

伟思信安
安全隔离与信息单向导入系统
ViGap V3.0
使用说明书

版本	作者	起止日期	备注	审查
V2.0	封勇兵	2022/7/9	初次编写	陈功湖

目 录

1 系统概述.....	1
1.1 系统简介.....	1
1.2 名词解释.....	1
2 运行环境.....	2
2.1 硬件运行环境.....	2
3 安装部署.....	3
3.1 前置工作.....	3
3.1.1 设备清单检查.....	3
3.1.2 安装环境要求.....	3
3.1.3 温度及湿度要求.....	3
3.1.4 环境洁净度要求.....	3
3.1.5 静电要求.....	4
3.1.6 雷电/电磁要求.....	4
3.1.7 安装台面检查.....	5
3.1.8 安全注意事项.....	5
3.1.9 安装工具准备.....	6
3.2 设备上架.....	6
3.3 安装到水平台面.....	6
3.4 安装到标准机架.....	7
3.5 系统部署检查.....	7
4 管理操作指南.....	8
4.1 登录管理.....	8
4.1.1 准备工作.....	8
4.1.2 管理方式.....	8
4.1.3 Web 页面管理.....	8
4.1.4 CLI 管理.....	9
4.1.5 USB 管理.....	9
5 运维操作.....	9

5.1 常见故障.....	9
5.1.1 CPU 高.....	9
5.1.2 内存高.....	10
5.1.3 网络异常.....	10
5.1.4 SYLOG 日志失效.....	10
5.2 运维指南.....	11
5.2.1 日常运维.....	11
5.2.2 应急处理.....	12
5.3 注意事项.....	13
6 功能介绍.....	13
6.1 系统配置.....	15
6.1.1 系统状态.....	15
6.1.2 系统时间.....	15
6.1.3 系统维护.....	16
6.1.4 登录设置.....	18
6.1.5 备份/恢复.....	18
6.1.6 存储管理.....	20
6.1.7 系统升级.....	20
6.1.8 设备信息.....	21
6.1.9 诊断工具.....	22
6.1.10 授权验证.....	22
6.2 网络配置.....	23
6.2.1 接口配置.....	23
6.2.2 网关设置.....	26
6.2.3 静态路由.....	26
6.2.4 IP/MAC 绑定.....	27
6.3 高可用性.....	28
6.3.1 双机热备.....	28
6.3.2 虚拟 IP.....	29

6.3.3 双机热备状态.....	30
6.4 本地服务.....	30
6.4.1 通信访问控制.....	30
6.4.2 FTP 服务.....	31
6.4.3 邮件服务.....	32
6.5 数据同步.....	32
6.5.1 数据资源.....	32
6.5.2 业务注册.....	34
6.5.3 业务与服务管理.....	34
6.6 病毒库管理.....	43
6.6.1 引擎信息.....	43
6.6.2 隔离区管理.....	44
7 用户管理员操作简介.....	44
7.1 用户配置.....	44
8 日记审计员操作简介.....	46
8.1 日志与审计.....	46
8.1.1 管理操作日志.....	46
8.1.2 数据库抽取日志.....	47
8.1.3 数据库基本信息日志.....	48
8.1.4 文件同步日志.....	48
8.1.5 文件同步流量.....	49
8.1.6 通道操作日志.....	49
8.1.7 安全事件日志.....	50
8.1.8 告警日志.....	50
8.1.9 认证状态日志.....	51
8.1.10 日志管理设置.....	51
9 典型配置.....	52
9.1 通道配置(与数据交换前后置配套使用).....	52
9.2 配置数据库同步业务.....	55

9.3 配置文件同步业务.....	59
-------------------	----

1 系统概述

1.1 系统简介

伟思信安安全隔离与信息单向导入系统 ViGap V3.0 采用先进的单向光通道传输技术和 GAP 硬件隔离技术独立研制生产的新一代网络隔离与单向数据传输产品。它放置在内部网络和外部网络之间，从发送系统采集数据并通过物理单向光通道(单向光闸)传输到接收系统，接收系统到发送系统无任何反向光信号传输物理通道，既实现了数据从低密级网络传输到高密级网络的应用需求，又在物理硬件上彻底保证了内网机密数据无法泄露到外网。

ViGap V3.0 具有强大的安全特性，能够满足高度可控环境下的安全数据交换需求，主要特点包括：

- ViGap V3.0 采用安全的操作系统

ViGap V3.0 采用经过安全优化的 Linux 操作系统，该系统经过 Linux 内核裁减，卸载所有对外系统服务并重构了 TCP/IP 协议栈，保证系统安全性。同时，系统内置了防内存溢出系统，能够有效保护系统进程包括光闸数据摆渡进程运行安全，进一步强化了系统抗攻击性。为保证系统稳定可靠运行以及防范病毒、木马对光闸操作系统造成影响，系统采用了 DOM 作为存储介质并将 Linux 系统以镜像方式引导到内存扩展运行，因此系统不可能再添加新的程序、驱动及服务。

- ViGap V3.0 采用安全可靠的数据传输模式

ViGap V3.0 采用模块化设计，采用推、拉模式完成外网服务器上指定文件、数据库表、邮件等向内网的单向同步，由于内外网间仅传输纯文件级数据，不含任何控制命令，因此，数据传输安全可靠。ViGap V3.0 模块可裁减，可根据用户需要在产品生产时定制适合用户需要的特定模块组合产品。

1.2 名词解释

- 接收系统：伟思信安安全隔离与信息单向导入系统可信端组成部分，可以连接涉密网络，用来保存文件或推送文件到涉密网络的服务器。
- 发送系统：伟思信安安全隔离与信息单向导入系统非可信端组成部分，可以连接非

涉密网络，用来保存或接收来自非涉密网络的文件。

- 前台管理：使用 WEB 管理的方式，操作简单易懂，不利于批量操作。
- 后台管理：是一种管理方式，通过采用串口或 SSH 方式连接到设备的命令行界面，用提供的命令查询运行状态。
- 三权分立：通系统实现系统管理员、系统审计员和系统安全员三权分产各司其职的管理，使得对系统的管理更加安全可控，避免人为因素带来的安全风险。
- 高速通道：系统实现针对高并发、高负载的，支持集群部署的通道实现，高速通道下通常着重数据的高速摆渡，常规模式侧重数据安全性核查。
- 高可用性：通过异常处理、自身检测，自恢复、双击热备技术等保障系统本身高可用，同时系统具备故障告警能力，系统能够主动推送告警日志、开放管理接口被动采集，通过多样化的日志接口：如日志，短信等实现故障定位、故障修复的及时性，实现业务 7x24 小时不间断运行。

2 运行环境

2.1 硬件运行环境

为保证系统能长期稳定的运行，保证电源有良好的接地措施、防尘措施、保持运行环境的空气通畅和室温稳定。

系统运行环境应满足以下标准：

参数	参数值
输入	250W
温度	-10℃~50 ℃
湿度	40%~70%
电源	220V 交流电

3 安装部署

3.1 前置工作

3.1.1 设备清单检查

在确认安装环境符合要求后,打开设备包装箱并对照定货合同及装箱单仔细核对设备及附件是否齐全,如有疑问或差错请与设备销售商取得联系。

3.1.2 安装环境要求

必须安装非露天的室内环境中,为保证设备的安全运行,系统要求安装环境具备以下条件。

3.1.3 温度及湿度要求

为保证设备正常工作并延长其使用寿命,安装环境需维持一定的温度和湿度。若安装环境内长期湿度过高,则容易造成绝缘材料绝缘不良,甚至漏电;还会发生材料性能变化,金属部件锈蚀等现象。若相对湿度过低绝缘垫片会干缩而引起紧固螺丝松动;在干燥的气候环境下还容易产生静电;从而危及设备上的电路。

温度过高危害更大,因为高温会加速绝缘材料的老化过程,使设备的可靠性大大降低并严重影响其使用寿命。

设备对环境的要求如下:

- 1) 温度: $0^{\circ}\text{C} \sim 40^{\circ}\text{C}$
- 2) 湿度: 40% \sim 70% (非凝结状态)

3.1.4 环境洁净度要求

尘埃对设备的安全运行也是一个重要影响因素,因为空气中的灰尘的累积会造成静电吸附;使金属接插件或金属接点接触不良或电路短路;这一因素不但会影响设备的使用寿命,同时也容易造成通信故障。尤其是在室内相对湿度偏低时,更易产生这种静电吸附。

除尘埃外,设备对空气中所含的腐蚀性酸性气体也有严格的要求,因为这些有害气体在

一定湿度环境下会加速对金属部分的腐蚀和某些部件的老化。

因此机房内对安装环境的要求为无爆炸性、导电性、导磁性及腐蚀性气体或尘埃。具体要求请参照的相关要求或规定。

3.1.5 静电要求

尽管设备在防静电方面作了大量的设计考虑，采取了多种措施来减少静电积累；但当静电积累超过一定限度时仍会对系统电路乃至整机产生巨大的破坏作用。在与设备连接的通信网中静电感应主要来自两个方面：一是高压输电线路、雷电等外界电场；二是环境建筑及装饰材料、整机结构等。

因此系统内部为防止静电损伤应做到：

- 1) 设备及地板有良好的接地连接；
- 2) 环境防尘；
- 3) 保持适当的环境温度与湿度；
- 4) 接触电路板时应佩戴防静电手腕套或手套，穿防静电工作服；
- 5) 拆卸下的电路板应板面朝上放置在具有抗静电作用的工作台上或放入防静电袋中；
- 6) 观察或转移已拆卸了的电路板时，应只接触电路板的外边缘，避免用手直接触摸电路板上的元器件。

3.1.6 雷电/电磁要求

设备的设计大量考虑了环境电磁及雷电对其的影响，但是在雷击强度超过一定范围时仍然有可能对安全网关造成损害；而使用过程中可能的电磁干扰源，无论是来自设备或应用系统外部，还是来自内部；都是以电容耦合、电感耦合、电磁波辐射、公共阻抗包括接地系统耦合的传导方式等对设备产生影响。为达到更好的防雷和抗干扰效果的要求，用户应做到：

- 1) 对供电系统采取有效的防电网干扰措施；
- 2) 设备安装环境最好不要与电力设备的接地装置或防雷接地装置合用，并尽可能相距远一些；

- 3) 远离强功率无线电发射台、雷达发射台、高频大电流设备等；
- 4) 必要时采取电磁屏蔽的方法；
- 5) 保证机箱的保护接地用保护地线与大地保持良好接触；
- 6) 保证电源插座的接地点与大地良好接触；
- 7) 为增强电源的防雷击效果，可以在电源的输入端安装电源避雷器，这样可大大增强电源的抗雷击能力。

3.1.7 安装台面检查

对设备进行安装前要保证以下安装环境的再确认：

- 1) 确认设备的入风口及通风口处留有足够的空间，以利于设备散热；
- 2) 确认安装环境自身有良好的通风散热系统；
- 3) 确认安装环境足够牢固，能够支撑要安装的设备及其安装附件的重量；
- 4) 确认安装环境有良好接地连接。

【注】：与墙壁的距离应不小于 15 厘米。

3.1.8 安全注意事项

基于安装设备的广泛应用及其在数据通信网络中担当的重要作用，再次强调：手册中的如下标志，在阅读过程中请多加注意：

以下安全建议对设备的安装和使用过程中要特别引起重视：

- 1) 请将设备放置在远离潮湿或远离热源的地方；
- 2) 请确认设备已经正确接地；
- 3) 请在安装维护过程中佩戴防静电手腕（套），并确保防静电手腕（套）与皮肤良好接触；
- 4) 注意不要将手指或其它物件伸入设备的散热风扇中；

5) 建议用户使用 UPS (Uninterrupted Power Supply 不间断电源) 系统。

【注】：表明该项操作不正确可能给操作者的人身安全带来极大的危险，操作者必须严格遵守正确的操作规程。

【注】：表示在安装使用中需要注意的操作，该操作不正确可能影响设备的正常使用。

3.1.9 安装工具准备

包装中不附带安装工具、仪表及相关设备，请准备相应的工具：

- 1) 十字螺丝刀
- 2) 一字螺丝刀
- 3) 防静电手腕套
- 4) 防静电袋
- 5) 电源线
- 6) 可选电缆

3.2 设备上架

根据用户安装环境，可以安装到两种环境中：

- 1) 直接放置在稳定的水平平台上；
- 2) 与其它网络设备一起安装在标准机架上。

3.3 安装到水平台面

这是一种最简便经济的安装方式，但安装操作过程中要注意以下事项：

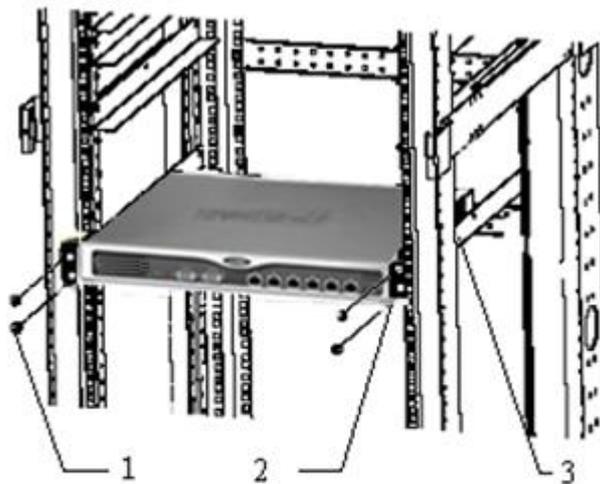
- 1) 保证水平平台的牢固性和稳定性，并保证有良好的接地连接；
- 2) 设备的通风口与形成通风障碍的障碍物之间要留有至少 15 厘米的通风通道；
- 3) 设备的上表面不要堆放重物。

3.4 安装到标准机架

外形尺寸设计是符合标准 19 英寸机架（以下称机架）上架装配要求的，因此它非常容易安装到机架上。

以下安装设备到机架的具体说明：

- 1) 检查并确认机架的安装是否合格并符合其安装标准；需要注意检查机架是否稳固并且有良好的接地连接；
- 2) 将挂耳用螺钉安装到设备靠前面板的两侧；
- 3) 确定设备要安装的位置，将设备安放到预定位置的托盘上（建议由用户提供与该机架配套的设备托盘），并注意设备与机架之间的距离要合适；
- 4) 用满足机柜安装尺寸要求的盘头螺钉将设备通过固定挂耳固定在机柜上，请保证位置水平并牢固。机柜和设备如图所示：



说明：

1. 螺钉 2. 挂耳 3. 导轨

3.5 系统部署检查

- 1) 连接电源线到设备后面的电源插口，然后插入另一端的电源插头到 220V 电插座；
- 2) 开启设备后面的电源开关和前面设备开关；

- 3) 查看设备液晶屏是否正确显示;
- 4) 连接网线的一端到设备的可信端接口, 连接另一端到内网交换机的网口;
- 5) 连接网线的一端到设备的非可信端接口, 连接另一端到外网设备的网口, 例如外网交换机、路由器、防火墙等;
- 6) 用内网管理主机登陆设备并进行适当的配置;
- 7) 测试网络的连通性以及是否可以正常访问服务器, 例如 ping。

4 管理操作指南

4.1 登录管理

4.1.1 准备工作

- 接通电源, 液晶屏显示序列号后表示启动完毕;
- 选用一带 Windows 系统 PC 作为管理主机;
- 使用交叉线, 管理光闸。

4.1.2 管理方式

- 串口命令行管理 - 常用于恢复工作
- Web 页面管理 ---- 常用于正常管理
- SSH 远程管理 ---- 常用于管理调试

4.1.3 Web 页面管理

- 上层板登陆入口: 在管理主机输入
- <https://192.168.10.254/index.php>, 按证书提示点击“确定”;
- 下层板登陆入口: 在管理主机输入
- <https://192.168.1.254/index.php>, 按证书提示点击“确定”;

- 管理员账号：在“用户名”一栏输入用户名 admin，在“密码”一栏输入其对应默认口令“admin*pwd”（管理人员应及时更改系统初始缺省管理员的用户名和口令），在验证栏输入验证码。点击“登录”。

4.1.4 CLI 管理

- CLI 管理：可以使用 console 和 ssh 两种方式来管理，串口波特率：115200，ssh 默认端口 6422，需要在 web 页面设备信息-系统服务里开启；登录账号 admin

```
#####  
#                               #  
#       伟思信安安全隔离与信息单向导入系统V3.0发送系统       #  
#                               #  
#####  
1) 显示网口配置信息  
2) 设置网口配置信息  
3) Ping 主机  
4) 恢复出厂设置  
5) 关闭SSH服务 (dropbear)  
6) 重启系统  
7) 关闭系统  
0) 退出  
请输入要进行的操作命令：
```

串口管理

4.1.5 USB 管理

- USB 接口作为外部 u-key 预留接口，默认禁止外部所有接入

5 运维操作

5.1 常见故障

5.1.1 CPU 高

设备出现 CPU 高通常有两种情况：

- 流量超过设备处理能力导致；
- 某些功能模块消耗 CPU 过高。

解决方法：关闭不必要开启的部分功能模块，查看系统流量是否超过 CPU 处理能力。

5.1.2 内存高

设备出现内存高主要可能是开启功能模块、大量的连接导致的内存消耗。

解决方法：检查系统当前状态，判断是否是因正常的功能开启或会话连接数量导致的内存消耗。

5.1.3 网络异常

出现网络慢、丢包、业务不通等现象，原因很多，需要根据现象逐个排除，例如：

- 流量超过设备处理能力导致；
- 设备配置导致（如用户主机被限速）；
- 模块不正常导致；
- 接口协商不正常导致。

解决方法：

- 1) 判断是否个别用户异常还是所有用户都有问题，如果是所有都有异常，需要判断异常产生的位置；个别用户网络异常，需要考虑是否由 BT 阻断、限速等配置引起。
如：IPMAC 绑定、连接数限制等；
- 2) 观察设备相关接口状态，判断用户流量，以及是否由接口硬件相关问题导致网络异常。

5.1.4 SYLOG 日志失效

在 SYSLOG 服务器上看不到对应模块日志。

解决方法：

- 1) 是否正确配置 SYLOG 服务器的地址和端口号；
- 2) 是否指定模块的日志类别和等级到 SYSLOG Server。

5.2 运维指南

5.2.1 日常运维

1) 连接数

如当前的连接数达到或接近系统最大值，将导致新会话不能及时建立连接，此时已经建立连接的通讯虽不会造成影响；但仅当现有的连接拆除后，释放出来的资源才可供新建连接使用。

2) 维护建议

当前连接数正常使用至 85% 时，需要考虑设备容量限制并及时升级，以避免因设备容量不足影响业务拓展。

3) CPU 检查

正常工作状态下设备 CPU 使用率应保持在 10% 以下，如出现 CPU 利用率过高情况需给予足够重视，应检查连接数使用情况和各类告警信息，并检查网络中是否存在攻击流量。通常情况下 CPU 利用率过高往往与攻击有关，可通过正确设置系统参数、攻击防护的对应选项进行防范。

4) 内存检查

设备对内存的使用把握得十分准确，正常情况下，内存的使用率应基本保持稳定，不会出现较大的浮动。如果出现内存使用率过高 (>90%) 时，可以查看连接数情况，或通过实时监控功能检查网络中是否存在异常流量和攻击流量。

5) 高峰期资源检查

在业务使用高峰时段检查设备关键资源（如：cpu、连接数、内存和接口流量）等使用情况，建立网络中业务流量对设备资源使用的基准指标，为今后确认网络是否处于正常运行状态提供参照依据。当连接数数量超过平常基准指标 20% 时，需通过实时监控检查当前网络是否存在异常流量。当 cpu 占用超过平常基准指标 20% 时，需查看异常流量、定位异常主机、检查策略是否优化。

5.2.2 应急处理

当网络出现故障时，应迅速检查设备状态并判断是否存在攻击流量，定位故障是否与设备有关。如果故障与设备有关，可首先检查设备的安全策略、访问控制策略、路由等是否按照实际使用需求配置，检验策略配置是否存在问题。一旦定位设备故障，可通过命令进行双机切换，单机环境下发生故障时利用备份的交换机/路由器配置，快速旁路光闸。在故障明确定位前不要关闭光闸。

1) 检查设备运行状态

网络出现故障时，应快速判断设备运行状态，通过管理器登陆到设备上，快速查看 CPU、内存、连接数以及相应信息，初步排除硬件故障并判断是否存在攻击行为。

2) 跟踪设备对数据包处理情况

如果出现部分网络无法正常访问，顺序检查接口状态、路由和策略配置是否有误，在确认上述配置无误后，通过 tcpdump 命令检查设备对特定网段数据报处理情况。

3) 检查是否存在攻击流量

通过实时监控确认是否有异常流量，同时在上行交换机中通过端口镜像捕获进出网络的数据包，据此确认异常流量和攻击类型，并在选项设置、入侵防护等项目中启用对应防护措施来屏蔽攻击流量。

4) 检查 HA 工作状态

检查 HA 工作状态，进一步确认引起切换的原因，引起 HA 切换原因通常为链路故障，交换机端口故障，设备断电或重启。设备运行时务请不要断开 HA 心跳线缆。

5) 发生故障时处理方法

如果出现以下情况可初步判断光闸硬件或系统存在故障：无法使用 console 口登陆设备，设备反复启动、无法建立 ARP 表、接口状态始终为 Down、无法进行配置调整等现象。为快速恢复业务，可通过调整上下行设备路由指向，快速将设备旁路，同时联系供应商进行故障诊断。

5.3 注意事项

故障处理后的总结与改进是进一步巩固网络可靠性的必要环节,有效的总结能够避免很多网络故障再次发生。

- 1) 在故障解决后,需要进一步总结故障产生原因,并确认该故障已经得到修复,避免故障重复发生;
- 2) 条件容许的情况下,构建设备业务测试环境,对所有需要调整的配置参数在上线前进行测试评估,避免因配置调整带来新的故障隐患;
- 3) 分析网络可能存在的薄弱环节和潜在隐患,通过技术论证和测试验证来修复隐患。

6 功能介绍

- 1) 伟思信安安全隔离与信息单向导入系统分为发送系统和接收系统;
- 2) 伟思信安安全隔离与信息单向导入系统采用 B/S 模式管理,且必须通过发送系统和接收系统两个管理口分别对伟思信安安全隔离与信息单向导入系统两端进行管理。发送系统管理口 IP 地址为 192.168.1.254/24,接收系统管理口 IP 地址为 192.168.10.254/24;
- 3) 管理发送系统时,选择一台安装有浏览器的客户机,与发送系统管理口相连,修改客户机 IP 地址,使其与发送系统管理接口(处于同一个网段,例如设置为 192.168.1.151/24;在浏览器地址栏输入: <https://192.168.1.254/index.php> 即出现发送系统管理系统登陆界面;



系统登录-发送系统

- 4) 管理接收系统时，选择一台安装有浏览器的客户机，与接收系统管理口相连，修改客户机 IP 地址，使其与接收系统管理接口处于同一个网段，例如设置为 192.168.10.152/24；在浏览器地址栏输入：`https://192.168.10.254/index.php` 即出现接收系统管理系统登陆界面；
- 5) 在“用户名”一栏输入用户名 admin，在“密码”中输入正确的密码，文件传输/数据库同步/UDP 通道在伟思信安安全隔离与信息单向导入系统的发送系统和接收系统同时配置。管理系统分为：系统配置、网络配置、高可用性、本地服务、数据同步、病毒库管理（此项仅在发送系统）六大模块。



系统首页

6.1 系统配置

6.1.1 系统状态

登录系统成功后，在主界面显示系统状态页面，这个页面显示伟思信安安全隔离与信息单向导入系统发送系统目前的状态。



系统状态信息

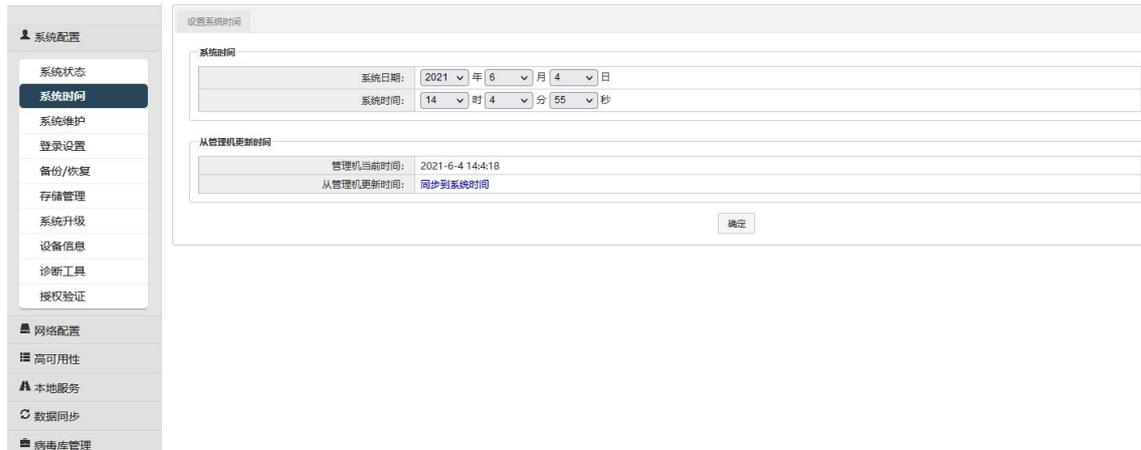
系统状态页面可以查看伟思信安安全隔离与信息单向导入系统发送系统的系统状态、接口状态、系统信息、网络吞吐量。

- 系统状态：内存使用率、CPU 使用率、磁盘使用率。
- 接口状态：序号、名称、IP 地址、状态。
- 系统信息：系统名称、系统版本、数据库同步程序版本、文件同步程序版本、监控程序版本、运行时长、当前日期/时间、最后更改配置时间。
- 网络吞吐量：系统上行和下行的吞吐量实时曲线图，以 kb 为单位。

6.1.2 系统时间

在系统时间页面可以对系统时间进行调整，在时间修改后，日志与审计显示时间，也将

按照修改后的时间显示。



系统时间

- 管理机当前时间：显示系统的当前时间。
- 同步到系统时间：从管理机更新时间到系统。

6.1.3 系统维护

为了清除系统运行中发生的故障和错误，维护人员可以对系统进行必要的修改与完善。可针对系统程序、文件同步程序、数据库同步程序进行定时维护。



系统维护

后台维护

此功能提供管理员输入一定指令在后台执行，并返回执行结果，方便管理员进行相关故障排查运维。

系统维护: 定时维护



后台维护

执行命令前需要进行二次认证，保证命令执行的安全性。

可执行命令以及效果说明(以下执行命令均临时生效，页面配置或重启配置均会失效，用于临时业务故障调试)

ifconfig

ifconfig : 【查看所有网卡的状态】

ifconfig ethX: 【查看指定网卡的状态】

ifconfig ethX down: 【关闭指定网卡】

ifconfig ethX UP: 【启用指定网卡】

ipaddr

ip addr: 【查看本机 IP 的状态】

ip addr show ethX: 【查看指定网卡 IP 的状态】

ip addr add xxx.xxx.xxx.xxx/xx dev ethX: 【添加 IP (临时生效)】

ip addr del dev ethX xxx.xxx.xxx.xxx/xx: 【删除指定 IP (临时生效)】

route

route -n: 【查看本机路由表】

route add -host xxx.xxx.xxx.xxx gw xxx.xxx.xxx.xxx: 【添加主机路由】

route add -net xxx.xxx.xxx.xxx netmask xxx.xxx.xxx.xxx gw xxx.xxx.xxx.xxx: 【添加网络路由】

route del -host xxx.xxx.xxx.xxx gw xxx.xxx.xxx.xxx: 【删除主机路由】

route del -net xxx.xxx.xxx.xxx netmask xxx.xxx.xxx.xxx gw xxx.xxx.xxx.xxx: 【删除网络路由】

ethtool

ethtool ethX: 【查看指定网卡的信息】

6.1.4 登录设置

在登录设置页面可以根据用户的需求，设置会话超时、登录可尝试次数、封锁 IP 时间，远程管理主机、证书认证、管理端口。

系统配置: 登录管理

登录管理

会话超时设置:	240	分钟
登录可尝试次数:	3	
封锁IP时间:	1	分钟
远程管理主机:	<input type="checkbox"/> 选中,则启用远程管理主机	
证书认证:	<input type="checkbox"/> 启用证书认证	
私钥口令:	注: 如果私钥是加密的, 需要输入口令	
SSLCertificateFile (root.crt):	浏览...	未选择文件, 最近修改: 2021-08-17 19:00
SSLCertificateKeyFile (serverkey):	浏览...	未选择文件, 最近修改: 2021-10-17 14:23
SSLCertificateFile (server.crt):	浏览...	未选择文件, 最近修改: 2021-08-17 19:00
客户端证书1 (cert_01.p12):	浏览...	未选择文件, 最近修改: 2021-08-17 19:00
客户端证书2 (cert_02.p12):	浏览...	未选择文件, 最近修改: 2021-08-17 19:00
注意: 如启用证书认证, 请确保你本地已保存有客户端证书或浏览器已导入证书, 否则将无法打开管理界面。		
点击下载客户端证书 (cert_01.p12) >>		
点击下载客户端证书 (cert_02.p12) >>		
管理端口:	443	

确定

登录设置

- 会话超时设置: 连接会话失效的时间, 默认为 240 分钟;
- 登录可尝试次数: 输错用户名或者密码所允许的最大次数, 默认为 3 次;
- 封锁 IP 时间: 封锁用户登录的时间, 默认为 1 分钟;
- 远程管理主机: 允许远程管理主机或禁止远程管理主机;
- 证书认证: 勾选之后启用证书认证, 选择下载证书。
- 管理端口: 默认为 443 端口。

6.1.5 备份/恢复

备份配置:

备份配置: 选择备份区域, 然后点击“下载配置”, 即可把现有配置下载到本机。

输入 key 值：输入 key 值，还原配置需核对 key 值，需牢记。

系统配置: 备份/恢复

备份配置

备份区域: 所有

key值: 注: 配置还原时要输入此key值

下载配置

还原配置

恢复区域: 所有

key值:

浏览... 未选择文件。

还原配置

注意:
还原配置后, 需重启系统才生效。

恢复出厂配置

恢复出厂配置

注意:
设备将在恢复出厂配置后自动重启。

配置备份

注：下载的配置文件是加密的。

还原配置：

还原配置可把下载配置上传系统，将系统恢复为备份的配置，如图：

系统配置: 备份/恢复

备份配置

备份区域: 所有

key值: 注: 配置还原时要输入此key值

下载配置

还原配置

恢复区域: 所有

key值:

浏览... 未选择文件。

还原配置

注意:
还原配置后, 需重启系统才生效。

恢复出厂配置

恢复出厂配置

注意:
设备将在恢复出厂配置后自动重启。

还原配置

输入 key 值：输入 key 值，还原配置输入备份配置输入的 key 值。

恢复出厂配置:

恢复出厂配置可将当前设备配置恢复为出厂默认设置状态,恢复出厂设置后,发送系统的 IP 为: 192.168.1.254,接收系统的 IP 为: 192.168.10.254。

6.1.6 存储管理

在存储管理页面,可以将设备日志备份到远程 SMB 服务器,填写服务器的地址、登录口令和远程目录,点击“确定”,即可定时将设备日志进行备份。

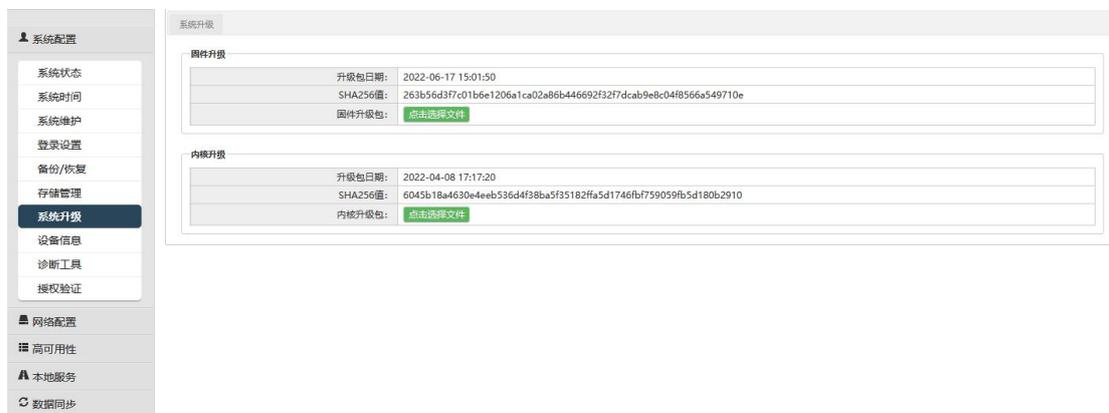


注: 同步间隔周期 1 分钟。

存储管理

6.1.7 系统升级

在系统升级页面,可以对系统固件和系统内核进行升级,只需上传升级包,然后重启系统,即可升级成功。

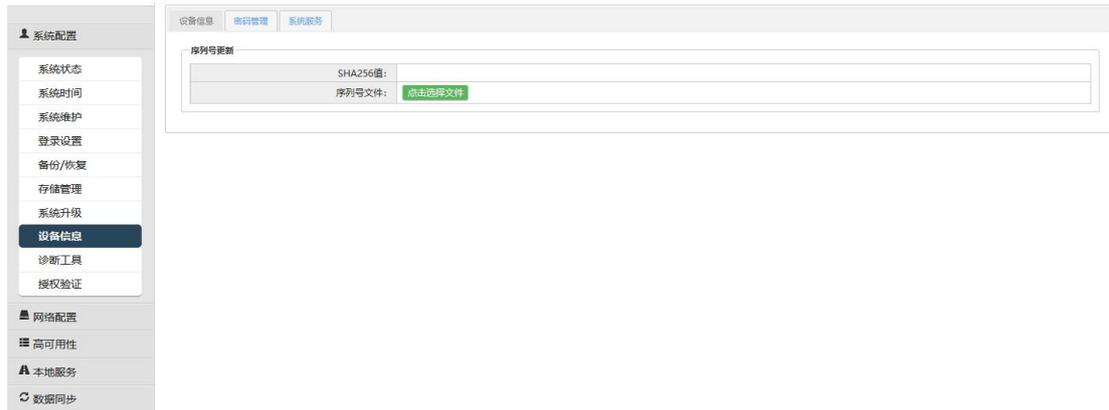


系统升级

6.1.8 设备信息

在系统设备信息页面，可以对系统相关信息进行查看，并修改相关的配置。

- 序列号更新：上传序列号文件；



序列号更新

- 工作密钥更新：更新工作密钥；
- MySQL 密码更新：查看修改 MySQL 账号密码；



密码管理

- SSH 服务：启动/关闭系统后台 SSH 服务，默认关闭。
- 带外管理：开启则只有管理口能访问 Web 管理和 SSH 服务。



系统服务

6.1.9 诊断工具

在诊断工具页面，可以使用一些工具对系统，对网络进行排查。



诊断工具

6.1.10 授权验证

在授权验证页面，可以查看系统相关注册信息，上传授权注册文件。



授权验证

6.2 网络配置

6.2.1 接口配置

添加网络接口：

进入“网络配置”>“接口配置”页面，点击“添加”按钮，选择网口和网络类型，输入正确的 IP 地址和子网掩码，点击“保存”按钮即可。

例如：

网口：选择 eth0，类型选择：静态，IP 地址：192.168.6.44，子网掩码为：24，如下。

网络配置: 接口设置

接口

状态: 禁用 启用

网口: eth0

类型: 静态IPv4

IPv4地址/掩码: / 24

注: 如果编辑的是管理口, 并且状态为'启用', 点击'保存'后系统将自动重启

保存 返回接口列表

添加接口

添加成功后, 在状态栏点击“禁用”按钮, 启用该接口, 并将此接口接上网线, 在与业务口相连的主机上配置与 192.168.6.* /24 同网段的 IP 地址, 即可 ping 通此 IP。

网络配置: 接口列表

序号	接口名称	接口类型	网络端口	类型	IP地址	子网掩码	状态	操作
1	NT0	通道口	eth4	静态IPv4	172.26.78.2	255.255.255.0		
2	NT1	管理口	eth8	静态IPv4	192.168.6.44	255.255.255.0	当前访问	
3	NT2	业务口	eth9	静态IPv4	192.168.12.44	255.255.255.0	启用	
4	NT3	业务口	eth9(eth9:0)	静态IPv6	2001::644	64	启用	

注: 如果把管理口状态更改为'启用', 系统将自动重启

接口列表

修改网络接口：

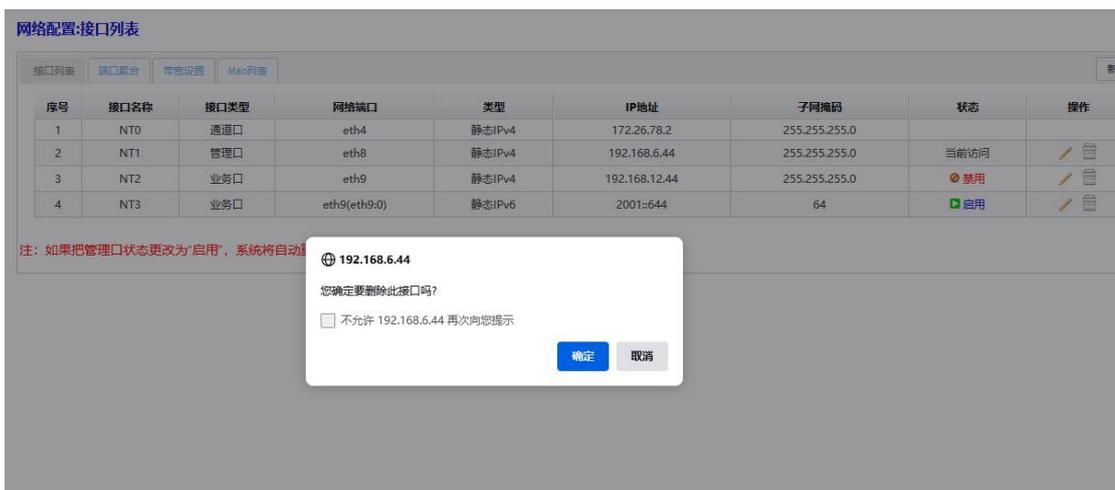
进入“网络配置”>“接口配置”页面，在状态栏点击“启用”按钮，禁用该接口，然后在操作栏点击“✎”按钮，进入到接口修改页面，输入接口名称，选择网络端口，输入正确的 IP 地址和子网掩码，点击“保存”按钮即可。



接口设置

删除网络接口：

进入“网络配置”>“接口配置”页面，在状态栏点击“启用”按钮，禁用该接口，然后在操作栏点击“🗑️”按钮，弹出删除确认对话框后点击“确定”按钮，即可删除该接口。



删除接口

新增端口聚合：

进入“网络配置”>“接口配置”页面，点击“端口聚合”，点击“添加”按钮，选择聚合模式，勾选要聚合的成员接口，点击“保存”按钮即可。

例如：

输入自定义名称，模式：选择 load balancing，成员接口：勾选 eth2、eth3，点击“保存”。

网络配置: 接口设置

接口

名称: test

模式: load balancing(round-robin)平衡轮循环策略

成员接口: eth2 eth3

保存 返回接口列表

新增聚合接口

添加成功后,可以在聚合列表查看聚合的接口信息，点击“”和“”可对聚合接口进行修改和删除，同“网络接口配置”一致，不再赘述。

网络配置:接口列表

序号	名称	接口	成员	模式	管理
1	test	bond0	eth2 eth3	load balancing(round-robin)平衡轮循环策略	 

新增端口聚合

聚合接口列表

带宽设置：

可以选择启用并对已经配置的网络接口进行带宽限制。

网络配置:带宽设置

接口列表 端口聚合 带宽设置 Mac列表

新增端口聚合

是否启用:	接口:	带宽:
<input checked="" type="radio"/> 禁用 <input type="radio"/> 启用	eth0	1024 Mbit
	eth1	1024 Mbit

保存

带宽设置

Mac 列表:

查看系统全部网络接口的真实 Mac 地址。

网络配置:Mac列表

序号	接口名称(真实)	Mac地址
1	bond0	00:0C:29:53:D6:74
2	eth0	00:0C:29:53:D6:60
3	eth1	00:0C:29:53:D6:6A
4	eth2	00:0C:29:53:D6:74
5	eth3	00:0C:29:53:D6:74

Mac 列表

6.2.2 网关设置

网关是一个网络连接到另一个网络的“关口”。一般情况下，在一个只有一个出口的网络中不需要修改网关设置，一个默认网关已经足够了。然而，当网络有两个以上出口或需要使用某些高级设置时就必须定义指定的网关。

网络配置: 编辑默认网关

名称	<input type="text" value="wg"/>
默认网关IP	<input type="text" value="192.168.0.1"/> <small>注: 请填写一个IPv4或IPv6地址</small>
描述	<input type="text"/>

网关设置

- 名称: 不能使用中文字符，只能单纯英文或数字（或者英文数字组合）。
- 网关 IP: 填写所对应的网关 IP 地址。
- 描述: 描述不限制，可以填写，也可以不填写。

6.2.3 静态路由

在静态路由页面可以对路由进行管理，路由用于访问默认网关无法到达的网络，在两个接临的不同子网的网络之间经常需要设置路由使两个网络之间能进行通讯。

网络配置: 编辑路由

静态路由	
目的网络	192.168.5.123 / 24 *目的主机选择掩码32
接口	eth1
网关	192.168.0.1
描述	

静态路由

- 目的网络：填写所对应的 IP 地址段，并选择对应的子网掩码。
- 接口：在下拉菜单选择对应的接口。
- 网关：填写所对应的网关 IP 地址。
- 描述：描述不限制，可以填写，也可以不填写。

6.2.4 IP/MAC 绑定

IP/MAC 绑定页面可以使主机 IP 和 MAC 地址进行绑定，别的主机盗用了绑定主机的 IP，也登录不了系统的页面。

网络配置: 编辑IP/MAC绑定

编辑IP/MAC绑定	
IP地址	
MAC地址	
描述	

IP/MAC 绑定

- IP 地址：需要绑定主机的 IP 地址。
- MAC 地址：需要绑定主机的 MAC 地址。
- 描述：描述不限制，可以填写，也可以不填写。

6.3 高可用性

6.3.1 双机热备

配置双机热备的目的是为了当主机出现故障，不能正常工作时，备机会主动接管主机服务，以保证数据链路不会中断。当主机修复正常后，主机又会重新接管服务。

高可用性: 双机热备配置

常规设置

启用双机热备:	<input type="checkbox"/>
备机IP:	<input type="text"/>
备机用户名:	<input type="text" value="admin"/>
备机密码:	<input type="password" value="*****"/>

配置同步选项

注: 勾选您需要同步到备机的配置

全选/取消	<input type="checkbox"/>
用户管理:	<input type="checkbox"/>
登录管理:	<input type="checkbox"/>
静态路由:	<input type="checkbox"/>
虚拟IPs:	<input type="checkbox"/>
访问控制:	<input type="checkbox"/>
强制访问控制:	<input type="checkbox"/>
FTP服务:	<input type="checkbox"/>
SMB服务:	<input type="checkbox"/>
数据资源:	<input type="checkbox"/>
业务与服务:	<input type="checkbox"/>

双机热备设置

◆ 常规设置:

- 启用双机热备: 勾选之后启用;
- 备机 IP: 输入备份机的 IP 地址;
- 备机用户名: 输入备份机的登录用户名;
- 备份机密码: 输入备份机的登录密码。

◆ 配置同步选项:

- 用户管理: 勾选之后主机的用户配置会同步到备机中;
- 登录管理: 勾选之后主机的登录管理配置会同步到备机中;
- 静态路由: 勾选之后主机的静态路由会同步到备机中;

- 虚拟 IPs：勾选之后主机的虚拟 IPs 会同步到备机中；
- 访问控制：勾选之后主机的访问控制会同步到备机中；
- 强访问控制：勾选之后主机的强访问控制会同步到备机中；
- FTP 服务：勾选之后主机的 FTP 服务会同步到备机中；
- SMB 服务：勾选之后主机的 SMB 服务会同步到备机中；
- 数据资源：勾选之后主机的数据资源会同步到备机中；
- 业务与服务：勾选之后主机的业务与服务会同步到备机中。

一般情况下都是勾选所有同步配置，即在主机配置的服务都会同步到备份机。

6.3.2 虚拟 IP

在配置高可用双机热备时，需要为主备设备配置一套虚拟 IP；虚拟 IP 只在主设备上激活，也就是说，通过虚拟 IP 访问到的都是主设备，其作用主要在访问本地服务在双机切换时体现。

高可用性：虚拟IP设置

网络接口:	eth2
IP地址:	/24
VHID组:	1
VHID组密码:	

保存 返回列表

虚拟 IP 管理

- 网络接口：选择虚拟 IP 的网络接口；
- IP 地址：输入虚拟 IP 的网络地址；
- VHID 组：互为主备的设备 VHID 组选择 VHID 组号不能相同，同一网络不是互为主备的设备 VHID 组号也不能相同；
- VHID 组密码：输入 VHID 组密码，同组密码需一致。

6.3.3 双机热备状态

当发送系统主机出现故障，不能正常工作时，发送系统主机会通知接收系统主机，然后发送系统主机跟接收系统主机的双机热备状态一同变为备机状态；发送系统备机跟接收系统备机的双机热备状态变为主机状态。

序号	双机热备接口	虚拟IP	状态
1	Eth2(eth2)	192.168.0.189/24	<input checked="" type="checkbox"/> MASTER
2	Eth3(eth3)	192.168.1.189/24	<input checked="" type="checkbox"/> MASTER

序号	双机热备接口	虚拟IP	状态
1	Eth2(eth2)	192.168.0.189/24	<input type="checkbox"/> BACKUP
2	Eth3(eth3)	192.168.1.189/24	<input type="checkbox"/> BACKUP

双机热备运行状态

这时，内接收系统备机会主动接管内接收系统主机的任务，使数据链路不会中断。

注 2：在配置双击热备前必须清掉所有的任务配置（最好是恢复默认值），否则同步可能异常。

6.4 本地服务

6.4.1 通信访问控制

通信访问控制包括访问控制和 UDP 协议通讯。

访问控制：防火墙过滤。

本地服务：访问控制：编辑

访问控制

动作：	ACCEPT
禁用：	<input type="checkbox"/> 禁用此规则
协议：	TCP
源：	类型：any
	地址： <input type="text"/>
	端口： <input type="text"/>
本地服务：	类型：any
	地址： <input type="text"/>
	端口： <input type="text"/>

访问控制

UDP 协议通讯：基于 Iptables 的 UDP 透明转发。

本地服务: UDP协议通信: 编辑

UDP协议通信	
禁用:	<input type="checkbox"/> 禁用此规则
网闸地址:	eth2: 192.168.5.66
转发端口:	
禁用转源:	<input type="checkbox"/> 勾选表示禁用
数据控制(黑名单):	字符串: <input type="text"/>
	ASCII: <input type="text"/>
	十六进制: <input type="text"/>
	正则表达式: <input type="text"/>
<input type="button" value="确定"/> <input type="button" value="取消"/>	

UDP 协议通信

TCP 协议通讯: TCP 转发。

本地服务: TCP协议通信: 编辑

TCP协议通信	
禁用:	<input type="checkbox"/> 禁用此规则
入口IP:	eth1: 172.26.78.2
入口端口:	
出口IP:	eth1: 172.26.78.2
目的IP:	
目的端口:	
<input type="button" value="确定"/> <input type="button" value="取消"/>	

TCP 协议通信-编辑

6.4.2 FTP 服务

在系统的 FTP 服务页面可以创建本地 FTP 服务，FTP 服务应用于文件同步业务。

本地服务: FTP服务

本地FTP服务	
用户名:	admin
密码:	*****
强制访问用户组:	无
<input type="button" value="确定"/> <input type="button" value="取消"/>	

FTP 服务

- 用户名: 不能使用中文字符, 只能纯英文或数字 (或者英文数字组合);
- 密码: 至少需要包含字母、数字和特殊字符各 1 位, 且禁止使用 3 个以上连续字符
- 强制访问用户组: 选择强制访问用户组。

6.4.3 邮件服务

填写邮件服务器的 IP 地址或域名，新增邮件账号。

在“本地服务”中，点击“邮件服务”，进入邮件服务配置页面。

本地服务: 邮件服务

邮件服务

邮件服务器设置

邮件服务器IP	<input type="text"/>	
smtp服务器端口	<input type="text"/>	默认端口为25
pop3服务器端口	<input type="text"/>	默认端口为110
邮件服务器最大连接数	<input type="text"/>	默认最大连接数为10
邮件服务器超时时间	<input type="text"/>	默认超时时间为20s
是否开启邮件服务器	<input type="checkbox"/>	

保存

新增邮件账号

邮件列表

序号	账号	操作
----	----	----

邮件服务器设置

输入相应的信息后，点击“保存” ；点击“新增邮件账号” ，进入新增邮件账号页面，输入相应的信息后，点击“确定” 。

本地服务: 邮件服务

本地邮件服务

用户名:

密码:

确定 取消

邮件账号编辑

6.5 数据同步

6.5.1 数据资源

在伟思信安安全隔离与信息单向导入系统的数据资源页面，创建数据库资源，要进行数据库同步必须先创建数据库资源。

数据同步: 数据资源: 编辑

数据资源配置

资源名称:	586
资源类型:	数据库服务器
数据库类型:	Oracle
IP地址:	192.168.5.86
端口:	1521
同步账号用户名:	longbu
同步账号密码:	*****
业务账号用户名:	rx1
业务账号密码:	****
数据库名:	orcl
模式名:	orcl
临时表前缀:	SYNCD_
触发器前缀:	SYNCD_TR_

连接测试 确定 取消

数据库资源-编辑

- 资源名称: 不能使用中文字符, 只能单纯英文或数字 (或者英文数字组合);
- 资源类型: 数据库服务器;
- 数据库类型: 选择发送系统数据库的类型。若同步“ORACLE”数据库, 则选择“ORACLE”, 若同步“MYSQL”数据库, 则选择“MYSQL”;
- IP 地址: 发送系统数据库的 IP 地址;
- 端口: 发送系统数据库的端口号。一般情况下, “ORACLE”数据库的端口号为 1521, “MYSQL”数据库的端口号为 3306, 也可以选择其他端口号;
- 同步帐号用户名: 数据库的用户帐号;
- 同步帐号密码: 数据库的用户密码;
- 业务帐号用户名: 建立文件同步的业务帐号;
- 业务帐号密码: 建立文件同步的业务帐号密码;
- 数据库名: 已创建的接收系统数据库实例名;
- 模式名: 该资源所属的模式;
- 临时表前缀: 定义生成临时表表名前缀;
- 触发器前缀: 定义生成触发器表表名前缀;

点击  按钮，测试发送系统数据库是否连接成功，测试连接成功后方可保存。

6.5.2 业务注册

要想建立结构化数据同步或非结构化数据同步，首先要注册业务。

数据同步：业务注册

业务名称：	数据同步
业务单位：	研发部
业务类型：	数据同步
数据传输类型：	结构化数据

业务注册

- 业务名称：可以是字母、数字、下划线、中文任意组合；
- 业务单位：可以是字母、数字、下划线、中文任意组合；
- 业务类型：可以是字母、数字、下划线、中文任意组合；
- 数据传输类型：选择“结构化数据”、“非结构化数据”、“结构化与非结构化数据”。

6.5.3 业务与服务管理

业务与服务管理中主要包括：结构化数据同步服务和非结构化数据服务两部分。

结构化数据同步任务配置：

创建结构化数据同步任务时，必须要创建好数据库资源（注意：要配置数据库业务，接收系统和发送系统必须要创建好数据库资源）。

以 oracle 数据库同步为例：

发送系统任务配置：

1. 在发送系统系统的数据资源中创建 oracle 数据资源。
 - 资源名称：可以是字母、数字、下划线、中文任意组合，如：oracle_neiduan；
 - 资源类型：可以是 Oracle、SQLServer、MySQL、DB2 等数据库类型，如：Oracle；

- IP 地址：该数据库所在服务器的 IP 地址，如：192.168.5.86；
- 端口：数据库使用的端口号，如：1521；
- 同步帐号用户名：数据库同步账户用户名，如：tongbu；
- 同步帐号密码：数据库同步账户密码，如：123456；
- 业务帐号用户名：数据库业务帐号用户名，如：yewu；
- 业务帐号密码：数据库业务帐号密码，如：123456；
- 数据库：该资源所在的数据库名称，如：orcl；

然后点击“连接测试”按钮，连接成功后方可保存。

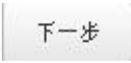
数据同步：数据资源：编辑

资源名称：	oracle_neiduan
资源类型：	数据库服务器
数据库类型：	Oracle
IP地址：	192.168.5.86
端口：	1521
同步帐号用户名：	tongbu
同步帐号密码：	*****
业务帐号用户名：	yewu
业务帐号密码：	*****
数据库名：	orcl
模式名：	orcl
临时表前缀：	SYNCD_
触发器前缀：	SYNCD_TR_

测试连接成功！ 点击确定保存配置

连接测试 确定 取消

数据资源-编辑 1

2. 在业务与服务管理中创建 oracle 数据库同步任务。
 - 服务名称：不能使用中文字符，只能纯英文或数字（或者英文数字组合），并且内接收系统的名称需保持一致；
 - 服务 ID：不能使用中文字符，只能纯英文或数字（或者英文数字组合），并且内接收系统的名称需保持一致；
 - 描述：描述不限制，可以填写，也可以不填写；
 - 点击  按钮。

➤ 同步方式：

触发器方式：是指在接收系统数据库同步表中插入、删除、更新若干条数据后，发送系统数据库同步表中也自动同步插入、删除、更新了同样的数据。

普通全表同步方式：是指把整张表的数据都进行同步。

- 冗余传输：可选择冗余传输次数，默认为 1。
- 传输模式：可选择“高速模式”和“常规模式”，默认选择“高速模式”
- 记入日志：勾选则表示同步过程种文件写入到文件文件日志中，反之则不写入

点击  按钮。

点击  按钮。

数据同步：数据库同步服务：编辑



数据库同步

1.服务定义 2.服务属性配置 3.业务表管理 4.执行计划

同步方式 * 触发器
备注：触发器方式是增量同步，为了达到同步效果需保证建立任务之前两边表数据已一致
 单临时表
 普通全表

冗余传输 次

开启鉴权

传输模式：

记入日志：

数据库同步服务-编辑

添加同步任务表

任务表映射关系

内端资源: 586
外端资源: 686

内端表: TABLE04 仅显示无主键表
外端表: TABLE04

表结构是否一致: 是 否
按条件更新: 条件表达式:

新增字段名:
新增字段值:

监控类型: 插入 删除 更新

源端条件过滤where子句: (注意: where子句里面的字段名前请加上"t.",例如:"t.id < 10")

序号	源表字段名	源数据类型	主键	源表标	同步字段顺序	序号	目标表字段	目标数据类
1	ID012	NUMBER	true	<input checked="" type="checkbox"/>	1	1	ID012	NUMBER
2	SNAME	VARCHAR2	--	<input type="checkbox"/>	2	2	SNAME	VARCHAR2

数据库同步服务

时间间隔：系统默认是 3 秒，也可以自己根据需要填写。

点击 按钮。

完成配置后，在接收系统配置数据库业务配置页面。

数据同步：数据库同步服务：编辑

数据库同步

1. 服务定义 > 2. 服务属性配置 > 3. 业务表管理 > 4. 执行计划

时间间隔: 3 秒
 定时:
 其它

数据库同步服务

接收系统业务配置：

- 在接收系统系统的数据资源中创建 oracle 数据资源。
- 资源名称：可以是字母、数字、下划线、中文任意组合，如：oracle_waiduan，

- 资源类型：可以是 Oracle、SQLServer、MySQL、DB2 等数据库类型，如：Oracle。
- IP 地址：该数据库所在服务器的 IP 地址，如：192.168.6.86。
- 端口：数据库使用的端口号，如：1521。
- 同步帐号用户名：数据库同步账户用户名，如：tongbu，
- 同步帐号密码：数据库同步账户密码，如：123456，
- 业务帐号用户名：数据库业务帐号用户名，如：yewu，
- 业务帐号密码：数据库业务帐号密码，如：123456，
- 数据库：该资源所在的数据库名称，如：orcl，

然后点击“连接测试”按钮，连接成功后方可保存。

数据同步：数据资源：编辑

数据资源配置	
资源名称：	oracle_waiduan
资源类型：	数据库服务器
数据库类型：	Oracle
IP地址：	192.168.6.86
端口：	1521
同步帐号用户名：	tongbu
同步帐号密码：	*****
业务帐号用户名：	yewu
业务帐号密码：	*****
数据库名：	orcl
模式名：	orcl
临时表前缀：	SYNCD_
触发器前缀：	SYNCD_TR_

测试连接成功！ 点击确定保存配置

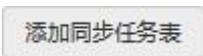
连接测试 确定 取消

数据资源

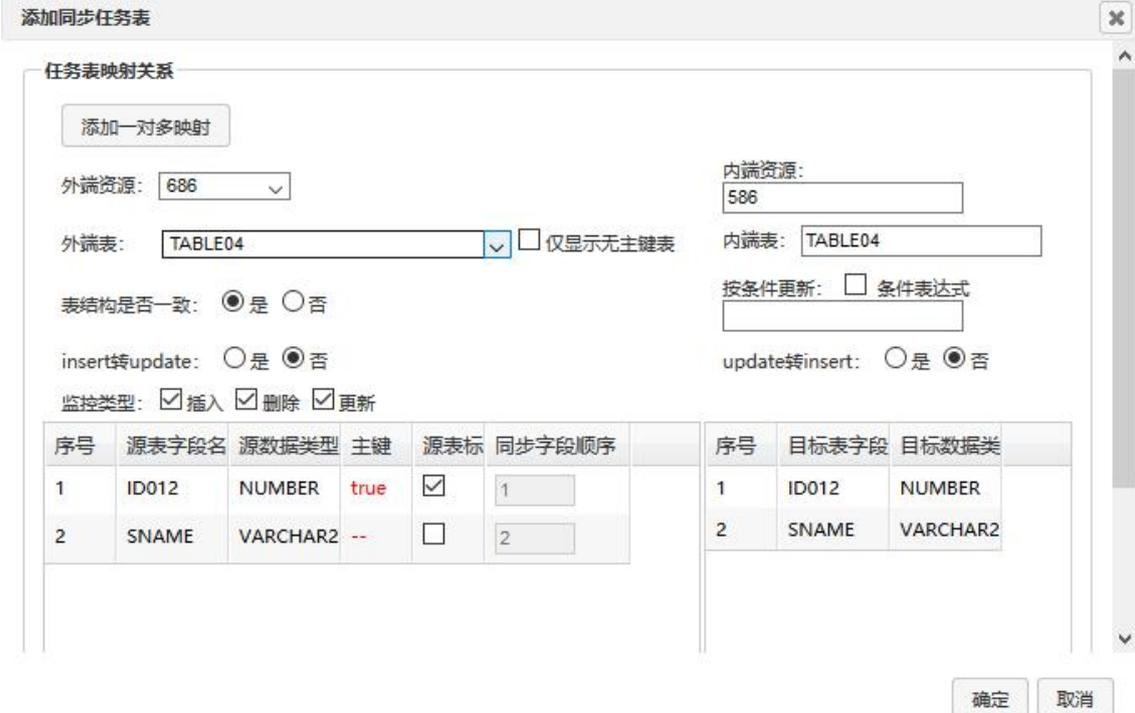
4. 在业务与服务管理中创建 oracle 数据库同步任务。
 - 服务名称：不能使用中文字符，只能纯英文或数字（或者英文数字组合），并且内接收系统的名称需保持一致。
 - 服务 ID：不能使用中文字符，只能纯英文或数字（或者英文数字组合），并且内接收系统的名称需保持一致。
 - 描述：描述不限制，可以填写，也可以不填写。

- 点击  按钮。
- 同步方式：
- 冗余传输：可选择冗余传输次数，默认为 1。
- 传输模式：可选择“高速模式”和“常规模式”，默认选择“高速模式”
- 记入日志：勾选则表示同步过程中文件写入到文件日志中，反之则不写入

点击  按钮。

点击  按钮。

点击  按钮后，进入添加同步任务表。选择发送系统资源的发送系统表，数入接收系统资源，勾选表结构一致，点击  按钮。



添加同步任务表

任务表映射关系

外端资源:

外端表: 仅显示无主键表

表结构是否一致: 是 否

insert转update: 是 否

监控类型: 插入 删除 更新

内端资源:

内端表:

按条件更新: 条件表达式

update转insert: 是 否

序号	源表字段名	源数据类型	主键	源表标	同步字段顺序	序号	目标表字段	目标数据类型
1	ID012	NUMBER	true	<input checked="" type="checkbox"/>	<input type="text" value="1"/>	1	ID012	NUMBER
2	SNAME	VARCHAR2	--	<input type="checkbox"/>	<input type="text" value="2"/>	2	SNAME	VARCHAR2

数据库同步服务-编辑 4

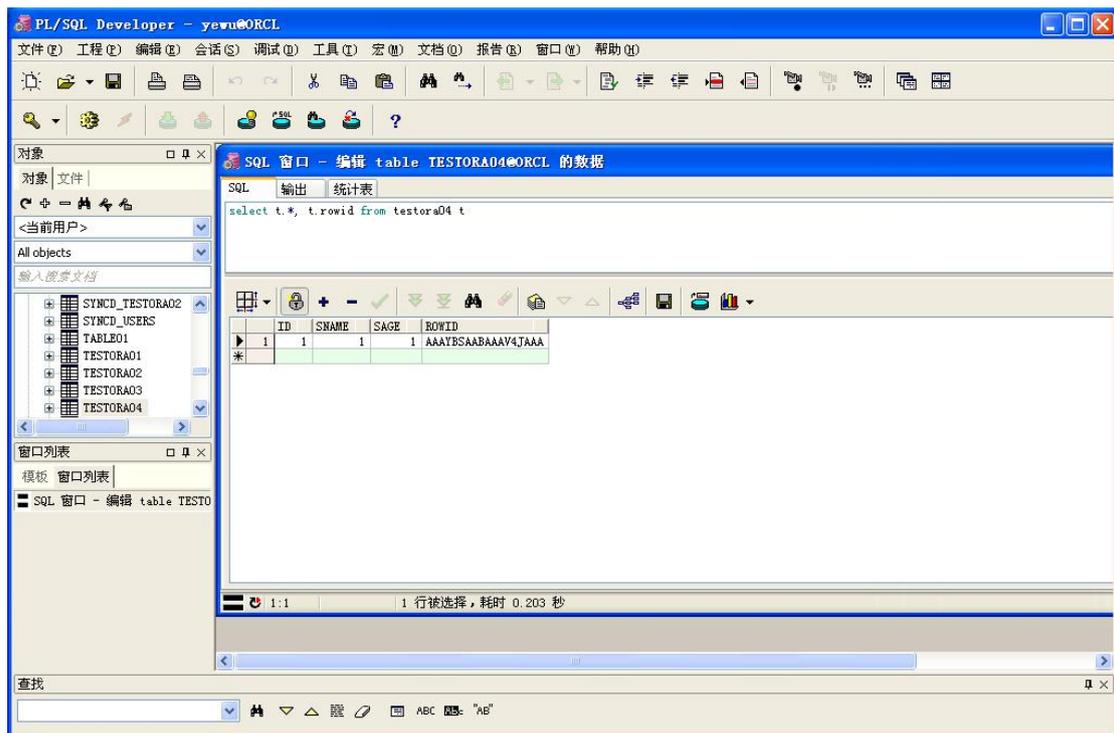
时间间隔：系统默认是 3 秒，也可以自己根据需要填写。点击  按钮。

5. 完成配置后，若选择同步方式“常规模式”，则先在接收系统（接收端）数据库业务配置页面开启该任务，再在发送系统（发送端）数据库业务配置页面开启任务。
6. 当选择“高速模式”，则先在接收系统（接收端）数据库业务配置页面开启该任务，再在发送系统（发送端）数据库业务配置页面开启任务，然后点击“服务管理”界面下的“生效配置”按钮。



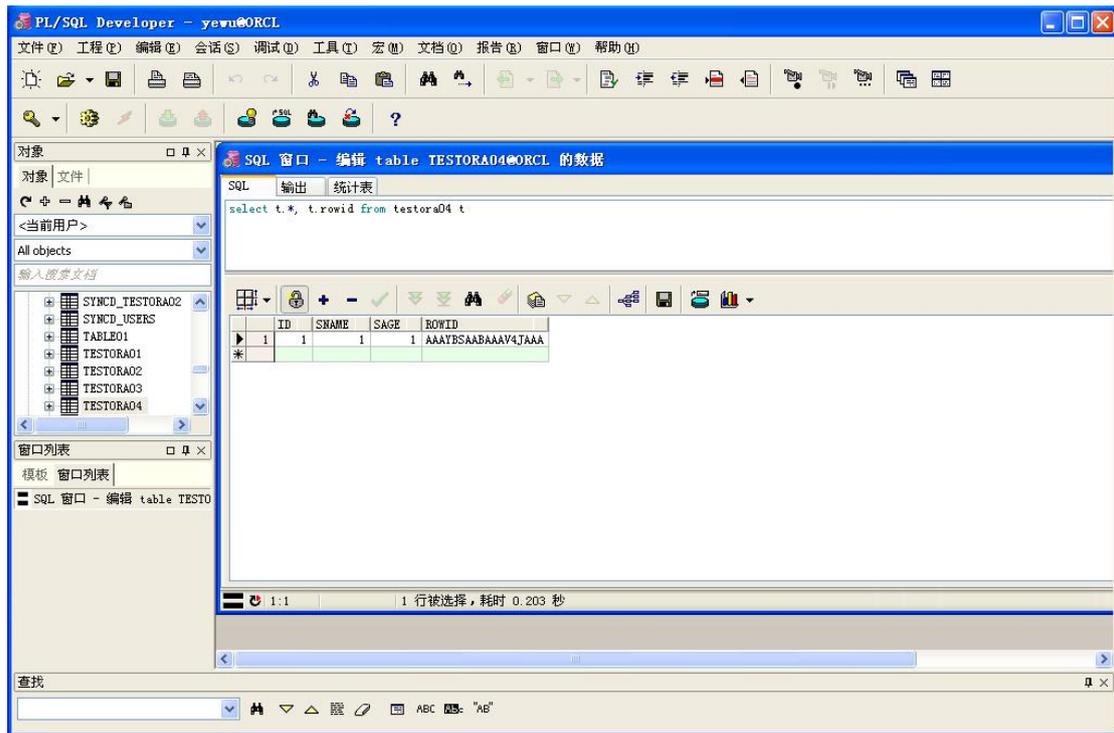
高速模式下生效配置

7. 在发送系统服务器中打开 plsqldev，输入用户名：yewu，密码：123456 进行登录。
 - a. 登录成功后，在 Tables 中找到 TESTORA04 表，并右键编辑数据，插入一条数据。



数据库添加数据-测试

- b. 在接收系统服务器中打开 plsqldev，输入用户名：yewu，密码：123456 进行登录。
- c. 登录成功后，在 Tables 中找到 TESTORA04 表，并右键编辑数据，会查看到一条同步数据。



查看同步数据-测试

非结构化数据同步任务配置：

如果是配置本地任务，必须要先创建本地 FTP 服务或者 SMB 服务或者 NFS 服务。（注意：要配置本地文件同步业务，接收系统和发送系统必须要创建好 FTP 服务、NFS 服务或者 SMB 服务）

如若创建远程同步任务，则必须要在内接收系统分别准备一台服务器，该服务器上装有 SMB 服务器或 FTP 服务器，然后在文件同步业务中进行任务配置。

配置本地任务（本地 FTP），选择“高速模式”时，但是无法配置文件相关过滤条件，传输速度有所提升。

选择“高速模式”进行业务同步时，在配置完内接收系统同步任务后，先启动接收系统（接受端）任务，再开启发送系统（接收端）任务并点击“生效配置”。

数据同步：业务与服务管理



高速模式生效配置

以本地 FTP 同步为例：

发送系统业务配置：

在 FTP 服务中创建远程 FTP 服务。

在业务与服务管理中创建远程 FTP 任务；

- 发送系统业务 id：请输入大于 2 的业务 id，例如：8800；
- 服务名称：不能使用中文字符、只能单纯英文或数字（或者英文数字组合），例如：
test_ftp；
- 资源类型：选择远程 FTP；
- 传输模式：选择“高速模式”或“常规模式”；
- 并发数：默认 5；
- 流量限制：单位 b/s, -1 为不限制；
- 验签：选择是否需要签名验证，默认不选择；
- 进行流量实时统计：选择是否需要流量实时统计，默认不选择；
- 后缀名过滤：输入要过滤的文件名，多个用空格分开；
- 文件特征：文件特征包括“不审计”、“白名单”以及“黑名单”；
- 文件同步后所采取的操作：选择删除，则删除源端文件，选择复制，则保留源端文件；
- 关键字过滤：输入要过滤的关键字，多个关键字用“;”隔开。（.txt 文件中包含的关键字）；
- 过滤最小字节数：大于此数值才可以同步；
- 过滤最大字节数：小于此数值才可以同步；
- 开启病毒扫描：开启病毒扫描的条件是必须在【病毒库管理】>【引擎信息】中启动杀毒引擎，勾选开启病毒扫描，不勾选不开启；
- 病毒文件处理方式：选择删除，则删除病毒；选择隔离，则在【病毒库管理】>【隔离

区管理】中可以查看到被隔离的病毒文件；

- 限速：留空则不限速；
- 定时同步：可以设置文件同步的周期时间；

内网服务id:	8800	注意:请输入大于2的服务id
服务名称:	test_ftp	
资源类型:	远程FTP	
用户名:	ftp1	
密码:	*****	
IP地址:	192.168.6.235	
端口:	21	
同步间隔:	3000	毫秒
编码:	UTF-8	
传输模式:	高速下载	
显示高级设置:	<input checked="" type="checkbox"/>	
并发数:	5	
流量限制:	-1	单位b/s,-1为不限制
任务最大传输量:	-1	-1为不限制
校验:	<input type="checkbox"/>	
进行流量实时统计:	<input type="checkbox"/>	
文件同步后所采取的操作:	删除	

文件同步服务配置

配置完成后点击“确定”按钮。

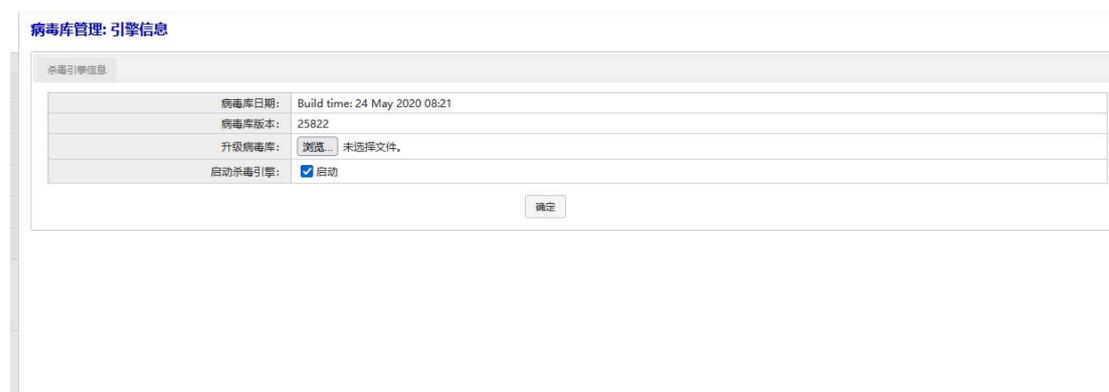
接收系统业务配置：

接收端系统参考发送端选择配置。

6.6 病毒库管理

6.6.1 引擎信息

在引擎信息管理页面，可以查看病毒库日期、病毒库版本，还可以升级病毒库。勾选【启动杀毒引擎】，开启杀毒引擎。



病毒库-引擎信息

6.6.2 隔离区管理

在引擎信息管理页面中启动杀毒引擎后，被拦截的病毒会在该页面显示出来。



病毒库-隔离区管理

7 用户管理员操作简介

7.1 用户配置

在浏览器地址栏输入：<https://192.168.1.254/index.php> 即出现发送系统管理系统登陆界面。输入用户名和密码即可登录。



用户管理-首页

在用户配置页面点击“新增用户按钮”，进入新增用户页面。

系统配置: 用户配置

用户 角色 密码强度设置

禁用:

用户名: *

密码: *

确认密码: *

角色: 系统管理员

保存

新增用户

- 禁用：勾选之后禁用此用户。
 - 用户名：字母和数字的组合。
 - 密码：密码必须包含特殊字符。
 - 确认密码：必须跟密码保持一致。
 - 角色：选择“系统管理员”、“日志审计员”或“管理员”；
- 角色： 查看所有管理员的操作权限以及各管理员的成员数量。

系统配置: 用户配置

组名	描述	成员数量
usermanager	用户管理管理员-只能访问用户配置页面, 有且仅有一个	1
admins	系统管理员-可以访问除用户配置之外的所有页面, 具有最高权限	1
manager	管理员-能查看(日志审计, 用户配置和登录设置)以外的所有页面, 但没有修改权限	0
logauditor	日志审计员-只能查看和操作日志审计页面	1

用户角色管理

8 日记审计员操作简介

8.1 日志与审计

在浏览器地址栏输入: <https://192.168.1.254/index.php> 即出现发送系统管理系统登陆界面。输入用户名: adminlog, 密码即可登录。



日志审计-首页

8.1.1 管理操作日志

管理操作日志中记录了管理员的所有操作, 可以根据查询条件(管理员、源 IP、事件、消息、级别、时间范围)来查看管理员对系统的操作。

日志与审计：管理操作日志

[导出日志](#) [清空日志](#)

查询条件

管理员: 源IP: 事件: 消息: 级别: 所有 ▾

时间范围: 到

显示: 1 到 3 共 3 条记录 第 1/1 页

序号	管理员	源	事件	消息	级别	配置时间
1	adminlog	192.168.5.109:53737	登陆管理界面	IP为192.168.5.109 用户名为adminlog的用户成功登录管理界面	消息	2020-11-12 15:37:33
2	adminlog	192.168.5.109:53734	退出管理界面	adminlog成功退出管理界面	消息	2020-11-12 15:37:26
3	adminlog	192.168.5.109:53732	清空管理操作日志	清空管理操作日志成功。	消息	2020-11-12 15:37:19

管理员日志

8.1.2 数据库抽取日志

数据库抽取日志中记录了管理员对数据库的操作，可以根据查询条件（业务名、服务名、数据流向、抽取表名、加载表名、时间范围）来查询数据库抽取日志。

日志与审计：数据库抽取日志

[导出日志](#) [清空日志](#)

查询条件

业务名: 数据流向: 抽取表名:

加载表名: 时间范围: 到

[首页](#) [«](#) [1](#) [2](#) [3](#) [»](#) [尾页](#)

日志详细列表如下 (注: 最多显示10000条记录) :

序号	业务名	数据流向	抽取表名	加载表名	抽取成功条数	抽取失败条数	时间
1	fyb2	586->686正向	TABLE04	TABLE04	3	0	2020-11-05 14:16:00
2	fyb2	586->686正向	TABLE04	TABLE04	1	0	2020-11-05 13:46:30
3	fyb2	586->686正向	TABLE04	TABLE04	1	0	2020-11-05 13:50:57
4	fyb2	586->686正向	TABLE04	TABLE04	1	0	2020-11-05 14:04:24
5	fyb2	586->686正向	TABLE04	TABLE04	1	0	2020-11-05 14:04:15
6	fyb2	586->686正向	TABLE04	TABLE04	4	0	2020-11-05 13:48:15
7	fyb2	586->686正向	TABLE04	TABLE04	5	0	2020-11-05 16:18:36
8	fyb2	586->686正向	TABLE04	TABLE04	1	0	2020-11-05 13:48:24
9	fyb2	586->686正向	TABLE04	TABLE04	1	0	2020-11-05 14:15:48
10	fyb2	586->686正向	TABLE04	TABLE04	1	0	2020-11-05 16:18:51
11	fyb2	586->686正向	TABLE04	TABLE04	1	0	2020-11-05 13:48:36
12	fyb2	586->686正向	TABLE04	TABLE04	1	0	2020-11-05 13:46:21
13	fyb2	586->686正向	TABLE04	TABLE04	2	0	2020-11-05 11:19:00
14	fyb2	586->686正向	TABLE04	TABLE04	4	0	2020-11-05 11:04:15

数据库同步抽取日志

8.1.3 数据库基本信息日志

数据库基本信息日志可以根据查询条件（业务名、服务名、业务流程号、级别、事件、时间范围）来查询，查看数据库状态是否正常。

日志与审计: 数据库基本信息日志

[导出日志](#) [清空日志](#)

查询条件

设备IP: 业务流程名: 事件: 等级:

事件消息内容: 时间范围: 到

首页 << 1 2 3 4 5 6 7 8 9 10 11 12 >> 尾页

日志详细列表如下 (注: 最多显示10000条记录) :

序号	设备ip	业务流程名	事件	等级	时间
1	172.26.78.2	与客户端进行通信交互	接收消息	0	2020-11-12 14:31:14
2	172.26.78.2	与客户端进行通信交互	打开会话	0	2020-11-12 14:31:14
3	172.26.78.2	与客户端进行通信交互	关闭会话	0	2020-11-12 14:31:14
4	172.26.78.2	与客户端进行通信交互	发送消息	0	2020-11-12 14:31:14
5	172.26.78.2	与客户端进行通信交互	接收消息	0	2020-11-12 14:30:44
6	172.26.78.2	与客户端进行通信交互	发送消息	0	2020-11-12 14:30:44
7	172.26.78.2	与客户端进行通信交互	接收消息	0	2020-11-12 14:30:44
8	172.26.78.2	与客户端进行通信交互	打开会话	0	2020-11-12 14:30:44
9	172.26.78.2	与客户端进行通信交互	发送消息	0	2020-11-12 14:30:44
10	172.26.78.2	与客户端进行通信交互	关闭会话	0	2020-11-12 14:30:44
11	172.26.78.2	与客户端进行通信交互	打开会话	0	2020-11-12 14:30:44
12	172.26.78.2	Get Version	Get Version	0	2020-11-12 10:00:08
13	172.26.78.2	触发器方式	[fyb2]700]尝试开启任务	0	2020-11-12 10:00:10
14	172.26.78.2	进行连接测试	加载国产数据库端	3	2020-11-12 10:00:07

数据库同步基本信息日志

8.1.4 文件同步日志

文件同步日志记录了所有文件同步产生的日志，可以根据查询条件（接收系统业务 ID、目录、文件名、操作状态）来查询，查看文件同步同步多少文件，文件同步是否成功。

日志与审计: 文件同步日志

文件同步日志 导出日志 清空日志

查询条件

业务ID: 文件名: 操作状态: 查询

首页 « 1 2 3 4 5 6 7 8 9 10 11 12 » 尾页

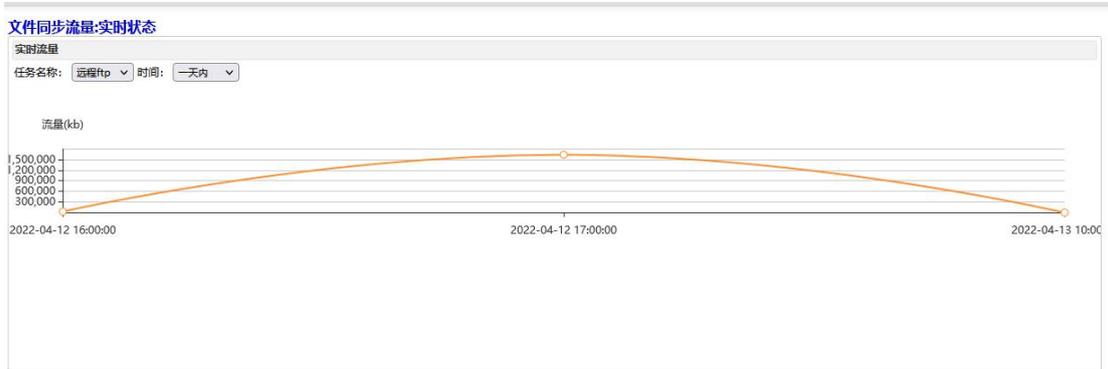
日志详细列表如下 (注: 最多显示10000条记录):

序号	内网业务ID	目录	文件名	大小	开始时间	完成时间	操作状态
1	667		mysql-connector-net-6.8.7.msi	11481088	2020-11-12 14:31:15	2020-11-12 14:31:15	成功
2	667		mysql-connector-net-6.8.7.msi	11481088	2020-11-12 10:57:52	2020-11-12 10:57:52	成功
3	667		mysql-connector-net-6.8.7.msi	11481088	2020-11-12 10:57:32	2020-11-12 10:57:32	成功
4	667		mysql-connector-net-6.8.7.msi	11481088	2020-11-12 09:52:01	2020-11-12 09:52:01	成功
5	667		mysql-connector-net-6.8.7.msi	11481088	2020-11-12 09:51:45	2020-11-12 09:51:45	成功
6	667		mysql-connector-net-6.8.7.msi	11481088	2020-11-12 09:51:26	2020-11-12 09:51:27	成功
7	667		mysql-connector-net-6.8.7.msi	0	2020-11-06 17:16:35	2020-11-06 17:16:35	成功
8	667		mysql-connector-net-6.8.7.msi	0	2020-11-06 15:25:11	2020-11-06 15:25:11	成功
9	667		mysql-connector-net-6.8.7.msi	6910829	2020-11-05 11:26:07	2020-11-05 11:26:07	成功
10	667		mysql-connector-net-6.8.7.msi	0	2020-11-05 11:25:39	2020-11-05 11:25:40	成功
11	667		mysql-connector-net-6.8.7.msi	0	2020-11-05 11:25:17	2020-11-05 11:25:17	成功
12	800	/	777788111.png	77133	2020-11-05 11:22:53	2020-11-05 11:22:53	成功
13	800	/	66664411.png	79871	2020-11-05 11:22:53	2020-11-05 11:22:53	成功
14	800	/	fastjson-1.2.16.jar	405317	2020-11-05 11:15:40	2020-11-05 11:15:40	成功

文件同步日志

8.1.5 文件同步流量

文件同步流量记录了所有文件同步产生的流量信息。



文件同步流量

8.1.6 通道操作日志

通道操作日志可以根据查询条件（业务 ID、描述、时间范围）来查询，可以查询从发送系统发送接收系统的通道信息是否成功。

日志与审计: 通道操作日志

导出日志 清空日志

查询条件

业务ID: 描述: 时间范围: 到 查询

首页 « 1 2 3 4 5 6 7 8 9 10 11 12 » 尾页

日志详细列表如下 (注: 最多显示10000条记录):

序号	业务ID	描述	时间
1	800	通道关闭, 源端口为 41505	2020-11-12 09:52:05
2	800	通道关闭, 源端口为 40233	2020-11-12 09:52:05
3	666	通道关闭, 源端口为 41184	2020-11-12 09:52:05
4	666	通道关闭, 源端口为 60690	2020-11-12 09:52:05
5	555	通道关闭, 源端口为 38733	2020-11-12 09:52:05
6	555	通道关闭, 源端口为 49822	2020-11-12 09:52:05
7	444	通道关闭, 源端口为 34727	2020-11-12 09:52:05
8	444	通道关闭, 源端口为 37977	2020-11-12 09:52:05
9	111	通道关闭, 源端口为 56308	2020-11-12 09:52:05
10	111	通道关闭, 源端口为 39829	2020-11-12 09:52:05
11	800	通道创建, 源端口为 41505	2020-11-12 09:52:05
12	800	通道创建, 源端口为 40233	2020-11-12 09:52:05
13	369	通道创建, 源端口为 41088	2020-11-12 09:52:05
14	369	通道创建, 源端口为 35396	2020-11-12 09:52:05
15	666	通道创建, 源端口为 41184	2020-11-12 09:52:05

通道操作日志

8.1.7 安全事件日志

安全事件日志查询非法访问等日志信息。

日志与审计: 安全事件日志

导出日志

查询条件

源IP: 目的IP: 级别: 所有

时间范围: 到 查询

显示: 1 到 10 共 0 条记录 第 1/0 页

序号	源IP	源端口	目的IP	目的端口	协议	动作	时间
						没有符合	

安全事件日志

8.1.8 告警日志

告警日志中记录了不能同步的文件，可以根据查询条件（业务 ID、告警模块、告警级别、描述、时间范围）来对报警日志进行查询。

日志与审计: 告警日志

导出日志 清空日志

查询条件

业务ID: 告警模块: 告警级别: 时间范围: 到

IP地址: 描述: 查询

首页 « 1 2 3 4 5 6 7 8 9 10 11 12 » 尾页

日志详细列表如下 (注: 最多显示500页):

序号	业务ID	所属模块	报警级别	IP	信息	时间
1	668	文件名过滤	告警		源端IP: 127.0.0.1目标端IP: 192.168.5.249;文件大小: 10240;服务: 668,黑名单文件后经过滤中...	2020-11-04 16:20:06
2	668	文件名过滤	告警		源端IP: 127.0.0.1目标端IP: 192.168.5.249;文件大小: 10240;服务: 668,黑名单文件后经过滤中...	2020-11-04 16:20:02
3	668	文件名过滤	告警		源端IP: 127.0.0.1目标端IP: 192.168.5.249;文件大小: 10240;服务: 668,黑名单文件后经过滤中...	2020-11-04 16:19:59
4	668	文件名过滤	告警		源端IP: 127.0.0.1目标端IP: 192.168.5.249;文件大小: 10240;服务: 668,黑名单文件后经过滤中...	2020-11-04 16:19:56
5	668	文件名过滤	告警		源端IP: 127.0.0.1目标端IP: 192.168.5.249;文件大小: 10240;服务: 668,黑名单文件后经过滤中...	2020-11-04 16:19:53
6	668	文件名过滤	告警		源端IP: 127.0.0.1目标端IP: 192.168.5.249;文件大小: 10240;服务: 668,黑名单文件后经过滤中...	2020-11-04 16:19:50
7	668	文件名过滤	告警		源端IP: 127.0.0.1目标端IP: 192.168.5.249;文件大小: 10240;服务: 668,黑名单文件后经过滤中...	2020-11-04 16:19:47
8	668	文件名过滤	告警		源端IP: 127.0.0.1目标端IP: 192.168.5.249;文件大小: 10240;服务: 668,黑名单文件后经过滤中...	2020-11-04 16:19:44
9	668	文件名过滤	告警		源端IP: 127.0.0.1目标端IP: 192.168.5.249;文件大小: 10240;服务: 668,黑名单文件后经过滤中...	2020-11-04 16:19:41
10	668	文件名过滤	告警		源端IP: 127.0.0.1目标端IP: 192.168.5.249;文件大小: 10240;服务: 668,黑名单文件后经过滤中...	2020-11-04 16:19:38
11	668	文件名过滤	告警		源端IP: 127.0.0.1目标端IP: 192.168.5.249;文件大小: 10240;服务: 668,黑名单文件后经过滤中...	2020-11-04 16:19:35
12	668	文件名过滤	告警		源端IP: 127.0.0.1目标端IP: 192.168.5.249;文件大小: 10240;服务: 668,黑名单文件后经过滤中...	2020-11-04 16:19:32
13	668	文件名过滤	告警		源端IP: 127.0.0.1目标端IP: 192.168.5.249;文件大小: 10240;服务: 668,黑名单文件后经过滤中...	2020-11-04 16:19:29

系统告警日志

8.1.9 认证状态日志

日志与审计: 认证状态日志

导出日志 清空日志

查询条件

业务ID: IP地址: 描述: 时间范围: 到 查询

首页 « 1 2 3 4 5 6 7 8 9 10 11 12 » 尾页

日志详细列表如下 (注: 最多显示500页):

没有查询到符合的数据

认证状态日志

8.1.10 日志管理设置

在日志管理设置页面中可以对日志进行常规设置，还可以配置 SNMP Traps 服务设置。

日志与审计: 日志管理设置

日志常规设置 SNMP Traps服务

启动远程syslog服务器:

远程服务器主机配置

IP	端口	描述
<input type="text"/>	<input type="text"/>	<input type="text"/>

启动SNMP服务器:

监听端口:

设备位置:

共同体:

SNMPv3:

当前日志存储空间:

报警阈值: KB

日志存档:

日志管理设置

日志与审计: 日志管理设置

日志常规设置 SNMP Traps服务

启用SNMP Traps:

SNMP Traps:

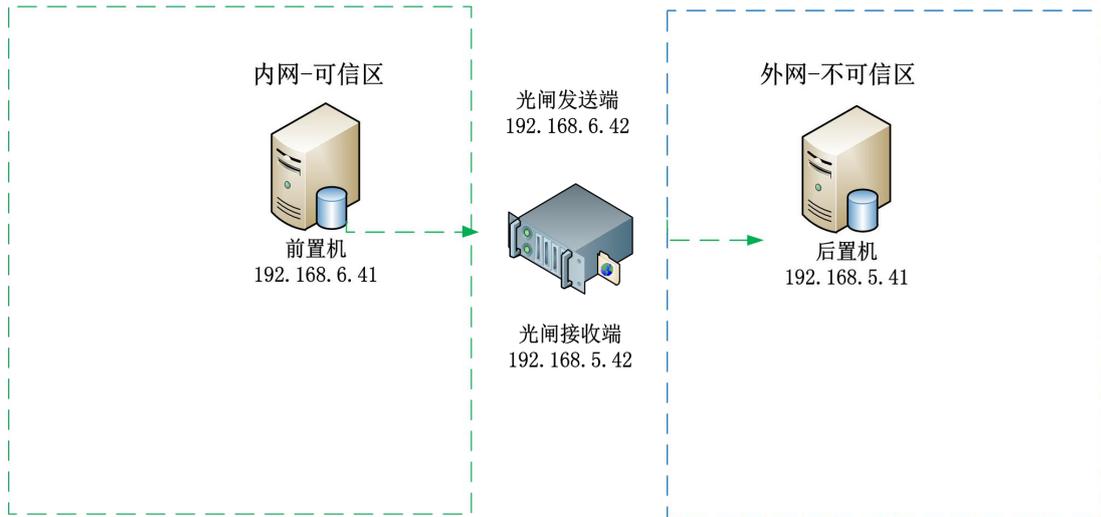
集控地址:	<input type="text"/>
集控端口:	<input type="text"/>
共同体:	<input type="text"/>
trap周期:	<input type="text"/>
在线检测网口:	<input type="text"/>
CPU使用率OID:	<input type="text"/>
磁盘使用率OID:	<input type="text"/>
内存使用率OID:	<input type="text"/>
接口流量OID:	<input type="text"/>
属性OID:	<input type="text"/>
在线状态OID:	<input type="text"/>
任务状态OID:	<input type="text"/>

系统 SNMP Trap 设置

9 典型配置

9.1 通道配置(与数据交换前后置配套使用)

一、案例拓扑



单向通道配置拓扑

二、操作流程

1. 进入伟思信安光闸发送系统进入光闸发送系统配置：

网络设置—>通道设置 dest_info.cnf：

序号	name	channel_num	proxy_addr	proxy_port	proxy_type	dest_addr	dest_port	dest_type	操作
1	dmon	123	172.26.78.1	5000	tcp	172.26.78.1	3355	tcp	
2	test	2	172.26.78.1	5000	tcp	192.168.5.41	3355	tcp	
3	red	44	172.26.78.1	5000	tcp	192.168.5.49	3355	tcp	

单向通道配置 dest_info.cnf

- name(标识):: appname 系统唯一，只允许英文和数字，例如 test；
- channel_num: appname 系统唯一 ID，数字，例如填写 22；
- proxy_addr: 默认 172.26.78.1；
- proxy_port: 5000；
- proxy_type: 默认 TCP；
- dest_addr: 对应光闸后端的 IP，例如 192.168.5.41；

- dest_port: 默认 3355;
- dest_type: 默认 TCP;
- 光闸前置地址(转发): 对应光闸前置地址, 例如 192.168.6.41;
- 光闸转发端口: 定义的转发端口, 例如: 9597。

填写完成后, 可参考如下图

name(标识):	test	
channel_num:	2	
proxy_addr:	172.26.78.1	
proxy_port:	5000	
proxy_type:	tcp	
dest_addr:	192.168.5.41	
dest_port:	3355	
dest_type:	tcp	
光闸前置地址(转发):	192.168.6.41	dest_addr等于172.26.78.1可忽略
光闸转发端口:	9597	dest_addr等于172.26.78.1可忽略

单向通道配置 dest_info.cnf

2. 进入伟思信安数据安全交换系统配置:

前置配置:

- 光闸 IP: 请填写【光闸发送端】业务通讯 IP;
- 对端前后置 IP: 请填写【数据交换对端前后置】业务通讯 IP;
- app name: 需与【光闸发送端】的 name 对应, 配置页面在网络配置->通道设置->目标端配置;
- channel num: 需与【光闸发送端】的 channel_num 对应, 配置页面在网络配置->通道设置->目标端配置;

光闸IP	192.168.6.42	请填写【光闸发送端】业务通讯IP
对端前后置IP	192.168.5.41	请填写【数据交换对端前后置】业务通讯IP
app name	test	需与【光闸发送端】的name对应, 配置页面在网络配置->通道设置->目标端配置
channel num	2	需与【光闸发送端】的channel_num对应, 配置页面在网络配置->通道设置->目标端配置

前置设置-发送端

后置配置：

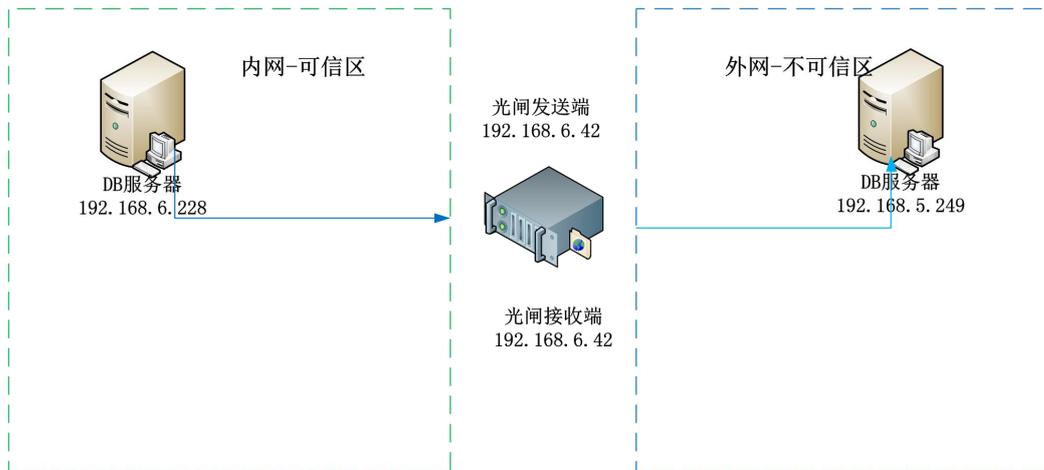
- wsg_frecvd 的接收地址 (recv_srv_addr)：



后置设置-接收端

9.2 配置数据库同步业务

一、案例拓扑



数据库同步业务拓扑

二、操作步骤

以 mysql 数据库同步为例：

发送系统任务配置：

1. 在发送系统系统的数据资源中创建 oracle 数据资源。
- 资源名称：可以是字母、数字、下划线、中文任意组合，如：mysql；

- 资源类型：可以是 Oracle、SQLServer、MySQL、DB2 等数据库类型，如：mysql；
- IP 地址：该数据库所在服务器的 IP 地址，如：192.168.6.228；
- 端口：数据库使用的端口号，如：3306；
- 同步帐号用户名：数据库同步账户用户名，如：admin；
- 同步帐号密码：数据库同步账户密码；
- 业务帐号用户名：数据库业务帐号用户名，如：root；
- 业务帐号密码：数据库业务帐号密码；
- 数据库：该资源所在的数据库名称，如：test；

然后点击“连接测试”按钮，连接成功后方可保存。

资源名称:	mysql
资源类型:	数据库服务器
数据库类型:	MySQL
IP地址:	192.168.6.228
端口:	3306
同步账号用户名:	admin
同步账号密码:
业务账号用户名:	root
业务账号密码:
数据库名:	test
模式名:	test
临时表前缀:	SYNCND_
触发器前缀:	SYNCND_TR_

连接测试 确定 取消

数据资源-1

2. 在业务与服务管理中创建 mysql 数据库同步任务。

- 服务名称：不能使用中文字符，只能纯英文或数字（或者英文数字组合），并且内接收系统的名称需保持一致；
- 服务 ID：不能使用中文字符，只能纯英文或数字（或者英文数字组合），并且内接收系统的名称需保持一致；

- 描述：描述不限制，可以填写，也可以不填写；

数据库同步

1. 服务定义 2. 服务属性配置 3. 业务表管理 4. 执行计划

服务名称 (内外请保持一致) dbsyncstest

服务ID (内外请保持一致) 1002

服务类型 客户端方式

描述

上一步 下一步

- 点击 **下一步** 按钮。

- 同步方式：

触发器方式：是指在接收系统数据库同步表中插入、删除、更新若干条数据后，发送系统数据库同步表中也自动同步插入、删除、更新了同样的数据。

普通全表同步方式：是指把整张表的数据都进行同步。

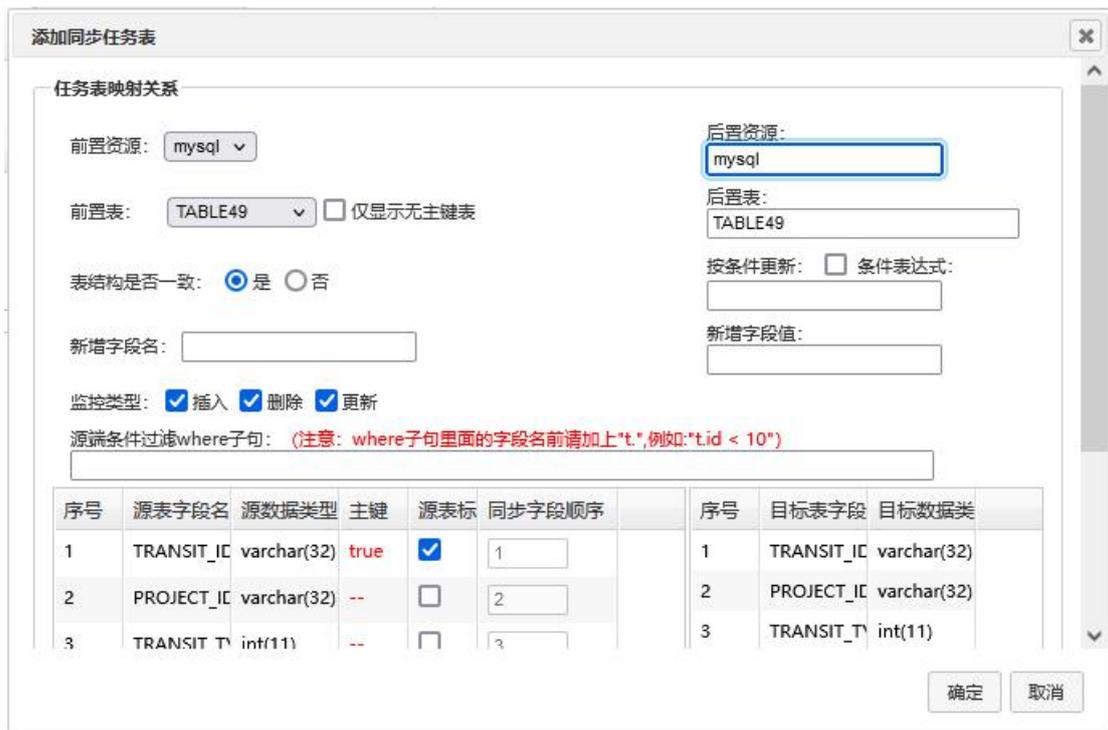
- 冗余传输：可选择冗余传输次数，默认为 1.
- 传输模式：可选择“高速模式”和“常规模式”，默认选择“高速模式”
- 记入日志：勾选则表示同步过程中文件写入到文件日志中，反之则不写入

点击 **下一步** 按钮。

点击 **添加同步任务表** 按钮。



数据库同步服务-编辑



数据库同步服务

时间间隔：系统默认是 3 秒，也可以自己根据需要填写。

点击  按钮。

完成配置后，在接收系统配置数据库业务配置页面。

数据同步：数据库同步服务：编辑

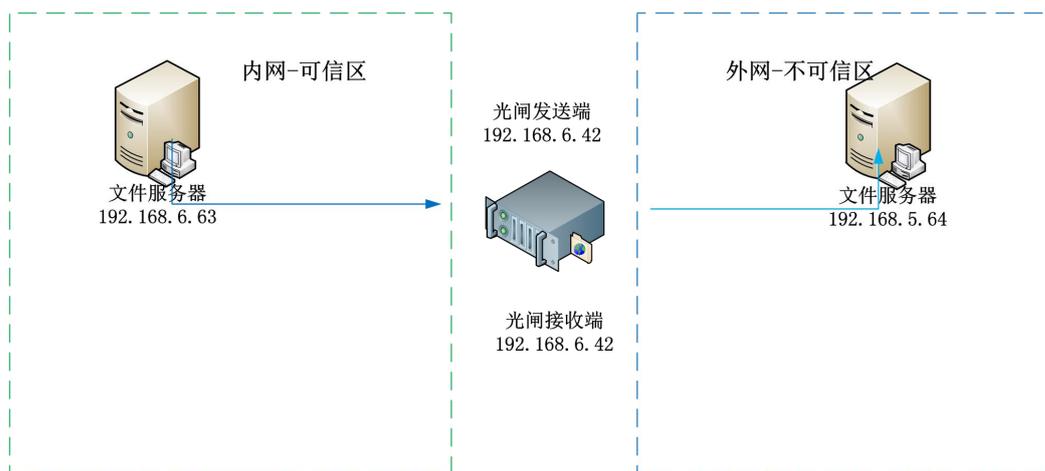


数据库同步服务

接收系统业务配置：可参考发送系统业务配置。

9.3 配置文件同步业务

一、案例拓扑



文件同步业务拓扑

二、操作步骤

以远程 FTP 同步为例：

发送系统业务配置：

在业务与服务管理中创建远程 FTP 任务；

- 发送系统业务 id：请输入大于 2 的业务 id，例如：1003；
- 服务名称：不能使用中文字符、只能单纯英文或数字（或者英文数字组合），例如：

ycftptest;

- 资源类型：选远程 FTP;
- 用户名：FTP 用户名;
- 密码：FTP 密码;
- 端口：FTP 端口;
- 同步间隔：设置同步间隔;
- 传输模式：选择“高速模式”或“常规模式”;
- 后缀名过滤：输入要过滤的文件名，多个用空格分开;
- 文件特征：文件特征包括“不审计”、“白名单”以及“黑名单”;
- 文件同步后所采取的操作：选择删除，则删除源端文件，选择复制，则保留源端文件;
- 关键字过滤：输入要过滤的关键字，多个关键字用“;”隔开。（.txt 文件中包含的关键字）;
- 过滤最小字节数：大于此数值才可以同步;
- 过滤最大字节数：小于此数值才可以同步;
- 开启病毒扫描：开启病毒扫描的条件是必须在【病毒库管理】>【引擎信息】中启动杀毒引擎，勾选开启病毒扫描，不勾选不开启;
- 病毒文件处理方式：选择删除，则删除病毒；选择隔离，则在【病毒库管理】>【隔离区管理】中可以查看到被隔离的病毒文件;

数据同步: 文件同步服务配置: 编辑

文件同步服务编辑

内网服务id:	1003	注意:请输入大于2的服务id
服务名称:	filesyncdest	
资源类型:	远程FTP	
用户名:	ftp1	
密码:	*****	
IP地址:	192.168.6.63	
端口:	21	
同步间隔:	3000	毫秒
编码:	UTF-8	
传输模式:	高速下载	
显示高级设置:	<input checked="" type="checkbox"/>	
并发数:	5	
文件同步后所采取的操作:	删除	
后增量过滤:		
超时时间(秒):	60	
ftp同步模式:	专用	
文件特征:	不审计	添加文件
启用监控目录清理:	<input type="checkbox"/>	
关键字过滤:		
过滤最小字节数:		

文件同步服务配置

配置完成后点击“确定”按钮。

接收系统业务配置：可参考发送系统业务配置。