堡垒机（BH）

产品文档

腾讯云TCE

文档目录

产品介绍

最近更新时间: 2024-10-17 17:10:00

1. 前所未有的运维挑战

- 随着信息技术的不断发展和信息化建设的不断进步，业务应用、办公系统、商务平台不断推出和投入运行，信息系统在企业的运营中全面渗透。电信行业、财政、税务、公安、金融、电力、石油、大中型企业和门户网站，使用数量众多的网络设备、服务器主机来提供基础网络服务、运行关键业务，提供电子商务、数据库应用、ERP和协同工作群件等服务。由于设备和服务器众多，系统管理员压力太大等因素，越权访问、误操作、滥用、恶意破坏等情况时有发生，这严重影响企业的经济运行效能，并对企业声誉造成重大影响。另外黑客的恶意访问也有可能获取系统权限，闯入部门或企业内部网络，造成不可估量的损失。如何提高系统运维管理水平，跟踪服务器上用户的操作行为，防止黑客的入侵和破坏，提供控制和审计依据，降低运维成本，满足相关标准要求，越来越成为企业关心的问题。

- 目前，面对日趋复杂的IT系统，不同背景的运维人员已给企业信息系统安全运行带来较大潜在风险，主要表现在：

1.1 账号缺乏统一管理，隐藏着巨大的风险

- 多个用户混用同一个账号
  这种情况主要出现在同一工作组中，由于工作需要，同时系统管理账号唯一，因此只能多用户共享同一账号。不仅在发生安全事故时难以定位账号的实际使用者和责任人，而且无法对账号的使用范围进行有效控制，存在较大安全隐患。

- 一个用户使用多个账号
  目前，一个维护人员使用多个账号是较为普遍的情况，用户需要记忆多套口令同时在多套主机系统、网络设备之间切换。如果设备数量达到几十甚至上百台时，维护人员进行一项简单的配置需要分别逐一登录相关设备，其工作量和复杂度成倍增加，直接导致的后果是工作效率低下、管理繁琐甚至出现误操作，影响系统正常运行。

1.2 粗放式权限管理，安全性难以保证

- 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。管理人员的权限大多是粗放式管理，由于缺少统一的运维操作授权策略，授权粒度粗，无法基于最小权限分配原则管理用户权限，难以与业务管理要求相协调。因此，出现运维人员权限过大、内部操作权限滥用等诸多问题，如果不及时解决，信息系统的安全性难以充分保证。

1.3 设备自身日志粒度粗，难以有效定位安全事件

- 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；因此，难以通过系统自身审计及时发现违规操作行为和追查取证。

1.4 第三方代维人员带来安全隐患

- 目前，很多大型企业，包括一些政府机构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。因此，需要通过严格的权限控制和操作行为审计，加强对代维人员的行为管理，从而达到消隐患、避风险的目的。

1.5 面临法规遵从的压力

- 为加强信息系统风险管理，政府、金融、运营商等陆续发布信息系统管理规范和要求，如“信息系统等级保护”、“商业银行信息科技风险管理指引”、“企业内部控制基本规范”等均要求采取信息系统风险内控与审计，但其缺乏有效的技术手段。
- 上述风险带来的运维安全风险和审计监管问题，已经成为企业信息系统安全运行的严重隐患。企业IT运维安全管理的变革已刻不容缓！

2. 产品概述

- 数据安全网关是集用户（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。该系统能够为企业提供集中的管理平台，减少系统维护工作；能够为企业提供全面的用户和资源管理，减少企业的维护成本；能够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，全面保障系统资源的安全；能够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。

- 数据安全网关采用层次化、模块化的设计，产品整体架构包括：资源层、接口管理层、核心服务层和统一展示层。
  - 资源层：负责提供各种类型资源的资源管理交互。
  - 接口管理层： 主要功能是实现核心层与外部产品、用户资源系统之间的数据交互，包括账号类、认证类、授权类和审计类四个方面的接口。其中账号/角色管理接口实现资源从账号的收集和同步管理，认证接口实现与第三方强身份认证产品的联动和主账号认证，访问控制策略接口实现访问控制策略的下发，审计接口能接收外部系统产生的各类日志。通过数据接口层完成与各种应用系统的相关接口通信。
  - 核心服务层：完成系统各功能模块的业务处理，包括身份管理，行为管理，审计管理以及协议 代理等服务，每个模块再细分若干子模块完成各自的管理功能。核心层具体的功能模块如下：
    - 账号管理
    - 授权管理
    - 认证管理
    - 审计管理

- 统一展示层：负责用户交互部分的展现，一方面对用户身份的认证，同时显示信息给系统操作人员，包括操作人员的可访问资源展现及自服务展现；另一方面接受管理人员的管理配置和审计人员的审计查看，将管理人员和审计人员的输入传递到核心服务层处理。

3. 产品特点

3.1 丰富的部署方式，架构部署灵活

- HA双机部署：一般HA双机基于监测网络存活状态进行切换，无法做到根据系统服务状态进行切换， 数据安全网关真正实现基于硬件和应用服务状态进行监控切换，从而为客户提供不间断的服务，同时采用双写技术，保证客户数据安全，确保高可靠性。
- 集群部署：对于大规模资产高并发访问且运维不可中断性质的客户，支持三台或三台以上的集群部署模式，确保运维访问能够均衡的由各个堡垒处理。
- 分布式部署：实现公司总部与各分公司之间，组织机构分散而需要统一集中管理的问题。

3.2 多元化的认证方法，支持组合认证

- 自身提供了证书认证、手机动态令牌、MAC地址认证、AD域认证等服务，也可与第三方CA、动态令牌等进行结合。支持任意组合认证，提高访问的安全性。

3.3 强大的资源管理能力，资源数据直观展现

- 资源数量统计：支持柱形图方式查看系统中不同资源所占比例。
- 资源类型：支持资源类型丰富，unix资源、网络资源、windows资源、数据库资源、C/S资源、B/S资源。
- 资源驱动管理：支持按资源类型上传资源管理驱动程序，可使资源的管理更具有针对性。
- 应用发布单独管理：支持应用发布代填驱动自定义上传，针对不同应用资源，采用相对应的代填脚本。

3.4用户账号及资源账号的全生命周期管理

- 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。
- 账号同步：将用户账号数据以excel方式导入运维审计与管理系统，实现数据统一，无需重复创建数据。
- 从账号管理：支持资源从账号的管理，系统具有各种资源类型驱动器能够将资源上的账号进行自动收集、推送、抽取、同步及属性的变更等。
- 支持手动登录账号、口令自动添加功能，操作员单点登录时，手动输入的从账号、口令，系统会自动添加到该资源账号列表中，避免重复添加。

3.5 灵活的授权管理功能，基于资源扩展属性的动态授权

- 角色管理：系统内部管理功能权限支持自定义角色。系统内置运维、管理、审计三大角色，角色可按照组节点进行定义，系统内置运维、管理、审计三大角色，从而实现分层分级管理模式。

- 岗位授权：资源授权模式基于岗位授权，岗位授权概念十分灵活，建立岗位授权后，岗位授权上可绑定已有用户及资源、账号，也可直接在岗位授权上新建用户及资源、账号，这样授权可迁移、授权粒度更细；并可针对岗位授权设置相关安全安全策略。
- 资源自动授权：支持资源按筛选规则定义资源属性，按照资源属性自动完成授权。
  - 资源账号批量授权：支持设置资源账号组策略，将资源账号组策略绑定至岗位授权后，单点登录时系统会自动从资源账号组中添加的账号集合中筛选出资源实际添加的账号并可进行登录代填口令。

3.6 基于HTML5技术的单点登录，多浏览器支持

- 支持快速登录功能：系统可将运维人员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。
  - 支持RDP、SSH1、SSH2、TELNET、FTP、SFTP、VNC、XWINDOW等协议。
- 支持 en、su、super用户角色自动切换操作并代填密码

3.7 强大的审计管理，基于WEB的审计回放与监控，无需安装插件

- 图形资源访问时，支持鼠标、键盘、剪切板、文件传输记录，并且对图形资源的审计回放时，可以从某个键盘、剪切板、文件传输记录的指定位置开始回放。
- 支持Windows图形审计的监控，管理员可以随时查看运维人员的操作，并且可以发送告警信息进行会话锁定和解锁。
- 图形审计支持画质如灰度、灰度低级的设置，帧间隔，压缩比等设置，可以大大缩减图形审计产生录像文件的大小，每十分钟真彩模式下的审计录像大小为10M左右。
  - 采用ES搜索引擎，审计数据查询速度更快，结果更准确。
- 所有审计回放及监控操作，均基于web实现，无需再安装客户端插件。
- 支持在审计录像回放中加入水印等安全功能，有效保障企业数据安全。

3.8 访问零信任

- 基于安全零信任策略和架构，遵循最小最少权限原则，构建基于身份的可 信赖计算机制，保障用户对企业资产的安全运维。对用户的异常行为，支持对接腾讯云金融专区 AI 模块进行判定，不放过任何可疑行为。

3.9 直观的可视化页面展现

- 支持对在线用户、在线主机、计划任务、运维数据、实时监控等统计数据进行页面展示；
- 支持对策略分布、威胁分布、系统运行状态等数据进行图形展示；
  - 支持对主机运维、计划任务、用户运维等数据TOP展示。

3.10 良好的扩展性及定制化能力,扩展灵活，定制安全

- 支持第三方应用程序获取密码接口
- 支持定制开发：平台自身根据技术发展和市场需求不断变化而变化着，保证充分满足市场及用户需求。

4 产品主要功能模块

- 部署方式 数据安全网关采用物理旁路单臂部署；不改变现有网络结构，不改变运维人员的运维习惯；
- 组织结构 基于综合、资源、岗位授权方式进行分层管理；
- 用户管理 提供用户帐号的集中管理，用户的树形分组展示及导入导出。
- 提供基于用户的配置口令、访问锁定、访问时间等安全策略。
- 资源管理 资源即我们的IT资产，比如服务器，网络设备，应用系统，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。
- 从账号管理（设备账号） 从账号即资源设备账号， 数据安全网关提供了账号管理，自动改密，密码拨测，账号导出等一系列从账号管理功能。
- 授权管理 资源授权模式基于岗位授权，岗位授权上绑定用户及资源、账号，并可针对岗位授权设置相关安全策略。
- 单点登录SS0 单点登录即通过 数据安全网关作为目标资源访问的统一入口，进行目标资源的运维管理。
- 认证管理 数据安全网关自身提供证书认证服务，也可与第三方CA、动态令牌等方式进行结合。支持组合认证，提高访问的安全性。
- 安全管理 数据安全网关提供了丰富的安全策略功能，如访问时间策略、地址策略、图形策略、字符命令、FTP、口令策略、锁定策略等；
- 提供审计策略如字符、图形、FTP等相关审计策略。
- 审计管理 数据安全网关支持图形审计、字符审计、实时监控、管理审计及审计报表。
- 系统管理 该模块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，系统服务配置清除、审计日志清理、还原出厂设置，关机重启等。
- 高可用性 数据安全网关针对不同的业务场景及可靠性要求，提供了HA、集群、分布式部署方式。

5 .产品价值

5.1 有效减少信息资产的破坏和泄漏

- 随着各行各业信息化建设的完善，越来越多的企业单位将核心信息资产存放在少数几个关键业务系统上，通过使用运维审计与管理系统，能够加强对这些关键系统的访问控制与审计，从而有效地减少核心信息资产的破坏和泄漏。

5.2 满足合规性要求，顺利通过IT审计

- 目前，越来越多的单位面临一种或者几种合规性要求。比如，在美上市的中国移动集团公司及其下属分子公司就面临SOX法案的合规性要求；而商业银行则面临Basel协议的合规性要求；政府的行政事业单位或者国有企业则有遵循等级保护的合规性要求。 数据安全网关起源于国内最早的4A项目。所以能够提供一套完整的审计方案，有助于完善组织的IT内控与审计体系，从而满足各种合规性要求，并且使组织能够顺利通过IT审计。

5.3 助力企业控制运维操作风险及事后原因与责任界定

- 通常在我们的企业内部，负责运维的部门拥有目标系统或者网络设备的最高权限，因而也承担着很高的运维风险，比如误操作或者是个别人员的恶意破坏。由于目标系统不能区别不同人员使用同一个帐号进行维护操作，所以不能界定维护人员的真实身份。 数据安全网关提供基于用户及岗位的实名制访问控制与审计，不但能够有效地控制运维操作风险，还能够有效地区分不同维护人员的身份，便于事后追查原因与界定责任。

5.4 源于4A的一体化、低成本、可操作的解决方案

- 数据安全网关源于4A，所以可以说是一种一种低成本、易实施的一体化4A解决方案，涵盖了账号管理、身份认证、访问授权以及操作审计等几方面的基本功能。

快速入门

最近更新时间: 2024-10-17 17:10:00

1. 堡垒机上线配置简介

新堡垒机上线时，需要配置内容有：修改根节点，创建组织结构；添加被管服务器，添加服务器账号；添加用户，将被管服务器权限分配和用户。基本操作涉及到模块分别为：组织结构，用户管理，资源管理，配置使用后可在审计管理查看相关操作审计。 涉及到的系统功能模块简介：

- 组织结构：主要提供定义分组，方便分层分级管理
- 用户管理：主要提供堡垒机系统用户账号管理与权限分配。
- 资源管理：主要提供接入堡垒的资源（被管服务器）和资源账号（被管服务器的后台账号）管理，资源账号可支持 SSH、TELNET、FTP、SFTP、VNC、XWINDOW、WINDOWS 文件共享等协议。
- 审计查看：主要提供堡垒机登陆或操作审计，以及运维用户单点登录资源后的操作行为审计查看。

2. 管理员上线配置

2.1. 管理员登陆

堡垒机系统采用加密型的 http 方式进行访问，在浏览器地址栏中输入 http://imgcache.finance.cloud.tencent.com:80堡垒机IP即可，例如：http://imgcache.finance.cloud.tencent.com:80192.168.30.66 / 由于采用 SSL 技术，访问会出现证书错误提示，此时点击“继续浏览此网站”，输入管理员账号和密码登陆进入堡垒机。

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。

2.2. 修改根节点

首次登陆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； 操作过程：点击主菜单【数据中心】>【编辑节点】>在名称处输入“”，将根目录修改为“腾讯云金融专区”

2.3. 新建组织结构

修改完根目录后创建组织结构，以便管理堡垒里的人员资源等信息，组织结构支持多层级分类创，可按照公司组织结构或资源分组管理情况来来建设；以下为“腾讯云金融专区”的“授权组”创建。 操作过程：点击【组织结构】>【新建】>输入组织结构名称“授权组”>选择组织结构类型“岗位授权”，点击【新建】完成组织结构“授权组”的新建；

2.4. 添加资源（目标设备）

组织结构创建完成后进行资源添加，通过【资源管理】模块将需要堡垒管理的设备信息导入堡垒，该模块可对资源和资源账号以及账号登陆方式进行管理；

2.4.1. 添加资源

以下为“授权组”下手动添加设备“linux 资源1”，IP：172.16.2.28，资源账号“root”的操作步骤； 操作过程：点击【授权组】-【绑定资源】-【新建并绑定】，选择资源类型、资源版本、资源名称以及资源 IP，点击保存关闭。如果需要绑定资源账号，点击【资源管理】--选择要添加账号的资源【账号列表】--点击添加按钮，填上相应的账号信息，点击保存

2.5. 新建用户

以上步骤完成后即完成了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，完成后堡垒机上线前的配置工作就完成了。 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。 新建用户操作过程：点击【授权组】--【绑定用户】--【新建并绑定】点击【保存】完成用户创建.，

2.6. 审计查看

审计查看可分为堡垒机管理端管理操作审计和运维人员单点登录操作服务器的行为审计，步骤如下； 审计查看操作过程：点击【审计平台】，即可查看审计内容

3. 运维人员使用

在浏览器地址栏中输入http://imgcache.finance.cloud.tencent.com:80堡垒机 IP/访问堡垒机，输入用户名密码登陆。

3.1. 安装控件（安装时全部默认安装）

运维用户第一次访问堡垒机系统，需下载单点登录控件，已安装过无需再安装。 登录运维用户，点击左上角圆形的套件，然后点击下载。

3.2. 单点登录

单点登录操作过程：点击【运维】>【授权列表】>输入账号密码和选择连接方式>【登录】连接到服务器，完成单点登录。

4. 角色管理

堡垒机系统基于最小安全特权原则，将所有角色分为8个角色模块：组织管理、用户管理、资源管理、岗位管理、安全策略、审计报表、系统参数。 对用户按其职责设定角色管理权限。

> **说明：**
>
> 角色管理依托组织结构创建角色，所以创建角色前，先创建组织结构。

4.1. 角色配置

场景说明： 根据系统管理任务创建三个角色，分别为：系统管理员、审计管理员、运维人员；

- 系统管理员权限：系统平台的组织管理、用户管理、资源管理和配置管理角色权限；
- 审计管理员权限：系统平台的内部审计和运维人员登录资源操作的行为审计；
- 运维人员：只有单点登录运维资源权限，没有对系统平台的管理和审计权限。普通用户默认为“运维人员”

用户（1）角色授权为系统管理员，处理系统平台管理配置工作，用户(1)角色授权为审计管理员，负责系统平台管理操作和运维操作审计工作，并定期生成业务报表汇报领导。 配置思路： 根据场景需求，对根节点“腾讯云金融专区”创建“系统管理员”和“审计管理员”角色，普通用户默认为“运维人员”。 用户（1）授权“系统管理员”角色、用户(1)授权“审计管理员”角色。

配置方法：

4.1.1. 角色权限配置

以下为根节点“腾讯云金融专区”的角色权限创建； 操作过程：点击“腾讯云金融专区”---【角色管理】选择需要创建的角色全选,勾选对应权限>【保存】完成组织管理角色的创建，别的角色也是同样步骤创建。

4.1.2. 用户角色授权

根据场景需求将用户（1）角色授权为系统管理员； 操作过程：点击【用户管理】>在对应账号下点击角色图标“ ”>【添加角色】>勾选对应的权限模块>【确定】完成角色授权。

根据需求将用户（1）角色授权为审计管理员 操作过程：点击【用户管理】>在对应账号下点击角色图标“ ”>【添加角色】>勾选“腾讯云金融专区”>【查询】>勾选对应的权限模块>【确定】完成角色授权。

4.1.3. 角色权限查看

用户（1）登录堡垒机系统，查看系统管理过程如下； 操作过程：登陆账号1>点击【系统管理】>点击相关模块进行权限确认。

操作指南
订购实例
创建堡垒机实例

最近更新时间: 2024-10-17 17:10:00

登录租户控制台，点击云产品导航“堡垒机（BH）”，进入堡垒机控制，默认展示实例管理页面，新用户可以点击按钮“新购”完成堡垒机实例创建。

点击“新购”按钮，页面跳转到选购页面，可以按需选择租户所需的CPU架构和堡垒机规格，点击立即下单。

点击“新购”按钮，页面跳转到选购页面，可以按需选择租户所需的CPU架构和堡垒机规格，点击立即下单。创建成功后，可以在实例列表查看堡垒机实例相关信息。

点击“登录”按钮，可以登录堡垒机，具体操作参考“3.登录系统”相关指导，也可以点击“更多”，进行初始化堡垒机密码、销毁实例等操作。

登录系统

最近更新时间: 2024-10-17 17:10:00

静态口令认证

系统默认用户登录方式为静态口令认证，输入访问地址 http://imgcache.finance.cloud.tencent.com:80IP ，登录界面如图所示，输入用户名、密码，拖动验证滑块，点击登录按钮访问系统。

证书认证

在登录界面输入用户名、密码后，正确拖动滑块，点击登录后，系统跳转到如下图页面，点击“”按钮，跳转到选择证书页面，选择正确证书，点击登录进入系统。

证书登录详细配置步骤：

- 下载根证书，安装到访问浏览器；
- 设置用户认证方式为证书认证；
- 生成用户证书；
- 开启用户证书认证。

AD 域认证

在登录界面输入用户名、密码后，正确拖动滑块，点击登录后，系统跳转到如下图页面，输入在AD中的口令，点击登录进入系统。

AD域登录详细配置步骤：

- 确定被设置用户为AD域中用户；
- 设置用认证方式为AD域认证；
- 开启并设置域服务。

OTP 认证

在登录界面输入用户名、密码后，正确拖动滑块，点击登录后，系统跳转到如下图页面，输入手机令牌口令，点击登录进入系统。

OTP令牌登录详细配置步骤：

- 设置用认证方式为OTP认证；
- 开启并设置域服务；
- 如果是手机令牌登录，使用手机令牌扫描用户唯一标识生成动态口令。

组织结构

最近更新时间: 2024-10-17 17:10:00

组织结构可以清晰显示企业各个职能机构之间的关联关系，是系统中的基础模块，系统中的其他模块都是基于组织结构存在的。

根节点

登录系统默认显示根节点“”，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、资源筛选规则、策略管理。

组织结构添加

点击页面最左侧组织结构列表上方“)”添加按钮，进入新建节点页面如图所示，可以添加综合组、资源组或岗位授

权。输入名称，选择相应的组类型，点击按钮，添加成功。

组织结构修改

在组织结构列表，选择已添加的组织结构，点击“”组织结构编辑按钮，输入要修改的组织结构名称，点击确定按钮，修改组织结构。

组织结构删除

在组织结构列表，选择已添加的组织结构，点击“”组织结构删除按钮，弹出操作确页面，点击确定按钮，删除组织结构。

综合组

在组织结构列表，点击 “” 综合组，查看右侧菜单栏显示相应的模块权限包括：用户管理、资源管理、计划管理、角色管理。

选中类型为“综合组”的组织结构，点击添加按钮，可以在此综合组下添加子组，包括综合组、资源组或岗位授权。

资源组

在组织结构列表，点击 “” 资源组，查看右侧菜单栏显示相应的模块权限包括：资源管理、扩展属性。

选中类型为“资源组”的组织结构，点击添加按钮，可以在此资源组下添加只能添加类型为“资源组”的子组。

岗位授权

在组织结构列表，点击 “” 岗位授权，查看右侧菜单栏显示相应的模块权限包括：绑定用户、绑定资源、绑定规则、绑定策略。

选中类型为“岗位授权”的组织结构，点击添加按钮，不可添加子组。

仪表盘

最近更新时间: 2024-10-17 17:10:00

点击左侧组织结构列表的【根节点】，系统默认显示【仪表盘】模块，如图所示，可以查看到计划任务数、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、运维数据总览图、一周主机运维TOP5、计划任务TOP5、一周用户运维TOP5、系统运行状态、实时监控、今日新增会话、许可证信息。

用户管理

概述

最近更新时间: 2024-10-17 17:10:00

该模块是处理系统用户的相关操作。主要用于系统用户生命周期管理（包括创建，修改，注销，删除等），基本信息管理与维护，用户认证管理，岗位授权管理，用户角色授权管理。

用户添加

最近更新时间: 2024-10-17 17:10:00

用户可以在根节点下添加，也可以组织结构类型为 “综合组”下添加用户。

点击“)”按钮，进入用户管理页面，点击“)”按钮，进入添加添加用户页面，输入用户ID、用户名称、口令、确认口令

等相关信息，点击保存。（页面标“)”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）。之后默认进入用户编辑页面，详见用户编辑。

用户删除

最近更新时间: 2024-10-17 17:10:00

点击“)”按钮，进入用户管理页面，在用户列表勾选需要删除的用户，点击“)”按钮，提示弹出操作确认页面，点击“”按钮删除用户。

用户编辑

最近更新时间: 2024-10-17 17:10:00

基本信息编辑

点击“”按钮，进入用户管理页面，在用户列表选择需要编辑的用户，点击 “)”编辑按钮，进入基本信息编辑页面，输入需要修改的用户信息，点击“”修改用户基本信息。

设置口令

点击“”按钮，进入用户管理页面，在用户列表选择需要编辑的用户，点击 “”编辑按钮，进入基本信息编辑页面，之后点击“”，如图所示，有3种口令设置方式。

- “手动输入口令”，输入口令，确认口令，点击保存即可完成配置。
- “初始化固定口令”，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）。
- “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。

设置认证方式

在用户编辑页面，点击“”按钮，进入设置用户访问方式页面，如图所示：

可以设置以下四种认证方式：

- 静态口令认证：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。
- OTP认证：在如图复选框勾选otp认证，点击保存按钮，设置完成。
- AD域认证：在如图复选框勾选AD域认证，点击保存按钮，设置完成。
- 证书认证：在如图复选框勾选证书认证，点击保存按钮，设置完成。

设置策略

在用户编辑页面，点击“”按钮，进入设置策略页面，如图所示：

可以设置一下几种用户访问策略：

- 口令策略：在口令策略下拉框，选择已配置的口令策略，之后点击“”按钮，完成配置。根据已配置的口令规则，用户在进行修改口令时生效。
- 访问锁定策略：在访问锁定策略下拉框，选择已配置的访问锁定策略，之后点击“”按钮，完成配置。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。管理员被锁定后，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。
- 访问地址策略：在访问地址策略下拉框，选择已配置的地址访问策略，之后点击“”按钮，完成配置。当用户访问系统时，如果用户登录地址在设置的地址策略允许范围内，可以登录系统；如果用户登录地址在禁止访问范围内，登录系统失败。
- 访问时间策略：在访问时间策略下拉框，选择已配置的时间访问策略，之后点击“”按钮，完成配置。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。

唯一标识

用户唯一标识用于用户手机动态令牌登录认证。使用指定的谷歌手机令牌软件，扫描二维码，生成6位数字动态口令。

证书管理

本地证书生成

进入证书管理页面如图，直接点击“”按钮，生成本地个人证书如图2。

生成证书后，点击“”按钮，注销证书。

国密证书序列号绑定

进入证书管理页面如图1，在输入框输入证书序列号，点击“”按钮，绑定个人证书如图2。

绑定证书后，点击“”按钮，注销证书。

MAC 管理

开启MAC地址绑定，可以在用户下绑定MAC地址，用于加强认证安全性。（配置MAC认证需要开启MAC服务）

在MAC管理页面，勾选开启MAC绑定，输入需要绑定的用户MAC地址，点击")"按钮，将MAC地址添加到MAC地址列表，点击""按钮，设置绑定MAC地址。

高级选项

可以设置用户为一个临时用户，开启临时用户时，用户在设置的指定时间段内可以访问系统。超过设置的访问时间段，用户显示"过期"。

查询用户

最近更新时间: 2024-10-17 17:10:00

在用户列表，点击“”按钮，弹出查询条件框，可以根据用户ID、用户名称、用户类型、用户状态查询。如果勾选“子树查询”可以查看到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。

用户类型管理

最近更新时间: 2024-10-17 17:10:00

在用户列表，点击“)”进入用户类型添加页面，“)”进入用户类型添加页面，添加用户类型。点击“”删除用户类型。

用户相关操作

最近更新时间: 2024-10-17 17:10:00

注销

在用户列表，勾选需要注销的用户，点击“)”按钮，选择“注销选中用户”，页面弹出“”按钮，注销用户。

> **注意：**
>
> 用户注销后，不可以再编辑使用。

锁定

在用户列表，勾选需要锁定的用户，点击“)”按钮，选择“锁定选中用户”，页面弹出“”按钮，锁定用户。

解锁

在用户列表，勾选需要解锁的用户，点击“)”按钮，选择“解锁选中用户”，页面弹出“”按钮，解锁用户。

为选中用户绑定角色

在用户列表，勾选需要绑定管理角色的用户，点击“)”按钮，选择“为选中用户绑定管理角色”，进入批量授权角色页面，选择需要授权用户的一个或者多个角色，点击“)”按钮，授权用户角色完成。（用户角色相关配置详见角色管理）

为选中用户绑定岗位

在用户列表，勾选需要绑定岗位的用户，点击“)”按钮，选择“为选中用户绑定岗位”，进入批量管理岗位页面，选择需要授权用户的一个或多个岗位，点击“)”按钮，授权用户岗位。（岗位配置详见授权管理）

用户导入

在用户列表，点击“)”按钮，点击用户导入，进入用户导入页面如图，点击“”按钮，下载导入用模板，按照模板添加需要导入的用户。

点击“)”按钮，选择需要导入的用户文件，点击“)”按钮，上传文件如图。之后点击“)”按钮，“”如图，完成用户导入。

用户导出

在用户列表，点击“”按钮，点击“用户导出”，导出组织结构下的用户。

用户角色授权

最近更新时间: 2024-10-17 17:10:00

根据不同用户职能，授权用户角色。

在用户列表，点击“)”按钮，可以为指定用户授权角色。进入角色授权页面，点击“)”按钮，可以选择已添加到组织结构下的角色（相关角色配置详见角色管理），点击“”按钮，授权用户角色完成。

用户岗位授权

最近更新时间: 2024-10-17 17:10:00

在用户列表，点击“)”按钮，可以为指定用户授权岗位。进入岗位授权页面，点击“)”按钮，可以选择已添加到组织结构下的岗位（相关岗位配置详见授权管理），点击“”按钮，授权用户岗位完成。

资源管理

概述

最近更新时间: 2024-10-17 17:10:00

资源管理模块提供各类资源的添加，删除，信息维护等内容。同时支持资源账号的抽取，修改口令等操作。

资源添加

最近更新时间: 2024-10-17 17:10:00

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。

系统支持多种资源类型，例如： unix、windows、网络设备、数据库、ActiveDirectory、web应用系统、C/S应用系统。

进入资源管理页面，点击“)”按钮，进入资源添加页面，选择相关资源类型，资源版本，资源名称，所属组织结构等

信息，点击“”按钮，完成资源添加。

> **说明：**
>
> 页面标“*”为必填项，一个资源可以选择多个所属组，超时时间：抽取、推送操作等待时间，相关输入规则查看页面相应提示

添加资源基本信息后，跳转到资源编辑页面详见资源编辑。

资源删除

最近更新时间: 2024-10-17 17:10:00

在资源管理页面，勾选需要删除的资源，点击“)”按钮，页面弹出提示，点击“”按钮，删除资源。

资源编辑

最近更新时间: 2024-10-17 17:10:00

基本信息编辑

在资源管理页面，点击资源列表的“)”按钮，进入资源编辑页面，默认进入基本信息页面，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，点击“”完成修改。

在资源编辑页面，点击“)”按钮，也可以进入“账号列表”查看资源账号列表及相关操作（账号列表详见资源账号列表）。

访问协议

在资源管理页面，点击资源列表的“)”按钮，进入资源编辑页面，点击“)”按钮，进入资源访问协议页面，可以选择资源开放的协议，以及协议对应的端口号。点击“”按钮，完成设置。

扩展属性

资源已设置扩展属性，会在此模块显示并且可以编辑。（配置详见扩展属性管理）

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、推送账号及口令。

在资源编辑页面，点击“”按钮，进入管理配置，如图所示，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。

管理配置信息配置完成后，点击“”可以进行资源口令抽取。

设置口令策略

在资源编辑页面，点击“”按钮，进入设置口令策略，可以选择系统已添加的口令策略，点击保存完成配置。

高级

在资源编辑页面，点击“”按钮，进入高级设置，可以在一个资源上添加多个IP。

查询

最近更新时间: 2024-10-17 17:10:00

在资源管理页面，点击“”按钮，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，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。

统计视图

最近更新时间: 2024-10-17 17:10:00

点击资源管理页面的“”按钮，进入资源统计页面，可以查看组织结构下资源分布情况、资源总数。

资源账号列表

最近更新时间: 2024-10-17 17:10:00

添加

在资源管理页面，点击“)”账号列表按钮，进入资源账号列表页面，点击“”按钮，可以添加资源账号。

删除

勾选需要删除的资源，点击“”按钮，删除资源。

编辑

在资源账号列表，点击“”按钮，可以对资源账号进行编辑修改，可以修改资源基本信息和口令。

查询

在资源账号列表，点击“”按钮，可以输入账号名称进行查询。

批量改口令

在账号列表，勾选需要修改口令的账号，点击“”按钮，可以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。

批量修改鉴别状态

在账号列表，点击“)”按钮，选择“”可以将资源账号鉴别状态修改成“已鉴别”或“未鉴别”。

> **说明：**
>
> 账号的鉴别状态与岗位授权密切相关。“已鉴别”那么该账号则可以在岗位绑定账号时被查出。“未鉴别”那么岗位授权中要自动清理掉该账号授权，岗位授权不能查询到该账号。

批量修改接管状态

在账号列表，点击“)”按钮，选择“”可以将资源账号接管状态修改成“全接管”或“半接管”或“不接管”。

> **说明：**
>
> 账号的接管状态和账号的修改口令方式密切相关，如果“全接管”，那么该账号则允许加入到修改口令计划任务中，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。“不接管”是系统将会不再维护该账号的口令修改工作。

批量删除被接管资源账号

在账号列表，点击“)”按钮，选择“”，可以批量删除资源账号。

查看目标资源账号口令修改历史

在账号列表，点击“”按钮，可以查看目标资源账号口令修改历史记录。

资源类型配置

最近更新时间: 2024-10-17 17:10:00

此模块用于根据不同的资源版本，绑定对应的驱动程序。如图所示，可以在绑定驱动栏选择对应驱动。

驱动管理

最近更新时间: 2024-10-17 17:10:00

用于管理不同资源或者是同一类资源不同版本的命令库。用于资源的口令修改、抽取账号、拨测等操作。

在资源管理模块，点击")"按钮，进入驱动管理模块如图所示，点击""按钮，可以删除不需要的资源驱动。

应用发布管理

最近更新时间: 2024-10-17 17:10:00

通过应用发布管理非标准协议资源如数据库、B/S资源，在发布服务器上配置相关登录客户端，代理程序后，实现对资源的登录和审计。

添加

在资源管理模块，点击“)”，进入应用发布模块，点击“)”按钮，进入添加应用发布页面，输入信息，点击保存，完成配置。（为必填项）

删除

在应用发布模块，勾选需要删除的应用发布，点击“”按钮，删除应用发布。

编辑

在应用发布模块，点击“”按钮，可以修改应用发布信息，点击保存按钮，完成配置。

工具

在应用发布模块，点击")"按钮，进入应用发布工具管理页面，点击""按钮，可以添加应用发布连接目标资源的代填工具。

账号导出计划

最近更新时间: 2024-10-17 17:10:00

用于定时的将资源账号导出，通过勾选“FTP发送”或者是“邮件发送”将账号口令文件发送到指定设备或者指定用户的邮箱。

点击“”按钮，相关配置进行保存。

点击“”按钮，保存相关配置并启动账号导出计划。

点击“”按钮，初始化相关配置，清空之前配置的内容。

点击“”按钮，关闭账号导出计划页面。

点击“”按钮，查看文件列表内容，并可以下载账号及密码文件。如图所示。

资源相关操作

最近更新时间: 2024-10-17 17:10:00

批量修改协议端口

在资源管理列表，勾选需要修改协议端口的资源，点击“)”按钮，选择“”，进入批量修改协议端口页面，如图所示选择协议，修改对应的端口号，点击保存完成配置。

资源导入

在资源管理列表，点击“)”按钮，选择“)”，进入导入资源页面，。点击“)”按钮，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，完成之后，点击“)”按钮，选择已添加的资源文件，点击“)”按钮，上传文件，之后点击“)”按钮，进入映射文件页面，点击“”完成资源导入。

资源导出

在资源管理列表，点击“)”按钮，选择“”，可以将所在组织结构下的资源全部导出。

扩展属性管理

最近更新时间: 2024-10-17 17:10:00

在类型为"资源组"的组织结构下，存在【扩展属性】模块，可以进行资源扩展属性的添加和删除。

扩展属性符合模块【资源筛选规则】的一类资源（具有相同的扩展属性值），会被集合到一组，用于资源授权。（岗位授权相关配置详见授权管理模块）

添加

在扩展属性模块，点击""按钮，添加资源属性。

> **说明：**
>
>)为必填项，最大长度为1-128；选中为必填：勾选这个选项就是必填项，不勾选则在扩展属性模块可以不填。
> 选中为显示：勾选资源属性就会在扩展属性模块显示，不勾选，资源属性不显示。

删除

勾选已添加的扩展属性，点击""按钮，可以删除对应扩展属性。

授权管理

概述

最近更新时间: 2024-10-17 17:10:00

通过在岗位授权下添加用户，绑定资源、绑定规则，绑定策略，完成用户资源授权。

除了岗位授权下直接添加用户和资源，形成授权关系之外，也可以在用户下直接授权已添加岗位（配置详见用户岗位授权）

绑定用户

最近更新时间: 2024-10-17 17:10:00

在岗位授权下添加或者新建用户后，用户按照已绑定到岗位授权下的策略限制，对岗位授权下绑定的资源进行登录使用。

选择或新建绑定用户

点击组织结构类型为“岗位授权”的组织结构，默认进入绑定用户页面，点击“”按钮，可以选择已添加到组织结构中的用户，到绑定用户列表。

也可以点击“)”按钮，跳转到添加用户页面，添加新用户并绑定到用户列表。（添加用户配置详见用户添加）

删除

在绑定用户列表，点击“”按钮，可以删除已绑定此岗位授权的用户。

刷新

在绑定用户列表，点击“”按钮，可以刷新绑定用户列表。

绑定资源

最近更新时间: 2024-10-17 17:10:00

选择或新建绑定资源

在岗位授权下，选择“绑定资源”模块，进入绑定资源页面后，点击“)”按钮，选择已添加到系统的资源，或者是点击“)”按钮，新建资源并绑定到此岗位授权。（新建资源详见资源添加）

删除

在绑定资源列表，点击“”按钮，可以删除已绑定此岗位授权的资源。

刷新

在绑定用户列表，点击“”按钮，可以刷新绑定资源列表。

允许提权口令代填

在资源列表如果勾选提权口令代填，那么用户在登录资源时，若该资源需要输入提权口令，且在资源信息中已添加提权用户名、口令时，系统可自动代填提权用户名、口令。

绑定规则

最近更新时间: 2024-10-17 17:10:00

通过添加资源筛选规则，可以通过资源扩展属性，匹配资源属性值一致的资源自动绑定致用户登录授权。

添加

在岗位授权下，选择“绑定规则”模块，进入绑定规则页面后，点击“”按钮，进入规则绑定页面，选择已添加到系统的资源筛选规则，点击确定按钮完成配置。

资源筛选一般步骤：

- 在资源组下添加资源扩展属性，详见资源扩展属性管理；
- 相关资源扩展属性修改，详见扩展属性；
- 配置资源筛选规则，详见资源筛选规则管理；
- 资源筛选规则使用，详见本章节。

删除

在绑定规则页面，点击“”按钮，可以删除已绑定在此岗位授权下的规则。

绑定策略

最近更新时间: 2024-10-17 17:10:00

在岗位授权下，选择“绑定策略”模块，进入绑定策略页面后，可以在下拉框选择已添加到系统的策略，也可以点击“”按钮，添加相关策略。（策略相关配置详见策略管理）

计划管理

概述

最近更新时间: 2024-10-17 17:10:00

计划管理用于定期对资源账号进行口令变更、拨测，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。

任务添加

最近更新时间: 2024-10-17 17:10:00

点击")"按钮，进入计划管理页面，点击""按钮，进入计划任务添加页面，输入相关配置信息后，点击保存完成配置。

> **说明：**
>
> 1. "" ：为必须输入项；
> 2. 计划所属者：选择本系统
> 3. 执行规则：可以选择单次执行、按周执行：按月执行。
> 4. 口令规则：
>
> - 指定策略：已添加到系统的口令策略（详见口令策略）
> - 使用资源策略：已绑定到资源上的口令策略（详见资源编辑）
>
> 5. 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（点击")"页面相关内容详见资源账号）
> - 拨测：通过此计划任务，使用已修改的口令账号尝试登录资源，并记录口令登录情况
>
> 6. 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。

任务编辑

最近更新时间: 2024-10-17 17:10:00

在计划管理列表，点击“”按钮，可以对计划任务进行编辑，修改相关任务信息，点击保存按钮，完成配置（注释：计划名称不可以修改，状态为启动或者是运行中的任务不允许编辑）。

资源账号

最近更新时间: 2024-10-17 17:10:00

资源账号添加

在计划任务列表，点击任务列表中的“”按钮，进入资源账号添加页面，选择需要添加的资源账号，点击确定按钮，完成配置。

资源账号删除

在计划任务列表，点击任务列表中的“)”按钮，进入资源账号添加页面，勾选已添加到列表的资源账号，点击“”按钮，删除资源账号。

资源账号查询

在计划任务列表，点击任务列表中的“)”按钮，进入资源账号添加页面，点击“”可以按照资源名称、资源IP、资源类型、资源账号查询信息。

任务删除

最近更新时间: 2024-10-17 17:10:00

在计划任务列表，勾选需要删除的计划任务，点击“”按钮，删除任务。（任务状态为“初始化”或者是“停止”的任务可删除）

任务查询

最近更新时间: 2024-10-17 17:10:00

在计划管理列表，可以根据任务类型、计划名称、任务状态查询计划任务，如输入计划名称，点击“”按钮，可以查看到对应的计划任务。

任务启动/停止

最近更新时间: 2024-10-17 17:10:00

进入计划管理列表，如图所示，查看计划任务“口令变更”为停止状态，点击“”可以将任务启动。

如图所示，此时任务状态为“运行中”，点击“”按钮，可将任务停止。

查看操作日志

最近更新时间: 2024-10-17 17:10:00

进入计划管理列表，点击“”按钮，可以查看对计划任务的操作日志，是否对计划任务进行启动、修改等操作。

查看执行日志

最近更新时间: 2024-10-17 17:10:00

在计划管理列表，点击“”执行日志按钮，可以查看资源账号口令计划的执行情况，如计划开始介绍时间，执行条目，失败条目，成功条目，执行内容等。

角色管理

最近更新时间: 2024-10-17 17:10:00

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、岗位、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。

角色添加

在角色列表，点击“)”按钮，可以添加角色。（ “)”为必填项，点击“”按钮，选择权限）

角色修改

在角色列表，点击“”按钮，可以修改角色。

角色删除

在角色列表，勾选需要删除的角色，点击“”按钮，删除角色。

角色查询

在角色管理列表，点击“”按钮，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相关角色。

资源筛选规则管理

最近更新时间: 2024-10-17 17:10:00

资源筛选规则添加

资源筛选规则是具有相同资源扩展属性值的资源的集合。

点击“)”按钮，进入新建资源筛选规则页面，如图所示，点击“)”按钮，进入新建资源规则页面，输信息后，点击保存

完成配置。点击规则列表的“”按钮，可以查看匹配资源。

资源筛选规则删除

在规则列表，勾选需要删除的规则，点击“”按钮，删除规则。

策略管理
普通策略

最近更新时间: 2024-10-17 17:10:00

资源账号策略

资源绑定策略后，单点登录时可以自动筛选关联的账号。

点击“策略管理”按钮，进入策略管理页面，选择普通策略->资源账号策略，进入资源账号策略设置页面，点击“+”按钮，可以添加策略，输入信息后，点击保存完成策略配置。

勾选已配置的策略，点击“删除”按钮，删除策略。

访问时间策略

用于设置资源被访问的时间范围或者是设置用户登录系统的时间范围。

点击“策略管理”按钮，进入策略管理页面，选择普通策略->访问时间策略，进入访问时间策略设置页面，点击“+”按钮，可以添加策略，输入信息后，点击保存完成策略配置。

勾选已配置的策略，点击“删除”按钮，删除策略。

访问地址策略

用于设置资源被访问的地址范围，也可以用于设置用户登录系统的地址范围。

点击“策略管理”按钮，进入策略管理页面，选择普通策略->访问地址策略，进入访问地址策略设置页面，点击“+”按钮，可以添加策略，输入信息后，点击保存完成策略配置。

勾选已配置的策略，点击“删除”按钮，删除策略。

口令策略

由于设置用户口令定义的规则范围，在使用有效天数、口令历史次数、口令长度等方面进行使用和限制。

点击"策略管理"按钮，进入策略管理页面，选择普通策略->口令策略，进入口令策略设置页面，点击"+"按钮，可以添加策略，输入信息后，点击保存完成策略配置。

勾选已配置的策略，点击"删除"按钮，删除策略。

锁定策略

用于设置用户访问的失败次数，及用户锁定时间。

点击"策略管理"按钮，进入策略管理页面，选择普通策略->锁定策略，进入锁定策略设置页面，点击"+"按钮，可以添加策略，输入信息后，点击保存完成策略配置。

勾选已配置的策略，点击"删除"按钮，删除策略。

控制策略

最近更新时间: 2024-10-17 17:10:00

字符命令控制策略

用于设置在资源上输入命令的规则。

点击“策略管理”按钮，进入策略管理页面，选控制策略->字符命令控制策略，进入字符命令控制策略设置页面，点击“+”按钮，可以添加策略，输入信息后，点击保存完成策略配置。

勾选已配置的策略，点击“删除”按钮，删除策略。

传输控制策略

用于设置用户单点登录时，FTP传输操作规则。

点击“策略管理”按钮，进入策略管理页面，选控制策略->FTP传输控制策略，进入FTP传输控制策略设置页面，点击“+”按钮，可以添加策略，输入信息后，点击保存完成策略配置。

勾选已配置的策略，点击“删除”按钮，删除策略。

图形控制策略

用于设置用户单点登录时，图形控制操作规则。

点击“策略管理”按钮，进入策略管理页面，选控制策略->图形控制策略，进入图形控制策略设置页面，点击“+”按钮，可以添加策略，输入信息后，点击保存完成策略配置。

勾选已配置的策略，点击“删除”按钮，删除策略。

审计策略

最近更新时间: 2024-10-17 17:10:00

字符审计策略

用于设置用户单点登录时，输入命令的审计规则。

点击“策略管理”按钮，进入策略管理页面，选审计策略->字符审计策略，进入字符审计策略设置页面，点击“+”按钮，可以添加策略，输入信息后，点击保存完成策略配置。

勾选已配置的策略，点击“删除”按钮，删除策略。

审计策略

用于设置用户单点登录时，输入命令的审计规则。

点击“策略管理”按钮，进入策略管理页面，选审计策略->文件传输审计策略，进入文件传输审计策略设置页面，点击“+”按钮，可以添加策略，输入信息后，点击保存完成策略配置。

勾选已配置的策略，点击“删除”按钮，删除策略。

图形审计策略

用于设置用户单点登录时，进行图形操作时的审计规则。

点击“策略管理”按钮，进入策略管理页面，选审计策略->图形审计策略，进入图形审计策略设置页面，点击“+”按钮，可以添加策略，输入信息后，点击保存完成策略配置。

勾选已配置的策略，点击“删除”按钮，删除策略。

系统管理
系统配置

最近更新时间: 2024-10-17 17:10:00

系统定制化

点击""系统管理按钮，选择系统配置->系统定制化，进入系统定制化页面后，输入产品名称，上传产品logo，输入版权信息，点击保存完成配置。配置完成后可以在系统登录、主界面等位置查看已设置的新产品logo版权等信息。

系统升级

点击""系统管理按钮，选择系统配置->系统升级，跳转到系统升级页面，选需要上传的升级包，点击上传按钮，升级系统。

系统监控

点击""系统管理按钮，选择系统配置->系统监控，进入系统监控页面，可以查看系统软件授权信息、硬件授权信息、CUP使用情况、内存使用情况、磁盘使用情况、网卡使用情况等。

系统维护

本管理单元各功能主要为系统管理者使用，完成对系统重启、关机、还原出厂设置功能，操作前请确定对功能，有深入了解，避免影响系统功能。

查看服务状态显示为“”，表示运行状态正常；

点击“”按钮，重新启动系统；

点击“”按钮，关闭系统；

点击“”，系统恢复出厂设置。

服务器配置

系统支持三种部署方式：单机模式、双机模式、集群模式。

选择任意部署模式，点击保存按钮，完成配置。

点击“”按钮，可以添加服务器。

勾选已添加到系统服务器，点击“”按钮，可以删除相关服务器。

点击“”按钮，刷新服务器列表。

本地时间

可以手动输入时间，进行系统时间校对；也可使用服务器对系统时间进行同步。

- 手动校对时间；如图所示，在校对时间框选择当前时间，点击“”完成。

- 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,点击“”完成配置。

邮件服务

设置邮件发送服务，用于向用户发送随机口令、计划管理结果等相关内容。

选择进入系统配置页面后，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，点击保存完成配置。

配置完成后，可以输入实际用户邮箱进行检查，点击“”可以确认发送邮件服务器是否设置成功。

网卡配置

进入系统管理页面，选择系统配置->网卡配置，可以查看网卡配置内容，点击网卡名称，可以对网卡地址进行页面编辑。

路由配置

在路由配置页面，选择路由类型，输入ip、子网掩码、网关、选择网卡后，点击“”按钮，添加路由。

在路由列表，点击“”按钮，可以删除已配置的路由。

端口开放管理

关闭禁止对外开放的端口，可以提高系统安全性。

在系统管理页面，选择系统设置->端口开放管理，进入端口开放管理页面，输入端口号、描述信息、选择对应的协

议类型，端口开关状态，点击“”按钮，可以将设置的端口添加到端口列表。

勾选已添加到列表的端口，点击“”按钮，可以删除端口信息。

勾选已添加到列表的端口，点击“”按钮，可以批量开启端口或批量关闭端口。

可以在端口列表，滑动“”开关，开启或关闭指定端口。

DNS配置

配置DNS前，要先配置好默认网关。 配置DNS后可能会影响邮件服务，建议配置完成后重启Tomcat服务器。

在系统管理页面，选择系统配置->DNS配置，进入天DNS配置页面，选择状态为“启用”输入DNS服务器地址（“”为必输项），点击保存完成配置。

SNMP配置

用于通过SNMP采集日志，该功能支持TRAP、V1、V2C、V3等方式。

选择相关模式，输入勾选SNMP服务，输入ip地址、端口等信息，点击保存按钮，完成配置。

SYSLOG配置

选择发送协议，输入指定的设备ip地址、设备端口，勾选需要发送的日志类型，点击保存按钮，完成配置。配置完成后点击“)”按钮启动日志外发。启动之后可以点击“”停止日志外发。

外接存储

外接存储可以添加linux或者是windows设备，输入ip、远端路径、本地路径，点击保存完成配置。（路径格式eg：/xxx/xxx）

消息公告

点击“)”系统管理按钮，选择系统配置->消息公告，编辑消息公告，后点击“)”按钮，消息配置完成，查看消息状态为未发布；编辑消息公告，后点击“”按钮，消息配置完成，查看消息为已发布。（在公告栏中可以看到发布的公告，到达截止时间不再显示）

安全认证设置

最近更新时间: 2024-10-17 17:10:00

全局认证方式

用于设置系统用户基础认证方式。可以设置一种主认证方式，也可以设置两种认证方式组合认证。

点击系统管理按钮，选择安全认证设置->全局认证方式，进入全局认证方式设置页面，选择认证方式后，点击保存按钮完成配置。

超时设置

设置系统超时后，到达规定时间，系统自动登出。

点击系统管理按钮，选择安全认证设置->超时设置，进入超时设置页面，输入时间后，点击保存按钮完成配置。（说明：时间范围10-1440分钟）

OTP认证配置

OTP服务开关开启后，系统会自动增加OTP强认证方式。 普通用户可以通过用户模块进行配置，来确定是否需要开启OTP认证（前提条件是OTP服务器开关处于开启状态）。

本地OTP服务

在OTP认证配置页面，勾选本地OTP服务，点击保存按钮，本地OTP服务开启。

第三方OTP服务

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，点击保存按钮，第三方OTP服务开启。

域认证配置

域认证服务开启时，系统自动增加域认证方式。

点击系统管理按钮，选择安全认证设置->域认证配置，进入域认证配置页面，输入相关的域认证地址、端口等信息，点击保存完成配置。

证书配置

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。

本地自签发证书认证

进入证书内容配置页面如图所示：

配置本地证书步骤如下：

- 选择本地签发证书认证，点击保存按钮；
- 之后点击启动按钮，页面提示需要重启web服务生效，重启web；

- 之后可以点击“停止”按钮，停止服务；
- 点击“初始化”按钮，清空之前的配置

第三方签发证书认证

进入证书内容配置页面如图所示：

选第三方签发证书认证:

配置第三方签发证书步骤如下：

- 选择第三方签发证书认证，输入匹配起始字符、匹配结束字符，点击“选择”按钮，导入证书文件，点击保存按钮；
- 之前点击启动按钮，页面提示需要重启web服务生效，重启web；
- 之后可以点击“停止”按钮，停止服务；
- 点击“初始化”按钮，清空之前的配置

MAC配置

MAC认证服务开关开启后，用户可以通过绑定MAC地址来加强认证安全性。此开关开启后，可以在用户模块设置绑定的MAC地址。

勾选MAC服务开关，点击保存，服务开启。

初始化口令配置

初始化口令设置模块有两个功能，一是设置初始化固定口令，二是设置随机口令规则。

点击系统管理按钮，选择安全认证设置->初始化口令配置，进入初始化口令配置页面，输入固定口令或配置初始化随机口令规则后，保存配置。点击“查看”按钮，可以查看已配置的固定口令。

数据维护

最近更新时间: 2024-10-17 17:10:00

配置数据维护

此模块用于配置数据的备份、下载、还原等。

点击“)”按钮，进入系统管理，选择数据维护->配置数据维护，点击“”按钮，进入新建备份页面，如图，输入相关描述，点击生成备份按钮，完成备份配置。

点击“”按钮，可以上传备份文件,如图所示。

点击“”按钮，可以查看备份任务。

如图所示，点击“)”按钮，可以还原相关的审计日志；点击“)”按钮，可以删除备份，点击“”按钮，可以下载备份。

审计数据维护

此模块用于管理审计数据、行为审计数据、行为审计录像的备份、下载、还原等。

点击“)”按钮，进入系统管理，选择数据维护->审计数据维护，点击“”按钮，进入新建备份页面，如图，勾选需要备份的审计内容，输入起始和结束时间，点击生成备份按钮，完成备份配置。

点击“”按钮，可以上传备份文件,如图所示。

点击“”按钮，可以查看备份任务。

如图所示，点击“)”按钮，可以还原相关的审计日志；点击“)”按钮，可以删除备份，点击“”按钮，可以下载备份。

自维护

最近更新时间: 2024-10-17 17:10:00

点击右上角工具栏中的“”按钮，可以对用户基本信息进行维护，包括基本信息修改、口令更改，证书查看。

控件下载

最近更新时间: 2024-10-17 17:10:00

运维用户登录系统，点击“”按钮，可以下载单点登录控件和根证书。

审计管理

概述

最近更新时间: 2024-10-17 17:10:00

具有审计权限的管理员，可以查看审计管理模块。对用户的的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。

管理审计

最近更新时间: 2024-10-17 17:10:00

安全认证审计

对拥有审计角色的用户进行审计角色授权并号登录系统，进入管理管理平台，默认进入管理审计模块，点击“”按钮，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。

可以输入起始时间、结束时间、用户IP、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。

基础信息维护审计

审计管理员进入管理管理平台，默认进入管理审计模块，点击“)”按钮，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。在列表中点击“”查看按钮，进入基础信息维护详细页面如图所示。

操作行为审计

最近更新时间: 2024-10-17 17:10:00

在线会话审计

审计管理员进入审计平台，点击“)”，进入操作行为审计页面，点击“”按钮，进入在线会话查看页面，可以查看在线会话相关信息，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。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。

历史会话审计

审计管理员进入审计平台，点击“)”，进入操作行为审计页面，点击“”按钮，进入历史会话查看页面，可以查看历史会话相关内容，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。

统计报表

最近更新时间: 2024-10-17 17:10:00

基础报表

系统信息报表

审计管理员进入审计平台，点击“)”按钮，默认进入“基础报表”模块，之后点击系统信息报表按钮，选择“系统巡检报表”，点击“”按钮，可以导出系统巡检报表。

用户信息报表

审计管理员进入审计平台，点击“”按钮，进入基础报表页面，点击“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。

资源信息报表

审计管理员进入审计平台，点击“”按钮，默认进入基础报表页面，点击“资源信息报表”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

运维人员统计报表

审计管理员进入审计平台，点击“)”按钮，进入统计报表模块，点击“”按钮，进入运维业务报表页面，点击“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

审计管理员进入审计平台，点击“)”按钮，进入统计报表模块，点击“”按钮，进入运维业务报表页面，点击“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

审计管理员进入审计平台，点击“)”按钮，进入统计报表模块，点击“”按钮，进入运维业务报表页面，点击“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。

搜索

最近更新时间: 2024-10-17 17:10:00

审计管理员进入审计平台，点击“”按钮，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。

普通运维用户操作手册

概述

最近更新时间: 2024-10-17 17:10:00

系统登录主要的工作就是系统认证。堡垒机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、数字证书认证、动态口令认证、LDAP域认证等。

无论堡垒机系统配置哪种认证方式，登录系统都需要在浏览器中输入服务地址。例如:http://imgcache.finance.cloud.tencent.com:80192.168.23.107。在该例中，192.168.23.107为堡垒机系统IP地址。当在浏览器中输入示例内容后，点击回车（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。下面列举常见的几种常见的认证方式界面。

静态口令认证登录

最近更新时间: 2024-10-17 17:10:00

静态口令登录认证是最基本得认证方式，登录界面入如图所示，输入用户名及口令后，拖动滑块，点击登录按钮后登录系统。

单点登录

最近更新时间: 2024-10-17 17:10:00

单点登录

系统支持两种登录资源方式， web页面登录，客户端工具登录。

进行单点登录之前需要下载单点登录工具（插件）并进行安装，下载详见【5.套件中心】。

首页快速登录

点击左侧菜单栏“)”选项进入运维首页，点击“)”按钮，进入首页历史登录列表。在资源列表登录方式栏中选择需要登录方式按钮（如“)”、“”等），直接登录系统。

授权列表

最近更新时间: 2024-10-17 17:10:00

资源列表可以查看用户实体授权资源，也可以查看通过绑定资源筛选规则后匹配到的资源。

点击左侧菜单栏")"选项进入运维首页，点击""按钮，进入授权列表页面。

Unix/Linux资源

在授权列表中，Unix/Linux类资源包含三种单点登录方式：字符登录、图形登录、XFTP登录。根据不同的登录协议，选择相应的登录工具。

web登录

堡垒机系统支持登录Unix/Linux资源协议,如ssh2、ssh1、Telnet、sftp、ftp、VNC、Xwindows等都支持web页面登录。

进入授权列表，如图所示。

选择linux资源，点击资源列表中的""，按钮，进入登录配置页面，选择登录协议、输入用户名、口令、选择web工具如图所示。

点击登录，成功登录系统如图所示。

工具登录

PuTTY登录

选择字符协议后，如ssh1、ssh2、Telnet协议后，可以使用系统自带putty工具登录，不需要再次安装下载。

进入授权列表，如图所示。

点击资源列表中的“”，按钮，进入登录配置页面，选择登录协议、输入用户名、口令、选择PUTTY工具如图所示。

点击登录，成功登录系统如图所示。

SecureCRT/X-Shell登录

选择字符协议后，如ssh1、ssh2、Telnet协议后，使用SecureCRT/X-Shell登录，首先需要下载按钮SecureCRT/X-Shell工具，配置登录路径。

找到安装单点登录控件的安装位置，找到db_path.ini文件，打开后修改客户端登录工具安装位置。

进入授权列表，如图所示。

点击资源列表中的“”，按钮，进入登录配置页面，选择登录协议、输入用户名、口令、选择X-Shell工具如图所示。

点击登录，成功登录系统如图所示。

Xftp登录

选择ftp或sftp登录协议后，使用Xftp登录系统，需要下载安装客户端WinSCP。

进入授权列表，如图所示。

点击资源列表中的“”，按钮，进入登录配置页面，选择登录协议、输入用户名、口令、选择xftp工具如图所示。

点击登录，成功登录系统如图所示。

Windows资源

在授权列表中，Windows类资源包含两种单点登录方式：图形登录、FTP登录。根据不同的登录协议，选择相应的登录工具。

Web登录

堡垒机系统支持登录Windows资源协议,如RDP、ftp、VNC、ftp等都支持web页面登录。

进入授权列表，如图所示。

选择windows资源，点击资源列表中的“”，按钮，进入登录配置页面，选择登录协议RDP、输入用户名、口令、选择web工具如图所示。

点击登录，成功登录系统如图所示。

工具登录

Xftp登录

选择ftp登录协议后，使用Xftp登录系统，需要下载安装客户端WinSCP。

进入授权列表，如图所示。

点击资源列表中的“”，按钮，进入登录配置页面，选择登录协议ftp、输入用户名、口令、选择xftp工具如图所示。

点击登录，成功登录系统如图所示。

Mstsc登录

进入授权列表，如图所示。

选择windows资源，点击资源列表中的“”，按钮，进入登录配置页面，选择登录协议RDP、输入用户名、口令、选择RDP工具如图所示。

点击登录，成功登录系统如图所示。

数据库资源

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。

Web登录

进入授权列表，如图所示。

选择数据库资源，点击资源列表中的“”，按钮，进入登录配置页面，选择登录输入用户名、口令、选择WEB工具，应用发布如图所示。

点击登录，成功登录系统如图3所示。

工具登录

Mstsc登录

进入授权列表，如图所示。

选择数据库资源，点击资源列表中的“”，按钮，进入登录配置页面，选择登录输入用户名、口令、选择RDP工具，应用发布如图所示。

点击登录，成功登录系统如图所示。

网络设备资源

Web登录

字符协议登录

堡垒机系统支持登录网络资源协议,如ssh2、ssh1、Telnet、https、http等都支持web页面登录。

进入授权列表，如图所示。

选择网络资源，点击资源列表中的“”，按钮，进入登录配置页面，选择登录协议、输入用户名、口令、选择web工具如图所示。

点击登录，成功登录系统如图3所示。

http/https协议登录

登录网络资源，如果选择http或者是https协议，需要配置应用发布服务器，配置完成后，

工具登录

putty登录

选择字符协议后，如ssh1、ssh2、Telnet协议后，可以使用系统自带putty工具登录，不需要再次安装下载。

进入登录配置页面，选择登录协议、输入用户名、口令、选择PUTTY工具如图所示。

点击登录，成功登录系统如图所示。

secureCRT/X –shell登录

进入登录配置页面，选择登录协议、输入用户名、口令、选择X-Shell工具如图所示。

点击登录，成功登录系统如图所示。

Mstsc登录

登录网络资源，如果选择http或者是https协议，需要配置应用发布服务器，配置完成后，可以选择RDP协议相关的工具登录资源。

Active Directory

Web登录

堡垒机系统支持登录AD域资源使用RDP协议web页面登录。

进入授权列表，如图所示。

选择AD资源，点击资源列表中的“”，按钮，进入登录配置页面，选择登录协议RDP、输入用户名、口令、选择web工具如图所示。

点击登录，成功登录系统如图所示。

工具登录

Mstsc登录

进入授权列表，如图所示。

选择AD域资源，点击资源列表中的“”，按钮，进入登录配置页面，选择登录协议RDP、输入用户名、口令、选择RDP工具如图所示。

点击登录，成功登录系统如图3所示。

C/S应用系统

登录cs资源需要配置应用发布，配置应用发布后，可以选择相关协议工具单点登录。

web登录

进入授权列表，如图所示。

选择C/S资源，点击资源列表中的“”，按钮，进入登录配置页面，选择登录输入用户名、口令、选择WEB工具如图所示。

点击登录，成功登录系统如图所示。

工具登录

Mstsc登录

进入授权列表，如图所示。

选择C/S资源，点击资源列表中的“”，按钮，进入登录配置页面，选择登录输入用户名、口令、选择RDP工具如图所示。

点击登录，成功登录系统如图所示。

套件中心（插件）

最近更新时间: 2024-10-17 17:10:00

用户登录运维门户后，点击“”进入套件中心，点击下载按钮，可以下载单点登录工具或根证书。根据安装提示进行安装卸载。