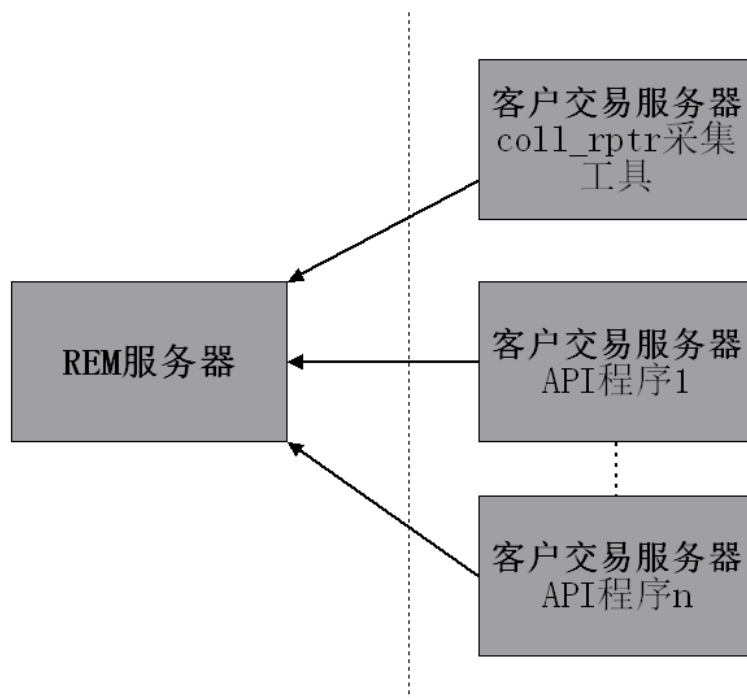


1 综述

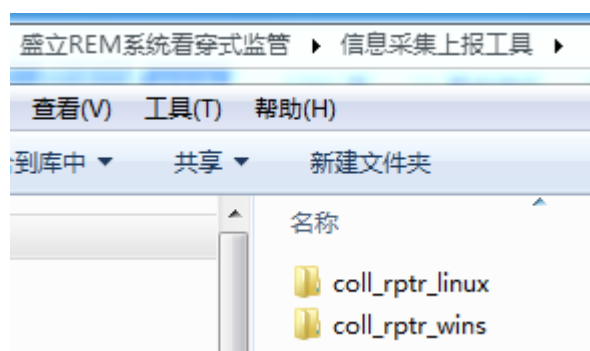
盛立 REM 系统看穿式监管实现的改造方案，采用了“独立信息采集上报工具”（coll_rptr）、客户的 API 程序“双路确认”的模式。需要在交易服务器上面，先运行采集工具（后续称为 coll_rptr），实现定时的信息上报，然后才能启动 API 程序登录 REM。API 程序在登录时必须使用 coll_rptr 里面配置过的 logon id、app id 及授权码。**API 版本不需要升级。**



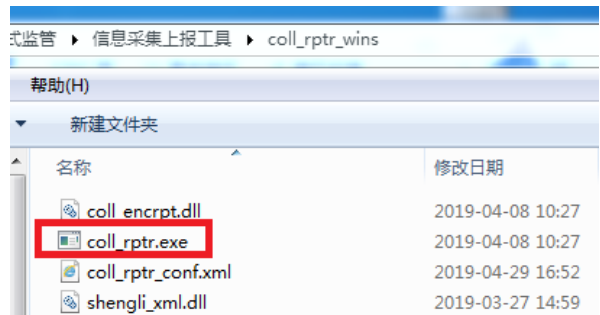
coll_rptr 工具在同一台服务器上面，只需运行一个实例即可，可配置多个用户的方式运行。api 程序在交易时，需要一直开着 coll_rptr 工具，以确保定时采集并上报信息。

2 信息采集上报工具

信息采集工具，分为 wins 版与 linux 版两个：



2.1 wins 采集工具



完成 coll_rptr_conf.xml 的参数配置以后，运行 coll_rptr_conf.exe 即可。配置参数如下：

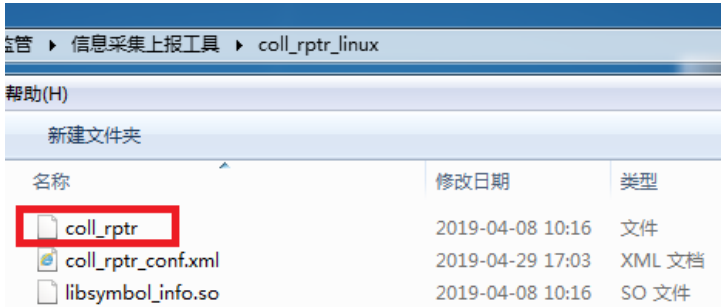
```
<?xml version="1.0" encoding="utf-8"?>
<config>
  <server_info ip="10.1.59.42" port="20001"/>
  <enable_log status="1"/>
  <clients rptr_time="300" reconnect_time="5">
    <client app_id="111" auth_id="111111" login_id="test001" password="1" />
    <client app_id="222" auth_id="222222" login_id="test002" password="1" ip="10.1.59.42"/>
    <client app_id="333" auth_id="333333" login_id="test003" password="1" ip="" />
  </clients>
</config>
```

参数说明：

序号	参数	描述
1	server_info ip	REM 服务器的查询 IP（注意下采集工具是连网卡的，不是 FPGA）
2	port	REM 服务器的查询端口
3	enable_log	自动重连开关，缺省开启
4	rptr_time	定时上报时间间隔（单位：秒），默认值 300，及 5 分钟上报一次
5	reconnect_time	采集工具断开重连时间（单位：秒），默认值 5
6	app_id	app id
7	auth_id	授权码
8	login_id	登录 ID（即用户名），用来登录 REM 使用
9	password	密码
10	ip	IP 地址，可以不用填，采集工具会自动采集交易段 IP

2.2 linux 采集工具

可执行程序为 coll_rptr（拷贝到 linux 以后可以用 chmod 命令为其授权执行权限）：



coll_rptr_conf.xml 为配置文件，与 wins 下一模一样。

需要注意的是，Linux 下**必须在 root 用户下面运行**，才能采集到完整的信息。

2.3 采集信息说明

在 linux 下运行采集工具（wins 下类似，只是绝大部分用户都是 linux 的），可以获取到需要采集上报的信息（返回 **succeed** 说明成功）：

```
use pubkey data!!!
-----system info-----
bios_serial_num: SystemSeri
collect_time: 2019-04-29 15:52:33
cpu_serial_num: A5060100FFFBEBBF
device_name: localhost
hd_serial_num: WD-WCC3F6JUH8JH
os_vesion: 6.4
private_ip1: 10.1.53.184
private_ip2:
private_mac1: 20CF3058729C
private_mac2:
disk_part: linux don't need
terminal_type: 2
-----
send app_id:client send login_id:3866008
on_tcp_client_data_recv
app_id:client login_id:3866008 user_id:16 report_result:succeed

use pubkey data!!!
-----system info-----
bios_serial_num: SystemSeri
collect_time: 2019-04-29 15:52:33
cpu_serial_num: A5060100FFFBEBBF
device_name: localhost
hd_serial_num: WD-WCC3F6JUH8JH
os_vesion: 6.4
private_ip1: 10.1.53.184
private_ip2:
private_mac1: 20CF3058729C
private_mac2:
disk_part: linux don't need
terminal_type: 2
-----
send app_id:client send login_id:38660081
on_tcp_client_data_recv
app_id:client login_id:38660081 user_id:17 report_result:succeed
```

采集内容如下：

变量	采集内容	变量	采集内容
bios_serial_num	BIOS 序列号	collect_time	采集时间
cpu_serial_num	CPU 序列号	device_name	设备名
hd_serial_num	硬盘序列号	os_vesion	操作系统版本
private_ip1	IP 地址 1	private_mac1	MAC 地址 1
disk_part	系统盘分区信息	terminal_type	终端类型

2.4 采集工具失败的情况

(1) 连了一套还不支持看穿式的 REM 系统

```
on_tcp_client_connected
connecting...
on_tcp_client_connected

use pubkey data!!!
-----system info-----
bios_serial_num: SystemSeri
collect_time: 2019-04-29 17:29:19
cpu_serial_num: A5060100FFFBEBBF
device_name: localhost
hd_serial_num: WD-WCC3F6JUH8JH
os_vesion: 6.4
private_ip1: 10.1.53.184
private_ip2:
private_mac1: 20CF3058729C
private_mac2:
disk_part: linux don't need
terminal_type: 2
-----
send app_id:client send login_id:3866008
on_tcp_client_remote_disconnected

use pubkey data!!!
-----system info-----
bios_serial_num: SystemSeri
collect_time: 2019-04-29 17:29:19
cpu_serial_num: A5060100FFFBEBBF
device_name: localhost
hd_serial_num: WD-WCC3F6JUH8JH
os_vesion: 6.4
private_ip1: 10.1.53.184
private_ip2:
private_mac1: 20CF3058729C
private_mac2:
disk_part: linux don't need
terminal_type: 2
-----
send app id:client send login id:38660081
on_tcp_client_remote_disconnected
```

连接建立以后，会立即断开！

(2) 查询地址错误

```
root:/home/user0/ldq/kanchuanshi/linux_kanchuanshi>./coll_rptr
not set conf file, using default file: coll_rptr_conf.xml (y/n)y
connecting...
17:32:57: [connect failed]
enter any key to exit
```

(3) app id 错误

```
-----system info-----
bios_serial_num: SystemSeri
collect_time: 2019-04-29 18:42:29
cpu_serial_num: A5060100FFFBEBBF
device_name: localhost
hd_serial_num: WD-WCC3F6JUH8JH
os_vesion: 6.4
private_ip1: 10.1.53.184
private_ip2:
private_mac1: 20CF3058729C
private_mac2:
disk_part: linux don't need
terminal_type: 2
-----
send app_id:client_ send login_id:38660081
on_tcp_client_data_recv
app_id:client_ login_id:38660081 user_id:0 report_result:appid error
█
```

(4) 授权码错误

```
-----system info-----
bios_serial_num: SystemSeri
collect_time: 2019-04-29 18:41:38
cpu_serial_num: A5060100FFFBEBBF
device_name: localhost
hd_serial_num: WD-WCC3F6JUH8JH
os_vesion: 6.4
private_ip1: 10.1.53.184
private_ip2:
private_mac1: 20CF3058729C
private_mac2:
disk_part: linux don't need
terminal_type: 2
-----
send app_id:client send login_id:38660081
on_tcp_client_data_recv
app_id:client login_id:38660081 user_id:0 report_result:appid error
█
```

(5) 采集工具用户名密码错误

```
-----system info-----
bios_serial_num: SystemSeri
collect_time: 2019-04-29 18:45:41
cpu_serial_num: A5060100FFFBEBBF
device_name: localhost
hd_serial_num: WD-WCC3F6JUH8JH
os_vesion: 6.4
private_ip1: 10.1.53.184
private_ip2:
private_mac1: 20CF3058729C
private_mac2:
disk_part: linux don't need
terminal_type: 2
-----
send app_id:client send login_id:38660081
on_tcp_client_data_recv
app_id:client login_id:38660081 user_id:0 report_result:login_id or password error
█
```

(6) IP 地址填写错误

IP 地址填错的情况, coll_rpnr 工具仍然会返回 succeed, 但会造成获取不到 mac 地址。所以, 必须确保填写正确的交易段 IP, 否则采集上报的信息里面将会因缺省 mac 而信息不完整。

3 API 程序

3.1 API 版本说明

REM 服务端版本	目前客户主要用的 API 版本	最新的 API 版本
普通版（不支持 UDP 报单）	rem_api_2.0.3.45	rem_api_2.0.3.51
极致版（支持 UDP 报单）	rem_api_3.1.3.48	rem_api_3.1.3.49

从 45 - 51 版本的 api 均相互兼容，REM 服务端升级到支持“看穿式监管”的版本后，客户的 api 版本可以不升级，继续使用老版本 api（当然也可以选择使用更新版本的 api）。

3.2 API 程序参数修改

EesTraderApi.h 文件：

```
305 // 用户登录
306
307 // \brief 这里输入的不是帐户名，是用户名
308 // \param const char* userId 用户名
309 // \param const char* userPwd 用户登录密码
310 // \return RESULT 返回值，参考 EesTraderErr.h 文件
311
312 virtual RESULT UserLogon(const char* user_id, const char* user_pwd, const char* prodInfo, const char* macAddr) = 0 ;
313
```

填入参数说明：

序	参数	填入值	最大长度
1	prodInfo	app id	29 字节
2	macAddr	auth_id（授权码）	17 字节

客户的程序的处理，分为两种情况：

第一、这两个参数的赋值，是硬代码程序里面写死的，这种情况下需要修改代码、重编译后进行替换；

第二、通过读配置文件（或者读数据库）的方式实现的，这种实现方式只需要修改下配置而不需要修改代码。比如读 ini 配置（具体可以参考 rem_penetrating_supervision_demo）：

```
1 [StrategyParam]
2 TraderServerIp=10.1.53.194
3 TraderServerPort=20000
4 TraderServerUdpPort=0
5 QueryServerIp=10.1.53.194
6 QueryServerPort=20001
7 LocalTradeIp=10.1.53.61
8 LocalTradeUdpPort=0
9 LogonId=38660081
10 LogonPwd=8
11 Account=3866008
12 AppId=client
13 AuthCode=client_auth_code
14
15
```

3.3 API 程序登录失败的情况

使用过盛立API的用户都知道，客户端程序发起登录请求UserLogon()，只要登录函数返回0（函数调用返回成功），则回调函数OnUserLogon()会被触发：

```
void TraderDemo::OnUserLogon(EES_LogonResponse* pLogon)
{
    switch(pLogon->m_Result)
    {
        case 0: cout << "Logon successfully! trading date is " << pLogon->m_TradingDate << ", token is " << pLogon->m_MaxToken << endl; break;
        case 1: cout << "pLogon->m_Result = " << "1, 用户名或密码错误!" << endl; break;
        case 2: cout << "pLogon->m_Result = " << "2, 该用户未绑定任何资金账户!" << endl; break;
        case 3: cout << "pLogon->m_Result = " << "3, 用户重复登录（后台配置成非互踢模式时）!" << endl; break;
        case 4: cout << "pLogon->m_Result = " << "4, 已经登录成功后，再次登录!" << endl; break;
        case 5: cout << "pLogon->m_Result = " << "5, 缺少客户端标识、mac地址!" << endl; break;
        case 6: cout << "pLogon->m_Result = " << "6, 系统内部错误!" << endl; break;
        case 8: cout << "pLogon->m_Result = " << "8, 连接查询通道失败!" << endl; break;
        case 99: cout << "pLogon->m_Result = " << "99, 服务器目前环境恶劣，内存、硬盘等空间不足，所有登录都被禁止!" << endl; break;
        // 11 12 13 为与看穿式监管相关的错误
        case 11: cout << "pLogon->m_Result = " << "11, 无合法采集信息，登录失败!" << endl; break;
        case 12: cout << "pLogon->m_Result = " << "12, 采集上报和交易端的远端IP不同，登录失败!" << endl; break;
        case 13: cout << "pLogon->m_Result = " << "13, 校验授权码错误，登录失败!" << endl; break;
        default: cout << "logon value unnormal!";
    }
}
```

返回 11, 12, 13 的错误，均是看穿式监管相关的错误。

（1）返回11，无合法采集信息，登录失败

场景：用户未运行“信息采集上报工具”或采集工具填的认证信息与 API 登录时填入的认证信息不一致（也就相当于没有运行采集工具），直接用 API 程序登录：

```
user0: /ldq/kanchuanshi/rem_penetrating_supervision_demo/bin/linux>./rem_penetrating_supervision_demo
pLogon->m_Result = 11, 无合法采集信息，登录失败!
client readline error(n_recved=-1, errno=104)
event_client_error, will close this sockt
disconnect from rem server(2), remote disconnected!
disconnect from rem server(3), local disconnected!
```

此时登录会失败，API 程序连接断开。

（2）返回12，采集上报和交易端的远端IP不同，登录失败

场景：用户在 A 服务器上面运行“信息采集上报工具”，在 B 服务器上面登录 API 程序：

```
user0: /ldq/kanchuanshi/rem_penetrating_supervision_demo/bin/linux>./rem_penetrating_supervision_demo
pLogon->m_Result = 12, 采集上报和交易端的远端IP不同，登录失败!
client readline error(n_recved=-1, errno=104)
event_client_error, will close this sockt
disconnect from rem server(2), remote disconnected!
disconnect from rem server(3), local disconnected!
```

此时登录也会失败，API 程序连接断开。证明该方案并不存在跨服务器使用的漏洞。

（3）返回13，校验授权码错误，登录失败

场景：用户 API 程序里面，填入了错误的授权码：

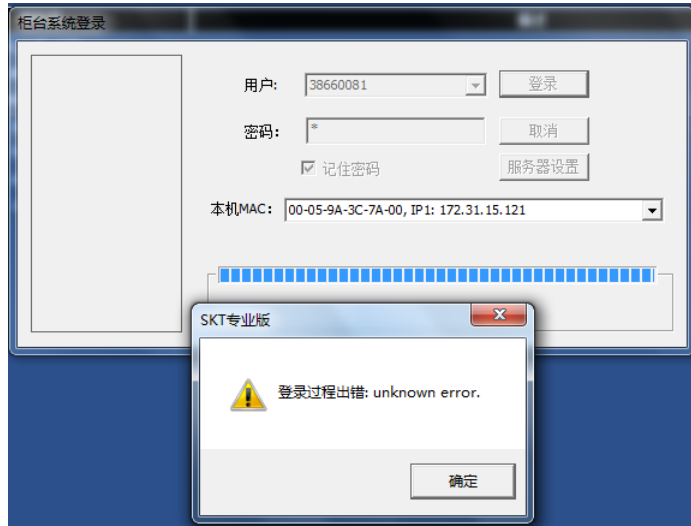
```
user0: /ldq/kanchuanshi/rem_penetrating_supervision_demo/bin/linux>./rem_penetrating_supervision_demo
pLogon->m_Result = 13, 校验授权码错误，登录失败!
client readline error(n_recved=-1, errno=104)
event_client_error, will close this sockt
disconnect from rem server(2), remote disconnected!
disconnect from rem server(3), local disconnected!
```

此时登录也会失败，API 程序连接断开。

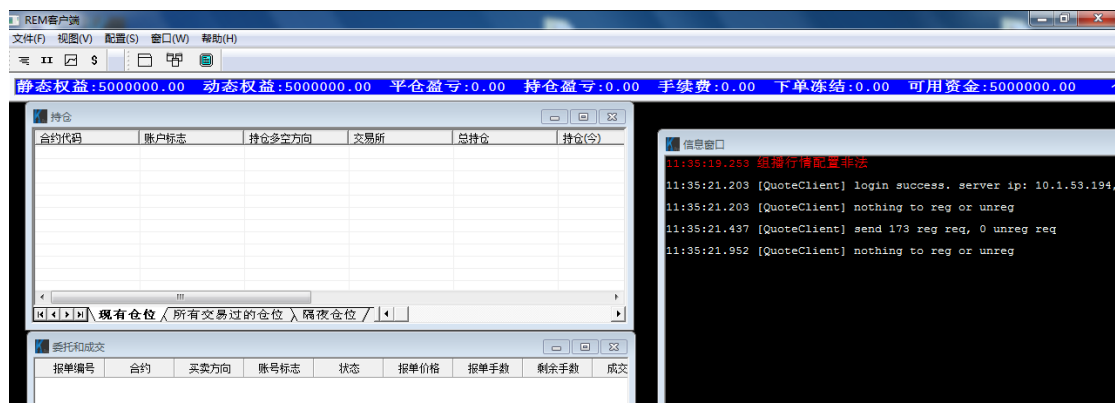
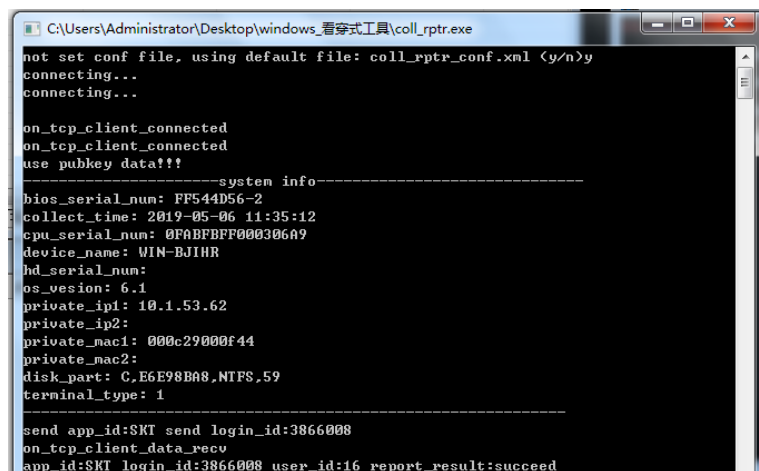
3.4 SKT 客户端

SKT 的 app id 及授权码，是写死的，appid = SKT，授权码 = skt_auth_code。

没有运行 wins 采集工具（并填入正确的 appid 及授权码）的情况下，登录 SKT 会报错：



运行采集上报工具后，可以登录 SKT：



4 期货公司后台人员界面配置

4.1 APPID 及授权码配置

在账户管理界面，增加了 APPID 及授权码管理 TAB 页。点击添加按钮后，手工输入 APPID-授权码（appid 最大长度 29，授权码最大长度 17），点击创建即可：

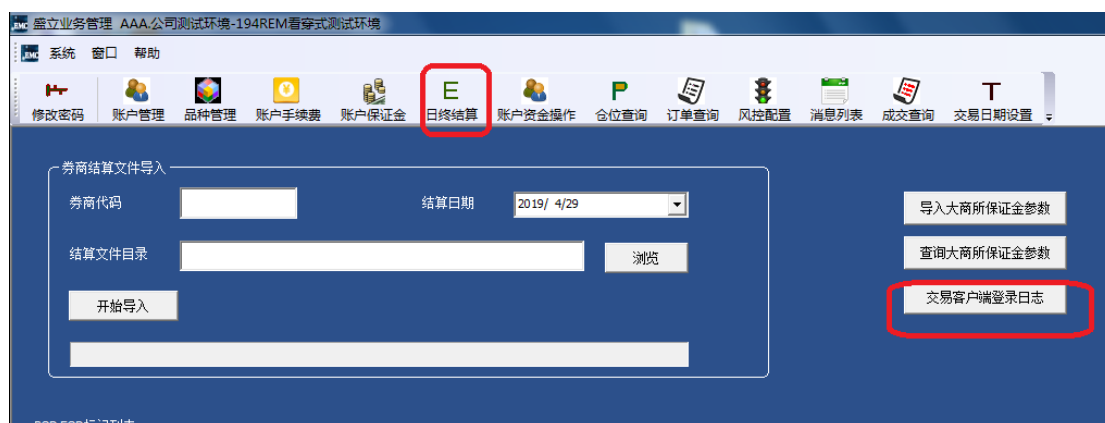


appid 与授权码配置实时上场。

另外，新版本支持了导入、导出的功能，也可以将主席上面的 APPID-授权码导出后，再导入到盛立系统。

4.2 导出交易客户端日志

在日终结算界面，增加了导出交易客户端日志功能：



点击后会弹出窗口：

交易客户端登录日志

交易日: 2019/ 4/29 登录ID: 用户ID: 是否代理: 查询

APPID: 授权码: 导出

交易日期	登录ID	用户ID	登录时间	APPID	授权码	加密信息	是否代理
20190429	3866008	16	2019-04-29 11:33:01	SPT_pro ...	shengli123	shengli@1@VOeK7c...	否
20190429	38660081	17	2019-04-29 13:51:41	SPT_pro ...	shengli123	shengli@1@TIXECO...	否
20190429	38660081	17	2019-04-29 13:56:00	client	client_au...	shengli@1@BW1Rg...	否
20190429	38660081	17	2019-04-29 14:01:15	client	client_au...	shengli@1@BW1Rg...	否
20190429	38660081	17	2019-04-29 14:03:37	SKT	skt_auth...	shengli@1@8H+TV...	否

客户端信息加密保存，可以导出 txt 文档。