡垒机导出的资产信息复制，并粘贴到 SaaS 型运维安全中心（堡垒机）导入主机模板当中，需要注意将信息粘贴到对应的位置。模板字段对应关系如下：

SaaS 型运维安全中心 (堡垒机)	传统型堡垒机	备注
操作系统类型	资源类型	传统型堡垒机资源类型 UNIX 对应 SaaS 型运维安全中心（堡垒机）的操作系统类型需修改为 Linux。
主机 IP	管理 IP (IPv4)	-
管理端口	-	传统型堡垒机导出之后无端口信息，需手动填写。

账号数据

账号密码信息，可通过导出/导入方式进行迁移。

1. 登录传统型堡垒机控制台，单击资源管理。
2. 在资源管理页面，单击账号导出计划，进入配置页面。



The screenshot shows the 'Resource Management' section of the traditional bastion host control console. The 'Account Export Plan' tab is highlighted with a red box. The table below lists five resources, each with a checkbox, IP address, group, type, and version. The last row indicates 'Total items: 5'. The bottom right corner shows a pagination setting of '每页显示条目 25'.

序号	名称	IP	所属组	类型	版本	状态	编辑	账号列表	工作组
1	[REDACTED]	1 [REDACTED]	数据中心	Windows	Windows-Essential-Business-Serve	[Green]	[Edit]	[Accounts]	[Groups]
2	[REDACTED]	1 [REDACTED]	数据中心	Unix/Linux	CentOS-7	[Green]	[Edit]	[Accounts]	[Groups]
3	[REDACTED]	1 [REDACTED]	数据中心	Unix/Linux	Ubuntu-Linux	[Green]	[Edit]	[Accounts]	[Groups]
4	[REDACTED]	1 [REDACTED]	数据中心	Unix/Linux	CentOS-7	[Green]	[Edit]	[Accounts]	[Groups]
5	[REDACTED]	1 [REDACTED]	数据中心	Windows	Windows-Server-2016	[Green]	[Edit]	[Accounts]	[Groups]

3. 在配置页面当中，配置导出任务的信息，建议执行时间为当天。

The screenshot shows the 'Resource Management' section of the 'Account Export Plan' configuration page. It includes fields for execution time (2023-12-01 17:40:55), interval period (1 day), and password configuration. It also includes sections for FTP and email file delivery, with the FTP section being active. At the bottom are buttons for Stop, Initialize, Close, and File List.

账号导出计划配置内容

执行时间 * 2023-12-01 17:40:55

间隔周期 (天) * 1

加密口令 * 口令已配置

确认加密口令 *

FTP发送 (提示：通过“FTP发送”设置可将账号口令导出文件发送到指定设备)

FTP地址 * 192.168.

目标目录 * /tmp/ji... (示例：/example/example1...)

用户名 * root

口令 * 口令已配置

邮件发送 (提示：通过“邮件发送”设置可将账号口令导出文件发送到指定用户的邮箱)

停止 初始化 关闭 文件列表

4. 当过了执行时间之后，去对应的服务器上下载导出的账号密码文件，也可以进入账号导出计划配置页面，单击文件列表，在文件列表当中下载账号密码文件。

序号	下载地址	操作
1	exp-p [REDACTED] ip	
2	exp-p [REDACTED] ip	
3	exp-p [REDACTED] ip	
4	exp-p [REDACTED] ip	
5	exp-p [REDACTED] ip	
6	exp-p [REDACTED] ip	
7	exp-p [REDACTED] ip	

5. 将从传统型堡垒机导出的账号信息复制，并粘贴到 SaaS 型运维安全中心（堡垒机）导入账号模板当中，需要注意将信息粘贴到对应的位置。模板字段对应关系如下：

SaaS 型运维安全中心（堡垒机）	传统型堡垒机
主机 IP	资源 IPv4
账号	账号名称
密码	账号密码

⚠ 注意：

SaaS 型运维安全中心（堡垒机）账号导入功能目前需加白体验，如有需求，请[提交工单](#)申请。

绑定运维安全中心（堡垒机）服务

资产数据迁移完成之后，需要将资产与堡垒机服务进行绑定。

1. 登录[运维安全中心（堡垒机）控制台](#)，单击侧边栏资产管理，进入资产管理页面。
2. 在资产管理页面，选中资产，单击托管资产。
3. 在弹窗完成绑定，选择运维安全中心（堡垒机）服务，单击确定。

权限配置

数据迁移完成之后，请重新配置用户的访问权限。详情请参见[新建访问权限](#)。

用户激活

管理员将运维页面链接告知运维用户，运维用户需要到运维页面进行激活。详情请参见 [运维人员首次登录](#)。

高危命令阻断

最近更新时间：2024-11-29 17:50:53

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运维安全中心（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 [运维安全中心（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。



The screenshot shows the 'High-risk Command' management page. At the top left is a breadcrumb navigation: '高危命令' (High-risk Command) > '普通区' (Normal Area). Below the navigation, there are two buttons: '新建模板' (Create Template) and '删除' (Delete). A search bar labeled '搜索模板名称' (Search Template Name) is positioned to the right. The main area displays a table with columns: '模板名称' (Template Name), '类型' (Type), '禁止执行的命令' (Commands Prohibited from Execution), and '操作' (Operations). A single row is visible in the table.

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。



The screenshot shows the 'Create High-risk Command Template' dialog box. It has a title bar '新建高危命令模板' (Create High-risk Command Template) and a close button 'X'. On the left, there are two input fields: '模板名称' (Template Name) with the placeholder '请输入模板名称' (Enter template name) and '禁止执行的命令' (Commands Prohibited from Execution) with a text area containing the note: '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' (Each line corresponds to a regular expression, indicating one or more commands. For example, "rm .*" indicates a file deletion command; "shutdown .*" indicates a shutdown command). At the bottom, there are two buttons: '确定' (Confirm) and '取消' (Cancel).

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 [运维安全中心（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。

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

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。

设置基本信息 > 选择用户 > 选择资产 > 选择账号 > 5 设置访问控制 > 6 完成

主机访问控制 主机高危命令 数据库访问控制

已选 Linux 主机: 0

请选择模板

搜索模板名称
模板名称 禁止执行的命令
<input checked="" type="checkbox"/> [REDACTED] p [REDACTED]
<input checked="" type="checkbox"/> [REDACTED] u [REDACTED]
<input type="checkbox"/> [REDACTED] h [REDACTED]
<input type="checkbox"/> [REDACTED] s [REDACTED]
<input type="checkbox"/> [REDACTED] c [REDACTED]
<input type="checkbox"/> [REDACTED] v [REDACTED]

已选择 (2)

模板名称	禁止执行的命令
[REDACTED]	p [REDACTED]
[REDACTED]	u [REDACTED]

上一步：选择账号 下一步：完成

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，将被运维安全中心（堡垒机）拦截。

文件传输控制

最近更新时间：2025-08-29 09:44:31

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运维安全中心（堡垒机）配置文件传输权限。

操作步骤

1. 登录 [运维安全中心（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。

The screenshot shows the 'Host Access Control' tab selected in a six-step configuration process. Under 'RDP Disk Mapping', 'Upload files' is checked and 'Download files' is unchecked. Under 'Clipboard', 'Upload files' and 'Upward text' are checked, while 'Download files' and 'Downward text' are unchecked. Under 'RZSZ', 'Upload files' is checked and 'Download files' is unchecked. Under 'SFTP Options', 'Upload files' is checked and 'Delete files' is unchecked. At the bottom, there are 'Previous Step: Select Account' and 'Next Step: Complete' buttons.

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 > 完成

配置项	配置详情
权限名称	...
有效期	长期有效
用户	n ... o
用户组	未选择
资产	可用 ... t)
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	搜索权限名称				
<input type="checkbox"/> 权限名称	状态	用户	用户组	资产	资产组	账号	操作
<input type="checkbox"/> ...	已生效						编辑 删除
<input type="checkbox"/> ...	已生效	1 ...					编辑 删除

安全事故追溯

最近更新时间：2024-12-11 16:45:44

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 [运维安全中心（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。

The screenshot shows the 'Character Session Audit' page. At the top, there are date range filters ('近7天', '近14天', '近30天') and a search bar ('2024-11-19 ~ 2024-11-25'). Below the search bar is a dropdown menu titled '请选择属性进行过滤' (Select attribute for filtering) containing fields: '用户名', '姓名', '资产名称', '外部IP', '内部IP', '来源IP', and '资产账号'. A red box highlights this dropdown. To the right of the dropdown is a table header with columns: '操作命令/阻断...', '状态', and '操作'. At the bottom right of the table area is a pagination control with '20 条 / 页' and a page number '1 / 1 页'.

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。

The screenshot shows the 'Session Playback' page. At the top, there are date range filters ('近7天', '近14天', '近30天') and a search bar ('2023-10-13 ~ 2023-10-19'). Below the search bar is a table header with columns: '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', and '操作'. Two rows of session data are listed. The second row has a '回放' (Playback) button to its right, which is highlighted with a red box.

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

搜索命令 

	MiB Mem : 3880160 total, 2957636 free, 209236 used, 713288 buff/cache										
	MiB Swap: 0 total, 0 free, 0 used. 3426916 avail Mem										
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
ls	7	root	rt	0	0	0	0	S	0.0	0.0	0:01.07 migration/0
ls	8	root	20	0	0	0	0	S	0.0	0.0	0:00.00 rcu_bh
ls	9	root	20	0	0	0	0	S	0.0	0.0	0:27.68 rcu_sched
ls	10	root	0	-20	0	0	0	S	0.0	0.0	0:00.00 lru-add-drain
ls	11	root	rt	0	0	0	0	S	0.0	0.0	0:00.64 watchdog/0
ls	12	root	rt	0	0	0	0	S	0.0	0.0	0:00.46 watchdog/1
ls	13	root	rt	0	0	0	0	S	0.0	0.0	0:01.08 migration/1
ls	14	root	20	0	0	0	0	S	0.0	0.0	0:01.05 ksoftirqd/1
ls	16	root	0	-20	0	0	0	S	0.0	0.0	0:00.00 kworker/1:0H
ls	18	root	20	0	0	0	0	S	0.0	0.0	0:00.00 kdevtmpfs
ls	19	root	0	-20	0	0	0	S	0.0	0.0	0:00.00 netns
ls	20	root	20	0	0	0	0	S	0.0	0.0	0:00.06 khungtaskd
ls	21	root	0	-20	0	0	0	S	0.0	0.0	0:00.00 writeback
ls	22	root	0	-20	0	0	0	S	0.0	0.0	0:00.00 kintegrityd
ls	23	root	0	-20	0	0	0	S	0.0	0.0	0:00.00 bioset
ls	24	root	0	-20	0	0	0	S	0.0	0.0	0:00.00 bioset
ls	25	root	0	-20	0	0	0	S	0.0	0.0	0:00.00 bioset
ls	26	root	0	-20	0	0	0	S	0.0	0.0	0:00.00 kblockd
ls	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：2025-08-29 09:44:31

操作场景

当资产（例如 CVM）分布在多个 VPC 时，需要通过运维安全中心（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. 进入 [运维安全中心（堡垒机）控制台](#)，在左侧导航选择开通服务。
2. 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。

The screenshot shows a table with a single row of data. The columns are: 资源ID/名称 (Resource ID/Name), 状态 (Status), IP, 剩余授权数 (Remaining Licenses), 带宽 (Bandwidth), 到期时间 (Expiration Time), 地域 (Region), VPC ID/名称 (VPC ID/Name), and 操作 (Operations). The status is '已开通' (Enabled). The IP column shows '(外) (内)' (External/Internal). The remaining licenses are 7/50. The bandwidth is 16Mbps. The expiration time is 2023-11-17. The region is Guangzhou (广州). The VPC ID/Name is partially visible. The operations column includes '续费' (Renew), '升级' (Upgrade), and '更多' (More).

3. 购买完成之后，返回开通服务页面，找到新购买的运维安全中心（堡垒机）服务，单击开通。

The screenshot shows a table with a single row of data. The columns are: 资源ID/名称 (Resource ID/Name), 状态 (Status), IP, 剩余授权数 (Remaining Licenses), 带宽 (Bandwidth), 到期时间 (Expiration Time), 地域 (Region), VPC ID/名称 (VPC ID/Name), and 操作 (Operations). The status is '未开通' (Not Enabled). The IP column is blank. The remaining licenses are 0/50. The bandwidth is 8Mbps. The expiration time is 2023-11-13. The region is blank. The VPC ID/Name is blank. The operations column includes '开通' (Activate) which is highlighted with a red box, '续费' (Renew), '升级' (Upgrade), and '更多' (More).

4. 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：请选择运维安全中心（堡垒机）纳管的资产的所属地域，可选择广州、上海、南京、北京、成都、重庆、西安。
- VPC：请选择需要运维安全中心（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。

资源ID * ▼

资产授权数 50 到期时间 2023-11-13

地域 * 华南地区 华东地区 华北地区 西南地区 西北地区

广州

上海

南京

北京

成都

重庆

西安

请选择需要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

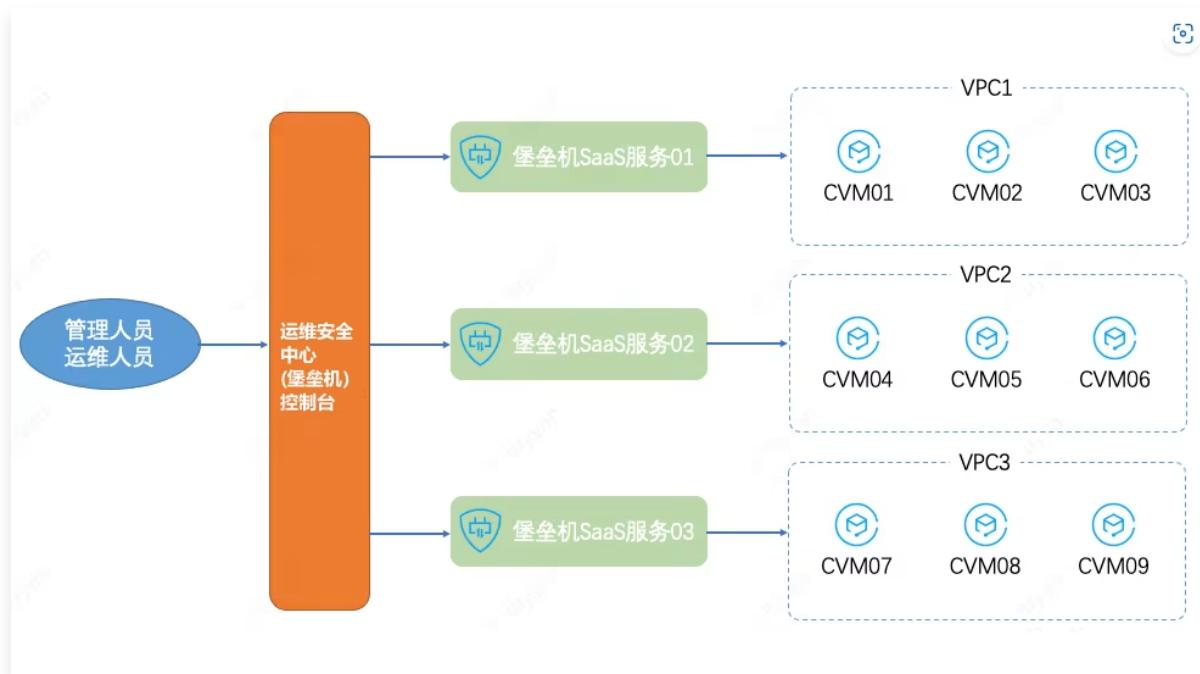
子网 * ▼

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。

确定 取消

5. 开通多个服务之后，不同 VPC 的资产可由对应 VPC 内的运维安全中心（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 运维安全中心（堡垒机）的 [快速入门](#)。
- 除开通运维安全中心（堡垒机）服务外，还可以通过 [网络域](#)、[对等连接](#)、[云联网](#) 等方式来打通运维安全中心（堡垒机）与 CVM 之间的网络。

等保实践教程

等保二级

最近更新时间：2025-09-03 11:25:11

为助力企业等保合规，本文为您介绍运维安全中心（堡垒机）各能力与等保二级相关条款的对应关系，以便有针对性地提供佐证材料。

前提条件

已购买[运维安全中心（堡垒机）](#)，并完成了[首次登录配置](#)和[入门操作](#)。

安全区域边界

安全审计

a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

本条款主要考察：是否有进行安全审计。运维安全中心（堡垒机）支持对云服务器运维操作进行监控和审计。

1. 登录[运维安全中心（堡垒机）控制台](#)。
2. 在左侧导航栏中，选择[操作审计 > 会话记录](#)，进入会话记录页面。
3. 在会话记录页面，可查看用户对服务器、数据库、Web 应用运维会话记录。

资产IP	来源IP	资产类型	资产账号	开始时间/结束时间	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
...	...	Linux	...	2025-08-28 18:07:01 2025-08-28 20:49:44	...	2小时42分钟42秒 227.98KB	20 0	结束	详情 回放
...	...	Linux	...	2025-08-28 17:17:26 2025-08-28 17:17:36	...	10秒 2.32KB	6 0	结束	详情 回放
...	...	Linux	...	2025-08-28 15:34:36 2025-08-28 20:35:38	...	5小时1分钟2秒 7.09KB	4 0	结束	详情 回放

4. 在审计管理页面，单击[详情](#)，进入会话详情页面可查看运维会话详细信息。

会话详情 ir 2

会话信息 运维操作 文件操作

资产IP	1 (外) / [REDACTED] (内)	资产账号
资产名称	[REDACTED]	用户
来源IP	● 开始时间 2023-10-10 10:52	
	● 结束时间 2023-10-10 10:28	
会话时长	36秒	
会话大小	0KB	

5. 在会话详情页面，单击运维操作，可查看用户对云服务器的操作命令记录。

会话详情 ins-

会话信息 运维操作 文件操作

请输入操作命令

操作时间	操作命令	状态	操作
2021-11-16 17:22:56	ls	• 已执行	回放
2021-11-16 17:22:57	cd	• 已阻断	回放
2021-11-16 17:22:58	cd	• 已阻断	回放
2021-11-16 17:22:58	cd	• 已阻断	回放
2021-11-16 17:23:00	ps	• 已执行	回放
2021-11-16 17:23:02	ps	• 已执行	回放

b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

本条款主要考察：日志是否按照要求进行记录。

1. 登录 [运维安全中心（堡垒机）控制台](#)，在左侧导航选择[审计管理](#)，进入运维审计页面。
2. 在审计管理页面，可查看用户对服务器、数据库运维会话记录，在会话审计当中记录了开始时间/结束时间（日期和时间）、用户名/姓名（用户）、会话类型（事件类型）、状态（事件状态）。

会话记录 普通区

字符会话 图形会话 文件传输会话 数据库会话 Web应用会话 运维任务执行记录

资产IP	来源IP	资产类型	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	操作命令/阻断命令	状态	操作
[REDACTED]	[REDACTED]	Linux	[REDACTED]	2025-08-28 18:07:01 2025-08-28 20:49:44	[REDACTED]	[REDACTED]	2小时42分钟42秒 227.98KB	20 0	结束	详情 回放
[REDACTED]	[REDACTED]	Linux	[REDACTED]	2025-08-28 17:17:26 2025-08-28 17:17:36	[REDACTED]	[REDACTED]	10秒 2.32KB	6 0	结束	详情 回放
[REDACTED]	[REDACTED]	Linux	[REDACTED]	2025-08-28 15:34:36 2025-08-28 20:35:38	[REDACTED]	[REDACTED]	5小时1分钟2秒 7.09KB	4 0	结束	详情 回放

c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；

本条款主要考察：日志是否有备份。

运维安全中心（堡垒机）审计日志存储在腾讯云 Elasticsearch Service 中，数据实时保存为2份，审计日志历史数据可保存180天。

Elasticsearch Service 提供了多可用区部署方案，可保证在单可用区网络、电力等不可抗力故障下不停服，保障数据在意外情况下丢失时快速恢复。此外还有为保障集群稳定而进行的内核优化等策略，可以全方位地保障数据的安全和服务的稳定。

安全计算环境

身份鉴别

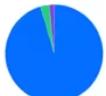
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

本条款主要考察如下三点：

- 是否对登录用户进行身份识别和鉴别

1.1 登录 [运维安全中心（堡垒机）控制台](#)，获取运维页面访问地址。

概览

本月运维安全风险	资产	用户	帮助
 未绑定堡垒机服务资产数 503	 ● Linux: 506 ● Windows: 16 ● MySQL: 8	 用户总数 42 在线用户数 0	运维页面 操作指引 已购买服务: 2个 购买 已开通服务: 2个 开通

1.2 使用浏览器访问运维页面，证明需要对用户身份进行鉴别之后才可正常使用产品功能。



- 身份标识是否具有唯一性

- 1.1 登录 [运维安全中心（堡垒机）控制台](#)，在左侧导航选择**用户管理 > 用户**，进入用户页面。
- 1.2 在用户页面，单击**新建用户**，尝试输入重复的用户名和手机号，用户无法新建成功。

新建用户 X

基本信息 [高级选项](#)

用户名 *	<input type="text" value=""/>	姓名 *	<input type="text" value="请输入姓名"/>
用户名重复			
认证方式 *	<input type="text" value="本地"/>	手机号 *	<input type="text" value="+86"/> <input type="text" value="请输入手机号"/>
邮箱 *	<input type="text" value="请输入邮箱"/>	用户组	<input type="text" value="请选择用户组"/>

确定 **取消**

新建用户

基本信息 高级选项

用户名 *	测试	姓名 *	请输入姓名
认证方式 *	本地	手机号 *	+86 1 [REDACTED] ! 手机号重复
邮箱 *	请输入邮箱	用户组	请选择用户组

确定 **取消**

● 身份鉴别信息是否具有复杂度要求并定期更换

- 1.1 登录 [运维安全中心（堡垒机）控制台](#)，在左侧导航选择系统设置 > 本地认证，进入本地认证页面。
- 1.2 在本地认证页面，查看本地认证的密码长度、复杂度和有效期要求（提前设置为强密码要求）。

系统设置 普通区

白名单设置 登录安全设置 **本地认证** 双因子认证 LDAP 日志投递 日志外发 资产自动同步

密码最小长度	12
密码复杂度	不限制
密码有效期	90天 ①
历史密码相同检查	3 ①

b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；本条款主要考察：是否有登录失败处理能力，以及对登录失败的处理措施。

1. 登录 [运维安全中心（堡垒机）控制台](#)，在左侧导航选择系统设置 > 登录安全设置，进入登录安全设置页面。
2. 在登录安全设置页面，查看密码错误锁定和锁定时长。

系统设置 普通区 ▾

白名单设置 登录安全设置 本地认证 双因子认证 LDAP 日志投递 日志外发 资产自动同步

Web闲置超时	55 分钟
密码错误锁定	5 次
锁定时长	10 分钟

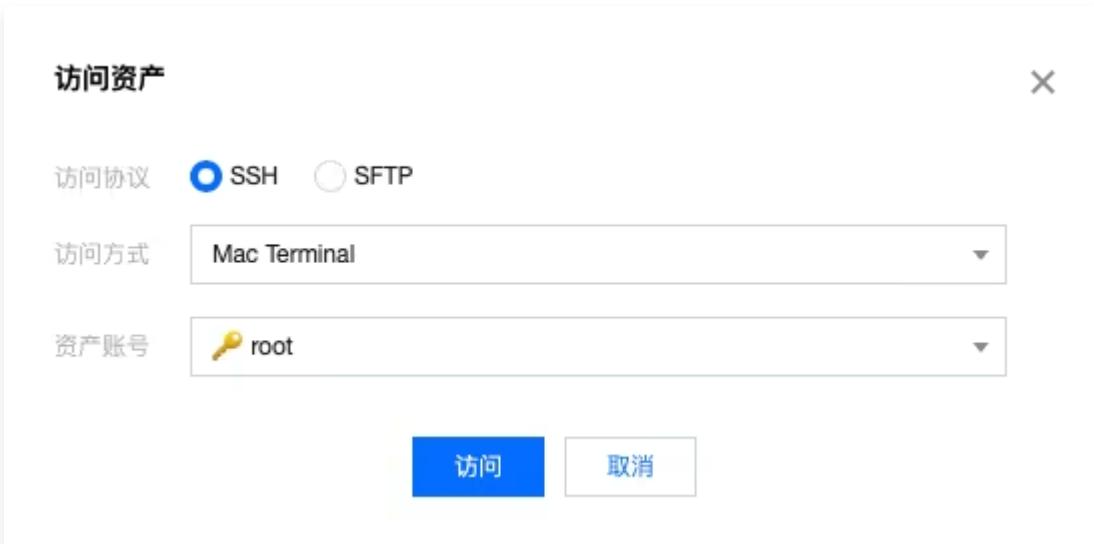
c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。

本条款主要考察：是否采用加密的协议进行远程管理。

1. 登录 运维安全中心（堡垒机）控制台，获取运维页面访问地址。



2. 使用浏览器访问运维页面，登录成功之后，访问一台 Linux 主机，在访问资产弹窗当中，可查看访问协议为 SSH 或 SFTP，均为加密的协议。



访问控制

a) 应对登录的用户分配账户和权限；

本条款主要考察：

- 是否给登录的用户分配账户

1.1 登录 运维安全中心（堡垒机）控制台，在左侧导航选择用户管理 > 用户，进入用户页面。

1.2 在用户页面，查看用户信息，证明给用户分配了账户。

The screenshot shows the 'User' tab selected in the navigation bar. Below it is a search bar labeled '搜索用户名/姓名'. There are several buttons: '新建用户' (Create New User), '导入用户' (Import User), '导出用户' (Export User), '编辑访问时间限制' (Edit Access Time Limit), and '删除' (Delete). A table lists two users:

用户名	姓名	状态	手机号	认证方式	邮箱	用户组	操作
2		正常	+86 4...	LDAP			编辑 重置 权限 删除
5		正常	+86 1...	LDAP			编辑 重置 权限 删除

- 是否给登录的用户分配权限

1.1 登录 [运维安全中心（堡垒机）控制台](#)，在左侧导航选择权限管理 > 访问权限，进入访问权限页面。

1.2 在访问权限页面，查看用户权限分配情况。

The screenshot shows the 'Access Permissions' tab selected. Below it is a search bar labeled '搜索权限名称'. There are buttons: '新建访问权限' (Create New Access Permission) and '删除' (Delete). A table lists two permission entries:

权限名称	状态	用户	用户组	资产	资产组	账号	操作
访...	已生效						编辑 删除
	已生效						编辑 删除

b) 应重命名或删除默认账户，修改默认账户的默认口令；

本条款主要考察：

- 是否有默认账户

1.1 登录 [运维安全中心（堡垒机）控制台](#)，在左侧导航选择用户管理 > 用户，进入用户页面。

1.2 在用户页面，查看用户信息，可尝试搜索 admin、root、sysadmin、super 等用户名，证明系统内无此默认用户。

The screenshot shows the 'User' tab selected. Below it is a search bar labeled '搜索用户名/姓名' with a red box around it. There are several buttons: '新建用户' (Create New User), '导入用户' (Import User), '导出用户' (Export User), '编辑访问时间限制' (Edit Access Time Limit), and '删除' (Delete). A table lists two users:

用户名	姓名	状态	手机号	认证方式	邮箱	用户组	操作
2		正常	+86 4...	LDAP			编辑 重置 权限 删除
5		正常	+86 1...	LDAP			编辑 重置 权限 删除

- 是否有默认口令

使用浏览器访问运维页面，单击账号激活，在激活页面，用户需要获取短信验证码、并自己设置登录密码，证明

用户无默认口令。



c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；

本条款主要考察：账户过期之后，能否继续使用。

说明

请提前准备一个已经到期的用户。

1. 登录 **运维安全中心（堡垒机）控制台**，在左侧导航选择**用户管理 > 用户**，进入用户页面。

2. 在用户页面，单击用户信息，查看一个过期用户的用户信息，确认用户已过有效期。



3. 使用浏览器访问运维页面，使用已过期的用户尝试进行登录，此时用户无法登录，并且页面提示“**用户不在有效期内**”，证明过期的用户无法继续使用。

d) 应授予管理用户所需的最小权限，实现管理用户的权限分离；

本条款主要考察：是否给用户分配了最小权限。

1. 登录 [运维安全中心（堡垒机）控制台](#)，在左侧导航选择**权限管理 > 访问权限**，进入访问权限页面。
2. 在访问权限页面，单击**新建访问权限**，在第5步可设置文件传输的最小权限、在第6步可以设置命令操作的最小权限。

The screenshot shows the 'New Access Permission' wizard at step 5: '设置访问操作' (Set Transfer Operation). The top navigation bar shows steps 1 through 7. The page lists several operations with checkboxes:

- 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

At the bottom are two buttons: '上一步：选择账号' (Previous Step: Select Account) and '下一步：选择高危命令模板' (Next Step: Select High-risk Command Template).

新建访问权限

The screenshot shows the 6th step of a 7-step wizard titled 'Create Access Permission'. The title bar includes icons for previous steps and the current step. The main area is titled 'Select High-risk Command Template' and contains a table with the following data:

Template Name	Description
7777	禁止执行的命令
新建	222
777	top
测试高危命令	whoami
xss	rm * shutdown *
高危	<script>alert('XSS');</script> <script>reboot*</script> <script>alert(123);</script>

On the right, there's a sidebar titled 'Selected (0)' and a vertical scroll bar. At the bottom, there are two buttons: 'Previous Step: Set Access Operation' and 'Next Step: Complete'.

安全审计

a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

本条款主要考察：是否启用了审计功能，是否可以审计用户行为。

1. 登录 **运维安全中心（堡垒机）控制台**，在左侧导航选择**审计管理 > 运维审计**，进入运维审计页面。
2. 在运维审计页面，可查看用户对服务器、数据库的操作日志。

The screenshot shows the 'Operations Audit' page with a table of audit logs. The columns include: Asset IP, Source IP, Asset Account, Start Time/End Time, Asset Name, User Name/Name, Session Duration/Session Size, Status, and Operation. The status column shows 'Completed' and the operation column shows 'Audit Log'.

3. 单击日志检索，进入日志搜索页面，可查看用户对运维安全中心（堡垒机）的操作日志。

The screenshot shows the 'Log Search' page with a table of audit logs. The columns include: Time, User Name/Name, Source IP, Login Method, and Login Result. The log entries show multiple failed attempts to log in via web page.

- b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

本条款主要考察：日志是否按照要求进行记录。

1. 登录 [运维安全中心（堡垒机）控制台](#)，在左侧导航选择[审计管理 > 日志检索 > 操作日志](#)，进入操作日志页面。
2. 在操作日志页面，可查看用户对运维安全中心（堡垒机）的操作日志详细内容，包含时间、用户、事件和结果，证明符合要求。

日志检索

登录日志 操作日志 审计日志

近7天 近14天 近30天 2021-11-19 ~ 2021-11-25

选择日志属性进行过滤

时间	用户名/姓名	来源IP	具体操作	操作结果
2021-11-25 10:30:43	10管:	9.2	修改用户	成功
2021-11-23 20:19:35	tes cw	120	激活OTP	成功
2021-11-23 20:16:34	10管:	9.7	重置用户密码	成功
2021-11-19 16:41:10	10管:	9.2	修改登录设置	成功
2021-11-19 14:50:17	10管:	9.2	修改密码强度设置	成功

共 5 条 20 条 / 页 1 / 1 页



其他

运维安全中心（堡垒机）用户密码的加密方式：采用 BCrypt 算法加密保存。

等保三级

最近更新时间：2024-05-29 17:00:44

为助力企业等保合规，本文为您介绍运维安全中心（堡垒机）各能力与等保三级相关条款的对应关系，以便有针对性地提供佐证材料。

前提条件

已购买[运维安全中心（堡垒机）](#)，并完成了[首次登录配置](#)和[入门操作](#)。

安全区域边界

安全审计

a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

本条款主要考察：是否有进行安全审计。运维安全中心（堡垒机）支持对云服务器运维操作进行监控和审计。

1. 登录[运维安全中心（堡垒机）控制台](#)，在左侧导航选择[审计管理](#)，进入审计管理页面。
2. 在审计管理页面，可查看用户对服务器、数据库运维会话记录。

The screenshot shows the Audit Management interface. At the top, there are tabs for '字符会话' (Character Session), '图形会话' (Graphic Session) [selected], '文件传输' (File Transfer), '数据库' (Database), '运维任务' (Operations and Maintenance Tasks), and '风险事件' (Risk Events). Below the tabs is a search bar with filters for time periods: '近7天' (Last 7 days), '近14天' (Last 14 days), and '近30天' (Last 30 days). A date range selector shows '2023-10-13 ~ 2023-10-19'. To the right is a search input and a refresh button. The main area displays a table of audit logs:

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
[REDACTED] (外) (内)	1 [REDACTED]	[REDACTED]	2023-10-13 15:52 2023-10-13 15:28	[REDACTED]	[REDACTED]	36秒 0KB	结束	详情
[REDACTED] (外) (内)	1 [REDACTED]	[REDACTED]	2023-10-13 15:59 2023-10-13 16:02	[REDACTED]	[REDACTED]	10小时32分钟2秒 1.55MB	结束	详情 回放

3. 在运维审计页面，单击[详情](#)，进入会话详情页面可查看运维会话详细信息。

会话详情 ir 2

会话信息 运维操作 文件操作

资产IP	1 (外) / [REDACTED] (内)	资产账号
资产名称	[REDACTED]	用户
来源IP	[REDACTED]	● 开始时间 2023-10-28 10:52
		● 结束时间 2023-10-28 10:28
会话时长	36秒	
会话大小	0KB	

4. 在会话详情页面，单击运维操作，可查看用户对云服务器的操作命令记录。

会话详情 ins- X

会话信息 运维操作 文件操作

请输入操作命令

操作时间	操作命令	状态	操作
2021-11-16 17:22:56	ls	• 已执行	回放
2021-11-16 17:22:57	cd	• 已阻断	回放
2021-11-16 17:22:58	cd	• 已阻断	回放
2021-11-16 17:22:58	cd	• 已阻断	回放
2021-11-16 17:23:00	ps	• 已执行	回放
2021-11-16 17:23:02	ps	• 已执行	回放

b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

本条款主要考察：日志是否按照要求进行记录。

1. 登录 [运维安全中心（堡垒机）控制台](#)，在左侧导航选择[审计管理](#)，进入审计管理页面。
2. 在审计管理页面，可查看用户对服务器、数据库运维会话记录，在会话审计当中记录了开始时间/结束时间（日期和时间）、用户名/姓名（用户）、会话类型（事件类型）、状态（事件状态）。

字符会话	图形会话	文件传输	数据库	运维任务	风险事件	事件类型
近7天	近14天	近30天	2023-09-20 ~ 2023-10-19			
日期和时间	用户	事件状态				
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		
2023-09-20 17:49:08 2023-09-20 17:53:31	4分钟23秒 619.74KB	结束	详情 回放			
2023-09-20 17:48:17 2023-09-20 17:49:00	43秒 122.06KB	结束	详情 回放			

c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；

本条款主要考察：日志是否有备份。

运维安全中心（堡垒机）审计日志存储在腾讯云 Elasticsearch Service 中，数据实时保存为2份，审计日志历史数据可保存180天；Elasticsearch Service 提供了多可用区部署方案，可保证在单可用区网络、电力等不可抗力故障下不停服，保障数据在意外情况下丢失时快速恢复。此外还有为保障集群稳定而进行的内核优化等策略，可以全方位地保障数据的安全和服务的稳定。

d) 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。

本条款主要考察：是否能够对远程访问的用户行为进行审计与数据分析。

1. 登录 [运维安全中心（堡垒机）控制台](#)，在左侧导航选择[审计管理](#)，进入审计管理页面。

2. 在审计管理页面，可查看用户对服务器、数据库运维会话记录，支持存储6个月的日志并提供日志分析能力。

字符会话	图形会话	文件传输	数据库	运维任务	风险事件		
近7天	近14天	近30天	2023-04-23 ~ 2023-10-19				
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		
1 (外) (内)	1	8	2023-10-28 2023-10-28	52	36秒 0KB	结束	详情
1 (外) (内)	1	8	2023-10-02 2023-10-02	59	10小时32分 钟2秒 1.55MB	结束	详情 回放

安全计算环境

身份鉴别

a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

本条款主要考察如下三点：

- 是否对登录用户进行身份识别和鉴别

1.1 登录 [运维安全中心（堡垒机）控制台](#)，获取运维页面访问地址。



1.2 使用浏览器访问运维页面，证明需要对用户身份进行鉴别之后才可正常使用产品功能。



● 身份标识是否具有唯一性

1.1 登录 [运维安全中心（堡垒机）控制台](#)，在左侧导航选择**用户管理 > 用户**，进入用户页面。

1.2 在用户页面，单击**新建用户**，尝试输入重复的用户名和手机号，用户无法新建成功。

新建用户



基本信息

高级选项

用户名 *



姓名 *

请输入姓名

用户名重复

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

新建用户



基本信息

高级选项

用户名 *

测试

姓名 *

请输入姓名

认证方式 *

本地

手机号 *

+86 1

手机号重复

邮箱 *

请输入邮箱

用户组

请选择用户组

确定

取消

● 身份鉴别信息是否具有复杂度要求并定期更换

1.1 登录 [运维安全中心（堡垒机）控制台](#)，在左侧导航选择系统设置 > 本地认证，进入本地认证页面。

1.2 在本地认证页面，查看本地认证的密码长度、复杂度和有效期要求（提前设置为强密码要求）。

系统设置 普通区 ▾

- [白名单设置](#)
- [登录安全设置](#)
- [本地认证](#) 本地认证
- [双因子认证](#)
- [LDAP](#)
- [日志投递](#)
- [日志外发](#)
- [资产自动同步](#)

密码最小长度	12
密码复杂度	不限制
密码有效期	90天 ⓘ
历史密码相同检查	3 ⓘ

b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；本条款主要考察：是否有登录失败处理能力，以及对登录失败的处理措施。

1. 登录 [运维安全中心（堡垒机）控制台](#)，在左侧导航选择 [系统设置 > 登录安全设置](#)，进入登录安全设置页面。
2. 在登录安全设置页面，查看密码错误锁定和锁定时长。

系统设置 普通区 ▾

- [白名单设置](#)
- [登录安全设置](#) 登录安全设置
- [本地认证](#)
- [双因子认证](#)
- [LDAP](#)
- [日志投递](#)
- [日志外发](#)
- [资产自动同步](#)

Web闲置超时	55 分钟
密码错误锁定	5 次
锁定时长	10 分钟

c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。

本条款主要考察：是否采用加密的协议进行远程管理。

1. 登录 [运维安全中心（堡垒机）控制台](#)，获取运维页面访问地址。

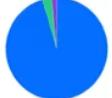
概览

本月运维安全风险



未绑定堡垒机服务资产数
503

资产



Linux: 506
Windows: 16
MySQL: 8

用户



用户总数
42
在线用户数
0

帮助

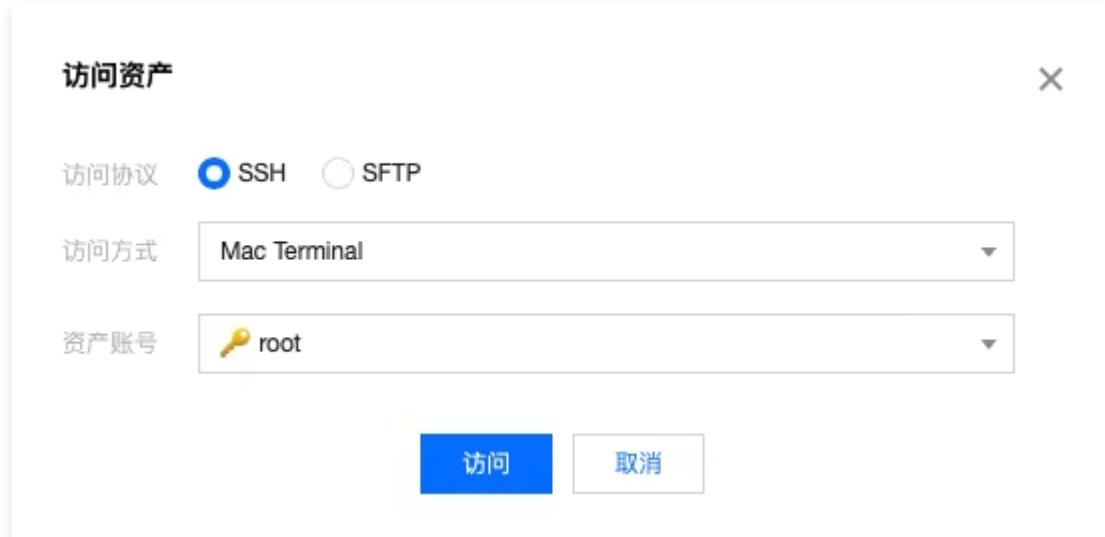
运维页面：<https://bh.cloud.tencent.com/login.html?appTag=fp>

操作指引：<https://cloud.tencent.com/document/product/1025/55182>

已购买服务：2个 [购买](#)

已开通服务：2个 [开通](#)

2. 使用浏览器访问运维页面，登录成功之后，访问一台 Linux 主机，在访问资产弹窗当中，可查看访问协议为 SSH 或 SFTP，均为加密的协议。



d) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现

本条款主要考察：是否采用双因子进行身份鉴别。

1. 登录 [运维安全中心（堡垒机）控制台](#)，在左侧导航选择系统设置 > 双因子认证，进入双因子认证页面。
2. 在双因子认证页面，查看双因子配置。

访问控制

a) 应对登录的用户分配账户和权限；

本条款主要考察：

- 是否给登录的用户分配账户

- 1.1 登录 [运维安全中心（堡垒机）控制台](#)，在左侧导航选择用户管理 > 用户，进入用户页面。
- 1.2 在用户页面，查看用户信息，证明给用户分配了账户。

- 是否给登录的用户分配权限

1.1 登录 [运维安全中心（堡垒机）控制台](#)，在左侧导航选择权限管理 > 访问权限，进入访问权限页面。

1.2 在访问权限页面，查看用户权限分配情况。

权限名称	状态	用户	用户组	资产	资产组	账号	操作
...访问...	已生效						编辑 删除
...	已生效						编辑 删除

b) 应重命名或删除默认账户，修改默认账户的默认口令；

本条款主要考察：

- 是否有默认账户

1.1 登录 [运维安全中心（堡垒机）控制台](#)，在左侧导航选择用户管理 > 用户，进入用户页面。

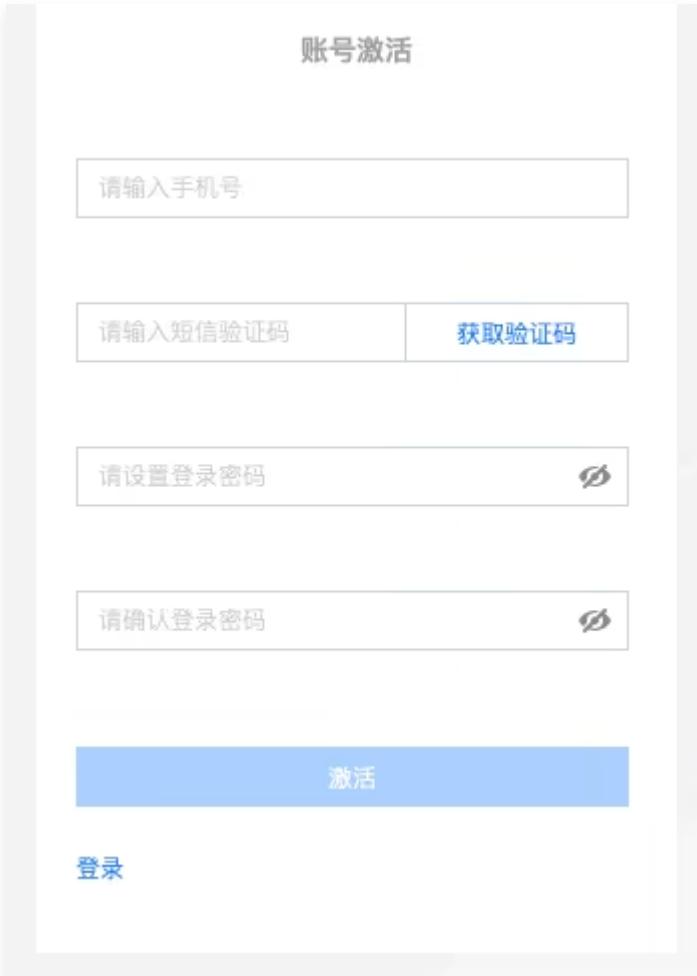
1.2 在用户页面，查看用户信息，可尝试搜索 admin、root、sysadmin、super 等用户名，证明系统内无此默认用户。

用户名	姓名	状态	手机号	认证方式	邮箱	用户组	操作
...2	...	正常	+86 ...4...	LDAP			编辑 重置 权限 删除
...3	...	正常	+86 1...3...	LDAP			编辑 重置 权限 删除

- 是否有默认口令

使用浏览器访问运维页面，单击账号激活，在激活页面，用户需要获取短信验证码、并自己设置登录密码，证明

用户无默认口令。



c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；

本条款主要考察：账户过期之后，能否继续使用。

说明

请提前准备一个已经到期的用户。

1. 登录 [运维安全中心（堡垒机）控制台](#)，在左侧导航选择 **用户管理 > 用户**，进入用户页面。

2. 在用户页面，单击用户信息，查看一个过期用户的用户信息，确认用户已过有效期。



3. 使用浏览器访问运维页面，使用已过期的用户尝试进行登录，此时用户无法登录，并且页面提示“**用户不在有效期内**”，证明过期的用户无法继续使用。

d) 应授予管理用户所需的最小权限，实现管理用户的权限分离；

本条款主要考察：是否给用户分配了最小权限。

1. 登录 **运维安全中心（堡垒机）控制台**，在左侧导航选择**权限管理 > 访问权限配置**，进入访问权限配置页面。
2. 在访问权限配置页面，单击**新建访问权限**，在第5步可设置文件传输的最小权限、在第6步可以设置命令操作的最小权限。

The screenshot shows the 'New Access Permission' configuration page. It displays a step-by-step process: 1. Set Permission Information, 2. Select User, 3. Select Asset, 4. Select Account, 5. Set Access Operation (highlighted in blue), 6. Select High-risk Command Template, and 7. Complete. Under step 5, there are sections for RDP mapping (RDP磁盘映射), RDP clipboard (RDP剪切板), RZSZ, and SFTP options. Each section has checkboxes for upload, download, and other file operations. At the bottom, there are 'Previous Step: Select Account' and 'Next Step: Select High-risk Command Template' buttons.

新建访问权限

设置权限信息 > 选择用户 > 选择资产 > 选择账号 > 设置访问操作 > 选择高危命令模板 > 完成

请选择模板

模板名称	描述	已选择 (0)
7777	禁止执行的命令	
新建	top	
777	whoami	
测试高危命令	rm * shutdown *	
xss	<script>alert('XSS');</script>	
高危	rm * reboot* <script>alert(123);</script>	

上一步：设置访问操作 下一步：完成

e) 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；

本条款主要考察：用户（主体）是否可以设置对资产（客体）的访问控制策略。

1. 登录 [运维安全中心（堡垒机）控制台](#)，在左侧导航选择权限管理 > 访问权限配置，进入访问权限配置页面。
2. 在访问权限配置页面，单击新建访问权限，证明可以配置访问控制策略。

新建访问权限

设置权限信息 > 选择用户 > 选择资产 > 选择账号 > 设置访问操作 > 选择高危命令模板 > 完成

用户 用户组

选择用户

用户名	姓名	手机	已选择 (0)
ch	ch	135	
cw	cw	158	
tes	tes	166	
as	qw	136	
tes	cw	187	
pe	pe	131	
vu	远... 远...	173...	

上一步：设置权限信息 下一步：选择资产

新建访问权限

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

资产 资产组

选择资产

搜索资产名/IP				已选择 (0)
ID/资产名	资产IP	地域	资产类型	
ins-gon	192.	广州	TencentOS Server 2.4	
ins-gon test	192.119.	广州	Windows Server 2008 R2 企业版 SP1 64位	
ins-gon	192.	广州	Debian 10.2 64位	
ins-gon	192.81.7	广州	CentOS 7.9 64位	
ins-				

上一步：选择用户 下一步：选择账号

安全审计

a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

本条款主要考察：是否启用了审计功能，是否可以审计用户行为。

1. 登录 [运维安全中心（堡垒机）控制台](#)，在左侧导航选择[审计管理 > 运维审计](#)，进入运维审计页面。
2. 在运维审计页面，可查看用户对服务器、数据库的操作日志。

运维审计

字符会话 图形会话 文件传输 数据库 运维任务

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
[REDACTED]	结束	详情 回放						
[REDACTED]	结束	详情 回放						

3. 单击日志检索，进入日志搜索页面，可查看用户对运维安全中心（堡垒机）的操作日志。

日志检索

登录日志 操作日志 审计日志

时间	用户名/姓名	来源IP	登录方式	登录结果
2021-11-26	[REDACTED]	[REDACTED]	web页面登录	失败
2021-11-26	[REDACTED]	[REDACTED]	web页面登录	失败
2021-11-26	[REDACTED]	[REDACTED]	web页面登录	失败
2021-11-26	[REDACTED]	[REDACTED]	web页面登录	失败

b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

本条款主要考察：日志是否按照要求进行记录。

1. 登录 [运维安全中心（堡垒机）控制台](#)，在左侧导航选择[审计管理 > 日志检索 > 操作日志](#)，进入操作日志页面。
2. 在操作日志页面，可查看用户对运维安全中心（堡垒机）的操作日志详细内容，包含时间、用户、事件和结果，证明符合要求。

The screenshot shows the 'Audit Log Search' interface. At the top, there are tabs for 'Log Search', 'Operation Log' (which is selected), and 'Audit Log'. Below the tabs are filters for time range ('Recent 7 days', 'Recent 14 days', 'Recent 30 days') and date ('2021-11-19 ~ 2021-11-25'). There is also a search bar and a filter button. The main area displays a table of audit logs with columns: Time, Username/Name, Source IP, Operation, and Result. The table contains five log entries from November 19 to November 25, 2021, detailing operations like modifying users, activating OTP, resetting passwords, changing login settings, and modifying password strength. At the bottom, it shows '5 items' and a pagination bar with page 1 of 1.

Time	Username/Name	Source IP	Operation	Result
2021-11-25 10:30:43	10管:	9.2	修改用户	成功
2021-11-23 20:19:35	tes cw	120	激活OTP	成功
2021-11-23 20:16:34	10 管:	9.7	重置用户密码	成功
2021-11-19 16:41:10	10 管:	9.2	修改登录设置	成功
2021-11-19 14:50:17	10 管:	9.2	修改密码强度设置	成功

其他

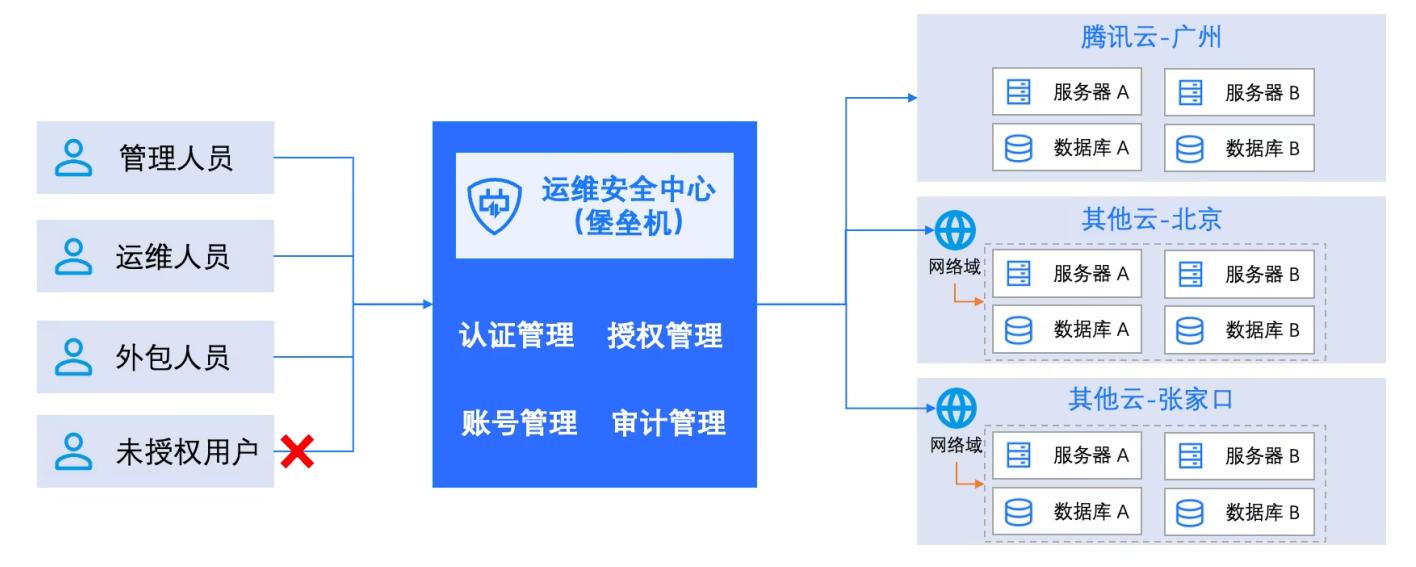
运维安全中心（堡垒机）用户密码的加密方式：采用 BCrypt 算法加密保存。

混合云管理实践教程

最近更新时间：2025-08-26 18:04:32

应用场景

当企业的资产分布在腾讯云和其他云平台时，每个云平台分布不同的资产，通过运维安全中心（堡垒机）可以帮助企业实现不同云平台的统一管理，确保只有经过授权的人员能够访问相应的资产。



混合云管理能力的优势在于：

- 统一管理：通过运维安全中心（堡垒机）提供统一运维入口，实现对所有网络环境资产的统一登录管理。
- 性价比高：相同网络环境中只需部署一台代理节点，无需独立部署堡垒机系统，降低部署和运营成本。
- 细粒度授权：支持基于用户、资产、账号、操作权限等维度进行细粒度授权，确保用户所拥有的权限是企业客户所需的访问资产、完成工作任务的最小化权限。

功能限制

- 网络域插件仅支持安装于 Linux 服务器。
- 安装网络域插件的服务器需配置公网 IP，或支持 NAT 转发方式出公网。

操作步骤

步骤1：购买网络域

1. 进入运维安全中心（堡垒机）控制台 [开通服务](#)，选择需要调整网络域的实例，单击实例右侧的更多 > 调整网络域。

开通服务 共通区

服务列表 网络域

搜索

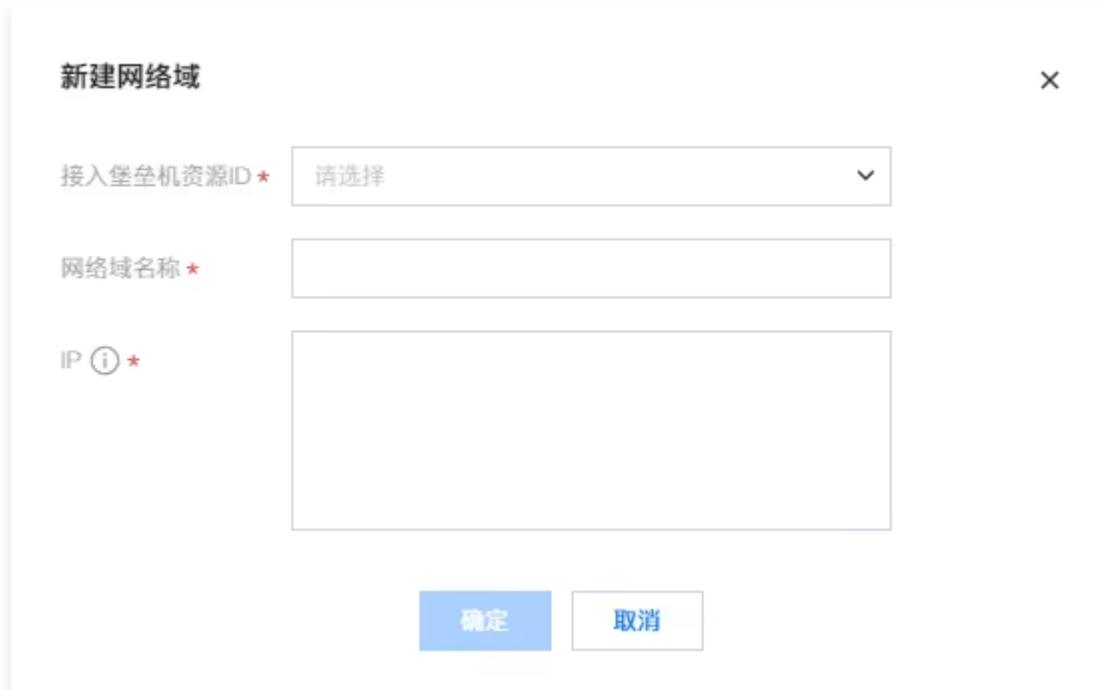
资源ID/名称	状态	IP	剩余授权数	剩余网络域数	带宽	到期时间	地域	VPC ID/名称	操作
[REDACTED]	已开通	[REDACTED]	46/50	0/0	10Mbps	2024-08-13	广州	[REDACTED]	续费 升级 更多 调整带宽 调整扩展包 调整网络域

2. 在调整网络域弹窗中，根据实际需求购买网络域数量，单击确定。



步骤2：配置网络域

1. 进入运维安全中心（堡垒机）控制台 [开通服务](#)，切换至网络域页面，单击新建。
2. 在新建网络域弹窗中，配置相关参数，单击确定。



参数名称	详情
接入堡垒机资源 ID	此网络域所属的运维安全中心（堡垒机）实例。当资产绑定到此运维安全中心（堡垒机）和此网络域时，运维安全中心（堡垒机）将通过此网络域的客户端发起连接。
网络域名称	网络域和资产中展示的名称。推荐使用良好的命名表达此网络域所属环境信息。
IP	允许网络域客户端（bh-gateway-client）连接到运维安全中心（堡垒机）实例的公网 IP 白名单。可配置单 IP 或者网段 CIDR，每行一条数据。多个 IP 需属于相同网络环境（统一 VPC 或局域网）。

步骤3：安装网络域

网络域配置好后，处于断开状态。需要下载安装脚本，部署到目标网络域内一台或多台可访问到运维安全中心（堡垒机）公网 IP 的服务器上。

说明：

一个网络域的客户端可安装在此网络域下的一台或多台服务器上提供服务，推荐至少配置两台服务器提供高可用。请确保客户端未安装在不同网络域下，避免部分服务器可访问，部分服务器不可访问的情况发生。

- 进入运维安全中心（堡垒机）控制台 [开通服务](#)，切换至网络域页面，选择需要进行安装操作的网络域，单击操作栏中的[下载安装脚本](#)。



- 上传安装脚本到服务器上后，执行脚本。

```
[root@VM-30-2-centos ~]# rm -f /var/log/tsecbh/bh_gateway.log
[root@VM-30-2-centos ~]# ll
total 12
-rw-r----- 1 root root 10104 May 11 10:51 net-nhmm1azp.sh
[root@VM-30-2-centos ~]# sh ./net-nhmm1azp.sh
package bh_gateway_client-1.0.1-7 is not installed
start install gateway client
--2024-05-11 10:52:54-- https://bh.cloud.tencent.com/download/bh_gateway_client-1.0.1-7.x86_64.rpm
Resolving bh.cloud.tencent.com (bh.cloud.tencent.com)... 183.47.103.73
Connecting to bh.cloud.tencent.com (bh.cloud.tencent.com)|183.47.103.73|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3515516 (3.4M) [application/x-redhat-package-manager]
Saving to: 'bh_gateway_client-1.0.1-7.x86_64.rpm'

100%[=====] 3,515,516 15.1MB/s in 0.2s

2024-05-11 10:52:54 (15.1 MB/s) - 'bh_gateway_client-1.0.1-7.x86_64.rpm' saved [3515516/3515516]

hash:6a773f912a4669054ce845025ba7988525e1686876bd112b5d65755c4afb3e
download and check success
package bhgatewayclient is not installed
old rpm not found. skip erase
Preparing... ################################################ [100%]
Updating / installing...
1:bh_gateway_client-1.0.1-7 ################################################ [100%]
install success
gateway client start success
[root@VM-30-2-centos ~]#
```

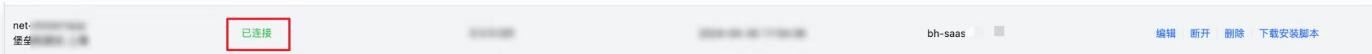
- 通过 `ps aux | grep bh_gateway_client` 检查是否正常启动。

```
[root@VM-30-2-centos ~]# ps aux | grep bh_gateway_client
root      28160  0.0  0.3 768008  7832 ?        Ssl  10:52   0:00 /usr/local/sbin/bh_gateway_client
```

4. 查看 `/var/log/tsecbh/bh_gateway.log` 日志文件，判断网络域服务器是否正常连接到运维安全中心（堡垒机）实例。

```
[root@VM-30-2-centos ~]# tail -f /var/log/tsecbh/bh_gateway.log
{"level":"INFO","ts":"2024-05-11T10:52:55.216+0800","caller":"cmd/main.go:90","msg":"local ip:192.168.30.2"}
{"level":"INFO","ts":"2024-05-11T10:52:55.359+0800","caller":"client/client.go:127","msg":"client auth success"}
```

5. 刷新控制台上网络域页面，该网络域状态应为已连接。



步骤4：配置资产

说明：

- 资产托管到运维安全中心（堡垒机）时，需要指定所属的网络域，若资产与运维安全中心（堡垒机）实例属于同一 VPC 下，请选择资产默认网络域。
- 资产属于其他网络域时，请根据实际情况配置网络域。

1. 进入运维安全中心（堡垒机）控制台 **资产管理**，选中需要配置网络域的主机资产，单击**托管资产**。

This screenshot shows the Asset Management interface. It lists several hosts with their asset IDs, IP addresses, and network domains. Two hosts have checkboxes checked. A red box highlights the '托管资产' (Assign Asset) button at the top of the list.

This screenshot shows the Asset Management interface again. Only one host's checkbox is checked. A red box highlights the '托管资产' (Assign Asset) button at the top of the list.

2. 在托管资产弹窗中，根据实际情况配置网络域，单击**确定**。

托管资产

X

资产数 1 (已有1台资产绑定选择的堡垒机服务)

堡垒机服务 *

1

▼

所属地域: 广州

所属VPC:

剩余授权数: 37/50

网络域 *

1

ain)

▼

确定

取消

3. 后续通过访问权限将资产授权给运维人员之后，运维人员即可正常访问，并且用户的所有操作行为都将被运维安全中心（堡垒机）记录。

暴露面收敛实践教程

最近更新时间：2025-08-19 15:19:31

为什么资产暴露面成为企业安全“致命伤”？

随着企业数字化转型加速，服务器、数据库等 IT 资产呈现指数级增长。黑客利用未备案的 IT 资产（例如未纳入管理的新服务器）、互联网直连高危端口（例如 SSH/RDP 端口暴露）等漏洞发起攻击，导致横移攻击、勒索病毒、数据泄露事件频发。

暴露面未收敛导致的典型问题如下：

- 爆破、横移风险提升：攻击者可直接从公网发现资产并通过爆破、钓鱼方式拿到资产访问权限。
- 权限管理失控：内外部人员均可绕过安全策略，通过 VPN 直接访问核心系统。
- 审计缺失：操作无审计记录、录像留存，安全事件无法追溯定位。

腾讯云运维安全中心（堡垒机）如何构建安全防护体系？

收敛攻击路径

对外仅开放运维安全中心（堡垒机）运维入口，将分散的服务器、数据库访问路径集中至运维安全中心（堡垒机），减少/关闭直接暴露在互联网的高危端口和服务，并通过安全组限制来源IP范围。

收敛资产账密

在运维安全中心（堡垒机）上托管资产账号密码，配置对应用户使用权限，防止直接接触明文账密，通过定期自动化改密，最小化资产账密泄漏面。同时基于运维安全中心（堡垒机）SaaS 化架构云原生能力自动同步云资产，防止绑定 AK 同步云资产方式导致的 AK 泄漏问题。

权限精细管控

基于 MFA 的强身份认证和最小权限原则，通过授权模型实现用户、资产、账号、权限管控，避免特权账号滥用，配置高危命令拦截策略，实时阻断 rm -rf、DROP TABLE 等高风险操作。

全链路溯源能力

完整记录包括用户、操作时间、命令执行、文件传输、数据库 SQL、会话录像等操作日志。

实战案例：企业资产如何实现安全闭环？

步骤一：将资产、账号托管至运维安全中心（堡垒机）

针对腾讯云资产（CVM 和数据库），可使用一键同步功能将资产信息同步至运维安全中心（堡垒机），并支持一键托管。针对非腾讯云资产，可手动进行添加并托管。

腾讯云资产托管

1. 登录 [运维安全中心（堡垒机）控制台](#)。
2. 在左侧导航栏中，选择资产管理 > 主机资产/数据库资产。
3. 在资产列表，单击同步资产，系统将自动同步主机资产。

The screenshot shows the 'Asset Management' interface under the 'Host Asset' tab. On the left sidebar, 'Asset Management' is selected. In the main area, there is a 'Sync Assets' button highlighted with a red box. Below it is a table listing assets with columns for Asset ID/Name, Asset IP, Network, Managed Status, Managed Host, Operation System, Department, and Operations.

4. 资产同步完成之后，选择未绑定运维安全中心（堡垒机）服务的主机，单击托管资产。即可完成资产的托管。

The screenshot shows the same 'Asset Management' interface after synchronization. A specific host asset's 'Managed Status' switch is highlighted with a red box, indicating it has been successfully managed by the堡垒机 service.

5. 在资产管理页，选择已绑定的目标资产，单击账号。

The screenshot shows the 'Asset Management' interface again. The 'Accounts' button at the bottom right of the table is highlighted with a red box.

6. 在账号管理窗口，单击添加资产账号。在添加资产账号窗口，配置账号名后，单击确定，即可保存。

The screenshot shows the 'Account Management' dialog box. The 'Add Asset Account' button at the top left is highlighted with a red box. The dialog includes fields for 'Asset Account' and 'Password', and a search bar at the top right.

7. 在账号管理窗口，添加资产已有的账号密码，单击对应账号的设置，弹出设置密码窗口。

The screenshot shows the 'Account Management' interface. At the top, there are buttons for 'Add Asset Account' (highlighted with a red box) and 'Delete'. A search bar is on the right. Below, a table lists accounts: 't' (unchecked) and '1' (unchecked). For account 't', there are buttons for 'Password' (disabled), 'Unmanaged Password' (checked), and 'Set' (highlighted with a red box). For account '1', there are buttons for 'Managed Password' (disabled), 'Set' (disabled), and 'Clear'. At the bottom, it says '共 2 条' (2 items) and has a page navigation section.

8. 在设置密码窗口，填写密码信息，单击确定，即可实现运维安全中心（堡垒机）上托管资产账号密码信息。

说明：

Linux 主机还支持设置密钥。

The screenshot shows the 'Account Management' interface. The 'Add Asset Account' button is highlighted with a red box. The table lists accounts: 'work3', 'work2', 'work1', and 'root'. For each account, there are sections for 'Password' and 'Private Key'. For 'root', the 'Password' section is highlighted with a red box, showing 'Unmanaged Password' (checked), 'Set' (disabled), and 'Clear' (disabled). The 'Private Key' section for 'root' shows 'Managed Private Key' (disabled), 'Set' (disabled), and 'Clear' (highlighted with a red box).

步骤二：确认运维安全中心（堡垒机）IP信息

进入运维安全中心（堡垒机）开通服务页面查看运维安全中心（堡垒机）内网 IP 信息，运维安全中心（堡垒机）将使用内网 IP 访问目标设备。

1. 登录 [运维安全中心（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，可查看运维安全中心（堡垒机）内网 IP 信息。

步骤三：将运维安全中心（堡垒机）IP 加入安全组

将运维安全中心（堡垒机）的内网 IP 加入安全组，并根据资产类型开放对应端口，例如 Linux 默认端口22，Windows 默认端口3389，如果目标设备修改了默认端口，则设置为实际访问端口。

1. 登录 [云服务器控制台](#)，单击实例与镜像菜单下的实例。
2. 在实例页面，单击需要绑定安全组的 CVM 实例 ID/实例名 > 安全组，进入该实例详情的安全组页面。

3. 在安全组页面，单击编辑规则，进入私有网络的安全组规则的入站规则页面。

4. 在入站规则页面，可增加入站规则，允许运维安全中心（堡垒机）内网 IP 访问资源远程桌面端口。

说明：

来源：添加运维安全中心（堡垒机）内网IP，是否需要添加其他IP根据业务实际情况评估。

端口协议：输入远程桌面端口。

添加入站规则

类型	来源 <i>i</i>	协议端口 <i>i</i>	策略	备注
自定义	如10.0.0.1或10.0.0.0/16	如UDP:53,TCP:80,443或TC	允许	
+新增一行				
完成 取消				

修

5. 在运维安全中心（堡垒机）的 [主机页面](#)，单击编辑，检查资源端口号配置，确认为在使用远程桌面端口，如果不正确请根据实际情况进行修改。

The screenshot shows the 'Host Management' interface. It lists assets with columns for Asset ID/Name, Asset IP, Network, Status, Host Machine, Operation System, and Operations. One row is selected, and its edit button is highlighted with a red box.

6. 检查其他入站规则是否需要保留。

资产由运维安全中心（堡垒机）进行托管后，运维安全中心（堡垒机）作为运维的统一入口，将其他运维来源 IP（运维人员IP）可移出安全组。同时，强烈建议尽量减少/关闭直接暴露在互联网的访问入口（可规避控制台直连的操作）

The screenshot shows the 'Inbound Rules' section of the security group configuration. It displays a list of rules with columns for Source, Protocol Port, Strategy, Remarks, Last Modified, and Actions. One rule is selected, and its delete button is highlighted with a red box.

步骤四：为运维人员创建运维安全中心（堡垒机）账号

创建运维用户账号，后续的运维操作都通过运维安全中心（堡垒机）进行。

1. 登录 [运维安全中心（堡垒机）控制台](#)。

2. 在左侧导航栏中，选择用户管理 > 用户。
3. 在用户页面，单击新建用户，需配置如下用户信息：

说明：

页面标*的为必填项。

如果您有 LDAP 认证的需求，请 [联系我们](#) 开通该功能。

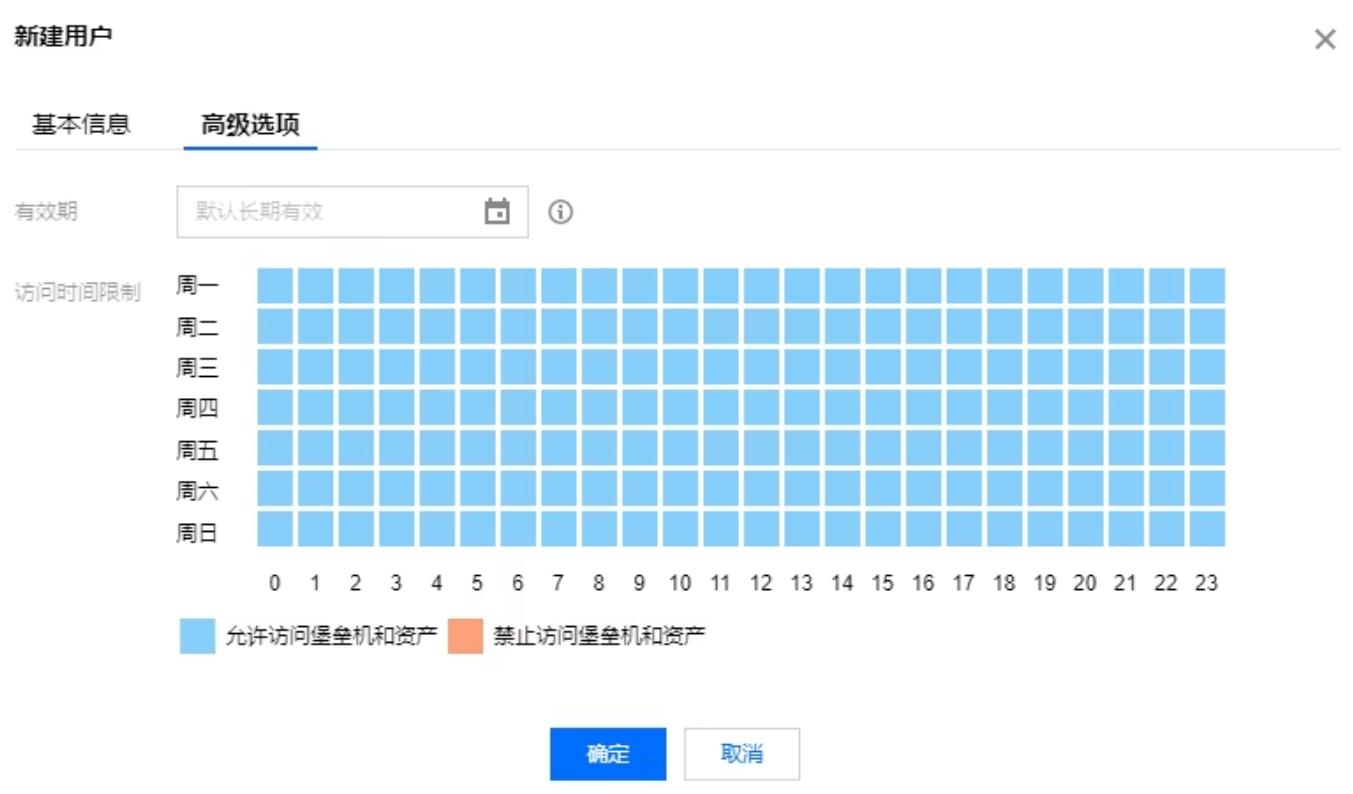
新建用户 ×

基本信息 **高级选项**

用户名 *	<input type="text" value="请输入用户名"/>	姓名 *	<input type="text" value="请输入姓名"/>
请输入用户名，长度范围 1 到 64，只能由a-zA-Z0-9以及+=,_组成，支持邮箱格式			
认证方式 *	<input type="text" value="本地"/>	手机号 *	<input type="text" value="+86"/> <input type="text" value="请输入手机号"/>
邮箱 *	<input type="text" value="请输入邮箱"/>	用户组	<input type="text" value="请选择用户组"/>
部门 *	<input type="text" value="请选择部门"/>		
确定 取消			

参数名称	说明
用户名	输入用户名。
姓名	输入用户姓名。
认证方式	选择用户的认证方式，例如本地或 LDAP。
手机号	输入用户的手机号码，登录时使用手机号码登录。
邮箱	输入用户邮箱。
用户组	选择用户所属的用户组。
部门	选择用户所属部门。

4. 如需对用户有效期和访问时间进行限制，可单击高级选项进行配置。



参数名称	说明
有效期	设置用户的有效期。
访问时间限制	设置用户能够访问运维安全中心（堡垒机）和资产的时间（以小时为单位）。

5. 用户信息配置完成之后，单击确定，即可创建用户。

步骤五：分配运维人员可访问的资产权限

基于最小权限原则，将资产的访问权限分配给运维用户。同时禁用一些敏感权限，例如删除数据。禁止手动输入资产账号密码。

1. 登录 [运维安全中心（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，按照步骤进行访问权限的配置。

4. 在设置基本信息页面，输入权限名称、部门、权限有效期，单击下一步：选择用户。

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 * ①

部门 *

有效期 

[下一步：选择用户](#)

5. 在选择用户页面，选择需要授予该访问权限的用户，同时也根据部门信息进行筛选，单击下一步：选择资产。

6. 在选择资产页面，需要选择用户可以访问的主机资产、数据库资产、Web 应用资产或资产组，同时也可根据部门、运维安全中心（堡垒机）服务、标签进行筛选，单击下一步：选择账号。

设置基本信息 > 选择用户 > ③ 选择资产 > ④ 选择账号 > ⑤ 设置访问控制 > ⑥ 完成

所属堡垒机服务	请选择			
标签	搜索标签 <input type="text"/> <input type="button" value="Q"/>			
主机 数据库 Web应用 资产组				
选择主机				
搜索主机名称/ID <input type="text"/> <input type="button" value="Q"/>				
资产ID/名称	资产IP	地址	网地址	资产类型
<input checked="" type="checkbox"/> 192.168.1.100 上海堡垒机	192.168.1.100	上海	net-reg-100	CentOS 7.9 64位
<input type="checkbox"/> 192.168.1.101 其他	192.168.1.101	其他	net-reg-101	Windows
<input type="checkbox"/> 192.168.1.102 其他	192.168.1.102	其他	net-reg-102	Linux
<input type="checkbox"/> 192.168.1.103 南京堡垒机	192.168.1.103	南京	net-reg-103	Windows Server 2012 R2 数据中心版

已选择 (1)

资产ID/名称	资产IP	地址	网地址	资产类型
192.168.1.100 上海堡垒机	192.168.1.100	上海	net-reg-100	CentOS 7.9 64位

7. 在选择账号页面，需要选择与该选中资产相关联的账号，单击下一步：设置访问控制。

设置基本信息 > 选择用户 > 选择资产 > ④ 选择账号 > ⑤ 设置访问控制 > ⑥ 完成

选择账号

资产账号	资产数
1	

已选择 (0)

资产账号

取消全部选择

允许自动填写资产账号

允许使用过滤器

上一步：选择资产 下一步：设置访问控制

说明：

建议关闭允许手动填写资产账号；数据库目前仅支持访问串方式进行访问。

8. 在设置访问控制页面，可以配置主机访问控制、主机高危命令、数据库访问控制，单击下一步：完成。

设置基本信息 > 选择用户 > 选择资产 > 选择账号 > ⑤ 设置访问控制 > ⑥ 完成

访问控制 主机高危命令 数据库高危命令

已选主机： 2

RDP磁盘映射 ① 上传文件 下载文件

RDP剪切板 ① 上传文件 下载文件 上行文本 下行文本

RDP更多选项 ① 键盘记录 ①

RZSZ ① 上传文件 下载文件

SFTP选项 ① 上传文件 下载文件 删除文件

上一步：选择账号 下一步：完成

主机访问控制配置项	配置项内容
RPD 磁盘映射	上传文件 下载文件
RPD 剪切板	上传文件 下载文件 上行文本 下行文本
RPD 更多选项	键盘记录（启动键盘记录后，有可能会记录敏感信息）
RZSZ	上传文件 下载文件
SFTP 选项	上传文件 下载文件

删除文件

说明：

- 主机高危命令、数据库访问控制规则创建详见 [新建高危命令模板、规则管理](#)。
- 键盘记录使用限制：
 - Mac 端远程连接 Windows 主机，按下 fn+F5 键，记录 F5 键盘操作事件，不记录 fn 按下事件；单独按 fn 也不会记录。
 - Windows 终端 MSTSC 连接，按下 Win 键旁边的“菜单”键不会记录该事件。
 - Windows 终端 Web 连接，按下 PrintScreen 键不会记录该事件。
 - Windows 终端，用 Web 方式连接 Windows 主机，按下 Ctrl+n 键，本地新打开浏览器，仅记录 Ctrl 键盘事件。
 - Windows 终端，用 Web 连接 Windows 主机，按下 Win+M 键，本地最小化整个浏览器，只记录 win 键盘事件。

9. 在权限信息确认页，确认权限配置无误后，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。

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

配置项	配置详情
权限名称	
有效期	
用户	
用户组	
主机	
数据库	
Web应用	
资产组	
账号	
允许手动填写账号	
允许使用访问串	
RDP磁盘映射	
RDP剪贴板	
RDP更多选项	
RZSZ	
SFTP选项	
高危命令	
数据库访问控制	

上一步：设置访问控制 确定提交 返回权限列表

步骤六：告知运维人员运维安全中心（堡垒机）登录地址

将概览页面的运维安全中心（堡垒机）运维页面地址复制、并告知运维人员。默认为公网运维模式，用户可启用内网运维模式。

1. 登录 [运维安全中心（堡垒机）控制台](#)，在左侧导航中，选择概览。
2. 在概览页面，复制右侧的帮助 > 公网运维页面链接，告知给已经授权的运维用户。



3. 同时，也可前往开通服务页面，单击目标资源 > 更多 > 调整内网运维功能，配置并启用内网运维模式。



步骤七：运维人员激活运维安全中心（堡垒机）账号

运维人员访问运维安全中心（堡垒机）页面后，需要先进行激活操作，设置自己登录运维安全中心（堡垒机）的密码，后续通过 MFA 认证登录。

1. 在主机运维页面，单击账号激活，跳转到账号激活页面。
2. 运维人员可以通过管理员授权的手机号码、邮箱，完成激活账号（登录密码初始化）操作。
3. 完成账号激活操作，单击登录，返回主机运维页面。



步骤八：运维人员登录运维安全中心（堡垒机）进行运维操作

1. 在浏览器中输入运维页面登录地址，打开运维安全中心（堡垒机）运维页面；输入手机号、密码登录运维安全中心（堡垒机）；也可以单击[账号密码](#)切换到账号名、密码方式登录。



2. 进入运维安全中心（堡垒机）之后，在左侧导航中，选择需要进行运维操作的资产类型。
3. 在资产列表页面，单击对应资产右侧的访问。

资产ID/名称	资产IP	操作系统	操作
资产1	192.168.1.100	CentOS 7.9 64位	访问 收藏
资产2	192.168.1.101	Windows Server 2019 数据中心版 64位 中文版	访问 已收藏

4. 运维安全中心（堡垒机）支持多种访问方式，例如本地客户端、Web 页面等。

访问资产

访问协议 SSH SFTP

访问方式 XShell

资产账号 root

认证方式 密码 私钥

[访问](#) [取消](#)

步骤九：管理员对运维人员操作进行审计

运维人员对授权资产的所有操作都会被运维安全中心（堡垒机）进行记录，管理员可通过审计管理查看对应审计日志。高危操作阻断记录在风险事件查阅。

1. 登录 [运维安全中心（堡垒机）控制台](#)。
2. 在左侧导航栏中，选择[操作审计 > 会话记录](#)。
3. 在会话记录页面，可以通过[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](#)、[Web应用会话](#)、运维任务执行记录，检查运维人员是否存在违规操作。

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	操作命令/阻断命令	状态	操作
...	结束	详情 回放
...	结束	详情 回放
...	结束	详情 回放
...	结束	详情 回放
...	结束	详情 回放

OrcaTerm 运维实践教程

最近更新时间：2025-07-01 11:22:11

应用场景

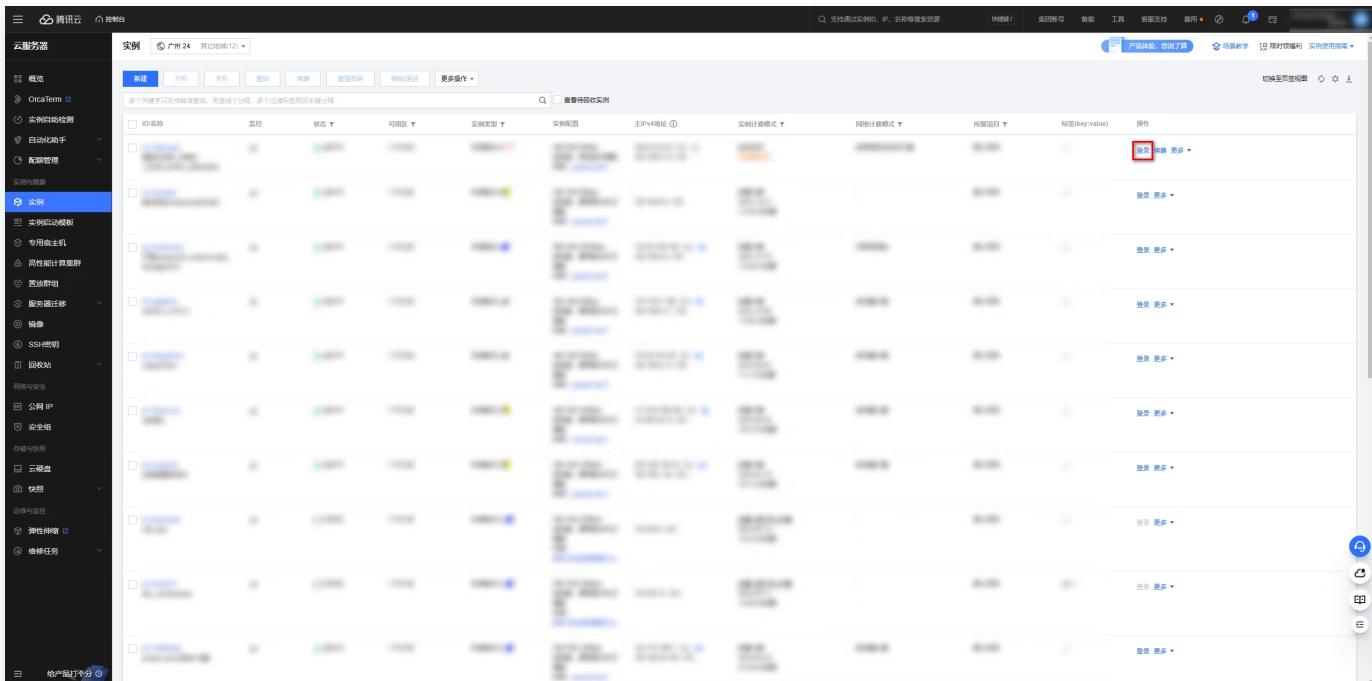
当用户通过 CVM 控制台直接登录 CVM 时，可选择堡垒机登录方式。通过堡垒机登录时，所有运维操作将会被记录，同时可结合堡垒机的权限控制能力，对高危命令进行拦截，这有利于提高运维操作的安全性，避免一些误操作或恶意操作事件的发生。

功能限制

- 本功能当前需要开白使用，如果需要开启，请[联系我们](#)开通此功能。
- 本功能当前仅支持 Linux 服务器。

操作步骤

1. 进入 CVM 控制台 [实例列表](#)，单击对应 CVM 实例后面的登录。



The screenshot shows the Tencent Cloud CVM Control Console interface. On the left, there is a sidebar with various service icons. The '实例' (Instances) icon is selected and highlighted in blue. The main area displays a table of instances with columns including ID/名称 (ID/Name), 监控 (Monitoring), 状态 (Status), 可用区 (Availability Zone), 实例类型 (Instance Type), 主IPV4地址 (Primary IPv4 Address), 实例计费模式 (Billing Mode), 所属项目 (Project), 标签(key:value) (Tags), and 操作 (Actions). A specific instance's 'Login' button is highlighted with a red box. The top navigation bar includes tabs like '便捷' (Convenient), '开机' (Power On), '关机' (Power Off), '重启' (Restart), '重置密码' (Reset Password), and '更多操作' (More Operations). The right side of the interface has several small icons for different functions.

2. 连接协议选择堡垒机，设置堡垒机实例、用户名密码后，单击登录。

登录

腾讯云产品
云服务器 (CVM) ins- [redacted]

连接协议
 免密连接 (TAT) 终端连接 (SSH) 堡垒机

于 > ② 登录堡垒机

堡垒机实例
bh-saas-[redacted]

账号类型
 已托管 未托管

验证方式
 密码验证 密钥验证

用户名	密码	端口
请输入	请输入	22

登录

由 [堡垒机](#) 提供支持，助力企业构筑数据安全堡垒
请确认安全组已放通来源为堡垒机 IP 的远程登录端口，[查看堡垒机IP信息](#)

3. 通过 H5 运维页面对服务器进行运维操作。

```
Welcome to TencentOS Server 3 x86_64
Version 3.1 20240227
Last failed login: Wed Oct 30 09:25:35 CST 2024 from 14.103.70.121 on ssh:notty
There were 4872 failed login attempts since the last successful login.
Last login: Wed Oct 16 20:24:56 2024 from 119.147.10.206
[root@VM-24-102-tencentos ~]# ls
```

4. 运维人员操作结束之后，管理员可进入运维安全中心（堡垒机）[会话记录](#)页面，查看审计日志。

运维安全中心（堡垒机）

会话记录 (普通区)

字符会话 图形会话 文件传输会话 数据库会话 Web应用会话 运维任务执行记录

近7天 近14天 近30天 2025-03-07 ~ 2025-03-13

请选择报告进行过滤 搜索 导出 打印

资产IP	来源IP	资产端口	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	操作命令/阻断命令	状态	操作
192.168.10.100 (内网)	192.168.10.100	22345	2025-03-12 17:55:44 2025-03-12 18:19:30	堡垒机 (普通)	admin	22分钟46秒 8.69KB	3 0	结束	详情 回滚
192.168.10.100 (内网)	192.168.10.100	22345	2025-03-12 17:50:19 2025-03-12 17:50:39	堡垒机 (普通)	admin	1分钟 5.09KB	11 4	结束	详情 回滚
192.168.10.100 (内网)	192.168.10.100	22345	2025-03-12 17:42:15 2025-03-12 17:42:15	堡垒机 (普通)	admin	49 0.19KB	0 0	结束	详情 回滚
192.168.10.100 (内网)	192.168.10.100	22345	2025-03-12 17:10:50 2025-03-12 17:52:51	堡垒机 (普通)	admin	42分钟08秒 1.33KB	6 4	结束	详情 回滚
192.168.10.100 (内网)	192.168.10.100	22345	2025-03-12 17:08:06 2025-03-12 17:08:37	堡垒机 (普通)	admin	2分钟 36.86KB	8 3	结束	详情 回滚
192.168.10.100 (内网)	192.168.10.100	22345	2025-03-12 16:59:15 2025-03-12 17:00:06	堡垒机 (普通)	admin	50秒 27.20KB	19 5	结束	详情 回滚
192.168.10.100 (内网)	192.168.10.100	22345	2025-03-12 16:58:00 2025-03-12 17:53:00	堡垒机 (普通)	admin	54分钟59秒 7.4KB	2 0	结束	详情 回滚
192.168.10.100 (内网)	192.168.10.100	22345	2025-03-12 15:44:53 2025-03-12 15:54:59	堡垒机 (普通)	admin	58秒 0.49KB	1 0	结束	详情 回滚
192.168.10.100 (内网)	192.168.10.100	22345	2025-03-12 15:33:10 2025-03-12 18:19:03	堡垒机 (普通)	admin	2小时45分钟53秒 2.69KB	2 0	结束	详情 回滚

共 0 条

20 < / 1页 1 / 1页 > / <

使用内网域名访问堡垒机运维页面

最近更新时间：2025-08-25 17:53:21

操作场景

内网运维是指通过内部网络访问运维安全中心（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。运维安全中心（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 [运维安全中心（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

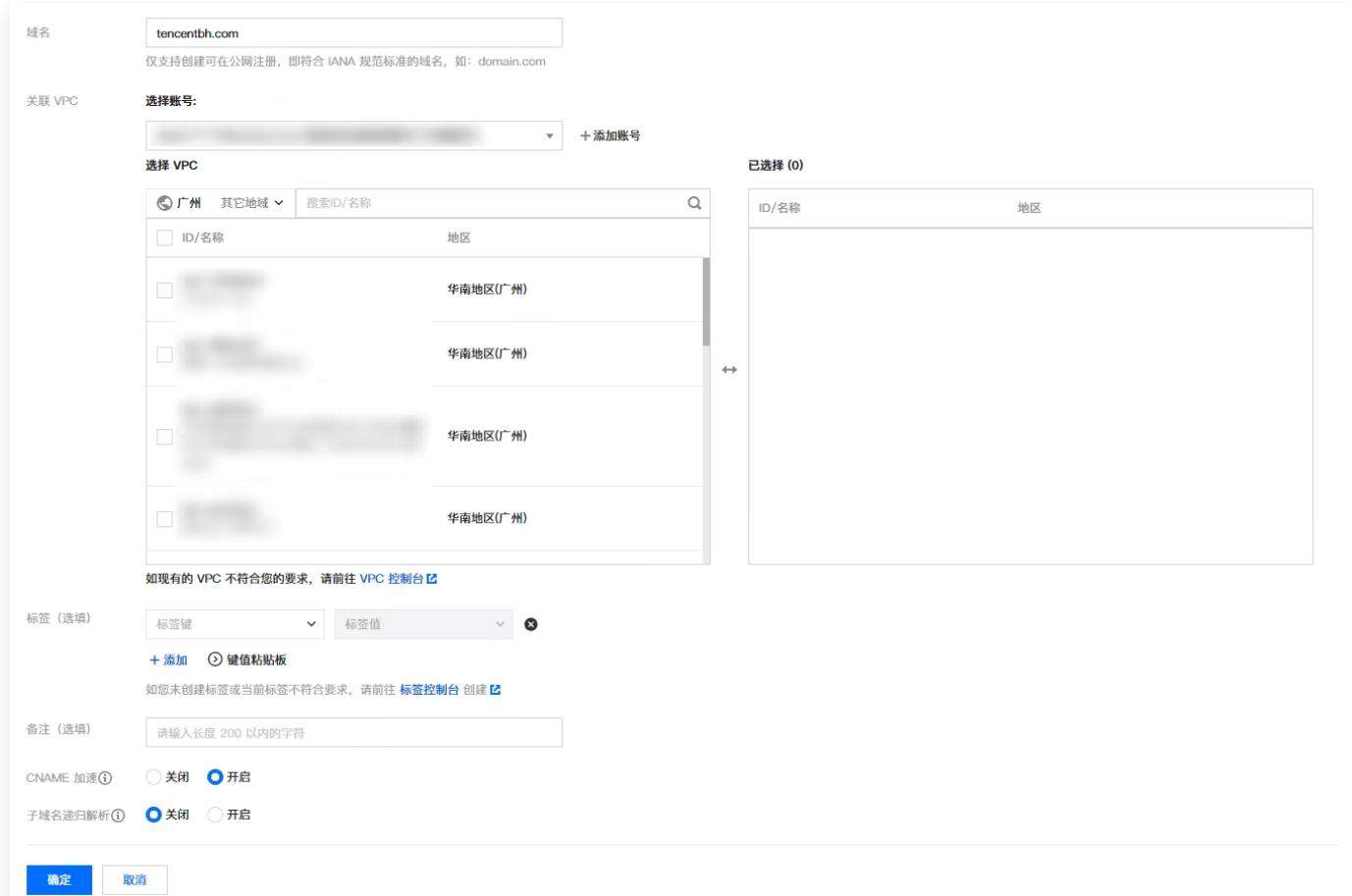
1. 登录 私有域解析 Private DNS 控制台。
2. 在左侧导航栏中，选择内网解析 > 域名列表。
3. 在域名列表中，单击新建私有域。



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

+ 添加账号

选择 VPC

广州 其它地域 搜索ID/名称

ID/名称	地区
华南地区(广州)	
华南地区(广州)	
华南地区(广州)	
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 (Optional)

标签键 标签值

+ 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 (Optional)

请输入长度 200 以内的字符

CNAME 加速① 关闭 启用

子域名递归解析① 关闭 启用

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。



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

① 说明：

- **主机记录：**建议格式为 {resource-id}-{vpc-id}。

例如：resource-id="bh-saas-xxxxxx", vpc-id="vpc-124debs9"，则主机记录应填写为xxxxx-124debs9。

- **记录值：**填写需要内网访问的 IP 地址，即 [运维安全中心（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。

① 说明：

访问域名：**主机记录.tencentbh.com**。

iOA 零信任堡垒机集成实践教程

最近更新时间：2025-11-06 15:38:01

概述

堡垒机（运维安全中心）与 iOA 零信任安全管理系统的集成，旨在构建“身份可信、终端合规、权限动态、操作可溯”的零信任运维体系。通过整合 iOA 的动态身份认证、终端安全检测能力与运维安全中心（堡垒机）的资产管控、操作审计功能，实现从用户登录到资产访问的全链路安全管控，解决传统运维中权限过度授予、身份认证薄弱、终端风险不可控等问题。

前提条件

- 已 [购买运维安全中心（堡垒机）基础版或专业版](#) 并开通零信任堡垒机服务；
- 运维安全中心（堡垒机）中已 [同步主机资产](#) 并 [已开启托管](#)。

操作步骤

步骤1：配置 iOA 认证源

iOA 支持 WindowsAD、SCIM2.0、政务微信/私有化企业微信等多种用户源。

参考[认证对接](#) 文档进行认证源配置。

步骤2：同步 iOA 零信任用户至运维安全中心（堡垒机）

将 iOA 零信任系统中的用户信息自动同步至运维安全中心（堡垒机），确保用户数据一致，为后续权限分配、身份鉴权奠定基础。

参考[同步 iOA 零信任用户](#) 文档，在 iOA 零信任用户页面，同步用户信息。

步骤3：配置用户访问权限

为同步后的 iOA 用户分配具体资产的访问权限，实现“最小权限”原则。

参考[新建访问权限](#) 文档，对同步过来的 iOA 零信任用户进行相关资产的访问权限配置。

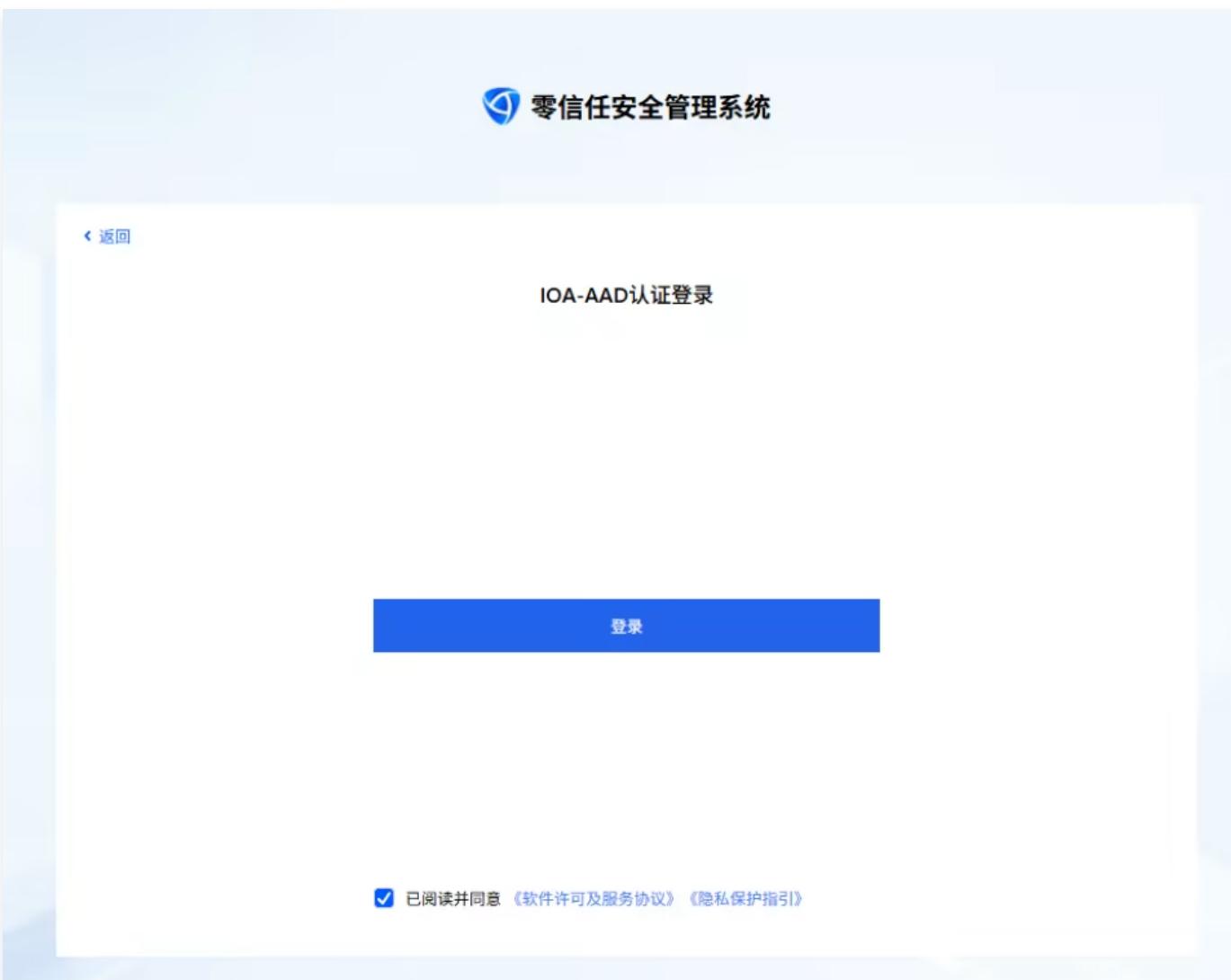
步骤4：通过 iOA 访问主机资产

运维人员通过 iOA 客户端发起访问，验证零信任流程的完整性。

- 登录[运维安全中心（堡垒机）](#)。
- 在左侧导航栏中，选择概览。
- 在概览页面，找到帮助 > 零信任运维页面，单击复制，并告知给已经授权的运维用户。



4. 在浏览器中输入运维页面登录地址，打开运维安全中心（堡垒机）的 iOA 运维登录页面。
5. 在 iOA 运维登录页面，选择对应的组织域，选择完成后，单击下一步。
6. 输入已同步至运维安全中心（堡垒机）的 iOA 用户密码，单击登录即可进入运维模式。



7. 在运维模式中，选择主机资产 > 资产列表。
8. 在资产列表页面，单击对应主机右侧的访问。

资产ID/名称	资产IP	操作系统	状态	堡垒机实例	堡垒机IP	堡垒机网络信息	操作
...	...	Windows Server 2022 数据中心版 64位 中文版	正常	访问 收藏
...	...	TencentOS Server 3.3 (TK4)	正常	访问 收藏
...	...	TencentOS Server 4 for x86_64	正常	访问 收藏

9. 在运维页面，您可输入相关的运维命令。

```
Linux VM-11-4-debian 4.19.0-11-amd64 #1 SMP Debian 4.19.146-1 (2020-09-17) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Dec 16 20:37:23 2021 from 192.168.1.11
root@VM-11-4-debian:~#
```

步骤5：查看操作审计

说明：

运维人员通过 iOA 客户端登录。验证是否成功跳转至运维安全中心（堡垒机）操作界面，并确认操作日志完整记录会话内容。

1. 登录 [运维安全中心（堡垒机）](#)。
2. 在左侧导航栏中，选择操作审计 > 会话记录。
3. 在会话记录页面，单击字符会话 Tab 标。
4. 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	资产类型	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	操作命令/阻断命令	状态	操作
192.168.1.11	192.168.1.11	Linux	root	2025-07-09 15:02:05 2025-07-09 15:02:10	VM-11-4-debian	root	0分 0.18KB	0 0	结束	详情 回放
192.168.1.11	192.168.1.11	Linux	root	2025-07-09 09:52:20 2025-07-09 09:52:39	VM-11-4-debian	root	10秒 0.39KB	2 0	结束	详情 回放

5. 在会话详情页面，可查看会话的基本会话信息、键盘操作、剪切板操作和文件操作记录。

说明：

通过 iOA 登录进行运维操作时，审计中的用户信息会显示 iOA。

6. 在字符会话页面，单击对应会话右侧的回放，查看是否和 [步骤4](#) 中的主机操作相同。

资产ID	来源IP	资产账号	开始时间/结束时间	资产名称	用户名/别名	会话时长/会...	操作命令/脚...	状态	操作
1 (外) (内)	5	root	2023-10-18 2023-10-18	[REDACTED]	[REDACTED]	[REDACTED] 0B	1 0	结束	详情 回放
2 (外) (内)	5	root	2023-10-18 2023-10-18	[REDACTED]	[REDACTED]	[REDACTED] 0B	1 0	结束	详情 回放