堡垒机

最佳实践

腾讯云

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

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。

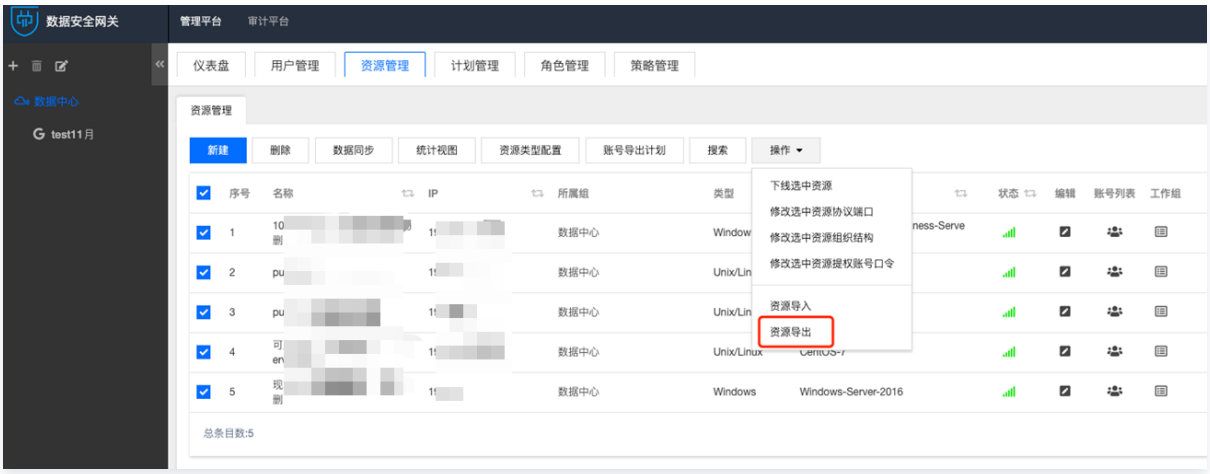
1. 登录 SaaS 型堡垒机控制台，单击侧边栏**资产管理**，进入资产管理页面。
2. 在资产管理页面，单击**同步**。

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。

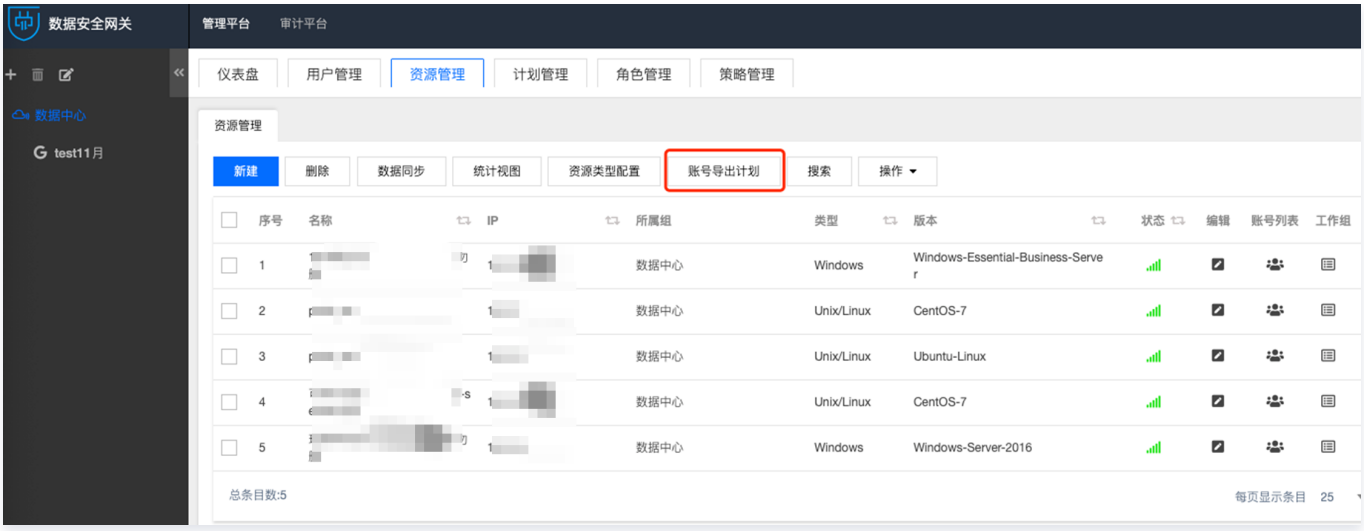
5. 将从传统型堡垒机导出的资产信息复制，并粘贴到 SaaS 型堡垒机导入主机模板当中，需要注意将信息粘贴到对应的位置。模板字段对应关系如下：

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。

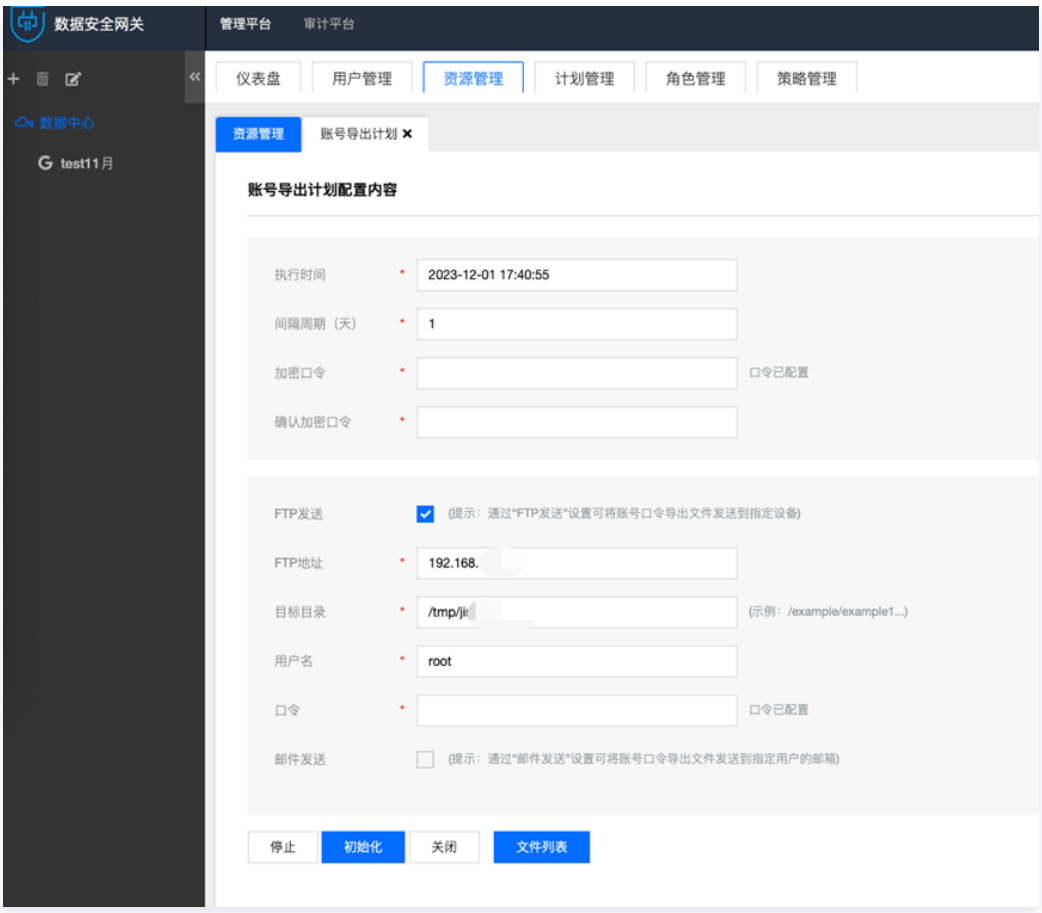
账号数据

账号密码信息，可通过导出/导入方式进行迁移。

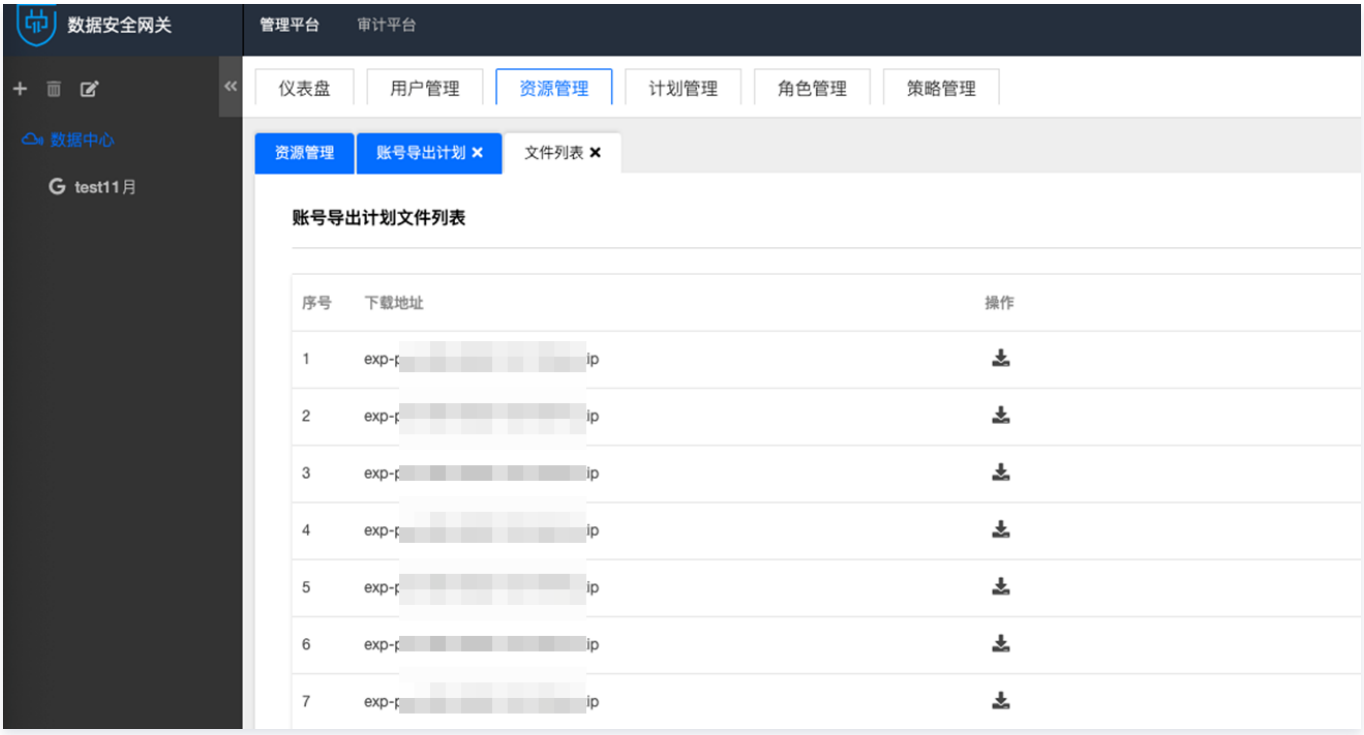
1. 登录传统型堡垒机控制台，单击**资源管理**。
2. 在资源管理页面，单击**账号导出计划**，进入配置页面。



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

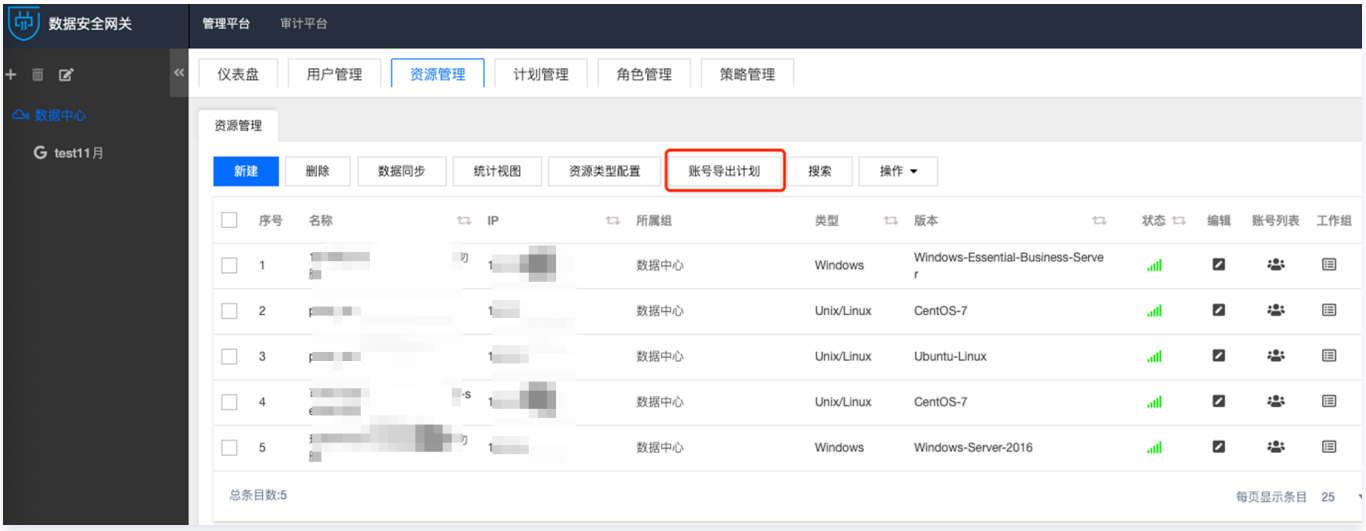
密码	账号密码

> **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。

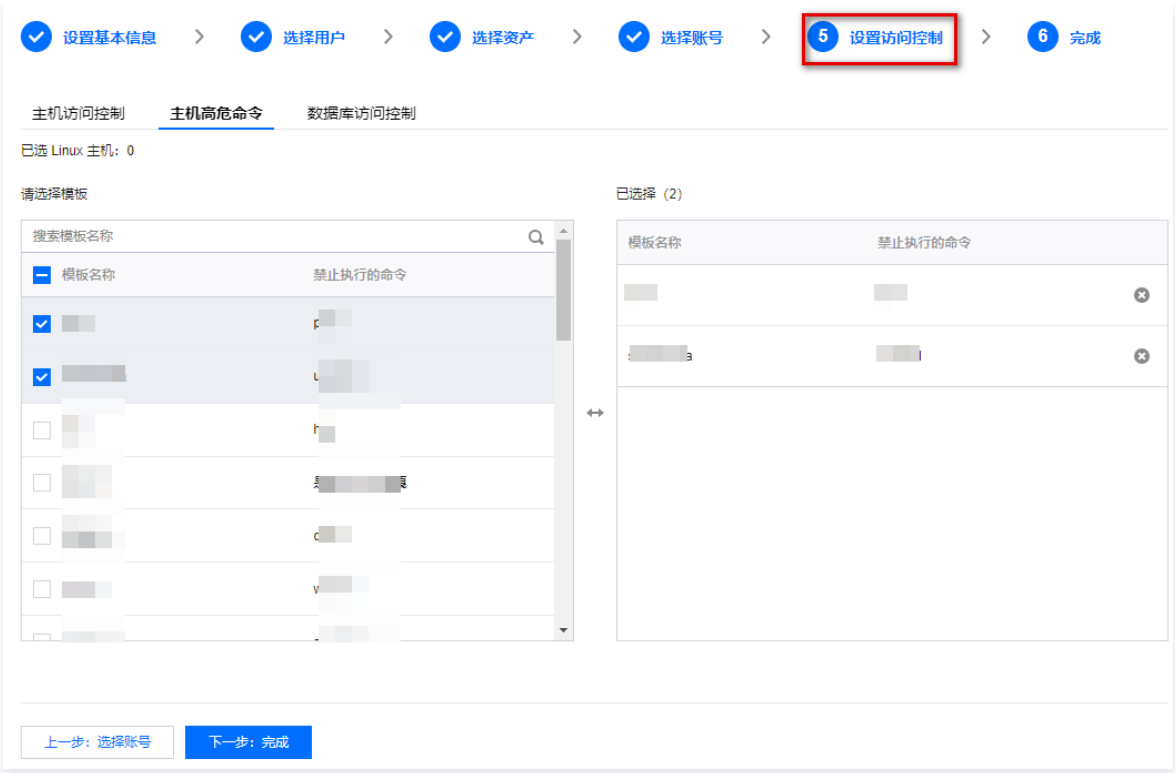
3. 在新建高危命令模板弹窗中，设置对应的模板名称和禁止执行的命令。

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

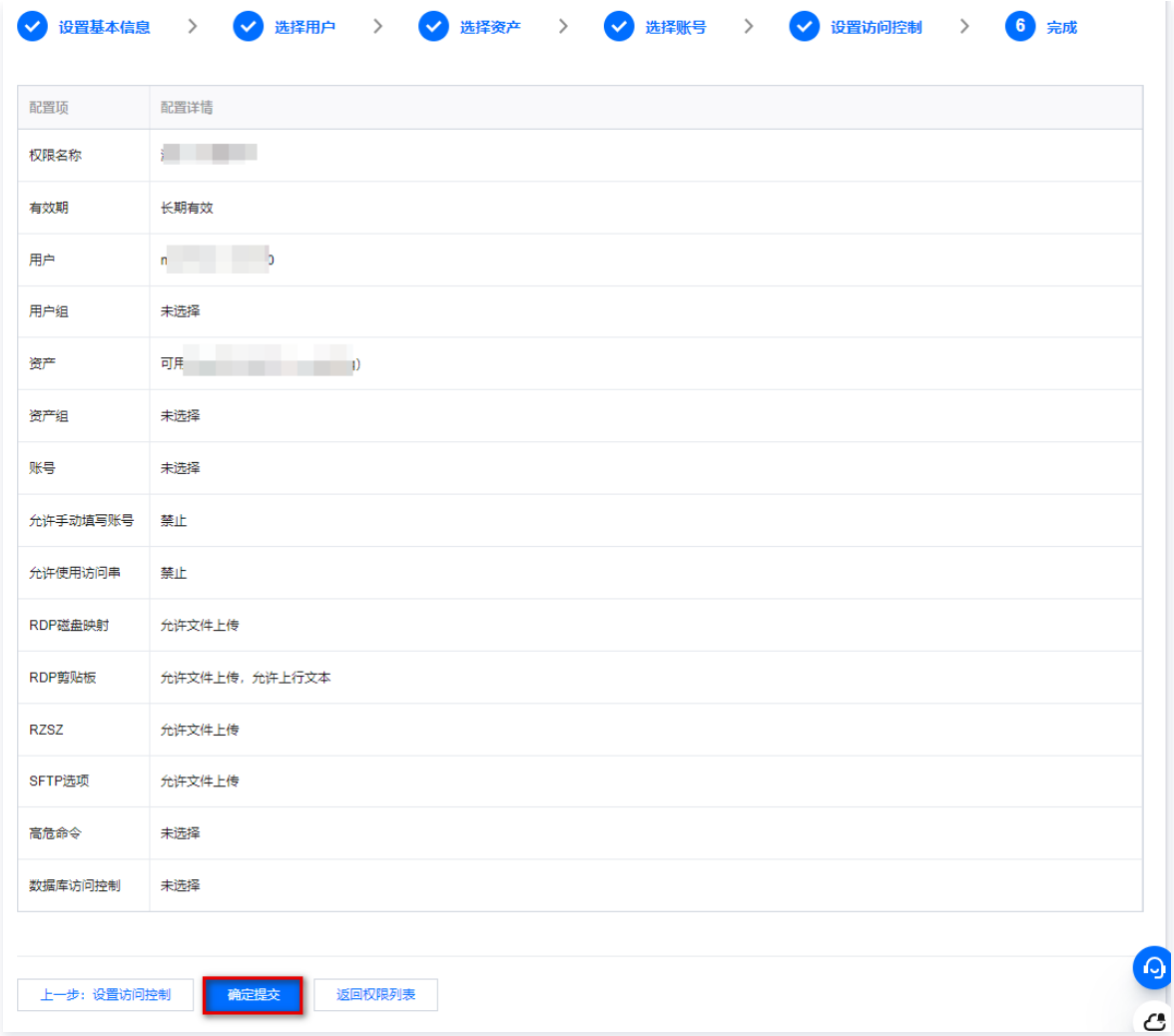
操作场景

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。



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。

安全事故追溯

最近更新时间：2023-10-20 14:46:54

操作场景

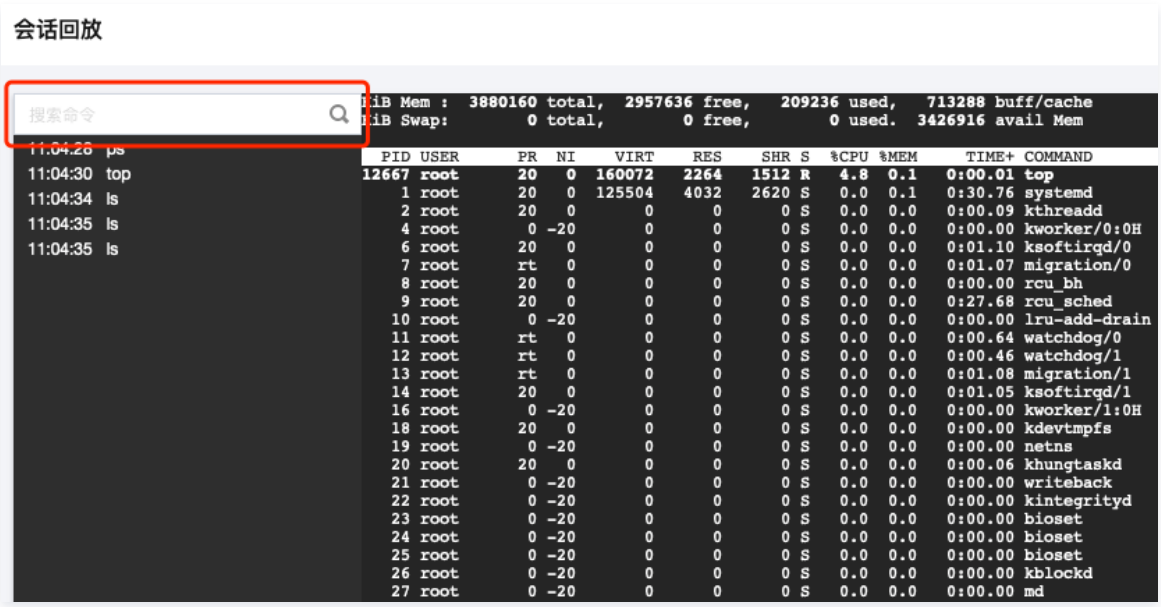
审计模块能够对用户的运维操作行为进行记录，并且展示运维操作日志，当发生安全事故时，可通过审计模块对安全事故进行追溯，本文以字符会话为例为您详细介绍如何审计用户运维操作。

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

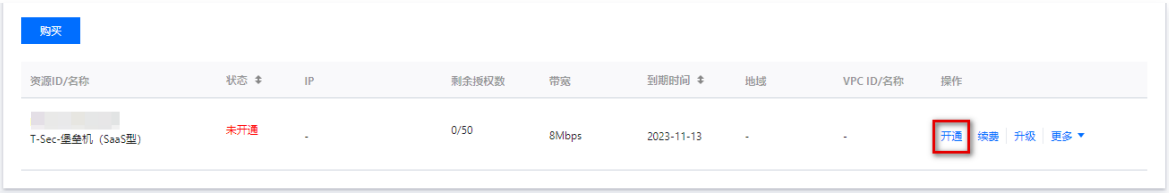
操作场景

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

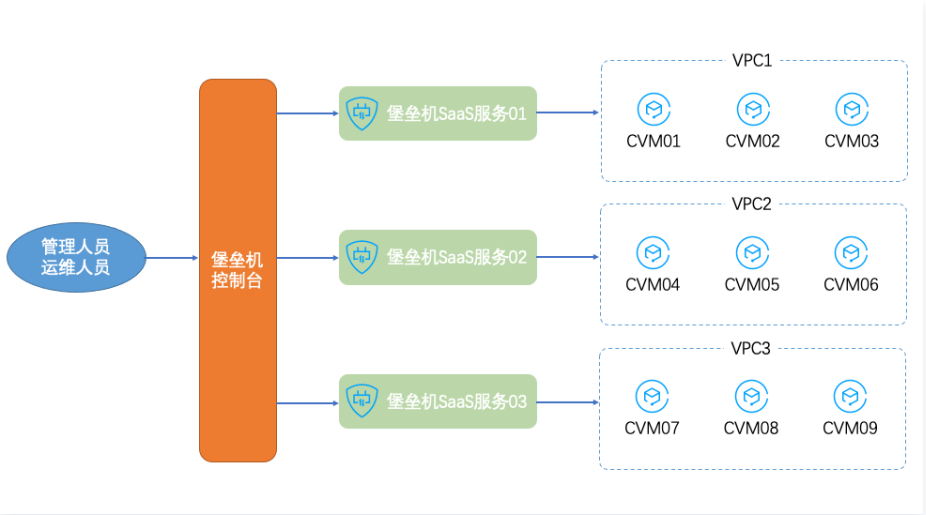
1. 进入 SaaS 型堡垒机控制台，在左侧导航选择**开通服务**，进入开通服务页面。
2. 在开通服务页面，单击**购买**，进入购买页面，选择合适的规格进行购买。

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。

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。



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。

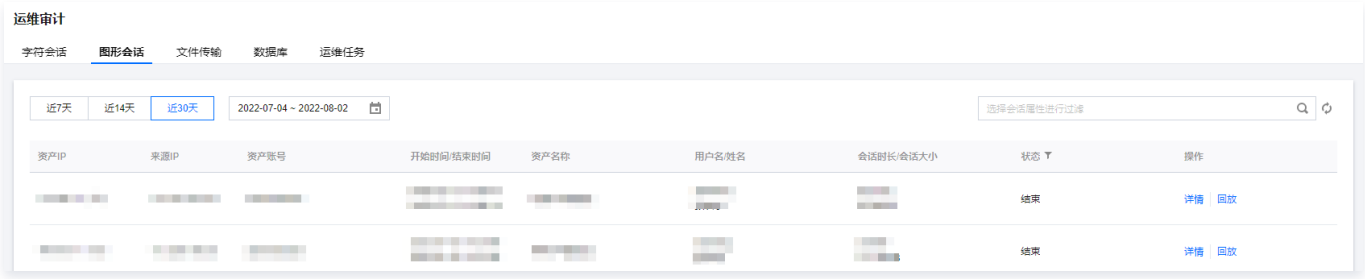
前提条件

已 购买 SaaS 型堡垒机，并完成了 首次登录配置 和 入门操作 。

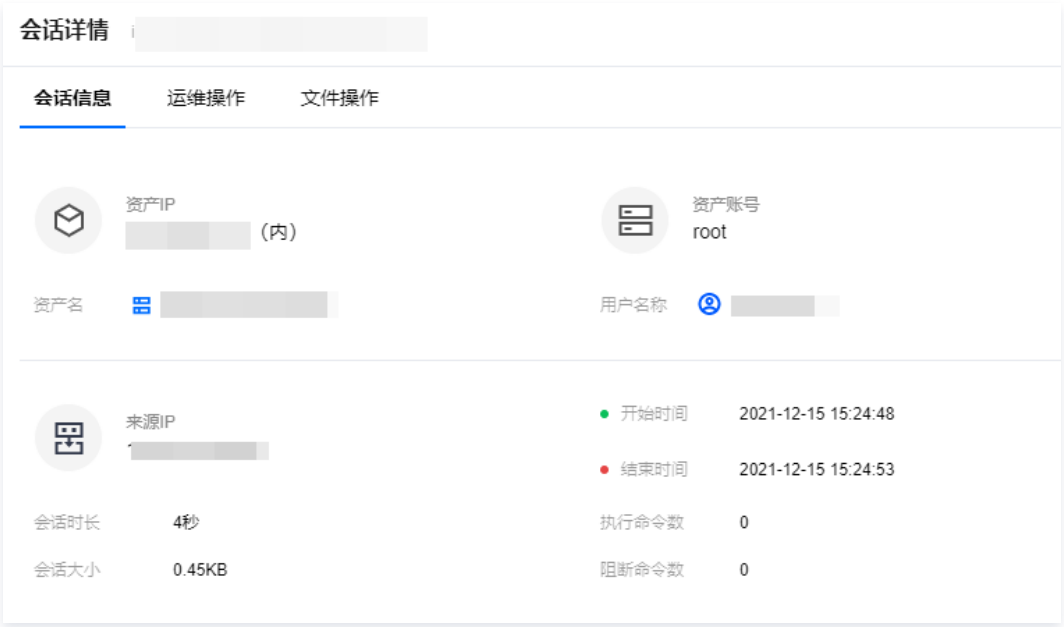
安全区域边界

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。

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）。

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

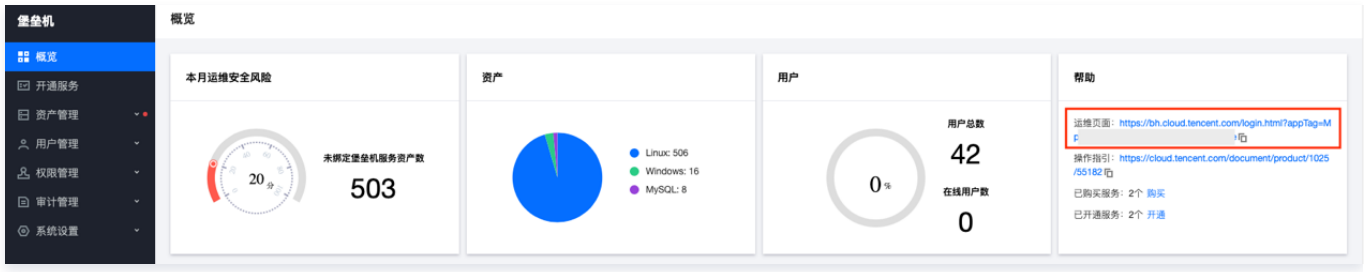
身份鉴别

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。

- **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；

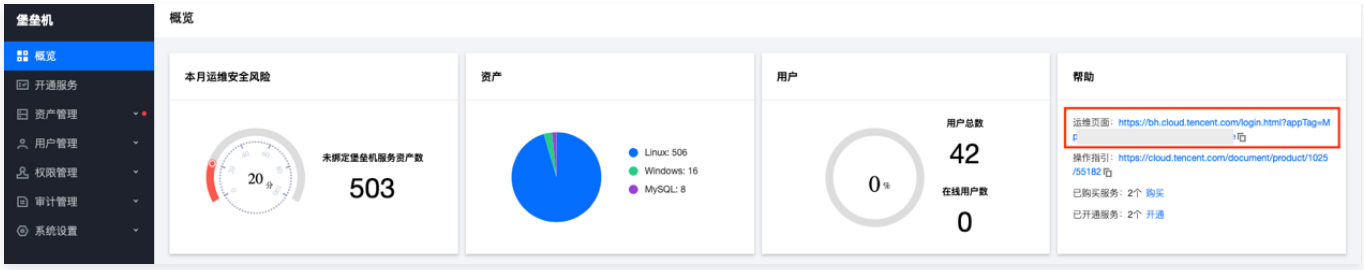
本条款主要考察：是否有登录失败处理能力，以及对登录失败的处理措施。

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。

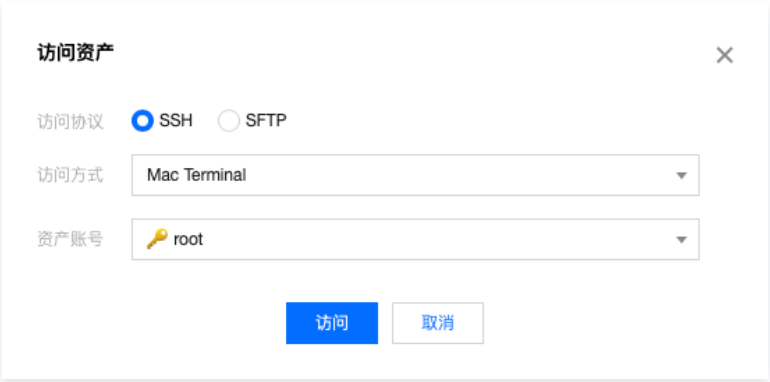
c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。

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

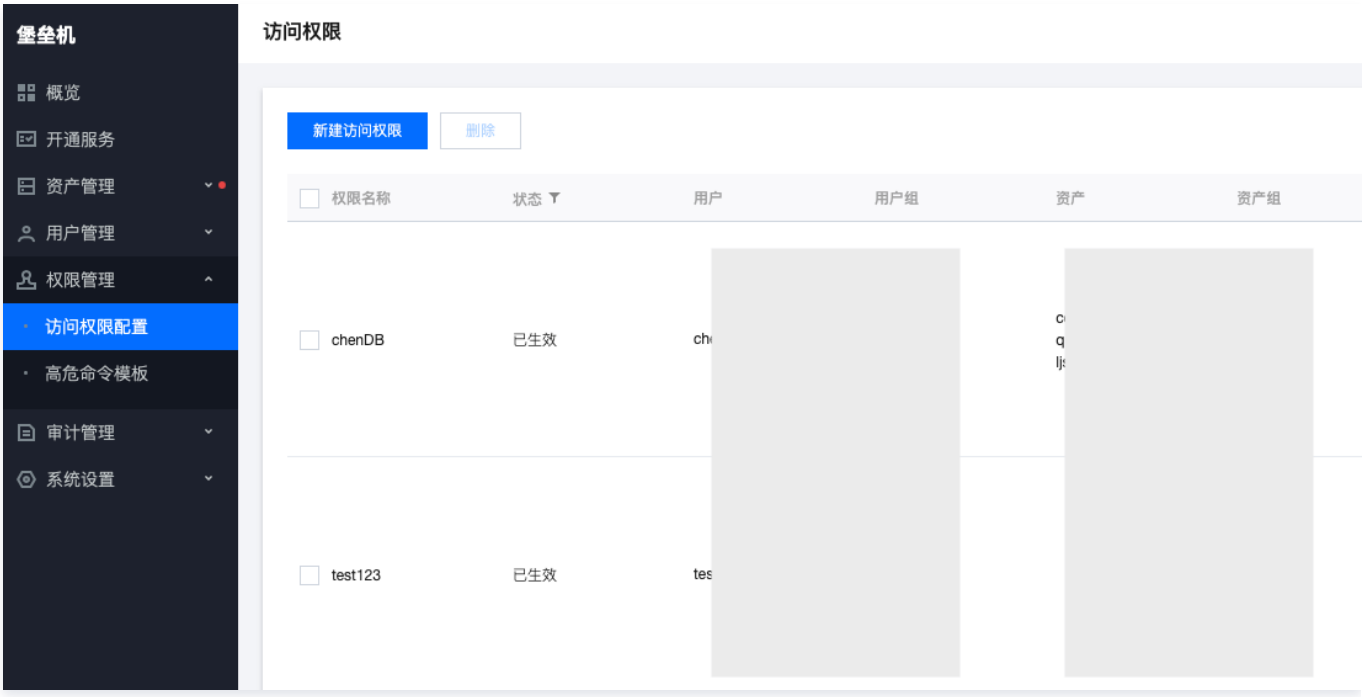
  1.1 登录 堡垒机控制台，在左侧导航选择**用户管理** > **用户**，进入用户页面。

  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。

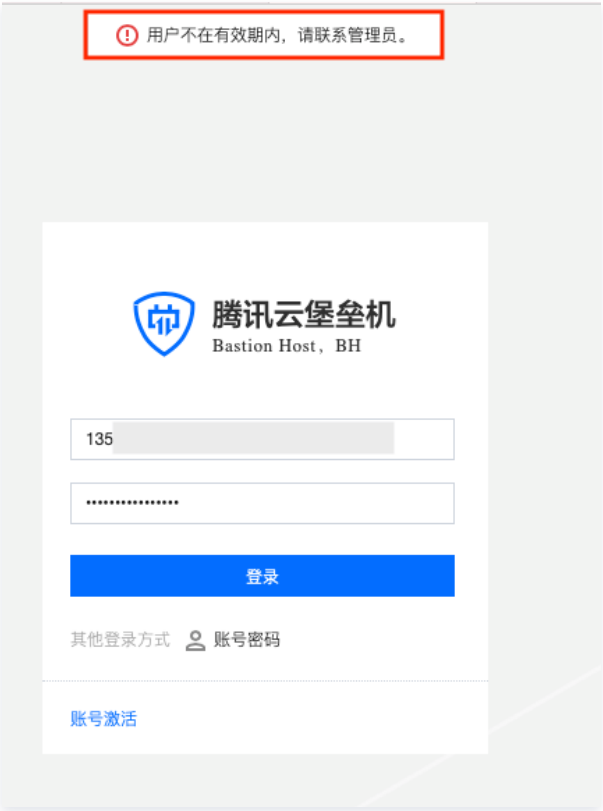
- 是否有默认口令
  使用浏览器访问运维页面，单击**账号激活**，在激活页面，用户需要获取短信验证码、并自己设置登录密码，证明用户无默认口令。

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。

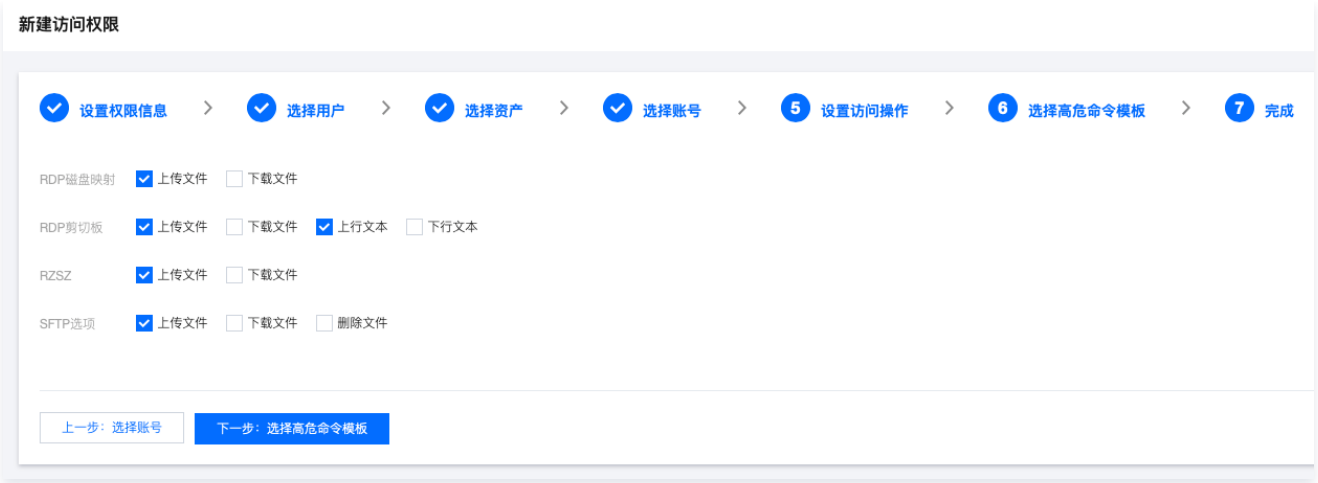
3. 使用浏览器访问运维页面，使用已过期的用户尝试进行登录，此时用户无法登录，并且页面提示“**用户不在有效期内**”，证明过期的用户无法继续使用。

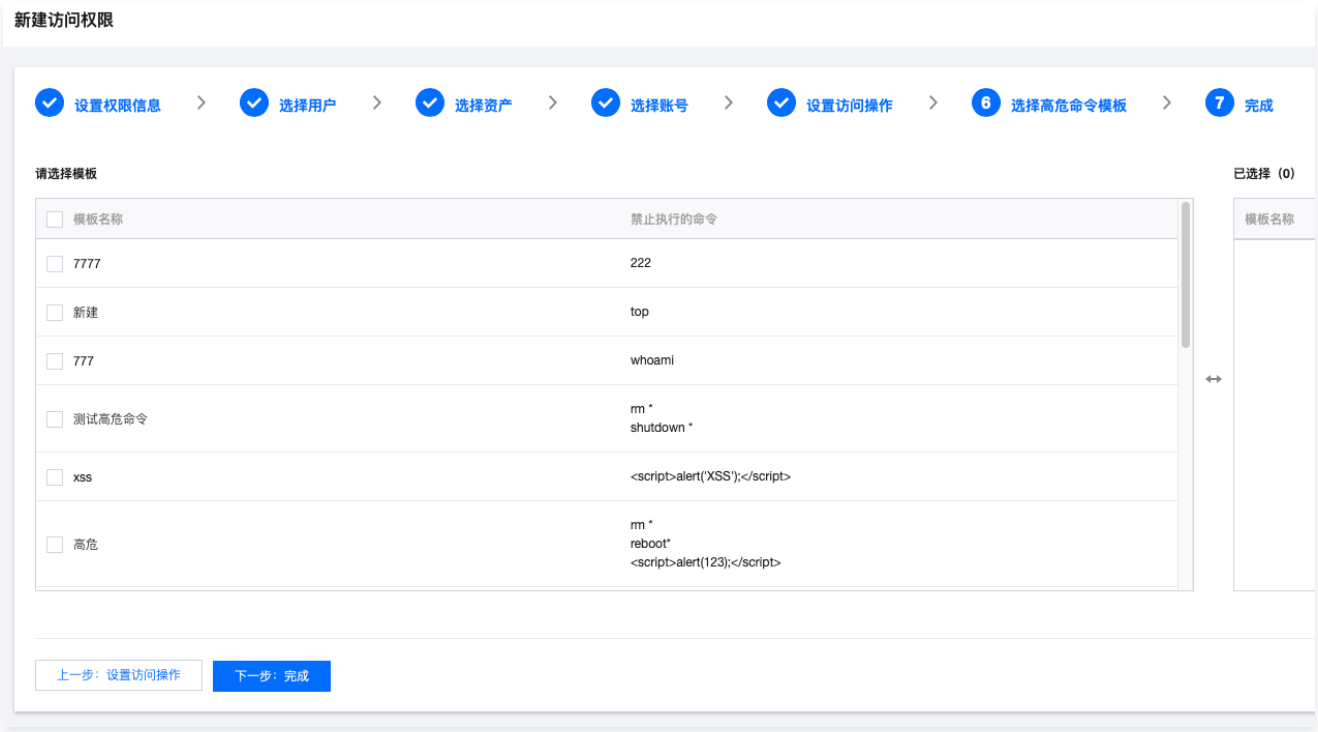


d) 应授予管理用户所需的最小权限，实现管理用户的权限分离；

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。



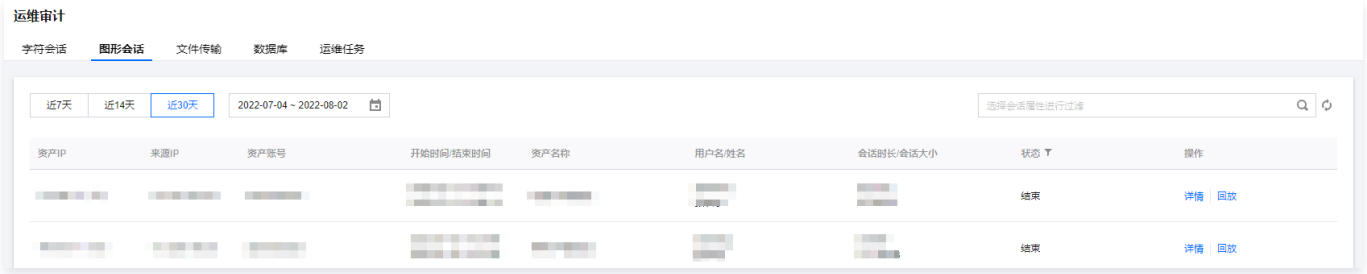


安全审计

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。

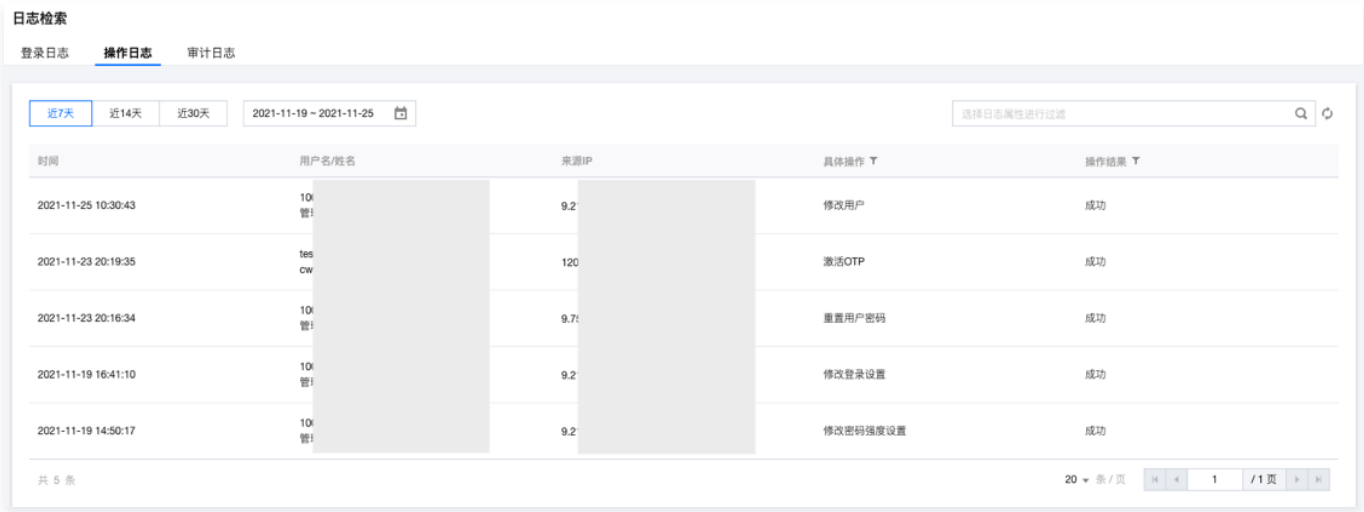


3. 单击**日志检索**，进入日志搜索页面，可查看用户对堡垒机的操作日志。

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。



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

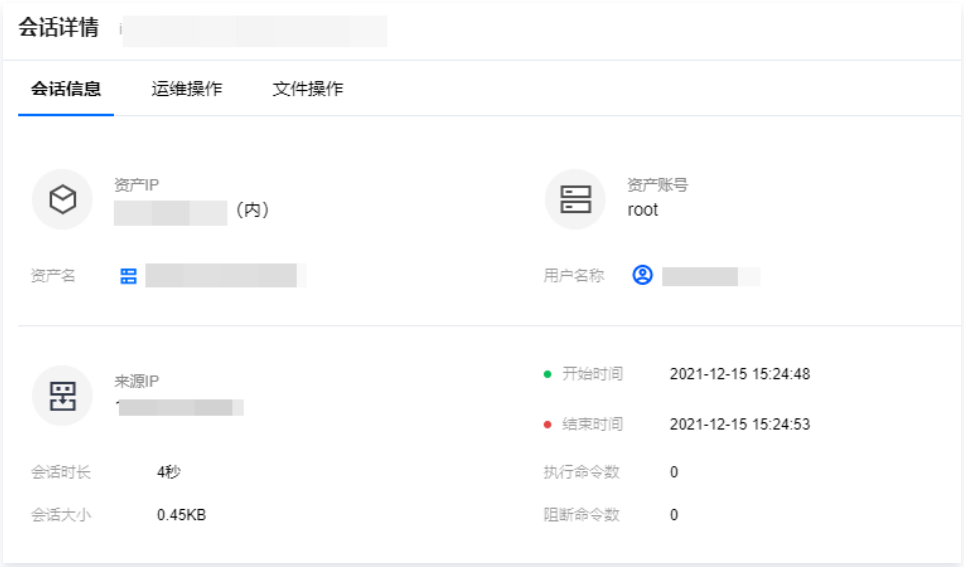
安全审计

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；

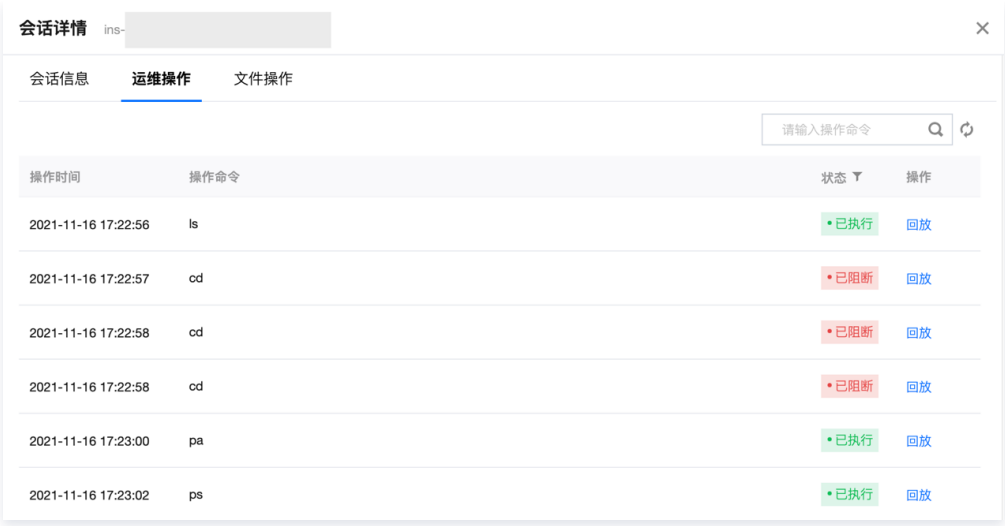
本条款主要考察：是否有进行安全审计。堡垒机支持对云服务器运维操作进行监控和审计。

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。



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）。

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 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。

安全计算环境

身份鉴别

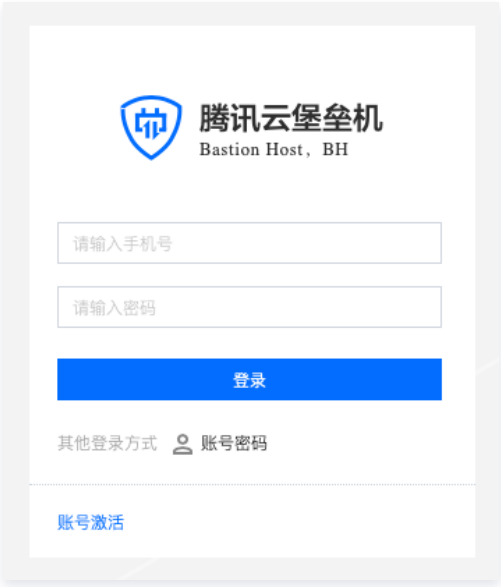
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

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。

- **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；

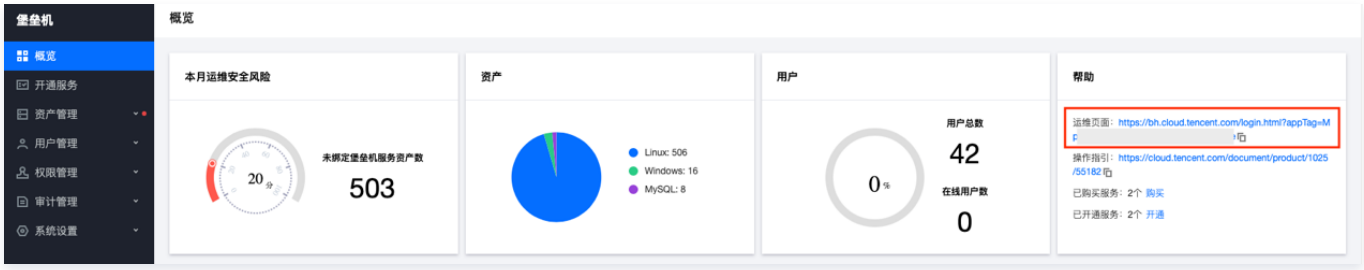
本条款主要考察：是否有登录失败处理能力，以及对登录失败的处理措施。

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。

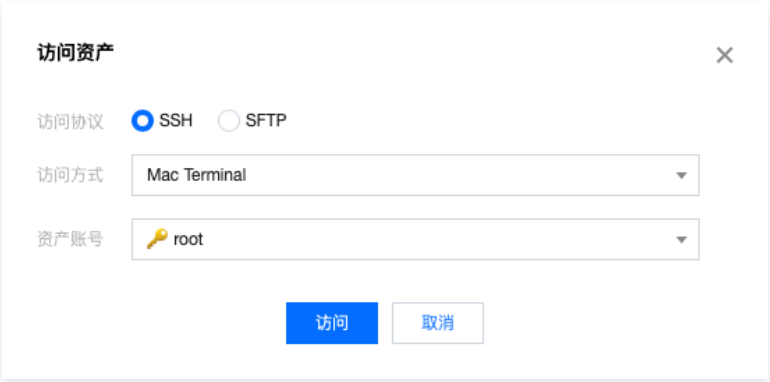
c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。

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。



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

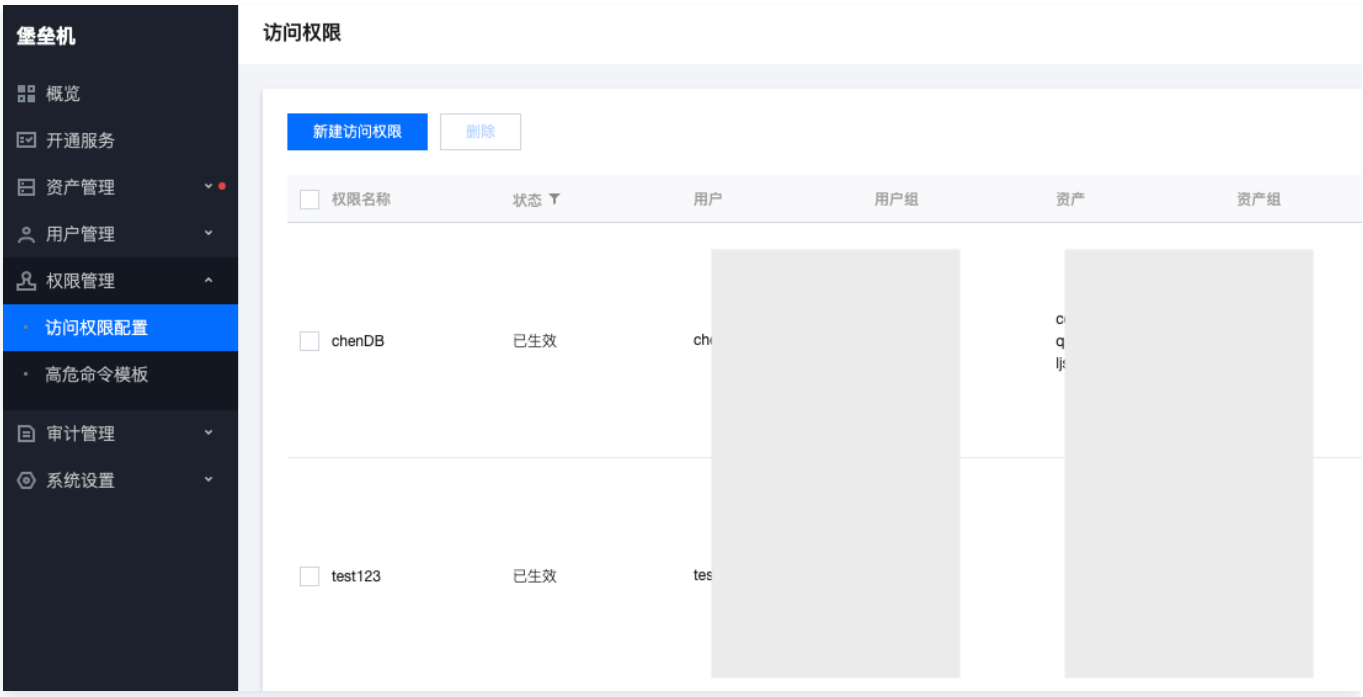
  1.1 登录 堡垒机控制台，在左侧导航选择**用户管理 > 用户**，进入用户页面。

  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。

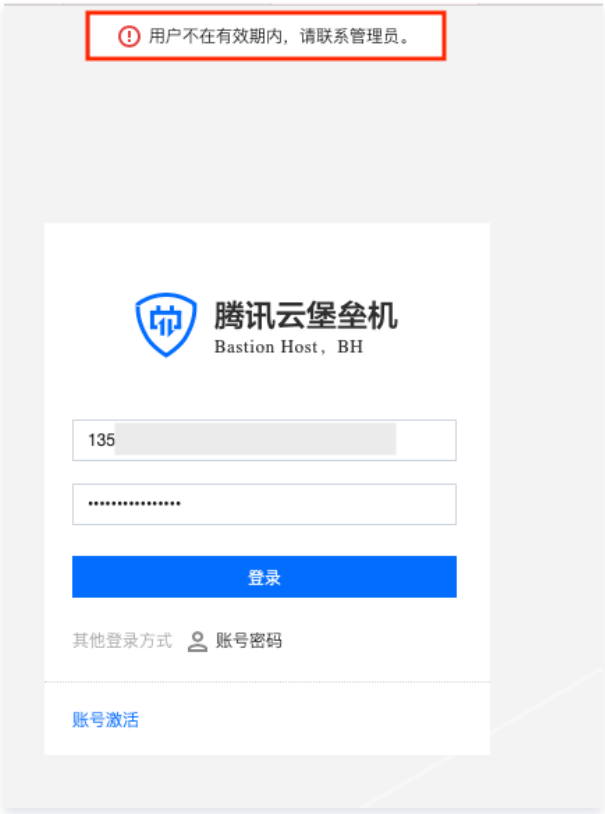
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；

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。

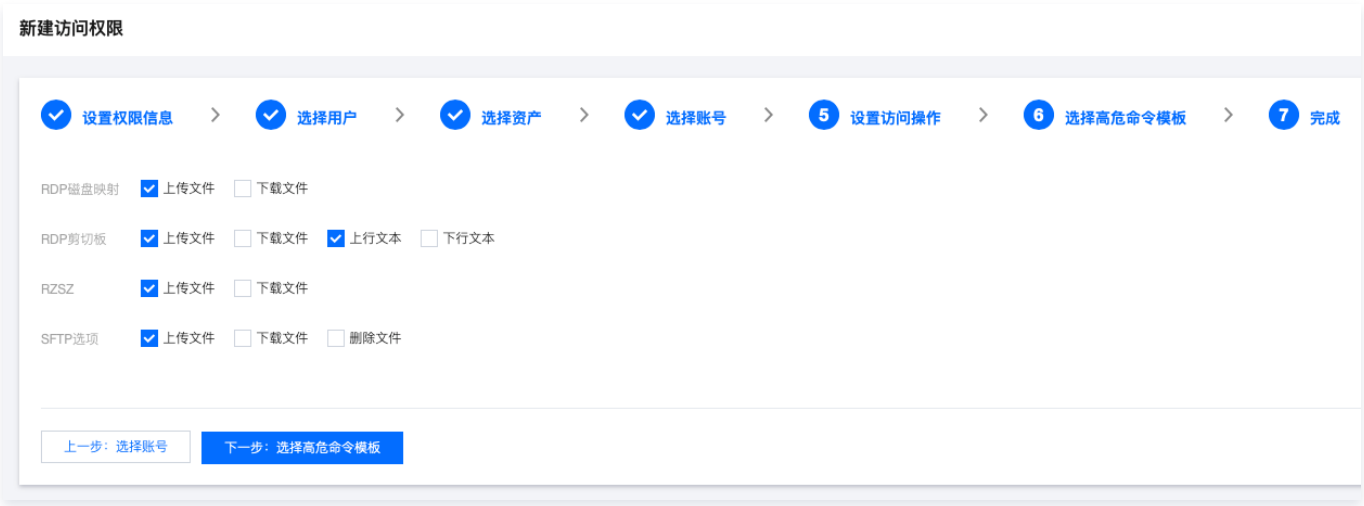
3. 使用浏览器访问运维页面，使用已过期的用户尝试进行登录，此时用户无法登录，并且页面提示“**用户不在有效期内**”，证明过期的用户无法继续使用。

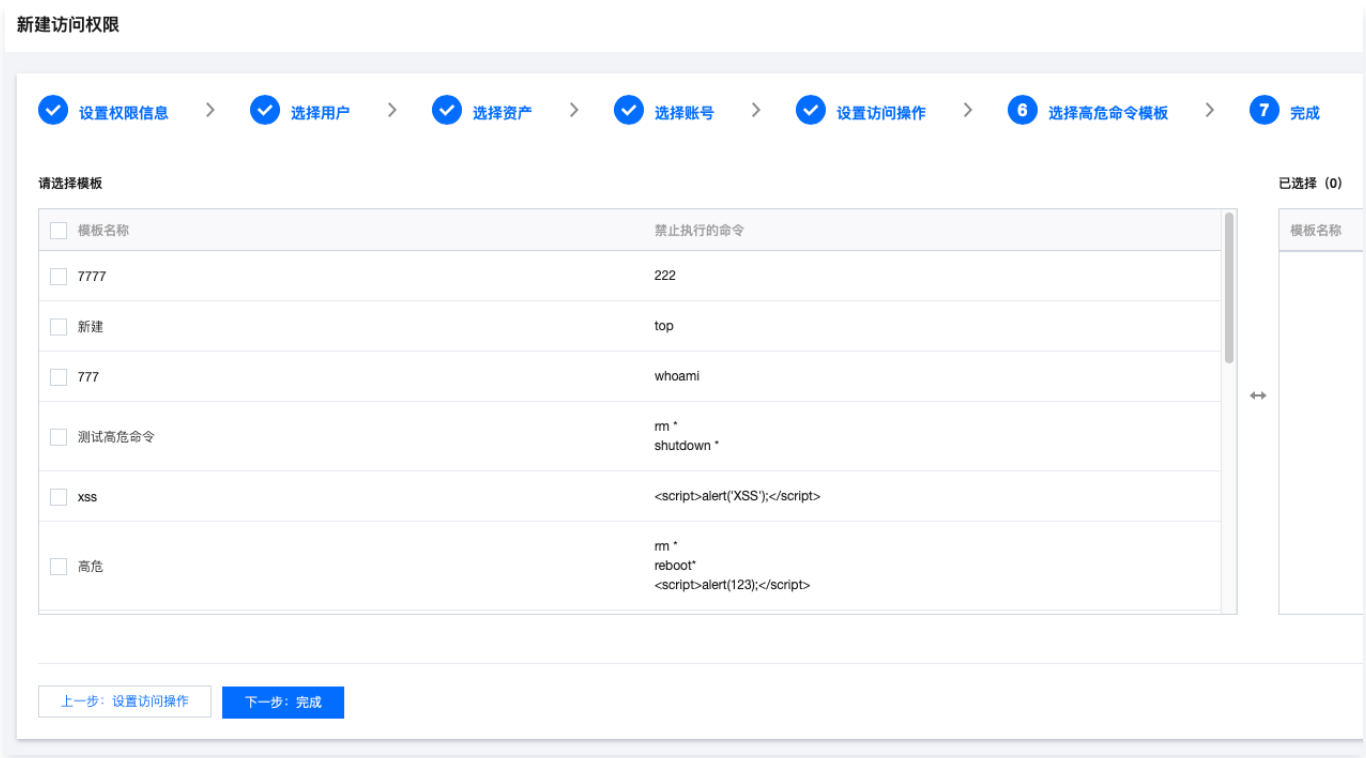


d) 应授予管理用户所需的最小权限，实现管理用户的权限分离；

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。

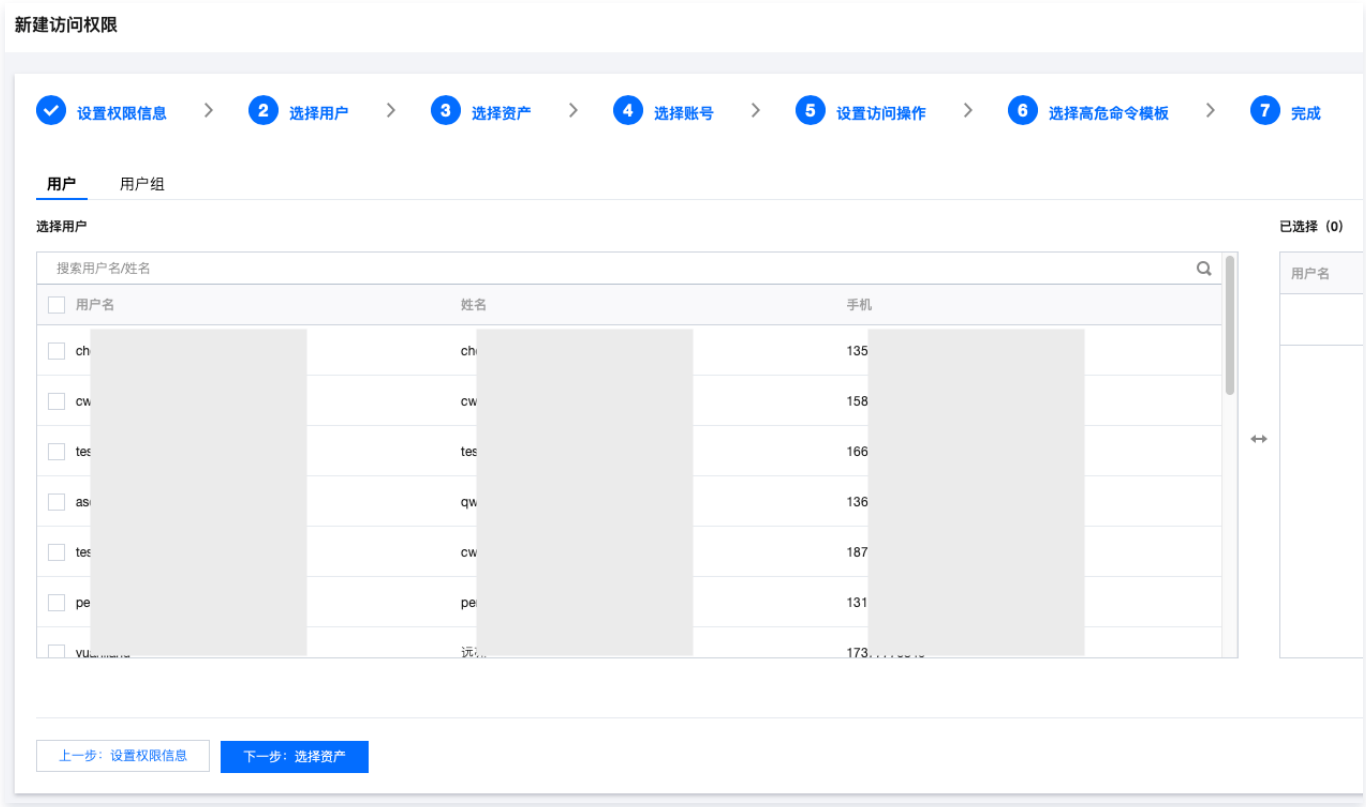


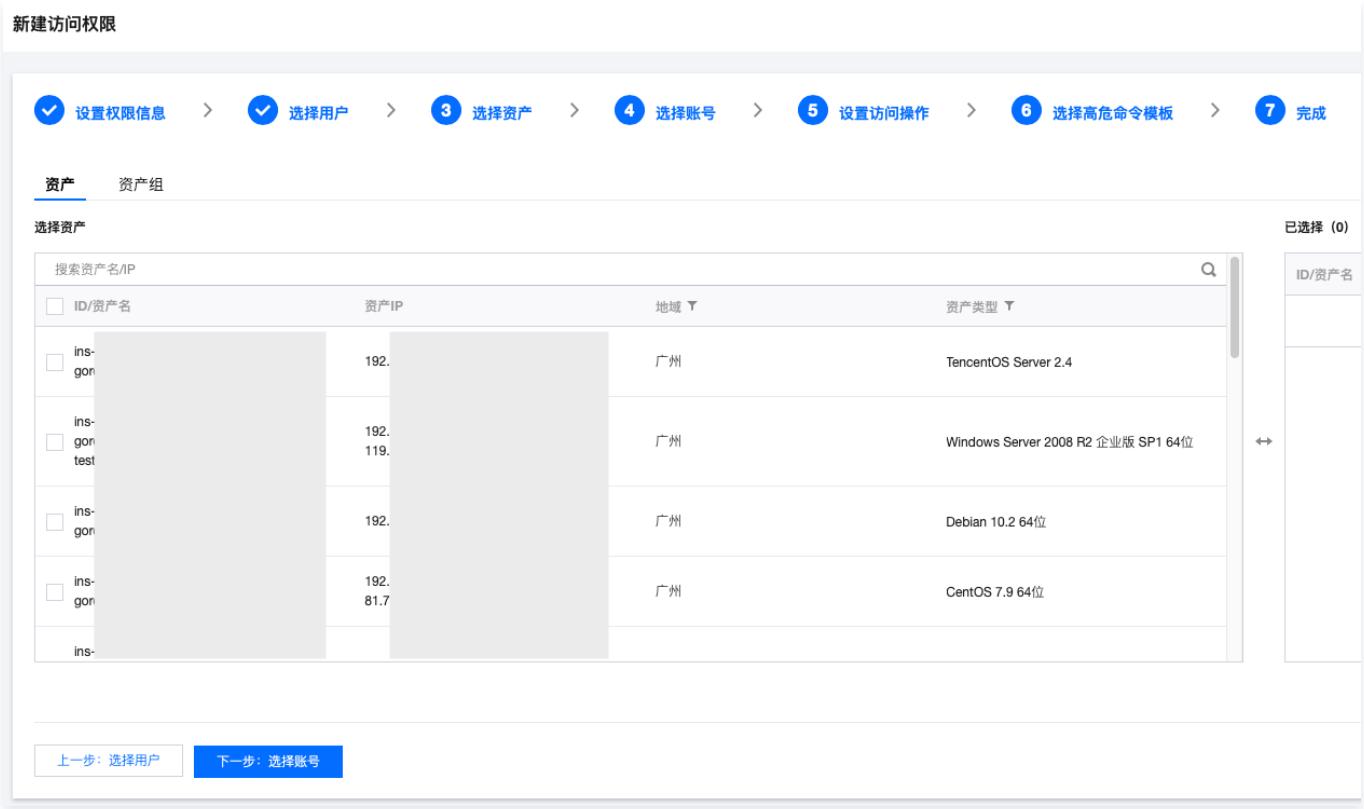


e) 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；

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。



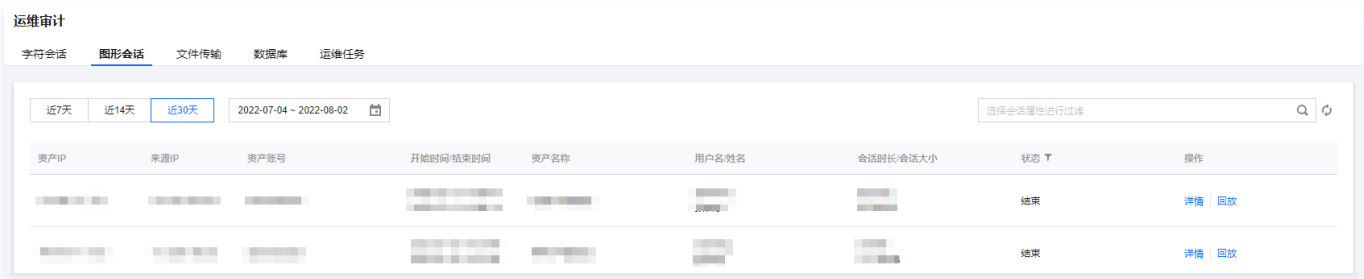


安全审计

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。

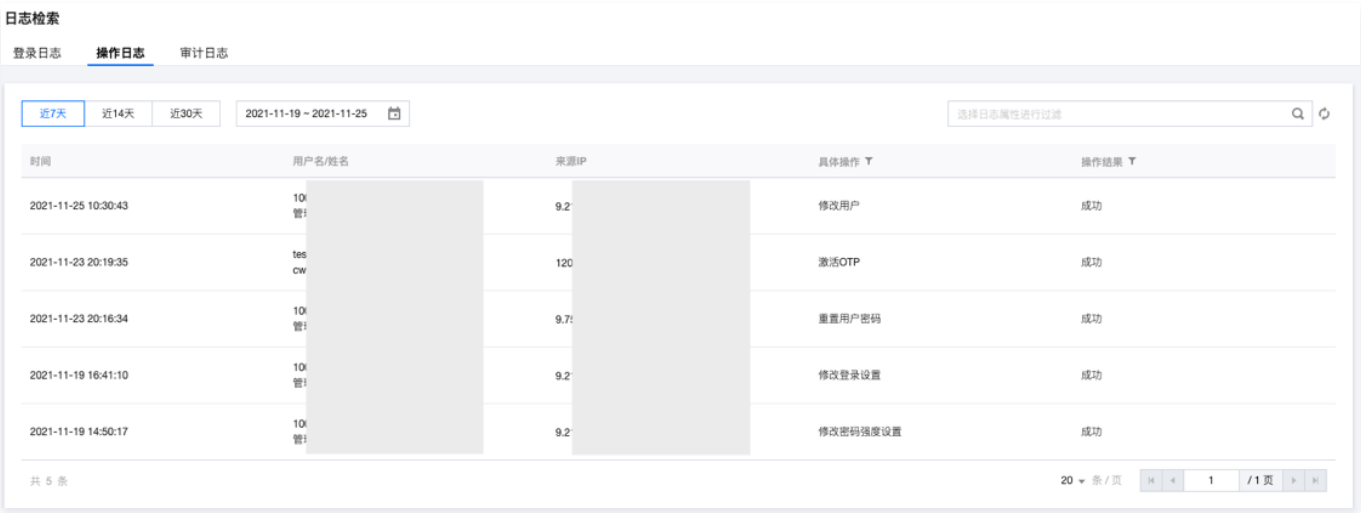


3. 单击**日志检索**，进入日志搜索页面，可查看用户对堡垒机的操作日志。

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。



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

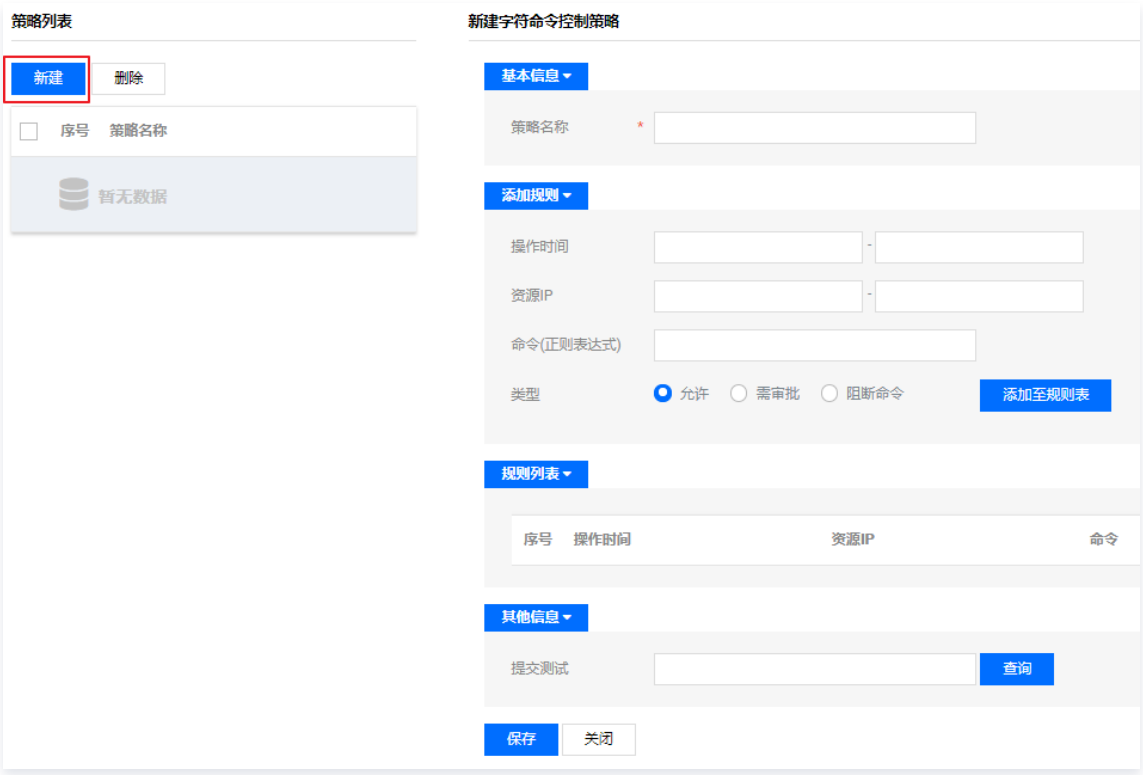
最近更新时间：2022-11-17 15:16:20

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。



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。

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

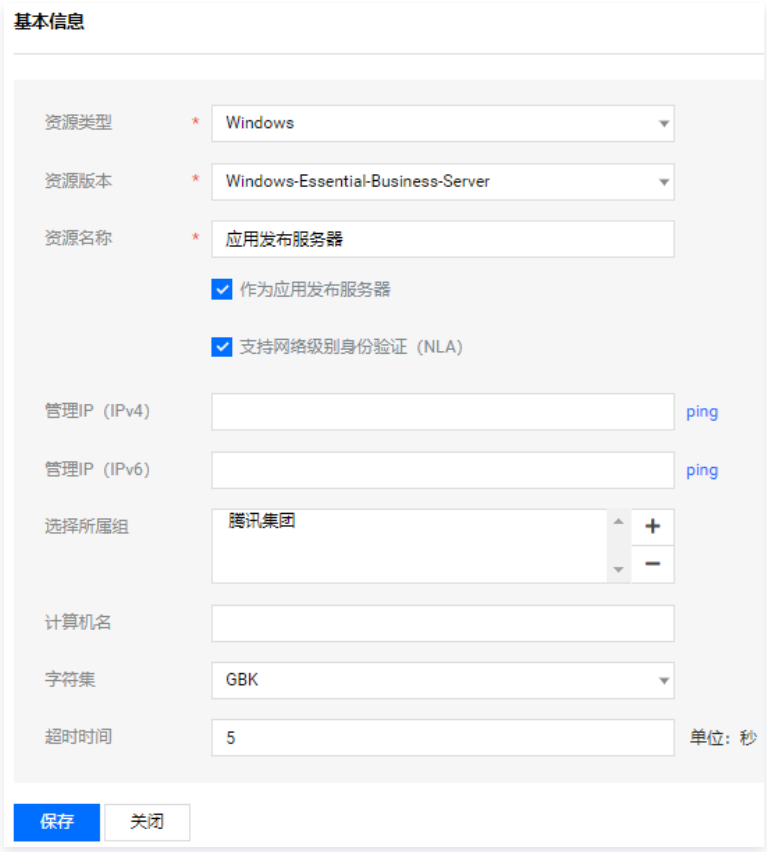
- 准备一台 Windows Server 2012 R2 作为应用发布服务器，并在 Windows 机器中安装好连接数据库工具（本文档以 Navicat for MySQL 为例进行说明）。
- 需要在安全组中放通堡垒机到应用发布服务器的10017、3389、443端口；应用发布服务器到堡垒机的3393、443端口，堡垒机到数据库端口放通，本地到堡垒机放通3392。详情请参见 创建安全组 。
- 已购买并激活 Windows 服务器的远程桌面服务。

> **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。



   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 。

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。

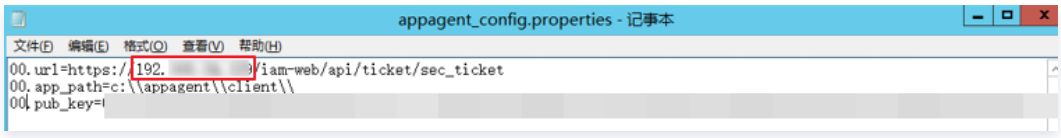
5.2 在资源类型配置页面的左侧导航中，单击**数据库**，选择已添加的数据库资源版本，绑定相应的驱动，并单击右侧扩展登录按钮。

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。

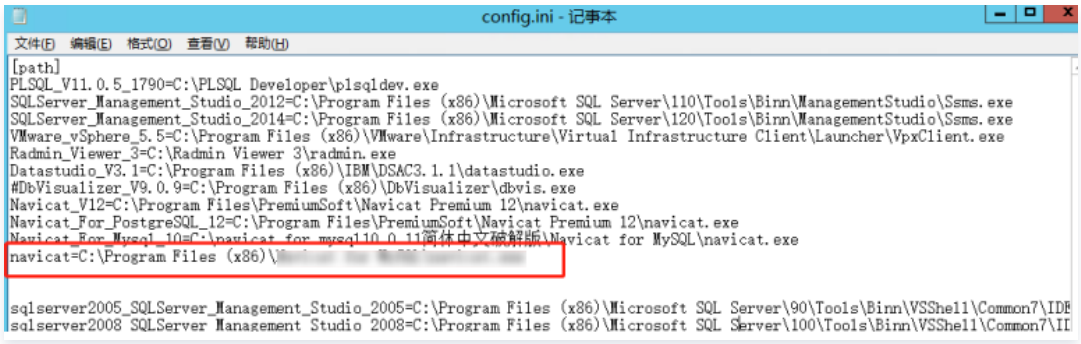
> **说明**
> 堡垒机已默认配置应用发布工具，若有特殊需求可自行配置。

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。

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
MSSQL
账号
口令
工具
WEB
应用发布
应用发布工具
选择分辨率
1024 × 768
超时时间
5
秒
登录

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。本文为您详细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：
   - **计划所属者**：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。

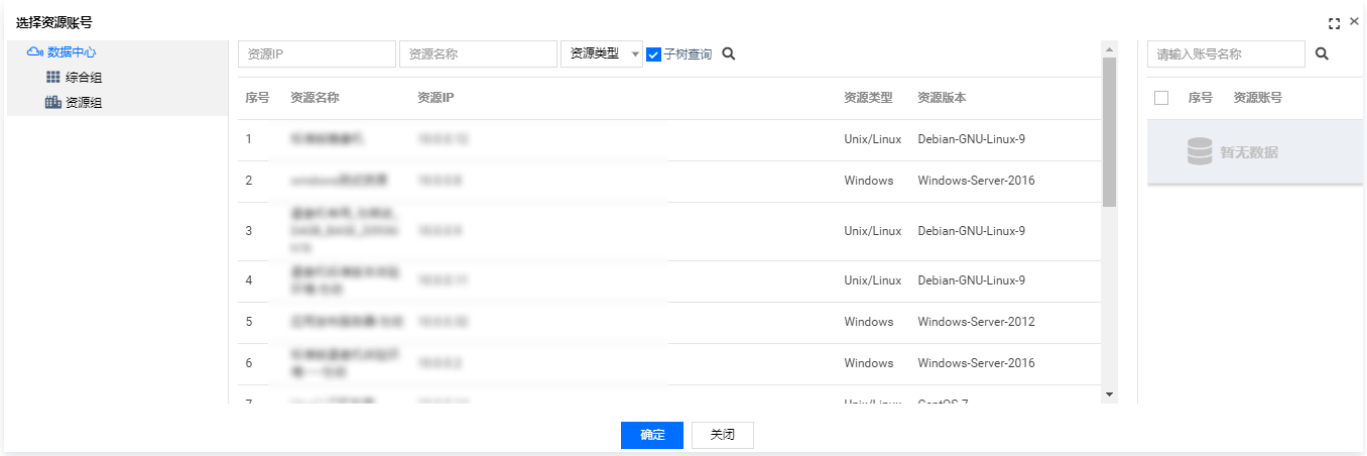
4. 单击**保存**，即可创建计划。

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。

2. 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。

3. 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

1. 单击**计划管理**，进入计划管理页面

2. 在计划任务列表，如下图所示，单击将任务启动。

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。

1. 单击**计划管理**，进入计划管理页面。

2. 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。

3. 在操作日志页面，您可查看该计划的操作记录日志。

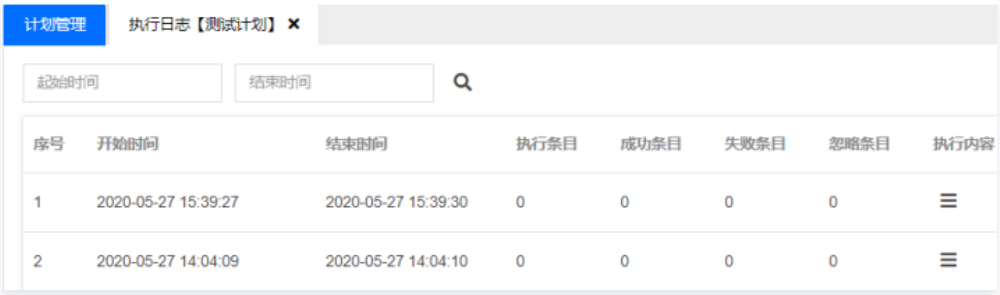
步骤5：查看执行日志

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。

1. 单击**计划管理**，进入计划管理页面。

2. 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。

3. 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】
起始时间
结束时间
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

安全事故事后追溯

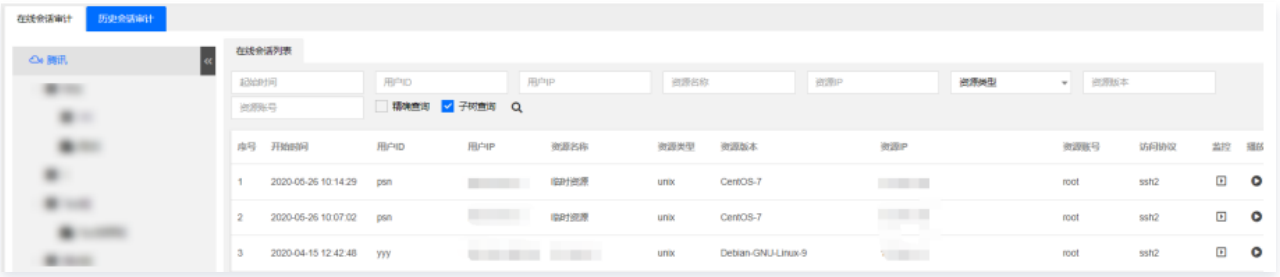
最近更新时间：2022-10-31 17:29:56

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。本文为您详细介绍如何查看在线和历史会话审计。

在线会话审计

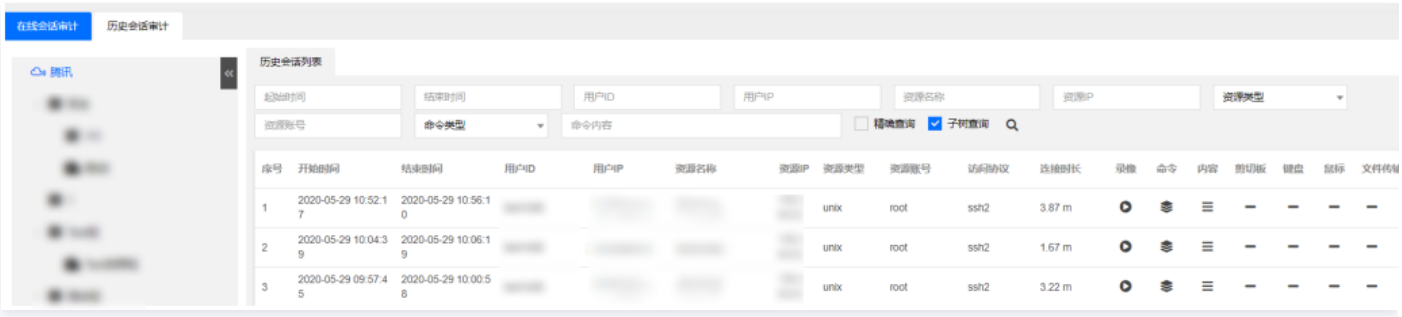
1. 在浏览器输入堡垒机 IP 地址，并输入账号和口令登录堡垒机。
2. 在左上角单击**审计平台**，进入审计平台，单击**操作行为审计**，进入操作行为审计页面。
3. 单击**在线会话审计**，进入在线会话查看页面。可以查看在线会话相关信息，例如开始时间、用户ID、资源名称、资源类型、资源登录账号、访问协议、监控、播放录像等内容。



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. 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

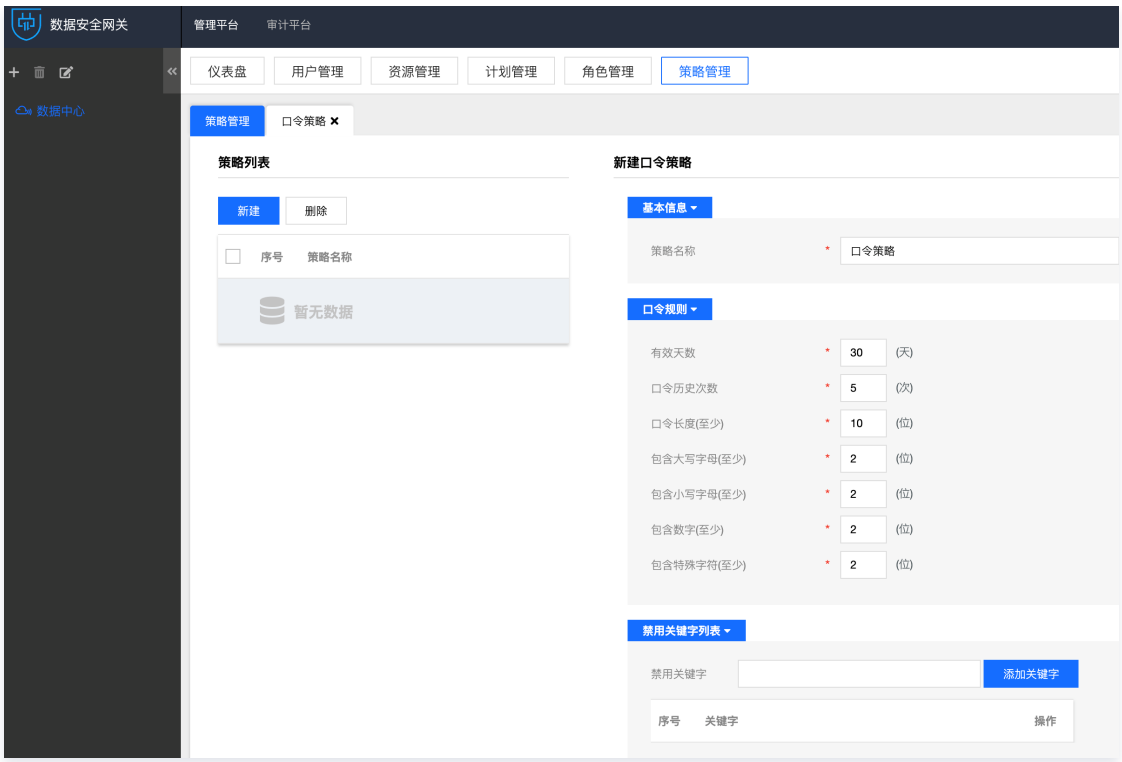
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

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。

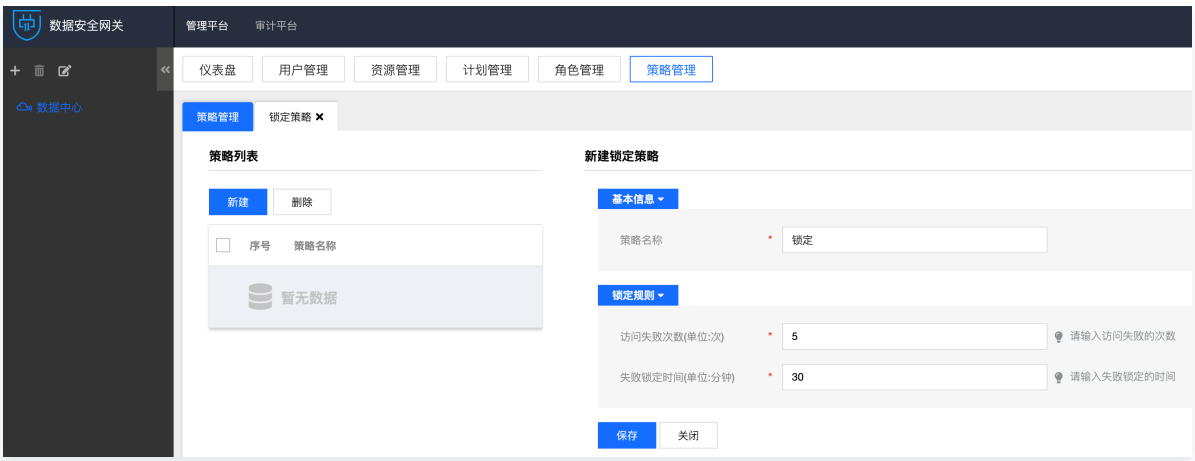


1.3 单击**用户管理**，选择一个用户，单击**编辑**，进入编辑页面之后，单击**设置策略**，设置口令策略。

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。

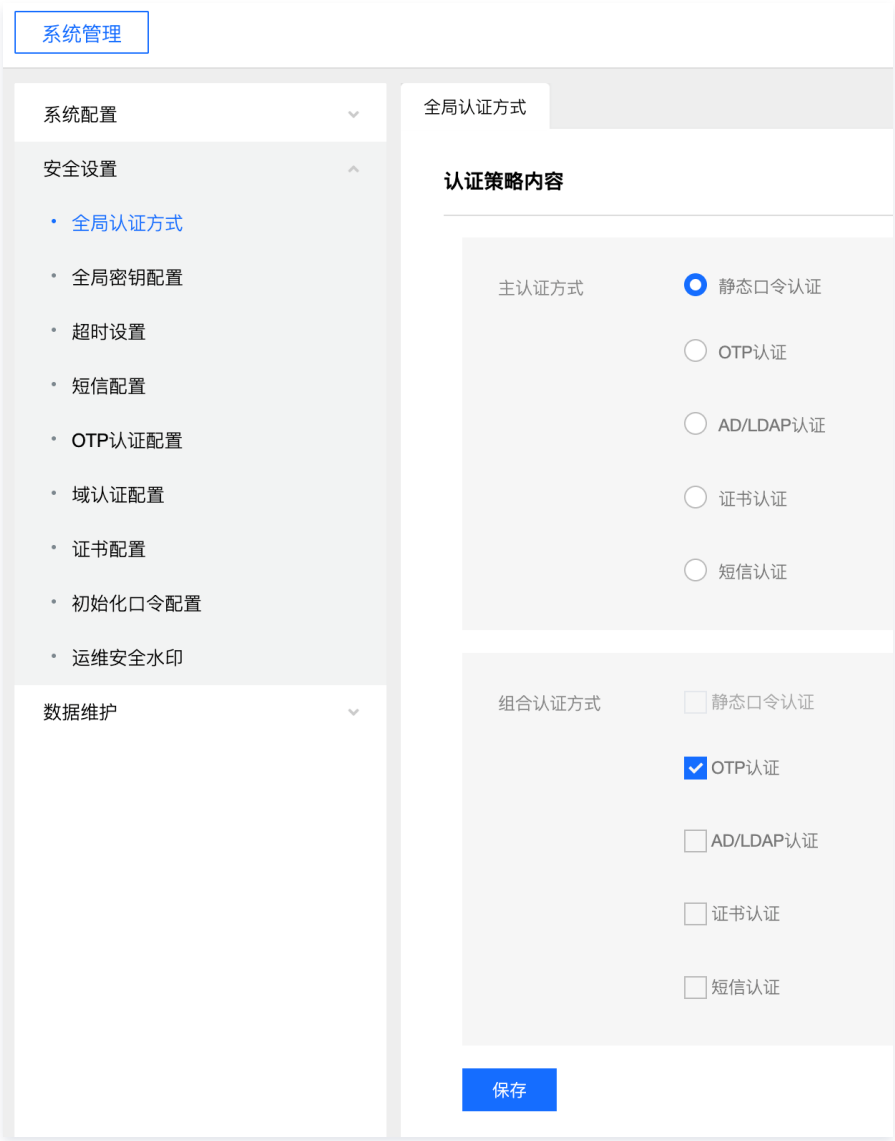
本条款主要考察：是否采用加密的协议进行远程管理。

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

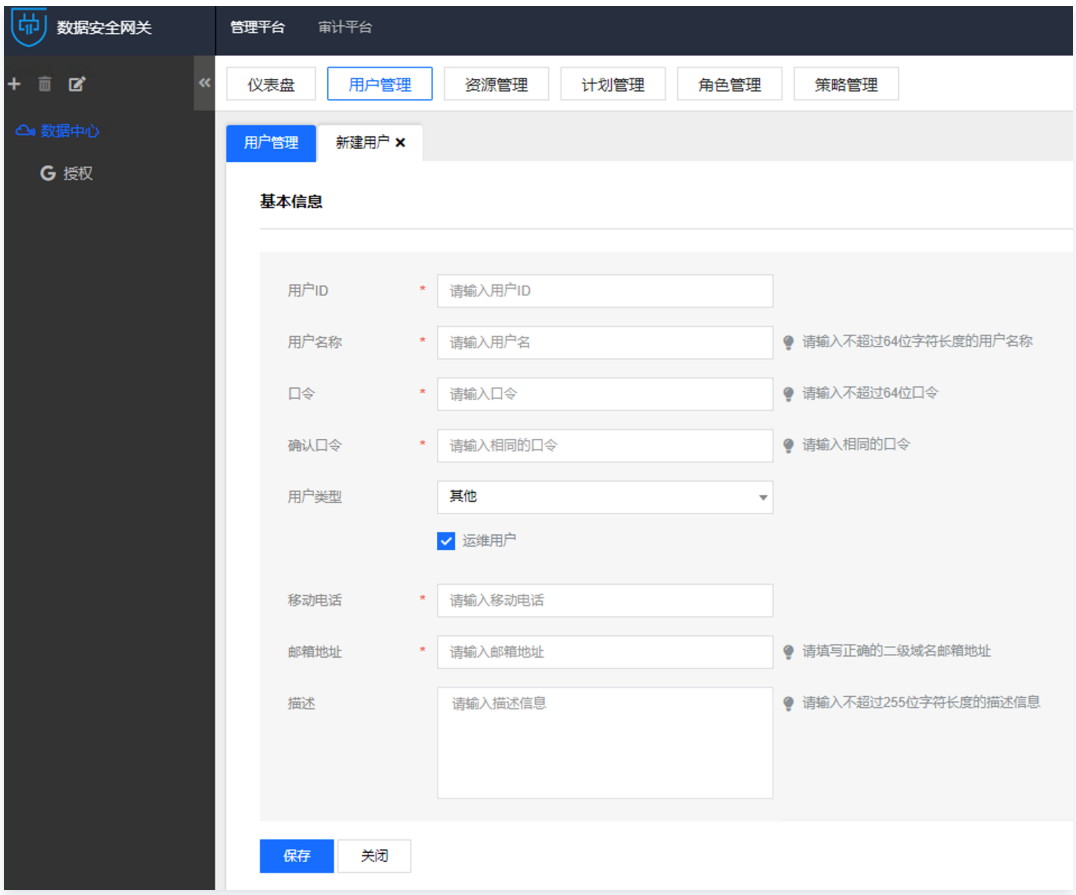
  1.1 使用管理员账号登录堡垒机，单击**用户管理**，进入用户页面。

  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。

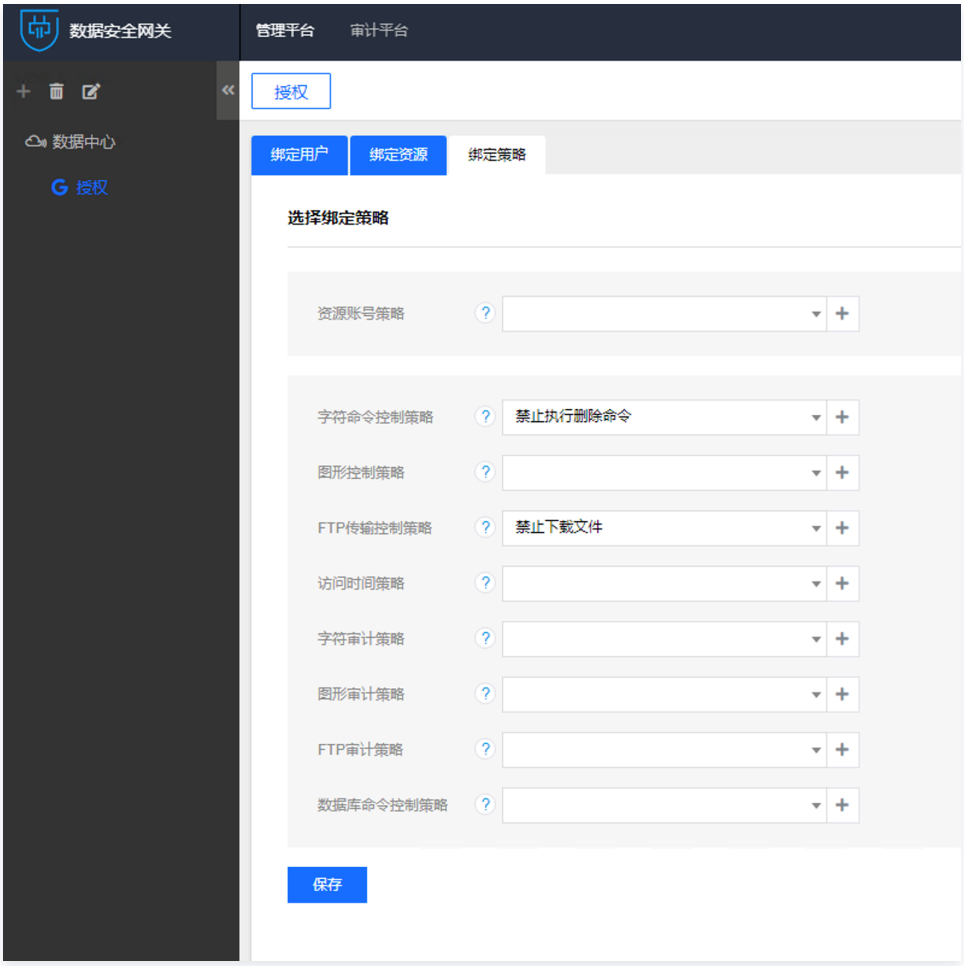
1. 使用管理员账号登录堡垒机，单击**用户管理**，进入用户页面。
2. 在用户页面，单击**编辑** > **高级选项**，查看一个过期用户的用户信息，确认用户已过有效期。

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。