运维安全中心（堡垒机）

传统型堡垒机

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【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

- 传统型堡垒机
  - 产品公告
    - 关于传统型堡垒机产品下线的公告
    - 关于传统型堡垒机停售的公告
    - 关于传统型堡垒机价格调整的公告
    - 关于传统型堡垒机安全漏洞修补的公告
  - 产品简介
    - 产品概述
    - 产品优势
    - 应用场景
  - 购买指南
    - 计费概述
    - 购买方式
    - 欠费说明
    - 退费说明
  - 快速入门
    - 控制台登录
    - 初次上线配置
    - 运维人员入门
  - 操作指南
    - 管理配置手册
      - 管理配置总览
      - 登录系统
        - 登录概述
        - 使用静态口令登录
        - 使用动态口令登录
        - 使用证书登录
        - 使用 AD 域认证登录
        - 使用短信认证登录
      - 组织管理
        - 根节点
          - 添加组织结构
          - 修改组织结构
          - 删除组织结构
        - 综合组
          - 新增综合组
          - 编辑综合组
          - 删除综合组
        - 资源组
          - 新增资源组
          - 编辑资源组
          - 删除资源组
        - 工作组
          - 新增工作组
          - 编辑工作组
          - 删除工作组
      - 仪表盘
      - 用户管理
        - 添加用户
        - 删除用户
        - 用户编辑

版权所有：腾讯云计算（北京）有限责任公司

编辑用户基本信息
设置口令
设置用户认证方式
设置用户策略
唯一标识
证书管理
用户相关操作
注销用户
锁定用户
解锁用户
批量修改组织结构
为选中用户绑定角色
为选中用户绑定授权
导入用户
导出用户
添加用户类型
查询用户
用户角色授权
用户授权
资源管理
添加资源
删除资源
编辑资源
查询资源
资源账号列表
添加账号
编辑账号
删除账号
查询账号
批量修改口令
批量修改鉴别状态
批量修改接管状态
批量删除被接管资源账号
查看口令修改日志
账号拨测
资源类型配置
资源相关操作
批量修改协议端口
导出资源
导入资源
批量资源下线
批量修改组织结构
资源同步
统计视图
账号导出计划
工作组
绑定用户
绑定资源
绑定策略
计划管理
创建任务
编辑任务
资源账号

版权所有：腾讯云计算（北京）有限责任公司

添加资源账号
删除资源账号
搜索资源账号
删除任务
查询任务
任务启动停止
查看操作日志
查看执行日志
角色管理
添加角色
修改组织角色
删除组织角色
搜索组织角色
策略管理
普通策略
添加资源账号策略
添加时间策略
添加口令策略
添加锁定策略
访问控制策略
添加字符命令策略
添加 FTP 访问控制策略
添加图形访问控制策略
审计策略
添加字符审计策略
添加 FTP 审计策略
添加图形审计策略
系统管理
系统配置
系统监控
系统维护
服务器配置
配置系统时间
配置邮件服务
端口开放管理
配置 Syslog
配置消息公告
安全认证配置
配置全局认证方式
配置全局密钥
超时设置
配置 OTP 认证
配置域认证
配置证书
配置短信认证
初始化口令配置
运维安全水印
数据维护
配置数据维护
审计数据维护
自维护
审计管理
管理审计

版权所有：腾讯云计算（北京）有限责任公司

基础信息维护审计
安全认证审计
操作行为审计
在线会话审计
历史会话审计
统计报表
基础报表
运维业务报表
计划报表
查询审计日志
告警设置
告警策略
告警配置
告警事件
运维配置手册
运维配置总览
下载控件
安装证书
Mac OS 系统安装证书
Windows 系统安装证书
单点登录
授权列表
登录 Windows 资源
使用 Web 登录
使用 XFTP 登录
使用 Mstsc 登录
登录 Linux 资源
使用 Web 登录
使用 PuTTY 登录
使用 XShell 或 SecureCRT 登录
使用 XFTP 登录
登录数据库资源
使用 Web 登录
使用 Mstsc 登录
工单
脚本计划
Mac 系统支持工具登录
实践教程
删库等高危命令阻断
配置应用发布管理数据库
服务器真实密码隐藏
安全事故事后追溯
等保实践教程
常见问题
购买部署相关
运维相关
端口相关
单点登录相关

传统型堡垒机
产品公告
关于传统型堡垒机产品下线的公告

最近更新时间：2024-04-23 10:20:41

尊敬的腾讯云用户，您好：
因业务调整，腾讯云传统型堡垒机将于2024年9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 型堡垒机，如果您有数据迁移需求，请参考以下文档：

- 如何迁移数据

SaaS 型堡垒机相关文档如下：

- 快速入门指南
- 等保最佳实践
- SaaS 型堡垒机产品动态

关于传统型堡垒机停售的公告

最近更新时间：2022-11-21 15:03:46

为聚焦产品能力，堡垒机产品将于2022年12月30日起停止用户新购传统型堡垒机。若您的业务仍在使用传统型堡垒机，为提供更好的用户体验，建议您尽快切换至 SaaS 型堡垒机。

停售内容

2022年12月30日起停止用户新购传统型堡垒机。

停售影响

从2022年12月30日起，您将无法新购传统型堡垒机，已有的存量传统型堡垒机实例可正常续费、不受影响。

版权所有：腾讯云计算（北京）有限责任公司

关于传统型堡垒机价格调整的公告

最近更新时间：2022-04-07 16:25:47

传统型堡垒机产品自上线以来，服务了众多用户。受当前成本浮动影响，自**2022年05月15日**起，将对传统型堡垒机原有定价进行调整。
调整后的价格如下所示：

售卖规格	管理资产数	单价（元/月）
基础版 S0	50	2,400
基础版 S1	100	4,200
基础版 S2	200	5,700
企业版 S1	500	8,600
企业版 S2	1000	12,500
旗舰版 S1	2000	20,000
旗舰版 S2	5000	30,000

本次价格调整生效日期为**2022年05月15日**，如您此前已经购买或已在使用传统型堡垒机产品，相关价格调整将自**2022年6月15日**起生效（但如您与腾讯云之间就产品价格有特别约定，腾讯云将继续按特别约定价格执行）。请您关注新的计费方式及余额变动，并及时做出业务调整。
若您有任何疑问，欢迎随时 联系我们 。衷心感谢各位用户对腾讯云堡垒机产品的信赖与支持！

关于传统型堡垒机安全漏洞修补的公告

最近更新时间：2023-08-21 15:18:17

近期堡垒机安全团队发现 Spring Framework 存在远程代码执行漏洞，该漏洞会影响部分传统型堡垒机产品，堡垒机安全团队已第一时间关注到该问题，并研判确认了该风险。

危害等级

高危

风险描述

Spring 框架（Framework）是一个开源的轻量级 J2EE 应用程序开发框架，提供了 IOC、AOP 及 MVC 等功能，解决了程序人员在开发中遇到的常见问题，提高了应用程序开发便捷度和软件系统构建效率。由于 Spring 框架存在处理流程缺陷，攻击者可在远程条件下，实现对目标主机的后门文件写入和配置修改，继而通过后门文件访问获得目标主机权限。使用 Spring 框架或衍生框架构建网站等应用，且同时使用 JDK 9及以上版本的，易受此漏洞攻击影响。

对传统型堡垒机的影响

该问题仅对部分传统型堡垒机造成影响，且目前已经发布补丁，我们将在2023年08月21号-2023年08月31号内，通过标准升级流程优先部署这些补丁。

该怎么做?

请您 提交工单 预约升级时间，我们将根据预约时间对您使用的产品进行升级。

产品简介
产品概述

最近更新时间：2024-05-29 17:00:45

堡垒机是集用户（Account）管理、授权（Authorization）管理、认证（Authentication）管理和综合审计（Audit）于一体的集中运维管理系统。
堡垒机主要特点：

- 为企业提供集中的管理平台，减少系统维护工作。
- 为企业提供用户和资源管理功能，降低企业维护成本。
- 帮助企业制定严格的资源访问策略，并且采用强身份认证手段，保障系统资源安全。
- 详细记录用户对资源的访问及操作，达到对用户行为审计的需要。

版权所有：腾讯云计算（北京）有限责任公司

产品优势

最近更新时间：2024-06-12 16:02:01

用户账号全生命周期管理

- 主账号支持分组管理：分组可以采用树形方式展现，不限制分组层级数量。
- 完整的用户账号管理：生命周期管理，实现账号的创建、维护、修改、删除的集中管理。

灵活的授权管理功能

资源授权模式基于工作组授权，工作组授权概念十分灵活，建立后可绑定已有用户及资源、账号，也可直接在工作组上新建用户及资源、账号，这样授权可迁移、授权粒度更细；并可针对工作组设置相关安全策略。

便捷的快速登录功能

运维人员可将经常访问的资源自动添加到历史登录记录中，运维人员点击历史记录，便可快速进行单点登录，体现平台运维便捷性，易用性。

完备的审计管理功能

支持对 Linux系统 和 Windows系统 会话进行审计回放，管理员可以随时查看运维人员的操作。

版权所有：腾讯云计算（北京）有限责任公司

应用场景

最近更新时间：2024-06-12 16:02:01

权限精细化管理

大多数企事业单位的 IT 运维均采用设备、操作系统自身的授权系统，授权功能分散在各设备和系统中。
使用堡垒机之后，管理人员可配置精细化的运维操作授权策略，实现基于企事业单位所需的最小权限分配原则管理用户权限。避免出现运维人员权限过大、内部操作权限滥用等问题。

协助安全事件定位

在运维工作中，大多是通过各网络设备、操作系统的系统日志进行监控审计，但是由于各系统自身审计日志分散、内容深浅不一，且无法根据业务要求制定统一审计策略。
使用堡垒机之后，运维人员通过堡垒机访问目标资产的行为将被记录下来，一旦出现安全事故，堡垒机可协助管理人员对安全事件进行定位，避免系统自身审计无法及时发现违规操作行为的问题。

第三方代维人员管理

目前，很多大型企业选择将非核心业务外包给设备商或代维公司，在享受便利的同时，由于代维人员流动性大、对操作行为缺少监控带来的风险日益凸显。
使用堡垒机之后，通过严格的权限控制和操作行为审计，实现对代维人员的行为审计和权限管理。

版权所有：腾讯云计算（北京）有限责任公司

购买指南
计费概述

最近更新时间：2022-06-14 14:35:03

计费说明

堡垒机包含两部分费用：堡垒机和云服务器。
堡垒机需另购云服务器作为软件系统的载体，云服务器费用另外结算。

选型指导

选购堡垒机时，一般以您的云服务器数作为依据。您在采购前可简单统计云服务器数量，以选择合适您的环境的规格型号。

售卖规格	管理资产数	单价（元/月）
基础版 S0	50	2,400
基础版 S1	100	4,200
基础版 S2	200	5,700
企业版 S1	500	8,600
企业版 S2	1000	12,500
旗舰版 S1	2000	20,000
旗舰版 S2	5000	30,000

版权所有：腾讯云计算（北京）有限责任公司

购买方式

最近更新时间：2023-06-30 15:42:15

传统型堡垒机已于2022年12月30日起停止用户新购，更多详情请参见 关于传统型堡垒机停售的公告 。

欠费说明

最近更新时间：2021-06-02 15:50:54

堡垒机除服务本身外，产品所在云服务器实例如果欠费也将导致服务停止，请确保云服务器处于正常状态。

到期预警

堡垒机服务或所在云服务器实例会在到期前第7天内，向您推送到期预警消息，预警消息将通过邮件及短信的方式通知到腾讯云账户的创建者以及全局资源协作者、财务协作者。

欠费预警

堡垒机服务或所在云服务器实例到期当天及以后，将向您推送欠费隔离预警消息，预警消息将通过邮件及短信的方式通知到腾讯云账户的创建者以及所有协作者。

回收机制

- 堡垒机服务或所在云服务器实例到期前7天内，系统会给您发送续费提醒通知。
- 账户余额充足的情况下，若您已设置自动续费，设备在到期当日会执行自动续费。
- 若您的堡垒机服务或所在云服务器实例在到期前（包括到期当天）未进行续费，系统将在到期时间点开始对其做停服处理（云服务器设备断网关机，堡垒机停止服务，仅保留数据），云服务器进入回收站。
  云服务器进入回收站后，将被强制解除与负载均衡、弹性云盘、基础网络互通的挂载关系。续费恢复后，其挂载关系不恢复，需要您重新配置。
- 到期次日至到期后7天，您仍可以在回收站对设备进行续费找回。**云服务器被续费找回的实例，其续费周期的起始时间为上一个周期的到期日。堡垒机，被续费找回的续费周期是续费起当天。**
- 若您的堡垒机所在云服务器实例在到期7天后（包括第7天）未进行续费，系统将在到期后第8天的0点开始对资源释放，到期服务器中的数据将被清除且不可恢复，并且绑定的弹性公网 IP 将被释放。
- 若您的堡垒机服务在到期7天后（包括第7天）未进行续费，但所在云服务器实例一直进行续费，则堡垒机服务将停止服务，但数据不清除。

> **说明**
> 云服务器实例在账户余额充足的情况下，若您已设置自动续费，设备在到期当日会执行自动续费。

退费说明

最近更新时间：2022-03-14 19:05:57

堡垒机服务一旦购买，不支持无理由退款。若您在使用中有任何疑问或需要帮助，您可 联系我们 。

快速入门
控制台登录

最近更新时间：2024-09-18 18:11:51

购买堡垒机后，您可进入堡垒机管理界面进行配置，下面将为您详细介绍如何进入管理页面。

操作步骤

1. 登录 堡垒机控制台，单击**查看传统型**。

2. 部署实例。在堡垒机控制台，可以看到您已购买的堡垒机实例，选择任意堡垒机实例，单击**部署**，即可完成堡垒机实例的部署。
3. 管理堡垒机实例。选择一台已部署好的堡垒机实例，在右侧操作栏，单击**管理**，浏览器将弹出新窗口以显示堡垒机登录界面。
4. 登录堡垒机系统。 在登录界面，输入系统管理员账户 admin 与密码（默认密码在购买时将通过站内信发送）进入管理界面，即可开始堡垒机的配置。配置堡垒机系统请您先查看 管理配置总览 。

> **说明：**
> 堡垒机登录界面参数说明：
> - 用户ID：输入堡垒机用户的用户名。
> - 静态口令：登录密码。
> - 堡垒机系统的主管理账号为 admin，具有配置系统所有参数的权限，为确保系统安全，不同用户的 admin 账号密码不同，admin 默认密码将在购买后由腾讯云站内信发送，烦请注意站内信消息。
> - 若您忘记管理账号密码，可以 提交工单 联系我们进行解决。

后续步骤

登录堡垒机后，可以根据需求进行相关操作，详情请参见 管理配置手册 。

初次上线配置

最近更新时间：2024-09-18 18:11:51

本文为您详细介绍堡垒机的基本配置。

操作步骤

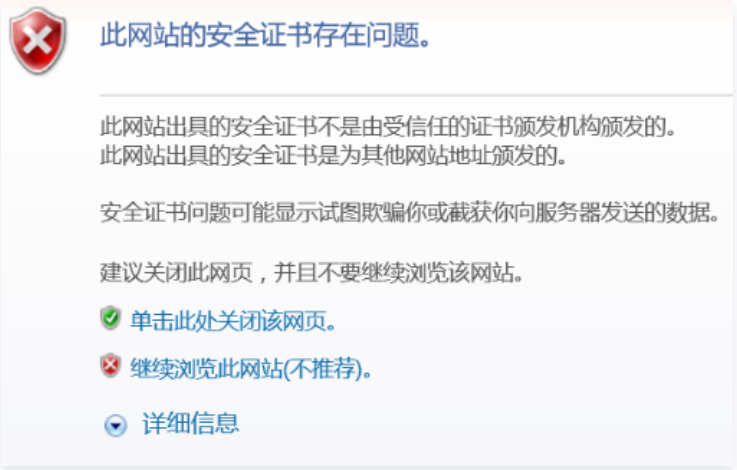
步骤1：登录系统

1. 在浏览器地址栏中，输入 `https://堡垒机IP` ，单击回车。

> **说明：**
> 堡垒机系统采用加密型的 HTTP 方式（即 HTTPS）进行访问。

2. 在弹出的证书错误（由于采用 SSL 技术）提示框中，单击**继续浏览此网站**，输入账号和静态口令，即可登录堡垒机。

> **说明：**
> 若出现登录失败的情况，请 提交工单 联系我们。



步骤2：修改根节点

首次登录可将根目录改为对应公司名称或项目名称，以便组织结构创建和管理。

1. 在主菜单中，选择**数据中心** > **编辑节点**。
2. 在名称处输入节点名称，如“Tencent”，则根目录将修改为“Tencent”。

步骤3：新建组织结构

修改完根目录后创建组织结构，以便管理堡垒机中的人员资源等信息，支持多层级分类创建组织结构，可按照公司组织结构或资源分组管理情况来建设，以为“Tencent”的“安全部门”创建组织结构为例进行说明。

1. 在左侧导航栏中，选择需要创建组织结构的节点。

2. 在左上角单击**+**，输入组织结构名称“授权组”，并选择组织结构类型为“工作组”：

3. 单击**确定**，完成组织结构“授权组”的新建。

步骤4：添加资源（目标设备）

组织结构创建完成后，可进行资源添加，通过“资源管理”模块，将需要管理的设备信息导入到堡垒机。

> **说明**
> 资源管理模块可对资源和资源账号以及账号登录方式进行管理。

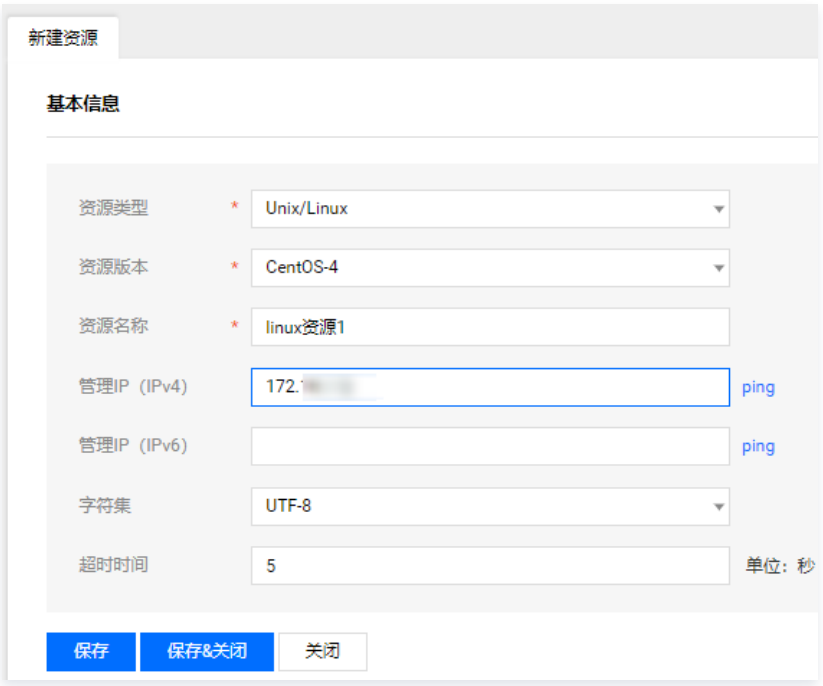
资源添加支持手动添加或自动导入，自动导入时，只导入资源名称和 IP，如果运维设备时，需堡垒机进行代填，需将设备账号手动录入堡垒机。

手动添加

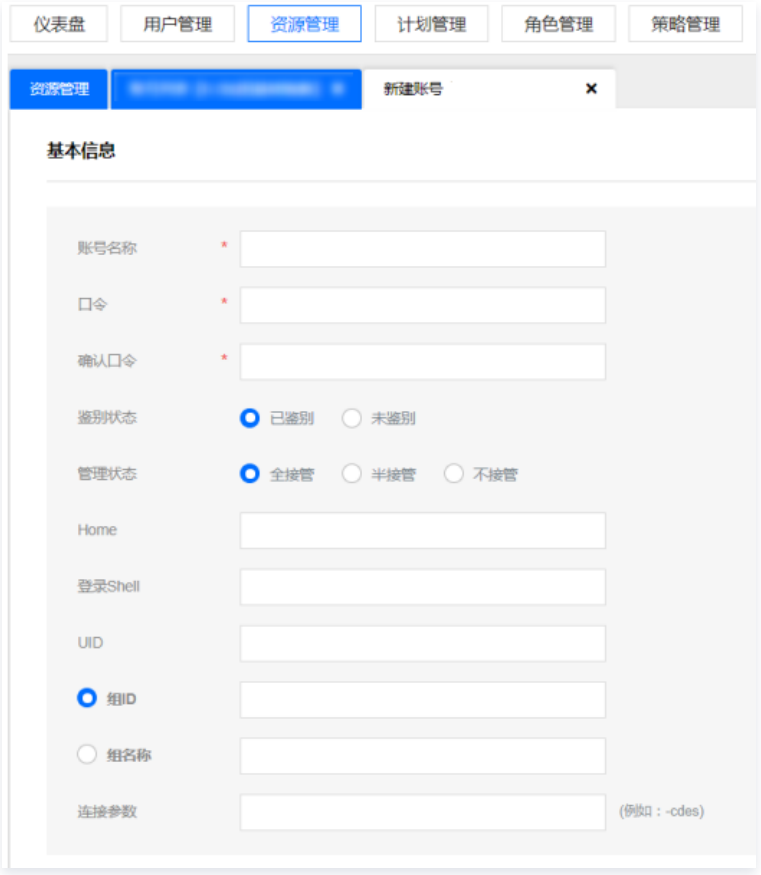
以下为“授权组”手动添加设备“linux资源1”，IP：172.16.x.x、资源账号“root”的操作步骤：

1. 在左侧导航中，单击**授权组**，进入授权组页面，选择**绑定资源** > **新建并绑定**。

2. 选择资源类型、资源版本、资源名称、管理 IP、字符集和超时时间，单击**保存&关闭**。



3. 如果需要绑定资源账号，在左侧导航中，选择授权组根节点，单击**资源管理**。
4. 选择需要添加账号的资源，在右侧的“账号列表”栏，单击，进入账号列表页面。
5. 在账号列表页面，单击**新建**，填上相应的账号信息，单击**保存**即可。



步骤5：新建用户

以上步骤完成后，即完成基本信息的录入工作，此时进行用户创建以及资源和用户授权绑定，所有操作完成后，堡垒机上线前的配置工作即可完成。

在相对应的组节点下创建和管理用户，通过“用户管理”模块进行用户账号管理和授权分配管理。以下是在“授权组”下创建普通运维用户“test”和授权资源步骤。

1. 在左侧导航中，单击**授权组**，在授权组页面选择**绑定用户** > **新建并绑定**。

2. 单击**保存**完成用户创建。

运维人员入门

最近更新时间：2024-09-18 18:11:51

本文为您详细介绍运维人员安装控件、登录堡垒机并使用单点登录工具登录资源等一系列操作。

操作步骤

步骤1：登录系统

在浏览器地址栏中输入 `https://堡垒机IP` ，打开堡垒机登录页面，输入运维用户的用户名和密码进行登录。

> **说明：**
> 运维用户由管理员账号进行创建，若运维用户忘记密码，可以联系管理员进行重置，详情请参见 设置口令 。

步骤2：安装控件

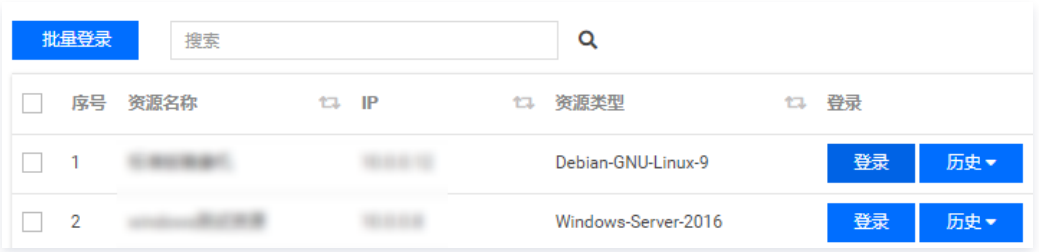
> **说明：**
> 运维用户第一次访问运维审计与管控系统，需下载单点登录工具，已安装过无需再安装。

单击，进入套件中心，根据需求下载单点登录工具或根证书。

- 单点登录工具（标准）：集成审计查看工具标准版。
- 根证书：根证书安装后可使页面响应速度加快，另外，使用证书认证的客户端需安装根证书。安装证书步骤请参见 安装证书 文档。

步骤3：单点登录

1. 在堡垒机中，选择**运维** > **授权列表**，进入授权列表中。
2. 在授权列表中，选择需要操作的资源，单击**登录**。



3. 在弹出的“配置登录”弹窗中，输入账号密码并选择连接方式，单击**登录**，连接到服务器，完成单点登录。

单点登录工具支持列表

资源类型	支持方式			
Windows	Mstsc	FTP	-	-
Linux	Xshell	SecureCRT	putty	VNC
	Xwindow	FTP	SFTP	-

说明：
除使用上述工具登录之外，还支持使用浏览器通过 Web 方式登录。

相关操作

MAC 和 Linux 终端运维操作

MAC 和 Linux 终端运维操作时，推荐使用 Safari、Firefox、Chrome 浏览器。针对 MAC、Linux 终端运维时，仅限于通过 WEB 工具进行目标资源登录。

Firefox、Chrome、Safari 浏览器操作

- Firefox 及 Chrome 浏览器访问时，需选择**高级 > 接受风险并继续**。

- Safari 浏览器操作时，需输入 MAC 系统管理员密码安装证书。

版权所有：腾讯云计算（北京）有限责任公司

操作指南
管理配置手册
管理配置总览

最近更新时间：2024-09-18 18:11:51

概述

您在使用堡垒机时，可能碰到诸如登录系统、策略配置、行为审计、网络配置、认证配置等问题。本文将介绍堡垒机产品使用过程中的常用操作，供您参考。

登录系统

为您介绍以下几种常用登录堡垒机的方式：

- 使用静态口令登录
- 使用动态口令登录
- 使用证书登录
- 使用 AD 域认证登录
- 使用短信认证登录

组织管理

基于用户、资源、综合方式进行分层分类分级管理。

- 根节点
  - 添加组织结构
  - 修改组织结构
  - 删除组织结构
- 综合组
  - 新增综合组
  - 编辑综合组
  - 删除综合组
- 资源组
- 新增资源组
- 编辑资源组
- 删除资源组
- 工作组
- 新增工作组
- 编辑工作组
- 删除工作组

用户管理

提供用户账号的创建、维护、修改、删除的集中管理，用户的树形分组展示及导入导出。提供资源与用户的授权关系绑定以及认证方式修改。可基于用户的配置口令、访问锁定、访问时间等安全策略。

- 添加用户
- 删除用户
- 用户编辑
  - 编辑用户基本信息
  - 设置口令
  - 设置用户认证方式
  - 设置用户策略
  - 唯一标识
  - 证书管理

- 用户相关操作
- 注销用户
- 锁定用户
- 解锁用户
- 批量修改组织结构
- 为选中用户绑定角色
- 为选中用户绑定授权
- 导入用户
- 导出用户
- 添加用户类型
- 查询用户
- 用户角色授权
- 用户授权

资源管理

资源即我们的 IT 资产，如服务器，数据库，应用系统等，该功能模块提供了资源的统计、分组管理、树形展现，支持主流的大部分资源类型和资源协议。

- 添加资源
- 删除资源
- 编辑资源
- 查询资源
- 资源账号列表
- 添加账号
- 编辑账号
- 删除账号
- 查询账号
- 批量修改口令
- 批量修改鉴别状态
- 批量修改接管状态
- 批量删除被接管资源账号
- 查看口令修改日志
- 账号拨测
- 资源类型配置
- 资源相关操作
- 批量修改协议端口
- 导出资源
- 导入资源
- 批量资源下线
- 批量修改组织结构
- 资源同步
- 统计视图
- 账号导出计划

策略管理

堡垒机提供了丰富的安全策略功能，可根据访问堡垒机或资源的权限需求来灵活设置访问或审计权限。

- 普通策略
- 添加资源账号策略
- 添加时间策略
- 添加口令策略

- 添加锁定策略
- 访问控制策略
- 添加字符命令策略
- 添加 FTP 访问控制策略
- 添加图形访问控制策略
- 审计策略
- 添加字符审计策略
- 添加 FTP 审计策略
- 添加图形审计策略

工作组

堡垒机基于工作组的资源授权模式，在工作组上绑定资源账号，并可针对工作组设置相关安全策略。

- 绑定用户
- 绑定资源
- 绑定策略

审计管理

堡垒机提供基础业务数据报表生成和下载，行为审计报表和接管资源账号的信息管理等报表生成和下载。

- 管理审计
- 安全认证审计
- 基础信息维护审计
- 操作行为审计
- 在线会话审计
- 历史会话审计
- 统计报表
- 基础报表
- 运维业务报表
- 查询审计日志

计划管理

堡垒机可对接管资源进行定期改密、账号抽取、拨测、推送。

- 创建任务
- 编辑任务
- 资源账号
- 添加资源账号
- 删除资源账号
- 搜索资源账号
- 删除任务
- 查询任务
- 任务启动停止
- 查看操作日志
- 查看执行日志

系统管理

提供了系统自身的管理功能，如数据备份、还原、系统运行状态的监控、审计日志清理、重启等。

- 系统配置
- 系统监控
- 系统维护
- 服务器配置

版权所有：腾讯云计算（北京）有限责任公司

- 配置系统时间
- 配置邮件服务
- 端口开放管理
- 配置 Syslog
- 配置消息公告
- 安全认证配置
- 配置全局认证方式
- 配置全局密钥
- 超时设置
- 配置 OTP 认证
- 配置域认证
- 配置证书
- 配置短信认证
- 初始化口令配置
- 运维安全水印
- 数据维护
- 配置数据维护
- 审计数据维护

版权所有：腾讯云计算（北京）有限责任公司

登录系统
登录概述

最近更新时间：2024-09-18 18:11:51

开放端口

堡垒机入站、从堡垒机到受管控机器，需要分别开放什么端口?

当用户操作堡垒机出现网络问题时，例如登录不了堡垒机，可参照下面入站规则和受管控机器提供的端口，检查对应端口号是否有开通。

入站规则

从客户端到堡垒机，需要开放的端口如下表所示：

端口号	说明	协议	备注	是否必开
61903	SSH/SFTP/FTP/文件共享	TCP	字符协议及文件传输访问端口	是
443	HTTPS	TCP	Web 管理端口	是
3392	RDP2	TCP	RDP2 单点登录和审计播放	是
10050	-	TCP	字符审计录像播放	是
11020	-	TCP	认证端口	是
8443	HTTPS	TCP	证书认证登录	否

说明：
堡垒机安全组的出站规则已自动配置，一般情况下，无需再对出站规则进行其他配置。

受管控机器

堡垒机管控的后端资源服务器的安全组里放开如下端口（**可根据自身服务器端口开启**）。

端口号	说明
20	FTP/SFTP（主动模式）
21	FTP/SFTP（主动/被动模式）
22	SSH
23	Telnet
389	AD LDAP
3389	RDP

说明：
对于 xwindow、vnc 协议，其端口采用实际使用的端口。

登录认证说明

系统登录主要的工作就是系统认证。系统登录界面随系统配置的认证方式不同而有所差异。堡垒机系统支持的认证方式包括静态口令认证、证书认证、动态口令认证、域认证等。
无论堡垒机系统配置哪种认证方式，登录堡垒机都需要在浏览器中输入服务地址。例如：`https://192.168.23.107`。在该例中，`192.168.23.107` 为堡垒机系统 IP 地址（堡垒机系统出厂设置的管理 IP，为购买后的内外网 IP）。当在浏览器中输入示例内容后，敲击回车（堡垒机系统配置双向认证时，如果需要域名方式访问的情况除外）系统自动转向到登录界面。

使用静态口令登录

最近更新时间：2024-09-18 18:11:51

概述

堡垒机默认使用静态口令方式进行登录。

登录系统

1. 登录 堡垒机控制台，找到需要操作的堡垒机，在右侧操作栏单击**管理**，进入堡垒机登录页面，也可以直接在浏览器中，输入访问地址 `https://IP`，进入登录页面。
2. 在登录界面输入用户 ID 与静态口令，并完成滑块验证。

3. 验证之后单击**登录**，即可登录堡垒机。

使用动态口令登录

最近更新时间：2024-09-18 18:11:51

堡垒机系统默认使用静态口令方式进行登录，若要使用 OTP 口令方式进行登录认证，您可查看本文档指引进行登录。

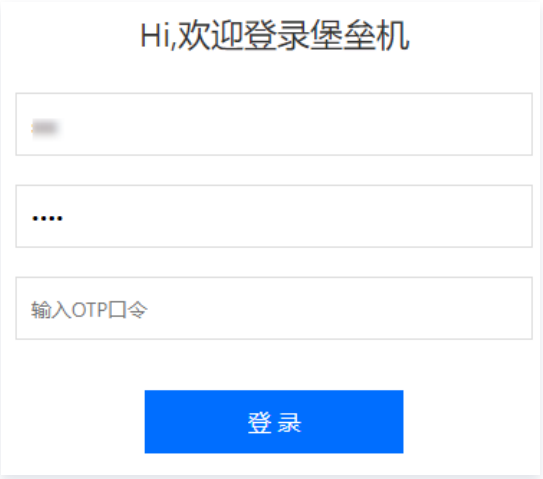
前提条件

管理员需要已完成 配置 OTP 认证 。

操作步骤

1. 登录 堡垒机控制台，找到需要操作的堡垒机，在右侧操作栏单击**管理**，进入堡垒机登录页面，也可以直接在浏览器中，输入访问地址 `https://IP` ，进入登录页面。
2. 使用管理员账号登录堡垒机，在上方导航中，单击**用户管理**，在用户管理页面找到需要生成个人证书的运维用户，在编辑栏，单击 。

3. 在用户编辑页面，单击**设置认证方式**，选择“静态口令认证”及“ OTP 认证（一次性口令）”，单击**保存**即完成设置。
4. 在用户编辑页面，单击**唯一标识**，使用 Google 动态密码验证器扫描二维码，生成6位数字动态口令，使用手机令牌登录。
5. 返回堡垒机登录页面，在登录堡垒机界面输入运维用户名、密码后，正确拖动滑块，单击**登录**，即可使用 OTP 口令，即使用手机令牌生成的6位数字动态口令登录堡垒机。



使用证书登录

最近更新时间：2024-09-18 18:11:51

本文档将介绍如何生成、下载并安装证书，并使用证书登录堡垒机。

概述

堡垒机默认使用静态口令方式进行登录，若管理员配置了使用证书认证方式登录堡垒机，您可查看本文档指引进行登录。系统支持第三方证书和本地证书登录认证，开启证书认证需客户端到堡垒机的8443端口畅通。证书服务使用前需提前设置用户证书登录认证和开启证书认证服务。
以下以堡垒机自带的本地证书认证为例进行说明，堡垒机开启运维用户使用本地自签发证书认证登录系统时，运维用户需要安装根证书和个人证书。

> **注意：**
> 证书认证需使用谷歌浏览器。

操作步骤

步骤1：安装根证书

1. 登录 堡垒机控制台，找到需要操作的堡垒机，在右侧操作栏单击**管理**，进入堡垒机登录页面，也可以直接在浏览器中，输入访问地址 `https://IP` ，进入登录页面。
2. 使用运维账号登录堡垒机，在页面左上角单击“套件中心”图标，进入套件中心页面，在根证书下方，单击**下载**。

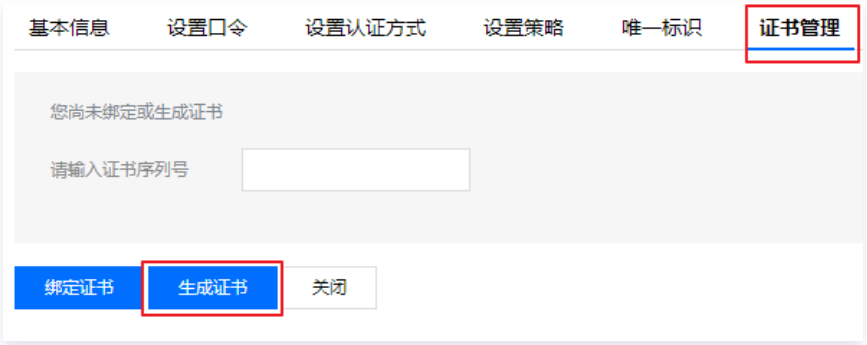
3. 下载完成后，将根证书安装到谷歌浏览器中，单击证书进行安装，安装时选择“受信任的根证书颁发机构”，选择完成后，单击**下一步**安装完成。

步骤2：生成并安装个人证书

1. 安装个人证书，个人证书由管理员生成后下发给各用户，登录 堡垒机控制台，找到需要操作的堡垒机，在右侧操作栏单击**管理**，进入堡垒机登录页面，也可以直接在浏览器中，输入访问地址 `https://IP` ，进入登录页面。

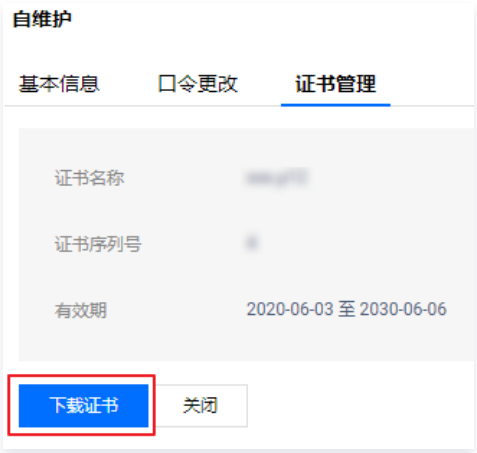
2. 使用管理员账号登录堡垒机，在上方导航中，单击**用户管理**，在用户管理页面找到需要生成个人证书的运维用户，在编辑栏，单击 。

3. 在用户编辑页面，选择**证书管理** > **生成证书**，即可完成证书生成。



4. 证书生成后，运维用户登录堡垒机，在页面右上角，选择**用户名>自维护**。

5. 在自维护页面，选择**证书管理** > **下载证书**，进行证书下载。



6. 下载完成后，单击证书进行安装，安装时选择“个人”，选择完成后，单击**下一步**安装完成。

> **说明：**
> 输入私钥密码 zD3A7S9B#&2uS。

步骤3：设置认证方式

1. 登录 堡垒机控制台，找到需要操作的堡垒机，在右侧操作栏单击**管理**，进入堡垒机登录页面，也可以直接在浏览器中，输入访问地址 `https://IP` ，进入登录页面。
2. 使用管理员账号登录堡垒机，在上方导航中，单击**用户管理**，在用户管理页面找到需要生成个人证书的运维用户，在编辑栏，单击 。

3. 在用户编辑页面，单击**设置认证方式**，选择“静态口令认证”及“证书认证”，单击**保存**即完成设置。

步骤4：使用证书登录系统

1. 登录 堡垒机控制台，找到需要操作的堡垒机，在右侧操作栏单击**管理**，进入堡垒机登录页面，也可以直接在浏览器中，输入访问地址 `https://IP` ，进入登录页面。
2. 在登录堡垒机界面输入运维用户名、密码后，正确拖动滑块，单击**登录**，即可选择证书登录堡垒机。

使用 AD 域认证登录

最近更新时间：2024-09-18 18:11:51

堡垒机系统默认使用静态口令方式进行登录，若要使用 AD 域方式进行登录认证，您可查看本文档指引进行登录。

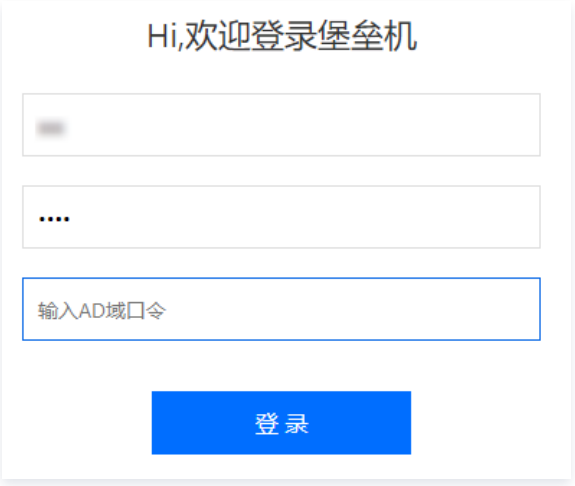
前提条件

管理员需要已完成 配置域服务 。

操作步骤

1. 登录 堡垒机控制台，找到需要操作的堡垒机，在右侧操作栏单击**管理**，进入堡垒机登录页面，也可以直接在浏览器中，输入访问地址 `https://IP` ，进入登录页面。
2. 使用管理员账号登录堡垒机，在上方导航中，单击**用户管理**，在用户管理页面找到需要生成个人证书的运维用户，在编辑栏，单击 。

3. 在用户编辑页面，单击**设置认证方式**，选择“静态口令认证”及“ AD 域认证”，单击**保存**即完成设置。
4. 返回堡垒机登录页面，在登录堡垒机界面输入运维用户名、密码后，正确拖动滑块，单击**登录**，即可使用 AD 域登录堡垒机。



使用短信认证登录

最近更新时间：2024-09-18 18:11:51

堡垒机系统默认使用静态口令方式进行登录，若要使用短信认证方式进行登录，您可查看本文档指引进行操作。

前提条件

管理员需要已完成 配置短信认证 。

操作步骤

1. 登录 堡垒机控制台，找到需要操作的堡垒机，在右侧操作栏单击**管理**，进入堡垒机登录页面，也可以直接在浏览器中，输入访问地址 `https://IP` ，进入登录页面，并使用管理员账号登录堡垒机。
2. 在堡垒机在上方导航中，单击**用户管理**，在用户管理页面找到需要使用短信登录的运维用户，在编辑栏，单击“用户编辑”图标。

3. 在用户编辑页面，单击**设置认证方式**，选择“静态口令认证”及“短信认证”，单击**保存**即完成设置。

4. 返回堡垒机登录页面，在登录堡垒机界面输入运维用户名、密码后，正确拖动滑块，单击**登录**，即可使用短信认证方式登录堡垒机。

组织管理
根节点
添加组织结构

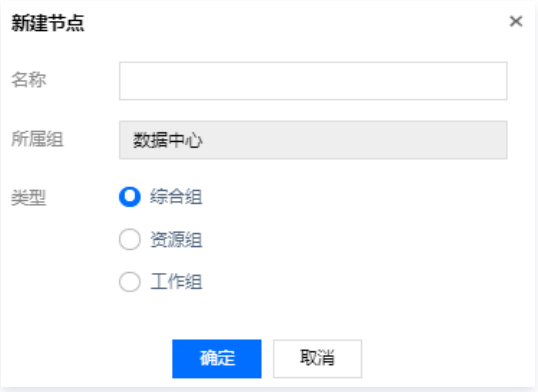
最近更新时间：2024-09-18 18:11:51

操作场景

堡垒机系统可通过组织结构模块统一管理用户、资源。组织结构支持分组管理，分组可以采用树形方式展现，不限制分组层级数量。下面将为您详细介绍如何添加组织结构。

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. 登录系统默认显示根节点（数据中心），选中根节点，可以查看右侧菜单栏显示以下模块：仪表盘、用户管理、资源管理、计划管理、角色管理、策略管理。
3. 单击页面最左侧组织结构列表上方的 + ，进入新建节点页面。
4. 可以添加综合组、资源组或工作组。输入名称，选择相应的组类型。



5. 单击**确定**，即可添加该组织结构。

修改组织结构

最近更新时间：2024-09-18 18:11:51

操作场景

若您需要修改组织结构信息，重新编辑该组织结构即可。下面将为您详细介绍如何修改组织结构。

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. 在组织结构列表中，选择已添加的组织结构，单击 组织结构编辑按钮。
3. 在编辑窗口中，输入要修改的组织结构名称。
4. 单击**确定**，即可修改组织结构。

删除组织结构

最近更新时间：2024-09-18 18:11:51

操作场景

当堡垒机系统上某组织不再维护时，您可将该组织结构删除。以下将为您详细介绍如何删除组织结构。

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. 在组织结构列表中，选择已添加的组织结构，单击 组织结构删除按钮。
3. 在弹出的确认提示框中，单击**确定**，即可删除该组织结构。

综合组
新增综合组

最近更新时间：2024-09-18 18:11:51

操作场景

若您需要综合的汇总用户管理、资源管理、计划管理及角色管理，或业务及组织结构需要多层级的创建子集时，可以新增综合组。

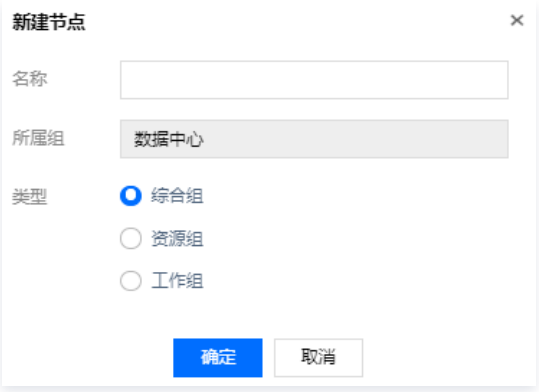
操作步骤

1. 登录腾讯云 堡垒机控制台 ，选择一台已部署好的堡垒机实例，在右侧操作栏，单击**管理**，进入堡垒机登录页面。
2. 使用管理员账号登录堡垒机。

> **说明**
> 若忘记管理员账号密码，可以 提交工单 联系我们进行解决。

3. 在左侧组织结构列表，单击需要添加综合组的节点或其子节点，在左侧组织结构列表上方，单击 + 按钮，进入新建节点页面。
4. 在新建节点页面，输入综合组名称、所属组为当前添加综合组所属根节点（无法编辑）、类型选择综合组，填写完成后，单击**确定**，即完成添加。

> **说明**
> 名称只能由中文、大小写字母、数字、@_-.字符组成，且长度在64位以内。



编辑综合组

最近更新时间：2024-09-18 18:11:51

操作场景

若您需要修改综合组名称时，可以对综合组进行编辑。

操作步骤

1. 登录腾讯云 堡垒机控制台 ，选择一台已部署好的堡垒机实例，在右侧操作栏，单击**管理**，进入堡垒机登录页面。
2. 使用管理员账号登录堡垒机。

> **说明**
> 若忘记管理员账号密码，可以 提交工单 联系我们进行解决。

3. 在左侧组织结构列表，单击需要编辑综合组的节点或其子节点，在左侧组织结构列表上方，单击 按钮，进入编辑节点页面。
4. 在编辑节点页面，可以修改综合组名称，所属组为当前添加综合组所属根节点（无法修改）、类型为综合组（无法修改），修改完成后，单击**确定**，即完成编辑。

> **说明**
> 名称只能由中文、大小写字母、数字、@_-.字符组成，且长度在64位以内。

删除综合组

最近更新时间：2024-09-18 18:11:51

操作场景

若您需要删除综合组或需要删除某综合组下所有相关信息（例如，用户、角色、独有资源、计划、工作组、账号及账号关联的授权信息等）时，可以直接对综合组进行删除操作。

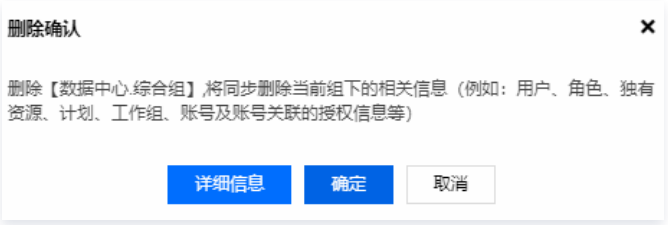
操作步骤

1. 登录腾讯云 堡垒机控制台 ，选择一台已部署好的堡垒机实例，在右侧操作栏，单击**管理**，进入堡垒机登录页面。
2. 使用管理员账号登录堡垒机。

> **说明**
> 若忘记管理员账号密码，可以 提交工单 联系我们进行解决。

3. 在左侧组织结构列表，选择需要删除综合组的节点或其子节点，在左侧组织结构列表上方，单击 按钮，进入删除节点操作确认页面。
4. 在操作确认页面，确认删除信息，单击**详细信息**，可以查看所删除节点详细信息，确认完成后，单击**确定**，即可删除该组织结构。

> **注意**
> 在删除综合组时，将同步删除当前组下的相关信息，例如，用户、角色、独有资源、计划、工作组、账号及账号关联的授权信息等，因此在非必要情况下，建议您删除相应子节点即可。



资源组
新增资源组

最近更新时间：2024-09-18 18:11:52

操作场景

资源组为资源的汇总，若您需要添加 Windows 或 Linux 资源类型及相应的资源版本，可以添加资源组，或当业务及组织结构需要多层级的创建资源分类时，也可以添加资源组。

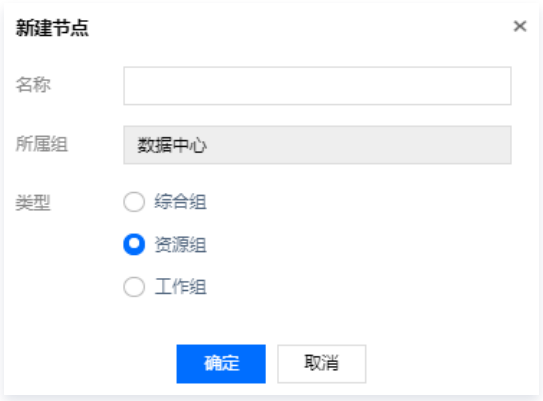
操作步骤

1. 登录腾讯云 堡垒机控制台 ，选择一台已部署好的堡垒机实例，在右侧操作栏，单击**管理**，进入堡垒机登录页面。
2. 使用管理员账号登录堡垒机。

> **说明**
> 若忘记管理员账号密码，可以 提交工单 联系我们进行解决。

3. 在左侧组织结构列表，单击需要添加资源组的节点或其子节点，在左侧组织结构列表上方，单击 + 按钮，进入新建节点页面。
4. 在新建节点页面，输入资源组名称、所属组为当前添加资源组所属根节点（无法编辑）、类型选择资源组，填写完成后，单击**确定**，即完成添加。

> **说明**
> 名称只能由中文、大小写字母、数字、@_-.字符组成，且长度在64位以内。



编辑资源组

最近更新时间：2024-09-18 18:11:52

操作场景

若您需要修改资源组名称时，可以对资源组进行编辑。

操作步骤

1. 登录腾讯云 堡垒机控制台 ，选择一台已部署好的堡垒机实例，在右侧操作栏，单击**管理**，进入堡垒机登录页面。
2. 使用管理员账号登录堡垒机。

> **说明**
> 若忘记管理员账号密码，可以 提交工单 联系我们进行重置。

3. 在左侧组织结构列表，单击需要编辑资源组的节点或其子节点，在左侧组织结构列表上方，单击按钮，进入编辑节点页面。
4. 在编辑节点页面，可以修改资源组名称，所属组为当前编辑资源组所属根节点（无法修改）、类型为资源组（无法修改），修改完成后，单击**确定**，即完成编辑。

> **说明**
> 名称只能由中文、大小写字母、数字、@_-.字符组成，且长度在64位以内。

删除资源组

最近更新时间：2024-09-18 18:11:52

操作场景

若您需要删除资源组或需要删除某资源组下所有相关信息（例如，独有资源、扩展属性等）时，可以直接对资源组进行删除操作。

操作步骤

1. 登录腾讯云 堡垒机控制台 ，选择一台已部署好的堡垒机实例，在右侧操作栏，单击**管理**，进入堡垒机登录页面。
2. 使用管理员账号登录堡垒机。

> **说明**
> 若忘记管理员账号密码，可以 提交工单 联系我们进行重置。

3. 在左侧组织结构列表，选择需要删除资源组的节点或其子节点，在左侧组织结构列表上方，单击 按钮，进入删除节点操作确认页面。
4. 在操作确认页面，确认删除信息，单击**详细信息**，可以查看所删除节点详细信息，确认完成后，单击**确定**，即可删除该资源组的组织结构。

> **注意**
> 在删除资源组时，将同步删除当前组下的相关信息（例如，独有资源、扩展属性等），因此在非必要情况下，建议您删除相应子节点即可。

工作组
新增工作组

最近更新时间：2024-09-18 18:11:52

操作场景

若需要对用户、资源、策略进行新建和绑定操作，可以通过新建工作组进行管理。

操作步骤

1. 登录腾讯云 堡垒机控制台 ，选择一台已部署好的堡垒机实例，在右侧操作栏，单击**管理**，进入堡垒机登录页面。
2. 使用管理员账号登录堡垒机。

> **说明**
> 若忘记管理员账号密码，可以 提交工单 联系我们进行解决。

3. 在左侧组织结构列表，单击需要添加工作组的节点，在左侧组织结构列表上方，单击 + 按钮，进入新建节点页面。
4. 在新建节点页面，输入工作组名称、所属组为当前添加工作组所属根节点（无法编辑）、类型选择工作组，填写完成后，单击**确定**，即完成添加。

> **说明**
> 名称只能由中文、大小写字母、数字、@_-.字符组成，且长度在64位以内。

编辑工作组

最近更新时间：2024-09-18 18:11:52

操作场景

若您需要修改工作组名称时，可以对工作组进行编辑。

操作步骤

1. 登录腾讯云 堡垒机控制台 ，选择一台已部署好的堡垒机实例，在右侧操作栏，单击**管理**，进入堡垒机登录页面。
2. 使用管理员账号登录堡垒机。

> **说明**
> 若忘记管理员账号密码，可以 提交工单 联系我们进行解决。

3. 在左侧组织结构列表，选择需要编辑工作组的节点，在左侧组织结构列表上方，单击按钮，进入编辑节点页面。
4. 在编辑节点页面，可以修改工作组名称，所属组为当前编辑工作组所属根节点（无法修改）、类型为工作组（无法修改），修改完成后，单击**确定**，即完成编辑。

> **说明**
> 名称只能由中文、大小写字母、数字、@_-.字符组成，且长度在64位以内。

删除工作组

最近更新时间：2024-09-18 18:11:52

操作场景

若您需要删除工作组或需要删除所有相关联的工作组授权时，可以直接对工作组进行删除操作。

操作步骤

1. 登录腾讯云 堡垒机控制台 ，选择一台已部署好的堡垒机实例，在右侧操作栏，单击**管理**，进入堡垒机登录页面。
2. 使用管理员账号登录堡垒机。

> **说明**
> 若忘记管理员账号密码，可以 提交工单 联系我们进行解决。

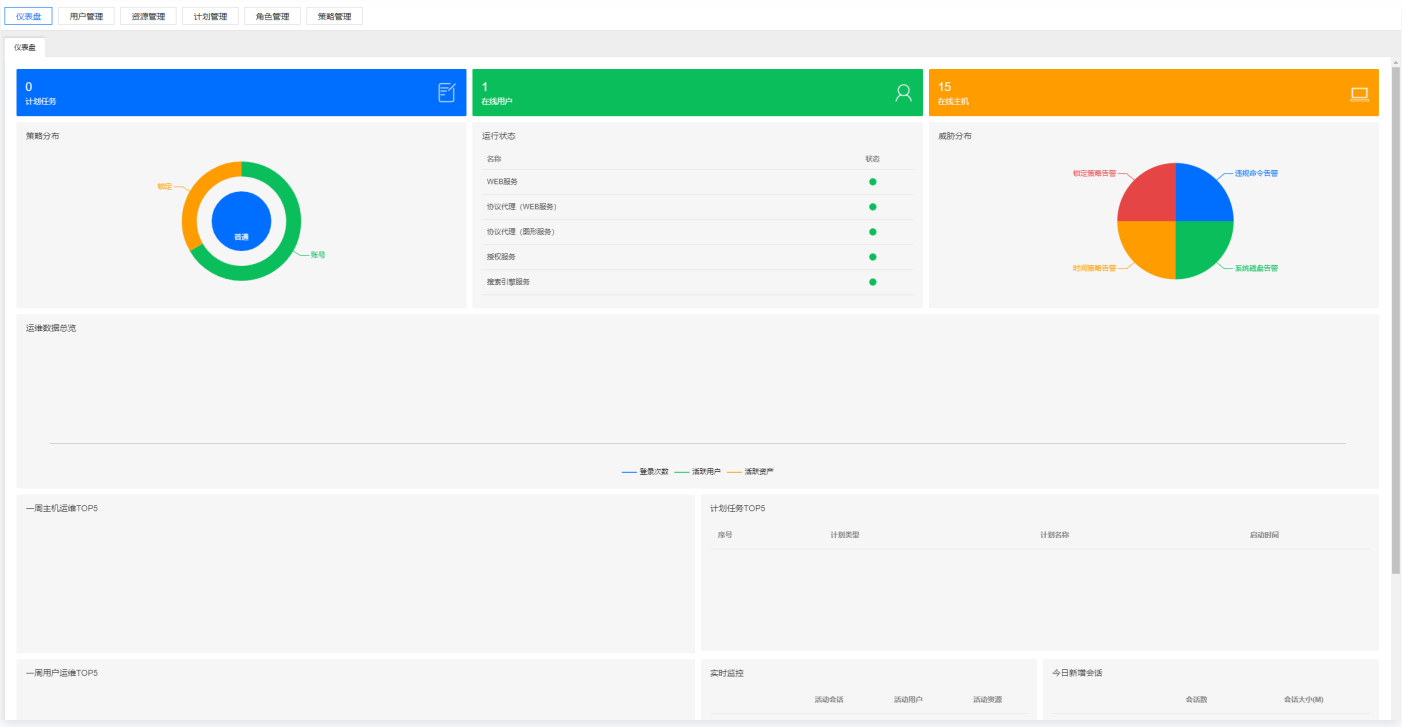
3. 在左侧组织结构列表，选择需要删除工作组的节点，在左侧组织结构列表上方，单击 按钮，进入删除节点操作确认页面。
4. 在操作确认页面，确认删除信息，单击**详细信息**，可以查看所删除节点详细信息，确认完成后，单击**确定**，即可删除该工作组的组织结构。

> **注意**
> 在删除工作组时，将同步删除与所选工作组相关联的工作组授权。

仪表盘

最近更新时间：2024-09-18 18:11:52

1. 登录 堡垒机控制台，找到需要操作的堡垒机，在右侧操作栏单击**管理**，进入堡垒机登录页面，也可以直接在浏览器中，输入访问地址 `https://IP`，进入登录页面。
2. 在堡垒机登录页面，输入堡垒机用户名及密码，进入堡垒机。
3. 在左侧组织结构列表，单击根节点，系统默认显示“仪表盘”模块，可以查看到在线用户、在线主机、离线主机数、策略分布图、运行状态图、威胁分布图等信息。



仪表盘展示说明：

- 在线用户:当前登录到系统的用户总数。
- 在线主机:系统资源在线总数。
- 离线主机:系统资源离线总数。
- 策略分布:查看系统策略分布情况。
- 运行状态：查看系统当前运行是否正常。
- 威胁分布：查看异常访问、弱口令、系统登录等对系统构成威胁相关操作及配置。
- 运维数据总览：查看登录次数、活跃用户、活跃资产的相关数据趋势。
- 一周主机运维 TOP5：查看近一周运维的 TOP5 主机。
- 计划任务 TOP5：查看 TOP5 计划任务。
- 一周用户运维 TOP5：查看近一周运维的 TOP5 用户。
- 实时监控：实时监控字符、图形、文件传输及应用发布的活动会话、活动用户及活动资源的相关数据。
- 今日新增会话：查看字符、图形、文件传输及应用发布的今日新增会话数及大小。
- 系统运行状态：查看当前堡垒机的部署方式及运行时长。
- 许可证信息：查看当前堡垒机的许可证信息。

版权所有：腾讯云计算（北京）有限责任公司

用户管理
添加用户

最近更新时间：2024-10-28 10:29:52

操作场景

堡垒机系统具备统一管理用户功能，下面将为您详细介绍如何在堡垒机创建用户。

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**用户管理**，进入用户管理页面。
3. 单击**新建**，进入添加用户页面，配置如下用户信息。
   - 用户 ID：输入用户 ID，即用于登录堡垒机的账号。
   - 用户名称：输入用户名称。
   - 口令：输入用户的密码。
   - 确认口令：确认用户密码。
   - 用户类型：默认为其他，并勾选“运维用户”。若您需更换类型，请先创建用户类型，详细配置请查看 添加用户类型 文档。

> **注意**
> - 您可以在根节点下添加，也可以在组织结构类型为 “综合组”下添加用户。
> - 页面标 `*` 的为必填项，输入规则查看页面相应提示，“运维用户”为必选项，否则在没有对用户进行角色授权情况下，运维用户无法登录系统。

4. 单击**保存**，即可创建用户。

删除用户

最近更新时间：2024-09-18 18:11:52

操作场景

在发生人员离职或职位变动的情况时，需要删除变动人员的堡垒机系统账号。下面将为您详细介绍如何删除用户。

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. 选择需要删除的节点，单击**用户管理**，进入用户管理页面。
3. 勾选您需要删除的用户，单击**删除**。

4. 在弹出的确认删除窗口中，单击**详细信息**，可查看所删除用户的 ID 及名称，确认完毕后，单击**确定**，即可删除该用户。

用户编辑
编辑用户基本信息

最近更新时间：2025-01-16 21:01:21

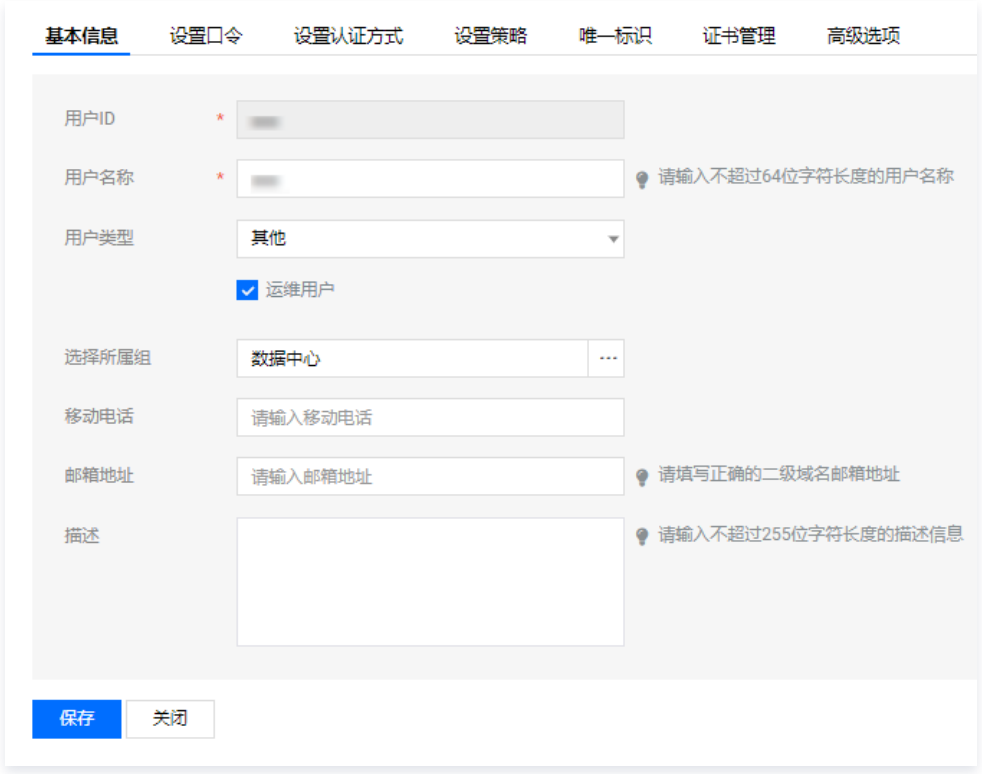
操作场景

该指南指导您在登录堡垒机后，通过用户管理功能修改已添加用户的相关信息。

操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 选择需要编辑用户信息的节点，单击**用户管理**，进入用户管理页面。
4. 找到您需要修改信息的用户，在右侧编辑栏中，单击 进入基本信息编辑页面。

5. 修改完用户信息后，单击**保存**即可完成修改。



设置口令

最近更新时间：2025-01-16 21:01:21

操作场景

本文将为您详细介绍如何设置用户口令，或当用户忘记密码、需要修改密码或密码过期时，如何对账户密码进行重置。

操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 单击**用户管理**，进入用户管理页面。
4. 在用户列表选择需要编辑的用户，单击 ，进入用户信息编辑页面。
5. 单击**设置口令**，有如下三种口令设置方式。
   - **手动指令口令**：输入口令，确认口令，单击**保存**即可完成配置。
   - **初始化为固定口令**：不需要用户输入口令，点击保存按钮完成配置。固定口令需要管理员手动配置，详细配置请参见 初始化口令配置 。
   - **初始化为随机口令**：需要提前在用户基本信息页面输入用户邮箱，确定设置邮箱可以接收系统发送的用户随机口令。随机口令详细设置请参见 初始化口令设置 。

设置用户认证方式

最近更新时间：2025-01-16 21:01:22

操作场景

堡垒机系统具备为每个用户单独配置登录认证方式功能，下面将为您详细介绍如何设置用户认证方式。

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**用户管理**，进入用户管理页面。
3. 找到您要设置角色的用户账号，在其所在行中，单击 ，即可进入用户信息编辑页面。
4. 单击**设置认证方式**，进入设置用户认证方式页面为用户勾选认证方式，认证方式支持以下几种：
   - **静态口令认证**：静态密码是系统默认设置的登录方式，选择其他三种任意认证方式后，都要与静态口令进行组合认证，如需修改系统默认登录方式可以参考 配置全局认证方式 。
   - **OTP 认证（一次性口令）**：动态口令，使用此方式进行认证，需先 配置 OTP 服务 和为用户 获取账号唯一标识码 。
   - **证书认证**：使用此方式进行认证，需先配置 证书服务 和为用户 获取个人证书 。
   - **AD 域认证**：使用此方式进行认证，需先配置 域服务 。

5. 单击**保存**，即可完成用户认证方式设置。

获取账号唯一身份标识

1. 管理员在设置运维用户使用动态口令认证之后，在用户管理页面，单击 ，进入用户编辑页面。
2. 在用户编辑页面，单击**唯一标识**，获取用户身份标识二维码，将此二维码发送给相关用户。

获取个人证书

进入证书管理页面，单击**生成证书**，生成用户个人证书，如需下载使用证书，请参见 安装证书 文档。

设置用户策略

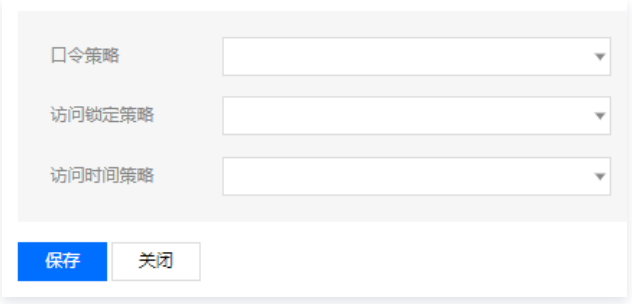
最近更新时间：2025-01-16 21:01:22

操作场景

在管理员需要对运维用户进行一些限制时，如登录系统时间，可以通过为用户设定策略来实现。下面将为您详细介绍如何设置用户策略。

操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 单击**用户管理**，进入用户管理页面。
4. 在用户列表选择需要编辑的用户，单击 ，进入用户信息编辑页面。
5. 单击**设置策略**，进入设置策略页面。
6. 根据需求配置相关策略：
   - **口令策略**：用户口令复杂度策略。具体配置您可以查看 添加口令策略 文档。
   - **访问锁定策略**：用户登录失败锁定策略。当用户访问系统时，输入的错误密码次数超过设定的“访问失败次数”时，用户被锁定。用户被锁定后，如果超过设定的失败锁定时间，解锁被触发，自动解除用户锁定。具体配置您可以查看 添加锁定策略 文档。
   - **访问时间策略**：用户访问系统的时间访问策略。当用户访问系统时，如果用户登录时间在访问时间策略允许登录的时间范围内，可以登录系统；如果用户登录时间在访问时间策略禁止范围内，登录系统失败。具体配置您可以查看 添加时间策略 文档。



7. 在确认配置策略无误后，单击**保存**，即可完成设置用户策略。

唯一标识

最近更新时间：2025-01-17 10:17:43

操作场景

用户唯一标识用于用户手机动态令牌登录认证。

操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 单击**用户管理**，进入用户管理页面。
4. 在用户列表选择需要编辑的用户，单击 ，进入用户信息编辑页面。
5. 在用户编辑页面，单击**唯一标识**，获取用户身份标识二维码。
6. 将此二维码发送给相关运维用户，并使用 Google 动态密码验证器扫描二维码，生成6位数字动态口令，使用手机令牌登录。

证书管理

最近更新时间：2025-01-16 21:01:22

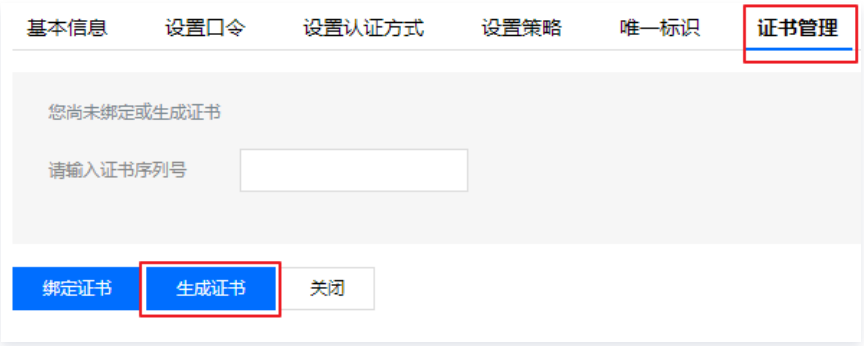
操作场景

用户唯一标识用于证书登录认证。

操作步骤

本地证书生成

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 单击**用户管理**，进入用户管理页面。
4. 在用户列表选择需要编辑的用户，单击，进入用户信息编辑页面。
5. 在用户编辑页面，选择**证书管理** > **生成证书**，即可完成证书生成。



6. 生成证书后，需要运维用户登录堡垒机，进入运维用户页面，在页面右上角，选择**用户名** > **自维护**下载证书，详情可参见 使用证书登录 。
7. （可选）证书生成后，可单击**注销证书**，将证书注销。

国密证书序列号绑定

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 单击**用户管理**，进入用户管理页面。
4. 在用户列表选择需要编辑的用户，单击，进入用户信息编辑页面。
5. 在用户编辑页面，单击**证书管理**，输入国密证书序列号，单击**绑定证书**，即可完成证书绑定。

6. （可选）绑定证书后，可单击**注销证书**，将证书注销。

用户相关操作
注销用户

最近更新时间：2025-01-17 10:17:43

操作场景

在需要停止用户访问登录堡垒机系统时，您可以注销该用户，注销后用户不仅无法登录系统，还将清除之前所有的授权。下面将为您详细介绍如何注销堡垒机的用户。

操作步骤

> **注意**
> 用户注销后，不可再编辑使用。

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 单击**用户管理**，进入用户管理页面。
4. 勾选需要注销的用户，单击**操作**，在下拉菜单中，单击**注销选中用户**。

5. 在弹出的注销用户确认窗口中，单击**详细信息**，可查看所注销用户的 ID 及名称，查看确认完毕后，单击**确定**，即可注销该用户。

锁定用户

最近更新时间：2025-01-16 21:01:22

操作场景

在需要临时限制用户登录堡垒机时，管理员可将该用户进行锁定。下面将为您详细介绍如何锁定堡垒机用户。

操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 单击**用户管理**，进入用户管理页面。
4. 在用户列表，勾选需要锁定的用户，单击**操作**，在下拉菜单中单击锁定选中用户。

5. 在弹出到确认提示框中，单击**详细信息**，可查看所锁定用户的 ID 及名称，查看确认完毕后，单击**确定**，即可锁定用户。

> **说明**
> 堡垒机系统支持自动锁定用户，当用户违反锁定策略的，用户将被自动锁定。具体策略配置您可查看相关 添加锁定策略 文档。

解锁用户

最近更新时间：2025-01-16 21:01:22

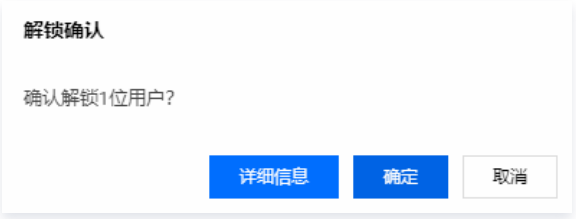
操作场景

堡垒机 用户锁定，可通过管理员修改用户操作进行解锁选中用户.

操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 单击**用户管理**，进入用户管理页面。
4. 在用户列表，勾选需要解锁的用户，单击**操作** ，在下拉菜单中单击**解锁选中用户**。

5. 在弹出到确认提示框中，单击**详细信息**，可查看所解锁用户的 ID 及名称，查看确认完毕后，单击**确定**，即可解锁该用户。



批量修改组织结构

最近更新时间：2025-01-16 21:01:22

操作场景

本文为您详细介绍如何批量修改用户的组织结构。

操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 单击**用户管理**，进入用户管理页面。
4. 在用户列表，勾选需要修改组织结构的用户，单击**操作**，在下拉菜单中单击**修改选中用户组织结构**，进入“选择所属组”页面。

5. 选择需要绑定的组织结构，单击**确定**，即可完成组织结构修改。

为选中用户绑定角色

最近更新时间：2025-01-16 21:01:22

操作场景

本文为您详细介绍如何为选中用户绑定角色，使用户具有相应角色的权限。

前提条件

在为用户绑定角色前，需已在角色管理中 添加角色 。

操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 单击**用户管理**，进入用户管理页面。
4. 在用户列表，勾选需要绑定管理角色的用户，单击**操作**，在下拉菜单中单击**为选中用户绑定管理角色**，进入批量授权角色页面。

5. 选择需要授权用户的一个或者多个角色，单击**保存&关闭**，即可完成用户绑定角色。用户角色相关配置，可参见 角色管理 。

为选中用户绑定授权

最近更新时间：2025-01-16 21:01:22

操作场景

在用户管理中，为用户绑定工作组后，即可在相应工作组中为该用户绑定授权，本文将为您详细介绍，如何在堡垒机中为选中用户绑定工作组。

前提条件

为选中用户绑定工作组前，需已在堡垒机中 新增工作组 。

操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 单击**用户管理**，进入用户管理页面。
4. 在用户列表，勾选需要绑定管理角色的用户，单击**操作**，在下拉菜单中单击**为选中用户绑定工作组**，进入批量管理授权页面。

5. 选择需要授权用户的一个或多个授权，单击**保存&关闭**，即可完成用户授权。

导入用户

最近更新时间：2025-01-16 21:01:22

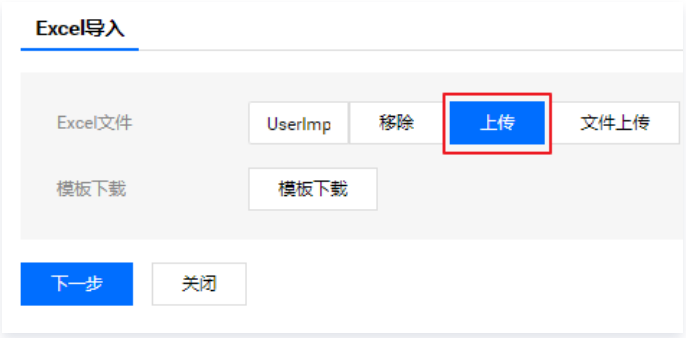
操作场景

在您需要添加大量用户到堡垒机系统时，可以通过导入功能来进行快速添加。下面将为您详细介绍如何导入用户。

操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 单击**用户管理**，进入管理页面。
4. 在用户列表页，单击**菜单**，在下拉菜单中单击**用户导入**，进入用户导入页面。
5. 单击**模板下载**，下载导入用户模板，按照模板添加需要导入的用户，单击**选择**，选择已添加好用户的模板文件。

6. 单击**上传**，用户文件上传完毕之后，单击**下一步**，确认用户模板映射项。



7. 确认无误之后，单击**导入数据**，即可将用户导入到堡垒机系统中。

导出用户

最近更新时间：2025-01-16 21:01:22

操作场景

当您需要修改大量用户信息时，可先将用户信息作为 Excel 文件导出，在文件中直接修改用户信息，而后将该文件导入堡垒机，减轻您修改工作量。下面将为您详细介绍如何导出用户文件。

操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 单击**用户管理**，进入用户管理页面。
4. 在用户列表，单击**菜单**，在下拉菜单中单击**用户导出**，按照提示即可导出组织结构下的用户。

添加用户类型

最近更新时间：2025-01-16 21:01:22

操作场景

该指南指导您如何添加用户类型。

操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 选择**用户管理** > **用户类型管理**，进入用户类型添加页面。
4. 单击**新建**，在新建用户类型弹窗中，填写类型名称。

5. 信息填写完成后，单击**保存**，即可添加此用户类型。

查询用户

最近更新时间：2025-01-16 21:01:22

操作场景

在您需要查询某个用户的具体信息时，可以通过用户查询功能进行查找。下面将为您详细介绍如何查询用户。

操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 单击**用户管理**，进入用户管理页面。
4. 单击**搜索**，设定查询条件，条件说明如下。

   - **用户 ID**：输入您要查询的用户 ID。
   - **用户名称**：输入您要查询用户名称。
   - **用户状态**：账号状态，根据实际环境进行选择。
   - **用户类型**：用户类型，根据实际环境进行选择。
   - **子树查询**：勾选此项，则可以查询组织结构下子组是否存在与输入查询条件匹配的用户。
5. 在设定查询条件后，单击 即可开始查询，并在该页面呈现查找到的记录。

用户角色授权

最近更新时间：2025-01-16 21:01:22

操作场景

该指南指导您在登录堡垒机系统后，通过为用户设定角色，授予用户相关权限。

前提条件

堡垒机需已添加组织结构和角色，具体操作您可查看 添加组织结构 和 设置组织角色 文档。

操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 单击**用户管理**，进入用户管理页面。
4. 找到您要设置角色的用户账号，在其所在行中，右侧工作组栏，单击 ，进入工作组授权页面。
5. 单击**绑定**，可以选择已添加到组织结构下的工作组。相关角色配置可参见 角色管理 文档。
6. 单击**确定**，即可为该用户设置工作组权限。

用户授权

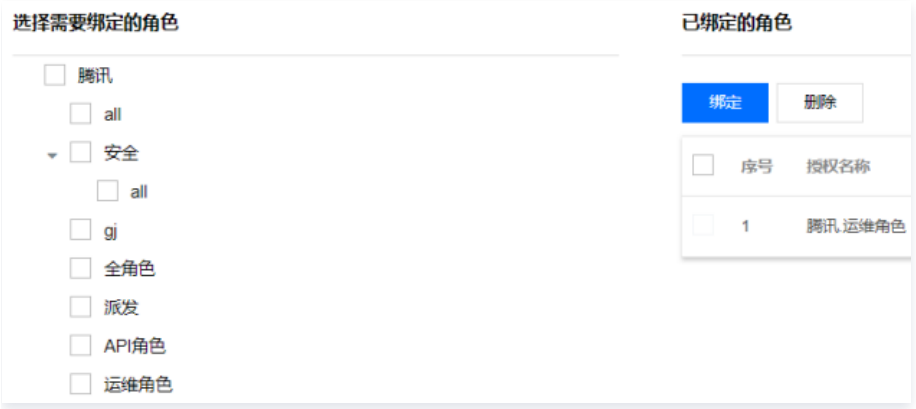
最近更新时间：2025-01-16 21:01:22

操作场景

本文为您详细介绍如何为用户授权。

操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 单击**用户管理**，进入用户管理页面。
4. 找到需要授权的用户，单击，进入授权页面。
5. 单击**绑定**，可以选择已添加到组织结构下的授权。相关授权配置可参见 工作组 。
6. 单击**确定**，即可完成用户授权。



资源管理
添加资源

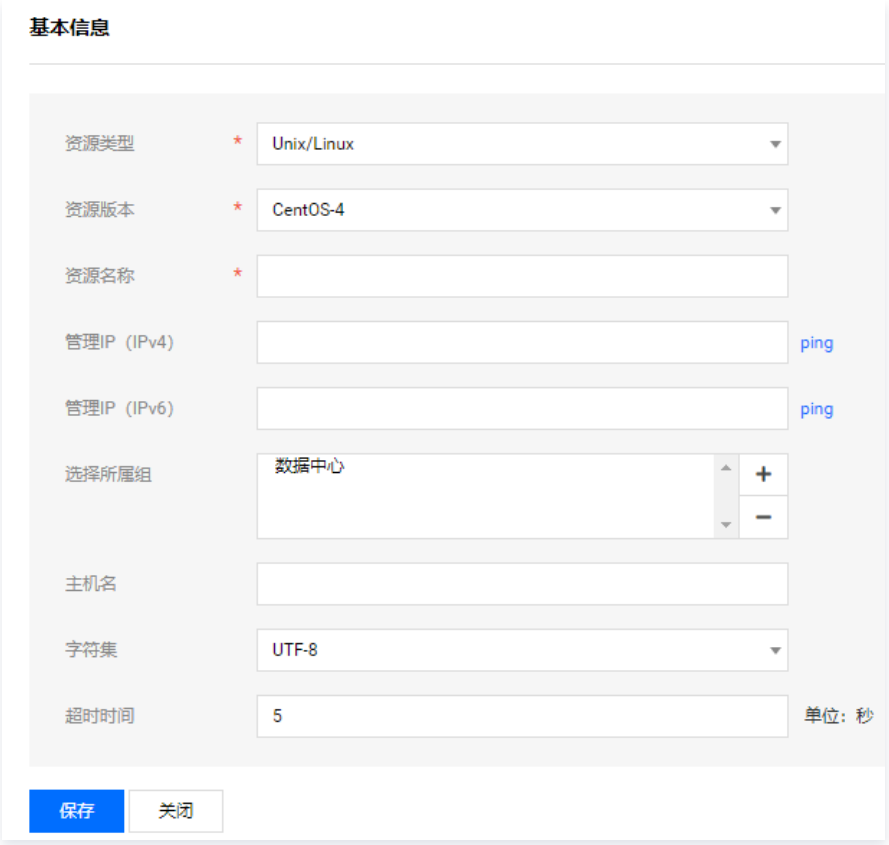
最近更新时间：2024-09-18 18:11:52

操作场景

在根节点、组织类型为“综合组”或“资源组”的组织结构下，都可以对资源进行管理和维护。堡垒机支持主流的大部分资源类型，例如 Unix/Linux、Windows 等其他资源类型。下面将为您详细介绍如何添加 Linux 资源。

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. 单击**新建**，进入资源添加页面，配置相关资源信息。
   - **资源类型**：选择 Unix/Linux。
   - **资源版本**：根据实际资源版本选择，此次我们选择 Centos-4。
   - **资源名称**：填写资源名称。
   - **管理IP（IPv4）**：填写资源 IPv4 地址。
   - **管理IP（IPv6）**：填写资源 IPv6 地址。
   - **选择所属组**：配置资源隶属于某个组织结构。组织结构相关操作您可查看 添加组织结构 文档。
   - **主机名**：填写资源的主机名称。
   - **字符集**：选择 Linux 系统的字符集。
   - **超时时间**：资源抽取等待时间。



> **说明**
> 页面标 * 的配置项为必填项，一个资源可以选择多个所属组，超时时间为抽取等待时间，相关输入规则查看页面相应提示。

4. **单击保存**，即可添加 Linux 资源。

删除资源

最近更新时间：2024-09-18 18:11:52

版权所有：腾讯云计算（北京）有限责任公司

操作场景

在资源下线或已不再进行维护时，建议您在堡垒机系统删除该资源。下面将为您详细介绍如何删除资源。

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. 勾选您需要删除的资源，单击**删除**。

4. 在弹出是确认提示框中，单击**确定**，即可删除资源。

编辑资源

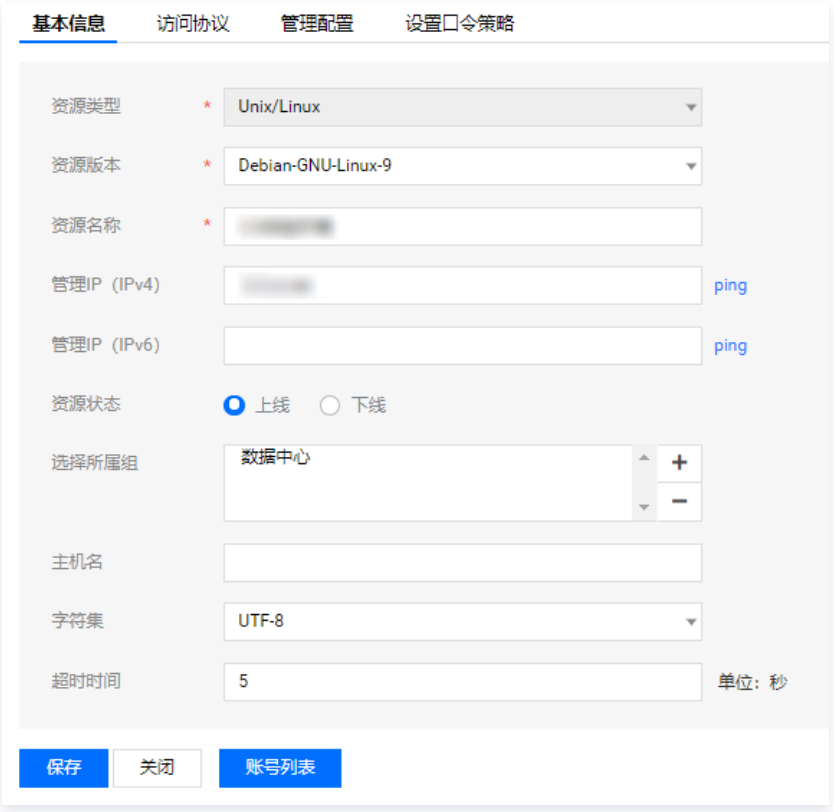
最近更新时间：2024-09-18 18:11:52

操作场景

堡垒机支持修改已添加的资源信息，下面为您详细介绍如何修改资源信息。

基本信息编辑

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. 在资源管理页面，单击资源列表的，进入资源编辑页面，默认进入基本信息页面。
4. 在此页面可以修改资源版本、资源名称、管理IP、资源状态、所属组等资源相关信息。



5. 修改完毕，单击**保存**即可更新资源信息。

访问协议编辑

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. 在资源管理页面，单击资源列表的，进入资源编辑页面。

4. 单击**访问协议**，进入资源访问协议页面。在此页面可以选择资源开放的协议，以及协议对应的端口号。

5. 修改完毕，单击【保存】即可更新信息。

管理配置

管理配置用于设置资源的管理员账号，口令，以及连接协议，用于抽取资源账号及口令。

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. 在资源管理页面，单击资源列表的 ，进入资源编辑页面。
4. 单击**管理配置**，进入管理配置页面。如下图所示，输入资源的账号，资源密码，选择连接资源协议，超时时间。如果勾选“提权设置”可以设置提权账号，提权命令，提权口令提示符，提权口令。

> **说明**
> - 提权账号：输入提权账号，可以提权指定资源账号。
> - 提权口令：是对应的所提权账的口令。
> - 提权命令：提权指定账号所使用的命令（Linux 一般都是 su，思科的是 enable）。
> - 提权口令提示符：输入相应提权命令后，资源系统提示符。

5. 管理配置信息配置完成后，单击**保存并获取账号**，即可进行资源口令抽取。

设置口令策略

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. 在资源管理页面，单击资源列表的 ，进入资源编辑页面。
4. 单击**设置口令策略**，进入设置口令策略，可以选择系统已添加的口令策略，详情可参见 添加口令策略 。

5. 单击**保存**完成配置。

查询资源

最近更新时间：2024-09-18 18:11:52

操作场景

在堡垒机系统上您需要快速定位资源时，您可以通过资源查询功能，快速定位资源。该指南指导您如何查询资源。

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. 单击**搜索**，可以根据资源名称、资源IP、资源从IP、资源类型、资源状态、进行查询。
4. 若勾选**子树查询**，可以查看到查询包括所在组织结构下子组是否存在与输入查询条件匹配的资源。

资源账号列表
添加账号

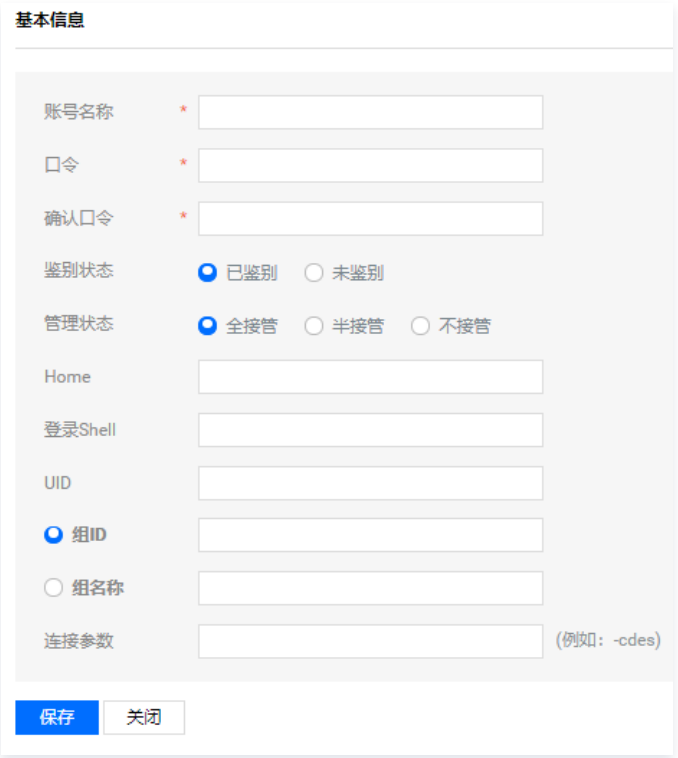
最近更新时间：2025-01-16 21:01:22

操作场景

该指南指导您如何为资源添加账号。

操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 单击**资源管理**，进入资源管理页面。
4. 找到您要配置管理员账号的资源，在其所在行中，在账号列表栏，单击，进入资源账号配置页面。
5. 单击**新建**，配置如下账号信息：
   - **账号名称**：填写资源账号名称。
   - **口令**：填写管理员密码。
   - **确认口令**：填写管理员密码。
   - **鉴别状态**：账号的鉴别状态与授权密切相关。“已鉴别”那么该账号则可以在绑定账号时被查出。“未鉴别”那么授权中要自动清理掉该账号授权，授权不能查询到该账号。
   - **管理状态**：账号的接管状态和账号的修改口令访方式密切相关，如果“全接管”，那么该账号则会被自动加入到修改口令计划中，系统会根据修改计划自动修改该账号口令。“半接管”是该账号的口令修改方式只限于手动修改，系统将不自动为其修改口令。“不接管”系统将会不再维护该账号的口令修改工作。



6. 单击**保存**，即可完成资源账号的添加。

编辑账号

最近更新时间：2025-01-16 21:01:22

操作场景

资源上的账号变动时，堡垒机系统上添加的资源账号也需要进行更新。下面将为您详细介绍如何在堡垒机上编辑资源账号。

操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 单击**资源管理**，进入资源管理页面。
4. 找到您要配置管理员账号的资源，在其所在行中，单击，进入资源账号配置页面。
5. 在资源账号列表，找到您需要编辑的账号，单击，进入账号编辑页面。

6. 编辑完账号信息，单击**保存**即可更新账号信息。

删除账号

最近更新时间：2025-01-16 21:01:22

操作场景

该指南指导您在堡垒机系统上如何删除资源账号。

操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 单击**资源管理**，进入资源管理页面。
4. 找到您要配置管理员账号的资源，在其所在行中，单击，进入资源账号配置页面。
5. 勾选您需要删除的账号，单击**删除**，在弹出窗中，确认删除，即可将该资源账号删除。

版权所有：腾讯云计算（北京）有限责任公司

查询账号

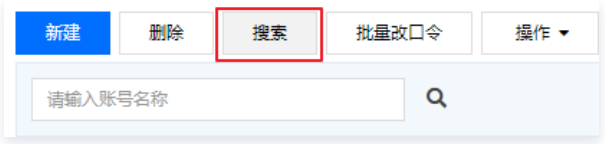
最近更新时间：2025-01-16 21:01:22

操作场景

堡垒机支持查询资源账号，通过查询功能可以快速定位资源账号。下面将为您详细介绍如何查询资源账号。

操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 单击**资源管理**，进入资源管理页面。
4. 找到您要配置查询账号的资源，在其所在行中，单击，进入资源账号配置页面。
5. 单击**搜索**，输入账号名称进行查询。



批量修改口令

最近更新时间：2025-01-16 21:01:22

操作场景

本文为您详细介绍批量修改资源账号的口令。

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. 找到您要批量修改账号口令的资源，在其所在行中，单击，进入资源账号配置页面。
4. 勾选需要修改口令的账号，单击**批量修改口令**，即可批量对账号口令进行修改。

说明

- 管理状态为半接管或不接管，不可修改口令。
- 修改账号口令默认使用资源本身的密码策略进行修改，若资源尚未配置密码策略，则按照默认策略修改资源账号口令。

批量修改鉴别状态

最近更新时间：2025-01-16 21:01:22

操作场景

堡垒机支持批量修改资源鉴别状态，下面将为您详细介绍如何批量修改资源鉴别状态。

操作步骤

> **注意**
> 账号的鉴别状态和岗位授权密切相关。
> - 如果账号的鉴别状态设置为 "已鉴别"，那么该账号则可以在绑定账号时被查出。
> - 如果账号的鉴别状态设置为 "未鉴别"，那么授权时会自动清理掉该账号授权，授权不能查询到该账号。

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 单击**资源管理**，进入资源管理页面。
4. 找到您要配置管理员账号的资源，在其所在行中，单击，进入资源账号配置页面。
5. 勾选您需要修改鉴别状态的账号，单击**操作**，在下拉菜单中单击**批量修改鉴别状态**，即可将资源账号鉴别状态修改成“已鉴别”或“未鉴别”。

批量修改接管状态

最近更新时间：2025-01-16 21:01:22

操作场景

堡垒机支持批量修改资源接管状态，下面将为您详细介绍如何批量修改资源接管状态。

操作步骤

通过堡垒机系统批量修改账号鉴别状态，支持修改 Linux 和 Windows 账号，其修改操作步骤类似，此处以修改 Linux 账号接管状态为例演示操作步骤。

> **注意**
> 账号的接管状态和账号的改口令方式密切相关。
> - 账号接管状态为 "全接管"，那么该账号则会被自动加入到修改口令计划中，系统会根据修改计划自动修改该账号口令。
> - 账号接管状态为 "半接管"，那么该账号的口令修改方式只限于手动修改，系统将不自动为其修改口令。
> - 账号接管状态为 "不接管"，系统将不再维护该账号的口令修改工作。

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 单击**资源管理**，进入资源管理页面。
4. 找到您要配置管理员账号的资源，在其所在行中，单击，进入资源账号配置页面。
5. 勾选您需要修改接管状态的账号，单击**操作**，在下拉菜单中单击**批量修改接管状态**，即可将资源账号接管状态修改成“全接管”或“半接管”或“不接管”。

批量删除被接管资源账号

最近更新时间：2025-01-16 21:01:22

操作场景

本文为您详细介绍如何批量删除被接管资源账号。

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. 找到您要批量删除被接管账号的资源，在其所在行中，单击，进入资源账号配置页面。
4. 勾选您需要批量修改的账号，单击**操作**，在下拉菜单中单击**批量删除被接管资源账号**。

5. 在弹出的确认提示框中，单击**确定**，即可批量删除资源账号。

查看口令修改日志

最近更新时间：2025-01-16 21:01:22

操作场景

该指南指导您在堡垒机系统上查看资源账号口令修改日志。

操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 单击**资源管理**，进入资源管理页面。
4. 找到您要查看账号口令修改日志的资源，在其所在行中，单击，进入资源账号配置页面。
5. 单击，即可查看目标资源账号口令修改历史记录。

账号拨测

最近更新时间：2025-01-16 21:01:22

该文档将指导您在堡垒机系统上，测试添加的资源管理账号密码是否正确，是否可以正常登录。

操作场景

添加资源管理账号 后，可通过拨测功能测试该资源管理账号密码是否正确，是否可以正常登录。

操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 单击**资源管理**，进入资源管理页面。
4. 找到您需要测试账号的资源，在“账号列表”列，单击，进入资源账号配置页面。
5. 在目标账号的“账号拨测”列，单击即可对该账号进行测试。

资源类型配置

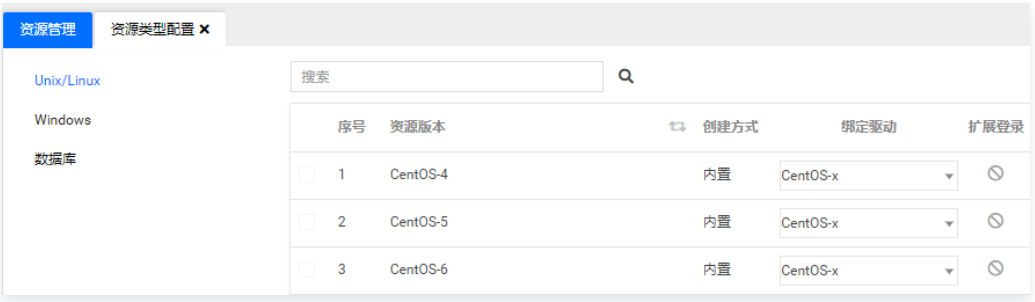
最近更新时间：2025-01-16 21:01:22

操作场景

堡垒机资源管理支持根据不同的资源版本，绑定对应的驱动程序。本文为您详细介绍如何进行配置资源类型。

操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 单击**资源类型配置**，进入资源类型配置页面。
4. 在此您可以进行资源类型配置，为资源版本绑定对应的驱动程序。



资源相关操作
批量修改协议端口

最近更新时间：2025-01-16 21:01:22

操作场景

本文为您详细介绍如何批量修改协议端口。

操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 单击**资源管理**，进入资源管理页面。
4. 勾选需要修改协议端口的资源，单击**操作**，在下拉菜单中单击**修改选中资源协议端口**，进入批量修改协议端口页面。

5. 根据实际需求，选择协议，修改对应的端口号。
6. 单击**保存**即可完成批量修改协议端口。

导出资源

最近更新时间：2025-01-16 21:01:22

操作场景

堡垒机支持将已添加的资源导出为 Excel 文件，您可在导出的文件添加编辑资源，再通过导入功能导入堡垒机，可节省配置资源时间。该指南指导您如何导出资源。

操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 单击**资源管理**，进入资源管理页面。
4. 勾选需要导出的资源，单击**操作**，在下拉菜单中单击**资源导出**，可以将所在组织结构下的资源全部导出。

导入资源

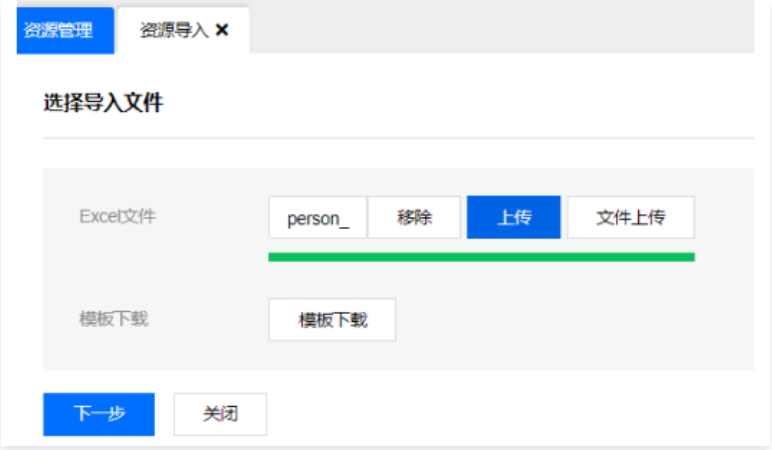
最近更新时间：2025-01-14 18:12:02

操作场景

您需要一次性添加大量资源至堡垒机时，可以使用堡垒机的导入功能，达到快速添加资源目的。下面将为您详细介绍如何导入资源至堡垒机。

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. 单击**操作**，在下拉菜单中单击**资源导入**，进入导入资源页面。
4. 单击**模板下载**，下载导入资源模板。之后按照模板相关提示，填写需要导入的资源。
5. 模板填写完成后，单击**选择**，选择模板文件，单击**上传**，上传资源模板文件。



6. 上传完毕，单击**下一步**，进入映射文件页面。
7. 确认模板文件映射无误后，单击**导入数据**，即可完成资源导入。

批量资源下线

最近更新时间：2025-01-16 21:01:22

操作场景

当您不需要组织结构下的某些资源时，可以使用批量下线功能，将所在组织结构下的资源进行批量下线。

操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 在右侧操作栏，单击**管理**，进入堡垒机登录页面。
4. 使用管理员账号登录堡垒机。

> **说明：**
> 若忘记管理员账号密码，可以 提交工单 联系我们进行解决。

5. 在左侧导航中，选择需要操作的综合组或资源组，在堡垒机页面上方导航中，单击**资源管理**，进入资源管理页面。
6. 在资源管理列表选择需要下线的资源，然后选择**操作 > 下线选中资源**，即可将资源批量下线。

批量修改组织结构

最近更新时间：2025-01-16 21:01:22

操作场景

当您需将某组织结构下的某些资源，移动至其他组织时，可以使用批量修改组织结构功能。

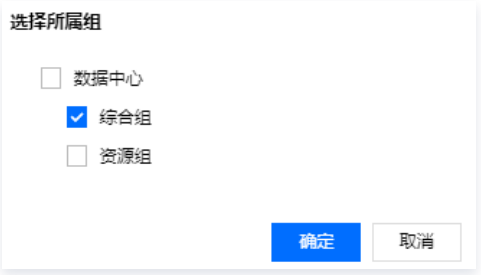
操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。

> **说明：**
> 若忘记管理员账号密码，可以 提交工单 联系我们进行解决。

3. 在左侧导航中，选择需要操作的综合组或资源组，在堡垒机页面上方导航中，单击**资源管理**，进入资源管理页面。
4. 在资源管理列表选择调整组织结构的资源，然后选择**操作** > **修改选中用户组织结构**，弹出“选择所属组”弹窗。

5. 在“选择所属组”弹窗中，选择需要移动至的组织结构名称，单击**确定**即可。



版权所有：腾讯云计算（北京）有限责任公司

资源同步

最近更新时间：2025-01-16 21:01:22

本文介绍了如何在堡垒机中，同步添加同账号下的 CVM 资源。

操作场景

若您需要在堡垒机中同步添加同账号下的 CVM 资源，可以使用数据同步功能。

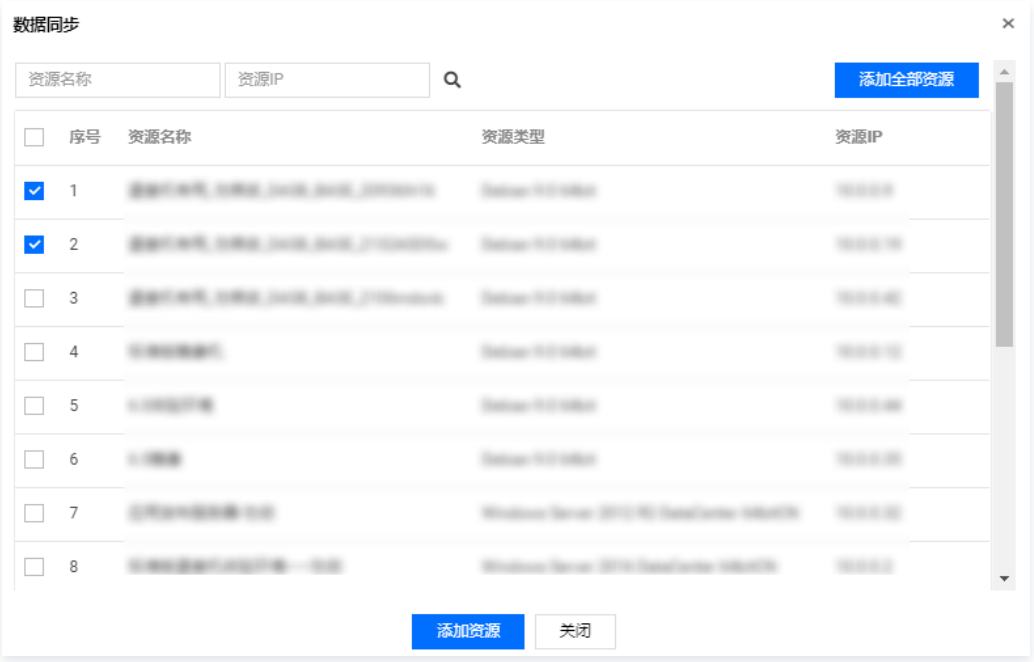
操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。

> **说明：**
> 若忘记管理员账号密码，可以 提交工单 联系我们进行解决。

3. 在左侧导航中，选择综合组或资源组，在堡垒机页面上方导航中，单击**资源管理**，进入资源管理页面。
4. 在资源管理列表，然后单击**数据同步**，弹出“数据同步”弹窗。

5. 在“数据同步”弹窗中，选择需要同步的资源，单击**添加资源**，即可将选择的 CVM 资源同步至堡垒机，也可单击**添加全部资源**，将全部 CVM 资源同步至堡垒机。



统计视图

最近更新时间：2025-01-16 21:01:22

本文介绍了如何在堡垒机中查看组织结构下资源分布情况及资源总数。

操作场景

若您需要在堡垒机中查看组织结构下资源分布情况及资源总数，可以使用统计视图功能。

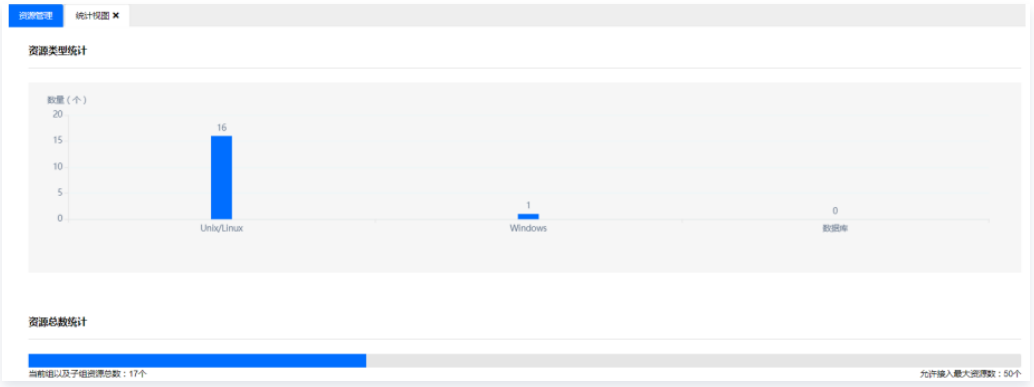
操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。

> **说明**
> 若忘记管理员账号密码，可以 提交工单 联系我们进行解决。

3. 在堡垒机页面上方导航中，单击**资源管理**，进入资源管理页面。
4. 在资源管理列表，然后单击**统计视图**，将进入“资源类型统计”页面。

5. 在“资源类型统计”页面中，可以查看组织结构下资源分布情况及资源总数。



账号导出计划

最近更新时间：2025-01-16 21:01:22

本文介绍了如何在堡垒机中，将资源账号定时导出。

操作场景

若您需要将资源账号定时导出，可以使用账号导出计划功能。

操作步骤

1. 登录腾讯云 堡垒机控制台 ，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。

> **说明**
> 若忘记管理员账号密码，可以 提交工单 联系我们进行解决。

3. 在堡垒机页面上方导航中，单击**资源管理**，进入资源管理页面。
4. 在资源管理列表，然后单击**账号导出计划**，将进入“账号导出计划配置内容”页面。
5. 在“账号导出计划配置内容”页面中，设置执行时间、间隔周期（天）、加密口令，并通过勾选“FTP发送”或“邮件发送”，将账号口令文件发送到指定设备或指定用户邮箱。

6. 若单击**保存**，可将相关配置进行保存。若单击**保存并启动**，可保存相关配置并启动账号导出计划。若单击**初始化**，初始化相关配置，清空之前配置的内容。若单击**关闭**，可关闭账号导出计划页面。若单击**文件列表**，可查看文件列表内容，并可以下载账号及密码文件。

工作组
绑定用户

最近更新时间：2024-09-18 18:11:52

操作场景

在工作组下添加或者新建用户后，用户按照已绑定到工作组下的策略限制，对工作组下绑定的资源进行登录使用。本文为您详细介绍如何在工作组中绑定用户。

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. 单击组织结构类型为“工作组”的组织结构，默认进入绑定用户页面。
3. 单击**绑定**，可以选择已添加到组织结构中的用户，到绑定用户列表。也可以单击**新建并绑定**，跳转到添加用户页面，添加新用户并绑定到用户列表。添加用户的详细操作请参见 添加用户 文档。

绑定资源

最近更新时间：2024-09-18 18:11:52

操作场景

在工作组下添加或者新建用户后，用户按照已绑定到工作组下的策略限制，对工作组下绑定的资源进行登录使用。本文为您详细介绍如何在工作组中绑定资源。

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. 单击组织结构类型为“工作组”的组织结构，选择绑定资源页签，进入资源绑定页面。
3. 单击**添加**，选择已添加到系统的资源，或者是单击**新建并绑定**，新建资源并绑定到此授权组。新建资源的详细操作请参见 添加资源 文档。

版权所有：腾讯云计算（北京）有限责任公司

绑定策略

最近更新时间：2024-09-18 18:11:52

操作场景

在工作组下添加或者新建用户后，用户按照已绑定到工作组下的策略限制，对工作组下绑定的资源进行登录使用。本文为您详细介绍如何在工作组中绑定策略。

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，进入资源策略页面。
3. 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。添加策略的详细操作请参见 策略管理 文档。

4. 绑定完策略，单击**保存**即可。

计划管理
创建任务

最近更新时间：2024-11-08 21:31:52

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，并将账号口令导出文件发送到指定设备或者指定用户邮箱。

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**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：
   - **计划名称（必填）**：建议使用场景命名计划名称。
   - **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，详情请参见 添加口令策略 。
     - 使用资源策略：已绑定到资源上的口令策略，详情请参见 资源编辑 。
   - **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。

编辑任务

最近更新时间：2024-09-18 18:11:52

操作场景

本文为您详细介绍如何编辑计划任务。

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**计划管理**，进入计划管理页面。
3. 在计划任务列表，单击 ，即可对计划任务进行编辑，修改相关任务信息。
4. 编辑完毕，单击**保存**即可完成编辑。

> **注意**
> 计划名称不可以修改，状态为启动或是运行中的任务不允许编辑。

资源账号
添加资源账号

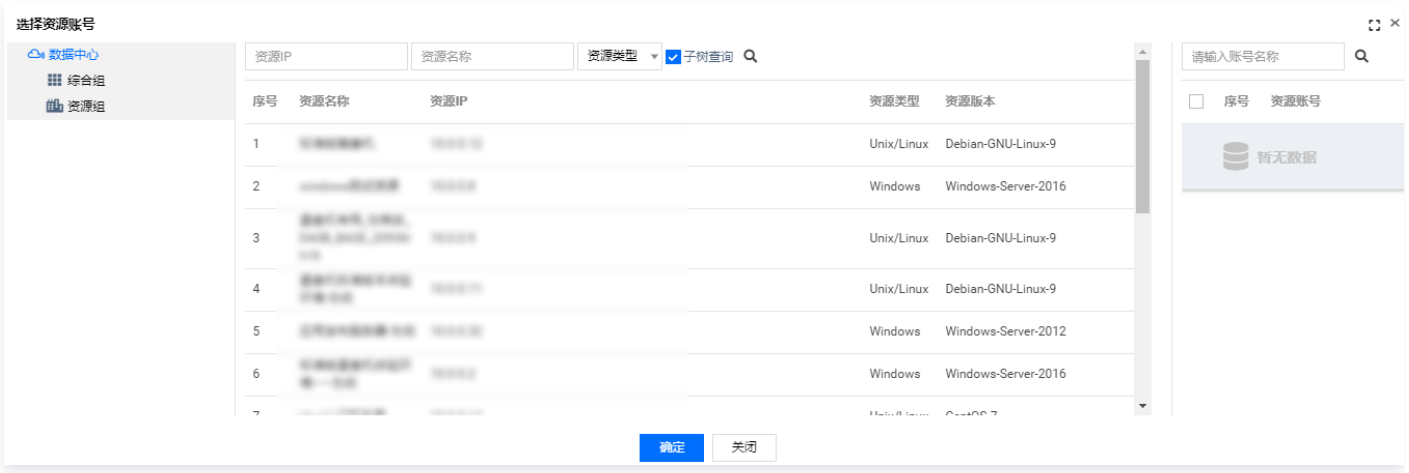
最近更新时间：2024-09-18 18:11:52

操作场景

本文为您详细介绍在计划任务中添加具体的资源账号，以通过计划任务修改资源账号口令。

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**计划管理**，进入任务计划管理页面。
3. 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。
4. 单击**绑定资源账号**，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。



删除资源账号

最近更新时间：2024-09-18 18:11:52

操作场景

本文为您详细介绍在计划任务中删除资源账号，删除后，计划任务将不再修改资源账号的口令。

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**计划管理**，进入任务计划管理页面。
3. 找到需要删除资源账号的计划任务，单击 ，进入资源账号页面。
4. 勾选已添加到列表的资源账号，单击**删除**，即可删除计划任务中的资源账号。删除后，计划任务将不再修改资源账号的口令。

搜索资源账号

最近更新时间：2024-09-18 18:11:52

操作场景

本文为您详细介绍在计划任务中搜索已添加到计划任务中的资源账号。

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**计划管理**，进入任务计划管理页面。
3. 单击，进入资源账号列表页面。
4. 单击**搜索**，可以按照资源名称、资源 IP、资源类型、资源账号查询信息。

删除任务

最近更新时间：2024-09-18 18:11:52

操作场景

该指南指导您如何在堡垒机删除口令变更计划。

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**计划管理**，进入计划管理页面。
3. 在计划任务列表，勾选需要删除的计划任务，单击**删除**，即可删除计划任务。

> **注意**
> 任务状态为“初始化”或者是“停止”的任务才可删除。

查询任务

最近更新时间：2024-09-18 18:11:52

操作场景

该指南指导您在堡垒机上如何查询计划。

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**计划管理**，进入计划管理页面。
3. 根据任务类型、计划名称、任务状态查询计划任务，例如输入计划名称，单击搜索按钮，系统将按照设定的查询条件进行查询，并在该页面呈现查询结果。

任务启动停止

最近更新时间：2024-09-18 18:11:52

操作场景

本文为您详细介绍如何启动和停止计划任务。

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**计划管理**，进入计划管理页面。

启动任务

在计划任务列表，如下图所示，若计划任务“口令变更”为停止状态，单击可以将任务启动。

停止任务

在计划任务列表，如下图所示，若计划任务“口令变更”为启动状态，单击可以将任务停止。

查看操作日志

最近更新时间：2025-01-16 21:01:22

操作场景

若您需要在堡垒机上查看某一计划的变更记录，您可通过操作日志进行查看。下面将为您详细介绍如何在堡垒机查看计划操作日志。

操作步骤

1. 登录腾讯云 堡垒机控制台，单击**查看传统型**。
2. 在堡垒机控制台，可以看到您已购买的堡垒机实例，并使用管理员账号登录堡垒机。
3. 单击**计划管理**，进入计划管理页面。
4. 找到您要查看操作日志的计划，在其所在行中，在操作日志列单击，进入操作日志页面。
5. 在操作日志页面，您可查看该计划的操作记录日志。

查看执行日志

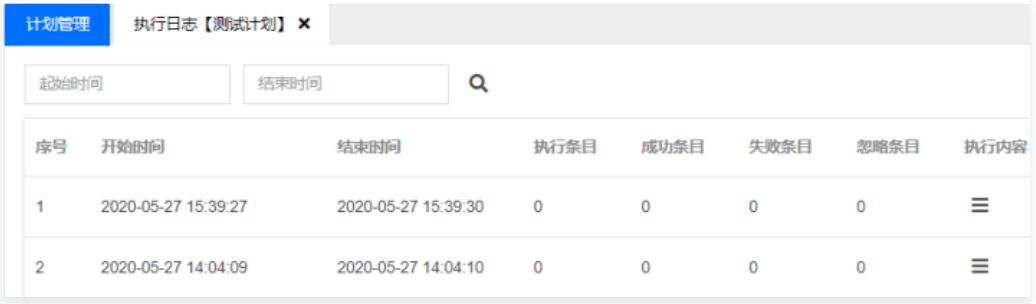
最近更新时间：2024-09-18 18:11:52

操作场景

若您需要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。下面将为您详细介绍在堡垒机上如何查看计划执行的日志。

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**计划管理**，进入计划管理页面。
3. 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。
4. 在执行日志页面，您可查看该计划执行的记录。



角色管理
添加角色

最近更新时间：2024-09-18 18:11:52

操作场景

本文指导您如何在堡垒机添加角色。

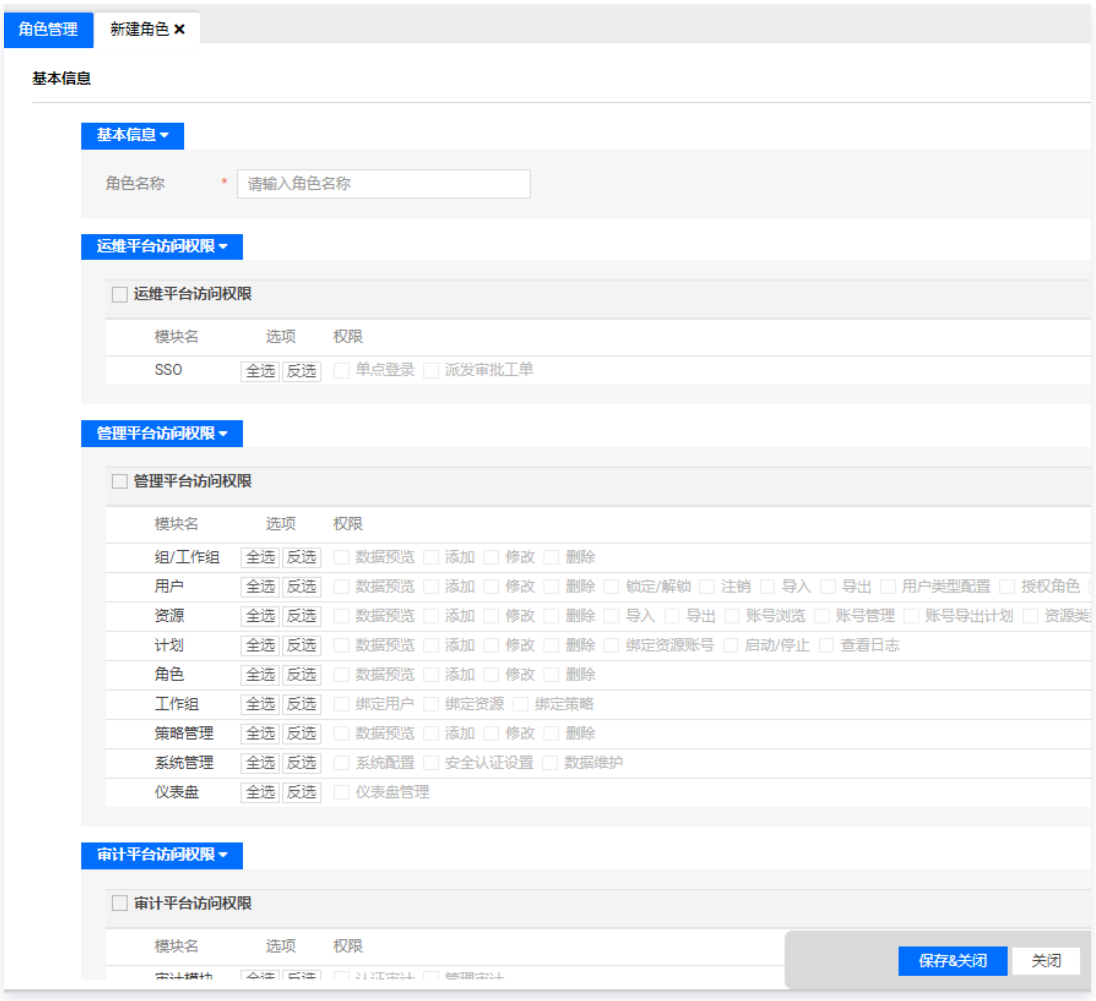
相关说明

运维平台权限：具有运维平台访问权限，单点登录功能。
管理平台访问权限：具有运维平台管理权限，用户、资源、授权、策略、系统等相关权限的管理。
审计平台访问权限：具有报表和审计权限。

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**角色管理**，进入角色管理页面。
3. 单击**新建**，输入角色名称，根据需求勾选相关权限。

> **说明**
> “*”为必填项，单击反选，可反向选择权限。



4. 配置完毕，单击**保存&关闭**即可创建角色。

修改组织角色

最近更新时间：2024-09-18 18:11:52

操作场景

本文指导为您详细介绍如何修改角色信息。

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**角色管理**，进入角色管理页面。
3. 找到您需要修改的角色，在右侧编辑栏，单击 ，进入角色编辑页面，即可根据实际需求修改角色信息。

删除组织角色

最近更新时间：2024-09-18 18:11:52

操作场景

本文为您详细介绍如何删除组织角色。

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**角色管理**，进入角色管理页面。
3. 勾选需要删除的角色，单击**删除**。

4. 在弹出的确认提示窗口中，单击**确定**，即可删除角色。

搜索组织角色

最近更新时间：2024-09-18 18:11:52

操作场景

本文为您详细介绍如何搜索组织角色。

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**角色管理**，进入角色管理页面。
3. 在角色管理页面，单击**搜索**，弹出查询输入框，可以根据名称查询，勾选“子树查询”可以查询组织结构下子组是否有所查询相关角色。

策略管理
普通策略
添加资源账号策略

最近更新时间：2024-09-18 18:11:52

操作场景

资源绑定策略后，单点登录时可以选择关联的账号。本文为您详细介绍如何添加资源账号策略。

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**策略管理**，进入策略管理页面。
3. 选择**普通策略** > **资源账号策略**，进入资源账号策略设置页面。
4. 单击**新建**，可以添加策略，输入信息后，单击**保存**完成策略配置。

> **说明**
> 其中关联密钥为在系统管理的全局密钥配置中，所创建的密钥，若存在多个密钥，可根据需求进行选择，详情请参见 配置全局密钥 。

添加时间策略

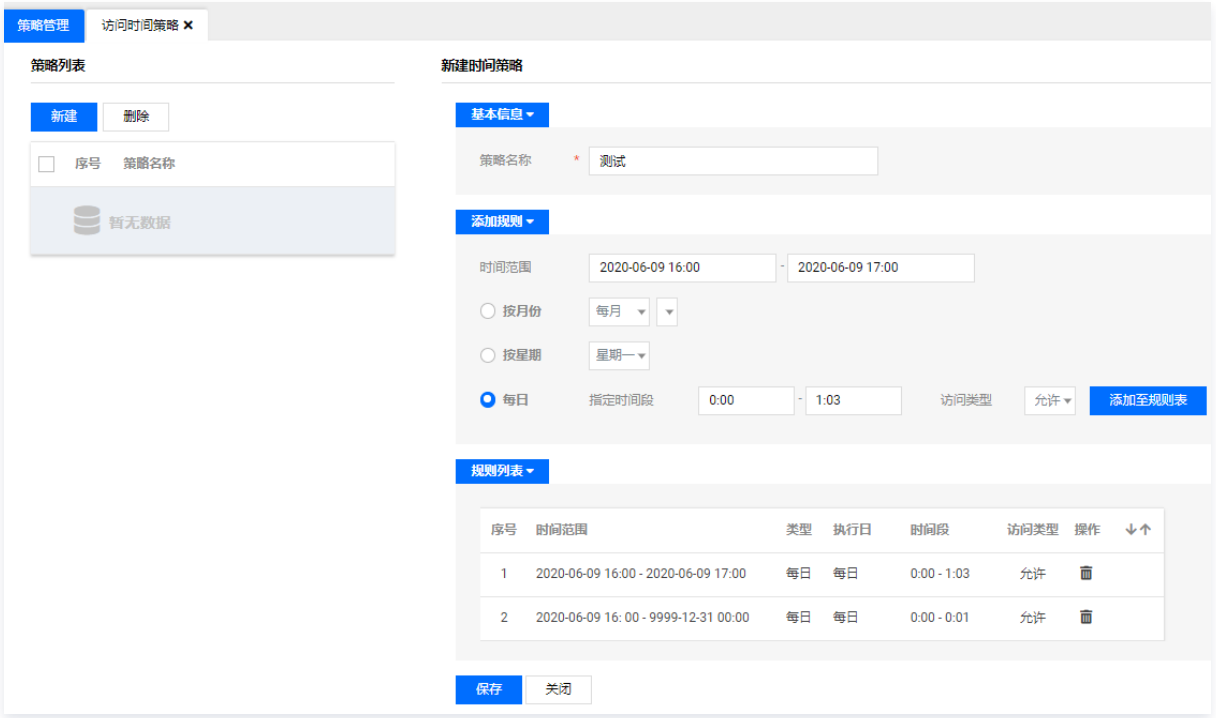
最近更新时间：2024-09-19 15:34:41

操作场景

在需要限制用户登录系统或运维资源的时间时，您可以通过配置时间策略来达到目的。下面将为您详细介绍如何添加时间策略。

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**策略管理**，进入策略管理页面。
3. 选择**普通策略 > 访问时间策略**，进入访问时间策略设置页面。
4. 单击**新建**，开始添加策略。
   - **策略名称（必填）**：填写策略名称。
   - **时间范围**：具体的时间范围。
   - **访问类型**：禁止和允许两种访问类型，选其中一种。



5. 确认配置信息无误后，单击**添加至规则表**，允许添加多条规则。
6. 规则添加完成后，单击**保存**，即可完成时间策略的添加。

> **说明**
> 添加时间策略后，需要开启或关联该策略，敬请参见 设置用户策略 。

添加口令策略

最近更新时间：2024-09-19 15:34:41

操作场景

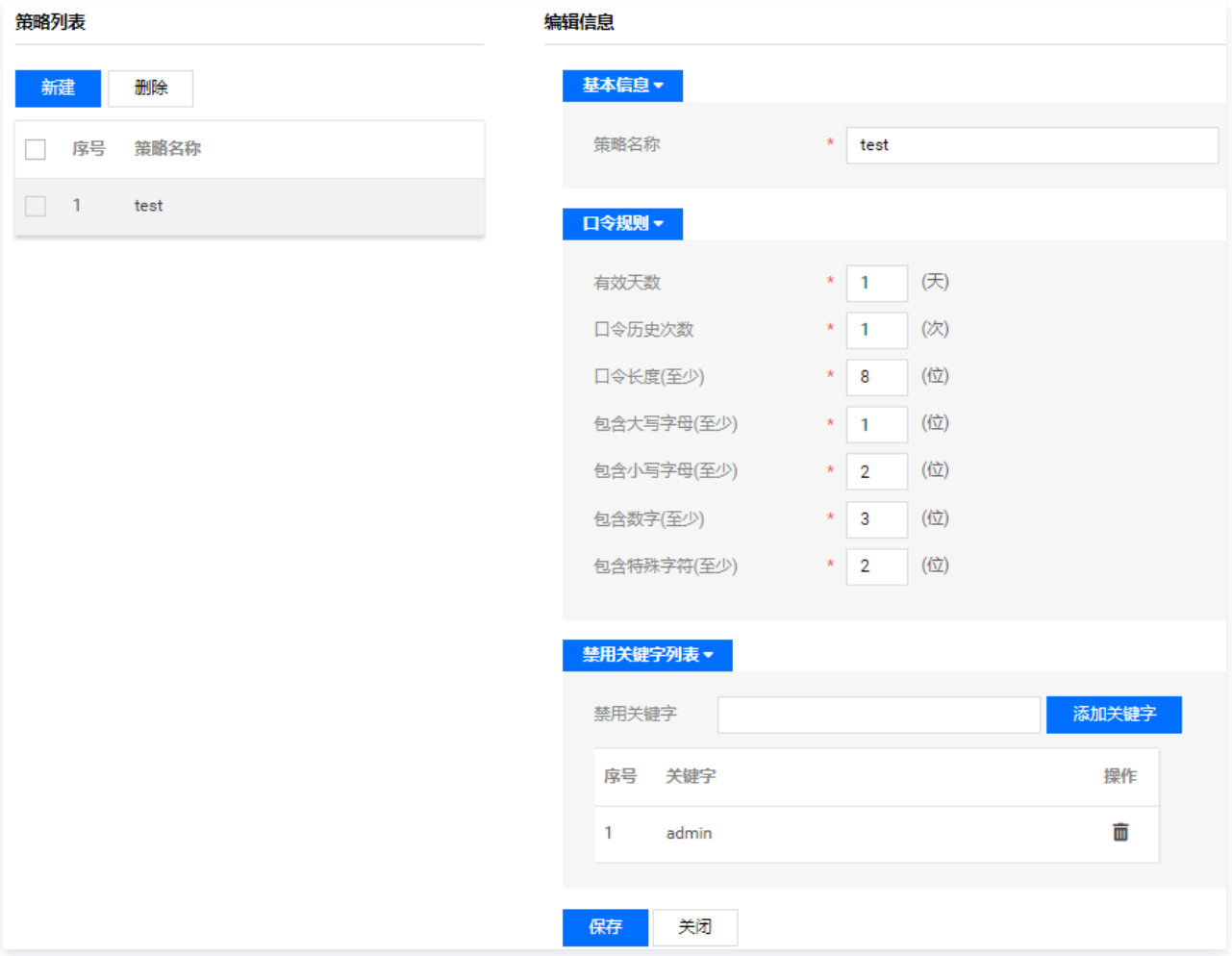
堡垒机具备用户口令策略功能，该策略可强制用户定期更新密码或设置复杂度高的密码。下面将为您详细介绍如何添加口令策略。

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**策略管理**，即可进入策略管理页面。
3. 选择**普通策略 > 口令策略**，进入口令策略设置页面。
4. 单击**新建**，开始添加策略。
   - **策略名称**：填写策略名称。
   - **有效天数**：口令有效时间，在口令有效天数内，系统会强制您更新口令。
   - **口令历史次数**：例如设置为2，则说明修改的口令不得与前两次的口令相同。

   > **说明**
   > 其中口令长度、大小写字母、数字和特殊字符您可根据需求进行配置，且口令长度最少应为包含字母、数字和特殊字符个数的总和。

   - **禁用关键字列表**：您可以设置禁止口令使用某些字符。



5. 确认配置信息无误后，单击**保存**，即可添加口令策略。

添加锁定策略

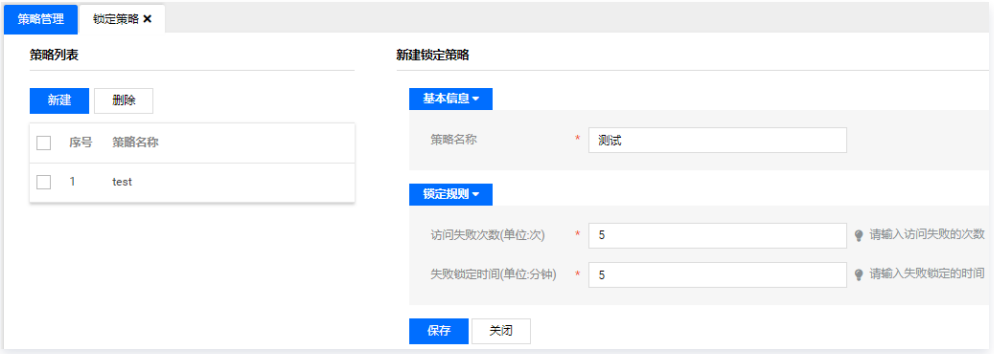
最近更新时间：2025-01-16 21:01:22

操作场景

在需要限制用户登录失败次数时，您可以通过配置锁定策略，对用户失败登录次数和锁定时间进行控制。下面将为您详细介绍如何添加锁定策略。

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**策略管理**，即可进入策略管理页面。
3. 选择**普通策略 > 锁定策略**，进入锁定策略设置页面。
4. 单击**新建**，开始添加策略。
   - **策略名称：**填写策略名称。
   - **访问失败次数（单位：次）：**填写允许用户登录失败的次数。
   - **失败锁定时间（单位：分钟）：**填写用户被系统锁定的时间。



> **注意**
> 该策略应用于除证书认证以外的所有认证失败后的安全措施。

5. 确认配置信息无误后，单击**保存**，即可添加锁定策略。

访问控制策略
添加字符命令策略

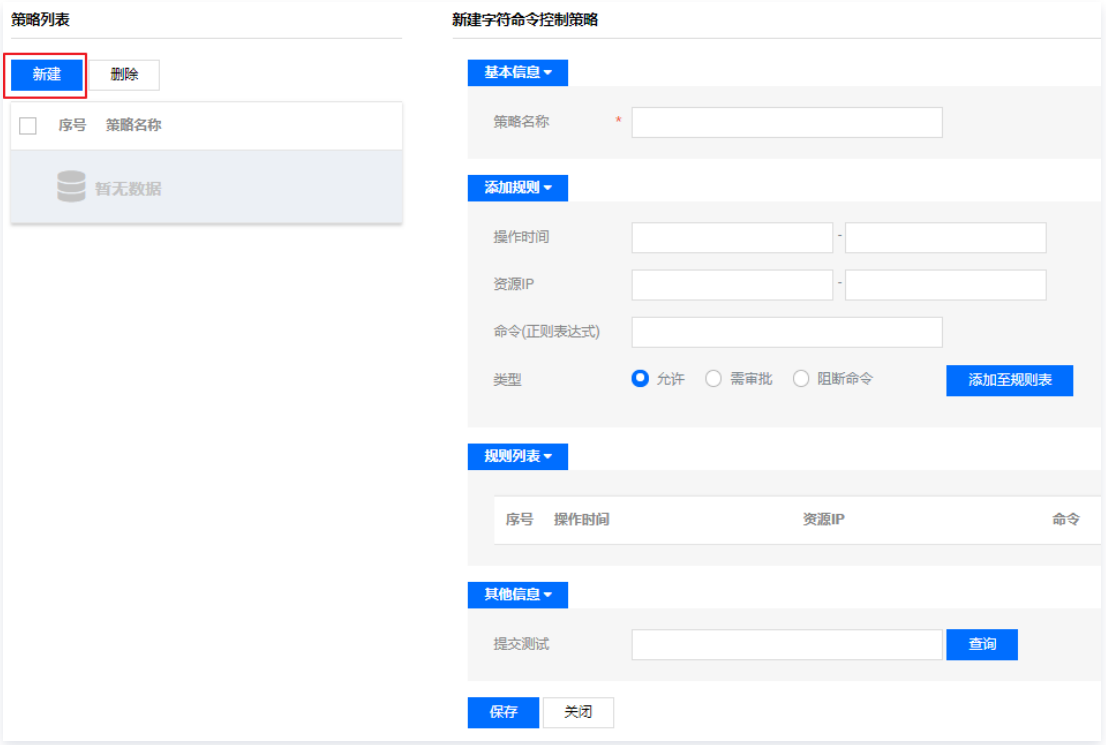
最近更新时间：2024-09-19 15:34:41

操作场景

需要禁止运维用户在操作资源时执行高危命令（例如 reboot、rm）时，可以通过堡垒机系统字符命令策略进行限制。下面将为您详细介绍如何添加字符命令策略。

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**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**：（必填）填写策略名称。
   - **操作时间**：策略生效时间范围。
   - **资源 IP**：策略生效 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、需审批或阻断命令。请根据实际需求配置。



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。

添加 FTP 访问控制策略

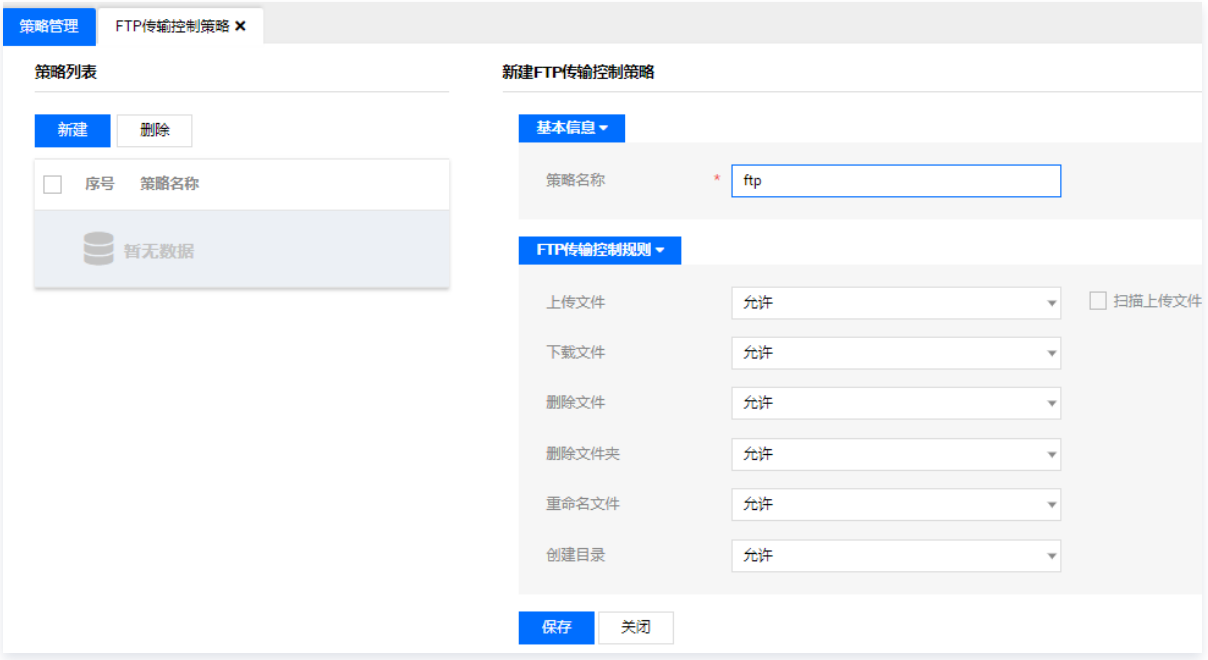
最近更新时间：2024-09-19 15:34:41

操作场景

运维用户使用 FTP 协议登录远程资源时，您可以配置策略限制运维用户的上传、下载和共享本地磁盘等操作，能够防止用户上传恶意程序，或泄露重要文件。下面将为您详细介绍如何添加 FTP 访问控制策略。

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**策略管理**，进入策略管理页面。
3. 选择**控制策略 >FTP 传输控制策略**，进入 FTP 传输控制策略设置页面。
4. 单击**新建**，开始添加策略。
   - **策略名称：**（必填）填写策略名称。
   - **FTP 传输控制规则：**
   - **上传文件：**允许或禁止。勾选**扫描上传文件**还可对文件进行扫描。
   - **下载文件：**允许或禁止。若为允许，则用户可以从资源下载文件至本地。
   - **删除文件：**允许或禁止。若为允许，则用户可以删除资源上的文件。
   - **删除文件夹：**允许或禁止。若为允许，则用户可以删除资源上的文件夹。
   - **重命名文件：**允许或禁止。若为允许，则用户可以重命名资源上的文件。
   - **创建目录：** 允许或禁止。若为允许，则用户可以在资源上创建目录。



5. 确认配置信息无误后，单击**保存**，即可添加 FTP 访问控制策略。

添加图形访问控制策略

最近更新时间：2024-09-19 15:34:41

操作场景

在用户使用图形协议登录时，您可以配置策略限制用户的上传、下载和共享本地磁盘等操作。能够防止用户上传病毒程序，或泄露重要文件。下面将为您详细介绍如何添加图形访问控制台策略。

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**策略管理**，即可进入管理页面。
3. 选择**控制策略** > **图形控制策略**，进入图形控制策略设置页面。
4. 单击**新建**，开始添加策略。
   - **策略名称**：填写策略名称。
   - **上行剪切板**：对上行进行文件剪切控制。
   - **下行剪切板**：对下行进行文件剪切控制。
   - **上行拷贝**：对上行进行文件拷贝控制。
   - **下行拷贝**：对下行进行文件拷贝控制。

5. 确认配置信息无误后，单击**保存**，即可添加图形访问控制台策略。

审计策略
添加字符审计策略

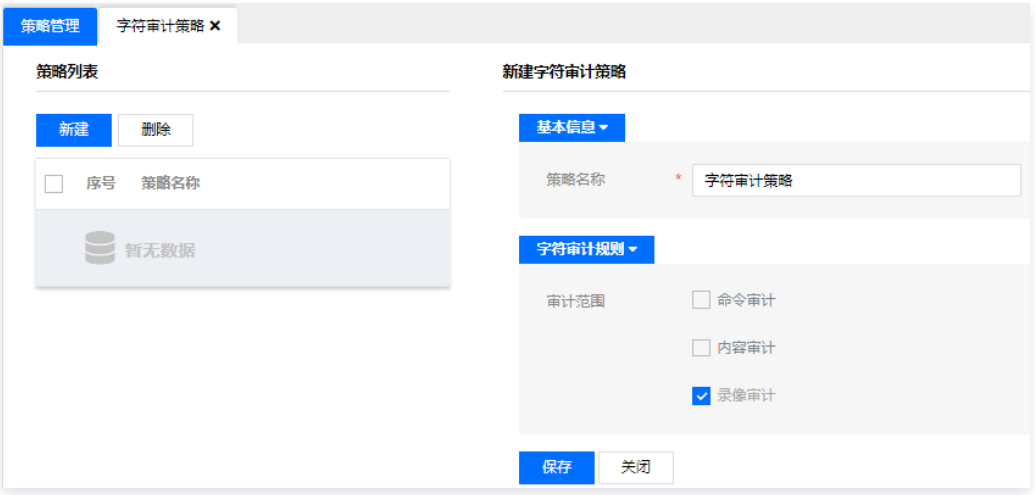
最近更新时间：2025-01-16 21:01:22

操作场景

堡垒机系统行为审计功能支持自定义，可以针对自身情况自定义审计功能。下面将为您详细介绍如何添加字符审计策略。

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. 在左侧导航栏中，单击**安全策略**，即可进入管理页面。
3. 选择**审计策略** > **字符审计策略**，进入字符审计策略设置页面。
4. 单击**新建**，开始添加策略。
   - **策略名称**：填写策略名称。
   - **审计范围**：
     - 命令审计：运维用户在资源操作时执行的命令。
     - 内容审计：运维用户在操作资源过程中的所有字符内容。
     - 录像审计：运维用户操作资源的录像。



5. 确认配置信息无误后，单击**保存**，即可添加字符审计策略。

添加 FTP 审计策略

最近更新时间：2024-09-19 15:34:41

操作场景

该指南指导您如何添加 FTP 行为审计策略。

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**策略管理**，进入策略管理页面。
3. 选择**审计策略 > 文件传输审计策略**，进入文件传输审计策略设置页面。
4. 单击**新建**，开始添加策略。
   - **策略名称**：填写策略名称。
   - **审计范围**：
     - 命令：用户通过 FTP 访问远程资源时，执行的命令。
     - 保留上传文件：开启时，用户通过 FTP 访问远程资源时，上传的文件将会保留一份在堡垒机。
     - 保留下载文件：开启时，用户通过 FTP 访问远程资源时，下载的文件将会保留一份在堡垒机。

5. 确认配置信息无误后，单击**保存**，即可添加 FTP 行为审计策略。

添加图形审计策略

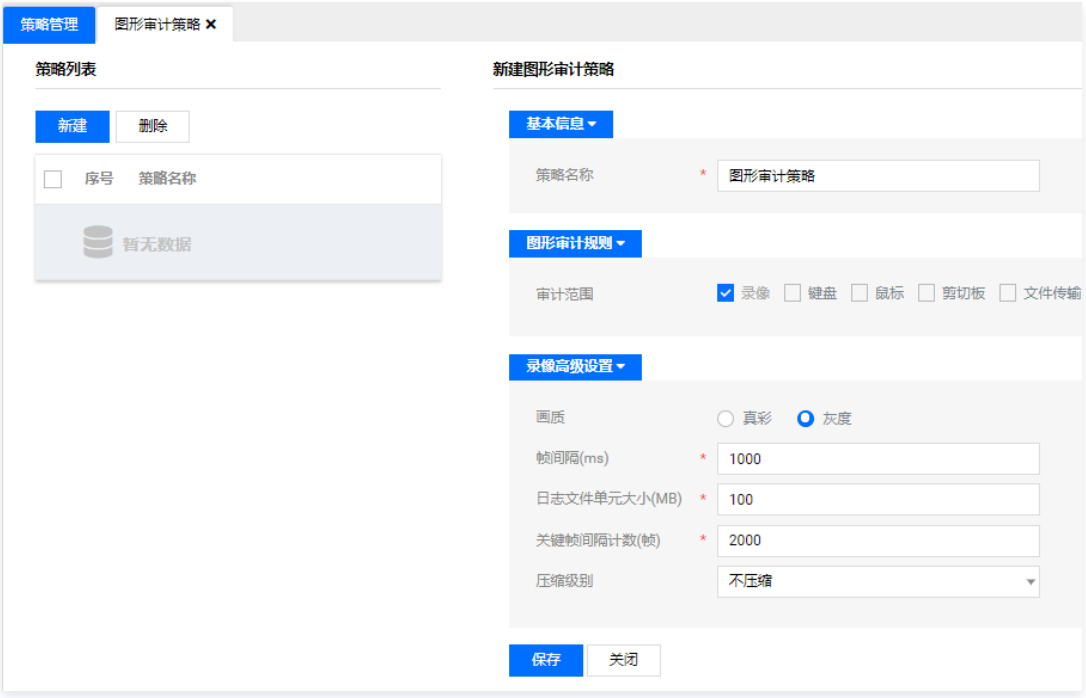
最近更新时间：2024-09-19 15:34:41

操作场景

该指南指导您如何添加图形审计策略。

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**策略管理**，进入策略管理页面。
3. 选择**审计策略 > 图形审计策略**，进入图形审计策略设置页面。
4. 单击**新建**，开始添加策略。
   - **策略名称**：填写策略名称。
   - **审计范围**：审计范围包含录像、键盘、鼠标、剪切板、文件传输。勾选审计范围，则系统审计内容包含该范围。
   - **录像高级设置**：包括画质、帧间隔（ms）、日志文件单元大小（MB）、关键帧间隔计数（帧）、压缩级别。



5. 确认配置信息无误后，单击**保存**，即可添加图形审计策略。

系统管理
系统配置
系统监控

最近更新时间：2024-09-19 15:34:41

操作场景

该指南指导您如何查看堡垒机系统资源使用情况。

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. 在页面右上角，单击**系统管理**，进入系统管理页面。
3. 在系统管理页面的左侧导航中，选择**系统配置** > **系统监控**，进入系统监控页面，可以查看系统授权信息、CPU 使用情况、内存与交互情况、磁盘使用情况、网卡状态等。

版权所有：腾讯云计算（北京）有限责任公司

系统维护

最近更新时间：2024-09-19 15:34:41

操作场景

该指南指导您如何进行堡垒机系统维护（例如重启、关机）。

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. 在页面右上角，单击**系统管理**，进入系统管理页面。
3. 在系统管理页面，选择**系统配置** > **系统维护**，进入系统维护内容页面。
4. 查看服务状态显示为 ，表示运行状态正常。

5. 单击**重启**，可以重新启动堡垒机系统，单击**关机**，将关闭堡垒机系统，单击**磁盘挂载**，可将堡垒机挂载。

服务器配置

最近更新时间：2024-09-19 15:34:41

下面将为您详细介绍如何在堡垒机上进行服务器配置。

操作场景

若您需要在堡垒机上进行配置服务器，可使用服务器配置功能。

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. 在右上角单击**系统管理**，进入系统管理页面。
3. 在系统管理页面，选择**系统配置** > **服务器配置**，进行服务器配置。
4. 系统支持两种部署方式：单机模式、双机模式，选择完成后单击**保存**。

> **说明**
> 如需使用双机模式，可以 提交工单 联系我们进行协助配置。

5. 单击**添加**，可以添加服务器。

6. 在服务器添加页面，填写相关信息，填写完成后，单击保存，即完成添加。

7. 单击**协议代理配置**，可以设置已添加的服务器状态。

配置系统时间

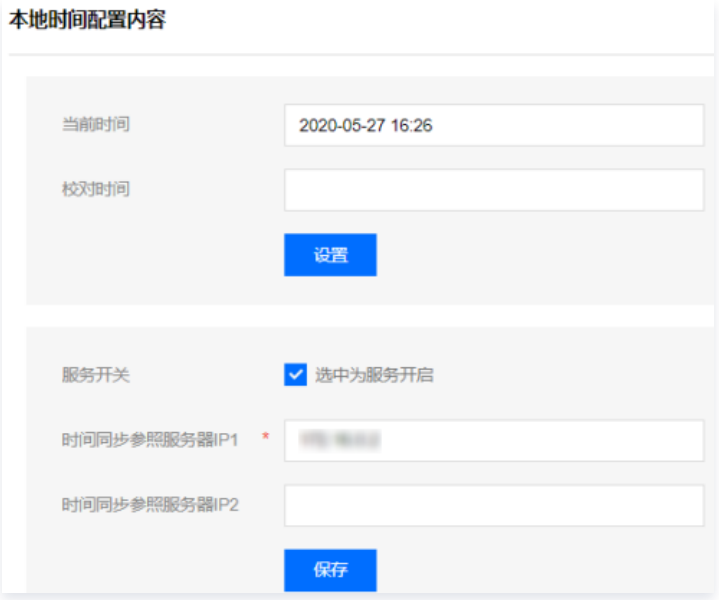
最近更新时间：2024-09-19 15:34:41

操作场景

在需要校对堡垒机系统时间时，您可以通过配置系统时间来进行校对。下面将为您详细介绍如何在堡垒机上配置系统时间。

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. 在右上角单击**系统管理**，进入系统管理页面。
3. 在系统管理页面选择**系统配置** > **本地时间**，进入本地时间配置内容页面。



4. 手动校对时间：如图所示，在校对时间框选择当前时间，单击**设置**即可完成。
5. 开启时间同步服务器：勾选“选中服务开启”，输入是按同步参照服务器 IP，单击**保存**完成配置。

配置邮件服务

最近更新时间：2024-09-19 15:34:41

操作场景

您需要将堡垒机产生的账号口令文件、审计记录等通过邮件接口发送到相关人员时，需先配置邮件服务接口。下面将为您详细介绍如何在堡垒机上配置邮件服务。

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. 在右上角单击**系统管理**，进入系统管理页面。
3. 在系统管理页面，选择**系统配置** > **邮件服务**，输入发送邮件服务器地址、发送用户名、口令等信息，单击**保存**完成配置。
4. 配置如下选项：
   - **发送邮件服务器地址（email）**：例如 `smtp.qq.com` 。
   - **发送方用户名**：邮件账号。
   - **发送口令**：QQ、163、126邮箱需填写邮箱授权码，其他邮箱填写邮箱账号密码。配置授权码，QQ 邮箱请参见 授权码帮助文档 。
   - **确认发送口令**：确认邮件密码。
   - **接收方邮件地址**：填写用来接收测试邮件的邮件地址。

5. 单击**检测**，系统会发送一封测试邮件到接收方邮件地址，若接收方邮件收到测试邮件，则说明邮件服务配置成功，否则配置失败。
6. 在测试成功之后，单击**保存**即可。

端口开放管理

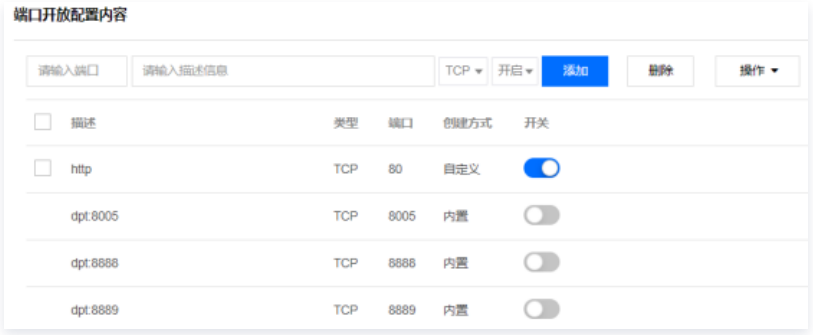
最近更新时间：2024-09-19 15:34:41

本文档将指导您如何添加、开启或关闭堡垒机相关的特殊端口，从而更好地保障堡垒机的安全。

> **说明**
> 堡垒机服务必须使用的端口是默认开放的，无需登录堡垒机处理，若有特殊需求可以在端口管理中进行端口设置，且不会影响堡垒机的正常使用。

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，登录详情可参见 控制台登录 。
2. 在堡垒机系统页面右上角，单击**系统管理**。
3. 在系统管理页面，选择**系统配置** > **端口开放管理**，进入端口开放配置内容页面。
4. 在端口开放配置内容页面，输入端口号、描述信息、选择对应的协议类型及端口开关状态，单击**添加**，可以将设置的端口添加到端口列表。
5. 端口添加完成后，可对已添加的端口进行删除、开启或关闭等操作。
   - 删除：选择需要删除的端口信息，单击**删除**，可以将端口信息删除。
   - 操作：选择需要操作的端口信息，单击**操作**，可以批量开启端口或批量关闭端口。
   - 开关：滑动状态开关，可以将已添加的端口进行开启或关闭操作。



配置 Syslog

最近更新时间：2024-09-19 15:34:41

操作场景

本文为您详细介绍配置堡垒机的 Syslog，将堡垒机运行产生的日志发送到 Syslog 服务器。

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. 在右上角单击**系统管理**，进入系统管理页面。
3. 在系统管理页面，选择**系统配置** > **Syslog**，进入 Syslog 配置页面。
4. 配置如下相关信息：
   - 发送协议：根据实际环境选择 Syslog 协议。
   - IP 地址：Syslog 服务器 IP 地址。
   - IP 端口：Syslog 服务器运行的 Syslog 端口，默认为514。
   - 发送日志类型：勾选需要发送到 Syslog 服务器的日志类型。日志类型有内部审计日志、行为审计日志、行为审计命令日志、登录日志。

5. 配置完毕，单击**保存**，保存配置。
6. 单击**开启**，即可开启 Syslog。

配置消息公告

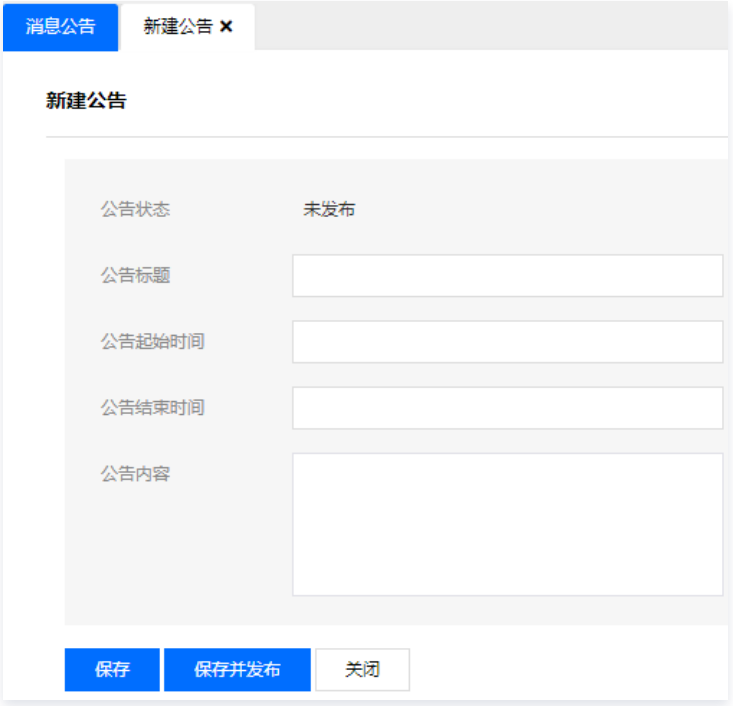
最近更新时间：2024-09-19 15:34:41

操作场景

本文为您详细介绍配置堡垒机消息公告，可将消息下发至运维人员。

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. 在右上角单击**系统管理**，进入系统管理页面。
3. 在系统管理页面，选择**系统配置** > **消息公告**，进入消息公告配置页面。
4. 单击**新建**，在新建公告页面编辑消息公告，配置如下信息：
   - 公告标题：输入公告标题。
   - 公告起始时间：公告的发布时间。
   - 公告结束时间：公告的结束时间。
   - 公告内容：输入具体需要公告的内容。



5. 单击**保存**，可保存公告配置。
6. 单击**保存并发布**。

> **说明**
> 在公告配置的同时将发布公告，到达截止时间后公告将不再显示。

安全认证配置
配置全局认证方式

最近更新时间：2024-09-19 15:34:41

操作场景

本文为您详细介绍如何配置全局认证方式。堡垒机支持设置一种主认证方式，也可以设置两种认证方式组合认证。

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. 在右上角单击**系统管理**，进入系统管理页面。
3. 在系统管理页面，选择**安全设置** > **全局认证方式**，进入全局认证方式设置页面。
4. 选择认证方式后，单击**保存**即可完成配置。

版权所有：腾讯云计算（北京）有限责任公司

配置全局密钥

最近更新时间：2024-09-19 15:34:41

操作场景

当运维人员需要 SSH key 免密登录服务器时，需要由管理员强认证方式登录堡垒机，配置全局密钥，并且通过 资源账号策略 关联账号和密钥。

操作步骤

1. 登录腾讯云 堡垒机控制台 ，选择一台已部署好的堡垒机实例，在右侧操作栏，单击**管理**，进入堡垒机登录页面。
2. 由管理员通过强认证方式登录堡垒机，详情可参见 配置全局认证方式 。

> **说明：**
> OPT 认证、AD/LDAP 认证以及证书认证为强认证方式。

3. 在右上角单击**系统管理**，进入系统管理页面。
4. 在系统管理页面，选择**安全设置** > **全局密钥配置**，进入全局密钥配置页面。
5. 填写密钥后，单击**添加**完成配置。
6. 配置完成后，管理员通过 资源账号策略 关联账号和密钥，即可以通过 SSH key 免密登录服务器。

版权所有：腾讯云计算（北京）有限责任公司

超时设置

最近更新时间：2024-09-19 15:34:41

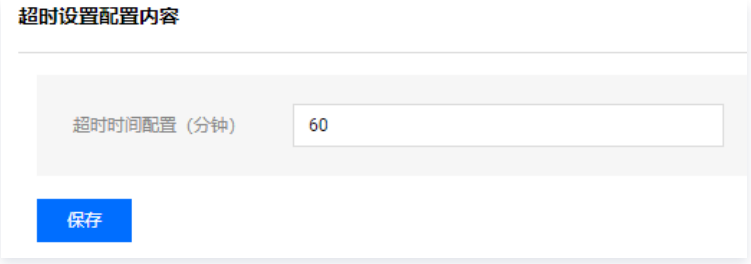
操作场景

如需设置系统在规定时间内自动退出登录，可使用超时设置功能。

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. 在右上角单击**系统管理**，进入系统管理页面。
3. 在系统管理页面，选择**安全设置** > **超时设置**，进入超时设置页面。
4. 在超时设置页面，输入时间后，单击**保存**完成配置，到达所设置的时间后，系统将自动退出登录。

> **注意**
> - 超时时间配置需要重启 Web 服务后才能生效。
> - 时间范围为10分钟 – 1440分钟。



配置 OTP 认证

最近更新时间：2024-09-19 15:34:41

操作场景

堡垒机支持运维用户使用动态口令（OTP）认证进行登录，使用 OTP 认证之前需先配置 OTP 服务，下面将为您详细介绍如何在堡垒机配置 OTP 服务。

操作步骤

堡垒机支持 本地 OTP 服务 和 第三方 OTP 服务 。本地 OTP 服务为堡垒机系统内建 OTP 服务，并提供微信小程序“数盾OTP”用于获取登录口令。第三方 OTP 服务需要额外的 OTP 服务器。

本地 OTP 服务

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. 在右上角单击**系统管理**，进入系统管理页面。
3. 在系统管理页面，选择**安全设置** > **OTP认证配置**，进入 OTP 认证配置页面。
4. 在 OTP 认证配置页面，勾选**本地 OTP 服务**，单击**保存**，即可开启本地 OTP 服务。

第三方 OTP 服务

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. 在右上角单击**系统管理**，进入系统管理页面。
3. 在系统管理页面， 选择**安全设置** > **OTP 认证配置**，进入 OTP 认证配置页面。
4. 在 OTP 认证配置页面，勾选**第三方 OTP 服务**，输入相关第三方OTP服务器地址,认证端口，认证方法等信息。
   - **OTP 服务器主机地址**：填写真实的 OTP 服务器主机地址。
   - **OTP 服务器备机地址**：OTP 备机地址，可不填。
   - **OTP 主机认证端口**：默认的 OTP 端口为1812，请根据实际环境填写。
   - **OTP 备机认证端口**：OTP 备机认证端，请根据实际环境填写。
   - **OTP 认证方法**：请根据实际环境填写。例如 PAP。

- **通信密钥**：OTP 认证密码。请根据实际环境填写。

5. 单击**保存**，即可完成 OTP 服务配置。

配置域认证

最近更新时间：2024-09-19 15:34:41

操作场景

堡垒机系统支持使用 AD 域认证进行登录，使用 AD 域认证之前需配置域服务。下面将为您详细介绍如何在堡垒机上配置域服务。

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. 在右上角单击**系统管理**，进入系统管理页面。
3. 在系统管理页面，选择**安全设置** > **域认证配置**，进入域认证配置页面。
4. 请根据实际环境填写您的域服务信息，相关配置说明如下：
   - **域服务开关**：勾选时，则域服务开启。
   - **域服务器主机地址**：请填写真实的域服务器主机地址。
   - **域服务器备机地址**：请填写真实的域服务器备机地址。
   - **域主机认证端口**：默认端口为389，请根据实际环境填写。
   - **域备机认证端口**：同上。
   - **域名格式**：$uid@domainname。其中 `$uid` 为固定格式，domainname 为域服务器的域名。

5. 单击**保存**，即可完成域服务配置。

配置证书

最近更新时间：2024-09-19 15:34:41

操作场景

堡垒机支持使用证书认证进行登录，使用证书认证之前需先配置证书服务，下面将为您详细介绍如何在堡垒机上配置证书服务。

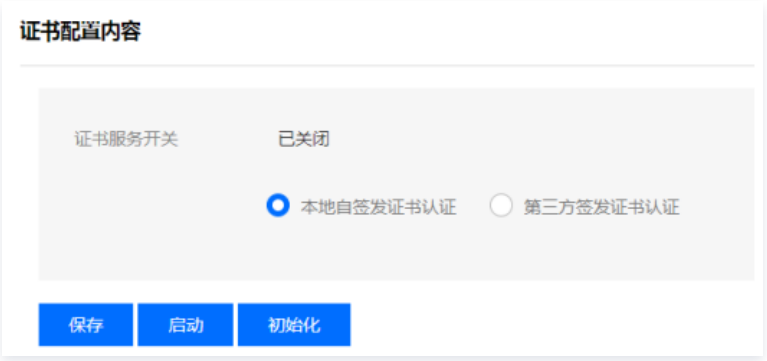
> **说明**
> 当系统开启证书认证方式时，此开关需要打开。若开关打开时，用户需要提供合法的身份认证才能进入系统。

操作步骤

堡垒机支持 本地自签发证书认证 和 第三方签发证书认证 。

本地自签发证书认证

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. 在右上角单击**系统管理**，进入系统管理页面。
3. 在系统管理页面，选择**安全设置** > **证书配置**，进入证书配置页面。
4. 选择认证类型：**本地自签发证书认证**，本地证书认证为堡垒机内部证书服务。

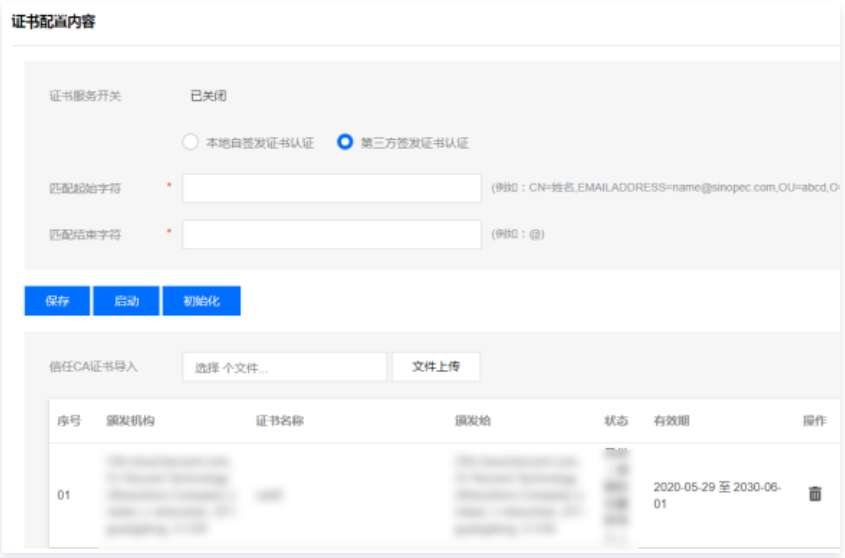


5. 进行相关操作，包括保存、启动及初始化。
   - 单击保存，保存该配置信息。
   - 单击**启动**，启动本地自签发证书认证。
   - 单击**初始化**，系统将清除已配置的信息，并恢复至默认值。

第三方签发证书认证

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. 在右上角单击**系统管理**，进入系统管理页面。
3. 在系统管理页面，选择**安全设置** > **证书配置**，进入证书配置页面。
4. 选择认证类型：**第三方签发证书认证**。
5. 配置证书起始和结束字符。说明如下：
   - 匹配起始字符：个人证书使用者的用户账号起始字符。
   - 匹配结束字符：个人证书使用者的用户账号结束字符。
     - 示例1：CN=姓名，EMAILADDRESS=name@xx.com，OU=abcd，O=SINOPEC，C=CN
       则匹配起始字符为：`EMAILADDRESS=` 匹配结束字符为：`@`

- 示例2：CN=test，则配置匹配起始字符为 `CN=`，匹配结束字符为 `,`



6. 进行相关操作，包括保存、启动、初始化及上传文件。
   - 单击保存，保存配置信息。
   - 单击启动，启动第三方签发证书认证。
   - 单击初始化，系统将清除已配置的信息，并恢复至默认值。
   - 单击文件上传，可导入证书文件。

版权所有：腾讯云计算（北京）有限责任公司

配置短信认证

最近更新时间：2024-09-19 15:34:41

当系统开启短信认证方式时，用户需要提供合法的身份认证才能进入系统。

前提条件

需已开通 腾讯云短信服务 。

操作步骤

1. 登录 堡垒机控制台，找到需要操作的堡垒机，在右侧操作栏单击**管理**，进入堡垒机登录页面，也可以直接在浏览器中，输入访问地址 `https://IP` ，进入登录页面，并使用管理员账号登录堡垒机。
2. 在右上角单击**系统管理**，进入系统管理页面。
3. 在系统管理页面，选择**安全设置** > **短信配置**，进入短信认证配置页面。
4. 在短信认证配置页面，输入相关字段，单击**保存**即可完成配置，详情请参见 国内短信快速入门 。

> **说明**
> 仅支持使用1个变量参数的模板。

字段说明：

- **短信应用 ID**：开通短信服务，创建短信时系统生成的 ID，由数字组成。
- **短信签名**：选择创建短信时新建的签名。例如，腾讯云，中英文都可以，无字符长度限制。
- **验证码正文模板 ID**：创建短信正文模板时，系统生成的 ID，由数字组成。
- **工单通知正文模板 ID**：创建短信工单通知正文模板时，系统生成的 ID，由数字组成。

初始化口令配置

最近更新时间：2024-09-19 15:34:41

操作场景

本文为您详细介绍如何初始化口令。

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. 在右上角单击**系统管理**，进入系统管理页面。
3. 在系统管理页面，选择**安全设置** > **初始化口令配置**，进入初始化口令配置页面。
4. 输入固定口令或配置初始化随机口令规则后，单击**保存**即可，也可以单击**查看**，查看已配置的固定口令。

运维安全水印

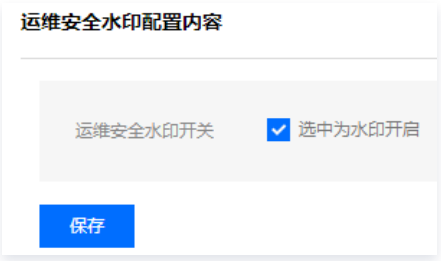
最近更新时间：2024-09-19 15:34:41

操作场景

本文为您详细介绍配置运维安全水印，运维安全水印开关开启后，运维用户单点登录页面会有该用户信息，当前时间形成的水印。

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. 在右上角单击**系统管理**，进入系统管理页面。
3. 在系统管理页面，选择**安全设置** > **运维安全水印**，进入配置页面。
4. 勾选**选中为水印开启**，单击**保存**，即可开启运维安全水印。



数据维护
配置数据维护

最近更新时间：2024-09-19 15:34:41

本文将为您介绍如何快速使用配置数据维护功能。

操作场景

配置数据维护功能用于配置数据的备份、下载、还原等。

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. 在右上角单击**系统管理**，进入系统管理页面。
3. 在系统管理页面的左侧导航中，选择**数据维护** > **配置数据维护**。
   - **新建备份任务**

     3.1.1 在配置数据维护页面，单击**新建备份任务**。

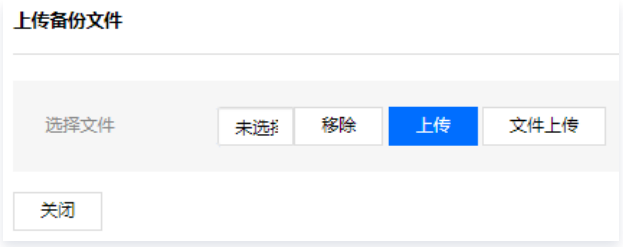
     3.1.2 在“新建备份任务”弹窗中，输入相关内容，单击**生成备份**，即可备份成功。

   - **上传备份**

     3.1.1 在配置数据维护页面，单击**上传备份**。

     3.1.2 在上传备份文件页面，单击**文件上传**，选择备份文件。

     3.1.3 选择完成后，确认无误，单击**上传**，即可成功上传备份。

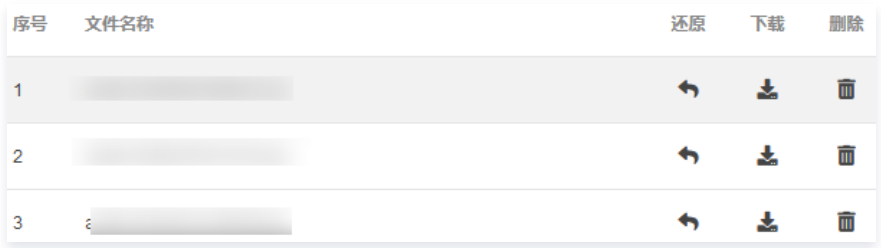


   - **备份任务**

     3.1.1 在配置数据维护页面，单击**备份任务**。

     3.1.2 在备份任务页面，可查看所有备份任务并可进行还原、下载和删除操作。
     - 还原：还原相关的配置数据。
     - 下载：下载备份文件。

- 删除：删除备份任务。



审计数据维护

最近更新时间：2024-09-12 15:56:21

本文将为您介绍如何快速使用审计数据维护功能。

操作场景

审计数据维护功能用于管理审计、行为审计全部及行为审计录像的备份、下载、上传等。

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. 在右上角单击**系统管理**，进入系统管理页面。
3. 在系统管理页面的左侧导航中，选择**数据维护>审计数据维护**。
   - **新建备份任务**

     3.1.1 在审计数据维护页面，单击**新建备份任务**。

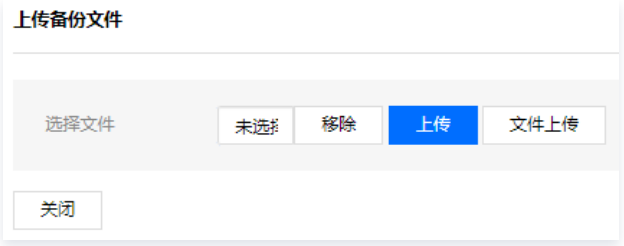
     3.1.2 在“新建备份任务”弹窗中，输入相关内容，单击**生成备份**，即可备份成功。

   - **上传备份**

     3.1.1 在审计数据维护页面，单击**上传备份**。

     3.1.2 在上传备份文件页面，单击**文件上传**，选择备份文件。

     3.1.3 选择完成后，确认无误，单击**上传**，即可成功上传备份。

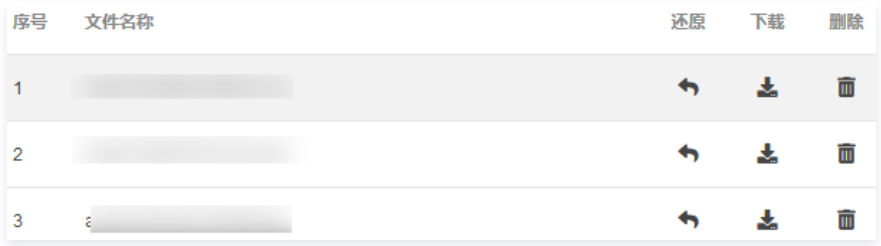


   - **备份任务**

     3.1.1 在审计数据维护页面，单击**备份任务**。

     3.1.2 在备份任务页面，可查看所有备份任务并可进行还原、下载和删除操作。

- 还原：还原相关的审计日志。
- 下载：下载备份文件。
- 删除：删除备份任务。



自维护

最近更新时间：2024-09-19 15:34:41

操作场景

本文为您介绍管理自身堡垒机账号信息。

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. 在页面右上角选择**用户名 > 自维护**，进入自维护页面。

3. 在自维护页面，可以对基本信息进行维护，包括口令更改、唯一标识、证书管理。

版权所有：腾讯云计算（北京）有限责任公司

审计管理
管理审计
基础信息维护审计

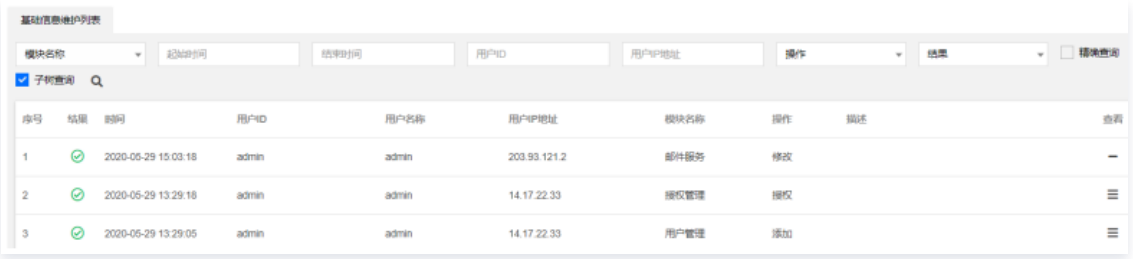
最近更新时间：2024-09-19 15:34:41

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询基础信息维护审计。

操作步骤

1. 登录腾讯云 堡垒机控制台，并使用审计管理员账号登录堡垒机。
2. 在右上角单击**审计平台**，即可进入审计平台，默认进入管理审计模块。
3. 单击**基础信息维护审计**，进入基础信息维护审计页面，可以查看用户对各个模块的操作记录，及操作结果。
4. 设定查询条件，可以输入起始时间、结束时间、用户 ID、用户 IP 地址、选择操作、选择结果、对用户安全认证日志进行查询。



5. 在审计结果中，单击右侧的 ≡，进入基础信息维护详细页面。

版权所有：腾讯云计算（北京）有限责任公司

安全认证审计

最近更新时间：2024-09-19 15:34:41

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。

操作步骤

1. 登录腾讯云 堡垒机控制台，并使用审计管理员账号登录堡垒机。
2. 在左上角单击**审计平台**，进入审计平台，默认进入管理审计模块。
3. 单击**认证审计**，进入安全审计日志查询页面，可以查看系统中用户的登录登出相关日志。
4. 设定查询条件，可以输入起始时间、结束时间、用户 ID、用户 IP 地址、选择操作、选择结果、对用户安全认证日志进行查询。

5. 在设定查询条件后，单击搜索按钮，系统将按照查询条件开始查询。

版权所有：腾讯云计算（北京）有限责任公司

操作行为审计
在线会话审计

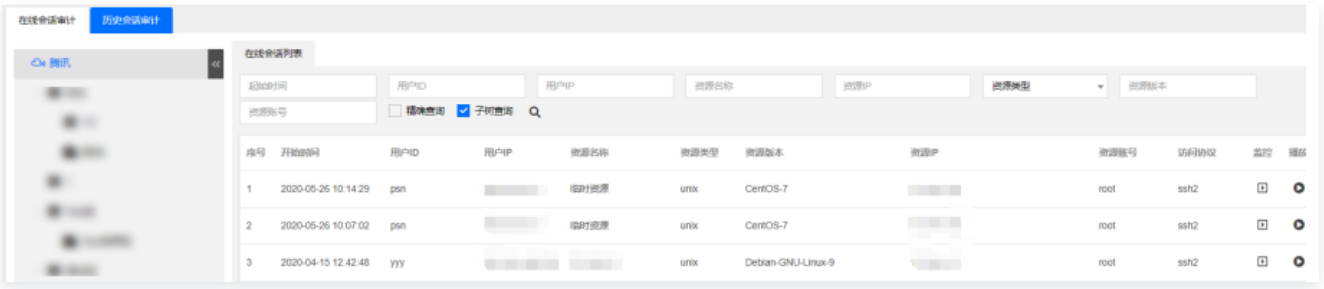
最近更新时间：2024-09-19 15:34:41

操作场景

本文为您详细介绍如何查询在线会话审计。

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. 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。

版权所有：腾讯云计算（北京）有限责任公司

历史会话审计

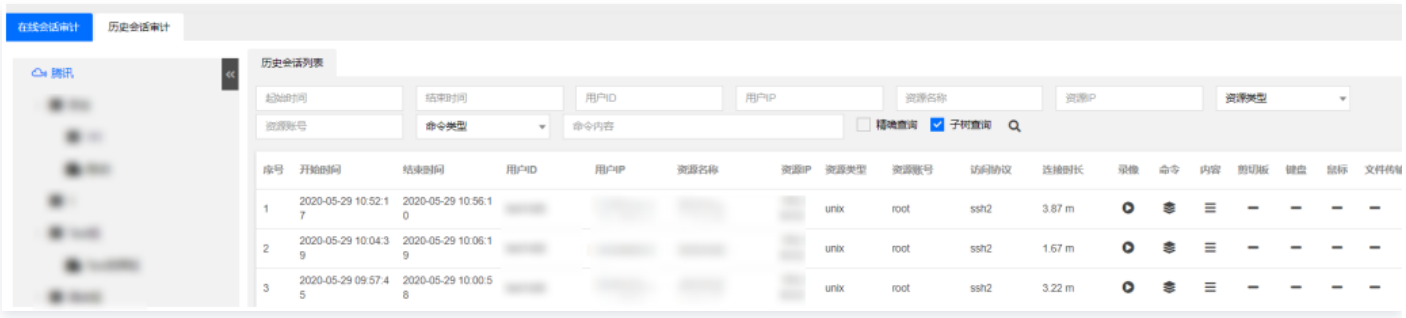
最近更新时间：2024-09-19 15:34:41

操作场景

本文为您详细介绍如何查询历史会话审计。

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. 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。



版权所有：腾讯云计算（北京）有限责任公司

统计报表
基础报表

最近更新时间：2024-09-19 15:34:41

操作场景

堡垒机系统支持将用户信息、组织信息、系统数据、审计数据等输出为报表，方便管理员查看。本文为您详细介绍在堡垒机如何生成用户信息审计报表和资源信息审计报表。

用户信息审计报表

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. 在左上角单击**审计平台**，进入审计平台，单击**统计报表**，进入基础报表页面。
3. 单击**用户信息报表**，可以生成并导出用户信息统计报表、用户归属组统计报表、用户类型统计报表、用户授权关系报表、用户角色关系报表、用户非法登录 TopN 报表、用户策略对应关系报表、策略用户对应关系报表。

资源信息审计报表

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. 在左上角单击**审计平台**，进入审计平台，单击**统计报表**，进入基础报表页面。
3. 单击**用户信息报表**，可以生成并导出资源信息统计报表、资源类型统计报表、资源账号接管状态报表、资源账号鉴别状态报表、资源在线统计报表、资源下线统计报表、资源系统版本统计报表。

运维业务报表

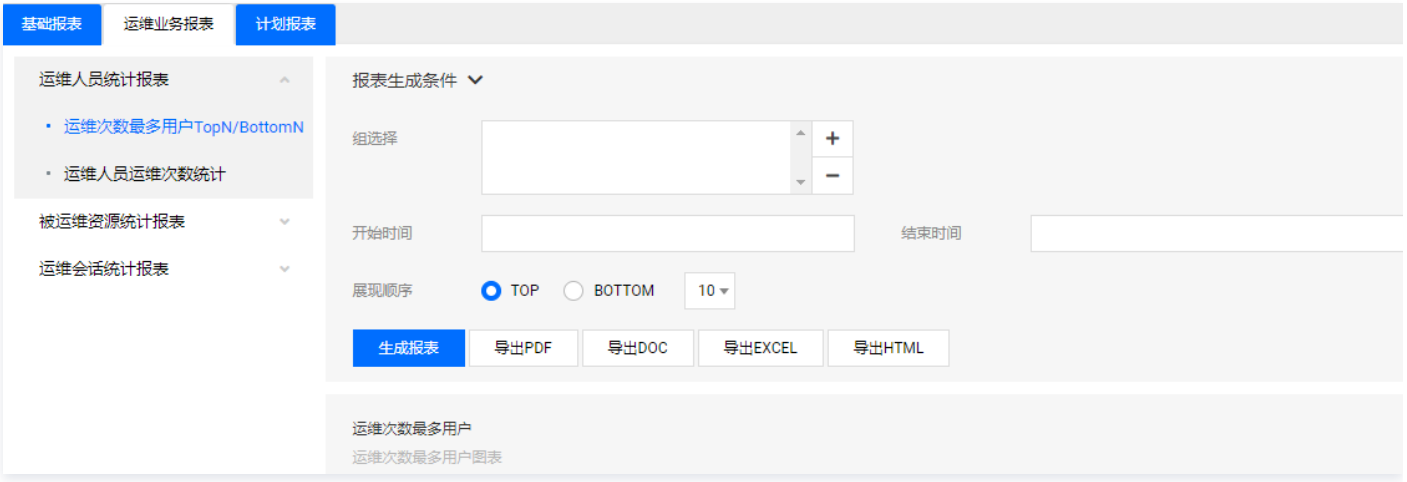
最近更新时间：2024-09-19 15:34:41

操作场景

堡垒机系统支持将用户信息、组织信息、系统数据、审计数据等输出为报表，方便管理员查看。本文为您详细介绍在堡垒机如何生成运维业务报表。

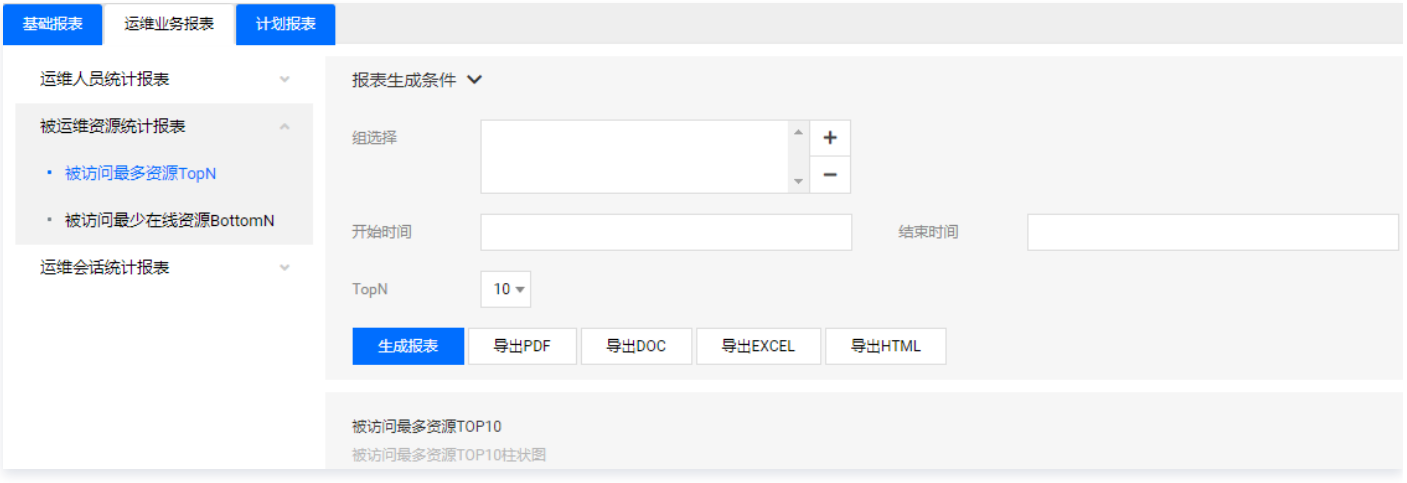
运维业务人员统计报表

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. 在右上角单击**审计平台**，进入审计平台，单击**统计报表**，进入基础报表页面。
3. 单击**运维业务报表**，进入运维业务报表页面，单击**运维人员统计报表**，可生成并导出运维次数最多用户TopN/BottomN/报表、运维人员运维次数统计报表。



被运维资源统计报表

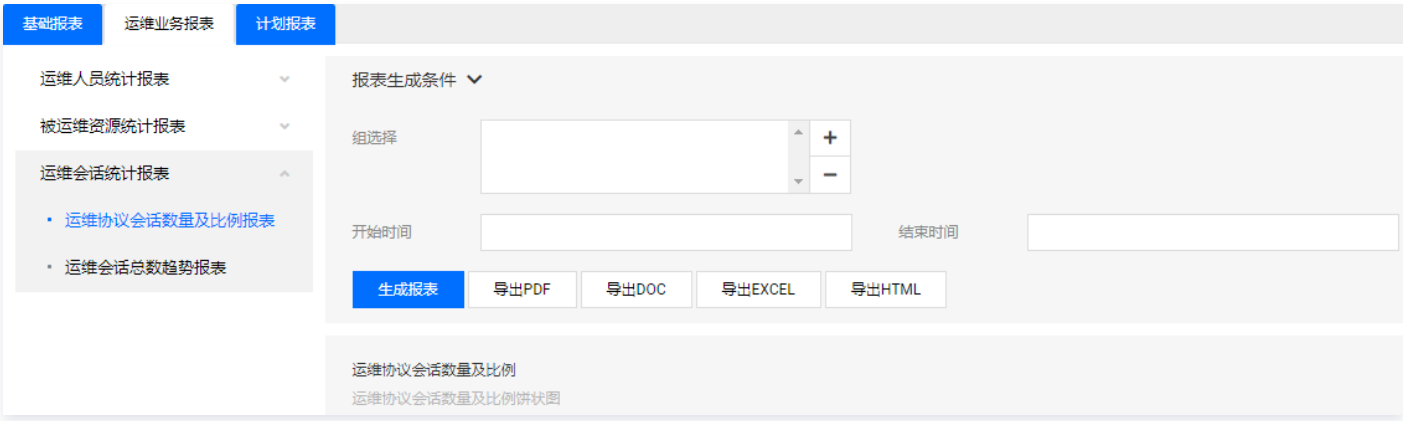
1. 登录腾讯云 堡垒机控制台，并使用管理员账号登录堡垒机。
2. 在右上角单击**审计平台**，进入审计平台，单击**统计报表**，进入基础报表页面。
3. 单击**运维业务报表**，进入运维业务报表页面，单击**被运维资源统计报表**，可生成并导出被访问最多资源 TopN 报表、被访问最少在线资源 BottomN 报表。



运维会话统计报表

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. 在右上角单击**审计平台**，进入审计平台，单击**统计报表**，进入基础报表页面。

3. 单击**运维业务报表**，进入运维业务报表页面，单击**运维会话统计报表**，可生成并导出运维协议会话数量及比例报表、运维会话总数趋势报表。



计划报表

最近更新时间：2024-09-19 15:34:41

本文档将为您介绍如何在堡垒机中使用计划报表功能。

操作场景

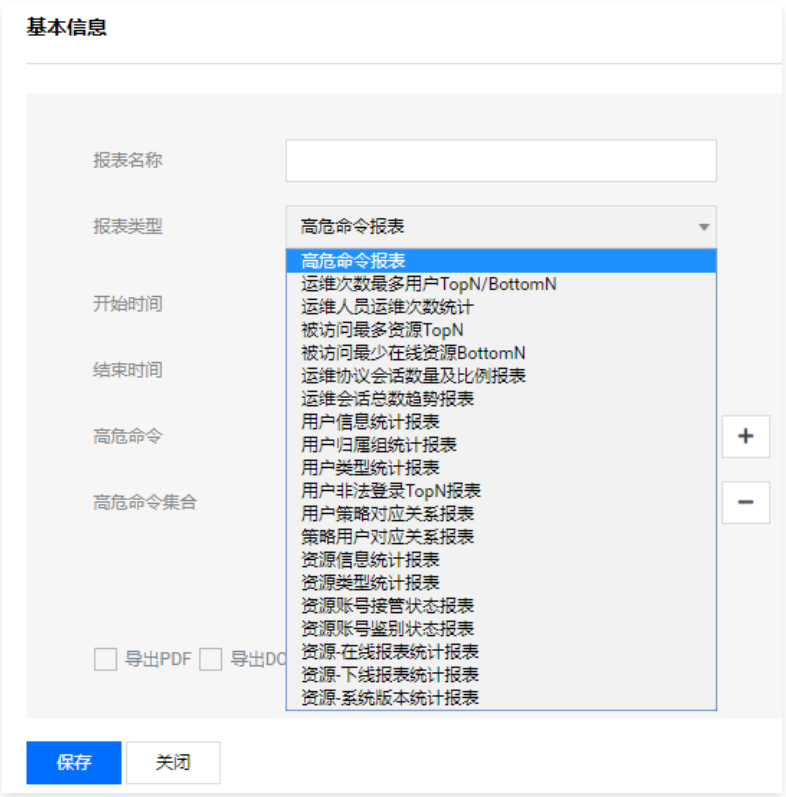
堡垒机系统支持设置计划报表任务，设置完后，将根据设置的规则进行任务调度。

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. 在右上角单击**审计平台**，进入审计平台，并单击**统计报表**。
3. 在统计报表页面，单击**计划报表**，进入计划报表页面。
4. 在计划报表页面，单击**新建**。
5. 在新建计划页面填写相关字段，单击**保存**。

6. 新建计划报表后，找到目标计划报表，在“报表条件列表”列，单击，进入报表条件页面。

7. 在报表条件页面，单击**新建**，填写报表名称，需导出的报表类型，及任务执行的开始和结束时间等，并选择要导出的报表类型，可导出 PDF\DOC\EXCEL\HTML 格式，单击**保存**。



8. 设置完成后，在目标计划报表的“启动/停止”列，单击**启动**，可将计划启动，同时可在“执行日志”列，单击**执行日志**，查看执行日志。

查询审计日志

最近更新时间：2024-09-19 15:34:41

操作场景

本文为您详细介绍如何全局搜索审计日志。

操作步骤

1. 登录腾讯云 堡垒机控制台，并使用审计管理员账号登录堡垒机。
2. 在左上方单击**审计平台**，进入审计平台，默认进入管理审计模块。
3. 单击**搜索**，进入全局搜索页面，可以根据起始时间、角色时间等查看用户操作行为审计日志。

> **说明：**
> 堡垒机可以保存全量审计日志，至少保存6个月操作审计日志。

告警设置
告警策略

最近更新时间：2024-09-19 15:34:41

操作场景

堡垒机系统支持设置告警策略，告警策略设置完成后，一旦满足所设置的告警策略，即会触发告警。

违规命令告警

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. 在左上角单击**审计平台**，进入审计平台，单击**告警**，进入告警策略页面。
3. 在告警策略页面，选择**运维类告警** > **违规命令告警**，进入告警策略列表。
4. 在告警策略列表中，单击**新建**，填写策略名称，并设置告警状态为“开启”，填写描述信息后，单击【保存】，可填写设置规则。

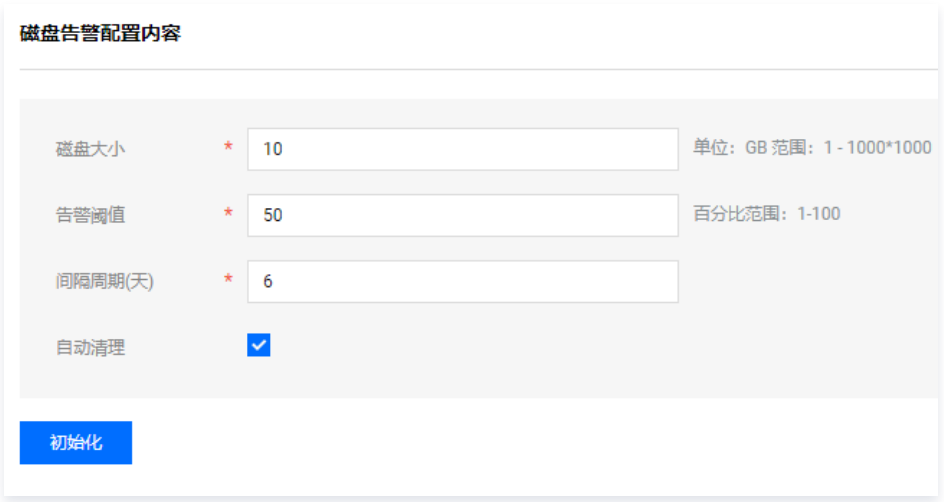
5. 在设置规则页面，可设置同一会话中被阻断命令次数，设置完成后，单击【保存】即可。

> **注意**
> - 需要创建相应的字符命令策略，在字符命令控制策略页面，创建一个字符命令策略，进行保存，详情请参见 添加字符命令策略 。
>
> 告警条件（违规次数）可设置次数为1 - 100。

系统磁盘告警

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. 在左上角单击**审计平台**，进入审计平台，单击**告警**，进入告警策略页面。
3. 在告警策略页面，选择**系统类告警** > **系统磁盘告警**，进入“磁盘告警配置内容”页面。
4. 在“磁盘告警配置内容”页面，填写相关配置内容，包括磁盘大小、告警阈值、间隔周期（天）。
   - 磁盘大小：设备的磁盘大小，单位：GB，范围：1 - 1000 * 1000。
   - 告警阈值：设置为百分比，磁盘使用达到百分百的时候启动告警。
   - 间隔周期（天）：告警间隔周期。

- 自动清理：勾选自动清理后，堡垒机会按照告警周期以及告警值进行磁盘清理。

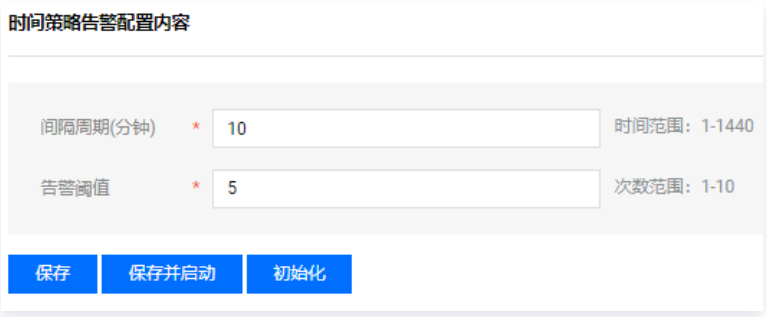


5. 告警内容填写完成后，单击**初始化**，即可设置完成。

时间策略告警

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. 在左上角单击**审计平台**，进入审计平台，单击**告警**，进入告警策略页面。
3. 在告警策略页面，选择**用户类告警** > **时间策略告警**，进入“时间策略告警配置内容”页面。
4. 在“时间策略告警配置内容”页面，设置告警阈值和告警周期后，单击**保存并启动**即可完成设置。

> **注意**
> 创建完时间策略告警后，要创建相应的时间策略，设置用户登录堡垒机的时间范围，详情请参见 添加时间策略 。



告警配置

最近更新时间：2024-09-24 17:01:32

操作场景

堡垒机系统支持设置多个接收告警邮件的邮箱。

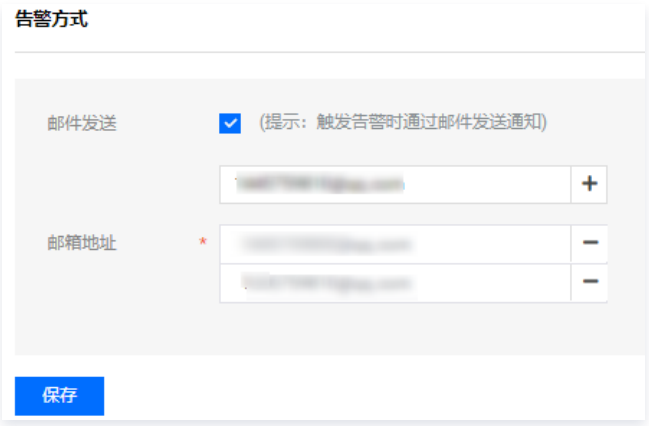
前提条件

需要已在系统配置的 配置邮件服务 中，设置邮件发送服务。

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. 在左上角单击**审计平台**，进入审计平台，单击**告警**，默认进入告警策略页面。
3. 单击**告警配置**，可添加接收告警信息通知的邮箱地址，允许添加多个。

> **注意：**
> 违规命令告警 触发后，需要关闭会话，等待两分钟才可收到告警邮件。



告警事件

最近更新时间：2024-09-19 15:34:41

操作场景

堡垒机系统支持查看并处理全部告警事件。

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. 在左上角单击**审计平台**，进入审计平台，单击**告警**，默认进入告警策略页面。
3. 单击**告警事件**，在告警事件页面可查看全部告警事件，并进行处理或忽略。

版权所有：腾讯云计算（北京）有限责任公司

运维配置手册
运维配置总览

最近更新时间：2024-11-26 15:34:54

概述

运维用户在使用堡垒机时，可能碰到诸如控件下载、单点登录等问题。本文将介绍堡垒机产品使用过程中的常用操作，供您参考。

运维使用

- 下载控件
- 安装证书
- 单点登录
- 授权列表
  - 登录 Windows 资源
    - 使用 Web 登录
    - 使用 XFTP 登录
    - 使用 Mstsc 登录
  - 登录 Linux 资源
    - 使用 Web 登录
    - 使用 PuTTY 登录
    - 使用 Xshell/SecureCRT 登录
    - 使用 XFTP 方式登录
  - 登录数据库资源
    - 使用 Web 登录
    - 使用 Mstsc 登录
- 工单
- 脚本计划
- Mac 系统支持工具登录

版权所有：腾讯云计算（北京）有限责任公司

下载控件

最近更新时间：2024-09-19 15:34:41

本文档将为您详细介绍如何下载控件并更好地使用堡垒机。

操作场景

运维用户在第一次登录堡垒机后，需要下载控件并安装，使用控件能帮助运维用户更好地使用堡垒机。

操作步骤

1. 登录腾讯云 堡垒机控制台，选择一台已部署好的堡垒机实例，在右侧操作栏，单击**管理**，进入堡垒机登录页面。
2. 使用运维用户账号登录堡垒机。

> **说明**
> 运维用户由管理员账号进行创建，若运维用户忘记密码，可以联系管理员进行重置，详情请参见 设置口令 。

3. 单击，进入套件中心。
   - **单点登录工具（标准）**：集成审计查看工具标准版。
   - **根证书**：根证书安装后可使页面响应速度加快，另外，使用证书认证的客户端需安装根证书。

4. 下载单点登录工具或根证书，并根据安装提示进行安装，安装证书步骤，请参见 安装根证书 。

安装证书
Mac OS 系统安装证书

最近更新时间：2024-09-19 15:34:41

本文档将指导用户在 Mac OS 系统中安装信任证书。

操作场景

运维用户使用本地自签发证书认证登录堡垒机时，运维用户需要在 Mac OS 系统中安装信任证书。

操作步骤

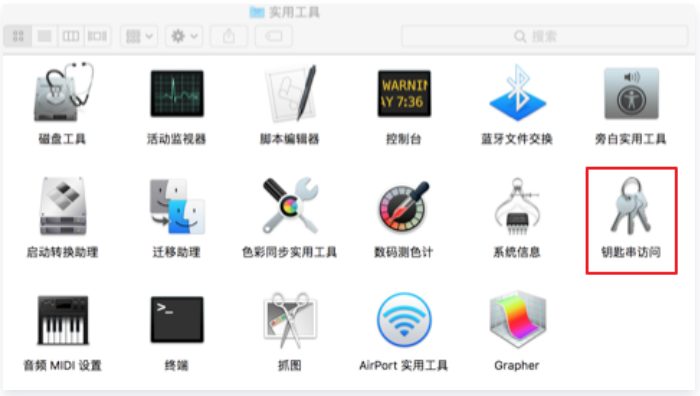
1. 使用 Safari 浏览器访问堡垒机网站，Safari 会提示该网站证书存在问题，单击**显示详细信息**，将出现风险提示。

2. 在出现风险提示框中，单击**访问此网站**，将弹出确认框。

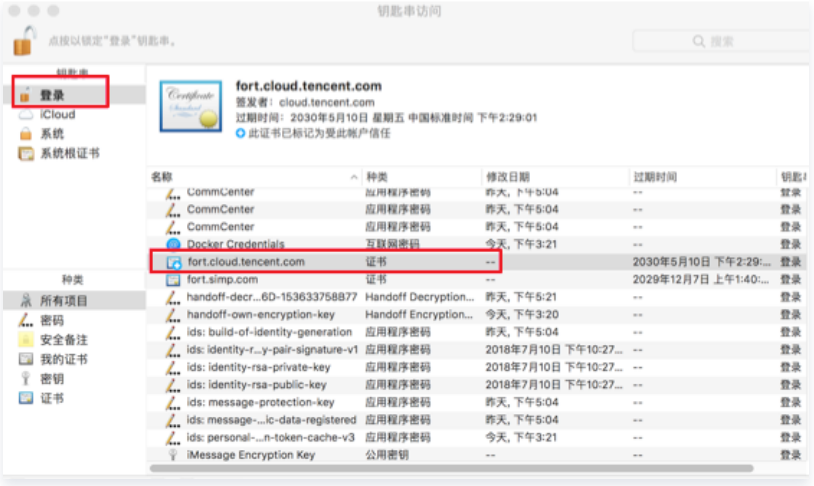
3. 在确认框中，单击**访问网站**，将弹出验证框。

4. 在验证框中，输入用户名及密码。

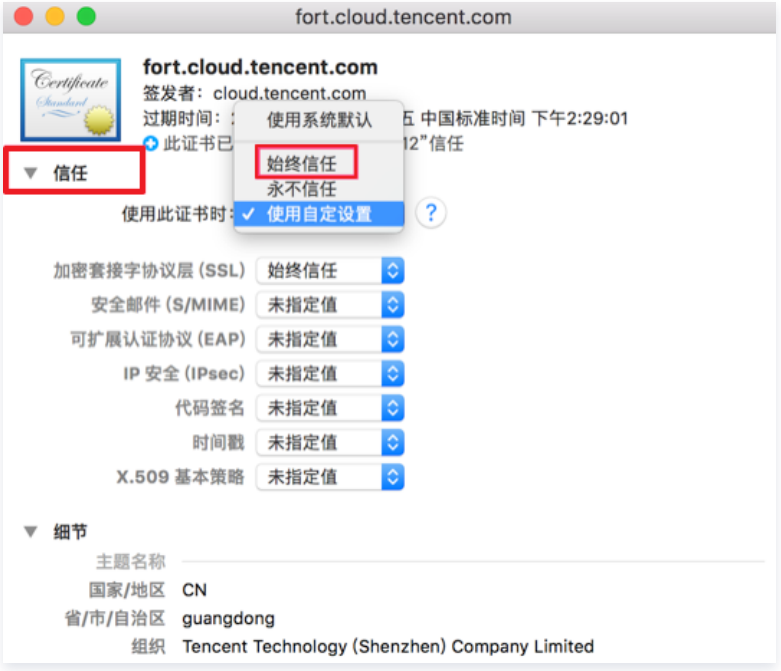
5. 确认完成后，在 Mac OS 的实用工具中，打开钥匙串访问应用。



6. 在登录选项卡中，找到网站的证书，双击证书。



7. 在信任选项中，改为始终信任。



8. 再次在弹出的验证框中，输入密码，将成功信任该网站的证书。

Windows 系统安装证书

最近更新时间：2024-09-19 15:34:41

本文档将指导用户在 Windows 系统中安装根证书和个人证书。

操作场景

当运维用户在 Windows 系统中，使用本地自签发证书认证登录堡垒机时，运维用户需要安装根证书和个人证书。下面将为运维用户详细介绍如何安装根证书和个人证书。

前提条件

1. 已下载根证书，下载方法请参见 下载控件 文档。
2. 个人证书需由管理员生成后，下发给各用户。若管理员未生成个人证书，请联系管理员生成。

操作步骤

安装根证书

1. 双击根证书文件。
2. 单击**安装证书** > **下一步**，进入证书导入向导页面。
3. 选择“受信任的根证书颁发机构”。

4. 单击**下一步** > **完成**，完成安装根证书。

下载安装个人证书

下载个人证书

1. 使用运维账号登录堡垒机系统。

2. 在页面右上角单击个人头像，进入自维护页面。

3. 选择**证书管理** > **下载证书**，将个人证书下载到本地。

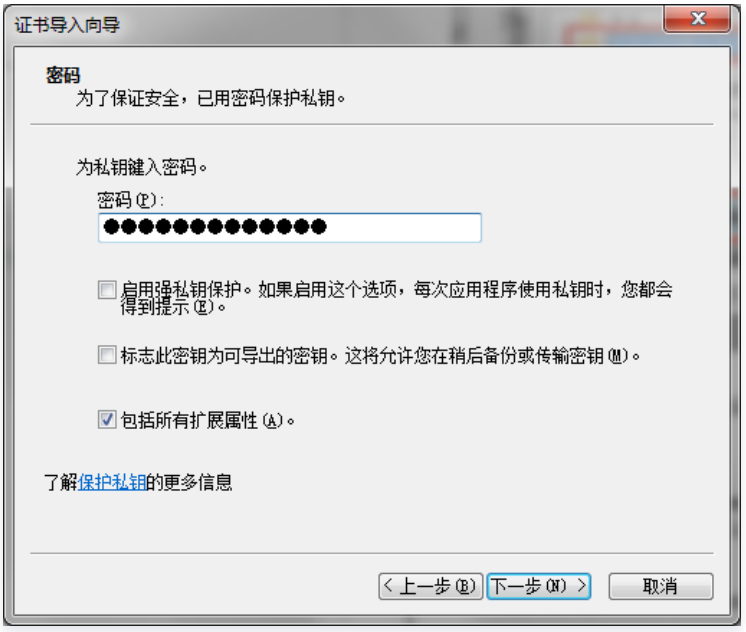
> **注意**
> 证书生成后，有效期为10年，过期后需重新生成。

安装个人证书

1. 双击个人证书文件。
2. 选择“个人”。

3. 单击**下一步** > **下一步**，进入输入密码界面。

4. 输入密码 `zD3A7S9B#&2uS` 。



5. 单击**下一步** > **完成**，即可完成安装个人证书。

单点登录

最近更新时间：2024-09-19 15:34:41

本文档将为您介绍如何通过堡垒机进行单点登录，即堡垒机代理的多个资源之间，通过一次登录完成所有业务的登录操作。

背景信息

堡垒机支持两种登录资源方式：Web 页面登录和客户端工具登录。

单点登录支持的方式

资源类型	支持方式			
Windows	Mstsc	FTP	-	-
Linux	Xshell	SecureCRT	putty	VNC
	Xwindow	FTP	SFTP	-

前提条件

进行单点登录前，需已下载安装 单点登录工具 。

操作步骤

1. 登录腾讯云 堡垒机控制台 ，选择一台已部署好的堡垒机实例，在右侧操作栏，单击**管理**，进入堡垒机登录页面。
2. 使用运维用户账号登录堡垒机。

> **说明**
> 运维用户由管理员进行创建，若运维用户忘记密码，可以联系管理员进行重置，详情请参见 设置口令 。

3. 在左侧菜单栏，单击**运维**，进入运维页面。
4. 单击**首页**，进入首页快速登录列表。

5. 在资源列表登录方式栏中，选择需要登录方式的按钮（例如 **WEB** 或 **RDP** 等），即可直接登录系统。

授权列表
登录 Windows 资源
使用 Web 登录

最近更新时间：2024-09-19 15:34:41

操作场景

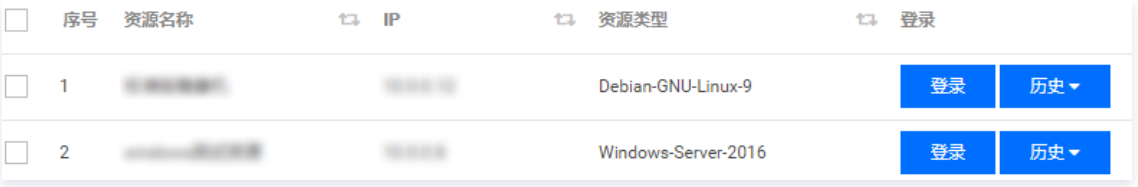
Windows 类资源包含两种单点登录方式：图形登录（WEB 登录）、FTP 登录。根据不同的登录协议，选择相应的登录工具。Windows 资源协议，例如 RDP、FTP、VNC 等协议都支持通过堡垒机 WEB 页面登录。
该指南指导运维用户在登录堡垒机系统后，使用 WEB 方式登录 Windows 资源。用户在资源上执行的操作能够被堡垒机记录并生成相关的审计数据。

前提条件

1. 已下载安装 控件 。
2. 拥有访问 Windows 资源权限，若无权限，请联系管理员进行配置。

操作步骤

1. 登录腾讯云 堡垒机控制台 。
2. 运维用户登录堡垒机系统。
3. 单击**授权列表**，进入资源列表页。
4. 找到您需要登录的 Windows 资源，在其右侧单击**登录**，进行登录配置。



5. 在配置窗口中，配置如下。
   - **协议**：选择“RDP”，Windows 默认远程协议使用 RDP。
   - **账号**：输入 Windows 的系统账号。
   - **口令**：输入 Windows 账号的密码。
   - **工具**：选择 WEB 工具。
   - **选择分辨率**：远程登录 Windows，其窗口的分辨率。

- **超时时间**：连接 Windows 资源的超时时间，默认为5秒。

6. 确认配置信息无误后，单击**登录**，登录到目标资源后，即可对资源进行运维操作。

使用 XFTP 登录

最近更新时间：2024-09-19 15:34:41

操作场景

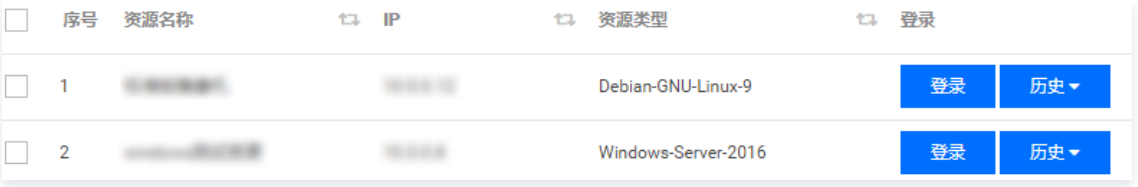
该指南指导运维用户在登录堡垒机系统后，使用 XFTP 方式登录 Windows 资源进行操作，通过 XFTP 工具能够上传下载文件。用户上传下载文件能够被堡垒机记录并生成相关的审计数据。

前提条件

1. 已下载安装 控件 。
2. 已下载安装 WinSCP 工具。
3. 拥有访问 Windows 资源权限，若无权限，请联系管理员进行配置。
4. Windows 资源机使用 XFTP 工具前，需要在 Windows 资源机上部署 FTP 服务。

操作步骤

1. 登录腾讯云 堡垒机控制台 。
2. 运维用户登录堡垒机系统。
3. 单击**授权列表**，进入资源列表页。
4. 找到您需要登录的 Windows 资源，在其右侧单击**登录**，进行登录配置。



5. 在配置窗口中，配置如下。
   - 协议：选择“FTP”。
   - 账号：输入 Windows 的系统账号。
   - 口令：输入 Windows 账号的密码。

     说明
     账号和口令为 添加资源 时设置的账号和口令。

   - 工具：选择 XFTP 工具。

- 超时时间：连接 Windows 资源的超时时间，默认为5秒。

6. 确认配置信息无误后，单击**登录**，系统将根据配置，调用本地的 WinSCP 工具连接到目标资源，目标资源连接成功后即可上传、下载文件。

使用 Mstsc 登录

最近更新时间：2024-09-19 15:34:41

操作场景

Windows 类资源包含两种单点登录方式：图形登录（WEB 登录）、FTP 登录。根据不同的登录协议，选择相应的登录工具。
该指南指导运维用户在登录堡垒机系统后，通过调用本地 Mstsc 登录 Windows 资源。用户在资源上执行的操作能够被堡垒机记录并生成相关的审计数据。

前提条件

1. 已下载安装 控件 。
2. 拥有访问 Windows 资源权限，若无权限，请联系管理员进行配置。

操作步骤

1. 登录腾讯云 堡垒机控制台 。
2. 运维用户登录堡垒机系统。
3. 单击**授权列表**，进入资源列表页。
4. 找到您需要登录的 Windows 资源，在其右侧单击**登录**，进行登录配置。

5. 在配置窗口中，配置如下。
   - **协议**：选择“RDP”，Windows 默认远程协议使用 RDP。
   - **账号**：输入 Windows 的系统账号。
   - **口令**：输入 Windows 账号的密码。
   - **工具**：选择 RDP 工具。
   - **选择分辨率**：远程登录 Windows，其窗口的分辨率。
   - **超时时间**：连接 Windows 资源的超时时间，默认为5秒。

6. 确认配置信息无误后，单击**登录**，系统将根据配置，调用本地的 Mstsc 连接到目标资源。

登录 Linux 资源
使用 Web 登录

最近更新时间：2024-09-19 15:34:41

本文档将指导运维用户在登录堡垒机系统后，使用 Web 方式登录 Linux 资源进行操作。用户的操作能够被堡垒机记录并生成相关的审计数据。

操作场景

堡垒机支持登录 Linux 资源协议，如 ssh2、ssh1、Telnet、sftp、ftp、VNC、XWindows 都支持使用 Web 页面进行登录。

前提条件

1. 已下载安装 控件 。
2. 拥有访问 Linux 资源权限，若无权限，请联系管理员进行配置。

操作步骤

1. 登录腾讯云 堡垒机控制台 。
2. 运维用户登录堡垒机系统。
3. 单击**授权列表**，进入资源列表页。
4. 找到您需要登录的 Linux 资源，在其右侧单击**登录**，进行登录配置。

5. 在配置登录窗口，配置如下：
   - **协议**：Linux 资源建议选择 SSH2 协议。
   - **账号**：输入 Linux 资源的账号
   - **连接工具**：选择 WEB。
   - **超时时间**：连接 Linux 资源的超时时间，默认为5秒。

6. 单击**登录**，即可通过 Web 方式登录到 Linux 资源。

使用 PuTTY 登录

最近更新时间：2024-09-19 15:34:42

操作场景

该指南指导运维用户在登录堡垒机系统后，使用图形方式登录 Linux 资源进行操作。用户在资源进行的运维操作，能够被堡垒机记录并生成相关的审计数据。

前提条件

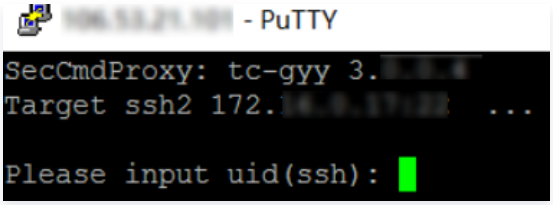
1. 已下载安装 控件 。
2. 拥有访问 Linux 资源权限，若无权限，请联系管理员进行配置。

操作步骤

1. 登录腾讯云 堡垒机控制台 。
2. 运维用户登录堡垒机。
3. 单击**授权列表**，进入资源列表页。
4. 找到您需要登录的 Linux 资源，在其右侧单击**登录**，在弹出的窗口中，进行登录配置。

5. 在配置登录窗口，配置如下：
   - 协议：Linux 资源建议选择 SSH2 协议。
   - 账号：输入 Linux 资源的账号。
   - 口令：输入 Linux 资源账号的密码。
   - 工具：选择 PuTTY 工具。
   - 超时时间：连接 Linux 资源的超时时间，默认为5秒。

6. 确认配置信息无误后，单击**登录**，登录到目标资源后，即可对资源进行运维操作。



使用 XShell 或 SecureCRT 登录

最近更新时间：2024-09-19 15:34:42

操作场景

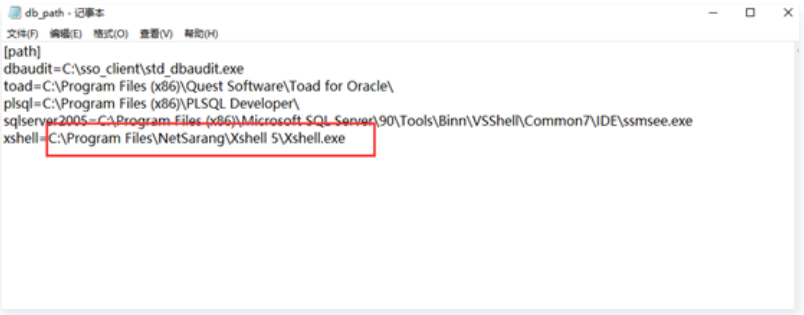
本文为您详细介绍如何通过 SecureCRT 或 XShell 登录 Linux 资源。

前提条件

1. 已下载安装 控件 。
2. 拥有访问 Linux 资源权限，若无权限，请联系管理员进行配置。
3. 已安装 SecureCRT 或 XShell。

配置路径

1. 控件安装之后，进入到控件安装路径下（默认安装路径为：C:\sso_client）。
2. 找到配置文件 db_path，将之前安装的 Xshell 安装路径复制到文件 xshell= 后，如下图所示。（ SecureCRT 无需添加路径）



操作步骤

通过 Xshell 登录

1. 登录腾讯云 堡垒机控制台 。
2. 运维用户登录堡垒机。
3. 单击**授权列表**，进入资源列表页。
4. 找到您需要登录的 Linux 资源，在其右侧单击**登录**，在弹出的窗口中，进行登录配置。

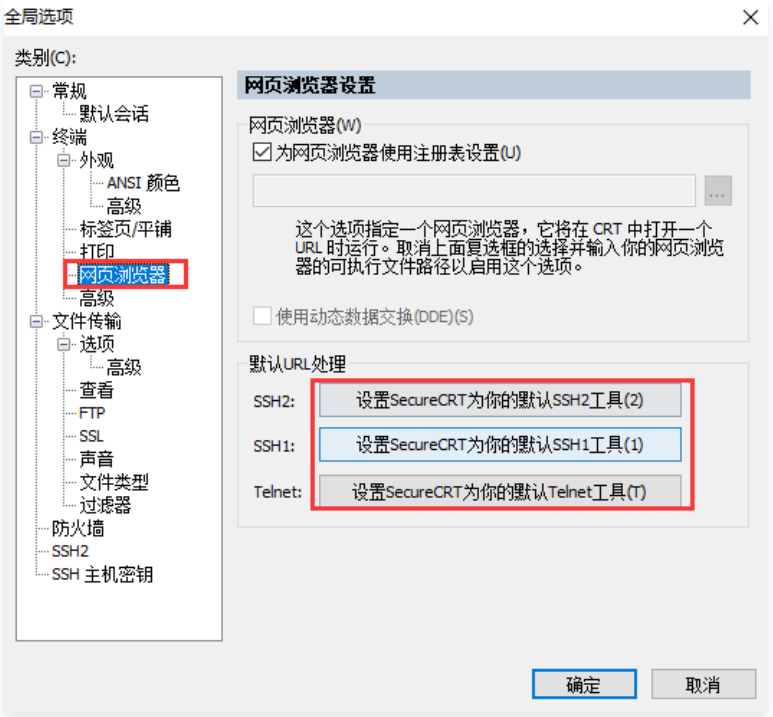
5. 在配置登录窗口，配置如下：
   - 协议：Linux 资源建议选择 SSH2 协议。
   - 账号：输入 Linux 资源的账号。
   - 口令：输入 Linux 资源账号的密码。
   - 工具：选择 X-Shell 工具。

- 超时时间：连接 Linux 资源的超时时间，默认为5秒。

6. 确认配置信息无误后，单击**登录**，登录到目标资源后，即可对资源进行运维操作。

SecureCRT 如何登录?

1. 打开 SecureCRT。
2. 单击**选项** > **全局选项**。
3. 单击**终端** > **网页浏览器**，进入网页浏览器设置页面。
4. 将 SSH2，SSH1 和 Telnet 选项，设置为 “设置SecureCRT为你的默认xxx工具”。



5. SecureCRT 设置完毕后，在运维界面登录 Linux 资源时，选择连接工具 SecureCRT 即可。

使用 XFTP 登录

最近更新时间：2024-09-19 15:34:42

操作场景

该指南指导运维用户在登录堡垒机系统后，使用 XFTP 方式登录 Linux 资源进行操作，通过 XFTP 工具能够上传下载文件。用户上传下载文件能够被堡垒机记录并生成相关的审计数据。

前提条件

1. 已下载安装 控件 。
2. 已下载安装 WinSCP 工具。
3. 拥有访问 Linux 资源权限，若无权限，请联系管理员进行配置。

操作步骤

1. 登录腾讯云 堡垒机控制台 。
2. 运维用户登录堡垒机系统。
3. 单击**授权列表**，进入资源列表页。
4. 找到您需要登录的 Linux 资源，在其右侧单击**登录**，进行登录配置。

5. 在配置登录窗口，配置如下：
   - 协议：选择 SFTP 协议。
   - 账号：输入 Linux 资源的账号。
   - 口令：输入 Linux 账号的口令。
   - 连接工具：选择 XFTP 工具。
   - 超时时间：连接 Linux 资源的超时时间，默认为5秒。

6. 单击**登录**，系统将调用 WinSCP 通过 SFTP 协议登录到 Linux 资源。

版权所有：腾讯云计算（北京）有限责任公司

登录数据库资源
使用 Web 登录

最近更新时间：2025-01-16 21:01:22

文档将指导运维用户在登录堡垒机系统后，使用 Web 方式登录数据库资源进行操作。

前提条件

登录数据库资源需要配置应用发布服务器，配置应用发布后，可以选择相关协议工具单点登录，详情请参见 配置应用发布管理数据库 。

操作步骤

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。

2. 单击**授权列表**，进入资源列表页。
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。

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。

使用 Mstsc 登录

最近更新时间：2025-01-16 21:01:22

文档将指导运维用户在登录堡垒机系统后，使用 Mstsc 登录数据库资源进行操作。

前提条件

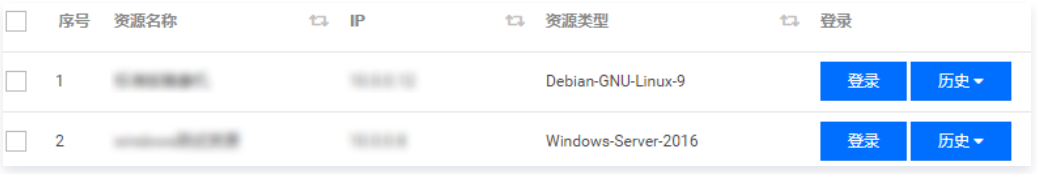
登录数据库资源需要配置应用发布服务器，配置应用发布后，可以选择相关协议工具单点登录，详情请参见 配置应用发布管理数据库 。

操作步骤

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。

2. 单击**授权列表**，进入资源列表页。
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。



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 RDP 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。

工单

最近更新时间：2024-09-19 15:34:42

操作场景

堡垒机提供工单申请入口，运维用户可以提交工单，申请运维资源。

操作步骤

1. 登录腾讯云 堡垒机控制台 ，选择一台已部署好的堡垒机实例，在右侧操作栏，单击**登录**，进入堡垒机登录页面。
2. 使用运维用户账号登录堡垒机。

> **说明**
> 若运维用户忘记密码，可以联系管理员进行重置，详情请参见 设置口令 。

运维工单

我的申请

1. 在页面左上角，单击**工单**，进入工单页面。
2. 在工单页面的左侧导航中，选择**运维工单** > **我的申请**，进入申请工单页面。
3. 单击**新建**，填写工单内容包括：标题、批注信息、计划工作开始和结束时间，填写完后，单击**保存**。

> **说明**
> 具有派发审批工单权限的用户才可以申请工单，由管理员设置派发权限。

4. 保存完成后，单击**指派**，即可进行指派工单执行人。

5. 创建完成的工单，将会出现在申请列表中，并可查看授权信息及运维历史。

未完成

1. 在页面左上角，单击**工单**，进入工单页面。
2. 在工单页面的左侧导航中，选择**运维工单** > **完成**，可查看未完成列表，包括“我待接受”和“我待执行”的工单。
3. 在未完成列表中，可以查看工单的详细信息，包括创建工单时间、工单号、工单标题及状态，同时可查看工单的详细内容。

已完成

1. 在页面左上角，单击**工单**，进入工单页面。
2. 在工单页面的左侧导航中，选择【**运维工单**】> **已完成**，可查看已完成的工单列表。
3. 在已完成工单页面，可以根据时间和工单号查询工单，并查看工单的详细信息。

> **注意**
> 已完结的工单无法重新激活，如有需要仅可以重新发起工单申请。

已归档

1. 在页面左上角，单击**工单**，进入工单页面。
2. 在工单页面的左侧导航中，选择**运维工单** >**已归档**，可查看已归档的工单列表。
3. 在已归档工单页面，可以根据时间和工单号查询归档工单，并查看已归档工单的详细信息。

命令审批

待审批

1. 在页面左上角，单击**工单**，进入工单页面。
2. 在工单页面的左侧导航中，选择**命令审批** > **待审批**，可查看我待办的命令列表。
3. 可在命令列表中，查看申请时间、申请人信息、资源信息、命令内容及相关操作。

审批历史

1. 在页面左上角，单击**工单**，进入工单页面。
2. 在工单页面的左侧导航中，选择**命令审批** > **审批历史**，可查看所有命令审批历史。
3. 可在我的待办历史列表中，可查看所有命令审批历史的申请时间、申请人信息、资源信息、命令内容及相关操作。

版权所有：腾讯云计算（北京）有限责任公司

脚本计划

最近更新时间：2024-09-19 15:34:42

本文档将指导您如何使用脚本计划功能。

操作场景

堡垒机提供脚本计划功能，运维用户可添加脚本计划，设置脚本计划执行规则、执行时间及相关任务信息，满足执行条件后，将执行相关脚本计划。

操作步骤

1. 登录腾讯云 堡垒机控制台 ，选择一台已部署好的堡垒机实例，在右侧操作栏，单击**管理**，进入堡垒机登录页面。
2. 使用运维用户账号登录堡垒机。

> **说明：**
> 若运维用户忘记密码，可以联系管理员进行重置，详情请参见 设置口令 。

3. 在堡垒机左上角，单击**脚本计划**，进入脚本计划页面。
4. 在脚本计划页面，单击**创建计划**。
5. 在创建计划页面，填写相关字段，单击**保存**，即可完成脚本创建。

6. 添加完成的脚本计划，将会出现在计划列表中，并可对任务进行相关操作，包括编辑、绑定资源账号、启动或停止执行任务、查看操作日志与执行日志。

Mac 系统支持工具登录

最近更新时间：2024-09-19 15:34:42

本文档将为您介绍 Mac 系统如何登录堡垒机。

操作场景

运维用户如需通过 Mac 系统登录堡垒机，可使用 Mac_SecureCRT、Mac_Terminal 或 Mac_Iterm 工具进行登录。

> **注意：**
> 仅3.0.7版本堡垒机支持使用 Mac 系统登录堡垒机功能，如需升级请 提交工单 联系我们。

操作步骤

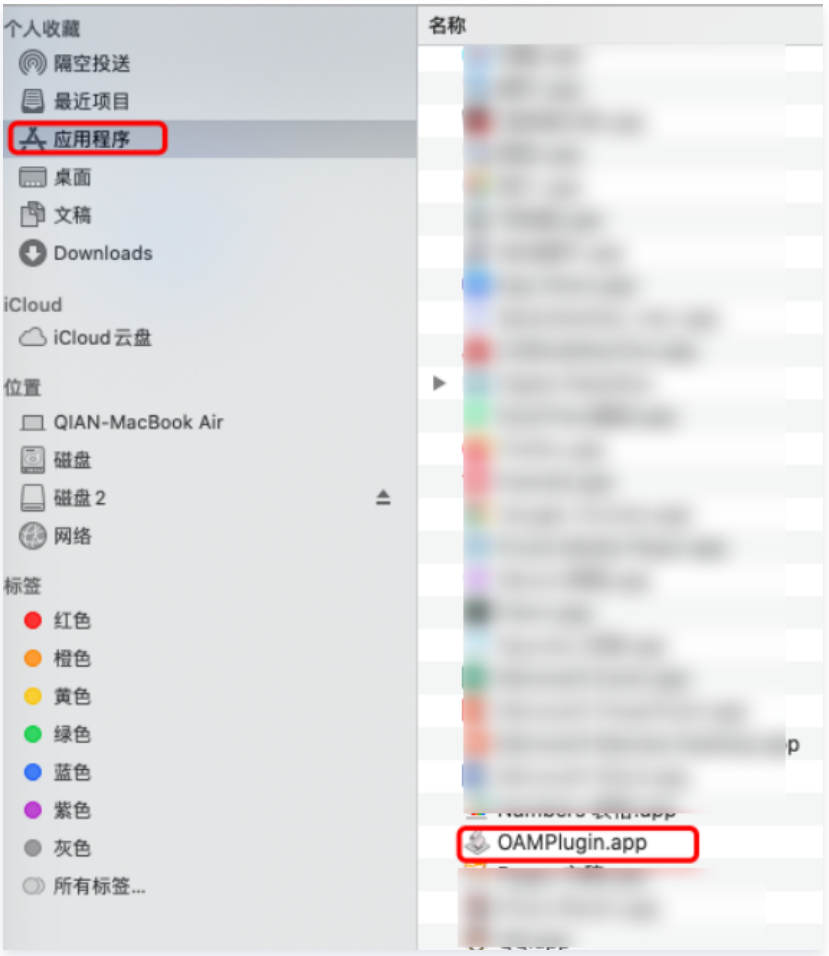
步骤1：下载并运行控件

1. 登录腾讯云 堡垒机控制台 ，选择一台已部署好的堡垒机实例，在右侧操作栏，单击**管理**，进入堡垒机登录页面。
2. 使用运维用户账号登录堡垒机。

> **说明**
> 若运维用户忘记密码，可以联系管理员进行重置，详情请参见 设置口令 。

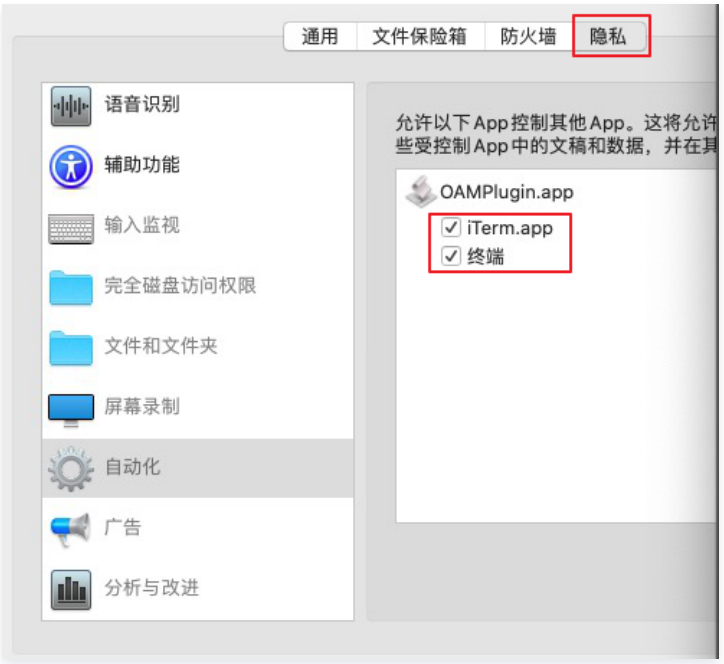
3. 单击 ，进入套件中心，下载 macos 控件包。

4. 将 OAMPlugin.app 程序移动到 macos 应用程序文件夹中，并运行一次。



5. （可选）若出现无法打开 OAMPlugin.app 问题：

需到隐私中进行设置，允许控制 App。



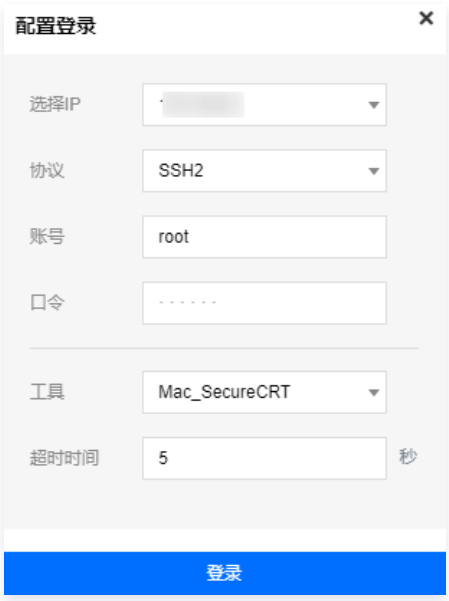
步骤2：使用 Mac_SecureCRT、Mac_Terminal 、Mac_Iterm 登录

1. 登录腾讯云 堡垒机控制台 。
2. 使用运维用户账号登录堡垒机。

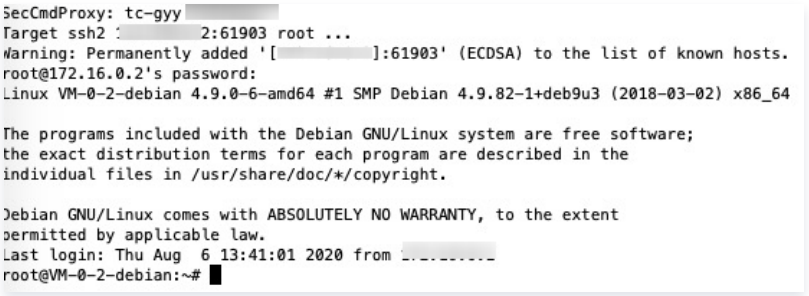
> **说明**
> 若运维用户忘记密码，可以联系管理员进行重置，详情请参见 设置口令 。

3. 单击**授权列表**，进入资源列表页。
4. 找到您需要登录的 Linux 资源，在其右侧单击**登录**，在弹出的窗口中，进行登录配置。

5. 在配置登录页面，根据需求填写相关字段，进行登录。
   - **使用 Mac_SecureCRT 登录**
     选择 IP 、协议、输入账号、口令并选择 Mac_SecureCRT 工具，单击**登录**。



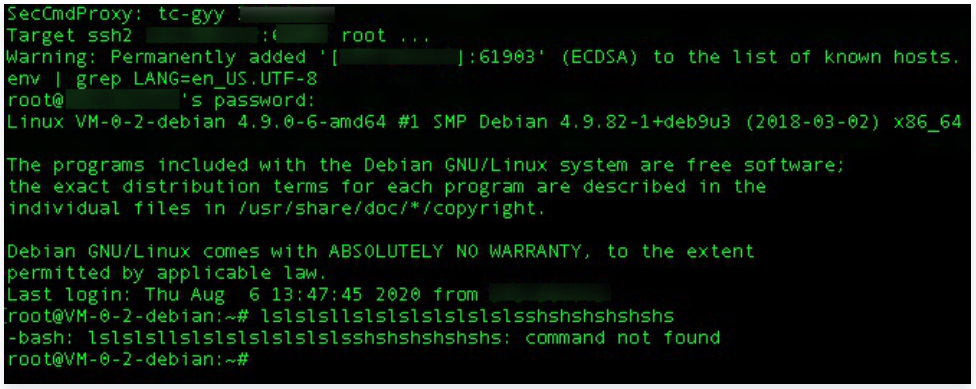
成功登录系统，如下图所示：



- **使用 Mac_Terminal 登录**

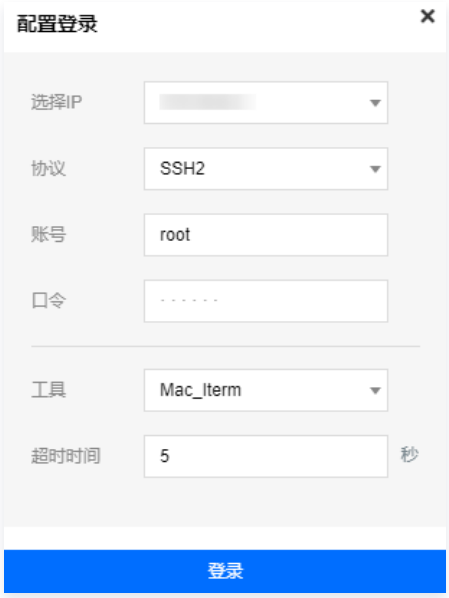
  选择 IP 、协议、输入账号、口令并选择 Mac_Terminal 工具，单击登录。

成功登录系统，如下图所示：

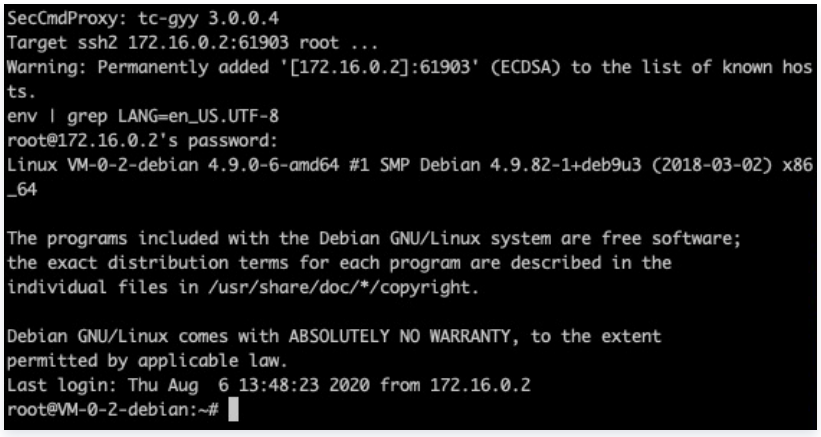


- **使用 Mac_Iterm 登录**

  选择 IP 、协议、输入账号、口令并选择 Mac_Iterm 工具，单击登录。



成功登录系统，如下图所示：



实践教程
删库等高危命令阻断

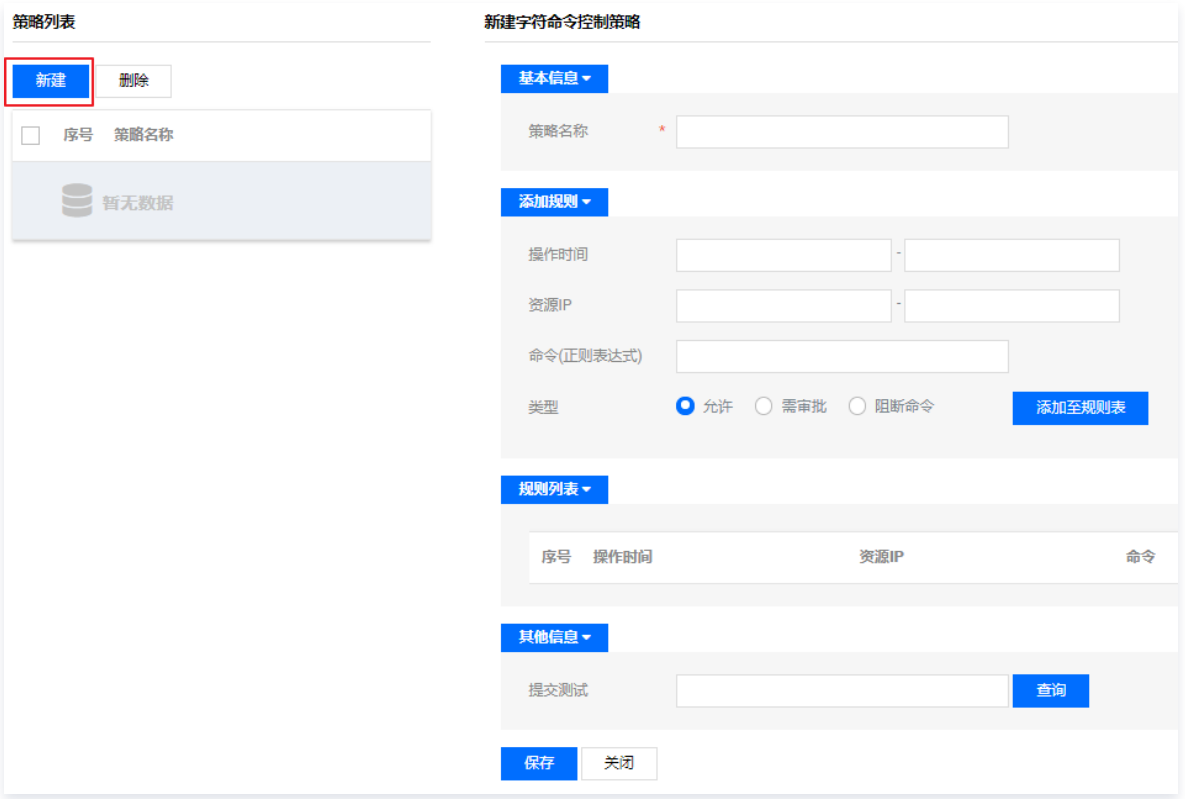
最近更新时间：2024-09-19 15:34:42

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。

配置应用发布管理数据库

最近更新时间：2024-08-22 22:04:21

本文档将指导您配置应用发布管理数据库。

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。

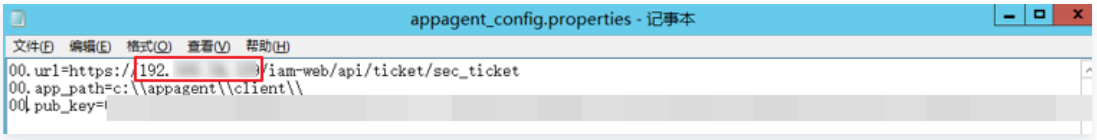
5.2 在资源类型配置页面的左侧导航中，单击**数据库**，选择已添加的数据库资源版本，绑定相应的驱动，并单击右侧扩展登录按钮。

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。

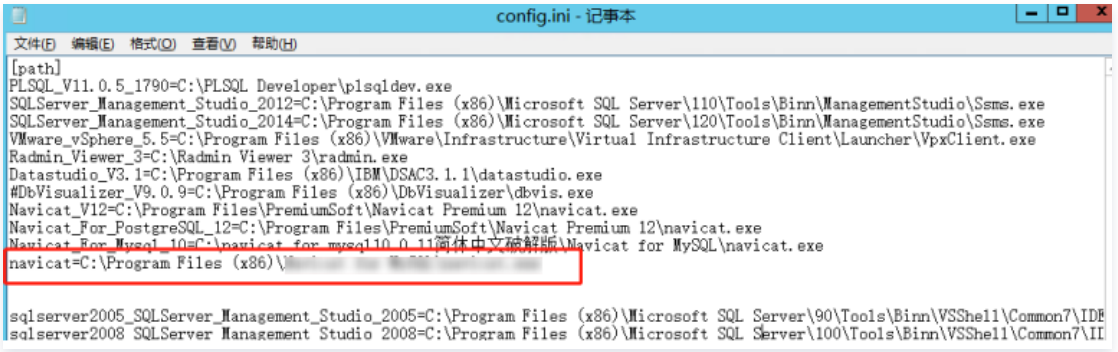
> **说明**
> 堡垒机已默认配置应用发布工具，若有特殊需求可自行配置。

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。

服务器真实密码隐藏

最近更新时间：2024-09-19 15:34:42

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。

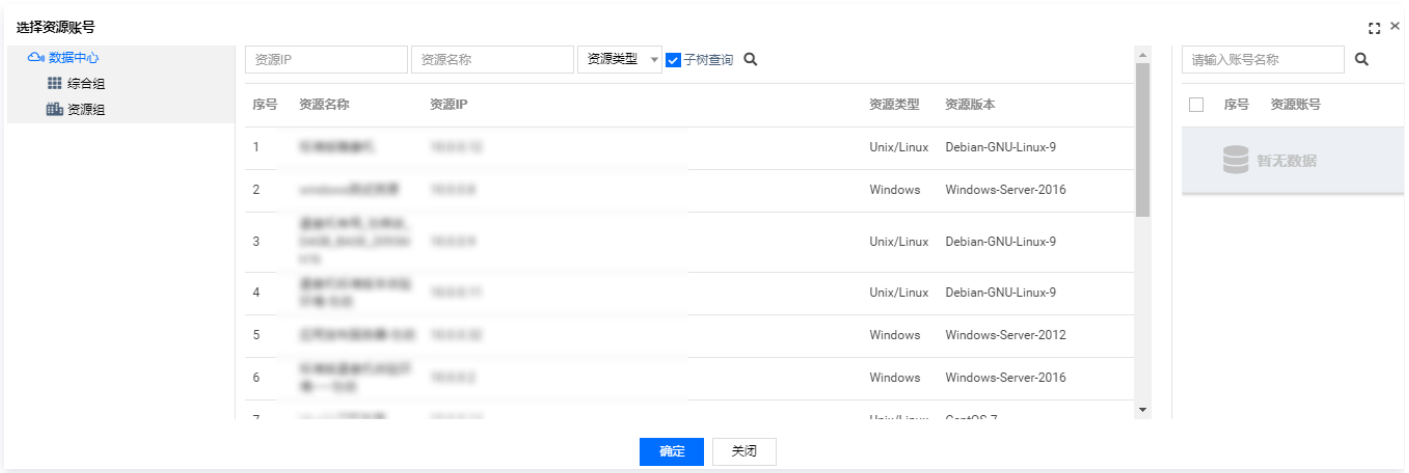
步骤1：添加任务

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。

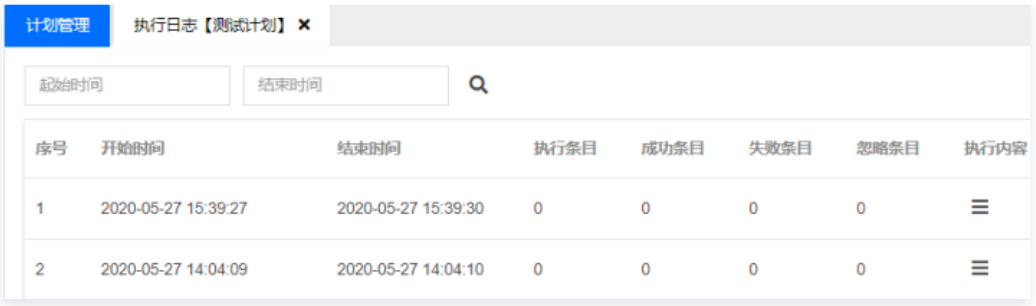
3. 在操作日志页面，您可查看该计划的操作记录日志。

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。



安全事故事后追溯

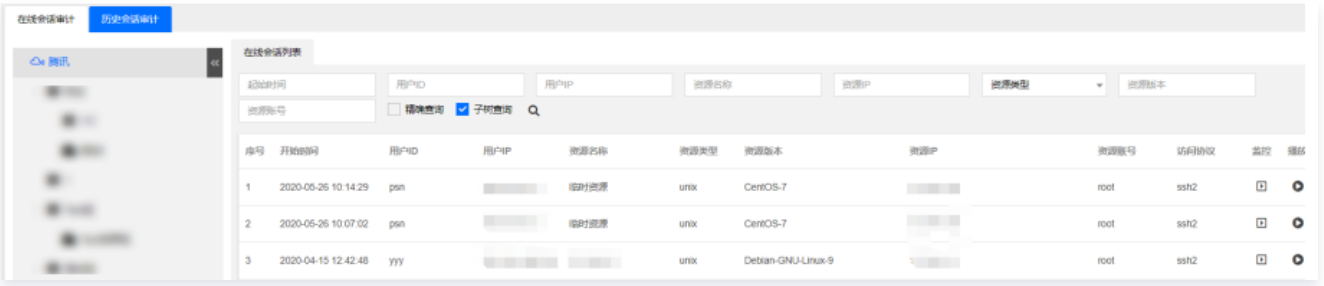
最近更新时间：2024-09-19 15:34:42

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

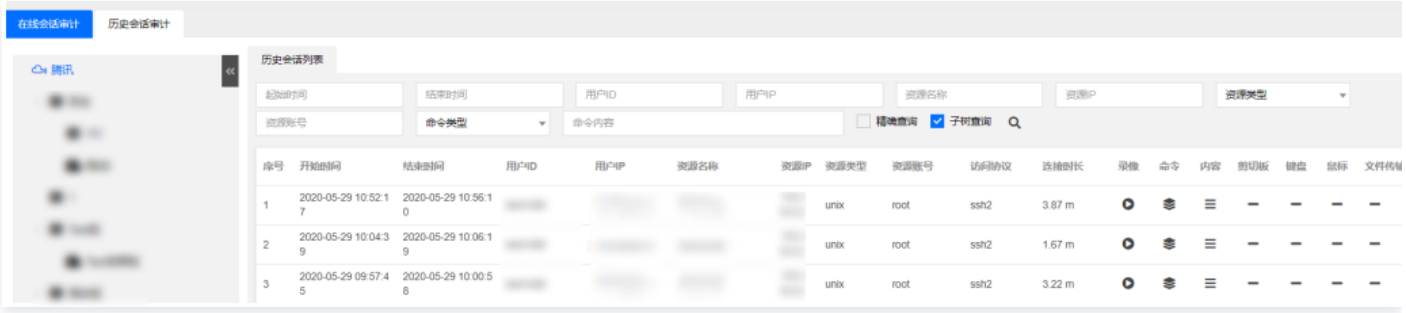
1. 在浏览器输入堡垒机 IP 地址，并输入账号和口令登录堡垒机。
2. 在左上角单击**审计平台**，进入审计平台，单击**操作行为审计**，进入操作行为审计页面。
3. 单击**在线会话审计**，进入在线会话查看页面。可以查看在线会话相关信息，例如开始时间、用户ID、资源名称、资源类型、资源登录账号、访问协议、监控、播放录像等内容。



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。



等保实践教程

最近更新时间：2024-09-19 15:34:42

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

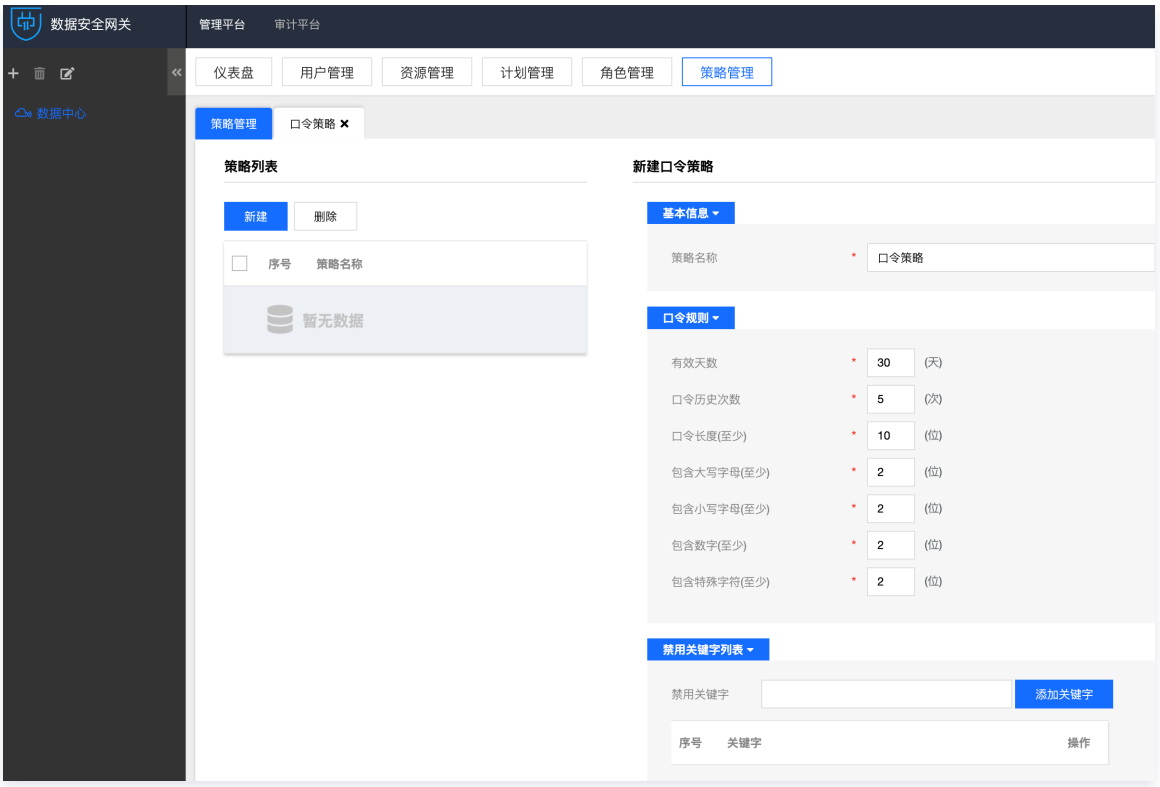
  1.1 使用管理员账号登录堡垒机，单击**用户管理**，进入用户页面。

  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。

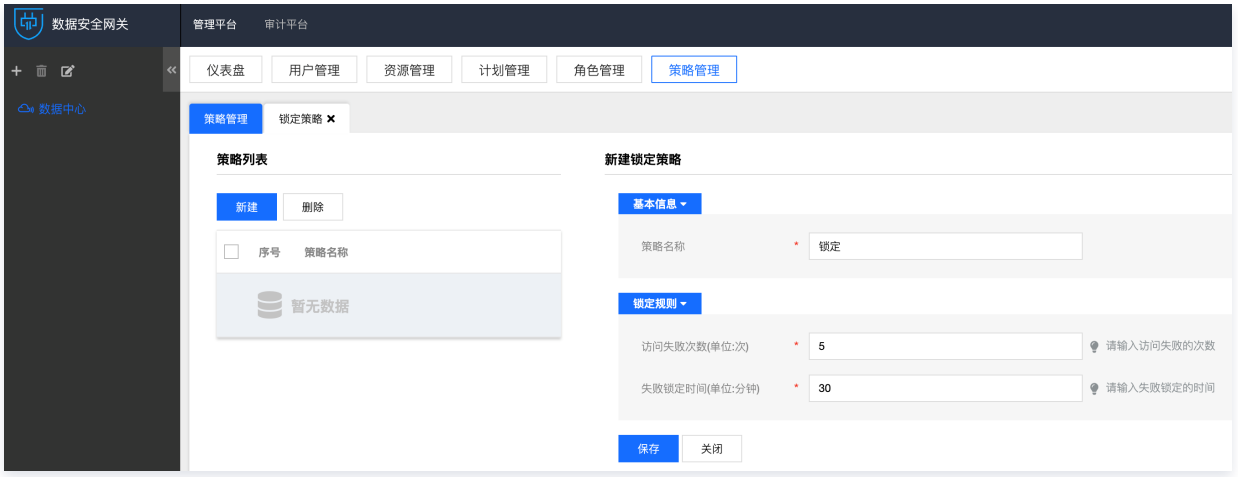


1.3 单击**用户管理**，选择一个用户，单击**编辑**，进入编辑页面之后，单击**设置策略**，设置口令策略。

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。

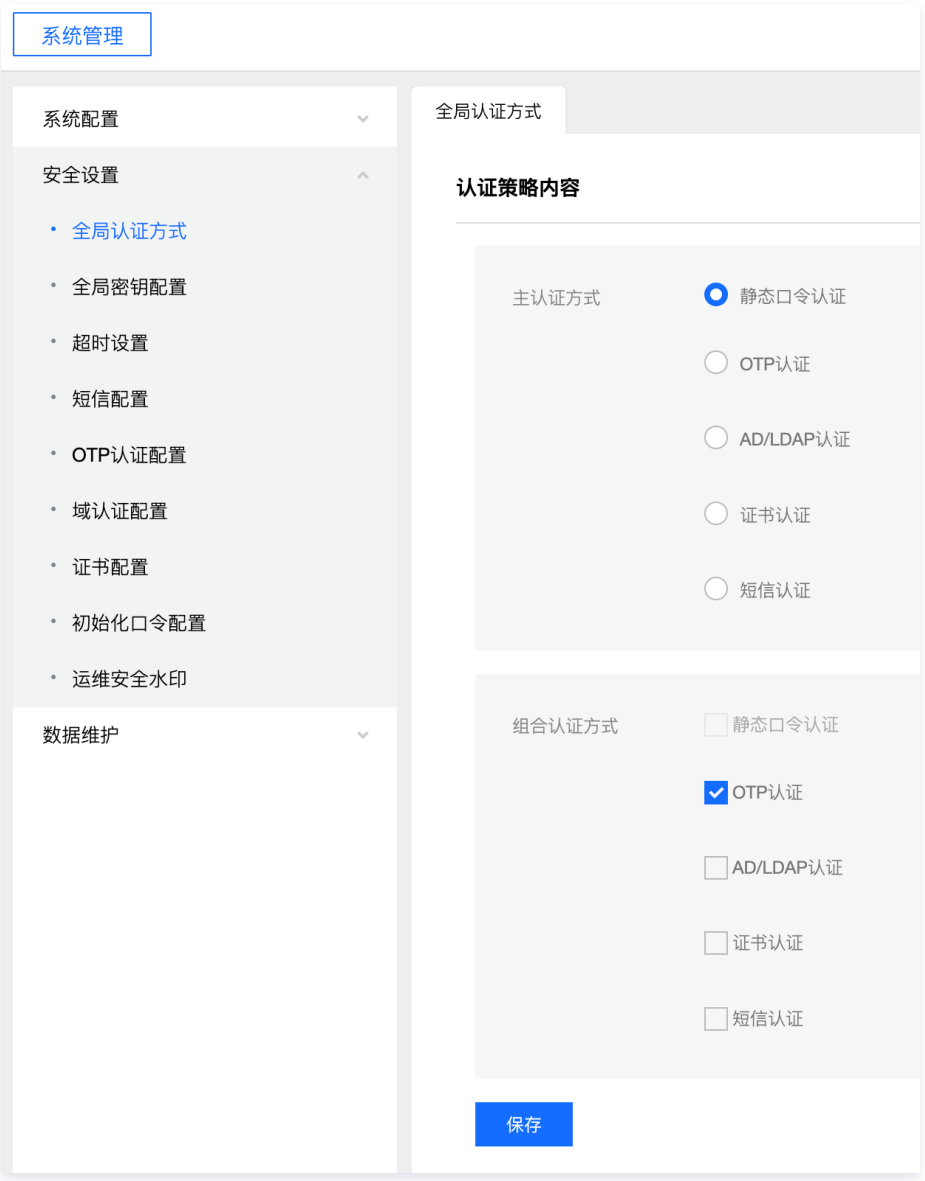
本条款主要考察：是否采用加密的协议进行远程管理。

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

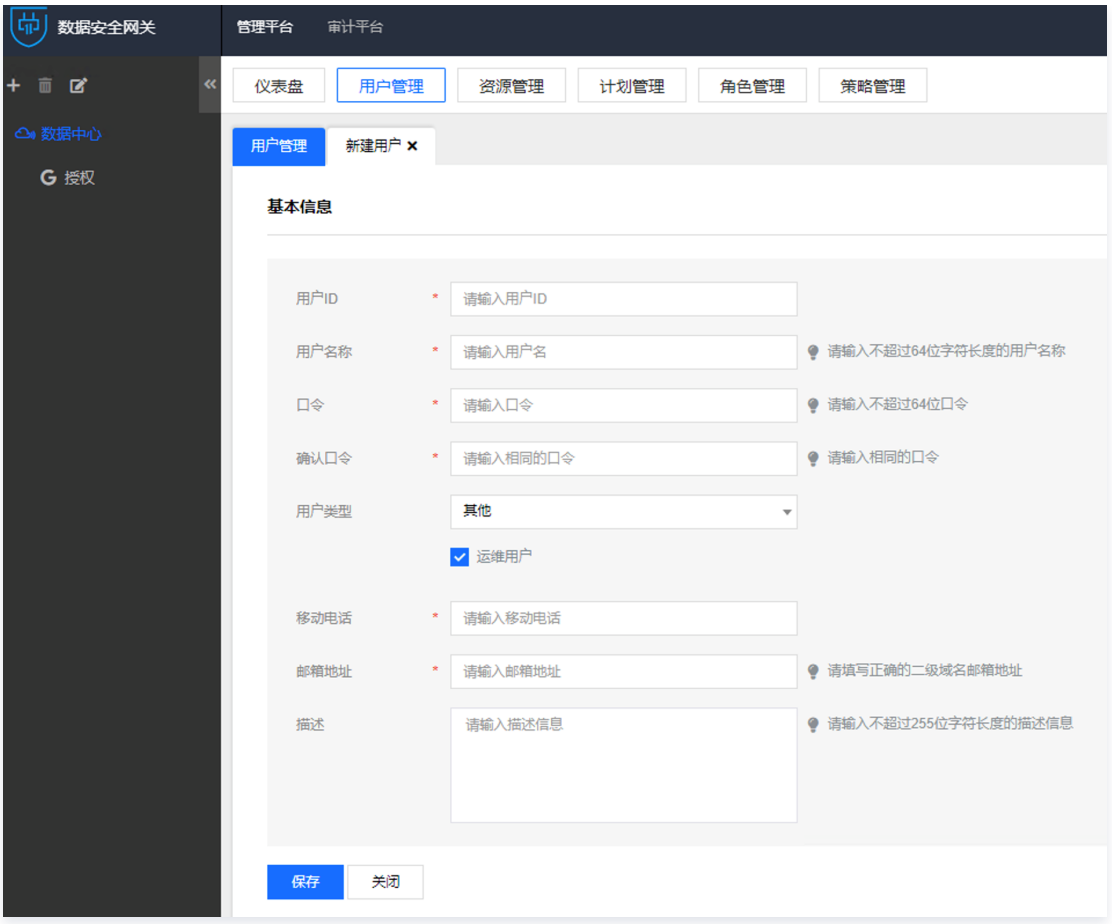
  1.1 使用管理员账号登录堡垒机，单击**用户管理**，进入用户页面。

  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。

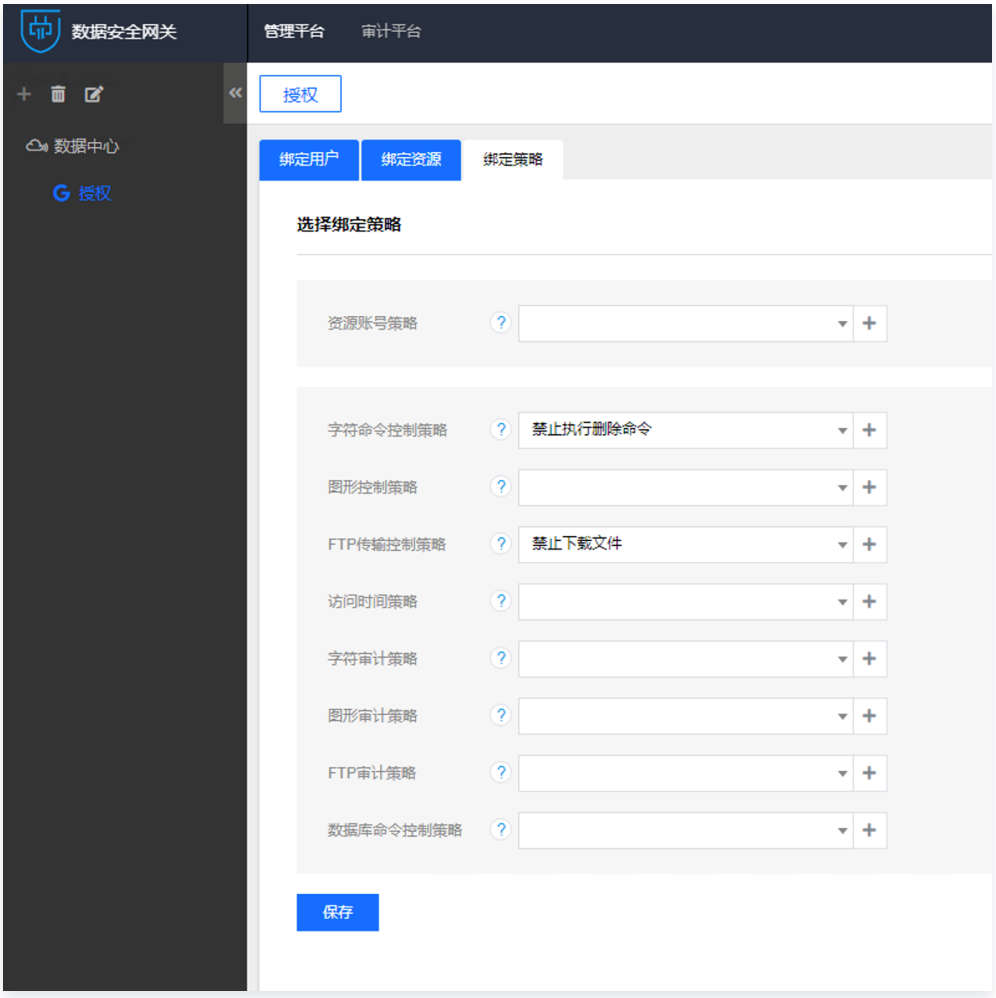
1. 使用管理员账号登录堡垒机，单击**用户管理**，进入用户页面。
2. 在用户页面，单击**编辑** > **高级选项**，查看一个过期用户的用户信息，确认用户已过有效期。

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。

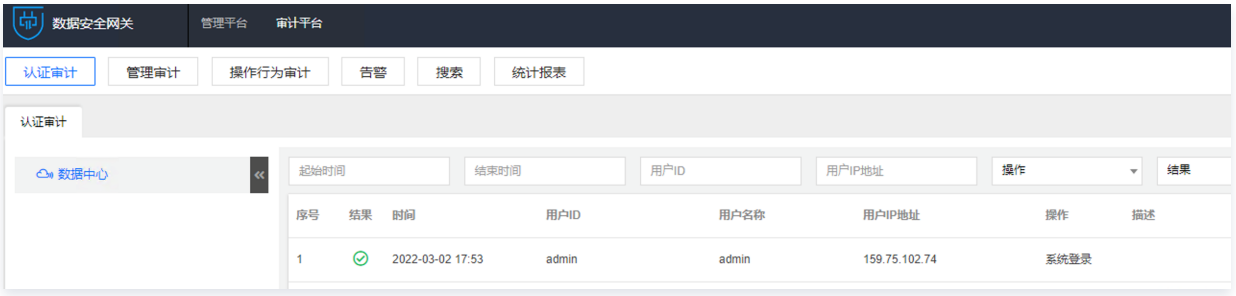
使用管理员账号登录堡垒机，选择一个岗位授权，可查看岗位授权绑定的用户、资源，证明可以配置访问控制策略。

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。

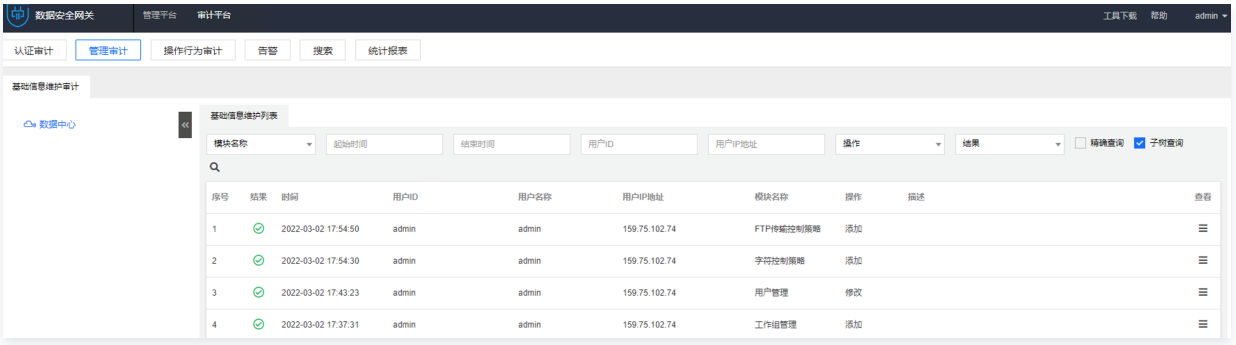
1. 使用管理员账号登录堡垒机，单击**审计平台**，进入审计页面。
2. 在会话审计页面，可查看认证、管理和操作行为的审计信息。



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。



版权所有：腾讯云计算（北京）有限责任公司

常见问题
购买部署相关

最近更新时间：2024-09-19 15:34:42

应该如何选择堡垒机的规格型号?

选购堡垒机时，一般以您云上资源节点数作为依据，一台云服务器均算作一个单独节点。您在采购前可简单统计云服务器实例数，以选择合适您环境的规格型号。另外，数盾堡垒机暂不支持动态扩容，如果您后续有增加云上资源的计划，建议您提前购买规格较高的型号。

在选购堡垒机时，应将其部署在哪个地域?

堡垒机必须与所防护的域上资源网络可达，建议最好将堡垒机与所防护的域上资源部署在同一个 VPC 中。如果需要管理跨 VPC 资源，需要将堡垒机所在的 VPC 与所要管理的资源所在的 VPC 打通，或为每个 VPC 购买一套堡垒机实例 。

购买时为何需要输入 SecurityID 与 SecurityKey?

只有知悉您的 SecurityID 与 SecurityKey 才能够将堡垒机部署到您的 VPC 中。Security 信息本身用于授权给相关业务方用于操作，授权动作不会影响您原有 VPC 资源，请正常授权。

> **说明：**
> 关于 SecurityID 与 SecurityKey 详细介绍可参考：主账号访问密钥管理 和 子账号访问密钥管理 文档。

如何确保所有的运维行为都已经纳入堡垒机的管理范围?

建议您在购买部署堡垒机后，将云服务器账号密码重新修改并配置到堡垒机实例中，详情请参见 控制台登录，由堡垒机统一发布资源，确保云服务器不能随意访问。

新建立的服务器无法通过数据同步功能自动同步至堡垒机如何处理?

请检查您新建立的服务器是否有放通安全组 ICMP 协议，若未放通请参见 创建安全组 文档进行放通，放通 ICMP 协议后，可以实现自动同步。

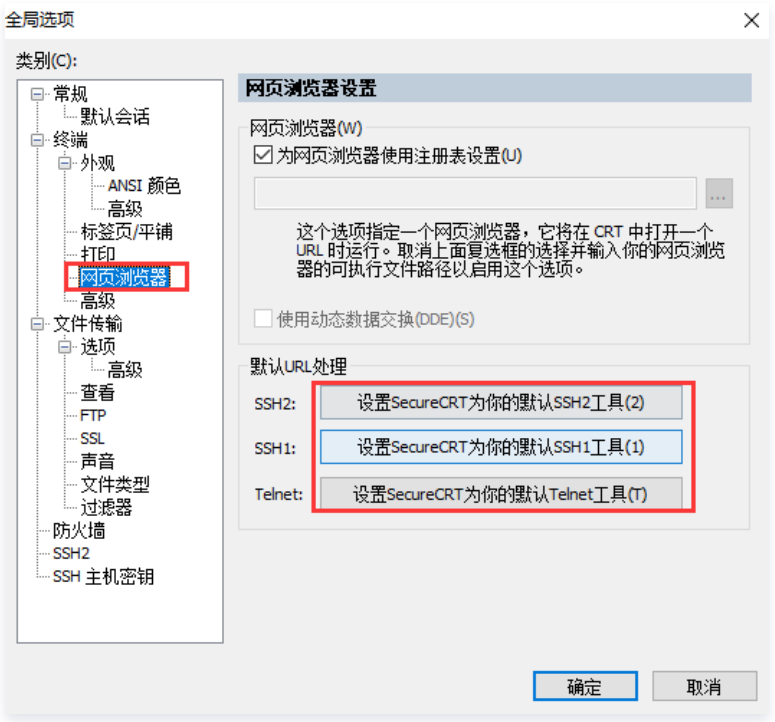
版权所有：腾讯云计算（北京）有限责任公司

运维相关

最近更新时间：2025-01-16 21:01:22

如何使用 SecureCRT 进行单点登录?

1. 打开 SecureCRT。
2. 单击**选项** > **全局选项**。
3. 单击**终端** > **网页浏览器**，进入网页浏览器设置页面。
4. 将 SSH2，SSH1 和 Telnet 选项，设置为 “设置 SecureCRT 为你的默认xxx工具”。

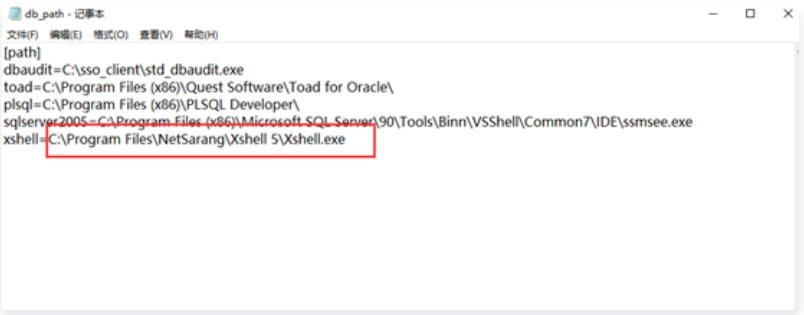


5. 单击**确定**，完成设置。
6. 关闭 SecureCRT。
7. 登录 堡垒机控制台，使用运维账号登录堡垒机。
8. 当登录 Linux 资源时，连接工具选择 SecureCRT 登录即可，详情请参见 使用 XShell/SecureCRT 登录。

如何使用 Xshell 进行单点登录?

1. 安装 Xshell 工具。
2. 登录 堡垒机控制台，并使用运维账号登录堡垒机。
3. 选择**我的管理** > **控件下载**，进入控件下载页面，
4. 单击**单点登录工具（标准）**，下载控件并完成安装。
5. 控件安装之后，进入到控件安装路径下（默认安装路径为：C:\sso_client）。

6. 找到配置文件 db_path，将之前安装的 Xshell 安装路径复制到文件 `xshell=` 后，如下图所示。

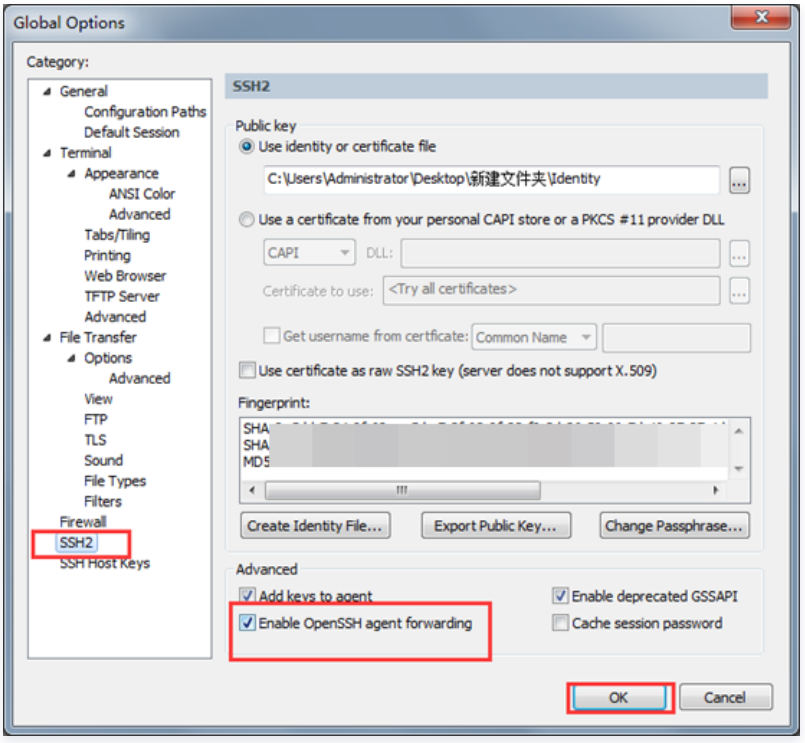


7. 完成后保存配置文件。
8. 回到 堡垒机控制台 并使用运维账号登录堡垒机。
9. 当登录 Linux 资源时，连接工具选择 Xshell 登录即可，详情请参见 使用 XShell/SecureCRT 登录。

如何通过 SecureCRT 使用 ssh key 实现单点登录服务器?

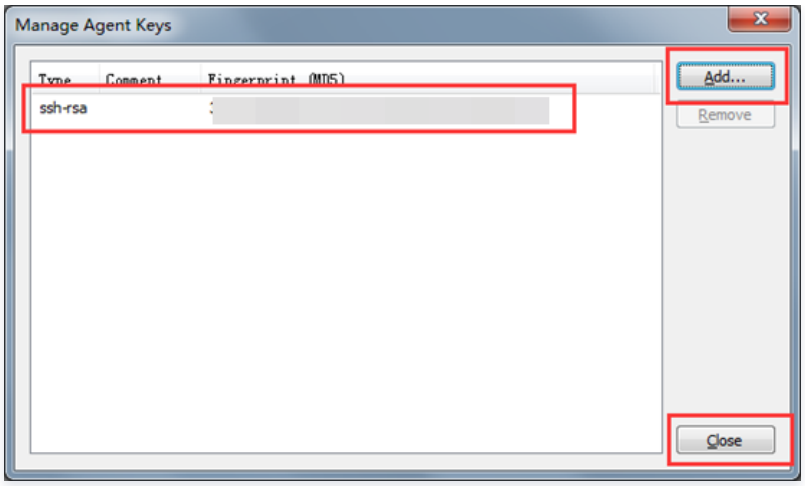
> **说明：**
> - 堡垒机无需进行配置。
> - 工具可随使用习惯灵活配置。以下举例为 SecureCRT 8.1.0 版本配置 key 单点登录。

1. 打开 SecureCRT 工具，选择 **Options** > **Global Options** > **SSH2**，将 Enable OpenSSHell agent forwarding（是否允许配置 SSH 工具进行密钥转发）选项勾选上。



2. 选择 **Tools** > **Manage Agent Keys**，将私钥文件加入到 Agent 服务中，即可生效进行目标设备的单点登录。

> **说明：**
> 在 SecureCRT 工具的 Manage Agent Keys 组件中添加私钥文件，关闭 SecureCRT 工具后私钥文件将失效，每次单点登录前，需打开 SecureCRT 工具，手动添加私钥文件并保持 SecureCRT 工具打开。



3. 登录 堡垒机控制台 ，并使用运维账号登录堡垒机，选择对应 key 服务器进行单点登录。

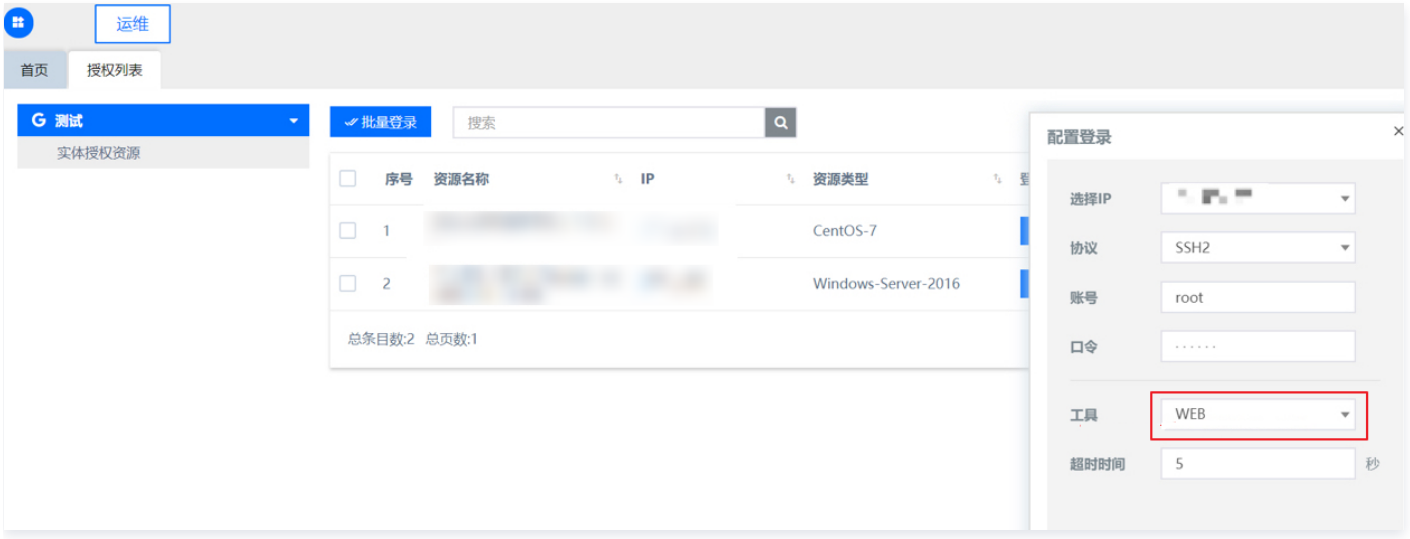
MAC、Linux 终端如何使用堡垒机?

管理端

堡垒机可以完全支持 MAC 和 Linux 的网页操作，建议使用 Chrome 浏览器。

运维端

堡垒机支持在 MAC 和 Linux 终端下通过 Web 方式（建议使用 Chrome 浏览器），进行资源单点登录与文件传输。登录 堡垒机控制台，并使用运维账号登录堡垒机后，在工具栏选择 Web，即可登录资源。



当系统提示运维用户的账户密码已过期，要如何处理?

若系统提示运维用户的账户密码已过期，可以联系管理员进行密码重置，详情可参见 设置口令。

若运维用户在堡垒机的套件中心，下载 macos 控件包后，无法打开要如何处理?

若 OAMPlugin.app 无法打开，可能是文件权限被限制，可在终端电脑的命令行中执行 `chmod +x /Applications/OAMPlugin.app/Contents/MacOS/applet` 命令。

端口相关

最近更新时间：2024-09-19 15:34:42

堡垒机入站、从堡垒机到受管控机器，需要分别开放什么端口?

当用户操作堡垒机出现网络问题时，例如，登录不了堡垒机，可参照下面入站规则和受管控机器提供的端口，检查对应端口号是否有开通。

入站规则

从客户端到堡垒机，需要开放的端口如下表所示：

端口号	说明	协议	备注	是否必开
61903	SSH/SFTP/FTP/文件共享	TCP	字符协议及文件传输访问端口	是
443	HTTPS	TCP	Web 管理端口	是
3392	RDP2	TCP	RDP2 单点登录和审计播放	是
10050	-	TCP	字符审计录像播放	是
11020	-	TCP	认证端口	是
8443	HTTPS	TCP	证书认证登录	否
3390	VNC	TCP	连接端口	否

说明：
堡垒机安全组的出站规则已自动配置，一般情况下，无需再对出站规则进行其他配置。

受管控机器

堡垒机管控的后端资源服务器的安全组里放开如下端口（**可根据自身服务器端口开启**）。

端口号	说明
20	FTP/SFTP（主动模式）
21	FTP/SFTP（主动/被动模式）
22	SSH
23	Telnet
389	AD LDAP
3389	RDP

说明：
对于 xwindow、vnc 协议，其端口采用实际使用的端口。

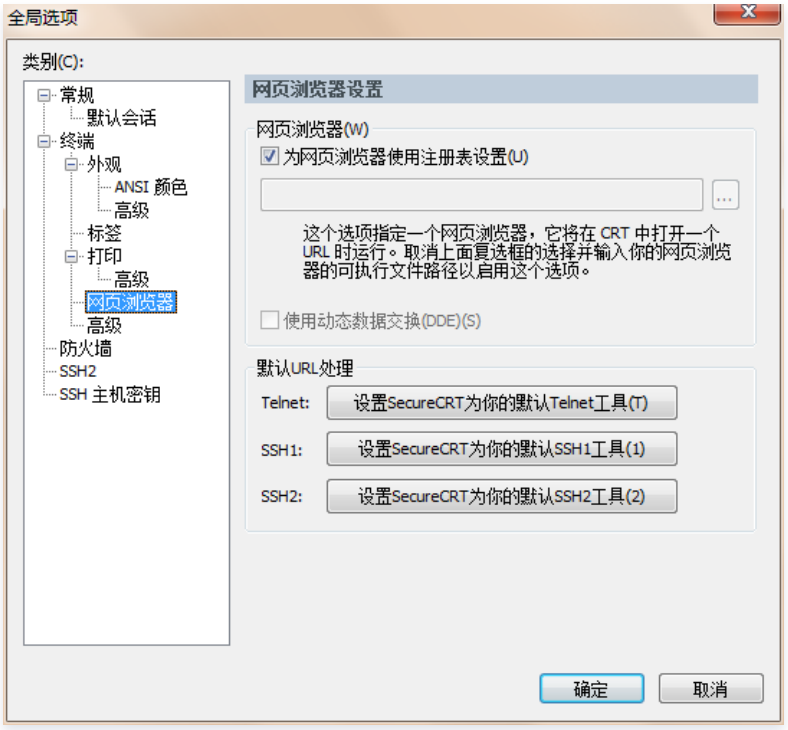
单点登录相关

最近更新时间：2024-09-19 15:34:42

如何解决单点登录时，未能正常启动 SecureCRT 等工具?

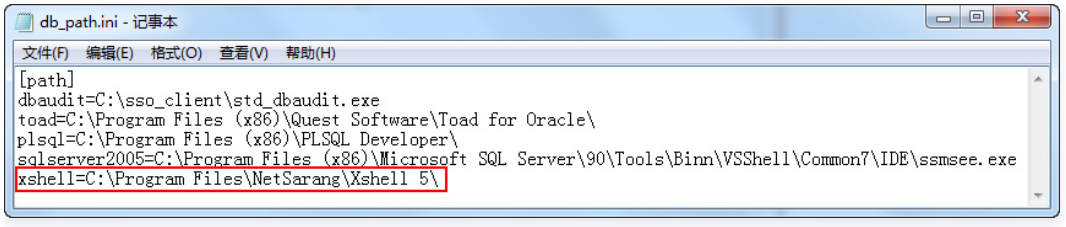
问题现象：单点登录时，单击连接工具，页面没反应，鼠标显示加载。
产生原因：单点登录工具没安装（例如 SecureCRT，VNC 等）。
解决方案：安装相应的登录工具，个别需要绑定。

- 例如 SecureCRT，选择**选项** > **全局选项** > **网页浏览器**，单击**设置...为默认工具**。



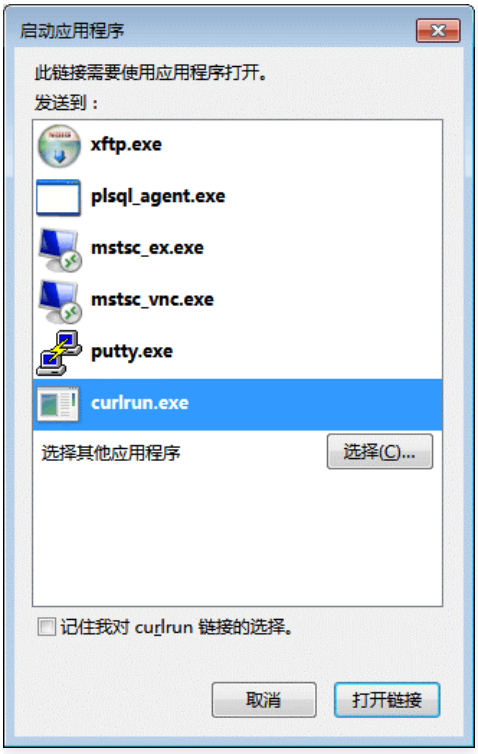
如何解决堡垒机调用 Xshell 失败?

解决方案：需要在 sso 控件安装目录（C:\sso_client）下的 db_path.ini 文件里，配置 Xshell 的安装路径。



使用火狐、谷歌浏览器单点登录，工具如何选择配置?

解决方案：单点登录单击连接时，会提示选择连接打开工具，需选择 curlrun.exe，不能选择 PuTTY 或者其他工具。


启动应用程序
此链接需要使用应用程序打开。
发送到：
xftp.exe
plsql_agent.exe
mstsc_ex.exe
mstsc_vnc.exe
putty.exe
curlrun.exe
选择其他应用程序
选择(C)...
记住我对 curlrun 链接的选择。
取消
打开链接