

数据安全交换平台 操作手册



北京天地和兴科技有限公司

目录

| | |
|---------------------------|--|
| 第 1 章 引言 | |
| 1.1 编写目的 | |
| 1.2 使用对象 | |
| 1.3 名词解释 | |
| 第 2 章 设备上架及管理 PC 配置 | |
| 2.1 设备上架要求 | |
| 2.1.1 环境要求 | |
| 2.1.2 交换平台开机 | |
| 2.1.3 常见问题 | |
| 2.2 管理 PC 配置 | |
| 2.2.1 IP 配置 | |
| 2.2.2 管理浏览器配置 | |
| 2.3 网络接线图 | |
| 2.4 登录管理界面 | |
| 2.5 常见问题 | |
| 第 3 章 系统管理 | |
| 3.1 网络配置 | |
| 3.1.1 IP 地址 | |
| 3.1.2 网络路由 | |
| 3.1.3 DNS 配置 | |

| | |
|--------|-------------------|
| 3.2 | 摆渡配置 |
| 3.3 | 日志管理 |
| 3.4 | 服务控制 |
| 3.5 | 日志空间设置 |
| 3.6 | 恢复出厂设置 |
| 3.7 | 升级服务 |
| 3.7.1 | 应用升级 |
| 3.7.2 | 导出配置 |
| 3.7.3 | 导入配置 |
| 3.8 | 系统调试 |
| 3.9 | 系统检测 |
| 3.10 | 系统重启 |
| 3.11 | 系统状态 |
| 3.12 | 病毒库设置 |
| 3.13 | 安全设置 |
| 3.14 | 双机热备 |
| 3.14.1 | 热备基本配置 |
| 3.14.2 | 常见问题 |
| 第 4 章 | 同步功能配置 |
| 4.1 | FTP 文件同步 |
| 4.1.1 | FTP 账号的基本要求 |

| | |
|---------------------------|--|
| 4.1.2 FTP 服务器环境搭建 | |
| 4.1.3 任务配置 | |
| 4.1.4 常见问题 | |
| 4.2 SMB 文件同步 | |
| 4.2.1 共享账号基本要求 | |
| 4.2.2 SMB 服务器搭建 | |
| 4.2.3 任务配置 | |
| 4.2.4 基本问题处理方法 | |
| 4.3 NFS 文件同步 | |
| 4.3.1 共享要求 | |
| 4.3.2 NFS 服务器搭建 | |
| 4.3.3 任务配置 | |
| 4.3.4 基本问题处理方法 | |
| 4.4 音视频交换 | |
| 4.4.1 音视频交换配 | |
| 4.5 服务数据交换 | |
| 4.5.1 业务流程图 | |
| 4.5.2 配置说明 | |
| 4.6 数据库同步 | |
| 4.6.1 网闸支持的数据库类型及版本 | |

| | |
|-------|----------------|
| 4.6.2 | 账号基本要求 |
| 4.6.3 | 配置方法 |
| 4.6.4 | 基本问题处理方法 |
| 4.7 | 其他常见问题 |
| 第 5 章 | 日志篇 |

第 1 章 引言

1.1 编写目的

本手册提供基本的管理和任务配置。

1.2 使用对象

数据安全交换平台用户或维护人员。

1.3 名词解释

| | |
|----------|---------------------------------|
| 同步服务器 | 数据交换所需的服务器环境，如 FTP/SMB/NFS、数据库等 |
| 数据安全交换平台 | 安全隔离与单向导入系统（单向数据安全交换平台） |
| 4 机模式 | 由前后置机各一台、单向光闸两台构成的 4 机模式数据交换平台。 |
| 6 机模式 | 由前后置机各两台、单向光闸两台构成的 6 机模式数据交换平台。 |
| | |

第 2 章 设备上架及管理 PC 配置

本章主要讲解对现场系统上架以及管理数据安全交换平台的 PC 相关配置等。

2.1 设备上架要求

2.1.1 环境要求

数据安全交换平台可在如下的环境中使用：

- 输入电压：100V~240V
- 温度：0~50℃
- 湿度：5%~95%无凝露

为保证交换平台能长期稳定的运行，请保证电源有良好的接地措施，保证使用环境的温湿度。本网闸设计符合国家标准，交换平台的安放、使用、报废请按照国家相关法律、法规要求。

2.1.2 交换平台开机

将电源适配器一端接入市电，一端插入网闸电源接口，轻按电源开关按键，此时前面板的 POWER 指示灯长亮，说明网闸正常启动；SWITCH 指示灯闪烁 1-2 分钟后长亮，说明网闸内前置机通讯正常工作。

请准备两条标准的 RJ45 以太网线，一条插入网闸的后置机网口与局域网相连，一条插入网闸的前置机网口与局域网相连。



交换平台正常工作时，POWER 指示灯长亮，SWITCH 指示灯闪烁 1-2 分钟后长亮(SWITCH 指示灯熄灭表示内前置机通讯异常，请与我们联系)，HDD.W、HDD.L 指示灯在硬盘工作时会闪烁，网口指示灯在该网口接入网络时会闪烁。

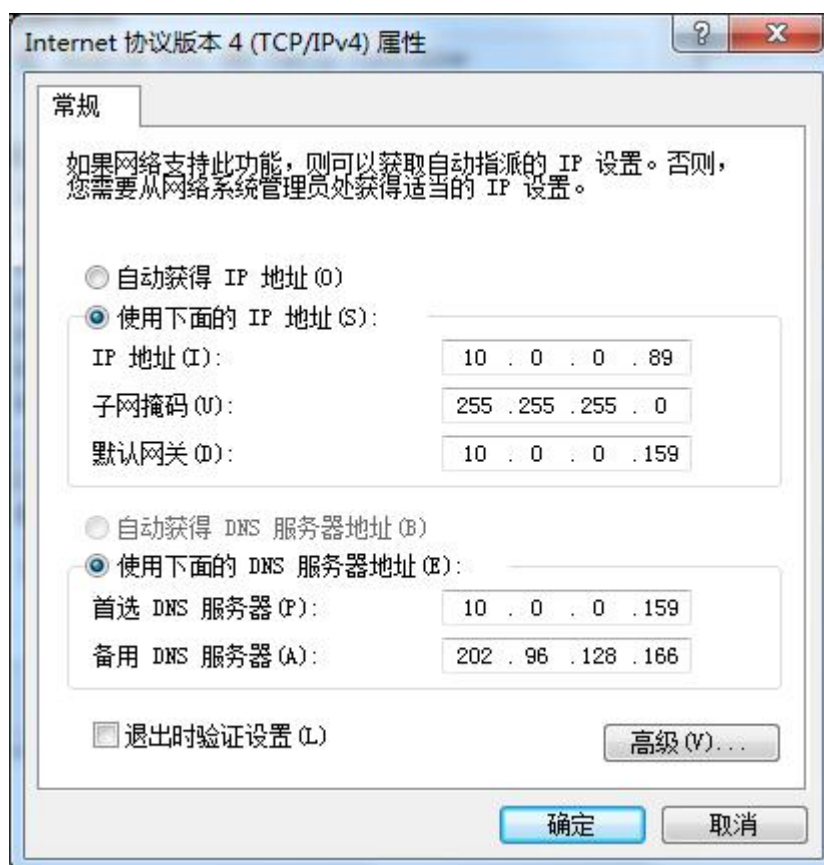
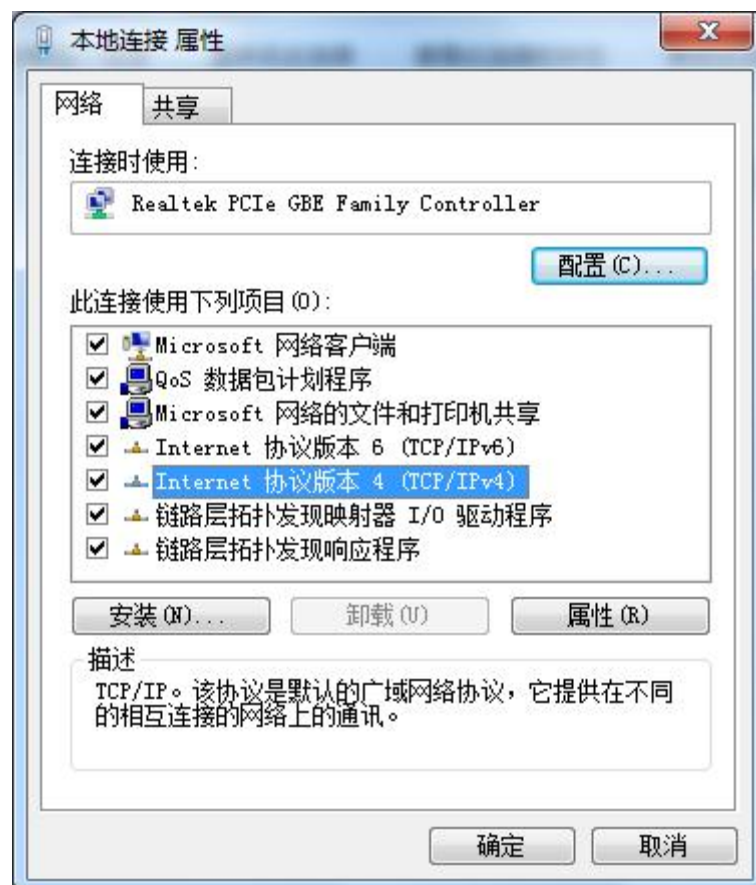
2.1.3 常见问题

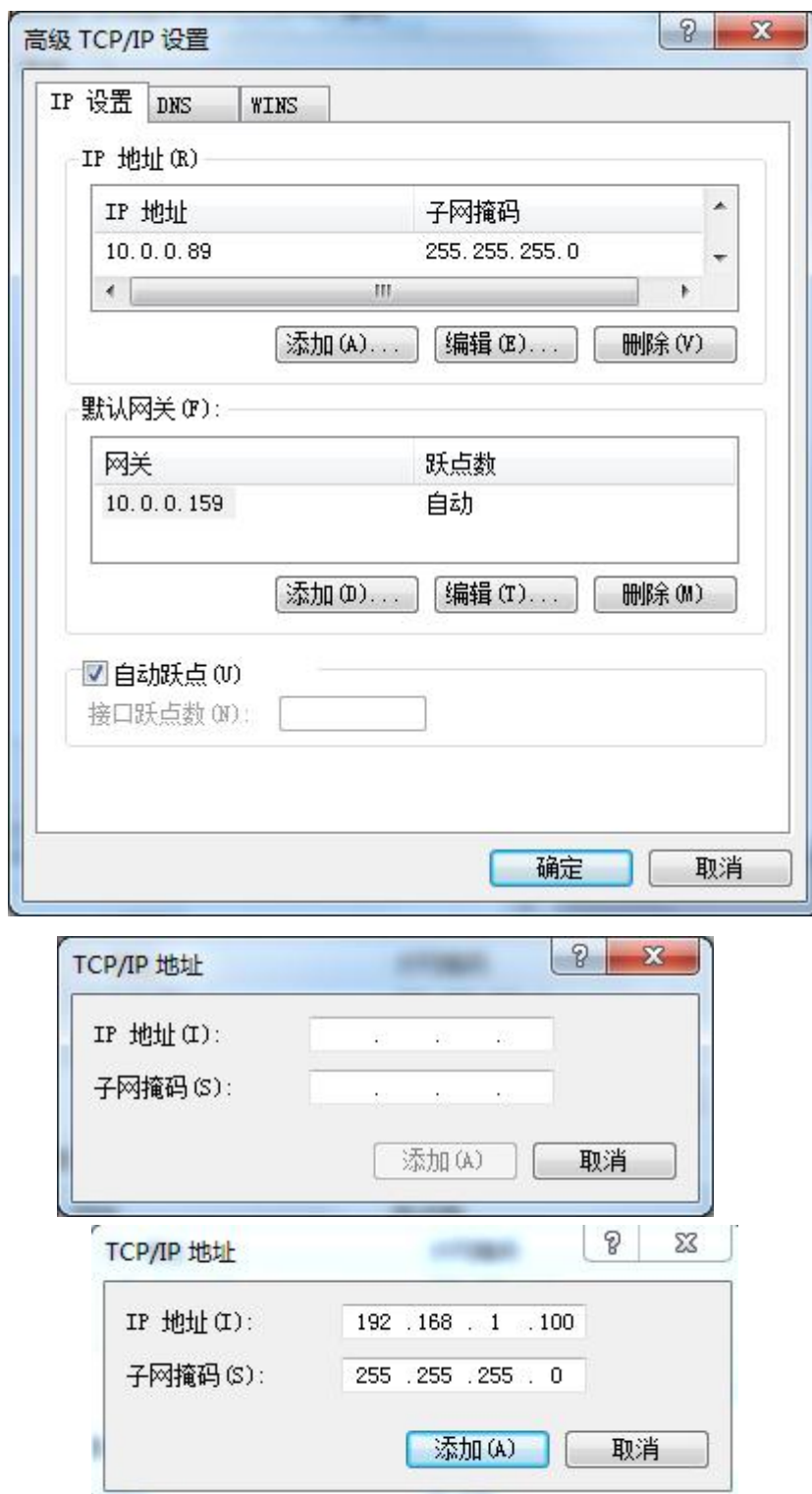
2.2 管理PC配置

2.2.1 IP 配置

右键“本地连接”选择【属性】弹出本地连接属性设置界面→双机选择【Internet 协议版本 4（TCP/IPv4）】→点击高级→点击添加→输入与网闸同网段的 IP 地址、子网掩码（如： 192.168.1.100、255.255.255.0）→点击添加完成新建 IP 地址；具体流程如下图所示：







配置 IP 地址流程示意图

如果需要同时管理内、前置机，则需要管理 PC 上同时添加内前置机网段的 IP，已 LAN1（默认 IP192.168.1.1）和 WAN1（默认 IP172.168.1.1）为例，PC 上添加两个 IP 地址，192.168.1.100/24 和 172.168.1.100/24，则可以同时登陆内前置机的管理页面。

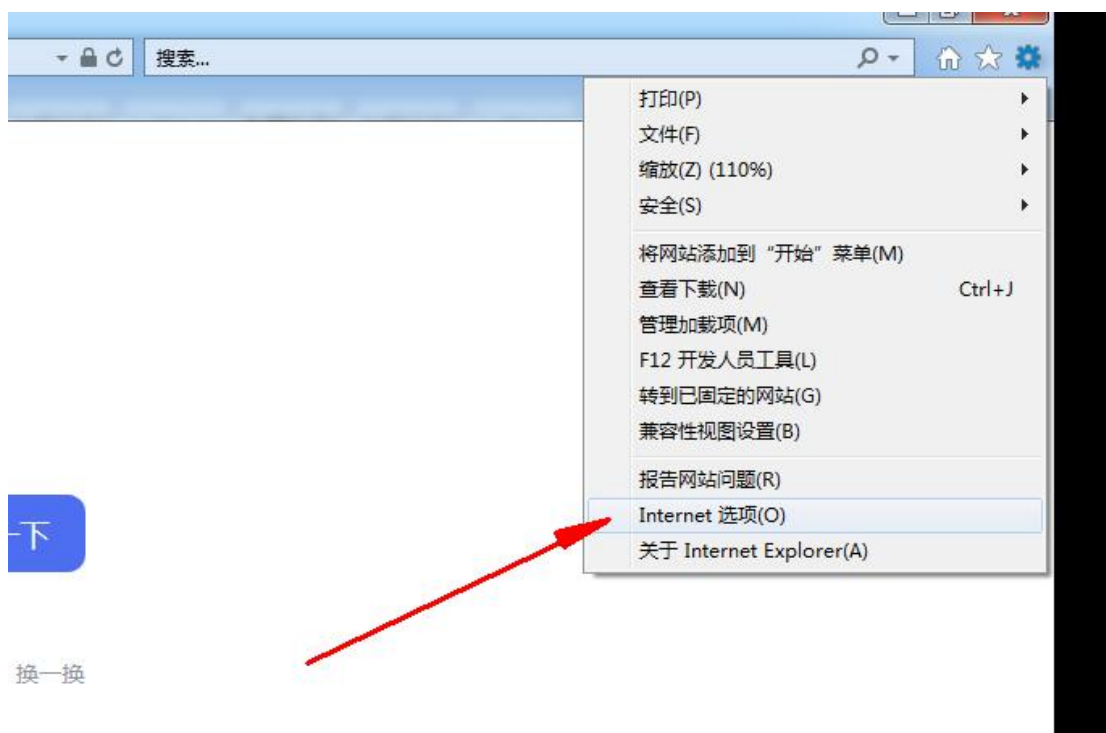
2.2.2 管理浏览器配置

登录交换平台管理页面推荐使用 IE9 及以上版本（10,11）的浏览器，或者使用 IE 内核的其他浏览器，像谷歌等浏览器可能会安装不了 USBKey 驱动导致无法登录。

交换平台管理页面登录之前，请先确保 PC 网络可以与数据安全交换平台 IP 通信，其次需要下载数据安全交换平台 USBKey 驱动并安装，以能够识别 USBKey 和登录管理界面。

由于 USBKey 的驱动是私有签名证书，很多 PC 下载安装不成功，一下是设置安装方法：

首先打开 IE 浏览器。点击浏览器设置-Internet 选项



点击“安全” - “自定义级别”：

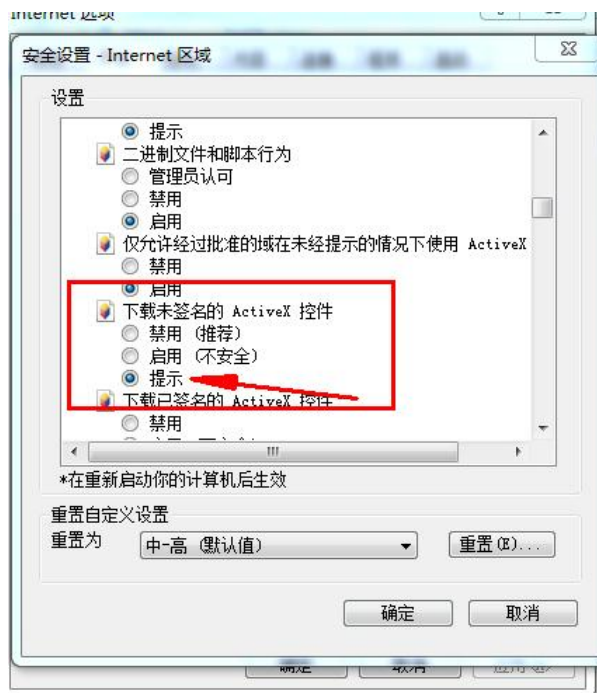


Bai

百度热榜

- 1 普京：中德正崛起为超级大国 热
- 2 iPhone12开售排队
- 3 林心如回应与霍建华吵架

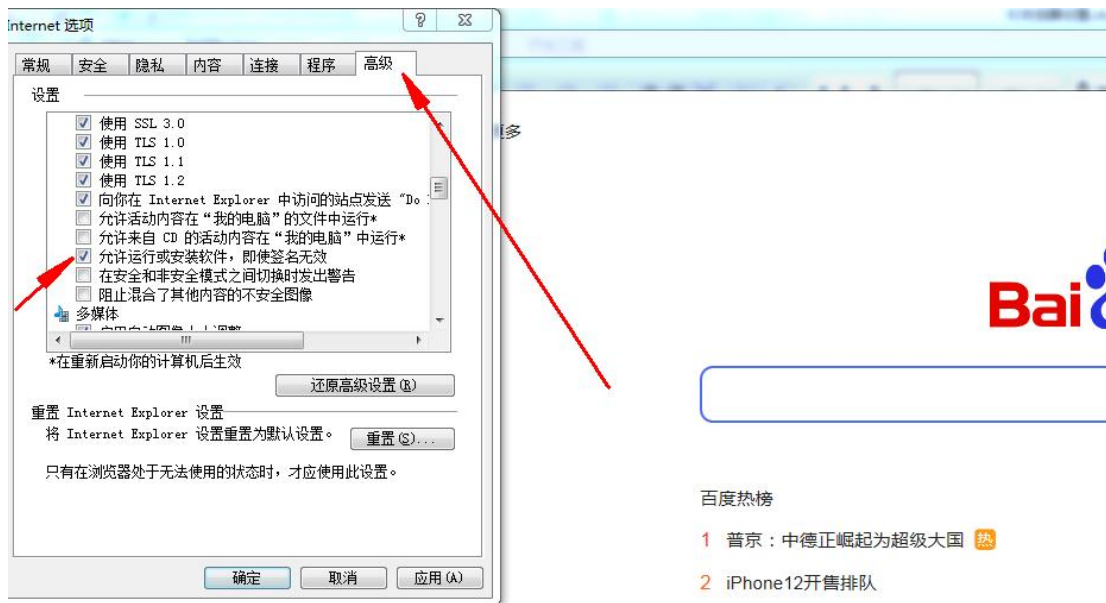
找到“下载未签名的 ActiveX 控件”，选择“提示”后点击确定：



百度热榜

- 1 普京：中德正崛起为超级大
- 2 iPhone12开售排队
- 3 林心如回应与霍建华吵架

再找到“高级” - “允许运行或安装软件，即使签名无效”，勾选并保存：



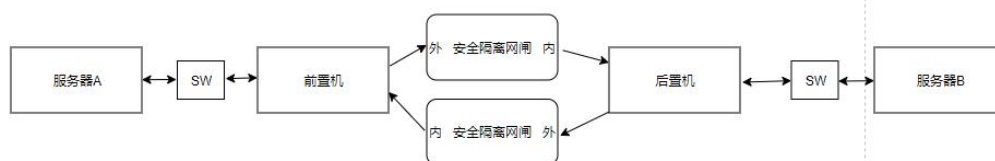
修改完成之后，重启浏览器，输入数据安全交换平台管理地址，后置机：

https://192.168.1.1，前置机:https://172.168.1.1，正常登陆时会提示下载驱动，安装完成后即可登录。

2.3 网络接线图

中间安全隔离网闸也可以用单向数据安全交换平台代替。

4机模式网络接线参考图



6机模式网络接线参考图



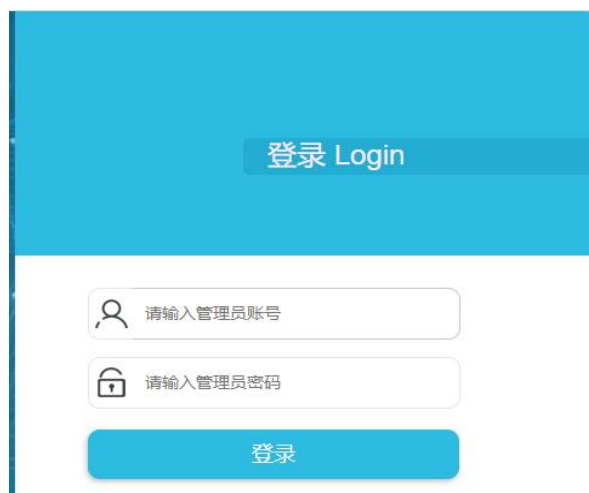
2.4 登录管理界面

选择与安全数据交换平台在同一局域网内的电脑, 按上述配置好电脑 IP→将安全数据交换平台 USB Key 插入电脑 USB 接口中→再在网页浏览器 (Internet Explore) 中输入 IP 地址 https://192.168.1.1 (默认 IP, 用户可自行配置, 该 IP 对应网闸后置机 LAN1 口)→轻按 Enter 键出现如下图所示安全提示窗口:



A. 数据安全交换平台默认标配 6 个后置机网口, (后置机 LAN1 默认 IP 地址: 192.168.1.1、后置机 LAN2 默认 IP 地址: 192.168.2.1、后置机 LAN3 默认 IP 地址: 192.168.3.1、后置机 LAN4 默认 IP 地址: 192.168.4.1 并以此类推, 如有 LAN7 以及更多, IP 地址按照规律递增); 可以使用后置机所有网卡登录配置界面。

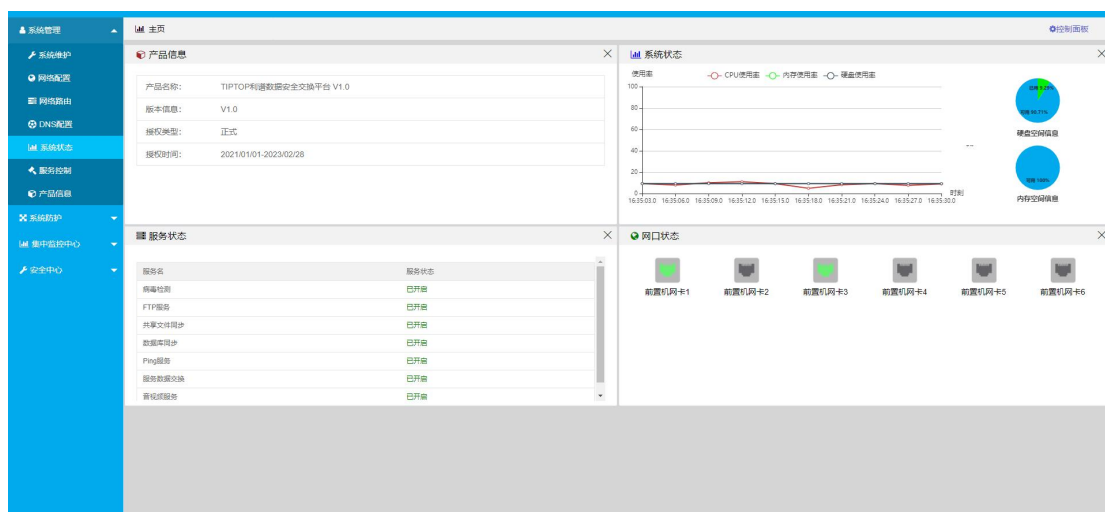
点击【继续浏览此网站 (不推荐)】出现如下图所示登录界面:



图示说明：

- 帐号：admin（系统管理员），adminsafes（系统保密员），adminaudit（日志审计员）
- 密码：Admin123456（三个角色默认密码相同）
- 登录：登录系统

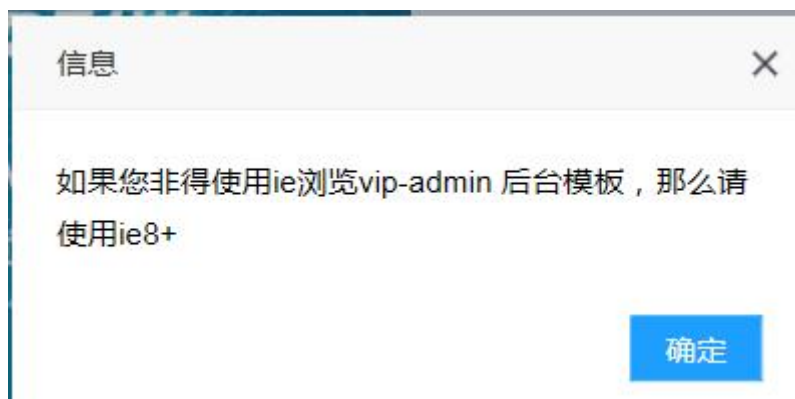
这里我们选择前置机的 admin 账号进行登录，输入账号密码登录后界面如下图所示：



欢迎页为系统状态展示页，此页面可以看到产品信息、系统资源使用图表、服务状态以及网口状态显示。

2.5 常见问题

1. 如果登录时提示下图情况，是因为使用了“兼容性视图”打开了管理地址，需要在浏览器兼容性视图设置中删除数据安全交换平台地址，重新打开即可。



2. 忘记登录用户名密码：数据安全交换平台出厂默认用户名有三个，admin、adminsafesafe、adminaudit，初始密码都是 Admin123456。

3. **关于三权分立：**

数据安全交换平台默认采用三权分立菜单，每个管理员能使用的功能不同而且互相制约，下面介绍不同管理员的权限。

admin（系统管理员）：摆渡配置、系统重启、网络配置，服务控制管理，系统信息、状态查看，系统调试和检测等。

adminsafesafe（安全保密员）：应用日志空间管理、升级和恢复出厂设置，文件同步、数据库同步、音视频交换、服务数据交换、入侵防御、双机热备策略等配置，审计员日志查看等。

adminaudit（安全审计员）：应用和其他管理员操作日志查看，日志下载和删除等。

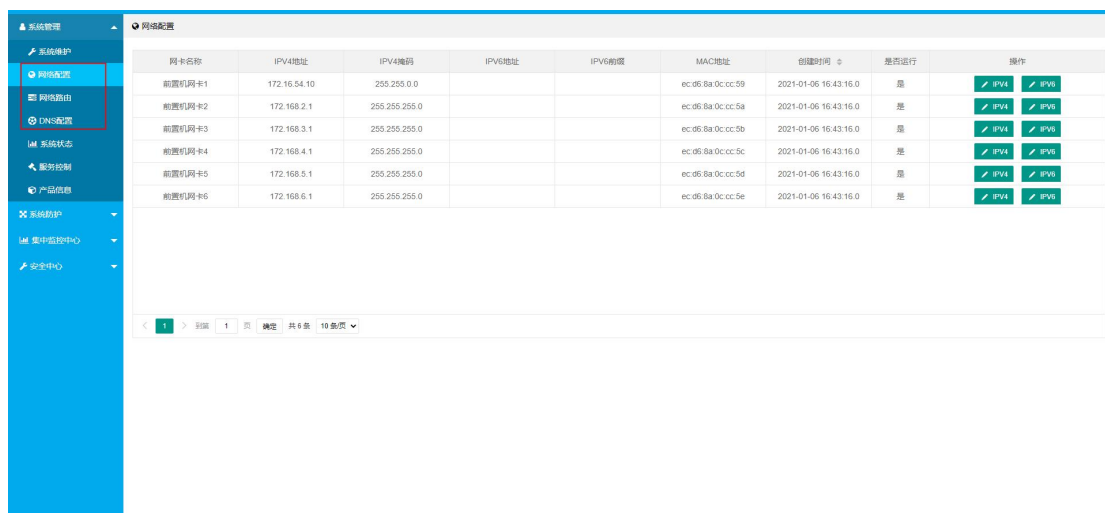
第 3 章 系统管理

本章讲解如何对系统进行配置和管理。

3.1 网络配置

admin 账号“系统管理”中，可以对网络相关进行配置，如 IPV4（暂不支持 IPV6）修改，网络路由添加，DNS 添加等。

3.1.1 IP 地址



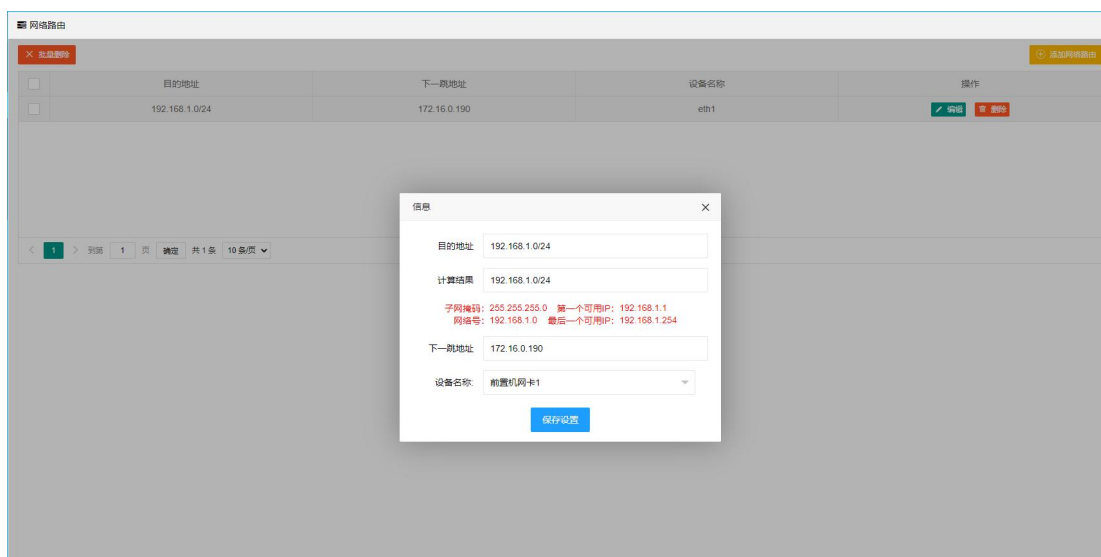
| 网卡名称 | IPV4地址 | IPV4掩码 | IPV6地址 | IPV6掩码 | MAC地址 | 创建时间 | 是否运行 | 操作 |
|-------|--------------|---------------|--------|--------|-------------------|-----------------------|------|---|
| 前置网卡1 | 172.16.54.10 | 255.255.0.0 | | | ec:05:8a:0c:cc:59 | 2021-01-06 16:43:16.0 | 是 | IPV4 IPV6 |
| 前置网卡2 | 172.168.2.1 | 255.255.255.0 | | | ec:05:8a:0c:cc:5a | 2021-01-06 16:43:16.0 | 是 | IPV4 IPV6 |
| 前置网卡3 | 172.168.3.1 | 255.255.255.0 | | | ec:05:8a:0c:cc:5b | 2021-01-06 16:43:16.0 | 是 | IPV4 IPV6 |
| 前置网卡4 | 172.168.4.1 | 255.255.255.0 | | | ec:05:8a:0c:cc:5c | 2021-01-06 16:43:16.0 | 是 | IPV4 IPV6 |
| 前置网卡5 | 172.168.5.1 | 255.255.255.0 | | | ec:05:8a:0c:cc:5d | 2021-01-06 16:43:16.0 | 是 | IPV4 IPV6 |
| 前置网卡6 | 172.168.6.1 | 255.255.255.0 | | | ec:05:8a:0c:cc:5e | 2021-01-06 16:43:16.0 | 是 | IPV4 IPV6 |

- IPV4 地址格式：首先**不能**设置为 10.0.1.x 网段，内部预留网段；其次地址格式为 4 段十进制表示，子网掩码相同，如 172.168.1.1 255.255.255.0，表示子网是 172.168.1.1-172.168.1.254。
- IPV6 地址格式：IPV6 地址为 8 段 16 进制表示，如果有连续的 0000，则可以直接用双冒号表示，如 “::”，前缀类似于 IPV4 的子网，最大 128 位，IPV6 地址示例：2001:fe80::ad16，前缀 64。双冒号省略了中间的 5 段 0000，前缀 64 表示同一子网的网段为：2001:fe80:0000:0000:xxxx。

3.1.2 网络路由

网络路由添加，需要注意的是当前没有配置默认路由入口，可以通过配置目的地址

为“0.0.0.0/0”作为默认路由，下一跳地址即为网关地址。其他网段的静态路由配置类似，在 IP 后面添加子网范围：



上图表示访问 192.168.1.1-192.168.1.254 的路由，下一跳指向 172.16.0.190。

3.1.3 DNS 配置

DNS 为域名解析服务器，根据现场用户实际的 DNS 服务器进行配置，国内运营商默认 DNS 地址为 114.114.114.114，谷歌默认 DNS 地址为 8.8.8.8。

3.2 摆渡配置

在摆渡配置中，可以对平台的进行流量控制可设置范围为：10-500mbps,同时也可以对平台的代理和监听端口进行配置，如下图：



- 网卡接口：选择业务接口。
- 目的 IP：填写下一跳代理 ip（一般为单向光闸外网 IP）。
- 发送数据端口：填写下一跳代理端口（一般为单向光闸外网监听端口）。
- 源 IP：接收数据源 IP（一般为单向光闸内网 IP）。
- 接收数据端口：设置接收数据监听端口。

3.3 日志管理

adminudit 账号“系统维护”-“日志管理”中，可以进行日志下载、上传以及删除操作。下载日志可以选择加密和非加密，上传日志只能上传加密格式的日志，防止有篡改，删除日志可以选择起止时间和日志类别进行删除。

常见问题：

1. 下载日志时页面无响应或等待很久：当系统存在大量日志，下载选择的时间跨度又比较大，那么日志下载的表格中包含日志数量很多，系统处理会出现延时或者直接无法下载的情况。
2. 下载下来的加密日志无法打开：加密格式的文件是无法打开查看的。

3.4 服务控制

admin 账号中可以对应用服务进行开关控制。应用功能需要在授权正常并且开启服务控制开关的情况下才能使用，如下图：

| 服务控制 | | | |
|--------|------|-----------------------|--|
| 服务名称 | 服务开关 | 授权期限 | |
| 病毒检测 | 开 | 2021/01/01-2023/02/28 | |
| FTP服务 | 开 | 2021/01/01-2023/02/28 | |
| 共享文件同步 | 开 | 2021/01/01-2023/02/28 | |
| 数据库同步 | 开 | 2021/01/01-2023/02/28 | |
| Ping服务 | 开 | 2021/01/01-2023/02/28 | |
| 服务数据交换 | 开 | 2021/01/01-2023/02/28 | |
| 音视频服务 | 开 | 2021/01/01-2023/02/28 | |

给需要开启的服务打开开关后即可使用，同时为了避免占用系统资源，不适用的服务建议保持关闭，需要用到时再打开。最右侧一列是系统授权时间，只有在授权范围内才可以正常使用。

3.5 日志空间设置

在 adminsafe 账号，“其他设置” - “日志空间设置”中，可以对日志占用空间、告警百分比以及保存天数等进行设置。在用户没有特殊要求的情况下，保持默认即可。

其他配置

日志空间设置

日志空间大小

4096

MB (已使用: 0MB)

告警百分比

80

%

☐ 日志空间达到告警阈值自动逐条覆盖

日志留存天数

180

天

☐ 日志扫描时间间隔

1800

分钟

☒ 日志扫描时间点

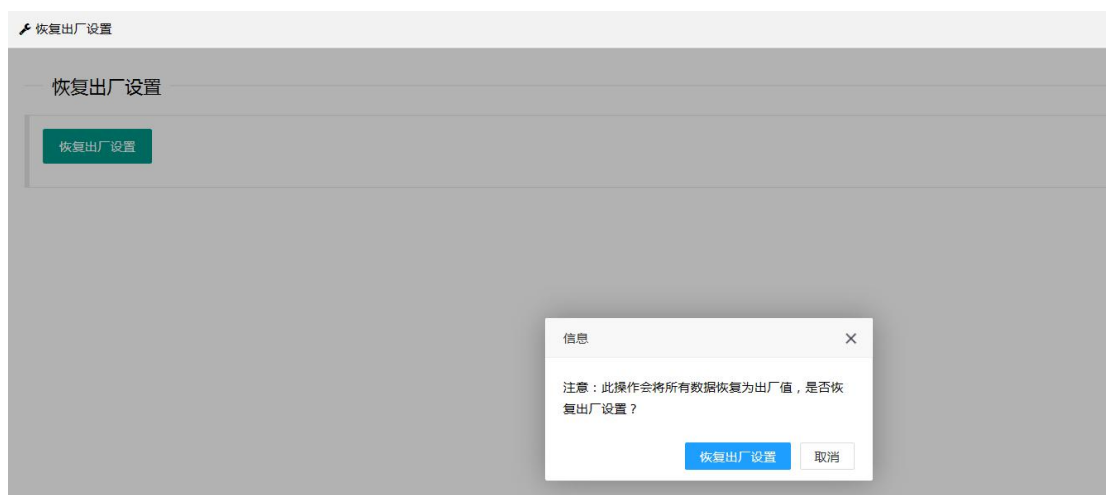
02:00:00

间隔天数: 1 天

保存设置

3.6 恢复出厂设置

adminsafe 账号中，恢复出厂设置可以对系统进行初始化，但要注意的是，**IP 地址不会恢复默认，保持恢复前的 IP**，其他的应用任务配置会被清空，如果需要保留，请先导出对应的配置。

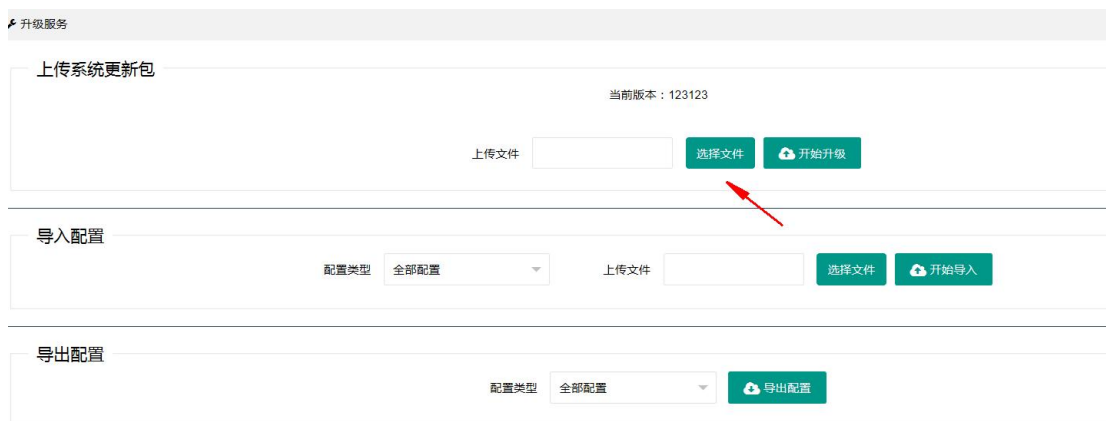


3.7 升级服务

adminsafesafe 账号中，目前升级服务仅支持部分应用的 WEB 入口升级，并且需要技术支持部提供专用的升级包。

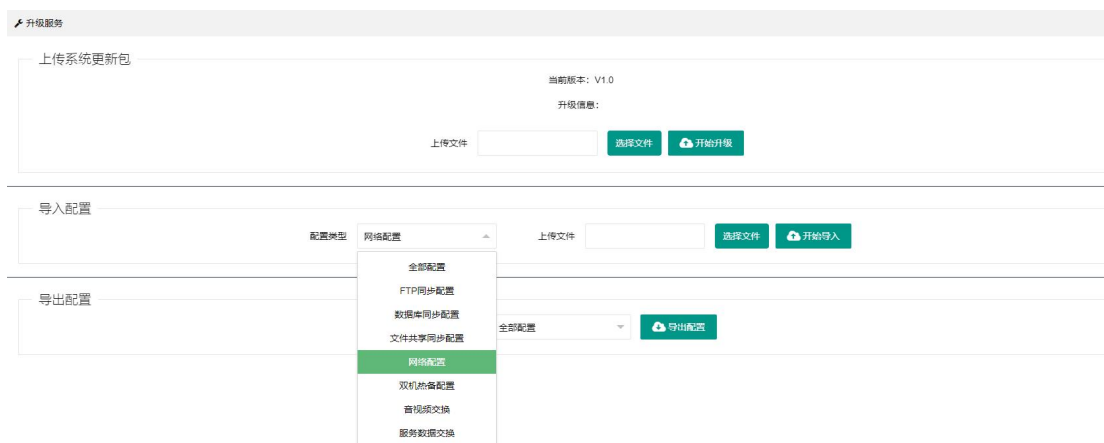
3.7.1 应用升级

在“升级服务”中，点击“选择文件”，选择研发中心发布的升级包，点击“开始升级”，等待提示升级成功后即表示升级成功。



3.7.2 导出配置

导出配置可以选择单个应用配置导出或者全部配置导出，目前可选的单个应用配置如下：



导出的全部配置包含上面图片中的单个应用配置。

注意：后置机导出的配置会带“out”标志，如 exportAll_out.zip、netWork_out.zip

表示前置机导出的配置，后置机导出的配置会带“in”标志。

3.7.3 导入配置

同导出配置章节，针对导出的配置可以选择性的导入。

同导出配置注意事项，导入配置时，选择标志与当前系统对应的配置文件进行导入，如前置机选择带“out”的配置文件导入，后置机选择带“in”的配置文件导入，否则会提示“上传的文件有误”。

3.8 系统调试

admin 账号中，系统调试工具可以简单的判断网络环境是否正常，配置入口：“系统防护” - “系统调试”，选择对应的工具及网口，输入参数，点击测试，会在下方的空白区域返回调试命令的结果，一下介绍命令用法：

- traceroute：路由跟踪命令，用来检测发出数据包的主机到目标主机之间经过的网关数量。使用方法：在参数中直接输入目标主机 IP 即可，或者输入-m 3 ip，指定存活数值=3，超过 3 跳便取消数据包。

- telnet: 检查 tcp 端口连通性。telnet 不用选择网卡, 直接输入目标主机 IP 和端口 (空格隔开), 点击测试即可。如果连通成功, 会显示 “Connected to xxx” 字样, 如果连接失败, 会显示 “Connection refused” 或者 “Connection fail”。
- ping: 可以检查网络是否通畅, 选择对应网卡, 输入目标主机 IP 点击测试。如果测试不通, 首先排除目标主机是否开启 ping 服务, 其次排查网络连接或者防火墙。
- arp: arp 提供查询本机对应网卡的 arp 信息, 信息包含主机 IP 和 MAC 地址, 如果出现有 arp 但是网络不通, 那么要确认目标主机的 MAC 是否与本机 arp 学习到的 MAC 是否一致, 不一致的情况下, 需要目标主机回包的 MAC 是否正确。
- tcpdump: linux 抓包命令, 目前调试仅支持输入 host 参数, 如 host 172.16.1.1, 暂不支持其他参数 (port 等), 测试开始后, 点击停止, 然后点击下载抓包文件, 使用 windows 的 wireshark 打开查看。

3.9 系统检测

admin 账号中, 可以进行硬件以及文件系统的检查, 检查过程中不能切换页面, 否则检测结果不会生成。具体内容见页面检测输出。同时还可以下载周期性检测报告, 相当于下载系统 messages 日志文件。

3.10 系统重启

设备支持从 WEB 重启和硬件开关重启, admin 账号中, “系统管理” - “系统维护” 中, 点击重启网闸。如果需要硬件重启设备, 请先停止所有服务。

3.11 系统状态

admin 账号中, “系统管理” - “系统状态”, 可以查看到当前系统的运行 CPU 等使用情况, 以及网口连接状态、服务控制开启状态和产品信息。如用户需要提供相关截图,

可在这里提供。

3.12 病毒库设置

在 admin 账号中-“系统防护”-“病毒库设置”，可以查看当前病毒库信息以及可以手动升级病毒库，升级步骤如下：

1. 使用能连接互联网的电脑，打开网址“<http://www.clamav.net/downloads>”，找到“Virus Database”，依次点击“main.cvd”“daily.cvd”“bytecode.cvd”进行下载。
2. 下载完成后，把三个病毒库文件拷贝至可以登录数据安全交换平台 WEB 的电脑上，进入“系统防护”-“病毒库设置”，点击上传病毒库，分别上传三个病毒库文件，上传成功后即可显示最新的病毒库信息。

3.13 安全设置

在 admin 账号中，安全设置可以对密码过期时间、登录失败最大次数、失败后锁定时长、空闲退出时间等进行配置，如果用户有特殊需求，按照用户要求进行配置，一般情况下保持默认即可。

单向数据安全交换平台视频网闸功能，用于和双向网闸组成“信令双向码流单向”功能，不能单独使用。

adminsafesafe 账号中，“其他设置”-“视频网闸配置”中，选择管理网口以及输入开放端口，点击保存，之后便可在双向网闸视频网闸配置中添加数据安全交换平台对应网口的 IP 和端口，可以成功连接数据安全交换平台。

3.14 双机热备

热备配置需要在 adminsafesafe 账号中“高可用功能”进行，下面介绍基本配置和常见问题。

3.14.1 热备基本配置

单向数据安全交换平台热备配置只需要在前置机进行配置，后置机无需配置。配置图如下：

| 网卡接口 | 虚拟IP | 子网掩码 | ICMP检测IP | 应用ICMP检测 | 操作 |
|------|------|------|----------|----------|----|
| 无数据 | | | | | |

本机 物理机: 1 优先级: 1258 心跳口网卡: 网卡1 心跳口IP(前置机): 172.168.1.1

热备机 物理机: 2 优先级: 1258 心跳口网卡: 网卡1 心跳口IP(前置机): 172.168.1.1

全部提交

配置解析：

1. 组 ID：两台设备组成热备的组 ID，相同则能进行热备。
2. 热备状态：量灯的是当前本机，可以展示优先级和当前热备机状态。
3. 添加后置机：添加后置机的业务虚拟 IP 和选择对应网卡。
4. 添加前置机：除了添加业务虚拟 IP 和选择网卡外，还可以配置 ICMP 检测功能开关以及配置检测目标 IP。
5. 本机：物理机数值是配置优先级，优先级越高，则优先抢占为主机；心跳口网卡，选择心跳网卡，可以直接带出当前 IP，不用输入。
6. 热备机：配置对端机的优先级，以及选择对端机心跳网卡和手动输入心跳 IP。
7. 全部提交：配置完成后点击全部提交，才会生效当前配置并发送到后置机端。

3.14.2 常见问题

- 热备模式默认只有抢占模式，即优先级高的主机正常情况下会抢占为主机。
- 无法获取到热备机状态：检查心跳口连接和 IP 是否配置正确。

- 热备切换后服务接管问题：热备切换后，业务虚拟 IP 切换到另外一台数据安全交换平台上，对于相同的 IP 来讲，MAC 地址发生了改变，部分网络交换机会认为 arp 欺骗从而丢弃了 arp 广播。研发已经针对该问题做了多次发出 arp 广播，如果还有该情况发生，则需要修改对端机的热备的任务虚拟 IP，使两台 IP 不同，切换后不会被交换机丢弃 arp 广播。
- 配置同步问题：当前版本取消了同步配置到热备机，需要**手动导出**具体的任务配置后导入到另外一台数据安全交换平台上（前后置机分开导出和导入）。
- 支持功能：所有应用都可以支持。

第 4 章 同步功能配置

本章将对文件、数据库同步进行配置讲解。

单向数据安全交换平台的所有应用策略配置只需要在**外网进行配置**，并且需要填入后置机的相关信息，保存后会自动发送到后置机端。

启动任务时，请先启动后置机任务，再启动外网；停止时请先停止外网，再停止后置机。目的是为了防止外网先启动或后置机先停止导致的数据丢失。

4.1 FTP文件同步

FTP 同步，是基于 FTP 共享服务器的文件单向传输功能，并且可对文件类型和关键字、病毒进行过滤拦截，同时提供三种同步模式选择。

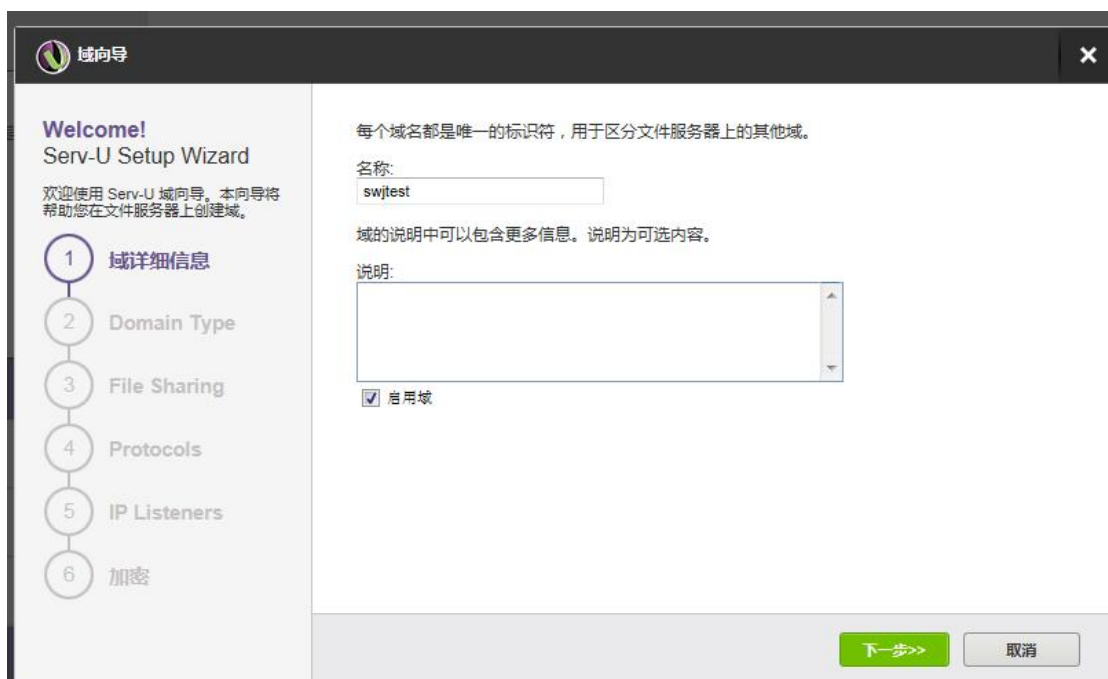
4.1.1 FTP 账号的基本要求

FTP 服务器账号，需要有账户根目录的读写权限，否则会出现任务启动成功，但是同步失败的问题。

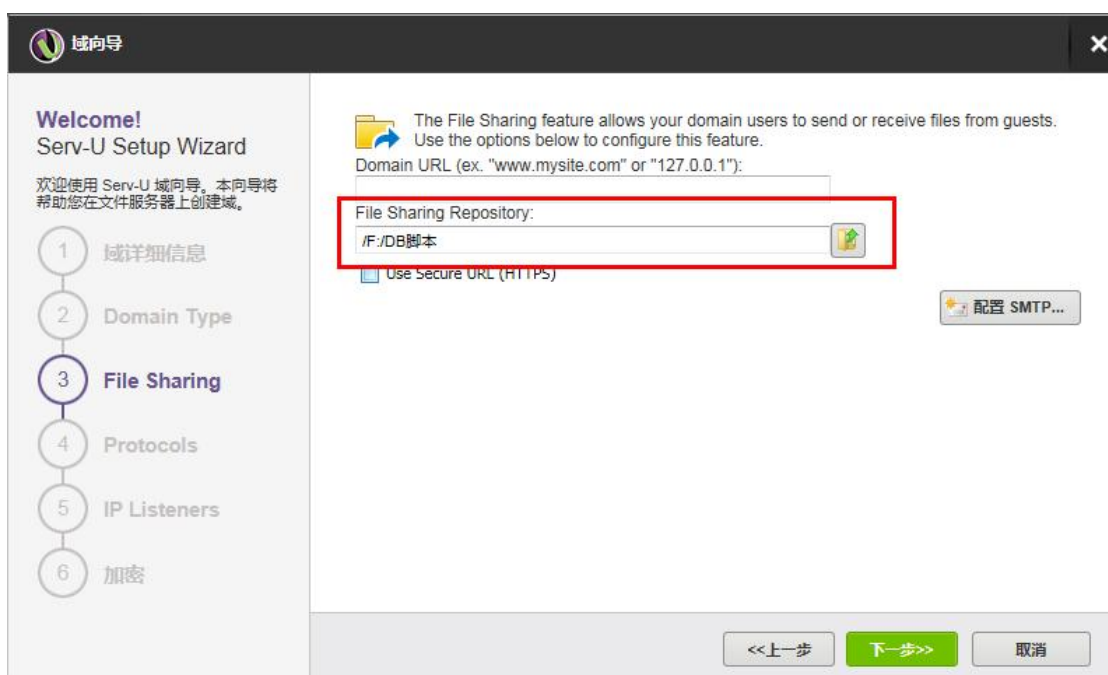
4.1.2 FTP 服务器环境搭建

1. windows 下的服务器搭建：

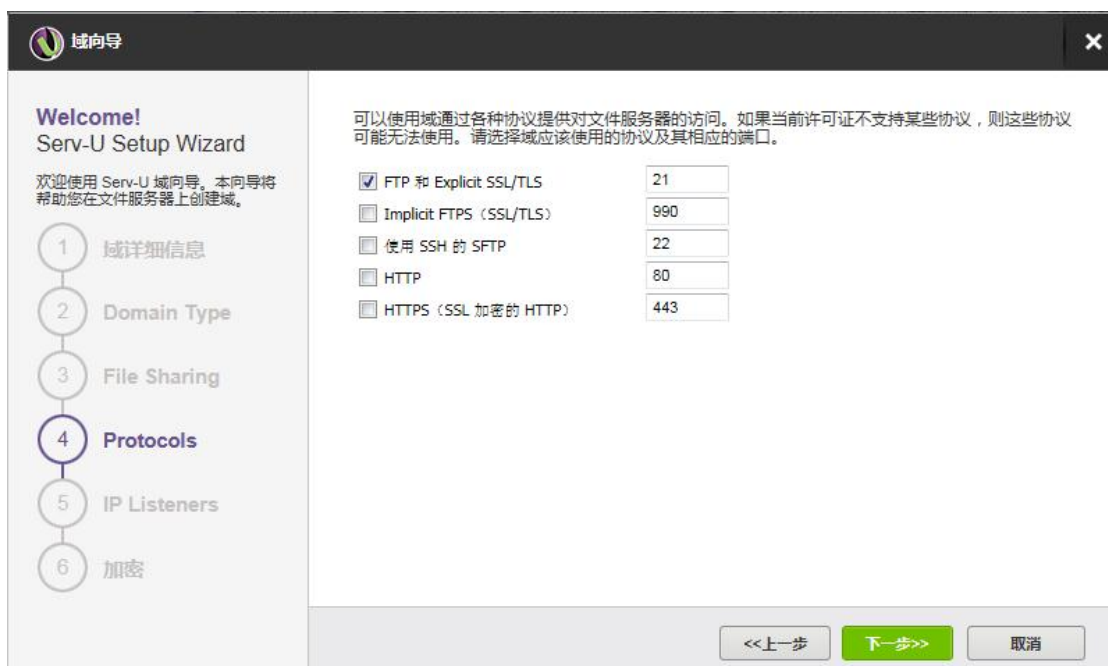
1) 运行 serv-u 管理控制台，点击“新建域”，输入域名称，点击下一步



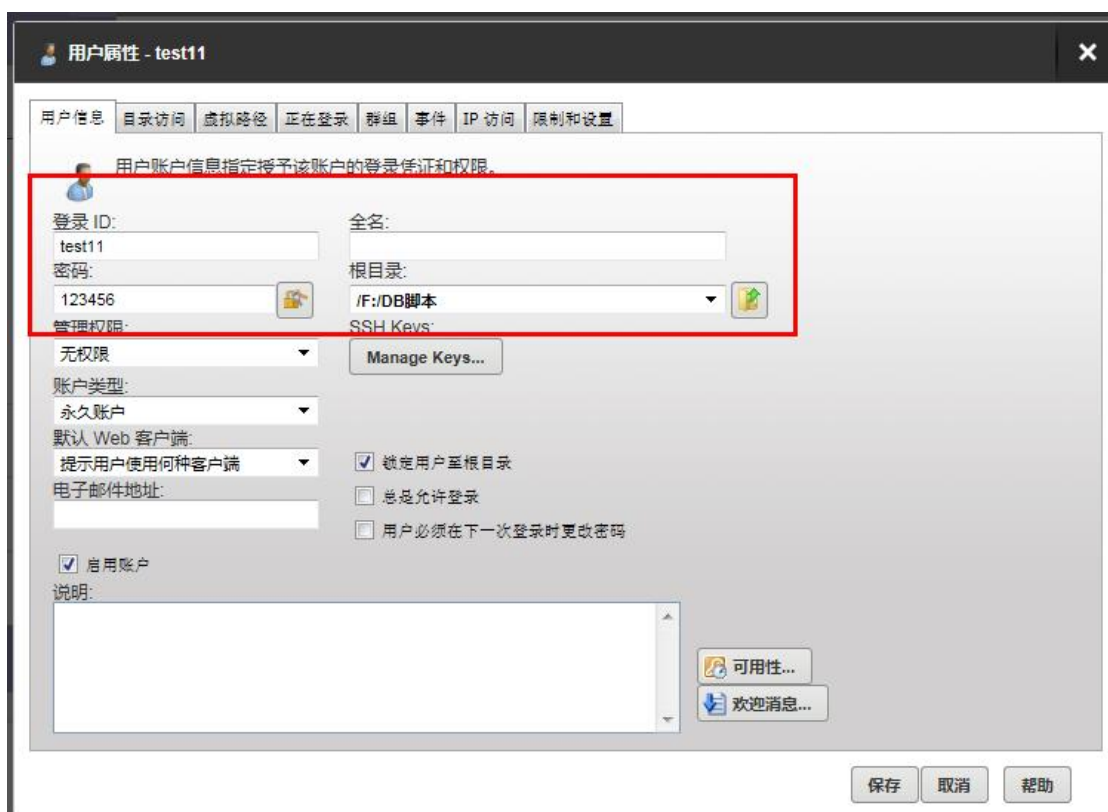
- 2) Domain Type 选择默认，点击下一步
- 3) 选择共享文件路径，domain URL 输入 127.0.0.1，点击下一步



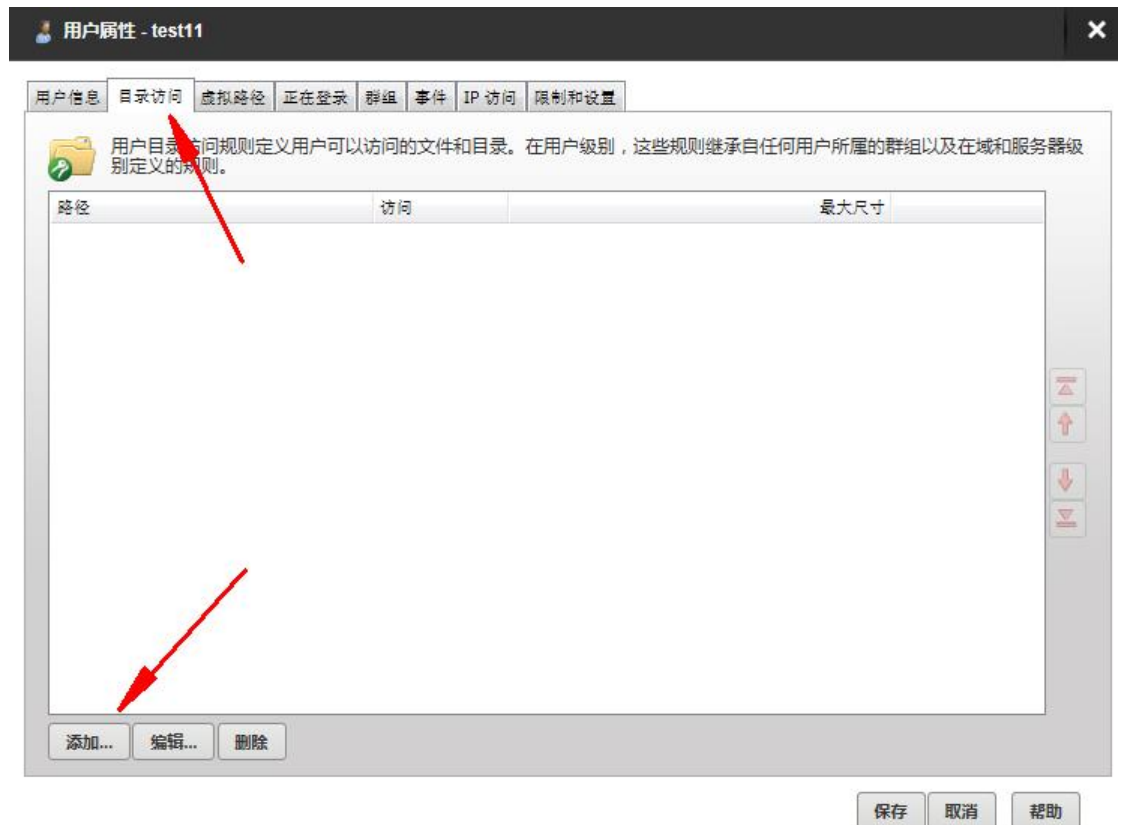
- 4) Protocols 只选择 “FTP 和 SSL/TLS”，其他去掉勾选



- 5) 选择监听 IP，保持默认或者根据用户要求进行配置。
- 6) 加密设置保持默认，点击完成。
- 7) 添加账号，输入用户名和密码，选择根目录（根目录只能选择域配置时绑定的域目录，可以在域的根目录下面创建子目录进行对应）

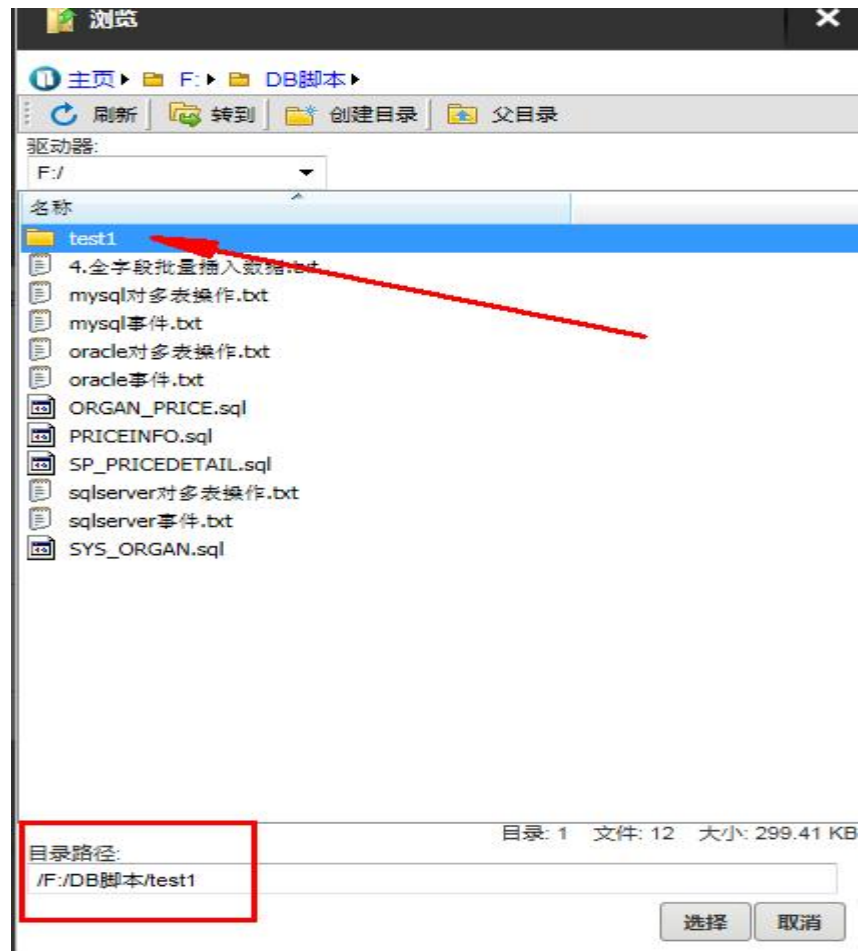


8) 点击目录访问导航，点击添加



9) 选择目录





给与完全访问权限，并保存



最后再点击保存，至此用户创建成功，可以测试用户是否可以登录和权限。

2. linux 下 vsftpd 环境搭建:

linux 下使用命令安装 vsftpd 服务, 主要的问题是在于配置文件中的配置以及系统防火墙开放 FTP 端口, 一下以 centos8 为例, 配置图如下

```
[root@localhost ~]# cat /etc/vsftpd/vsftpd.conf |grep -v "#"  
anonymous_enable=NO  
local_enable=YES  
write_enable=YES  
local_umask=022  
dirmessage_enable=YES  
xferlog_enable=YES  
connect_from_port_20=YES  
xferlog_std_format=YES  
chroot_local_user=YES  
allow_writeable_chroot=YES  
listen=YES  
listen_ipv6=NO  
  
pam_service_name=vsftpd  
userlist_enable=YES
```

主要是添加 `chroot_local_user=YES` 和 `allow_writeable_chroot=YES` 这两行。配置完成之后需要添加 FTP 用户, 如 `useradd ftp1` (新增用户 ftp1), `passwd ftp1` (回车后输入密码)。创建目录, 并修改 ftp1 账户绑定目录:

```
mkdir /srv/ftp/ftp1 ----创建目录
```

```
chmod 755 /srv/ftp/ftp1 ----赋予执行权限
```

```
chown ftp1:ftp1 /srv/ftp/ftp1 ----修改目录所有者为 ftp1 账户
```

```
vi /etc/passwd
```

```
修改 ftp1:x:1004:1004::/home/ftp1:/bin/bash
```

```
改为 ftp1:x:1016:1016::/srv/ftp/ftp1:/bin/bash
```

最后重启 vsftpd 服务, `systemctl restart vsftpd`。重启后使用 `systemctl status vsftpd` 查看运行状态。

4.1.3 任务配置

任务配置之前, 首先需要在 admin 服务控制中, 开启 FTP 服务 (下同, 开启对应服

务), 开启服务控制后, 进入 adminsafe 页面- “数据交换” - “FTP 同步”, 点击添 “添加任务”, 输入任务信息, 如下图所示:

信息

任务名

请输入

基本配置

高级配置

内网FTP服务器

IP

请输入

端口

请输入

账号

请输入

密码

请输入

服务器模式

被动模式

服务器编码

UTF-8

外网FTP服务器

IP

请输入

端口

请输入

账号

请输入

密码

请输入

服务器模式

被动模式

服务器编码

UTF-8

同步类型

☒ 周期同步

1

分

☐ 定时同步

请选择定时时间

☐ 时间段同步

请选择定时时间段

同步模式

☒ 先镜像后增量

☐ 增量同步

☐ 镜像同步

确认提交

- 任务名：用于区分同步策略。
- 后置机 FTP 服务器：数据安全交换平台后置机端 FTP 服务器信息。
- IP：FTP 服务器 IP 地址，可输入 IPV4 或者 IPV6。
- 端口：FTP 服务器端口，默认是 21。
- 账号密码：FTP 服务器提供的账号和密码，用于下载和上传文件。
- 服务器模式：数据传输模式分为主动和被动模式，主动模式默认使用 20 端口，被动模式端口可以自由配置。
- 服务器编码：推荐服务器编码设置为 UTF-8，如果不是，请选择对应服务器编码，否则会出现同步后名称乱码的情况。
- 同步类型：可选择三种类型，周期同步（同步时间间隔），定时同步（设置定时启动任务），时间段同步（配置时间段内同步）。

- 同步模式：先镜像后增量同步首先会把任务启动时源服务器存在的文件镜像同步一次，然后再同步新增的文件；其他模式参考镜像和增量部分。
- 高级功能：可开启“同步完删除文件”、“同步完删除文件夹”、“病毒检测”和关键字过滤等功能。

4.1.4 常见问题

1. 任务启动异常：任务提示启动异常，大多数情况是 FTP 服务器连接异常或者账号密码错误导致，请检查任务配置信息是否正确。
2. 运行正常但是不同步：可能是后置机账号没有读写权限导致文件无法上传。

4.2 SMB文件同步

提供功能类似 FTP 同步，只是共享协议不同。文件同步默认共享端口 445，并且任务配置支持端口自定义输入。

4.2.1 共享账号基本要求

权限要求需要读写权限，账号**不能有中文**，只支持英文账号。

4.2.2 SMB 服务器搭建

1. windows 下搭建 SMB 服务器：

创建文件夹，右键属性，点击“共享”，设置共享名称和选择共享账户，再点击高级共享-共享此文件夹，在权限中添加账号，并给与读写权限。

如果没有显示账号，点击权限-添加-高级-立即查找，即可找到对应的账号，点击添加。

2. linux 搭建 SMB 服务器

安装有 SMB 服务方法有很多，这里简单介绍 yum 安装，前提是安装服务器主机可以连接互联网。

a) `yum -y install smb` # yum 安装 smb 服务（没有指定版本，默认安装最新版本）

b) 配置 `smb.conf`

`--[global]`

`workgroup = WORKGROUP` #工作组

`security = user` #需要认证

`netbios name = 172.16.1.33`

`passdb backend = tdbsam`

`printing = cups`

`printcap name = cups`

`load printers = yes`

`cups options = raw`

`log file = /var/log/samba/log.%m` # 日志位置

`smb ports = 445` # 端口

`--[in1]`

`comment = usershare`

`path = /srv/samba/in1` # 共享路径

`unix charset = UTF-8`

`valid users = in1` # 限制只允许 in1 用户访问

`public = no`

`writable = yes` # 读写

`browseable = yes` # 工作组可被发现

`guest ok = yes`

c) 添加系统用户

`--useradd share1`

`--passwd share1` # 输入用户密码，此密码是系统用户密码，不是 samba 共享密码

d) 添加 samba 共享组，以及把共享账号加入该组

```
--groups -g 888 samba
```

```
--gpasswd -a share1
```

e) 设置 samba 共享密码

```
--smbpasswd -a share # 不加-a 参数可能会配置失败
```

f) 修改共享目录权限

```
--chown -R share1:samba /srv/samba/in1
```

```
--chmod -R 777 /srv/samba/in1
```

g) 关闭 linux 防火墙

--需要关闭 iptables 和 firewalld，根据实际情况而定。可用命令：service

iptables stop, setenforce 0 等，centos8 使用 systemctl disable firewalld.service

关闭防火墙，或者防火墙放行 smb 端口。

h) 重启 smb 服务

```
--systemctl restart smb
```

i) 使用 windows 测试共享目录访问，或者用 linux 来 mount 测试共享目录

windows 直接打开文件夹，在路径输入共享主机 IP，弹框输入用户名密码即可。

linux 使用 mount 命令测试挂载：

```
mount -t cifs -o username=administrator,password='tiptop' //hosttip/smb_out  
/tmp/in2
```

4.2.3 任务配置

任务配置之前，首先需要在 admin 服务控制中，开启文件共享同步服务（，开启服务控制后，进入 adminsafe 页面- “数据交换” - “文件共享同步”，点击添 “添加任务”，输入任务信息，如下图所示：

信息

×

任务名 请输入

基本配置

高级配置

内网共享参数

传输协议 SMB

文件夹 请输入共享文件夹名

IP 请输入共享IP

账号 请输入用户名

密码 请输入密码

服务器编码 无需选择

外网共享参数

传输协议 SMB

文件夹 请输入共享文件夹名

IP 请输入共享IP

账号 请输入用户名

密码 请输入密码

服务器编码 无需选择

同步类型

☒ 周期同步

1 分

☐ 定时同步

请选择定时时间

☐ 时间段同步

请选择定时时间段

同步模式

☒ 先镜像后增量

☐ 增量同步

☐ 镜像同步

确认提交

- 任务名：同步策略名称，用于区分。
- 传输协议：可选 SMB 和 NFS，这里讲解 SMB 协议。
- 文件夹：共享文件夹名称，如果是 windows 共享服务器，只需要输入共享名称，不能输入绝对路径。
- 账号密码：FTP 服务器提供的账号和密码，用于下载和上传文件。
- 同步类型：可选择三种类型，周期同步（同步时间间隔），定时同步（设置定时启动任务），时间段同步（配置时间段内同步）。
- 同步模式：先镜像后增量同步首先会把任务启动时源服务器存在的文件镜像同步一次，然后再同步新增的文件；其他模式参考镜像和增量部分。
- 高级功能：可开启“同步完删除文件”、“同步完删除文件夹”、“病毒检测”和关键字过滤等功能。

4.2.4 基本问题处理方法

1. windows 搭建的 smb 服务器，底层挂载是出现报错：cannot allocate memory

解决方法为：在 windows 电脑上，管理员权限运行 cmd，执行

Set

"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\IRPStackSize" DWORD 18

Set "HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\LargeSystemCache" to "1"

Set "HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\Size" to "3"

然后重启电脑即可。

2. linux 下 SMB 服务器无法同步

SMB 服务器无法同步，分为两个方面：一个是挂载不了，一个是文件同步异常。

无法挂载可能是版本不匹配或者账号信息不对，在确认环境信息没错的情况下，需要收集 SMB 服务版本，目前同步程序能够最高支持到 SMB 4.8 版本，超过 4.8 版本无法挂载。

文件同步异常基本上是账号权限配置的问题，首先检查 smb.conf 配置文件是否正确，其次检查账号是否有读写权限。

4.3 NFS文件同步

同步功能类似 SMB 协议。NFS 同步默认端口是 111，同步异常时先检查端口是否可以访问。

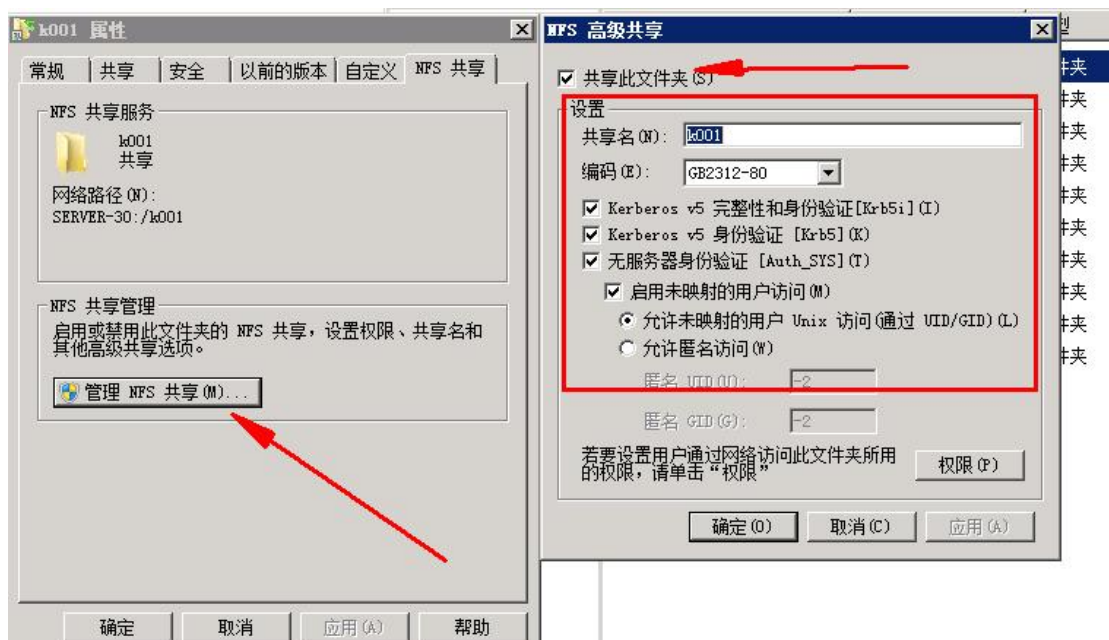
4.3.1 共享要求

NFS 共享是网络文件系统，挂载时不需要账号密码。数据安全交换平台配置时用户名密码可以随意输入（当前版本要求不能为空，但实际不起作用）

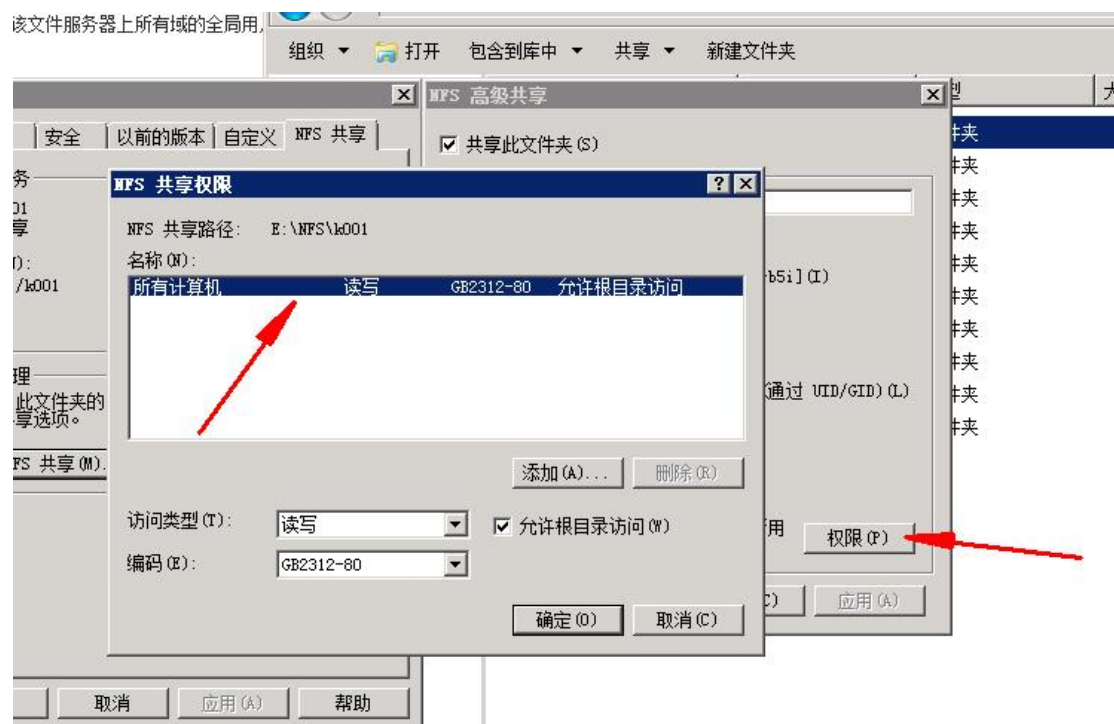
4.3.2 NFS 服务器搭建

1. windows NFS 环境搭建:

win7 及以上只提供了 NFSclient 功能，NFS server 必须在 window server 版本中使用，如 winserver 2008 等。



基本配置如上图，设置共享名称以及编码格式。



权限配置如上图，需要给与读写权限。

2. linux NFS 服务器搭建

a) 安装 NFS 服务（需要连接互联网）

```
yum -y install nfs-utils rpcbind
```

b) 在 NFS 服务端上创建共享目录/srv/nfs/in1 并设置权限

```
mkdir -p /srv/nfs/in1  
chmod 666 /srv/nfs/in1
```

c) 编辑 export 文件

```
vim /etc/exports
```

新增内容

```
/srv/nfs/in1 服务器 IP(rw,no_root_squash,no_all_squash,sync)
```

d) 配置生效， exportfs -r

e) 启动 rpcbind、nfs 服务，需要关闭防火墙或者添加防火墙放行，参考 SMB。

```
service rpcbind start  
service nfs-server start
```

f) 服务器端输入 showmount -e，查看是否生效。

4.3.3 任务配置

任务配置跟 SMB 相同，需要注意的是 NFS 是匿名共享协议，不需要提供账号和密码，这里任务配置中的账号密码**输入随意字符即可**。

4.3.4 基本问题处理方法

主要故障与 SMB 类似，网络连接和读写权限等问题，参考 SMB 处理方法。

测试命令：

```
mount -t nfs -o nolock 172.16.80.15:/nfs_out1 /mnt/test
```

正常挂载，执行 mount 命令可以看到挂载目录：

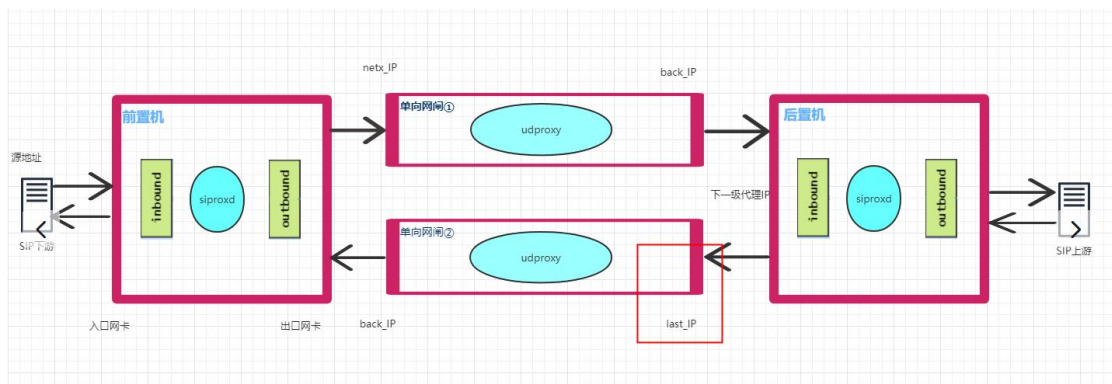
```
172.16.4.90:/nfs_out1 on /mnt/test type nfs (rw,nolock,addr=172.16.4.90)
```

挂载失败：

mount.nfs: mounting 172.16.4.90:/nfs_out failed, reason given by server: No such file or directory (共享目录不存在)

4.4 音视频交换 (6机模式不支持此功能)

本模块 (siproxd) 前置机 siproxd 处理来自 sip 下游服务器的 sip 信令并将它们转发到单向网闸①上面, 单向网闸①通过 udp 代理将 sip 信令再转发到后置机上面, 再通过后置机的 siproxd 转发到对应的 sip 上游服务器上, 后置机处理逻辑类似, 这样就完成了 sip 信令的 register, invite 等交互过程, 达成了音视频数据交换的目的, 如下图。



4.4.1 音视频交换配

音视频交换

参数配置

基础配置 (必填)

| | | | | | |
|----------|-------------|---------|----------|---------|-----------|
| 机位选择 | 请选择机器位置 | 入口网卡 | 请选择入口网卡 | 出口网卡 | 请选择出口网卡 |
| 代理监听端口 | 请输入代理监听端口 | 源IP地址 | 请输入源IP地址 | NEXT_IP | 请输入IP地址 |
| BACK_IP | 请输入IP地址 | LAST_IP | 请选择机位 | 下级代理端口 | 请输入下级代理端口 |
| 下级代理IP地址 | 请输入下级代理IP地址 | | | | |

服务黑名单配置

| 用户代理 | Media Format | MIME TYPE | 操作 |
|------|--------------|-----------|----|
| 无数据 | | | |

刷新 保存参数

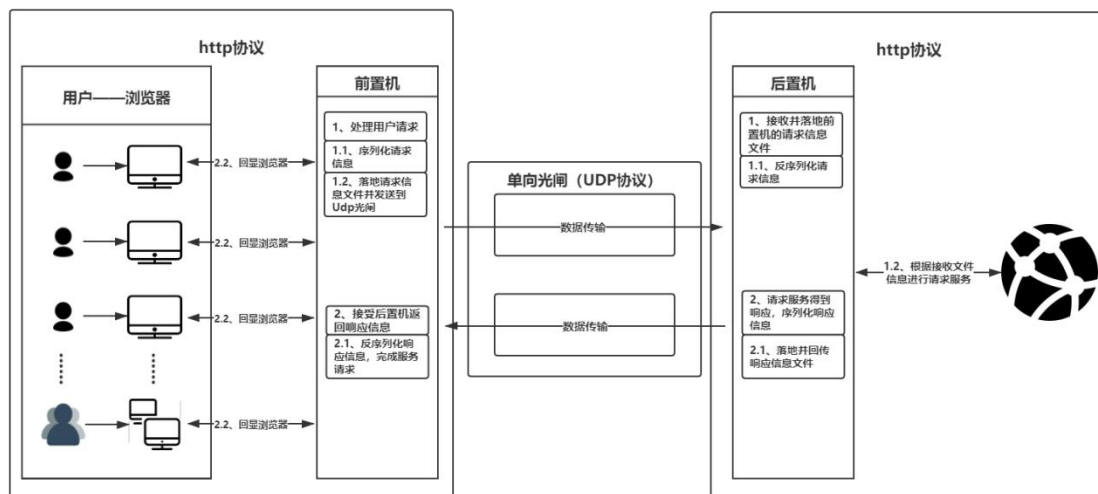
- 机位选择: 选择机器位置 (一级代理和二级代理)。
- 入口网卡: 选择与下游服务连接的入口网卡。

- 出口网卡：选择代理出口网卡。
- 代理监听端口：填写本机监听端口。
- 源 IP 地址：填写下游服务器地址。
- NEXT_IP：填写数据安全交换平台 1 外网 IP。
- BACK_IP：填写数据安全交换平台 2 内网 IP。
- LAST_IP：填写数据安全交换平台 2 外网 IP。
- 下级代理端口：填写下级代理的端口。
- 下级代理 IP：填写下级代理 IP。

4.5 服务数据交换(6机模式不支持此功能)

实现 http 访问代理功能。

4.5.1 业务流程图



4.5.2 配置说明

服务数据交换配置

服务数据交换配置

网卡接口: 网卡1 *

最大响应时间(秒): 30 *

下一跳代理地址: 172.16.54.11 *

服务监听ip: 172.16.54.11 *

http代理端口: 80 *

下一跳代理端口: 2222 *

服务监听端口: 2223 *

保存设置

- 网卡接口：选择业务网卡。
- 最大响应时间：设置服务器最大响应时间。
- http 代理端口：目的服务器代理端口。
- 下一跳代理端口：填写数据安全交换平台外网监听的端口。
- 下一跳代理地址：填写数据安全交换平台外网业务 IP。
- 服务监听 IP：填写本机监听 IP。
- 服务监听端口：添加本机监听端口。

4.6 数据库同步

4.6.1 网闸支持的数据库类型及版本

数据交换平台 v1.0 版本支持同步的数据库及版本如下：

| 数据库类型 | 版本 | 备注 |
|-------|----------|--|
| Mysql | 5.7, 8.0 | 默认是 5.7 都能支持,8.0 需要选择对应版本。其他版本（如 5.1）等，可能需要研发对应添加驱动。 |

| | | |
|-----------|-------------------------------|---------------|
| Sqlserver | 2005,2008,2012,2014,2016,2017 | 选择使用最新驱动，向下兼容 |
| Oracle | 10g,11g,12c | 选择使用最新驱动，向下兼容 |
| 达梦 | V7 | 各自只支持一个版本 |
| Kingbase | Kingbase V7 | |
| Gbase | V8.8 | |

4.6.2 账号基本要求

能够访问数据库，并且有创建触发器权限。

4.6.3 配置方法

服务控制开启“数据库同步”，进入 adminsafe 页面进行任务配置，**外网端只需要输入外网数据库服务器信息，配置完后再到后置机选择刚刚创建的任务信息编辑，输入后置机数据库服务器信息和选择同步表。**外网配置如下：

信息

×

任务名 test

基本配置 高级配置 同步表配置

源数据库参数

数据库 mysql 版本 默认(8.0除外)

IP 192.168.1.50 端口 3306

用户 root 密码

数据库名/SID test

目的数据库参数

数据库 mysql 版本 默认(8.0除外)

IP 请输入IP 端口 请输入端口

用户 请输入用户 密码 请输入密码

数据库名/SID 请输入数据库名/SID

同步模式

☒ 周期同步 10 秒 ☐ 定时同步 定时时间 ☐ 时间段同步 时间段

同步方式

☒ 先镜像后增量 ☐ 增量同步 ☐ 镜像同步 ☐ 删除目的端数据

确认提交

- 任务名：用于区分策略。
- 数据库参数：源端表示数据安全交换平台外网端连接的数据库服务器参数。目的数据库表示后置机端连接的数据库服务器。
- 数据库类型：根据数据库服务器类型选择同步策略的类型，支持的数据库类型请参照 4.4.1 章节。
- IP 和端口：数据库服务器 IP 地址和默认开放端口。用于数据库连接。
- 用户名密码：数据库用户名和密码，用于数据库操作。
- 数据库名：需要选择同步表的数据库名称。
- 同步类型：可选择三种类型，周期同步（同步时间间隔），定时同步（设置定时启动任务），时间段同步（配置时间段内同步）。
- 同步模式：先镜像后增量同步首先会把任务启动时源服务器存在的数据镜像同步一次，然后再同步新增的数据；其他模式参考镜像和增量部分。
- 删除目的数据库：勾选后，启动任务时会先清空目的端表数据。
- 高级配置：选择冲突处理方法、同步操作选择、设置批处理量。

基本信息配置完成之后，点击“高级配置”，如无需修改，则保持默认，继续点击“同步表配置”，选择需要同步的表：

信息

任务名test

基本配置

高级配置

同步表配置

筛选当前页显示的表

| <input type="checkbox"/> | 源表 | 操作 |
|-------------------------------------|---------|-----------------|
| <input checked="" type="checkbox"/> | test002 | <div>上移下移</div> |
| <input type="checkbox"/> | test003 | <div>上移下移</div> |
| <input type="checkbox"/> | test004 | <div>上移下移</div> |
| <input type="checkbox"/> | test009 | <div>上移下移</div> |

< 1 > 到第 1 页 确定 共 13 条 50 条/页

筛选当前页显示的字段

| | |
|-------------------------------------|------|
| <input checked="" type="checkbox"/> | 源表字段 |
| <input checked="" type="checkbox"/> | id |
| <input checked="" type="checkbox"/> | num1 |
| <input checked="" type="checkbox"/> | num2 |
| <input checked="" type="checkbox"/> | num3 |

确认提交

勾选表之后点击保存，登录数据安全交换平台后置机管理页面，进入数据库配置中，输入后置机相关信息，并选择同步表（需要字段属性与源表对应），保存完成配置：

信息

任务名test

基本配置

高级配置

同步表配置

源数据库参数

数据库mysql

版本默认(8.0除外)

IP192.168.1.50

端口3306

用户root

密码

数据库名/SIDtest

目的数据库参数

数据库mysql

版本默认(8.0除外)

IP162.2.1.50

端口3306

用户root

密码

数据库名/SIDtest

同步模式

周期同步

10秒

定时同步

定时时间

时间段同步

时间段

同步方式

先镜像后增量

增量同步

镜像同步

删除目的端数据

确认提交

信息

任务名test

基本配置高级配置同步表配置

同步表选择

| 源表 | 目的表 | 操作 |
|---------|---------|-------------------------------|
| test002 | test002 | <div>编辑表</div> <div>删除表</div> |

<1>

>到第1页

确定

共1条

50条/页

同步表字段对应关系

| 源表字段 | 目的表字段 | 操作 |
|------|-------|---------------------------------|
| id | id | <div>编辑字段</div> <div>删除字段</div> |
| num1 | num1 | <div>编辑字段</div> <div>删除字段</div> |
| num2 | num2 | |

 编辑字段 删除字段 || num3 | num3 | 编辑字段 删除字段 |

确认提交

4.6.4 基本问题处理方法

1. 配置任务获取不到表信息

基本上是数据库连接有问题，出现问题首先要排查网闸到数据库端口是否通畅；异构同步问题。异构同步不成功，很多情况是源表字段长度与目的表字段长度不一致，目的端无法写入数据。这时候需要查看表结构和字段属性，针对大字段的需要查询能否支持字段长度。

2. 勾选删除同步，但是后置机数据没有删除。之前案例有出现过，原因是源表和目的表都有数据插入前的触发器，触发器会自动修改字段 ID 的值，外网删除成功，但是后置机 ID 已经发生了变化，找不到对应数据。处理方法是删除后置机的 befor insert 的触发器。

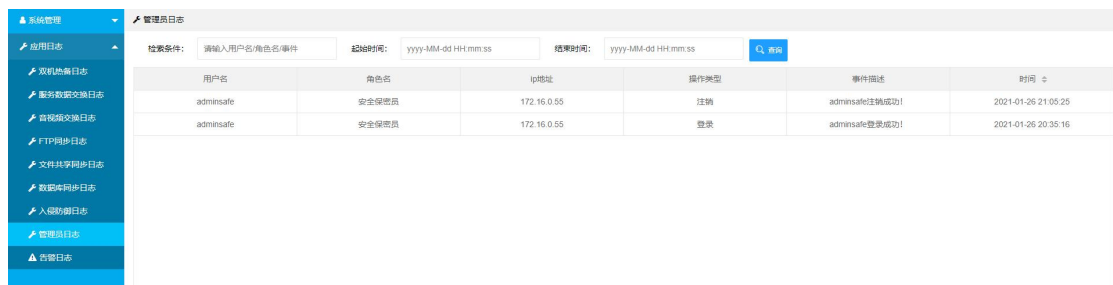
4.7 其他常见问题

同步文件并发问题：文件同步任务开启时，如果源文件堆积过多，可能会导致内存不够出现程序崩溃，目前 FTP、SMB、NFS 同步，最大支持源文件数量不超过 40 万个，

如果超过 40 万个源文件，建议任务开启时先手动备份一部分，同步一段时间后，再放入备份的文件。数据库同步，如果源表条数很多（如 1000 万等），同步程序先会把数据镜像到临时表，这个过程可能要花费一定的时间，所以同步结果可能会有延时。

第 5 章 日志篇

用 adminaudit 账号登录管理页面，可以查看数据安全交换平台常用业务相关日志记录，如文件同步、数据同步、音视频交换等。



| 用户名 | 角色名 | ip地址 | 操作类型 | 事件描述 | 时间 |
|-----------|-------|-------------|------|----------------|---------------------|
| adminsafe | 安全保密员 | 172.16.0.55 | 注册 | adminsafe注册成功! | 2021-01-26 21:05:25 |
| adminsafe | 安全保密员 | 172.16.0.55 | 登录 | adminsafe登录成功! | 2021-01-26 20:35:16 |