# 密钥账号管理服务器 (2台)

# 技术参数

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标项要求** |
|  | ★ | 硬件配置 | 专用千兆多核硬件平台，4≥个千兆电口；2≥个千兆光口；1≥个接口扩展槽位；硬盘容量≥4TB硬盘，电源：冗余双电源；CPU≥2核，主频≥3.3GHz；内存≥8G；三年产品标准维保服务。 |
|  | ★ | 性能要求 | 账号改密/验证 ≥15账号/s，账号签出 ≥300TPS。含350点资产授权 |
|  | ★ | 系统功能 | 采用专用千兆多核硬件平台和安全操作系统。产品功能支持： 密钥管理、用户账号管理、角色权限管理、密码保险箱、账号发现、策略管理、工单系统等功能。 |
|  |  | 密钥管理 | 密钥在生成完毕后，会存储到数据库中，并且在密钥管理的设备密钥页面下映射显示信息 |
|  |  | 密钥的生成会根据其所属方案的方案模板进行生成，生后密钥在设备列表中显示 |
|  |  | 密钥可进行更换操作，更换完成后密钥将变为未用状态 |
|  |  | 用户账号管理 | 支持本地、RADIUS、AD域等用户认证方式 |
|  |  | 支持AD域用户的认证模式和同步模式 |
|  |  | 支持细颗粒度用户权限设置；支持基于部门、用户、用户组、内嵌账号应用、资产类型、资产、策略、审计、工单等多个维度进行权限划分；支持编辑权限具体到到每个模块的功能按钮，例如用户权限支持新建用户、修改用户、删除用户三个具体功能 |
|  |  | 支持按IP黑白名单、访问时间段限制用户访问系统 |
|  |  | 安全设置 | 支持连续输入错误的密码后系统自动锁定用户账号，密码尝试次数、锁定时间可自定义  |
|  |  | 支持用户密码强度、首次登录改密、历史密码校验、密码修改周期等设置 |
|  |  | 支持登录失败锁定策略，前端用户登录平台时口令输入多次错误则锁定，避免前端用户密码被暴力破解。支持设置锁定方式为锁定用户或锁定来源IP，支持设置登录失败的次数和锁定时间 |
|  |  | 支持通过邮件的方式重置密码，可支持设置禁用重置密码方式、验证尝试次数、禁用时长、重置计数时长、图形验证码和邮件验证码过期时间 |
|  |  | 部门管理 | 支持按部门划分管理范围，实现不同部门管理各自资源及账号密码 |
|  |   | 支持设置多个部门安全码管理员和安全码，账号备份和导出文件均通过需通过部门安全码解密 |
|  |  | 账号策略管理 | 支持新建账号的密码验证，保障新建账号的准确性 |
|  |  | 支持批量导入账号的验证和覆盖已有账号（重复性校验）；支持批量导出账号，对于有查看密码权限的账号支持批量导出； |
|  |  | 支持登录账号关联，当账号为无法登录账号时可以关联登录账号进行提权；支持提权账号关联，当账号没有改密权限时可以关联提权账号进行改密； |
|  |  | 支持账号组管理，支持设置账号组为普通账号组或等密账号组。等密账号组即支持当某个账号改密时，会触发其他账号改成相同密码，可应用于同类资产类型同步目标设备账号的密码 |
|  |  | 支持账号手动验证和手动释放 |
|  |  | 账号改密 | 支持自定义账号密码改密复杂度生成规则，包括自动改密周期、同密码、不同密码或指定密码的改密模式以及自定义改密规则，可基于资产、账号属性动态配置改密、验证策略。 |
|  |  | 支持新建改密策略时设置多个改密时间（精确到秒） |
|  |  | 支持设置一次一密的使用策略，特权账号被签入使用后立即改密，保证账号的安全性，可基于资产、账号属性动态配置一次一密策略。 |
|  |  | 支持密码校正，即密码验证失败时使用特权账号将目标设备密码校正为系统内密码 |
|  |  | 账号验证 | 可设置密码验证策略，支持自动、手动验证，验证周期及验证时间，并且一个执行日期可设置多个执行时间。系统类型包括Windows/Linux/Unix，Huawei/H3C等网络设备，数据库类型包括MySQL、Oracle、SQL Server等 |
|  |  | 密码备份管理 | 支持设置逃生通道，包括但不限于邮件和SFTP等方式外发；账号密码信息加密之后定期备份到指定的服务器和邮箱。 |
|  |  | 支持密码外发分段备份策略，解密密码由不同的管理员负责设置和维护 |
|  |  | 账号发现 | 支持纳管账号或指定IP范围进行一次性和周期性账号发现任务，可同时对多账号、多设备进行账号发现； |
|  |  | 支持账号发现排除策略配置，在执行账号发现任务时将不必要的账号排除 |
|  |  | 支持对发现的账号进行历史任务比对，找出并展示新增的账号并显示其纳管状态、风险状态、上次登录时间、上次改密时间、权限变更、部门和处理状态等信息 |
|  |  | 弱密码检测 | 支持对目标资源上的账号进行一次性或周期性弱密码扫描，可自定义弱密码规则、密码与账号相同检测、上传自定义弱密码集等，支持的资源类型至少包括windows、Linux、MySQL、Oracle、SQL Server、Weblogic、AD域等。 |
|  |  | 支持弱密码检测创建离线任务，即支持通过离线工具扫描任务检测目标设备账号的弱口令，并形成整体的报告 |
|  |  | 支持内嵌弱密码集生成工具，弱密码集生成规则包括固定字符串、大小写字母、特殊字符、数字、字符集、IP地址，支持规则组合生成弱密码集 |
|  |  | 工单管理 | 支持访问授权工单，即通过工单申请资源的密码权限，实现基于时间对用户的账号使用权限的申请，支持撤销已审批工单使工单失效。 |
|  |  | 支持访问授权工单对账号允许访问次数进行审批 |
|  |  | 支持账号操作工单，即管理员可通过工单审核流程，对目标资源系统账号进行变更操作，包括新增、删除、编辑、启用、禁用等操作 |
|  |  | 逃生通道 | 提供Linux/Unix特权账号逃生密钥通道，可启动定期或手动更新逃生密钥的SFTP外发备份功能，若发生宕机密码丢失的情况下能找回目标资产上所有账号的密码。 |
|  |  | 安全审计 | 支持操作系统审计，内容包括但不限于：登录/退出系统、对系统进行的操作、系统用户密码变更记录、用户权限分配、账号活动记录等 |
|  |  | 与现有堡垒机系统联动 | 支持与现有堡垒机系统进行联动，当堡垒机需要使用账号连接目标设备运维时，实时签出该设备的账号密码，堡垒机本地不保存账号密码。 |
|  |  | 产品资质 | 具备公安部颁发的网络安全专用产品安全检测证书  |