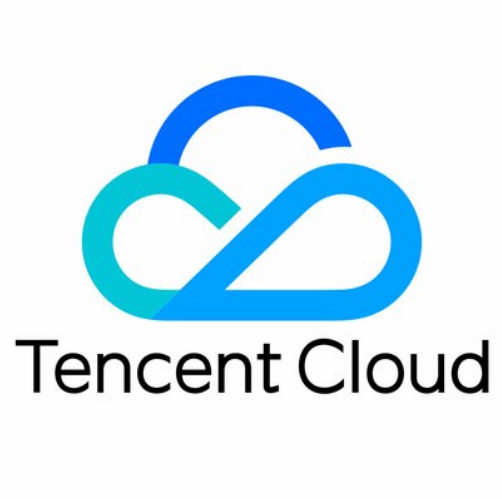
堡垒机

实践教程

产品文档



文档目录

实践教程
高危命令阻断

最近更新时间：2025-04-18 11:17:40

操作场景

高危命令阻断可有效防止运维人员由于误操作，或者恶意操作导致的运维安全事故，本文为您详细介绍如何在堡垒机配置高危命令阻断策略。

> **说明：**
> 该功能仅支持 Linux 服务器。

步骤1：创建高危命令模板

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

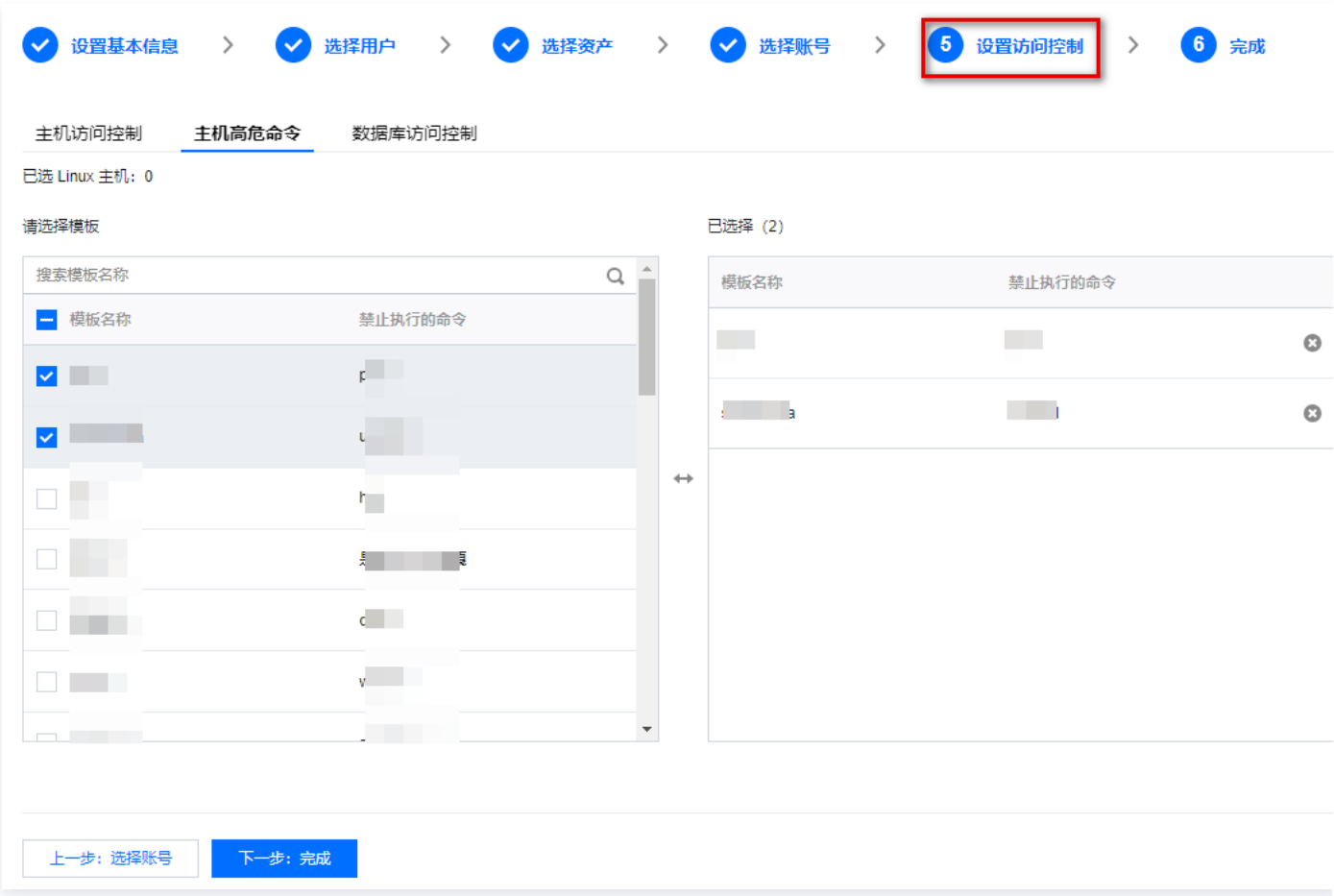
4. 在新建高危命令模板弹窗中，设置对应的模板名称和禁止执行的命令。

5. 单击**确定**，即可创建高危命令模板。

步骤2：访问权限关联高危命令模板

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

4. 在编辑访问权限页面，跳转到第5步，设置访问权限的主机高危命令。



5. 单击**下一步：完成**，确认访问权限配置信息。
6. 确认信息无误之后，单击**确定提交**，即可保存对访问权限的修改，此时通过该访问权限授权的用户，在访问 Linux 主机时如果执行高危命令模板里面的命令，将被堡垒机拦截。

文件传输控制

最近更新时间：2025-04-18 11:17:40

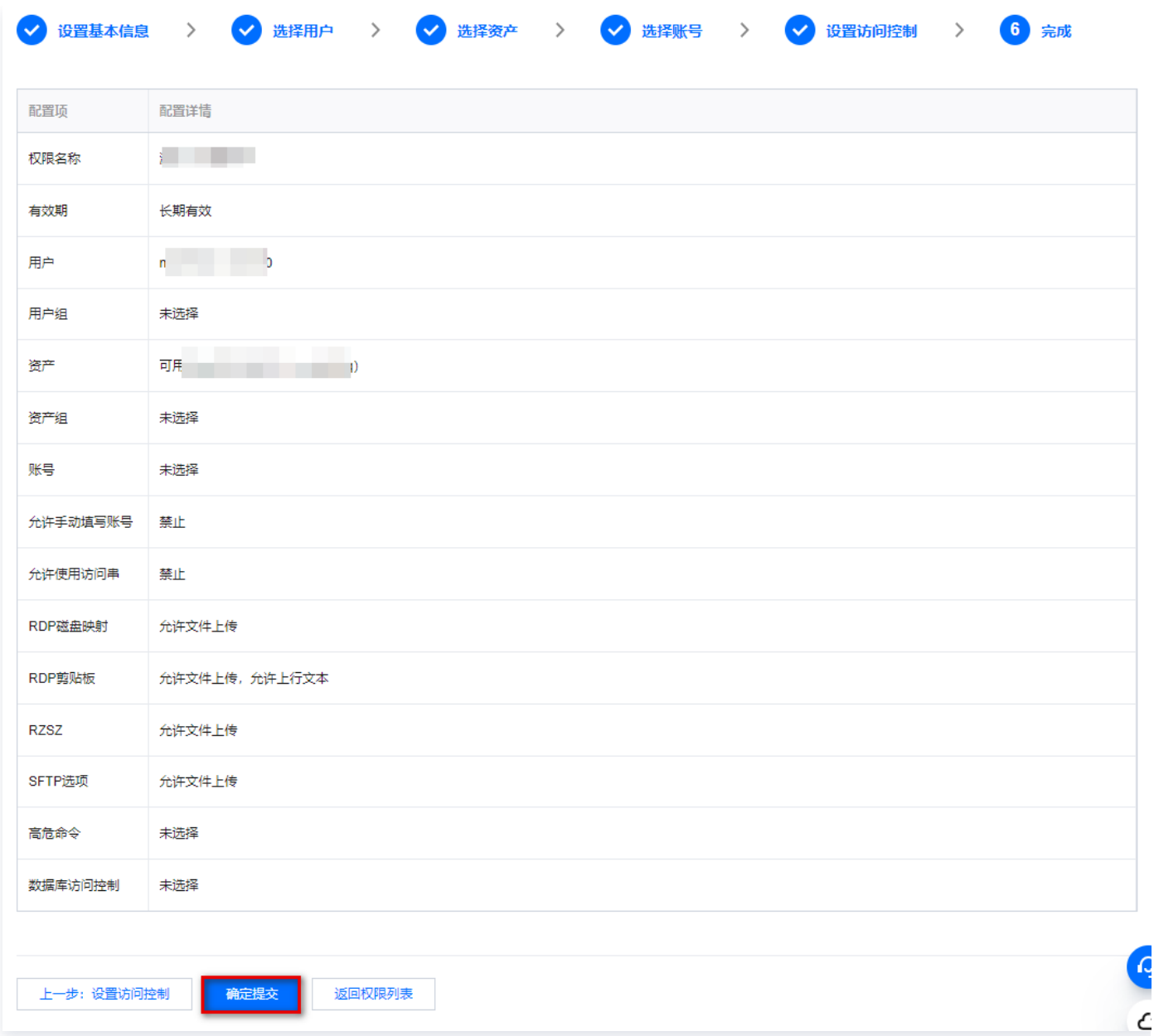
操作场景

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

操作步骤

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

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。



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。

安全事故追溯

最近更新时间：2025-04-18 11:17:40

操作场景

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

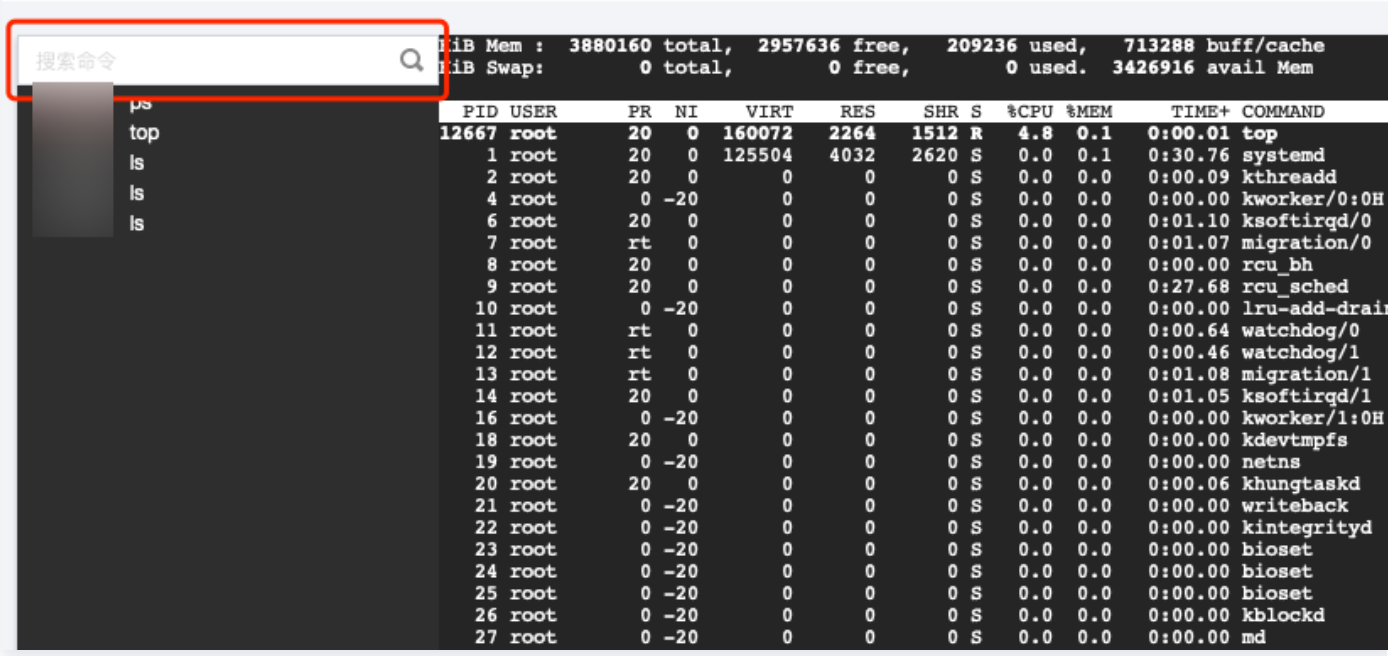
操作步骤

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

4. 查找到相关会话之后，可单击对应会话右侧的**回放**，通过会话回放方式真实还原用户操作行为。

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



跨 VPC 资产管理

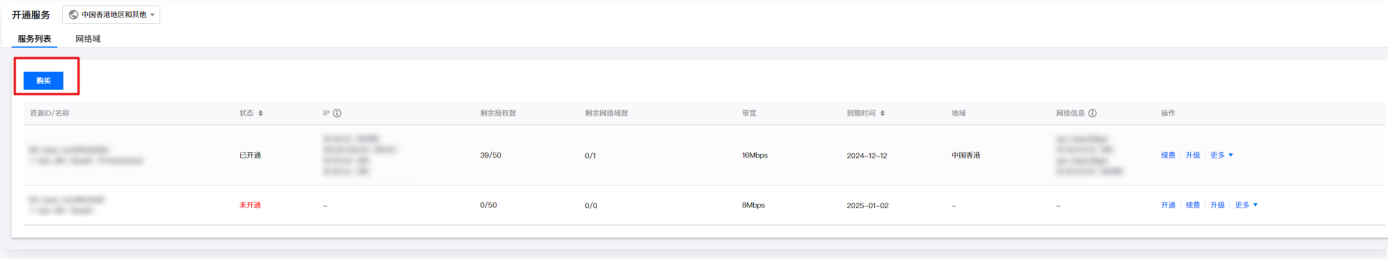
最近更新时间：2025-04-18 11:17:40

操作场景

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

操作步骤

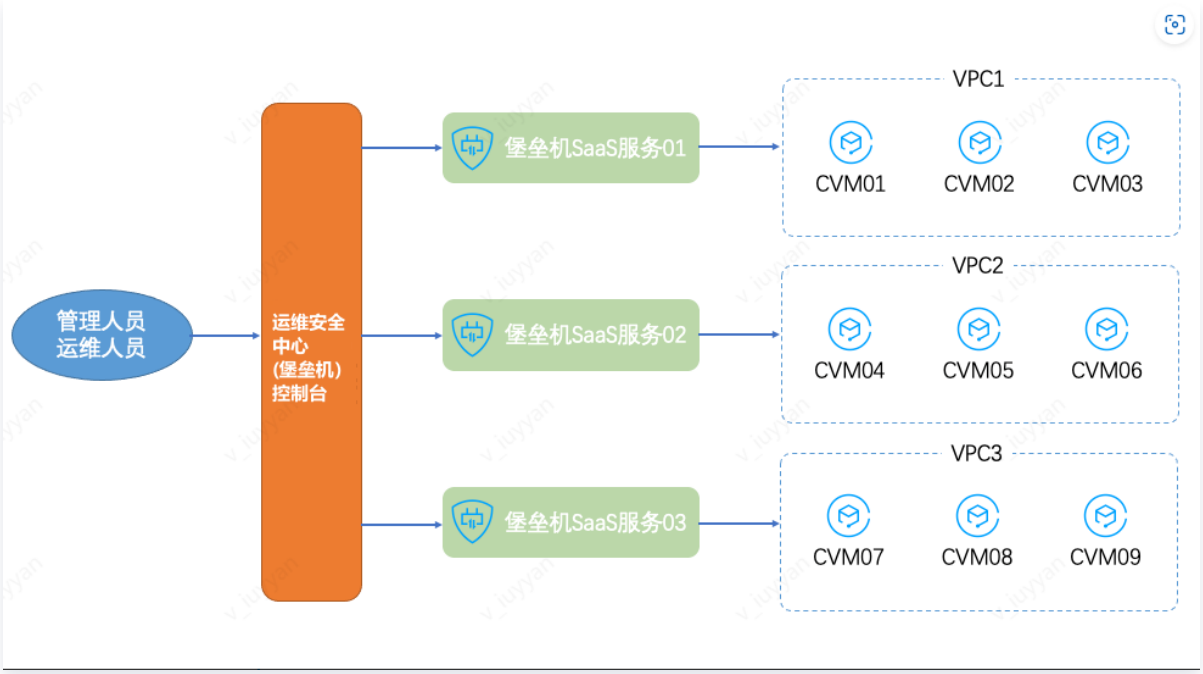
1. 登录 堡垒机控制台 。
2. 在左侧导航栏中，选择**开通服务**。
3. 在开通服务页面，单击**购买**，进入购买页面，选择合适的规格进行购买。



4. 购买完成之后，返回开通服务页面，找到新购买的堡垒机服务，单击**开通**。

5. 在开通服务弹窗中，配置地域、VPC 和子网信息后，单击**确定**，完成开通服务。
   - 地域：请选择堡垒机纳管的资产的所属地域。
   - VPC：请选择需要堡垒机纳管的资产的所属 VPC，选择之后 VPC 无法修改。
   - 子网：选择任意子网均可，但完成初始化操作后，该子网不能被销毁。建议选择资产数量较多的子网。

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



说明

- 管理和维护工作操作详情请参见 堡垒机的 快速入门。

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

使用内网域名访问堡垒机运维页面

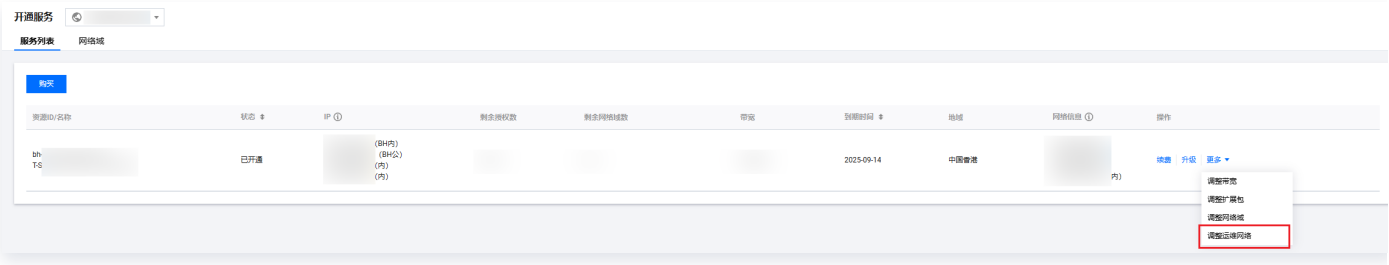
最近更新时间：2025-08-28 17:26:34

操作场景

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

步骤一：开通内网运维

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



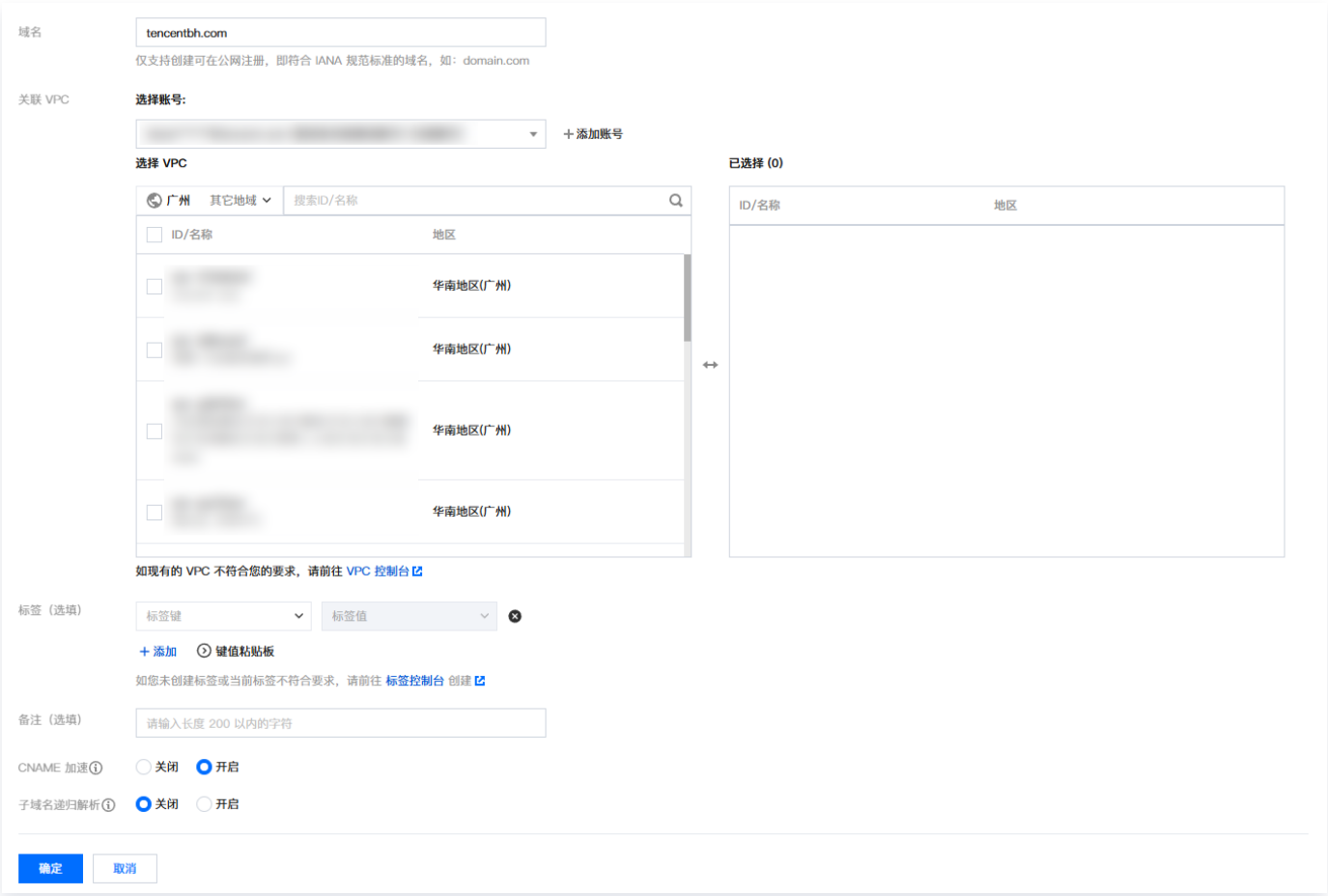
4. 在调整运维网络窗口中，选择**内网**作为运维方式，然后选择 VPC 和子网，单击**确定**。

> **说明：**
> 需确保运维人员终端网络和所选的VPC/子网网络能够连通。

步骤二：关联内网域名

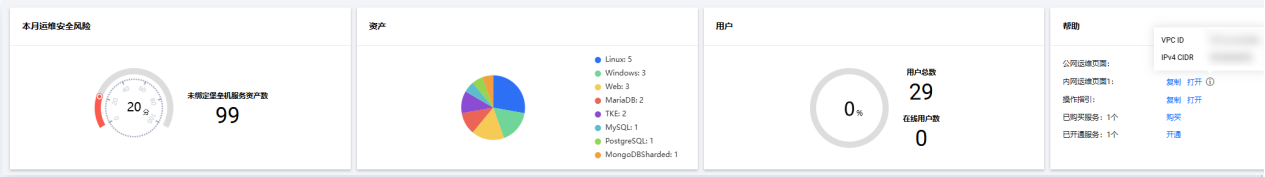
1. 登录 私有域解析 Private DNS 控制台 。
2. 在左侧导航栏中，选择**内网解析** > **域名列表**。
3. 在域名列表中，单击**新建私有域**。

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。



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**。

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。

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

步骤三：使用内网域名访问运维页面

内网域名关联成功后，即可通过配置的访问域名访问运维页面。

> **说明：**
>
> 访问域名：主机记录.tencentbh.com。