

堡垒机 最佳实践



腾讯云

【 版权声明 】

©2013-2024 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內容。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

最佳实践

SaaS 型堡垒机

传统型堡垒机迁移数据到 SaaS 型堡垒机

高危命令阻断

文件传输控制

安全事故追溯

跨 VPC 资产管理

等保最佳实践

 等保二级

 等保三级

传统型堡垒机

删库等高危命令阻断

配置应用发布收纳管理数据库

服务器真实密码隐藏

安全事故事后追溯

等保最佳实践

最佳实践

SaaS 型堡垒机

传统型堡垒机迁移数据到 SaaS 型堡垒机

最近更新时间：2023-12-06 16:55:21

传统型堡垒机数据迁移到 SaaS 型堡垒机，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。



3. 登录 **SaaS 型堡垒机控制台**，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。



5. 将从传统型堡垒机导出的用户信息复制，并粘贴到 SaaS 型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 型堡垒机，并完成导入操作。



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 [SaaS 型堡垒机控制台](#)，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**。

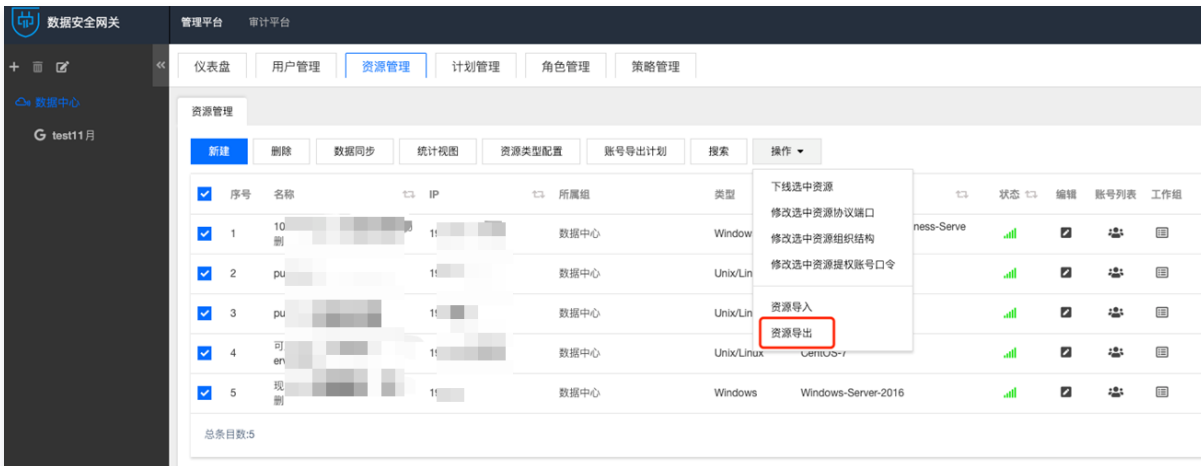


3. 在确认同步窗口中，确认同步的地域范围和资产类型，单击**确定**，即可将腾讯云的资产同步到 SaaS 型堡垒机。

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。



3. 登录 [SaaS 型堡垒机控制台](#)，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。



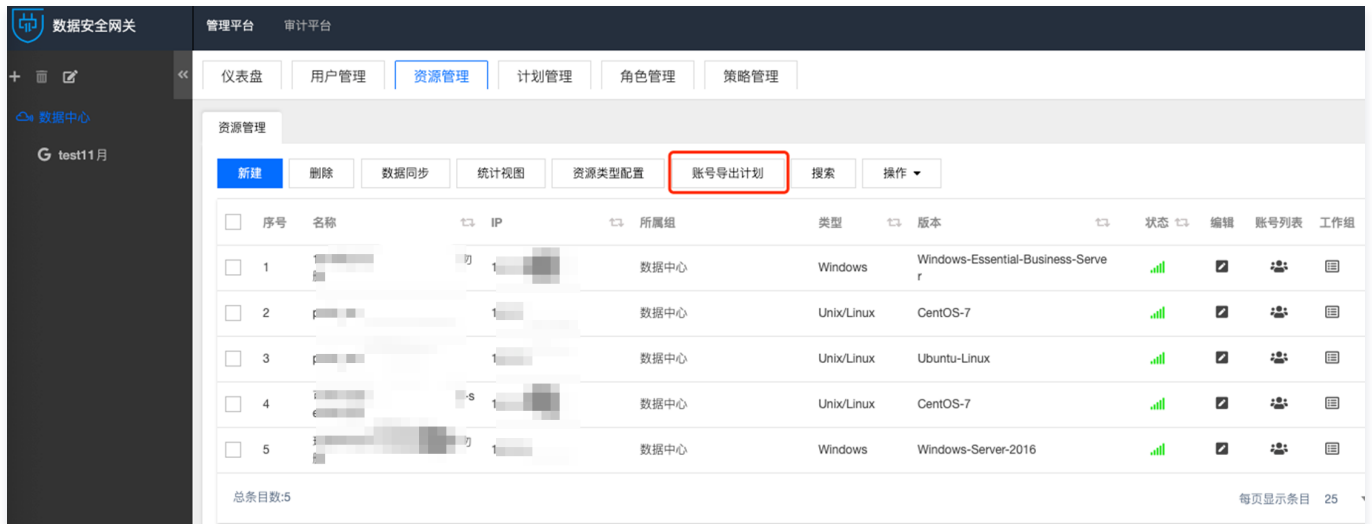
5. 将从传统型堡垒机导出的资产信息复制，并粘贴到 SaaS 型堡垒机导入主机模板当中，需要注意将信息粘贴到对应的位置。模板字段对应关系如下：

| 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。 |

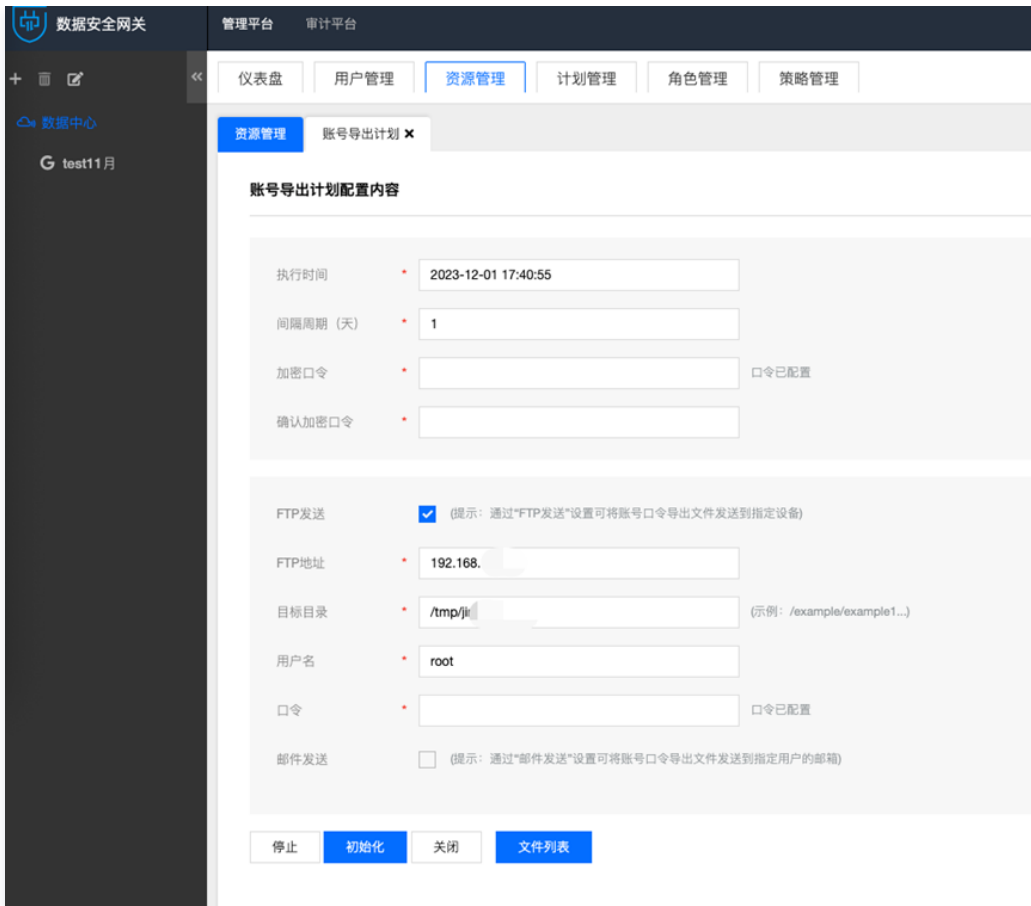
账号数据

账号密码信息，可通过导出/导入方式进行迁移。

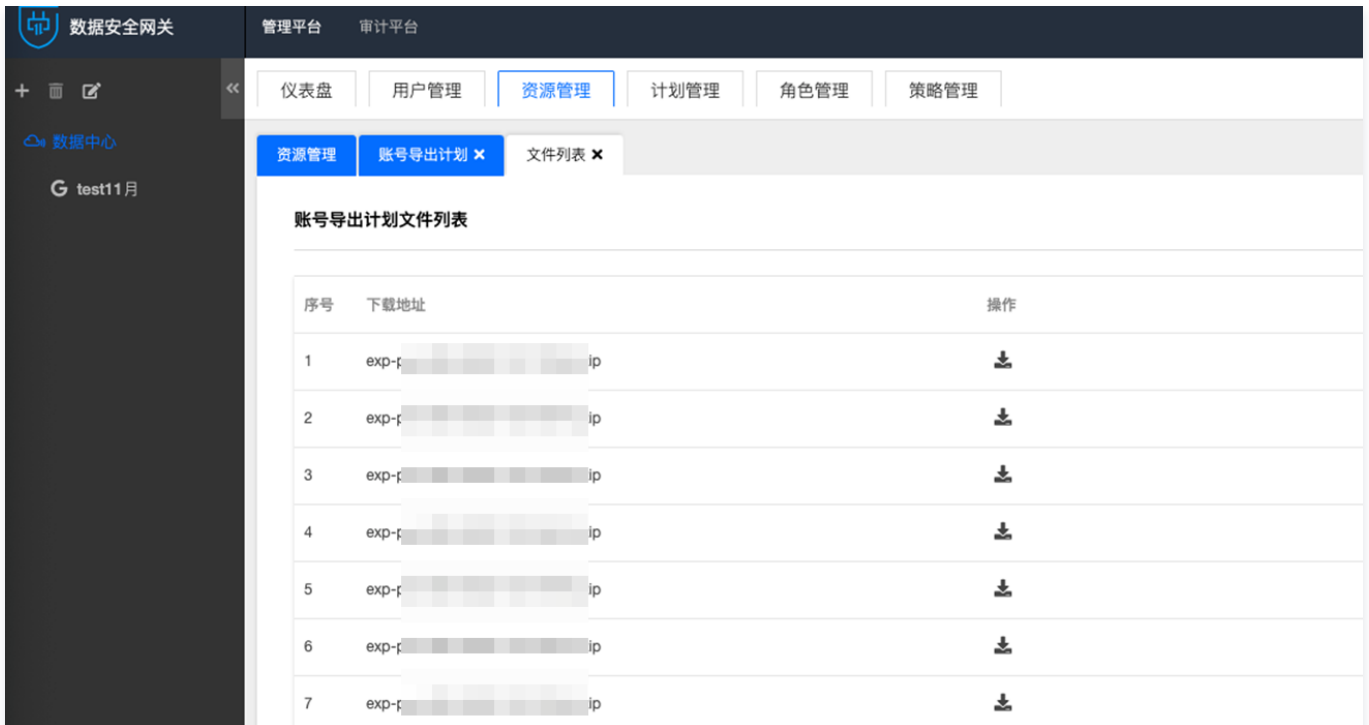
1. 登录传统型堡垒机控制台，单击**资源管理**。
2. 在资源管理页面，单击**账号导出计划**，进入配置页面。



3. 在配置页面当中，配置导出任务的信息，建议执行时间配置为当天。



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。



5. 将从传统型堡垒机导出的账号信息复制，并粘贴到 SaaS 型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 |

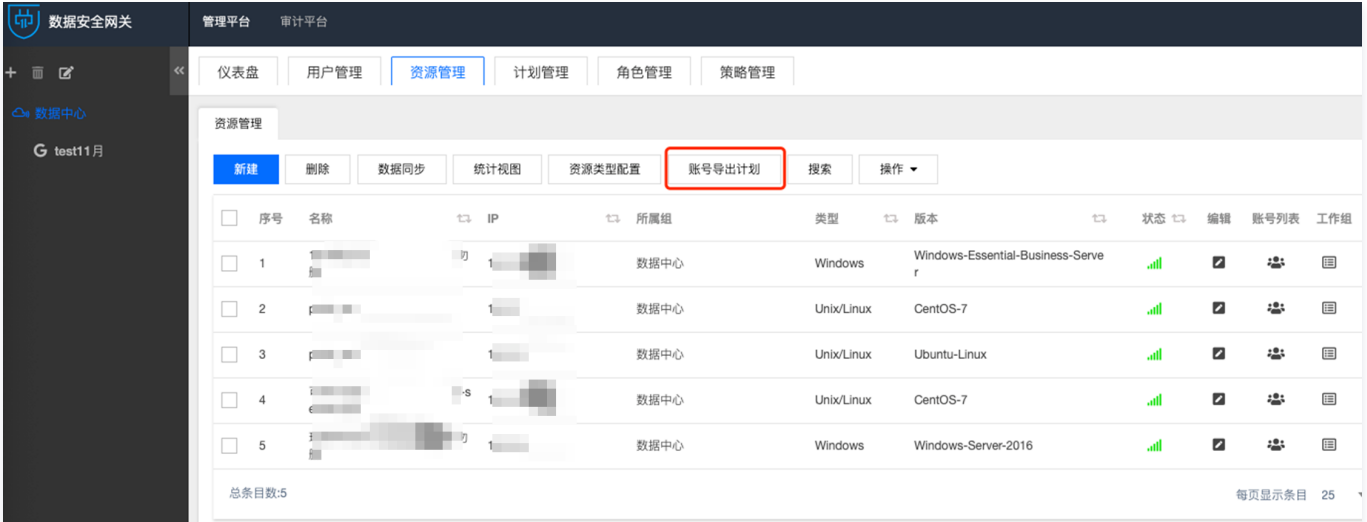
| | |
|----|------|
| 密码 | 账号密码 |
|----|------|

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 [SaaS 型堡垒机控制台](#)，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，单击修改堡垒机服务。



3. 在弹窗完成绑定，选择堡垒机服务，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：2023-11-21 18:18:11

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. 进入 [SaaS 型堡垒机控制台](#)，在左侧导航选择权限管理 > 高危命令，进入高危命令页面。
2. 在高危命令页面，单击新建模板，弹出新建高危命令模板弹窗。



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。



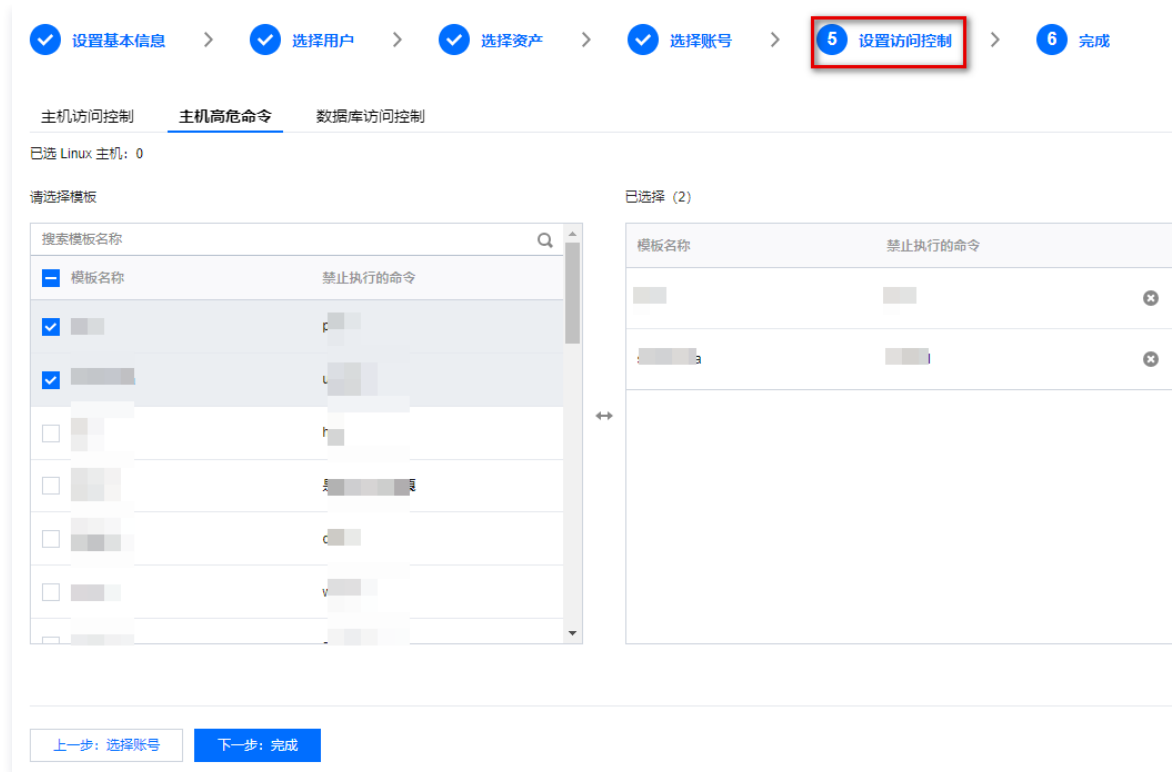
4. 单击确定，即可创建高危命令模板。

步骤2：访问权限关联高危命令模板

1. 进入 [SaaS 型堡垒机控制台](#)，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，单击对应访问权限右侧的编辑，进入编辑访问权限页面。



3. 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。



4. 单击**下一步: 完成**，确认访问权限配置信息。
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，将被堡垒机拦截。

文件传输控制

最近更新时间：2023-10-20 14:46:54

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. 进入 [SaaS 型堡垒机控制台](#)，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**，进入新建访问权限页面。
3. 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。



4. 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。
5. 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 | [模糊] |
| 有效期 | 长期有效 |
| 用户 | n [模糊] |
| 用户组 | 未选择 |
| 资产 | 可 [模糊] |
| 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](#)

6. 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"/> | [模糊] | 已生效 | | | | | | 编辑 删除 |
| <input type="checkbox"/> | [模糊] | 已生效 | [模糊] | | [模糊] | | [模糊] | 编辑 删除 |

安全事故追溯

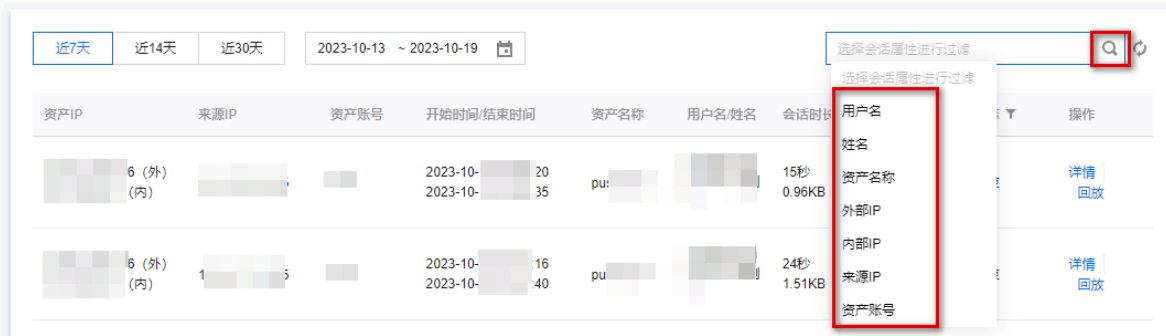
最近更新时间：2023-10-20 14:46:54

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介绍如何审计用户运维操作。

操作步骤

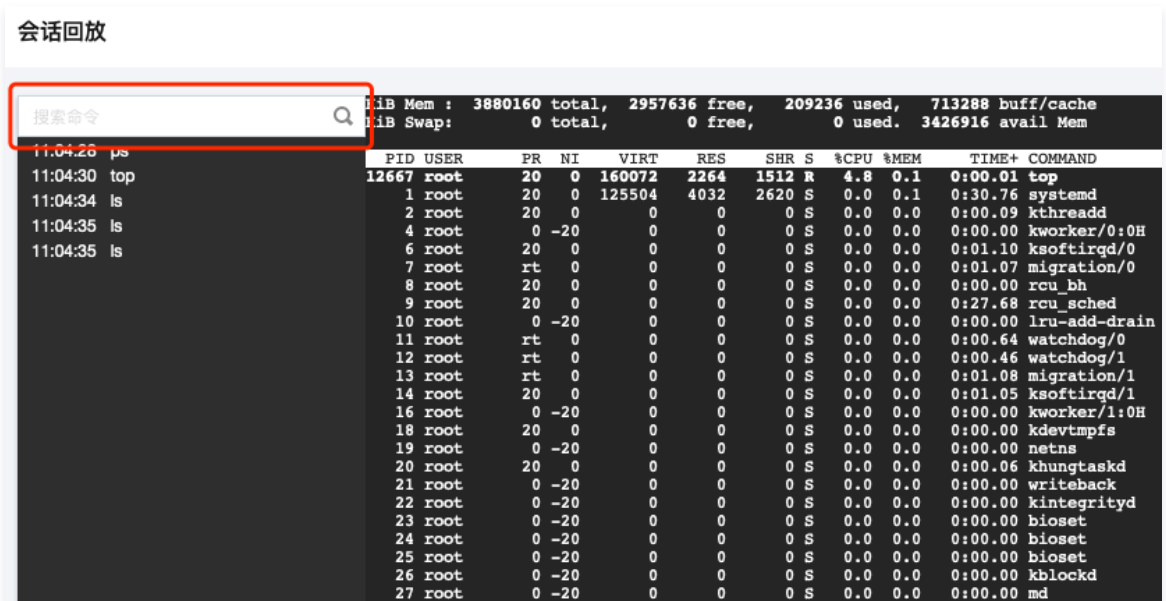
1. 进入 [SaaS 型堡垒机控制台](#)，在左侧导航选择 **审计管理 > 字符会话**，进入字符会话页面。
2. 在字符会话页面，单击搜索框，可通过“用户名、姓名、资产名称”等关键字对会话进行过滤。



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。



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。



跨 VPC 资产管理

最近更新时间：2023-10-20 14:46:54

操作场景

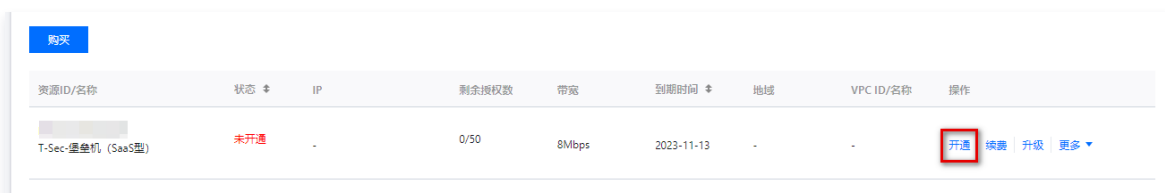
当资产（例如 CVM）分布在多个 VPC 时，需要通过堡垒机统一进行管理，本文为您详细介绍如何实现跨 VPC 的资产管理。

操作步骤

1. 进入 [SaaS 型堡垒机控制台](#)，在左侧导航选择**开通服务**，进入开通服务页面。
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。



3. 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**。



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 ✕

资源ID * bh-xxxxxx
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

广州
上海
南京
北京
成都
重庆

-西北地区-
西安

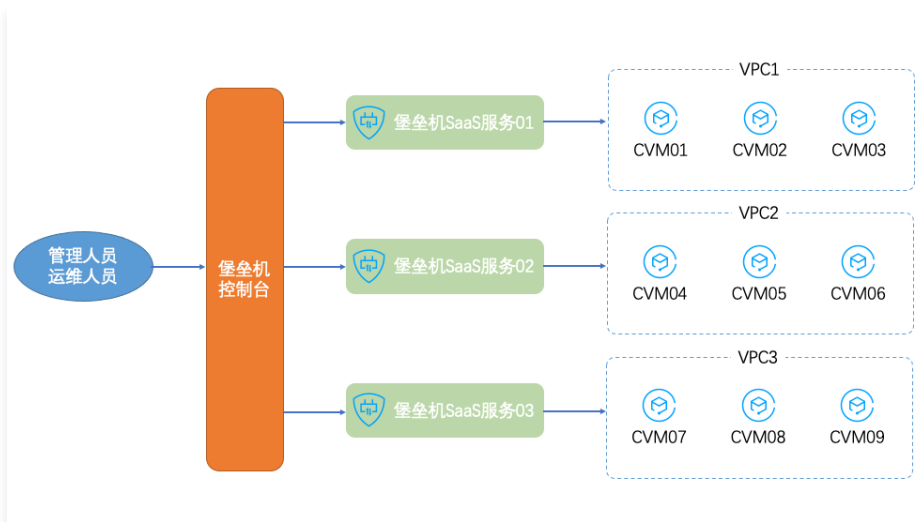
请选择需要堡垒机纳管的资产的所属地域

VPC * xxxxxx
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 * xxxxxx
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。



① 说明

- 管理和维护工作操作详情请参见 SaaS 型堡垒机的 [快速入门](#)。
- 除开通堡垒机服务外，还可以通过 [对等连接](#) 和 [云联网](#) 来打通堡垒机与 CVM 之间的网络。

等保最佳实践

等保二级

最近更新时间：2023-09-28 17:09:11

为助力企业等保合规，本文为您介绍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 SaaS 型堡垒机](#)，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

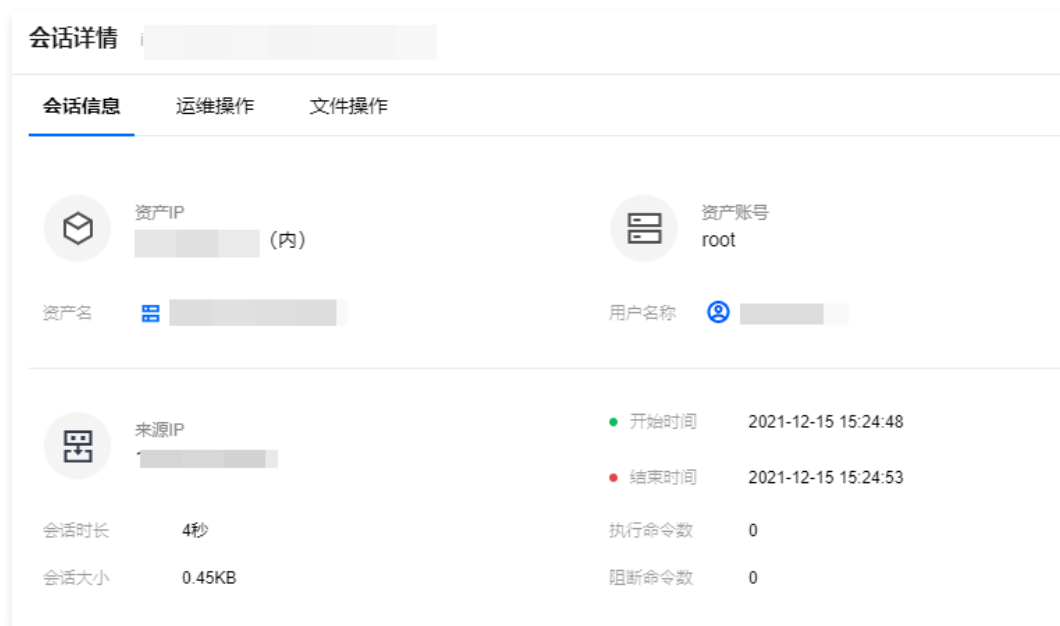
a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

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

1. 登录 [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、数据库运维会话记录。



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。



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- [redacted]

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 | pa | 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 [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 事件类型

近7天 近14天 近30天 2021-12-10 - 2021-12-16 选择会话属性进行过滤 🔍 ↻

| 资产IP | 来源IP | 账号 | 日期和时间 | 资产名 | 用户 | 会话时长/会话大小 | 操作命令/阻断命令 | 事件状态 | 操作 |
|-----------------|-----------------|------|--|--------|--------------|--------------|-----------|------|---------|
| | | | 开始时间/结束时间 | | 用户名/姓名 | | | 状态 | |
| 192. [redacted] | 101. [redacted] | root | 2021-12-15 15:24:48 2021-12-15 15:24:53 | gordan | chen chen | 4秒 0.45KB | 0 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。

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

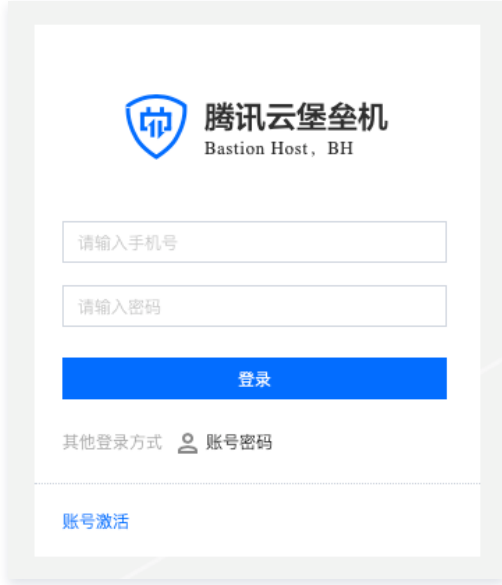
身份鉴别

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 [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 [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
✕

用户名

姓名

认证方式

手机号 ❗

手机号重复

邮箱

用户组

有效时间 📅 ℹ️

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 [堡垒机控制台](#)，在左侧导航选择系统设置 > 认证设置 > 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）。



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 [堡垒机控制台](#)，在左侧导航选择系统设置 > 安全设置，进入安全设置页面。
2. 在安全设置页面，查看密码错误锁定和锁定时长。



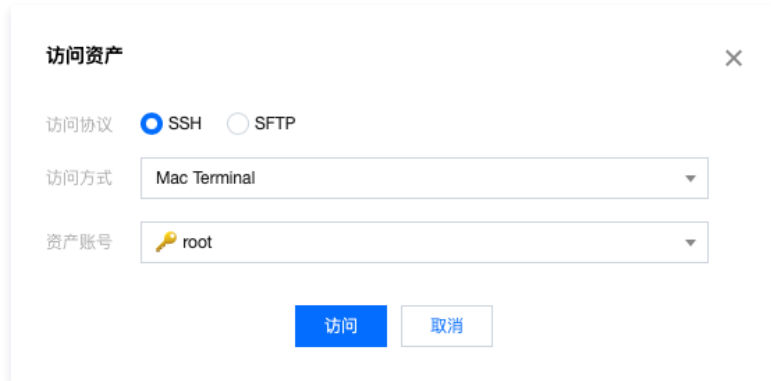
c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。

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 [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：

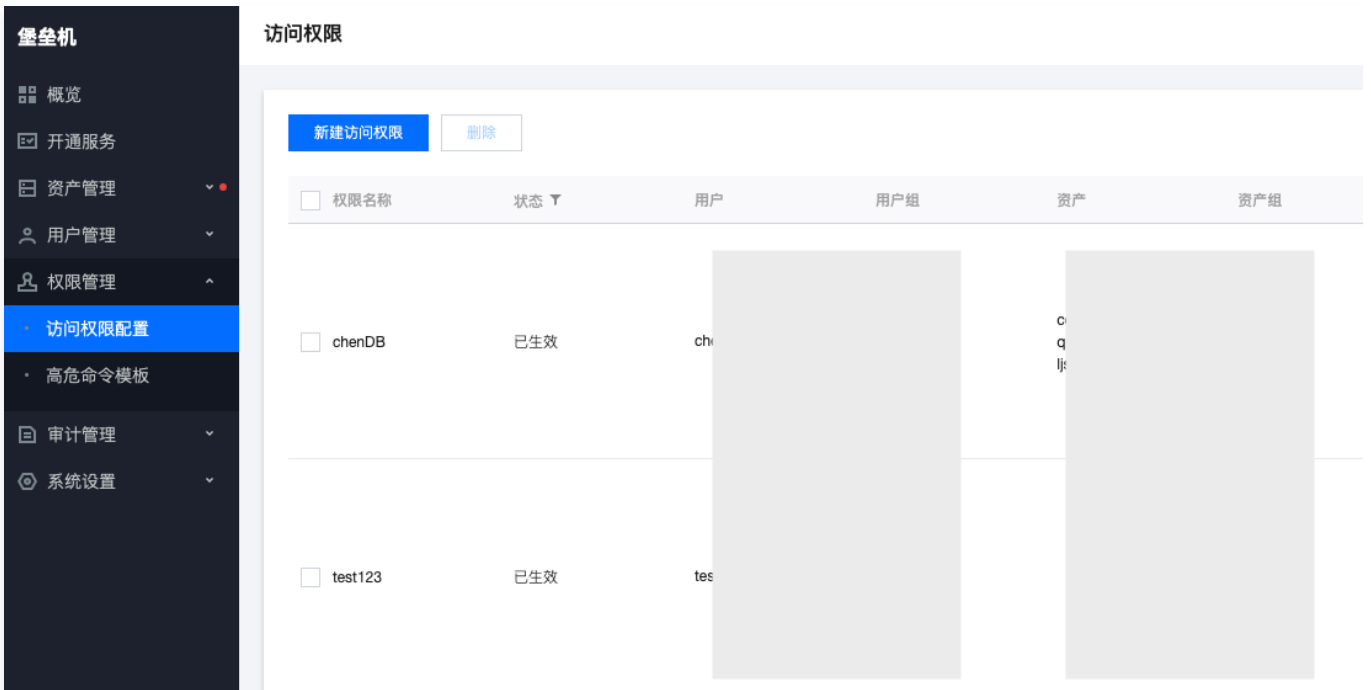
- 是否给登录的用户分配账户
 - 1.1 登录 [堡垒机控制台](#)，在左侧导航选择用户管理 > 用户，进入用户页面。
 - 1.2 在用户页面，查看用户信息，证明给用户分配了账户。



• 是否给登录的用户分配权限

1.1 登录 [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。

1.2 在访问权限配置页面，查看用户权限分配情况。



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

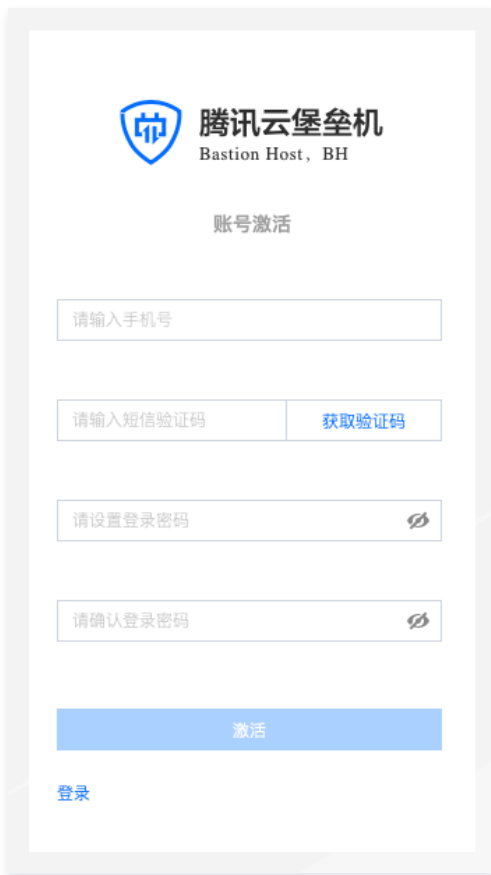
1.1 登录 [堡垒机控制台](#)，在左侧导航选择**用户管理 > 用户**，进入用户页面。

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。



• 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；

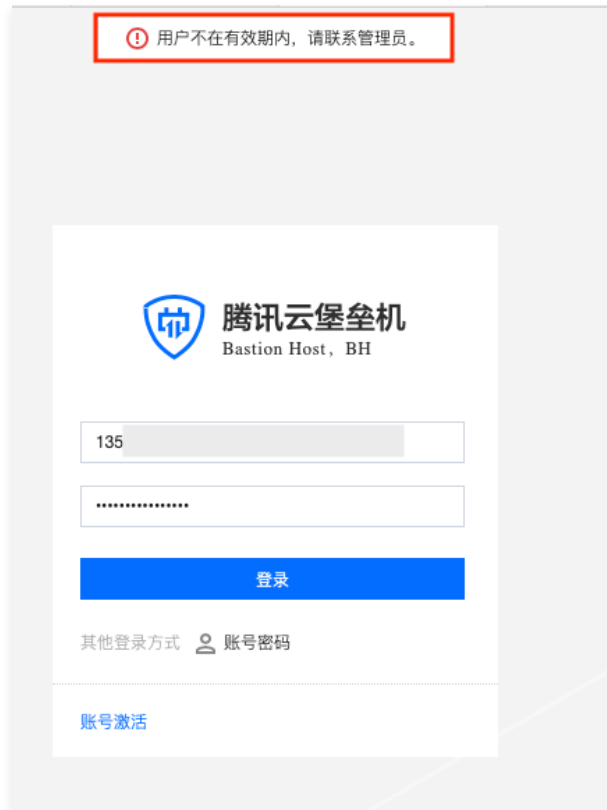
本条款主要考察：账户过期之后，能否继续使用。

ⓘ 说明

请提前准备一个已经到期的用户。

1. 登录 **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 [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。

新建访问权限

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

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

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 >
 6 选择高危命令模板 >
 7 完成

请选择模板 已选择 (0)

| <input type="checkbox"/> 模板名称 | 禁止执行的命令 | <input type="checkbox"/> 模板名称 |
|---------------------------------|--|-------------------------------|
| <input type="checkbox"/> 7777 | 222 | |
| <input type="checkbox"/> 新建 | top | |
| <input type="checkbox"/> 777 | whoami | |
| <input type="checkbox"/> 测试高危命令 | m * shutdown * | |
| <input type="checkbox"/> xss | <script>alert('XSS');</script> | |
| <input type="checkbox"/> 高危 | m * reboot* <script>alert(123);</script> | |

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 [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

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 T | 操作 |
|------|------|------|-----------|------|--------|-----------|------|---------------------------------------|
| ... | ... | ... | ... | ... | ... | ... | 结束 | 详情 回故 |
| ... | ... | ... | ... | ... | ... | ... | 结束 | 详情 回故 |

3. 单击**日志检索**，进入日志搜索页面，可查看用户对堡垒机的操作日志。

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 2021-10-31 ~ 2021-11-29 选择日志属性进行过滤

| 时间 | 用户名/姓名 | 来源IP | 登录方式 | 登录结果 |
|------------|--------|------|---------|------|
| 2021-11-26 | | | web页面登录 | 失败 |
| 2021-11-26 | | | web页面登录 | 失败 |
| 2021-11-26 | | | web页面登录 | 失败 |
| 2021-11-26 | | | 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 [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 | 10i 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 | 10i 管! | 9.7 | 重置用户密码 | 成功 |
| 2021-11-19 16:41:10 | 10i 管! | 9.2 | 修改登录设置 | 成功 |
| 2021-11-19 14:50:17 | 10i 管! | 9.2 | 修改密码强度设置 | 成功 |

共 5 条 20 条 / 页 1 / 1 页

其他

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：2023-09-28 17:09:11

为助力企业等保合规，本文为您介绍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 SaaS 型堡垒机](#)，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。堡垒机支持对云服务器运维操作进行监控和审计。

1. 登录 [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、数据库运维会话记录。



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。



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- [redacted]

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 | pa | 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 [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 **事件类型**

近7天 近14天 近30天 2021-12-10 ~ 2021-12-16

选择会话属性进行过滤

| 资产IP | 来源IP | 账号 | 日期和时间 | 资产名 | 用户名/姓名 | 会话时长/会话大小 | 操作命令/阻断命令 | 事件状态 | 操作 |
|-----------------|-----------------|------|--|--------|--------------|--------------|-----------|------|-------|
| 192. [redacted] | 101. [redacted] | root | 2021-12-15 15:24:48 2021-12-15 15:24:53 | gordan | chen chen | 4秒 0.45KB | 0 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。

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) 应对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 [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。

运维审计

字符会话 图形会话 文件传输 数据库 **运维任务**

近7天 近14天 **近30天** 2022-07-04 ~ 2022-08-02

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 |
|------------|------------|------------|------------|------------|------------|------------|----|-------|
| [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | 结束 | 详情 回放 |
| [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | 结束 | 详情 回放 |

安全计算环境

身份鉴别

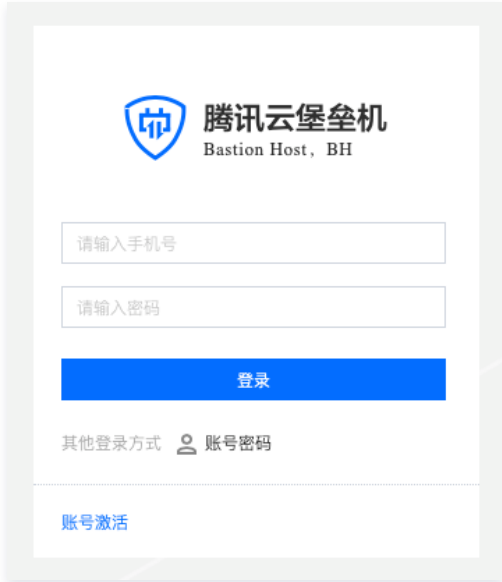
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

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 [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 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
✕

用户名

姓名

认证方式

手机号 ❗

手机号重复

邮箱

用户组

有效时间 📅 ℹ️

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 [堡垒机控制台](#)，在左侧导航选择系统设置 > 认证设置 > 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）。

堡垒机

- ☰ 概览
- ☑️ 开通服务
- 📁 资产管理
- 👤 用户管理
- 👤 权限管理
- 📄 审计管理
- ⚙️ 系统设置
 - 访问白名单
 - 安全设置
 - 认证设置
 - 数据维护

认证设置

本地认证
双因子认证
LDAP

| | |
|----------|---|
| 密码最小长度 | 10 |
| 密码复杂度 | 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 | 30天 ℹ️ |
| 历史密码相同检查 | 5 ℹ️ |

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 [堡垒机控制台](#)，在左侧导航选择系统设置 > 安全设置，进入安全设置页面。

2. 在安全设置页面，查看密码错误锁定和锁定时长。



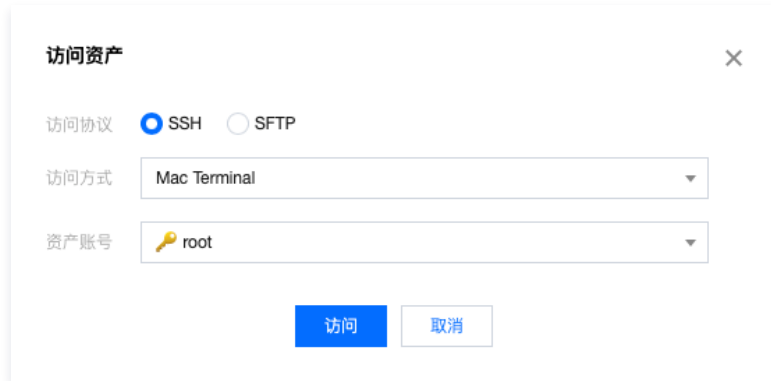
c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。

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 [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。



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 [堡垒机控制台](#)，在左侧导航选择系统设置 > 认证设置 > 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

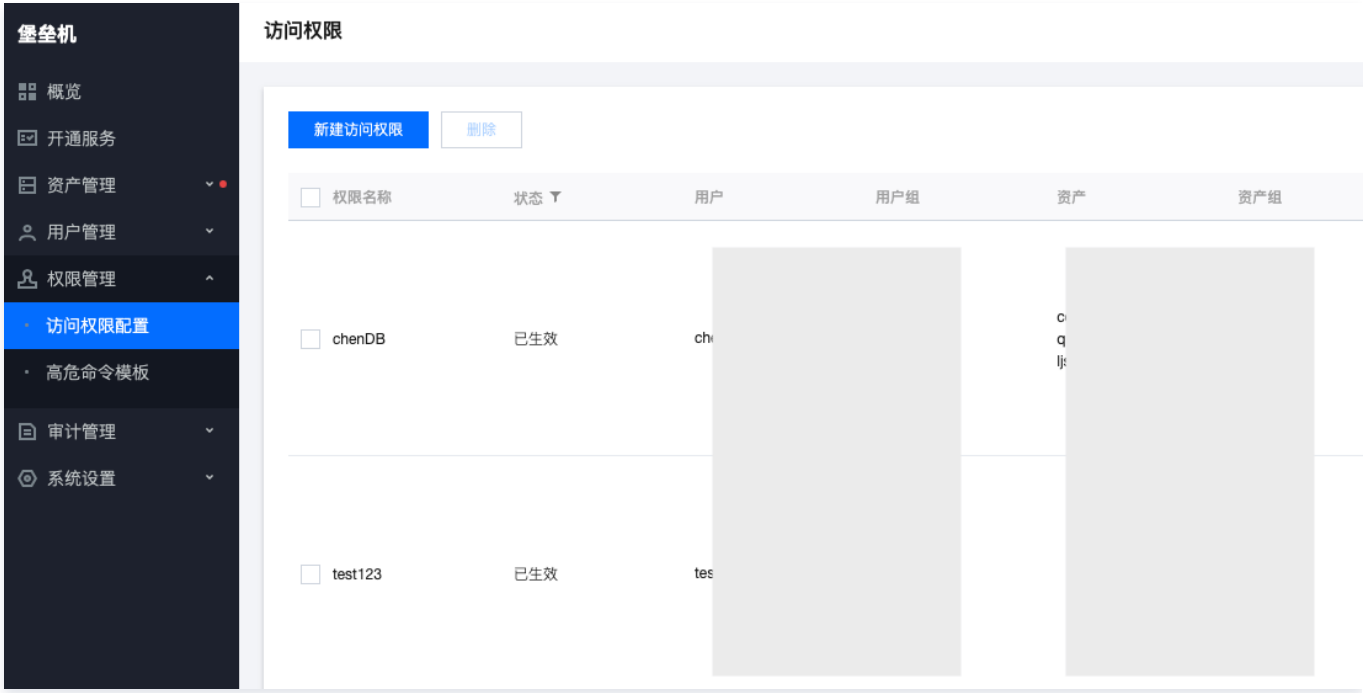
a) 应对登录的用户分配账户和权限；

本条款主要考察：

- 是否给登录的用户分配账户
 - 1.1 登录 [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 [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。
 - 1.2 在访问权限配置页面，查看用户权限分配情况。



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 [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。



- 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；

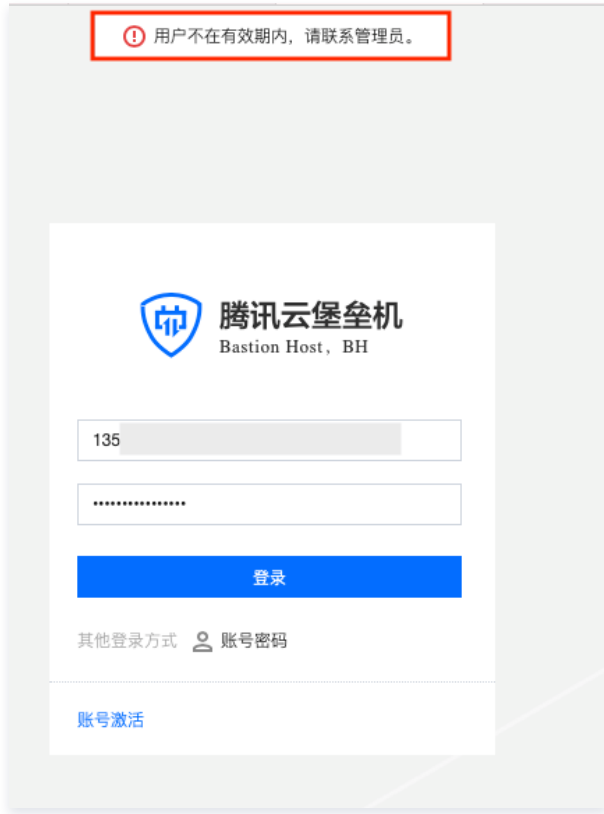
本条款主要考察：账户过期之后，能否继续使用。

说明

请提前准备一个已经到期的用户。

1. 登录 [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。

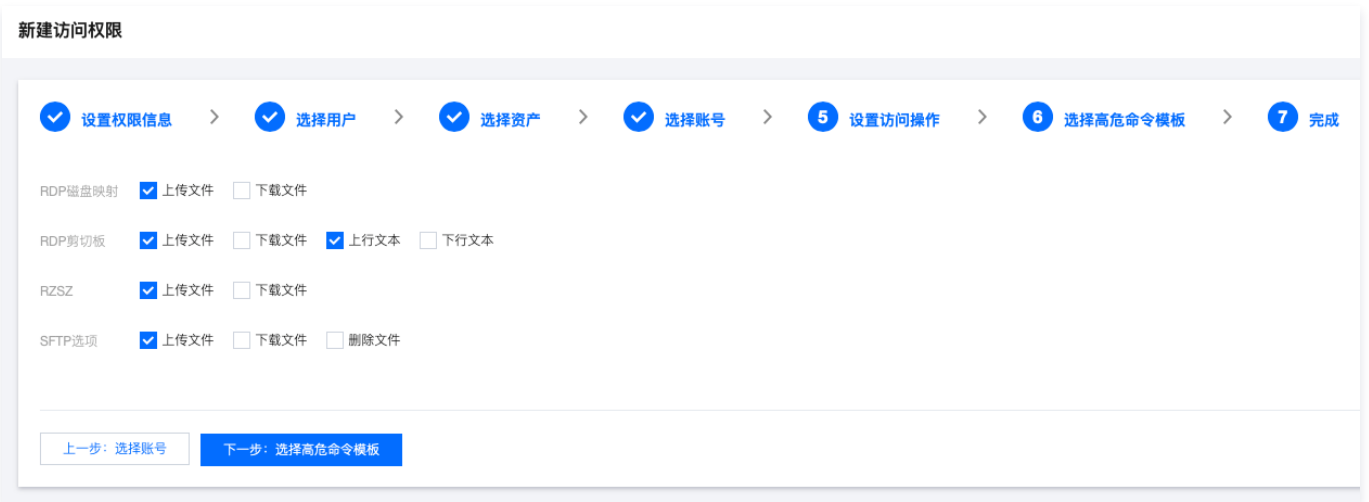
3. 使用浏览器访问运维页面，使用已过期的用户尝试进行登录，此时用户无法登录，并且页面提示“用户不在有效期内”，证明过期的用户无法继续使用。



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 **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。



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 >
 6 选择高危命令模板 >
 7 完成

请选择模板 已选择 (0)

| 模板名称 | 禁止执行的命令 |
|---------------------------------|---|
| <input type="checkbox"/> 7777 | 222 |
| <input type="checkbox"/> 新建 | top |
| <input type="checkbox"/> 777 | whoami |
| <input type="checkbox"/> 测试高危命令 | rm * shutdown * |
| <input type="checkbox"/> xss | <script>alert('XSS');</script> |
| <input type="checkbox"/> 高危 | rm * reboot* <script>alert(123);</script> |

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 [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 >
 2 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

用户 用户组

选择用户 已选择 (0)

搜索用户名/姓名

| 用户名 | 姓名 | 手机 |
|------------------------------|-----|-----|
| <input type="checkbox"/> ch | ch | 135 |
| <input type="checkbox"/> cw | cw | 158 |
| <input type="checkbox"/> tes | tes | 166 |
| <input type="checkbox"/> as | qw | 136 |
| <input type="checkbox"/> tes | cw | 187 |
| <input type="checkbox"/> pe | pe | 131 |
| <input type="checkbox"/> vu | 远 | 173 |

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

| ID/资产名 | 资产IP | 地域 | 资产类型 |
|---------------------------------------|----------|----|------------------------------------|
| <input type="checkbox"/> ins-gon | 192. | 广州 | TencentOS Server 2.4 |
| <input type="checkbox"/> ins-gon-test | 192.119. | 广州 | Windows Server 2008 R2 企业版 SP1 64位 |
| <input type="checkbox"/> ins-gon | 192. | 广州 | Debian 10.2 64位 |
| <input type="checkbox"/> ins-gon | 192.81.7 | 广州 | CentOS 7.9 64位 |

已选择 (0)

[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 [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](#)

[近7天](#)
[近14天](#)
[近30天](#)
2022-07-04 ~ 2022-08-02

| 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 |
|------|------|------|-----------|------|--------|-----------|----|---------------------------------------|
| ... | ... | ... | ... | ... | ... | ... | 结束 | 详情 回故 |
| ... | ... | ... | ... | ... | ... | ... | 结束 | 详情 回故 |

3. 单击日志检索，进入日志搜索页面，可查看用户对堡垒机的操作日志。

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](#)
2021-10-31 ~ 2021-11-29

| 时间 | 用户名/姓名 | 来源IP | 登录方式 | 登录结果 |
|------------|--------|------|---------|------|
| 2021-11-26 | ... | ... | web页面登录 | 失败 |
| 2021-11-26 | ... | ... | web页面登录 | 失败 |
| 2021-11-26 | ... | ... | web页面登录 | 失败 |
| 2021-11-26 | ... | ... | 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 [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 | 10x管i | 9.2 | 修改用户 | 成功 |
| 2021-11-23 20:19:35 | tescw | 120 | 激活OTP | 成功 |
| 2021-11-23 20:16:34 | 10x管i | 9.7 | 重置用户密码 | 成功 |
| 2021-11-19 16:41:10 | 10x管i | 9.2 | 修改登录设置 | 成功 |
| 2021-11-19 14:50:17 | 10x管i | 9.2 | 修改密码强度设置 | 成功 |

共 5 条 20 条 / 页 1 / 1 页

其他

堡垒机用户密码的加密方式：采用 BCrypt 算法加密保存。

传统型堡垒机

删库等高危命令阻断

最近更新时间：2022-11-17 15:16:20

操作场景

本文为您详细介绍如何在堡垒机配置字符命令控制策略，以阻断删库等高危命令。

步骤1：创建命令控制策略

1. 在浏览器输入堡垒机 IP 地址，并输入账号和口令登录堡垒机。
2. 单击**策略管理**，进入策略管理页面。
3. 选择**控制策略 > 字符命令控制策略**，进入字符命令控制策略设置页面。
4. 单击**新建**，开始添加策略。
 - 策略名称：填写策略名称。
 - 操作时间：策略生效时间范围。
 - 资源 IP：托管在堡垒机系统的资源 IP。
 - 命令（正则表达式）：输入具体的命令，建议使用正则表达式来填写。
 - 类型：允许、需审批和阻断命令。

策略列表

新建 删除

| 序号 | 策略名称 |
|------|------|
| 暂无数据 | |

新建字符命令控制策略

基本信息

策略名称 *

添加规则

操作时间

资源IP

命令(正则表达式)

类型 允许 需审批 阻断命令 添加至规则表

规则列表

| 序号 | 操作时间 | 资源IP | 命令 |
|----|------|------|----|
|----|------|------|----|

其他信息

提交测试 查询

保存 关闭

5. 确认配置信息无误后，单击**添加至规则表**。
6. 单击**保存**，即可完成策略的创建。

步骤2：绑定策略

1. 单击组织结构类型为“工作组”的组织结构，选择**绑定策略**页签，进入绑定策略页面。
2. 您可以在下拉框选择已添加到系统的策略，也可以单击 **+**，添加相关策略。

选择绑定策略

| | | | | |
|-----------|---|--|---|---|
| 资源账号策略 | ? | | ▼ | + |
| 字符命令控制策略 | ? | | ▼ | + |
| 图形控制策略 | ? | | ▼ | + |
| FTP传输控制策略 | ? | | ▼ | + |
| 访问时间策略 | ? | | ▼ | + |
| 字符审计策略 | ? | | ▼ | + |
| 图形审计策略 | ? | | ▼ | + |
| FTP审计策略 | ? | | ▼ | + |
| 数据库命令控制策略 | ? | | ▼ | + |

保存

3. 此处我们在**字符命令控制策略**中，下拉选择我们步骤1创建的策略。

4. 单击**保存**，即可完成策略绑定。

配置应用发布收纳管理数据库

最近更新时间：2022-11-17 15:20:31

本文档将指导您配置应用发布收纳管理数据库。

前提条件

- 准备一台 Windows Server 2012 R2 作为应用发布服务器，并在 Windows 机器中安装好连接数据库工具（本文档以 Navicat for MySQL 为例进行说明）。
- 需要在安全组中放通堡垒机到应用发布服务器的10017、3389、443端口；应用发布服务器到堡垒机的3393、443端口，堡垒机到数据库端口放通，本地到堡垒机放通3392。详情请参见 [创建安全组](#)。
- 已购买并激活 Windows 服务器的远程桌面服务。

⚠ 注意

未购买远程桌面服务时，只有120天试用期，超过试用期后需购买并激活 Windows 服务器的远程桌面服务。

操作步骤

1. 登录腾讯云 [堡垒机控制台](#)，并使用管理员账号登录堡垒机。
2. 单击[资源管理](#)，进入资源管理页面。
3. 添加应用发布服务器。
 - 3.1 在资源管理页面，单击[新建](#)，进入资源添加页面。
 - 3.2 在新建资源页面，选择资源类型（Windows）、资源版本、输入资源名称、勾选“作为应用发布服务器”，并根据需求填写其他字段，详情请参见 [添加资源](#)。

📌 说明

“支持网络级别身份认证（NLA）”：对端服务器开启了该认证后，RDP 会话发起方需要先认证用户名密码，才能登录 RDP 会话。若服务器开启该认证，堡垒机也必须开启。若服务器没开，堡垒机建议不要开启。

基本信息

| | | | |
|------------|---|-------------------------------------|-----------------|
| 资源类型 | * | Windows | ▼ |
| 资源版本 | * | Windows-Essential-Business-Server | ▼ |
| 资源名称 | * | 应用发布服务器 | |
| | | <input checked="" type="checkbox"/> | 作为应用发布服务器 |
| | | <input checked="" type="checkbox"/> | 支持网络级别身份验证（NLA） |
| 管理IP（IPv4） | | | ping |
| 管理IP（IPv6） | | | ping |
| 选择所属组 | | 腾讯集团 | ▲ + ▼ - |
| 计算机名 | | | |
| 字符集 | | GBK | ▼ |
| 超时时间 | | 5 | 单位：秒 |

- 3.3 填写完成后，单击[保存](#)，即可完成添加应用发布服务器。

4. 添加数据库资源，以 MySQL5.7 为例进行说明。

4.1 在资源管理页面，单击**新建**，进入资源添加页面。

4.2 在新建资源页面，根据需求选择资源类型（数据库）、资源版本、输入资源名称、实例或数据库名称、访问端口（此处填写 MySQL 默认端口3306），并根据需求填写其他字段，详情请参见 [添加资源](#)。

基本信息

资源类型 * 数据库

资源版本 * Mysql-5.7

资源名称 * 数据库资源

实例名/数据库名 * MySQL

管理IP (IPv4) ping

管理IP (IPv6) ping

访问端口 * 3306

选择所属组 腾讯集团

计算机名

字符集 GBK

超时时间 5 单位: 秒

保存 关闭

4.3 填写完成后，单击**保存**，即可完成添加数据库资源。

5. 为数据库绑定相应的驱动并配置应用发布工具。

5.1 在资源管理页面，单击**资源类型配置**，进入资源类型配置页面。







5.2 在资源类型配置页面的左侧导航中，单击**数据库**，选择已添加的数据库资源版本，绑定相应的驱动，并单击右侧扩展登录  按钮。

资源管理 资源类型配置 x

Unix/Linux

Windows

数据库

| 序号 | 资源版本 | 创建方式 | 绑定驱动 | 扩展登录 |
|--------------------------|---------------|------|------------|---|
| <input type="checkbox"/> | DB2-V7.1 | 内置 | DB2-x |  |
| <input type="checkbox"/> | DB2-V8.1 | 内置 | DB2-x |  |
| <input type="checkbox"/> | Informix-12.1 | 内置 | Informix-x |  |
| <input type="checkbox"/> | Mysql-5.5 | 内置 | MySQL-x |  |
| <input type="checkbox"/> | Mysql-5.6 | 内置 | MySQL-x |  |
| <input type="checkbox"/> | Mysql-5.7 | 内置 | MySQL-x |  |

5.3 (可选) 在扩展登录信息页面，单击**添加工具**，输入应用发布工具名称。

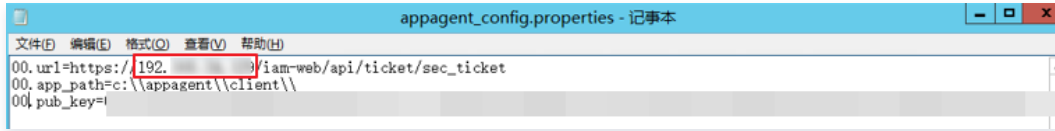
说明

堡垒机已默认配置应用发布工具，若有特殊需求可自行配置。

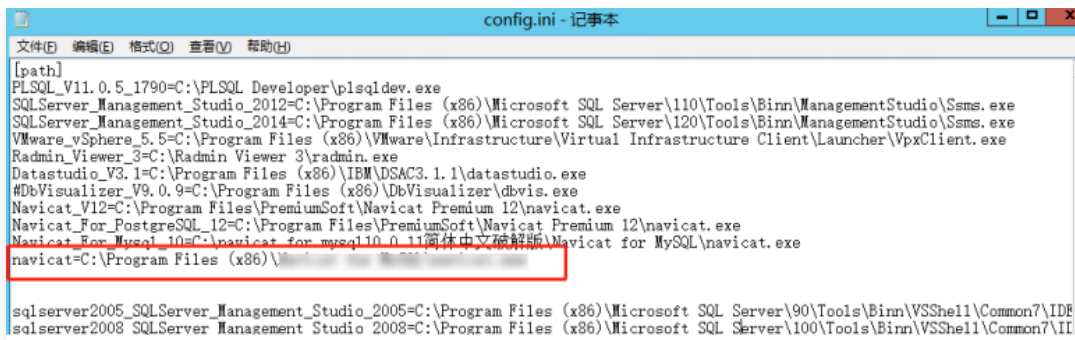


5.4 单击保存，即可完成扩展登录信息配置。

6. 在已添加的应用发布服务器中，修改 c:\appagent\appagent_config.properties 的 IP 为堡垒机 IP，堡垒机 IP 查看方式，请参见 [服务器配置](#)。



7. 在已添加的应用发布服务器中，编辑 C:\appagent\client\config.ini 文件，配置连接数据库工具路径。



8. 进入运维平台，选择数据库资源登录。

8.1 登录腾讯云 [堡垒机控制台](#)，使用运维账号登录堡垒机。

说明

若忘记运维账号及密码，可与管理员联系进行获取。

8.2 单击授权列表，进入资源列表页。

8.3 找到您需要登录的数据库资源，在其右侧单击登录，进行登录配置。

| <input type="checkbox"/> | 序号 | 资源名称 | IP | 资源类型 | 登录 |
|--------------------------|----|-------|---------------|---------------------|---------|
| <input type="checkbox"/> | 1 | 数据库资源 | 192.168.1.100 | Debian-GNU-Linux-9 | 登录 历史 ▾ |
| <input type="checkbox"/> | 2 | 数据库资源 | 192.168.1.100 | Windows-Server-2016 | 登录 历史 ▾ |

8.4 进入配置登录页面，输入账号（运维账号）、口令（运维密码）、选择 WEB 工具，选择应用发布工具，全部设置完后，单击登录，即可成功登录系统。

配置登录 ×

选择IP

协议

账号

口令

工具

应用发布

应用发布工具

选择分辨率

超时时间 秒

服务器真实密码隐藏

最近更新时间：2022-11-17 15:15:49

操作场景

计划管理用于定期修改对资源账号进行口令变更，并把账号口令导出文件发送到指定设备或者指定用户邮箱，因此可以通过计划管理功能实现服务器真实密码隐藏。本文为您介绍如何添加计划任务、为任务添加资源账号、启动任务以及查看计划任务等。

步骤1：添加任务

1. 在浏览器输入堡垒机 IP 地址，并输入账号和口令登录堡垒机。
2. 单击**计划管理**，进入任务计划管理页面。
3. 单击**新建**，进入计划任务添加页面，输入如下相关配置信息：
 - **计划所有者**：选择本系统
 - **执行规则**：可以选择单次执行、按周执行、按月执行。
 - **口令规则**：
 - 指定策略：已添加到系统的口令策略。
 - 使用资源策略：已绑定到资源上的口令策略。
 - **任务类型**：
 - 口令变更：通过此计划任务，修改指定资源的账号口令。
 - **FTP 发送**：可将账号导出文件发送到指定的 FTP 设备。
 - **邮件发送**：将账号口令导出文件发送到指定用户的邮箱。

计划管理 新建计划 ×

基本信息

任务调度

计划名称 * 请输入计划名称

计划所有者 10.0.0.9

执行规则 单次执行 按周执行 按月执行

执行时间

任务信息

任务类型 口令变更

口令规则 指定策略 使用资源策略

选择口令策略

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)

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)

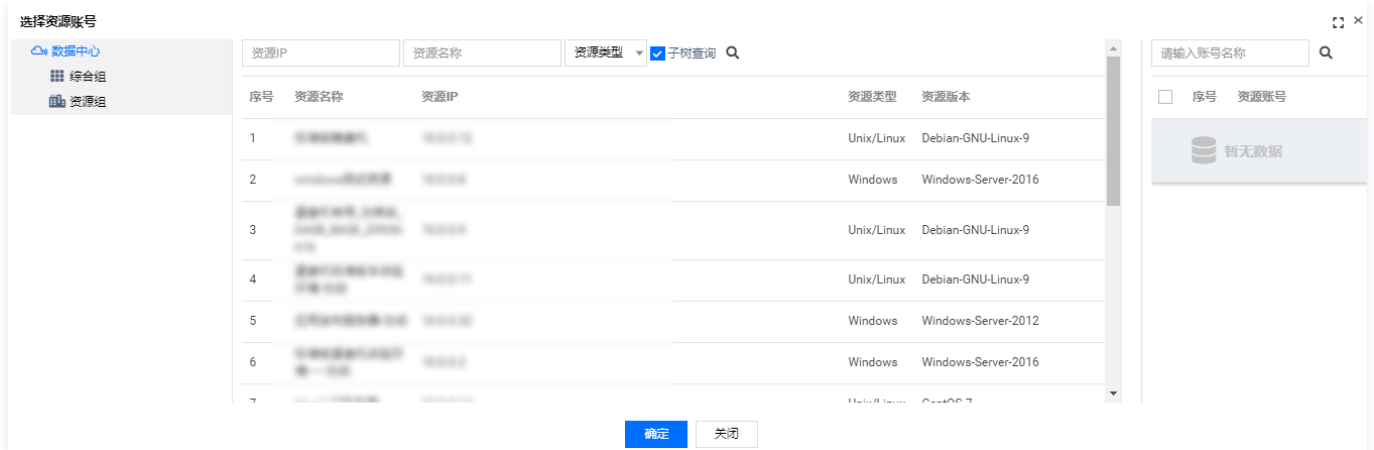
保存 关闭 保存并添加资源

4. 单击**保存**，即可创建计划。

步骤2：为任务添加资源账号

1. 单击**计划管理**，进入计划管理页面。

- 在计划管理页面，找到需要添加资源账号的计划任务，单击 ，进入资源账号添加页面。
- 在资源账号页面，单击绑定资源账号，在右侧资源账号中选择账号，单击确定，即可为该计划添加资源账号。在计划执行时，将修改这些账号的口令。



步骤3：启动任务

- 单击计划管理，进入计划管理页面
- 在计划任务列表，如下图所示，单击 将任务启动。

| <input type="checkbox"/> | 序号 | 计划类型 | 计划名称 | 状态 | 编辑 | 账号 | 启动/停止 | 操作日志 | 执行日志 |
|--------------------------|----|------|------|----|----|----|-------|------|------|
| <input type="checkbox"/> | 1 | 口令变更 | 2 | 停止 | | | | | |

步骤4：查看操作日志

在堡垒机上查看计划的变更记录，您可通过操作日志进行查看。

- 单击计划管理，进入计划管理页面。
- 找到您要查看操作日志的计划，在其所在行中，单击 ，进入操作日志页面。

| 序号 | 时间 | 计划类型 | 计划名称 | 来源 | 操作 |
|----|---------------------|------|------|------|--------|
| 1 | 2020-06-09 16:26:54 | 口令变更 | | 手工操作 | 停止计划 |
| 2 | 2020-06-09 16:26:53 | 口令变更 | | 手工操作 | 停止计划 |
| 3 | 2020-06-09 16:25:09 | 口令变更 | | 手工操作 | 启动计划 |
| 4 | 2020-06-09 16:15:06 | 口令变更 | | 手工操作 | 添加基本信息 |

总条目数: 4

- 在操作日志页面，您可查看该计划的操作记录日志。

步骤5：查看执行日志

查看在堡垒机上配置的口令变更计划是否成功执行等其他记录，您可查看计划执行日志。

- 单击计划管理，进入计划管理页面。
- 找到您要查看操作日志的计划，在其所在行中，单击 ，即可打开执行日志页面。
- 在执行日志页面，您可查看该计划执行的记录。

计划管理 执行日志【测试计划】 x

起始时间 结束时间 Q

| 序号 | 开始时间 | 结束时间 | 执行条目 | 成功条目 | 失败条目 | 忽略条目 | 执行内容 |
|----|---------------------|---------------------|------|------|------|------|------|
| 1 | 2020-05-27 15:39:27 | 2020-05-27 15:39:30 | 0 | 0 | 0 | 0 | ☰ |
| 2 | 2020-05-27 14:04:09 | 2020-05-27 14:04:10 | 0 | 0 | 0 | 0 | ☰ |

安全事件事后追溯

最近更新时间：2022-10-31 17:29:56

操作场景

具有审计权限的管理员，可以查看审计管理模块，对用户相关的管理日志和操作行为日志进行查看和安全评估，并生成各类统计报表。本文为您介绍如何查看在线和历史会话审计。

在线会话审计

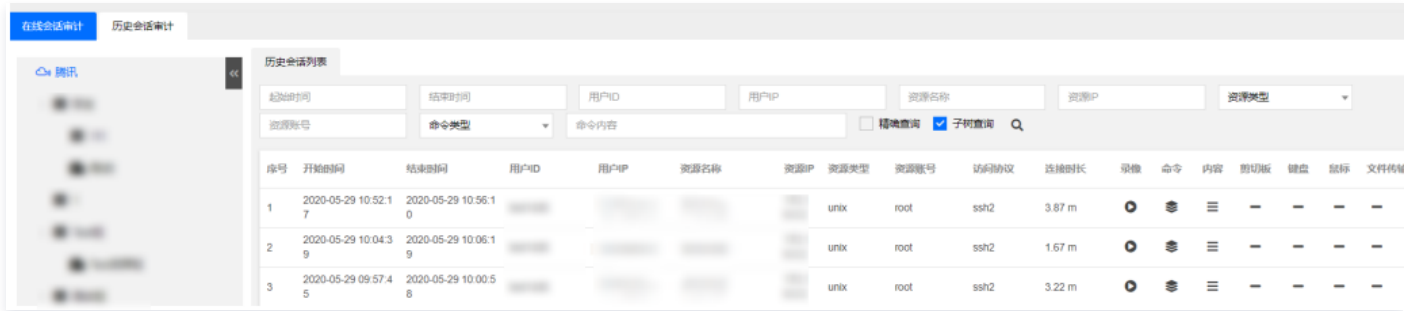
1. 在浏览器输入堡垒机 IP 地址，并输入账号和口令登录堡垒机。
2. 在左上角单击**审计平台**，进入审计平台，单击**操作行为审计**，进入操作行为审计页面。
3. 单击**在线会话审计**，进入在线会话查看页面。可以查看在线会话相关信息，例如开始时间、用户ID、资源名称、资源类型、资源登录账号、访问协议、监控、播放录像等内容。



4. 审计用户能以视频的方式实时地监控运维用户的所有操作。单击审计列表右侧的**监控**按钮，即可在线监控运维用户的所有操作。

历史会话审计

1. 在浏览器输入堡垒机 IP 地址，并输入账号和口令登录堡垒机。
2. 在左上角单击**审计平台**，进入审计平台，单击**操作行为审计**，进入操作行为审计页面。
3. 单击**历史会话审计**，进入历史会话查看页面，可以查看历史会话相关内容，例如开始时间、结束时间、用户 ID、用户 IP、资源类型、名称、资源账号、访问时长、查看录像、命令记录、内容、文件传输等信息。



等保最佳实践

最近更新时间：2022-03-03 16:51:29

为助力企业等保合规，本文为您介绍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

已购买传统型堡垒机，并完成了 [初次上线配置](#)。

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。堡垒机支持对云服务器运维操作进行监控和审计。

1. 使用管理员账号登录堡垒机，单击 **审计平台 > 操作行为审计 > 历史会话审计**，进入会话审计页面。
2. 在会话审计页面，可查看用户对服务器的运维会话记录。



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. 使用管理员账号登录堡垒机，单击 **审计平台 > 操作行为审计 > 历史会话审计**，进入会话审计页面。
2. 在会话审计页面，可查看用户对服务器的运维会话记录。



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；

1. 使用管理员账号登录堡垒机，单击 **系统管理 > 数据维护 > 审计数据维护**，进入审计数据维护页面。
2. 在审计数据维护页面，可新建备份任务、下载备份的日志。



d) 应对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. 使用管理员账号登录堡垒机，单击 **审计平台 > 操作行为审计 > 历史会话审计**，进入会话审计页面。
2. 在会话审计页面，可查看用户对服务器的运维会话记录。



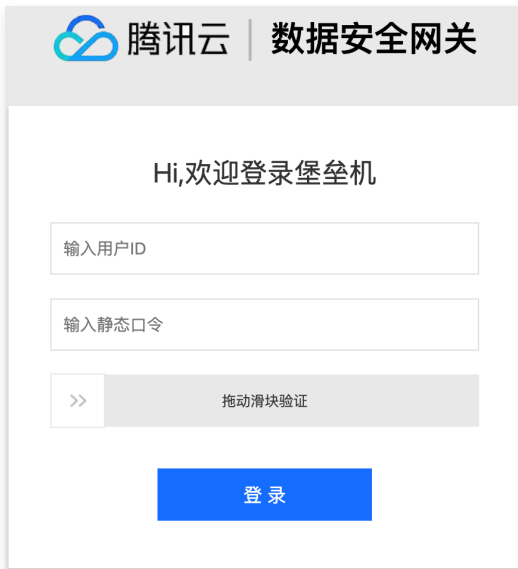
安全计算环境

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：

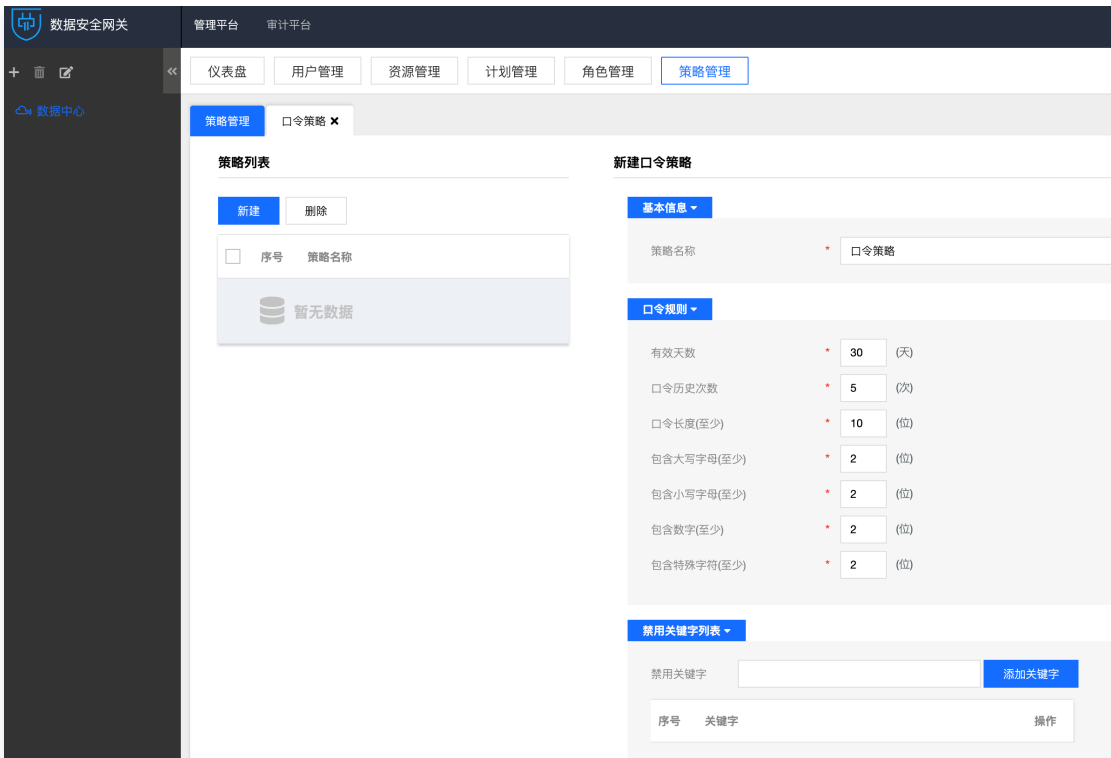
- 是否对登录用户进行身份识别和鉴别
使用浏览器访问堡垒机页面，证明需要对用户身份进行鉴别之后才可正常使用产品功能。



- 身份标识是否具有唯一性
 - 1.1 使用管理员账号登录堡垒机，单击**用户管理**，进入用户页面。
 - 1.2 在用户页面，单击**新建**，尝试输入重复的用户名和手机号，用户无法新建成功。



- 身份鉴别信息是否具有复杂度要求并定期更换
 - 1.1 使用管理员账号登录堡垒机，单击**策略管理** > **普通策略** > **口令策略**，进入策略列表。
 - 1.2 单击**新建**，新建符合要求的口令策略。



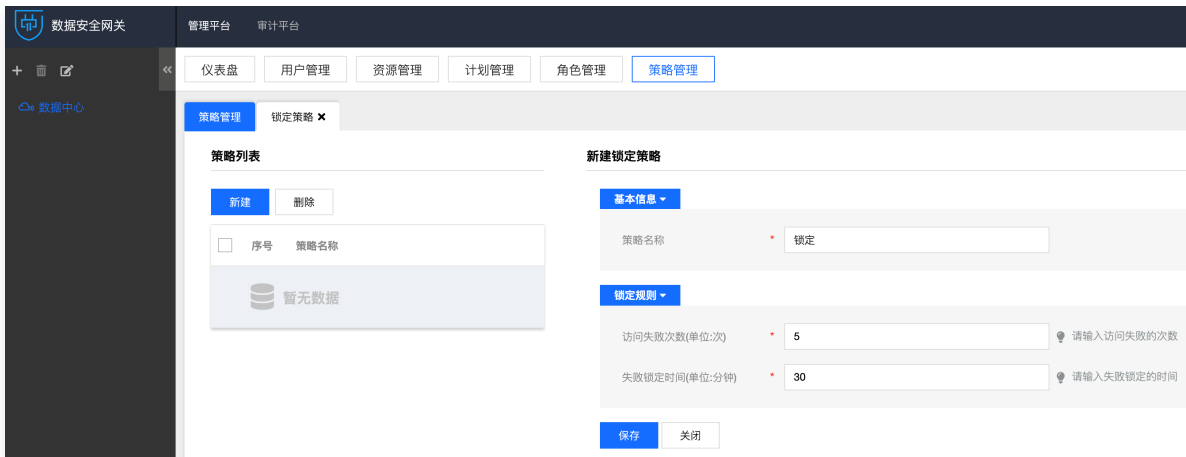
1.3 单击**用户管理**，选择一个用户，单击**编辑**，进入编辑页面之后，单击**设置策略**，设置口令策略。



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. 使用**管理员**账号登录堡垒机，单击**策略管理 > 普通策略 > 锁定策略**，进入策略列表。
2. 单击**新建**，新建符合要求的**锁定策略**。



3. 单击用户管理，选择一个用户，单击编辑，进入编辑页面之后，单击设置策略，设置访问锁定策略。



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。

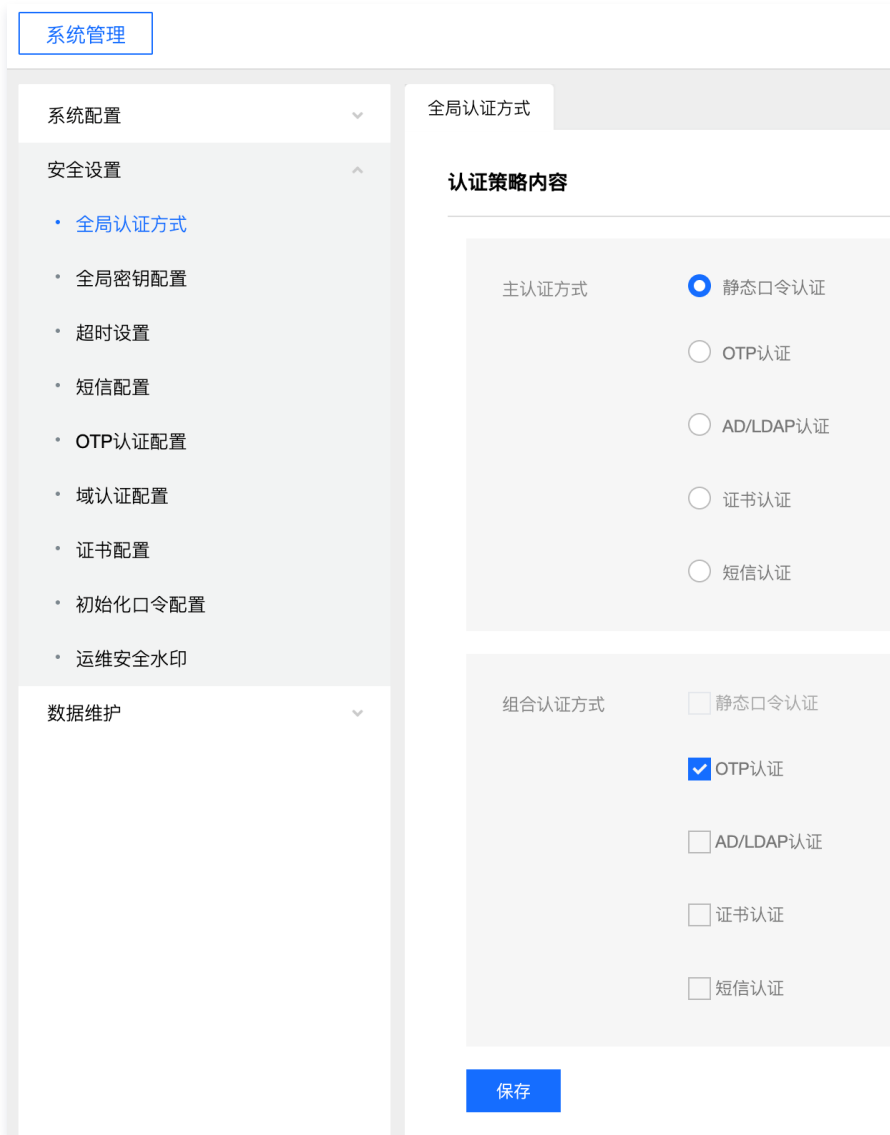
使用运维账号登录堡垒机，登录成功之后，访问一台 Linux 主机，在访问资产弹窗当中，可查看访问协议为 SSH2，为加密的协议。



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. 使用管理员账号登录堡垒机，单击**系统管理** > **安全设置** > **全局认证方式**，进入全局认证方式配置页面。
2. 选择 OTP 作为组合认证方式。



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 使用管理员账号登录堡垒机，单击**用户管理**，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

使用管理员账号登录堡垒机，堡垒机通过工作组对用户进行授权，单击任意工作组，可查看工作组绑定的用户、资源和策略信息。



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 使用管理员账号登录堡垒机，单击用户管理，进入用户页面。

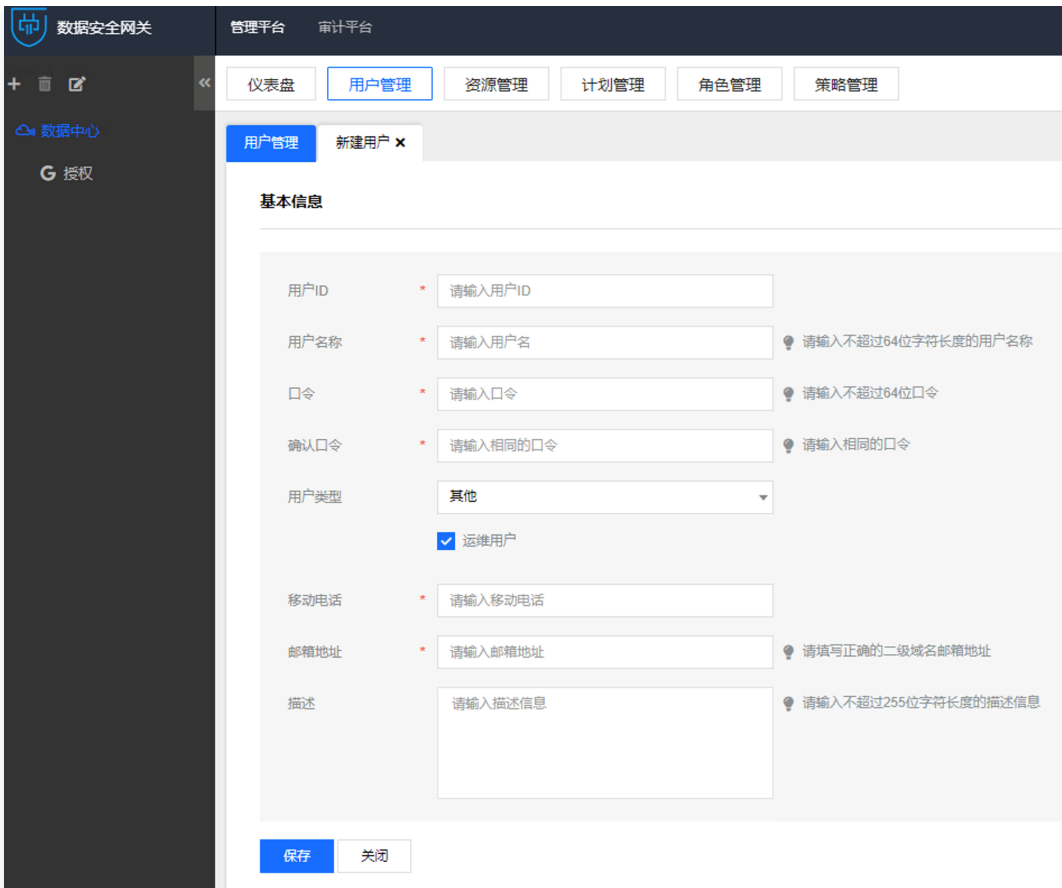
1.2 在用户页面，查看用户信息，可尝试搜索 admin、root、sysadmin、super 等用户名，证明系统内无此默认用户。



• 是否有默认口令

1.1 使用管理员账号登录堡垒机，单击用户管理，进入用户页面。

1.2 在用户页面，单击新建，用户需要管理员设置密码，证明用户无默认口令。



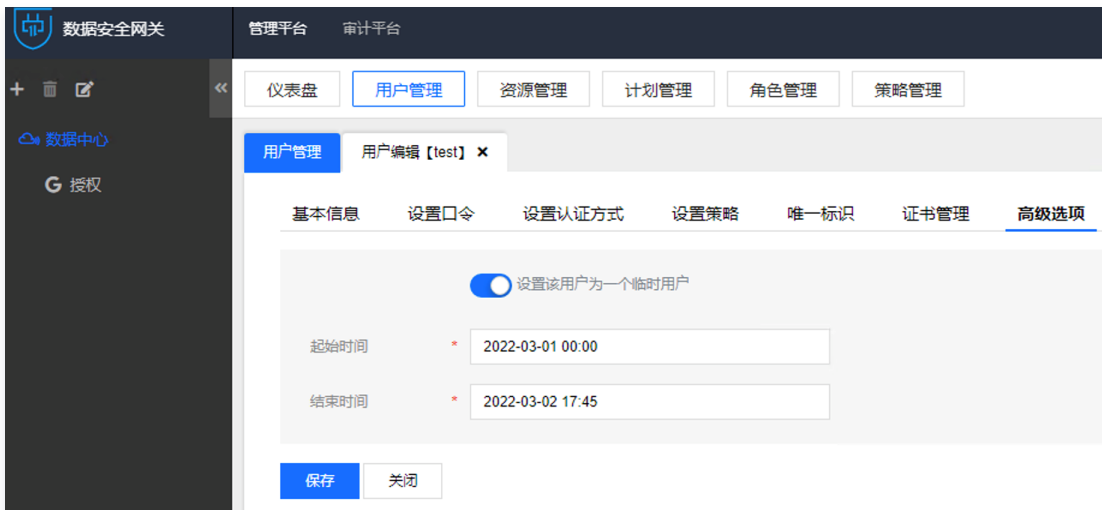
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；

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. 使用管理员账号登录堡垒机，单击**用户管理**，进入用户页面。
2. 在用户页面，单击**编辑 > 高级选项**，查看一个过期用户的用户信息，确认用户已过有效期。



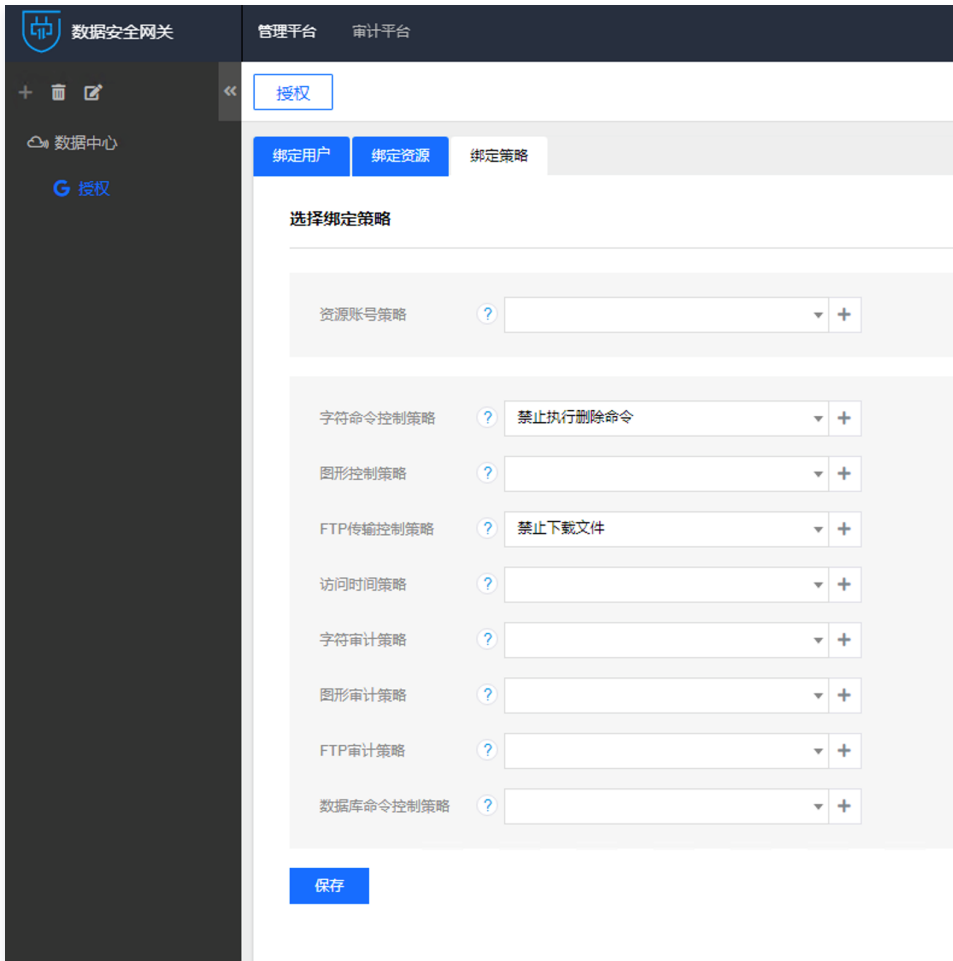
3. 使用已过期的用户尝试进行登录，此时用户无法登录，并且页面提示“临时用户，已到期，失效”，证明过期的用户无法继续使用。



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. 使用管理员账号登录堡垒机，选择一个岗位授权，单击绑定策略。
2. 在绑定策略页面，可设置字符命令、图形访问、文件传输、访问时间等的最小权限。



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。

使用管理员账号登录堡垒机，选择一个岗位授权，可查看岗位授权绑定的用户、资源，证明可以配置访问控制策略。



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. 使用管理员账号登录堡垒机，单击**审计平台**，进入审计页面。
2. 在会话审计页面，可查看认证、管理和操作行为的审计信息。



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. 使用管理员账号登录堡垒机，单击**审计平台 > 管理审计**，进入管理审计页面。
2. 在管理审计页面，可查看用户对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。

